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

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 uti lizadas 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.

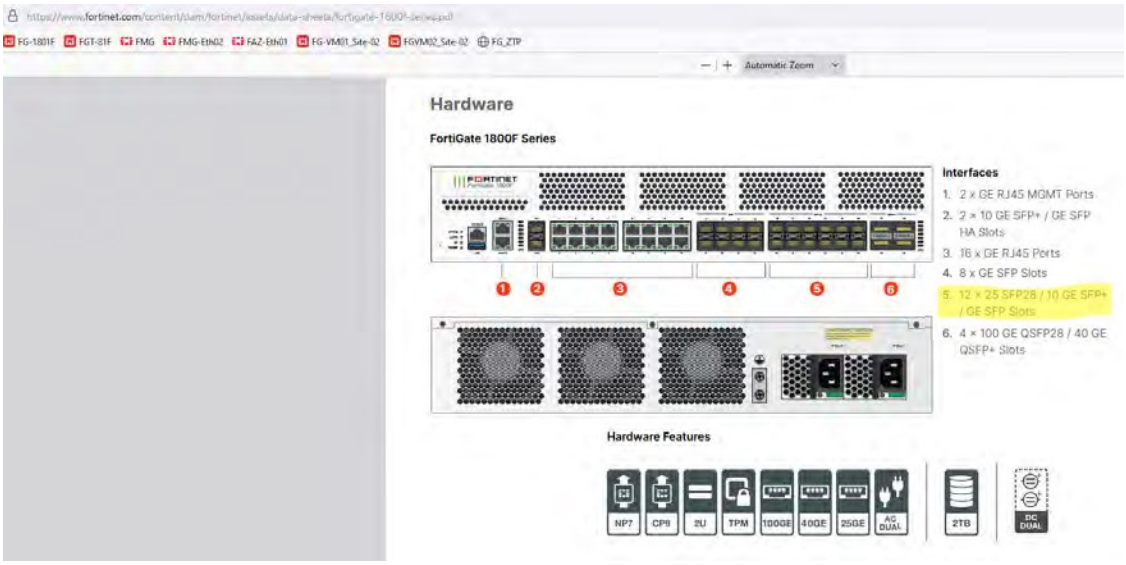
A escolha foi realizada em razão de se tratar de última versão mais estável, sendo a recomendada pelo fabricante. Além de ter sido a mais recente utilizada durante o processo de elaboração de planilha ponto a ponto no presente processo.

7. ITENS OBRIGATÓRIOS PARA TESTE DE CONFORMIDADE

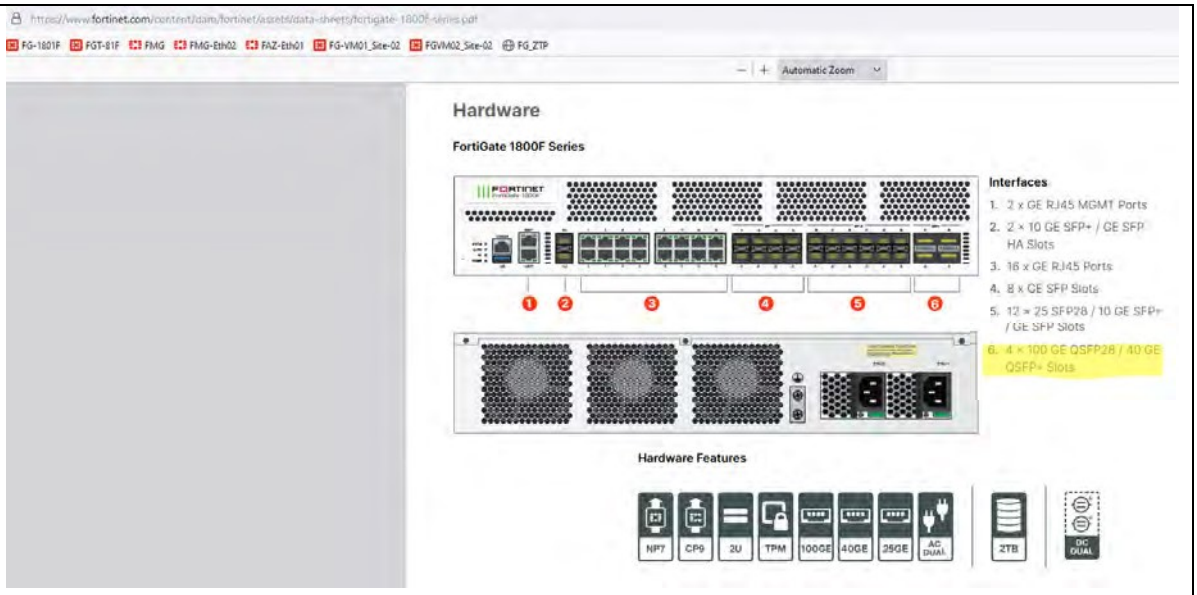
5.1 Cluster de Firewall Tipo 1

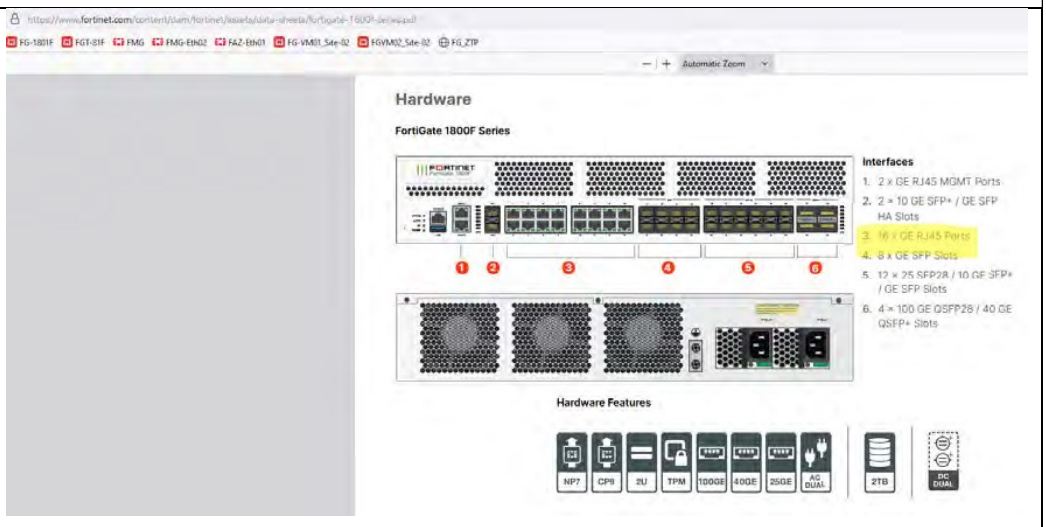
5.1.4 INTERFACES

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

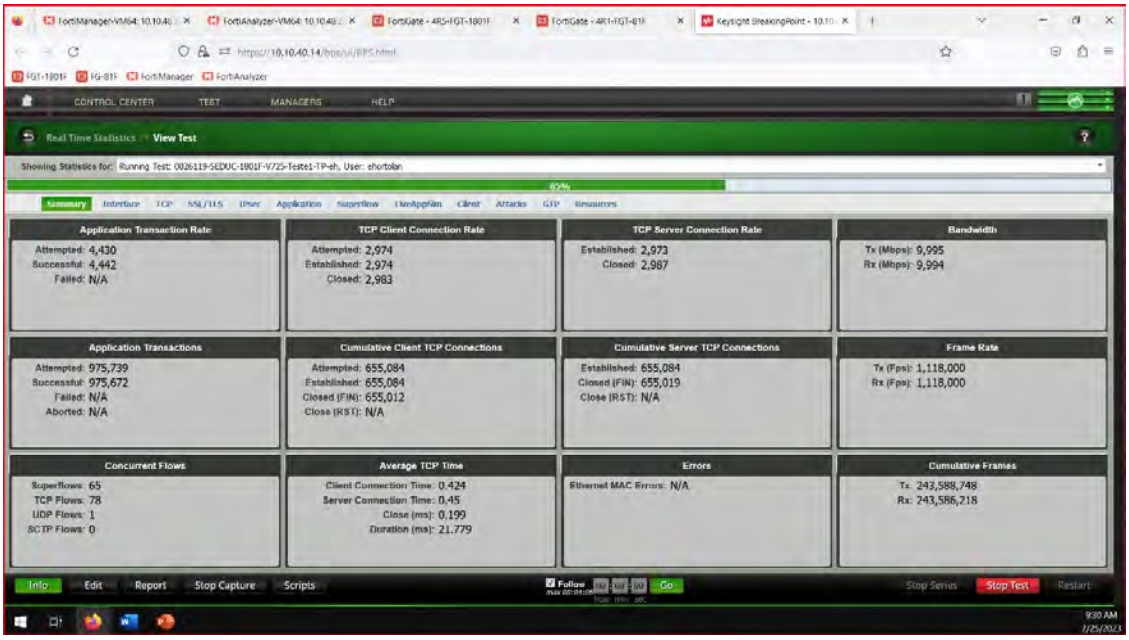
Item 5.1.4.2	Possuir no mínimo 02 (duas) interfaces 40 Gigabit QSFP+ (ou superior)
Objetivo do Teste	Validar se o appliance possui 02 (duas) interfaces de 40 Gigabit QSFP+ (ou superior)
Configuração do Teste	Validar que o equipamento possui 02 interfaces de 40 Gigabit QSFP+
Procedimento do Teste	Visual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

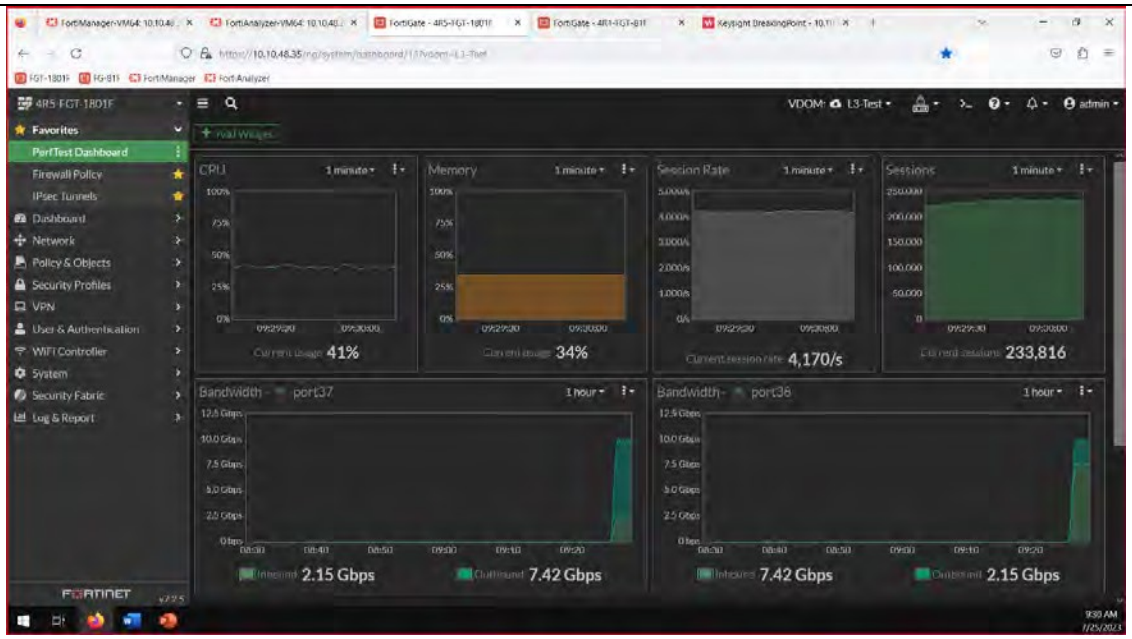
Evidências	 **TESTE OK**
Comentário	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1800f-series.pdf

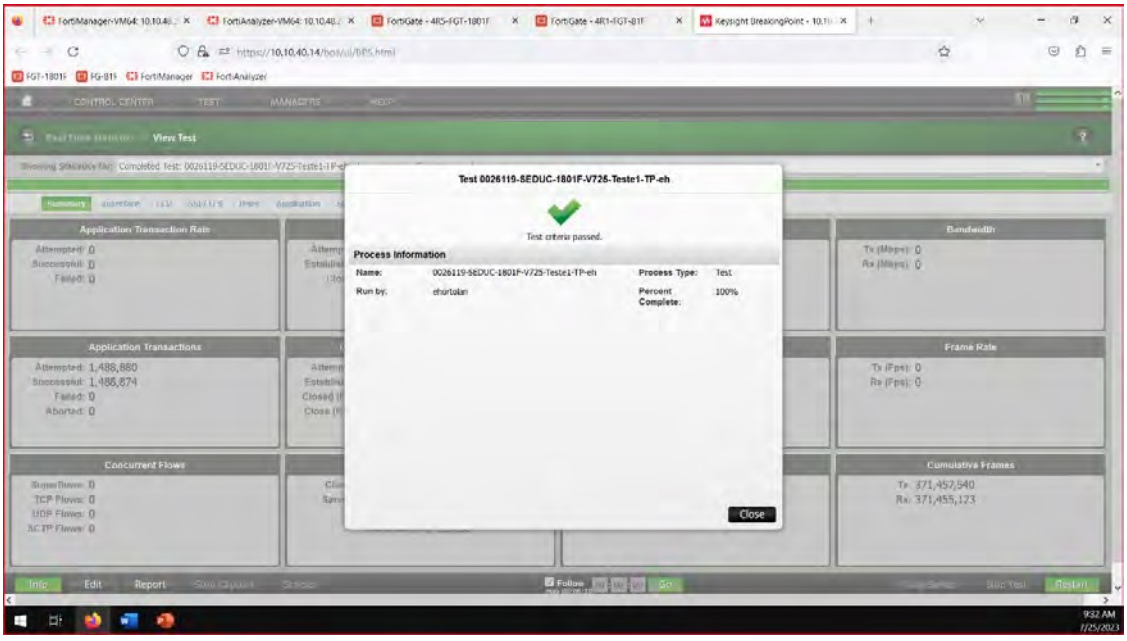
Item de Teste 5.1.4.3	Possuir no mínimo 04 (quatro) interfaces RJ45 de no mínimo 1 Gigabit
Objetivo do Teste	Validar se o appliance possui no mínimo 04 interfaces RJ45 de no mínimo 1GB
Configuração do Teste	Validar que o equipamento possui 04 interfaces RJ45 1 Gigabit
Procedimento do Teste	Visual e comprovação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

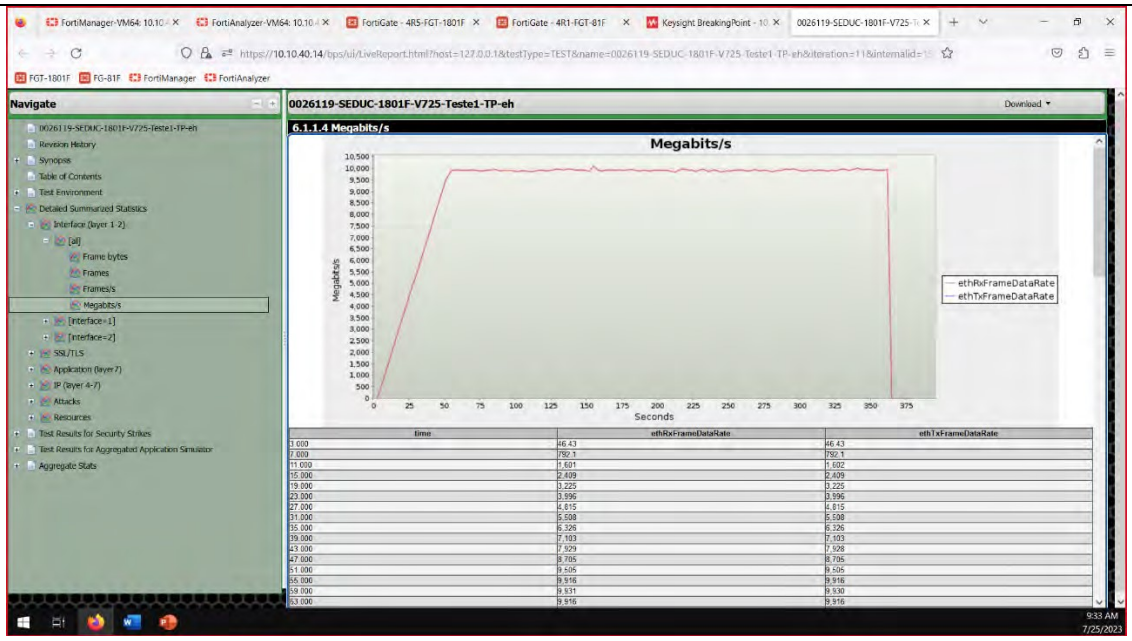
	TESTE OK
Comentário	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate-1800f-series.pdf

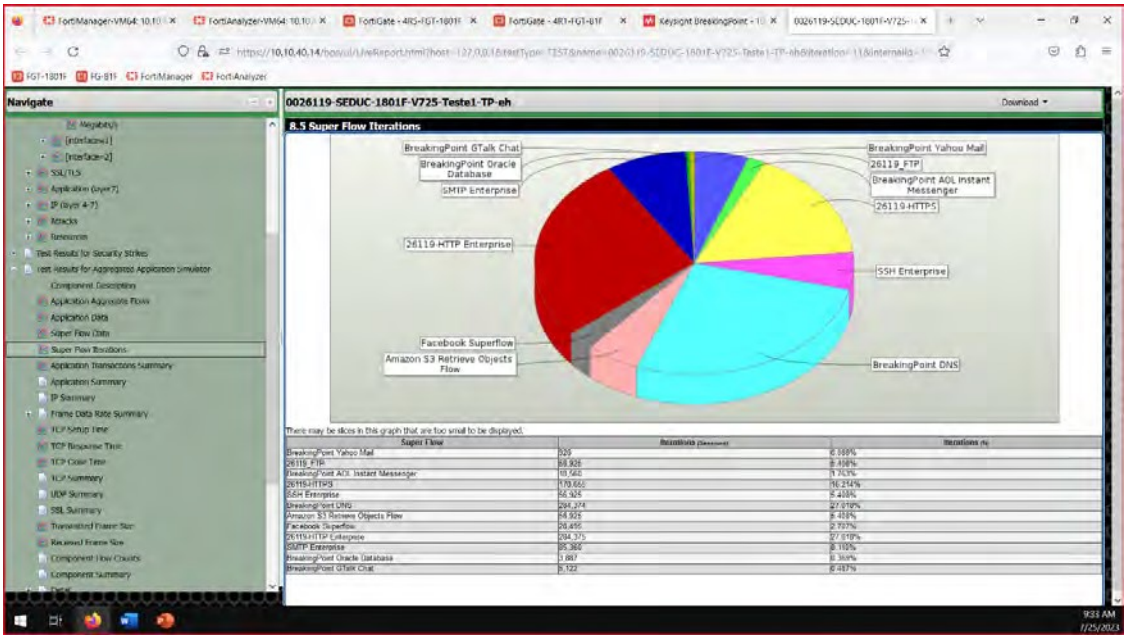
5.1.5 TROUGHPUT

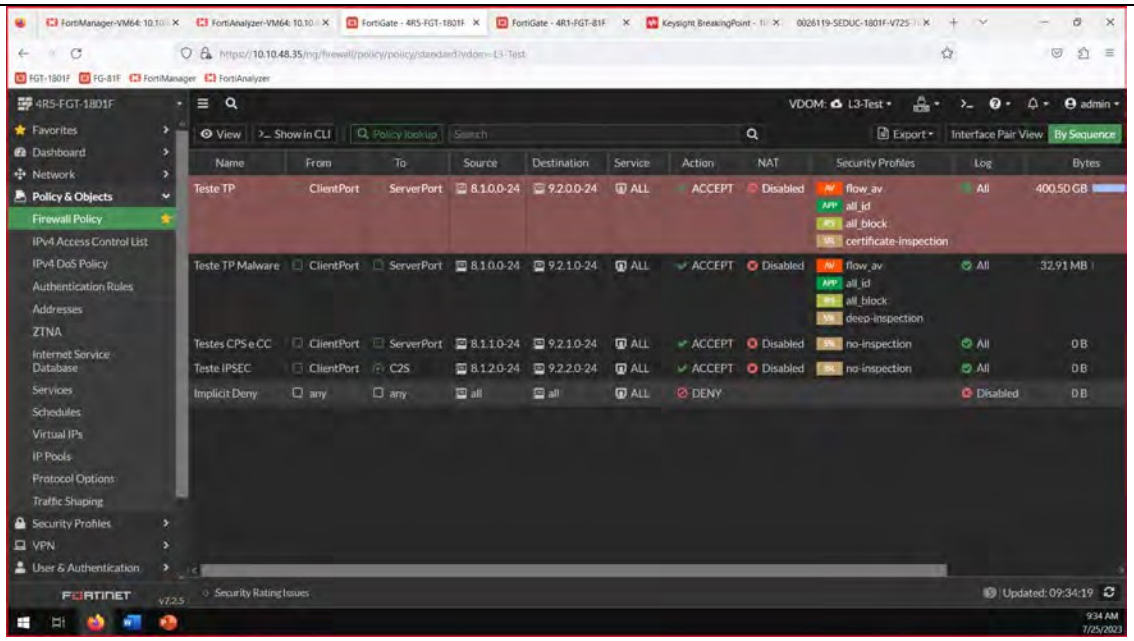
Item de Teste 5.1.5.1	Possuir throughput de no mínimo 9 (Nove) Gbps de tráfego real por nó do cluster com as funcionalidades de segurança habilitadas (Firewall,IPS, Logging, Controle de Aplicação, Proteção contra Malware)
Objetivo do Teste	Validar o throughput de no mínimo 9 Gbps de tráfego real com 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. 

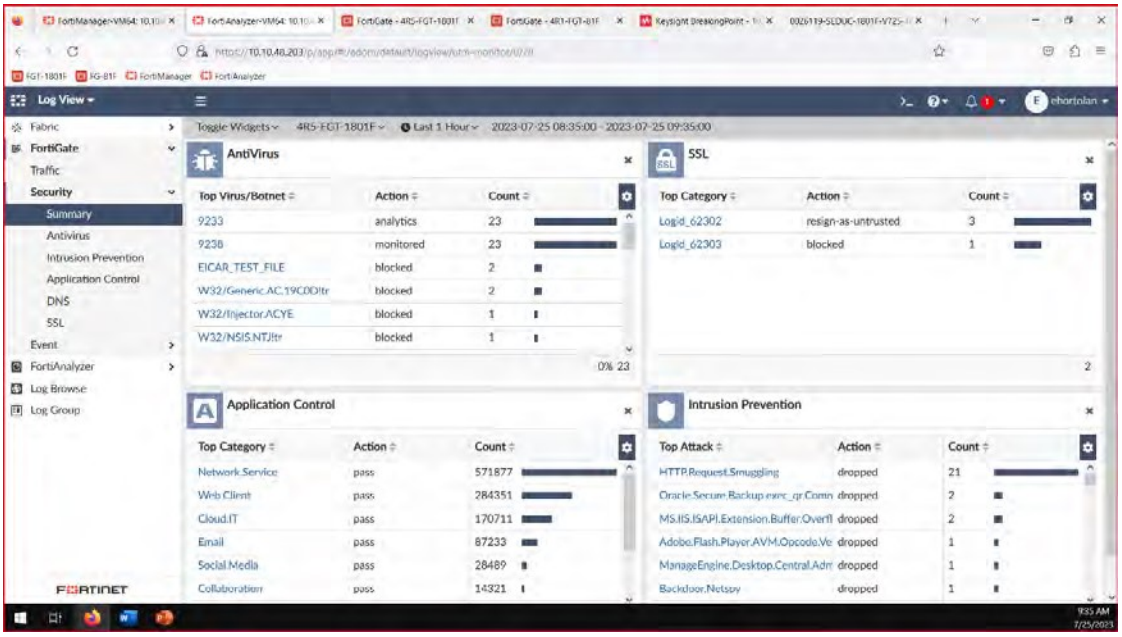

4RS-FGT-1801F
Favorites
PerfTest Dashboard
Firewall Policy
IPsec Tunnels
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
System
Security Fabric
Log & Report
VDOM: L3-Test
admin
CPU
1 minute
41%
Memory
34%
Session Rate
4,170/s
Sessions
233,816
Bandwidth - port37
1 hour
2.15 Gbps
7.42 Gbps
Bandwidth - port36
7.42 Gbps
2.15 Gbps
FORTINET

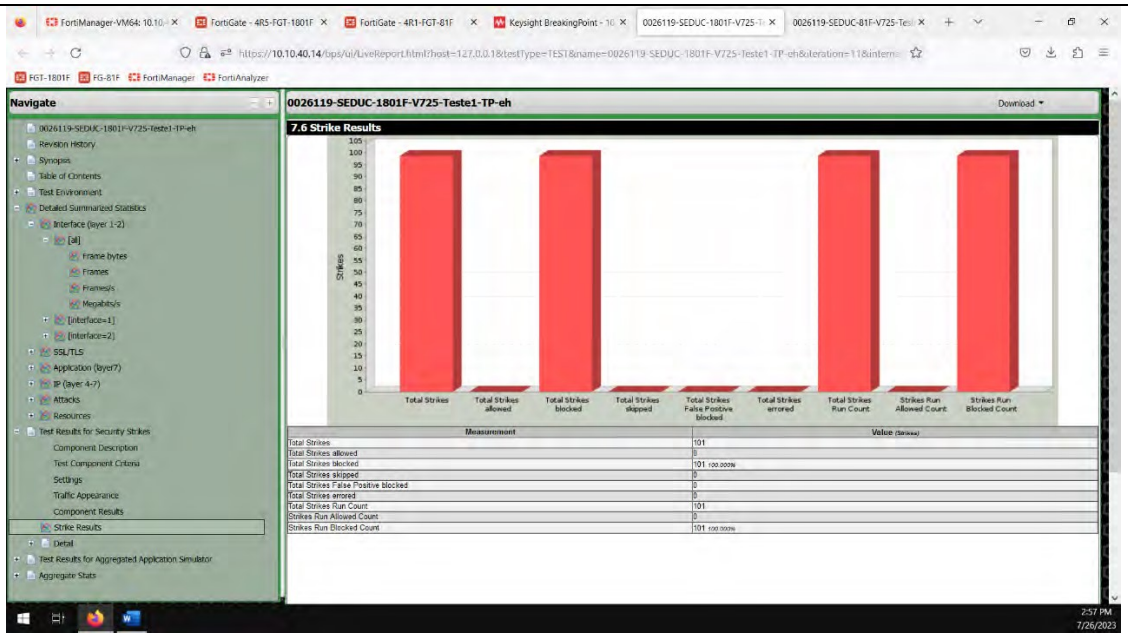

Test 0026119-SEDUC-1801F-V725-Teste1-TP-eh
Test criteria passed.
Process Information
Name:
0026119-SEDUC-1801F-V725-Teste1-TP-eh
Process Type:
Test
Run by:
ehortolan
Percent Complete:
100%
Close
Application Transaction Rate
Application Transactions
Attempted: 1,486,880
Successful: 1,486,874
Failed: 0
Aborted: 0
Concurrent Flows
TCP Flows: 0
UDP Flows: 0
SCTP Flows: 0
Frame Rate
Cumulative Frames
Tx: 371,457,540
Rx: 371,455,123
Info
Edit
Report


Navigate
0026119-SEDUC-1801F-V725-Teste1-TP-eh
6.1.1.4 Megabits/s
Megabits/s
Megabits/s
Seconds
ethRxFrameDataRate
ethTxFrameDataRate

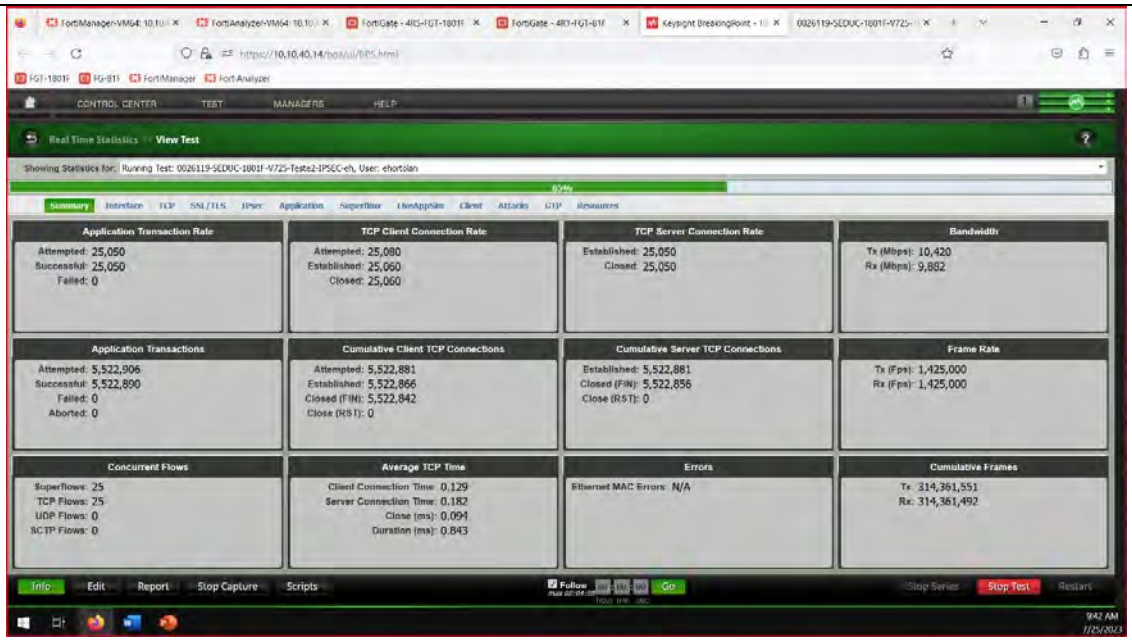

Navigate
0026119-SEDUC-1801F-V725-Teste1-TP-eh
8.5 Super Flow Iterations
BreakingPoint GTalk Chat
BreakingPoint Oracle Database
SMTP Enterprise
26119-HTTP Enterprise
FaceBook Superflow
Amazon S3 Retrieve Objects Flow
BreakingPoint Yahoo Mail
26119_FTP
BreakingPoint AOL Instant Messenger
26119-HTTPS
SSH Enterprise
BreakingPoint DNS

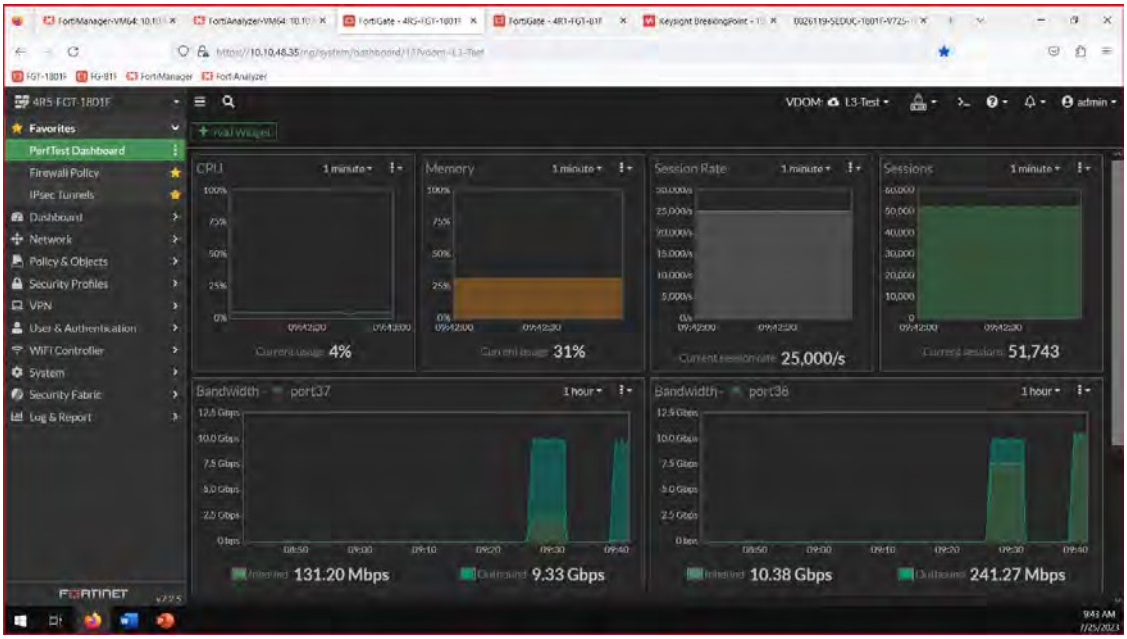

4R5-FGT-1801F
Favorites
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 Access Control List
IPv4 DoS Policy
Authentication Rules
Addresses
ZTNA
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
VDOM: L3-Test
admin
View
Show in CLI
Policy lookup
Search
Export
Interface Pair View
By Sequence
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
FORTINET
v7.2.5
Security Rating Issues
Updated: 09:34:19
9:34 AM
7/25/2023

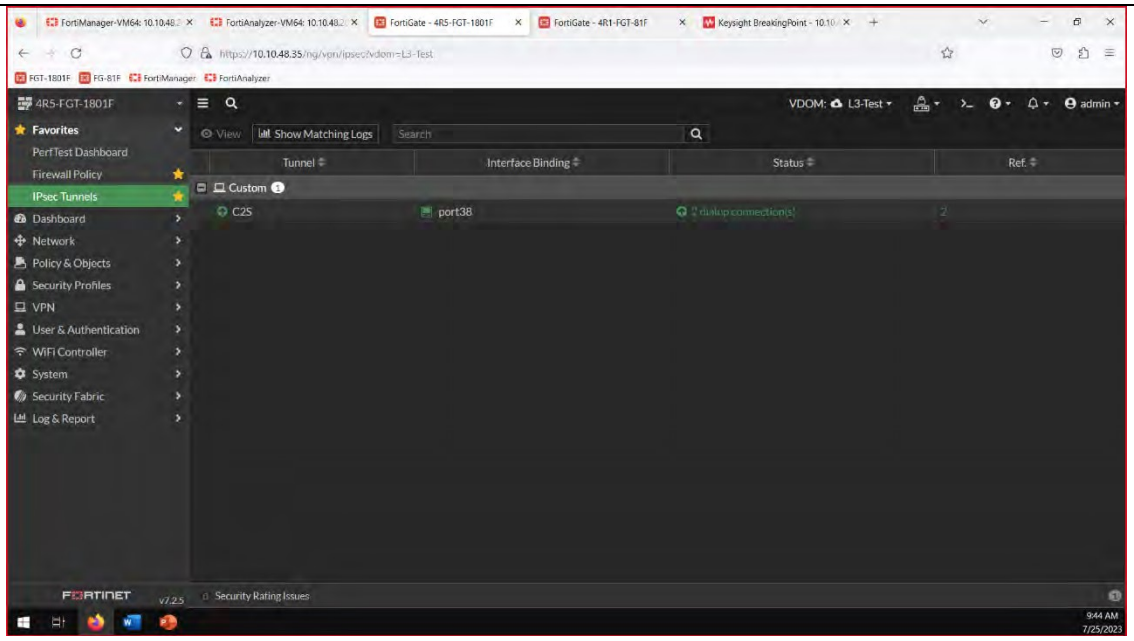

Log View
Fabric
FortiGate
Traffic
Security
Summary
Antivirus
Intrusion Prevention
Application Control
DNS
SSL
Event
FortiAnalyzer
Log Browse
Log Group
Toggle Widgets
4R5-FGT-1801F
Last 1 Hour
2023-07-25 08:35:00 - 2023-07-25 09:35:00
AntiVirus
Top Virus/Botnet
Action
Count
9233
analytics
23
9238
monitored
23
EICAR_TEST_FILE
blocked
2
W32/Generic.AC.19CDD!tr
blocked
2
W32/Injector.ACYE
blocked
1
W32/NSIS.NTJ!tr
blocked
1
0% 23
SSL
Top Category
Action
Count
Logid_62302
resign-as-untrusted
3
Logid_62303
blocked
1
2
Application Control
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
Top Attack
Action
Count
HTTP.Request.Smuggling
dropped
21
dropped
2
MS.IIS.ISAPI.Extension.Buffer.Overfl
dropped
2
Adobe.Flash.Player.AVM.Opcode.Ve
dropped
1
ManageEngine.Desktop.Central.Adr
dropped
1
Backdoor.Netsoy
dropped
1
FORTINET
9:35 AM
7/25/2023

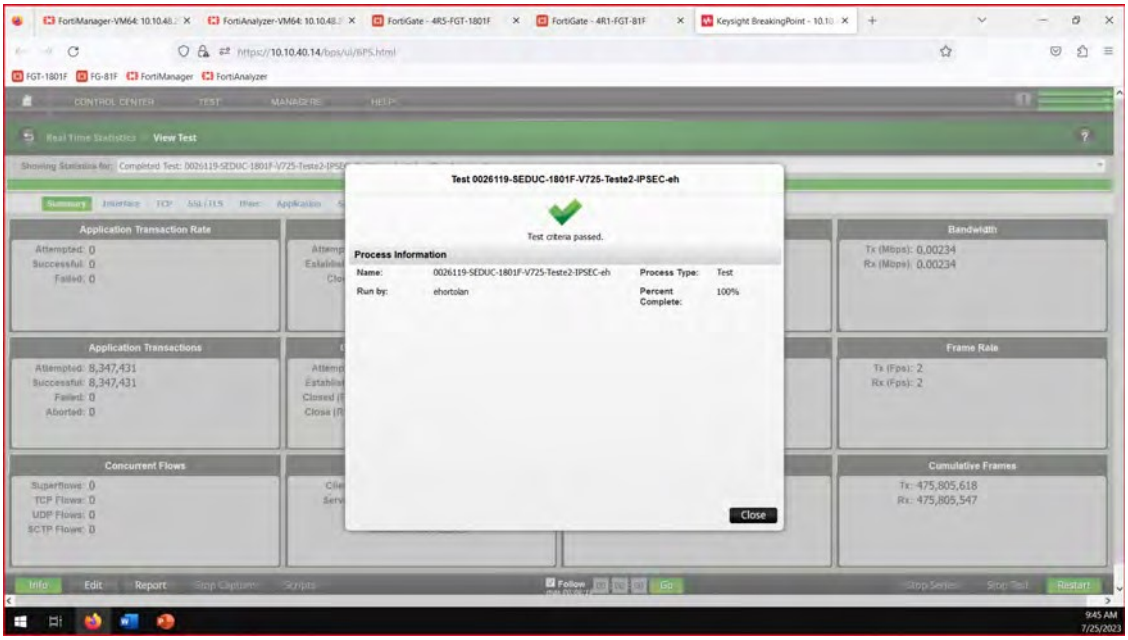
	 **TESTE OK**
Comentário	

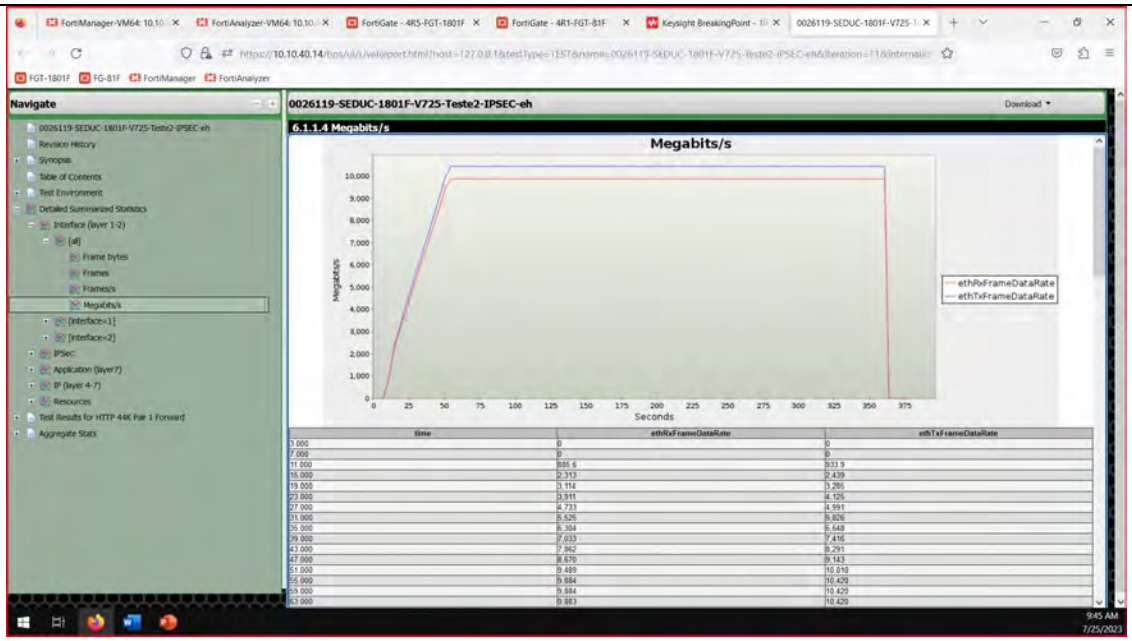
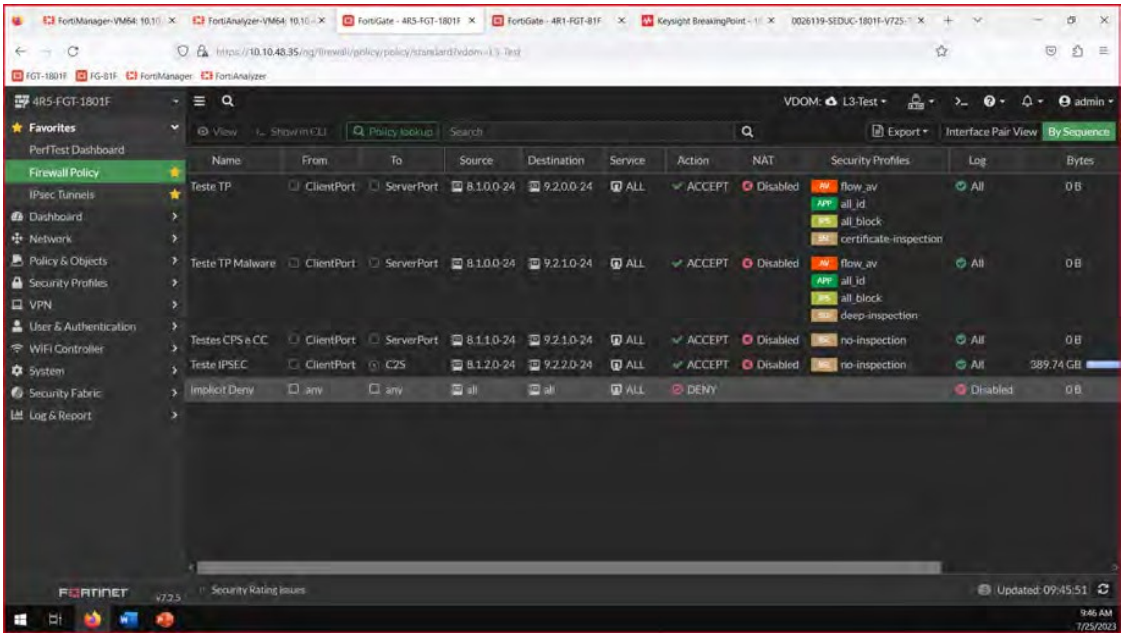
Item de Teste 5.1.5.2	Possuir no mínimo 9,5 (Nove e cinco décimos) Gbps de throughput para VPN IPsec;
Objetivo do Teste	Validar o throughput de no mínimo 9,5 Gbps de tráfego VPN IPsec.
Configuração do Teste	Teste a ser realizado no laboratório Fortinet. Será apresentado o perfil de tráfego que será gerado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


CONTROL CENTER
TEST
MANAGERS
HELP
Real Time Statistics
View Test
Application Transaction Rate
Attempted: 25,050
Successful: 25,050
Failed: 0
TCP Client Connection Rate
Attempted: 25,080
Established: 25,060
Closed: 25,060
TCP Server Connection Rate
Established: 25,050
Closed: 25,050
Bandwidth
Tx (Mbps): 10,420
Rx (Mbps): 9,882
Application Transactions
Attempted: 5,522,906
Successful: 5,522,890
Failed: 0
Aborted: 0
Cumulative Client TCP Connections
Attempted: 5,522,881
Established: 5,522,866
Closed (FIN): 5,522,842
Close (RST): 0
Cumulative Server TCP Connections
Established: 5,522,881
Closed (FIN): 5,522,856
Close (RST): 0
Frame Rate
Tx (Fps): 1,425,000
Rx (Fps): 1,425,000
Concurrent Flows
Superflows: 25
TCP Flows: 25
UDP Flows: 0
SCTP Flows: 0
Average TCP Time
Client Connection Time: 0.129
Server Connection Time: 0.182
Close (ms): 0.094
Duration (ms): 0.843
Errors
Ethernet MAC Errors: N/A
Cumulative Frames
Tx: 314,361,551
Rx: 314,361,492
Info
Edit
Report
Stop Capture
Scripts
Go
Stop Test
Restart

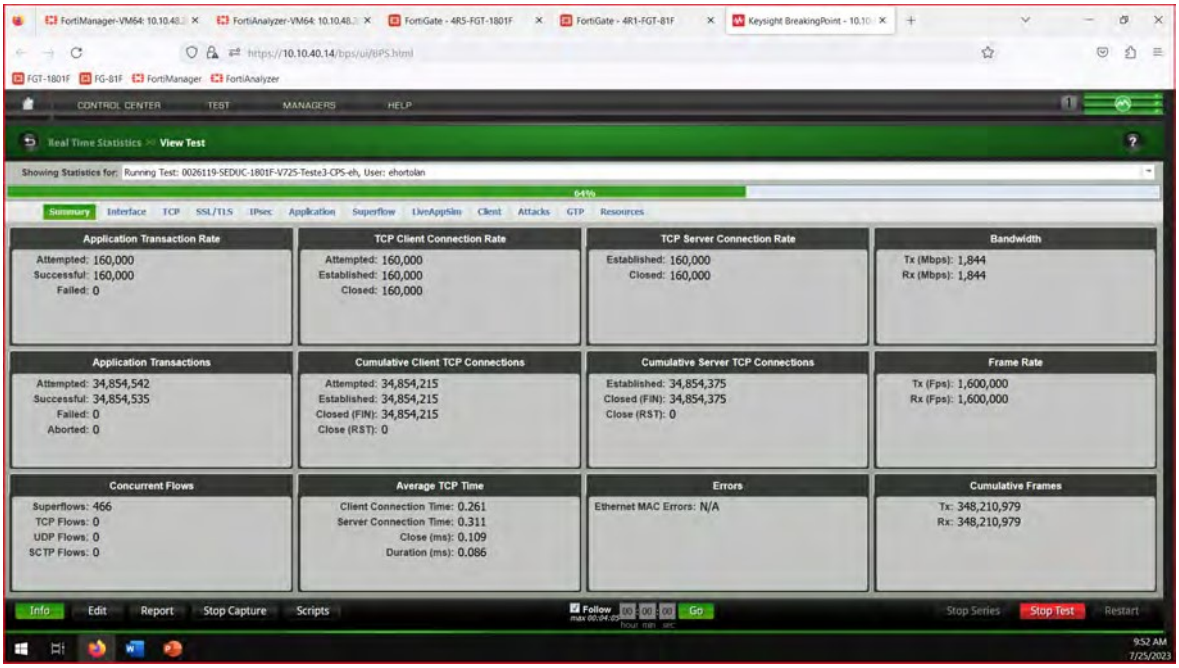

4RS-FGT-1801F
Favorites
PerfTest Dashboard
Firewall Policy
IPsec Tunnels
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
System
Security Fabric
Log & Report
VDOM: L3-Test
admin
CPU
Memory
Session Rate
Sessions
4%
31%
25,000/s
51,743
Bandwidth - port37
Bandwidth - port38
131.20 Mbps
9.33 Gbps
10.38 Gbps
241.27 Mbps

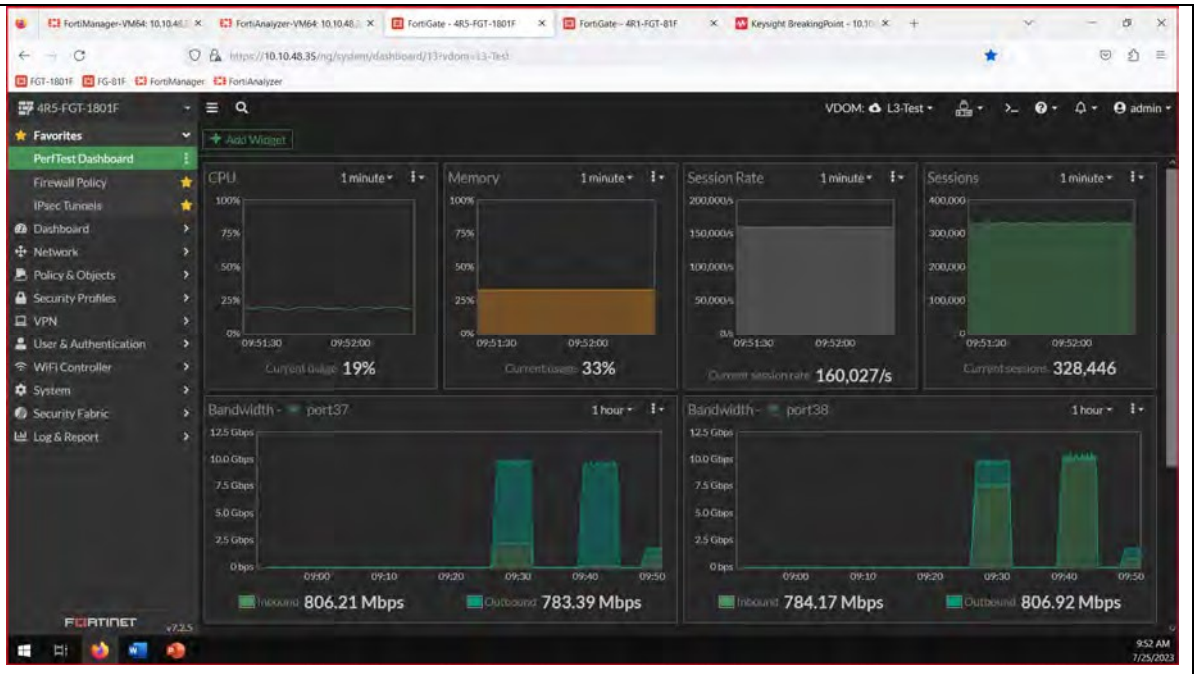

FortiManager-VM64: 10.10.48.2
FortiAnalyzer-VM64: 10.10.48.2
FortiGate - 4R5-FGT-1801F
FortiGate - 4R1-FGT-81F
Keysight BreakingPoint - 10.10
https://10.10.48.35/ng/vpn/ipsec?vdom=L3-Test
FGT-1801F
FG-81F
FortiManager
FortiAnalyzer
4R5-FGT-1801F
VDOM: L3-Test
admin
Favorites
PerfTest Dashboard
Firewall Policy
IPsec Tunnels
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
System
Security Fabric
Log & Report
View
Show Matching Logs
Search
Tunnel
Interface Binding
Status
Ref.
Custom
C2S
port38
dialup connection(s)
FORTINET
v7.2.5
Security Rating Issues
9:44 AM
7/25/2023

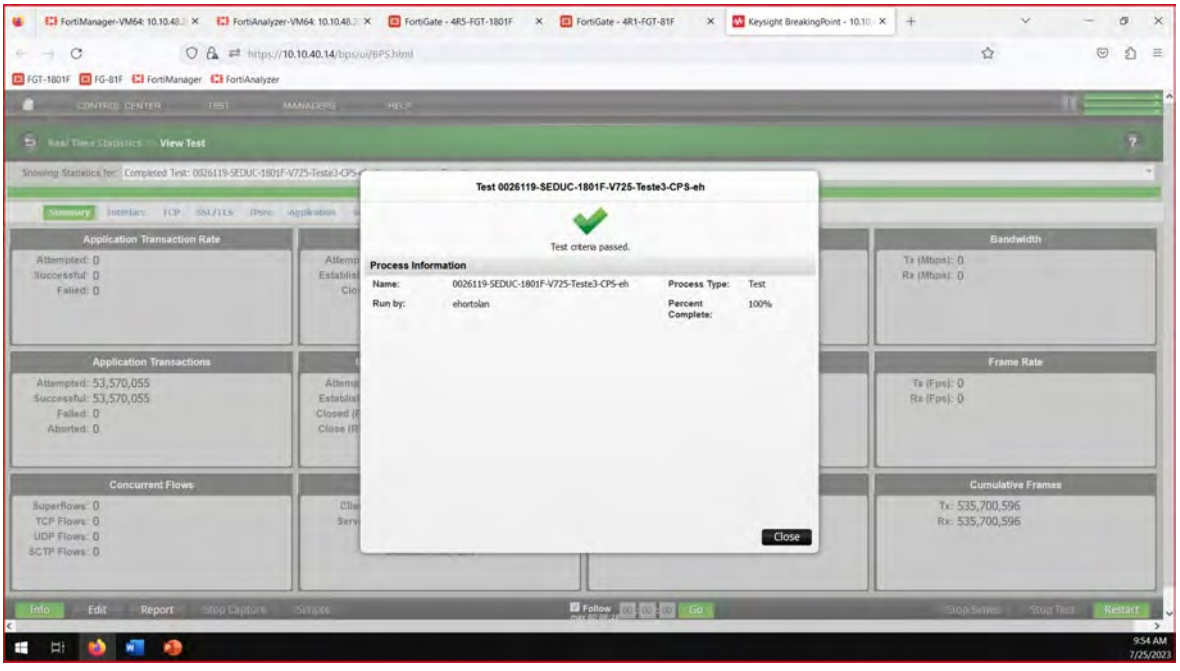

FortiManager-VM64: 10.10.48.2
FortiAnalyzer-VM64: 10.10.48.2
FortiGate - 4R5-FGT-1801F
FortiGate - 4R1-FGT-81F
Keysight BreakingPoint - 10.10
https://10.10.40.14/bps/ui/BPS.html
FGT-1801F
FG-81F
FortiManager
FortiAnalyzer
CONTROL CENTER
TEST
MANAGERS
HELP
Real Time Statistics
View Test
Test 0026119-SEDUC-1801F-V725-Teste2-IPSEC-eh
Test criteria passed.
Process Information
Name:
0026119-SEDUC-1801F-V725-Teste2-IPSEC-eh
Process Type:
Test
Run by:
ehortolan
Percent Complete:
100%
Close
Application Transaction Rate
Attempted: 0
Successful: 0
Failed: 0
Bandwidth
Tx (Mbps): 0.00234
Rx (Mbps): 0.00234
Application Transactions
Attempted: 8,347,431
Successful: 8,347,431
Failed: 0
Aborted: 0
Frame Rate
Tx (Fps): 2
Rx (Fps): 2
Concurrent Flows
Superflows: 0
TCP Flows: 0
UDP Flows: 0
SCTP Flows: 0
Cumulative Frames
Tx: 475,805,618
Rx: 475,805,547
Info
Edit
Report
Stop Capture
Scripts
Follow
Go
Stop Series
Stop Test
Restart
9:45 AM
7/25/2023

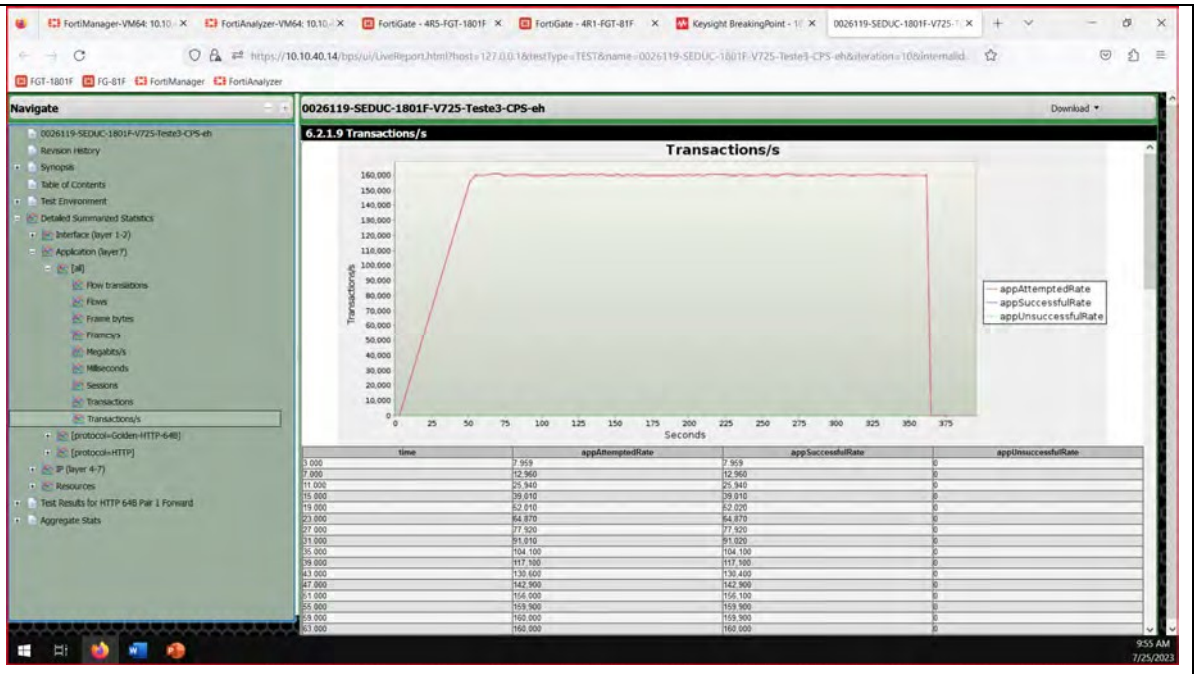
	  **TESTE OK**
Comentário	

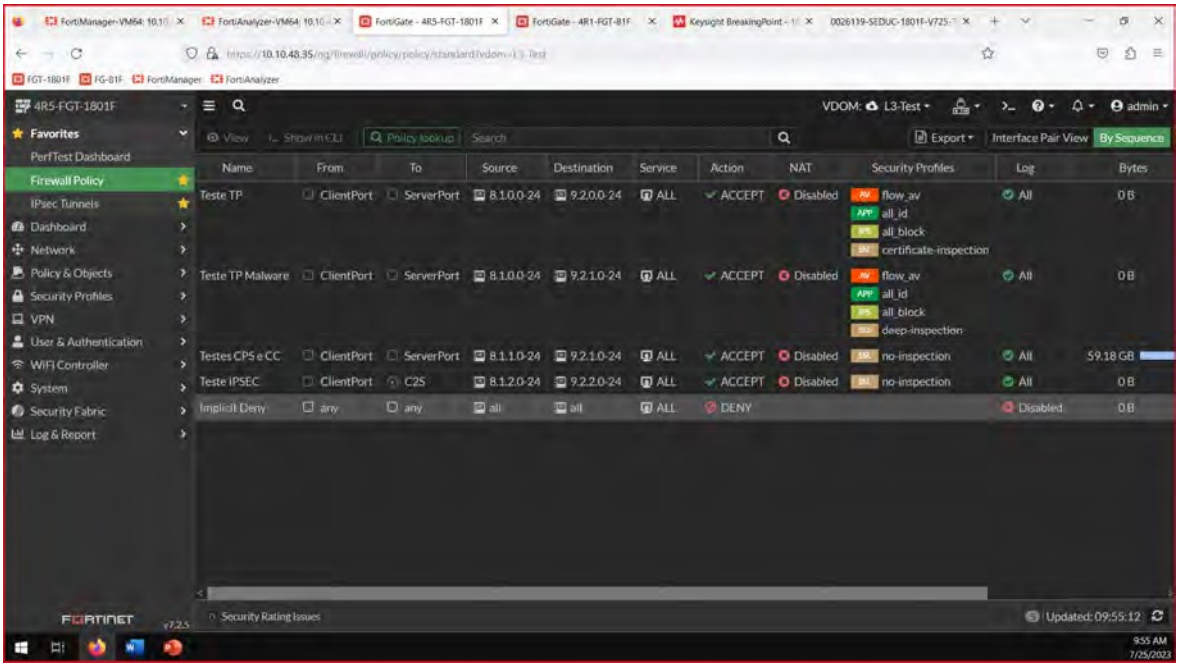
5.1.6 CONEXÕES

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


4R5-FGT-1801F
Favorites
PerfTest Dashboard
Firewall Policy
IPsec Tunnels
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
System
Security Fabric
Log & Report
CPU
1 minute
19%
Memory
33%
Session Rate
160,027/s
Sessions
328,446
Bandwidth - port37
806.21 Mbps
783.39 Mbps
Bandwidth - port38
784.17 Mbps
806.92 Mbps

