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 - 8° 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

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

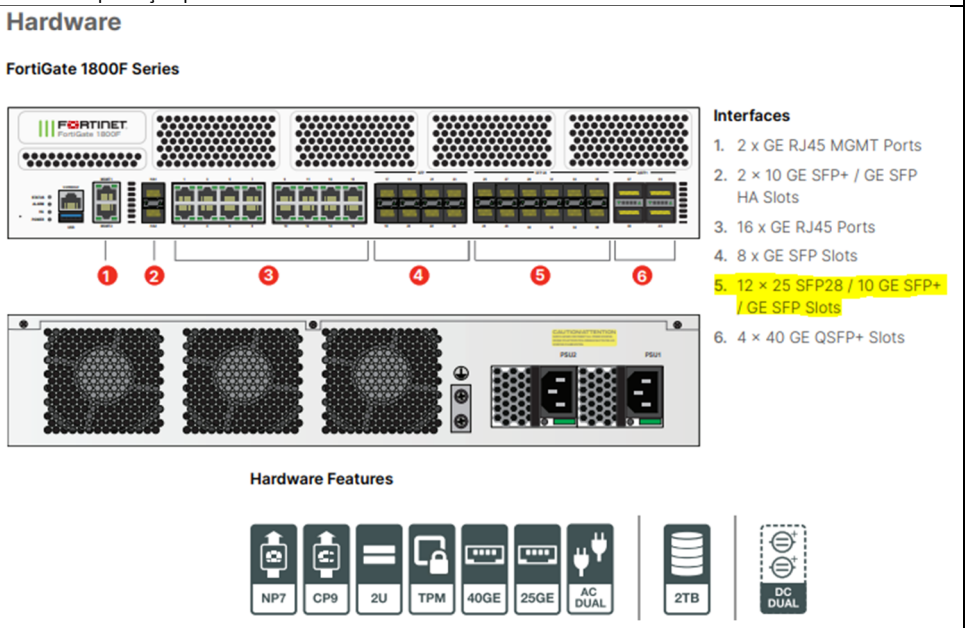
Os testes serão realizados na versão 7.2 do sistema operacional FortiOS.

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.

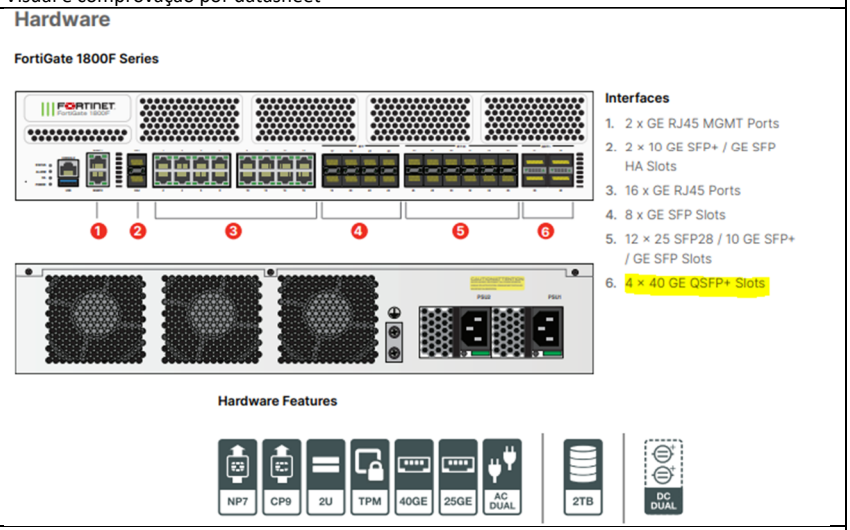
7. ITENS OBRIGATÓRIOS PARA TESTE DE CONFORMIDADE

5.1 Cluster de Firewall Tipo 1

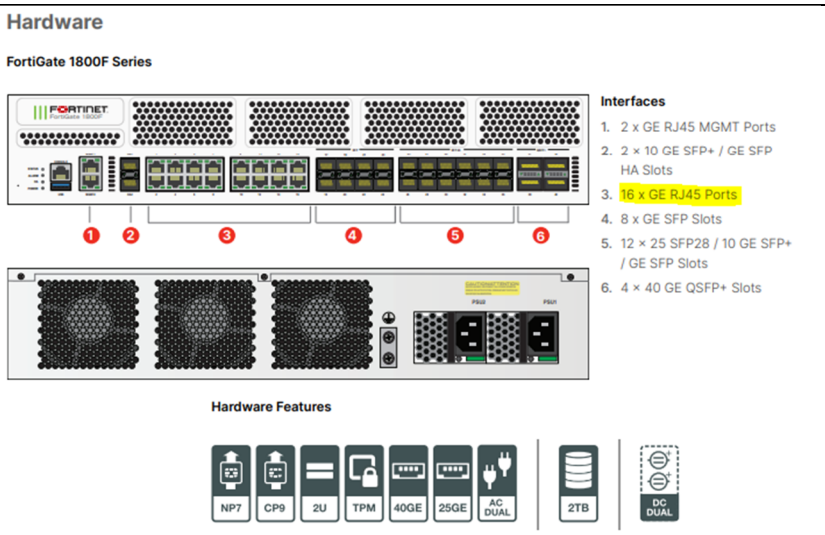
5.1.4 INTERFACES

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	

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	
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	
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	

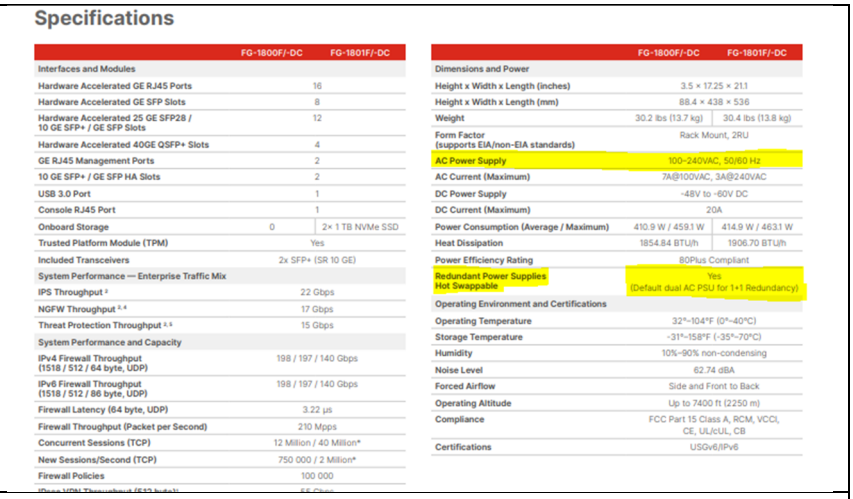
Item de Teste - 5.1.6.2	Permitir no mínimo 4.000.000 (quatro milhões) conexões simultâneas por nó do cluster;
Objetivo do Teste	Validar a capacidade mínima de 4.000.000 de conexões simultâneas por nó do cluster
Configuração do Teste	Teste a ser realizado no laboratório Fortinet. Será apresentado o perfil 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:

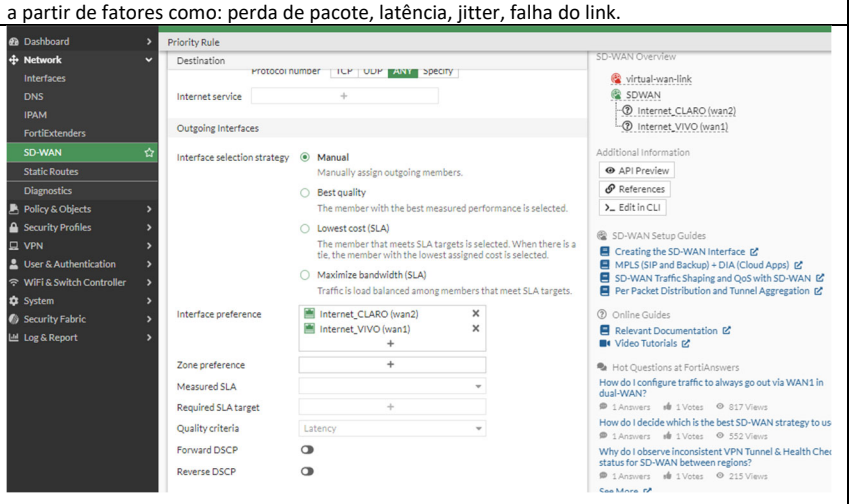
Item de Teste - 5.1.7.1	Possuir unidade de armazenamento interno redundante configurada em RAID-1 de no mínimo 240 GB cada, do tipo memória Flash ou SSD;
Objetivo do Teste	Verificar se o appliance possui armazenamento interno redundante de no mínimo 240 Gb cada em RAID-1
Configuração do Teste	Execução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

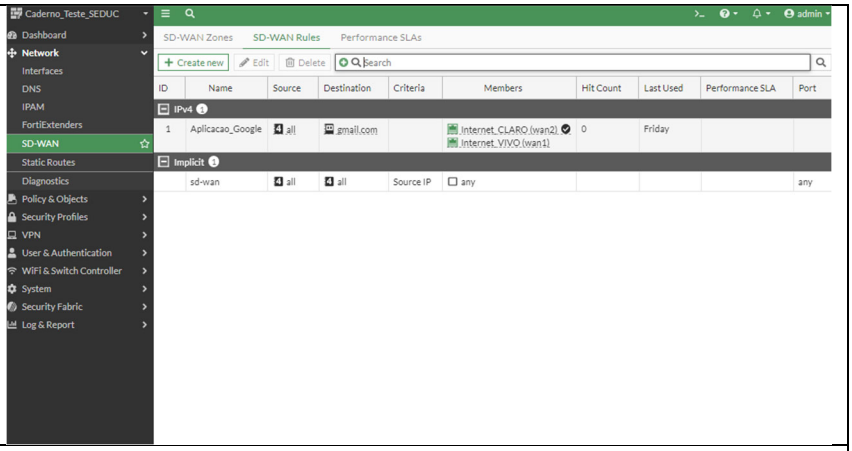
Evidências	**Specifications** |	FG-1800F/-DC	FG-1801F/-DC
---	---	---
Interfaces and Modules		
Hardware Accelerated GE RJ45 Ports		16
Hardware Accelerated GE SFP Slots		8
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots		12
Hardware Accelerated 40GE QSFP+ Slots		4
GE RJ45 Management Ports		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	 Exemplo de saída do comando: To check the RAID status: • RAID enabled: ``` # 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 ```
Comentário	https://docs.fortinet.com/document/FortiGate/6.2.13/cookbook/443180/raid

Item de Teste - 5.1.7.8	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;
Objetivo do Teste	Demonstrar redundância de fontes de energia
Configuração do Teste	Teste físico
Procedimento do Teste	Demonstrar ambas as fontes alimentadas e em operação. 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.
Evidências	

	
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	

	
Comentário	

5.2 Solução de Segurança Tipo 2

5.2.2 INTERFACES

Item de Teste - 5.2.2.1	Possuir no mínimo 08 (oito) interfaces Gigabit RJ45;
Objetivo do Teste	Validar se o equipamento possui no mínimo 8 interfaces Gigabit RJ45
Configuração do Teste	Inspeção visual
Procedimento do Teste	Comprovação visual e por meio do datasheet
Evidências	**Specifications** 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: 1× 128 GB SSD / 1× 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

Item de Teste - 5.2.2.2	Possuir no mínimo 01 (uma) interface console;

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	**Specifications** 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: 1× 128 GB SSD | 1× 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 troughput para Ipsec VPN;
Objetivo do Teste	Validar a capacidade mínima de 1,5 Gbps de troughput 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 *diagnose hardware deviceinfo disk* 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		1× 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:
			`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`

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 possuí 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	**Specifications** |	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 × 8.5 × 7.0	2.4 × 8.5 × 7.0	2.4 × 8.5 × 7.0	2.4 × 8.5 × 7.0
Height x Width x Length (mm)	60 × 216 × 178	60 × 216 × 178	60 × 216 × 178	60 × 216 × 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				

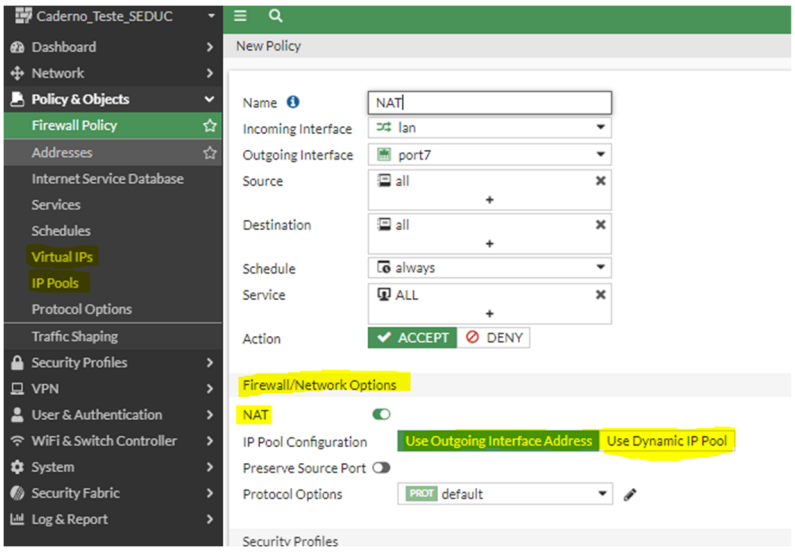
Comentário	Fonte: Acessado em https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-80f-series.pdf

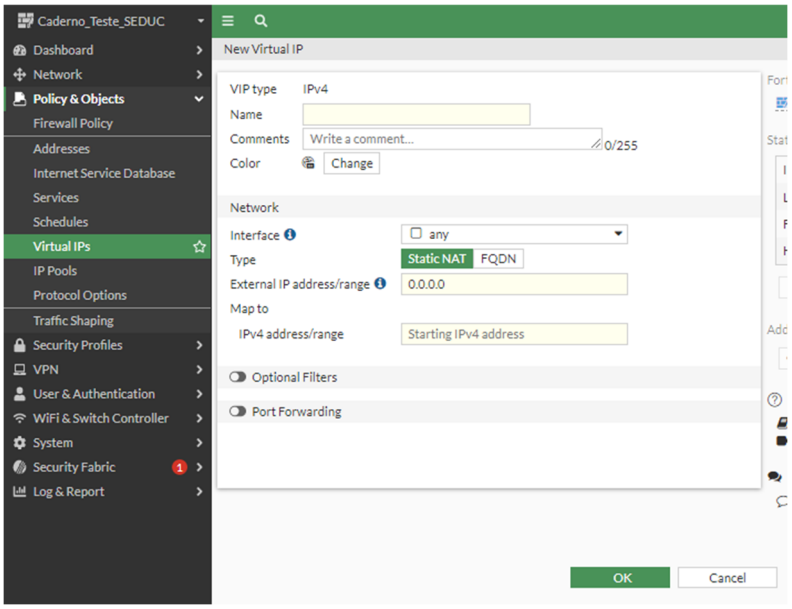
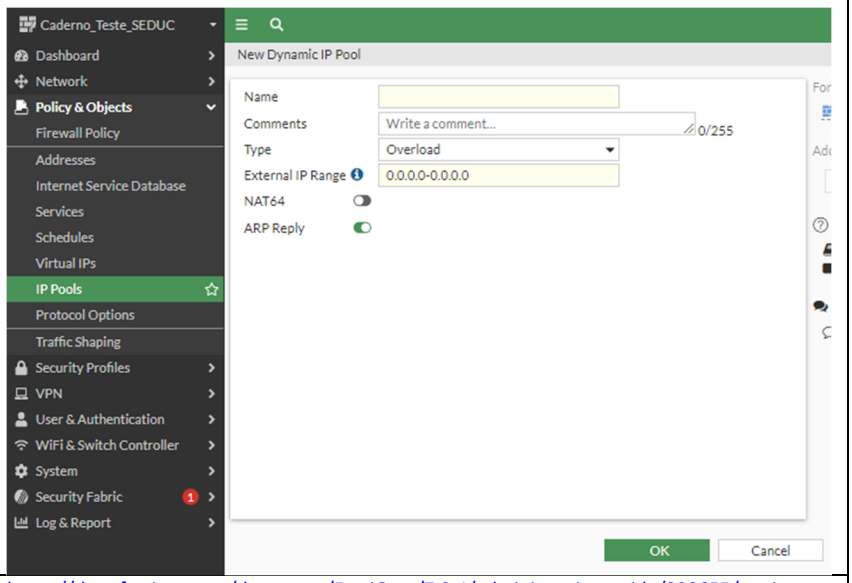
5.3 Funcionalidades gerais para Solução de Segurança Tipo 1, Tipo 2

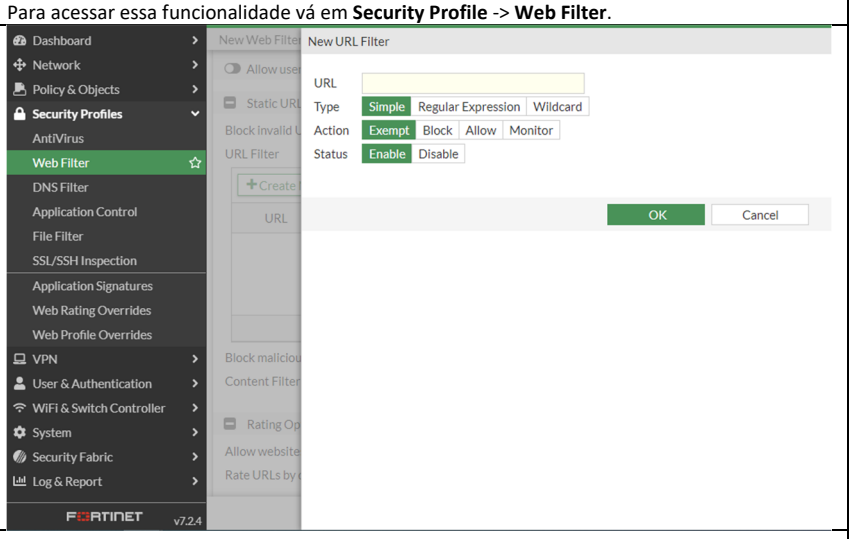
5.3.1 CARACTERISTICAS GERAIS

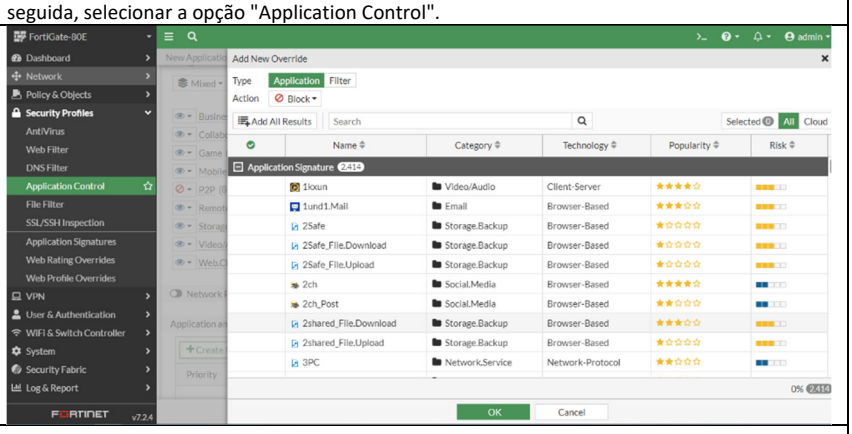
5.3.1.1 Deve implementar:

