



SECRETARIA DE ESTADO DA EDUCAÇÃO DO GOIÁS
RELATÓRIO DOS TESTES DA AMOSTRA
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 RELATÓRIO DOS TESTES DA AMOSTRA

O objetivo deste relatório é apresentar informações sobre o atendimento da solução proposta para o Lote 01, considerando a execução dos testes da amostra, de acordo com o estabelecido nos itens 13.14.19 e 13.14.20 do Edital, a saber:

13.14.19. A licitante deve disponibilizar em até 5(cinco) dias úteis contados da data da finalização dos testes o Relatório dos Testes da Amostra, o qual deverá conter todas as informações e resultados apurados.

13.14.20. No Relatório dos Testes de Amostra deverá constar, no mínimo: informações da topologia do ambiente de teste utilizado, arquivos, impressões de telas, scripts de configuração, versões de software utilizadas e registros de logs com evidências capturadas e quaisquer informações que a equipe de apoio ao pregoeiro ache pertinente, seguindo a estrutura estabelecida no Caderno de Teste. Ou seja, espera-se do relatório a mesma sequência do Caderno de Teste as respectivas comprovações e ou evidências para os itens constante deste documento.

Conforme determinação, o relatório foi elaborado seguindo a estrutura estabelecida no Caderno de Teste, que teve 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.

Constam neste documento as evidências de pleno atendimento ao Termo de Referência, coletadas durante os dias de execução dos testes (25 e 26/07), superando apontamentos já comprovados no documento de contrarrazões e, no que for aplicável, esclarecimento de dúvidas complementares.

Todas as evidências estão disponíveis na gravação das sessões, realizadas pelo grupo técnico de apoio, com consulta disponível em caso de informação complementar.

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
6.0	Tiago Marques	25/07/2023	Inclusão das evidências dos testes
6.0	Tiago Marques	26/07/2023	Inclusão das evidências dos testes
7.0	Armando Costa	27/07/2023	Revisão e alterações
7.0	Crystine Rodrigues	31/07/2023	Revisão e alterações

3. LOCAL DE REALIZAÇÃO DOS TESTES

Os testes de conformidade conforme certame, foram realizados de forma remota no laboratório da Fortinet, por meio de aplicativo Teams, com link disponibilizado pela equipe técnica do SEDUC-GO.

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.br

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 foram realizados na versão 7.2 do sistema operacional FortiOS.

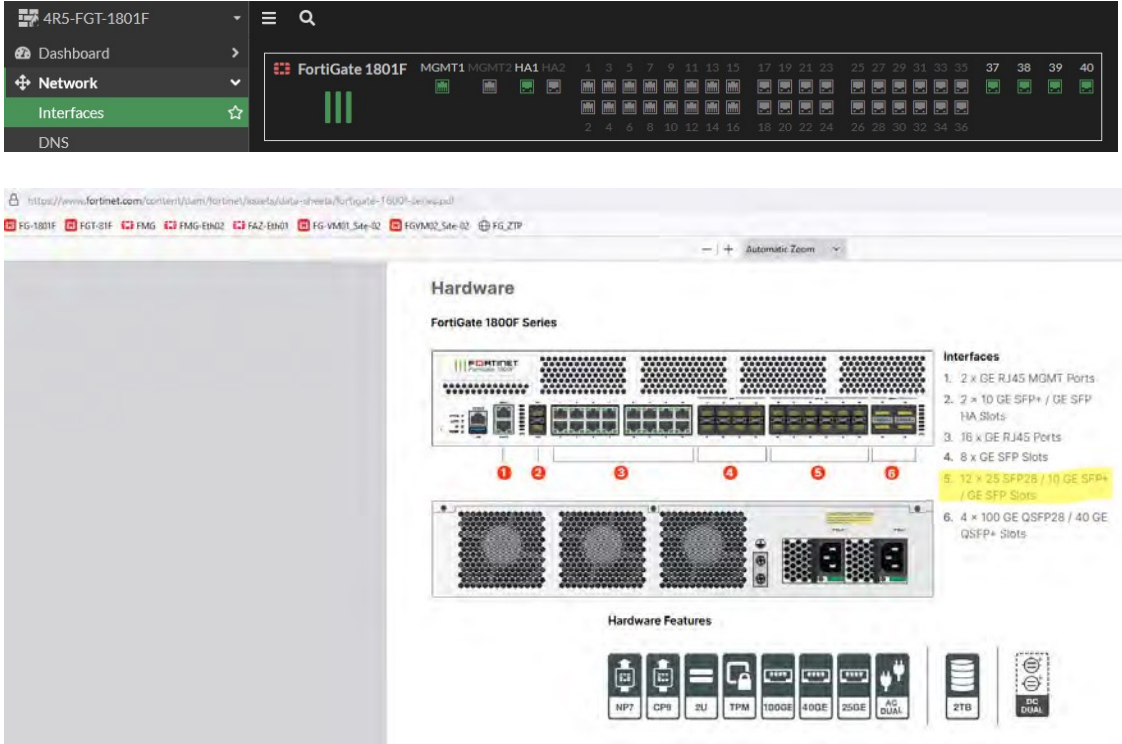
A escolha foi realizada em razão de se tratar de última versão mais estável, sendo a recomendada pelo fabricante. Além de ter sido a mais recente utilizada durante o processo de elaboração de planilha ponto a ponto no presente processo.

7. ITENS OBRIGATÓRIOS PARA TESTE DE CONFORMIDADE

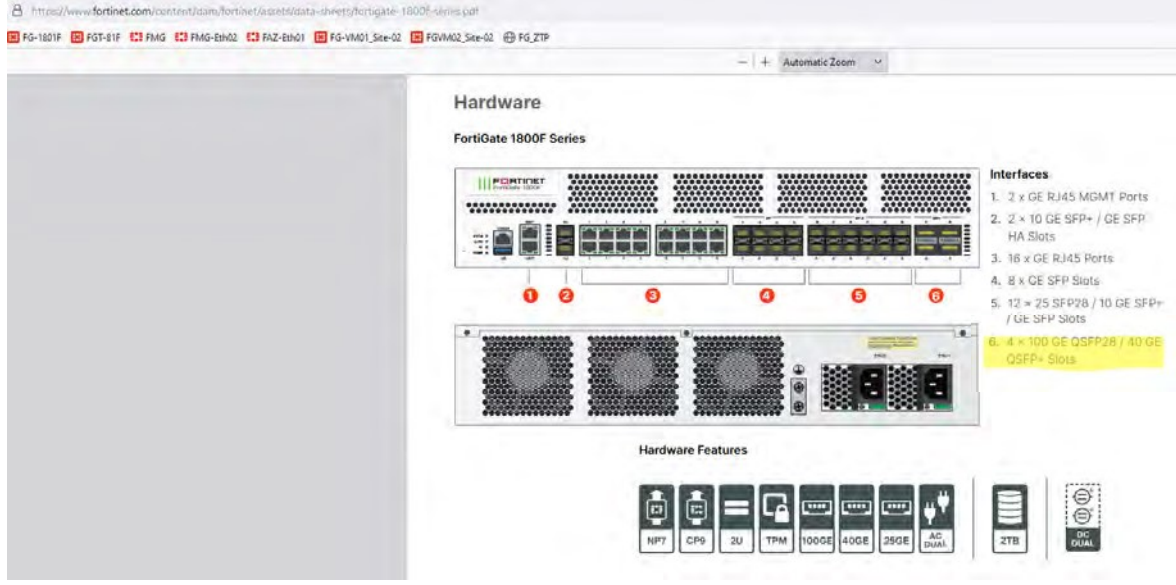
5.1 Cluster de Firewall Tipo 1

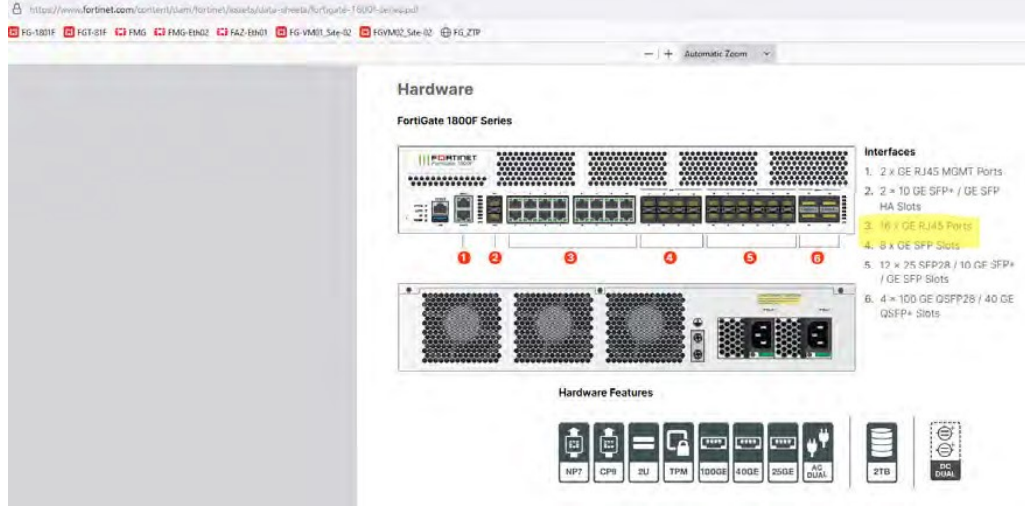
5.1.4 INTERFACES

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>TESTE OK</p>
Comentário	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1800f-series.pdf

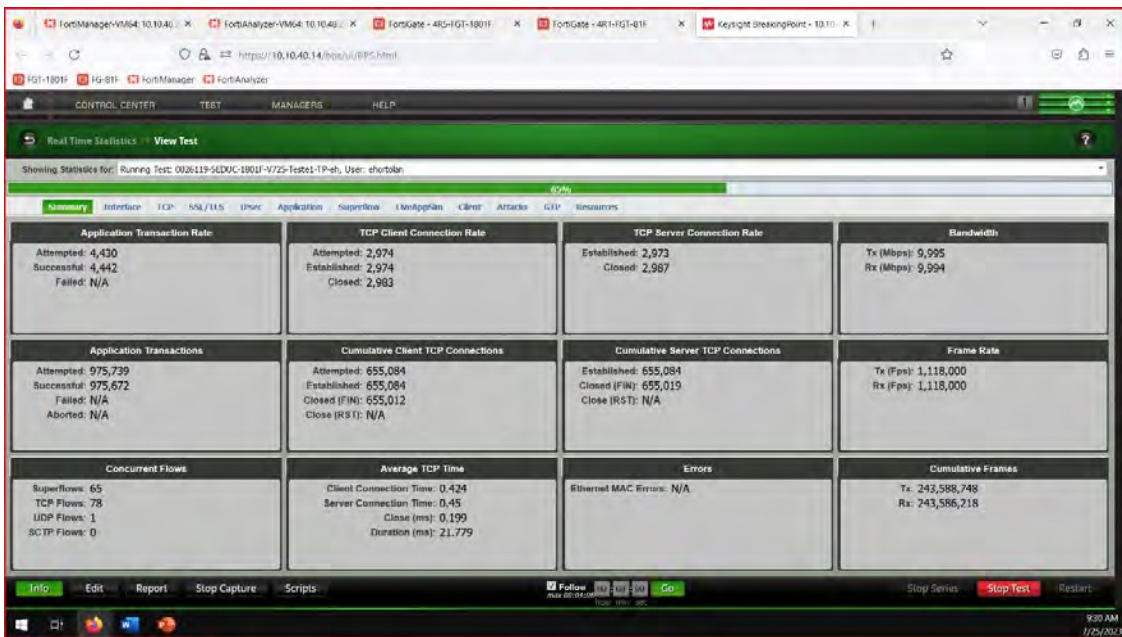
Item 5.1.4.2	Possuir no mínimo 02 (duas) interfaces 40 Gigabit QSFP+ (ou superior)
Objetivo do Teste	Validar se o appliance possui 02 (duas) interfaces de 40 Gigabit QSFP+ (ou superior)
Configuração do Teste	Validar que o equipamento possui 02 interfaces de 40 Gigabit QSFP+
Procedimento do Teste	Visual e comprovação por datasheet

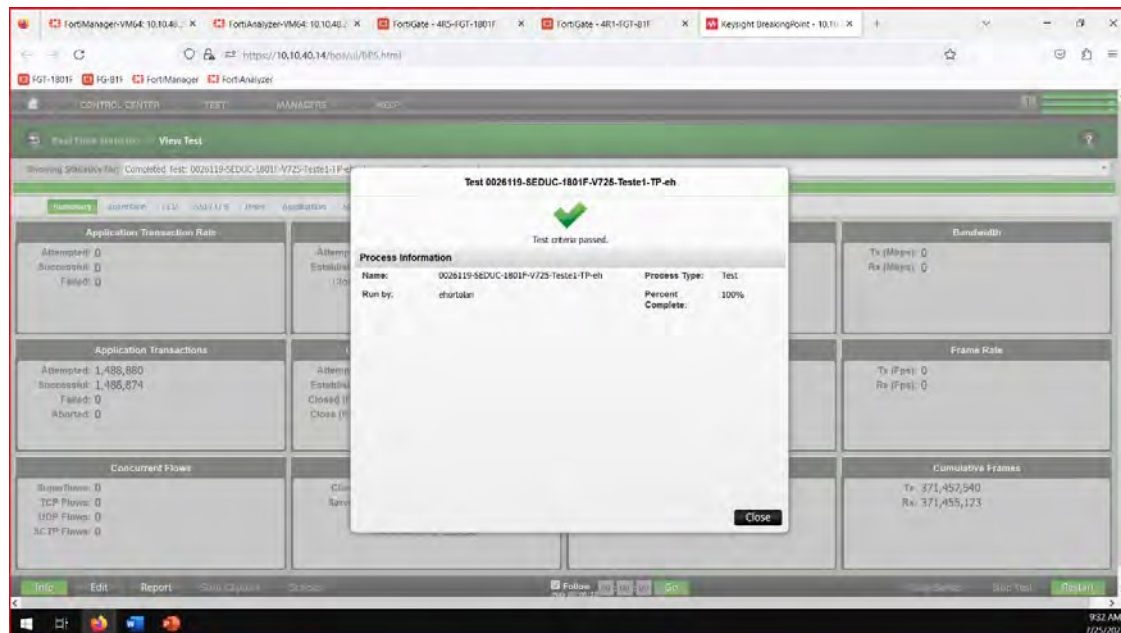
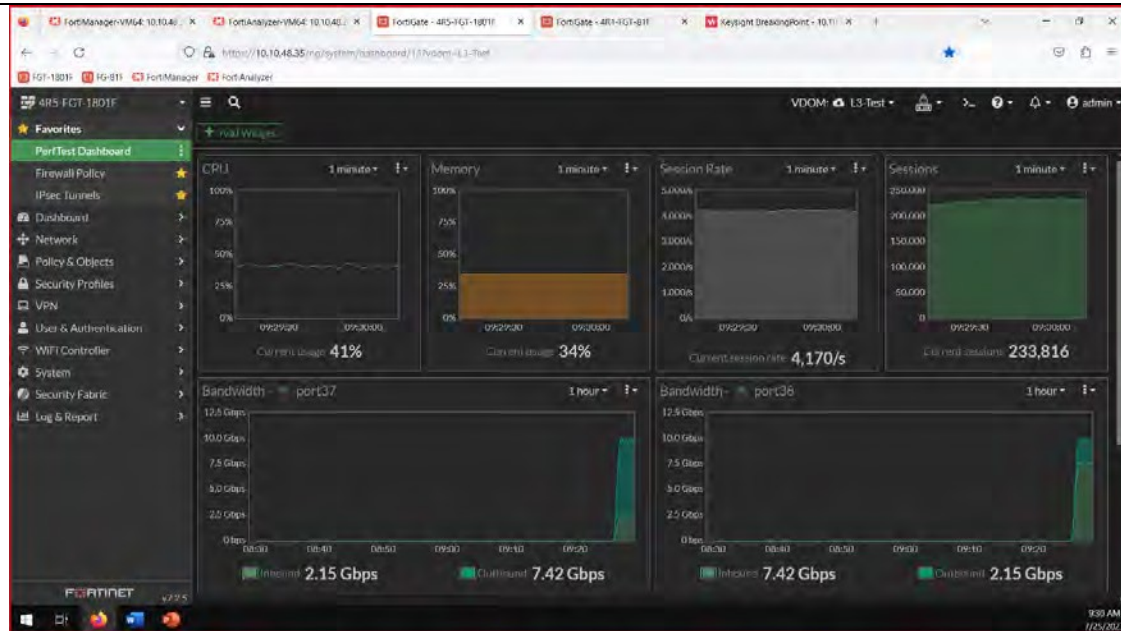
<p>Evidências</p>	 <p>TESTE OK</p>
<p>Comentário</p>	<p>https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1800f-series.pdf</p>

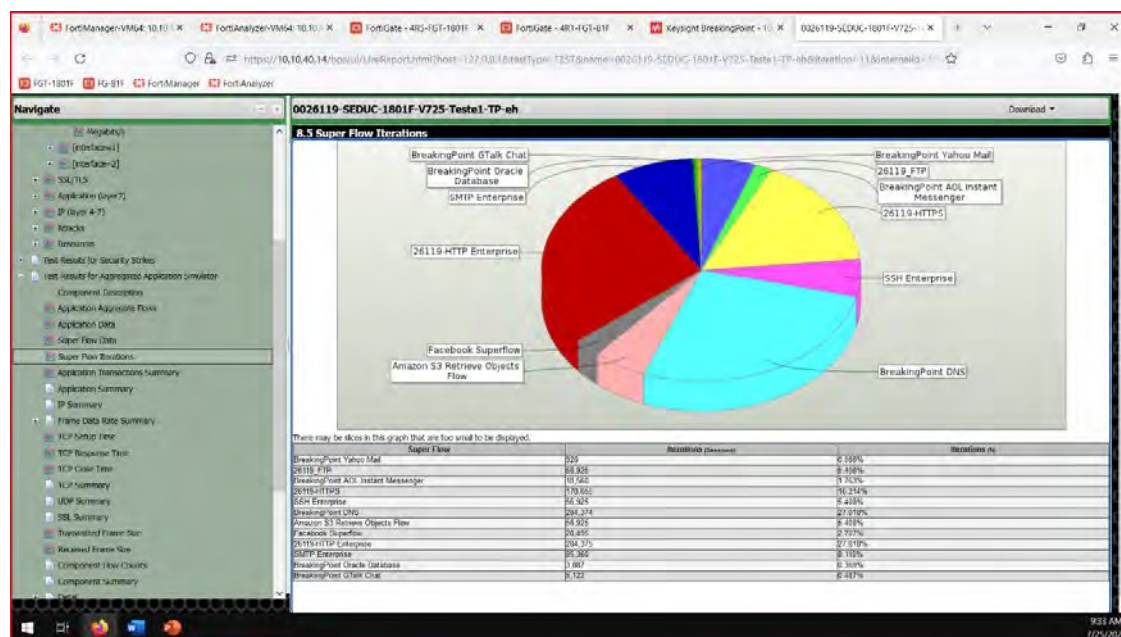
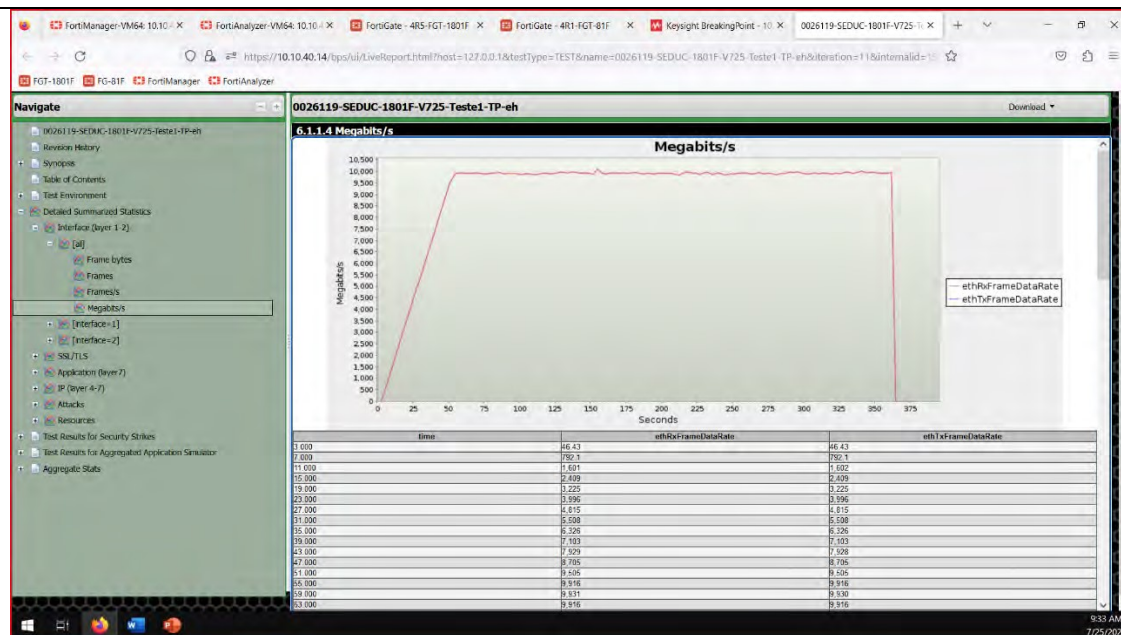
<p>Item de Teste 5.1.4.3</p>	<p>Possuir no mínimo 04 (quatro) interfaces RJ45 de no mínimo 1 Gigabit</p>
<p>Objetivo do Teste</p>	<p>Validar se o appliance possui no mínimo 04 interfaces RJ45 de no mínimo 1GB</p>
<p>Configuração do Teste</p>	<p>Validar que o equipamento possui 04 interfaces RJ45 1 Gigabit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

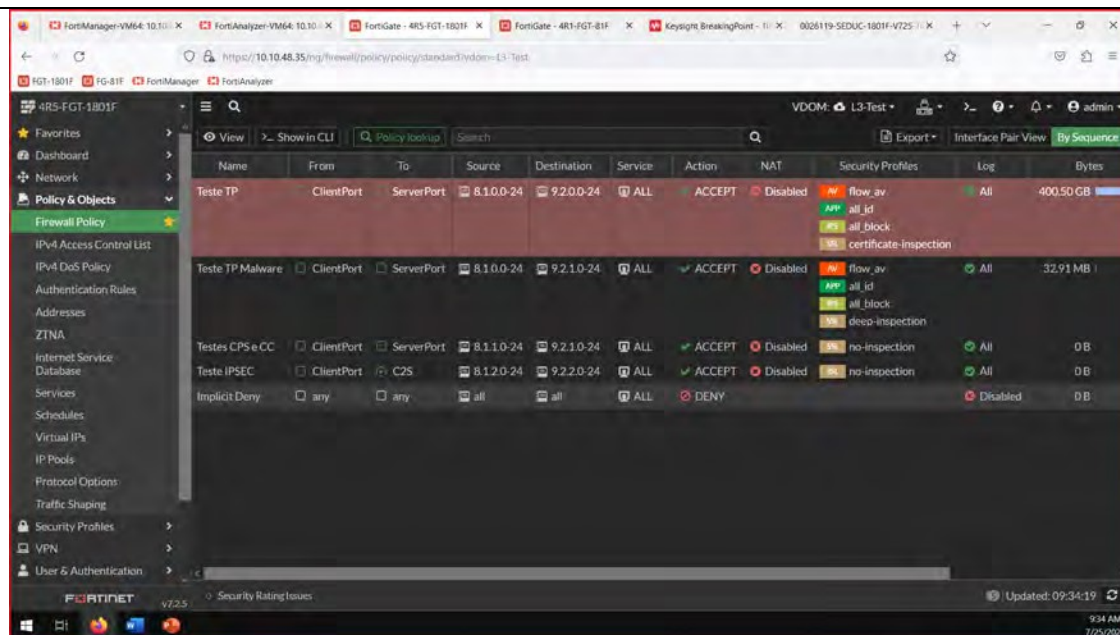
	TESTE OK
Comentário	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate-1800f-series.pdf

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. 

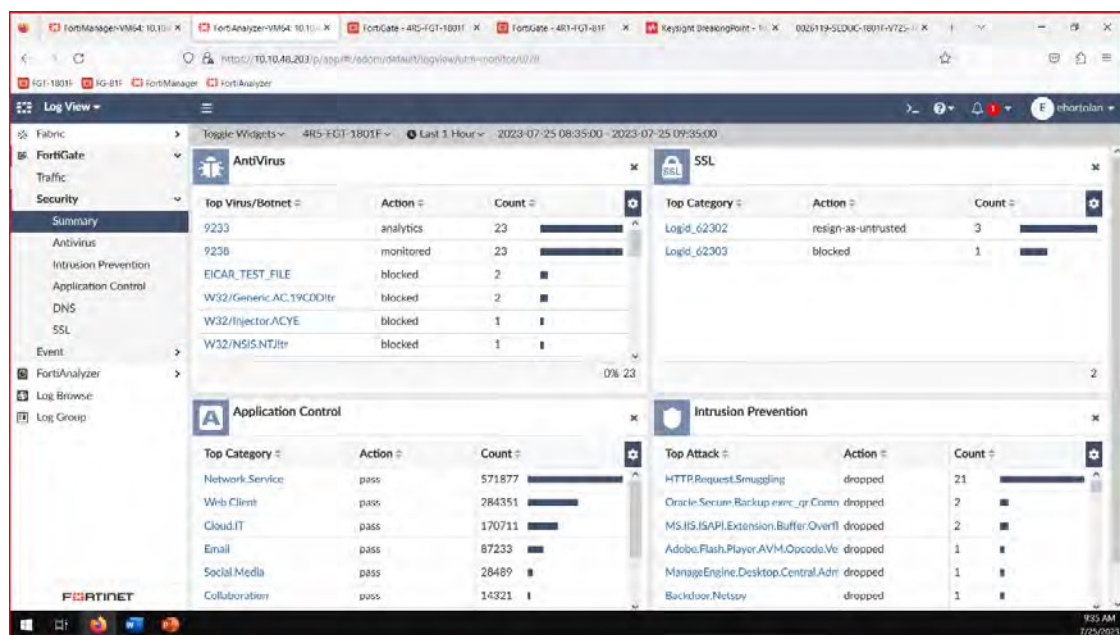






The screenshot shows the FortiAnalyzer interface for configuring a Firewall Policy. The left sidebar contains navigation options like Dashboard, Network, Policy & Objects, and Security Profiles. The main area displays a table of firewall policies.

Name	From	To	Source	Destination	Service	Action	NAT	Security Profiles	Log	Bytes
Teste TP	ClientPort	ServerPort	8.1.0.0/24	9.2.0.0/24	ALL	ACCEPT	Disabled	flow_av, all_id, all_block, certificate-inspection	All	400.50 GB
Teste TP Malware	ClientPort	ServerPort	8.1.0.0/24	9.2.1.0/24	ALL	ACCEPT	Disabled	flow_av, all_id, all_block, deep-inspection	All	32.91 MB
Testes CPS e CC	ClientPort	ServerPort	8.1.1.0/24	9.2.1.0/24	ALL	ACCEPT	Disabled	no-inspection	All	0 B
Teste IPSEC	ClientPort	C2S	8.1.2.0/24	9.2.2.0/24	ALL	ACCEPT	Disabled	no-inspection	All	0 B
Implicit Deny	any	any	all	all	ALL	DENY			Disabled	0 B



The screenshot shows the FortiAnalyzer Log View page with various security event widgets. The left sidebar shows navigation options like Fabric, FortiGate, Traffic, Security, and FortiAnalyzer. The main area displays several widgets:

- AntiVirus:** Shows top virus/botnet detections.

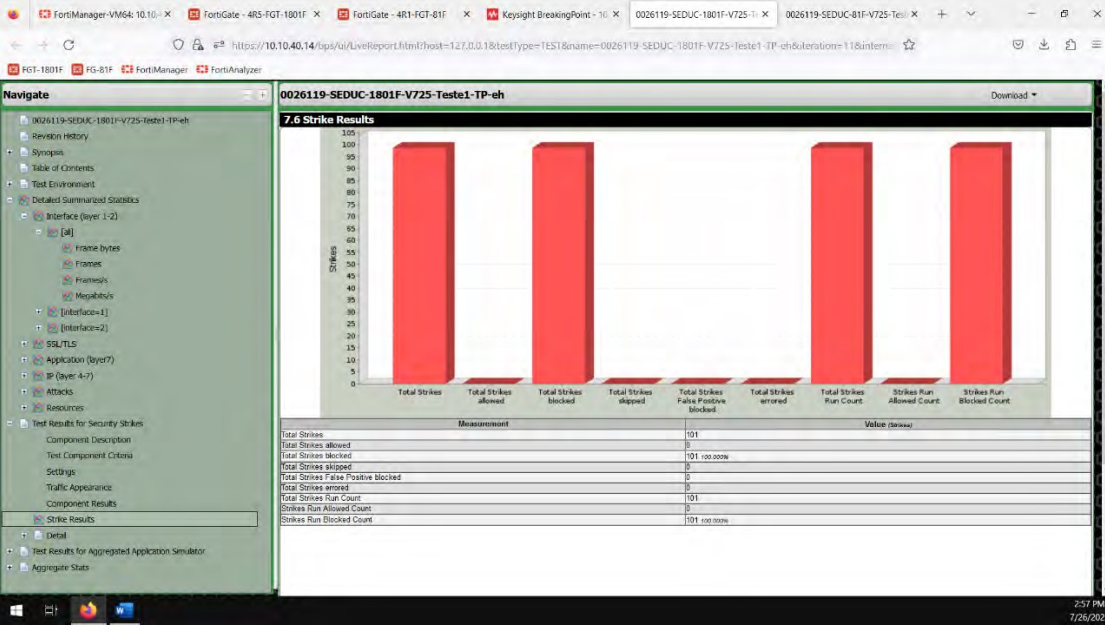
Top Virus/Botnet	Action	Count
9233	analytics	23
9238	monitored	23
EICAR_TEST_FILE	blocked	2
W32/Generic.AC.19C001tr	blocked	2
W32/Injector.AC.YE	blocked	1
W32/NSIS.NTJ1tr	blocked	1
- SSL:** Shows top SSL categories.

Top Category	Action	Count
Logid_62302	resign-as-untrusted	3
Logid_62303	blocked	1
- Application Control:** Shows top application categories.

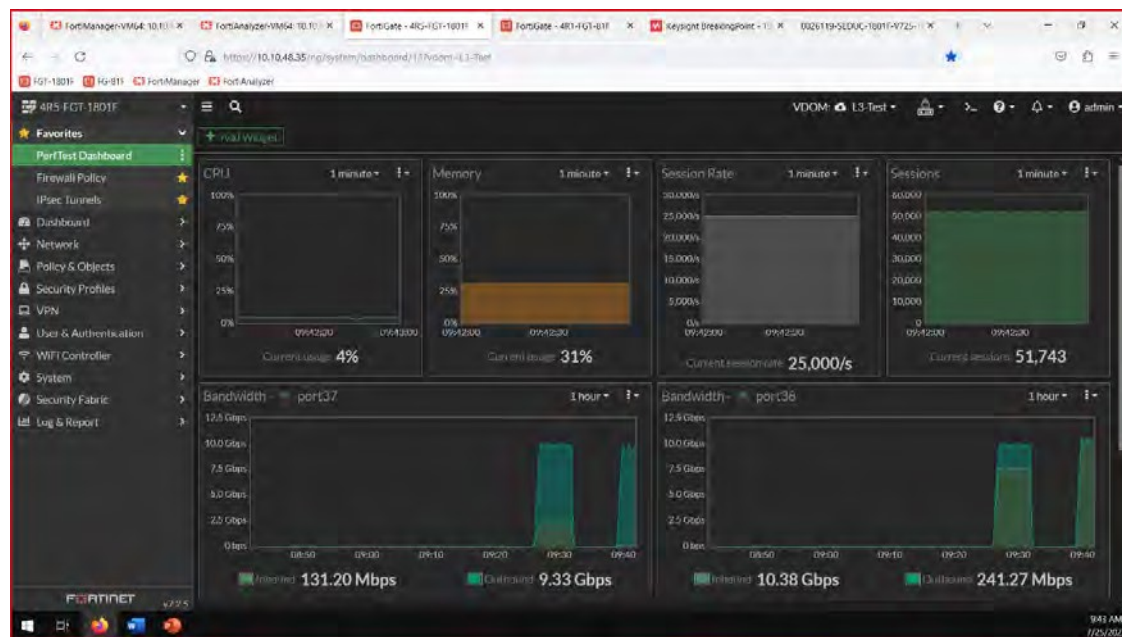
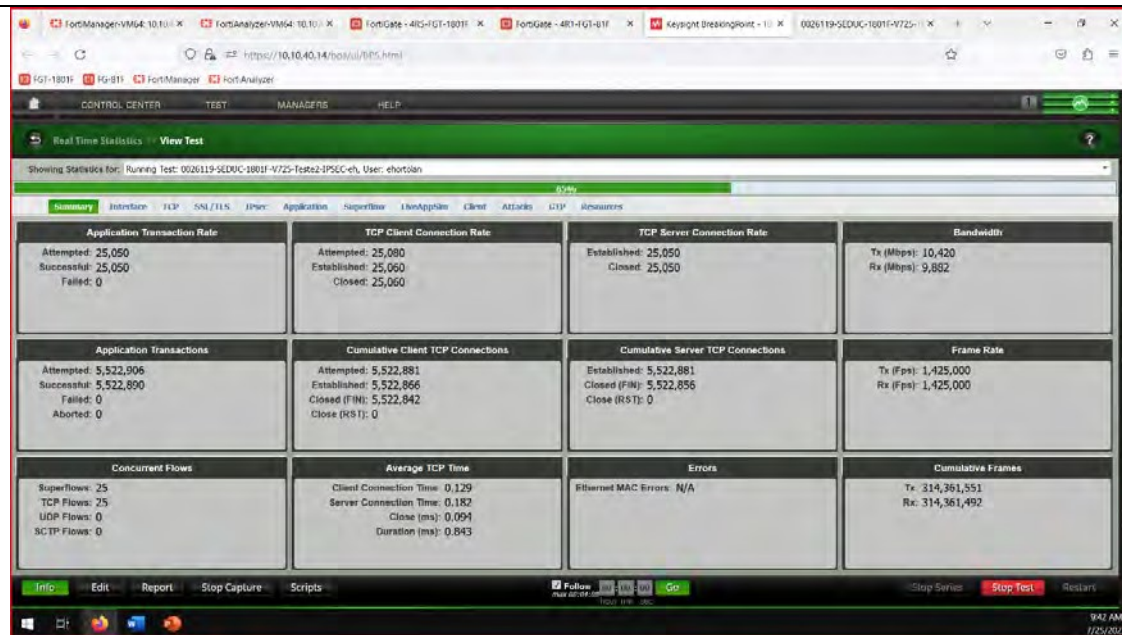
Top Category	Action	Count
Network.Service	pass	571877
Web Client	pass	284351
Cloud.IT	pass	170711
Email	pass	87233
Social.Media	pass	28489
Collaboration	pass	14321
- Intrusion Prevention:** Shows top attacks.

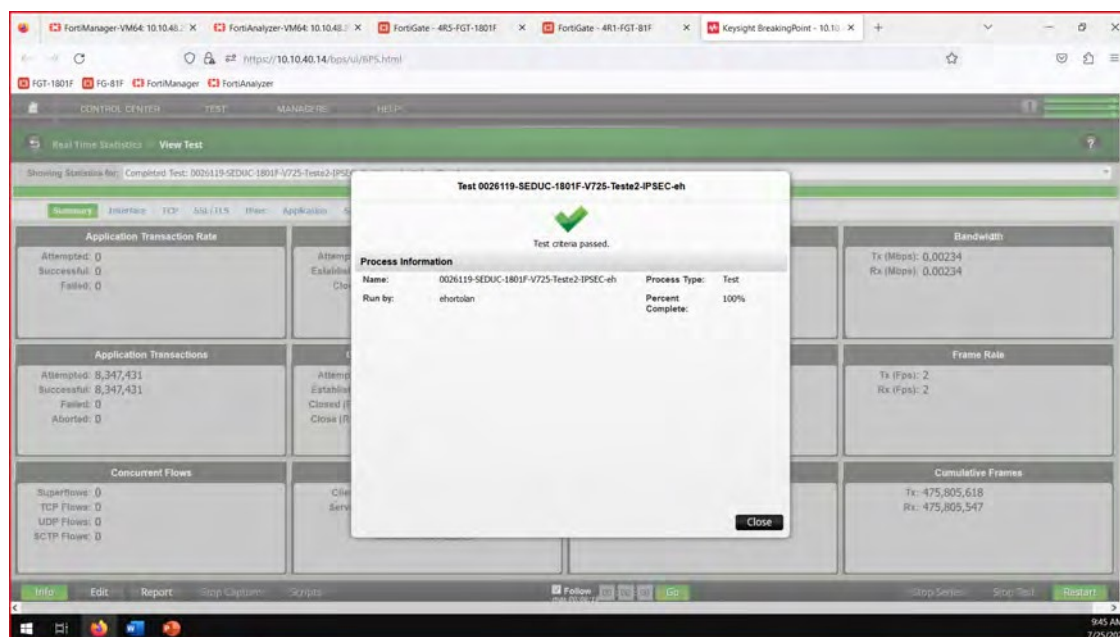
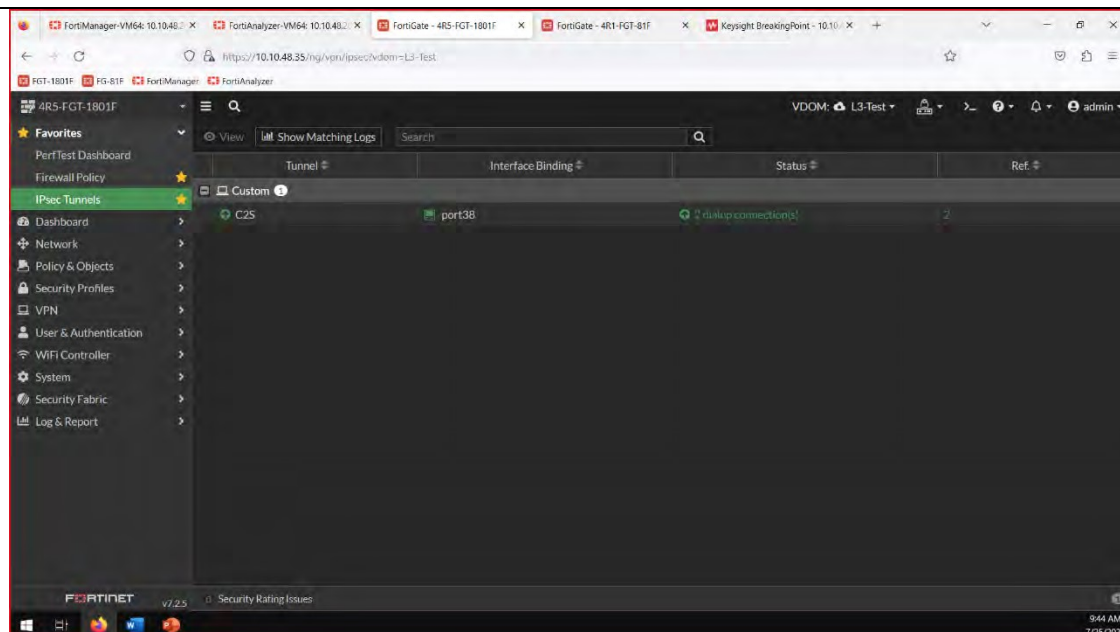
Top Attack	Action	Count
HTTP.Request.Smuggling	dropped	21
Oracle.Secur.Backup.exec_cp.Comn	dropped	2
MS.IIS.ISAPI.Extension.Buffer.Overfl	dropped	2
Adobe.Flash.Player.AVM.Opocods.Ve	dropped	1
ManageEngine.Desktop.Central.Admi	dropped	1
Backdoor.Netspy	dropped	1

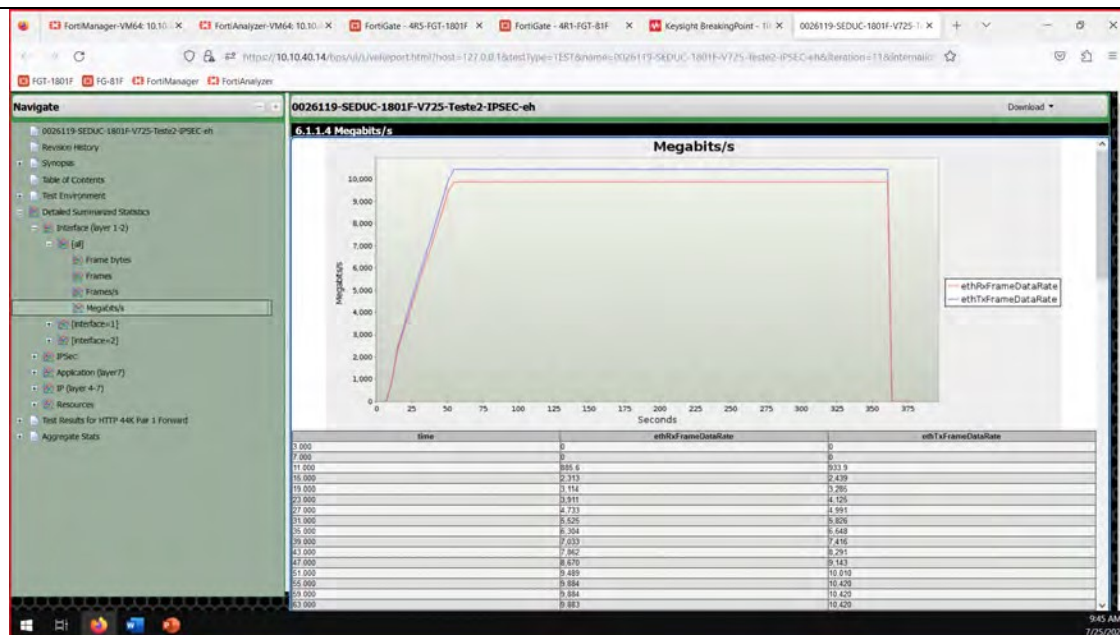
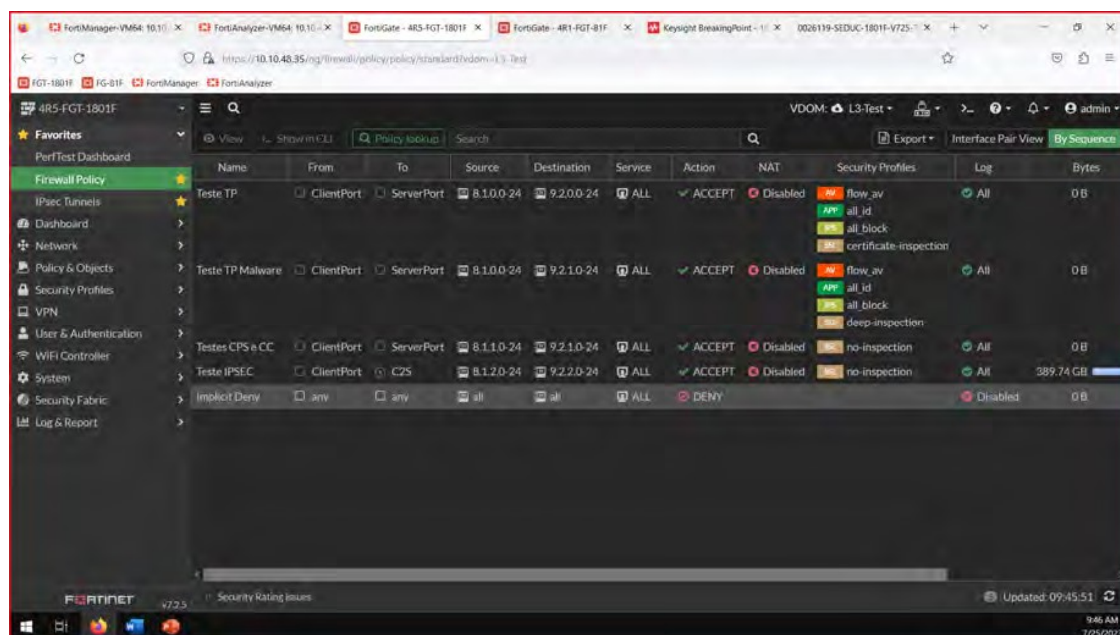
SETOR BANCÁRIO SUL - QUADRA 2 - EDIFÍCIO JOÃO CARLOS SAAD - 8º ANDAR - CEP 70.070-120 - ASA SUL - BRASÍLIA/DF

	 <p>7.6 Strike Results</p> <table border="1"> <thead> <tr> <th>Measurement</th> <th>Value (max)</th> </tr> </thead> <tbody> <tr> <td>Total Strikes</td> <td>101</td> </tr> <tr> <td>Total Strikes allowed</td> <td>0</td> </tr> <tr> <td>Total Strikes blocked</td> <td>0</td> </tr> <tr> <td>Total Strikes skipped</td> <td>0</td> </tr> <tr> <td>Total Strikes False Positive Blocked</td> <td>0</td> </tr> <tr> <td>Total Strikes ignored</td> <td>0</td> </tr> <tr> <td>Total Strikes Run Count</td> <td>101</td> </tr> <tr> <td>Strikes Run Allowed Count</td> <td>0</td> </tr> <tr> <td>Strikes Run Blocked Count</td> <td>0</td> </tr> </tbody> </table> <p>TESTE OK</p>	Measurement	Value (max)	Total Strikes	101	Total Strikes allowed	0	Total Strikes blocked	0	Total Strikes skipped	0	Total Strikes False Positive Blocked	0	Total Strikes ignored	0	Total Strikes Run Count	101	Strikes Run Allowed Count	0	Strikes Run Blocked Count	0
Measurement	Value (max)																				
Total Strikes	101																				
Total Strikes allowed	0																				
Total Strikes blocked	0																				
Total Strikes skipped	0																				
Total Strikes False Positive Blocked	0																				
Total Strikes ignored	0																				
Total Strikes Run Count	101																				
Strikes Run Allowed Count	0																				
Strikes Run Blocked Count	0																				
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	<p>Teste a ser realizado no laboratório Fortinet.</p> <p>Será apresentado o perfil de tráfego que será gerado e submetido ao appliance em teste.</p>
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.





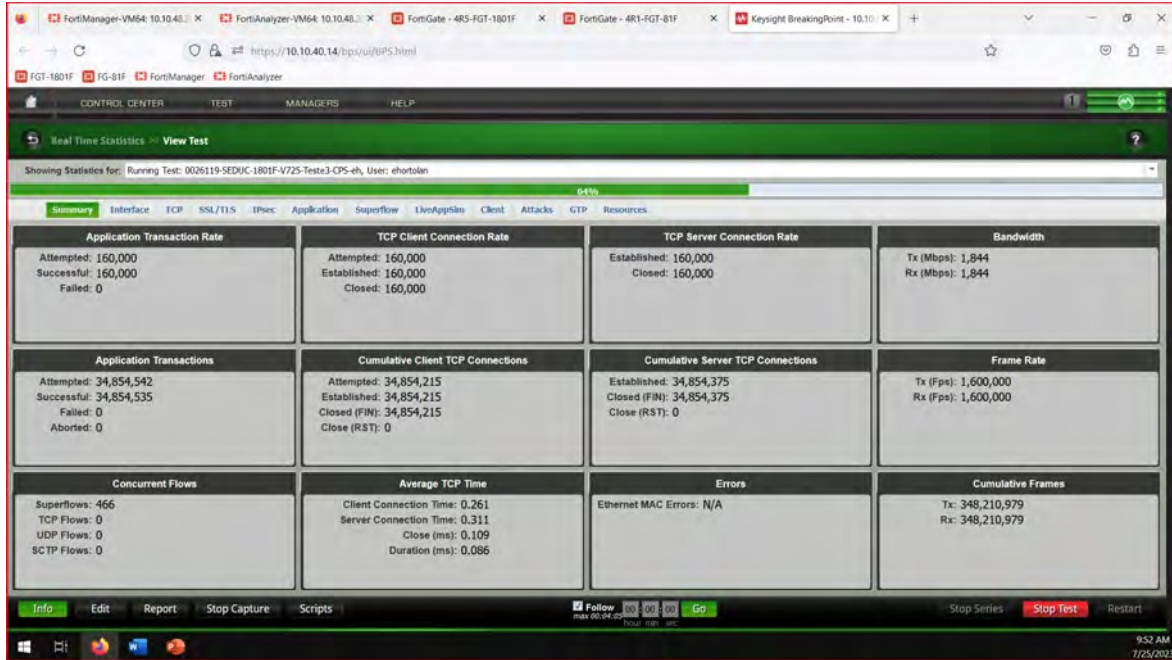
Name	From	To	Source	Destination	Service	Action	NAT	Security Profiles	Log	Bytes
Teste TP	ClientPort	ServerPort	8.1.0.0/24	9.2.0.0/24	ALL	ACCEPT	Disabled	flow_av, all_id, all_block, certificate-inspection	All	0 B
Teste TP Malware	ClientPort	ServerPort	8.1.0.0/24	9.2.1.0/24	ALL	ACCEPT	Disabled	flow_av, all_id, all_block, deep-inspection	All	0 B
Testes CPS e CC	ClientPort	ServerPort	8.1.1.0/24	9.2.1.0/24	ALL	ACCEPT	Disabled	no-inspection	All	0 B
Teste IPSEC	ClientPort	C2S	8.1.2.0/24	9.2.2.0/24	ALL	ACCEPT	Disabled	no-inspection	All	389.74 GB
Implicit Deny	any	any	all	all	ALL	DENY			Disabled	0 B

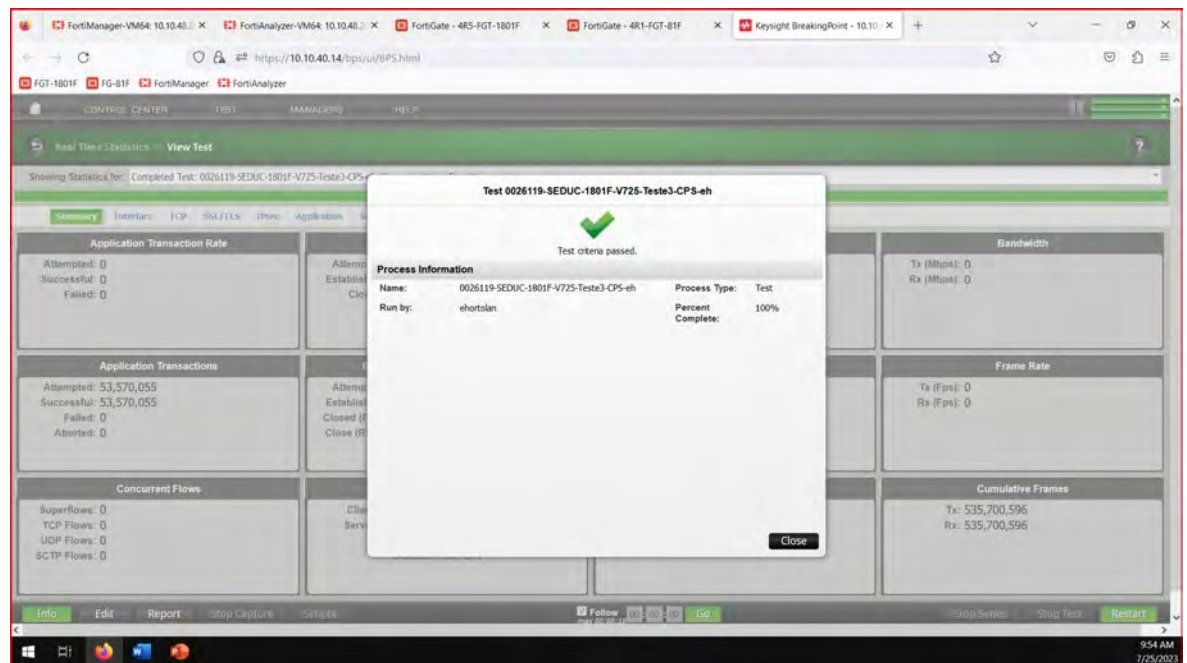
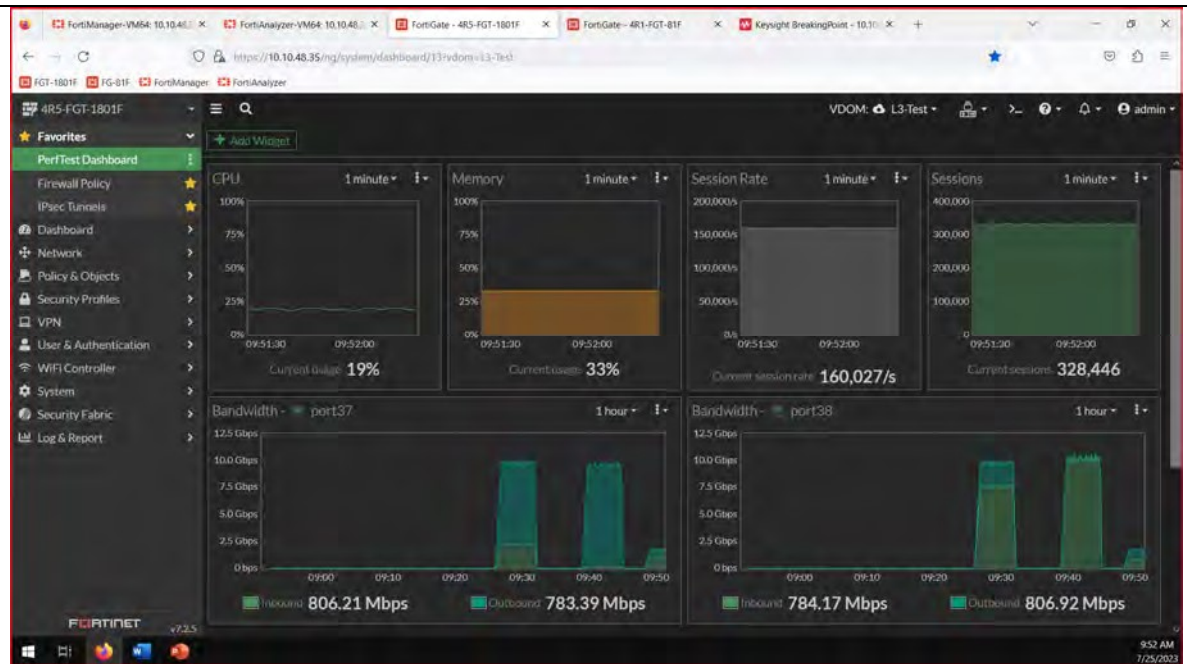
TESTE OK

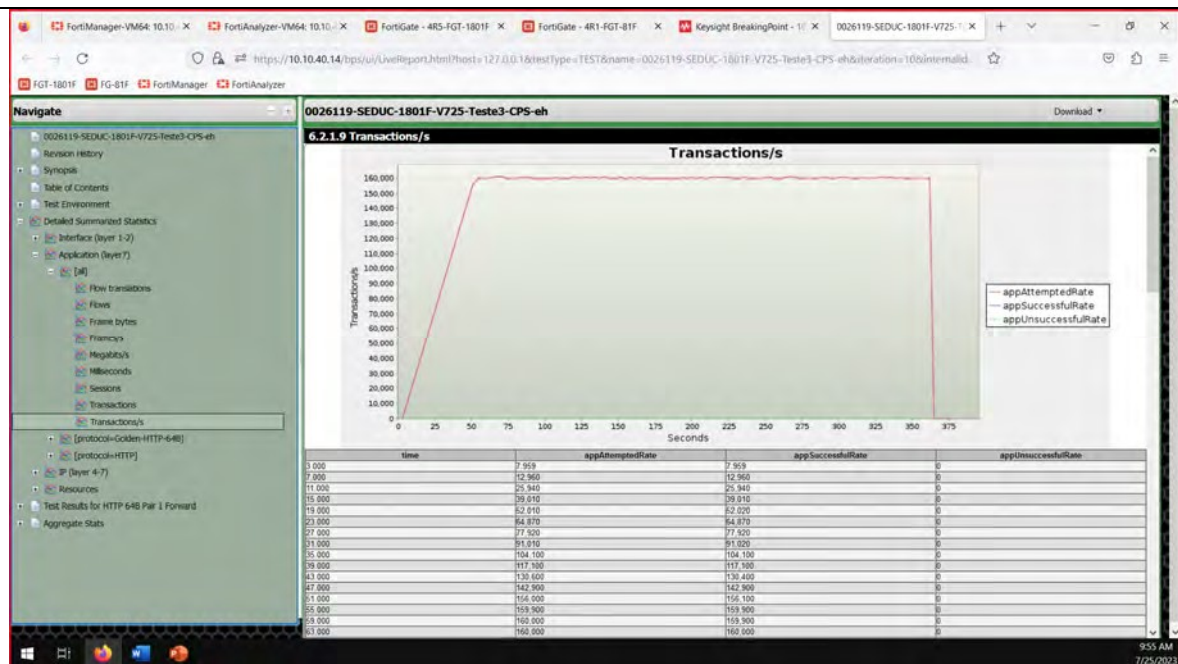
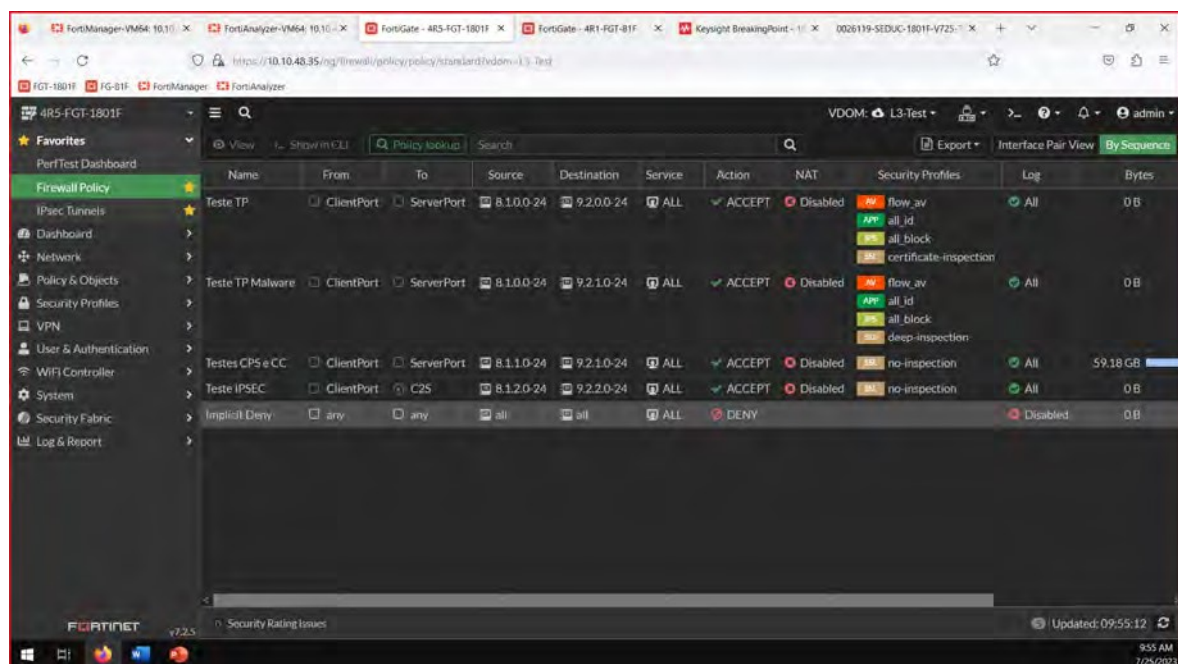
Comentário

5.1.6 CONEXÕES

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

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.  <p>The screenshot displays the FortiAnalyzer 'Real Time Statistics' interface for a test named 'Running Test: 0026119-SEDUC-1801F-V725-Teste3-CPS-eh, User: ehortalan'. The test is running at 64%. The statistics are as follows:</p> <table border="1"> <thead> <tr> <th>Application Transaction Rate</th> <th>TCP Client Connection Rate</th> <th>TCP Server Connection Rate</th> <th>Bandwidth</th> </tr> </thead> <tbody> <tr> <td>Attempted: 160,000 Successful: 160,000 Failed: 0</td> <td>Attempted: 160,000 Established: 160,000 Closed: 160,000</td> <td>Established: 160,000 Closed: 160,000</td> <td>Tx (Mbps): 1,844 Rx (Mbps): 1,844</td> </tr> <tr> <th>Application Transactions</th> <th>Cumulative Client TCP Connections</th> <th>Cumulative Server TCP Connections</th> <th>Frame Rate</th> </tr> <tr> <td>Attempted: 34,854,542 Successful: 34,854,535 Failed: 0 Aborted: 0</td> <td>Attempted: 34,854,215 Established: 34,854,215 Closed (FIN): 34,854,215 Close (RST): 0</td> <td>Established: 34,854,375 Closed (FIN): 34,854,375 Close (RST): 0</td> <td>Tx (Fps): 1,600,000 Rx (Fps): 1,600,000</td> </tr> <tr> <th>Concurrent Flows</th> <th>Average TCP Time</th> <th>Errors</th> <th>Cumulative Frames</th> </tr> <tr> <td>Superflows: 466 TCP Flows: 0 UDP Flows: 0 SCTP Flows: 0</td> <td>Client Connection Time: 0.261 Server Connection Time: 0.311 Close (ms): 0.109 Duration (ms): 0.086</td> <td>Ethernet MAC Errors: N/A</td> <td>Tx: 348,210,979 Rx: 348,210,979</td> </tr> </tbody> </table>	Application Transaction Rate	TCP Client Connection Rate	TCP Server Connection Rate	Bandwidth	Attempted: 160,000 Successful: 160,000 Failed: 0	Attempted: 160,000 Established: 160,000 Closed: 160,000	Established: 160,000 Closed: 160,000	Tx (Mbps): 1,844 Rx (Mbps): 1,844	Application Transactions	Cumulative Client TCP Connections	Cumulative Server TCP Connections	Frame Rate	Attempted: 34,854,542 Successful: 34,854,535 Failed: 0 Aborted: 0	Attempted: 34,854,215 Established: 34,854,215 Closed (FIN): 34,854,215 Close (RST): 0	Established: 34,854,375 Closed (FIN): 34,854,375 Close (RST): 0	Tx (Fps): 1,600,000 Rx (Fps): 1,600,000	Concurrent Flows	Average TCP Time	Errors	Cumulative Frames	Superflows: 466 TCP Flows: 0 UDP Flows: 0 SCTP Flows: 0	Client Connection Time: 0.261 Server Connection Time: 0.311 Close (ms): 0.109 Duration (ms): 0.086	Ethernet MAC Errors: N/A	Tx: 348,210,979 Rx: 348,210,979
Application Transaction Rate	TCP Client Connection Rate	TCP Server Connection Rate	Bandwidth																						
Attempted: 160,000 Successful: 160,000 Failed: 0	Attempted: 160,000 Established: 160,000 Closed: 160,000	Established: 160,000 Closed: 160,000	Tx (Mbps): 1,844 Rx (Mbps): 1,844																						
Application Transactions	Cumulative Client TCP Connections	Cumulative Server TCP Connections	Frame Rate																						
Attempted: 34,854,542 Successful: 34,854,535 Failed: 0 Aborted: 0	Attempted: 34,854,215 Established: 34,854,215 Closed (FIN): 34,854,215 Close (RST): 0	Established: 34,854,375 Closed (FIN): 34,854,375 Close (RST): 0	Tx (Fps): 1,600,000 Rx (Fps): 1,600,000																						
Concurrent Flows	Average TCP Time	Errors	Cumulative Frames																						
Superflows: 466 TCP Flows: 0 UDP Flows: 0 SCTP Flows: 0	Client Connection Time: 0.261 Server Connection Time: 0.311 Close (ms): 0.109 Duration (ms): 0.086	Ethernet MAC Errors: N/A	Tx: 348,210,979 Rx: 348,210,979																						

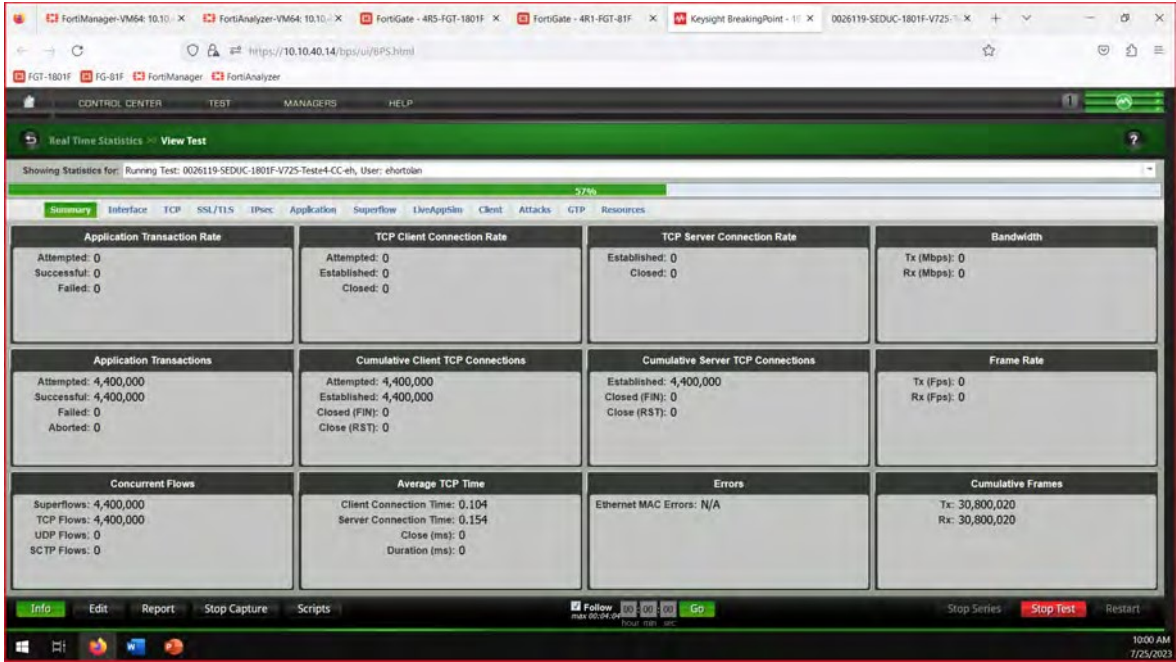


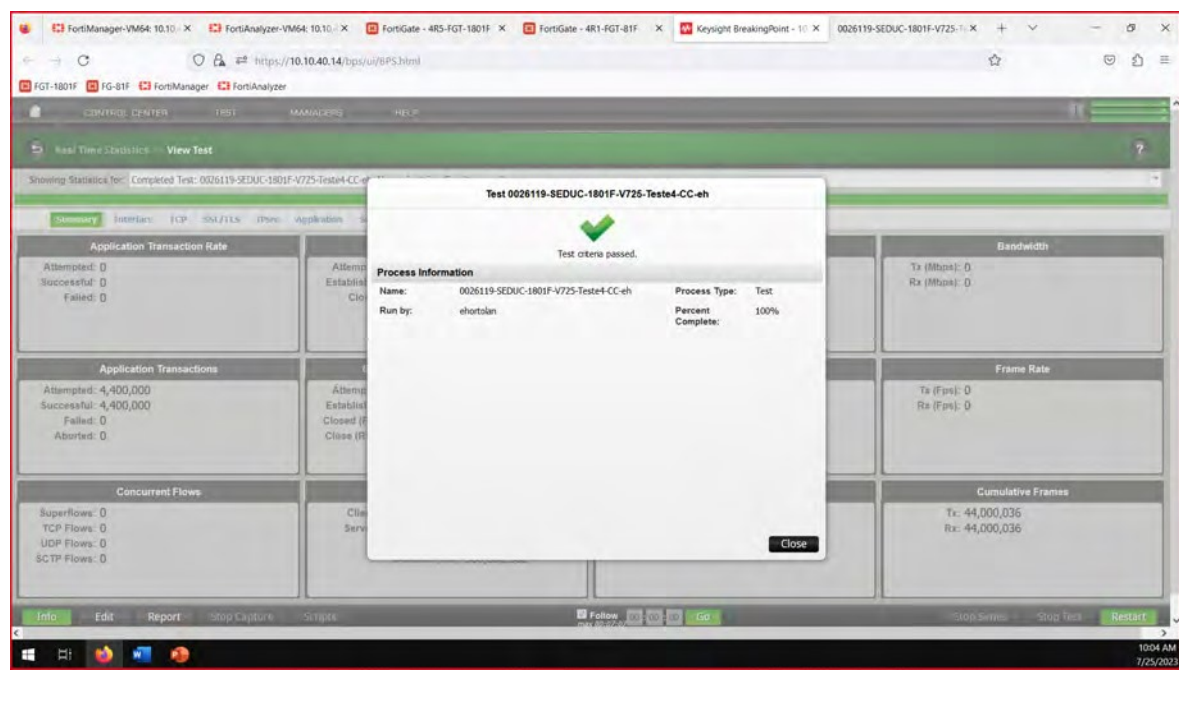
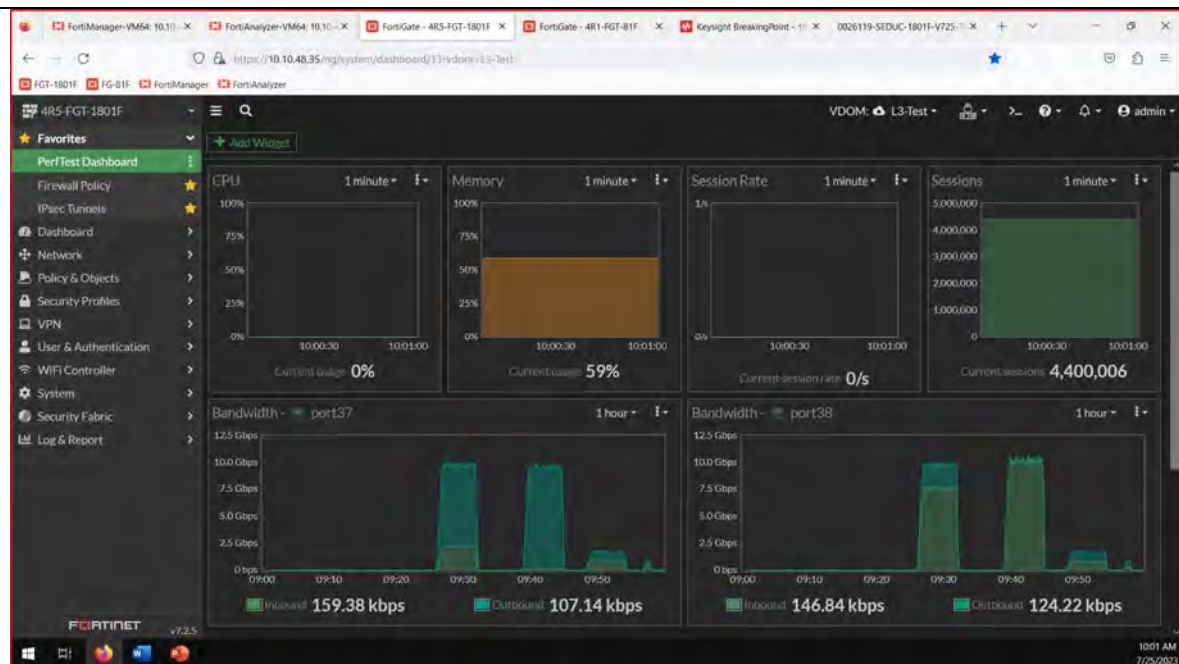



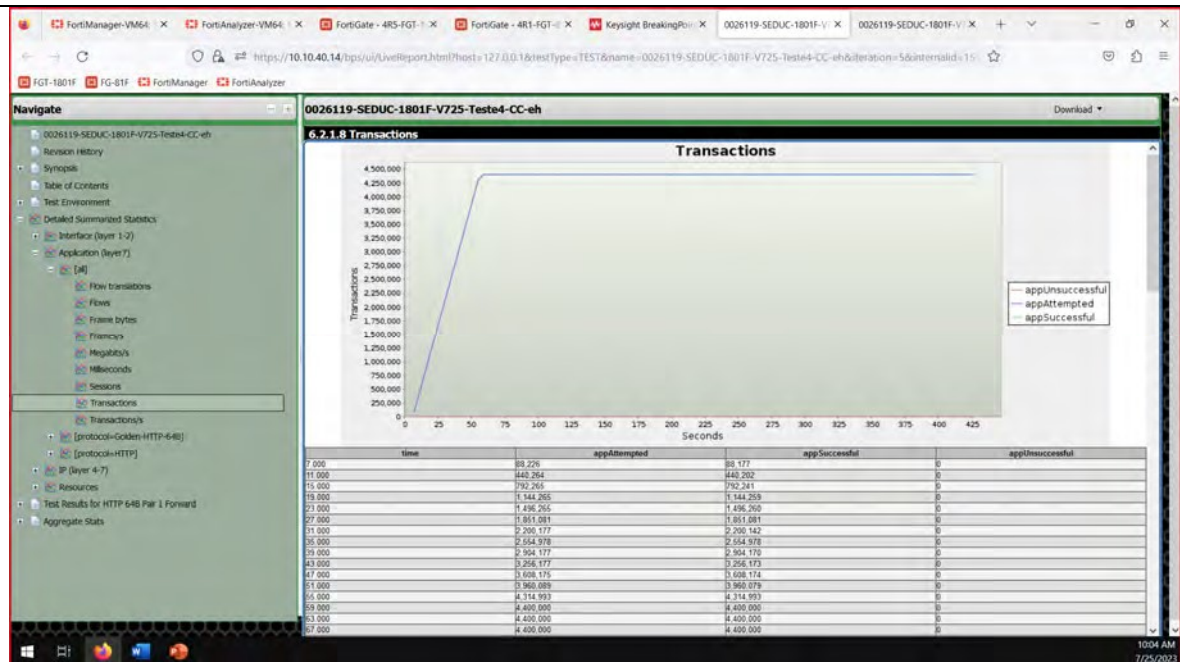
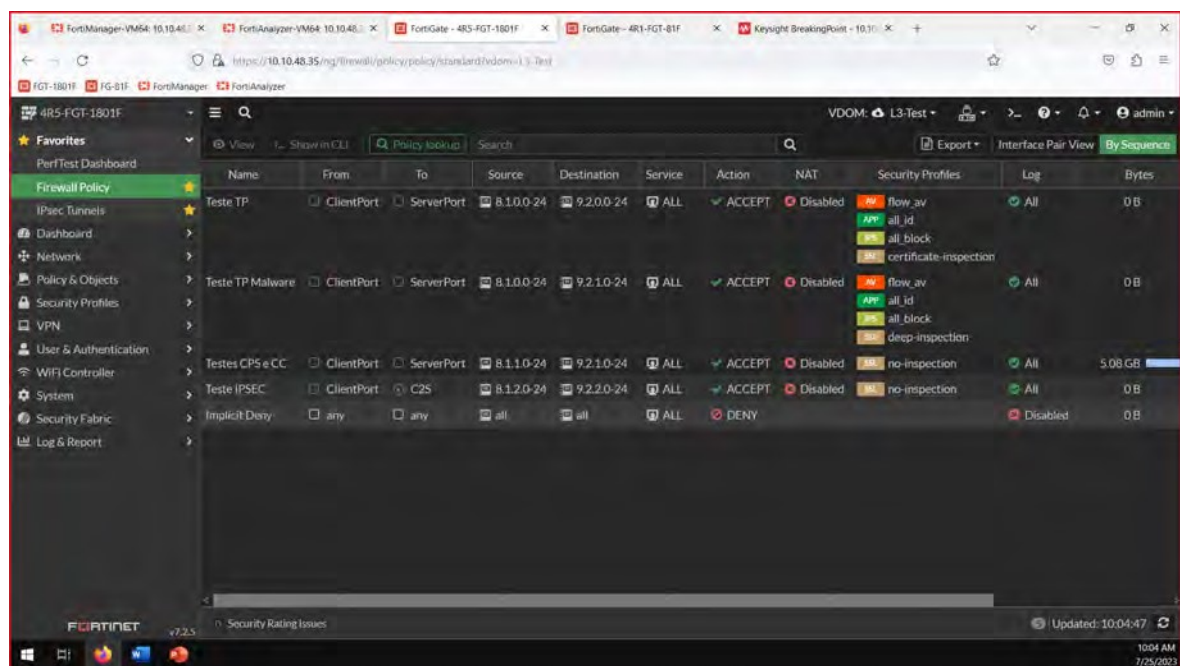
Name	From	To	Source	Destination	Service	Action	NAT	Security Profiles	Log	Bytes
Teste TP	ClientPort	ServerPort	8.1.0.0-24	9.2.0.0-24	ALL	ACCEPT	Disabled	flow_av, all_id, all_block, certificate-inspection	All	0 B
Teste TP Malware	ClientPort	ServerPort	8.1.0.0-24	9.2.1.0-24	ALL	ACCEPT	Disabled	flow_av, all_id, all_block, deep-inspection	All	0 B
Testes CPS e CC	ClientPort	ServerPort	8.1.1.0-24	9.2.1.0-24	ALL	ACCEPT	Disabled	no-inspection	All	59.18 GB
Teste IPSEC	ClientPort	C2S	8.1.2.0-24	9.2.2.0-24	ALL	ACCEPT	Disabled	no-inspection	All	0 B
Implicit Deny	any	any	all	all	ALL	DENY			Disabled	0 B

TESTE OK

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.  <p>The screenshot displays the FortiAnalyzer 'Real Time Statistics' interface for a test named 'Running Test: 0026119-SEDUC-1801F-V725-Teste4-CC-eh, User: ehorton'. The interface shows a progress bar at 57%. The 'Application Transactions' section indicates 4,400,000 attempted, successful, and aborted transactions. The 'Cumulative Client TCP Connections' section shows 4,400,000 attempted and established connections, with 0 closed (FIN) and 0 closed (RST). The 'Average TCP Time' section shows a client connection time of 0.104 and a server connection time of 0.154. The 'Cumulative Frames' section shows 30,800,020 transmitted and received frames. The 'Errors' section shows 'Ethernet MAC Errors: N/A'. The interface includes navigation tabs (Summary, Interface, TCP, etc.) and control buttons (Info, Edit, Report, Stop Capture, Scripts, Follow, Stop Test, Restart).</p>



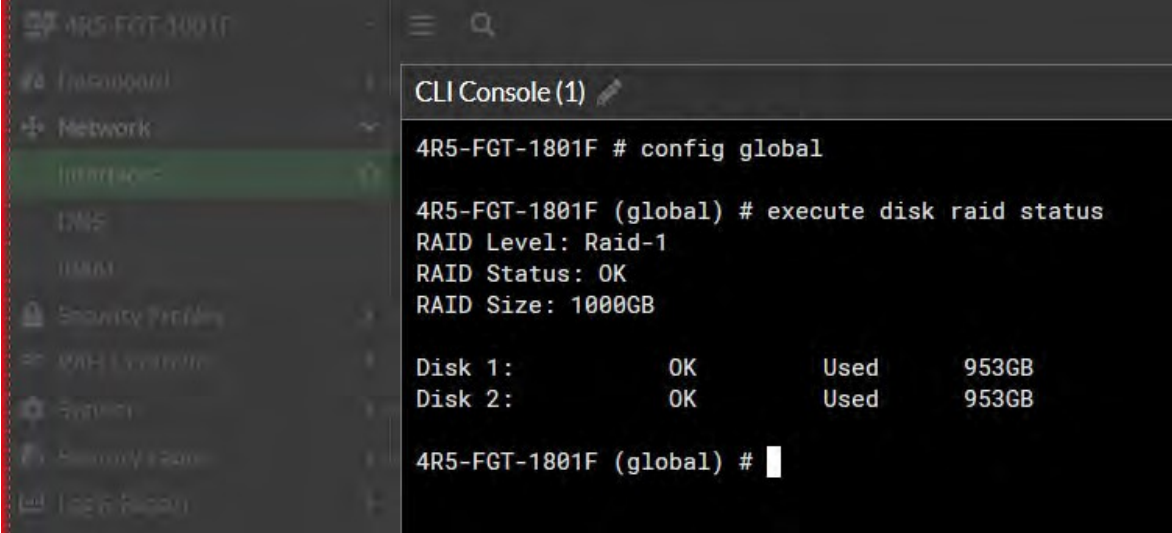



Name	From	To	Source	Destination	Service	Action	NAT	Security Profiles	Log	Bytes
Teste TP	ClientPort	ServerPort	8.1.0.0-24	9.2.0.0-24	ALL	ACCEPT	Disabled	flow_av, all_id, all_block, certificate-inspection	All	0 B
Teste TP Malware	ClientPort	ServerPort	8.1.0.0-24	9.2.1.0-24	ALL	ACCEPT	Disabled	flow_av, all_id, all_block, deep-inspection	All	0 B
Testes CPS e CC	ClientPort	ServerPort	8.1.1.0-24	9.2.1.0-24	ALL	ACCEPT	Disabled	no-inspection	All	5 08 GB
Teste IPSEC	ClientPort	C2S	8.1.2.0-24	9.2.2.0-24	ALL	ACCEPT	Disabled	no-inspection	All	0 B
Implicit Deny	any	any	all	all	ALL	DENY			Disabled	0 B

TESTE OK

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	<p>Executar comando via cli:</p> <pre>execute disk raid status</pre> <p>Certificar a saída do comando com resultado Raid Level e Status, esperado:</p> <pre># execute disk raid status</pre> <pre>RAID Level: Raid-1</pre> <pre>RAID Status: OK</pre> <pre>RAID Size:</pre>
Evidências	 <p>TESTE - OK</p>

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 2x 1 TB NVMe SSD
Trusted Platform Module (TPM)	Yes

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 delas evidenciando que uma fonte deixou de funcionar enquanto a outra continuou alimentando plenamente o equipamento.
Evidências	

```
4R5-FGT-1801F
CLI Console (1)
81 PS1 Status          alarm=0 OK
82 PS2 VIN             alarm=0 value=114 threshold_status=0
83 PS2 VOUT_12V        alarm=0 value=12.221 threshold_status=0
84 PS2 IIN              alarm=0 value=0.75 threshold_status=0
85 PS2 IOOUT_12V       alarm=0 value=8 threshold_status=0
86 PS2 POUT            alarm=0 value=96 threshold_status=0
87 PS2 Temp 1          alarm=0 value=26 threshold_status=0
88 PS2 Temp 2          alarm=0 value=23 threshold_status=0
89 PS2 Temp 3          alarm=0 value=38 threshold_status=0
90 PS2 Fan 1           alarm=0 value=1664 threshold_status=0
91 PS2 Status          alarm=0 OK

----- Extra Sensor List -----
PHY B50185->P17_P24 TEMP: 44.46(C)
PHY 88E1514->MGMT1 TEMP: 25(C)
PHY 88E1514->MGMT2 TEMP: 15(C)

4R5-FGT-1801F (global) #
4R5-FGT-1801F (global) #
4R5-FGT-1801F (global) #
4R5-FGT-1801F (global) #
4R5-FGT-1801F (global) #
4R5-FGT-1801F (global) # diag hardware deviceinfo psu
PSU 01:
  Product Manufacturer : DELTA
  Product Name         : DPS-800AB-40 B
  Product Version      : 00F
  Product Serial       : JNPD2012002532
PSU 02:
  Product Manufacturer : DELTA
  Product Name         : DPS-800AB-40 B
  Product Version      : 00F
  Product Serial       : JNPD2012002529
```



```
CLI Console (1)
61 TMP1075 U101      alarm=0 value=24 threshold_status=0
62 CPU0 DTS         alarm=0 value=42 threshold_status=0
63 CPU0 DIMM 1 Temp alarm=0 value=26 threshold_status=0
64 CPU0 DIMM 2 Temp alarm=0 value=26 threshold_status=0
65 CPU0 DIMM 3 Temp alarm=0 value=25 threshold_status=0
66 CPU0 DIMM 4 Temp alarm=0 value=26 threshold_status=0
67 CPU0 DIMM 5 Temp alarm=0 value=25 threshold_status=0
68 CPU0 DIMM 6 Temp alarm=0 value=24 threshold_status=0
69 Fan 1            alarm=0 value=5000 threshold_status=0
70 Fan 2            alarm=0 value=4900 threshold_status=0
71 Fan 3            alarm=0 value=5000 threshold_status=0
72 PS1 VIN          alarm=0 value=118 threshold_status=0
73 PS1 VOUT_12V     alarm=0 value=12.221 threshold_status=0
74 PS1 IIN          alarm=0 value=1 threshold_status=0
75 PS1 IOUT_12V     alarm=0 value=8.5 threshold_status=0
76 PS1 POUT         alarm=0 value=104 threshold_status=0
77 PS1 Temp 1       alarm=0 value=27 threshold_status=0
78 PS1 Temp 2       alarm=0 value=24 threshold_status=0
79 PS1 Temp 3       alarm=0 value=38 threshold_status=0
80 PS1 Fan 1        alarm=0 value=1664 threshold_status=0
81 PS1 Status       alarm=0 OK
82 PS2 VIN          alarm=0 value=118 threshold_status=0
83 PS2 VOUT_12V     alarm=0 value=12.221 threshold_status=0
84 PS2 IIN          alarm=0 value=0.75 threshold_status=0
85 PS2 IOUT_12V     alarm=0 value=8 threshold_status=0
86 PS2 POUT         alarm=0 value=96 threshold_status=0
87 PS2 Temp 1       alarm=0 value=26 threshold_status=0
88 PS2 Temp 2       alarm=0 value=23 threshold_status=0
89 PS2 Temp 3       alarm=0 value=38 threshold_status=0
90 PS2 Fan 1        alarm=0 value=1664 threshold_status=0
91 PS2 Status       alarm=0 OK

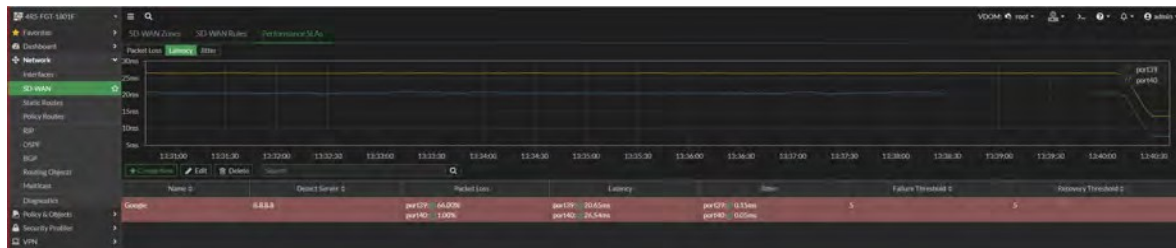
----- Extra Sensor List -----
PHY B50185->P17_P24 TEMP: 44.46(C)
PHY 88E1514->MGMT1 TEMP: 25(C)
PHY 88E1514->MGMT2 TEMP: 15(C)
```

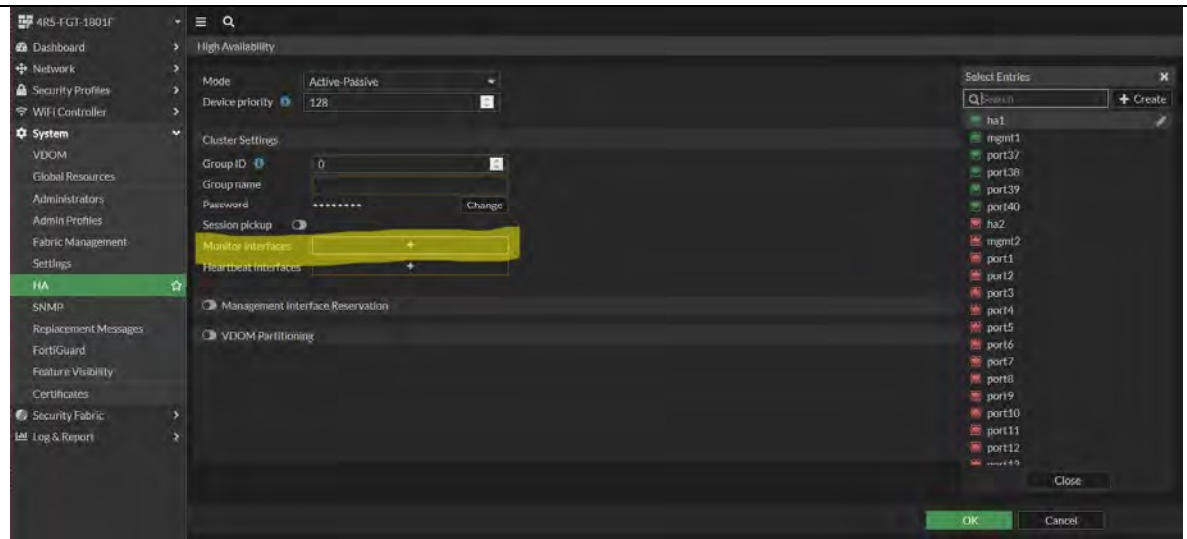
TESTE OK

Specifications	
	FG-1800F-DC FG-1801F-DC
Interfaces and Modules	
Hardware Accelerated GE RJ45 Ports	16
Hardware Accelerated GE SFP Ports	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 ¹	22 Gbps
NGFW Throughput ^{1,4}	17 Gbps
Threat Protection Throughput ^{1,5}	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)	215 Mpps
Concurrent Sessions (TCP)	12 Million / 40 Million*
New Sessions/Second (TCP)	750 000 / 2 Million*
Firewall Policies	500 000
IPsec VPN Throughput (256 byte, SPI)	44 Gbps
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 536
Weight	30.2 lbs (13.7 kg) 30.4 lbs (13.8 kg)
Form Factor (Supports EIA/EIAE standards)	Rack Mount, 2RU
AC Power Supply	100-240VAC, 3000VA
AC Current (Maximum)	7.6/10.0/15.0/20.0/24.0VAC
DC Power Supply	-48V to -60V DC
DC Current (Maximum)	20A
Power Consumption (Average / Maximum)	410.9 W / 459.1 W 434.9 W / 463.1 W
Heat Dissipation	1854.84 BTU/h 1936.70 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 (-32°–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/ULC, CB
Certifications	USGv6/IPv6

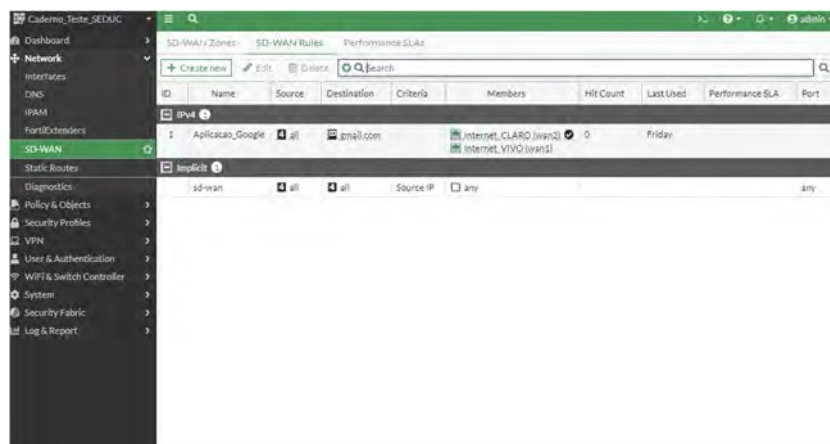
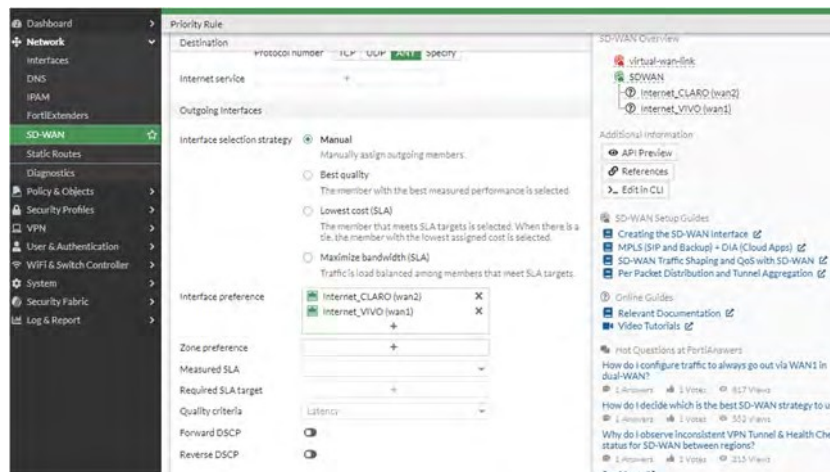
Comentário FortiGate
<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1800f-series.pdf>

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. At the top, there's a graph for 'Packet Loss' over time. Below it, a table displays the status of two links:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Object</th> <th>Server</th> <th>Packet Loss</th> <th>Latency</th> <th>Down</th> <th>Failure Threshold</th> <th>Recovery Threshold</th> </tr> </thead> <tbody> <tr> <td>Google</td> <td>6.8.8.8</td> <td>per107-64.078.net140</td> <td>0.00%</td> <td>20.65ms</td> <td>0.00ms</td> <td>5</td> <td>5</td> </tr> <tr> <td></td> <td></td> <td>per140-26.548s.net140</td> <td>1.00%</td> <td>26.54ms</td> <td>0.00ms</td> <td></td> <td></td> </tr> </tbody> </table>	Name	Object	Server	Packet Loss	Latency	Down	Failure Threshold	Recovery Threshold	Google	6.8.8.8	per107-64.078.net140	0.00%	20.65ms	0.00ms	5	5			per140-26.548s.net140	1.00%	26.54ms	0.00ms		
Name	Object	Server	Packet Loss	Latency	Down	Failure Threshold	Recovery Threshold																		
Google	6.8.8.8	per107-64.078.net140	0.00%	20.65ms	0.00ms	5	5																		
		per140-26.548s.net140	1.00%	26.54ms	0.00ms																				



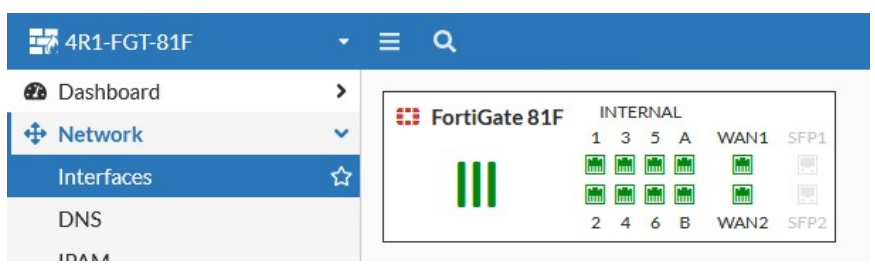
TESTE OK



Comentário

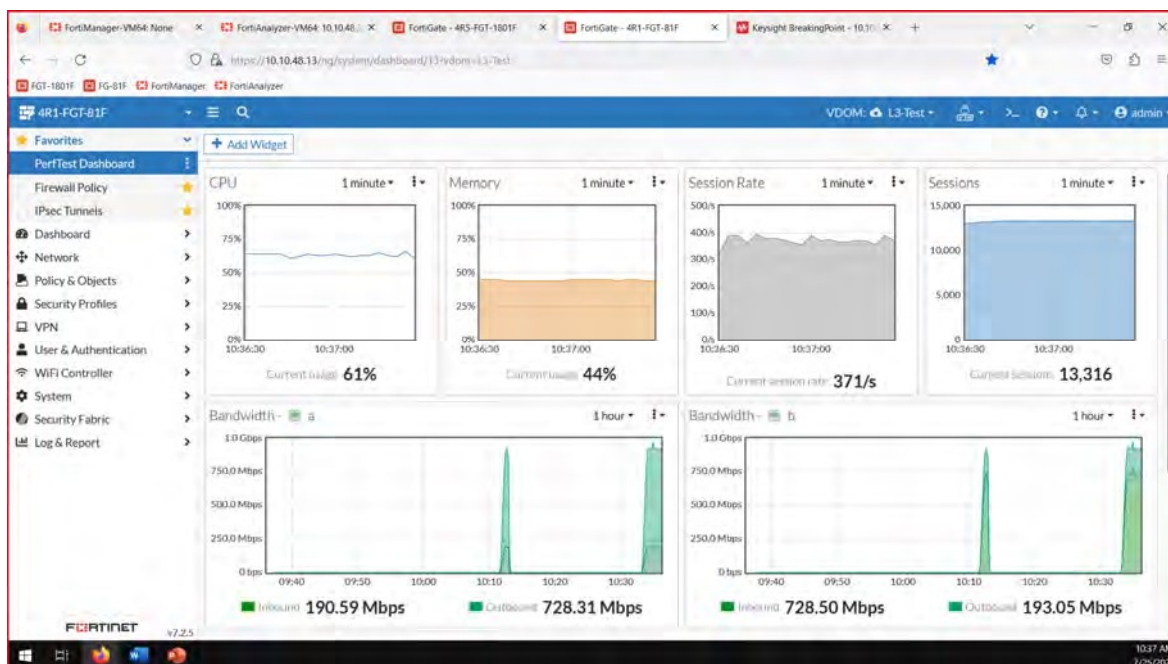
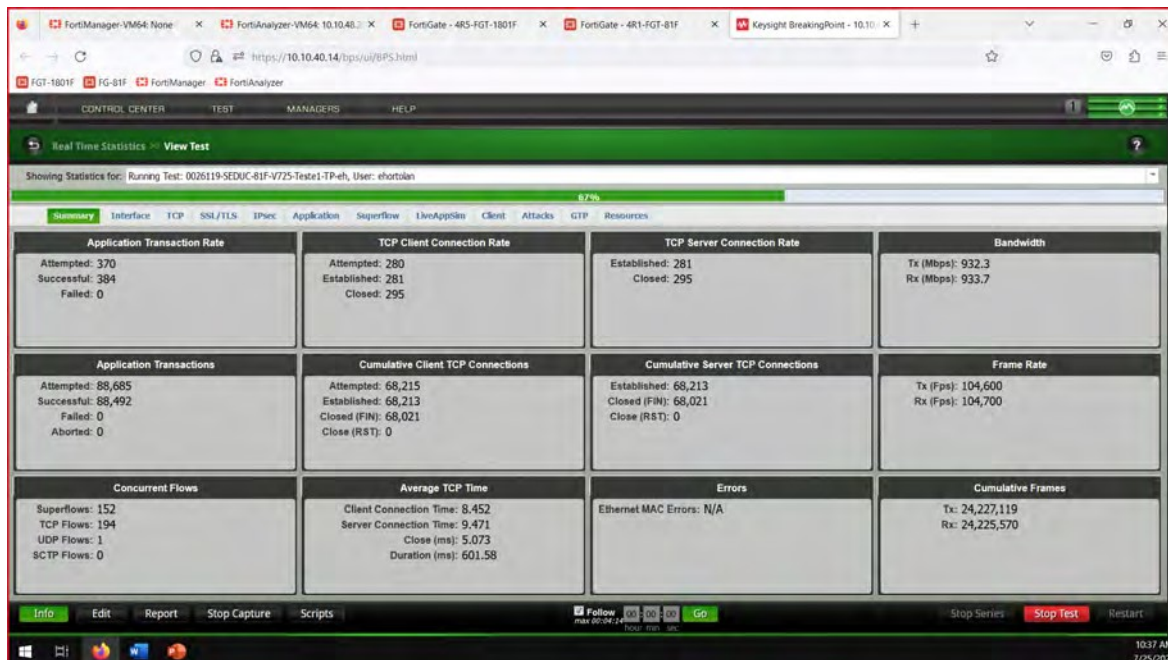
Specifications		FG-80F	FG-81F	FG-80F-BYPASS	FG-80F-POE	FG-81F-POE
Interfaces and Modules						
GE RJ45/SFP Shared Media Pairs	2	2	2	2	2	
GE RJ45 Internal Ports	6	6	6	6	6	
GE RJ45 FortiLink Ports (Default)	2	2	2	2	2	
GE RJ45 PoE/+ Ports	—	—	—	6	6	
GE RJ45 PoE/+ FortiLink Ports (Default)	—	—	—	2	2	
Bypass 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 **			800 Mbps			
System Performance and Capacity						
IPv4 Firewall Throughput (150 / 32 / 64 byte, UDP)			30 / 6 / 7 Gbps			
Firewall Latency (64 byte, UDP)			3.23 µs			
Firewall Throughput (Packet per Second)			10.5 Million			
Concurrent Sessions (TCP)			15 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			850 Mbps			
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)			200			
SSL Inspection Throughput (IPS, avg HTTPS)			715 Mbps			
SSL Inspection CPS (IPS, avg, HTTPS)			100			

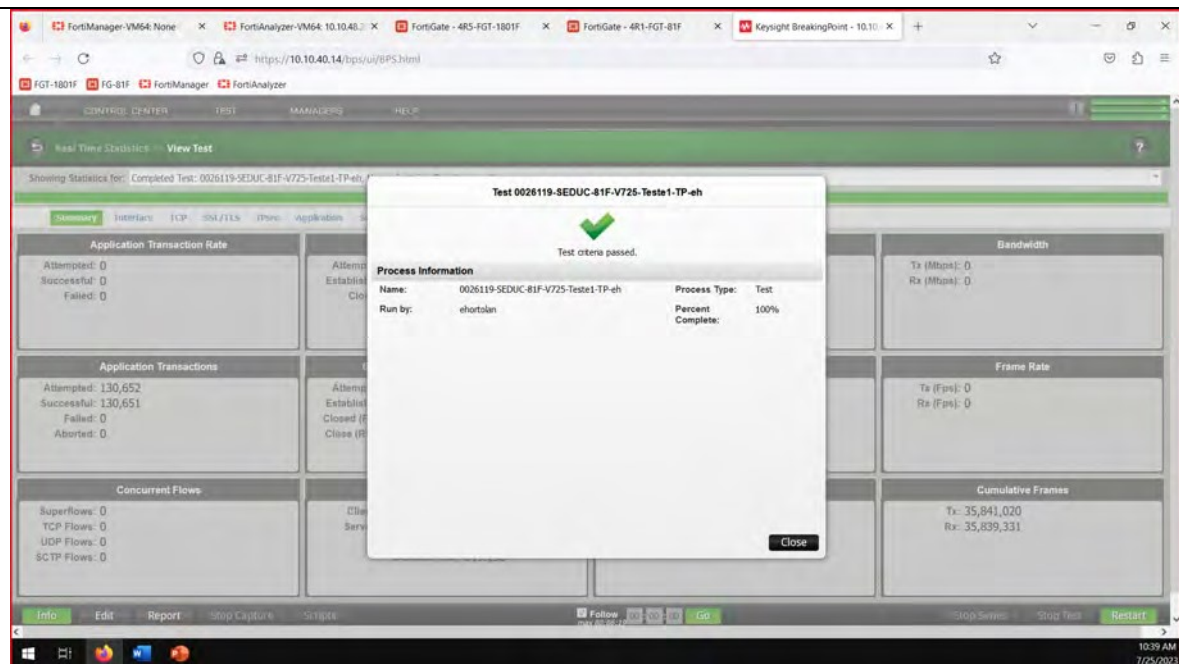
Comentário <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-80f-series.pdf>

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	

Procedimento do Teste

Será apresentado o perfil de tráfego que será gerado e submetido ao appliance em teste.
 Submeter o equipamento ao tráfego de 900 Mbps com as funcionalidades supracitadas inspecionando este tráfego.



