



**SECRETARIA DE ESTADO DA EDUCAÇÃO DO GOIÁS
CADERNO DE TESTES
EQUIPAMENTOS DE SEGURANÇA NGFW APPLIANCE - LOTE 1
HOMOLOGAÇÃO DO PREGÃO ELETRÔNICO 01/2023**

SETOR BANCÁRIO SUL - QUADRA 2 - EDIFÍCIO JOÃO CARLOS SAAD - 8º ANDAR - CEP 70.070-120 - ASA SUL-
BRASÍLIA/DF

www.nct.com.br



1. OBJETIVO DO CADERNO DE TESTE

O caderno de teste tem como objetivo destacar os itens que serão objeto de teste de conformidade, conforme declarado no item 13.7. “O Teste de Conformidade será feito com base no CADERNO DE TESTES aprovado pelo grupo técnico de apoio ao pregoeiro. Nesse caderno deverão ser incluídos, pelo menos, os testes descritos e ordem especificada.”

O presente documento terá por base o Anexo VIII conforme subitem “7.8. O CADERNO DE TESTES deve no mínimo, os itens descritos no ANEXO VIII – ITENS OBRIGATÓRIOS PARA O TESTE DE CONFORMIDADE” do Item “7. AMOSTRAS E COMPROVAÇÃO DA ESPECIFICAÇÃO” do referido edital.

2. HISTÓRICO DE REVISÕES

Versão	Modificado por	Data	Descrição das Alterações
1.0	Hélio Batista	09/03/2023	Criação do documento
1.0	Victor Nakagomi	09/03/2023	Alterações
1.0	Flávio Barbosa	11/03/2023	Alterações
2.0	Tiago Marques	12/04/2023	Revisão e alterações
2.0	Armando Costa	16/06/2023	Revisão
2.0	Tiago Marques	19/06/2023	Revisão e alterações
3.0	Crystine Rodrigues	22/06/2023	Revisão
4.0	Armando Costa	23/06/2023	Revisão e alterações
4.0	Crystine Rodrigues	23/06/2023	Revisão
5.0	Armando Costa	23/06/2023	Revisão e alterações

3. LOCAL DE REALIZAÇÃO DOS TESTES

Os testes de conformidade conforme certame, serão realizados de forma remota no laboratório da Fortinet, por meio de aplicativo Teams, com link a ser disponibilizado conforme data e horário solicitado.

4. EQUIPE TÉCNICA PARA PARTICIPAÇÃO DOS TESTES

Érico Veríssimo Hortolan - ehortolan@fortinet.com

Bruno Noronha - bnoronha@fortinet.com

Tiago Marques - tmarques@fortinet.com

Armando Costa - armando@nct.com.br

Rodrigo Andrade - rodrigo.andrade@nct.com

5. TABELA DA SOLUÇÃO

Equipamentos, licenciamento e insumos, conforme edital.

Quantidade	Modelo Equipamento	Descrição
1	FortiGate-1801F	Firewall tipo 1
1	Licenciamento UTP para FortiGate-1801F	Firewall tipo 1 - Licenciamento

SETOR BANCÁRIO SUL - QUADRA 2 - EDIFÍCIO JOÃO CARLOS SAAD - 8º ANDAR - CEP 70.070-120 - ASA SUL - BRASÍLIA/DF

www.nct.com.br

1	Licenciamento VPN para FortiGate-1801F	Firewall tipo 1 - Licenciamento
1	FortiGate-81F	Firewall tipo 2
1	SP-FG60E-PDC	Firewall tipo 2 - Fonte
1	Licenciamento UTP para FortiGate-81F	Firewall tipo 2 - Licenciamento
1	FortiAnalyzer VM	Solução de Gerenciamento e Controle -Concentrador de Logs
1	FortiManager VM	Solução de Gerenciamento e Controle - Gerência Centralizada

6. VERSÃO DOS SOFTWARES

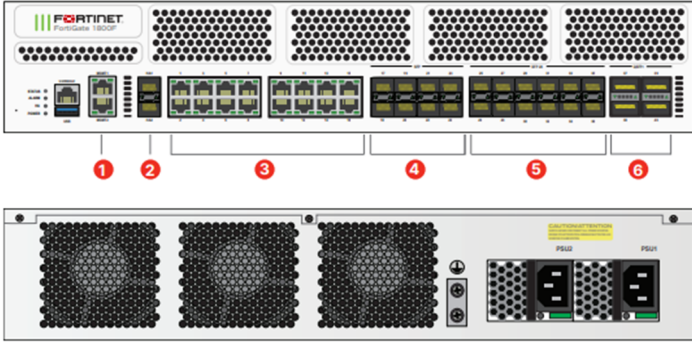

Os testes serão realizados na versão 7.2 do sistema operacional FortiOS.

A escolha foi realizada em razão de se tratar de última versão mais estável, sendo a recomendada pelo fabricante. Além de ter sido a mais recente utilizada durante o processo de elaboração de planilha ponto a ponto no presente processo.

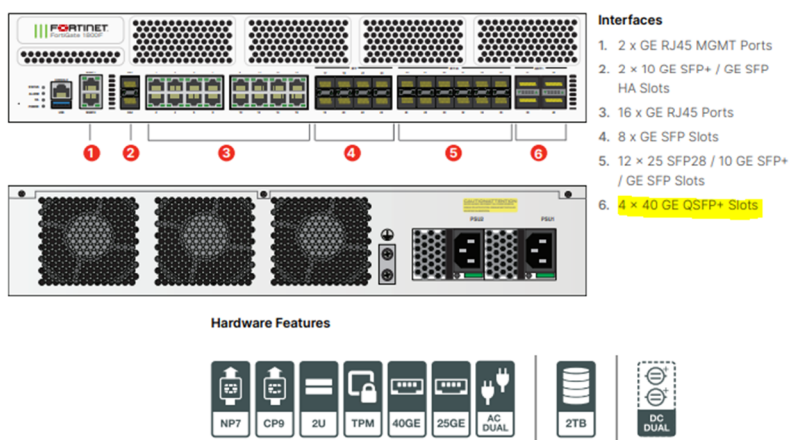
7. ITENS OBRIGATÓRIOS PARA TESTE DE CONFORMIDADE

5.1 Cluster de Firewall Tipo 1

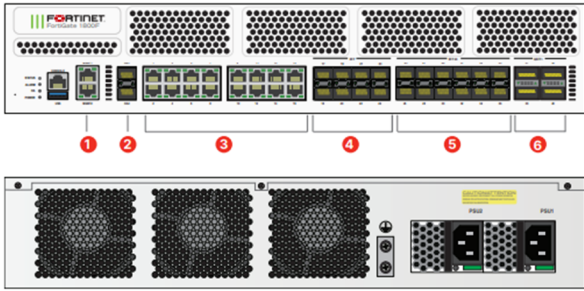

5.1.4 INTERFACES

Item 5.1.4.1	Possuir no mínimo 08 (oito) interfaces 10 Gigabit SFP+
Objetivo do Teste	Verificar se o appliance possui 08 interfaces de 10 Gigabit SFP+
Configuração do Teste	Validar que o equipamento possui 08 interfaces de 10 Gigabit SFP+
Procedimento do Teste	Visual e comprovação por datasheet
Evidências	<p>Hardware</p> <p>FortiGate 1800F Series</p>  <p>Interfaces</p> <ol style="list-style-type: none"> 2 x GE RJ45 MGMT Ports 2 x 10 GE SFP+ / GE SFP HA Slots 16 x GE RJ45 Ports 8 x GE SFP Slots 12 x 25 SFP28 / 10 GE SFP+ / GE SFP Slots 4 x 40 GE QSFP+ Slots <p>Hardware Features</p> 

Comentário	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate-1800f-series.pdf
------------	---

Item 5.1.4.2	Possuir no mínimo 02 (duas) interfaces 40 Gigabit QSFP+ (ou superior)
Objetivo do Teste	Validar se o appliance possui 02 (duas) interfaces de 40 Gigabit QSFP+ (ou superior)
Configuração do Teste	Validar que o equipamento possui 02 interfaces de 40 Gigabit QSFP+
Procedimento do Teste	Visual e comprovação por datasheet
Evidências	<p>Hardware</p> <p>FortiGate 1800F Series</p>  <p>Interfaces</p> <ol style="list-style-type: none"> 1. 2 x GE RJ45 MGMT Ports 2. 2 x 10 GE SFP+ / GE SFP HA Slots 3. 16 x GE RJ45 Ports 4. 8 x GE SFP Slots 5. 12 x 25 SFP28 / 10 GE SFP+ / GE SFP Slots 6. 4 x 40 GE QSFP+ Slots <p>Hardware Features</p> <ul style="list-style-type: none"> NP7 CP9 2U TPM 40GE 25GE AC DUAL 2TB DC DUAL
Comentário	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate-1800f-series.pdf

Item de Teste 5.1.4.3	Possuir no mínimo 04 (quatro) interfaces RJ45 de no mínimo 1 Gigabit
Objetivo do Teste	Validar se o appliance possui no mínimo 04 interfaces RJ45 de no mínimo 1GB
Configuração do Teste	Validar que o equipamento possui 04 interfaces RJ45 1 Gigabit
Procedimento do Teste	Visual e comprovação por datasheet

Evidências	<p>Hardware</p> <p>FortiGate 1800F Series</p>  <p>Interfaces</p> <ol style="list-style-type: none"> 1. 2 x GE RJ45 MGMT Ports 2. 2 x 10 GE SFP+ / GE SFP HA Slots 3. 16 x GE RJ45 Ports 4. 8 x GE SFP Slots 5. 12 x 25 SFP28 / 10 GE SFP+ / GE SFP Slots 6. 4 x 40 GE QSFP+ Slots <p>Hardware Features</p> 
Comentário	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate-1800f-series.pdf

5.1.5 TROUGHPUT

Item de Teste 5.1.5.1	Possuir throughput de no mínimo 9 (Nove) Gbps de tráfego real por nó do cluster com as funcionalidades de segurança habilitadas (Firewall, IPS, Logging, Controle de Aplicação, Proteção contra Malware)
Objetivo do Teste	Validar o throughput de no mínimo 9 Gbps de tráfego real com as funcionalidades de Firewall, IPS, Logging, controle de aplicação e proteção contra Malwares.
Configuração do Teste	Teste a ser realizado no laboratório Fortinet. Será apresentado o perfil de tráfego que será gerado e submetido ao appliance em teste.
Procedimento do Teste	Submeter o equipamento ao tráfego de 9 Gbps com as funcionalidades supracitadas inspecionando este tráfego.
Evidências	Coletar durante o teste imagens com o equipamento performando 9 Gbps.
Comentário	

Item de Teste 5.1.5.2	Possuir no mínimo 9,5 (Nove e cinco décimos) Gbps de throughput para VPN IPsec;
Objetivo do Teste	Validar o throughput de no mínimo 9,5 Gbps de tráfego VPN IPsec.
Configuração do Teste	Teste a ser realizado no laboratório Fortinet. Será apresentado o perfil de tráfego que será gerado e submetido ao appliance em teste.
Procedimento do Teste	Submeter o equipamento ao tráfego de 9,5 Gbps de tráfego VPN IPsec.
Evidências	Coletar durante o teste imagens com o equipamento performando 9,5 Gbps de tráfego VPN IPsec.
Comentário	

5.1.6 CONEXÕES



Item de Teste - 5.1.6.1	Permitir no mínimo 150.000 (cento e cinquenta mil) novas conexões por segundo por nó do cluster;
Objetivo do Teste	Validar a capacidade mínima de 150.000 novas conexões por segundo por nó do cluster
Configuração do Teste	Teste a ser realizado no laboratório Fortinet. Será apresentado o perfil de tráfego que será gerado e submetido ao appliance em teste.
Procedimento do Teste	Submeter o equipamento as 150 mil novas conexões por segundo.
Evidências	Coletar durante o teste imagens com o equipamento performando as 150 mil novas conexões por segundo.
Comentário	

Item de Teste - 5.1.6.2	Permitir no mínimo 4.000.000 (quatro milhões) conexões simultâneas por nó do cluster;
Objetivo do Teste	Validar a capacidade mínima de 4.000.000 de conexões simultâneas por nó do cluster
Configuração do Teste	Teste a ser realizado no laboratório Fortinet. Será apresentado o perfil de tráfego que será gerado e submetido ao appliance em teste.
Procedimento do Teste	Submeter o equipamento as 4 milhões de conexões por segundo
Evidências	Coletar durante o teste imagens com o equipamento performando as 4 milhões de conexões por segundo.
Comentário	

5.1.7 HARDWARE:

Item de Teste - 5.1.7.1	Possuir unidade de armazenamento interno redundante configurada em RAID-1 de no mínimo 240 GB cada, do tipo memória Flash ou SSD;
Objetivo do Teste	Verificar se o appliance possui armazenamento interno redundante de no mínimo 240 Gb cada em RAID-1
Configuração do Teste	Execução via linha de comando para atestar o uso da tecnologia RAID-1
Procedimento do Teste	Executar comando via cli: <code>execute disk raid status</code> Certificar a saída do comando com resultado Raid Level e Status, esperado: <code># execute disk raid status</code> <code>RAID Level: Raid-1</code> <code>RAID Status: OK</code> <code>RAID Size:</code>



<p>Evidências</p>	<h2 style="text-align: center;">Specifications</h2> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #f28b82; color: white;"> <th></th> <th style="text-align: center;">FG-1800F/-DC</th> <th style="text-align: center;">FG-1801F/-DC</th> </tr> </thead> <tbody> <tr> <td colspan="3">Interfaces and Modules</td> </tr> <tr> <td>Hardware Accelerated GE RJ45 Ports</td> <td></td> <td style="text-align: center;">16</td> </tr> <tr> <td>Hardware Accelerated GE SFP Slots</td> <td></td> <td style="text-align: center;">8</td> </tr> <tr> <td>Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots</td> <td></td> <td style="text-align: center;">12</td> </tr> <tr> <td>Hardware Accelerated 40GE QSFP+ Slots</td> <td></td> <td style="text-align: center;">4</td> </tr> <tr> <td>GE RJ45 Management Ports</td> <td></td> <td style="text-align: center;">2</td> </tr> <tr> <td>10 GE SFP+ / GE SFP HA Slots</td> <td></td> <td style="text-align: center;">2</td> </tr> <tr> <td>USB 3.0 Port</td> <td></td> <td style="text-align: center;">1</td> </tr> <tr> <td>Console RJ45 Port</td> <td></td> <td style="text-align: center;">1</td> </tr> <tr> <td style="background-color: #ffff00;">Onboard Storage</td> <td style="text-align: center;">0</td> <td style="text-align: center; background-color: #ffff00;">2× 1 TB NVMe SSD</td> </tr> <tr> <td>Trusted Platform Module (TPM)</td> <td></td> <td style="text-align: center;">Yes</td> </tr> </tbody> </table> <p>Exemplo de saída do comando:</p> <p>To check the RAID status:</p> <ul style="list-style-type: none"> RAID enabled: <pre># execute disk raid status RAID Level: Raid-1 RAID Status: OK (Background-Synchronizing) (9%) RAID Size: 239GB Disk 1: OK Used 228GB Disk 2: OK Used 228GB</pre> 		FG-1800F/-DC	FG-1801F/-DC	Interfaces and Modules			Hardware Accelerated GE RJ45 Ports		16	Hardware Accelerated GE SFP Slots		8	Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots		12	Hardware Accelerated 40GE QSFP+ Slots		4	GE RJ45 Management Ports		2	10 GE SFP+ / GE SFP HA Slots		2	USB 3.0 Port		1	Console RJ45 Port		1	Onboard Storage	0	2× 1 TB NVMe SSD	Trusted Platform Module (TPM)		Yes
	FG-1800F/-DC	FG-1801F/-DC																																			
Interfaces and Modules																																					
Hardware Accelerated GE RJ45 Ports		16																																			
Hardware Accelerated GE SFP Slots		8																																			
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots		12																																			
Hardware Accelerated 40GE QSFP+ Slots		4																																			
GE RJ45 Management Ports		2																																			
10 GE SFP+ / GE SFP HA Slots		2																																			
USB 3.0 Port		1																																			
Console RJ45 Port		1																																			
Onboard Storage	0	2× 1 TB NVMe SSD																																			
Trusted Platform Module (TPM)		Yes																																			
<p>Comentário</p>	<p>https://docs.fortinet.com/document/FortiGate/6.2.13/cookbook/443180/raid</p>																																				

<p>Item de Teste - 5.1.7.8</p>	<p>Possuir alimentação elétrica a partir de no mínimo 2 (duas) fontes independentes, redundantes e hot-swappable, capazes de operar entre 110-240VAC, 60 Hz, por reconhecimento automático do nível de tensão;</p>
<p>Objetivo do Teste</p>	<p>Demonstrar redundância de fontes de energia</p>
<p>Configuração do Teste</p>	<p>Teste físico</p>
<p>Procedimento do Teste</p>	<p>Demonstrar ambas as fontes alimentadas e em operação.</p> <p>Desligar uma das fontes e demonstrar o status das mesmas evidenciando que uma fonte deixou de funcionar enquanto a outra continuou alimentando plenamente o equipamento.</p>
<p>Evidências</p>	



		Specifications																																																																																																																																																	
		<table border="1"> <thead> <tr> <th></th> <th>FG-1800F/-DC</th> <th>FG-1801F/-DC</th> </tr> </thead> <tbody> <tr> <td colspan="3">Interfaces and Modules</td> </tr> <tr> <td>Hardware Accelerated GE RJ45 Ports</td> <td>16</td> <td></td> </tr> <tr> <td>Hardware Accelerated GE SFP Slots</td> <td>8</td> <td></td> </tr> <tr> <td>Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots</td> <td>12</td> <td></td> </tr> <tr> <td>Hardware Accelerated 40GE QSFP+ Slots</td> <td>4</td> <td></td> </tr> <tr> <td>GE RJ45 Management Ports</td> <td>2</td> <td></td> </tr> <tr> <td>10 GE SFP+ / GE SFP HA Slots</td> <td>2</td> <td></td> </tr> <tr> <td>USB 3.0 Port</td> <td>1</td> <td></td> </tr> <tr> <td>Console RJ45 Port</td> <td>1</td> <td></td> </tr> <tr> <td>Onboard Storage</td> <td>0</td> <td>2x 1 TB NVMe SSD</td> </tr> <tr> <td>Trusted Platform Module (TPM)</td> <td></td> <td>Yes</td> </tr> <tr> <td>Included Transceivers</td> <td></td> <td>2x SFP+ (SR 10 GE)</td> </tr> <tr> <td colspan="3">System Performance — Enterprise Traffic Mix</td> </tr> <tr> <td>IPS Throughput *</td> <td></td> <td>22 Gbps</td> </tr> <tr> <td>NGFW Throughput **</td> <td></td> <td>17 Gbps</td> </tr> <tr> <td>Threat Protection Throughput **</td> <td></td> <td>15 Gbps</td> </tr> <tr> <td colspan="3">System Performance and Capacity</td> </tr> <tr> <td>IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)</td> <td></td> <td>198 / 197 / 140 Gbps</td> </tr> <tr> <td>IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)</td> <td></td> <td>198 / 197 / 140 Gbps</td> </tr> <tr> <td>Firewall Latency (64 byte, UDP)</td> <td></td> <td>3.22 µs</td> </tr> <tr> <td>Firewall Throughput (Packet per Second)</td> <td></td> <td>210 Mpps</td> </tr> <tr> <td>Concurrent Sessions (TCP)</td> <td></td> <td>12 Million / 40 Million*</td> </tr> <tr> <td>New Sessions/Second (TCP)</td> <td></td> <td>750 000 / 2 Million*</td> </tr> <tr> <td>Firewall Policies</td> <td></td> <td>100 000</td> </tr> </tbody> </table>		FG-1800F/-DC	FG-1801F/-DC	Interfaces and Modules			Hardware Accelerated GE RJ45 Ports	16		Hardware Accelerated GE SFP Slots	8		Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots	12		Hardware Accelerated 40GE QSFP+ Slots	4		GE RJ45 Management Ports	2		10 GE SFP+ / GE SFP HA Slots	2		USB 3.0 Port	1		Console RJ45 Port	1		Onboard Storage	0	2x 1 TB NVMe SSD	Trusted Platform Module (TPM)		Yes	Included Transceivers		2x SFP+ (SR 10 GE)	System Performance — Enterprise Traffic Mix			IPS Throughput *		22 Gbps	NGFW Throughput **		17 Gbps	Threat Protection Throughput **		15 Gbps	System Performance and Capacity			IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)		198 / 197 / 140 Gbps	IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)		198 / 197 / 140 Gbps	Firewall Latency (64 byte, UDP)		3.22 µs	Firewall Throughput (Packet per Second)		210 Mpps	Concurrent Sessions (TCP)		12 Million / 40 Million*	New Sessions/Second (TCP)		750 000 / 2 Million*	Firewall Policies		100 000	<table border="1"> <thead> <tr> <th></th> <th>FG-1800F/-DC</th> <th>FG-1801F/-DC</th> </tr> </thead> <tbody> <tr> <td colspan="3">Dimensions and Power</td> </tr> <tr> <td>Height x Width x Length (inches)</td> <td colspan="2">3.5 x 17.25 x 21.1</td> </tr> <tr> <td>Height x Width x Length (mm)</td> <td colspan="2">88.4 x 438 x 538</td> </tr> <tr> <td>Weight</td> <td>30.2 lbs (13.7 kg)</td> <td>30.4 lbs (13.8 kg)</td> </tr> <tr> <td>Form Factor (supports EIA/non-EIA standards)</td> <td colspan="2">Rack Mount, 2RU</td> </tr> <tr> <td>AC Power Supply</td> <td colspan="2">100-240VAC, 50/60 Hz</td> </tr> <tr> <td>AC Current (Maximum)</td> <td colspan="2">7A@100VAC, 3A@240VAC</td> </tr> <tr> <td>DC Power Supply</td> <td colspan="2">-48V to -60V DC</td> </tr> <tr> <td>DC Current (Maximum)</td> <td colspan="2">20A</td> </tr> <tr> <td>Power Consumption (Average / Maximum)</td> <td>410.9 W / 459.1 W</td> <td>414.9 W / 463.1 W</td> </tr> <tr> <td>Heat Dissipation</td> <td>185.84 BTU/h</td> <td>196.70 BTU/h</td> </tr> <tr> <td>Power Efficiency Rating</td> <td colspan="2">80Plus Compliant</td> </tr> <tr> <td>Redundant Power Supplies Hot Swappable</td> <td colspan="2">Yes (Default dual AC PSU for 1+1 Redundancy)</td> </tr> <tr> <td colspan="3">Operating Environment and Certifications</td> </tr> <tr> <td>Operating Temperature</td> <td colspan="2">32~104°F (0~40°C)</td> </tr> <tr> <td>Storage Temperature</td> <td colspan="2">-31~158°F (-35~70°C)</td> </tr> <tr> <td>Humidity</td> <td colspan="2">10%-90% non-condensing</td> </tr> <tr> <td>Noise Level</td> <td colspan="2">62.74 dBA</td> </tr> <tr> <td>Forced Airflow</td> <td colspan="2">Side and Front to Back</td> </tr> <tr> <td>Operating Altitude</td> <td colspan="2">Up to 7400 ft (2250 m)</td> </tr> <tr> <td>Compliance</td> <td colspan="2">FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB</td> </tr> <tr> <td>Certifications</td> <td colspan="2">USGv6/IPv6</td> </tr> </tbody> </table>		FG-1800F/-DC	FG-1801F/-DC	Dimensions and Power			Height x Width x Length (inches)	3.5 x 17.25 x 21.1		Height x Width x Length (mm)	88.4 x 438 x 538		Weight	30.2 lbs (13.7 kg)	30.4 lbs (13.8 kg)	Form Factor (supports EIA/non-EIA standards)	Rack Mount, 2RU		AC Power Supply	100-240VAC, 50/60 Hz		AC Current (Maximum)	7A@100VAC, 3A@240VAC		DC Power Supply	-48V to -60V DC		DC Current (Maximum)	20A		Power Consumption (Average / Maximum)	410.9 W / 459.1 W	414.9 W / 463.1 W	Heat Dissipation	185.84 BTU/h	196.70 BTU/h	Power Efficiency Rating	80Plus Compliant		Redundant Power Supplies Hot Swappable	Yes (Default dual AC PSU for 1+1 Redundancy)		Operating Environment and Certifications			Operating Temperature	32~104°F (0~40°C)		Storage Temperature	-31~158°F (-35~70°C)		Humidity	10%-90% non-condensing		Noise Level	62.74 dBA		Forced Airflow	Side and Front to Back		Operating Altitude	Up to 7400 ft (2250 m)		Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB		Certifications	USGv6/IPv6	
	FG-1800F/-DC	FG-1801F/-DC																																																																																																																																																	
Interfaces and Modules																																																																																																																																																			
Hardware Accelerated GE RJ45 Ports	16																																																																																																																																																		
Hardware Accelerated GE SFP Slots	8																																																																																																																																																		
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots	12																																																																																																																																																		
Hardware Accelerated 40GE QSFP+ Slots	4																																																																																																																																																		
GE RJ45 Management Ports	2																																																																																																																																																		
10 GE SFP+ / GE SFP HA Slots	2																																																																																																																																																		
USB 3.0 Port	1																																																																																																																																																		
Console RJ45 Port	1																																																																																																																																																		
Onboard Storage	0	2x 1 TB NVMe SSD																																																																																																																																																	
Trusted Platform Module (TPM)		Yes																																																																																																																																																	
Included Transceivers		2x SFP+ (SR 10 GE)																																																																																																																																																	
System Performance — Enterprise Traffic Mix																																																																																																																																																			
IPS Throughput *		22 Gbps																																																																																																																																																	
NGFW Throughput **		17 Gbps																																																																																																																																																	
Threat Protection Throughput **		15 Gbps																																																																																																																																																	
System Performance and Capacity																																																																																																																																																			
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)		198 / 197 / 140 Gbps																																																																																																																																																	
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)		198 / 197 / 140 Gbps																																																																																																																																																	
Firewall Latency (64 byte, UDP)		3.22 µs																																																																																																																																																	
Firewall Throughput (Packet per Second)		210 Mpps																																																																																																																																																	
Concurrent Sessions (TCP)		12 Million / 40 Million*																																																																																																																																																	
New Sessions/Second (TCP)		750 000 / 2 Million*																																																																																																																																																	
Firewall Policies		100 000																																																																																																																																																	
	FG-1800F/-DC	FG-1801F/-DC																																																																																																																																																	
Dimensions and Power																																																																																																																																																			
Height x Width x Length (inches)	3.5 x 17.25 x 21.1																																																																																																																																																		
Height x Width x Length (mm)	88.4 x 438 x 538																																																																																																																																																		
Weight	30.2 lbs (13.7 kg)	30.4 lbs (13.8 kg)																																																																																																																																																	
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 2RU																																																																																																																																																		
AC Power Supply	100-240VAC, 50/60 Hz																																																																																																																																																		
AC Current (Maximum)	7A@100VAC, 3A@240VAC																																																																																																																																																		
DC Power Supply	-48V to -60V DC																																																																																																																																																		
DC Current (Maximum)	20A																																																																																																																																																		
Power Consumption (Average / Maximum)	410.9 W / 459.1 W	414.9 W / 463.1 W																																																																																																																																																	
Heat Dissipation	185.84 BTU/h	196.70 BTU/h																																																																																																																																																	
Power Efficiency Rating	80Plus Compliant																																																																																																																																																		
Redundant Power Supplies Hot Swappable	Yes (Default dual AC PSU for 1+1 Redundancy)																																																																																																																																																		
Operating Environment and Certifications																																																																																																																																																			
Operating Temperature	32~104°F (0~40°C)																																																																																																																																																		
Storage Temperature	-31~158°F (-35~70°C)																																																																																																																																																		
Humidity	10%-90% non-condensing																																																																																																																																																		
Noise Level	62.74 dBA																																																																																																																																																		
Forced Airflow	Side and Front to Back																																																																																																																																																		
Operating Altitude	Up to 7400 ft (2250 m)																																																																																																																																																		
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB																																																																																																																																																		
Certifications	USGv6/IPv6																																																																																																																																																		
Comentário	FortiGate https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate-1800f-series.pdf																																																																																																																																																		