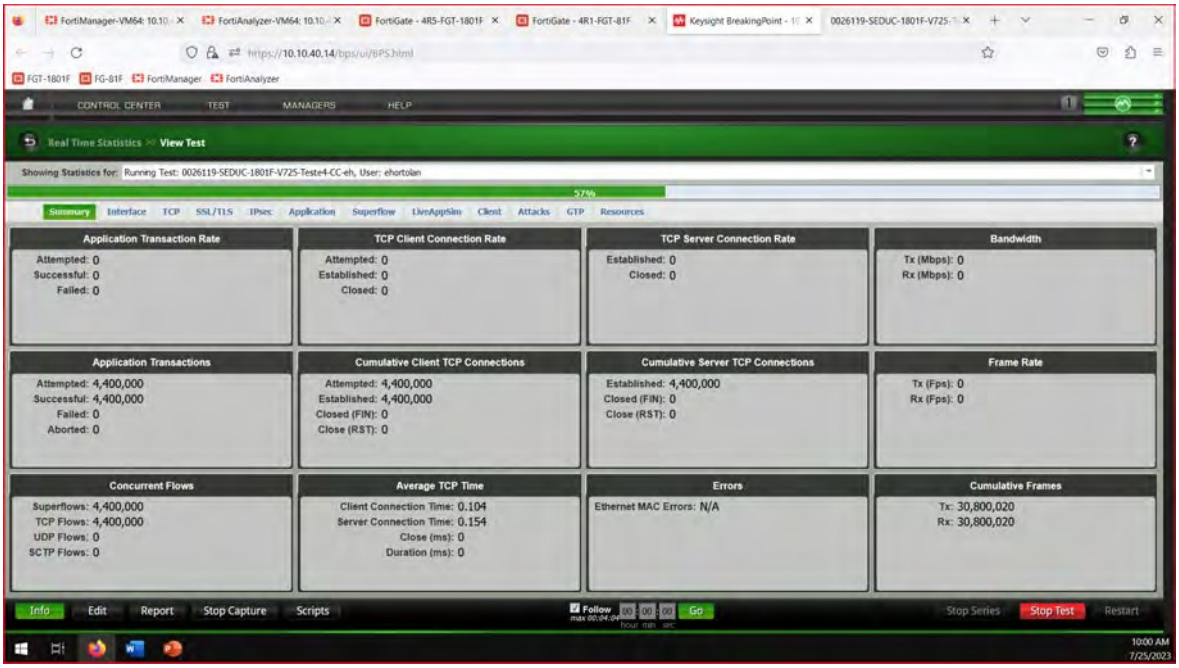

Test 0026119-SEDUC-1801F-V725-Teste3-CPS-eh
Test criteria passed.
Process Information
Name: 0026119-SEDUC-1801F-V725-Teste3-CPS-eh
Process Type: Test
Run by: ehortolan
Percent Complete: 100%
Close
Application Transaction Rate
Application Transactions
Attempted: 53,570,055
Successful: 53,570,055
Bandwidth
Frame Rate
Concurrent Flows
Cumulative Frames
Tx: 535,700,596
Rx: 535,700,596

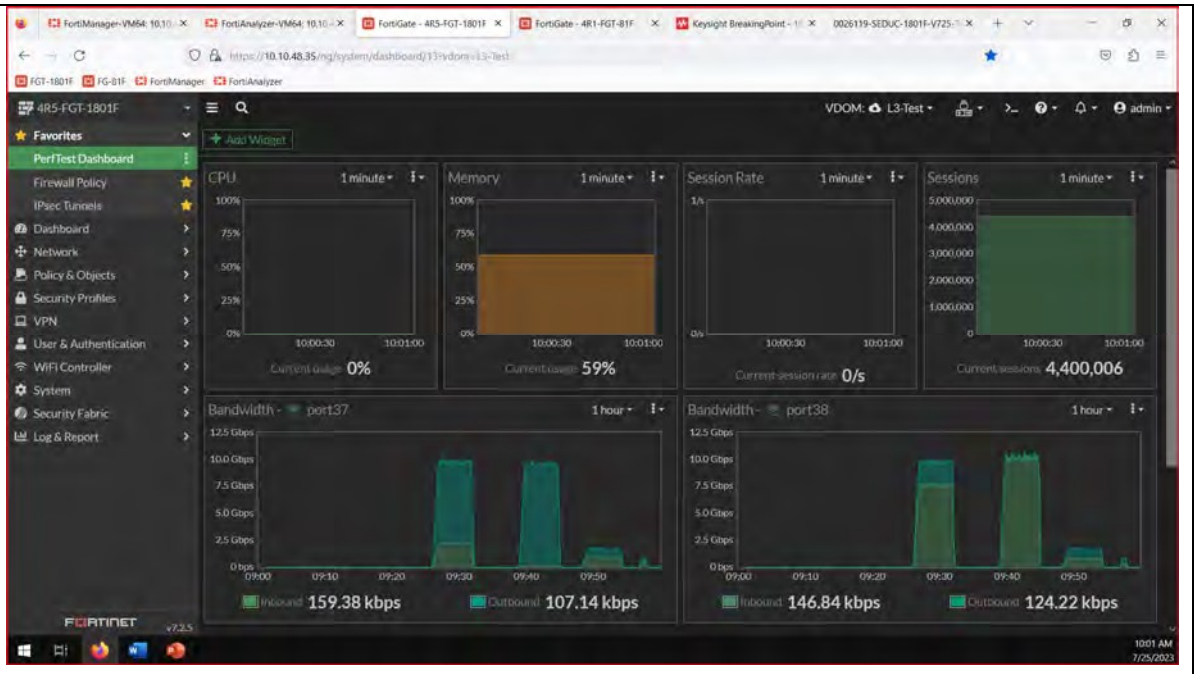


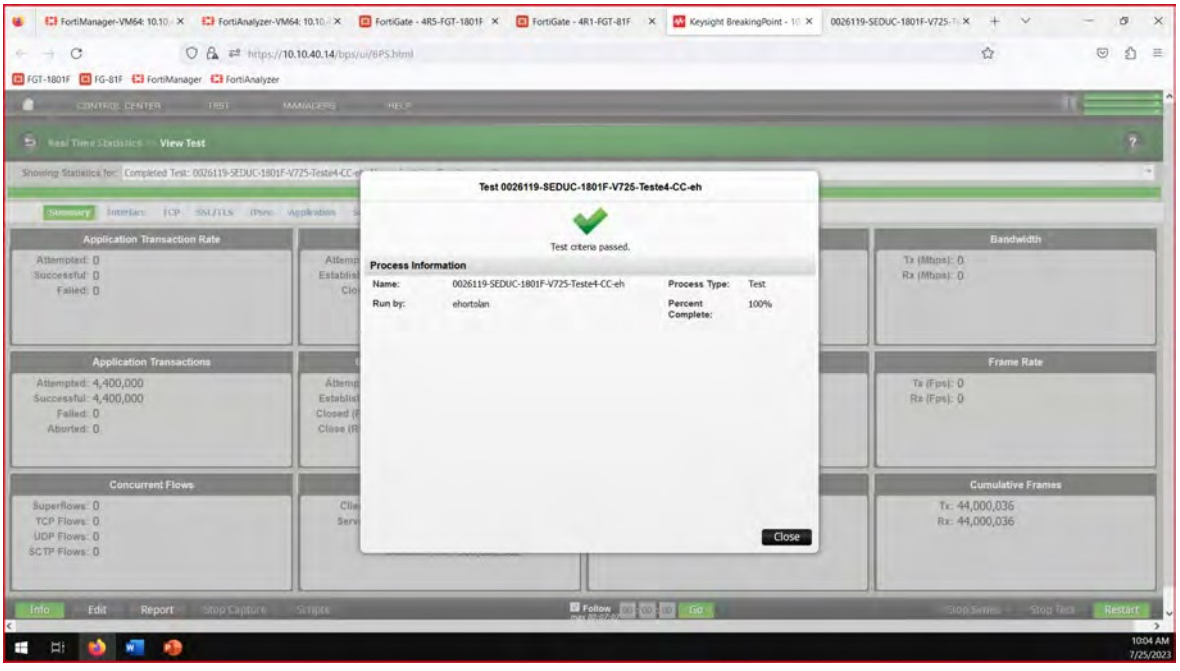


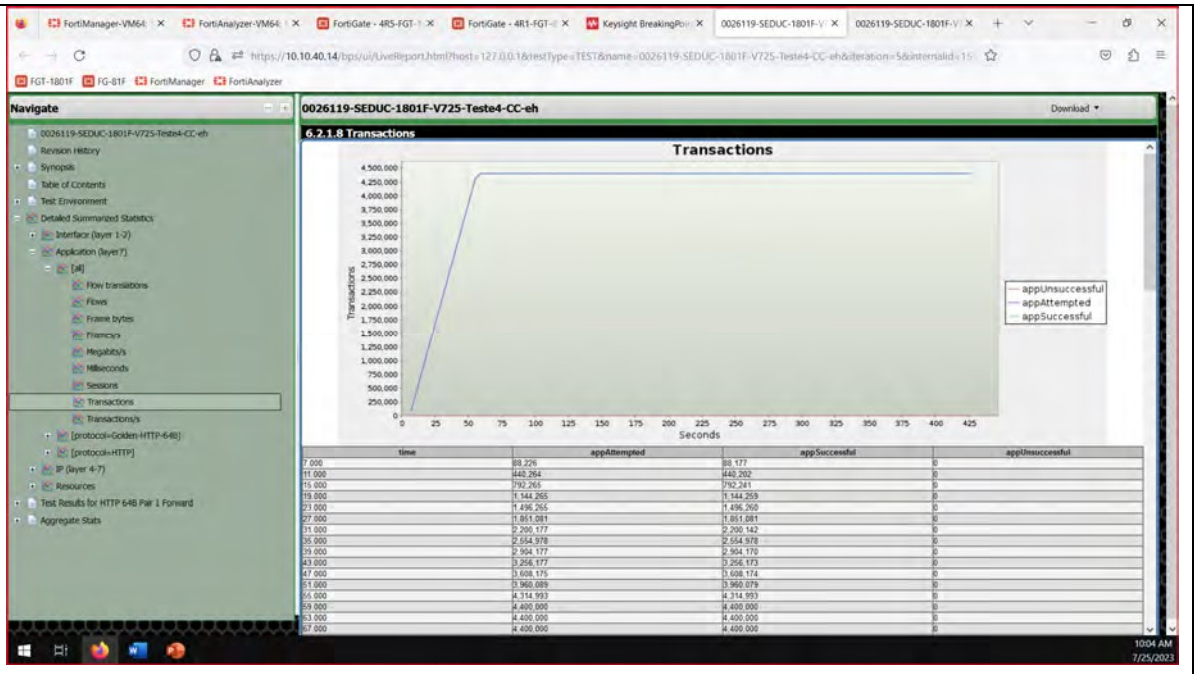
TESTE OK

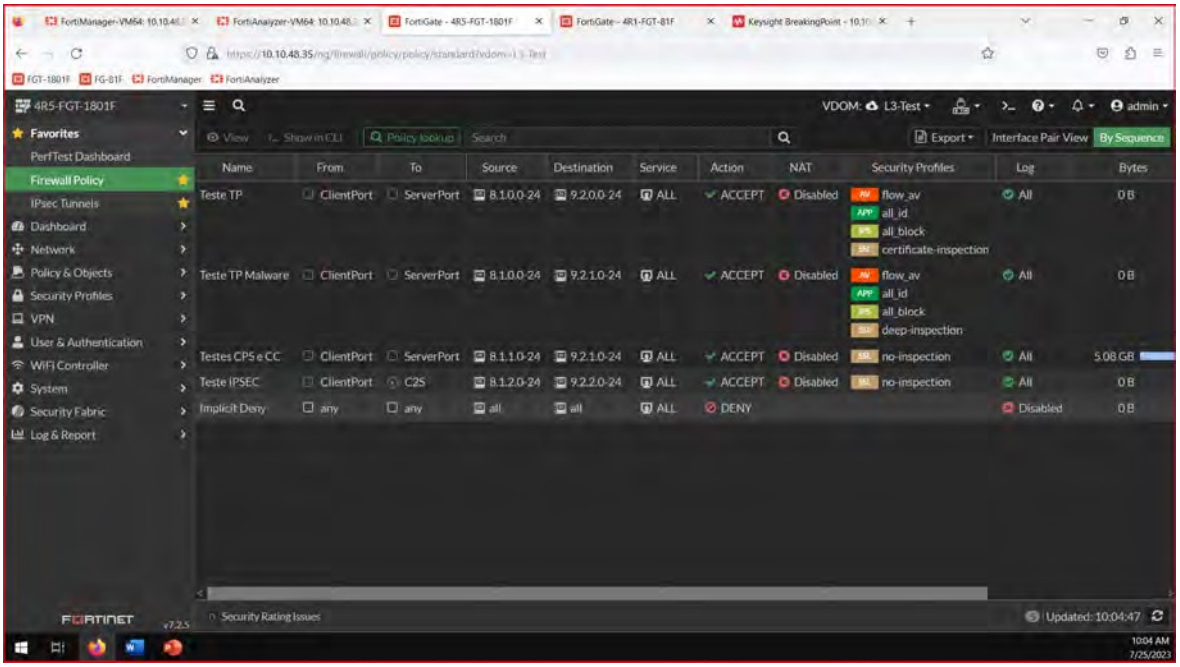
Comentário	

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. 


4R5-FGT-1801F
Favorites
PerfTest Dashboard
Firewall Policy
IPsec Tunnels
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
System
Security Fabric
Log & Report
VDOM: L3-Test
admin
Add Widget
CPU
1 minute
0%
Memory
59%
Session Rate
0/s
Sessions
4,400,006
Bandwidth - port37
1 hour
Inbound 159.38 kbps
Outbound 107.14 kbps
Bandwidth - port38
Inbound 146.84 kbps
Outbound 124.22 kbps
FORTINET
v7.2.5
10:01 AM
7/25/2023


Test 0026119-SEDUC-1801F-V725-Teste4-CC-eh
Test criteria passed.
Process Information
Name: 0026119-SEDUC-1801F-V725-Teste4-CC-eh
Process Type: Test
Run by: ehortolan
Percent Complete: 100%
Close
Application Transaction Rate
Application Transactions
Attempted: 4,400,000
Successful: 4,400,000
Failed: 0
Aborted: 0
Bandwidth
Frame Rate
Concurrent Flows
Cumulative Frames
Tx: 44,000,036
Rx: 44,000,036
Info
Edit
Report
Restart
10:04 AM
7/25/2023

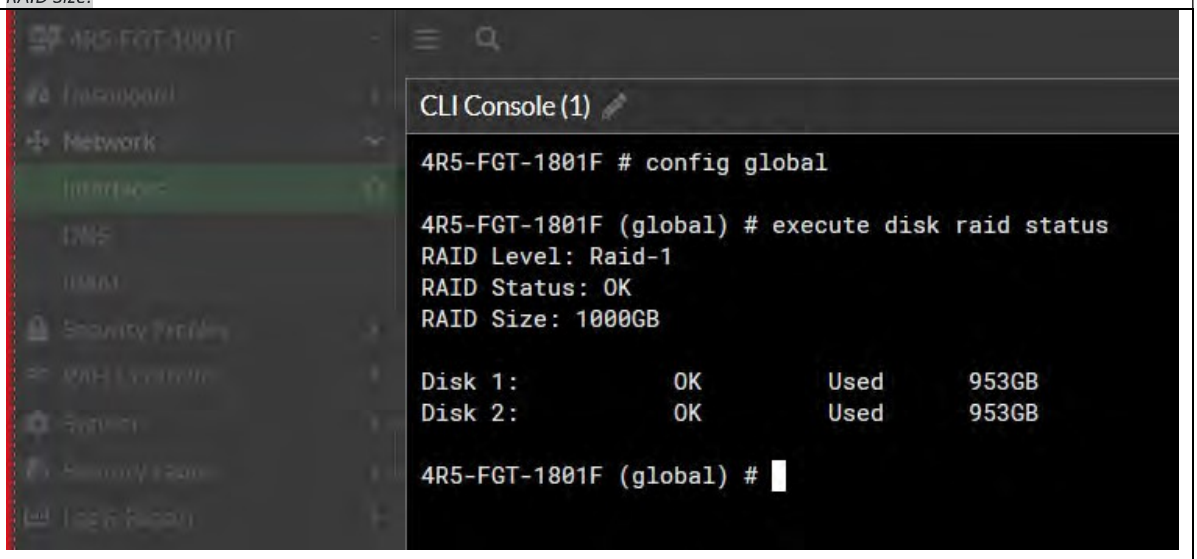


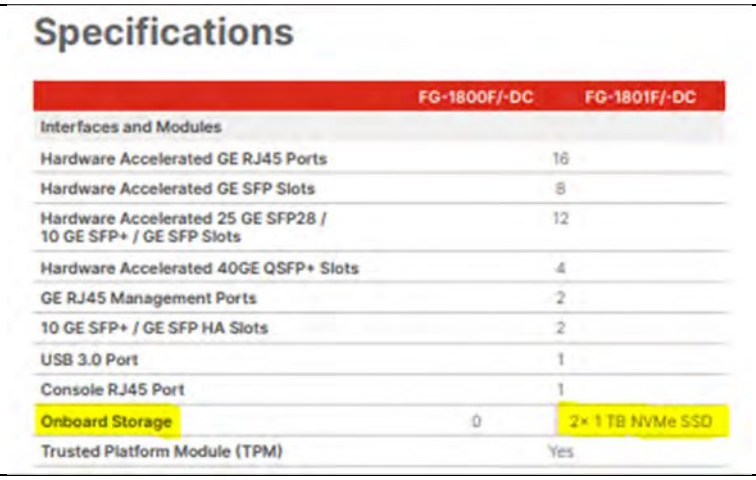


TESTE OK

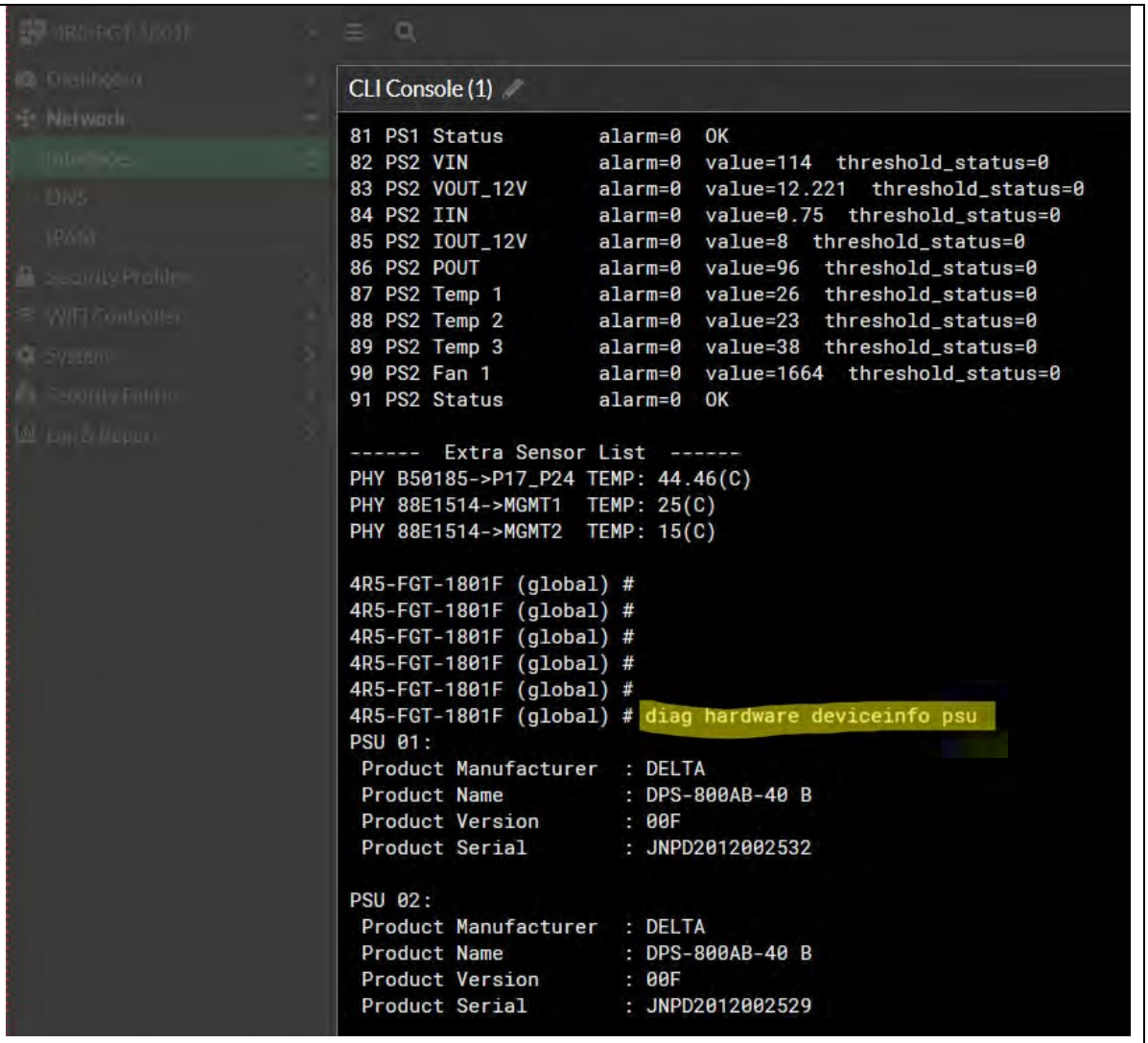
Comentário	

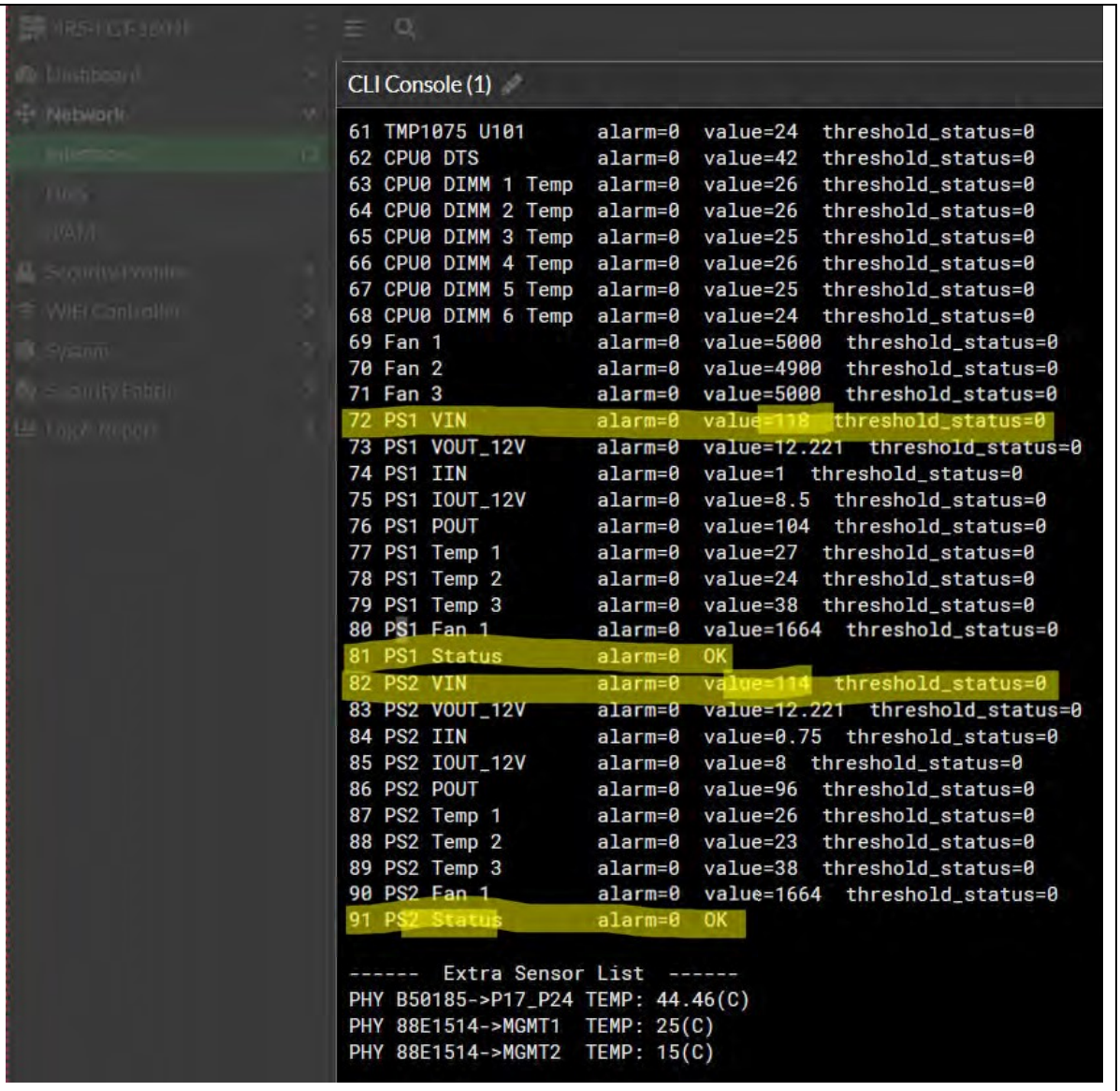
5.1.7 HARDWARE:

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

	
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	


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 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)
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

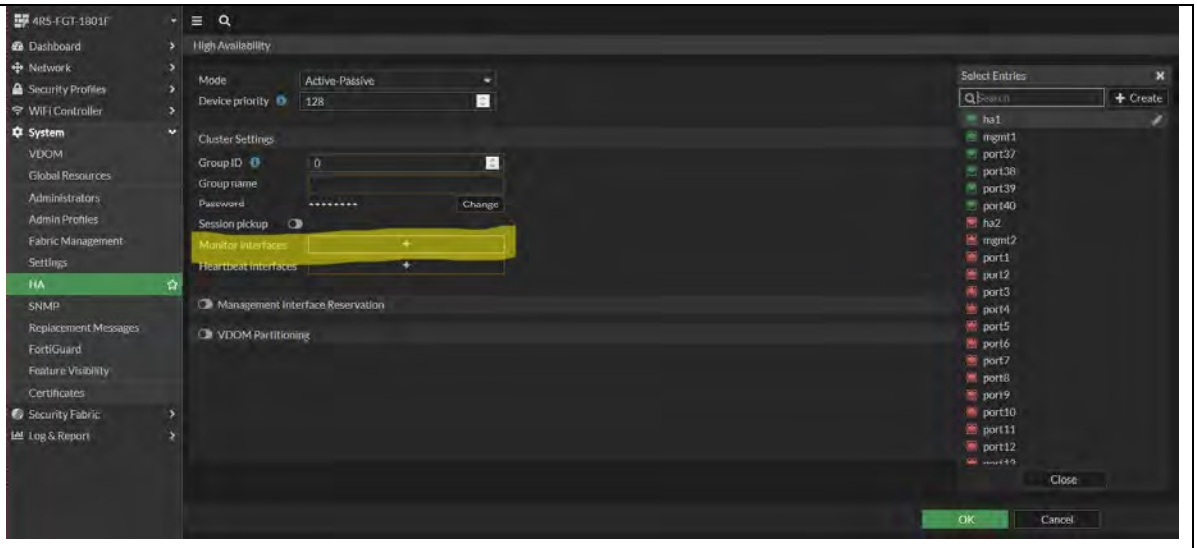

CLI Console (1)
61 TMP1075 U101 alarm=0 value=24 threshold_status=0
62 CPU0 DTS alarm=0 value=42 threshold_status=0
63 CPU0 DIMM 1 Temp alarm=0 value=26 threshold_status=0
64 CPU0 DIMM 2 Temp alarm=0 value=26 threshold_status=0
65 CPU0 DIMM 3 Temp alarm=0 value=25 threshold_status=0
66 CPU0 DIMM 4 Temp 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=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 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

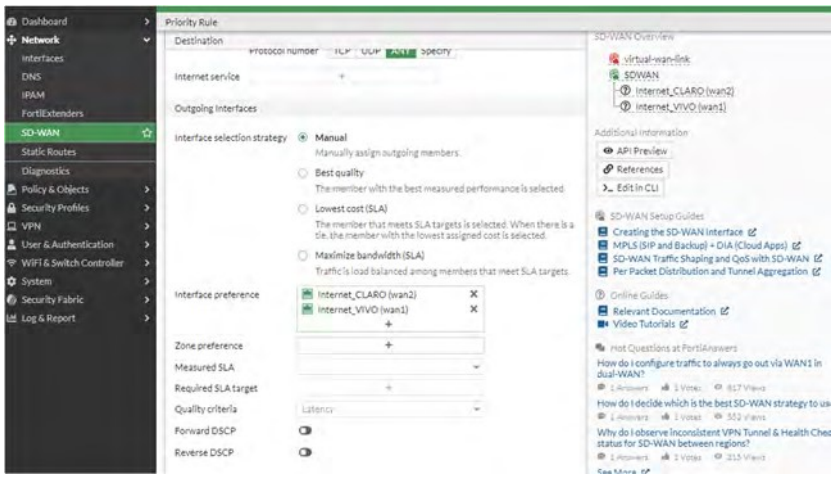
	
Comentário	FortiGate https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1800f-series.pdf

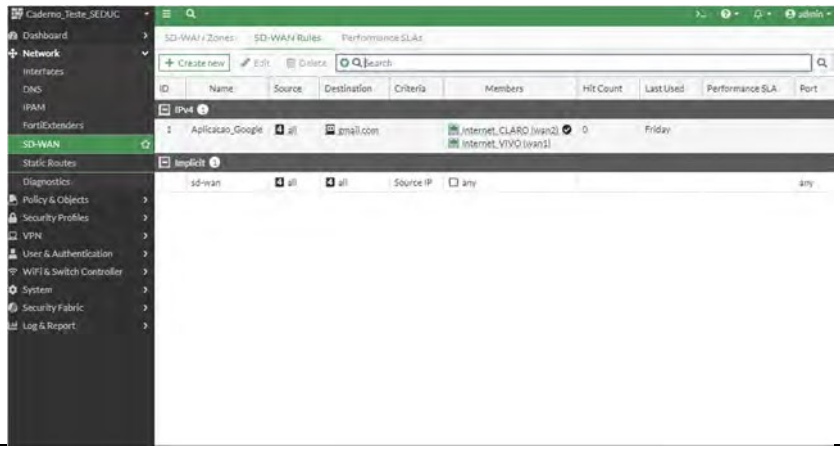
5.1.8 ALTA DISPONIBILIDADE E BALANCEAMENTO DE CARGA:

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	



TESTE OK

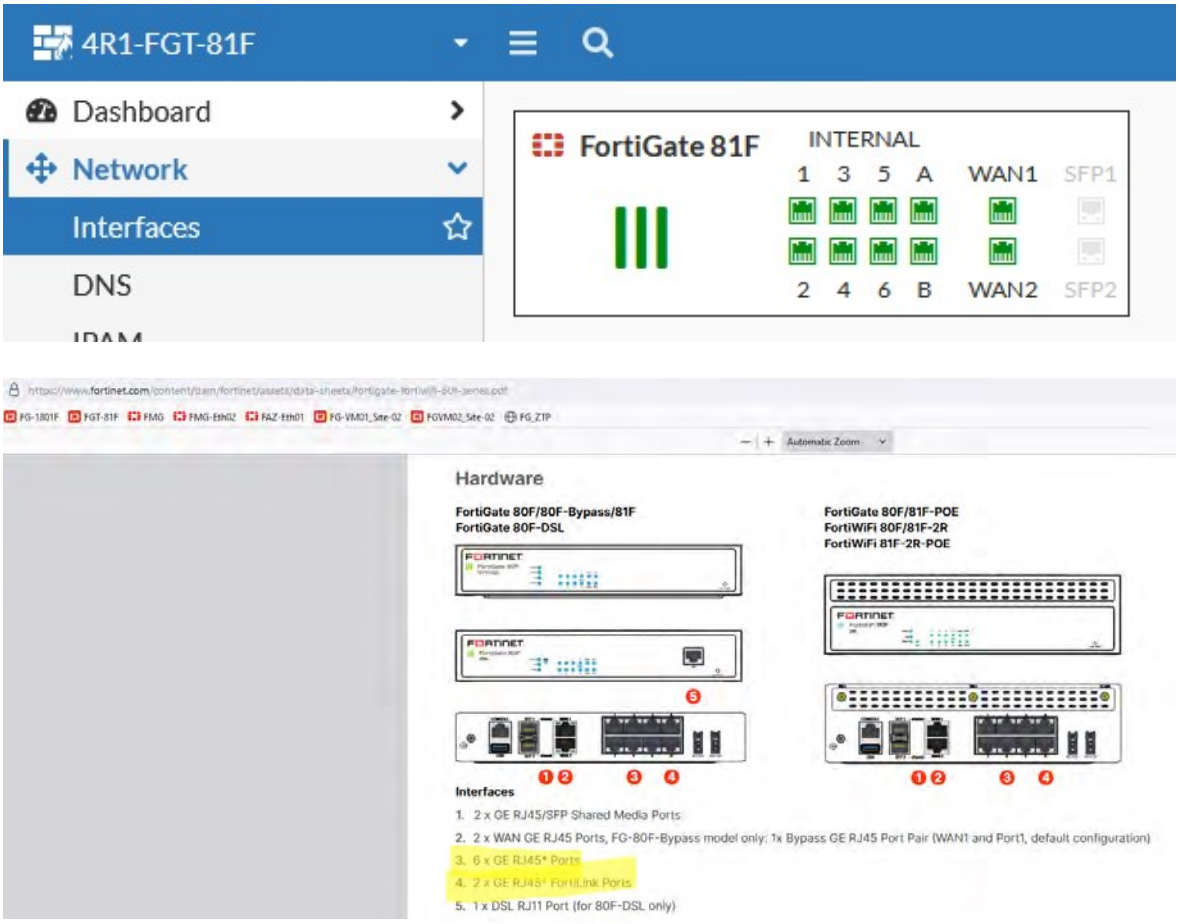


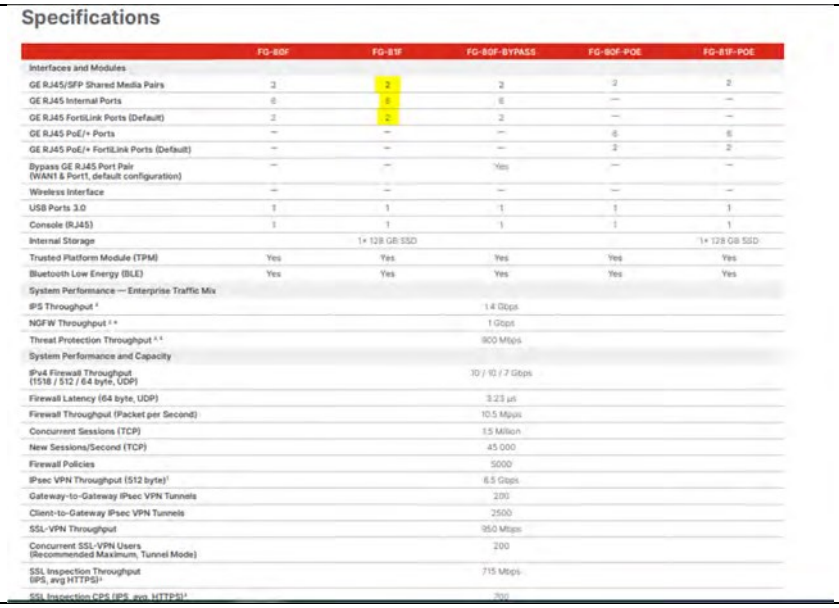


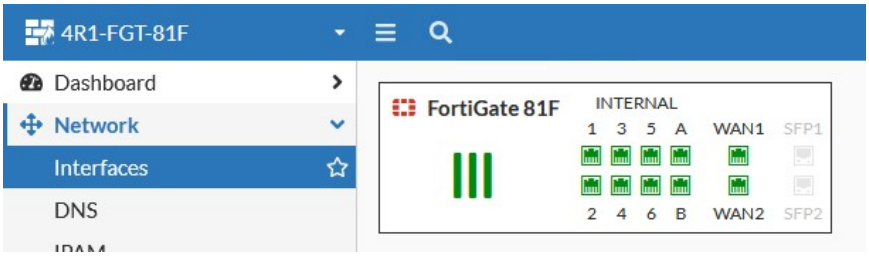
Comentário	

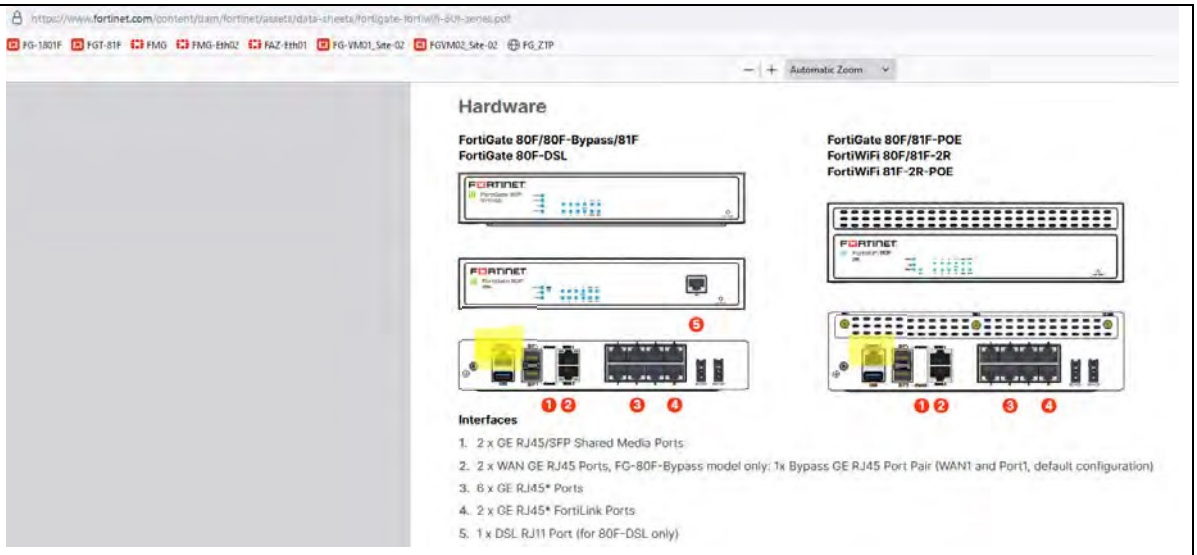
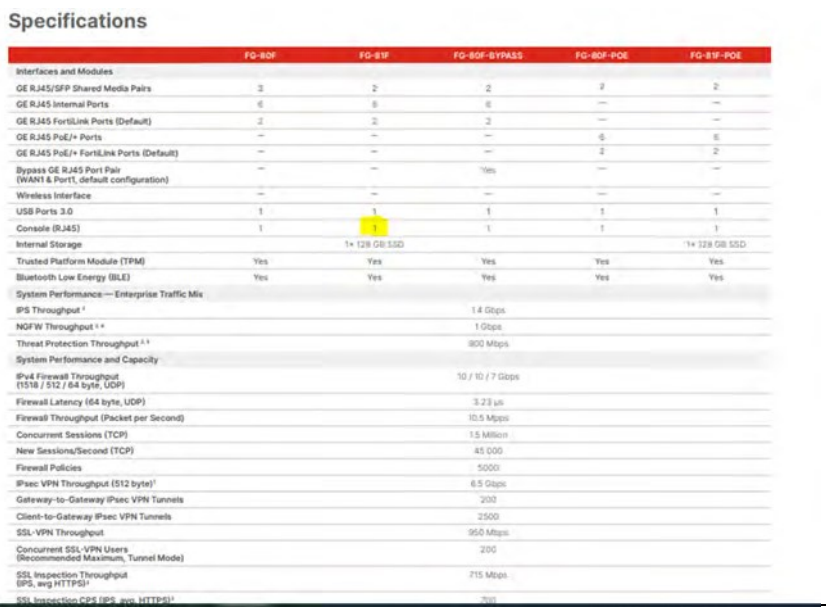
5.2 Solução de Segurança Tipo 2

5.2.2 INTERFACES

Item de Teste - 5.2.2.1	Possuir no mínimo 08 (oito) interfaces Gigabit RJ45;
Objetivo do Teste	Validar se o equipamento possui no mínimo 8 interfaces Gigabit RJ45
Configuração do Teste	Inspeção visual
Procedimento do Teste	Comprovação visual e por meio do datasheet
Evidências	 **TESTE OK**

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

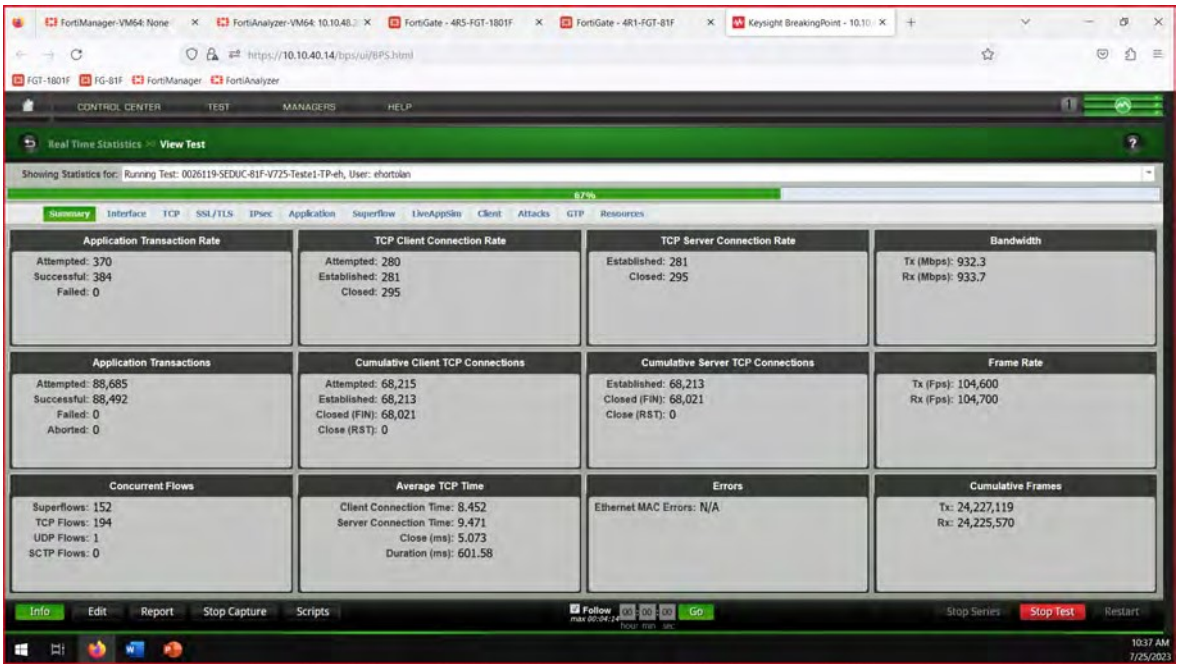
Item de Teste - 5.2.2.2	Possuir no mínimo 01 (uma) interface console;
Objetivo do Teste	Validar se o equipamento FortiGate 81F possui pelo menos 1 interface console
Configuração do Teste	Validar que o equipamento possui 01 interfaces de console
Procedimento do Teste	Comprovação visual e por meio do datasheet
Evidências	

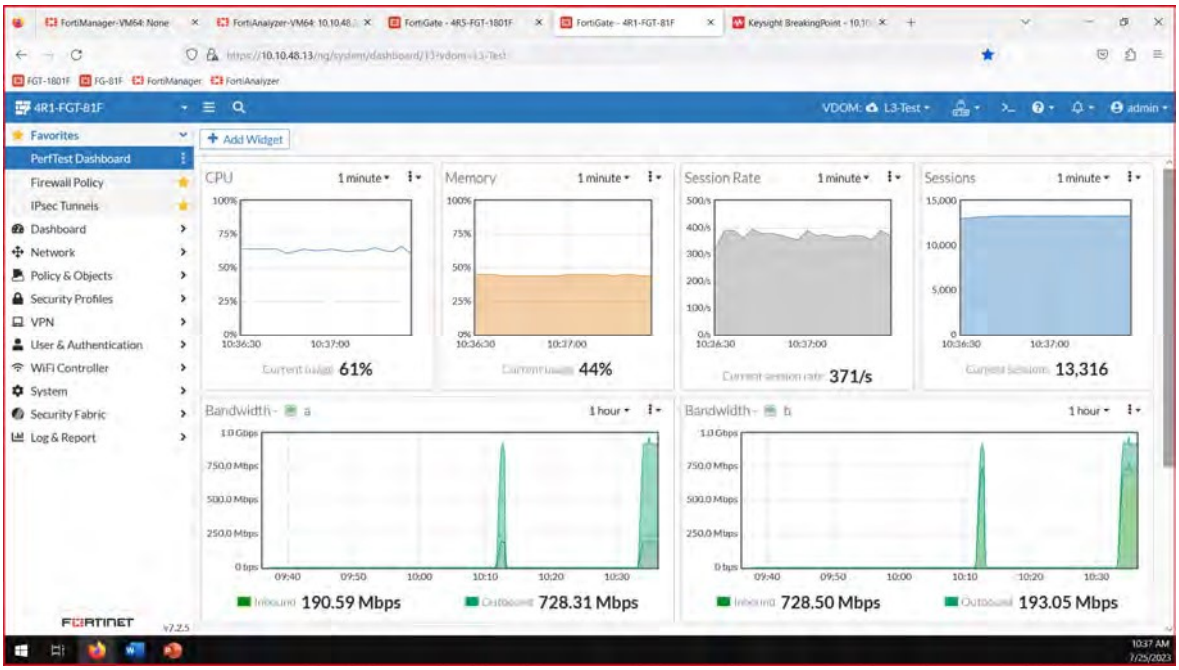
	 **TESTE OK** 
Comentário	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-80f-series.pdf

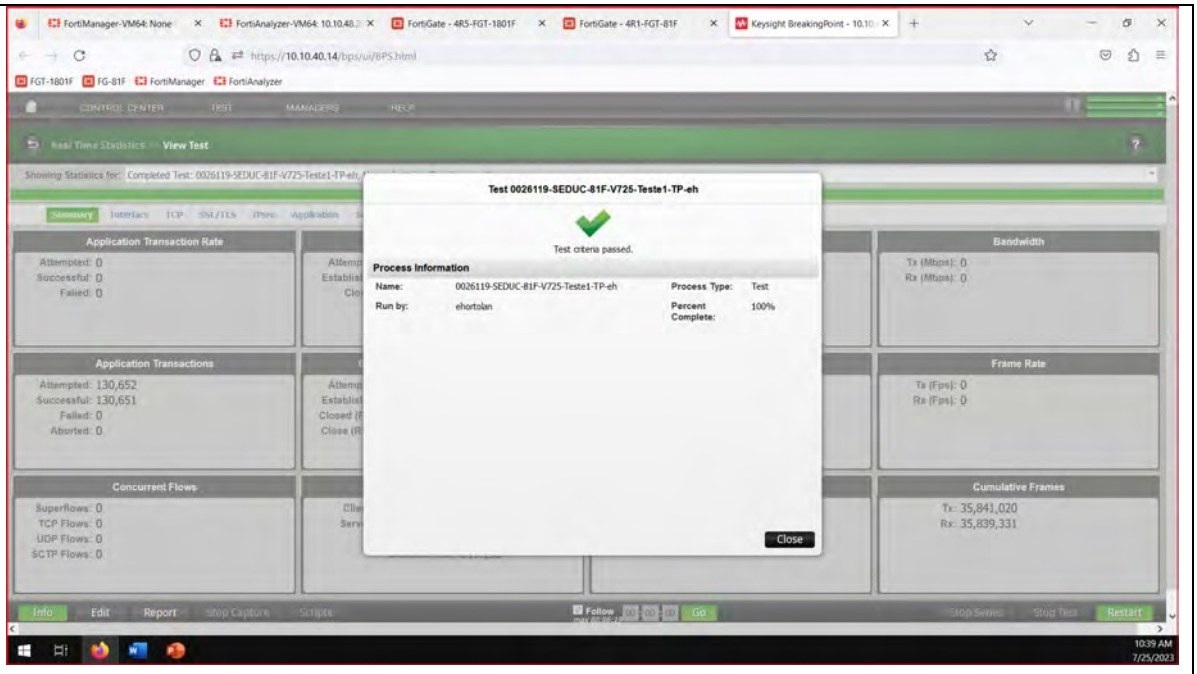
5.2.3 TROUGHPUT

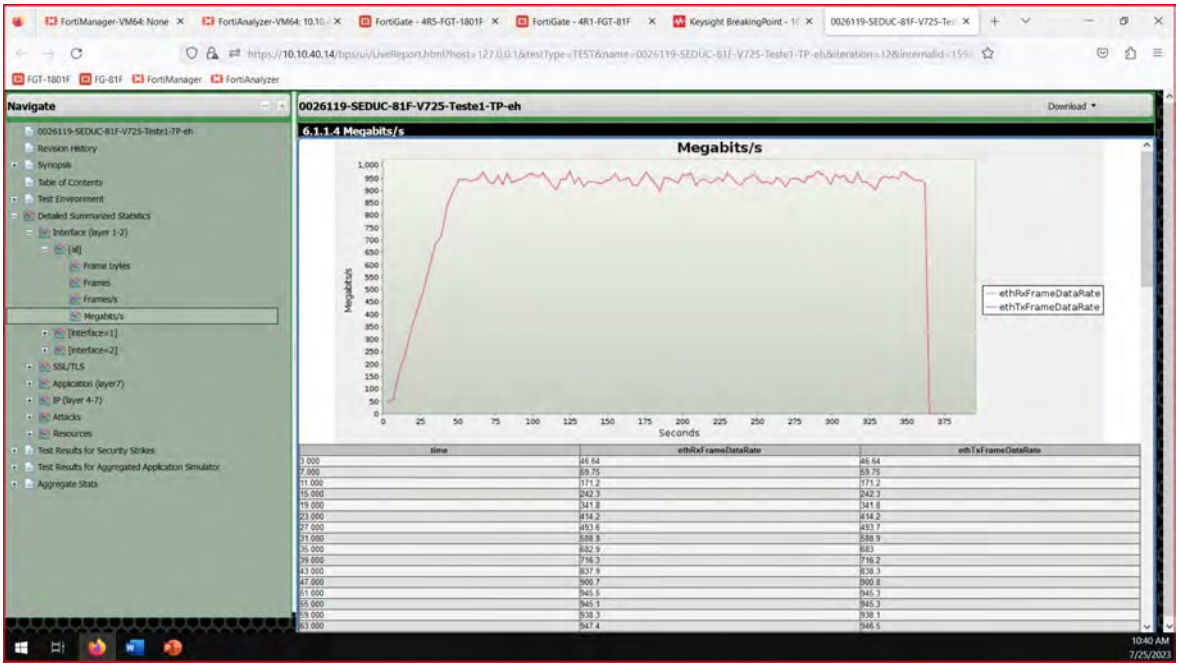
Item de Teste - 5.2.3.1	Possuir no mínimo 900 (novecentos) Mbps de tráfego real com as funcionalidades de segurança habilitadas (Firewall, IPS, Logging, Controle de Aplicação, Proteção contra Malware);
Objetivo do Teste	Validar o throughput de no mínimo 900 Mbps de tráfego real com as funcionalidades de Firewall, IPS, Logging, controle de aplicação e proteção contra Malwares.
Configuração do Teste	Teste a ser realizado no laboratório Fortinet.

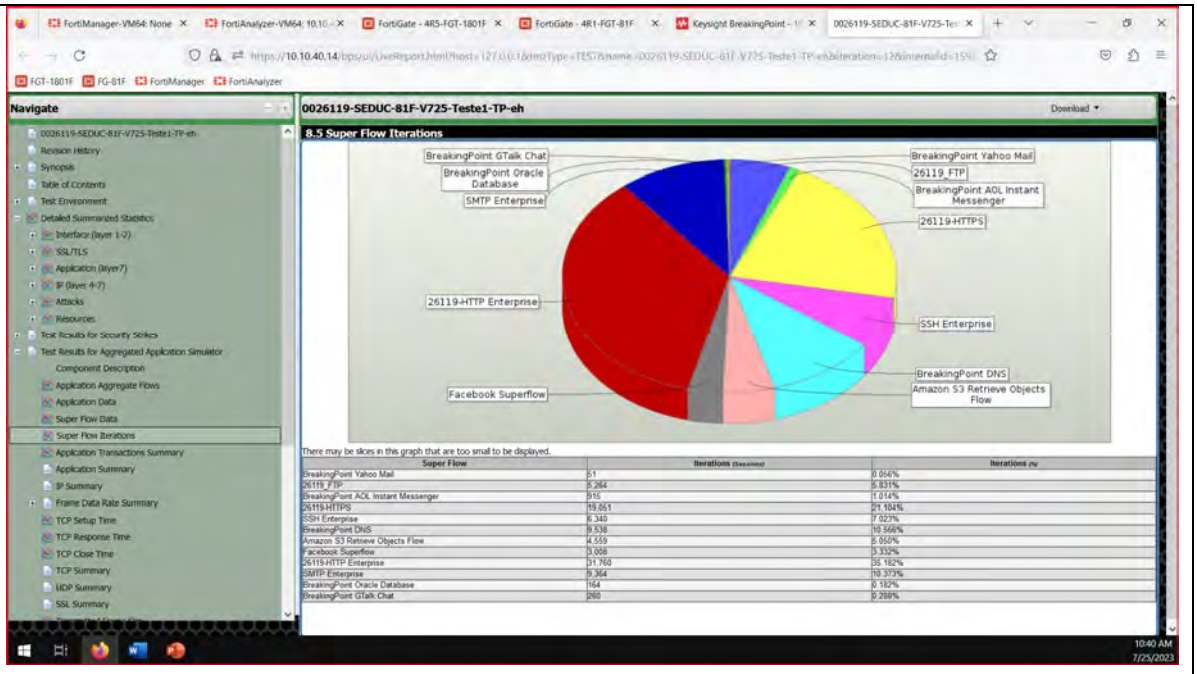
	Será apresentado o perfil de tráfego que será gerado e submetido ao appliance em teste.
Procedimento do Teste	Submeter o equipamento ao tráfego de 900 Mbps com as funcionalidades supracitadas inspecionando este tráfego.

