35ª ALTERAÇÃO E CONSOLIDAÇÃO CONTRATUAL DA SOCIEDADE EMPRESARIAL "SUPRISERVI COMÉRCIO REPRESENTAÇÕES E SERVIÇOS LTDA''.

JOSÉ ALVES MUNIZ JÚNIOR

Brasileiro, casado no regime da comunhão parcial de bens, nascido em 19/06/1968, empresário, Registro Geral nº 638.963 SSP-AL, CPF: nº. 349.227.334-34, residente e domiciliado à Rua General Abreu e Lima, 233 - Apto.402 - Rosarinho – CEP: 52041-040 - Recife/PE.

CARLA FERNANDA DE ALMEIDA MONTEIRO MUNIZ

Brasileira, casada no regime da comunhão parcial de bens, nascida em 28/03/1970, empresária, Registro Geral nº 6.394.352 SDS/PE, CPF nº 724.940.694-91, residente e domiciliada à Rua General Abreu e Lima, 233 - Apto.402 - Rosarinho – CEP: 52041-040 - Recife/PE.

LUCINDA MUNIZ

Brasileira, solteira, nascida em 28/10/1953, empresária, Registro Geral nº 1.623.530 SSP/PE, CPF nº 271.069.344-53, residente e domiciliada no Parque Residencial Jatiúca, Quadra F, Bloco C 04, Apto. 01 – CEP: 57037-190 - Maceió/AL.

Os sócios da sociedade limitada de nome empresarial **SUPRISERVI COMÉRCIO REPRESENTAÇÕES E SERVIÇOS LTDA**, com sede em na Av. Governador Agamenon Magalhães, nº 4779, sala 401, Edf. Isaac Newton, e salas: 402, 403, 404, Ilha do Leite, Recife/PE, CEP: 50.070-425. , inscrita no CNPJ sob o nº **12.707.105/0001-64**, constituída legalmente com o contrato social devidamente registrado e arquivado na junta comercial do Estado de Pernambuco (JUCEPE) sob o nº **26.2.0131970-7** em 12 de agosto de 1987, resolvem: alterar, adequar e consolidar o contrato social, nos termos da Lei nº 10.406/202, mediante as condições estabelecidas nas cláusulas destacadas abaixo:

DA ATUALIZAÇÃO DE ENDEREÇO DOS SOCIOS NO PREÂMBULO

28/11/2019

Certifico o Registro em 28/11/2019
Arquivamento 20198199724 de 28/11/2019 Protocolo 198199724 de 08/11/2019 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 115640199432162

CLAUSULA PRIMEIRA: A sócia **LUCINDA MUNIZ**, Brasileira, solteira, nascida em 28/10/1953, empresária, Registro Geral nº 1.623.530 SSP/PE, CPF nº 271.069.344-53, residente e domiciliada no Parque Residencial Jatiúca, Quadra F, Bloco C 04, Apto. 01 – CEP: 57037-190 - Maceió/AL. **Passa a parti desse alteração ao seguinte endereço:** Parque Residencial, Jatiuca, S/N, APTº 01, Quadra F, Bloco 04, Maceió-AL, CEP: 57.035-610.

CLAUSULA SEGUNDA: O sócio **JOSÉ ALVES MUNIZ JÚNIOR,** Brasileiro, casado no regime da comunhão parcial de bens, nascido em 19/06/1968, empresário, Registro Geral nº 638.963 SSP-AL, CPF: nº. 349.227.334-34, residente e domiciliado à Rua General Abreu e Lima, 233 - Apto.402 - Rosarinho – CEP: 52041-040 - Recife/PE. **Passa a parti desse alteração ao seguinte endereço:** Rua General Abreu e Lima, 233 - Apto.402 - Rosarinho – CEP: 52.041-042- Recife/PE.

CLAUSULA TERCEIRA: A sócia **CARLA FERNANDA DE ALMEIDA MONTEIRO MUNIZ,** Brasileira, casada no regime da comunhão parcial de bens, nascida em 28/03/1970, empresária, Registro Geral nº 6.394.352 SDS/PE, CPF nº 724.940.694-91, residente e domiciliada à Rua General Abreu e Lima, 233 - Apto.402 - Rosarinho – CEP: 52041-040 - Recife/PE. **Passa a parti desse alteração ao seguinte endereço:** Rua General Abreu e Lima, 233 - Apto.402 - Rosarinho – CEP: 52.041-042- Recife/PE

DA ALTERAÇÃO DO ENDEREÇO DA FILIAL ARACAJU

CLAUSULA QUARTA: A **FILIAL ARACAJÚ**, situada à Av. Dep. Silvio Teixeira, nº 1300 Empresarial Carlos Cunha, salas 113 e 144, Grageru, Aracaju/SE, CEP: 49.025-100, inscrita no CNPJ sob o nº **12.707.105/0002-45** e inscrição estadual sob o nº 27.084.831.2, devidamente registrada e arquivada na Junta Comercial do Estado de Sergipe sob o NIRE sob o nº **28.9.0005304-0. Passa a partir dessa alteração a ter o seguinte sito como endereço:** situada à Av. Dep. Silvio Teixeira, nº 1300, sala 114, 1º andar, Grageru, Aracaju/SE, CEP: 49.025-400.

28/11/2019

Certifico o Registro em 28/11/2019
Arquivamento 20198199724 de 28/11/2019 Protocolo 198199724 de 08/11/2019 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 115640199432162

EM VIRTUDE DAS ALTERAÇÕES ACIMA, CONSOLIDA-SE O CONTRATO SOCIAL, NOS TERMOS DA LEI Nº 10.406/2002, QUE DORAVAMENTE PASSARÁ A VIGORAR MEDIANTE AS CONDIÇÕES E CLÁUSULAS SEGUINTES:

CLÁUSULA PRIMEIRA - DO NOME EMPRESARIAL

A sociedade gira sob o nome empresarial **SUPRISERVI COMÉRCIO REPRESENTAÇÕES E SERVIÇOS LTDA.**

CLÁUSULA SEGUNDA - DA SEDE, NOME DE FANTASIA E FILIAIS.

A sociedade tem sede em Recife/PE, à Av. Governador Agamenon Magalhães, nº 4779, sala 401, Edf. Isaac Newton, e salas: 402, 403, 404, Ilha do Leite, Recife-PE, CEP: 50.070-425., e está inscrita no CNPJ sob o nº **12.707.105/0001-64**, com a inscrição estadual **0201069-04**, tendo sido constituída legalmente com contrato social devidamente registrado e arquivado na Junta Comercial do Estado de Pernambuco sob o NIRE sob o nº **26.2.0131970-7.**

PARÁGRAFO PRIMEIRO – A sociedade possui o nome fantasia **NEWSUPRI**.

PARÁGRAFO SEGUNDO- A sociedade possui as seguintes filiais:

FILIAL ARACAJÚ, situada à Av. Dep. Silvio Teixeira, nº 1300, sala 114, 1º andar, Grageru, Aracaju/SE, CEP: 49.025-400, inscrita no CNPJ sob o nº **12.707.105/0002-45** e inscrição estadual sob o nº 27.084.831.2, devidamente registrada e arquivada na Junta Comercial do Estado de Sergipe sob o NIRE sob o nº **28.9.0005304-0.**

FILIAL MACEIÓ: Situada à Rua José Soares Sobrinho, nº 119, sala 903, Empresarial Le Monde, Jatiúca, Maceió/AL, CEP: 57036-640, inscrita no CNPJ sob o nº **12.707.105/0003-26** e na inscrição estadual sob o n º **24.072.844-0**, devidamente registrada e arquivada na Junta Comercial do Estado de Alagoas sob o NIRE sob nº **27.9.0008801-2**.

28/11/2019

Certifico o Registro em 28/11/2019
Arquivamento 20198199724 de 28/11/2019 Protocolo 198199724 de 08/11/2019 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 115640199432162

FILIAL OLINDA: Situada à Av. Presidente Kennedy, nº 1001, sala 216, bloco D, Peixinhos, Olinda/PE, CEP: 53.230-630, inscrita no CNPJ sob o nº **12.707.105/0006-79**, devidamente registrada e arquivada na Junta Comercial do Estado de Pernambuco sob o NIRE sob nº **26.9.0052171-8**.

PARÁGRAFO TERCEIRO- A sociedade poderá, a qualquer tempo, abrir ou fechar filial ou outra dependência, mediante alteração contratual, desde que aprovado pelos votos correspondentes dos sócios, no mínimo, a três quartos do capital social, nos termos do art. 1.076 da Lei nº 10.406/2002.

CLÁUSULA TERCEIRA - DO OBJETO SOCIAL

A sociedade tem por objeto prestação de serviços de Consultoria em Tecnologia da Informação (**6204-0-00**); Implementação, Suporte, Manutenção de computadores e de equipamentos periféricos (**6209-1-00**); Treinamento em Tecnologia da Informação (**8599-6-03**); Tratamento de Dados, Provedores de Serviços de Aplicações e Serviços de Hospedagem na Internet (**6311-9-00**); Aluguel de Maquinas e Equipamentos para escritórios (**7733-1-00**); Comercio Varejista especializado de equipamentos e suprimentos de informática (**4751-2-01**); Importação e Exportação de mercadorias e serviços (**4614-1-00**); Reparação e Manutenção de computadores e de equipamentos periféricos (**9511-8-00**); Representação Comercial e agentes do comércio de máquinas, equipamentos, e aeronave (**4614-1-00**), Fornecimento e Gestão de Recursos para terceiros (**7830-2-00**), todos estes ligados à Tecnologia da Informação.

PARÁGRAFO ÚNICO- A sociedade desenvolverá suas atividades, conforme seus interesses, sendo permitida a sua participação em qualquer outro tipo de sociedade.

CALUSULA QUARTA - DO PRAZO DE DURAÇÃO

O prazo de duração da sociedade é por tempo indeterminado.

28/11/2019

Certifico o Registro em 28/11/2019
Arquivamento 20198199724 de 28/11/2019 Protocolo 198199724 de 08/11/2019 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 115640199432162

CLÁUSULA QUINTA - DO CAPITAL SOCIAL

O capital social é de **R$ 204.000,00 (duzentos e quatro mil reais)**, sendo dividido em 204.000,00 (duzentos e quatro mil) quotas no valor nominal de R$ 1,00 (um real) cada uma, integralizadas em moeda corrente do país e assim divididas entre sócios.

NOME DOS SOCIOS	QUOTAS	%	VALOR
JOSE ALVES MUNIZ JÚNIOR	201.042	98,55	201.042,00
CARLA FERNANDA DE ALMEIDA MONTEIRO MUNIZ	2.040	1,00	2.040,00
LUCINDA MUNIZ	918	0,45	918,00
TOTAIS	204.000	100,00	204.000,00

PARÁGRAFO PRIMEIRO – As quotas são indivisíveis e não poderão ser cedidas ou transferidas a terceiros sem consentimentos dos outros sócios, aos quais ficam assegurados, em igualdade de condições e peço direito de preferência para a sua aquisição, se posta a venda, formalizando, se realizada a cessão delas, a devida alteração contratual.

PARÁGRAFO SEGUNDO - A responsabilidade de cada sócio é restrita ao valor de suas quotas, mas todos respondem solidariamente pela integração do capital social, nos termos do art. 1.052 da Lei nº 10.406/02.

CLÁUSULA SEXTA - DA ADMINISTRAÇÃO DA SOCIEDADE E PRO LABORE

A administração da sociedade caberá ao sócio, **JOSE ALVES MUNIZ JUNIOR,** com os poderes e atribuições de representação ativa e passiva na sociedade, judicial e extrajudicialmente, podendo praticar todos os atos compreendidos no objeto social, sempre de interesse da sociedade, autorizado o uso do nome empresarial, vedado, no entanto, fazê-lo em atividades estranhas ao interesse social ou assumir obrigações seja em favor de qualquer dos quotistas ou de terceiros.

PARÁGRAFO PRIMEIRO – O administrador poderá constituir procurador, outorgando-lhe poderes para a prática dos atos em que se exija a qualidade de representante legal da empresa, constando da procuração, dentre outros

28/11/2019

Certifico o Registro em 28/11/2019
Arquivamento 20198199724 de 28/11/2019 Protocolo 198199724 de 08/11/2019 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 115640199432162

necessários, os poderes de acordar, discordar, transigir, confessar e depor em juízo pessoalmente como representante legal da sociedade.

PARÁGRAFO SEGUNDO- Na constituição de procurador será expressamente mencionado o limite de poderes do outorgado e fixado o prazo do mandato, que não poderá exceder a 12 meses, exceto quando se trata de poderes ad judicia ou para processos administrativos, nos quais o prazo coincidirá com fim da demanda.

PARÁGRAFO TERCEIRO- Os sócios terão direito a uma retirada mensal a título de pró labore, cujo valor será definido de comum acordo, observando o limite estabelecido pela legislação do imposto de renda.

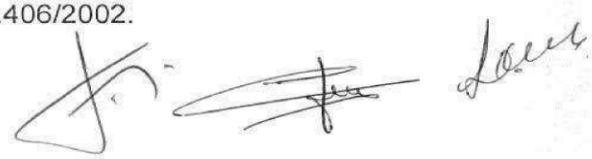
PARÁGRAFO QUARTO- Em caso de falecimento do sócio administrador, a sociedade não será dissolvida, continuará suas atividades e a sócia **CARLA FERNANDA DE ALMEIDA MONTEIRO MUNIZ** passará automaticamente a ser a sócia administradora com os mesmos poderes do sócio administrador falecido.

CLÁUSULA SÉTIMA – DA DELIBERAÇÃO DOS SOCIOS

Ao término de cada exercício social o administrador prestara contas justificadas de sua administração, procedendo a elaboração do inventario de estoques, das demonstrações contábeis exigidas em lei, cabendo aos sócios, na proporção de suas quotas, os lucros ou prejuízos apurados.

PARÁGRAFO PRIMEIRO- Nos quatro meses seguintes ao término do exercício social, os sócios deliberarão sobre a aprovação das contas da administração, designarão administrador(es), se for o caso, e tratarão dos demais temas de interesse da sociedade.

PARÁGRAFO SEGUNDO- Quando os sócios deliberarem em unanimidade, assuntos do interesse da sociedade, fica dispensada a realização de reunião, conforme previsto no art. 1.072 da lei 10.406/2002.



28/11/2019

JUCEPE

Certifico o Registro em 28/11/2019
Arquivamento 20198199724 de 28/11/2019 Protocolo 198199724 de 08/11/2019 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 115640199432162

PARÁGRAFO TERCEIRO- Os lucros apurados em balancetes intermediários poderão ser distribuídos aos sócios, sendo compensados com que houver sido apurado por ocasião do encerramento do exercício.

CLAUSULA OITAVA – DISSOLUÇÃO

A sociedade não se dissolverá por morte, internação ou retirada de quaisquer dos sócios, continuando com o(s) sócio(s) remanescente(s).

PARÁGRAFO PRIMEIRO- Falecendo ou interditado qualquer sócio, a sociedade continuará sua atividade com os sócios remanescentes. Não sendo possível ou inexistindo estes, o valor de seus haveres será apurado e liquidado com base na situação patrimonial da sociedade, à data da resolução, verificada em balanço especialmente levantado para tal finalidade.

PARÁGRAFO SEGUNDO – Por este ato determina-se, somente quando se fizer necessário, a regência supletiva desta sociedade pelo regramento pertinente à sociedade anônima, conforme permite o parágrafo único do art. 1.053, da lei 10.406/2002.

PARÁGRAFO TERCEIRO- O uso do direito de recesso, a declaração judicial de incapacidade e a exclusão de qualquer dos sócios não acarretará a dissolução da sociedade, desde que o sócio remanescente queira com ela continuar e promova o ingresso de um novo sócio na sociedade, no prazo de 180 (cento e oitenta) dias, em conformidade com a legislação em vigor.

CLÁUSULA NONA – DA DECLARAÇÃO DE DESIMPEDIMENTO

Os administradores declaram, sob as penas da lei, que não estão impedidos de exercerem a administração da sociedade, por lei especial ou em virtude de condenação criminal, ou por se encontrarem sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos, ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência contra as relações de consumo, fé publica ou propriedade.

28/11/2019

JUCEPE
Certifico o Registro em 28/11/2019
Arquivamento 20198199724 de 28/11/2019 Protocolo 198199724 de 08/11/2019 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 115640199432162

CLAUSULA DÉCIMA - DO FORO

Para qualquer divergência entre os sócios, fica eleito o foro da Cidade do Recife/PE, com a renúncia expressa de qualquer outro, por mais privilegiado que seja.

E, por estarem assim justas e contratadas, as partes assinam o presente instrumento de alteração contratual em 01 (uma) única via.

Recife/PE, 31 de Outubro de 2019.

Tabelionato Figueiredo

JOSÉ ALVES MUNIZ JUNIOR

Tabelionato Figueiredo

CARLA FERNANDA DE ALMEIDA MONTEIRO MUNIZ

1º OFÍCIO

LUCINDA MUNIZ

28/11/2019

Certifico o Registro em 28/11/2019
Arquivamento 20198199724 de 28/11/2019 Protocolo 198199724 de 08/11/2019 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 115640199432162

FIRMA(S) RETRO

1º TABELIONATO DE NOTAS E PROTESTOS DE MACEIÓ
CELSO SARMENTO PONTES DE MIRANDA

Rua Dr. Luiz Pontes de Miranda, 42 - Centro
CEP 57.020-140 - Maceió - Alagoas
Fones: (82) 3223-2600 / 3221-5000

1º Ofício de Notas e Protestos
R. Dr. Pontes de Miranda, 42
Centro
Fone (82) 3221-5000
Maceió - AL

REC. DE FIRMA Nº 2019 – 714996

Reconheço por semelhança a firma de:
LUCINDA MUNIZ**********

Em Testemunho ____ da verdade. MACEIO - AL - 13/11/2019 08:08:43
SELO DIGITAL: AAF93335 – OZJI
Confira os dados do ato em http://selodigital.tjal.jus.br/ Total: R$ 4,34

CELSO SARMENTO PONTES DE MIRANDA – TITULAR

8º TABELIONATO DE NOTAS DO RECIFE
Ivanildo de Figueiredo Andrade de Oliveira Filho
Tabelião Público

www.tabelionatofigueiredo.com.br
Fone: (81) 3073-0800

Reconheço a(s) firma(s) por semelhança de:
[0002090]--JOSE ALVES MUNIZ JUNIOR. . . . . .
. . . . . .
Recife, 20 de Novembro de 2019 - Em test. ____ da verdade.
BRENO ANDRADE DE OLIVEIRA
Emol.: R$ 4,71; TSNR: 0,80; FERC: 0,40; FERM: 0,04;
FUNSEG: 0,08; ISS: 0,20; Total: 4,91
Selo digital 0073783.RRX11201904.00550

Consulte Autenticidade em: www.tjpe.jus.br/selodigital

8º TABELIONATO DE NOTAS DO RECIFE
Ivanildo de Figueiredo Andrade de Oliveira Filho
Tabelião Público

www.tabelionatofigueiredo.com.br
Fone: (81) 3073-0800

Reconheço a(s) firma(s) por semelhança de:
[0010931]--CARLA FERNANDA DE ALMEIDA MONTEIRO MUNIZ. . . . . .
Recife, 20 de Novembro de 2019 - Em test. ____ da verdade.
BRENO ANDRADE DE OLIVEIRA
Emol.: R$ 4,71; TSNR: 0,80; FERC: 0,40; FERM: 0,04;
FUNSEG: 0,08; ISS: 0,20; Total: 4,91
Selo digital 0073783.TCM11201904.00551

Consulte Autenticidade em: www.tjpe.jus.br/selodigital

28/11/2019

Certifico o Registro em 28/11/2019
Arquivamento 20198199724 de 28/11/2019 Protocolo 198199724 de 08/11/2019 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 115640199432162

JUCEPE
JUNTA COMERCIAL DE PERNAMBUCO

198199724

TERMO DE AUTENTICAÇÃO

NOME DA EMPRESA	**SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA**
PROTOCOLO	**198199724 - 08/11/2019**
ATO	**002 - ALTERACÃO**
EVENTO	**021 - ALTERACAO DE DADOS (EXCETO NOME EMPRESARIAL)**

MATRIZ

NIRE 26201319707
CNPJ 12.707.105/0001-64
CERTIFICO O REGISTRO EM 28/11/2019
SOB N: 20198199724

EVENTOS

027 - ALTERACAO DE FILIAL EM OUTRA UF ARQUIVAMENTO: 20198199724
051 - CONSOLIDACAO DE CONTRATO/ESTATUTO ARQUIVAMENTO: 20198199724

Assinado eletronicamente por
ILAYNE LARISSA LEANDRO MARQUES
SECRETÁRIA - GERAL

28/11/2019

JUCEPE
Certifico o Registro em 28/11/2019
Arquivamento 20198199724 de 28/11/2019 Protocolo 198199724 de 08/11/2019 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 115640199432162

1º OFÍCIO DE DISTRIBUIÇÃO DA CAPITAL
FORUM DESEMBARGADOR RODOLFO AURELIANO
Av. Des. Guerra Barreto, s/n, térreo, Ilha Joana Bezerra - RECIFE/PE

CERTIDÃO FALÊNCIA

JOSÉ GILSON DE OLIVEIRA CABRAL,
Titular do 1º Ofício de Contador –distribuidor da Comarca de Recife, Capital do Estado de PE

CERTIFICO, por me haver sido pedido que, conforme pesquisa realizada no sistema JUDWIN, onde são lançadas as distribuições do ofício, a meu cargo, **Seção CIVEL** no período de **05 (CINCO)** anos até a presente data, **não** encontrei **DISTRIBUIDO** Processo de **Falência, Concordata, Recuperação Judicial, inexistindo pedido de homologação judicial de plano de recuperação extrajudicial** em face de:

Supriservi Comércio Representações e Serviços LTDA, CPF/CNPJ: 12.707.105/0001-64.

Certifico ainda que, nesta comarca, podem ser obtidas certidões desse tipo de feitos ajuizados em 1° grau, quanto aos processos eletrônicos do PJE, abrangendo todas as comarcas de PE, diretamente no site TJPE.JUS.BR.

ESSA CERTIDÃO NÃO INCLUI OS PROCESSOS DISTRIBUIDOS ANTES DO PRAZO ESTIPULADO NA PESQUISA, AINDA QUE EM TRAMITAÇÃO.

OBS: sem cobrança de taxa em cumprimento ao ofício circular n° 12/2016 de 04/07/2016

Pesquisa realizada até o dia 18 de SETEMBRO de 2020, por MIGUEL LIRA BARBOSA.

1º DISTRIBUIDOR DA CAPITAL

Assinado eletronicamente por: ADRIANA BARBOSA LOPES:1815415
SERVIDOR - Informação
em 21/09/2020 às 14:10N/S Cert.: 143284524456795850781933916198067346955
http://www.tjpe.jus.br/validardocumento
Autenticação:
XC.M1.SB.97.A7

PODER JUDICIÁRIO DO ESTADO DE PERNAMBUCO

TRIBUNAL DE JUSTIÇA

Fórum Des. Rodolfo Aureliano
Av. Desembargador Guerra Barreto, 200 – Térreo – Ala Sul, bairro Joana Bezerra
Fones nº (081) 3181-0400 (FAX)/ 3181-0476 e 3181-0470
CEP 50.090-700 - RECIFE - PE

CERTIDÃO NEGATIVA LICITAÇÃO

VALIDADE 30 DIAS DA EMISSÃO

Data da Emissão: 08/10/2020 05h08min **Data de Validade: 07/11/2020**

Nº da Certidão: 641743/2020 **Nº da Autenticidade: 4V.6N.CD.UM.0N**

Os dados dos documentos constantes nesta certidão foram informados pelo solicitante, sua titularidade e autenticidade deverão ser conferidas pelo interessado, conforme o documento original	
Razão Social: SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA	
CNPJ: 12.707.105/0001-64	**Inscrição Estadual: 020106904**
Endereço Residencial: AV.GOV.AGAMENON MAGALHÃES, 4779	**Compl:** SALAS 401 A 404- EMPRESAIRL ISAAC NEWTON
Bairro: ILHA DO LEITE	**Cidade: Recife/PE**

Certifico que NADA CONSTA nos registros de distribuição do Sistema Processo Judicial Eletrônico – PJe 1º Grau, implantado nas Unidades Judiciárias, no âmbito do Tribunal de Justiça do Estado de Pernambuco, FALÊNCIA DE EMPRESÁRIOS, SOCIEDADES EMPRESARIAIS, MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE; RESTITUIÇÃO DE COISA OU DINHEIRO NA FALÊNCIA DO DEVEDOR EMPRESÁRIO; RECUPERAÇÃO JUDICIAL E RECUPERAÇÃO EXTRAJUDICIAL protocolada e que esteja em tramitação contra a pessoa acima identificada.

A presente certidão, em consonância com a legislação vigente, atende ao disposto na Instrução Normativa do TJPE nº 07 de 02/06/2014, na Resolução do CNJ nº 185 e na Lei 11.419/2006 e foi expedida gratuitamente através da Internet.

Observações:
A autenticidade desta certidão deverá ser confirmada no sítio eletrônico do Tribunal de Justiça do Estado de Pernambuco, através do link https://www.tjpe.jus.br/certidaopje/xhtml/main.xhtml, na opção - Validar Certidão Negativa de Processos Cíveis (PJe) - utilizando o número de autenticidade acima identificado.

Esta certidÃ£o nÃ£o abrange os processos distribuÃdos antes da implantaÃ§Ã£o do Sistema Processo Judicial EletrÃ´nico â€“ PJe, no Ã¢mbito do Tribunal de JustiÃ§a de Pernambuco. O referido Ã© verdade e dou fÃ©.

PODER JUDICIÁRIO DO ESTADO DE PERNAMBUCO

TRIBUNAL DE JUSTIÇA

Núcleo de Distribuição Processual - NUDIP 2º grau
Praça da República, s/n, bairro Santo Antônio
Fones nºs (081) 3182-0519 ou 3182-0594
CEP 50.010-040 RECIFE - PE

CERTIDÃO NEGATIVA LICITAÇÃO

VALIDADE 30 DIAS DA EMISSÃO

Data da Emissão: 08/10/2020 05h10min **Data de Validade: 07/11/2020**

Nº da Certidão: 641744/2020 **Nº da Autenticidade: 4R.VC.YF.RB.YB**

Os dados dos documentos constantes nesta certidão foram informados pelo solicitante, sua titularidade e autenticidade deverão ser conferidas pelo interessado, conforme o documento original	
Razão Social: SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA	
CNPJ: 12.707.105/0001-64	**Inscrição Estadual: 020106904**
Endereço Residencial: AV.GOV.AGAMENON MAGALHÃES, 4779	**Compl:** SALAS 401 A 404- EMPRESAIRL ISAAC NEWTON
Bairro: ILHA DO LEITE	**Cidade: Recife/PE**

Certifico que NADA CONSTA nos registros de distribuição do Sistema Processo Judicial Eletrônico – PJe 2º Grau, implantado nas Unidades Judiciárias, no âmbito do Tribunal de Justiça do Estado de Pernambuco, FALÊNCIA DE EMPRESÁRIOS, SOCIEDADES EMPRESARIAIS, MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE; RESTITUIÇÃO DE COISA OU DINHEIRO NA FALÊNCIA DO DEVEDOR EMPRESÁRIO; RECUPERAÇÃO JUDICIAL E RECUPERAÇÃO EXTRAJUDICIAL protocolada e que esteja em tramitação contra a pessoa acima identificada.

A presente certidão, em consonância com a legislação vigente, atende ao disposto na Instrução Normativa do TJPE nº 07 de 02/06/2014, na Resolução do CNJ nº 185 e na Lei 11.419/2006 e foi expedida gratuitamente através da Internet.

Observações:
A autenticidade desta certidão deverá ser confirmada no sítio eletrônico do Tribunal de Justiça do Estado de Pernambuco, através do link https://www.tjpe.jus.br/certidaopje/xhtml/main.xhtml, na opção - Validar Certidão Negativa de Processos Cíveis (PJe) - utilizando o número de autenticidade acima identificado.

Esta certidÃ£o nÃ£o abrange os processos distribuÃdos antes da implantaÃ§Ã£o do Sistema Processo Judicial EletrÃ´nico â€“ PJe, no Ã¢mbito do Tribunal de JustiÃ§a de Pernambuco. O referido Ã© verdade e dou fÃ©.

TERMO DE ABERTURA

BALANÇO 2019 - Referente ao periodo de 01/01/2019 a 31/12/2019.

Nome da Empresa ... :	**SUPRISERVI COMÉRCIO, REPRESENTAÇÕES E SERVIÇOS LTDA.**
Endereço ..... :	**AV. GOV. AGAMENON MAGALHÃES, 4779, SLS. 401 a 404, ILHA DO LEITE**
Cidade ..... :	**RECIFE CEP: 50.070-425**
Estado ..... :	**PE**
NIRE ..... :	**2620.131970-7**
Insc. Estadual .... :	**0201069-04**
CNPJ ..... :	**12.707.105/0001-64**
Insc. Municipal ... :	**239.461-8**
Data de encerramento:	**31/12/2019**

A - Sob as penas da lei, declaramos que as informações aqui contidas são verdadeiras, nos responsabilizando por todas elas.
B - As informações foram extraídas das folhas nºs 002 a 609 do Livro Diário nº 27, registrado na Junta Comercial do Estado de Pernambuco JUCEPE, sob nº 20/948244-3 em 07/04/2020.
C - A sociedade não possui Conselho Fiscal instalado.
D - A sociedade não possui Auditoria Independente.

Recife, 01 de Janeiro de 2019.

Supriservi Comércio Representações e Serviços Ltda.
José Alves Muniz Junior
RG nº 638.963 SSP/AL
CPF nº 349.227.334-34
Sócio Administrador

Juliana Angelo de Lima Ribeiro
Contadora - CRC/PE 018.192/O8
RG nº 4.678.385 SDS/PE
CPF nº 022.396.254-65

19/05/2020
Certifico o Registro em 19/05/2020
Arquivamento 20209436328 de 19/05/2020 Protocolo 209436328 de 11/05/2020 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 194881714117747

http://assinador.pscs.com.br/assinadorweb/autenticacao?chave1=ampwYnSCA9EwwBYxwajsIQ&chave2=bivYHKotzXwAGXcKi4FdLw
ASSINADO DIGITALMENTE POR: 34922733434-JOSE ALVES MUNIZ JUNIOR|02239625465-JULIANA ANGELO DE LIMA RIBEIRO

Empresa: Supriservi Comércio Representações e Serviços Ltda.

CNPJ: 12.707.105/0001-64

NIRE: 2620.131.970-7 de 23/10/2001

BALANÇO PATRIMONIAL encerrado em 31/12/2019

ATIVO			PASSIVO		
ATIVO CIRCULANTE	**2018**	**2019**	**PASSIVO CIRCULANTE**	**2018**	**2019**
Caixa/Fundo Fixo	1.000,00	1.000,00	Fornecedores	272.481,73	1.295.382,70
Bancos Cta. Movimento	12.103,45	54.766,60	Provisões IRPJ e CSLL	325.119,93	307.969,42
Aplicações Financeiras	1.050.549,45	1.694.735,54	Obrigações Fiscais	83.654,12	286.388,18
Duplicatas a Receber	1.560.962,35	1.557.505,46	Obrigações Trabalhistas	183.414,33	196.519,26
Adiantamentos	1.176.068,17	1.187.855,59	Outras Obrigações	8.220,23	-
Impostos a Recuperar	354.664,09	339.362,30			
Estoque	1.419.961,53	1.593.612,75			
TOTAL DO ATIVO CIRCULANTE	**5.575.309,04**	**6.428.838,24**	**TOTAL DO PASSIVO CIRCULANTE**	**872.890,34**	**2.086.259,56**
REALIZÁVEL A LONGO PRAZO			**EXIGÍVEL A LONGO PRAZO**		
Títulos e Valores Mobiliários	174.853,68	159.990,61	Emprestimos & Financiamentos	-	471.428,56
Despesas de Exercícios Seguintes	2.282.571,18	2.076.618,66	Tributos	4.521.654,64	4.070.376,95
TOTAL DO REALIZÁVEL A LONGO PRAZO	**2.457.424,86**	**2.236.609,27**	**TOTAL DO EXIGÍVEL A LONGO PRAZO**	**4.521.654,64**	**4.541.805,51**
PERMANENTE			**RESULTADO DE EXERCÍCIOS FUTUROS**		
Imobilizado	1.555.932,97	1.745.427,10	Resultado de Exercícios Futuros	-	-
TOTAL DO PERMANENTE	**1.555.932,97**	**1.745.427,10**	**TOTAL DE RESULTADO DE EXERCÍCIOS FUTUROS**	**-**	**-**
CONTAS DE COMPENSAÇÃO			**PATRIMÔNIO LÍQUIDO**		
Mercadorias próprias em Poder de Terceiros	596.764,54	1.108.979,55	Capital Realizado	204.000,00	204.000,00
Mercadorias de Terceiros em Demonstração	-	141.165,31	Lucros/Prejuízos Acumulados	3.269.517,99	2.667.335,00
TOTAL DAS CONTAS DE COMPENSAÇÃO	**596.764,54**	**1.250.144,86**	Lucros/Prejuízos Exerc.Atual	720.603,90	911.474,54
			TOTAL DO PATRIMÔNIO LÍQUIDO	**4.194.121,89**	**3.782.809,54**
			CONTAS DE COMPENSAÇÃO		
			Mercadorias próprias em Poder de Terceiros	596.764,54	1.108.979,55
			Mercadorias de Terceiros em Demonstração		141.165,31
			TOTAL DAS CONTAS DE COMPENSAÇÃO	**596.764,54**	**1.250.144,86**
TOTAL DO ATIVO	**10.185.431,41**	**11.661.019,47**	**TOTAL DO PASSIVO**	**10.185.431,41**	**11.661.019,47**

ÍNDICES - Balanço/2019	
Liquidez Corrente - AC/PC	3,08
Liquidez Geral - AC + ARLP / PC + ELP	1,31
Endividamento - PC + ELP / AT	0,57
Solvência Geral - AT / PC + ELP	1,76
Rentabilidade do Capital Próprio - LL / PL	24,10%
Rentabilidade sobre as Vendas - LL / ROL	5,51%

DECLARAÇÃO

A - Sob as penas da lei, declaramos que as informações aqui contidas são verdadeiras, nos responsabilizando por todas elas.
B - As informações foram extraídas das folhas nºs 002 a 609 do Livro Diário nº 27, registrado na Junta Comercial do Estado de Pernambuco JUCEPE, sob nº 20/948244-3 em 07/04/2020.
C - A sociedade não possui Conselho Fiscal instalado.
D - A sociedade não possui Auditoria Independente.

Recife/PE, 31 de Dezembro de 2019.

José Alves Muniz Junior
Sócio Administrador
RG nº 638.963 SSP/AL
CPF nº 349.227.334-34

Juliana Angelo de Lima Ribeiro
Contadora - CRC/PE 018.192/O8
RG nº 4.678.385 SDS/PE
CPF nº 022.396.254-65

http://assinador.pscs.com.br/assinadorweb/autenticacao?chave1=ampwYnSCA9EwwBYxwajsIQ&chave2=bivVHKotzXwAGXcKi4FdLw
ASSINADO DIGITALMENTE POR: 34922733434-JOSE ALVES MUNIZ JUNIOR|02239625465-JULIANA ANGELO DE LIMA RIBEIRO

19/05/2020
Certifico o Registro em 19/05/2020
Arquivamento 20209436328 de 19/05/2020 Protocolo 209436328 de 11/05/2020 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 194881714117747

http://assinador.pscs.com.br/assinadorweb/autenticacao?chave1=ampwYnSCA9EwwBYxwajsIQ&chave2=bivYHKotzXwAGXcKi4FdLw
ASSINADO DIGITALMENTE POR: 34922733434-JOSE ALVES MUNIZ JUNIOR|02239625465-JULIANA ANGELO DE LIMA RIBEIRO

Empresa: Supriservi Comércio Representações e Serviços Ltda.
CNPJ: 12.707.105/0001-64
NIRE: 2620.131.970-7 de 23/10/2001

DEMONSTRAÇÃO DO RESULTADO DO EXERCÍCIO encerrado em 31/12/2019

	2018	2019
RECEITA OPERACIONAL BRUTA		
Receita Bruta Operacional	**16.156.064,62**	**20.404.685,68**
Vendas de Mercadorias	9.678.784,71	15.648.155,07
Vendas de Serviços	6.477.279,91	4.756.530,61
Deduções de Vendas	**(1.834.757,21)**	**(3.855.669,06)**
Devoluções	(339.567,06)	(1.919.985,84)
Tributos s/ Vendas	(1.495.190,15)	(1.935.683,22)
RECEITA OPERACIONAL LÍQUIDA	**14.321.307,41**	**16.549.016,62**
Custos das Vendas	**(9.444.912,01)**	**(11.370.239,32)**
Mercadorias Vendidas	(4.576.625,92)	(4.658.898,53)
Serviços Prestados	(4.868.286,09)	(6.711.340,79)
RESULTADO OPERACIONAL BRUTO	**4.876.395,40**	**5.178.777,30**
Despesas Operacionais	**(3.392.209,84)**	**(3.866.824,06)**
Despesas Gerais e Administrativas	(3.173.753,24)	(3.745.031,37)
Despesas Financeiras	(254.812,71)	(143.107,68)
Receitas Financeiras	36.356,11	21.314,99
Resultado Não Operacional	**220.000,00**	**519.172,78**
Receitas Não Operacionais	220.000,00	519.172,78
Despesas Não Operacionais	0,00	0,00
Resultado antes do IRPJ e CSLL	**1.704.185,56**	**1.831.126,02**
Provisão da CSLL	(690.840,57)	(633.522,12)
Provisão do IRPJ	(292.741,09)	(286.129,36)
LUCRO LÍQUIDO DO EXERCÍCIO	**720.603,90**	**911.474,54**

DECLARAÇÃO

A - Sob as penas da lei, declaramos que as informações aqui contidas são verdadeiras, nos responsabilizando por todas elas.

B - As informações foram extraídas das folhas nºs 002 a 609 do Livro Diário nº 27, registrado na Junta Comercial do Estado de Pernambuco - JUCEPE, sob nº 20/948244-3 em 07/04/2020.

C - A sociedade não possui Conselho Fiscal instalado.

D - A sociedade não possui Auditoria Independente.

Recife/PE, 31 de Dezembro de 2019.

Supriservi Comércio Representações e Serviços Ltda.
José Alves Muniz Junior
RG nº 638.963 SSP/AL
Sócio Administrador
CPF nº 349.227.334-34

Juliana Angelo de Lima Ribeiro
Contadora - CRC/PE 018.192/O8
RG nº 4.678.385 SDS/PE
CPF nº 022.396.254-65

19/05/2020
Certifico o Registro em 19/05/2020
Arquivamento 20209436328 de 19/05/2020 Protocolo 209436328 de 11/05/2020 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 194881714117747

http://assinador.pscs.com.br/assinadorweb/autenticacao?chave1=ampwYnSCA9EwwEYxwajsIQ&chave2=bivVHKotzXwAGXcKi4FdLw
ASSINADO DIGITALMENTE POR: 34922733434-JOSE ALVES MUNIZ JUNIOR|02239625465-JULIANA ANGELO DE LIMA RIBEIRO

DEMONSTRAÇÃO DAS MUTAÇÕES DO PATRIMÔNIO LÍQUIDO EM 31.12.2019

Contas	Capital Social	Adto p/ Aum. Capital	Lucros Acumulados	Patrimônio Líquido
Saldo Inicial do Exercício	**204.000,00**	**0,00**	**3.990.121,89**	**4.194.121,89**
Ajuste de Exerc. Anteriores	0,00	0,00	-205.952,52	-205.952,52
Lucro (Prejuízo) do Exercício	0,00	0,00	911.474,54	911.474,54
Adiant p/ Aumento de Capital	0,00	0,00	0,00	0,00
Distribuição de Lucro	0,00	0,00	-1.116.834,37	-1.116.834,37
Saldo Final do Exercício	**204.000,00**	**0,00**	**3.578.809,54**	**3.782.809,54**

DECLARAÇÃO

A - Sob as penas da lei, declaramos que as informações aqui contidas são verdadeiras, nos responsabilizando por todas elas.

B - As informações foram extraídas das folhas nºs 002 a 609 do Livro Diário nº 27, registrado na Junta Comercial do Estado de Pernambuco JUCEPE, sob nº 20/948244-3 em 07/04/2020.

C - A sociedade não possui Conselho Fiscal instalado.

D - A sociedade não possui Auditoria Independente.

Recife/PE, 31 de dezembro de 2019.

Supriservi Comércio Representações e Serviços Ltda.
José Alves Muniz Junior
Sócio Administrador
RG nº 638.963 SSP/AL
CPF nº 349.227.334-34

Juliana Angelo de Lima Ribeiro
Contadora - CRC/PE 018.192/O8
RG nº 4.678.385 SDS/PE
CPF nº 022.396.254-65

19/05/2020
Certifico o Registro em 19/05/2020
Arquivamento 20209436328 de 19/05/2020 Protocolo 209436328 de 11/05/2020 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 194881714117747

SUPRISERVI COMÉRCIO REPRESENTAÇÕES E SERVIÇOS LTDA.
CNPJ nº 12.707.105/0001-64
NIRE nº 2620.131.970-7 de 23/10/2001

ENCERRADO EM 31 DE DEZEMBRO DE 2019

NOTAS EXPLICATIVAS ÀS DEMONSTRAÇÕES CONTÁBEIS EM 31 DE DEZEMBRO DE 2019

1) CONTEXTO OPERACIONAL

A Supriservi Comércio Representações e Serviços Ltda - Newsupri - é uma Sociedade Empresária Limitada, com sede e foro na cidade de Recife/PE, com filiais nas cidades de Olinda/PE, Maceió/AL e Aracajú/SE, tendo como principal objeto social a prestação de serviços de Consultoria em Tecnologia da Informação, com início de suas atividades em 21/08/1987.

2) APRESENTAÇÃO DAS DEMONSTRAÇÕES CONTÁBEIS (DECLARAÇÃO DE CONFORMIDADE)

As demonstrações contábeis foram elaboradas em consonância com os ditames da NBC-ITG 1000, além dos Princípios Fundamentais de Contabilidade e demais práticas emanadas da legislação societária brasileira.

3) PRINCIPAIS PRÁTICAS CONTÁBEIS

3.1 Disponível
Composto de Caixa e equivalentes de caixa, que incluem o dinheiro em caixa, os depósitos bancários e aplicações financeiras com vencimentos originais de curto prazo e com risco insignificante de mudança de valor;

3.2 Duplicatas a Receber
As duplicatas a receber correspondem aos valores a receber de clientes pela venda de produtos e serviços e são registradas e mantidas pelo valor nominal dos títulos;

3.3 Estoques
Os estoques são demonstrados ao custo ou ao valor líquido de realização, dos dois o menor, sendo determinado pelo método do custo médio;

3.4 Títulos e Valores Mobiliários
Composto pelo saldo de aplicações de longo prazo em Títulos de Capitalização BB, com vencimentos superiores a 12 meses;

3.5 Despesas do Exercício Seguinte
Consta neste subgrupo despesas a realizar nos exercícios seguintes, decorrentes de encargos sobre parcelamento de tributos federais em 145 meses, formalizados no PERT 2017 - Programa Especial de Regularização Tributária, com o início da realização das parcelas a partir de Jan/2018.

3.6 Imobilizado
O imobilizado é composto pelas contas Máquinas & Equipamentos, Móveis & Utensílios, Veículos, Equipamentos de Informática, Outros Bens e Benfeitorias em Imóveis de Terceiros (gastos com reforma da nova sede) e é mensurado pelo seu custo histórico, menos depreciação acumulada, conforme inventário de bens realizado em dez/2019.

DECLARAÇÃO

A - Sob as penas da lei, declaramos que as informações aqui contidas são verdadeiras, nos responsabilizando por todas elas.

B - As informações foram extraídas das folhas nºs 002 a 609 do Livro Diário nº 27, registrado na Junta Comercial do Estado de Pernambuco JUCEPE, sob nº 20/948244-3 em 07/04/2020.

C - A sociedade não possui Conselho Fiscal instalado.

D - A sociedade não possui Auditoria Independente.

Recife/PE, 31 de dezembro de 2019.

José Alves Muniz Junior
Sócio Administrador
RG nº 638.963 SSP/AL
CPF nº 349.227.334-34

Juliana Angelo de Lima Ribeiro
Contadora - CRC/PE 018.192/O8
RG nº 4.678.385 SDS/PE
CPF nº 022.396.254-65

19/05/2020
Certifico o Registro em 19/05/2020
Arquivamento 20209436328 de 19/05/2020 Protocolo 209436328 de 11/05/2020 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 194881714117747

http://assinador.pscs.com.br/assinadorweb/autenticacao?chave1=ampwYnSCA9EwwEYxwajsIQ&chave2=bivYHKotzXwAGXcKi4FdLw
ASSINADO DIGITALMENTE POR: 34922733434-JOSE ALVES MUNIZ JUNIOR|02239625465-JULIANA ANGELO DE LIMA RIBEIRO

SUPRISERVI COMÉRCIO REPRESENTAÇÕES E SERVIÇOS LTDA.
CNPJ nº 12.707.105/0001-64
NIRE nº 2620.131.970-7 de 23/10/2001

http://assinador.pscs.com.br/assinadorweb/autenticacao?chave1=ampwYnSCA9EwwEYxwajsIQ&chave2=bivVHKotzXwAGXcKi4FdLw
ASSINADO DIGITALMENTE POR 34922733434-JOSE ALVES MUNIZ JUNIOR|02239625465-JULIANA ANGELO DE LIMA RIBEIRO

ENCERRADO EM 31 DE DEZEMBRO DE 2019

NOTAS EXPLICATIVAS ÀS DEMONSTRAÇÕES CONTÁBEIS EM 31 DE DEZEMBRO DE 2019

3.7 Contas de Compensação
Estão presentes neste grupo os registros dos produtos para revenda em demonstração a terceiros, contabilizados pelos valores de face das notas fiscais, com os lançamentos fazendo contrapartida entre Ativo e Passivo.

3.8 Fornecedores
As contas a pagar aos fornecedores são obrigações a pagar por bens ou serviços que foram adquiridos no curso normal dos exercícios, cujos vencimentos ocorrem no exercício fiscal subsequente ao deste balanço;

3.9 Tributos a Recolher
Compõe as Provisões para IRPJ e CSLL, Obrigações Fiscais, Trabalhistas e Outras e são calculados com base em alíquotas de imposto e legislações fiscais e trabalhistas em vigor na data base das demonstrações financeiras;

3.10 Tributos de Longo Prazo
Composto pelo saldo a pagar de parcelamentos de tributos federais realizados junto à Receita Federal através do PERT - Programa Especial de Regularização Tributária firmado em 29/08/2017, conforme recibo nº 08978599898234992210, vencíveis a longo prazo em 145 parcelas a partir de jan/2018;

3.11 Impostos Federais
A empresa opera no regime Lucro Presumido e contabiliza seus encargos tributários pelo regime de competência.

4) RESPONSABILIDADES E CONTINGÊNCIAS
Não há passivo contingente registrado contabilmente, tendo em vista que os administradores da empresa, escudados em opinião de seus consultores e advogados, não apontam contingências de qualquer natureza.

5) CAPITAL SOCIAL
O capital social é de R$ 204.000,00, dividido em 204.000 quotas de R$ 1,00, totalmente integralizado, apresentando a seguinte composição:
José Alves Muniz Júnior – 98,55%
Carla Fernanda de Almeida Monteiro Muniz - 1,00%
Lucinda Muniz - 0,45%

6) AJUSTES DE EXERCÍCIOS ANTERIORES
O valor lançado como ajuste de exercícios anteriores refere-se a juros sobre parcelamento de impostos (PERT) incorridos dentro do exercício, ora registrados.

7) EVENTOS SUBSEQUENTES
Os administradores declaram a inexistência de fatos ocorridos subseqüentemente à data de encerramento do corrente exercício que venham a ter efeito relevante sobre a situação patrimonial ou financeira da empresa ou que possam provocar efeitos sobre seus resultados futuros.

DECLARAÇÃO

A - Sob as penas da lei, declaramos que as informações aqui contidas são verdadeiras, nos responsabilizando por todas elas.
B - As informações foram extraídas das folhas nºs 002 a 609 do Livro Diário nº 27, registrado na Junta Comercial do Estado de Pernambuco JUCEPE, sob nº 20/948244-3 em 07/04/2020.
C - A sociedade não possui Conselho Fiscal instalado.
D - A sociedade não possui Auditoria Independente.

Recife/PE, 31 de dezembro de 2019.

José Alves Muniz Junior
Sócio Administrador
RG nº 638.963 SSP/AL
CPF nº 349.227.334-34

Juliana Angelo de Lima Ribeiro
Contadora - CRC/PE 018.192/O8
RG nº 4.678.385 SDS/PE
CPF nº 022.396.254-65

19/05/2020
Certifico o Registro em 19/05/2020
Arquivamento 20209436328 de 19/05/2020 Protocolo 209436328 de 11/05/2020 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 194881714117747

http://assinador.pscs.com.br/assinadorweb/autenticacao?chave1=ampwYnSCA9EwwBYxwajsIQ&chave2=bivYHKotzXwAGXcKi4FdLw
ASSINADO DIGITALMENTE POR: 34922733434-JOSE ALVES MUNIZ JUNIOR|02239625465-JULIANA ANGELO DE LIMA RIBEIRO

TERMO DE ENCERRAMENTO

BALANÇO 2019 - Referente ao periodo de 01/01/2019 a 31/12/2019.

Nome da Empresa ... :	**SUPRISERVI COMÉRCIO, REPRESENTAÇÕES E SERVIÇOS LTDA.**
Endereço ..... :	**AV. GOV. AGAMENON MAGALHÃES, 4779, SLS. 401 a 404, ILHA DO LEITE**
Cidade ..... :	**RECIFE CEP: 50.070-425**
Estado ..... :	**PE**
NIRE ..... :	**2620.131970-7**
Insc. Estadual .... :	**0201069-04**
CNPJ ..... :	**12.707.105/0001-64**
Insc. Municipal ... :	**239.461-8**
Data de encerramento:	**31/12/2019**

A - Sob as penas da lei, declaramos que as informações aqui contidas são verdadeiras, nos responsabilizando por todas elas.
B - As informações foram extraídas das folhas nºs 002 a 609 do Livro Diário nº 27, registrado na Junta Comercial do Estado de Pernambuco JUCEPE, sob nº 20/948244-3 em 07/04/2020.
C - A sociedade não possui Conselho Fiscal instalado.
D - A sociedade não possui Auditoria Independente.

Recife, 31 de Dezembro de 2019.

Supriservi Comércio Representações e Serviços Ltda.
José Alves Muniz Junior
RG nº 638.963 SSP/AL
Sócio Administrador
CPF nº 349.227.334-34

Juliana Angelo de Lima Ribeiro
Contadora - CRC/PE 018.192/O8
RG nº 4.678.385 SDS/PE
CPF nº 022.396.254-65

19/05/2020
Certifico o Registro em 19/05/2020
Arquivamento 20209436328 de 19/05/2020 Protocolo 209436328 de 11/05/2020 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 194881714117747

JUCEPE
JUNTA COMERCIAL DE PERNAMBUCO

209436328

TERMO DE AUTENTICAÇÃO

NOME DA EMPRESA	**SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA**
PROTOCOLO	**209436328 - 11/05/2020**
ATO	**223 - BALANCO PUBLICADO**
EVENTO	**223 - BALANCO PUBLICADO**

MATRIZ

NIRE 26201319707
CNPJ 12.707.105/0001-64
CERTIFICO O REGISTRO EM 19/05/2020
SOB N: 20209436328

REPRESENTANTES QUE ASSINARAM DIGITALMENTE

Cpf: 34922733434 - JOSE ALVES MUNIZ JUNIOR

Cpf: 02239625465 - JULIANA ANGELO DE LIMA RIBEIRO

Assinado eletronicamente por
ILAYNE LARISSA LEANDRO MARQUES
SECRETÁRIA - GERAL

19/05/2020

JUCEPE
Certifico o Registro em 19/05/2020
Arquivamento 20209436328 de 19/05/2020 Protocolo 209436328 de 11/05/2020 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 194881714117747

http://assinador.pscs.com.br/assinadorweb/autenticacao?chave1=ampwYnSCA9EwwBYxwajsIQ&chave2=bivYHKotzXwAGXcKi4FdLw
ASSINADO DIGITALMENTE POR: 34922733434-JOSE ALVES MUNIZ JUNIOR|02239625465-JULIANA ANGELO DE LIMA RIBEIRO

PROCURAÇÃO

SUPRISERVI COMÉRCIO REPRESENTAÇÕES E SERVIÇOS LTDA , pessoa jurídica de direito privado, inscrita no CNPJ sob o nº. 12.707.105/0001-64, estabelecida a Av. Agamenon Magalhães nº 4779, Ilha do Leite, Recife/PE, neste ato representada por seu sócio representante **José Alves Muniz Júnior, CPF:349.227.334-34, RG:638963-SSP-AL vem** pelo presente instrumento particular **outorgar** a **Juliana Angelo de Lima Ribeiro**, Contadora, RG nº /SSP-PE e CPF nº 022.396.254-65,CRCPE:018.192/O8 com endereço profissional a Av. Agamenon Magalhães, Empresarial Thomas Edison nº 4775, sala 1301, Ilha do Leite, Recife, Estado de Pernambuco, com poderes para agir, para o foro em geral, especialmente para requerer junto a Junta Comercial do Estado de Pernambuco - JUCEPE, entrada de processos administrativos, emissão de certidões, entrega de documentações solicitados, receber orientações, dar e receber ciente, ou ainda, requerer e assinar qualquer outro documento que se faça necessário para os devidos fins, na qualidade de contadora, enfim, podendo praticar tudo o que for necessário para o pleno desempenho do presente mandato, de entrega de Livros, arquivamentos e demais processos digitais, no que tange a representá-lo junto ao órgão acima indicado, em suas secretarias, regionais e demais órgãos colegiados, tudo isso em nome da outorgante.

Recife (PE), 11/05/2020.

_____

José Alves Muniz Júnior
Sócio Administrador
CPF:349.227.334-34
RG:638963- SSP/AL

_____

Juliana Angelo de Lima Ribeiro
Contadora
CPF:022.396.254-65
RG:4678385- SDS/PE
Crc/pe:018.192/O8

19/05/2020
Certifico o Registro em 19/05/2020
Arquivamento 20209436328 de 19/05/2020 Protocolo 209436328 de 11/05/2020 NIRE 26201319707
Nome da empresa SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
Este documento pode ser verificado em http://redesim.jucepe.pe.gov.br/autenticacaodocumentos/autenticacao.aspx
Chancela 194881714117747

REPÚBLICA FEDERATIVA DO BRASIL

CADASTRO NACIONAL DA PESSOA JURÍDICA

NÚMERO DE INSCRIÇÃO	COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL	DATA DE ABERTURA
12.707.105/0001-64 **MATRIZ**		**21/08/1987**

NOME EMPRESARIAL
SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA

TÍTULO DO ESTABELECIMENTO (NOME DE FANTASIA)	PORTE
NEWSUPRI	**DEMAIS**

CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL
62.04-0-00 - Consultoria em tecnologia da informação

CÓDIGO E DESCRIÇÃO DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS
85.99-6-03 - Treinamento em informática
62.09-1-00 - Suporte técnico, manutenção e outros serviços em tecnologia da informação
63.11-9-00 - Tratamento de dados, provedores de serviços de aplicação e serviços de hospedagem na internet
77.33-1-00 - Aluguel de máquinas e equipamentos para escritórios
47.51-2-01 - Comércio varejista especializado de equipamentos e suprimentos de informática
46.14-1-00 - Representantes comerciais e agentes do comércio de máquinas, equipamentos, embarcações e aeronaves
95.11-8-00 - Reparação e manutenção de computadores e de equipamentos periféricos
78.30-2-00 - Fornecimento e gestão de recursos humanos para terceiros

CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA
206-2 - Sociedade Empresária Limitada

LOGRADOURO	NÚMERO	COMPLEMENTO
AV GOVERNADOR AGAMENON MAGALHAES	**4779**	**SALA 401 EDF ISAAC NEWTON E SALAS 402 403 404**

CEP	BAIRRO/DISTRITO	MUNICÍPIO	UF
50.070-425	**ILHA DO LEITE**	**RECIFE**	**PE**

ENDEREÇO ELETRÔNICO	TELEFONE
JUNIOR@NEWSUPRI.COM.BR	**(81) 3366-8500**

ENTE FEDERATIVO RESPONSÁVEL (EFR)
*****

SITUAÇÃO CADASTRAL	DATA DA SITUAÇÃO CADASTRAL
ATIVA	**03/11/2005**

MOTIVO DE SITUAÇÃO CADASTRAL

SITUAÇÃO ESPECIAL	DATA DA SITUAÇÃO ESPECIAL
********	********

Aprovado pela Instrução Normativa RFB nº 1.863, de 27 de dezembro de 2018.

Emitido no dia **18/09/2020** às **15:23:52** (data e hora de Brasília). Página: **1/1**

PREFEITURA DO RECIFE
SECRETARIA DE FINANÇAS
GOTM - Gerência Operacional de Tributos Mercantis

CIM - CARTÃO DE INSCRIÇÃO MUNICIPAL

COMPETÊNCIA	VÁLIDO ATÉ	SITUAÇÃO	PENDÊNCIAS	DATA CADASTRAMENTO
2020/02	10/02/2021	ATIVO COM ALVARÁ	NÃO	23/08/1994

CPF/CNPJ	INSCRIÇÃO MERCANTIL
12.707.105/0001-64	239.461-8

NOME/RAZÃO SOCIAL E NOME FANTASIA:
SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
NEWSUPRI

NATUREZA JURÍDICA
SOCIEDADE EMPRESÁRIA LIMITADA

E-MAIL
race@raceconsultoria.com.br

FONE
21257654

TRIBUTOS
ISS HOM TRIBUTAÇÃO NORMAL
TLF TRIBUTAÇÃO NORMAL

SEQÜENCIAL IMOBILIÁRIO
735535-1

ENDEREÇO DO ESTABELECIMENTO
AV GOV AGAMENON MAGALHAES 4779 SALA 401 EDF ISAAC NEWTON
ILHA DO LEITE 50070-425 RECIFE PERNAMBUCO

MÁQUINAS, MOTORES E AFINS

☐ MÁQUINA ☐ GUINDASTE ☐ FORNO MOTOR

TIPO EMPRESA
CONVENCIONAL

ENDEREÇO DE CORRESPONDÊNCIA
AV GOV AGAMENON MAGALHAES 4779 SALA 401 EDF ISAAC NEWTON
ILHA DO LEITE 50070-425 RECIFE PERNAMBUCO

OCUPAÇÃO DE ÁREA PÚBLICA

ATIVIDADE(S)
CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO AP
CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO APP

PUBLICIDADE

ACRÉSCIMO DE 2,54% EM RELAÇÃO A 2019 COM BASE NO IPCA (LEI 16.607/2000).
VERIFIQUE A DATA DE VALIDADE DO CIM. PAGAMENTOS DEVEM SER EFETUADOS NA REDE BANCÁRIA AUTORIZADA OU NAS CASAS LOTÉRICAS.
UTILIZE O 0800 0811255 PARA ATUALIZAR TELEFONES, E-MAIL E PARA TIRAR DÚVIDAS. TENHA EM MÃOS A INSCRIÇÃO MERCANTIL.

MINISTÉRIO DA FAZENDA
Secretaria da Receita Federal do Brasil
Procuradoria-Geral da Fazenda Nacional

CERTIDÃO POSITIVA COM EFEITOS DE NEGATIVA DE DÉBITOS RELATIVOS AOS TRIBUTOS FEDERAIS E À DÍVIDA ATIVA DA UNIÃO

Nome: SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA
CNPJ: 12.707.105/0001-64

Ressalvado o direito de a Fazenda Nacional cobrar e inscrever quaisquer dívidas de responsabilidade do sujeito passivo acima identificado que vierem a ser apuradas, é certificado que:

1. constam débitos administrados pela Secretaria da Receita Federal do Brasil (RFB) com exigibilidade suspensa nos termos do art. 151 da Lei nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional (CTN), ou objeto de decisão judicial que determina sua desconsideração para fins de certificação da regularidade fiscal, ou ainda não vencidos; e

2. não constam inscrições em Dívida Ativa da União (DAU) na Procuradoria-Geral da Fazenda Nacional (PGFN).

Conforme disposto nos arts. 205 e 206 do CTN, este documento tem os mesmos efeitos da certidão negativa.

Esta certidão é válida para o estabelecimento matriz e suas filiais e, no caso de ente federativo, para todos os órgãos e fundos públicos da administração direta a ele vinculados. Refere-se à situação do sujeito passivo no âmbito da RFB e da PGFN e abrange inclusive as contribuições sociais previstas nas alíneas 'a' a 'd' do parágrafo único do art. 11 da Lei nº 8.212, de 24 de julho de 1991.

A aceitação desta certidão está condicionada à verificação de sua autenticidade na Internet, nos endereços <http://rfb.gov.br> ou <http://www.pgfn.gov.br>.

Certidão emitida gratuitamente com base na Portaria Conjunta RFB/PGFN nº 1.751, de 2/10/2014.
Emitida às 04:10:37 do dia 13/08/2020 <hora e data de Brasília>.
Válida até 09/02/2021.
Código de controle da certidão: **14C2.1923.8EC1.7A0A**
Qualquer rasura ou emenda invalidará este documento.

SECRETARIA DA FAZENDA

GOVERNO DO ESTADO Pernambuco

CERTIDÃO DE REGULARIDADE FISCAL

Número da Certidão: 2020.000004667637-71 **Data de Emissão: 04/09/2020**

DADOS DO CONTRIBUINTE

Razão Social:	**SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA**
Endereço:	**AVENIDA GOVERNADOR AGAMENON MAGALHAES N. 4779, SALA 401 EDF ISAAC NEWTON E SALAS 402,403,404, ILHA DO LEITE, RECIFE - PE, CEP: 50070160**
CNPJ:	**12.707.105/0001-64**

Certificamos, observadas as disposições da legislação vigente e de acordo com os registros existentes neste órgão, que o contribuinte acima identificado está em situação **REGULAR** perante a Fazenda Pública Estadual.

A presente certidão não compreende débitos cuja exigibilidade esteja suspensa nem exclui o direito da Fazenda Pública Estadual, a qualquer tempo, cobrar valores a ela porventura devidos pelo referido requerente.

Esta certidão é válida até **02/12/2020** devendo ser confirmada sua autenticidade através do serviço "ARE VIRTUAL" na página www.sefaz.pe.gov.br.

Emitido em: 04/09/2020 02:42:27

PREFEITURA DO RECIFE
SECRETARIA DE FINANÇAS
Secretaria Executiva de Tributação

Nº da Certidão
138388805

Certidão Negativa
Débitos Fiscais

1. Denominação Social/Nome

SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA

2. CMC

239.461-8

3. Endereço

AV GOV AGAMENON MAGALHAES, 4779 SALA 401 EDF ISAAC NEWTON
BAIRRO ILHA DO LEITE, CEP 50070-425, RECIFE-PE

4. CNPJ/CPF

12.707.105/0001-64

5. Atividade Econômica

6209-10-0 SUPORTE TECNICO, MANUTENCAO E OUTROS SERVICOS EM TECNOLOGIA DA INFORMACAO
6204-00-0 CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO
8599-60-3 TREINAMENTO EM INFORMÁTICA
7733-10-0 ALUGUEL DE MÁQUINAS E EQUIPAMENTOS PARA ESCRITÓRIO
4751-20-1 Comercio varejista especializado de equipamentos e suprimentos de informatica
4614-10-0 REPRESENTANTES COMERCIAIS E AGENTES DO COM DE MÁQ, EQUIP, EMBARC E AERONAVES
7830-20-0 FORNECIMENTO E GESTÃO DE RECURSOS HUMANOS PARA TERCEIROS
9511-80-0 REPARAÇÃO E MANUTENÇÃO DE COMPUTADORES E DE EQUIPAMENTOS PERIFÉRICOS
6311-90-0 TRATAMENTO DE DADOS, PROVEDORES DE SERV DE APLIC E SERV DE HOSPED NA INTERNET

6. Descrição

Certifico, de acordo com a legislação em vigor e na conformidade com os registros cadastrais / fiscais, nesta data, que o contribuinte de que trata a presente certidão está regularizado com o erário municipal no que concerne aos lançamentos relativos aos tributos municipais.

7. Ressalva

* * * * * * * * * * *

8. Validade/Autenticidade

Esta certidão é válida por 60 (sessenta) dias a contar da data de sua expedição e sua autenticidade deverá ser confirmada na página **portalfinancas.recife.pe.gov.br/certidoes**

Certidão equivalente ao Certificado de Regularidade Fiscal, nos termos da Lei 8.666/93 e abrange as esferas administrativa e judicial (dívida ativa)

A Prefeitura do Recife poderá cobrar e inscrever quaisquer dívidas de responsabilidade do sujeito passivo acima identificado, que vierem a ser apuradas.

9. Código de Autenticidade

668.5239.1726

10. Expedida em

Recife, 08 de OUTUBRO de 2020

11. Certidão emitida com base nos pagamentos registrados até

05 de OUTUBRO de 2020

Voltar Imprimir

CAIXA ECONÔMICA FEDERAL

Certificado de Regularidade do FGTS - CRF

Inscrição: 12.707.105/0001-64

Razão Social: SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA

Endereço: AV GOVERNADOR AGAMENON MAGALHAES 4779 SALA 401 / ILHA DO LEITE / RECIFE / PE / 50070-425

A Caixa Econômica Federal, no uso da atribuição que lhe confere o Art. 7, da Lei 8.036, de 11 de maio de 1990, certifica que, nesta data, a empresa acima identificada encontra-se em situação regular perante o Fundo de Garantia do Tempo de Servico - FGTS.

O presente Certificado não servirá de prova contra cobrança de quaisquer débitos referentes a contribuições e/ou encargos devidos, decorrentes das obrigações com o FGTS.

Validade:17/10/2020 a 15/11/2020

Certificação Número: 2020101702345045542471

Informação obtida em 20/10/2020 10:45:58

A utilização deste Certificado para os fins previstos em Lei esta condicionada a verificação de autenticidade no site da Caixa: **www.caixa.gov.br**

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO

CERTIDÃO NEGATIVA DE DÉBITOS TRABALHISTAS

Nome: SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA (MATRIZ E FILIAIS)
CNPJ: 12.707.105/0001-64
Certidão nº: 16752152/2020
Expedição: 22/07/2020, às 22:03:59
Validade: 17/01/2021 - 180 (cento e oitenta) dias, contados da data de sua expedição.

Certifica-se que **SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA (MATRIZ E FILIAIS),** inscrito(a) no CNPJ sob o nº **12.707.105/0001-64, NÃO CONSTA** do Banco Nacional de Devedores Trabalhistas.
Certidão emitida com base no art. 642-A da Consolidação das Leis do Trabalho, acrescentado pela Lei nº 12.440, de 7 de julho de 2011, e na Resolução Administrativa nº 1470/2011 do Tribunal Superior do Trabalho, de 24 de agosto de 2011.
Os dados constantes desta Certidão são de responsabilidade dos Tribunais do Trabalho e estão atualizados até 2 (dois) dias anteriores à data da sua expedição.
No caso de pessoa jurídica, a Certidão atesta a empresa em relação a todos os seus estabelecimentos, agências ou filiais.
A aceitação desta certidão condiciona-se à verificação de sua autenticidade no portal do Tribunal Superior do Trabalho na Internet (http://www.tst.jus.br).
Certidão emitida gratuitamente.

INFORMAÇÃO IMPORTANTE
Do Banco Nacional de Devedores Trabalhistas constam os dados necessários à identificação das pessoas naturais e jurídicas inadimplentes perante a Justiça do Trabalho quanto às obrigações estabelecidas em sentença condenatória transitada em julgado ou em acordos judiciais trabalhistas, inclusive no concernente aos recolhimentos previdenciários, a honorários, a custas, a emolumentos ou a recolhimentos determinados em lei; ou decorrentes de execução de acordos firmados perante o Ministério Público do Trabalho ou Comissão de Conciliação Prévia.

Ao
TRIBUNAL DE JUSTIÇA DO ESTADO DA PARAÍBA

Ref. **EDITAL DE LICITAÇÃO – MODALIDADE PREGÃO ELETRÔNICO – Nº 019/2020**
PROCESSO ADMINISTRATIVO ELETRÔNICO: 2020012776

ANEXO V - DECLARAÇÕES

SUPRISERVI COMÉRCIO REPRESENTAÇÕES E SERVIÇOS LTDA, inscrita no CNPJ n.º 12.707.105/0001-64, sediada na Av. Agamenon Magalhães, 4779 - Empresarial Isaac Newton - 4º Andar – Ilha do Leite – Recife/ PE – CEP: 50.070-425, DECLARAMOS:

1- Sob as penas da lei, que até a presente data inexistem fatos impeditivos para nossa habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores. (DECLARAÇÃO DE FATOS IMPEDITIVOS)

2 - Para efeito de participação no processo licitatório pertinente ao Pregão Eletrônico n° 19/2020 do Tribunal de Justiça do Estado da Paraíba, bem assim para fins do disposto no inciso V do art. 27 da Lei n° 8.666, de 21 de junho de 1993, acrescido pela Lei nº 9.854, de 27 de outubro de 1999, que não empregamos menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não empregamos menor de 16 anos. (DECLARAÇÃO DE QUE NÃO EMPREGA MÃO DEOBRA INFANTIL)

3 - Para fins do disposto no inciso VII do art. 4º da Lei nº 10.520, de 17/07/2002, estamos cientes plenamente dos requisitos de habilitação para participar do procedimento licitatório Pregão Eletrônico nº 19/2020 do Tribunal de Justiça da Paraíba. (DECLARAÇÃO DE HABILITAÇÃO)

4 - Através deste instrumento, sem prejuízo dos ditames insertos no art. 2º, VI da Resolução CNJ 07/2005, declaramos a inexistência, bem como assumindo compromisso de não permitir ingresso nos quadros societários e/ou de empregados da Pessoa Jurídica, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive, dos magistrados ocupantes de cargos de direção ou no exercício de funções administrativas, assim como de servidores ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação, ficando desde já ciente de que a inobservância dessa vedação acarretará a rescisão imediata do fornecimento a ser celebrado com o Tribunal de Justiça do Estado da Paraíba, conforme modelo constante Anexo ao presente edital; (TERMO DECOMPROMISSO)

Recife, 02 de novembro de 2020

JOSE ALVES MUNIZ JUNIOR:34922733434

Digitally signed by JOSE ALVES MUNIZ JUNIOR:34922733434
DN: C=BR, O=ICP-Brasil, OU=Secretaria da Receita Federal do Brasil - RFB, OU=RFB e-CPF A3, OU=(EM BRANCO), OU=Autenticado por AR RG Tecnologia, CN=JOSE ALVES MUNIZ JUNIOR:34922733434
Reason: Assinado de forma digital por
Location: Recife-PE
Date: 2020-11-02 21:40:17

José Alves Muniz Junior
Diretor

você também está obrigado a usá-los, para prevenir acidentes e evitar as doenças profissionais.

Mostre ao seu novo companheiro os perigos que o cercam no trabalho.

Cada acidente é uma lição que deve ser apreciada, para evitar maiores desgraças.

Todo o acidente tem uma causa que é preciso ser pesquisada, para evitar a sua repetição.

Se você for acidentado, procure logo o socorro médico adequado. Não deixe que "entendidos" e "curiosos" concorram para o agravamento de sua lesão.

Se você não é eletricista, não se meta a fazer serviços de eletricidade.

Procure o socorro médico imediato, se você for vítima de um acidente, amanhã será tarde demais.

As máquinas não respeitam ninguém; mas você deve respeitá-las.

Atenda às recomendações dos Membros da CIPA e de seus mestres e chefes.

Conheça sempre as regras de segurança da seção onde você trabalha.

Conversa e discussão no trabalho predispõem a acidentes pela desatenção.

Leia e reflita sempre os ensinamentos contidos nos cartazes e avisos sobre prevenção de acidentes.

Os anéis, pulseiras, gravatas e mangas compridas não fazem parte do seu uniforme de trabalho.

Mantenha sempre as guardas protetoras das máquinas nos devidos lugares.

Para a máquina quando tiver que consertá-la ou lubrificá-la.

Habitue-se a trabalhar protegido contra os acidentes.

Use equipamentos de proteção adequados a seu serviço.

Conheça o manejo dos extintores e demais dispositivos de combate ao fogo existentes em seu local de trabalho. Você pode ter necessidade de usá-los algum dia.

MINISTÉRIO DO TRABALHO E EMPREGO

CARTEIRA DE TRABALHO E PREVIDÊNCIA SOCIAL

Número 86.939 Série 00074

Eden Jaime de Lima

ASSINATURA DO PORTADOR

8º TABELIONATO DE NOTAS DO RECIFE
Ivanildo de Figueiredo Andrade de Oliveira Filho
Tabelião Publico

www.tabelionatofigueiredo.com.br
Fone: (81) 3073-0800

Cópia autêntica conforme o original

Selo Digital 0073783 PBV10202006 03606

Emolumentos 4,33 TSNR 0,70 FERC 0,35 FERM 0,04
FUNSEG 0,08 ISS 0,18 Total R$ 4,51
Recife, 28/10/2020

AUGUSTO JOSE MALTA RIBEIRO SUPERVISOR NOTARIAL

Consulte Autenticidade em: www.tjpe.jus.br/selodigital

Digitalizado com CamScanner

QUALIFICAÇÃO CIVIL

Nome Eder Jairo de Lima

Loc. Nasc. Recife Est. PE Data 15/12/84

Filiação Edinalva Batista de Lima

Doc. Nº CNN 64 628 2 280 254

ESTRANGEIROS

Chegada ao Brasil em ..... / ..... / ..... Doc. Ident. Nº .....

Exp. em ..... / ..... / ..... Estado .....

Obs.: .....

Data Emissão 17/04/02 DRT PE

Assinatura do Funcionário

Sandra

ALTERAÇÕES DE IDENTIDADE

(Com relação nome, est. civil e data nasc.)

Nome .....

Doc. .....

Nome .....

Doc. .....

Nome .....

Doc. .....

Est. Civil .....

Doc. .....

Est. Civil .....

Doc. .....

Nascimento .....

Doc. .....

8º TABELIONATO DE NOTAS DO RECIFE
Ivanildo de Figueiredo Andrade de Oliveira Filho
Tabelião Público

www.tabelionatofigueiredo.com.br
Fone: (81) 3073-0800

Cópia autêntica conforme o original

Selo Digital 0073783 KYY10202006.03605

Emolumentos 4,33 TSNR 0,70 FERC 0,35 FERM 0,04
FUNSEG 0,08 ISS 0,18 Total R$ 4,51
Recife, 28/10/2020

AUGUSTO JOSE MALTA RIBEIRO SUPERVISOR NOTARIAL

Consulte Autenticidade em: www.tjpe.jus.br/selodigital

Digitalizado com CamScanner

CONTRATO DE TRABALHO

Empregador: SUPRISERVI COM REPRES E SERVICOS LTDA
CNPJ/CPF/CEI: 12.707.105/0001-64
Endereço: RUA GAL GOES MONTEIRO 308, IMBIRIBEIRA

Municipio: RECIFE UF: PE
Esp. do estabelecimento:

Cargo: ANALISTA DE SUPORTE
CBO N°: 212420
Data de admissão: 02 de Janeiro de 2018
Registro N°: 587 Fls./Ficha: 587
Remuneração especificada: R$ 5.500,00 (cinco mil e quinhentos reais) por mês.