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

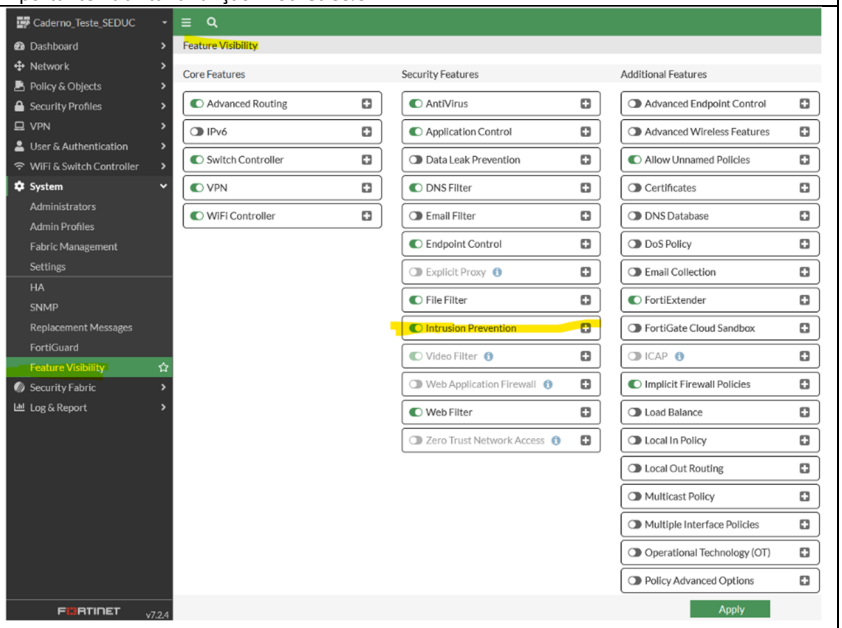
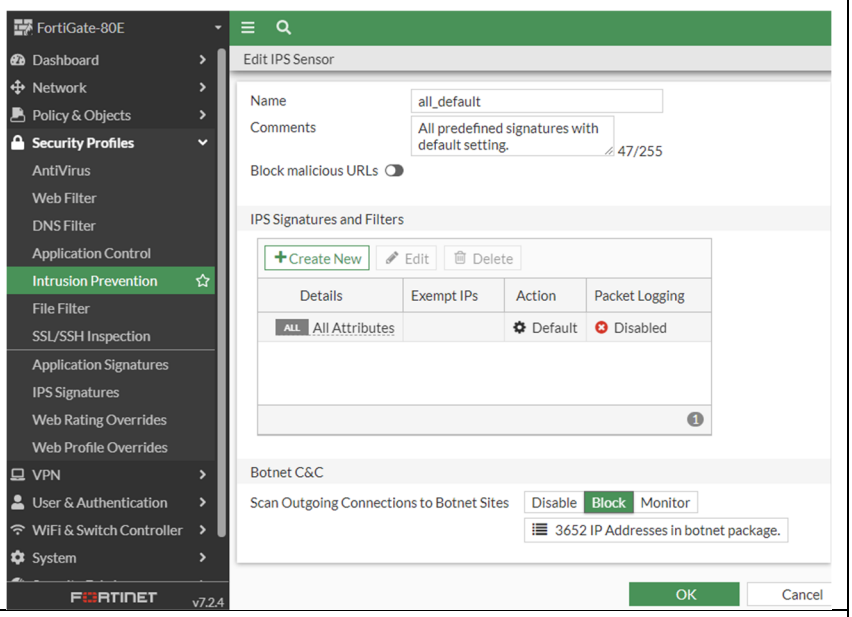
Item de Teste - 5.3.1.1.2	NAT
Objetivo do Teste	Verificar se o Firewall possui a funcionalidade de NAT.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Em Policy & Objects e possível criar o NAT de destino DNAT (VIP) ou uma NAT de origem SNAT (IPPOLL), esses NATs são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

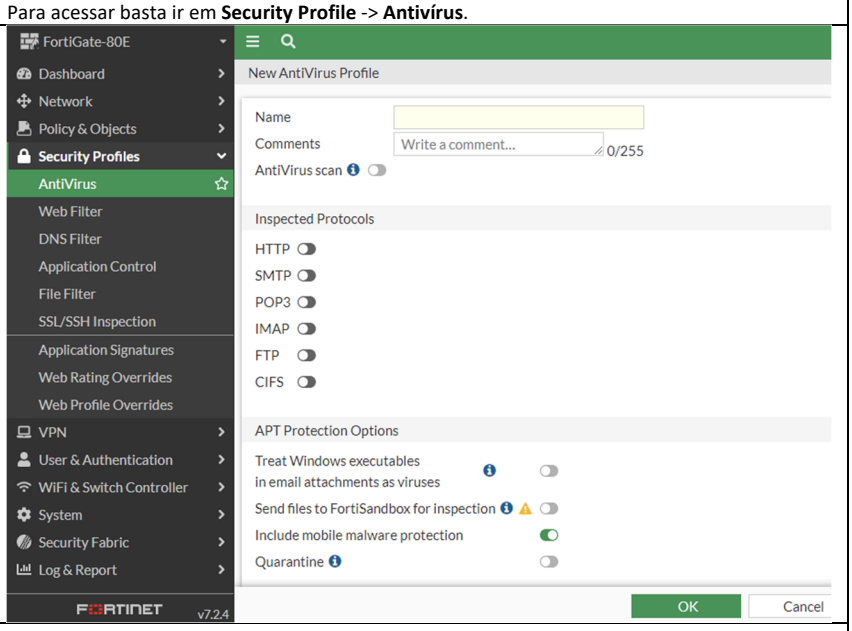
	2 – Virtual IPS  3 – IP Pools 
Comentário	https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/898655/static-snat https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/29961/dynamic-snat https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/728694/destination-nat

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	

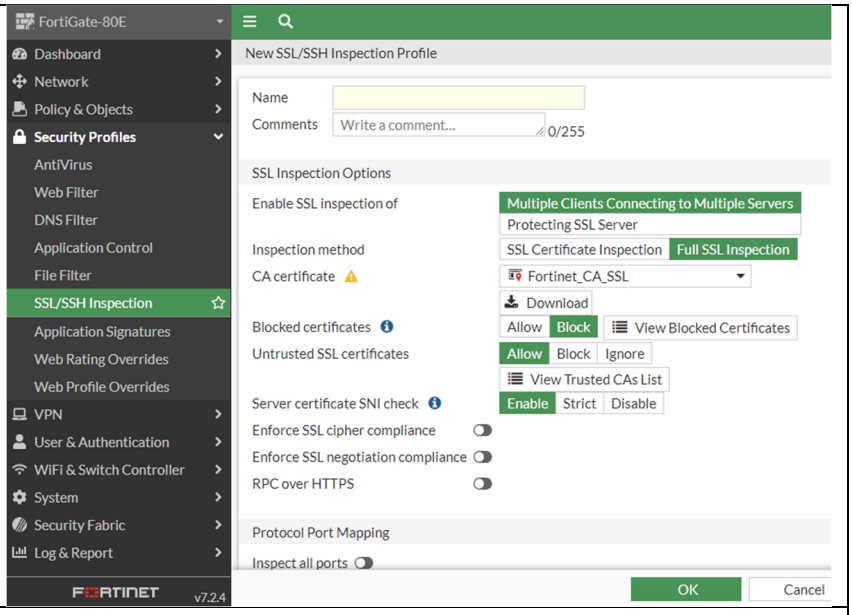
Item de Teste - 5.3.1.1.4	Application Control;
Objetivo do Teste	Demostrar capacidade de executar filtros por Aplicação.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Para ter acesso a essa funcionalidade, é necessário acessar o menu "Security Profile" e, em seguida, selecionar a opção "Application Control".
Evidências	
Comentário	

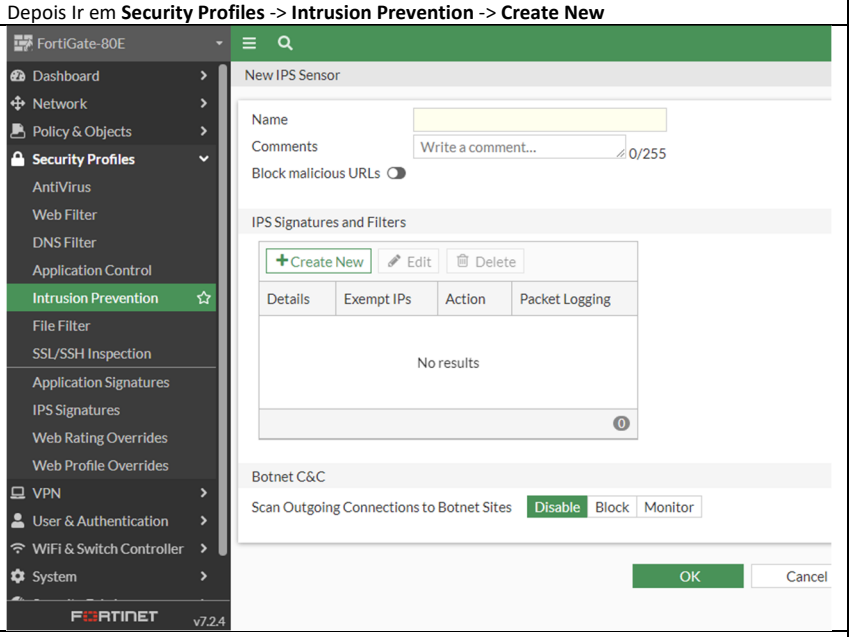
Item de Teste - 5.3.1.1.5	Anti-bot;
Objetivo do Teste	Validar se a solução tem ferramenta Anti-bot de forma nativa
Configuração do Teste	Demonstrar base de regras do FortiGate

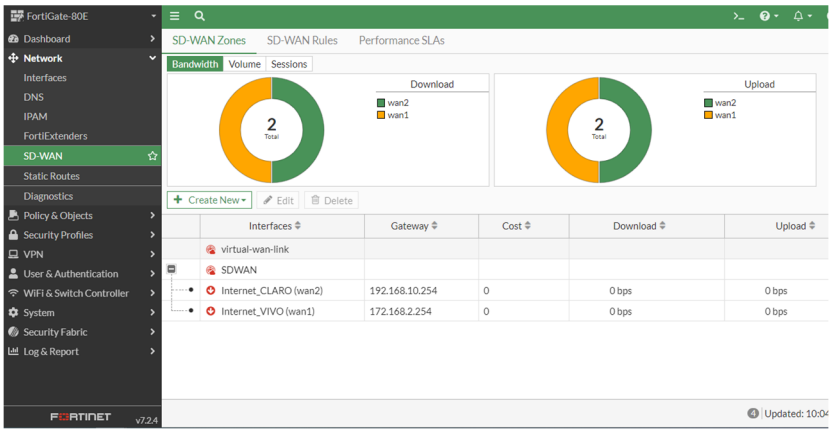
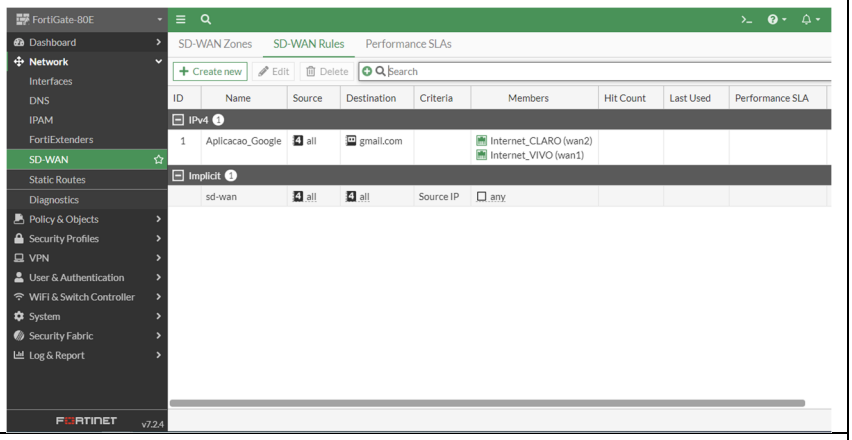
Procedimento do Teste	Para ter acesso a esta funcionalidade, é necessário habilitar a função de Prevenção de Intrusões (IPS) por meio do menu "System" e, em seguida, acessar a opção "Feature Visibility" e habilitar a funcionalidade de IPS. Posteriormente, é necessário criar um sensor de IPS na seção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

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	

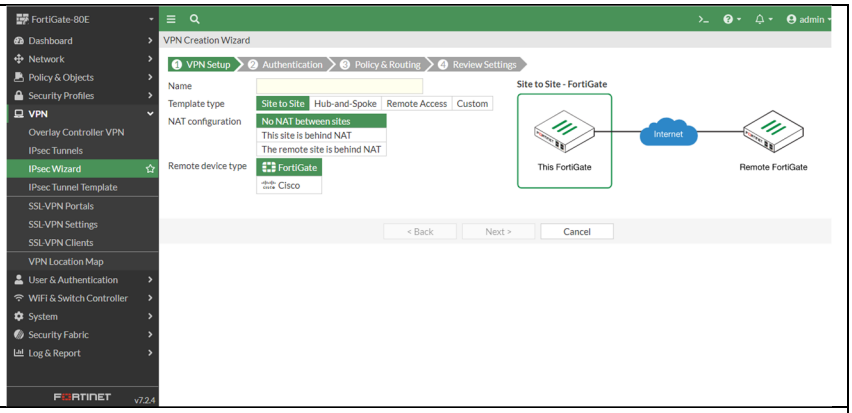
Item de Teste - 5.3.1.1.7	SSL Inspection;
Objetivo do Teste	Validar se o firewall realiza SSL Inspection de forma nativa.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Para acessar basta ir em **Security Profile** -> **SSL/SSH Inspection**.

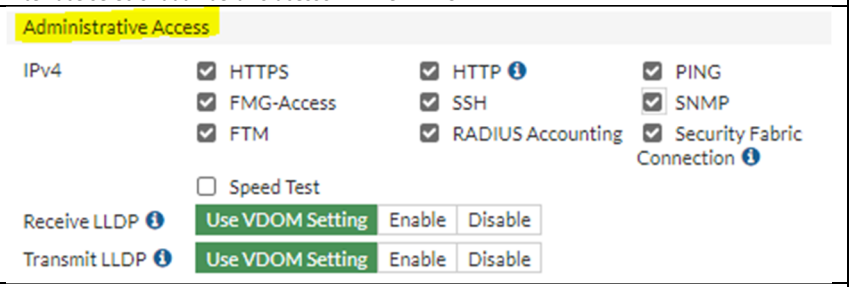
Evidências	
Comentário	

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. Depois Ir em **Security Profiles** -> **Intrusion Prevention** -> **Create New**
Evidências	
Comentário	

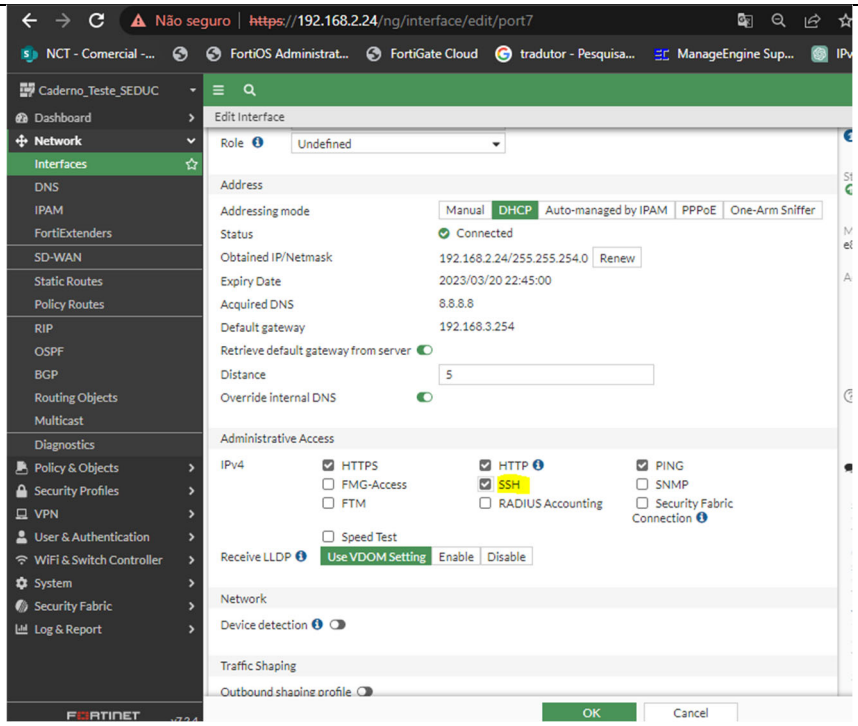
Item de Teste - 5.3.1.1.9	SDWAN;
Objetivo do Teste	Validar se o equipamento possui a funcionalidade de SDWAN.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Navegando por **Network -> SDWAN-** > **Create new member** é possível acrescentar links para serem balanceados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

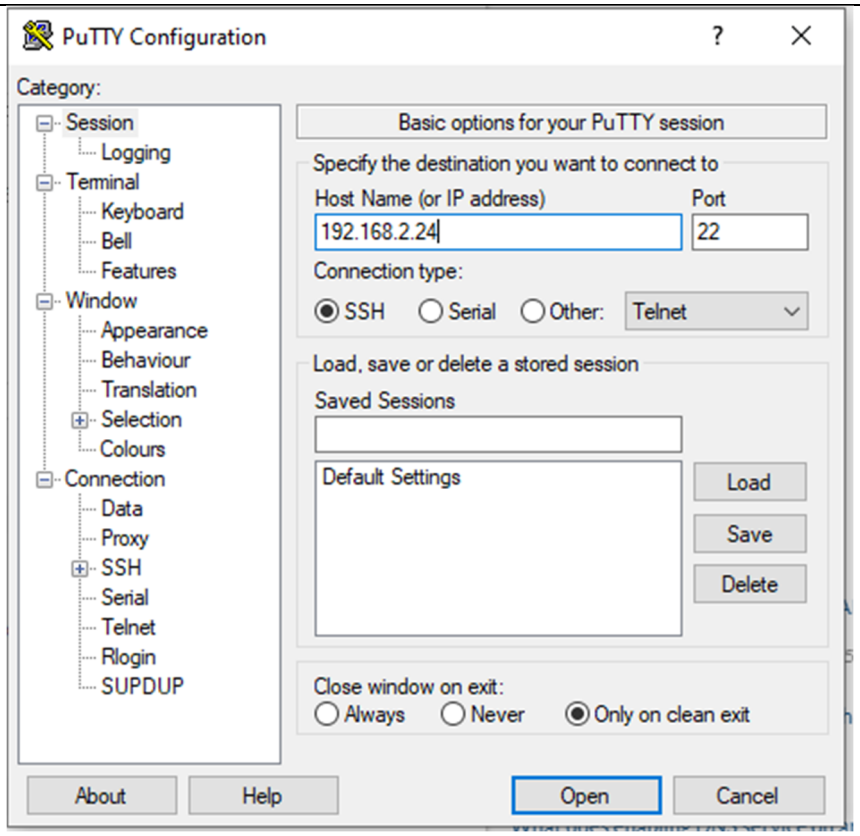
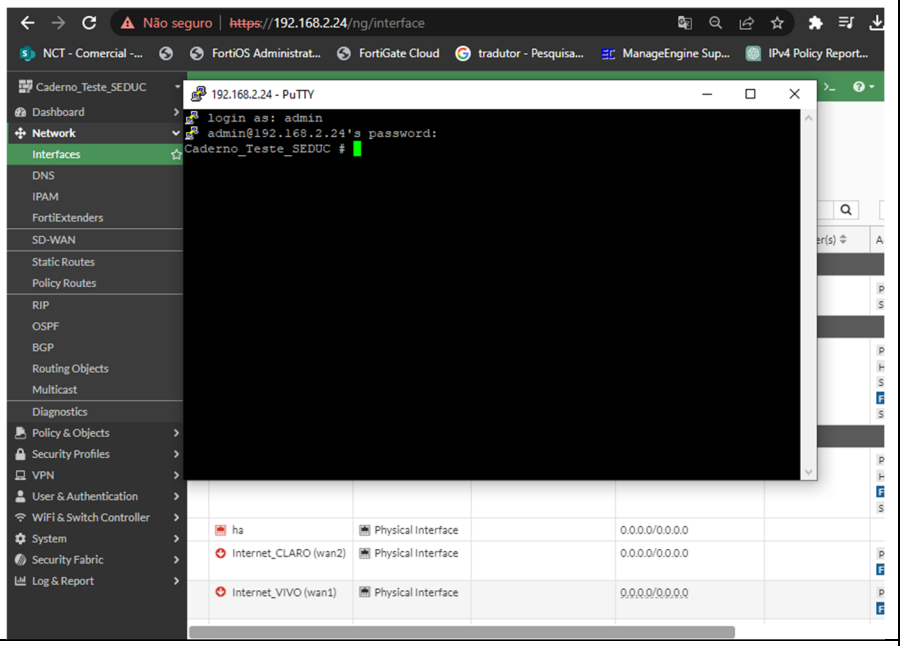
Item de Teste - 5.3.1.1.10	VPN site-to-site;
Objetivo do Teste	Validar se a ferramenta possibilita a criação de VPN site-to-site
Configuração do Teste	Demonstrar base de regras do FortiGate.
Procedimento do Teste	Para acessar basta ir em **VPN** -> **IPSec Tunnels** -> **Create New** -> **IPsec Tunnel**.