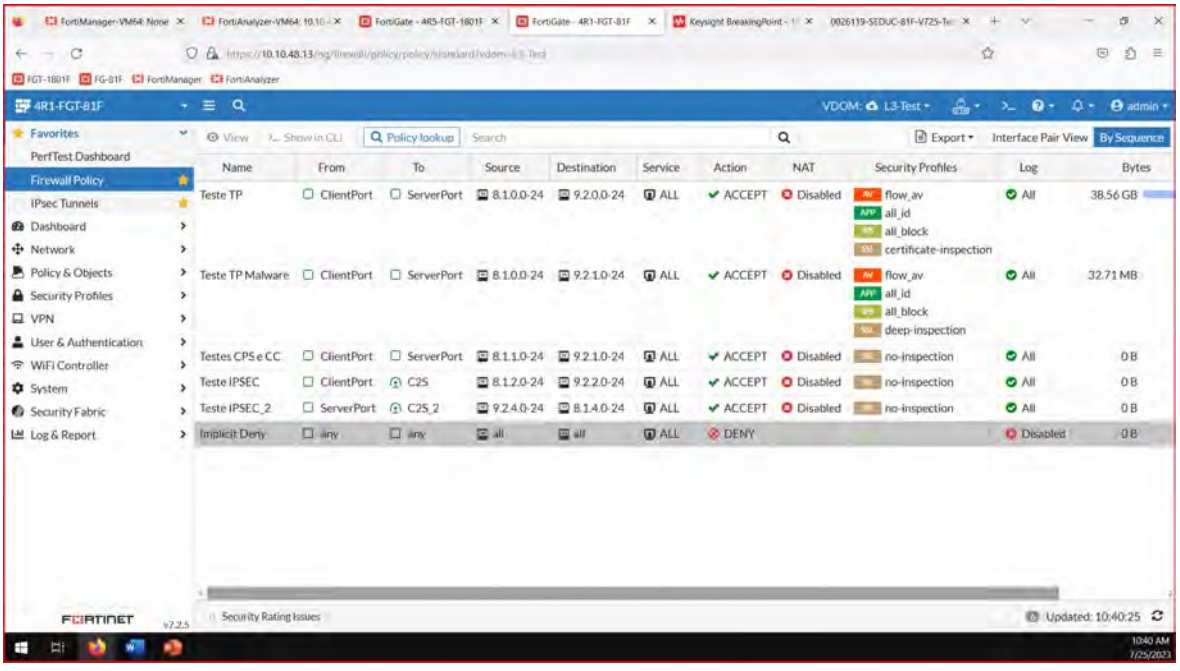


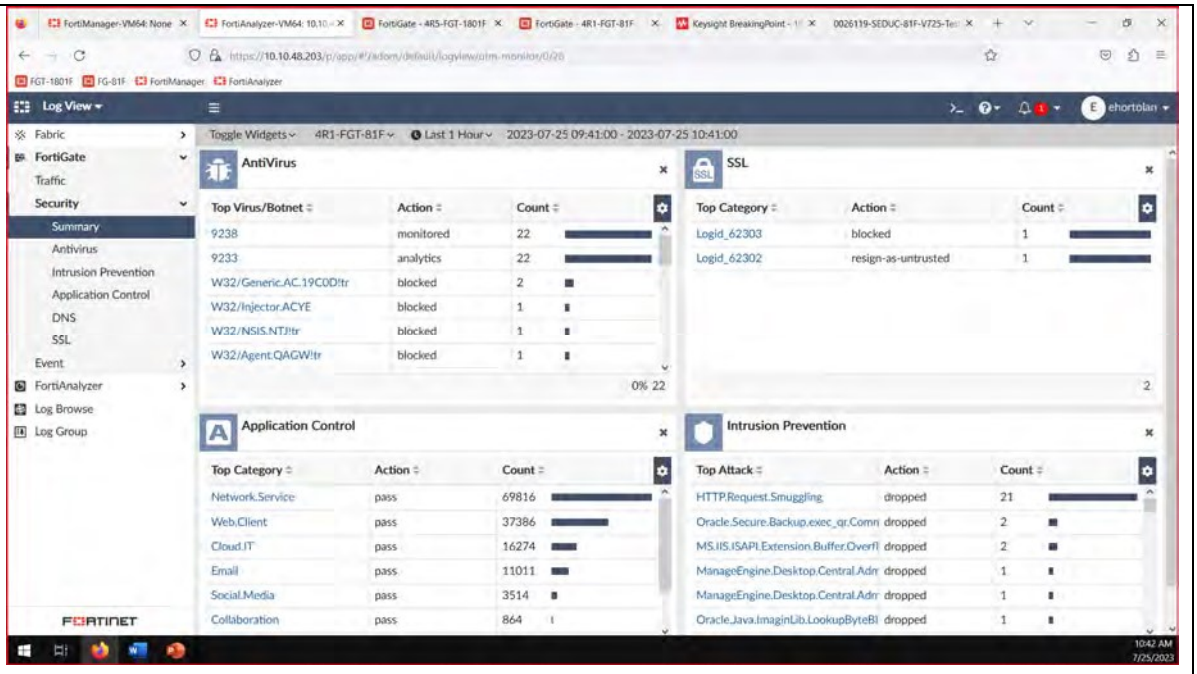


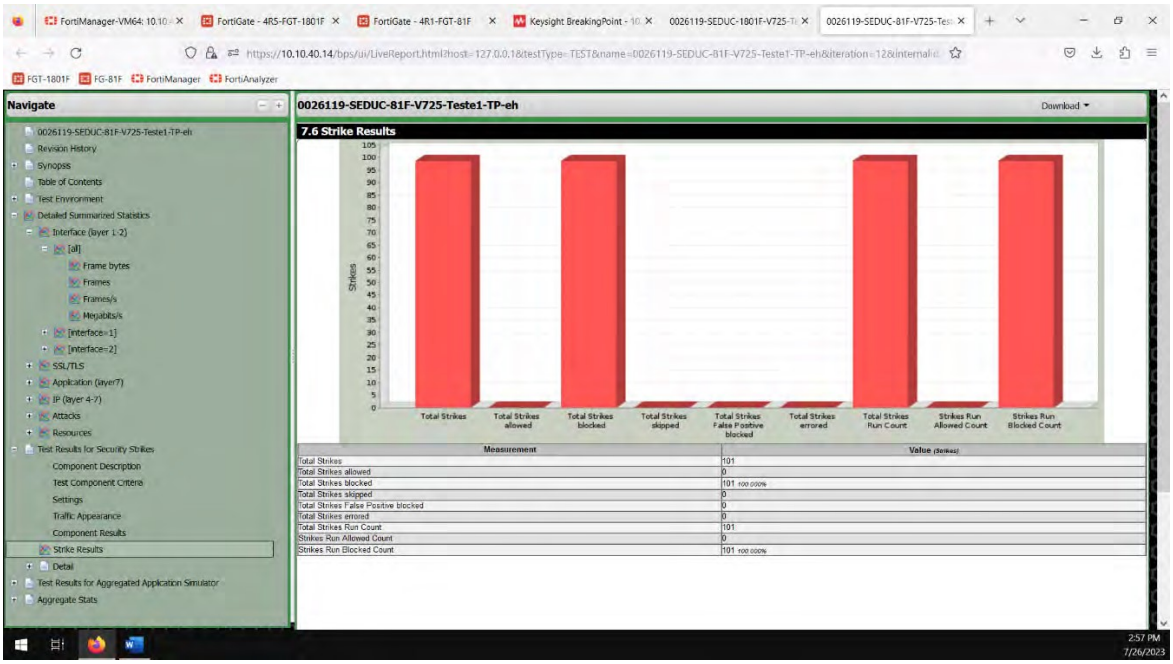

Test 0026119-SEDUC-81F-V725-Teste1-TP-eh
Test criteria passed.
Process Information
Name: 0026119-SEDUC-81F-V725-Teste1-TP-eh
Process Type: Test
Run by: ehortolan
Percent Complete: 100%
Close
Application Transaction Rate
Application Transactions
Attempted: 130,652
Successful: 130,651
Failed: 0
Aborted: 0
Concurrent Flows
Bandwidth
Frame Rate
Cumulative Frames
Tx: 35,841,020
Rx: 35,839,331


Navigate
0026119-SEDUC-81F-V725-Teste1-TP-eh
6.1.1.4 Megabits/s
Megabits/s
Seconds
ethRxFrameDataRate
ethTxFrameDataRate


Navigate
0026119-SEDUC-81F-V725-Teste1-TP-eh
8.5 Super Flow Iterations
BreakingPoint GTalk Chat
BreakingPoint Oracle Database
SMTP Enterprise
BreakingPoint Yahoo Mail
26119_FTP
BreakingPoint AOL Instant Messenger
26119-HTTPS
26119-HTTP Enterprise
SSH Enterprise
BreakingPoint DNS
Amazon S3 Retrieve Objects Flow
Facebook Superflow

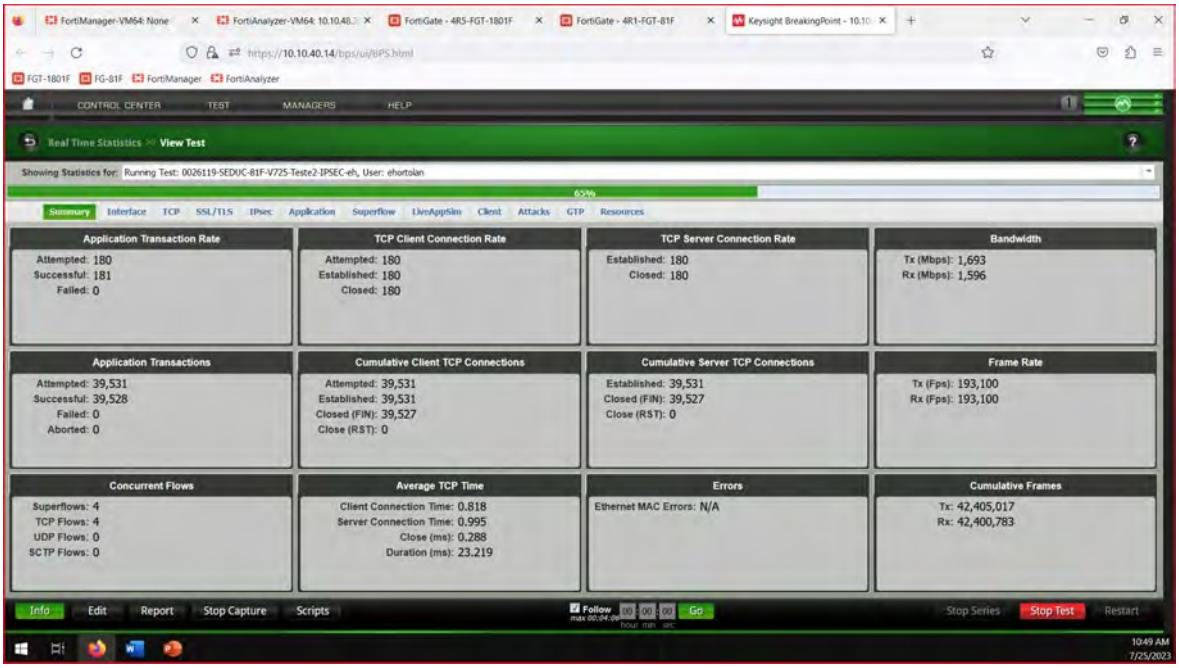

4R1-FGT-81F
Favorites
PerfTest Dashboard
Firewall Policy
IPsec Tunnels
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
System
Security Fabric
Log & Report
Teste TP
Teste TP Malware
Testes CPS e CC
Teste IPSEC
Teste IPSEC_2
Implicit Deny

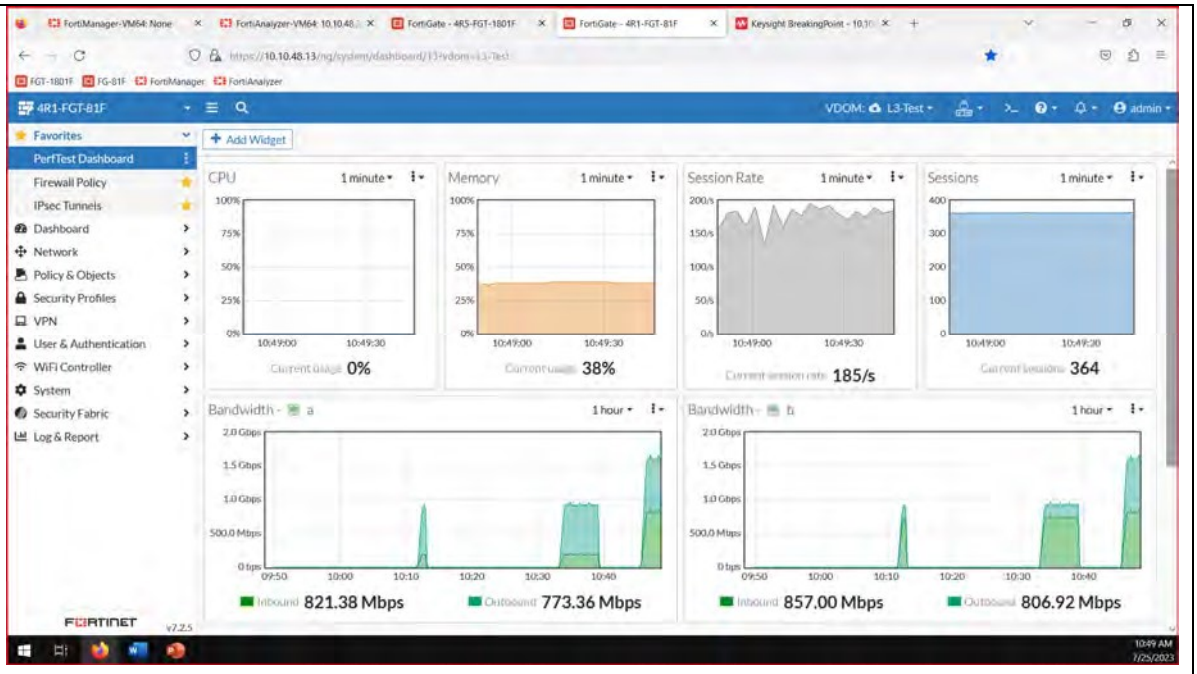


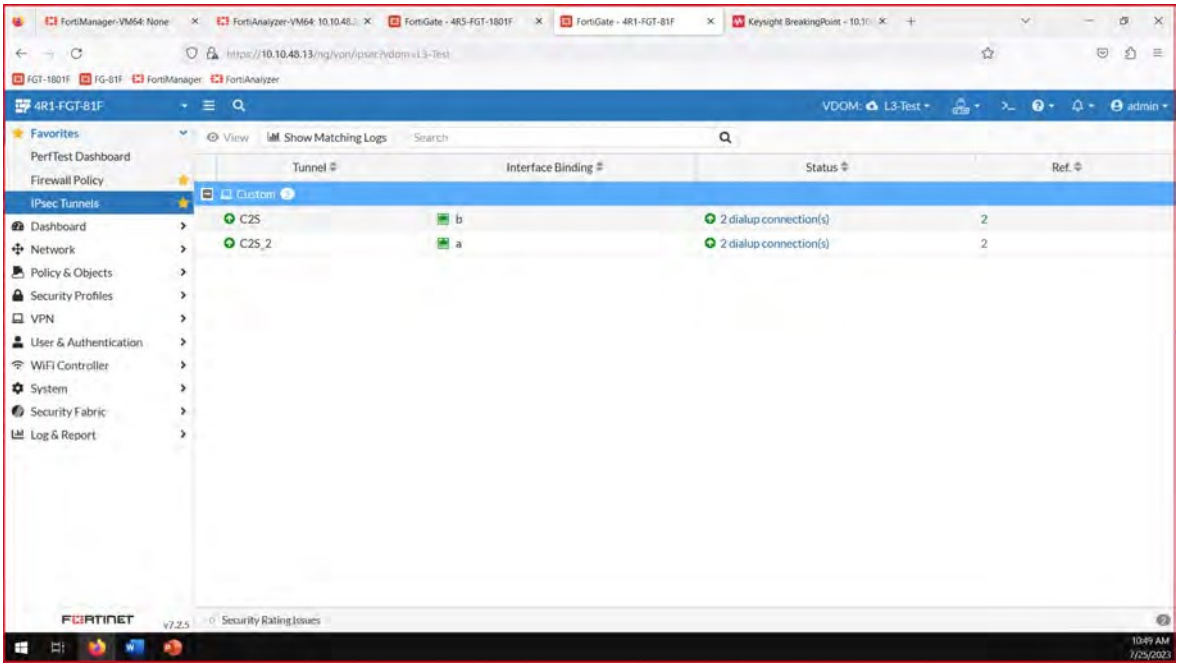


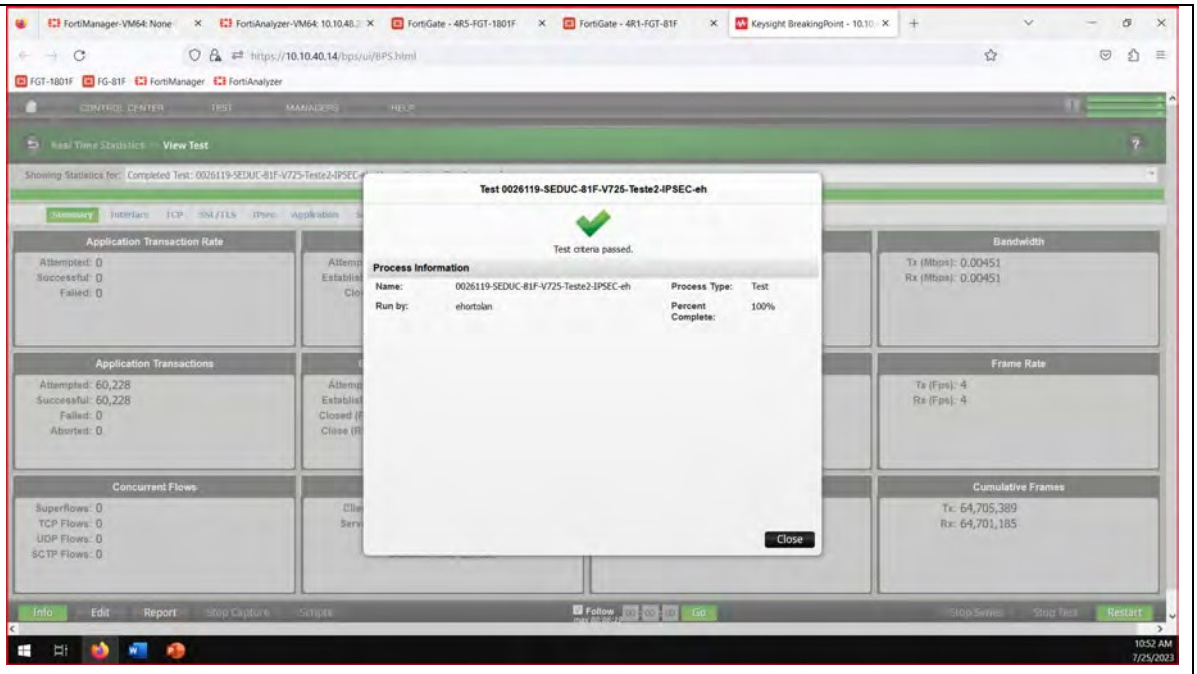
TESTE OK

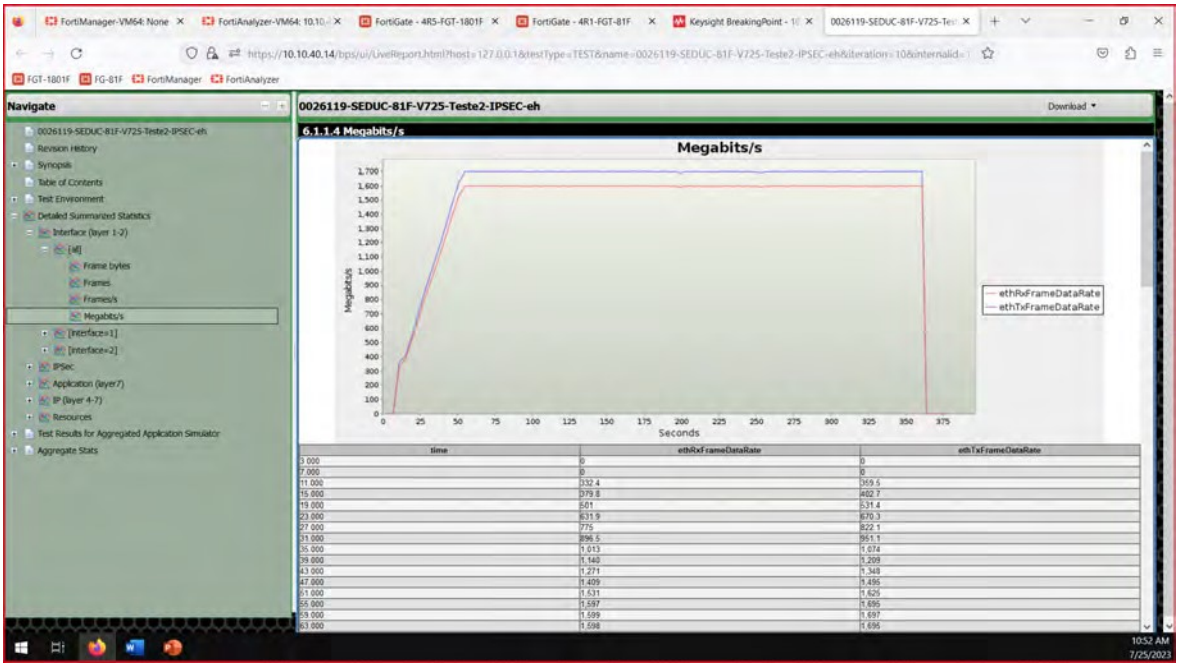
Evidências	Coletar durante o teste imagens com o equipamento performando 900 Mbps.
Comentário	

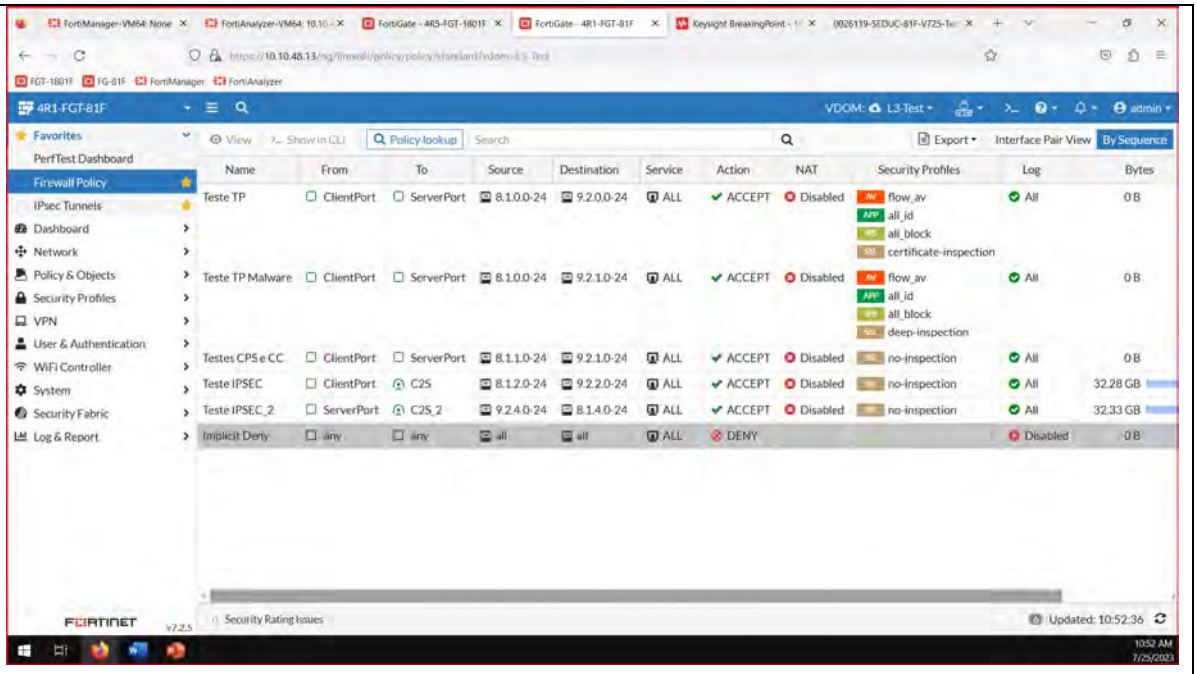
Item de Teste - 5.2.3.2	Possuir no mínimo 1,5 (Um e cinco décimos) Gbps de troughput para Ipsec VPN;
Objetivo do Teste	Validar a capacidade mínima de 1,5 Gbps de troughput para Ipsec VPN
Configuração do Teste	Teste a ser realizado no laboratório Fortinet. Será apresentado o perfil de tráfego que será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


4R1-FGT-81F
VDOM: L3-Test
admin
Favorites
PerfTest Dashboard
Firewall Policy
IPsec Tunnels
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
System
Security Fabric
Log & Report
Add Widget
CPU
1 minute
Current usage: 0%
Memory
Current usage: 38%
Session Rate
Current session rate: 185/s
Sessions
Current sessions: 364
Bandwidth - a
1 hour
Inbound 821.38 Mbps
Outbound 773.36 Mbps
Bandwidth - b
Inbound 857.00 Mbps
Outbound 806.92 Mbps
FORTINET
v7.2.5


4R1-FGT-81F
VDOM: L3-Test
admin
Favorites
PerfTest Dashboard
Firewall Policy
IPsec Tunnels
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
System
Security Fabric
Log & Report
View
Show Matching Logs
Search
Tunnel
Interface Binding
Status
Ref.
Custom
C2S
b
2 dialup connection(s)
2
C2S_2
a
2 dialup connection(s)
2
FORTINET
v7.2.5
Security Rating Issues

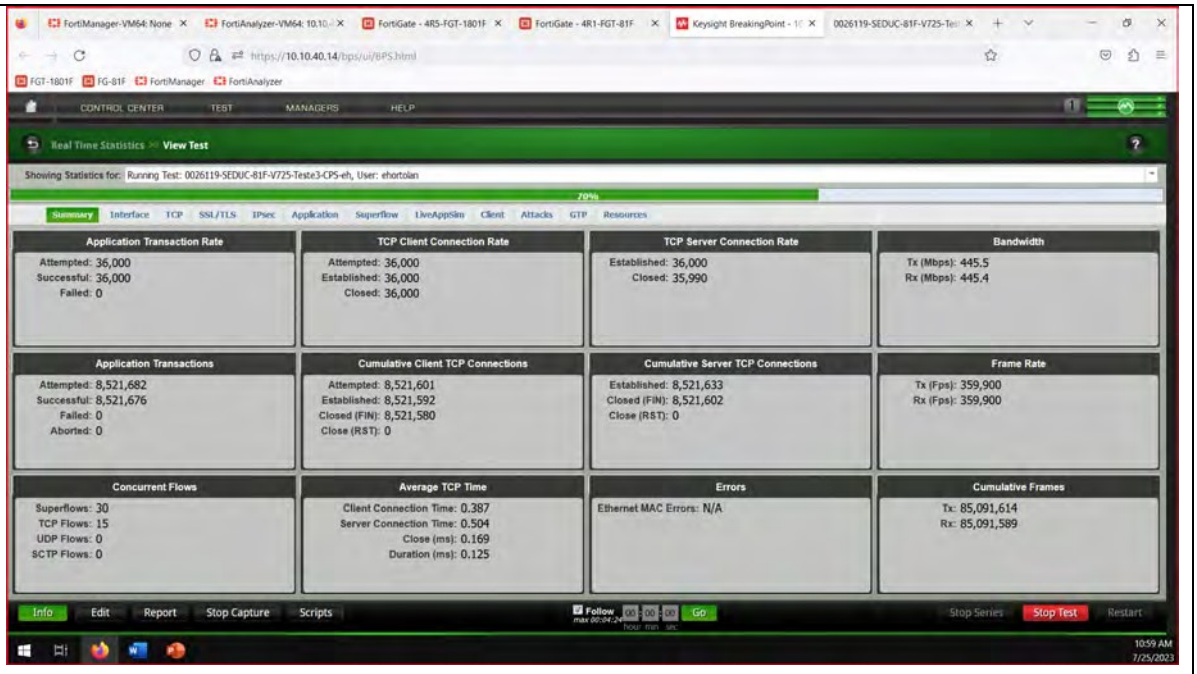
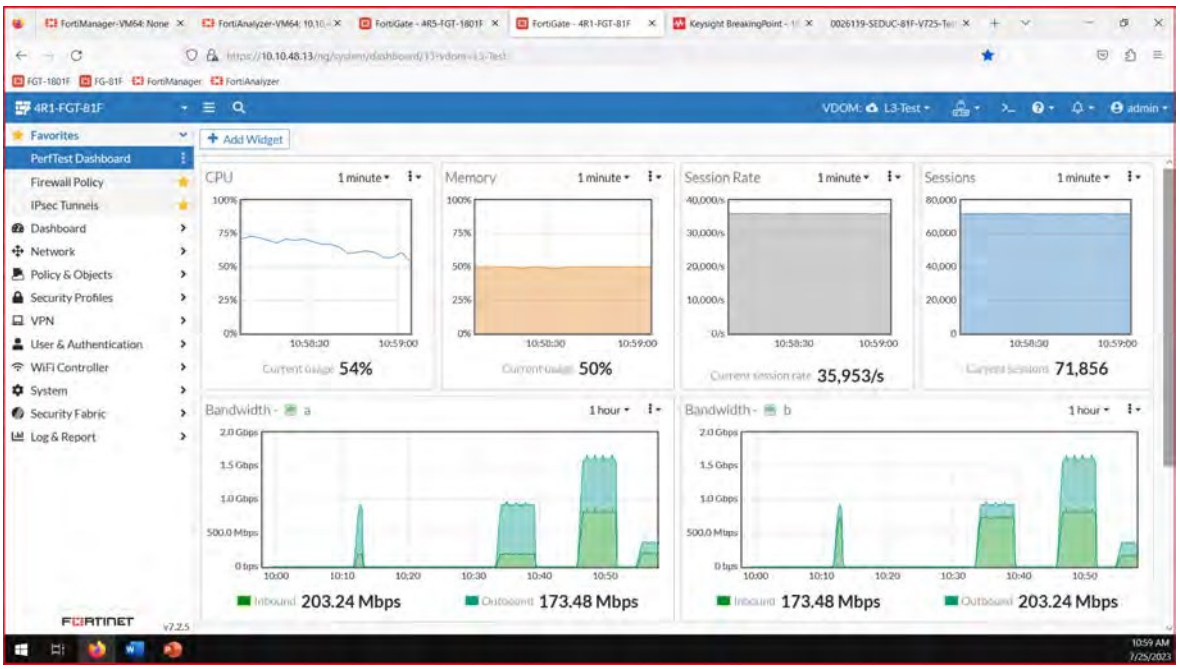

Test 0026119-SEDUC-81F-V725-Teste2-IPSEC-eh
Test criteria passed.
Process Information
Name: 0026119-SEDUC-81F-V725-Teste2-IPSEC-eh
Process Type: Test
Run by: ehortolan
Percent Complete: 100%
Close
Application Transaction Rate
Application Transactions
Bandwidth
Frame Rate
Concurrent Flows
Cumulative Frames

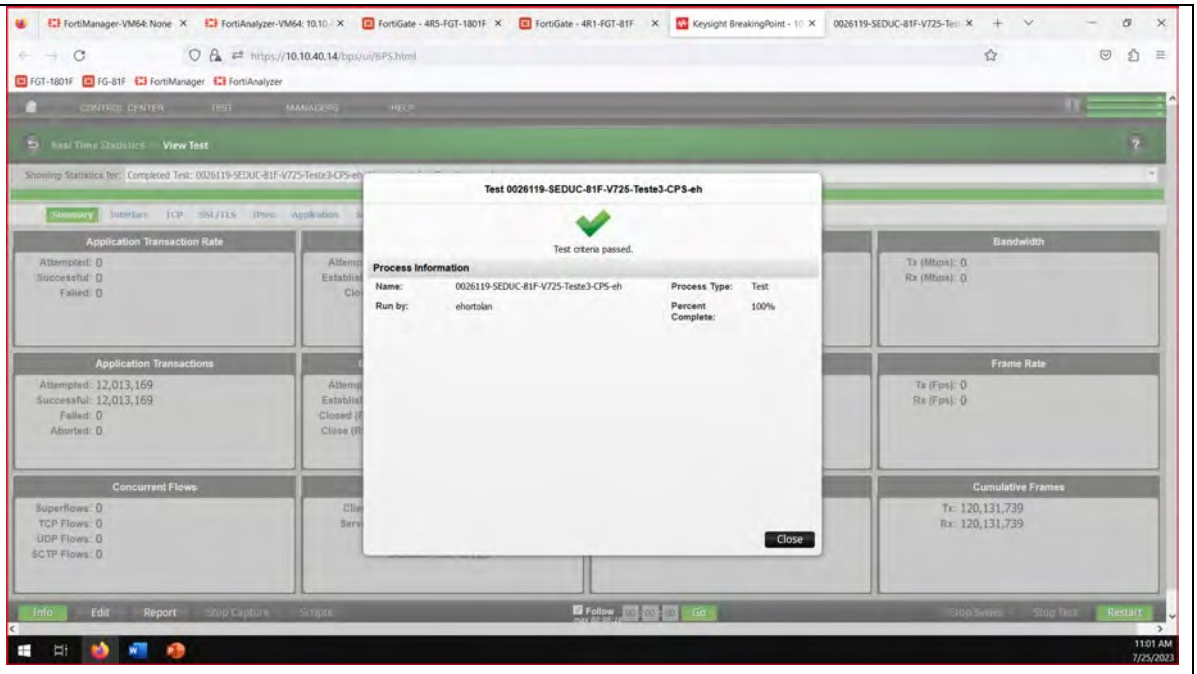

Navigate
0026119-SEDUC-81F-V725-Teste2-IPSEC-eh
6.1.1.4 Megabits/s
Megabits/s
Seconds
ethRxFrameDataRate
ethTxFrameDataRate

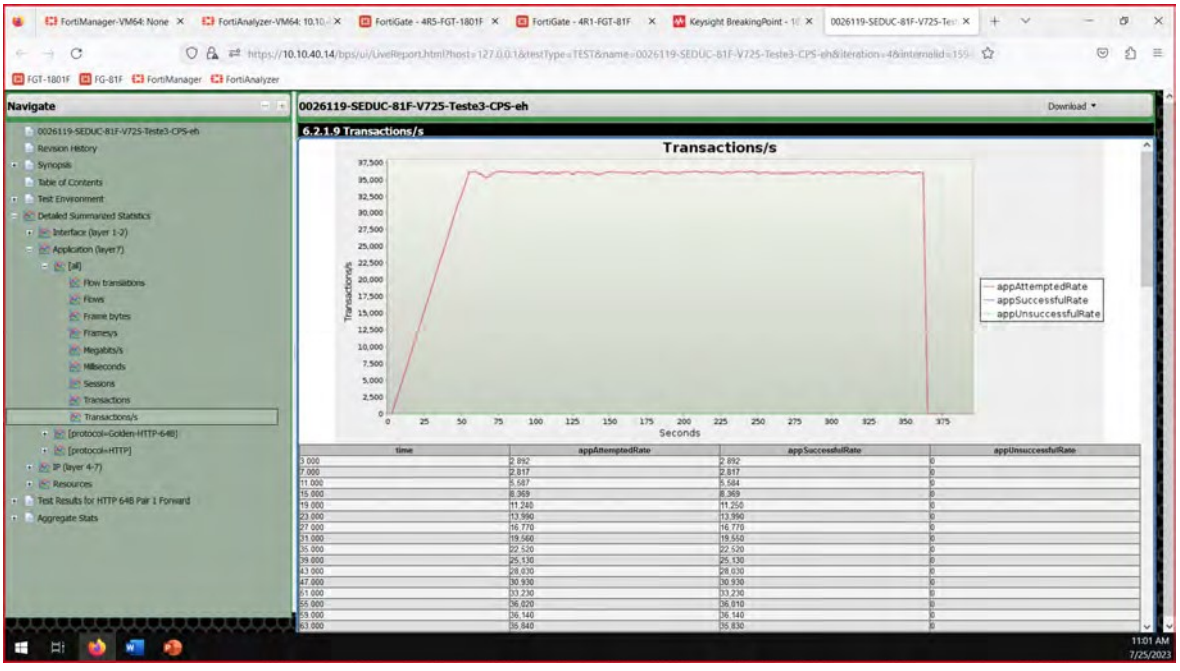
	 **TESTE OK**
Comentário	

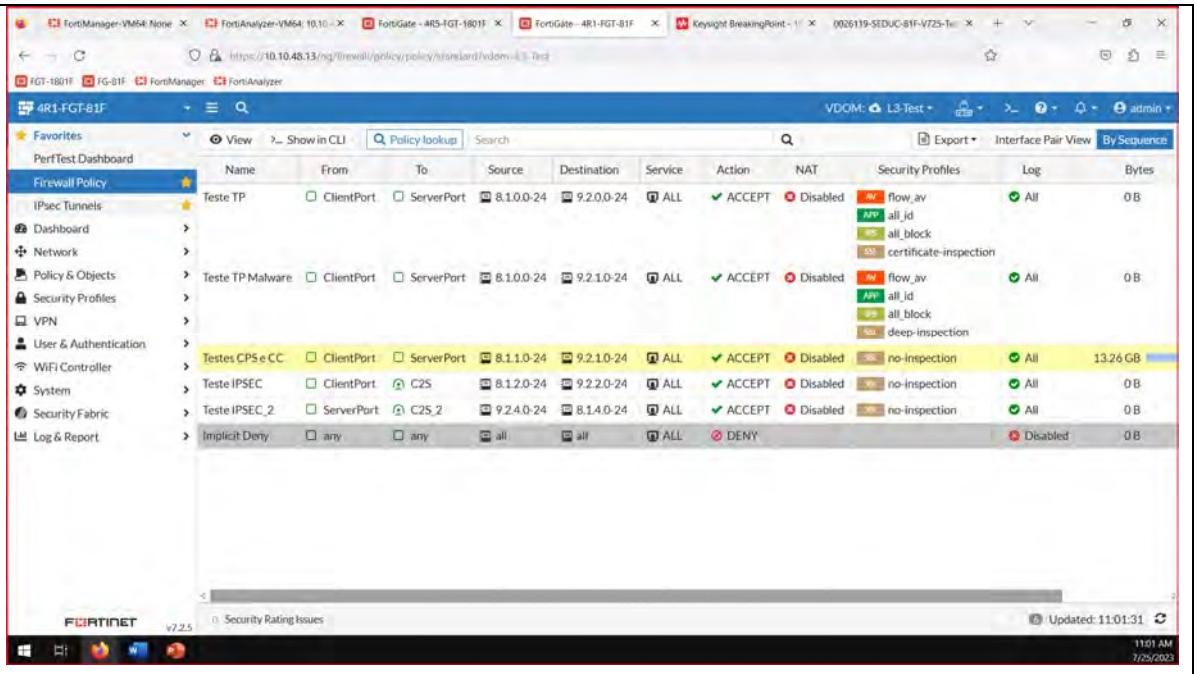
5.2.4 CONEXÕES

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

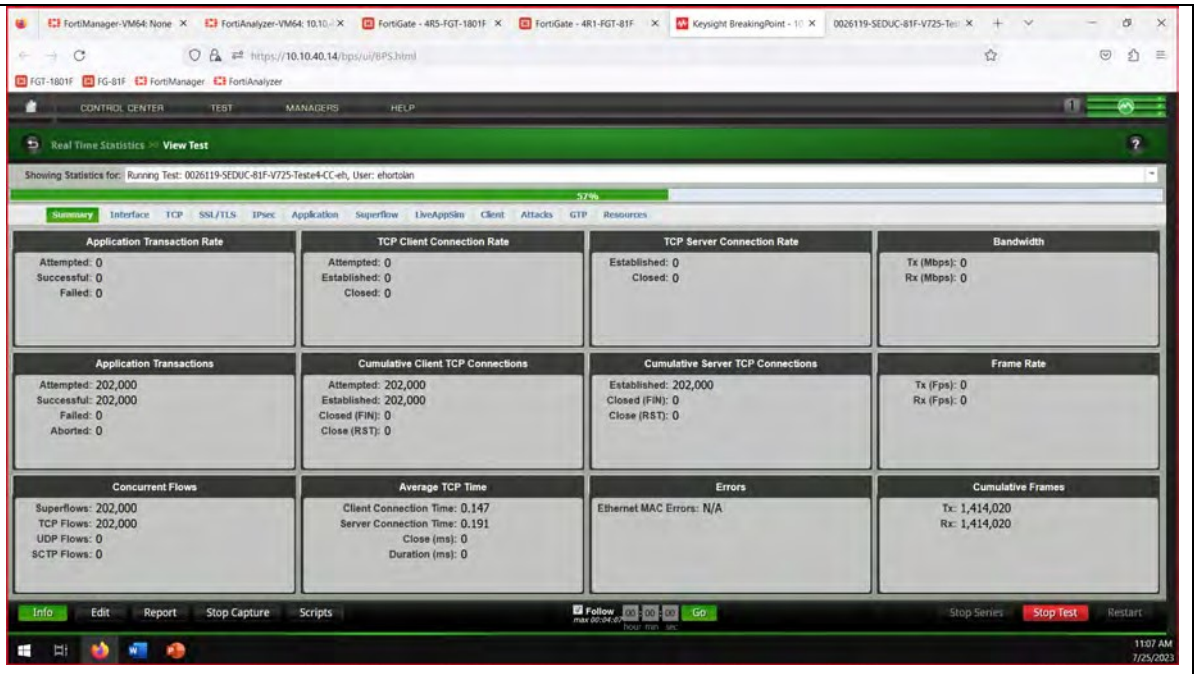
Evidências	 

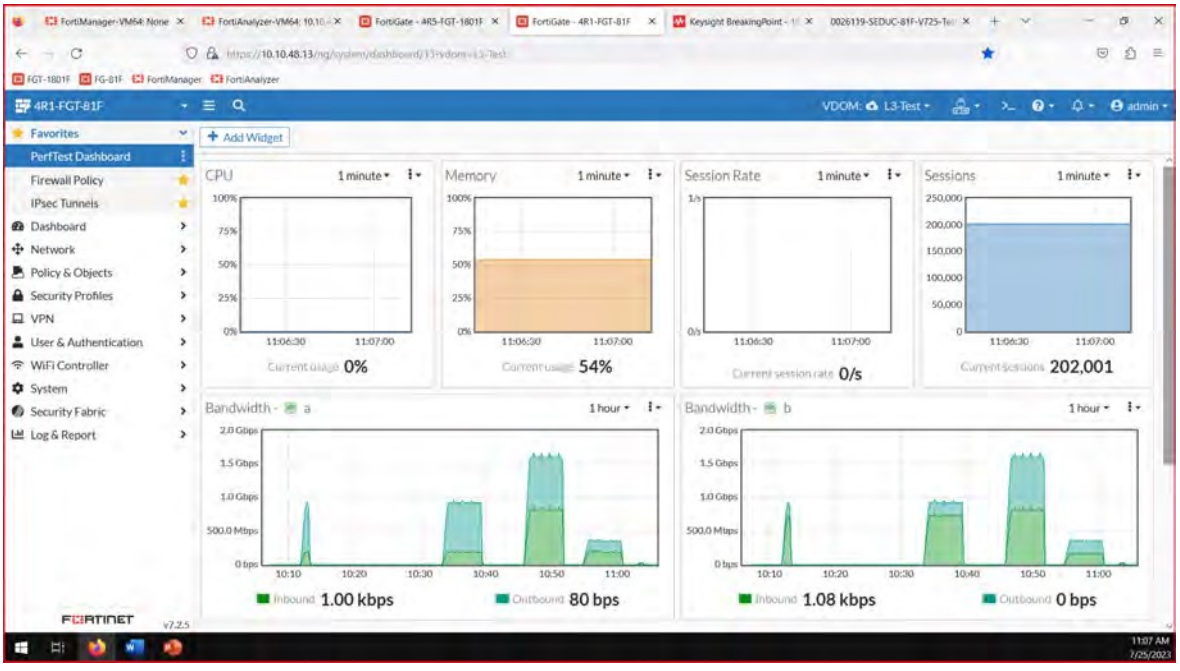

Test 0026119-SEDUC-81F-V725-Teste3-CPS-eh
Test criteria passed.
Process Information
Name: 0026119-SEDUC-81F-V725-Teste3-CPS-eh
Process Type: Test
Run by: ehortolan
Percent Complete: 100%
Close
Application Transaction Rate
Application Transactions
Attempted: 12,013,169
Successful: 12,013,169
Failed: 0
Aborted: 0
Bandwidth
Frame Rate
Concurrent Flows
Cumulative Frames
Tx: 120,131,739
Rx: 120,131,739

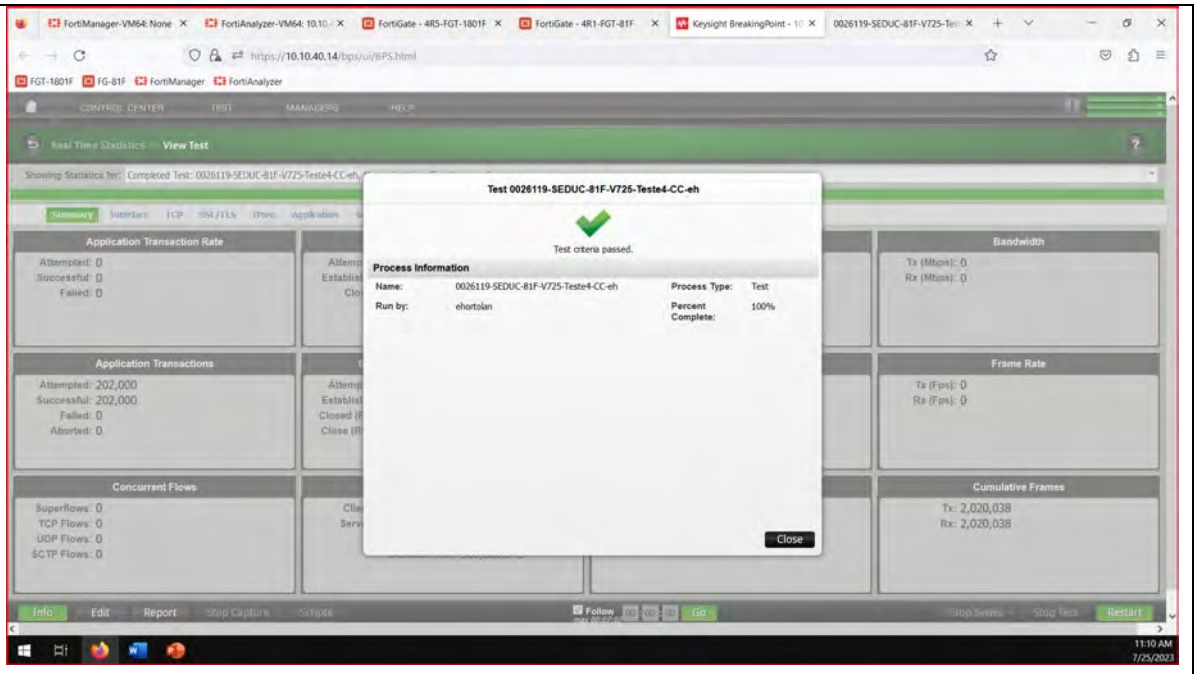

Navigate
0026119-SEDUC-81F-V725-Teste3-CPS-eh
6.2.1.9 Transactions/s
Transactions/s
appAttemptedRate
appSuccessfulRate
appUnsuccessfulRate
Seconds

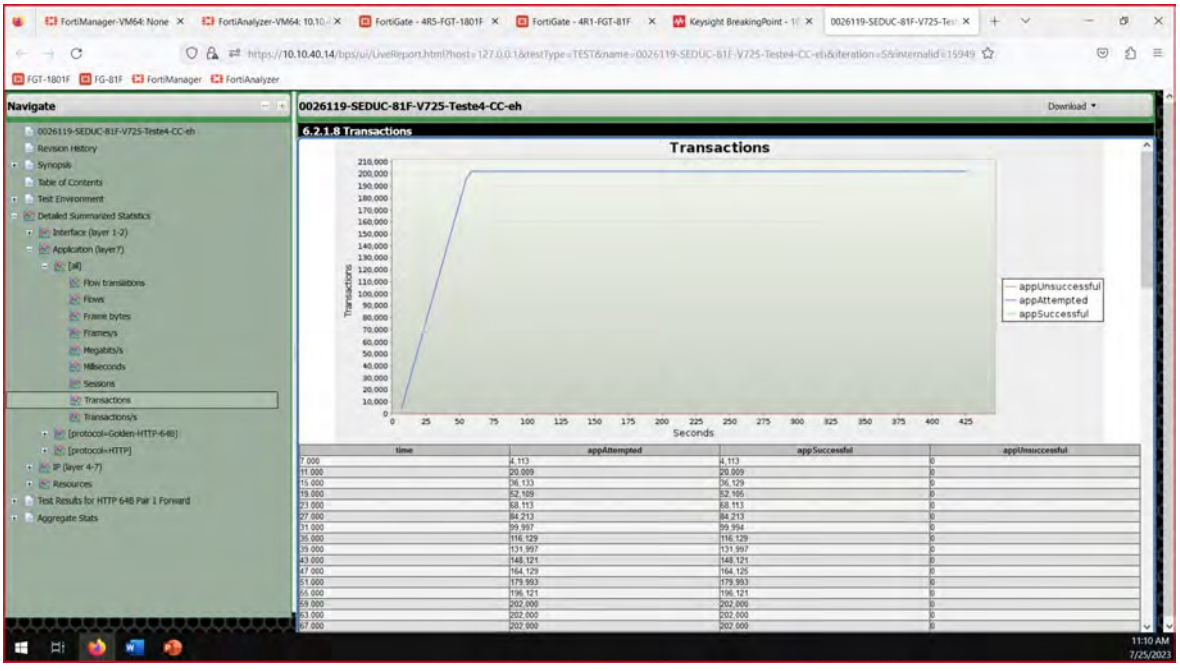
	 **TESTE OK**
Comentário	

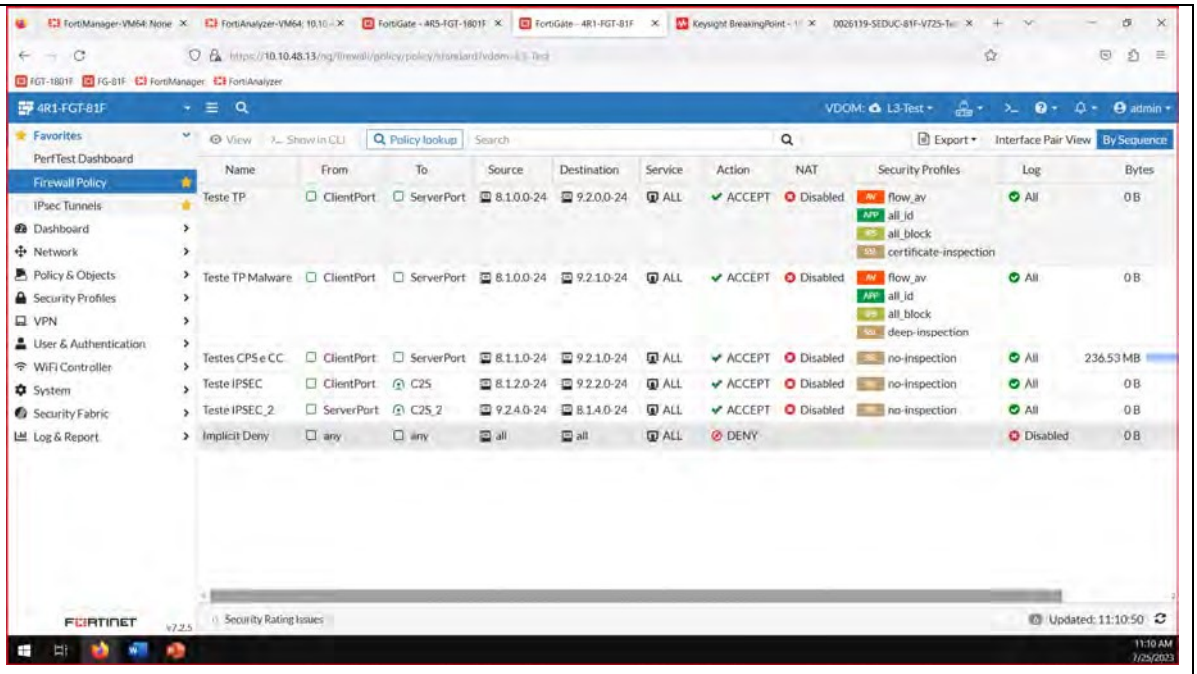
Item de Teste - 5.2.4.2	Permitir no mínimo 200.000 (duzentas mil) conexões simultâneas;
Objetivo do Teste	Validar se o FortiGate 81F permite no mínimo 200.000 conexões simultâneas
Configuração do Teste	Teste em laboratório
Procedimento do Teste	Teste a ser realizado no laboratório da Fortinet
Evidências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


CONTROL CENTER
TEST
MANAGERS
HELP
Real Time Statistics >> View Test
Application Transaction Rate
Attempted: 0
Successful: 0
Failed: 0
TCP Client Connection Rate
Attempted: 0
Established: 0
Closed: 0
TCP Server Connection Rate
Established: 0
Closed: 0
Bandwidth
Tx (Mbps): 0
Rx (Mbps): 0
Application Transactions
Attempted: 202,000
Successful: 202,000
Failed: 0
Aborted: 0
Cumulative Client TCP Connections
Attempted: 202,000
Established: 202,000
Closed (FIN): 0
Close (RST): 0
Cumulative Server TCP Connections
Established: 202,000
Closed (FIN): 0
Close (RST): 0
Frame Rate
Tx (Fps): 0
Rx (Fps): 0
Concurrent Flows
Superflows: 202,000
TCP Flows: 202,000
UDP Flows: 0
SCTP Flows: 0
Average TCP Time
Client Connection Time: 0.147
Server Connection Time: 0.191
Close (ms): 0
Duration (ms): 0
Errors
Ethernet MAC Errors: N/A
Cumulative Frames
Tx: 1,414,020
Rx: 1,414,020
Info
Edit
Report
Stop Capture
Scripts
Go
Stop Series
Stop Test
Restart


4R1-FGT-81F
Favorites
PerfTest Dashboard
Firewall Policy
IPsec Tunnels
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
System
Security Fabric
Log & Report
Add Widget
CPU
Memory
Session Rate
Sessions
Current usage 0%
Current usage 54%
Current session rate 0/s
Current sessions 202,001
Bandwidth - a
Bandwidth - b
Inbound 1.00 kbps
Outbound 80 bps
Inbound 1.08 kbps
Outbound 0 bps

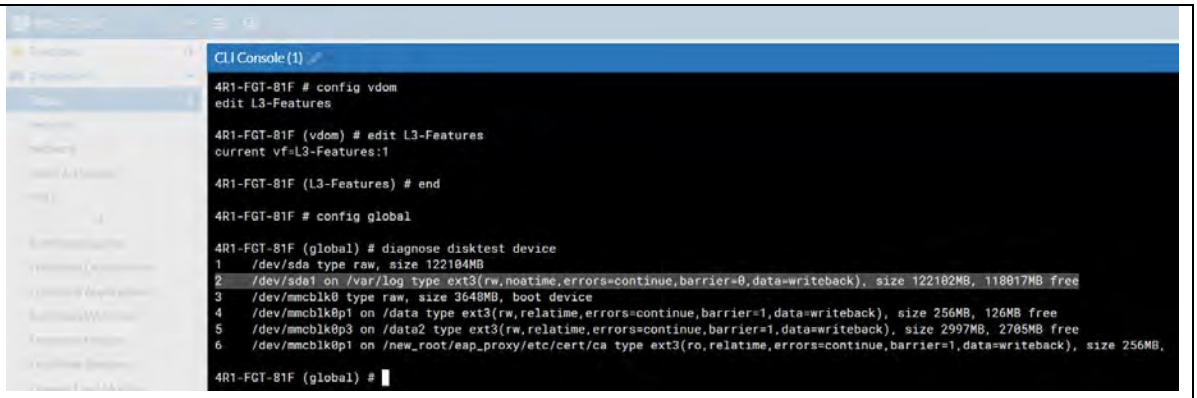
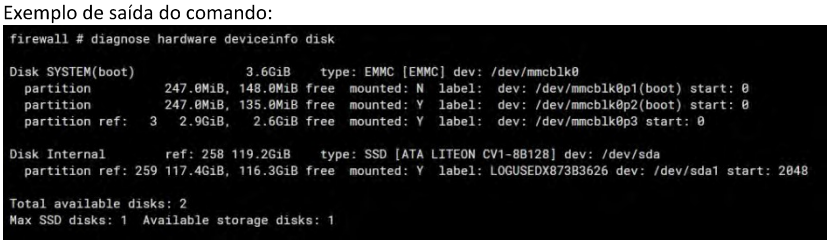

Test 0026119-SEDUC-81F-V726-Teste4-CC-eh
Test criteria passed.
Process Information
Name: 0026119-SEDUC-81F-V725-Teste4-CC-eh
Process Type: Test
Run by: ehortolan
Percent Complete: 100%
Close
Application Transaction Rate
Application Transactions
Attempted: 202,000
Successful: 202,000
Failed: 0
Aborted: 0
Concurrent Flows
Bandwidth
Frame Rate
Cumulative Frames
Tx: 2,020,038
Rx: 2,020,038

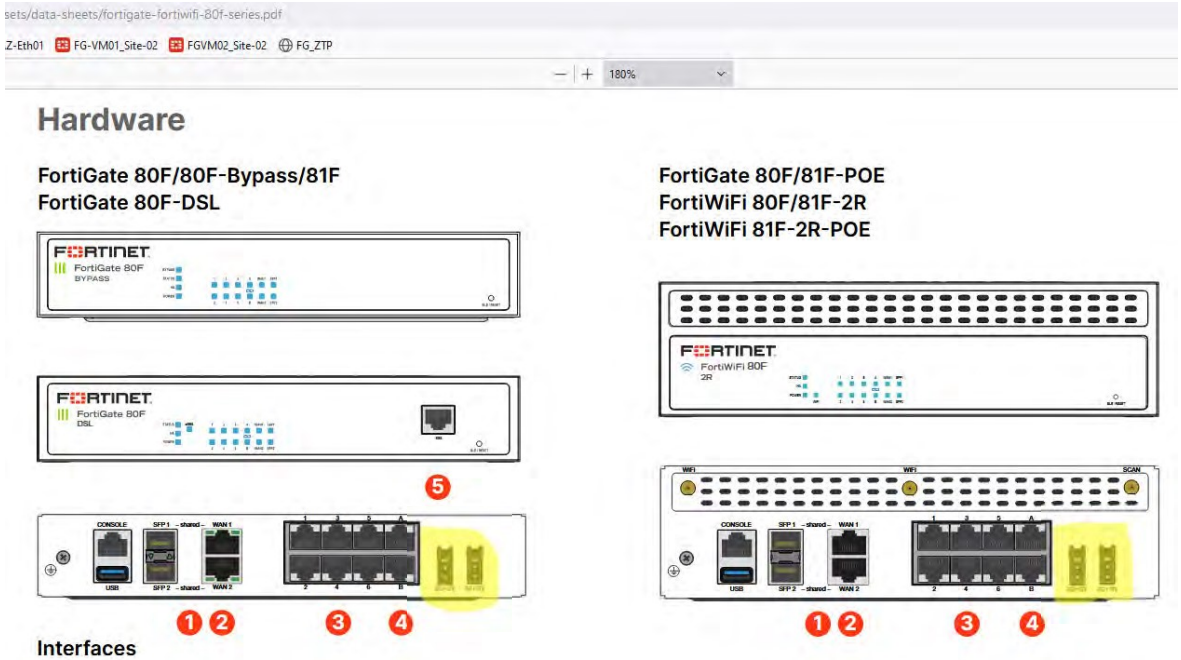

Navigate
0026119-SEDUC-81F-V725-Teste4-CC-eh
6.2.1.8 Transactions
Transactions
Seconds
appUnsuccessful
appAttempted
appSuccessful

	 **TESTE OK**
Comentário	

5.2.5 HARDWARE:

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

Evidências	 **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: 
Comentário	

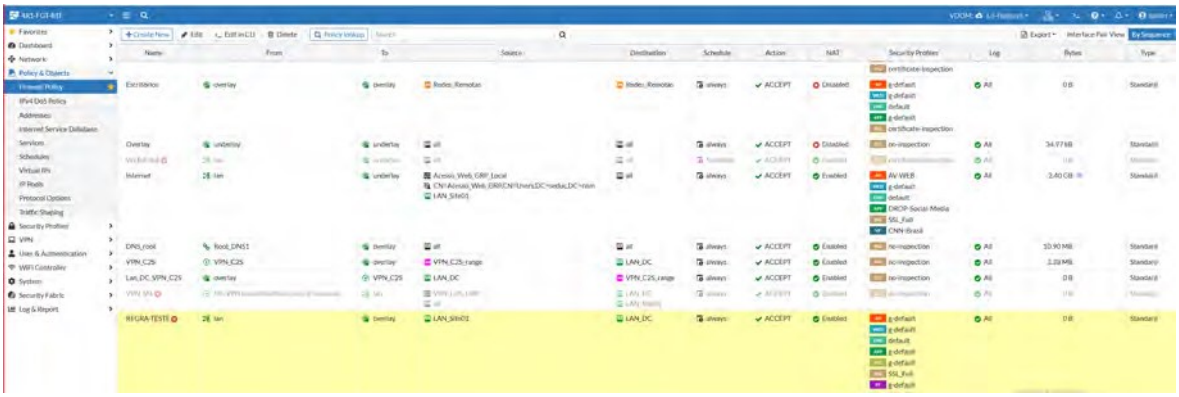
Item de Teste - 5.2.5.3	Possuir alimentação elétrica a partir de no mínimo 2 (duas) fontes independentes e redundantes, capazes de operar entre 110-240VAC, 60 Hz;
Objetivo do Teste	Mostrar que o equipamento possuí alimentação elétrica de no mínimo 2 (duas) fontes independentes e redundantes, capazes de operar entre 110-240VAC, 60 Hz.
Configuração do Teste	Teste físico
Procedimento do Teste	Comprovação visual e por meio do datasheet.
Evidências	  **Specifications** **Dimensions and Power** **Operating Environment and Certifications** **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/0.4A, 115VAC/0.4A, 115VAC/0.4A, 115VAC/2.2A, 115VAC/1.2A

	TESTE OK  Specifications FG-80F-DSL / FWF-80F-2R-3G4G-DSL / FWF-81F-2R-3G4G-DSL / FWF-81F-2R-3G4G-POE Dimensions and Power Height x Width x Length (inches) 2.4 × 8.5 × 7.0 Height x Width x Length (mm) 60 × 216 × 178 Weight 3.07 lbs (1.39 kg) / 3.5 lbs (1.6 kg) Form Factor (supports EIA/non-EIA standards) Desktop / Wallmount (optional) Input Rating 12V DC, 5A / 54V DC, 2.78A Power Required (Redundancy Optional) Powered by up to two external DC power adapters (one adapter included), 100-240V AC, 50/60 Hz Current (Maximum) 115Vac/0.5A, 230Vac/0.6A Total Available PoE Power Budget* – / 96W Power Consumption (Average / Maximum) 28.0 W / 31.6 W / 28.07 W / 34.31 W / 29.2 W / 35.6 W / 109.3 W / 133.6 W Heat Dissipation 108 BTU/h / 117.0 BTU/h / 121.5 BTU/h / 455.6 BTU/h Operating Environment and Certifications
Comentário	Fonte: Acessado em https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-80f-series.pdf

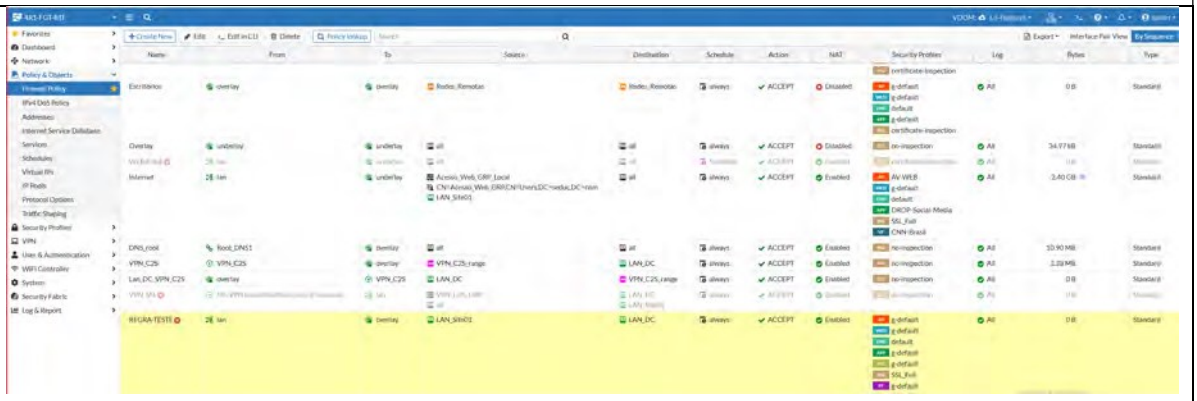
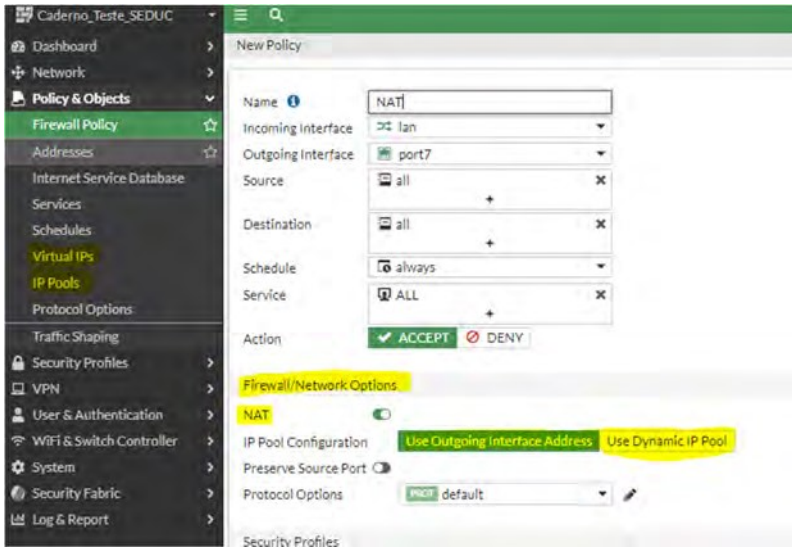
5.3 Funcionalidades gerais para Solução de Segurança Tipo 1, Tipo 2

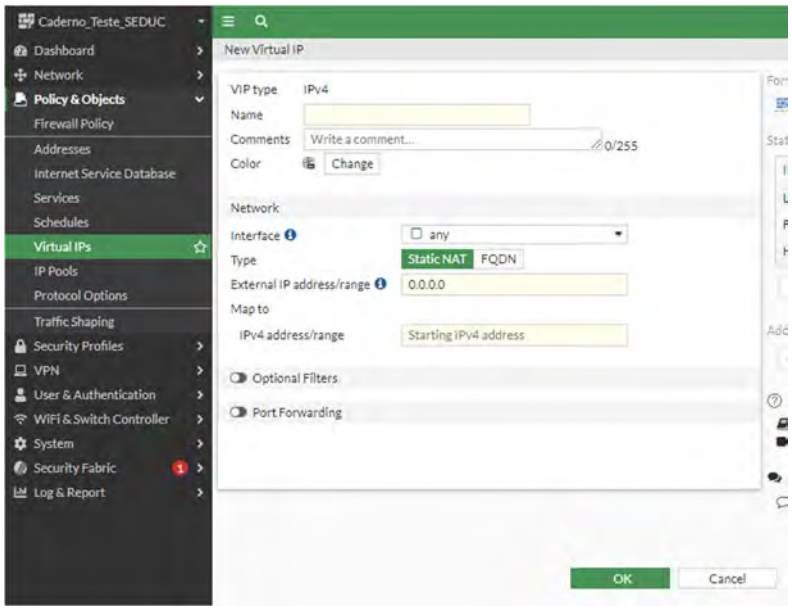
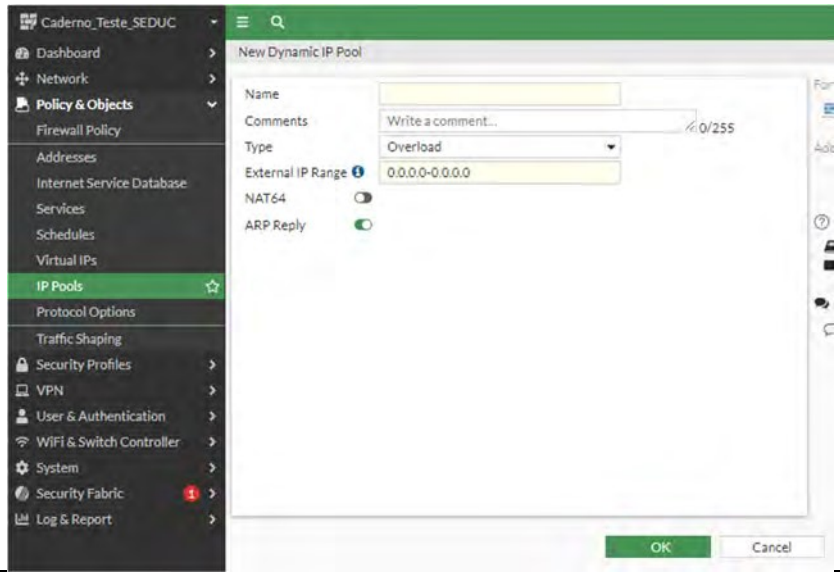
5.3.1 CARACTERISTICAS GERAIS

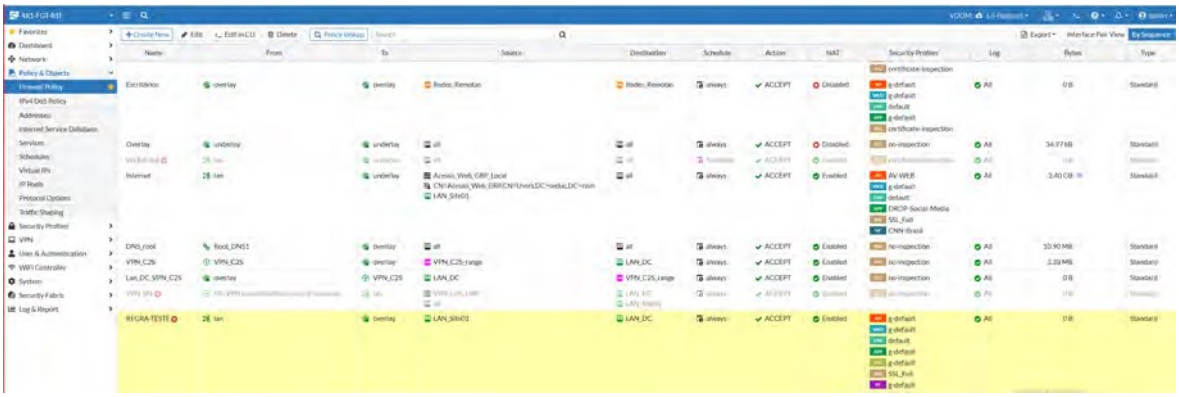
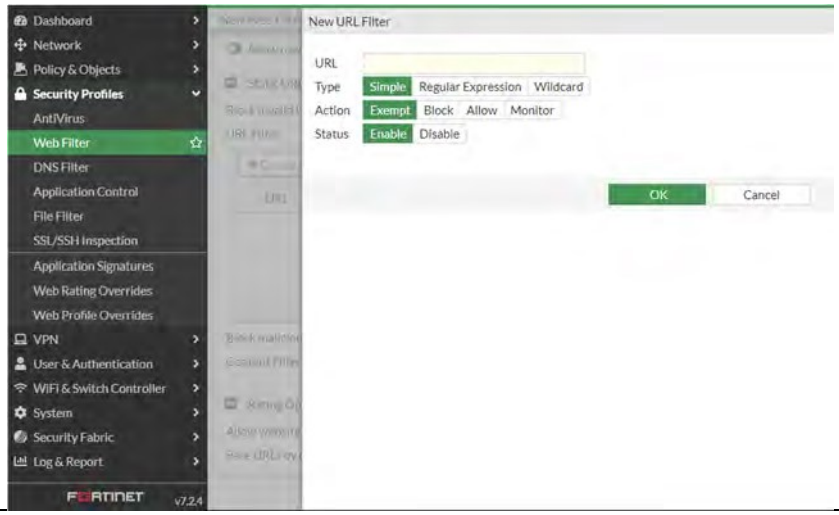
5.3.1.1 Deve implementar:

Item de Teste - 5.3.1.1.1	Firewall
Objetivo do Teste	Evidenciar que os equipamentos FortiGate1800F e FortiGate 81F são dispositivos de firewall com capacidade de filtrar pacotes e tomar decisão.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Demonstrar base de regras do FortiGate
Evidências	 **TESTE OK** 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.