SUPRISERVI COM. REPR. E SERVIC. LTDA
Emerson Silva
Ass. do empregador ou a rogo c/test.
Ger. Adm. Financeiro CPF: 794.717.814-34

1° ..... 2° .....

Data saída ..... de ..... de .....

.....

Ass. do empregador ou a rogo c/test.

1° ..... 2° .....

Com. Dispensa CD N° .....

8° TABELIONATO DE NOTAS DO RECIFE
Ivanildo de Figueiredo Andrade de Oliveira Filho
Tabelião Público
www.tabelionatofigueiredo.com.br
Fone: (81) 3073-0800

Cópia autêntica conforme o original

Selo Digital 0073783 KXB10202006.03604

Emolumentos 4,33 TSNR 0,70 FERC 0,35 FERM 0,04 FUNSEG 0,08 ISS 0,18 Total R$ 4,51
Recife, 28/10/2020

AUGUSTO JOSE MALTA RIBEIRO SUPERVISOR NOTARIAL

Consulte Autenticidade em www.tjpe.jus.br/selodigital

Digitalizado com CamScanner

Certificado de Revendedor Autorizado

Date: 10/28/2020

AO TRIBUNAL DE JUSTIÇA DO ESTADO DA PARAÍBA
DIRETORIA ADMINISTRATIVA - PREGOEIRO E EQUIPE DE APOIO
Ref.: PREGÃO ELETRÔNICO – Nº 019/2020 - PROCESSO ADMINISTRATIVO ELETRÔNICO: 2020012776

Fortinet, Inc. reconhece que: SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA (NEWSUPRI)

Localizado na Rua:
Agamenon Magalhães, 4779 - Empresarial Isaac Newton - 4º Andar - Ilha do Leite – Recife, RECIFE, Pernambuco 50070-425, Brazil;

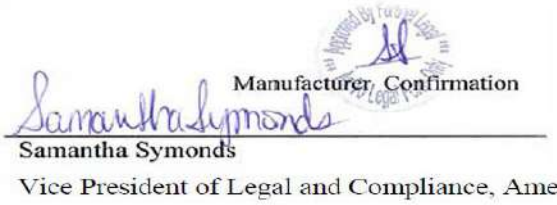
É atualmente um parceiro autorizado no BR a vender os produtos da Fortinet nas seguintes qualificacoes:

- Nivel de certificações: Advanced
- Modelo de Negócio: Integrator
- Especializações: Secure SD-WAN, LAN Edge and SD-Branch

Este certificado é emitido em 28/10/2020, e é valido até 27/11/2020

Sempre que o FortiPartner , identificado anteriormente, comprar os serviços de suporte e estes forem registrados e contratados junto à Fortinet, a Fortinet concorda em oferecer os suportes cabíveis de acordo com os termos do contrato de suporte da Fortinet, disponível em https://support.fortinet.com. A garantia do equipamento Fortinet é limitado às garantias do fabricante que se encontram no site, http://www.fortinet.com/doc/legal/EULA.pdf.

Este certificado se dá na condição do FortiPartner manter seu contrato vigente com a Fortinet e seguir as políticas e diretrizes da Fortinet. O programa de parceiros da Fortinet e suas diretrizes estão disponíveis em http://www.fortinet.com/partners/partner_program/fpp.html. Não obstante serem parceiros autorizados, os FortiPartners não representam a Fortinet e consequentemente não podem fazer declarações em nome da Fortinet.



FORTINET, INC.
899 Kifer Road
Sunnyvale, CA 94086

Telephone: +1-866-868-3678
Email: sales@fortinet.com
Website: www.fortinet.com

Data: 28 de outubro de 2020

Cliente: TRIBUNAL DE JUSTIÇA DO ESTADO DA PARAÍBA
LICITAÇÃO Nº 019/2020
PROCESSO ADMINISTRATIVO ELETRÔNICO: 2020012776

Por meio desta carta, informamos que o equipamento FortiGate modelo FG-600E permite o número de 80.000 usuários autenticados.

Atenciosamente,
Fortinet, Inc.

Digitally signed by ALEXANDRE OLIVEIRA BONATTI:07311140609
Date: 2020.10.29 10:35:01 -03'00'

Alexandre Bonatti
Director, Systems Engineering – Brasil

Observe que, não obstante qualquer disposição em contrário: (1) as obrigações da Fortinet relacionadas a especificações, licenças, suporte, assinaturas, certificações, garantias e quaisquer outras garantias do produto são: (a) inválidas para produtos que foram adulterados ou modificados por terceiros e (b) sujeita em todos os aspectos aos processos, políticas e termos padrão da Fortinet, que a Fortinet pode mudar a qualquer momento a seu exclusivo e absoluto critério; (2) A Fortinet se reserva o direito de modificar planos técnicos, roadmaps e datas de liberação a qualquer momento a exclusivo e absoluto critério da Fortinet. (3) A Fortinet se isenta de responsabilidade por erros de digitação, tradução ou impressão. (4) Este documento é para fins informativos e não se destina a criar obrigações contratuais pela Fortinet ou comprometimento promissório ou direito de confiar nas declarações. (5) Declarações aqui sobre o desempenho do produto e características podem ser contextuais, por exemplo, baseadas em testes em em um ambiente particular, como em um ambiente de laboratório, e pode não ser preciso em todos os contextos, como em um ambiente em produção. (6) O signatário deste documento está baseando todas as declarações aqui em seus conhecimentos no momento da assinatura sem qualquer obrigação para investigar as declarações, e pode confiar totalmente na revisão e informações de outros. (7) Produtos e serviços não são oferecidos gratuitamente e os direitos só são concedidos sujeitos a pagamento integral à Fortinet e seus distribuidores e revendedores, todas as vendas são finais e aplicam-se as políticas e termos e condições da Fortinet, como o EULA padrão da Fortinet e os termos de suporte, alguns dos quais estão localizados em https://www.fortinet.com/corporate/about-us/legal.html .(8) A Fortinet não tem nenhuma obrigação de atualizar e não pretende atualizar as declarações aqui contidas, mesmo que, por exemplo, o signatário descubra que as declarações são de fato falsas ou que os planos mudaram.

GRUPOMOURA

ATESTADO DE CAPACIDADE TÉCNICA E OPERACIONAL

A Acumuladores Moura S/A, inscrita no CNPJ (MF) sob o no. 09.811.654/0001-70, declara para os devidos fins, que adquiriu os produtos e serviços técnicos, detalhados abaixo, através da empresa SUPRISERVI COMÉRCIO, REPRESENTAÇÕES E SERVIÇOS LTDA – NEWSUPRI, cnpj 12707105/0001-64. Os produtos estão devidamente instalados nesta empresa e encontram-se em operação e produção. Atestamos ainda que os serviços prestados pela SUPRISERVI COMÉRCIO, REPRESENTAÇÕES E SERVIÇOS LTDA — NEWSUPRI têm sido executados sempre com elevado padrão de qualidade e rapidez no atendimento dos chamados, estando tudo de acordo com os prazos estabelecidos.

PRODUTOS
Blade Enclosures HP Serie C, com Módulos de interconexão virtual Convergente para Blade Enclosures
Servidores Blade HPE Proliant Serie BL4XX (2P)
Servidores Rack HPE Proliant Serie DL3XX (2P)
Servidores Rack HPE Proliant Serie DL380 com solução de hiperconvergencia HPE VSA
Servidores Torre HPE Proliant Serie ML3xx 92P)
Switches Aruba Serie 2000
Switches Ethernet Chassi HP Serie 8000
Switches Ethernet Rack HP Serie 5000
Switches Ethernet Rack HP Serie 1000/2000/3000
HP WLAN Controller
HP WLAN Access Point
Disk Backup Apppliance HPE StoreOnce
Tape Library HPE MSL
HP Switches Fibre Channel Serie B
Roteador Ethernet Cisco
Storage HPE 3PAR Serie 8000
Storage HPE 3PAR Serie 7000
Storage HPE EVA Serie P6000
Appliance Fortinet Fortigate 90D, 300C, 1000D, 1500D
Appliance Fortinet FortiManeger
Appliance Fortinet FortiAnalizer
Appliance Fortinet FortiMail

Fábrica
Rua Diário de Pernambuco, 195
Fone (081) 3726 1044 Fax (081) 3726 2032
CEP 55150-000 Belo Jardim PE Brasil

Escritório Central
Estrada da Batalha, 4900 Prazeres
Fone (081) 21211600 Fax (081) 21211644
CEP 54315-570 Jaboatão dos Guararapes PE Brasil

GRUPOMOURA

SOFTWARES
HPE Insigth Control e IRS
HPE (Microfocus) Data Protector
HPE IMC
HPE Virtual Storage Appliance
HP 3PAR Software
VMware vSphere e vCenter
Microsoft Windows Server
Microsoft Hyper-v
Microsoft Sharepoint Server
Microsoft SQL Server
Microsoft Link Server
Microsoft Exchange Server
Microsoft System Center
Microsoft Office 365
TREINAMENTOS
Treinamentos oficiais HPE
Treinamentos oficiais Fortinet

Fábrica
Rua Diário de Pernambuco, 195
Fone (081) 3726 1044 Fax (081) 3726 2032
CEP 55150-000 Belo Jardim PE Brasil

Escritório Central
Estrada da Batalha, 4900 Prazeres
Fone (081) 21211600 Fax (081) 21211644
CEP 54315-570 Jaboatão dos Guararapes PE Brasil

GRUPOMOURA

SERVIÇOS **Projetos de Implementação (Visão/Escopo, Planejamento, Implantação, Integração, Migração e Documentação), Treinamento hands on, Serviços de Manutenção e Suporte, Serviços de Administração e Melhoria Continua.**
Servidores (HPE Proliant Rack, Torre e Blades)
SAN/Storage (HPE Brocade, Storages EVA e 3Par)
Datacenter Networking L2/L3 e Convergencia LAN/SAN (HPE Flex Fabric)
Edge Networking WLAN e Switching (HPE MSM)
Backup (HPE Data Protector, StoreOnce e StoreEver)
Alta Disponibilidade (MS Cluster Services, HPE 3Par
Hiperconvergência (HPE VSA)
Gerenciamento de Infraestrutura (HPE OneView, HPE IMC, MS System Center, Fortinet FortiManeger e FortiAnalyzer),
Virtualização de Servidores (VMware vSphere e MS Hyper-V) e Desktops (MS RDS)
Segurança (UTM, NgFW, IsFW, e-Mail, AD)
Colaboração (Microsoft Exchange, Skype e O365)

Belo Jardim (PE), 04/09/2018.

Assinatura

ACUMULADORES MOURA S.A.
Luis João Torres
GERENTE DE TIC
CPF: 427. 405.094-72

Nome completo	Luis João Torres		
Cargo	Gerente de Infraestrutura de TIC	**Setor**	DTISS
e-mail	luis.torres@grupomoura.com	**Telefone**	81 3411-1186

Comprovação Técnica- Equipamentos e Softwares ofertados

Item	DESCRIÇÃO	Comprovação	Página	Texto
1	**Objeto**			
1.1.	Aquisição de solução de Segurança da Informação com gerenciamento centralizado, incluindo equipamentos, softwares, licenciamentos, treinamento, garantia e suporte técnico para o Poder Judiciário do Estado da Paraíba de acordo com as especificações técnicas e quantidades constantes neste Termo de Referência e seus anexos.	-	-	
2	**Arquitetura**	-	-	-
2.1.	A solução do presente objeto é composta por firewalls remotos conectados a um firewall concentrador, gerenciados de forma centralizada.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	-	*A solução do presente objeto é composta por firewalls remotos conectados a um firewall concentrador, gerenciados de forma centralizada.*
2.2.	Os firewalls remotos devem ser capazes de encaminhar pacotes para serem analisados pelo firewall concentrador.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	-	*Os firewalls remotos (FortiGate 60F e FortiGate 100F) são capazes de encaminhar pacotes para serem analisados pelo firewall concentrador (FortiGate 600E).*

2.3.	O gerenciamento centralizado é composto por um sistema que administra, configura e gerencia todos os firewalls da solução do presente objeto.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	-	*O gerenciamento centralizado (FortiManager) é composto por um sistema que administra, configura e gerencia todos os firewalls da solução do presente objeto.*
2.4.	Todos os equipamentos firewall, a solução de gerenciamento centralizado e a solução de gerenciamento de logs devem ser do mesmo fabricante.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	-	*Todos os equipamentos firewall (FortiGate), a solução de gerenciamento centralizado (FortiMananger) e a solução de gerenciamento de logs (FortiAnalyzer) são do mesmo fabricante.*
3	**Licenciamento**	-	-	-
3.1	**Licença Padrão**	-	-	-
3.1.1.	Entende-se por Licença Padrão a licença de uso do fabricante em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas neste Termo, com exceção aos itens relacionados à Atualização de Assinaturas de Proteção.	-		*Ciente*

3.1.2.	Entende-se por Atualização de Assinaturas de Proteção todas as funcionalidades, manuais ou automatizadas, necessárias para manter a solução em seu nível de identificação e proteção mais atualizado, tais como: atualização de assinaturas de prevenção de intrusão, assinaturas de identificação de vírus, assinaturas de identificação de aplicações, listas de classificação de URLs, listas de geolocalização, listas de endereços IPs utilizados por botnets, listas de endereços IPs de reputação duvidosa etc.	-		*Ciente*
3.1.3.	Todos os equipamentos firewall devem possuir esta licença ativada.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	-	*Todos os equipamentos firewall possuem esta licença ativada.*
3.2	**Licença de Atualização de Segurança**	-	-	-
3.2.1.	Entende-se por Licença de Atualização de Segurança a licença de uso do fabricante que permita a utilização das funcionalidades e quantidades mencionadas neste Termo para os itens relacionados à Atualização de Assinaturas de Proteção (item 3.1.2).	Ciente	-	-
3.2.2.	A licença deve permitir que todas as assinaturas, listas e demais métodos de detecção e prevenção de ameaças e de filtros de conteúdo e aplicação empregados pela solução sejam atualizados até suas últimas versões disponíveis.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGuard_Security_Services.pdf	2-3	*Subscription Benefits* *Up-to-the minute threat intelligence in real time to stop the latest threats* *Seção* Subscription Services
3.2.3.	As Licenças de Atualização de Segurança devem ter prazo de vigência de 60 (sessenta) meses, contados a partir da aplicação destas nos produtos.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGuard_Security_Services.pdf	-	*As Licenças de Atualização de Segurança (FortiGuard Bundle UNIFIED PROTECTION)estão configuradas com prazo de vigência de 60 (sessenta) meses, contados a partir da aplicação destas nos produtos.*
4	**Firewall**	-	-	-
4.1	**Hardware**	-	-	-

4.1.1.	Deve ser fornecido em formato appliance físico.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf	1,2	Appliance FortiGate-60F Appliance FortiGate-100F Appliance FortiGate-600E
4.1.2.	Deve ser novo, sem uso, entregue em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	-	*São novos, sem uso, serão entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais.*
4.1.3.	Nenhum dos equipamentos fornecidos podem estar em modo End of Life, End of Sale e End of Support.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	-	*Nenhum dos equipamentos fornecidos estão em modo End of Life, End of Sale e End of Support.*
4.1.4.	Deve ser apropriado para o uso em ambiente tropical com umidade relativa na faixa de 10 a 90% (sem condensação) e temperatura ambiente na faixa de 0 a 40°C.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdfhttps://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdfhttps://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	6, 5, 5	Humidity 10–90% non-condensingOperating Temperature 32–104°F (0–40°C)

4.1.5.	Deve possuir fonte com alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz ou auto-ranging. Deve vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	6, 5, 5	Power Required 100–240V AC, 50–60 Hz Power Source 100–240V 50–60Hz Os Firewalls acompanham cabo de alimentação com 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.
4.1.6.	Deve possuir, no mínimo, 1 (uma) interface Ethernet para gerenciamento.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	3, 3	FG-60F: 10x GE RJ45 FG-100F: 3. 2x GE RJ45 MGMT/DMZ Ports FG-600E: 3. 2x GE RJ45 MGMT/HA Ports *FG-60F: 8 Portas serão utilizadas para atender ao item 4.6.10.* *2 Portas estarão disponíveis para atuar como interface de Gerenciamento.*
4.1.7.	Deve ser fornecido em sua capacidade máxima de processamento, memória e armazenamento interno.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	-	*Os Firewalls estão sendo fornecidos em sua capacidade máxima de processamento, memória e armazenamento interno.* *Não existe upgrade de CPU, Memória e Disco para os Appliances FG-60F, FG-100F e FG-600E.*

4.1.8.	Deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, inclusive com seus respectivos transceivers instalados, sem custos adicionais.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	-	*Os Firewalls estão sendo fornecidos com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, inclusive com seus respectivos transceivers instalados, sem custos adicionais.*
4.1.9.	Deve possuir certificação de conformidade sustentável de acordo com os padrões EPA (Environmental Protection Agency) ou similares, tais como EnergyStar, RoHS (Restriction on Harzardous Substances) ou WEEE (Waste Electrical and Eletronic Equipment).	https://www.fortinet.com/corporate/about-us/corporate-social-responsibility.html	-	RoHS compliance WEEE compliance
4.2.1.	**Funcionalidades Básicas**	-	-	-
4.2.1.1.	Deve possuir MIB própria contemplando, no mínimo, indicadores de estado do hardware e de performance do equipamento.	FORTINET-FORTIGATE-MIB	-	fgSysCpuUsage OBJECT-TYPE"...Current CPU usage (percentage)..."fgSysMemUsage OBJECT-TYPE"...Current memory utilization (percentage)..."fgHwSensorEntry OBJECT-TYPE SYNTAX FgHwSensorEntry MAX-ACCESS not-accessible STATUS current DESCRIPTION "An entry containing the name, value, and alarm status of a given hardware sensor" INDEX { fgHwSensorEntIndex } ::= { fgHwSensorTable 1 }FgHwSensorEntry ::= SEQUENCE { fgHwSensorEntIndex FnIndex, fgHwSensorEntName DisplayString, fgHwSensorEntValue DisplayString, fgHwSensorEntAlarmStatus INTEGER

4.2.1.2.	Deve suportar o envio de notificações via e-mail, SNMP traps e mensagens de log.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/893788/alert-email https://docs.fortinet.com/document/fortigate/6.0.0/handbook/92582/snmp https://docs.fortinet.com/document/fortigate/6.0.0/handbook/289288/logging	-	"Alert emails provide an efficient and direct method of notifying an administrator of events." "...You can configure the hardware, such as the FortiGate SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers..." "...you to monitor, store, and report traffic information and FortiGate events, including attempted log ins and hardware status..."
4.2.1.3.	Deve permitir o acesso ao equipamento via SSH e interface web HTTPS.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	Management access: HTTPS via web browser, SSH, telnet, console
4.2.1.4.	A comunicação entre a estação de trabalho do administrador e o firewall deve ser autenticada e criptografada.	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/241541/connecting-using-a-web-browser	-	"...an interface must be configured to allow administrative access over HTTPS..."
4.2.1.5.	Deve informar a utilização dos recursos de CPU, memória e atividade de rede.	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/882981/dashboard-widgets https://docs.fortinet.com/document/fortigate/6.0.0/handbook/799410/fortiview-consoles	-	"...System Usage: System usage information, such as CPU, memory, and disk usage, as well as the number of active sessions..." "...Interfaces displays the number of interfaces connected to your network, how many sessions there are in each interface, and what sort of traffic is occurring..."
4.2.1.6.	Deve possuir visualização mínima sumarizada de aplicações, ameaças, URLs, endereços de origem, endereços de destino, levando-se em conta o quantitativo de sessões, de consumo de banda e categorização.	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/433781/fortiview-monitors-and-widgets	-	FortiView monitors and widgets FortiView Sources FortiView Destinations FortiView Applications FortiView Websites FortiView Policies FortiView Sessions

4.2.1.7.	Deve possuir a funcionalidade de exportação automática dos logs para servidor syslog e para a Solução de Gerenciamento de Logs.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	Logging facilities support: Local memory & storage (if available), multiple syslog servers, multiple FortiAnalyzers, WebTrends servers, FortiCloud hosted service
4.2.2.	**Rede**	-	-	-
4.2.2.1.	Deve suportar os protocolos IPv4 e IPv6.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	1	Highlights — What's New Consolidate IPv4 and IPv6 policy configuration
4.2.2.2.	Deve suportar VLAN no padrão 802.1q.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	Layer-2 interface modes: Port aggregated, loopback, VLANs (802.1Q and Trunking), virtual hardware, software, and VLAN switches
4.2.2.3.	Deve suportar os protocolos DHCP e DHCPv6 e suas funcionalidades como cliente, servidor e relay.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/2c229bb9-78ed-11ea-9384-00505692583a/FortiOS-6.4-Supported_RFCs.pdf https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/783526/dhcp-server	7-8	RFC 2131: Dynamic Host Configuration Protocol RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6) "..You can configure one or more DHCP servers on any FortiGate interface..." "..You can configure a FortiGate interface as a DHCP relay..."
4.2.2.4.	Deve suportar Jumbo Frames.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/822669/interface-mtu-packet-size	-	"...Jumbo frames are supported on FortiGate models..."
4.2.2.5.	Deve suportar subinterfaces Ethernet lógicas.	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/402940/vlans	-	"...You can define VLAN subinterfaces on all FortiGate physical interfaces..."
4.2.2.6.	Deve suportar o protocolo NTP.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	9	Essential Network Services - A wealth of networking services such as DHCP, DNS server, NTP server and more

4.2.2.7	Deve implementar mecanismo de conversão de endereços NAT (Network Address Translation), de forma a possibilitar a realização de NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional (possibilitando que um endereço tenha mais de um NAT dependendo da origem, destino ou porta).	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/474356/static-nat https://docs.fortinet.com/document/fortigate/6.0.0/handbook/248992/dynamic-nat https://docs.fortinet.com/document/fortigate/6.0.0/handbook/801437/ip-pools https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/898655/static-snat https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/155333/virtual-ips-with-port-forwarding	- - - -	Static NAT "...In FortiGate firewall configurations this is most commonly done with the use of Virtual IP addressing..." Dynamic NAT "..In the FortiGate firewall this can be done by using IP Pools..." "..IP Pools are a mechanism that allow sessions leaving the FortiGate Firewall to use NAT..." Seção "Static SNAT" "Virtual IPs with port forwarding"
4.2.2.8	Deve permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/986892/sample-logs-by-log-type	-	# Corresponding traffic log # "...date=2019-05-13 time=16:29:50..." "...srcip=10.1.100.11..." "...dstip=185.244.31.158..." "...trandisp="snat" transip=172.16.200.2..."
4.2.2.9	Deve suportar tradução de porta (PAT).	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	NAT support: NAT64, NAT46, static NAT, dynamic NAT, PAT, Full Cone NAT, STUN
4.2.2.10	Deve suportar as funcionalidades de roteamento estático e dinâmico em IPv4 e IPv6.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/691160/routing-concepts	-	The type values assigned to FortiGate routes (Static, Connected, RIP, OSPF, or BGP). "...Static: The static routes that have been added to the routing table manually..." "...OSPF: All routes learned through OSPF..." "...OSPF6: All routes learned through OSPF version 6 (which enables the sharing of routes through IPv6 networks)..."
4.2.2.11	Deve suportar os protocolos RIP, OSPF v2, OSPF v3 e BGP v4.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	Dynamic routing protocols: RIPv1 and v2, OSPF v2 and v3, ISIS, BGP4

4.2.2.12	Deve suportar os protocolos IGMP v2, IGMP v3, PIM-SM.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/308396/sparse-mode https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	- 12	"To receive multicast traffic, a client application can use Internet Group Management Protocol (IGMP) version 1 (RFC 1112), 2 (RFC 2236), or 3 (RFC 3376)..." Multicast traffic: sparse and dense mode, PIM support
4.2.2.13	Deve suportar Virtual Routing Redundancy Protocol (VRRP) ou equivalente.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	8	Support for industry-standard VRRP and various proprietary solutions, with ability to combine more than one high availability solution into a single configuration
4.2.2.14	Deve suportar os protocolos SNMP v2 e SNMP v3.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	- SNMP v1 and v2c support - SNMP v3 implementation includes support for queries, traps, authentication, and privacy
4.2.2.15	Deve permitir monitorar, via SNMP, falhas de hardware, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN, CPU, memória, status do cluster de Alta Disponibilidade e estatísticas de uso das interfaces de rede.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/92582/snmp FORTINET-FORTIGATE-MIB	-	"SNMP fields contain information about the FortiGate unit, such as CPU usage percentage or the number of sessions." "Power Supply Failure event trap is available only on some models." "... you can use the value ifHighSpeed. It reports interface speeds in megabits/second..." "..fgVpnTunnelUpCount OBJECT-TYPE The number of IPsec VPN tunnels with at least one SA..." fgSysMemUsage OBJECT-TYPE "...Current memory utilization (percentage)..." fgHaSystemMode OBJECT-TYPE "High-availability mode (Standalone, A-A or A-P)"
4.2.2.16	Deve suportar Policy Based Routing (PBR), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD46603	-	"Technical Tip: Configuring the firewall Policy Routes"

4.2.3.	**Autenticação e Identificação de Usuários**	-	-	-
4.2.3.1.	Deve promover a integração com serviços de diretório LDAP e Active Directory, baseados em caracteres da língua portuguesa, para a identificação, autenticação, autorização e registro de eventos de acessos ou ameaças.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/888827/poll-active-directory-server https://docs.fortinet.com/document/fortigate/6.2.2/cookbook/896276/cli-basics	10 - -	Local user database and remote user authentication service support: LDAP "The FortiGate unit can authenticate users and allow them network access based on groups membership in Windows Active Directory (AD)" Seção "Language support and regular expressions"
4.2.3.2.	Deve identificar de forma transparente os usuários autenticados por meio de serviço de diretório LDAP ou Active Directory.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/615946/agent-based-fsso-for-windows-ad https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/731999/fsso-in-polling-mode-for-windows-ad	-	Single-sign-on: Integration with Windows AD Agent-based FSSO for Windows AD FSSO in polling mode for Windows AD
4.2.3.3.	Não será permitida a utilização de agentes instalados nos servidores LDAP, Active Directory, proxies internos e equipamentos dos usuários, nem configuração adicional no navegador.	N/A	N/A	*A solução ofertada não necessita de utilização de agentes instalados nos servidores LDAP, Active Directory, proxies internos e equipamentos dos usuários, nem configuração adicional no navegador.*
4.2.3.4.	Não será permitida a interceptação ou espelhamento do tráfego destinado aos servidores LDAP, Active Directory e proxies internos.	N/A	N/A	*A solução ofertada não utiliza interceptação ou espelhamento do tráfego destinado aos servidores LDAP, Active Directory e proxies internos.*
4.2.3.5.	Deve possuir portal de autenticação (captive portal) para a identificação e autenticação de usuários não registrados ou não reconhecidos.	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/574723/interface-settings	-	"...After enabling captive portal authentication, you can configure the authentication portal, user and group access..."

4.2.3.6.	O portal de autenticação deve ser capaz de identificar e autenticar usuários cadastrados em serviço de diretório LDAP e Active Directory.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/868644/captive-portalshttps://docs.fortinet.com/document/fortigate/6.0.0/handbook/518646/users-and-user-groups#User_groups	--	"...User Groups: Select permitted user groups.""User groups a remote user account (password stored on a RADIUS, LDAP, or TACACS+ server)"
4.2.3.7.	Deve permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP ou ao Active Directory.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies	-	Firewall policies Source User(s) This parameter is based on a user identity that can be from a number of authentication authorities. It will be an account or group that has been set up in advance that can be selected from the drop down menu. The exception to this is the feature that allows the importing of LDAP Users..."
4.2.3.8.	Deve registrar a identificação do usuário em todos os logs de eventos de acesso ou de ameaças gerados pelo equipamento.	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/536166/viewing-event-logs	-	"User Events View events relating to users"
4.2.3.9.	Deve registrar os eventos dos usuários em tempo real, sem a utilização de processos em lote (batches) ou processos de correlação após a ocorrência do evento em questão.	https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/476970	-	FortiView is a logging tool made up of a number of dashboards that show real time and historical logs.
4.2.3.10.	Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/829757/administrators	-	"...For example, you can configure a profile so that the administrator can only read/write Firewall configuration, which includes firewall policies, addresses, services, schedules, packet capture, and some other parts of the FortiGate configuration. Any other aspects of the FortiGate configuration, including VPNs and security profiles, would be hidden from this administrator."
4.2.4.	**Geolocalização**	-	-	-

4.2.4.1.	Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/133721/fortiview	-	"FortiView is the FortiOS log view tool which is a comprehensive monitoring system for your network. FortiView integrates real-time and historical data into a single view on your FortiGate." "...The following are just some of the FortiView categories: Sources, Destinations, Applications, Cloud Application, Country..."
4.2.4.2.	Deve identificar, no mínimo, 180 países.	4.2.4.2_253_Paises_Codigo.png	-	"Total countries loaded: 253"
4.2.4.3.	Deve armazenar as listas de geolocalização no próprio equipamento.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD40832	-	"This article describes how to update the GeoIP database on FortiGate equipment. The GeoIP database version does not always update when the following command is run: # execute update now"
4.2.4.4.	Deve permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD40500	-	"This article shows the configuration to protect a server from attacks from countries that user has no business with."
4.2.4.5.	Deve possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/133721/fortiview	-	"FortiView is the FortiOS log view tool which is a comprehensive monitoring system for your network. FortiView integrates real-time and historical data into a single view on your FortiGate." "...The following are just some of the FortiView categories: Sources, Destinations, Applications, Cloud Application, Country..."
4.2.5.	**VPN**	-	-	-

4.2.5.1.	Deve suportar VPN site-to-site em topologia Full Meshed (todos os gateways possuem links específicos para todos os demais gateways) e Estrela (gateways satélites se comunicam somente com um único gateway central).	https://docs.fortinet.com/document/fortimanager/6.4.0/administration-guide/556949/configuring-a-full-mesh-vpn-topology-within-a-vpn-console-example https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/755287/redundant-hub-and-spoke-vpn	-	"Configuring a full mesh VPN topology within a VPN console" "Redundant hub and spoke VPN"
4.2.5.2.	Deve suportar criptografia 3DES, AES-128, AES-256.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	IPsec VPN:- Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128. AES192, AES256, ARIA128, ARIA192, ARIA256, SEED
4.2.5.3.	Deve suportar integridade de dados com MD5, SHA-1 e SHA-256.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	IPsec VPN: - Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
4.2.5.4.	Deve suportar o protocolo IKE, fases I e II.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	IPsec VPN: - Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
4.2.5.5.	Deve suportar os algoritmos RSA e Diffie-Hellman groups 1, 2, 5 e 14.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/156465/configuring-phase-2-parameters	-	"Diffie-Hellman Group - Select one Diffie-Hellman group (1, 2, 5, 14 through 21, or 27 through 30)."
4.2.5.6.	Deve suportar Certificado Digital X.509.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	10	PKI and certificates: X.509 certificates, SCEP support, Certificate Signing Request (CSR) creation, autorenewal of certificates before expiry, OCSP support
4.2.5.7.	Deve suportar NAT-T (NAT Transversal).	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	IPsec VPN: - XAuth for dialup users: Server type option (PAP, CHAP, Auto), NAT Traversal option - Configurable IKE encryption key expiry, NAT traversal keepalive frequency
4.2.5.8.	Deve permitir a criação de túneis VPN SSL/TLS e IPSec.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	6	Feature / VPN SSL and IPsec VPN wizards
4.2.5.9.	Deve suportar VPN IPSec client-to-site (acesso remoto).	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf	1, 2	"Max Client to G/W IPSEC Tunnels "

4.2.5.10.	Deve possuir cliente próprio para instalação nos dispositivos móveis dos usuários, sem custo adicional.	https://docs.fortinet.com/document/forticlient/6.2.0/new-features/673187/free-vpn-client	-	For FortiGate administrators, a free version of FortiClient VPN is available which supports basic IPsec and SSL VPN and does not require registration with EMS.
4.2.5.11.	Deve permitir que o usuário realize a conexão VPN por meio de cliente instalado no sistema operacional Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 8.1 (32 e 64 bits), Windows 10 (32 e 64 bits), Apple IOS, Android, Mac OS 10 ou Linux do seu equipamento ou por meio de interface web do tipo portal.	https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/912474/ssl-vpn-using-web-and-tunnel-mode	-	"...allow remote users to access the corporate network using an SSL VPN, connecting either by web mode using a web browser..."
4.2.5.12.	O acesso por meio da interface Web deverá ser compatível com, no mínimo, os navegadores Internet Explorer 9 ou superior e Firefox 4.0 ou superior.	https://docs.fortinet.com/document/fortigate/6.2.3/fortios-release-notes/973252/ssl-vpn-support	-	Microsoft Windows 10 (64-bit) Microsoft Edge Mozilla Firefox version 61 Google Chrome version 68
4.2.5.13.	Deve suportar atribuição de endereço IP nos clientes remotos de VPN.	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/6896/fortigate-as-dialup-client	-	config firewall address edit "client_range" set type iprange set start-ip 10.10.10.1 set end-ip 10.10.10.200
4.2.5.14.	Deve suportar atribuição de DNS nos clientes remotos de VPN.	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/6896/fortigate-as-dialup-client	-	set dns-mode auto
4.2.5.15.	Deve suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF e BGP.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD47665 https://kb.fortinet.com/kb/documentLink.do?externalID=FD38847	-	"Technical Tip: Dynamic dial-up VPN with OSPF" "Technical Note: Dynamic routing (BGP) over IPsec tunnel"
4.2.5.16.	O túnel IPSec VPN do cliente ao gateway (client-to-site) deve fornecer uma solução de autenticação única (single-sign-on) aos usuários, integrando-se com as ferramentas de Windows login.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD45619	-	"This article describes how to configure SSO Auto with LDAP users for SSL-VPN bookmarks."

4.2.5.17.	Deve permitir criar políticas por usuário e grupos para tráfego de VPN client-to-site.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/527388/multiple-user-groups-with-different-access-permissions	-	"You need to define security policies to permit your SSL VPN clients, web-mode or tunnel-mode, to connect to the protected networks behind the FortiGate unit."
4.2.5.18.	Deve suportar autoridade certificadora integrada ao gateway VPN ou à solução de gerenciamento centralizado.	https://docs.fortinet.com/document/fortimanager/6.2.0/administration-guide/549422/certificate-templates	-	Certificate templates The certificate templates menu allows you to create certificate templates for an external certificate authority (CA) or the local FortiManager CA.
4.2.5.19.	Deve promover a integração com diretórios LDAP e Active Directory para a autenticação de usuários de VPN e regras de acesso.	https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/115783/ssl-vpn-with-ldap-user-authentication	-	"This is a sample configuration of SSL VPN for LDAP users. In this example, the LDAP server is a Windows 2012 AD server. A user ldu1 is configured on Windows 2012 AD server."

4.2.5.20.	Deve suportar os métodos de autenticação de VPN: usuário e senha de base interna do próprio equipamento, usuário e senha de diretório LDAP, usuário e senha do Active Directory, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao Active Directory, certificação digital por meio de certificados emitidos por autoridade certificadora no padrão ICP-Brasil.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/544195/ssl-vpn-with-local-user-password-policy https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/688719/ssl-vpn-with-ldap-user-password-renew https://docs.fortinet.com/document/fortimanager/6.2.0/administration-guide/549422/certificate-templates https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/680736/microsoft-ca-deep-packet-inspection https://kb.fortinet.com/kb/documentLink.do?externalID=FD48647	-	**usuário e senha de base interna do próprio equipamento,** - SSL VPN with local user password policy **usuário e senha de diretório LDAP,** **usuário e senha do Active Directory,** This is a sample configuration of SSL VPN for LDAP users with Force Password Change on next logon. In this example, the LDAP server is a Windows 2012 AD server. **certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado,** - The certificate templates menu allows you to create certificate templates for an external certificate authority (CA) or the local FortiManager CA. **certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao Active Directory,** An existing Microsoft root CA can be used to issue a subordinate CA (sub CA) certificate that is installed as a DPI certificate on the FortiGate. **certificação digital por meio de certificados emitidos por autoridade certificadora no padrão ICP-Brasil.** - This article describes how to authenticate PKI users on FortiGate via SSL VPN using two factor authentication with certificate.
4.2.5.21.	Deve suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKCS#12.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/943479/certificate-based-authentication#Example	-	Seção "To import a PKCS12 certificate from the CLI"

4.2.5.22.	Deve suportar a solicitação de emissão de certificados à uma autoridade certificadora de confiança (enrollment) via SCEP (Simple Certificate Enrollment Protocol) ou CSR (Certificate Signing Requests).	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/943479/certificate-based-authentication#Example	-	In Enrollment Method, you have two methods to choose from. Select File Based to generate the certificate request, or Online SCEP to obtain a signed SCEP-based certificate automatically over the network. For the SCEP method, enter the URL of the SCEP server from which to retrieve the CA certificate, and the CA server challenge password.
4.2.5.23.	Deve suportar a leitura e verificação de CRLs (Certification Revogation Lists).	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/943479/certificate-based-authentication	-	Seção "Certificate revocation list"
4.2.5.24.	Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/350451/configuring-security-policieshttps://help.fortinet.com/fmgr/50hlp/56/5-6-2/FMG-FAZ/1900_FortiView/0015_Summary_list.htm	-	"The SSL VPN security policy specifies...""...The UTM features and logging that are applied to the connection.""FortiView - VPN - SSL & Dialup IPsec""Displays the users who are accessing the network by using the following types of security over a virtual private network (VPN) tunnel: secure socket layers (SSL) and Internet protocol security (IPsec)."
4.2.6.	**Qualidade de Serviço (QoS)**	-	-	-

4.2.6.1.	Deve permitir o controle de políticas de uso com base nas aplicações: permitir, negar, inspecionar, agendar, e controlar o uso da largura de banda que utilizam cada aplicação ou usuário.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/19814/basic-category-filters-and-overrides https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/122688/traffic-shaping-schedules https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	- - 12	"Basic category filters and overrides" "Under Categories, left click the icon next to the category name to view a dropdown of actions: Allow, Monitor, Block..." "...apply a traffic shaper or shaping group to the traffic, including using schedules..." "Traffic shaping and QoS per policy or applications: Shared policy shaping, per-IP shaping, interface-based traffic shaping, maximum and guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS), ,Differentiated Services (DiffServ) and Forward Error Correction (FEC) for VPN support"
4.2.6.2.	Deve suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp).	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/204835/configuring-application-control-traffic-shaping https://docs.fortinet.com/document/fortigate/6.0.0/handbook/350790/configuring-per-ip-traffic-shaping	- -	" Applying traffic shaping to applications is useful for managing bandwidth-intensive applications, such as YouTube, that use the same TCP and UDP port numbers as mission-critical applications." "Per-IP traffic shaping allows you to define traffic control on a more granular level by managing bandwidth use by user IP addresses." "Traffic shaping by IP address allows you to apply traffic shaping to all source IP addresses in the security..."
4.2.6.3.	Deve suportar a priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	FIREWALL: VoIP traffic support: SIP/H.323 /SCCP NAT traversal, RTP pin holing

4.2.6.4.	Deve suportar a marcação de pacotes DiffServ.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	Traffic shaping and QoS per policy or applications: Differentiated Services (DiffServ) and Forward Error Correction (FEC) for VPN support
4.2.6.5.	Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/575292/all-sessions	-	**Aplicações / Sessões**The All Sessions console provides information about all FortiGate traffic. This console can be filtered by Application, Country, Destination Interface, Destination IP, Destination Port, NAT Source IP, NAT Source Port, Policy, Protocol, Source, Source Interface, Source IP, and Source Port. **bytes**This would be useful to display alongside other columns such as the Source, Destination, and Bytes (Sent/Received) columns, as patterns or inconsistencies can be analyzed.**usuários**From the All Sessions console, a wide variety of filters can be applied to sort the session data. In this example, the All Sessions filters will be used to locate a specific user's recent Skype activity.
4.2.7.	Balanceamento de Links	-	-	-

4.2.7.1.	Deve implementar balanceamento de links utilizando as seguintes métricas e critérios para a escolha do caminho: aplicações, jitter, latência e perda de pacotes, permitindo que administradores configurem os valores de tais parâmetros para definir por qual interface certo tipo de tráfego será enviado	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/382233/performance-sla-sla-targets	12 -	SD WAN "WAN link checks for SLAs:" "...- Monitoring criteria including latency, jitter, and packet loss..." "Multi-path intelligence using rules defined by:" "...- Destination address and/or a selection of over 3,000 applications..." Latency threshold: Latency for SLA to make decision, in milliseconds (0 - 10000000, default = 5). Jitter threshold: Jitter for SLA to make decision, in milliseconds (0 - 10000000, default = 5). Packet loss threshold: Packet loss for SLA to make decision, in percentage (0 - 100, default = 0).
4.2.7.1.1	Caso o item acima não seja atendido em sua totalidade, será aceita composição com outro equipamento, do tipo appliance físico, desde que a configuração seja realizada através da interface de gerenciamento do firewall e da Solução de Gerenciamento Centralizada, sem nenhum ônus para a CONTRATANTE, garantindo o pleno atendimento das métricas e critérios para a escolha do caminho, segundo o item acima a) O appliance físico do item anterior deve possuir throughput igual ou superior à discriminada no throughput das “funcionalidades de Filtro de Pacotes, IPS, Filtro de Conteúdo e Proteção contra Malwares habilitadas simultaneamente” do respectivo firewall. b) O appliance físico do item anterior deve possuir os mesmos requisitos de fontes de	-	-	-

	alimentação e de afixação em rack, quando exigidos, do respectivo firewall.			
4.2.7.2	Os valores dos parâmetros jitter e latência devem poder ser configurados em unidade mínima de milissegundos (ms).	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/382233/performance-sla-sla-targets	-	Latency threshold: Latency for SLA to make decision, in milliseconds (0 - 10000000, default = 5). Jitter threshold: Jitter for SLA to make decision, in milliseconds (0 - 10000000, default = 5). Packet loss threshold: Packet loss for SLA to make decision, in percentage (0 - 100, default = 0).
4.2.7.3	A interface virtual de balanceamento deve suportar agregar no mínimo 4 (quatro)interfaces, podendo ser do tipo: física, subinterface e VPN.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/19246/sd-wanhttps://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/218559/configuring-the-sd-wan-interface	--	At least one interface must be configured for SD-WAN to function; up to 255 member interfaces can be configuredFirst, SD-WAN must be enabled and member interfaces must be selected. The selected FortiGate interfaces can be of any type (physical, aggregate, VLAN, IPsec, and others)
4.2.7.4	Deve suportar balanceamento de link por hash do IP de origem e destino.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	WAN load balancing (weighted) algorithms by: volume, sessions, source-destination IP, Source IP, and spillover
4.2.7.5	Deve suportar balanceamento de link por peso. Nesta opção deve ser possível definir o peso de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, 4 (quatro) links WAN.	https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/477154/configuring-sd-wan-load-balancing https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/19246/sd-wan	- -	"In the example, the ISP connected to WAN1 is a 40Mb link, and the ISP connected to WAN2 is a 10Mb link, so we balance the weight 75% to 25% in favor of WAN1." "At least one interface must be configured for SD-WAN to function; up to 255 member interfaces can be configured"

4.2.7.6	Deve permitir a configuração da funcionalidade de balanceamento em qualquer interface WAN, seja ela MPLS, Internet, 4G/LTE etc.	https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/218559/configuring-the-sd-wan-interface https://docs.fortinet.com/document/fortigate/6.0.0/handbook/836394/setting-up-your-supported-lte-modem https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/125874/mpls-sip-and-backup-dia-cloud-apps	- - -	"First, SD-WAN must be enabled and member interfaces must be selected. The selected FortiGate interfaces can be of any type (physical, aggregate, VLAN, IPsec, and others)" "If you are using your LTE modem for a backup or redundant internet connection, you can add an SD-WAN interface that includes the FortiGate wired internet connecting interface and the wwan interface." "This topic covers a typical customer usage scenario where the customer's SD-WAN has two members: MPLS and DIA."
4.2.7.7	Deve possuir roteamento baseado em políticas e múltiplas saídas (e tipos de saídas) WANs.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/672387/using-bgp-tags-with-sd-wan-rules	-	"In this example, a customer has two ISP connections, wan1 and wan2. wan1 is used primarily for direct access to internet applications, and wan2 is used primarily for traffic to the customer's data center." "This example assumes that SD-WAN is enable on the FortiGate, wan1 and wan2 are added as SD-WAN members, and a policy and static route have been created."
4.2.7.8	Deve permitir a configuração de failover entre links principais e secundários, caso os links utilizados ultrapassem os limites previamente definidos de jitter, latência e perda de pacotes. Estes limites podem ser configurados para forçar o failover caso apenas um ou todos os limites sejam atingidos simultaneamente.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/382233/performance-sla-sla-targets	-	Seção "Performance SLA - SLA targets" Latency threshold: Latency for SLA to make decision, in milliseconds (0 - 10000000, default = 5). Jitter threshold: Jitter for SLA to make decision, in milliseconds (0 - 10000000, default = 5). Packet loss threshold: Packet loss for SLA to make decision, in percentage (0 - 100, default = 0).

4.2.7.9	Deve suportar a configuração de regras que permita o failback imediato.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/370572/configuring-link-health-monitoring	-	Restore link after Set the number of successful status checks before the FortiGate restores the interface to SD-WAN load balancing groups. The range is 1 to 10. The default is 5. This setting helps prevent flapping, where the system continuously transfers traffic back and forth between links.
4.2.7.10	Deve ser compatível com a solução de VPN, permitindo que suas características e análises sejam realizadas nas VPNs, assim como em links WAN.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD41297	-	Artigo "Technical Tip: Configure FortiGate SD-WAN with an IPSEC VPN"
4.2.7.11	Deve ser compatível com VPNs montadas em interfaces virtuais com roteamentodinâmico.	https://kb.fortinet.com/kb/documentLink.do?popup=true&externalID=FD41389&languageId=	-	Artigo "Technical Note: How to use BGP and SD-WAN for advertising routes and path selection in FortiGate"
4.2.7.12	Deve realizar o gerenciamento de tráfego por tipo de aplicação	https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/80739/dynamic-application-steering-with-lowest-cost-and-best-quality-strategies	-	"...Under Destination, set Application to your required applications. In this example: Microsoft.Office.365, Microsoft.Office.Online, Google.Docs, Dropbox, and SIP..."
4.2.7.13	Deve selecionar o melhor caminho baseado em tipo de tráfego e do host de origem	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	Multi-path intelligence using rules defined by: - Source address and/or user group - Destination address and/or a selection of over 3,000 applications - path selection using particular link quality criteria or SLAs defined
4.2.7.14	Deve suportar o monitoramento de link com ping e TCP-echo.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/370572/configuring-link-health-monitoring	-	Configure link health monitoring – CLI set protocol {ping | ping6 | tcp-echo | udp-echo | http | twamp}

4.2.7.15	Deve suportar o monitoramento de links VPN (interfaces virtuais).	https://kb.fortinet.com/kb/documentLink.do?externalID=FD41297 https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FMG-FAZ/1900_FortiView/0015_Summary_list.htm	-	Technical Tip: Configure FortiGate SD-WAN with an IPSEC VPN VPN - SSL & Dialup IPsec "Displays the users who are accessing the network by using the following types of security over a virtual private network (VPN) tunnel: secure socket layers (SSL) and Internet protocol security (IPsec)."
4.2.7.16	Deve permitir a exportação de informações via netflow.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD36460	-	Technical Tip: How to Configure Netflow on a FortiGate
4.3	**Recursos de Segurança**	-	-	-
4.3.1.	**Características Gerais**	-	-	-
4.3.1.1.	Deve possuir, no mínimo, funcionalidades Anti-Vírus, Anti-Bot, Anti-Malware, Anti-Spyware, Sistema de Prevenção de Intrusão (IPS), Filtro de Conteúdo Web e Controle de Aplicação.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGuard_Security_Services.pdf	2,3	"FortiGuard Advanced Malware Protection is a robust service providing core technologies needed for security protection for known threats and emerging threats. And includes: Antivirus, Botnet IP/Domain Service, Mobile Malware Security..." "FortiGuard Antivirus delivers automated updates that protect against the latest viruses, spyware..." "Intrusion Prevention (IPS)" "Web Filtering" "Application Control"
4.3.1.2.	Deve suportar o funcionamento nos modos sniffer (para inspeção de tráfego gerado por uma porta de rede espelhada), layer-2, layer-3.	https://kb.fortinet.com/kb/documentLink.do?externalID=11186 https://kb.fortinet.com/kb/documentLink.do?externalID=FD31207	- -	Sniff 3 packets of all traffic with verbose Level 4 on internal Interface # diag sniffer packet internal none 4 3 A sniffer trace will tell if OSPF HELLO packets are sent/received : FGT2# diagnose sniffer packet any "proto 89" 4 (stop sniffer with CTRL+C)

4.3.1.3.	Deve aplicar novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas.	https://docs.fortinet.com/document/fortigate/6.0.0/best-practices/502147/policy-configuration	-	Policy configuration changesOn a heavy-loaded system, plan configuration changes during low usage periods in order to minimize impact on CPU usage and established sessions. In this scenario, it is considered a best practice to de-accelerate the hardware-accelerated sessions.where you want the following to be true:check-all-CPU flushes all current sessions and re-evaluates them. This is the default option.check-new-CPU keeps existing sessions and applies policy changes to new sessions only. This reduces CPU load and the possibility of packet loss.check-policy-option- Use the option selected in the firewall-session-dirty field of the firewall policy (check-all or check-new, as above, but per policy).
4.3.1.4.	Deve suportar as atualizações automáticas da bases de assinaturas utilizadas na identificação de vírus, intrusões (IPS) e aplicações sem a necessidade de intervenção manual pelo administrador, sem perda das conexões ativas e sem reinicialização do equipamento.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/547335/automatic-updates	-	Automatic updates Push updates Push updates enable you to get immediate updates when new viruses or intrusions are discovered and new signatures are created. This ensures that the latest signature are sent to the FortiGate as soon as possible.

4.3.1.5.	Deve suportar as atualizações automáticas das listas de geolocalização e das listas e categorias de URLs sem a necessidade de intervenção manual pelo administrador, sem perda das conexões ativas e sem reinicialização do equipamento.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD40832 https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/790156/external-resources-for-web-filter	- -	"1) First check the geoip database current version: # diagnose autoupdate versions IP Geography DB" "External resources for web filter If the external resource is updated, FortiGate objects will update dynamically. External Resource are categorized into 4 types: URL list (Type=category) Domain Name List (Type=domain) IP Address list (Type=address) Malware hash list (Type=malware)"
4.3.1.6.	Deve possuir proteção contra ataques do tipo: IP Spoofing, Negação de Serviço (DoS e DDoS), SYN Flood Attack, ICMP Flood Attack e UDP Flood Attack, Buffer Overflow, Port Scanning, Man-id-the-Middle.	https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/117178/firewall-ipmacbinding-settinghttps://docs.fortinet.com/document/fortigate/6.0.0/handbook/626319/inside-fortios-denial-of-service-dos-protectionhttps://docs.fortinet.com/document/fortigate/6.0.0/handbook/372693/defending-against-dos-attackshttps://docs.fortinet.com/document/fortiweb/6.1.2/administration-guide/277489/http-https-protocol-constraintshttps://kb.fortinet.com/kb/documentLink.do?externalID=FD40206https://docs.fortinet.com/document/fortigate/6.0.0/handbook/745988/ssh-mitm-deep-inspection	-----	"Use this command to configure IP to MAC address binding settings. IP/MAC binding protects the FortiGate unit and/or the network from IP address spoofing attacks. IP spoofing attacks attempt to use the IP address of a trusted computer to connect to, or through, the FortiGate unit from a different computer...""FortiOS DoS and DDoS protection""Configuring the SYN threshold to prevent SYN floods""Use the udp_flood and icmp_flood thresholds to defend against these DoS attacks.""Use protocol constraints to prevent attacks such as buffer overflows.""Techncial Note: How to block NMAP Port Scanner""SSH MITM deep inspection"

4.3.1.7.	Deve identificar, decriptografar e analisar o tráfego SSL tanto em conexões de entrada (inbound) quanto de saída (outbound).	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/929997/ssl-inspection https://kb.fortinet.com/kb/documentLink.do?externalID=FD40937	- -	Deep inspection (also known as SSL/SSH inspection) is typically applied to outbound policies where destinations are unknown. Technical Note: Configuring Inbound SSL Deep Inspection
4.3.1.8.	Deve permitir a decriptografia da área útil do pacote de dados (payload) para fins de controle de acesso à Internet e proteção contra ameaças.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/122078/deep-inspection	-	When you use deep inspection, the FortiGate impersonates the recipient of the originating SSL session, then decrypts and inspects the content to find threats and block them. It then re-encrypts the content and sends it to the real recipient.
4.3.1.9.	Deve permitir a diferenciação de conexões pessoais (bancos, shopping etc) e conexões não pessoais por meio de classificação automática.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/122078/deep-inspection	-	Exempt web sites from deep inspection If you want to exempt all bank web sites, an easy way is to exempt the Finance and Banking category which includes all finance and bank web sites identified in FortiGuard.
4.3.1.10.	Deve possuir funcionalidade de backup/restore da configuração e das políticas de segurança.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/702257/configuration-backups	-	Backing up the configuration Restoring a configuration
4.3.1.11.	Deve armazenar os backups localmente, ou na solução de gerenciamento centralizado, e permitir que sejam transferidos para equipamentos externos por meio dos protocolos FTP ou SCP.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/702257/configuration-backups	-	You have the option to save the configuration file to various locations including the local PC, USB key, FTP, and TFTP server.
4.3.1.12.	Deve possuir a capacidade de identificar ataques de Advanced Persistent Threat (APT) e Zero-Day.	https://www.fortinet.com/br/resources/cyberglossary/advanced-persistent-threat https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ATP-Framework.pdf https://docs.fortinet.com/document/fortigate/6.0.0/handbook/817681/fortiguard	-	"...Fortinet integrates the intelligence of FortiGuard Labs into FortiGate next-generation firewalls..." As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGates. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats.

4.3.1.12.1.	Deve possuir a capacidade de emular um ambiente operacional isolado e seguro (Sandbox), na nuvem do fabricante, para execução e observação de código malicioso, sem a utilização de assinaturas, com base na atividade, como, por exemplo, operações de arquivo, alterações de registro e sistema etc.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/904357/using-fortisandbox-cloud-with-antivirus	-	FortiSandbox Cloud allows users to take advantage of FortiSandbox features without having to purchase, operate, and maintain a physical appliance. It works the same way as the physical FortiSandbox appliance.
4.3.1.12.2.	Deve suportar a análise no sistema operacional Windows.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf	4	▪ OS type supported: Windows 7, Windows 8.1, Windows 10, macOS, Linux, Android, and ICS systems
4.3.1.12.3.	Deve suportar a análise dos tipos de arquivos: documentos Microsoft Office, dll, exe, pdf, gzip, tar, zip.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf	4	✓ File type support: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .elf, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, .rl, .vbs,EBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
4.3.1.12.4.	Deve suportar a análise dos protocolos HTTP/HTTPS, FTP e SMTP.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	13	AV Inspected protocols and file types: - Support for HTTP, FTP, IMAP, POP3, SMTP, NNTP, MAPI, CIFS and SSH - Scan encrypted traffic with SSL inspection
4.3.2.	**Filtro de Pacotes**	-	-	-
4.3.2.1.	Não deve possuir restrições ao número de máquinas ou usuários protegidos.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf	12	*Não existe restrições para quantidade de máquinas e usuários protegidos.*
4.3.2.2.	Deve informar o número de sessões simultâneas.	https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/476970	-	Generate network traffic through the FortiGate, then go to FortiView > All Sessions and select the now view. A real time display of active sessions is shown.
4.3.2.3.	Deve suportar a implementação tanto em modo transparente (layer-2) quanto em modo gateway (layer-3).	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	FIREWALL Operating modes: NAT/route and transparent (bridge)

4.3.2.4.	Deve suportar Statefull Packet Inspection de tráfego IPv4 e IPv6.	http://docs.fortinet.com/document/fortigate/6.2.0/parallel-path-processing-life-of-a-packet/86811/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading https://kb.fortinet.com/kb/documentLink.do?externalID=FD30063	- -	Stateful inspection makes the decision to drop or allow a session and apply security features to it based on what is found in the first packet of the session. Then all subsequent packets in the same session are processed in the same way. FortiGate units are dual IP layer IPv6/IPv4 nodes. They support IPv6 over IPv4 tunneling, routing, firewall policies and IPSec VPN. You can assign both an IPv4 and an IPv6 address to any interface on a FortiGate unit - the interface functions as two interfaces, one for IPv4 addressed packets and another for IPv6 addressed packets.
4.3.2.5.	Deve suportar controle de acesso para pelo menos 80 serviços e protocolos pré-definidos.	4.3.2.5._87_Services.png	-	*91 Serviços protocolos pré-definidos*
4.3.2.6.	Deve suportar os protocolos H.323, SIP.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	Session helpers and ALGs: DCE/RPC, DNS-TCP, DNS-UDP, FTP, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)
4.3.2.7.	Deve implementar mecanismo de proteção contra ataques de falsificação de endereços IP (anti-spoofing).	https://docs.fortinet.com/document/fortigate/6.2.0/hardening-your-fortigate/995103/building-security-into-fortios	-	"FortiOS implements a mechanism called Reverse Path Forwarding (RPF), or Anti Spoofing..."
4.3.2.8.	Deve implementar mecanismo de captura de pacotes.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD45907	-	This article describes how to use the build in packet capture feature in FortiOS from the GUI interface.
4.3.2.9.	Deve identificar os usuários para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP.	https://docs.fortinet.com/document/ipsengine/3.6.0/custom-ips-and-application-control-signature-syntax-guide/677384/protocol-options	-	Protocol optionsUse these options to detect IP/ICMP/UDP/TCP protocol headers. The keyword protocol is highly recommended for all custom signatures.
4.3.2.10.	Deve suportar a utilização simultânea de políticas de segurança em IPv4 e IPv6.	https://docs.fortinet.com/document/fortigate/6.2.0/new-features/516182/combined-ipv4-and-ipv6-policy	-	In consolidated policy mode, there is a single policy table for the GUI. The same source interface, destination interface, service, user, and schedule are shared for both IPv4 and IPv6, while

				there are different IP addresses and IP pool settings.
4.3.2.11.	Deve suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período de tempo, e suas combinações.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies https://docs.fortinet.com/document/fortigate/6.0.0/handbook/736325/ip-netmask-addresses	- -	Firewall policy parameters - - When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number). It also registers the incoming interface, the outgoing interface it will need to use and the time of day. - Service The service or service chosen here represent the TCP/IP suite port numbers that will most commonly be used to transport the named protocols or group of protocols. - Source User(s) This parameter is based on a user identity that can be from a number of authentication authorities. It will be an account or group - Using this information the FortiGate firewall attempts to locate a security policy that matches the packet. If it finds a policy that matches the parameters it then looks at the action for that policy. If it is ACCEPT the traffic is allowed to proceed to the next step. If the Action is DENY or a match cannot be found the traffic is not allowed to proceed. - The FortiGate unit automatically converts CIDR formatted netmasks to dotted decimal format.
4.3.3.	**Filtro de Conteúdo**	-	-	-

4.3.3.1.	Deve prover o controle e proteção de acesso à Internet por meio do reconhecimento de aplicações, independente de porta e protocolo, e da classificação de URLs.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/756500/web-filtering https://docs.fortinet.com/document/fortigate/6.0.0/handbook/72943/application-control https://docs.fortinet.com/document/fortigate/6.0.0/handbook/849310/concepts	- -	NGFW mode simplifies applying application control and web filtering to traffic by allowing you to add applications and web filtering profiles directly to policies. This is used in conjunction with flow-based inspection. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols. Application control does not require knowledge of any server addresses or ports.
4.3.3.2.	Deve ser capaz de identificar aplicações, independentemente das portas e protocolos, bem como das técnicas de evasão utilizadas.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/72943/application-control https://docs.fortinet.com/document/fortigate/6.0.0/handbook/849310/concepts	- -	Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols. Application control does not require knowledge of any server addresses or ports.
4.3.3.3.	Deve ser capaz de identificar se as aplicações estão utilizando sua porta padrão.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	Port enforcement check: block applications detected on non-default ports
4.3.3.4.	Deve ser capaz de identificar aplicações encapsuladas dentro de protocolos, como HTTP e HTTPS.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control	-	Application control technologies detect and take action against network traffic based on the application that generated the traffic. Application control uses protocol decoders with signatures that analyze network traffic to detect application traffic, even if the traffic uses nonstandard ports or protocols.
4.3.3.5.	Deve ser capaz de identificar aplicações criptografadas usando SSL.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	6	Effectively examine SSL-encrypted traffic with various security controls, such as AV and content filtering

4.3.3.6.	Deve ser capaz de identificar um mínimo de 1.400 (mil e quatrocentas) aplicações, incluindo, mas não se limitando a: peer-to-peer, streaming e download de aúdio, streaming e download de vídeo, update de software, instant messaging, redes sociais, proxies, anonymizers, acesso e controle remoto, VOIP e email.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/849310/concepts https://docs.fortinet.com/document/fortigate/6.0.0/handbook/721617/configuring-profiles	- -	The FortiGate unit includes signatures for over 2,000 applications, services, and protocols. Under Categories, you may select from the following: Collaboration, Email, P2P, Proxy, Remote.Access, Social.Media, Update, Video/Audio, VoIP, Unknown Applications
4.3.3.7.	Deve ser capaz de identificar, no mínimo, as seguintes aplicações: Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Instagram, Twitter, Linkedin, Dropbox, Google Drive, One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR, Webex.	https://www.fortiguard.com/appcontrol	-	Pesquisar: "Bittorrent" "Youtube" "Livestream" "Skype" "Viber" "WhatsApp" "Snapchat" "Facebook" "Facebook Messenger" "Instagram" "Twitter" "Linkedin" "Dropbox" "Google Drive", One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR, Webex.
4.3.3.8.	Deve armazenar a base de assinaturas no próprio equipamento.	https://docs.fortinet.com/document/fortigate/6.0.0/fortinet-communication-ports-and-protocols/649403/fortiguard	-	The FortiGuard subscription update services include: AntiVirus (AV) Intrusion Protection Service (IPS) Application Control Anti-Spam Web Filtering
4.3.3.9.	Deve classificar as aplicações em categorias.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	APPLICATION CONTROL Detects thousands of applications in 18 categories
4.3.3.10.	Deve permitir o agrupamento de aplicações em grupos personalizados.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control	-	The application database is classified into 20 intuitive categories for ease of use. Administrators may also create specific application overrides that differ from the category settings.
4.3.3.11.	Deve identificar os usuários que estão utilizando as aplicações.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control	-	The FortiGate is able to operate in inline route and transparent mode. It can also operate in offline sniffer mode for passive monitoring of user activitie
4.3.3.12.	Deve permitir o bloqueio de aplicações que não estejam utilizando suas portas padrão.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	Port enforcement check: block applications detected on non-default ports

4.3.3.13.	Deve suportar a implementação de políticas de segurança baseadas em: aplicações,categorias de aplicações,endereço IP de origem ou destino,rede CIDR/VLSM de origem ou destino,usuário ou grupo de usuários,horário ou período de tempo,e suas combinações.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policieshttps://docs.fortinet.com/document/fortigate/6.0.0/handbook/736325/ip-netmask-addresses	-	- In addition to parameters like schedule and service, NGFW policies can filter by application or application category.- Source address(es) / Destination address(es)- "Schedule - The time frame that is applied to the policy..."- Source User(s) - This parameter is based on a user identity that can be from a number of authentication authorities. It will be an account or group- Using this information the FortiGate firewall attempts to locate a security policy that matches the packet. If it finds a policy that matches the parameters it then looks at the action for that policy. If it is ACCEPT the traffic is allowed to proceed to the next step. If the Action is DENY or a match cannot be found the traffic is not allowed to proceed.- The FortiGate unit automatically converts CIDR formatted netmasks to dotted decimal format.
4.3.3.14.	Deve permitir a utilização ou bloqueio individualizado das aplicações, como BitTorrent e Skype, para determinados usuários ou grupos de usuários.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies https://www.fortiguard.com/appcontrol	-	From the editing page for the New Application Group, choose a group type of Application and select individual applications for membership in the group. "...you can apply it to a policy in the Application field, by clicking on the + in the field... Pesquisar: "Bittorrent" " "Skype"
4.3.3.15.	Deve permitir registrar todos os fluxos autorizados/bloqueados das aplicações, incluindo o usuário identificado.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies	-	"There can also be a number of instructions associated with a FortiGate firewall in addition to the ACCEPT or DENY actions, some of which are optional. Instructions on how to process the traffic can also include such things as: - Logging Traffic..."

4.3.3.16.	Deve permitir o controle de uso de banda de download ou upload utilizada pelas aplicações (traffic shaping) baseado em: endereço IP ou rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/204835/configuring-application-control-traffic-shaping	-	Configuring application control traffic shaping Enable application control in a security policy – GUI Set the Incoming Interface Set the Outgoing Interface Set the Source Set the Schedule Creating a traffic shaping policy
4.3.3.17.	Deve ser capaz de efetuar a classificação de conteúdo de páginas web em HTTP e HTTPS, baseado em listas de categoria.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD31710 https://docs.fortinet.com/document/fortigate/6.4.1/administration-guide/833698/web-filter	- -	The FortiGate can perform both HTTP and HTTPS Web URL filtering, as well as HTTPS Fortiguard Web Filtering - FortiGuard Web Filtering service: provides many additional categories you can use to filter web traffic.
4.3.3.18.	Deve possuir funcionalidades de tratamento de conteúdo web, devendo sua base de dados conter, no mínimo, 10 (dez) milhões de sites internet web já registrados e classificados, distribuídos em, no mínimo, 60 (sessenta) categorias ou subcategorias pré-definidas ou suas semelhantes: conteúdo adulto, chat, drogas ilegais, jogos de azar, jogos, pirataria, proxy remoto, redes sociais, streaming media, violência, pornografia, racismo, malware.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf https://docs.fortinet.com/document/fortigate/6.0.0/handbook/120269/fortiguard-web-filtering	11	- Over 250 million URLs rated into 78 categories, in 70 languages Other Adult Materials; Web Chat; Drug Abuse; Games; Sports Hunting and War Games; Plagiarism; Proxy Avoidance; Streaming Media and Download; Explicit Violence; Discrimination; Malicious Websites;
4.3.3.19.	Deve permitir a inclusão de URLs customizadas por política (whitelist).	https://docs.fortinet.com/document/fortigate/6.4.1/administration-guide/615462/url-filter	-	ExemptThe traffic is allowed to bypass the remaining FortiGuard web filters, web content filters, web script filters, antivirus scanning, and DLP proxy operations

4.3.3.20.	Deve armazenar as listas de categoria no próprio equipamento.	https://docs.fortinet.com/document/fortigate/6.0.0/fortinet-communication-ports-and-protocols/649403/fortiguard	-	The FortiGuard subscription update services include: AntiVirus (AV) Intrusion Protection Service (IPS) Application Control Anti-Spam Web Filtering
4.3.3.21.	Deve identificar os usuários que estão acessando as páginas web.	https://docs.fortinet.com/document/fortigate/6.4.1/administration-guide/675558/fortiguard-filter	-	To view the log of a blocked website in the GUI: Go to Log & Report > Web Filter.
4.3.3.22.	Deve suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies https://docs.fortinet.com/document/fortigate/6.0.0/handbook/736325/ip-netmask-addresses https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/701862/blocking-facebook-with-web-filtering https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/546110/blocking-social-media-websites-using-fortiguard-categories#Blocking_social_media_websites_using_FortiGuard_categories	- - - -	- Source address(es) / Destination address(es) - "Schedule - The time frame that is applied to the policy..." - Source User(s) - This parameter is based on a user identity that can be from a number of authentication authorities. It will be an account or group - Using this information the FortiGate firewall attempts to locate a security policy that matches the packet. If it finds a policy that matches the parameters it then looks at the action for that policy. If it is ACCEPT the traffic is allowed to proceed to the next step. If the Action is DENY or a match cannot be found the traffic is not allowed to proceed. - The FortiGate unit automatically converts CIDR formatted netmasks to dotted decimal format. - 3. Creating the Web filtering security policy - Blocking social media websites using FortiGuard categories
4.3.3.23.	Deve alertar o usuário quando uma URL for bloqueada, por meio de página de bloqueio que possa ser customizada, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control	-	User education is central to an effective security implementation. In response to this, FortiOS lets you provide user notification when blocking an unauthorized application. The notification appears as an HTML block page for web-based applications.

4.3.3.24.	Deve permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado, informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para possibilitar o usuário continuar acessando o site).	https://docs.fortinet.com/document/fortigate/6.4.1/administration-guide/675558/fortiguard-filter	-	Sample configuration of issuing a warning This example shows issuing a warning when a user visits a website based on its category (rating), for example, information technology.
4.3.3.25.	Deve permitir registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado.	https://docs.fortinet.com/document/fortigate/6.4.1/administration-guide/615462/url-filter		To check web filter logs in the GUI: Go to Log & Report > Web Filter.
4.3.4.	**Prevenção de Intrusão (IPS)**	-	-	-
4.3.4.1.	Deve possuir tecnologia de detecção e prevenção de ataques e intrusões baseada em assinatura.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	IPS engine: 11,000+ up-to-date signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic pull or push signature update, threat encyclopedia integration
4.3.4.2.	Possuir, no mínimo, um conjunto de 2.000 (duas mil) assinaturas de detecção e prevenção de ataques.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	IPS engine: 11,000+ up-to-date signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic pull or push signature update, threat encyclopedia integration
4.3.4.3.	Detectar protocolos independentemente da porta utilizada, identificando aplicações conhecidas em portas não-padrão.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	944	The FortiGate Intrusion Prevention system uses protocol decoders to identify the abnormal traffic patterns that do notmeet the protocol requirements and standards. For example, the HTTP decoder monitors traffic to identify any HTTPpackets that do not meet the HTTP protocol standards. These decoders can detect their traffic on any port.

4.3.4.4.	Deve possuir, no mínimo, os seguintes mecanismos de detecção e prevenção: assinaturas de vulnerabilidades e exploits, assinaturas de ataques, validação de protocolos, detecção de anomalias, IP defragmentation, remontagem de pacotes TCP, nível de severidade do ataque.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	590, 934, 935, 938	Assinaturas de vulnerabilidades e exploits - Página 935 Signature-based defense is used against known attacks or vulnerability exploits. Assinaturas de ataques - Página 935 To view the complete list of signatures, go to Security Profiles > Intrusion Prevention, and select View IPS Signatures. This will include the predefined signatures and any custom signatures that you may have created. Validação de protocolos - Página 935 Before examining network traffic for attacks, the IPS engine uses protocol decoders to identify each protocol appearing in the traffic. Detecção de anomalias - Página 934 Anomaly-based defense is used when network traffic itself is used as a weapon. A host can be flooded with far more traffic than it can handle, making the host accessible. The most common example is the denial of service (DoS) attack, in

				which an attacker directs a large number of computers to attempt normal access of the target system. IP defragmentation e remontagem de pacotes TCP - Página 590 The FortiGate unit automatically reassembles fragmented packets before processing them because fragmented packets can evade security measures. This reassembly of packets affects TCP, UDP and IP packets. There can be some variation though in what process does the reassembling. The IPS engine, nTurbo and the kernel all can do defragmentation. Nível de Severidade - Página 938 Severity refers to the level of threat posed by the attack. The options include Critical, High, Medium, Low, and Info.
4.3.4.5.	Deve ser capaz de inspecionar tráfego criptografado usando SSL.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	Inspect SSL encrypted traffic option for IPS, application control, antivirus, web filtering, and DLP
4.3.4.6.	Deve ser capaz de inspecionar integralmente todos os pacotes de dados, independentemente de seus tamanhos.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	943	Starting with FortiOS 5.2, intelligent-mode is a new adaptive detection method. This command is enabled thedefault and it means that the IPS engine will perform adaptive scanning so that, for some traffic, the FortiGate canquickly finish scanning and offload the traffic to NPU or kernel. It is a balanced method which could cover all knownexploits. When disabled, the IPS engine scans every single byte

4.3.4.7.	Deve identificar os usuários relacionados aos eventos de intrusão.	https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/FortiGate_6_0/FortiOS%206.0.4%20Log%20Reference.pdf	907	16384 - LOGID_ATTCK_SIGNATURE_TCP_UDP. Ver tabela de logs
4.3.4.8.	Deve identificar os usuários relacionados aos eventos de bloqueio.	https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/FortiGate_6_0/FortiOS%206.0.4%20Log%20Reference.pdf	907	16384 - LOGID_ATTCK_SIGNATURE_TCP_UDP. Ver tabela de logs
4.3.4.9.	Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de um determinado ataque ou ameaça.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	939	Select Monitor to allow traffic to continue to its destination and log the activity. The log will appear under Log & Report but will only be visible in the GUI in the event of an intrusion.
4.3.4.10.	Deve permitir a criação de políticas de segurança que bloqueiem uma determinada ameaça.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	939	Select Block to drop traffic matching any the signatures included in the filter.
4.3.4.11.	Deve permitir a criação de políticas de segurança que bloqueiem um determinado ataque por meio de uma ação de DROP/RESET.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook		Select Reset to reset the session whenever the signature is triggered. In the CLI this action is referred to as Reject.
4.3.4.12.	Deve permitir registrar todos os eventos de IPS, incluindo o usuário identificado.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	945	Packet logging saves the network packets containing the traffic matching an IPS signature to the attack log. The FortiGate unit will save the logged packets to wherever the logs are configured to be stored, whether memory, internal hard drive, a FortiAnalyzer unit, or the FortiGuard Analysis and Management Service
4.3.4.13.	Deve identificar e bloquear a comunicação com botnets.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	939	You can set Botnet C&C protection to Block outgoing connections to Botnet sites or just record log messages (Monitor) when an outgoing Botnet connection attempt is detected.

4.3.4.14.	Deve bloquear malwares e spywares.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	854	Antivirus scanning examines files for viruses, worms, trojans, and other malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action. "Antivirus scanning examines files for viruses, worms, trojans, and other malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action"
4.3.4.15.	Deve inspecionar e bloquear vírus nos seguintes tipos de tráfego, no mínimo: HTTP, HTTPS e SMTP.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	854	This section describes how to configure the antivirus options. From an antivirus profile you can configure the FortiGateunit to apply antivirus protection to HTTP, FTP, IMAP, POP3, SMTP, and NNTP sessions. If your FortiGate unitsupports SSL/SSH content scanning and inspection, you can also configure antivirus protection for HTTPS, IMAPS,POP3S, SMTPS, and FTPS sessions.