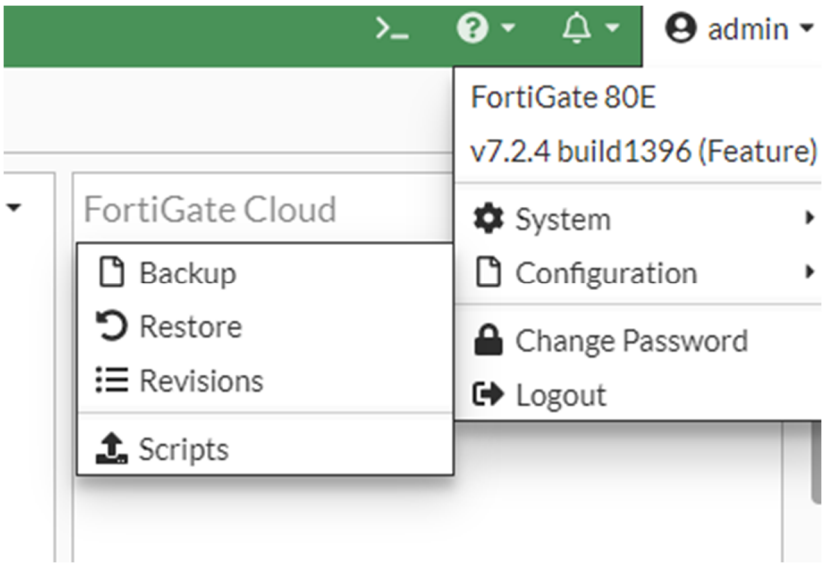
Evidências	
Comentário	

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

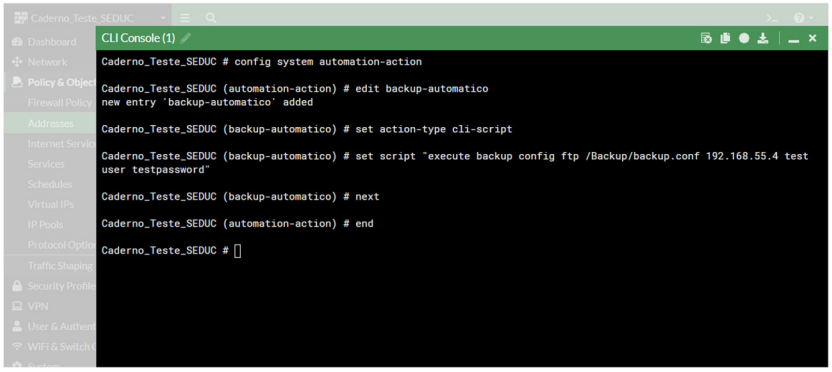
Item de Teste - 5.3.1.6	Implementar interface CLI segura através do protocolo SSH;
Objetivo do Teste	Verificar se o firewall é capaz de implementar interface CLI por meio do protocolo SSH porta 22 para acesso administrativo.
Configuração do Teste	Liberar acesso administrativo seguro SSH na interface 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.
Procedimento do Teste	1 - Liberação do acesso administrativo SSH na interface desejada para acesso administrativo. 2- Realizar o acesso por meio de terminal Putty na função SSH.

Evidências	 Não seguro | https://192.168.2.24/ng/interface/edit/port7 NCT - Comercial -... FortiOS Administrat... FortiGate Cloud tradutor - Pesquisa... ManageEngine Sup... Caderno_Teste_SEDUC Dashboard Network Interfaces DNS IPAM FortiExtenders SD-WAN Static Routes Policy Routes RIP OSPF BGP Routing Objects Multicast Diagnostics Policy & Objects Security Profiles VPN User & Authentication WiFi & Switch Controller System Security Fabric Log & Report Edit Interface Role Undefined Address Addressing mode Manual DHCP Auto-managed by IPAM PPPoE One-Arm Sniffer Status Connected Obtained IP/Netmask 192.168.2.24/255.255.254.0 Renew 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 Distance 5 Override internal DNS Administrative Access IPv4 HTTPS HTTP PING FMG-Access SSH SNMP FTM RADIUS Accounting Security Fabric Connection Speed Test Receive LLDP Use VDOM Setting Enable Disable Network Device detection Traffic Shaping Outbound shaping profile OK Cancel

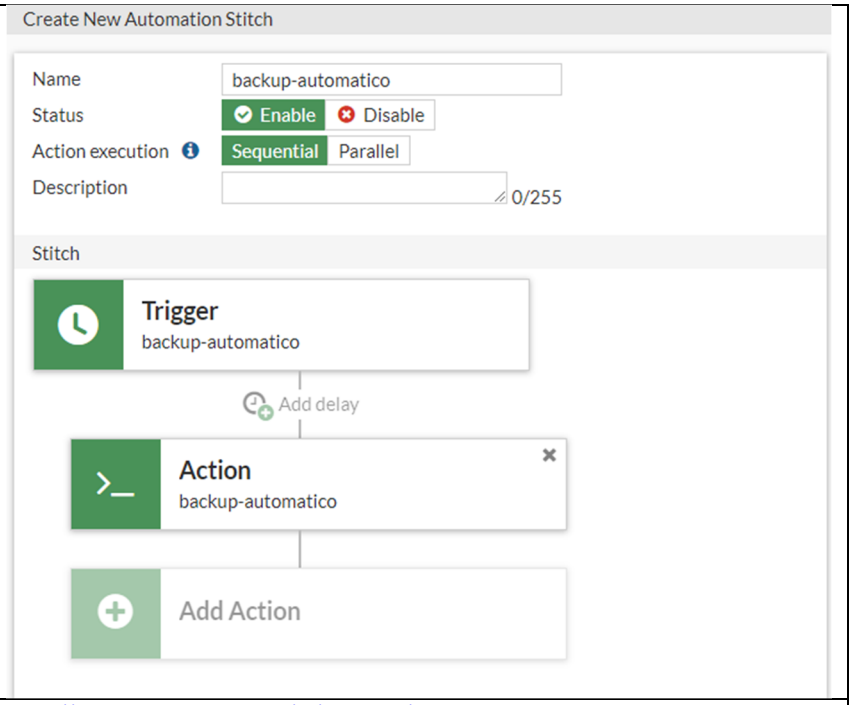
	 
Comentário	

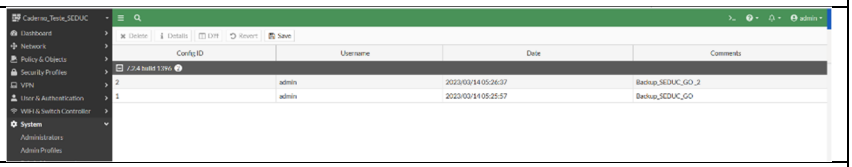
Item de Teste - 5.3.1.9	Deve oferecer as funcionalidades de backup/restore e deve permitir ao administrador agendar backups da configuração em determinado dia e hora;
Objetivo do Teste	Verificar se o FortiGate é capaz de realizar backup/restore e se é possível realizar de forma agendada.
Configuração 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	

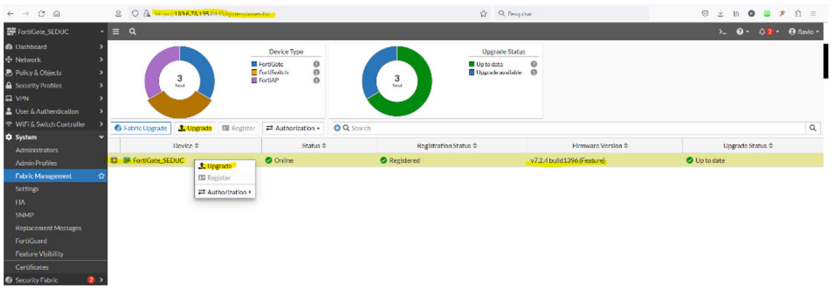
```
FortiGate-80E (automation-trigger) # end

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 #
```



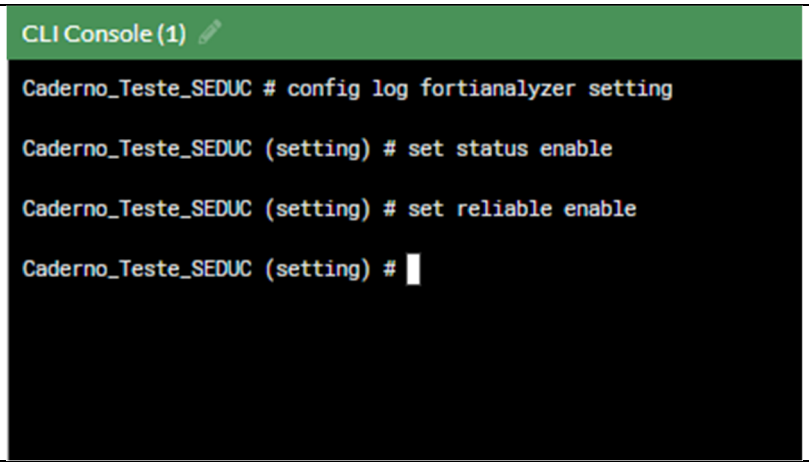

```
config system automation-stitch
    edit "backup-automatico"
        set trigger "backup-automatico"
        config actions
            edit 1
                set action "backup-automatico"
                set required enable
            next
        end
    next
end
```

	
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	Demostrar 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	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" 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; # execute backup config ftp <backup_filename> <ftp_server>[<:ftp_port>] [<user_name>] [<password>] [<backup_password>]
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	Demostrar 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	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. 
Comentário	Fonte: https://docs.fortinet.com/document/FortiGate/7.2.3/administration-guide/596131

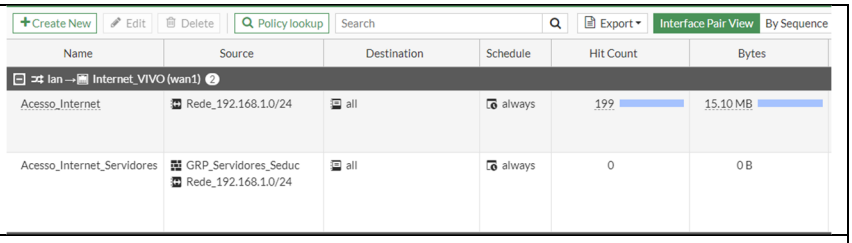
Item de Teste - 5.3.1.14	A solução deve permitir que em caso de falha da comunicação entre o appliance de segurança e a solução de armazenamento de logs seja possível a retenção temporária dos logs localmente no appliance de segurança;
Objetivo do Teste	Verificar se a solução é capaz de armazenar logs 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 “Realiable” no FortiGate. Tal funcionalidade fica dentro de: config log fortianalyzer setting
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.

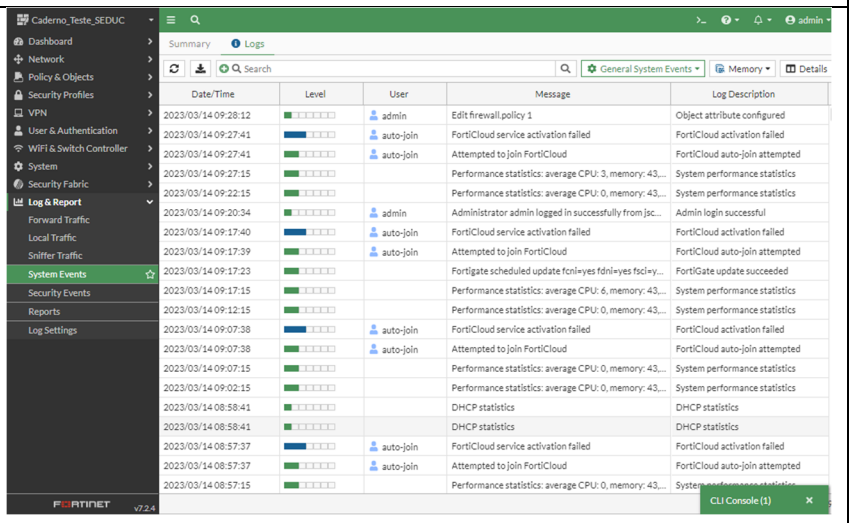
	
Comentário	https://docs.fortinet.com/document/FortiGate/7.2.0/new-features/942202/improve-fortianalyzer-log-caching

5.3.2 POLÍTICAS DE FIREWALL

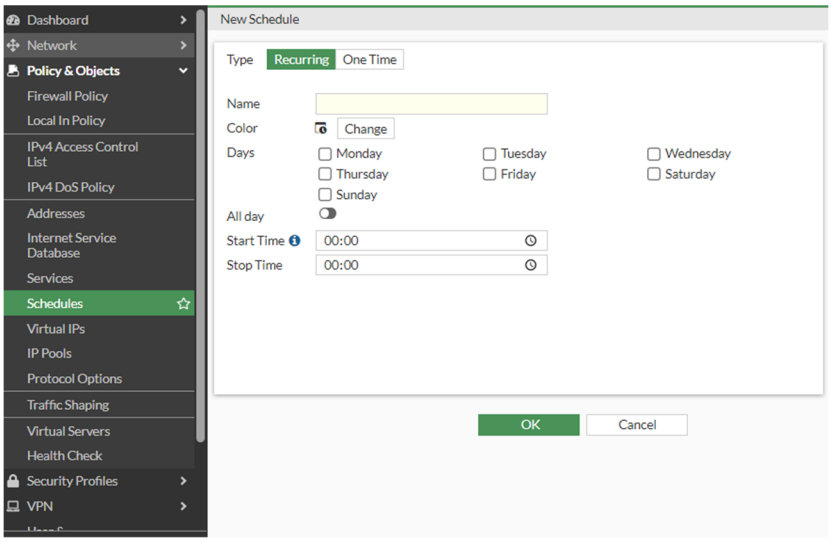
Item de Teste - 5.3.2.18	Deve inspecionar e bloquear os dados operando como default gateway das redes protegidas e controlar o tráfego em nível de aplicações;
Objetivo do Teste	Demonstrar base de regras do FortiGate
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Demonstrar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

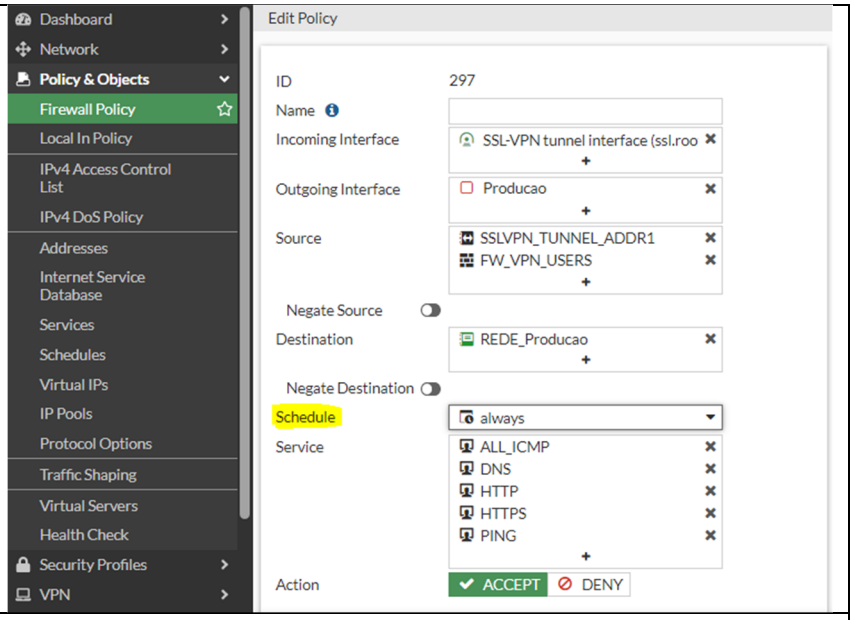
Item de Teste - 5.3.2.20	A solução de Firewall, deve ser capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização;
Objetivo do Teste	Verificar se a solução de firewall é capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	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. Dentre esses dados, destaca-se o "Hit Count", que consiste em uma contagem de quantas vezes determinada regra foi utilizada.
Evidências	

	
Comentário	

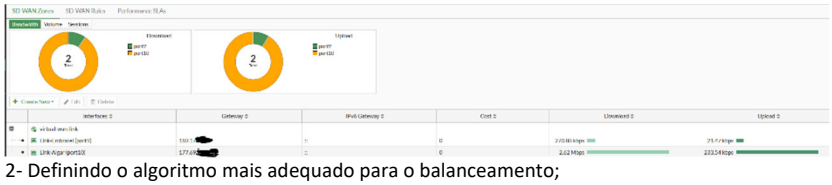
Item de Teste - 5.3.2.21	Toda alteração de políticas e definições na console de gerenciamento deverá ser registrada e passível de auditoria;
Objetivo do Teste	Validar se a ferramenta faz o registro de todas as alterações feitas em regras e configurações, sendo passível de auditoria.
Configuração do Teste	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	
Comentário	

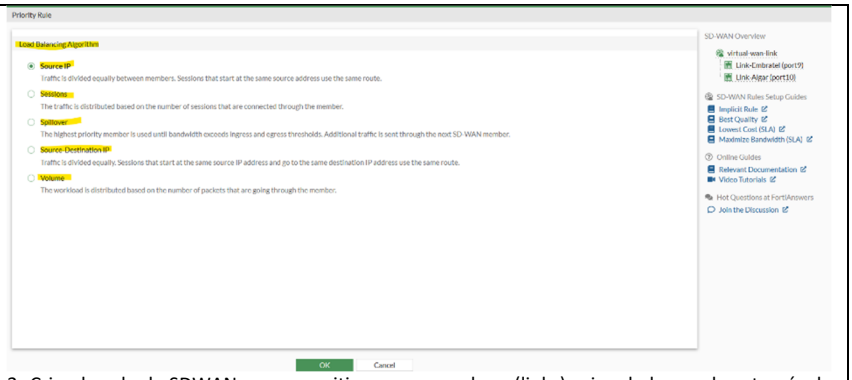
Item de Teste - 5.3.2.23	Deverá permitir a ativação/desativação de regras de forma programada conforme a data/hora;
Objetivo do Teste	Validar se o FortiGate permite a ativação e desativação de regras de forma programada.
Configuração do Teste	Demonstrar base de regras do FortiGate

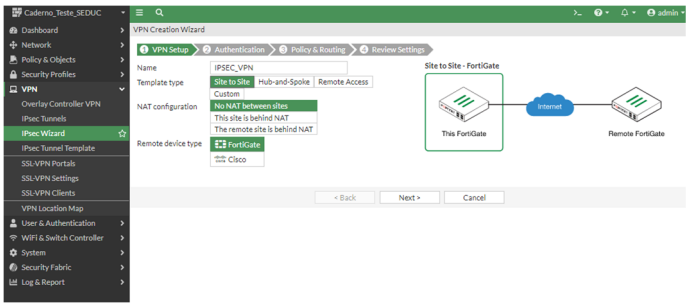
Procedimento do Teste	1 - Navegando por **Policy & Objects** > **Firewall Policy** > **Schedules** é possível criar um período que a regra irá funcionar. 2 - Navegando por **Policy & Objects** > **Firewall Policy** > é possível adicionar o objeto de Schedule criado anteriormente em qualquer uma das políticas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