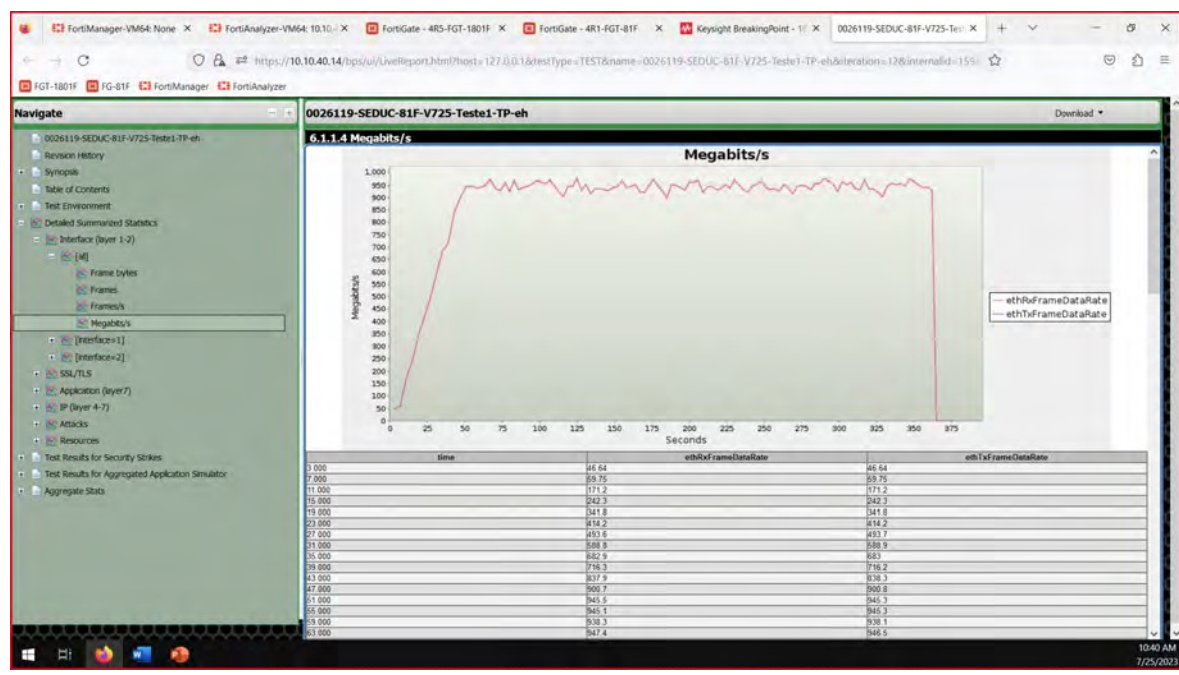


Test 0026119-SEDUC-81F-V725-Teste1-TP-eh

Test criteria passed.

Process Information

Name:	0026119-SEDUC-81F-V725-Teste1-TP-eh	Process Type:	Test
Run by:	ehortolan	Percent Complete:	100%



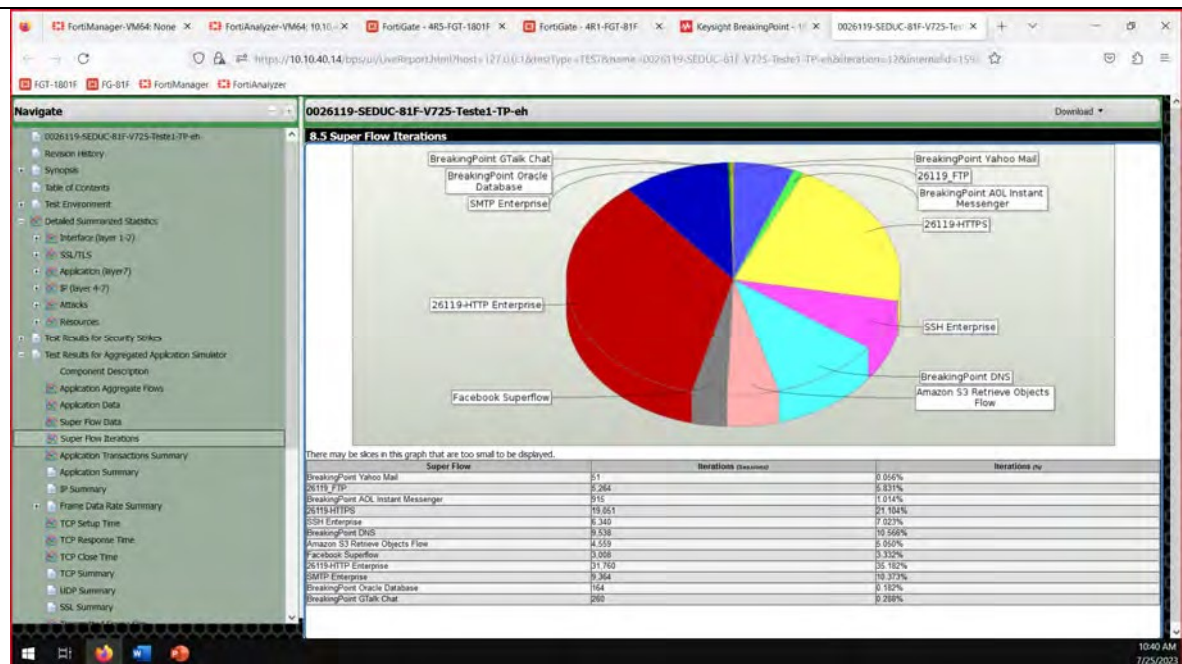
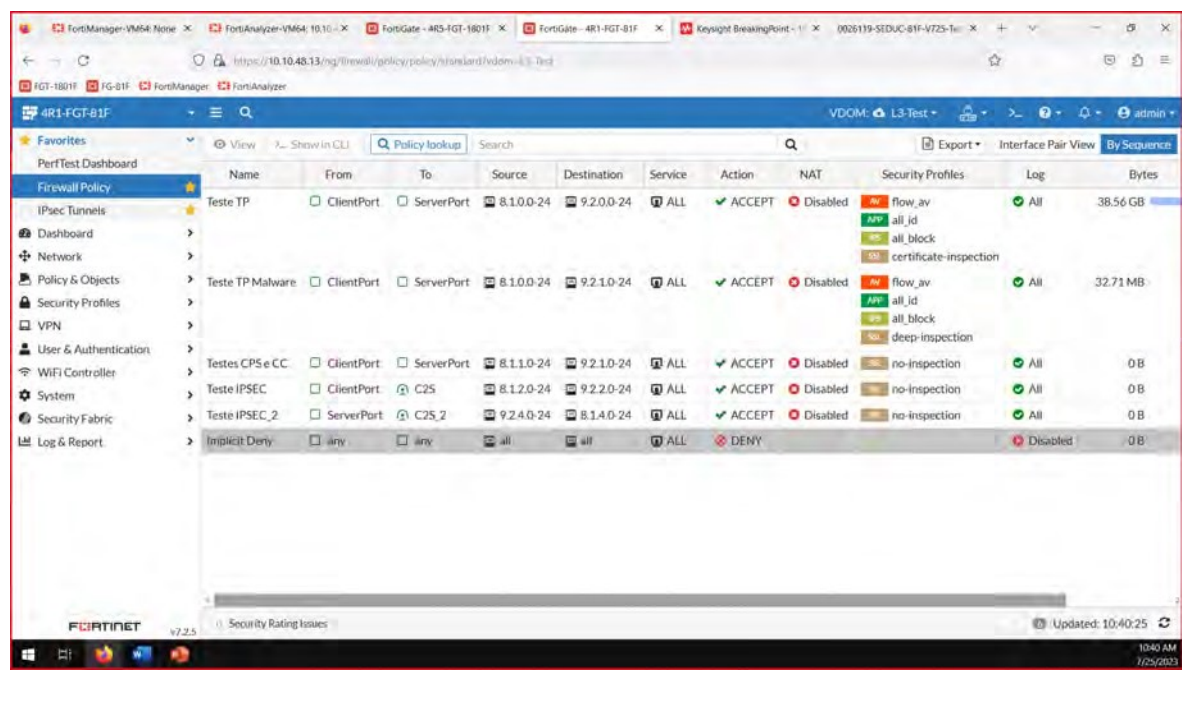
0026119-SEDUC-81F-V725-Teste1-TP-eh

6.114 Megabits/s

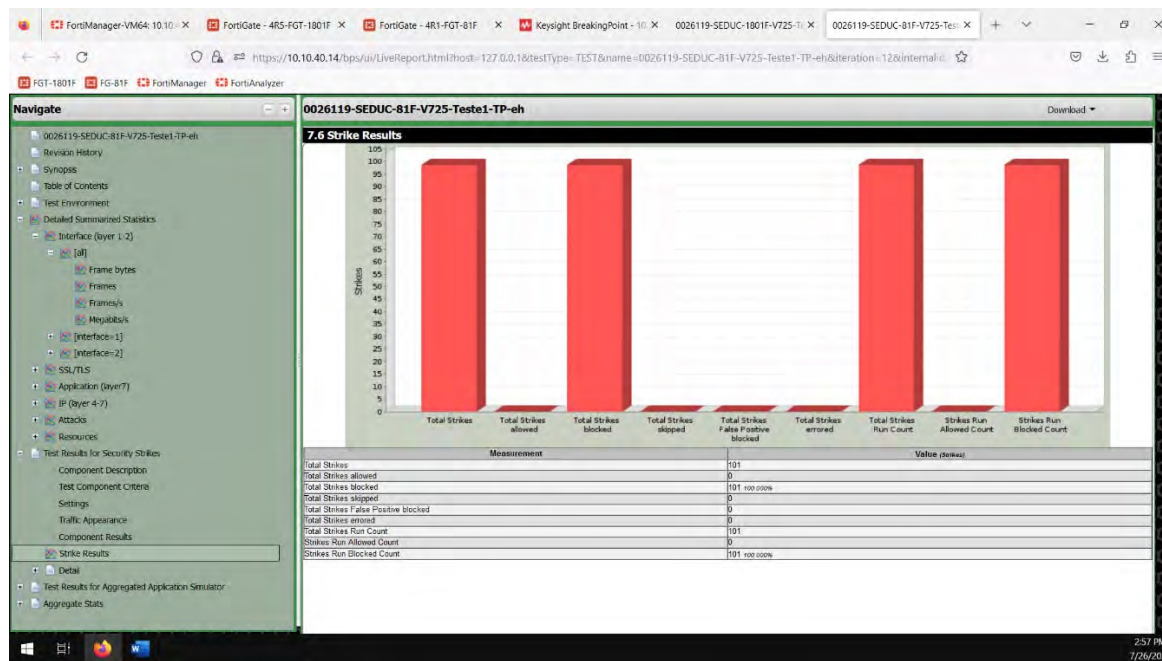
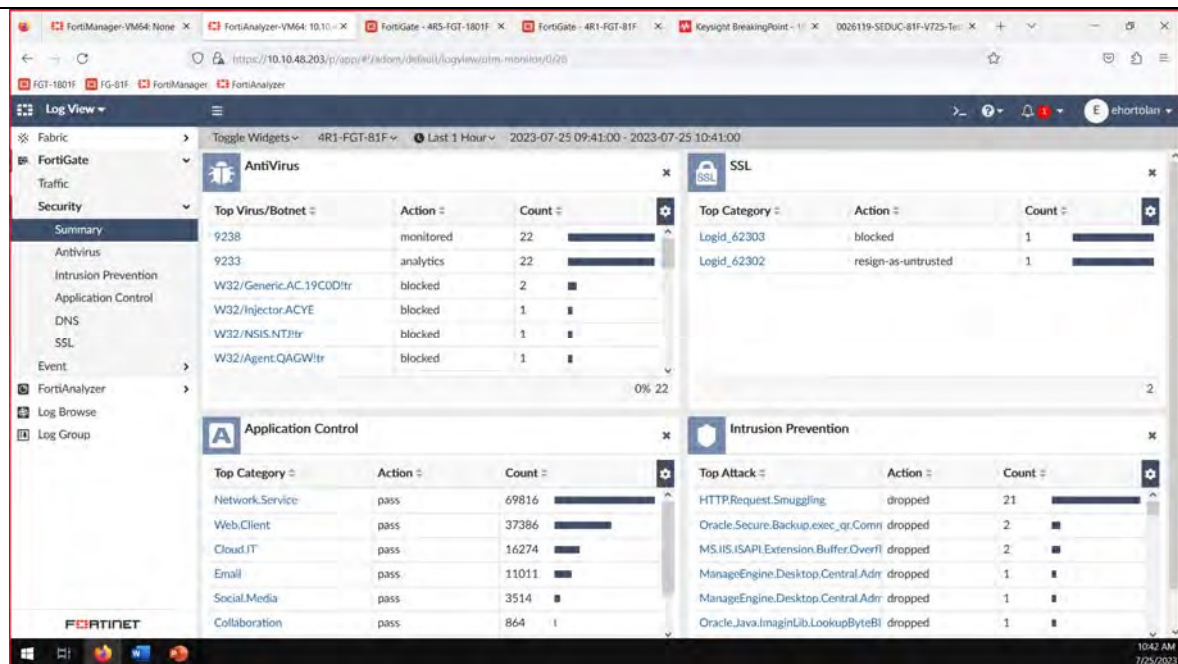
Megabits/s

Graph showing bandwidth over time (Seconds).

time	ethRxFrameDataRate	ethTxFrameDataRate
0 000	46.64	46.64
5 000	89.75	89.75
10 000	171.2	171.2
15 000	242.3	242.3
19 000	341.8	341.8
23 000	414.2	414.8
27 000	493.6	483.7
31 000	588.9	589.9
35 000	687.9	683
39 000	716.3	716.2
43 000	837.9	836.3
47 000	900.7	900.6
51 000	945.5	945.3
55 000	945.1	945.3
59 000	943.3	938.1
63 000	947.4	948.5

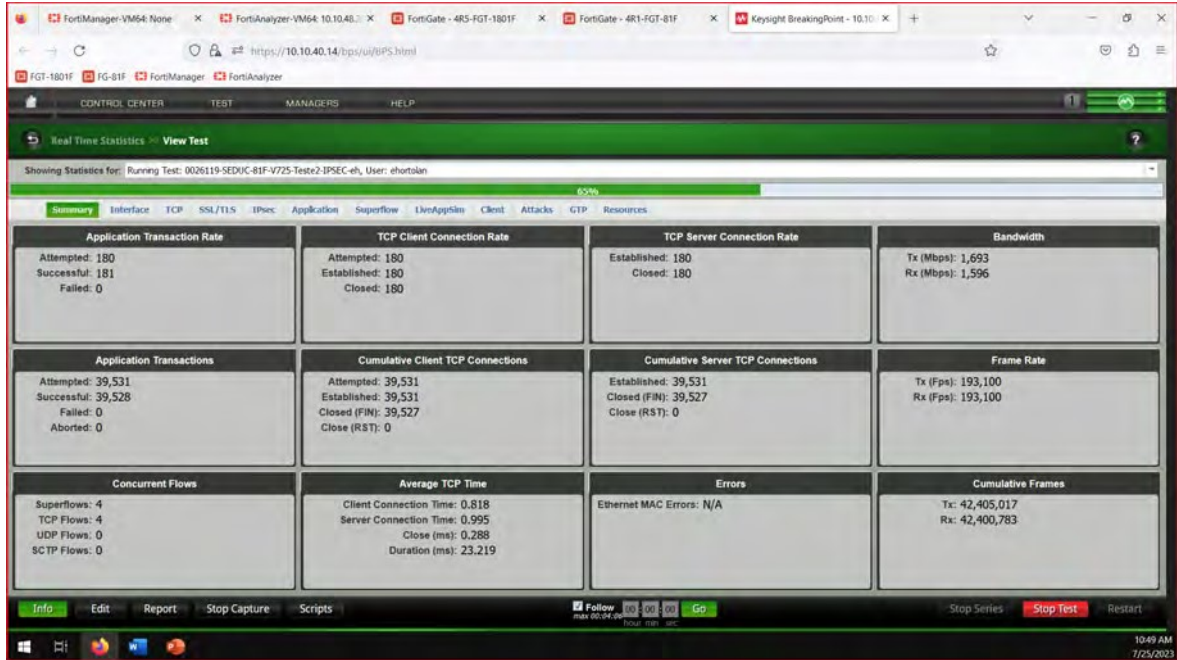



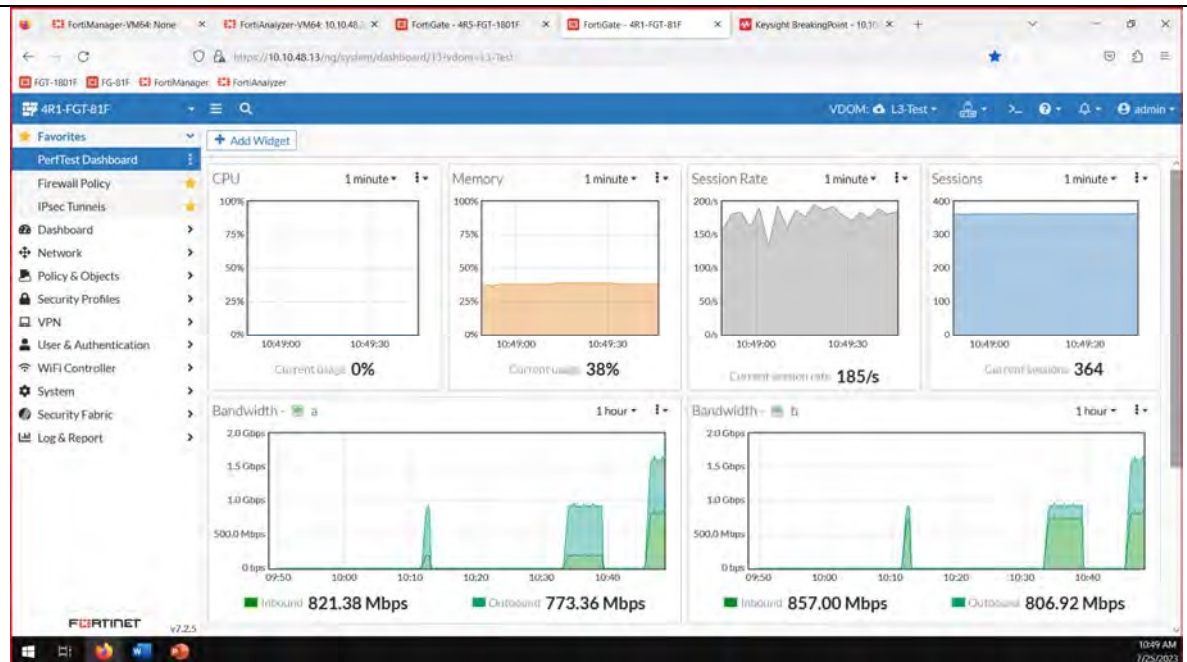
Name	From	To	Source	Destination	Service	Action	NAT	Security Profiles	Log	Bytes
Teste TP	ClientPort	ServerPort	8.1.0.0-24	9.2.0.0-24	ALL	ACCEPT	Disabled	flow_av, all_block, certificate-inspection	All	38.56 GB
Teste TP Malware	ClientPort	ServerPort	8.1.0.0-24	9.2.1.0-24	ALL	ACCEPT	Disabled	flow_av, all_block, deep-inspection	All	32.71 MB
Testes CPS e CC	ClientPort	ServerPort	8.1.1.0-24	9.2.1.0-24	ALL	ACCEPT	Disabled	no-inspection	All	0 B
Teste IPSEC	ClientPort	C2S	8.1.2.0-24	9.2.2.0-24	ALL	ACCEPT	Disabled	no-inspection	All	0 B
Teste IPSEC_2	ServerPort	C2S_2	9.2.4.0-24	8.1.4.0-24	ALL	ACCEPT	Disabled	no-inspection	All	0 B
Implicit Deny	any	any	all	all	ALL	DENY			Disabled	0 B



TESTE OK

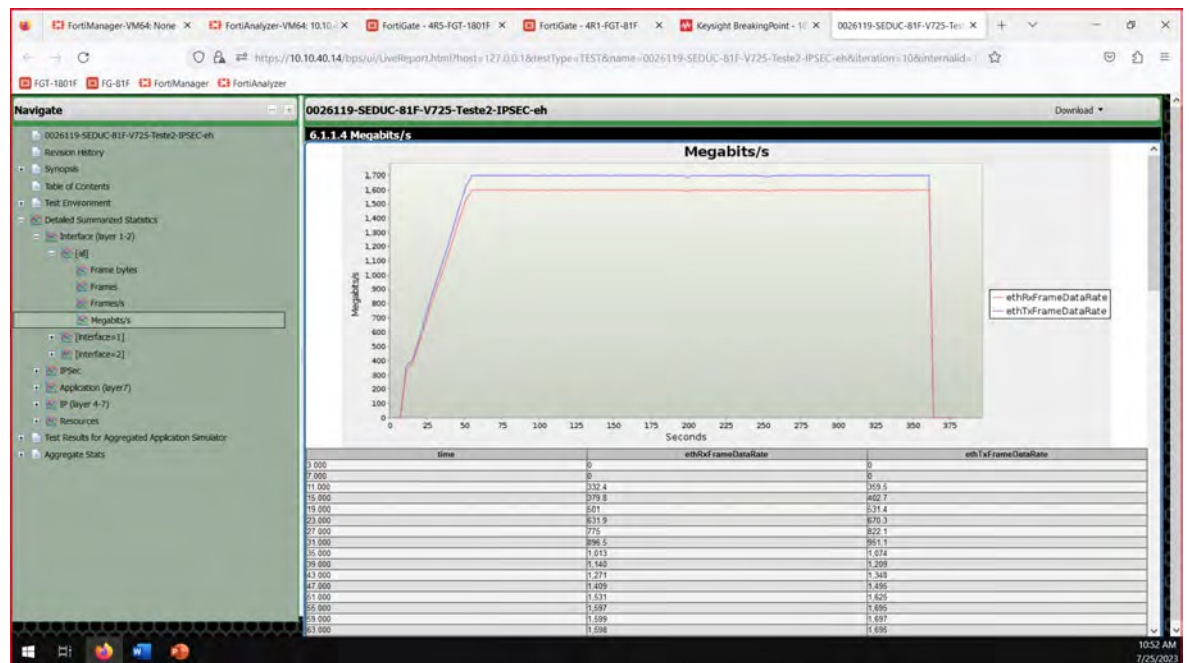
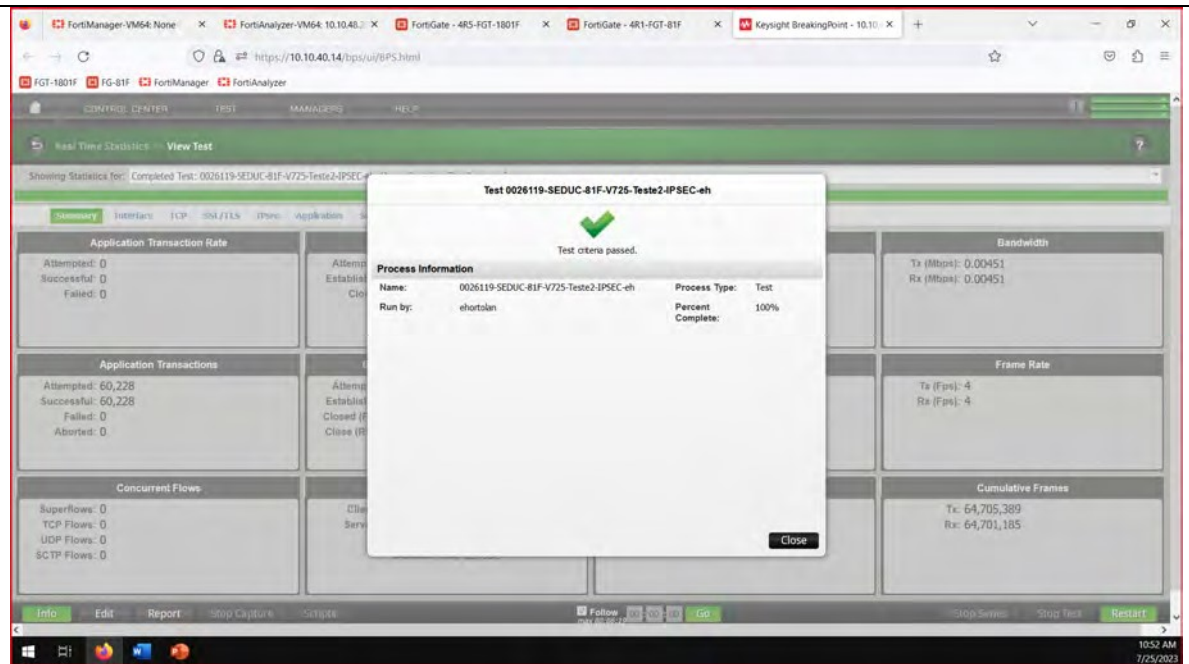
Evidências	Coletar durante o teste imagens com o equipamento performando 900 Mbps.
Comentário	

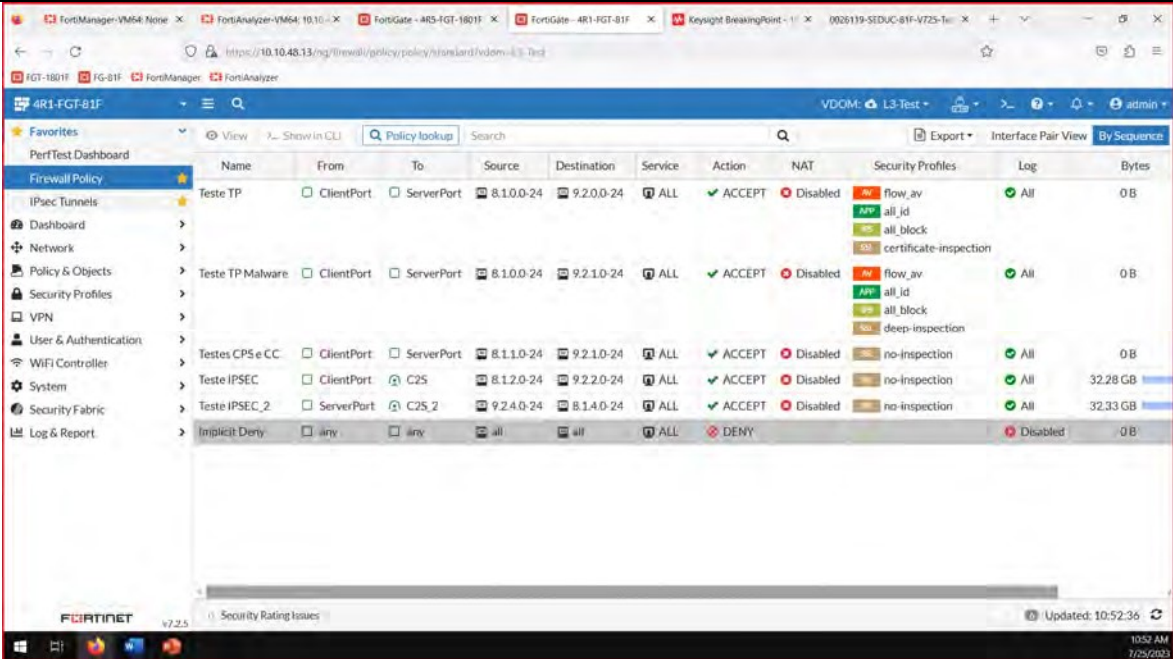
Item de Teste - 5.2.3.2	Possuir no mínimo 1,5 (Um e cinco décimos) Gbps de throughput para Ipsec VPN;
Objetivo do Teste	Validar a capacidade mínima de 1,5 Gbps de throughput para Ipsec VPN
Configuração do Teste	Teste a ser realizado no laboratório Fortinet. Será apresentado o perfil de tráfego que será 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. 



The screenshot shows the IPsec Tunnels configuration page. A search bar is visible at the top. The table below lists the configured tunnels:

Tunnel #	Interface Binding #	Status	Ref.
Custom			
C2S	b	2 dialup connection(s)	2
C2S_2	a	2 dialup connection(s)	2

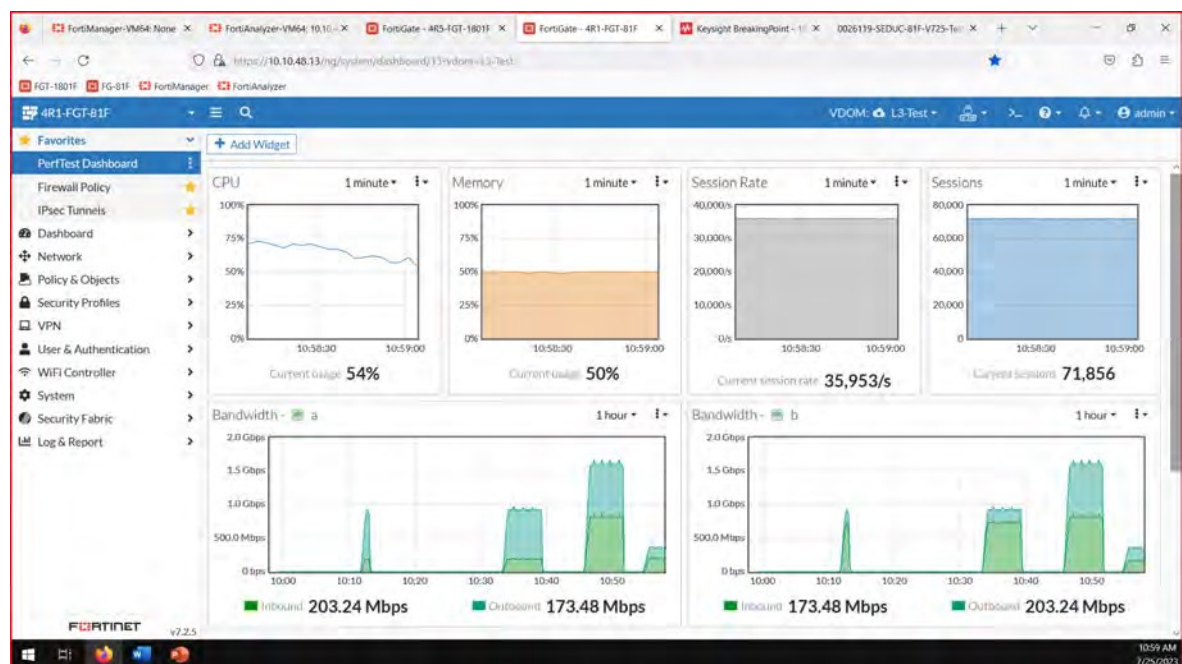
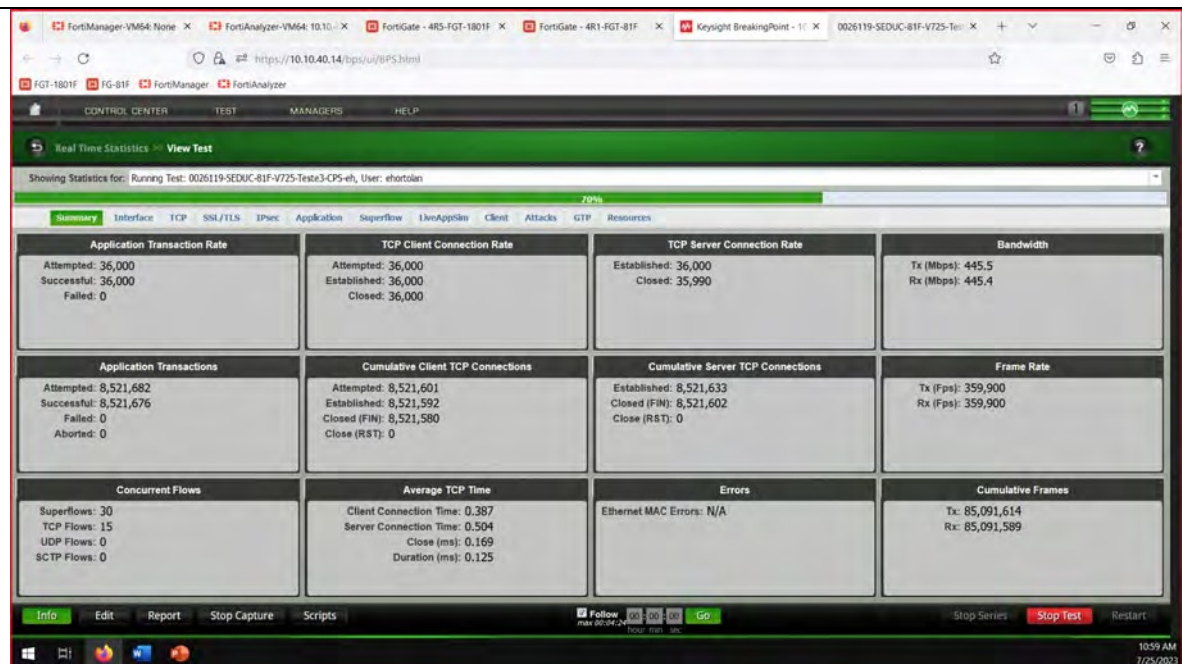


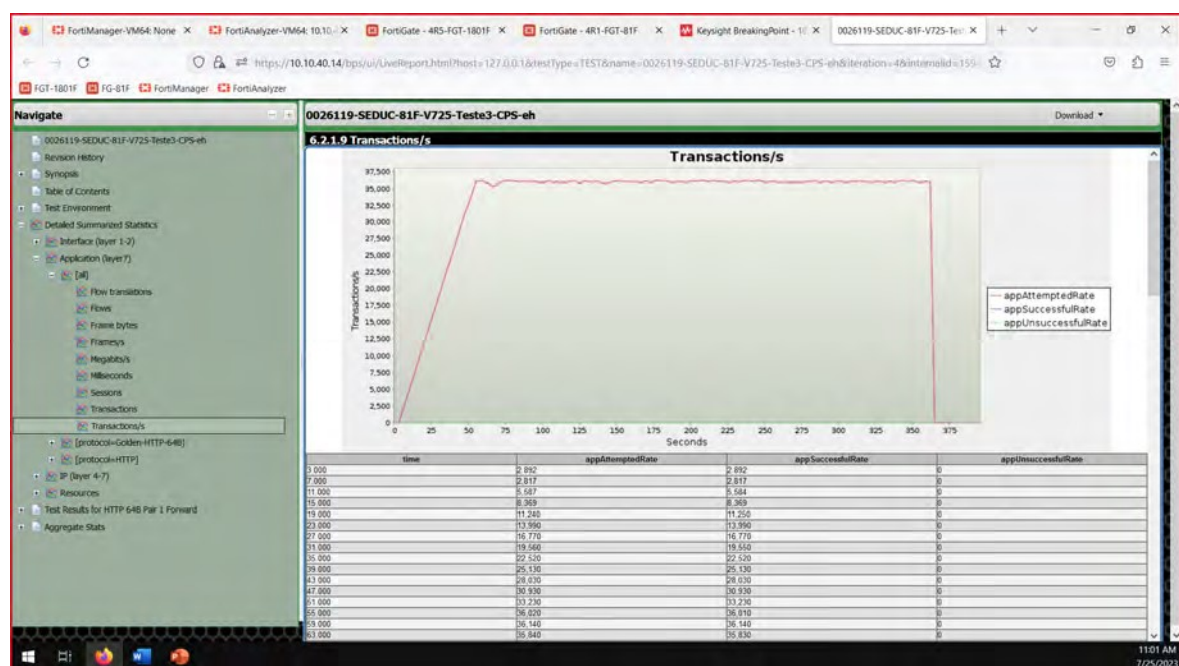
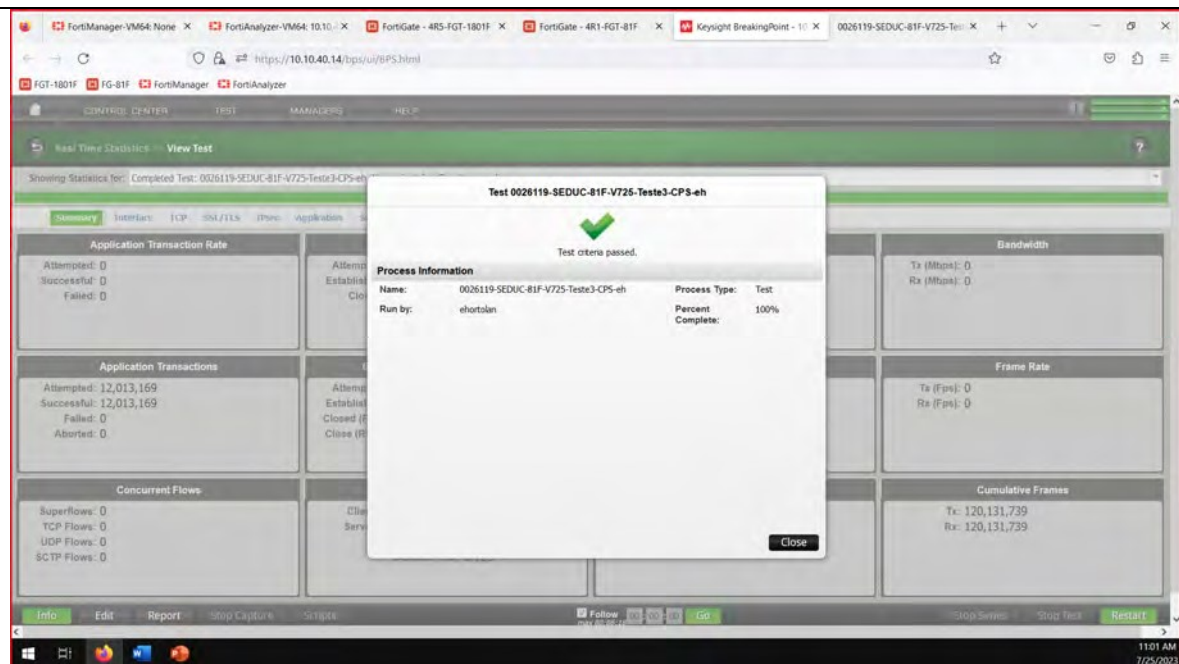
	 <p>TESTE OK</p>
Comentário	

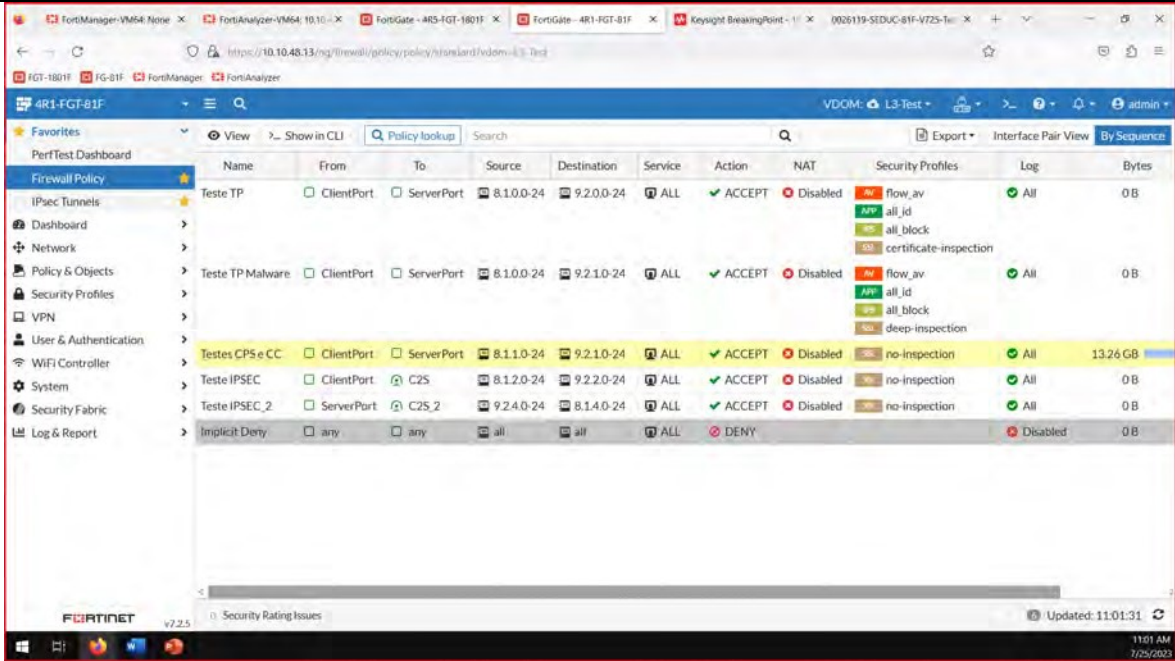
5.2.4 CONEXÕES

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	<p>Teste a ser realizado no laboratório Fortinet.</p> <p>Será apresentado o perfil de tráfego que será gerado e submetido ao appliance em teste.</p>
Procedimento do Teste	Teste a ser realizado no laboratório da Fortinet

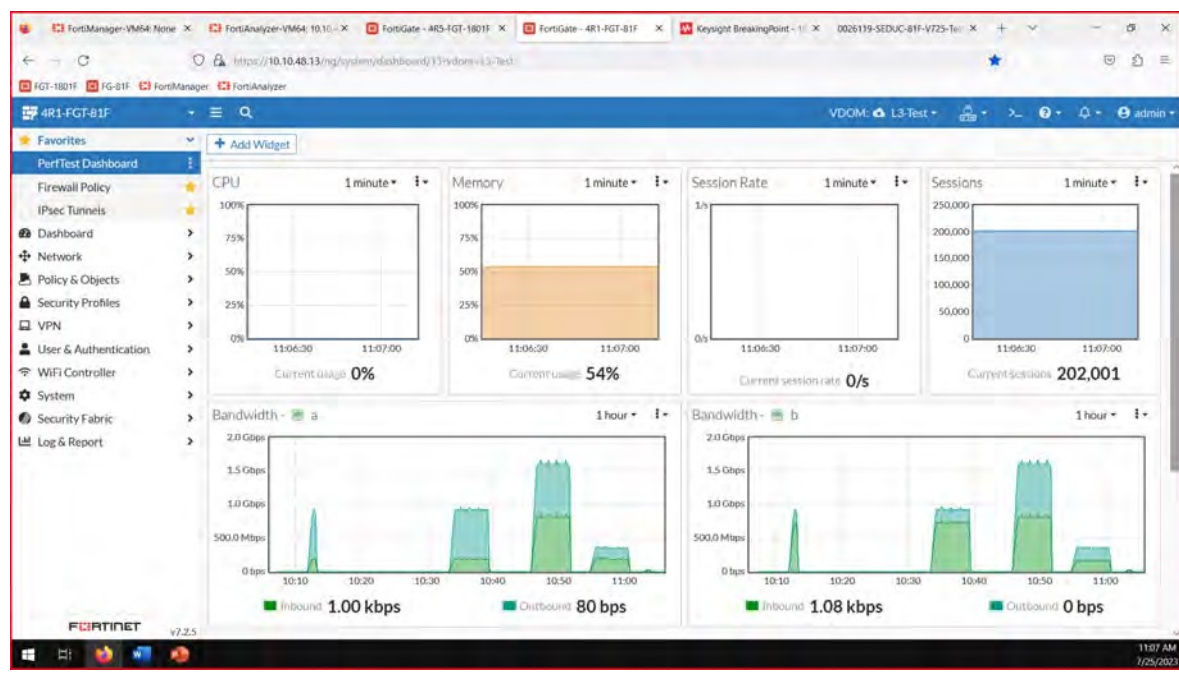
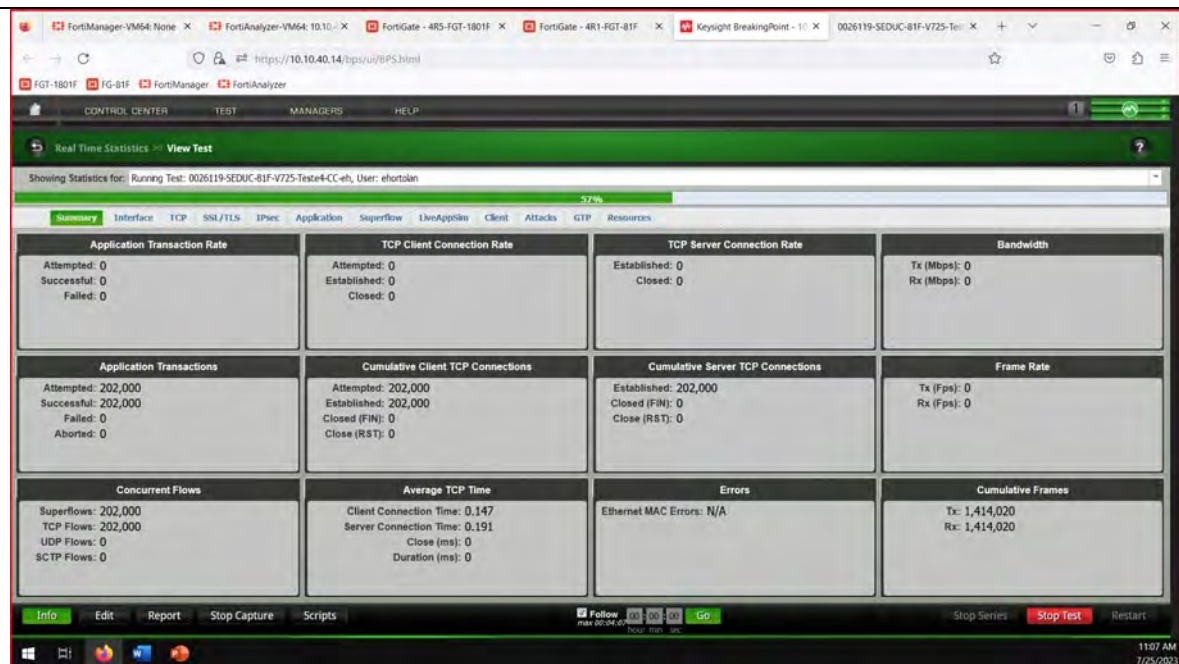
Evidências

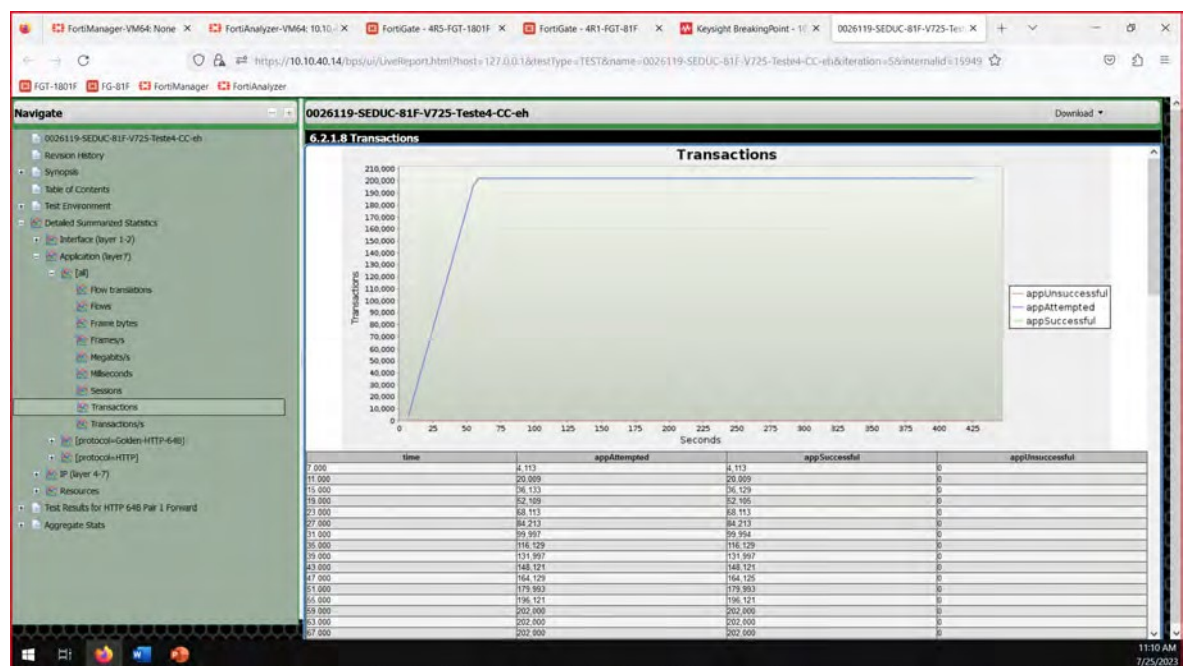
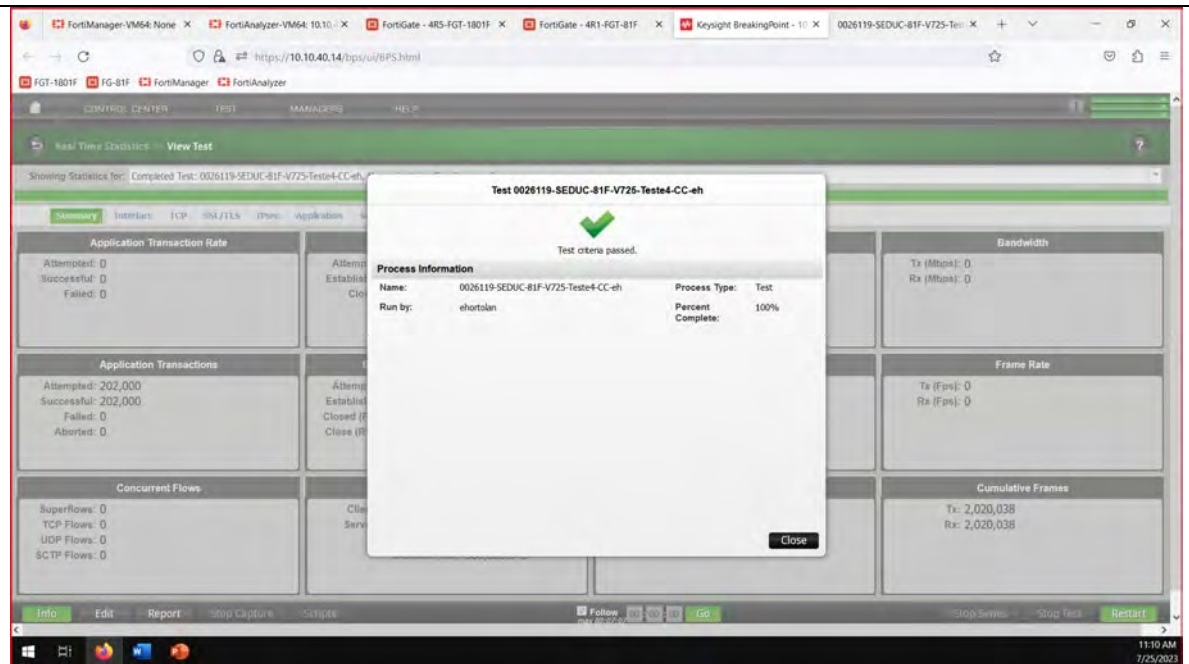


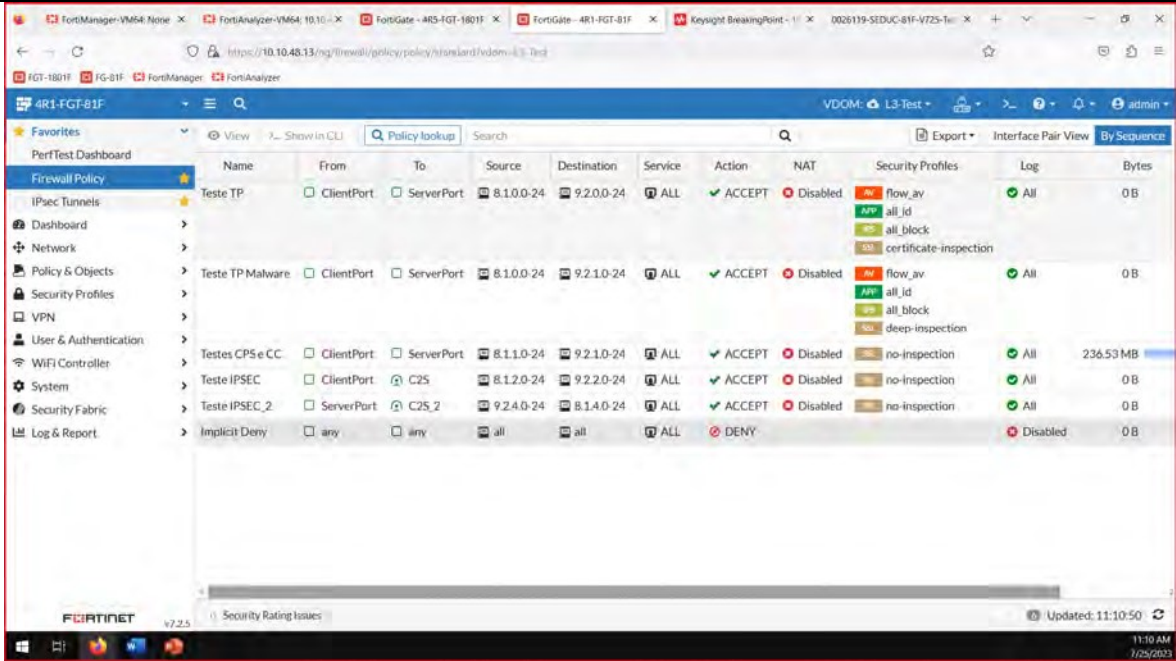


	 <p>TESTE OK</p>
Comentário	

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.





	 <p>TESTE OK</p>
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	<p>Execução de comando</p> <p><i>diagnose hardware deviceinfo disk</i></p> <p>Análise de saída do comando acima</p>

Evidências

```

CLI Console(1)
4R1-FGT-81F # config vdom
edit L3-Features

4R1-FGT-81F (vdom) # edit L3-Features
current vf-L3-Features:1

4R1-FGT-81F (L3-Features) # end

4R1-FGT-81F # config global

4R1-FGT-81F (global) # diagnose disktest device
1 /dev/sda type raw, size 122184MB
2 /dev/sda1 on /var/log type ext3(rw,noatime,errors=continue,barrier=0,data=writeback), size 122182MB, 118017MB free
3 /dev/mmcblk0 type raw, size 3648MB, boot device
4 /dev/mmcblk0p1 on /data type ext3(rw,relatime,errors=continue,barrier=1,data=writeback), size 256MB, 126MB free
5 /dev/mmcblk0p3 on /data2 type ext3(rw,relatime,errors=continue,barrier=1,data=writeback), size 2997MB, 2705MB free
6 /dev/mmcblk0p1 on /new_root/eap_proxy/etc/cert/ca type ext3(ro,relatime,errors=continue,barrier=1,data=writeback), size 256MB,
4R1-FGT-81F (global) #
    
```

TESTE OK

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
partition                  247.8MiB, 148.8MiB free  mounted: N  label: dev:/dev/mmcblk0p1(boot) start: 0
partition                  247.8MiB, 135.8MiB 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: LOGUSEDX87383626 dev:/dev/sda1 start: 2848

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 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>Hardware</p> <p>FortiGate 80F/80F-Bypass/81F FortiGate 80F-DSL</p> <p>FortiGate 80F/81F-POE FortiWiFi 80F/81F-2R FortiWiFi 81F-2R-POE</p> <p>Interfaces</p> <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">Dimensions and Power</td> </tr> <tr> <td>Height x Width x Length (inches)</td> <td>1.6 × 8.5 × 7.0</td> <td>1.6 × 8.5 × 7.0</td> <td>1.6 × 8.5 × 7.0</td> <td>2.4 × 8.5 × 7.0</td> <td>2.4 × 8.5 × 7.0</td> </tr> <tr> <td>Height x Width x Length (mm)</td> <td>40 × 216 × 178</td> <td>40 × 216 × 178</td> <td>40 × 216 × 178</td> <td>60 × 216 × 178</td> <td>60 × 216 × 178</td> </tr> <tr> <td>Weight</td> <td>2.4 lbs (1.1 kg)</td> <td>2.4 lbs (1.1 kg)</td> <td>2.6 lbs (1.2 kg)</td> <td>3.1 lbs (1.4 kg)</td> <td>3.1 lbs (1.4 kg)</td> </tr> <tr> <td colspan="6">Form Factor (supports EIA/non-EIA standards)</td> </tr> <tr> <td colspan="6">Desktop/ Wall Mount/ Rack Tray</td> </tr> <tr> <td colspan="6">Operating Environment and Certifications</td> </tr> <tr> <td>Input Rating</td> <td>12V DC, 3A (dual redundancy optional)</td> <td>12V DC, 3A (dual redundancy optional)</td> <td>12V DC, 3A (dual redundancy optional)</td> <td>+54V DC, 3A (dual redundancy optional)</td> <td>+54V DC, 3A (dual redundancy optional)</td> </tr> <tr> <td>Power Required (Redundancy Optional)</td> <td colspan="5">Powered by up to 2 External DC Power Adapters (1 adapter included), 100-240V AC, 50/60 Hz</td> </tr> <tr> <td>Maximum Current</td> <td>115VAC/0.10 A</td> <td>115VAC/0.10 A</td> <td>115VAC/0.10 A</td> <td>115VAC/0.22 A</td> <td>115VAC/0.22 A</td> </tr> </tbody> </table>		FG-80F	FG-81F	FG-80F-BYPASS	FG-80F-POE	FG-81F-POE	Dimensions and Power						Height x Width x Length (inches)	1.6 × 8.5 × 7.0	1.6 × 8.5 × 7.0	1.6 × 8.5 × 7.0	2.4 × 8.5 × 7.0	2.4 × 8.5 × 7.0	Height x Width x Length (mm)	40 × 216 × 178	40 × 216 × 178	40 × 216 × 178	60 × 216 × 178	60 × 216 × 178	Weight	2.4 lbs (1.1 kg)	2.4 lbs (1.1 kg)	2.6 lbs (1.2 kg)	3.1 lbs (1.4 kg)	3.1 lbs (1.4 kg)	Form Factor (supports EIA/non-EIA standards)						Desktop/ Wall Mount/ Rack Tray						Operating Environment and Certifications						Input Rating	12V DC, 3A (dual redundancy optional)	12V DC, 3A (dual redundancy optional)	12V DC, 3A (dual redundancy optional)	+54V DC, 3A (dual redundancy optional)	+54V DC, 3A (dual redundancy optional)	Power Required (Redundancy Optional)	Powered by up to 2 External DC Power Adapters (1 adapter included), 100-240V AC, 50/60 Hz					Maximum Current	115VAC/0.10 A	115VAC/0.10 A	115VAC/0.10 A	115VAC/0.22 A	115VAC/0.22 A
	FG-80F	FG-81F	FG-80F-BYPASS	FG-80F-POE	FG-81F-POE																																																														
Dimensions and Power																																																																			
Height x Width x Length (inches)	1.6 × 8.5 × 7.0	1.6 × 8.5 × 7.0	1.6 × 8.5 × 7.0	2.4 × 8.5 × 7.0	2.4 × 8.5 × 7.0																																																														
Height x Width x Length (mm)	40 × 216 × 178	40 × 216 × 178	40 × 216 × 178	60 × 216 × 178	60 × 216 × 178																																																														
Weight	2.4 lbs (1.1 kg)	2.4 lbs (1.1 kg)	2.6 lbs (1.2 kg)	3.1 lbs (1.4 kg)	3.1 lbs (1.4 kg)																																																														
Form Factor (supports EIA/non-EIA standards)																																																																			
Desktop/ Wall Mount/ Rack Tray																																																																			
Operating Environment and Certifications																																																																			
Input Rating	12V DC, 3A (dual redundancy optional)	12V DC, 3A (dual redundancy optional)	12V DC, 3A (dual redundancy optional)	+54V DC, 3A (dual redundancy optional)	+54V DC, 3A (dual redundancy optional)																																																														
Power Required (Redundancy Optional)	Powered by up to 2 External DC Power Adapters (1 adapter included), 100-240V AC, 50/60 Hz																																																																		
Maximum Current	115VAC/0.10 A	115VAC/0.10 A	115VAC/0.10 A	115VAC/0.22 A	115VAC/0.22 A																																																														

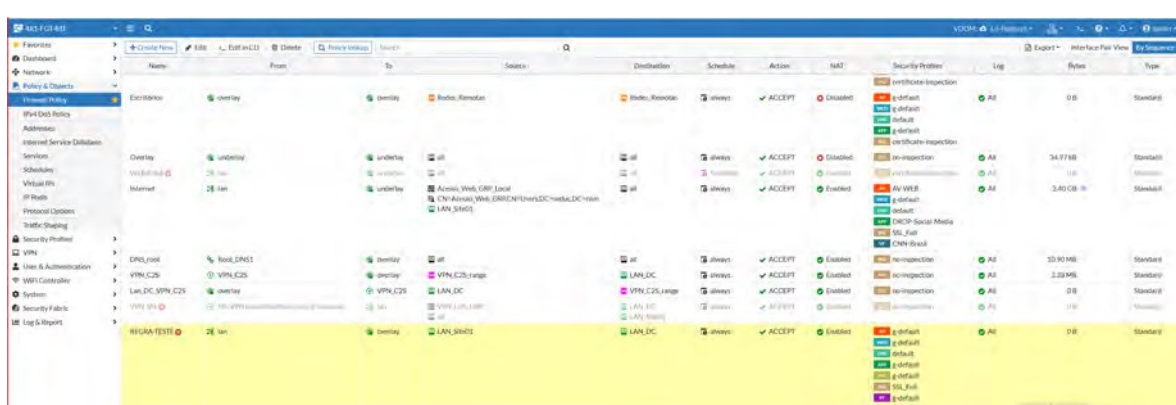
TESTE OK				
Specifications				
	FG-80F-DSL	FWF-80F-2R-304G-DSL	FWF-81F-2R-304G-DSL	FWF-81F-2R-304G-POE
Dimensions and Power				
Height x Width x Length (inches)	2.4 x 8.5 x 7.0	2.4 x 8.5 x 7.0	2.4 x 8.5 x 7.0	2.4 x 8.5 x 7.0
Height x Width x Length (mm)	60 x 216 x 178	60 x 216 x 178	60 x 216 x 178	60 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, 2.75A
Power Required (Redundancy Optional)	Powered by up to two external DC power adapters (one adapter included, 100-240V AC, 50/60 Hz, 115Vdc/0.5A, 230Vdc/0.6A)			
Current (Maximum)	—	—	—	38W
Total Available PoE Power Budget*	—	—	—	38W
Power Consumption (Average / Maximum)	28.0 W / 31.6 W	28.0 W / 34.31 W	29.2 W / 35.6 W	108.3 W / 133.8 W
Heat Dissipation	106 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

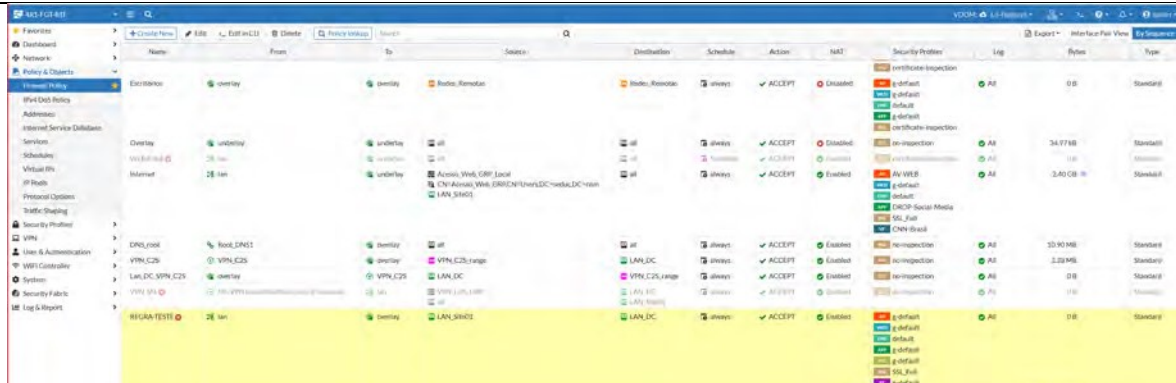
5.3.1.1 Deve implementar:

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	 <p>TESTE OK</p> <p>Na página 822 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.</p>

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.

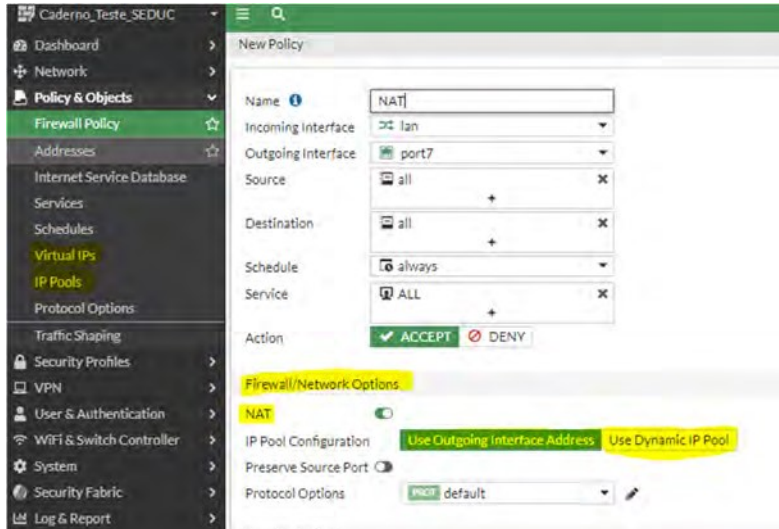
Evidências



The screenshot shows the FortiGate web interface for Policy & Objects. A table of firewall policies is displayed, with the 'NAT' column highlighted in yellow. The policies listed include 'REGRA-TESTE' and several others with various NAT settings like 'DNAT', 'SNAT', and 'IP Pool'.

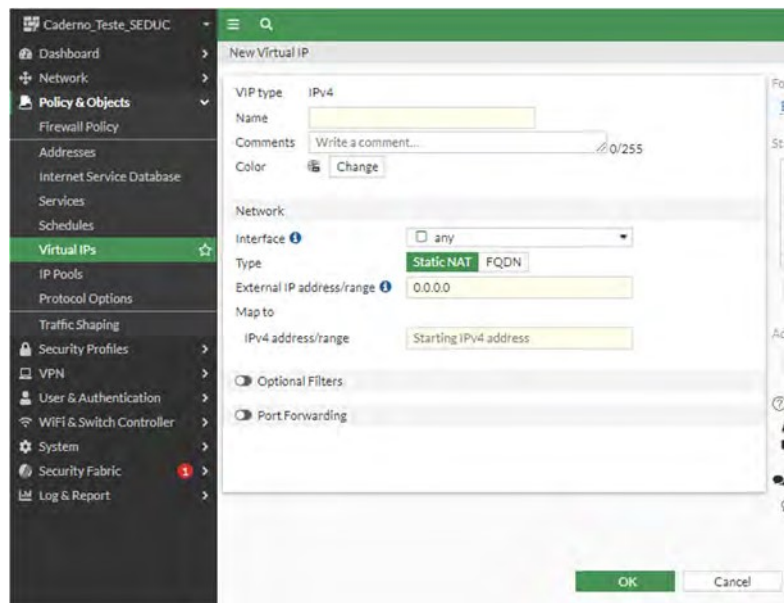
TESTE OK

NAT

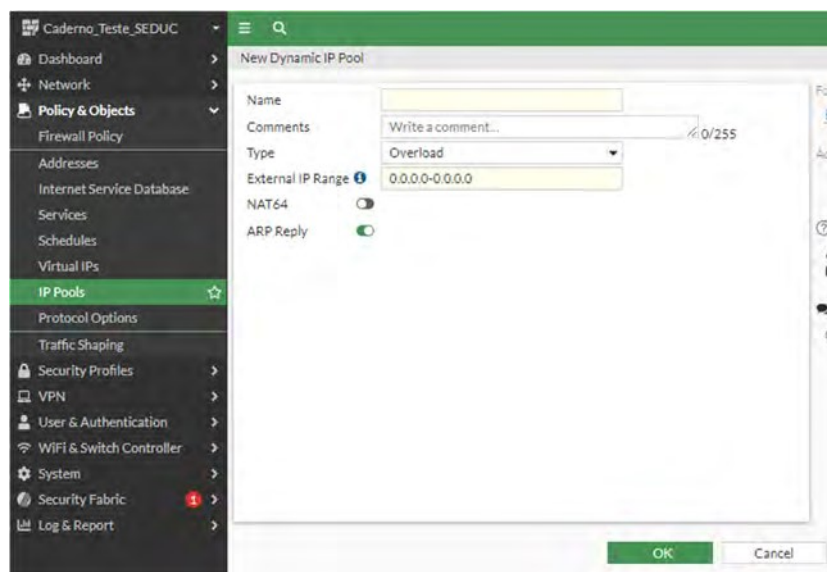


The screenshot shows the 'New Policy' configuration page in FortiGate. The 'Name' field is set to 'NAT'. The 'Incoming Interface' is 'lan' and the 'Outgoing Interface' is 'port7'. The 'Source' and 'Destination' are both set to 'all'. The 'Schedule' is 'always' and the 'Service' is 'ALL'. The 'Action' is set to 'ACCEPT'. Under 'Firewall/Network Options', the 'NAT' checkbox is checked. The 'IP Pool Configuration' section shows 'Use Outgoing Interface Address' and 'Use Dynamic IP Pool' options.

2 – Virtual IPS

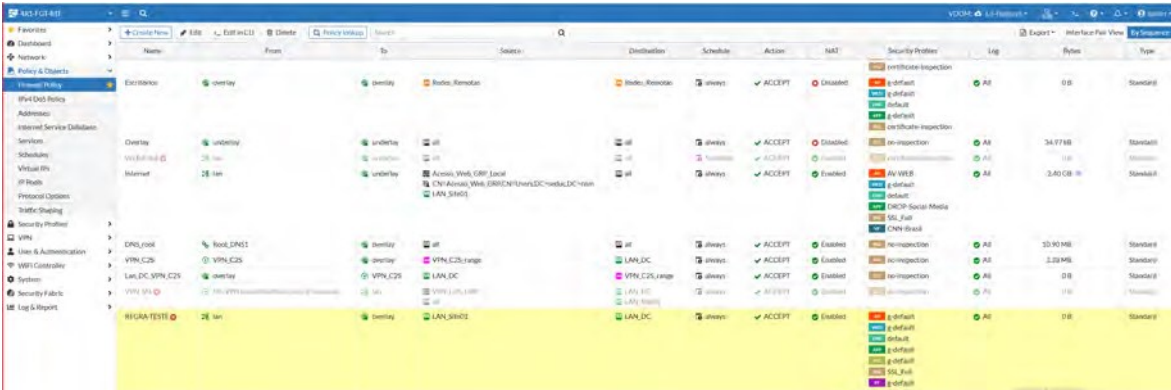
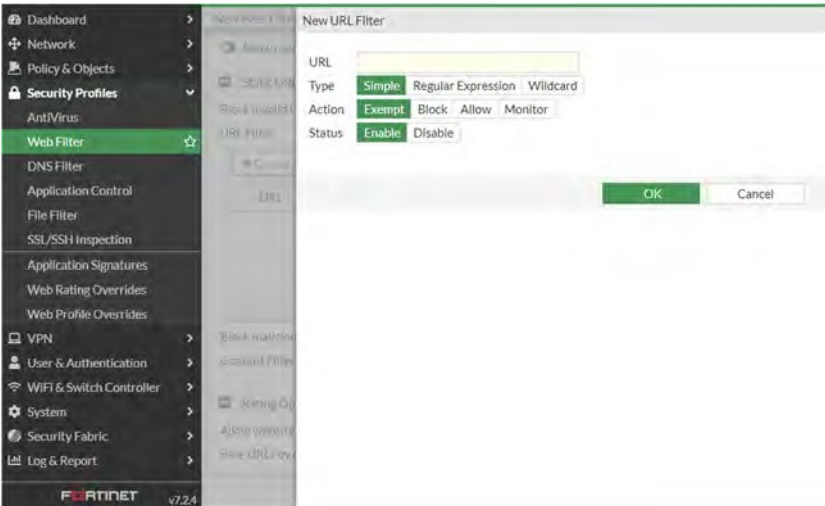


3 – IP Pools

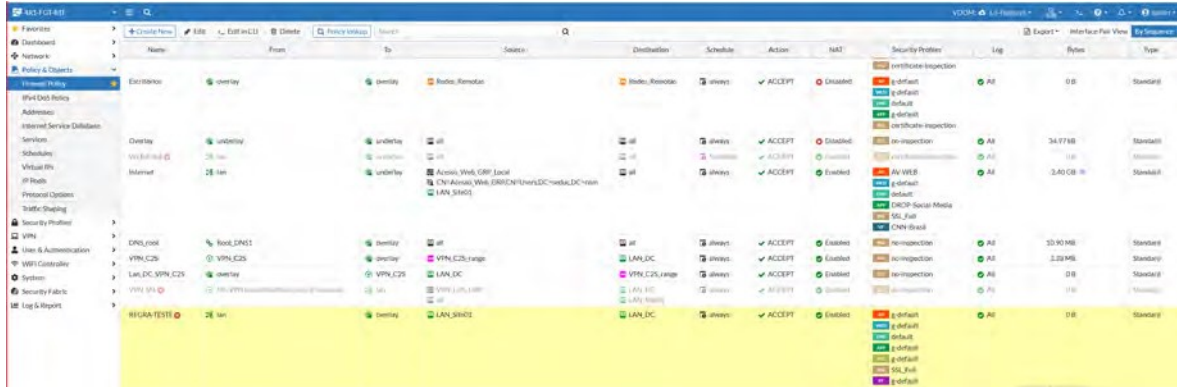
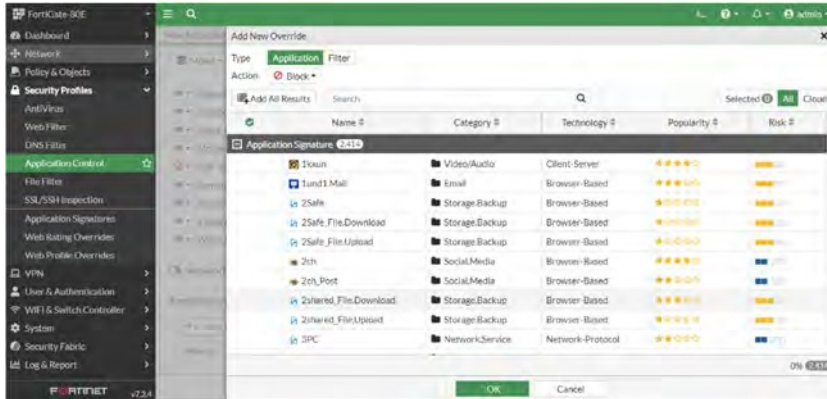


Comentário

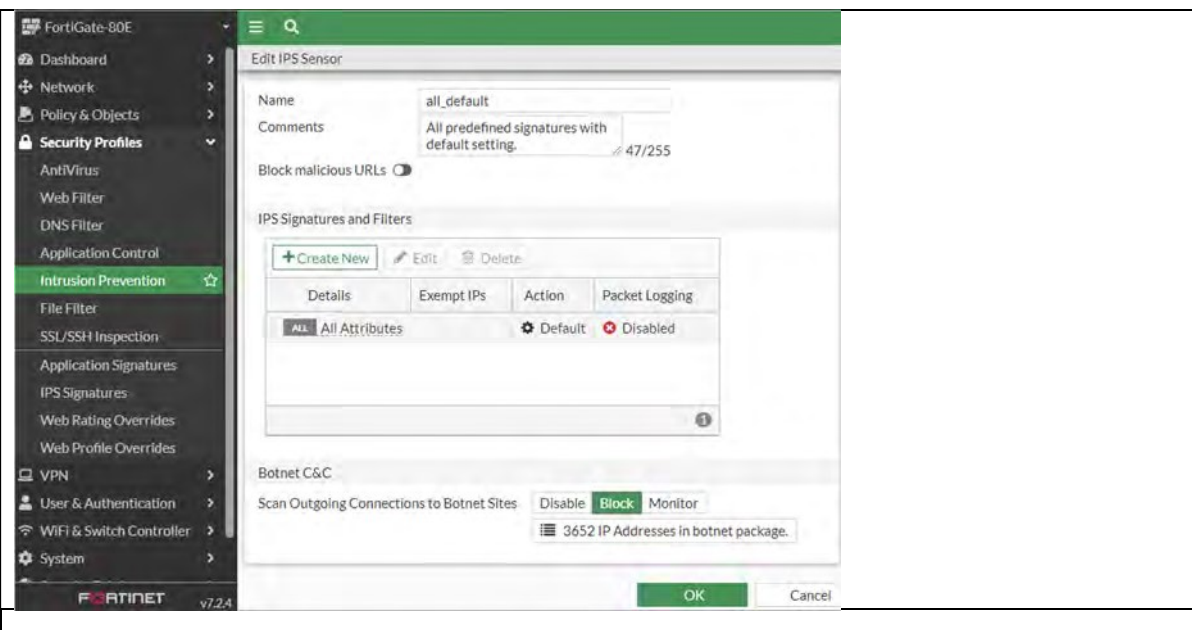
<https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/898655/static-snat>
<https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/29961/dynamic-snat>
<https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/728694/destination-nat>

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	 <p>TESTE OK</p> 
Comentário	

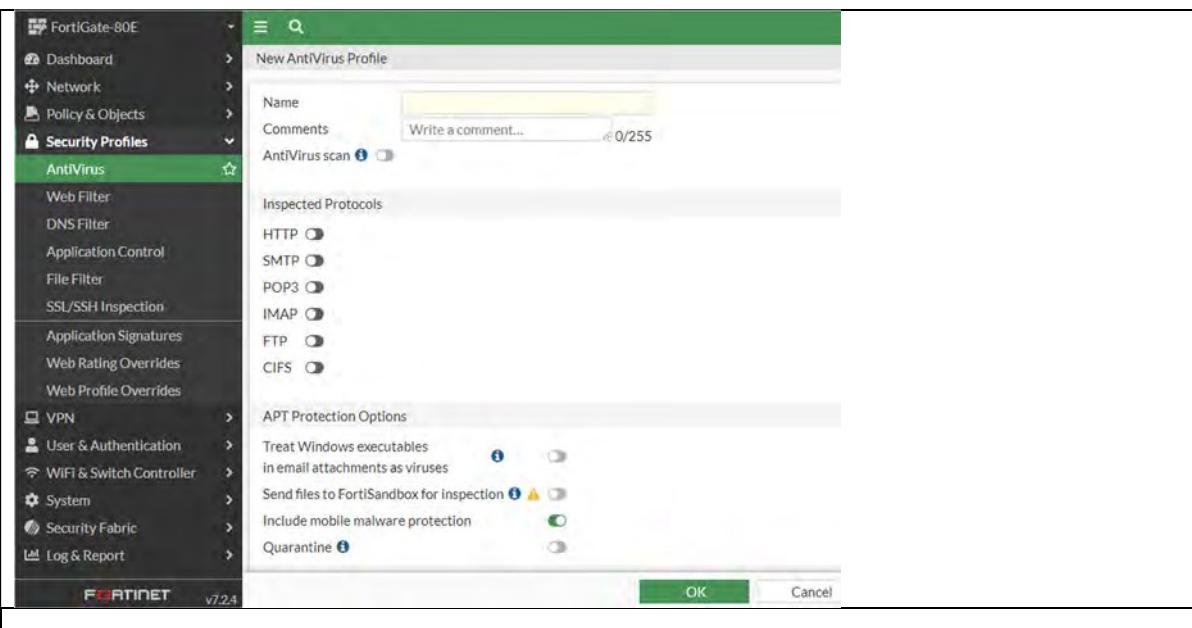
Item de Teste - 5.3.1.1.4	Application Control;
Objetivo do Teste	Demonstrar capacidade de executar filtros por Aplicação.

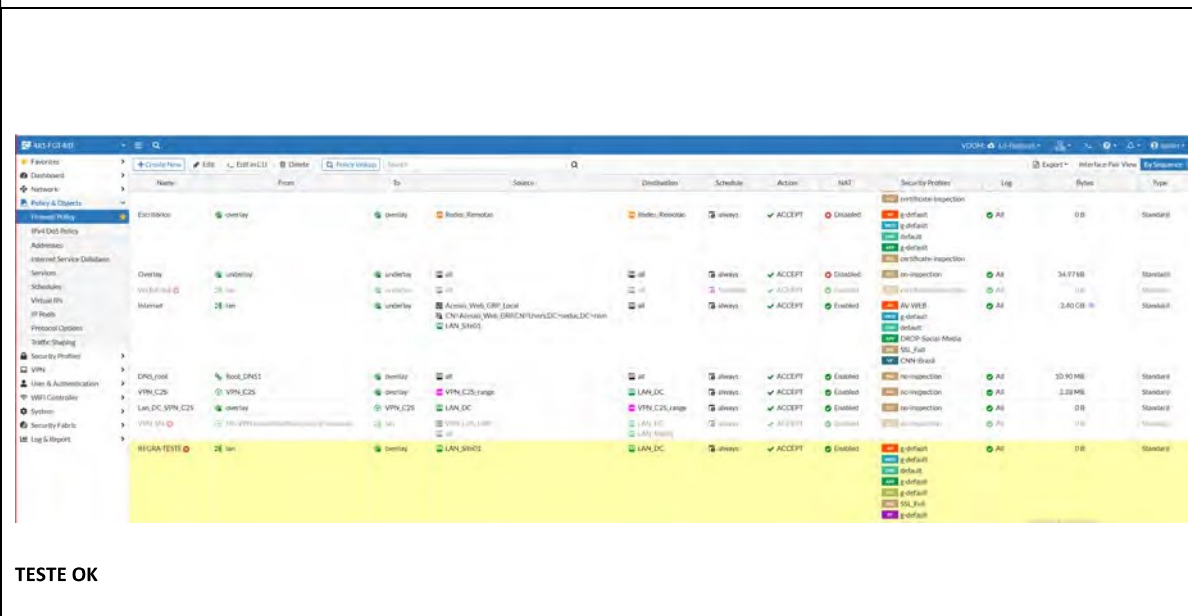
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Para ter acesso a essa funcionalidade, é necessário acessar o menu "Security Profile" e, em seguida, selecionar a opção "Application Control".
Evidências	<div data-bbox="240 479 1422 864">  </div> <p data-bbox="240 904 328 927">TESTE OK</p> <div data-bbox="240 1155 1070 1552">  </div>
Comentário	

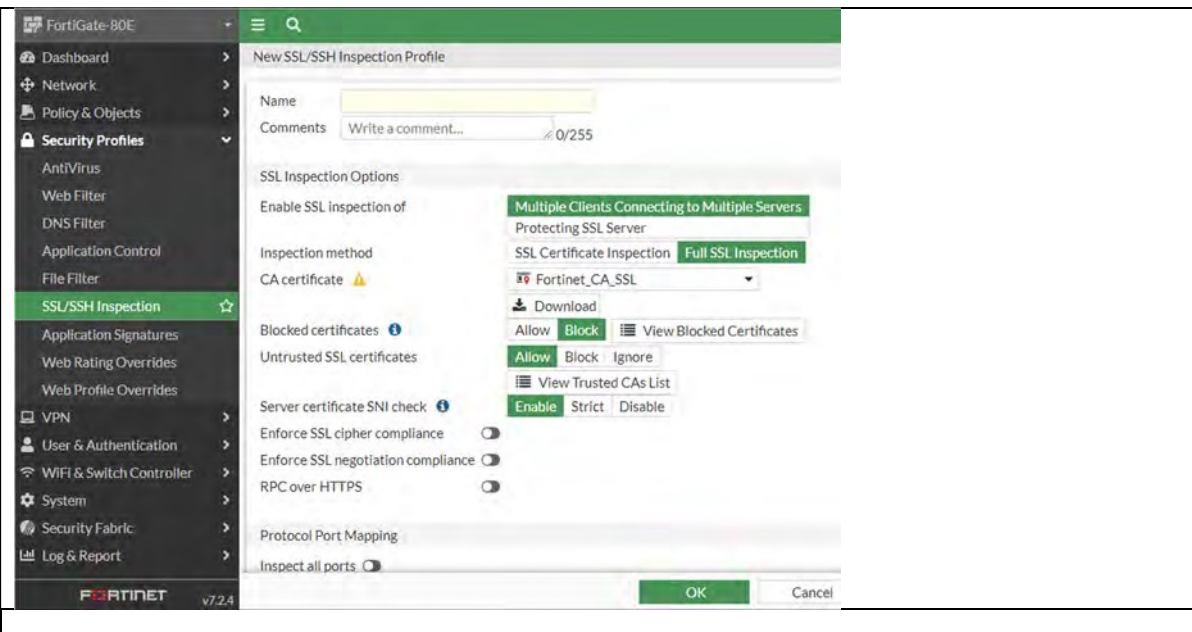
Item de Teste - 5.3.1.1.5	Anti-bot;
Objetivo do Teste	Validar se a solução tem ferramenta Anti-bot de forma nativa
Configuração do Teste	Demonstrar base de regras do FortiGate

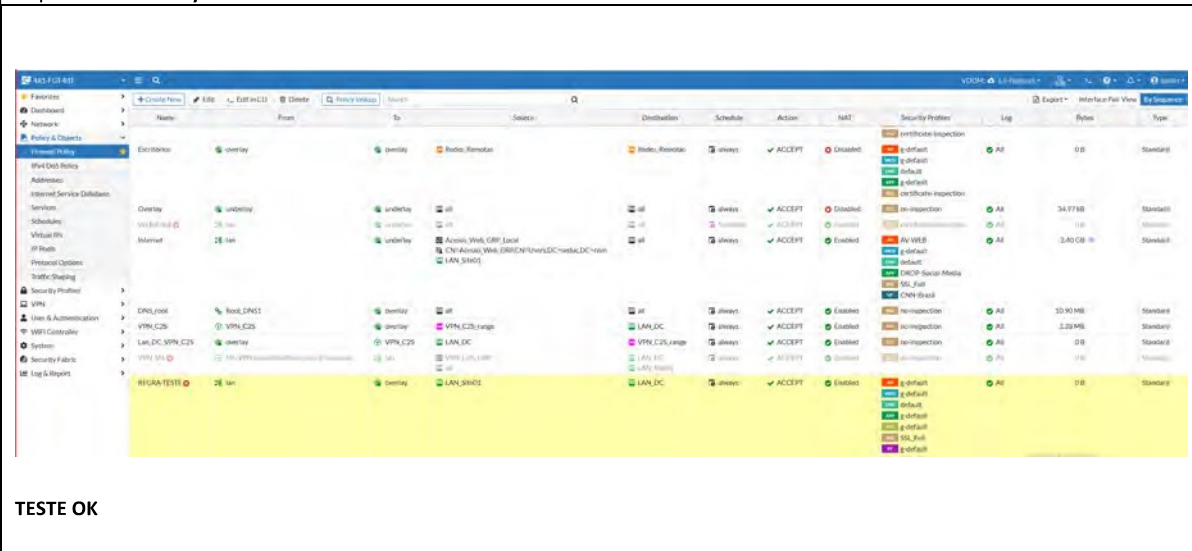
<p>Comentário</p>	
--------------------------	--

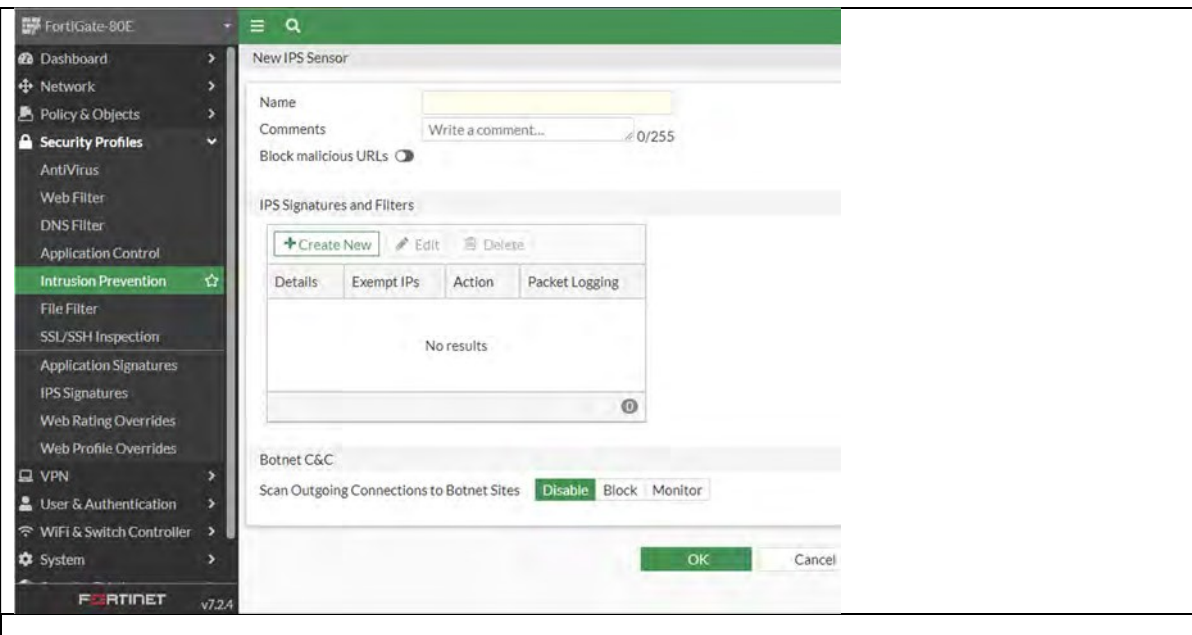
<p>Item de Teste - 5.3.1.1.6</p>	<p>Anti-Virus;</p>
<p>Objetivo do Teste</p>	<p>Validar se o FortiGate possui ferramenta de Anti-virus de forma nativa.</p>
<p>Configuração do Teste</p>	<p>Demonstrar base de regras do FortiGate.</p>
<p>Procedimento do Teste</p>	<p>Para acessar basta ir em Security Profile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

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

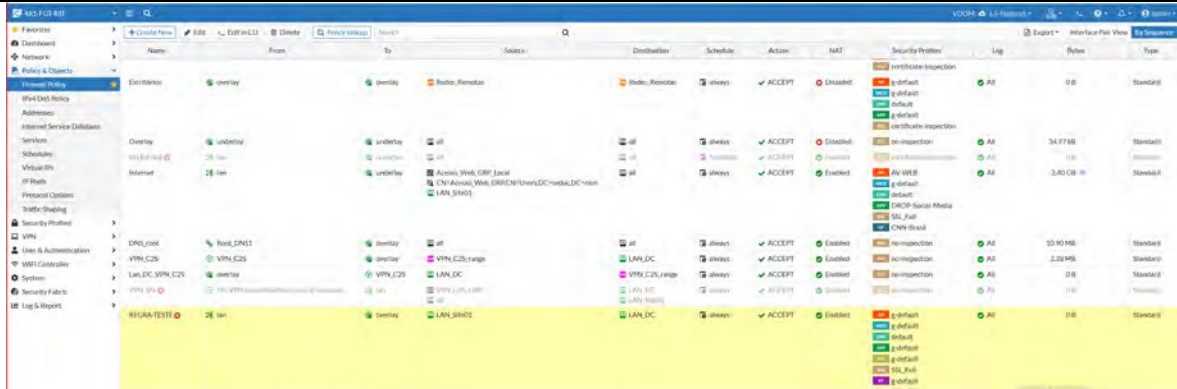
<p>Item de Teste - 5.3.1.1.7</p>	<p>SSL Inspection;</p>
<p>Objetivo do Teste</p>	<p>Validar se o firewall realiza SSL Inspection de forma nativa.</p>
<p>Configuração do Teste</p>	<p>Demonstrar base de regras do FortiGate</p>
<p>Procedimento do Teste</p>	<p>Para acessar basta ir em Security Profile ->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

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

<p>Item de Teste - 5.3.1.1.8</p>	<p>IDS/IPS;</p>
<p>Objetivo do Teste</p>	<p>Validar se o FortiGate tem as funcionalidades de IDS/IPS de forma nativa.</p>
<p>Configuração do Teste</p>	<p>Demonstrar base de regras do FortiGate</p>
<p>Procedimento do Teste</p>	<p>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</p>
<p>Evidências</p>	 <p>TESTE OK</p>

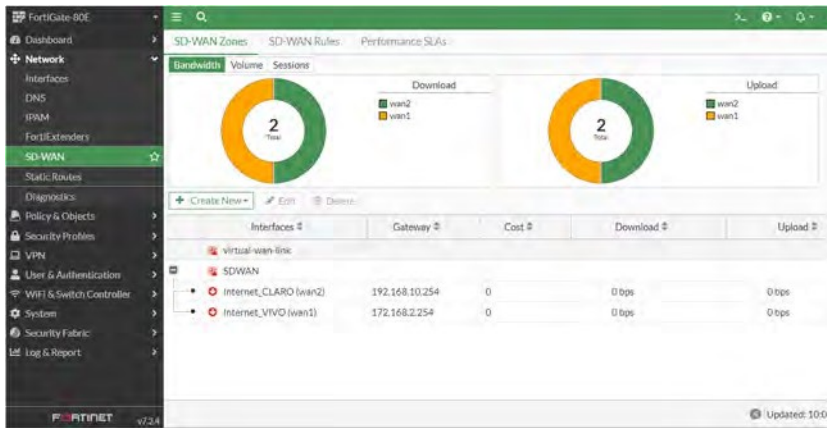
<p>Comentário</p>	
--------------------------	--

<p>Item de Teste - 5.3.1.1.9</p>	<p>SDWAN;</p>
<p>Objetivo do Teste</p>	<p>Validar se o equipamento possui a funcionalidade 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 regrar para enquadrar o algoritmo de balanceamento.</p>
<p>Evidências</p>	

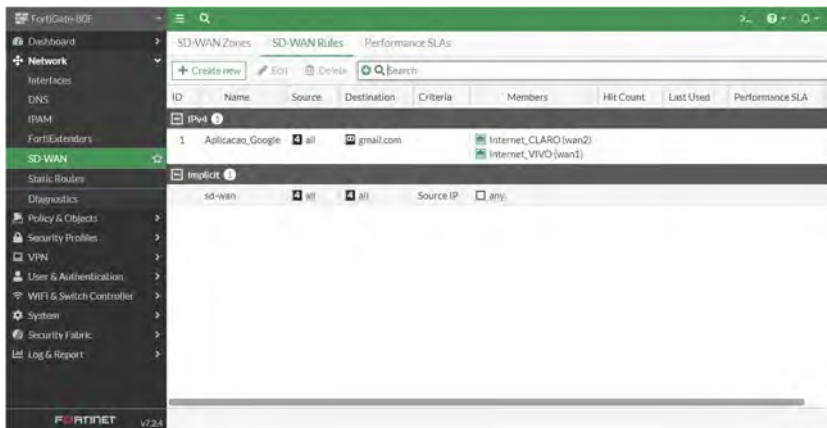


Name	From	To	Schedule	Action	NAT	Security Profile	Log	Bytes	Type
VPN_SITE_TO_SITE	VPN_SITE_TO_SITE	VPN_SITE_TO_SITE	anytime	ACCEPT	Enabled	no-inspection	ALL	0 B	Standard

TESTE OK





Interfaces	Gateway	Cost	Download	Upload
Internet_CLARO (wan2)	192.168.10.254	0	0 bps	0 bps
Internet_VIVO (wan1)	172.168.2.254	0	0 bps	0 bps



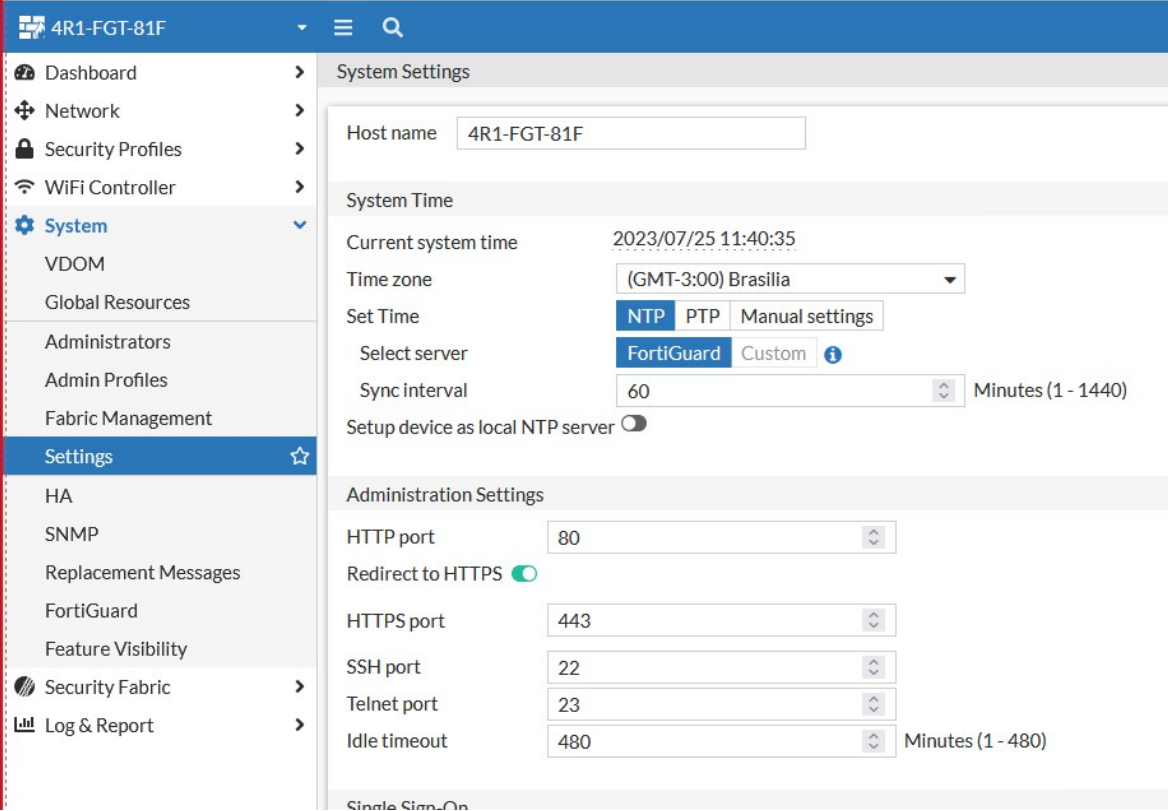
ID	Name	Source	Destination	Criteria	Members	Hit Count	Last Used	Performance SLA
1	Aplicacao_Google	all	gmail.com		Internet_CLARO (wan2) Internet_VIVO (wan1)			

Comentário

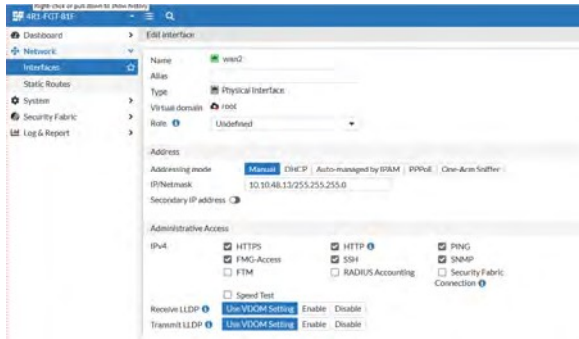
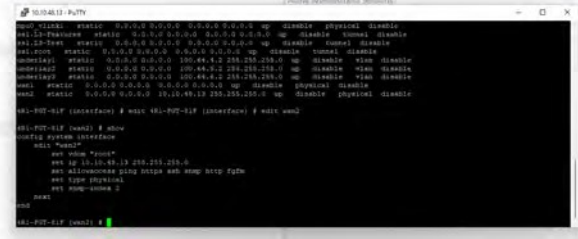
Item de Teste - 5.3.1.1.10	VPN site-to-site;
Objetivo do Teste	Validar se a ferramenta possibilita a criação de VPN site-to-site

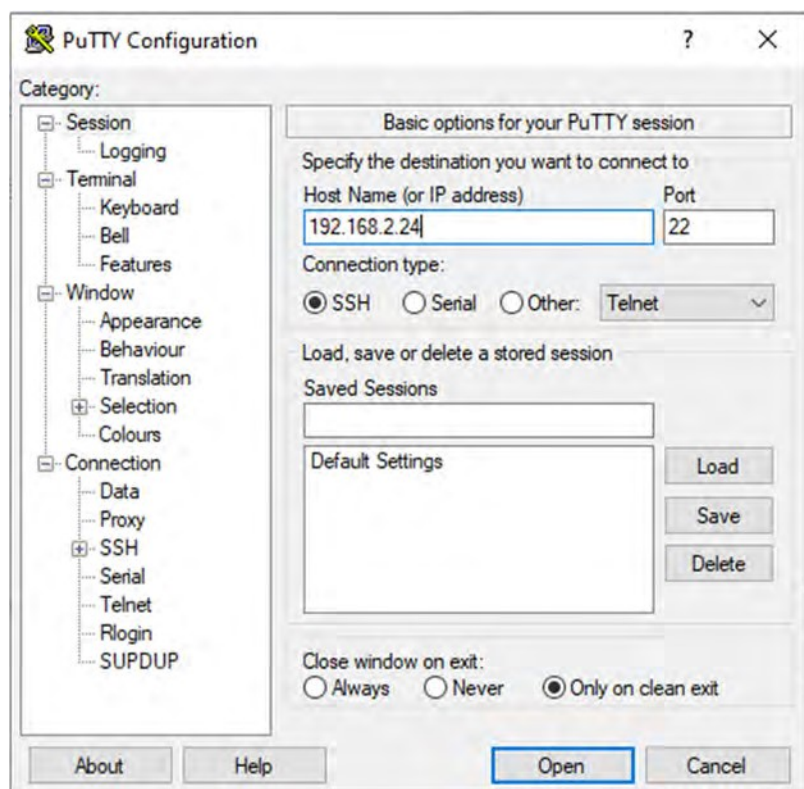
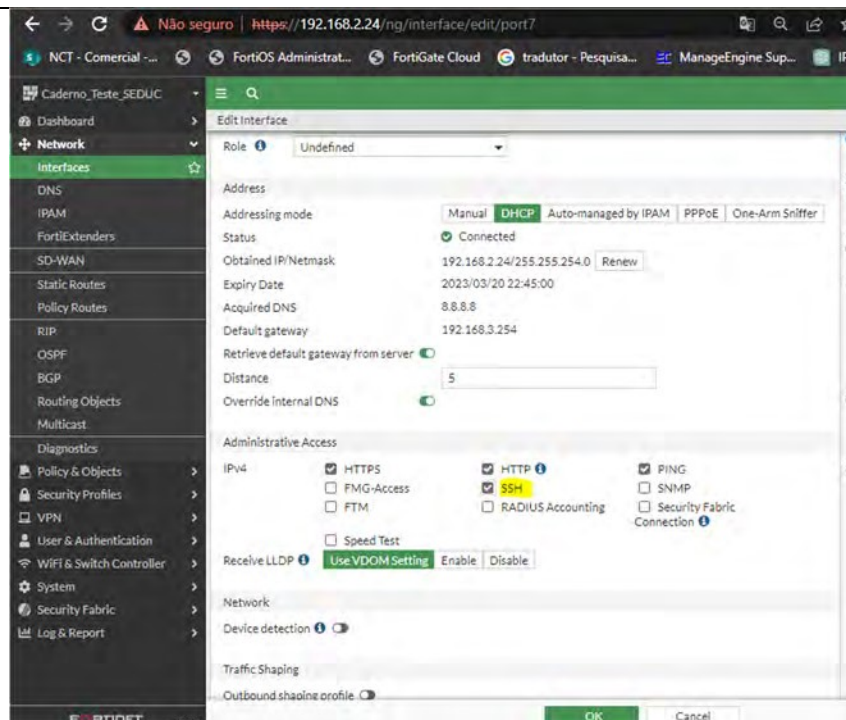
Configuração do Teste	Demonstrar base de regras do FortiGate.
Procedimento do Teste	Para acessar basta ir em VPN -> IPsec Tunnels -> Create New -> IPsec Tunnel.
Evidências	<div style="text-align: center;">  </div> <p>TESTE OK</p> <div style="text-align: center;">  </div>
Comentário	

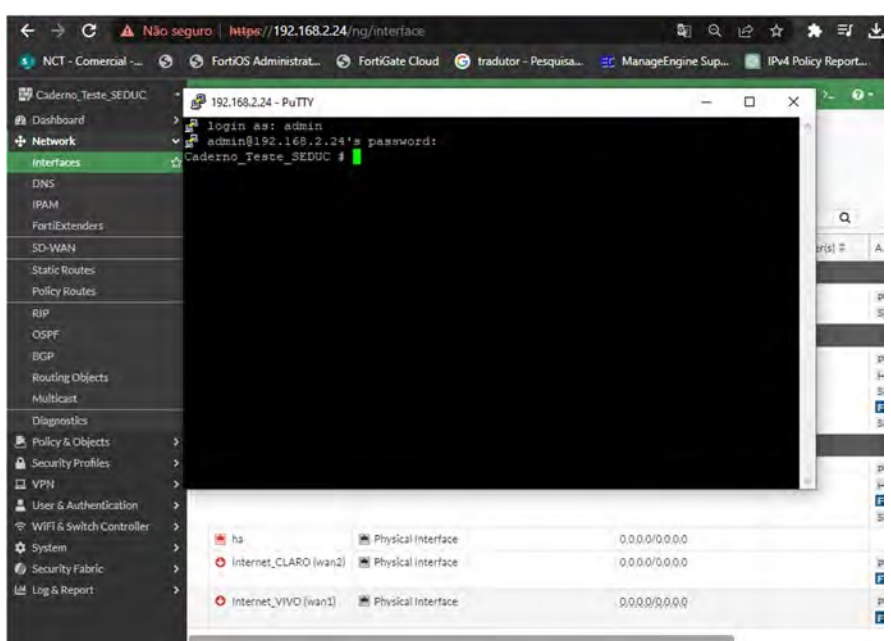
Item de Teste - 5.3.1.4	Implementar interface gráfica Web segura, utilizando o protocolo HTTPS ou Console do próprio fabricante;
Objetivo do Teste	Validar se é possível realizar o acesso seguro por meio de HTTPS
Configuração do Teste	Visual e comprovação por meio de documentação.
Procedimento do Teste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