4.3.4.16.	Deve inspecionar e bloquear vírus nos seguintes tipos de tráfego, no mínimo: HTTP, HTTPS e SMTP.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/842733/malware https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/788313/content-disarm-and-reconstruction-for-antivirus https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR1/fortigate-utm-40-mr1.pdf	- - 25	Worms, Spyware "Content Disarm and Reconstruction (CDR) allows the FortiGate to sanitize Microsoft documents and PDF (disarm) by removing active content such as hyperlinks, embedded media, javascript..." "Attackers encode HTML links using various formats to evade detection and bypass security measures. For example, the URL www.example.com/cgi.bin could be encoded in a number of ways to avoid detection but still work properly, and be interpreted the same, in a web browser. The FortiGate prevents the obfuscation by converting the URL to ASCII before inspection."
4.3.4.17.	Deve suportar a inspeção de vírus em arquivos comprimidos utilizando o algoritmo deflate (zip, gzip etc).	https://kb.fortinet.com/kb/documentLink.do?externalID=10187	-	FortiGate units support the following compression formats for antivirus checking: tar, gzip, rar, lzh, cab, arj, zip, bzip, bzip2, msc
4.3.4.18.	Deve suportar bloqueio de download de pelo menos 45 tipos de arquivos.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/610893/file-filter	-	File Filter allows the Web Filter profile to block files passing through a FortiGate based on file type.
4.3.4.19.	Deve armazenar as bases de assinaturas no próprio equipamento.	https://docs.fortinet.com/document/fortigate/6.0.0/fortinet-communication-ports-and-protocols/649403/fortiguard	-	The FortiGuard subscription update services include: AntiVirus (AV) Intrusion Protection Service (IPS) Application Control Anti-Spam Web Filtering
4.4.	**Firewall Tipo 1**	-	-	-
4.4.1.	Deve possuir o throughput mínimo de 6 Gbps com as funcionalidades de Filtro de Pacotes, IPS, Filtro de Conteúdo e Proteção contra Malwares habilitadas simultaneamente.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	Threat Protection Throughput 7 Gbps *Threat Protection performance is measured with Firewall, IPS, Application Control, and Malware Protection enabled.*

4.4.2.	Em relação ao filtro de pacotes, deve possuir o throughput mínimo de 13 Gbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) 36 / 36 / 27 Gbps
4.4.3.	Em relação ao túnel IPSec VPN, deve possuir o throughput mínimo de 10 Gbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	IPsec VPN Throughput (512 byte) 20 Gbps
4.4.4.	Em relação à inspeção SSL/TLS, deve possuir o throughput mínimo de 2 Gbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	SSL Inspection Throughput (IPS, avg. HTTPS) 8 Gbps
4.4.5.	Deve permitir, no mínimo, 7.500.000 de conexões simultâneas.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	Concurrent Sessions (TCP) 8 Million
4.4.6.	Deve permitir, no mínimo, 130.000 novas conexões por segundo.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	New Sessions/Second (TCP) 450,000
4.4.7.	Deve permitir, no mínimo, 512 VLANs.	https://docs.fortinet.com/max-value-table	-	system interface 8192
4.4.8.	Deve permitir, no mínimo, 80.000 usuários autenticados	Carta do Fabricante	-	*O FortiGate 600E permite 80.000 usuários autenticados*
4.4.9.	Deve permitir, no mínimo, 2.000 túneis VPN site-to-site simultâneos.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	Gateway-to-Gateway IPsec VPN Tunnels 2,000
4.4.10.	Deve permitir, no mínimo, 9.000 túneis VPN client-to-site simultâneos.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	Client-to-Gateway IPsec VPN Tunnels 50,000
4.4.11.	Deve suportar afixação em bastidor (rack) padrão EIA-310 com largura de 19’ (dezenove polegadas) e altura de até duas unidades de rack (2U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/186de9b7-1a21-11e9-9685-f8bc1258b856/FortiGate-600E-601E-Supplement.pdf	5 4	Form Factor (supports EIA / non-EIA standards) Rack Mount, 1 RU This device mounts in a standard 19 inch rack. (O FortiGate 600E está acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc))
4.4.12.	Deve possuir 2 (duas) fontes de alimentação independentes, redundantes e hot-swappable.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	Redundant Power Supplies (Hot Swappable) optional (Fonte Redundante Configurada)
4.4.13.	Deve possuir, no mínimo, 8 (oito) interfaces 1 (um) Gigabit-Ethernet padrão 1000Base-T, para conexão ao meio via cabo par trançado.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	GE RJ45 Interfaces: 8

4.4.14.	Deve possuir, no mínimo, 2 (duas) interfaces 10 (dez) Gigabit-Ethernet padrão SFP+, com transceivers SFP+ 10GB-SR, para conexão ao meio via cabo de fibra ótica.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	10 GE SFP+ Slots: 2 *O FortiGate 600E está configurado com 2 Transceivers 10GbE SFP+ SR*
4.4.15.	**Alta Disponibilidade**	-	-	-
4.4.15.1.	Deve operar em alta disponibilidade (HA) nativamente no equipamento, permitindo uma arquitetura ativo/ativo e ativo/passivo com no mínimo 2 (dois) membros, com sincronismo de estados integrado.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	High Availability Configurations Active-Active, Active-Passive, Clustering
4.4.15.2.	Deve suportar o balanceamento de carga interno na arquitetura ativo/ativo.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	High Availability Configurations Active-Active, Active-Passive, Clustering
4.4.15.3.	Deve sincronizar sessões TCP/IP, tabelas NAT, tabelas FIB, associações de segurança das VPNs e todas as configurações necessárias para a manutenção da continuidade dos serviços.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/347538/fortigate-cluster-protocol-fgcp https://docs.fortinet.com/document/fortigate/6.0.0/handbook/20224/synchronizing-kernel-routing-tables https://docs.fortinet.com/document/fortigate/6.0.0/handbook/738546/device-failover	- - -	Also contributing to enhanced reliability is session failover protection for most IPv4 and IPv6 sessions including TCP, UDP, ICMP, IPsec VPN, and NAT sessions In a functioning cluster, the primary unit keeps all subordinate unit kernel routing tables (also called the forwarding information base FIB) up to date and synchronized with the primary unit. IPsec VPN SA synchronization synchronizes IPsec VPN security associations (SAs)
4.4.15.4.	Deve monitorar a falha dos links de comunicação.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	366	Link failover means that if a monitored interface fails, the cluster reorganizes to reestablish a link to the network that the monitored interface was connected to and to continue operating with minimal or no disruption of network traffic. You configure monitored interfaces (also called interface monitoring or port monitoring) by selecting the interfaces to monitor as part of the

				cluster HA configuration. You can monitor up to 64 interfaces.
4.4.15.5.	Deve ser capaz de identificar e iniciar automaticamente um procedimento de failover sempre que ocorrer: a falha de um dos membros do cluster,a falha de qualquer componente ou processo crítico de um dos membros do cluster,a falha de um dos links de comunicação monitorados.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/223313/failover-protectionhttps://docs.fortinet.com/document/fortigate/6.0.0/handbook/320113/device-link-and-session-failover	--	The FGCP supports three kinds of failover protection. Device failover automatically replaces a failed device and restarts traffic flow with minimal impact on the network. Link failover maintains traffic flow if a link fails. Session failover resumes communication sessions with minimal loss of data if a device or link failover occurs.The FGCP provides transparent device and link failover. You can also enable session pickup to provide session failover. A failover can be caused by a hardware failure, a software failure, or something as simple as a network cable being disconnected causing a link failover.
4.4.15.6.	Deve ser capaz de realizar os procedimentos de failover sem perda das conexões ativas e sessões estabelecidas de forma transparente para o usuário.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/284323/fortigate-session-life-support-protocol-fgsp	-	If one of the FortiGates fails, session failover occurs and active sessions fail over to the unit that is still operating. This failover occurs without any loss of data.
4.5.	**Firewall Tipo 2**	-	-	-
4.5.1.	Deve possuir o throughput mínimo de 700 Mbps com as funcionalidades de Filtro de Pacotes, IPS, Filtro de Conteúdo e Proteção contra Malwares habilitadas simultaneamente.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	Threat Protection Throughput 1 Gbps *Threat Protection performance is measured with Firewall, IPS, Application Control, and Malware Protection enabled.*
4.5.2.	Em relação ao filtro de pacotes, deve possuir o throughput mínimo de 5 Gbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	Firewall Throughput (1518 / 512 / 64 byte UDP packets) 20 / 18 / 10 Gbps

4.5.3.	Em relação ao túnel IPSec VPN, deve possuir o throughput mínimo de 1,5 Gbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	IPsec VPN Throughput (512 byte) 11.5 Gbps
4.5.4.	Em relação à inspeção SSL/TLS, deve possuir o throughput mínimo de 500 Mbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	SSL Inspection Throughput (IPS, avg. HTTPS) 1 Gbps
4.5.5.	Deve permitir, no mínimo, 1.500.000 de conexões simultâneas.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	Concurrent Sessions (TCP) 1.5 Million
4.5.6.	Deve permitir, no mínimo, 25.000 novas conexões por segundo.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	New Sessions/Second (TCP) 56,000
4.5.7.	Deve permitir, no mínimo, 200 VLANs.	https://docs.fortinet.com/max-value-table	-	system interface 4096
4.5.8.	Deve permitir, no mínimo, 100 túneis VPN site-to-site simultâneos.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	Gateway-to-Gateway IPsec VPN Tunnels 2,500
4.5.9.	Deve permitir, no mínimo, 100 túneis VPN client-to-site simultâneos.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	Client-to-Gateway IPsec VPN Tunnels 16,000
4.5.10.	Deve suportar a fixação em bastidor (rack) padrão EIA-310 com largura de 19’ (dezenove polegadas) e altura de uma unidade de rack (1U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/42d64717-83f1-11e9-81a4-00505692583a/FortiGate-100F-Series-QSG.pdf	5 10	Form Factor (supports EIA / non-EIA standards) Rack Mount, 1 RU Your FortiGate includes rack mount brackets and screws to mount in any 19 inch rack. (O FortiGate 100F está acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc))
4.5.11.	Deve possuir, no mínimo, 8 (oito) interfaces 1 (um) Gigabit-Ethernet padrão 1000Base-T, para conexão ao meio via cabo par trançado.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	GE RJ45 Ports: 12
4.6.	**Firewall Tipo 3**	-	-	-
4.6.1.	Deve possuir o throughput mínimo de 300 Mbps com as funcionalidades de Filtro de Pacotes, IPS, Filtro de Conteúdo e Proteção contra Malwares habilitadas simultaneamente.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	5	Threat Protection Throughput 700 Mbps *Threat Protection performance is measured with Firewall, IPS, Application Control, and Malware Protection enabled.*

4.6.2.	Em relação ao filtro de pacotes, deve possuir o throughput mínimo de 1,5 Gbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	5	Firewall Throughput (1518 / 512 / 64 byte UDP packets) 10/10/6 Gbps
4.6.3.	Em relação ao túnel IPSec VPN, deve possuir o throughput mínimo de 700 Mbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	5	IPsec VPN Throughput (512 byte) 6.5 Gbps
4.6.4.	Em relação à inspeção SSL/TLS, deve possuir o throughput mínimo de 250 Mbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	5	SSL Inspection Throughput (IPS, avg. HTTPS) 630 Mbps
4.6.5.	Deve permitir, no mínimo, 150.000 de conexões simultâneas.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	5	Concurrent Sessions (TCP) 700,000
4.6.6.	Deve permitir, no mínimo, 12.000 novas conexões por segundo.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	5	New Sessions/Second (TCP) 35,000
4.6.7.	Deve permitir, no mínimo, 50 VLANs.	https://docs.fortinet.com/max-value-table	-	system interface 256
4.6.8.	Deve permitir, no mínimo, 50 túneis VPN site-to-site simultâneos.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	5	Gateway-to-Gateway IPsec VPN Tunnels 200
4.6.9.	Deve permitir, no mínimo, 60 túneis VPN client-to-site simultâneos.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	5	Client-to-Gateway IPsec VPN Tunnels 500
4.6.10.	Deve possuir, no mínimo, 8 (oito) interfaces 1 (um) Gigabit-Ethernet padrão 1000Base-T, para conexão ao meio via cabo par trançado.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf	5	Interfaces: 10x GE RJ45
5	**Solução de Gerenciamento Centralizado (SGC)**	-	-	-
5.1.	Deve ser fornecida em appliance virtual, compatível VMware vSphere ESXi 6.0 ou superior, ou baseado em software, compatível com Windows Server 2012 R2 ou superior.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	4	FORTIMANAGER VIRTUAL APPLIANCES Hypervisor Support VMware ESX/ESXi 5.5/6.0/6.5/6.7/7.0
5.2.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows 7 ou superior ou no Linux.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	15	Connecting to the GUI The FortiManager unit can be configured and managed using the GUI or the CLI. This section will step you through connecting to the unit via the GUI. 3. On the management computer, start a supported web browse and browse to https://192.168.1.99.

5.3.	Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	4	*O FortiManager esta licenciado em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas (110 Equipamentos do tipo Firewall).*
5.4.	Deve estar licenciada e permitir a gerência centralizada de, no mínimo, 100 equipamentos que compõem a solução.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	4	FMG-VM-BASE Devices/VDOMs (Maximum): 10 + FMG-VM-100-UG Devices/VDOMs (Maximum): 100 +
5.5.	Deve estar licenciada para o limite máximo de usuários, objetos, regras de segurança, NAT e endereços IP suportados pela solução.	https://docs.fortinet.com/document/fortimanager/6.2.2/administration-guide/435148/license	-	License count rules for FortiManager VM, Cloud (Fortinet, Azure, or AWS), and Hardware: VDOM disabled: 1 FortiGate = 1 license. VDOM enabled: 1 VDOM = 1 license. VDOM enabled but no VDOMs: root = 1 license. FortiGate in HA mode: No license count for secondary FortiGate. *A Solução de Gerenciamento Centralizado (SGC) ofertada, FortiManager, está licenciada para todos os Firewalls (FortiGates) ofertados neste edital. Não existe licenciamento com limites para máximo de usuários, objetos, regras de segurança, NAT e endereços IP suportados pela solução.*
5.6.	As comunicações entre a SGC e os firewalls e entre a SGC e as estações dos administradores do sistema devem ser criptografadas e autenticadas.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD40494https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	N/A 461516	set fgfm-ssl-protocol {sslv3 | tlsv1.0 | tlsv1.1 | tlsv1.2} #<-- for use with FGFM tunnel with FortiGateExample of adding a model device by pre-shared key3. On the management computer, start a supported web browser and browse to https://192.168.1.99.Configure administrator accounts using RADIUS, LDAP, TACACS+, or PKI

5.7.	Deve ser capaz de realizar todas as configurações nos firewalls descritas neste Termo de Referência.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	2	Central Management of Network Infrastructure Centrally manage FortiGate, FortiSwitch, FortiExtender & FortiAP.
5.8.	Deve possibilitar a aplicação de configurações em todos os firewalls, simultaneamente.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	2	Collectively configure the device settings - using the provisioning templates and advance CLI templates improves management of a large number of devices.
5.9.	Deve permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	27 2	FortiManager provides centralized policy-based provisioning and configuration management for FortiGate, FortiWiFi, FortiAP, and other devices FortiManager equips admins with granular device and role based administration for deploying zero-trust, multi-tenancy architecture to large enterprises, with a hierarchical objects database to facilitate re-use of common configurations and serve multiple customers.

5.10.	Deve suportar, por meio da interface gráfica de gerenciamento, a criação e administração de políticas de filtro de pacotes, prevenção de intrusão, controle de aplicação, filtragem de URLs, monitoração de logs, debugging, troubleshooting e captura de pacotes.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	2 628 674 138 222	**políticas de filtro de pacotes** Define global objects such as Firewall Objects, Policies and Security Profiles to share across multiple ADOMs FortiManager's new IPS admin is a restricted user role for performing only IPS related object configuration and install. **monitoração de logs,** FortiManager, coupled with the FortiAnalyzer family of centralized logging **controle de aplicação, filtragem de URLs e prevenção de intrusão** Restricted administrator accounts are used to delegate management of Web Filter, IPS, and Application Control profiles, **debugging,** CLI for management extensions You can use the CLI console to enable, disable, update, debug, and check the management extension. **troubleshooting** Troubleshooting Tips **e captura de pacotes.** Capture Packets Select to capture packets.
5.11.	Deve ser capaz de gerenciar os firewalls em unidades remotas, fora da rede local.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	1	*Ver Figura Página 1*
5.12.	Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou Active Directory.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	627	The FortiManager system supports authentication of administrators locally, remotely with RADIUS, LDAP, or TACACS+ servers, and using PKI.

5.13.	Será permitido que a solução de gerenciamento centralizado possua um “appliance virtual” específico para atendimento às necessidades de identificação e autenticação de usuários.	N/A	N/A	N/A
5.14.	Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	16	Configure the administrator profile to only allow read/write permission as required and restrict access using read only or no permission to settings which are not applicable to that administrator
5.15.	Deve permitir a criação de perfis customizados.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	625-626	To create a custom administrator profile:
5.16.	Deve permitir, de forma granular, assinalar permissões para os administradores criarem outros usuários, alterarem e ler configurações etc.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	625-626	To create a custom administrator profile:
5.17.	Deve permitir a delegação de funções de administração.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	610	Restricted administrator accounts are used to delegate management of Web Filter, IPS, and Application Control profiles, and then install those objects to their assigned ADOM.
5.18.	Deve permitir múltiplos administradores acessando o equipamento simultaneamente, sem restrição para leitura e escrita.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	568	Concurrent ADOM access is controlled by enabling or disabling the workspace function. Concurrent access is enabled by default. To prevent multiple administrators from making changes to the FortiManager database at the same time and causing conflicts, the workspace function must be enabled.

5.19.	Deve suportar o bloqueio de alterações, evitando o conflito de configurações entre diferentes administradores efetuando alterações simultaneamente.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	568	Concurrent ADOM access is controlled by enabling or disabling the workspace function. Concurrent access is enabled by default. To prevent multiple administrators from making changes to the FortiManager database at the same time and causing conflicts, the workspace function must be enabled.
5.20.	Deve registrar, em log de auditoria, as ações dos usuários administradores com o horário da alteração.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	580	The Event Log pane provides an audit log of actions made by users on FortiManager. It allows you to view log messages that are stored in memory or on the internal hard disk drive.
5.21.	Deve suportar a identificação e utilização de usuários nas políticas de segurança.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	221	IP policies The section describes how to create new IPv4 and IPv6 policies. 5. Enter the following information: - Source User - Source User Group
5.22.	Deve suportar agrupamento lógico de objetos ("object grouping") para criação de regras.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	248	Many objects now include the option to enable dynamic mapping. You can create new dynamic maps. When this feature is enabled, a table is displayed which lists the dynamic mapping information. You can also choose to add the object to groups, when available, and add tags.

5.23.	Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deve ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9644ee7-09ac-11eb-96b9-00505692583a/FortiManager-6.4.3-Administration_Guide.pdf	2512 5227 1273 2702 58	**Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede.** Managing objects and dynamic objects- Many objects now include the option to enable dynamic mapping. -Create a new object- Remove an object- Edit an object**Deve ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede.** Search objects - The search objects tool allows you to search objects based on keywordsFind unused objects - To find unused objects**Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas.**Map a dynamic device objectMap a dynamic device groupObjects from an ADOM can be promoted to the Global Database for reuse.
5.24.	Deve possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	227	To create a new Security Policy: 5. Enter the following information: Schedule: Select schedules, one time or recurring, and schedule groups.
5.25.	Deve garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e atualização remota, de maneira centralizada.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	35 e 36 493	Firmware management FortiManager can centrally manage firmware images and schedule managed devices for upgrade Device Firmware and Security Updates

5.26.	Deve ser capaz de testar a conectividade dos equipamentos gerenciados.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	73	Connection Summary Connectivity The device connectivity status and the time it was last checked. A green arrow means that the connection between the device and the FortiManager system is up; a red arrow means that the connection is down. Select Refresh to test the connection between the device and the FortiManager system
5.27.	Deve monitorar a performance e o estado dos links conectados.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	177 173	Monitor SD-WAN Health-Check Servers
5.28.	Deve suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	64	It is recommended to configure HA settings directly on FortiGate units. Another option is to run CLI scripts directly against FortiGate devices.
5.29.	Deve permitir localizar em quais regras um objeto está sendo utilizado.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9644ee7-09ac-11eb-96b9-00505692583a/FortiManager-6.4.3-Administration_Guide.pdf	271	On the Policy & Objects > Object Configuration pane, you can see whether an object is used in the Used column, and you can right-click on an object to find out where the object is used (Where Used) or to add the object to a group (Grouping).
5.30.	Deve permitir a identificação e exclusão de regras e objetos que estão aplicadas nos dispositivos, mas não afetam o desempenho e a segurança da rede (regras e objetos em desuso sob o ponto de vista lógico).	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9644ee7-09ac-11eb-96b9-00505692583a/FortiManager-6.4.3-Administration_Guide.pdf	210	Policy hit count When you run a policy check on a policy package or select the Find Unused Policies option from the Tools dropdown for a policy package, FortiManager shows hit count information for unused policies with zero hit count.

5.31.	Deve suportar a geração de alertas automáticos via SNMP e syslog.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	584 11	Enable the SNMP agent on the FortiManager device so it can send traps to and receive queries from the computer that is designated as its SNMP manager. This allows for monitoring the FortiManager with an SNMP manager. Log Settings Select Send Logs to FortiAnalyzer/FortiManager and/or Send Logs to Syslog.
5.32	Deve informar a utilização dos recursos de CPU, memória e atividade de rede dos equipamentos gerenciados.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9644ee7-09ac-11eb-96b9-00505692583a/FortiManager-6.4.3-Administration_Guide.pdf	75 181	Hardware Status The number of CPUs and the amount of RAM for the device. Map View To monitor SD-WAN with Map View: Bandwidth (TX/RX) Bandwidth of data transmitted and received. Volume (TX/RX) Volume of data transmitted and received.
5.33	Deve informar o número de conexões simultâneas dos equipamentos gerenciados.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9644ee7-09ac-11eb-96b9-00505692583a/FortiManager-6.4.3-Administration_Guide.pdf	75	Current Administrators Displays the number of administrators configured on this device.
6.	**Solução de Gerenciamento de Logs**	-	-	-
6.1.	Deve ser fornecida em appliance virtual, compatível VMware vSphere ESXi 6.0 ou superior, ou baseado em software, compatível com Windows Server 2012 R2 ou superior, ou em appliance físico com suporte à fixação em bastidor (rack) padrão EIA-310 com largura de 19’ (dezenove polegadas) e altura de até duas unidades de rack (2U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	5	FORTIANALYZER 800F Fornecido em appliance físico com suporte à fixação em bastidor (rack) padrão EIA-310 com largura de 19’ (dezenove polegadas) e altura de uma unidade de rack (2U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc)

6.2.	Deve possuir relatórios de utilização dos recursos por aplicação, URLs, ameaças etc.	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide	156, 157	FortiAnalyzer includes report templates you can use as is or build upon when you create a new report. FortiAnalyzer provide different templates for different devices. Application templates - Template - Application Risk and Control Security templates - Template - Threat Report Web templates - Template - Hourly Website Hits
6.3.	Deve possuir visualização sumarizada de todas as aplicações, ameaças e URLs que foram identificadas e controladas pela solução.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/3e37b5e2-0991-11eb-96b9-00505692583a/FortiAnalyzer-6.4.3-Administration_Guide.pdf	124123	FortiView allows you to use multiple filters in the consoles, enabling you to narrow your view to a specific time, by userID or local IP address, by application, and others. You can use it to investigate traffic activity such as useruploads/downloads or videos watched on YouTube on a network-wide user group or on an individual-user level.Displays the top applications used on the network including the application name, category, risk level, and sessions blocked and allowed. Bytes sent and received can also be enabled through the widget settings. Top Applications can be viewed as a stackbar, bar, table, or bubble chart. Displays the top allowed and blocked website domains on the network.
6.4.	Deve permitir a criação de relatórios customizados.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	1	provides customizable dashboards, reports and advanced workflow handlers for both Security & Network teams to accelerate workflows & assist with regulation and compliance audits.

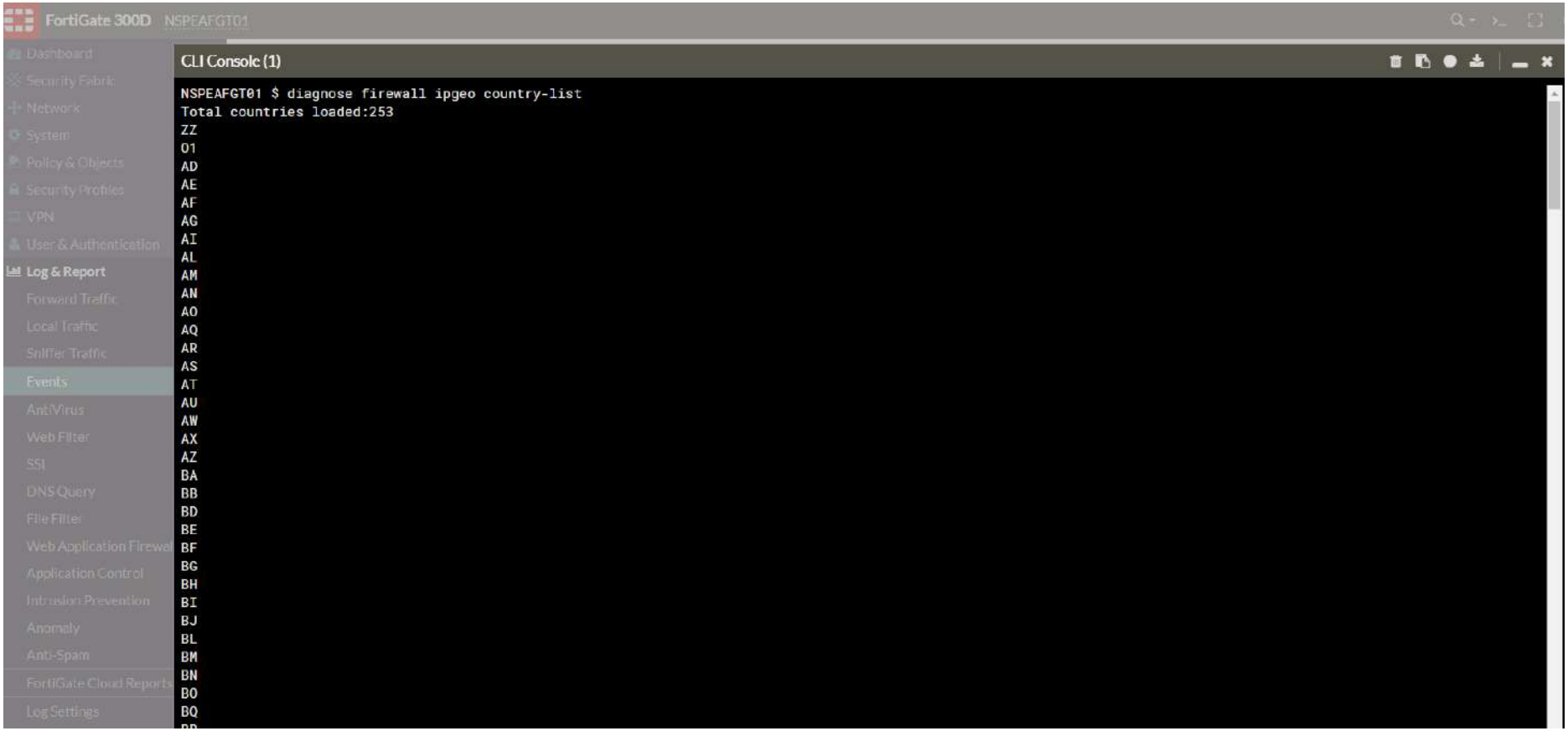
6.5.	Deve ser capaz de receber logs de todos os firewalls especificados neste Termo.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	1 5	Scalable Log Management collects logs from FortiGate, FortiClient, FortiManager, FortiSandbox, FortiMail, FortiWeb, FortiAuthenticator, Generic syslog and others. FORTIANALYZER 800F GB/Day of Logs 300 Analytic Sustained Rate (logs/sec) 8,250 Collector Sustained Rate (logs/sec) 12,000 Devices/VDOMs (Maximum) 800 Max Number of Days Analytics 30
6.6.	Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/3e37b5e2-0991-11eb-96b9-00505692583a/FortiAnalyzer-6.4.3-Administration_Guide.pdf FAZ_6.6_Country.png	51 -	**aplicação, endereço IP de origem e destino, usuário e horário.** Viewing message details **país de origem e destino,** Destination Country: Source Country

6.7.	Deve possibilitar o registro dos fluxos de dados relativos a cada sessão, armazenando:- endereços IP de origem e destino dos pacotes, - traduções NAT, portas e protocolos de origem e destino, usuário identificado, ação sobre o pacote (permitido ou negado).	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/98087932-d021-11ea-8b7d-00505692583a/FortiAnalyzer-6.4.2-Administration_Guide.pdf	425155	Within a single FortiGate, the correlation is performed by grouping logs with the same session IDs, source and destination IP addresses, and source and destination portsNAT translation is also considered when searching sources and destinations in both traffic and UTM logs. The FortiGate will generate a special traffic log to indicate the NAT IP addresses to the FortiAnalyzer within the CSF.Viewing message detailsThe Action column displays a green checkmark Accept icon when both policy and UTM profile allow the traffic to pass through, that is, both the log field action and UTM profile action specify allow to this traffic.The Action column displays a red X Deny icon and the reason when either the log field action or UTM profile action deny the traffic.

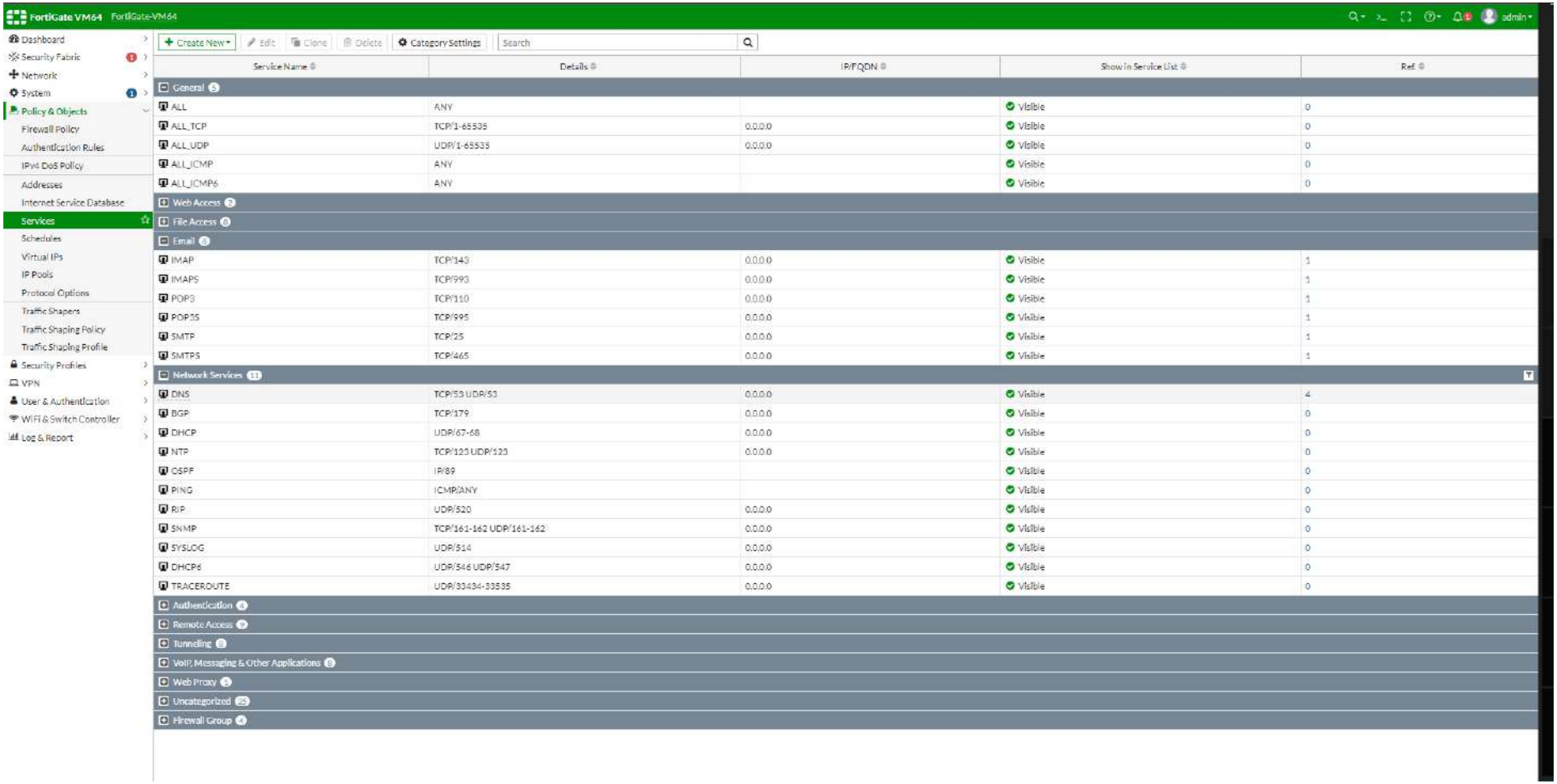
6.8.	Deve possuir relatórios com informações consolidadas sobre: as mais frequentes fontes de conexões bloqueadas com seus destinos e serviços; os mais frequentes ataques e ameaças de segurança detectados com suas origens e destinos; os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de Internet; os usuários maiores consumidores de banda de Internet; e os sítios na Internet mais visitados.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/3e37b5e2-0991-11eb-96b9-00505692583a/FortiAnalyzer-6.4.3-Administration_Guide.pdf	156 157	**as mais frequentes fontes de conexões bloqueadas com seus destinos e serviços;** Template - Top Allowed and Blocked with Timestamps **os mais frequentes ataques e ameaças de segurança detectados com suas origens e destinos;** Template - Threat Report Template - Security Analysis **os serviços de rede mais utilizados,** Template - High Bandwidth Application Usage Report **as aplicações maiores consumidoras de banda de Internet;** Template - High Bandwidth Application Usage Report **os usuários maiores consumidores de banda de Internet;** Template - User Top 500 Websites by Bandwidth **e os sítios na Internet mais visitados.** Template - Top 20 Category and Websites (Bandwidth)
6.9.	Deve possuir funcionalidade de exportação de relatórios e logs para o computador local ou via FTP, SFTP ou SCP.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/98087932-d021-11ea-8b7d-00505692583a/FortiAnalyzer-6.4.2-Administration_Guide.pdf	164	Output profiles allow you to define email addresses to which generated reports are sent and provide an option to upload the reports to FTP, SFTP, or SCP servers. Once created, an output profile can be specified for a report.
6.10.	Deve permitir a geração automática e agendada dos relatórios.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	2	Run reports on-demand or on a schedule with automated email notifications, uploads and an easy to manage calendar view.
6.11.	Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas.	-	-	*O Appliance FortiAnalyzer 800F está licenciado em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas.*

6.12.	Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõem a solução.	https://docs.fortinet.com/document/fortianalyzer/6.2.0/new-features/408516/utm-and-traffic-log-correlation-across-security-fabric	-	FortiAnalyzer correlates traffic logs to corresponding UTM logs so that it can report sessions/bandwidth together with its UTM threats. Within a single FortiGate, the correlation is performed by grouping logs with the same session IDs, source and destination IP addresses, and source and destination ports.
6.13.	Deve ser capaz de armazenar, no mínimo, 150 GB de logs diários.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	4	FORTIANALYZER 800F - GB/Day of Logs: 300
6.14.	Deve ser capaz de armazenar, no mínimo, 9 TB de logs em disco.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	4	FORTIANALYZER 800F- Storage Capacity: 16 TB (4 x 4 TB) | RAID Levels Supported: 0/1/5/10

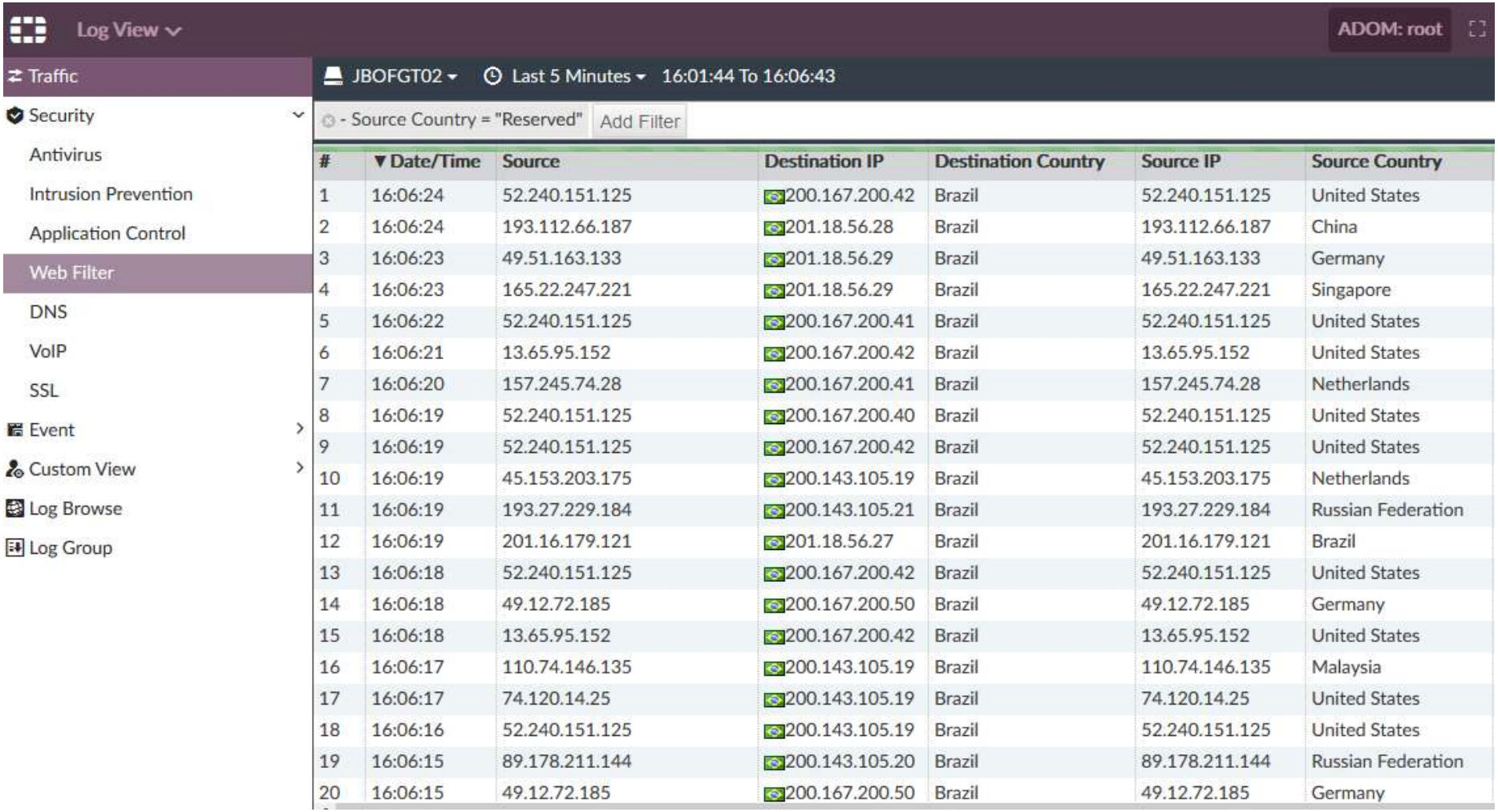
4.2.4.2_253_Paises_Codigo.PNG



4.3.2.5._87_Services.png



FAZ_6.6_Country.png



#	▼Date/Time	Source	Destination IP	Destination Country	Source IP	Source Country
1	16:06:24	52.240.151.125	200.167.200.42	Brazil	52.240.151.125	United States
2	16:06:24	193.112.66.187	201.18.56.28	Brazil	193.112.66.187	China
3	16:06:23	49.51.163.133	201.18.56.29	Brazil	49.51.163.133	Germany
4	16:06:23	165.22.247.221	201.18.56.29	Brazil	165.22.247.221	Singapore
5	16:06:22	52.240.151.125	200.167.200.41	Brazil	52.240.151.125	United States
6	16:06:21	13.65.95.152	200.167.200.42	Brazil	13.65.95.152	United States
7	16:06:20	157.245.74.28	200.167.200.41	Brazil	157.245.74.28	Netherlands
8	16:06:19	52.240.151.125	200.167.200.40	Brazil	52.240.151.125	United States
9	16:06:19	52.240.151.125	200.167.200.42	Brazil	52.240.151.125	United States
10	16:06:19	45.153.203.175	200.143.105.19	Brazil	45.153.203.175	Netherlands
11	16:06:19	193.27.229.184	200.143.105.21	Brazil	193.27.229.184	Russian Federation
12	16:06:19	201.16.179.121	201.18.56.27	Brazil	201.16.179.121	Brazil
13	16:06:18	52.240.151.125	200.167.200.42	Brazil	52.240.151.125	United States
14	16:06:18	49.12.72.185	200.167.200.50	Brazil	49.12.72.185	Germany
15	16:06:18	13.65.95.152	200.167.200.42	Brazil	13.65.95.152	United States
16	16:06:17	110.74.146.135	200.143.105.19	Brazil	110.74.146.135	Malaysia
17	16:06:17	74.120.14.25	200.143.105.19	Brazil	74.120.14.25	United States
18	16:06:16	52.240.151.125	200.143.105.19	Brazil	52.240.151.125	United States
19	16:06:15	89.178.211.144	200.143.105.20	Brazil	89.178.211.144	Russian Federation
20	16:06:15	49.12.72.185	200.167.200.50	Brazil	49.12.72.185	Germany

GRUPOMOURA

ATESTADO DE CAPACIDADE TÉCNICA E OPERACIONAL

A Acumuladores Moura S/A, inscrita no CNPJ (MF) sob o no. 09.811.654/0001-70, declara para os devidos fins, que adquiriu os produtos e serviços técnicos, detalhados abaixo, através da empresa SUPRISERVI COMÉRCIO, REPRESENTAÇÕES E SERVIÇOS LTDA – NEWSUPRI, cnpj 12707105/0001-64. Os produtos estão devidamente instalados nesta empresa e encontram-se em operação e produção. Atestamos ainda que os serviços prestados pela SUPRISERVI COMÉRCIO, REPRESENTAÇÕES E SERVIÇOS LTDA — NEWSUPRI têm sido executados sempre com elevado padrão de qualidade e rapidez no atendimento dos chamados, estando tudo de acordo com os prazos estabelecidos.

PRODUTOS
Blade Enclosures HP Serie C, com Módulos de interconexão virtual Convergente para Blade Enclosures
Servidores Blade HPE Proliant Serie BL4XX (2P)
Servidores Rack HPE Proliant Serie DL3XX (2P)
Servidores Rack HPE Proliant Serie DL380 com solução de hiperconvergencia HPE VSA
Servidores Torre HPE Proliant Serie ML3xx 92P)
Switches Aruba Serie 2000
Switches Ethernet Chassi HP Serie 8000
Switches Ethernet Rack HP Serie 5000
Switches Ethernet Rack HP Serie 1000/2000/3000
HP WLAN Controller
HP WLAN Access Point
Disk Backup Apppliance HPE StoreOnce
Tape Library HPE MSL
HP Switches Fibre Channel Serie B
Roteador Ethernet Cisco
Storage HPE 3PAR Serie 8000
Storage HPE 3PAR Serie 7000
Storage HPE EVA Serie P6000
Appliance Fortinet Fortigate 90D, 300C, 1000D, 1500D
Appliance Fortinet FortiManeger
Appliance Fortinet FortiAnalizer
Appliance Fortinet FortiMail

Fábrica
Rua Diário de Pernambuco, 195
Fone (081) 3726 1044 Fax (081) 3726 2032
CEP 55150-000 Belo Jardim PE Brasil

Escritório Central
Estrada da Batalha, 4900 Prazeres
Fone (081) 21211600 Fax (081) 21211644
CEP 54315-570 Jaboatão dos Guararapes PE Brasil

GRUPOMOURA

SOFTWARES
HPE Insigth Control e IRS
HPE (Microfocus) Data Protector
HPE IMC
HPE Virtual Storage Appliance
HP 3PAR Software
VMware vSphere e vCenter
Microsoft Windows Server
Microsoft Hyper-v
Microsoft Sharepoint Server
Microsoft SQL Server
Microsoft Link Server
Microsoft Exchange Server
Microsoft System Center
Microsoft Office 365
TREINAMENTOS
Treinamentos oficiais HPE
Treinamentos oficiais Fortinet

Fábrica
Rua Diário de Pernambuco, 195
Fone (081) 3726 1044 Fax (081) 3726 2032
CEP 55150-000 Belo Jardim PE Brasil

Escritório Central
Estrada da Batalha, 4900 Prazeres
Fone (081) 21211600 Fax (081) 21211644
CEP 54315-570 Jaboatão dos Guararapes PE Brasil

GRUPOMOURA

SERVIÇOS **Projetos de Implementação (Visão/Escopo, Planejamento, Implantação, Integração, Migração e Documentação), Treinamento hands on, Serviços de Manutenção e Suporte, Serviços de Administração e Melhoria Continua.**
Servidores (HPE Proliant Rack, Torre e Blades)
SAN/Storage (HPE Brocade, Storages EVA e 3Par)
Datacenter Networking L2/L3 e Convergencia LAN/SAN (HPE Flex Fabric)
Edge Networking WLAN e Switching (HPE MSM)
Backup (HPE Data Protector, StoreOnce e StoreEver)
Alta Disponibilidade (MS Cluster Services, HPE 3Par
Hiperconvergência (HPE VSA)
Gerenciamento de Infraestrutura (HPE OneView, HPE IMC, MS System Center, Fortinet FortiManeger e FortiAnalyzer),
Virtualização de Servidores (VMware vSphere e MS Hyper-V) e Desktops (MS RDS)
Segurança (UTM, NgFW, IsFW, e-Mail, AD)
Colaboração (Microsoft Exchange, Skype e O365)

Belo Jardim (PE), 04/09/2018.

Assinatura

ACUMULADORES MOURA S.A.
Luis João Torres
GERENTE DE TIC
CPF: 427. 405.094-72

Nome completo	Luis João Torres		
Cargo	Gerente de Infraestrutura de TIC	**Setor**	DTISS
e-mail	luis.torres@grupomoura.com	**Telefone**	81 3411-1186

Certificado de Revendedor Autorizado

Date: 10/28/2020

AO TRIBUNAL DE JUSTIÇA DO ESTADO DA PARAÍBA
DIRETORIA ADMINISTRATIVA - PREGOEIRO E EQUIPE DE APOIO
Ref.: PREGÃO ELETRÔNICO – Nº 019/2020 - PROCESSO ADMINISTRATIVO ELETRÔNICO: 2020012776

Fortinet, Inc. reconhece que: SUPRISERVI COMERCIO REPRESENTACOES E SERVICOS LTDA (NEWSUPRI)

Localizado na Rua:
Agamenon Magalhães, 4779 - Empresarial Isaac Newton - 4º Andar - Ilha do Leite – Recife, RECIFE, Pernambuco 50070-425, Brazil;

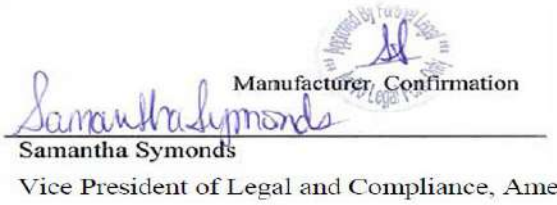
É atualmente um parceiro autorizado no BR a vender os produtos da Fortinet nas seguintes qualificacoes:

- Nivel de certificações: Advanced
- Modelo de Negócio: Integrator
- Especializações: Secure SD-WAN, LAN Edge and SD-Branch

Este certificado é emitido em 28/10/2020, e é valido até 27/11/2020

Sempre que o FortiPartner , identificado anteriormente, comprar os serviços de suporte e estes forem registrados e contratados junto à Fortinet, a Fortinet concorda em oferecer os suportes cabíveis de acordo com os termos do contrato de suporte da Fortinet, disponível em https://support.fortinet.com. A garantia do equipamento Fortinet é limitado às garantias do fabricante que se encontram no site, http://www.fortinet.com/doc/legal/EULA.pdf.

Este certificado se dá na condição do FortiPartner manter seu contrato vigente com a Fortinet e seguir as políticas e diretrizes da Fortinet. O programa de parceiros da Fortinet e suas diretrizes estão disponíveis em http://www.fortinet.com/partners/partner_program/fpp.html. Não obstante serem parceiros autorizados, os FortiPartners não representam a Fortinet e consequentemente não podem fazer declarações em nome da Fortinet.



FORTINET, INC.
899 Kifer Road
Sunnyvale, CA 94086

Telephone: +1-866-868-3678
Email: sales@fortinet.com
Website: www.fortinet.com

FORTINET

NSE Institute

NSE Training

This certifies that

Eder Lima

has successfully completed the course

SD-WAN 6.2 Self-Paced

Rob Rashotte
Vice President, Global Training &
Technical Field Enablement at Fortinet

Date: April 8, 2020

FORTINET

NSE Institute

NSE Training

This certifies that

Eder Lima

has successfully completed the course

Secure Access 6.2 Self-Paced

Rob Rashotte
Vice President, Global Training &
Technical Field Enablement at Fortinet

Date: April 29, 2020

FORTINET

NSE CERTIFIED

This certifies that

Eder Jairo de Lima

has successfully completed

NSE 1 Network Security Associate

DATE: January 16, 2018

CERTIFICATE NUMBER: 7WrcQZ6m3P

KEN XIE
CHIEF EXECUTIVE OFFICER
FORTINET

MICHAEL XIE
CHIEF TECHNOLOGY OFFICER
FORTINET

FORTINET
NSE Certification Program

FORTINET
NSE Institute

NSE Certified

This certifies that

Eder Lima

has achieved Fortinet's Network Security Expert certification

NSE 2 Network Security Associate

Certification Date: January 17, 2018

Certification Validity: 2 years

Certification Number: avWS5OpM0T

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/mod/customcert/verify_certificate.php

FORTINET

NSE Institute

NSE Certified

This certifies that

Eder Lima

has achieved Fortinet's Network Security Expert certification

NSE 3 Network Security Associate

Certification Date: January 16, 2018

Certification Validity: 2 years

Certification Number: B4q8reLhCG

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/mod/customcert/verify_certificate.php

FORTINET®
NSE Institute

NSE Certified

This certifies that

Eder Lima

has achieved Fortinet's Network Security Expert certification

NSE 4 Network Security Professional

Certification Date: April 26, 2019

Certification Validity: 2 years

Certification Number: 9nGzz9PCIB

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/mod/customcert/verify_certificate.php

FORTINET
NSE Institute

NSE Certified

This certifies that

Eder Lima

has achieved Fortinet's Network Security Expert certification

NSE 5 Network Security Analyst

Certification Date: April 26, 2019

Certification Validity: 2 years

Certification Number: xzL8vtNKoH

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/mod/customcert/verify_certificate.php

FORTINET
NSE Institute

NSE Certified

This certifies that

Eder Lima

has achieved Fortinet's Network Security Expert certification

NSE 6 Network Security Specialist

Certification Date: March 1, 2018

Certification Validity: 2 years

Certification Number: c65oa5CUDi

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/mod/customcert/verify_certificate.php

FORTINET®
NSE Institute

NSE Certified

This certifies that

Eder Lima

has achieved Fortinet's Network Security Expert certification

NSE 7 Network Security Architect

Certification Date: April 26, 2019

Certification Validity: 2 years

Certification Number: u7Yp78MzNr

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/mod/customcert/verify_certificate.php

ertificado

CERTIDÃO DE COLAÇÃO DE GRAU

C E R T I F I C O, em atendimento ao requerimento do graduado e conferida a documentação do registro acadêmico arquivada nesta Faculdade de Tecnologia, que

EDER JAIRO DE LIMA

C O N C L U I U, no ano de 2012, o Curso Superior de Tecnologia em Redes de Computadores reconhecido pela Portaria Nº. 286 de 21 Dezembro de 2012, D.O.U de 27/12/2012.

COLOU GRAU de TECNÓLOGO em 22 de Abril do ano de 2013.

Expedido pela Coordenação de Registro Acadêmico da Faculdade de Tecnologia IBRATEC em 22 de Abril de 2013.

Secretária Acadêmica

Paloma Santana Alves
Secretária Acadêmica
UNIBRATEC

UNIBRATEC®
Ensino superior e técnico em gestão e tecnologia

Diretor Acadêmico

Eduardo da Costa Aguiar
Diretor Acadêmico
UNIBRATEC

Comprovação Técnica- Equipamentos e Softwares ofertados

Item	DESCRIÇÃO	Comprovação	Página	Texto
1	**Objeto**			
1.1.	Aquisição de solução de Segurança da Informação com gerenciamento centralizado, incluindo equipamentos, softwares, licenciamentos, treinamento, garantia e suporte técnico para o Poder Judiciário do Estado da Paraíba de acordo com as especificações técnicas e quantidades constantes neste Termo de Referência e seus anexos.	-	-	
2	**Arquitetura**	-	-	-
2.1.	A solução do presente objeto é composta por firewalls remotos conectados a um firewall concentrador, gerenciados de forma centralizada.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	-	*A solução do presente objeto é composta por firewalls remotos conectados a um firewall concentrador, gerenciados de forma centralizada.*
2.2.	Os firewalls remotos devem ser capazes de encaminhar pacotes para serem analisados pelo firewall concentrador.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	-	*Os firewalls remotos (FortiGate 60F e FortiGate 100F) são capazes de encaminhar pacotes para serem analisados pelo firewall concentrador (FortiGate 600E).*

2.3.	O gerenciamento centralizado é composto por um sistema que administra, configura e gerencia todos os firewalls da solução do presente objeto.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	-	*O gerenciamento centralizado (FortiManager) é composto por um sistema que administra, configura e gerencia todos os firewalls da solução do presente objeto.*
2.4.	Todos os equipamentos firewall, a solução de gerenciamento centralizado e a solução de gerenciamento de logs devem ser do mesmo fabricante.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	-	*Todos os equipamentos firewall (FortiGate), a solução de gerenciamento centralizado (FortiMananger) e a solução de gerenciamento de logs (FortiAnalyzer) são do mesmo fabricante.*
3	**Licenciamento**	-	-	-
3.1	**Licença Padrão**	-	-	-
3.1.1.	Entende-se por Licença Padrão a licença de uso do fabricante em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas neste Termo, com exceção aos itens relacionados à Atualização de Assinaturas de Proteção.	-		*Ciente*

3.1.2.	Entende-se por Atualização de Assinaturas de Proteção todas as funcionalidades, manuais ou automatizadas, necessárias para manter a solução em seu nível de identificação e proteção mais atualizado, tais como: atualização de assinaturas de prevenção de intrusão, assinaturas de identificação de vírus, assinaturas de identificação de aplicações, listas de classificação de URLs, listas de geolocalização, listas de endereços IPs utilizados por botnets, listas de endereços IPs de reputação duvidosa etc.	-		*Ciente*
3.1.3.	Todos os equipamentos firewall devem possuir esta licença ativada.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	-	*Todos os equipamentos firewall possuem esta licença ativada.*
3.2	**Licença de Atualização de Segurança**	-	-	-
3.2.1.	Entende-se por Licença de Atualização de Segurança a licença de uso do fabricante que permita a utilização das funcionalidades e quantidades mencionadas neste Termo para os itens relacionados à Atualização de Assinaturas de Proteção (item 3.1.2).	Ciente	-	-
3.2.2.	A licença deve permitir que todas as assinaturas, listas e demais métodos de detecção e prevenção de ameaças e de filtros de conteúdo e aplicação empregados pela solução sejam atualizados até suas últimas versões disponíveis.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGuard_Security_Services.pdf	2-3	*Subscription Benefits* *Up-to-the minute threat intelligence in real time to stop the latest threats* *Seção* Subscription Services
3.2.3.	As Licenças de Atualização de Segurança devem ter prazo de vigência de 60 (sessenta) meses, contados a partir da aplicação destas nos produtos.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGuard_Security_Services.pdf	-	*As Licenças de Atualização de Segurança (FortiGuard Bundle UNIFIED PROTECTION)estão configuradas com prazo de vigência de 60 (sessenta) meses, contados a partir da aplicação destas nos produtos.*
4	**Firewall**	-	-	-
4.1	**Hardware**	-	-	-

4.1.1.	Deve ser fornecido em formato appliance físico.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf	1,2	Appliance FortiGate-60F Appliance FortiGate-100F Appliance FortiGate-600E
4.1.2.	Deve ser novo, sem uso, entregue em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	-	*São novos, sem uso, serão entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais.*
4.1.3.	Nenhum dos equipamentos fornecidos podem estar em modo End of Life, End of Sale e End of Support.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	-	*Nenhum dos equipamentos fornecidos estão em modo End of Life, End of Sale e End of Support.*
4.1.4.	Deve ser apropriado para o uso em ambiente tropical com umidade relativa na faixa de 10 a 90% (sem condensação) e temperatura ambiente na faixa de 0 a 40°C.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdfhttps://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdfhttps://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	6, 5, 5	Humidity 10–90% non-condensingOperating Temperature 32–104°F (0–40°C)

4.1.5.	Deve possuir fonte com alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz ou auto-ranging. Deve vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	6, 5, 5	Power Required 100–240V AC, 50–60 Hz Power Source 100–240V 50–60Hz Os Firewalls acompanham cabo de alimentação com 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.
4.1.6.	Deve possuir, no mínimo, 1 (uma) interface Ethernet para gerenciamento.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	3, 3	FG-60F: 10x GE RJ45 FG-100F: 3. 2x GE RJ45 MGMT/DMZ Ports FG-600E: 3. 2x GE RJ45 MGMT/HA Ports *FG-60F: 8 Portas serão utilizadas para atender ao item 4.6.10.* *2 Portas estarão disponíveis para atuar como interface de Gerenciamento.*
4.1.7.	Deve ser fornecido em sua capacidade máxima de processamento, memória e armazenamento interno.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	-	*Os Firewalls estão sendo fornecidos em sua capacidade máxima de processamento, memória e armazenamento interno.* *Não existe upgrade de CPU, Memória e Disco para os Appliances FG-60F, FG-100F e FG-600E.*

4.1.8.	Deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, inclusive com seus respectivos transceivers instalados, sem custos adicionais.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	-	*Os Firewalls estão sendo fornecidos com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, inclusive com seus respectivos transceivers instalados, sem custos adicionais.*
4.1.9.	Deve possuir certificação de conformidade sustentável de acordo com os padrões EPA (Environmental Protection Agency) ou similares, tais como EnergyStar, RoHS (Restriction on Harzardous Substances) ou WEEE (Waste Electrical and Eletronic Equipment).	https://www.fortinet.com/corporate/about-us/corporate-social-responsibility.html	-	RoHS compliance WEEE compliance
4.2.1.	**Funcionalidades Básicas**	-	-	-
4.2.1.1.	Deve possuir MIB própria contemplando, no mínimo, indicadores de estado do hardware e de performance do equipamento.	FORTINET-FORTIGATE-MIB	-	fgSysCpuUsage OBJECT-TYPE"...Current CPU usage (percentage)..."fgSysMemUsage OBJECT-TYPE"...Current memory utilization (percentage)..."fgHwSensorEntry OBJECT-TYPE SYNTAX FgHwSensorEntry MAX-ACCESS not-accessible STATUS current DESCRIPTION "An entry containing the name, value, and alarm status of a given hardware sensor" INDEX { fgHwSensorEntIndex } ::= { fgHwSensorTable 1 }FgHwSensorEntry ::= SEQUENCE { fgHwSensorEntIndex FnIndex, fgHwSensorEntName DisplayString, fgHwSensorEntValue DisplayString, fgHwSensorEntAlarmStatus INTEGER

4.2.1.2.	Deve suportar o envio de notificações via e-mail, SNMP traps e mensagens de log.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/893788/alert-email https://docs.fortinet.com/document/fortigate/6.0.0/handbook/92582/snmp https://docs.fortinet.com/document/fortigate/6.0.0/handbook/289288/logging	-	"Alert emails provide an efficient and direct method of notifying an administrator of events." "...You can configure the hardware, such as the FortiGate SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers..." "...you to monitor, store, and report traffic information and FortiGate events, including attempted log ins and hardware status..."
4.2.1.3.	Deve permitir o acesso ao equipamento via SSH e interface web HTTPS.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	Management access: HTTPS via web browser, SSH, telnet, console
4.2.1.4.	A comunicação entre a estação de trabalho do administrador e o firewall deve ser autenticada e criptografada.	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/241541/connecting-using-a-web-browser	-	"...an interface must be configured to allow administrative access over HTTPS..."
4.2.1.5.	Deve informar a utilização dos recursos de CPU, memória e atividade de rede.	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/882981/dashboard-widgets https://docs.fortinet.com/document/fortigate/6.0.0/handbook/799410/fortiview-consoles	-	"...System Usage: System usage information, such as CPU, memory, and disk usage, as well as the number of active sessions..." "...Interfaces displays the number of interfaces connected to your network, how many sessions there are in each interface, and what sort of traffic is occurring..."
4.2.1.6.	Deve possuir visualização mínima sumarizada de aplicações, ameaças, URLs, endereços de origem, endereços de destino, levando-se em conta o quantitativo de sessões, de consumo de banda e categorização.	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/433781/fortiview-monitors-and-widgets	-	FortiView monitors and widgets FortiView Sources FortiView Destinations FortiView Applications FortiView Websites FortiView Policies FortiView Sessions

4.2.1.7.	Deve possuir a funcionalidade de exportação automática dos logs para servidor syslog e para a Solução de Gerenciamento de Logs.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	Logging facilities support: Local memory & storage (if available), multiple syslog servers, multiple FortiAnalyzers, WebTrends servers, FortiCloud hosted service
4.2.2.	**Rede**	-	-	-
4.2.2.1.	Deve suportar os protocolos IPv4 e IPv6.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	1	Highlights — What's New Consolidate IPv4 and IPv6 policy configuration
4.2.2.2.	Deve suportar VLAN no padrão 802.1q.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	Layer-2 interface modes: Port aggregated, loopback, VLANs (802.1Q and Trunking), virtual hardware, software, and VLAN switches
4.2.2.3.	Deve suportar os protocolos DHCP e DHCPv6 e suas funcionalidades como cliente, servidor e relay.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/2c229bb9-78ed-11ea-9384-00505692583a/FortiOS-6.4-Supported_RFCs.pdf https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/783526/dhcp-server	7-8	RFC 2131: Dynamic Host Configuration Protocol RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6) "..You can configure one or more DHCP servers on any FortiGate interface..." "..You can configure a FortiGate interface as a DHCP relay..."
4.2.2.4.	Deve suportar Jumbo Frames.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/822669/interface-mtu-packet-size	-	"...Jumbo frames are supported on FortiGate models..."
4.2.2.5.	Deve suportar subinterfaces Ethernet lógicas.	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/402940/vlans	-	"...You can define VLAN subinterfaces on all FortiGate physical interfaces..."
4.2.2.6.	Deve suportar o protocolo NTP.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	9	Essential Network Services - A wealth of networking services such as DHCP, DNS server, NTP server and more

4.2.2.7	Deve implementar mecanismo de conversão de endereços NAT (Network Address Translation), de forma a possibilitar a realização de NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional (possibilitando que um endereço tenha mais de um NAT dependendo da origem, destino ou porta).	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/474356/static-nat https://docs.fortinet.com/document/fortigate/6.0.0/handbook/248992/dynamic-nat https://docs.fortinet.com/document/fortigate/6.0.0/handbook/801437/ip-pools https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/898655/static-snat https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/155333/virtual-ips-with-port-forwarding	- - - -	Static NAT "...In FortiGate firewall configurations this is most commonly done with the use of Virtual IP addressing..." Dynamic NAT "..In the FortiGate firewall this can be done by using IP Pools..." "..IP Pools are a mechanism that allow sessions leaving the FortiGate Firewall to use NAT..." Seção "Static SNAT" "Virtual IPs with port forwarding"
4.2.2.8	Deve permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/986892/sample-logs-by-log-type	-	# Corresponding traffic log # "...date=2019-05-13 time=16:29:50..." "...srcip=10.1.100.11..." "...dstip=185.244.31.158..." "...trandisp="snat" transip=172.16.200.2..."
4.2.2.9	Deve suportar tradução de porta (PAT).	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	NAT support: NAT64, NAT46, static NAT, dynamic NAT, PAT, Full Cone NAT, STUN
4.2.2.10	Deve suportar as funcionalidades de roteamento estático e dinâmico em IPv4 e IPv6.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/691160/routing-concepts	-	The type values assigned to FortiGate routes (Static, Connected, RIP, OSPF, or BGP). "...Static: The static routes that have been added to the routing table manually..." "...OSPF: All routes learned through OSPF..." "...OSPF6: All routes learned through OSPF version 6 (which enables the sharing of routes through IPv6 networks)..."
4.2.2.11	Deve suportar os protocolos RIP, OSPF v2, OSPF v3 e BGP v4.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	Dynamic routing protocols: RIPv1 and v2, OSPF v2 and v3, ISIS, BGP4

4.2.2.12	Deve suportar os protocolos IGMP v2, IGMP v3, PIM-SM.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/308396/sparse-mode https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	- 12	"To receive multicast traffic, a client application can use Internet Group Management Protocol (IGMP) version 1 (RFC 1112), 2 (RFC 2236), or 3 (RFC 3376)..." Multicast traffic: sparse and dense mode, PIM support
4.2.2.13	Deve suportar Virtual Routing Redundancy Protocol (VRRP) ou equivalente.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	8	Support for industry-standard VRRP and various proprietary solutions, with ability to combine more than one high availability solution into a single configuration
4.2.2.14	Deve suportar os protocolos SNMP v2 e SNMP v3.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	- SNMP v1 and v2c support - SNMP v3 implementation includes support for queries, traps, authentication, and privacy
4.2.2.15	Deve permitir monitorar, via SNMP, falhas de hardware, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN, CPU, memória, status do cluster de Alta Disponibilidade e estatísticas de uso das interfaces de rede.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/92582/snmp FORTINET-FORTIGATE-MIB	-	"SNMP fields contain information about the FortiGate unit, such as CPU usage percentage or the number of sessions." "Power Supply Failure event trap is available only on some models." "... you can use the value ifHighSpeed. It reports interface speeds in megabits/second..." "..fgVpnTunnelUpCount OBJECT-TYPE The number of IPsec VPN tunnels with at least one SA..." fgSysMemUsage OBJECT-TYPE "...Current memory utilization (percentage)..." fgHaSystemMode OBJECT-TYPE "High-availability mode (Standalone, A-A or A-P)"
4.2.2.16	Deve suportar Policy Based Routing (PBR), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD46603	-	"Technical Tip: Configuring the firewall Policy Routes"

4.2.3.	**Autenticação e Identificação de Usuários**	-	-	-
4.2.3.1.	Deve promover a integração com serviços de diretório LDAP e Active Directory, baseados em caracteres da língua portuguesa, para a identificação, autenticação, autorização e registro de eventos de acessos ou ameaças.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/888827/poll-active-directory-server https://docs.fortinet.com/document/fortigate/6.2.2/cookbook/896276/cli-basics	10 - -	Local user database and remote user authentication service support: LDAP "The FortiGate unit can authenticate users and allow them network access based on groups membership in Windows Active Directory (AD)" Seção "Language support and regular expressions"
4.2.3.2.	Deve identificar de forma transparente os usuários autenticados por meio de serviço de diretório LDAP ou Active Directory.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/615946/agent-based-fsso-for-windows-ad https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/731999/fsso-in-polling-mode-for-windows-ad	-	Single-sign-on: Integration with Windows AD Agent-based FSSO for Windows AD FSSO in polling mode for Windows AD
4.2.3.3.	Não será permitida a utilização de agentes instalados nos servidores LDAP, Active Directory, proxies internos e equipamentos dos usuários, nem configuração adicional no navegador.	N/A	N/A	*A solução ofertada não necessita de utilização de agentes instalados nos servidores LDAP, Active Directory, proxies internos e equipamentos dos usuários, nem configuração adicional no navegador.*
4.2.3.4.	Não será permitida a interceptação ou espelhamento do tráfego destinado aos servidores LDAP, Active Directory e proxies internos.	N/A	N/A	*A solução ofertada não utiliza interceptação ou espelhamento do tráfego destinado aos servidores LDAP, Active Directory e proxies internos.*
4.2.3.5.	Deve possuir portal de autenticação (captive portal) para a identificação e autenticação de usuários não registrados ou não reconhecidos.	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/574723/interface-settings	-	"...After enabling captive portal authentication, you can configure the authentication portal, user and group access..."

4.2.3.6.	O portal de autenticação deve ser capaz de identificar e autenticar usuários cadastrados em serviço de diretório LDAP e Active Directory.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/868644/captive-portalshttps://docs.fortinet.com/document/fortigate/6.0.0/handbook/518646/users-and-user-groups#User_groups	--	"...User Groups: Select permitted user groups.""User groups a remote user account (password stored on a RADIUS, LDAP, or TACACS+ server)"
4.2.3.7.	Deve permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP ou ao Active Directory.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies	-	Firewall policies Source User(s) This parameter is based on a user identity that can be from a number of authentication authorities. It will be an account or group that has been set up in advance that can be selected from the drop down menu. The exception to this is the feature that allows the importing of LDAP Users..."
4.2.3.8.	Deve registrar a identificação do usuário em todos os logs de eventos de acesso ou de ameaças gerados pelo equipamento.	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/536166/viewing-event-logs	-	"User Events View events relating to users"
4.2.3.9.	Deve registrar os eventos dos usuários em tempo real, sem a utilização de processos em lote (batches) ou processos de correlação após a ocorrência do evento em questão.	https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/476970	-	FortiView is a logging tool made up of a number of dashboards that show real time and historical logs.
4.2.3.10.	Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/829757/administrators	-	"...For example, you can configure a profile so that the administrator can only read/write Firewall configuration, which includes firewall policies, addresses, services, schedules, packet capture, and some other parts of the FortiGate configuration. Any other aspects of the FortiGate configuration, including VPNs and security profiles, would be hidden from this administrator."
4.2.4.	**Geolocalização**	-	-	-

4.2.4.1.	Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/133721/fortiview	-	"FortiView is the FortiOS log view tool which is a comprehensive monitoring system for your network. FortiView integrates real-time and historical data into a single view on your FortiGate." "...The following are just some of the FortiView categories: Sources, Destinations, Applications, Cloud Application, Country..."
4.2.4.2.	Deve identificar, no mínimo, 180 países.	4.2.4.2_253_Paises_Codigo.png	-	"Total countries loaded: 253"
4.2.4.3.	Deve armazenar as listas de geolocalização no próprio equipamento.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD40832	-	"This article describes how to update the GeoIP database on FortiGate equipment. The GeoIP database version does not always update when the following command is run: # execute update now"
4.2.4.4.	Deve permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD40500	-	"This article shows the configuration to protect a server from attacks from countries that user has no business with."
4.2.4.5.	Deve possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/133721/fortiview	-	"FortiView is the FortiOS log view tool which is a comprehensive monitoring system for your network. FortiView integrates real-time and historical data into a single view on your FortiGate." "...The following are just some of the FortiView categories: Sources, Destinations, Applications, Cloud Application, Country..."
4.2.5.	**VPN**	-	-	-

4.2.5.1.	Deve suportar VPN site-to-site em topologia Full Meshed (todos os gateways possuem links específicos para todos os demais gateways) e Estrela (gateways satélites se comunicam somente com um único gateway central).	https://docs.fortinet.com/document/fortimanager/6.4.0/administration-guide/556949/configuring-a-full-mesh-vpn-topology-within-a-vpn-console-example https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/755287/redundant-hub-and-spoke-vpn	-	"Configuring a full mesh VPN topology within a VPN console" "Redundant hub and spoke VPN"
4.2.5.2.	Deve suportar criptografia 3DES, AES-128, AES-256.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	IPsec VPN:- Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128. AES192, AES256, ARIA128, ARIA192, ARIA256, SEED
4.2.5.3.	Deve suportar integridade de dados com MD5, SHA-1 e SHA-256.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	IPsec VPN: - Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
4.2.5.4.	Deve suportar o protocolo IKE, fases I e II.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	IPsec VPN: - Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
4.2.5.5.	Deve suportar os algoritmos RSA e Diffie-Hellman groups 1, 2, 5 e 14.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/156465/configuring-phase-2-parameters	-	"Diffie-Hellman Group - Select one Diffie-Hellman group (1, 2, 5, 14 through 21, or 27 through 30)."
4.2.5.6.	Deve suportar Certificado Digital X.509.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	10	PKI and certificates: X.509 certificates, SCEP support, Certificate Signing Request (CSR) creation, autorenewal of certificates before expiry, OCSP support
4.2.5.7.	Deve suportar NAT-T (NAT Transversal).	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	IPsec VPN: - XAuth for dialup users: Server type option (PAP, CHAP, Auto), NAT Traversal option - Configurable IKE encryption key expiry, NAT traversal keepalive frequency
4.2.5.8.	Deve permitir a criação de túneis VPN SSL/TLS e IPSec.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	6	Feature / VPN SSL and IPsec VPN wizards
4.2.5.9.	Deve suportar VPN IPSec client-to-site (acesso remoto).	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf	1, 2	"Max Client to G/W IPSEC Tunnels "

4.2.5.10.	Deve possuir cliente próprio para instalação nos dispositivos móveis dos usuários, sem custo adicional.	https://docs.fortinet.com/document/forticlient/6.2.0/new-features/673187/free-vpn-client	-	For FortiGate administrators, a free version of FortiClient VPN is available which supports basic IPsec and SSL VPN and does not require registration with EMS.
4.2.5.11.	Deve permitir que o usuário realize a conexão VPN por meio de cliente instalado no sistema operacional Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 8.1 (32 e 64 bits), Windows 10 (32 e 64 bits), Apple IOS, Android, Mac OS 10 ou Linux do seu equipamento ou por meio de interface web do tipo portal.	https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/912474/ssl-vpn-using-web-and-tunnel-mode	-	"...allow remote users to access the corporate network using an SSL VPN, connecting either by web mode using a web browser..."
4.2.5.12.	O acesso por meio da interface Web deverá ser compatível com, no mínimo, os navegadores Internet Explorer 9 ou superior e Firefox 4.0 ou superior.	https://docs.fortinet.com/document/fortigate/6.2.3/fortios-release-notes/973252/ssl-vpn-support	-	Microsoft Windows 10 (64-bit) Microsoft Edge Mozilla Firefox version 61 Google Chrome version 68
4.2.5.13.	Deve suportar atribuição de endereço IP nos clientes remotos de VPN.	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/6896/fortigate-as-dialup-client	-	config firewall address edit "client_range" set type iprange set start-ip 10.10.10.1 set end-ip 10.10.10.200
4.2.5.14.	Deve suportar atribuição de DNS nos clientes remotos de VPN.	https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/6896/fortigate-as-dialup-client	-	set dns-mode auto
4.2.5.15.	Deve suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF e BGP.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD47665 https://kb.fortinet.com/kb/documentLink.do?externalID=FD38847	-	"Technical Tip: Dynamic dial-up VPN with OSPF" "Technical Note: Dynamic routing (BGP) over IPsec tunnel"
4.2.5.16.	O túnel IPSec VPN do cliente ao gateway (client-to-site) deve fornecer uma solução de autenticação única (single-sign-on) aos usuários, integrando-se com as ferramentas de Windows login.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD45619	-	"This article describes how to configure SSO Auto with LDAP users for SSL-VPN bookmarks."