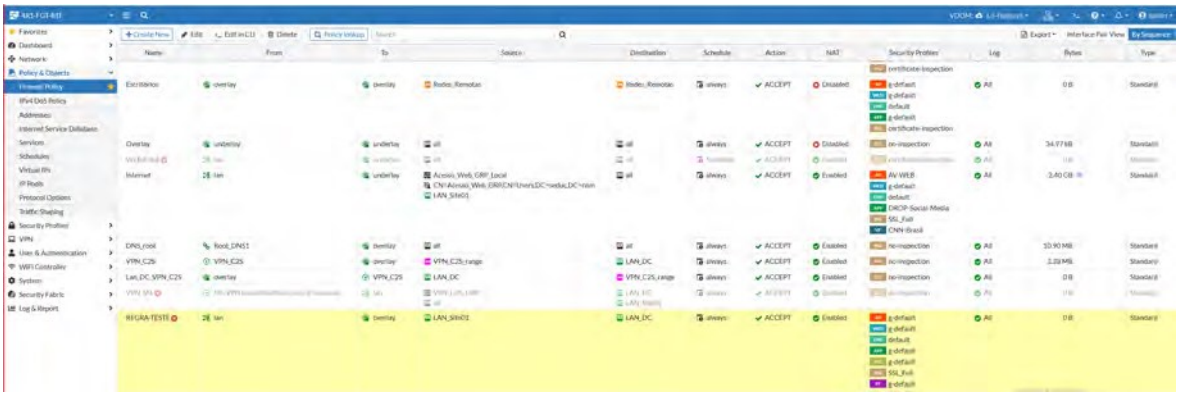
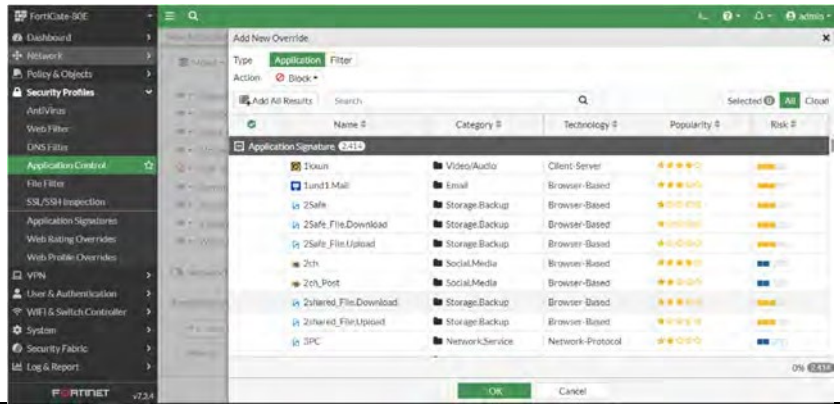
Comentário	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a06117ca-5fbf-11ed-96f0-fa163e15d75b/FortiOS-7.2.3-Administration_Guide.pdf

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

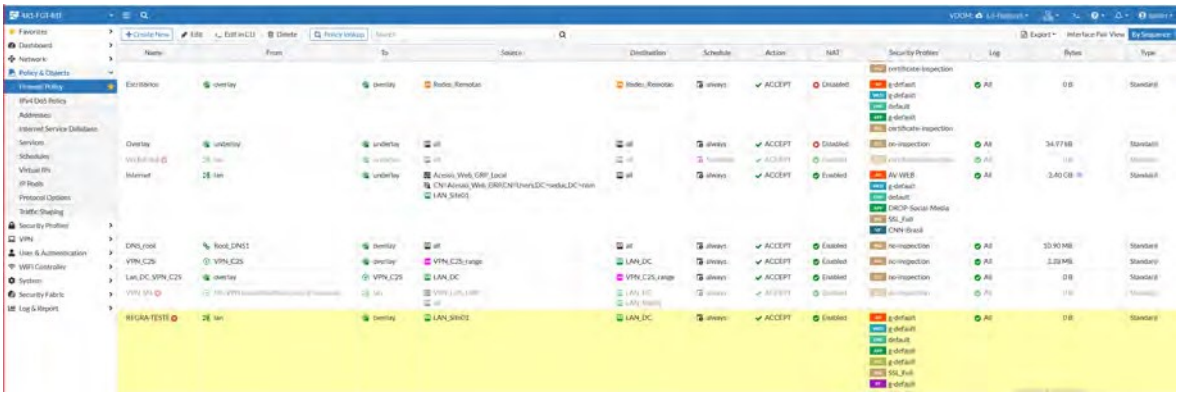
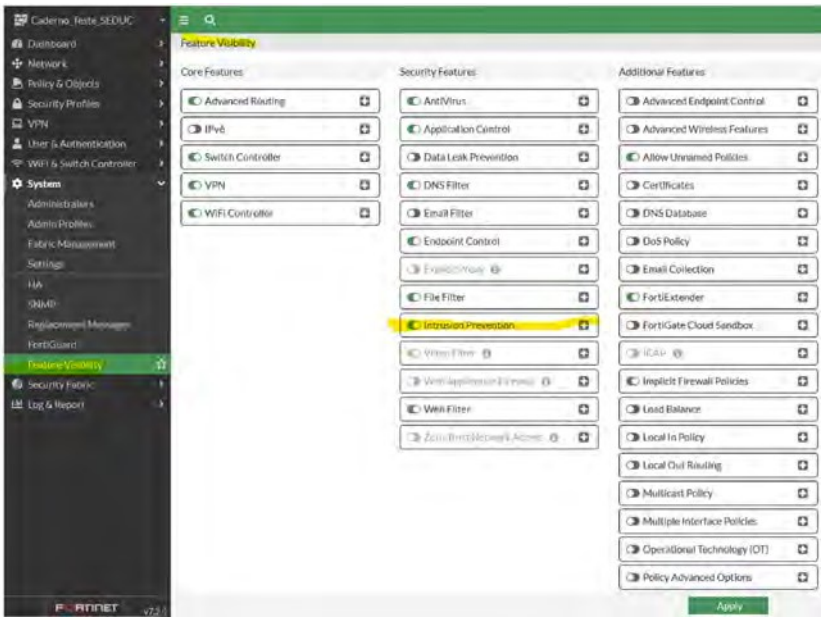
	2 – Virtual IPS  3 – IP Pools 
Comentário	https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/898655/static-snat https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/29961/dynamic-snat https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/728694/destination-nat

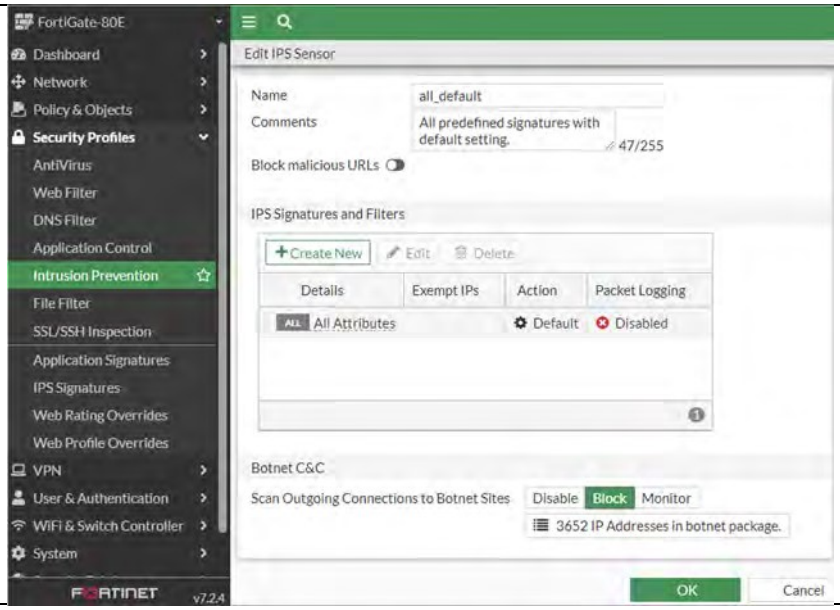
Item de Teste - 5.3.1.1.3	URL Filtering,
Objetivo do Teste	Demonstrar capacidade de criar filtros por URL
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Para acessar essa funcionalidade vá em **Security Profile** -> **Web Filter**.
Evidências	 **TESTE OK** 
Comentário	

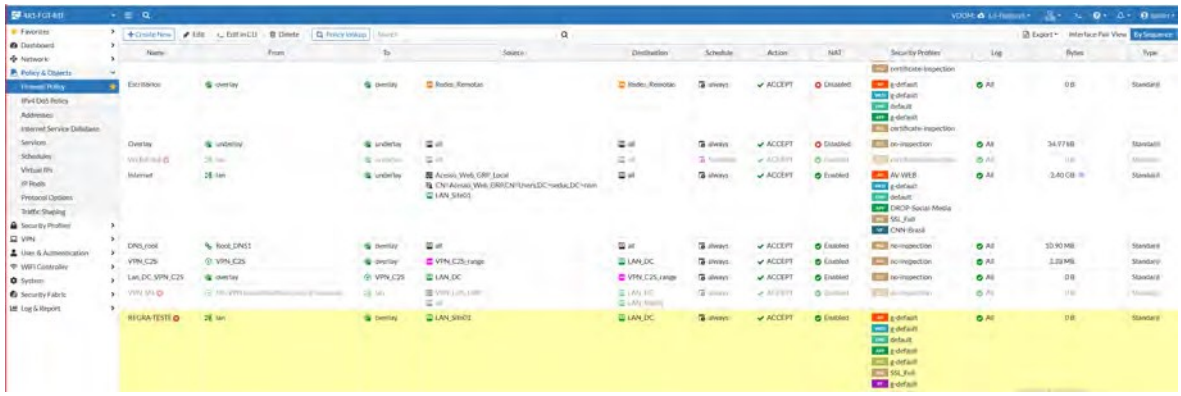
Item de Teste - 5.3.1.1.4	Application Control;
Objetivo do Teste	Demostrar capacidade de executar filtros por Aplicação.

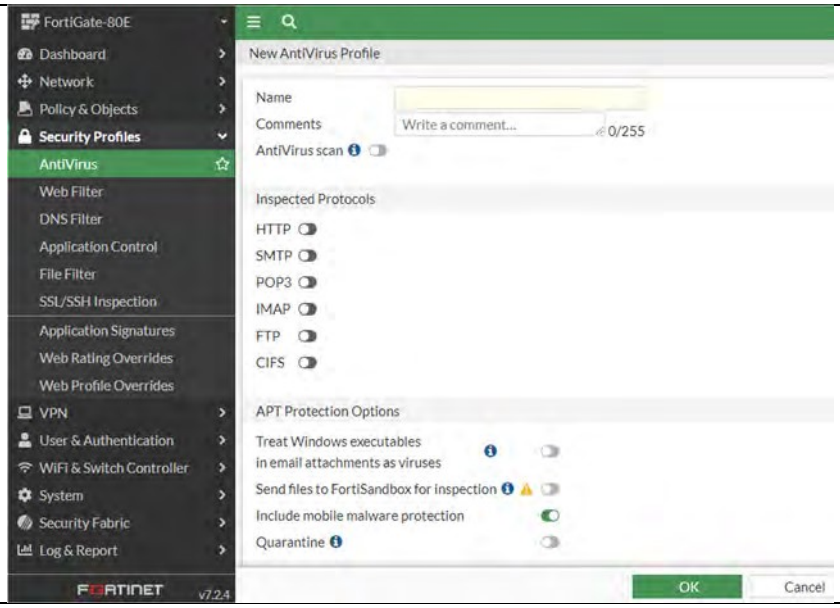
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Para ter acesso a essa funcionalidade, é necessário acessar o menu "Security Profile" e, em seguida, selecionar a opção "Application Control".
Evidências	 **TESTE OK** 
Comentário	

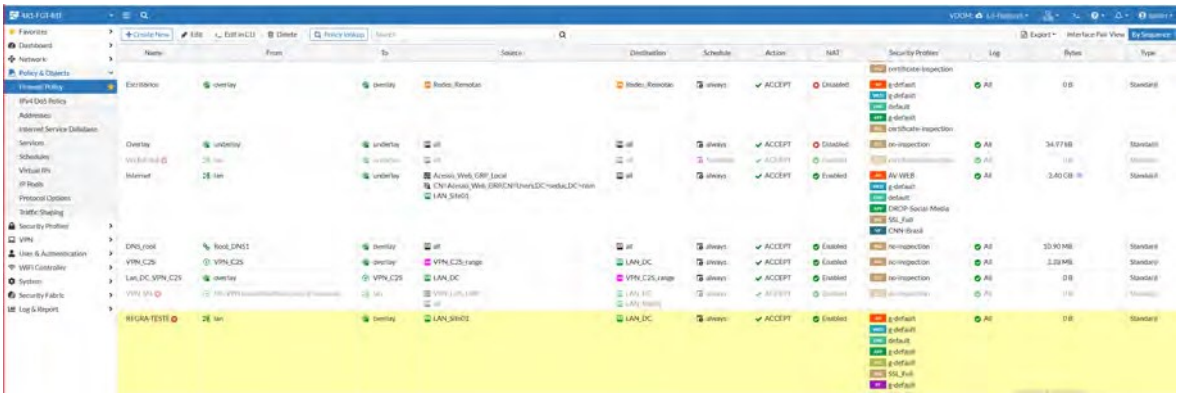
Item de Teste - 5.3.1.1.5	Anti-bot;
Objetivo do Teste	Validar se a solução tem ferramenta Anti-bot de forma nativa
Configuração do Teste	Demonstrar base de regras do FortiGate

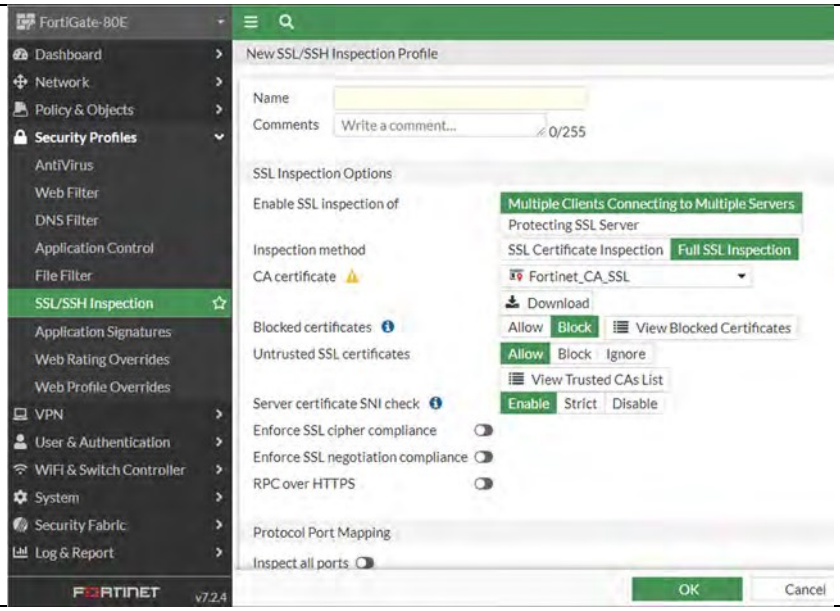
Procedimento do Teste	Para ter acesso a esta funcionalidade, é necessário habilitar a função de Prevenção de Intrusões (IPS) por meio do menu "System" e, em seguida, acessar a opção "Feature Visibility" e habilitar a funcionalidade de IPS. Posteriormente, é necessário criar um sensor de IPS na seção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

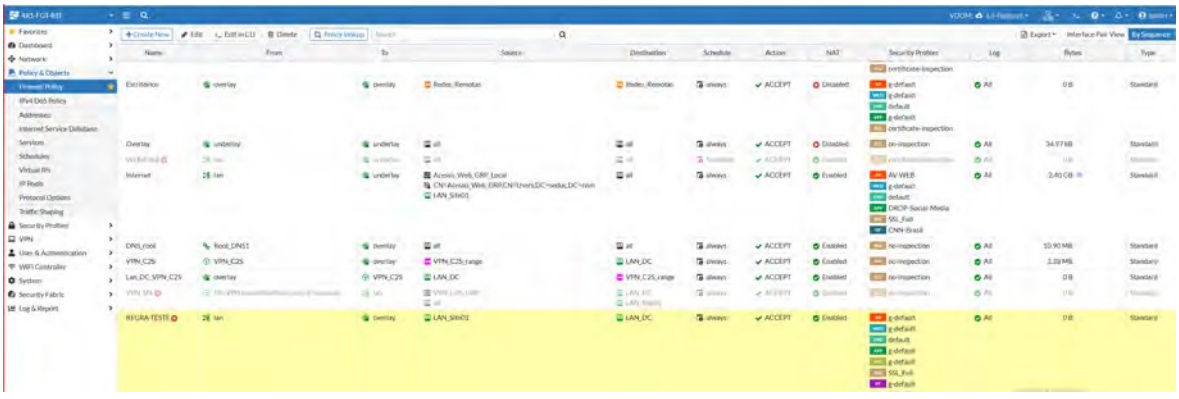
	
Comentário	

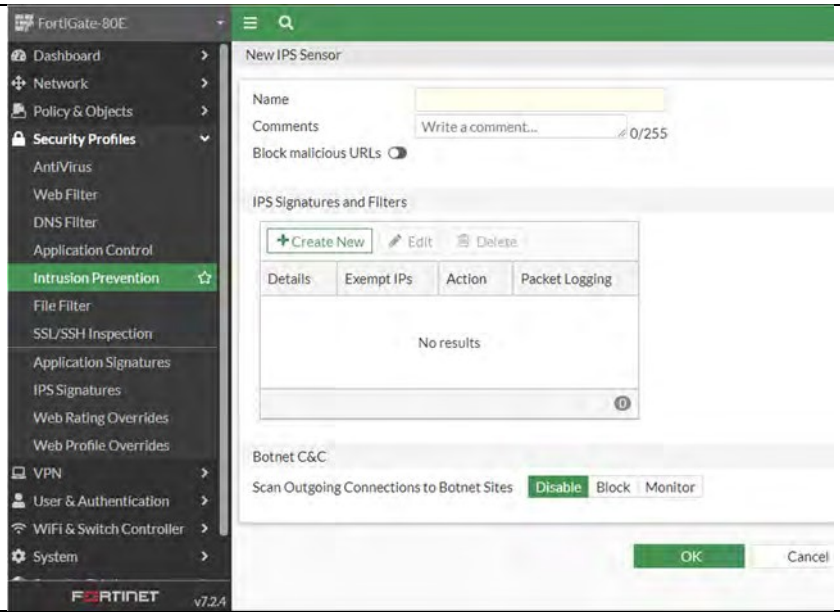
Item de Teste - 5.3.1.1.6	Anti-Virus;
Objetivo do Teste	Validar se o FortiGate possui ferramenta de Anti-vírus de forma nativa.
Configuração do Teste	Demonstrar base de regras do FortiGate.
Procedimento do Teste	Para acessar basta ir em **Security Profile** -> **Antivírus**.
Evidências	 **TESTE OK**

	
Comentário	

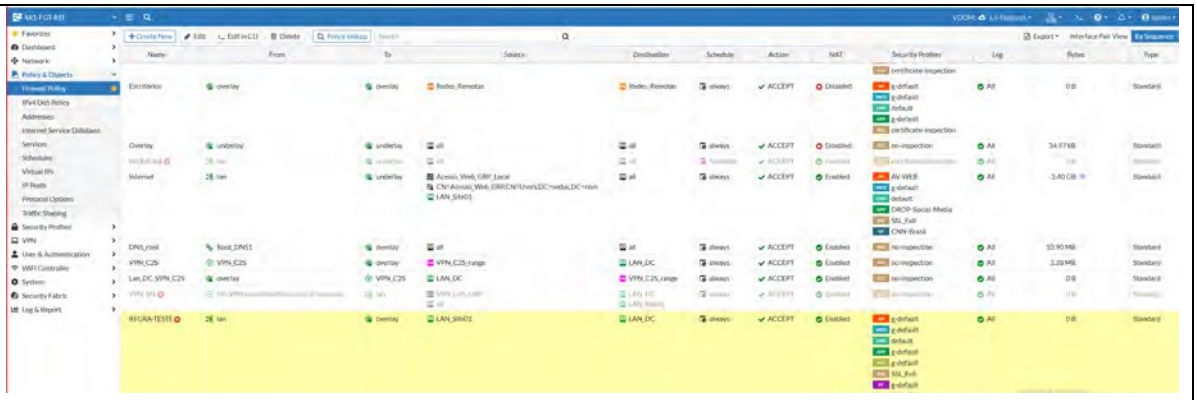
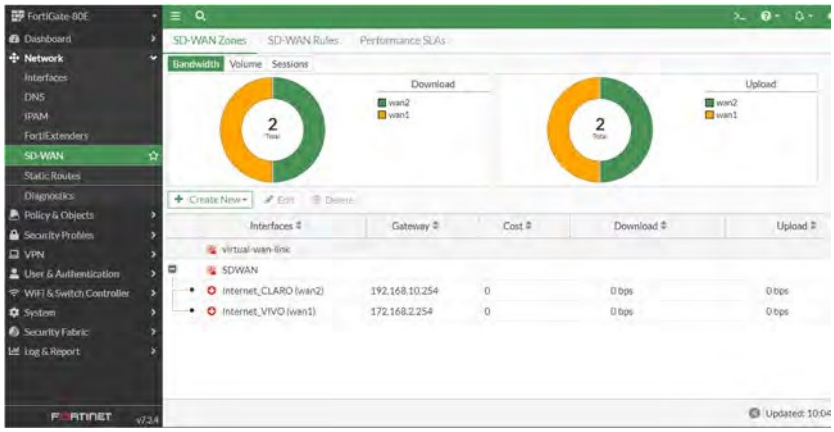
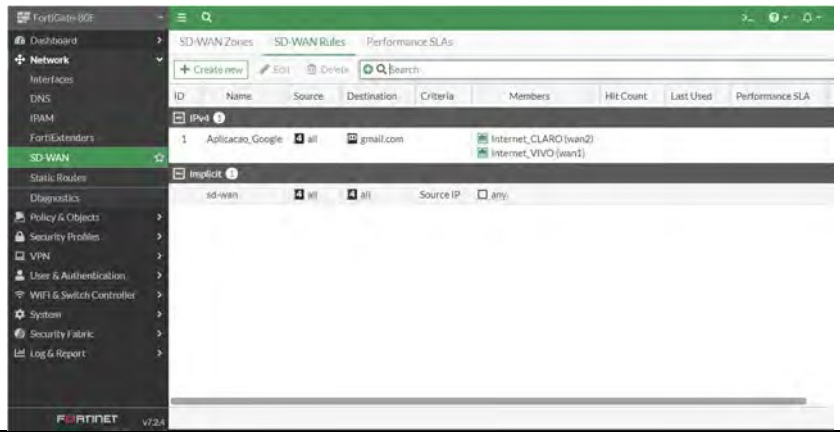
Item de Teste - 5.3.1.1.7	SSL Inspection;
Objetivo do Teste	Validar se o firewall realiza SSL Inspection de forma nativa.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Para acessar basta ir em **Security Profile** -> **SSL/SSH Inspection**.
Evidências	 **TESTE OK**

	
Comentário	

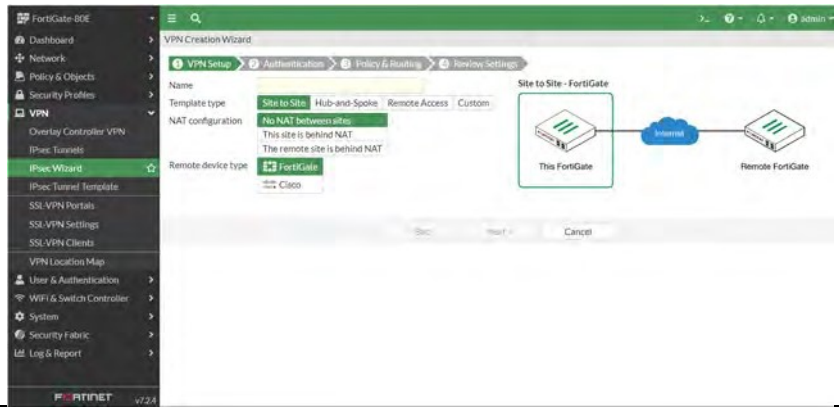
Item de Teste - 5.3.1.1.8	IDS/IPS;
Objetivo do Teste	Validar se o FortiGate tem as funcionalidades de IDS/IPS de forma nativa.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Para realizar essa configuração, há a necessidade primeiro de habilitar ela, para isso vá em **System** -> **Feature Visibility** e habilite o Intrusion Prevention. Depois Ir em **Security Profiles** -> **Intrusion Prevention** -> **Create New**
Evidências	 **TESTE OK**

	
Comentário	

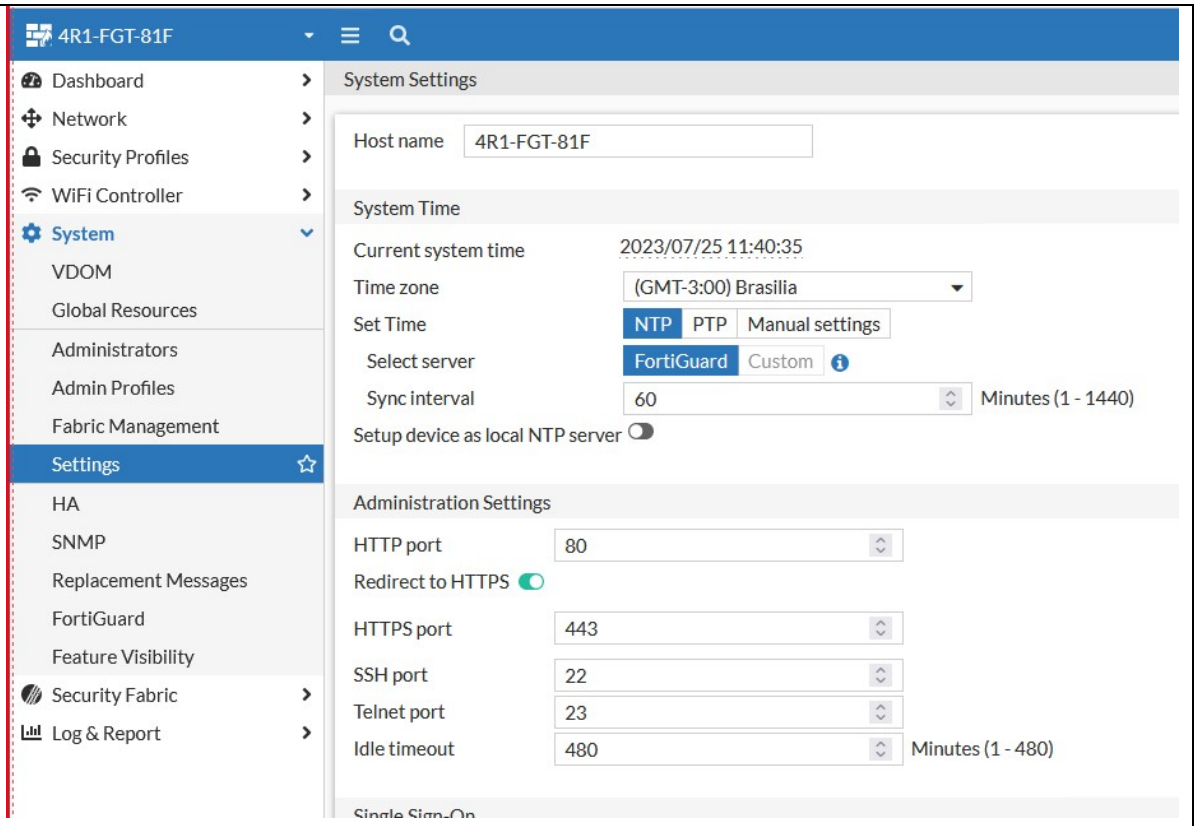
Item de Teste - 5.3.1.1.9	SDWAN;
Objetivo do Teste	Validar se o equipamento possui a funcionalidade de SDWAN.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Navegando por **Network** -> **SDWAN-** > **Create new member** é possível acrescentar links para serem balanceados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

	 **TESTE OK**  
Comentário	

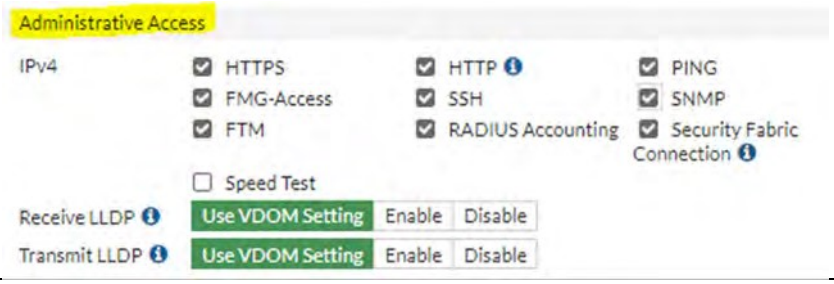
Item de Teste - 5.3.1.1.10	VPN site-to-site;
Objetivo do Teste	Validar se a ferramenta possibilita a criação de VPN site-to-site

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	 **TESTE OK** 
Comentário	

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

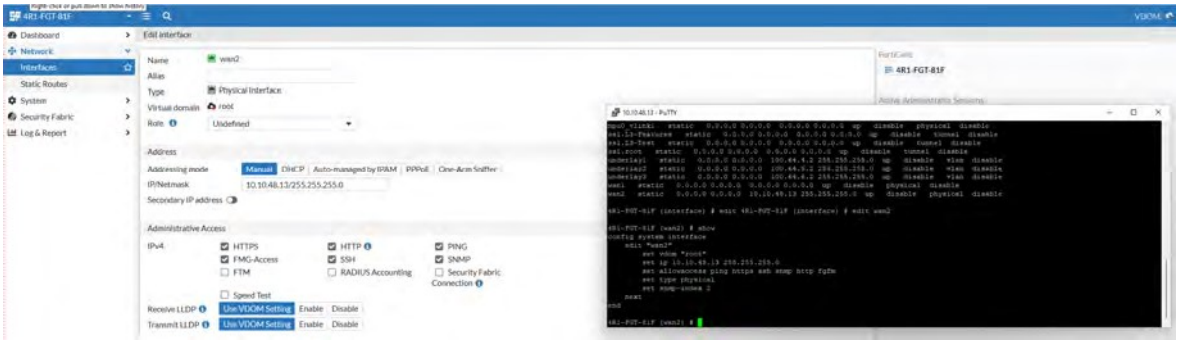


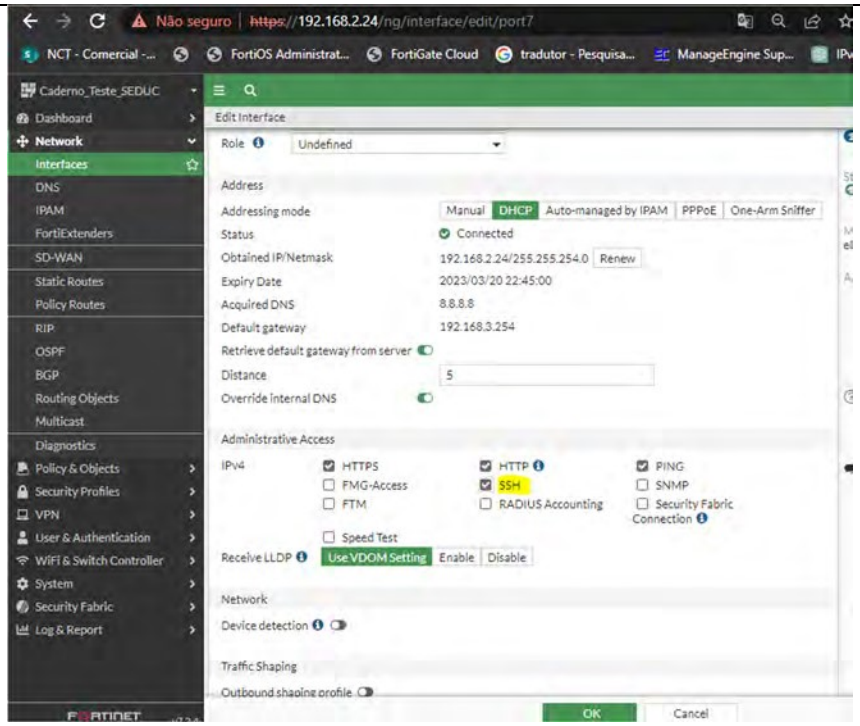
TESTE OK

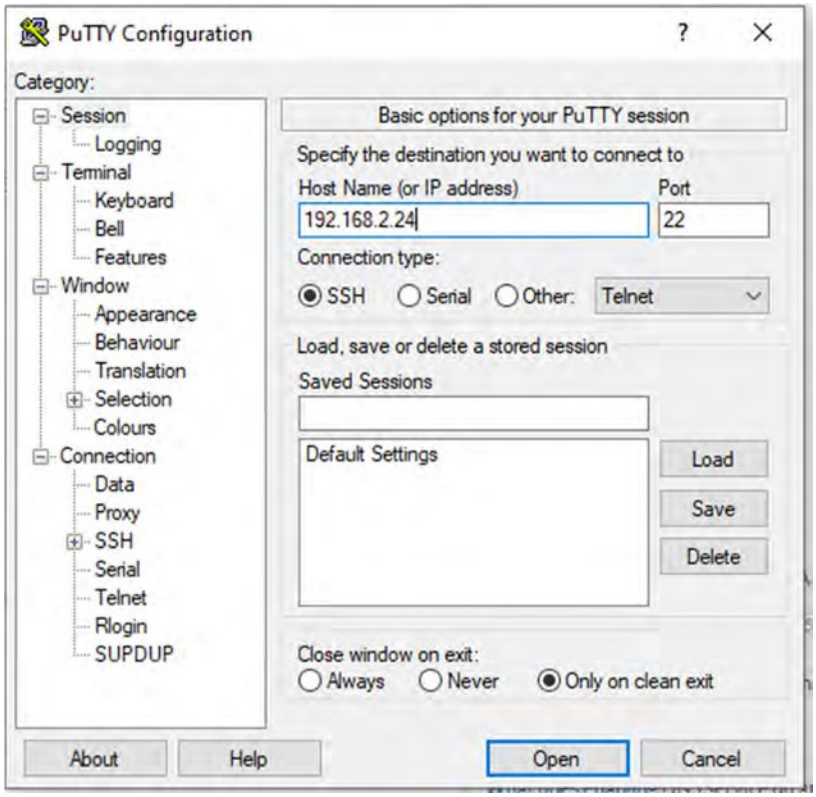


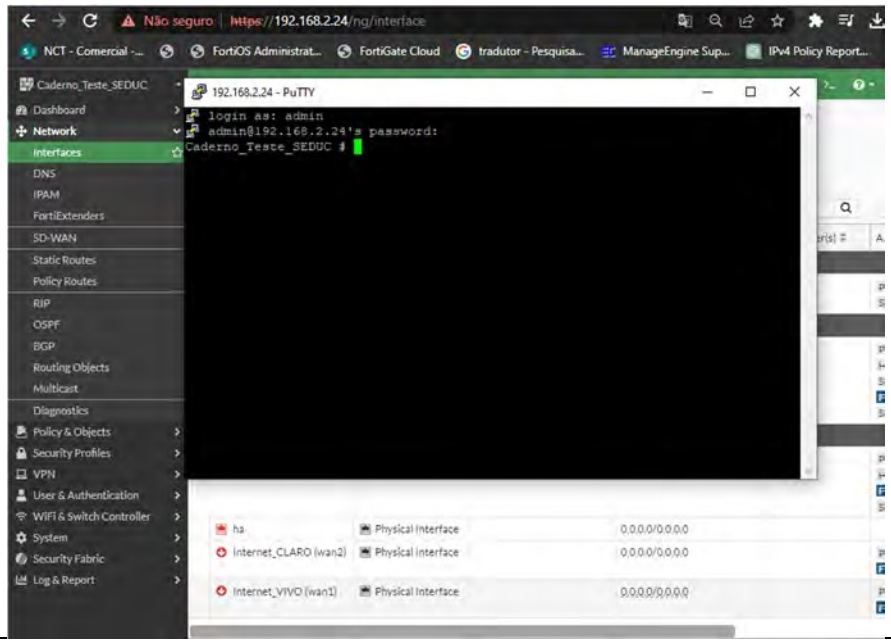
Comentário	

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

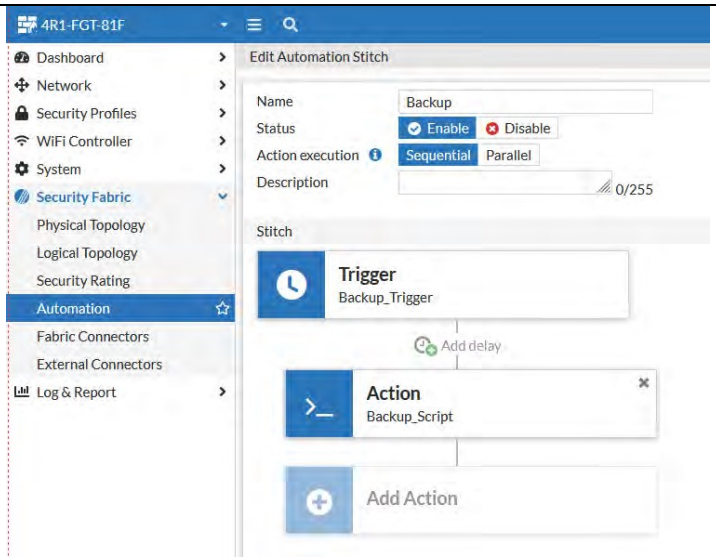
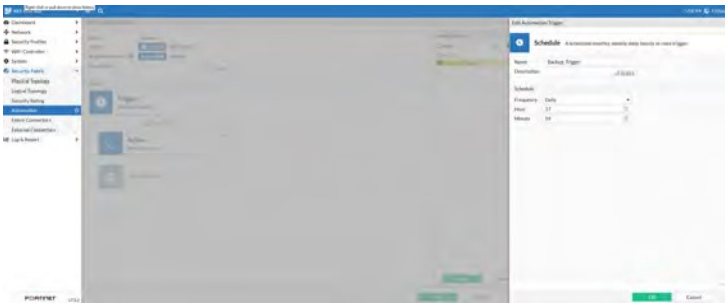
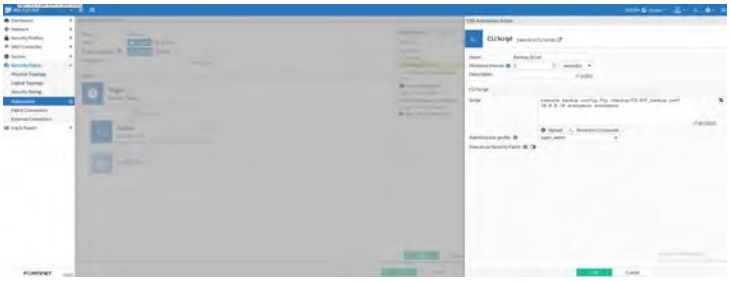
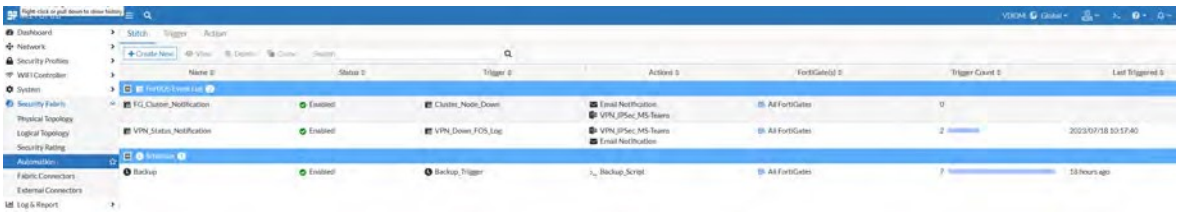
Objetivo do Teste	Verificar se o firewall é capaz de implementar interface CLI por meio do protocolo SSH porta 22 para acesso administrativo.
Configuração do Teste	Liberar acesso administrativo seguro SSH na interface que deseja fazer o acesso, após liberar o acesso é necessário utilizar alguma ferramenta 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	 **TESTE OK**


Não seguro | https://192.168.2.24/ng/interface/edit/port7
Caderno_Teste_SEDUC
Dashboard
Network
Interfaces
DNS
IPAM
FortiExtenders
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Diagnostics
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi & Switch Controller
System
Security Fabric
Log & Report
Edit Interface
Role
Undefined
Address
Addressing mode
Manual
DHCP
Auto-managed by IPAM
PPPoE
One-Arm Sniffer
Status
Connected
Obtained IP/Netmask
192.168.2.24/255.255.254.0
Renew
Expiry Date
2023/03/20 22:45:00
Acquired DNS
8.8.8.8
Default gateway
192.168.3.254
Retrieve default gateway from server
Distance
5
Override Internal DNS
Administrative Access
IPv4
HTTPS
HTTP
PING
FMG-Access
SSH
SNMP
FTM
RADIUS Accounting
Security Fabric Connection
Speed Test
Receive LLDP
Use VDOM Setting
Enable
Disable
Network
Device detection
Traffic Shaping
Outbound shaping profile
OK
Cancel

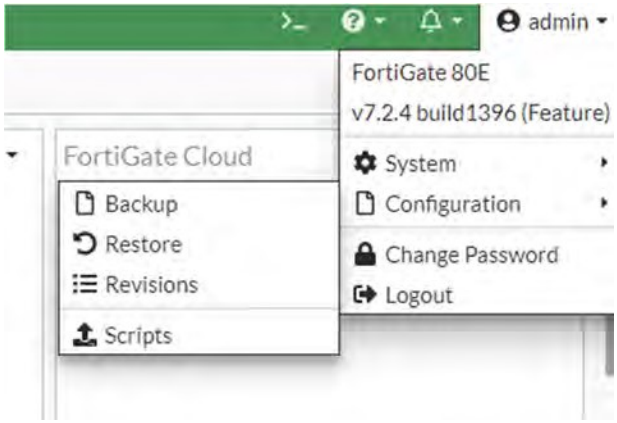

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
192.168.2.24
22
Connection type:
SSH
Serial
Other:
Telnet
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel

	
Comentário	

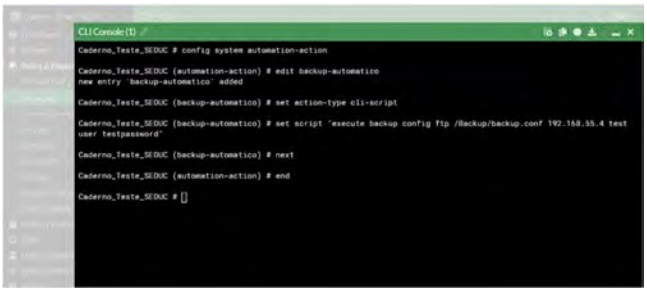
Item de Teste - 5.3.1.9	Deve oferecer as funcionalidades de backup/restore e deve permitir ao administrador agendar backups da configuração em determinado dia e hora;
Objetivo do Teste	Verificar se o FortiGate é capaz de realizar backup/restore e se é possível realizar de forma agendada.
Configuração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

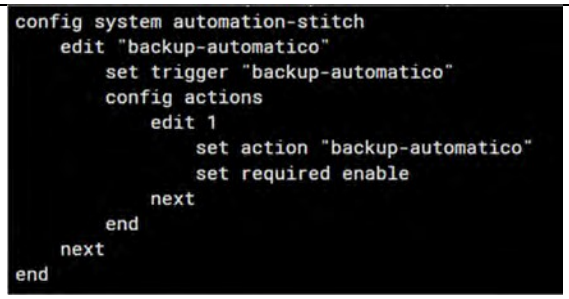
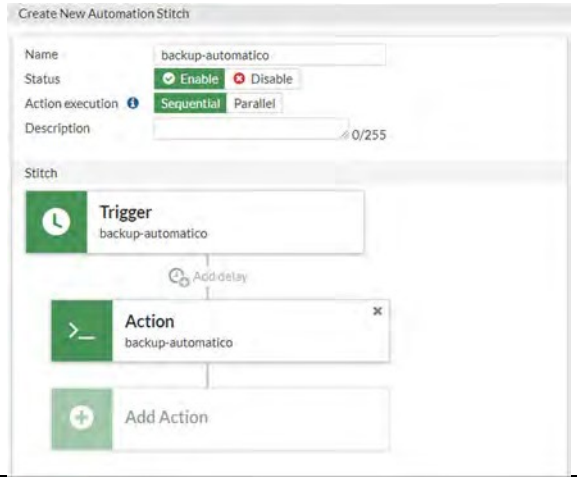
Evidências	   