5.1.8 ALTA DISPONIBILIDADE E BALANCEAMENTO DE CARGA:

Item de Teste - 5.1.8.4	Deve realizar monitoramento de falha de link;
Objetivo do Teste	Validar se o FortiGate realiza monitoramento de falha de link
Configuração do Teste	Acesso a Gui do equipamento.
Procedimento do Teste	Navegando por Network > SD WAN é possível adicionar links para o SDWAN realizar o balanceamento de carga e o monitoramento dos links. A escolha e convergência de links é feita a partir de fatores como: perda de pacote, latência, jitter, falha do link.
Evidências	<p>The screenshot shows the FortiGate SD-WAN configuration page. The 'Interface selection strategy' is set to 'Manual'. Under 'Outgoing interfaces', two members are listed: 'Internet_CLARO (wan2)' and 'Internet_VIVO (wan1)'. The 'Manual' strategy description states: 'Manually assign outgoing members. The member with the best measured performance is selected.' The 'Quality criteria' is set to 'Latency'. The 'Forward DSCP' and 'Reverse DSCP' are both set to 'On'.</p>



<p>Comentário</p>	
--------------------------	--

5.2 Solução de Segurança Tipo 2

5.2.2 INTERFACES

<p>Item de Teste - 5.2.2.1</p>	<p>Possuir no mínimo 08 (oito) interfaces Gigabit RJ45;</p>																																																																																																																																																																																																
<p>Objetivo do Teste</p>	<p>Validar se o equipamento possui no mínimo 8 interfaces Gigabit RJ45</p>																																																																																																																																																																																																
<p>Configuração do Teste</p>	<p>Inspeção visual</p>																																																																																																																																																																																																
<p>Procedimento do Teste</p>	<p>Comprovação visual e por meio do datasheet</p>																																																																																																																																																																																																
<p>Evidências</p>	<p>Specifications</p> <table border="1"> <thead> <tr> <th></th> <th>FO-80F</th> <th>FO-81F</th> <th>FO-80F-BYPASS</th> <th>FO-80F-POE</th> <th>FO-81F-POE</th> </tr> </thead> <tbody> <tr> <td colspan="6">Interfaces and Modules</td> </tr> <tr> <td>GE RJ45/GFP Shared Media Pairs</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> </tr> <tr> <td>GE RJ45 Internal Ports</td> <td>6</td> <td>6</td> <td>6</td> <td>—</td> <td>—</td> </tr> <tr> <td>GE RJ45 FortiLink Ports (Default)</td> <td>2</td> <td>2</td> <td>2</td> <td>—</td> <td>—</td> </tr> <tr> <td>GE RJ45 PoE/+ Ports</td> <td>—</td> <td>—</td> <td>—</td> <td>6</td> <td>6</td> </tr> <tr> <td>GE RJ45 PoE/+ FortiLink Ports (Default)</td> <td>—</td> <td>—</td> <td>—</td> <td>2</td> <td>2</td> </tr> <tr> <td>Bypass GE RJ45 Port Pair (WAN1 & Port1, default configuration)</td> <td>—</td> <td>—</td> <td>Yes</td> <td>—</td> <td>—</td> </tr> <tr> <td>Wireless Interface</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> </tr> <tr> <td>USB Ports 3.0</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> </tr> <tr> <td>Console (RJ45)</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> </tr> <tr> <td>Internal Storage</td> <td colspan="3">1x 128 GB SSD</td> <td colspan="2">1x 128 GB SSD</td> </tr> <tr> <td>Trusted Platform Module (TPM)</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> </tr> <tr> <td>Bluetooth Low Energy (BLE)</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> </tr> <tr> <td colspan="6">System Performance — Enterprise Traffic Mix</td> </tr> <tr> <td>IPS Throughput ²</td> <td colspan="3">1.4 Gbps</td> <td colspan="2"></td> </tr> <tr> <td>NGFW Throughput ^{1,4}</td> <td colspan="3">1 Gbps</td> <td colspan="2"></td> </tr> <tr> <td>Threat Protection Throughput ^{1,4}</td> <td colspan="3">900 Mbps</td> <td colspan="2"></td> </tr> <tr> <td colspan="6">System Performance and Capacity</td> </tr> <tr> <td>IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)</td> <td colspan="3">10 / 10 / 7 Gbps</td> <td colspan="2"></td> </tr> <tr> <td>Firewall Latency (64 byte, UDP)</td> <td colspan="3">3.23 µs</td> <td colspan="2"></td> </tr> <tr> <td>Firewall Throughput (Packet per Second)</td> <td colspan="3">10.5 Mpps</td> <td colspan="2"></td> </tr> <tr> <td>Concurrent Sessions (TCP)</td> <td colspan="3">1.5 Million</td> <td colspan="2"></td> </tr> <tr> <td>New Sessions/Second (TCP)</td> <td colspan="3">45 000</td> <td colspan="2"></td> </tr> <tr> <td>Firewall Policies</td> <td colspan="3">5000</td> <td colspan="2"></td> </tr> <tr> <td>IPsec VPN Throughput (512 byte)¹</td> <td colspan="3">6.5 Gbps</td> <td colspan="2"></td> </tr> <tr> <td>Gateway-to-Gateway IPsec VPN Tunnels</td> <td colspan="3">200</td> <td colspan="2"></td> </tr> <tr> <td>Client-to-Gateway IPsec VPN Tunnels</td> <td colspan="3">2500</td> <td colspan="2"></td> </tr> <tr> <td>SSL-VPN Throughput</td> <td colspan="3">950 Mbps</td> <td colspan="2"></td> </tr> <tr> <td>Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)</td> <td colspan="3">200</td> <td colspan="2"></td> </tr> <tr> <td>SSL Inspection Throughput (IPS, avg HTTPS)¹</td> <td colspan="3">715 Mbps</td> <td colspan="2"></td> </tr> <tr> <td>SSL Inspection CPS (IPS, avg HTTPS)¹</td> <td colspan="3">700</td> <td colspan="2"></td> </tr> </tbody> </table>		FO-80F	FO-81F	FO-80F-BYPASS	FO-80F-POE	FO-81F-POE	Interfaces and Modules						GE RJ45/GFP Shared Media Pairs	2	2	2	2	2	GE RJ45 Internal Ports	6	6	6	—	—	GE RJ45 FortiLink Ports (Default)	2	2	2	—	—	GE RJ45 PoE/+ Ports	—	—	—	6	6	GE RJ45 PoE/+ FortiLink Ports (Default)	—	—	—	2	2	Bypass GE RJ45 Port Pair (WAN1 & Port1, default configuration)	—	—	Yes	—	—	Wireless Interface	—	—	—	—	—	USB Ports 3.0	1	1	1	1	1	Console (RJ45)	1	1	1	1	1	Internal Storage	1x 128 GB SSD			1x 128 GB SSD		Trusted Platform Module (TPM)	Yes	Yes	Yes	Yes	Yes	Bluetooth Low Energy (BLE)	Yes	Yes	Yes	Yes	Yes	System Performance — Enterprise Traffic Mix						IPS Throughput ²	1.4 Gbps					NGFW Throughput ^{1,4}	1 Gbps					Threat Protection Throughput ^{1,4}	900 Mbps					System Performance and Capacity						IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	10 / 10 / 7 Gbps					Firewall Latency (64 byte, UDP)	3.23 µs					Firewall Throughput (Packet per Second)	10.5 Mpps					Concurrent Sessions (TCP)	1.5 Million					New Sessions/Second (TCP)	45 000					Firewall Policies	5000					IPsec VPN Throughput (512 byte) ¹	6.5 Gbps					Gateway-to-Gateway IPsec VPN Tunnels	200					Client-to-Gateway IPsec VPN Tunnels	2500					SSL-VPN Throughput	950 Mbps					Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200					SSL Inspection Throughput (IPS, avg HTTPS) ¹	715 Mbps					SSL Inspection CPS (IPS, avg HTTPS) ¹	700				
	FO-80F	FO-81F	FO-80F-BYPASS	FO-80F-POE	FO-81F-POE																																																																																																																																																																																												
Interfaces and Modules																																																																																																																																																																																																	
GE RJ45/GFP Shared Media Pairs	2	2	2	2	2																																																																																																																																																																																												
GE RJ45 Internal Ports	6	6	6	—	—																																																																																																																																																																																												
GE RJ45 FortiLink Ports (Default)	2	2	2	—	—																																																																																																																																																																																												
GE RJ45 PoE/+ Ports	—	—	—	6	6																																																																																																																																																																																												
GE RJ45 PoE/+ FortiLink Ports (Default)	—	—	—	2	2																																																																																																																																																																																												
Bypass GE RJ45 Port Pair (WAN1 & Port1, default configuration)	—	—	Yes	—	—																																																																																																																																																																																												
Wireless Interface	—	—	—	—	—																																																																																																																																																																																												
USB Ports 3.0	1	1	1	1	1																																																																																																																																																																																												
Console (RJ45)	1	1	1	1	1																																																																																																																																																																																												
Internal Storage	1x 128 GB SSD			1x 128 GB SSD																																																																																																																																																																																													
Trusted Platform Module (TPM)	Yes	Yes	Yes	Yes	Yes																																																																																																																																																																																												
Bluetooth Low Energy (BLE)	Yes	Yes	Yes	Yes	Yes																																																																																																																																																																																												
System Performance — Enterprise Traffic Mix																																																																																																																																																																																																	
IPS Throughput ²	1.4 Gbps																																																																																																																																																																																																
NGFW Throughput ^{1,4}	1 Gbps																																																																																																																																																																																																
Threat Protection Throughput ^{1,4}	900 Mbps																																																																																																																																																																																																
System Performance and Capacity																																																																																																																																																																																																	
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	10 / 10 / 7 Gbps																																																																																																																																																																																																
Firewall Latency (64 byte, UDP)	3.23 µs																																																																																																																																																																																																
Firewall Throughput (Packet per Second)	10.5 Mpps																																																																																																																																																																																																
Concurrent Sessions (TCP)	1.5 Million																																																																																																																																																																																																
New Sessions/Second (TCP)	45 000																																																																																																																																																																																																
Firewall Policies	5000																																																																																																																																																																																																
IPsec VPN Throughput (512 byte) ¹	6.5 Gbps																																																																																																																																																																																																
Gateway-to-Gateway IPsec VPN Tunnels	200																																																																																																																																																																																																
Client-to-Gateway IPsec VPN Tunnels	2500																																																																																																																																																																																																
SSL-VPN Throughput	950 Mbps																																																																																																																																																																																																
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200																																																																																																																																																																																																
SSL Inspection Throughput (IPS, avg HTTPS) ¹	715 Mbps																																																																																																																																																																																																
SSL Inspection CPS (IPS, avg HTTPS) ¹	700																																																																																																																																																																																																
<p>Comentário</p>	<p>https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate-fortiwifi-80f-series.pdf</p>																																																																																																																																																																																																

<p>Item de Teste - 5.2.2.2</p>	<p>Possuir no mínimo 01 (uma) interface console;</p>
---------------------------------------	--



Objetivo do Teste	Validar se o equipamento FortiGate 81F possui pelo menos 1 interface console																																																																																																																																																																																																
Configuração do Teste	Validar que o equipamento possui 01 interfaces de console																																																																																																																																																																																																
Procedimento do Teste	Comprovação visual e por meio do datasheet																																																																																																																																																																																																
Evidências	<p>Specifications</p> <table border="1"> <thead> <tr> <th></th> <th>FG-80F</th> <th>FG-81F</th> <th>FG-80F-BYPASS</th> <th>FG-80F-POE</th> <th>FG-81F-POE</th> </tr> </thead> <tbody> <tr> <td colspan="6">Interfaces and Modules</td> </tr> <tr> <td>GE RJ45/SFP Shared Media Pairs</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> </tr> <tr> <td>GE RJ45 Internal Ports</td> <td>6</td> <td>6</td> <td>6</td> <td>—</td> <td>—</td> </tr> <tr> <td>GE RJ45 FortiLink Ports (Default)</td> <td>2</td> <td>2</td> <td>2</td> <td>—</td> <td>—</td> </tr> <tr> <td>GE RJ45 PoE/+ Ports</td> <td>—</td> <td>—</td> <td>—</td> <td>6</td> <td>6</td> </tr> <tr> <td>GE RJ45 PoE/+ FortiLink Ports (Default)</td> <td>—</td> <td>—</td> <td>—</td> <td>2</td> <td>2</td> </tr> <tr> <td>Bypass GE RJ45 Port Pair (WAN1 & Port1, default configuration)</td> <td>—</td> <td>—</td> <td>Yes</td> <td>—</td> <td>—</td> </tr> <tr> <td>Wireless Interface</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> </tr> <tr> <td>USB Ports 3.0</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> </tr> <tr> <td>Console (RJ45)</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> </tr> <tr> <td>Internal Storage</td> <td>—</td> <td>1x 128 GB SSD</td> <td>—</td> <td>—</td> <td>1x 128 GB SSD</td> </tr> <tr> <td>Trusted Platform Module (TPM)</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> </tr> <tr> <td>Bluetooth Low Energy (BLE)</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> </tr> <tr> <td colspan="6">System Performance — Enterprise Traffic Mix</td> </tr> <tr> <td>IPS Throughput *</td> <td colspan="2"></td> <td>1.4 Gbps</td> <td colspan="2"></td> </tr> <tr> <td>NGFW Throughput **</td> <td colspan="2"></td> <td>1 Gbps</td> <td colspan="2"></td> </tr> <tr> <td>Threat Protection Throughput **</td> <td colspan="2"></td> <td>900 Mbps</td> <td colspan="2"></td> </tr> <tr> <td colspan="6">System Performance and Capacity</td> </tr> <tr> <td>IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)</td> <td colspan="2"></td> <td>10 / 10 / 7 Gbps</td> <td colspan="2"></td> </tr> <tr> <td>Firewall Latency (64 byte, UDP)</td> <td colspan="2"></td> <td>3.23 µs</td> <td colspan="2"></td> </tr> <tr> <td>Firewall Throughput (Packet per Second)</td> <td colspan="2"></td> <td>10.5 Mpps</td> <td colspan="2"></td> </tr> <tr> <td>Concurrent Sessions (TCP)</td> <td colspan="2"></td> <td>1.5 Million</td> <td colspan="2"></td> </tr> <tr> <td>New Sessions/Second (TCP)</td> <td colspan="2"></td> <td>45 000</td> <td colspan="2"></td> </tr> <tr> <td>Firewall Policies</td> <td colspan="2"></td> <td>5000</td> <td colspan="2"></td> </tr> <tr> <td>IPsec VPN Throughput (512 byte)</td> <td colspan="2"></td> <td>6.5 Gbps</td> <td colspan="2"></td> </tr> <tr> <td>Gateway-to-Gateway IPsec VPN Tunnels</td> <td colspan="2"></td> <td>200</td> <td colspan="2"></td> </tr> <tr> <td>Client-to-Gateway IPsec VPN Tunnels</td> <td colspan="2"></td> <td>2500</td> <td colspan="2"></td> </tr> <tr> <td>SSL-VPN Throughput</td> <td colspan="2"></td> <td>950 Mbps</td> <td colspan="2"></td> </tr> <tr> <td>Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)</td> <td colspan="2"></td> <td>200</td> <td colspan="2"></td> </tr> <tr> <td>SSL Inspection Throughput (IPS, avg HTTPS)</td> <td colspan="2"></td> <td>715 Mbps</td> <td colspan="2"></td> </tr> <tr> <td>SSL Inspection CPS (IPS, avg HTTPS)</td> <td colspan="2"></td> <td>700</td> <td colspan="2"></td> </tr> </tbody> </table>		FG-80F	FG-81F	FG-80F-BYPASS	FG-80F-POE	FG-81F-POE	Interfaces and Modules						GE RJ45/SFP Shared Media Pairs	2	2	2	2	2	GE RJ45 Internal Ports	6	6	6	—	—	GE RJ45 FortiLink Ports (Default)	2	2	2	—	—	GE RJ45 PoE/+ Ports	—	—	—	6	6	GE RJ45 PoE/+ FortiLink Ports (Default)	—	—	—	2	2	Bypass GE RJ45 Port Pair (WAN1 & Port1, default configuration)	—	—	Yes	—	—	Wireless Interface	—	—	—	—	—	USB Ports 3.0	1	1	1	1	1	Console (RJ45)	1	1	1	1	1	Internal Storage	—	1x 128 GB SSD	—	—	1x 128 GB SSD	Trusted Platform Module (TPM)	Yes	Yes	Yes	Yes	Yes	Bluetooth Low Energy (BLE)	Yes	Yes	Yes	Yes	Yes	System Performance — Enterprise Traffic Mix						IPS Throughput *			1.4 Gbps			NGFW Throughput **			1 Gbps			Threat Protection Throughput **			900 Mbps			System Performance and Capacity						IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)			10 / 10 / 7 Gbps			Firewall Latency (64 byte, UDP)			3.23 µs			Firewall Throughput (Packet per Second)			10.5 Mpps			Concurrent Sessions (TCP)			1.5 Million			New Sessions/Second (TCP)			45 000			Firewall Policies			5000			IPsec VPN Throughput (512 byte)			6.5 Gbps			Gateway-to-Gateway IPsec VPN Tunnels			200			Client-to-Gateway IPsec VPN Tunnels			2500			SSL-VPN Throughput			950 Mbps			Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)			200			SSL Inspection Throughput (IPS, avg HTTPS)			715 Mbps			SSL Inspection CPS (IPS, avg HTTPS)			700		
	FG-80F	FG-81F	FG-80F-BYPASS	FG-80F-POE	FG-81F-POE																																																																																																																																																																																												
Interfaces and Modules																																																																																																																																																																																																	
GE RJ45/SFP Shared Media Pairs	2	2	2	2	2																																																																																																																																																																																												
GE RJ45 Internal Ports	6	6	6	—	—																																																																																																																																																																																												
GE RJ45 FortiLink Ports (Default)	2	2	2	—	—																																																																																																																																																																																												
GE RJ45 PoE/+ Ports	—	—	—	6	6																																																																																																																																																																																												
GE RJ45 PoE/+ FortiLink Ports (Default)	—	—	—	2	2																																																																																																																																																																																												
Bypass GE RJ45 Port Pair (WAN1 & Port1, default configuration)	—	—	Yes	—	—																																																																																																																																																																																												
Wireless Interface	—	—	—	—	—																																																																																																																																																																																												
USB Ports 3.0	1	1	1	1	1																																																																																																																																																																																												
Console (RJ45)	1	1	1	1	1																																																																																																																																																																																												
Internal Storage	—	1x 128 GB SSD	—	—	1x 128 GB SSD																																																																																																																																																																																												
Trusted Platform Module (TPM)	Yes	Yes	Yes	Yes	Yes																																																																																																																																																																																												
Bluetooth Low Energy (BLE)	Yes	Yes	Yes	Yes	Yes																																																																																																																																																																																												
System Performance — Enterprise Traffic Mix																																																																																																																																																																																																	
IPS Throughput *			1.4 Gbps																																																																																																																																																																																														
NGFW Throughput **			1 Gbps																																																																																																																																																																																														
Threat Protection Throughput **			900 Mbps																																																																																																																																																																																														
System Performance and Capacity																																																																																																																																																																																																	
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)			10 / 10 / 7 Gbps																																																																																																																																																																																														
Firewall Latency (64 byte, UDP)			3.23 µs																																																																																																																																																																																														
Firewall Throughput (Packet per Second)			10.5 Mpps																																																																																																																																																																																														
Concurrent Sessions (TCP)			1.5 Million																																																																																																																																																																																														
New Sessions/Second (TCP)			45 000																																																																																																																																																																																														
Firewall Policies			5000																																																																																																																																																																																														
IPsec VPN Throughput (512 byte)			6.5 Gbps																																																																																																																																																																																														
Gateway-to-Gateway IPsec VPN Tunnels			200																																																																																																																																																																																														
Client-to-Gateway IPsec VPN Tunnels			2500																																																																																																																																																																																														
SSL-VPN Throughput			950 Mbps																																																																																																																																																																																														
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)			200																																																																																																																																																																																														
SSL Inspection Throughput (IPS, avg HTTPS)			715 Mbps																																																																																																																																																																																														
SSL Inspection CPS (IPS, avg HTTPS)			700																																																																																																																																																																																														
Comentário	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate-fortiwifi-80f-series.pdf																																																																																																																																																																																																

5.2.3 TROUGHPUT

Item de Teste - 5.2.3.1	Possuir no mínimo 900 (novecentos) Mbps de tráfego real com as funcionalidades de segurança habilitadas (Firewall, IPS, Logging, Controle de Aplicação, Proteção contra Malware);
Objetivo do Teste	Validar o throughput de no mínimo 900 Mbps de tráfego real com as funcionalidades de Firewall, IPS, Logging, controle de aplicação e proteção contra Malwares.
Configuração do Teste	Teste a ser realizado no laboratório Fortinet. Será apresentado o perfil de tráfego que será gerado e submetido ao appliance em teste.
Procedimento do Teste	Submeter o equipamento ao tráfego de 900 Mbps com as funcionalidades supra citadas inspecionando este tráfego.
Evidências	Coletar durante o teste imagens com o equipamento performando 900 Mbps.
Comentário	

Item de Teste - 5.2.3.2	Possuir no mínimo 1,5 (Um e cinco décimos) Gbps de throughput para Ipsec VPN;
Objetivo do Teste	Validar a capacidade mínima de 1,5 Gbps de throughput para Ipsec VPN
Configuração do Teste	Teste a ser realizado no laboratório Fortinet. Será apresentado o perfil de tráfego que será gerado e submetido ao appliance em teste.
Procedimento do Teste	Teste a ser realizado no laboratório da Fortinet
Evidências	Coletar durante o teste imagens com o equipamento performando 1,5 Gbps de tráfego IPsec VPN.
Comentário	



5.2.4 CONEXÕES

Item de Teste - 5.2.4.1	Permitir no mínimo 35.000 (trinta e cinco mil) novas conexões por segundo;
Objetivo do Teste	Validar a capacidade mínima de 35.000 novas conexões por segundo
Configuração do Teste	Teste a ser realizado no laboratório Fortinet. Será apresentado o perfil de tráfego que será gerado e submetido ao appliance em teste.
Procedimento do Teste	Teste a ser realizado no laboratório da Fortinet
Evidências	
Comentário	

Item de Teste - 5.2.4.2	Permitir no mínimo 200.000 (duzentas mil) conexões simultâneas;
Objetivo do Teste	Validar se o FortiGate 81F permite no mínimo 200.000 conexões simultâneas
Configuração do Teste	Teste em laboratório
Procedimento do Teste	Teste a ser realizado no laboratório da Fortinet
Evidências	Coletar durante o teste imagens com o equipamento performando 200.000 conexões simultâneas.
Comentário	

5.2.5 HARDWARE:

Item de Teste - 5.2.5.2	Possuir unidade de armazenamento interna de no mínimo 120 GB, capaz de armazenar todo o software, configuração e logs
Objetivo do Teste	Validar se a unidade de armazenamento interna tem no mínimo 120 GB e se é capaz de armazenar todo software, configurações e logs
Configuração do Teste	Comprovação por datasheet e saída de comando
Procedimento do Teste	Execução de comando <i>diagnose hardware deviceinfo disk</i> Análise de saída do comando acima
Evidências	1 - Especificações sobre o Storage interno



Specifications		
	FG-80F	FG-81F
Interfaces and Modules		
GE RJ45/SFP Shared Media Pairs	2	2
GE RJ45 Internal Ports	6	6
GE RJ45 FortiLink Ports (Default)	2	2
GE RJ45 PoE/+ Ports	—	—
GE RJ45 PoE/+ FortiLink Ports (Default)	—	—
Bypass GE RJ45 Port Pair (WAN1 & Port1, default configuration)	—	—
Wireless Interface	—	—
USB Ports 3.0	1	1
Console (RJ45)	1	1
Internal Storage		1x 128 GB SSD
Trusted Platform Module (TPM)	Yes	Yes
Bluetooth Low Energy (BLE)	Yes	Yes
System Performance — Enterprise Traffic Mix		
IPS Throughput ²		
.....		
Exemplo de saída do comando:		
<pre>firewall # diagnose hardware deviceinfo disk Disk SYSTEM(boot) 3.6GiB type: EMMC [EMMC] dev: /dev/mmcblk0 partition 247.0MiB, 148.0MiB free mounted: N label: dev: /dev/mmcblk0p1(boot) start: 0 partition 247.0MiB, 135.0MiB free mounted: Y label: dev: /dev/mmcblk0p2(boot) start: 0 partition ref: 3 2.9GiB, 2.6GiB free mounted: Y label: dev: /dev/mmcblk0p3 start: 0 Disk Internal ref: 258 119.2GiB type: SSD [ATA LITEON CV1-8B128] dev: /dev/sda partition ref: 259 117.4GiB, 116.3GiB free mounted: Y label: LOGUSEDX873B3626 dev: /dev/sda1 start: 2048 Total available disks: 2 Max SSD disks: 1 Available storage disks: 1</pre>		
Comentário		