4.2.5.17.	Deve permitir criar políticas por usuário e grupos para tráfego de VPN client-to-site.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/527388/multiple-user-groups-with-different-access-permissions	-	"You need to define security policies to permit your SSL VPN clients, web-mode or tunnel-mode, to connect to the protected networks behind the FortiGate unit."
4.2.5.18.	Deve suportar autoridade certificadora integrada ao gateway VPN ou à solução de gerenciamento centralizado.	https://docs.fortinet.com/document/fortimanager/6.2.0/administration-guide/549422/certificate-templates	-	Certificate templates The certificate templates menu allows you to create certificate templates for an external certificate authority (CA) or the local FortiManager CA.
4.2.5.19.	Deve promover a integração com diretórios LDAP e Active Directory para a autenticação de usuários de VPN e regras de acesso.	https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/115783/ssl-vpn-with-ldap-user-authentication	-	"This is a sample configuration of SSL VPN for LDAP users. In this example, the LDAP server is a Windows 2012 AD server. A user ldu1 is configured on Windows 2012 AD server."

4.2.5.20.	Deve suportar os métodos de autenticação de VPN: usuário e senha de base interna do próprio equipamento, usuário e senha de diretório LDAP, usuário e senha do Active Directory, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao Active Directory, certificação digital por meio de certificados emitidos por autoridade certificadora no padrão ICP-Brasil.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/544195/ssl-vpn-with-local-user-password-policy https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/688719/ssl-vpn-with-ldap-user-password-renew https://docs.fortinet.com/document/fortimanager/6.2.0/administration-guide/549422/certificate-templates https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/680736/microsoft-ca-deep-packet-inspection https://kb.fortinet.com/kb/documentLink.do?externalID=FD48647	-	**usuário e senha de base interna do próprio equipamento,** - SSL VPN with local user password policy **usuário e senha de diretório LDAP,** **usuário e senha do Active Directory,** This is a sample configuration of SSL VPN for LDAP users with Force Password Change on next logon. In this example, the LDAP server is a Windows 2012 AD server. **certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado,** - The certificate templates menu allows you to create certificate templates for an external certificate authority (CA) or the local FortiManager CA. **certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao Active Directory,** An existing Microsoft root CA can be used to issue a subordinate CA (sub CA) certificate that is installed as a DPI certificate on the FortiGate. **certificação digital por meio de certificados emitidos por autoridade certificadora no padrão ICP-Brasil.** - This article describes how to authenticate PKI users on FortiGate via SSL VPN using two factor authentication with certificate.
4.2.5.21.	Deve suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKCS#12.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/943479/certificate-based-authentication#Example	-	Seção "To import a PKCS12 certificate from the CLI"

4.2.5.22.	Deve suportar a solicitação de emissão de certificados à uma autoridade certificadora de confiança (enrollment) via SCEP (Simple Certificate Enrollment Protocol) ou CSR (Certificate Signing Requests).	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/943479/certificate-based-authentication#Example	-	In Enrollment Method, you have two methods to choose from. Select File Based to generate the certificate request, or Online SCEP to obtain a signed SCEP-based certificate automatically over the network. For the SCEP method, enter the URL of the SCEP server from which to retrieve the CA certificate, and the CA server challenge password.
4.2.5.23.	Deve suportar a leitura e verificação de CRLs (Certification Revogation Lists).	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/943479/certificate-based-authentication	-	Seção "Certificate revocation list"
4.2.5.24.	Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/350451/configuring-security-policieshttps://help.fortinet.com/fmgr/50hlp/56/5-6-2/FMG-FAZ/1900_FortiView/0015_Summary_list.htm	-	"The SSL VPN security policy specifies...""...The UTM features and logging that are applied to the connection.""FortiView - VPN - SSL & Dialup IPsec""Displays the users who are accessing the network by using the following types of security over a virtual private network (VPN) tunnel: secure socket layers (SSL) and Internet protocol security (IPsec)."
4.2.6.	**Qualidade de Serviço (QoS)**	-	-	-

4.2.6.1.	Deve permitir o controle de políticas de uso com base nas aplicações: permitir, negar, inspecionar, agendar, e controlar o uso da largura de banda que utilizam cada aplicação ou usuário.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/19814/basic-category-filters-and-overrides https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/122688/traffic-shaping-schedules https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	- - 12	"Basic category filters and overrides" "Under Categories, left click the icon next to the category name to view a dropdown of actions: Allow, Monitor, Block..." "...apply a traffic shaper or shaping group to the traffic, including using schedules..." "Traffic shaping and QoS per policy or applications: Shared policy shaping, per-IP shaping, interface-based traffic shaping, maximum and guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS), ,Differentiated Services (DiffServ) and Forward Error Correction (FEC) for VPN support"
4.2.6.2.	Deve suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp).	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/204835/configuring-application-control-traffic-shaping https://docs.fortinet.com/document/fortigate/6.0.0/handbook/350790/configuring-per-ip-traffic-shaping	- -	" Applying traffic shaping to applications is useful for managing bandwidth-intensive applications, such as YouTube, that use the same TCP and UDP port numbers as mission-critical applications." "Per-IP traffic shaping allows you to define traffic control on a more granular level by managing bandwidth use by user IP addresses." "Traffic shaping by IP address allows you to apply traffic shaping to all source IP addresses in the security..."
4.2.6.3.	Deve suportar a priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	FIREWALL: VoIP traffic support: SIP/H.323 /SCCP NAT traversal, RTP pin holing

4.2.6.4.	Deve suportar a marcação de pacotes DiffServ.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	Traffic shaping and QoS per policy or applications: Differentiated Services (DiffServ) and Forward Error Correction (FEC) for VPN support
4.2.6.5.	Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/575292/all-sessions	-	**Aplicações / Sessões**The All Sessions console provides information about all FortiGate traffic. This console can be filtered by Application, Country, Destination Interface, Destination IP, Destination Port, NAT Source IP, NAT Source Port, Policy, Protocol, Source, Source Interface, Source IP, and Source Port. **bytes**This would be useful to display alongside other columns such as the Source, Destination, and Bytes (Sent/Received) columns, as patterns or inconsistencies can be analyzed.**usuários**From the All Sessions console, a wide variety of filters can be applied to sort the session data. In this example, the All Sessions filters will be used to locate a specific user's recent Skype activity.
4.2.7.	Balanceamento de Links	-	-	-

4.2.7.1.	Deve implementar balanceamento de links utilizando as seguintes métricas e critérios para a escolha do caminho: aplicações, jitter, latência e perda de pacotes, permitindo que administradores configurem os valores de tais parâmetros para definir por qual interface certo tipo de tráfego será enviado	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/382233/performance-sla-sla-targets	12 -	SD WAN "WAN link checks for SLAs:" "...- Monitoring criteria including latency, jitter, and packet loss..." "Multi-path intelligence using rules defined by:" "...- Destination address and/or a selection of over 3,000 applications..." Latency threshold: Latency for SLA to make decision, in milliseconds (0 - 10000000, default = 5). Jitter threshold: Jitter for SLA to make decision, in milliseconds (0 - 10000000, default = 5). Packet loss threshold: Packet loss for SLA to make decision, in percentage (0 - 100, default = 0).
4.2.7.1.1	Caso o item acima não seja atendido em sua totalidade, será aceita composição com outro equipamento, do tipo appliance físico, desde que a configuração seja realizada através da interface de gerenciamento do firewall e da Solução de Gerenciamento Centralizada, sem nenhum ônus para a CONTRATANTE, garantindo o pleno atendimento das métricas e critérios para a escolha do caminho, segundo o item acima a) O appliance físico do item anterior deve possuir throughput igual ou superior à discriminada no throughput das “funcionalidades de Filtro de Pacotes, IPS, Filtro de Conteúdo e Proteção contra Malwares habilitadas simultaneamente” do respectivo firewall. b) O appliance físico do item anterior deve possuir os mesmos requisitos de fontes de	-	-	-

	alimentação e de afixação em rack, quando exigidos, do respectivo firewall.			
4.2.7.2	Os valores dos parâmetros jitter e latência devem poder ser configurados em unidade mínima de milissegundos (ms).	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/382233/performance-sla-sla-targets	-	Latency threshold: Latency for SLA to make decision, in milliseconds (0 - 10000000, default = 5). Jitter threshold: Jitter for SLA to make decision, in milliseconds (0 - 10000000, default = 5). Packet loss threshold: Packet loss for SLA to make decision, in percentage (0 - 100, default = 0).
4.2.7.3	A interface virtual de balanceamento deve suportar agregar no mínimo 4 (quatro)interfaces, podendo ser do tipo: física, subinterface e VPN.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/19246/sd-wanhttps://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/218559/configuring-the-sd-wan-interface	--	At least one interface must be configured for SD-WAN to function; up to 255 member interfaces can be configuredFirst, SD-WAN must be enabled and member interfaces must be selected. The selected FortiGate interfaces can be of any type (physical, aggregate, VLAN, IPsec, and others)
4.2.7.4	Deve suportar balanceamento de link por hash do IP de origem e destino.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	WAN load balancing (weighted) algorithms by: volume, sessions, source-destination IP, Source IP, and spillover
4.2.7.5	Deve suportar balanceamento de link por peso. Nesta opção deve ser possível definir o peso de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, 4 (quatro) links WAN.	https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/477154/configuring-sd-wan-load-balancing https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/19246/sd-wan	- -	"In the example, the ISP connected to WAN1 is a 40Mb link, and the ISP connected to WAN2 is a 10Mb link, so we balance the weight 75% to 25% in favor of WAN1." "At least one interface must be configured for SD-WAN to function; up to 255 member interfaces can be configured"

4.2.7.6	Deve permitir a configuração da funcionalidade de balanceamento em qualquer interface WAN, seja ela MPLS, Internet, 4G/LTE etc.	https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/218559/configuring-the-sd-wan-interface https://docs.fortinet.com/document/fortigate/6.0.0/handbook/836394/setting-up-your-supported-lte-modem https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/125874/mpls-sip-and-backup-dia-cloud-apps	- - -	"First, SD-WAN must be enabled and member interfaces must be selected. The selected FortiGate interfaces can be of any type (physical, aggregate, VLAN, IPsec, and others)" "If you are using your LTE modem for a backup or redundant internet connection, you can add an SD-WAN interface that includes the FortiGate wired internet connecting interface and the wwan interface." "This topic covers a typical customer usage scenario where the customer's SD-WAN has two members: MPLS and DIA."
4.2.7.7	Deve possuir roteamento baseado em políticas e múltiplas saídas (e tipos de saídas) WANs.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/672387/using-bgp-tags-with-sd-wan-rules	-	"In this example, a customer has two ISP connections, wan1 and wan2. wan1 is used primarily for direct access to internet applications, and wan2 is used primarily for traffic to the customer's data center." "This example assumes that SD-WAN is enable on the FortiGate, wan1 and wan2 are added as SD-WAN members, and a policy and static route have been created."
4.2.7.8	Deve permitir a configuração de failover entre links principais e secundários, caso os links utilizados ultrapassem os limites previamente definidos de jitter, latência e perda de pacotes. Estes limites podem ser configurados para forçar o failover caso apenas um ou todos os limites sejam atingidos simultaneamente.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/382233/performance-sla-sla-targets	-	Seção "Performance SLA - SLA targets" Latency threshold: Latency for SLA to make decision, in milliseconds (0 - 10000000, default = 5). Jitter threshold: Jitter for SLA to make decision, in milliseconds (0 - 10000000, default = 5). Packet loss threshold: Packet loss for SLA to make decision, in percentage (0 - 100, default = 0).

4.2.7.9	Deve suportar a configuração de regras que permita o failback imediato.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/370572/configuring-link-health-monitoring	-	Restore link after Set the number of successful status checks before the FortiGate restores the interface to SD-WAN load balancing groups. The range is 1 to 10. The default is 5. This setting helps prevent flapping, where the system continuously transfers traffic back and forth between links.
4.2.7.10	Deve ser compatível com a solução de VPN, permitindo que suas características e análises sejam realizadas nas VPNs, assim como em links WAN.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD41297	-	Artigo "Technical Tip: Configure FortiGate SD-WAN with an IPSEC VPN"
4.2.7.11	Deve ser compatível com VPNs montadas em interfaces virtuais com roteamentodinâmico.	https://kb.fortinet.com/kb/documentLink.do?popup=true&externalID=FD41389&languageId=	-	Artigo "Technical Note: How to use BGP and SD-WAN for advertising routes and path selection in FortiGate"
4.2.7.12	Deve realizar o gerenciamento de tráfego por tipo de aplicação	https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/80739/dynamic-application-steering-with-lowest-cost-and-best-quality-strategies	-	"...Under Destination, set Application to your required applications. In this example: Microsoft.Office.365, Microsoft.Office.Online, Google.Docs, Dropbox, and SIP..."
4.2.7.13	Deve selecionar o melhor caminho baseado em tipo de tráfego e do host de origem	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	Multi-path intelligence using rules defined by: - Source address and/or user group - Destination address and/or a selection of over 3,000 applications - path selection using particular link quality criteria or SLAs defined
4.2.7.14	Deve suportar o monitoramento de link com ping e TCP-echo.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/370572/configuring-link-health-monitoring	-	Configure link health monitoring – CLI set protocol {ping | ping6 | tcp-echo | udp-echo | http | twamp}

4.2.7.15	Deve suportar o monitoramento de links VPN (interfaces virtuais).	https://kb.fortinet.com/kb/documentLink.do?externalID=FD41297 https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FMG-FAZ/1900_FortiView/0015_Summary_list.htm	-	Technical Tip: Configure FortiGate SD-WAN with an IPSEC VPN VPN - SSL & Dialup IPsec "Displays the users who are accessing the network by using the following types of security over a virtual private network (VPN) tunnel: secure socket layers (SSL) and Internet protocol security (IPsec)."
4.2.7.16	Deve permitir a exportação de informações via netflow.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD36460	-	Technical Tip: How to Configure Netflow on a FortiGate
4.3	**Recursos de Segurança**	-	-	-
4.3.1.	**Características Gerais**	-	-	-
4.3.1.1.	Deve possuir, no mínimo, funcionalidades Anti-Vírus, Anti-Bot, Anti-Malware, Anti-Spyware, Sistema de Prevenção de Intrusão (IPS), Filtro de Conteúdo Web e Controle de Aplicação.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGuard_Security_Services.pdf	2,3	"FortiGuard Advanced Malware Protection is a robust service providing core technologies needed for security protection for known threats and emerging threats. And includes: Antivirus, Botnet IP/Domain Service, Mobile Malware Security..." "FortiGuard Antivirus delivers automated updates that protect against the latest viruses, spyware..." "Intrusion Prevention (IPS)" "Web Filtering" "Application Control"
4.3.1.2.	Deve suportar o funcionamento nos modos sniffer (para inspeção de tráfego gerado por uma porta de rede espelhada), layer-2, layer-3.	https://kb.fortinet.com/kb/documentLink.do?externalID=11186 https://kb.fortinet.com/kb/documentLink.do?externalID=FD31207	- -	Sniff 3 packets of all traffic with verbose Level 4 on internal Interface # diag sniffer packet internal none 4 3 A sniffer trace will tell if OSPF HELLO packets are sent/received : FGT2# diagnose sniffer packet any "proto 89" 4 (stop sniffer with CTRL+C)

4.3.1.3.	Deve aplicar novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas.	https://docs.fortinet.com/document/fortigate/6.0.0/best-practices/502147/policy-configuration	-	Policy configuration changesOn a heavy-loaded system, plan configuration changes during low usage periods in order to minimize impact on CPU usage and established sessions. In this scenario, it is considered a best practice to de-accelerate the hardware-accelerated sessions.where you want the following to be true:check-all-CPU flushes all current sessions and re-evaluates them. This is the default option.check-new-CPU keeps existing sessions and applies policy changes to new sessions only. This reduces CPU load and the possibility of packet loss.check-policy-option- Use the option selected in the firewall-session-dirty field of the firewall policy (check-all or check-new, as above, but per policy).
4.3.1.4.	Deve suportar as atualizações automáticas da bases de assinaturas utilizadas na identificação de vírus, intrusões (IPS) e aplicações sem a necessidade de intervenção manual pelo administrador, sem perda das conexões ativas e sem reinicialização do equipamento.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/547335/automatic-updates	-	Automatic updates Push updates Push updates enable you to get immediate updates when new viruses or intrusions are discovered and new signatures are created. This ensures that the latest signature are sent to the FortiGate as soon as possible.

4.3.1.5.	Deve suportar as atualizações automáticas das listas de geolocalização e das listas e categorias de URLs sem a necessidade de intervenção manual pelo administrador, sem perda das conexões ativas e sem reinicialização do equipamento.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD40832 https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/790156/external-resources-for-web-filter	- -	"1) First check the geoip database current version: # diagnose autoupdate versions IP Geography DB" "External resources for web filter If the external resource is updated, FortiGate objects will update dynamically. External Resource are categorized into 4 types: URL list (Type=category) Domain Name List (Type=domain) IP Address list (Type=address) Malware hash list (Type=malware)"
4.3.1.6.	Deve possuir proteção contra ataques do tipo: IP Spoofing, Negação de Serviço (DoS e DDoS), SYN Flood Attack, ICMP Flood Attack e UDP Flood Attack, Buffer Overflow, Port Scanning, Man-id-the-Middle.	https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/117178/firewall-ipmacbinding-settinghttps://docs.fortinet.com/document/fortigate/6.0.0/handbook/626319/inside-fortios-denial-of-service-dos-protectionhttps://docs.fortinet.com/document/fortigate/6.0.0/handbook/372693/defending-against-dos-attackshttps://docs.fortinet.com/document/fortiweb/6.1.2/administration-guide/277489/http-https-protocol-constraintshttps://kb.fortinet.com/kb/documentLink.do?externalID=FD40206https://docs.fortinet.com/document/fortigate/6.0.0/handbook/745988/ssh-mitm-deep-inspection	-----	"Use this command to configure IP to MAC address binding settings. IP/MAC binding protects the FortiGate unit and/or the network from IP address spoofing attacks. IP spoofing attacks attempt to use the IP address of a trusted computer to connect to, or through, the FortiGate unit from a different computer...""FortiOS DoS and DDoS protection""Configuring the SYN threshold to prevent SYN floods""Use the udp_flood and icmp_flood thresholds to defend against these DoS attacks.""Use protocol constraints to prevent attacks such as buffer overflows.""Techncial Note: How to block NMAP Port Scanner""SSH MITM deep inspection"

4.3.1.7.	Deve identificar, decriptografar e analisar o tráfego SSL tanto em conexões de entrada (inbound) quanto de saída (outbound).	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/929997/ssl-inspection https://kb.fortinet.com/kb/documentLink.do?externalID=FD40937	- -	Deep inspection (also known as SSL/SSH inspection) is typically applied to outbound policies where destinations are unknown. Technical Note: Configuring Inbound SSL Deep Inspection
4.3.1.8.	Deve permitir a decriptografia da área útil do pacote de dados (payload) para fins de controle de acesso à Internet e proteção contra ameaças.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/122078/deep-inspection	-	When you use deep inspection, the FortiGate impersonates the recipient of the originating SSL session, then decrypts and inspects the content to find threats and block them. It then re-encrypts the content and sends it to the real recipient.
4.3.1.9.	Deve permitir a diferenciação de conexões pessoais (bancos, shopping etc) e conexões não pessoais por meio de classificação automática.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/122078/deep-inspection	-	Exempt web sites from deep inspection If you want to exempt all bank web sites, an easy way is to exempt the Finance and Banking category which includes all finance and bank web sites identified in FortiGuard.
4.3.1.10.	Deve possuir funcionalidade de backup/restore da configuração e das políticas de segurança.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/702257/configuration-backups	-	Backing up the configuration Restoring a configuration
4.3.1.11.	Deve armazenar os backups localmente, ou na solução de gerenciamento centralizado, e permitir que sejam transferidos para equipamentos externos por meio dos protocolos FTP ou SCP.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/702257/configuration-backups	-	You have the option to save the configuration file to various locations including the local PC, USB key, FTP, and TFTP server.
4.3.1.12.	Deve possuir a capacidade de identificar ataques de Advanced Persistent Threat (APT) e Zero-Day.	https://www.fortinet.com/br/resources/cyberglossary/advanced-persistent-threat https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ATP-Framework.pdf https://docs.fortinet.com/document/fortigate/6.0.0/handbook/817681/fortiguard	-	"...Fortinet integrates the intelligence of FortiGuard Labs into FortiGate next-generation firewalls..." As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGates. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats.

4.3.1.12.1.	Deve possuir a capacidade de emular um ambiente operacional isolado e seguro (Sandbox), na nuvem do fabricante, para execução e observação de código malicioso, sem a utilização de assinaturas, com base na atividade, como, por exemplo, operações de arquivo, alterações de registro e sistema etc.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/904357/using-fortisandbox-cloud-with-antivirus	-	FortiSandbox Cloud allows users to take advantage of FortiSandbox features without having to purchase, operate, and maintain a physical appliance. It works the same way as the physical FortiSandbox appliance.
4.3.1.12.2.	Deve suportar a análise no sistema operacional Windows.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf	4	▪ OS type supported: Windows 7, Windows 8.1, Windows 10, macOS, Linux, Android, and ICS systems
4.3.1.12.3.	Deve suportar a análise dos tipos de arquivos: documentos Microsoft Office, dll, exe, pdf, gzip, tar, zip.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf	4	✓ File type support: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .elf, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, .rl, .vbs,EBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
4.3.1.12.4.	Deve suportar a análise dos protocolos HTTP/HTTPS, FTP e SMTP.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	13	AV Inspected protocols and file types: - Support for HTTP, FTP, IMAP, POP3, SMTP, NNTP, MAPI, CIFS and SSH - Scan encrypted traffic with SSL inspection
4.3.2.	**Filtro de Pacotes**	-	-	-
4.3.2.1.	Não deve possuir restrições ao número de máquinas ou usuários protegidos.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf	12	*Não existe restrições para quantidade de máquinas e usuários protegidos.*
4.3.2.2.	Deve informar o número de sessões simultâneas.	https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/476970	-	Generate network traffic through the FortiGate, then go to FortiView > All Sessions and select the now view. A real time display of active sessions is shown.
4.3.2.3.	Deve suportar a implementação tanto em modo transparente (layer-2) quanto em modo gateway (layer-3).	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	FIREWALL Operating modes: NAT/route and transparent (bridge)

4.3.2.4.	Deve suportar Statefull Packet Inspection de tráfego IPv4 e IPv6.	http://docs.fortinet.com/document/fortigate/6.2.0/parallel-path-processing-life-of-a-packet/86811/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading https://kb.fortinet.com/kb/documentLink.do?externalID=FD30063	- -	Stateful inspection makes the decision to drop or allow a session and apply security features to it based on what is found in the first packet of the session. Then all subsequent packets in the same session are processed in the same way. FortiGate units are dual IP layer IPv6/IPv4 nodes. They support IPv6 over IPv4 tunneling, routing, firewall policies and IPSec VPN. You can assign both an IPv4 and an IPv6 address to any interface on a FortiGate unit - the interface functions as two interfaces, one for IPv4 addressed packets and another for IPv6 addressed packets.
4.3.2.5.	Deve suportar controle de acesso para pelo menos 80 serviços e protocolos pré-definidos.	4.3.2.5._87_Services.png	-	*91 Serviços protocolos pré-definidos*
4.3.2.6.	Deve suportar os protocolos H.323, SIP.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	12	Session helpers and ALGs: DCE/RPC, DNS-TCP, DNS-UDP, FTP, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)
4.3.2.7.	Deve implementar mecanismo de proteção contra ataques de falsificação de endereços IP (anti-spoofing).	https://docs.fortinet.com/document/fortigate/6.2.0/hardening-your-fortigate/995103/building-security-into-fortios	-	"FortiOS implements a mechanism called Reverse Path Forwarding (RPF), or Anti Spoofing..."
4.3.2.8.	Deve implementar mecanismo de captura de pacotes.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD45907	-	This article describes how to use the build in packet capture feature in FortiOS from the GUI interface.
4.3.2.9.	Deve identificar os usuários para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP.	https://docs.fortinet.com/document/ipsengine/3.6.0/custom-ips-and-application-control-signature-syntax-guide/677384/protocol-options	-	Protocol optionsUse these options to detect IP/ICMP/UDP/TCP protocol headers. The keyword protocol is highly recommended for all custom signatures.
4.3.2.10.	Deve suportar a utilização simultânea de políticas de segurança em IPv4 e IPv6.	https://docs.fortinet.com/document/fortigate/6.2.0/new-features/516182/combined-ipv4-and-ipv6-policy	-	In consolidated policy mode, there is a single policy table for the GUI. The same source interface, destination interface, service, user, and schedule are shared for both IPv4 and IPv6, while

				there are different IP addresses and IP pool settings.
4.3.2.11.	Deve suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período de tempo, e suas combinações.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies https://docs.fortinet.com/document/fortigate/6.0.0/handbook/736325/ip-netmask-addresses	- -	Firewall policy parameters - - When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number). It also registers the incoming interface, the outgoing interface it will need to use and the time of day. - Service The service or service chosen here represent the TCP/IP suite port numbers that will most commonly be used to transport the named protocols or group of protocols. - Source User(s) This parameter is based on a user identity that can be from a number of authentication authorities. It will be an account or group - Using this information the FortiGate firewall attempts to locate a security policy that matches the packet. If it finds a policy that matches the parameters it then looks at the action for that policy. If it is ACCEPT the traffic is allowed to proceed to the next step. If the Action is DENY or a match cannot be found the traffic is not allowed to proceed. - The FortiGate unit automatically converts CIDR formatted netmasks to dotted decimal format.
4.3.3.	**Filtro de Conteúdo**	-	-	-

4.3.3.1.	Deve prover o controle e proteção de acesso à Internet por meio do reconhecimento de aplicações, independente de porta e protocolo, e da classificação de URLs.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/756500/web-filtering https://docs.fortinet.com/document/fortigate/6.0.0/handbook/72943/application-control https://docs.fortinet.com/document/fortigate/6.0.0/handbook/849310/concepts	- -	NGFW mode simplifies applying application control and web filtering to traffic by allowing you to add applications and web filtering profiles directly to policies. This is used in conjunction with flow-based inspection. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols. Application control does not require knowledge of any server addresses or ports.
4.3.3.2.	Deve ser capaz de identificar aplicações, independentemente das portas e protocolos, bem como das técnicas de evasão utilizadas.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/72943/application-control https://docs.fortinet.com/document/fortigate/6.0.0/handbook/849310/concepts	- -	Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols. Application control does not require knowledge of any server addresses or ports.
4.3.3.3.	Deve ser capaz de identificar se as aplicações estão utilizando sua porta padrão.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	Port enforcement check: block applications detected on non-default ports
4.3.3.4.	Deve ser capaz de identificar aplicações encapsuladas dentro de protocolos, como HTTP e HTTPS.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control	-	Application control technologies detect and take action against network traffic based on the application that generated the traffic. Application control uses protocol decoders with signatures that analyze network traffic to detect application traffic, even if the traffic uses nonstandard ports or protocols.
4.3.3.5.	Deve ser capaz de identificar aplicações criptografadas usando SSL.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	6	Effectively examine SSL-encrypted traffic with various security controls, such as AV and content filtering

4.3.3.6.	Deve ser capaz de identificar um mínimo de 1.400 (mil e quatrocentas) aplicações, incluindo, mas não se limitando a: peer-to-peer, streaming e download de aúdio, streaming e download de vídeo, update de software, instant messaging, redes sociais, proxies, anonymizers, acesso e controle remoto, VOIP e email.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/849310/concepts https://docs.fortinet.com/document/fortigate/6.0.0/handbook/721617/configuring-profiles	- -	The FortiGate unit includes signatures for over 2,000 applications, services, and protocols. Under Categories, you may select from the following: Collaboration, Email, P2P, Proxy, Remote.Access, Social.Media, Update, Video/Audio, VoIP, Unknown Applications
4.3.3.7.	Deve ser capaz de identificar, no mínimo, as seguintes aplicações: Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Instagram, Twitter, Linkedin, Dropbox, Google Drive, One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR, Webex.	https://www.fortiguard.com/appcontrol	-	Pesquisar: "Bittorrent" "Youtube" "Livestream" "Skype" "Viber" "WhatsApp" "Snapchat" "Facebook" "Facebook Messenger" "Instagram" "Twitter" "Linkedin" "Dropbox" "Google Drive", One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR, Webex.
4.3.3.8.	Deve armazenar a base de assinaturas no próprio equipamento.	https://docs.fortinet.com/document/fortigate/6.0.0/fortinet-communication-ports-and-protocols/649403/fortiguard	-	The FortiGuard subscription update services include: AntiVirus (AV) Intrusion Protection Service (IPS) Application Control Anti-Spam Web Filtering
4.3.3.9.	Deve classificar as aplicações em categorias.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	APPLICATION CONTROL Detects thousands of applications in 18 categories
4.3.3.10.	Deve permitir o agrupamento de aplicações em grupos personalizados.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control	-	The application database is classified into 20 intuitive categories for ease of use. Administrators may also create specific application overrides that differ from the category settings.
4.3.3.11.	Deve identificar os usuários que estão utilizando as aplicações.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control	-	The FortiGate is able to operate in inline route and transparent mode. It can also operate in offline sniffer mode for passive monitoring of user activitie
4.3.3.12.	Deve permitir o bloqueio de aplicações que não estejam utilizando suas portas padrão.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	Port enforcement check: block applications detected on non-default ports

4.3.3.13.	Deve suportar a implementação de políticas de segurança baseadas em: aplicações,categorias de aplicações,endereço IP de origem ou destino,rede CIDR/VLSM de origem ou destino,usuário ou grupo de usuários,horário ou período de tempo,e suas combinações.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policieshttps://docs.fortinet.com/document/fortigate/6.0.0/handbook/736325/ip-netmask-addresses	-	- In addition to parameters like schedule and service, NGFW policies can filter by application or application category.- Source address(es) / Destination address(es)- "Schedule - The time frame that is applied to the policy..."- Source User(s) - This parameter is based on a user identity that can be from a number of authentication authorities. It will be an account or group- Using this information the FortiGate firewall attempts to locate a security policy that matches the packet. If it finds a policy that matches the parameters it then looks at the action for that policy. If it is ACCEPT the traffic is allowed to proceed to the next step. If the Action is DENY or a match cannot be found the traffic is not allowed to proceed.- The FortiGate unit automatically converts CIDR formatted netmasks to dotted decimal format.
4.3.3.14.	Deve permitir a utilização ou bloqueio individualizado das aplicações, como BitTorrent e Skype, para determinados usuários ou grupos de usuários.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies https://www.fortiguard.com/appcontrol	-	From the editing page for the New Application Group, choose a group type of Application and select individual applications for membership in the group. "...you can apply it to a policy in the Application field, by clicking on the + in the field... Pesquisar: "Bittorrent" " "Skype"
4.3.3.15.	Deve permitir registrar todos os fluxos autorizados/bloqueados das aplicações, incluindo o usuário identificado.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies	-	"There can also be a number of instructions associated with a FortiGate firewall in addition to the ACCEPT or DENY actions, some of which are optional. Instructions on how to process the traffic can also include such things as: - Logging Traffic..."

4.3.3.16.	Deve permitir o controle de uso de banda de download ou upload utilizada pelas aplicações (traffic shaping) baseado em: endereço IP ou rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/204835/configuring-application-control-traffic-shaping	-	Configuring application control traffic shaping Enable application control in a security policy – GUI Set the Incoming Interface Set the Outgoing Interface Set the Source Set the Schedule Creating a traffic shaping policy
4.3.3.17.	Deve ser capaz de efetuar a classificação de conteúdo de páginas web em HTTP e HTTPS, baseado em listas de categoria.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD31710 https://docs.fortinet.com/document/fortigate/6.4.1/administration-guide/833698/web-filter	- -	The FortiGate can perform both HTTP and HTTPS Web URL filtering, as well as HTTPS Fortiguard Web Filtering - FortiGuard Web Filtering service: provides many additional categories you can use to filter web traffic.
4.3.3.18.	Deve possuir funcionalidades de tratamento de conteúdo web, devendo sua base de dados conter, no mínimo, 10 (dez) milhões de sites internet web já registrados e classificados, distribuídos em, no mínimo, 60 (sessenta) categorias ou subcategorias pré-definidas ou suas semelhantes: conteúdo adulto, chat, drogas ilegais, jogos de azar, jogos, pirataria, proxy remoto, redes sociais, streaming media, violência, pornografia, racismo, malware.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf https://docs.fortinet.com/document/fortigate/6.0.0/handbook/120269/fortiguard-web-filtering	11	- Over 250 million URLs rated into 78 categories, in 70 languages Other Adult Materials; Web Chat; Drug Abuse; Games; Sports Hunting and War Games; Plagiarism; Proxy Avoidance; Streaming Media and Download; Explicit Violence; Discrimination; Malicious Websites;
4.3.3.19.	Deve permitir a inclusão de URLs customizadas por política (whitelist).	https://docs.fortinet.com/document/fortigate/6.4.1/administration-guide/615462/url-filter	-	ExemptThe traffic is allowed to bypass the remaining FortiGuard web filters, web content filters, web script filters, antivirus scanning, and DLP proxy operations

4.3.3.20.	Deve armazenar as listas de categoria no próprio equipamento.	https://docs.fortinet.com/document/fortigate/6.0.0/fortinet-communication-ports-and-protocols/649403/fortiguard	-	The FortiGuard subscription update services include: AntiVirus (AV) Intrusion Protection Service (IPS) Application Control Anti-Spam Web Filtering
4.3.3.21.	Deve identificar os usuários que estão acessando as páginas web.	https://docs.fortinet.com/document/fortigate/6.4.1/administration-guide/675558/fortiguard-filter	-	To view the log of a blocked website in the GUI: Go to Log & Report > Web Filter.
4.3.3.22.	Deve suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies https://docs.fortinet.com/document/fortigate/6.0.0/handbook/736325/ip-netmask-addresses https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/701862/blocking-facebook-with-web-filtering https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/546110/blocking-social-media-websites-using-fortiguard-categories#Blocking_social_media_websites_using_FortiGuard_categories	- - - -	- Source address(es) / Destination address(es) - "Schedule - The time frame that is applied to the policy..." - Source User(s) - This parameter is based on a user identity that can be from a number of authentication authorities. It will be an account or group - Using this information the FortiGate firewall attempts to locate a security policy that matches the packet. If it finds a policy that matches the parameters it then looks at the action for that policy. If it is ACCEPT the traffic is allowed to proceed to the next step. If the Action is DENY or a match cannot be found the traffic is not allowed to proceed. - The FortiGate unit automatically converts CIDR formatted netmasks to dotted decimal format. - 3. Creating the Web filtering security policy - Blocking social media websites using FortiGuard categories
4.3.3.23.	Deve alertar o usuário quando uma URL for bloqueada, por meio de página de bloqueio que possa ser customizada, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control	-	User education is central to an effective security implementation. In response to this, FortiOS lets you provide user notification when blocking an unauthorized application. The notification appears as an HTML block page for web-based applications.

4.3.3.24.	Deve permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado, informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para possibilitar o usuário continuar acessando o site).	https://docs.fortinet.com/document/fortigate/6.4.1/administration-guide/675558/fortiguard-filter	-	Sample configuration of issuing a warning This example shows issuing a warning when a user visits a website based on its category (rating), for example, information technology.
4.3.3.25.	Deve permitir registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado.	https://docs.fortinet.com/document/fortigate/6.4.1/administration-guide/615462/url-filter		To check web filter logs in the GUI: Go to Log & Report > Web Filter.
4.3.4.	**Prevenção de Intrusão (IPS)**	-	-	-
4.3.4.1.	Deve possuir tecnologia de detecção e prevenção de ataques e intrusões baseada em assinatura.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	IPS engine: 11,000+ up-to-date signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic pull or push signature update, threat encyclopedia integration
4.3.4.2.	Possuir, no mínimo, um conjunto de 2.000 (duas mil) assinaturas de detecção e prevenção de ataques.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	IPS engine: 11,000+ up-to-date signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic pull or push signature update, threat encyclopedia integration
4.3.4.3.	Detectar protocolos independentemente da porta utilizada, identificando aplicações conhecidas em portas não-padrão.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	944	The FortiGate Intrusion Prevention system uses protocol decoders to identify the abnormal traffic patterns that do notmeet the protocol requirements and standards. For example, the HTTP decoder monitors traffic to identify any HTTPpackets that do not meet the HTTP protocol standards. These decoders can detect their traffic on any port.

4.3.4.4.	Deve possuir, no mínimo, os seguintes mecanismos de detecção e prevenção: assinaturas de vulnerabilidades e exploits, assinaturas de ataques, validação de protocolos, detecção de anomalias, IP defragmentation, remontagem de pacotes TCP, nível de severidade do ataque.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	590, 934, 935, 938	Assinaturas de vulnerabilidades e exploits - Página 935 Signature-based defense is used against known attacks or vulnerability exploits. Assinaturas de ataques - Página 935 To view the complete list of signatures, go to Security Profiles > Intrusion Prevention, and select View IPS Signatures. This will include the predefined signatures and any custom signatures that you may have created. Validação de protocolos - Página 935 Before examining network traffic for attacks, the IPS engine uses protocol decoders to identify each protocol appearing in the traffic. Detecção de anomalias - Página 934 Anomaly-based defense is used when network traffic itself is used as a weapon. A host can be flooded with far more traffic than it can handle, making the host accessible. The most common example is the denial of service (DoS) attack, in

				which an attacker directs a large number of computers to attempt normal access of the target system. IP defragmentation e remontagem de pacotes TCP - Página 590 The FortiGate unit automatically reassembles fragmented packets before processing them because fragmented packets can evade security measures. This reassembly of packets affects TCP, UDP and IP packets. There can be some variation though in what process does the reassembling. The IPS engine, nTurbo and the kernel all can do defragmentation. Nível de Severidade - Página 938 Severity refers to the level of threat posed by the attack. The options include Critical, High, Medium, Low, and Info.
4.3.4.5.	Deve ser capaz de inspecionar tráfego criptografado usando SSL.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	11	Inspect SSL encrypted traffic option for IPS, application control, antivirus, web filtering, and DLP
4.3.4.6.	Deve ser capaz de inspecionar integralmente todos os pacotes de dados, independentemente de seus tamanhos.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	943	Starting with FortiOS 5.2, intelligent-mode is a new adaptive detection method. This command is enabled thedefault and it means that the IPS engine will perform adaptive scanning so that, for some traffic, the FortiGate canquickly finish scanning and offload the traffic to NPU or kernel. It is a balanced method which could cover all knownexploits. When disabled, the IPS engine scans every single byte

4.3.4.7.	Deve identificar os usuários relacionados aos eventos de intrusão.	https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/FortiGate_6_0/FortiOS%206.0.4%20Log%20Reference.pdf	907	16384 - LOGID_ATTCK_SIGNATURE_TCP_UDP. Ver tabela de logs
4.3.4.8.	Deve identificar os usuários relacionados aos eventos de bloqueio.	https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/FortiGate_6_0/FortiOS%206.0.4%20Log%20Reference.pdf	907	16384 - LOGID_ATTCK_SIGNATURE_TCP_UDP. Ver tabela de logs
4.3.4.9.	Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de um determinado ataque ou ameaça.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	939	Select Monitor to allow traffic to continue to its destination and log the activity. The log will appear under Log & Report but will only be visible in the GUI in the event of an intrusion.
4.3.4.10.	Deve permitir a criação de políticas de segurança que bloqueiem uma determinada ameaça.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	939	Select Block to drop traffic matching any the signatures included in the filter.
4.3.4.11.	Deve permitir a criação de políticas de segurança que bloqueiem um determinado ataque por meio de uma ação de DROP/RESET.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook		Select Reset to reset the session whenever the signature is triggered. In the CLI this action is referred to as Reject.
4.3.4.12.	Deve permitir registrar todos os eventos de IPS, incluindo o usuário identificado.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	945	Packet logging saves the network packets containing the traffic matching an IPS signature to the attack log. The FortiGate unit will save the logged packets to wherever the logs are configured to be stored, whether memory, internal hard drive, a FortiAnalyzer unit, or the FortiGuard Analysis and Management Service
4.3.4.13.	Deve identificar e bloquear a comunicação com botnets.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	939	You can set Botnet C&C protection to Block outgoing connections to Botnet sites or just record log messages (Monitor) when an outgoing Botnet connection attempt is detected.

4.3.4.14.	Deve bloquear malwares e spywares.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	854	Antivirus scanning examines files for viruses, worms, trojans, and other malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action. "Antivirus scanning examines files for viruses, worms, trojans, and other malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action"
4.3.4.15.	Deve inspecionar e bloquear vírus nos seguintes tipos de tráfego, no mínimo: HTTP, HTTPS e SMTP.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	854	This section describes how to configure the antivirus options. From an antivirus profile you can configure the FortiGateunit to apply antivirus protection to HTTP, FTP, IMAP, POP3, SMTP, and NNTP sessions. If your FortiGate unitsupports SSL/SSH content scanning and inspection, you can also configure antivirus protection for HTTPS, IMAPS,POP3S, SMTPS, and FTPS sessions.

4.3.4.16.	Deve inspecionar e bloquear vírus nos seguintes tipos de tráfego, no mínimo: HTTP, HTTPS e SMTP.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/842733/malware https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/788313/content-disarm-and-reconstruction-for-antivirus https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR1/fortigate-utm-40-mr1.pdf	- - 25	Worms, Spyware "Content Disarm and Reconstruction (CDR) allows the FortiGate to sanitize Microsoft documents and PDF (disarm) by removing active content such as hyperlinks, embedded media, javascript..." "Attackers encode HTML links using various formats to evade detection and bypass security measures. For example, the URL www.example.com/cgi.bin could be encoded in a number of ways to avoid detection but still work properly, and be interpreted the same, in a web browser. The FortiGate prevents the obfuscation by converting the URL to ASCII before inspection."
4.3.4.17.	Deve suportar a inspeção de vírus em arquivos comprimidos utilizando o algoritmo deflate (zip, gzip etc).	https://kb.fortinet.com/kb/documentLink.do?externalID=10187	-	FortiGate units support the following compression formats for antivirus checking: tar, gzip, rar, lzh, cab, arj, zip, bzip, bzip2, msc
4.3.4.18.	Deve suportar bloqueio de download de pelo menos 45 tipos de arquivos.	https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/610893/file-filter	-	File Filter allows the Web Filter profile to block files passing through a FortiGate based on file type.
4.3.4.19.	Deve armazenar as bases de assinaturas no próprio equipamento.	https://docs.fortinet.com/document/fortigate/6.0.0/fortinet-communication-ports-and-protocols/649403/fortiguard	-	The FortiGuard subscription update services include: AntiVirus (AV) Intrusion Protection Service (IPS) Application Control Anti-Spam Web Filtering
4.4.	**Firewall Tipo 1**	-	-	-
4.4.1.	Deve possuir o throughput mínimo de 6 Gbps com as funcionalidades de Filtro de Pacotes, IPS, Filtro de Conteúdo e Proteção contra Malwares habilitadas simultaneamente.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	Threat Protection Throughput 7 Gbps *Threat Protection performance is measured with Firewall, IPS, Application Control, and Malware Protection enabled.*

4.4.2.	Em relação ao filtro de pacotes, deve possuir o throughput mínimo de 13 Gbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) 36 / 36 / 27 Gbps
4.4.3.	Em relação ao túnel IPSec VPN, deve possuir o throughput mínimo de 10 Gbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	IPsec VPN Throughput (512 byte) 20 Gbps
4.4.4.	Em relação à inspeção SSL/TLS, deve possuir o throughput mínimo de 2 Gbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	SSL Inspection Throughput (IPS, avg. HTTPS) 8 Gbps
4.4.5.	Deve permitir, no mínimo, 7.500.000 de conexões simultâneas.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	Concurrent Sessions (TCP) 8 Million
4.4.6.	Deve permitir, no mínimo, 130.000 novas conexões por segundo.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	New Sessions/Second (TCP) 450,000
4.4.7.	Deve permitir, no mínimo, 512 VLANs.	https://docs.fortinet.com/max-value-table	-	system interface 8192
4.4.8.	Deve permitir, no mínimo, 80.000 usuários autenticados	Carta do Fabricante	-	*O FortiGate 600E permite 80.000 usuários autenticados*
4.4.9.	Deve permitir, no mínimo, 2.000 túneis VPN site-to-site simultâneos.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	Gateway-to-Gateway IPsec VPN Tunnels 2,000
4.4.10.	Deve permitir, no mínimo, 9.000 túneis VPN client-to-site simultâneos.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	Client-to-Gateway IPsec VPN Tunnels 50,000
4.4.11.	Deve suportar afixação em bastidor (rack) padrão EIA-310 com largura de 19’ (dezenove polegadas) e altura de até duas unidades de rack (2U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/186de9b7-1a21-11e9-9685-f8bc1258b856/FortiGate-600E-601E-Supplement.pdf	5 4	Form Factor (supports EIA / non-EIA standards) Rack Mount, 1 RU This device mounts in a standard 19 inch rack. (O FortiGate 600E está acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc))
4.4.12.	Deve possuir 2 (duas) fontes de alimentação independentes, redundantes e hot-swappable.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	Redundant Power Supplies (Hot Swappable) optional (Fonte Redundante Configurada)
4.4.13.	Deve possuir, no mínimo, 8 (oito) interfaces 1 (um) Gigabit-Ethernet padrão 1000Base-T, para conexão ao meio via cabo par trançado.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	GE RJ45 Interfaces: 8

4.4.14.	Deve possuir, no mínimo, 2 (duas) interfaces 10 (dez) Gigabit-Ethernet padrão SFP+, com transceivers SFP+ 10GB-SR, para conexão ao meio via cabo de fibra ótica.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	10 GE SFP+ Slots: 2 *O FortiGate 600E está configurado com 2 Transceivers 10GbE SFP+ SR*
4.4.15.	**Alta Disponibilidade**	-	-	-
4.4.15.1.	Deve operar em alta disponibilidade (HA) nativamente no equipamento, permitindo uma arquitetura ativo/ativo e ativo/passivo com no mínimo 2 (dois) membros, com sincronismo de estados integrado.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	High Availability Configurations Active-Active, Active-Passive, Clustering
4.4.15.2.	Deve suportar o balanceamento de carga interno na arquitetura ativo/ativo.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf	5	High Availability Configurations Active-Active, Active-Passive, Clustering
4.4.15.3.	Deve sincronizar sessões TCP/IP, tabelas NAT, tabelas FIB, associações de segurança das VPNs e todas as configurações necessárias para a manutenção da continuidade dos serviços.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/347538/fortigate-cluster-protocol-fgcp https://docs.fortinet.com/document/fortigate/6.0.0/handbook/20224/synchronizing-kernel-routing-tables https://docs.fortinet.com/document/fortigate/6.0.0/handbook/738546/device-failover	- - -	Also contributing to enhanced reliability is session failover protection for most IPv4 and IPv6 sessions including TCP, UDP, ICMP, IPsec VPN, and NAT sessions In a functioning cluster, the primary unit keeps all subordinate unit kernel routing tables (also called the forwarding information base FIB) up to date and synchronized with the primary unit. IPsec VPN SA synchronization synchronizes IPsec VPN security associations (SAs)
4.4.15.4.	Deve monitorar a falha dos links de comunicação.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook	366	Link failover means that if a monitored interface fails, the cluster reorganizes to reestablish a link to the network that the monitored interface was connected to and to continue operating with minimal or no disruption of network traffic. You configure monitored interfaces (also called interface monitoring or port monitoring) by selecting the interfaces to monitor as part of the

				cluster HA configuration. You can monitor up to 64 interfaces.
4.4.15.5.	Deve ser capaz de identificar e iniciar automaticamente um procedimento de failover sempre que ocorrer: a falha de um dos membros do cluster,a falha de qualquer componente ou processo crítico de um dos membros do cluster,a falha de um dos links de comunicação monitorados.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/223313/failover-protectionhttps://docs.fortinet.com/document/fortigate/6.0.0/handbook/320113/device-link-and-session-failover	--	The FGCP supports three kinds of failover protection. Device failover automatically replaces a failed device and restarts traffic flow with minimal impact on the network. Link failover maintains traffic flow if a link fails. Session failover resumes communication sessions with minimal loss of data if a device or link failover occurs.The FGCP provides transparent device and link failover. You can also enable session pickup to provide session failover. A failover can be caused by a hardware failure, a software failure, or something as simple as a network cable being disconnected causing a link failover.
4.4.15.6.	Deve ser capaz de realizar os procedimentos de failover sem perda das conexões ativas e sessões estabelecidas de forma transparente para o usuário.	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/284323/fortigate-session-life-support-protocol-fgsp	-	If one of the FortiGates fails, session failover occurs and active sessions fail over to the unit that is still operating. This failover occurs without any loss of data.
4.5.	**Firewall Tipo 2**	-	-	-
4.5.1.	Deve possuir o throughput mínimo de 700 Mbps com as funcionalidades de Filtro de Pacotes, IPS, Filtro de Conteúdo e Proteção contra Malwares habilitadas simultaneamente.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	Threat Protection Throughput 1 Gbps *Threat Protection performance is measured with Firewall, IPS, Application Control, and Malware Protection enabled.*
4.5.2.	Em relação ao filtro de pacotes, deve possuir o throughput mínimo de 5 Gbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	Firewall Throughput (1518 / 512 / 64 byte UDP packets) 20 / 18 / 10 Gbps

4.5.3.	Em relação ao túnel IPSec VPN, deve possuir o throughput mínimo de 1,5 Gbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	IPsec VPN Throughput (512 byte) 11.5 Gbps
4.5.4.	Em relação à inspeção SSL/TLS, deve possuir o throughput mínimo de 500 Mbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	SSL Inspection Throughput (IPS, avg. HTTPS) 1 Gbps
4.5.5.	Deve permitir, no mínimo, 1.500.000 de conexões simultâneas.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	Concurrent Sessions (TCP) 1.5 Million
4.5.6.	Deve permitir, no mínimo, 25.000 novas conexões por segundo.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	New Sessions/Second (TCP) 56,000
4.5.7.	Deve permitir, no mínimo, 200 VLANs.	https://docs.fortinet.com/max-value-table	-	system interface 4096
4.5.8.	Deve permitir, no mínimo, 100 túneis VPN site-to-site simultâneos.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	Gateway-to-Gateway IPsec VPN Tunnels 2,500
4.5.9.	Deve permitir, no mínimo, 100 túneis VPN client-to-site simultâneos.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	Client-to-Gateway IPsec VPN Tunnels 16,000
4.5.10.	Deve suportar a fixação em bastidor (rack) padrão EIA-310 com largura de 19’ (dezenove polegadas) e altura de uma unidade de rack (1U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/42d64717-83f1-11e9-81a4-00505692583a/FortiGate-100F-Series-QSG.pdf	5 10	Form Factor (supports EIA / non-EIA standards) Rack Mount, 1 RU Your FortiGate includes rack mount brackets and screws to mount in any 19 inch rack. (O FortiGate 100F está acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc))
4.5.11.	Deve possuir, no mínimo, 8 (oito) interfaces 1 (um) Gigabit-Ethernet padrão 1000Base-T, para conexão ao meio via cabo par trançado.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	5	GE RJ45 Ports: 12
4.6.	**Firewall Tipo 3**	-	-	-
4.6.1.	Deve possuir o throughput mínimo de 300 Mbps com as funcionalidades de Filtro de Pacotes, IPS, Filtro de Conteúdo e Proteção contra Malwares habilitadas simultaneamente.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	5	Threat Protection Throughput 700 Mbps *Threat Protection performance is measured with Firewall, IPS, Application Control, and Malware Protection enabled.*

4.6.2.	Em relação ao filtro de pacotes, deve possuir o throughput mínimo de 1,5 Gbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	5	Firewall Throughput (1518 / 512 / 64 byte UDP packets) 10/10/6 Gbps
4.6.3.	Em relação ao túnel IPSec VPN, deve possuir o throughput mínimo de 700 Mbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	5	IPsec VPN Throughput (512 byte) 6.5 Gbps
4.6.4.	Em relação à inspeção SSL/TLS, deve possuir o throughput mínimo de 250 Mbps.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	5	SSL Inspection Throughput (IPS, avg. HTTPS) 630 Mbps
4.6.5.	Deve permitir, no mínimo, 150.000 de conexões simultâneas.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	5	Concurrent Sessions (TCP) 700,000
4.6.6.	Deve permitir, no mínimo, 12.000 novas conexões por segundo.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	5	New Sessions/Second (TCP) 35,000
4.6.7.	Deve permitir, no mínimo, 50 VLANs.	https://docs.fortinet.com/max-value-table	-	system interface 256
4.6.8.	Deve permitir, no mínimo, 50 túneis VPN site-to-site simultâneos.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	5	Gateway-to-Gateway IPsec VPN Tunnels 200
4.6.9.	Deve permitir, no mínimo, 60 túneis VPN client-to-site simultâneos.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	5	Client-to-Gateway IPsec VPN Tunnels 500
4.6.10.	Deve possuir, no mínimo, 8 (oito) interfaces 1 (um) Gigabit-Ethernet padrão 1000Base-T, para conexão ao meio via cabo par trançado.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf	5	Interfaces: 10x GE RJ45
5	**Solução de Gerenciamento Centralizado (SGC)**	-	-	-
5.1.	Deve ser fornecida em appliance virtual, compatível VMware vSphere ESXi 6.0 ou superior, ou baseado em software, compatível com Windows Server 2012 R2 ou superior.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	4	FORTIMANAGER VIRTUAL APPLIANCES Hypervisor Support VMware ESX/ESXi 5.5/6.0/6.5/6.7/7.0
5.2.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows 7 ou superior ou no Linux.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	15	Connecting to the GUI The FortiManager unit can be configured and managed using the GUI or the CLI. This section will step you through connecting to the unit via the GUI. 3. On the management computer, start a supported web browse and browse to https://192.168.1.99.

5.3.	Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	4	*O FortiManager esta licenciado em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas (110 Equipamentos do tipo Firewall).*
5.4.	Deve estar licenciada e permitir a gerência centralizada de, no mínimo, 100 equipamentos que compõem a solução.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	4	FMG-VM-BASE Devices/VDOMs (Maximum): 10 + FMG-VM-100-UG Devices/VDOMs (Maximum): 100 +
5.5.	Deve estar licenciada para o limite máximo de usuários, objetos, regras de segurança, NAT e endereços IP suportados pela solução.	https://docs.fortinet.com/document/fortimanager/6.2.2/administration-guide/435148/license	-	License count rules for FortiManager VM, Cloud (Fortinet, Azure, or AWS), and Hardware: VDOM disabled: 1 FortiGate = 1 license. VDOM enabled: 1 VDOM = 1 license. VDOM enabled but no VDOMs: root = 1 license. FortiGate in HA mode: No license count for secondary FortiGate. *A Solução de Gerenciamento Centralizado (SGC) ofertada, FortiManager, está licenciada para todos os Firewalls (FortiGates) ofertados neste edital. Não existe licenciamento com limites para máximo de usuários, objetos, regras de segurança, NAT e endereços IP suportados pela solução.*
5.6.	As comunicações entre a SGC e os firewalls e entre a SGC e as estações dos administradores do sistema devem ser criptografadas e autenticadas.	https://kb.fortinet.com/kb/documentLink.do?externalID=FD40494https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	N/A 461516	set fgfm-ssl-protocol {sslv3 | tlsv1.0 | tlsv1.1 | tlsv1.2} #<-- for use with FGFM tunnel with FortiGateExample of adding a model device by pre-shared key3. On the management computer, start a supported web browser and browse to https://192.168.1.99.Configure administrator accounts using RADIUS, LDAP, TACACS+, or PKI

5.7.	Deve ser capaz de realizar todas as configurações nos firewalls descritas neste Termo de Referência.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	2	Central Management of Network Infrastructure Centrally manage FortiGate, FortiSwitch, FortiExtender & FortiAP.
5.8.	Deve possibilitar a aplicação de configurações em todos os firewalls, simultaneamente.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	2	Collectively configure the device settings - using the provisioning templates and advance CLI templates improves management of a large number of devices.
5.9.	Deve permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	27 2	FortiManager provides centralized policy-based provisioning and configuration management for FortiGate, FortiWiFi, FortiAP, and other devices FortiManager equips admins with granular device and role based administration for deploying zero-trust, multi-tenancy architecture to large enterprises, with a hierarchical objects database to facilitate re-use of common configurations and serve multiple customers.

5.10.	Deve suportar, por meio da interface gráfica de gerenciamento, a criação e administração de políticas de filtro de pacotes, prevenção de intrusão, controle de aplicação, filtragem de URLs, monitoração de logs, debugging, troubleshooting e captura de pacotes.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	2 628 674 138 222	**políticas de filtro de pacotes** Define global objects such as Firewall Objects, Policies and Security Profiles to share across multiple ADOMs FortiManager's new IPS admin is a restricted user role for performing only IPS related object configuration and install. **monitoração de logs,** FortiManager, coupled with the FortiAnalyzer family of centralized logging **controle de aplicação, filtragem de URLs e prevenção de intrusão** Restricted administrator accounts are used to delegate management of Web Filter, IPS, and Application Control profiles, **debugging,** CLI for management extensions You can use the CLI console to enable, disable, update, debug, and check the management extension. **troubleshooting** Troubleshooting Tips **e captura de pacotes.** Capture Packets Select to capture packets.
5.11.	Deve ser capaz de gerenciar os firewalls em unidades remotas, fora da rede local.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	1	*Ver Figura Página 1*
5.12.	Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou Active Directory.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	627	The FortiManager system supports authentication of administrators locally, remotely with RADIUS, LDAP, or TACACS+ servers, and using PKI.

5.13.	Será permitido que a solução de gerenciamento centralizado possua um “appliance virtual” específico para atendimento às necessidades de identificação e autenticação de usuários.	N/A	N/A	N/A
5.14.	Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	16	Configure the administrator profile to only allow read/write permission as required and restrict access using read only or no permission to settings which are not applicable to that administrator
5.15.	Deve permitir a criação de perfis customizados.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	625-626	To create a custom administrator profile:
5.16.	Deve permitir, de forma granular, assinalar permissões para os administradores criarem outros usuários, alterarem e ler configurações etc.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	625-626	To create a custom administrator profile:
5.17.	Deve permitir a delegação de funções de administração.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	610	Restricted administrator accounts are used to delegate management of Web Filter, IPS, and Application Control profiles, and then install those objects to their assigned ADOM.
5.18.	Deve permitir múltiplos administradores acessando o equipamento simultaneamente, sem restrição para leitura e escrita.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	568	Concurrent ADOM access is controlled by enabling or disabling the workspace function. Concurrent access is enabled by default. To prevent multiple administrators from making changes to the FortiManager database at the same time and causing conflicts, the workspace function must be enabled.

5.19.	Deve suportar o bloqueio de alterações, evitando o conflito de configurações entre diferentes administradores efetuando alterações simultaneamente.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	568	Concurrent ADOM access is controlled by enabling or disabling the workspace function. Concurrent access is enabled by default. To prevent multiple administrators from making changes to the FortiManager database at the same time and causing conflicts, the workspace function must be enabled.
5.20.	Deve registrar, em log de auditoria, as ações dos usuários administradores com o horário da alteração.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	580	The Event Log pane provides an audit log of actions made by users on FortiManager. It allows you to view log messages that are stored in memory or on the internal hard disk drive.
5.21.	Deve suportar a identificação e utilização de usuários nas políticas de segurança.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	221	IP policies The section describes how to create new IPv4 and IPv6 policies. 5. Enter the following information: - Source User - Source User Group
5.22.	Deve suportar agrupamento lógico de objetos ("object grouping") para criação de regras.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	248	Many objects now include the option to enable dynamic mapping. You can create new dynamic maps. When this feature is enabled, a table is displayed which lists the dynamic mapping information. You can also choose to add the object to groups, when available, and add tags.

5.23.	Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deve ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9644ee7-09ac-11eb-96b9-00505692583a/FortiManager-6.4.3-Administration_Guide.pdf	2512 5227 1273 2702 58	**Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede.** Managing objects and dynamic objects- Many objects now include the option to enable dynamic mapping. -Create a new object- Remove an object- Edit an object**Deve ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede.** Search objects - The search objects tool allows you to search objects based on keywordsFind unused objects - To find unused objects**Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas.**Map a dynamic device objectMap a dynamic device groupObjects from an ADOM can be promoted to the Global Database for reuse.
5.24.	Deve possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	227	To create a new Security Policy: 5. Enter the following information: Schedule: Select schedules, one time or recurring, and schedule groups.
5.25.	Deve garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e atualização remota, de maneira centralizada.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	35 e 36 493	Firmware management FortiManager can centrally manage firmware images and schedule managed devices for upgrade Device Firmware and Security Updates

5.26.	Deve ser capaz de testar a conectividade dos equipamentos gerenciados.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	73	Connection Summary Connectivity The device connectivity status and the time it was last checked. A green arrow means that the connection between the device and the FortiManager system is up; a red arrow means that the connection is down. Select Refresh to test the connection between the device and the FortiManager system
5.27.	Deve monitorar a performance e o estado dos links conectados.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	177 173	Monitor SD-WAN Health-Check Servers
5.28.	Deve suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	64	It is recommended to configure HA settings directly on FortiGate units. Another option is to run CLI scripts directly against FortiGate devices.
5.29.	Deve permitir localizar em quais regras um objeto está sendo utilizado.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9644ee7-09ac-11eb-96b9-00505692583a/FortiManager-6.4.3-Administration_Guide.pdf	271	On the Policy & Objects > Object Configuration pane, you can see whether an object is used in the Used column, and you can right-click on an object to find out where the object is used (Where Used) or to add the object to a group (Grouping).
5.30.	Deve permitir a identificação e exclusão de regras e objetos que estão aplicadas nos dispositivos, mas não afetam o desempenho e a segurança da rede (regras e objetos em desuso sob o ponto de vista lógico).	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9644ee7-09ac-11eb-96b9-00505692583a/FortiManager-6.4.3-Administration_Guide.pdf	210	Policy hit count When you run a policy check on a policy package or select the Find Unused Policies option from the Tools dropdown for a policy package, FortiManager shows hit count information for unused policies with zero hit count.

5.31.	Deve suportar a geração de alertas automáticos via SNMP e syslog.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/15ff1fbc-d112-11ea-8b7d-00505692583a/FortiManager-6.4.2-Administration_Guide.pdf	584 11	Enable the SNMP agent on the FortiManager device so it can send traps to and receive queries from the computer that is designated as its SNMP manager. This allows for monitoring the FortiManager with an SNMP manager. Log Settings Select Send Logs to FortiAnalyzer/FortiManager and/or Send Logs to Syslog.
5.32	Deve informar a utilização dos recursos de CPU, memória e atividade de rede dos equipamentos gerenciados.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9644ee7-09ac-11eb-96b9-00505692583a/FortiManager-6.4.3-Administration_Guide.pdf	75 181	Hardware Status The number of CPUs and the amount of RAM for the device. Map View To monitor SD-WAN with Map View: Bandwidth (TX/RX) Bandwidth of data transmitted and received. Volume (TX/RX) Volume of data transmitted and received.
5.33	Deve informar o número de conexões simultâneas dos equipamentos gerenciados.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a9644ee7-09ac-11eb-96b9-00505692583a/FortiManager-6.4.3-Administration_Guide.pdf	75	Current Administrators Displays the number of administrators configured on this device.
6.	**Solução de Gerenciamento de Logs**	-	-	-
6.1.	Deve ser fornecida em appliance virtual, compatível VMware vSphere ESXi 6.0 ou superior, ou baseado em software, compatível com Windows Server 2012 R2 ou superior, ou em appliance físico com suporte à fixação em bastidor (rack) padrão EIA-310 com largura de 19’ (dezenove polegadas) e altura de até duas unidades de rack (2U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	5	FORTIANALYZER 800F Fornecido em appliance físico com suporte à fixação em bastidor (rack) padrão EIA-310 com largura de 19’ (dezenove polegadas) e altura de uma unidade de rack (2U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc)

6.2.	Deve possuir relatórios de utilização dos recursos por aplicação, URLs, ameaças etc.	https://docs.fortinet.com/document/fortianalyzer/6.4.3/administration-guide	156, 157	FortiAnalyzer includes report templates you can use as is or build upon when you create a new report. FortiAnalyzer provide different templates for different devices. Application templates - Template - Application Risk and Control Security templates - Template - Threat Report Web templates - Template - Hourly Website Hits
6.3.	Deve possuir visualização sumarizada de todas as aplicações, ameaças e URLs que foram identificadas e controladas pela solução.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/3e37b5e2-0991-11eb-96b9-00505692583a/FortiAnalyzer-6.4.3-Administration_Guide.pdf	124123	FortiView allows you to use multiple filters in the consoles, enabling you to narrow your view to a specific time, by userID or local IP address, by application, and others. You can use it to investigate traffic activity such as useruploads/downloads or videos watched on YouTube on a network-wide user group or on an individual-user level.Displays the top applications used on the network including the application name, category, risk level, and sessions blocked and allowed. Bytes sent and received can also be enabled through the widget settings. Top Applications can be viewed as a stackbar, bar, table, or bubble chart. Displays the top allowed and blocked website domains on the network.
6.4.	Deve permitir a criação de relatórios customizados.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	1	provides customizable dashboards, reports and advanced workflow handlers for both Security & Network teams to accelerate workflows & assist with regulation and compliance audits.

6.5.	Deve ser capaz de receber logs de todos os firewalls especificados neste Termo.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	1 5	Scalable Log Management collects logs from FortiGate, FortiClient, FortiManager, FortiSandbox, FortiMail, FortiWeb, FortiAuthenticator, Generic syslog and others. FORTIANALYZER 800F GB/Day of Logs 300 Analytic Sustained Rate (logs/sec) 8,250 Collector Sustained Rate (logs/sec) 12,000 Devices/VDOMs (Maximum) 800 Max Number of Days Analytics 30
6.6.	Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/3e37b5e2-0991-11eb-96b9-00505692583a/FortiAnalyzer-6.4.3-Administration_Guide.pdf FAZ_6.6_Country.png	51 -	**aplicação, endereço IP de origem e destino, usuário e horário.** Viewing message details **país de origem e destino,** Destination Country: Source Country

6.7.	Deve possibilitar o registro dos fluxos de dados relativos a cada sessão, armazenando:- endereços IP de origem e destino dos pacotes, - traduções NAT, portas e protocolos de origem e destino, usuário identificado, ação sobre o pacote (permitido ou negado).	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/98087932-d021-11ea-8b7d-00505692583a/FortiAnalyzer-6.4.2-Administration_Guide.pdf	425155	Within a single FortiGate, the correlation is performed by grouping logs with the same session IDs, source and destination IP addresses, and source and destination portsNAT translation is also considered when searching sources and destinations in both traffic and UTM logs. The FortiGate will generate a special traffic log to indicate the NAT IP addresses to the FortiAnalyzer within the CSF.Viewing message detailsThe Action column displays a green checkmark Accept icon when both policy and UTM profile allow the traffic to pass through, that is, both the log field action and UTM profile action specify allow to this traffic.The Action column displays a red X Deny icon and the reason when either the log field action or UTM profile action deny the traffic.

6.8.	Deve possuir relatórios com informações consolidadas sobre: as mais frequentes fontes de conexões bloqueadas com seus destinos e serviços; os mais frequentes ataques e ameaças de segurança detectados com suas origens e destinos; os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de Internet; os usuários maiores consumidores de banda de Internet; e os sítios na Internet mais visitados.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/3e37b5e2-0991-11eb-96b9-00505692583a/FortiAnalyzer-6.4.3-Administration_Guide.pdf	156 157	**as mais frequentes fontes de conexões bloqueadas com seus destinos e serviços;** Template - Top Allowed and Blocked with Timestamps **os mais frequentes ataques e ameaças de segurança detectados com suas origens e destinos;** Template - Threat Report Template - Security Analysis **os serviços de rede mais utilizados,** Template - High Bandwidth Application Usage Report **as aplicações maiores consumidoras de banda de Internet;** Template - High Bandwidth Application Usage Report **os usuários maiores consumidores de banda de Internet;** Template - User Top 500 Websites by Bandwidth **e os sítios na Internet mais visitados.** Template - Top 20 Category and Websites (Bandwidth)
6.9.	Deve possuir funcionalidade de exportação de relatórios e logs para o computador local ou via FTP, SFTP ou SCP.	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/98087932-d021-11ea-8b7d-00505692583a/FortiAnalyzer-6.4.2-Administration_Guide.pdf	164	Output profiles allow you to define email addresses to which generated reports are sent and provide an option to upload the reports to FTP, SFTP, or SCP servers. Once created, an output profile can be specified for a report.
6.10.	Deve permitir a geração automática e agendada dos relatórios.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	2	Run reports on-demand or on a schedule with automated email notifications, uploads and an easy to manage calendar view.
6.11.	Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas.	-	-	*O Appliance FortiAnalyzer 800F está licenciado em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas.*

6.12.	Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõem a solução.	https://docs.fortinet.com/document/fortianalyzer/6.2.0/new-features/408516/utm-and-traffic-log-correlation-across-security-fabric	-	FortiAnalyzer correlates traffic logs to corresponding UTM logs so that it can report sessions/bandwidth together with its UTM threats. Within a single FortiGate, the correlation is performed by grouping logs with the same session IDs, source and destination IP addresses, and source and destination ports.
6.13.	Deve ser capaz de armazenar, no mínimo, 150 GB de logs diários.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	4	FORTIANALYZER 800F - GB/Day of Logs: 300
6.14.	Deve ser capaz de armazenar, no mínimo, 9 TB de logs em disco.	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf	4	FORTIANALYZER 800F- Storage Capacity: 16 TB (4 x 4 TB) | RAID Levels Supported: 0/1/5/10

você também está obrigado a usá-los, para prevenir acidentes e evitar as doenças profissionais.

Mostre ao seu novo companheiro os perigos que o cercam no trabalho.

Cada acidente é uma lição que deve ser apreciada, para evitar maiores desgraças.

Todo o acidente tem uma causa que é preciso ser pesquisada, para evitar a sua repetição.

Se você for acidentado, procure logo o socorro médico adequado. Não deixe que "entendidos" e "curiosos" concorram para o agravamento de sua lesão.

Se você não é eletricista, não se meta a fazer serviços de eletricidade.

Procure o socorro médico imediato, se você for vítima de um acidente, amanhã será tarde demais.

As máquinas não respeitam ninguém; mas você deve respeitá-las.

Atenda às recomendações dos Membros da CIPA e de seus mestres e chefes.

Conheça sempre as regras de segurança da seção onde você trabalha.

Conversa e discussão no trabalho predispõem a acidentes pela desatenção.

Leia e reflita sempre os ensinamentos contidos nos cartazes e avisos sobre prevenção de acidentes.

Os anéis, pulseiras, gravatas e mangas compridas não fazem parte do seu uniforme de trabalho.

Mantenha sempre as guardas protetoras das máquinas nos devidos lugares.

Para a máquina quando tiver que consertá-la ou lubrificá-la.

Habitue-se a trabalhar protegido contra os acidentes.

Use equipamentos de proteção adequados a seu serviço.

Conheça o manejo dos extintores e demais dispositivos de combate ao fogo existentes em seu local de trabalho. Você pode ter necessidade de usá-los algum dia.

MINISTÉRIO DO TRABALHO E EMPREGO

CARTEIRA DE TRABALHO E PREVIDÊNCIA SOCIAL

Número 86.939 Série 00074

Eden Jaime de Lima

ASSINATURA DO PORTADOR

8º TABELIONATO DE NOTAS DO RECIFE
Ivanildo de Figueiredo Andrade de Oliveira Filho
Tabelião Publico

www.tabelionatofigueiredo.com.br
Fone: (81) 3073-0800

Cópia autêntica conforme o original

Selo Digital 0073783 PBV10202006 03606

Emolumentos 4,33 TSNR 0,70 FERC 0,35 FERM 0,04
FUNSEG 0,08 ISS 0,18 Total R$ 4,51
Recife, 28/10/2020

AUGUSTO JOSE MALTA RIBEIRO SUPERVISOR NOTARIAL

Consulte Autenticidade em: www.tjpe.jus.br/selodigital

Digitalizado com CamScanner

QUALIFICAÇÃO CIVIL

Nome Eder Jairo de Lima

Loc. Nasc. Recife Est. PE Data 15/12/84

Filiação Edinalva Batista de Lima

Doc. Nº CNN 64 628 2 280 254

ESTRANGEIROS

Chegada ao Brasil em ..... / ..... / ..... Doc. Ident. Nº .....

Exp. em ..... / ..... / ..... Estado .....

Obs.: .....

Data Emissão 17/04/02 DRT PE

Assinatura do Funcionário

Sandra

ALTERAÇÕES DE IDENTIDADE

(Com relação nome, est. civil e data nasc.)

Nome .....

Doc. .....

Nome .....

Doc. .....

Nome .....

Doc. .....

Est. Civil .....

Doc. .....

Est. Civil .....

Doc. .....

Nascimento .....

Doc. .....

8º TABELIONATO DE NOTAS DO RECIFE
Ivanildo de Figueiredo Andrade de Oliveira Filho
Tabelião Público

www.tabelionatofigueiredo.com.br
Fone: (81) 3073-0800

Cópia autêntica conforme o original

Selo Digital 0073783 KYY10202006.03605

Emolumentos 4,33 TSNR 0,70 FERC 0,35 FERM 0,04
FUNSEG 0,08 ISS 0,18 Total R$ 4,51
Recife, 28/10/2020

AUGUSTO JOSE MALTA RIBEIRO SUPERVISOR NOTARIAL

Consulte Autenticidade em: www.tjpe.jus.br/selodigital

Digitalizado com CamScanner

CONTRATO DE TRABALHO

Empregador: SUPRISERVI COM REPRES E SERVICOS LTDA
CNPJ/CPF/CEI: 12.707.105/0001-64
Endereço: RUA GAL GOES MONTEIRO 308, IMBIRIBEIRA

Municipio: RECIFE UF: PE
Esp. do estabelecimento:

Cargo: ANALISTA DE SUPORTE
CBO N°: 212420
Data de admissão: 02 de Janeiro de 2018
Registro N°: 587 Fls./Ficha: 587
Remuneração especificada: R$ 5.500,00 (cinco mil e quinhentos reais) por mês.

SUPRISERVI COM. REPR. E SERVIC. LTDA
Emerson Silva
Ass. do empregador ou a rogo c/test.
Ger. Adm. Financeiro CPF: 794.717.814-34

1° ..... 2° .....

Data saída ..... de ..... de .....

.....

Ass. do empregador ou a rogo c/test.

1° ..... 2° .....

Com. Dispensa CD N° .....