	 <p>The screenshot shows the FortiGate web interface for device 4R1-FGT-81F. The left sidebar contains navigation options: Dashboard, Network, Security Profiles, WiFi Controller, System (selected), VDOM, Global Resources, Administrators, Admin Profiles, Fabric Management, Settings (starred), HA, SNMP, Replacement Messages, FortiGuard, Feature Visibility, Security Fabric, and Log & Report. The main content area is titled 'System Settings' and includes sections for System Time (Host name: 4R1-FGT-81F, Current system time: 2023/07/25 11:40:35, Time zone: (GMT-3:00) Brasilia, Set Time: NTP/PTP/Manual settings, Select server: FortiGuard/Custom, Sync interval: 60 Minutes), Administration Settings (HTTP port: 80, Redirect to HTTPS: ON, HTTPS port: 443, SSH port: 22, Telnet port: 23, Idle timeout: 480 Minutes), and Administrative Access (IPv4: HTTPS, FMG-Access, FTM, HTTP, SSH, RADIUS Accounting, PING, SNMP, Security Fabric Connection, Speed Test; Receive/Transmit LLDP: Use VDOM Setting, Enable, Disable).</p> <p>TESTE OK</p> <p>Administrative Access</p> <p>IPv4</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> FMG-Access <input checked="" type="checkbox"/> FTM <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> SSH <input checked="" type="checkbox"/> RADIUS Accounting <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> SNMP <input checked="" type="checkbox"/> Security Fabric Connection <input type="checkbox"/> Speed Test <p>Receive LLDP <input checked="" type="checkbox"/> Use VDOM Setting Enable Disable</p> <p>Transmit LLDP <input checked="" type="checkbox"/> Use VDOM Setting Enable Disable</p>
Comentário	

Item de Teste - 5.3.1.6	Implementar interface CLI segura através do protocolo SSH;
-----------------------------------	--

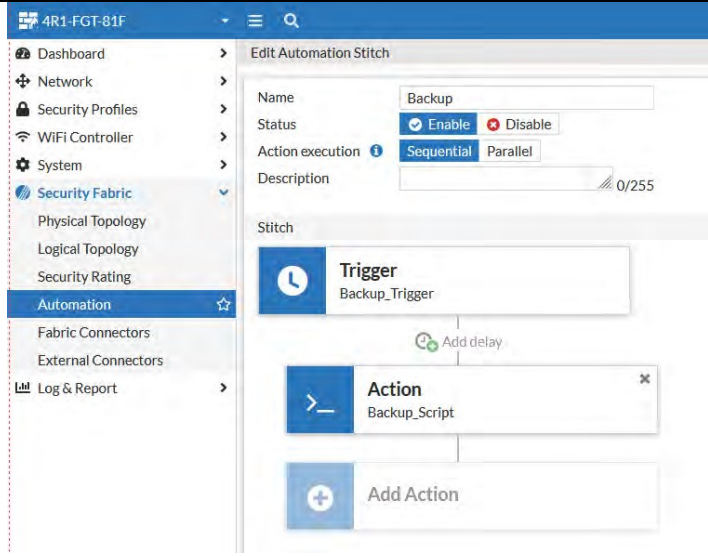
Objetivo do Teste	Verificar se o firewall é capaz de implementar interface CLI por meio do protocolo SSH porta 22 para acesso administrativo.
Configuração do Teste	Liberar acesso administrativo seguro SSH na interface que deseja fazer o acesso, após liberar o acesso é necessário utilizar alguma ferramenta 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	<div style="display: flex; align-items: center;">   </div> <p style="margin-top: 10px;">TESTE OK</p>



<p>Comentário</p>	 <p>The screenshot shows the FortiGate web management interface. On the left, a navigation menu is visible with categories like Network, Policy & Objects, and Security Profiles. The 'Network' section is expanded, showing 'Interfaces'. A terminal window (PuTTY) is overlaid on the interface, displaying a successful login for the 'admin' user at IP 192.168.2.24. Below the terminal, a table lists physical interfaces: 'ha', 'Internet_CLARO (wan2)', and 'Internet_VIVO (wan1)', all with IP addresses of 0.0.0.0/0.0.0.</p>
--------------------------	---

<p>Item de Teste - 5.3.1.9</p>	<p>Deve oferecer as funcionalidades de backup/restore e deve permitir ao administrador agendar backups da configuração em determinado dia e hora;</p>
<p>Objetivo do Teste</p>	<p>Verificar se o FortiGate é capaz de realizar backup/restore e se é possível realizar de forma agendada.</p>
<p>Configuração do Teste</p>	<p>1 – Validar se o Firewall possui as funcionalidades de backup/restore</p> <p>2- Validar se a ferramenta permite o agendamento de backups de forma automática.</p>
<p>Procedimento do Teste</p>	<p>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".</p>

Evidências



4R1-FGT-81F

Dashboard

Network

Security Profiles

WiFi Controller

System

Security Fabric

Physical Topology

Logical Topology

Security Rating

Automation

Fabric Connectors

External Connectors

Log & Report

Edit Automation Stitch

Name: Backup

Status: Enable Disable

Action execution: Sequential Parallel

Description: /255

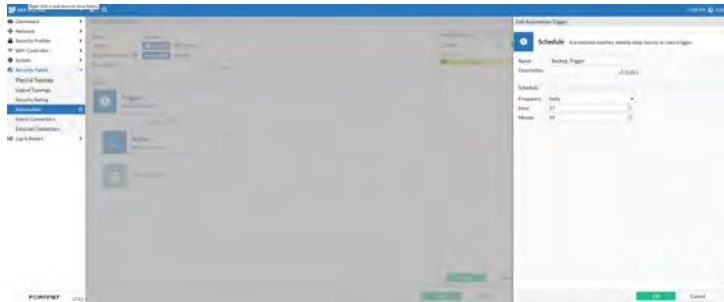
Stitch

Trigger: Backup_Trigger

Add delay

Action: Backup_Script

Add Action



Edit Automation Trigger

Name: Backup_Trigger

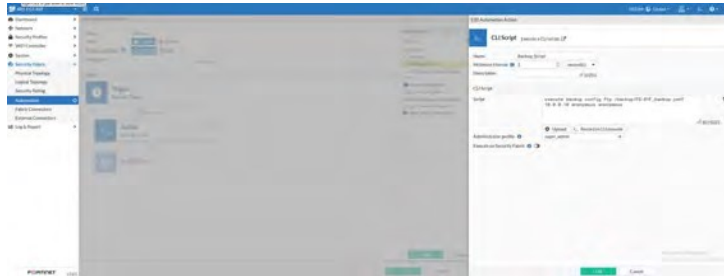
Description: /255

Schedule: /255

Frequency: Daily

Hour: 17

Minute: 00



Edit Automation Action

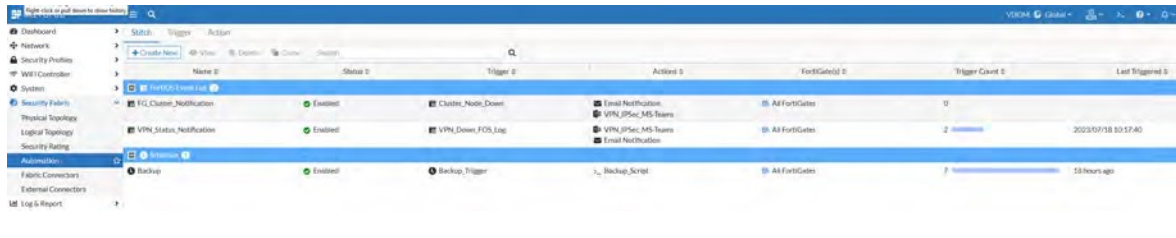
Name: Backup_Script

Description: /255

Script: /255

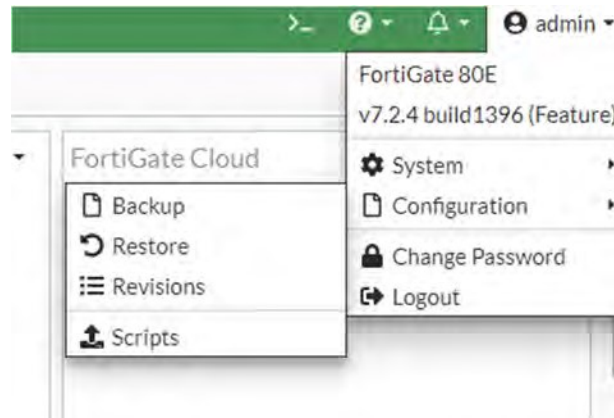
Script: curl -s -o /dev/null -w '%{httpcode}%' http://10.10.10.10:8080/

Authentication profile: /255

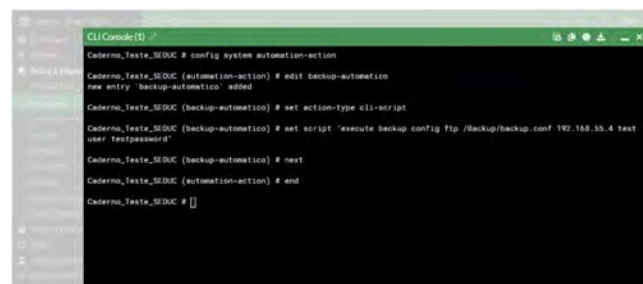


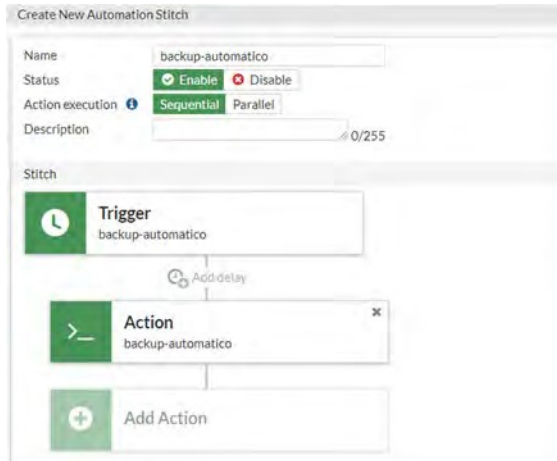
Name	Status	Trigger	Action	FortiGate(s)	Trigger Count	Last Triggered
FortiGate_Health_Web	Enabled	Cluster_Node_Down	Email_Notification	All FortiGates	0	
FCI_Cluster_Notification	Enabled	VPN_Down_FOS_Exp	VPN_Profile_MIS_Suave	All FortiGates	2	2023/07/18 10:17:40
Backup	Enabled	Backup_Trigger	Backup_Script	All FortiGates	7	53 hours ago

TESTE OK



```
FortiGate-80E (automation-trigger) # end
FortiGate-80E # config system automation-trigger
FortiGate-80E (automation-trigger) # edit backup-automatigo
FortiGate-80E (backup-automatigo) # set trigger-type scheduled
FortiGate-80E (backup-automatigo) # set trigger-frequency daily
FortiGate-80E (backup-automatigo) # set trigger-hour 23
FortiGate-80E (backup-automatigo) # set trigger-minute 58
FortiGate-80E (backup-automatigo) # next
FortiGate-80E (automation-trigger) # end
FortiGate-80E #
```



	<pre> config system automation-stitch edit "backup-automatigo" set trigger "backup-automatigo" config actions edit 1 set action "backup-automatigo" set required enable next end next end end </pre> 	
Comentário	https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-send-automated-backups-of-the-configuration/ta-p/198364	

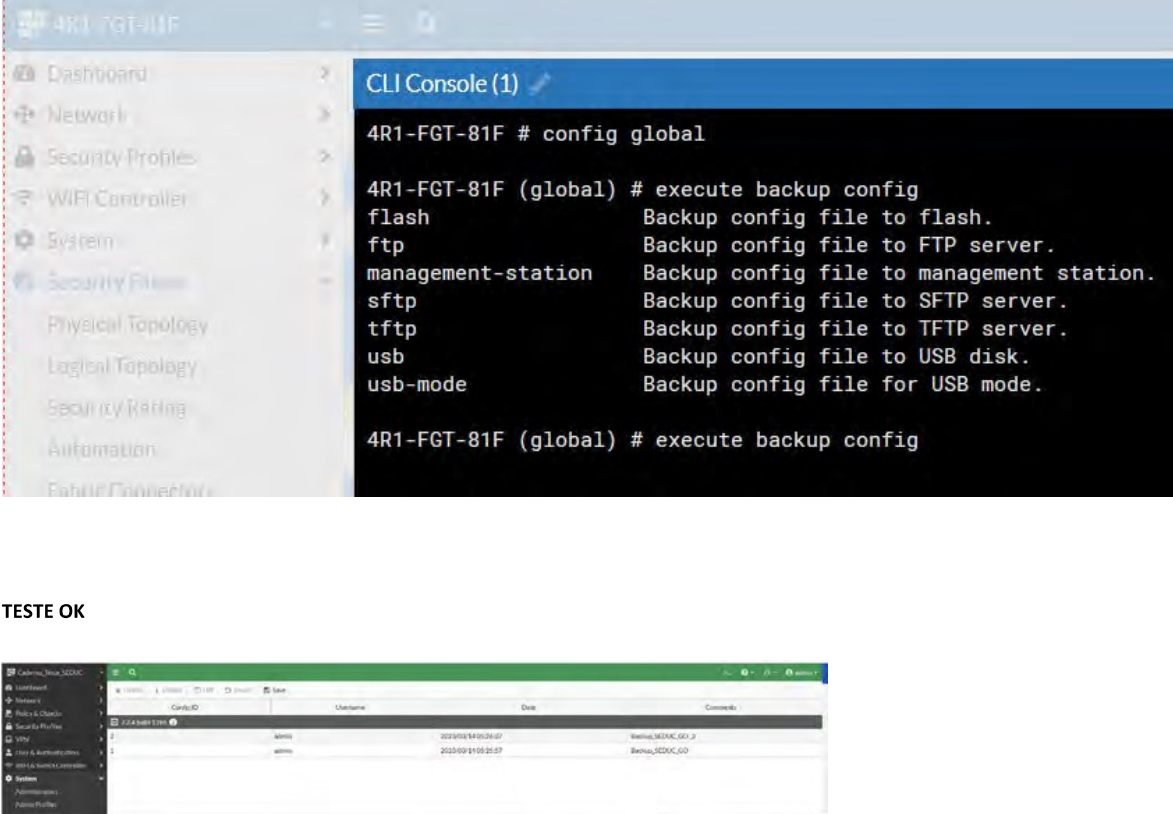
Item de Teste - 5.3.1.10	A solução de permitir armazenar os backups localmente, bem como transferi-los para um servidor remoto;
Objetivo do Teste	Demonstrar capacidade de realizar backup de configurações de forma local (no FortiGate) e de forma remota.
Configuração do Teste	Demonstrar base de regras 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	

Automation Stitches List:

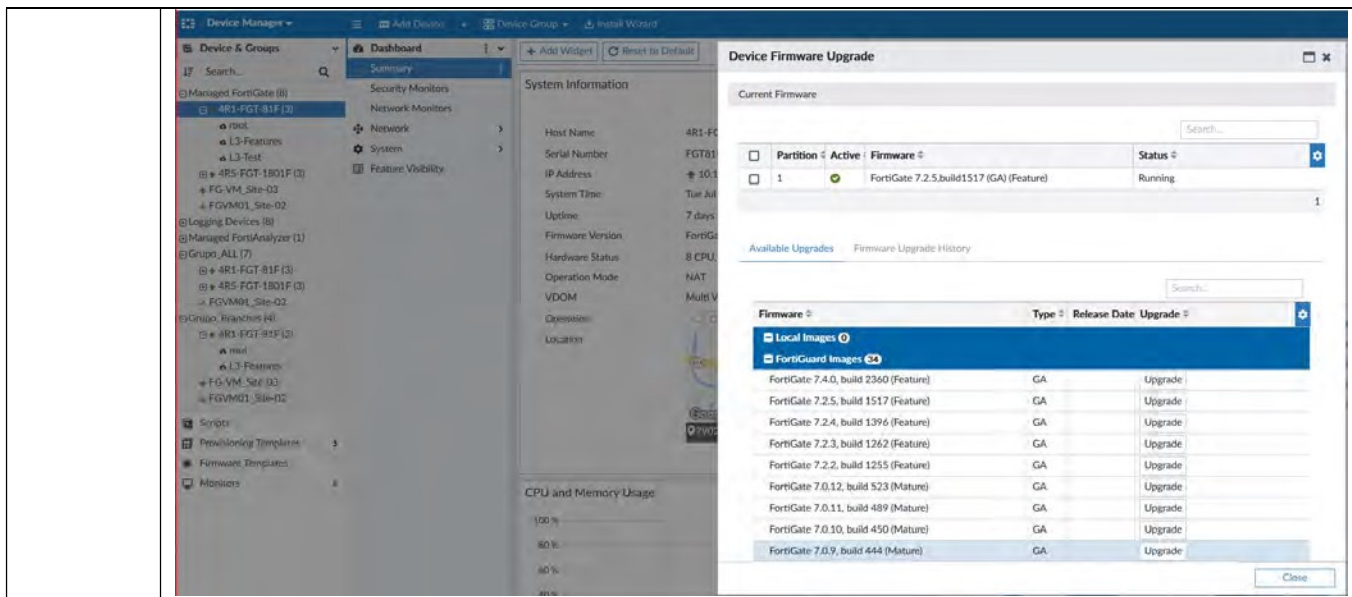
ID	Name	User	Date	Action
1	7411554010400	admin	2023/03/08 18:28:03	Automatic backup Logg (4)
2	7411554010400	admin	2023/03/08 18:49:52	Automatic backup Logg (4)
3	7411554010400	admin	2023/03/08 18:52:56	Automatic backup Logg (4)

Create New Automation Stitch Configuration:

- Name: backup-automatico
- Status: Enable Disable
- Action execution: Sequential Parallel
- Description: 0/255
- Stitch:
 - Trigger: backup-automatico
 - Action: backup-automatico
 - Buttons: Add delay, Add Action

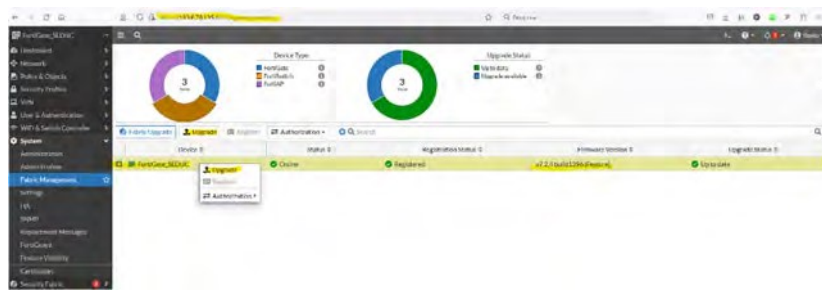
	 <p>TESTE OK</p>
Comentário	<p>Fonte: https://docs.fortinet.com/document/FortiGate/7.2.3/administration-guide/702257</p>

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	




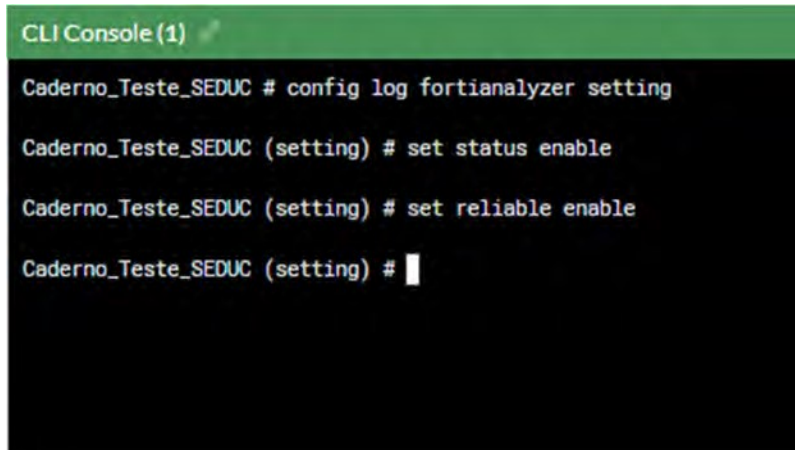
TESTE OK

O processo de atualização pode acontecer de diversas formas, umas delas é acessando a console gráfica do equipamento pelo IP de uma interface, através do protocolo seguro HTTPS, via CLI com SSH, ou por meio de uma VPN executando o mesmo procedimento.



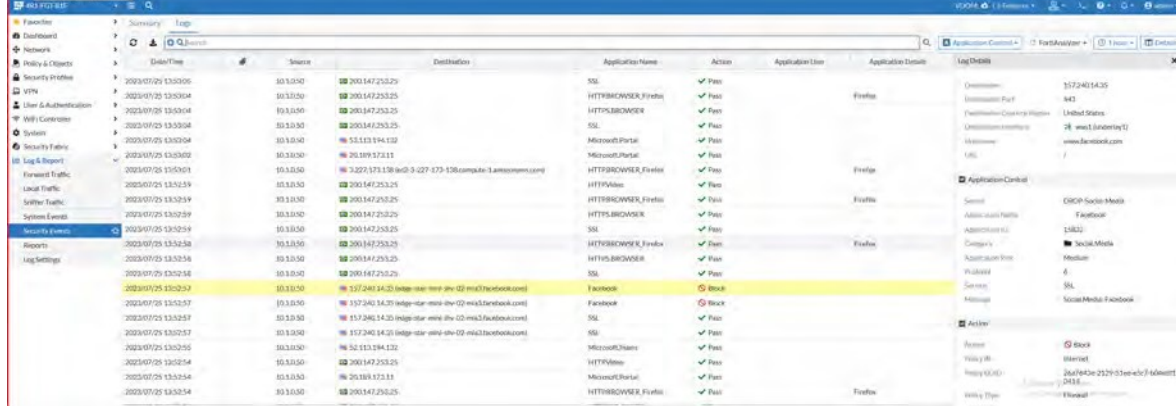
Comentário Fonte: <https://docs.fortinet.com/document/FortiGate/7.2.3/administration-guide/596131>

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 "Reliable" no FortiGate. Tal funcionalidade fica dentro de: config log fortianalyzer setting

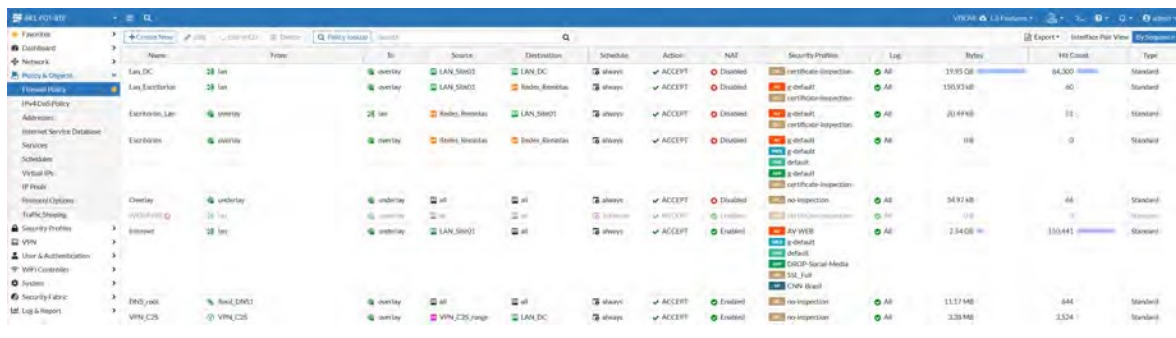
<p>Evidências</p>	 <p>TESTE OK</p> <p>Tal funcionalidade habilita a função de armazenamento em cache dos logs caso aconteça a perda de comunicação com o FortiAnalyzer, assim criando uma fila de logs a serem enviados para o FAZ quando a comunicação for restabelecida.</p>  <pre> CLI Console (1) Caderno_Testes_SEDUC # config log fortianalyzer setting Caderno_Testes_SEDUC (setting) # set status enable Caderno_Testes_SEDUC (setting) # set reliable enable Caderno_Testes_SEDUC (setting) # </pre>
<p>Comentário</p>	<p>https://docs.fortinet.com/document/FortiGate/7.2.0/new-features/942202/improve-fortianalyzer-log-caching</p>

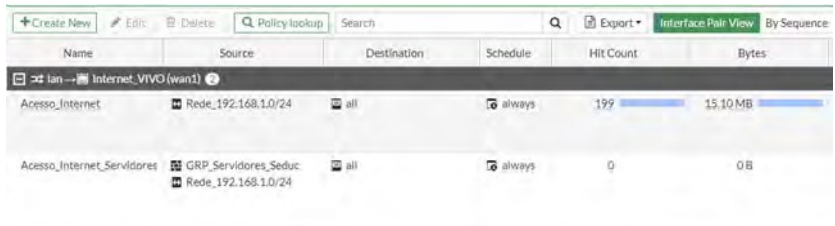
5.3.2 POLÍTICAS DE FIREWALL

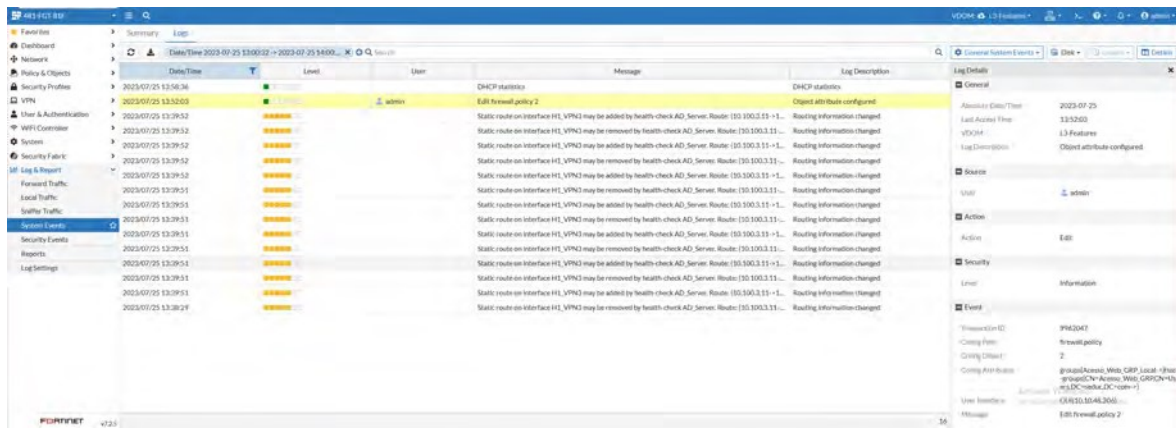
<p>Item de Teste - 5.3.2.18</p>	<p>Deve inspecionar e bloquear os dados operando como default gateway das redes protegidas e controlar o tráfego em nível de aplicações;</p>
<p>Objetivo do Teste</p>	<p>Demonstrar base de regras do FortiGate</p>
<p>Configuração do Teste</p>	<p>Demonstrar base de regras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

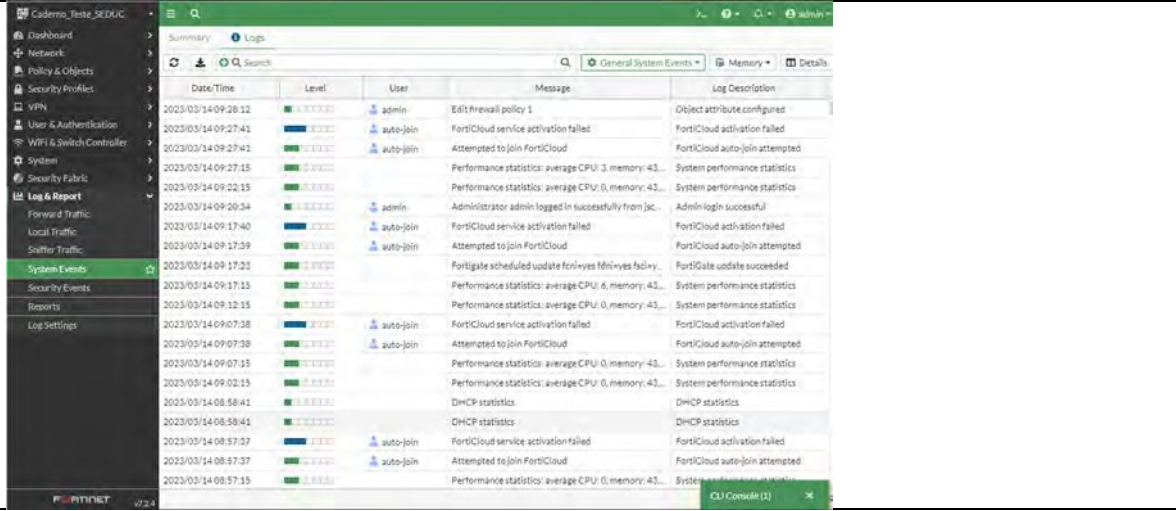
<p>Comentário</p>	 <p>TESTE OK</p>
--------------------------	---

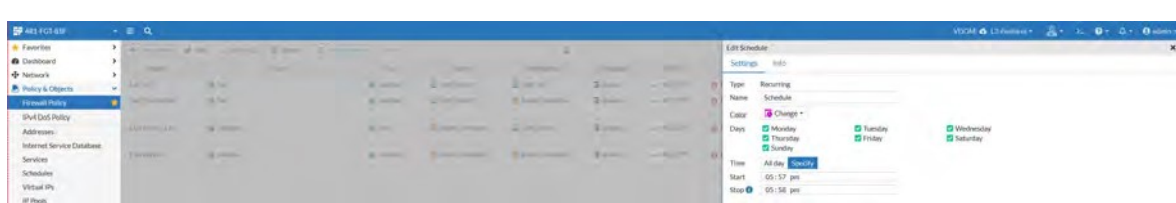
<p>Item de Teste - 5.3.2.20</p>	<p>A solução de Firewall, deve ser capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização;</p>
<p>Objetivo do Teste</p>	<p>Verificar se a solução de firewall é capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização.</p>
<p>Configuração do Teste</p>	<p>Demonstrar base de regras do FortiGate</p>
<p>Procedimento do Teste</p>	<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>

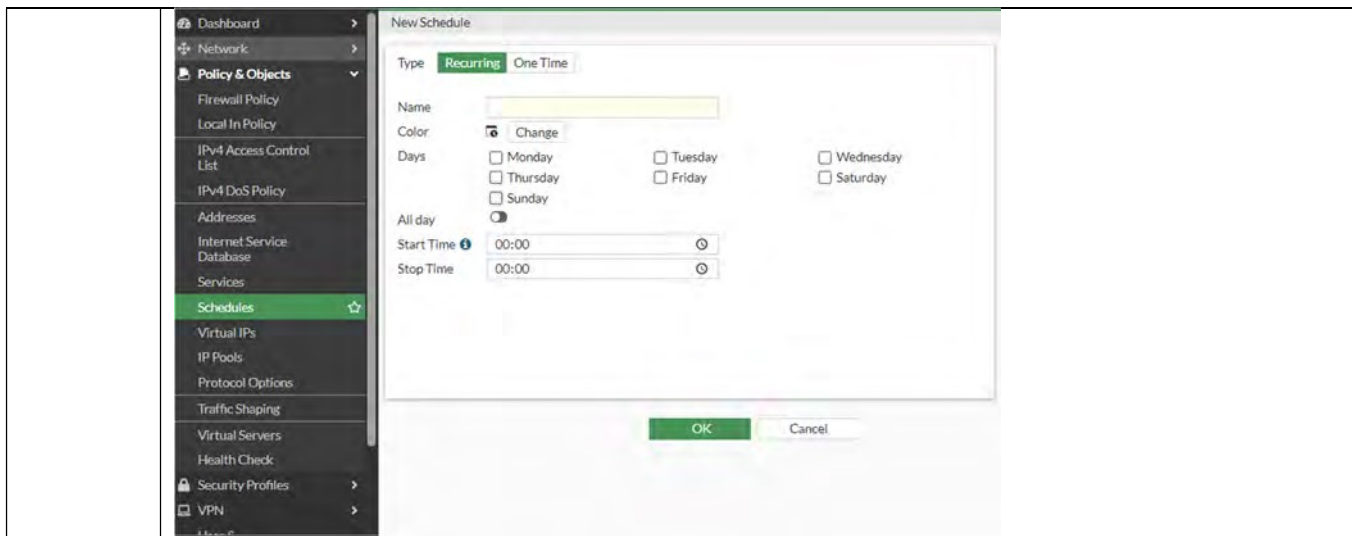
<p>Evidências</p>	 <p>TESTE OK</p>
--------------------------	---

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

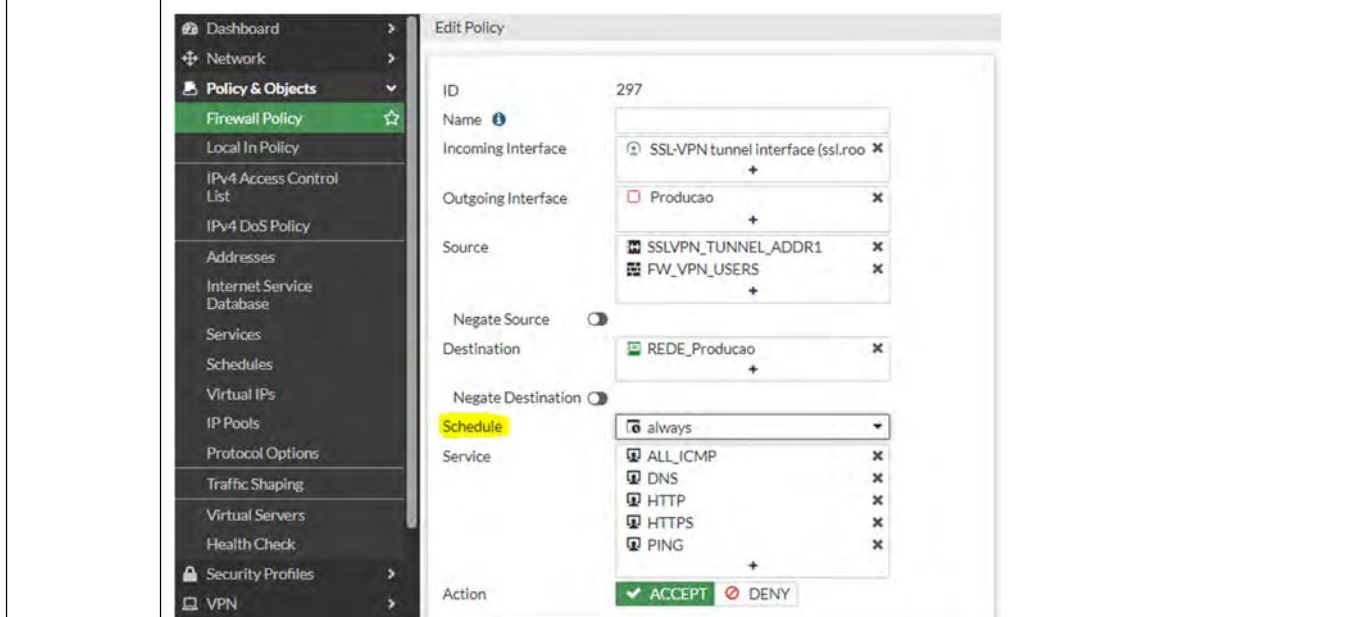
<p>Item de Teste - 5.3.2.21</p>	<p>Toda alteração de políticas e definições na console de gerenciamento deverá ser registrada e passível de auditoria;</p>
<p>Objetivo do Teste</p>	<p>Validar se a ferramenta faz o registro de todas as alterações feitas em regras e configurações, sendo passível de auditoria.</p>
<p>Configuração do Teste</p>	<p>Criar regras e demonstrar respectivo log.</p>
<p>Procedimento do Teste</p>	<p>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.</p>
<p>Evidências</p>	 <p>TESTE OK</p>

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

<p>Item de Teste - 5.3.2.23</p>	<p>Deverá permitir a ativação/desativação de regras de forma programada conforme a data/hora;</p>
<p>Objetivo do Teste</p>	<p>Validar se o FortiGate permite a ativação e desativação de regras de forma programada.</p>
<p>Configuração do Teste</p>	<p>Demonstrar base de regras do FortiGate</p>
<p>Procedimento do Teste</p>	<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>
<p>Evidências</p>	 <p>TESTE OK</p> <p>Criação do objeto de tempo "Schedule"</p>



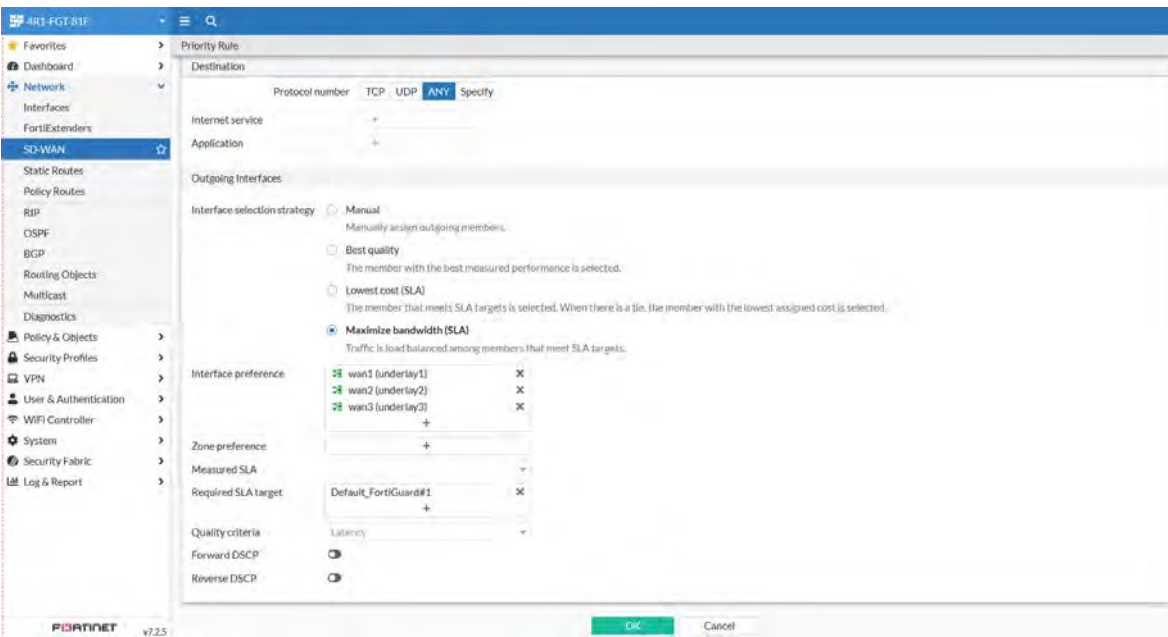
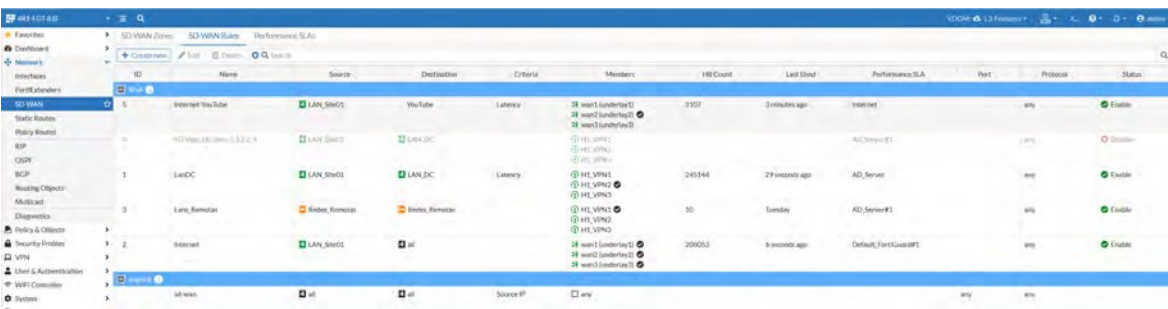

Aplicação do objeto "Schedule" dentro de uma política de firewall.



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	Demonstrar capacidade de balancear o tráfego de 2 links distintos através de SDWAN
Configuração do Teste	Demonstrar base de regras do FortiGate

<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>TESTE OK</p> <p>1- Criação dos membros (links) que vão participar do SDWAN</p> 

2- Definindo o algoritmo mais adequado para o balanceamento;

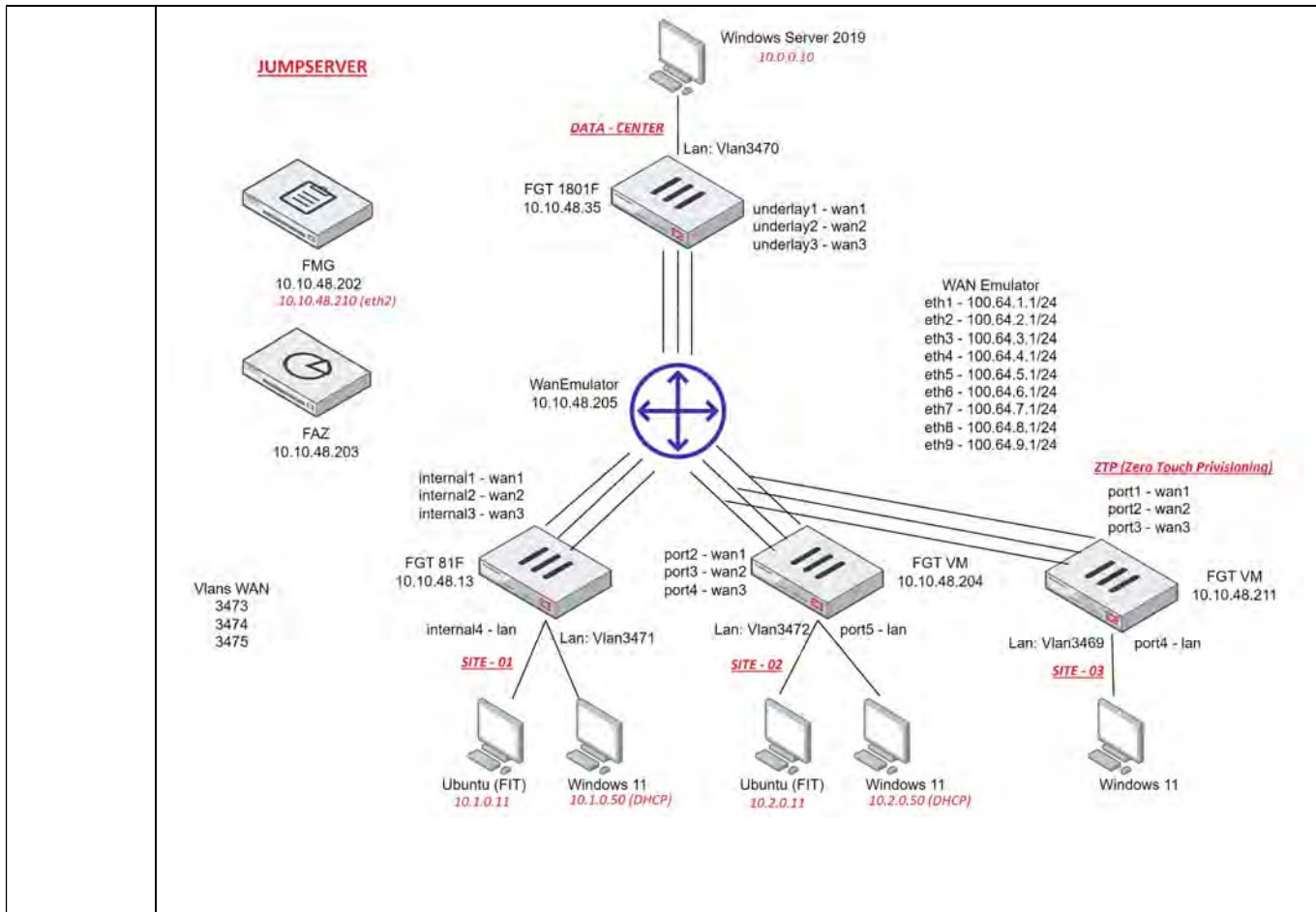


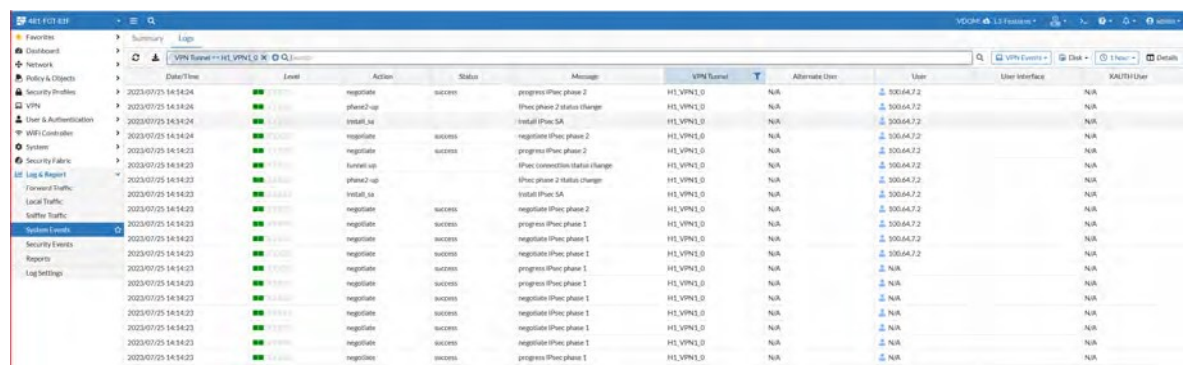
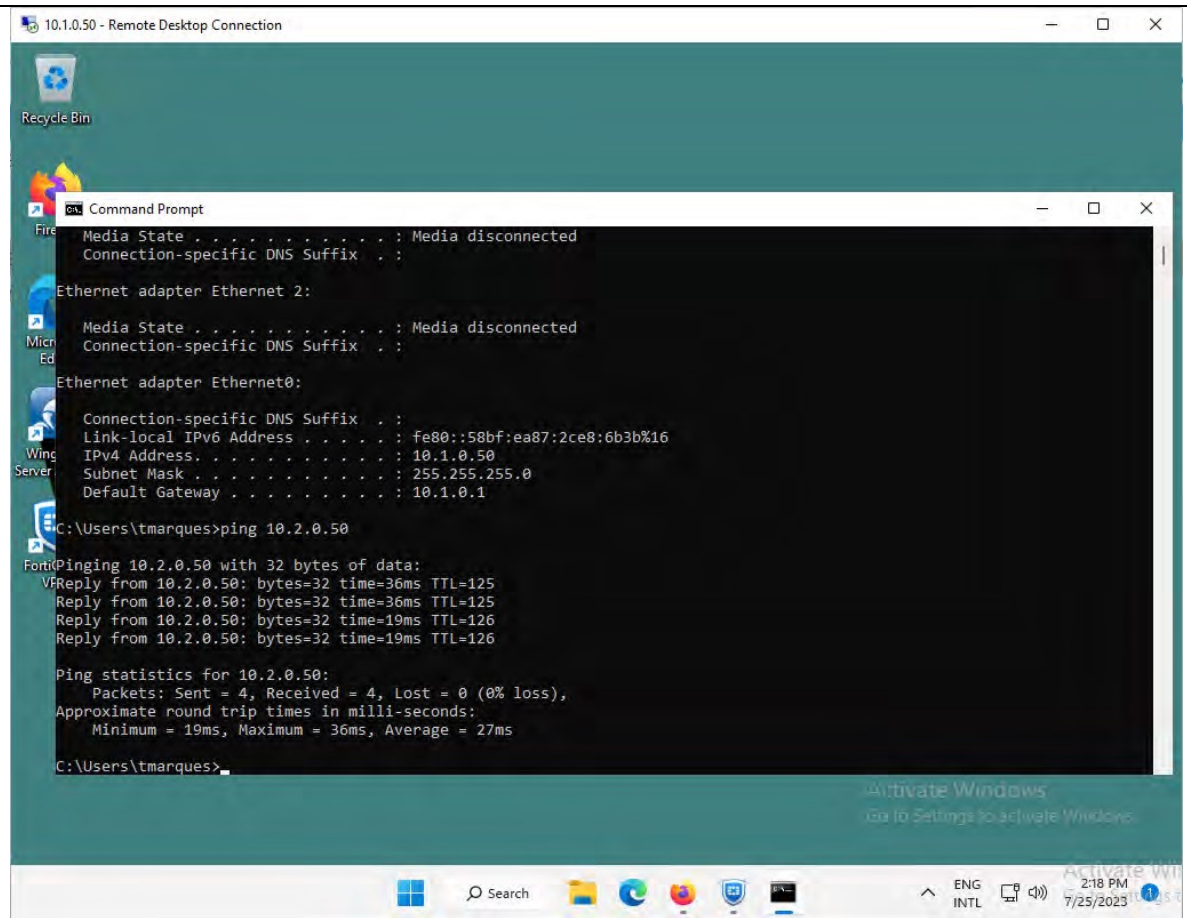
3- Criando rule de SDWAN para permitir que os membros (links) sejam balanceados através do algoritmo selecionado.

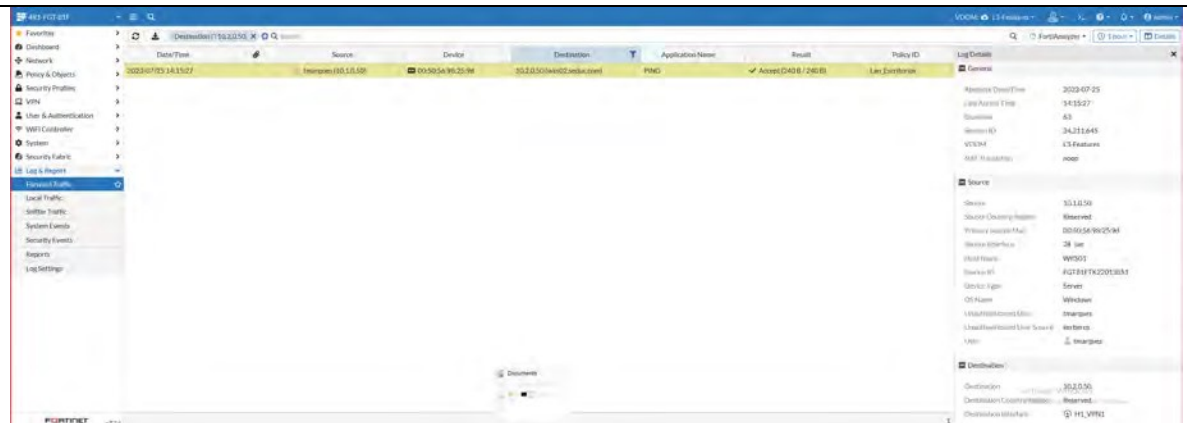


Comentário Fonte: <https://docs.fortinet.com/document/FortiGate/7.2.3/administration-guide/683285>

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 possível realizar a criação de tuneis IPsec VPN de forma dinâmica e criptografada, conforme evidências abaixo
Evidências	

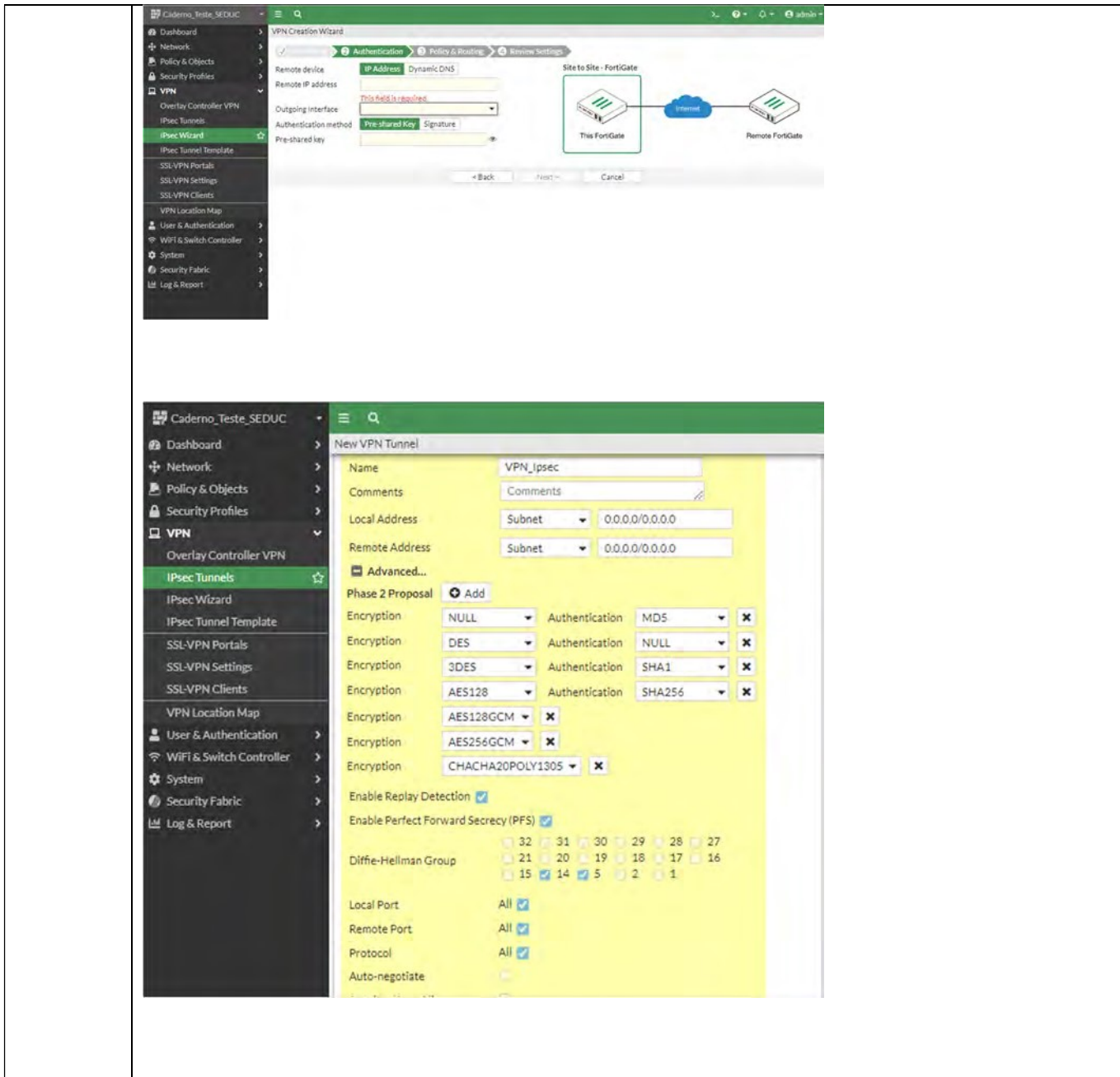






TESTE OK



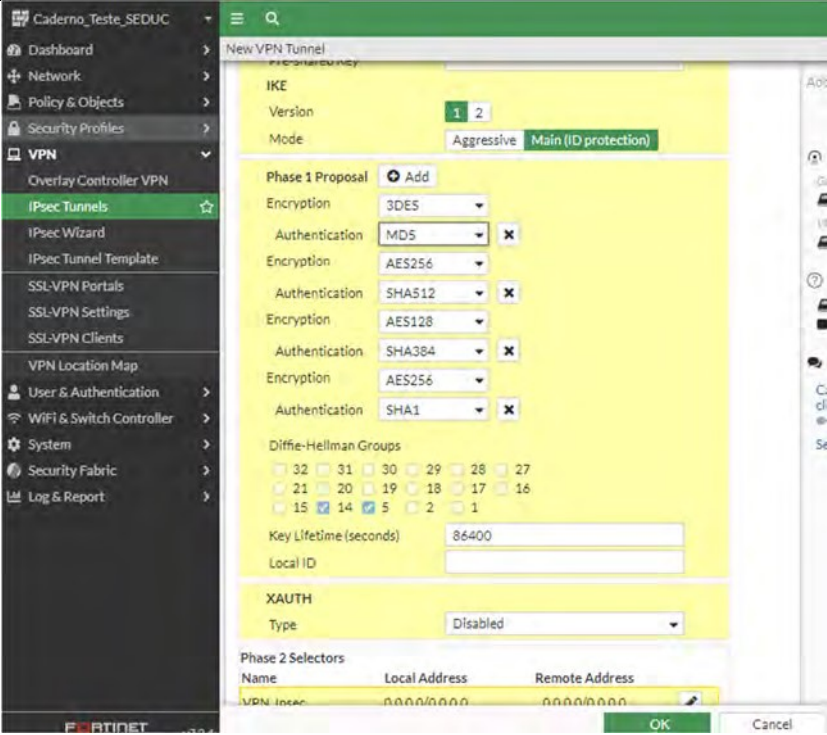


The top screenshot shows the 'VPN Creation Wizard' in the 'Authentication' step. It includes fields for 'Remote device' (IP Address), 'Remote IP address' (Dynamic DNS), 'Outgoing interface', 'Authentication method' (Pre-shared Key), and 'Pre-shared key'. A diagram shows 'This FortiGate' connected to 'Remote FortiGate' via an 'Internet' cloud.

The bottom screenshot shows the 'New VPN Tunnel' configuration page. It includes fields for 'Name' (VPN_ipsec), 'Local Address' (Subnet 0.0.0.0/0.0.0.0), and 'Remote Address' (Subnet 0.0.0.0/0.0.0.0). Under 'Advanced...', there is a list of Phase 2 proposals:

Encryption	Authentication	Action
NULL	MDS	X
DES	NULL	X
3DES	SHA1	X
AES128	SHA256	X
AES128GCM		X
AES256GCM		X
CHACHA20POLY1305		X

Additional options include 'Enable Replay Detection' (checked), 'Enable Perfect Forward Secrecy (PFS)' (checked), and 'Diffie-Hellman Group' (15, 14, 5, 2, 1). Local, Remote, and Protocol ports are set to 'All'.

	 <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 Fonte: Acessado em https://docs.fortinet.com/document/FortiGate/7.2.0/administration-guide/978793</p>
--	---

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;

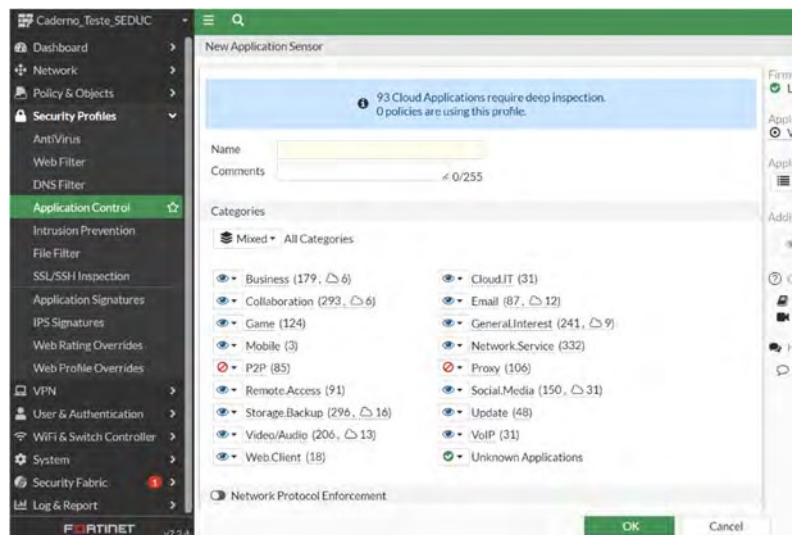
Navegando por **Security Profile > Application Control > Create new** é possível criar um novo perfil enquadrando as aplicações que deseja bloquear, monitorar ou aprovar;

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

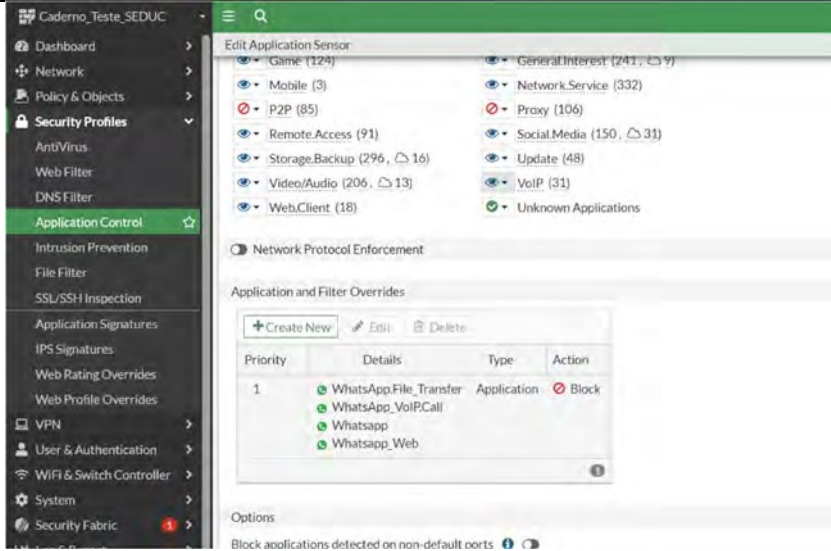
Date/Time	Source	Device	Destination	Application Name	Result	Policy ID	SID/AVN/Rule Name	Log Details
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	21.13.47.174 (instagram-p42-shv-01-mad3.facebook.net)	Instagram	Deny (Deny: UTM Blocked)	Internet	Internet	Deny (Deny: UTM Blocked)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	21.13.47.174 (instagram-p42-shv-01-mad3.facebook.net)	Instagram	Deny (Deny: UTM Blocked)	Internet	Internet	Deny (Deny: UTM Blocked)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	151.105.11.137	Microsoft/Outlook	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	21.13.47.174 (instagram-p42-shv-01-mad3.facebook.net)	Instagram	Deny (Deny: UTM Blocked)	Internet	Internet	Deny (Deny: UTM Blocked)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	151.105.11.137	Microsoft/Outlook	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	21.13.47.174 (instagram-p42-shv-01-mad3.facebook.net)	Instagram	Deny (Deny: UTM Blocked)	Internet	Internet	Deny (Deny: UTM Blocked)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	151.105.11.137	Microsoft/Outlook	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	104.92.229.104 (97-2-219.dyn.iad.comcast.com)	HTTBBROWSER	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	104.92.229.104 (97-2-219.dyn.iad.comcast.com)	HTTBBROWSER	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	84.2.226.223	Amazon/AMZ	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	84.2.226.223	HTTBBROWSER	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	84.2.226.223	HTTBBROWSER	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	142.251.127.340 (google.com)	YouTube	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	142.251.127.340 (google.com)	YouTube	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	142.251.127.340 (google.com)	YouTube	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	213.219.135.139 (ads-213-115-139.dsp.cloudflare.com)	Microsoft/Outlook	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	213.219.135.139 (ads-213-115-139.dsp.cloudflare.com)	Microsoft/Outlook	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	32.133.194.122	Microsoft/Outlook	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	104.103.100.100 (amazon.com)	DN6	Accept (UTM Allowed)	LAN, JTC	LAN, JTC	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	104.103.100.100 (amazon.com)	DN6	Accept (UTM Allowed)	LAN, JTC	LAN, JTC	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	151.105.11.137	Microsoft/Outlook	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	151.105.11.137	Microsoft/Outlook	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	139.127.42.138 (ads-139-127-42-138.dsp.cloudflare.com)	HTTBBROWSER	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	139.127.42.138 (ads-139-127-42-138.dsp.cloudflare.com)	HTTBBROWSER	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	200.147.57.200 (147-57.static.optonline.net)	HTTBBROWSER	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	200.147.57.200 (147-57.static.optonline.net)	HTTBBROWSER	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	84.2.226.223	SSL_TLS-12	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	84.2.226.223	HTTBBROWSER	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	84.2.226.223	HTTBBROWSER	Accept (UTM Allowed)	Internet	Internet	Accept (UTM Allowed)
2023/07/25 14:59:30	10.0.0.10	10.0.0.10	21.13.47.174 (instagram-p42-shv-01-mad3.facebook.net)	Instagram	Deny (Deny: UTM Blocked)	Internet	Internet	Deny (Deny: UTM Blocked)

TESTE OK

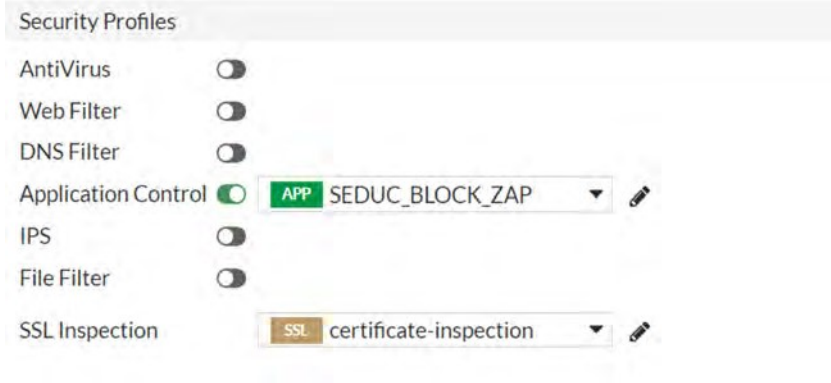
1 – Criando um perfil de Application Control



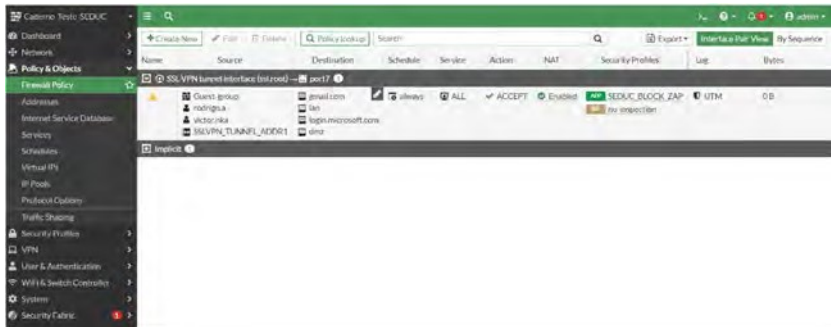
2 – Escolhendo quais categorias de aplicações vão ser permitidas, monitoradas e bloqueadas. Também é possível criar exceções dentro dessas categorias. No exemplo abaixo a categoria Social Media está para monitorar e a aplicação WhatsApp está com uma exceção para bloquear



3 – Enquadrando o perfil na política



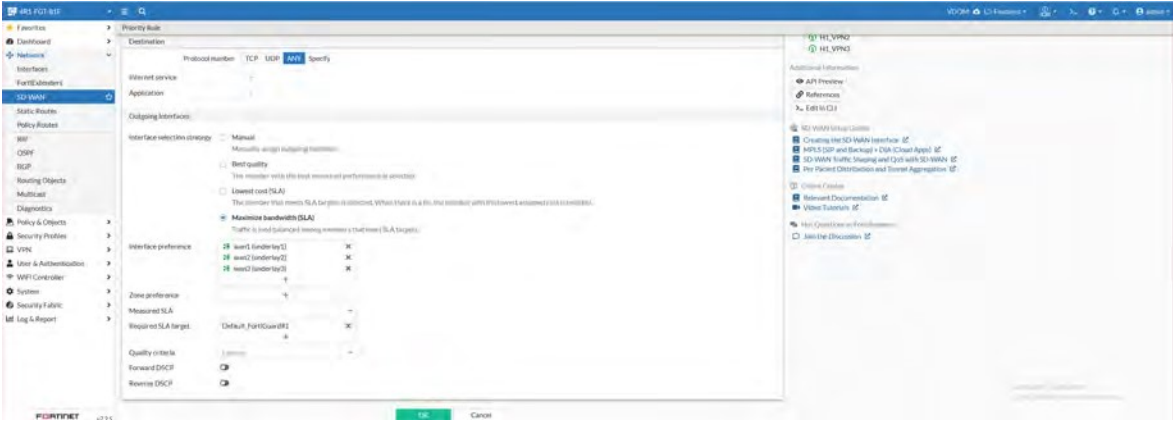
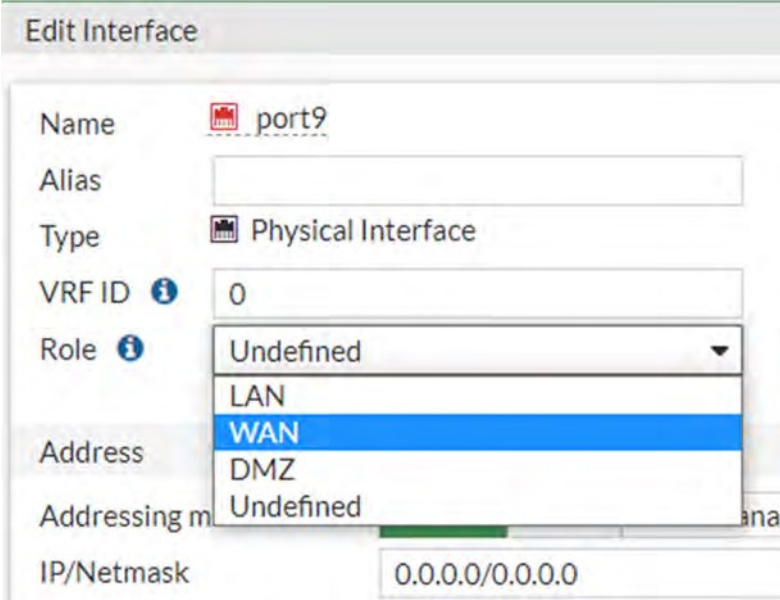
fica com o perfil enquadrado



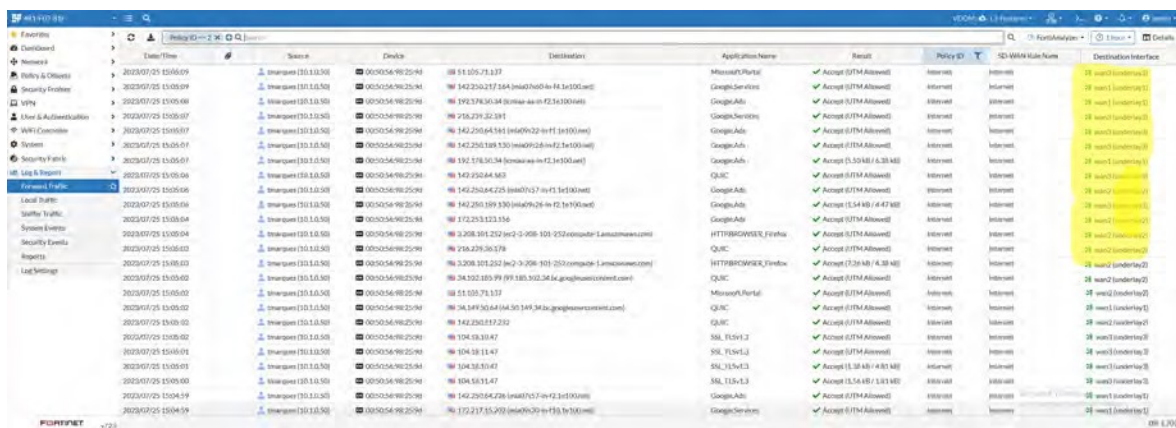
4 – Abaixo o exemplo de como a política

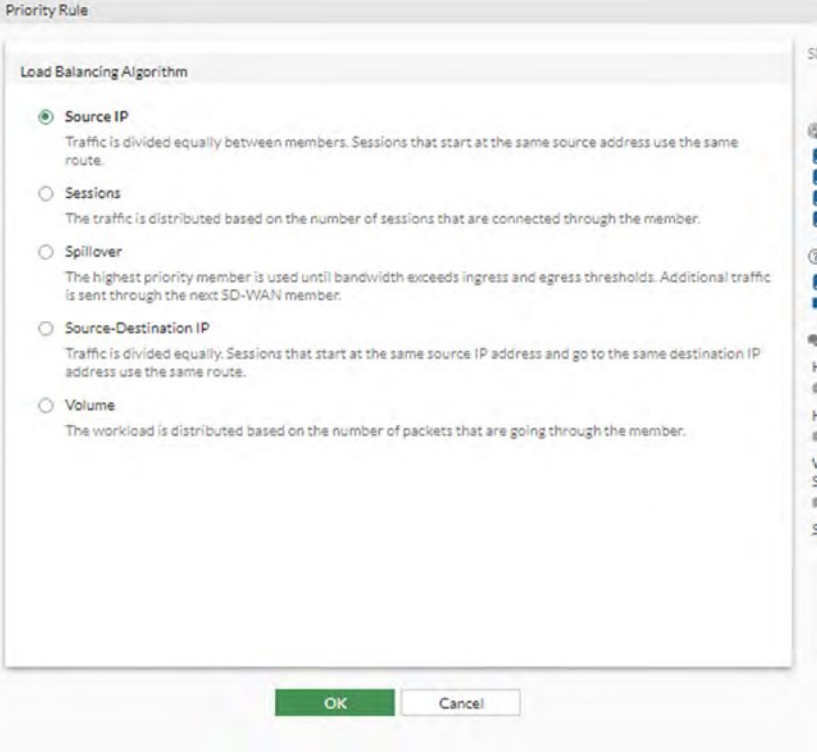
Comentário

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	 <p>TESTE OK</p> <p>Qualquer interface no FortiGate pode ser definida como uma interface WAN.</p> 

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	 <p>TESTE OK</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>	

441-FC1-837

ID	Name	Source	Destination	Criteria	Members	Hit Count	Last Used	Performance SLA	Port	Protocol	Status
5	Internet YouTube	LAN_SSH01	YouTube	Latency	sw1 (underlay1) sw2 (underlay2) sw3 (underlay3)	53	3 minutes ago	EdgeNet		any	Enable
1	LANDC	LAN_SSH01	LAN_DC	Latency	H1_VPN1 H1_VPN2 H1_VPN3	2300	14 seconds ago	AD_Server		any	Enable
2	Internet	LAN_SSH01	all		sw1 (underlay1) sw2 (underlay2) sw3 (underlay3)	2401	8 seconds ago	Default_FortiGuard#1		any	Enable

441-FC1-837

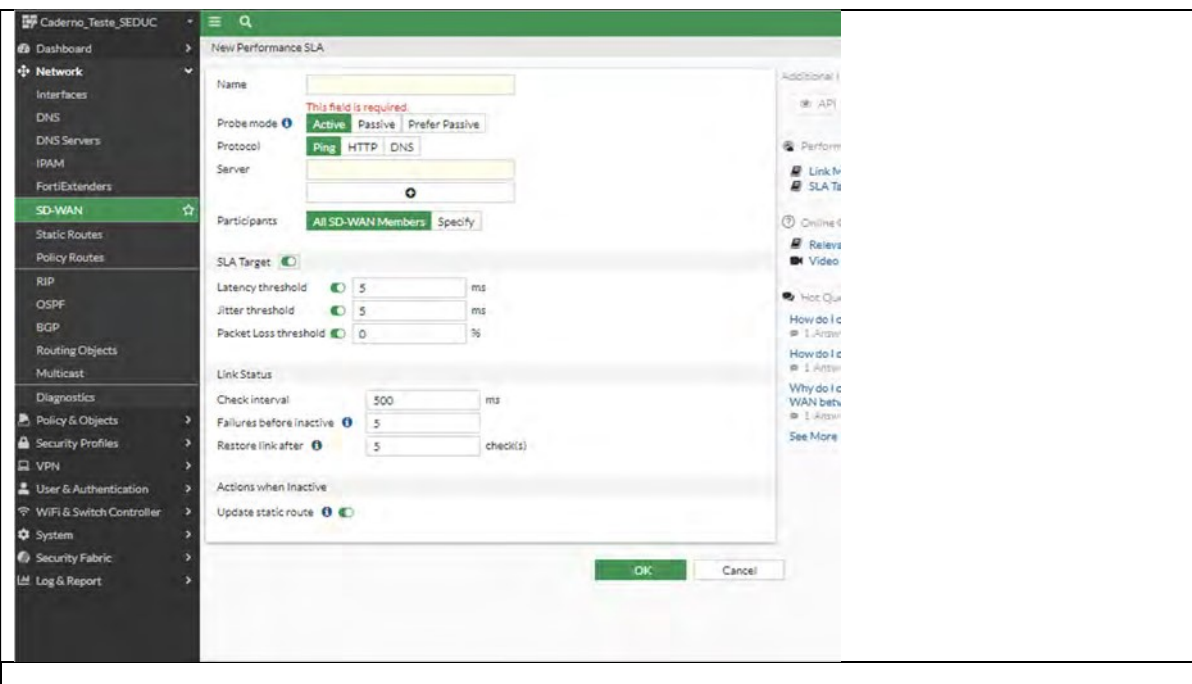


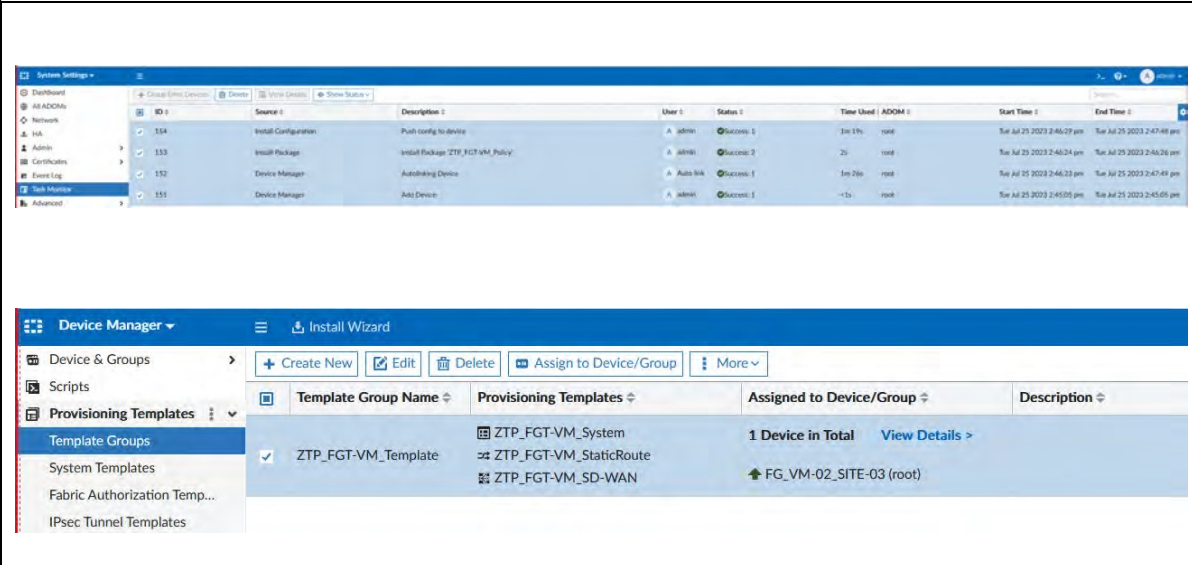
Name ID	Detected Server ID	Packet Loss	Latency	Jitter	Failure Threshold %	Recovery Threshold %
AD_Server	10.0.0.30	H1_VPN1 @ 0.00%	H1_VPN1 @ 22.29ms	H1_VPN1 @ 0.05ms	2	2
		H1_VPN2 @ 0.00%	H1_VPN2 @ 33.34ms	H1_VPN2 @ 0.09ms		
		H1_VPN3 @ 0.00%	H1_VPN3 @ 37.34ms	H1_VPN3 @ 0.13ms		

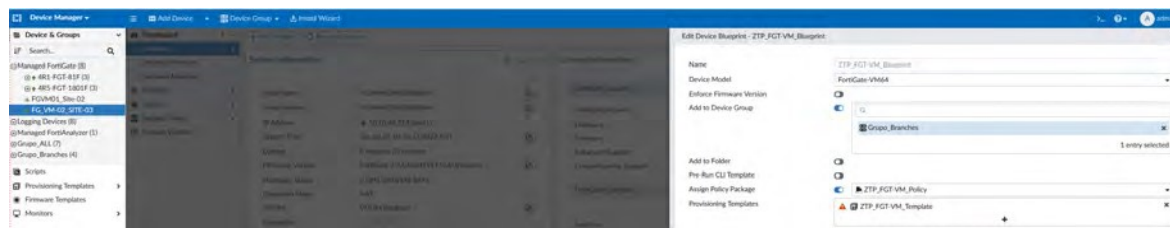
441-FC1-837

ID	Name	Source	Destination	Criteria	Members	Hit Count	Last Used	Performance SLA	Port	Protocol	Status
5	Internet YouTube	LAN_SSH01	YouTube	Latency	sw1 (underlay1) sw2 (underlay2) sw3 (underlay3)	54	24 seconds ago	Internet		any	Enable
1	LANDC	LAN_SSH01	LAN_DC	Latency	H1_VPN1 H1_VPN2 H1_VPN3	2311	9 seconds ago	AD_Server		any	Enable
2	Internet	LAN_SSH01	all		sw1 (underlay1) sw2 (underlay2) sw3 (underlay3)	2357	9 seconds ago	Default_FortiGuard#1		any	Enable

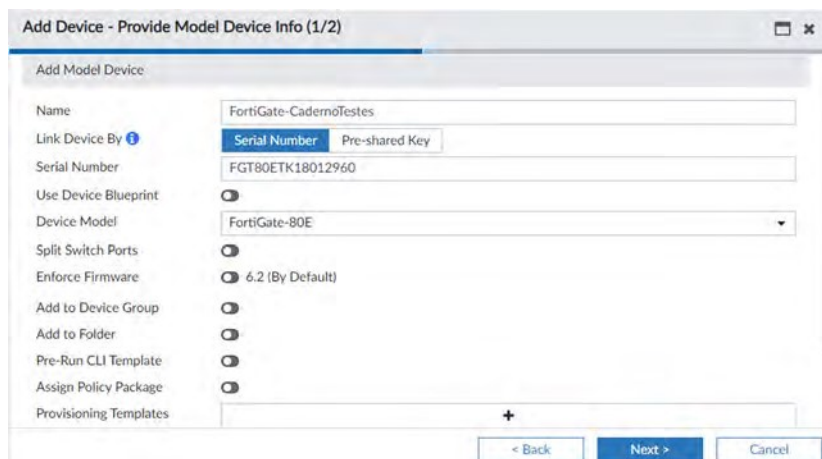
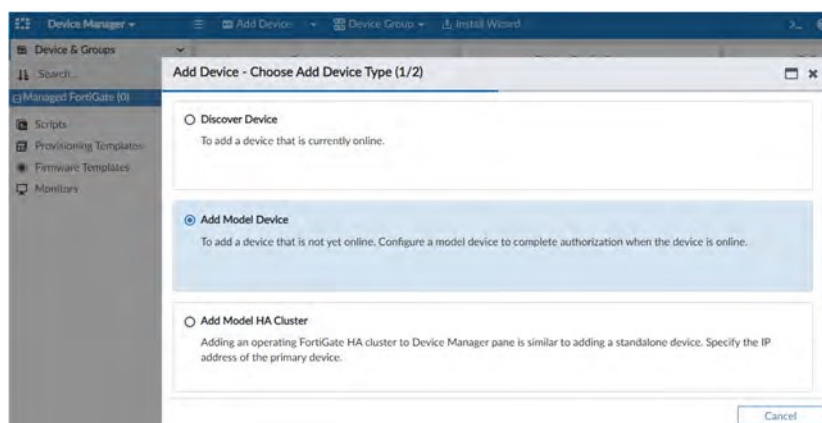
TESTE OK

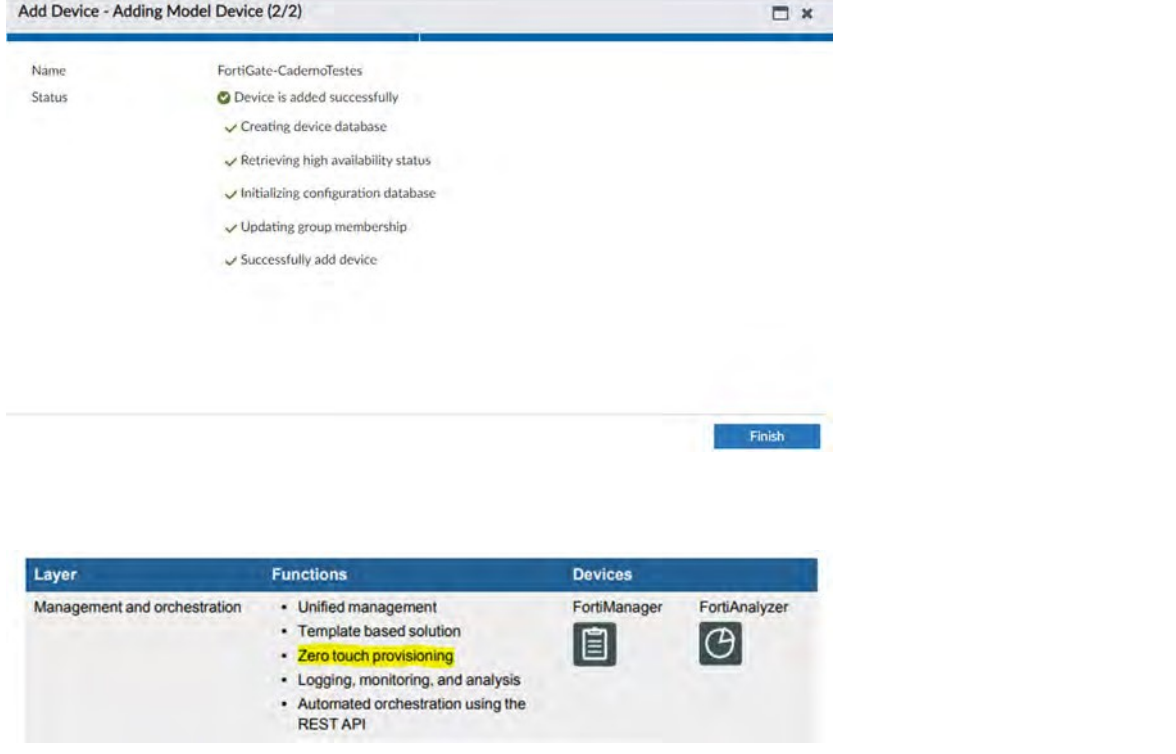






<p>Comentário</p>	
--------------------------	--


<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>								
<p>Evidências</p>	 <table border="1" data-bbox="239 1702 1420 1814"> <thead> <tr> <th>Template Group Name</th> <th>Provisioning Templates</th> <th>Assigned to Device/Group</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> ZTP_FGT-VM_Template</td> <td> <ul style="list-style-type: none"> ZTP_FGT-VM_System ZTP_FGT-VM_StaticRoute ZTP_FGT-VM_SD-WAN </td> <td>1 Device in Total View Details ></td> <td> <ul style="list-style-type: none"> FG_VM-02_SITE-03 (root) </td> </tr> </tbody> </table>	Template Group Name	Provisioning Templates	Assigned to Device/Group	Description	<input checked="" type="checkbox"/> ZTP_FGT-VM_Template	<ul style="list-style-type: none"> ZTP_FGT-VM_System ZTP_FGT-VM_StaticRoute ZTP_FGT-VM_SD-WAN 	1 Device in Total View Details >	<ul style="list-style-type: none"> FG_VM-02_SITE-03 (root)
Template Group Name	Provisioning Templates	Assigned to Device/Group	Description						
<input checked="" type="checkbox"/> ZTP_FGT-VM_Template	<ul style="list-style-type: none"> ZTP_FGT-VM_System ZTP_FGT-VM_StaticRoute ZTP_FGT-VM_SD-WAN 	1 Device in Total View Details >	<ul style="list-style-type: none"> FG_VM-02_SITE-03 (root) 						

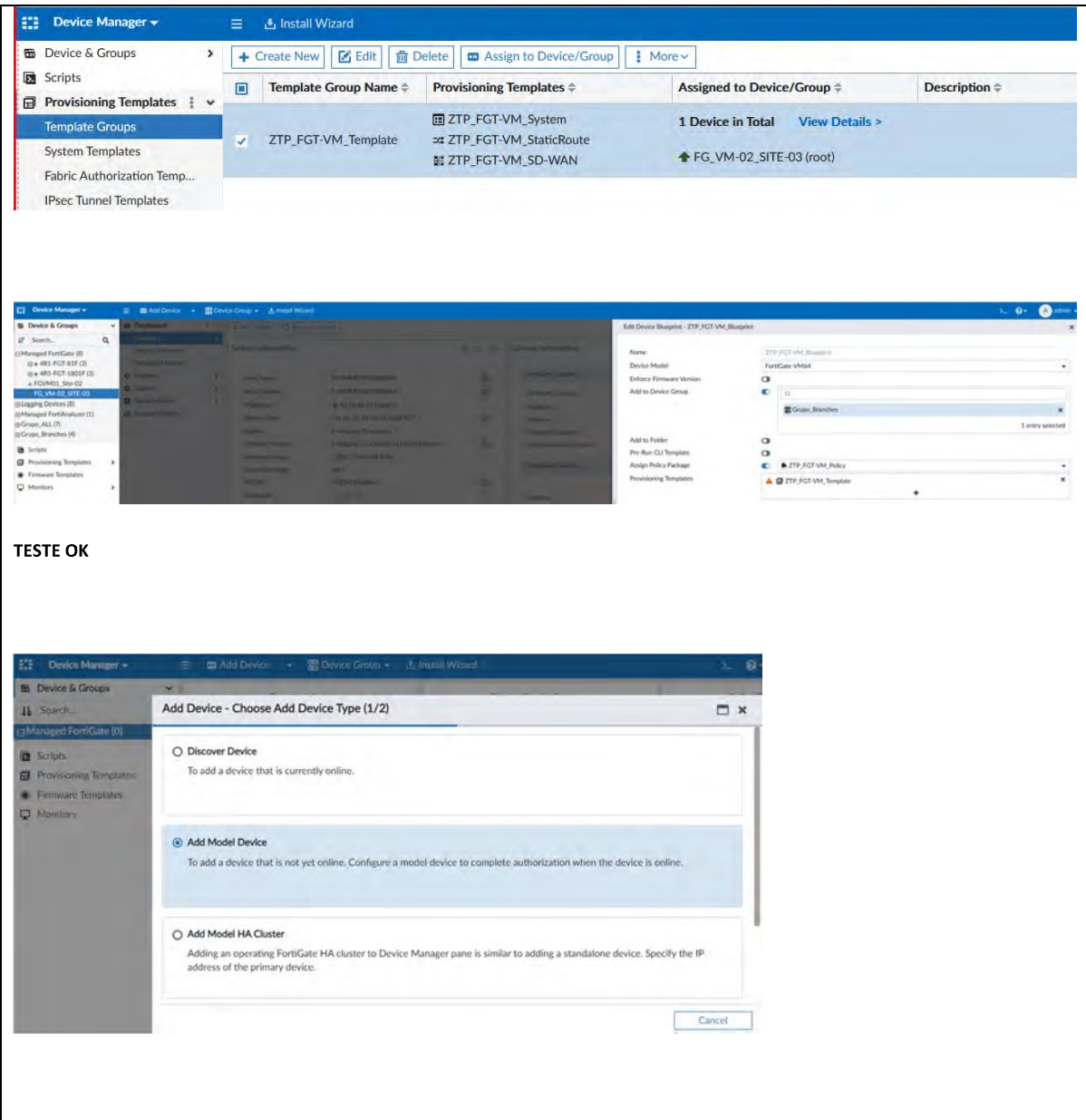


TESTE OK



	 <p>Add Device - Adding Model Device (2/2)</p> <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 <p style="text-align: right;">Finish</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #0056b3; color: white;"> <th>Layer</th> <th>Functions</th> <th colspan="2">Devices</th> </tr> </thead> <tbody> <tr> <td>Management and orchestration</td> <td> <ul style="list-style-type: none"> • Unified management • Template based solution • Zero touch provisioning • Logging, monitoring, and analysis • Automated orchestration using the REST API </td> <td style="text-align: center;">FortiManager </td> <td style="text-align: center;">FortiAnalyzer </td> </tr> </tbody> </table>	Layer	Functions	Devices		Management and orchestration	<ul style="list-style-type: none"> • Unified management • Template based solution • 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 • Zero touch provisioning • Logging, monitoring, and analysis • Automated orchestration using the REST API 	FortiManager 	FortiAnalyzer 						
<p>Comentário</p>	<p>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</p> <p>https://docs.fortinet.com/document/FortiGate/6.2.14/cookbook/861490/zero-touch-provisioning-with-fortimanager</p>								

<p>Item de Teste - 5.3.3.12</p>	<p>Gerenciamento centralizado e implantação Zero Touch;</p>																																													
<p>Objetivo do Teste</p>	<p>Mostrar que o equipamento de gerência centralizada com suporte a funcionalidade de implantação ZTP.</p>																																													
<p>Configuração do Teste</p>	<p>Mostrar que os dispositivos remotos suportam a funcionalidade ZTP.</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>																																													
<p>Evidências</p>	 <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>ID</th> <th>Source</th> <th>Description</th> <th>User</th> <th>Status</th> <th>Time Used</th> <th>ADOM</th> <th>Start Time</th> <th>End Time</th> </tr> </thead> <tbody> <tr> <td>154</td> <td>Install Configuration</td> <td>Push config to device</td> <td>admin</td> <td>Success: 1</td> <td>3m 17s</td> <td>root</td> <td>Tue Jul 25 2023 2:46:29 pm</td> <td>Tue Jul 25 2023 2:47:48 pm</td> </tr> <tr> <td>153</td> <td>Install Package</td> <td>Install Package 'ZTP_FCFvM_Policy'</td> <td>admin</td> <td>Success: 2</td> <td>2s</td> <td>root</td> <td>Tue Jul 25 2023 2:46:24 pm</td> <td>Tue Jul 25 2023 2:46:26 pm</td> </tr> <tr> <td>152</td> <td>Device Manager</td> <td>Auto-Add Device</td> <td>Admin</td> <td>Success: 1</td> <td>3m 26s</td> <td>root</td> <td>Tue Jul 25 2023 2:46:33 pm</td> <td>Tue Jul 25 2023 2:47:49 pm</td> </tr> <tr> <td>151</td> <td>Device Manager</td> <td>Add Device</td> <td>admin</td> <td>Success: 1</td> <td>~1s</td> <td>root</td> <td>Tue Jul 25 2023 2:45:08 pm</td> <td>Tue Jul 25 2023 2:45:08 pm</td> </tr> </tbody> </table>	ID	Source	Description	User	Status	Time Used	ADOM	Start Time	End Time	154	Install Configuration	Push config to device	admin	Success: 1	3m 17s	root	Tue Jul 25 2023 2:46:29 pm	Tue Jul 25 2023 2:47:48 pm	153	Install Package	Install Package 'ZTP_FCFvM_Policy'	admin	Success: 2	2s	root	Tue Jul 25 2023 2:46:24 pm	Tue Jul 25 2023 2:46:26 pm	152	Device Manager	Auto-Add Device	Admin	Success: 1	3m 26s	root	Tue Jul 25 2023 2:46:33 pm	Tue Jul 25 2023 2:47:49 pm	151	Device Manager	Add Device	admin	Success: 1	~1s	root	Tue Jul 25 2023 2:45:08 pm	Tue Jul 25 2023 2:45:08 pm
ID	Source	Description	User	Status	Time Used	ADOM	Start Time	End Time																																						
154	Install Configuration	Push config to device	admin	Success: 1	3m 17s	root	Tue Jul 25 2023 2:46:29 pm	Tue Jul 25 2023 2:47:48 pm																																						
153	Install Package	Install Package 'ZTP_FCFvM_Policy'	admin	Success: 2	2s	root	Tue Jul 25 2023 2:46:24 pm	Tue Jul 25 2023 2:46:26 pm																																						
152	Device Manager	Auto-Add Device	Admin	Success: 1	3m 26s	root	Tue Jul 25 2023 2:46:33 pm	Tue Jul 25 2023 2:47:49 pm																																						
151	Device Manager	Add Device	admin	Success: 1	~1s	root	Tue Jul 25 2023 2:45:08 pm	Tue Jul 25 2023 2:45:08 pm																																						



The screenshot displays the Fortinet Device Manager interface. The top navigation bar includes 'Device Manager' and 'Install Wizard'. A sidebar on the left lists 'Device & Groups', 'Scripts', 'Provisioning Templates', 'Template Groups', 'System Templates', 'Fabric Authorization Temp...', and 'IPsec Tunnel Templates'. The main area shows a table of provisioning templates:

Template Group Name	Provisioning Templates	Assigned to Device/Group	Description
<input checked="" type="checkbox"/> ZTP_FGT-VM_Template	<ul style="list-style-type: none"> ZTP_FGT-VM_System ZTP_FGT-VM_StaticRoute ZTP_FGT-VM_SD-WAN 	1 Device in Total View Details >	FG_VM-02_SITE-03 (root)

Below the table, there are two smaller screenshots. The first shows the 'Add Device' wizard with the 'Add Model Device' option selected. The second shows the 'Edit Device Blueprint' for 'ZTP_FGT-VM_Blueprint', with fields for Name, Device Model (FortiGate-VM64), and various configuration options like 'Add to Folder', 'Per-Run CLI Template', 'Assign Policy Package', and 'Provisioning Templates'.