Item de Teste - 5.2.5.3	Possuir alimentação elétrica a partir de no mínimo 2 (duas) fontes independentes e redundantes, capazes de operar entre 110-240VAC, 60 Hz;																																																																	
Objetivo do Teste	Mostrar que o equipamento possui alimentação elétrica de no mínimo 2 (duas) fontes independentes e redundantes, capazes de operar entre 110-240VAC, 60 Hz.																																																																	
Configuração do Teste	Teste físico																																																																	
Procedimento do Teste	Comprovação visual e por meio do datasheet.																																																																	
Evidências	<p style="text-align: center;">Specifications</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #f28b82; color: white;"> <th></th> <th style="text-align: center;">FG-80F-DSL</th> <th style="text-align: center;">FWF-80F-2R-3G4G-DSL</th> <th style="text-align: center;">FWF-81F-2R-3G4G-DSL</th> <th style="text-align: center;">FWF-81F-2R-3G4G-POE</th> </tr> </thead> <tbody> <tr> <td colspan="5">Dimensions and Power</td> </tr> <tr> <td>Height x Width x Length (inches)</td> <td style="text-align: center;">2.4 x 8.5 x 7.0</td> <td style="text-align: center;">2.4 x 8.5 x 7.0</td> <td style="text-align: center;">2.4 x 8.5 x 7.0</td> <td style="text-align: center;">2.4 x 8.5 x 7.0</td> </tr> <tr> <td>Height x Width x Length (mm)</td> <td style="text-align: center;">60 x 216 x 178</td> <td style="text-align: center;">60 x 216 x 178</td> <td style="text-align: center;">60 x 216 x 178</td> <td style="text-align: center;">60 x 216 x 178</td> </tr> <tr> <td>Weight</td> <td style="text-align: center;">3.07 lbs (1.39 kg)</td> <td style="text-align: center;">3.5 lbs (1.6 kg)</td> <td style="text-align: center;">3.5 lbs (1.6 kg)</td> <td style="text-align: center;">3.5 lbs (1.6 kg)</td> </tr> <tr> <td>Form Factor (supports EIA/non-EIA standards)</td> <td colspan="4" style="text-align: center;">Desktop / Wallmount (optional)</td> </tr> <tr> <td>Input Rating</td> <td style="text-align: center;">12V DC, 5A</td> <td style="text-align: center;">12V DC, 5A</td> <td style="text-align: center;">12V DC, 5A</td> <td style="text-align: center;">54V DC, 2.78A</td> </tr> <tr> <td>Power Required (Redundancy Optional)</td> <td colspan="4" style="text-align: center;">Powered by up to two external DC power adapters (one adapter included), 100-240V AC, 50/60 Hz</td> </tr> <tr> <td>Current (Maximum)</td> <td colspan="4" style="text-align: center;">115Vac/0.9A, 230Vac/0.6A</td> </tr> <tr> <td>Total Available PoE Power Budget*</td> <td colspan="3" style="text-align: center;">—</td> <td style="text-align: center;">96W</td> </tr> <tr> <td>Power Consumption (Average / Maximum)</td> <td style="text-align: center;">28.0 W / 31.6 W</td> <td style="text-align: center;">28.07 W / 34.31 W</td> <td style="text-align: center;">29.2 W / 35.6 W</td> <td style="text-align: center;">109.3 W / 133.6 W</td> </tr> <tr> <td>Heat Dissipation</td> <td style="text-align: center;">108 BTU/h</td> <td style="text-align: center;">117.0 BTU/h</td> <td style="text-align: center;">121.5 BTU/h</td> <td style="text-align: center;">455.6 BTU/h</td> </tr> <tr> <td colspan="5">Operating Environment and Certifications</td> </tr> </tbody> </table>		FG-80F-DSL	FWF-80F-2R-3G4G-DSL	FWF-81F-2R-3G4G-DSL	FWF-81F-2R-3G4G-POE	Dimensions and Power					Height x Width x Length (inches)	2.4 x 8.5 x 7.0	2.4 x 8.5 x 7.0	2.4 x 8.5 x 7.0	2.4 x 8.5 x 7.0	Height x Width x Length (mm)	60 x 216 x 178	60 x 216 x 178	60 x 216 x 178	60 x 216 x 178	Weight	3.07 lbs (1.39 kg)	3.5 lbs (1.6 kg)	3.5 lbs (1.6 kg)	3.5 lbs (1.6 kg)	Form Factor (supports EIA/non-EIA standards)	Desktop / Wallmount (optional)				Input Rating	12V DC, 5A	12V DC, 5A	12V DC, 5A	54V DC, 2.78A	Power Required (Redundancy Optional)	Powered by up to two external DC power adapters (one adapter included), 100-240V AC, 50/60 Hz				Current (Maximum)	115Vac/0.9A, 230Vac/0.6A				Total Available PoE Power Budget*	—			96W	Power Consumption (Average / Maximum)	28.0 W / 31.6 W	28.07 W / 34.31 W	29.2 W / 35.6 W	109.3 W / 133.6 W	Heat Dissipation	108 BTU/h	117.0 BTU/h	121.5 BTU/h	455.6 BTU/h	Operating Environment and Certifications				
	FG-80F-DSL	FWF-80F-2R-3G4G-DSL	FWF-81F-2R-3G4G-DSL	FWF-81F-2R-3G4G-POE																																																														
Dimensions and Power																																																																		
Height x Width x Length (inches)	2.4 x 8.5 x 7.0	2.4 x 8.5 x 7.0	2.4 x 8.5 x 7.0	2.4 x 8.5 x 7.0																																																														
Height x Width x Length (mm)	60 x 216 x 178	60 x 216 x 178	60 x 216 x 178	60 x 216 x 178																																																														
Weight	3.07 lbs (1.39 kg)	3.5 lbs (1.6 kg)	3.5 lbs (1.6 kg)	3.5 lbs (1.6 kg)																																																														
Form Factor (supports EIA/non-EIA standards)	Desktop / Wallmount (optional)																																																																	
Input Rating	12V DC, 5A	12V DC, 5A	12V DC, 5A	54V DC, 2.78A																																																														
Power Required (Redundancy Optional)	Powered by up to two external DC power adapters (one adapter included), 100-240V AC, 50/60 Hz																																																																	
Current (Maximum)	115Vac/0.9A, 230Vac/0.6A																																																																	
Total Available PoE Power Budget*	—			96W																																																														
Power Consumption (Average / Maximum)	28.0 W / 31.6 W	28.07 W / 34.31 W	29.2 W / 35.6 W	109.3 W / 133.6 W																																																														
Heat Dissipation	108 BTU/h	117.0 BTU/h	121.5 BTU/h	455.6 BTU/h																																																														
Operating Environment and Certifications																																																																		



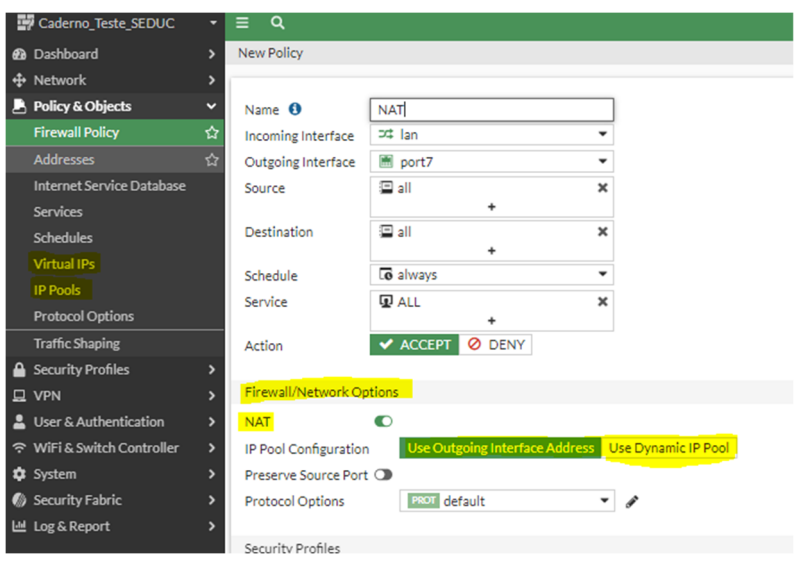
Comentário	Fonte: Acessado em https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-80f-series.pdf
-------------------	--

5.3 Funcionalidades gerais para Solução de Segurança Tipo 1, Tipo 2

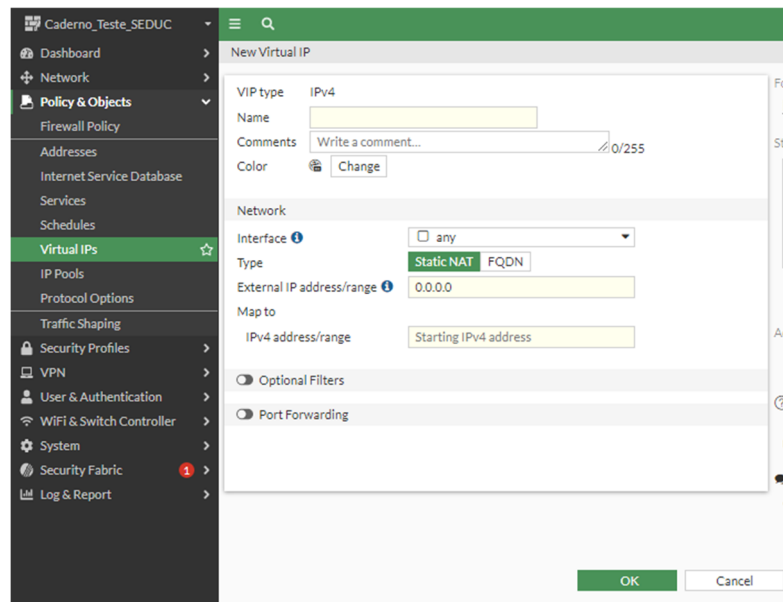
5.3.1 CARACTERISTICAS GERAIS

5.3.1.1 Deve implementar:

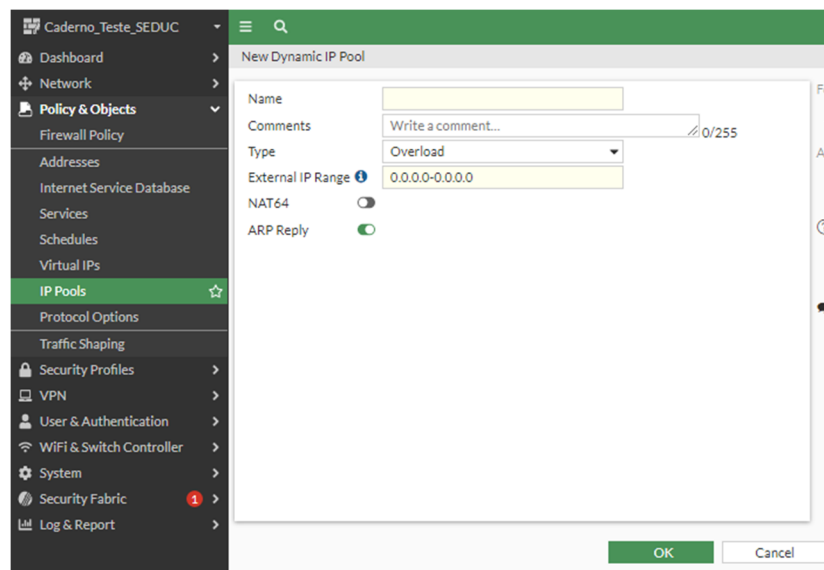
Item de Teste - 5.3.1.1.1	Firewall
Objetivo do Teste	Evidenciar que os equipamentos FortiGate1800F e FortiGate 81F são dispositivos de firewall com capacidade de filtrar pacotes e tomar decisão.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Demonstrar base de regras do FortiGate
Evidências	Na página 821 do documento utilizado na comprovação, o fabricante informa as características de filtro de pacote do produto FortiGate, e também é de conhecimento público que o FortiGate é sim um filtro de pacote denominado firewall, inclusive líder do ranking Gartner 2022 para firewall de rede.
Comentário	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a06117ca-5fbf-11ed-96f0-fa163e15d75b/FortiOS-7.2.3-Administration_Guide.pdf

Item de Teste - 5.3.1.1.2	NAT
Objetivo do Teste	Verificar se o Firewall possui a funcionalidade de NAT.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Em Policy & Objects é possível criar o NAT de destino DNAT (VIP) ou uma NAT de origem SNAT (IPPOLL), esses NATs são aplicados em Policy & Objects > Firewall Policy > Firewall Network Options .
Evidências	

2 – Virtual IPS



3 – IP Pools



Comentário

<https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/898655/static-snat>

<https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/29961/dynamic-snat>

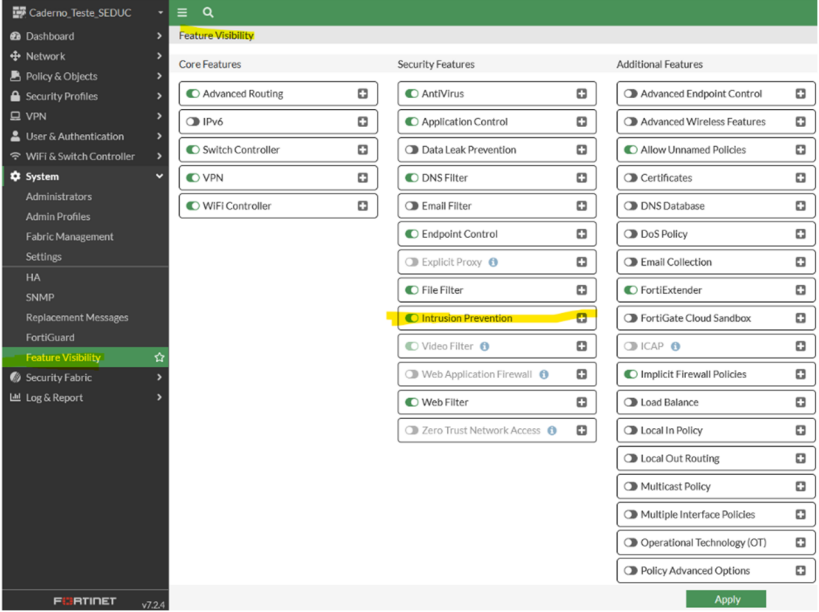
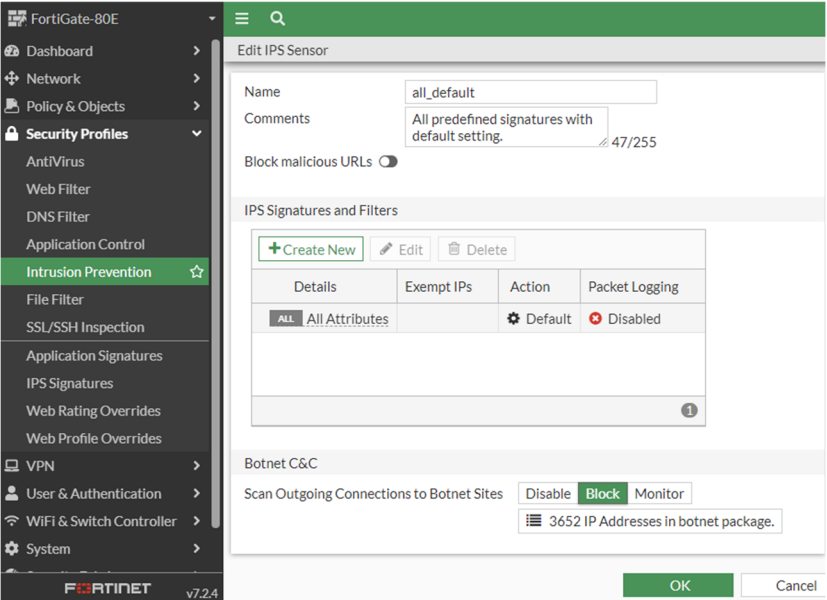
<https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/728694/destination-nat>



Item de Teste - 5.3.1.1.3	URL Filtering;
Objetivo do Teste	Demonstrar capacidade de criar filtros por URL
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Para acessar essa funcionalidade vá em Security Profile -> Web Filter .
Evidências	
Comentário	

Item de Teste - 5.3.1.1.4	Application Control;																																																							
Objetivo do Teste	Demonstrar capacidade de executar filtros por Aplicação.																																																							
Configuração do Teste	Demonstrar base de regras do FortiGate																																																							
Procedimento do Teste	Para ter acesso a essa funcionalidade, é necessário acessar o menu "Security Profile" e, em seguida, selecionar a opção "Application Control".																																																							
Evidências	<table border="1"> <thead> <tr> <th>Name</th> <th>Category</th> <th>Technology</th> <th>Popularity</th> <th>Risk</th> </tr> </thead> <tbody> <tr> <td>1koun</td> <td>Video/Audio</td> <td>Client-Server</td> <td>★★★★☆</td> <td>☆☆☆☆</td> </tr> <tr> <td>1und1.Mall</td> <td>Email</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>☆☆☆☆</td> </tr> <tr> <td>2Safe</td> <td>Storage.Backup</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>☆☆☆☆</td> </tr> <tr> <td>2Safe_File.Download</td> <td>Storage.Backup</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>☆☆☆☆</td> </tr> <tr> <td>2Safe_File.Upload</td> <td>Storage.Backup</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>☆☆☆☆</td> </tr> <tr> <td>2ch</td> <td>Social-Media</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>☆☆☆☆</td> </tr> <tr> <td>2ch_Post</td> <td>Social-Media</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>☆☆☆☆</td> </tr> <tr> <td>2shared_File.Download</td> <td>Storage.Backup</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>☆☆☆☆</td> </tr> <tr> <td>2shared_File.Upload</td> <td>Storage.Backup</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>☆☆☆☆</td> </tr> <tr> <td>3PC</td> <td>Network.Service</td> <td>Network-Protocol</td> <td>★★★★☆</td> <td>☆☆☆☆</td> </tr> </tbody> </table>	Name	Category	Technology	Popularity	Risk	1koun	Video/Audio	Client-Server	★★★★☆	☆☆☆☆	1und1.Mall	Email	Browser-Based	★★★★☆	☆☆☆☆	2Safe	Storage.Backup	Browser-Based	★★★★☆	☆☆☆☆	2Safe_File.Download	Storage.Backup	Browser-Based	★★★★☆	☆☆☆☆	2Safe_File.Upload	Storage.Backup	Browser-Based	★★★★☆	☆☆☆☆	2ch	Social-Media	Browser-Based	★★★★☆	☆☆☆☆	2ch_Post	Social-Media	Browser-Based	★★★★☆	☆☆☆☆	2shared_File.Download	Storage.Backup	Browser-Based	★★★★☆	☆☆☆☆	2shared_File.Upload	Storage.Backup	Browser-Based	★★★★☆	☆☆☆☆	3PC	Network.Service	Network-Protocol	★★★★☆	☆☆☆☆
Name	Category	Technology	Popularity	Risk																																																				
1koun	Video/Audio	Client-Server	★★★★☆	☆☆☆☆																																																				
1und1.Mall	Email	Browser-Based	★★★★☆	☆☆☆☆																																																				
2Safe	Storage.Backup	Browser-Based	★★★★☆	☆☆☆☆																																																				
2Safe_File.Download	Storage.Backup	Browser-Based	★★★★☆	☆☆☆☆																																																				
2Safe_File.Upload	Storage.Backup	Browser-Based	★★★★☆	☆☆☆☆																																																				
2ch	Social-Media	Browser-Based	★★★★☆	☆☆☆☆																																																				
2ch_Post	Social-Media	Browser-Based	★★★★☆	☆☆☆☆																																																				
2shared_File.Download	Storage.Backup	Browser-Based	★★★★☆	☆☆☆☆																																																				
2shared_File.Upload	Storage.Backup	Browser-Based	★★★★☆	☆☆☆☆																																																				
3PC	Network.Service	Network-Protocol	★★★★☆	☆☆☆☆																																																				
Comentário																																																								

Item de Teste - 5.3.1.1.5	Anti-bot;
Objetivo do Teste	Validar se a solução tem ferramenta Anti-bot de forma nativa
Configuração do Teste	Demonstrar base de regras do FortiGate

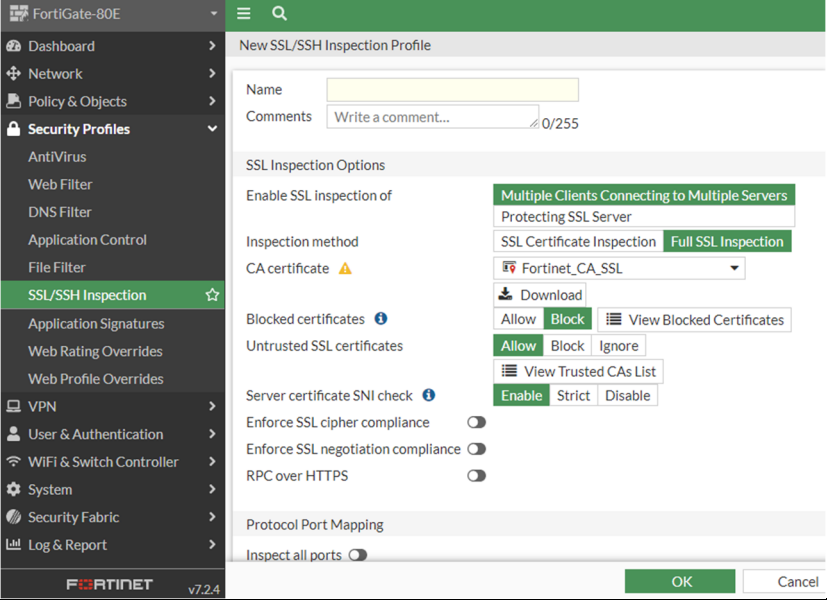
<p>Procedimento do Teste</p>	<p>Para ter acesso a esta funcionalidade, é necessário habilitar a função de Prevenção de Intrusões (IPS) por meio do menu "System" e, em seguida, acessar a opção "Feature Visibility" e habilitar a funcionalidade de IPS.</p> <p>Posteriormente, é necessário criar um sensor de IPS na seção "Security Profiles", selecionando a opção "Intrusion Prevention" e, em seguida, clicando em "Create New". Nesse sentido, é importante habilitar a função "Botnet C&C".</p>
<p>Evidências</p>	 
<p>Comentário</p>	

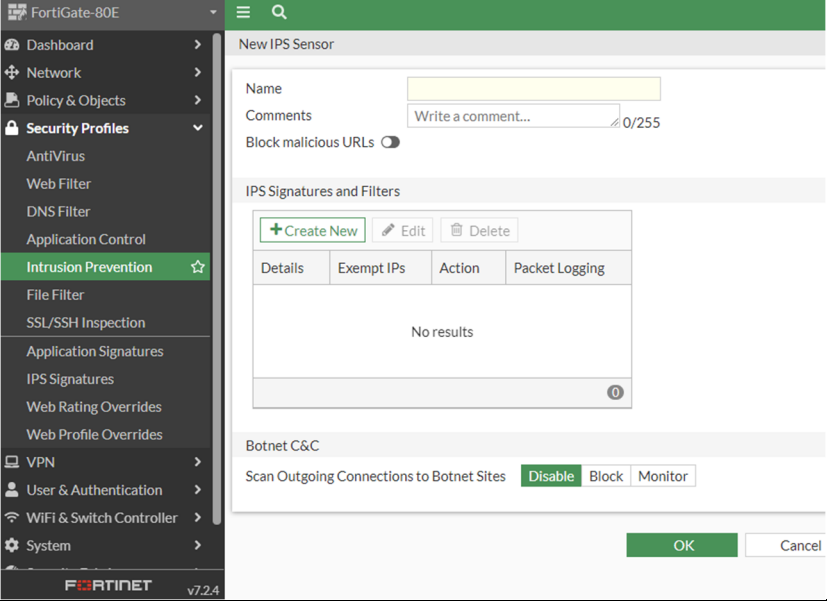


Item de Teste - 5.3.1.1.6	Anti-Virus;
Objetivo do Teste	Validar se o FortiGate possui ferramenta de Anti-vírus de forma nativa.
Configuração do Teste	Demonstrar base de regras do FortiGate.
Procedimento do Teste	Para acessar basta ir em Security Profile -> Antivírus.
Evidências	
Comentário	

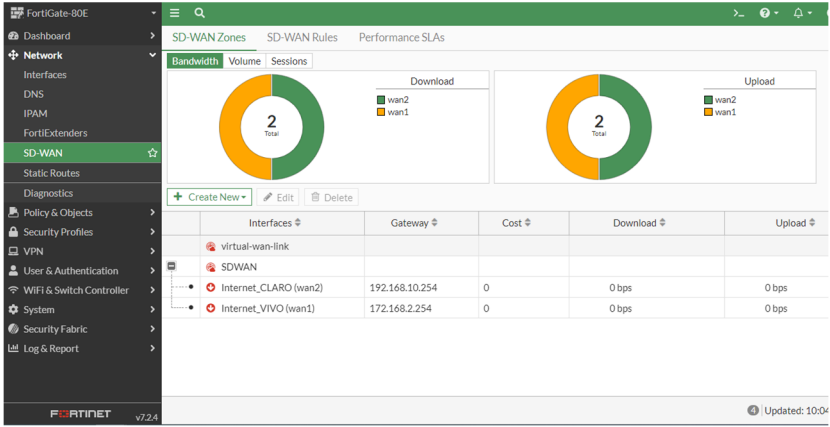
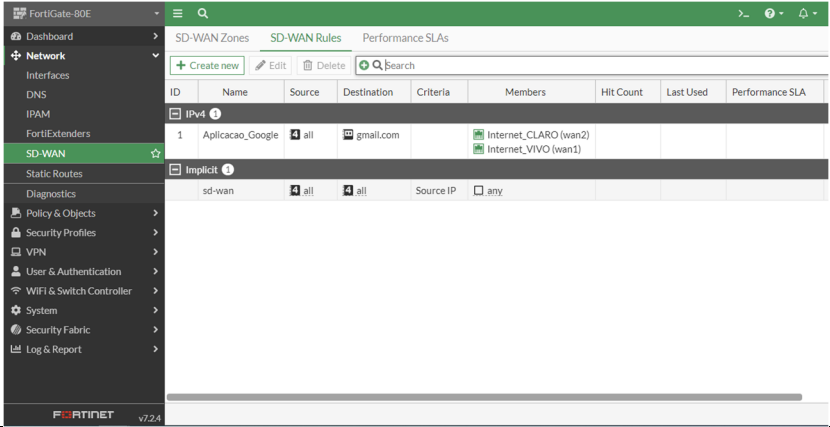
Item de Teste - 5.3.1.1.7	SSL Inspection;
Objetivo do Teste	Validar se o firewall realiza SSL Inspection de forma nativa.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Para acessar basta ir em Security Profile -> SSL/SSH Inspection.



Evidências	 <p>FortiGate-80E</p> <p>Dashboard</p> <p>Network</p> <p>Policy & Objects</p> <p>Security Profiles</p> <p>AntiVirus</p> <p>Web Filter</p> <p>DNS Filter</p> <p>Application Control</p> <p>File Filter</p> <p>SSL/SSH Inspection</p> <p>Application Signatures</p> <p>Web Rating Overrides</p> <p>Web Profile Overrides</p> <p>VPN</p> <p>User & Authentication</p> <p>WiFi & Switch Controller</p> <p>System</p> <p>Security Fabric</p> <p>Log & Report</p> <p>FortiGate-80E v7.2.4</p> <p>New SSL/SSH Inspection Profile</p> <p>Name</p> <p>Comments Write a comment... 0/255</p> <p>SSL Inspection Options</p> <p>Enable SSL inspection of Multiple Clients Connecting to Multiple Servers Protecting SSL Server</p> <p>Inspection method SSL Certificate Inspection Full SSL Inspection</p> <p>CA certificate Fortinet_CA_SSL</p> <p>Blocked certificates</p> <p>Untrusted SSL certificates</p> <p>Server certificate SNI check</p> <p>Enforce SSL cipher compliance</p> <p>Enforce SSL negotiation compliance</p> <p>RPC over HTTPS</p> <p>Protocol Port Mapping</p> <p>Inspect all ports</p> <p>OK Cancel</p>
Comentário	

Item de Teste - 5.3.1.1.8	IDS/IPS;
Objetivo do Teste	Validar se o FortiGate tem as funcionalidades de IDS/IPS de forma nativa.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Para realizar essa configuração, há a necessidade primeiro de habilitar ela, para isso vá em System -> Feature Visibility e habilite o Intrusion Prevention.
Evidências	<p>Depois Ir em Security Profiles -> Intrusion Prevention -> Create New</p>  <p>FortiGate-80E</p> <p>Dashboard</p> <p>Network</p> <p>Policy & Objects</p> <p>Security Profiles</p> <p>AntiVirus</p> <p>Web Filter</p> <p>DNS Filter</p> <p>Application Control</p> <p>Intrusion Prevention</p> <p>File Filter</p> <p>SSL/SSH Inspection</p> <p>Application Signatures</p> <p>IPS Signatures</p> <p>Web Rating Overrides</p> <p>Web Profile Overrides</p> <p>VPN</p> <p>User & Authentication</p> <p>WiFi & Switch Controller</p> <p>System</p> <p>FortiGate-80E v7.2.4</p> <p>New IPS Sensor</p> <p>Name</p> <p>Comments Write a comment... 0/255</p> <p>Block malicious URLs</p> <p>IPS Signatures and Filters</p> <p>+ Create New Edit Delete</p> <p>Details Exempt IPs Action Packet Logging</p> <p>No results</p> <p>Botnet C&C</p> <p>Scan Outgoing Connections to Botnet Sites Disable Block Monitor</p> <p>OK Cancel</p>
Comentário	



Item de Teste - 5.3.1.1.9	SDWAN;
Objetivo do Teste	Validar se o equipamento possui a funcionalidade de SDWAN.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	<p>Navegando por Network -> SDWAN -> Create new member é possível acrescentar links para serem balanceados pelo SDWAN</p> <p>Navegando por Network -> SDWAN -> Performace SLA é definindo o algoritmo mais adequado para o balanceamento;</p> <p>Navegando por Network -> SDWAN -> SDWAN Rules é possível criar regra para enquadrar o algoritmo de balanceamento.</p>
Evidências	 
Comentário	

Item de Teste - 5.3.1.1.10	VPN site-to-site;
Objetivo do Teste	Validar se a ferramenta possibilita a criação de VPN site-to-site
Configuração do Teste	Demonstrar base de regras do FortiGate.
Procedimento do Teste	Para acessar basta ir em VPN -> IPsec Tunnels -> Create New -> IPsec Tunnel .