TESTE OK

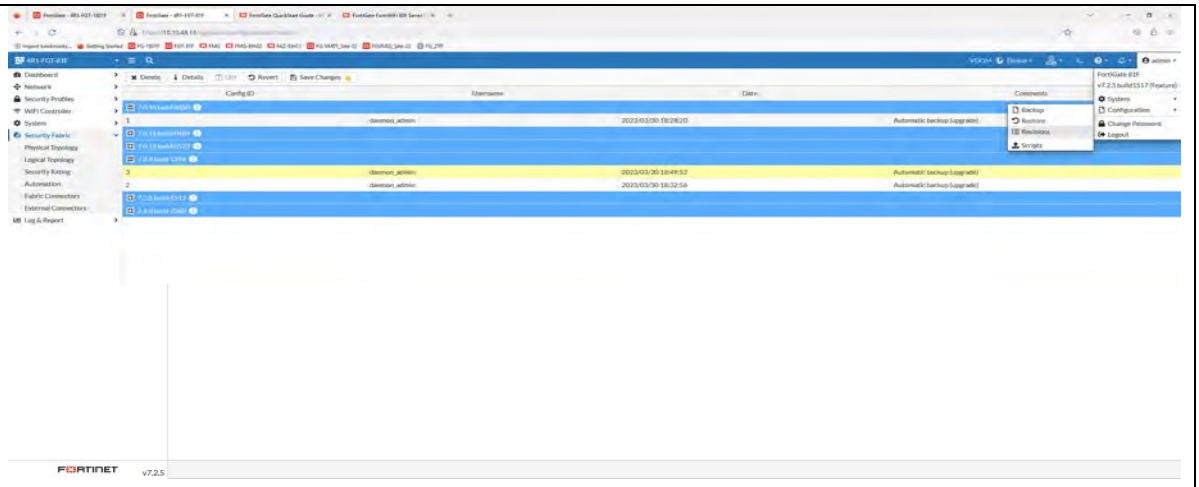


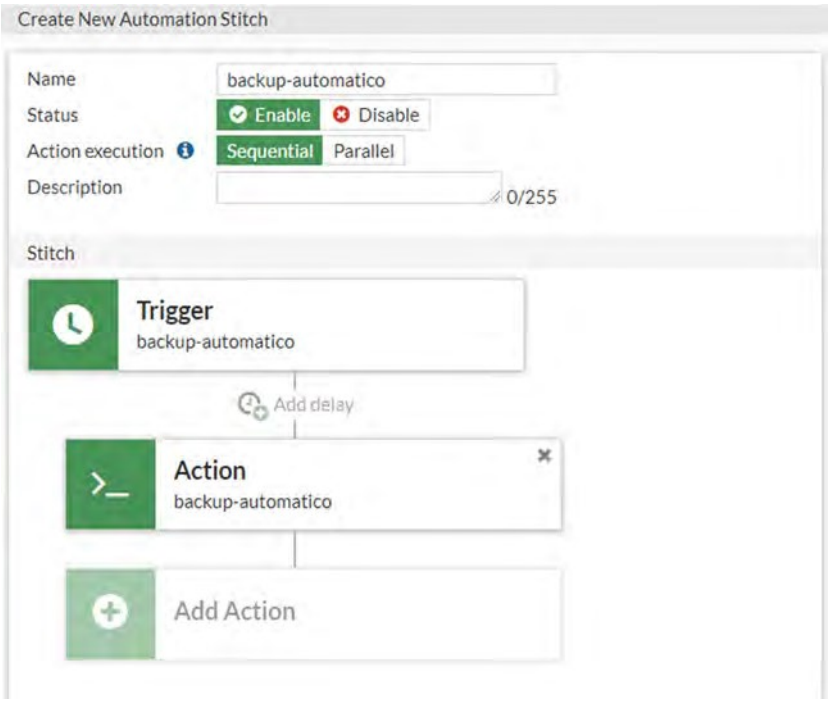

```
FortiGate-80E (automation-trigger) # end
FortiGate-80E # config system automation-trigger
FortiGate-80E (automation-trigger) # edit backup-automatico
FortiGate-80E (backup-automatico) # set trigger-type scheduled
FortiGate-80E (backup-automatico) # set trigger-frequency daily
FortiGate-80E (backup-automatico)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

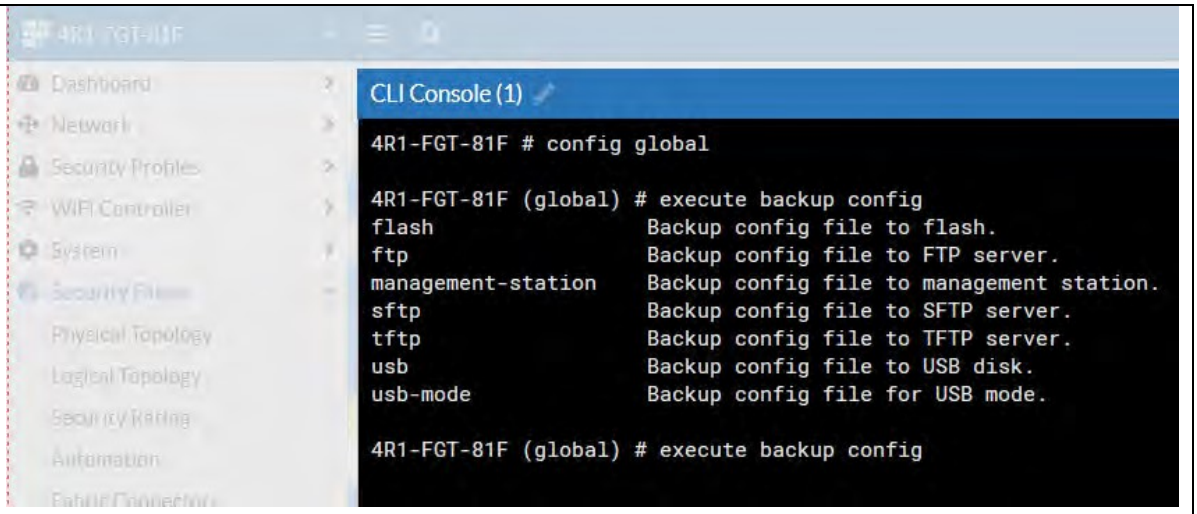


	 
Comentário	https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-send-automated-backups-of-the-configuration/ta-p/198364

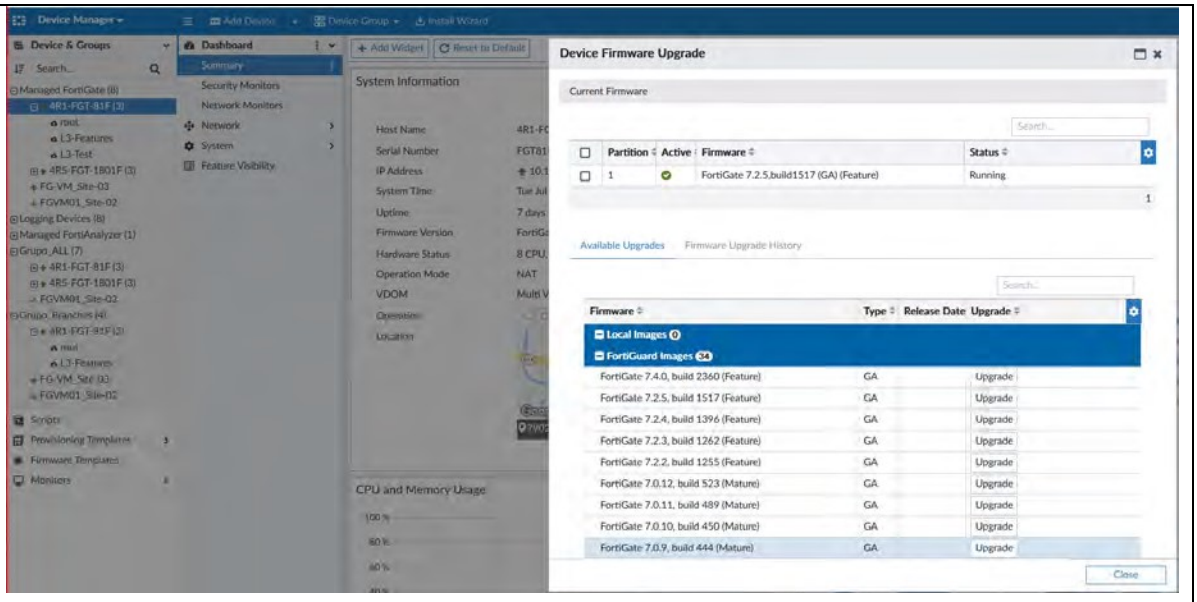
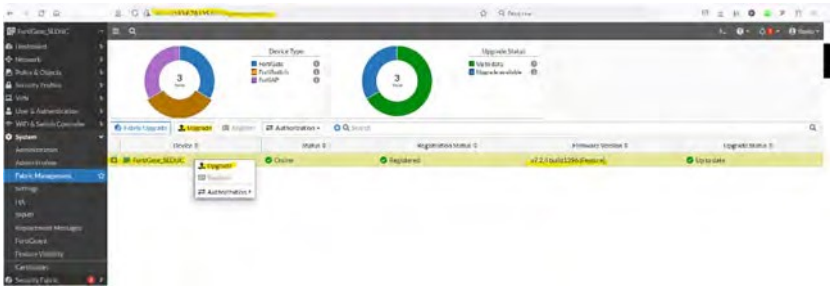
Item de Teste - 5.3.1.10	A solução de permitir armazenar os backups localmente, bem como transferi-los para um servidor remoto;
Objetivo do Teste	Demostrar capacidade de realizar backup de configurações de forma local (no FortiGate) e de forma remota.
Configuração do Teste	Demonstrar base de regras do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



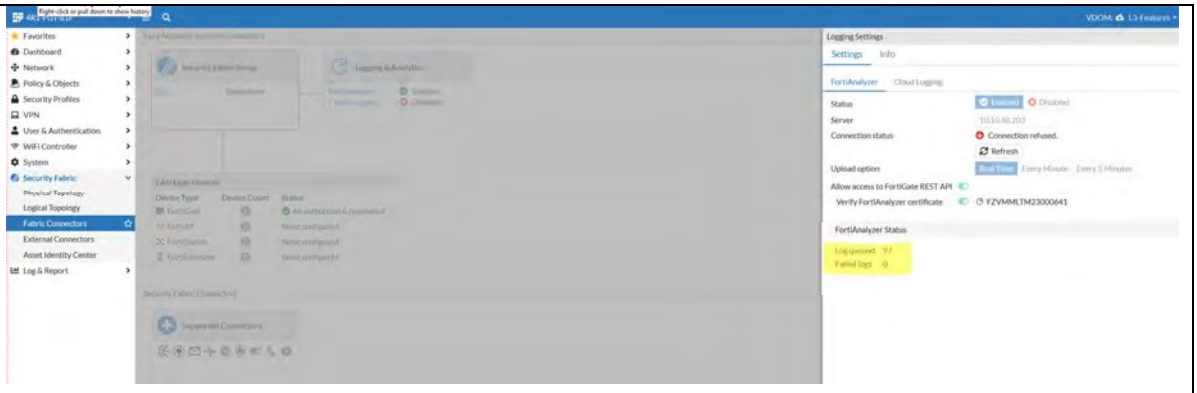
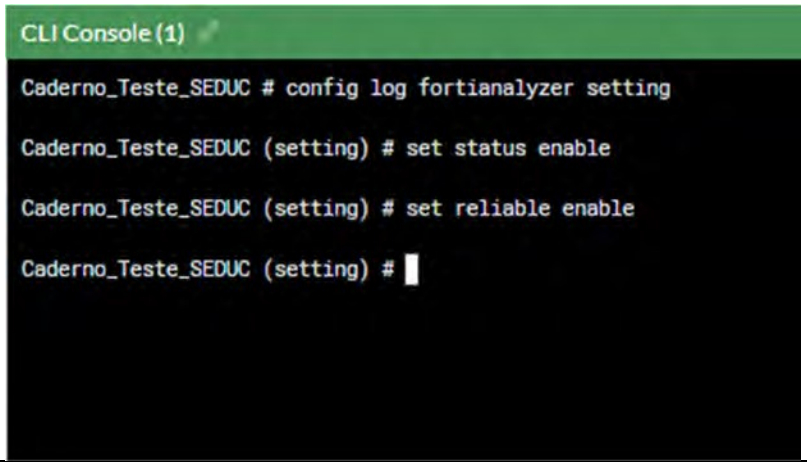

Create New Automation Stitch
Name
backup-automatico
Status
Enable
Disable
Action execution
Sequential
Parallel
Description
0/255
Stitch
Trigger
backup-automatico
Add delay
Action
backup-automatico
Add Action

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

Item de Teste - 5.3.1.11	Habilidade de realizar upgrade remotamente;
Objetivo do Teste	Demostrar capacidade de realizar upgrade de firmware de forma remota.
Configuração do Teste	Demonstrar base de regras do FortiGate.
Procedimento do Teste	Acessar remotamente o equipamento, através de VPN ou de acesso diretamente na interface externa do equipamento e executar o upgrade, acesso ao equipamento demonstrado no item 5.3.1.4 e 5.3.1.6
Evidências	

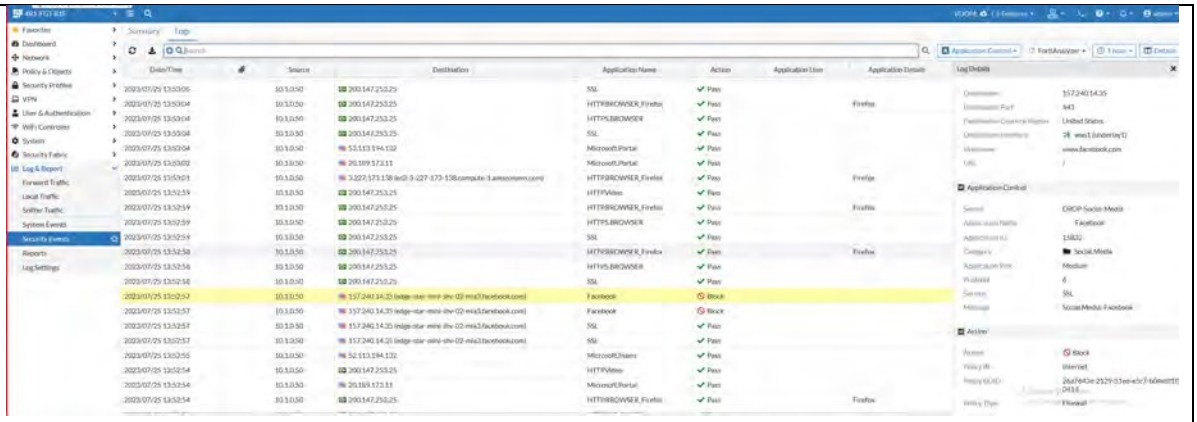
	 **TESTE OK** O processo de atualização pode acontecer de diversas formas, umas delas é acessando a console gráfica do equipamento pelo IP de uma interface, através do protocolo seguro HTTPS, via CLI com SSH, ou por meio de uma VPN executando o mesmo procedimento. 
Comentário	Fonte: https://docs.fortinet.com/document/FortiGate/7.2.3/administration-guide/596131

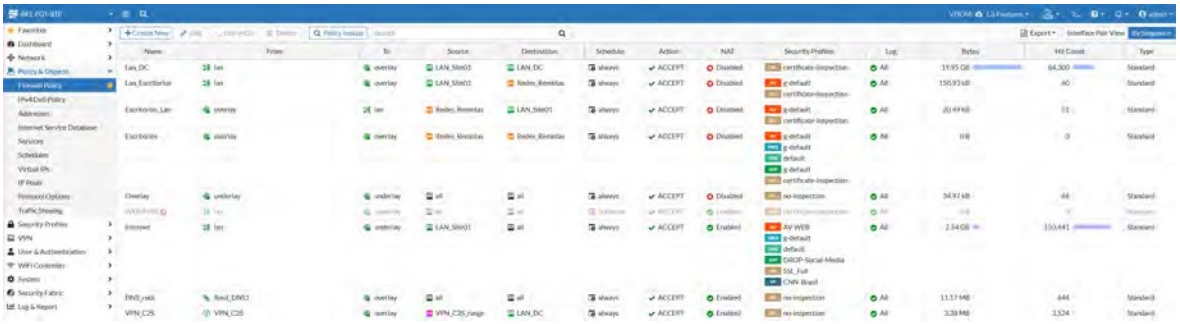
Item de Teste - 5.3.1.14	A solução deve permitir que em caso de falha da comunicação entre o appliance de segurança e a solução de armazenamento de logs seja possível a retenção temporária dos logs localmente no appliance de segurança;
Objetivo do Teste	Verificar se a solução é capaz de armazenar logs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

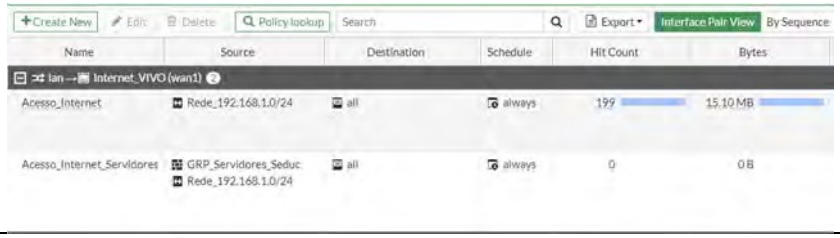
Evidências	 **TESTE OK** Tal funcionalidade habilita a função de armazenamento em cache dos logs caso aconteça a perda de comunicação com o FortiAnalyzer, assim criando uma fila de logs a serem enviados para o FAZ quando a comunicação for restabelecida. 
Comentário	https://docs.fortinet.com/document/FortiGate/7.2.0/new-features/942202/improve-fortianalyzer-log-caching

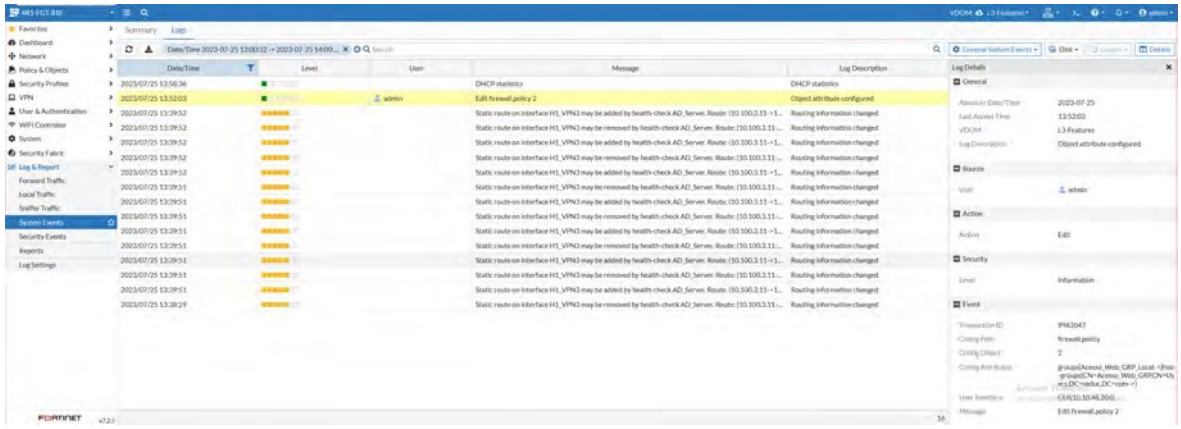
5.3.2 POLÍTICAS DE FIREWALL

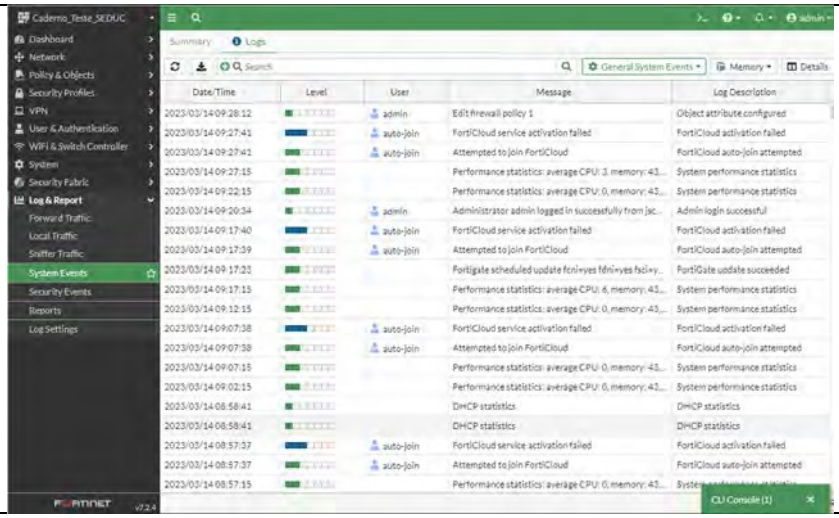
Item de Teste - 5.3.2.18	Deve inspecionar e bloquear os dados operando como default gateway das redes protegidas e controlar o tráfego em nível de aplicações;
Objetivo do Teste	Demonstrar base de regras do FortiGate
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Demonstrar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

	 **TESTE OK**
Comentário	

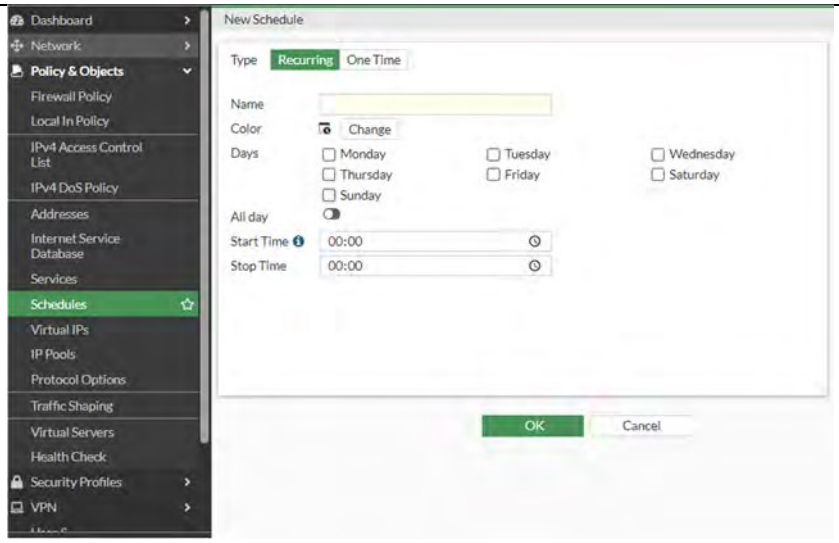
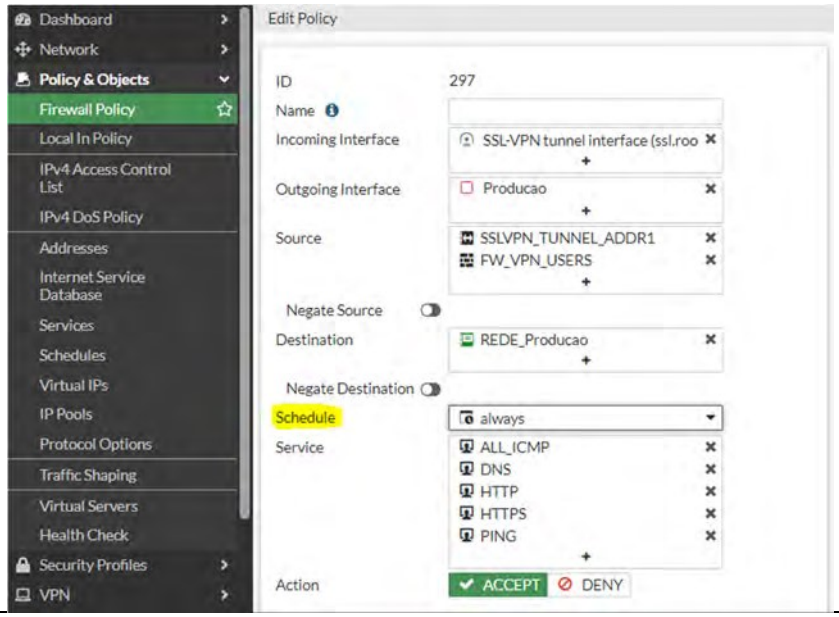
Item de Teste - 5.3.2.20	A solução de Firewall, deve ser capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização;
Objetivo do Teste	Verificar se a solução de firewall é capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização.
Configuração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

	
Comentário	

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

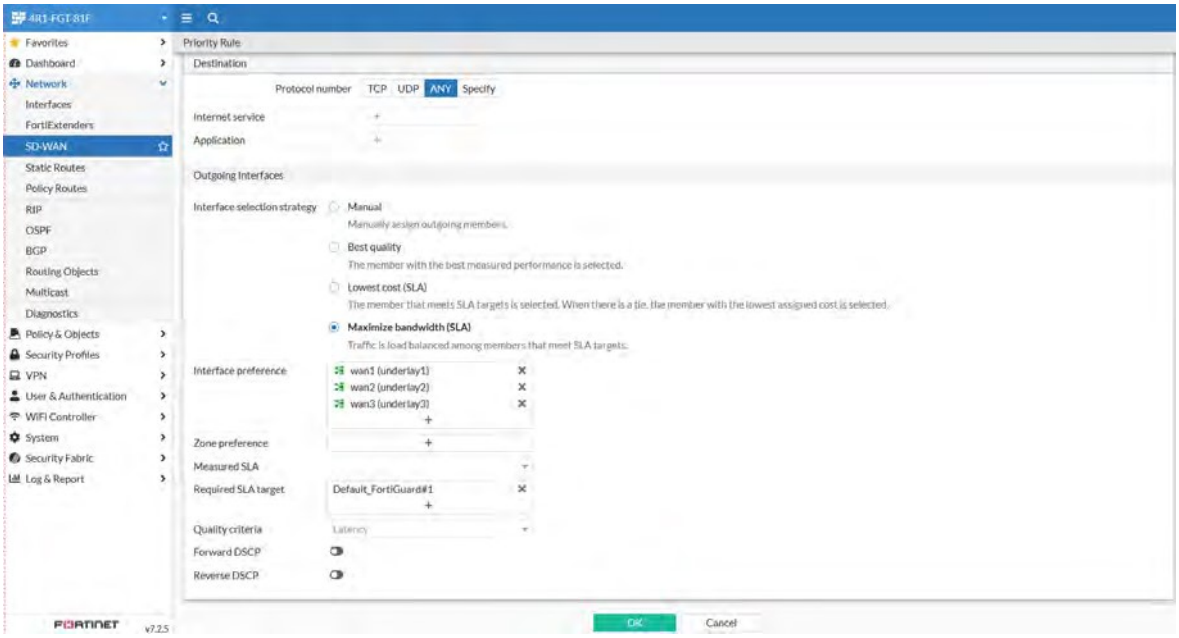
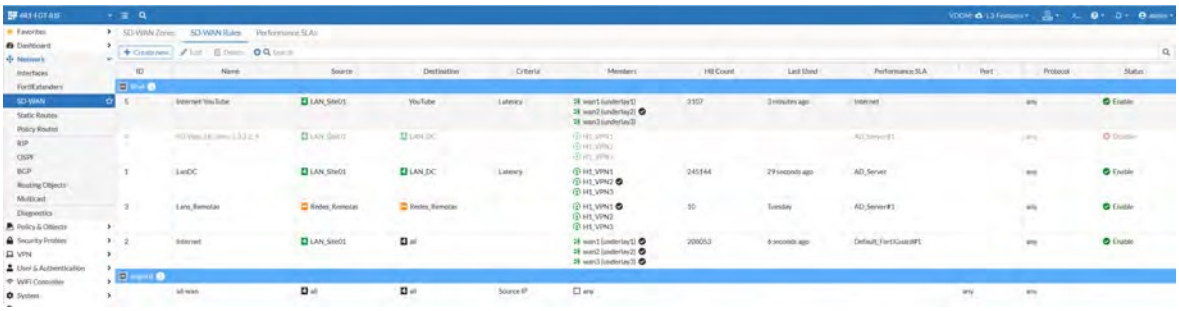
	
Comentário	

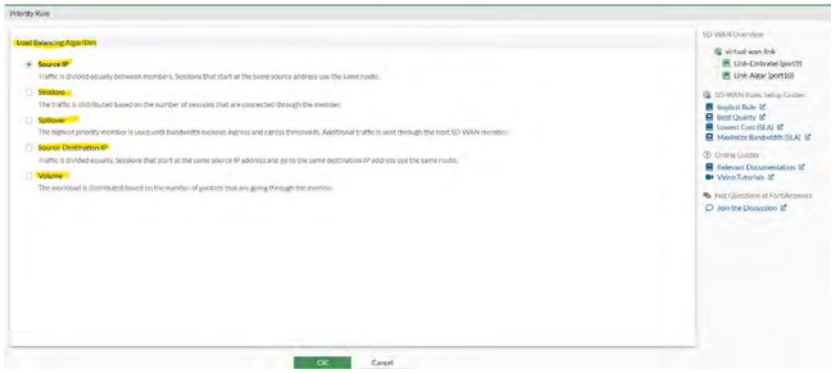
Item de Teste - 5.3.2.23	Deverá permitir a ativação/desativação de regras de forma programada conforme a data/hora;
Objetivo do Teste	Validar se o FortiGate permite a ativação e desativação de regras de forma programada.
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	1 - Navegando por **Policy & Objects** > **Firewall Policy** > **Schedules** é possível criar um período que a regra irá funcionar. 2 - Navegando por **Policy & Objects** > **Firewall Policy** > é possível adicionar o objeto de Schedule criado anteriormente em qualquer uma das políticas existentes, basta selecionar o objeto de Schedule dentro do respectivo campo dentro da política, no campo “Schedule”:
Evidências	 **TESTE OK** Criação do objeto de tempo “Schedule”

	 Aplicação do objeto “Schedule” dentro de uma política de firewall. 
Comentário	

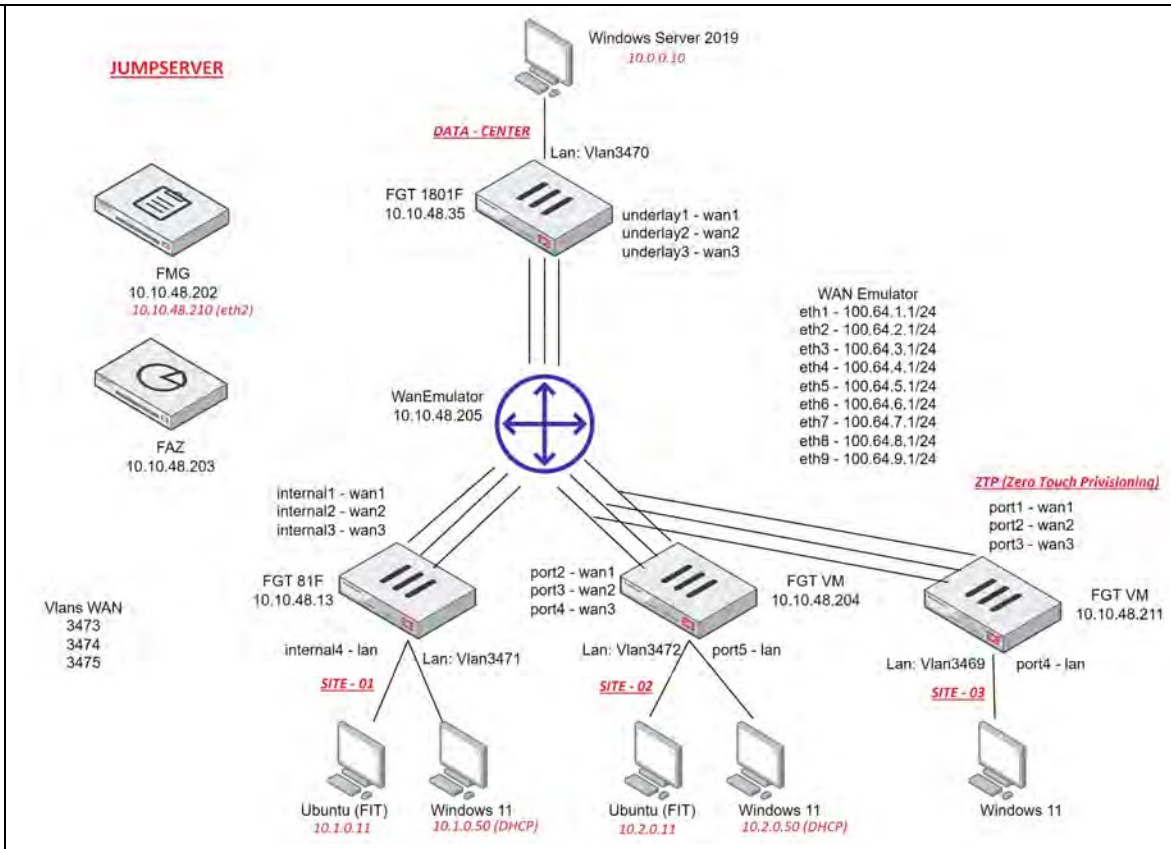
5.3.3 SDWAN

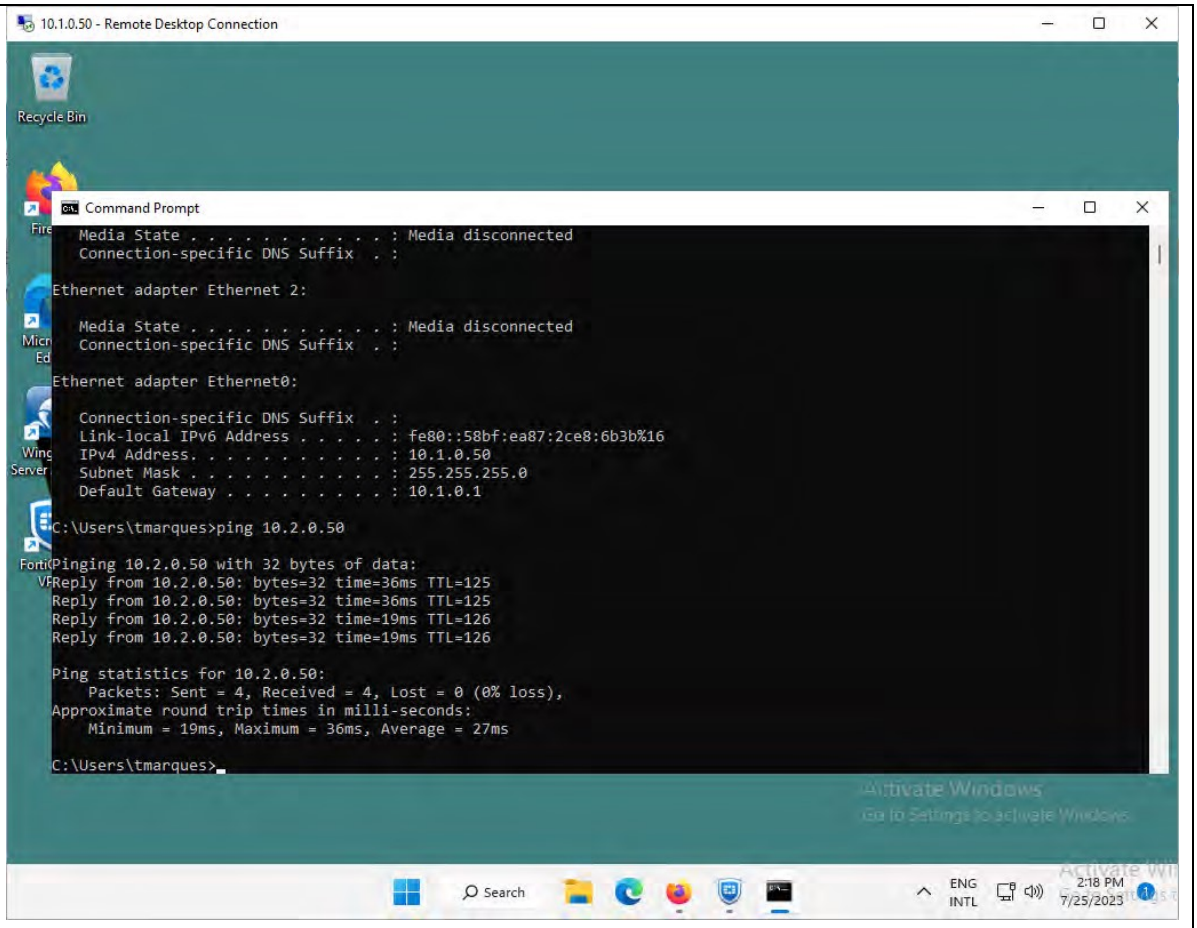
Item de Teste - 5.3.3.2	A solução deverá ser capaz de balancear cargas entre dois links distintos;
Objetivo do Teste	Demostrar capacidade de balancear o tráfego de 2 links distintos através de SDWAN
Configuração do Teste	Demonstrar base de regras do FortiGate

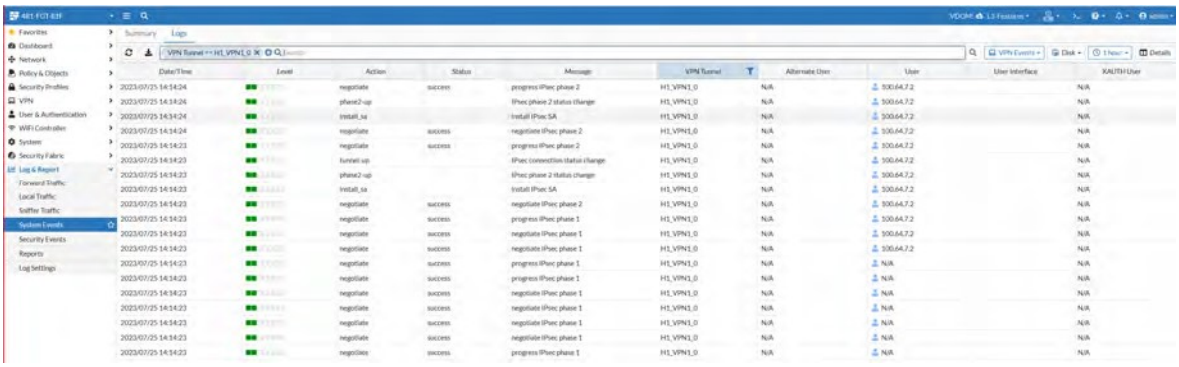
Procedimento do Teste	Navegando por **Network** > **SDWAN** > **Create new member** é possível acrescentar links para serem balanceados pelo SDWAN Navegando por **Network** > **SDWAN** > **Performace SLA** é definindo o algoritmo mais adequado para o balanceamento; Navegando por **Network** > **SDWAN** > **SDWAN Rules** é possível criar regrar para enquadrar o algoritmo de balanceamento.
Evidências	  **TESTE OK** 1- Criação dos membros (links) que vão participar do SDWAN 

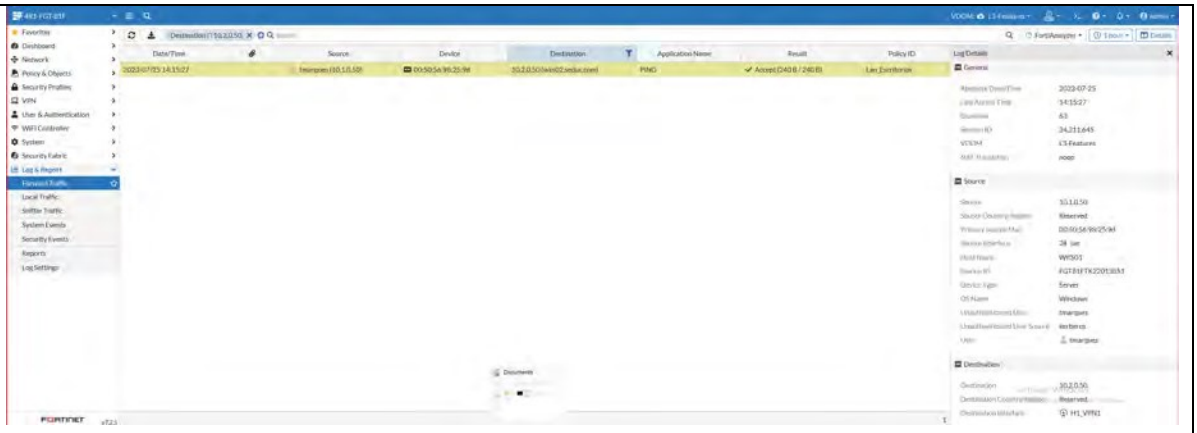
	2- Definindo o algoritmo mais adequado para o balanceamento;  3- Criando rule de SDWAN para permitir que os membros (links) sejam balanceados através do algoritmo selecionado. 
Comentário	Fonte: https://docs.fortinet.com/document/FortiGate/7.2.3/administration-guide/683285

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

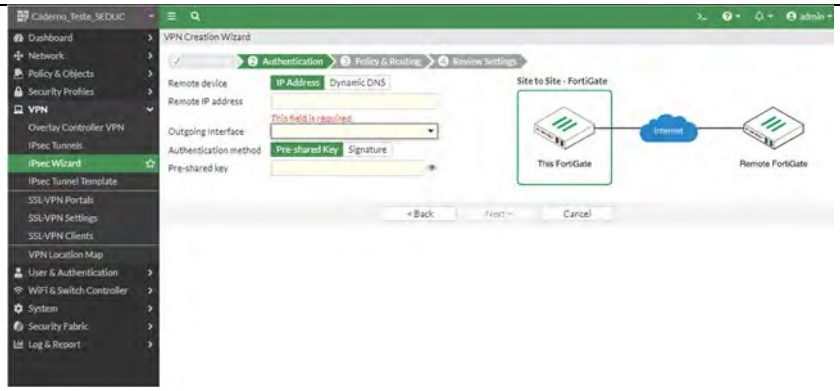

JUMPSERVER
Windows Server 2019
10.0.0.10
DATA - CENTER
Lan: Vlan3470
FGT 1801F
10.10.48.35
underlay1 - wan1
underlay2 - wan2
underlay3 - wan3
FMG
10.10.48.202
10.10.48.210 (eth2)
FAZ
10.10.48.203
WAN Emulator
eth1 - 100.64.1.1/24
eth2 - 100.64.2.1/24
eth3 - 100.64.3.1/24
eth4 - 100.64.4.1/24
eth5 - 100.64.5.1/24
eth6 - 100.64.6.1/24
eth7 - 100.64.7.1/24
eth8 - 100.64.8.1/24
eth9 - 100.64.9.1/24
WanEmulator
10.10.48.205
ZTP (Zero Touch Privisioning)
port1 - wan1
port2 - wan2
port3 - wan3
internal1 - wan1
internal2 - wan2
internal3 - wan3
Vlans WAN
3473
3474
3475
FGT 81F
10.10.48.13
port2 - wan1
port3 - wan2
port4 - wan3
FGT VM
10.10.48.204
FGT VM
10.10.48.211
internal4 - lan
Lan: Vlan3471
SITE - 01
Lan: Vlan3472
port5 - lan
SITE - 02
Lan: Vlan3469
port4 - lan
SITE - 03
Ubuntu (FIT)
10.1.0.11
Windows 11
10.1.0.50 (DHCP)
Ubuntu (FIT)
10.2.0.11
Windows 11
10.2.0.50 (DHCP)
Windows 11

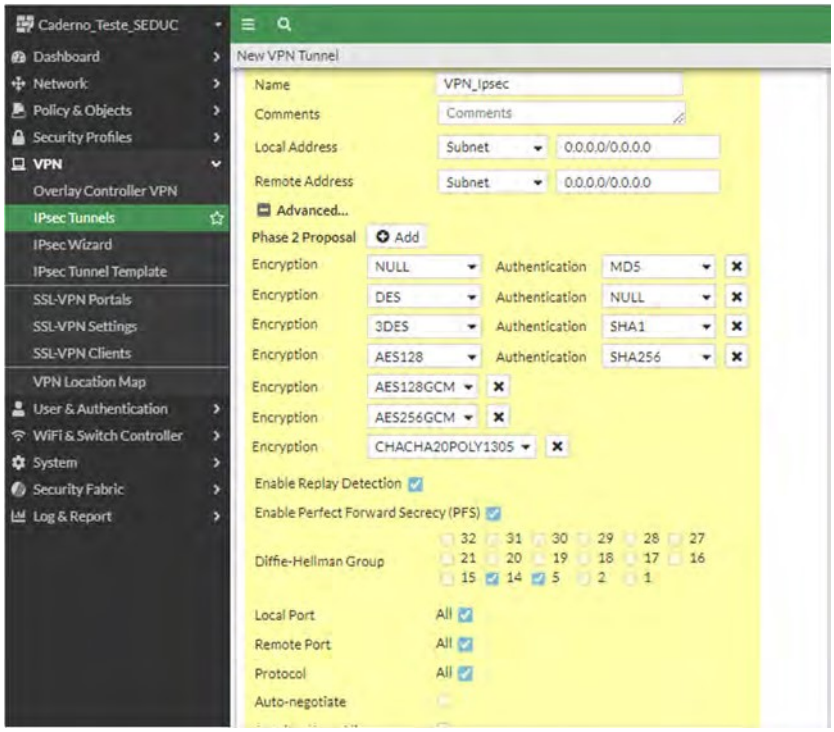

10.1.0.50 - Remote Desktop Connection
Recycle Bin
Command Prompt
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter Ethernet 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::58bf:ea87:2ce8:6b3b%16
IPv4 Address. . . . . : 10.1.0.50
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.1.0.1
C:\Users\tmarques>ping 10.2.0.50
Pinging 10.2.0.50 with 32 bytes of data:
Reply from 10.2.0.50: bytes=32 time=36ms TTL=125
Reply from 10.2.0.50: bytes=32 time=36ms TTL=125
Reply from 10.2.0.50: bytes=32 time=19ms TTL=126
Reply from 10.2.0.50: bytes=32 time=19ms TTL=126
Ping statistics for 10.2.0.50:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 19ms, Maximum = 36ms, Average = 27ms
C:\Users\tmarques>
Activate Windows
Search
ENG
INTL
2:18 PM
7/25/2023

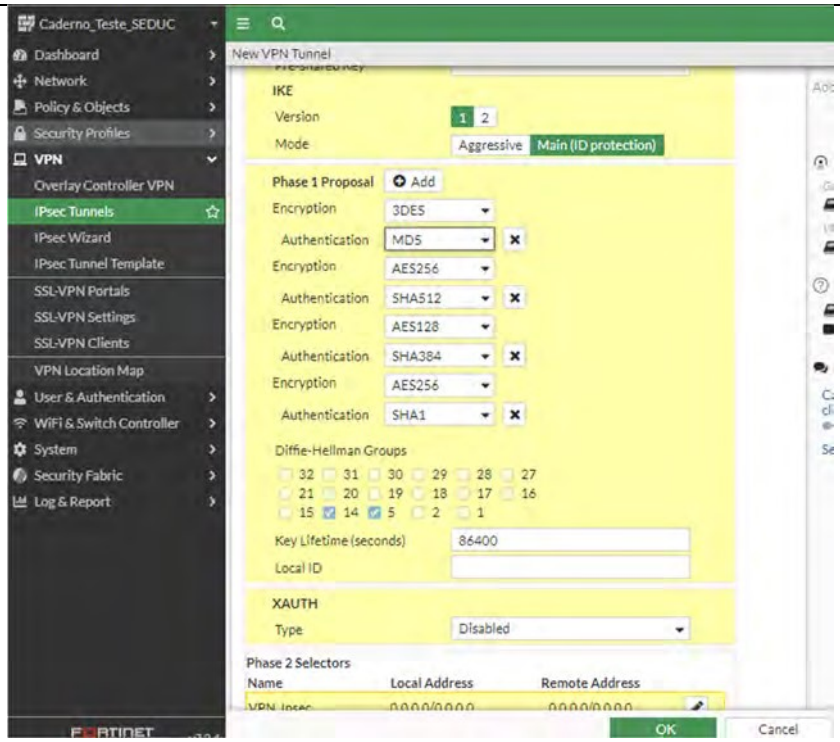




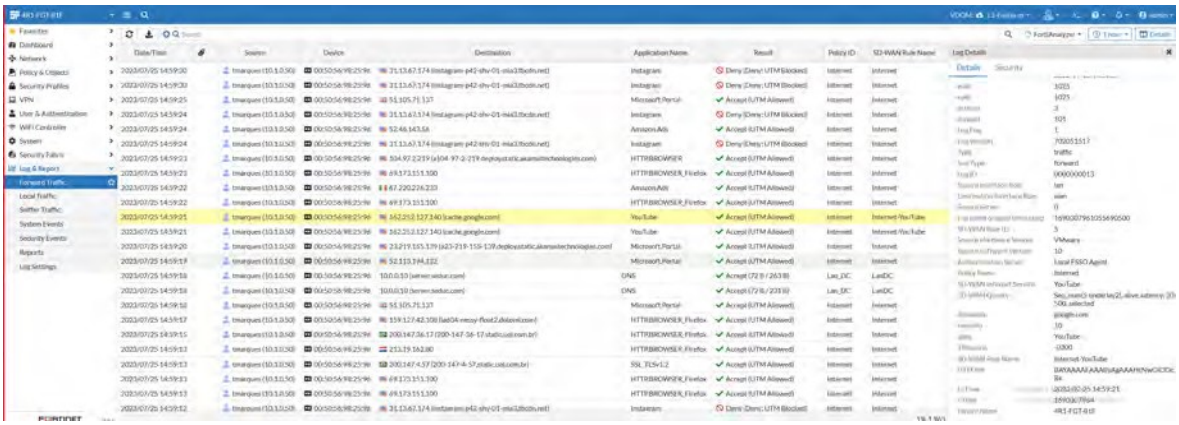
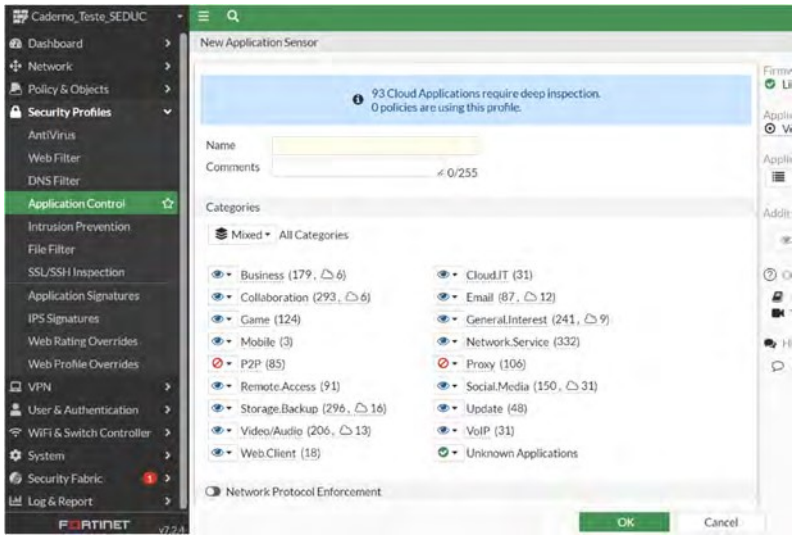
TESTE OK

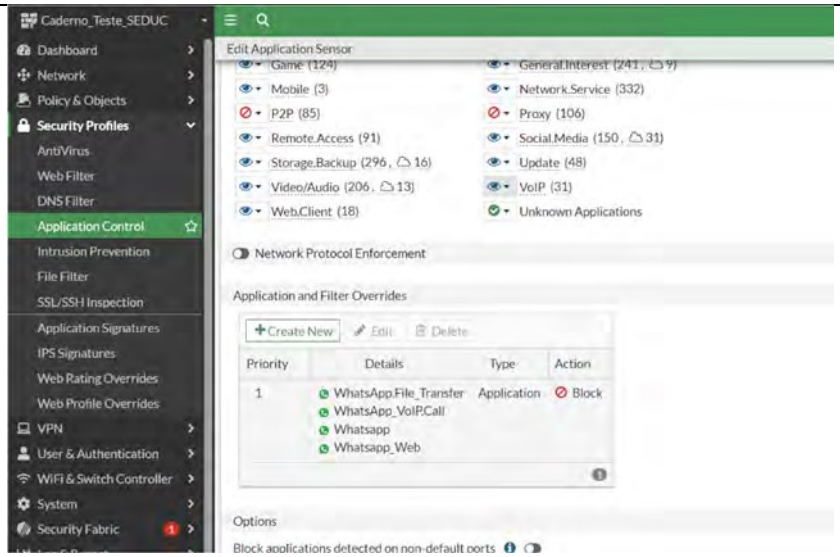

Caderno_Teste_SEDUC
Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication
WiFi & Switch Controller
System
Security Fabric
Log & Report
VPN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


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

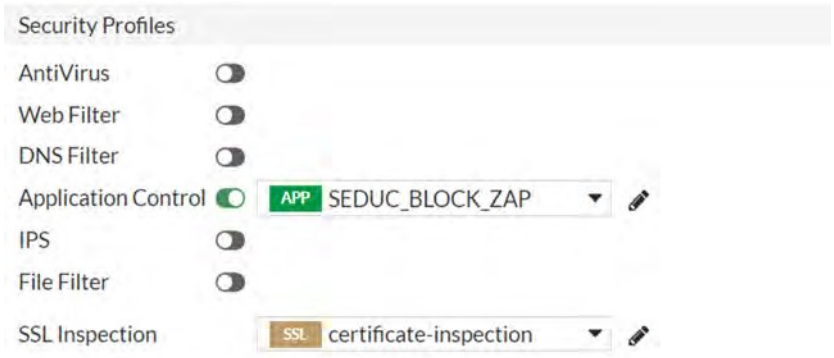
	 ADVPN Auto-Discovery VPN (ADVPN) allows the central hub to dynamically inform spokes about a better path for traffic between two spokes. The following topics provide instructions on configuring ADVPN: • IPsec VPN wizard hub-and-spoke ADVPN support • ADVPN with BGP as the routing protocol • ADVPN with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

Item de Teste - 5.3.3.5	Deverá implementar controle de tráfego por aplicação;
Objetivo do Teste	Validar se o FortiGate é capaz de realizar controle de tráfego por aplicação
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Para realizar o controle de tráfego por aplicação é necessário configurar um Application Control Profile e enquadrar o perfil em alguma regra onde o fluxo tenha como destino a internet;

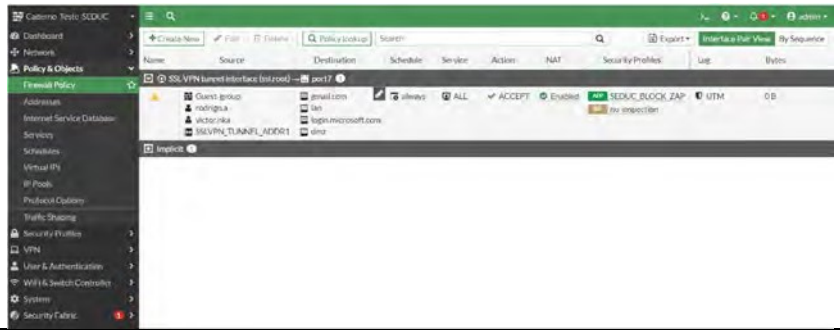