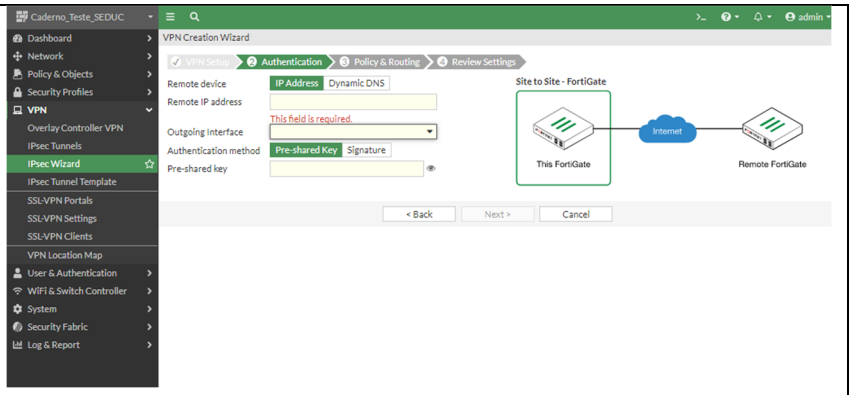
	
Comentário	

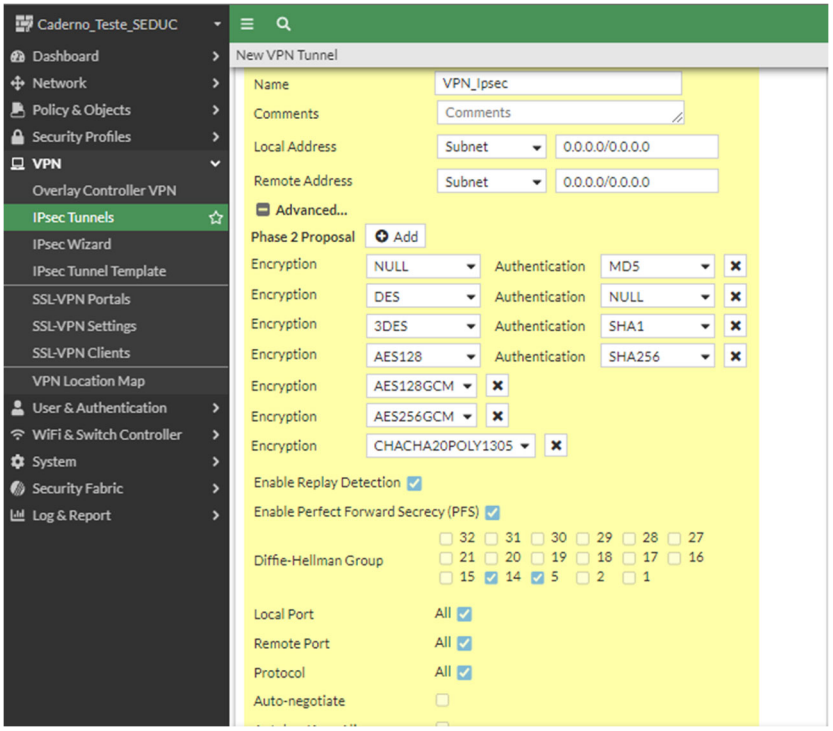
5.3.3 SDWAN

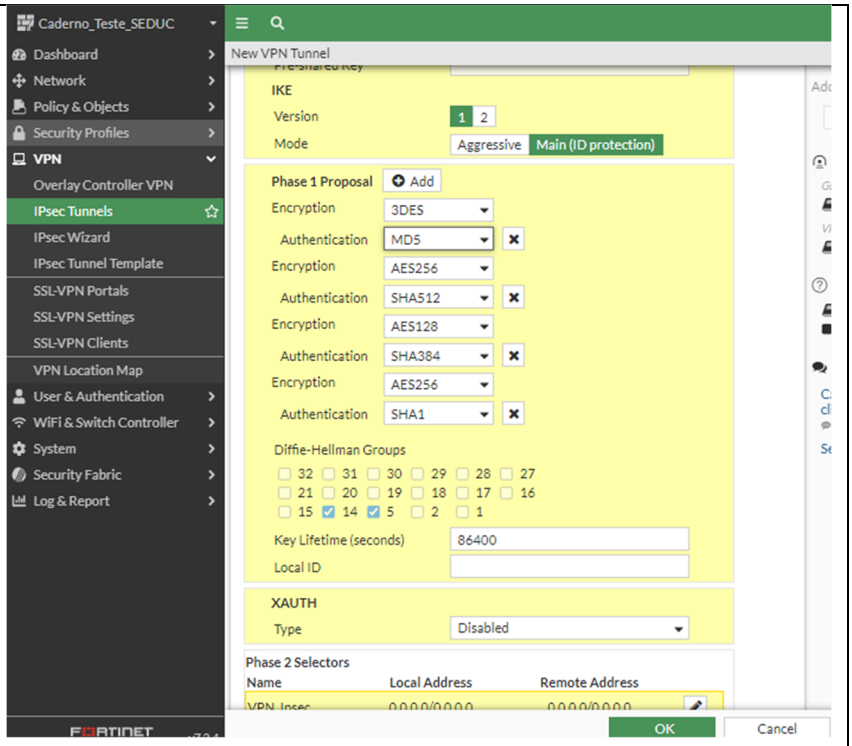
Item de Teste - 5.3.3.2	A solução deverá ser capaz de balancear cargas entre dois links distintos;
Objetivo do Teste	Demostrar capacidade de balancear o tráfego de 2 links distintos através de SDWAN
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Navegando por **Network**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

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

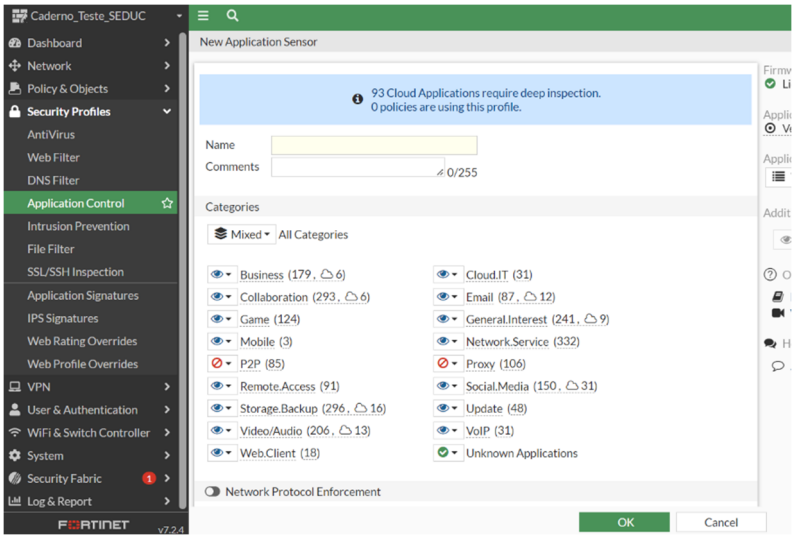
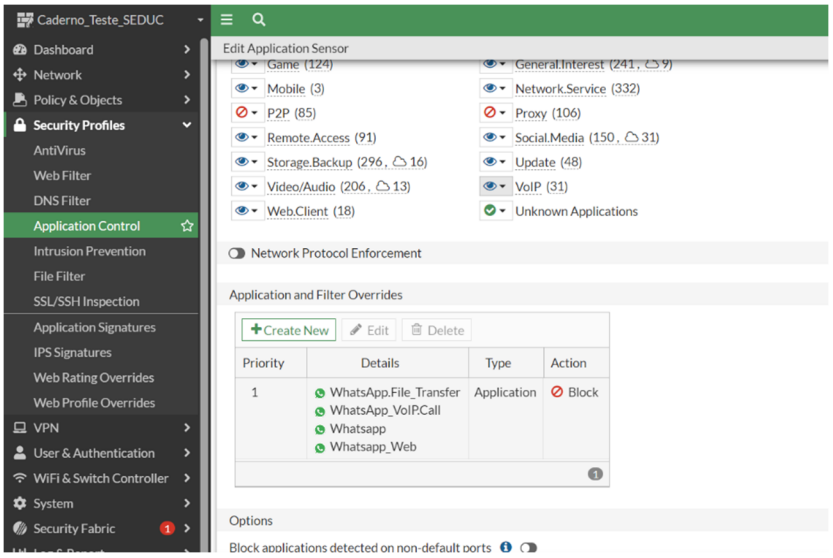
Item de Teste - 5.3.3.3	Deverá implementar a criação de tuneis criptografados de forma dinâmica entre os sites;
Objetivo do Teste	Validar se o FortiGate permite a criação de tuneis IPsecVPN de forma dinâmica e criptografado, site-to-site.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento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

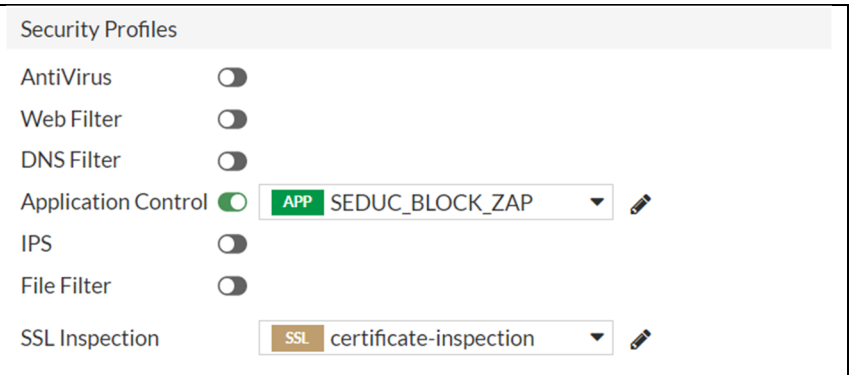
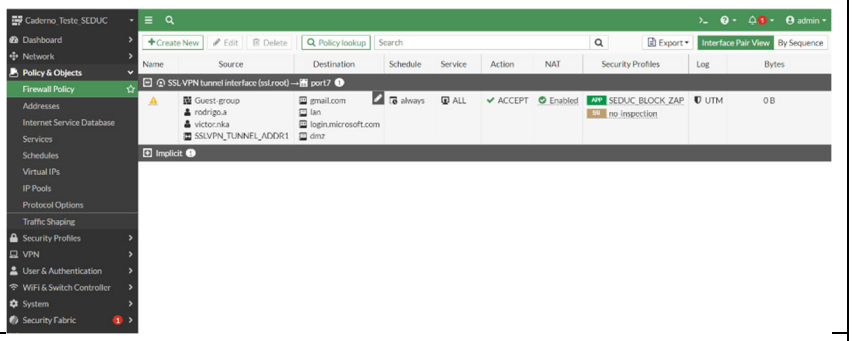

Caderno_Teste_SEDUC
admin
Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication
WiFi & Switch Controller
System
Security Fabric
Log & Report
VPN Creation Wizard
VPN Setup
2 Authentication
3 Policy & Routing
4 Review Settings
Remote device
IP Address
Dynamic DNS
Remote IP address
This field is required.
Outgoing Interface
Authentication method
Pre-shared Key
Signature
Pre-shared key
Site to Site - FortiGate
This FortiGate
Internet
Remote FortiGate
< Back
Next >
Cancel


Caderno_Teste_SEDUC
Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication
WiFi & Switch Controller
System
Security Fabric
Log & Report
New VPN Tunnel
Name
VPN_Ipsec
Comments
Comments
Local Address
Subnet
0.0.0.0/0.0.0.0
Remote Address
Subnet
0.0.0.0/0.0.0.0
Advanced...
Phase 2 Proposal
Add
Encryption
NULL
Authentication
MD5
Encryption
DES
Authentication
NULL
Encryption
3DES
Authentication
SHA1
Encryption
AES128
Authentication
SHA256
Encryption
AES128GCM
Encryption
AES256GCM
Encryption
CHACHA20POLY1305
Enable Replay Detection
Enable Perfect Forward Secrecy (PFS)
Diffie-Hellman Group
32 31 30 29 28 27
21 20 19 18 17 16
15 14 5 2 1
Local Port
All
Remote Port
All
Protocol
All
Auto-negotiate

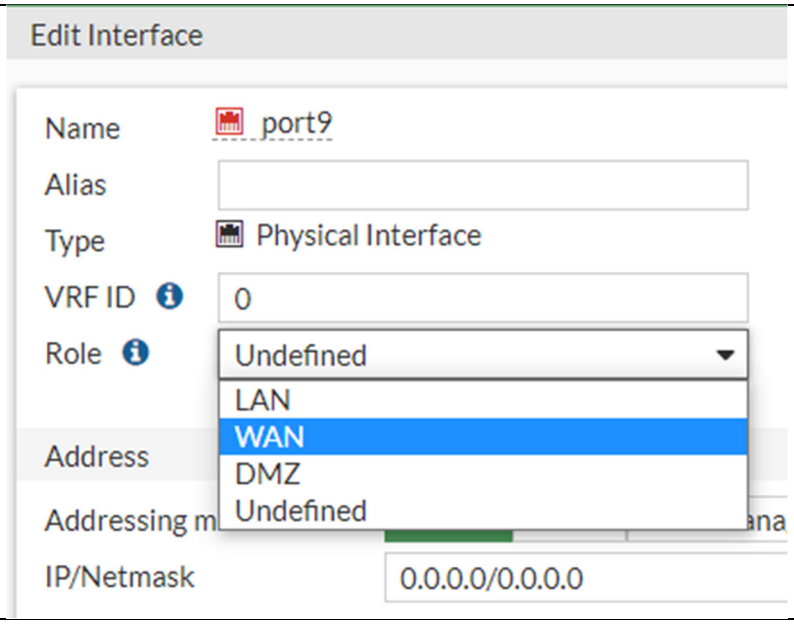
	 ADVPN Auto-Discovery VPN (ADVPN) allows the central hub to dynamically inform spokes about a better path for traffic between two spokes. The following topics provide instructions on configuring ADVPN: • IPsec VPN wizard hub-and-spoke ADVPN support • ADVPN with BGP as the routing protocol • ADVPN with OSPF as the routing protocol • ADVPN with RIP as the routing protocol • UDP hole punching for spokes behind NAT
Comentário	Fonte: Acessado em https://docs.fortinet.com/document/FortiGate/7.2.0/administration-guide/978793

Item de Teste - 5.3.3.5	Deverá implementar controle de tráfego por aplicação;
Objetivo do Teste	Validar se o FortiGate é capaz de realizar controle de tráfego por aplicação
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	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; Navegando por **Security Profile** > **Application Control** > **Create new** é possível criar um novo perfil enquadrando as aplicações que deseja bloquear, monitorar ou aprovar;

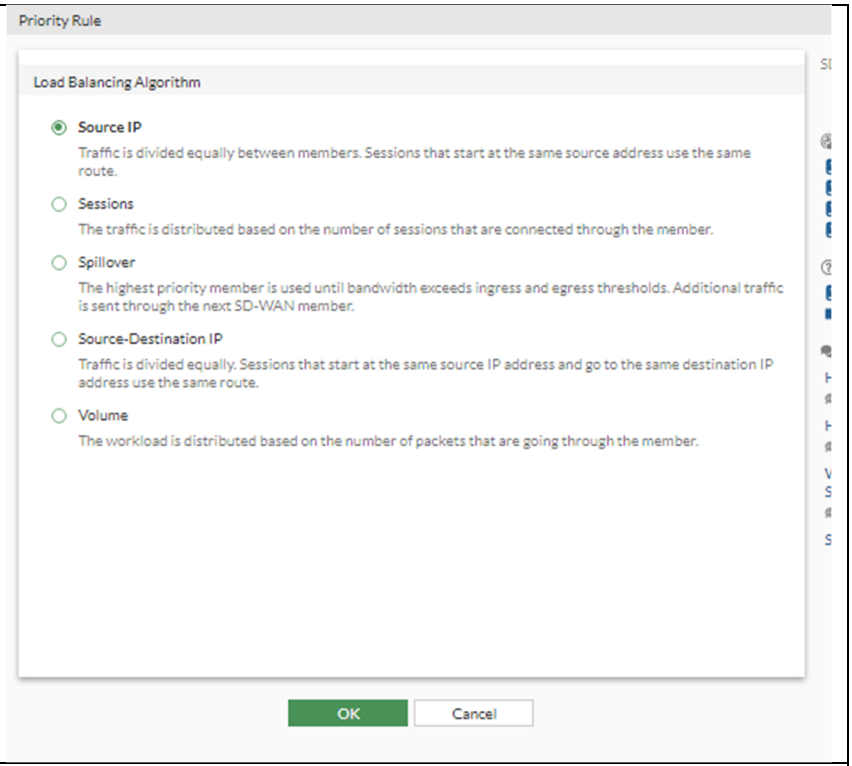
	Navegando por **Policy & Objects** > **Firewall Policy** é possível enquadrar o perfil de Application Control criado para determinar em qual fluxo ocorrera o controle de tráfego por aplicação.
	1 – Criando um perfil de Application Control  2 – Escolhendo quais categorias de aplicações vão ser permitidas, 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

	 4 – Abaixo o exemplo de como a política fica com o perfil enquadrado 
Comentário	

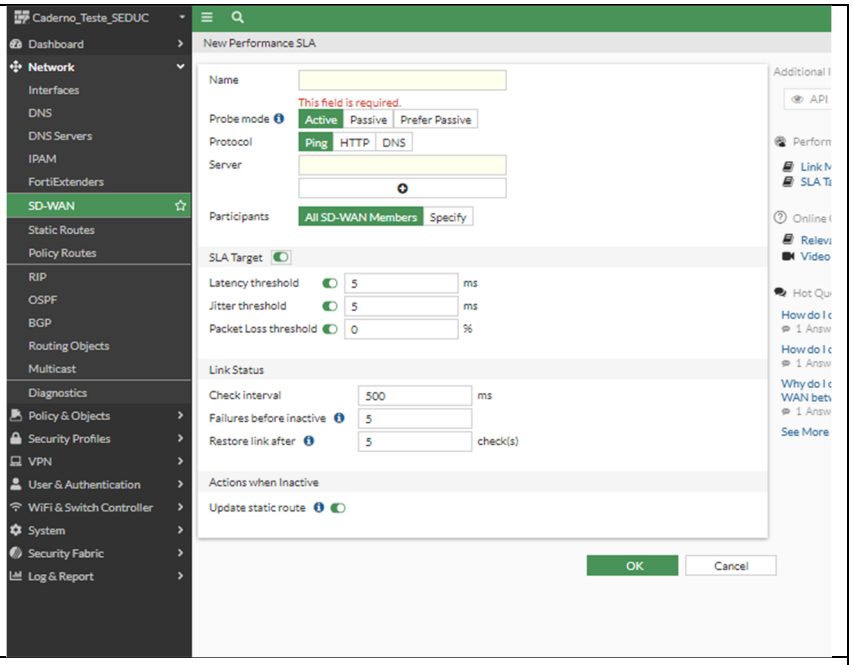
Item de Teste - 5.3.3.6	Deverá suportar, no mínimo, 3 (três) links de WAN;
Objetivo do Teste	Demonstrar que a ferramenta possui mais de três links de WAN
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Demonstrar base de regras do FortiGate
Evidências	Qualquer interface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

	
Comentário	

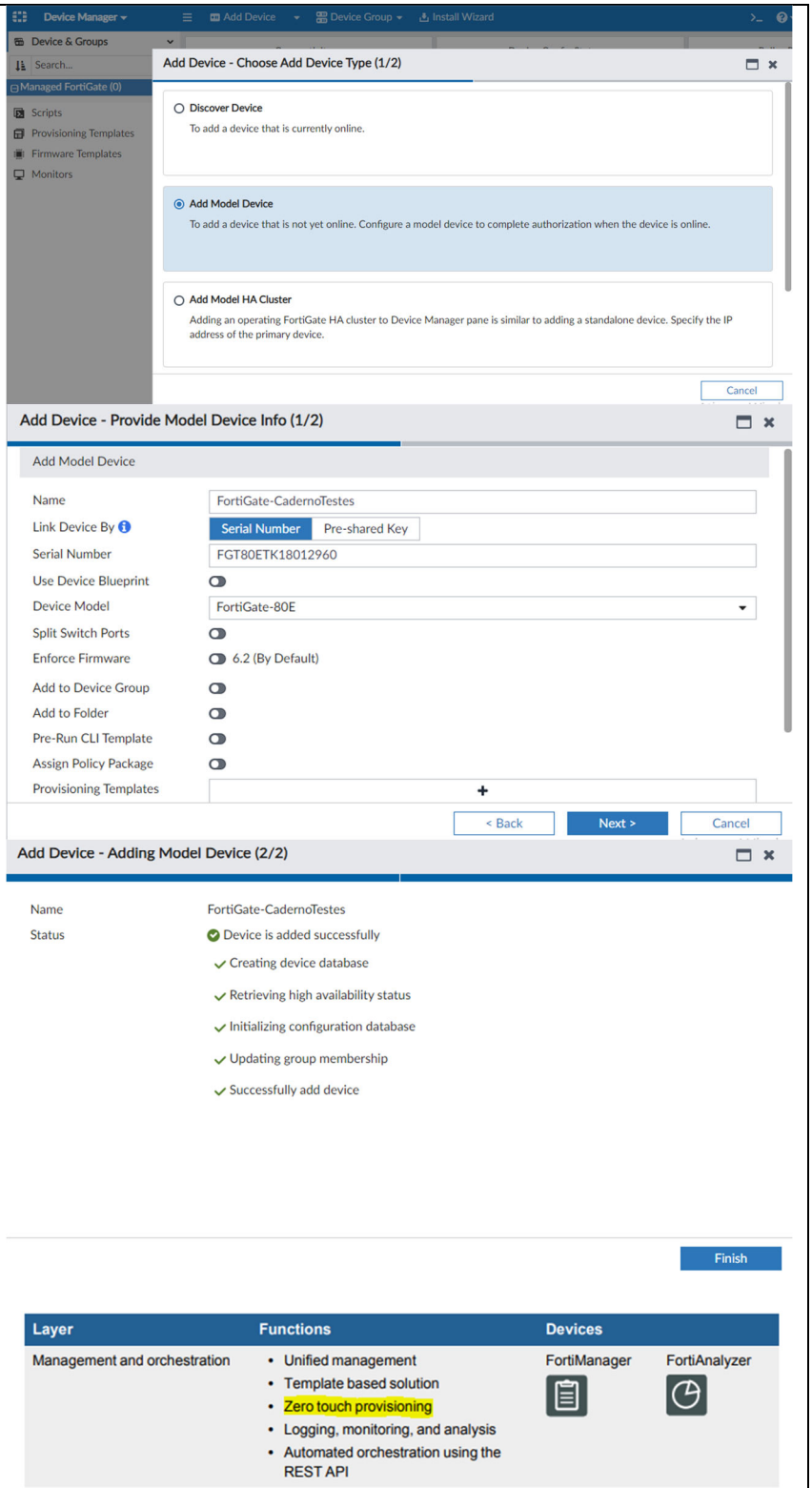
Item de Teste - 5.3.3.9	Distribuição de tráfego com balanceamento de sessão entre os circuitos existentes;
Objetivo do Teste	Criar regra que balanceie o tráfego entres todos os links wan
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Demonstrar base de regras do FortiGate