SETOR BANCÁRIO SUL - QUADRA 2 - EDIFÍCIO JOÃO CARLOS SAAD - 8º ANDAR - CEP 70.070-120 - ASA SUL - BRASÍLIA/DF

www.nct.com.br



<p>Evidências</p>	
<p>Comentário</p>	

<p>Item de Teste - 5.3.1.4</p>	<p>Implementar interface gráfica Web segura, utilizando o protocolo HTTPS ou Console do próprio fabricante;</p>
<p>Objetivo do Teste</p>	<p>Validar se é possível realizar o acesso seguro por meio de HTTPS</p>
<p>Configuração do Teste</p>	<p>Visual e comprovação por meio de documentação.</p>
<p>Procedimento do Teste</p>	<p>Para liberar o acesso basta navegar por Network -> Interface -> Administrative Access e dentro interface selecionada liberar o acesso HTTP e HTTPS.</p>
<p>Evidências</p>	
<p>Comentário</p>	

<p>Item de Teste - 5.3.1.6</p>	<p>Implementar interface CLI segura através do protocolo SSH;</p>
<p>Objetivo do Teste</p>	<p>Verificar se o firewall é capaz de implementar interface CLI por meio do protocolo SSH porta 22 para acesso administrativo.</p>
<p>Configuração do Teste</p>	<p>Liberar acesso administrativo seguro SSH na interface que deseja fazer o acesso, após liberar o acesso é necessário utilizar alguma ferramenta que permita o acesso SSH, a utilizada no exemplo abaixo foi o PUTTY.</p>
<p>Procedimento do Teste</p>	<p>1 - Liberação do acesso administrativo SSH na interface desejada para acesso administrativo. 2- Realizar o acesso por meio de terminal Putty na função SSH.</p>



Evidências

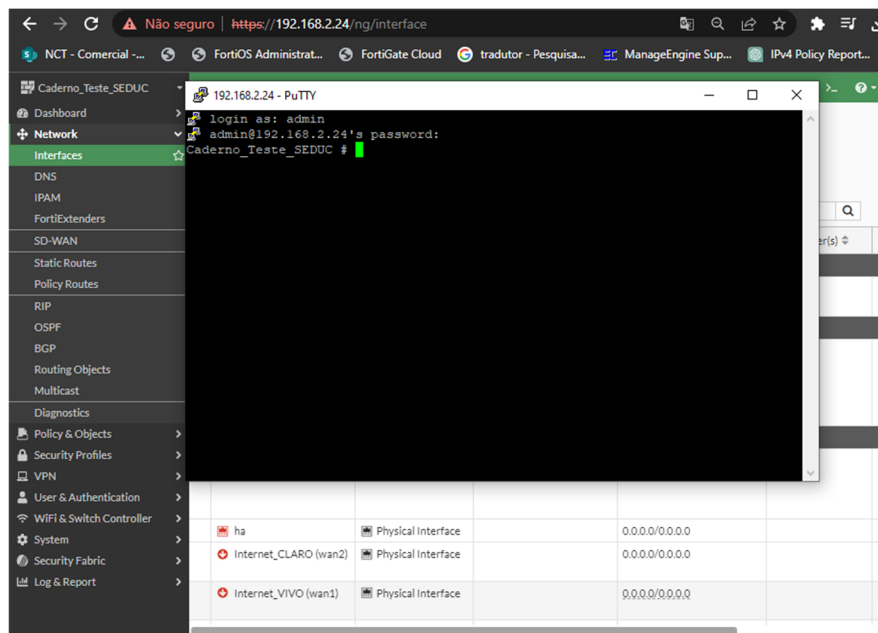
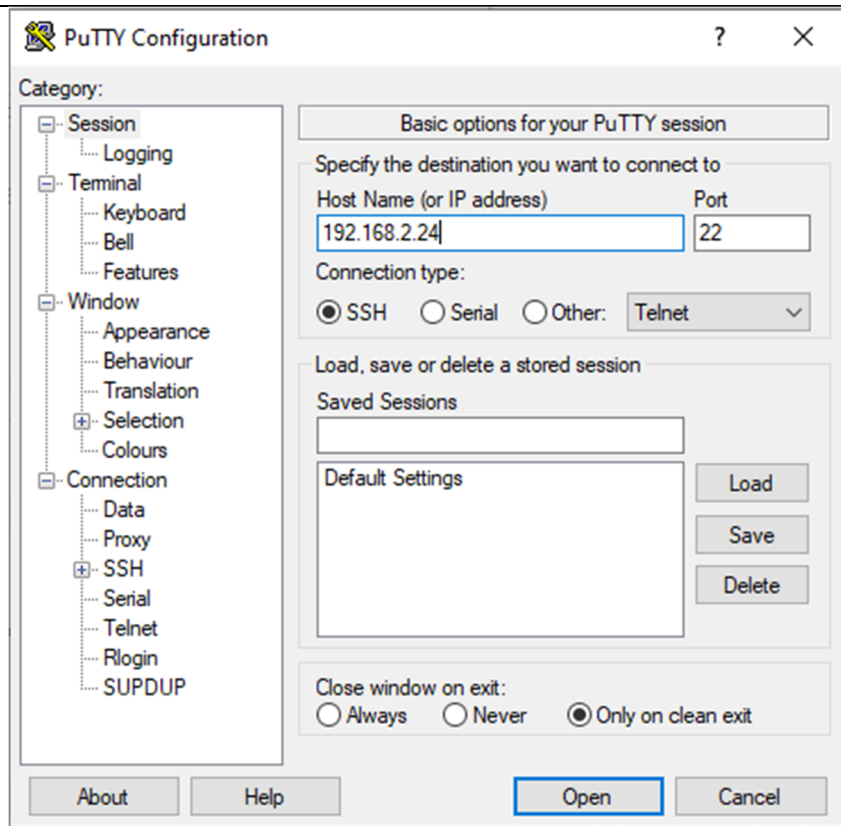
The screenshot shows the FortiGate web interface for editing the 'port7' interface. The left sidebar contains a navigation menu with categories like Network, Policy & Objects, and System. The main content area is titled 'Edit Interface' and shows the following configuration:

- Role: Undefined
- Addressing mode: Manual DHCP (selected)
- Status: Connected
- Obtained IP/Netmask: 192.168.2.24/255.255.254.0
- Expiry Date: 2023/03/20 22:45:00
- Acquired DNS: 8.8.8.8
- Default gateway: 192.168.3.254
- Retrieve default gateway from server: Disabled
- Distance: 5
- Override internal DNS: Disabled
- Administrative Access:
 - IPV4: HTTPS, SSH, PING, FMG-Access, RADIUS Accounting, SNMP, Security Fabric Connection
 - Speed Test:
- Receive LLDP: Use VDOM Setting, Enable, Disable
- Network: Device detection: Disabled
- Traffic Shaping: Outbound shapine profile: Disabled

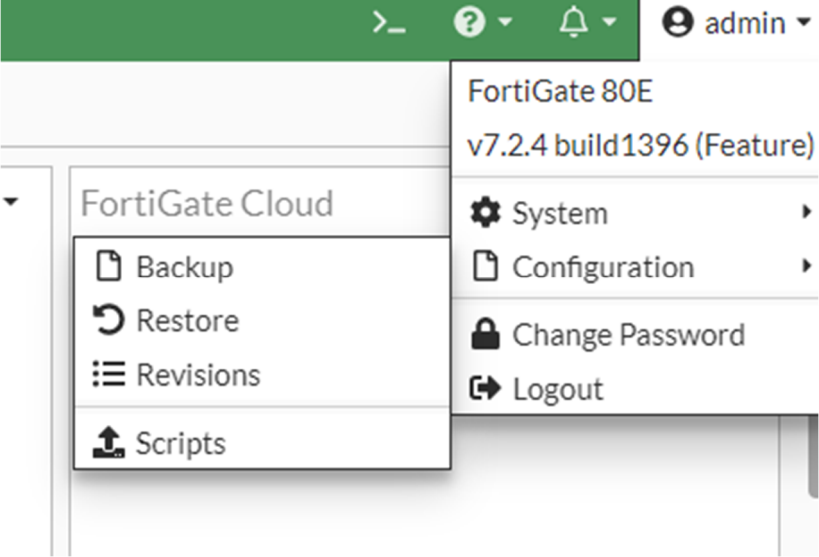
Buttons for 'OK' and 'Cancel' are visible at the bottom right of the configuration panel.

SETOR BANCÁRIO SUL - QUADRA 2 - EDIFÍCIO JOÃO CARLOS SAAD - 8º ANDAR - CEP 70.070-120 - ASA SUL-BRASÍLIA/DF

www.nct.com.br



Comentário

Item de Teste - 5.3.1.9	Deve oferecer as funcionalidades de backup/restore e deve permitir ao administrador agendar backups da configuração em determinado dia e hora;
Objetivo do Teste	Verificar se o FortiGate é capaz de realizar backup/restore e se é possível realizar de forma agendada.
Configuração do Teste	1 – Validar se o Firewall possui as funcionalidades de backup/restore 2- Validar se a ferramenta permite o agendamento de backups de forma automática.
Procedimento do Teste	Para ter acesso a funcionalidade de backup e restore, é necessário clicar no ícone correspondente ao usuário que está logado, localizado no canto superior direito da tela, e, em seguida, selecionar a opção "Configuration" e, posteriormente, acessar a seção "Backup/Restore".
Evidências	



```
FortiGate-80E (automation-trigger) # end

FortiGate-80E # config system automation-trigger

FortiGate-80E (automation-trigger) # edit backup-automatico

FortiGate-80E (backup-automatico) # set trigger-type scheduled

FortiGate-80E (backup-automatico) # set trigger-frequency daily

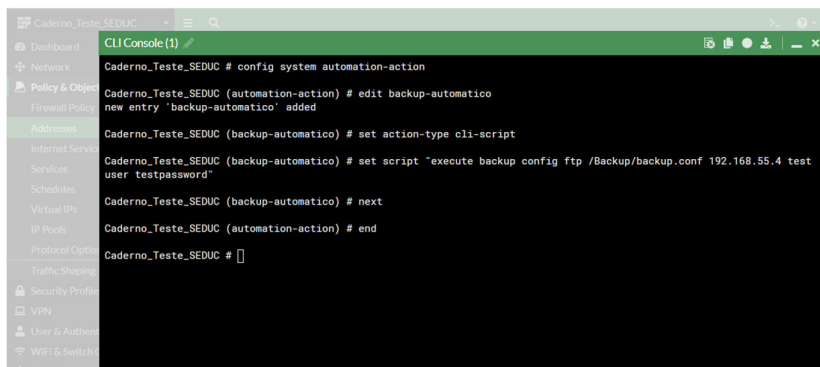
FortiGate-80E (backup-automatico) # set trigger-hour 23

FortiGate-80E (backup-automatico) # set trigger-minute 58

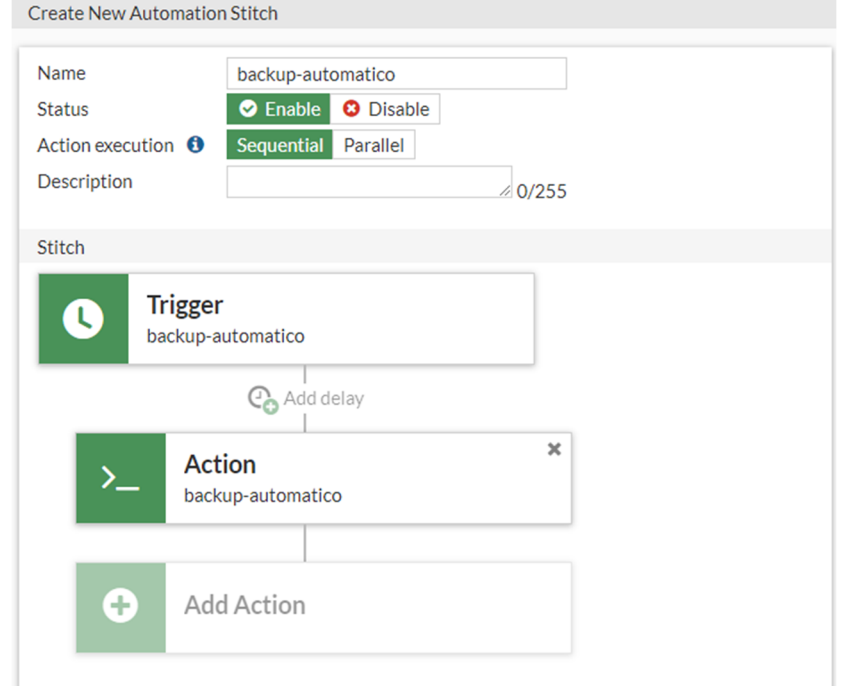
FortiGate-80E (backup-automatico) # next

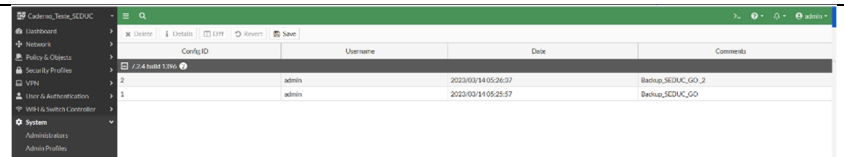
FortiGate-80E (automation-trigger) # end

FortiGate-80E #
```

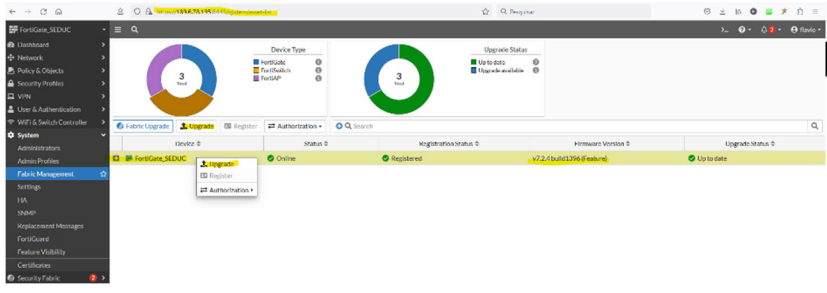


```
config system automation-stitch
edit "backup-automatico"
set trigger "backup-automatico"
config actions
edit 1
set action "backup-automatico"
set required enable
next
end
next
end
```


	
Comentário	https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-send-automated-backups-of-the-configuration/ta-p/198364

Item de Teste - 5.3.1.10	A solução de permitir armazenar os backups localmente, bem como transferi-los para um servidor remoto;
Objetivo do Teste	Demonstrar capacidade de realizar backup de configurações de forma local (no FortiGate) e de forma remota.
Configuração do Teste	Demonstrar base de regras do FortiGate.
Procedimento do Teste	<p>Para permitir backup local no FortiGate, basta clicar no nome do usuário autenticado no FortiGate, no canto superior direito, depois em Configuration -> Revisions e clicar em "Save"</p> <p>Para transferir o arquivo de backup para um servidor remoto através de FTP, basta ir até a console de comando CLI do FortiGate e digitar os seguintes parâmetros;</p> <pre># execute backup config ftp <backup_filename> <ftp_server>[<ftp_port>] [<user_name>] [<password>] [<backup_password>]</pre>
Evidências	
Comentário	Fonte: https://docs.fortinet.com/document/FortiGate/7.2.3/administration-guide/702257



Item de Teste - 5.3.1.11	Habilidade de realizar upgrade remotamente;
Objetivo do Teste	Demonstrar capacidade de realizar upgrade de firmware de forma remota.
Configuração do Teste	Demonstrar base de regras do FortiGate.
Procedimento do Teste	Acessar remotamente o equipamento, através de VPN ou de acesso diretamente na interface externa do equipamento e executar o upgrade, acesso ao equipamento demonstrado no item 5.3.1.4 e 5.3.1.6
Evidências	<p>O processo de atualização pode acontecer de diversas formas, umas delas e acessando a console do equipamento remotamente pela interface externa (IP público) através dos seguintes protocolos seguros HTTPS ou CLI com SSH, ou por meio de uma VPN executando o mesmo procedimento.</p> 
Comentário	Fonte: https://docs.fortinet.com/document/FortiGate/7.2.3/administration-guide/596131

Item de Teste - 5.3.1.14	A solução deve permitir que em caso de falha da comunicação entre o appliance de segurança e a solução de armazenamento de logs seja possível a retenção temporária dos logs localmente no appliance de segurança;
Objetivo do Teste	Verificar se a solução é capaz de armazenar logs localmente caso aconteça alguma falha de comunicação entre o FortiGate e o FortiAnalyzer.
Configuração do Teste	Demonstrar base de regras do FortiGate.
Procedimento do Teste	Para realizar esse teste é preciso habilitar a funcionalidade "Reliable" no FortiGate. Tal funcionalidade fica dentro de: <code>config log fortianalyzer setting</code>
Evidências	Tal funcionalidade habilita a função de armazenamento em cache dos logs caso aconteça a perda de comunicação com o FortiAnalyzer, assim criando uma fila de logs a serem enviados para o FAZ quando a comunicação for restabelecida.



	<pre> CLI Console (1) Caderno_Teste_SEDUC # config log fortianalyzer setting Caderno_Teste_SEDUC (setting) # set status enable Caderno_Teste_SEDUC (setting) # set reliable enable Caderno_Teste_SEDUC (setting) # </pre>
Comentário	https://docs.fortinet.com/document/FortiGate/7.2.0/new-features/942202/improve-fortianalyzer-log-caching

5.3.2 POLÍTICAS DE FIREWALL

Item de Teste - 5.3.2.18	Deve inspecionar e bloquear os dados operando como default gateway das redes protegidas e controlar o tráfego em nível de aplicações;
Objetivo do Teste	Demonstrar base de regras do FortiGate
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Demonstrar base de regras do FortiGate
Evidências	
Comentário	

Item de Teste - 5.3.2.20	A solução de Firewall, deve ser capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização;
Objetivo do Teste	Verificar se a solução de firewall é capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	<p>Dentro da solução de firewall podemos navegar em "Policy & Objects" e em seguida em "Firewall Policies". Nesta seção, é possível visualizar todas as políticas implementadas no equipamento, bem como alguns dados visuais relevantes acerca de cada política.</p> <p>Dentre esses dados, destaca-se o "Hit Count", que consiste em uma contagem de quantas vezes determinada regra foi utilizada.</p>
Evidências	

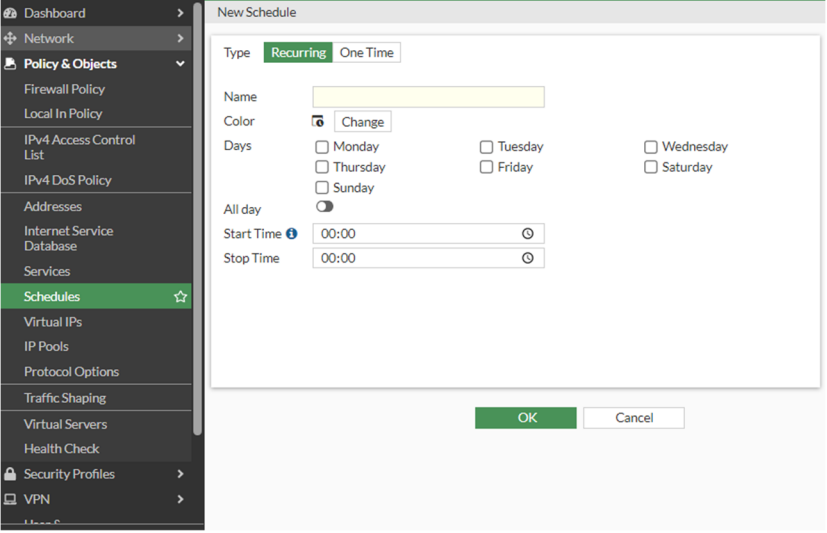


	<table border="1"> <thead> <tr> <th>Name</th> <th>Source</th> <th>Destination</th> <th>Schedule</th> <th>Hit Count</th> <th>Bytes</th> </tr> </thead> <tbody> <tr> <td>Acesso_Internet</td> <td>Rede_192.168.1.0/24</td> <td>all</td> <td>always</td> <td>199</td> <td>15.10.MB</td> </tr> <tr> <td>Acesso_Internet_Servidores</td> <td>GRP_Servidores_Seduc Rede_192.168.1.0/24</td> <td>all</td> <td>always</td> <td>0</td> <td>0 B</td> </tr> </tbody> </table>	Name	Source	Destination	Schedule	Hit Count	Bytes	Acesso_Internet	Rede_192.168.1.0/24	all	always	199	15.10.MB	Acesso_Internet_Servidores	GRP_Servidores_Seduc Rede_192.168.1.0/24	all	always	0	0 B
Name	Source	Destination	Schedule	Hit Count	Bytes														
Acesso_Internet	Rede_192.168.1.0/24	all	always	199	15.10.MB														
Acesso_Internet_Servidores	GRP_Servidores_Seduc Rede_192.168.1.0/24	all	always	0	0 B														
Comentário																			

Item de Teste - 5.3.2.21	Toda alteração de políticas e definições na console de gerenciamento deverá ser registrada e passível de auditoria;
Objetivo do Teste	Validar se a ferramenta faz o registro de todas as alterações feitas em regras e configurações, sendo passível de auditoria.
Configuração do Teste	Criar regras e demonstrar respectivo log.
Procedimento do Teste	Navegando por Log & Report > System Events > General System Events é possível realizar auditoria sobre as alterações feitas em políticas e outras configurações. Tal registro mostra qual administrador realizou as alterações e quais foram elas.

Evidências	<table border="1"> <thead> <tr> <th>Date/Time</th> <th>Level</th> <th>User</th> <th>Message</th> <th>Log Description</th> </tr> </thead> <tbody> <tr> <td>2023/03/14 09:28:12</td> <td>Info</td> <td>admin</td> <td>Edit firewall policy 1</td> <td>Object attribute configured</td> </tr> <tr> <td>2023/03/14 09:27:41</td> <td>Warn</td> <td>auto-join</td> <td>FortiCloud service activation failed</td> <td>FortiCloud activation failed</td> </tr> <tr> <td>2023/03/14 09:27:41</td> <td>Warn</td> <td>auto-join</td> <td>Attempted to join FortiCloud</td> <td>FortiCloud auto-join attempted</td> </tr> <tr> <td>2023/03/14 09:27:15</td> <td>Info</td> <td></td> <td>Performance statistics: average CPU: 3, memory: 43...</td> <td>System performance statistics</td> </tr> <tr> <td>2023/03/14 09:22:15</td> <td>Info</td> <td></td> <td>Performance statistics: average CPU: 0, memory: 43...</td> <td>System performance statistics</td> </tr> <tr> <td>2023/03/14 09:20:34</td> <td>Info</td> <td>admin</td> <td>Administrator admin logged in successfully from jsc...</td> <td>Admin login successful</td> </tr> <tr> <td>2023/03/14 09:17:40</td> <td>Warn</td> <td>auto-join</td> <td>FortiCloud service activation failed</td> <td>FortiCloud activation failed</td> </tr> <tr> <td>2023/03/14 09:17:39</td> <td>Warn</td> <td>auto-join</td> <td>Attempted to join FortiCloud</td> <td>FortiCloud auto-join attempted</td> </tr> <tr> <td>2023/03/14 09:17:23</td> <td>Info</td> <td></td> <td>Fortigate scheduled update fcnl+yes fdn+yes fsci+...</td> <td>FortiGate update succeeded</td> </tr> <tr> <td>2023/03/14 09:17:15</td> <td>Info</td> <td></td> <td>Performance statistics: average CPU: 6, memory: 43...</td> <td>System performance statistics</td> </tr> <tr> <td>2023/03/14 09:12:15</td> <td>Info</td> <td></td> <td>Performance statistics: average CPU: 0, memory: 43...</td> <td>System performance statistics</td> </tr> <tr> <td>2023/03/14 09:07:38</td> <td>Warn</td> <td>auto-join</td> <td>FortiCloud service activation failed</td> <td>FortiCloud activation failed</td> </tr> <tr> <td>2023/03/14 09:07:38</td> <td>Warn</td> <td>auto-join</td> <td>Attempted to join FortiCloud</td> <td>FortiCloud auto-join attempted</td> </tr> <tr> <td>2023/03/14 09:07:15</td> <td>Info</td> <td></td> <td>Performance statistics: average CPU: 0, memory: 43...</td> <td>System performance statistics</td> </tr> <tr> <td>2023/03/14 09:02:15</td> <td>Info</td> <td></td> <td>Performance statistics: average CPU: 0, memory: 43...</td> <td>System performance statistics</td> </tr> <tr> <td>2023/03/14 08:58:41</td> <td>Info</td> <td></td> <td>DHCP statistics</td> <td>DHCP statistics</td> </tr> <tr> <td>2023/03/14 08:58:41</td> <td>Info</td> <td></td> <td>DHCP statistics</td> <td>DHCP statistics</td> </tr> <tr> <td>2023/03/14 08:57:37</td> <td>Warn</td> <td>auto-join</td> <td>FortiCloud service activation failed</td> <td>FortiCloud activation failed</td> </tr> <tr> <td>2023/03/14 08:57:37</td> <td>Warn</td> <td>auto-join</td> <td>Attempted to join FortiCloud</td> <td>FortiCloud auto-join attempted</td> </tr> <tr> <td>2023/03/14 08:57:15</td> <td>Info</td> <td></td> <td>Performance statistics: average CPU: 0, memory: 43...</td> <td>System performance statistics</td> </tr> </tbody> </table>	Date/Time	Level	User	Message	Log Description	2023/03/14 09:28:12	Info	admin	Edit firewall policy 1	Object attribute configured	2023/03/14 09:27:41	Warn	auto-join	FortiCloud service activation failed	FortiCloud activation failed	2023/03/14 09:27:41	Warn	auto-join	Attempted to join FortiCloud	FortiCloud auto-join attempted	2023/03/14 09:27:15	Info		Performance statistics: average CPU: 3, memory: 43...	System performance statistics	2023/03/14 09:22:15	Info		Performance statistics: average CPU: 0, memory: 43...	System performance statistics	2023/03/14 09:20:34	Info	admin	Administrator admin logged in successfully from jsc...	Admin login successful	2023/03/14 09:17:40	Warn	auto-join	FortiCloud service activation failed	FortiCloud activation failed	2023/03/14 09:17:39	Warn	auto-join	Attempted to join FortiCloud	FortiCloud auto-join attempted	2023/03/14 09:17:23	Info		Fortigate scheduled update fcnl+yes fdn+yes fsci+...	FortiGate update succeeded	2023/03/14 09:17:15	Info		Performance statistics: average CPU: 6, memory: 43...	System performance statistics	2023/03/14 09:12:15	Info		Performance statistics: average CPU: 0, memory: 43...	System performance statistics	2023/03/14 09:07:38	Warn	auto-join	FortiCloud service activation failed	FortiCloud activation failed	2023/03/14 09:07:38	Warn	auto-join	Attempted to join FortiCloud	FortiCloud auto-join attempted	2023/03/14 09:07:15	Info		Performance statistics: average CPU: 0, memory: 43...	System performance statistics	2023/03/14 09:02:15	Info		Performance statistics: average CPU: 0, memory: 43...	System performance statistics	2023/03/14 08:58:41	Info		DHCP statistics	DHCP statistics	2023/03/14 08:58:41	Info		DHCP statistics	DHCP statistics	2023/03/14 08:57:37	Warn	auto-join	FortiCloud service activation failed	FortiCloud activation failed	2023/03/14 08:57:37	Warn	auto-join	Attempted to join FortiCloud	FortiCloud auto-join attempted	2023/03/14 08:57:15	Info		Performance statistics: average CPU: 0, memory: 43...	System performance statistics
Date/Time	Level	User	Message	Log Description																																																																																																						
2023/03/14 09:28:12	Info	admin	Edit firewall policy 1	Object attribute configured																																																																																																						
2023/03/14 09:27:41	Warn	auto-join	FortiCloud service activation failed	FortiCloud activation failed																																																																																																						
2023/03/14 09:27:41	Warn	auto-join	Attempted to join FortiCloud	FortiCloud auto-join attempted																																																																																																						
2023/03/14 09:27:15	Info		Performance statistics: average CPU: 3, memory: 43...	System performance statistics																																																																																																						
2023/03/14 09:22:15	Info		Performance statistics: average CPU: 0, memory: 43...	System performance statistics																																																																																																						
2023/03/14 09:20:34	Info	admin	Administrator admin logged in successfully from jsc...	Admin login successful																																																																																																						
2023/03/14 09:17:40	Warn	auto-join	FortiCloud service activation failed	FortiCloud activation failed																																																																																																						
2023/03/14 09:17:39	Warn	auto-join	Attempted to join FortiCloud	FortiCloud auto-join attempted																																																																																																						
2023/03/14 09:17:23	Info		Fortigate scheduled update fcnl+yes fdn+yes fsci+...	FortiGate update succeeded																																																																																																						
2023/03/14 09:17:15	Info		Performance statistics: average CPU: 6, memory: 43...	System performance statistics																																																																																																						
2023/03/14 09:12:15	Info		Performance statistics: average CPU: 0, memory: 43...	System performance statistics																																																																																																						
2023/03/14 09:07:38	Warn	auto-join	FortiCloud service activation failed	FortiCloud activation failed																																																																																																						
2023/03/14 09:07:38	Warn	auto-join	Attempted to join FortiCloud	FortiCloud auto-join attempted																																																																																																						
2023/03/14 09:07:15	Info		Performance statistics: average CPU: 0, memory: 43...	System performance statistics																																																																																																						
2023/03/14 09:02:15	Info		Performance statistics: average CPU: 0, memory: 43...	System performance statistics																																																																																																						
2023/03/14 08:58:41	Info		DHCP statistics	DHCP statistics																																																																																																						
2023/03/14 08:58:41	Info		DHCP statistics	DHCP statistics																																																																																																						
2023/03/14 08:57:37	Warn	auto-join	FortiCloud service activation failed	FortiCloud activation failed																																																																																																						
2023/03/14 08:57:37	Warn	auto-join	Attempted to join FortiCloud	FortiCloud auto-join attempted																																																																																																						
2023/03/14 08:57:15	Info		Performance statistics: average CPU: 0, memory: 43...	System performance statistics																																																																																																						
Comentário																																																																																																										