8° TABELIONATO DE NOTAS DO RECIFE
Ivanildo de Figueiredo Andrade de Oliveira Filho
Tabelião Público
www.tabelionatofigueiredo.com.br
Fone: (81) 3073-0800

Cópia autêntica conforme o original

Selo Digital 0073783 KXB10202006.03604

Emolumentos 4,33 TSNR 0,70 FERC 0,35 FERM 0,04 FUNSEG 0,08 ISS 0,18 Total R$ 4,51
Recife, 28/10/2020

AUGUSTO JOSE MALTA RIBEIRO SUPERVISOR NOTARIAL

Consulte Autenticidade em www.tjpe.jus.br/selodigital

Digitalizado com CamScanner

Data: 28 de outubro de 2020

Cliente: TRIBUNAL DE JUSTIÇA DO ESTADO DA PARAÍBA
LICITAÇÃO Nº 019/2020
PROCESSO ADMINISTRATIVO ELETRÔNICO: 2020012776

Por meio desta carta, informamos que o equipamento FortiGate modelo FG-600E permite o número de 80.000 usuários autenticados.

Atenciosamente,
Fortinet, Inc.

Digitally signed by ALEXANDRE OLIVEIRA BONATTI:07311140609
Date: 2020.10.29 10:35:01 -03'00'