Evidências	
Comentário	

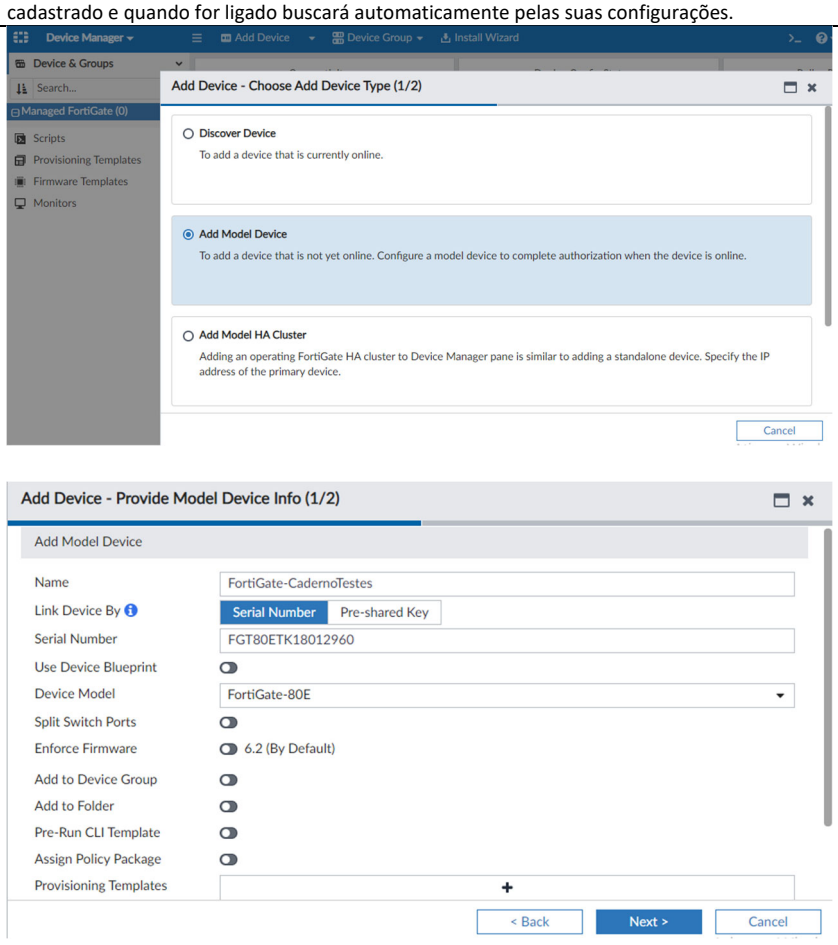
Item de Teste - 5.3.3.10	Distribuição orientada a qualidade, o dispositivo deve validar o melhor caminho disponível e utilizar deste path para manter sessões ativas, caso o melhor caminho entre em degradação por fatores anômalos o dispositivo deverá entender estes fatores e distribuir para os demais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

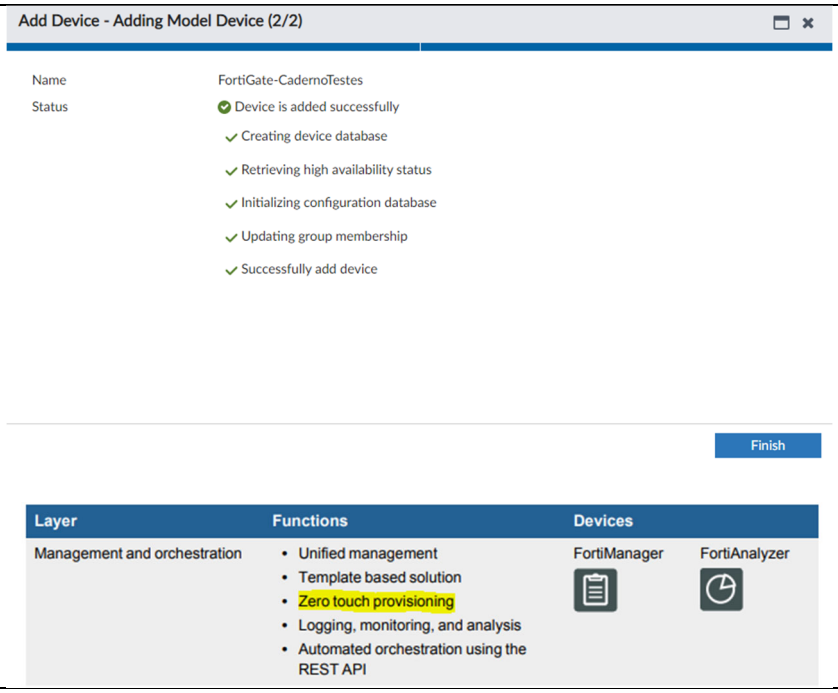
Evidências	
Comentário	

Item de Teste -5.3.3.11	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;
Objetivo do Teste	Mostrar que os dispositivos remotos suportam a funcionalidade ZTP.
Configuração do Teste	Integração com o FortiManager
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	 Device Manager Add Device Device Group Install Wizard Device & Groups Search... Managed FortiGate (0) Scripts Provisioning Templates Firmware Templates Monitors Add Device - Choose Add Device Type (1/2) Discover Device To add a device that is currently online. Add Model Device To add a device that is not yet online. Configure a model device to complete authorization when the device is online. Add Model HA Cluster Adding an operating FortiGate HA cluster to Device Manager pane is similar to adding a standalone device. Specify the IP address of the primary device. Cancel Add Device - Provide Model Device Info (1/2) Add Model Device Name FortiGate-CadernoTestes Link Device By Serial Number Pre-shared Key Serial Number FGT80ETK18012960 Use Device Blueprint Device Model FortiGate-80E Split Switch Ports Enforce Firmware 6.2 (By Default) Add to Device Group Add to Folder Pre-Run CLI Template Assign Policy Package Provisioning Templates < Back Next > Cancel Add Device - Adding Model Device (2/2) Name FortiGate-CadernoTestes Status Device is added successfully Creating device database Retrieving high availability status Initializing configuration database Updating group membership Successfully add device Finish Layer Functions Devices Management and orchestration Unified management Template based solution Zero touch provisioning Logging, monitoring, and analysis Automated orchestration using the REST API FortiManager FortiAnalyzer

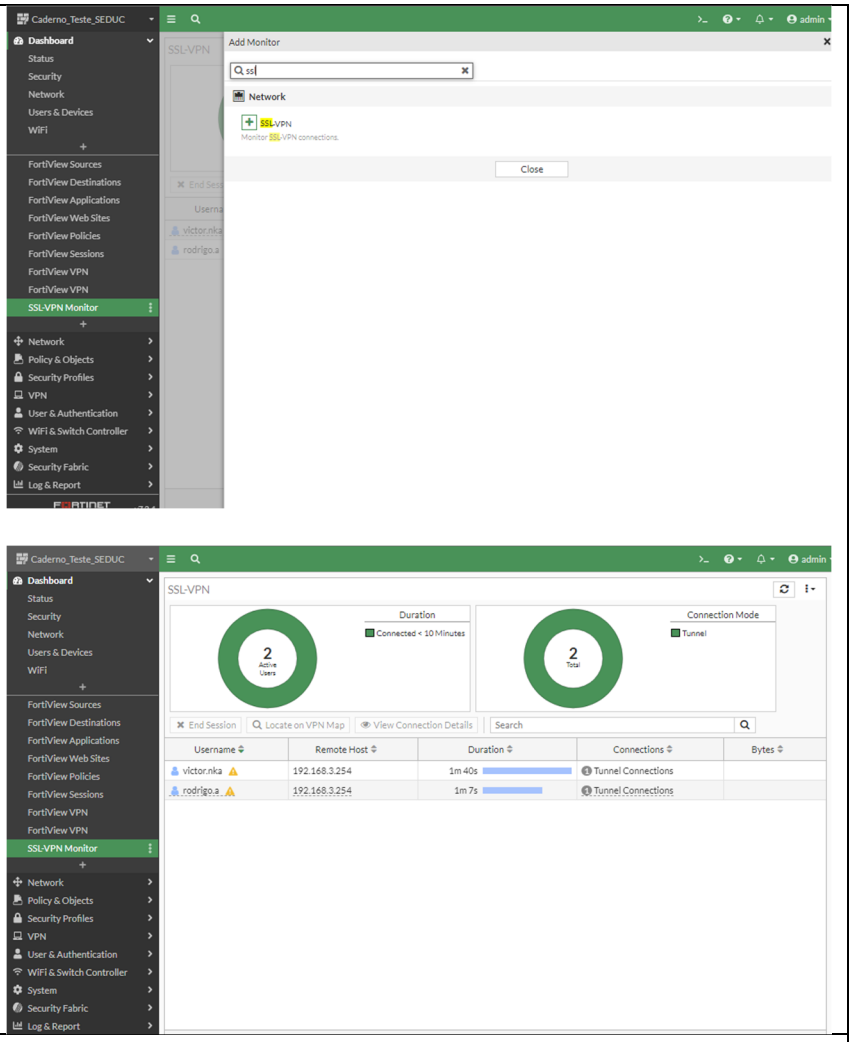
Comentário	Fonte: FortiOS-7.2.3-Administration_Guide disponível em https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a06117ca-5fbf-11ed-96f0-fa163e15d75b/FortiOS-7.2.3-Administration_Guide.pdf https://docs.fortinet.com/document/FortiGate/6.2.14/cookbook/861490/zero-touch-provisioning-with-fortimanager

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	

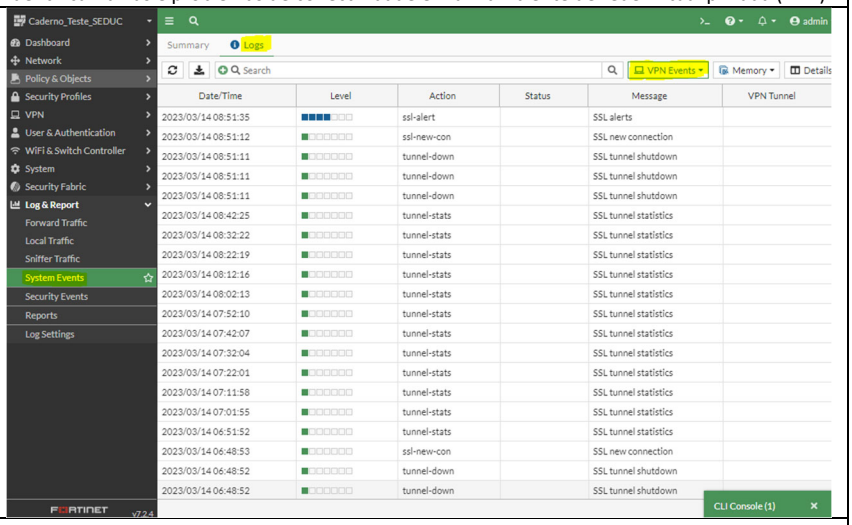
	
Comentário	Fonte: FortiOS-7.2.3-Administration_Guide disponível em https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a06117ca-5fbf-11ed-96f0-fa163e15d75b/FortiOS-7.2.3-Administration_Guide.pdf

5.3.4 ACESSO REMOTO - VPN:

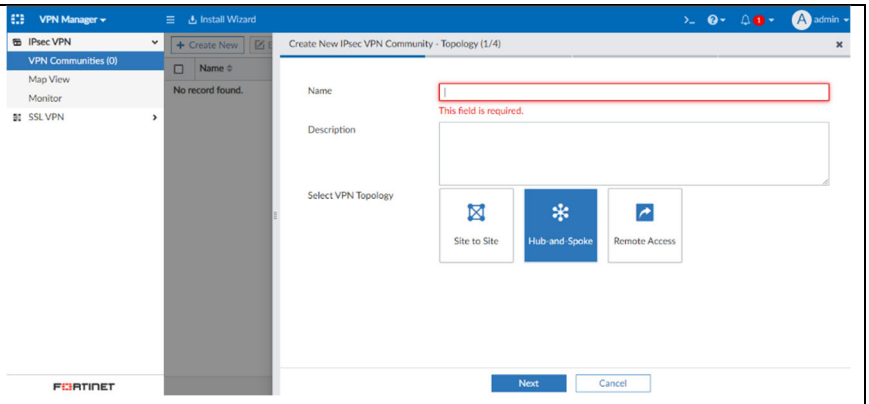
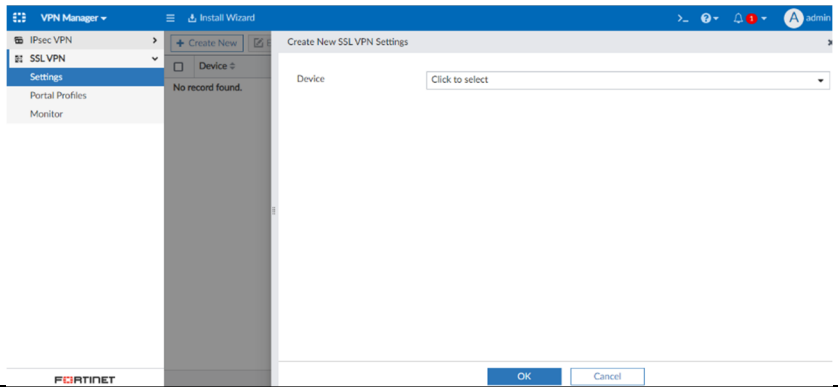
Item de Teste - 5.3.4.10	Deverá ser capaz de monitorar todos os usuários remotos logados;
Objetivo do Teste	Validar se o FortiGate é capaz de realizar o monitoramento de todos os usuários conectados remotamente por meio de VPN.
Configuração do Teste	Demontrar os usuários VPN conectados
Procedimento do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

Evidências	
Comentário	

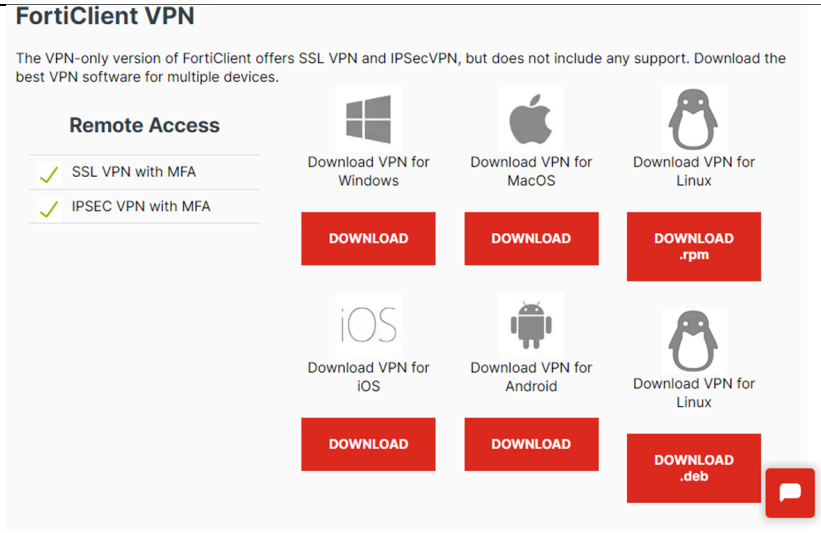
Item de Teste - 5.3.4.11	Deverá ser capaz de reconhecer falhas e problemas de conectividade entre dois pontos conectados através de uma VPN, e registrar e alertar quando o túnel VPN está desconectado;
Objetivo do Teste	Validar se o appliance é capaz de reconhecer falhas e problemas de conectividade entre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

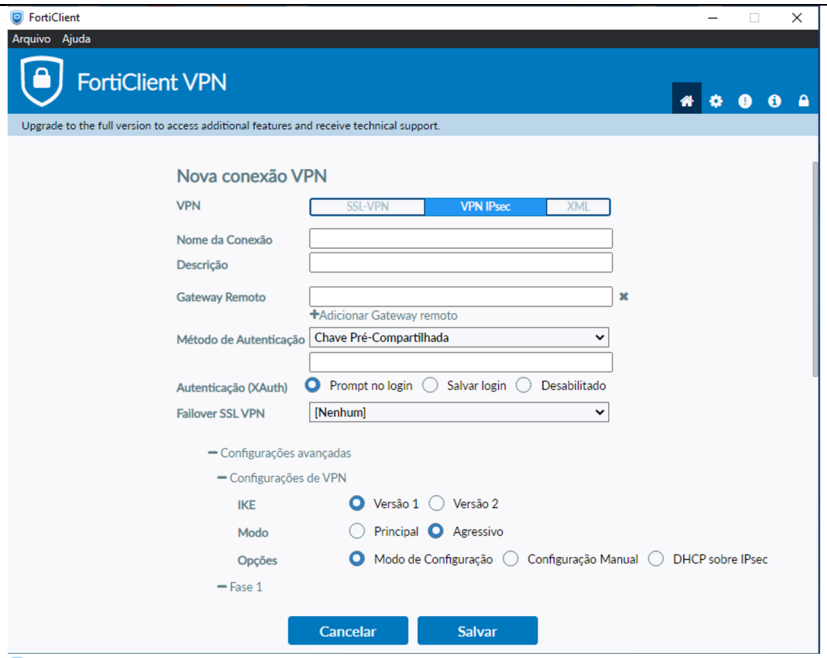
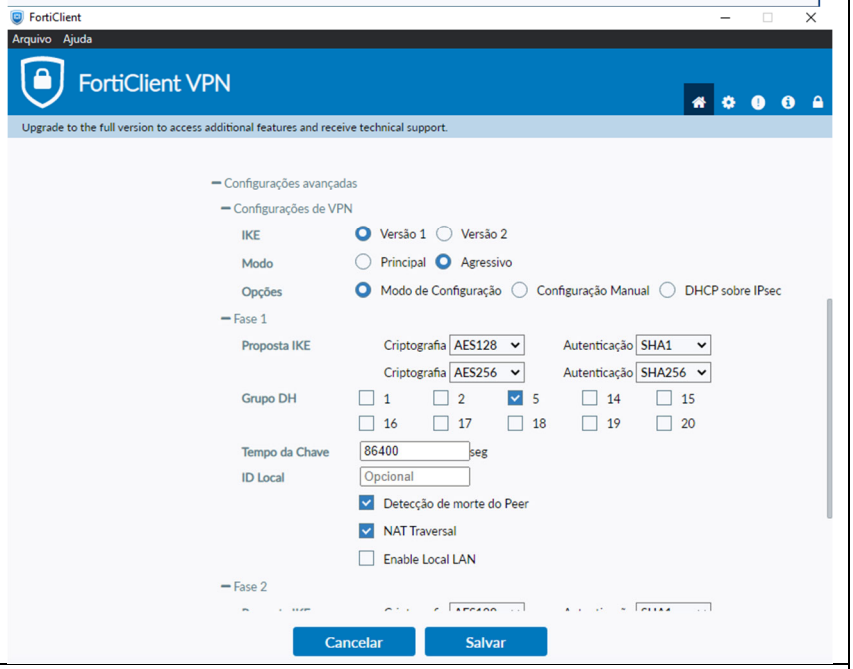
	- Email subject. - Email body. No gatilho colocar “IPsec connection status changed”. Ao acessar a seção "Log & Report" e, em seguida, "System Events" e "VPN Events", é possível identificar falhas e problemas de conectividade em um ambiente de rede virtual privada (VPN).
Evidências	
Comentário	

Item de Teste - 5.3.4.12	Deve incluir gerenciamento centralizado de VPNs, com a possibilidade de estabelecimento de VPNs com vários peers remotos ao mesmo tempo;
Objetivo do Teste	Validar se é possível estabelecer VPNs com vários peers remotos ao mesmo tempo e realizar o gerenciamento centralizado de VPNs.
Configuração do Teste	Demonstrar a capacidade de estabelecimento de múltiplos túneis VPN com diversos peers.
Procedimento do Teste	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.
Evidências	