	Navegando por **Security Profile** > **Application Control** > **Create new** é possível criar um novo perfil enquadrando as aplicações que deseja bloquear, monitorar ou aprovar; Navegando por **Policy & Objects** > **Firewall Policy** é possível enquadrar o perfil de Application Control criado para determinar em qual fluxo ocorrera o controle de tráfego por aplicação.
	 **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

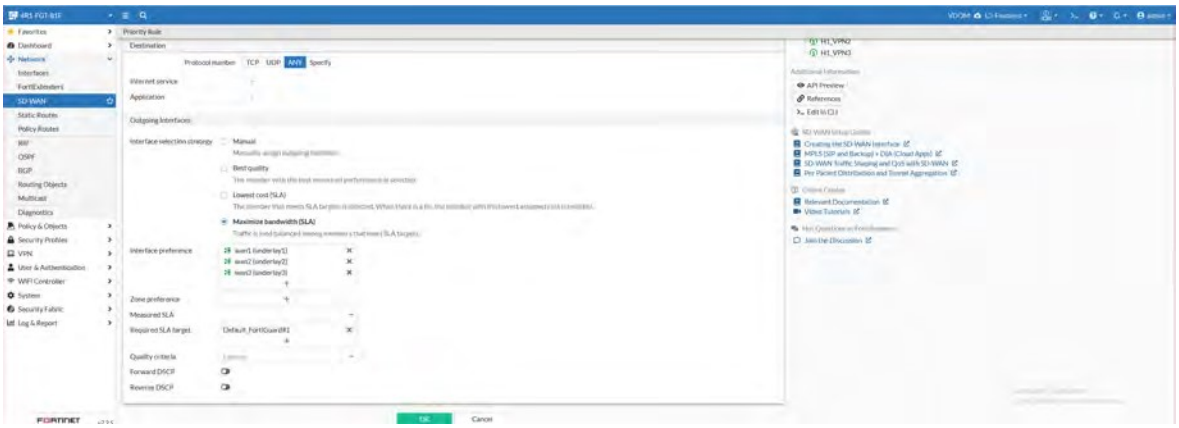
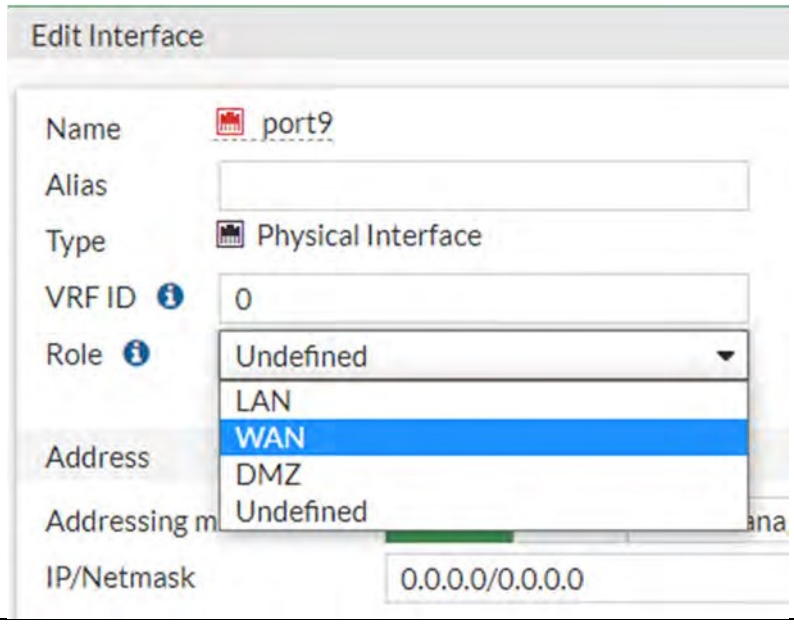


4 – Abaixo o exemplo de como a política fica com o perfil enquadrado

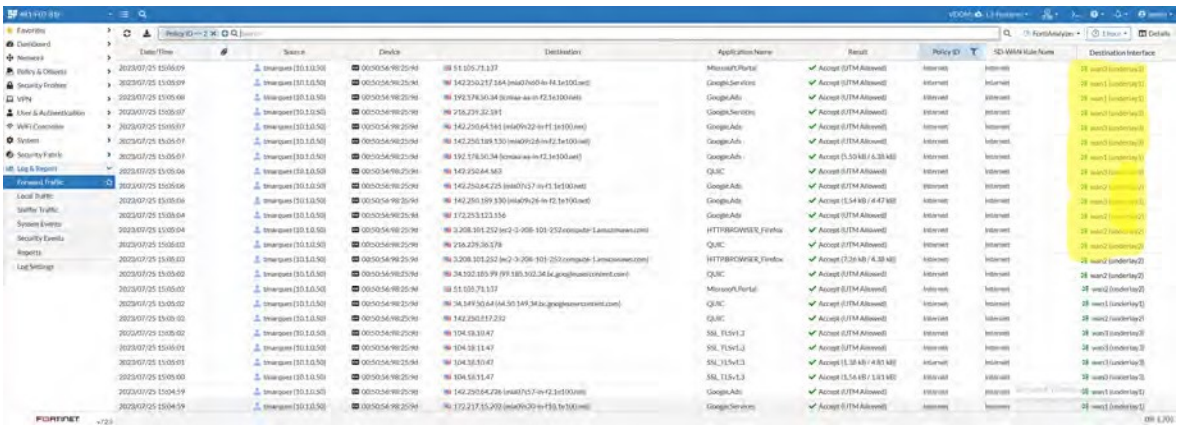


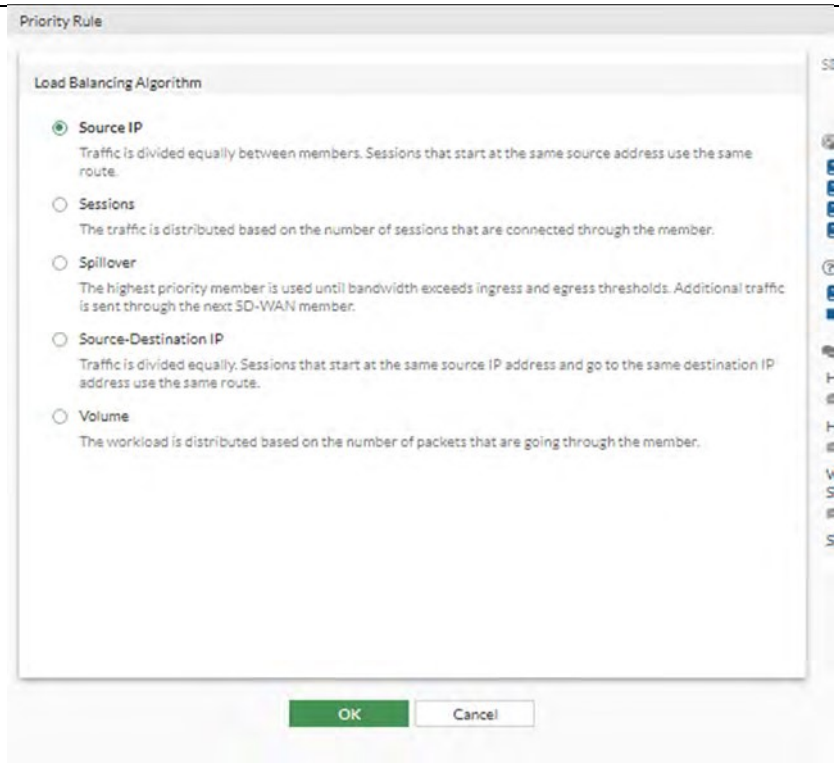
Comentário	

Item de Teste - 5.3.3.6	Deverá suportar, no mínimo, 3 (três) links de WAN;

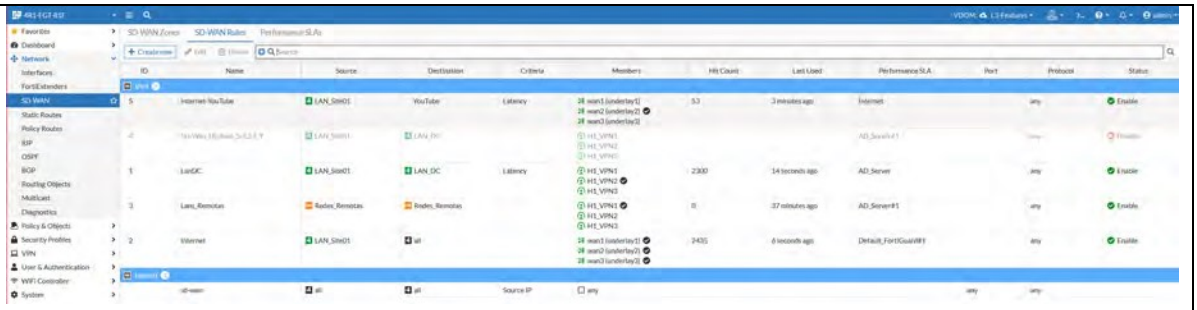
Objetivo do Teste	Demonstrar que a ferramenta possui mais de três links de WAN
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Demonstrar base de regras do FortiGate
Evidências	 **TESTE OK** Qualquer interface no FortiGate pode ser definida como uma interface WAN. 

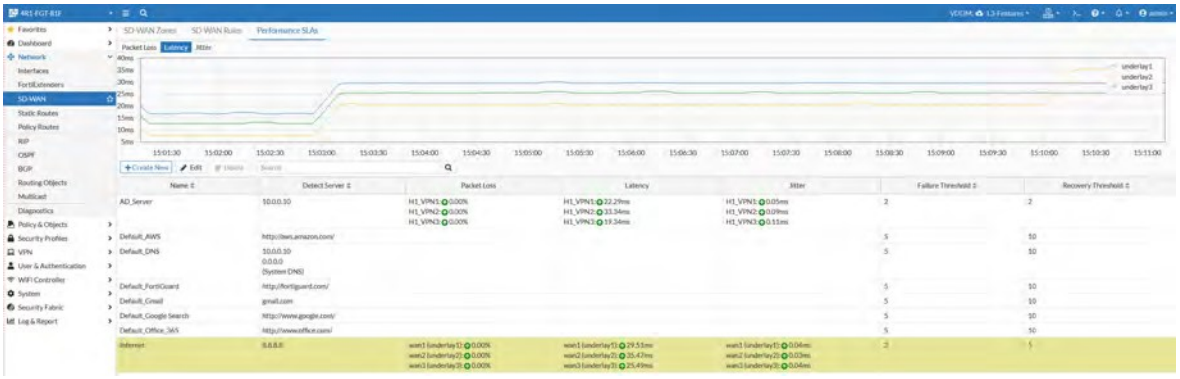
Comentário	

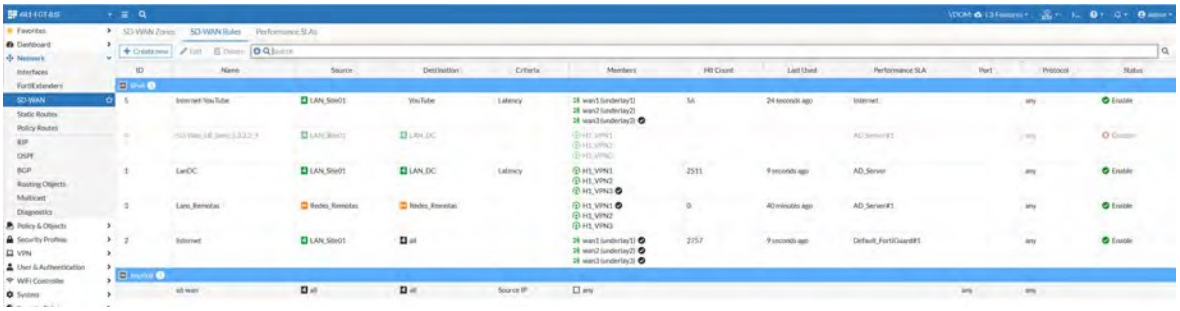
Item de Teste - 5.3.3.9	Distribuição de tráfego com balanceamento de sessão entre os circuitos existentes;
Objetivo do Teste	Criar regra que balanceie o tráfego entres todos os links wan
Configuração do Teste	Demonstrar base de regras do FortiGate
Procedimento do Teste	Demonstrar base de regras do FortiGate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

	
Comentário	

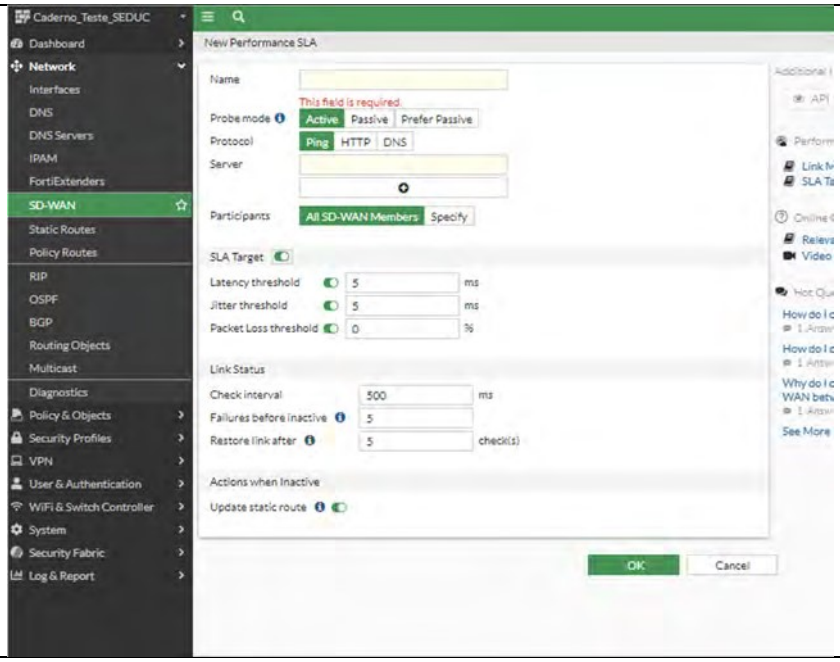
Item de Teste - 5.3.3.10	Distribuição orientada a qualidade, o dispositivo deve validar o melhor caminho disponível e utilizar deste path para manter sessões ativas, caso o melhor caminho entre em degradação por fatores anômalos o dispositivo deverá entender estes fatores e distribuir para os demais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

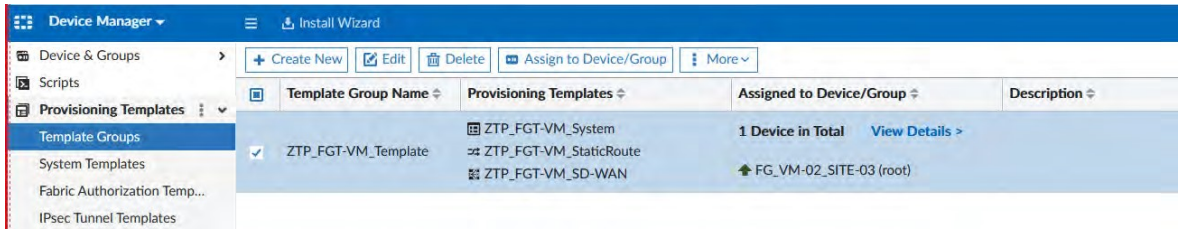


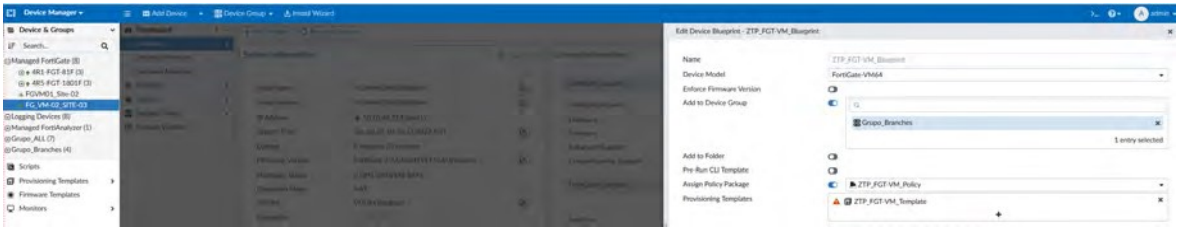




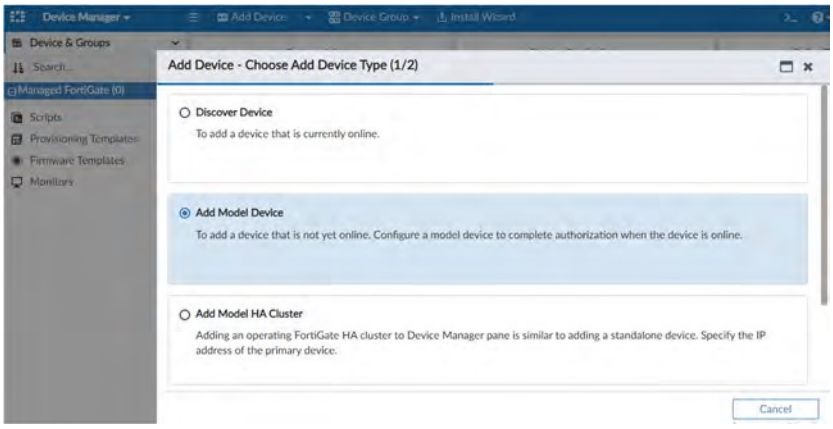
TESTE OK

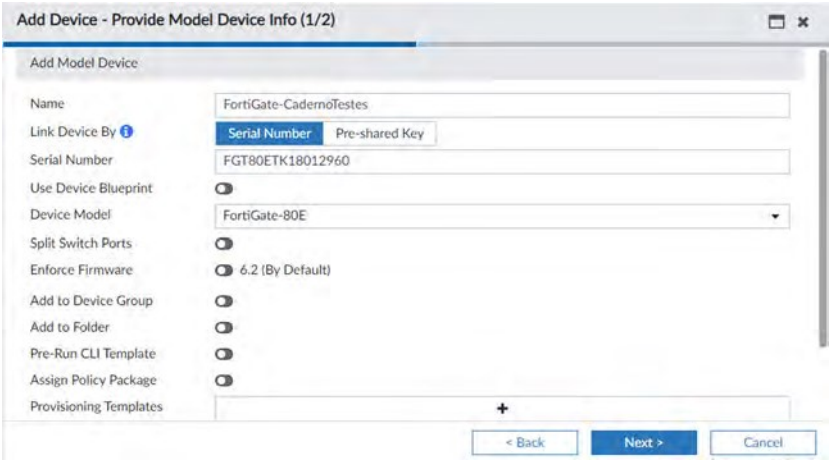
	
Comentário	

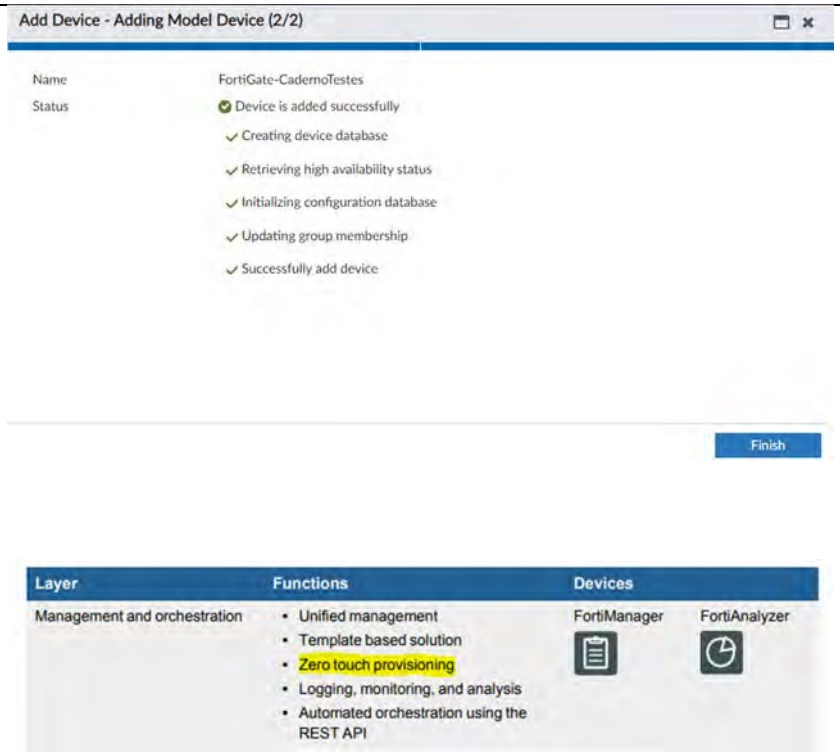
Item de Teste -5.3.3.11	Os dispositivos remotos devem suportar a funcionalidade de ZTP (Zero Touch Provisioning) para que assim, inseridos nas estruturas remotas, possam buscar automaticamente por suas configurações, com o objetivo de facilitar a instalação nas unidades remotas ou a troca de um dispositivo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



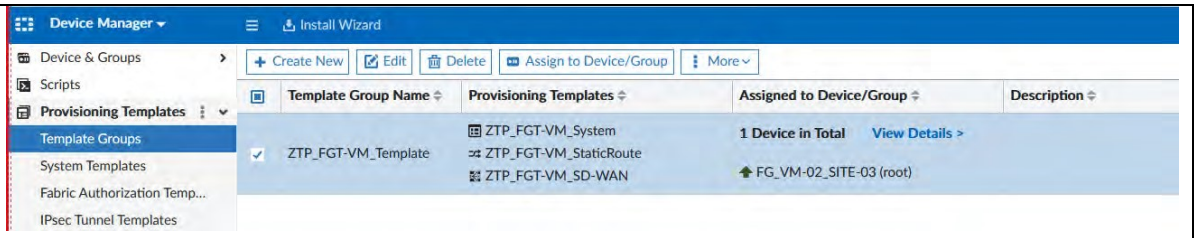
TESTE OK

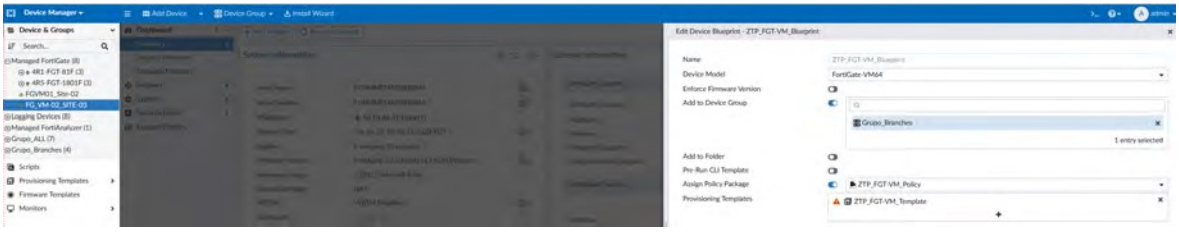

Device Manager
Add Device
Device Group
Install Wizard
Device & Groups
Search...
Managed FortiGate (0)
Scripts
Provisioning Templates
Firmware Templates
Monitors
Add Device - Choose Add Device Type (1/2)
Discover Device
To add a device that is currently online.
Add Model Device
To add a device that is not yet online. Configure a model device to complete authorization when the device is online.
Add Model HA Cluster
Adding an operating FortiGate HA cluster to Device Manager pane is similar to adding a standalone device. Specify the IP address of the primary device.
Cancel


Add Device - Provide Model Device Info (1/2)
Add Model Device
Name
FortiGate-CadernoTestes
Link Device By
Serial Number
Pre-shared Key
Serial Number
FGT80ETK18012960
Use Device Blueprint
Device Model
FortiGate-80E
Split Switch Ports
Enforce Firmware
6.2 (By Default)
Add to Device Group
Add to Folder
Pre-Run CLI Template
Assign Policy Package
Provisioning Templates
< Back
Next >
Cancel

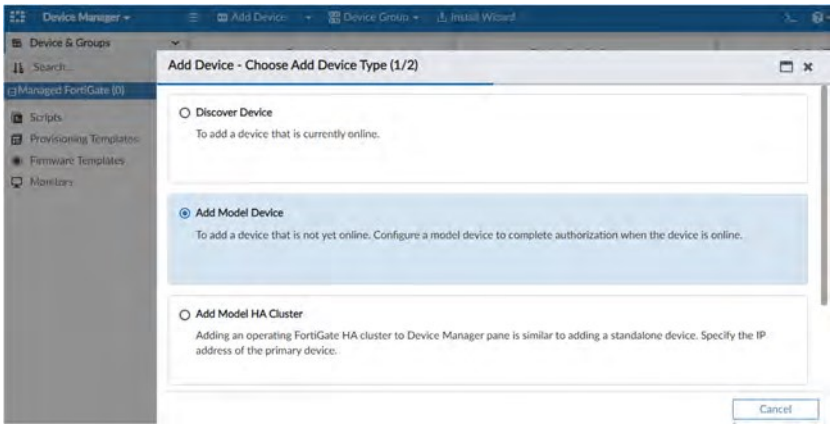
	
Comentário	Fonte: FortiOS-7.2.3-Administration_Guide disponível em https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a06117ca-5fbf-11ed-96f0-fa163e15d75b/FortiOS-7.2.3-Administration_Guide.pdf https://docs.fortinet.com/document/FortiGate/6.2.14/cookbook/861490/zero-touch-provisioning-with-fortimanager

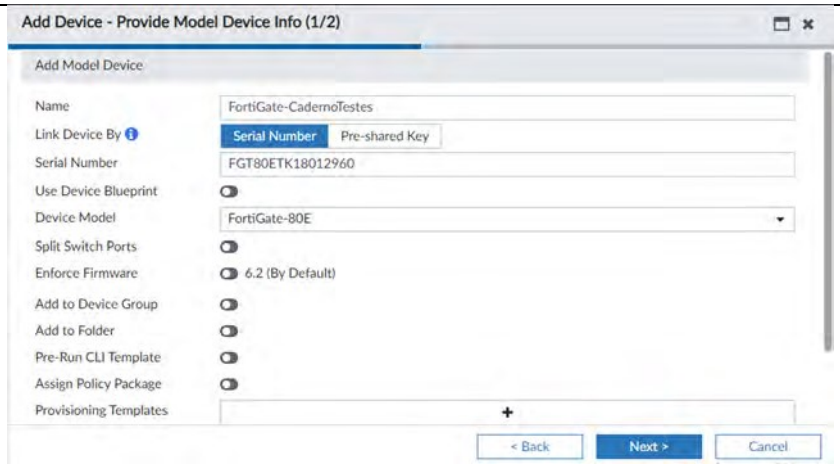
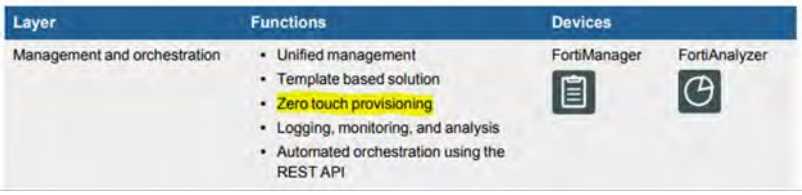
Item de Teste - 5.3.3.12	Gerenciamento centralizado e implantação Zero Touch;
Objetivo do Teste	Mostrar que o equipamento de gerência centralizada com suporte a funcionalidade de implantação ZTP.
Configuração do Teste	Mostrar que os dispositivos remotos suportam a funcionalidade ZTP.
Procedimento do Teste	Para realizar essa configuração basta adicionar um novo dispositivo e colocar as especificações dele, assim ele será cadastrado e quando for ligado buscará automaticamente pelas suas configurações.
Evidências	


Device Manager
Install Wizard
Device & Groups
Scripts
Provisioning Templates
Template Groups
System Templates
Fabric Authorization Temp...
IPsec Tunnel Templates
Create New
Edit
Delete
Assign to Device/Group
More
Template Group Name
Provisioning Templates
Assigned to Device/Group
Description
ZTP_FGT-VM_Template
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)



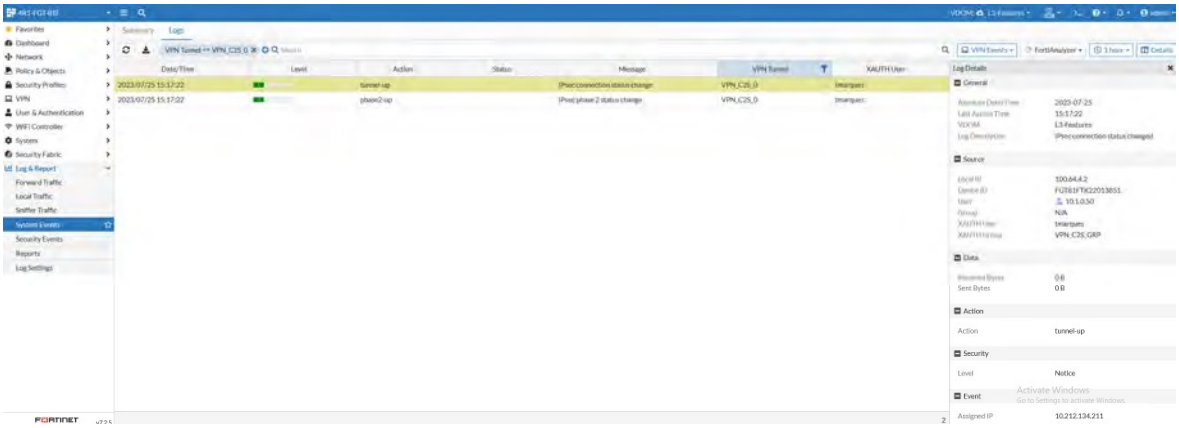
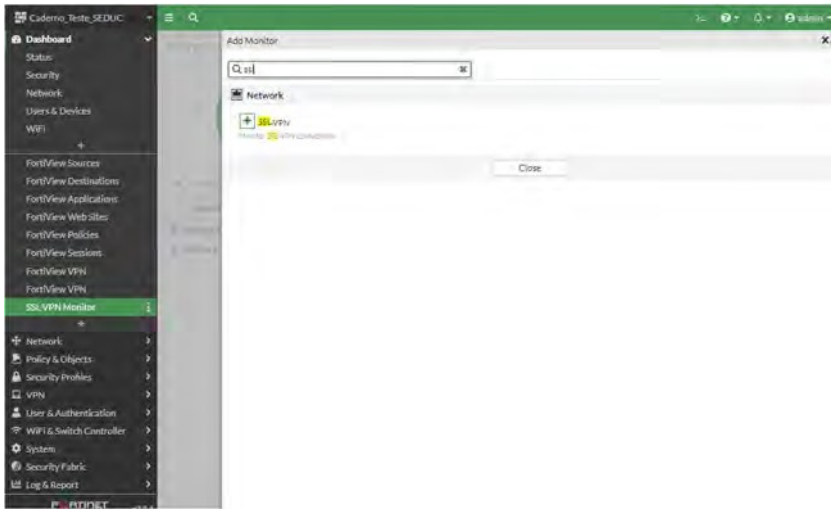
TESTE OK

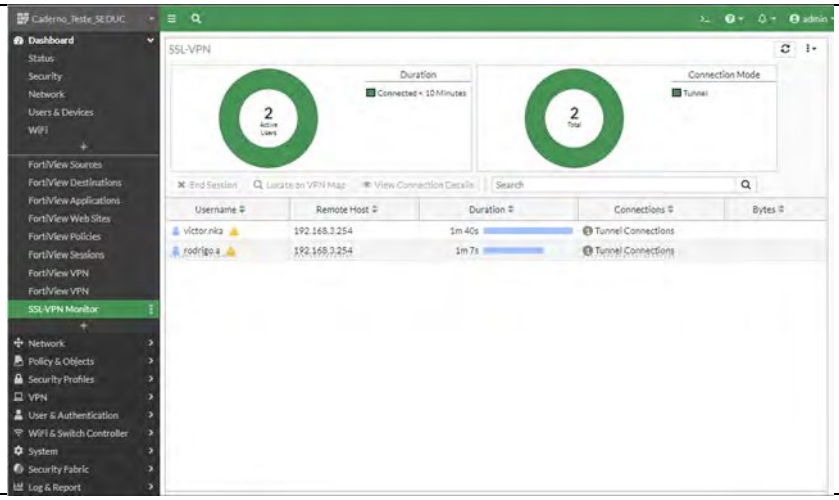

Device Manager
Add Device
Device Group
Install Wizard
Device & Groups
Add Device - Choose Add Device Type (1/2)
Discover Device
To add a device that is currently online.
Add Model Device
To add a device that is not yet online. Configure a model device to complete authorization when the device is online.
Add Model HA Cluster
Adding an operating FortiGate HA cluster to Device Manager pane is similar to adding a standalone device. Specify the IP address of the primary device.
Cancel

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

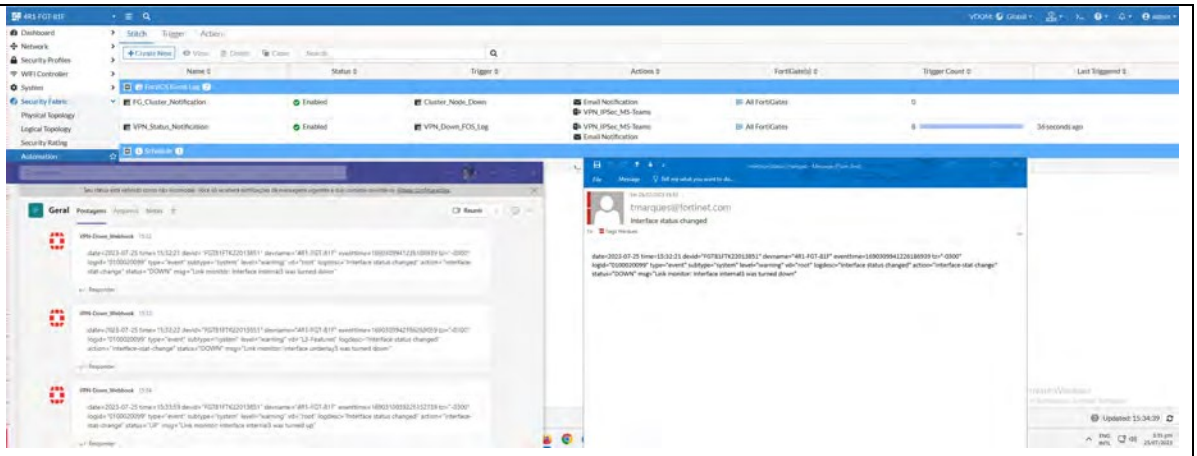
5.3.4 ACESSO REMOTO - VPN:

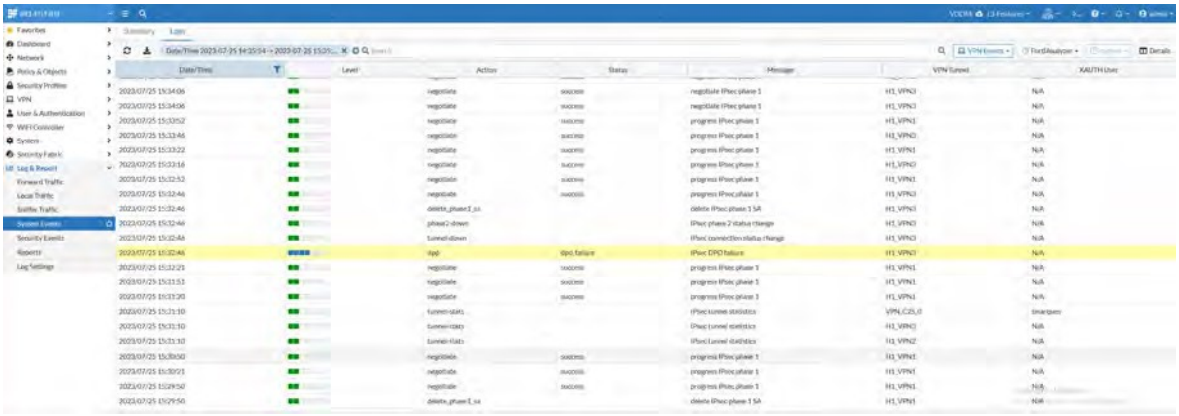
Item de Teste - 5.3.4.10	Deverá ser capaz de monitorar todos os usuários remotos logados;

Objetivo do Teste	Validar se o FortiGate é capaz de realizar o monitoramento de todos os usuários conectados remotamente por meio de VPN.
Configuração do Teste	Demontrar os usuários VPN conectados
Procedimento do Teste	Navegando por **Dashboard** > **+** > **Add Monitor** > **SSL-VPN** é possível adicionar um widgets SSL-VPN que permite o monitoramento de usuários conectados remotamente.
Evidências	 **TESTE OK** 

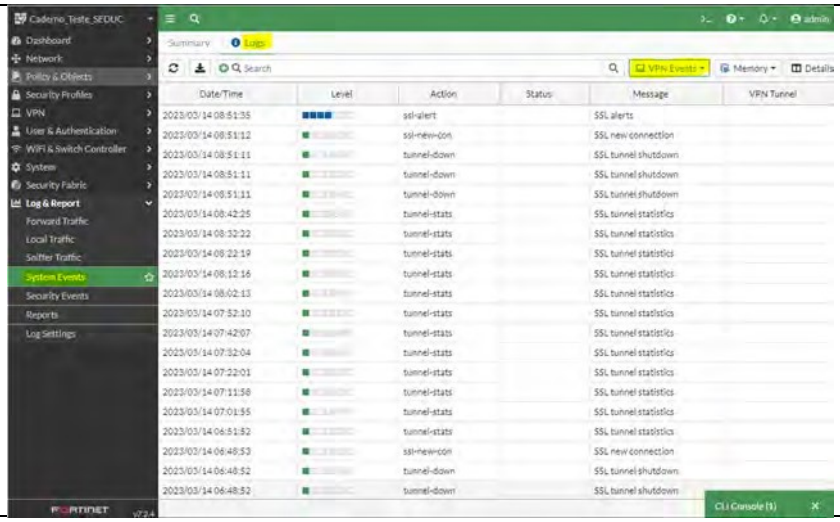
	
Comentário	

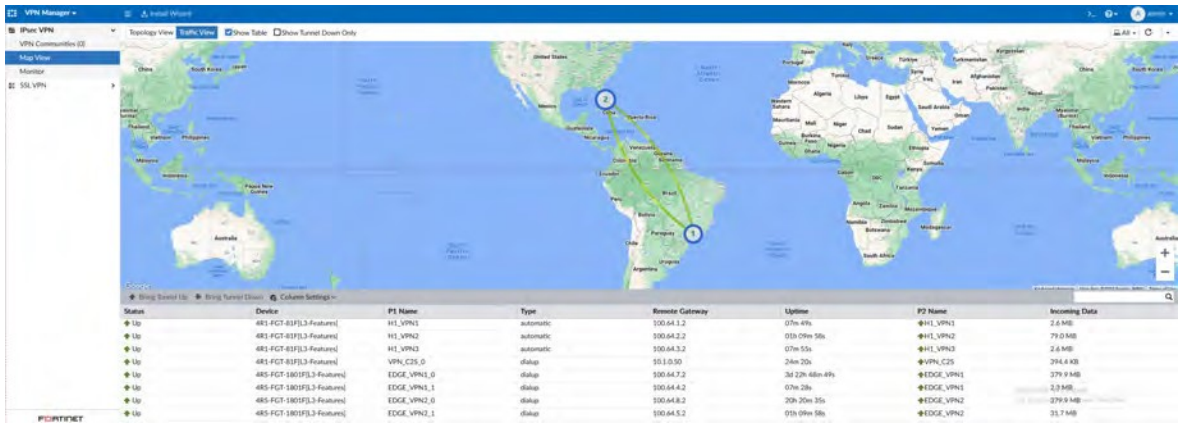
Item de Teste - 5.3.4.11	Deverá ser capaz de reconhecer falhas e problemas de conectividade entre dois pontos conectados através de uma VPN, e registrar e alertar quando o túnel VPN está desconectado;
Objetivo do Teste	Validar se o appliance é capaz de reconhecer falhas e problemas de conectividade entre dois pontos de uma VPN e realizar o registro de alertas quando o túnel VPN está desconectado.
Configuração do Teste	Demonstrar notificação de Túnel VPN desconectado, como exemplo via email.
Procedimento do Teste	Para criar um novo stitch automático vá em **Security Fabric** -> **Automation** -> **Create New.** Depois de colocar um nome, selecionar no gatilho do evento “Event Log” e em ação selecionar “e-mail”. Preencher os campos: - To. - Email subject. - Email body. No gatilho colocar “IPsec connection status changed”. Ao acessar a seção "Log & Report" e, em seguida, "System Events" e "VPN Events", é possível identificar falhas e problemas de conectividade em um ambiente de rede virtual privada (VPN).
Evidências	

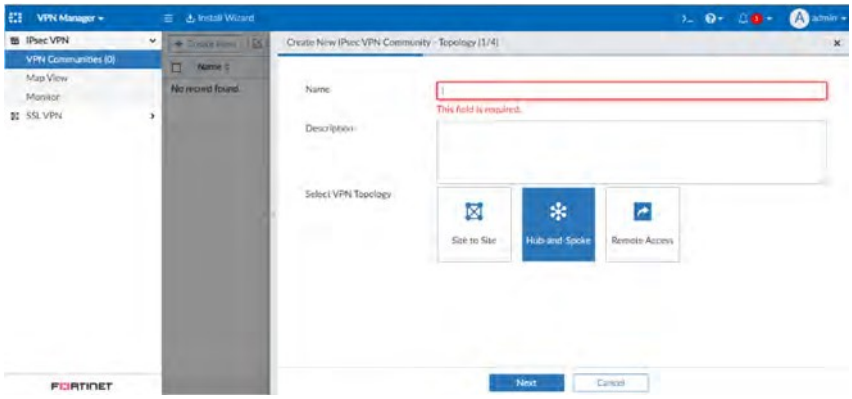
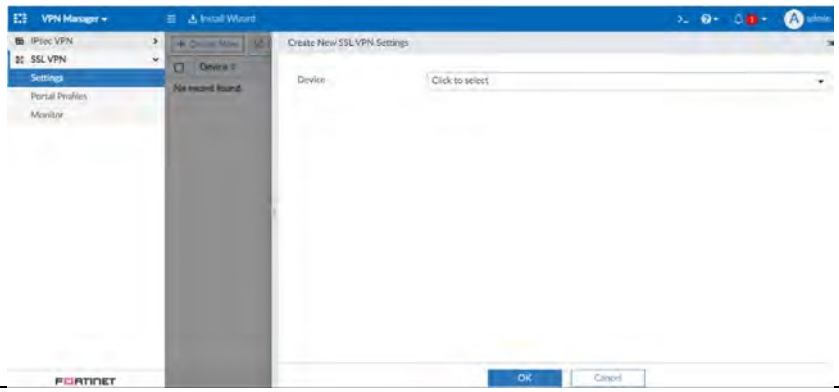




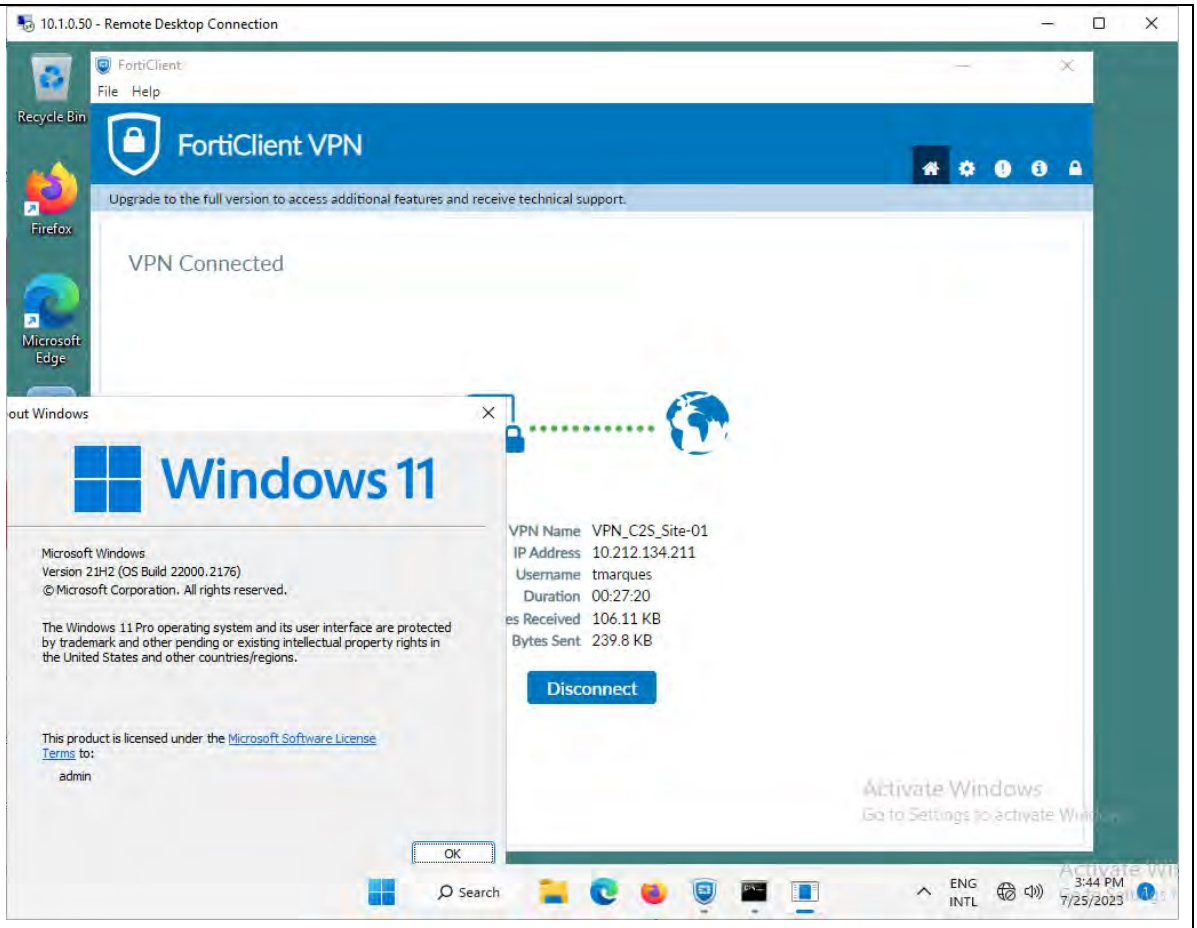
TESTE OK

	
Comentário	

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

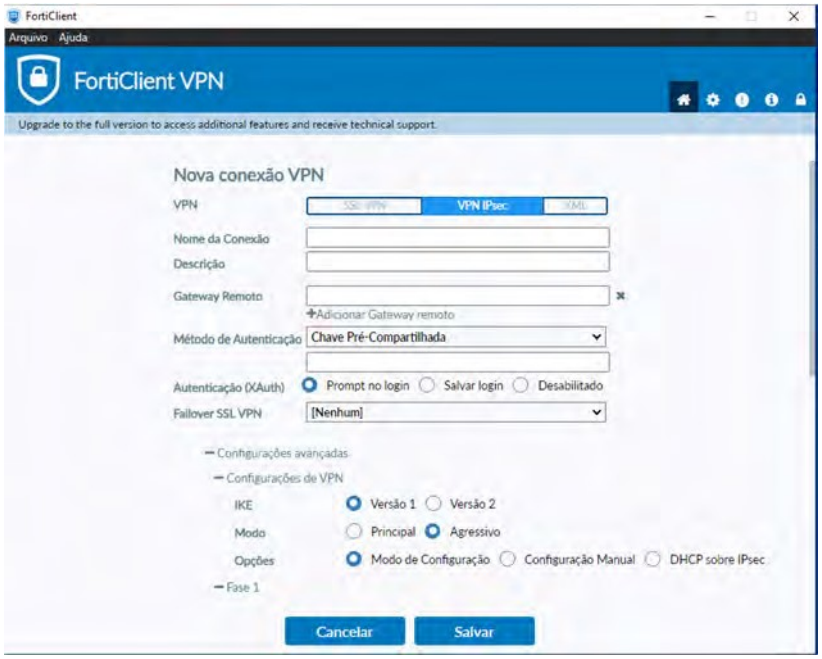
	TESTE OK  
Comentário	https://docs.fortinet.com/document/fortimanager/7.2.3/administration-guide/9083

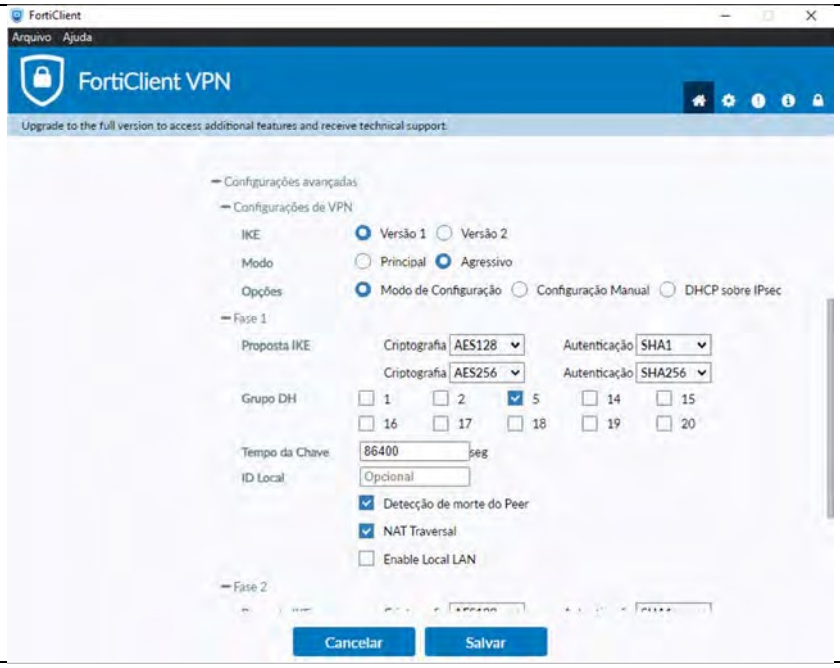
Item de Teste - 5.3.4.13	Clientes IPSec do mesmo fabricante devem estar disponíveis para pelo menos Windows 10 (64 bits);
Objetivo do Teste	Validar se o Forticlient está disponível para Windows 10 (64 bits)
Configuração do Teste	Forticlient é totalmente compatível com Windows 10 e permite conexões tanto 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	`


10.1.0.50 - Remote Desktop Connection
FortiClient
File Help
FortiClient VPN
Upgrade to the full version to access additional features and receive technical support.
VPN Connected
Recycle Bin
Firefox
Microsoft Edge
out Windows
Windows 11
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
OK
VPN Name VPN_C2S_Site-01
IP Address 10.212.134.211
Username tmarques
Duration 00:27:20
es Received 106.11 KB
Bytes Sent 239.8 KB
Disconnect
Activate Windows
Search
ENG
INTL
3:44 PM
7/25/2023

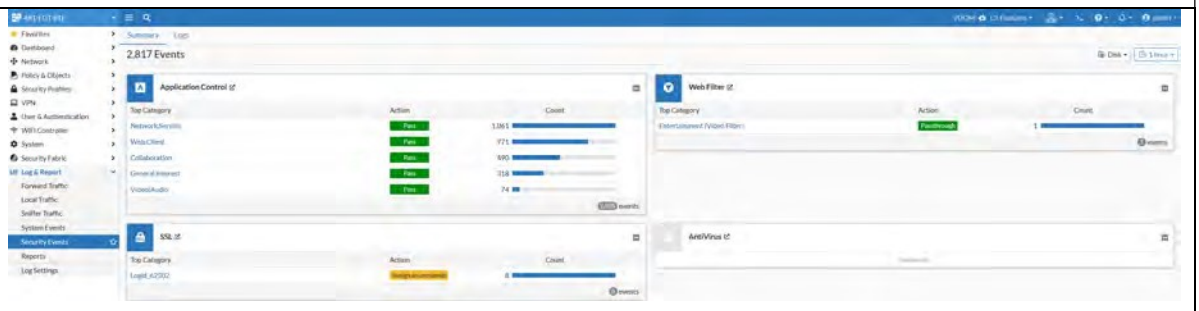
TESTE OK

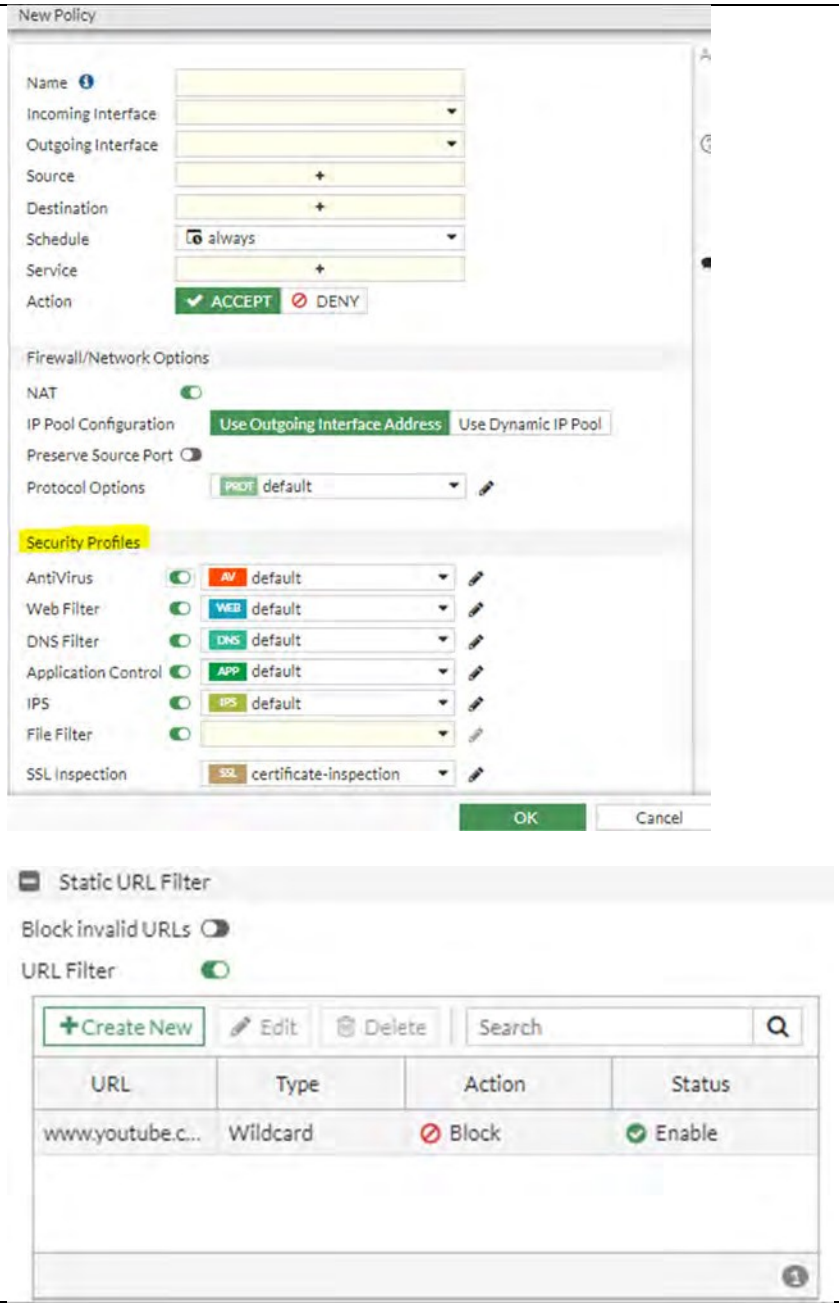

FortiClient VPN
The VPN-only version of FortiClient offers SSL VPN and IPSecVPN, but does not include any support. Download the best VPN software for multiple devices.
Remote Access
SSL VPN with MFA
IPSEC VPN with MFA
Download VPN for Windows
DOWNLOAD
Download VPN for MacOS
DOWNLOAD
Download VPN for Linux
DOWNLOAD .rpm
Download VPN for iOS
DOWNLOAD
Download VPN for Android
DOWNLOAD
Download VPN for Linux
DOWNLOAD .deb


FortiClient
Arquivo Ajuda
FortiClient VPN
Upgrade to the full version to access additional features and receive technical support.
Nova conexão VPN
VPN
VPN IPsec
Nome da Conexão
Descrição
Gateway Remoto
Adicionar Gateway remoto
Método de Autenticação
Chave Pré-Compartilhada
Autenticação (XAuth)
Prompt no login
Salvar login
Desabilitado
Failover SSL VPN
[Nenhum]
Configurações avançadas
Configurações de VPN
IKE
Versão 1
Versão 2
Modo