TESTE OK

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:

Add Device - Adding Model Device (2/2)

Name: FortiGate-CademoTestes

Status: ✔ Device is added successfully

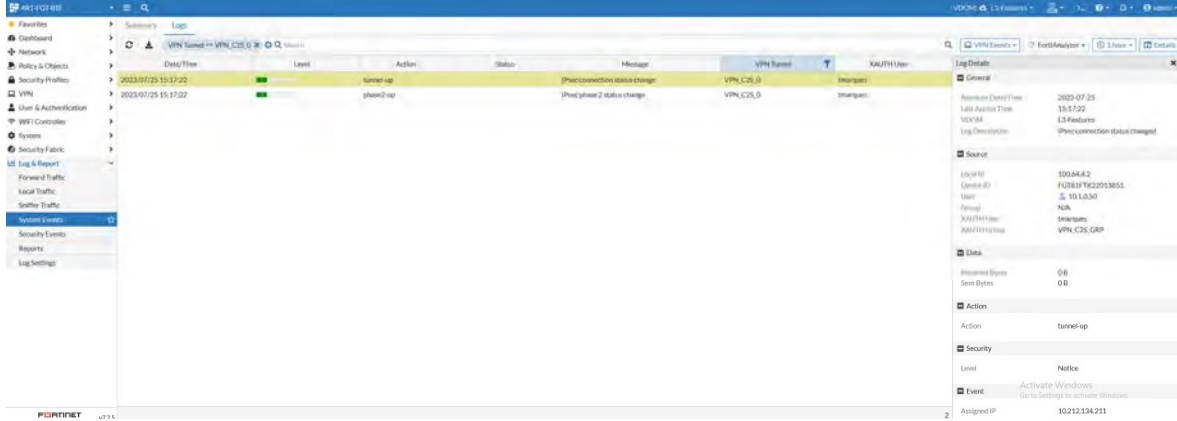
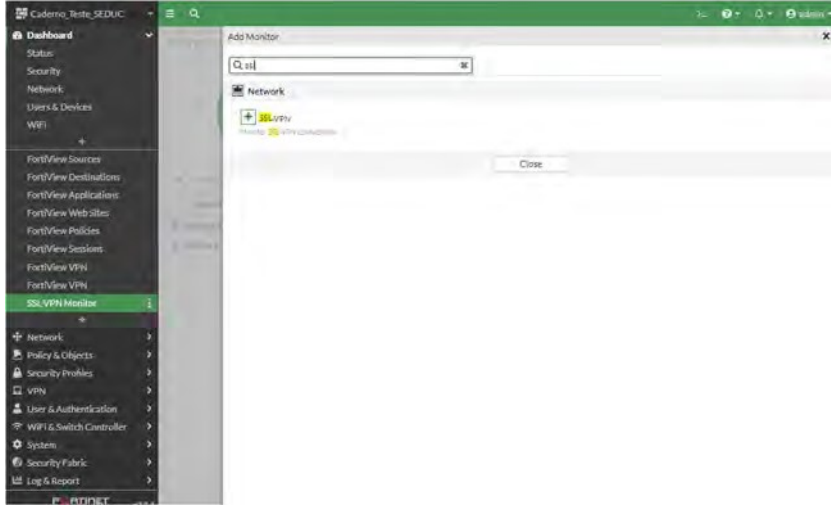
- ✔ Creating device database
- ✔ Retrieving high availability status
- ✔ Initializing configuration database
- ✔ Updating group membership
- ✔ Successfully add device

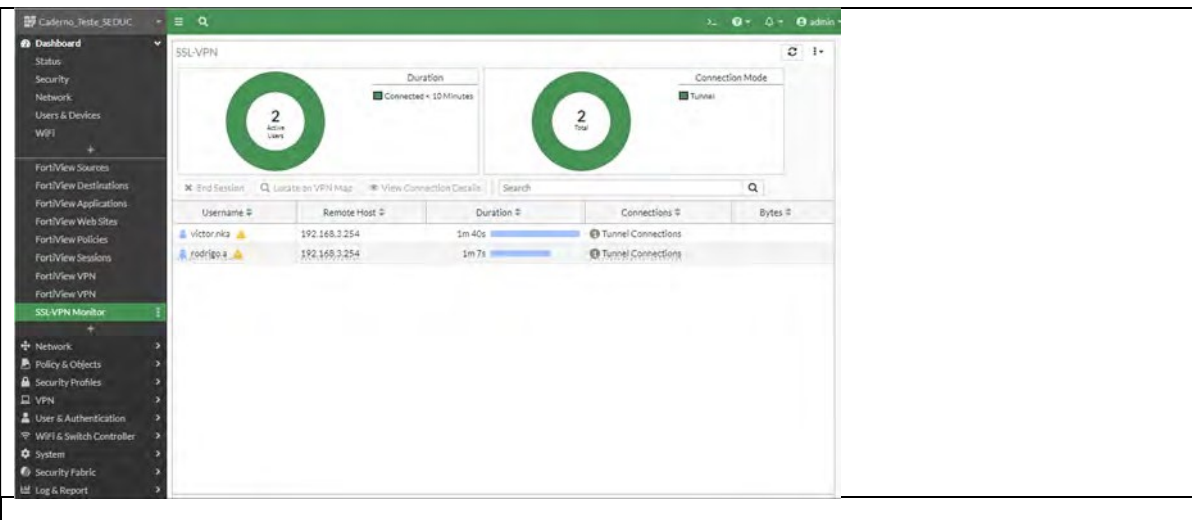
Layer	Functions	Devices	
Management and orchestration	<ul style="list-style-type: none"> • Unified management • Template based solution • Zero touch provisioning • Logging, monitoring, and analysis • Automated orchestration using the REST API 	FortiManager 	FortiAnalyzer 

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

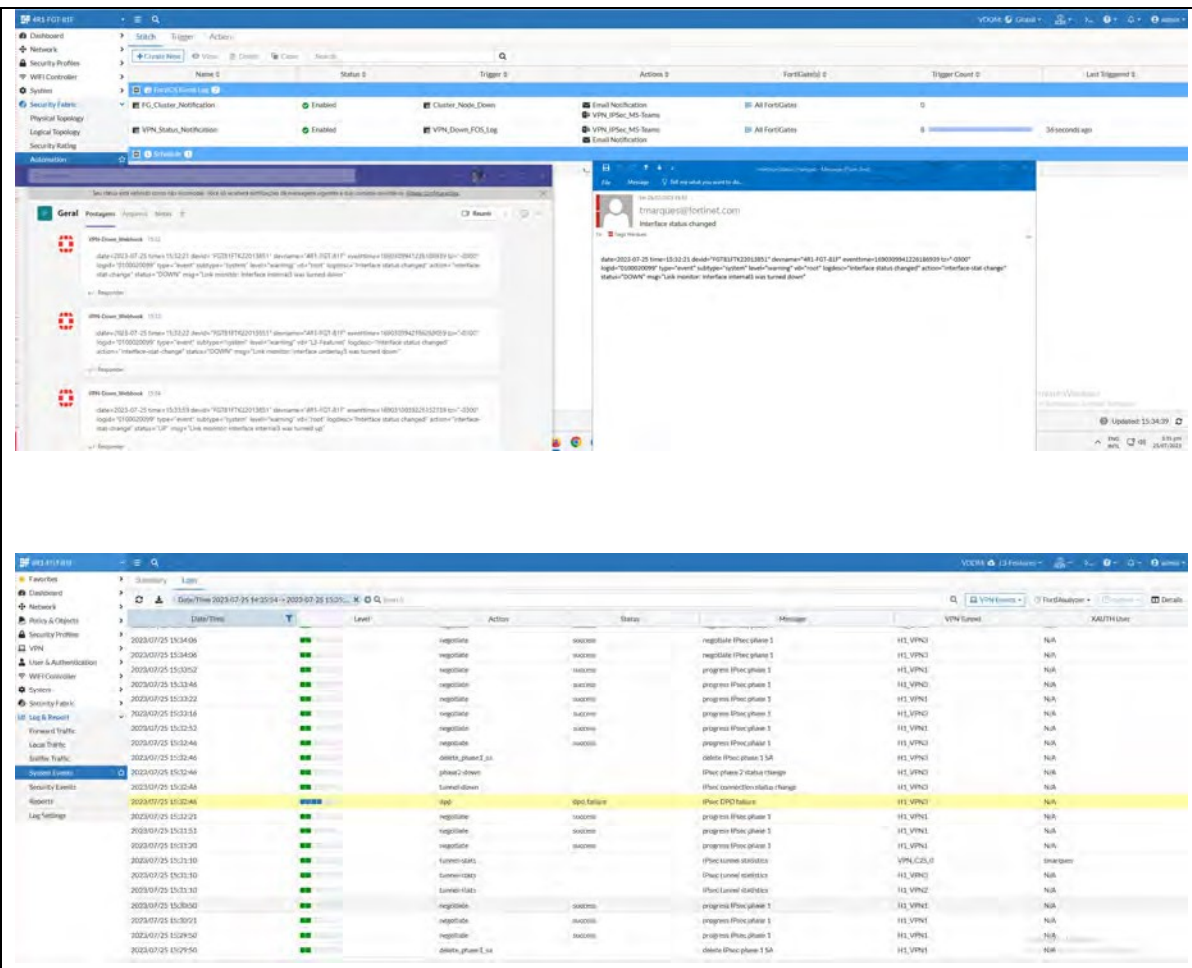
5.3.4 ACESSO REMOTO - VPN:

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.
Evidências	 <p>TESTE OK</p> 

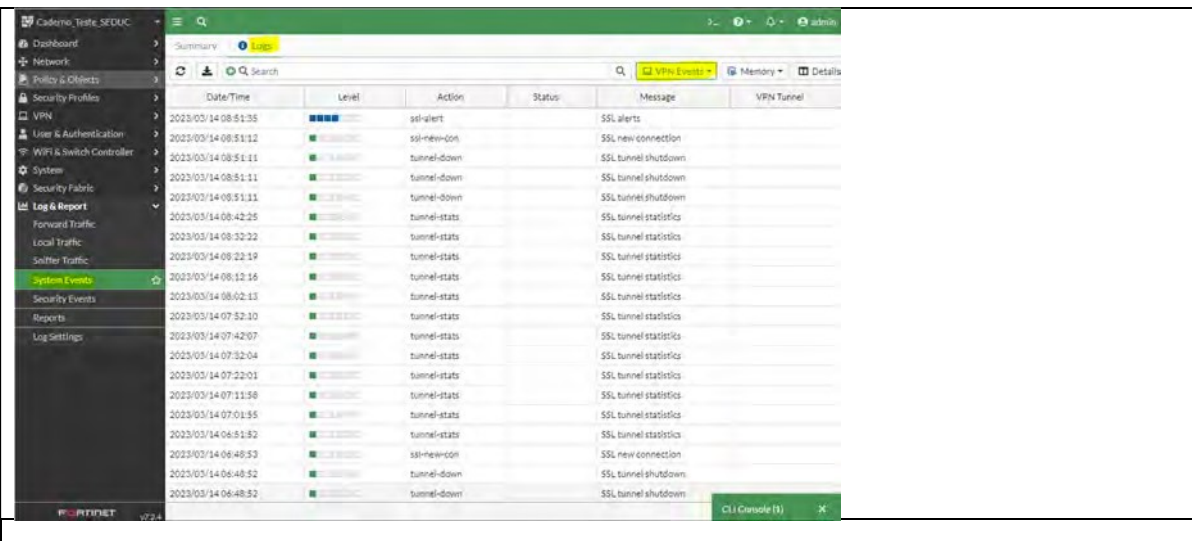
<p>Comentário</p>	 <p>The screenshot shows the FortiGate SSL-VPN Monitor interface. It features two circular gauges: one for 'Active Users' showing '2' and another for 'Tunnels' showing '2'. Below these are two summary cards: 'Duration' with 'Connected + 10 Minutes' and 'Connection Mode' with 'Tunnel'. A table below lists active sessions with columns for Username, Remote Host, Duration, Connections, and Bytes. The table contains two entries: 'victor.nka' connected to '192.168.3.254' for 1m 40s, and 'rodrigo.a' connected to '192.168.3.254' for 1m 7s. The left sidebar shows the navigation menu with 'SSL-VPN Monitor' selected.</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> <ul style="list-style-type: none"> - To. - Email subject. - Email body. <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>	

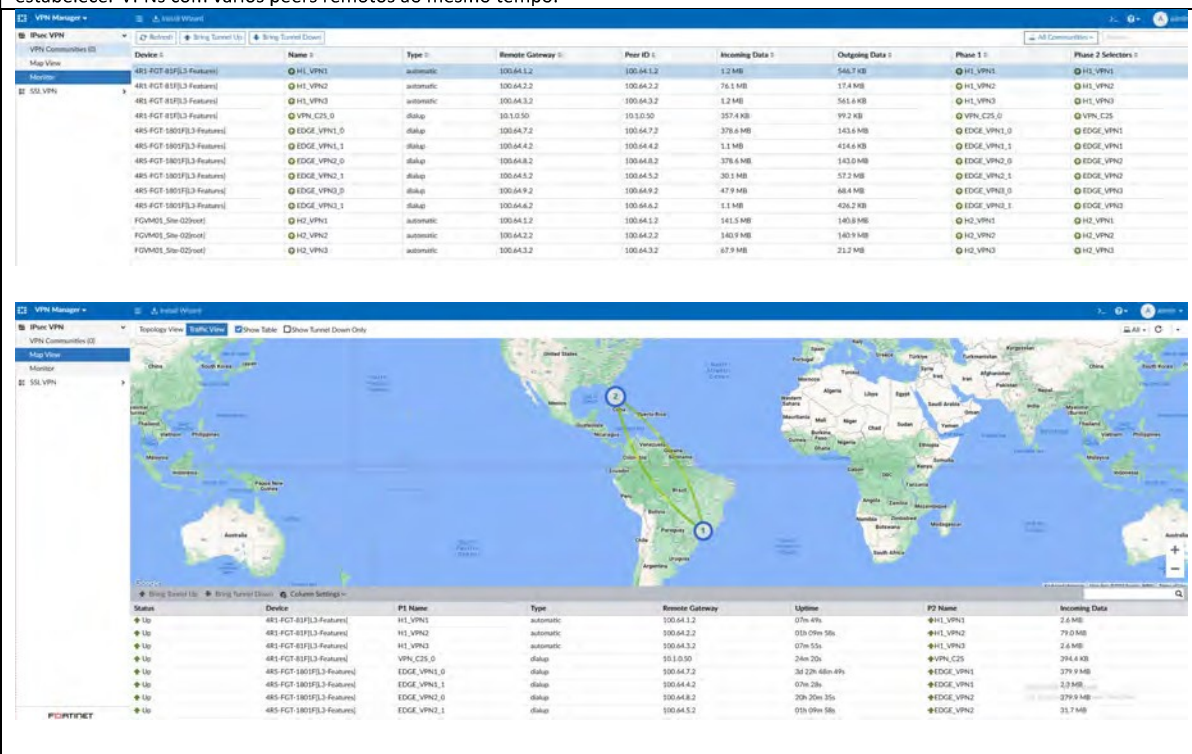


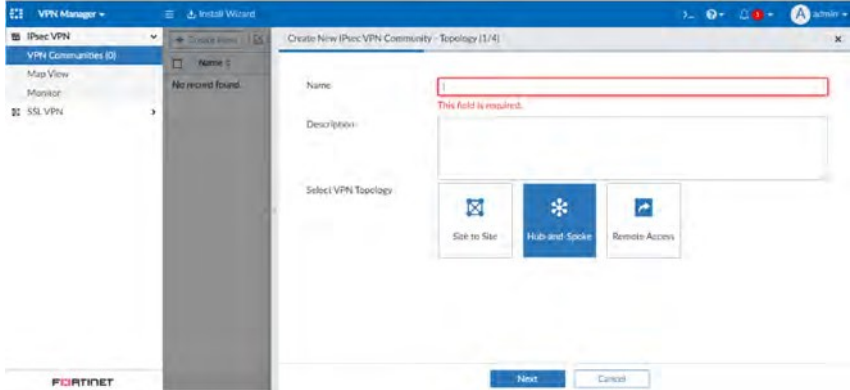
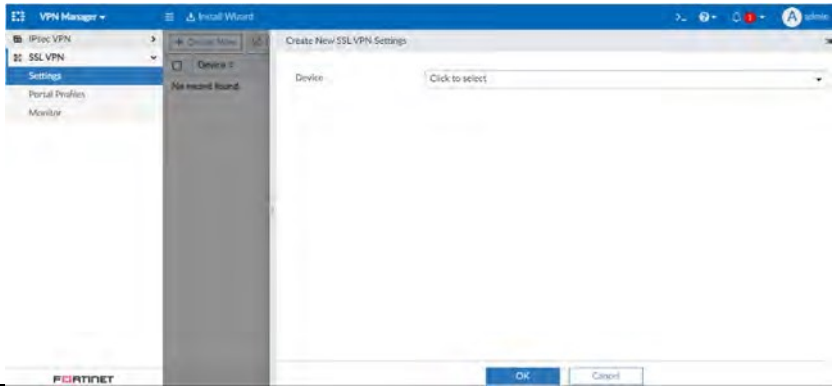
TESTE OK

Date/Time	Level	Action	Status	Message	VPN Tunnel	XAUTH User
2023-07-25 15:34:06	INFO	negotiate	success	negotiate IPsec phase 1	H1_VPN2	N/A
2023-07-25 15:34:06	INFO	negotiate	success	negotiate IPsec phase 1	H1_VPN1	N/A
2023-07-25 15:33:52	INFO	negotiate	success	program IPsec phase 1	H1_VPN1	N/A
2023-07-25 15:33:46	INFO	negotiate	success	program IPsec phase 1	H1_VPN1	N/A
2023-07-25 15:33:32	INFO	negotiate	success	program IPsec phase 1	H1_VPN1	N/A
2023-07-25 15:33:16	INFO	negotiate	success	program IPsec phase 1	H1_VPN1	N/A
2023-07-25 15:32:52	INFO	negotiate	success	program IPsec phase 1	H1_VPN1	N/A
2023-07-25 15:32:46	INFO	negotiate	success	program IPsec phase 1	H1_VPN1	N/A
2023-07-25 15:32:46	INFO	delete IPsec phase 1 SA	success	delete IPsec phase 1 SA	H1_VPN1	N/A
2023-07-25 15:32:44	INFO	phase1-down	success	IPsec phase 1 status change	H1_VPN1	N/A
2023-07-25 15:32:44	INFO	turnoff-down	success	IPsec tunnel ID/status change	H1_VPN1	N/A
2023-07-25 15:32:44	INFO	api	Spcl failure	IPsec CPD failure	H1_VPN1	N/A
2023-07-25 15:32:25	INFO	negotiate	success	program IPsec phase 1	H1_VPN1	N/A
2023-07-25 15:32:13	INFO	negotiate	success	program IPsec phase 1	H1_VPN1	N/A
2023-07-25 15:31:26	INFO	negotiate	success	program IPsec phase 1	H1_VPN1	N/A
2023-07-25 15:31:10	INFO	turnoff-up	success	IPsec tunnel statistics	VPN_C25,0	Imargem
2023-07-25 15:31:10	INFO	turnoff-up	success	IPsec tunnel statistics	H1_VPN2	N/A
2023-07-25 15:30:00	INFO	negotiate	success	program IPsec phase 1	H1_VPN1	N/A
2023-07-25 15:29:53	INFO	negotiate	success	program IPsec phase 1	H1_VPN1	N/A
2023-07-25 15:29:50	INFO	negotiate	success	program IPsec phase 1	H1_VPN1	N/A
2023-07-25 15:29:50	INFO	delete IPsec phase 1 SA	success	delete IPsec phase 1 SA	H1_VPN1	N/A

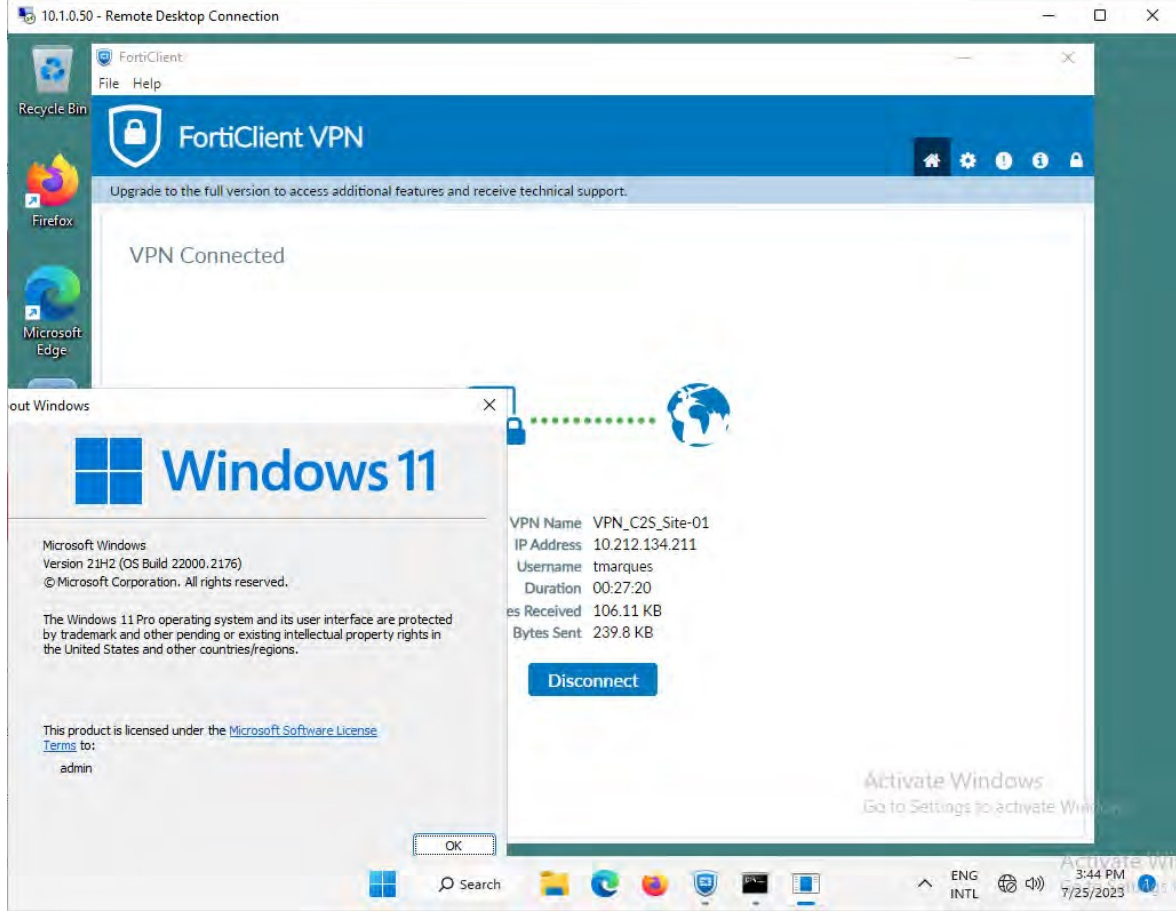
<p>Comentário</p>	
--------------------------	--

<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>	
--------------------------	--

	<p>TESTE OK</p>  
Comentário	https://docs.fortinet.com/document/fortimanager/7.2.3/administration-guide/9083

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	`



The screenshot shows a remote desktop session titled "10.1.0.50 - Remote Desktop Connection". The main window is the FortiClient VPN interface, which displays "VPN Connected". A "Disconnect" button is visible. A Windows 11 activation dialog box is overlaid on the VPN window, showing the Windows logo and the text "Windows 11". The dialog box includes the following information:

- Microsoft Windows
- Version 21H2 (OS Build 22000.2176)
- © Microsoft Corporation. All rights reserved.
- The Windows 11 Pro operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.
- This product is licensed under the [Microsoft Software License Terms](#) to: admin

Additional details from the VPN interface:

- VPN Name: VPN_C2S_Site-01
- IP Address: 10.212.134.211
- Username: tmarques
- Duration: 00:27:20
- Bytes Received: 106.11 KB
- Bytes Sent: 239.8 KB

The taskbar at the bottom of the remote desktop shows the Start button, Search, File Explorer, Microsoft Edge, Firefox, and Recycle Bin. The system tray includes the language indicator (ENG INTL), network and volume icons, and the system clock showing 3:44 PM on 7/25/2023.

TESTE OK

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

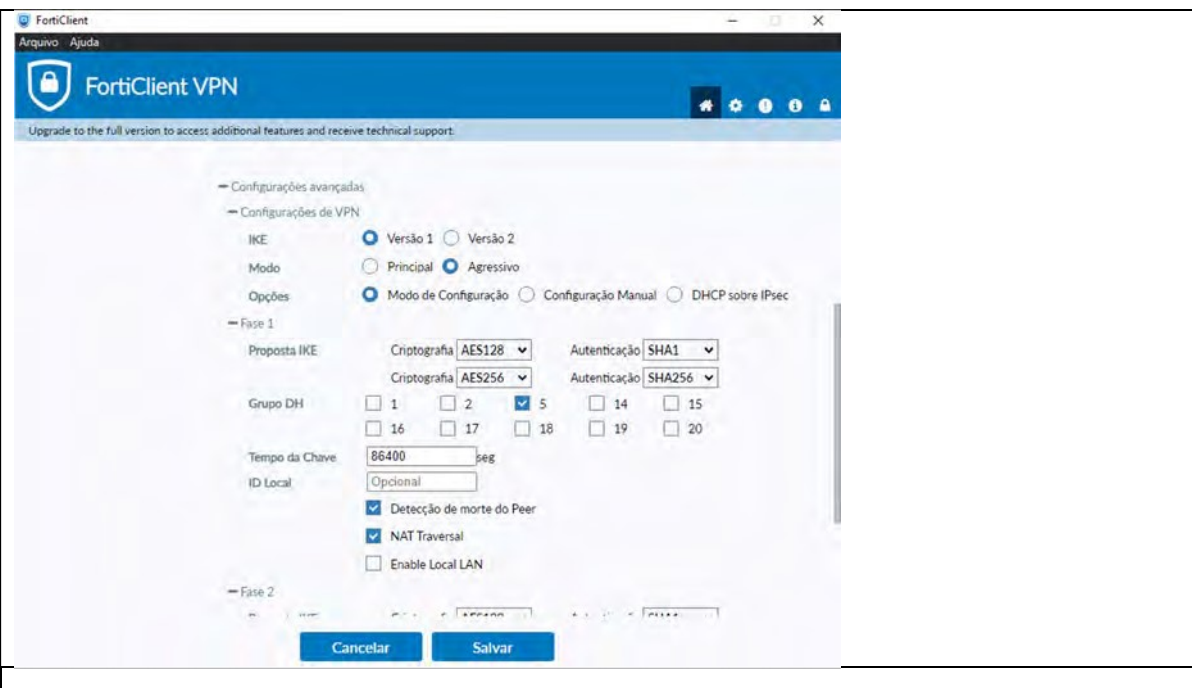
- ✓ SSL VPN with MFA
- ✓ IPSEC VPN with MFA

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

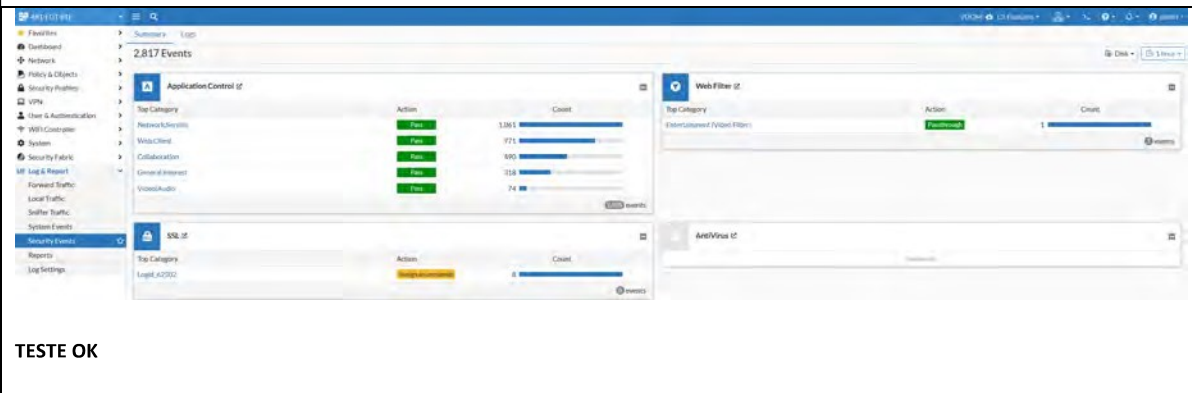
The screenshot shows the FortiClient VPN configuration window. The title bar reads "FortiClient" and "Arquivo Ajuda". The main header is "FortiClient VPN" with a notification: "Upgrade to the full version to access additional features and receive technical support." The main content area is titled "Nova conexão VPN" and contains the following fields and options:

- VPN: Radio buttons for SSL VPN, VPN IPsec (selected), and SSL.
- Nome da Conexão: Text input field.
- Descrição: Text input field.
- Gateway Remoto: Text input field with a search icon.
- Método de Autenticação: Dropdown menu set to "Chave Pré-Compartilhada".
- Autenticação (XAuth): Radio buttons for "Prompt no login" (selected), "Salvar login", and "Desabilitado".
- Fallover SSL VPN: Dropdown menu set to "[Nenhum]".
- Configurações avançadas (expanded):
 - Configurações de VPN:
 - IKE: Radio buttons for "Versão 1" and "Versão 2" (selected).
 - Modo: Radio buttons for "Principal" and "Agressivo" (selected).
 - Opções: Radio buttons for "Modo de Configuração" (selected), "Configuração Manual", and "DHCP sobre IPsec".
 - Fase 1: (collapsed)

At the bottom, there are "Cancelar" and "Salvar" buttons.

<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>
<p>Objetivo do Teste</p>	<p>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.</p>
<p>Configuração do Teste</p>	<p>Configuração de regra de segurança NGFW com filtro de aplicação e URL.</p>
<p>Procedimento do Teste</p>	<p>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.</p>
<p>Evidências</p>	 <p>TESTE OK</p>

New Policy

Name

Incoming Interface

Outgoing Interface

Source

Destination

Schedule always

Service

Action ACCEPT DENY

Firewall/Network Options

NAT

IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port

Protocol Options

Security Profiles

AntiVirus AV default

Web Filter WEB default

DNS Filter DNS default

Application Control APP default

IPS IPS default

File Filter

SSL Inspection SSL certificate-inspection

Static URL Filter

Block invalid URLs

URL Filter

URL	Type	Action	Status
www.youtube.c...	Wildcard	<input checked="" type="checkbox"/> Block	<input checked="" type="checkbox"/> 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

<p>Procedimento do Teste</p>	<p>Criar regra contendo filtro de aplicação de camada 7.</p>
<p>Evidências</p>	<p>Application control</p> <p>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).</p> <p>TESTE OK</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”

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).



ActMobile.VPN

ID **43286**

Summary **This indicates an attempt to use ActMobile VPN service.**

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.

Category **Proxy**

Risk **■■■■■**

Popularity **★☆☆☆☆**

Protocol **TCP, SSL, UDP, DNS**

Technology **Client-Server**

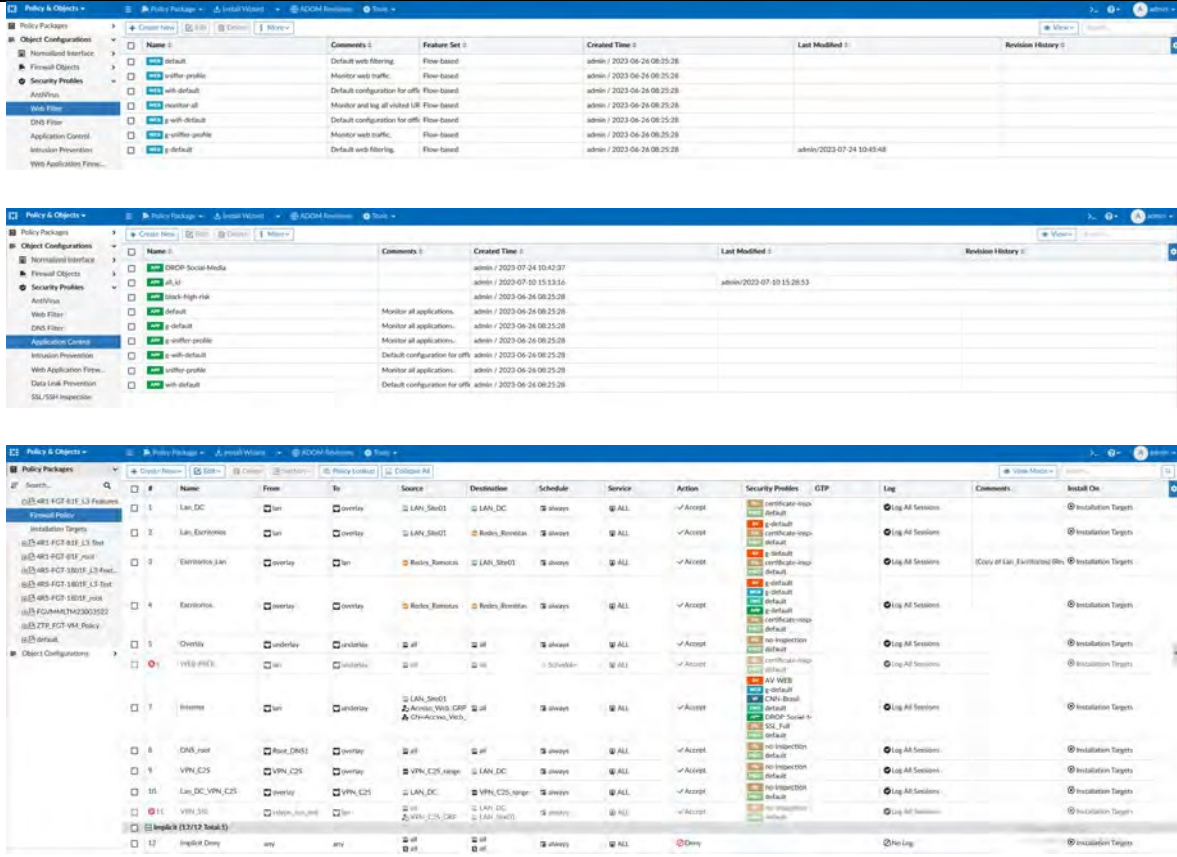
Behavior **Tunneling**

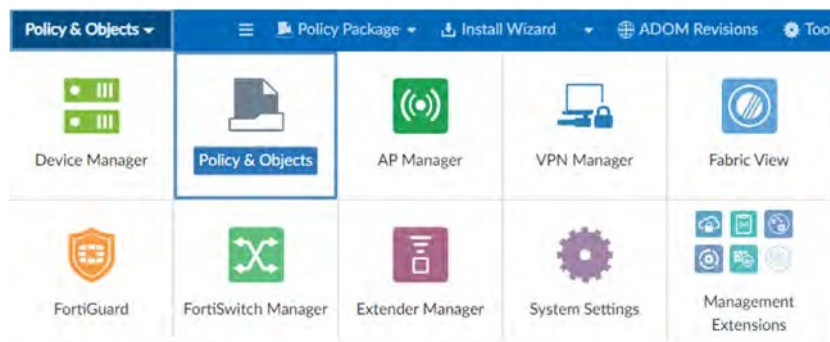
Vendor **Other**

Comentário

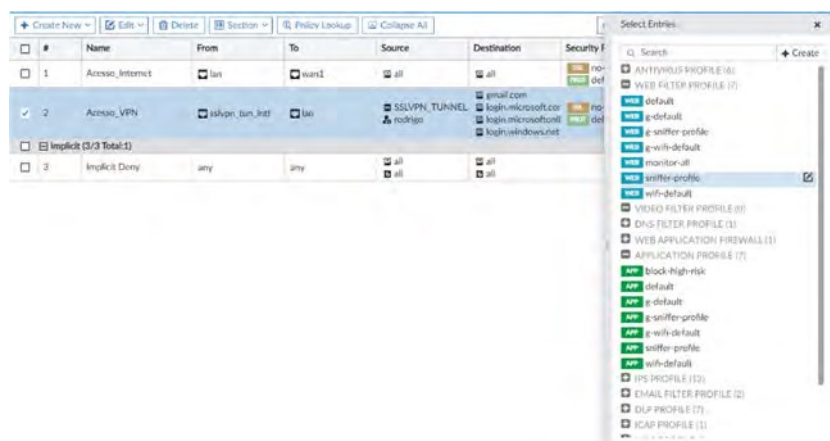
Fonte: FortiOS-7.2.3Administration_Guide acessado em

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

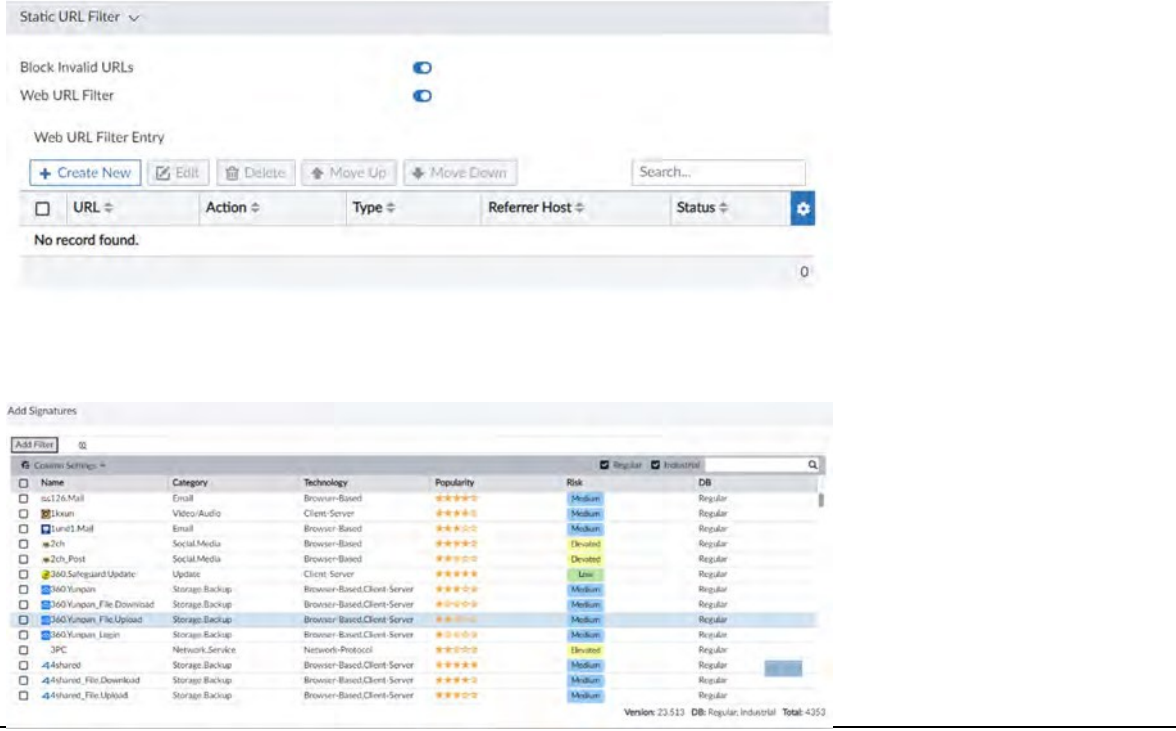
<p>Item de Teste - 5.3.5.3</p>	<p>A gestão das políticas de segurança de controle de aplicação e controle de URL's deverá ser centralizada na mesma console de gerenciamento;</p>
<p>Objetivo do Teste</p>	<p>Verificar se o equipamento possui a funcionalidade de gerenciar as políticas de segurança de controle de aplicação e controle de URL's de forma centralizada.</p>
<p>Configuração do Teste</p>	<p>Utilizar um FortiGate com os serviços de Fabric connector enable, linkado a um FortiManager que realiza a gerência centralizada.</p>
<p>Procedimento do Teste</p>	<p>Criação de uma política que possui controle de aplicação e um controle de URL's.</p> <p>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.</p> <p>Assim, basta selecionar a regra desejada e aplicar um perfil de segurança.</p> <p>Dentro desses "Security Profiles" temos as opções de WebFilter Profile (controle de URL'S) e o Application Control (Controle de Aplicação).</p>
<p>Evidências</p>	 <p>The first screenshot shows the 'Policy & Objects' configuration page with 'Security Profiles' selected. It lists various profiles like 'default', 'web-filter-profile', 'monitor-all', etc., with their respective comments and feature sets.</p> <p>The second screenshot shows the 'Application Control' configuration page, where a profile is being configured to monitor all applications.</p> <p>The third screenshot shows a detailed view of a policy package configuration, including source/destination, schedule, service, action, and security profiles.</p> <p>TESTE OK</p>




#	Name	From	To	Source	Destination	Security Profile	Schedule	Service
1	Acesso_Internet	lan	wan1	all	all	no-inspection default	always	All
2	Acesso_VPN	skype_san_int	lan	SSLVPN_TUNNEL	logon.microsoft.com, logon.microsoft.com, logon.microsoft.com, logon.microsoft.com	no-inspection default	always	All
3	Implicit_Deny	any	any	all	all		always	All

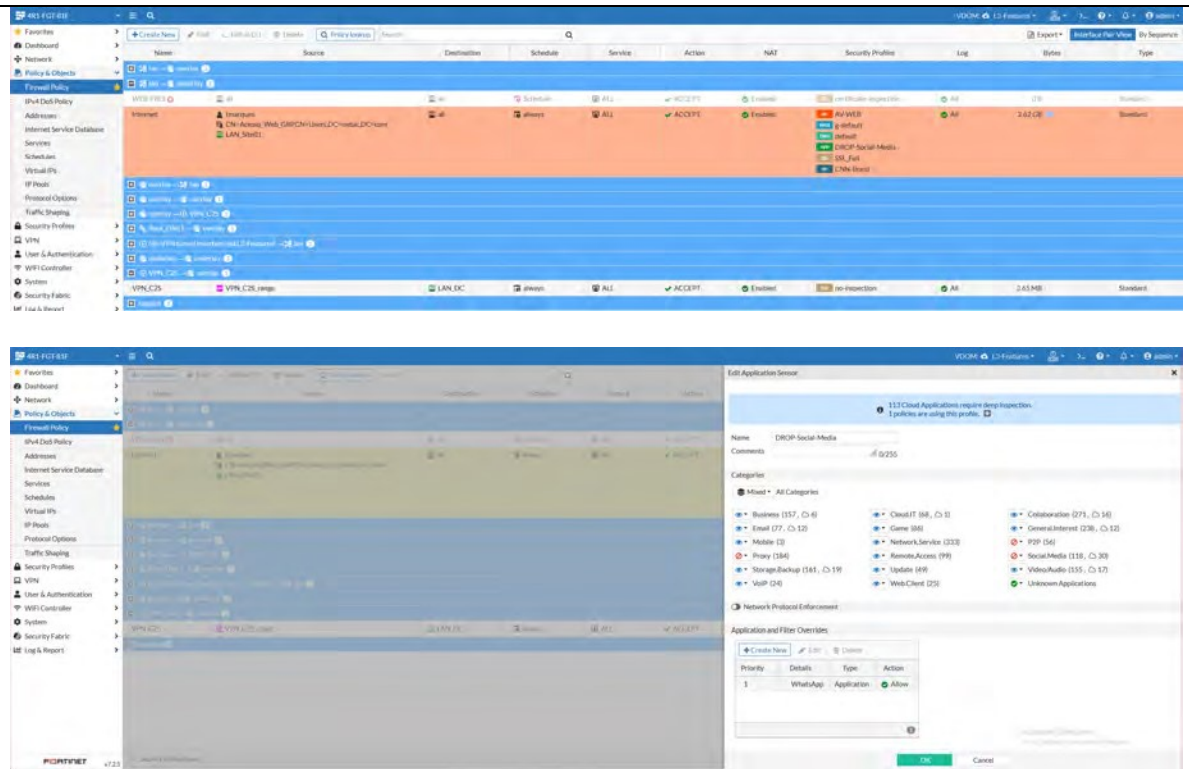


#	Name	From	To	Source	Destination	Security F
1	Acesso_Internet	lan	wan1	all	all	no-inspection default
2	Acesso_VPN	skype_san_int	lan	SSLVPN_TUNNEL	logon.microsoft.com, logon.microsoft.com, logon.microsoft.com, logon.microsoft.com	no-inspection default
3	Implicit_Deny	any	any	all	all	

<p>Comentário</p>	 <p>The screenshot shows the Cisco ASA configuration interface. At the top, there are sections for 'Static URL Filter', 'Block Invalid URLs', and 'Web URL Filter'. Below these is a table for 'Web URL Filter Entry' with columns for 'URL', 'Action', 'Type', 'Referrer Host', and 'Status'. A message 'No record found.' is displayed. Below that is the 'Add Signatures' section, which contains a table of signatures with columns for 'Name', 'Category', 'Technology', 'Popularity', 'Risk', and 'DB'. The table lists various signatures like 'isc126.Mail', '1kxan', 'Lure1.Mail', etc., with their respective risk levels (Medium, Devoted, Low) and database types (Regular, Industrial).</p>
--------------------------	---

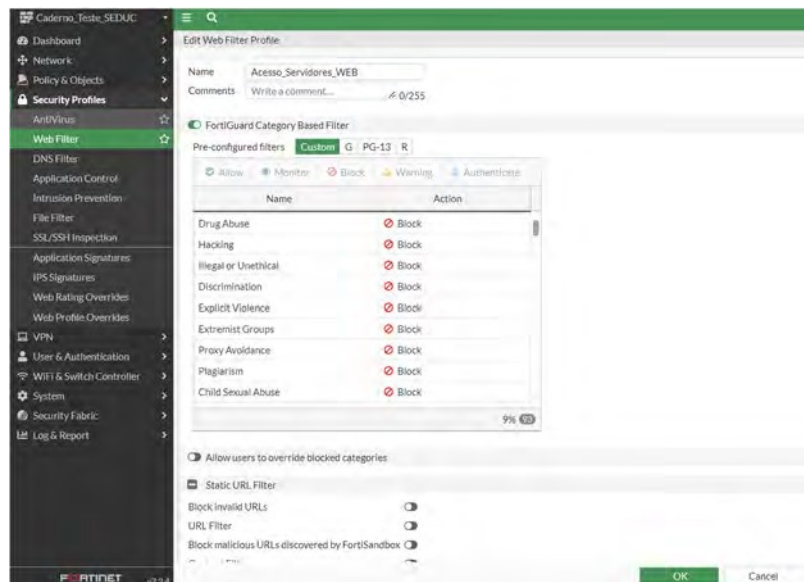
<p>Item de Teste - 5.3.5.5</p>	<p>Possuir controle de regras de aplicações, grupos de aplicações, categorias de aplicações com controle granular para usuários ou grupos de usuários;</p>
<p>Objetivo do Teste</p>	<p>Validar se a solução possui ferramentas de controle de regras de aplicações, grupos de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

Evidências

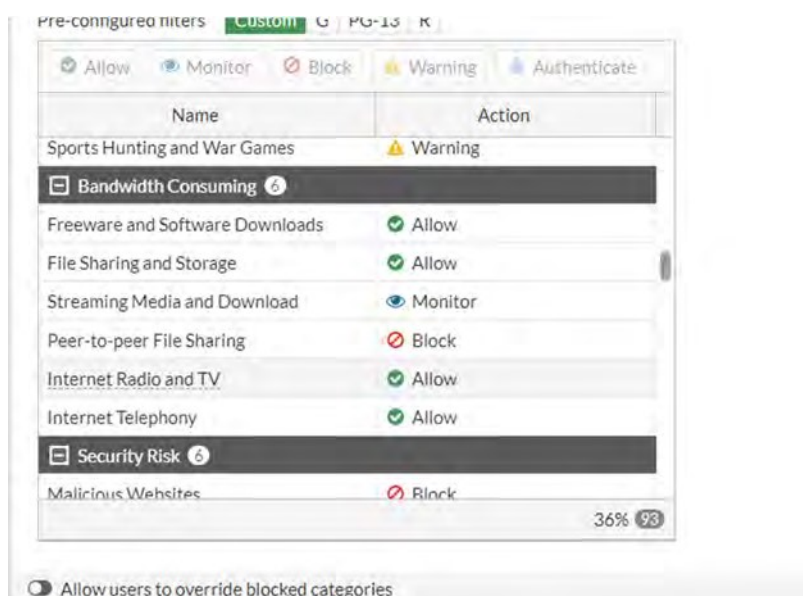


TESTE OK

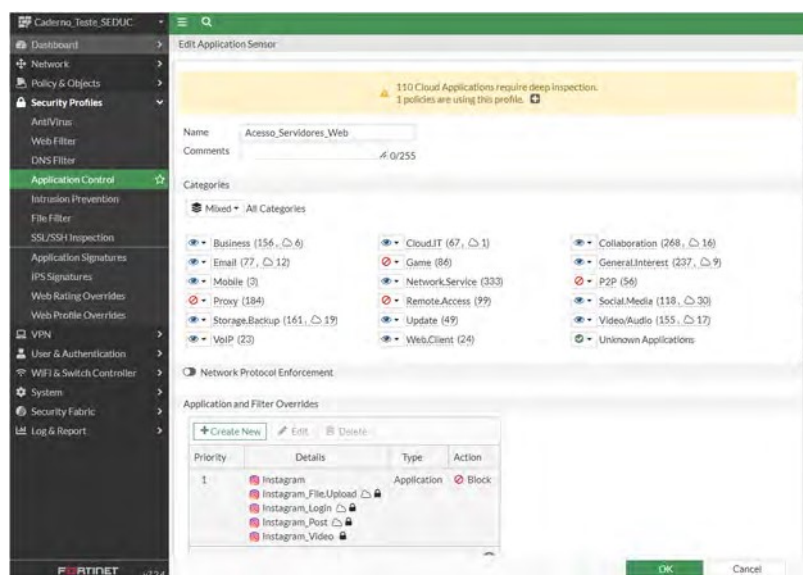
1 – Criando Web Filter.



2 - Selecionando categorias.



3 – Criando Application Control.



3 – Definindo grupos e usuários.

Edit Policy

Name i

Incoming Interface

Outgoing Interface

Source

Destination

Schedule

Service

Action ACCEPT DENY

4 – Definindo Profiles WEB e de Aplicação para política.

Security Profiles

AntiVirus AV

Web Filter WEB

DNS Filter

Application Control APP

IPS

File Filter

SSL Inspection SSL

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	

The image displays two screenshots of the Fortinet FortiGate web interface. The top screenshot shows the Firewall Policy configuration page. A table lists several policies, with the 'Internet' policy selected. The table columns include Name, Source, Destination, Schedule, Service, Action, NAT, Security Profiles, Log, Bytes, and Type. The 'Internet' policy is configured for Internet Service Database, with services including HTTP, HTTPS, and others. The bottom screenshot shows the SSL Inspection Profile configuration page for 'SSL_Full'. The 'Enable SSL Inspection of' section is set to 'Protecting SSL Server'. The 'Inspection method' is 'Full SSL Inspection'. The 'CA certificate' is set to 'Fortinet CA SSL'. The 'Blocked certificates' and 'Untrusted SSL certificates' sections are set to 'Allow'. The 'Server certificate SNI check' is set to 'Enforce'. The 'Enforce SSL regulation compliance' and 'SIP over HTTPS' options are also visible. The 'Protocol Port Mapping' section shows ports for HTTP, HTTPS, SIPS, IMAPS, and FTPS. The 'Exempt from SSL Inspection' section is set to 'Respectable websites'. The 'Web categories' section is set to 'Finance and Banking, Health and Wellness'.

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

10.1.0.50 - Remote Desktop Connection

UOL - Seu universo online

UOL - Seu universo online

https://www.uol.com.br

INGRESSO.COM BATE-PAPO

Connection security for www.uol.com.br

You are securely connected to this site.

Verified by: Fortinet

Mozilla does not recognize this certificate issuer. It may have been added from your operating system or by an administrator. [Learn more](#)

SAC EMAIL ENTRE ASSINE UOL

PagBank O BANCO COMPLETO

São Paulo 26°C 15°C

Dólar ↑ 4,75 Euro ↑ 5,249

PRODUTOS NOTÍCIAS CARRÃO

More information

VABEM TILT ECOA CANAL UOL MOV NOSSA TAB UOL PRIME

PUBLICIDADE

VIEW

1. Click "View"
2. Install Firefox Extension
3. Enjoy EasyView!

EasyView

José Paulo Kupfer
Cresce aposta em corte de meio ponto na Selic

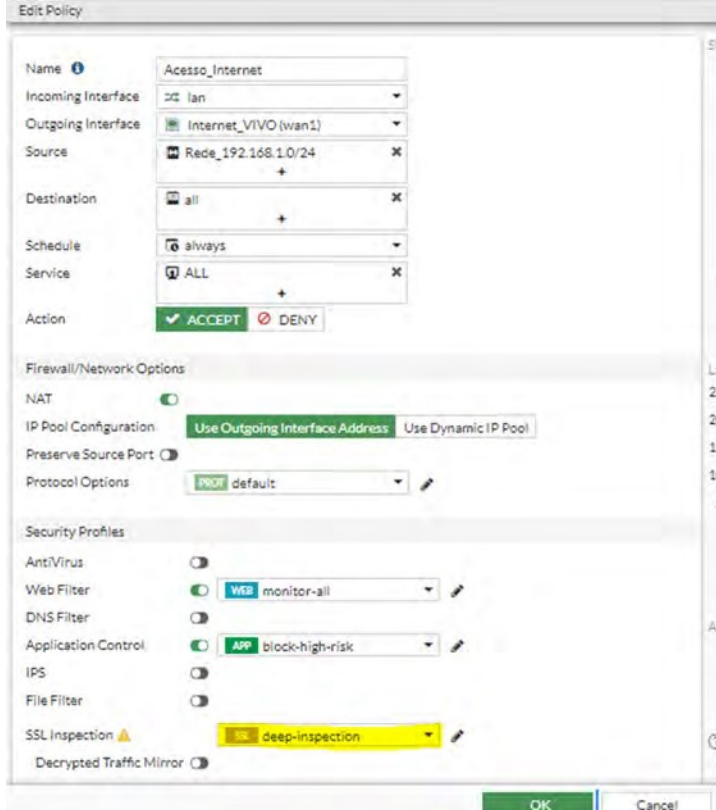
André Santana
Por que ler escritoras da América Latina e do Caribe

Maria Ribeiro
Talvez desaponte alguns: me emocionei com 'Barbie'

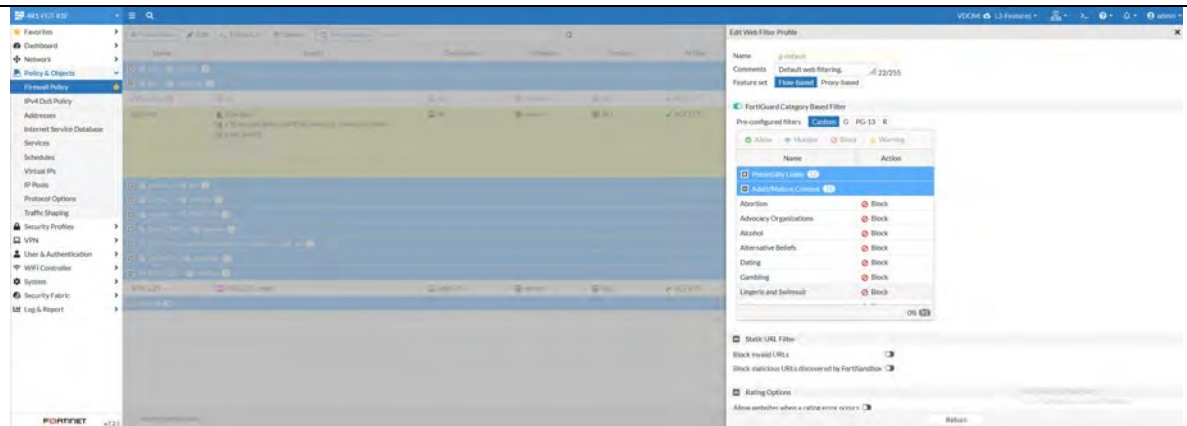
Mari Rodrigues
Barbie médica com atriz trans é recado forte

ENG INTL 4:18 PM 7/25/2023

TESTE OK

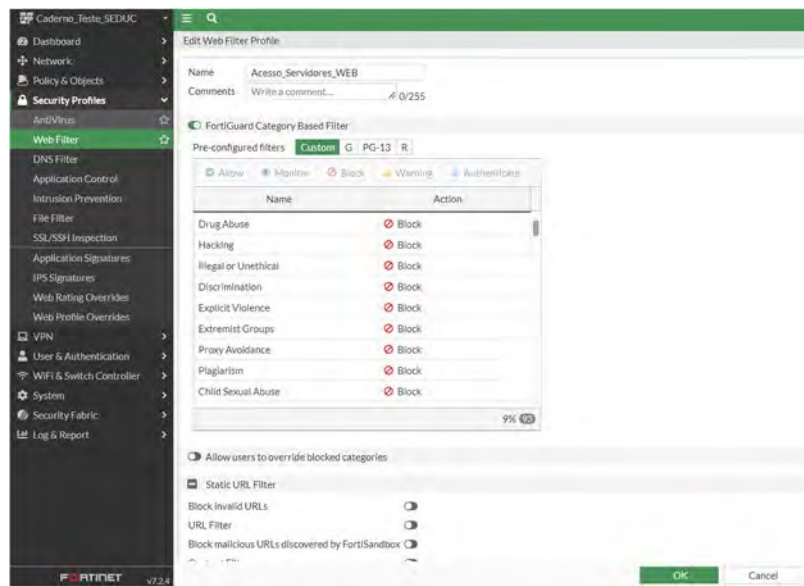
<p>Comentário</p>	
--------------------------	--

<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>	

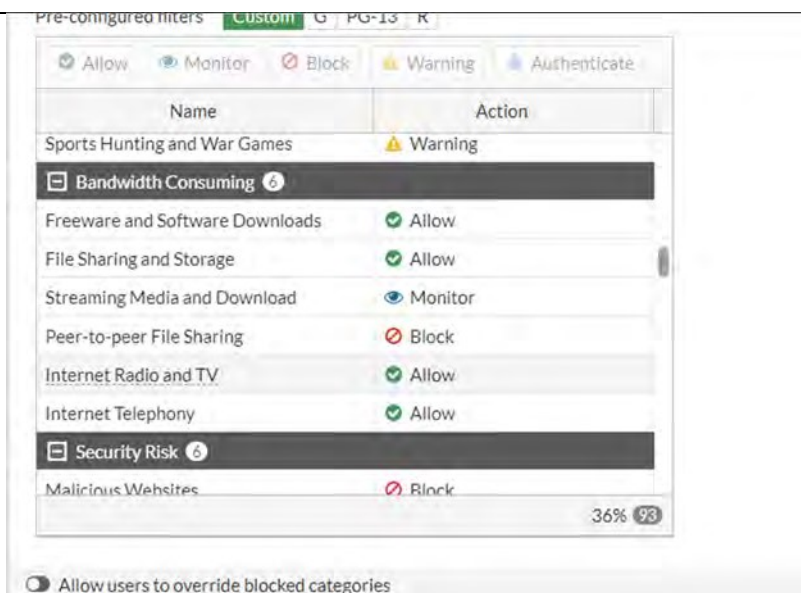


TESTE OK

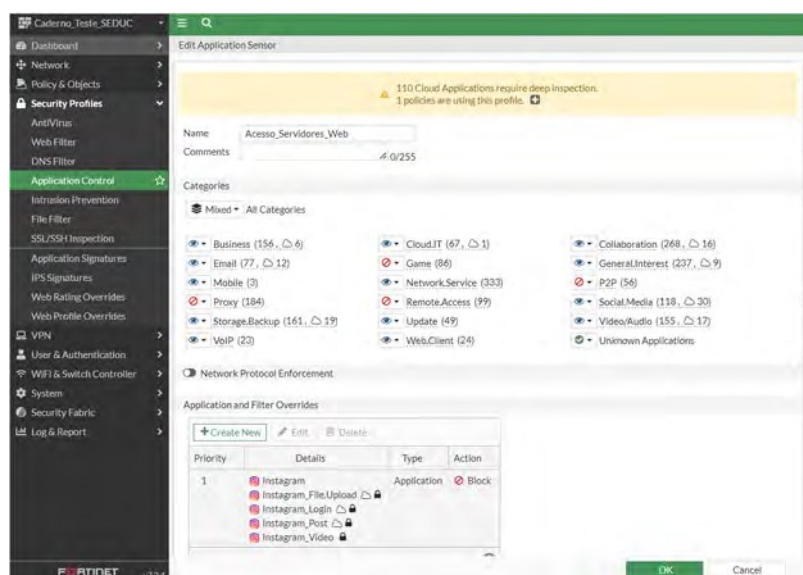
1 – Criando Web Filter.



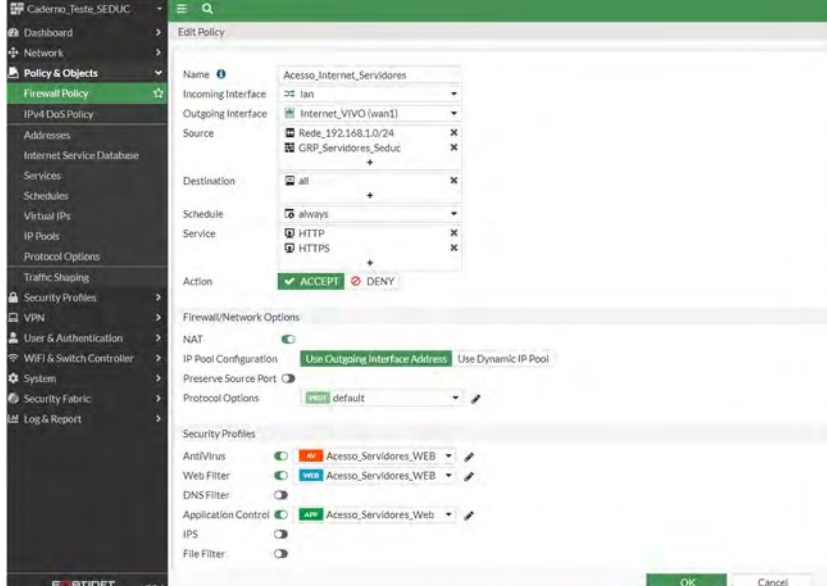
2 - Selecionando categorias.



3 – Criando Application Control.

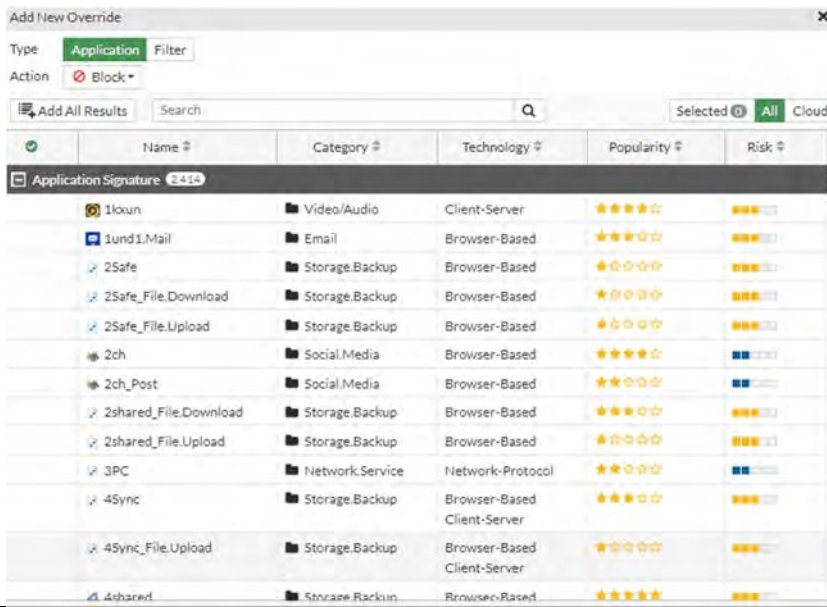


4 – Adicionando perfis de segurança em políticas.

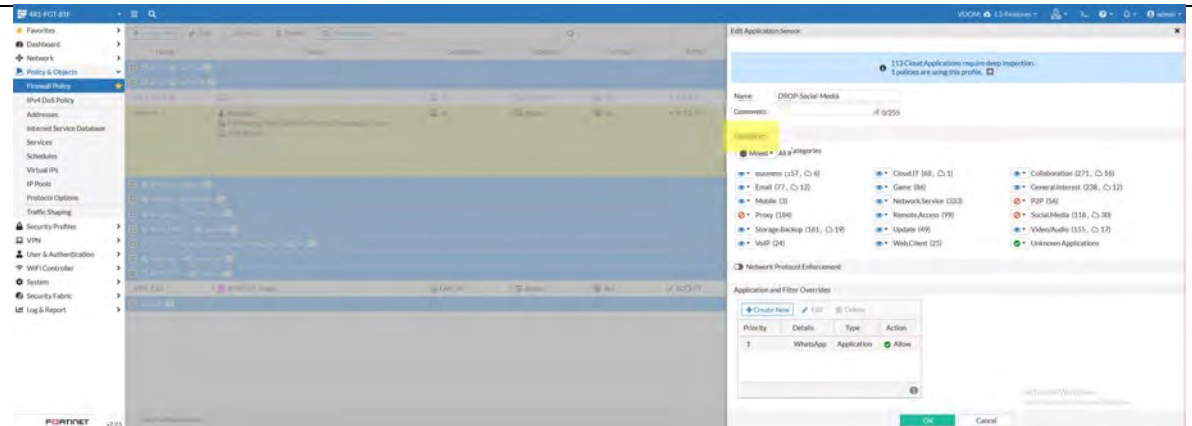
		
<p>Comentário</p>	<p>https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/615462/url-filter</p> <p>https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/019814/basic-category-filters-and-overrides</p>	

5.3.5.9 Deve possibilitar a permissão ou bloqueio de aplicações ou URLs por pelo menos os seguintes critérios:

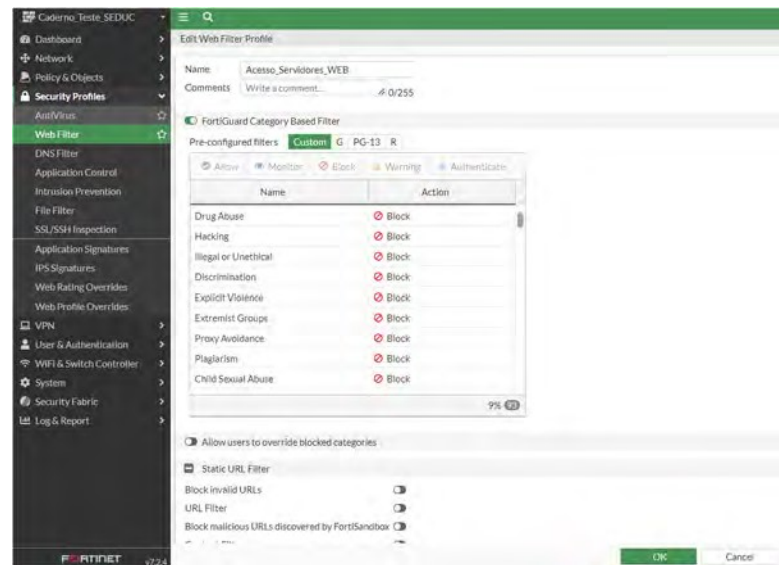
<p>Item de Teste - 5.3.5.9.1</p>	<p>Aplicação da Web;</p>
<p>Objetivo do Teste</p>	<p>Validar se o Firewall possibilita o bloqueio ou permissão de aplicações da Web</p>
<p>Configuração do Teste</p>	<p>Navegando por Security Profiles > Application Control é possível realizar o bloqueio ou liberação de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

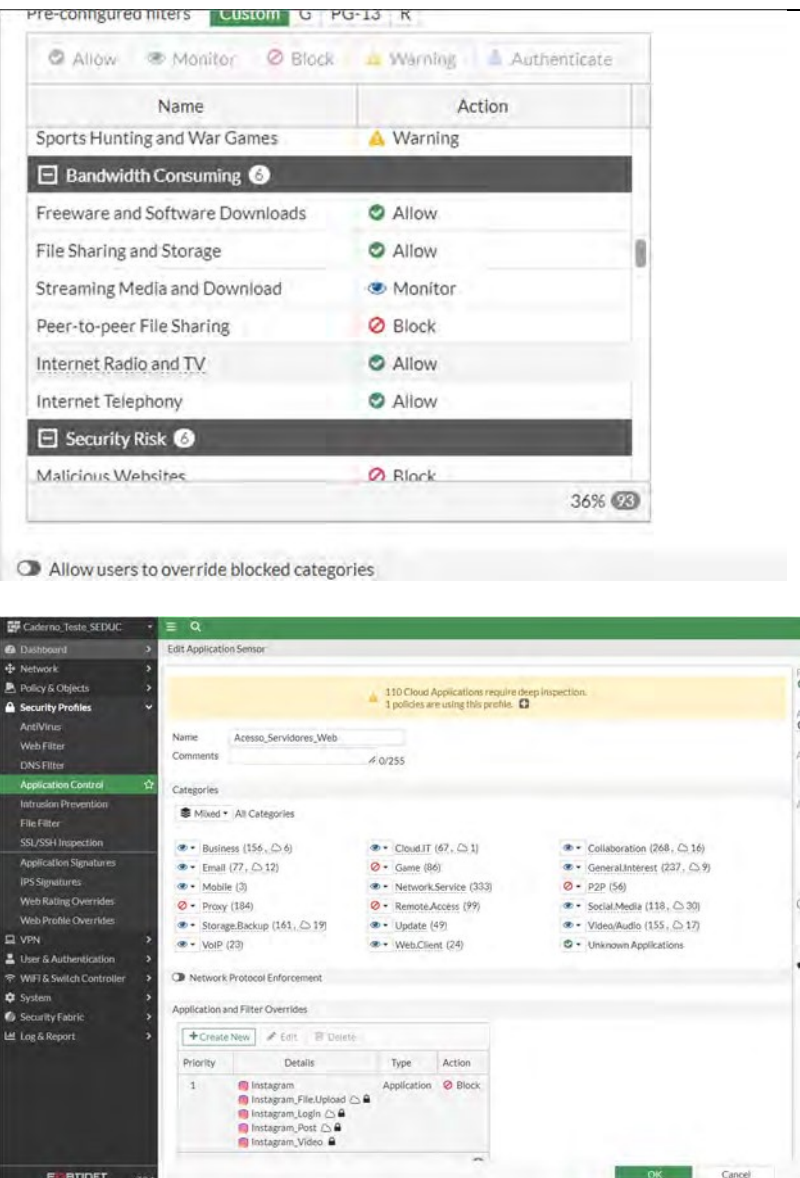
<p>Comentário</p>	<p>TESTE OK</p>  <p>The screenshot shows the 'Add New Override' window in Fortinet's Application Control interface. It displays a list of application signatures with the following columns: Name, Category, Technology, Popularity, and Risk. The list includes various applications such as 1boxun, 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>
--------------------------	---

<p>Item de Teste - 5.3.5.9.2</p>	<p>Categorias;</p>
<p>Objetivo do Teste</p>	<p>Validar se o Firewall possibilita o bloqueio ou permissão de aplicações web por meio de categorias</p>
<p>Configuração 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>Procedimento do Teste</p>	<p>Criar regra de segurança NGFW selecionando categoria de reputação web.</p>
<p>Evidências</p>	

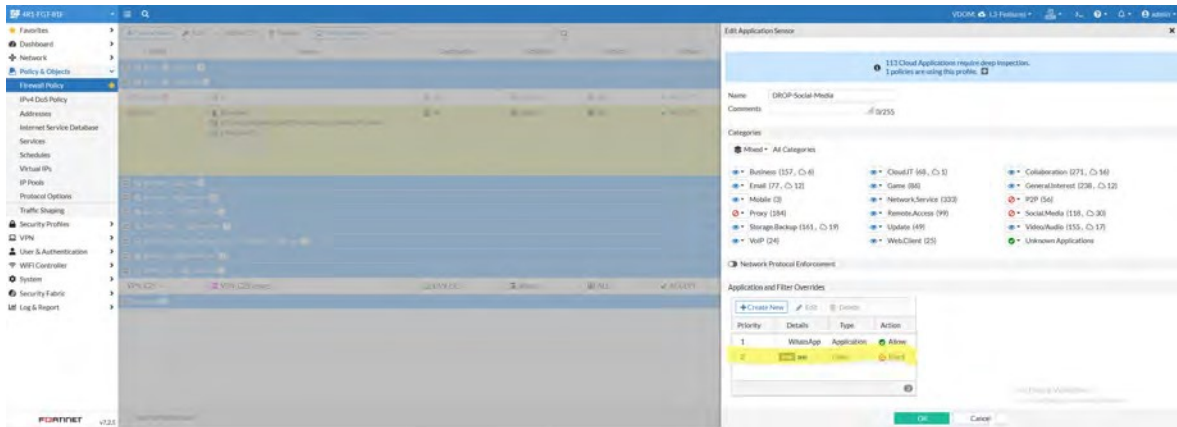
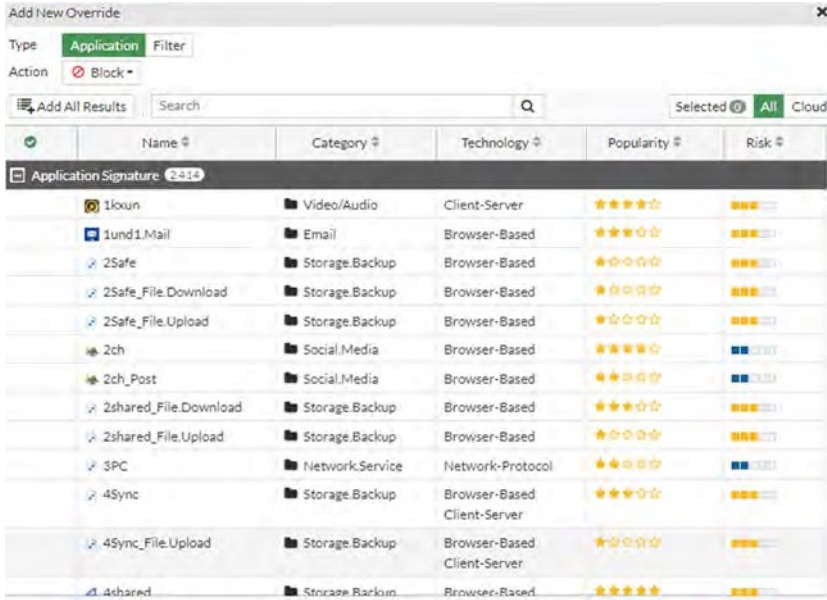


TESTE OK

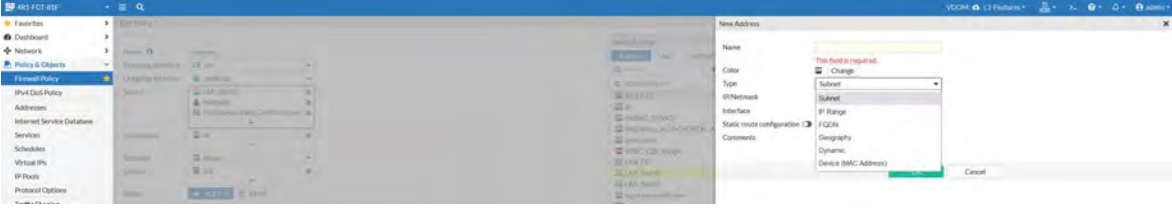
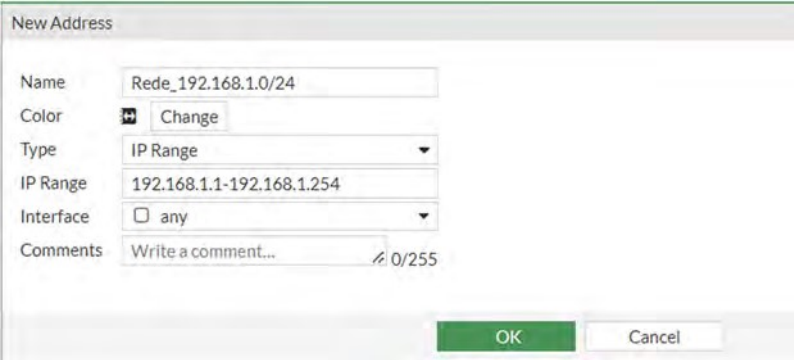


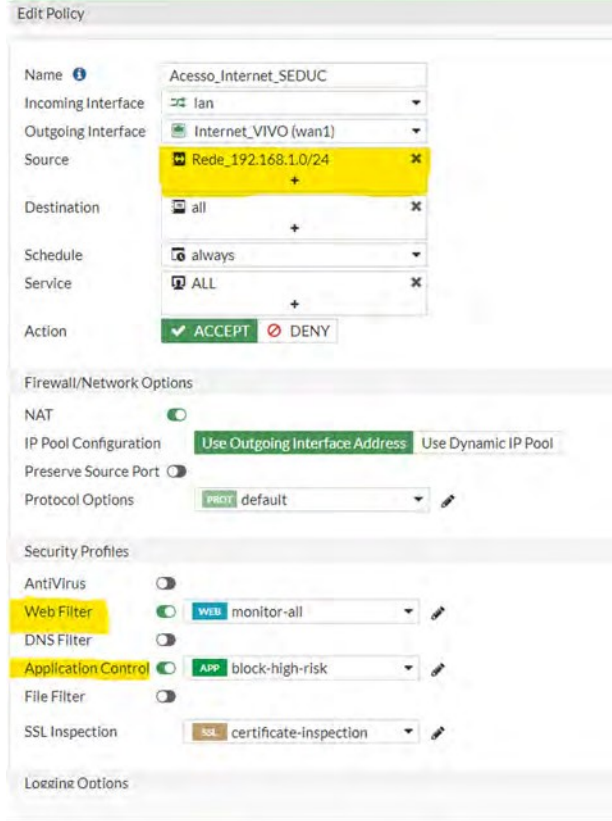
	 <p>The top screenshot shows the 'Pre-configured filters' window with a table of categories and their actions:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>Sports Hunting and War Games</td> <td>Warning</td> </tr> <tr> <td>Bandwidth Consuming</td> <td></td> </tr> <tr> <td>Freeware and Software Downloads</td> <td>Allow</td> </tr> <tr> <td>File Sharing and Storage</td> <td>Allow</td> </tr> <tr> <td>Streaming Media and Download</td> <td>Monitor</td> </tr> <tr> <td>Peer-to-peer File Sharing</td> <td>Block</td> </tr> <tr> <td>Internet Radio and TV</td> <td>Allow</td> </tr> <tr> <td>Internet Telephony</td> <td>Allow</td> </tr> <tr> <td>Security Risk</td> <td></td> </tr> <tr> <td>Malicious Websites</td> <td>Block</td> </tr> </tbody> </table> <p>The bottom screenshot shows the 'Edit Application Sensor' configuration for 'Acesso_Servidores_Web'. It displays a list of categories with their respective counts and actions. A table at the bottom shows 'Application and Filter Overrides' for Instagram:</p> <table border="1"> <thead> <tr> <th>Priority</th> <th>Details</th> <th>Type</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Instagram, Instagram_File.Upload, Instagram_Login, Instagram_Post, Instagram_Video</td> <td>Application</td> <td>Block</td> </tr> </tbody> </table>	Name	Action	Sports Hunting and War Games	Warning	Bandwidth Consuming		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		Malicious Websites	Block	Priority	Details	Type	Action	1	Instagram, Instagram_File.Upload, Instagram_Login, Instagram_Post, Instagram_Video	Application	Block
Name	Action																														
Sports Hunting and War Games	Warning																														
Bandwidth Consuming																															
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																															
Malicious Websites	Block																														
Priority	Details	Type	Action																												
1	Instagram, Instagram_File.Upload, Instagram_Login, Instagram_Post, Instagram_Video	Application	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>TESTE OK</p> 
<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>

Procedimento do Teste	<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>
Evidências	 <p>TESTE OK</p>  <p>The 'New Address' dialog box contains the following fields:</p> <ul style="list-style-type: none">Name: Rede_192.168.1.0/24Color: ChangeType: IP RangeIP Range: 192.168.1.1-192.168.1.254Interface: anyComments: Write a comment... 0/255 <p>Buttons: OK, Cancel</p>

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

<p>Item de Teste - 5.3.5.9.5</p>	<p>Usuários;</p>
<p>Objetivo do Teste</p>	<p>Validar se o equipamento possibilita a permissão ou bloqueio de aplicações ou URLs pelo critério de usuários</p>
<p>Configuração do Teste</p>	<p>Utilizar usuários do FortiGate para realizar o bloqueio ou permissão de aplicações e URLs</p>
<p>Procedimento do Teste</p>	<ol style="list-style-type: none"> 1 - Criação de um novo usuário 2 - Navegando por Policy & Objects > Firewall Policy > Source é possível enquadrar o usuário criado no campo "Source" 3- Por último basta enquadrar um perfil de Web Filter ou Application Control na política

Evidências

The screenshot shows the 'Edit Policy' configuration for a policy named 'Internet'. The configuration includes:

- Name:** Internet
- Incoming Interface:** lan
- Outgoing Interface:** underlay
- Source:** LAN_Site01, tmarques, CN=Acesso_Web_GRP:CN=Users
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY
- Inspection Mode:** Flow-based (selected), Proxy-based
- Firewall/Network Options:** NAT, IP Pool Configuration (Use Outgoing Interface Address, Use Dynamic IP Pool), Preserve Source Port, Passive Health Check, Protocol Options (default)
- Security Profiles:** Antivirus (AV-WEB), Web Filter (g-default), Video Filter (CNN-Brasil), DNS Filter (default)

A 'Select Entries' dialog box is open, showing a search for 'User'. The results include:

- USER (5)
- Local (2)
- Administrador
- Tiago Marques
- Tiago Marques 02
- Local (2)
- tmarques (highlighted)
- tmarqueswebuser
- USER GROUP (3)
- Acesso_Web_GRP_Local
- SSO_Guest_Users
- VPN_C2S_GRP
- FSSO GROUP (1)
- Local FSSO Agent (1)
- CN=Acesso_Web_GRP:CN=Users,DC=...

TESTE OK

The close-up shows the 'Select Entries' dialog box with the 'User' tab selected. The search results are:

- USER (2)
- Local (2)
- guest
- rodrigo (highlighted)
- USER GROUP (2)
- Guest-group
- SSO_Guest_Users

Users/Groups Creation Wizard

1 User Type
 2 **Login Credentials**
 3 Contact Info
 4 Extra Info

Username:

Password:

Edit Policy

Name: Acesso_Internet_SEDUC

Incoming Interface: lan

Outgoing Interface: Internet_VIVO (wan1)

Source: Rede_192.168.1.0/24, victor.nka

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT DENY

Firewall/Network Options

NAT:

IP Pool Configuration: Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port:

Protocol Options: protocol default

Security Profiles

AntiVirus:

Web Filter: monitor-all

DNS Filter:

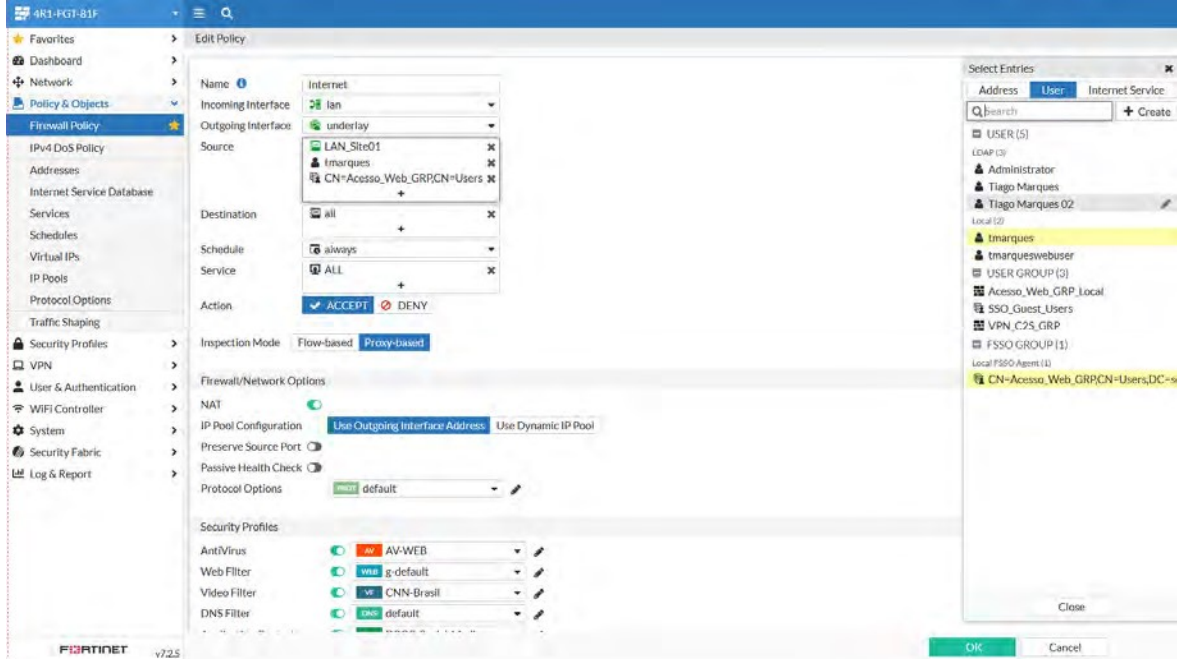
Application Control: block-high-risk

File Filter:

SSL Inspection: certificate-inspection

Comentário

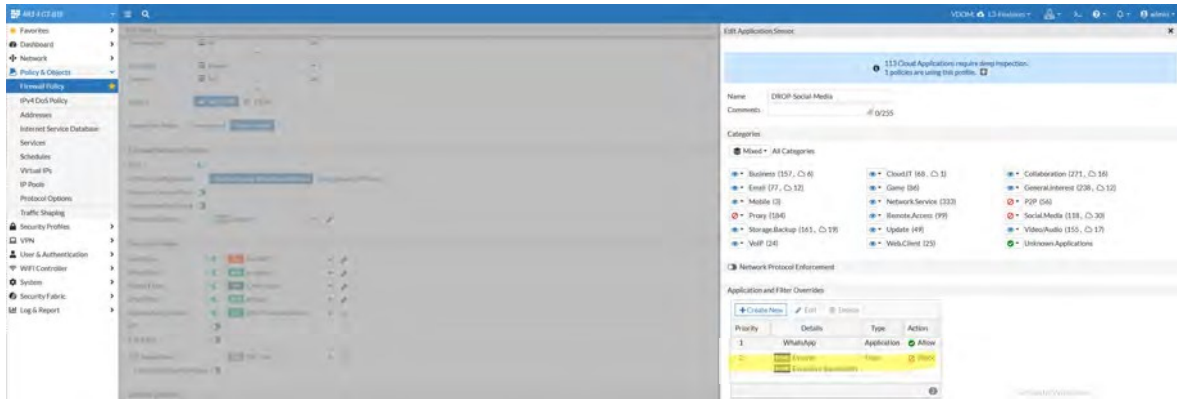
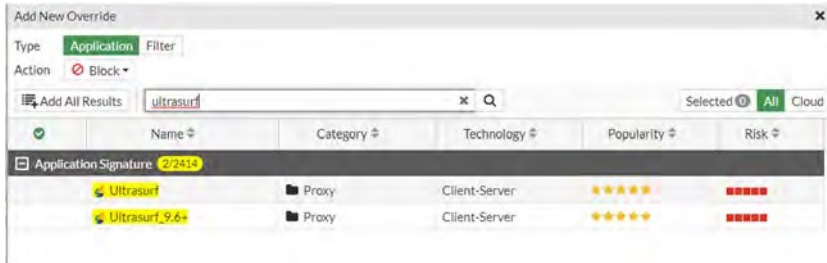
Item de Teste - 5.3.5.9.6	Diferentes grupos de usuários;
Objetivo do Teste	Validar se o equipamento possibilita a permissão ou bloqueio de aplicações ou URLs pelo critério de diferentes grupos de usuários
Configuração do Teste	1 - Criação de um novo grupo de usuários 2 - Navegando por Policy & Objects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

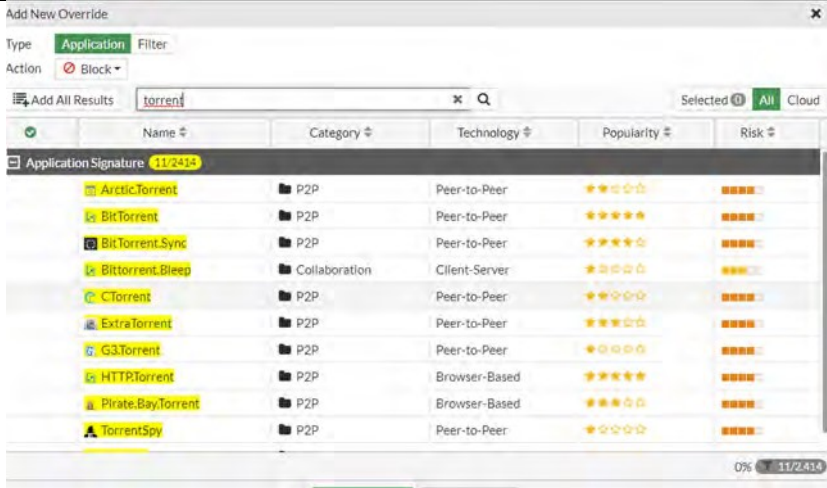
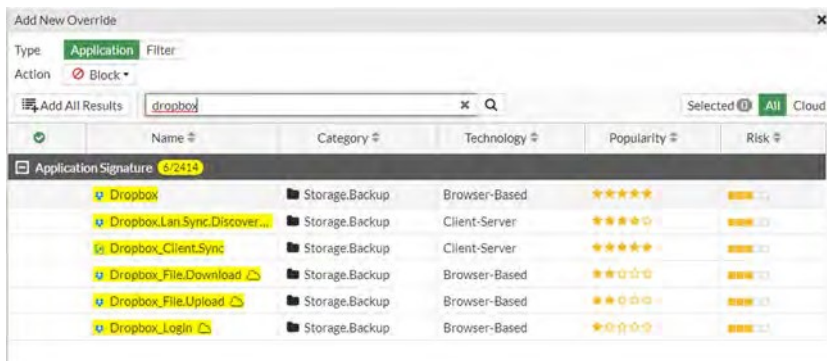
<p>Procedimento do Teste</p>	<p>Criar duas regras NGFW com origem de grupos distintos</p>
<p>Evidências</p>	 <p>TESTE OK</p> <p>Criando um novo Grupo</p>

2 – Definindo membros no grupo

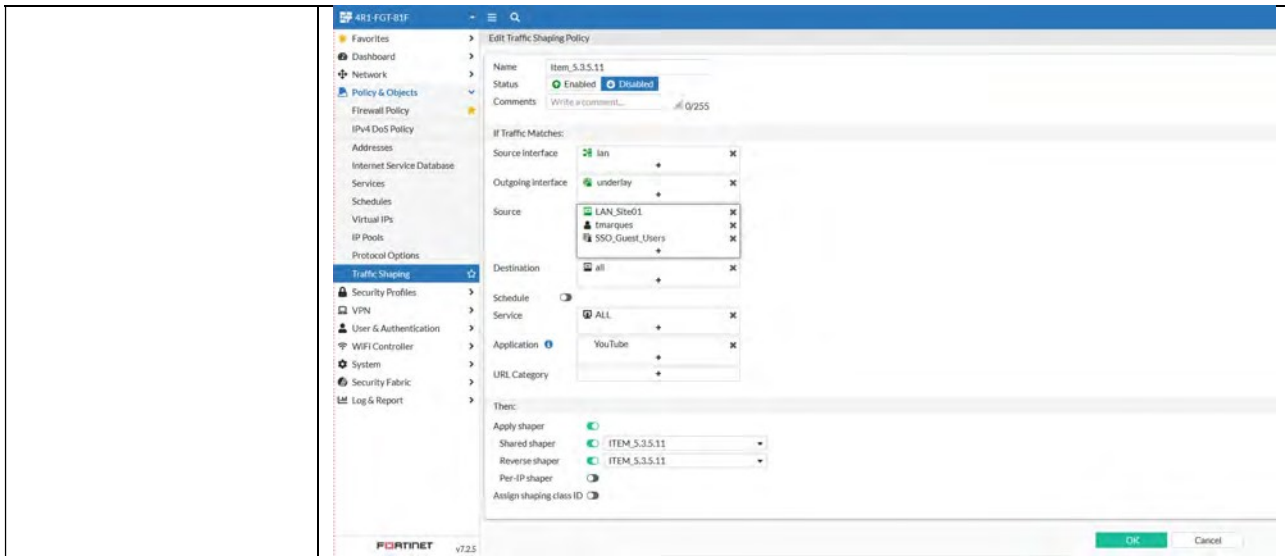
3 - Adicionando o Grupo no campo Source e adicionando filtros de Web e Aplicações

Comentário

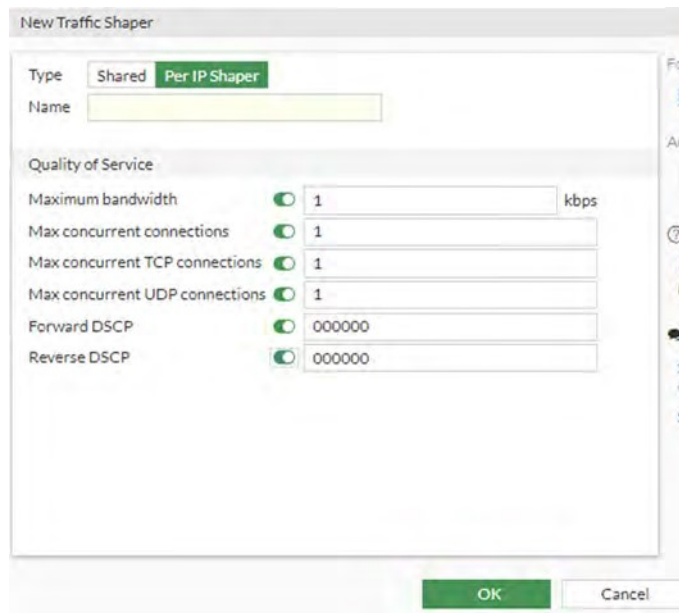
Item de Teste - 5.3.5.10	Aplicações que sejam passíveis a técnicas de evasão por malwares e uso excessivo de banda (EX:ultrasurf, torrent, dropbox e file sharing);																				
Objetivo do Teste	Validar se o FortiGate consegue bloquear as aplicações passíveis a técnicas de evasão por malwares 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	<div data-bbox="240 680 1422 1077">  </div> <p>TESTE OK</p> <div data-bbox="240 1301 1070 1563">  <table border="1" data-bbox="240 1422 1070 1563"> <thead> <tr> <th>Name</th> <th>Category</th> <th>Technology</th> <th>Popularity</th> <th>Risk</th> </tr> </thead> <tbody> <tr> <td>Application Signature (2/2414)</td> <td></td> <td></td> <td></td> <td></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> </div>	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	★★★★★	★★★★★																	

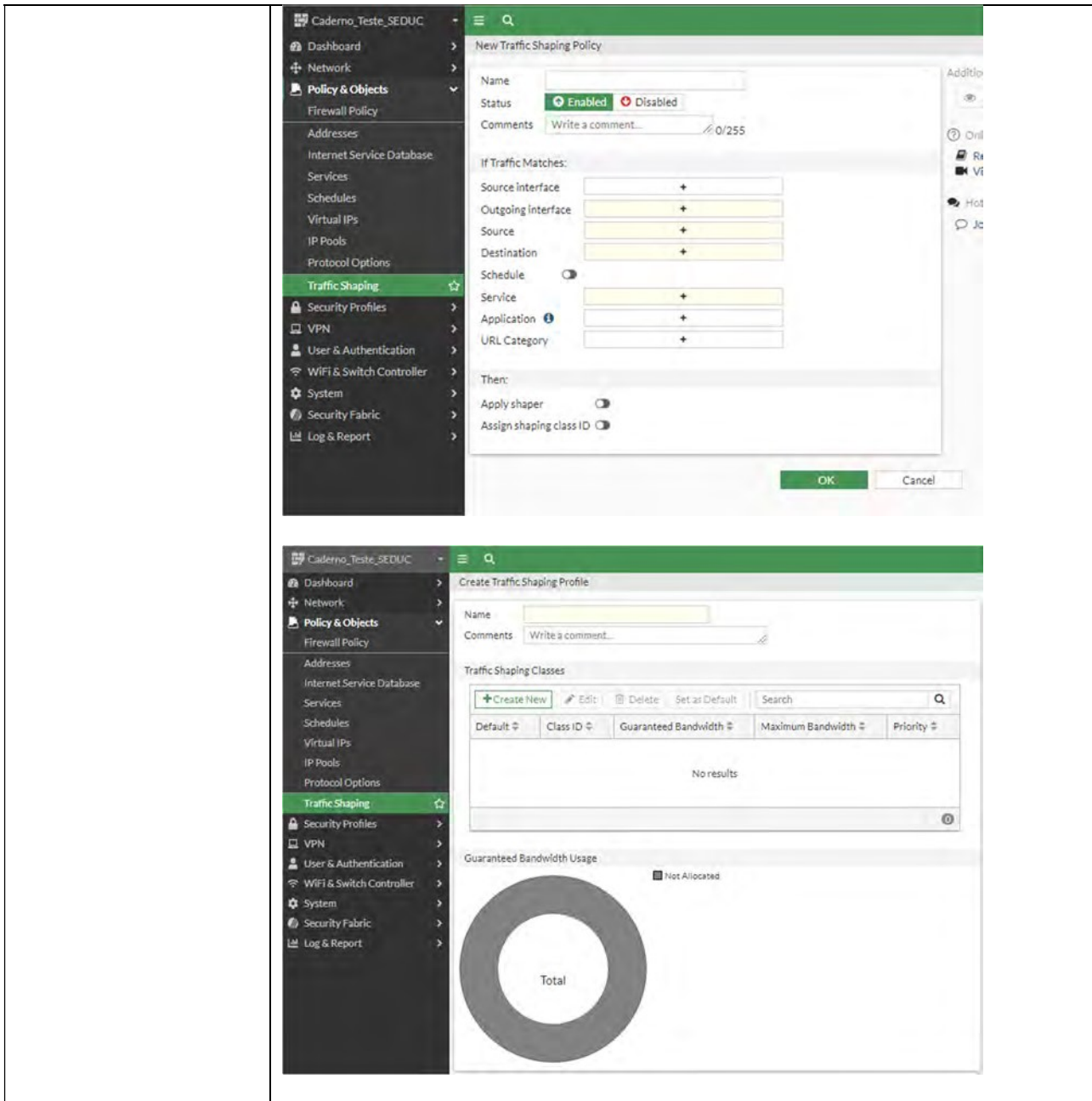
<p>Comentário</p>	 <p>The screenshot shows the 'Add New Override' window in Snort. The search filter is set to 'torrent'. The table lists various torrent-related applications with their categories, technologies, popularity, and risk levels.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Category</th> <th>Technology</th> <th>Popularity</th> <th>Risk</th> </tr> </thead> <tbody> <tr><td>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>C.Torrent</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>HTTR.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>  <p>The second screenshot shows the 'Add New Override' window with the search filter set to 'dropbox'. The table lists various Dropbox-related applications.</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>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	ArcticTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	☆☆☆☆	BitTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	☆☆☆☆	BitTorrent.Sync	P2P	Peer-to-Peer	☆☆☆☆☆	☆☆☆☆	Bittorrent.Bleep	Collaboration	Client-Server	☆☆☆☆☆	☆☆☆☆	C.Torrent	P2P	Peer-to-Peer	☆☆☆☆☆	☆☆☆☆	ExtraTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	☆☆☆☆	G3.Torrent	P2P	Peer-to-Peer	☆☆☆☆☆	☆☆☆☆	HTTR.Torrent	P2P	Browser-Based	☆☆☆☆☆	☆☆☆☆	Pirate.Bay.Torrent	P2P	Browser-Based	☆☆☆☆☆	☆☆☆☆	TorrentSpy	P2P	Peer-to-Peer	☆☆☆☆☆	☆☆☆☆	Name	Category	Technology	Popularity	Risk	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																																																																																						
ArcticTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	☆☆☆☆																																																																																							
BitTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	☆☆☆☆																																																																																							
BitTorrent.Sync	P2P	Peer-to-Peer	☆☆☆☆☆	☆☆☆☆																																																																																							
Bittorrent.Bleep	Collaboration	Client-Server	☆☆☆☆☆	☆☆☆☆																																																																																							
C.Torrent	P2P	Peer-to-Peer	☆☆☆☆☆	☆☆☆☆																																																																																							
ExtraTorrent	P2P	Peer-to-Peer	☆☆☆☆☆	☆☆☆☆																																																																																							
G3.Torrent	P2P	Peer-to-Peer	☆☆☆☆☆	☆☆☆☆																																																																																							
HTTR.Torrent	P2P	Browser-Based	☆☆☆☆☆	☆☆☆☆																																																																																							
Pirate.Bay.Torrent	P2P	Browser-Based	☆☆☆☆☆	☆☆☆☆																																																																																							
TorrentSpy	P2P	Peer-to-Peer	☆☆☆☆☆	☆☆☆☆																																																																																							
Name	Category	Technology	Popularity	Risk																																																																																							
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	☆☆☆☆☆	☆☆☆☆																																																																																							

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



TESTE OK





The image displays two screenshots of the NCT management interface, showing the configuration of traffic shaping policies and profiles.

Top Screenshot: New Traffic Shaping Policy

The interface shows the configuration for a new traffic shaping policy. The left sidebar lists various network management options, with "Traffic Shaping" selected. The main panel is titled "New Traffic Shaping Policy" and includes the following fields and options:

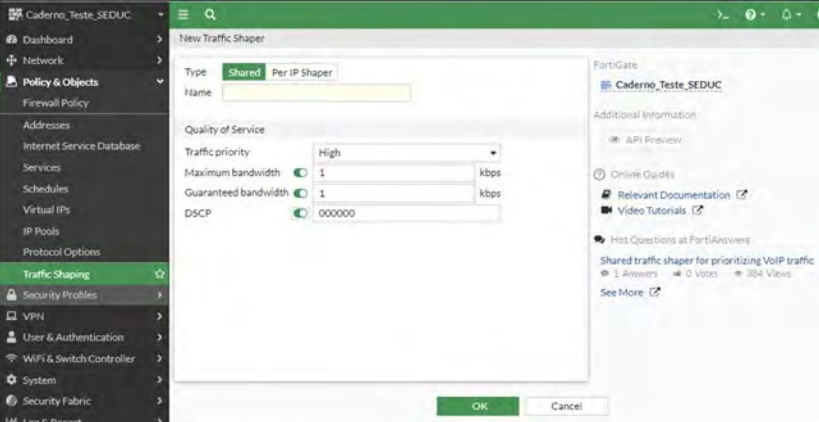
- Name:** A text input field.
- Status:** A toggle switch set to "Enabled" (with "Disabled" as an alternative).
- Comments:** A text area with a character count of 0/255.
- If Traffic Matches:** A section with several dropdown menus:
 - Source Interface
 - Outgoing Interface
 - Source
 - Destination
 - Schedule (with a toggle switch)
 - Service
 - Application
 - URL Category
- Then:** A section with two toggle switches:
 - Apply shaper
 - Assign shaping class ID

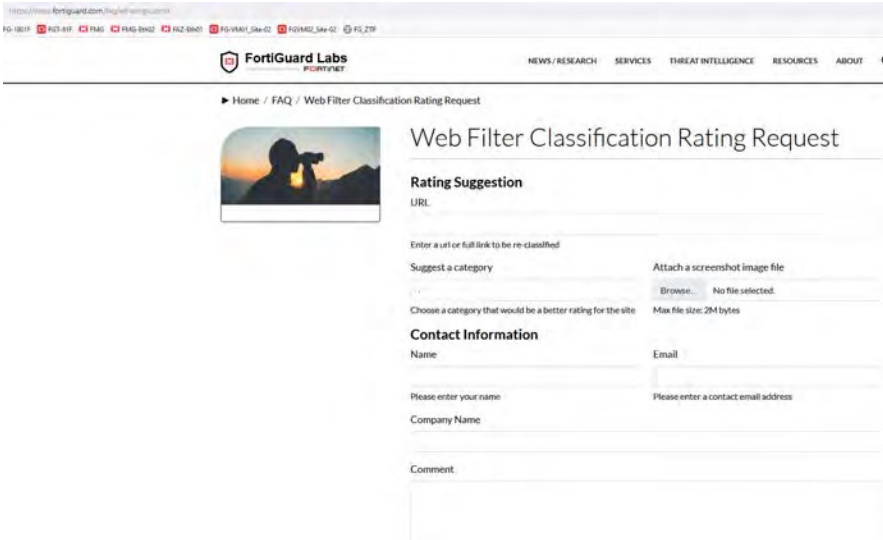
Buttons for "OK" and "Cancel" are located at the bottom right.

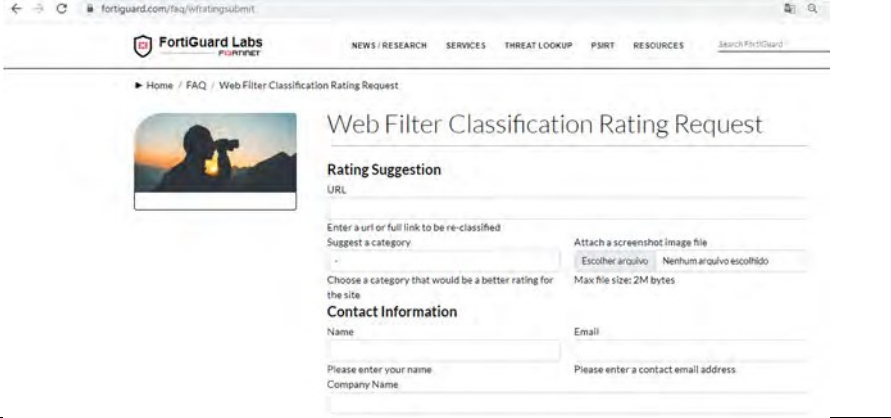
Bottom Screenshot: Create Traffic Shaping Profile

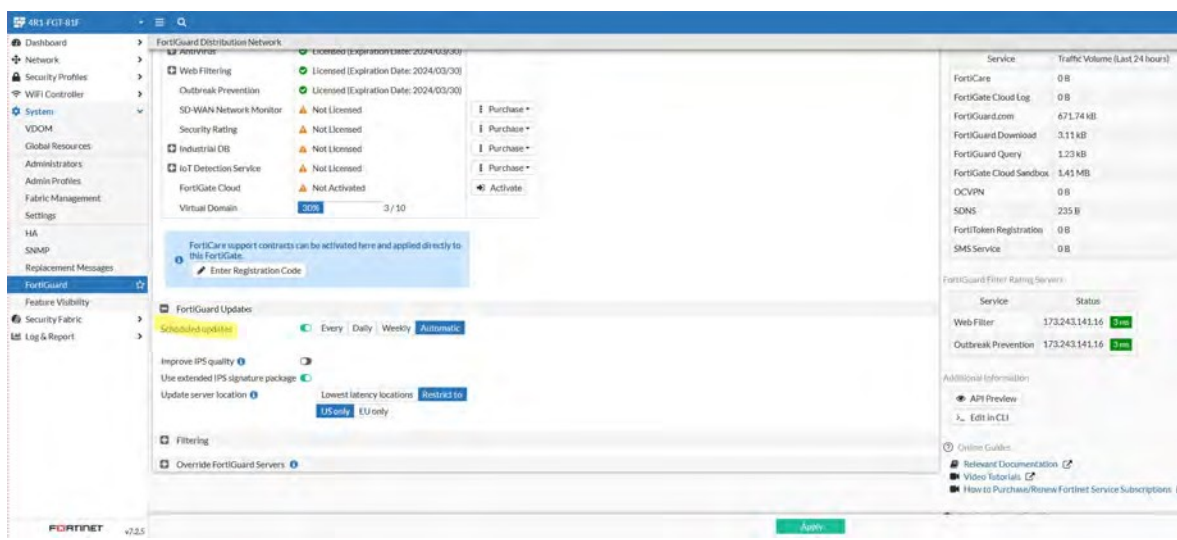
The interface shows the configuration for a new traffic shaping profile. The left sidebar is the same, with "Traffic Shaping" selected. The main panel is titled "Create Traffic Shaping Profile" and includes the following elements:

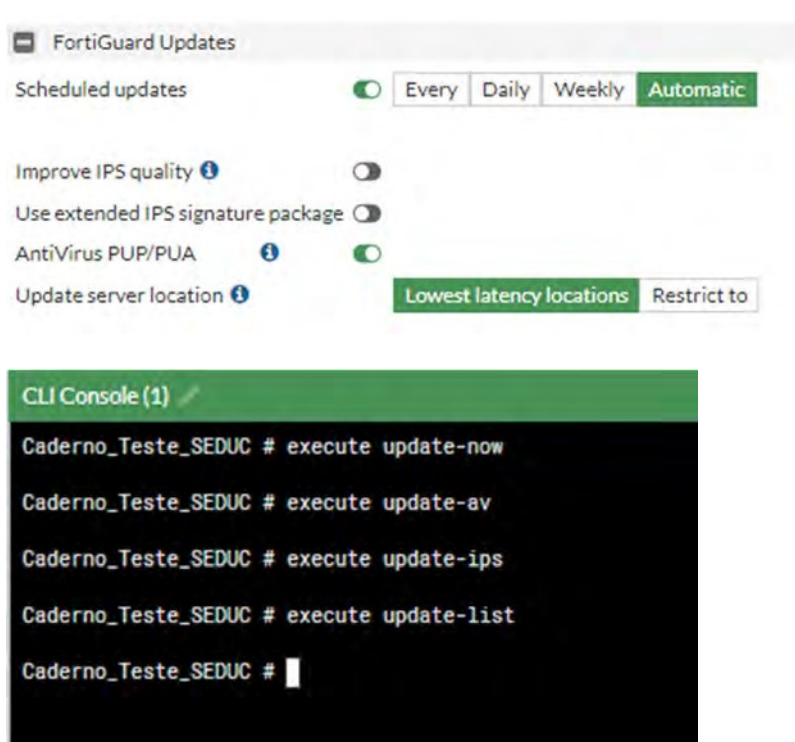
- Name:** A text input field.
- Comments:** A text area.
- Traffic Shaping Classes:** A table with columns: Default, Class ID, Guaranteed Bandwidth, Maximum Bandwidth, and Priority. The table currently shows "No results".
- Guaranteed Bandwidth Usage:** A donut chart showing usage. The chart is currently empty, with a legend indicating "Not Allocated" and a label "Total" in the center.