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

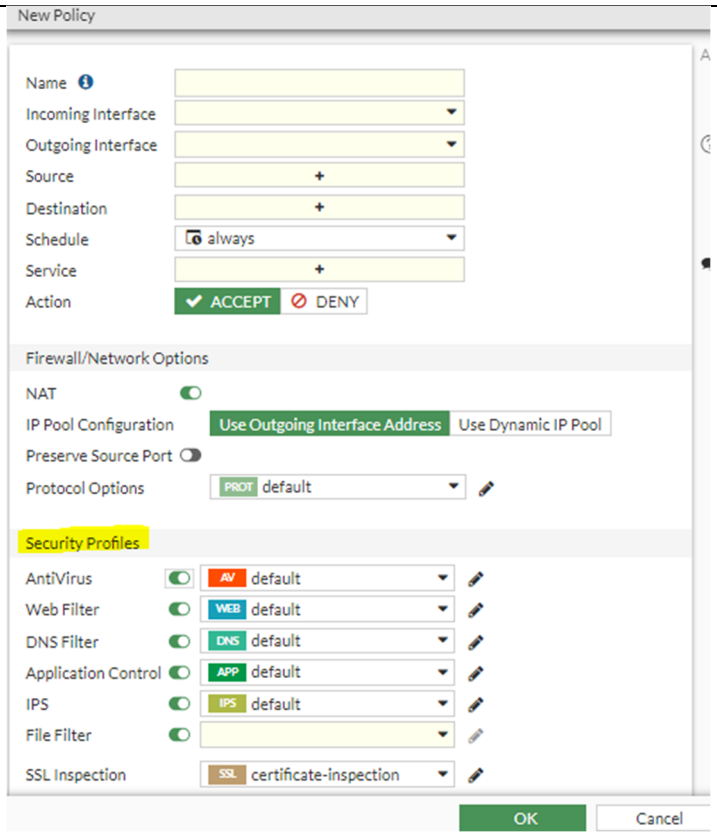
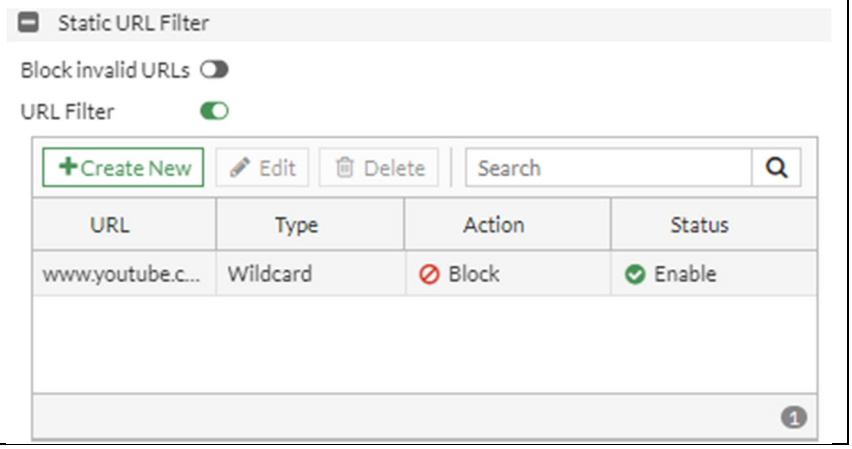
Item de Teste - 5.3.4.13	Clientes IPSec do mesmo fabricante devem estar disponíveis para pelo menos Windows 10 (64 bits);
Objetivo do Teste	Validar se o Forticlient está disponível para Windows 10 (64 bits)
Configuração do Teste	Forticlient é totalmente compatível com Windows 10 e permite conexões tanto 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 Download VPN for MacOS DOWNLOAD Download VPN for Linux DOWNLOAD .rpm iOS Download VPN for iOS DOWNLOAD Download VPN for Android DOWNLOAD Download VPN for Linux DOWNLOAD .deb

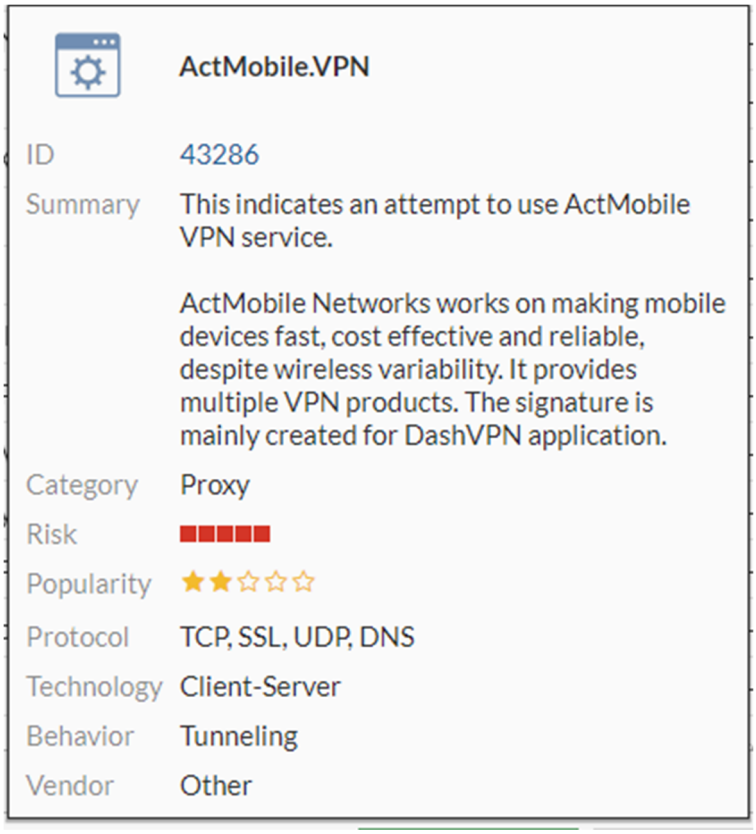
	 
Comentário	

5.3.5 CONTROLE DE APLICAÇÕES WEB E FILTRO URL:

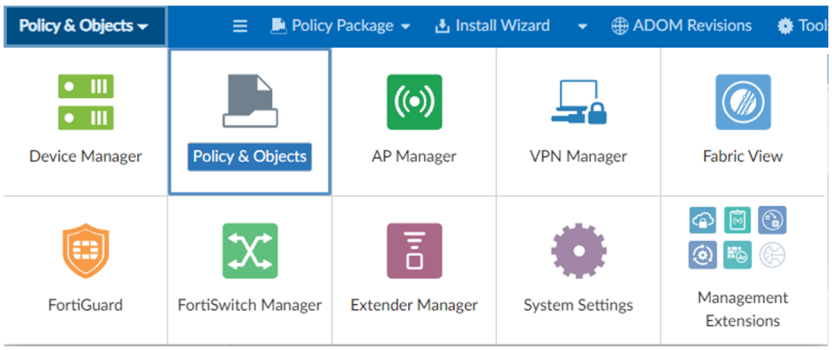
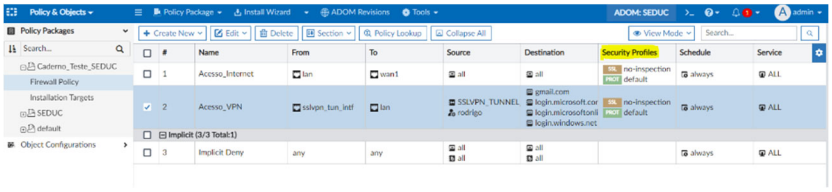
Item de Teste - 5.3.5.1	A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança, que permita a criação de políticas de liberação ou bloqueio;

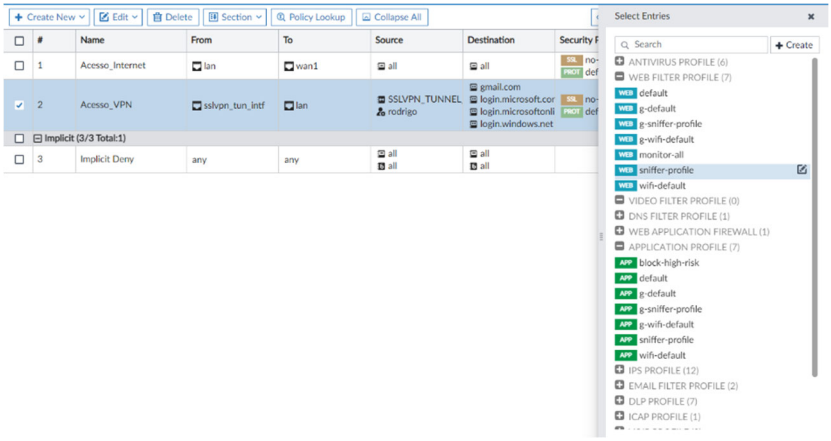
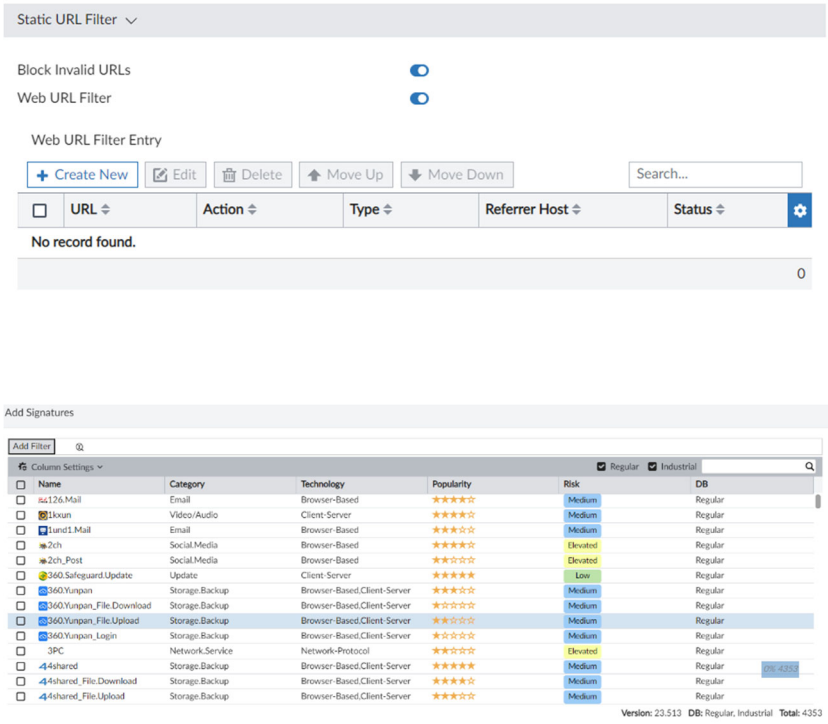
Objetivo do Teste	Validar se a solução conta com ferramentas de visibilidade e controle de aplicações Web e Filtro URL integrada, que permita a criação de políticas de liberação ou bloqueio.
Configuração do Teste	Configuração de regra de segurança NGFW com filtro de aplicação e URL.
Procedimento do Teste	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	 

Comentário	

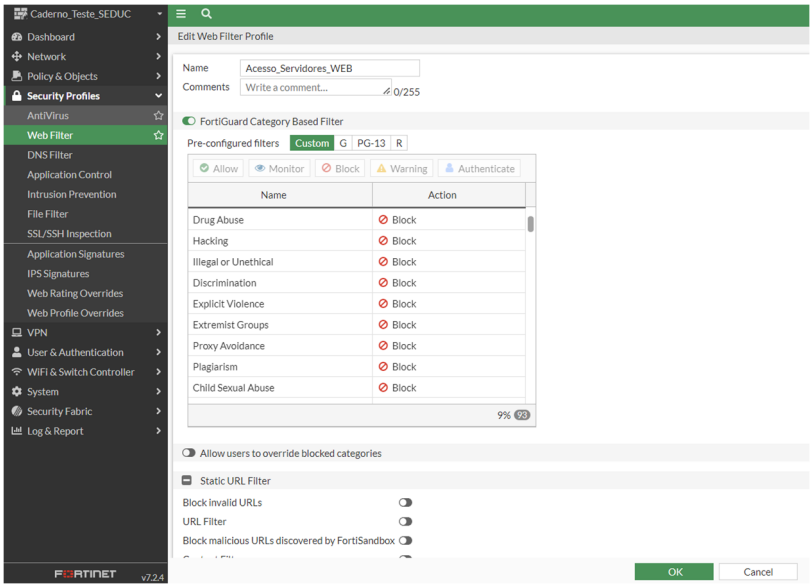
Item de Teste - 5.3.5.2	A solução deve ser capaz de identificar qualquer tipo de aplicação, em até camada 7, independente de porta e protocolo;
Objetivo do Teste	Verificar se o equipamento identifica uma aplicação independente de porta ou protocolo.
Configuração do Teste	Criar filtro de aplicação de camada 7
Procedimento do Teste	Criar regra contendo filtro de aplicação de camada 7.
Evidências	"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" **Application control** FortiGates 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). 

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

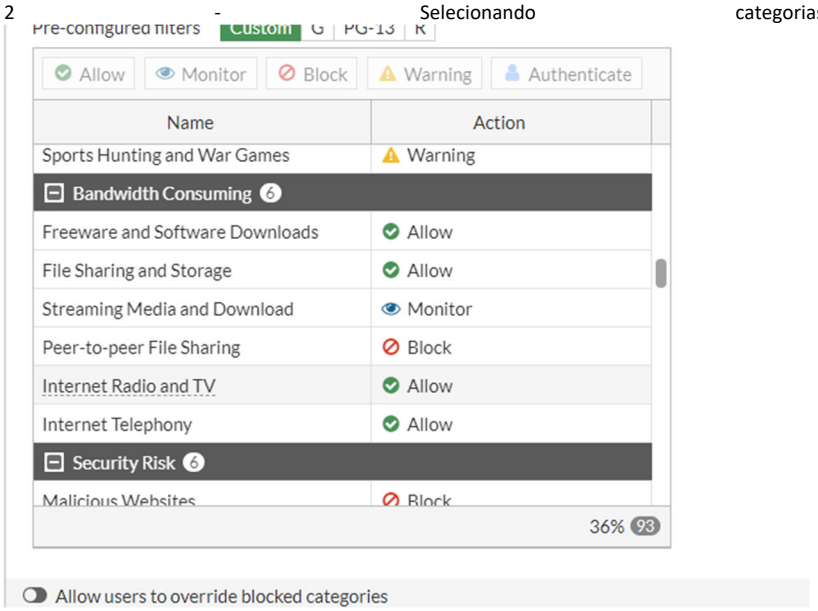
Item de Teste - 5.3.5.3	A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser centralizada na mesma console de gerenciamento;
Objetivo do Teste	Verificar se o equipamento possui a funcionalidade de gerenciar as políticas de segurança de controle de aplicação e 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 possuí 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	 

	 
Comentário	

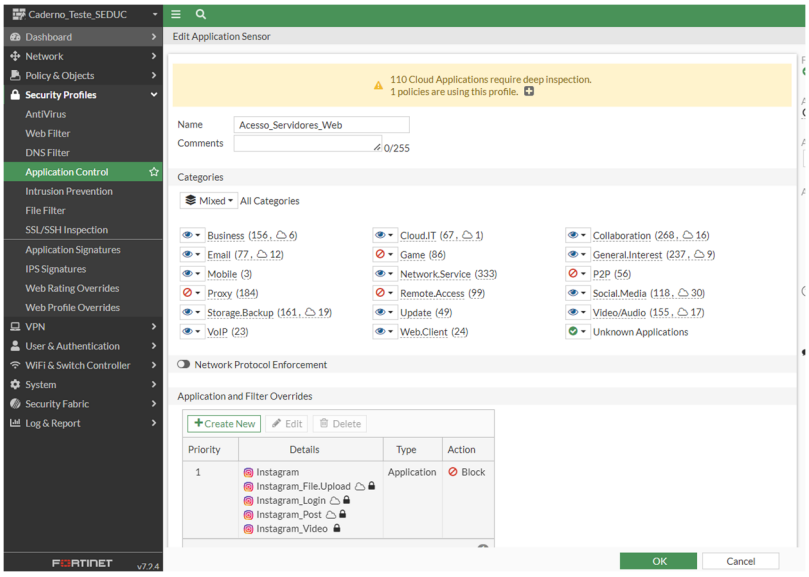
Item de Teste - 5.3.5.5	Possuir controle de regras de aplicações, grupos de aplicações, categorias de aplicações com controle granular para usuários ou grupos de usuários;
Objetivo do Teste	Validar se a solução possui ferramentas de controle de regras de aplicações, grupos de aplicações, categorias de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

Procedimento do Teste	Navegando por **Security Profile** > **Application Control** > **Create New** é possível criar um novo perfil enquadrando as aplicações que deseja bloquear, monitorar ou aprovar Navegando por **Policy & Objects** > **Firewall Policy** é possível enquadrar o perfil de Application Control criado para determinar em qual fluxo ocorrera o controle de tráfego por aplicação No campo “Source” da política, podemos realizar o controle de qual grupo ou usuário a regra se enquadra No campo Security Profiles determinamos quais categorias de sites e aplicações o grupo de usuários se enquadra
Evidências	1 – Criando Web Filter. 

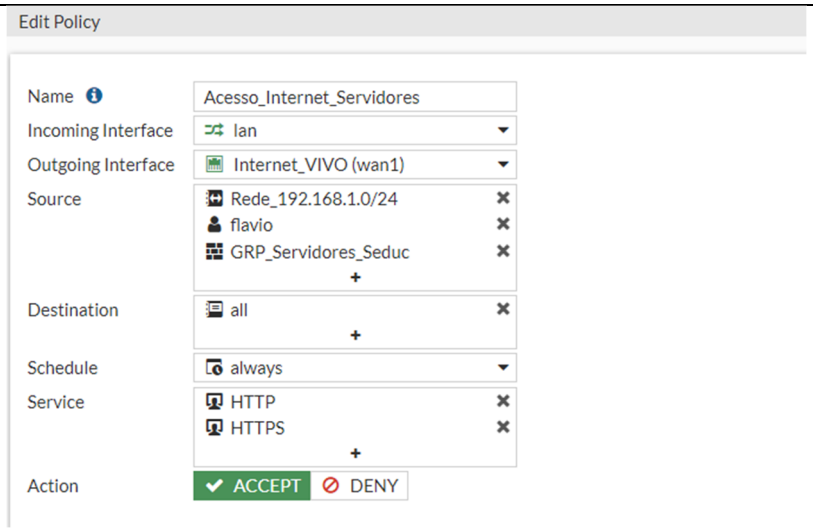
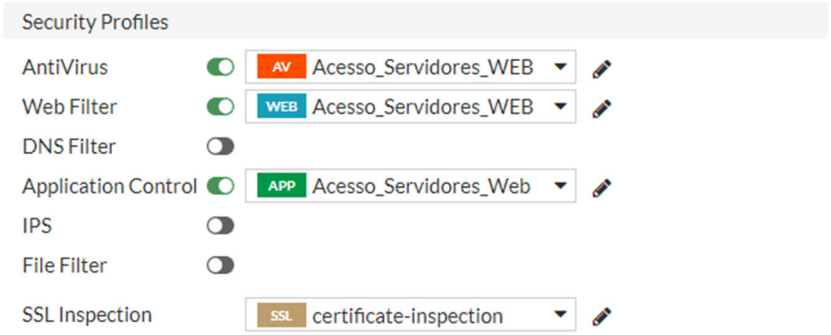
2 - Selecionando categorias.



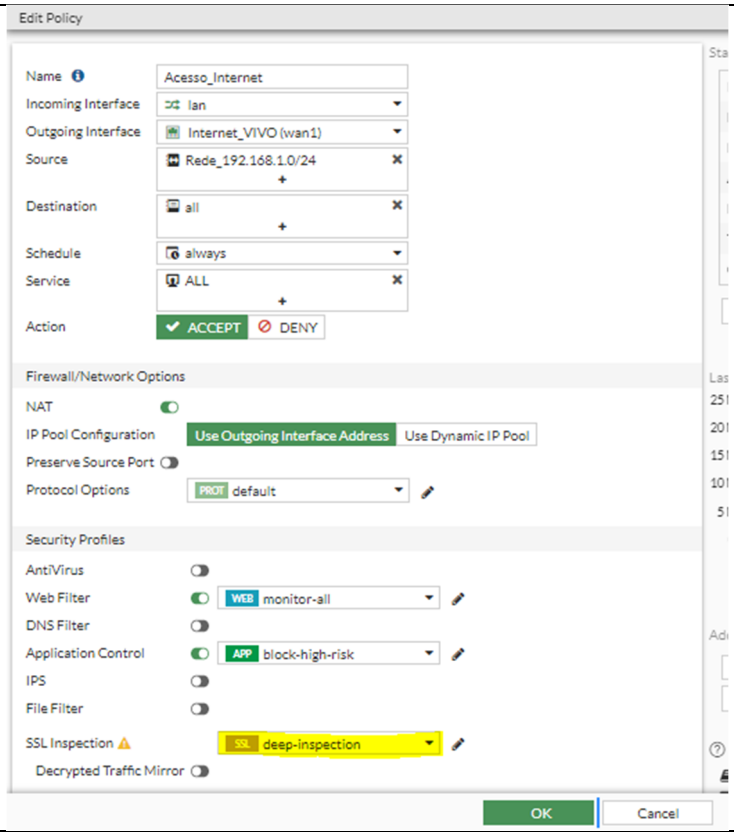
3 – Criando Application Control.



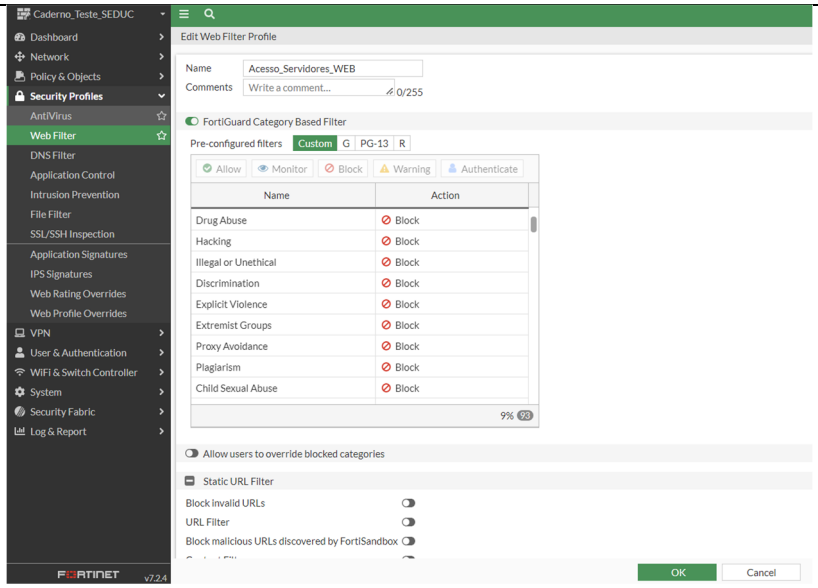
3 – Definindo grupos e usuários.