Item de Teste - 5.3.2.23	Deverá permitir a ativação/desativação de regras de forma programada conforme a data/hora;
Objetivo do Teste	Validar se o FortiGate permite a ativação e desativação de regras de forma programada.
Configuração do Teste	Demonstrar base de regras do FortiGate

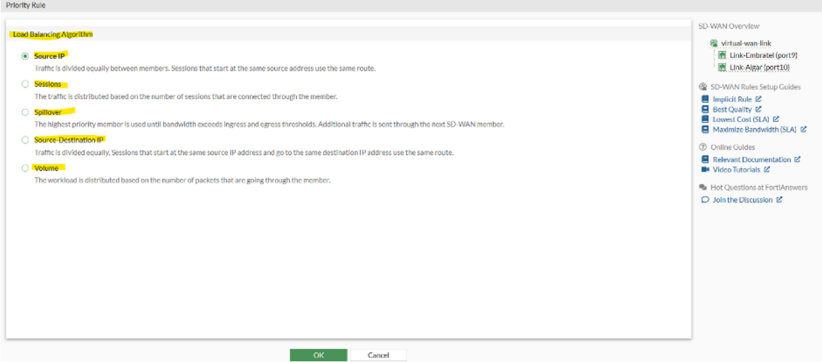
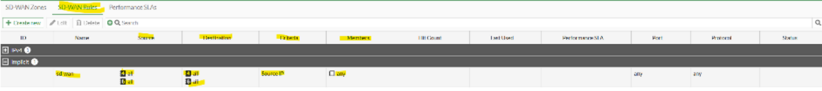
Procedimento do Teste	<p>1 - Navegando por Policy & Objects > Firewall Policy > Schedules é possível criar um período que a regra irá funcionar.</p> <p>2 - Navegando por Policy & Objects > Firewall Policy > é possível adicionar o objeto de Schedule criado anteriormente em qualquer uma das políticas existentes, basta selecionar o objeto de Schedule dentro do respectivo campo dentro da política, no campo "Schedule":</p>
Evidências	<p>Criação do objeto de tempo "Schedule"</p>  <p>Aplicação do objeto "Schedule" dentro de uma política de firewall.</p>

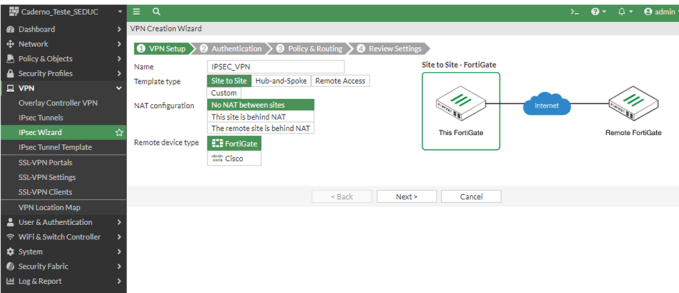


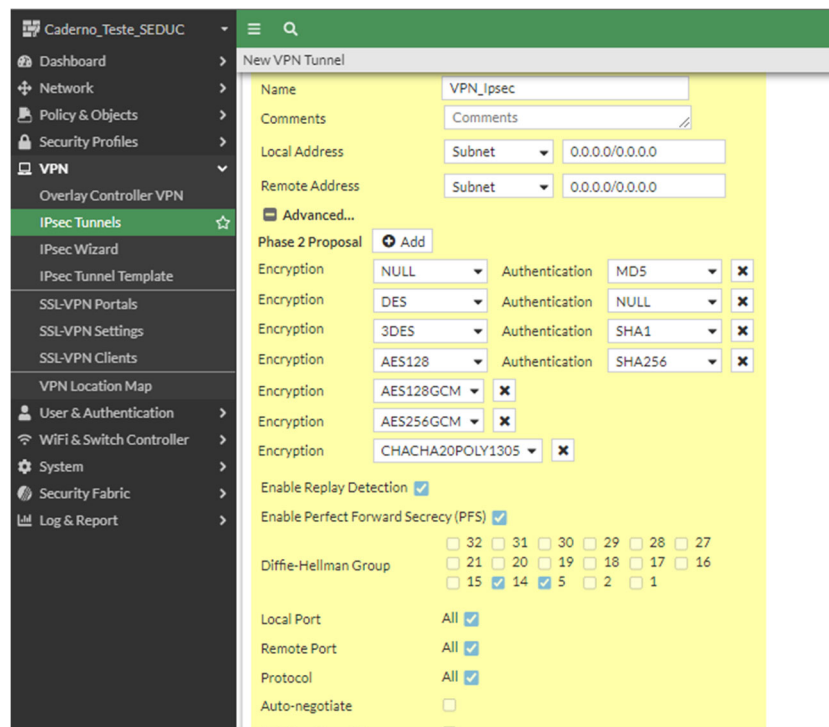
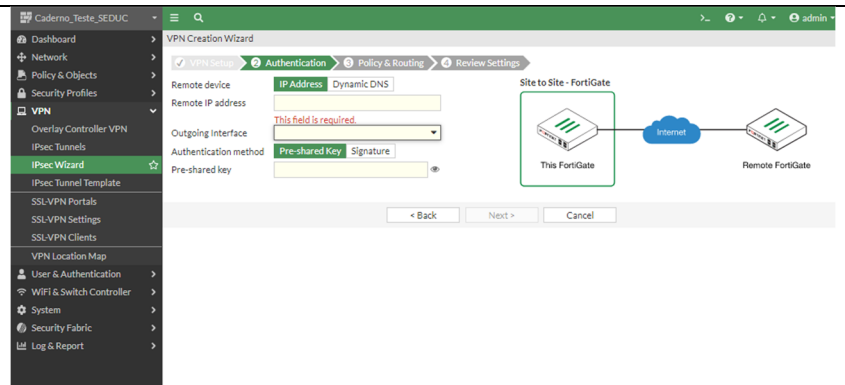
<p>Comentário</p>	
-------------------	--

5.3.3 SDWAN

<p>Item de Teste - 5.3.3.2</p>	<p>A solução deverá ser capaz de balancear cargas entre dois links distintos;</p>
<p>Objetivo do Teste</p>	<p>Demonstrar capacidade de balancear o tráfego de 2 links distintos através de SDWAN</p>
<p>Configuração do Teste</p>	<p>Demonstrar base de regras do FortiGate</p>
<p>Procedimento do Teste</p>	<p>Navegando por Network > SDWAN > Create new member é possível acrescentar links para serem balanceados pelo SDWAN</p> <p>Navegando por Network > SDWAN > Performace SLA é definindo o algoritmo mais adequado para o balanceamento;</p> <p>Navegando por Network > SDWAN > SDWAN Rules é possível criar regra para enquadrar o algoritmo de balanceamento.</p>
<p>Evidências</p>	<p>Criação dos membros (links) que vão participar do SDWAN</p> <p>2- Definindo o algoritmo mais adequado para o balanceamento;</p>

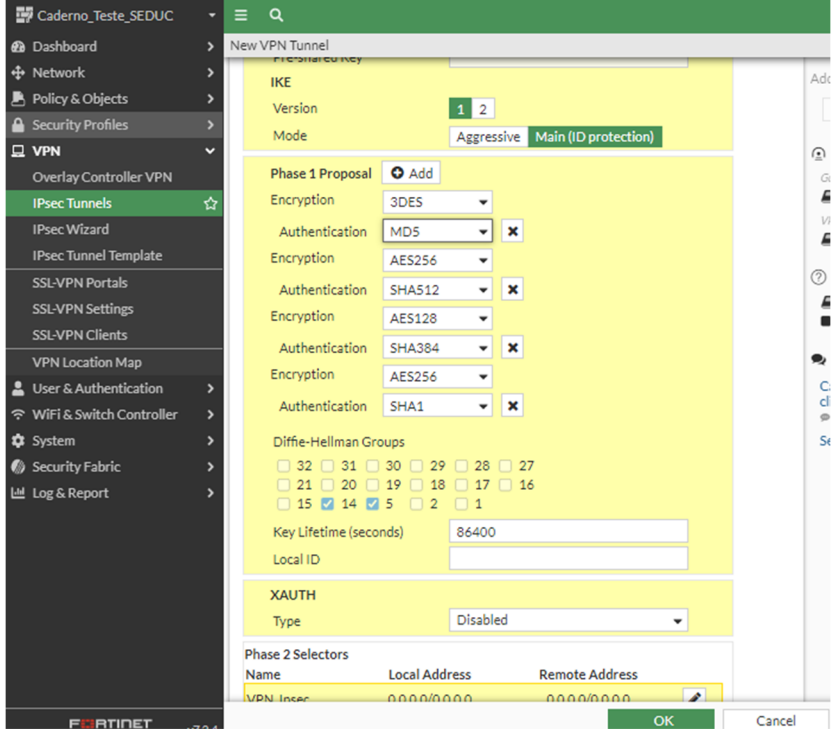
	 <p>3- Criando rule de SDWAN para permitir que os membros (links) sejam balanceados através do algoritmo selecionado.</p> 
Comentário	Fonte: https://docs.fortinet.com/document/FortiGate/7.2.3/administration-guide/683285

Item de Teste - 5.3.3.3	Deverá implementar a criação de tuneis criptografados de forma dinâmica entre os sites;
Objetivo do Teste	Validar se o FortiGate permite a criação de tuneis IPsecVPN de forma dinâmica e criptografado, site-to-site.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	1 – Navegando por VPN > IPsec Tunnels > Create New é possível realizar a criação de tuneis IPsec VPN de forma dinâmica e criptografada, conforme evidências abaixo
Evidências	



SETOR BANCÁRIO SUL - QUADRA 2 - EDIFÍCIO JOÃO CARLOS SAAD - 8º ANDAR - CEP 70.070-120 - ASA SUL - BRASÍLIA/DF

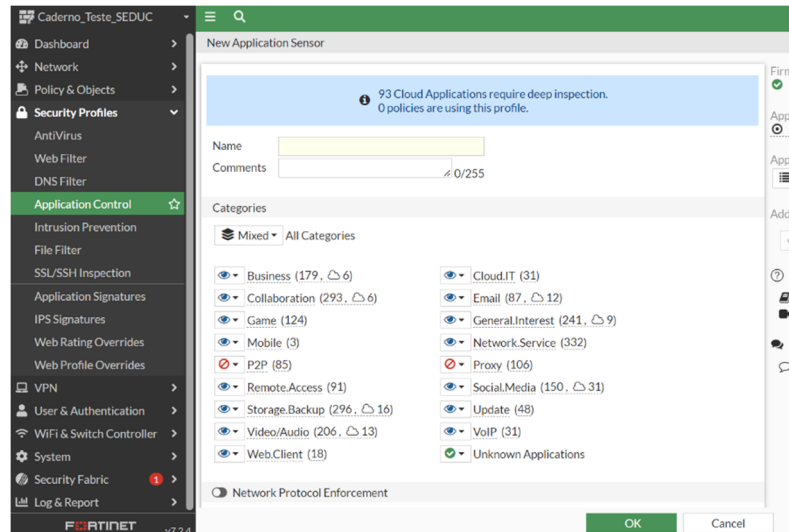
www.nct.com.br

	 <p>ADVPN</p> <p>Auto-Discovery VPN (ADVPN) allows the central hub to dynamically inform spokes about a better path for traffic between two spokes.</p> <p>The following topics provide instructions on configuring ADVPN:</p> <ul style="list-style-type: none"> • IPsec VPN wizard hub-and-spoke ADVPN support • ADVPN with BGP as the routing protocol • ADVPN with OSPF as the routing protocol • ADVPN with RIP as the routing protocol • UDP hole punching for spokes behind NAT
<p>Comentário</p>	<p>Fonte: Acessado em https://docs.fortinet.com/document/FortiGate/7.2.0/administration-guide/978793</p>

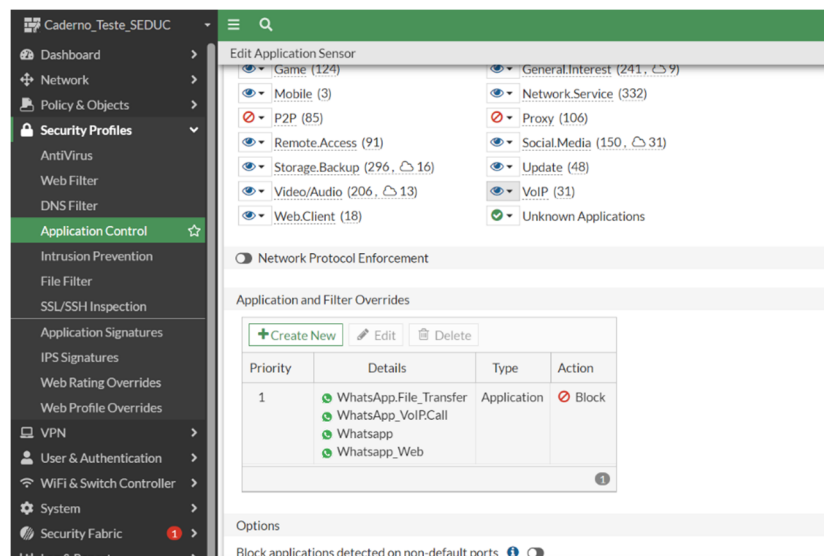
<p>Item de Teste - 5.3.3.5</p>	<p>Deverá implementar controle de tráfego por aplicação;</p>
<p>Objetivo do Teste</p>	<p>Validar se o FortiGate é capaz de realizar controle de tráfego por aplicação</p>
<p>Configuração do Teste</p>	<p>Demonstrar base de regras do FortiGate</p>
<p>Procedimento do Teste</p>	<p>Para realizar o controle de tráfego por aplicação é necessário configurar um Application Control Profile e enquadrar o perfil em alguma regra onde o fluxo tenha como destino a internet;</p> <p>Navegando por Security Profile > Application Control > Create new é possível criar um novo perfil enquadrando as aplicações que deseja bloquear, monitorar ou aprovar;</p>

Navegando por **Policy & Objects > Firewall Policy** é possível enquadrar o perfil de Application Control criado para determinar em qual fluxo ocorrerá o controle de tráfego por aplicação.

1 – Criando um perfil de Application Control

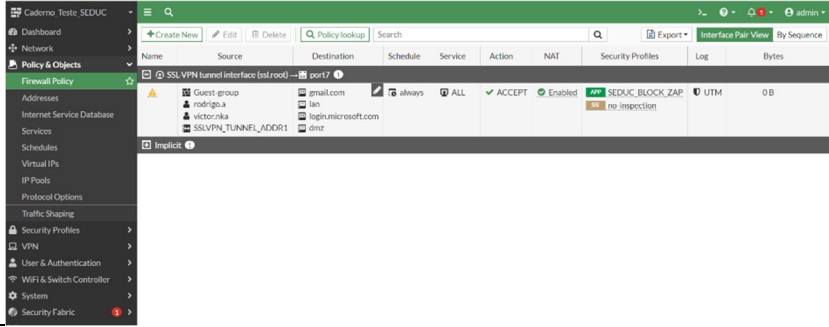


2 – Escolhendo quais categorias de aplicações vão ser permitidas, monitoradas e bloqueadas. Também é possível criar exceções dentro dessas categorias. No exemplo abaixo a categoria Social Media está para monitorar e a aplicação WhatsApp está com uma exceção para bloquear



3 – Enquadrando o perfil na política



	<p>Security Profiles</p> <p>AntiVirus <input type="checkbox"/></p> <p>Web Filter <input type="checkbox"/></p> <p>DNS Filter <input type="checkbox"/></p> <p>Application Control <input checked="" type="checkbox"/> APP SEDUC_BLOCK_ZAP</p> <p>IPS <input type="checkbox"/></p> <p>File Filter <input type="checkbox"/></p> <p>SSL Inspection <input checked="" type="checkbox"/> SSL certificate-inspection</p> <p>4 – Abaixo o exemplo de como a política fica com o perfil enquadrado</p> 
Comentário	

Item de Teste - 5.3.3.6	Deverá suportar, no mínimo, 3 (três) links de WAN;
Objetivo do Teste	Demonstrar que a ferramenta possui mais de três links de WAN
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Demonstrar base de regras do FortiGate
Evidências	Qualquer interface no FortiGate pode ser definida como uma interface WAN.



	<p>Edit Interface</p> <p>Name port9</p> <p>Alias <input type="text"/></p> <p>Type Physical Interface</p> <p>VRF ID ⓘ 0</p> <p>Role ⓘ <ul style="list-style-type: none">UndefinedLANWANDMZUndefined</p> <p>Address <input type="text"/></p> <p>Addressing m <input type="text"/> ana</p> <p>IP/Netmask <input type="text"/> 0.0.0.0/0.0.0.0</p>
	<p>Comentário</p>

Item de Teste - 5.3.3.9	Distribuição de tráfego com balanceamento de sessão entre os circuitos existentes;
Objetivo do Teste	Criar regra que balanceie o tráfego entres todos os links wan
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Demonstrar base de regras do FortiGate



<p>Evidências</p>	
<p>Comentário</p>	

<p>Item de Teste - 5.3.3.10</p>	<p>Distribuição orientada a qualidade, o dispositivo deve validar o melhor caminho disponível e utilizar deste path para manter sessões ativas, caso o melhor caminho entre em degradação por fatores anômalos o dispositivo deverá entender estes fatores e distribuir para os demais circuitos existentes;</p>
<p>Objetivo do Teste</p>	<p>Validar se o firewall possibilita a distribuição orientada a qualidade, o dispositivo deve validar o melhor caminho disponível e utilizar deste path para manter sessões ativas, caso o melhor caminho entre em degradação por fatores anômalos o dispositivo deverá entender estes fatores e distribuir para os demais circuitos existentes;</p>
<p>Configuração do Teste</p>	<p>Demonstrar base de regras do FortiGate com SLA selecionado</p>
<p>Procedimento do Teste</p>	<p>Vá em Network -> SDWAN.</p>



<p>Evidências</p>	
<p>Comentário</p>	

<p>Item de Teste -5.3.3.11</p>	<p>Os dispositivos remotos devem suportar a funcionalidade de ZTP (Zero Touch Provisioning) para que assim, inseridos nas estruturas remotas, possam buscar automaticamente por suas configurações, com o objetivo de facilitar a instalação nas unidades remotas ou a troca de um dispositivo defeituoso;</p>
<p>Objetivo do Teste</p>	<p>Mostrar que os dispositivos remotos suportam a funcionalidade ZTP.</p>
<p>Configuração do Teste</p>	<p>Integração com o FortiManager</p>
<p>Procedimento do Teste</p>	<p>Para realizar essa configuração basta adicionar um novo dispositivo e colocar as especificações dele, assim ele será cadastrado e quando for ligado buscará automaticamente pelas suas configurações.</p>



Evidências

The screenshot displays the FortiManager Device Manager interface. It shows three sequential steps in the 'Add Device' wizard:

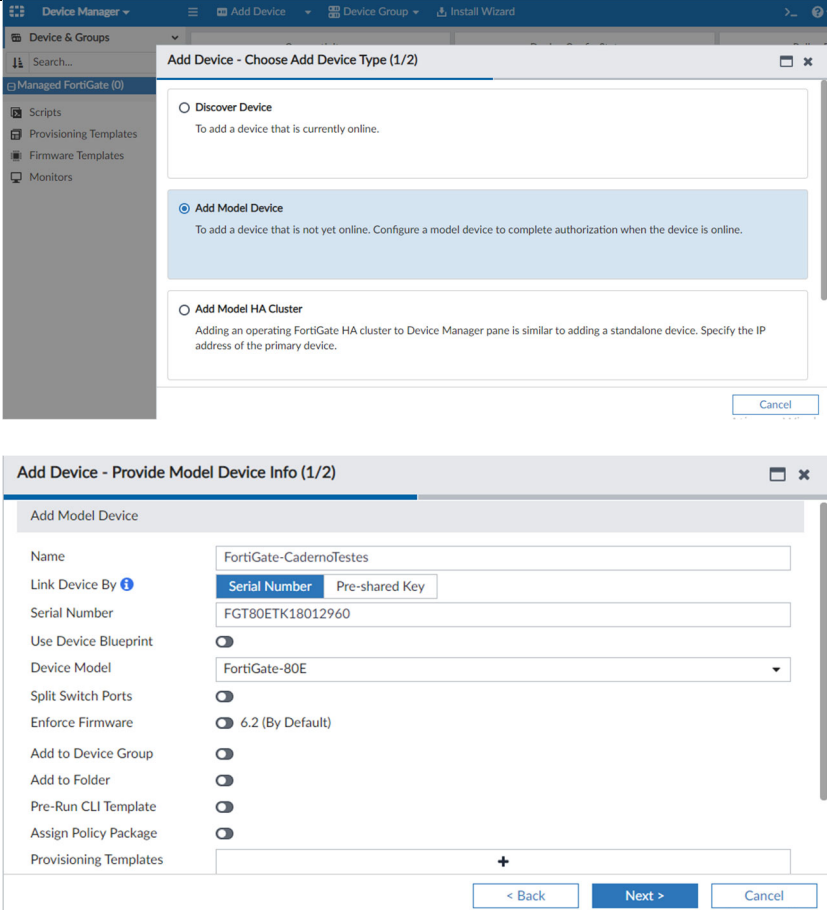
- Add Device - Choose Add Device Type (1/2):** The 'Add Model Device' option is selected.
- Add Device - Provide Model Device Info (1/2):** Fields include Name (FortiGate-CademoTestes), Link Device By (Serial Number), Serial Number (FGT80ETK18012960), Device Model (FortiGate-80E), and various configuration options like Enforce Firmware (6.2) and Add to Device Group.
- Add Device - Adding Model Device (2/2):** Shows a success message: 'Device is added successfully' with a list of completed steps: Creating device database, Retrieving high availability status, Initializing configuration database, Updating group membership, and Successfully add device.