	
Comentário	

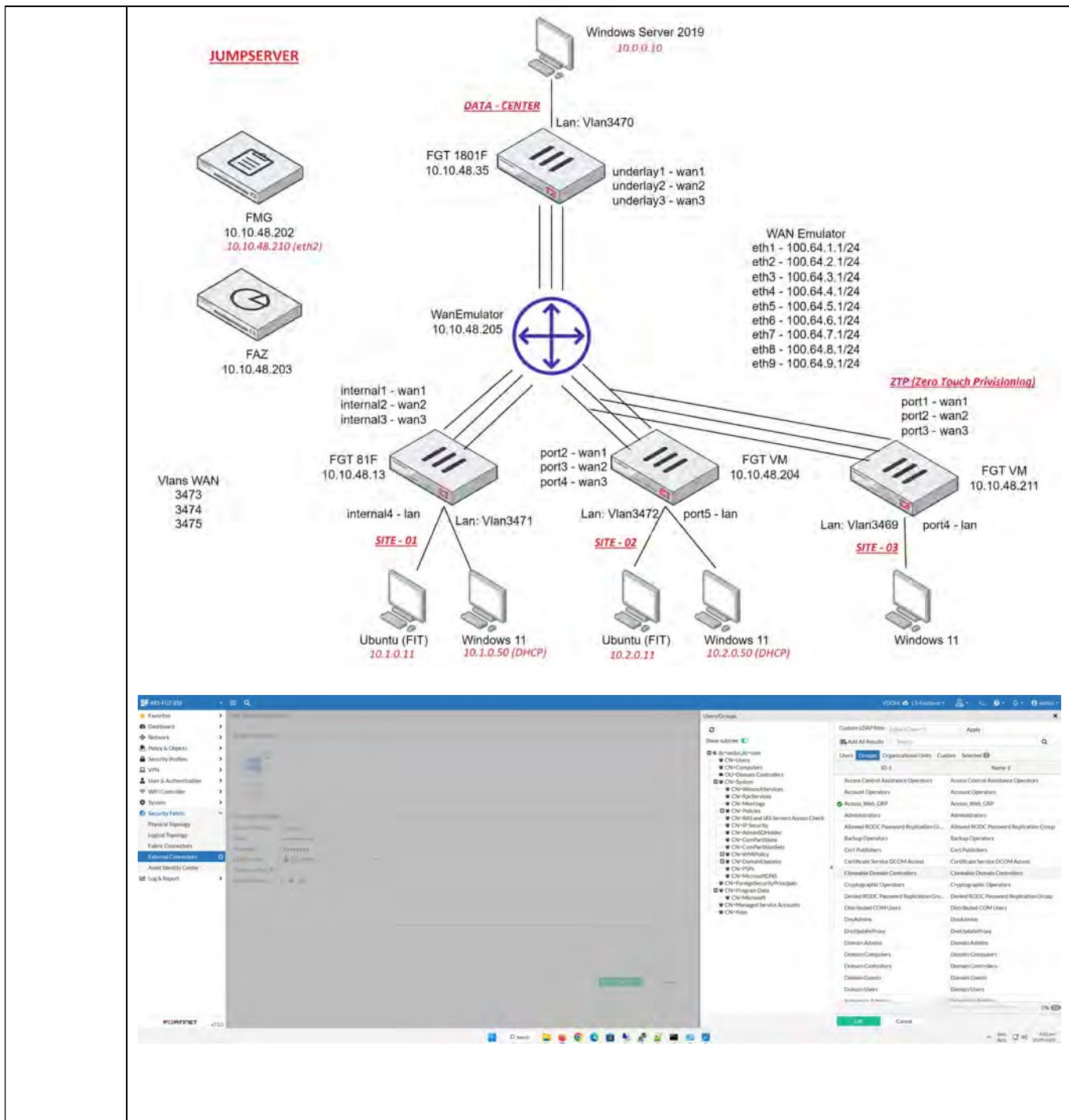
Item de Teste - 5.3.5.12	A solução deve fornecer uma forma para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;
Objetivo do Teste	Validar se a solução fornece uma forma para solicitação de categorização de URL caso a mesma não esteja categorizada ou categorizada incorretamente
Configuração do Teste	Acessar site de sugestão de recategorização na nuvem de inteligência Fortinet
Procedimento do Teste	<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/wfratingsubmit</p>
Evidências	<p>Acessar https://www.fortiguard.com/faq/wfratingsubmit</p>  <p>TESTE OK</p>

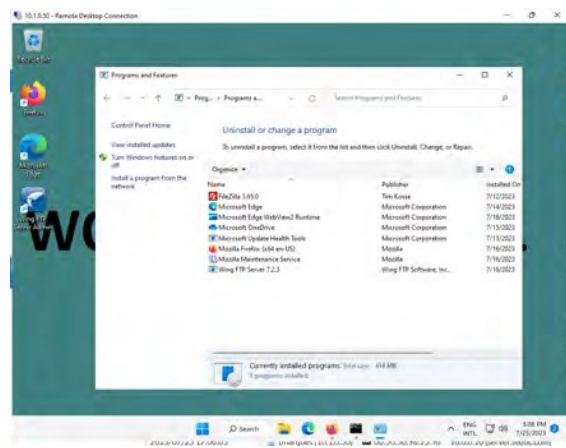
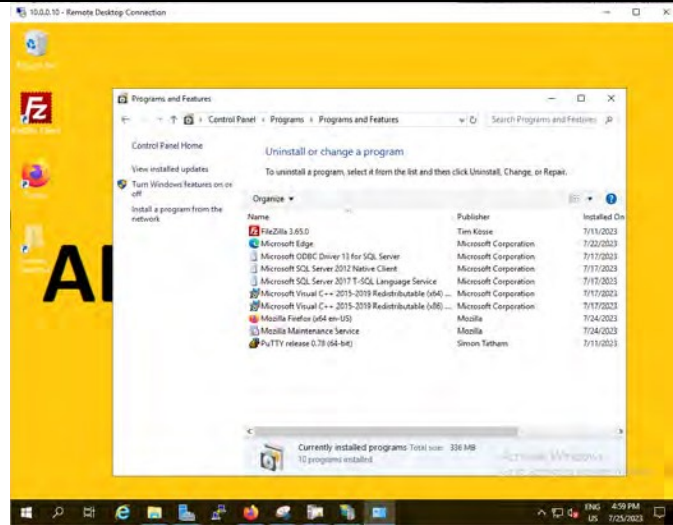
<p>Comentário</p>	
--------------------------	--

<p>Item de Teste - 5.3.5.13</p>	<p>Deve atualizar a base de assinaturas de aplicações automaticamente sem a necessidade de reboot nos gateways e no módulo de gerência;</p>
<p>Objetivo do Teste</p>	<p>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</p>
<p>Configuração do Teste</p>	<p>Demonstrar página de update</p>
<p>Procedimento do Teste</p>	<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>Evidências</p>	 <p>TESTE OK</p>

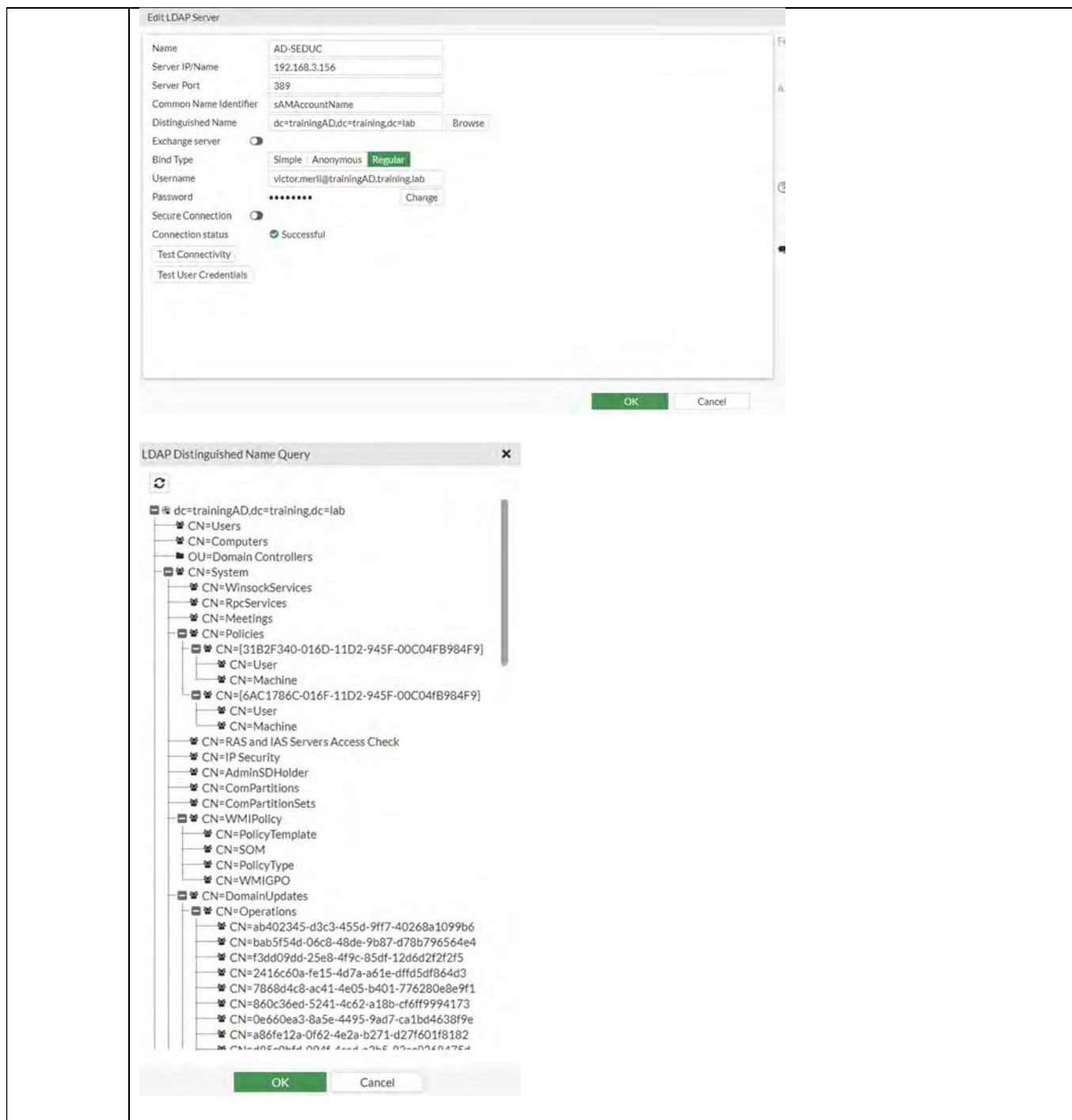
	 <p>The screenshot shows the FortiGuard Updates configuration interface. Under 'Scheduled updates', the 'Automatic' option is selected. Other options include 'Improve IPS quality', 'Use extended IPS signature package', 'AntiVirus PUP/PUA', and 'Update server location' (set to 'Lowest latency locations'). Below this is a CLI console window showing the following commands:</p> <pre> Caderno_Testes_SEDUC # execute update-now Caderno_Testes_SEDUC # execute update-av Caderno_Testes_SEDUC # execute update-ips Caderno_Testes_SEDUC # execute update-list Caderno_Testes_SEDUC # </pre>
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 .
Evidências	A integração não necessita da instalação de nenhum software no Active Directory e nem nas estações dos usuários.





TESTE OK



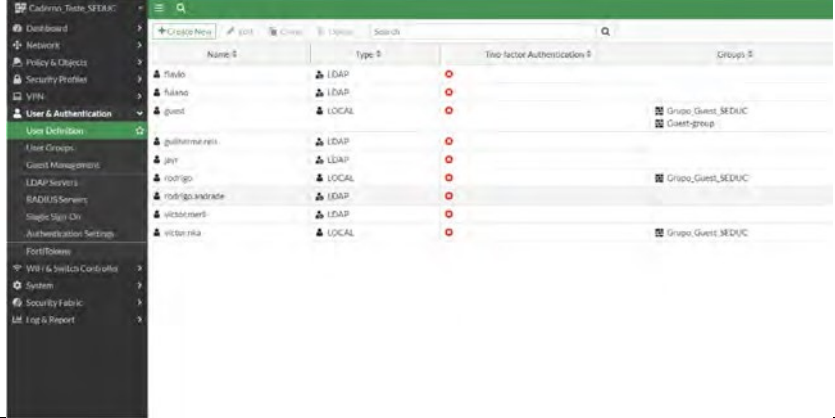
The image shows two screenshots from a software application. The top screenshot is titled "Edit LDAP Server" and contains the following fields:

- Name: AD-SEDUC
- Server IP/Name: 192.168.3.156
- Server Port: 389
- Common Name Identifier: sAMAccountName
- Distinguished Name: dc=trainingAD,dc=training,dc=lab (with a "Browse" button)
- Exchange server:
- Bind Type: Simple | Anonymous | **Regular**
- Username: victor.merli@trainingAD.training.lab
- Password: [masked]
- Secure Connection:
- Connection status: Successful
- Buttons: Test Connectivity, Test User Credentials, OK, Cancel

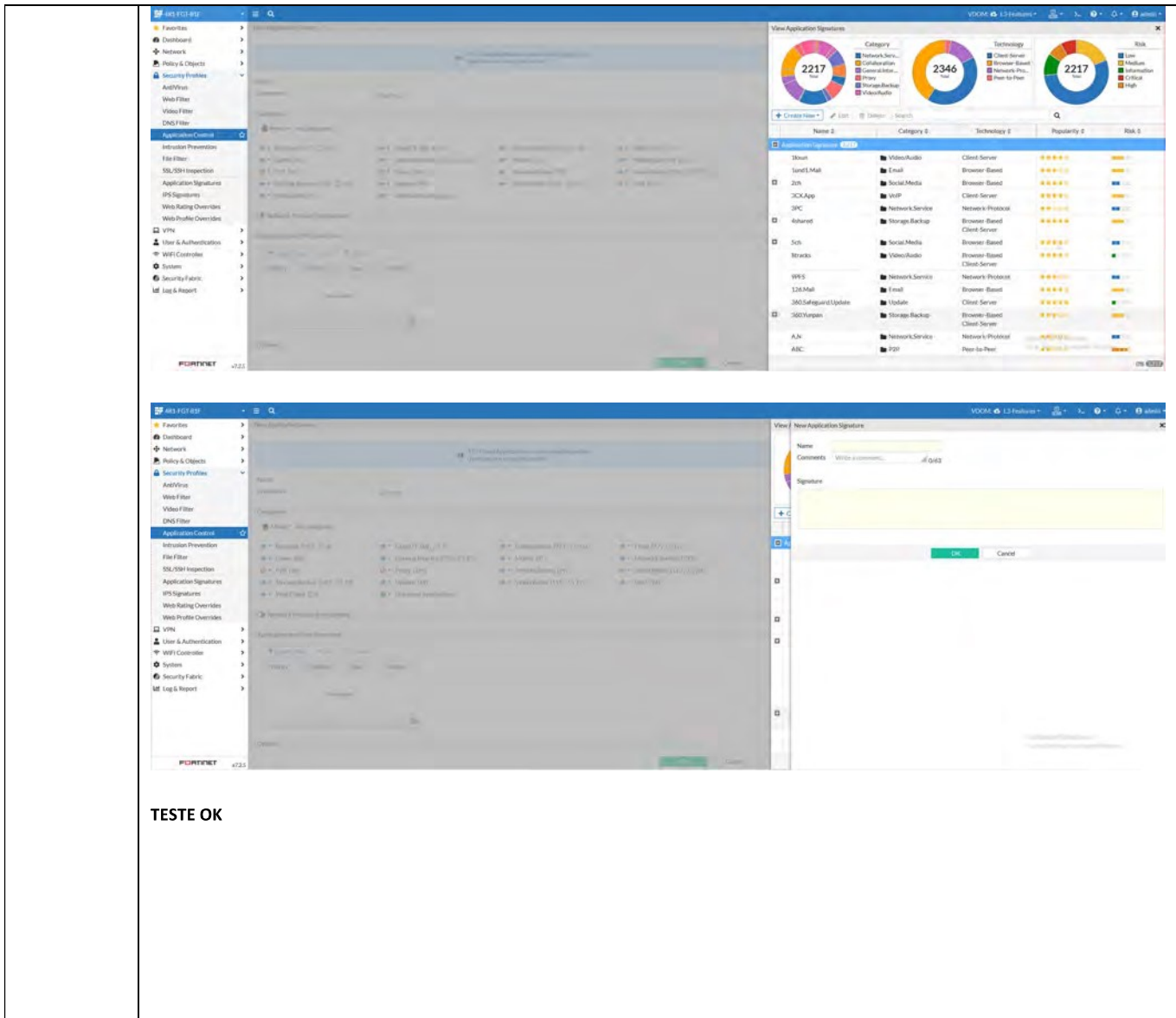
The bottom screenshot is titled "LDAP Distinguished Name Query" and displays a tree view of LDAP objects under the root "dc=trainingAD,dc=training,dc=lab":

- [-] CN=Users
- [-] CN=Computers
- [-] OU=Domain Controllers
- [-] CN=System
 - [-] CN=WinsockServices
 - [-] CN=RpcServices
 - [-] CN=Meetings
 - [-] CN=Policies
 - [-] CN=[31B2F340-016D-11D2-945F-00C04FB984F9]
 - [-] CN=User
 - [-] CN=Machine
 - [-] CN=[6AC1786C-016F-11D2-945F-00C04FB984F9]
 - [-] CN=User
 - [-] CN=Machine
 - [-] CN=RAS and IAS Servers Access Check
 - [-] CN=IP Security
 - [-] CN=AdminSDHolder
 - [-] CN=ComPartitions
 - [-] CN=ComPartitionSets
 - [-] CN=WMIPolicy
 - [-] CN=PolicyTemplate
 - [-] CN=SOM
 - [-] CN=PolicyType
 - [-] CN=WMIGPO
 - [-] CN=DomainUpdates
 - [-] CN=Operations
 - [-] CN=ab402345-d3c3-455d-9ff7-40268a1099b6
 - [-] CN=bab5f54d-06c8-48de-9b87-d78b796564e4
 - [-] CN=f3dd09dd-25e8-4f9c-85df-12d6d2f2f5
 - [-] CN=2416c60a-fe15-4d7a-a61e-dffd5df864d3
 - [-] CN=7868d4c8-ac41-4e05-b401-776280e8e9f1
 - [-] CN=860c36ed-5241-4c62-a18b-cf6ff9994173
 - [-] CN=0e660ea3-8a5e-4495-9ad7-ca1bd4638f9e
 - [-] CN=a86fe12a-0f62-4e2a-b271-d27f601f8182
 - [-] CN=d85c06f4-0044-4e2d-42e5-02cc0360a754

Buttons: OK, Cancel

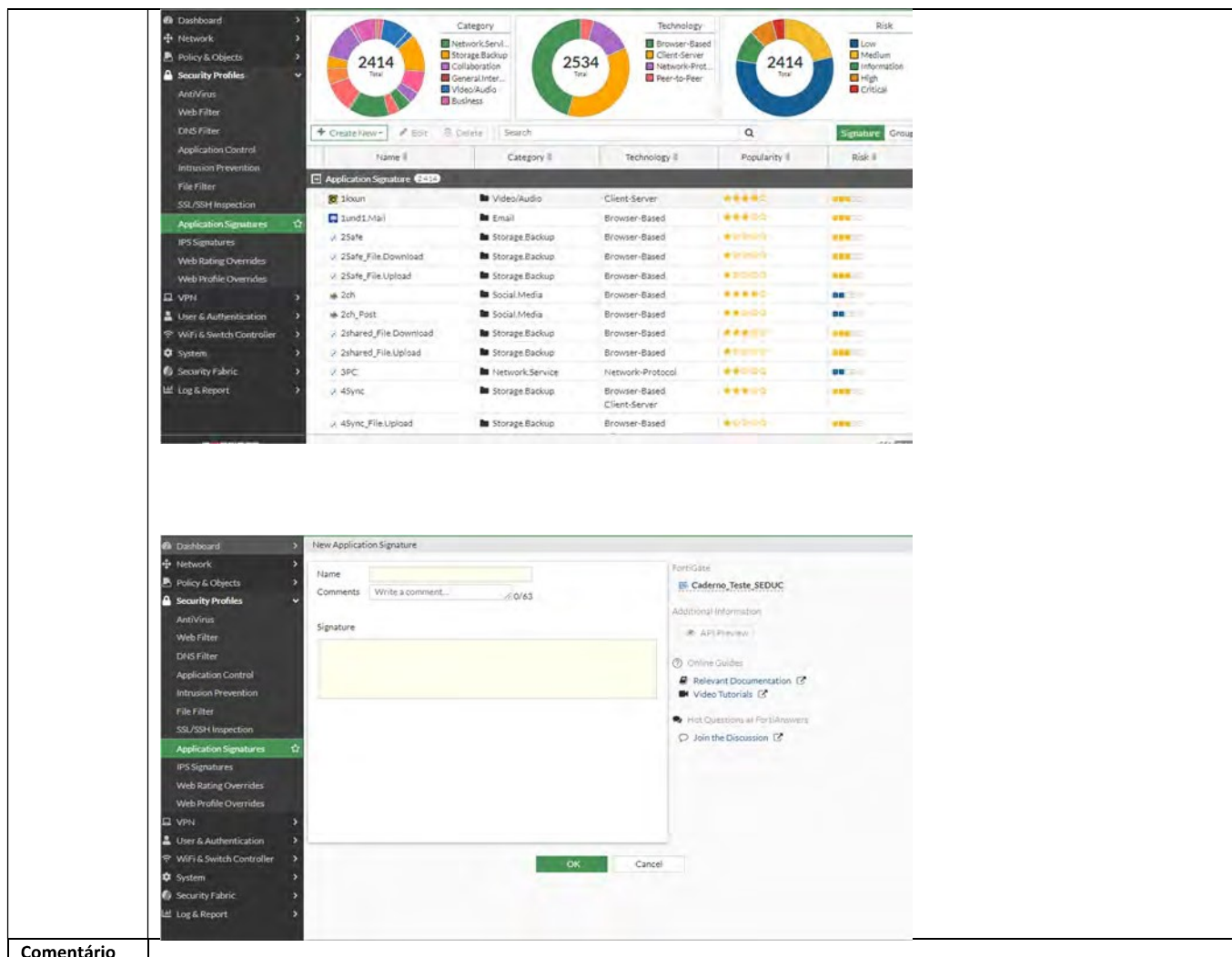
<p>Comentário</p>	 <p>The screenshot shows the 'User & Authentication' configuration page in Fortinet's GUI. It displays a table with columns for Name, Type, Two-factor Authentication, and Groups. The table lists several users: paulo, fulano, guest, guilhermeluis, jay, rodrigo, rodrigo.andrada, vicente.rossi, and vicente.rita. Most are of type LDAP, while 'guest' is LOCAL. Two-factor authentication is disabled for all. Groups include 'Grupo_Guest_SEE/UC' and 'Guest-group'.</p>
--------------------------	---

<p>Item de Teste - 5.3.5.15</p>	<p>Deve suportar o controle de aplicações conhecidas e possibilitar a inclusão de aplicações desconhecidas, sendo possível executar esta tarefa através da interface de gerência GUI ou WEB, ou, através de ticket direto com o fabricante;</p>
<p>Objetivo do Teste</p>	<p>Validar se o equipamento suporta controle de aplicações conhecidas, e se é possível incluir novas assinaturas por meio da interface gráfica ou pela WEB, ou, através de ticket direto com a fabricante.</p>
<p>Configuração do Teste</p>	<p>Demonstrar capacidade de criação de aplicação</p>
<p>Procedimento do Teste</p>	<p>1 – Validar o controle de aplicações feito em assinaturas já conhecidas pela ferramenta.</p> <p>2 – Realizar a criação de uma nova assinatura.</p> <p>Navegando por Security Profiles > Application Signatures > Create New é possível criar novas assinaturas de aplicações customizadas, ou utilizar as mais de 2414 assinaturas conhecidas.</p> <p>1 – Navegando por Security Profiles > Application signatures é possível visualizar as assinaturas já conhecidas pela Fabricante.</p> <p>2 – Navegando por Security Profiles > Application signatures > Create New é possível criar novas assinaturas para aplicações não conhecidas pela fabricante.</p>
<p>Evidências</p>	



The image displays two screenshots of the Fortinet FortiGate web interface. The top screenshot shows the 'Application Control' configuration page, which includes a sidebar with navigation options like 'Dashboard', 'Network', 'Policy & Objects', 'Security Profiles', and 'Application Control'. The main area shows a table of application signatures with columns for Name, Category, Technology, Popularity, and Risk. A 'View Application Signatures' pop-up window is open, showing three donut charts: 'Category' (2217), 'Technology' (2346), and 'Risk' (2217). The bottom screenshot shows the 'New Application Signature' configuration page, with a sidebar and a main area for defining a signature, including fields for Name, Comments, and Signature.

TESTE OK

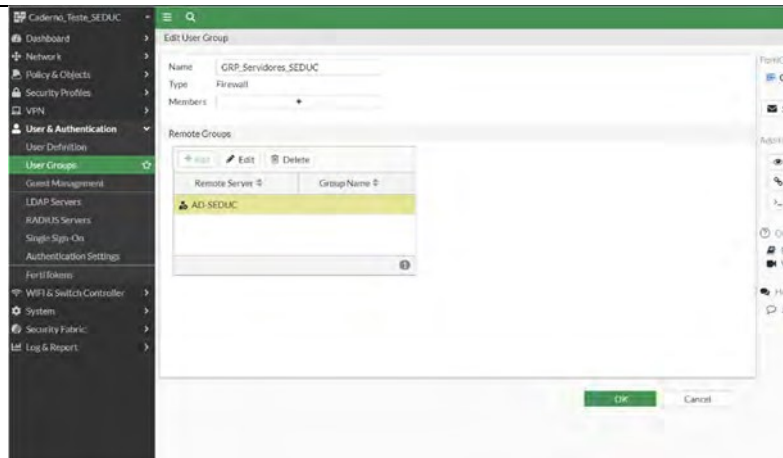


The image shows two screenshots of the FortiGate web interface. The top screenshot displays the 'Application Signatures' page with three donut charts showing counts for Category (2414), Technology (2534), and Risk (2414). Below the charts is a table listing various application signatures with columns for Name, Category, Technology, Popularity, and Risk. The bottom screenshot shows the 'New Application Signature' dialog box, which includes fields for Name, Comments, and a large text area for the Signature. On the right side of the dialog, there is a 'FortiGate' section with a dropdown menu set to 'Caderno_Teste_SEDUC' and several links for additional information like API Preview, Online Guides, Relevant Documentation, Video Tutorials, and a section for 'Hot Questions of FortiGate' with a 'Join the Discussion' link. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

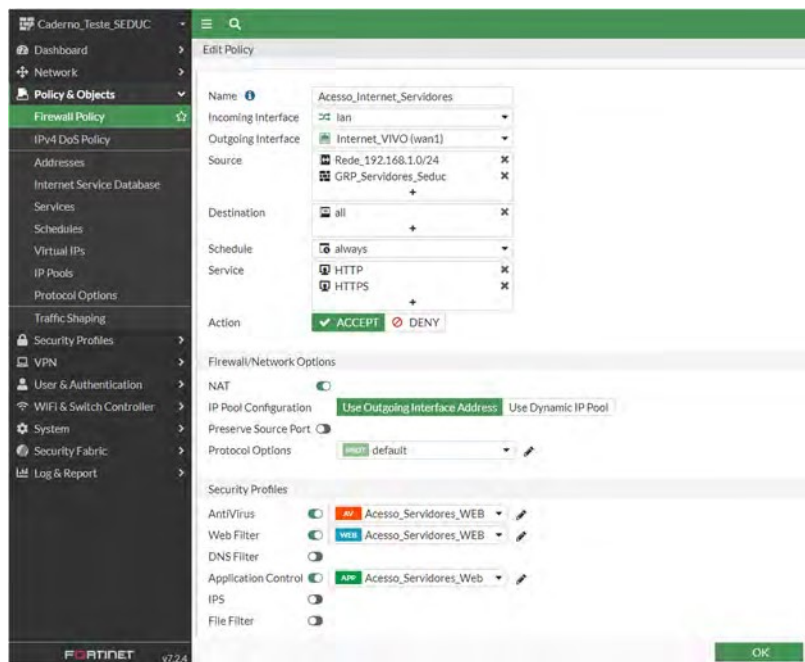
Comentário

5.3.6 IDENTIFICAÇÃO DE USUÁRIOS:

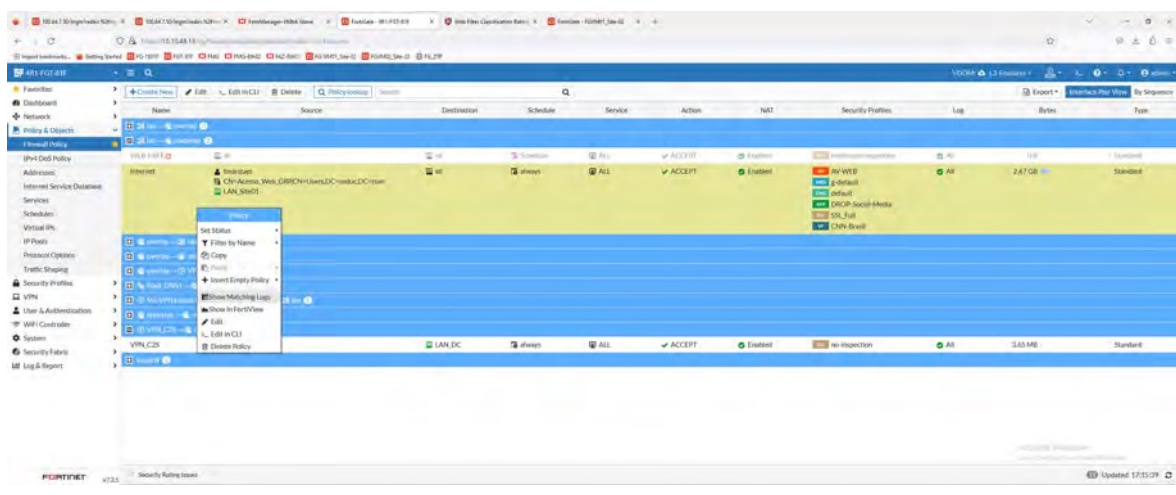
<p>Item de Teste - 5.3.6.1</p>	<p>Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório;</p>
<p>Objetivo do Teste</p>	<p>Validar se a ferramenta tem a capacidade de realizar o controle de qual usuário está utilizando determinada aplicação, por meio de integração com serviços de diretório</p>
<p>Configuração do Teste</p>	<p>Demonstrar capacidade de integração com o AD.</p>
<p>Procedimento do Teste</p>	<p>Navegando por User and Authentication > LDAP Servers > Create New é possível realizar a integração com os serviços de diretório</p> <p>Navegando por User and Authentication > User Group > Create New podemos criar um novo grupo de usuários linkado com o grupo do AD</p>



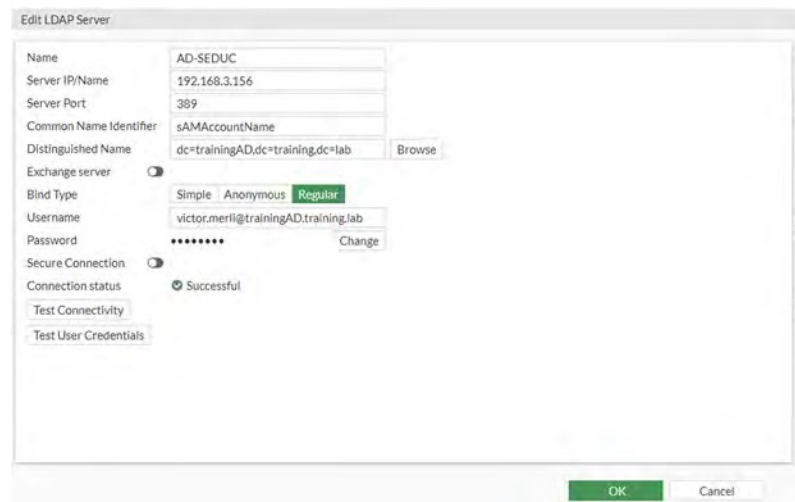
3- Criação de uma política com filtro de aplicação e web



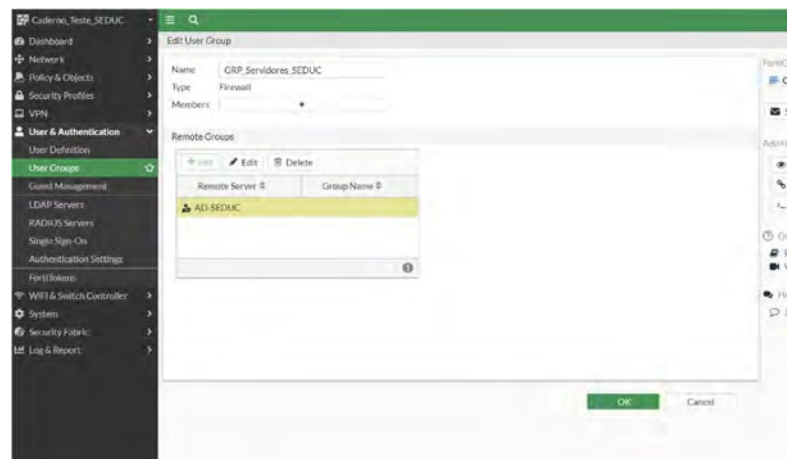
	
Comentário	Fonte: https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/656084/firewall-policy

Item de Teste - 5.3.6.2	Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
Objetivo do Teste	Validar se a ferramenta possibilita integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas
Configuração do Teste	Criar duas regras NGFW com filtros distintos de grupos do AD
Procedimento do Teste	<p>Para realizar esse teste é necessário primeiro realizar a integração do AD com o FortiGate da forma que está descrita no item “5.3.5.14” deste documento.</p> <p>Após ter realizado a integração, basta incluir os usuários e grupos LDAP nas políticas, para realizar o controle de quais aplicações serão liberadas para esse grupo ou usuário.</p>
Evidências	 <p>TESTE OK</p>

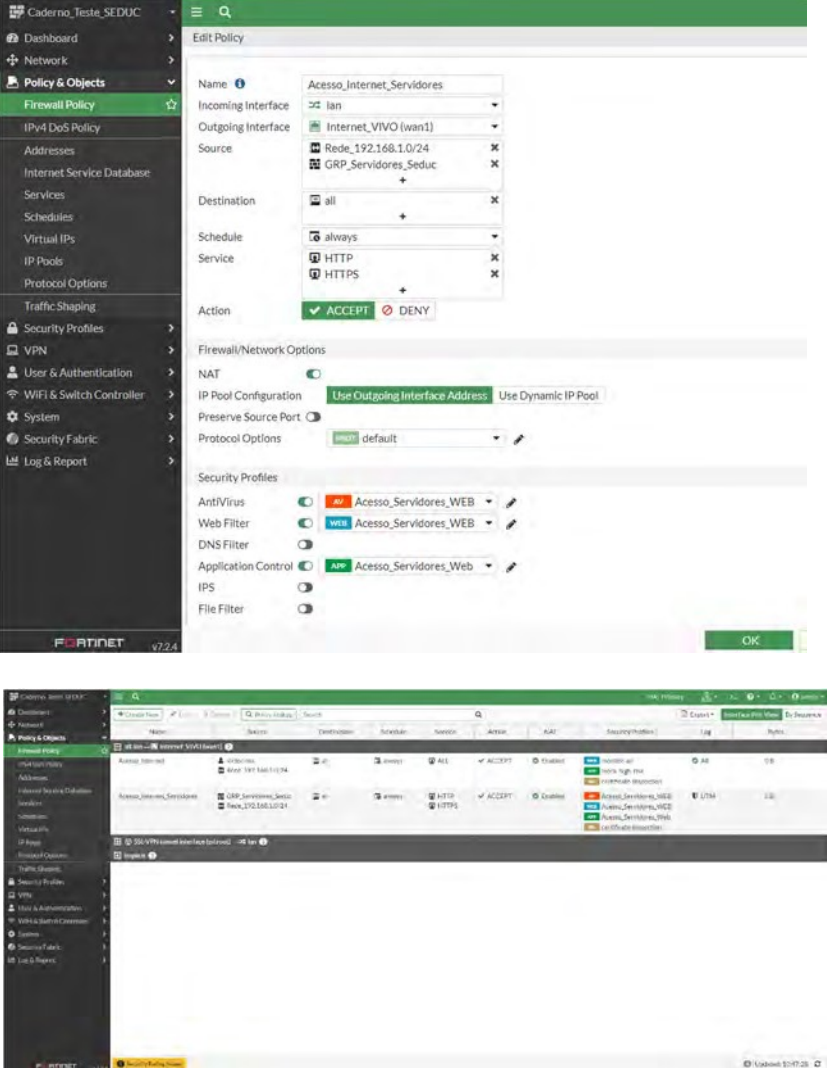
1 - Integração com AD via LDAP



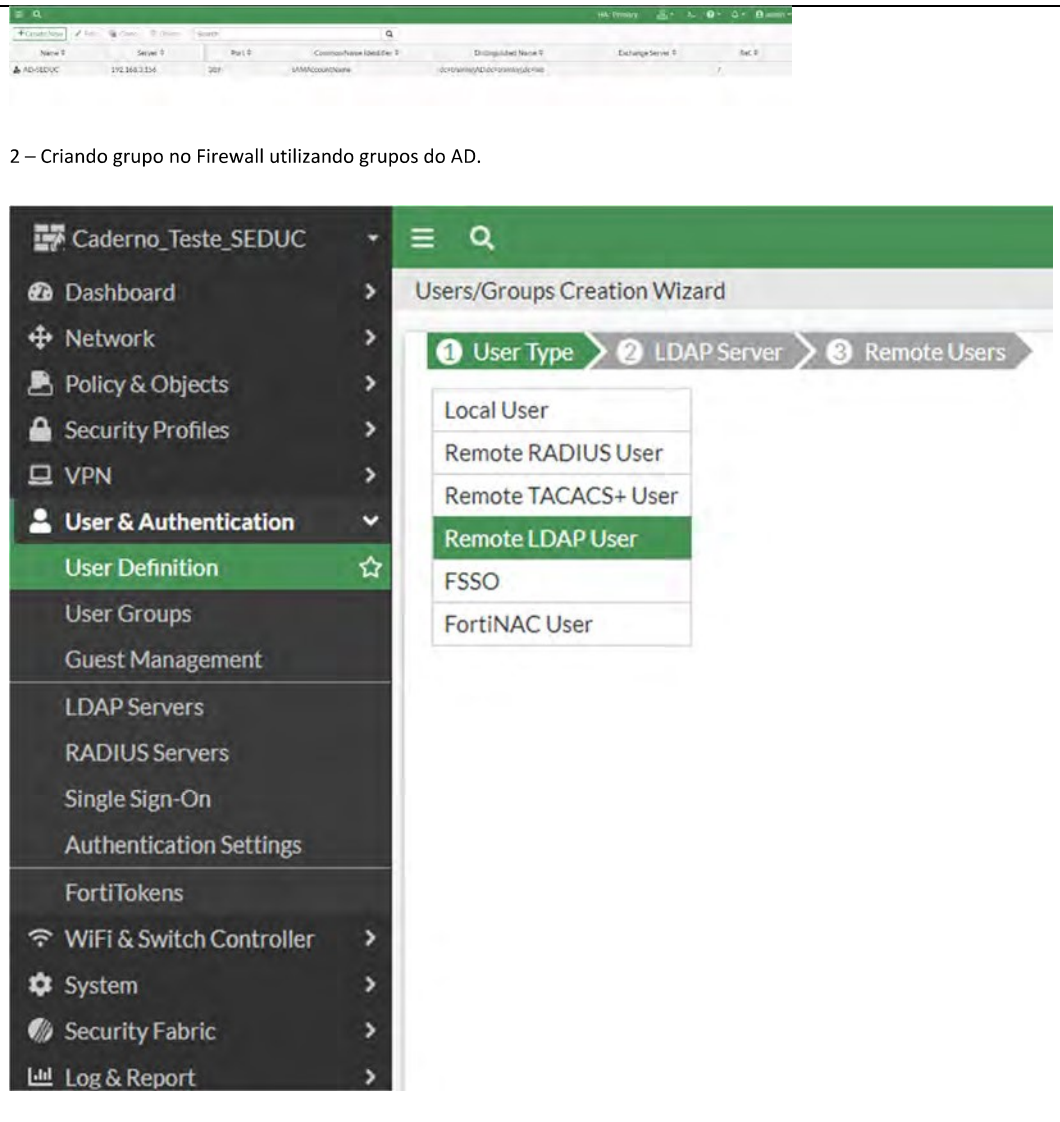
2 - Criação de um novo grupo no Firewall que utilizando a integração com o AD.



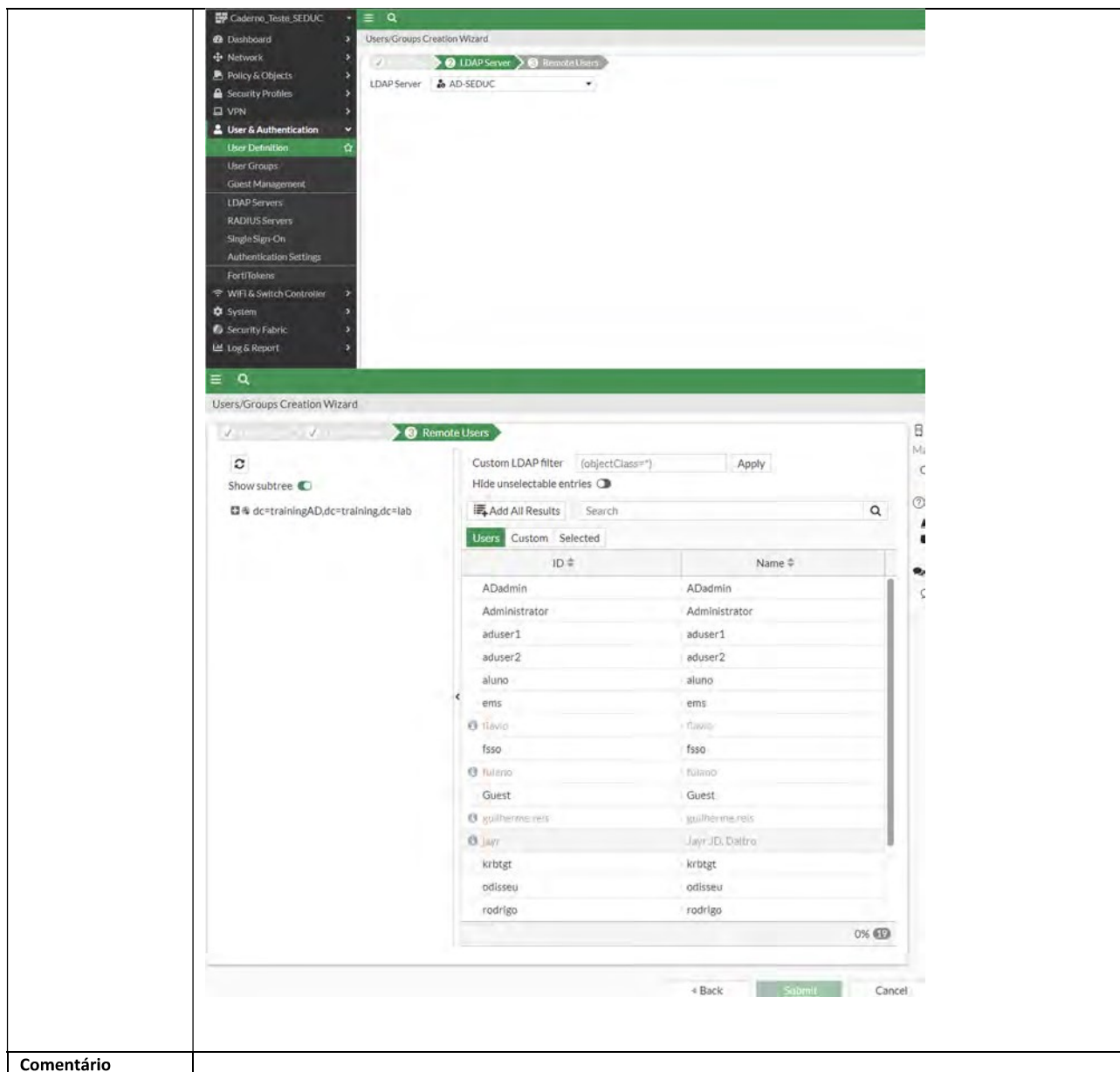
3 – Navegando por Policy & Objects > Firewall Policy é possível realizar a criação de regras utilizando como origem o grupo criado com a integração do AD

	 <table border="1" data-bbox="247 996 1077 1176"> <thead> <tr> <th>Name</th> <th>Outgoing Interface</th> <th>Source</th> <th>Destination</th> <th>Schedule</th> <th>Service</th> <th>Action</th> <th>Security Profiles</th> <th>Log</th> <th>Rules</th> </tr> </thead> <tbody> <tr> <td>Acesso_Internet_Servidores</td> <td>Internet_VIVO (wan1)</td> <td>Rede_192.168.1.0/24</td> <td>all</td> <td>always</td> <td>HTTP, HTTPS</td> <td>ACCEPT</td> <td>AV: Acesso_Servidores_WEB, WEB: Acesso_Servidores_WEB, AMP: Acesso_Servidores_Web</td> <td></td> <td>1/0</td> </tr> </tbody> </table>	Name	Outgoing Interface	Source	Destination	Schedule	Service	Action	Security Profiles	Log	Rules	Acesso_Internet_Servidores	Internet_VIVO (wan1)	Rede_192.168.1.0/24	all	always	HTTP, HTTPS	ACCEPT	AV: Acesso_Servidores_WEB, WEB: Acesso_Servidores_WEB, AMP: Acesso_Servidores_Web		1/0
Name	Outgoing Interface	Source	Destination	Schedule	Service	Action	Security Profiles	Log	Rules												
Acesso_Internet_Servidores	Internet_VIVO (wan1)	Rede_192.168.1.0/24	all	always	HTTP, HTTPS	ACCEPT	AV: Acesso_Servidores_WEB, WEB: Acesso_Servidores_WEB, AMP: Acesso_Servidores_Web		1/0												
Comentário																					

Item de Teste - 5.3.6.3	A identificação do usuário registrado no Microsoft Active Directory deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;
Objetivo do Teste	Validar se a identificação do usuário registrado no Microsoft Active Directory ocorre sem a necessidade de instalar um agente nos controladores de domínio e nas estações dos usuários
Configuração do Teste	
Procedimento do Teste	<p>Demonstrar integração via WMI sem instalação de agente no cliente e no servidor AD.</p> <p>Para realizar a integração dos serviços do Active Directory com o FortiGate, basta navegar por User and Authentication > LDAP Servers > Create New.</p> <p>A integração não necessita da instalação de nenhum software no Active Directory e nem nas estações dos usuários.</p>



The screenshot shows the FortiNAC web interface. At the top, there is a table with columns: Name, Serial, Port, Common Name Used For, Disconnected Name, Exchange Server, and Port. Below the table, the text "2 – Criando grupo no Firewall utilizando grupos do AD." is displayed. The main interface shows a sidebar menu on the left with "User & Authentication" selected, and a "Users/Groups Creation Wizard" panel on the right. The wizard has three steps: "1 User Type", "2 LDAP Server", and "3 Remote Users". A dropdown menu is open under "1 User Type", listing options: Local User, Remote RADIUS User, Remote TACACS+ User, Remote LDAP User (highlighted), FSSO, and FortiNAC User.



The screenshot shows the Fortinet User & Authentication configuration page. The left sidebar contains a navigation menu with options like Dashboard, Network, Policy & Objects, Security Profiles, VPN, User & Authentication, and System. The main content area is titled 'Users/Groups Creation Wizard' and is currently on the 'Remote Users' step. It displays a table of LDAP entries with columns for ID and Name. The table lists various users such as ADAdmin, Administrator, aduser1, aduser2, aluno, emis, flávio, fsso, fulano, Guest, guilherme.reis, jayr, krbtgt, odisseu, and rodrigo. At the bottom of the interface, there are 'Back', 'Submit', and 'Cancel' buttons.

Comentário

5.3.7 SISTEMA DE PREVENÇÃO DE INTRUSÃO - IPS:

Item de Teste - 5.3.7.1	Deve possuir módulo de IPS integrado no próprio appliance, sem a necessidade de uso de quaisquer interfaces externas, para proteção do ambiente contra-ataques, onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança;
Objetivo do Teste	Verificar se a appliance possui módulo IPS integrado sem a necessidade de uso de quaisquer interfaces externas.
Configuração do Teste	Demonstrar configuração de IPS.
Procedimento do Teste	Demonstrar configuração de IPS.

New Policy

Name:

Incoming Interface:

Outgoing Interface:

Source:

Destination:

Schedule:

Service:

Action: ACCEPT DENY

Firewall/Network Options

NAT:

IP Pool Configuration: Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port:

Protocol Options:

Security Profiles

AntiVirus:

Web Filter:

DNS Filter:

Application Control:

IPS:

File Filter:

E dentro desse perfil de segurança podemos ter acesso a todas as assinaturas que ele conhece, como também o CVE daquela vulnerabilidade, a ação padrão e por fim o grau de severidade dela.

Edit IP Add Signatures

Type: Filter Signature

Action: Default

Packet logging: Enable Disable

Status: Enable Disable Default

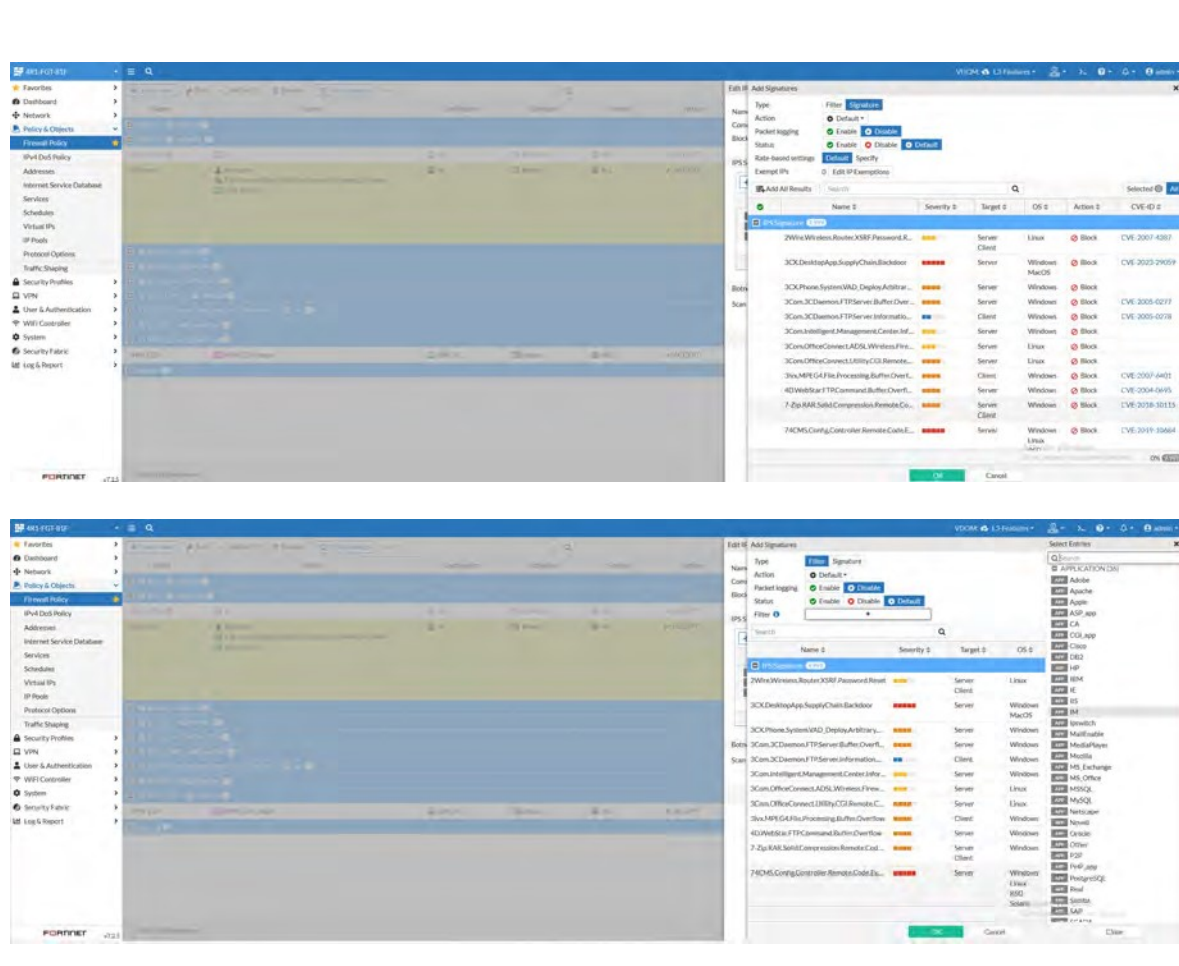
Filter:

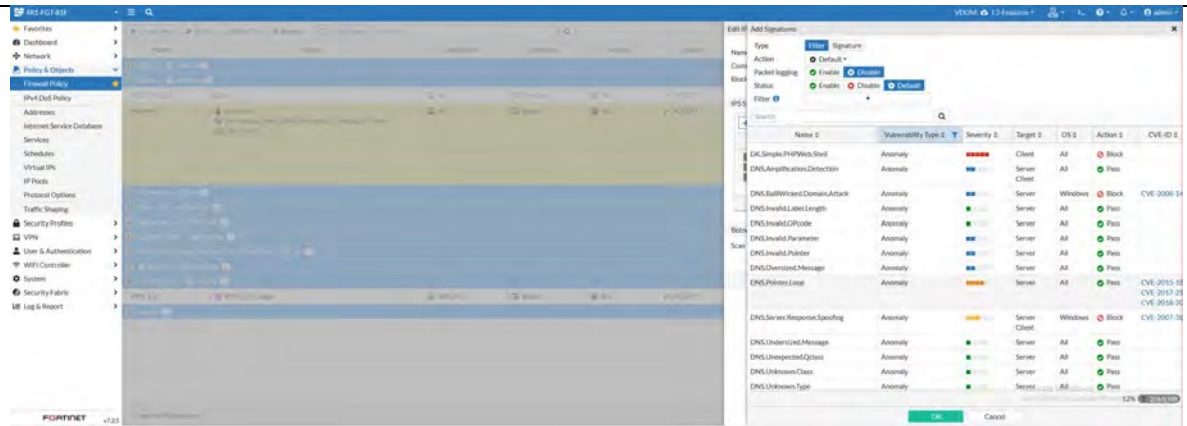
Name	Severity	Target	OS	Action	CVE-ID
3Com.3CDaemon.FTP.Server.Buffer.Over...	High	Server	Windows	Block	CVE-2005-0277
3Com.Intelligent.Management.Center.Info...	High	Server	Windows	Block	
3Com.OfficeConnect.ADSL.Wireless.Fire...	High	Server	Linux	Block	
3S.Pocknet.VMS.ActiveX.Control.Buffer.O...	High	Client	Windows	Block	CVE-2014-9263
3ivx.MPEG4.File.Processing.Buffer.Overf...	High	Client	Windows	Block	CVE-2007-6401
427BB.Cookie.Based.Authentication.Bypass	High	Server	Other	Block	CVE-2006-0153
427BB.Showthread.PHP.ForumID.Parame...	High	Server	Other	Block	CVE-2006-0154
A32S.Botnet	High	Server/Client	All	Block	
AAEH.Botnet	High	Server	All	Block	

0% 5,655

OK Cancel

Comentário

Item de Teste - 5.3.7.2	A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas, anomalias de protocolos, controle de aplicações;
Objetivo do Teste	Validar se a solução de IPS possui os seguintes mecanismos de detecção: assinaturas, anomalias de protocolos, controle de aplicações.
Configuração do Teste	Demonstrar na configuração de regra NGFW de IPS contendo: assinaturas, anomalias de protocolos, controle de aplicações;
Procedimento do Teste	Demonstrar na configuração de regra NGFW de IPS contendo: assinaturas, anomalias de protocolos, controle de aplicações;
Evidências	



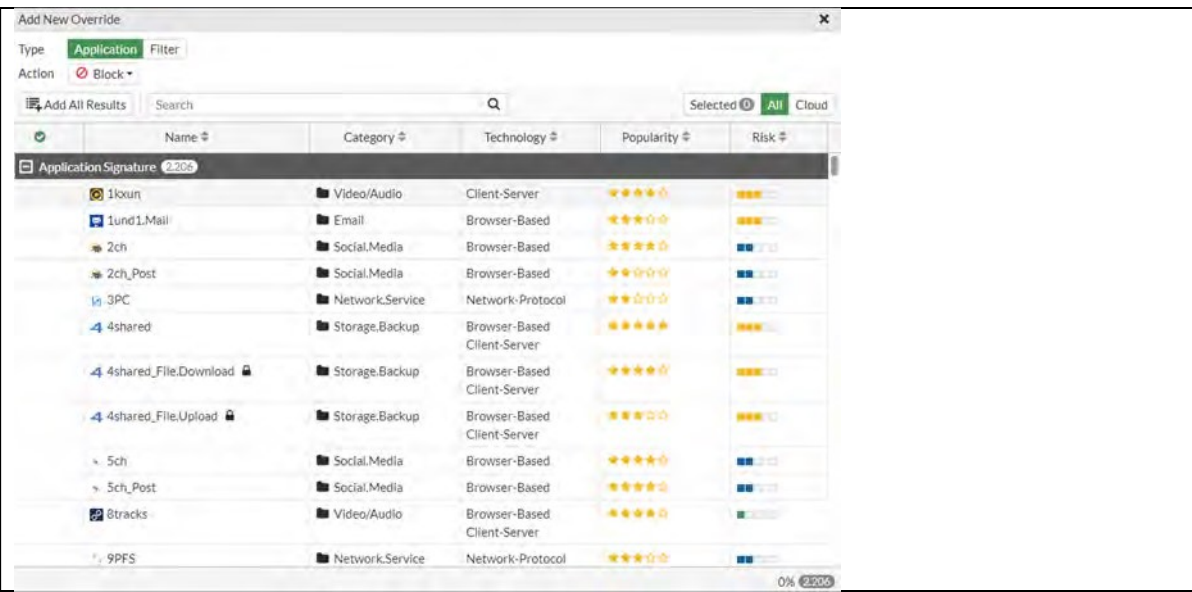
TESTE OK

Nessa parte podemos ter visibilidade de todas as assinaturas que o filtro IPS possui naquele momento, sendo possível adicionar assinaturas novas sem contar as que são adicionadas frequentemente pelo FortiGuard.



Vale ressaltar que a solução de IPS já faz uma decodificação de protocolo, ou seja, ela já faz a validação de anomalia de protocolo, caso este esteja com algum problema, ele é então descartado.

Já o mecanismo de controle de aplicação é feito pelo Application Control.

	
<p>Comentário</p>	<p>Fonte: “How does the IPS engine determine if a packet contains an attack or anomaly” acessado em: https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-does-the-IPS-engine-determine-if-a-packet/ta-p/199692</p>

<p>Item de Teste - 5.3.7.3</p>	<p>O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;</p>
<p>Objetivo do Teste</p>	<p>Verificar se a ferramenta recebe e implementa em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance.</p>
<p>Configuração do Teste</p>	<p>Demonstrar tela de atualização de funcionalidades</p>
<p>Procedimento do Teste</p>	<p>Demonstrar tela de atualização de funcionalidades</p>
<p>Evidências</p>	

4R1-FGT-81F
☰
🔍

- Dashboard >
- Network >
- Security Profiles >
- WiFi Controller >
- System** >
- VDOM
- Global Resources
- Administrators
- Admin Profiles
- Fabric Management
- Settings
- HA
- SNMP
- Replacement Messages
- FortiGuard** ☆
- Feature Visibility
- Security Fabric >
- Log & Report >

FortiGuard Distribution Network

- Antivirus
✔ Licensed (Expiration Date: 2024/03/30)
- Web Filtering
✔ Licensed (Expiration Date: 2024/03/30)
- Outbreak Prevention
✔ Licensed (Expiration Date: 2024/03/30)
- SD-WAN Network Monitor
⚠ Not Licensed
- Security Rating
⚠ Not Licensed
- Industrial DB
⚠ Not Licensed
- IoT Detection Service
⚠ Not Licensed
- FortiGate Cloud
⚠ Not Activated
- Virtual Domain

30%
3 / 10

FortiCare support contracts can be activated here and applied directly to this FortiGate.

FortiGuard Updates

Scheduled updates Every Daily Weekly Automatic

Improve IPS quality

Use extended IPS signature package

Update server location Lowest latency locations Restrict to

Filtering

Override FortiGuard Servers

TESTE OK

FortiGuard Updates

Scheduled updates Every Daily Weekly Automatic

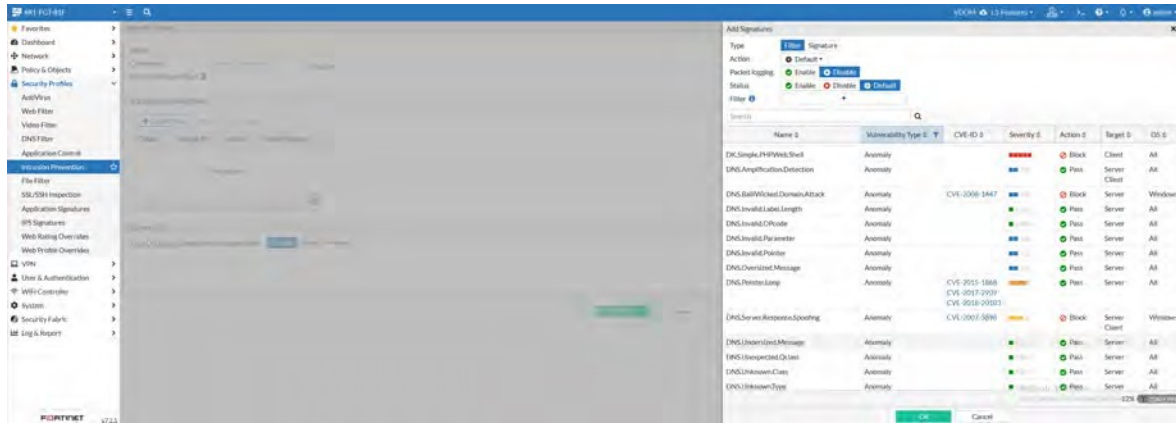
Improve IPS quality

Use extended IPS signature package

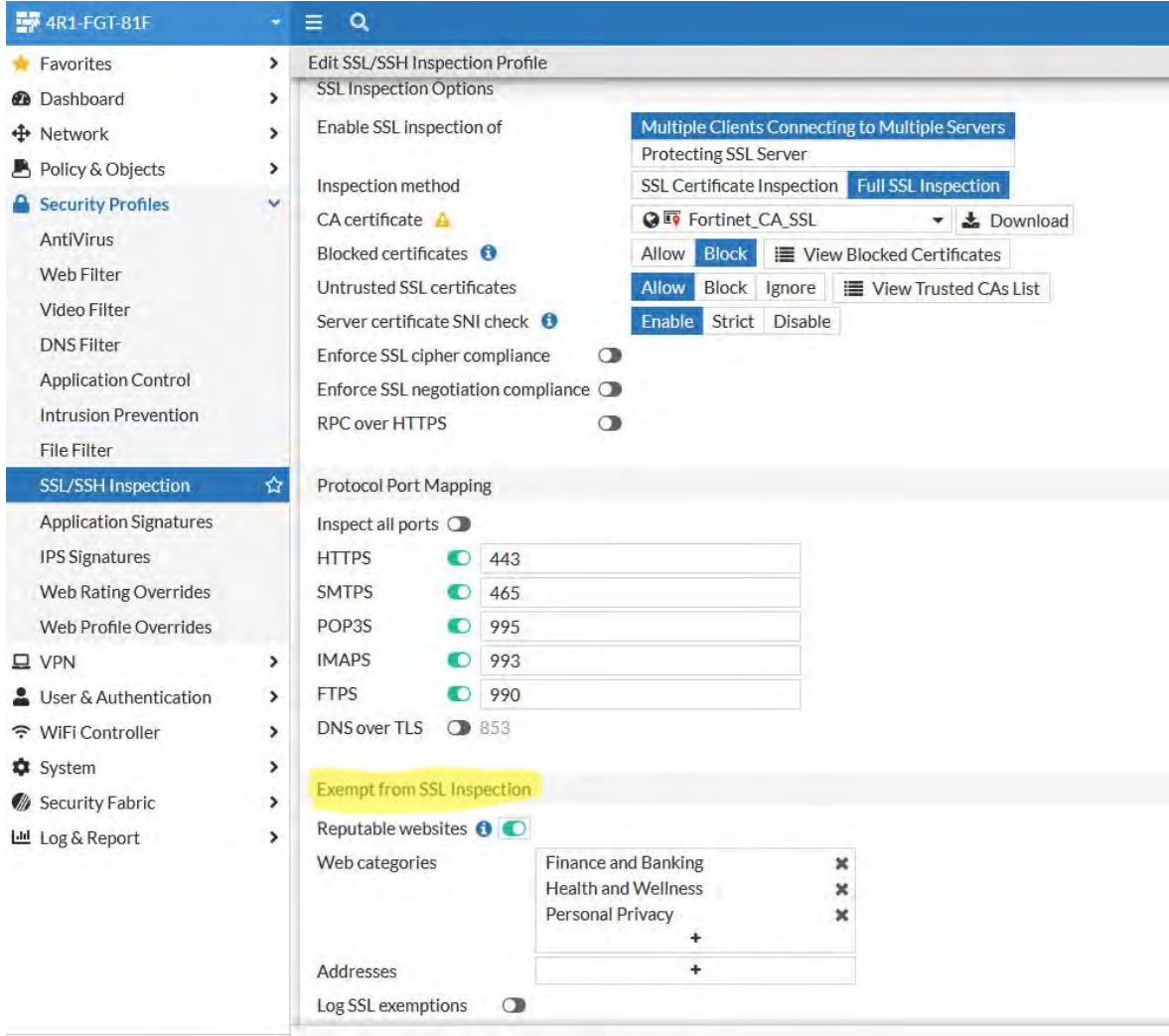
AntiVirus PUP/PUA

Update server location Lowest latency locations Restrict to

Comentário

Item de Teste - 5.3.7.4	Possuir proteções de segurança, informações como: código CVE, severidade, e tipo de ação que a mesma irá executar;																																																																		
Objetivo do Teste	Verificar se o sistema de proteção de segurança possui as informações de código CVE, severidade, e tipo de ação que a mesma irá executar;																																																																		
Configuração do Teste	Demonstrar lista de assinaturas e suas características																																																																		
Procedimento do Teste	Demonstrar lista de assinaturas e suas características																																																																		
Evidências	<div data-bbox="239 582 1420 1008" data-label="Image">  </div> <p data-bbox="239 1030 319 1064">TESTE OK</p> <p data-bbox="239 1209 1420 1254">Podemos ver na imagem abaixo retirada de um perfil de IPS do FortiGate, que ele apresenta as seguintes informações:</p> <p data-bbox="239 1276 1420 1321">Grau de Severidade, Ação a ser tomada e como também o código CVE daquela vulnerabilidade.</p> <table border="1" data-bbox="239 1344 1069 1635"> <thead> <tr> <th>Nome</th> <th>Severidade</th> <th>Ação</th> <th>Alvo</th> <th>OS</th> <th>CVE-ID</th> </tr> </thead> <tbody> <tr> <td>3Com.3CDaemon.FTP.Server.Buffer.Over...</td> <td>Alta</td> <td>Block</td> <td>Server</td> <td>Windows</td> <td>CVE-2005-0277</td> </tr> <tr> <td>3Com.3CDaemon.FTP.Server.Information...</td> <td>Alta</td> <td>Pass</td> <td>Client</td> <td>Windows</td> <td>CVE-2005-0278</td> </tr> <tr> <td>3Com.Intelligent.Management.Center.Info...</td> <td>Alta</td> <td>Block</td> <td>Server</td> <td>Windows</td> <td></td> </tr> <tr> <td>3Com.OfficeConnect.ADSL.Wireless.Fire...</td> <td>Alta</td> <td>Block</td> <td>Server</td> <td>Linux</td> <td></td> </tr> <tr> <td>3S.Pocknet.VMS.ActiveX.Control.Buffer.O...</td> <td>Alta</td> <td>Block</td> <td>Client</td> <td>Windows</td> <td>CVE-2014-9263</td> </tr> <tr> <td>3ivx.MPEG4.File.Processing.Buffer.Overfl...</td> <td>Alta</td> <td>Block</td> <td>Client</td> <td>Windows</td> <td>CVE-2007-6401</td> </tr> <tr> <td>427BB.Cookie.Based.Authentication.Bypass</td> <td>Alta</td> <td>Block</td> <td>Server</td> <td>Other</td> <td>CVE-2006-0153</td> </tr> <tr> <td>427BB.Showthread.PHP.ForumID.Parame...</td> <td>Alta</td> <td>Block</td> <td>Server</td> <td>Other</td> <td>CVE-2006-0154</td> </tr> <tr> <td>A32S.Botnet</td> <td>Alta</td> <td>Block</td> <td>Server</td> <td>All</td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td>Client</td> <td></td> <td></td> </tr> </tbody> </table>	Nome	Severidade	Ação	Alvo	OS	CVE-ID	3Com.3CDaemon.FTP.Server.Buffer.Over...	Alta	Block	Server	Windows	CVE-2005-0277	3Com.3CDaemon.FTP.Server.Information...	Alta	Pass	Client	Windows	CVE-2005-0278	3Com.Intelligent.Management.Center.Info...	Alta	Block	Server	Windows		3Com.OfficeConnect.ADSL.Wireless.Fire...	Alta	Block	Server	Linux		3S.Pocknet.VMS.ActiveX.Control.Buffer.O...	Alta	Block	Client	Windows	CVE-2014-9263	3ivx.MPEG4.File.Processing.Buffer.Overfl...	Alta	Block	Client	Windows	CVE-2007-6401	427BB.Cookie.Based.Authentication.Bypass	Alta	Block	Server	Other	CVE-2006-0153	427BB.Showthread.PHP.ForumID.Parame...	Alta	Block	Server	Other	CVE-2006-0154	A32S.Botnet	Alta	Block	Server	All					Client		
Nome	Severidade	Ação	Alvo	OS	CVE-ID																																																														
3Com.3CDaemon.FTP.Server.Buffer.Over...	Alta	Block	Server	Windows	CVE-2005-0277																																																														
3Com.3CDaemon.FTP.Server.Information...	Alta	Pass	Client	Windows	CVE-2005-0278																																																														
3Com.Intelligent.Management.Center.Info...	Alta	Block	Server	Windows																																																															
3Com.OfficeConnect.ADSL.Wireless.Fire...	Alta	Block	Server	Linux																																																															
3S.Pocknet.VMS.ActiveX.Control.Buffer.O...	Alta	Block	Client	Windows	CVE-2014-9263																																																														
3ivx.MPEG4.File.Processing.Buffer.Overfl...	Alta	Block	Client	Windows	CVE-2007-6401																																																														
427BB.Cookie.Based.Authentication.Bypass	Alta	Block	Server	Other	CVE-2006-0153																																																														
427BB.Showthread.PHP.ForumID.Parame...	Alta	Block	Server	Other	CVE-2006-0154																																																														
A32S.Botnet	Alta	Block	Server	All																																																															
			Client																																																																
Comentário																																																																			

Item de Teste - 5.3.7.18	A solução deve possuir inspeção de tráfego HTTPS sendo possível criar bypass para sites evitando qualquer tipo de quebra de sigilo de informações pessoais;
Objetivo do Teste	Verificar se a solução possui uma forma de dar bypass na inspeção de tráfego HTTPS.

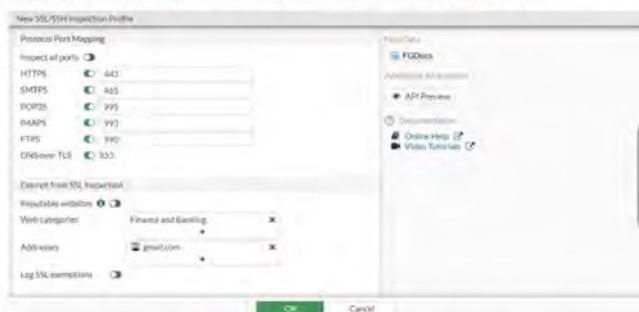
Configuração do Teste	Demonstrar by-pass de https
Procedimento do Teste	Demonstrar by-pass de https
Evidências	 <p>TESTE OK</p>

Exempt web sites from deep inspection

If you do not want to apply deep inspection for privacy or other reasons, you can exempt the session by address, category, or allowlist.

If you know the address of the server you want to exempt, you can exempt that address. You can exempt specific address type including IP address, IP address range, IP subnet, FQDN, wildcard-FQDN, and geography.

If you want to exempt all bank web sites, an easy way is to exempt the *Finance and Banking* category, which includes all finance and bank web sites identified in FortiGuard. For information about creating and using custom local and remote categories, see *Web rating override* on page 1419 and *Threat feeds* on page 2693.



If you want to exempt commonly trusted web sites, you can bypass the SSL allowlist in the SSL/SSH profile by enabling *Reputable websites*. The allowlist includes common web sites trusted by FortiGuard.

Há uma funcionalidade no perfil de SSL Inspection chamada de “Exempt from SSL Inspection” que faz esse bypass. Basta colocar os endereços dos sites desejados ou então por categoria, como Finanças e Bancário.

Exempt from SSL Inspection

Reputable websites 📘

Web categories 🗑️

Finance and Banking 🗑️

Health and Wellness 🗑️

Personal Privacy 🗑️

+

Addresses +

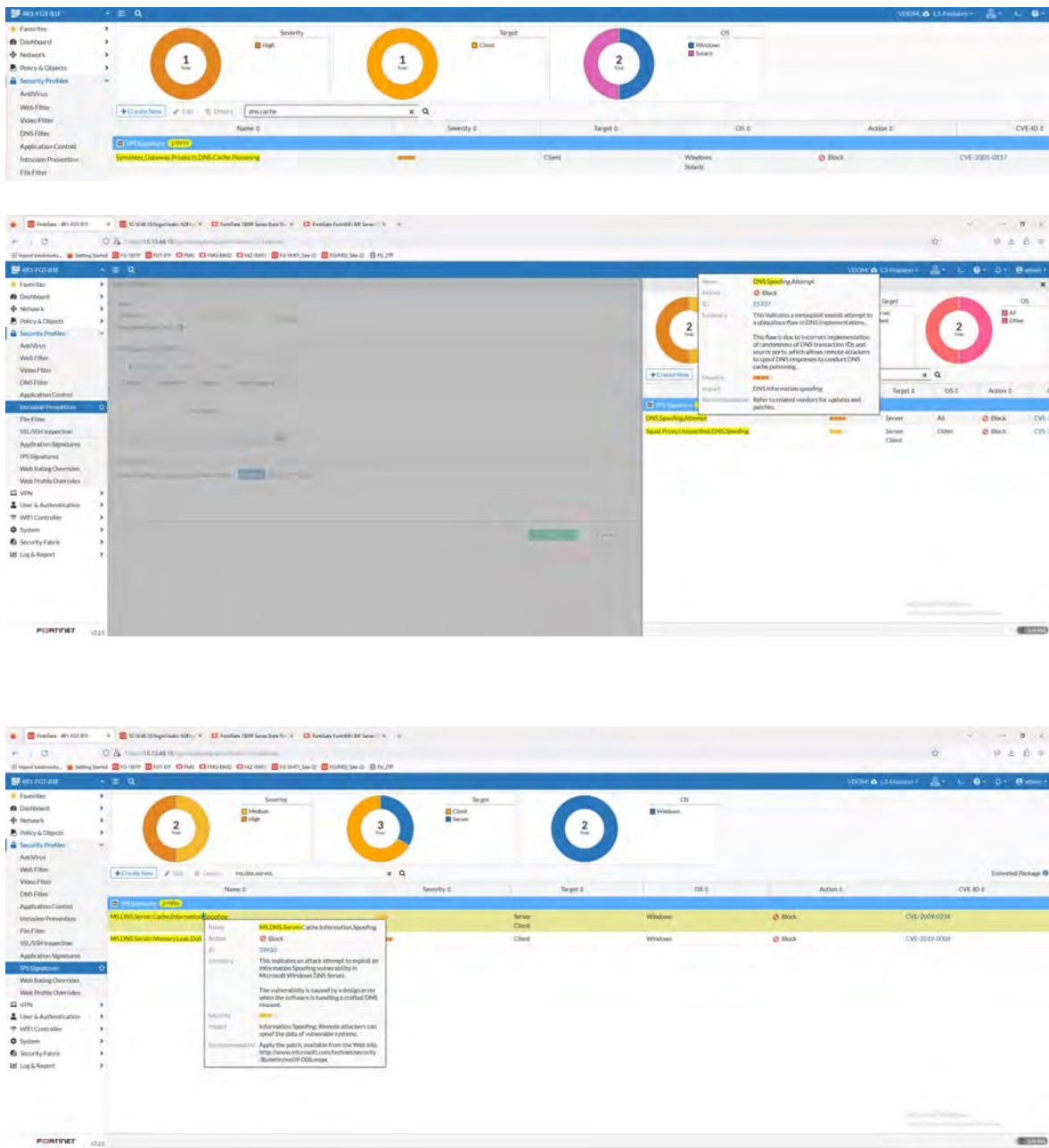
Log SSL exemptions

SSH Inspection Options

SSH deep scan

Comentário	<p>Fonte: FortiOS Administration 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</p>
-------------------	--

Item de Teste - 5.3.7.22	A solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning), e impedir que os usuários acessem endereços de domínios bloqueados ou maliciosos;
Objetivo do Teste	Verificar se a solução protege contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning), e impedir que os usuários acessem endereços de domínios bloqueados ou maliciosos.

<p>Configuração do Teste</p>	<p>Demonstrar assinatura DNS.Server.Cache.Poisoning</p>
<p>Procedimento do Teste</p>	<p>Demonstrar assinatura DNS.Server.Cache.Poisoning</p>
<p>Evidências</p>	 <p>The evidence consists of three screenshots from the Fortinet FortiGate security gateway interface, demonstrating the detection of DNS poisoning attacks. The top screenshot shows a search for 'dns.cache' resulting in one detected rule. The middle screenshot shows a detailed view of a 'DNS Spoofing Attempt' rule with a severity of High and a description of the attack. The bottom screenshot shows a search for 'dns.poisoning' resulting in three detected rules, including 'MS DNS Server' and 'MS DNS Server Memory Leak DoS'.</p>

4R1-FGT-81F
☰
🔍

- ★ Favorites >
- 🏠 Dashboard >
- 🌐 Network >
- 📄 Policy & Objects >
- 🔒 Security Profiles >
- AntiVirus
- Web Filter
- Video Filter
- DNS Filter ☆
- Application Control
- Intrusion Prevention
- File Filter
- SSL/SSH Inspection
- Application Signatures
- IPS Signatures
- Web Rating Overrides
- Web Profile Overrides
- 🖥️ VPN >
- 👤 User & Authentication >
- 📶 WiFi Controller >
- ⚙️ System >
- 🌐 Security Fabric >
- 📊 Log & Report >

New DNS Filter Profile

Name

Comments 0/255

Redirect botnet C&C requests to Block Portal

Enforce 'Safe Search' on Google, Bing, YouTube

FortiGuard Category Based Filter

Pre-configured filters Custom G PG-13 R

Name	Action
Adult/Mature Content 15	👁️ 15
Alternative Beliefs	👁️ Monitor
Abortion	👁️ Monitor
Other Adult Materials	👁️ Monitor
Advocacy Organizations	👁️ Monitor
Gambling	👁️ Monitor
Nudity and Risque	👁️ Monitor
Pornography	👁️ Monitor
Dating	👁️ Monitor


Static Domain Filter

Domain Filter

External IP Block Lists

DNS Translation i

TESTE OK



Threat Encyclopedia

DNS.Server.Cache.Poisoning

Description

This indicates a possible DNS Cache Poisoning attack towards a DNS Server. The vulnerability is caused by insufficient validation of query response from other DNS servers. This could result in DNS spoofing or redirection to other websites.

Affected Products

DNS Server

Impact

Information Spoofing: Remote attackers can serve spoof contents to unsuspecting targets.

Dentro do perfil de IPS já existe a assinatura dessa vulnerabilidade especificada no CVE-2005-0817, que ele bloqueia por default.

Add Signatures x

Type: Filter Signature

Action: Default

Packet logging: Enable Disable

Status: Enable Disable Default

Filter: +

poisoning x Q

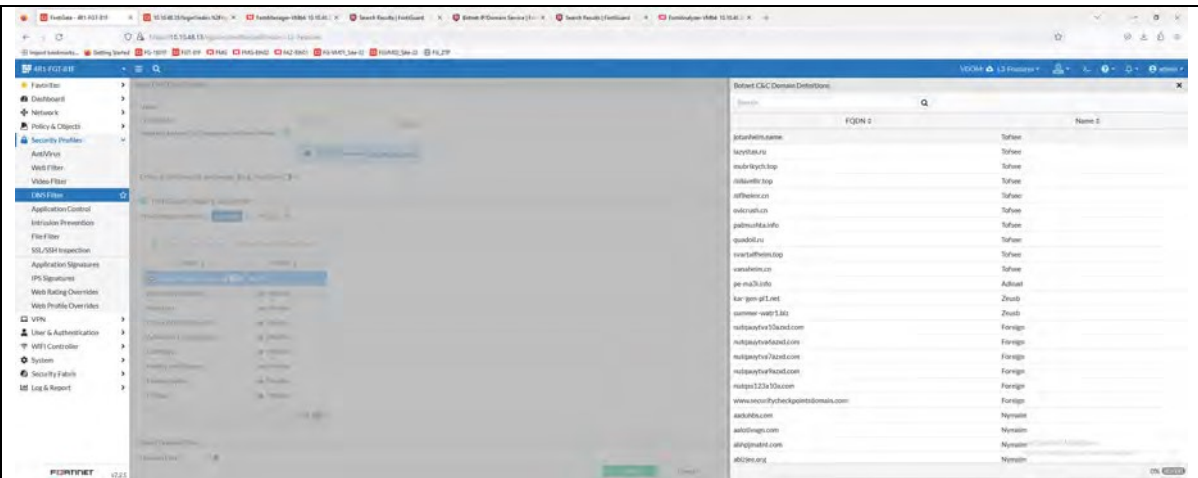
Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 1586					
Symantec.Gateway.Products.DNS.Cache.Poisoning	■■■■	Client	Windows Solaris	Block	CVE-2005-0817

Comentário Fonte: IPS Threat Encyclopedia acessado em <https://www.fortiguard.com/encyclopedia/ips/43827/dns-server-cache-poisoning>

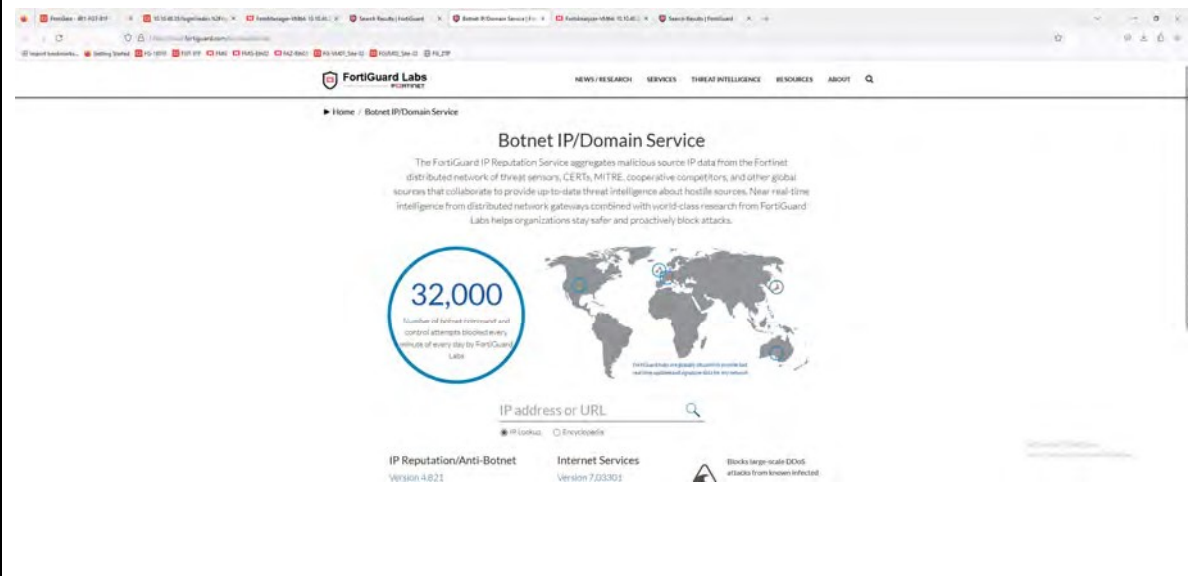
5.3.8 ANTI-MALWARE:

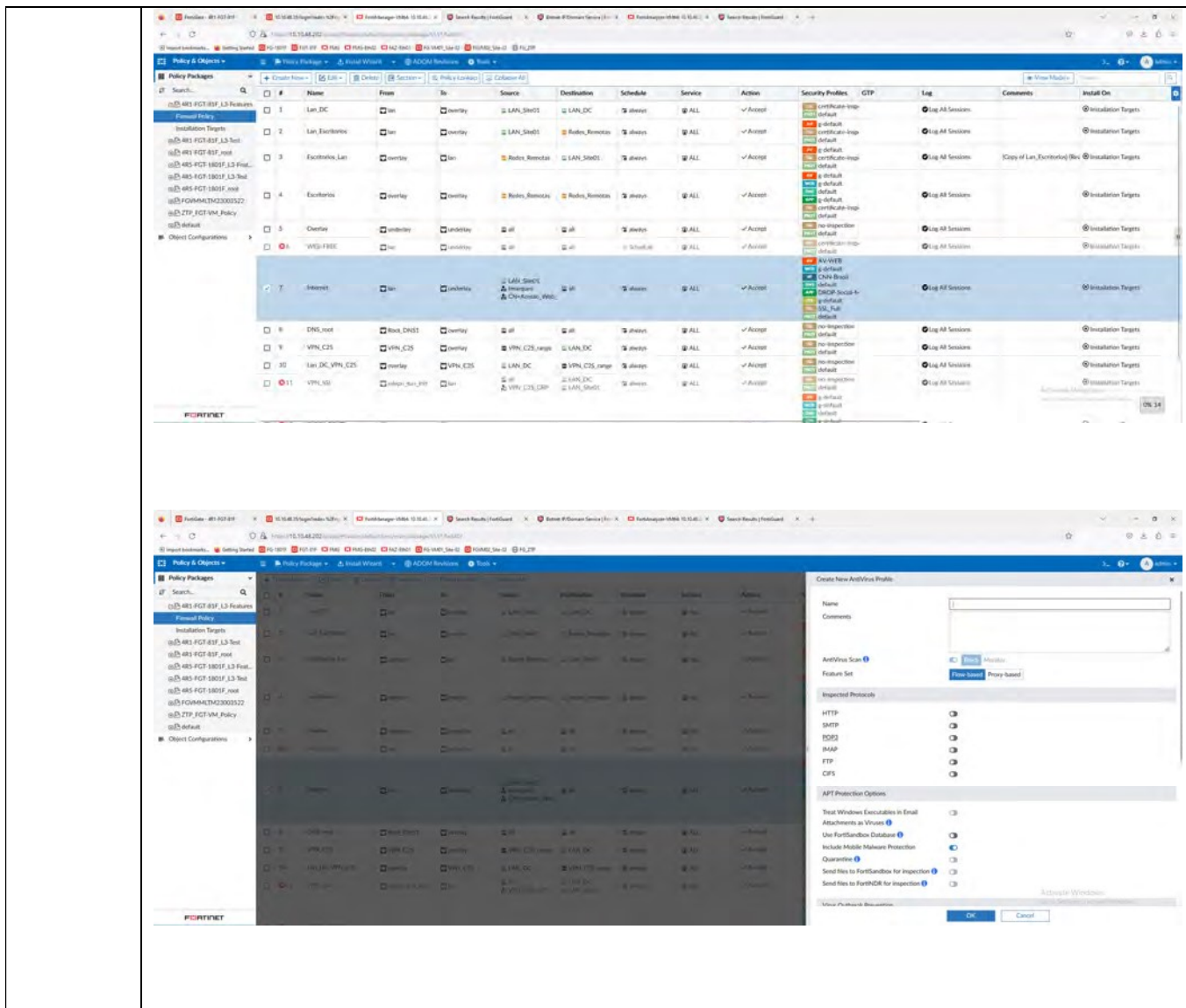
Item de Teste - 5.3.8.1	Possuir módulo de Antivírus, Antispyware e Antibot integrado no próprio appliance de segurança e integrado à gerência centralizada de administração, monitoração e logs;
Objetivo do Teste	Verificar se a solução possui módulo de Antivírus, Antispyware e Antibot integrado no próprio appliance de segurança e integrado à gerência centralizada de administração, monitoração e logs;
Configuração do Teste	Demonstrar regra com funcionalidades: Antivírus, Antispyware e Antibot
Procedimento do Teste	Demonstrar regra com funcionalidades: Antivírus, Antispyware e Antibot
Evidências	Na interface de gerenciamento, é possível configurar o perfil de Antivírus, responsável pela proteção contra vírus e malwares, bem como o perfil de IPS, que atua como uma medida Antibot e aplicá-los em qualquer política selecionada.

The image displays two screenshots from a computer screen. The top screenshot shows the FortiGuard Labs search results page for the keyword 'spyware'. It lists several malware entries, including 'W32/FakeAV_SpywareGuard.2!tr', 'MSIL/SpyWares.92D5!tr', 'W32/XPAntiSpyware.AF', and 'W32/SpywareX.F05A!tr'. The bottom screenshot shows the FortiGate configuration interface, specifically the 'Web Filter Profiles' section. A profile named 'Default' is selected, showing a list of categories with their respective actions. The 'FortiGuard Category Based Filter' is enabled, and a table lists categories such as 'Alternative Media', 'Alcoholism', 'Child Abuse', etc., with actions like 'Monitor' or 'Block'.



<https://www.fortiguard.com/services/botnet>

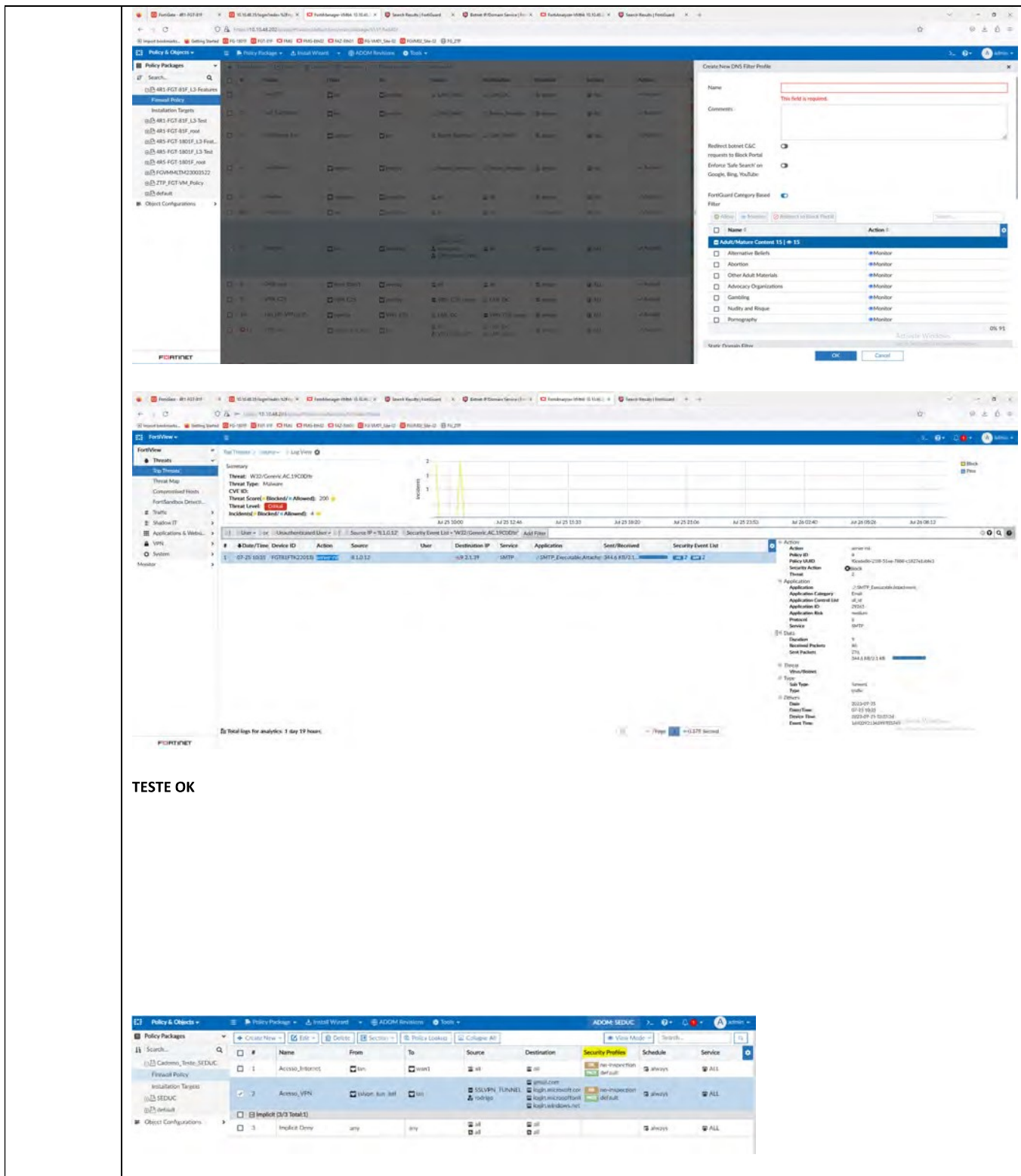




The image displays two screenshots of the Fortinet FortiGate configuration interface, specifically the Policy & Objects section.

The top screenshot shows a table of Policy Packages. The columns include: #, Name, From, To, Source, Destination, Schedule, Service, Action, Security Profiles, GTP, Log, Comments, and Install On. The table lists several policies, including LAN_DC, LAN_Escortado, Escortado_Lan, Escortado, Overlay, WEB-FREE, Internet, DNS_resolver, VPN_C2S, LAN_DC_VPN_C2S, and VPN_S0.

The bottom screenshot shows the 'Create New AntiVirus Profile' dialog box. It includes fields for Name and Comments. Under 'AntiVirus Scan', there are options for 'Flow-based' and 'Proxy-based'. The 'Inspected Protocols' section lists HTTP, SMTP, DDP2, RASP, FTP, and CIFS. The 'APT Protection Options' section includes checkboxes for 'Treat Windows Executables in Email Attachments as Viruses', 'Use FortiSandbox Database', 'Include Mobile Malware Protection', 'Quarantine', 'Send files to FortiSandbox for inspection', and 'Send files to FortiDR for inspection'. There are 'OK' and 'Cancel' buttons at the bottom.



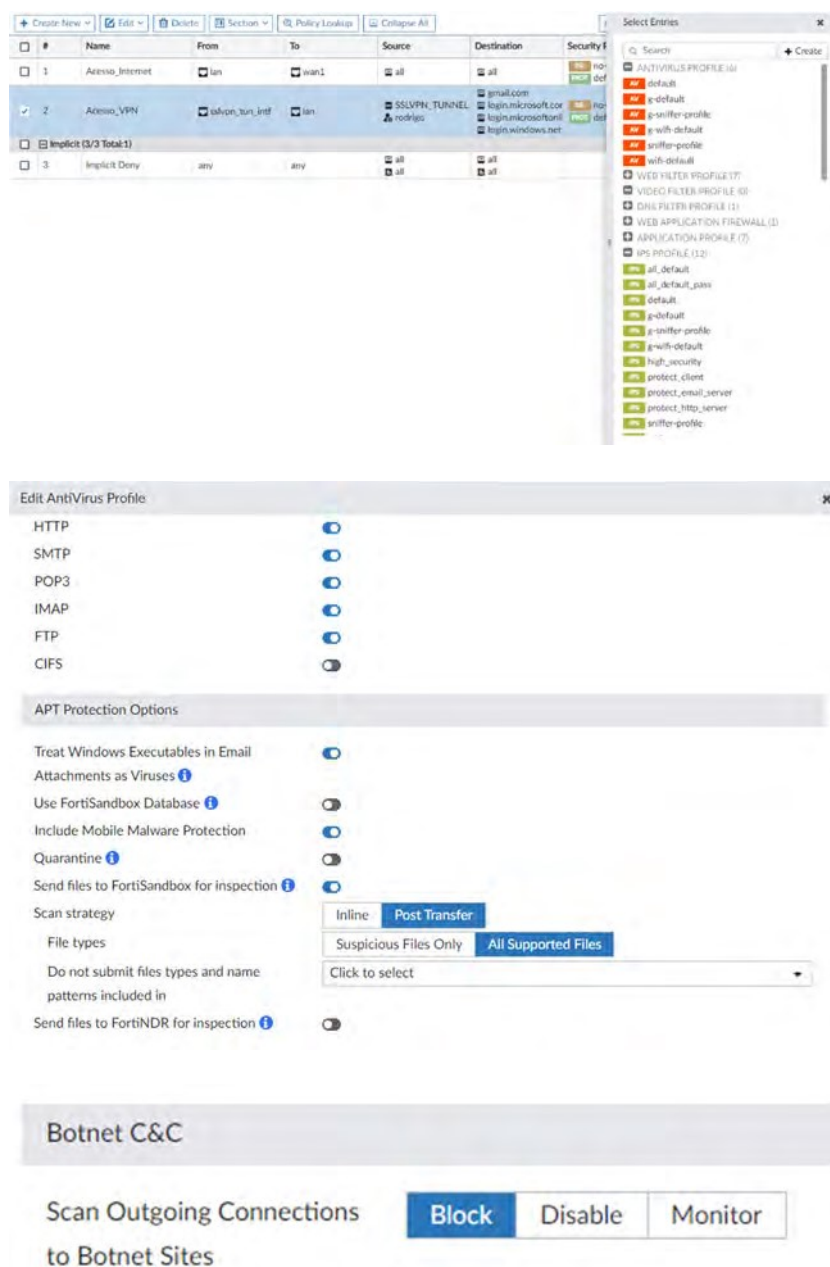
The screenshot displays the Fortinet Security Manager (SM) interface, divided into three main sections:

- Policy Packages:** A table listing various security policies. The table includes columns for Name, Status, and Action. A 'Create New DNS Filter Profile' dialog box is open on the right side of this section.
- Threats:** A section showing a threat analysis. It includes a 'Threat Map' and a 'Threat Details' panel. The threat is identified as 'W32/Generic.AC.190009' with a 'Threat Type' of 'Malware' and a 'Threat Score' of 'Blocked/Allowed: 200'. A 'Total logs for analysis: 1 day 19 hours' is noted at the bottom.
- Policy Objects:** A table listing network objects and their associated policies. The table has columns for Name, From, To, Source, Destination, Security Profile, Schedule, and Service.

TESTE OK

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

Para isso, basta ir na aba de de “Security Profiles” e lá estará os perfis de Antivírus e IPS.