Alexandre Bonatti
Director, Systems Engineering – Brasil

Observe que, não obstante qualquer disposição em contrário: (1) as obrigações da Fortinet relacionadas a especificações, licenças, suporte, assinaturas, certificações, garantias e quaisquer outras garantias do produto são: (a) inválidas para produtos que foram adulterados ou modificados por terceiros e (b) sujeita em todos os aspectos aos processos, políticas e termos padrão da Fortinet, que a Fortinet pode mudar a qualquer momento a seu exclusivo e absoluto critério; (2) A Fortinet se reserva o direito de modificar planos técnicos, roadmaps e datas de liberação a qualquer momento a exclusivo e absoluto critério da Fortinet. (3) A Fortinet se isenta de responsabilidade por erros de digitação, tradução ou impressão. (4) Este documento é para fins informativos e não se destina a criar obrigações contratuais pela Fortinet ou comprometimento promissório ou direito de confiar nas declarações. (5) Declarações aqui sobre o desempenho do produto e características podem ser contextuais, por exemplo, baseadas em testes em em um ambiente particular, como em um ambiente de laboratório, e pode não ser preciso em todos os contextos, como em um ambiente em produção. (6) O signatário deste documento está baseando todas as declarações aqui em seus conhecimentos no momento da assinatura sem qualquer obrigação para investigar as declarações, e pode confiar totalmente na revisão e informações de outros. (7) Produtos e serviços não são oferecidos gratuitamente e os direitos só são concedidos sujeitos a pagamento integral à Fortinet e seus distribuidores e revendedores, todas as vendas são finais e aplicam-se as políticas e termos e condições da Fortinet, como o EULA padrão da Fortinet e os termos de suporte, alguns dos quais estão localizados em https://www.fortinet.com/corporate/about-us/legal.html .(8) A Fortinet não tem nenhuma obrigação de atualizar e não pretende atualizar as declarações aqui contidas, mesmo que, por exemplo, o signatário descubra que as declarações são de fato falsas ou que os planos mudaram.

```
--
-- MODULE-IDENTITY
--  OrgName
--     Fortinet Technologies, Inc.
--  ContactInfo
--     Technical Support
--     e-mail: support@fortinet.com
--     http://www.fortinet.com
--

FORTINET-FORTIGATE-MIB DEFINITIONS ::= BEGIN

IMPORTS
    FnBoolState, FnIndex, fnAdminEntry, fnSysSerial, fortinet
        FROM FORTINET-CORE-MIB
    ifEntry, ifName, ifIndex
        FROM IF-MIB
    InetAddress, InetAddressPrefixLength, InetAddressType, InetPortNumber
        FROM INET-ADDRESS-MIB
    MODULE-COMPLIANCE, NOTIFICATION-GROUP, OBJECT-GROUP
        FROM SNMPv2-CONF
    sysName
        FROM SNMPv2-MIB
    Counter32, Counter64, Gauge32, Unsigned32, Integer32, IpAddress,
    MODULE-IDENTITY, NOTIFICATION-TYPE, OBJECT-TYPE, TimeTicks, OBJECT-IDENTITY
        FROM SNMPv2-SMI
    Ipv6Address
        FROM IPV6-TC
    CounterBasedGauge64
        FROM HCNUM-TC
    DisplayString, TEXTUAL-CONVENTION, AutonomousType, DateAndTime, PhysAddress, TimeStamp
        FROM SNMPv2-TC;

fnFortiGateMib MODULE-IDENTITY
    LAST-UPDATED "201910280000Z"
    ORGANIZATION
        "Fortinet Technologies, Inc."
    CONTACT-INFO
        "
         Technical Support
         email: support@fortinet.com
         http://www.fortinet.com"
    DESCRIPTION
        "MIB module for Fortinet FortiGate devices."
    REVISION    "201910280000Z"
    DESCRIPTION
        "Added fgDpdkEngs in fnFortiGateMib.fgSystem."
    REVISION    "201905310000Z"
    DESCRIPTION
        "Added ingress shaping OIDs in fgIntfBcs"
    REVISION    "201905270000Z"
    DESCRIPTION
        "Added fgConfig."
    REVISION    "201901240000Z"
    DESCRIPTION
        "Added fgSysNeedLogPartitionScan to indicate whether a disk scan is needed."
    REVISION    "201812120000Z"
    DESCRIPTION
        "Added fgLog OIDs for global log device statistics."
    REVISION    "201806110000Z"
    DESCRIPTION
        "Added OIDs for fnbam stats info."
    REVISION    "201806060000Z"
    DESCRIPTION
```

```
        "Added DNS Proxy stats info OIDs."
    REVISION    "201804060000Z"
    DESCRIPTION
        "Added fgIntfBcs OIDs for a interface"
    REVISION    "201801180000Z"
    DESCRIPTION
        "Revert fgAvOversizedDetected and fgAvOversizedBlocked OIDs numbers."
    REVISION    "201801100000Z"
    DESCRIPTION
        "Added fgFwGtp OIDs."
    REVISION    "201711160000Z"
    DESCRIPTION
        "Added fgSlaProbeClient OIDs for server probe feature."
    REVISION    "201710180000Z"
    DESCRIPTION
        "Added NPU counters in fgNPU."
    REVISION    "201710030000Z"
    DESCRIPTION
        "Added fgIntfEntEstUpBandwidth and fgIntfEntEstDownBandwidth in fgIntfTable."
    REVISION    "201709070000Z"
    DESCRIPTION
        "Added fgDisks in fnFortiGateMib.fgSystem, and created fgWebCacheDiskFailure
        and fgWanOptDiskFailure in fnFortiGateMib.fgSystem.fgDisks."
    REVISION    "201708300000Z"
    DESCRIPTION
        "Added fgVWLHealthCheckLink OIDs for virtual-wan-link health-check per member
link."
    REVISION    "201708250000Z"
    DESCRIPTION
        "Added per-CPU high trap."
    REVISION    "201707210000Z"
    DESCRIPTION
        "Added fgServerLoadBalanceRealServerAddress6 in
fgTrapServerLoadBalanceRealServerDown."
    REVISION    "201707120000Z"
    DESCRIPTION
        "Added fgInternalLTEModemsInfo under fnFortiGateMib, Added Modem, SIM card, Signal
Info,
        Traffic Info, Data Session Info OIDs."
    REVISION    "201704280000Z"
    DESCRIPTION
        "Added fgAvSMBVirusDetected and fgAvSMBVirusBlocked OIDs."
    REVISION    "201704050000Z"
    DESCRIPTION
        "Added fgAvMAPIVirusDetected and fgAvMAPIVirusBlocked OIDs."
    REVISION    "201701160000Z"
    DESCRIPTION
        "Added extended database version OIDs for AV and IPS."
    REVISION    "201609150000Z"
    DESCRIPTION
        "Added fgFwIppools OIDs."
    REVISION    "201606170000Z"
    DESCRIPTION
        "Various non-monotonically increase Counter32 values have been changed to
Gauge32."
    REVISION    "201504230000Z"
    DESCRIPTION
        "Added fgProcessorFnNP6 in fgProcessorTypes."
    REVISION    "201503160000Z"
    DESCRIPTION
         "Added fgDevice OIDs"
    REVISION    "201501100000Z"
    DESCRIPTION
         "Added fgIntfVlanHbs OIDs for vlan interface heartbeat feature"
    REVISION    "201412040000Z"
```

```
DESCRIPTION
     "Added fgLinkMonitor OIDs for link-monitor feature"
REVISION    "201406040000Z"
DESCRIPTION
     "Added fgUsbModemInfoObjects OIDs for LTE Modem"
REVISION    "201402130000Z"
DESCRIPTION
     "Added fgUsbports OIDs for external USB ports"
REVISION    "201308120000Z"
DESCRIPTION
     "Added fgIntfVrrps OIDs for VRRP"
REVISION    "201307260000Z"
DESCRIPTION
     "Added fgServerLoadBalance OIDs."
REVISION    "201304120000Z"
DESCRIPTION
     "Added fgTrapIpsFailOpen OID in fgTraps"
REVISION    "201304060000Z"
DESCRIPTION
    "Added fgWc wireless controller OIDs"
REVISION    "201211290000Z"
DESCRIPTION
    "Added fgVpnTrapPhase1Name OID in VPN traps"
REVISION    "201207100000Z"
DESCRIPTION
    "Added OID for 64-bit sysUpTime"
REVISION    "201205160000Z"
DESCRIPTION
    "Added OID for a virtual domain's HA cluster member state."
REVISION    "201202060000Z"
DESCRIPTION
    "Added OIDs for advanced system info and NP4/NP2 processors."
REVISION    "201109120000Z"
DESCRIPTION
    "Added OIDs for IPv6 statistics."
REVISION    "201101100000Z"
DESCRIPTION
    "Added OIDs for session setup rates and VPN tunnel stats"
REVISION    "200911030000Z"
DESCRIPTION
    "Added OIDs for Proxy information, CPU and low-memory usage"
REVISION    "200910010000Z"
DESCRIPTION
    "Added new FortiGate models."
REVISION    "200907070000Z"
DESCRIPTION
    "Added fgTrapFazDisconnect."
REVISION    "200811030000Z"
DESCRIPTION
    "Added fgVdTpTable. Re-ordered MIB tree to improve readability.
     Replaced indexes for tables that had a dependent relationship
     with another table."
REVISION    "200809020000Z"
DESCRIPTION
    "Added OIDs for compatibility with FORTIOS-300-MIB."
REVISION    "200808190000Z"
DESCRIPTION
    "Conformance statements."
REVISION    "200806160000Z"
DESCRIPTION
    "Spelling corrections."
REVISION    "200804140000Z"
DESCRIPTION
    "Initial version of FORTINET-FORTIGATE-MIB."
::= { fortinet 101 }
```

```
FgVdIndex ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS      current
    DESCRIPTION
        "data type for virtual-domain indexes"
    SYNTAX      Integer32 (1..2147483647)

FgOpMode ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "enumerated type for device operation modes"
    SYNTAX      INTEGER { nat(1), transparent(2) }

FgHaMode ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "enumerated type for HA cluster modes"
    SYNTAX      INTEGER { standalone(1), activeActive(2),
                    activePassive(3) }

FgHaState ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "enumerated type for HA cluster member state"
    SYNTAX      INTEGER { master(1), backup(2), standalone(3) }

FgHaLBSchedule ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "enumerated type for HA load-balancing schedules"
    SYNTAX      INTEGER { none(1), hub(2), leastConnections(3),
                    roundRobin(4), weightedRoundRobin(5), random(6),
                    ipBased(7), ipPortBased(8) }

FgAdminPermLevel ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "enumerated type for administrative permissions"
    SYNTAX      INTEGER { readAdmin(0), writeAdmin(1), domainAdmin(15),
                    superAdmin(255) }

FgFwUserAuthType ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "enumerated type for user authentication types"
    SYNTAX      INTEGER { local(1), radiusSingle(2), radiusMultiple(3),
                    ldap(4) }

FgSessProto ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "data type for session protocols"
    SYNTAX      INTEGER { ip(0), icmp(1), igmp(2), ipip(4), tcp(6),
                    egp(8), pup(12), udp(17), idp(22), ipv6(41),
                    rsvp(46), gre(47), esp(50), ah(51), ospf(89),
                    pim(103), comp(108), raw(255) }

FgP2PProto ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "data type for session protocols"
    SYNTAX      INTEGER { bitTorrent(0), eDonkey(1), gnutella(2),
                    kaZaa(3), skype(4), winNY(5) }
```

```
FgScanAvDisposition ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Scan AV Disposition for detected anomalies"
    SYNTAX      INTEGER { detected(1), blocked(2) }

FgWanOptProtocols ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "WAN optimization protocol types"
    SYNTAX      INTEGER { http(1), mapi(2), cifs(3),
                    ftp(4), tcp(5) }

FgWanOptHistPeriods ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "WAN optimization history statistics time period types"
    SYNTAX      INTEGER { last10Min(1), lastHour(2), lastDay(3),
                    lastMonth(4) }

FgHaStatsSyncStatusType ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Current HA Sync status types"
    SYNTAX      INTEGER { unsynchronized(0), synchronized(1) }

FgWcWlanSecurityType ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "enumerated type for WLAN security methods"
    SYNTAX      INTEGER {
                  other(0),
                  open(1),
                  captivePortal(2),
                  wep64(3),
                  wep128(4),
                  wpaOnlyPersonal(5),
                  wpaOnlyEnterprise(6),
                  wpa2OnlyPersonal(7),
                  wpa2OnlyEnterprise(8),
                  wpaPersonal(9),
                  wpaEnterprise(10),
                  wpaOnlyPersonalCaptivePortal(11),
                  wpa2OnlyPersonalCaptivePortal(12),
                  wpaPersonalCaptivePortal(13),
                  wpa3Sae(14),
                  wpa3SaeTransition(15),
                  wpa3Enterprise(16),
                  wpa3Owe(17),
                  osen(18)  }

FgWcWlanAuthenticationType ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "enumerated type for WLAN authentication methods"
    SYNTAX      INTEGER {
                  other(0),
                  psk(1),
                  radiusServer(2),
                  userGroup(3) }

FgWcWlanEncryptionType ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
```

```
        "enumerated type for WLAN encryption methods"
    SYNTAX      INTEGER {
                  other(0),
                  none(1),
                  tkip(2),
                  aes(3),
                  tkipAes(4) }

FgWcWtpRadioId ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS      current
    DESCRIPTION
        "unique identifier of a radio on a WTP"
    SYNTAX      Unsigned32 (1..31)

FgWcWtpRadioType ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Enumerated types for WTP radio.
         The following enumerated values are supported:
           other(0)             - radio type is unknown
           dot11a(1)            - 802.11a radio
           dot11b(2)            - 802.11b radio
           dot11g(3)            - 802.11g/b radio
           dot11n5g(4)          - 802.11n/a radio at 5GHz band
           dot11n2g(5)          - 802.11n/g/b radio at 2.4GHz band
           dot11ac(6)           - 802.11ac/n/a radio
           dot11ngOnly(7)       - 802.11n/g radio at 2.4GHz band
           dot11gOnly(8)        - 802.11g radio
           dot11n2GHzOnly(9)    - 802.11n radio at 2.4GHz band
           dot11n5GHzOnly(10)   - 802.11n radio at 5GHz band
           dot11acnOnly(11)     - 802.11ac/n radio
           dot11acOnly(12)      - 802.11ac radio"
    SYNTAX      INTEGER {
                  other(0),
                  dot11a(1),
                  dot11b(2),
                  dot11g(3),
                  dot11n5g(4),
                  dot11n2g(5),
                  dot11ac(6),
                  dot11ngOnly(7),
                  dot11gOnly(8),
                  dot11n2GHzOnly(9),
                  dot11n5GHzOnly(10),
                  dot11acnOnly(11),
                  dot11acOnly(12) }

FgWcWtpChannelWidthType ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "enumerated type for WTP radio channel width"
    SYNTAX      INTEGER {
                  other(0),
                  width20MHz(1),
                  width40MHz(2),
                  width80MHz(3) }

FgWcWtpRadioBandType ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "enumerated type for WTP radio band"
    SYNTAX      INTEGER {
                  other(0),
                  band2GHz(1),
```

```
                band5GHz(2) }

FgWcWtpRadioChannelNumber ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS      current
    DESCRIPTION
        "channel number of a WTP radio"
    SYNTAX      Integer32 (0..200)

FgWcWtpRadioMode ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Represents the operating mode of the WTP radio.
         The following enumerated values are supported:
           other(0)        - The radio mode is unknown.
           notExist(1)     - The radio does not physically exist.
           disabled(2)     - The radio is administratively disabled.
           ap(3)           - The radio is configured as an access point.
           monitor(4)      - The radio is configured as a dedicated rogue AP scanner.
           sniffer(5)      - The radio is configured as a wireless sniffer."
    SYNTAX      INTEGER {
                  other(0),
                  notExist(1),
                  disabled(2),
                  ap(3),
                  monitor(4),
                  sniffer(5) }

FgWcCountryString ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "3a"
    STATUS      current
    DESCRIPTION
        "This attribute identifies the country or non-country
         entity in which the station is operating. If it is a
         country, the first two octets of this
         string is the two character country code as described
         in document ISO/IEC 3166-1. The third octet shall
         be one of the following:
         1. an ASCII space character, if the regulations under
         which the station is operating encompass all
         environments in the country,
         2. an ASCII 'O' character, if the regulations under
         which the station is operating are for an Outdoor
         environment only, or
         3. an ASCII 'I' character, if the regulations under
         which the station is operating are for an Indoor
         environment only.
         4. an ASCII 'X' character, if the station is operating
         under a non-country entity. The first two octets of the
         non-country entity shall be two ASCII 'XX' characters."
    SYNTAX      OCTET STRING (SIZE(3))

--
-- fortinet.fnFortiGateMib.fgModel
--

fgModel OBJECT IDENTIFIER ::= { fnFortiGateMib 1 }

-- fgModel start

-- fgModel end

--
-- fortinet.fnFortiGateMib.fgTraps
--
```

```
fgTraps OBJECT IDENTIFIER
    ::= { fnFortiGateMib 2 }

fgTrapPrefix OBJECT IDENTIFIER
    ::= { fgTraps 0 }

--
-- fortinet.fnFortiGateMib.fgVirtualDomain
--

fgVirtualDomain OBJECT IDENTIFIER
    ::= { fnFortiGateMib 3 }

--
-- fortinet.fnFortiGateMib.fgVirtualDomain.fgVdInfo
--

fgVdInfo OBJECT IDENTIFIER
    ::= { fgVirtualDomain 1 }

fgVdNumber OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of virtual domains in vdTable"
    ::= { fgVdInfo 1 }

fgVdMaxVdoms OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The maximum number of virtual domains allowed on the device as allowed by
hardware and/or licensing"
    ::= { fgVdInfo 2 }

fgVdEnabled OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Whether virtual domains are enabled on this device"
    ::= { fgVdInfo 3 }

--
-- fortinet.fnFortiGateMib.fgVirtualDomain.fgVdTables
--

fgVdTables OBJECT IDENTIFIER
    ::= { fgVirtualDomain 2 }

--
-- fortinet.fnFortiGateMib.fgVirtualDomain.fgVdTables.fgVdTable
--

fgVdTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgVdEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of virtual domains configured on the device"
    ::= { fgVdTables 1 }
```

```
fgVdEntry OBJECT-TYPE
    SYNTAX      FgVdEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information applicable
         to a particular virtual domain"
    INDEX       { fgVdEntIndex }
    ::= { fgVdTable 1 }

FgVdEntry ::= SEQUENCE {
    fgVdEntIndex    FgVdIndex,
    fgVdEntName     DisplayString,
    fgVdEntOpMode   FgOpMode,
    fgVdEntHaState  FgHaState,
    fgVdEntCpuUsage Gauge32,
    fgVdEntMemUsage Gauge32,
    fgVdEntSesCount Gauge32,
    fgVdEntSesRate  Gauge32
}

fgVdEntIndex OBJECT-TYPE
    SYNTAX      FgVdIndex
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Internal virtual domain index used to uniquely identify rows in this table. This
index is also used by other tables referencing a virtual domain."
    ::= { fgVdEntry 1 }

fgVdEntName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The name of the virtual domain"
    ::= { fgVdEntry 2 }

fgVdEntOpMode OBJECT-TYPE
    SYNTAX      FgOpMode
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Operation mode of the virtual domain (NAT or Transparent)"
    ::= { fgVdEntry 3 }

fgVdEntHaState OBJECT-TYPE
    SYNTAX      FgHaState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "HA cluster member state of the virtual domain on this device
         (master, backup or standalone)"
    ::= { fgVdEntry 4 }

fgVdEntCpuUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "CPU usage of the virtual domain (percentage)."
    ::= { fgVdEntry 5 }

fgVdEntMemUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
```

```
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Memory usage of the virtual domain (percentage)."
    ::= { fgVdEntry 6 }

fgVdEntSesCount OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of active sessions on the virtual domain."
    ::= { fgVdEntry 7 }

fgVdEntSesRate OBJECT-TYPE
    SYNTAX      Gauge32
    UNITS       "Sessions Per Second"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The session setup rate on the virtual domain."
    ::= { fgVdEntry 8 }

--
-- fortinet.fnFortiGateMib.fgVirtualDomain.fgVdTables.fgVdTpTable
--

fgVdTpTable OBJECT-TYPE
    SYNTAX SEQUENCE OF FgVdTpEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "A table of virtual domains in transparent operation mode.  This table has a
         sparse dependent relationship with fgVdTable."
    ::= { fgVdTables 2 }

fgVdTpEntry OBJECT-TYPE
    SYNTAX FgVdTpEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "An entry containing information applicable
         to a particular virtual domain in transparent mode"
    INDEX { fgVdEntIndex }
    ::= { fgVdTpTable 1 }

FgVdTpEntry ::= SEQUENCE {
    fgVdTpMgmtAddrType InetAddressType,
    fgVdTpMgmtAddr InetAddress,
    fgVdTpMgmtMask InetAddressPrefixLength
}

fgVdTpMgmtAddrType OBJECT-TYPE
    SYNTAX InetAddressType
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The type of address stored in fgVdTpMgmtAddr, in compliance with INET-ADDRESS-
MIB"
    ::= { fgVdTpEntry 1 }

fgVdTpMgmtAddr OBJECT-TYPE
    SYNTAX InetAddress
    MAX-ACCESS read-only
    STATUS current
```

```
    DESCRIPTION
        "The management IP address of the virtual domain in transparent mode,
         typically an IPv4 address. The address type/format is determined by
fgVdTpMgmtAddrType."
    ::= { fgVdTpEntry 2 }

fgVdTpMgmtMask OBJECT-TYPE
    SYNTAX InetAddressPrefixLength
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The address prefix length (or network mask) applied to the fgVdTpMgmtAddr"
    ::= { fgVdTpEntry 3 }

--
-- fortinet.fnFortiGateMib.fgSystem
--

fgSystem OBJECT IDENTIFIER
    ::= { fnFortiGateMib 4 }

--
-- fortinet.fnFortiGateMib.fgSystem.fgSystemInfo
--

fgSystemInfo OBJECT IDENTIFIER
    ::= { fgSystem 1 }

fgSysVersion OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..128))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Firmware version of the device"
    ::= { fgSystemInfo 1 }

fgSysMgmtVdom OBJECT-TYPE
    SYNTAX      FgVdIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Index that identifies the management virtual domain. This index corresponds to
the index used by fgVdTable."
    ::= { fgSystemInfo 2 }

fgSysCpuUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current CPU usage (percentage)"
    ::= { fgSystemInfo 3 }

fgSysMemUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current memory utilization (percentage)"
    ::= { fgSystemInfo 4 }

fgSysMemCapacity OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
        "Total physical memory (RAM) installed (KB)"
    ::= { fgSystemInfo 5 }

fgSysDiskUsage OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current hard disk usage (MB), if disk is present"
    ::= { fgSystemInfo 6 }

fgSysDiskCapacity OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Total hard disk capacity (MB), if disk is present"
    ::= { fgSystemInfo 7 }

fgSysSesCount OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of active sessions on the device"
    ::= { fgSystemInfo 8 }

fgSysLowMemUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current lowmem utilization (percentage). Lowmem is memory available
         for the kernel's own data structures and kernel specific tables. The
         system can get into a bad state if it runs out of lowmem."
    ::= { fgSystemInfo 9 }

fgSysLowMemCapacity OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Total lowmem capacity (KB). See fgSysLowMemUsage for the description
         of lowmem."
    ::= { fgSystemInfo 10 }

fgSysSesRate1 OBJECT-TYPE
    SYNTAX      Gauge32
    UNITS       "Sessions Per Second"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The average session setup rate over the past minute."
    ::= { fgSystemInfo 11 }

fgSysSesRate10 OBJECT-TYPE
    SYNTAX      Gauge32
    UNITS       "Sessions Per Second"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The average session setup rate over the past 10 minutes."
    ::= { fgSystemInfo 12 }
```

```
fgSysSesRate30 OBJECT-TYPE
    SYNTAX      Gauge32
    UNITS       "Sessions Per Second"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The average session setup rate over the past 30 minutes."
    ::= { fgSystemInfo 13 }

fgSysSesRate60 OBJECT-TYPE
    SYNTAX      Gauge32
    UNITS       "Sessions Per Second"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The average session setup rate over the past 60 minutes."
    ::= { fgSystemInfo 14 }

fgSysSes6Count OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of active ipv6 sessions on the device"
    ::= { fgSystemInfo 15 }

fgSysSes6Rate1 OBJECT-TYPE
    SYNTAX      Gauge32
    UNITS       "Sessions Per Second"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The average ipv6 session setup rate over the past minute."
    ::= { fgSystemInfo 16 }

fgSysSes6Rate10 OBJECT-TYPE
    SYNTAX      Gauge32
    UNITS       "Sessions Per Second"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The average ipv6 session setup rate over the past 10 minutes."
    ::= { fgSystemInfo 17 }

fgSysSes6Rate30 OBJECT-TYPE
    SYNTAX      Gauge32
    UNITS       "Sessions Per Second"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The average ipv6 session setup rate over the past 30 minutes."
    ::= { fgSystemInfo 18 }

fgSysSes6Rate60 OBJECT-TYPE
    SYNTAX      Gauge32
    UNITS       "Sessions Per Second"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The average ipv6 session setup rate over the past 60 minutes."
    ::= { fgSystemInfo 19 }

fgSysUpTime OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "hundredths of a second"
```

```
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The 64bit time (in hundredths of a second) since the network management portion
of the system was last re-initialized."
    ::= { fgSystemInfo 20 }

fgSysNeedLogPartitionScan OBJECT-TYPE
    SYNTAX      FnBoolState
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Whether the log partition needs a scan."
        ::= { fgSystemInfo 21 }

--
-- fortinet.fnFortiGateMib.fgSystem.fgSoftware
--

fgSoftware OBJECT IDENTIFIER
    ::= { fgSystem 2 }

fgSysVersionAv OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..128))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Virus signature database version installed on the device"
    ::= { fgSoftware 1 }

fgSysVersionIps OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..128))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "IPS signature database version installed on the device"
    ::= { fgSoftware 2 }

fgSysVersionAvEt OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..128))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Virus signature extended database version installed on the device"
    ::= { fgSoftware 3 }

fgSysVersionIpsEt OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..128))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "IPS signature extended database version installed on the device"
    ::= { fgSoftware 4 }

--
-- fortinet.fnFortiGateMib.fgSystem.fgHwSensors
--

fgHwSensors OBJECT IDENTIFIER
    ::= { fgSystem 3 }

fgHwSensorCount OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
        "The number of entries in fgHwSensorTable"
    ::= { fgHwSensors 1 }

fgHwSensorTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgHwSensorEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A list of device specific hardware sensors and values. Because different devices
have different hardware sensor capabilities, this table may or may not contain any
values."
    ::= { fgHwSensors 2 }

fgHwSensorEntry OBJECT-TYPE
    SYNTAX      FgHwSensorEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing the name, value, and alarm status of a given hardware sensor"
    INDEX       { fgHwSensorEntIndex }
    ::= { fgHwSensorTable 1 }

FgHwSensorEntry ::= SEQUENCE {
    fgHwSensorEntIndex          FnIndex,
    fgHwSensorEntName           DisplayString,
    fgHwSensorEntValue          DisplayString,
    fgHwSensorEntAlarmStatus    INTEGER
}

fgHwSensorEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A unique identifier within the fgHwSensorTable"
    ::= { fgHwSensorEntry 1 }

fgHwSensorEntName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "A string identifying the sensor by name"
    ::= { fgHwSensorEntry 2 }

fgHwSensorEntValue OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "A string representation of the value of the sensor. Because sensors can present
data in different formats, string representation is most general format. Interpretation of
the value (units of measure, for example) is dependent on the individual sensor."
    ::= { fgHwSensorEntry 3 }

fgHwSensorEntAlarmStatus OBJECT-TYPE
    SYNTAX      INTEGER { false(0), true(1) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "If the sensor has an alarm threshold and has exceeded it, this will indicate its
status. Not all sensors have alarms."
    ::= { fgHwSensorEntry 4 }
```

```
--
-- fortinet.fnFortiGateMib.fgSystem.fgProcessors
--

fgProcessors OBJECT IDENTIFIER
    ::= { fgSystem 4 }

fgProcessorCount OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of entries in fgProcessorTable"
    ::= { fgProcessors 1 }

fgProcessorTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgProcessorEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table that lists information for each processor"
    ::= { fgProcessors 2 }

fgProcessorEntry OBJECT-TYPE
    SYNTAX      FgProcessorEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information for a particular processor"
    INDEX       { fgProcessorEntIndex }
    ::= { fgProcessorTable 1 }

FgProcessorEntry ::= SEQUENCE {
    fgProcessorEntIndex    FnIndex,
    fgProcessorUsage       Gauge32,
    fgProcessorUsage5sec   Gauge32,
    fgProcessorType        AutonomousType,
    fgProcessorContainedIn FnIndex,
    fgProcessorPktRxCount  Counter64,
    fgProcessorPktTxCount  Counter64,
    fgProcessorPktDroppedCount Counter64,
    fgProcessorUserUsage   Gauge32,
    fgProcessorSysUsage    Gauge32
}

fgProcessorEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A unique identifier within the fgProcessorTable"
    ::= { fgProcessorEntry 1 }

fgProcessorUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    UNITS       "%"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The processor's CPU usage (percentage), which is an average
        calculated over the last minute.
        (only valid for processors types that support this statistic)."
    ::= { fgProcessorEntry 2 }

fgProcessorUsage5sec OBJECT-TYPE
```

```
        SYNTAX      Gauge32 (0..100)
        UNITS       "%"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The processor's CPU usage (percentage), which is an average
            calculated over the last 5 sec.
            (only valid for processors types that support this statistic)."
        ::= { fgProcessorEntry 3 }

    fgProcessorType OBJECT-TYPE
        SYNTAX      AutonomousType
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "An indication of the type of the processor.
            Types are defined in fgProcessorTypes."
        ::= { fgProcessorEntry 4 }

    fgProcessorContainedIn OBJECT-TYPE
        SYNTAX      FnIndex
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The index to the processor module entry in the fgProcessorModuleTable
            that contains this processor."
        ::= { fgProcessorEntry 5 }

    fgProcessorPktRxCount OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The total number of packets received by this processor
             (only valid for processors types that support this statistic)."
        ::= { fgProcessorEntry 6 }

    fgProcessorPktTxCount OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The total number of packets transmitted by this processor
             (only valid for processors types that support this statistic)."
        ::= { fgProcessorEntry 7 }

    fgProcessorPktDroppedCount OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The total number of packets dropped by this processor
             (only valid for processors types that support this statistic)."
        ::= { fgProcessorEntry 8 }

    fgProcessorUserUsage OBJECT-TYPE
        SYNTAX      Gauge32 (0..100)
        UNITS       "%"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The processor's CPU user space usage, which is an average
             calculated over the last minute.
             (only valid for processors types that support this statistic)."
        ::= { fgProcessorEntry 9 }
```

```
fgProcessorSysUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    UNITS       "%"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The processor's CPU system space usage, which is an average
         calculated over the last minute.
         (only valid for processors types that support this statistic)."
    ::= { fgProcessorEntry 10 }

--
-- Registrations for processor types, for use with fgProcessorType
--
fgProcessorTypes OBJECT IDENTIFIER
    ::= { fgProcessors 3 }

fgProcessorOther OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor type identifier used when no other defined
        type is appropriate."
    ::= { fgProcessorTypes 1 }

fgProcessorIntel OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor type identifier used for Intel CPU."
    ::= { fgProcessorTypes 2 }

fgProcessorAMD OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor type identifier used for AMD CPU."
    ::= { fgProcessorTypes 3 }

fgProcessorXlr OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor type identifier used for RMI XLR processor."
    ::= { fgProcessorTypes 4 }

fgProcessorFnSoc OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor type identifier used for Fortinet FortiSoc processor."
    ::= { fgProcessorTypes 5 }

fgProcessorFnNP2 OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor type identifier used for Fortinet NP2 security processor."
    ::= { fgProcessorTypes 6 }

fgProcessorFnNP4 OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor type identifier used for Fortinet NP4 security processor."
    ::= { fgProcessorTypes 7 }

fgProcessorFnNP6 OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor type identifier used for Fortinet NP6 security processor."
```

```
    ::= { fgProcessorTypes 8 }

--
-- fortinet.fnFortiGateMib.fgSystem.fgProcessors.fgProcessorsTrapObjects
--

fgProcessorsTrapObjects OBJECT IDENTIFIER
    ::= { fgProcessors 4 }

fgPerCpuHighDetails OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "CPUs index string that the CPU usage has exceeded the configured threshold."
    ::= { fgProcessorsTrapObjects 1 }

--
-- fortinet.fnFortiGateMib.fgSystem.fgProcessorModules
--

fgProcessorModules OBJECT IDENTIFIER
    ::= { fgSystem 5 }

--
-- Registrations for processor module types, for use with fgProcModType
--
fgProcessorModuleTypes OBJECT IDENTIFIER
    ::= { fgProcessorModules 1 }

fgProcModOther OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor module type identifier used when no other defined
        type is appropriate."
    ::= { fgProcessorModuleTypes 1 }

fgProcModIntegrated OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor module type identifier used for the main CPUs
        built in the device."
    ::= { fgProcessorModuleTypes 2 }

fgProcModFnXE2 OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor module type identifier used for
        Fortinet AMC module ADM-XE2."
    ::= { fgProcessorModuleTypes 3 }

fgProcModFnCE4 OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor module type identifier used for
        Fortinet AMC module ASM-CE4."
    ::= { fgProcessorModuleTypes 4 }

fgProcModFnFE8 OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor module type identifier used for
        Fortinet AMC module ADM-FE8."
    ::= { fgProcessorModuleTypes 5 }
```

```
fgProcModFnXG2 OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor module type identifier used for
        Fortinet FMC module FMC-XG2."
    ::= { fgProcessorModuleTypes 6 }

fgProcModIntegratedNPU OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor module type identifier used for the NPU(s)
        built in the device."
    ::= { fgProcessorModuleTypes 7 }

fgProcModFnXD2 OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor module type identifier used for
        Fortinet FMC module FMC-XD2."
    ::= { fgProcessorModuleTypes 8 }

fgProcModFnF20 OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor module type identifier used for
        Fortinet FMC module FMC-F20."
    ::= { fgProcessorModuleTypes 9 }

fgProcModFnC20 OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor module type identifier used for
        Fortinet FMC module FMC-C20."
    ::= { fgProcessorModuleTypes 10 }

fgProcModFnXD4 OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor module type identifier used for
        Fortinet AMC module ADM-XD4."
    ::= { fgProcessorModuleTypes 11 }

fgProcModFnFB4 OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor module type identifier used for
        Fortinet AMC module ASM-FB4."
    ::= { fgProcessorModuleTypes 12 }

fgProcModFnFB8 OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor module type identifier used for
        Fortinet AMC module ADM-FB8."
    ::= { fgProcessorModuleTypes 13 }

fgProcModFnXB2 OBJECT-IDENTITY
    STATUS current
    DESCRIPTION
        "The processor module type identifier used for
        Fortinet AMC module ADM-XB2."
    ::= { fgProcessorModuleTypes 14 }

fgProcessorModuleCount OBJECT-TYPE
    SYNTAX      Integer32
```

```
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of entries in fgProcessorModuleTable"
    ::= { fgProcessorModules 2 }

fgProcessorModuleTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgProcessorModuleEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table that lists information for each processor module"
    ::= { fgProcessorModules 3 }

fgProcessorModuleEntry OBJECT-TYPE
    SYNTAX      FgProcessorModuleEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information for a particular processor module"
    INDEX       { fgProcModIndex }
    ::= { fgProcessorModuleTable 1 }


FgProcessorModuleEntry ::= SEQUENCE {
    fgProcModIndex          FnIndex,
    fgProcModType           AutonomousType,
    fgProcModName           DisplayString,
    fgProcModDescr          DisplayString,
    fgProcModProcessorCount Integer32,
    fgProcModMemCapacity    Gauge32,
    fgProcModMemUsage       Gauge32,
    fgProcModSessionCount   Gauge32,
    fgProcModSACount        Gauge32
}

fgProcModIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A unique identifier within the fgProcessorModuleTable"
    ::= { fgProcessorModuleEntry 1 }

fgProcModType OBJECT-TYPE
    SYNTAX     AutonomousType
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "An indication of the type of the processor module.
        Types are defined in fgProcessorModuleTypes."
    ::= { fgProcessorModuleEntry 2 }

fgProcModName OBJECT-TYPE
    SYNTAX     DisplayString (SIZE (0..32))
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "A textual name of this processor module."
    ::= { fgProcessorModuleEntry 3 }

fgProcModDescr OBJECT-TYPE
    SYNTAX     DisplayString (SIZE (0..64))
    MAX-ACCESS read-only
    STATUS     current
```

```
    DESCRIPTION
        "A textual description of this processor module."
    ::= { fgProcessorModuleEntry 4 }

fgProcModProcessorCount OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Total number of processors contained by this module."
    ::= { fgProcessorModuleEntry 5}

fgProcModMemCapacity OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Total physical memory (RAM) installed (KB) on this processor module."
    ::= { fgProcessorModuleEntry 6 }

fgProcModMemUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current memory utilization (percentage) on this processor module."
    ::= { fgProcessorModuleEntry 7 }

fgProcModSessionCount OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of active sessions on this processor module
         (only valid for processors types that support this statistic)."
    ::= { fgProcessorModuleEntry 8}

fgProcModSACount OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of IPsec Security Associations on this processor module
         (only valid for processors types that support this statistic)."
    ::= { fgProcessorModuleEntry 9}

--
-- fortinet.fnFortiGateMib.fgSystem.fgSystemInfoAdvanced
--

fgSystemInfoAdvanced OBJECT IDENTIFIER
    ::= { fgSystem 6 }

--
-- fortinet.fnFortiGateMib.fgSystem.fgSystemInfoAdvanced.fgSysInfoAdvMem
--

fgSysInfoAdvMem OBJECT IDENTIFIER
    ::= { fgSystemInfoAdvanced 1 }

fgSIAdvMemPageCache OBJECT-TYPE
    SYNTAX      Gauge32
    UNITS       "KB"
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
        "The amount of physical RAM used as cache memory for files read from
         the disk (the page cache)."
    ::= { fgSysInfoAdvMem 1 }

fgSIAdvMemCacheActive OBJECT-TYPE
    SYNTAX      Gauge32
    UNITS       "KB"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The toal amount of buffer or page cache memory that are active.
         This part of the memory is used recently and usually not reclaimed
         unless absolutely necessary."
    ::= { fgSysInfoAdvMem 2 }

fgSIAdvMemCacheInactive OBJECT-TYPE
    SYNTAX      Gauge32
    UNITS       "KB"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total amount of buffer or page cache memory that are free and
         available. This is memory that has not been recently used and can be
         reclaimed for other purposes by the paging algorithm."
    ::= { fgSysInfoAdvMem 3 }

fgSIAdvMemBuffer OBJECT-TYPE
    SYNTAX      Gauge32
    UNITS       "KB"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The amount of physical RAM used for filesystem buffers."
    ::= { fgSysInfoAdvMem 4 }

fgSIAdvMemEnterKerConsThrsh OBJECT-TYPE
    SYNTAX      Gauge32
    UNITS       "KB"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current memory threshold level to enter kernel conserve mode."
    ::= { fgSysInfoAdvMem 5 }

fgSIAdvMemLeaveKerConsThrsh OBJECT-TYPE
    SYNTAX      Gauge32
    UNITS       "KB"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current memory threshold level to leave kernel conserve mode."
    ::= { fgSysInfoAdvMem 6 }

fgSIAdvMemEnterProxyConsThrsh OBJECT-TYPE
    SYNTAX      Gauge32
    UNITS       "KB"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current memory threshold level to enter proxy conserve mode."
    ::= { fgSysInfoAdvMem 7 }

fgSIAdvMemLeaveProxyConsThrsh OBJECT-TYPE
    SYNTAX      Gauge32
```

```
    UNITS       "KB"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current memory threshold level to leave proxy conserve mode."
    ::= { fgSysInfoAdvMem 8 }

--
-- fortinet.fnFortiGateMib.fgSystem.fgSystemInfoAdvanced.fgSysInfoAdvSessions
--

fgSysInfoAdvSessions OBJECT IDENTIFIER
    ::= { fgSystemInfoAdvanced 2 }

fgSIAdvSesEphemeralCount OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The current number of ephemeral sessions on the device."
    ::= { fgSysInfoAdvSessions 1 }

fgSIAdvSesEphemeralLimit OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The limit number of allowed ephemeral sessions on the device."
    ::= { fgSysInfoAdvSessions 2 }

fgSIAdvSesClashCount OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of new sessions which have collision with existing sessions.
         This generally highlights a shortage of ports or IP in ip-pool during
         source natting (PNAT)."
    ::= { fgSysInfoAdvSessions 3 }

fgSIAdvSesExpCount OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of current expectation sessions."
    ::= { fgSysInfoAdvSessions 4 }

fgSIAdvSesSyncQFCount OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The sync queue full counter, reflecting bursts on the sync queue."
    ::= { fgSysInfoAdvSessions 5 }

fgSIAdvSesAcceptQFCount OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The accept queue full counter, reflecting bursts on the accept queue."
    ::= { fgSysInfoAdvSessions 6 }

fgSIAdvSesNoListenerCount OBJECT-TYPE
```

```
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of direct requests to Fortigate local stack from external,
         reflecting DOS attack towards the Fortigate."
    ::= { fgSysInfoAdvSessions 7 }

--
-- fortinet.fnFortiGateMib.fgSystem.fgUsbports
--

fgUsbports OBJECT IDENTIFIER
    ::= { fgSystem 7 }

fgUsbportCount OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of entries in fgUsbportTable."
    ::= { fgUsbports 1 }

fgUsbportTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgUsbportEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table that lists information for each external USB port."
    ::= { fgUsbports 2 }

fgUsbportEntry OBJECT-TYPE
    SYNTAX      FgUsbportEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information for a particular USB port."
    INDEX       { fgUsbportEntIndex }
    ::= { fgUsbportTable 1 }

FgUsbportEntry ::= SEQUENCE {
    fgUsbportEntIndex      FnIndex,
    fgUsbportPlugged       INTEGER,
    fgUsbportVersion       DisplayString,
    fgUsbportClass         INTEGER,
    fgUsbportVendId        OCTET STRING,
    fgUsbportProdId        OCTET STRING,
    fgUsbportRevision      DisplayString,
    fgUsbportManufacturer  DisplayString,
    fgUsbportProduct       DisplayString,
    fgUsbportSerial        DisplayString
}

fgUsbportEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A unique identifier within the fgUsbportTable."
    ::= { fgUsbportEntry 1 }

fgUsbportPlugged OBJECT-TYPE
    SYNTAX      INTEGER { unplugged(0), plugged(1) }
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
        "The USB port's plugged status."
    ::= { fgUsbportEntry 2 }

fgUsbportVersion OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The USB port's version."
    ::= { fgUsbportEntry 3 }

fgUsbportClass OBJECT-TYPE
    SYNTAX      INTEGER { ifc(0), audio(1), comm(2), hid(3), physical(5),
                  image(6), printer(7), storage(8), hub(9), cdcData(10),
                  chipSmartCard(11), contentSecurity(13), appSpec(254), vendorSpec(255)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The device class."
    ::= { fgUsbportEntry 4 }

fgUsbportVendId OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The Vendor ID of the device."
    ::= { fgUsbportEntry 5 }

fgUsbportProdId OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The Product ID of the device."
    ::= { fgUsbportEntry 6 }

fgUsbportRevision OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The release number of the device."
    ::= { fgUsbportEntry 7 }

fgUsbportManufacturer OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The manufacturer of the device."
    ::= { fgUsbportEntry 8 }

fgUsbportProduct OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The product of the device."
    ::= { fgUsbportEntry 9 }

fgUsbportSerial OBJECT-TYPE
    SYNTAX      DisplayString
```

```
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The serial number of the device."
    ::= { fgUsbportEntry 10 }

--
-- fortinet.fnFortiGateMib.fgSystem.fgLinkMonitor
--
fgLinkMonitor OBJECT IDENTIFIER
    ::= { fgSystem 8 }

fgLinkMonitorNumber OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of link monitor in fgLinkMonitorTable"
    ::= { fgLinkMonitor 1 }

fgLinkMonitorTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgLinkMonitorEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Link Monitor statistics table.  This table has a dependent expansion relationship
with fgVdTable.
         Only virtual domains with enabled link monitor are present in this table."
    ::= { fgLinkMonitor 2 }

fgLinkMonitorEntry OBJECT-TYPE
    SYNTAX      FgLinkMonitorEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Link Monitor statistics on a virtual domain"
    INDEX       {fgLinkMonitorID}
    ::= { fgLinkMonitorTable 1 }

FgLinkMonitorEntry ::= SEQUENCE {
    fgLinkMonitorID         FnIndex,
    fgLinkMonitorName       DisplayString,
    fgLinkMonitorState      INTEGER,
    fgLinkMonitorLatency    DisplayString,
    fgLinkMonitorJitter     DisplayString,
    fgLinkMonitorPacketSend Counter64,
    fgLinkMonitorPacketRecv Counter64,
    fgLinkMonitorPacketLoss DisplayString,
    fgLinkMonitorVdom       DisplayString,
    fgLinkMonitorBandwidthIn  Counter32,
    fgLinkMonitorBandwidthOut Counter32,
    fgLinkMonitorBandwidthBi  Counter32,
    fgLinkMonitorOutofSeq   Counter64
}

fgLinkMonitorID OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Link Monitor ID. Only enabled link monitor entries are present in this table.
Link Monitor IDs are only unique within a virtual domain."
    ::= { fgLinkMonitorEntry 1 }

fgLinkMonitorName OBJECT-TYPE
```

```
        SYNTAX      DisplayString
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Link Monitor name."
        ::= { fgLinkMonitorEntry 2 }

    fgLinkMonitorState OBJECT-TYPE
        SYNTAX      INTEGER { alive(0), dead(1) }
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Link Monitor state."
        ::= { fgLinkMonitorEntry 3 }

    fgLinkMonitorLatency OBJECT-TYPE
        SYNTAX      DisplayString
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The average latency of link monitor in float number within last 30 probes."
        ::= { fgLinkMonitorEntry 4 }

    fgLinkMonitorJitter OBJECT-TYPE
        SYNTAX      DisplayString
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The average jitter of link monitor in float number within last 30 probes."
        ::= { fgLinkMonitorEntry 5 }

    fgLinkMonitorPacketSend OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The total number of packets sent by link monitor."
        ::= { fgLinkMonitorEntry 6 }

    fgLinkMonitorPacketRecv OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The total number of packets received by link monitor."
        ::= { fgLinkMonitorEntry 7 }

    fgLinkMonitorPacketLoss OBJECT-TYPE
        SYNTAX      DisplayString
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The average packet loss percentage in float number within last 30 probes."
        ::= { fgLinkMonitorEntry 8 }

    fgLinkMonitorVdom OBJECT-TYPE
        SYNTAX      DisplayString
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Virtual domain the link monitor entry exists in. This name corresponds to the
    fgVdEntName used in fgVdTable."
        ::= { fgLinkMonitorEntry 9 }

    fgLinkMonitorBandwidthIn OBJECT-TYPE
```

```
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The available bandwidth in Mbps of incoming traffic detected by a link monitor on
its interface."
    ::= { fgLinkMonitorEntry 10 }

fgLinkMonitorBandwidthOut OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The available bandwidth in Mbps of outgoing traffic detected by a link monitor on
its interface."
    ::= { fgLinkMonitorEntry 11 }

fgLinkMonitorBandwidthBi OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
         "The available bandwidth in Mbps of bi-direction traffic detected by a link
monitor on its interface."
    ::= { fgLinkMonitorEntry 12 }

fgLinkMonitorOutofSeq OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of out of sequence packets received."
    ::= { fgLinkMonitorEntry 13 }

--
-- fortinet.fnFortiGateMib.fgSystem.fgVWLHealthCheckLink
--
fgVWLHealthCheckLink OBJECT IDENTIFIER
    ::= { fgSystem 9 }

fgVWLHealthCheckLinkNumber OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of health check links in fgVWLHealthCheckLinkTable"
    ::= { fgVWLHealthCheckLink 1 }

fgVWLHealthCheckLinkTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgVWLHealthCheckLinkTableEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Virtual-wan-link health check statistics table.  This table has a dependent
expansion relationship with fgVdTable.
         Only health-checks with configured member link are present in this table."
    ::= { fgVWLHealthCheckLink 2 }

fgVWLHealthCheckLinkTableEntry OBJECT-TYPE
    SYNTAX      FgVWLHealthCheckLinkTableEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Virtual-wan-link health check statistics on a virtual domain"
    INDEX       {fgVWLHealthCheckLinkID}
```

```
    ::= { fgVWLHealthCheckLinkTable 1 }

FgVWLHealthCheckLinkTableEntry ::= SEQUENCE {
    fgVWLHealthCheckLinkID           FnIndex,
    fgVWLHealthCheckLinkName         DisplayString,
    fgVWLHealthCheckLinkSeq          Gauge32,
    fgVWLHealthCheckLinkState        INTEGER,
    fgVWLHealthCheckLinkLatency      DisplayString,
    fgVWLHealthCheckLinkJitter       DisplayString,
    fgVWLHealthCheckLinkPacketSend   Counter64,
    fgVWLHealthCheckLinkPacketRecv   Counter64,
    fgVWLHealthCheckLinkPacketLoss   DisplayString,
    fgVWLHealthCheckLinkVdom         DisplayString,
    fgVWLHealthCheckLinkBandwidthIn  Counter32,
    fgVWLHealthCheckLinkBandwidthOut Counter32,
    fgVWLHealthCheckLinkBandwidthBi  Counter32
}

fgVWLHealthCheckLinkID OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Virtual-wan-link health-check link ID. Only health-checks with configured member
link are present in this table. Virtuwal-wan-link health check link IDs are only unique
within a virtual domain."
    ::= { fgVWLHealthCheckLinkTableEntry 1 }

fgVWLHealthCheckLinkName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Health check name."
    ::= { fgVWLHealthCheckLinkTableEntry 2 }

fgVWLHealthCheckLinkSeq OBJECT-TYPE
    SYNTAX      Gauge32(1..255)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Virtual-wan-link member link sequence."
    ::= { fgVWLHealthCheckLinkTableEntry 3 }

fgVWLHealthCheckLinkState OBJECT-TYPE
    SYNTAX      INTEGER { alive(0), dead(1) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Heatlth check state on a specific member link."
    ::= { fgVWLHealthCheckLinkTableEntry 4 }

fgVWLHealthCheckLinkLatency OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The average latency of a health check on a specific member link in float number
within last 30 probes."
    ::= { fgVWLHealthCheckLinkTableEntry 5 }

fgVWLHealthCheckLinkJitter OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
        "The average jitter of a health check on a specific member link in float number
within last 30 probes."
    ::= { fgVWLHealthCheckLinkTableEntry 6 }

fgVWLHealthCheckLinkPacketSend OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of packets sent by a health check on a specific member link."
    ::= { fgVWLHealthCheckLinkTableEntry 7 }

fgVWLHealthCheckLinkPacketRecv OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of packets received by a health check on a specific member
link."
    ::= { fgVWLHealthCheckLinkTableEntry 8 }

fgVWLHealthCheckLinkPacketLoss OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The packet loss percentage of a health check on a specific member link in float
number within last 30 probes."
    ::= { fgVWLHealthCheckLinkTableEntry 9 }

fgVWLHealthCheckLinkVdom OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Virtual domain the link monitor entry exists in. This name corresponds to the
fgVdEntName used in fgVdTable."
    ::= { fgVWLHealthCheckLinkTableEntry 10 }

fgVWLHealthCheckLinkBandwidthIn OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The available bandwidth in Mbps of incoming traffic detected by a health-check on
a specific member link."
    ::= { fgVWLHealthCheckLinkTableEntry 11 }

fgVWLHealthCheckLinkBandwidthOut OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The available bandwidth in Mbps of outgoing traffic detected by a health-check on
a specific member link."
    ::= { fgVWLHealthCheckLinkTableEntry 12 }

fgVWLHealthCheckLinkBandwidthBi OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The available bandwidth in Mbps of bi-direction traffic detected by a health-
check on a specific member link."
```

```
    ::= { fgVWLHealthCheckLinkTableEntry 13 }

--
-- fortinet.fnFortiGateMib.fgSystem.fgDisks
--

fgDisks OBJECT IDENTIFIER
    ::= { fgSystem 10 }

fgDiskCount OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of entries in fgDiskTable."
    ::= { fgDisks 1 }

fgDiskTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgDiskEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A list of disks."
    ::= { fgDisks 2 }

fgDiskEntry OBJECT-TYPE
    SYNTAX      FgDiskEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A disk entry containing the storage name."
    INDEX       { fgDiskIndex }
    ::= { fgDiskTable 1 }

FgDiskEntry ::= SEQUENCE {
    fgDiskIndex         FnIndex,
    fgDiskName          DisplayString
}

fgDiskIndex OBJECT-TYPE
    SYNTAX     FnIndex
    MAX-ACCESS not-accessible
    STATUS     current
    DESCRIPTION
        "The storage index."
    ::= { fgDiskEntry 1 }

fgDiskName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The name of the storage."
    ::= { fgDiskEntry 2 }

--
-- fortinet.fnFortiGateMib.fgSystem.fgSlaProbeClient
--

fgSlaProbeClient OBJECT IDENTIFIER
    ::= {fgSystem 11}

fgSlaProbeClientNumber OBJECT-TYPE
    SYNTAX     Integer32
    MAX-ACCESS read-only
```

```
    STATUS     current
    DESCRIPTION
        "The number of sla probe clients in fgSlaProbeClientTable"
    ::= { fgSlaProbeClient 1 }

fgSlaProbeClientTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgSlaProbeClientEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Server Probe client statistics table. This table is global.
         All server probe clients are present in this table. Currently, twamp clients
only."
    ::= { fgSlaProbeClient 2 }

fgSlaProbeClientEntry OBJECT-TYPE
    SYNTAX      FgSlaProbeClientEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Server Probe client statistics."
    INDEX       {fgSlaProbeClientID}
    ::= { fgSlaProbeClientTable 1 }

FgSlaProbeClientEntry ::= SEQUENCE {
    fgSlaProbeClientID            FnIndex,
    fgSlaProbeClientIP            IpAddress,
    fgSlaProbeClientState         INTEGER,
    fgSlaProbeClientAvgLatency    DisplayString,
    fgSlaProbeClientAvgLatencySD  DisplayString,
    fgSlaProbeClientAvgLatencyDS  DisplayString,
    fgSlaProbeClientMinLatency    DisplayString,
    fgSlaProbeClientMinLatencySD  DisplayString,
    fgSlaProbeClientMinLatencyDS  DisplayString,
    fgSlaProbeClientMaxLatency    DisplayString,
    fgSlaProbeClientMaxLatencySD  DisplayString,
    fgSlaProbeClientMaxLatencyDS  DisplayString,
    fgSlaProbeClientAvgJitter     DisplayString,
    fgSlaProbeClientAvgJitterSD   DisplayString,
    fgSlaProbeClientAvgJitterDS   DisplayString,
    fgSlaProbeClientMinJitter     DisplayString,
    fgSlaProbeClientMinJitterSD   DisplayString,
    fgSlaProbeClientMinJitterDS   DisplayString,
    fgSlaProbeClientMaxJitter     DisplayString,
    fgSlaProbeClientMaxJitterSD   DisplayString,
    fgSlaProbeClientMaxJitterDS   DisplayString,
    fgSlaProbeClientPktloss       DisplayString,
    fgSlaProbeClientPktlossSD     DisplayString,
    fgSlaProbeClientPktlossDS     DisplayString,
    fgSlaProbeClientOutofSeq      Counter64,
    fgSlaProbeClientOutofSeqSD    Counter64,
    fgSlaProbeClientOutofSeqDS    Counter64
}

fgSlaProbeClientID OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Server Probe client ID."
    ::= { fgSlaProbeClientEntry 1 }

fgSlaProbeClientIP OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
```

```
    STATUS      current
    DESCRIPTION
        "IP address of server probe client."
    ::= { fgSlaProbeClientEntry 2 }

fgSlaProbeClientState OBJECT-TYPE
    SYNTAX      INTEGER { alive(0), dead(1) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Server Probe client state."
    ::= { fgSlaProbeClientEntry 3 }

fgSlaProbeClientAvgLatency OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The average latency of server probe client in float number within last 30
probes."
    ::= { fgSlaProbeClientEntry 4 }

fgSlaProbeClientAvgLatencySD OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The average latency from source to destination of server probe client in float
number within last 30 probes."
    ::= { fgSlaProbeClientEntry 5 }

fgSlaProbeClientAvgLatencyDS OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The average latency from destination to source of server probe in float number
within last 30 probes."
    ::= { fgSlaProbeClientEntry 6 }

fgSlaProbeClientMinLatency OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The minimal latency of server probe client in float number within last 30
probes."
    ::= {  fgSlaProbeClientEntry 7 }

fgSlaProbeClientMinLatencySD OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The minimal latency from source to destination of server probe client in float
number within last 30 probes."
    ::= { fgSlaProbeClientEntry 8 }

fgSlaProbeClientMinLatencyDS OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The minimal latency from destination to source of server probe client in float
number within last 30 probes."
```

```
    ::= { fgSlaProbeClientEntry 9 }

fgSlaProbeClientMaxLatency OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The maximum latency of server probe client in float number within last 30
probes."
    ::= { fgSlaProbeClientEntry 10 }

fgSlaProbeClientMaxLatencySD OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The maximum latency from source to destination of server probe client in float
number within last 30 probes."
    ::= { fgSlaProbeClientEntry 11 }

fgSlaProbeClientMaxLatencyDS OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The maximum latency from destination to source of server probe client in float
number within last 30 probes."
    ::= { fgSlaProbeClientEntry 12 }

fgSlaProbeClientAvgJitter OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The average jitter of server probe client in float number within last 30 probes."
    ::= { fgSlaProbeClientEntry 13 }

fgSlaProbeClientAvgJitterSD OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The average jitter from source to destination of server probe client in float
number within last 30 probes."
    ::= { fgSlaProbeClientEntry 14 }

fgSlaProbeClientAvgJitterDS OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The average jitter from destination to source of server probe client in float
number within last 30 probes."
    ::= { fgSlaProbeClientEntry 15 }

fgSlaProbeClientMinJitter OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The minimal jitter of server probe client in float number within last 30 probes."
    ::= { fgSlaProbeClientEntry 16 }

fgSlaProbeClientMinJitterSD OBJECT-TYPE
    SYNTAX      DisplayString
```

```
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The minimal jitter from source to destination of server probe client in float
number within last 30 probes."
    ::= { fgSlaProbeClientEntry 17 }

fgSlaProbeClientMinJitterDS OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The minimal jitter from destination to source of server probe client in float
number within last 30 probes."
    ::= { fgSlaProbeClientEntry 18 }

fgSlaProbeClientMaxJitter OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The maximum jitter of server probe client in float number within last 30 probes."
    ::= { fgSlaProbeClientEntry 19 }

fgSlaProbeClientMaxJitterSD OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The maximum jitter from source to destination of server probe client in float
number within last 30 probes."
    ::= { fgSlaProbeClientEntry 20 }

fgSlaProbeClientMaxJitterDS OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The maximum jitter from destination to source of server probe client in float
number within last 30 probes."
    ::= { fgSlaProbeClientEntry 21 }

fgSlaProbeClientPktloss OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The average packet loss percentage of server probe client in float number within
last 30 probes."
    ::= { fgSlaProbeClientEntry 22 }

fgSlaProbeClientPktlossSD OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The average packet loss percentage of server probe client from source to
destination in float number within last 30 probes."
    ::= { fgSlaProbeClientEntry 23 }

fgSlaProbeClientPktlossDS OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
```

```
        "The average packet loss percentage of server probe client from destionation to
source in float number within last 30 probes."
    ::= { fgSlaProbeClientEntry 24 }

fgSlaProbeClientOutofSeq OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of packets out of sequence order received by server probe
client."
    ::= { fgSlaProbeClientEntry 25 }

fgSlaProbeClientOutofSeqSD OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of packets out of sequence order received by server probe client
from source to destination."
    ::= { fgSlaProbeClientEntry 26 }

fgSlaProbeClientOutofSeqDS OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of packets out of sequence order received by server probe client
from destination to source."
    ::= { fgSlaProbeClientEntry 27 }

--
-- fortinet.fnFortiGateMib.fgSystem.fgDpdkEngs
--

fgDpdkEngs OBJECT IDENTIFIER
    ::= {fgSystem 12}

fgDpdkEngCount OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of entries in fgDpdkEngTable"
    ::= { fgDpdkEngs 1 }

fgDpdkEngTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgDpdkEngEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table that lists information for each dpdk engine"
    ::= { fgDpdkEngs 2 }

fgDpdkEngEntry OBJECT-TYPE
    SYNTAX      FgDpdkEngEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information for a particular dpdk engine"
    INDEX       { fgDpdkEngEntIndex }
    ::= { fgDpdkEngTable 1 }

FgDpdkEngEntry ::= SEQUENCE {
    fgDpdkEngEntIndex    FnIndex,
```

```
    fgDpdkEngRxUsage     Gauge32,
    fgDpdkEngVnpUsage    Gauge32,
    fgDpdkEngIpsUsage    Gauge32,
    fgDpdkEngTxUsage     Gauge32,
    fgDpdkEngIdle        Gauge32
}

fgDpdkEngEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A unique identifier within the fgDpdkEngTable"
    ::= { fgDpdkEngEntry 1 }

fgDpdkEngRxUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    UNITS       "%"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The DpdkEng's Rx usage (percentage)."
    ::= { fgDpdkEngEntry 2 }

fgDpdkEngVnpUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    UNITS       "%"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The DpdkEng's Vnp usage (percentage)."
    ::= { fgDpdkEngEntry 3 }

fgDpdkEngIpsUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    UNITS       "%"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The DpdkEng's Ips usage (percentage)."
    ::= { fgDpdkEngEntry 4 }

fgDpdkEngTxUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    UNITS       "%"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The DpdkEng's Tx usage (percentage)."
    ::= { fgDpdkEngEntry 5 }

fgDpdkEngIdle OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    UNITS       "%"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The DpdkEng's Idle usage (percentage)."
    ::= { fgDpdkEngEntry 6 }


--
-- fortinet.fnFortiGateMib.fgFirewall
--
```

```
fgFirewall OBJECT IDENTIFIER
    ::= { fnFortiGateMib 5 }

--
-- fortinet.fnFortiGateMib.fgFirewall.fgFwPolicies
--

fgFwPolicies OBJECT IDENTIFIER
    ::= { fgFirewall 1 }

fgFwPolInfo OBJECT IDENTIFIER
    ::= { fgFwPolicies 1 }

fgFwPolTables OBJECT IDENTIFIER
    ::= { fgFwPolicies 2 }

--
-- fortinet.fnFortiGateMib.fgFirewall.fgFwPolicies.fgFwPolTables.fgFwPolStatsTable
--

fgFwPolStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgFwPolStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Firewall policy statistics table.  This table has a dependent expansion
relationship with fgVdTable.
         Only virtual domains with enabled policies are present in this table."
    ::= { fgFwPolTables 1 }

fgFwPolStatsEntry OBJECT-TYPE
    SYNTAX      FgFwPolStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Firewall policy statistics on a virtual domain"
    INDEX       { fgVdEntIndex, fgFwPolID }
    ::= { fgFwPolStatsTable 1 }

FgFwPolStatsEntry ::= SEQUENCE {
    fgFwPolID               FnIndex,
    fgFwPolPktCount         Counter32,
    fgFwPolByteCount        Counter32,
    fgFwPolLastUsed         DisplayString,
    fgFwPolPktCountHc       Counter64,
    fgFwPolByteCountHc      Counter64
}

fgFwPolID OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Firewall policy ID. Only enabled policies are present in this table. Policy IDs
are only unique within a virtual domain."
    ::= { fgFwPolStatsEntry 1 }

fgFwPolPktCount OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of packets matched to policy (passed or blocked, depending on policy
action). Count is from the time the policy became active."
    ::= { fgFwPolStatsEntry 2 }
```

```
fgFwPolByteCount OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of bytes in packets matching the policy. See fgFwPolPktCount."
    ::= { fgFwPolStatsEntry 3 }

fgFwPolLastUsed OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "How many minutes since last used."
    ::= { fgFwPolStatsEntry 4 }

fgFwPolPktCountHc OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "64-bit Number of packets matched to policy (passed or blocked, depending on
policy action). Count is from the time the policy became active."
    ::= { fgFwPolStatsEntry 5 }

fgFwPolByteCountHc OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "64-bit Number of bytes in packets matching the policy. See fgFwPolPktCountHc."
    ::= { fgFwPolStatsEntry 6 }

--
-- fortinet.fnFortiGateMib.fgFirewall.fgFwPolicies.fgFwPolTables.fgFwPol6StatsTable
--

fgFwPol6StatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgFwPol6StatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Firewall policy6 statistics table.  This table has a dependent
         expansion relationship with fgVdTable.
         Only virtual domains with enabled policies are present in this table."
    ::= { fgFwPolTables 2 }

fgFwPol6StatsEntry OBJECT-TYPE
    SYNTAX      FgFwPol6StatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Firewall policy6 statistics on a virtual domain"
    INDEX       { fgVdEntIndex, fgFwPol6ID }
    ::= { fgFwPol6StatsTable 1 }

FgFwPol6StatsEntry ::= SEQUENCE {
    fgFwPol6ID         FnIndex,
    fgFwPol6PktCount   Counter64,
    fgFwPol6ByteCount  Counter64,
    fgFwPol6LastUsed   DisplayString
}

fgFwPol6ID OBJECT-TYPE
```

```
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Firewall policy6 ID. Only enabled policies are present in this table.
         Policy IDs are only unique within a virtual domain."
    ::= { fgFwPol6StatsEntry 1 }

fgFwPol6PktCount OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of packets matched to policy (passed or blocked, depending
         on policy action). Count is from the time the policy became active."
    ::= { fgFwPol6StatsEntry 2 }

fgFwPol6ByteCount OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of bytes in packets matching the policy. See fgFwPol6PktCount."
    ::= { fgFwPol6StatsEntry 3 }

fgFwPol6LastUsed OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "How many minutes since last used."
    ::= { fgFwPol6StatsEntry 4 }

--
-- fortinet.fnFortiGateMib.fgFirewall.fgFwUsers
--

fgFwUsers OBJECT IDENTIFIER
    ::= { fgFirewall 2 }

fgFwUserInfo OBJECT IDENTIFIER
    ::= { fgFwUsers 1 }

fgFwUserNumber OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of user accounts in fgFwUserTable"
    ::= { fgFwUserInfo 1 }

fgFwUserAuthTimeout OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Idle period after which a firewall-authentication user's session
         is automatically expired"
    ::= { fgFwUserInfo 2 }

fgFwUserTables OBJECT IDENTIFIER
    ::= { fgFwUsers 2 }

fgFwUserTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgFwUserEntry
```

```
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A list of local and proxy (Radius server)
         user accounts for use with firewall user authentication"
    ::= { fgFwUserTables 1 }

fgFwUserEntry OBJECT-TYPE
    SYNTAX      FgFwUserEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information applicable
         to a particular user account"
    INDEX       { fgFwUserIndex }
    ::= { fgFwUserTable 1 }

FgFwUserEntry ::= SEQUENCE {
    fgFwUserIndex   FnIndex,
    fgFwUserName    DisplayString,
    fgFwUserAuth    FgFwUserAuthType,
    fgFwUserState   FnBoolState,
    fgFwUserVdom    FgVdIndex
}

fgFwUserIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An index for uniquely identifying the users in fgFwUserTable"
    ::= { fgFwUserEntry 1 }

fgFwUserName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "User-name of the specified account"
    ::= { fgFwUserEntry 2 }

fgFwUserAuth OBJECT-TYPE
    SYNTAX      FgFwUserAuthType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Type of authentication the account uses (local, RADIUS, LDAP, etc.)"
    ::= { fgFwUserEntry 3 }

fgFwUserState OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Status of the user account (enable/disable)"
    ::= { fgFwUserEntry 4 }

fgFwUserVdom OBJECT-TYPE
    SYNTAX      FgVdIndex
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Virtual domain the user account exists in. This index corresponds to the index
used in fgVdTable."
    ::= { fgFwUserEntry 5 }
```

```
--
-- fortinet.fnFortiGateMib.fgFirewall.fgFwIppools
--

fgFwIppools OBJECT IDENTIFIER
    ::= { fgFirewall 3 }

fgFwIppTables OBJECT IDENTIFIER
    ::= { fgFwIppools 2 }

fgFwIppStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgFwIppStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Firewall ippool statistics table."
    ::= { fgFwIppTables 1 }

fgFwIppStatsEntry OBJECT-TYPE
    SYNTAX      FgFwIppStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing an ippool statistics."
    INDEX       { fgFwIppStatsStartIp, fgFwIppStatsEndIp }
    ::= { fgFwIppStatsTable 1 }

FgFwIppStatsEntry ::= SEQUENCE {
    fgFwIppStatsName          DisplayString,
    fgFwIppStatsType          DisplayString,
    fgFwIppStatsStartIp       IpAddress,
    fgFwIppStatsEndIp         IpAddress,
    fgFwIppStatsTotalSessions Gauge32,
    fgFwIppStatsTcpSessions   Gauge32,
    fgFwIppStatsUdpSessions   Gauge32,
    fgFwIppStatsOtherSessions Gauge32
}

fgFwIppStatsName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Name of the ippool."
    ::= { fgFwIppStatsEntry 1 }

fgFwIppStatsType OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Type of the ippool."
    ::= { fgFwIppStatsEntry 2 }

fgFwIppStatsStartIp OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Startip of the ippool."
    ::= { fgFwIppStatsEntry 3 }

fgFwIppStatsEndIp OBJECT-TYPE
    SYNTAX      IpAddress
```

```
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Endip of the ippool."
    ::= { fgFwIppStatsEntry 4 }

fgFwIppStatsTotalSessions OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Total session number of the ippool."
    ::= { fgFwIppStatsEntry 5 }

fgFwIppStatsTcpSessions OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Tcp session number of the ippool."
    ::= { fgFwIppStatsEntry 6 }

fgFwIppStatsUdpSessions OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Udp session number of the ippool."
    ::= { fgFwIppStatsEntry 7 }

fgFwIppStatsOtherSessions OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Other session number of the ippool."
    ::= { fgFwIppStatsEntry 8 }

--
-- fortinet.fnFortiGateMib.fgFirewall.fgFwGtp
--

fgFwGtp OBJECT IDENTIFIER
    ::= { fgFirewall 4 }

fgFwGtpStats OBJECT IDENTIFIER
    ::= { fgFwGtp 1 }

fgFwGtpStatsRequest OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of request in firewall gtp statistics."
    ::= { fgFwGtpStats 1 }

fgFwGtpStatsEchoRequest OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of echo_request in firewall gtp statistics."
    ::= { fgFwGtpStats 2 }

fgFwGtpStatsTunnel OBJECT-TYPE
```

```
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of tunnel in firewall gtp statistics."
    ::= { fgFwGtpStats 3 }

fgFwGtpStatsTunnelV0 OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of tunnel_v0 in firewall gtp statistics."
    ::= { fgFwGtpStats 4 }

fgFwGtpStatsPath OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of path in firewall gtp statistics."
    ::= { fgFwGtpStats 5 }

fgFwGtpStatsBearer OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of bearer in firewall gtp statistics."
    ::= { fgFwGtpStats 6 }

fgFwGtpStatsFteid OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of fteid in firewall gtp statistics."
    ::= { fgFwGtpStats 7 }

fgFwGtpStatsProfile OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of profile in firewall gtp statistics."
    ::= { fgFwGtpStats 8 }

fgFwGtpStatsImsi OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of imsi in firewall gtp statistics."
    ::= { fgFwGtpStats 9 }

fgFwGtpStatsApn OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of apn in firewall gtp statistics."
    ::= { fgFwGtpStats 10 }

fgFwGtpStatsApnShaper OBJECT-TYPE
    SYNTAX      Gauge32
```

```
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of apn_shaper in firewall gtp statistics."
    ::= { fgFwGtpStats 11 }

fgFwGtpStatsTunnelLimiter OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of tunnel_limiter in firewall gtp statistics."
    ::= { fgFwGtpStats 12 }

fgFwGtpStatsAdvPolicies OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of adv_policy in firewall gtp statistics."
    ::= { fgFwGtpStats 13 }

fgFwGtpStatsIeRemovePolicies OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of ie_remove_policy in firewall gtp statistics."
    ::= { fgFwGtpStats 14 }

fgFwGtpStatsIpPolicy OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of ip_policy in firewall gtp statistics."
    ::= { fgFwGtpStats 15 }

fgFwGtpStatsNoipPolicy OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of noip_policy in firewall gtp statistics."
    ::= { fgFwGtpStats 16 }

fgFwGtpStatsIeWlEntry OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of ie_wl_entry in firewall gtp statistics."
    ::= { fgFwGtpStats 17 }

fgFwGtpStatsClash OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of clash in firewall gtp statistics."
    ::= { fgFwGtpStats 18 }

fgFwGtpStatsDrop OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
```

```
    STATUS      current
    DESCRIPTION
        "Number of drop in firewall gtp statistics."
    ::= { fgFwGtpStats 19 }

fgFwGtpRtStats OBJECT IDENTIFIER
    ::= { fgFwGtp 2 }

fgFwGtpRtStatsCPkts OBJECT IDENTIFIER
    ::= { fgFwGtpRtStats 1 }

fgFwGtpRtStatsCForwarded OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet forwarded in firewall gtp runtime statistics."
    ::= { fgFwGtpRtStatsCPkts 1 }

fgFwGtpRtStatsCRejected OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet rejected in firewall gtp runtime statistics."
    ::= { fgFwGtpRtStatsCPkts 2 }

fgFwGtpRtStatsCDropped0 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by unknown in firewall gtp runtime statistics."
    ::= { fgFwGtpRtStatsCPkts 3 }

fgFwGtpRtStatsCDropped1 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by sanity in firewall gtp runtime statistics."
    ::= { fgFwGtpRtStatsCPkts 4 }

fgFwGtpRtStatsCDropped2 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by reserved-field in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 5 }

fgFwGtpRtStatsCDropped3 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by msg-reserved in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 6 }

fgFwGtpRtStatsCDropped4 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
        "Number of control packet dropped by msg-out-state in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 7 }

fgFwGtpRtStatsCDropped5 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by ie-reserved in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 8 }

fgFwGtpRtStatsCDropped6 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by ie-out-state in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 9 }

fgFwGtpRtStatsCDropped7 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by msg-length in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 10 }

fgFwGtpRtStatsCDropped8 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by ie-length in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 11 }

fgFwGtpRtStatsCDropped9 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by mandatory-ie in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 12 }

fgFwGtpRtStatsCDropped10 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by ip-policy in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 13 }

fgFwGtpRtStatsCDropped11 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by noip-policy in firewall gtp runtime
```

```
statistics."
    ::= { fgFwGtpRtStatsCPkts 14 }

fgFwGtpRtStatsCDropped12 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by sgsn-auth in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 15 }

fgFwGtpRtStatsCDropped13 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by sgsn-handover in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 16 }

fgFwGtpRtStatsCDropped14 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by ggsn-auth in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 17 }

fgFwGtpRtStatsCDropped15 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by seq-num in firewall gtp runtime statistics."
    ::= { fgFwGtpRtStatsCPkts 18 }

fgFwGtpRtStatsCDropped16 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by msg-filter in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 19 }

fgFwGtpRtStatsCDropped17 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by apn-filter in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 20 }

fgFwGtpRtStatsCDropped18 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by adv-policy-filter in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 21 }
```

```
fgFwGtpRtStatsCDropped19 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by imsi-filter in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 22 }

fgFwGtpRtStatsCDropped20 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by rate-limited in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 23 }

fgFwGtpRtStatsCDropped21 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by tunnel-limited in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 24 }

fgFwGtpRtStatsCDropped22 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by invalid-state in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 25 }

fgFwGtpRtStatsCDropped23 OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of control packet dropped by unknown-gtp-version in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsCPkts 26 }

fgFwGtpRtStatsDPkts OBJECT IDENTIFIER
    ::= { fgFwGtpRtStats 2 }

fgFwGtpRtStatsDForwarded OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of data packet forwarded in firewall gtp runtime statistics."
    ::= { fgFwGtpRtStatsDPkts 1 }

fgFwGtpRtStatsDDroppedSanity OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of data packet dropped by sanity in firewall gtp runtime statistics."
    ::= { fgFwGtpRtStatsDPkts 2 }

fgFwGtpRtStatsDDroppedMalMsg OBJECT-TYPE
```

```
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of data packet dropped by mal-msg in firewall gtp runtime statistics."
        ::= { fgFwGtpRtStatsDPkts 3 }

    fgFwGtpRtStatsDDroppedNoState OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of data packet dropped by no-state in firewall gtp runtime statistics."
        ::= { fgFwGtpRtStatsDPkts 4 }

    fgFwGtpRtStatsDDroppedMalIe OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of data packet dropped by mal-ie in firewall gtp runtime statistics."
        ::= { fgFwGtpRtStatsDPkts 5 }

    fgFwGtpRtStatsDDroppedGtpInGtp OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of data packet dropped by gtp-in-gtp in firewall gtp runtime statistics."
        ::= { fgFwGtpRtStatsDPkts 6 }

    fgFwGtpRtStatsDDroppedSpoof OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of data packet dropped by spoof in firewall gtp runtime statistics."
        ::= { fgFwGtpRtStatsDPkts 7 }

    fgFwGtpRtStatsDDroppedIpPol OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of data packet dropped by ip-policy in firewall gtp runtime statistics."
        ::= { fgFwGtpRtStatsDPkts 8 }

    fgFwGtpRtStatsDDroppedMsgFilter OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of data packet dropped by msg-filter in firewall gtp runtime statistics."
        ::= { fgFwGtpRtStatsDPkts 9 }

    fgFwGtpRtStatsDDroppedMsgRateLimit OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of data packet dropped by msg-rate-limit in firewall gtp runtime
    statistics."
        ::= { fgFwGtpRtStatsDPkts 10 }

    fgFwGtpRtStatsDDroppedUnknownVersion OBJECT-TYPE
```

```
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of data packet dropped by unknown-gtp-version in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsDPkts 11 }

fgFwGtpRtStatsBPkts OBJECT IDENTIFIER
    ::= { fgFwGtpRtStats 3 }

fgFwGtpRtStatsBForwarded OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of billing packet forwarded in firewall gtp runtime statistics."
    ::= { fgFwGtpRtStatsBPkts 1 }

fgFwGtpRtStatsBDroppedSanity OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of billing packet dropped by sanity in firewall gtp runtime statistics."
    ::= { fgFwGtpRtStatsBPkts 2 }

fgFwGtpRtStatsBDroppedMalMsg OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of billing packet dropped by mal-msg in firewall gtp runtime statistics."
    ::= { fgFwGtpRtStatsBPkts 3 }

fgFwGtpRtStatsBDroppedMalIe OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of billing packet dropped by mal-ie in firewall gtp runtime statistics."
    ::= { fgFwGtpRtStatsBPkts 4 }

fgFwGtpRtStatsBDroppedMsgFilter OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of billing packet dropped by msg-filter in firewall gtp runtime
statistics."
    ::= { fgFwGtpRtStatsBPkts 5 }

--
-- fortinet.fnFortiGateMib.fgMgmt
--

fgMgmt OBJECT IDENTIFIER
    ::= { fnFortiGateMib 6 }

fgFmTrapPrefix OBJECT IDENTIFIER
    ::= { fgMgmt 0 }

fgAdmin OBJECT IDENTIFIER
    ::= { fgMgmt 1 }
```

```
--
-- fortinet.fnFortiGateMib.fgMgmt.fgAdmin.fgAdminOptions
--

fgAdminOptions OBJECT IDENTIFIER
    ::= { fgAdmin 1 }

fgAdminIdleTimeout OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Idle period after which an administrator
         is automatically logged out of the system"
    ::= { fgAdminOptions 1 }

fgAdminLcdProtection OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Status of the LCD protection (enabled/disabled)"
    ::= { fgAdminOptions 2 }

--
-- fortinet.fnFortiGateMib.fgMgmt.fgAdmin.fgAdminTables
--

fgAdminTables OBJECT IDENTIFIER
    ::= { fgAdmin 2 }

fgAdminTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgAdminEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of administrator accounts on the device"
    ::= { fgAdminTables 1 }

fgAdminEntry OBJECT-TYPE
    SYNTAX      FgAdminEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information applicable
         to a particular admin account"
    AUGMENTS    { fnAdminEntry }
    ::= { fgAdminTable 1 }

FgAdminEntry ::= SEQUENCE {
    fgAdminVdom     FgVdIndex
}

fgAdminVdom OBJECT-TYPE
    SYNTAX      FgVdIndex
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The virtual domain the administrator belongs to"
    ::= { fgAdminEntry 1 }

--
-- fortinet.fnFortiGateMib.fgMgmt.fgAdmin.fgMgmtTrapObjects
--
```

```
fgMgmtTrapObjects OBJECT IDENTIFIER
    ::= { fgMgmt 2 }

fgManIfIp OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "IP address of the interface listed in the trap"
    ::= { fgMgmtTrapObjects 1 }

fgManIfMask OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Mask of subnet the interface belongs to"
    ::= { fgMgmtTrapObjects 2 }

fgManIfIp6 OBJECT-TYPE
    SYNTAX      Ipv6Address
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "IPv6 address of the interface listed in the trap"
    ::= { fgMgmtTrapObjects 3 }

--
-- fortinet.fnFortiGateMib.fgIntf
--

fgIntf OBJECT IDENTIFIER
    ::= { fnFortiGateMib 7 }

fgIntfInfo OBJECT IDENTIFIER
    ::= { fgIntf 1 }

fgIntfTables OBJECT IDENTIFIER
    ::= { fgIntf 2 }

fgIntfTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgIntfEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Fortinet specific extensions to MIB-2 ifTable"
    ::= { fgIntfTables 1 }

fgIntfEntry OBJECT-TYPE
    SYNTAX      FgIntfEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Fortinet specific information about an ifEntry. This table augments the standard
ifTable, so the same indexing is used."
    AUGMENTS    { ifEntry }
    ::= { fgIntfTable 1 }

FgIntfEntry ::= SEQUENCE {
    fgIntfEntVdom             FgVdIndex,
    fgIntfEntEstUpBandwidth   Unsigned32,
    fgIntfEntEstDownBandwidth Unsigned32
}

fgIntfEntVdom OBJECT-TYPE
```

```
    SYNTAX      FgVdIndex
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The virtual domain the interface belongs to. This index corresponds to the index
used by fgVdTable."
    ::= { fgIntfEntry 1 }

fgIntfEntEstUpBandwidth OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Estimated maximum upstream bandwidth (Kbps). Used to estimate link utilization."
    ::= { fgIntfEntry 2 }

fgIntfEntEstDownBandwidth OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Estimated maximum downstream bandwidth (Kbps). Used to estimate link
utilization."
    ::= { fgIntfEntry 3 }

fgIntfVrrps OBJECT IDENTIFIER
    ::= { fgIntf 3 }

fgIntfVrrpCount OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of entries in fgIntfVrrpTable"
    ::= { fgIntfVrrps 1 }

fgIntfVrrpTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgIntfVrrpEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A list of VRRPs and values."
    ::= { fgIntfVrrps 2 }

fgIntfVrrpEntry OBJECT-TYPE
    SYNTAX      FgIntfVrrpEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing the ID, group ID, interface name, state and IP address of a
given virtual router."
    INDEX       { fgIntfVrrpEntIndex }
    ::= { fgIntfVrrpTable 1 }

FgIntfVrrpEntry ::= SEQUENCE {
    fgIntfVrrpEntIndex   FnIndex,
    fgIntfVrrpEntVrId    FnIndex,
    fgIntfVrrpEntGrpId   FnIndex,
    fgIntfVrrpEntIfName  DisplayString,
    fgIntfVrrpEntState   INTEGER,
    fgIntfVrrpEntVrIp    IpAddress
}

fgIntfVrrpEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
```

```
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "A unique identifier within the fgIntfVrrpTable"
        ::= { fgIntfVrrpEntry 1 }

    fgIntfVrrpEntVrId OBJECT-TYPE
        SYNTAX      FnIndex
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "ID of a virtual router."
        ::= { fgIntfVrrpEntry 2 }

    fgIntfVrrpEntGrpId OBJECT-TYPE
        SYNTAX      FnIndex
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The group ID of a virtual router."
        ::= { fgIntfVrrpEntry 3 }

    fgIntfVrrpEntIfName OBJECT-TYPE
        SYNTAX      DisplayString
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The interface name of a virtual router."
        ::= { fgIntfVrrpEntry 4 }

    fgIntfVrrpEntState OBJECT-TYPE
        SYNTAX      INTEGER { backup(1), master(2) }
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "State of a virtual router."
        ::= { fgIntfVrrpEntry 5 }

    fgIntfVrrpEntVrIp OBJECT-TYPE
        SYNTAX      IpAddress
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "IP address of a virtual router."
        ::= { fgIntfVrrpEntry 6 }

    fgIntfVlanHbs OBJECT IDENTIFIER
        ::= { fgIntf 4 }

    fgIntfVlanHbCount OBJECT-TYPE
        SYNTAX      Integer32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The number of entries in fgIntfVlanHbTable"
        ::= { fgIntfVlanHbs 1 }

    fgIntfVlanHbTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF FgIntfVlanHbEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "A list of VlanHbs and values."
        ::= { fgIntfVlanHbs 2 }
```

```
fgIntfVlanHbEntry OBJECT-TYPE
    SYNTAX      FgIntfVlanHbEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing the vlan interface name, peer's serial number and state of a
given vlan interface heartbeat."
    INDEX       { fgIntfVlanHbEntIndex }
    ::= { fgIntfVlanHbTable 1 }

FgIntfVlanHbEntry ::= SEQUENCE {
    fgIntfVlanHbEntIndex   FnIndex,
    fgIntfVlanHbEntIfName  DisplayString,
    fgIntfVlanHbEntSerial  DisplayString,
    fgIntfVlanHbEntState   INTEGER
}

fgIntfVlanHbEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A unique identifier within the fgIntfVlanHbTable"
    ::= { fgIntfVlanHbEntry 1 }

fgIntfVlanHbEntIfName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The vlan interface name."
    ::= { fgIntfVlanHbEntry 2 }

fgIntfVlanHbEntSerial OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Serial number of a vlan HA peer."
    ::= { fgIntfVlanHbEntry 3 }

fgIntfVlanHbEntState OBJECT-TYPE
    SYNTAX      INTEGER { active(1), inactive(2) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "State of a vlan interface heartbeat."
    ::= { fgIntfVlanHbEntry 4 }

fgIntfBcs OBJECT IDENTIFIER
    ::= { fgIntf 5 }

fgIntfBcTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgIntfBcEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A list of all class-levels with bandwidth usage and packet drop counter."
    ::= { fgIntfBcs 2 }

fgIntfBcEntry OBJECT-TYPE
    SYNTAX      FgIntfBcEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
```

```
        "An entry containing the Bandwidth Control statistics, packet drop counter of a
given interface."
    INDEX       { ifIndex }
    ::= { fgIntfBcTable 1 }

FgIntfBcEntry ::= SEQUENCE {
    fgIntfBcAllocatedBandwidth  Integer32,
    fgIntfBcGuaranteedBandwidth Integer32,
    fgIntfBcMaxBandwidth        Integer32,
    fgIntfBcCurrentBandwidth    Integer32,
    fgIntfBcBytes               Counter64,
    fgIntfBcDrops               Counter64
}

fgIntfBcAllocatedBandwidth OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Allocated Bandwidth of a given interface and class-level."
    ::= { fgIntfBcEntry 1 }

fgIntfBcGuaranteedBandwidth OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Guaranteed Bandwidth of a given interface and class-level."
    ::= { fgIntfBcEntry 2 }

fgIntfBcMaxBandwidth OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Max Bandwidth of a given interface and class-level."
    ::= { fgIntfBcEntry 3 }

fgIntfBcCurrentBandwidth OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current Bandwidth of a given interface and class-level."
    ::= { fgIntfBcEntry 4 }

fgIntfBcBytes OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Bytes of a given inteface and class-level."
    ::= { fgIntfBcEntry 5 }

fgIntfBcDrops OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Packet drop counter of a given interface and class-level."
    ::= { fgIntfBcEntry 6 }

fgIntfBcInTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgIntfBcInEntry
    MAX-ACCESS  not-accessible
```

```
    STATUS      current
    DESCRIPTION
        "A list of all class-levels with bandwidth usage and packet drop counter."
    ::= { fgIntfBcs 3 }

fgIntfBcInEntry OBJECT-TYPE
    SYNTAX      FgIntfBcInEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing the Bandwidth Control statistics, packet drop counter of a
given interface."
    INDEX       { ifIndex }
    ::= { fgIntfBcInTable 1 }

FgIntfBcInEntry ::= SEQUENCE {
    fgIntfBcInAllocatedBandwidth  Integer32,
    fgIntfBcInGuaranteedBandwidth Integer32,
    fgIntfBcInMaxBandwidth        Integer32,
    fgIntfBcInCurrentBandwidth    Integer32,
    fgIntfBcInBytes               Counter64,
    fgIntfBcInDrops               Counter64
}

fgIntfBcInAllocatedBandwidth OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Allocated Bandwidth of a given interface and class-level."
    ::= { fgIntfBcInEntry 1 }

fgIntfBcInGuaranteedBandwidth OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Guaranteed Bandwidth of a given interface and class-level."
    ::= { fgIntfBcInEntry 2 }

fgIntfBcInMaxBandwidth OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Max Bandwidth of a given interface and class-level."
    ::= { fgIntfBcInEntry 3 }

fgIntfBcInCurrentBandwidth OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current Bandwidth of a given interface and class-level."
    ::= { fgIntfBcInEntry 4 }

fgIntfBcInBytes OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Bytes of a given inteface and class-level."
    ::= { fgIntfBcInEntry 5 }

fgIntfBcInDrops OBJECT-TYPE
```

```
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Packet drop counter of a given interface and class-level."
    ::= { fgIntfBcInEntry 6 }

--
-- fortinet.fnFortiGateMib.fgAntivirus
--

fgAntivirus OBJECT IDENTIFIER
    ::= { fnFortiGateMib 8 }

fgAvInfo OBJECT IDENTIFIER
    ::= { fgAntivirus 1 }

fgAvTables OBJECT IDENTIFIER
    ::= { fgAntivirus 2 }

fgAvStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgAvStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of Anti-virus statistics per virtual domain"
    ::= { fgAvTables 1 }

fgAvStatsEntry OBJECT-TYPE
    SYNTAX      FgAvStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Anti-virus statistics for a particular virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgAvStatsTable 1 }

FgAvStatsEntry ::= SEQUENCE {
    fgAvVirusDetected       Counter32,
    fgAvVirusBlocked        Counter32,
    fgAvHTTPVirusDetected   Counter32,
    fgAvHTTPVirusBlocked    Counter32,
    fgAvSMTPVirusDetected   Counter32,
    fgAvSMTPVirusBlocked    Counter32,
    fgAvPOP3VirusDetected   Counter32,
    fgAvPOP3VirusBlocked    Counter32,
    fgAvIMAPVirusDetected   Counter32,
    fgAvIMAPVirusBlocked    Counter32,
    fgAvFTPVirusDetected    Counter32,
    fgAvFTPVirusBlocked     Counter32,
    fgAvIMVirusDetected     Counter32,
    fgAvIMVirusBlocked      Counter32,
    fgAvNNTPVirusDetected   Counter32,
    fgAvNNTPVirusBlocked    Counter32,
    fgAvOversizedDetected   Counter32,
    fgAvOversizedBlocked    Counter32,
    fgAvMAPIVirusDetected   Counter32,
    fgAvMAPIVirusBlocked    Counter32,
    fgAvSMBVirusDetected    Counter32,
    fgAvSMBVirusBlocked     Counter32
}

fgAvVirusDetected OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
```

```
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions detected in the virtual domain since start-up"
    ::= { fgAvStatsEntry 1 }

fgAvVirusBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions blocked in the virtual domain since start-up"
    ::= { fgAvStatsEntry 2 }

fgAvHTTPVirusDetected OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over HTTP detected in the virtual domain since
start-up"
    ::= { fgAvStatsEntry 3 }

fgAvHTTPVirusBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over HTTP blocked in the virtual domain since
start-up"
    ::= { fgAvStatsEntry 4 }

fgAvSMTPVirusDetected OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over SMTP detected in the virtual domain since
start-up"
    ::= { fgAvStatsEntry 5 }

fgAvSMTPVirusBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over SMTP blocked in the virtual domain since
start-up"
    ::= { fgAvStatsEntry 6 }

fgAvPOP3VirusDetected OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over POP3 detected in the virtual domain since
start-up"
    ::= { fgAvStatsEntry 7 }

fgAvPOP3VirusBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over POP3 blocked in the virtual domain since
start-up"
```

```
    ::= { fgAvStatsEntry 8 }

fgAvIMAPVirusDetected OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over IMAP detected in the virtual domain since
start-up"
    ::= { fgAvStatsEntry 9 }

fgAvIMAPVirusBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over IMAP blocked in the virtual domain since
start-up"
    ::= { fgAvStatsEntry 10 }

fgAvFTPVirusDetected OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over FTP detected in the virtual domain since
start-up"
    ::= { fgAvStatsEntry 11 }

fgAvFTPVirusBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over FTP blocked in the virtual domain since start-
up"
    ::= { fgAvStatsEntry 12 }

fgAvIMVirusDetected OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over IM protocols detected in the virtual domain
since start-up"
    ::= { fgAvStatsEntry 13 }

fgAvIMVirusBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over IM protocols blocked in the virtual domain
since start-up"
    ::= { fgAvStatsEntry 14 }

fgAvNNTPVirusDetected OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over NNTP detected in the virtual domain since
start-up"
    ::= { fgAvStatsEntry 15 }
```

```
fgAvNNTPVirusBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over NNTP blocked in the virtual domain since
start-up"
    ::= { fgAvStatsEntry 16 }

fgAvOversizedDetected OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of over-sized file transmissions detected in the virtual domain since
start-up"
    ::= { fgAvStatsEntry 17 }

fgAvOversizedBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of over-sized file transmissions blocked in the virtual domain since
start-up"
    ::= { fgAvStatsEntry 18 }

fgAvMAPIVirusDetected OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over MAPI detected in the virtual domain since
start-up"
    ::= { fgAvStatsEntry 19 }

fgAvMAPIVirusBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over MAPI blocked in the virtual domain since
start-up"
    ::= { fgAvStatsEntry 20 }

fgAvSMBVirusDetected OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over SMB detected in the virtual domain since
start-up"
    ::= { fgAvStatsEntry 21 }

fgAvSMBVirusBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of virus transmissions over SMB blocked in the virtual domain since start-
up"
    ::= { fgAvStatsEntry 22 }

--
-- fortinet.fnFortiGateMib.fgAntivirus.fgAvTrapObjects
```

```
--

fgAvTrapObjects OBJECT IDENTIFIER
    ::= { fgAntivirus 3 }

fgAvTrapVirName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Virus name that triggered event"
    ::= { fgAvTrapObjects 1 }

--
-- fortinet.fnFortiGateMib.fgIps
--

fgIps OBJECT IDENTIFIER
    ::= { fnFortiGateMib 9 }

fgIpsInfo OBJECT IDENTIFIER
    ::= { fgIps 1 }

fgIpsTables OBJECT IDENTIFIER
    ::= { fgIps 2 }

fgIpsStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgIpsStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of IPS/IDS statistics per virtual domain"
    ::= { fgIpsTables 1 }

fgIpsStatsEntry OBJECT-TYPE
    SYNTAX      FgIpsStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "IPS/IDS statistics for a particular virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgIpsStatsTable 1 }

FgIpsStatsEntry ::= SEQUENCE {
    fgIpsIntrusionsDetected     Counter32,
    fgIpsIntrusionsBlocked      Counter32,
    fgIpsCritSevDetections      Counter32,
    fgIpsHighSevDetections      Counter32,
    fgIpsMedSevDetections       Counter32,
    fgIpsLowSevDetections       Counter32,
    fgIpsInfoSevDetections      Counter32,
    fgIpsSignatureDetections    Counter32,
    fgIpsAnomalyDetections      Counter32
}

fgIpsIntrusionsDetected OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of intrusions detected since start-up in this virtual domain"
    ::= { fgIpsStatsEntry 1 }

fgIpsIntrusionsBlocked OBJECT-TYPE
    SYNTAX      Counter32
```

```
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of intrusions blocked since start-up in this virtual domain"
        ::= { fgIpsStatsEntry 2 }

    fgIpsCritSevDetections OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of critical severity intrusions
             detected since start-up in this virtual domain"
        ::= { fgIpsStatsEntry 3 }

    fgIpsHighSevDetections OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of high severity intrusions
             detected since start-up in this virtual domain"
        ::= { fgIpsStatsEntry 4 }

    fgIpsMedSevDetections OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of medium severity intrusions
             detected since start-up in this virtual domain"
        ::= { fgIpsStatsEntry 5 }

    fgIpsLowSevDetections OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of low severity intrusions
             detected since start-up in this virtual domain"
        ::= { fgIpsStatsEntry 6 }

    fgIpsInfoSevDetections OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of informational severity intrusions
             detected since start-up in this virtual domain"
        ::= { fgIpsStatsEntry 7 }

    fgIpsSignatureDetections OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of intrusions detected by signature
             since start-up in this virtual domain"
        ::= { fgIpsStatsEntry 8 }

    fgIpsAnomalyDetections OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
```

```
        "Number of intrusions DECed as anomalies
         since start-up in this virtual domain"
    ::= { fgIpsStatsEntry 9 }

--
-- fortinet.fnFortiGateMib.fgIps.fgIpsTrapObjects
--

fgIpsTrapObjects OBJECT IDENTIFIER
    ::= { fgIps 3 }

fgIpsTrapSigId OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "ID of IPS signature identified in trap"
    ::= { fgIpsTrapObjects 1 }

fgIpsTrapSrcIp OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Source IP Address of the IPS signature trigger"
    ::= { fgIpsTrapObjects 2 }

fgIpsTrapSigMsg OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Message associated with IPS event"
    ::= { fgIpsTrapObjects 3 }

--
-- fortinet.fnFortiGateMib.fgApplications
--

fgApplications OBJECT IDENTIFIER
    ::= { fnFortiGateMib 10 }

fgWebfilter OBJECT IDENTIFIER
    ::= { fgApplications 1 }

fgWebfilterInfo OBJECT IDENTIFIER
    ::= { fgWebfilter 1 }

fgWebfilterTables OBJECT IDENTIFIER
    ::= { fgWebfilter 2 }

--
--
fortinet.fnFortiGateMib.fgApplications.fgWebfilter.fgWebfilterTables.fgWebfilterStatsTable
--

fgWebfilterStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgWebfilterStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of Web-filter statistics per virtual domain"
    ::= { fgWebfilterTables 1 }

fgWebfilterStatsEntry OBJECT-TYPE
```

```
    SYNTAX      FgWebfilterStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Web-filter statistics for a particular virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgWebfilterStatsTable 1 }

FgWebfilterStatsEntry ::= SEQUENCE {
    fgWfHTTPBlocked         Counter32,
    fgWfHTTPSBlocked        Counter32,
    fgWfHTTPURLBlocked      Counter32,
    fgWfHTTPSURLBlocked     Counter32,
    fgWfActiveXBlocked      Counter32,
    fgWfCookieBlocked       Counter32,
    fgWfAppletBlocked       Counter32
}

fgWfHTTPBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of HTTP sessions blocked by Web-filter since start-up"
    ::= { fgWebfilterStatsEntry 1 }

fgWfHTTPSBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of HTTPS sessions blocked by Web-filter since start-up"
    ::= { fgWebfilterStatsEntry 2 }

fgWfHTTPURLBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of HTTP URLs blocked by Web-filter since start-up"
    ::= { fgWebfilterStatsEntry 3 }

fgWfHTTPSURLBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of HTTPS URLs blocked by Web-filter since start-up"
    ::= { fgWebfilterStatsEntry 4 }

fgWfActiveXBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of ActiveX downloads blocked by Web-filter since start-up"
    ::= { fgWebfilterStatsEntry 5 }

fgWfCookieBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of HTTP Cookies blocked by Web-filter since start-up"
    ::= { fgWebfilterStatsEntry 6 }
```

```
fgWfAppletBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of Applets blocked by Web-filter since start-up"
    ::= { fgWebfilterStatsEntry 7 }

--
--
fortinet.fnFortiGateMib.fgApplications.fgWebfilter.fgWebfilterTables.fgFortiGuardStatsTabl
e
--

fgFortiGuardStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgFortiGuardStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of FortiGuard statistics per virtual domain"
    ::= { fgWebfilterTables 2 }

fgFortiGuardStatsEntry OBJECT-TYPE
    SYNTAX      FgFortiGuardStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "FortiGuard statistics for a particular virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgFortiGuardStatsTable 1 }

FgFortiGuardStatsEntry ::= SEQUENCE {
    fgFgWfHTTPExamined      Counter32,
    fgFgWfHTTPSExamined     Counter32,
    fgFgWfHTTPAllowed       Counter32,
    fgFgWfHTTPSAllowed      Counter32,
    fgFgWfHTTPBlocked       Counter32,
    fgFgWfHTTPSBlocked      Counter32,
    fgFgWfHTTPLogged        Counter32,
    fgFgWfHTTPSLogged       Counter32,
    fgFgWfHTTPOverridden    Counter32,
    fgFgWfHTTPSOverridden   Counter32
}

fgFgWfHTTPExamined OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of HTTP requests examined using FortiGuard since start-up"
    ::= { fgFortiGuardStatsEntry 1 }

fgFgWfHTTPSExamined OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of HTTPS requests examined using FortiGuard since start-up"
    ::= { fgFortiGuardStatsEntry 2 }

fgFgWfHTTPAllowed OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
        "Number of HTTP requests allowed to proceed using FortiGuard since start-up"
    ::= { fgFortiGuardStatsEntry 3 }

fgFgWfHTTPSAllowed OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of HTTPS requests allowed to proceed using FortiGuard since start-up"
    ::= { fgFortiGuardStatsEntry 4 }

fgFgWfHTTPBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of HTTP requests blocked using FortiGuard since start-up"
    ::= { fgFortiGuardStatsEntry 5 }

fgFgWfHTTPSBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of HTTPS requests blocked using FortiGuard since start-up"
    ::= { fgFortiGuardStatsEntry 6 }

fgFgWfHTTPLogged OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of HTTP requests logged using FortiGuard since start-up"
    ::= { fgFortiGuardStatsEntry 7 }

fgFgWfHTTPSLogged OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of HTTPS requests logged using FortiGuard since start-up"
    ::= { fgFortiGuardStatsEntry 8 }

fgFgWfHTTPOverridden OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of HTTP requests overridden using FortiGuard since start-up"
    ::= { fgFortiGuardStatsEntry 9 }

fgFgWfHTTPSOverridden OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of HTTPS requests overridden using FortiGuard since start-up"
    ::= { fgFortiGuardStatsEntry 10 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppProxyHTTP
--

fgAppProxyHTTP OBJECT IDENTIFIER
```

```
    ::= { fgApplications 100 }

fgApHTTPUpTime OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
        "HTTP proxy up-time (in seconds)"
    ::= { fgAppProxyHTTP 1 }

fgApHTTPMemUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
        "HTTP proxy memory usage (percentage of system total)"
    ::= { fgAppProxyHTTP 2 }

fgApHTTPConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "HTTP proxy current connections"
    ::= { fgAppProxyHTTP 4 }

fgApHTTPMaxConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Maximum number of connections supported by HTTP proxy"
    ::= { fgAppProxyHTTP 5 }

fgApHTTPStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgApHTTPStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of HTTP Proxy statistics per virtual domain"
    ::= { fgAppProxyHTTP 3 }

fgApHTTPStatsEntry OBJECT-TYPE
    SYNTAX      FgApHTTPStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "HTTP Proxy statistics for a particular virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgApHTTPStatsTable 1 }

FgApHTTPStatsEntry ::= SEQUENCE {
    fgApHTTPReqProcessed    Counter32
}

fgApHTTPReqProcessed OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of HTTP requests in this virtual domain processed by the HTTP proxy since
start-up"
    ::= { fgApHTTPStatsEntry 1 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppProxySMTP
--
```

```
fgAppProxySMTP OBJECT IDENTIFIER
    ::= { fgApplications 101 }

fgApSMTPUpTime OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
        "SMTP Proxy up-time, in seconds"
    ::= { fgAppProxySMTP 1 }

fgApSMTPMemUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
        "SMTP Proxy memory utilization (percentage of system total)"
    ::= { fgAppProxySMTP 2 }

fgApSMTPConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "SMTP proxy current connections"
    ::= { fgAppProxySMTP 4 }

fgApSMTPMaxConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Maximum number of connections supported by SMTP proxy"
    ::= { fgAppProxySMTP 5 }

fgApSMTPStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgApSMTPStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of SMTP proxy statistics per virtual domain"
    ::= { fgAppProxySMTP 3 }

fgApSMTPStatsEntry OBJECT-TYPE
    SYNTAX      FgApSMTPStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "SMTP Proxy statistics for a particular virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgApSMTPStatsTable 1 }

FgApSMTPStatsEntry ::= SEQUENCE {
    fgApSMTPReqProcessed    Counter32,
    fgApSMTPSpamDetected    Counter32
}

fgApSMTPReqProcessed OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of requests in this virtual domain processed by the SMTP proxy since
start-up"
    ::= { fgApSMTPStatsEntry 1 }
```

```
fgApSMTPSpamDetected OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of spam detected in this virtual domain by the SMTP proxy since start-up"
    ::= { fgApSMTPStatsEntry 2 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppProxyPOP3
--

fgAppProxyPOP3 OBJECT IDENTIFIER
    ::= { fgApplications 102 }

fgApPOP3UpTime OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
        "Up-time of the POP3 proxy, in seconds"
    ::= { fgAppProxyPOP3 1 }

fgApPOP3MemUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
        "Memory usage of the POP3 Proxy (percentage of system total)"
    ::= { fgAppProxyPOP3 2 }

fgApPOP3Connections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "POP3 proxy current connections"
    ::= { fgAppProxyPOP3 4 }

fgApPOP3MaxConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Maximum number of connections supported by POP3 proxy"
    ::= { fgAppProxyPOP3 5 }

fgApPOP3StatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgApPOP3StatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of POP3 proxy statistics per virtual domain"
    ::= { fgAppProxyPOP3 3 }

fgApPOP3StatsEntry OBJECT-TYPE
    SYNTAX      FgApPOP3StatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Proxy pop3 statistics for a particular virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgApPOP3StatsTable 1 }

FgApPOP3StatsEntry ::= SEQUENCE {
    fgApPOP3ReqProcessed    Counter32,
    fgApPOP3SpamDetected    Counter32
```

```
}

fgApPOP3ReqProcessed OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of requests in this virtual domain processed by the POP3 proxy since
start-up"
    ::= { fgApPOP3StatsEntry 1 }

fgApPOP3SpamDetected OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of spam detected in this virtual domain by the POP3 Proxy since start-up"
    ::= { fgApPOP3StatsEntry 2 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppProxyIMAP
--

fgAppProxyIMAP OBJECT IDENTIFIER
    ::= { fgApplications 103 }

fgApIMAPUpTime OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
        "Up-time of the IMAP proxy, in seconds"
    ::= { fgAppProxyIMAP 1 }

fgApIMAPMemUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
        "Memory utilization of the IMAP Proxy (as a percentage of the system total)"
    ::= { fgAppProxyIMAP 2 }

fgApIMAPConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "IMAP proxy current connections"
    ::= { fgAppProxyIMAP 4 }

fgApIMAPMaxConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Maximum number of connections supported by IMAP proxy"
    ::= { fgAppProxyIMAP 5 }

fgApIMAPStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgApIMAPStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of IMAP proxy statistics per virtual domain"
    ::= { fgAppProxyIMAP 3 }

fgApIMAPStatsEntry OBJECT-TYPE
```

```
    SYNTAX      FgApIMAPStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "IMAP Proxy statistics for a particular virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgApIMAPStatsTable 1 }

FgApIMAPStatsEntry ::= SEQUENCE {
    fgApIMAPReqProcessed    Counter32,
    fgApIMAPSpamDetected    Counter32
}

fgApIMAPReqProcessed OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of requests in this virtual domain processed by the IMAP proxy since
start-up"
    ::= { fgApIMAPStatsEntry 1 }

fgApIMAPSpamDetected OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of spam detected in this virtual domain by the IMAP proxy since start-up"
    ::= { fgApIMAPStatsEntry 2 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppProxyNNTP
--

fgAppProxyNNTP OBJECT IDENTIFIER
    ::= { fgApplications 104 }

fgApNNTPUpTime OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
        "Up-time of the NNTP proxy, in seconds"
    ::= { fgAppProxyNNTP 1 }

fgApNNTPMemUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
        "Memory utilization of the NNTP proxy, as a percentage of the system total"
    ::= { fgAppProxyNNTP 2 }

fgApNNTPConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "NNTP proxy current connections"
    ::= { fgAppProxyNNTP 4 }

fgApNNTPMaxConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Maximum number of connections supported by NNTP proxy"
```

```
    ::= { fgAppProxyNNTP 5 }

fgApNNTPStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgApNNTPStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of NNTP proxy statistics per virtual domain"
    ::= { fgAppProxyNNTP 3 }

fgApNNTPStatsEntry OBJECT-TYPE
    SYNTAX      FgApNNTPStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "NNTP Proxy statistics for a particular virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgApNNTPStatsTable 1 }

FgApNNTPStatsEntry ::= SEQUENCE {
    fgApNNTPReqProcessed    Counter32
}

fgApNNTPReqProcessed OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of requests in the virtual domain processed by the NNTP proxy since start-
up"
    ::= { fgApNNTPStatsEntry 1 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppProxyIM
--

fgAppProxyIM OBJECT IDENTIFIER
    ::= { fgApplications 105 }

fgApIMUpTime OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Up-time of the IM proxy, in seconds"
    ::= { fgAppProxyIM 1 }

fgApIMMemUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "IM Proxy memory usage, as a percentage of the system total"
    ::= { fgAppProxyIM 2 }

fgApIMStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgApIMStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of IM proxy statistics per virtual domain"
    ::= { fgAppProxyIM 3 }

fgApIMStatsEntry OBJECT-TYPE
    SYNTAX      FgApIMStatsEntry
```

```
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "IM Proxy statistics for a particular virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgApIMStatsTable 1 }

FgApIMStatsEntry ::= SEQUENCE {
    fgApIMReqProcessed  Counter32
}

fgApIMReqProcessed OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of requests in this virtual domain processed by the IM proxy since start-
up"
    ::= { fgApIMStatsEntry 1 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppProxySIP
--

fgAppProxySIP OBJECT IDENTIFIER
    ::= { fgApplications 106 }

fgApSIPUpTime OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Up-time of the SIP Proxy, in seconds"
    ::= { fgAppProxySIP 1 }

fgApSIPMemUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "SIP Proxy memory utilization, as a percentage of the system total"
    ::= { fgAppProxySIP 2 }

fgApSIPStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgApSIPStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of SIP proxy statistics per virtual domain"
    ::= { fgAppProxySIP 3 }

fgApSIPStatsEntry OBJECT-TYPE
    SYNTAX      FgApSIPStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "SIP Proxy statistics for a particular virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgApSIPStatsTable 1 }

FgApSIPStatsEntry ::= SEQUENCE {
    fgApSIPClientReg        Counter32,
    fgApSIPCallHandling     Counter32,
    fgApSIPServices         Counter32,
    fgApSIPOtherReq         Counter32
```

```
}

fgApSIPClientReg OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of client registration requests (Register and Options) in this virtual
domain
         processed by the SIP proxy since start-up"
    ::= { fgApSIPStatsEntry 1 }

fgApSIPCallHandling OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of call handling requests (Invite, Ack, Bye, Cancel and Refer) in this
virtual domain
         processed by the SIP proxy since start-up"
    ::= { fgApSIPStatsEntry 2 }

fgApSIPServices OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of service requests (Subscribe, notify and Message) in this virtual domain
         processed by the SIP proxy since start-up"
    ::= { fgApSIPStatsEntry 3 }

fgApSIPOtherReq OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of other sip requests in this virtual domain processed by the SIP proxy
since start-up"
    ::= { fgApSIPStatsEntry 4 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppScanUnit
--

fgAppScanUnit OBJECT IDENTIFIER
    ::= { fgApplications 107 }

fgAppSuNumber OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of scan units in the fgAppSuStatsTable"
    ::= { fgAppScanUnit 1 }

fgAppSuStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgAppSuStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of scan unit statistics"
    ::= { fgAppScanUnit 2 }

fgAppSuStatsEntry OBJECT-TYPE
    SYNTAX      FgAppSuStatsEntry
```

```
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Statistics entry for a particular scan unit"
    INDEX       { fgAppSuIndex }
    ::= { fgAppSuStatsTable 1 }

FgAppSuStatsEntry ::= SEQUENCE {
    fgAppSuIndex        FnIndex,
    fgAppSuFileScanned  Counter32
}

fgAppSuIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Index that uniquely identifies a scan unit in the fgAppSuStatsTable"
    ::= { fgAppSuStatsEntry 1 }

fgAppSuFileScanned OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of files scanned by this scan unit"
    ::= { fgAppSuStatsEntry 2 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppVoIP
--

fgAppVoIP OBJECT IDENTIFIER
    ::= { fgApplications 108 }

fgAppVoIPStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgAppVoIPStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of VoIP related statistics per virtual domain"
    ::= { fgAppVoIP 1 }

fgAppVoIPStatsEntry OBJECT-TYPE
    SYNTAX      FgAppVoIPStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "VoIP statistics for a particular virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgAppVoIPStatsTable 1 }

FgAppVoIPStatsEntry ::= SEQUENCE {
    fgAppVoIPConn           Gauge32,
    fgAppVoIPCallBlocked    Counter32
}

fgAppVoIPConn OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The current number of VoIP connections on the virtual domain"
    ::= { fgAppVoIPStatsEntry 1 }
```

```
fgAppVoIPCallBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of VoIP calls blocked (SIP Invites blocked and
         SCCP calls blocked) in this virtual domain"
    ::= { fgAppVoIPStatsEntry 2 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppP2P
--

fgAppP2P OBJECT IDENTIFIER
    ::= { fgApplications 109 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppP2P.fgAppP2PStatsTable
--

fgAppP2PStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgAppP2PStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of P2P protocol related statistics per virtual domain"
    ::= { fgAppP2P 1 }

fgAppP2PStatsEntry OBJECT-TYPE
    SYNTAX      FgAppP2PStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "P2P statistics for a particular virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgAppP2PStatsTable 1 }

FgAppP2PStatsEntry ::= SEQUENCE {
    fgAppP2PConnBlocked     Counter32
}

fgAppP2PConnBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of P2P connections blocked in this virtual domain"
    ::= { fgAppP2PStatsEntry 1 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppP2P.fgAppP2PProtoTable
--

fgAppP2PProtoTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgAppP2PProtoEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of peer to peer statistics per virtual domain per protocol.
         This table has a dependent expansion relationship with fgVdTable."
    ::= { fgAppP2P 2 }

fgAppP2PProtoEntry OBJECT-TYPE
    SYNTAX      FgAppP2PProtoEntry
    MAX-ACCESS  not-accessible
```

```
    STATUS      current
    DESCRIPTION
        "P2P statistics for a particular virtual domain and protocol"
    INDEX       { fgVdEntIndex, fgAppP2PProtEntProto }
    ::= { fgAppP2PProtoTable 1 }

FgAppP2PProtoEntry ::= SEQUENCE {
    fgAppP2PProtEntProto        FgP2PProto,
    fgAppP2PProtEntBytes        Counter64,
    fgAppP2PProtoEntLastReset   TimeTicks
}

fgAppP2PProtEntProto OBJECT-TYPE
    SYNTAX      FgP2PProto
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "P2P protocol this row of statistics is for, within the specified virtual domain"
    ::= { fgAppP2PProtoEntry 1 }

fgAppP2PProtEntBytes OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of bytes transferred through this virtual domain on this P2P protocol
since last reset"
    ::= { fgAppP2PProtoEntry 2 }

fgAppP2PProtoEntLastReset OBJECT-TYPE
    SYNTAX      TimeTicks
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Time elapsed since the corresponding fgAppP2PProtEntBytes was
         last reset to 0."
    ::= { fgAppP2PProtoEntry 3 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppIM
--

fgAppIM OBJECT IDENTIFIER
    ::= { fgApplications 110 }

fgAppIMStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgAppIMStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of instant messaging statistics per virtual domain"
    ::= { fgAppIM 1 }

fgAppIMStatsEntry OBJECT-TYPE
    SYNTAX      FgAppIMStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "IM statistics for a particular virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgAppIMStatsTable 1 }

FgAppIMStatsEntry ::= SEQUENCE {
    fgAppIMMessages         Counter32,
    fgAppIMFileTransfered   Counter32,
```

```
    fgAppIMFileTxBlocked    Counter32,
    fgAppIMConnBlocked      Counter32
}

fgAppIMMessages OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Total number of IM messages processed in this virtual domain"
    ::= { fgAppIMStatsEntry 1 }

fgAppIMFileTransfered OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of files transferred through this virtual domain"
    ::= { fgAppIMStatsEntry 2 }

fgAppIMFileTxBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of blocked file transfers in this virtual domain"
    ::= { fgAppIMStatsEntry 3 }

fgAppIMConnBlocked OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of connections blocked in this virtual domain"
    ::= { fgAppIMStatsEntry 4 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppProxyFTP
--

fgAppProxyFTP OBJECT IDENTIFIER
    ::= { fgApplications 111 }

fgApFTPUpTime OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
        "Up-time of the FTP proxy, in seconds"
    ::= { fgAppProxyFTP 1 }

fgApFTPMemUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
        "FTP Proxy memory utilization, as a percentage of the system total"
    ::= { fgAppProxyFTP 2 }

fgApFTPConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "FTP proxy current connections"
    ::= { fgAppProxyFTP 4 }
```

```
fgApFTPMaxConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Maximum number of connections supported by FTP proxy"
    ::= { fgAppProxyFTP 5 }

fgApFTPStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgApFTPStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of FTP proxy statistics per virtual domain"
    ::= { fgAppProxyFTP 3 }

fgApFTPStatsEntry OBJECT-TYPE
    SYNTAX      FgApFTPStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "FTP Proxy statistics for a particular virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgApFTPStatsTable 1 }

FgApFTPStatsEntry ::= SEQUENCE {
    fgApFTPReqProcessed     Counter32
}

fgApFTPReqProcessed OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of requests in this virtual domain processed by the FTP proxy since start-
up"
    ::= { fgApFTPStatsEntry 1 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppExplicitProxy
--

fgAppExplicitProxy OBJECT IDENTIFIER
    ::= { fgApplications 112 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppExplicitProxy.fgExplicitProxyInfo
--

fgExplicitProxyInfo OBJECT IDENTIFIER
    ::= { fgAppExplicitProxy 1 }

fgExplicitProxyUpTime OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Explicit proxy up-time (in seconds)"
    ::= { fgExplicitProxyInfo 1 }

fgExplicitProxyMemUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
```

```
        "Explicit proxy memory usage (percentage of system total)"
    ::= { fgExplicitProxyInfo 2 }

fgExplicitProxyRequests OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Explicit proxy total number of requests"
    ::= { fgExplicitProxyInfo 3 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppExplicitProxy.fgExplicitProxyStatsTable
--

fgExplicitProxyStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgExplicitProxyStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of explicit proxy statistics per virtual domain"
    ::= { fgAppExplicitProxy 2 }

fgExplicitProxyStatsEntry OBJECT-TYPE
    SYNTAX      FgExplicitProxyStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Explicit proxy statistics for a particular virtual domain"
    INDEX       { fgVdEntIndex }
    ::= { fgExplicitProxyStatsTable 1 }

FgExplicitProxyStatsEntry ::= SEQUENCE {
    fgExplicitProxyUsers     Integer32,
    fgExplicitProxySessions  Integer32
}

fgExplicitProxyUsers OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of current users in this virtual domain"
    ::= { fgExplicitProxyStatsEntry 1 }

fgExplicitProxySessions OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of current sessions in this virtual domain"
    ::= { fgExplicitProxyStatsEntry 2 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppExplicitProxy.fgExplicitProxyScanStatsTable
--

fgExplicitProxyScanStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgExplicitProxyScanStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of explicit proxy scan statistics per virtual domain"
    ::= { fgAppExplicitProxy 3 }
```

```
fgExplicitProxyScanStatsEntry OBJECT-TYPE
    SYNTAX      FgExplicitProxyScanStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Explicit proxy scan statistics for a particular virtual domain"
    INDEX       { fgVdEntIndex, fgExplicitProxyScanStatsDisp }
    ::= { fgExplicitProxyScanStatsTable 1 }

FgExplicitProxyScanStatsEntry ::= SEQUENCE {
    fgExplicitProxyScanStatsDisp     FgScanAvDisposition,
    fgExplicitProxyVirus             Counter32,
    fgExplicitProxyBannedWords       Counter32,
    fgExplicitProxyPolicy            Counter32,
    fgExplicitProxyOversized         Counter32,
    fgExplicitProxyArchNest          Counter32,
    fgExplicitProxyArchSize          Counter32,
    fgExplicitProxyArchEncrypted     Counter32,
    fgExplicitProxyArchMultiPart     Counter32,
    fgExplicitProxyArchUnsupported   Counter32,
    fgExplicitProxyArchBomb          Counter32,
    fgExplicitProxyArchCorrupt       Counter32
}

fgExplicitProxyScanStatsDisp OBJECT-TYPE
    SYNTAX      FgScanAvDisposition
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Disposition of an Scan result"
   ::= { fgExplicitProxyScanStatsEntry 1 }

fgExplicitProxyVirus OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of viruses in this virtual domain"
    ::= { fgExplicitProxyScanStatsEntry 2 }

fgExplicitProxyBannedWords OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of elements containing banned words in this virtual domain"
    ::= { fgExplicitProxyScanStatsEntry 3 }

fgExplicitProxyPolicy OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of elements violating policy (e.g. filename or file type rules) in this
virtual domain"
    ::= { fgExplicitProxyScanStatsEntry 4 }

fgExplicitProxyOversized OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of oversized elements in this virtual domain"
    ::= { fgExplicitProxyScanStatsEntry 5 }
```

```
    fgExplicitProxyArchNest OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of too deeply nested archives in this virtual domain"
        ::= { fgExplicitProxyScanStatsEntry 6 }

    fgExplicitProxyArchSize OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of archives that decompress beyond size limit in this virtual domain"
        ::= { fgExplicitProxyScanStatsEntry 7 }

    fgExplicitProxyArchEncrypted OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of encrypted archives in this virtual domain"
        ::= { fgExplicitProxyScanStatsEntry 8 }

    fgExplicitProxyArchMultiPart OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of multipart archives in this virtual domain"
        ::= { fgExplicitProxyScanStatsEntry 9 }

    fgExplicitProxyArchUnsupported OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of archives with unsupported (but known) formats in this virtual domain"
        ::= { fgExplicitProxyScanStatsEntry 10 }

    fgExplicitProxyArchBomb OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of archive bombs in this virtual domain"
        ::= { fgExplicitProxyScanStatsEntry 11 }

    fgExplicitProxyArchCorrupt OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of corrupt archives in this virtual domain"
        ::= { fgExplicitProxyScanStatsEntry 12 }

    --
    --
    fortinet.fnFortiGateMib.fgApplications.fgAppExplicitProxy.fgExplicitProxyScriptStatsTable
    --

    fgExplicitProxyScriptStatsTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF FgExplicitProxyScriptStatsEntry
        MAX-ACCESS  not-accessible
        STATUS      current
```

```
    DESCRIPTION
        "A table of explicit proxy script filtering statistics per virtual domain"
    ::= { fgAppExplicitProxy 4 }

fgExplicitProxyScriptStatsEntry OBJECT-TYPE
    SYNTAX      FgExplicitProxyScriptStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Explicit proxy scan statistics for a particular virtual domain"
    INDEX       { fgVdEntIndex }
    ::= { fgExplicitProxyScriptStatsTable 1 }

FgExplicitProxyScriptStatsEntry ::= SEQUENCE {
    fgExplicitProxyFilteredApplets   Counter32,
    fgExplicitProxyFilteredActiveX   Counter32,
    fgExplicitProxyFilteredJScript   Counter32,
    fgExplicitProxyFilteredJS        Counter32,
    fgExplicitProxyFilteredVBS       Counter32,
    fgExplicitProxyFilteredOthScript Counter32
}

fgExplicitProxyFilteredApplets OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of applets filtered from files in this virtual domain"
    ::= { fgExplicitProxyScriptStatsEntry 1 }

fgExplicitProxyFilteredActiveX OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of ActiveX scripts filtered from files in this virtual domain"
    ::= { fgExplicitProxyScriptStatsEntry 2 }

fgExplicitProxyFilteredJScript OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of JScript scripts filtered from files in this virtual domain"
    ::= { fgExplicitProxyScriptStatsEntry 3 }

fgExplicitProxyFilteredJS OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of JavaScript scripts filtered from files in this virtual domain"
    ::= { fgExplicitProxyScriptStatsEntry 4 }

fgExplicitProxyFilteredVBS OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of Visual Basic scripts filtered from files in this virtual domain"
    ::= { fgExplicitProxyScriptStatsEntry 5 }

fgExplicitProxyFilteredOthScript OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
```

```
    STATUS      current
    DESCRIPTION
        "Number of other types of scripts filtered from files in this virtual domain"
    ::= { fgExplicitProxyScriptStatsEntry 6 }

--
--
fortinet.fnFortiGateMib.fgApplications.fgAppExplicitProxy.fgExplicitProxyFilterStatsTable
--

fgExplicitProxyFilterStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgExplicitProxyFilterStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of explicit proxy policy enforcement statistics per virtual domain"
    ::= { fgAppExplicitProxy 5 }

fgExplicitProxyFilterStatsEntry OBJECT-TYPE
    SYNTAX      FgExplicitProxyFilterStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Explicit proxy scan statistics for a particular virtual domain"
    INDEX       { fgVdEntIndex }
    ::= { fgExplicitProxyFilterStatsTable 1 }

FgExplicitProxyFilterStatsEntry ::= SEQUENCE {
    fgExplicitProxyBlockedDLP        Counter32,
    fgExplicitProxyBlockedConType    Counter32,
    fgExplicitProxyExaminedURLs      Counter32,
    fgExplicitProxyAllowedURLs       Counter32,
    fgExplicitProxyBlockedURLs       Counter32,
    fgExplicitProxyLoggedURLs        Counter32,
    fgExplicitProxyOverriddenURLs    Counter32
}

fgExplicitProxyBlockedDLP OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of elements blocked due to Data Leak Prevention in this virtual domain"
    ::= { fgExplicitProxyFilterStatsEntry 1 }

fgExplicitProxyBlockedConType OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of elements blocked due to Content-Type filtering rules in this virtual
domain"
    ::= { fgExplicitProxyFilterStatsEntry 2 }

fgExplicitProxyExaminedURLs OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of URLs inspected against filtering rules in this virtual domain"
    ::= { fgExplicitProxyFilterStatsEntry 3 }

fgExplicitProxyAllowedURLs OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
```

```
    STATUS      current
    DESCRIPTION
        "Number of URLs explicitly allowed due to filtering rules in this virtual domain"
    ::= { fgExplicitProxyFilterStatsEntry 4 }

fgExplicitProxyBlockedURLs OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of URLs explicitly blocked due to filtering rules in this virtual domain"
    ::= { fgExplicitProxyFilterStatsEntry 5 }

fgExplicitProxyLoggedURLs OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of URLs logged due to filtering rules in this virtual domain"
    ::= { fgExplicitProxyFilterStatsEntry 6 }

fgExplicitProxyOverriddenURLs OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of URLs access due to overriding filtering rules in this virtual domain"
    ::= { fgExplicitProxyFilterStatsEntry 7 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppWebCache
--

fgAppWebCache OBJECT IDENTIFIER
    ::= { fgApplications 113 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppWebCache.fgWebCacheInfo
--

fgWebCacheInfo OBJECT IDENTIFIER
    ::= { fgAppWebCache 1 }

fgWebCacheRAMLimit OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "RAM available for web cache in bytes"
    ::= { fgWebCacheInfo 1 }

fgWebCacheRAMUsage OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "RAM used by web cache in bytes"
    ::= { fgWebCacheInfo 2 }

fgWebCacheRAMHits OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of cache hits in RAM since last reset"
```

```
    ::= { fgWebCacheInfo 3 }

fgWebCacheRAMMisses OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of cache misses in RAM since last reset"
    ::= { fgWebCacheInfo 4 }

fgWebCacheRequests OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of cache requests since last reset"
    ::= { fgWebCacheInfo 5 }

fgWebCacheBypass OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of cache bypasses since last reset"
    ::= { fgWebCacheInfo 6 }

fgWebCacheUpTime OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Web Cache up-time (in seconds)"
    ::= { fgWebCacheInfo 7 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppWebCache.fgWebCacheDiskStatsTable
--

fgWebCacheDiskStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgWebCacheDiskStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of the Web Cache disk statistics per disk"
    ::= { fgAppWebCache 2 }

fgWebCacheDiskStatsEntry OBJECT-TYPE
    SYNTAX      FgWebCacheDiskStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The Web Cache disk statistics for a particular disk"
    INDEX       { fgWebCacheDisk }
    ::= { fgWebCacheDiskStatsTable 1 }

FgWebCacheDiskStatsEntry ::= SEQUENCE {
    fgWebCacheDisk              Unsigned32,
    fgWebCacheDiskLimit         CounterBasedGauge64,
    fgWebCacheDiskUsage         CounterBasedGauge64,
    fgWebCacheDiskHits          Counter32,
    fgWebCacheDiskMisses        Counter32,
    fgWebCacheDiskFailure       Counter64
}

fgWebCacheDisk OBJECT-TYPE
```

```
    SYNTAX     Unsigned32
    MAX-ACCESS not-accessible
    STATUS     current
    DESCRIPTION
        "The Web Cache Disk index"
    ::= { fgWebCacheDiskStatsEntry 1 }

fgWebCacheDiskLimit OBJECT-TYPE
    SYNTAX     CounterBasedGauge64
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "The about of storage (in bytes) available for the Web Cache on a particular disk"
    ::= { fgWebCacheDiskStatsEntry 2 }

fgWebCacheDiskUsage OBJECT-TYPE
    SYNTAX     CounterBasedGauge64
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "The about of storage (in bytes) in use by the Web Cache on a paricular disk"
    ::= { fgWebCacheDiskStatsEntry 3 }

fgWebCacheDiskHits OBJECT-TYPE
    SYNTAX     Counter32
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "The number of cache hits on a paricular disk"
    ::= { fgWebCacheDiskStatsEntry 4 }

fgWebCacheDiskMisses OBJECT-TYPE
    SYNTAX     Counter32
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "The number of cache misses on a paricular disk"
    ::= { fgWebCacheDiskStatsEntry 5 }

fgWebCacheDiskFailure OBJECT-TYPE
    SYNTAX     Counter64
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "The number of disk failures on a paricular disk from webcache disk daemon"
    ::= { fgWebCacheDiskStatsEntry 6 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppWanOpt
--

fgAppWanOpt OBJECT IDENTIFIER
    ::= { fgApplications 114 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppWanOpt.fgWanOptInfo
--

fgWanOptInfo OBJECT IDENTIFIER
    ::= { fgAppWanOpt 1 }

fgMemCacheLimit OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
        "RAM available for mem cache in bytes"
    ::= { fgWanOptInfo 1 }

fgMemCacheUsage OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "RAM used by mem cache in bytes"
    ::= { fgWanOptInfo 2 }

fgMemCacheHits OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of hits in mem cache since last reset"
    ::= { fgWanOptInfo 3 }

fgMemCacheMisses OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of misses in mem cache since last reset"
    ::= { fgWanOptInfo 4 }

fgByteCacheRAMLimit OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "RAM available for byte cache in bytes"
    ::= { fgWanOptInfo 5 }

fgByteCacheRAMUsage OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "RAM used by byte cache in bytes"
    ::= { fgWanOptInfo 6 }

fgWanOptUpTime OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wan Optimization up-time (in seconds)"
    ::= { fgWanOptInfo 7 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppWanOpt.fgWanOptStatsTable
--

fgWanOptStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgWanOptStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of WAN optimization statistics per virtual domain"
    ::= { fgAppWanOpt 2 }

fgWanOptStatsEntry OBJECT-TYPE
```

```
    SYNTAX      FgWanOptStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "WAN optimization statistics for a particular virtual domain"
    INDEX       { fgVdEntIndex }
    ::= { fgWanOptStatsTable 1 }

FgWanOptStatsEntry ::= SEQUENCE {
    fgWanOptTunnels     Gauge32,
    fgWanOptLANBytesIn  Gauge32,
    fgWanOptLANBytesOut Gauge32,
    fgWanOptWANBytesIn  Gauge32,
    fgWanOptWANBytesOut Gauge32
}

fgWanOptTunnels OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of current tunnels in this virtual domain"
    ::= { fgWanOptStatsEntry 1 }

fgWanOptLANBytesIn OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of bytes received on LAN in last 5 seconds"
    ::= { fgWanOptStatsEntry 2 }

fgWanOptLANBytesOut OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of bytes sent on LAN in last 5 seconds"
    ::= { fgWanOptStatsEntry 3 }

fgWanOptWANBytesIn OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of bytes received on WAN in last 5 seconds"
    ::= { fgWanOptStatsEntry 4 }

fgWanOptWANBytesOut OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of bytes sent on WAN in last 5 seconds"
    ::= { fgWanOptStatsEntry 5 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppWanOpt.fgWanOptHistoryStatsTable
--

fgWanOptHistoryStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgWanOptHistoryStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
```

```
        "A table of the WAN optimization history per protocol"
    ::= { fgAppWanOpt 3 }

fgWanOptHistoryStatsEntry OBJECT-TYPE
    SYNTAX      FgWanOptHistoryStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The WAN optimization history for a particular virtual domain, period, and
protocol"
    INDEX       { fgVdEntIndex, fgWanOptHistPeriod, fgWanOptProtocol }
    ::= { fgWanOptHistoryStatsTable 1 }

FgWanOptHistoryStatsEntry ::= SEQUENCE {
    fgWanOptHistPeriod          FgWanOptHistPeriods,
    fgWanOptProtocol            FgWanOptProtocols,
    fgWanOptReductionRate       Gauge32,
    fgWanOptLanTraffic          CounterBasedGauge64,
    fgWanOptWanTraffic          CounterBasedGauge64
}

fgWanOptHistPeriod OBJECT-TYPE
    SYNTAX      FgWanOptHistPeriods
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "WAN optimization table entry period"
    ::= { fgWanOptHistoryStatsEntry 1 }

fgWanOptProtocol OBJECT-TYPE
    SYNTAX      FgWanOptProtocols
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Internal WAN optimization table entry protocol"
    ::= { fgWanOptHistoryStatsEntry 2 }

fgWanOptReductionRate OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Reduction rate achieved by WAN optimization"
    ::= { fgWanOptHistoryStatsEntry 3 }

fgWanOptLanTraffic OBJECT-TYPE
    SYNTAX      CounterBasedGauge64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of bytes transferred via LAN"
    ::= { fgWanOptHistoryStatsEntry 4 }

fgWanOptWanTraffic OBJECT-TYPE
    SYNTAX      CounterBasedGauge64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of bytes transferred via WAN"
    ::= { fgWanOptHistoryStatsEntry 5 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppWanOpt.fgWanOptTrafficStatsTable
--
```

```
fgWanOptTrafficStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgWanOptTrafficStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of the WAN optimization traffic for a particular virtual domain and
protocol"
    ::= { fgAppWanOpt 4 }

fgWanOptTrafficStatsEntry OBJECT-TYPE
    SYNTAX      FgWanOptTrafficStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The WAN optimization history for a particular protocol"
    INDEX       { fgVdEntIndex, fgWanOptProtocol }
    ::= { fgWanOptTrafficStatsTable 1 }

FgWanOptTrafficStatsEntry ::= SEQUENCE {
    fgWanOptLanInTraffic        Counter64,
    fgWanOptLanOutTraffic       Counter64,
    fgWanOptWanInTraffic        Counter64,
    fgWanOptWanOutTraffic       Counter64
}

fgWanOptLanInTraffic OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Amount of traffic received from the LAN by WAN optimization"
    ::= { fgWanOptTrafficStatsEntry 1 }

fgWanOptLanOutTraffic OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Amount of traffic sent to the LAN by WAN optimization"
    ::= { fgWanOptTrafficStatsEntry 2 }

fgWanOptWanInTraffic OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Amount of traffic received from the WAN by WAN optimization"
    ::= { fgWanOptTrafficStatsEntry 3 }

fgWanOptWanOutTraffic OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Amount of traffic sent to the WAN by WAN optimization"
    ::= { fgWanOptTrafficStatsEntry 4 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppWanOpt.fgWanOptDiskStatsTable
--

fgWanOptDiskStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgWanOptDiskStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
```

```
    DESCRIPTION
        "A table of the Web Cache disk statistics per disk"
    ::= { fgAppWanOpt 5 }

fgWanOptDiskStatsEntry OBJECT-TYPE
    SYNTAX      FgWanOptDiskStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The Web Cache disk statistics for a particular disk"
    INDEX       { fgWanOptDisk }
    ::= { fgWanOptDiskStatsTable 1 }

FgWanOptDiskStatsEntry ::= SEQUENCE {
    fgWanOptDisk              Unsigned32,
    fgWanOptDiskLimit         CounterBasedGauge64,
    fgWanOptDiskUsage         CounterBasedGauge64,
    fgWanOptDiskHits          Counter32,
    fgWanOptDiskMisses        Counter32,
    fgWanOptDiskFailure       Counter64
}

fgWanOptDisk OBJECT-TYPE
    SYNTAX     Unsigned32
    MAX-ACCESS not-accessible
    STATUS     current
    DESCRIPTION
        "The Web Cache Disk index"
    ::= { fgWanOptDiskStatsEntry 1 }

fgWanOptDiskLimit OBJECT-TYPE
    SYNTAX     CounterBasedGauge64
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "The about of storage (in bytes) available for the Web Cache on a particular disk"
    ::= { fgWanOptDiskStatsEntry 2 }

fgWanOptDiskUsage OBJECT-TYPE
    SYNTAX     CounterBasedGauge64
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "The about of storage (in bytes) in use by the Web Cache on a paricular disk"
    ::= { fgWanOptDiskStatsEntry 3 }

fgWanOptDiskHits OBJECT-TYPE
    SYNTAX     Counter32
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "The number of cache hits on a paricular disk"
    ::= { fgWanOptDiskStatsEntry 4 }

fgWanOptDiskMisses OBJECT-TYPE
    SYNTAX     Counter32
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "The number of cache misses on a paricular disk"
    ::= { fgWanOptDiskStatsEntry 5 }

fgWanOptDiskFailure OBJECT-TYPE
    SYNTAX     Counter64
    MAX-ACCESS read-only
```

```
    STATUS     current
    DESCRIPTION
        "The number of disk failures on a paricular disk from wanopt disk daemon"
    ::= { fgWanOptDiskStatsEntry 6 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppDNSProxy
--

fgAppDNSProxy OBJECT IDENTIFIER