	 4 – Definindo Profiles WEB e de Aplicação para política. 
Comentário	

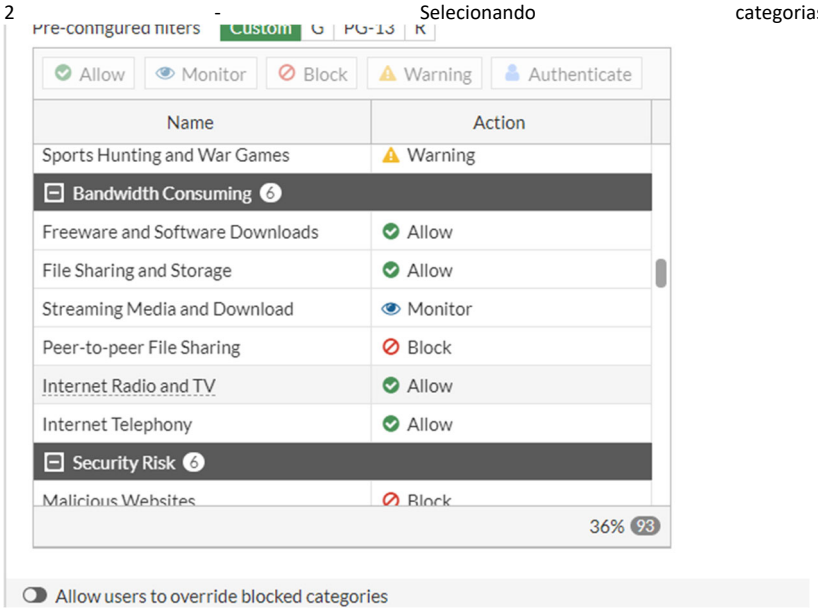
Item de Teste - 5.3.5.6	Deve possibilitar a inspeção de tráfego criptografado HTTPS (Inbound/Outbund);
Objetivo do Teste	Validar se a solução possui ferramentas de inspeção de tráfego criptografado HTTPS (Inbound/Outbund);
Configuração do Teste	1 - Criação da política 2 – Adicionar perfil de deep-inspection no campo SSL_Inspection da política
Procedimento do Teste	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.

Evidências	
Comentário	

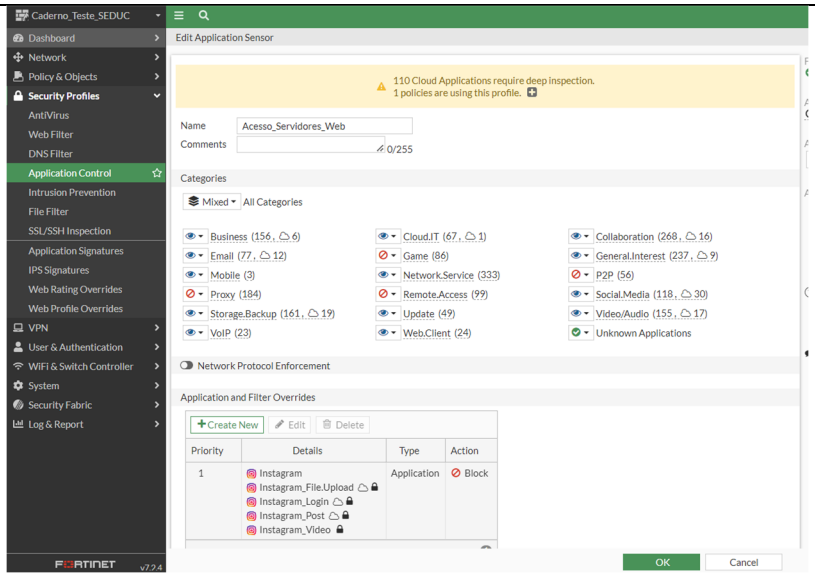
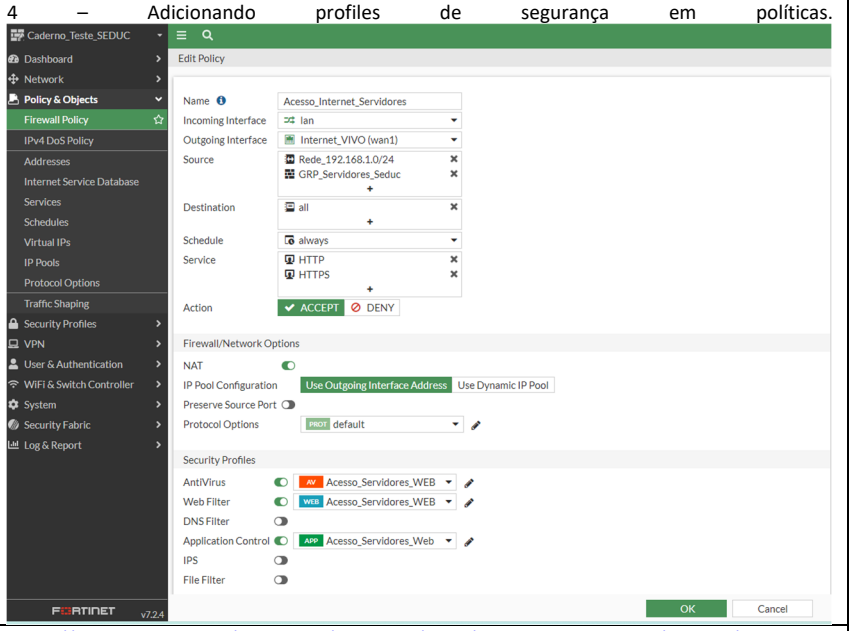
Item de Teste - 5.3.5.8	A solução deve ser capaz de criar regras com mais de uma categoria;
Objetivo do Teste	Validar se o FortiGate permite a criação de regras com mais de uma categoria
Configuração do Teste	Criar duas regras de acesso com categorização de sites distintas
Procedimento do Teste	Navegando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



2 - Selecionando categorias.

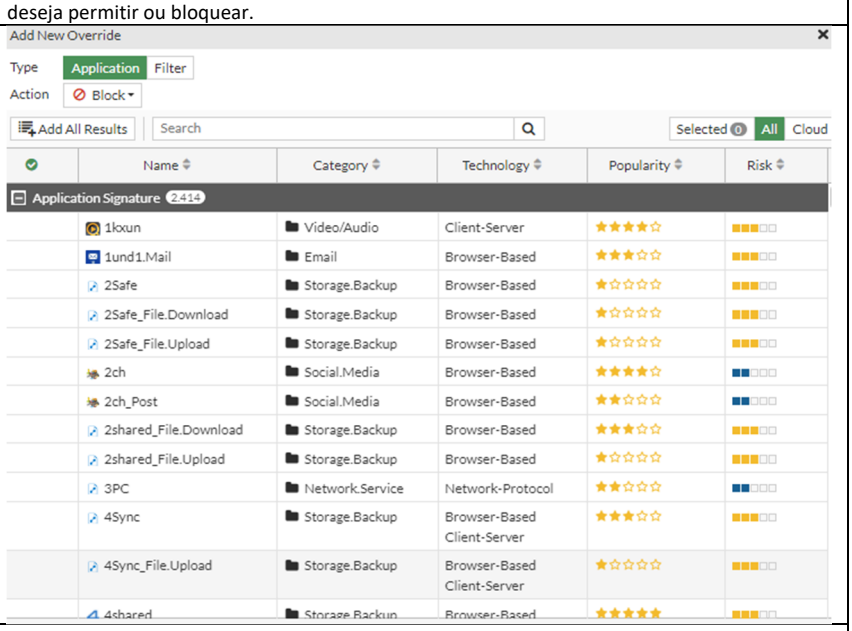


3 – Criando Application Control.

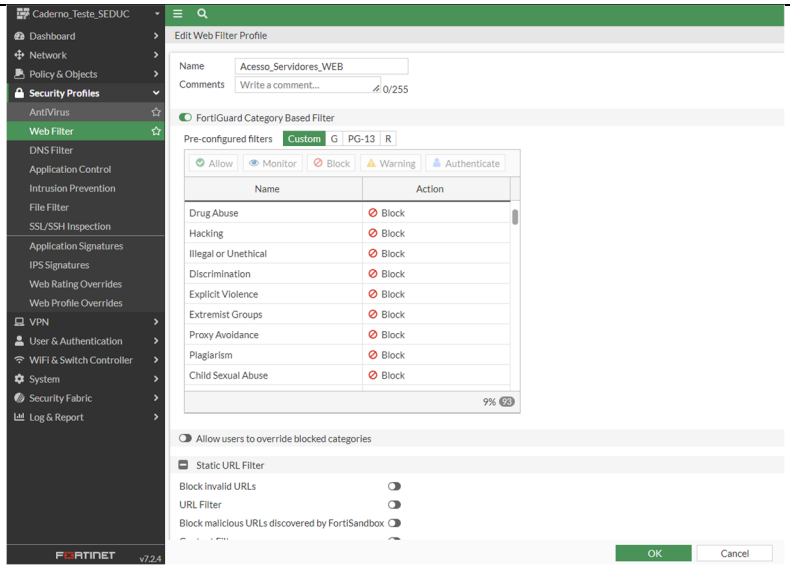
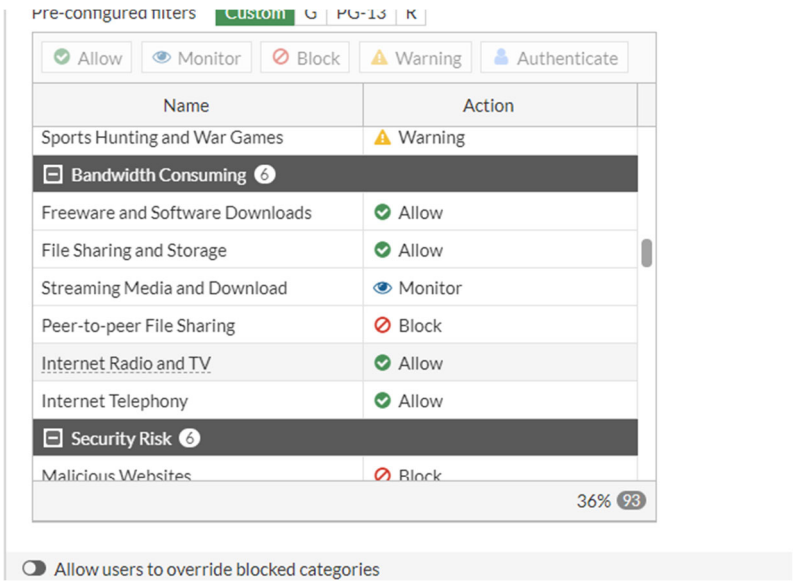
	 4 – Adicionando profiles de segurança em políticas. 
Comentário	https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/615462/url-filter https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/019814/basic-category-filters-and-overrides

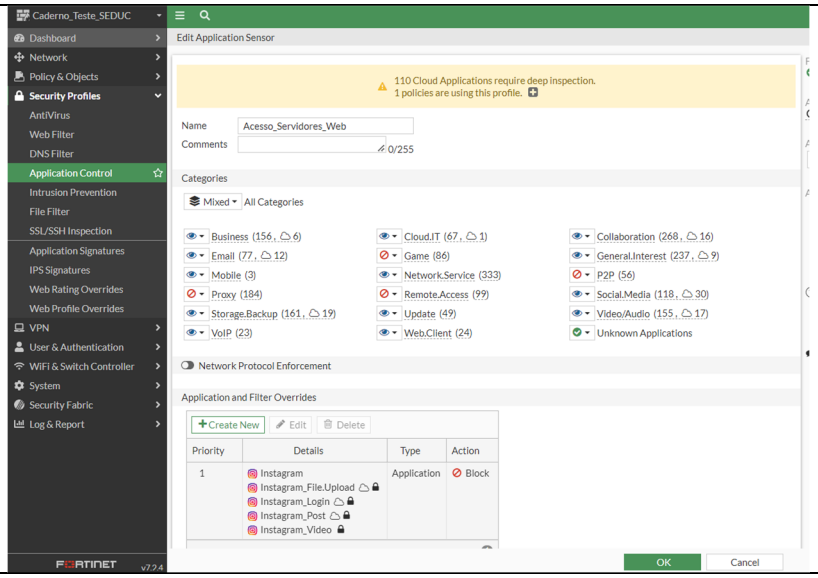
5.3.5.9 Deve possibilitar a permissão ou bloqueio de aplicações ou URLs por pelo menos

os seguintes critérios:

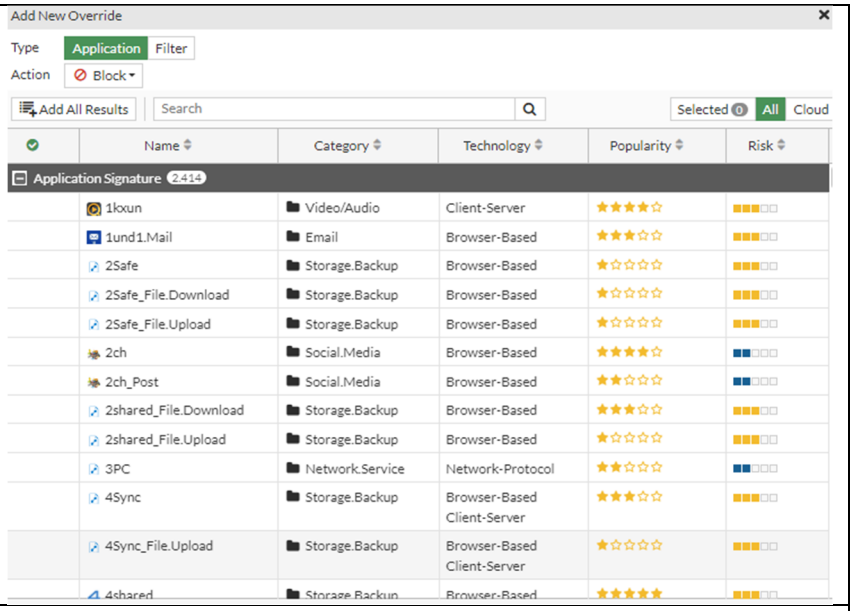
Item de Teste - 5.3.5.9.1	Aplicação da Web;
Objetivo do Teste	Validar se o Firewall possibilita o bloqueio ou permissão de aplicações da Web
Configuração do Teste	Navegando por Security Profiles > Application Control é possível realizar o bloqueio ou liberação de aplicações web
Procedimento do Teste	Para realizar o teste basta em Security Profiles > Application Control e escolher quais aplicações deseja permitir ou bloquear.
Evidências	
Comentário	

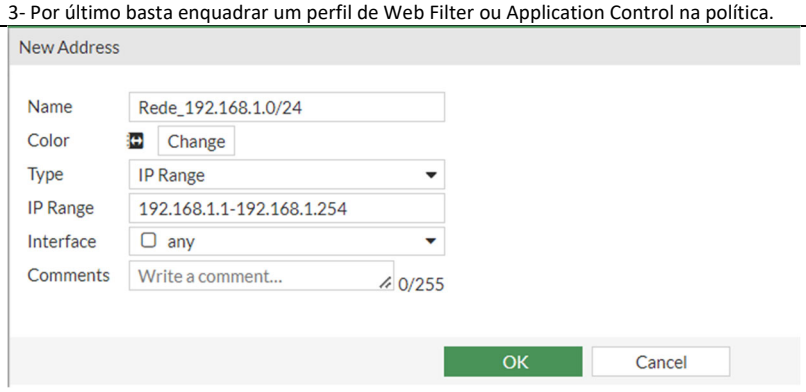
Item de Teste - 5.3.5.9.2	Categorias;
Objetivo do Teste	Validar se o Firewall possibilita o bloqueio ou permissão de aplicações web por meio de categorias
Configuração do Teste	Navegando por **Security Profiles > Web Filter > Create New** é possível criar profiles de Web Filter bloqueando, monitorando,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

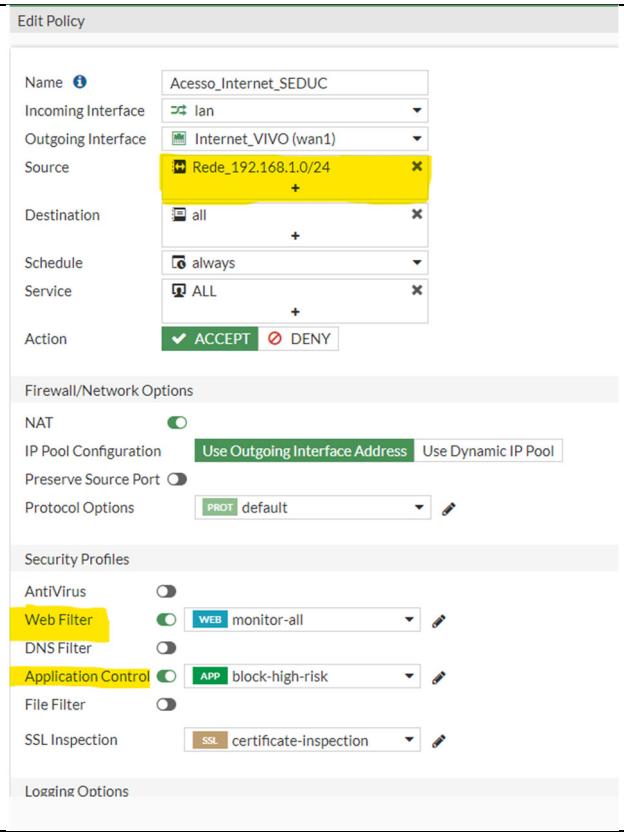
Evidências	 

	
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

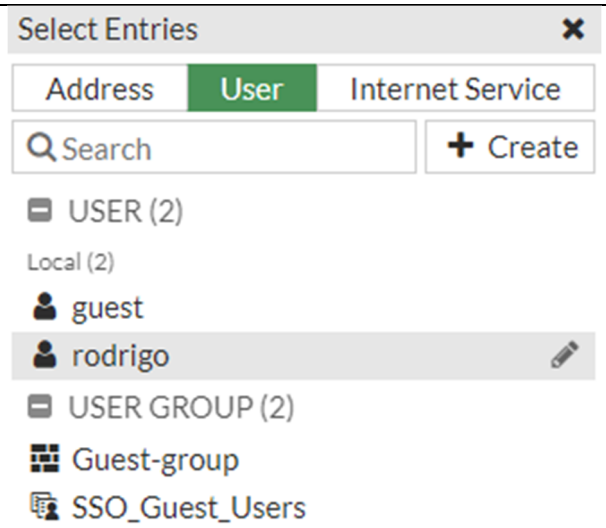
Item de Teste - 5.3.5.9.3	Nível de risco;
Objetivo do Teste	Validar se o Firewall possibilita o bloqueio ou permissão de aplicações web por meio de nível de risco
Configuração do Teste	Para realizar o controle de aplicações por nível de risco basta entrar no profile de Application Control e utilizar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