#	Name	From	To	Source	Destination	Security
1	Acesso_Internet	lan	wan1	all	all	no-antivirus
2	Acesso_VPN	lan_vpn_tun1	lan	SSLVPN_TUNNEL	login.microsoft.com, login.microsoft.com, login.windows.net	no-antivirus
Implicit (3/3 Total-1)						
3	Implicit Deny	any	any	all	all	all

Edit AntiVirus Profile

HTTP
 SMTP
 POP3
 IMAP
 FTP
 CIFS

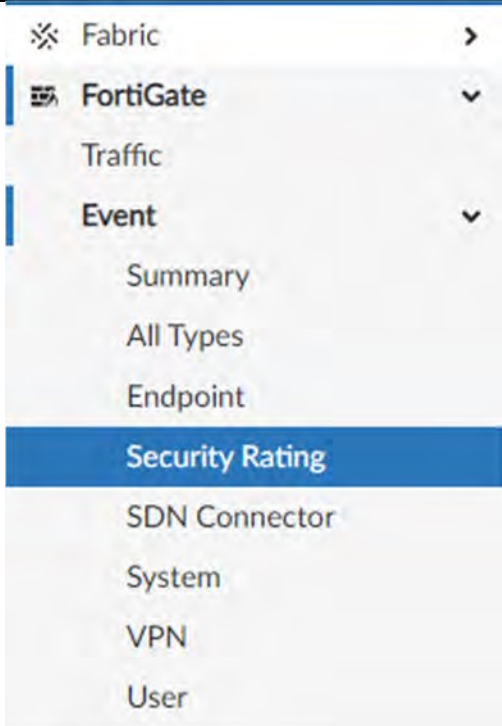
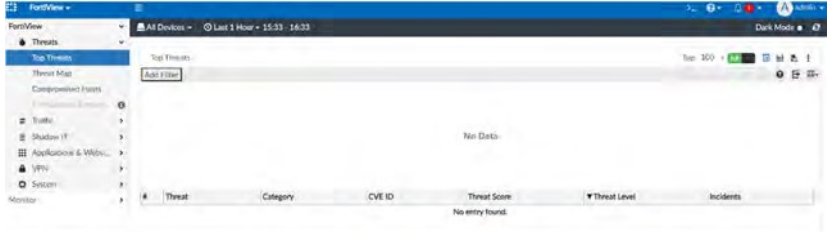
APT Protection Options

Treat Windows Executables in Email Attachments as Viruses
 Use FortiSandbox Database
 Include Mobile Malware Protection
 Quarantine
 Send files to FortiSandbox for inspection
 Scan strategy: **Post Transfer**
 File types: Suspicious Files Only, All Supported Files
 Do not submit files types and name patterns included in
 Send files to FortiNDR for inspection

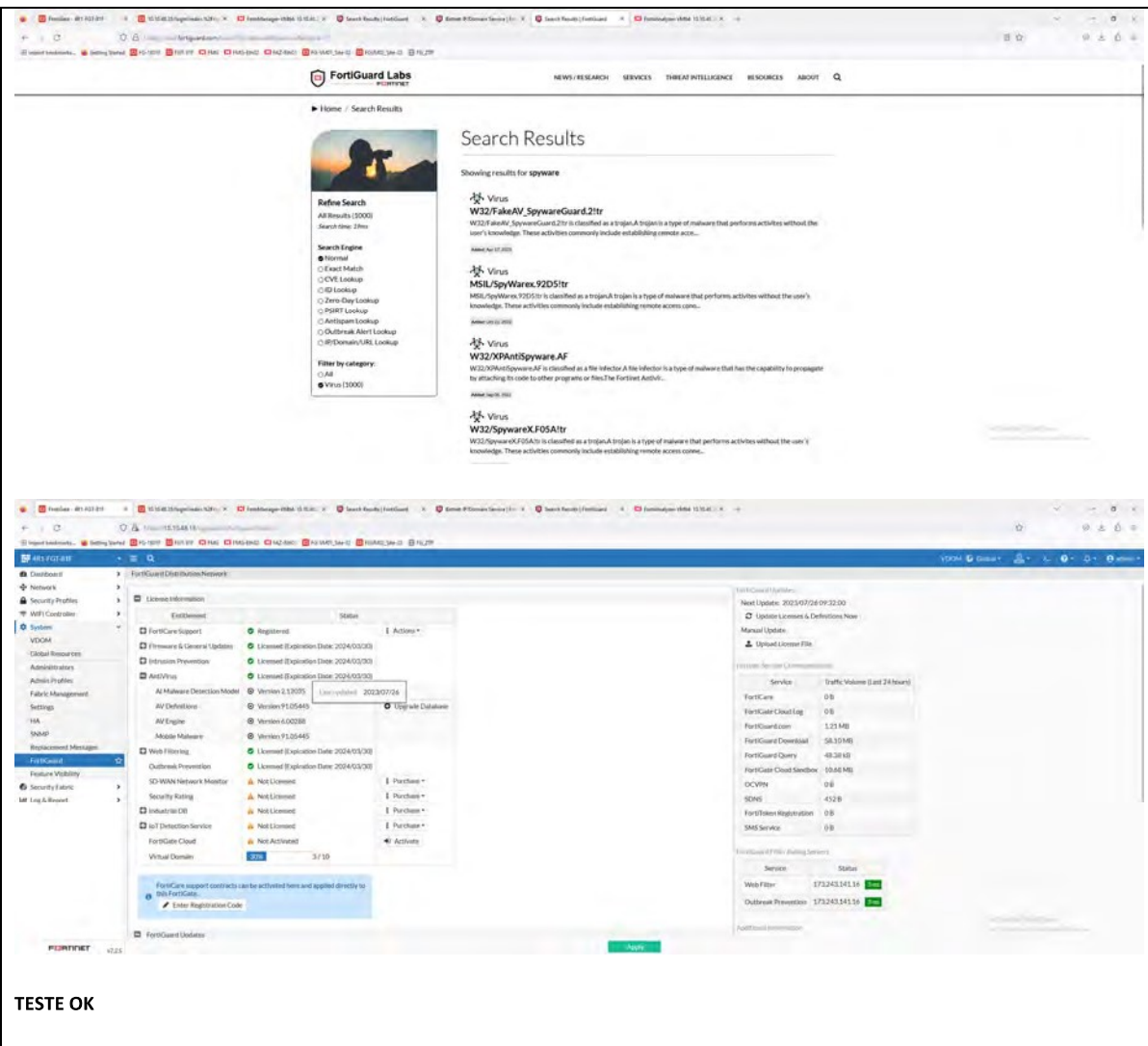
Botnet C&C

Scan Outgoing Connections to Botnet Sites: **Block** | Disable | Monitor

Na parte de logs podemos ver na seguinte forma:

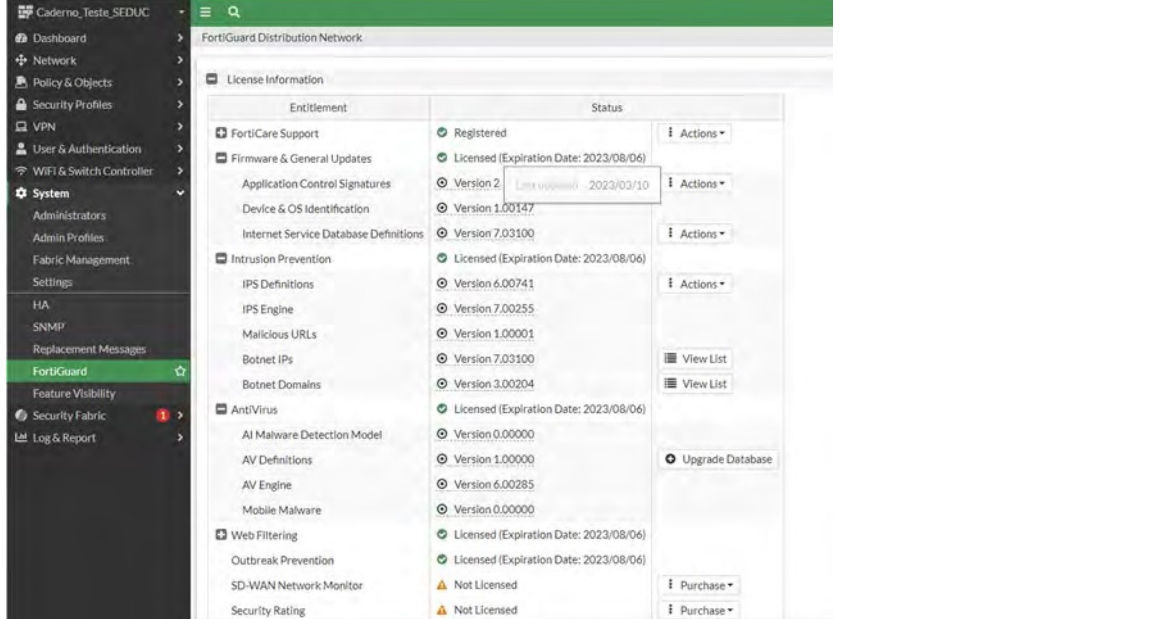
		
	<p>E na de monitoração:</p> 	
Comentário		

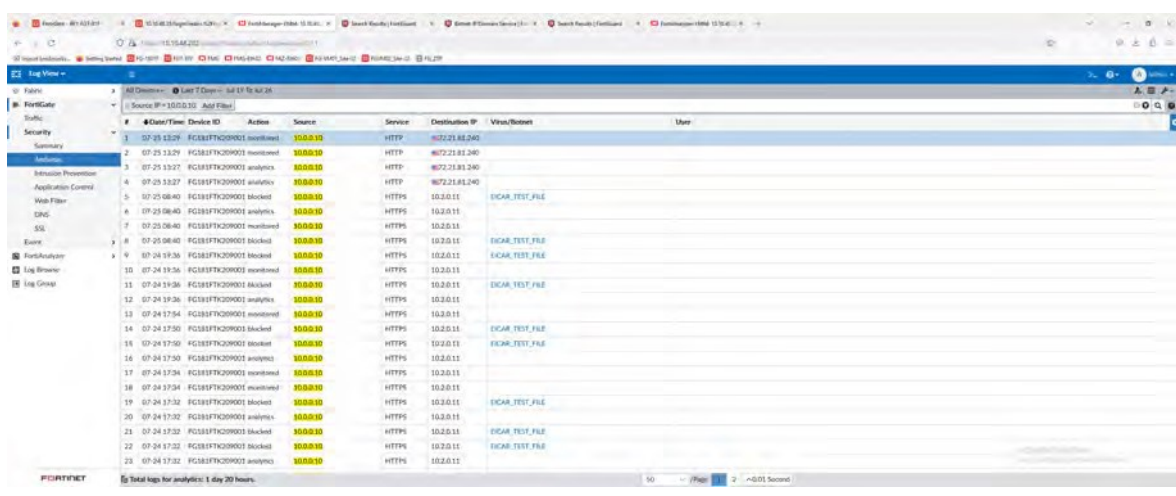
Item de Teste - 5.3.8.2	A solução deve possuir nuvem proprietária inteligente do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas;
Objetivo do Teste	Validar se a solução possui nuvem proprietária e inteligente do mesmo fabricante e se é possível atualizar toda a base de segurança dos appliances através de assinaturas
Configuração do Teste	Demonstrar o site da Nuvem de Inteligência
Procedimento do Teste	Para verificar o status das assinaturas e realizar a atualização das mesmas, basta navegar por System > FortiGuard .
Evidências	

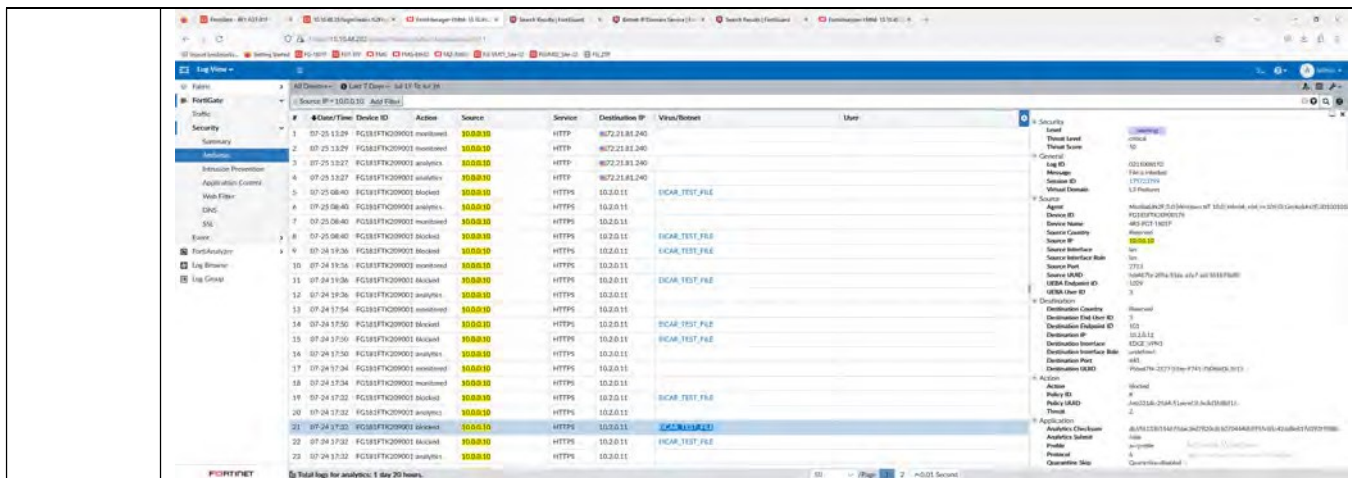


The image shows two screenshots from a computer screen. The top screenshot is a web browser displaying the FortiGuard Labs search results for the term "spyware". It lists several malware entries, including "W32/FakeAV_SpywareGuard.2!tr", "MSIL/SpyWare.92D5!tr", "W32/XPAntiSpyware.AF", and "W32/SpywareX.F05A!tr". The bottom screenshot shows the FortiGate management interface, specifically the "Licenses Information" section. It displays a table of various licenses such as "FortiCare Support", "Firewall & General Updates", "Intrusion Prevention", "AntiVirus", "AI Malware Detection Model", "AI Definitions", "AI Engine", "Mobile Malware", "Web Filtering", "Outbreak Prevention", "SD-WAN Network Monitor", "Security Rating", "Industrial DB", "IoT Detection Service", and "FortiGate Cloud". Each license entry includes its status (e.g., "Registered", "Licensed", "Not Licensed", "Not Activated") and an expiration date. A "FortiGate Updater" button is visible at the bottom of the interface.

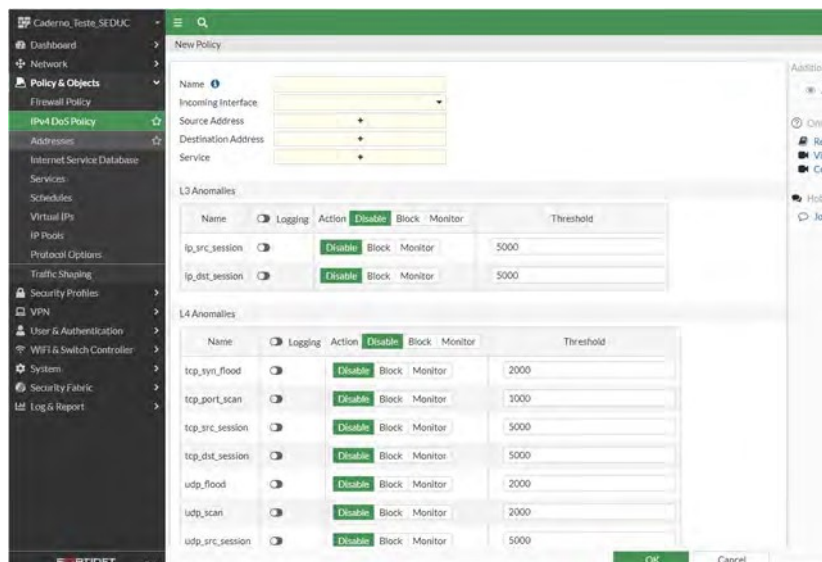
TESTE OK

<p>Comentário</p>	 <p>https://www.fortiguard.com/services/ips</p>
--------------------------	---

<p>Item de Teste - 5.3.8.4</p>	<p>A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;</p>
<p>Objetivo do Teste</p>	<p>Validar se a solução detecta e bloqueia comportamentos suspeitos ou anormais da rede</p>
<p>Configuração do Teste</p>	<p>Criar regra de acesso NGFW de anomalia</p>
<p>Procedimento do Teste</p>	<p>Navegando por Policy & Objects > IPv4 Dos Policy > Create New é possível criar regras que analisando o tráfego e detectam ou bloqueiam anomalias suspeitos da rede.</p>
<p>Evidências</p>	

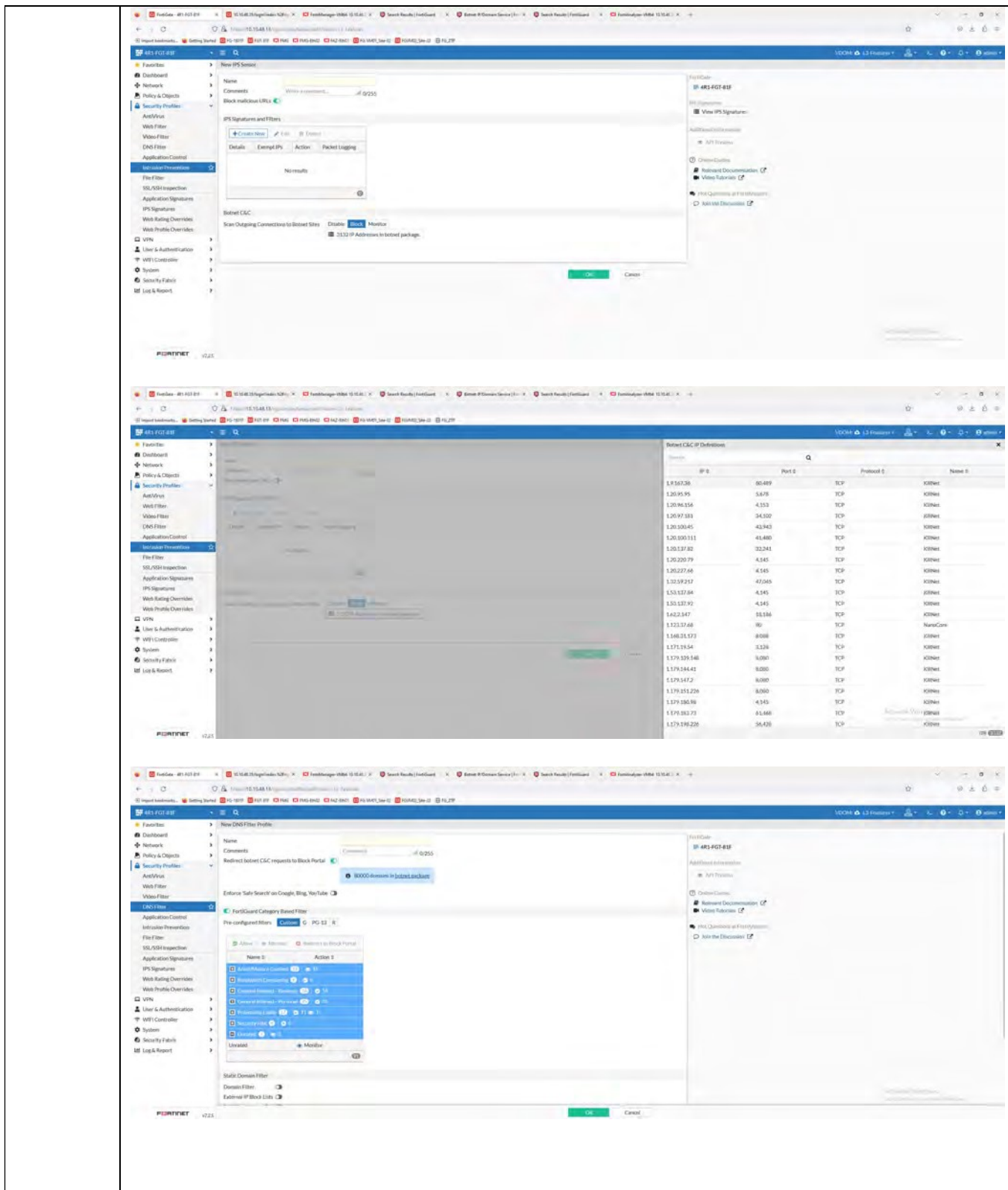


TESTE OK



Comentário

Item de Teste - 5.3.8.6	A solução Antibot deve possuir mecanismo de detecção em multicamadas que inclui, reputação de endereço IP, URLs e endereços DNS e detectar padrões de comunicação e assinaturas;
Objetivo do Teste	Verificar se a solução Antibot deve possuir mecanismo de detecção em multicamadas que inclui, reputação de endereço IP, URLs e endereços DNS e detectar padrões de comunicação e assinaturas;
Configuração do Teste	Demonstrar regra NGFW
Procedimento do Teste	Demonstrar regra NGFW
Evidências	



The image displays three sequential screenshots of the Fortinet FortiGate configuration interface, showing the setup of various security features:

- Top Screenshot:** Shows the configuration of a new IPS (Intrusion Prevention System) sensor. The 'Name' field is set to 'New IPS Sensor'. The 'Block malicious URLs' checkbox is checked. The 'Botnet CAC' (Content Advisory Control) section is visible, with 'Scan Outgoing Connections to Botnet Sites' checked and 'Block' selected as the action. A note indicates '3132 IP Addresses in botnet package'.
- Middle Screenshot:** Displays the 'Botnet CAC IP Definitions' table, which lists various IP addresses and their associated ports and protocols. The table includes columns for IP, Port, Protocol, and Name.
- Bottom Screenshot:** Shows the configuration of a new DNS Filter profile. The 'Name' field is set to 'New DNS Filter Profile'. The 'Enforce Safe Search on Google, Bing, YouTube' checkbox is checked. The 'Pre-configured Filters' section is expanded, showing a list of filters such as 'Adult/Explicit Content', 'Inappropriate Content', 'Copyright Infringement', etc., with their respective actions (Allow, Block, or Monitor).

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

Botnet C&C Domain Definitions

FQDN #	Name #
moduleconnector.at	Netwire
fonades.com	Ramnit
briancrabs.cm	Tofsee
defeatwax.ru	Tofsee
hugersi.com	Tofsee
lakeflex.ru	Tofsee
lazystax.ru	Tofsee
mubrikvch.top	Tofsee
ovicrush.cn	Tofsee
ooxyfx.xyz	Tofsee
parubey.info	Tofsee
quadoll.ru	Tofsee
boombom.at	Gameover-zeus
donios.at	Gameover-zeus
dopiertool.com	Gameover-zeus
hipohook.cn	Gameover-zeus
lujdhsndjfsk.com	Gameover-zeus
karilor.at	Gameover-zeus
iloptyp.at	Gameover-zeus

Ambas são perfis de segurança que podem ser aplicados juntamente em uma política específica.

New Policy

Name ? Política de Antibot

Incoming Interface ▼

Outgoing Interface ▼

Source +

Destination +

Schedule 🕒 always ▼

Service +

Action ACCEPT DENY

Firewall/Network Options

NAT

IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port

Protocol Options 🔍 ✎

Security Profiles

AntiVirus

Web Filter

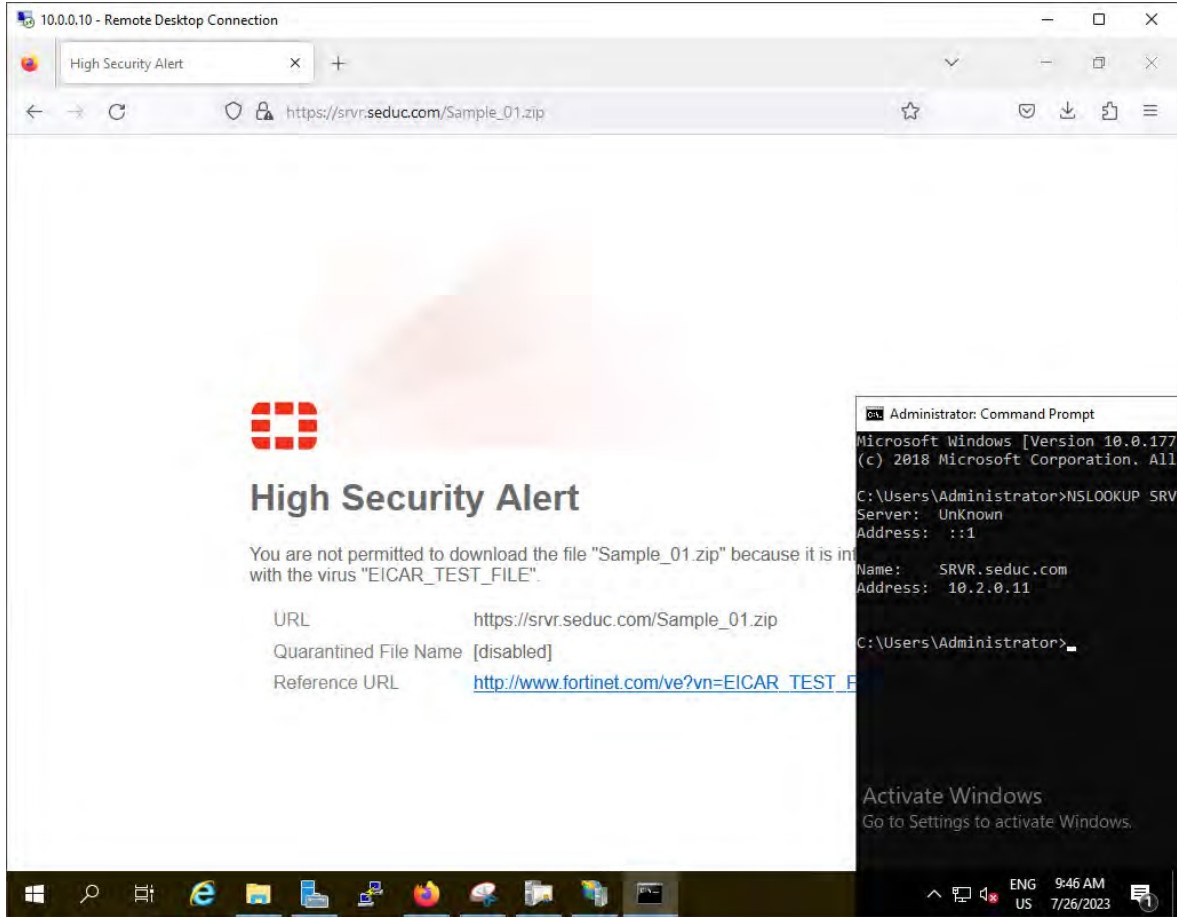
DNS Filter 🔍 ✎

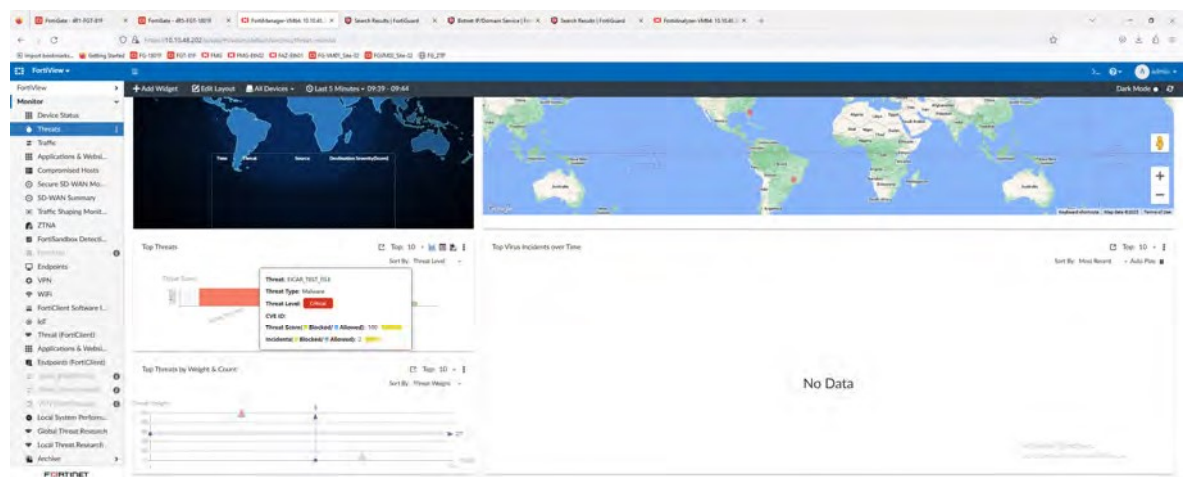
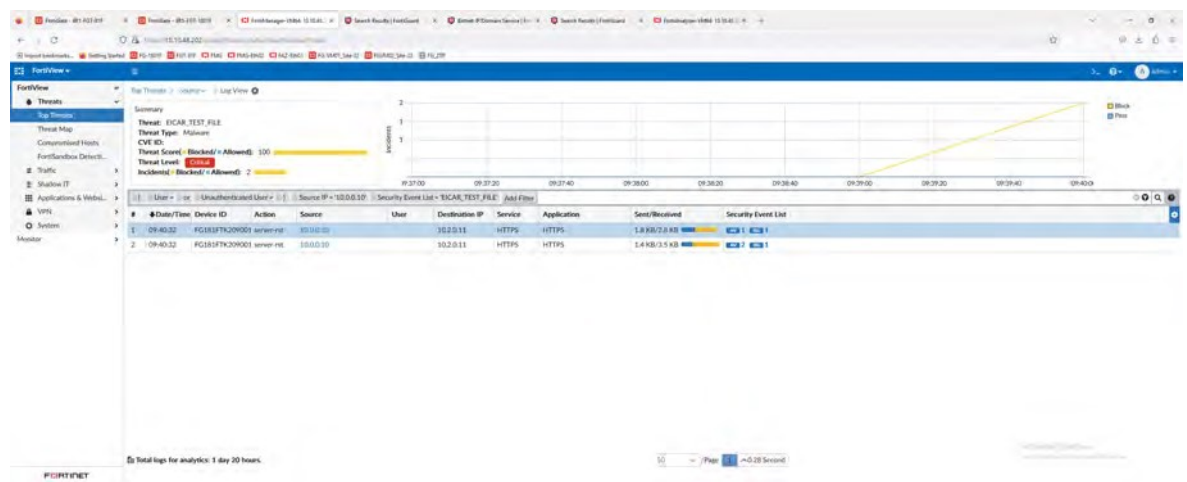
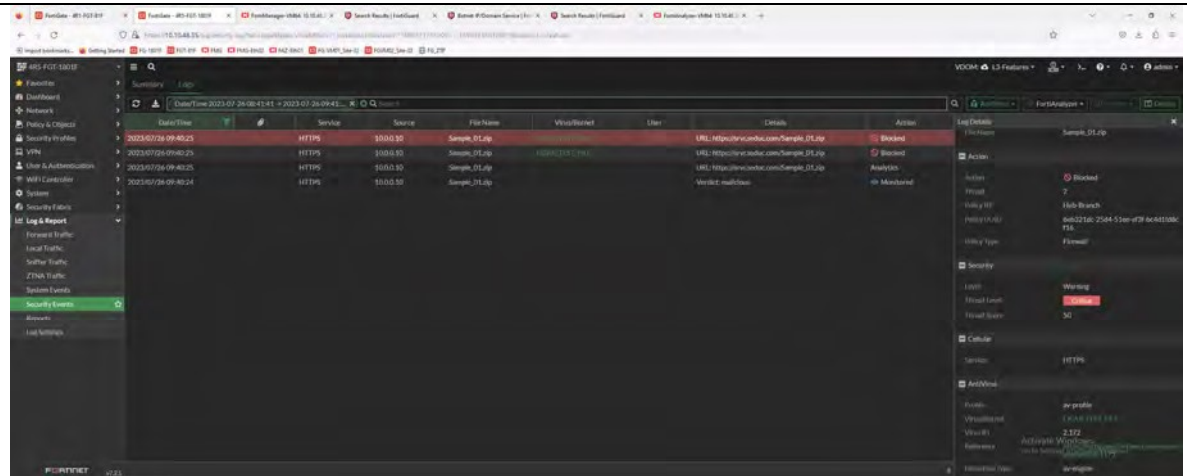
Application Control

IPS 🔍 ✎

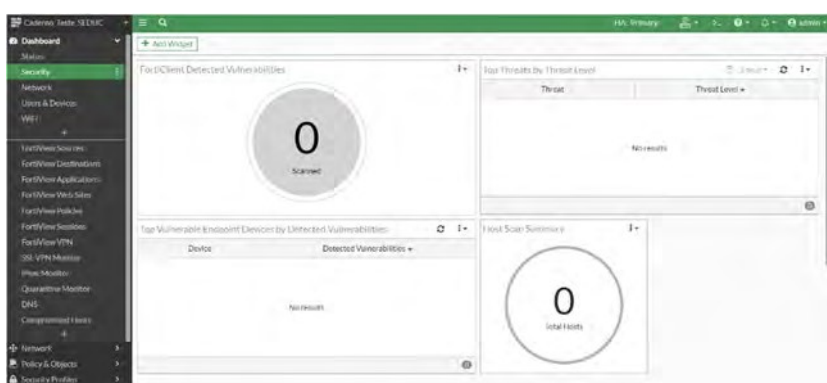
File Filter

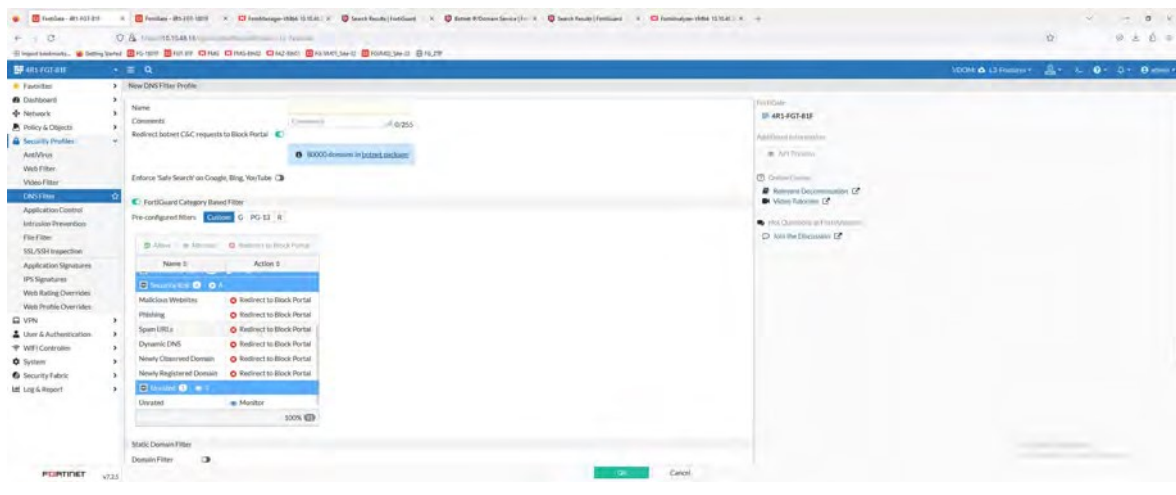
Comentário

Item de Teste - 5.3.8.9	A solução deve possuir na própria interface de gerência, gráfico contendo informações em tempo real sobre as atividades recentes de malwares detectados na solução;
Objetivo do Teste	Verificar se a solução possui na própria interface de gerência gráfico contendo informações em tempo real sobre as atividades recentes de malwares detectados na solução;
Configuração do Teste	Demonstrar dashboards de detecção de malwares
Procedimento do Teste	Na aba "Dashboard" temos a opção de selecionar "Security".
Evidências	Lá podemos ter acesso a diversas funcionalidades referentes a visualização de eventos de segurança detectados pela solução.
	 <p>The screenshot shows a remote desktop connection to a Windows 10 machine. The main window is a web browser displaying a 'High Security Alert' from Fortinet. The alert message states: 'You are not permitted to download the file "Sample_01.zip" because it is infected with the virus "EICAR_TEST_FILE"'. Below the message, it lists the URL as 'https://srvr.seduc.com/Sample_01.zip', the quarantined file name as '[disabled]', and a reference URL as 'http://www.fortinet.com/ve?vn=EICAR_TEST_FILE'. An 'Administrator: Command Prompt' window is overlaid on the right side of the browser, showing the following command and output:</p> <pre> Administrator: Command Prompt Microsoft Windows [Version 10.0.17763.1013] (c) 2018 Microsoft Corporation. All rights reserved. C:\Users\Administrator>NSLOOKUP SRV Server: UnKnown Address: ::1 Name: SRVR.seduc.com Address: 10.2.0.11 C:\Users\Administrator> </pre> <p>The Windows taskbar at the bottom shows the system tray with the date and time: 9:46 AM, 7/26/2023, and the language set to ENG US.</p>



TESTE OK

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

<p>Item de Teste - 5.3.8.10</p>	<p>Deve possuir engine onde faça Mitigação DNS, sendo ela possível identificar hosts infectados tentando acessar endereços conhecidos por conter conteúdo malicioso;</p>
<p>Objetivo do Teste</p>	<p>Verificar se a solução possui uma engine onde faça Mitigação DNS, sendo ela possível identificar hosts infectados tentando acessar endereços conhecidos por conter conteúdo malicioso.</p>
<p>Configuração do Teste</p>	<p>Criar regra NGFW contendo filtro de mitigação DNS</p>
<p>Procedimento do Teste</p>	<p>Criar regra NGFW contendo filtro de mitigação DNS</p>
<p>Evidências</p>	

10.1.0.50 - Remote Desktop Connection

10.0.0.10 - /arquivos/

Web Filter Violation

aaduhs.com

FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

You have tried to access a web page that is in violation of your Internet usage policy.

Category Malicious Websites
URL <http://aaduhs.com/>

To have the rating of this web page re-evaluated [please click here](#).

Activate Windows
Go to Settings to activate Windows.

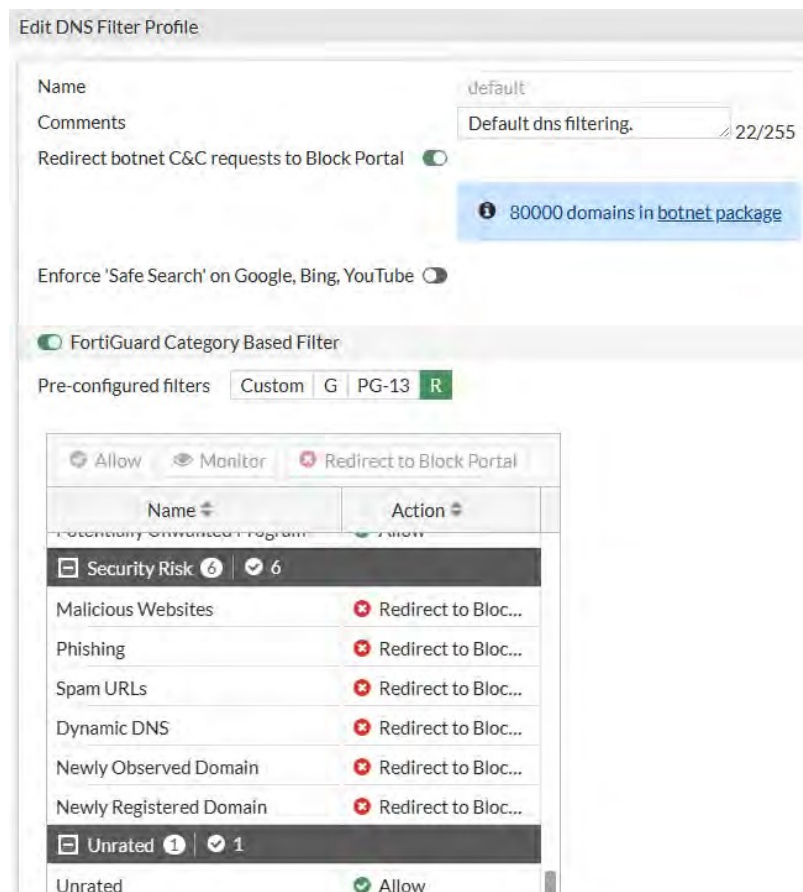
ENG INTL 9:50 AM 7/26/2023

Source	Destinations	Summary
		Summary of Domain: aaduhs.com Category: Malicious Websites Blocking Time: 0s Blocked Sites: 0 Bytes: 0 B

Time	User	Source	Action	URL	Category	Hit/Block
59 seconds ago	tharperm	10.1.0.50	Blocked	http://aaduhs.com/Paincoo.co	Malicious Websites	2/0 / 0/0
59 seconds ago	tharperm	10.1.0.50	Blocked	http://aaduhs.com/	Malicious Websites	3/0 / 0/0

TESTE OK

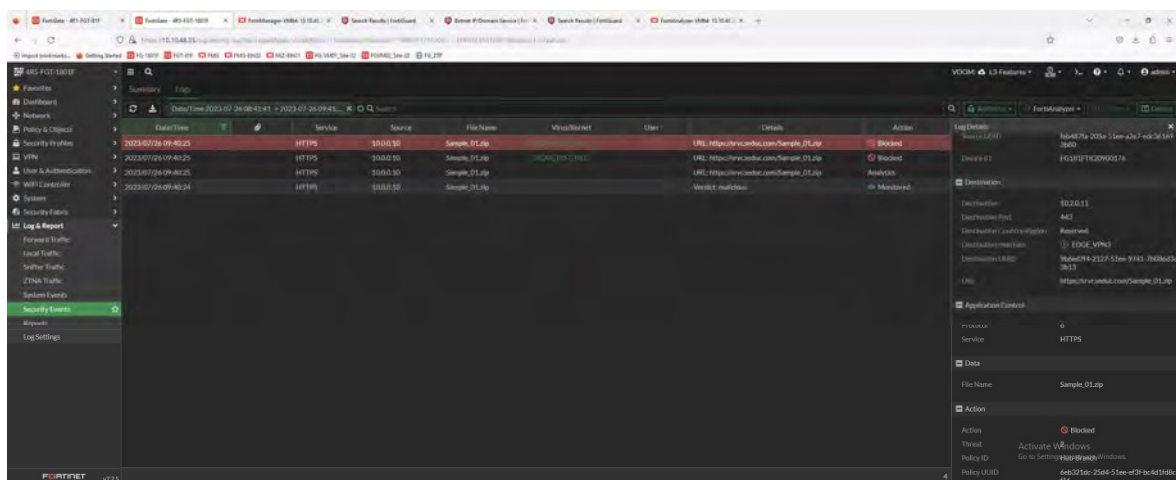
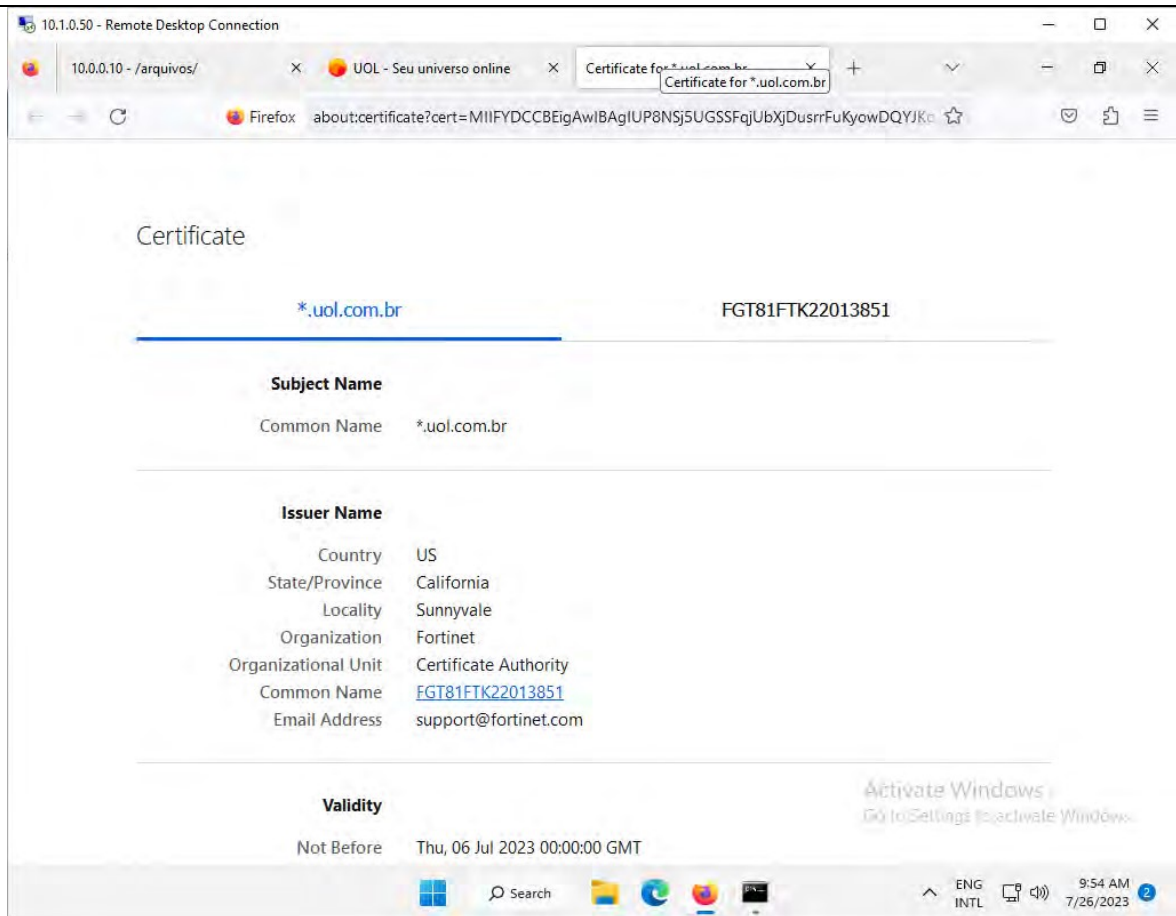
O FortiGate possui uma funcionalidade chamada de "DNS Filter"



Comentário

Item de Teste - 5.3.8.11	Deve ser capaz de inspecionar o tráfego criptografado SSL;
Objetivo do Teste	Validar se o FortiGate realiza inspeção SSL de pacotes de tráfego criptografado
Configuração do Teste	Demonstrar regra NGFW com inspeção SSL.
Procedimento do Teste	Para realizar SSL Inspection basta navegar por Policy & Objects > Firewall Policy > Security Profiles e no campo SSL Inspection selecionar Deep-Inspection, no fluxo da política selecionada o firewall irá realizar a inspeção de pacotes.
Evidências	

The screenshot shows a remote desktop connection to a Windows machine. The browser window displays the UOL website with a security warning: "Connection security for www.uol.com.br" and "You are not securely connected to this site." A large green button labeled "EMPEZAR" is prominent. Below it, instructions in Spanish are listed: "1) Haga clic en 'Empezar' | 2) Iniciar la instalación | 3) Bloquear anuncios y malware". The Windows taskbar at the bottom shows the date and time as 9:53 AM on 7/26/2023.



TESTE OK

Security Profiles

- AntiVirus
- Web Filter
- DNS Filter
- Application Control
- IPS
- File Filter
- SSL Inspection** SSL deep-inspection
- Decrypted Traffic Mirror

Edit SSL/SSH Inspection Profile

SSL Inspection Options

Enable SSL inspection of Multiple Clients Connecting to Multiple Servers

Inspection method Protecting SSL Server

CA certificate SSL Certificate Inspection Full SSL Inspection

Blocked certificates Fortinet_CA_SSL Download

Untrusted SSL certificates Allow Block View Blocked Certificates

Server certificate SNI check Allow Block Ignore View Trusted CAs List

Enforce SSL cipher compliance

Enforce SSL negotiation compliance

RPC over HTTPS

Protocol Port Mapping

Inspect all ports

HTTPS	<input checked="" type="checkbox"/>	443
SMTPTS	<input checked="" type="checkbox"/>	465
POP3S	<input checked="" type="checkbox"/>	995
IMAPS	<input checked="" type="checkbox"/>	993
FTPS	<input checked="" type="checkbox"/>	990
DNS over TLS	<input checked="" type="checkbox"/>	853

Exempt from SSL Inspection

Reputable websites

Web categories

- Finance and Banking x
- Health and Wellness x
- +

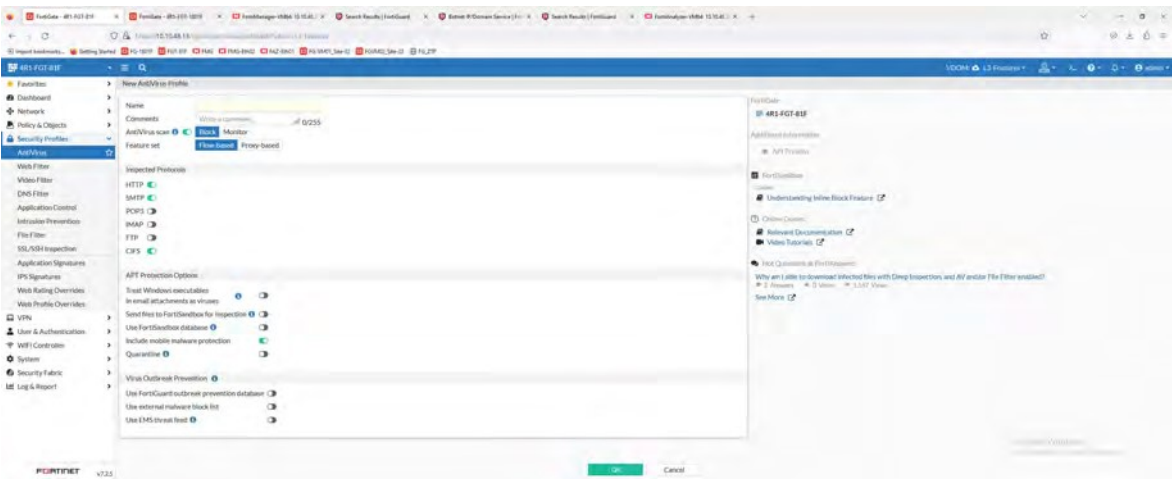
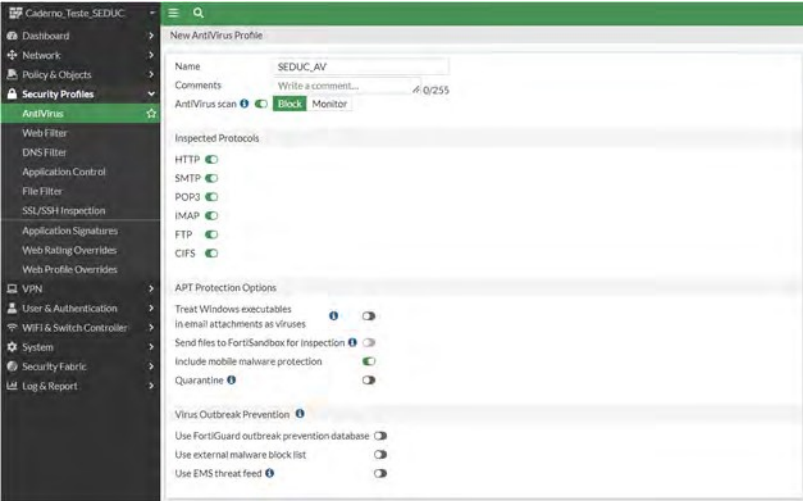
Addresses

- adobe x
- Adobe Login x

[Return](#)

Comentário

Item de Teste - 5.3.8.12	Deve ser capaz de inspecionar protocolos SMB/CIFS, SMTP, HTTP e HTTPS;
Objetivo do Teste	Validar se a ferramenta é capaz de inspecionar protocolos SMB/CIFS, SMTP, HTTP e HTTPS;
Configuração do Teste	Demonstrar inspeção: SMB/CIFS, SMTP, HTTP e HTTPS

<p>Procedimento do Teste</p>	<p>A inspeção de protocolos é feita de duas formas. A primeira é utilizando o Security Profile de Antivírus, onde é possível inspecionar os protocolos HTTP, SMTP, POP3, IMAP, FTP, CIFS. A segunda forma é utilizando SSL Deep Inspection onde é possível realizar a inspeção de protocolos seguros.</p>
<p>Evidências</p>	 <p>TESTE OK</p> 

Security Profiles

- AntiVirus
- Web Filter
- DNS Filter
- Application Control
- IPS
- File Filter
- SSL Inspection** SSL deep-inspection
- Decrypted Traffic Mirror

Edit SSL/SSH Inspection Profile

SSL Inspection Options

Enable SSL inspection of Multiple Clients Connecting to Multiple Servers

Inspection method Protecting SSL Server

CA certificate SSL Certificate Inspection Full SSL Inspection

Blocked certificates Fortinet_CA_SSL Download

Untrusted SSL certificates Allow Block View Blocked Certificates

Server certificate SNI check Allow Block Ignore View Trusted CAs List

Enforce SSL cipher compliance

Enforce SSL negotiation compliance

RPC over HTTPS

Protocol Port Mapping

Inspect all ports

HTTPS	<input checked="" type="checkbox"/>	443
SMTPS	<input checked="" type="checkbox"/>	465
POP3S	<input checked="" type="checkbox"/>	995
IMAPS	<input checked="" type="checkbox"/>	993
FTPS	<input checked="" type="checkbox"/>	990
DNS over TLS	<input checked="" type="checkbox"/>	853

Exempt from SSL Inspection

Reputable websites

Web categories

- Finance and Banking
- Health and Wellness

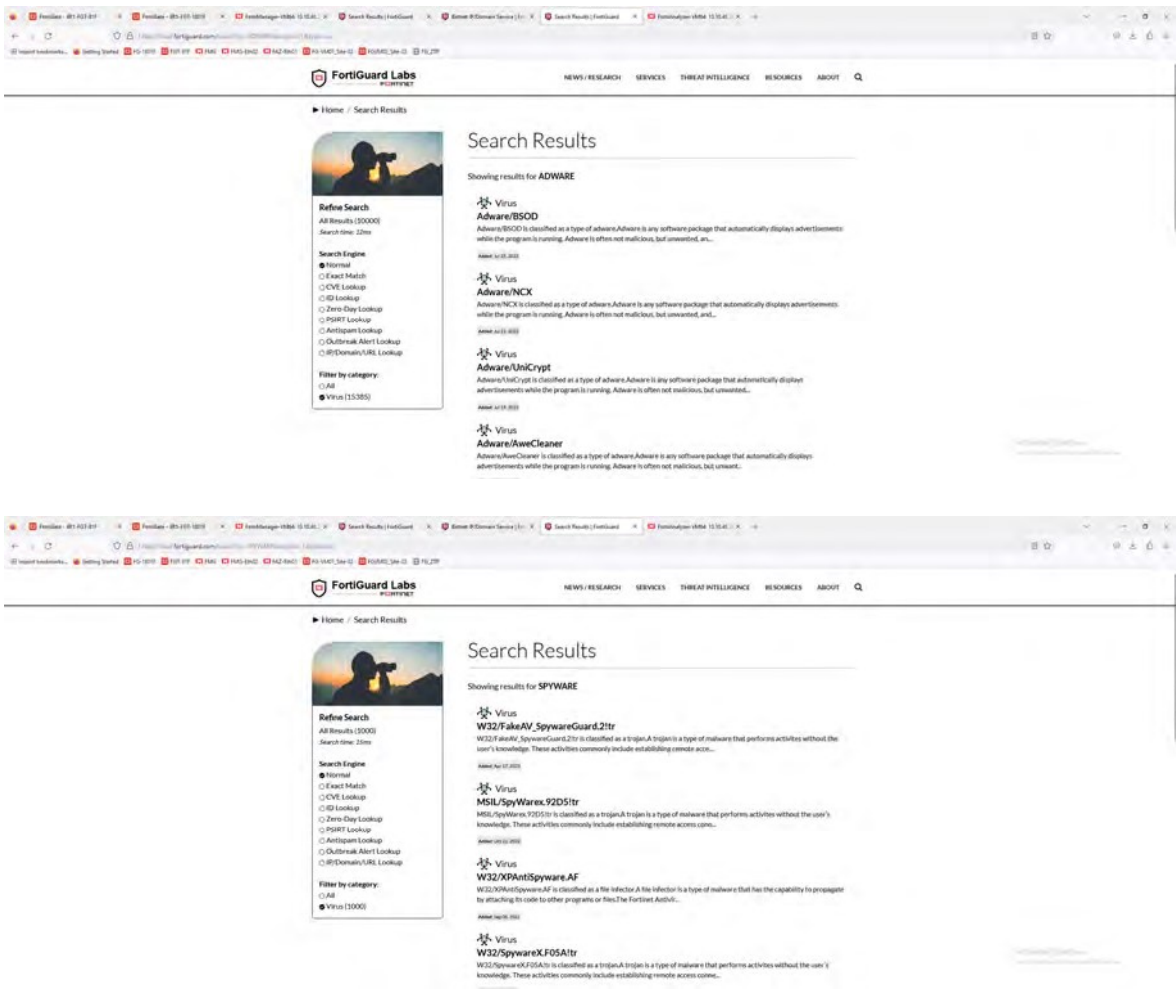
Addresses

- adobe
- Adobe Login

Return

Comentário

Item de Teste - 5.3.8.13	Deve permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.);
Objetivo do Teste	Verificar se a solução permite o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.).
Configuração do Teste	Demonstrar a configuração de regra com filtro de Antivírus.

<p>Procedimento do Teste</p>	<p>Demonstrar a configuração de regra com filtro de Antivírus.</p>
<p>Evidências</p>	

The image shows two screenshots of the FortiGuard Labs search results page. The top screenshot displays search results for 'HIJACKER', listing several virus signatures such as W32/Hjacker.Ultr, W32/DIHjacker.ELTr, W32/Hjacker.Str, and W32/DIHjacker.QKTr. The bottom screenshot displays search results for 'KEYLOGGER', listing signatures like MSIL/KeyLogger.FRjTr.spy, W44/KeyLogger.JAtr.spy, W32/KeyLogger.QKQTr.spy, and W32/KeyLogger.PLAtr. Both screenshots include a 'Refine Search' sidebar with filters for search engine and category.

TESTE OK

Todos os bloqueios de malwares são feitos pelo Antivírus do FortiGate, caso haja a necessidade de adicionar outras assinaturas além das que já são mapeadas pela FortiGuard, o FortiGate te dá a opção de adicioná-las à base de dados dele.

	<div style="border: 1px solid #ccc; padding: 10px;"> <p>Edit AntiVirus Profile</p> <hr/> <p>Name <input type="text" value="default"/></p> <p>Comments <input type="text" value="Scan files and block viruses."/> 29/255</p> <p>AntiVirus scan <input checked="" type="checkbox"/></p> <hr/> <p>Inspected Protocols</p> <p>HTTP <input type="checkbox"/></p> <p>SMTP <input type="checkbox"/></p> <p>POP3 <input type="checkbox"/></p> <p>IMAP <input type="checkbox"/></p> <p>FTP <input type="checkbox"/></p> <p>CIFS <input type="checkbox"/></p> <hr/> <p>APT Protection Options</p> <p>Treat Windows executables in email attachments as viruses <input type="checkbox"/></p> <p>Send files to FortiSandbox for inspection <input type="checkbox"/></p> <p>Include mobile malware protection <input checked="" type="checkbox"/></p> <p>Quarantine <input type="checkbox"/></p> <hr/> <p>Virus Outbreak Prevention</p> <p>Use FortiGuard outbreak prevention database <input type="checkbox"/></p> <p>Use external malware block list <input type="checkbox"/></p> <p>Use EMS threat feed <input type="checkbox"/></p> <hr/> <p>External malware block list</p> <p>The external malware block list allows users to add their own malware signatures in the form of MD5, SHA1, and SHA256 hashes. The FortiGate's antivirus database retrieves an external malware hash list from a remote server and polls the hash list every <i>n</i> minutes for updates. Enabling the AV engine scan is not required to use this feature.</p> <p>The external malware block list can be used in both proxy-based and flow-based policy inspections, but it is not supported in AV quick scan mode.</p> <p>Note that using different types of hashes simultaneously may slow down the performance of malware scanning. It is recommended to use one type of hash.</p> </div>
Comentário	https://docs.fortinet.com/document/fortigate/7.2.0/administration-guide/254346

5.3.9 AMEAÇAS AVANÇADAS PERSISTENTES - APT:

Item de Teste - 5.3.9.1	Deverá prover as funcionalidades de inspeção de tráfego de entrada de malwares não conhecidos (dia zero) ou do tipo APT (Advanced Persistent Threat) com filtro de ameaças avançadas e análise de execução em tempo real;
Objetivo do Teste	Validar se a solução promove a funcionalidade de inspeção de tráfego de entrada de malwares não conhecidos (dia zero) ou do tipo APT (Advanced Persistent Threat) utilizando filtro de ameaças avançadas e análise de execução em tempo real.
Configuração do Teste	Realizar uma inspeção de tráfego de malwares.
Procedimento do Teste	Primeiro é necessário configurar a funcionalidade "FortiGate Cloud Sandbox" no FortiGate.

7.2.4 ↓
Copy Link
Download PDF

Configuring sandboxing

The Security Fabric supports the following FortiSandbox deployments.

Type	Description	Requirements
FortiGate Cloud Sandbox	Files are sent to Fortinet's Cloud Sandbox cluster for processing.	<ul style="list-style-type: none"> The FortiGate must have a valid AV license. The FortiCloud account provides access to a portal to view submissions. This is not required for the Security Fabric.

7.2.4 ↓
Copy Link
Download PDF

Using FortiSandbox post-transfer scanning with antivirus

Antivirus profiles can submit potential zero-day viruses to FortiSandbox for inspection. Based on FortiSandbox's analysis, the FortiGate can supplement its own antivirus database with FortiSandbox's threat intelligence to detect files determined as malicious or suspicious. This augments the FortiGate antivirus with zero-day detection.

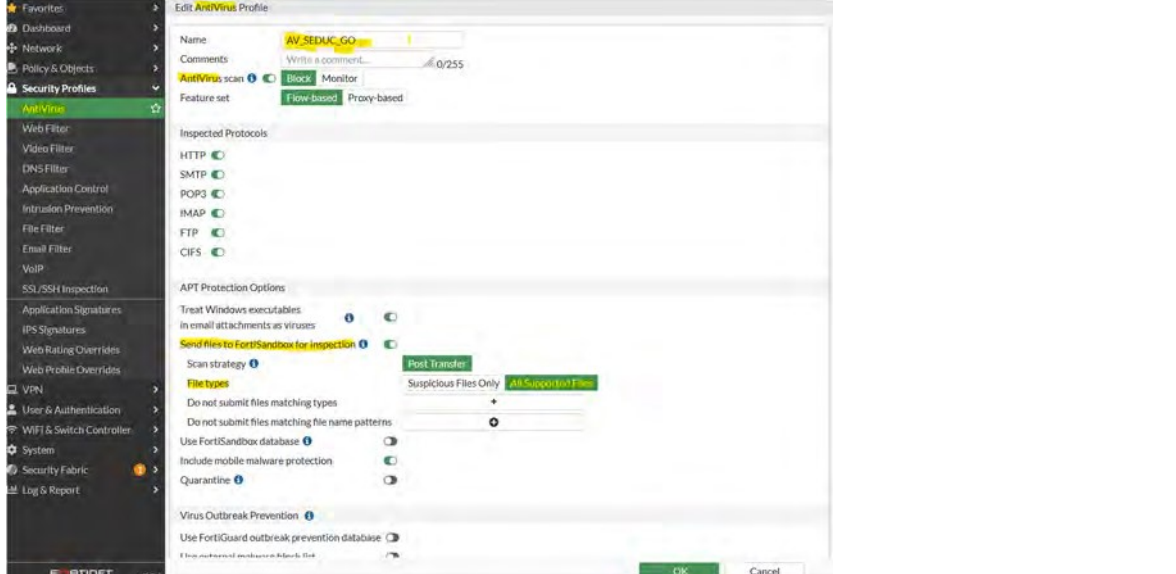
FortiSandbox can be used with antivirus in both proxy-based and flow-based inspection modes. The FortiGate first examines the file for any known viruses. When a match is found, the file is tagged as known malware. If no match is found, the files are forwarded to FortiSandbox using the following options:

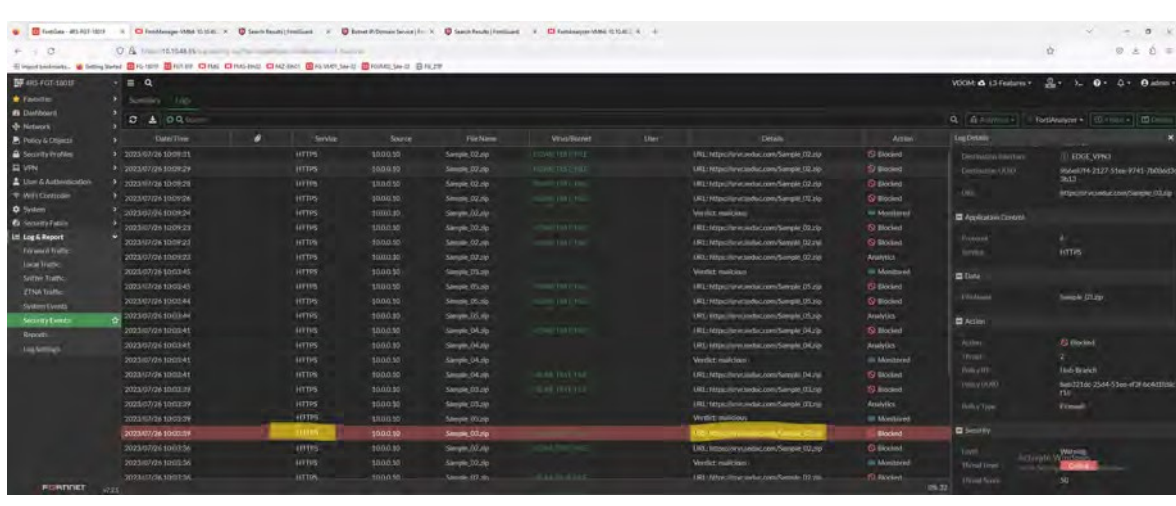
- All Supported Files*: all files matching the file types defined in the scan profile of the FortiSandbox are forwarded.
- Suspicious Files Only*: files classified by the antivirus as having any possibility of active content are forwarded to FortiSandbox. When using FortiGate Cloud Sandbox, we recommend selecting this option due to its submission limits.
- None*: files are not forwarded to FortiSandbox.

For more information, see [Configuring sandboxing](#).

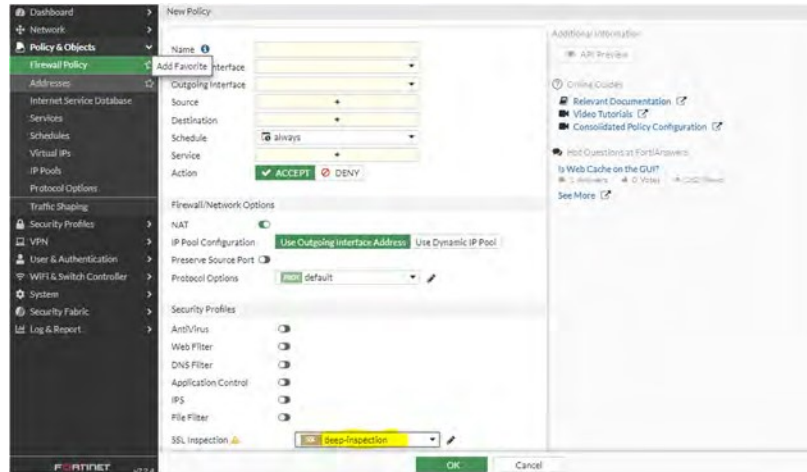
To enable FortiSandbox inspection in an antivirus profile:

1. Go to *Security Profiles > AntiVirus*.
2. Create, edit, or clone an antivirus profile.
3. In the *APT Protection Options* section, set *Send Files to FortiSandbox for Inspection* to either *Suspicious Files Only* or *All Supported Files*.

	
<p>Comentário</p>	<p>https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/481589</p> <p>https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/660221/configuring-sandboxing</p>

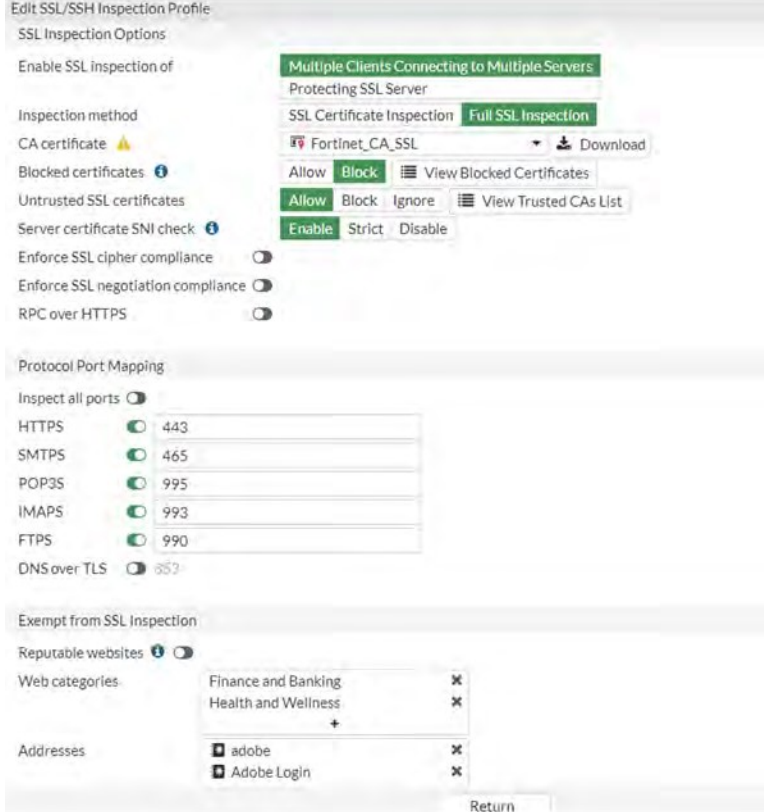
<p>Item de Teste - 5.3.9.2</p>	<p>A solução deve ser capaz de inspecionar o tráfego criptografado SSL;</p>
<p>Objetivo do Teste</p>	<p>Validar se o FortiGate realiza inspeção SSL de pacotes de tráfego criptografado</p>
<p>Configuração do Teste</p>	<p>Criar regra de inspeção SSL</p>
<p>Procedimento do Teste</p>	<p>Para realizar SSL Inspection basta navegar por Policy & Objects > Firewall Policy > Security Profiles e no campo SSL Inspection selecionar deep-inspection, no fluxo da política selecionada o firewall irá realizar a inspeção de pacotes.</p>
<p>Evidências</p>	

TESTE OK

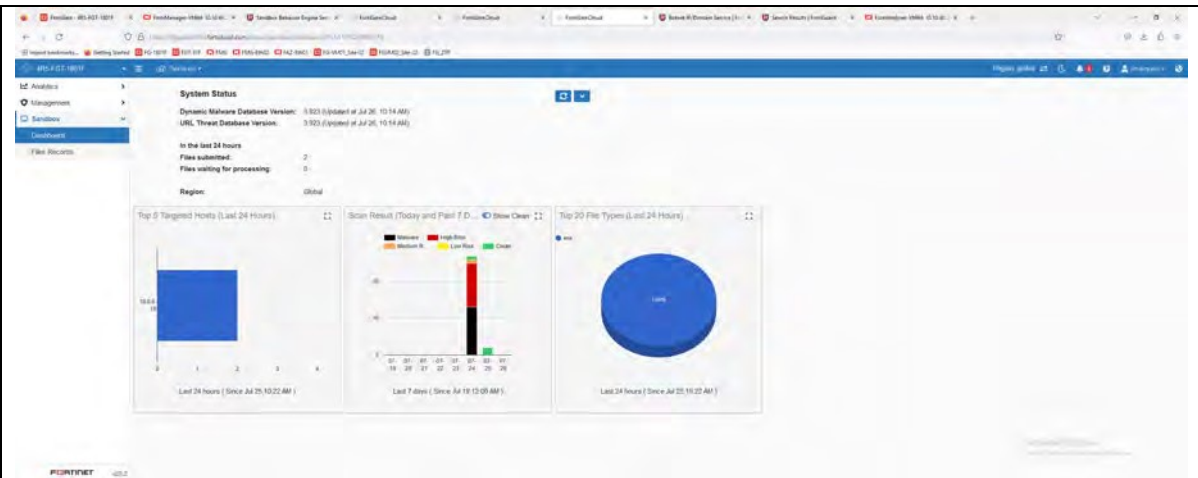


Security Profiles

- AntiVirus
- Web Filter
- DNS Filter
- Application Control
- IPS
- File Filter
- SSL Inspection SSL deep-inspection
- Decrypted Traffic Mirror

	
<p>Comentário</p>	

<p>Item de Teste - 5.3.9.5</p>	<p>Implementar atualização da base de dados da rede de inteligência de forma automática;</p>
<p>Objetivo do Teste</p>	<p>Verificar se a base de dados da rede de inteligência atualiza de forma automatizada.</p>
<p>Configuração do Teste</p>	<p>Demonstrar tela de atualização</p>
<p>Procedimento do Teste</p>	<p>Para ter acesso a essa funcionalidade é necessário acessar a aba "FortiGuard" em "System". Na parte de baixo podemos ter acesso as configurações de quantas vezes por dia verificar novas atualizações</p>
<p>Evidências</p>	



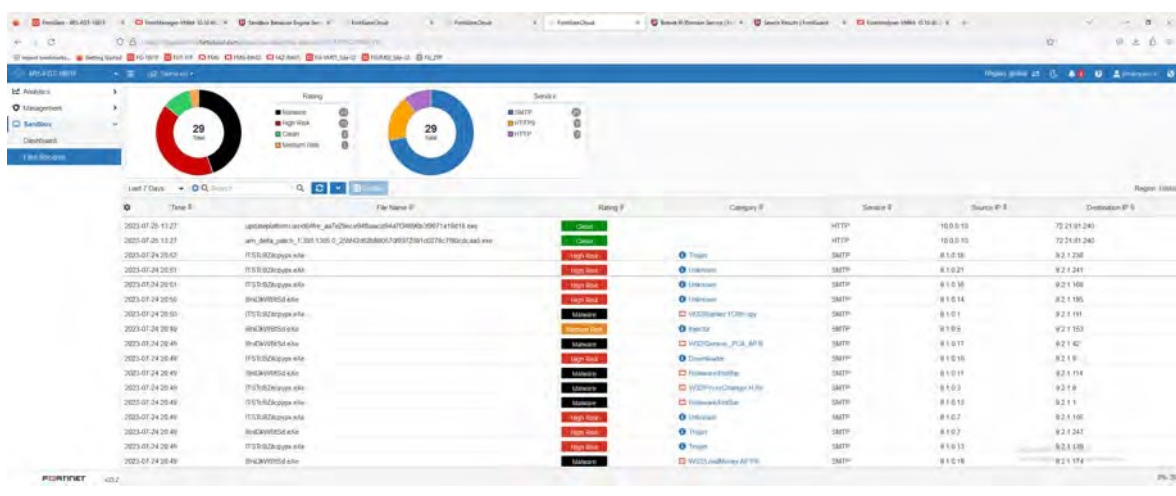
TESTE OK

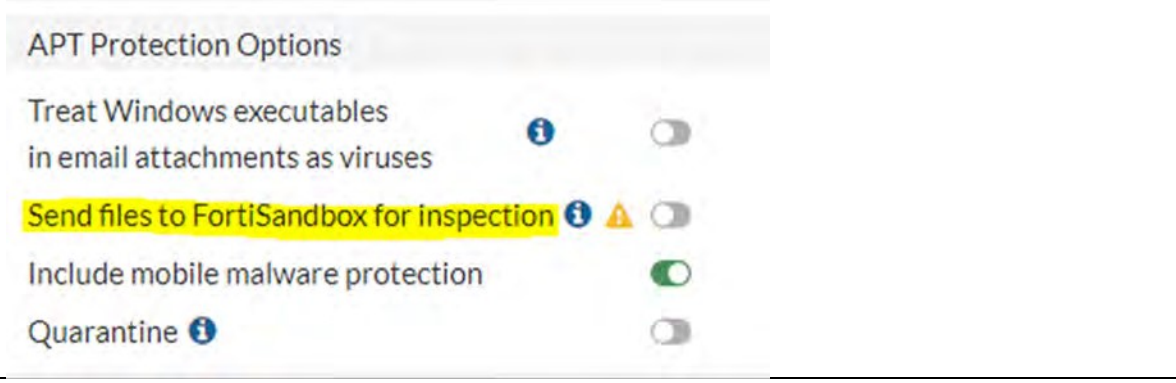
The screenshot shows the 'FortiGuard Distribution Network' configuration page in the Fortinet v7.2.4 management console. The left sidebar contains a navigation menu with 'FortiGuard' selected. The main content area includes the following settings:

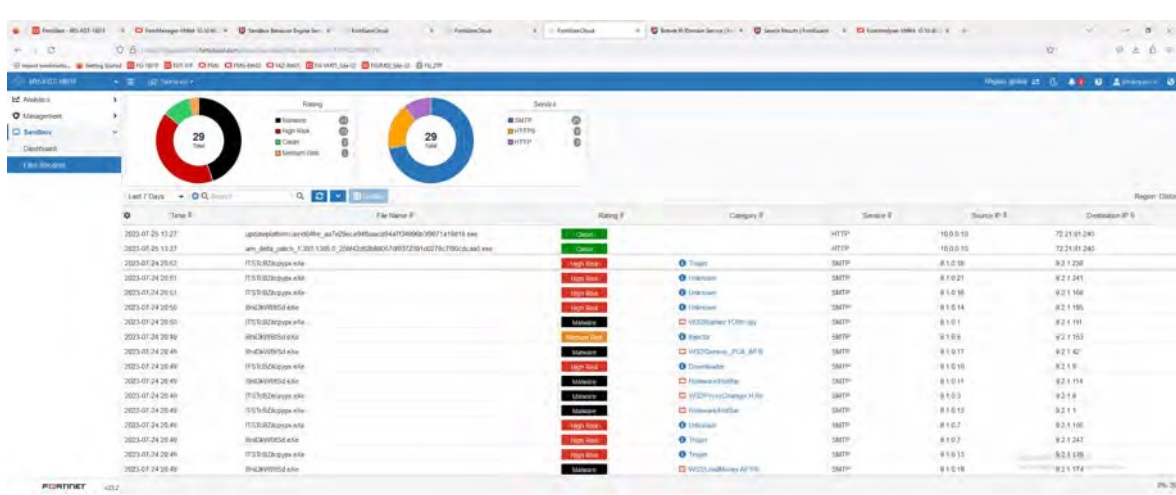
- FortiGuard Updates:** Scheduled updates are set to 'Automatic' (with 'Every', 'Daily', and 'Weekly' options also visible).
- Improve IPS quality:** Toggled off.
- Use extended IPS signature package:** Toggled off.
- AntiVirus PUP/PUA:** Toggled on.
- Update server location:** Set to 'Lowest latency locations' with a 'Restrict to' field.
- Filtering:** Section header.
- Override FortiGuard Servers:** Section header.

An 'Apply' button is located at the bottom right of the configuration area.

Comentário	<div style="border: 1px solid #ccc; padding: 10px;"> <p>FortiGuard Updates</p> <p>Next Update: 2023/03/14 11:17:00</p> <p>Update Licenses & Definitions Now</p> <p>Manual Update</p> <p>Upload License File</p> </div>
------------	--

Item de Teste - 5.3.9.6	A solução deve implementar a emulação, detecção ou bloqueio de qualquer malware e/ou código malicioso detectado;
Objetivo do Teste	Verificar se a solução implementa a emulação, detecção ou bloqueio de qualquer malware e/ou código malicioso detectado.
Configuração do Teste	Demonstrar configuração da regra com sandbox.
Procedimento do Teste	É necessário habilitar essa funcionalidade em "Security Profile" e "Antivírus".
Evidências	 <p>TESTE OK</p> <p>O serviço de antivírus faz a parte de detecção e bloqueio utilizando como base o FortiGuard, além disso para a parte de emulação de um Malware ele manda o código malicioso para o FortiGateCloud Sandbox, que verifica este código em um ambiente controlado em nuvem daí devolve para o FortiGate a ação a ser tomada dependendo do que ele avalia daquele código.</p>

Comentário	 <p>APT Protection Options</p> <ul style="list-style-type: none"> Treat Windows executables in email attachments as viruses <input type="checkbox"/> Send files to FortiSandbox for inspection <input type="checkbox"/> Include mobile malware protection <input checked="" type="checkbox"/> Quarantine <input type="checkbox"/>
------------	---

Item de Teste - 5.3.9.7	Toda análise deverá ser realizada de forma interna em Appliance ou próprio fabricante ou nuvem do próprio fabricante, não sendo aceitas soluções que necessitem de módulos e/ou servidores externos para a implementação de máquinas virtuais;
Objetivo do Teste	Demonstrar que a solução possui estrutura interna ou na nuvem do fabricante para solução Sandbox.
Configuração do Teste	Demonstrar relatórios na nuvem do fabricante Fortinet.
Procedimento do Teste	Demonstrar relatórios na nuvem do fabricante Fortinet.
Evidências	 <p>TESTE OK</p>

O Antivírus do FortiGate faz o envio de códigos maliciosas para o FortiGate Cloud Sandbox, um ambiente na nuvem que faz a emulação desses códigos e retorna para o FortiGate um veredicto.

Configuring Sandboxing

The Security Fabric supports the following FortiSandbox deployments.

Type	Description	Requirements
FortiGate Cloud Sandbox	Files are sent to Fortinet's Cloud Sandbox cluster for processing.	<ul style="list-style-type: none"> The FortiGate must have a valid AV license. The FortiCloud account provides access to a portal to view submissions. This is not required for the Security Fabric.
FortiSandbox Cloud	Files are sent to a dedicated FortiCloud hosted instance of FortiSandbox for processing.	<ul style="list-style-type: none"> FortiCloud premium license FortiSandbox Cloud entitlement The FortiGate and FortiCloud license are registered to the same account.
FortiSandbox appliance	Files are sent to a physical appliance or VM, typically residing on premise, for processing.	<ul style="list-style-type: none"> None

7.2.4

Copy Link

Download PDF

Using FortiSandbox post-transfer scanning with antivirus

Antivirus profiles can submit potential zero-day viruses to FortiSandbox for inspection. Based on FortiSandbox's analysis, the FortiGate can supplement its own antivirus database with FortiSandbox's threat intelligence to detect files determined as malicious or suspicious. This augments the FortiGate antivirus with zero-day detection.

FortiSandbox can be used with antivirus in both proxy-based and flow-based inspection modes. The FortiGate first examines the file for any known viruses. When a match is found, the file is tagged as known malware. If no match is found, the files are forwarded to FortiSandbox using the following options:

- All Supported Files: all files matching the file types defined in the scan profile of the FortiSandbox are forwarded.
- Suspicious Files Only: files classified by the antivirus as having any possibility of active content are forwarded to FortiSandbox. When using FortiGate Cloud Sandbox, we recommend selecting this option due to its submission limits.
- None: files are not forwarded to FortiSandbox.

For more information, see Configuring sandboxing.

To enable FortiSandbox inspection in an antivirus profile:

- Go to *Security Profiles > Antivirus*.
- Create, edit, or clone an antivirus profile.
- In the *APT Protection Options* section, set *Send Files to FortiSandbox for Inspection* to either *Suspicious Files Only* or *All Supported Files*.

APT Protection Options

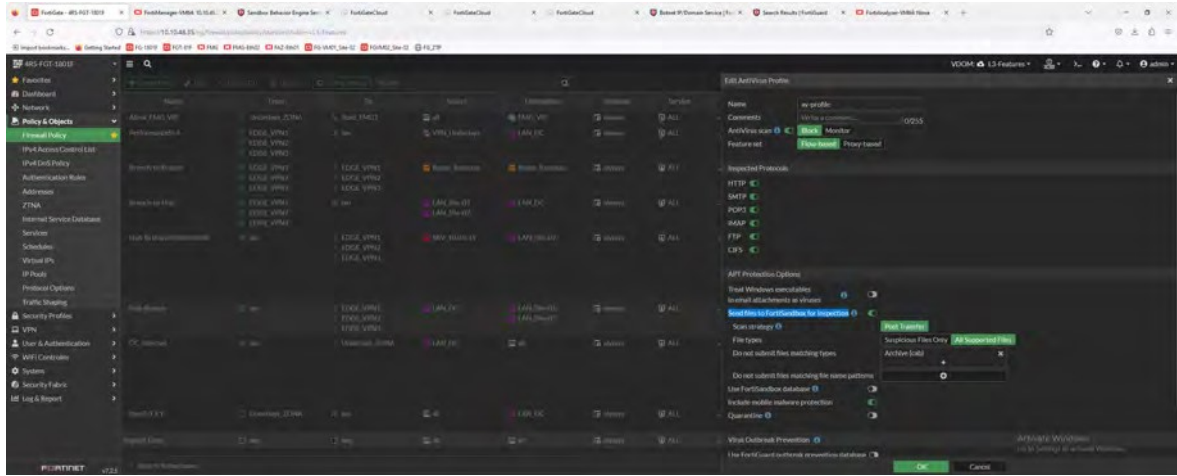
Treat Windows executables in email attachments as viruses [i] [toggle off]

Send files to FortiSandbox for inspection [i] [warning] [toggle off]

Include mobile malware protection [toggle on]

Quarantine [i] [toggle off]

Comentário

Item de Teste - 5.3.9.9	Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador para solicitar a análise;
Objetivo do Teste	Validar se a solução realiza a análise de forma automatizada ou sem a necessidade de solicitar a análise para a proteção ATP
Configuração do Teste	Demonstrar ativação da funcionalidade de Sandbox.
Procedimento do Teste	<p>Primeiro é necessário configurar a funcionalidade “FortiGate Cloud Sandbox” no FortiGate.</p> <p>Após realizar as configurações para habilitar o Sandbox basta navegar por Security Profiles > AntiVirus > Create New > APT Protection Options e habilitar o envio de arquivos para a inspeção do Sandbox.</p> <p>Por último basta incluir o perfil criado no fluxo da política em que deseja realizar a inspeção.</p>
Evidências	 <p>TESTE OK</p>

7.2.3 ↓

Copy Link

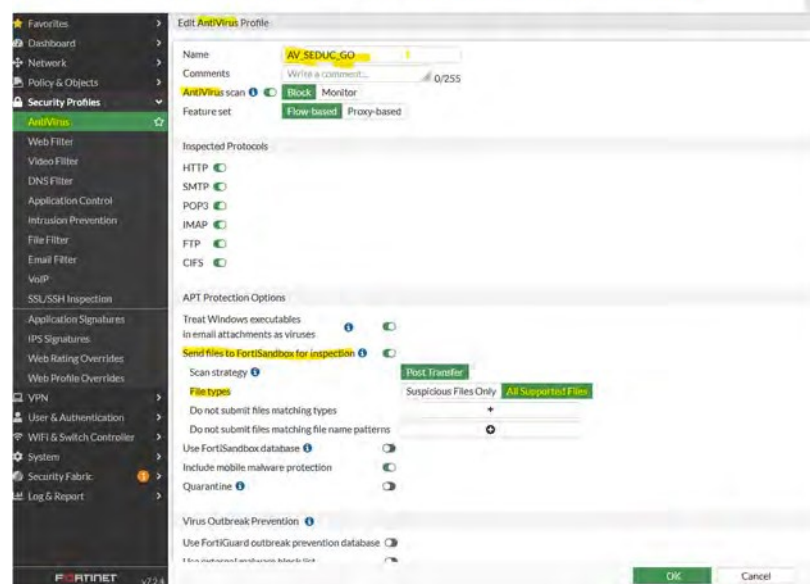
Download PDF

Using FortiSandbox post-transfer scanning with antivirus


Antivirus profiles can submit potential zero-day viruses to FortiSandbox for inspection. Based on FortiSandbox's analysis, the FortiGate can supplement its own antivirus database with FortiSandbox's threat intelligence to detect files determined as malicious or suspicious. This augments the FortiGate antivirus with zero-day detection.

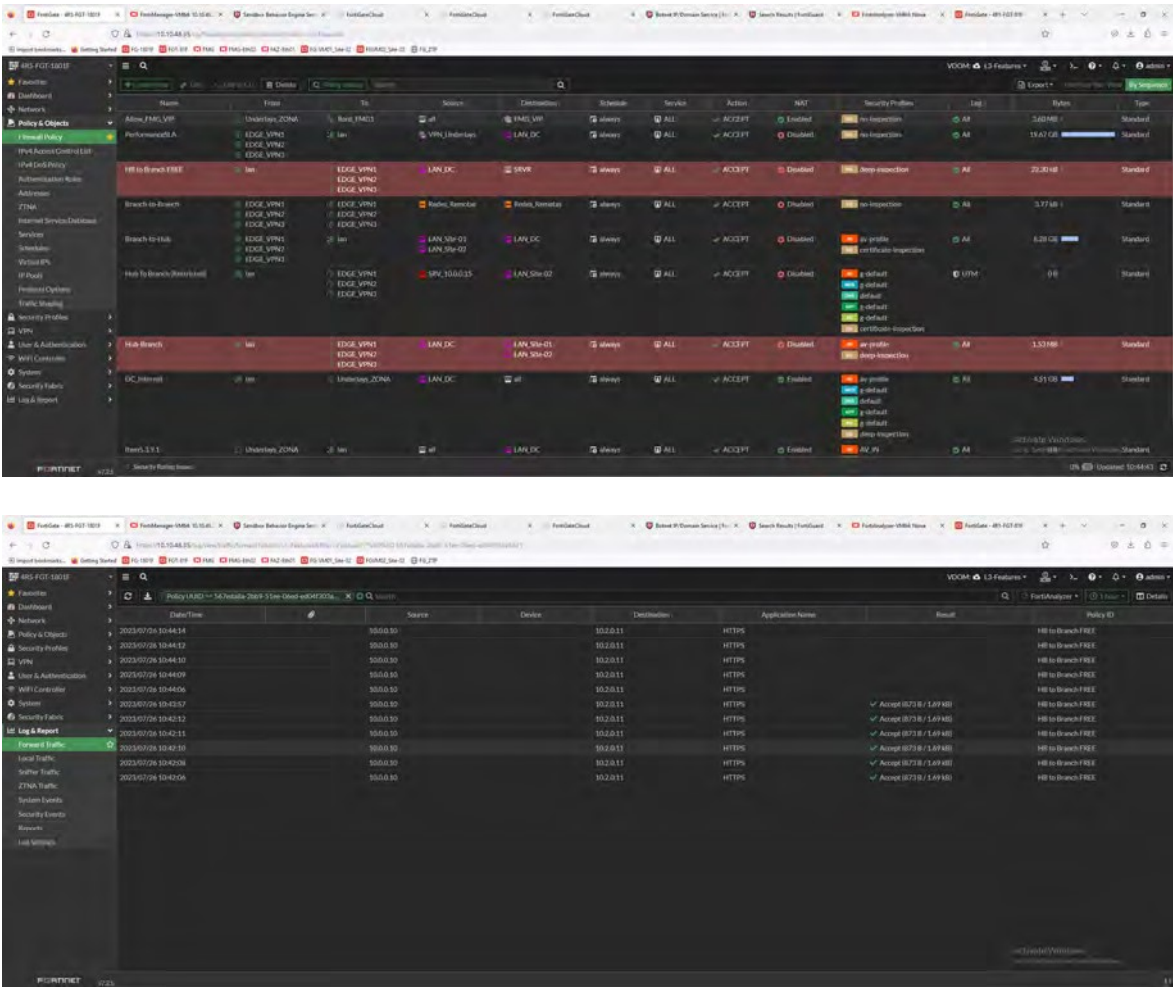
FortiSandbox can be used with antivirus in both proxy-based and flow-based inspection modes. The FortiGate first examines the file for any known viruses. When a match is found, the file is tagged as known malware. If no match is found, the files are forwarded to FortiSandbox using the following options:

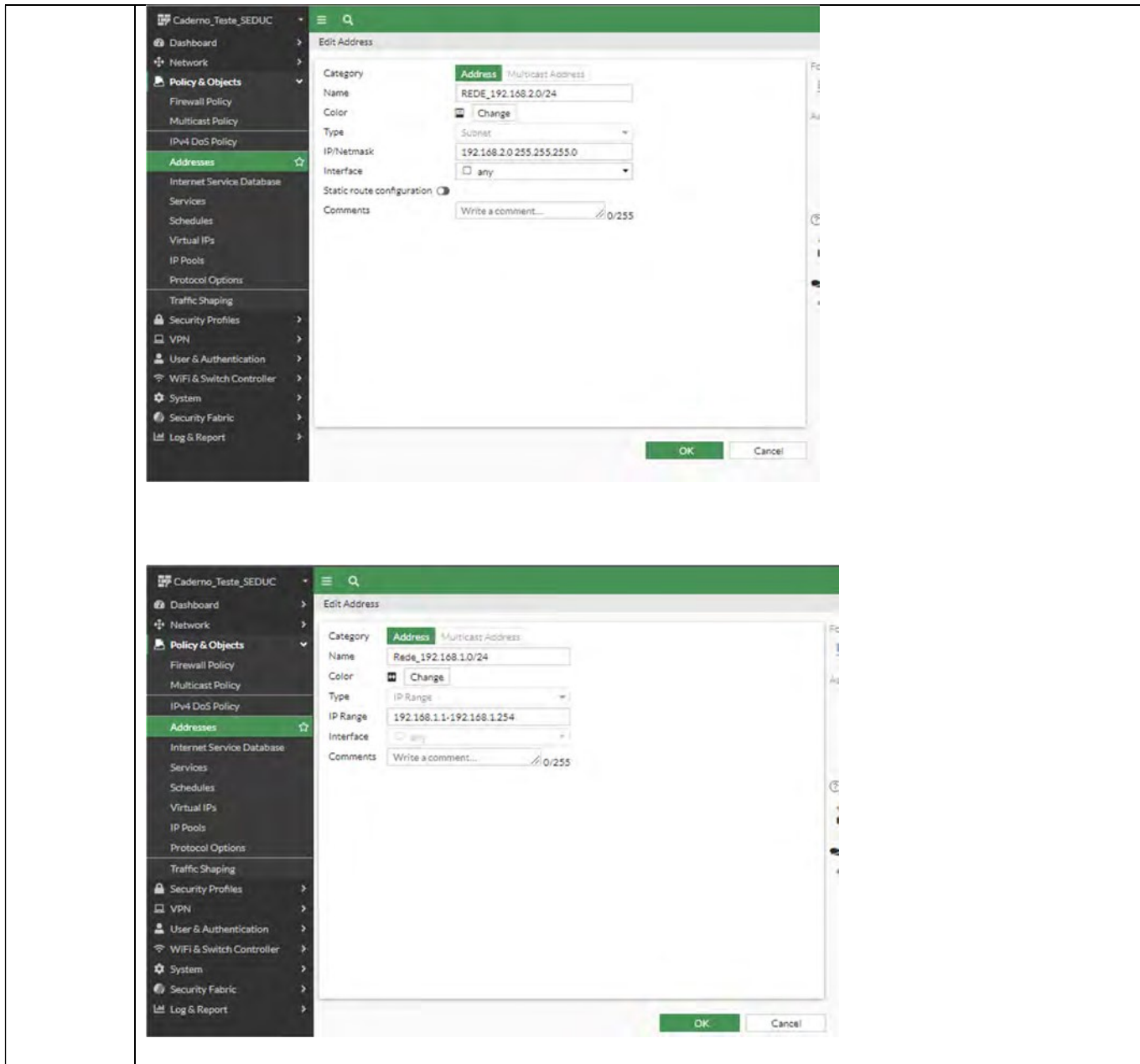
- *All Supported Files*: all files matching the file types defined in the scan profile of the FortiSandbox are forwarded.
- *Suspicious Files Only*: files classified by the antivirus as having any possibility of active content are forwarded to FortiSandbox. When using FortiGate Cloud Sandbox, we recommend selecting this option due to its submission limits.



	 <p>APT Protection Options</p> <ul style="list-style-type: none"> Treat Windows executables in email attachments as viruses <input type="checkbox"/> Send files to FortiSandbox for inspection <input checked="" type="checkbox"/> Include mobile malware protection <input checked="" type="checkbox"/> Quarantine <input type="checkbox"/>
<p>Comentário</p>	<p>https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/481589</p> <p>https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/660221/configuring-sandboxing</p>

<p>Item de Teste - 5.3.9.11</p>	<p>Toda a análise ou bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real;</p>										
<p>Objetivo do Teste</p>	<p>Validar que a aplicação faz a análise ou bloqueio de malwares e/ou códigos maliciosos em tempo real</p>										
<p>Configuração do Teste</p>	<p>Possuir 1(um) FortiGate com uma regra de firewall contendo um Perfil de Antivírus configurado.</p>										
<p>Procedimento do Teste</p>	<p>Demonstrar relatórios no site do Fabricante.</p>										
<p>Evidências</p>	<p>Conforme subitem comprovado 5.3.9.1</p> <p>TESTE OK</p> <p>Quando uma política é configurada para incluir um perfil de antivírus, todo o tráfego que corresponde a essa regra será submetido à filtragem desse perfil. Consequentemente, todo o tráfego que transita nessa regra no momento da sua aplicação será submetido a um processo de bloqueio em tempo real de malwares e códigos maliciosos.</p>  <table border="1"> <thead> <tr> <th>Name</th> <th>Source</th> <th>Destination</th> <th>Security Profiles</th> <th>Hit Count</th> </tr> </thead> <tbody> <tr> <td>Acesso_Internet</td> <td>Rede_192.168.1.0/24</td> <td>all</td> <td>Acesso_Servidores_WEB monitor-all block-high-risk certificate-inspection</td> <td>199</td> </tr> </tbody> </table>	Name	Source	Destination	Security Profiles	Hit Count	Acesso_Internet	Rede_192.168.1.0/24	all	Acesso_Servidores_WEB monitor-all block-high-risk certificate-inspection	199
Name	Source	Destination	Security Profiles	Hit Count							
Acesso_Internet	Rede_192.168.1.0/24	all	Acesso_Servidores_WEB monitor-all block-high-risk certificate-inspection	199							
<p>Comentário</p>											

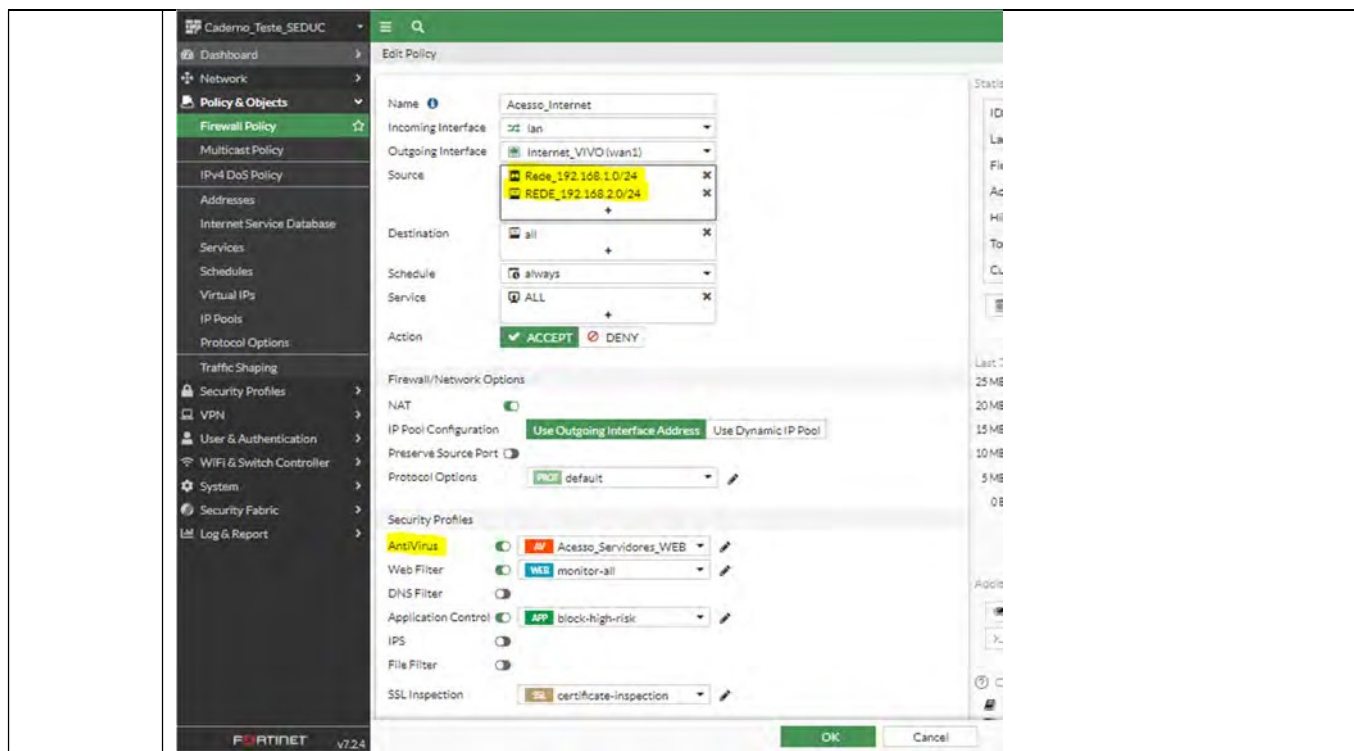
Item de Teste - 5.3.9.12	Implementar mecanismo de exceção, permitindo a criação de regras por sub-rede e endereço IP;
Objetivo do Teste	Validar se a solução implementa mecanismo de exceção, permitindo a criação de regras utilizando sub-redes e endereços de IP
Configuração do Teste	Demonstrar regras de exceção.
Procedimento do Teste	<p>Para realizar esse teste é necessário primeiro criar objetos de sub-rede e de endereço IP, navegando por Policy & Objects > Adresses > Create New é possível criar os objetos para serem usados em regras</p> <p>Navegando por Security Profiles > Antivírus > Create New é possível criar um novo profile de Antivírus onde é ativado a função de ATP (FortiGate Sandbox)</p> <p>Por último basta enquadrar os usuários e grupos criados no campo "source" da política.</p>
Evidências	 <p>TESTE OK</p> <p>1 - Criação dos objetos</p>



The image displays two screenshots of the Mikrotik WinBox interface, specifically the 'Edit Address' dialog box. Both screenshots show the 'Addresses' section selected in the left-hand navigation menu.

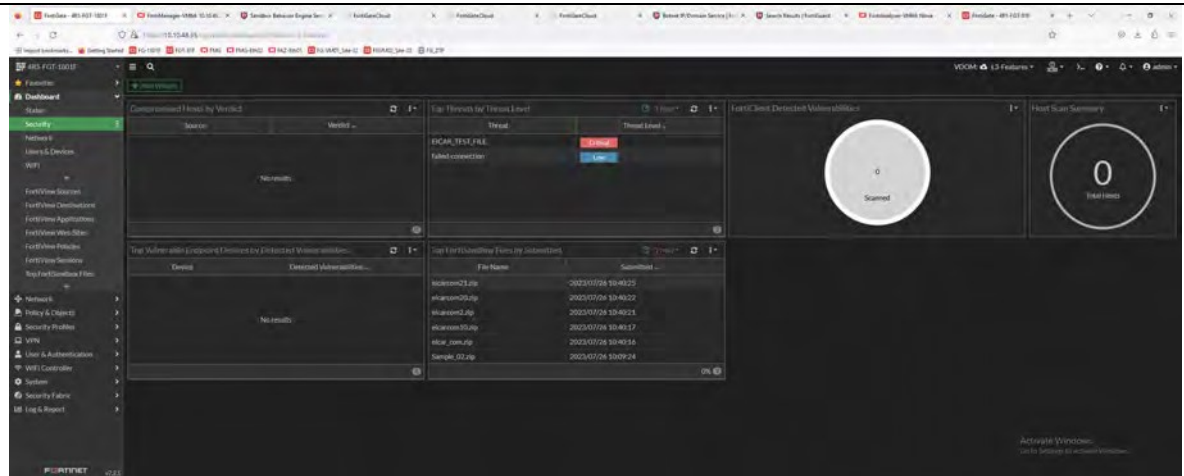
Top Screenshot: The 'Edit Address' dialog is configured for a Subnet. The 'Category' is 'Address' (with 'Multicast Address' also visible). The 'Name' is 'REDE_192.168.2.0/24'. The 'Color' is set to 'Change'. The 'Type' is 'Subnet'. The 'IP/Netmask' is '192.168.2.0 255.255.255.0'. The 'Interface' is set to 'any'. The 'Static route configuration' is disabled. The 'Comments' field contains 'Write a comment...' and '0/255'. The 'OK' and 'Cancel' buttons are visible at the bottom.

Bottom Screenshot: The 'Edit Address' dialog is configured for an IP Range. The 'Category' is 'Address' (with 'Multicast Address' also visible). The 'Name' is 'Rede_192.168.1.0/24'. The 'Color' is set to 'Change'. The 'Type' is 'IP Range'. The 'IP Range' is '192.168.1.1-192.168.1.254'. The 'Interface' is set to 'any'. The 'Comments' field contains 'Write a comment...' and '0/255'. The 'OK' and 'Cancel' buttons are visible at the bottom.



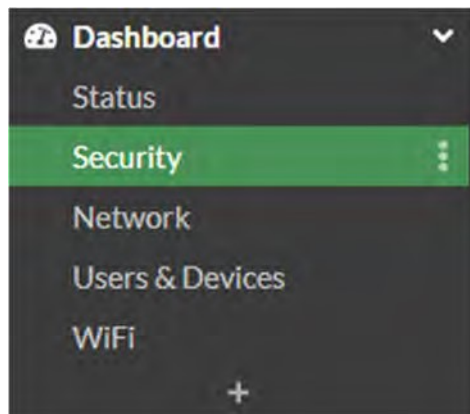
Comentário <https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/656084/firewall-policy#FirewallPolicyParameters>

Item de Teste - 5.3.9.13	Implementar através da interface gráfica mecanismo de painel de controle onde seja possível a visualização de estatísticas das ameaças;
Objetivo do Teste	Verificar se a ferramenta possui uma interface gráfica com um painel de controle onde seja possível a visualização de estatísticas das ameaças.
Configuração do Teste	Demonstrar dashboards de estatísticas de ameaças.
Procedimento do Teste	Demonstrar dashboards de estatísticas de ameaças.
Evidências	

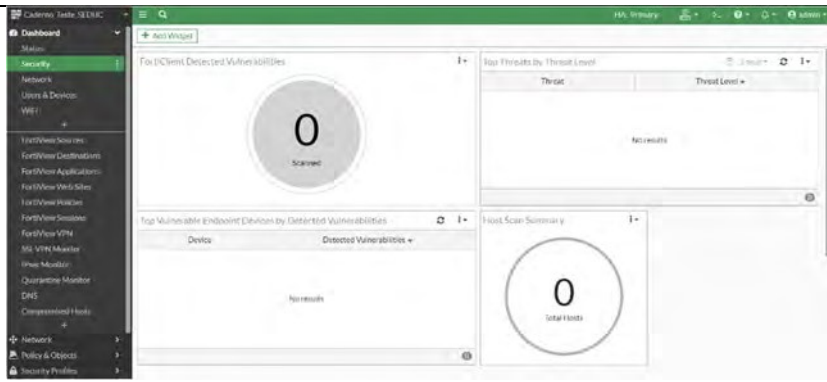


TESTE OK

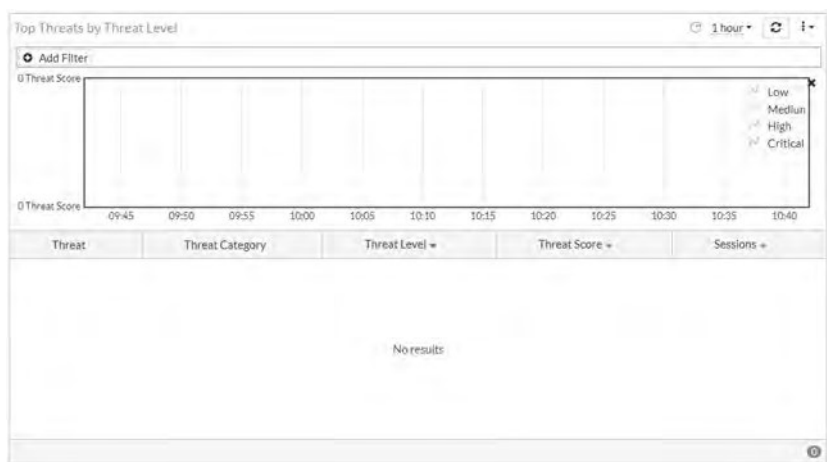
Na aba “Dashboard” temos a opção de selecionar “Security”.



Lá podemos ter acesso a diversas funcionalidades referentes a visualização de eventos de segurança detectados pela solução.