At the bottom, a 'Finish' button is visible, followed by a summary table:

Layer	Functions	Devices
Management and orchestration	<ul style="list-style-type: none">Unified managementTemplate based solutionZero touch provisioningLogging, monitoring, and analysisAutomated orchestration using the REST API	FortiManager FortiAnalyzer



Comentário	Fonte: FortiOS-7.2.3-Administration_Guide disponível em https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a06117ca-5fbf-11ed-96f0-fa163e15d75b/FortiOS-7.2.3-Administration_Guide.pdf https://docs.fortinet.com/document/FortiGate/6.2.14/cookbook/861490/zero-touch-provisioning-with-fortimanager
-------------------	--

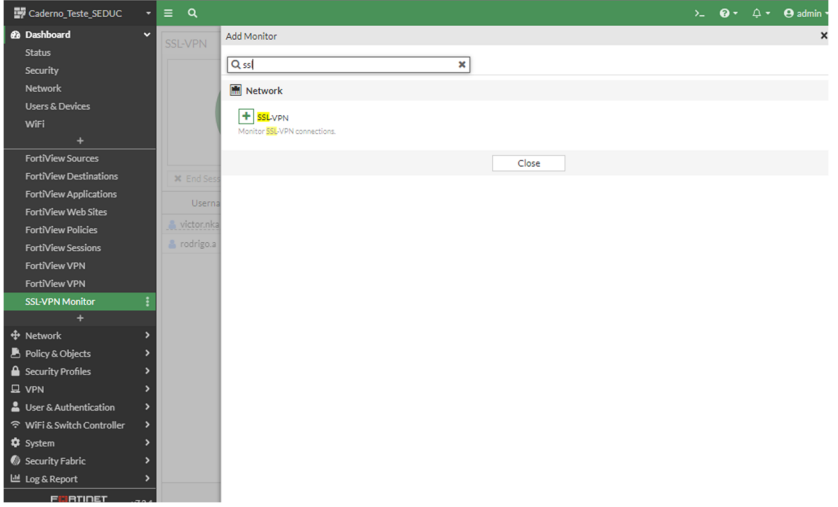
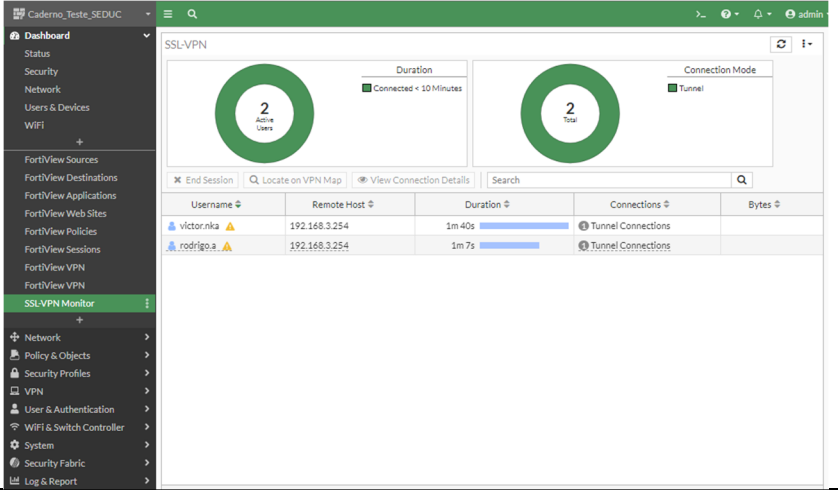
Item de Teste - 5.3.3.12	Gerenciamento centralizado e implantação Zero Touch;
Objetivo do Teste	Mostrar que o equipamento de gerência centralizada com suporte a funcionalidade de implantação ZTP.
Configuração do Teste	Mostrar que os dispositivos remotos suportam a funcionalidade ZTP.
Procedimento do Teste	Para realizar essa configuração basta adicionar um novo dispositivo e colocar as especificações dele, assim ele será cadastrado e quando for ligado buscará automaticamente pelas suas configurações.
Evidências	 <p>The screenshot shows two windows from the FortiManager interface. The top window is titled 'Add Device - Choose Add Device Type (1/2)' and contains three radio button options: 'Discover Device' (unselected), 'Add Model Device' (selected), and 'Add Model HA Cluster' (unselected). The bottom window is titled 'Add Device - Provide Model Device Info (1/2)' and contains a form with the following fields: Name (FortiGate-CadernoTestes), Link Device By (Serial Number selected), Serial Number (FGT80ETK18012960), Use Device Blueprint (off), Device Model (FortiGate-80E), Split Switch Ports (off), Enforce Firmware (6.2 (By Default)), Add to Device Group (off), Add to Folder (off), Pre-Run CLI Template (off), Assign Policy Package (off), and Provisioning Templates (empty). Navigation buttons '< Back', 'Next >', and 'Cancel' are visible at the bottom of the second window.</p>



	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px;">Add Device - Adding Model Device (2/2) x</div> <p>Name: FortiGate-CademoTestes</p> <p>Status: ✔ Device is added successfully</p> <ul style="list-style-type: none"> ✔ Creating device database ✔ Retrieving high availability status ✔ Initializing configuration database ✔ Updating group membership ✔ Successfully add device <div style="text-align: right; margin-top: 10px;">Finish</div> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr style="background-color: #0070c0; color: white;"> <th>Layer</th> <th>Functions</th> <th colspan="2">Devices</th> </tr> </thead> <tbody> <tr> <td style="background-color: #f0f0f0;">Management and orchestration</td> <td style="background-color: #f0f0f0;"> <ul style="list-style-type: none"> Unified management Template based solution <li style="background-color: yellow;">Zero touch provisioning Logging, monitoring, and analysis Automated orchestration using the REST API </td> <td style="background-color: #f0f0f0; text-align: center;">FortiManager </td> <td style="background-color: #f0f0f0; text-align: center;">FortiAnalyzer </td> </tr> </tbody> </table> </div>	Layer	Functions	Devices		Management and orchestration	<ul style="list-style-type: none"> Unified management Template based solution <li style="background-color: yellow;">Zero touch provisioning Logging, monitoring, and analysis Automated orchestration using the REST API 	FortiManager 	FortiAnalyzer
Layer	Functions	Devices							
Management and orchestration	<ul style="list-style-type: none"> Unified management Template based solution <li style="background-color: yellow;">Zero touch provisioning Logging, monitoring, and analysis Automated orchestration using the REST API 	FortiManager 	FortiAnalyzer 						
Comentário	Fonte: FortiOS-7.2.3-Administration_Guide disponível em https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a06117ca-5fbf-11ed-96f0-fa163e15d75b/FortiOS-7.2.3-Administration_Guide.pdf								

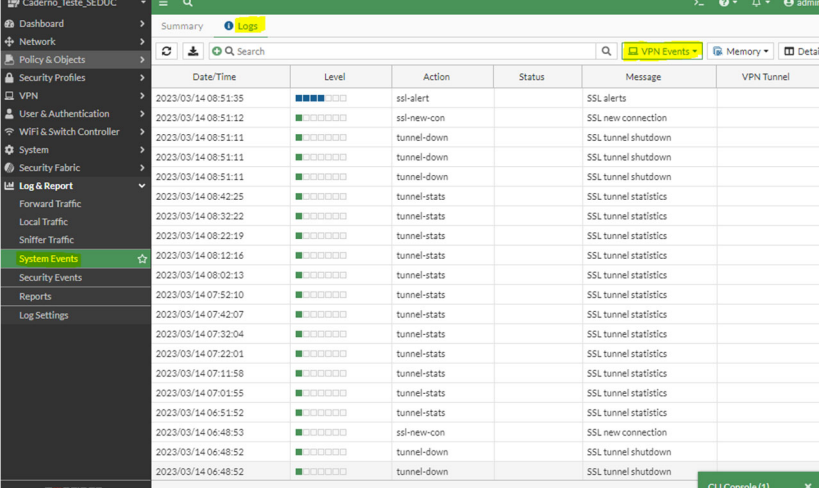
5.3.4 ACESSO REMOTO - VPN:

Item de Teste - 5.3.4.10	Deverá ser capaz de monitorar todos os usuários remotos logados;
Objetivo do Teste	Validar se o FortiGate é capaz de realizar o monitoramento de todos os usuários conectados remotamente por meio de VPN.
Configuração do Teste	Demonstrar os usuários VPN conectados
Procedimento do Teste	Navegando por Dashboard > + > Add Monitor > SSL-VPN é possível adicionar um widgets SSL-VPN que permite o monitoramento de usuários conectados remotamente.

<p>Evidências</p>	  <table border="1" data-bbox="683 1048 1353 1120"> <thead> <tr> <th>Username</th> <th>Remote Host</th> <th>Duration</th> <th>Connections</th> <th>Bytes</th> </tr> </thead> <tbody> <tr> <td>Victor.nka</td> <td>192.168.3.254</td> <td>1m 40s</td> <td>Tunnel Connections</td> <td></td> </tr> <tr> <td>rodrigo.a</td> <td>192.168.3.254</td> <td>1m 7s</td> <td>Tunnel Connections</td> <td></td> </tr> </tbody> </table>	Username	Remote Host	Duration	Connections	Bytes	Victor.nka	192.168.3.254	1m 40s	Tunnel Connections		rodrigo.a	192.168.3.254	1m 7s	Tunnel Connections	
Username	Remote Host	Duration	Connections	Bytes												
Victor.nka	192.168.3.254	1m 40s	Tunnel Connections													
rodrigo.a	192.168.3.254	1m 7s	Tunnel Connections													
<p>Comentário</p>																

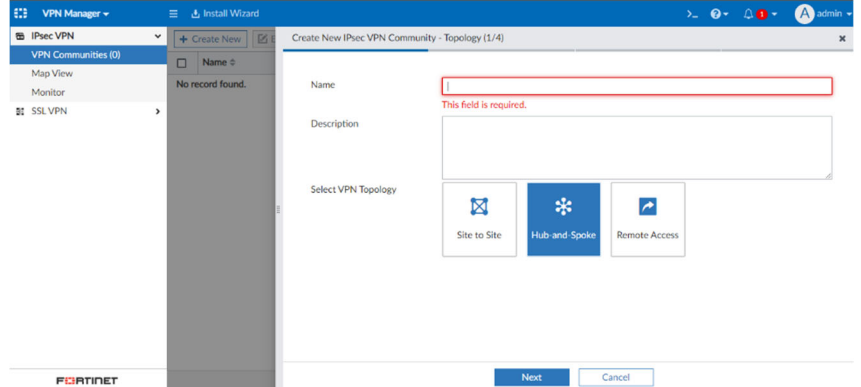
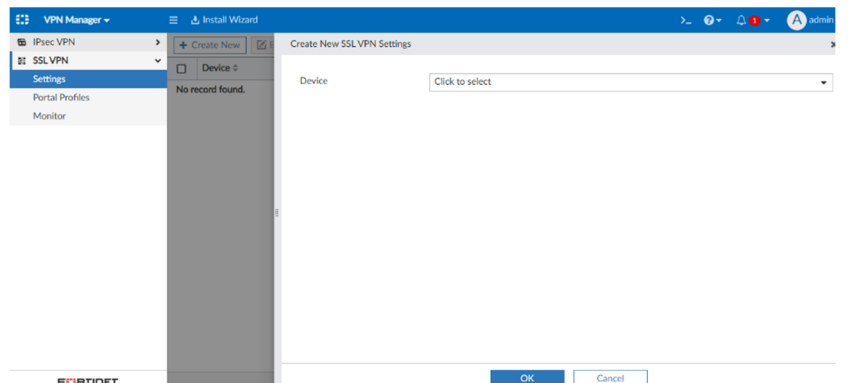
<p>Item de Teste - 5.3.4.11</p>	<p>Deverá ser capaz de reconhecer falhas e problemas de conectividade entre dois pontos conectados através de uma VPN, e registrar e alertar quando o túnel VPN está desconectado;</p>
<p>Objetivo do Teste</p>	<p>Validar se o appliance é capaz de reconhecer falhas e problemas de conectividade entre dois pontos de uma VPN e realizar o registro de alertas quando o túnel VPN está desconectado.</p>
<p>Configuração do Teste</p>	<p>Demonstrar notificação de Túnel VPN desconectado, como exemplo via email.</p>
<p>Procedimento do Teste</p>	<p>Para criar um novo stitch automático vá em Security Fabric -> Automation -> Create New.</p> <p>Depois de colocar um nome, selecionar no gatilho do evento "Event Log" e em ação selecionar "e-mail".</p> <p>Preencher os campos:</p> <p>- To.</p>



	<p>- Email subject.</p> <p>- Email body.</p> <p>No gatilho colocar "IPsec connection status changed".</p> <p>Ao acessar a seção "Log & Report" e, em seguida, "System Events" e "VPN Events", é possível identificar falhas e problemas de conectividade em um ambiente de rede virtual privada (VPN).</p>
<p>Evidências</p>	 <p>The screenshot shows the Fortinet VPN Manager interface. The left sidebar is expanded to 'Log & Report', with 'System Events' and 'VPN Events' selected. The main area displays a table of logs with columns for Date/Time, Level, Action, Status, Message, and VPN Tunnel. The logs show various events such as 'ssl-alert', 'ssl-new-con', 'tunnel-down', and 'tunnel-stats'.</p>
<p>Comentário</p>	

<p>Item de Teste - 5.3.4.12</p>	<p>Deve incluir gerenciamento centralizado de VPNs, com a possibilidade de estabelecimento de VPNs com vários peers remotos ao mesmo tempo;</p>
<p>Objetivo do Teste</p>	<p>Validar se é possível estabelecer VPNs com vários peers remotos ao mesmo tempo e realizar o gerenciamento centralizado de VPNs.</p>
<p>Configuração do Teste</p>	<p>Demonstrar a capacidade de estabelecimento de múltiplos túneis VPN com diversos peers.</p>
<p>Procedimento do Teste</p>	<p>Navegando por VPN Manager é possível criar, monitorar e gerenciar configurações de VPN, tanto de SSL como IPsec. Sendo possível estabelecer VPNs com vários peers remotos ao mesmo tempo.</p>
<p>Evidências</p>	



	 
Comentário	https://docs.fortinet.com/document/fortimanager/7.2.1/administration-guide/9083 na Página 484.

Item de Teste - 5.3.4.13	Clientes IPsec do mesmo fabricante devem estar disponíveis para pelo menos Windows 10 (64 bits);
Objetivo do Teste	Validar se o Forticlient está disponível para Windows 10 (64 bits)
Configuração do Teste	Forticlient é totalmente compatível com Windows 10 e permite conexões tanto SSL VPN quanto IPsec VPN.
Procedimento do Teste	1 – Realizar o download do FortiClient VPN pelo link " Link para baixar " cliente gratuito fornecido pela mesma fabricante das soluções 2 – Configurar IPsec VPN







Evidências


FortiClient VPN

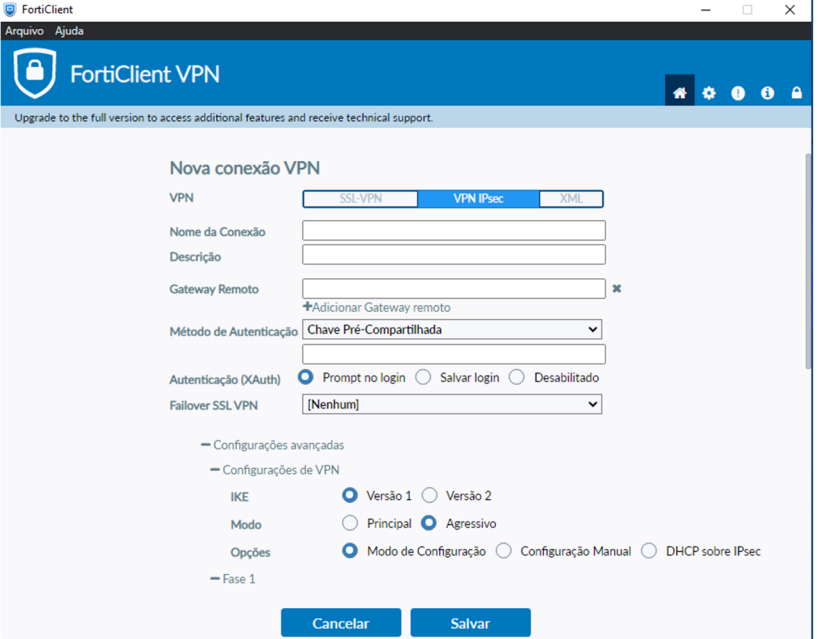
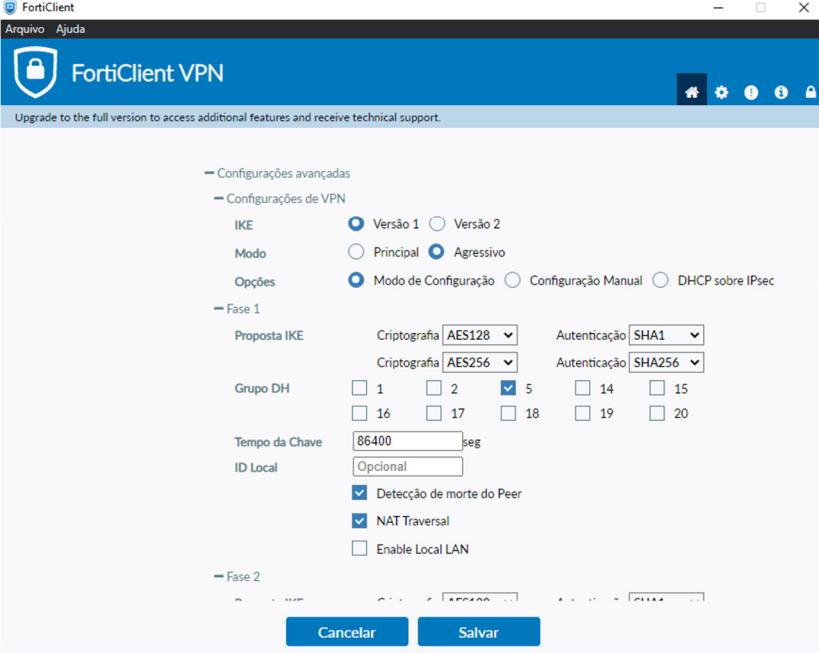
The VPN-only version of FortiClient offers SSL VPN and IPsecVPN, but does not include any support. Download the best VPN software for multiple devices.

Remote Access

- ✓ SSL VPN with MFA
- ✓ IPSEC VPN with MFA

 Download VPN for Windows	 Download VPN for MacOS	 Download VPN for Linux
DOWNLOAD	DOWNLOAD	DOWNLOAD .rpm
 Download VPN for iOS	 Download VPN for Android	 Download VPN for Linux
DOWNLOAD	DOWNLOAD	DOWNLOAD .deb

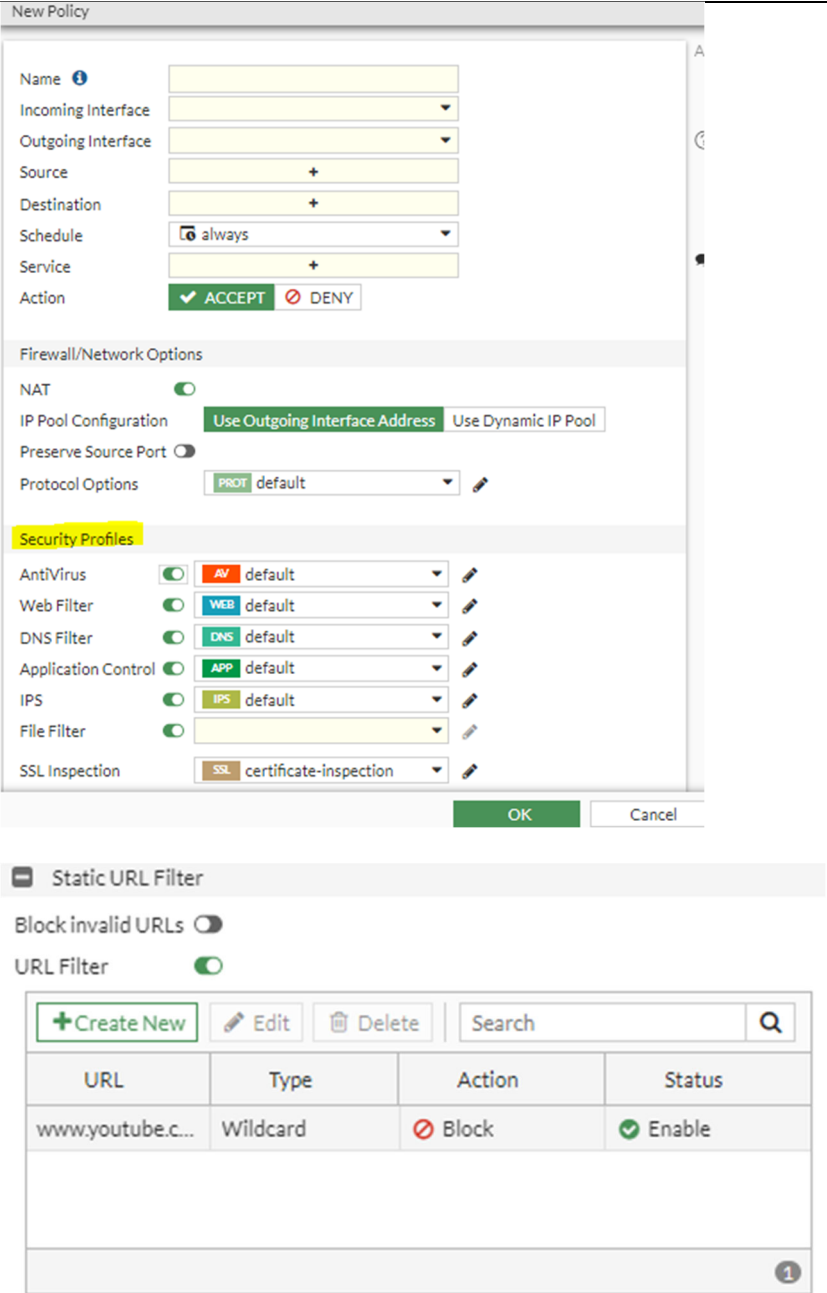


<p>Comentário</p>	
	


5.3.5 CONTROLE DE APLICAÇÕES WEB E FILTRO URL:

<p>Item de Teste - 5.3.5.1</p>	<p>A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança, que permita a criação de políticas de liberação ou bloqueio;</p>
---------------------------------------	--



Objetivo do Teste	Validar se a solução conta com ferramentas de visibilidade e controle de aplicações Web e Filtro URL integrada, que permita a criação de políticas de liberação ou bloqueio.								
Configuração do Teste	Configuração de regra de segurança NGFW com filtro de aplicação e URL.								
Procedimento do Teste	Navegando por Security Profiles > Web Filter é possível criar filtro de URL que pode ser adicionado as regras em Security Profile, assim liberando ou bloqueando URL, tal funcionalidade é nativa do appliance.								
Evidências	 <p>The screenshot displays the configuration interface for a New Policy. The 'Name' field is empty. The 'Incoming Interface' and 'Outgoing Interface' are set to default. The 'Source' and 'Destination' fields have a '+' icon. The 'Schedule' is set to 'always'. The 'Service' field has a '+' icon. The 'Action' is set to 'ACCEPT'. The 'Firewall/Network Options' section includes 'NAT' (checked), 'IP Pool Configuration' (Use Outgoing Interface Address and Use Dynamic IP Pool), 'Preserve Source Port' (unchecked), and 'Protocol Options' (PROT default). The 'Security Profiles' section is highlighted and includes: 'AntiVirus' (checked, AV default), 'Web Filter' (checked, WEB default), 'DNS Filter' (checked, DNS default), 'Application Control' (checked, APP default), 'IPS' (checked, IPS default), 'File Filter' (checked), and 'SSL Inspection' (SSL certificate-inspection). Below this is the 'Static URL Filter' section, which includes 'Block invalid URLs' (unchecked) and 'URL Filter' (checked). A table lists the URL filters:</p> <table border="1"><thead><tr><th>URL</th><th>Type</th><th>Action</th><th>Status</th></tr></thead><tbody><tr><td>www.youtube.c...</td><td>Wildcard</td><td>Block</td><td>Enable</td></tr></tbody></table>	URL	Type	Action	Status	www.youtube.c...	Wildcard	Block	Enable
URL	Type	Action	Status						
www.youtube.c...	Wildcard	Block	Enable						

Comentário	
------------	--

Item de Teste - 5.3.5.2	A solução deve ser capaz de identificar qualquer tipo de aplicação, em até camada 7, independente de porta e protocolo;
Objetivo do Teste	Verificar se o equipamento identifica uma aplicação independente de porta ou protocolo.
Configuração do Teste	Criar filtro de aplicação de camada 7
Procedimento do Teste	Criar regra contendo filtro de aplicação de camada 7.
Evidências	<p>“Controle de aplicação utiliza do decodificador de protocolos IPS que consegue analisar o tráfego da rede e identificar as aplicações mesmo se elas utilizarem portas ou protocolos que não são padrões”</p> <p>Application control</p> <p>FortiGate can recognize network traffic generated by a large number of applications. Application control sensors specify what action to take with the application traffic. 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 supports traffic detection using the HTTP protocol (versions 1.0, 1.1, and 2.0).</p> <div data-bbox="523 994 1273 1809" style="border: 1px solid black; padding: 10px;">  <p>ActMobile.VPN</p> <p>ID 43286</p> <p>Summary This indicates an attempt to use ActMobile VPN service.</p> <p>ActMobile Networks works on making mobile devices fast, cost effective and reliable, despite wireless variability. It provides multiple VPN products. The signature is mainly created for DashVPN application.</p> <p>Category Proxy</p> <p>Risk ■■■■■</p> <p>Popularity ★☆☆☆☆</p> <p>Protocol TCP, SSL, UDP, DNS</p> <p>Technology Client-Server</p> <p>Behavior Tunneling</p> <p>Vendor Other</p> </div>



Comentário	Fonte: FortiOS-7.2.3Administration_Guide acessado em https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a06117ca-5fbf-11ed-96f0-fa163e15d75b/FortiOS-7.2.3-Administration_Guide.pdf
-------------------	---

Item de Teste - 5.3.5.3	A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser centralizada na mesma console de gerenciamento;
Objetivo do Teste	Verificar se o equipamento possui a funcionalidade de gerenciar as políticas de segurança de controle de aplicação e controle de URL's de forma centralizada.
Configuração do Teste	Utilizar um FortiGate com os serviços de Fabric connector enable, linkado a um FortiManager que realiza a gerência centralizada.
Procedimento do Teste	Criação de uma política que possui controle de aplicação e um controle de URL's. Para realizar essa configuração primeiramente tem que acessar a aba de "Policy & Objects", lá terá visibilidades de todos os pacotes de políticas presentes no equipamento de gerência. Assim, basta selecionar a regra desejada e aplicar um perfil de segurança. Dentro desses "Security Profiles" temos as opções de WebFilter Profile (controle de URL'S) e o Application Control (Controle de Aplicação).

Evidências

The screenshot displays the FortiGate management interface. The top navigation bar includes 'Policy & Objects', 'Policy Package', 'Install Wizard', 'ADOM Revisions', and 'Tools'. Below this is a grid of management modules: Device Manager, Policy & Objects (highlighted), AP Manager, VPN Manager, Fabric View, FortiGuard, FortiSwitch Manager, Extender Manager, System Settings, and Management Extensions.