    ::= { fgApplications 115 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppDNSProxy.fgDNSProxyStatsInfo
--

fgDNSProxyStatsInfo OBJECT IDENTIFIER
    ::= { fgAppDNSProxy 1 }

fgDNSProxyStatsUdpCacheHit OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of DNS cache hit"
    ::= { fgDNSProxyStatsInfo 1 }

fgDNSProxyStatsUdpRatingCacheHit OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of secure-DNS cache hit"
    ::= { fgDNSProxyStatsInfo 2 }

fgDNSProxyStatsUdpReq OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of DNS request"
    ::= { fgDNSProxyStatsInfo 3 }

fgDNSProxyStatsUdpRes OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of DNS response"
    ::= { fgDNSProxyStatsInfo 4 }

fgDNSProxyStatsUdpFwd OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of DNS forwarded"
    ::= { fgDNSProxyStatsInfo 5 }

fgDNSProxyStatsUdpRetrans OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of DNS retransmission"
```

```
    ::= { fgDNSProxyStatsInfo 6 }

fgDNSProxyStatsUdpTo OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of DNS timeout"
    ::= { fgDNSProxyStatsInfo 7 }

fgDNSProxyStatsUdpFtgRes OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of secure-DNS response"
    ::= { fgDNSProxyStatsInfo 8 }

fgDNSProxyStatsUdpFtgFwd OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of secure-DNS forwarded"
    ::= { fgDNSProxyStatsInfo 9 }

fgDNSProxyStatsUdpFtgRetrans OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of secure-DNS retransmission"
    ::= { fgDNSProxyStatsInfo 10 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppFnbam
--

fgAppFnbam OBJECT IDENTIFIER
    ::= { fgApplications 116 }

--
-- fortinet.fnFortiGateMib.fgApplications.fgAppFnbam.fgAppFnbamStatsInfo
--

fgAppFnbamStatsInfo OBJECT IDENTIFIER
    ::= { fgAppFnbam 1 }

fgAppFnbamStatsTotalAuthReqs OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of total authentication requests"
    ::= { fgAppFnbamStatsInfo 1 }

fgAppFnbamStatsTotalEagainErrs OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of total EAGAIN errors"
    ::= { fgAppFnbamStatsInfo 2 }

fgAppFnbamStatsTotalLdapFails OBJECT-TYPE
```

```
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of total LDAP connection failures"
    ::= { fgAppFnbamStatsInfo 3 }

--
-- fortinet.fnFortiGateMib.fgInetProto
--

fgInetProto OBJECT IDENTIFIER
    ::= { fnFortiGateMib 11 }

fgInetProtoInfo OBJECT IDENTIFIER
    ::= { fgInetProto 1 }

fgInetProtoTables OBJECT IDENTIFIER
    ::= { fgInetProto 2 }

--
-- fortinet.fnFortiGateMib.fgInetProto.fgInetProtoTables.fgIpSessTable
--

fgIpSessTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgIpSessEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Information on the IP sessions active on the device"
    ::= { fgInetProtoTables 1 }

fgIpSessEntry OBJECT-TYPE
    SYNTAX      FgIpSessEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Information on a specific session, including source and destination"
    INDEX       { fgIpSessIndex }
    ::= { fgIpSessTable 1 }

FgIpSessEntry ::= SEQUENCE {
    fgIpSessIndex       FnIndex,
    fgIpSessProto       FgSessProto,
    fgIpSessFromAddr    IpAddress,
    fgIpSessFromPort    InetPortNumber,
    fgIpSessToAddr      IpAddress,
    fgIpSessToPort      InetPortNumber,
    fgIpSessExp         Gauge32,
    fgIpSessVdom        FgVdIndex
}

fgIpSessIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An index value that uniquely identifies
         an IP session within the fgIpSessTable"
    ::= { fgIpSessEntry 1 }

fgIpSessProto OBJECT-TYPE
    SYNTAX      FgSessProto
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
        "The protocol the session is using (IP, TCP, UDP, etc.)"
    ::= { fgIpSessEntry 2 }

fgIpSessFromAddr OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Source IP address (IPv4 only) of the session"
    ::= { fgIpSessEntry 3 }

fgIpSessFromPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Source port number (UDP and TCP only) of the session"
    ::= { fgIpSessEntry 4 }

fgIpSessToAddr OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Destination IP address (IPv4 only) of the session"
    ::= { fgIpSessEntry 5 }

fgIpSessToPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Destination Port number (UDP and TCP only) of the session"
    ::= { fgIpSessEntry 6 }

fgIpSessExp OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of seconds remaining before the session expires (if idle)"
    ::= { fgIpSessEntry 7 }

fgIpSessVdom OBJECT-TYPE
    SYNTAX      FgVdIndex
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Virtual domain the session is part of. This index corresponds to the index used
by fgVdTable."
    ::= { fgIpSessEntry 8 }

--
-- fortinet.fnFortiGateMib.fgInetProto.fgInetProtoTables.fgIpSessStatsTable
--

fgIpSessStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgIpSessStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "IP session statistics table"
    ::= { fgInetProtoTables 2 }
```

```
fgIpSessStatsEntry OBJECT-TYPE
    SYNTAX      FgIpSessStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "IP session statistics on a virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgIpSessStatsTable 1 }

FgIpSessStatsEntry ::= SEQUENCE {
    fgIpSessNumber  Gauge32
}

fgIpSessNumber OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current number of sessions on the virtual domain"
    ::= { fgIpSessStatsEntry 1 }

--
-- fortinet.fnFortiGateMib.fgInetProto.fgInetProtoTables.fgIp6SessStatsTable
--

fgIp6SessStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgIp6SessStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "IP session statistics table"
    ::= { fgInetProtoTables 3 }

fgIp6SessStatsEntry OBJECT-TYPE
    SYNTAX      FgIp6SessStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "IP session statistics on a virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgIp6SessStatsTable 1 }

FgIp6SessStatsEntry ::= SEQUENCE {
    fgIp6SessNumber  Gauge32
}

fgIp6SessNumber OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current number of sessions on the virtual domain"
    ::= { fgIp6SessStatsEntry 1 }


--
-- fortinet.fnFortiGateMib.fgVpn
--

fgVpn OBJECT IDENTIFIER
    ::= { fnFortiGateMib 12 }

--
-- fortinet.fnFortiGateMib.fgVpn.fgVpnInfo
--
```

```
fgVpnInfo OBJECT IDENTIFIER
    ::= { fgVpn 1 }

fgVpnTunnelUpCount OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of IPsec VPN tunnels with at least one SA"
    ::= { fgVpnInfo 1 }

--
-- fortinet.fnFortiGateMib.fgVpn.fgVpnTables
--

fgVpnTables OBJECT IDENTIFIER
    ::= { fgVpn 2 }

--
-- fortinet.fnFortiGateMib.fgVpn.fgVpnTables.fgVpnDialupTable
--

fgVpnDialupTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgVpnDialupEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Dial-up VPN peers information"
    ::= { fgVpnTables 1 }

fgVpnDialupEntry OBJECT-TYPE
    SYNTAX      FgVpnDialupEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Dial-up VPN peer info"
    INDEX       { fgVpnDialupIndex }
    ::= { fgVpnDialupTable 1 }

FgVpnDialupEntry ::= SEQUENCE {
    fgVpnDialupIndex        FnIndex,
    fgVpnDialupGateway      IpAddress,
    fgVpnDialupLifetime     Integer32,
    fgVpnDialupTimeout      Integer32,
    fgVpnDialupSrcBegin     IpAddress,
    fgVpnDialupSrcEnd       IpAddress,
    fgVpnDialupDstAddr      IpAddress,
    fgVpnDialupVdom         FgVdIndex,
    fgVpnDialupInOctets     Counter64,
    fgVpnDialupOutOctets    Counter64
}

fgVpnDialupIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An index value that uniquely identifies
         an VPN dial-up peer within the fgVpnDialupTable"
    ::= { fgVpnDialupEntry 1 }

fgVpnDialupGateway OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
```

```
    STATUS      current
    DESCRIPTION
        "Remote gateway IP address of the tunnel"
    ::= { fgVpnDialupEntry 2 }

fgVpnDialupLifetime OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Tunnel life time (seconds) of the tunnel"
    ::= { fgVpnDialupEntry 3 }

fgVpnDialupTimeout OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Time before the next key exchange (seconds) of the tunnel"
    ::= { fgVpnDialupEntry 4 }

fgVpnDialupSrcBegin OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Remote subnet address of the tunnel"
    ::= { fgVpnDialupEntry 5 }

fgVpnDialupSrcEnd OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Remote subnet mask of the tunnel"
    ::= { fgVpnDialupEntry 6 }

fgVpnDialupDstAddr OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Local subnet address of the tunnel"
    ::= { fgVpnDialupEntry 7 }

fgVpnDialupVdom OBJECT-TYPE
    SYNTAX      FgVdIndex
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Virtual domain tunnel is part of. This index corresponds to the index used by
fgVdTable."
    ::= { fgVpnDialupEntry 8 }

fgVpnDialupInOctets OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of bytes received on tunnel since instantiation."
    ::= { fgVpnDialupEntry 9 }

fgVpnDialupOutOctets OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
```

```
    STATUS      current
    DESCRIPTION
        "Number of bytes sent on tunnel since instantiation."
    ::= { fgVpnDialupEntry 10 }

--
-- fortinet.fnFortiGateMib.fgVpn.fgVpnTables.fgVpnTunTable
--

fgVpnTunTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgVpnTunEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Table of non-dial-up IPsec VPN tunnels"
    ::= { fgVpnTables 2 }

fgVpnTunEntry OBJECT-TYPE
    SYNTAX      FgVpnTunEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Tunnel VPN peer info"
    INDEX       { fgVpnTunEntIndex }
    ::= { fgVpnTunTable 1 }

FgVpnTunEntry ::= SEQUENCE {
    fgVpnTunEntIndex                FnIndex,
    fgVpnTunEntPhase1Name           DisplayString,
    fgVpnTunEntPhase2Name           DisplayString,
    fgVpnTunEntRemGwyIp             IpAddress,
    fgVpnTunEntRemGwyPort           InetPortNumber,
    fgVpnTunEntLocGwyIp             IpAddress,
    fgVpnTunEntLocGwyPort           InetPortNumber,
    fgVpnTunEntSelectorSrcBeginIp   IpAddress,
    fgVpnTunEntSelectorSrcEndIp     IpAddress,
    fgVpnTunEntSelectorSrcPort      InetPortNumber,
    fgVpnTunEntSelectorDstBeginIp   IpAddress,
    fgVpnTunEntSelectorDstEndIp     IpAddress,
    fgVpnTunEntSelectorDstPort      InetPortNumber,
    fgVpnTunEntSelectorProto        Integer32,
    fgVpnTunEntLifeSecs             Gauge32,
    fgVpnTunEntLifeBytes            Gauge32,
    fgVpnTunEntTimeout              Gauge32,
    fgVpnTunEntInOctets             Counter64,
    fgVpnTunEntOutOctets            Counter64,
    fgVpnTunEntStatus               INTEGER,
    fgVpnTunEntVdom                 FgVdIndex
}

fgVpnTunEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An index value that uniquely identifies
         a VPN tunnel within the fgVpnTunTable"
    ::= { fgVpnTunEntry 1 }

fgVpnTunEntPhase1Name OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Descriptive name of phase1 configuration for the tunnel"
```

```
    ::= { fgVpnTunEntry 2 }

fgVpnTunEntPhase2Name OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Descriptive name of phase2 configuration for the tunnel"
    ::= { fgVpnTunEntry 3 }

fgVpnTunEntRemGwyIp OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "IP of remote gateway used by the tunnel"
    ::= { fgVpnTunEntry 4 }

fgVpnTunEntRemGwyPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "port of remote gateway used by tunnel, if UDP"
    ::= { fgVpnTunEntry 5 }

fgVpnTunEntLocGwyIp OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "IP of local gateway used by the tunnel"
    ::= { fgVpnTunEntry 6 }

fgVpnTunEntLocGwyPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "port of local gateway used by tunnel, if UDP"
    ::= { fgVpnTunEntry 7 }

fgVpnTunEntSelectorSrcBeginIp OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Beginning of address range of source selector"
    ::= { fgVpnTunEntry 8 }

fgVpnTunEntSelectorSrcEndIp OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "End of address range of source selector"
    ::= { fgVpnTunEntry 9 }

fgVpnTunEntSelectorSrcPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Source selector port"
    ::= { fgVpnTunEntry 10 }
```

```
fgVpnTunEntSelectorDstBeginIp OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Beginning of address range of destination
         selector"
    ::= { fgVpnTunEntry 11 }

fgVpnTunEntSelectorDstEndIp OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "End of address range of destination selector"
    ::= { fgVpnTunEntry 12 }

fgVpnTunEntSelectorDstPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Destination selector port"
    ::= { fgVpnTunEntry 13 }

fgVpnTunEntSelectorProto OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Protocol number for selector"
    ::= { fgVpnTunEntry 14 }

fgVpnTunEntLifeSecs OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Lifetime of tunnel in seconds, if time based lifetime used"
    ::= { fgVpnTunEntry 15 }

fgVpnTunEntLifeBytes OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Lifetime of tunnel in bytes, if byte transfer based lifetime used"
    ::= { fgVpnTunEntry 16 }

fgVpnTunEntTimeout OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Timeout of tunnel in seconds"
    ::= { fgVpnTunEntry 17 }

fgVpnTunEntInOctets OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of bytes received on tunnel"
    ::= { fgVpnTunEntry 18 }
```

```
fgVpnTunEntOutOctets OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of bytes sent out on tunnel"
    ::= { fgVpnTunEntry 19 }

fgVpnTunEntStatus OBJECT-TYPE
    SYNTAX      INTEGER { down(1), up(2) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current status of tunnel (up or down)"
    ::= { fgVpnTunEntry 20 }

fgVpnTunEntVdom OBJECT-TYPE
    SYNTAX      FgVdIndex
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Virtual domain the tunnel is part of. This index corresponds to the index used by
fgVdTable."
    ::= { fgVpnTunEntry 21 }

--
-- fortinet.fnFortiGateMib.fgVpn.fgVpnTables.fgVpnSslStatsTable
--

fgVpnSslStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgVpnSslStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "SSL VPN statistics table"
    ::= { fgVpnTables 3 }

fgVpnSslStatsEntry OBJECT-TYPE
    SYNTAX      FgVpnSslStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "SSL VPN statistics for a given virtual domain"
    AUGMENTS    { fgVdEntry }
    ::= { fgVpnSslStatsTable 1 }

FgVpnSslStatsEntry ::= SEQUENCE {
    fgVpnSslState                   FnBoolState,
    fgVpnSslStatsLoginUsers         Gauge32,
    fgVpnSslStatsMaxUsers           Counter32,
    fgVpnSslStatsActiveWebSessions  Gauge32,
    fgVpnSslStatsMaxWebSessions     Counter32,
    fgVpnSslStatsActiveTunnels      Gauge32,
    fgVpnSslStatsMaxTunnels         Counter32
}

fgVpnSslState OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Whether SSL-VPN is enabled on this virtual domain"
    ::= { fgVpnSslStatsEntry 1 }
```

```
fgVpnSslStatsLoginUsers OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The current number of users logged in through SSL-VPN tunnels in the virtual
domain"
    ::= { fgVpnSslStatsEntry 2 }

fgVpnSslStatsMaxUsers OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The maximum number of total users that can be logged in
         at any one time on the virtual domain"
    ::= { fgVpnSslStatsEntry 3 }

fgVpnSslStatsActiveWebSessions OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The current number of active SSL web sessions in the virtual domain"
    ::= { fgVpnSslStatsEntry 4 }

fgVpnSslStatsMaxWebSessions OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The maximum number of active SSL web sessions
         at any one time within the virtual domain"
    ::= { fgVpnSslStatsEntry 5 }

fgVpnSslStatsActiveTunnels OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The current number of active SSL tunnels in the virtual domain"
    ::= { fgVpnSslStatsEntry 6 }

fgVpnSslStatsMaxTunnels OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The maximum number of active SSL tunnels
         at any one time in the virtual domain"
    ::= { fgVpnSslStatsEntry 7 }

--
-- fortinet.fnFortiGateMib.fgVpn.fgVpnTables.fgVpnSslTunnelTable
--

fgVpnSslTunnelTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgVpnSslTunnelEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A list of active SSL VPN tunnel entries"
    ::= { fgVpnTables 4 }

fgVpnSslTunnelEntry OBJECT-TYPE
```

```
    SYNTAX      FgVpnSslTunnelEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An SSL VPN tunnel entry containing connection information
         and traffic statistics"
    INDEX       { fgVpnSslTunnelIndex }
    ::= { fgVpnSslTunnelTable 1 }

FgVpnSslTunnelEntry ::= SEQUENCE {
    fgVpnSslTunnelIndex     FnIndex,
    fgVpnSslTunnelVdom      FgVdIndex,
    fgVpnSslTunnelUserName  DisplayString,
    fgVpnSslTunnelSrcIp     IpAddress,
    fgVpnSslTunnelIp        IpAddress,
    fgVpnSslTunnelUpTime    Counter32,
    fgVpnSslTunnelBytesIn   Counter64,
    fgVpnSslTunnelBytesOut  Counter64
}

fgVpnSslTunnelIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An index value that uniquely identifies
         an active SSL VPN tunnel within the fgVpnSslTunnelTable"
    ::= { fgVpnSslTunnelEntry 1 }

fgVpnSslTunnelVdom OBJECT-TYPE
    SYNTAX      FgVdIndex
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The index of the virtual domain this tunnel belongs to. This index corresponds to
the index used by fgVdTable."
    ::= { fgVpnSslTunnelEntry 2 }

fgVpnSslTunnelUserName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The user name used to authenticate the tunnel"
    ::= { fgVpnSslTunnelEntry 3 }

fgVpnSslTunnelSrcIp OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The source IP address of this tunnel"
    ::= { fgVpnSslTunnelEntry 4 }

fgVpnSslTunnelIp OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The connection IP address of this tunnel"
    ::= { fgVpnSslTunnelEntry 5 }

fgVpnSslTunnelUpTime OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
```

```
    STATUS      current
    DESCRIPTION
        "The up-time of this tunnel in seconds"
    ::= { fgVpnSslTunnelEntry 6 }

fgVpnSslTunnelBytesIn OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of incoming bytes of L2 traffic through this tunnel since it was
established"
    ::= { fgVpnSslTunnelEntry 7 }

fgVpnSslTunnelBytesOut OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of outgoing bytes of L2 traffic through this tunnel since it was
established"
    ::= { fgVpnSslTunnelEntry 8 }

--
-- fortinet.fnFortiGateMib.fgVpn.fgVpnTrapObjects
--

fgVpnTrapObjects OBJECT IDENTIFIER
    ::= { fgVpn 3 }

fgVpnTrapLocalGateway OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Local gateway IP address. Used in VPN related traps."
    ::= { fgVpnTrapObjects 2 }

fgVpnTrapRemoteGateway OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Remote gateway IP address. Used in VPN related traps."
    ::= { fgVpnTrapObjects 3 }

fgVpnTrapPhase1Name OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Name of the phase 1. Used in VPN related traps."
    ::= { fgVpnTrapObjects 4 }

--
-- fortinet.fnFortiGateMib.fgHighAvailability
--

fgHighAvailability OBJECT IDENTIFIER
    ::= { fnFortiGateMib 13 }

--
-- fortinet.fnFortiGateMib.fgHighAvailability.fgHaInfo
--
```

```
fgHaInfo OBJECT IDENTIFIER
    ::= { fgHighAvailability 1 }

fgHaSystemMode OBJECT-TYPE
    SYNTAX      FgHaMode
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "High-availability mode (Standalone, A-A or A-P)"
    ::= { fgHaInfo 1 }

fgHaGroupId OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "HA cluster group ID device is configured for"
    ::= { fgHaInfo 2 }

fgHaPriority OBJECT-TYPE
    SYNTAX      Integer32 (0..255)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "HA clustering priority of the device (default = 127)"
    ::= { fgHaInfo 3 }

fgHaOverride OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Status of a master override flag"
    ::= { fgHaInfo 4 }

fgHaAutoSync OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Configuration of an automatic configuration
         synchronization (enabled or disabled)"
    ::= { fgHaInfo 5 }

fgHaSchedule OBJECT-TYPE
    SYNTAX      FgHaLBSchedule
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Load-balancing schedule of cluster (in A-A mode)"
    ::= { fgHaInfo 6 }

fgHaGroupName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "HA cluster group name"
    ::= { fgHaInfo 7 }

--
-- fortinet.fnFortiGateMib.fgHighAvailability.fgHaTables
--

fgHaTables OBJECT IDENTIFIER
```

```
    ::= { fgHighAvailability 2 }

fgHaStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgHaStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Some useful statistics for all members of a cluster. This table is also available
in standalone mode."
    ::= { fgHaTables 1 }

fgHaStatsEntry OBJECT-TYPE
    SYNTAX      FgHaStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Statistics for a particular HA cluster's unit"
    INDEX       { fgHaStatsIndex }
    ::= { fgHaStatsTable 1 }

FgHaStatsEntry ::= SEQUENCE {
    fgHaStatsIndex      FnIndex,
    fgHaStatsSerial     DisplayString,
    fgHaStatsCpuUsage   Gauge32,
    fgHaStatsMemUsage   Gauge32,
    fgHaStatsNetUsage   Gauge32,
    fgHaStatsSesCount   Gauge32,
    fgHaStatsPktCount   Counter32,
    fgHaStatsByteCount  Counter32,
    fgHaStatsIdsCount   Counter32,
    fgHaStatsAvCount    Counter32,
    fgHaStatsHostname   DisplayString,
    fgHaStatsSyncStatus         FgHaStatsSyncStatusType,
    fgHaStatsSyncDatimeSucc     DateAndTime,
    fgHaStatsSyncDatimeUnsucc   DateAndTime,
    fgHaStatsGlobalChecksum     DisplayString,
    fgHaStatsMasterSerial       DisplayString
}

fgHaStatsIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An index value that uniquely identifies an
         unit in the HA Cluster"
    ::= { fgHaStatsEntry 1 }

fgHaStatsSerial OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Serial number of the HA cluster member for this row"
    ::= { fgHaStatsEntry 2 }

fgHaStatsCpuUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "CPU usage of the specified cluster member (percentage)"
    ::= { fgHaStatsEntry 3 }

fgHaStatsMemUsage OBJECT-TYPE
```

```
        SYNTAX      Gauge32 (0..100)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Memory usage of the specified cluster member (percentage)"
        ::= { fgHaStatsEntry 4 }

    fgHaStatsNetUsage OBJECT-TYPE
        SYNTAX      Gauge32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Network bandwidth usage of specified cluster member (kbps)"
        ::= { fgHaStatsEntry 5 }

    fgHaStatsSesCount OBJECT-TYPE
        SYNTAX      Gauge32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Current session count of specified cluster member"
        ::= { fgHaStatsEntry 6 }

    fgHaStatsPktCount OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of packets processed by the specified cluster member since start-up"
        ::= { fgHaStatsEntry 7 }

    fgHaStatsByteCount OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of bytes processed by the specified cluster member since start-up"
        ::= { fgHaStatsEntry 8 }

    fgHaStatsIdsCount OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of IDS/IPS events triggered on the specified cluster member since start-
    up"
        ::= { fgHaStatsEntry 9 }

    fgHaStatsAvCount OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Number of anti-virus events triggered on the specified cluster member since
    start-up"
        ::= { fgHaStatsEntry 10 }

    fgHaStatsHostname OBJECT-TYPE
        SYNTAX      DisplayString (SIZE(0..255))
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Host name of the specified cluster member"
        ::= { fgHaStatsEntry 11 }
```

```
fgHaStatsSyncStatus OBJECT-TYPE
    SYNTAX      FgHaStatsSyncStatusType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current HA Sync status"
    ::= { fgHaStatsEntry 12 }

fgHaStatsSyncDatimeSucc OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Date and time of last successful sync"
    ::= { fgHaStatsEntry 13 }

fgHaStatsSyncDatimeUnsucc OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Date and time of last unsuccessful sync"
    ::= { fgHaStatsEntry 14 }

fgHaStatsGlobalChecksum OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current HA global checksum value"
    ::= { fgHaStatsEntry 15 }

fgHaStatsMasterSerial OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Serial number of master during the last synch attempt (successful of not)"
    ::= { fgHaStatsEntry 16 }

--
-- fortinet.fnFortiGateMib.fgHighAvailability.fgHaTrapObjects
--

fgHaTrapObjects OBJECT IDENTIFIER
    ::= { fgHighAvailability 3 }

fgHaTrapMemberSerial OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Serial number of an HA cluster member. Used to identify the origin of a trap when
a cluster is configured."
    ::= { fgHaTrapObjects 1 }

--
-- fortinet.fnFortiGateMib.fgWc
--

fgWc OBJECT IDENTIFIER
    ::= { fnFortiGateMib 14 }

--
-- fortinet.fnFortiGateMib.fgWc.fgWcTrapObjects
```

```
--

fgWcTrapObjects OBJECT IDENTIFIER
    ::= { fgWc 1 }

fgWcApVdom OBJECT-TYPE
    SYNTAX      FgVdIndex
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Virtual domain the wtp is part of"
    ::= { fgWcTrapObjects 1 }

fgWcApSerial OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Serial number of the wtp"
    ::= { fgWcTrapObjects 2 }

fgWcApName OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Name of the wtp"
    ::= { fgWcTrapObjects 3 }

--
-- fortinet.fnFortiGateMib.fgWc.fgWcInfo
--

fgWcInfo OBJECT IDENTIFIER
    ::= { fgWc 2 }

fgWcInfoName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the name of an AC"
    ::= { fgWcInfo 1 }

fgWcInfoLocation OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the location of an AC"
    ::= { fgWcInfo 2 }

fgWcInfoWtpCapacity  OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the maximum number of WTPs that can be managed on the AC."
    ::= { fgWcInfo 3 }

fgWcInfoWtpManaged  OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
```

```
        "Represents the number of WTPs being managed on the AC."
    ::= { fgWcInfo 4 }

fgWcInfoWtpSessions OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the number of WTPs that are connecting to the AC."
    ::= { fgWcInfo 5 }

fgWcInfoStationCapacity  OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the maximum number of stations that can be supported on the AC."
    ::= { fgWcInfo 6 }

fgWcInfoStationCount  OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the number of stations that are accessing the wireless service
         provided by the AC."
    ::= { fgWcInfo 7 }

--
-- fortinet.fnFortiGateMib.fgWc.fgWcWlanTable
--

fgWcWlanTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgWcWlanEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table that allows the operator to display WLAN profiles."
    ::= { fgWc 3 }

fgWcWlanEntry  OBJECT-TYPE
    SYNTAX      FgWcWlanEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A set of objects that stores the settings of a WLAN profile."
    INDEX       { fgVdEntIndex, ifIndex }
    ::= { fgWcWlanTable 1 }

FgWcWlanEntry ::= SEQUENCE {
      fgWcWlanSsid                  OCTET STRING,
      fgWcWlanBroadcastSsid         FnBoolState,
      fgWcWlanSecurity              FgWcWlanSecurityType,
      fgWcWlanEncryption            FgWcWlanEncryptionType,
      fgWcWlanAuthentication        FgWcWlanAuthenticationType,
      fgWcWlanRadiusServer          DisplayString,
      fgWcWlanUserGroup             DisplayString,
      fgWcWlanLocalBridging         FnBoolState,
      fgWcWlanVlanId                Integer32,
      fgWcWlanMeshBackhaul          FnBoolState,
      fgWcWlanStationCapacity       Unsigned32,
      fgWcWlanStationCount          Gauge32
    }

fgWcWlanSsid OBJECT-TYPE
```

```
    SYNTAX      OCTET STRING (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Service set ID of this WLAN profile."
    ::= { fgWcWlanEntry 1 }

fgWcWlanBroadcastSsid OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Whether SSID broadcast is enabled on this WLAN profile."
    ::= { fgWcWlanEntry 2 }

fgWcWlanSecurity  OBJECT-TYPE
    SYNTAX      FgWcWlanSecurityType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the security type of the WLAN profile."
    ::= { fgWcWlanEntry 3 }

fgWcWlanEncryption OBJECT-TYPE
    SYNTAX      FgWcWlanEncryptionType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the encryption method of the WLAN profile."
    ::= { fgWcWlanEntry 4 }

fgWcWlanAuthentication OBJECT-TYPE
    SYNTAX      FgWcWlanAuthenticationType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the authentication method of the WLAN profile."
    ::= { fgWcWlanEntry 5 }

fgWcWlanRadiusServer OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the specified RADIUS server of the WLAN profile."
    ::= { fgWcWlanEntry 6 }

fgWcWlanUserGroup OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the specified user group of the WLAN profile."
    ::= { fgWcWlanEntry 7 }

fgWcWlanLocalBridging OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Whether local bridging is enabled on this WLAN profile."
    ::= { fgWcWlanEntry 8 }

fgWcWlanVlanId OBJECT-TYPE
    SYNTAX      Integer32 (0 | 1..4094 | 4095)
```

```
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the VLAN ID of the WLAN profile."
    ::= { fgWcWlanEntry 9 }

fgWcWlanMeshBackhaul OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Whether mesh backhaul is enabled on this WLAN profile."
    ::= { fgWcWlanEntry 10 }

fgWcWlanStationCapacity OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the maximum number of clients allowed on this WLAN profile."
    ::= { fgWcWlanEntry 11 }

fgWcWlanStationCount OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the number of clients currently connected to this WLAN profile."
    ::= { fgWcWlanEntry 12 }

--
-- fortinet.fnFortiGateMib.fgWc.fgWcWtpTables
--

fgWcWtpTables OBJECT IDENTIFIER
    ::= { fgWc 4 }

--
-- fortinet.fnFortiGateMib.fgWc.fgWcWtpTables.fgWcWtpProfileTable
--

fgWcWtpProfileTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgWcWtpProfileEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of objects that display WTP profiles for WTPs to be managed before they
connect
         to the AC. A WTP could get the new configuration through the CAPWAP control
channel."
    ::= { fgWcWtpTables 1 }

fgWcWtpProfileEntry OBJECT-TYPE
    SYNTAX      FgWcWtpProfileEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A set of objects that display a WTP profile."
    INDEX { fgVdEntIndex, fgWcWtpProfileName }
    ::= { fgWcWtpProfileTable 1 }

FgWcWtpProfileEntry ::= SEQUENCE {
      fgWcWtpProfileName                    DisplayString,
      fgWcWtpProfilePlatform                DisplayString,
      fgWcWtpProfileDataChannelDtlsPolicy   BITS,
```

```
      fgWcWtpProfileCountryString           FgWcCountryString
    }

fgWcWtpProfileName OBJECT-TYPE
    SYNTAX      DisplayString (SIZE (1..36))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Represents the name of a WTP profile."
    ::= { fgWcWtpProfileEntry 1 }

fgWcWtpProfilePlatform OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the hardware platform of a WTP profile."
    ::= { fgWcWtpProfileEntry 2 }

fgWcWtpProfileDataChannelDtlsPolicy OBJECT-TYPE
    SYNTAX      BITS { other(0), clear(1), dtls(2), ipsec(3) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The AC communicates its policy on the use of DTLS for the CAPWAP data channel.
         The AC MAY support more than one option, represented by the bit field below:
           other(0) - Other method, for example, vendor specific
           clear(1) - Clear text
           dtls(2)  - DTLS
           ipsec(3) - IPsec"
    ::= { fgWcWtpProfileEntry 3 }

fgWcWtpProfileCountryString OBJECT-TYPE
    SYNTAX      FgWcCountryString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the country setting of a WTP profile, in ISO string format."
    ::= { fgWcWtpProfileEntry 4 }

--
-- fortinet.fnFortiGateMib.fgWc.fgWcWtpTables.fgWcWtpProfileRadioTable
--

fgWcWtpProfileRadioTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgWcWtpProfileRadioEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of objects that display WTP radio profiles for WTP radios to be managed
         before the WTPs connect to the AC. A WTP radio could get the new configuration
         through the CAPWAP control channel."
    ::= { fgWcWtpTables 2 }

fgWcWtpProfileRadioEntry  OBJECT-TYPE
    SYNTAX      FgWcWtpProfileRadioEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A set of objects that display a WTP radio profile."
    INDEX { fgVdEntIndex, fgWcWtpProfileRadioProfileName, fgWcWtpProfileRadioRadioId }
    ::= { fgWcWtpProfileRadioTable 1 }

FgWcWtpProfileRadioEntry ::= SEQUENCE {
      fgWcWtpProfileRadioProfileName        DisplayString,
```

```
      fgWcWtpProfileRadioRadioId            FgWcWtpRadioId,
      fgWcWtpProfileRadioMode               FgWcWtpRadioMode,
      fgWcWtpProfileRadioApScan             FnBoolState,
      fgWcWtpProfileRadioWidsProfile        DisplayString,
      fgWcWtpProfileRadioDarrp              FnBoolState,
      fgWcWtpProfileRadioFrequencyHandoff   FnBoolState,
      fgWcWtpProfileRadioApHandoff          FnBoolState,
      fgWcWtpProfileRadioBeaconInterval     Integer32,
      fgWcWtpProfileRadioDtimPeriod         Integer32,
      fgWcWtpProfileRadioBand               FgWcWtpRadioType,
      fgWcWtpProfileRadioChannelBonding     FnBoolState,
      fgWcWtpProfileRadioChannel            DisplayString,
      fgWcWtpProfileRadioAutoTxPowerControl FnBoolState,
      fgWcWtpProfileRadioAutoTxPowerLow     Integer32,
      fgWcWtpProfileRadioAutoTxPowerHigh    Integer32,
      fgWcWtpProfileRadioTxPowerLevel       Gauge32,
      fgWcWtpProfileRadioVaps               DisplayString,
      fgWcWtpProfileRadioStationCapacity    Unsigned32,
      fgWcWtpProfileRadioChannelWidth       FgWcWtpChannelWidthType
    }

fgWcWtpProfileRadioProfileName OBJECT-TYPE
    SYNTAX      DisplayString (SIZE (1..36))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Represents the name of a WTP profile."
    ::= { fgWcWtpProfileRadioEntry 1 }

fgWcWtpProfileRadioRadioId OBJECT-TYPE
    SYNTAX      FgWcWtpRadioId
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Represents the radio Id of a WTP radio."
    ::= { fgWcWtpProfileRadioEntry 2 }

fgWcWtpProfileRadioMode OBJECT-TYPE
    SYNTAX      FgWcWtpRadioMode
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the operating mode of a WTP radio."
    ::= { fgWcWtpProfileRadioEntry 3 }

fgWcWtpProfileRadioApScan OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Whether background scan is enabled on this WTP radio."
    ::= { fgWcWtpProfileRadioEntry 4 }

fgWcWtpProfileRadioWidsProfile OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the WIDS profile configured for this WTP radio."
    ::= { fgWcWtpProfileRadioEntry 5 }

fgWcWtpProfileRadioDarrp OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
        "Whether DARRP is enabled on this WTP radio."
    ::= { fgWcWtpProfileRadioEntry 6 }

fgWcWtpProfileRadioFrequencyHandoff OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Whether frequency handoff is enabled on this WTP radio."
    ::= { fgWcWtpProfileRadioEntry 7 }

fgWcWtpProfileRadioApHandoff OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Whether AP handoff is enabled on this WTP radio."
    ::= { fgWcWtpProfileRadioEntry 8 }

fgWcWtpProfileRadioBeaconInterval OBJECT-TYPE
    SYNTAX      Integer32 (1..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "This attribute shall specify the number of TUs that a station shall use for
scheduling
         Beacon transmissions. This value is transmitted in Beacon and Probe Response
frames."
    ::= { fgWcWtpProfileRadioEntry 9 }

fgWcWtpProfileRadioDtimPeriod OBJECT-TYPE
    SYNTAX      Integer32 (1..255)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "This attribute shall specify the number of beacon intervals that shall elapse
between
         transmission of Beacon frames containing a TIM element whose DTIM Count field is
0.
         This value is transmitted in the DTIM Period field of Beacon frames."
    ::= { fgWcWtpProfileRadioEntry 10 }

fgWcWtpProfileRadioBand OBJECT-TYPE
    SYNTAX      FgWcWtpRadioType
    MAX-ACCESS  read-only
    STATUS current
    DESCRIPTION
        "Represents the radio band setting configured for this WTP radio."
    ::= { fgWcWtpProfileRadioEntry 11 }

fgWcWtpProfileRadioChannelBonding OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Whether channel bonding is enabled on this WTP radio."
    ::= { fgWcWtpProfileRadioEntry 12 }

fgWcWtpProfileRadioChannel OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents a list of channels configured for this WTP radio."
```

```
    ::= { fgWcWtpProfileRadioEntry 13 }

fgWcWtpProfileRadioAutoTxPowerControl OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Whether automatic TX power control is enabled on this WTP radio."
    ::= { fgWcWtpProfileRadioEntry 14 }

fgWcWtpProfileRadioAutoTxPowerLow OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the low limit of the power level configured for this WTP radio, in
dBm.
         Applicable only when auto power leveling is enabled."
    ::= { fgWcWtpProfileRadioEntry 15 }

fgWcWtpProfileRadioAutoTxPowerHigh OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the high limit of the power level configured for this WTP radio, in
dBm.
         Applicable only when auto power leveling is enabled."
    ::= { fgWcWtpProfileRadioEntry 16 }

fgWcWtpProfileRadioTxPowerLevel OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the radio TX power setting configured for this WTP radio, in
percentage.
         Application only when auto power leveling is disabled."
    ::= { fgWcWtpProfileRadioEntry 17 }

fgWcWtpProfileRadioVaps OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents a list of WLANs configured for this WTP radio."
    ::= { fgWcWtpProfileRadioEntry 18 }

fgWcWtpProfileRadioStationCapacity OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the maximum number of clients allowed on this WTP radio."
    ::= { fgWcWtpProfileRadioEntry 19 }

fgWcWtpProfileRadioChannelWidth OBJECT-TYPE
    SYNTAX      FgWcWtpChannelWidthType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the channel width on this WTP radio."
    ::= { fgWcWtpProfileRadioEntry 20 }

--
```

```
-- fortinet.fnFortiGateMib.fgWc.fgWcWtpTables.fgWcWtpConfigTable
--

fgWcWtpConfigTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgWcWtpConfigEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of objects that display the configuration of WTPs."
    ::= { fgWcWtpTables 3 }

fgWcWtpConfigEntry  OBJECT-TYPE
    SYNTAX      FgWcWtpConfigEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A set of objects that display the configuration of a WTP."
    INDEX { fgVdEntIndex, fgWcWtpConfigWtpId }
    ::= { fgWcWtpConfigTable 1 }

FgWcWtpConfigEntry ::= SEQUENCE {
      fgWcWtpConfigWtpId                    DisplayString,
      fgWcWtpConfigWtpAdmin                 INTEGER,
      fgWcWtpConfigWtpName                  DisplayString,
      fgWcWtpConfigWtpLocation              DisplayString,
      fgWcWtpConfigWtpProfile               DisplayString,
      fgWcWtpConfigRadioEnable              FnBoolState,
      fgWcWtpConfigRadioAutoTxPowerControl  FnBoolState,
      fgWcWtpConfigRadioAutoTxPowerLow      Integer32,
      fgWcWtpConfigRadioAutoTxPowerHigh     Integer32,
      fgWcWtpConfigRadioTxPowerLevel        Gauge32,
      fgWcWtpConfigRadioBand                FgWcWtpRadioBandType,
      fgWcWtpConfigRadioApScan              FnBoolState,
      fgWcWtpConfigVapAll                   FnBoolState,
      fgWcWtpConfigVaps                     DisplayString
    }

fgWcWtpConfigWtpId OBJECT-TYPE
    SYNTAX      DisplayString (SIZE (1..36))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Represents the unique identifier of a WTP."
    ::= { fgWcWtpConfigEntry 1 }

fgWcWtpConfigWtpAdmin OBJECT-TYPE
    SYNTAX      INTEGER {
                  other(0),
                  discovered(1),
                  disable(2),
                  enable(3)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the administrative status of this WTP.
         The following enumerated values are supported:
           discovered(1)   - This WTP was discovered though discovery or join request
messages.
           disable(2)      - Controller is configured to not provide service to this WTP.
           enable(3),      - Controller is configured to provide service to this WTP.
           other(0)        - The administration state of the WTP is unknown."
    ::= { fgWcWtpConfigEntry 2 }

fgWcWtpConfigWtpName OBJECT-TYPE
```

```
        SYNTAX      DisplayString
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Represents the name configured for this WTP."
        ::= { fgWcWtpConfigEntry 3 }

    fgWcWtpConfigWtpLocation OBJECT-TYPE
        SYNTAX      DisplayString
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Represents the location of this WTP."
        ::= { fgWcWtpConfigEntry 4 }

    fgWcWtpConfigWtpProfile OBJECT-TYPE
        SYNTAX      DisplayString
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Represents the WTP profile configured for this WTP."
        ::= { fgWcWtpConfigEntry 5 }

    fgWcWtpConfigRadioEnable OBJECT-TYPE
        SYNTAX      FnBoolState
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Whether radio is enabled for this WTP."
        ::= { fgWcWtpConfigEntry 6 }

    fgWcWtpConfigRadioAutoTxPowerControl OBJECT-TYPE
        SYNTAX      FnBoolState
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Whether radio automatic TX power control is enabled on this WTP."
        ::= { fgWcWtpConfigEntry 7 }

    fgWcWtpConfigRadioAutoTxPowerLow OBJECT-TYPE
        SYNTAX      Integer32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Represents the low limit of radio automatic TX power control configured for this
    WTP, in dBm."
        ::= { fgWcWtpConfigEntry 8 }

    fgWcWtpConfigRadioAutoTxPowerHigh OBJECT-TYPE
        SYNTAX      Integer32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Represents the high limit of radio automatic TX power control configured for this
    WTP, in dBm."
        ::= { fgWcWtpConfigEntry 9 }

    fgWcWtpConfigRadioTxPowerLevel OBJECT-TYPE
        SYNTAX      Gauge32 (0..100)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Represents the radio TX power setting configured for this WTP, in percentage."
        ::= { fgWcWtpConfigEntry 10 }
```

```
fgWcWtpConfigRadioBand OBJECT-TYPE
    SYNTAX      FgWcWtpRadioBandType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the radio band configured for this WTP."
    ::= { fgWcWtpConfigEntry 11 }

fgWcWtpConfigRadioApScan OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Whether background scan is enabled on this WTP."
    ::= { fgWcWtpConfigEntry 12 }

fgWcWtpConfigVapAll OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Whether all VAPs are selected for this WTP."
    ::= { fgWcWtpConfigEntry 13 }

fgWcWtpConfigVaps OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents a list of VAPs configured for this WTP."
    ::= { fgWcWtpConfigEntry 14 }

--
-- fortinet.fnFortiGateMib.fgWc.fgWcWtpTables.fgWcWtpSessionTable
--

fgWcWtpSessionTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgWcWtpSessionEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of objects that indicate the AC's CAPWAP FSM state for each WTP,
         and helps the operator to query a WTP's current status."
    ::= { fgWcWtpTables 4 }

fgWcWtpSessionEntry  OBJECT-TYPE
    SYNTAX      FgWcWtpSessionEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A set of objects that displays the AC's CAPWAP FSM state for each WTP.
         Also, the operator could query the current status of a WTP by using
         the identifier of the corresponding WTP."
    INDEX { fgVdEntIndex, fgWcWtpSessionWtpId }
    ::= { fgWcWtpSessionTable 1 }

FgWcWtpSessionEntry ::= SEQUENCE {
      fgWcWtpSessionWtpId                   DisplayString,
      fgWcWtpSessionWtpIpAddressType        InetAddressType,
      fgWcWtpSessionWtpIpAddress            InetAddress,
      fgWcWtpSessionWtpLocalIpAddressType   InetAddressType,
      fgWcWtpSessionWtpLocalIpAddress       InetAddress,
      fgWcWtpSessionWtpBaseMacAddress       PhysAddress,
      fgWcWtpSessionConnectionState         INTEGER,
      fgWcWtpSessionWtpUpTime               TimeTicks,
```

```
      fgWcWtpSessionWtpDaemonUpTime         TimeTicks,
      fgWcWtpSessionWtpSessionUpTime        TimeTicks,
      fgWcWtpSessionWtpProfileName          DisplayString,
      fgWcWtpSessionWtpModelNumber          DisplayString,
      fgWcWtpSessionWtpHwVersion            DisplayString,
      fgWcWtpSessionWtpSwVersion            DisplayString,
      fgWcWtpSessionWtpBootVersion          DisplayString,
      fgWcWtpSessionWtpRegionCode           DisplayString,
      fgWcWtpSessionWtpStationCount         Gauge32,
      fgWcWtpSessionWtpByteRxCount          Counter64,
      fgWcWtpSessionWtpByteTxCount          Counter64,
      fgWcWtpSessionWtpCpuUsage             Gauge32,
      fgWcWtpSessionWtpMemoryUsage          Gauge32,
      fgWcWtpSessionWtpMemoryCapacity       Unsigned32
    }

fgWcWtpSessionWtpId OBJECT-TYPE
    SYNTAX      DisplayString (SIZE (1..36))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Represents the unique identifier of a WTP."
    ::= { fgWcWtpSessionEntry 1 }

fgWcWtpSessionWtpIpAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the IP address type of a WTP.
         Only ipv4(1) and ipv6(2) are supported by the object."
    ::= { fgWcWtpSessionEntry 2 }

fgWcWtpSessionWtpIpAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the IP address of a WTP that corresponds to the IP address in
         the IP packet header.
         The format of this IP address is determined by the corresponding instance of
         object fgWcWtpWtpIpAddressType."
    ::= { fgWcWtpSessionEntry 3 }

fgWcWtpSessionWtpLocalIpAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the local IP address type of a WTP.
         Only ipv4(1) and ipv6(2) are supported by the object."
    ::= { fgWcWtpSessionEntry 4 }

fgWcWtpSessionWtpLocalIpAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the local IP address of a WTP and models the CAPWAP Local IPv4 Address
         or CAPWAP Local IPv6 Address fields [RFC5415].
         If a Network Address Translation (NAT) device is present between WTP and AC, the
value of
         fgWcWtpWtpLocalIpAddress will be different from the value of fgWcWtpWtpIpAddress.
         The format of this IP address is determined by the corresponding instance of
object
```

```
          fgWcWtpSessionWtpLocalIpAddressType."
    ::= { fgWcWtpSessionEntry 5 }

fgWcWtpSessionWtpBaseMacAddress OBJECT-TYPE
    SYNTAX      PhysAddress (SIZE(6|8))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the WTP's Base MAC Address, which MAY be assigned to the primary
         Ethernet interface.
         The instance of the object corresponds to the Base MAC Address sub-element
         in the CAPWAP protocol [RFC5415]."
    ::= { fgWcWtpSessionEntry 6 }

fgWcWtpSessionConnectionState OBJECT-TYPE
    SYNTAX      INTEGER {
                  other(0),
                  offLine(1),
                  onLine(2),
                  downloadingImage(3),
                  connectedImage(4)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the connection state of a WTP to AC.
         The following enumerated values are supported:
           offLine(1)           - The WTP is not connected.
           onLine(2)            - The WTP is connected.
           downloadingImage(3)  - The WTP is downloading software image from the AC on
joining.
           connectedImage(4)    - The AC is pushing software image to the connected WTP.
           other(0)             - The WTP connection state is unknown."
    ::= { fgWcWtpSessionEntry 7 }

fgWcWtpSessionWtpUpTime OBJECT-TYPE
    SYNTAX      TimeTicks
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the time (in hundredths of a second) since the WTP boots."
    ::= { fgWcWtpSessionEntry 8 }

fgWcWtpSessionWtpDaemonUpTime OBJECT-TYPE
    SYNTAX      TimeTicks
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the time (in hundredths of a second) since the WTP daemon has been
started."
    ::= { fgWcWtpSessionEntry 9 }

fgWcWtpSessionWtpSessionUpTime OBJECT-TYPE
    SYNTAX      TimeTicks
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the time (in hundredths of a second) since the WTP connects to the
AC."
    ::= { fgWcWtpSessionEntry 10 }

fgWcWtpSessionWtpProfileName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
        "Represents the profile configured for this WTP."
    ::= { fgWcWtpSessionEntry 11 }

fgWcWtpSessionWtpModelNumber OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the model number of a WTP."
    ::= { fgWcWtpSessionEntry 12 }

fgWcWtpSessionWtpHwVersion OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the hardware version of a WTP."
    ::= { fgWcWtpSessionEntry 13 }

fgWcWtpSessionWtpSwVersion OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the software version of a WTP."
    ::= { fgWcWtpSessionEntry 14 }

fgWcWtpSessionWtpBootVersion OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the boot loader version of a WTP."
    ::= { fgWcWtpSessionEntry 15 }

fgWcWtpSessionWtpRegionCode OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the region code programmed for this WTP."
    ::= { fgWcWtpSessionEntry 16 }

fgWcWtpSessionWtpStationCount OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the number of clients currently connected to this WTP."
    ::= { fgWcWtpSessionEntry 17 }

fgWcWtpSessionWtpByteRxCount OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the number of bytes received by this WTP."
    ::= { fgWcWtpSessionEntry 18 }

fgWcWtpSessionWtpByteTxCount OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
```

```
        "Represents the number of bytes transmitted by this WTP."
    ::= { fgWcWtpSessionEntry 19 }

fgWcWtpSessionWtpCpuUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the current CPU usage of a WTP (percentage)."
    ::= { fgWcWtpSessionEntry 20 }

fgWcWtpSessionWtpMemoryUsage OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the current memory usage of a WTP (percentage)."
    ::= { fgWcWtpSessionEntry 21 }

fgWcWtpSessionWtpMemoryCapacity OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the total physical memory (RAM) installed (KB)."
    ::= { fgWcWtpSessionEntry 22 }

--
-- fortinet.fnFortiGateMib.fgWc.fgWcWtpTables.fgWcWtpSessionRadioTable
--

fgWcWtpSessionRadioTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgWcWtpSessionRadioEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of objects that display the status of radios in WTP sessions."
    ::= { fgWcWtpTables 5 }

fgWcWtpSessionRadioEntry  OBJECT-TYPE
    SYNTAX      FgWcWtpSessionRadioEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A set of objects that display the status of a radio in a WTP session."
    INDEX { fgVdEntIndex, fgWcWtpSessionRadioWtpId, fgWcWtpSessionRadioRadioId}
    ::= { fgWcWtpSessionRadioTable 1 }

FgWcWtpSessionRadioEntry ::= SEQUENCE {
      fgWcWtpSessionRadioWtpId              DisplayString,
      fgWcWtpSessionRadioRadioId            FgWcWtpRadioId,
      fgWcWtpSessionRadioMode               FgWcWtpRadioMode,
      fgWcWtpSessionRadioBaseBssid          PhysAddress,
      fgWcWtpSessionRadioCountryString      FgWcCountryString,
      fgWcWtpSessionRadioCountryCode        Integer32,
      fgWcWtpSessionRadioOperatingChannel   FgWcWtpRadioChannelNumber,
      fgWcWtpSessionRadioOperatingPower     Integer32,
      fgWcWtpSessionRadioStationCount       Gauge32
    }

fgWcWtpSessionRadioWtpId OBJECT-TYPE
    SYNTAX      DisplayString (SIZE (1..36))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
```

```
        "Represents the unique identifier of a WTP."
    ::= { fgWcWtpSessionRadioEntry 1 }

fgWcWtpSessionRadioRadioId OBJECT-TYPE
    SYNTAX      FgWcWtpRadioId
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Represents the radio Id of a radio."
    ::= { fgWcWtpSessionRadioEntry 2 }

fgWcWtpSessionRadioMode  OBJECT-TYPE
    SYNTAX      FgWcWtpRadioMode
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the operating mode of this radio."
    ::= { fgWcWtpSessionRadioEntry 3 }

fgWcWtpSessionRadioBaseBssid  OBJECT-TYPE
    SYNTAX      PhysAddress (SIZE(6|8))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents base bssid of this radio."
    ::= { fgWcWtpSessionRadioEntry 4 }

fgWcWtpSessionRadioCountryString OBJECT-TYPE
    SYNTAX      FgWcCountryString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the current operating country string, in ISO string format."
    ::= { fgWcWtpSessionRadioEntry 5 }

fgWcWtpSessionRadioCountryCode OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the current operating country code."
    ::= { fgWcWtpSessionRadioEntry 6 }

fgWcWtpSessionRadioOperatingChannel OBJECT-TYPE
    SYNTAX      FgWcWtpRadioChannelNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the current operating channel of this radio."
    ::= { fgWcWtpSessionRadioEntry 7 }

fgWcWtpSessionRadioOperatingPower OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the current operating power of this radio, in dBm."
    ::= { fgWcWtpSessionRadioEntry 8 }

fgWcWtpSessionRadioStationCount OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the number of clients currently connected to this radio."
```

```
    ::= { fgWcWtpSessionRadioEntry 9 }

--
-- fortinet.fnFortiGateMib.fgWc.fgWcWtpTables.fgWcWtpSessionVapTable
--

fgWcWtpSessionVapTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgWcWtpSessionVapEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of objects that display the status of VAPs in WTP sessions.
         A VAP represents an SSID that is assigned on a WTP radio."
    ::= { fgWcWtpTables 6 }

fgWcWtpSessionVapEntry  OBJECT-TYPE
    SYNTAX      FgWcWtpSessionVapEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A set of objects that display the status of a VAP in a WTP session."
    INDEX { fgVdEntIndex, fgWcWtpSessionVapWtpId, fgWcWtpSessionVapRadioId, ifIndex }
    ::= { fgWcWtpSessionVapTable 1 }

FgWcWtpSessionVapEntry ::= SEQUENCE {
      fgWcWtpSessionVapWtpId                DisplayString,
      fgWcWtpSessionVapRadioId              FgWcWtpRadioId,
      fgWcWtpSessionVapSsid                 OCTET STRING,
      fgWcWtpSessionVapStationCount         Gauge32,
      fgWcWtpSessionVapByteRxCount          Counter64,
      fgWcWtpSessionVapByteTxCount          Counter64
    }

fgWcWtpSessionVapWtpId OBJECT-TYPE
    SYNTAX      DisplayString (SIZE (1..36))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Represents the unique identifier of a WTP."
    ::= { fgWcWtpSessionVapEntry 1 }

fgWcWtpSessionVapRadioId OBJECT-TYPE
    SYNTAX      FgWcWtpRadioId
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Represents the radio Id of a VAP."
    ::= { fgWcWtpSessionVapEntry 2 }

fgWcWtpSessionVapSsid OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Service set ID of this VAP interface."
    ::= { fgWcWtpSessionVapEntry 3 }

fgWcWtpSessionVapStationCount OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the number of clients currently connected to this VAP."
    ::= { fgWcWtpSessionVapEntry 4 }
```

```
fgWcWtpSessionVapByteRxCount OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the number of bytes received by this VAP."
    ::= { fgWcWtpSessionVapEntry 5 }

fgWcWtpSessionVapByteTxCount OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the number of bytes transmitted by this VAP."
    ::= { fgWcWtpSessionVapEntry 6 }

--
-- fortinet.fnFortiGateMib.fgWc.fgWcStaTable
--

fgWcStaTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgWcStaEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table that provides information of all the wireless stations that are accessing
         the wireless service provided by the AC."
    ::= { fgWc 5 }

fgWcStaEntry OBJECT-TYPE
    SYNTAX      FgWcStaEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A set of objects that display information of a wireless station."
    INDEX       { fgVdEntIndex, ifIndex, fgWcStaMacAddress }
    ::= { fgWcStaTable 1 }

FgWcStaEntry ::= SEQUENCE {
      fgWcStaMacAddress             PhysAddress,
      fgWcStaWlan                   DisplayString,
      fgWcStaWtpId                  DisplayString,
      fgWcStaRadioId                FgWcWtpRadioId,
      fgWcStaVlanId                 Integer32,
      fgWcStaIpAddressType          InetAddressType,
      fgWcStaIpAddress              InetAddress,
      fgWcStaVci                    DisplayString,
      fgWcStaHost                   DisplayString,
      fgWcStaUser                   DisplayString,
      fgWcStaGroup                  DisplayString,
      fgWcStaSignal                 Integer32,
      fgWcStaNoise                  Integer32,
      fgWcStaIdle                   Gauge32,
      fgWcStaBandwidthTx            Gauge32,
      fgWcStaBandwidthRx            Gauge32,
      fgWcStaChannel                FgWcWtpRadioChannelNumber,
      fgWcStaRadioType              FgWcWtpRadioType,
      fgWcStaSecurity               FgWcWlanSecurityType,
      fgWcStaEncrypt                FgWcWlanEncryptionType,
      fgWcStaOnline                 INTEGER
    }

fgWcStaMacAddress OBJECT-TYPE
    SYNTAX      PhysAddress (SIZE(6|8))
    MAX-ACCESS  not-accessible
```

```
        STATUS      current
        DESCRIPTION
            "Represents the MAC address of a wireless station."
        ::= { fgWcStaEntry 1 }

    fgWcStaWlan OBJECT-TYPE
        SYNTAX      DisplayString
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "WLAN interface that a wireless station is connected to."
        ::= { fgWcStaEntry 2 }

    fgWcStaWtpId OBJECT-TYPE
        SYNTAX      DisplayString
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Unique identifier of the WTP that a wireless station is connected to."
        ::= { fgWcStaEntry 3 }

    fgWcStaRadioId OBJECT-TYPE
        SYNTAX      FgWcWtpRadioId
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Represents the radio of the WTP that a wireless station is connected to."
        ::= { fgWcStaEntry 4 }

    fgWcStaVlanId OBJECT-TYPE
        SYNTAX      Integer32 (0 | 1..4094 | 4095)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Represents the VLAN ID that is assigned to a wireless station."
        ::= { fgWcStaEntry 5 }

    fgWcStaIpAddressType OBJECT-TYPE
        SYNTAX      InetAddressType
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Represents the IP address type of a wireless station.
             Only ipv4(1) and ipv6(2) are supported by the object."
        ::= { fgWcStaEntry 6 }

    fgWcStaIpAddress OBJECT-TYPE
        SYNTAX      InetAddress
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Represents the IP address of a wireless station."
        ::= { fgWcStaEntry 7 }

    fgWcStaVci OBJECT-TYPE
        SYNTAX      DisplayString
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Represents the vendor class identifier of a wireless station."
        ::= { fgWcStaEntry 8 }

    fgWcStaHost OBJECT-TYPE
        SYNTAX      DisplayString
        MAX-ACCESS  read-only
```

```
    STATUS      current
    DESCRIPTION
        "Represents the host name of a wireless station."
    ::= { fgWcStaEntry 9 }

fgWcStaUser OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the user name of a wireless station."
    ::= { fgWcStaEntry 10 }

fgWcStaGroup OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the user group of a wireless station."
    ::= { fgWcStaEntry 11 }

fgWcStaSignal OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the signal strengh of a wireless station, in dBm."
    ::= { fgWcStaEntry 12 }

fgWcStaNoise OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the noise level of a wireless station, in dBm."
    ::= { fgWcStaEntry 13 }

fgWcStaIdle OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Indicates how long a wireless station in inactive, in seconds."
    ::= { fgWcStaEntry 14 }

fgWcStaBandwidthTx OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the TX bandwidth of a wireless station, in kbps."
    ::= { fgWcStaEntry 15 }

fgWcStaBandwidthRx OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the RX bandwidth of a wireless station, in kbps."
    ::= { fgWcStaEntry 16 }

fgWcStaChannel OBJECT-TYPE
    SYNTAX      FgWcWtpRadioChannelNumber
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
        "Represents the frequency channel that a wireless station is using."
    ::= { fgWcStaEntry 17 }

fgWcStaRadioType OBJECT-TYPE
    SYNTAX      FgWcWtpRadioType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the radio physical type of a wireless station."
    ::= { fgWcStaEntry 18 }

fgWcStaSecurity OBJECT-TYPE
    SYNTAX      FgWcWlanSecurityType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the security type of a wireless station."
    ::= { fgWcStaEntry 19 }

fgWcStaEncrypt OBJECT-TYPE
    SYNTAX      FgWcWlanEncryptionType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents the encryption method of a wireless station."
    ::= { fgWcStaEntry 20 }

fgWcStaOnline OBJECT-TYPE
    SYNTAX      INTEGER { yes(1), no(2) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represent online status of a wireless station."
    ::= { fgWcStaEntry 21 }

--
-- fortinet.fnFortiGateMib.fgFc
--

fgFc OBJECT IDENTIFIER
    ::= { fnFortiGateMib 15 }

--
-- fortinet.fnFortiGateMib.fgFc.fgFcTrapObjects
--

fgFcTrapObjects OBJECT IDENTIFIER
    ::= { fgFc 1 }

fgFcSwVdom OBJECT-TYPE
    SYNTAX      FgVdIndex
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Virtual domain the switch is part of"
    ::= { fgFcTrapObjects 1 }

fgFcSwSerial OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Serial number of the switch"
    ::= { fgFcTrapObjects 2 }
```

```
fgFcSwName OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Name of the switch"
    ::= { fgFcTrapObjects 3 }

--
-- fortinet.fnFortiGateMib.fgServerLoadBalance
--

fgServerLoadBalance OBJECT IDENTIFIER
    ::= { fnFortiGateMib 16 }

--
-- fortinet.fnFortiGateMib.fgServerLoadBalance.fgServerLoadBalanceTrapObjects
--

fgServerLoadBalanceTrapObjects OBJECT IDENTIFIER
    ::= { fgServerLoadBalance 1 }

fgServerLoadBalanceRealServerAddress OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "IP of the real server."
    ::= { fgServerLoadBalanceTrapObjects 1 }

fgServerLoadBalanceVirtualServerName OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..64))
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Name of the virual server."
    ::= { fgServerLoadBalanceTrapObjects 2 }

fgServerLoadBalanceRealServerAddress6 OBJECT-TYPE
    SYNTAX      Ipv6Address
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "IPv6 of the real server."
    ::= { fgServerLoadBalanceTrapObjects 3 }

--
-- fortinet.fnFortiGateMib.fgUsbModemInfo
--

fgUsbModemInfo OBJECT IDENTIFIER
    ::= { fnFortiGateMib 17 }

--
-- fortinet.fnFortiGateMib.fgUsbModemInfo.fgUsbModemInfoObjects
--

fgUsbModemInfoObjects OBJECT IDENTIFIER
    ::= { fgUsbModemInfo 1 }

fgUsbModemSignalStrength OBJECT-TYPE
    SYNTAX      INTEGER { level0(0), level1(1), level2(2), level3(3), level4(4) }
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
        "3G/4G USB Modem signal Strength."
    ::= { fgUsbModemInfoObjects 1 }

fgUsbModemStatus OBJECT-TYPE
    SYNTAX      INTEGER { disconnected(0), connected(1) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        " 3G/4G USB Modem status."
    ::= { fgUsbModemInfoObjects 2 }

fgUsbModemSimState OBJECT-TYPE
    SYNTAX      INTEGER { invalid(0), valid(1) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "3G/4G USB Modem sim card status."
    ::= { fgUsbModemInfoObjects 3 }

fgUsbModemVendor OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..64))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "3G/4G USB Modem vendor name."
    ::= { fgUsbModemInfoObjects 4 }

fgUsbModemProduct OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..64))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "3G/4G USB Modem product name."
    ::= { fgUsbModemInfoObjects 5 }

fgUsbModemNetwork OBJECT-TYPE
    SYNTAX      INTEGER { network3G(0), networkLTE(1) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "3G/4G USB Modem network type."
    ::= { fgUsbModemInfoObjects 6 }

fgUsbModemId OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..64))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "3G/4G USB Modem identifier."
    ::= { fgUsbModemInfoObjects 7 }

fgUsbModemSimId OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..64))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "3G/4G USB Modem sim card identifier."
    ::= { fgUsbModemInfoObjects 8 }

--
-- fortinet.fnFortiGateMib.fgDevice
--

fgDevice OBJECT IDENTIFIER
```

```
    ::= { fnFortiGateMib 18 }

--
-- fortinet.fnFortiGateMib.fgDevice.fgDeviceTrapObjects
--

fgDeviceTrapObjects OBJECT IDENTIFIER
    ::= { fgDevice 1 }

fgDeviceMacAddress OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..64))
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "The MAC address pertaining the Device."
    ::= { fgDeviceTrapObjects 1 }

fgDeviceCreated OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "The created time pertaining the Device."
    ::= { fgDeviceTrapObjects 2 }

fgDeviceLastSeen OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "The last seen time pertaining the Device."
    ::= { fgDeviceTrapObjects 3 }

--
-- fortinet.fnFortiGateMib.fgInternalLTEModemsInfo
--

fgInternalLTEModemsInfo OBJECT IDENTIFIER
    ::= { fnFortiGateMib 19 }

--
-- fortinet.fnFortiGateMib.fgInternalLTEModemsInfo.fgMdmInfoTable
--

fgMdmInfoTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgMdmInfoEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table containing information applicable
         to internal LTE modems."
    ::= { fgInternalLTEModemsInfo 1 }

--
-- fortinet.fnFortiGateMib.fgInternalLTEModemsInfo.fgMdmInfoTable.fgMdmInfoEntry
--

fgMdmInfoEntry OBJECT-TYPE
    SYNTAX      FgMdmInfoEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information applicable
         to a particular LTE Modem. OIDs from fgMdmVendor are
         not displayed if a modem is not detected."
```

```
    INDEX       { fgMdmEntIndex }
    ::= { fgMdmInfoTable 1 }

FgMdmInfoEntry ::= SEQUENCE {
    fgMdmEntIndex       FnIndex,
    fgMdmDetected       INTEGER,
    fgMdmVendor         DisplayString,
    fgMdmModel          DisplayString,
    fgMdmRevision       DisplayString,
    fgMdmMsisdn         DisplayString,
    fgMdmEsn            DisplayString,
    fgMdmImei           DisplayString,
    fgMdmHwRevision     DisplayString,
    fgMdmMeid           DisplayString,
    fgMdmSwRev          DisplayString,
    fgMdmSku            DisplayString,
    fgMdmFsn            DisplayString,
    fgMdmPrlVer         DisplayString,
    fgMdmFwVer          DisplayString,
    fgMdmPriFwVer       DisplayString,
    fgMdmCarrierAbbr    DisplayString,
    fgMdmActState       INTEGER,
    fgMdmOpMode         INTEGER
}

fgMdmEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Index used to identify the instance of an internal LTE modem."
    ::= { fgMdmInfoEntry 1 }

fgMdmDetected OBJECT-TYPE
    SYNTAX      INTEGER { no(0), yes(1) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        " Internal Modem Detected."
    ::= { fgMdmInfoEntry 2 }

fgMdmVendor OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..64))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Vendor Name."
    ::= { fgMdmInfoEntry 3 }

fgMdmModel OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..64))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Model Name."
    ::= { fgMdmInfoEntry 4 }

fgMdmRevision OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..128))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Modem Firmware Revision."
    ::= { fgMdmInfoEntry 5 }
```

```
fgMdmMsisdn OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "MSISDN."
    ::= { fgMdmInfoEntry 6 }

fgMdmEsn OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..16))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "ESN."
    ::= { fgMdmInfoEntry 7 }

fgMdmImei OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "IMEI."
    ::= { fgMdmInfoEntry 8 }

fgMdmHwRevision OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..8))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Hardware Revision."
    ::= { fgMdmInfoEntry 9 }

fgMdmMeid OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "MEID."
    ::= { fgMdmInfoEntry 10 }

fgMdmSwRev OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Software Revision."
    ::= { fgMdmInfoEntry 11 }

fgMdmSku OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "SKU."
    ::= { fgMdmInfoEntry 12 }

fgMdmFsn OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "FSN."
    ::= { fgMdmInfoEntry 13 }

fgMdmPrlVer OBJECT-TYPE
```

```
        SYNTAX      DisplayString (SIZE(0..8))
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Prl Version."
        ::= { fgMdmInfoEntry 14 }

    fgMdmFwVer OBJECT-TYPE
        SYNTAX      DisplayString (SIZE(0..16))
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Modem Firmware Version."
        ::= { fgMdmInfoEntry 15 }

    fgMdmPriFwVer OBJECT-TYPE
        SYNTAX      DisplayString (SIZE(0..16))
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "PRI Firmware Version."
        ::= { fgMdmInfoEntry 16 }

    fgMdmCarrierAbbr OBJECT-TYPE
        SYNTAX      DisplayString (SIZE(0..16))
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Modem Carrier Abbriviation."
        ::= { fgMdmInfoEntry 17 }

    fgMdmActState OBJECT-TYPE
        SYNTAX      INTEGER {
                            notActivated(0),
                            activated(1),
                            connecting(2),
                            connected(3),
                            otaspAuthenticated(4),
                            otaspNamDownloaded(5),
                            otaspMdnDownloaded(6),
                            otaspImsiDownloaded(7),
                            otaspPrlDownloaded(8),
                            otaspSpcDownloaded(9),
                            otaspSettingsCmted(10)
                    }
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Modem Activation State.
             The following enumerated values are supported:
                            notActivated(0)         - Service not activated.
                            activated(1)            - Service is activated.
                            connecting(2)           - Connection in progress for automatic
    activation.
                            connected(3)            - Connection connected for automatic
    activation.
                            otaspAuthenticated(4)   - OTASP security authenticated.
                            otaspNamDownloaded(5)   - OTASP NAM downloaded.
                            otaspMdnDownloaded(6)   - OTASP MDN downloaded.
                            otaspImsiDownloaded(7)  - OTASP IMSI downloaded.
                            otaspPrlDownloaded(8)   - OTASP PRL downloaded.
                            otaspSpcDownloaded(9)   - OTASP SPC downloaded.
                            otaspSettingsCmted(10)  - OTASP settings committed."
        ::= { fgMdmInfoEntry 18 }
```

```
fgMdmOpMode OBJECT-TYPE
    SYNTAX      INTEGER {
                        online(0),
                        lowPower(1),
                        factoryTest(2),
                        offLine(3),
                        reset(4),
                        shuttingDown(5),
                        persistentLowPower(6),
                        modeOnlyLowPower(7),
                        unknown(255)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Modem Operation Mode.
         The following enumerated values are supported:
                        online(0)              - Device can acquire a system and make
calls.
                        lowPower(1)            - Device has temporarily disabled RF.
                        factoryTest(2)         - Special mode for manufacturer tests.
                        offLine(3)             - Device has deactivated RF and is
partially shutdown.
                        reset(4)               - Device is in the process of power
cycling.
                        shuttingDown(5)        - Device is in the process of shutting
down.
                        persistentLowPower(6)  - Device has disabled RF and state persists
even after a reset.
                        modeOnlyLowPower(7)    - Mode-only Low Power.
                        unknown(255)           - Unknown. "
    ::= { fgMdmInfoEntry 19 }

--
-- fortinet.fnFortiGateMib.fgInternalLTEModemsInfo.fgSimInfoTable
--

fgSimInfoTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgSimInfoEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table containing information applicable
         to SIM cards on internal LTE modems."
    ::= { fgInternalLTEModemsInfo 2 }

--
-- fortinet.fnFortiGateMib.fgInternalLTEModemsInfo.fgSimInfoTable.fgSimInfoEntry
--

fgSimInfoEntry OBJECT-TYPE
    SYNTAX      FgSimInfoEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information applicable
         to a particular SIM card on an particular LTE Modem.
         Although we only have one SIM slot and one internal modem now,
         in fact one modem supports multiple SIM slots, that's why we have
         fgMdmEntIndex in the record. It shows nothing if the modem is not detected."
    INDEX       { fgSimEntIndex }
    ::= { fgSimInfoTable 1 }

FgSimInfoEntry ::= SEQUENCE {
    fgSimEntIndex       FnIndex,
```

```
    fgSimMdmEntIndex    FnIndex,
    fgSimState          INTEGER,
    fgSimIccid          DisplayString,
    fgSimImsi           DisplayString,
    fgSimCountry        DisplayString,
    fgSimNetwork        DisplayString
}

fgSimEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Index used to identify the instance of a SIM card."
    ::= { fgSimInfoEntry 1 }

fgSimMdmEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Index used to identify the instance of an internal LTE modem."
    ::= { fgSimInfoEntry 2 }

fgSimState OBJECT-TYPE
    SYNTAX      INTEGER {
                            initialized(0),
                            lockedOrFailed(1),
                            notPresent(2),
                            reserved(3),
                            unknown(255)
                        }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        " SIM card state.
         The following enumerated values are supported:
                        initialized(0)        - UIM initialization completed.
                        lockedOrFailed(1)     - UIM is locked or failed.
                        notPresent(2)         - No UIM in the device.
                        reserved(3)           - Reserved, unknown.
                        unknown(255)          - UIM state currently unavailable. "
    ::= { fgSimInfoEntry 3 }

fgSimIccid OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "ICCID."
    ::= { fgSimInfoEntry 4 }

fgSimImsi OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "IMSI."
    ::= { fgSimInfoEntry 5 }

fgSimCountry OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..8))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
```

```
        "Carrier Country."
    ::= { fgSimInfoEntry 6 }

fgSimNetwork OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..16))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Carrier Network."
    ::= { fgSimInfoEntry 7 }

--
-- fortinet.fnFortiGateMib.fgInternalLTEModemsInfo.fgSignalInfoTable
--

fgSignalInfoTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgSignalInfoEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table containing information applicable
         to signal strength on an internal LTE modems."
    ::= { fgInternalLTEModemsInfo 3 }

--
-- fortinet.fnFortiGateMib.fgInternalLTEModemsInfo.fgSignalInfoTable.fgSignalInfoEntry
--

fgSignalInfoEntry OBJECT-TYPE
    SYNTAX      FgSignalInfoEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information applicable
         to signal strength on an internal LTE modem. If the modem with the modem index
         is not present, it shows nothing. If the specific type of signal is not present,
         the OID shows nothing either."
    INDEX       { fgSigMdmEntIndex }
    ::= { fgSignalInfoTable 1 }

FgSignalInfoEntry ::= SEQUENCE {
    fgSigMdmEntIndex    FnIndex,
    fgCdmaRssi          Integer32,
    fgCdmaEcio          Integer32,
    fgHdrRssi           Integer32,
    fgHdrEcio           Integer32,
    fgHdrSinr           Integer32,
    fgHdrIo             Integer32,
    fgGsm               Integer32,
    fgWcdmaRssi         Integer32,
    fgWcdmaEcio         Integer32,
    fgLteRssi           Integer32,
    fgLteRsrq           Integer32,
    fgLteRsrp           Integer32,
    fgLteSnr            Integer32,
    fgTdma              Integer32
}

fgSigMdmEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Index used to identify the instance of an internal LTE modem."
    ::= { fgSignalInfoEntry 1 }
```

```
fgCdmaRssi OBJECT-TYPE
    SYNTAX      Integer32(-128..127)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "RSSI for CDMA."
    ::= { fgSignalInfoEntry 2 }

fgCdmaEcio OBJECT-TYPE
    SYNTAX      Integer32(-65536..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "ECIO for CDMA."
    ::= { fgSignalInfoEntry 3 }

fgHdrRssi OBJECT-TYPE
    SYNTAX      Integer32(-128..127)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "RSSI for HDR."
    ::= { fgSignalInfoEntry 4 }

fgHdrEcio OBJECT-TYPE
    SYNTAX      Integer32(-65536..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "ECIO for HDR."
    ::= { fgSignalInfoEntry 5 }

fgHdrSinr OBJECT-TYPE
    SYNTAX      Integer32(0..8)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "SINR for HDR."
    ::= { fgSignalInfoEntry 6 }

fgHdrIo OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "IO for HDR."
    ::= { fgSignalInfoEntry 7 }

fgGsm OBJECT-TYPE
    SYNTAX      Integer32(-128..127)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "GSM Signal Strength."
    ::= { fgSignalInfoEntry 8 }

fgWcdmaRssi OBJECT-TYPE
    SYNTAX      Integer32(-128..127)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "RSSI for WCDMA."
    ::= { fgSignalInfoEntry 9 }
```

```
    fgWcdmaEcio OBJECT-TYPE
        SYNTAX      Integer32(-65536..65535)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "ECIO for WCDMA."
        ::= { fgSignalInfoEntry 10 }

    fgLteRssi OBJECT-TYPE
        SYNTAX      Integer32(-128..127)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "RSSI for LTE."
        ::= { fgSignalInfoEntry 11 }

    fgLteRsrq OBJECT-TYPE
        SYNTAX      Integer32(-128..127)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "RSRQ for LTE."
        ::= { fgSignalInfoEntry 12 }

    fgLteRsrp OBJECT-TYPE
        SYNTAX      Integer32(-65536..65535)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "RSRP for LTE."
        ::= { fgSignalInfoEntry 13 }

    fgLteSnr OBJECT-TYPE
        SYNTAX      Integer32(-65536..65535)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "SNR for LTE."
        ::= { fgSignalInfoEntry 14 }

    fgTdma OBJECT-TYPE
        SYNTAX      Integer32(-128..127)
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "TDMA Signal Strength."
        ::= { fgSignalInfoEntry 15 }

    --
    -- fortinet.fnFortiGateMib.fgInternalLTEModemsInfo.fgTrafficInfoTable
    --

    fgTrafficInfoTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF FgTrafficInfoEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "A table containing information applicable
             to data traffic information on an internal LTE modems."
        ::= { fgInternalLTEModemsInfo 4 }

    --
    -- fortinet.fnFortiGateMib.fgInternalLTEModemsInfo.fgTrafficInfoTable.fgTrafficInfoEntry
    --
```

```
fgTrafficInfoEntry OBJECT-TYPE
    SYNTAX      FgTrafficInfoEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information applicable
         to data traffic information on an internal LTE modem. If the modem with the modem
index
         is not present, it shows nothing."
    INDEX       { fgTrafMdmEntIndex }
    ::= { fgTrafficInfoTable 1 }

FgTrafficInfoEntry ::= SEQUENCE {
    fgTrafMdmEntIndex     FnIndex,
    fgTxPacksOK           Counter32,
    fgRxPacksOK           Counter32,
    fgTxPacksErr          Counter32,
    fgRxPacksErr          Counter32,
    fgTxPacksOverflow     Counter32,
    fgRxPacksOverflow     Counter32,
    fgTxBytesOK           Counter64,
    fgRxBytesOK           Counter64,
    fgLastCallTxBytesOK   Counter64,
    fgLastCallRxBytesOK   Counter64,
    fgTxPacksDrop         Counter32,
    fgRxPacksDrop         Counter32
}

fgTrafMdmEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Index used to identify the instance of an internal LTE modem."
    ::= { fgTrafficInfoEntry 1 }

fgTxPacksOK OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Tx Packets OK."
    ::= { fgTrafficInfoEntry 2 }

fgRxPacksOK OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Rx Packets OK."
    ::= { fgTrafficInfoEntry 3 }

fgTxPacksErr OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Tx Packets Error."
    ::= { fgTrafficInfoEntry 4 }

fgRxPacksErr OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
```

```
        "Rx Packets Error."
    ::= { fgTrafficInfoEntry 5 }

fgTxPacksOverflow OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Tx Packets Overflow."
    ::= { fgTrafficInfoEntry 6 }

fgRxPacksOverflow OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Rx Packets Olverflow."
    ::= { fgTrafficInfoEntry 7 }

fgTxBytesOK OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Tx Bytes OK."
    ::= { fgTrafficInfoEntry 8 }

fgRxBytesOK OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Rx Bytes OK."
    ::= { fgTrafficInfoEntry 9 }

fgLastCallTxBytesOK OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Last Call Tx Bytes OK."
    ::= { fgTrafficInfoEntry 10 }

fgLastCallRxBytesOK OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Last Call Rx Bytes OK."
    ::= { fgTrafficInfoEntry 11 }

fgTxPacksDrop OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Tx Packets Dropped."
    ::= { fgTrafficInfoEntry 12 }

fgRxPacksDrop OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Rx Packets Dropped."
```

```
    ::= { fgTrafficInfoEntry 13 }

--
-- fortinet.fnFortiGateMib.fgInternalLTEModemsInfo.fgSessInfoTable
--

fgSessInfoTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgSessInfoEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table containing information applicable
         to data session information on an internal LTE modems."
    ::= { fgInternalLTEModemsInfo 5 }

--
-- fortinet.fnFortiGateMib.fgInternalLTEModemsInfo.fgSessInfoTable.fgSessInfoEntry
--

fgSessInfoEntry OBJECT-TYPE
    SYNTAX      FgSessInfoEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information applicable
         to data session information on an internal LTE modem. In QMI stack, each modem
can have 2
         sessions at the same time, IPv4 and IPv6. In the future if MBIM is adopted, we
can have
         multiple VLAN sessions at the same time. It shows nothing if the modem is not
present."
    INDEX       { fgLteSessEntIndex }
    ::= { fgSessInfoTable 1 }

FgSessInfoEntry ::= SEQUENCE {
    fgLteSessEntIndex           FnIndex,
    fgSessMdmEntIndex           FnIndex,
    fdLteIfName                 DisplayString,
    fdLteSessConnStat           INTEGER,
    fdLteProfId                 Integer32,
    fdLteProfName               DisplayString,
    fdLteProfType               INTEGER,
    fdLtePdpType                INTEGER,
    fdLteProfApn                DisplayString,
    fdLteProfIpFamily           INTEGER,
    fdLteIpv4Addr               IpAddress,
    fdLteIpv4GwAddr             IpAddress,
    fdLteIpv4NetMask            IpAddress,
    fdLteIpv4PriDns             IpAddress,
    fdLteIpv4SecDns             IpAddress,
    fdLteIpv6Addr               Ipv6Address,
    fdLteIpv6PrefLen            Integer32,
    fdLteIpv6GwAddr             Ipv6Address,
    fdLteIpv6GwPrefLen          Integer32,
    fdLteIpv6PriDns             Ipv6Address,
    fdLteIpv6SecDns             Ipv6Address,
    fdLteMtu                    Integer32,
    fdLteAutoConn               INTEGER,
    fdLteNetType                INTEGER,
    fdLteNetTypeLas             INTEGER,
    fdLteLinkProto              INTEGER
}

fgLteSessEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
```

```
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Index used to identify the instance of a data session on an internal LTE modem."
    ::= { fgSessInfoEntry 1 }

fgSessMdmEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Index used to identify the instance of an internal LTE modem."
    ::= { fgSessInfoEntry 2 }

fdLteIfName OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..16))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Interface Name of an internal LTE modem."
    ::= { fgSessInfoEntry 3 }

fdLteSessConnStat OBJECT-TYPE
    SYNTAX      INTEGER {
                        unknown(0),
                        disconnected(1),
                        connected(2),
                        suspended(3),
                        authenticating(4)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Connection Status of a data session on an Internal LTE modem.
         The following enumerated values are supported:
                        unknown(0)            - Unknown status.
                        disconnected(1)       - Network is disconnected.
                        connected(2)          - Network is connected.
                        suspended(3)          - Network connection is suspended.
                        authenticating(4)     -  Network authentication is ongoing."
    ::= { fgSessInfoEntry 4 }

fdLteProfId OBJECT-TYPE
    SYNTAX      Integer32(0..255)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile index of a data session on an internal LTE modem."
    ::= { fgSessInfoEntry 5 }

fdLteProfName OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile name of a data session on an internal LTE modem."
    ::= { fgSessInfoEntry 6 }

fdLteProfType OBJECT-TYPE
    SYNTAX      INTEGER {
                        lpt3gpp(0),
                        lpt3gpp2(1)
                }
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
        "Wireless profile type of a data session on an internal LTE modem.
         The following enumerated values are supported:
                        lpt3gpp(0)   - 3GPP profile type.
                        lpt3gpp2(1)  - 3gpp2 profile type. "
    ::= { fgSessInfoEntry 7 }

fdLtePdpType OBJECT-TYPE
    SYNTAX      INTEGER {
                        ipv4(0),
                        ppp(1),
                        ipv6(2),
                        ipv4v6(3)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile PDP context type of a data session on an internal LTE modem.
         The following enumerated values are supported:
                        ipv4(0)   - IPv4.
                        ppp(1)    - PPP.
                        ipv6(2)   - IPv6.
                        ipv4v6(3) - IPv4 and IPv6. "
    ::= { fgSessInfoEntry 8 }

fdLteProfApn OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile APN name of a data session on an internal LTE modem."
    ::= { fgSessInfoEntry 9 }

fdLteProfIpFamily OBJECT-TYPE
    SYNTAX      INTEGER {
                        ipv4(4),
                        ipv6(6),
                        unspecified(8)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile IP Family of a data session on an internal LTE modem.
         The following enumerated values are supported:
                        ipv4(4)        - IPv4.
                        ipv6(6)        - IPv6.
                        unspecified(3) - None specified. "
    ::= { fgSessInfoEntry 10 }

fdLteIpv4Addr OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile IPv4 Address of a data session on an internal LTE modem.
        It shows nothing if a data session does not exist or the data session is not
        of IP Family IPv4."
    ::= { fgSessInfoEntry 11 }

fdLteIpv4GwAddr OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile IPv4 Gateway Address of a data session on an internal LTE modem.
```

```
        It shows nothing if a data session does not exist or the data session is not
        of IP Family IPv4."
    ::= { fgSessInfoEntry 12 }

fdLteIpv4NetMask OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile IPv4 Net Mask of a data session on an internal LTE modem.
        It shows nothing if a data session does not exist or the data session is not
        of IP Family IPv4."
    ::= { fgSessInfoEntry 13 }

fdLteIpv4PriDns OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile IPv4 Primary DNS Server Address of a data session on an internal
LTE modem.
        It shows nothing if a data session does not exist or the data session is not
        of IP Family IPv4."
    ::= { fgSessInfoEntry 14 }

fdLteIpv4SecDns OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile IPv4 Secondary DNS Server Address of a data session on an
internal LTE modem.
        It shows nothing if a data session does not exist or the data session is not
        of IP Family IPv4."
    ::= { fgSessInfoEntry 15 }

fdLteIpv6Addr OBJECT-TYPE
    SYNTAX      Ipv6Address
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile IPv6 Address of a data session on an internal LTE modem.
        It shows nothing if a data session does not exist or the data session is not
        of IP Family IPv6."
    ::= { fgSessInfoEntry 16 }

fdLteIpv6PrefLen OBJECT-TYPE
    SYNTAX      Integer32(0..127)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile IPv6 Address Prefix of a data session on an internal LTE modem.
        It shows nothing if a data session does not exist or the data session is not
        of IP Family IPv6."
    ::= { fgSessInfoEntry 17 }

fdLteIpv6GwAddr OBJECT-TYPE
    SYNTAX      Ipv6Address
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile IPv6 Gateway Address of a data session on an internal LTE modem.
        It shows nothing if a data session does not exist or the data session is not
        of IP Family IPv6."
    ::= { fgSessInfoEntry 18 }
```

```
fdLteIpv6GwPrefLen OBJECT-TYPE
    SYNTAX      Integer32(0..127)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile IPv6 Gateway Address Prefix of a data session on an internal LTE
modem.
        It shows nothing if a data session does not exist or the data session is not
        of IP Family IPv6."
    ::= { fgSessInfoEntry 19 }

fdLteIpv6PriDns OBJECT-TYPE
    SYNTAX      Ipv6Address
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile Primary DNS IPv6 Address of a data session on an internal LTE
modem.
        It shows nothing if a data session does not exist or the data session is not
        of IP Family IPv6."
    ::= { fgSessInfoEntry 20 }

fdLteIpv6SecDns OBJECT-TYPE
    SYNTAX      Ipv6Address
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile Secondary DNS IPv6 Address of a data session on an internal LTE
modem.
        It shows nothing if a data session does not exist or the data session is not
        of IP Family IPv6."
    ::= { fgSessInfoEntry 21 }

fdLteMtu OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile MTU of a data session on an internal LTE modem.
        It shows nothing if a data session does not exist."
    ::= { fgSessInfoEntry 22 }

fdLteAutoConn OBJECT-TYPE
    SYNTAX      INTEGER {
                        disabled(0),
                        enabled(1),
                        paused(2)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile auto connection status of a data session on an internal LTE
modem.
         The following enumerated values are supported:
                        disabled(0)       - Disabled.
                        enabled(1)        - Enabled.
                        paused(2)         - Paused (resume on power cycle). "
    ::= { fgSessInfoEntry 23 }

fdLteNetType OBJECT-TYPE
    SYNTAX      INTEGER {
                        unknown(-1),
                        cdma1x(1),
                        evdo(2),
```

```
                        gsm(3),
                        umts(4),
                        evdoReva(5),
                        edge(6),
                        hsdpa(7),
                        hsupa(8),
                        hsdpaHsupa(9),
                        lte(10),
                        ehrpd(11),
                        hsdpaPlus(12),
                        hsdpaPlusHsupa(13),
                        dchsdpaPlus(14),
                        dchspdaPlusHsupa(15)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile network type of a data session on an internal LTE modem.
         The following enumerated values are supported:
                        unknown(-1)             - Unknown.
                        cdma1x(1)               - CDMA2000 1x.
                        evdo(2)                 - CDMA2000 HRPD 1xEV-DO.
                        gsm(3)                  - GSM.
                        umts(4)                 - UMTS.
                        evdoReva(5)             - CDMA2000 HRPD 1xEV-DO RevA.
                        edge(6)                 - EDGE.
                        hsdpa(7)                - HSDPA and WCDMA.
                        hsupa(8)                - WCDMA and HSUPA.
                        hsdpaHsupa(9)           - HSDPA and HSUPA.
                        lte(10)                 - LTE.
                        ehrpd(11)               - CDMA2000 eHRPD.
                        hsdpaPlus(12)           - HSDPA+ and WCDMA.
                        hsdpaPlusHsupa(13)      - HSDPA+ and HSUPA.
                        dchsdpaPlus(14)         - DC-HSDPA+ and WCDMA.
                        dchspdaPlusHsupa(15)    - DC-HSDPA+ and HSUPA."
    ::= { fgSessInfoEntry 24 }

fdLteNetTypeLas OBJECT-TYPE
    SYNTAX      INTEGER {
                        unknown(-1),
                        cdma1x(1),
                        evdo(2),
                        gsm(3),
                        umts(4),
                        evdoReva(5),
                        edge(6),
                        hsdpa(7),
                        hsupa(8),
                        hsdpaHsupa(9),
                        lte(10),
                        ehrpd(11),
                        hsdpaPlus(12),
                        hsdpaPlusHsupa(13),
                        dchsdpaPlus(14),
                        dchspdaPlusHsupa(15)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile network type of the last data session on an internal LTE modem.
         The following enumerated values are supported:
                        unknown(-1)             - Unknown.
                        cdma1x(1)               - CDMA2000 1x.
                        evdo(2)                 - CDMA2000 HRPD 1xEV-DO.
                        gsm(3)                  - GSM.
```

```
                        umts(4)                 - UMTS.
                        evdoReva(5)             - CDMA2000 HRPD 1xEV-DO RevA.
                        edge(6)                 - EDGE.
                        hsdpa(7)                - HSDPA and WCDMA.
                        hsupa(8)                - WCDMA and HSUPA.
                        hsdpaHsupa(9)           - HSDPA and HSUPA.
                        lte(10)                 - LTE.
                        ehrpd(11)               - CDMA2000 eHRPD.
                        hsdpaPlus(12)           - HSDPA+ and WCDMA.
                        hsdpaPlusHsupa(13)      - HSDPA+ and HSUPA.
                        dchsdpaPlus(14)         - DC-HSDPA+ and WCDMA.
                        dchspdaPlusHsupa(15)    - DC-HSDPA+ and HSUPA."
    ::= { fgSessInfoEntry 25 }

fdLteLinkProto OBJECT-TYPE
    SYNTAX      INTEGER {
                        unknown(0),
                        ieee8023(1),
                        rawIp(2)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Wireless profile data link protocol of a data session on an internal LTE modem.
         The following enumerated values are supported:
                        unknown(0)      - Unknown.
                        ieee8023(1)     - IEEE 802.3 ethernet mode.
                        rawIp(2)        - Raw IP mode. "
    ::= { fgSessInfoEntry 26 }

--
-- fortinet.fnFortiGateMib.fgInternalLTEModemsInfo.fgGpsInfoTable
--

fgGpsInfoTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgGpsInfoEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table containing information applicable
         to GPS information on an internal LTE modems."
    ::= { fgInternalLTEModemsInfo 6 }

--
-- fortinet.fnFortiGateMib.fgInternalLTEModemsInfo.fgGpsInfoTable.fgGpsInfoEntry
--

fgGpsInfoEntry OBJECT-TYPE
    SYNTAX      FgGpsInfoEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information applicable
         to GPS information on an internal LTE modem. If the modem with the modem index
         is not present, GPS deamon is not enabled, or a GPS location is not acquired
successfully,
         it shows nothing. Also since no matter how many modems we have in a device, the
location
         information is the same, here the index is always 1."
    INDEX       { fgGpsMdmEntIndex }
    ::= { fgGpsInfoTable 1 }

FgGpsInfoEntry ::= SEQUENCE {
    fgGpsMdmEntIndex     FnIndex,
    fgGpsEnabled         INTEGER,
```

```
    fgLatitude           DisplayString,
    fgLongitude          DisplayString,
    fgUtcTime            DisplayString,
    fgLocalTime          DisplayString
}

fgGpsMdmEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Index used to identify the instance of an internal LTE modem, here it is always
1."
    ::= { fgGpsInfoEntry 1 }

fgGpsEnabled OBJECT-TYPE
    SYNTAX      INTEGER { no(0), yes(1) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Is GPS daemon enabled."
    ::= { fgGpsInfoEntry 2 }

fgLatitude OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..16))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Latitude."
    ::= { fgGpsInfoEntry 3 }

fgLongitude OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..16))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Longitude."
    ::= { fgGpsInfoEntry 4 }

fgUtcTime OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..64))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "UTC Time."
    ::= { fgGpsInfoEntry 5 }

fgLocalTime OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..64))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Local Time."
    ::= { fgGpsInfoEntry 6 }

--
-- fortinet.fnFortiGateMib.fgInternalLTEModemsInfo.fgDatausageInfoTable
--

fgDatausageInfoTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgDatausageInfoEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table containing information applicable
```

```
          to data usage information on an internal LTE modems."
    ::= { fgInternalLTEModemsInfo 7 }

--
--
fortinet.fnFortiGateMib.fgInternalLTEModemsInfo.fgDatausageInfoTable.fgDatausageInfoEntry
--

fgDatausageInfoEntry OBJECT-TYPE
    SYNTAX      FgDatausageInfoEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information applicable
         to data usage information on an internal LTE modem. If the modem with the modem
index
         is not present,  data usage trackingis not enabled, it shows nothing."
    INDEX       { fgDatausageMdmEntIndex }
    ::= { fgDatausageInfoTable 1 }

FgDatausageInfoEntry ::= SEQUENCE {
    fgDatausageMdmEntIndex     FnIndex,
    fgDatausageEnabled         INTEGER,
    fgDataOut                  Counter64,
    fgDataIn                   Counter64
}

fgDatausageMdmEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Index used to identify the instance of an internal LTE modem."
    ::= { fgDatausageInfoEntry 1 }

fgDatausageEnabled OBJECT-TYPE
    SYNTAX      INTEGER{ no(0), yes(1) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Data usage tracking enabled."
    ::= { fgDatausageInfoEntry 2 }

fgDataOut OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Bytes Out."
    ::= { fgDatausageInfoEntry 3 }

fgDataIn OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Bytes In."
    ::= { fgDatausageInfoEntry 4 }

--
-- fortinet.fnFortiGateMib.fgNPU
--

fgNPU OBJECT IDENTIFIER
    ::= { fnFortiGateMib 20 }
```

```
--
-- fortinet.fnFortiGateMib.fgNPU.fgNPUInfo
--

FgNPUIndex ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS      current
    DESCRIPTION
        "data type for NPU indexes"
    SYNTAX      Integer32 (0..255)

fgNPUInfo OBJECT IDENTIFIER
    ::= { fgNPU 1 }

fgNPUNumber OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of NPUs in NPUTable"
    ::= { fgNPUInfo 1 }

fgNPUName OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..64))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Name of the NPU"
    ::= { fgNPUInfo 2 }

fgNPUDrvDriftSum OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Summation of driver session drift counters(fgNPUDrvDrift)"
    ::= { fgNPUInfo 3 }

--
-- fortinet.fnFortiGateMib.fgNPU.fgNPUTables
--

fgNPUTables OBJECT IDENTIFIER
    ::= { fgNPU 2 }

--
-- fortinet.fnFortiGateMib.fgNPU.fgNPUTables.fgNPUTable
--

fgNPUTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FgNPUEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of NPUs in the device"
    ::= { fgNPUTables 1 }

fgNPUEntry OBJECT-TYPE
    SYNTAX      FgNPUEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information applicable
         to a particular NPU"
```

```
    INDEX       { fgNPUEntIndex }
    ::= { fgNPUTable 1 }

FgNPUEntry ::= SEQUENCE {
    fgNPUEntIndex    FgNPUIndex,
    fgNPUSessionTblSize Gauge32,
    fgNPUSessionCount Gauge32,
    fgNPUDrvDrift Integer32
}

fgNPUEntIndex OBJECT-TYPE
    SYNTAX      FgNPUIndex (0..255)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "NPU index used to uniquely identify NPU in the system."
    ::= { fgNPUEntry 1 }

fgNPUSessionTblSize OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Size of session table in the NPU"
    ::= { fgNPUEntry 2 }

fgNPUSessionCount OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of active sessions in the NPU"
    ::= { fgNPUEntry 3 }

fgNPUDrvDrift OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Difference of session count between driver and hardware"
    ::= { fgNPUEntry 4 }

--
-- fortinet.fnFortiGateMib.fgLog
--

fgLog OBJECT IDENTIFIER
    ::= { fnFortiGateMib 21}

--
-- fortinet.fnFortiGateMib.fgLog.fgLogInfo
--

FgLogDeviceIndex ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS      current
    DESCRIPTION
        "Data type for log device indexes"
    SYNTAX      Integer32 (0..255)

fgLogInfo OBJECT IDENTIFIER
    ::= { fgLog 1 }

fgLogDeviceNumber OBJECT-TYPE
    SYNTAX      Integer32
```

```
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The number of log devices in LogDevices"
        ::= { fgLogInfo 1 }

--
-- fortinet.fnFortiGateMib.fgLog.fgLogDevices
--

fgLogDevices OBJECT IDENTIFIER
        ::= { fgLog 2 }

--
-- fortinet.fnFortiGateMib.fgLog.fgLogDevices.fgLogDeviceTable
--
fgLogDeviceTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF FgLogDeviceEntry
        MAX-ACCESS   not-accessible
        STATUS       current
        DESCRIPTION
            "Table of log devices on the fortigate"
        ::= { fgLogDevices 1 }

fgLogDeviceEntry OBJECT-TYPE
    SYNTAX      FgLogDeviceEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information about a specific log device"
    INDEX       { fgLogDeviceEntryIndex }
    ::= { fgLogDeviceTable 1 }

FgLogDeviceEntry ::= SEQUENCE {
        fgLogDeviceEntryIndex     FgLogDeviceIndex,
        fgLogDeviceEnabled        Integer32,
        fgLogDeviceName           DisplayString,
        fgLogDeviceSentCount      Counter32,
        fgLogDeviceRelayedCount   Counter32,
        fgLogDeviceCachedCount    Gauge32,
        fgLogDeviceFailedCount    Counter32,
        fgLogDeviceDroppedCount   Counter32
}

fgLogDeviceEntryIndex OBJECT-TYPE
    SYNTAX      FgLogDeviceIndex (0..255)
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "Log device index in the list of reported log devices"
        ::= { fgLogDeviceEntry 1 }

fgLogDeviceEnabled OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  not-accessible
    STATUS      current
        DESCRIPTION
            "Indicated whether the log device is enabled"
        ::= { fgLogDeviceEntry 2 }

fgLogDeviceName OBJECT-TYPE
        SYNTAX      DisplayString (SIZE(0..64))
        MAX-ACCESS  read-only
        STATUS      current
    DESCRIPTION
```

```
            "Name of the log device"
        ::= { fgLogDeviceEntry 3 }

    fgLogDeviceSentCount OBJECT-TYPE
        SYNTAX       Counter32
            MAX-ACCESS   read-only
            STATUS       current
            DESCRIPTION
                "Number of logs which have been sent"
            ::= { fgLogDeviceEntry 4 }

    fgLogDeviceRelayedCount OBJECT-TYPE
        SYNTAX       Counter32
            MAX-ACCESS   read-only
            STATUS       current
            DESCRIPTION
                "Number of logs which have been relayed"
            ::= { fgLogDeviceEntry 5 }

    fgLogDeviceCachedCount OBJECT-TYPE
        SYNTAX       Gauge32
            MAX-ACCESS   read-only
            STATUS       current
            DESCRIPTION
                "Number of logs which are cached for later sending"
            ::= { fgLogDeviceEntry 6 }

    fgLogDeviceFailedCount OBJECT-TYPE
        SYNTAX       Counter32
            MAX-ACCESS   read-only
            STATUS       current
            DESCRIPTION
                "Number of logs which have failed to send"
            ::= { fgLogDeviceEntry 7 }

    fgLogDeviceDroppedCount OBJECT-TYPE
        SYNTAX       Counter32
            MAX-ACCESS   read-only
            STATUS       current
            DESCRIPTION
                "Number of logs which have been dropped"
            ::= { fgLogDeviceEntry 8 }

    --
    -- fortinet.fnFortiGateMib.fgConfig
    --

    fgConfig OBJECT IDENTIFIER
        ::= { fnFortiGateMib 22 }

    fgConfigStatus OBJECT IDENTIFIER
        ::= { fgConfig 1 }

    fgConfigSerial OBJECT-TYPE
        SYNTAX      Counter32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The serial number of the current configuration, it is increased each time the
    configuration changes."
        ::= { fgConfigStatus 1 }

    fgConfigChecksum OBJECT-TYPE
        SYNTAX      OCTET STRING
        MAX-ACCESS  read-only
```

```
    STATUS      current
    DESCRIPTION
        "The checksum of the current configuration."
    ::= { fgConfigStatus 2 }

fgConfigLastChangeTime OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The value of sysUpTime when the configuration was last changed."
    ::= { fgConfigStatus 3 }


--
-- fortinet.fnFortiGateMib.fgMibConformance
--

fgMibConformance OBJECT IDENTIFIER
    ::= { fnFortiGateMib 100 }

--
-- fortinet.fnFortiGateMib.fgTraps
--

fgTrapVpnTunUp NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fgVpnTrapLocalGateway,
                  fgVpnTrapRemoteGateway, fgVpnTrapPhase1Name }
    STATUS      current
    DESCRIPTION
        "Indicates that the specified VPN tunnel has been brought up."
    ::= { fgTrapPrefix 301 }

fgTrapVpnTunDown NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fgVpnTrapLocalGateway,
                  fgVpnTrapRemoteGateway, fgVpnTrapPhase1Name }
    STATUS      current
    DESCRIPTION
        "The specified VPN tunnel has been brought down."
    ::= { fgTrapPrefix 302 }

fgTrapHaSwitch NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "The specified cluster member has transitioned from a slave role to a master
role."
    ::= { fgTrapPrefix 401 }

fgTrapHaStateChange NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial }
    STATUS      deprecated
    DESCRIPTION
        "Trap being sent when the HA cluster
         member changes its state"
    ::= { fgTrapPrefix 402 }

fgTrapHaHBFail NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial }
    STATUS      current
    DESCRIPTION
        "The heartbeat device failure count has exceeded the configured threshold."
    ::= { fgTrapPrefix 403 }

fgTrapHaMemberDown NOTIFICATION-TYPE
```

```
    OBJECTS     { fnSysSerial }
    STATUS      current
    DESCRIPTION
        "The specified device (by serial number) is moving to a down state."
    ::= { fgTrapPrefix 404 }

fgTrapHaMemberUp NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial }
    STATUS      current
    DESCRIPTION
        "A new cluster member has joined the cluster."
    ::= { fgTrapPrefix 405 }

fgTrapIpsSignature NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fgIpsTrapSigId, fgIpsTrapSrcIp, fgIpsTrapSigMsg }
    STATUS      current
    DESCRIPTION
        "An IPS signature has been triggered"
    ::= { fgTrapPrefix 503 }

fgTrapIpsAnomaly NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fgIpsTrapSigId, fgIpsTrapSrcIp, fgIpsTrapSigMsg }
    STATUS      current
    DESCRIPTION
        "An IPS anomaly has been detected"
    ::= { fgTrapPrefix 504 }

fgTrapIpsPkgUpdate NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "The IPS signature database has been updated"
    ::= { fgTrapPrefix 505 }

fgTrapIpsFailOpen NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "The IPS network buffer is full"
    ::= { fgTrapPrefix 506 }

fgTrapAvVirus NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fgAvTrapVirName }
    STATUS      current
    DESCRIPTION
        "A virus has been detected by the anti-virus engine"
    ::= { fgTrapPrefix 601 }

fgTrapAvOversize NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "An over-sized file has been detected by the anti-virus engine"
    ::= { fgTrapPrefix 602 }

fgTrapAvPattern NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "The anti-virus engine has blocked a file because it matched a configured pattern"
    ::= { fgTrapPrefix 603 }

fgTrapAvFragmented NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
```

```
    DESCRIPTION
        "The anti-virus engine has detected a fragmented file"
    ::= { fgTrapPrefix 604 }

fgTrapAvEnterConserve NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "The anti-virus engine has entered conservation mode due to low memory conditions"
    ::= { fgTrapPrefix 605 }

fgTrapAvBypass NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "The anti-virus engine has been bypassed due to conservation mode"
    ::= { fgTrapPrefix 606 }

fgTrapAvOversizePass NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "An over-sized file has been detected,
         but has been passed due to configuration"
    ::= { fgTrapPrefix 607 }

fgTrapAvOversizeBlock NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "An over-sized file has been detected
         and has been blocked"
    ::= { fgTrapPrefix 608 }

fgTrapFazDisconnect NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial }
    STATUS      current
    DESCRIPTION
        "The device has been disconnected from the FortiAnalyzer."
    ::= { fgTrapPrefix 701 }

fgTrapWcApUp NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fgWcApVdom, fgWcApSerial, fgWcApName }
    STATUS      current
    DESCRIPTION
        "Indicates that the specified AP is up."
    ::= { fgTrapPrefix 801 }

fgTrapWcApDown NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fgWcApVdom, fgWcApSerial, fgWcApName }
    STATUS      current
    DESCRIPTION
        "Indicates that the specified AP is down."
    ::= { fgTrapPrefix 802 }

fgTrapFcSwUp NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fgFcSwVdom, fgFcSwSerial, fgFcSwName }
    STATUS      current
    DESCRIPTION
        "Indicates that the specified switch controller session is up."
    ::= { fgTrapPrefix 901 }

fgTrapFcSwDown NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fgFcSwVdom, fgFcSwSerial, fgFcSwName }
    STATUS      current
```

```
    DESCRIPTION
        "Indicates that the specified switch controller session is down."
    ::= { fgTrapPrefix 902 }

fgFmTrapDeployComplete NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial }
    STATUS      current
    DESCRIPTION
        "Indicates when deployment of a new configuration has been completed. Used for
verification by FortiManager."
    ::= { fgFmTrapPrefix 1000 }

fgFmTrapDeployInProgress NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial }
    STATUS      current
    DESCRIPTION
        "Indicates that a configuration change was not immediate and that the change is
currently in progress. Used for verification by FortiManager."
    ::= { fgFmTrapPrefix 1002 }

fgFmTrapConfChange NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial }
    STATUS      current
    DESCRIPTION
        "The device configuration has been changed by something other than the managing
FortiManager device."
    ::= { fgFmTrapPrefix 1003 }

fgFmTrapIfChange NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, ifName, fgManIfIp, fgManIfMask, fgManIfIp6 }
    STATUS      current
    DESCRIPTION
        "Trap is sent to the managing FortiManager if an interface IP is changed"
    ::= { fgFmTrapPrefix 1004 }

fgTrapServerLoadBalanceRealServerDown NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fgServerLoadBalanceRealServerAddress,
fgServerLoadBalanceVirtualServerName, fgServerLoadBalanceRealServerAddress6 }
    STATUS      current
    DESCRIPTION
        "One of servers in a Server Load Balance group goes down."
    ::= { fgTrapPrefix 1101 }

fgTrapPerCpuHigh NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fgPerCpuHighDetails }
    STATUS      current
    DESCRIPTION
        "Indicates that per-CPU usage has exceeded the configured threshold."
    ::= { fgTrapPrefix 1102 }

fgTrapDeviceNew NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, ifIndex, fgVdEntIndex, fgDeviceCreated,
fgDeviceLastSeen, fgDeviceMacAddress }
    STATUS      current
    DESCRIPTION
        "A new device is found."
    ::= { fgTrapPrefix 1201 }

--
-- fortinet.fnFortiGateMib.fgMibConformance
--

fgFmTrapGroup NOTIFICATION-GROUP
    NOTIFICATIONS { fgFmTrapDeployComplete, fgFmTrapDeployInProgress,
                    fgFmTrapConfChange, fgFmTrapIfChange }
```

```
    STATUS      current
    DESCRIPTION
        "Traps are intended for use in conjunction with a FortiManager."
    ::= { fgMibConformance 1 }

fgFmTrapObjectGroup OBJECT-GROUP
    OBJECTS     { fgManIfIp, fgManIfMask,fgManIfIp6 }
    STATUS      current
    DESCRIPTION
        "These objects support the traps in the fgFmTrapGroup."
    ::= { fgMibConformance 2 }

fgAdminObjectGroup OBJECT-GROUP
    OBJECTS     { fgAdminIdleTimeout, fgAdminLcdProtection }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to administration of the device."
    ::= { fgMibConformance 3 }

fgSystemObjectGroup OBJECT-GROUP
    OBJECTS     { fgSysVersion, fgSysCpuUsage,
                  fgSysMemUsage, fgSysMemCapacity,
                  fgSysDiskUsage, fgSysDiskCapacity,
                  fgSysSesCount, fgSysLowMemUsage,
                  fgSysLowMemCapacity, fgSysSesRate1,
                  fgSysSesRate10, fgSysSesRate30,
                  fgSysSesRate60,
                  fgSysSes6Count, fgSysSes6Rate1,
                  fgSysSes6Rate10, fgSysSes6Rate30,
                  fgSysSes6Rate60, fgSysUpTime,
                  fgSysNeedLogPartitionScan }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to the system status of the device."
    ::= { fgMibConformance 4 }

fgSoftwareObjectGroup OBJECT-GROUP
    OBJECTS     { fgSysVersionAv, fgSysVersionIps, fgSysVersionAvEt, fgSysVersionIpsEt }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to software running on the device."
    ::= { fgMibConformance 5 }

fgHwSensorsObjectGroup OBJECT-GROUP
    OBJECTS     { fgHwSensorCount, fgHwSensorEntName,
                  fgHwSensorEntValue, fgHwSensorEntAlarmStatus }
    STATUS      current
    DESCRIPTION
        "Object pertaining to hardware sensors on the device."
    ::= { fgMibConformance 6 }

fgHighAvailabilityObjectGroup OBJECT-GROUP
    OBJECTS     { fgHaSystemMode, fgHaGroupId, fgHaPriority, fgHaOverride,
                  fgHaAutoSync, fgHaSchedule, fgHaGroupName, fgHaStatsSerial,
                  fgHaStatsCpuUsage, fgHaStatsMemUsage,
                  fgHaStatsNetUsage, fgHaStatsSesCount,
                  fgHaStatsPktCount, fgHaStatsByteCount,
                  fgHaStatsIdsCount, fgHaStatsAvCount, fgHaStatsHostname,
                  fgHaStatsSyncStatus, fgHaStatsSyncDatimeSucc, fgHaStatsSyncDatimeUnsucc,
                  fgHaStatsGlobalChecksum, fgHaStatsMasterSerial,
                  fgHaTrapMemberSerial }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to High Availability clustering of FortiGate devices."
    ::= { fgMibConformance 7 }
```

```
fgVpnObjectGroup OBJECT-GROUP
    OBJECTS     { fgVpnDialupGateway, fgVpnDialupLifetime,
                  fgVpnDialupTimeout, fgVpnDialupSrcBegin,
                  fgVpnDialupSrcEnd, fgVpnDialupDstAddr, fgVpnDialupVdom,
                  fgVpnDialupInOctets, fgVpnDialupOutOctets,
                  fgVpnTunEntPhase1Name, fgVpnTunEntPhase2Name,
                  fgVpnTunEntRemGwyIp, fgVpnTunEntRemGwyPort,
                  fgVpnTunEntLocGwyIp, fgVpnTunEntLocGwyPort,
                  fgVpnTunEntSelectorSrcBeginIp,
                  fgVpnTunEntSelectorSrcEndIp,
                  fgVpnTunEntSelectorSrcPort,
                  fgVpnTunEntSelectorDstBeginIp,
                  fgVpnTunEntSelectorDstEndIp,
                  fgVpnTunEntSelectorDstPort, fgVpnTunEntSelectorProto,
                  fgVpnTunEntLifeSecs, fgVpnTunEntLifeBytes,
                  fgVpnTunEntTimeout, fgVpnTunEntInOctets,
                  fgVpnTunEntOutOctets, fgVpnTunEntStatus,
                  fgVpnTunEntVdom, fgVpnSslState,
                  fgVpnSslStatsLoginUsers, fgVpnSslStatsMaxUsers,
                  fgVpnSslStatsActiveWebSessions,
                  fgVpnSslStatsMaxWebSessions,
                  fgVpnSslStatsActiveTunnels, fgVpnSslStatsMaxTunnels,
                  fgVpnSslTunnelVdom, fgVpnSslTunnelUserName,
                  fgVpnSslTunnelSrcIp, fgVpnSslTunnelIp,
                  fgVpnSslTunnelUpTime, fgVpnSslTunnelBytesIn,
                  fgVpnSslTunnelBytesOut, fgVpnTrapLocalGateway,
                  fgVpnTrapRemoteGateway, fgVpnTrapPhase1Name, fgVpnTunnelUpCount }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to Virtual Priavet Networking on FortiGate devices."
    ::= { fgMibConformance 8 }

fgFirewallObjectGroup OBJECT-GROUP
    OBJECTS     { fgFwPolPktCount, fgFwPolByteCount, fgFwUserNumber,
                  fgFwPolPktCountHc, fgFwPolByteCountHc,
                  fgFwUserAuthTimeout, fgFwUserName, fgFwUserAuth,
                  fgFwUserState, fgFwUserVdom, fgIpSessProto,
                  fgIpSessFromAddr, fgIpSessFromPort, fgIpSessToAddr,
                  fgIpSessToPort, fgIpSessExp, fgIpSessVdom,
                  fgIpSessNumber, fgIp6SessNumber, fgFwPol6PktCount,
                  fgFwPol6ByteCount, fgFwPolLastUsed, fgFwPol6LastUsed,
                  fgFwIppStatsName, fgFwIppStatsType,
                  fgFwIppStatsTotalSessions, fgFwIppStatsTcpSessions,
                  fgFwIppStatsUdpSessions, fgFwIppStatsOtherSessions,
                  fgFwGtpStatsRequest, fgFwGtpStatsEchoRequest, fgFwGtpStatsTunnel,
                  fgFwGtpStatsTunnelV0, fgFwGtpStatsPath, fgFwGtpStatsBearer,
                  fgFwGtpStatsFteid, fgFwGtpStatsProfile, fgFwGtpStatsImsi,
                  fgFwGtpStatsApn, fgFwGtpStatsApnShaper, fgFwGtpStatsTunnelLimiter,
                  fgFwGtpStatsAdvPolicies, fgFwGtpStatsIeRemovePolicies,
fgFwGtpStatsIpPolicy,
                  fgFwGtpStatsNoipPolicy, fgFwGtpStatsIeWlEntry, fgFwGtpStatsClash,
fgFwGtpStatsDrop,
                  fgFwGtpRtStatsCForwarded, fgFwGtpRtStatsCRejected,
fgFwGtpRtStatsCDropped0,
                  fgFwGtpRtStatsCDropped1, fgFwGtpRtStatsCDropped2,
fgFwGtpRtStatsCDropped3,
                  fgFwGtpRtStatsCDropped4, fgFwGtpRtStatsCDropped5,
fgFwGtpRtStatsCDropped6,
                  fgFwGtpRtStatsCDropped7, fgFwGtpRtStatsCDropped8,
fgFwGtpRtStatsCDropped9,
                  fgFwGtpRtStatsCDropped10, fgFwGtpRtStatsCDropped11,
fgFwGtpRtStatsCDropped12,
                  fgFwGtpRtStatsCDropped13, fgFwGtpRtStatsCDropped14,
fgFwGtpRtStatsCDropped15,
```

```
                    fgFwGtpRtStatsCDropped16, fgFwGtpRtStatsCDropped17,
fgFwGtpRtStatsCDropped18,
                    fgFwGtpRtStatsCDropped19, fgFwGtpRtStatsCDropped20,
fgFwGtpRtStatsCDropped21,
                    fgFwGtpRtStatsCDropped22, fgFwGtpRtStatsCDropped23,
fgFwGtpRtStatsDForwarded,
                    fgFwGtpRtStatsDDroppedSanity, fgFwGtpRtStatsDDroppedMalMsg,
fgFwGtpRtStatsDDroppedNoState,
                    fgFwGtpRtStatsDDroppedMalIe, fgFwGtpRtStatsDDroppedGtpInGtp,
fgFwGtpRtStatsDDroppedSpoof,
                    fgFwGtpRtStatsDDroppedIpPol, fgFwGtpRtStatsDDroppedMsgFilter,
fgFwGtpRtStatsDDroppedMsgRateLimit,
                    fgFwGtpRtStatsDDroppedUnknownVersion, fgFwGtpRtStatsBForwarded,
fgFwGtpRtStatsBDroppedSanity,
                    fgFwGtpRtStatsBDroppedMalMsg, fgFwGtpRtStatsBDroppedMalIe,
fgFwGtpRtStatsBDroppedMsgFilter }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to Firewall functionality on FortiGate devices."
    ::= { fgMibConformance 9 }

fgAppServicesObjectGroup OBJECT-GROUP
    OBJECTS     { fgApHTTPReqProcessed,
                  fgApSMTPReqProcessed, fgApSMTPSpamDetected,
                  fgApPOP3ReqProcessed, fgApPOP3SpamDetected,
                  fgApIMAPReqProcessed, fgApIMAPSpamDetected,
                  fgApNNTPReqProcessed, fgApIMUpTime, fgApIMMemUsage,
                  fgApIMReqProcessed, fgApSIPUpTime, fgApSIPMemUsage,
                  fgApSIPClientReg, fgApSIPCallHandling, fgApSIPServices,
                  fgApSIPOtherReq, fgAppSuNumber, fgAppSuFileScanned,
                  fgAppVoIPConn, fgAppVoIPCallBlocked,
                  fgAppP2PConnBlocked, fgAppP2PProtEntBytes,
                  fgAppP2PProtoEntLastReset, fgAppIMMessages,
                  fgAppIMFileTransfered, fgAppIMFileTxBlocked,
                  fgAppIMConnBlocked, fgAppFnbamStatsTotalAuthReqs,
                  fgAppFnbamStatsTotalEagainErrs, fgAppFnbamStatsTotalLdapFails,
                  fgApFTPReqProcessed, fgApHTTPConnections, fgApFTPConnections,
                  fgApSMTPConnections, fgApPOP3Connections, fgApIMAPConnections,
                  fgApNNTPConnections, fgApHTTPMaxConnections,
                  fgApFTPMaxConnections, fgApSMTPMaxConnections,
                  fgApPOP3MaxConnections, fgApIMAPMaxConnections,
                  fgApNNTPMaxConnections }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to application proxy and filtering services on FortiGate
devices."
    ::= { fgMibConformance 10 }

fgAntivirusObjectGroup OBJECT-GROUP
    OBJECTS     { fgAvVirusDetected, fgAvVirusBlocked,
                  fgAvHTTPVirusDetected, fgAvHTTPVirusBlocked,
                  fgAvSMTPVirusDetected, fgAvSMTPVirusBlocked,
                  fgAvPOP3VirusDetected, fgAvPOP3VirusBlocked,
                  fgAvIMAPVirusDetected, fgAvIMAPVirusBlocked,
                  fgAvFTPVirusDetected, fgAvFTPVirusBlocked,
                  fgAvIMVirusDetected, fgAvIMVirusBlocked,
                  fgAvNNTPVirusDetected, fgAvNNTPVirusBlocked,
                  fgAvOversizedDetected, fgAvOversizedBlocked,
                  fgAvMAPIVirusDetected, fgAvMAPIVirusBlocked,
                  fgAvSMBVirusDetected, fgAvSMBVirusBlocked,
                  fgAvTrapVirName }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to Antivirus services on FortiGate devices."
    ::= { fgMibConformance 11 }
```

```
fgIntrusionPrevtObjectGroup OBJECT-GROUP
    OBJECTS     { fgIpsTrapSigId, fgIpsTrapSrcIp, fgIpsTrapSigMsg,
                  fgIpsIntrusionsDetected, fgIpsIntrusionsBlocked,
                  fgIpsCritSevDetections, fgIpsHighSevDetections,
                  fgIpsMedSevDetections, fgIpsLowSevDetections,
                  fgIpsInfoSevDetections, fgIpsSignatureDetections,
                  fgIpsAnomalyDetections }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to Intrusion Detection and Prevention services on FortiGate
devices."
    ::= { fgMibConformance 12 }

fgWebFilterObjectGroup OBJECT-GROUP
    OBJECTS     { fgWfHTTPBlocked, fgWfHTTPSBlocked, fgWfHTTPURLBlocked,
                  fgWfHTTPSURLBlocked, fgWfActiveXBlocked,
                  fgWfCookieBlocked, fgWfAppletBlocked,
                  fgFgWfHTTPExamined, fgFgWfHTTPSExamined,
                  fgFgWfHTTPAllowed, fgFgWfHTTPSAllowed,
                  fgFgWfHTTPBlocked, fgFgWfHTTPSBlocked,
                  fgFgWfHTTPLogged, fgFgWfHTTPSLogged,
                  fgFgWfHTTPOverridden, fgFgWfHTTPSOverridden }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to FortiGate and FortiGuard based Web Filtering services on
FortiGate devices."
    ::= { fgMibConformance 13 }

fgVirtualDomainObjectGroup OBJECT-GROUP
    OBJECTS     { fgVdNumber, fgVdMaxVdoms, fgVdEnabled, fgVdEntName, fgVdEntIndex,
                  fgVdEntOpMode, fgVdTpMgmtAddrType, fgVdTpMgmtAddr,
                  fgVdEntCpuUsage, fgVdEntMemUsage, fgVdEntSesCount, fgVdEntSesRate,
                  fgVdTpMgmtMask, fgVdEntHaState }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to Virtual Firewall Domain services on FortiGate devices."
    ::= { fgMibConformance 14 }

fgAdministrationObjectGroup OBJECT-GROUP
    OBJECTS     { fgAdminVdom }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to the administration of FortiGate device."
    ::= { fgMibConformance 15 }

fgIntfObjectGroup OBJECT-GROUP
    OBJECTS     { fgIntfEntVdom, fgIntfEntEstUpBandwidth, fgIntfEntEstDownBandwidth,
                  fgIntfVrrpCount, fgIntfVrrpEntVrId, fgIntfVrrpEntGrpId,
                  fgIntfVrrpEntIfName, fgIntfVrrpEntState, fgIntfVrrpEntVrIp,
                  fgIntfVlanHbCount, fgIntfVlanHbEntIfName, fgIntfVlanHbEntSerial,
fgIntfVlanHbEntState,
                  fgIntfBcAllocatedBandwidth, fgIntfBcGuaranteedBandwidth,
fgIntfBcMaxBandwidth,
                  fgIntfBcCurrentBandwidth, fgIntfBcBytes, fgIntfBcDrops,
                  fgIntfBcInAllocatedBandwidth, fgIntfBcInGuaranteedBandwidth,
fgIntfBcInMaxBandwidth,
                  fgIntfBcInCurrentBandwidth, fgIntfBcInBytes, fgIntfBcInDrops }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to the interface table of FortiGate device."
    ::= { fgMibConformance 16 }

fgProcessorsObjectGroup OBJECT-GROUP
    OBJECTS     { fgProcessorCount, fgProcessorUsage, fgProcessorUsage5sec,
```

```
                fgProcessorType, fgProcessorContainedIn, fgProcessorPktRxCount,
                fgProcessorPktTxCount, fgProcessorPktDroppedCount,
                fgProcessorUserUsage, fgProcessorSysUsage,
                fgProcessorModuleCount, fgProcModType,
                fgProcModName, fgProcModDescr, fgProcModProcessorCount,
                fgProcModMemCapacity, fgProcModMemUsage, fgPerCpuHighDetails,
                fgProcModSessionCount, fgProcModSACount }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to the processors table of FortiGate device."
    ::= { fgMibConformance 17 }

fgNotificationGroup NOTIFICATION-GROUP
    NOTIFICATIONS { fgTrapVpnTunUp, fgTrapVpnTunDown, fgTrapHaSwitch,
                    fgTrapHaHBFail, fgTrapHaMemberDown, fgTrapHaMemberUp,
                    fgTrapIpsSignature, fgTrapIpsAnomaly,
                    fgTrapIpsPkgUpdate, fgTrapIpsFailOpen,
                    fgTrapAvVirus, fgTrapAvOversize,
                    fgTrapAvPattern, fgTrapAvFragmented,
                    fgTrapAvEnterConserve, fgTrapAvBypass,
                    fgTrapAvOversizePass, fgTrapAvOversizeBlock,
                    fgTrapFazDisconnect, fgTrapWcApUp, fgTrapWcApDown, fgTrapDeviceNew,
                    fgTrapPerCpuHigh,
                    fgTrapFcSwUp, fgTrapFcSwDown, fgTrapServerLoadBalanceRealServerDown }
    STATUS      current
    DESCRIPTION
        "Notifications that can be generated from a FortiGate device."
    ::= { fgMibConformance 18 }

fgObsoleteNotificationsGroup NOTIFICATION-GROUP
    NOTIFICATIONS { fgTrapHaStateChange }
    STATUS      deprecated
    DESCRIPTION
        "Notifications that have been deprecated, but may still be generated by older
models."
    ::= { fgMibConformance 19 }

fgExplicitProxyObjectGroup OBJECT-GROUP
    OBJECTS     { fgExplicitProxyUpTime, fgExplicitProxyMemUsage, fgExplicitProxyRequests,
                fgExplicitProxyUsers, fgExplicitProxySessions,
                fgExplicitProxyVirus, fgExplicitProxyBannedWords, fgExplicitProxyPolicy,
                fgExplicitProxyOversized, fgExplicitProxyArchNest,
fgExplicitProxyArchSize,
                fgExplicitProxyArchEncrypted, fgExplicitProxyArchMultiPart,
                fgExplicitProxyArchUnsupported, fgExplicitProxyArchBomb,
fgExplicitProxyArchCorrupt,
                fgExplicitProxyFilteredApplets, fgExplicitProxyFilteredActiveX,
                fgExplicitProxyFilteredJScript, fgExplicitProxyFilteredJS,
                fgExplicitProxyFilteredVBS, fgExplicitProxyFilteredOthScript,
                fgExplicitProxyBlockedDLP, fgExplicitProxyBlockedConType,
                fgExplicitProxyExaminedURLs, fgExplicitProxyAllowedURLs,
fgExplicitProxyBlockedURLs,
                fgExplicitProxyLoggedURLs, fgExplicitProxyOverriddenURLs }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to explicit proxy"
    ::= { fgMibConformance 20 }

fgWebCacheObjectGroup OBJECT-GROUP
    OBJECTS     { fgWebCacheUpTime,
                fgWebCacheRAMLimit, fgWebCacheRAMUsage, fgWebCacheRAMHits,
                fgWebCacheRAMMisses, fgWebCacheRequests, fgWebCacheBypass,
                fgWebCacheDiskLimit, fgWebCacheDiskUsage, fgWebCacheDiskHits,
                fgWebCacheDiskMisses, fgWebCacheDiskFailure }
    STATUS      current
```

```
    DESCRIPTION
        "Objects pertaining to explicit proxy, web cache and wan optimization."
    ::= { fgMibConformance 21 }

fgWanOptObjectGroup OBJECT-GROUP
    OBJECTS     { fgMemCacheLimit, fgMemCacheUsage, fgMemCacheHits, fgMemCacheMisses,
                fgByteCacheRAMLimit, fgByteCacheRAMUsage,
                fgWanOptUpTime, fgWanOptReductionRate, fgWanOptLanTraffic,
fgWanOptWanTraffic,
                fgWanOptLanInTraffic, fgWanOptLanOutTraffic, fgWanOptWanInTraffic,
fgWanOptWanOutTraffic,
                fgWanOptTunnels, fgWanOptLANBytesIn, fgWanOptLANBytesOut,
                fgWanOptWANBytesIn, fgWanOptWANBytesOut, fgWanOptDiskLimit,
fgWanOptDiskUsage,
                fgWanOptDiskHits, fgWanOptDiskMisses, fgWanOptDiskFailure }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to explicit proxy, web cache and wan optimization."
    ::= { fgMibConformance 22 }

fgObsoleteAppServicesObjectGroup OBJECT-GROUP
    OBJECTS     { fgApHTTPUpTime, fgApHTTPMemUsage,
                  fgApSMTPUpTime, fgApSMTPMemUsage,
                  fgApPOP3UpTime, fgApPOP3MemUsage,
                  fgApIMAPUpTime, fgApIMAPMemUsage,
                  fgApNNTPUpTime, fgApNNTPMemUsage,
                  fgApFTPUpTime, fgApFTPMemUsage }
    STATUS      deprecated
    DESCRIPTION
        "Objects that have been deprecated, but may still be generated by older models."
    ::= { fgMibConformance 23 }

fgSystemAdvancedObjectGroup OBJECT-GROUP
    OBJECTS     { fgSIAdvMemPageCache, fgSIAdvMemCacheActive,
                  fgSIAdvMemCacheInactive, fgSIAdvMemBuffer,
                  fgSIAdvMemEnterKerConsThrsh,
                  fgSIAdvMemLeaveKerConsThrsh,
                  fgSIAdvMemEnterProxyConsThrsh,
                  fgSIAdvMemLeaveProxyConsThrsh,
                  fgSIAdvSesEphemeralCount, fgSIAdvSesEphemeralLimit,
                  fgSIAdvSesClashCount, fgSIAdvSesExpCount,
                  fgSIAdvSesSyncQFCount, fgSIAdvSesAcceptQFCount,
                  fgSIAdvSesNoListenerCount }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to the system advanced status of the device."
    ::= { fgMibConformance 24 }

fgWcObjectGroup OBJECT-GROUP
    OBJECTS     { fgWcApVdom, fgWcApSerial, fgWcApName,
                  fgWcInfoName, fgWcInfoLocation, fgWcInfoWtpCapacity, fgWcInfoWtpManaged,
                  fgWcInfoWtpSessions, fgWcInfoStationCapacity, fgWcInfoStationCount,
                  fgWcWlanSsid, fgWcWlanBroadcastSsid, fgWcWlanSecurity,
fgWcWlanEncryption,
                  fgWcWlanAuthentication, fgWcWlanRadiusServer, fgWcWlanUserGroup,
                  fgWcWlanLocalBridging, fgWcWlanVlanId, fgWcWlanMeshBackhaul,
                  fgWcWlanStationCapacity, fgWcWlanStationCount,
                  fgWcWtpProfilePlatform, fgWcWtpProfileDataChannelDtlsPolicy,
                  fgWcWtpProfileCountryString,
                  fgWcWtpProfileRadioMode, fgWcWtpProfileRadioApScan,
fgWcWtpProfileRadioWidsProfile,
                  fgWcWtpProfileRadioDarrp, fgWcWtpProfileRadioFrequencyHandoff,
                  fgWcWtpProfileRadioApHandoff, fgWcWtpProfileRadioBeaconInterval,
                  fgWcWtpProfileRadioDtimPeriod, fgWcWtpProfileRadioBand,
                  fgWcWtpProfileRadioChannelBonding, fgWcWtpProfileRadioChannel,
```

```
                    fgWcWtpProfileRadioAutoTxPowerControl,
    fgWcWtpProfileRadioAutoTxPowerLow,
                    fgWcWtpProfileRadioAutoTxPowerHigh, fgWcWtpProfileRadioTxPowerLevel,
                    fgWcWtpProfileRadioVaps, fgWcWtpProfileRadioStationCapacity,
    fgWcWtpProfileRadioChannelWidth,
                    fgWcWtpConfigWtpAdmin, fgWcWtpConfigWtpName, fgWcWtpConfigWtpLocation,
                    fgWcWtpConfigWtpProfile, fgWcWtpConfigRadioEnable,
    fgWcWtpConfigRadioAutoTxPowerControl,
                    fgWcWtpConfigRadioAutoTxPowerLow, fgWcWtpConfigRadioAutoTxPowerHigh,
                    fgWcWtpConfigRadioTxPowerLevel, fgWcWtpConfigRadioBand,
    fgWcWtpConfigRadioApScan,
                    fgWcWtpConfigVapAll, fgWcWtpConfigVaps,
                    fgWcWtpSessionWtpIpAddressType, fgWcWtpSessionWtpIpAddress,
    fgWcWtpSessionWtpLocalIpAddressType,
                    fgWcWtpSessionWtpLocalIpAddress, fgWcWtpSessionWtpBaseMacAddress,
                    fgWcWtpSessionConnectionState, fgWcWtpSessionWtpUpTime,
                    fgWcWtpSessionWtpDaemonUpTime, fgWcWtpSessionWtpSessionUpTime,
                    fgWcWtpSessionWtpProfileName, fgWcWtpSessionWtpModelNumber,
                    fgWcWtpSessionWtpHwVersion, fgWcWtpSessionWtpSwVersion,
                    fgWcWtpSessionWtpBootVersion, fgWcWtpSessionWtpRegionCode,
                    fgWcWtpSessionWtpStationCount, fgWcWtpSessionWtpByteRxCount,
                    fgWcWtpSessionWtpByteTxCount, fgWcWtpSessionWtpCpuUsage,
                    fgWcWtpSessionWtpMemoryUsage, fgWcWtpSessionWtpMemoryCapacity,
                    fgWcWtpSessionRadioMode, fgWcWtpSessionRadioBaseBssid,
                    fgWcWtpSessionRadioCountryString, fgWcWtpSessionRadioCountryCode,
                    fgWcWtpSessionRadioOperatingChannel, fgWcWtpSessionRadioOperatingPower,
                    fgWcWtpSessionRadioStationCount,
                    fgWcWtpSessionVapSsid, fgWcWtpSessionVapStationCount,
                    fgWcWtpSessionVapByteRxCount, fgWcWtpSessionVapByteTxCount,
                    fgWcStaWlan, fgWcStaWtpId, fgWcStaRadioId, fgWcStaVlanId,
    fgWcStaIpAddressType, fgWcStaIpAddress,
                    fgWcStaVci, fgWcStaHost, fgWcStaUser, fgWcStaGroup, fgWcStaSignal,
    fgWcStaNoise,
                    fgWcStaIdle, fgWcStaBandwidthTx, fgWcStaBandwidthRx, fgWcStaChannel,
                    fgWcStaRadioType, fgWcStaSecurity, fgWcStaEncrypt, fgWcStaOnline
                }
        STATUS      current
        DESCRIPTION
            "Objects pertaining to wireless controller."
        ::= { fgMibConformance 25 }

    fgFcObjectGroup OBJECT-GROUP
        OBJECTS     { fgFcSwVdom, fgFcSwSerial, fgFcSwName }
        STATUS      current
        DESCRIPTION
            "Objects pertaining to switch controller."
        ::= { fgMibConformance 26 }

    fgServerLoadBalanceObjectGroup OBJECT-GROUP
        OBJECTS     { fgServerLoadBalanceRealServerAddress,
    fgServerLoadBalanceVirtualServerName, fgServerLoadBalanceRealServerAddress6 }
        STATUS      current
        DESCRIPTION
            "Objects pertaining to Server Load Balance group."
        ::= { fgMibConformance 27 }

    fgUsbportsObjectGroup OBJECT-GROUP
        OBJECTS     { fgUsbportCount, fgUsbportPlugged, fgUsbportVersion,
                      fgUsbportClass, fgUsbportVendId, fgUsbportProdId, fgUsbportRevision,
                      fgUsbportManufacturer, fgUsbportProduct, fgUsbportSerial
                    }
        STATUS      current
        DESCRIPTION
            "Objects pertaining to USB device group."
        ::= { fgMibConformance 28 }
```

```
fgUsbModemInfoGroup OBJECT-GROUP
    OBJECTS     { fgUsbModemSignalStrength, fgUsbModemStatus, fgUsbModemSimState,
                fgUsbModemVendor, fgUsbModemProduct, fgUsbModemNetwork, fgUsbModemId,
fgUsbModemSimId }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to USB Modem Info group."
    ::= { fgMibConformance 29 }

fgDeviceObjectGroup OBJECT-GROUP
    OBJECTS     { fgDeviceMacAddress, fgDeviceCreated, fgDeviceLastSeen }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to Device group."
    ::= { fgMibConformance 30 }

fgLinkMonitorGroup OBJECT-GROUP
    OBJECTS     { fgLinkMonitorNumber, fgLinkMonitorName, fgLinkMonitorState,
                  fgLinkMonitorLatency, fgLinkMonitorJitter, fgLinkMonitorPacketSend,
fgLinkMonitorPacketRecv,
                  fgLinkMonitorPacketLoss, fgLinkMonitorVdom,
                  fgLinkMonitorBandwidthIn, fgLinkMonitorBandwidthOut,
fgLinkMonitorBandwidthBi,
                  fgLinkMonitorOutofSeq
                }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to Link Monitor group."
    ::= { fgMibConformance 31 }

fgInternalModemInfoGroup OBJECT-GROUP
    OBJECTS     { fgMdmDetected, fgMdmVendor,
                fgMdmModel, fgMdmRevision, fgMdmMsisdn, fgMdmEsn, fgMdmImei,
                fgMdmHwRevision, fgMdmMeid, fgMdmSwRev, fgMdmSku, fgMdmFsn, fgMdmPrlVer,
                fgMdmFwVer, fgMdmPriFwVer, fgMdmCarrierAbbr, fgMdmActState, fgMdmOpMode}
    STATUS      current
    DESCRIPTION
        "Objects pertaining to Internal Modem Info group."
    ::= { fgMibConformance 32 }

fgInternalModemSIMInfoGroup OBJECT-GROUP
    OBJECTS     { fgSimMdmEntIndex, fgSimState,
                fgSimIccid, fgSimImsi, fgSimCountry, fgSimNetwork}
    STATUS      current
    DESCRIPTION
        "Objects pertaining to Internal Modem SIM card Info group."
    ::= { fgMibConformance 33 }

fgInternalModemSigInfoGroup OBJECT-GROUP
    OBJECTS     { fgCdmaRssi, fgCdmaEcio,
                fgHdrRssi, fgHdrEcio, fgHdrSinr, fgHdrIo,
                fgGsm, fgWcdmaRssi, fgWcdmaEcio, fgLteRssi,
                fgLteRsrq, fgLteRsrp, fgLteSnr, fgTdma}
    STATUS      current
    DESCRIPTION
        "Objects pertaining to Internal Modem Signal Info group."
    ::= { fgMibConformance 34 }

fgInternalModemTrafficInfoGroup OBJECT-GROUP
    OBJECTS     { fgTxPacksOK, fgRxPacksOK,
                fgTxPacksErr, fgRxPacksErr, fgTxPacksOverflow, fgRxPacksOverflow,
                fgTxBytesOK, fgRxBytesOK, fgLastCallTxBytesOK, fgLastCallRxBytesOK,
                fgTxPacksDrop, fgRxPacksDrop}
    STATUS      current
```

```
    DESCRIPTION
        "Objects pertaining to Internal Modem Data Traffic Info group."
    ::= { fgMibConformance 35 }

fgInternalModemSessInfoGroup OBJECT-GROUP
    OBJECTS     { fgSessMdmEntIndex, fdLteIfName,
                fdLteSessConnStat, fdLteProfId, fdLteProfName, fdLteProfType,
                fdLtePdpType, fdLteProfApn, fdLteProfIpFamily, fdLteIpv4Addr,
                fdLteIpv4GwAddr, fdLteIpv4NetMask, fdLteIpv4PriDns, fdLteIpv4SecDns,
                fdLteIpv6Addr, fdLteIpv6PrefLen, fdLteIpv6GwAddr, fdLteIpv6GwPrefLen,
                fdLteIpv6PriDns, fdLteIpv6SecDns, fdLteMtu, fdLteAutoConn,
                fdLteNetType, fdLteNetTypeLas, fdLteLinkProto}
    STATUS      current
    DESCRIPTION
        "Objects pertaining to Internal Modem Data Traffic Info group."
    ::= { fgMibConformance 36 }

fgInternalModemGpsInfoGroup OBJECT-GROUP
    OBJECTS     { fgGpsEnabled, fgLatitude,
                fgLongitude, fgUtcTime, fgLocalTime}
    STATUS      current
    DESCRIPTION
        "Objects pertaining to Internal Modem GPS Info group."
    ::= { fgMibConformance 37 }

fgInternalModemDatausageInfoGroup OBJECT-GROUP
    OBJECTS     { fgDatausageEnabled, fgDataOut, fgDataIn}
    STATUS      current
    DESCRIPTION
        "Objects pertaining to Internal Modem data usage Info group."
    ::= { fgMibConformance 38 }

fgVWLHealthCheckLinkGroup OBJECT-GROUP
    OBJECTS     { fgVWLHealthCheckLinkNumber, fgVWLHealthCheckLinkName,
fgVWLHealthCheckLinkSeq,
                  fgVWLHealthCheckLinkState, fgVWLHealthCheckLinkLatency,
fgVWLHealthCheckLinkJitter,
                  fgVWLHealthCheckLinkPacketSend, fgVWLHealthCheckLinkPacketRecv,
fgVWLHealthCheckLinkPacketLoss,
                  fgVWLHealthCheckLinkVdom, fgVWLHealthCheckLinkBandwidthIn,
fgVWLHealthCheckLinkBandwidthOut,
                  fgVWLHealthCheckLinkBandwidthBi
                }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to VWL health check group."
    ::= { fgMibConformance 39 }

fgDisksObjectGroup OBJECT-GROUP
    OBJECTS     { fgDiskCount, fgDiskName }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to disks name list."
    ::= { fgMibConformance 40 }

fgNPUGroup OBJECT-GROUP
    OBJECTS     { fgNPUNumber, fgNPUName, fgNPUDrvDriftSum, fgNPUSessionTblSize,
                      fgNPUSessionCount, fgNPUDrvDrift }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to NPU on FortiGate devices."
    ::= { fgMibConformance 41 }

fgSlaProbeClientGroup OBJECT-GROUP
    OBJECTS     { fgSlaProbeClientNumber, fgSlaProbeClientIP, fgSlaProbeClientState,
```

```
                    fgSlaProbeClientAvgLatency, fgSlaProbeClientAvgLatencySD,
                    fgSlaProbeClientAvgLatencyDS, fgSlaProbeClientMinLatency,
                    fgSlaProbeClientMinLatencySD, fgSlaProbeClientMinLatencyDS,
                    fgSlaProbeClientMaxLatency, fgSlaProbeClientMaxLatencySD,
                    fgSlaProbeClientMaxLatencyDS, fgSlaProbeClientAvgJitter,
                    fgSlaProbeClientAvgJitterSD, fgSlaProbeClientAvgJitterDS,
                    fgSlaProbeClientMinJitter, fgSlaProbeClientMinJitterSD,
                    fgSlaProbeClientMinJitterDS, fgSlaProbeClientMaxJitter,
                    fgSlaProbeClientMaxJitterSD, fgSlaProbeClientMaxJitterDS,
                    fgSlaProbeClientPktloss, fgSlaProbeClientPktlossSD,
                    fgSlaProbeClientPktlossDS, fgSlaProbeClientOutofSeq,
                    fgSlaProbeClientOutofSeqSD, fgSlaProbeClientOutofSeqDS
                }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to SLA Probe client group."
    ::= { fgMibConformance 42 }

fgDNSProxyObjectGroup OBJECT-GROUP
    OBJECTS     { fgDNSProxyStatsUdpCacheHit, fgDNSProxyStatsUdpRatingCacheHit,
fgDNSProxyStatsUdpReq,
                    fgDNSProxyStatsUdpRes, fgDNSProxyStatsUdpFwd, fgDNSProxyStatsUdpRetrans,
fgDNSProxyStatsUdpTo,
                    fgDNSProxyStatsUdpFtgRes, fgDNSProxyStatsUdpFtgFwd,
fgDNSProxyStatsUdpFtgRetrans }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to DNS Proxy group."
    ::= { fgMibConformance 43 }

fgLogGroup OBJECT-GROUP
    OBJECTS     { fgLogDeviceNumber, fgLogDeviceName, fgLogDeviceSentCount,
fgLogDeviceRelayedCount,
                      fgLogDeviceCachedCount, fgLogDeviceFailedCount,
fgLogDeviceDroppedCount }
        STATUS      current
        DESCRIPTION
            "Objects pertaining to log group."
        ::= { fgMibConformance 44 }

fgConfigGroup OBJECT-GROUP
    OBJECTS     { fgConfigSerial, fgConfigChecksum, fgConfigLastChangeTime }
        STATUS      current
        DESCRIPTION
            "Objects pertaining to log group."
        ::= { fgMibConformance 45 }

fgDpdkEngsObjectGroup OBJECT-GROUP
    OBJECTS     { fgDpdkEngCount, fgDpdkEngRxUsage, fgDpdkEngVnpUsage,
                fgDpdkEngIpsUsage, fgDpdkEngTxUsage, fgDpdkEngIdle}
    STATUS      current
    DESCRIPTION
        "Objects pertaining to the Dpdk Engine table of FortiGate device."
    ::= { fgMibConformance 46 }


fgMIBCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
        "The compliance statement for the application MIB."

    MODULE      -- this module

        GROUP   fgFmTrapGroup
        DESCRIPTION
```

```
            "This group is mandatory for any FortiGate device being managed by a
FortiManager."

        GROUP   fgNotificationGroup
        DESCRIPTION
              "Notifications are feature dependant. See manual for feature
               information."

        GROUP   fgFmTrapObjectGroup
        DESCRIPTION
              "Model and feature specific."

        GROUP   fgAdminObjectGroup
        DESCRIPTION
              "Model and feature specific."

        GROUP   fgSystemObjectGroup
        DESCRIPTION
              "Model and feature specific."

        GROUP   fgSoftwareObjectGroup
        DESCRIPTION
              "Model and feature specific."

        GROUP   fgHwSensorsObjectGroup
        DESCRIPTION
              "Model and feature specific."

        GROUP   fgHighAvailabilityObjectGroup
        DESCRIPTION
              "Model and feature specific."

        GROUP   fgVpnObjectGroup
        DESCRIPTION
              "Model and feature specific."

        GROUP   fgFirewallObjectGroup
        DESCRIPTION
              "Model and feature specific."

        GROUP   fgAppServicesObjectGroup
        DESCRIPTION
              "Model and feature specific."

        GROUP   fgAntivirusObjectGroup
        DESCRIPTION
              "Model and feature specific."

        GROUP   fgIntrusionPrevtObjectGroup
        DESCRIPTION
              "Model and feature specific."

        GROUP   fgWebFilterObjectGroup
        DESCRIPTION
              "Model and feature specific."

        GROUP   fgVirtualDomainObjectGroup
        DESCRIPTION
              "Model and feature specific."

        GROUP   fgAdministrationObjectGroup
        DESCRIPTION
              "Model and feature specific."

        GROUP   fgIntfObjectGroup
```

```
DESCRIPTION
      "Model and feature specific."

GROUP   fgProcessorsObjectGroup
DESCRIPTION
      "Model and feature specific."

GROUP   fgExplicitProxyObjectGroup
DESCRIPTION
      "Model and feature specific."

GROUP   fgWebCacheObjectGroup
DESCRIPTION
      "Model and feature specific."

GROUP   fgWanOptObjectGroup
DESCRIPTION
      "Model and feature specific."

GROUP   fgSystemAdvancedObjectGroup
DESCRIPTION
      "Model and feature specific."

GROUP   fgWcObjectGroup
DESCRIPTION
      "Model and feature specific."

GROUP   fgFcObjectGroup
DESCRIPTION
      "Model and feature specific."

GROUP   fgServerLoadBalanceObjectGroup
DESCRIPTION
      "Model and feature specific."

GROUP   fgUsbportsObjectGroup
DESCRIPTION
      "Model and feature specific."

GROUP   fgUsbModemInfoGroup
DESCRIPTION
      "Model and feature specific."

GROUP   fgDeviceObjectGroup
DESCRIPTION
      "Model and feature specific."

GROUP   fgLinkMonitorGroup
DESCRIPTION
      "Model and feature specific."

GROUP   fgInternalModemInfoGroup
DESCRIPTION
      "Model and feature specific."

GROUP   fgInternalModemSIMInfoGroup
DESCRIPTION
      "Model and feature specific."

GROUP   fgInternalModemSigInfoGroup
DESCRIPTION
      "Model and feature specific."

GROUP   fgInternalModemTrafficInfoGroup
DESCRIPTION
```

```
                "Model and feature specific."

            GROUP   fgInternalModemSessInfoGroup
            DESCRIPTION
                "Model and feature specific."

            GROUP   fgInternalModemGpsInfoGroup
            DESCRIPTION
                "Model and feature specific."

            GROUP   fgInternalModemDatausageInfoGroup
            DESCRIPTION
                "Model and feature specific."

            GROUP   fgVWLHealthCheckLinkGroup
            DESCRIPTION
                "Model and feature specific."

            GROUP   fgDisksObjectGroup
            DESCRIPTION
                "Model and feature specific."

            GROUP   fgNPUGroup
            DESCRIPTION
                "Model and feature specific."

            GROUP   fgSlaProbeClientGroup
            DESCRIPTION
                "Model and feature specific."

            GROUP   fgDNSProxyObjectGroup
            DESCRIPTION
                "Model and feature specific."
            GROUP   fgLogGroup
            DESCRIPTION
                "Model and feature specific."
            GROUP   fgConfigGroup
            DESCRIPTION
                "Model and feature specific."
            GROUP   fgDpdkEngsObjectGroup
            DESCRIPTION
                "Model and feature specific."


        ::= { fgMibConformance 100 }

    fg300MibCompliance MODULE-COMPLIANCE
        STATUS      deprecated
        DESCRIPTION
            "The backwards compatibility compliance statement for the application MIB."

        MODULE      -- this module

            GROUP   fgObsoleteNotificationsGroup
            DESCRIPTION
                "Model and feature specific. May be implemented by some firmwares, but
    should not be relied on."

        ::= { fgMibConformance 101 }

    fgObsolteMIBCompliance MODULE-COMPLIANCE
        STATUS      deprecated
        DESCRIPTION
            "The compliance statement for the application MIB."
```

```
    MODULE      -- this module

        GROUP   fgObsoleteAppServicesObjectGroup
        DESCRIPTION
              "Deprecated AppService objects."

    ::= { fgMibConformance 102 }

END -- end of module FORTINET-FORTIGATE-MIB.
```