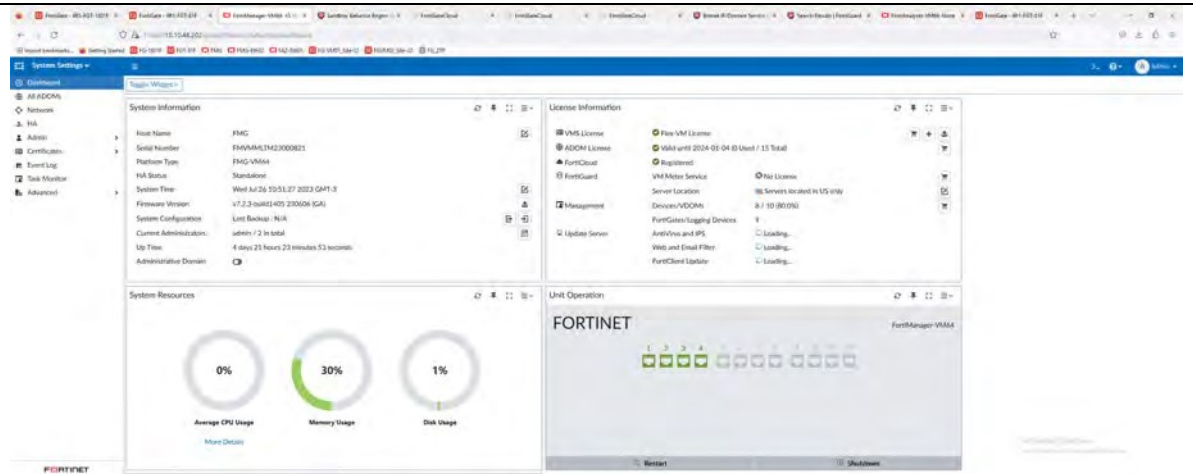
Em conjunto com isso temos outra aba de “Top Threats” que separa as ameaças que apareceram rede por nível de periculosidade.



Comentário

5.4 Solução de Gerenciamento e Controle do Firewall

Item de Teste - 5.4.1	A solução deve ser do mesmo fabricante dos demais itens ofertados no Lote 01;
Objetivo do Teste	Comprovar que a solução ofertada é da mesma fabricante que os demais itens ofertados.
Configuração do Teste	Demonstrar o FortiGate, FortiManager e FortiAnalyzer que são do fabricante Fortinet.
Procedimento do Teste	Demonstrar o FortiGate, FortiManager e FortiAnalyzer que são do fabricante Fortinet. Demonstrar o FortiGate, FortiManager e FortiAnalyzer que são do fabricante Fortinet.
Evidências	



TESTE OK



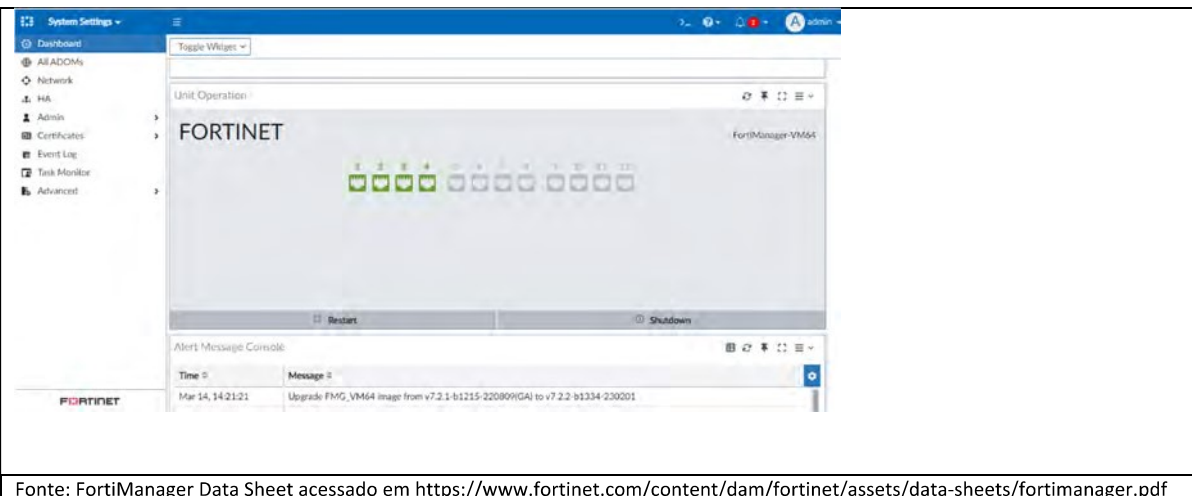
DATA SHEET
FortiManager

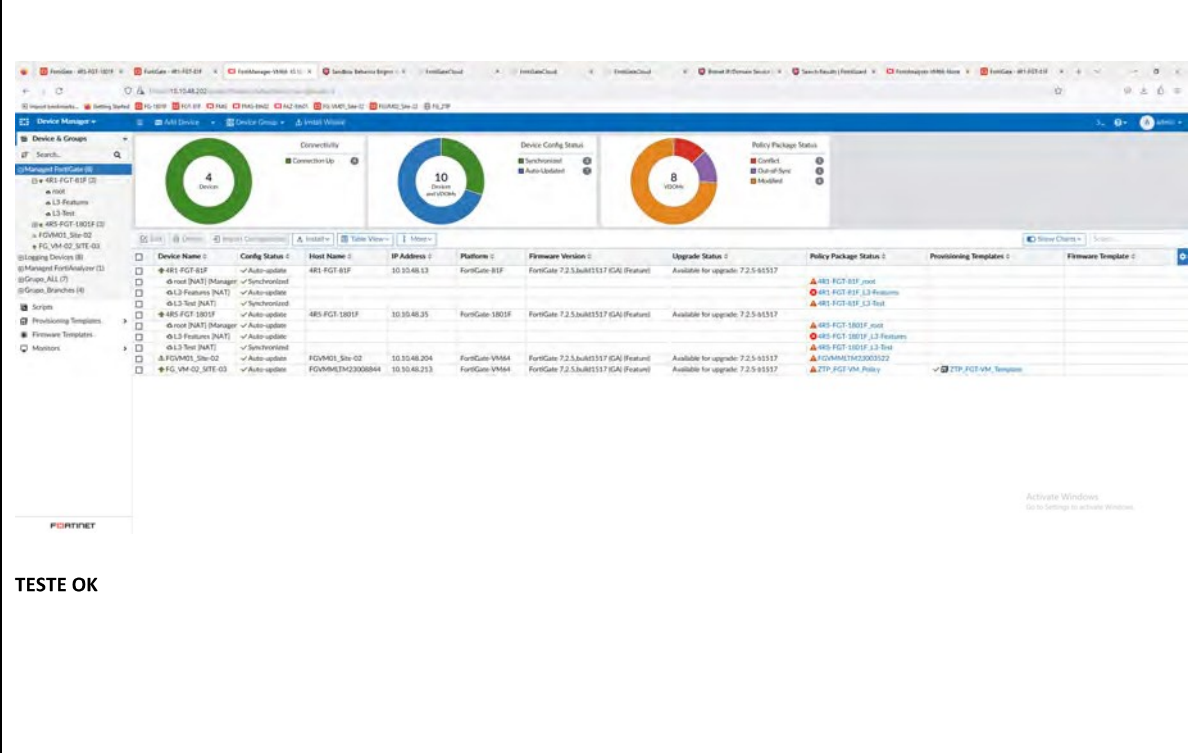
Available in:

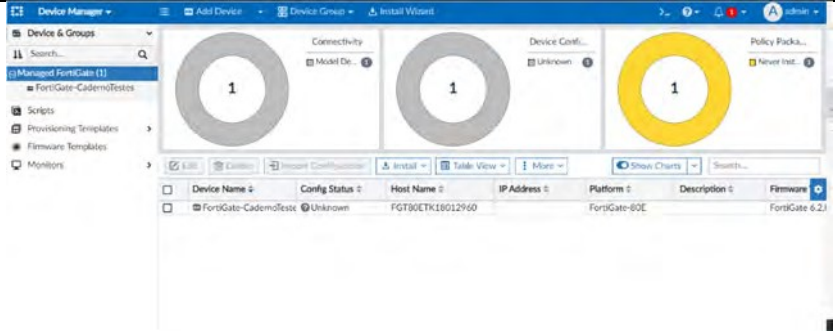


FortiManager provides automation-driven centralized management of your Fortinet devices from a single console. This process enables full administration and visibility of your network devices through streamlined provisioning and innovative automation tools.

Integrated with the Fortinet Security Fabric advanced security architecture and automation driven network operations capabilities provide a solid foundation to secure and optimize your network security.

	
Comentário	Fonte: FortiManager Data Sheet acessado em https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf

Item de Teste - 5.4.2	A solução deve ser capaz de gerenciar todos os equipamentos de Segurança de forma centralizada;
Objetivo do Teste	Comprovar que a solução consegue gerenciar todos os equipamentos de segurança de forma centralizada.
Configuração do Teste	Demonstrar que o FortiManager suporta gerenciar o FG-1801F e FG-81F
Procedimento do Teste	Para ter acesso a essa funcionalidade basta acessar o FortiManager e ir na aba de "Device Manager" que automaticamente vão mostrar os equipamentos de segurança gerenciados pelo equipamento.
Evidências	 <p>TESTE OK</p>



DATA SHEET | FortiManager

FEATURE HIGHLIGHTS

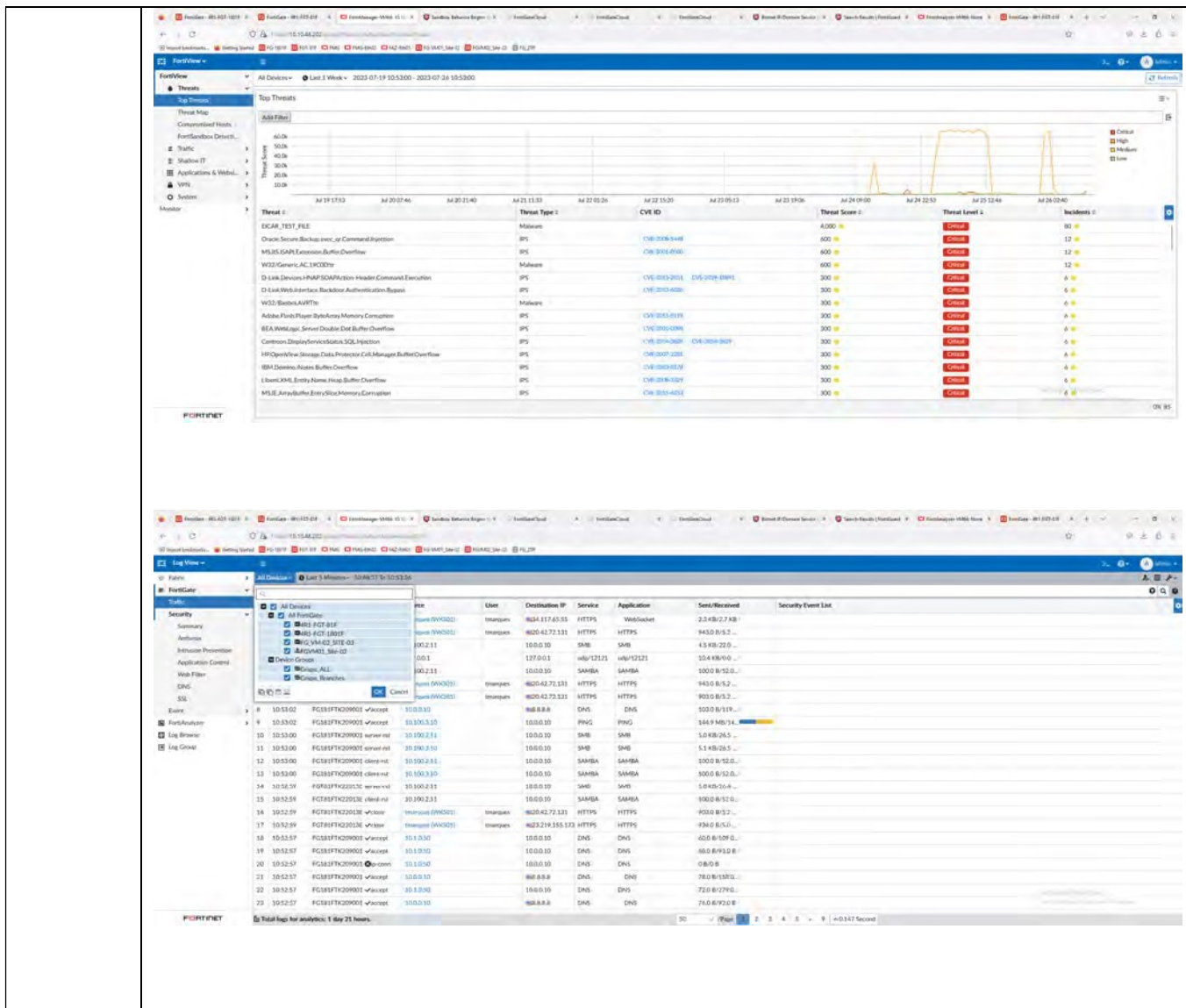
Monitoring and Visibility

Manage and Monitor with Deep Visibility

The FortiManager Device Manager provides full visibility, access, and management of Fortinet managed devices, interfaces, scripts, templates, automation, users, settings, and more. Install, edit, and delete policies. Monitor the health of FortiGate devices through customizable dashboards and widgets to see resource usage, network status of DHCP, IPsec and SSL VPN, routing, traffic shapers, and more. Easily navigate the hierarchical tree with categories for managed devices, logging devices, unauthorized devices, and customize to display as a table, folder, or a map view.

Comentário | Fonte: FortiManager Data Sheet acessado em <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf>

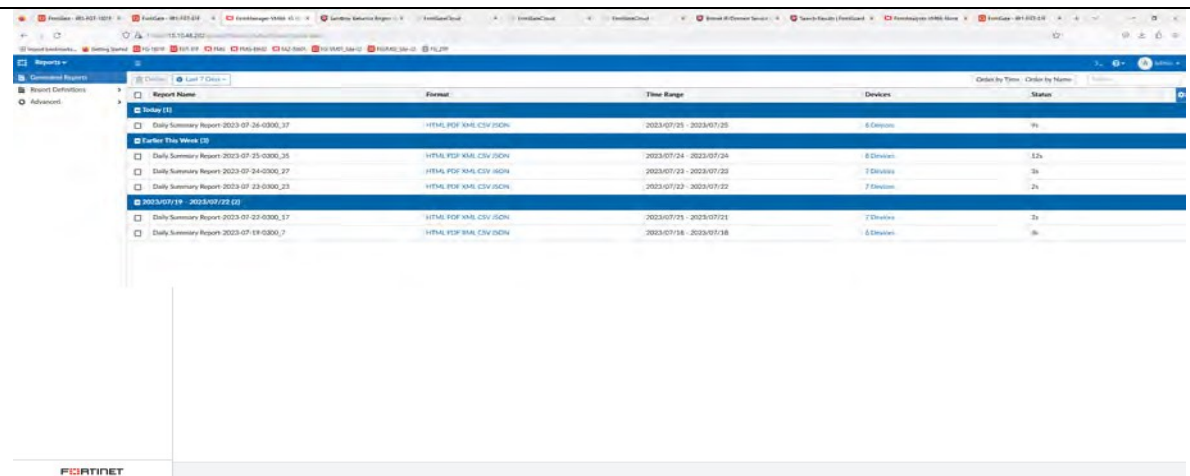
Item de Teste - 5.4.3	A solução deve ser responsável pela concentração dos logs e emissão de relatórios;
Objetivo do Teste	Comprovar que a solução é responsável pela concentração dos logs e emissão de relatórios.
Configuração do Teste	Acesso a um FortiAnalyzer com a conexão entre os equipamentos estabelecida.
Procedimento do Teste	Demonstrar configuração e ativação do FortiAnalyzer nos FortiGates.
Evidências	



The image displays two screenshots of the Fortinet FortiView interface. The top screenshot shows the 'Top Threats' section, which includes a threat map and a table of detected threats. The bottom screenshot shows the 'Log View' section, displaying a detailed traffic log with columns for ID, Action, User, Destination IP, Service, Application, Sent/Received, and Security Event List.

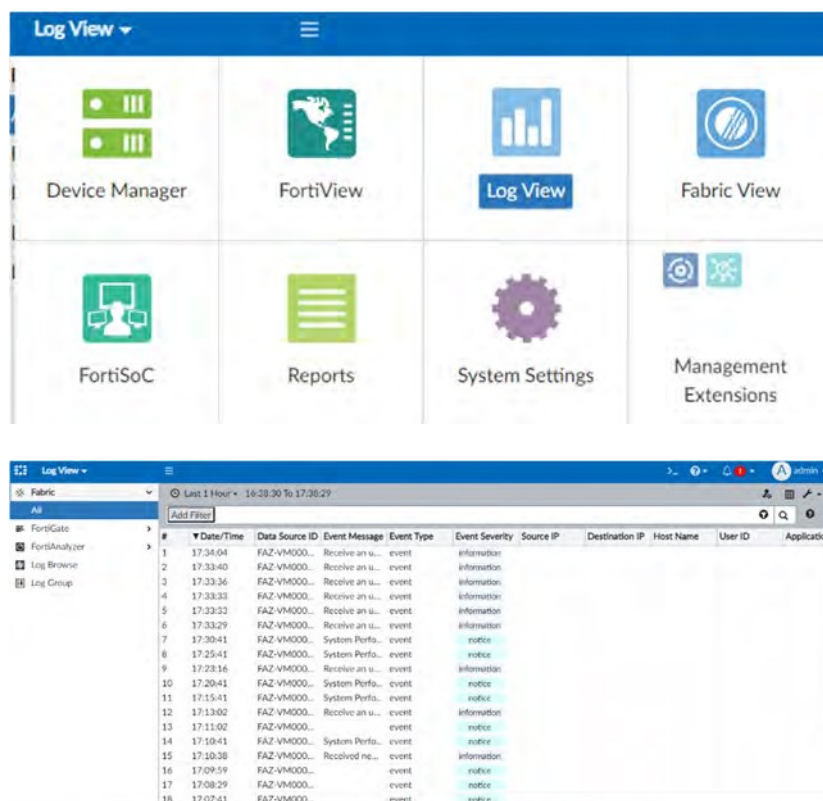
Threat ID	Threat Type	CVE ID	Threat Score	Threat Level	Incidents
ICAR_TEST_FILE	Malware		4200	Critical	81
Oracle Secure Backups exec, or Command Injection	IPS	CVE-2023-5448	600	Critical	12
MSJMS-GAPI Extension Buffer Overflow	IPS	CVE-2023-4760	600	Critical	12
W32/Generic.AC.L3X007R	Malware		600	Critical	12
D-Link Devices JNMP/SDA/PA/Box Header Command Execution	IPS	CVE-2023-2011, CVE-2023-3895	300	Critical	6
D-Link Web Interface Backdoor Authentication Bypass	IPS	CVE-2023-4020	300	Critical	6
W32/Booby-LA/RTT	Malware		300	Critical	6
Adobe Flash Player Style Array Memory Corruption	IPS	CVE-2023-5115	300	Critical	6
IEA/MS/Exp_Servlet Double DoS Buffer Overflow	IPS	CVE-2023-4095	300	Critical	6
Common Desktop Environment CDE Injection	IPS	CVE-2023-3287, CVE-2023-3289	300	Critical	6
HP OpenView Storage Data Protector CUI Manager Buffer Overflow	IPS	CVE-2023-2284	300	Critical	6
IBM Domino Admins Buffer Overflow	IPS	CVE-2023-0131	300	Critical	6
Libevent XML Entity Name Heap Buffer Overflow	IPS	CVE-2023-1029	300	Critical	6
MSIE Array Buffer Entry Stack Memory Corruption	IPS	CVE-2023-4031	300	Critical	6

ID	Action	User	Destination IP	Service	Application	Sent/Received	Security Event List
10	Accept	Interscan	823.417.63.53	HTTPS	WebContent	2.5 KB/2.7 KB	
11	Accept	Interscan	8202.42.72.131	HTTPS	HTTPS	943.0 B/5.2 ...	
12	Accept		10.0.0.10	SMB	SMB	4.5 KB/22.0 ...	
13	Accept		127.0.0.1	http/12121	http/12121	15.4 KB/0.0 ...	
14	Accept		10.0.0.10	SAMBA	SAMBA	100.0 B/52.0 ...	
15	Accept	Interscan	8202.42.72.131	HTTPS	HTTPS	943.0 B/5.2 ...	
16	Accept	Interscan	8202.42.72.131	HTTPS	HTTPS	903.0 B/119 ...	
17	Accept		10.0.0.10	DNS	DNS	144.9 MB/34 ...	
18	Accept		10.0.0.10	SSH	SSH	5.0 KB/0.5 ...	
19	Accept		10.0.0.10	SSH	SSH	1.1 KB/0.5 ...	
20	Accept		10.0.0.10	SAMBA	SAMBA	100.0 B/52.0 ...	
21	Accept		10.0.0.10	SAMBA	SAMBA	300.0 B/52.0 ...	
22	Accept		10.0.0.10	SMB	SMB	5.0 KB/50.8 ...	
23	Accept		10.0.0.10	SAMBA	SAMBA	100.0 B/52.0 ...	
24	Accept		10.0.0.10	SAMBA	SAMBA	100.0 B/52.0 ...	
25	Accept		10.0.0.10	DNS	DNS	60.0 B/109.0 ...	
26	Accept		10.0.0.10	DNS	DNS	88.0 B/93.0 ...	
27	Accept		10.0.0.10	DNS	DNS	0.0 B/0 ...	
28	Accept		10.0.0.10	DNS	DNS	78.0 B/180.0 ...	
29	Accept		10.0.0.10	DNS	DNS	72.0 B/179.0 ...	
30	Accept		10.0.0.10	DNS	DNS	74.0 B/170.0 ...	

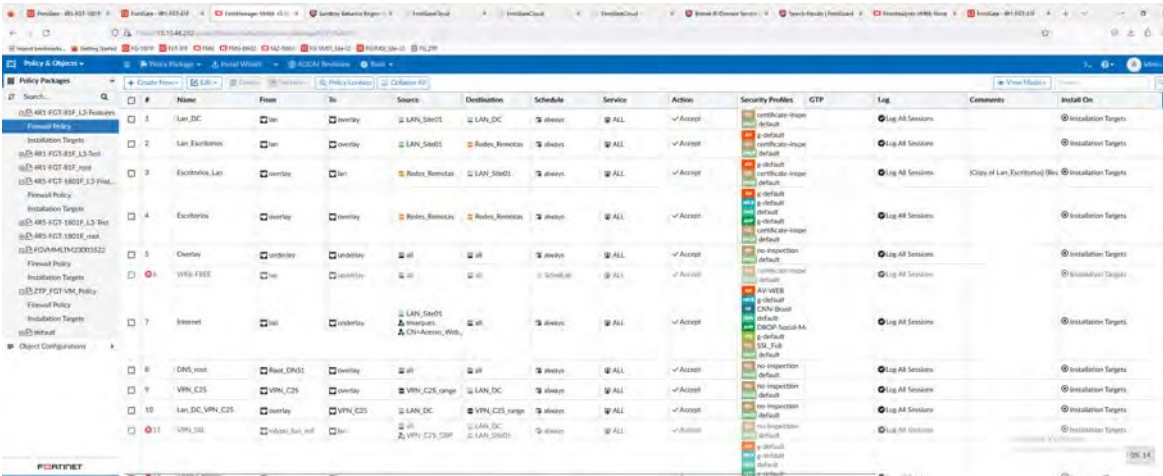


TESTE OK

Para acessar essa funcionalidade basta acessar o "Log View".



Comentário

Item de Teste - 5.4.5	O gerenciamento de políticas será realizado em um único ponto centralizado;
Objetivo do Teste	Validar que o equipamento de gerência realiza esse gerenciamento das políticas em um só lugar.
Configuração do Teste	Demonstrar o FortiManager com os FortiGates integrados
Procedimento do Teste	<p>Para ter acesso as políticas dos equipamentos gerenciados, primeiro tem de ser feita essa importação das políticas.</p> <p>Após isso, basta ir ao canto superior esquerdo e selecionar a aba "Policy & Objects" e assim ficará visível as políticas de todos os equipamentos gerenciados.</p>
Evidências	 <p>TESTE OK</p>

1

Connectivity

- Quick Install (Device DB)
- Install Wizard
- Import Configuration
- Re-install Policy
- Policy Package Diff
- Configuration
- Edit
- Delete
- Grouping
- Add VDOM
- Run Script
- Edit Variable Mapping
- Refresh Device
- Fabric Topology
- Install VM License
- Firmware Upgrade

Policy & Objects
Policy Package
Install Wizard
ADOM Revisions
Tools

Device Manager

Policy & Objects

AP Manager

VPN Manager

Fabric View

FortiGuard

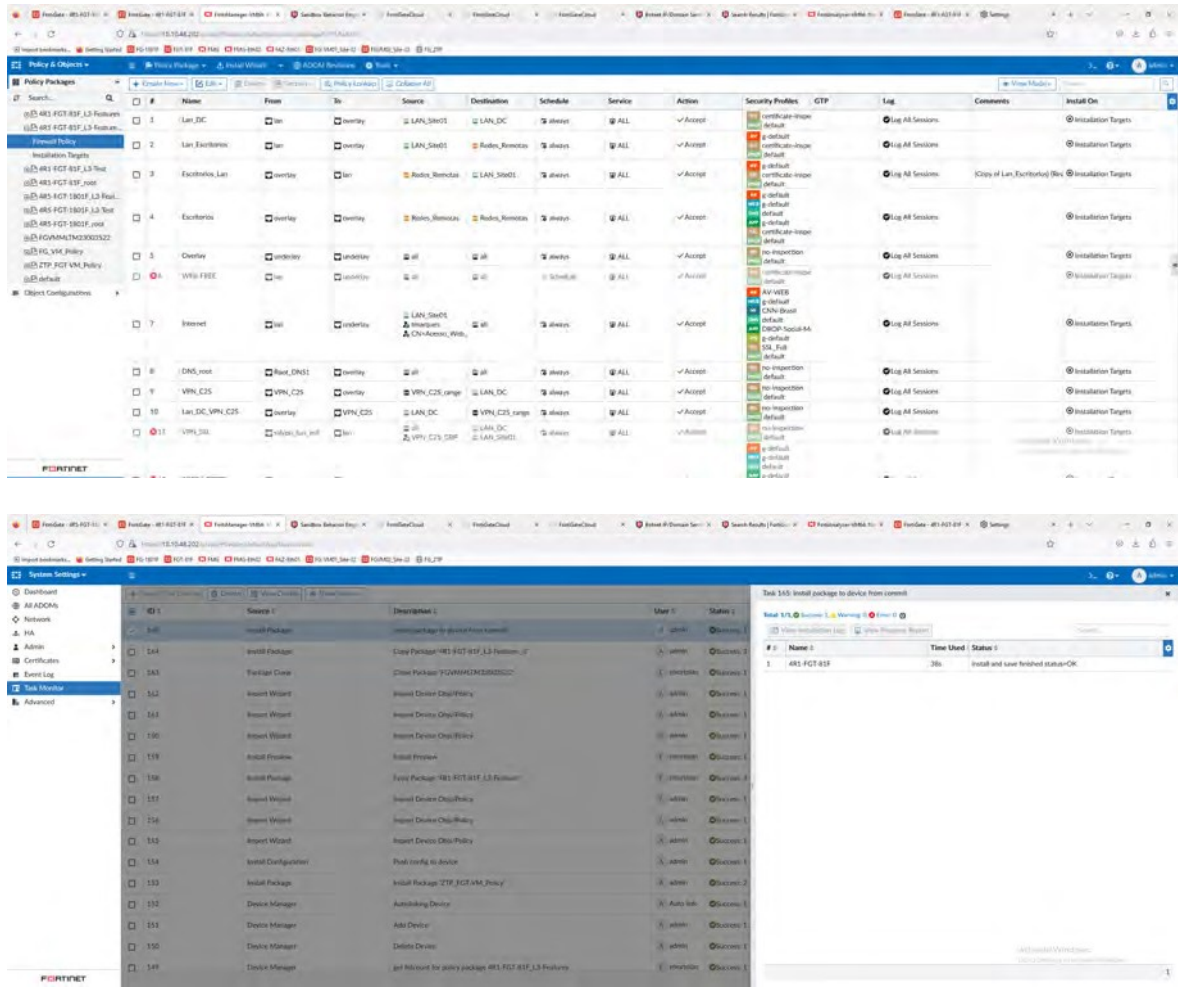
FortiSwitch Manager

Extender Manager

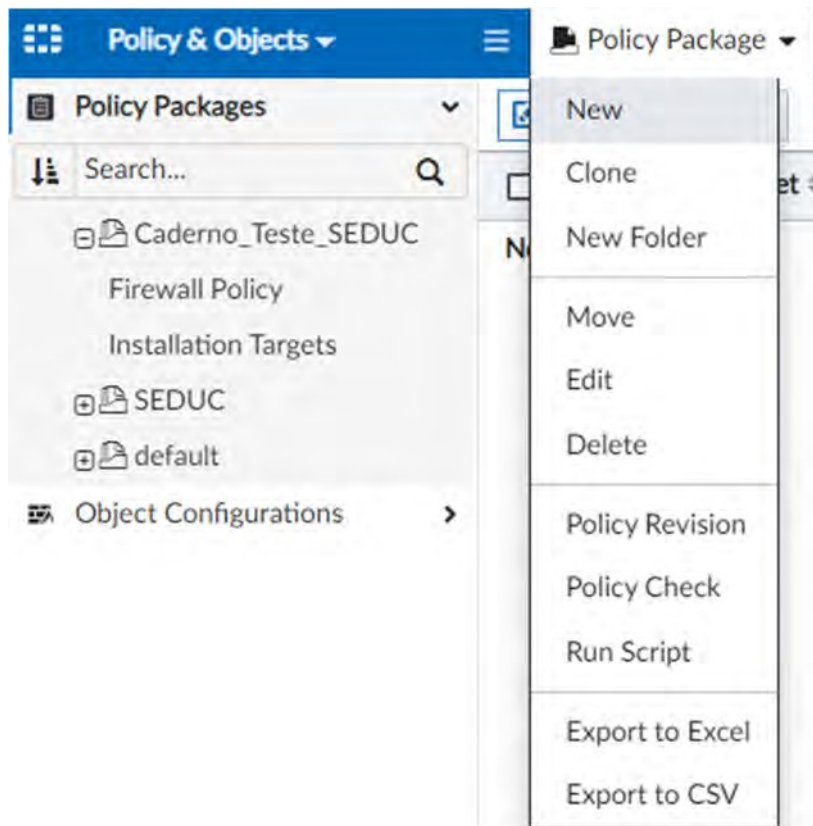
System Settings

Policy Packages	#	Name	From	To	Source	Destination	Schedule	Service
FortiGate-CademoTestes	1	Implicit (2-2 / Total: 1)	any	wan1	all	all	always	ALL
IPsec Policy	2	Implicit Deny	any	any	all	all	always	ALL

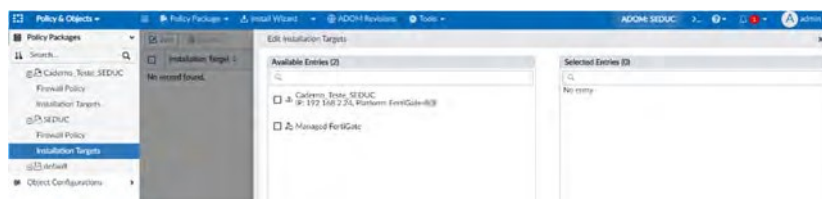
Comentário

Item de Teste - 5.4.6	Permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os equipamentos;
Objetivo do Teste	Validar se o equipamento de gerência centralizada possui a funcionalidade de criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os equipamentos.
Configuração do Teste	Demonstrar a configuração do Pacote de Políticas
Procedimento do Teste	Demonstrar a configuração do Pacote de Políticas
Evidências	

Na aba de "Policy & Objects "é possível criar um novo pacote de políticas.

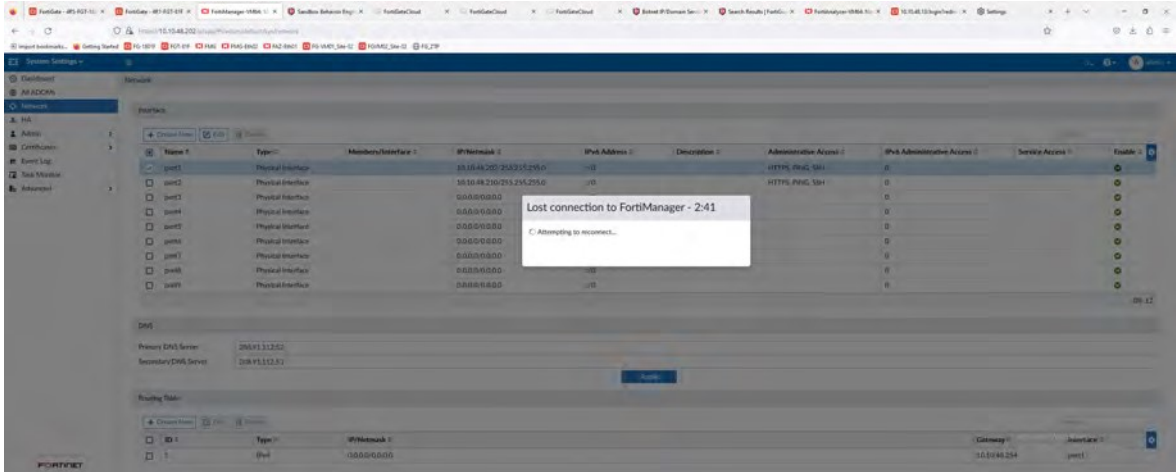
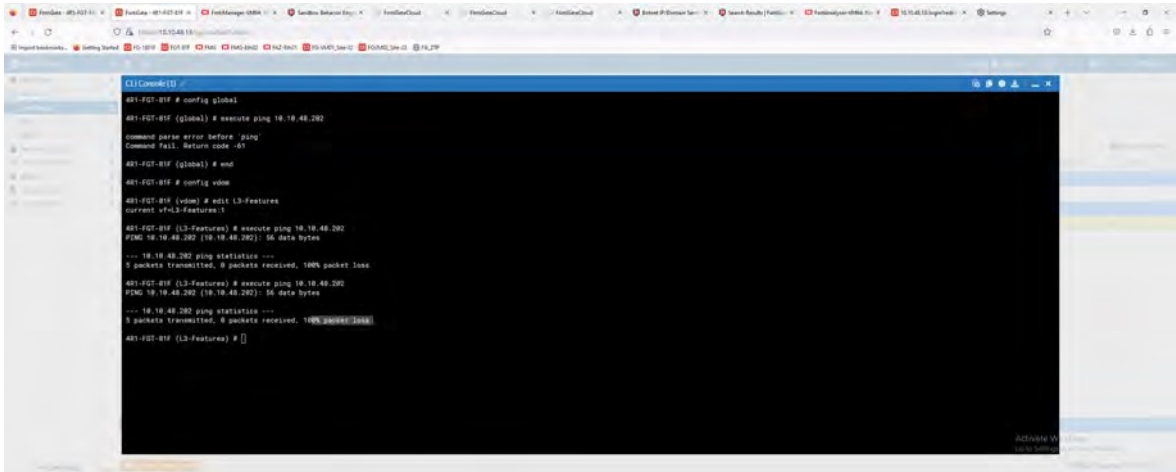


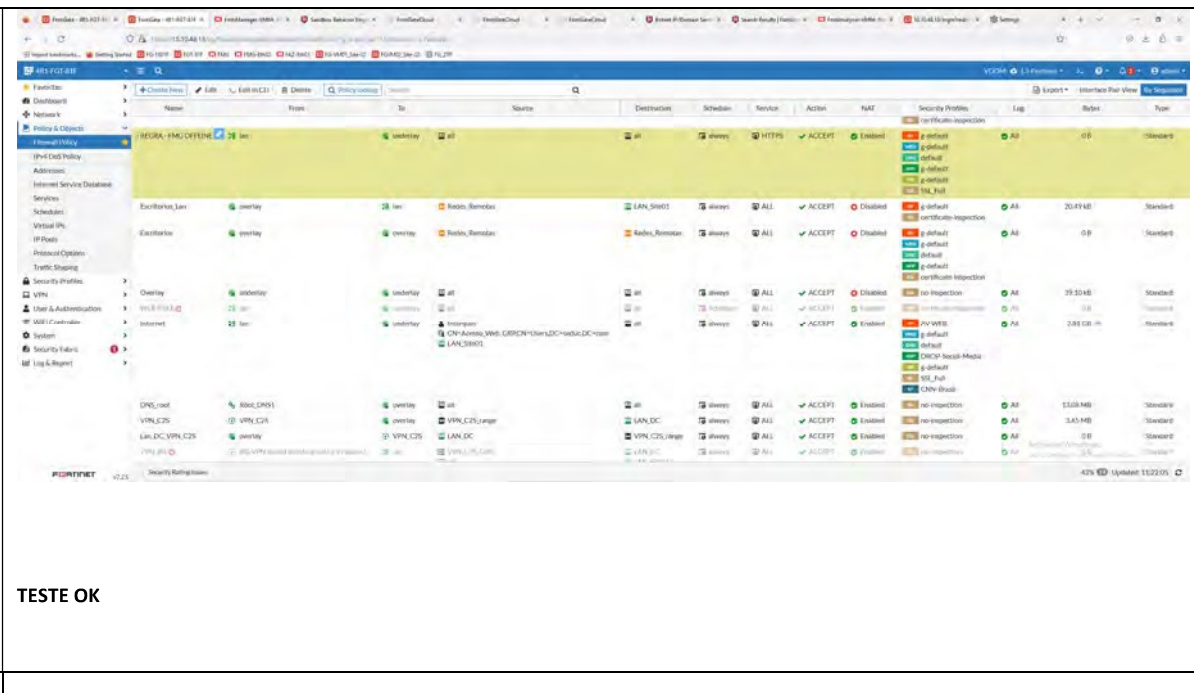
Como também, selecionar quais equipamentos receberão esse pacote recém-criado. Para isto, basta acessar a guia "Installation Targets", em seguida ir em "Edit" e selecionar os equipamentos desejados.

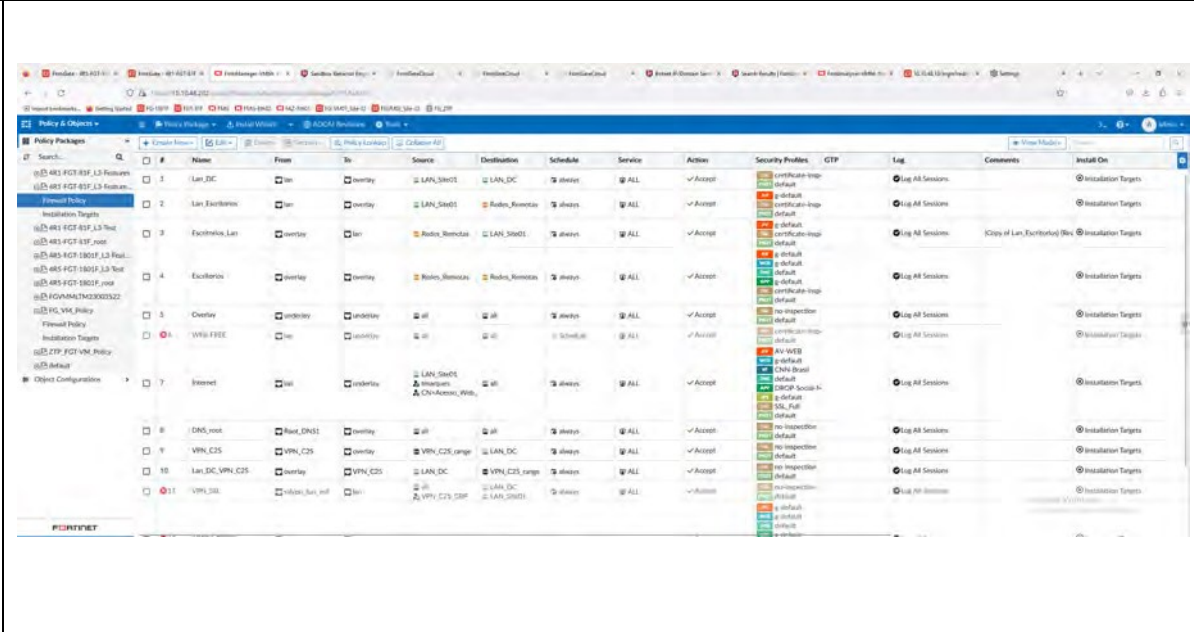


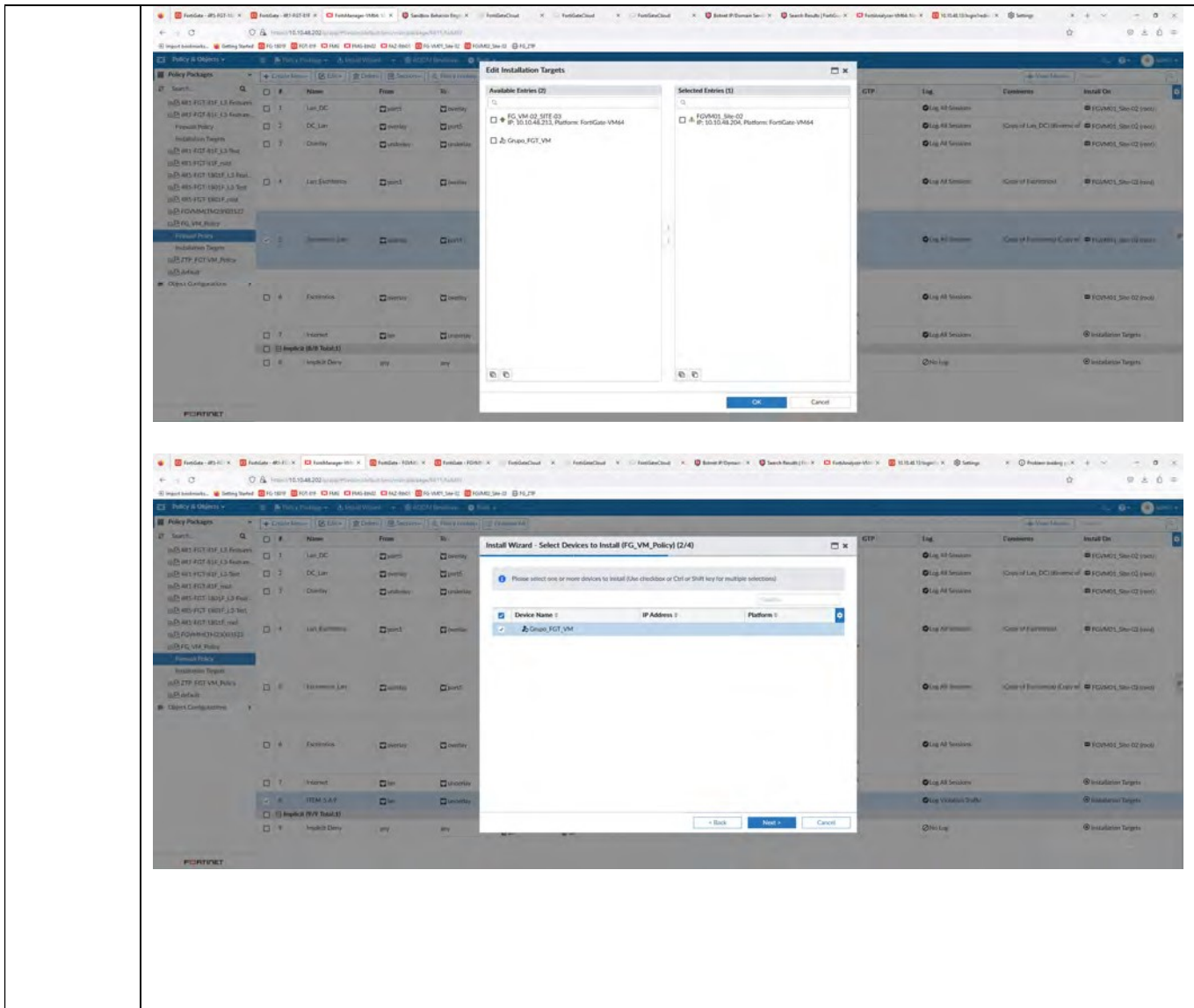
Comentário	Fonte: FortiManager Administration Guide acessado em: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/04f80bb3-e03c-11ec-bb32-fa163e15d75b/FortiManager-7.2.1-Administration_Guide.pdf
-------------------	---

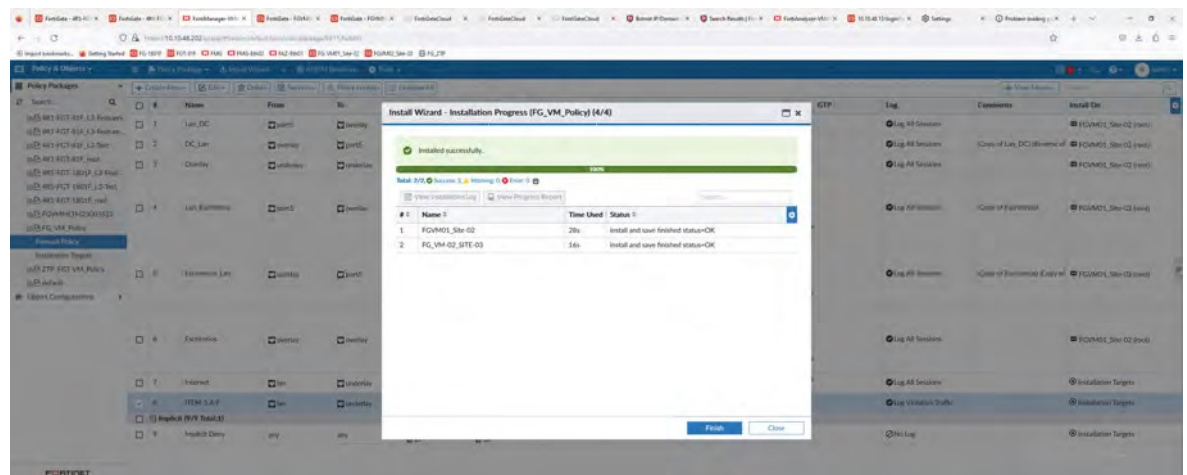
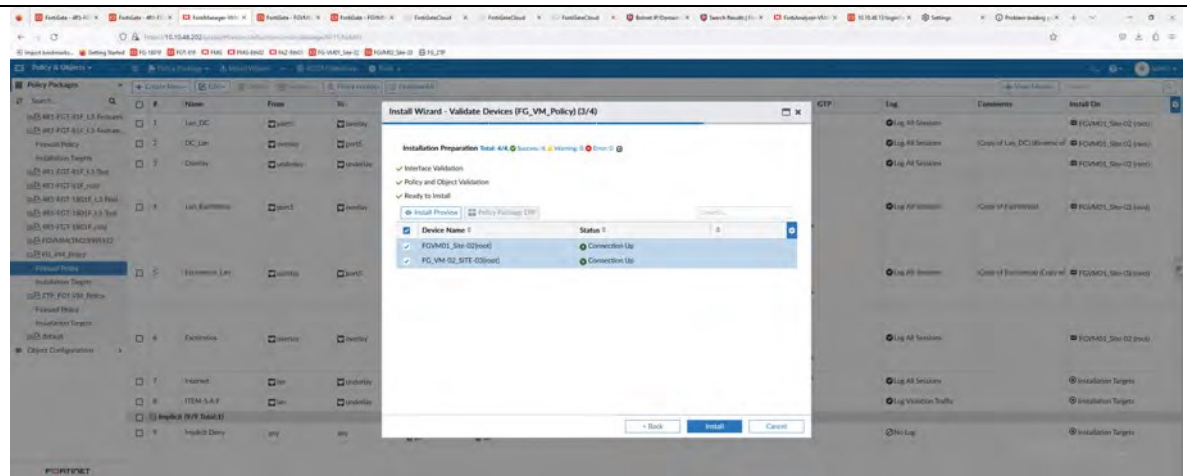
Item de Teste - 5.4.8	Caso a Solução de Gerenciamento Centralizada torne-se indisponível, todos os seus gateways gerenciados devem continuar funcionando normalmente, permitindo a administração, operação e total controle sobre cada gateway enquanto a gerência continuar indisponível;
Objetivo do Teste	Demonstrar que o gateway independe da gerência para funcionar plenamente.

<p>Configuração do Teste</p>	<p>Tornar indisponível a gerência e demonstrar o Firewall</p>
<p>Procedimento do Teste</p>	<p>Tornar indisponível a gerência e demonstrar o Firewall</p>
<p>Evidências</p>	  <p>The first screenshot shows the FortiGate GUI configuration page for interfaces. A modal dialog box is displayed in the center with the text: "Lost connection to FortiManager - 2:41" and "Attempting to reconnect...". The background shows a table of interfaces with columns for Name, Type, Member/Interface, IP/Network, IPV6 Address, Description, Administrative Access, IPv6 Administrative Access, and Service Access.</p> <p>The second screenshot shows the FortiGate CLI terminal. The user is in the global configuration mode and has executed several commands: <code>config global</code>, <code>execute ping 10.10.48.202</code>, <code>comment ping error before ping</code>, <code>Command fail. Return code -67</code>, <code>end</code>, <code>config vdom</code>, <code>edit (vdom) # set l3-features</code>, <code>current vdom-features</code>, <code>execute ping 10.10.48.202</code>, <code>ping 10.10.48.202 (10.10.48.202): 56 data bytes</code>, <code>ping 10.10.48.202 (10.10.48.202): 56 data bytes</code>, <code>ping 10.10.48.202 (10.10.48.202): 56 data bytes</code>, and <code>end</code>.</p>

<p>TESTE OK</p>	
<p>Comentário</p>	

<p>Item de Teste - 5.4.9</p>	<p>A Solução de Gerenciamento Centralizada deve permitir a instalação de políticas individuais (somente para 1 gateway), para um grupo de gateways e para todos os seus gateways gerenciados, não sendo aceito soluções com aplicações de apenas uma das opções;</p>
<p>Objetivo do Teste</p>	<p>Validar se a ferramenta permite a instalação de políticas individuais (somente para 1 gateway), para um grupo de gateways e para todos os seus gateways gerenciados.</p>
<p>Configuração do Teste</p>	<p>Demonstrar distribuição de política por gateway.</p>
<p>Procedimento do Teste</p>	

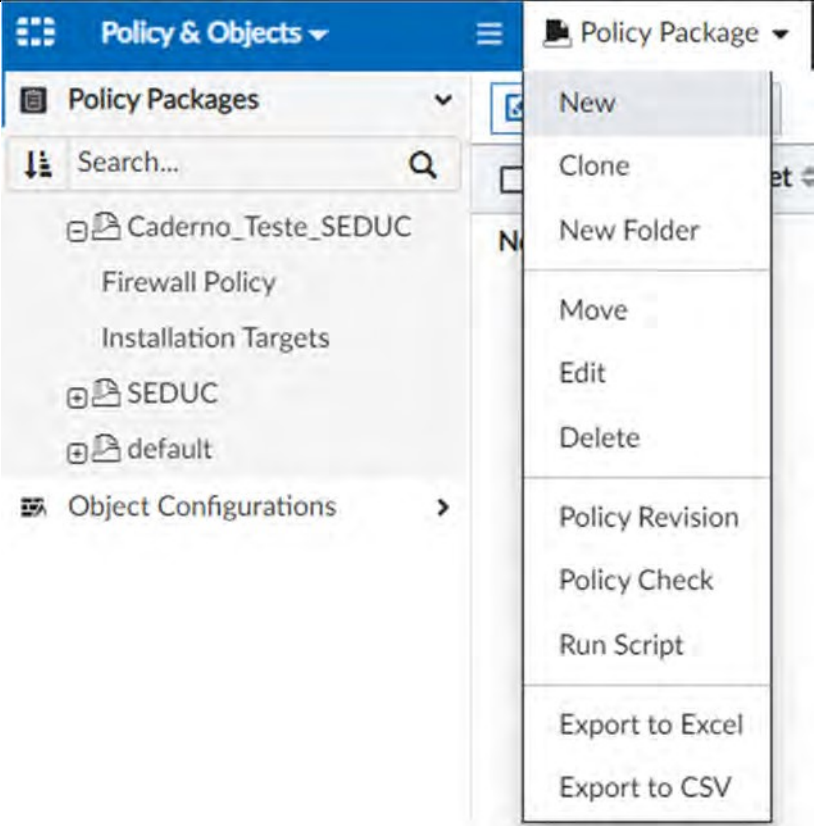
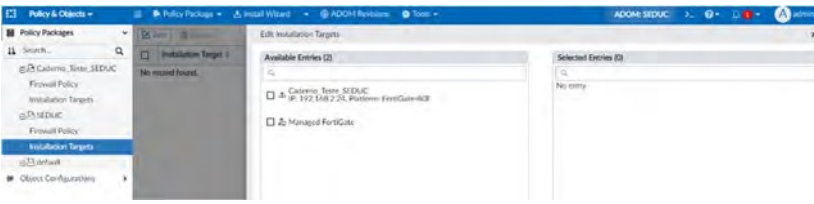




TESTE OK

Na aba de “Policy & Objects” é possível criar um novo pacote de políticas.

Como também, selecionar quais equipamentos receberão esse pacote recém-criado. Para isto, basta acessar a guia “Installation Targets”, em seguida ir em “Edit” e selecionar os equipamentos desejados.

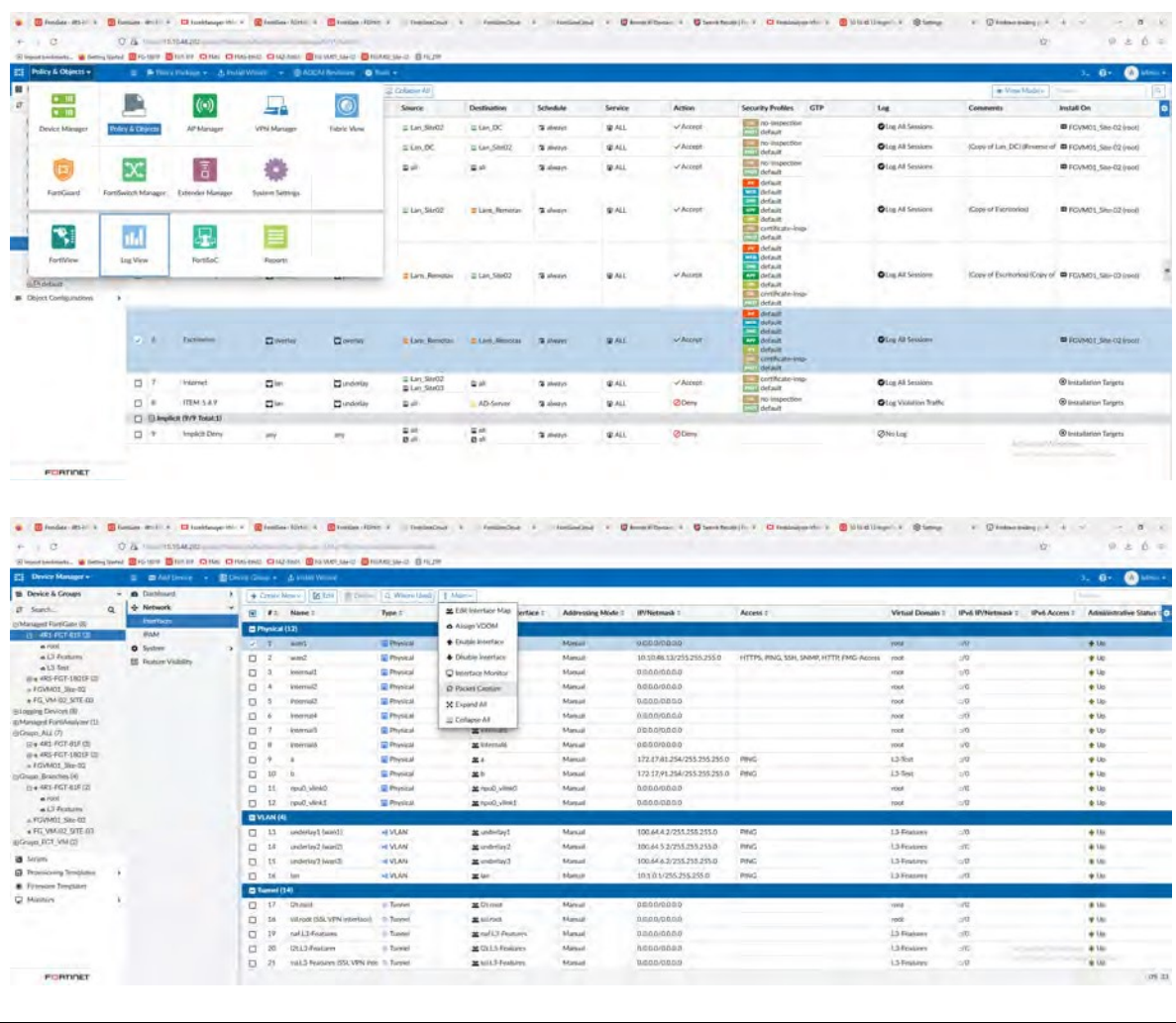
<p>Evidências</p>	 
<p>Comentário</p>	<p>Fonte: FortiManager Administration Guide acessado em: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/04f80bb3-e03c-11ec-bb32-fa163e15d75b/FortiManager-7.2.1-Administration_Guide.pdf</p>

<p>Item de Teste - 5.4.10</p>	<p>Possibilitar a execução das seguintes tarefas: criação e administração de políticas de firewall e controle de aplicação; criação e administração de políticas de IPS, antivírus e anti-spyware; criação e administração de políticas de conteúdo Web e filtro de URL; monitoração de logs; ferramentas de investigação de logs; debugging; troubleshooting; visualização de eventos; dashboards; captura de pacotes;</p>
<p>Objetivo do Teste</p>	<p>Verificar se a ferramenta tem a capacidade de executar as seguintes tarefas: criação e administração de políticas de firewall e controle de aplicação; criação e administração de políticas de IPS, antivírus e anti-spyware; criação e administração de políticas de conteúdo Web e filtro de URL; monitoração de logs; ferramentas de investigação de logs; debugging; troubleshooting; visualização de eventos; dashboards; captura de pacotes;</p>

Configuração do Teste

Demonstrar operação do FortiManager

Procedimento do Teste

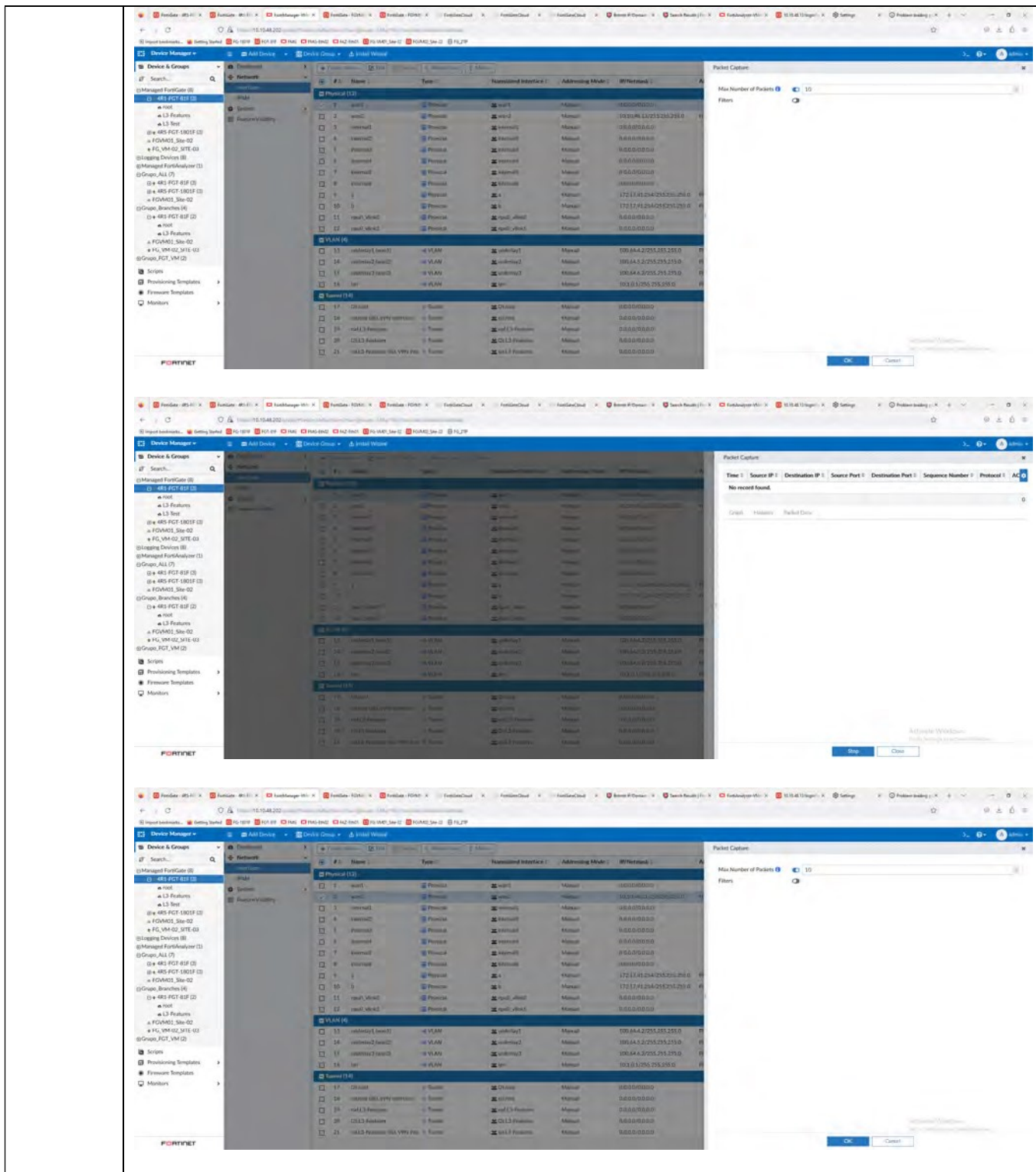


The top screenshot displays the 'Policy & Objects' configuration page in FortiManager. It shows a table of security policies with columns for Source, Destination, Schedule, Service, Action, Security Profiles, GTP, Log, and Comments. The policies are listed as follows:

Source	Destination	Schedule	Service	Action	Security Profiles	GTP	Log	Comments	Install On
Lin_Site02	Lin_DC	always	ALL	Accept	no-inspection, default		Log All Sessions		FGM01_Site-02 (root)
Lin_DC	Lin_Site02	always	ALL	Accept	no-inspection, default		Log All Sessions	Copy of Lin_DC (owner of	FGM01_Site-02 (root)
all	all	always	ALL	Accept	no-inspection, default		Log All Sessions	Copy of Extended	FGM01_Site-02 (root)
Lin_Site02	Lin_Remote1	always	ALL	Accept	no-inspection, default		Log All Sessions	Copy of Extended (Copy of	FGM01_Site-02 (root)
Lin_Remote1	Lin_Site02	always	ALL	Accept	no-inspection, default		Log All Sessions	Copy of Extended (Copy of	FGM01_Site-02 (root)
Lin_Remote1	Lin_Remote2	always	ALL	Accept	no-inspection, default		Log All Sessions		FGM01_Site-02 (root)
Internet	in	undelay	Lin_Site02	all	always	ALL	Accept	Log All Sessions	Insulation Targets
ITM 5.4.7	in	undelay	Lin_Site03	all	always	ALL	Deny	Log Violation Traffic	Insulation Targets
Implicit (IPv4 Subnet)	any	any	all	all	always	ALL	Deny	No Log	Insulation Targets
Implicit Deny	any	any	all	all	always	ALL	Deny	No Log	Insulation Targets

The bottom screenshot displays the 'Device Manager' configuration page. It shows a table of network devices with columns for #, Name, Type, Interface, Addressing Mode, IP/Network, Access, Virtual Domain, IPV4/Network, IPV4/Access, and Administrative Status. The devices are listed as follows:

#	Name	Type	Interface	Addressing Mode	IP/Network	Access	Virtual Domain	IPV4/Network	IPV4/Access	Administrative Status
1	wan1	Physical	Manual	0.0.0.0/0.0.0.0			root	-/0		Use
2	wan2	Physical	Manual	10.10.86.13/255.255.255.0	HTTP, PNG, SSH, SANMP, HTTP, PNG, Access	root	-/0			Use
3	internal1	Physical	Manual	0.0.0.0/0.0.0.0		root	-/0			Use
4	internal2	Physical	Manual	0.0.0.0/0.0.0.0		root	-/0			Use
5	internal3	Physical	Manual	0.0.0.0/0.0.0.0		root	-/0			Use
6	internal4	Physical	Manual	0.0.0.0/0.0.0.0		root	-/0			Use
7	internal5	Physical	Manual	0.0.0.0/0.0.0.0		root	-/0			Use
8	internal6	Physical	Manual	0.0.0.0/0.0.0.0		root	-/0			Use
9	4	Physical	Manual	172.17.1.254/255.255.255.0	PNG	1.3-Test	-/0			Use
10	6	Physical	Manual	172.17.1.254/255.255.255.0	PNG	1.3-Test	-/0			Use
11	vpn0_vh040	Physical	Manual	0.0.0.0/0.0.0.0		root	-/0			Use
12	vpn0_vh041	Physical	Manual	0.0.0.0/0.0.0.0		root	-/0			Use
VLAN (4)										
13	undelay1_vlan1	VLAN	Manual	100.64.4.2/255.255.255.0	PNG	1.3-Testers	-/0			Use
14	undelay2_vlan2	VLAN	Manual	100.64.5.2/255.255.255.0	PNG	1.3-Testers	-/0			Use
15	undelay3_vlan3	VLAN	Manual	100.64.6.2/255.255.255.0	PNG	1.3-Testers	-/0			Use
16	lan	VLAN	Manual	10.1.1.255/255.255.0	PNG	1.3-Testers	-/0			Use
Tunnel (4)										
17	01-ssl	Tunnel	Manual	0.0.0.0/0.0.0.0		root	-/0			Use
18	01-ssl-VPN-internal	Tunnel	Manual	0.0.0.0/0.0.0.0		root	-/0			Use
19	01-L3-Features	Tunnel	Manual	0.0.0.0/0.0.0.0		1.3-Testers	-/0			Use
20	01-L3-Features	Tunnel	Manual	0.0.0.0/0.0.0.0		1.3-Testers	-/0			Use
21	01-L3-Features (SSL-VPN-Int)	Tunnel	Manual	0.0.0.0/0.0.0.0		1.3-Testers	-/0			Use



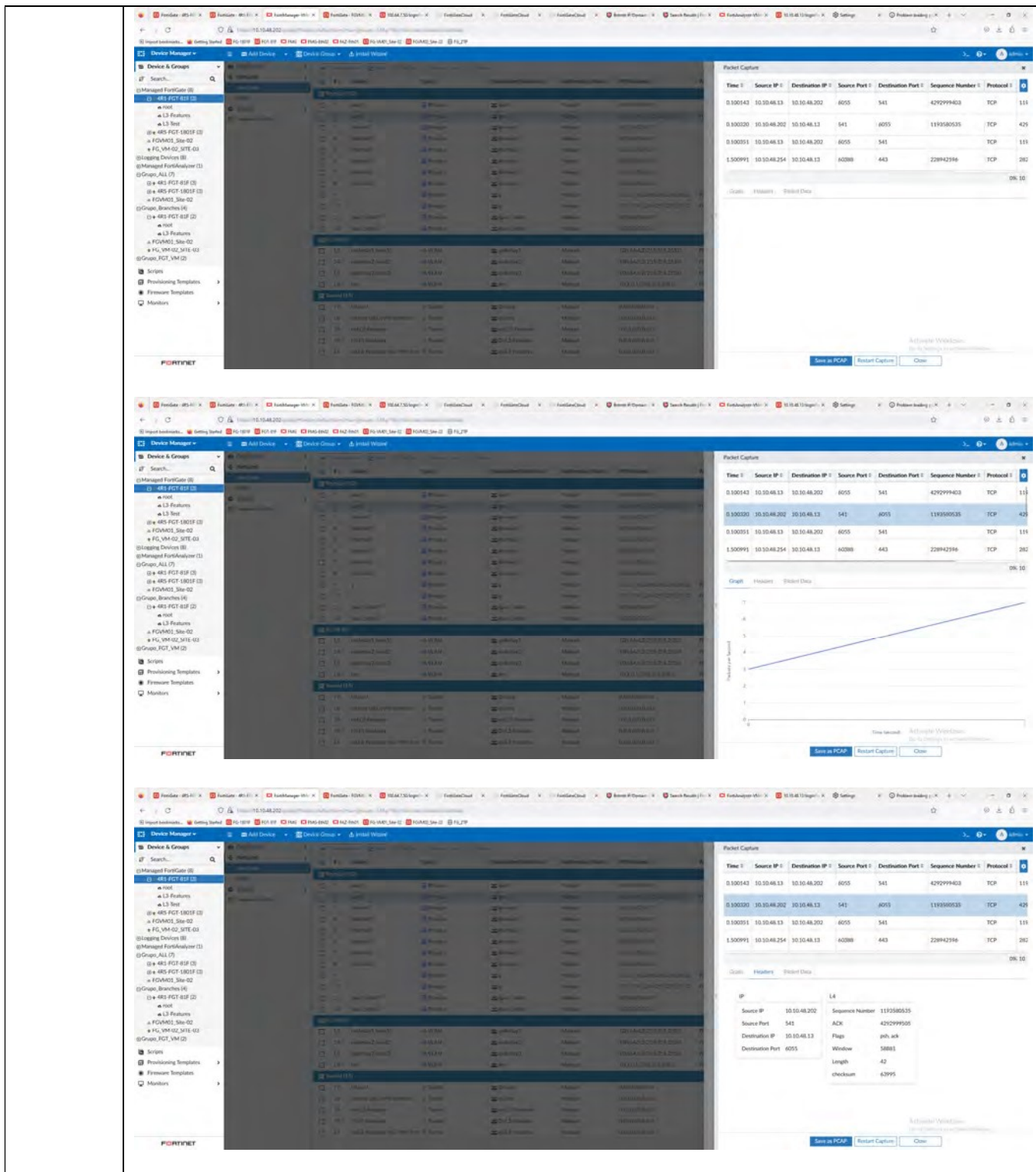
The image displays three sequential screenshots of the Fortinet FortiGate web interface, illustrating network configuration and packet capture operations.

Top Screenshot: Shows the 'Device Manager' view for a FortiGate device. The 'Physical' interface list is expanded, showing details for interfaces 'port1' through 'port12'. The 'VLAN' section shows configurations for 'vlan1' through 'vlan4'. The 'Packet Capture' dialog is open, with 'Max Number of Packets' set to 10 and 'Filters' empty. The 'OK' button is highlighted.

Middle Screenshot: Shows the same configuration view, but the 'Packet Capture' dialog now displays 'No record found.' and '0' records. The 'Stop' button is highlighted.

Bottom Screenshot: Shows the configuration view again, with the 'Packet Capture' dialog open and 'Max Number of Packets' set to 10. The 'OK' button is highlighted.

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



The image displays three sequential screenshots of the Fortinet FortiGate web interface, specifically the Packet Capture (PCAP) analysis tool. Each screenshot shows a different view of the captured traffic data.

Top Screenshot: Packet List

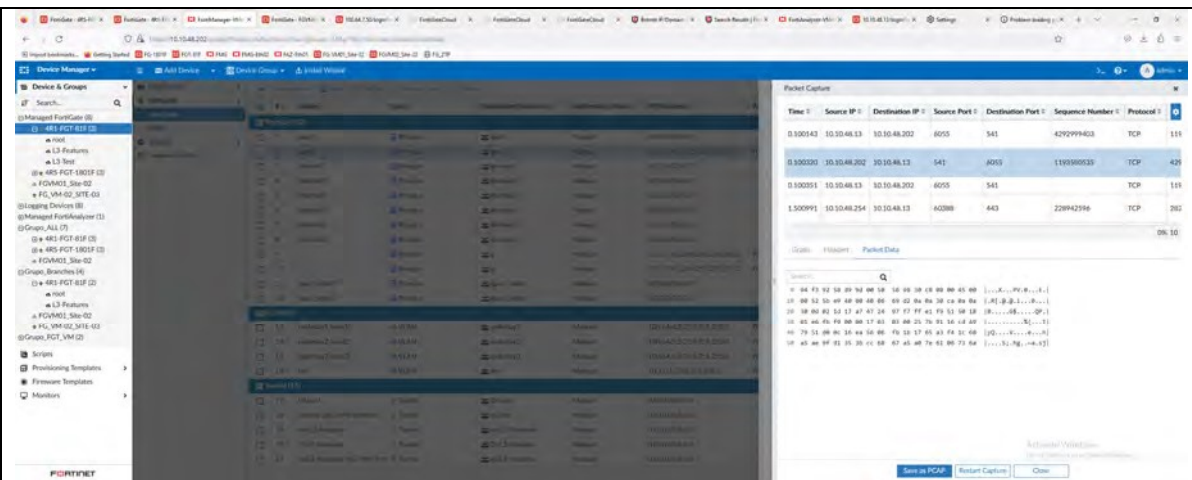
Time	Source IP	Destination IP	Source Port	Destination Port	Sequence Number	Protocol
0.000143	10.10.48.13	10.10.48.202	6055	541	4292999403	TCP
0.000320	10.10.48.202	10.10.48.13	541	6055	1193580535	TCP
0.000351	10.10.48.13	10.10.48.202	6055	541		TCP
1.500991	10.10.48.254	10.10.48.13	40388	443	228942396	TCP

Middle Screenshot: Traffic Graph

The graph shows the volume of traffic over time. The Y-axis is labeled 'Bytes Received' and ranges from 0 to 7. The X-axis is labeled 'Time (seconds)' and ranges from 0 to 10. A blue line shows a steady increase in traffic, starting at approximately 1.5 bytes at 0 seconds and reaching about 6.5 bytes at 10 seconds.

Bottom Screenshot: Packet Details (L4)

Field	Value
Source IP	10.10.48.202
Source Port	541
Destination IP	10.10.48.13
Destination Port	6055
Sequence Number	1193580535
Flags	rst, ack
Window	58881
Length	42
Checksum	63995



TESTE OK

Dentro de um pacote de políticas podemos adicionar uma nova regra e dentro dela colocar todos os filtros necessários.

Entre eles, controle de aplicação (Applicatin Control), IPS, antivírus e anti-spyware(Antivírus), conteúdo Web e filtro de URL's(Web Filter Profile).

Para realização de debugging e troubleshooting deve se usar do seguinte caminho para se acessar qualquer FortiGate gerenciado pelo FortiManager.

Em “Device Manager” selecionar o FortiGate desejado e clicar duas vezes nele, assim aparecerá uma aba de informações sobre aquele ativo.

Clicando no ícone indicado, se tem acesso a interface cli daquele equipamento, te dando assim, a possibilidade de debuggar e dar troubleshooting no equipamento com o auxílio deste documento:

<https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/244292/troubleshooting>

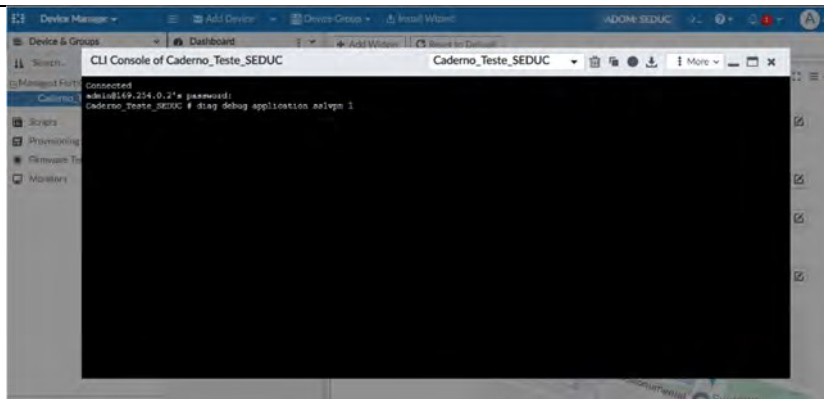
Evidências

The image shows two screenshots from the FortiGate management interface. The top screenshot is the 'Policy & Objects' page. The 'Policy Packages' section is expanded to show 'SEDUC'. A table lists the policies under 'Implicit (1/1 Total:1)'. The 'Create New' button is highlighted in yellow.

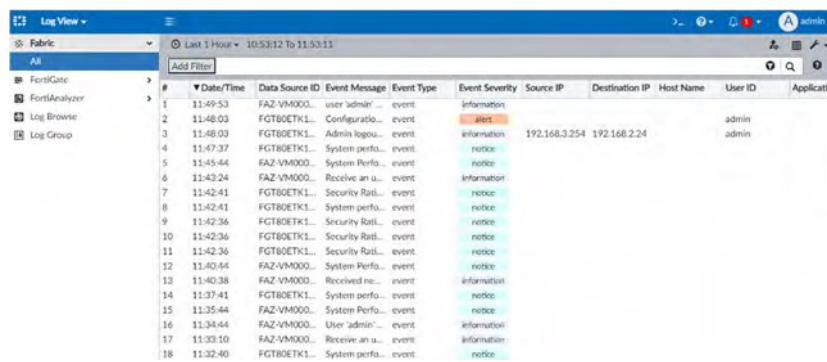
#	Name
1	Implicit Deny

The bottom screenshot is the 'Device Manager' page for 'Caderno_Teste_SEDUC'. The 'System Information' section is visible, showing details like Host Name, Serial Number, IP Address, System Time, Uptime, Firmware Version, Hardware Status, Operation Mode, VDOM, and Operation. The 'Operation' status is highlighted in yellow.

System Information	Value
Host Name	Caderno_Teste_SEDUC
Serial Number	FGT80ETK18012960
IP Address	192.168.2.24 (wan1)
System Time	Fri Mar 17 10:08:39 2023 PDT
Uptime	2 days 3 hours 38 minutes 10 seconds
Firmware Version	FortiGate 7.2.4.build1396 (GA) (Feature)
Hardware Status	4 CPU, 1866 MB RAM
Operation Mode	NAT
VDOM	VDOM Disabled
Operation	Operation



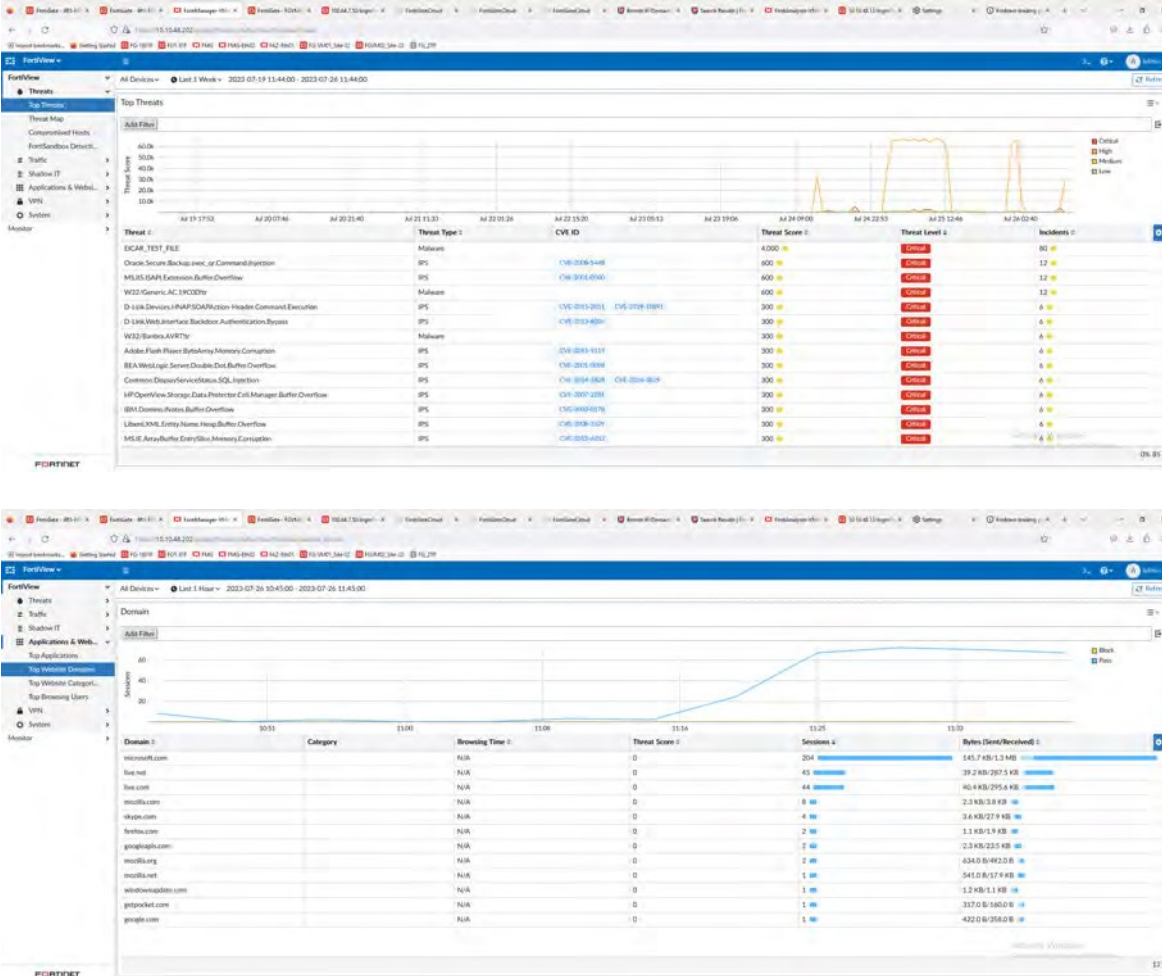
Para monitoração e investigação de logs deve-se utilizar o FortiAnalyzer, que é uma ferramenta própria para análise de logs, investigação de eventos.

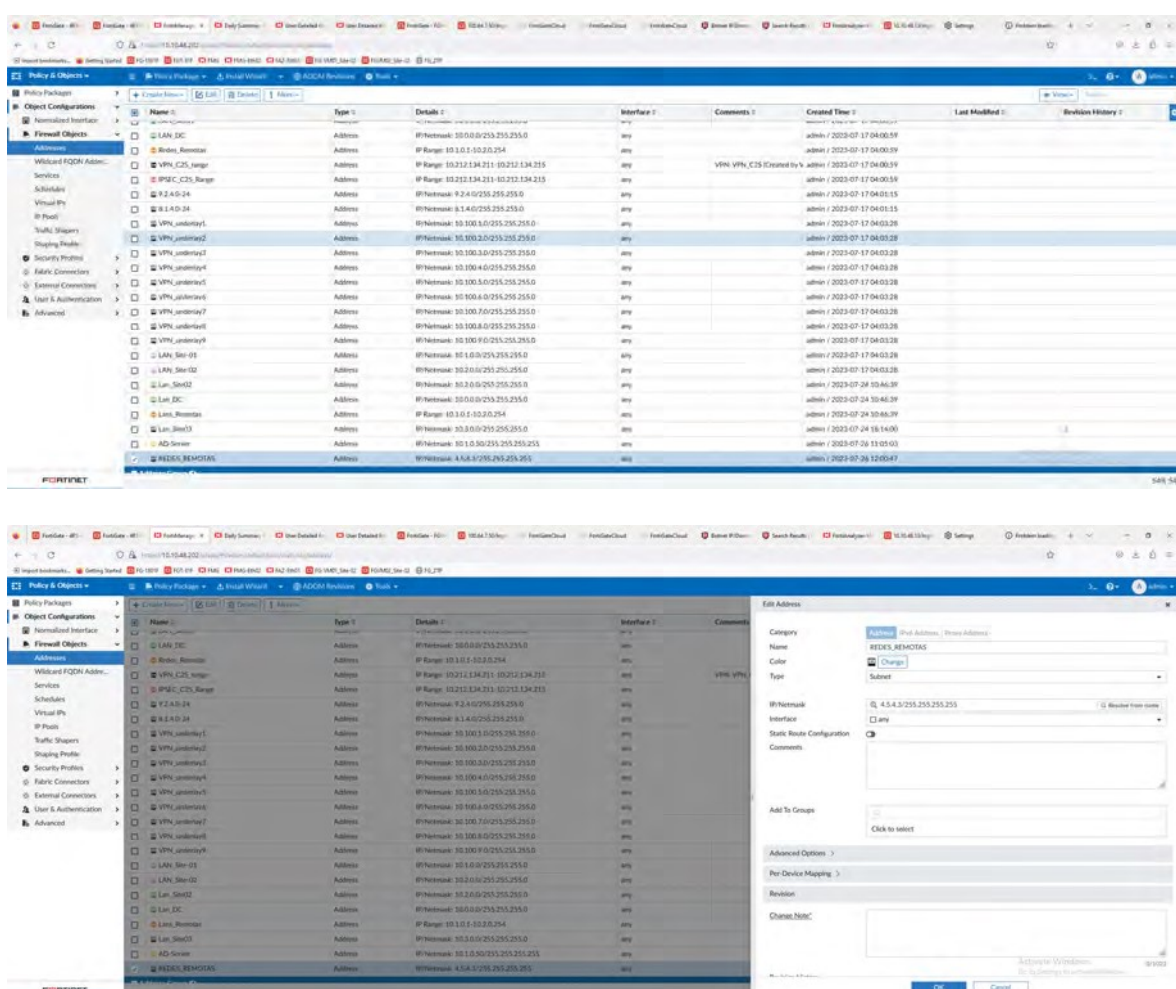


#	Date/Time	Data Source ID	Event Message	Event Type	Event Severity	Source IP	Destination IP	Host Name	User ID	Application
1	11:49:53	FAZ-VM000...	user 'admin' ...	event	information					
2	11:48:03	FGT80ETK1...	Configuratio...	event	notice				admin	
3	11:48:03	FGT80ETK1...	Admin logou...	event	information	192.168.3.254	192.168.2.24		admin	
4	11:47:37	FGT80ETK1...	System perfo...	event	notice					
5	11:45:44	FAZ-VM000...	System Perfo...	event	notice					
6	11:43:24	FAZ-VM000...	Receive an u...	event	information					
7	11:42:41	FGT80ETK1...	Security Rat...	event	notice					
8	11:42:41	FGT80ETK1...	System perfo...	event	notice					
9	11:42:36	FGT80ETK1...	Security Rat...	event	notice					
10	11:42:36	FGT80ETK1...	Security Rat...	event	notice					
11	11:42:36	FGT80ETK1...	Security Rat...	event	notice					
12	11:40:44	FAZ-VM000...	System Perfo...	event	notice					
13	11:40:38	FAZ-VM000...	Received no...	event	information					
14	11:37:41	FGT80ETK1...	System perfo...	event	notice					
15	11:35:44	FAZ-VM000...	System Perfo...	event	notice					
16	11:34:44	FAZ-VM000...	User 'admin'...	event	information					
17	11:33:10	FAZ-VM000...	Receive an u...	event	information					
18	11:32:40	FGT80ETK1...	System perfo...	event	notice					



Comentário

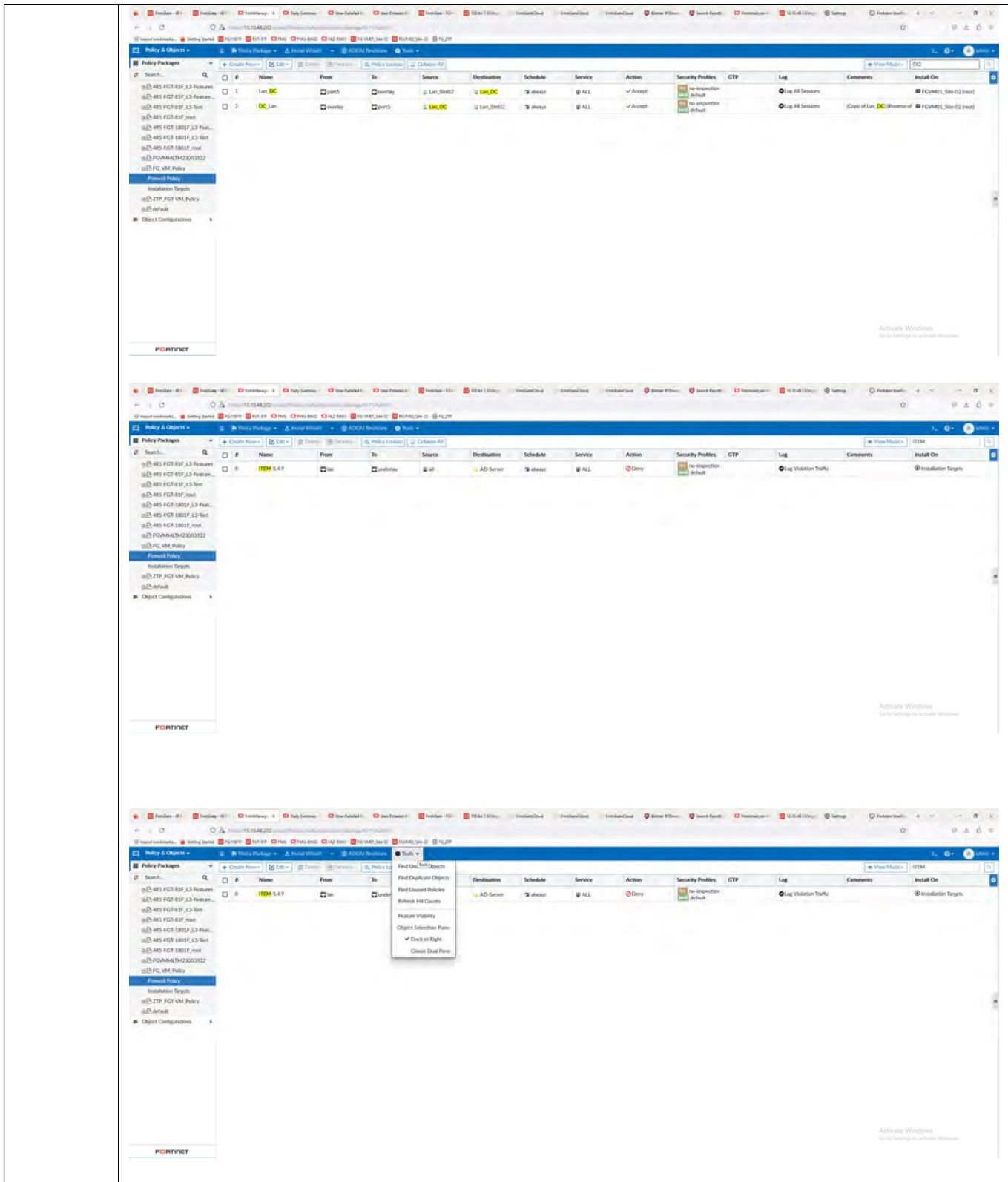
Item de Teste - 5.4.11	Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, antivírus, anti-malware) e URLs analisadas pelo firewall;
Objetivo do Teste	Demonstrar na gerência centralizada os dashboards de eventos.
Configuração do Teste	Demonstrar dashboards do FortiAnalyzer.
Procedimento do Teste	Demonstrar dashboards do FortiAnalyzer.
Evidências	 <p>TESTE OK</p>
Comentário	Fonte: FortiAnalyzer Data Sheet acessado em https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf

Item de Teste - 5.4.12	Possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deverá ainda permitir detectar onde, na base de regras, está sendo utilizado determinado objeto de rede;
Objetivo do Teste	Verificar se o equipamento de gerência realiza criação, alteração, monitoração e exclusão de objetos de rede. Como também detectar onde, na base de regras, está sendo utilizado determinado objeto de rede.
Configuração do Teste	Demonstrar caixa de pesquisa para filtro de objetos da base de regras
Procedimento do Teste	Em “Policy & Objects” podemos ter acesso a todos os tipos de objetos gerenciado por aquele equipamento. Dentro de cada aba, o FortiManager lhe dá a opção de criação de um novo objeto.
Evidências	

The screenshots illustrate the configuration of Firewall Objects in Fortinet FortiGate. The first image shows a confirmation dialog for deleting selected objects. The second image shows the Firewall Objects list, highlighting the 'VPN_VPN_C2S' object. The third image shows the configuration details for 'VPN_VPN_C2S', including the ADOM, Policy Package, and various fields like Name, Type, Details, and Interface.

Name	Type	Details	Interface	Comments	Created Time	Last Modified	Revision History
LAN_ZC	Address	@Network: 10.0.0.0/255.255.255.0	any		admin / 2023-07-17 04:00:59		
Redes_Remota	Address	@Range: 10.1.0.1-10.2.0.254	any		admin / 2023-07-17 04:00:59		
VPN_VPN_C2S	Address	@Range: 10.212.134.211-10.212.134.211	any	VPN_VPN_C2S Created by...	admin / 2023-07-17 04:00:59		
IPSEC_C2S_Range	Address	@Range: 10.212.134.211-10.212.134.211	any		admin / 2023-07-17 04:00:59		
9.2.0-24	Address	@Network: 9.2.0/255.255.255.0	any		admin / 2023-07-17 04:01:11		
9.1.0-24	Address	@Network: 9.1.0/255.255.255.0	any		admin / 2023-07-17 04:01:15		
VPN_gateway1	Address	@Network: 10.100.0.0/255.255.255.0	any		admin / 2023-07-17 04:03:28		
VPN_gateway2	Address	@Network: 10.100.10.0/255.255.255.0	any		admin / 2023-07-17 04:03:28		
VPN_gateway3	Address	@Network: 10.100.20.0/255.255.255.0	any		admin / 2023-07-17 04:03:28		
VPN_gateway4	Address	@Network: 10.100.30.0/255.255.255.0	any		admin / 2023-07-17 04:03:28		
VPN_gateway5	Address	@Network: 10.100.40.0/255.255.255.0	any		admin / 2023-07-17 04:03:28		
VPN_gateway6	Address	@Network: 10.100.50.0/255.255.255.0	any		admin / 2023-07-17 04:03:28		
VPN_gateway7	Address	@Network: 10.100.60.0/255.255.255.0	any		admin / 2023-07-17 04:03:28		
VPN_gateway8	Address	@Network: 10.100.70.0/255.255.255.0	any		admin / 2023-07-17 04:03:28		
VPN_gateway9	Address	@Network: 10.100.80.0/255.255.255.0	any		admin / 2023-07-17 04:03:28		
VPN_gateway10	Address	@Network: 10.100.90.0/255.255.255.0	any		admin / 2023-07-17 04:03:28		
LAN_Ser-01	Address	@Network: 10.1.0.0/255.255.255.0	any		admin / 2023-07-17 04:03:28		
LAN_Ser-02	Address	@Network: 10.2.0.0/255.255.255.0	any		admin / 2023-07-17 04:03:28		
LAN_Ser-03	Address	@Network: 10.3.0.0/255.255.255.0	any		admin / 2023-07-24 10:46:39		
LAN_Ser-04	Address	@Network: 10.4.0.0/255.255.255.0	any		admin / 2023-07-24 10:46:39		
LAN_Ser-05	Address	@Network: 10.5.0.0/255.255.255.0	any		admin / 2023-07-24 10:46:39		
AD_Server	Address	@Network: 10.1.0.0/255.255.255.0	any		admin / 2023-07-26 11:05:07		

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



The image displays three sequential screenshots of the Microsoft Group Policy Editor (GPO) interface, showing the configuration of various policies. The interface includes a left-hand navigation pane with a search bar and a list of policy packages, and a main table of policy objects.

Top Screenshot: Shows a table of policy objects. The selected policy is "Lan_DC".

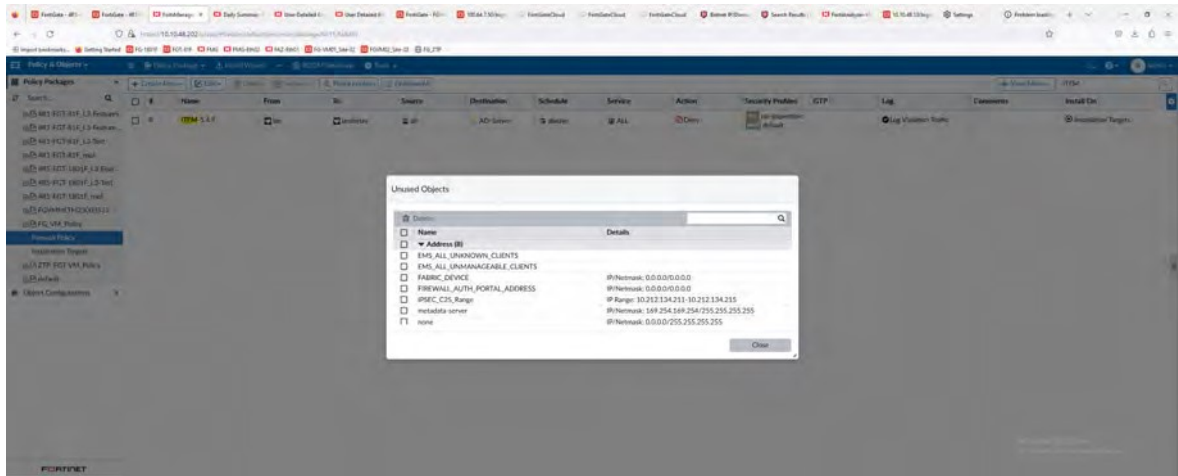
Policy Package	ID	Name	From	To	Source	Destination	Schedule	Service	Action	Security Profiles	GTP	Log	Comments	Install On
481-FGT-83F-L3-Features	1	Lan_DC	port5	Deny	@ Lan_Sm02	Lan_DC	always	@ ALL	Accept	No-Inspection-Default		Log All Sessions		FGM01_Sec-02 (read)
481-FGT-83F-L3-Features	2	DC_Lan	every	port5	Lan_DC	Lan_Sm02	always	@ ALL	Accept	No-Inspection-Default		Log All Sessions	(Key of Lan_DC) (Source of FGT481_Sec-02 (read)	

Middle Screenshot: Shows a table of policy objects. The selected policy is "ITM 5.4.9".

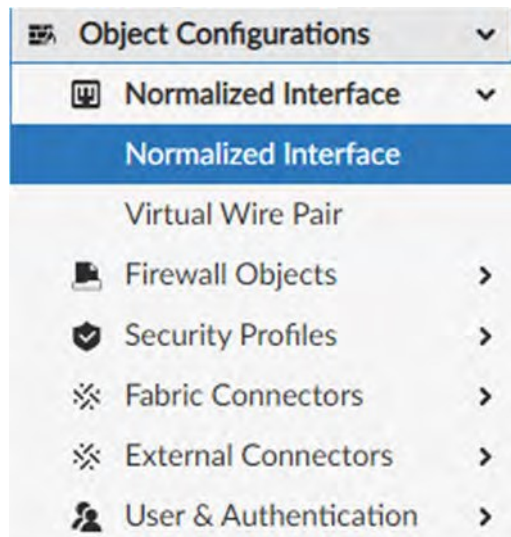
Policy Package	ID	Name	From	To	Source	Destination	Schedule	Service	Action	Security Profiles	GTP	Log	Comments	Install On
481-FGT-83F-L3-Features	8	ITM 5.4.9	in	unblock	@	AD-Server	always	@ ALL	Deny	No-Inspection-Default		Log Violation Traffic		Installation Targets

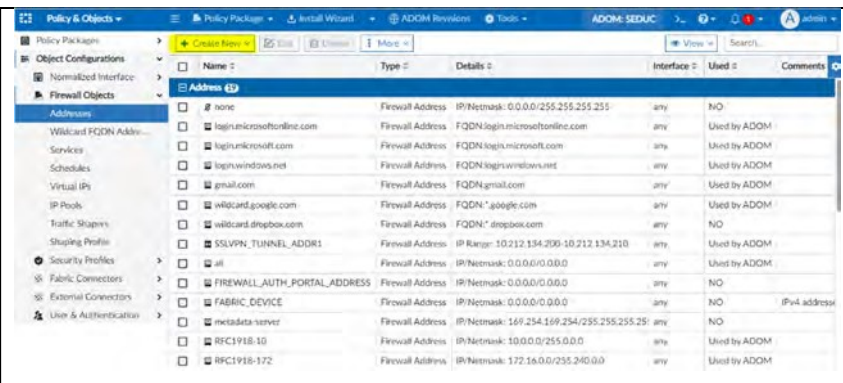
Bottom Screenshot: Shows the same table as the middle screenshot, but with a context menu open over the "ITM 5.4.9" policy. The menu options are:

- Find Unlink Objects
- Find Duplicate Objects
- Find Unused Policies
- Refresh All Counts
- Feature Visibility
- Object Selection Pane
- Check on Right
- Classic Dual Pane



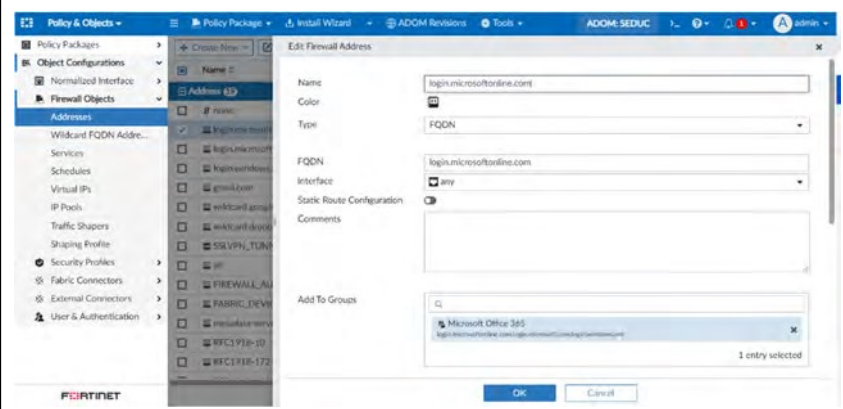
TESTE OK





Name	Type	Details	Interface	Used	Comments
none	Firewall Address	IP/Netmask: 0.0.0.0/255.255.255.255	any	NO	
login.microsoftonline.com	Firewall Address	FQDN:login.microsoftonline.com	any	Used by ADOM	
login.microsoft.com	Firewall Address	FQDN:login.microsoft.com	any	Used by ADOM	
login.windows.net	Firewall Address	FQDN:login.windows.net	any	Used by ADOM	
gmail.com	Firewall Address	FQDN:gmail.com	any	Used by ADOM	
wildcard.google.com	Firewall Address	FQDN:*google.com	any	Used by ADOM	
wildcard.dropbox.com	Firewall Address	FQDN:*dropbox.com	any	NO	
SSLVPN_TUNNEL_ADDR1	Firewall Address	IP Range: 10.212.134.200-10.212.134.210	any	Used by ADOM	
all	Firewall Address	IP/Netmask: 0.0.0.0/0.0.0.0	any	Used by ADOM	
FIREWALL_AUTH_PORTAL_ADDRESS	Firewall Address	IP/Netmask: 0.0.0.0/0.0.0.0	any	NO	
FABRIC_DEVICE	Firewall Address	IP/Netmask: 0.0.0.0/0.0.0.0	any	NO	(IPv4 address)
meta-data-server	Firewall Address	IP/Netmask: 169.254.169.254/255.255.255.255	any	NO	
RFC1918-10	Firewall Address	IP/Netmask: 10.0.0.0/255.0.0.0	any	Used by ADOM	
RFC1918-172	Firewall Address	IP/Netmask: 172.16.0.0/255.240.0.0	any	Used by ADOM	

Edição de um já existente



Edit Firewall Address

Name: login.microsoftonline.com

Color: [Color Picker]

Type: FQDN

FQDN: login.microsoftonline.com

Interface: any

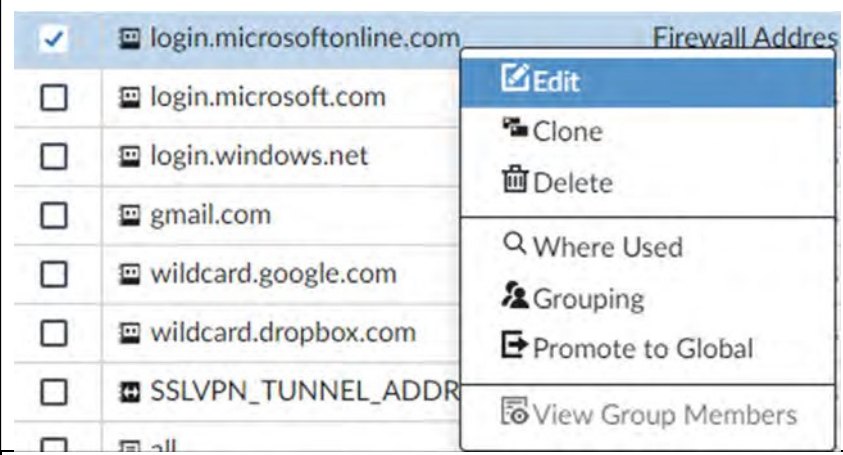
Static Route Configuration: [Checked]

Comments: [Text Area]

Add To Groups: [Search Box] (1 entry selected)

Buttons: OK, Cancel

Como também exclusão e visualização de onde está sendo usado.