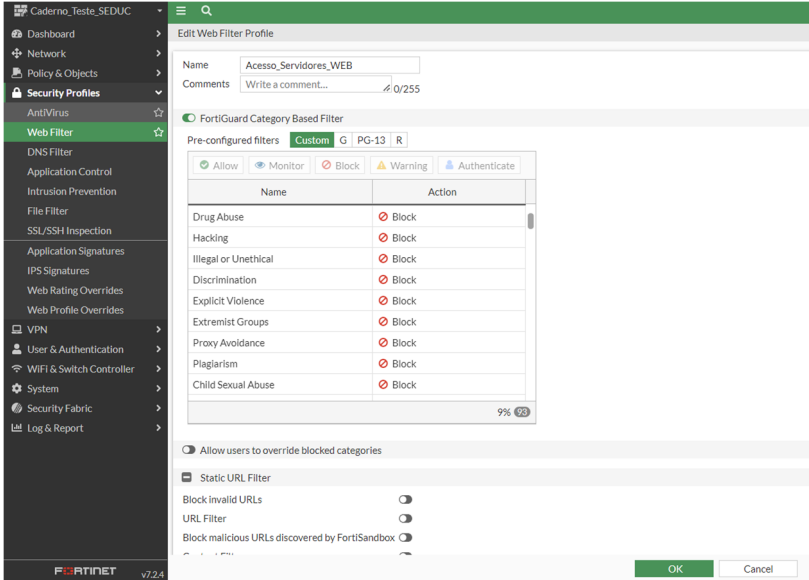
Below the grid is a table of Policy Packages:

#	Name	From	To	Source	Destination	Security Profiles	Schedule	Service
1	Acesso_Internet	lan	wan1	all	all	No-Inspection default	always	ALL
2	Acesso_VPN	osvpn_lan_intf	lan	SSLVPN_TUNNEL rod-ipo	gmail.com login.microsoft.com login.microsoft.com login.microsoft.com login.microsoft.com	No-Inspection default	always	ALL
3	Implicit Deny (3/3 Total)	any	any	all	all		always	ALL



<p>Comentário</p>	<p>The screenshot shows the Mikrotik WinBox interface. At the top, there's a table of Firewall Rules. Rule 2, 'Acesso_VPN', is selected. Below it, the 'Static URL Filter' section is visible, with 'Block Invalid URLs' and 'Web URL Filter' both set to 'On'. Under 'Web URL Filter Entry', there is a table with columns: URL, Action, Type, Referrer Host, and Status. The table is currently empty, showing 'No record found.' Below this is the 'Add Signatures' section, which contains a table of signatures with columns: Name, Category, Technology, Popularity, Risk, and DB. The signature table lists various categories like Email, Video/Audio, Social Media, and Storage.Backup.</p>																																																																																																			
	<p>Static URL Filter</p> <p>Block Invalid URLs: <input checked="" type="checkbox"/></p> <p>Web URL Filter: <input checked="" type="checkbox"/></p> <p>Web URL Filter Entry</p> <p>+ Create New Edit Delete Move Up Move Down Search...</p> <table border="1"> <thead> <tr> <th>URL</th> <th>Action</th> <th>Type</th> <th>Referrer Host</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td colspan="5" style="text-align: center;">No record found.</td> </tr> </tbody> </table> <p>0</p> <p>Add Signatures</p> <p>Add Filter Search</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Category</th> <th>Technology</th> <th>Popularity</th> <th>Risk</th> <th>DB</th> </tr> </thead> <tbody> <tr> <td>ic126.Mail</td> <td>Email</td> <td>Browser-Based</td> <td>★★★★★</td> <td>Medium</td> <td>Regular</td> </tr> <tr> <td>ixoun</td> <td>Video/Audio</td> <td>Client-Server</td> <td>★★★★★</td> <td>Medium</td> <td>Regular</td> </tr> <tr> <td>lund1.Mail</td> <td>Email</td> <td>Browser-Based</td> <td>★★★★★</td> <td>Medium</td> <td>Regular</td> </tr> <tr> <td>u2h</td> <td>Social Media</td> <td>Browser-Based</td> <td>★★★★★</td> <td>Elevated</td> <td>Regular</td> </tr> <tr> <td>u2h.Post</td> <td>Social Media</td> <td>Browser-Based</td> <td>★★★★★</td> <td>Elevated</td> <td>Regular</td> </tr> <tr> <td>360.Safeguard.Update</td> <td>Update</td> <td>Client-Server</td> <td>★★★★★</td> <td>Low</td> <td>Regular</td> </tr> <tr> <td>360.Yunpan</td> <td>Storage.Backup</td> <td>Browser-Based.Client-Server</td> <td>★★★★★</td> <td>Medium</td> <td>Regular</td> </tr> <tr> <td>360.Yunpan_File.Download</td> <td>Storage.Backup</td> <td>Browser-Based.Client-Server</td> <td>★★★★★</td> <td>Medium</td> <td>Regular</td> </tr> <tr> <td>360.Yunpan_File.Upload</td> <td>Storage.Backup</td> <td>Browser-Based.Client-Server</td> <td>★★★★★</td> <td>Medium</td> <td>Regular</td> </tr> <tr> <td>360.Yunpan_Login</td> <td>Storage.Backup</td> <td>Browser-Based.Client-Server</td> <td>★★★★★</td> <td>Medium</td> <td>Regular</td> </tr> <tr> <td>3PC</td> <td>Network.Service</td> <td>Network-Protocol</td> <td>★★★★★</td> <td>Elevated</td> <td>Regular</td> </tr> <tr> <td>44shared</td> <td>Storage.Backup</td> <td>Browser-Based.Client-Server</td> <td>★★★★★</td> <td>Medium</td> <td>Regular</td> </tr> <tr> <td>44shared_File.Download</td> <td>Storage.Backup</td> <td>Browser-Based.Client-Server</td> <td>★★★★★</td> <td>Medium</td> <td>Regular</td> </tr> <tr> <td>44shared_File.Upload</td> <td>Storage.Backup</td> <td>Browser-Based.Client-Server</td> <td>★★★★★</td> <td>Medium</td> <td>Regular</td> </tr> </tbody> </table> <p>Version: 23.513 DB: Regular, Industrial Total: 4353</p>	URL	Action	Type	Referrer Host	Status	No record found.					Name	Category	Technology	Popularity	Risk	DB	ic126.Mail	Email	Browser-Based	★★★★★	Medium	Regular	ixoun	Video/Audio	Client-Server	★★★★★	Medium	Regular	lund1.Mail	Email	Browser-Based	★★★★★	Medium	Regular	u2h	Social Media	Browser-Based	★★★★★	Elevated	Regular	u2h.Post	Social Media	Browser-Based	★★★★★	Elevated	Regular	360.Safeguard.Update	Update	Client-Server	★★★★★	Low	Regular	360.Yunpan	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium	Regular	360.Yunpan_File.Download	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium	Regular	360.Yunpan_File.Upload	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium	Regular	360.Yunpan_Login	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium	Regular	3PC	Network.Service	Network-Protocol	★★★★★	Elevated	Regular	44shared	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium	Regular	44shared_File.Download	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium	Regular	44shared_File.Upload	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium
URL	Action	Type	Referrer Host	Status																																																																																																
No record found.																																																																																																				
Name	Category	Technology	Popularity	Risk	DB																																																																																															
ic126.Mail	Email	Browser-Based	★★★★★	Medium	Regular																																																																																															
ixoun	Video/Audio	Client-Server	★★★★★	Medium	Regular																																																																																															
lund1.Mail	Email	Browser-Based	★★★★★	Medium	Regular																																																																																															
u2h	Social Media	Browser-Based	★★★★★	Elevated	Regular																																																																																															
u2h.Post	Social Media	Browser-Based	★★★★★	Elevated	Regular																																																																																															
360.Safeguard.Update	Update	Client-Server	★★★★★	Low	Regular																																																																																															
360.Yunpan	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium	Regular																																																																																															
360.Yunpan_File.Download	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium	Regular																																																																																															
360.Yunpan_File.Upload	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium	Regular																																																																																															
360.Yunpan_Login	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium	Regular																																																																																															
3PC	Network.Service	Network-Protocol	★★★★★	Elevated	Regular																																																																																															
44shared	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium	Regular																																																																																															
44shared_File.Download	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium	Regular																																																																																															
44shared_File.Upload	Storage.Backup	Browser-Based.Client-Server	★★★★★	Medium	Regular																																																																																															

Item de Teste - 5.3.5.5	Possuir controle de regras de aplicações, grupos de aplicações, categorias de aplicações com controle granular para usuários ou grupos de usuários;
Objetivo do Teste	Validar se a solução possui ferramentas de controle de regras de aplicações, grupos de aplicações, categorias de aplicações com controle granular para usuários ou grupos.
Configuração do Teste	Criar regra de segurança.

<p>Procedimento do Teste</p>	<p>Navegando por Security Profile > Application Control > Create New é possível criar um novo perfil enquadrando as aplicações que deseja bloquear, monitorar ou aprovar</p> <p>Navegando por Policy & Objects > Firewall Policy é possível enquadrar o perfil de Application Control criado para determinar em qual fluxo ocorrerá o controle de tráfego por aplicação</p> <p>No campo “Source” da política, podemos realizar o controle de qual grupo ou usuário a regra se enquadra</p> <p>No campo Security Profiles determinamos quais categorias de sites e aplicações o grupo de usuários se enquadra</p>																				
<p>Evidências</p>	<p>1 – Criando Web Filter.</p>  <table border="1" data-bbox="703 853 1054 1122"> <thead> <tr> <th>Name</th> <th>Action</th> </tr> </thead> <tbody> <tr><td>Drug Abuse</td><td>Block</td></tr> <tr><td>Hacking</td><td>Block</td></tr> <tr><td>Illegal or Unethical</td><td>Block</td></tr> <tr><td>Discrimination</td><td>Block</td></tr> <tr><td>Explicit Violence</td><td>Block</td></tr> <tr><td>Extremist Groups</td><td>Block</td></tr> <tr><td>Proxy Avoidance</td><td>Block</td></tr> <tr><td>Plagiarism</td><td>Block</td></tr> <tr><td>Child Sexual Abuse</td><td>Block</td></tr> </tbody> </table>	Name	Action	Drug Abuse	Block	Hacking	Block	Illegal or Unethical	Block	Discrimination	Block	Explicit Violence	Block	Extremist Groups	Block	Proxy Avoidance	Block	Plagiarism	Block	Child Sexual Abuse	Block
Name	Action																				
Drug Abuse	Block																				
Hacking	Block																				
Illegal or Unethical	Block																				
Discrimination	Block																				
Explicit Violence	Block																				
Extremist Groups	Block																				
Proxy Avoidance	Block																				
Plagiarism	Block																				
Child Sexual Abuse	Block																				

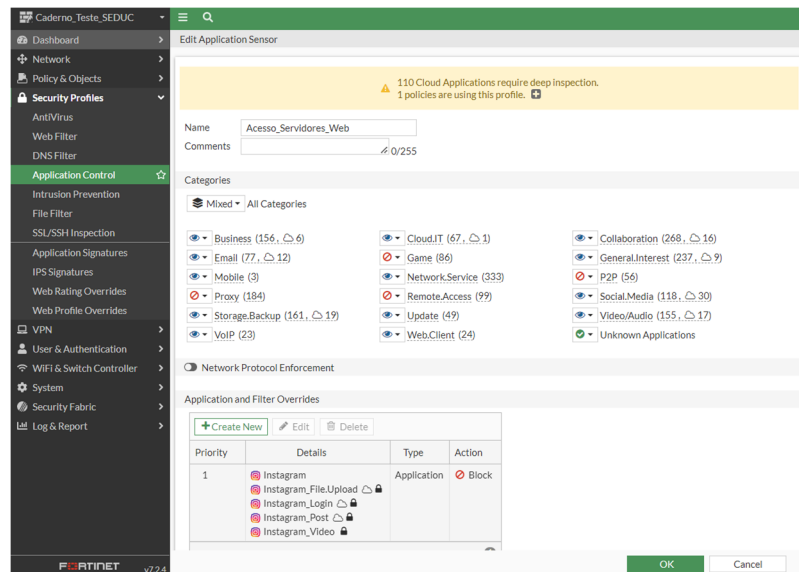
2 Pre-congure niters **Custom** PG-13 Selecionando categorias.

Name	Action
Sports Hunting and War Games	Warning
Bandwidth Consuming 6	
Freeware and Software Downloads	Allow
File Sharing and Storage	Allow
Streaming Media and Download	Monitor
Peer-to-peer File Sharing	Block
Internet Radio and TV	Allow
Internet Telephony	Allow
Security Risk 6	
Malicious Websites	Block

36% 93

Allow users to override blocked categories

3 – Criando Application Control.



The screenshot shows the Fortinet management console for 'Cadastro_Testes_SEDIC'. The left sidebar lists various security features, with 'Application Control' selected. The main panel is titled 'Edit Application Sensor' and shows configuration for a sensor named 'Acesso_Servidores_Web'. A warning message states: '110 Cloud Applications require deep inspection. 1 policies are using this profile.' Below this, there are sections for 'Categories' (showing a grid of application categories like Business, Email, Mobile, etc.), 'Network Protocol Enforcement', and 'Application and Filter Overrides'. The 'Application and Filter Overrides' section contains a table with the following data:

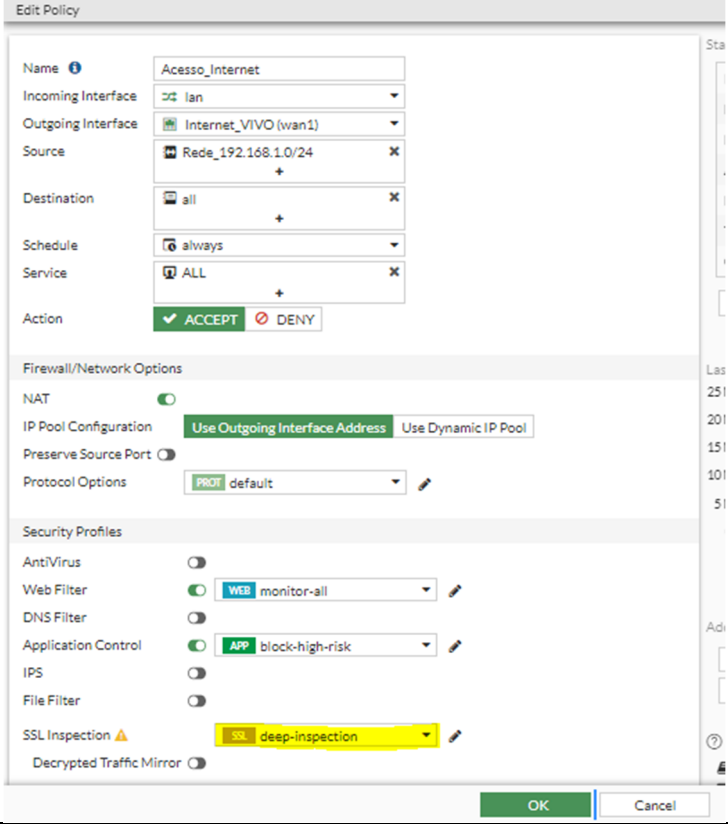
Priority	Details	Type	Action
1	Instagram, Instagram_File.Upload, Instagram_Login, Instagram_Post, Instagram_Video	Application	Block

3 – Definindo grupos e usuários.

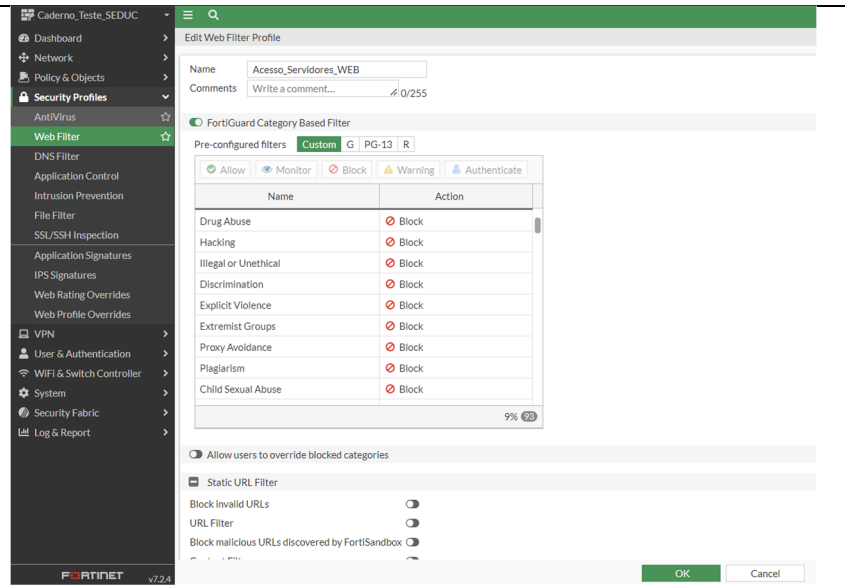
	<div data-bbox="523 320 1326 835"> <p>Edit Policy</p> <p>Name Acesso_Internet_Servidores</p> <p>Incoming Interface lan</p> <p>Outgoing Interface Internet_VIVO (wan1)</p> <p>Source Rede_192.168.1.0/24 flavio GRP_Servidores_Seduc</p> <p>Destination all</p> <p>Schedule always</p> <p>Service HTTP HTTPS</p> <p>Action ACCEPT DENY</p> </div> <p>4 – Definindo Profiles WEB e de Aplicação para política.</p> <div data-bbox="523 936 1326 1283"> <p>Security Profiles</p> <p>AntiVirus AV Acesso_Servidores_WEB</p> <p>Web Filter WEB Acesso_Servidores_WEB</p> <p>DNS Filter</p> <p>Application Control APP Acesso_Servidores_Web</p> <p>IPS</p> <p>File Filter</p> <p>SSL Inspection SSL certificate-inspection</p> </div>
Comentário	

Item de Teste - 5.3.5.6	Deve possibilitar a inspeção de tráfego criptografado HTTPS (Inbound/Outbund);
Objetivo do Teste	Validar se a solução possui ferramentas de inspeção de tráfego criptografado HTTPS (Inbound/Outbund);
Configuração do Teste	1 - Criação da política
Procedimento do Teste	2 – Adicionar perfil de deep-inspection no campo SSL_Inspection da política Para realizar esse teste basta utilizar o Security Profile de deep-inspection, em políticas que deseja inspecionar o fluxo, tais políticas devem estar em modo Proxy.



<p>Evidências</p>	
<p>Comentário</p>	

<p>Item de Teste - 5.3.5.8</p>	<p>A solução deve ser capaz de criar regras com mais de uma categoria;</p>
<p>Objetivo do Teste</p>	<p>Validar se o FortiGate permite a criação de regras com mais de uma categoria</p>
<p>Configuração do Teste</p>	<p>Criar duas regras de acesso com categorização de sites distintas</p>
<p>Procedimento do Teste</p>	<p>Navegando por Security Profiles > Web Filter > Create New é possível criar profiles de Web Filter bloqueando, monitorando, avisando ou aceitando determinadas categorias de sites</p> <p>A categorização acontece por meio da nuvem da Fortinet, porém é possível realizar uma mudança de categoria</p> <p>Navegando por Security Profiles > Application Control > Create New é possível criar profiles de Controle de Aplicação bloqueando, monitorando, avisando ou aceitando determinadas categorias de aplicações</p> <p>Navegando por Policy & Objects > Firewall Policy > Security Profiles é possível adicionar os profiles de segurança</p>
<p>Evidências</p>	<p>1 – Criando Web Filter.</p>



FortiGuard Category Based Filter

Pre-configured filters: Custom G PG-13 R

Name	Action
Drug Abuse	Block
Hacking	Block
Illegal or Unethical	Block
Discrimination	Block
Explicit Violence	Block
Extremist Groups	Block
Proxy Avoidance	Block
Plagiarism	Block
Child Sexual Abuse	Block

9% 83

Allow users to override blocked categories

Static URL Filter

Block Invalid URLs

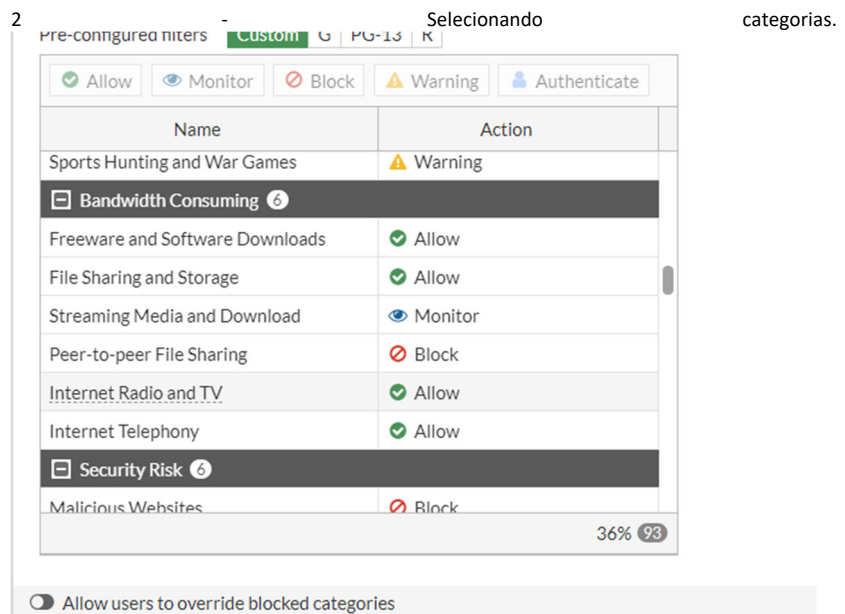
URL Filter

Block malicious URLs discovered by FortiSandbox

OK Cancel

2

Pre-configured filters - Custom G PG-13 R Selecionando categorias.



Pre-configured filters: Custom G PG-13 R

Allow Monitor Block Warning Authenticate

Name	Action
Sports Hunting and War Games	Warning
Bandwidth Consuming 6	
Freeware and Software Downloads	Allow
File Sharing and Storage	Allow
Streaming Media and Download	Monitor
Peer-to-peer File Sharing	Block
Internet Radio and TV	Allow
Internet Telephony	Allow
Security Risk 6	
Malicious Websites	Block

36% 93

Allow users to override blocked categories

3 – Criando Application Control.



Priority	Details	Type	Action
1	Instagram Instagram_File.Upload Instagram_Login Instagram_Post Instagram_Video	Application	Block

4 - Adicionando perfis de segurança em políticas.

Priority	Details	Type	Action
1	Instagram Instagram_File.Upload Instagram_Login Instagram_Post Instagram_Video	Application	Block

Comentário

<https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/615462/url-filter>

<https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/019814/basic-category-filters-and-overrides>

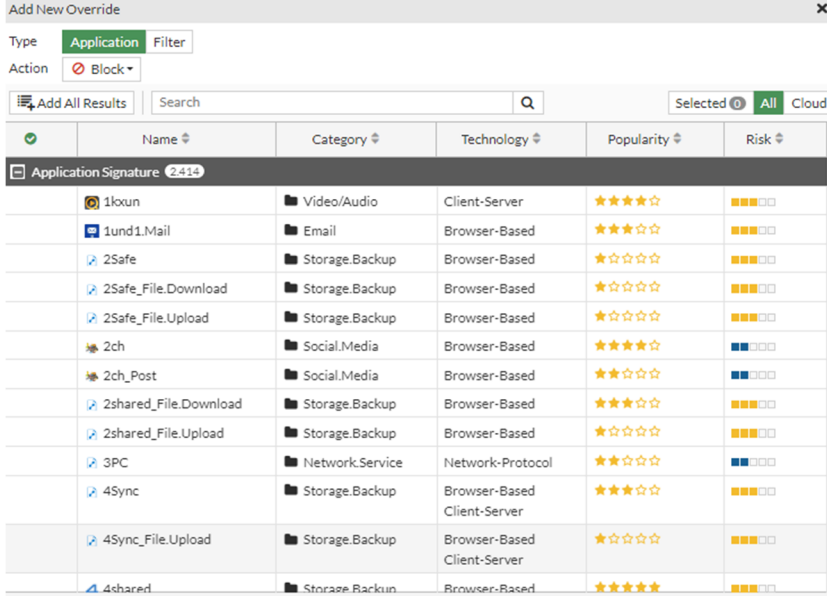
5.3.5.9 Deve possibilitar a permissão ou bloqueio de aplicações ou URLs por pelo menos

os seguintes critérios:

SETOR BANCÁRIO SUL - QUADRA 2 - EDIFÍCIO JOÃO CARLOS SAAD - 8º ANDAR - CEP 70.070-120 - ASA SUL - BRASÍLIA/DF

www.nct.com.br



Item de Teste - 5.3.5.9.1	Aplicação da Web;
Objetivo do Teste	Validar se o Firewall possibilita o bloqueio ou permissão de aplicações da Web
Configuração do Teste	Navegando por Security Profiles > Application Control é possível realizar o bloqueio ou liberação de aplicações web
Procedimento do Teste	Para realizar o teste basta em Security Profiles > Application Control e escolher quais aplicações deseja permitir ou bloquear.
Evidências	 <p>The screenshot shows the 'Add New Override' window in Fortinet's Security Profiles Application Control. It displays a list of applications with columns for Name, Category, Technology, Popularity, and Risk. The list includes applications like 1loxun, 1und1.Mail, 2Safe, 2Safe_File.Download, 2Safe_File.Upload, 2ch, 2ch_Post, 2shared_File.Download, 2shared_File.Upload, 3PC, 4Sync, 4Sync_File.Upload, and 4shared.</p>
Comentário	

Item de Teste - 5.3.5.9.2	Categorias;
Objetivo do Teste	Validar se o Firewall possibilita o bloqueio ou permissão de aplicações web por meio de categorias
Configuração do Teste	<p>Navegando por Security Profiles > Web Filter > Create New é possível criar profiles de Web Filter bloqueando, monitorando, avisando ou aceitando determinadas categorias de sites</p> <p>A categorização acontece por meio da nuvem da fortinet, porém é possível realizar uma mudança de categoria</p> <p>Navegando por Security Profiles > Application Control > Create New é possível criar profiles de Controle de Aplicação bloqueando, monitorando, avisando ou aceitando determinadas categorias de aplicações</p>
Procedimento do Teste	Criar regra de segurança NGFW selecionando categoria de reputação web.



Evidências

The screenshot displays the FortiGate Web Filter configuration page. The left sidebar shows the navigation menu with 'Web Filter' selected. The main area shows the configuration for the profile 'Acesso_Servidores_WEB'. The 'Pre-configured filters' section is set to 'Custom' and shows a list of categories and their actions. Below this, there are sections for 'Bandwidth Consuming' and 'Security Risk' categories.