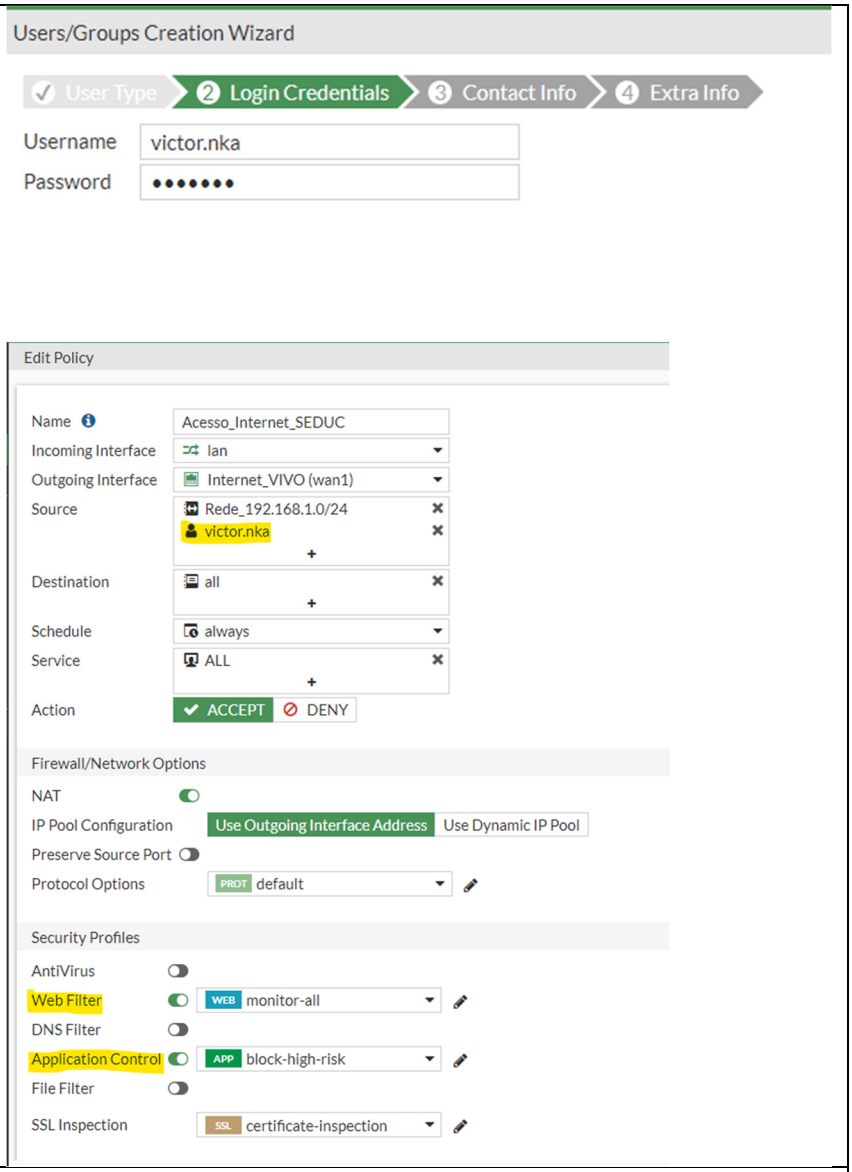
Evidências	
Comentário	

Item de Teste - 5.3.5.9.4	IP/Range de IPs/Redes;
Objetivo do Teste	Validar se o equipamento possibilita a permissão ou bloqueio de aplicações ou URLs pelo critério de IP/Range.
Configuração do Teste	Navegando por Security Profiles > Web filter e Application Control é possível criar perfis de segurança.
Procedimento do Teste	1- Criação de um IP Range 2-Navegando por **Policy & Objects** > **Firewall Policy** > **Source** é possível enquadra o IP Range criado no campo “Source” 3- Por último basta enquadrar um perfil de Web Filter ou Application Control na política.
Evidências	

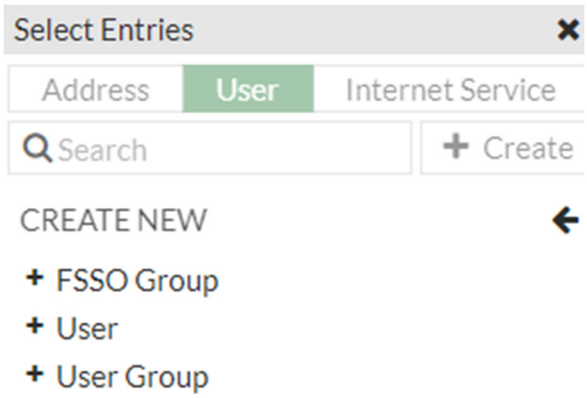
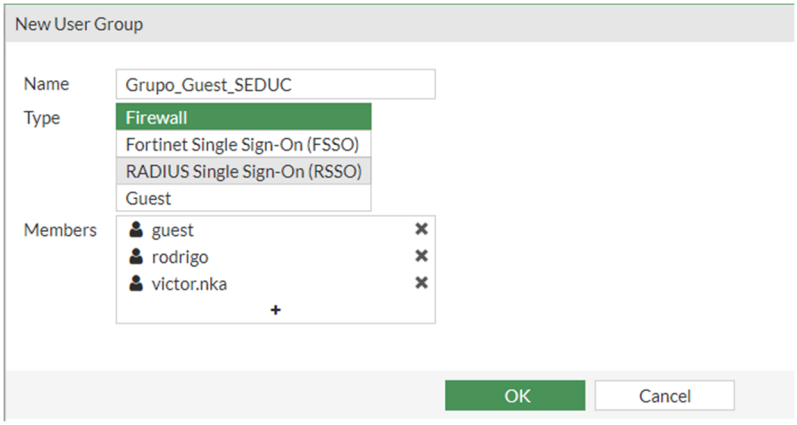
	
Comentário	

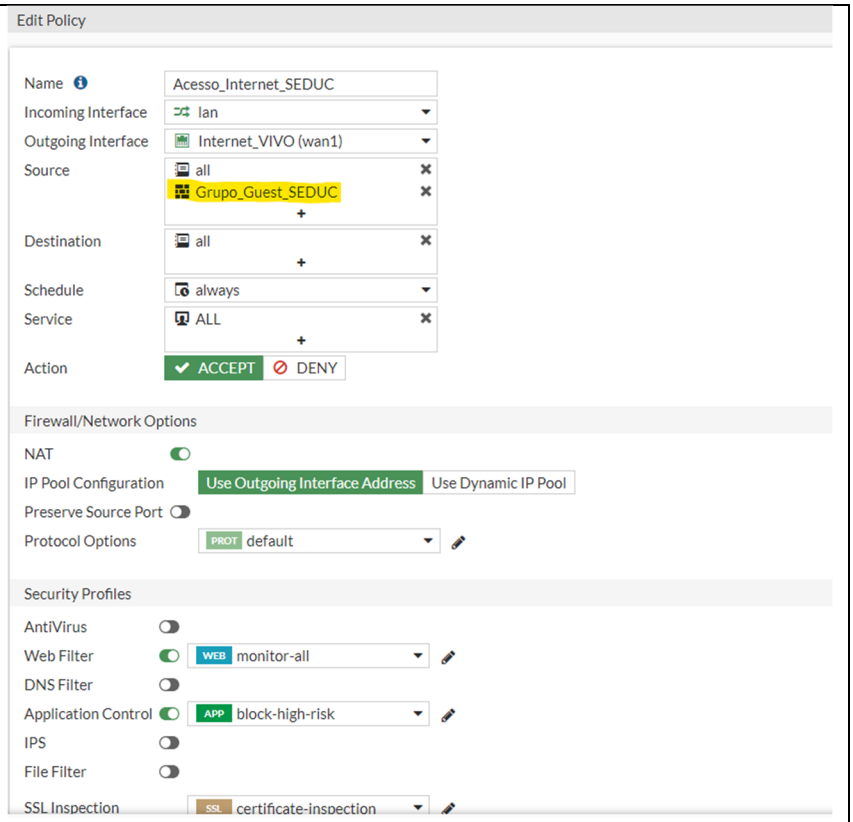
Item de Teste - 5.3.5.9.5	Usuários;
Objetivo do Teste	Validar se o equipamento possibilita a permissão ou bloqueio de aplicações ou URLs pelo critério de usuários
Configuração do Teste	Utilizar usuários do FortiGate para realizar o bloqueio ou permissão de aplicações e URLs
Procedimento do Teste	1 -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

Evidências	 Select Entries Address User Internet Service Search Create USER (2) Local (2) guest rodrigo USER GROUP (2) Guest-group SSO_Guest_Users

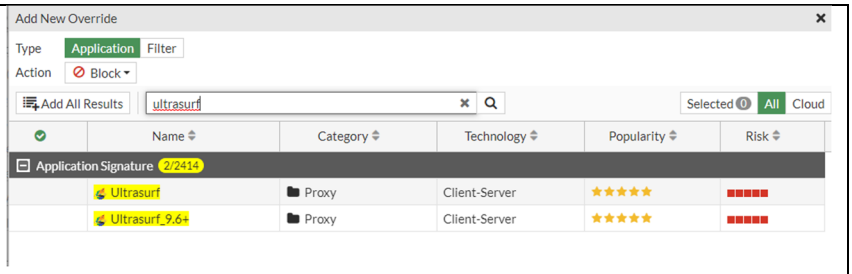
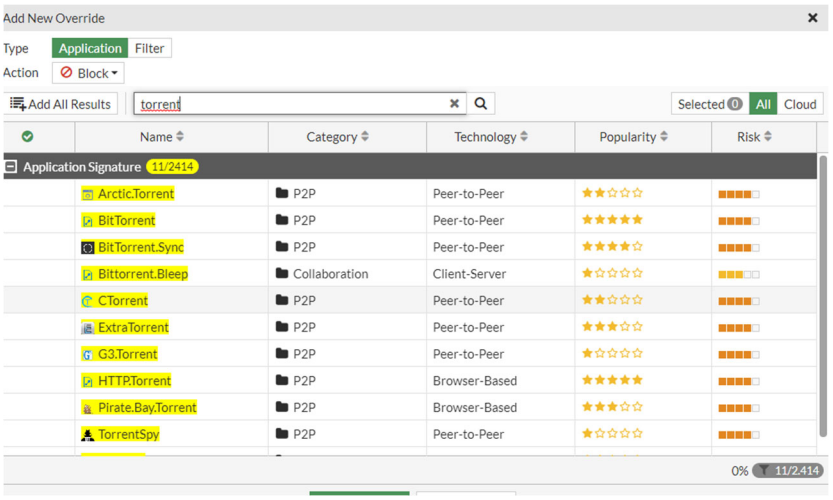
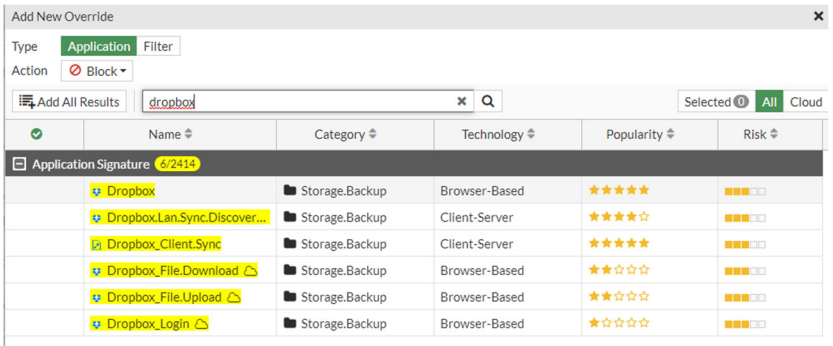
	
Comentário	

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	1 - Criação de um novo grupo de usuários 2 - Navegando por **Policy & Objects** > **Firewall Policy** > **Source** é possível enquadra o grupo criado no campo “Source” 3- Por último basta enquadrar um perfil de Web Filter ou Application Control na política

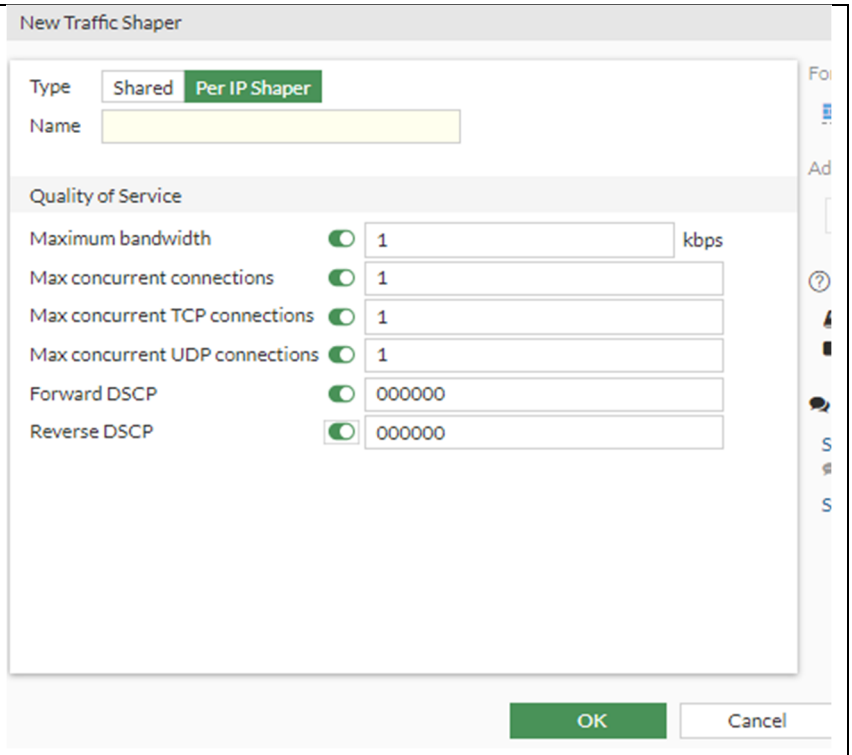
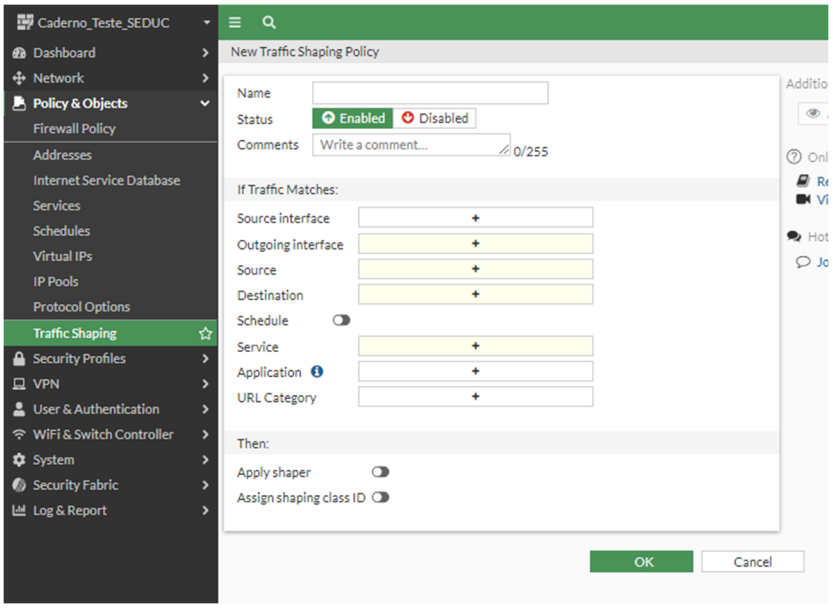
Procedimento do Teste	Criar duas regras NGFW com origem de grupos distintos
Evidências	Criando um novo Grupo  2 – Definindo membros no grupo  3 - Adicionando o Grupo no campo Source e adicionando filtros de Web e Aplicações

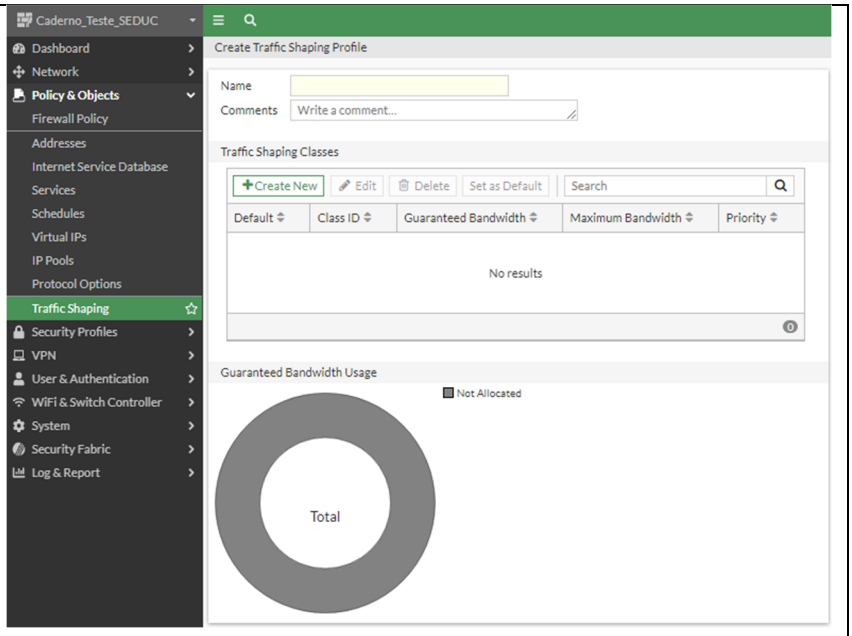
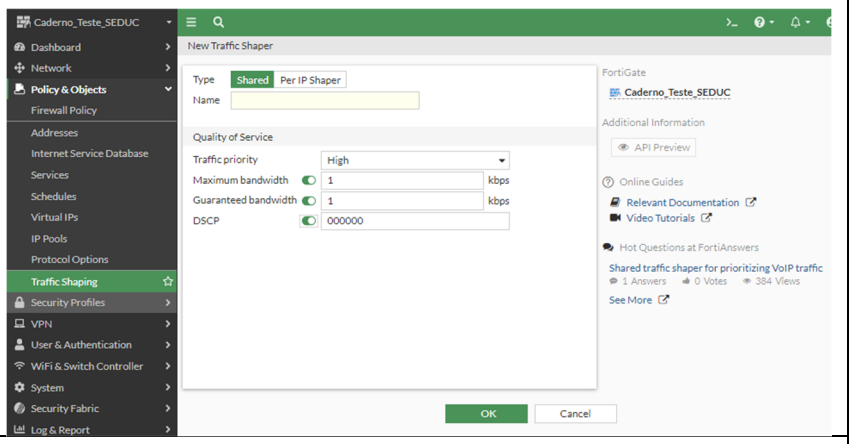
	
Comentário	

Item de Teste - 5.3.5.10	Aplicações que sejam passiveis 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 passiveis 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.

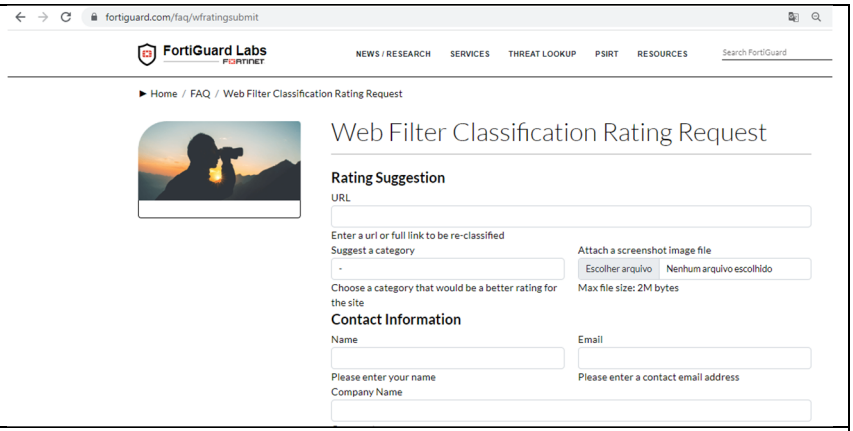
Evidências	  
Comentário	

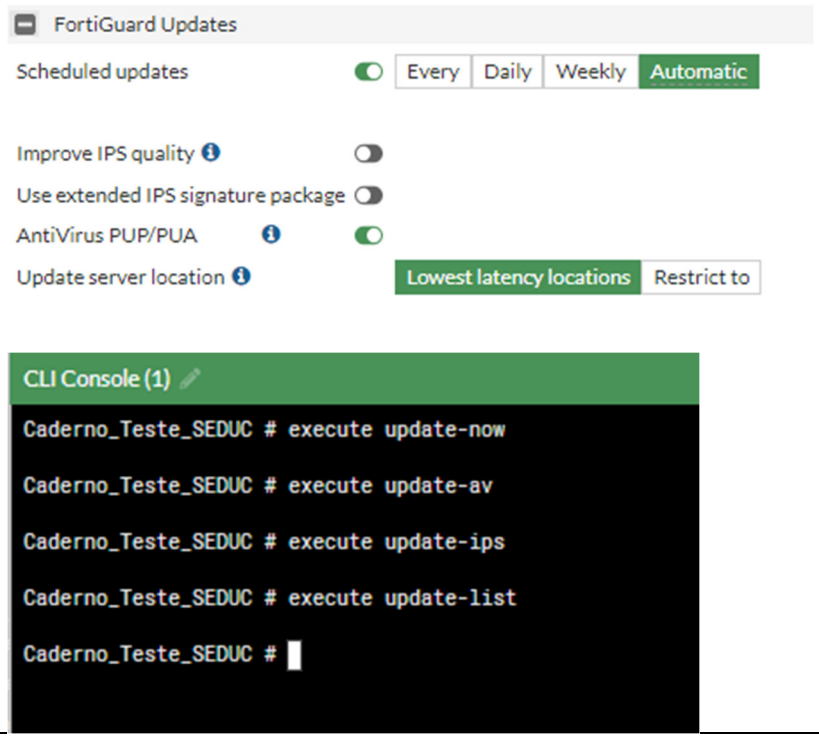
Item de Teste - 5.3.5.11	Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários ou grupos do AD;
Objetivo do Teste	Validar a criação de traffic shaping baseado no IP de origem, usuários ou grupos do AD.
Configuração do Teste	Criar duas regras contendo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

Evidências	 

	 
Comentário	

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

	
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	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. Também tem a possibilidade de realizar as atualizações de forma manual, utilizando comandos de cli.
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