Principal
Agressivo
Opções
Modo de Configuração
Configuração Manual
DHCP sobre IPsec
Fase 1
Cancelar
Salvar

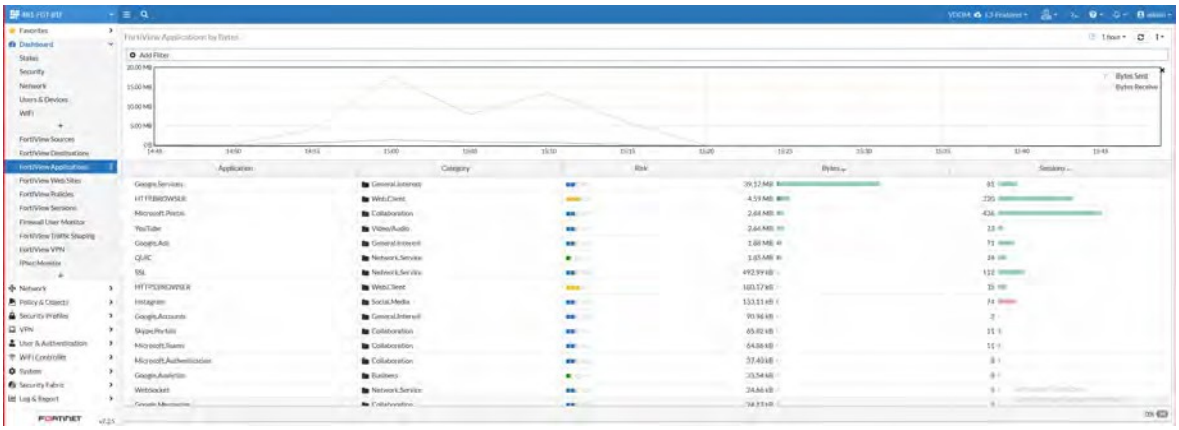
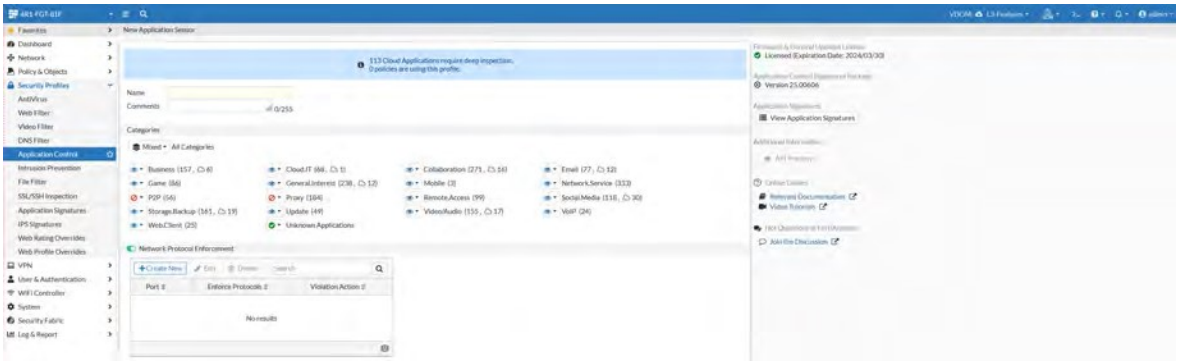
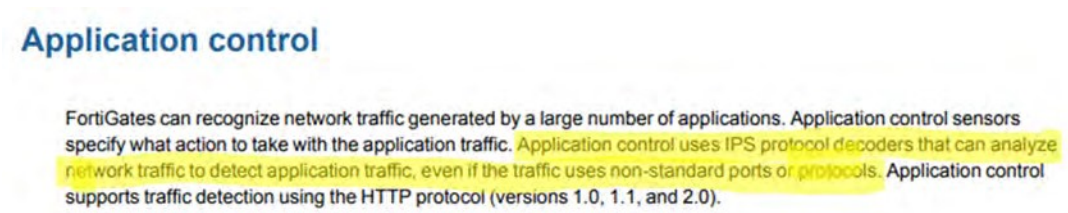
	
Comentário	

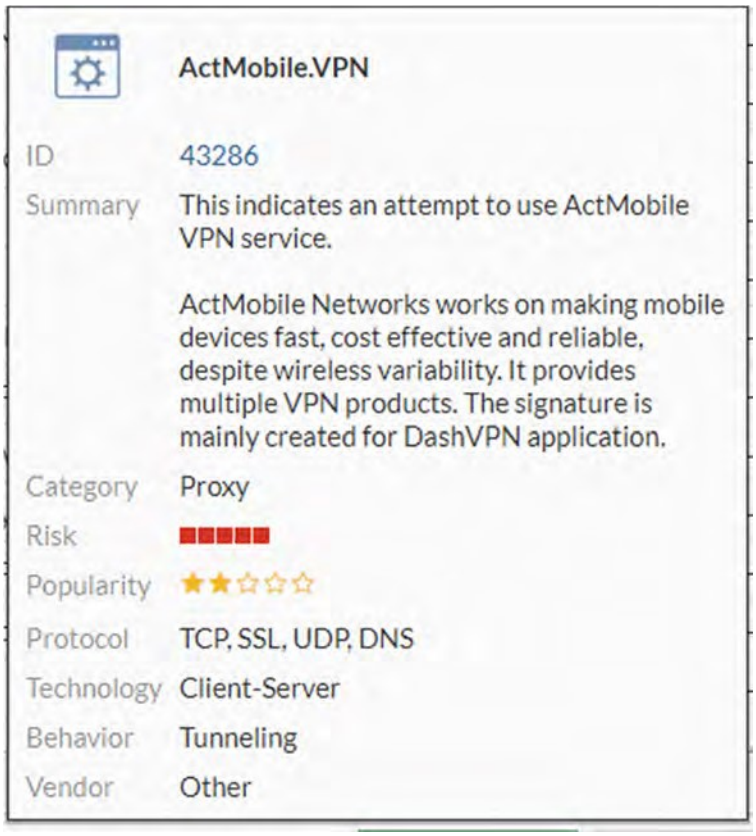
5.3.5 CONTROLE DE APLICAÇÕES WEB E FILTRO URL:

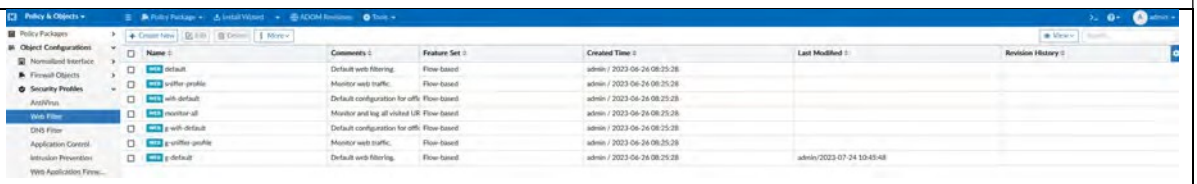
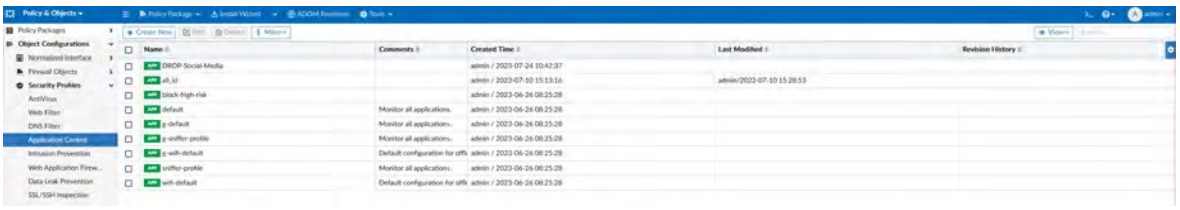
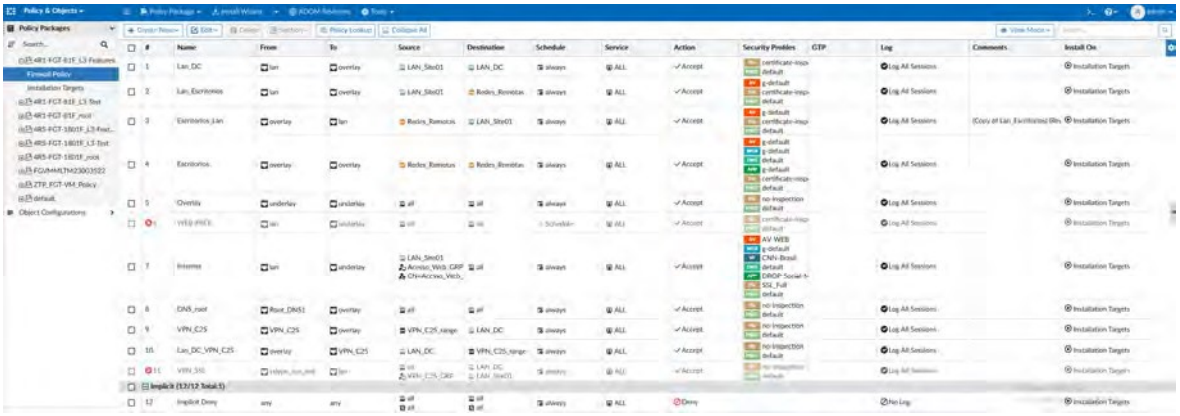
Item de Teste - 5.3.5.1	A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança, que permita a criação de políticas de liberação ou bloqueio;
Objetivo do Teste	Validar se a solução conta com ferramentas de visibilidade e controle de aplicações Web e Filtro URL integrada, que permita a criação de políticas de liberação ou bloqueio.
Configuração do Teste	Configuração de regra de segurança NGFW com filtro de aplicação e URL.
Procedimento do Teste	Navegando por **Security Profiles** > **Web Filter** é possível criar filtro de URL que pode ser adicionado as regras em Security Profile, assim liberando ou bloqueando URL, tal funcionalidade é nativa do appliance.
Evidências	 **TESTE OK**

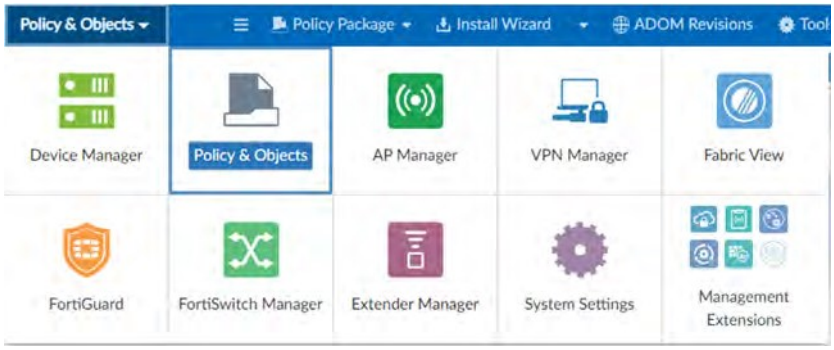
	
Comentário	

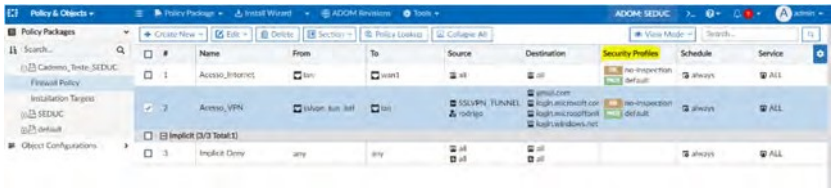
Item de Teste - 5.3.5.2	A solução deve ser capaz de identificar qualquer tipo de aplicação, em até camada 7, independente de porta e protocolo;
Objetivo do Teste	Verificar se o equipamento identifica uma aplicação independente de porta ou protocolo.
Configuração do Teste	Criar filtro de aplicação de camada 7

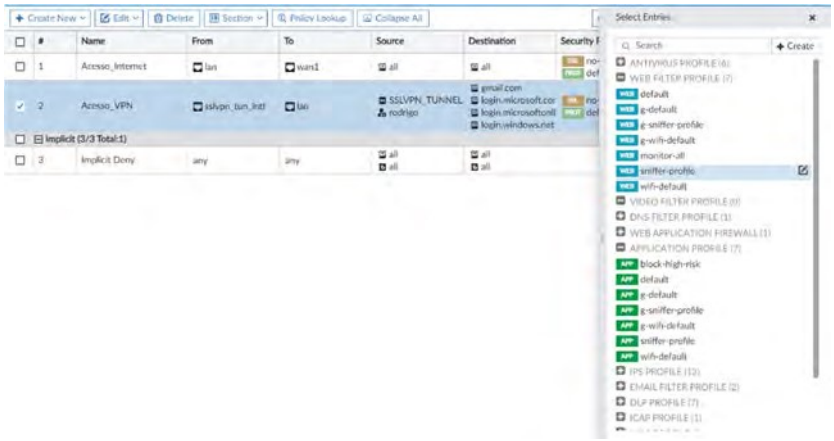
Procedimento do Teste	Criar regra contendo filtro de aplicação de camada 7.
Evidências	   **TESTE OK**

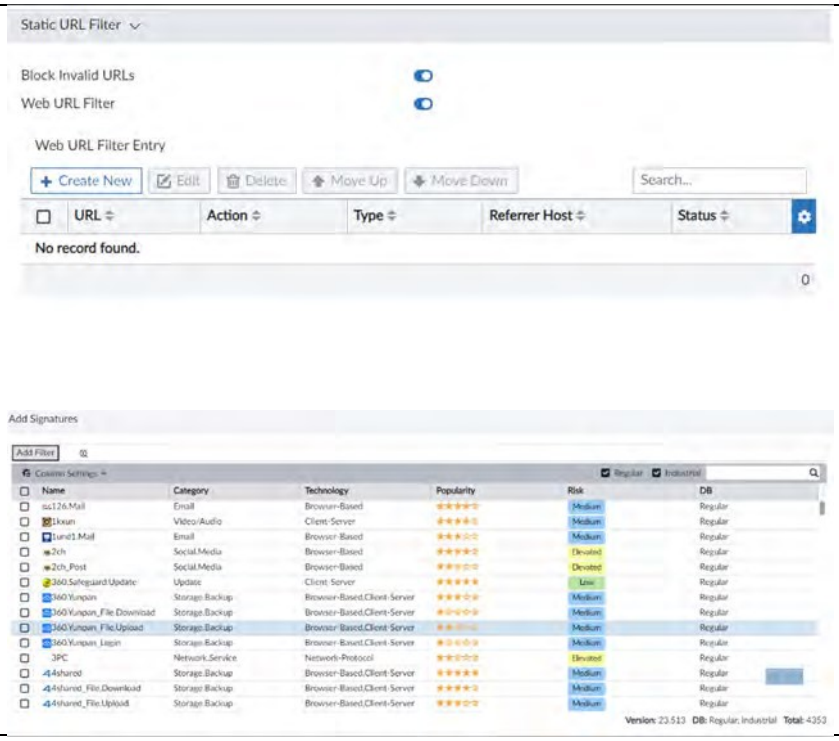
	"Controle de aplicação utiliza do decodificador de protocolos IPS que consegue analisar o tráfego da rede e identificar as aplicações mesmo se elas utilizarem portas ou protocolos que não são padrões" **Application control** FortiGates can recognize network traffic generated by a large number of applications. Application control sensors specify what action to take with the application traffic. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic, even if the traffic uses non-standard ports or protocols. Application control supports traffic detection using the HTTP protocol (versions 1.0, 1.1, and 2.0). 
Comentário	Fonte: FortiOS-7.2.3Administration_Guide acessado em https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a06117ca-5fbf-11ed-96f0-fa163e15d75b/FortiOS-7.2.3-Administration_Guide.pdf

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

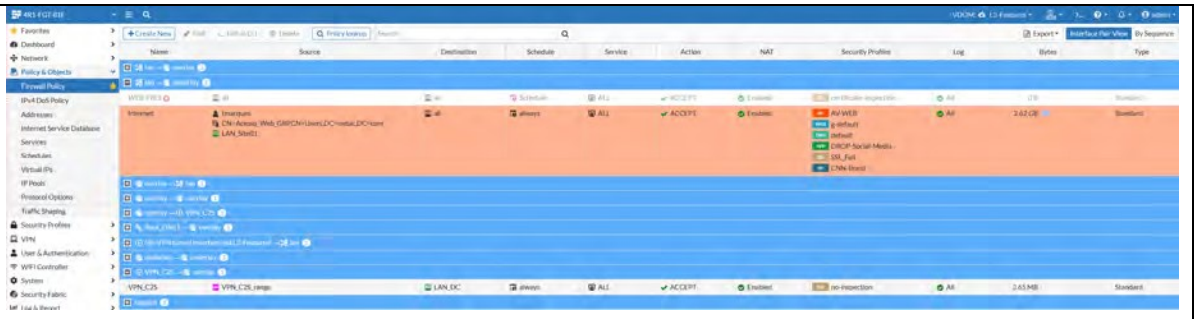
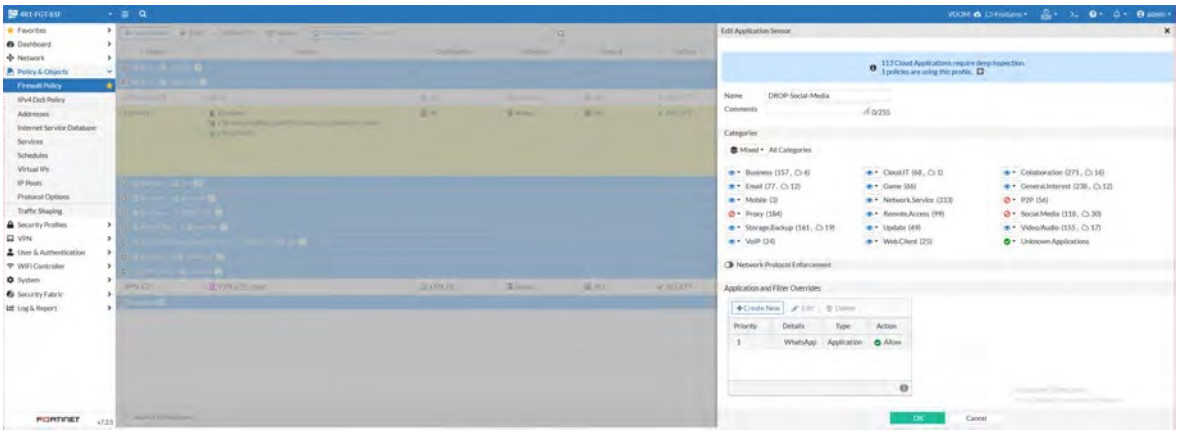
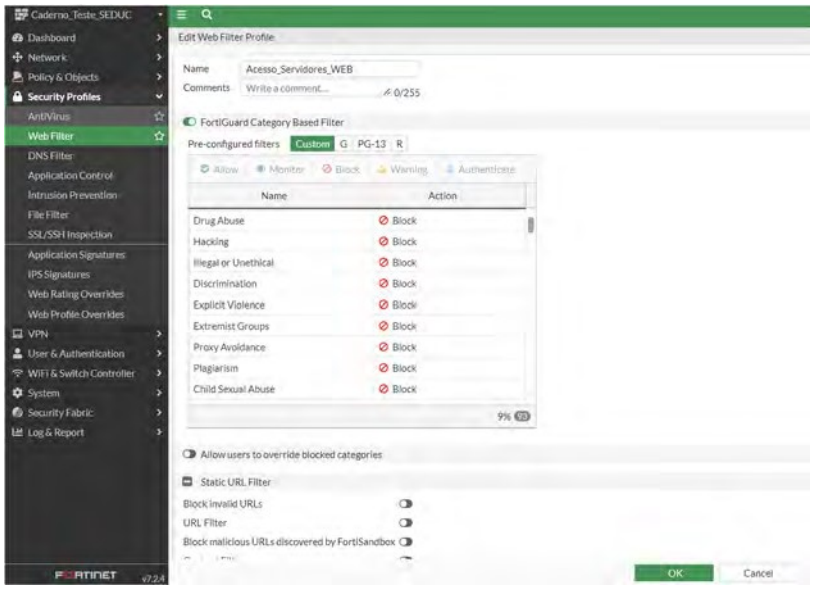

Policy & Objects
Policy Package
Install Wizard
ADOM Revisions
Tool
Device Manager
Policy & Objects
AP Manager
VPN Manager
Fabric View
FortiGuard
FortiSwitch Manager
Extender Manager
System Settings
Management Extensions



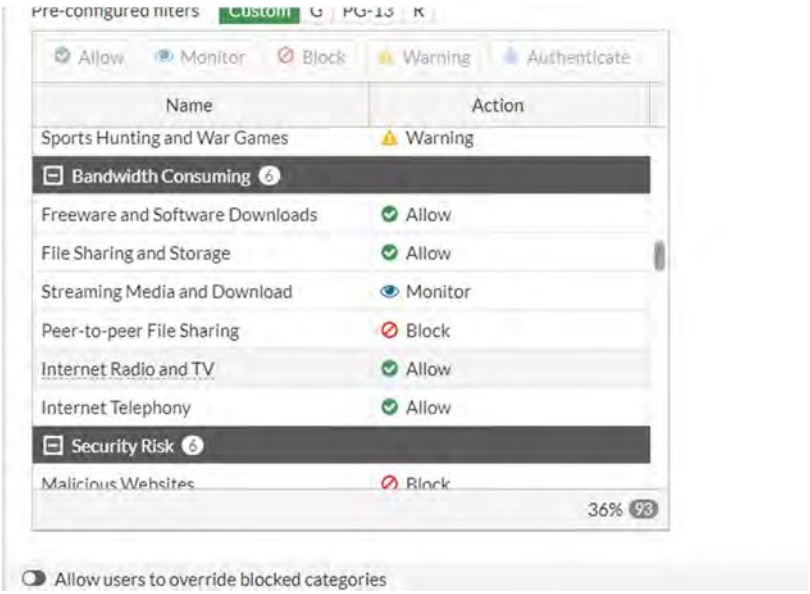


	
Comentário	

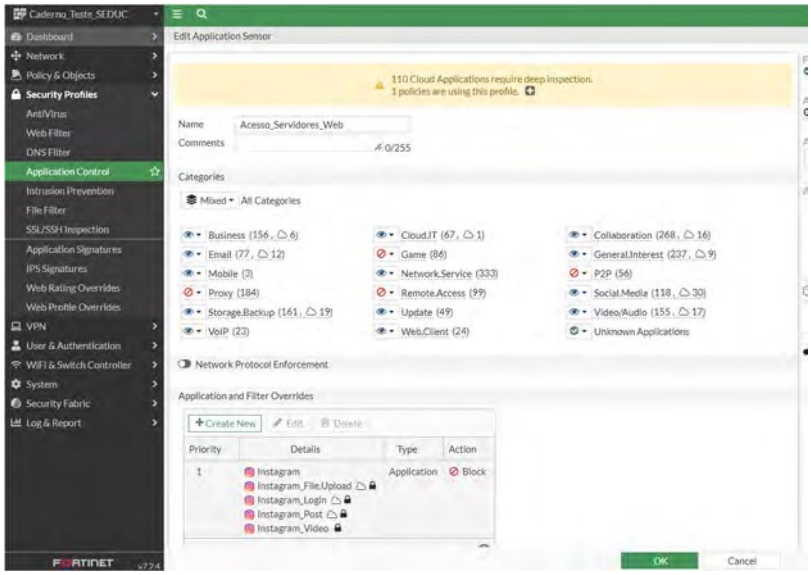
Item de Teste - 5.3.5.5	Possuir controle de regras de aplicações, grupos de aplicações, categorias de aplicações com controle granular para usuários ou grupos de usuários;
Objetivo do Teste	Validar se a solução possui ferramentas de controle de regras de aplicações, grupos de aplicações, categorias de aplicações com controle granular para usuários ou grupos.
Configuração do Teste	Criar regra de segurança.
Procedimento do Teste	Navegando por **Security Profile** > **Application Control** > **Create New** é possível criar um novo perfil enquadrando as aplicações que deseja bloquear, monitorar ou aprovar Navegando por **Policy & Objects** > **Firewall Policy** é possível enquadrar o perfil de Application Control criado para determinar em qual fluxo ocorrera o controle de tráfego por aplicação No campo “Source” da política, podemos realizar o controle de qual grupo ou usuário a regra se enquadra No campo Security Profiles determinamos quais categorias de sites e aplicações o grupo de usuários se enquadra

Evidências	  **TESTE OK** 1 – Criando Web Filter. 

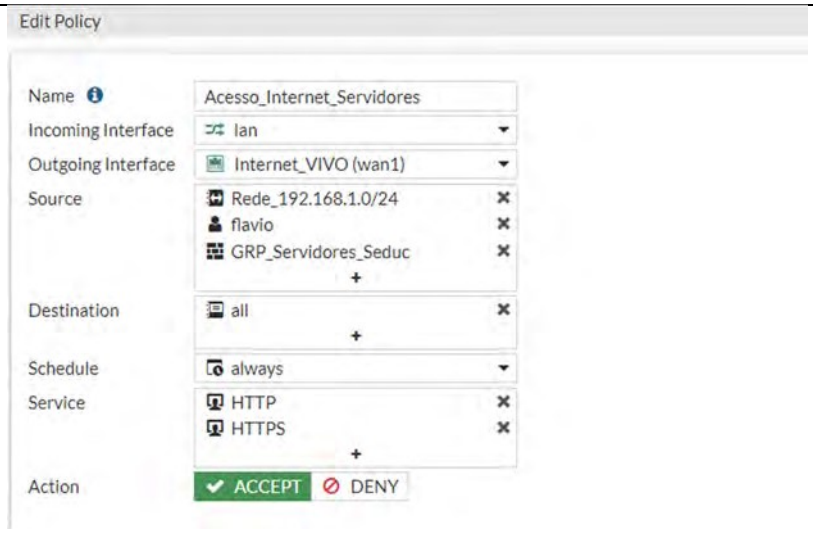
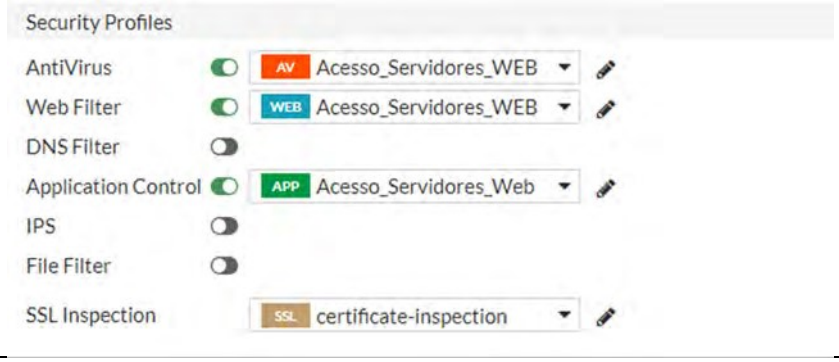
2 - Selecionando categorias.



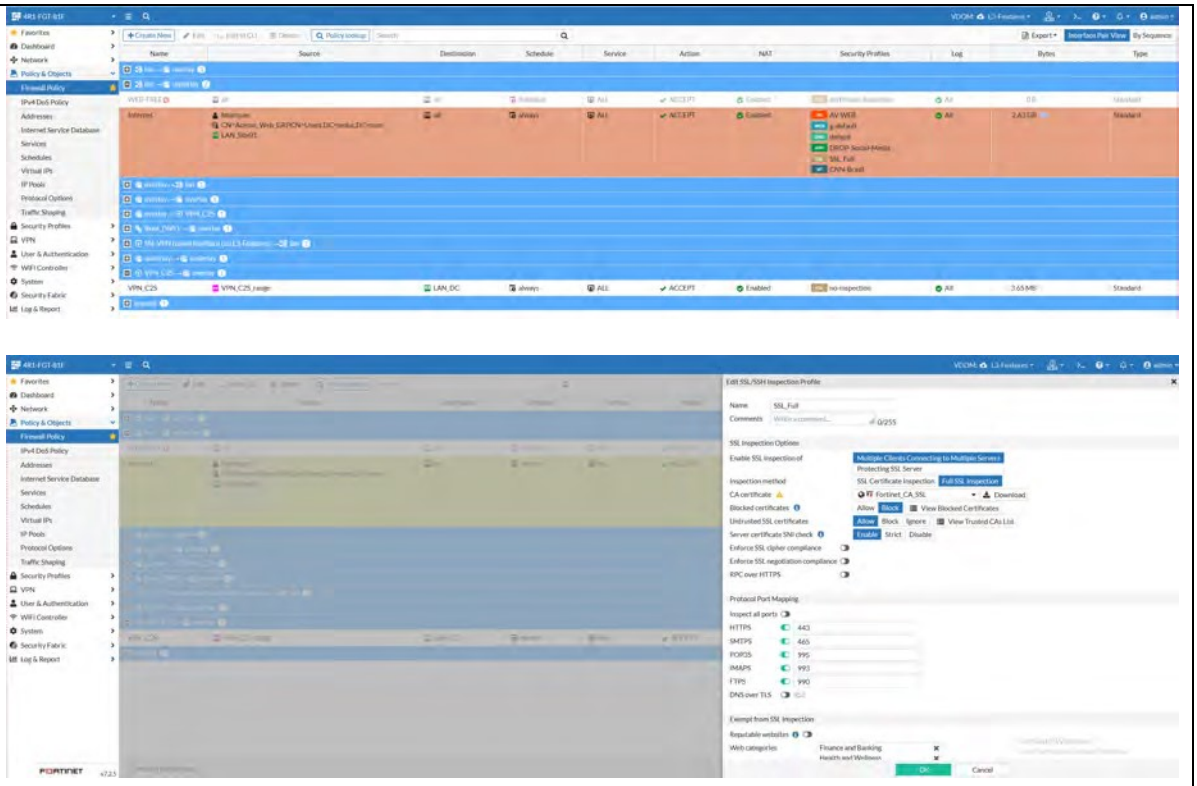
3 – Criando Application Control.

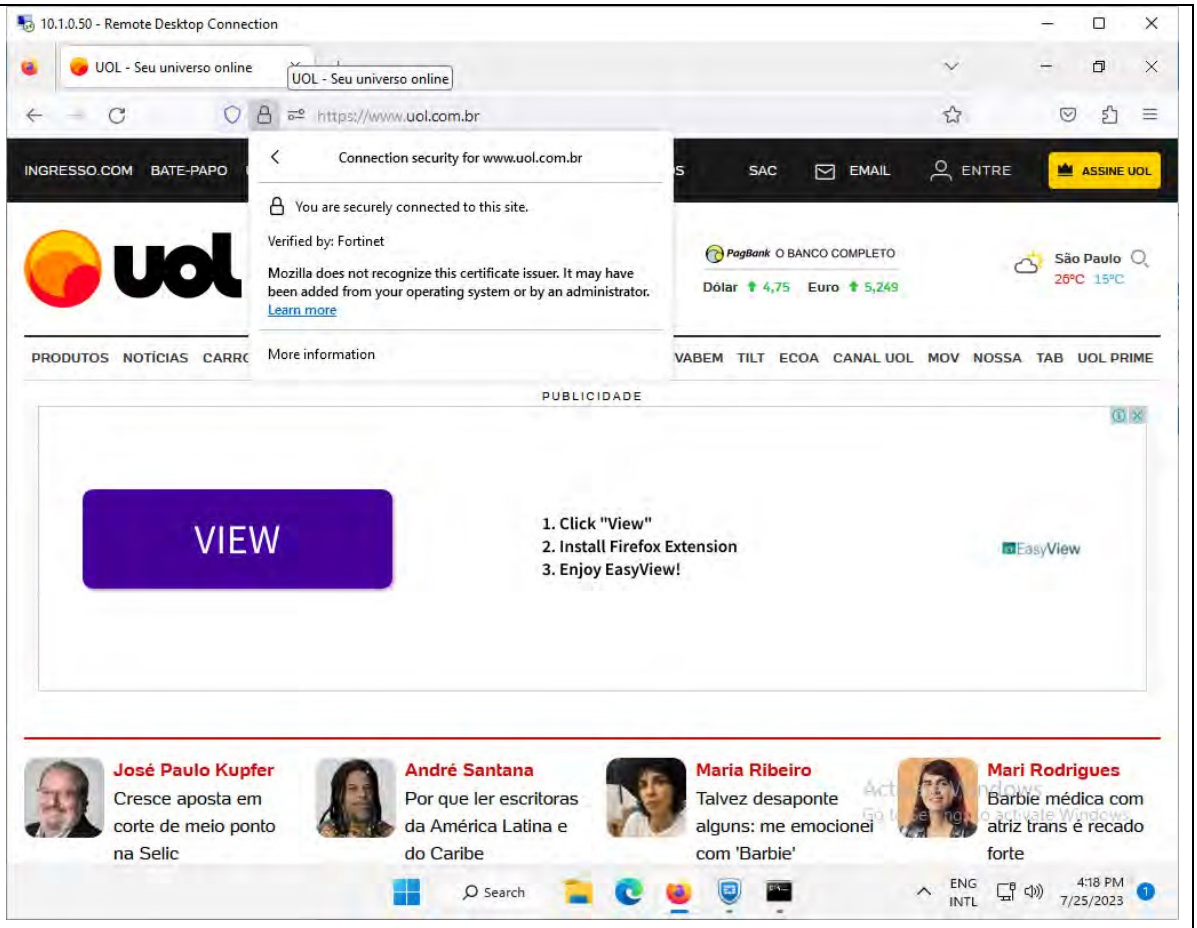


3 – Definindo grupos e usuários.

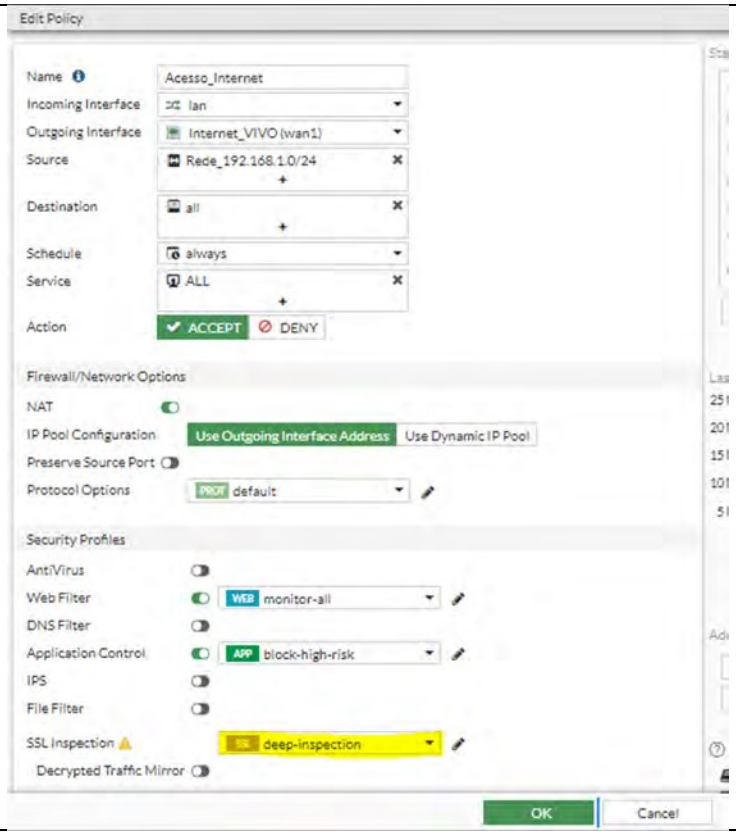
	 4 – Definindo Profiles WEB e de Aplicação para política. 
Comentário	

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

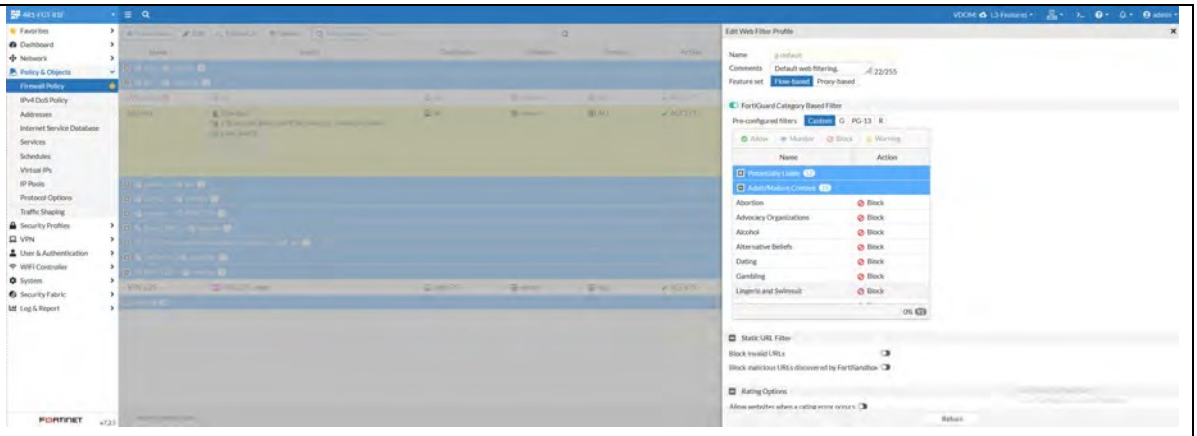



10.1.0.50 - Remote Desktop Connection
UOL - Seu universo online
https://www.uol.com.br
Connection security for www.uol.com.br
You are securely connected to this site.
Verified by: Fortinet
Mozilla does not recognize this certificate issuer. It may have been added from your operating system or by an administrator.
Learn more
More information
INGRESSO.COM
BATE-PAPO
SAC
EMAIL
ENTRE
ASSINE UOL
PagBank O BANCO COMPLETO
Dólar 4,75 Euro 5,249
São Paulo
26°C 15°C
PRODUTOS NOTÍCIAS
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
Search
ENG INTL
4:18 PM 7/25/2023

TESTE OK

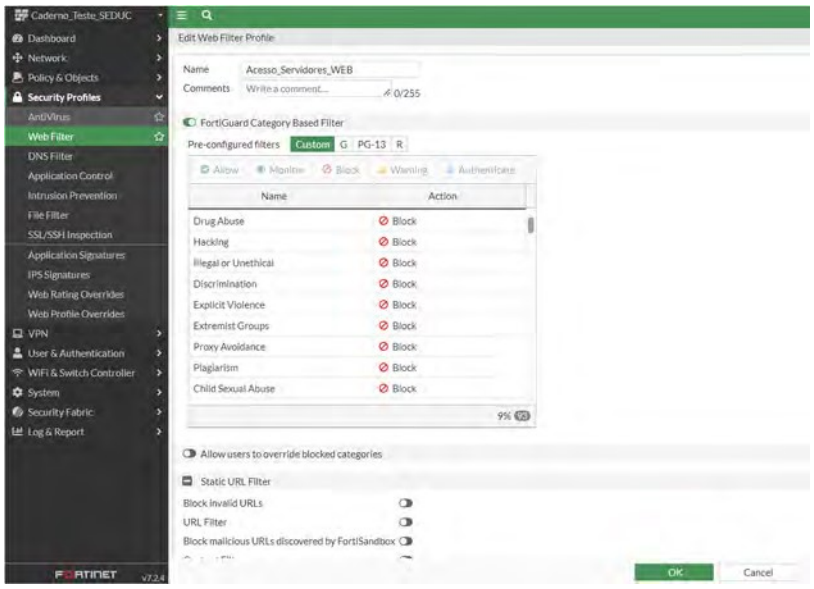
	
Comentário	

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

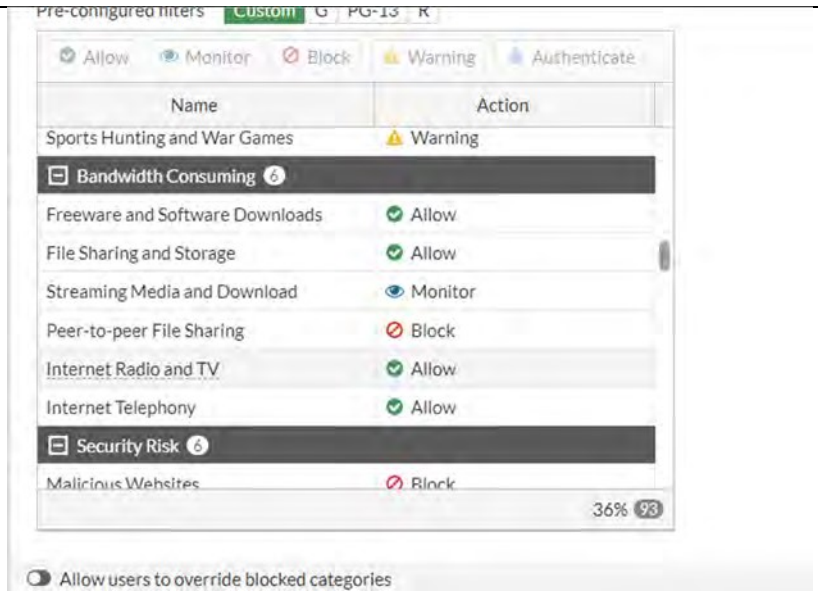


TESTE OK

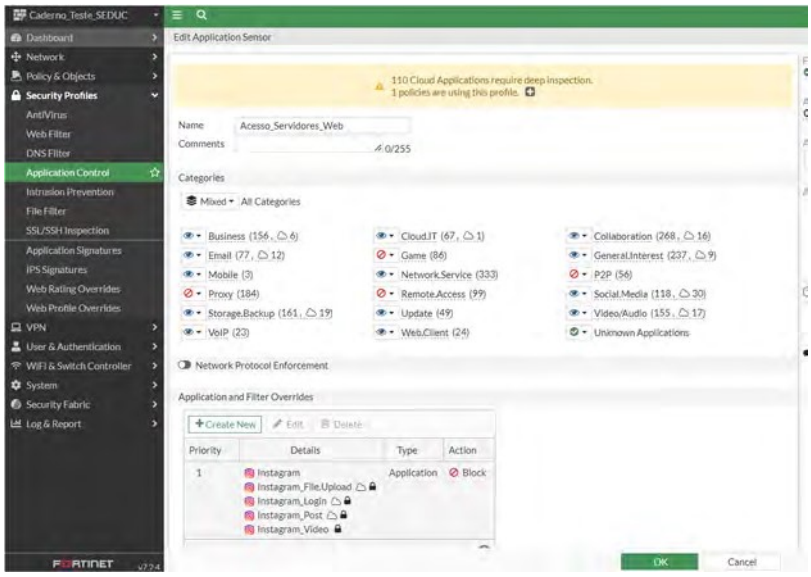
1 – Criando Web Filter.



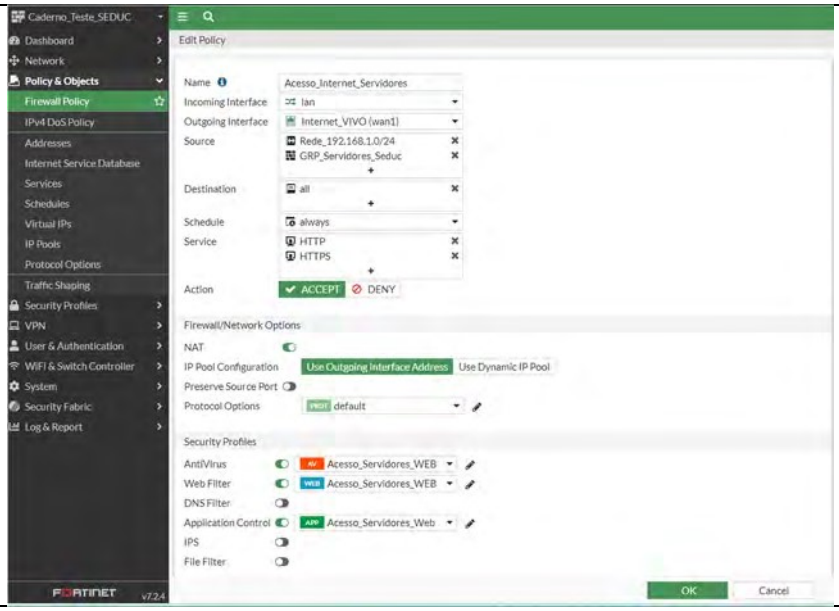
2 - Selecionando categorias.



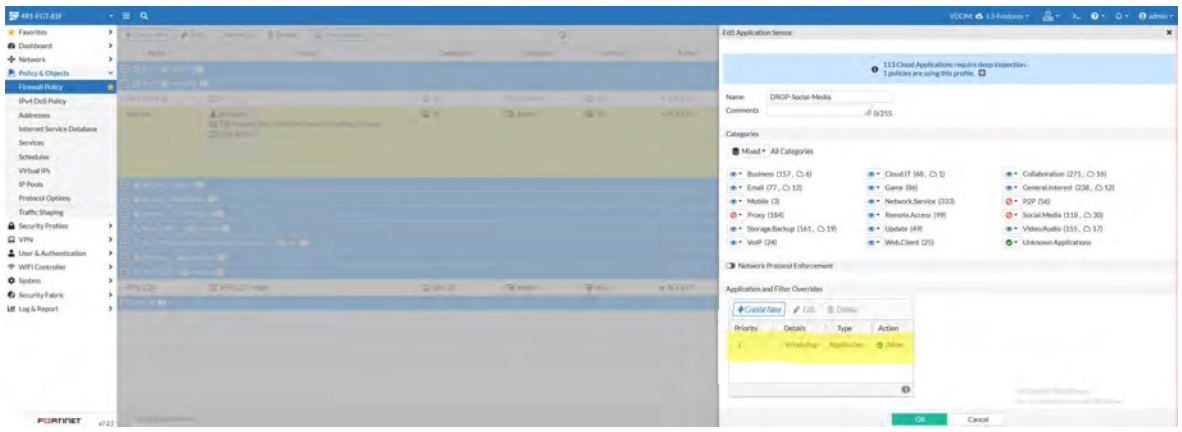
3 – Criando Application Control.

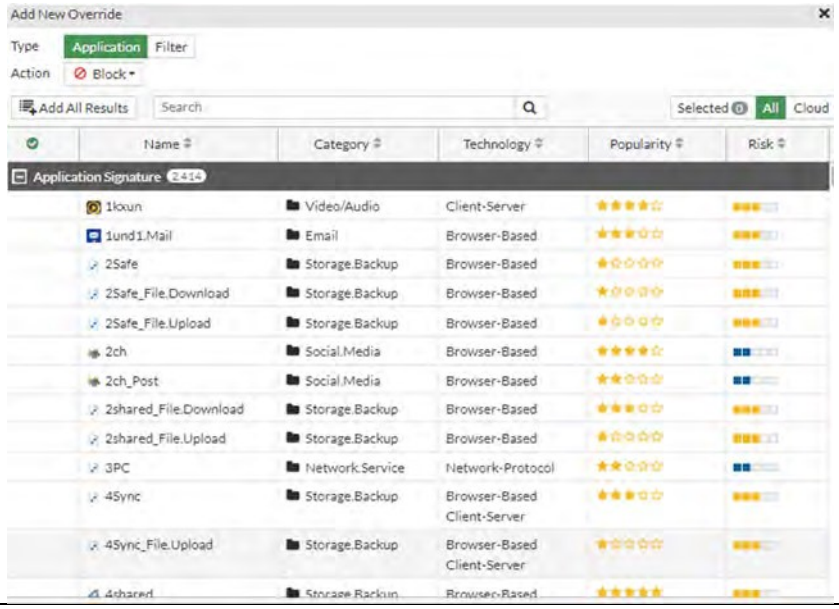


4 – Adicionando profiles de segurança em políticas.

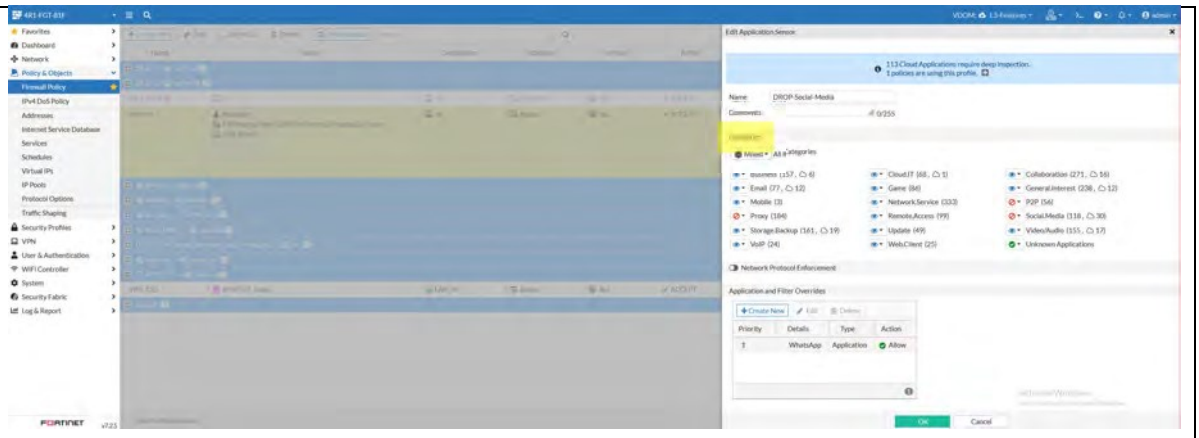
	
Comentário	https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/615462/url-filter https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/019814/basic-category-filters-and-overrides

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

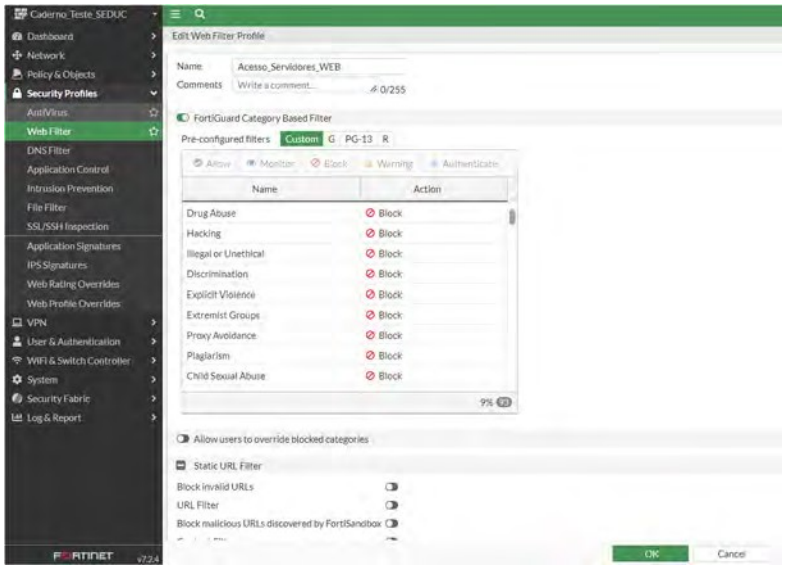
Item de Teste - 5.3.5.9.1	Aplicação da Web;
Objetivo do Teste	Validar se o Firewall possibilita o bloqueio ou permissão de aplicações da Web
Configuração do Teste	Navegando por Security Profiles > Application Control é possível realizar o bloqueio ou liberação de aplicações web
Procedimento do Teste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

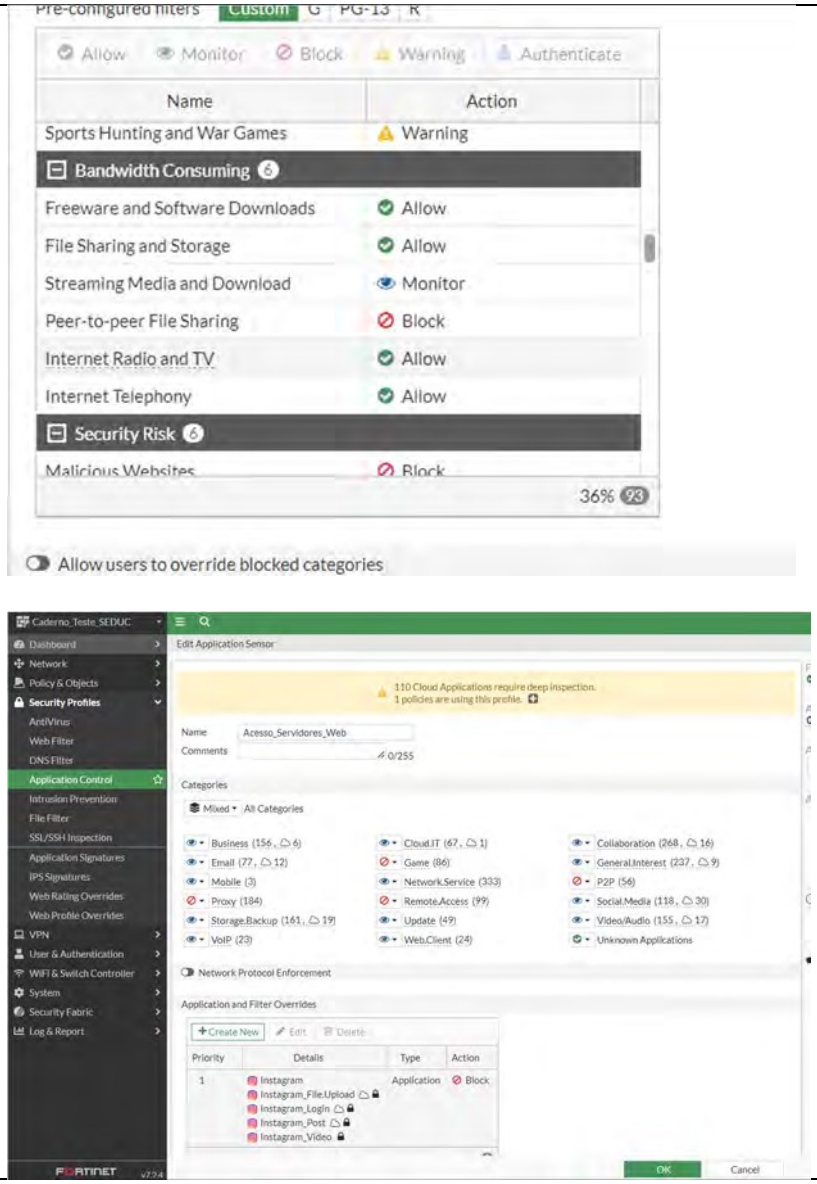
	TESTE OK 
Comentário	

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

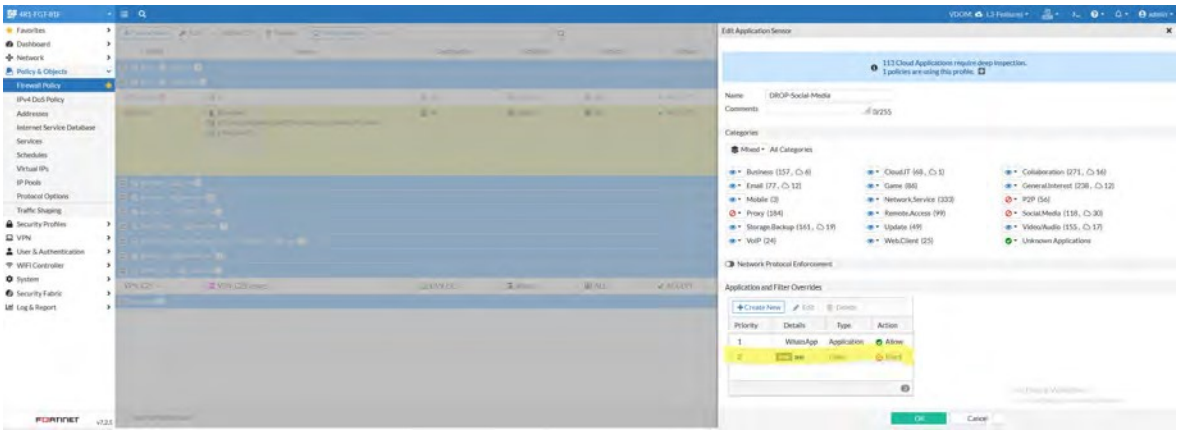
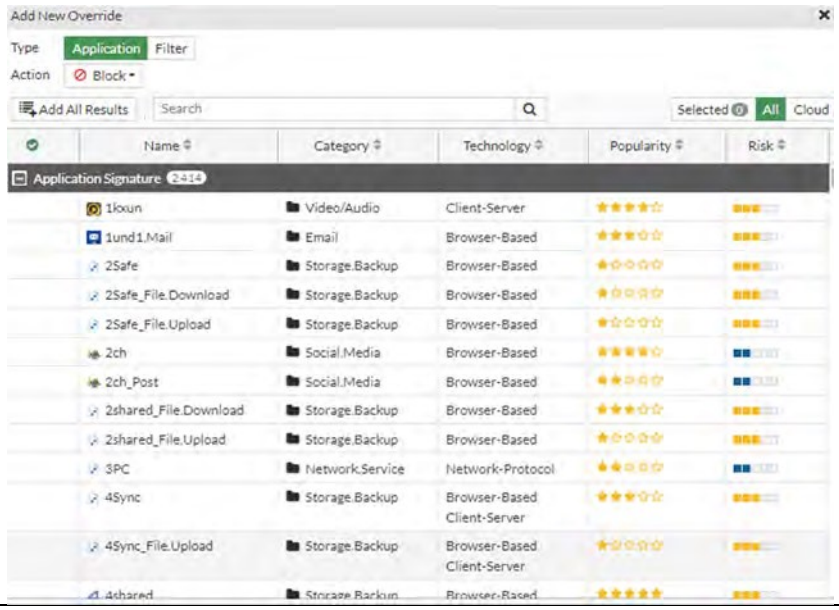


TESTE OK

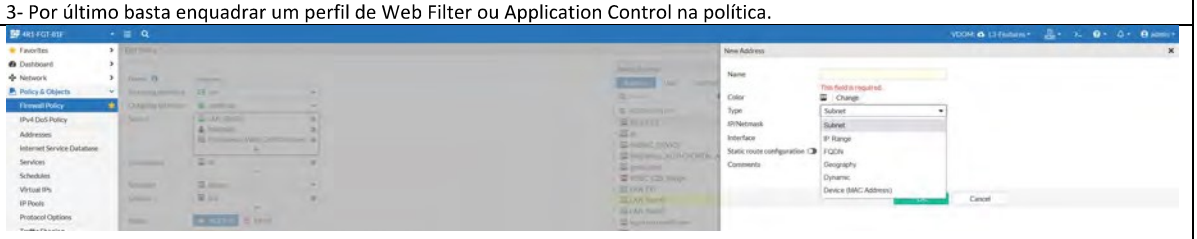
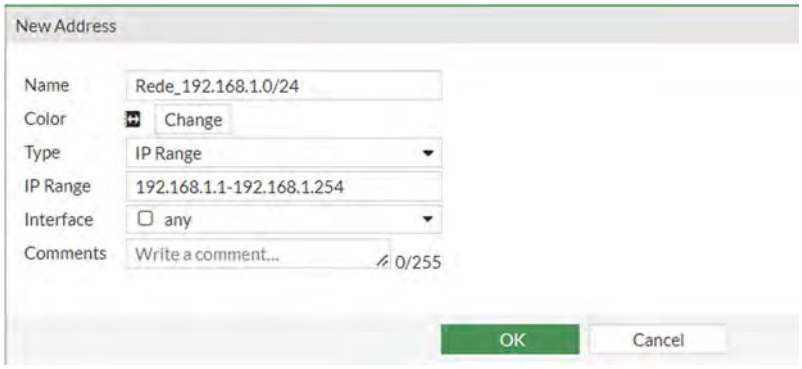

Caderno_Teste_SEDUC
Dashboard
Network
Policy & Objects
Security Profiles
AntiVirus
Web Filter
DNS Filter
Application Control
Intrusion Prevention
File Filter
SSL/SSH Inspection
Application Signatures
IPS Signatures
Web Rating Overrides
Web Profile Overrides
VPN
User & Authentication
WiFi & Switch Controller
System
Security Fabric
Log & Report
Edit Web Filter Profile
Name
Acesso_Servidores_WEB
Comments
Write a comment...
0/255
FortiGuard Category Based Filter
Pre-configured filters
Custom
G
PG-13
R
Allow
Monitor
Block
Warning
Authenticate
Name
Action
Drug Abuse
Hacking
Illegal or Unethical
Discrimination
Explicit Violence
Extremist Groups
Proxy Avoidance
Plagiarism
Child Sexual Abuse
Block
9%
Allow users to override blocked categories
Static URL Filter
Block invalid URLs
URL Filter
Block malicious URLs discovered by FortiSandbox
OK
Cancel

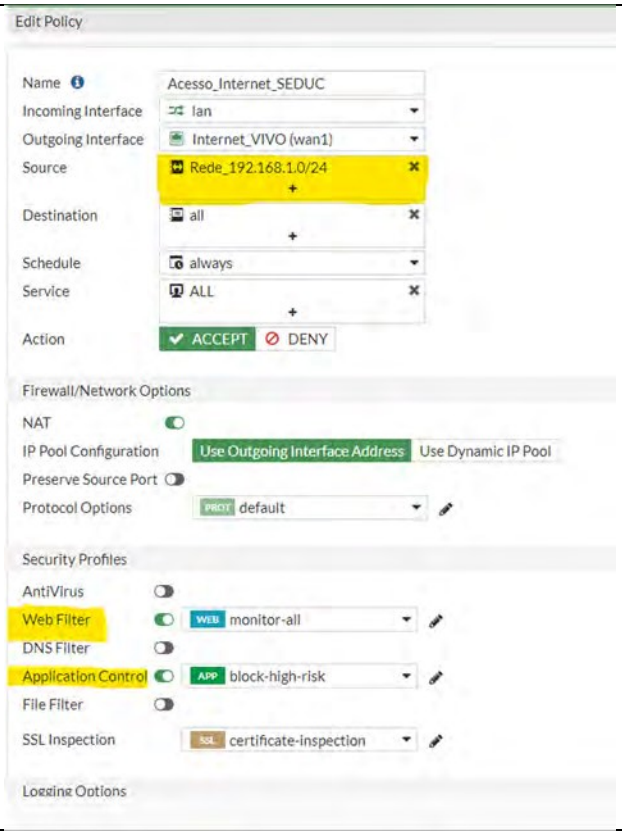
	
Comentário	https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/615462/url-filter https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/019814/basic-category-filters-and-overrides

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

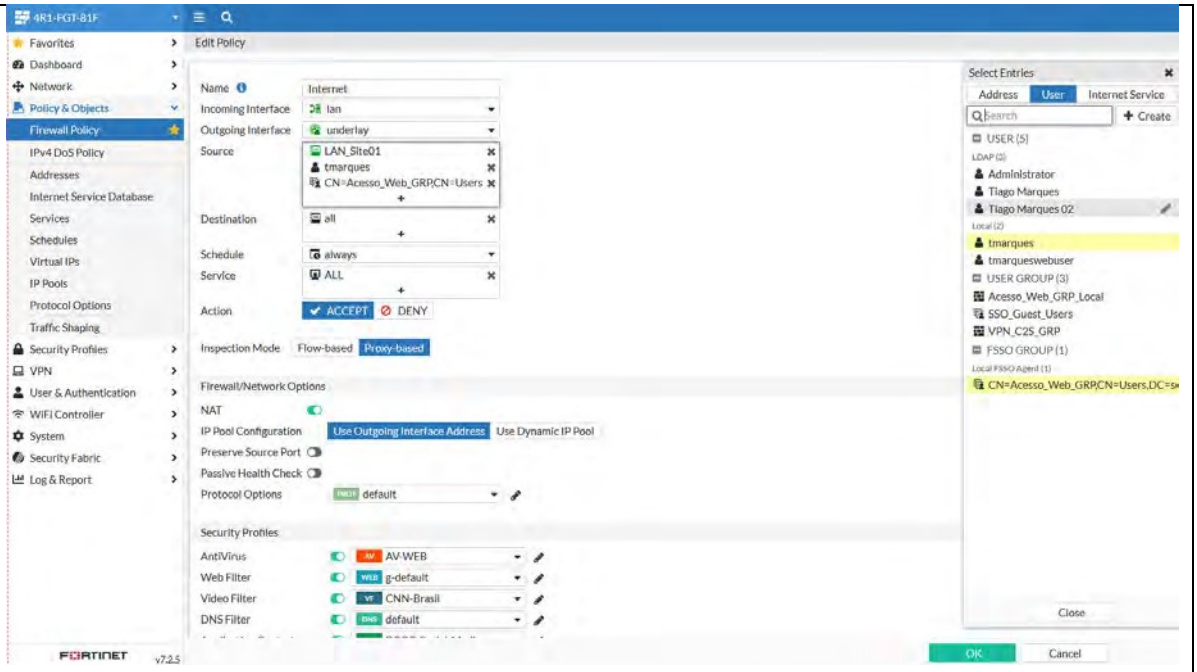
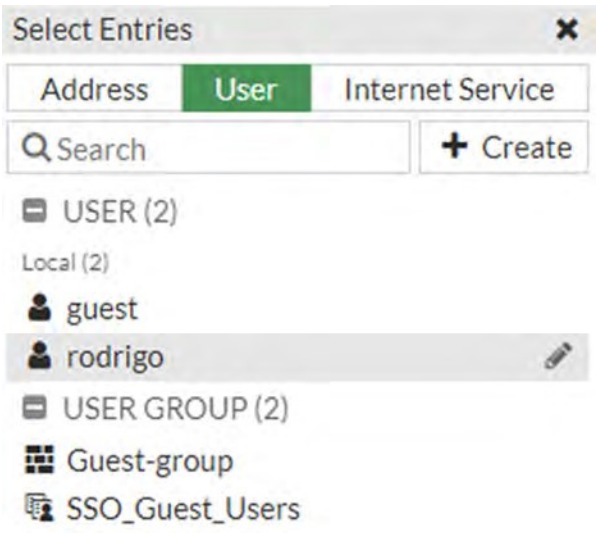
Procedimento do Teste	Criar regra de segurança NGFW com filtro por risco
Evidências	 **TESTE OK** 
Comentário	

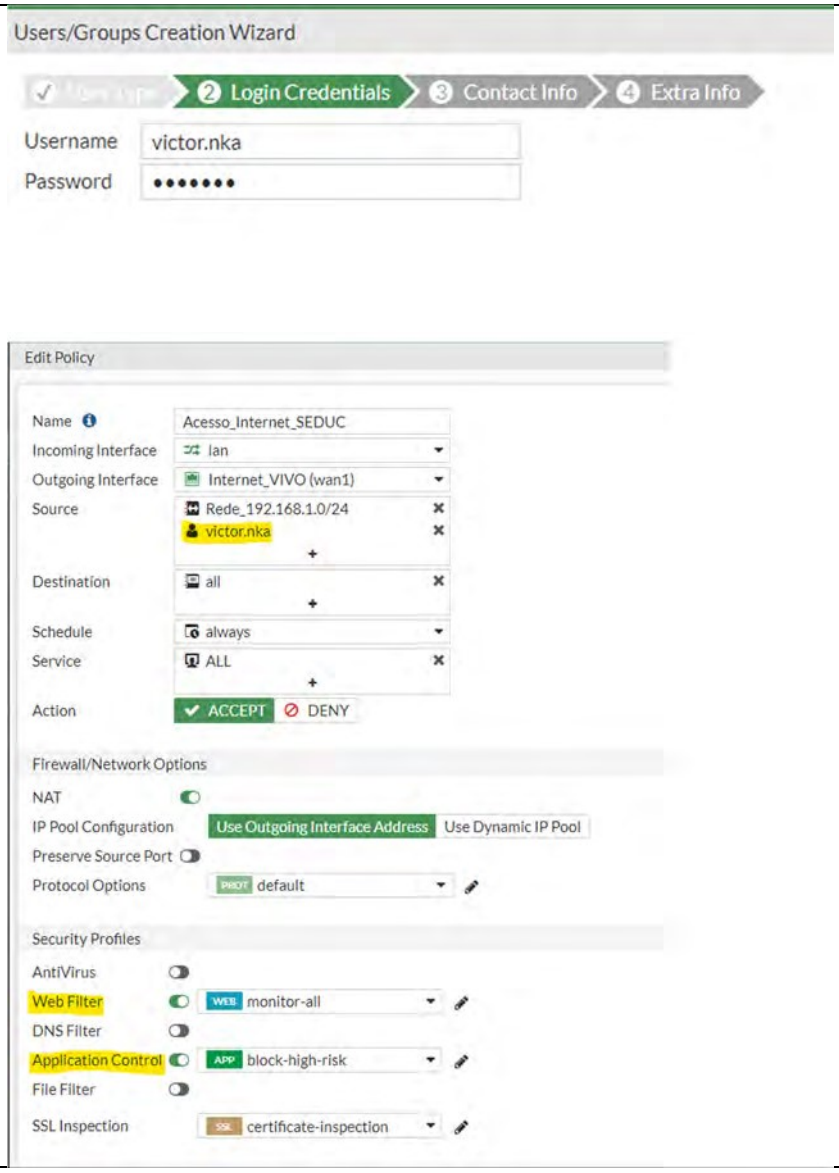
Item de Teste - 5.3.5.9.4	IP/Range de IPs/Redes;
Objetivo do Teste	Validar se o equipamento possibilita a permissão ou bloqueio de aplicações ou URLs pelo critério de IP/Range.
Configuração do Teste	Navegando por Security Profiles > Web filter e Application Control é possível criar perfis de segurança.

Procedimento do Teste	1- Criação de um IP Range 2-Navegando por **Policy & Objects** > **Firewall Policy** > **Source** é possível enquadra o IP Range criado no campo “Source” 3- Por último basta enquadrar um perfil de Web Filter ou Application Control na política.
Evidências	 **TESTE OK** 

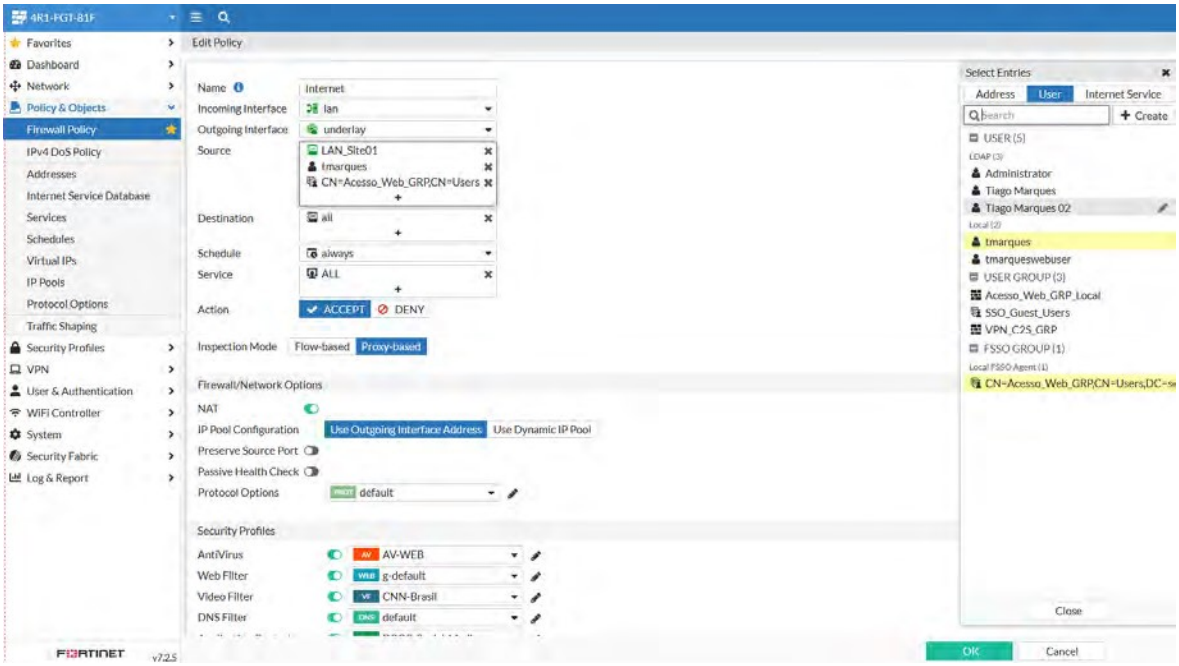
	
Comentário	

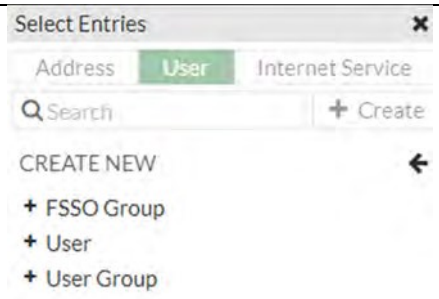
Item de Teste - 5.3.5.9.5	Usuários;
Objetivo do Teste	Validar se o equipamento possibilita a permissão ou bloqueio de aplicações ou URLs pelo critério de usuários
Configuração do Teste	Utilizar usuários do FortiGate para realizar o bloqueio ou permissão de aplicações e URLs
Procedimento do Teste	1 -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

Evidências	 **TESTE OK** 

	
Comentário	

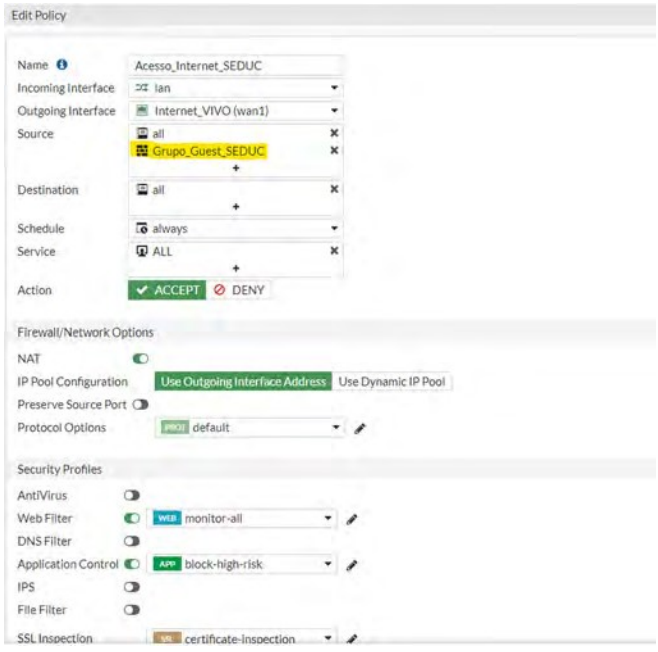
Item de Teste - 5.3.5.9.6	Diferentes grupos de usuários;
Objetivo do Teste	Validar se o equipamento possibilita a permissão ou bloqueio de aplicações ou URLs pelo critério de diferentes grupos de usuários