Data: 28 de outubro de 2020

Cliente: TRIBUNAL DE JUSTIÇA DO ESTADO DA PARAÍBA
LICITAÇÃO Nº 019/2020
PROCESSO ADMINISTRATIVO ELETRÔNICO: 2020012776

Por meio desta carta, informamos que o equipamento FortiGate modelo FG-600E permite o número de 80.000 usuários autenticados.

Atenciosamente,
Fortinet, Inc.

Digitally signed by ALEXANDRE OLIVEIRA BONATTI:07311140609
Date: 2020.10.29 10:35:01 -03'00'

Alexandre Bonatti
Director, Systems Engineering – Brasil

Observe que, não obstante qualquer disposição em contrário: (1) as obrigações da Fortinet relacionadas a especificações, licenças, suporte, assinaturas, certificações, garantias e quaisquer outras garantias do produto são: (a) inválidas para produtos que foram adulterados ou modificados por terceiros e (b) sujeita em todos os aspectos aos processos, políticas e termos padrão da Fortinet, que a Fortinet pode mudar a qualquer momento a seu exclusivo e absoluto critério; (2) A Fortinet se reserva o direito de modificar planos técnicos, roadmaps e datas de liberação a qualquer momento a exclusivo e absoluto critério da Fortinet. (3) A Fortinet se isenta de responsabilidade por erros de digitação, tradução ou impressão. (4) Este documento é para fins informativos e não se destina a criar obrigações contratuais pela Fortinet ou comprometimento promissório ou direito de confiar nas declarações. (5) Declarações aqui sobre o desempenho do produto e características podem ser contextuais, por exemplo, baseadas em testes em em um ambiente particular, como em um ambiente de laboratório, e pode não ser preciso em todos os contextos, como em um ambiente em produção. (6) O signatário deste documento está baseando todas as declarações aqui em seus conhecimentos no momento da assinatura sem qualquer obrigação para investigar as declarações, e pode confiar totalmente na revisão e informações de outros. (7) Produtos e serviços não são oferecidos gratuitamente e os direitos só são concedidos sujeitos a pagamento integral à Fortinet e seus distribuidores e revendedores, todas as vendas são finais e aplicam-se as políticas e termos e condições da Fortinet, como o EULA padrão da Fortinet e os termos de suporte, alguns dos quais estão localizados em https://www.fortinet.com/corporate/about-us/legal.html .(8) A Fortinet não tem nenhuma obrigação de atualizar e não pretende atualizar as declarações aqui contidas, mesmo que, por exemplo, o signatário descubra que as declarações são de fato falsas ou que os planos mudaram.

Recife, 27 de novembro de 2020.

Ao
TRIBUNAL DE JUSTIÇA DA PARAÍBA
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO
GERÊNCIA DE INFRAESTRUTURA DE TI

ATT. Sr. José de Oliveira e José Medeiros

Ref.: **PREGÃO ELETRÔNICO Nº 019/2020**
RESPOSTA À DILIGÊNCIA

Prezados Senhores,

Em resposta à diligência recebida nesta data, esclarecemos:

ITEM 1
3.2.3. As Licenças de Atualização de Segurança devem ter prazo de vigência de 60 (sessenta) meses, contados a partir da aplicação destas nos produtos.
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGuard_Security_Services.pdf - As Licenças de Atualização de Segurança (FortiGuard Bundle UNIFIED PROTECTION) estão configuradas com prazo de vigência de 60 (sessenta) meses, contados a partir da aplicação destas nos produtos.
R.: No documento indicado, não ficou claro o cumprimento relativo ao prazo de vigência de 60 (sessenta) meses
Resposta Newsupri:
O prazo de vigência das licenças e garantia é variável, podendo ser de 12, 36 ou 60 meses, por exemplo. Na página 5 do referido documento é possível observar part number com este formato "FC-10-#####-247-02-DD". O símbolo "#####" indicará o produto e o "DD" indicará a quantidade de meses de cobertura. Os documentos não mostram todas as possibilidades de configuração de produtos e vigências. Para o item em questão, foram configurados 60 meses conforme pode ser observado no nosso documento de Comprovação Técnica. Os part numbers destes itens são FC-10-F6H0E-950-02-60, FC-10-F100F-950-02-60 e FC-10-0060F-950-02-60, respectivamente.

ITEM 2
5.3. Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas. https://www.fortinet.com/content/dam/fortinet/assets/datasheets/fortimanager.pdf 4 O FortiManager esta licenciado em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas (110 Equipamentos do tipo Firewall).
R.: Na página do documento indicado, não ficou claro o cumprimento relativo ao caráter permanente/perpétuo da licença para todas as funcionalidades e quantidades mencionadas

Resposta Newsupri:
Na página 6 do documento do fabricante referenciado na diligência, é possível observar todas as possibilidades de ordem (aquisição ou assinatura/subscrição) para este produto.
No primeiro grupo pode ser observada as opções de HARDWARE (FMG-200F até FMG-3700F) com opção de upgrade para uma maior quantidade de dispositivos gerenciados.

Documento 78 página 1 assinado, do processo nº 2020012776, nos termos da Lei 11.419. ADME.19484.46061.78169.01285-0
Nelson de Espindola Vasconcelos [033.228.264-30] em 27/11/2020 13:56

Na sequência observa-se as opções do mesmo produto em formato de MÁQUINA VIRTUAL (VM), também com opção de upgrade para uma maior quantidade de dispositivos gerenciados.
Pode-se observar que para opção de MÁQUINA VIRTUAL, existe a opção VM e a opção VM Subscription.
Como pode ser observado na página 2 da nossa proposta comercial, ofertamos o produto VM, que é uma licença perpetua, e não a opção VM Subscription que indicaria ser uma assinatura (não perpétua).
Em relação as quantidades mencionadas, refere-se a soma total de 110 dispositivos, onde 10 unidades fazem parte da licença FMG-VM-BASE e 100 unidades fazem parte da licença FMG-VM-100-UG como pode ser observado na mesma seção do referido documento.
Em relação às funcionalidades, pode-se observar que não existe nenhum tipo de opção para ser adquirida ou assinada em relação às funcionalidades, o que indica que todas as funcionalidades do produto já estão incluídas no mesmo.

ITEM 3
6.11. Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas. - - O Appliance FortiAnalyzer 800F está licenciado em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas.
R.: Não ficou claro o cumprimento relativo à cobertura da licença em caráter permanente/ perpétuo para todas as funcionalidades e quantidades mencionadas em documentação oficial do fabricante

Na página 7 do documento do fabricante referenciado na diligência, é possível observar todas as possibilidades de ordem (aquisição ou assinatura/subscrição) para este produto.
No primeiro grupo pode ser observada as opções de HARDWARE (FAZ-150G até FAZ-3700F) que se diferenciam pela capacidade de interfaces, GB/dia e capacidade de armazenamento. E não há opções de upgrade.
Na sequência observa-se as opções do mesmo produto em formato de MÁQUINA VIRTUAL (VM), com opção de upgrade para quantidade de GB/dia e capacidade de armazenamento. E também existem subscrição de funcionalidades que são opcionais.
Como pode ser observado na página 3 da nossa proposta comercial, ofertamos o produto FAZ-800F. É possível observar no referido documento que não existe opção de licenciamento, indicando que já está incluído no mesmo. Também é possível observar no referido documento que não existe opção de subscription, indicando que o licenciamento é perpétuo, e já inclui todas as funcionalidades para atender todas as funcionalidades mencionadas no termo de referência. As funcionalidades opcionais que existem no documento (backup em cloud, indicadores de comprometimento e SOC) não foram contempladas na proposta, por não serem mencionadas no termo de referência.

Atenciosamente.

JOSE ALVES MUNIZ JUNIOR:34922733434

Digitally signed by JOSE ALVES MUNIZ JUNIOR:34922733434
DN: C=BR, O=ICP-Brasil, OU=Secretaria da Receita Federal do Brasil - RFB, OU=RFB e-CPF A3, OU=(EM BRANCO), OU=Autenticado por AR RG Tecnologia, CN=JOSE ALVES MUNIZ JUNIOR:34922733434
Reason: Assinado de forma digital por
Location: Recife-PE
Date: 2020-11-27 13:19:38

José Alves Muniz Junior - Diretor – NEWSUPRI
Fones: (81) 3366-8500 e-mail: junior@newsupri.com.br

Documento 78 página 2 assinado, do processo nº 2020012776, nos termos da Lei 11.419. ADME.19484.46061.78169.01285-0
Nelson de Espindola Vasconcelos [033.228.264-30] em 27/11/2020 13:56