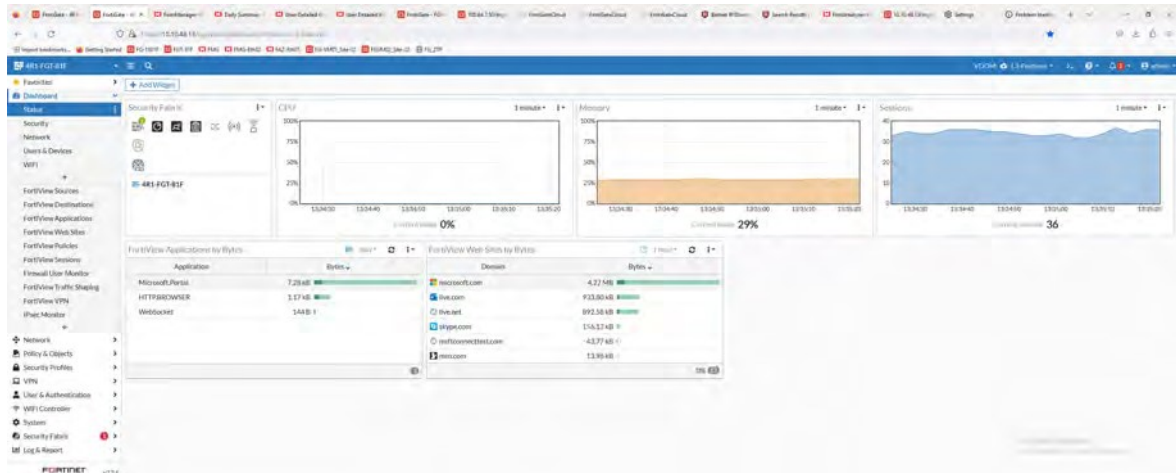
Firewall Address

- login.microsoftonline.com
- login.microsoft.com
- login.windows.net
- gmail.com
- wildcard.google.com
- wildcard.dropbox.com
- SSLVPN_TUNNEL_ADDR1
- all

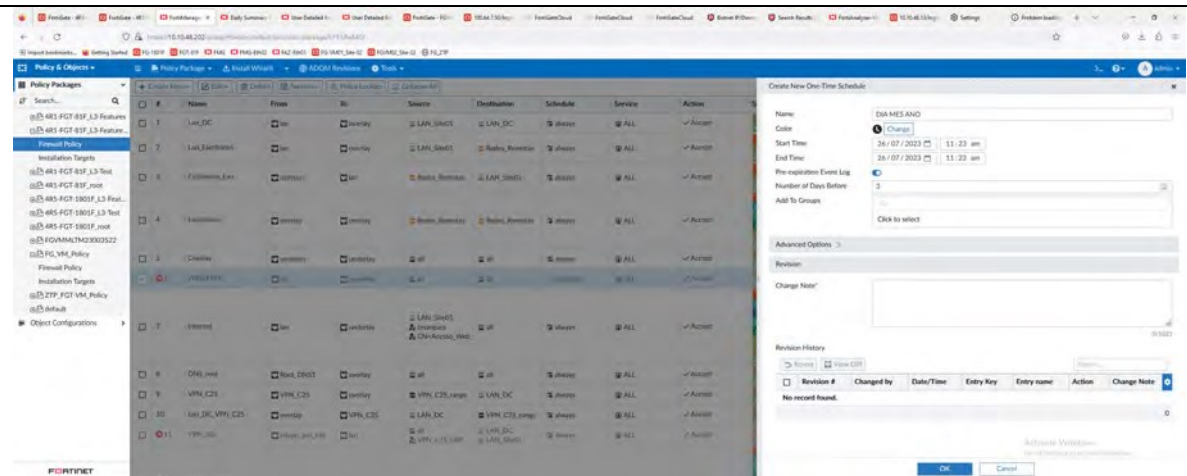
Context Menu:

- Edit
- Clone
- Delete
- Where Used
- Grouping
- Promote to Global
- View Group Members

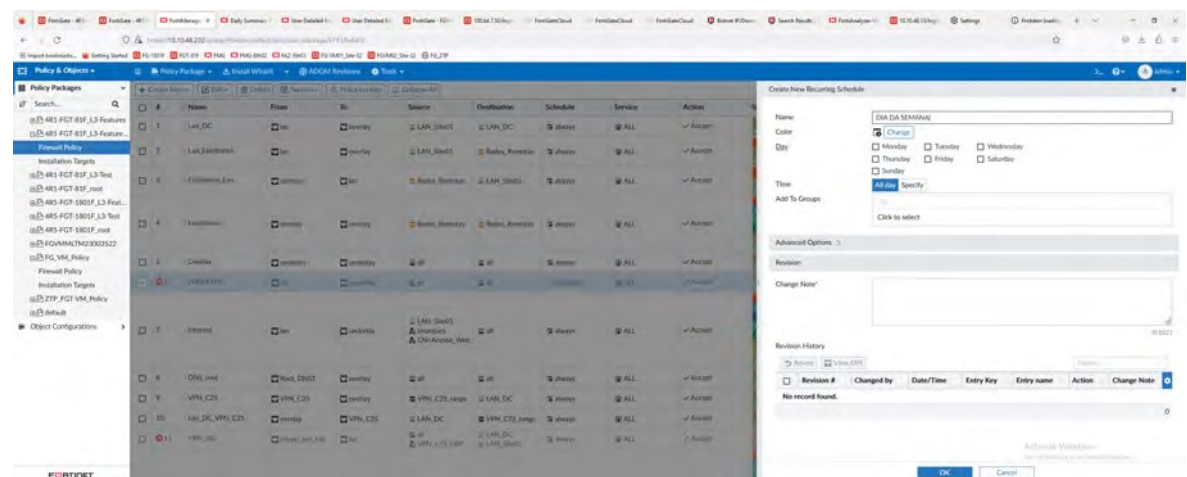
Comentário

Item de Teste - 5.4.13	Caso haja a necessidade de instalação de algum software para a administração da solução, o mesmo deve ser compatível com o Microsoft Windows 11;
Objetivo do Teste	Demonstrar que toda a operação da Gerência Centralizada é feita via interface WEB (HTTPS) ou CLI (SSH).
Configuração do Teste	Demonstrar navegação nas consoles operacionais da Gerência Centralizada.
Procedimento do Teste	Demonstrar navegação nas consoles operacionais da Gerência Centralizada.
Evidências	 <p>TESTE OK</p> <p>Não existe a necessidade de instalar nenhum software para realizar a administração da solução, utilizando qualquer navegador web suportado.</p>
Comentário	

Item de Teste - 5.4.14	Deve possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
Objetivo do Teste	Validar se a ferramenta possui a funcionalidade de atribuir tempo à uma política.
Configuração do Teste	Necessita ter um FortiManager e uma conta de administrador com acesso para escrita e visualização.
Procedimento do Teste	Na aba de "Policy and Objects", é possível visualizar todas as regras presentes no dispositivo. Para cada regra, há um campo denominado "Agendamento", onde é possível programá-la para um período específico ou torná-la recorrente durante um determinado intervalo de tempo.
Evidências	



The screenshot shows the Fortinet Policy & Objects configuration page. A table lists various policies with columns for ID, Name, From, To, Source, Destination, Schedule, Service, and Action. A dialog box titled 'Create New One-Time Schedule' is open on the right, with fields for Name, Color, Start Time, End Time, Pre-expiration Event Log, and Number of Days Before. The 'Advanced Options' section includes Revision and Change Note fields, and a Revision History table.



The screenshot shows the Fortinet Policy & Objects configuration page. A dialog box titled 'Create New Recurring Schedule' is open on the right, with fields for Name, Color, Day (Monday through Saturday), Time, and Add To Groups. The 'Advanced Options' section includes Revision and Change Note fields, and a Revision History table.

TESTE OK

#	Name	From	To	Source	Destination	Schedule	Service	Action
1		lan	lan1	all	all	always	ALL	Accept
2		svlvpn_tun_intf	lan	SSLVPN_TUNNEL rodrigo	gmail.com login.microsoft.com login.microsoftfl login.windows.net	always	ALL	Accept

Para criação de regras para um período de tempo:

	<p>Create New One-Time Schedule</p> <p>Name: <input type="text" value="Agendamento-Seduc"/></p> <p>Color: <input type="color" value="#000000"/></p> <p>Start Time: <input type="text" value="15/03/2023"/> <input type="text" value="14:58"/></p> <p>End Time: <input type="text" value="15/03/2023"/> <input type="text" value="14:58"/></p> <p>Pre-expiration Event Log: <input checked="" type="checkbox"/></p> <p>Number of Days Before: <input type="text" value="3"/></p> <p>Add To Groups: <input type="text" value=""/></p> <p>Click to select</p> <p>Para regras recorrentes:</p> <p>Create New Recurring Schedule</p> <p>Name: <input type="text" value="Agendamento-Seduc"/></p> <p>Color: <input type="color" value="#000000"/></p> <p>Day: <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday <input type="checkbox"/> Sunday</p> <p>Time: <input checked="" type="button" value="All day"/> <input type="button" value="Specify"/></p> <p>Add To Groups: <input type="text" value=""/></p> <p>Click to select</p>
Comentário	

Item de Teste - 5.4.15	Deve registrar logs de auditoria referente as ações dos usuários administradores;
Objetivo do Teste	Validar se a solução é capaz de registrar de auditoria referente as ações dos usuários administradores.
Configuração do Teste	Demonstrar logs de rastreamento de ações locais dos administradores.
Procedimento do Teste	Para isso, é necessário acessar a aba de "System Settings" e, em seguida, a seção "Event Log", onde serão exibidas todas as alterações efetuadas por determinado administrador juntamente com a data e a origem correspondentes.
Evidências	

The image displays two screenshots of a Fortinet system log interface. The top screenshot shows a list of events from July 26, 2023, at 11:37:20. The bottom screenshot shows a similar list of events from July 26, 2023, at 11:30:44. Both screenshots show detailed information for each event, including the user, the policy name, and the status of the operation.

Log Entry 1 (Top Screenshot):

#	Time	Event
1	2023-07-26 11:37:20	Security console global policy assignment status: user=admin msg=FG_M01_Site-02[not] feat package 250-2 status updated to INSTALLED
2	2023-07-26 11:37:20	Security console global policy assignment status: user=admin msg=FG_M01_Site-02[not] wip package 250-2 status updated to INSTALLED
3	2023-07-26 11:37:20	Security console global policy assignment status: user=admin msg=FG_VM_02_SITE-02[not] feat package 293-2 status updated to INSTALLED
4	2023-07-26 11:37:20	Security console global policy assignment status: user=admin msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED
5	2023-07-26 11:37:20	Security console global policy assignment status: user=admin msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED
6	2023-07-26 11:37:20	Security console global policy assignment status: user=admin msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED
7	2023-07-26 11:37:20	Security console global policy assignment status: user=admin msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED
8	2023-07-26 11:37:20	Security console global policy assignment status: user=admin msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED
9	2023-07-26 11:37:20	Security console global policy assignment status: user=admin msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED
10	2023-07-26 11:37:20	Security console global policy assignment status: user=admin msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED
11	2023-07-26 11:37:20	Security console global policy assignment status: user=admin msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED
12	2023-07-26 11:37:20	Security console global policy assignment status: user=admin msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED
13	2023-07-26 11:37:20	Security console global policy assignment status: user=admin msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED
14	2023-07-26 11:37:20	Security console global policy assignment status: user=admin msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED
15	2023-07-26 11:37:20	Security console global policy assignment status: user=admin msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED
16	2023-07-26 11:37:20	Security console global policy assignment status: user=admin msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED
17	2023-07-26 11:37:20	Security console global policy assignment status: user=admin msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED

Log Entry 2 (Bottom Screenshot):

#	Time	Event
1	2023-07-26 11:30:44	Security console global policy assignment status: user=whorhulda msg=FG_M01_Site-02[not] feat package 250-2 status updated to INSTALLED
2	2023-07-26 11:30:44	Security console global policy assignment status: user=whorhulda msg=FG_M01_Site-02[not] wip package 250-2 status updated to INSTALLED
3	2023-07-26 11:30:44	Security console global policy assignment status: user=whorhulda msg=FG_VM_02_SITE-02[not] feat package 293-2 status updated to INSTALLED
4	2023-07-26 11:30:44	Security console global policy assignment status: user=whorhulda msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED
5	2023-07-26 11:30:44	Security console global policy assignment status: user=whorhulda msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED
6	2023-07-26 11:30:44	Security console global policy assignment status: user=whorhulda msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED
7	2023-07-26 11:30:44	Security console global policy assignment status: user=whorhulda msg=FG_VM_02_SITE-02[not] wip package 293-2 status updated to INSTALLED


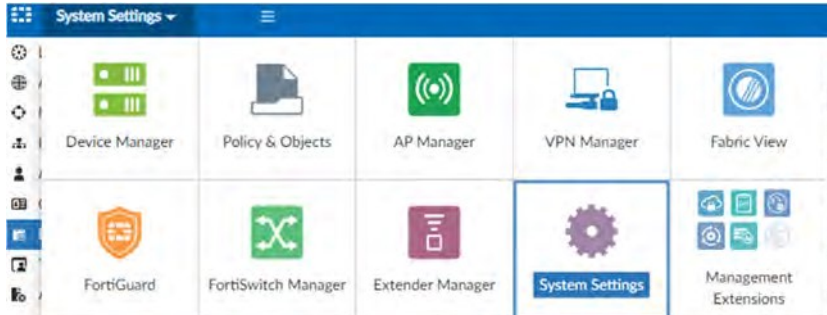
TESTE OK

Event Log

The *Event Log* pane provides an audit log of actions made by users on FortiManager. It allows you to view log messages that are stored in memory or on the internal hard disk drive. You can use filters to search the messages and download the messages to the management computer.

See the *FortiManager Log Message Reference*, available from the Fortinet Document Library, for more information about the log messages.

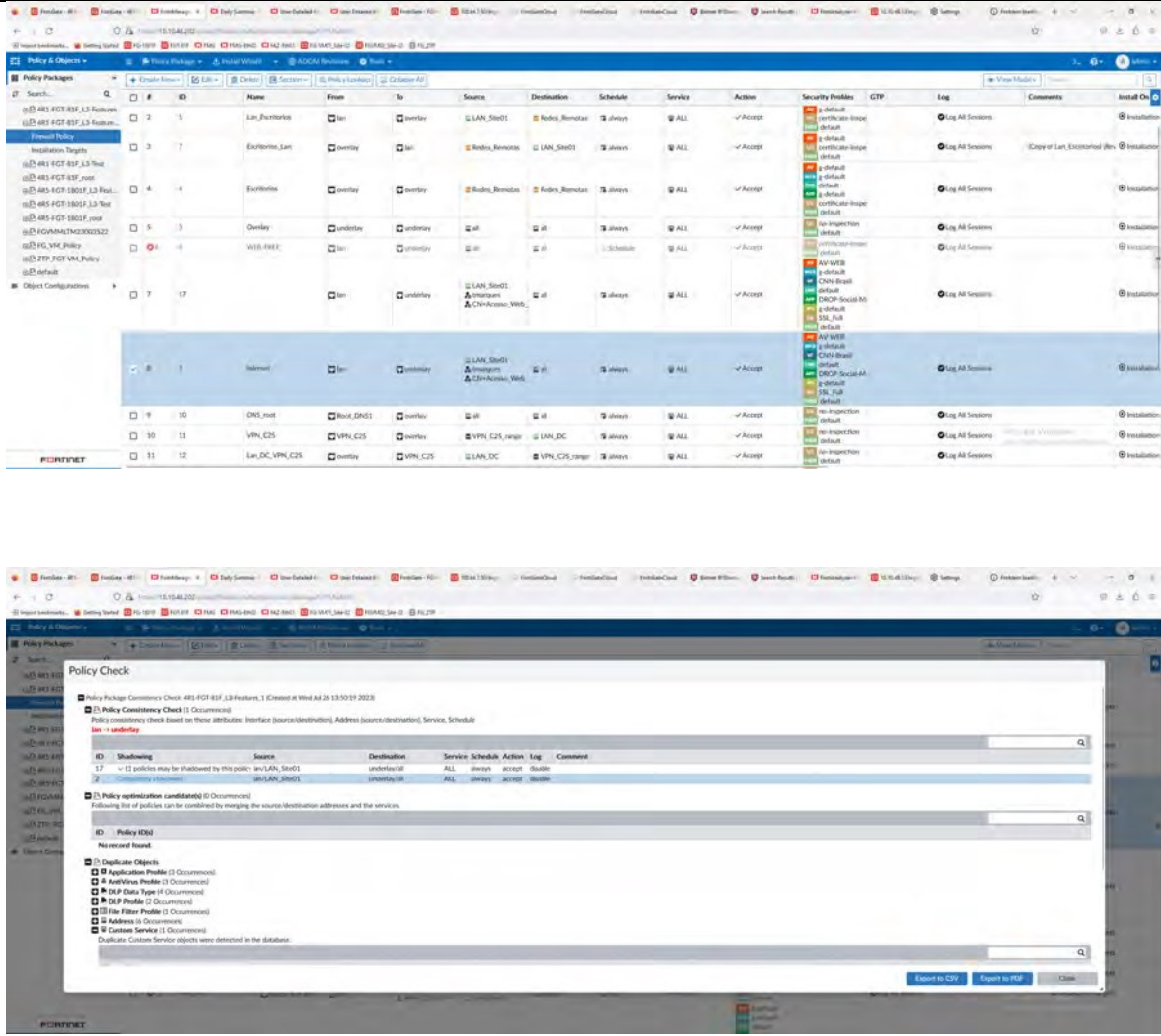
Go to *System Settings > Event Log* to view the local log list.

#	Date Time	Label	User	Job Type	Description	Operation	Performed On	Changes
7	2021-04-26 12:27:29	admin	admin	admin	Job event log for object changed	edit	2021-04-26 12:27:29	forti-fg_message: 2021-04-26 12:27:29: 2021-04-26 12:27:29
8	2021-04-26 12:24:07	admin	admin	admin	Job event log for object changed	edit	2021-04-26 12:24:07	forti-fg_message: 2021-04-26 12:24:07: 2021-04-26 12:24:07
9	2021-04-26 12:24:07	admin	admin	admin	Job event log for object changed	edit	2021-04-26 12:24:07	forti-fg_message: 2021-04-26 12:24:07: 2021-04-26 12:24:07
10	2021-04-26 12:24:07	admin	admin	admin	Job event log for object changed	edit	2021-04-26 12:24:07	forti-fg_message: 2021-04-26 12:24:07: 2021-04-26 12:24:07
11	2021-04-26 12:23:10	admin	admin	admin	Job event log for object changed	edit	2021-04-26 12:23:10	forti-fg_message: 2021-04-26 12:23:10: 2021-04-26 12:23:10
12	2021-04-26 12:19:51	admin	admin	admin	Package update request from FortiGuard server received	Update Response	11/24/21 12:19:51	Received an update from FortiGuard server: 11/24/21 12:19:51
13	2021-04-26 12:09:41	admin	admin	admin	Package update request from FortiGuard server received	Update Response	11/24/21 12:09:41	Received an update from FortiGuard server: 11/24/21 12:09:41

Comentário Fonte: FortiManager Administration Guide acessado em: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/04f80bb3-e03c-11ec-bb32-fa163e15d75b/FortiManager-7.2.1-Administration_Guide.pdf

Item de Teste - 5.4.16	A solução deve possuir registro de todas as alterações realizadas em uma política de segurança, por um determinado administrador, permitindo a identificação do responsável pela mudança, contendo registros de autoria, data e origem;
Objetivo do Teste	Verificar se a solução consegue registrar todas as alterações realização em uma política de segurança, por um determinado administrador, permitindo a identificação do responsável pela mudança, contendo registros de autoria, data e origem.
Configuração do Teste	Demonstrar logs de rastreamento de ações locais dos administradores.
Procedimento do Teste	Para isso, é necessário acessar a aba de "System Settings" e, em seguida, a seção "Event Log", onde serão exibidas todas as alterações efetuadas por determinado indivíduo, juntamente com a data e a origem correspondentes.
Evidências	

<p>Item de Teste - 5.4.17</p>	<p>Prover funcionalidade para análise e auditoria de regras com capacidade de detectar regras conflitantes ou não conformes;</p>
<p>Objetivo do Teste</p>	<p>Verificar se o equipamento faz uma validação de políticas que estão conflitantes entre si ou em não conformação.</p>
<p>Configuração do Teste</p>	<p>Demonstrar a sobreposição de regras que se anulam ou se repetem.</p>
<p>Procedimento do Teste</p>	<p>Primeiramente, é necessário importar as políticas presentes no dispositivo.</p> <p>Posteriormente, deve-se acessar a guia "Políticas e Objetos" e, utilizando o botão direito do mouse, selecionar a opção "Política de Firewall" e, em seguida, "Verificação de Política" para realizar a referida verificação.</p>
<p>Evidências</p>	 <p>The top screenshot shows a table of Firewall Policy Packages in WinBox. The table has columns for ID, Name, From, To, Source, Destination, Schedule, Service, Action, Security Profiles, GTP, Log, and Comments. The bottom screenshot shows the 'Policy Check' dialog box with the following details:</p> <ul style="list-style-type: none"> Policy Package Consistency Check: 481-FGT-83F-L3-Features_1 (Created at Wed Jul 26 13:50:19 2023) Policy Consistency Check (1 Occurrences): Policy consistency check based on these attributes: Interface (source/destination), Address (source/destination), Service, Schedule. Status: fail - undetected Policy optimization candidates (0 Occurrences): Following list of policies can be combined by merging the source/destination addresses and the services. Duplicate Objects (0 Occurrences): Application Profiles (0 Occurrences), AntiVirus Profiles (0 Occurrences), DLP Data Type (0 Occurrences), DLP Profiles (0 Occurrences), Filter Profiles (0 Occurrences), Address (0 Occurrences), Custom Service (1 Occurrences). Duplicate Custom Service objects were detected in the database. <p>TESTE OK</p>

Perform a policy consistency check

The policy check tool allows you to check all policy packages within an ADOM to ensure consistency and eliminate conflicts that may prevent your devices from passing traffic. This allows you to optimize your policy sets and potentially reduce the size of your databases.

The check will verify:

- Object duplication: two objects that have identical definitions
- Object shadowing: a higher priority object completely encompasses another object of the same type
- Object overlap: one object partially overlaps another object of the same type
- Object orphaning: an object has been defined but has not been used anywhere.

The policy check uses an algorithm to evaluate policy objects, based on the following attributes:

- The source and destination interface policy objects
- The source and destination address policy objects
- The service and schedule policy objects.

Import Device - Caderno_Testes_SEDUC - Interface Mapping & Policy (2/5)

Create a new policy package for import.

Policy Package Name:

Folder:

Policy Selection:

Object Selection:

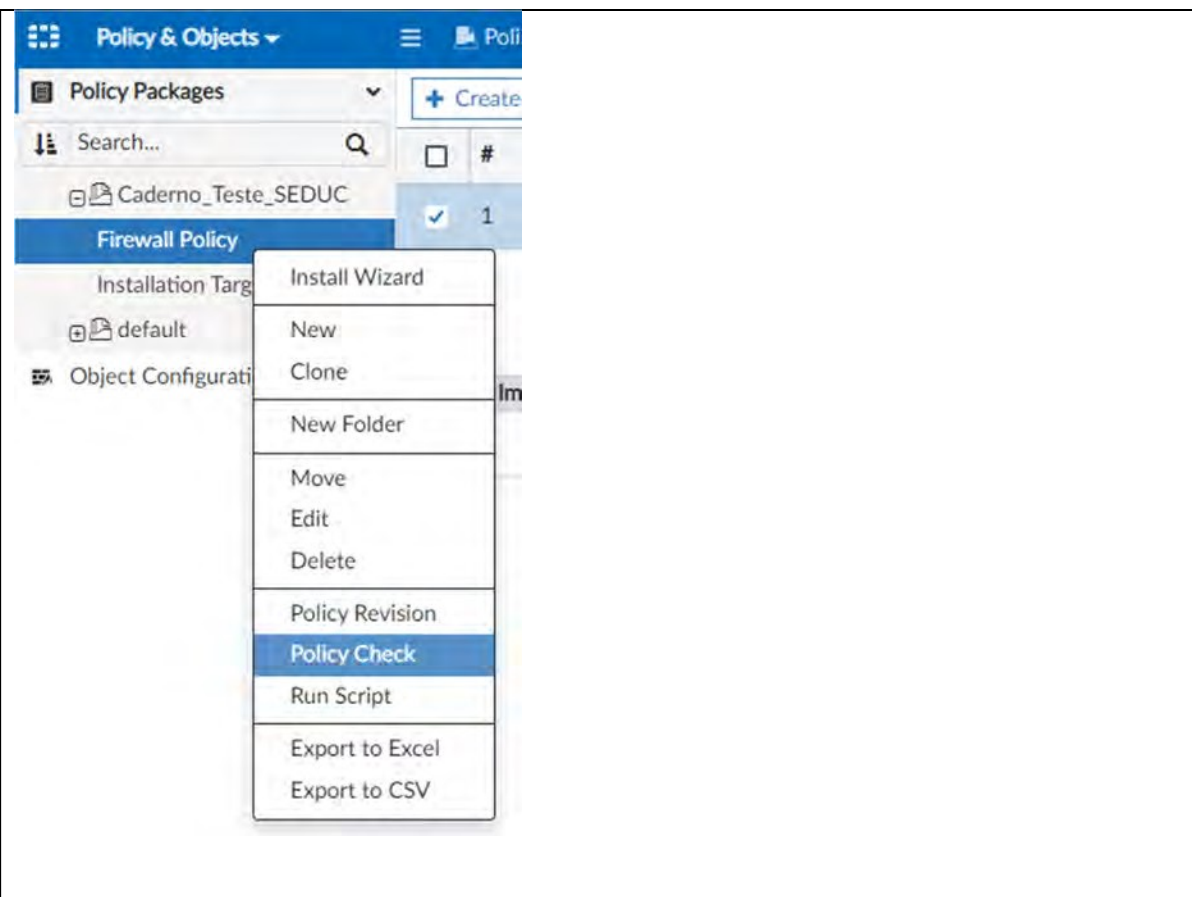
i When importing configuration from this device, all enabled interfaces require a mapping to an ADOM Level interface. Note, the same ADOM Level interface can map to different interfaces on the each device.

Search...

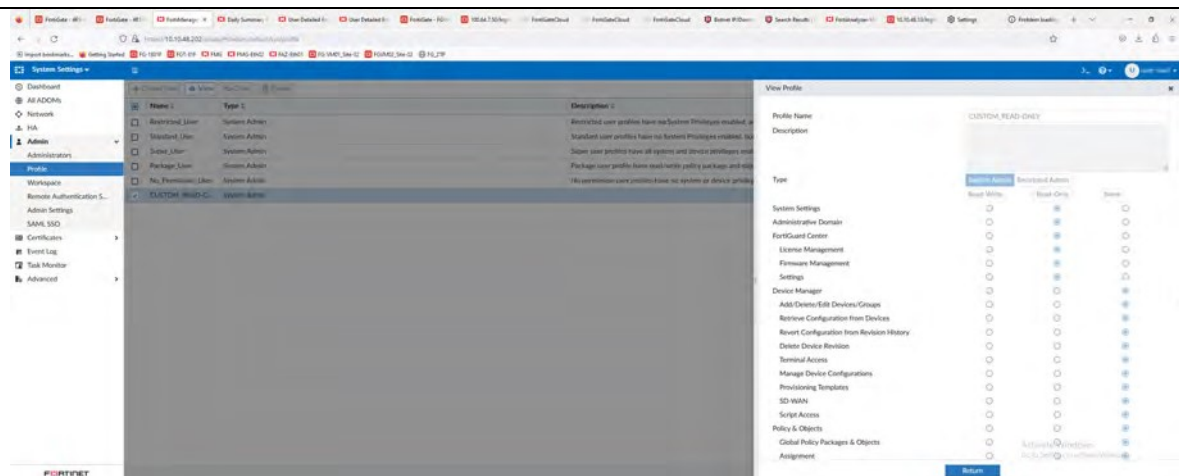
Device Interface	Mapping Type	Normalized Interface
<input checked="" type="checkbox"/> lan	<input type="button" value="Per-Device"/> <input type="button" value="Per-Platform"/>	lan
<input checked="" type="checkbox"/> ssl.root	<input type="button" value="Per-Device"/> <input type="button" value="Per-Platform"/>	ssl.root
<input checked="" type="checkbox"/> wan1	<input type="button" value="Per-Device"/> <input type="button" value="Per-Platform"/>	wan1

3

Add mappings for all unused

	
Comentário	<p>Fonte: FortiManager Administration Guide acessado em: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/04f80bb3-e03c-11ec-bb32-fa163e15d75b/FortiManager-7.2.1-Administration_Guide.pdf</p>

Item de Teste - 5.4.18	Suportar acesso baseado em perfil de usuário com as permissões de visualizar e modificar;
Objetivo do Teste	Verificar se o equipamento de gerência centralizada suporta o Suportar acesso baseado em perfil de usuário com as permissões de visualizar e modificar;
Configuração do Teste	Demonstrar os perfis de acesso ao FortiManager
Procedimento do Teste	Demonstrar os perfis de acesso ao FortiManager
Evidências	

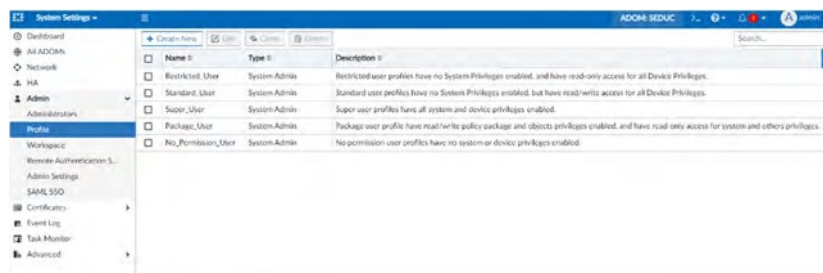


TESTE OK

Por padrão, o FortiManager já vem com os seguintes perfis:

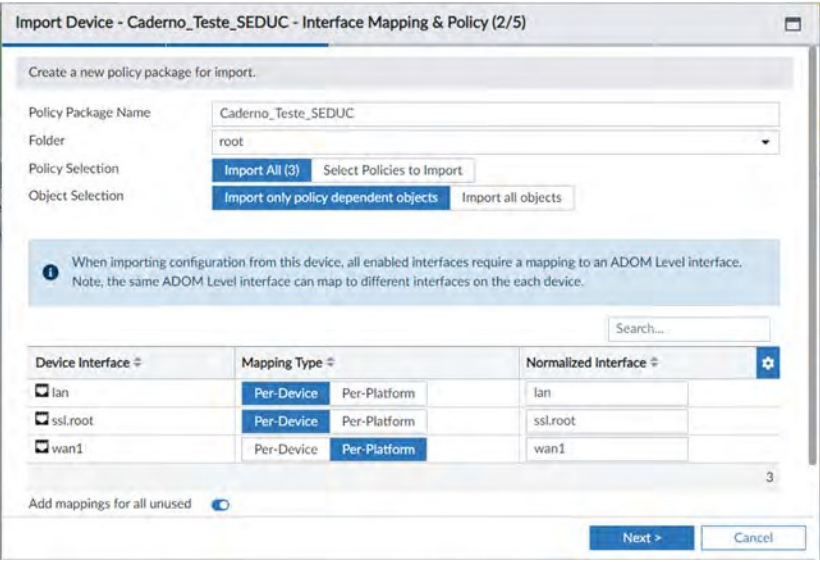
Restricted_User	Restricted user profiles have no system privileges enabled, and have read-only access for all device privileges.
Standard_User	Standard user profiles have no system privileges enabled, and have read/write access for all device privileges.
Super_User	Super user profiles have all system and device privileges enabled. It cannot be edited.
Package_User	Package user profile have read/write policy and objects privileges enabled, and have read-only access for system and other privileges.

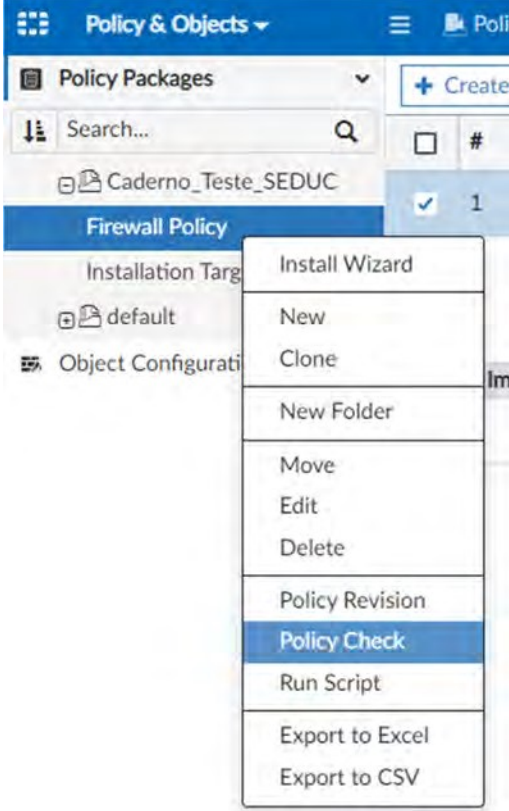
Caso haja a necessidade de criação de outro tipo de perfil, é possível fazê-lo acessando a seção "System Settings" e, em seguida, navegando até "Administração" e "Profile". Nessa área, é possível visualizar todos os perfis já criados, bem como editar os perfis que foram fornecidos como padrão.



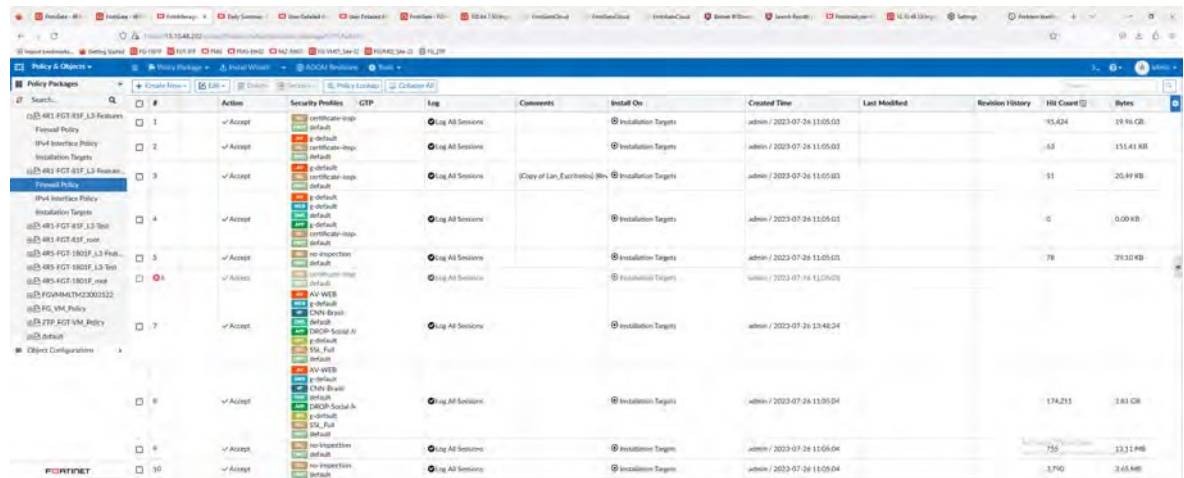
Comentário

Fonte: FortiManager Administration Guide acessado em: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/04f80bb3-e03c-11ec-bb32-fa163e15d75b/FortiManager-7.2.1-Administration_Guide.pdf

Item de Teste - 5.4.19	Deverá possuir validação da política avisando quando houver regras que ofusquem ou conflitem com outras regras;
Objetivo do Teste	Verificar se o equipamento faz uma validação de políticas que estão sendo ofuscadas ou em conflitos com outras regras.
Configuração do Teste	Demonstrar a sobreposição de regras que se anulam ou se repetem.
Procedimento do Teste	<p>Primeiramente, é necessário importar as políticas presentes no dispositivo.</p> <p>Posteriormente, deve-se acessar a guia "Políticas e Objetos" e, utilizando o botão direito do mouse, selecionar a opção "Política de Firewall" e, em seguida, "Verificação de Política" para realizar a referida verificação.</p>
Evidências	<p>Atendido conforme subitem 5.4.17</p> <p>TESTE OK</p> <p>Perform a policy consistency check</p> <p>The policy check tool allows you to check all policy packages within an ADOM to ensure consistency and eliminate conflicts that may prevent your devices from passing traffic. This allows you to optimize your policy sets and potentially reduce the size of your databases.</p> <p>The check will verify:</p> <ul style="list-style-type: none"> Object duplication: two objects that have identical definitions Object shadowing: a higher priority object completely encompasses another object of the same type Object overlap: one object partially overlaps another object of the same type Object orphaning: an object has been defined but has not been used anywhere. <p>The policy check uses an algorithm to evaluate policy objects, based on the following attributes:</p> <ul style="list-style-type: none"> The source and destination interface policy objects The source and destination address policy objects The service and schedule policy objects 

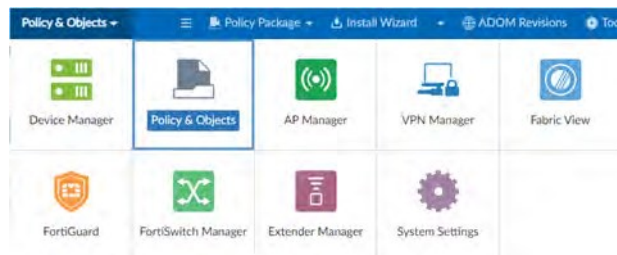
	
<p>Comentário</p>	<p>Fonte: FortiManager Administration Guide acessado em: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/04f80bb3-e03c-11ec-bb32-fa163e15d75b/FortiManager-7.2.1-Administration_Guide.pdf</p>

<p>Item de Teste -5.4.20</p>	<p>A solução deve possuir “hit”/volume de regras para identificar possíveis melhorias na performance reordenando as mesmas;</p>
<p>Objetivo do Teste</p>	<p>Verificar se o equipamento de gerência centralizada possui uma forma de verificar a quantidade de “hit”/volume de regras para identificar possíveis melhorias na performance reordenando as mesmas;</p>
<p>Configuração do Teste</p>	<p>Demonstrar hit counts de regras em uso.</p>
<p>Procedimento do Teste</p>	<p>Para isto, é necessário acessar a aba de “Policy & Objects”.</p> <p>Em seguida, é necessário selecionar um pacote de políticas. Depois, caso não esteja habilitado a opção de visualização de “Hit Counts”, basta ir ao canto superior direito e clicar no símbolo de engrenagem. Lá aparecerá várias informações referentes às políticas, entre elas, “Hit Count”.</p>
<p>Evidências</p>	



#	Action	Security Profiles	GTP	Log	Comments	Install On	Created Time	Last Modified	Revision History	Hit Count	Bytes
1	Accept	certificat-insp, default		Log All Sessions		Installation Targets	admin / 2023-07-26 11:05:03			15,824	19.94 GB
2	Accept	certificat-insp, default		Log All Sessions		Installation Targets	admin / 2023-07-26 11:05:03			63	115.41 KB
3	Accept	certificat-insp, default		Log All Sessions	(Copy of Lan_Ethernet0/3)	Installation Targets	admin / 2023-07-26 11:05:03			51	25.84 KB
4	Accept	certificat-insp, default		Log All Sessions		Installation Targets	admin / 2023-07-26 11:05:03			0	0.00 KB
5	Accept	no-inspection, default		Log All Sessions		Installation Targets	admin / 2023-07-26 11:05:03			78	29.32 KB
6	Accept	certificat-insp, default		Log All Sessions		Installation Targets	admin / 2023-07-26 11:07:07				
7	Accept	AV-Web, DNS-Brazil, CNV-Brazil, default, DISOP-Susp, default, SSL-Full, default		Log All Sessions		Installation Targets	admin / 2023-07-26 13:42:24				
8	Accept	AV-Web, DNS-Brazil, default, DISOP-Social, default, SSL-Full, default		Log All Sessions		Installation Targets	admin / 2023-07-26 13:30:04			179,211	3.83 GB
9	Accept	no-inspection, default		Log All Sessions		Installation Targets	admin / 2023-07-26 11:05:04			750	13.1 MB
10	Accept	no-inspection, default		Log All Sessions		Installation Targets	admin / 2023-07-26 11:05:04			3,740	3.65 MB

TESTE OK

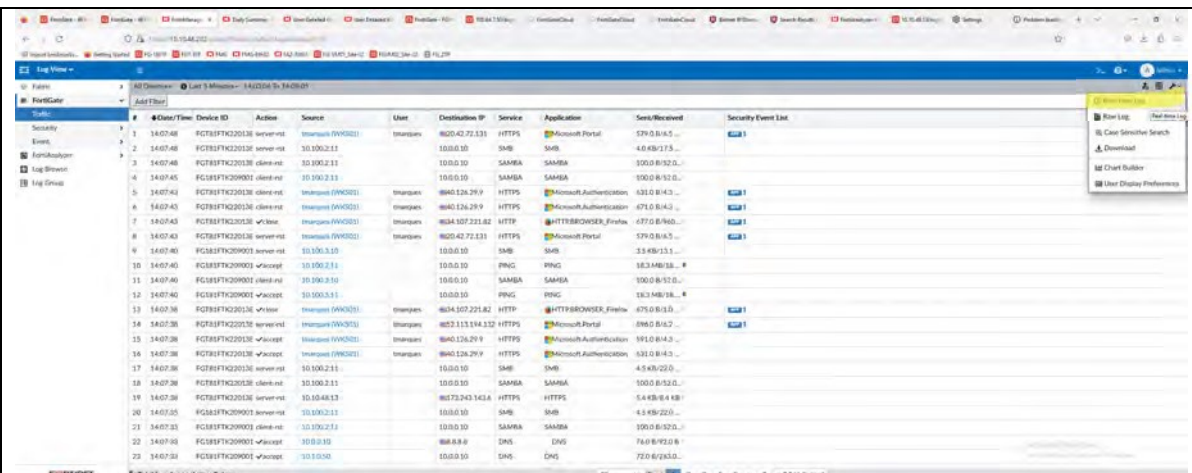


Policy & Objects

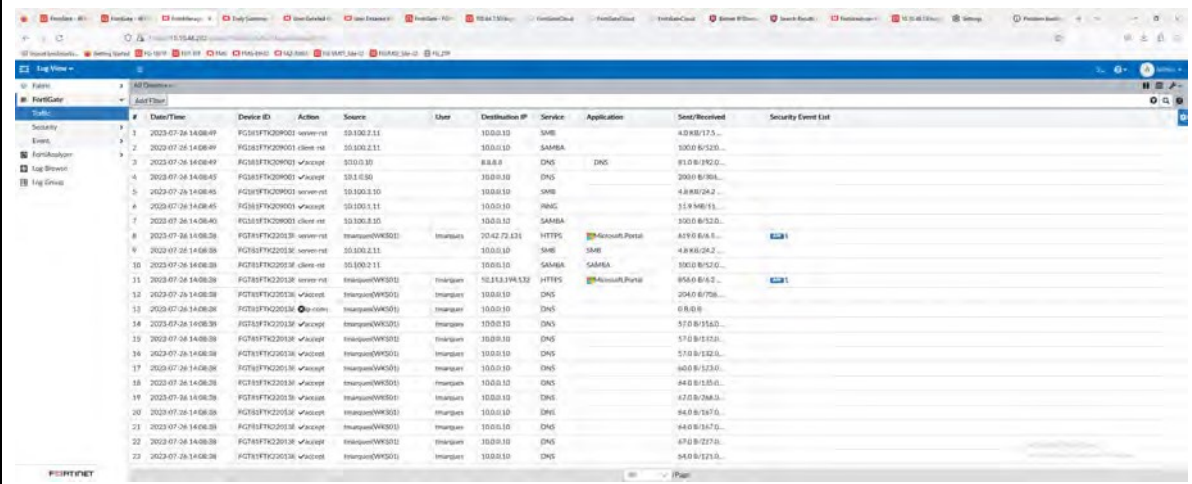
- Device Manager
- Policy & Objects**
- AP Manager
- VPN Manager
- Fabric View
- FortiGuard
- FortiSwitch Manager
- Extender Manager
- System Settings

	<ul style="list-style-type: none"> <input type="checkbox"/> Users <input checked="" type="checkbox"/> Action <input checked="" type="checkbox"/> Security Profiles <input checked="" type="checkbox"/> Log <input type="checkbox"/> NAT <input type="checkbox"/> Traffic Shaping <input type="checkbox"/> Enforce ZTNA <input type="checkbox"/> EMS Tag <input type="checkbox"/> Geographic Tag <input checked="" type="checkbox"/> Hit Count <input type="checkbox"/> Bytes <input type="checkbox"/> Packets <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr> <th>#</th> <th>Name</th> <th>From</th> <th>To</th> <th>Hit Count</th> <th>Source</th> <th>Destination</th> <th>Schedule</th> <th>Service</th> </tr> </thead> <tbody> <tr> <td>1</td> <td></td> <td>lan</td> <td>wan1</td> <td></td> <td>all</td> <td>all</td> <td>always</td> <td>ALL</td> </tr> <tr> <td>2</td> <td></td> <td>sslvpn_tun_inet</td> <td>lan</td> <td></td> <td>SSLVPN_TUNNEL rodrigo</td> <td>gmail.com login.microsoft.com login.microsoft.com login.microsoft.com</td> <td>always</td> <td>ALL</td> </tr> </tbody> </table>	#	Name	From	To	Hit Count	Source	Destination	Schedule	Service	1		lan	wan1		all	all	always	ALL	2		sslvpn_tun_inet	lan		SSLVPN_TUNNEL rodrigo	gmail.com login.microsoft.com login.microsoft.com login.microsoft.com	always	ALL
#	Name	From	To	Hit Count	Source	Destination	Schedule	Service																				
1		lan	wan1		all	all	always	ALL																				
2		sslvpn_tun_inet	lan		SSLVPN_TUNNEL rodrigo	gmail.com login.microsoft.com login.microsoft.com login.microsoft.com	always	ALL																				
Comentário																												

Item de Teste - 5.4.21	Deve possuir visualização de log em tempo próximo ao real;
Objetivo do Teste	Verificar se o equipamento possui a funcionalidade de visualização de logs em tempo próximo ao real.
Configuração do Teste	Demonstrar a sobreposição de regras que se anulam ou se repetem.
Procedimento do Teste	<p>Para acessar a funcionalidade de visualização dos registros em tempo real, é necessário acessar a seção "Visualização de Logs".</p> <p>A seguir, é necessário selecionar o equipamento desejado, pressionar o ícone de chave de fenda localizado no canto superior direito e, em seguida, selecionar a opção "Registro em Tempo Real".</p>
Evidências	

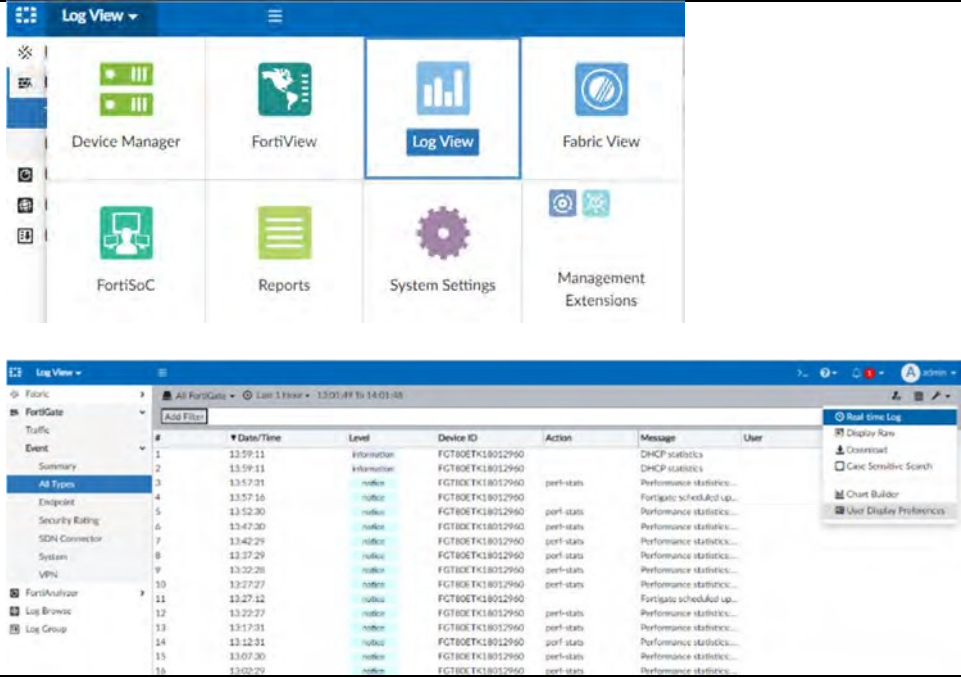


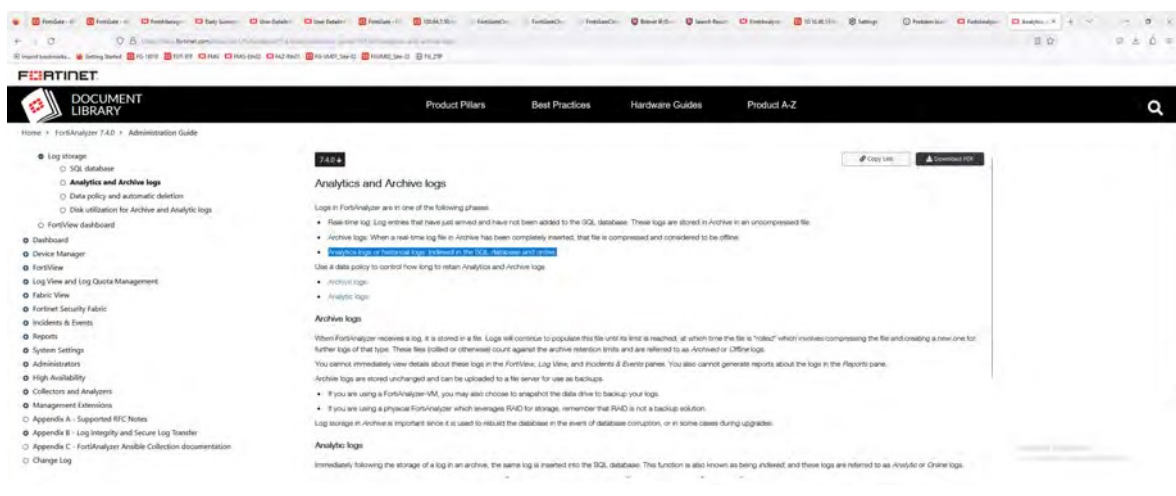
#	Date/Time	Device ID	Action	Source	User	Destination IP	Service	Application	Sent/Received	Security Event List
1	14:07:48	FGT8FTK20138	server-nt	10.100.2.11	Anonymous	10.0.0.10	SMB	Microsoft Portal	579 B/14.5...	
2	14:07:48	FGT8FTK20138	client-nt	10.100.2.11		10.0.0.10	SAMBA	SAMBA	4.0 KB/17.5...	
3	14:07:48	FGT8FTK20138	client-nt	10.100.2.11		10.0.0.10	SAMBA	SAMBA	100.0 B/102.0...	
4	14:07:48	FGT8FTK20138	client-nt	10.100.2.11		10.0.0.10	SAMBA	SAMBA	100.0 B/102.0...	
5	14:07:48	FGT8FTK20138	client-nt	10.100.2.11	Anonymous	10.0.0.10	SMB	Microsoft Authentication	431.0 B/14.3...	
6	14:07:48	FGT8FTK20138	client-nt	10.100.2.11	Anonymous	10.0.0.10	SMB	Microsoft Authentication	431.0 B/14.3...	
7	14:07:48	FGT8FTK20138	client-nt	10.100.2.11	Anonymous	10.0.0.10	SMB	Microsoft Authentication	431.0 B/14.3...	
8	14:07:48	FGT8FTK20138	server-nt	10.100.2.11	Anonymous	10.0.0.10	SMB	Microsoft Portal	579 B/14.5...	
9	14:07:48	FGT8FTK20138	server-nt	10.100.2.11		10.0.0.10	SMB	SMB	33.4 KB/13.1...	
10	14:07:48	FGT8FTK20138	accept	10.100.2.11		10.0.0.10	PING	PING	16.3 MB/18...	
11	14:07:48	FGT8FTK20138	client-nt	10.100.2.11		10.0.0.10	SAMBA	SAMBA	100.0 B/102.0...	
12	14:07:48	FGT8FTK20138	accept	10.100.2.11		10.0.0.10	PING	PING	18.3 MB/18...	
13	14:07:48	FGT8FTK20138	accept	10.100.2.11	Anonymous	10.0.0.10	HTTP	HTTPBROWSER_Firefox	476.0 B/10.0...	
14	14:07:48	FGT8FTK20138	server-nt	10.100.2.11	Anonymous	10.0.0.10	HTTP	Microsoft Portal	884.0 B/12.7...	
15	14:07:48	FGT8FTK20138	accept	10.100.2.11	Anonymous	10.0.0.10	HTTP	Microsoft Authentication	101.0 B/14.3...	
16	14:07:48	FGT8FTK20138	accept	10.100.2.11	Anonymous	10.0.0.10	HTTP	Microsoft Authentication	431.0 B/14.3...	
17	14:07:48	FGT8FTK20138	server-nt	10.100.2.11		10.0.0.10	SMB	SMB	4.5 KB/22.0...	
18	14:07:48	FGT8FTK20138	client-nt	10.100.2.11		10.0.0.10	SAMBA	SAMBA	100.0 B/102.0...	
19	14:07:48	FGT8FTK20138	server-nt	10.100.2.11		10.0.0.10	HTTP	HTTP	5.4 KB/8.4 KB	
20	14:07:48	FGT8FTK20138	server-nt	10.100.2.11		10.0.0.10	SMB	SMB	4.3 KB/22.0...	
21	14:07:48	FGT8FTK20138	client-nt	10.100.2.11		10.0.0.10	SAMBA	SAMBA	100.0 B/102.0...	
22	14:07:48	FGT8FTK20138	accept	10.0.0.10		88.8.8.8	DNS	DNS	76.0 B/10.0 B	
23	14:07:48	FGT8FTK20138	accept	10.0.0.10		10.0.0.10	DNS	DNS	72.0 B/10.0 B	



#	Date/Time	Device ID	Action	Source	User	Destination IP	Service	Application	Sent/Received	Security Event List
1	2023-07-26 14:08:39	FGT8FTK20138	server-nt	10.100.2.11		10.0.0.10	SMB		4.0 KB/17.5...	
2	2023-07-26 14:08:39	FGT8FTK20138	client-nt	10.100.2.11		10.0.0.10	SAMBA		100.0 B/102.0...	
3	2023-07-26 14:08:49	FGT8FTK20138	accept	10.0.0.10		8.8.8.8	DNS	DNS	91.0 B/102.0...	
4	2023-07-26 14:08:45	FGT8FTK20138	accept	10.1.1.50		10.0.0.10	DNS		200.0 B/101...	
5	2023-07-26 14:08:45	FGT8FTK20138	server-nt	10.100.2.10		10.0.0.10	SMB		4.8 KB/24.2...	
6	2023-07-26 14:08:45	FGT8FTK20138	accept	10.100.2.11		10.0.0.10	PING		15.8 MB/11...	
7	2023-07-26 14:08:40	FGT8FTK20138	client-nt	10.100.2.10		10.0.0.10	SAMBA		100.0 B/102.0...	
8	2023-07-26 14:08:39	FGT8FTK20138	server-nt	10.100.2.11	Anonymous	10.0.0.10	HTTP	Microsoft Portal	419.0 B/8.1...	
9	2023-07-26 14:08:39	FGT8FTK20138	server-nt	10.100.2.11		10.0.0.10	SMB		4.8 KB/24.2...	
10	2023-07-26 14:08:39	FGT8FTK20138	client-nt	10.100.2.11		10.0.0.10	SAMBA		100.0 B/102.0...	
11	2023-07-26 14:08:39	FGT8FTK20138	server-nt	10.100.2.11	Anonymous	10.100.2.11	HTTP	Microsoft Portal	856.0 B/14.3...	
12	2023-07-26 14:08:39	FGT8FTK20138	accept	10.100.2.10	Anonymous	10.0.0.10	DNS		204.0 B/708...	
13	2023-07-26 14:08:39	FGT8FTK20138	accept	10.100.2.10	Anonymous	10.0.0.10	DNS		0.0 B/0	
14	2023-07-26 14:08:39	FGT8FTK20138	accept	10.100.2.10	Anonymous	10.0.0.10	DNS		17.0 B/152.0...	
15	2023-07-26 14:08:39	FGT8FTK20138	accept	10.100.2.10	Anonymous	10.0.0.10	DNS		17.0 B/152.0...	
16	2023-07-26 14:08:39	FGT8FTK20138	accept	10.100.2.10	Anonymous	10.0.0.10	DNS		17.0 B/152.0...	
17	2023-07-26 14:08:39	FGT8FTK20138	accept	10.100.2.10	Anonymous	10.0.0.10	DNS		140.0 B/133.0...	
18	2023-07-26 14:08:39	FGT8FTK20138	accept	10.100.2.10	Anonymous	10.0.0.10	DNS		140.0 B/133.0...	
19	2023-07-26 14:08:39	FGT8FTK20138	accept	10.100.2.10	Anonymous	10.0.0.10	DNS		17.0 B/152.0...	
20	2023-07-26 14:08:39	FGT8FTK20138	accept	10.100.2.10	Anonymous	10.0.0.10	DNS		140.0 B/133.0...	
21	2023-07-26 14:08:39	FGT8FTK20138	accept	10.100.2.10	Anonymous	10.0.0.10	DNS		140.0 B/133.0...	
22	2023-07-26 14:08:39	FGT8FTK20138	accept	10.100.2.10	Anonymous	10.0.0.10	DNS		14.0 B/127.0...	
23	2023-07-26 14:08:39	FGT8FTK20138	accept	10.100.2.10	Anonymous	10.0.0.10	DNS		14.0 B/127.0...	

TESTE OK

<p>Comentário</p>	 <table border="1"> <thead> <tr> <th>#</th> <th>Date/Time</th> <th>Level</th> <th>Device ID</th> <th>Action</th> <th>Message</th> <th>User</th> </tr> </thead> <tbody> <tr><td>1</td><td>13:59:11</td><td>Information</td><td>FGT806TK18012960</td><td></td><td>DHCP statistics</td><td></td></tr> <tr><td>2</td><td>13:59:11</td><td>Information</td><td>FGT806TK18012960</td><td></td><td>DHCP statistics</td><td></td></tr> <tr><td>3</td><td>13:57:31</td><td>notice</td><td>FGT806TK18012960</td><td>perf-stats</td><td>Performance statistics...</td><td></td></tr> <tr><td>4</td><td>13:57:16</td><td>notice</td><td>FGT806TK18012960</td><td>perf-stats</td><td>Fortigate scheduled up...</td><td></td></tr> <tr><td>5</td><td>13:52:30</td><td>notice</td><td>FGT806TK18012960</td><td>perf-stats</td><td>Performance statistics...</td><td></td></tr> <tr><td>6</td><td>13:47:30</td><td>notice</td><td>FGT806TK18012960</td><td>perf-stats</td><td>Performance statistics...</td><td></td></tr> <tr><td>7</td><td>13:42:29</td><td>notice</td><td>FGT806TK18012960</td><td>perf-stats</td><td>Performance statistics...</td><td></td></tr> <tr><td>8</td><td>13:37:29</td><td>notice</td><td>FGT806TK18012960</td><td>perf-stats</td><td>Performance statistics...</td><td></td></tr> <tr><td>9</td><td>13:32:28</td><td>notice</td><td>FGT806TK18012960</td><td>perf-stats</td><td>Performance statistics...</td><td></td></tr> <tr><td>10</td><td>13:27:27</td><td>notice</td><td>FGT806TK18012960</td><td>perf-stats</td><td>Performance statistics...</td><td></td></tr> <tr><td>11</td><td>13:22:12</td><td>notice</td><td>FGT806TK18012960</td><td>perf-stats</td><td>Fortigate scheduled up...</td><td></td></tr> <tr><td>12</td><td>13:22:27</td><td>notice</td><td>FGT806TK18012960</td><td>perf-stats</td><td>Performance statistics...</td><td></td></tr> <tr><td>13</td><td>13:17:31</td><td>notice</td><td>FGT806TK18012960</td><td>perf-stats</td><td>Performance statistics...</td><td></td></tr> <tr><td>14</td><td>13:12:31</td><td>notice</td><td>FGT806TK18012960</td><td>perf-stats</td><td>Performance statistics...</td><td></td></tr> <tr><td>15</td><td>13:07:30</td><td>notice</td><td>FGT806TK18012960</td><td>perf-stats</td><td>Performance statistics...</td><td></td></tr> <tr><td>16</td><td>13:02:29</td><td>notice</td><td>FGT806TK18012960</td><td>perf-stats</td><td>Performance statistics...</td><td></td></tr> </tbody> </table>	#	Date/Time	Level	Device ID	Action	Message	User	1	13:59:11	Information	FGT806TK18012960		DHCP statistics		2	13:59:11	Information	FGT806TK18012960		DHCP statistics		3	13:57:31	notice	FGT806TK18012960	perf-stats	Performance statistics...		4	13:57:16	notice	FGT806TK18012960	perf-stats	Fortigate scheduled up...		5	13:52:30	notice	FGT806TK18012960	perf-stats	Performance statistics...		6	13:47:30	notice	FGT806TK18012960	perf-stats	Performance statistics...		7	13:42:29	notice	FGT806TK18012960	perf-stats	Performance statistics...		8	13:37:29	notice	FGT806TK18012960	perf-stats	Performance statistics...		9	13:32:28	notice	FGT806TK18012960	perf-stats	Performance statistics...		10	13:27:27	notice	FGT806TK18012960	perf-stats	Performance statistics...		11	13:22:12	notice	FGT806TK18012960	perf-stats	Fortigate scheduled up...		12	13:22:27	notice	FGT806TK18012960	perf-stats	Performance statistics...		13	13:17:31	notice	FGT806TK18012960	perf-stats	Performance statistics...		14	13:12:31	notice	FGT806TK18012960	perf-stats	Performance statistics...		15	13:07:30	notice	FGT806TK18012960	perf-stats	Performance statistics...		16	13:02:29	notice	FGT806TK18012960	perf-stats	Performance statistics...	
#	Date/Time	Level	Device ID	Action	Message	User																																																																																																																		
1	13:59:11	Information	FGT806TK18012960		DHCP statistics																																																																																																																			
2	13:59:11	Information	FGT806TK18012960		DHCP statistics																																																																																																																			
3	13:57:31	notice	FGT806TK18012960	perf-stats	Performance statistics...																																																																																																																			
4	13:57:16	notice	FGT806TK18012960	perf-stats	Fortigate scheduled up...																																																																																																																			
5	13:52:30	notice	FGT806TK18012960	perf-stats	Performance statistics...																																																																																																																			
6	13:47:30	notice	FGT806TK18012960	perf-stats	Performance statistics...																																																																																																																			
7	13:42:29	notice	FGT806TK18012960	perf-stats	Performance statistics...																																																																																																																			
8	13:37:29	notice	FGT806TK18012960	perf-stats	Performance statistics...																																																																																																																			
9	13:32:28	notice	FGT806TK18012960	perf-stats	Performance statistics...																																																																																																																			
10	13:27:27	notice	FGT806TK18012960	perf-stats	Performance statistics...																																																																																																																			
11	13:22:12	notice	FGT806TK18012960	perf-stats	Fortigate scheduled up...																																																																																																																			
12	13:22:27	notice	FGT806TK18012960	perf-stats	Performance statistics...																																																																																																																			
13	13:17:31	notice	FGT806TK18012960	perf-stats	Performance statistics...																																																																																																																			
14	13:12:31	notice	FGT806TK18012960	perf-stats	Performance statistics...																																																																																																																			
15	13:07:30	notice	FGT806TK18012960	perf-stats	Performance statistics...																																																																																																																			
16	13:02:29	notice	FGT806TK18012960	perf-stats	Performance statistics...																																																																																																																			

<p>Item de Teste - 5.4.22</p>	<p>A solução deve possuir mecanismo de indexação de logs para permitir uma busca acelerada dos eventos sem a necessidade de abertura de arquivos de logs mais antigos;</p>
<p>Objetivo do Teste</p>	<p>Validar se a solução possui um mecanismo de indexação de logs para permitir uma busca acelerada dos eventos sem a necessidade de abertura de arquivos de logs mais antigos.</p>
<p>Configuração do Teste</p>	<p>Navegar no dashboard analíticos e demonstrar drill down de logs.</p>
<p>Procedimento do Teste</p>	<p>Navegar no dashboard analíticos e demonstrar drill down de logs.</p>
<p>Evidências</p>	 <p>Analytics and Archive logs</p> <p>Logs in FortiAnalyzer are in one of the following phases:</p> <ul style="list-style-type: none"> • Real-time log: Log entries that have just arrived and have not been added to the SQL database. These logs are stored in Archive in an uncompressed file. • Archive logs: When a real-time log file in Archive has been completely inserted, that file is compressed and considered to be offline. • Analytics logs or Analytic logs: Indexed in the SQL database. <p>Use a data policy to control how long to retain Analytics and Archive logs:</p> <ul style="list-style-type: none"> • Analytic logs • Archive logs <p>Archive logs</p> <p>When FortiAnalyzer receives a log, it is stored in a file. Logs will continue to populate this file until its limit is reached, at which time the file is "rotated" which involves compressing the file and creating a new one for further logs of that type. These files rotated or otherwise count against the archive retention limits and are referred to as Archived or Offline logs.</p> <p>You cannot immediately view details about these logs in the FortiView, Log View, and Incident & Event panels. You also cannot generate reports about the logs in the Reports pane.</p> <p>Archive logs are stored unchanged and can be uploaded to a file server for use as backups.</p> <ul style="list-style-type: none"> • If you are using a FortiAnalyzer VM, you may also choose to snapshot the data drive to backup your logs. • If you are using a physical FortiAnalyzer which leverages RAID for storage, remember that RAID is not a backup solution. <p>Log storage in Archive is important since it is used to rebuild the database in the event of database corruption, or in some cases during upgrades.</p> <p>Analytic logs</p> <p>Immediately following the storage of a log in an archive, the same log is inserted into the SQL database. This function is also known as being indexed, and these logs are referred to as Analytic or Online logs.</p>

System Settings

Name	Analytics (Annual/Config/Event)	Archive (Annual/Config/Event)	Max Storage	Analytics Usage (Block/Max)	Archive Usage (Block/Max)
Security Fabric (1)	272 (100%)	1.0 (100%)	70 GB	24.5 GB (35%)	2.9 GB (4%)

Activate Windows
Go to Settings to activate Windows.

FortiAnalyzer

System Settings

Edit Log Storage Policy - ADOM: root

Analytics Policy

Analytics Details

14%

Max Limit

History of Disk Utilization for Logs

Disk Policy

Keep Logs for Analytics: 2 Days

Keep Logs for Archive: 2 Days

Disk Utilization

Allocated: 70 GB (Maximum Available: 75.9 GB)

Analytics Archive: 20%

Alert and Delete When Usage Reaches: 90%

OK Cancel

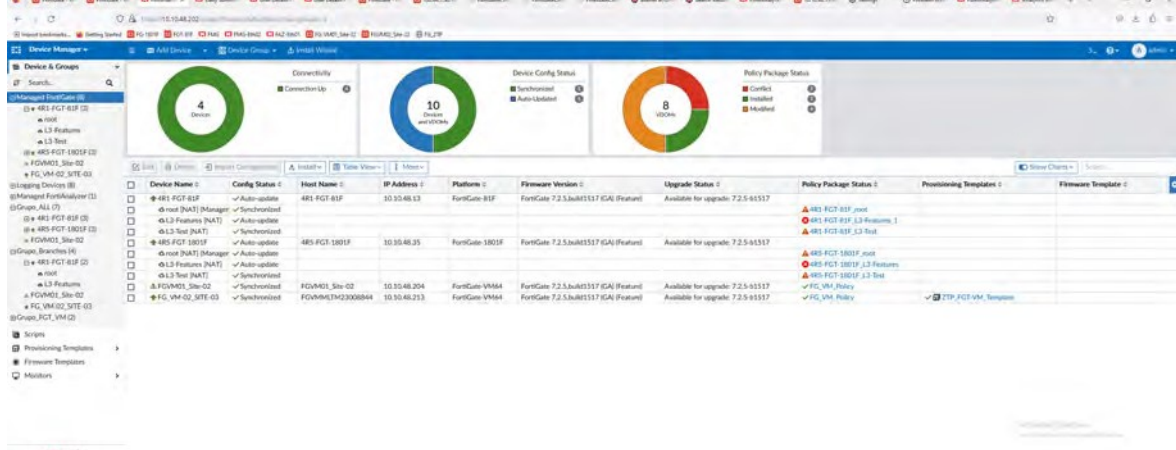
TESTE OK

O FortiAnalyzer faz uma distinção dos logs de duas formas, uma são os logs arquivados e outras são de logs analíticos, os logs arquivados são os logs de tempo real que são arquivados e comprimidos e considerados offline, já os logs analíticos são indexados em um banco de dados SQL e considerados online.

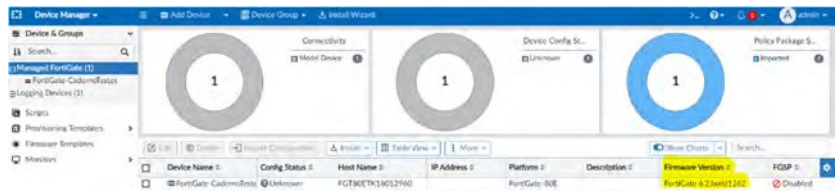
	<h3>Analytics and Archive logs</h3> <p>Logs in FortiAnalyzer are in one of the following phases.</p> <ul style="list-style-type: none"> Real-time log: Log entries that have just arrived and have not been added to the SQL database. These logs are stored in Archive in an uncompressed file. Archive logs: When a real-time log file in Archive has been completely inserted, that file is compressed and considered to be offline. Analytics logs or historical logs: Indexed in the SQL database and online. <p>Use a data policy to control how long to retain Analytics and Archive logs.</p> <ul style="list-style-type: none"> Archive logs Analytic logs
Comentário	Fonte: "Analytics and Archive logs" acessado em: https://docs.fortinet.com/document/fortianalyzer/7.2.2/administration-guide/761825/analytcs-and-archive-logs

5.4.39 Solução deve incluir monitoramento gráfico que fornece uma maneira fácil

monitorar o status de gateways, apresentando os seguintes status:

Item de Teste - 5.4.39.1	Versão do sistema operacional;
Objetivo do Teste	Verificar se a solução de gerenciamento possui visualização das versões do sistema operacional dos equipamentos gerenciados.
Configuração do Teste	Demonstrar versões de sistemas operacionais gerenciados.
Procedimento do Teste	Demonstrar versões de sistemas operacionais gerenciados.
Evidências	 <p>The screenshot shows the FortiManager web interface. At the top, there are three circular gauges: '4 Devices' (green), '10 Devices not online' (blue), and '8 100%' (orange). Below these is a table with columns: Device Name, Config Status, Host Name, IP Address, Platform, Firmware Version, Upgrade Status, Policy Package Status, Provisioning Template, and Firmware Template. The table lists several devices including 481-FGT-81F, 485-FGT-1801F, FGV401-Site-02, and FGV401-Site-03. The bottom left of the screenshot shows the Fortinet logo and the text 'TESTE OK'.</p>

Na aba de “Device Manager” podemos ter acesso a algumas informações dos equipamentos gerenciados, entre elas, a versão do sistema operacional.



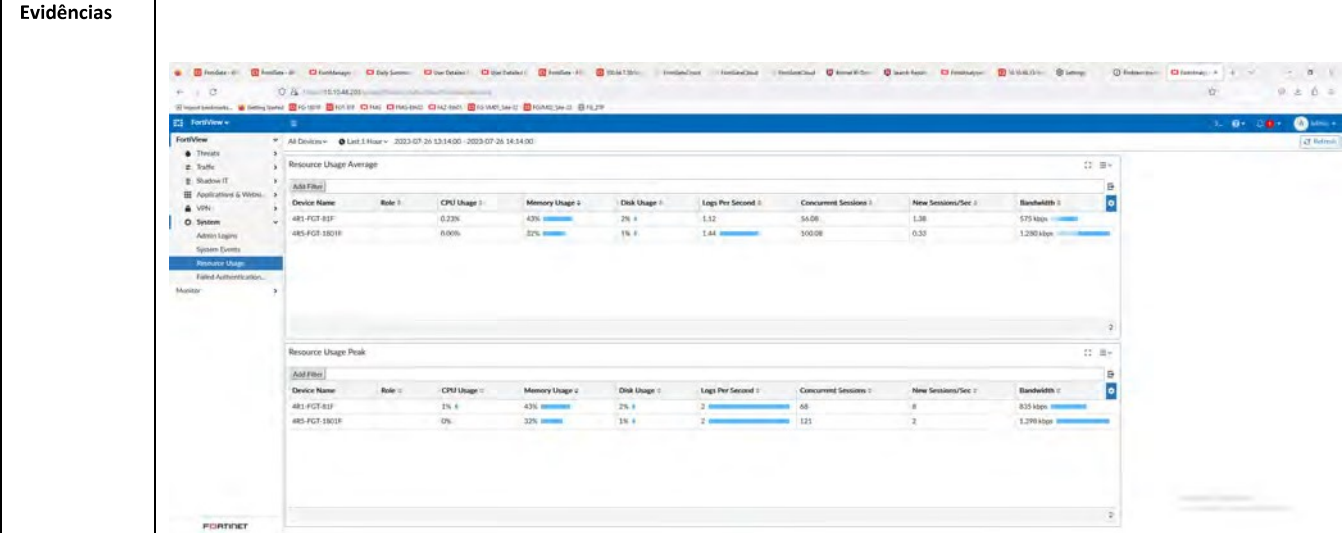
Comentário

Item de Teste - 5.4.39.2 Informações de utilização de CPU dos gateways gerenciados;

Objetivo do Teste Verificar se a solução de gerenciamento possui visualização da utilização de CPU dos gateways gerenciados.

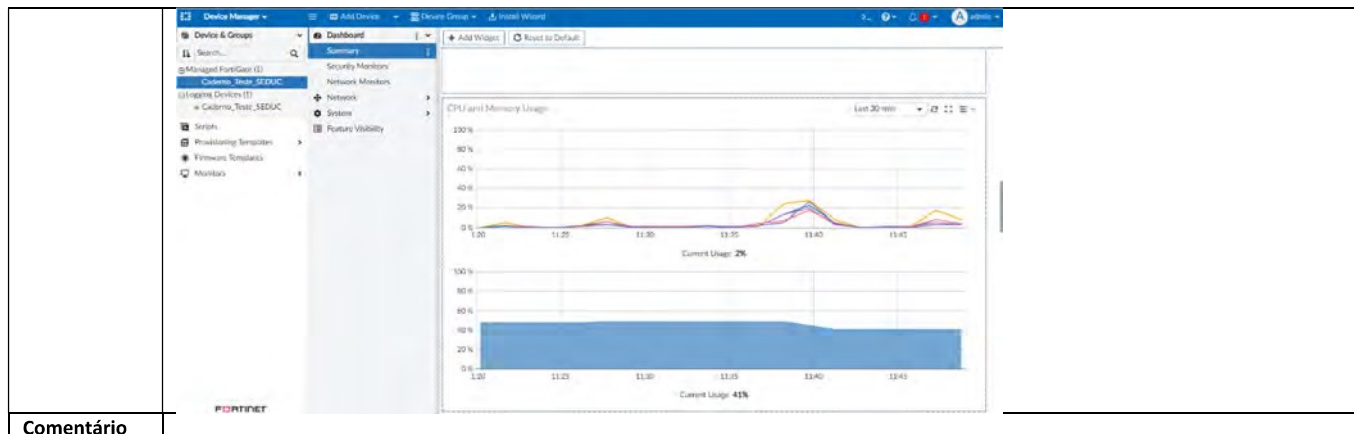
Configuração do Teste Demonstrar consumo de CPU dos gateways gerenciados.

Procedimento do Teste Demonstrar consumo de CPU dos gateways gerenciados.

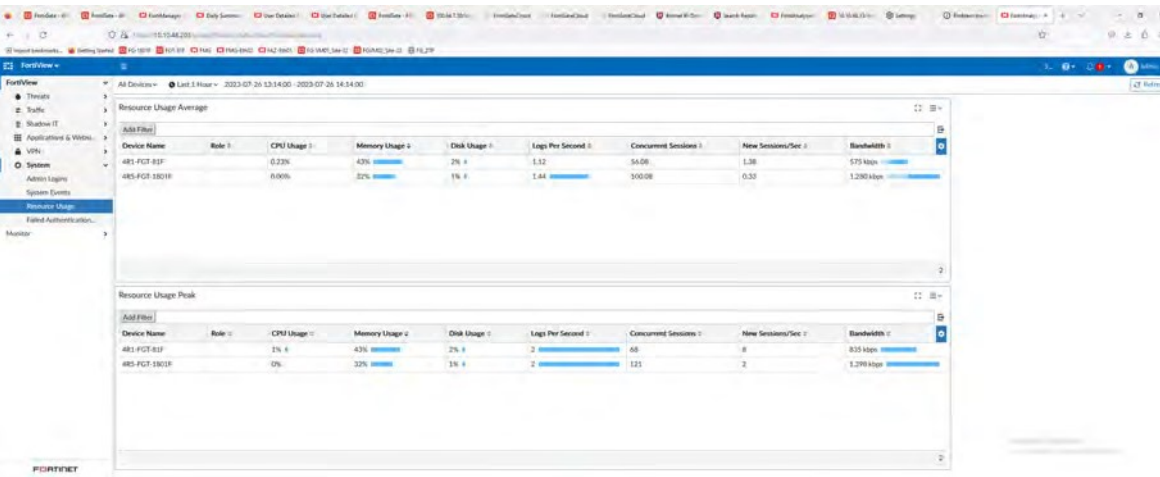


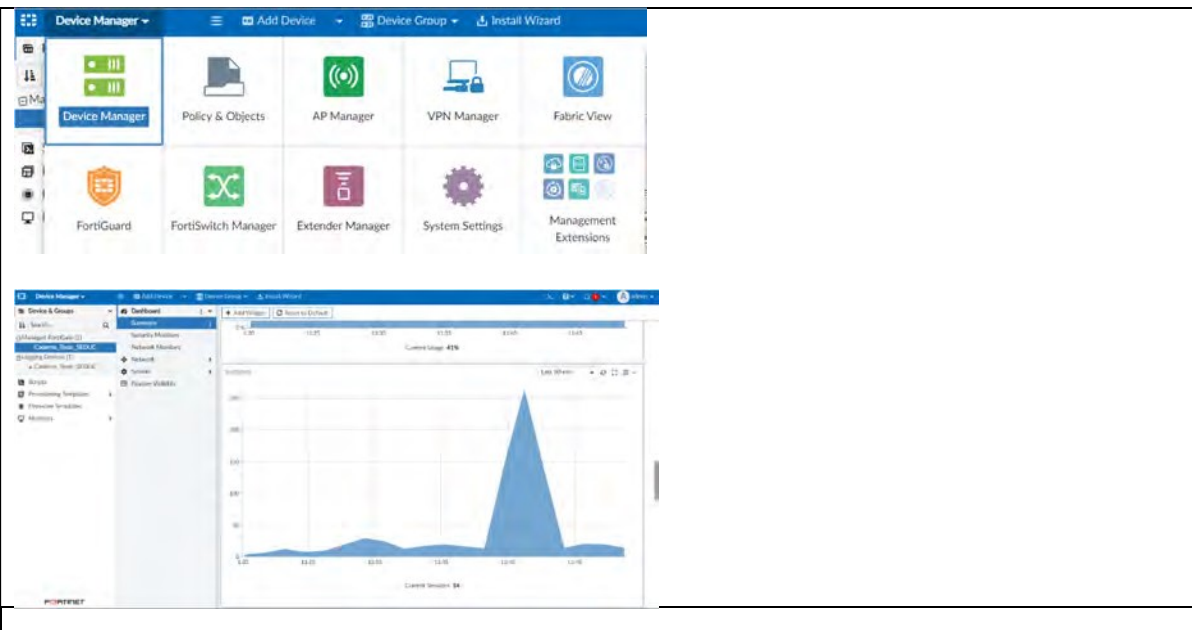
TESTE OK

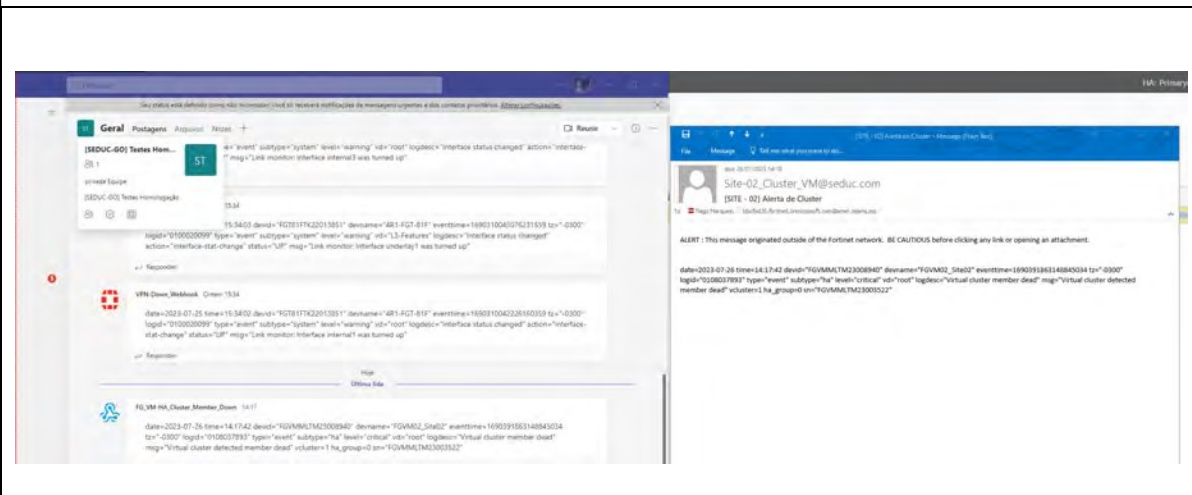
Na aba de “Device Manager” podemos selecionar qualquer um dos equipamentos gerenciados. Quando fazemos isso, podemos ter visualização de diversas informações daquele equipamento, entre elas, a quantidade de CPU que está sendo utilizada.

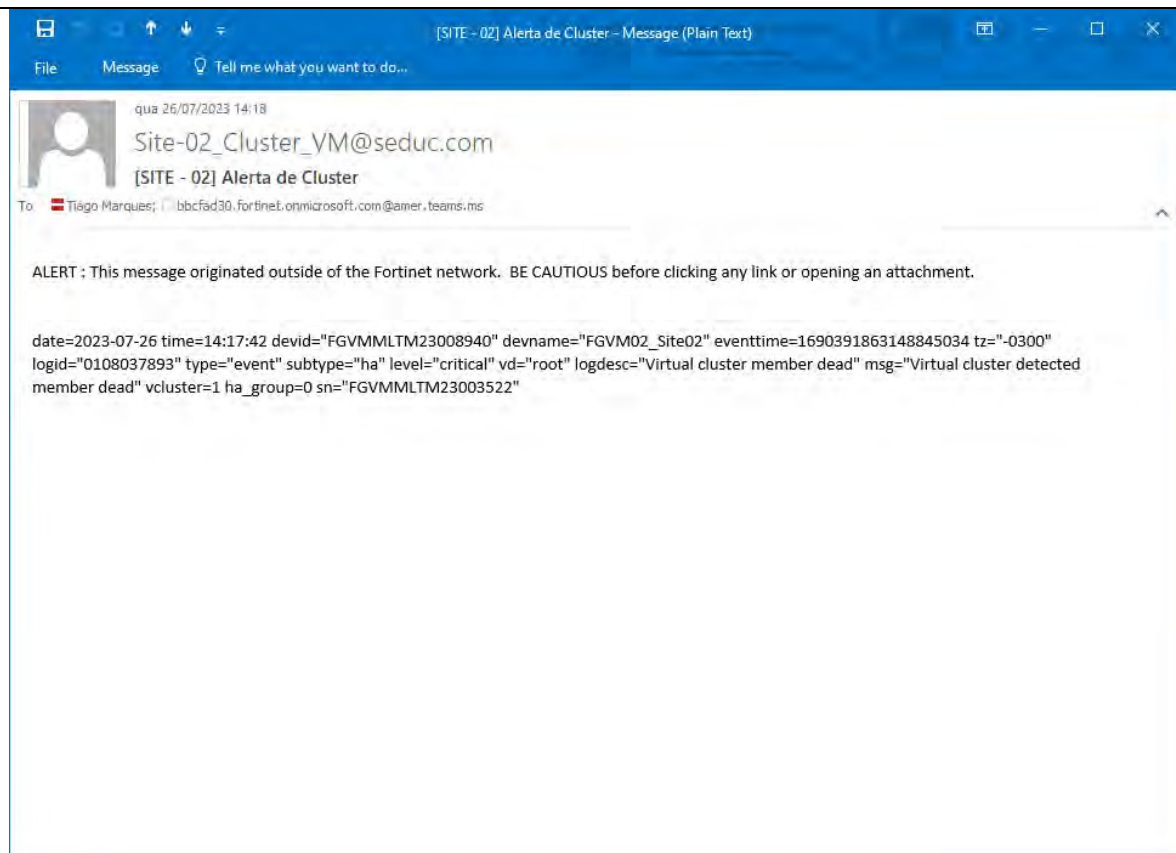


Comentário

Item de Teste - 5.4.39.3	Informações de conexões concorrentes dos gateways gerenciados;
Objetivo do Teste	Verificar se a solução de gerenciamento possui visualização da quantidade de conexões concorrentes dos gateways gerenciados.
Configuração do Teste	Demonstrar consumo de conexões concorrentes por gateways gerenciados.
Procedimento do Teste	Demonstrar consumo de conexões concorrentes por gateways gerenciados.
Evidências	 <p>The screenshot shows the Fortinet FortiView interface. It displays a table of resource usage for managed devices. The table has columns for Device Name, Role, CPU Usage, Memory Usage, Disk Usage, Logs Per Second, Concurrent Sessions, New Sessions/Sec, and Bandwidth. Below the table, there are two more tables: 'Resource Usage Average' and 'Resource Usage Peak', both showing similar metrics for the same devices.</p> <p>TESTE OK</p> <p>Na aba de “Device Manager” podemos selecionar qualquer um dos equipamentos gerenciados. Quando fazemos isso, podemos ter visualização de diversas informações daquele equipamento, entre elas, a quantidade de conexões concorrentes.</p>

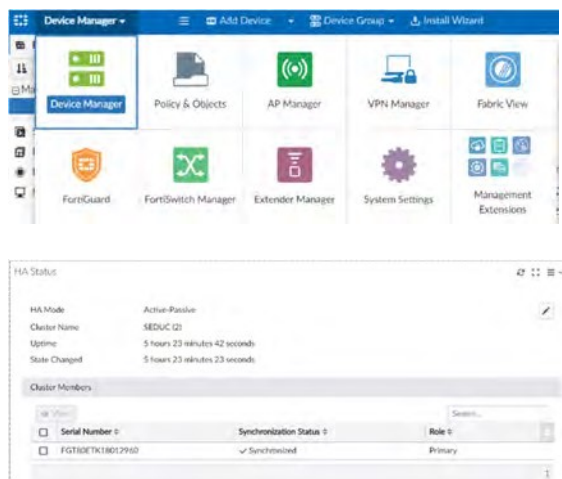
<p>Comentário</p>	
--------------------------	--

<p>Item de Teste - 5.4.40</p>	<p>Alertar quando um membro estiver desconectado do cluster;</p>
<p>Objetivo do Teste</p>	<p>Verificar se o equipamento de gerência alerta quando um membro estiver desconectado do cluster.</p>
<p>Configuração do Teste</p>	<p>Demonstrar alerta de equipamento indisponível.</p>
<p>Procedimento do Teste</p>	<p>Demonstrar alerta de equipamento indisponível.</p>
<p>Evidências</p>	

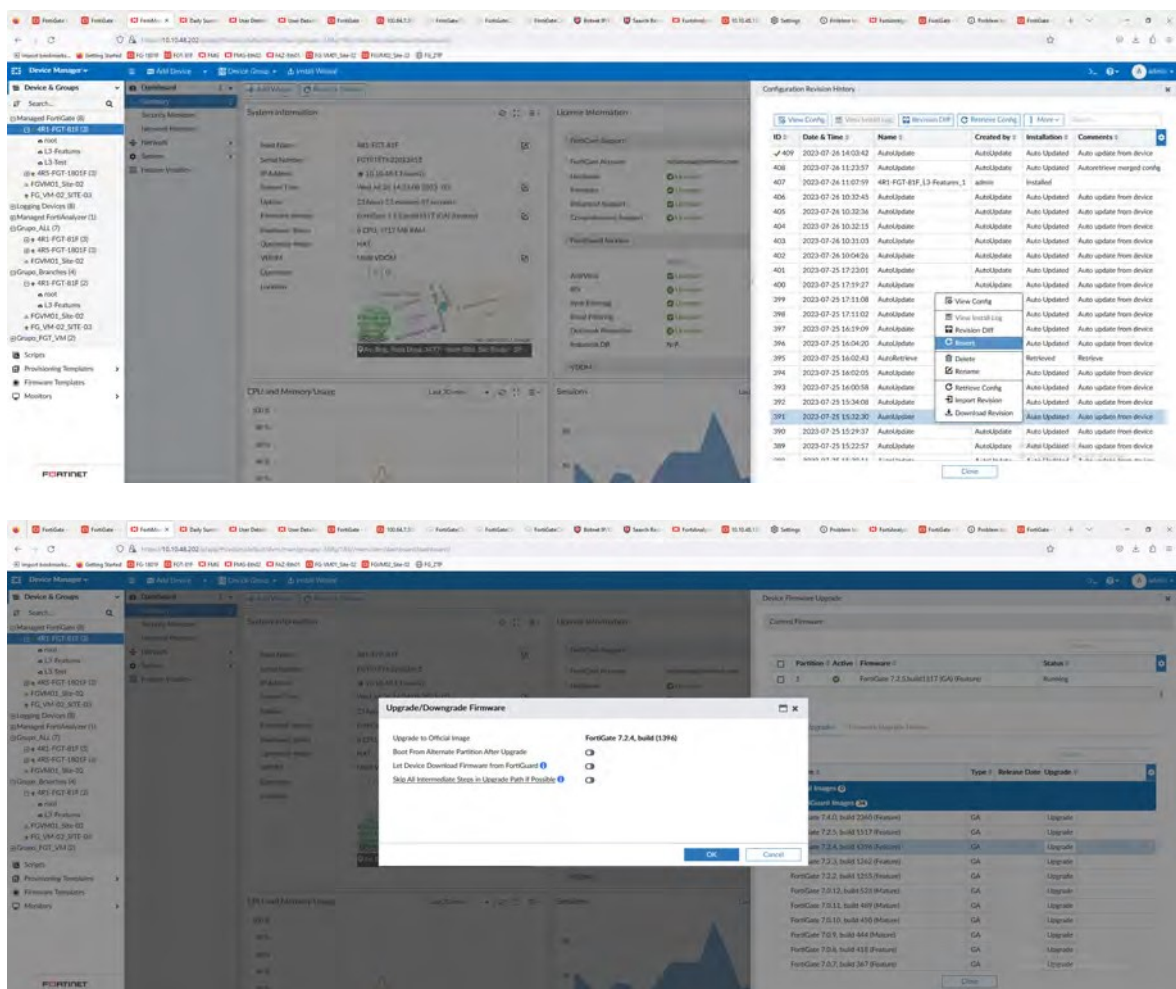


TESTE OK

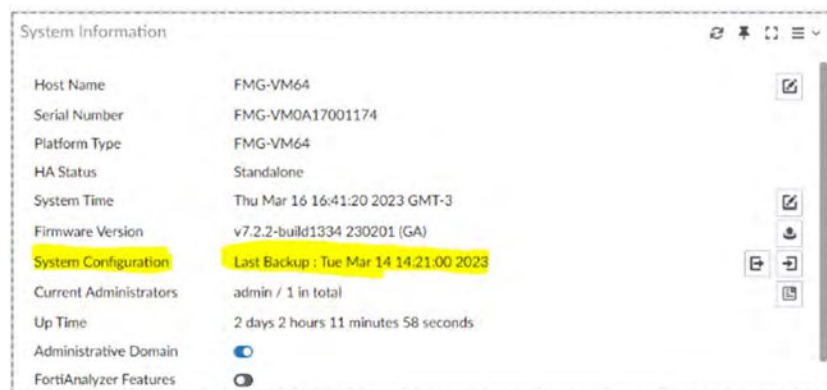
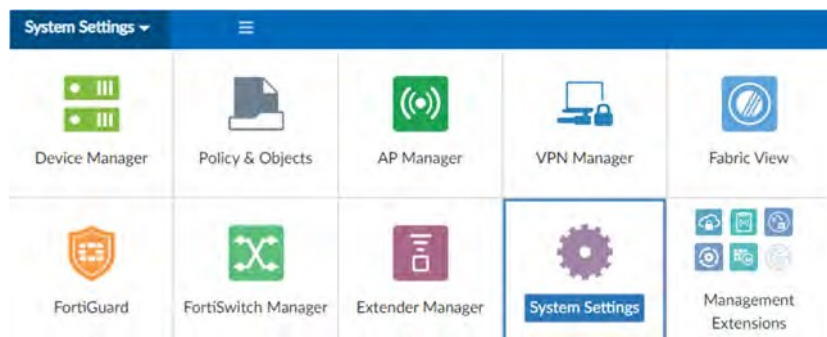
Na aba de "Device Manager" podemos selecionar qualquer um dos equipamentos gerenciados. Quando fazemos isso, podemos ter visualização de diversas informações daquele equipamento, entre elas, o estado dos clusters.



Comentário	
------------	--

Item de Teste - 5.4.42	Suportar rollback de configuração para a última configuração salva e do sistema operacional para a última versão local;
Objetivo do Teste	Verificar se o equipamento de gerência suporta rollback de configuração.
Configuração do Teste	Demonstrar rollback de configuração.
Procedimento do Teste	Demonstrar rollback de configuração.
Evidências	 <p>The top screenshot shows the 'Configuration Revision History' window in the FortiGate GUI. It displays a table of configuration revisions with columns for ID, Date & Time, Name, Created by, Installation, and Comments. A context menu is open over the entry with ID 397, showing options like 'View Config', 'View Install Log', 'Reversion Diff', 'Reversion Config', 'Rollback', 'Download Revision', and 'Download Revision'. The bottom screenshot shows the 'Upgrade/Downgrade Firmware' dialog box, which offers to upgrade to the official image 'FortiGate 7.2.4, build 1394' and includes checkboxes for 'Build From Alternate Partition After Upgrade' and 'Set All Intermediate Seros to Upgrade Path if Possible'.</p>
	TESTE OK

Na parte de “System Settings podemos ter uma tabela com diversas informações do FortiManager, entre elas a configuração atual do sistema e qual foi a última vez que um backup foi tirado



Caso haja a necessidade basta apertar a tecla de “Restore” e importar a configuração desejada.

Comentário	<p>System Configuration Last Backup : Tue Mar 14 14:21:00 2023</p> <p>Restore System</p> <p>Upload file by drag & drop here or Browse</p> <p>Password <input type="password"/> Maximum password length: 63 <input type="checkbox"/></p> <p><input checked="" type="checkbox"/> Overwrite current IP, routing and HA settings</p> <p><input checked="" type="checkbox"/> Restore in Offline Mode <input type="checkbox"/></p> <p>OK Cancel</p>
------------	--

8. TESTES

Os testes serão separados considerando Capacidades e Funcionalidades.

Os testes de capacidade foram separados em 4 testes, seguindo a dinâmica do edital.

Os testes de funcionalidades serão executados conforme orientação da equipe técnica da SEDUC, de acordo com a necessidade do item a ser testado, seguindo topologia apresentada.

8.1. TESTES DE CAPACIDADE

Serão executadas 4 baterias de Testes de Capacidade por equipamento, sendo os seguintes testes:

8.1.1. THROUGHPUT CONFORME SUBITENS DO ANEXO VII:

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);

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);

8.1.2. IPSEC VPN CONFORME OS SUBITENS DO ANEXO VII:

5.1.5.2 Possuir no mínimo 9,5 (Nove e cinco décimos) Gbps de throughput para VPN IPsec;

5.2.3.2 Possuir no mínimo 1,5 (Um e cinco décimos) Gbps de troughput para Ipsec VPN;

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

www.nct.com.br

8.1.3. NOVAS CONEXÕES POR SEGUNDO:

5.1.6.1 Permitir no mínimo 150.000 (cento e cinquenta mil) novas conexões por segundo por nó do cluster;

5.2.4.1 Permitir no mínimo 35.000 (trinta e cinco mil) novas conexões por segundo;

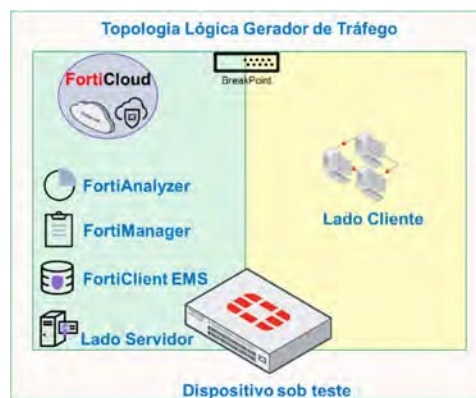
8.1.4. CONEXÕES CONCORRENTES:

5.1.6.2 Permitir no mínimo 4.000.000 (quatro milhões) conexões simultâneas por nó do cluster;

5.2.4.2 Permitir no mínimo 200.000 (duzentas mil) conexões simultâneas;

8.2. TESTES DE CAPACIDADE

8.2.1. TOPOLOGIA



8.2.1.1. • TESTE 01 – THROUGHPUT

- Tráfego Enterprise Mix
- Base de Regras com funcionalidades:
 - Firewall, IPS, Controle de Aplicação, Proteção Contra Malware;
 - Logging habilitado para todas as sessões e conexões;
- Capacidade mínima considerada para aferimento sendo acima do requisitado conforme itens supracitados;
- Janela de teste composta por duas fases sendo:
 - Rampa de subida com tempo inferior a 1 minuto que não será considerada para aferição;
 - Curso após estabilização com tempo de 5 minutos, sendo considerado para aferição.
- Taxa de erro aceitáveis inferior a 0.5% para todo o teste
- Conexões TCP encerradas via handshake completo (FIN), visando de fato submeter o hardware a situação real e mais onerosa, não sendo considerado qualquer "reset"
- Inspeção de SSL
 - Para identificação dos campos SNI (cliente -> server); CN (server -> cliente)
- Todas as assinaturas de: IPS, antivírus e aplicações ativas com base atualizada no momento do teste
- Funcionalidades de bypass desativadas, sendo apresentada no momento do teste as saídas dos seguintes comandos:
 - Antivirus
 - config system global
 - get | grep av-failopen
 - >> resultado esperado:
 - av-failopen: off
 - av-failopen-session : disable

- IPS
 - config ips global
 - get | grep fail-open
 - resultado esperado
 - fail-open : disable
 - get |grep database
 - resultado esperado
 - database : extended
- Mecanismos de alívio de fila desativados
- Envio de malware e tráfegos de ataque
- Evidências utilizadas na comprovação de pleno atendimento editalício:
 - Telas dos appliances sob teste
 - Telas do gerador
 - Logs de bloqueio visando demonstrar o bloqueio de conteúdo malicioso nas funcionalidades de Antivírus e IPS durante o período de curso do teste

8.2.1.2. TESTE 02 – IPSEC VPN

- Criptografia AES256-SHA256
- Janela de teste composta por duas fases sendo:
 - Rampa de subida com tempo inferior a 1 minuto que não será considerada para aferição;
 - Curso após estabilização com tempo de 5 minutos, sendo considerado para aferição.
- Taxa de erro aceitáveis inferior a 0.5% para todo o teste

8.2.1.3. TESTE 03 – NOVAS CONEXÕES POR SEGUNDO

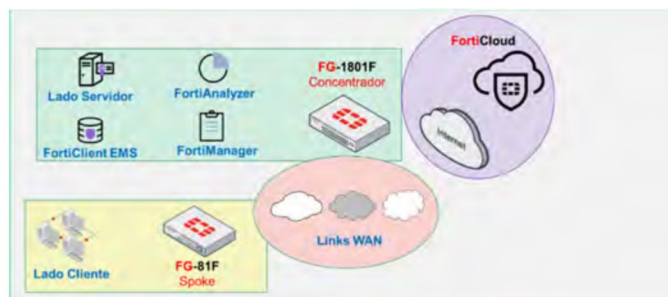
- Fluxo em HTTP 64 bytes
- Janela de teste composta por duas fases sendo:
 - Rampa de subida com tempo inferior a 1 minuto que não será considerada para aferição;
 - Curso após estabilização com tempo de 5 minutos, sendo considerado para aferição.
- Foco em abrir e fechar conexões
- Conexões TCP encerradas via handshake completo (FIN), visando de fato submeter o hardware a situação real e mais onerosa, não sendo considerado qualquer “reset”
- Taxa de erro aceitáveis inferior a 0.5% para todo o teste

8.2.1.4. TESTE 04 – CONEXÕES SIMULTÂNEAS

- Fluxo em HTTP 64 bytes
- Janela de teste composta por duas fases sendo:
 - Rampa de subida com tempo inferior a 1 minuto que não será considerada para aferição;
 - Curso após estabilização com tempo de 5 minutos, sendo considerado para aferição.
- Conexões TCP serão mantidas abertas como requisitado em teste.
- Taxa de erro aceitáveis inferior a 0.5% para todo o teste

8.2.1.5. TESTE DE FUNCIONALIDADES

8.2.2. TOPOLOGIA



9. CONCLUSÃO

Encerradas as demonstrações, e conforme detalhamento neste documento, em conjunto com documentação técnica e apontamentos complementares já apresentados em outras fases do processo, resta comprovado o atendimento da solução ofertada pela NCT no Lote 01 do PREGÃO ELETRÔNICO 01/2023.

Brasília/DF, 01 de agosto de 2023

JOSÉ ARMANDO DOS REIS COSTA
DIRETOR TÉCNICO
NCT INFORMÁTICA

JOSE ARMANDO DOS REIS COSTA:6362503210
4

Digitally signed by JOSE ARMANDO DOS REIS COSTA:6362503210
DN: c=BR, o=ICP-Brasil, ou=00000101872465, ou=Superintendência Federal do Brasil - SFB, ou=SEFE - OFF A3, ou=AC SERASA RFB, ou=871948700116, ou=PRESENCIAL, cn=JOSE ARMANDO DOS REIS COSTA:6362503210
Reason: I am approving this document
Location:
Date: 2023.08.01 13:29:55-03'00'
Foxit PDF Reader Version: 12.1.2

Assinado de forma digital
por CRYSTINE
JORANHEZON
RODRIGUES
Dados: 2023.08.01
13:59:24 -03'00'

CRYSTINE JORANHEZON RODRIGUES
GERENTE DE DESENVOLVIMENTO DE NEGÓCIOS
NCT INFORMÁTICA