Name	Action
Drug Abuse	Block
Hacking	Block
Illegal or Unethical	Block
Discrimination	Block
Explicit Violence	Block
Extremist Groups	Block
Proxy Avoidance	Block
Plagiarism	Block
Child Sexual Abuse	Block

Name	Action
Sports Hunting and War Games	Warning
Bandwidth Consuming 6	
Freeware and Software Downloads	Allow
File Sharing and Storage	Allow
Streaming Media and Download	Monitor
Peer-to-peer File Sharing	Block
Internet Radio and TV	Allow
Internet Telephony	Allow
Security Risk 6	
Malicious Websites	Block



<p>Comentário</p>	<p>https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/615462/url-filter</p> <p>https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/019814/basic-category-filters-and-overrides</p>

<p>Item de Teste - 5.3.5.9.3</p>	<p>Nível de risco;</p>
<p>Objetivo do Teste</p>	<p>Validar se o Firewall possibilita o bloqueio ou permissão de aplicações web por meio de nível de risco</p>
<p>Configuração do Teste</p>	<p>Para realizar o controle de aplicações por nível de risco basta entrar no profile de Application Control e utilizar a coluna Risk para filtrar as aplicações.</p>
<p>Procedimento do Teste</p>	<p>Criar regra de segurança NGFW com filtro por risco</p>



<p>Evidências</p>	<p>The screenshot shows a window titled "Add New Override" with a search bar and a table of application signatures. The table has columns for Name, Category, Technology, Popularity (represented by stars), and Risk (represented by colored squares). The first few entries are:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Category</th> <th>Technology</th> <th>Popularity</th> <th>Risk</th> </tr> </thead> <tbody> <tr> <td>1koun</td> <td>Video/Audio</td> <td>Client-Server</td> <td>★★★★☆</td> <td>■■■■□</td> </tr> <tr> <td>1und1.Mail</td> <td>Email</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>■■■■□</td> </tr> <tr> <td>2Safe</td> <td>Storage.Backup</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>■■■■□</td> </tr> <tr> <td>2Safe_File.Download</td> <td>Storage.Backup</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>■■■■□</td> </tr> <tr> <td>2Safe_File.Upload</td> <td>Storage.Backup</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>■■■■□</td> </tr> <tr> <td>2ch</td> <td>Social.Media</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>■■■■□</td> </tr> <tr> <td>2ch_Post</td> <td>Social.Media</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>■■■■□</td> </tr> <tr> <td>2shared_File.Download</td> <td>Storage.Backup</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>■■■■□</td> </tr> <tr> <td>2shared_File.Upload</td> <td>Storage.Backup</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>■■■■□</td> </tr> <tr> <td>3PC</td> <td>Network.Service</td> <td>Network-Protocol</td> <td>★★★★☆</td> <td>■■■■□</td> </tr> <tr> <td>4Sync</td> <td>Storage.Backup</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>■■■■□</td> </tr> <tr> <td>4Sync_File.Upload</td> <td>Storage.Backup</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>■■■■□</td> </tr> <tr> <td>4shared</td> <td>Storage.Backup</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>■■■■□</td> </tr> </tbody> </table>	Name	Category	Technology	Popularity	Risk	1koun	Video/Audio	Client-Server	★★★★☆	■■■■□	1und1.Mail	Email	Browser-Based	★★★★☆	■■■■□	2Safe	Storage.Backup	Browser-Based	★★★★☆	■■■■□	2Safe_File.Download	Storage.Backup	Browser-Based	★★★★☆	■■■■□	2Safe_File.Upload	Storage.Backup	Browser-Based	★★★★☆	■■■■□	2ch	Social.Media	Browser-Based	★★★★☆	■■■■□	2ch_Post	Social.Media	Browser-Based	★★★★☆	■■■■□	2shared_File.Download	Storage.Backup	Browser-Based	★★★★☆	■■■■□	2shared_File.Upload	Storage.Backup	Browser-Based	★★★★☆	■■■■□	3PC	Network.Service	Network-Protocol	★★★★☆	■■■■□	4Sync	Storage.Backup	Browser-Based	★★★★☆	■■■■□	4Sync_File.Upload	Storage.Backup	Browser-Based	★★★★☆	■■■■□	4shared	Storage.Backup	Browser-Based	★★★★☆	■■■■□
Name	Category	Technology	Popularity	Risk																																																																			
1koun	Video/Audio	Client-Server	★★★★☆	■■■■□																																																																			
1und1.Mail	Email	Browser-Based	★★★★☆	■■■■□																																																																			
2Safe	Storage.Backup	Browser-Based	★★★★☆	■■■■□																																																																			
2Safe_File.Download	Storage.Backup	Browser-Based	★★★★☆	■■■■□																																																																			
2Safe_File.Upload	Storage.Backup	Browser-Based	★★★★☆	■■■■□																																																																			
2ch	Social.Media	Browser-Based	★★★★☆	■■■■□																																																																			
2ch_Post	Social.Media	Browser-Based	★★★★☆	■■■■□																																																																			
2shared_File.Download	Storage.Backup	Browser-Based	★★★★☆	■■■■□																																																																			
2shared_File.Upload	Storage.Backup	Browser-Based	★★★★☆	■■■■□																																																																			
3PC	Network.Service	Network-Protocol	★★★★☆	■■■■□																																																																			
4Sync	Storage.Backup	Browser-Based	★★★★☆	■■■■□																																																																			
4Sync_File.Upload	Storage.Backup	Browser-Based	★★★★☆	■■■■□																																																																			
4shared	Storage.Backup	Browser-Based	★★★★☆	■■■■□																																																																			
<p>Comentário</p>																																																																							

<p>Item de Teste - 5.3.5.9.4</p>	<p>IP/Range de IPs/Redes;</p>
<p>Objetivo do Teste</p>	<p>Validar se o equipamento possibilita a permissão ou bloqueio de aplicações ou URLs pelo critério de IP/Range.</p>
<p>Configuração do Teste</p>	<p>Navegando por Security Profiles > Web filter e Application Control é possível criar perfis de segurança.</p>
<p>Procedimento do Teste</p>	<p>1- Criação de um IP Range</p>
	<p>2-Navegando por Policy & Objects > Firewall Policy > Source é possível enquadrar o IP Range criado no campo "Source"</p>
	<p>3- Por último basta enquadrar um perfil de Web Filter ou Application Control na política.</p>
<p>Evidências</p>	<p>The screenshot shows a "New Address" dialog box with the following fields:</p> <ul style="list-style-type: none"> Name: Rede_192.168.1.0/24 Color: Change Type: IP Range IP Range: 192.168.1.1-192.168.1.254 Interface: any Comments: Write a comment... 0/255 <p>Buttons for OK and Cancel are visible at the bottom.</p>



	<p>Edit Policy</p> <p>Name Acesso_Internet_SEDUC</p> <p>Incoming Interface lan</p> <p>Outgoing Interface Internet_VIVO (wan1)</p> <p>Source Rede_192.168.1.0/24</p> <p>Destination all</p> <p>Schedule always</p> <p>Service ALL</p> <p>Action ACCEPT DENY</p> <p>Firewall/Network Options</p> <p>NAT <input checked="" type="checkbox"/></p> <p>IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool</p> <p>Preserve Source Port <input type="checkbox"/></p> <p>Protocol Options default</p> <p>Security Profiles</p> <p>AntiVirus <input type="checkbox"/></p> <p>Web Filter <input checked="" type="checkbox"/> monitor-all</p> <p>DNS Filter <input type="checkbox"/></p> <p>Application Control <input checked="" type="checkbox"/> block-high-risk</p> <p>File Filter <input type="checkbox"/></p> <p>SSL Inspection certificate-inspection</p> <p>Logging Options</p>
Comentário	

Item de Teste - 5.3.5.9.5	Usuários;
Objetivo do Teste	Validar se o equipamento possibilita a permissão ou bloqueio de aplicações ou URLs pelo critério de usuários
Configuração do Teste	Utilizar usuários do FortiGate para realizar o bloqueio ou permissão de aplicações e URLs
Procedimento do Teste	<p>1 - Criação de um novo usuário</p> <p>2 - Navegando por Policy & Objects > Firewall Policy > Source é possível enquadrar o usuário criado no campo "Source"</p> <p>3- Por último basta enquadrar um perfil de Web Filter ou Application Control na política</p>



Evidências

Select Entries ✕

Address **User** Internet Service

🔍 Search + Create

🗄 USER (2)

Local (2)

- 👤 guest
- 👤 rodrigo ✎

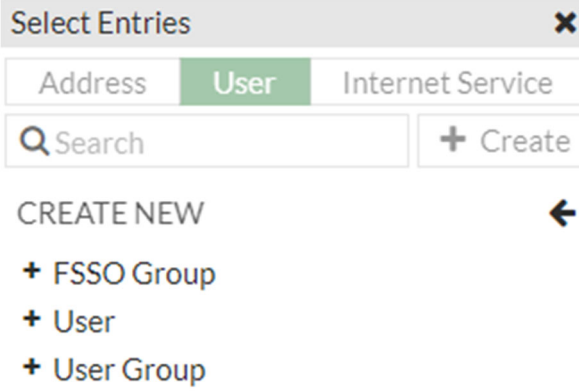
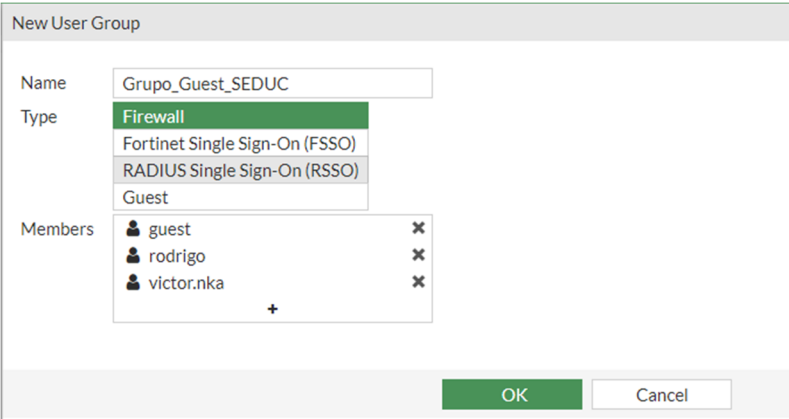
🗄 USER GROUP (2)

- 🗄 Guest-group
- 🗄 SSO_Guest_Users



	<p>Users/Groups Creation Wizard</p> <p> <input checked="" type="checkbox"/> User Type <input checked="" type="checkbox"/> 2 Login Credentials <input type="checkbox"/> 3 Contact Info <input type="checkbox"/> 4 Extra Info </p> <p> Username: victor.nka Password: ●●●●●● </p>
	<p>Edit Policy</p> <p>Name: Acesso_Internet_SEDUC</p> <p>Incoming Interface: lan</p> <p>Outgoing Interface: Internet_VIVO (wan1)</p> <p>Source: Rede_192.168.1.0/24, victor.nka</p> <p>Destination: all</p> <p>Schedule: always</p> <p>Service: ALL</p> <p>Action: <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY</p> <p>Firewall/Network Options</p> <p>NAT: <input checked="" type="checkbox"/></p> <p>IP Pool Configuration: Use Outgoing Interface Address, Use Dynamic IP Pool</p> <p>Preserve Source Port: <input type="checkbox"/></p> <p>Protocol Options: default</p> <p>Security Profiles</p> <p>AntiVirus: <input type="checkbox"/></p> <p>Web Filter: <input checked="" type="checkbox"/> WEB monitor-all</p> <p>DNS Filter: <input type="checkbox"/></p> <p>Application Control: <input checked="" type="checkbox"/> APP block-high-risk</p> <p>File Filter: <input type="checkbox"/></p> <p>SSL Inspection: SSL certificate-inspection</p>
Comentário	

Item de Teste - 5.3.5.9.6	Diferentes grupos de usuários;
Objetivo do Teste	Validar se o equipamento possibilita a permissão ou bloqueio de aplicações ou URLs pelo critério de diferentes grupos de usuários
Configuração do Teste	<p>1 - Criação de um novo grupo de usuários</p> <p>2 - Navegando por Policy & Objects > Firewall Policy > Source é possível enquadrar o grupo criado no campo "Source"</p> <p>3- Por último basta enquadrar um perfil de Web Filter ou Application Control na política</p>

Procedimento do Teste	Criar duas regras NGFW com origem de grupos distintos
Evidências	<p>Criando um novo Grupo</p>  <p>2 – Definindo membros no grupo</p>  <p>3 - Adicionando o Grupo no campo Source e adicionando filtros de Web e Aplicações</p>



	<div style="border: 1px solid #ccc; padding: 5px;"> <p style="text-align: center; margin: 0;">Edit Policy</p> <hr/> <p>Name i <input type="text" value="Acesso_Internet_SEDUC"/></p> <p>Incoming Interface <input type="text" value="lan"/></p> <p>Outgoing Interface <input type="text" value="Internet_VIVO (wan1)"/></p> <p>Source</p> <ul style="list-style-type: none"> <input type="text" value="all"/> ✕ <li style="background-color: #ffff00;"><input type="text" value="Grupo_Guest_SEDUC"/> ✕ <li style="text-align: center;">+ <p>Destination</p> <ul style="list-style-type: none"> <input type="text" value="all"/> ✕ <li style="text-align: center;">+ <p>Schedule <input type="text" value="always"/></p> <p>Service <input type="text" value="ALL"/> ✕ <li style="text-align: center;">+ <p>Action <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY</p> <hr/> <p>Firewall/Network Options</p> <p>NAT <input checked="" type="checkbox"/></p> <p>IP Pool Configuration <input checked="" type="text" value="Use Outgoing Interface Address"/> <input type="text" value="Use Dynamic IP Pool"/></p> <p>Preserve Source Port <input type="checkbox"/></p> <p>Protocol Options <input type="text" value="PROT default"/> ✎</p> <hr/> <p>Security Profiles</p> <p>AntiVirus <input type="checkbox"/></p> <p>Web Filter <input checked="" type="checkbox"/> <input type="text" value="WEB monitor-all"/> ✎</p> <p>DNS Filter <input type="checkbox"/></p> <p>Application Control <input checked="" type="checkbox"/> <input type="text" value="APP block-high-risk"/> ✎</p> <p>IPS <input type="checkbox"/></p> <p>File Filter <input type="checkbox"/></p> <p>SSL Inspection <input type="text" value="SSL certificate-inspection"/> ✎</p> </p></div>
Comentário	

Item de Teste - 5.3.5.10	Aplicações que sejam passíveis a técnicas de evasão por malwares e uso excessivo de banda (EX:ultrasurf, torrent, dropbox e file sharing);
Objetivo do Teste	Validar se o FortiGate consegue bloquear as aplicações passíveis a técnicas de evasão por malwares e uso excessivo de banda.
Configuração do Teste	Criar regra NGFW com filtro anti evasão e uso de banda
Procedimento do Teste	Navegando por Security Profiles > Application Control > Create New é possível criar filtros para aplicações específicas, basta pesquisar o nome das aplicações ou a categoria e indicar que deve ser bloqueado.

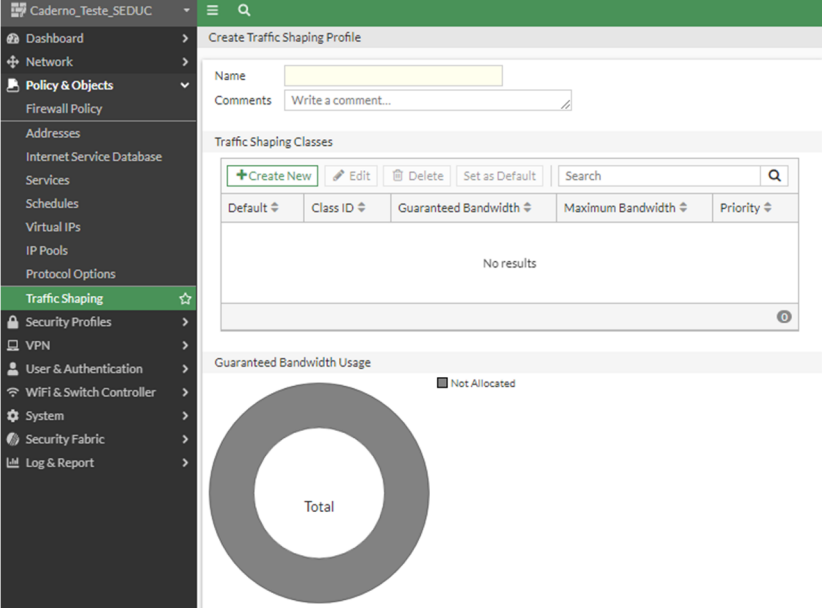
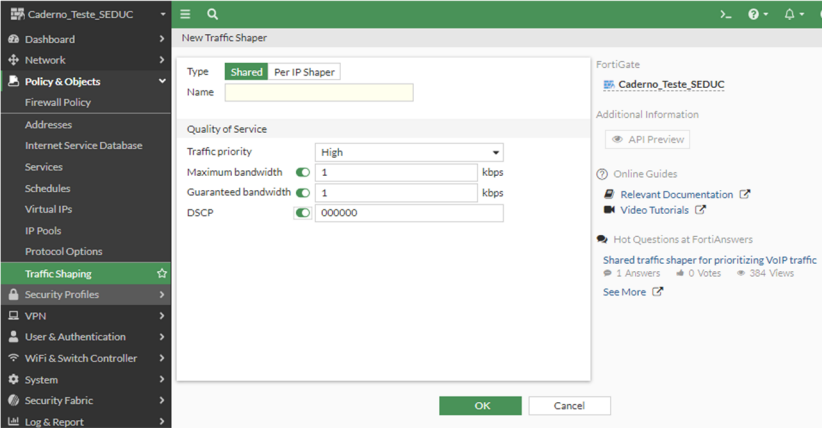


Evidências	<p>Add New Override</p> <p>Type: Application Filter</p> <p>Action: Block</p> <p>Search: ultrasurf</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Category</th> <th>Technology</th> <th>Popularity</th> <th>Risk</th> </tr> </thead> <tbody> <tr> <td colspan="5">Application Signature (2/2414)</td> </tr> <tr> <td>Ultrasurf</td> <td>Proxy</td> <td>Client-Server</td> <td>★★★★★</td> <td>■■■■■</td> </tr> <tr> <td>Ultrasurf_9.6+</td> <td>Proxy</td> <td>Client-Server</td> <td>★★★★★</td> <td>■■■■■</td> </tr> </tbody> </table>	Name	Category	Technology	Popularity	Risk	Application Signature (2/2414)					Ultrasurf	Proxy	Client-Server	★★★★★	■■■■■	Ultrasurf_9.6+	Proxy	Client-Server	★★★★★	■■■■■																																							
	Name	Category	Technology	Popularity	Risk																																																							
	Application Signature (2/2414)																																																											
Ultrasurf	Proxy	Client-Server	★★★★★	■■■■■																																																								
Ultrasurf_9.6+	Proxy	Client-Server	★★★★★	■■■■■																																																								
<p>Add New Override</p> <p>Type: Application Filter</p> <p>Action: Block</p> <p>Search: torrent</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Category</th> <th>Technology</th> <th>Popularity</th> <th>Risk</th> </tr> </thead> <tbody> <tr> <td colspan="5">Application Signature (11/2414)</td> </tr> <tr> <td>ArcticTorrent</td> <td>P2P</td> <td>Peer-to-Peer</td> <td>☆☆☆☆☆</td> <td>■■■■■</td> </tr> <tr> <td>BitTorrent</td> <td>P2P</td> <td>Peer-to-Peer</td> <td>☆☆☆☆☆</td> <td>■■■■■</td> </tr> <tr> <td>BitTorrent.Sync</td> <td>P2P</td> <td>Peer-to-Peer</td> <td>☆☆☆☆☆</td> <td>■■■■■</td> </tr> <tr> <td>Bittorrent.Bleep</td> <td>Collaboration</td> <td>Client-Server</td> <td>☆☆☆☆☆</td> <td>■■■■■</td> </tr> <tr> <td>CTorrent</td> <td>P2P</td> <td>Peer-to-Peer</td> <td>☆☆☆☆☆</td> <td>■■■■■</td> </tr> <tr> <td>ExtraTorrent</td> <td>P2P</td> <td>Peer-to-Peer</td> <td>☆☆☆☆☆</td> <td>■■■■■</td> </tr> <tr> <td>G3.Torrent</td> <td>P2P</td> <td>Peer-to-Peer</td> <td>☆☆☆☆☆</td> <td>■■■■■</td> </tr> <tr> <td>HTTP.Torrent</td> <td>P2P</td> <td>Browser-Based</td> <td>☆☆☆☆☆</td> <td>■■■■■</td> </tr> <tr> <td>Pirate.Bay.Torrent</td> <td>P2P</td> <td>Browser-Based</td> <td>☆☆☆☆☆</td> <td>■■■■■</td> </tr> <tr> <td>TorrentSpy</td> <td>P2P</td> <td>Peer-to-Peer</td> <td>☆☆☆☆☆</td> <td>■■■■■</td> </tr> </tbody> </table>	Name	Category	Technology	Popularity	Risk	Application Signature (11/2414)					ArcticTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	■■■■■	BitTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	■■■■■	BitTorrent.Sync	P2P	Peer-to-Peer	☆☆☆☆☆	■■■■■	Bittorrent.Bleep	Collaboration	Client-Server	☆☆☆☆☆	■■■■■	CTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	■■■■■	ExtraTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	■■■■■	G3.Torrent	P2P	Peer-to-Peer	☆☆☆☆☆	■■■■■	HTTP.Torrent	P2P	Browser-Based	☆☆☆☆☆	■■■■■	Pirate.Bay.Torrent	P2P	Browser-Based	☆☆☆☆☆	■■■■■	TorrentSpy	P2P	Peer-to-Peer	☆☆☆☆☆	■■■■■
Name	Category	Technology	Popularity	Risk																																																								
Application Signature (11/2414)																																																												
ArcticTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	■■■■■																																																								
BitTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	■■■■■																																																								
BitTorrent.Sync	P2P	Peer-to-Peer	☆☆☆☆☆	■■■■■																																																								
Bittorrent.Bleep	Collaboration	Client-Server	☆☆☆☆☆	■■■■■																																																								
CTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	■■■■■																																																								
ExtraTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	■■■■■																																																								
G3.Torrent	P2P	Peer-to-Peer	☆☆☆☆☆	■■■■■																																																								
HTTP.Torrent	P2P	Browser-Based	☆☆☆☆☆	■■■■■																																																								
Pirate.Bay.Torrent	P2P	Browser-Based	☆☆☆☆☆	■■■■■																																																								
TorrentSpy	P2P	Peer-to-Peer	☆☆☆☆☆	■■■■■																																																								
<p>Add New Override</p> <p>Type: Application Filter</p> <p>Action: Block</p> <p>Search: dropbox</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Category</th> <th>Technology</th> <th>Popularity</th> <th>Risk</th> </tr> </thead> <tbody> <tr> <td colspan="5">Application Signature (6/2414)</td> </tr> <tr> <td>Dropbox</td> <td>Storage.Backup</td> <td>Browser-Based</td> <td>★★★★★</td> <td>■■■■■</td> </tr> <tr> <td>Dropbox.Lan.Sync.Discover...</td> <td>Storage.Backup</td> <td>Client-Server</td> <td>★★★★☆</td> <td>■■■■■</td> </tr> <tr> <td>Dropbox_Client.Sync</td> <td>Storage.Backup</td> <td>Client-Server</td> <td>★★★★★</td> <td>■■■■■</td> </tr> <tr> <td>Dropbox_File.Download</td> <td>Storage.Backup</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>■■■■■</td> </tr> <tr> <td>Dropbox_File.Upload</td> <td>Storage.Backup</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>■■■■■</td> </tr> <tr> <td>Dropbox_Login</td> <td>Storage.Backup</td> <td>Browser-Based</td> <td>★★★★☆</td> <td>■■■■■</td> </tr> </tbody> </table>	Name	Category	Technology	Popularity	Risk	Application Signature (6/2414)					Dropbox	Storage.Backup	Browser-Based	★★★★★	■■■■■	Dropbox.Lan.Sync.Discover...	Storage.Backup	Client-Server	★★★★☆	■■■■■	Dropbox_Client.Sync	Storage.Backup	Client-Server	★★★★★	■■■■■	Dropbox_File.Download	Storage.Backup	Browser-Based	★★★★☆	■■■■■	Dropbox_File.Upload	Storage.Backup	Browser-Based	★★★★☆	■■■■■	Dropbox_Login	Storage.Backup	Browser-Based	★★★★☆	■■■■■																				
Name	Category	Technology	Popularity	Risk																																																								
Application Signature (6/2414)																																																												
Dropbox	Storage.Backup	Browser-Based	★★★★★	■■■■■																																																								
Dropbox.Lan.Sync.Discover...	Storage.Backup	Client-Server	★★★★☆	■■■■■																																																								
Dropbox_Client.Sync	Storage.Backup	Client-Server	★★★★★	■■■■■																																																								
Dropbox_File.Download	Storage.Backup	Browser-Based	★★★★☆	■■■■■																																																								
Dropbox_File.Upload	Storage.Backup	Browser-Based	★★★★☆	■■■■■																																																								
Dropbox_Login	Storage.Backup	Browser-Based	★★★★☆	■■■■■																																																								
Comentário																																																												

Item de Teste - 5.3.5.11	Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários ou grupos do AD;
Objetivo do Teste	Validar a criação de traffic shaping baseado no IP de origem, usuários ou grupos do AD.
Configuração do Teste	Criar duas regras contendo em uma a origem de endereço IP e outra com usuário
Procedimento do Teste	1 – Configurar um novo traffic shaper

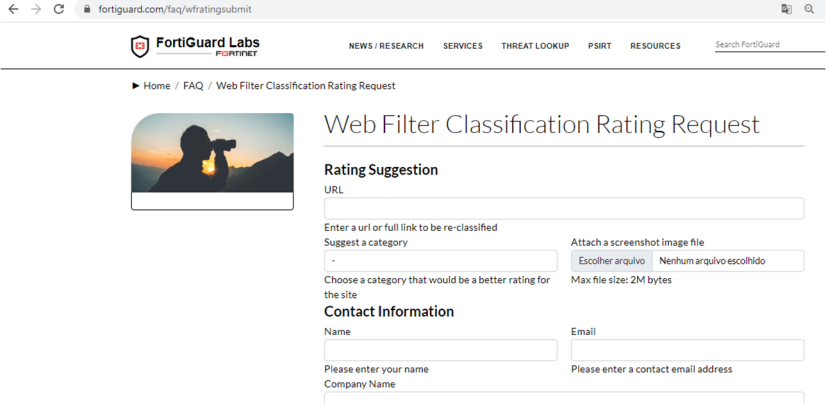
Evidências

The image shows two overlapping configuration windows in Mikrotik WinBox. The top window is titled "New Traffic Shaper" and is set to "Per IP Shaper" type. It includes a "Name" field and a "Quality of Service" section with the following settings: Maximum bandwidth (1 kbps), Max concurrent connections (1), Max concurrent TCP connections (1), Max concurrent UDP connections (1), Forward DSCP (000000), and Reverse DSCP (000000). The bottom window is titled "New Traffic Shaping Policy" and shows a sidebar menu with "Traffic Shaping" selected. The main area of this window includes fields for Name, Status (Enabled), Comments, and a list of matching criteria: Source interface, Outgoing interface, Source, Destination, Schedule, Service, Application, and URL Category. Below these are "Then:" options for "Apply shaper" and "Assign shaping class ID".

<p>Comentário</p>	
	

<p>Item de Teste - 5.3.5.12</p>	<p>A solução deve fornecer uma forma para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;</p>
<p>Objetivo do Teste</p>	<p>Validar se a solução fornece uma forma para solicitação de categorização de URL caso a mesma não esteja categorizada ou categorizada incorretamente</p>
<p>Configuração do Teste</p>	<p>Acessar site de sugestão de recategorização na nuvem de inteligência Fortinet</p>
<p>Procedimento do Teste</p>	<p>Para realizar este procedimento, deve-se abrir o navegador e acessar a página da FortiGuard e ir em "Submit"</p> <p>Ou então acessar o seguinte link: https://www.fortiguard.com/faq/wfratingssubmit</p>
<p>Evidências</p>	



	
Comentário	

Item de Teste - 5.3.5.13	Deve atualizar a base de assinaturas de aplicações automaticamente sem a necessidade de reboot nos gateways e no módulo de gerência;
Objetivo do Teste	Validar se a solução atualiza a base de assinaturas de aplicações automaticamente e sem a necessidade de reboot nos gateways e no módulo de gerência
Configuração do Teste	Demonstrar página de update
Procedimento do Teste	<p>A solução permite realizar de forma automática as atualizações de assinaturas de aplicações, o equipamento não precisa ser reiniciado para aplicar os pacotes baixados da nuvem da Fortinet.</p> <p>Também tem a possibilidade de realizar as atualizações de forma manual, utilizando comandos de cli.</p>
Evidências	
Comentário	



Item de Teste - 5.3.5.14	Deve possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
Objetivo do Teste	Validar se a ferramenta é capaz de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalar um agente no Domain Controller
Configuração do Teste	Demonstrar integração com AD sem instalação de agente
Procedimento do Teste	Para realizar a integração dos serviços do Active Directory com o FortiGate, basta navegar por User and Authentication > LDAP Servers > Create New . A integração não necessita da instalação de nenhum software no Active Directory e nem nas estações dos usuários.
Evidências	