Configuração do Teste	1 - Criação de um novo grupo de usuários 2 - Navegando por **Policy & Objects**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

Procedimento do Teste	Criar duas regras NGFW com origem de grupos distintos
Evidências	 **TESTE OK** Criando um novo Grupo

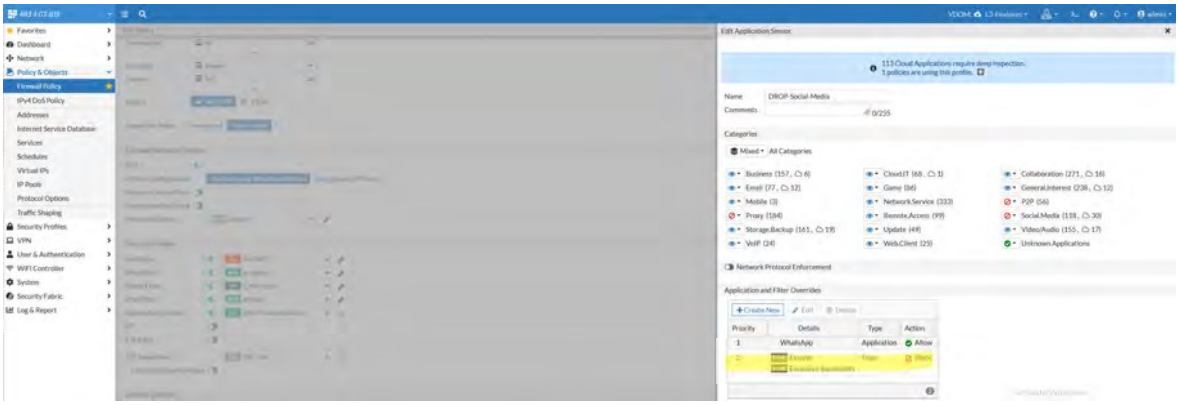
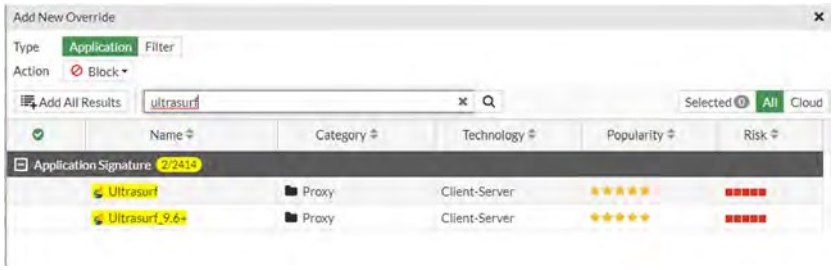


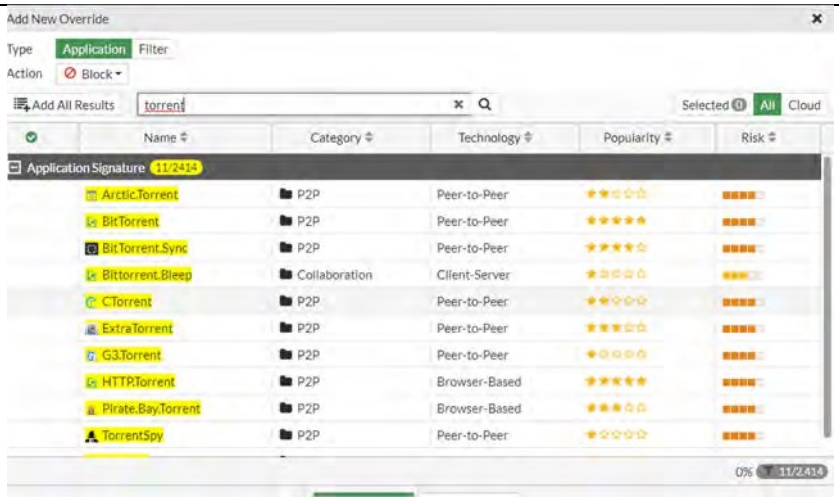
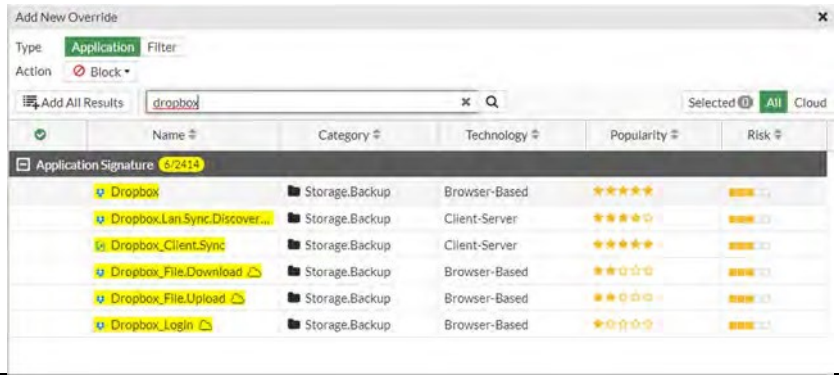
2 – Definindo membros no grupo

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

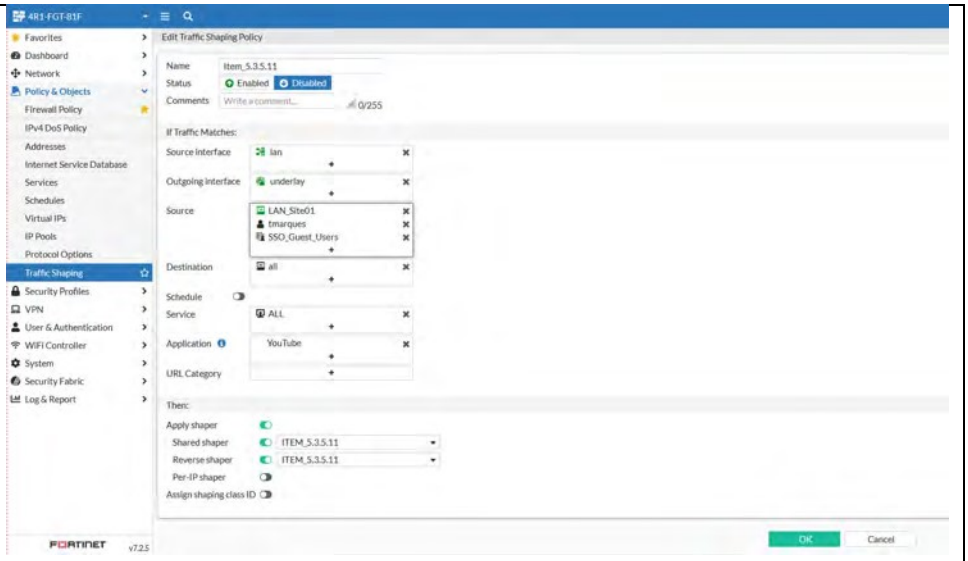


Comentário	

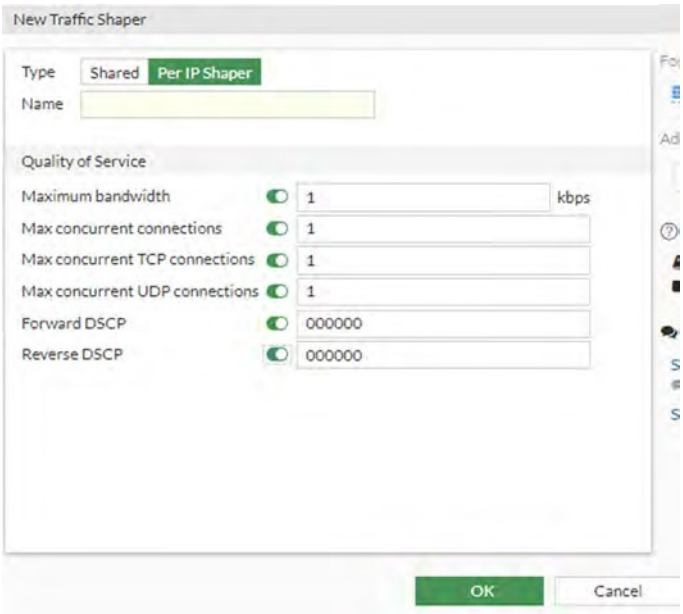
Item de Teste - 5.3.5.10	Aplicações que sejam passiveis a técnicas de evasão por malwares e uso excessivo de banda (EX:ultrasurf, torrent, dropbox e file sharing);
Objetivo do Teste	Validar se o FortiGate consegue bloquear as aplicações passiveis a técnicas de evasão por malwares e uso excessivo de banda.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

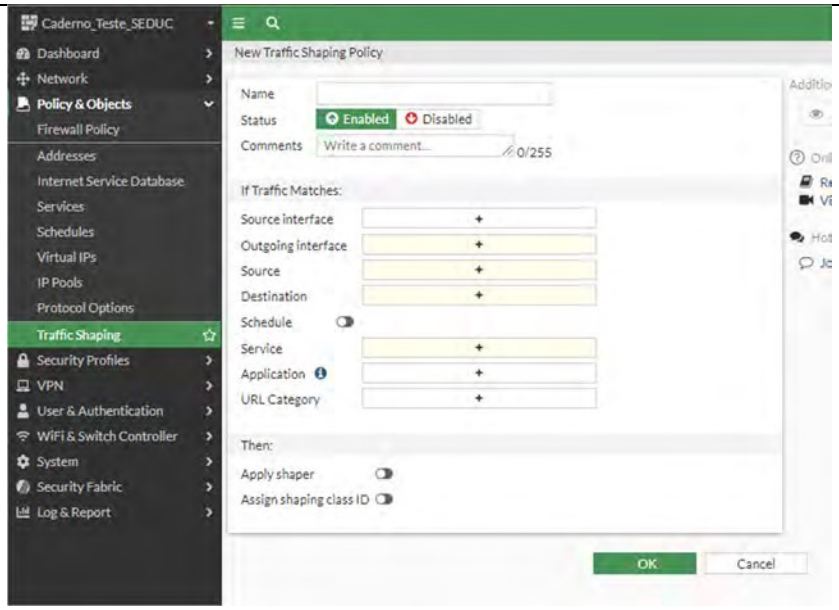
	 
Comentário	

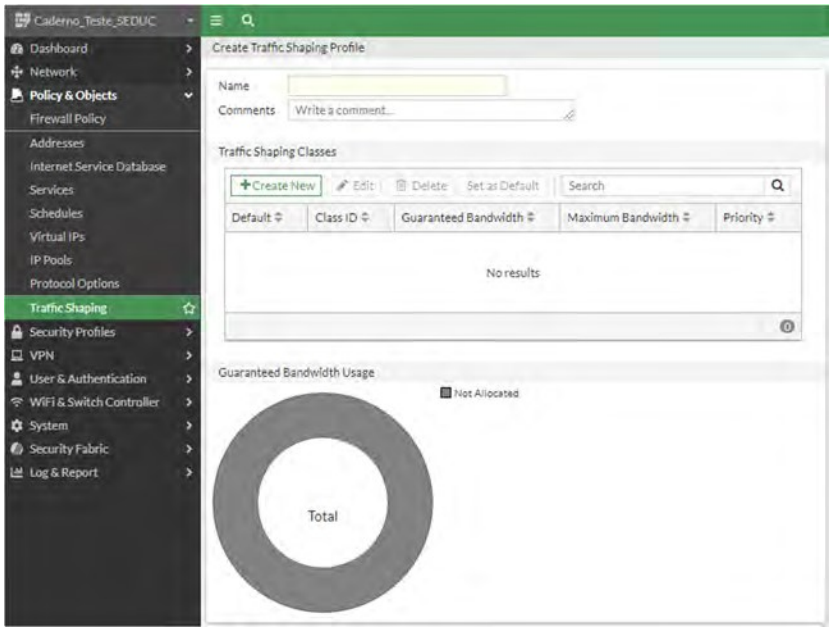
Item de Teste - 5.3.5.11	Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários ou grupos do AD;
Objetivo do Teste	Validar a criação de traffic shaping baseado no IP de origem, usuários ou grupos do AD.
Configuração do Teste	Criar duas regras contendo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

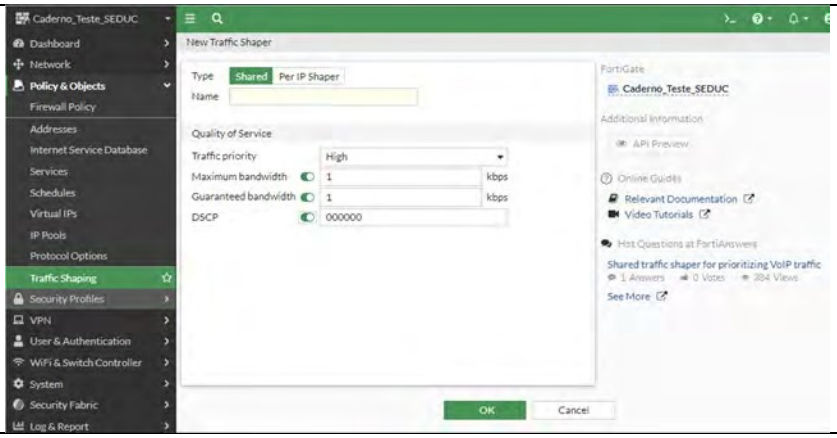

4R1-FGT-81F
Favorites
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
WiFi Controller
System
Security Fabric
Log & Report
Edit Traffic Shaping Policy
Name
Item_5.3.5.11
Status
Enabled
Disabled
Comments
0/255
If Traffic Matches:
Source Interface
lan
Outgoing Interface
underlay
Source
LAN_Site01
tmarques
SSO_Guest_Users
Destination
all
Schedule
Service
ALL
Application
YouTube
URL Category
Then:
Apply shaper
Shared shaper
ITEM_5.3.5.11
Reverse shaper
ITEM_5.3.5.11
Per-IP shaper
Assign shaping class ID
FORTINET
v7.2.5
OK
Cancel

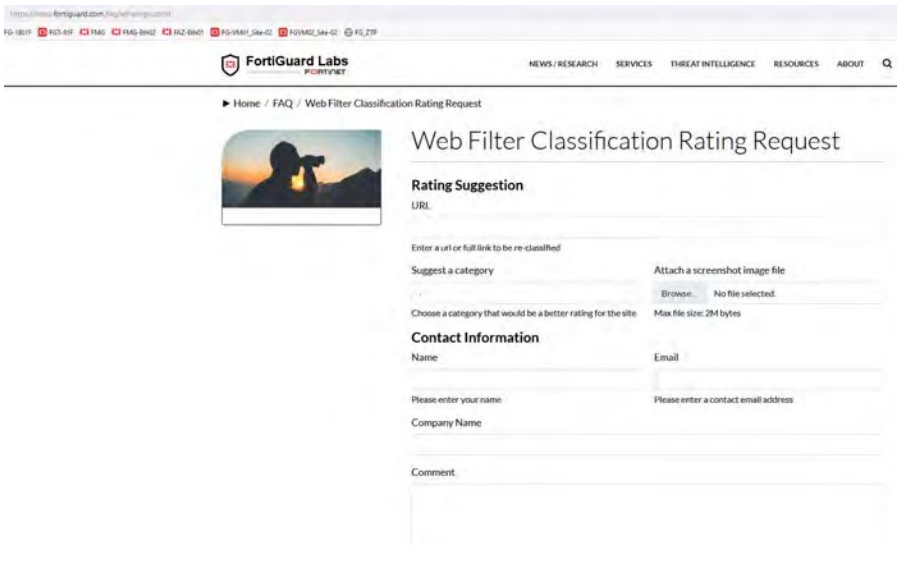
TESTE OK

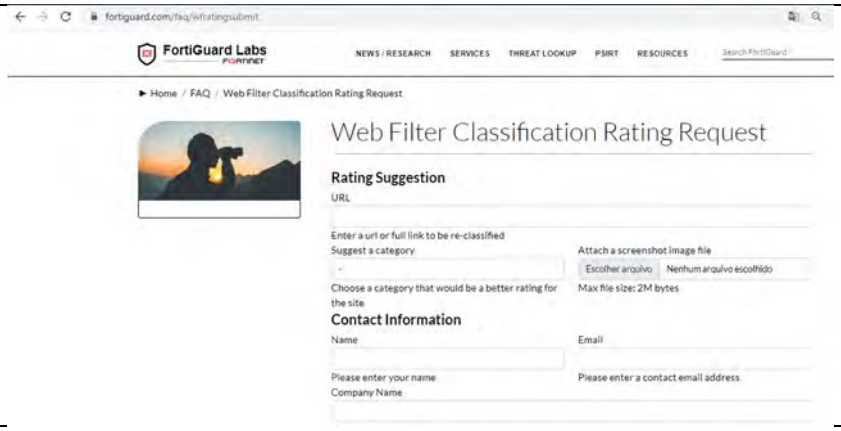

New Traffic Shaper
Type
Shared
Per IP Shaper
Name
Quality of Service
Maximum bandwidth
1
kbps
Max concurrent connections
1
Max concurrent TCP connections
1
Max concurrent UDP connections
1
Forward DSCP
000000
Reverse DSCP
000000
OK
Cancel

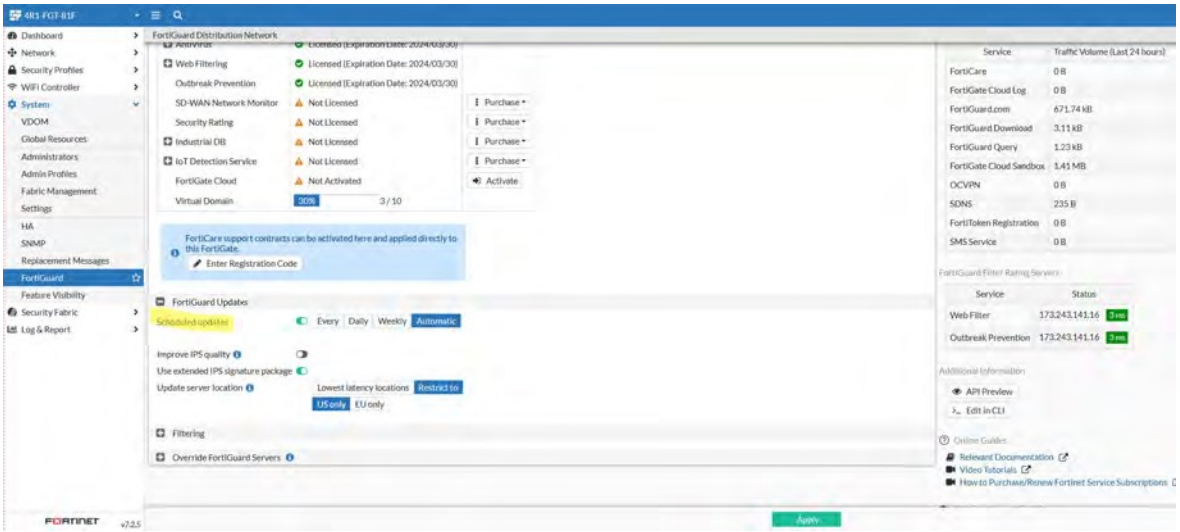

Caderno_Teste_SEDUC
Dashboard
Network
Policy & Objects
Firewall Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
WiFi & Switch Controller
System
Security Fabric
Log & Report
New Traffic Shaping Policy
Name
Status
Enabled
Disabled
Comments
Write a comment...
0/255
If Traffic Matches:
Source interface
Outgoing interface
Source
Destination
Schedule
Service
Application
URL Category
Then:
Apply shaper
Assign shaping class ID
OK
Cancel

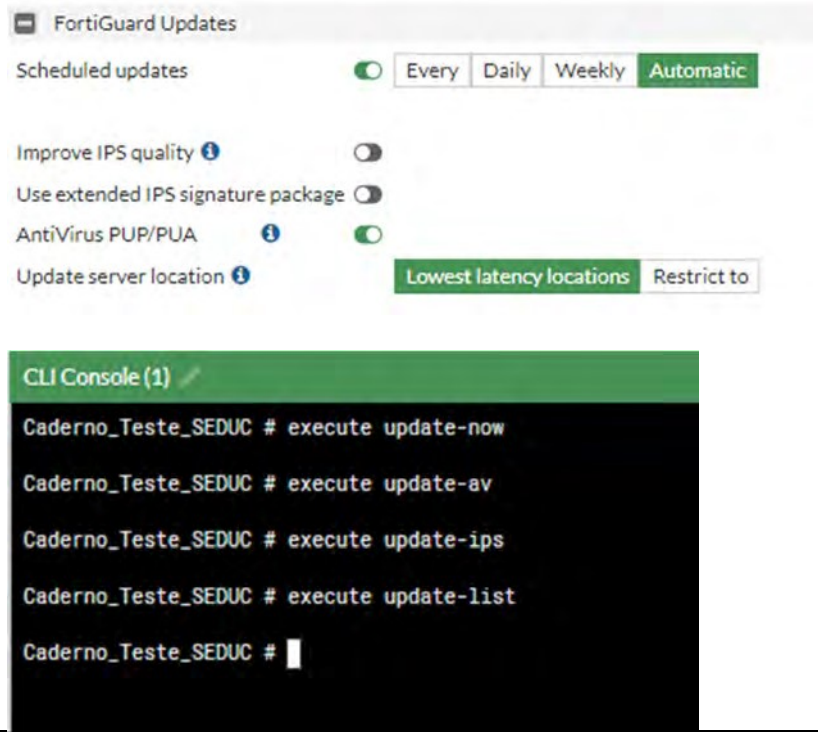

Caderno_Teste_SEDUC
Dashboard
Network
Policy & Objects
Firewall Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
WiFi & Switch Controller
System
Security Fabric
Log & Report
Create Traffic Shaping Profile
Name
Comments
Write a comment...
Traffic Shaping Classes
+Create New
Edit
Delete
Set as Default
Search
Default
Class ID
Guaranteed Bandwidth
Maximum Bandwidth
Priority
No results
Guaranteed Bandwidth Usage
Not Allocated
Total

	
Comentário	

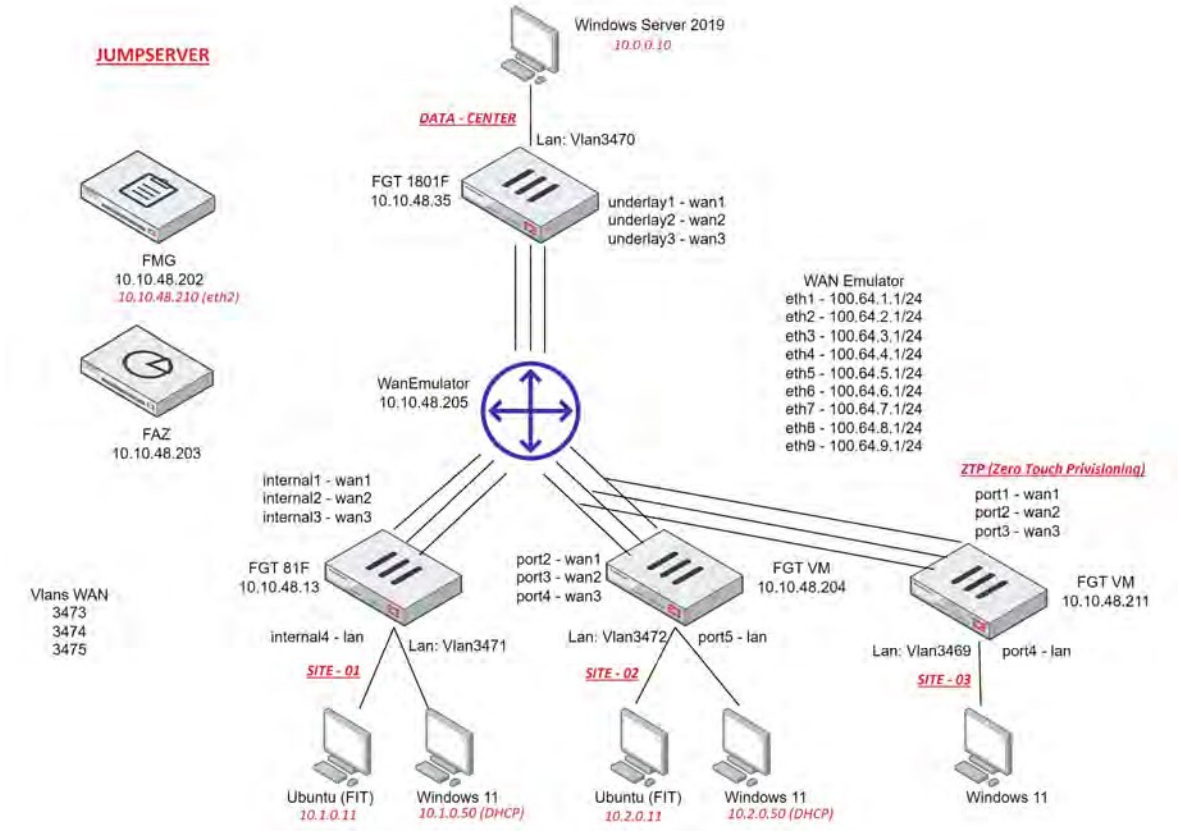
Item de Teste - 5.3.5.12	A solução deve fornecer uma forma para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;
Objetivo do Teste	Validar se a solução fornece uma forma para solicitação de categorização de URL caso a mesma não esteja categorizada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

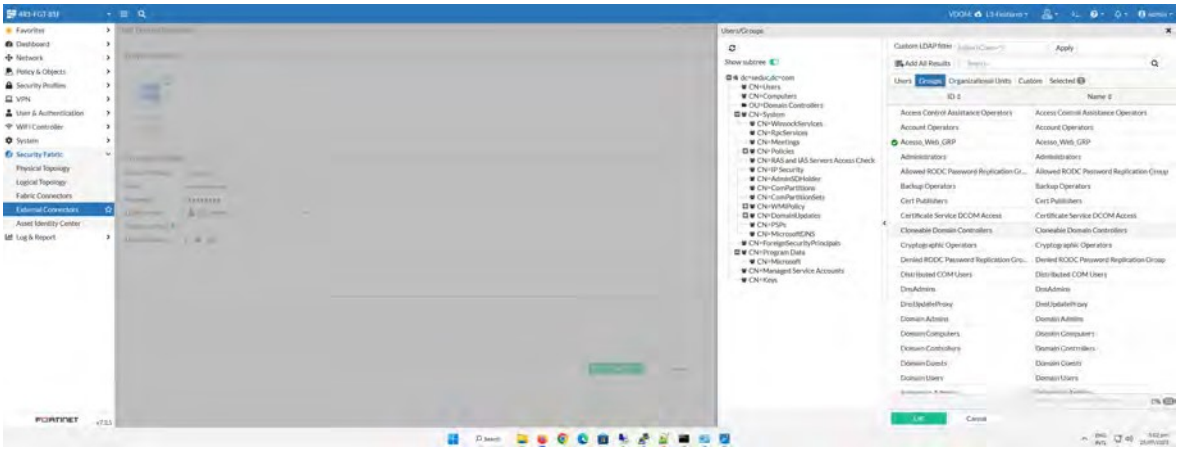
	
Comentário	

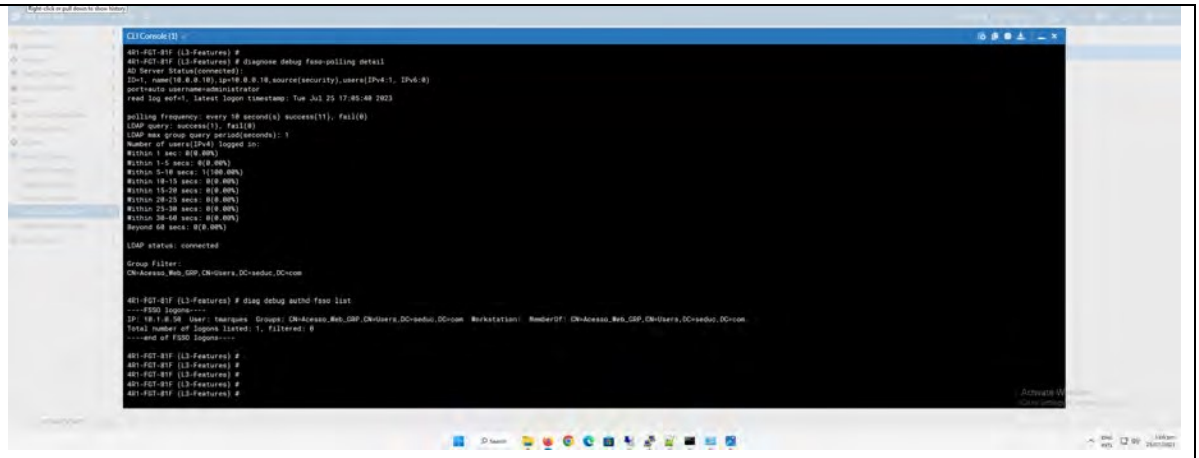
Item de Teste - 5.3.5.13	Deve atualizar a base de assinaturas de aplicações automaticamente sem a necessidade de reboot nos gateways e no módulo de gerência;
Objetivo do Teste	Validar se a solução atualiza a base de assinaturas de aplicações automaticamente e sem a necessidade de reboot nos gateways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

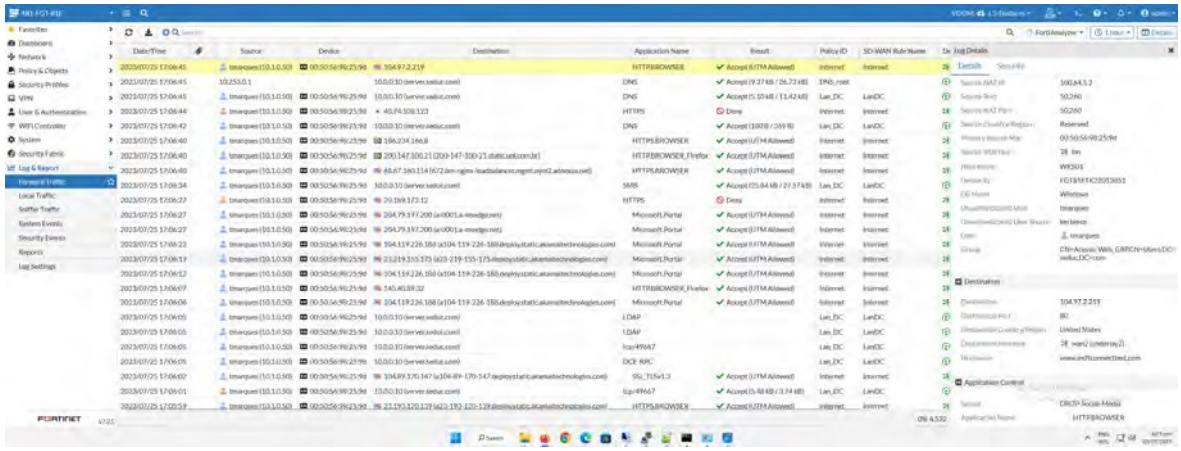
	
Comentário	

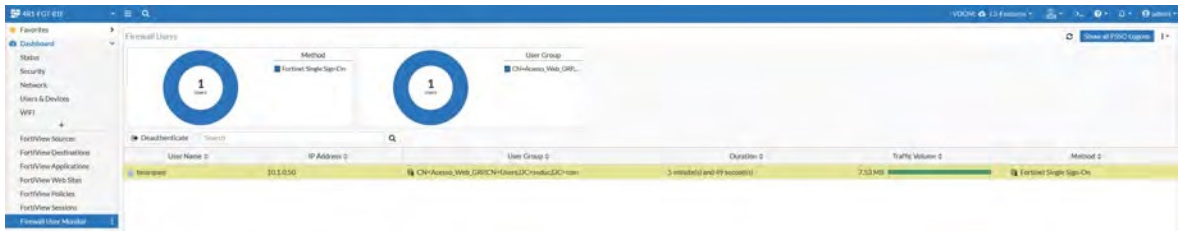
Item de Teste - 5.3.5.14	Deve possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
Objetivo do Teste	Validar se a ferramenta é capaz de identificar o usuário de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

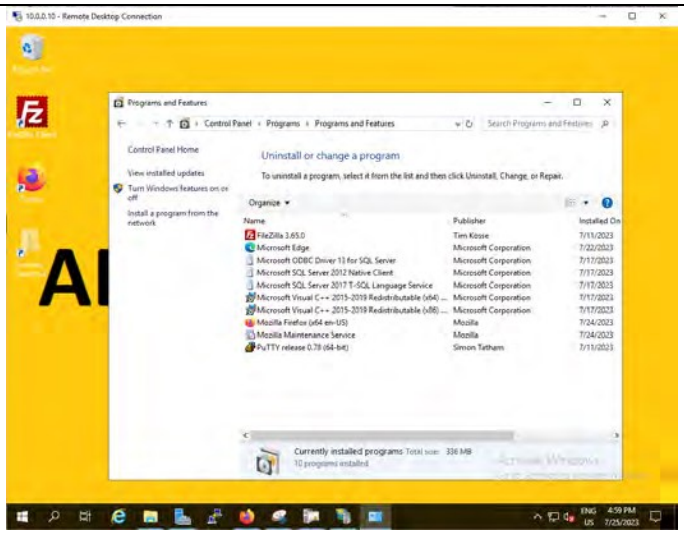

JUMPSERVER
Windows Server 2019
10.0.0.10
DATA - CENTER
Lan: Vlan3470
FGT 1801F
10.10.48.35
underlay1 - wan1
underlay2 - wan2
underlay3 - wan3
FMG
10.10.48.202
10.10.48.210 (eth2)
FAZ
10.10.48.203
WAN Emulator
eth1 - 100.64.1.1/24
eth2 - 100.64.2.1/24
eth3 - 100.64.3.1/24
eth4 - 100.64.4.1/24
eth5 - 100.64.5.1/24
eth6 - 100.64.6.1/24
eth7 - 100.64.7.1/24
eth8 - 100.64.8.1/24
eth9 - 100.64.9.1/24
WanEmulator
10.10.48.205
ZTP (Zero Touch Privisioning)
internal1 - wan1
internal2 - wan2
internal3 - wan3
port1 - wan1
port2 - wan2
port3 - wan3
FGT 81F
10.10.48.13
port2 - wan1
port3 - wan2
port4 - wan3
FGT VM
10.10.48.204
FGT VM
10.10.48.211
Vlans WAN
3473
3474
3475
internal4 - lan
Lan: Vlan3471
SITE - 01
Lan: Vlan3472
port5 - lan
SITE - 02
Lan: Vlan3469
port4 - lan
SITE - 03
Ubuntu (FIT)
10.1.0.11
Windows 11
10.1.0.50 (DHCP)
Ubuntu (FIT)
10.2.0.11
Windows 11
10.2.0.50 (DHCP)
Windows 11

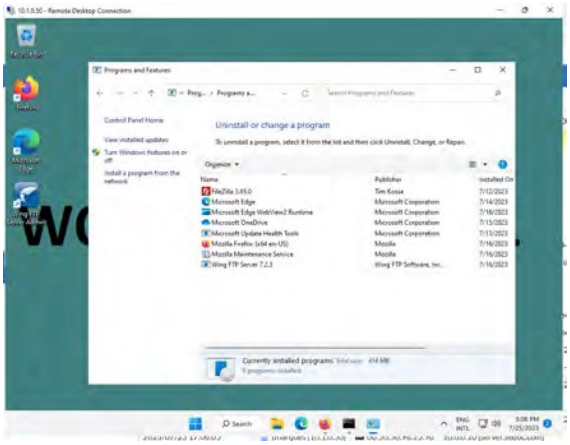




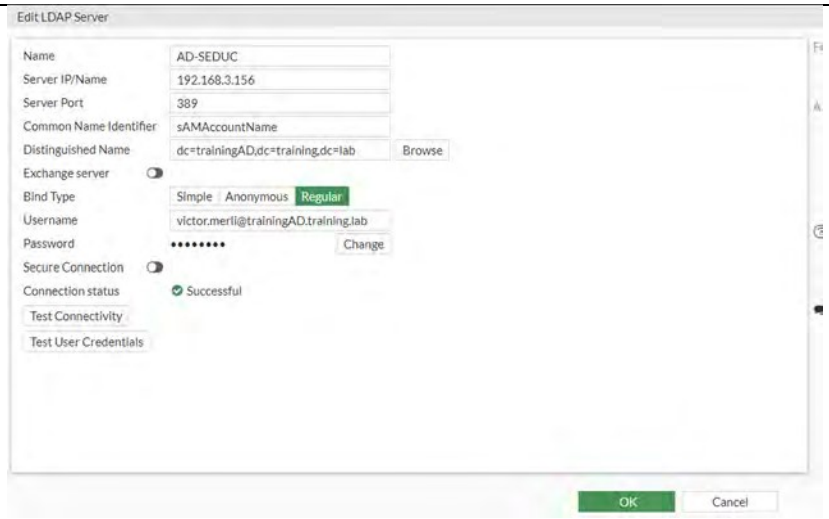


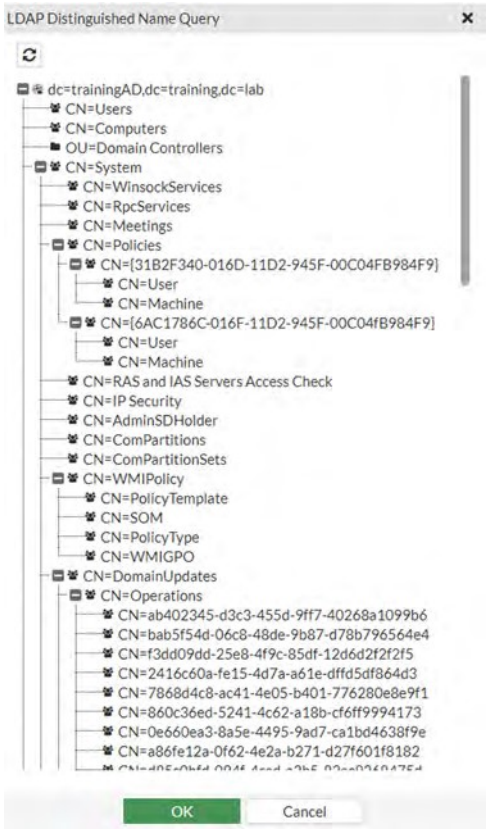


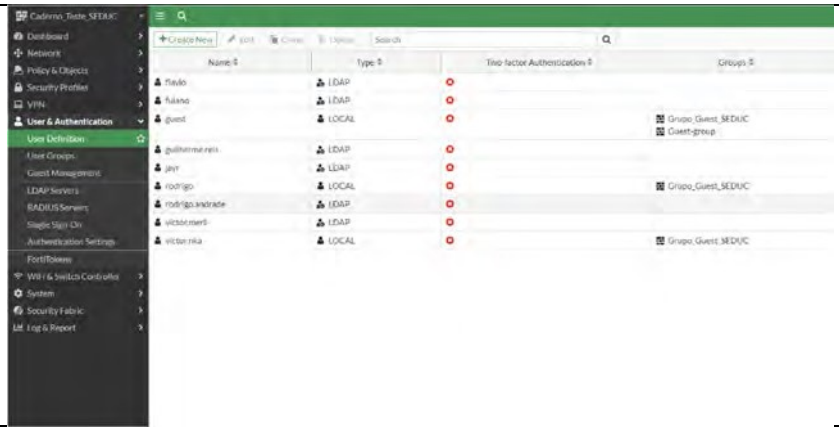

Programs and Features
Control Panel Home
Uninstall or change a program
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.
Organize
Name
Publisher
Installed On
FileZilla 3.65.0
Microsoft Edge
Microsoft ODBC Driver 13 for SQL Server
Microsoft SQL Server 2012 Native Client
Microsoft SQL Server 2017 T-SQL Language Service
Microsoft Visual C++ 2015-2019 Redistributable (x64) ...
Microsoft Visual C++ 2015-2019 Redistributable (x86) ...
Mozilla Firefox (x64 en-US)
Mozilla Maintenance Service
PuTTY release 0.78 (64-bit)
Tim Kosse
Microsoft Corporation
Mozilla
Simon Tatham
Currently installed programs
10 programs installed


Programs and Features
Uninstall or change a program

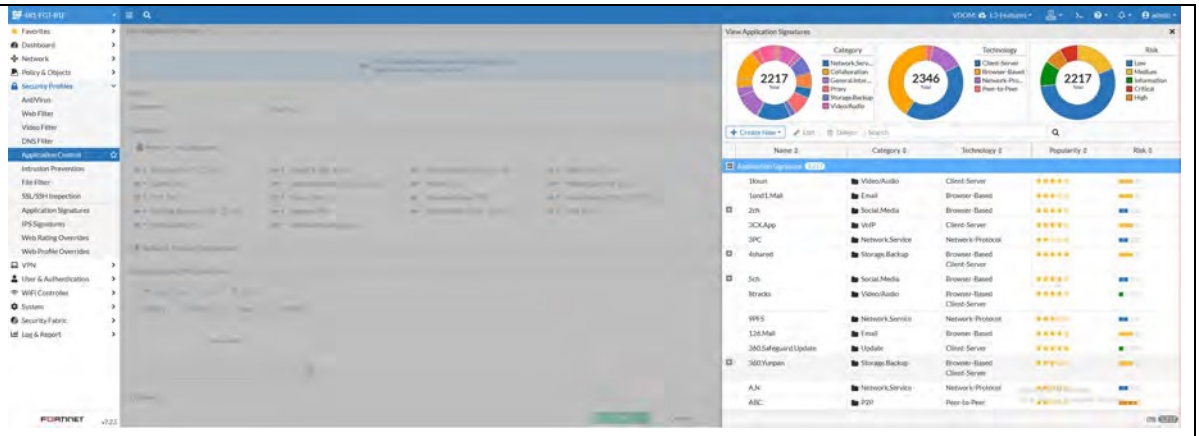
TESTE OK

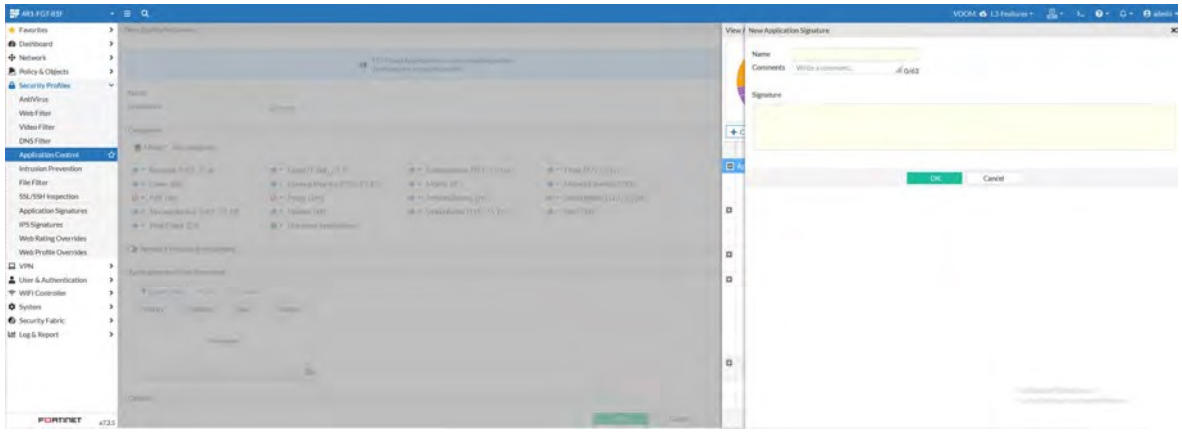

Edit LDAP Server
Name
AD-SEDUC
Server IP/Name
192.168.3.156
Server Port
389
Common Name Identifier
sAMAccountName
Distinguished Name
dc=trainingAD,dc=training,dc=lab
Browse
Exchange server
Bind Type
Simple
Anonymous
Regular
Username
victor.merli@trainingAD.training.lab
Password
Change
Secure Connection
Connection status
Successful
Test Connectivity
Test User Credentials
OK
Cancel


LDAP Distinguished Name Query
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-12d6d2f2f2f5
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
OK
Cancel

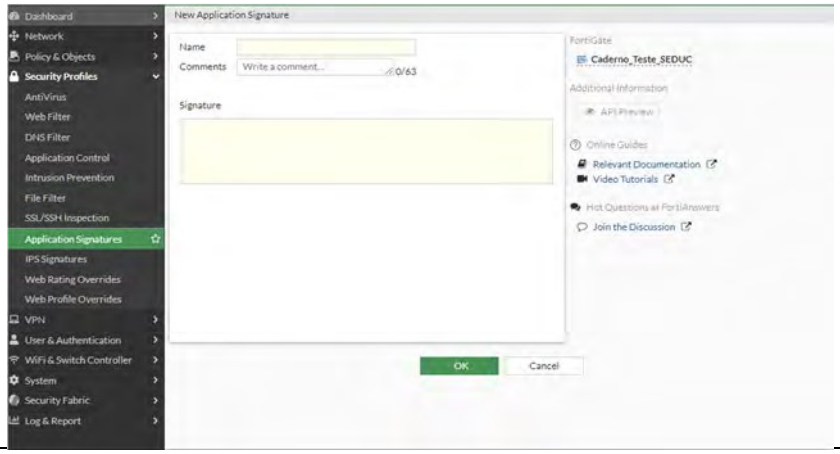
	
Comentário	

Item de Teste - 5.3.5.15	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;
Objetivo do Teste	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.
Configuração do Teste	Demonstrar capacidade de criação de aplicação
Procedimento do Teste	1 – Validar o controle de aplicações feito em assinaturas já conhecidas pela ferramenta. 2 – Realizar a criação de uma nova assinatura. Navegando por **Security Profiles** > **Application Signatures** > **Create New** é possível criar novas assinaturas de aplicações customizadas, ou utilizar as mais de 2414 assinaturas conhecidas. 1 – Navegando por **Security Profiles** > **Application signatures** é possível visualizar as assinaturas já conhecidas pela Fabricante. 2 – Navegando por **Security Profiles** > **Application signatures** > **Create New** é possível criar novas assinaturas para aplicações não conhecidas pela fabricante.
Evidências	


View Application Signatures
2217
2346
2217

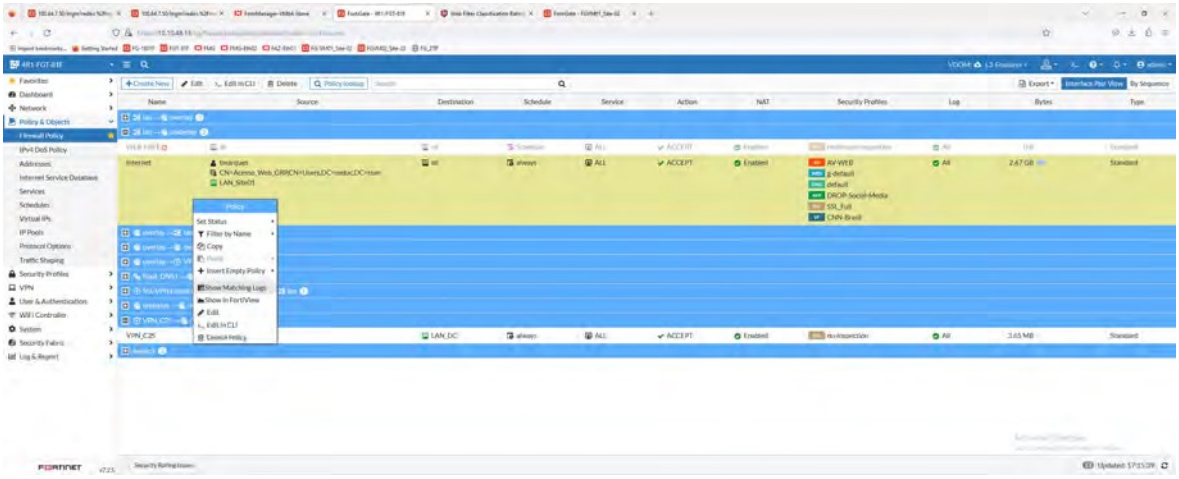
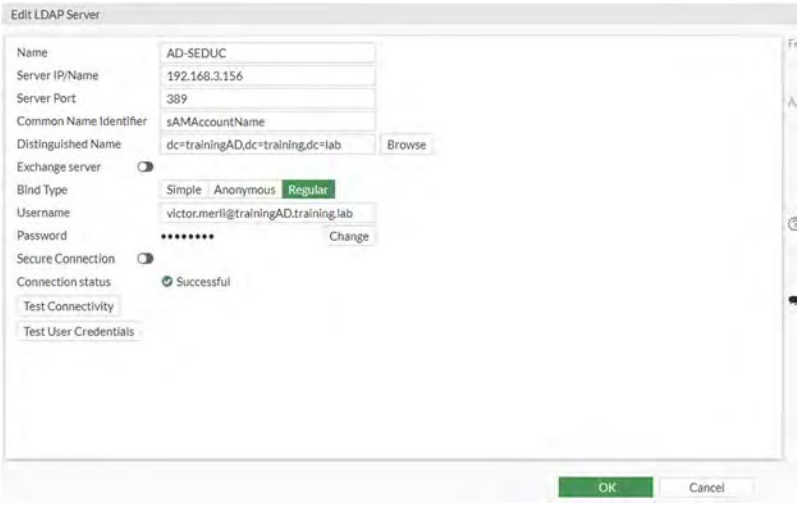

New Application Signature
Name
Comments
Signature
OK
Cancel

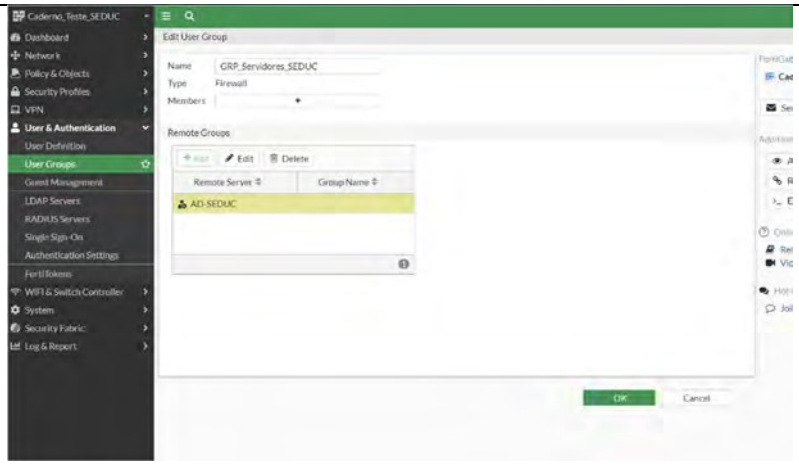
TESTE OK

	 
Comentário	

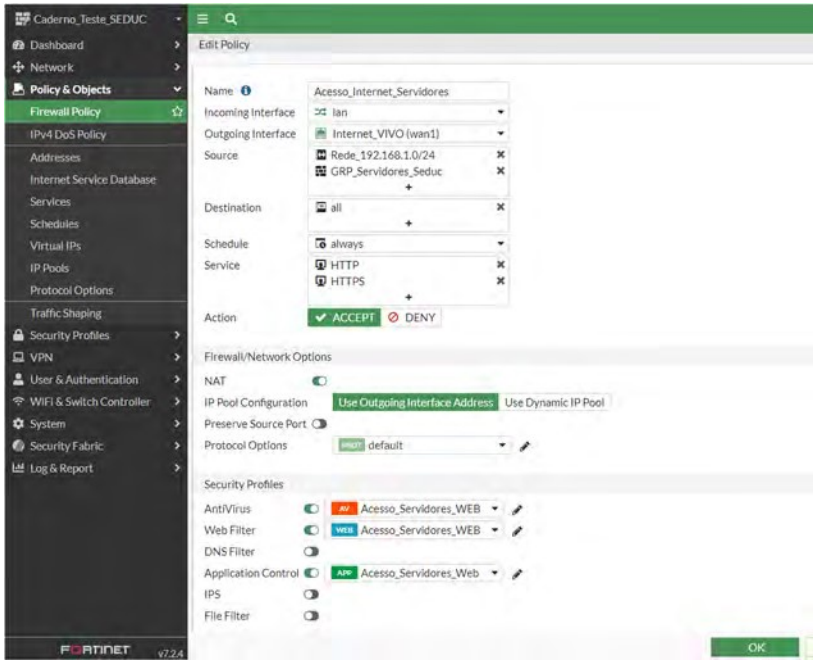
5.3.6 IDENTIFICAÇÃO DE USUÁRIOS:

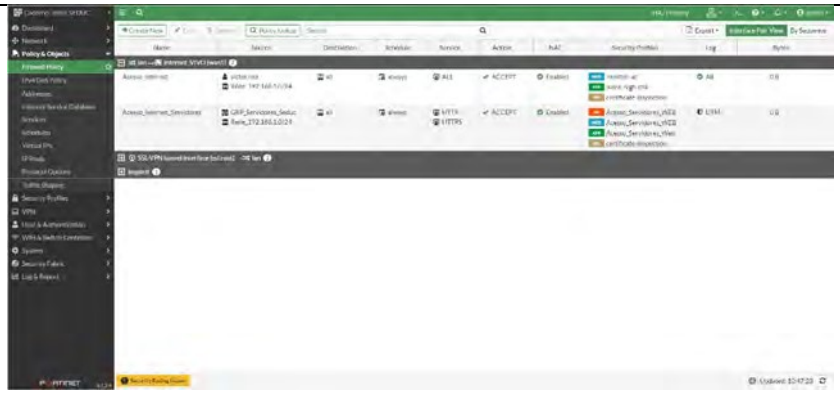
Item de Teste - 5.3.6.1	Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório;
Objetivo do Teste	Validar se a ferramenta tem a capacidade de realizar o controle de qual usuário está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

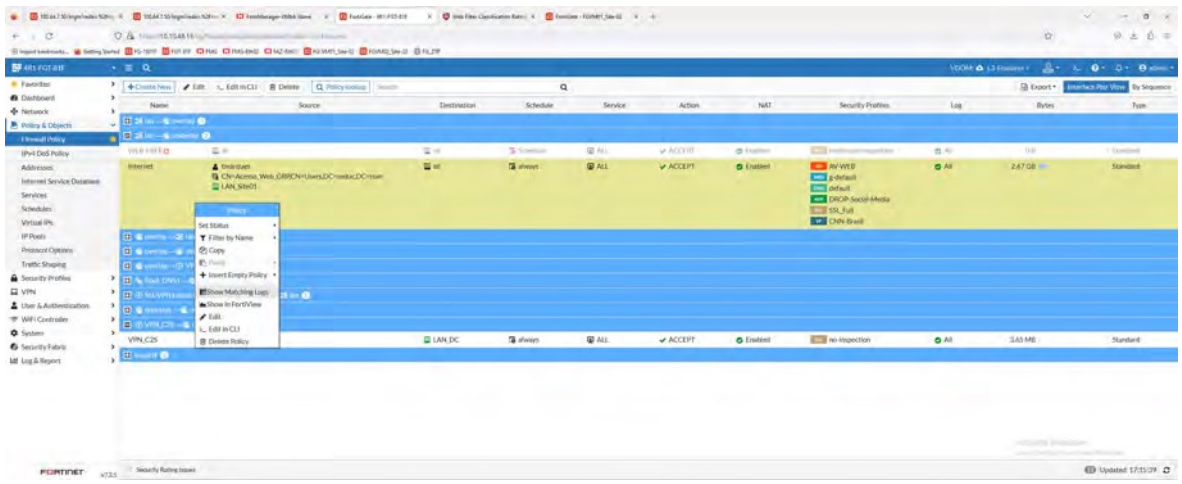
	Navegando por **Policy & Objects > Firewall Policy** é possível realizar a criação de regras utilizando como origem o grupo criado com a integração do AD; Navegando por **Policy & Objects > Firewall Policy** podemos criar uma nova política utilizando o grupo do firewall no campo “source”. Na mesma política podemos incluir profiles de segurança específicos para os grupos.
Evidências	 **TESTE OK** 1 - Integração com AD via LDAP  2 - Criação de um novo grupo no Firewall que utilizando a integração com o AD.



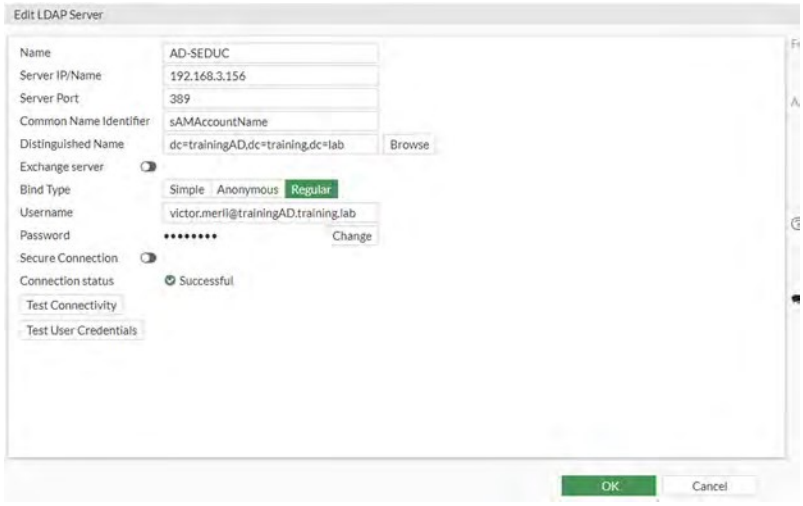
3- Criação de uma política com filtro de aplicação e web



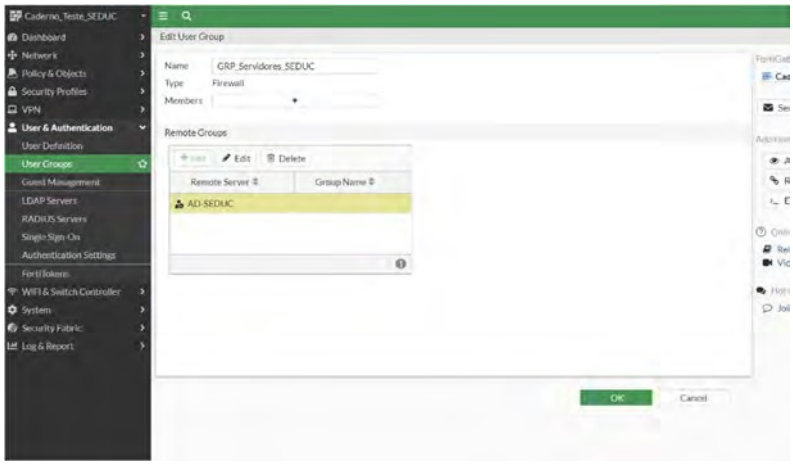
	
Comentário	Fonte: https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/656084/firewall-policy

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	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. 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.
Evidências	 **TESTE OK**

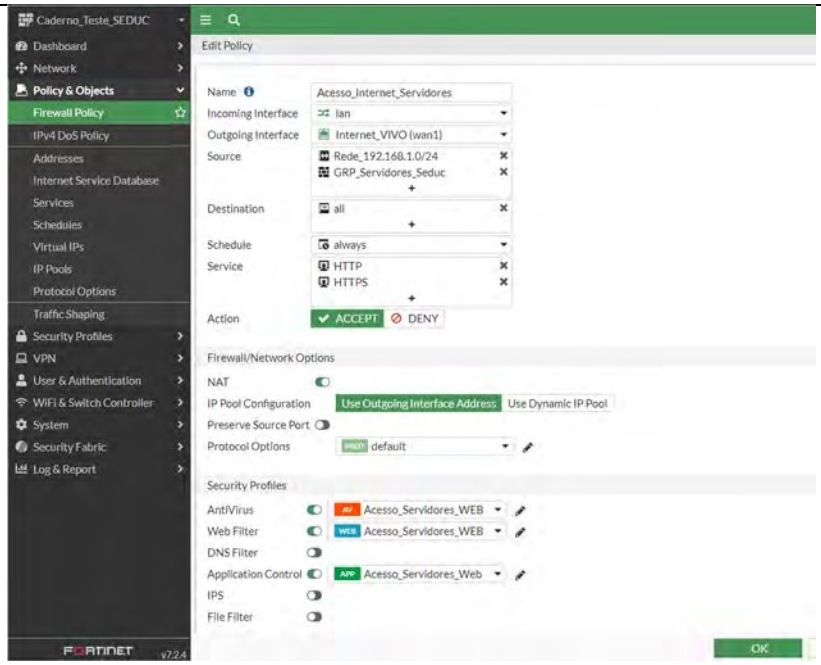
1 - Integração com AD via LDAP



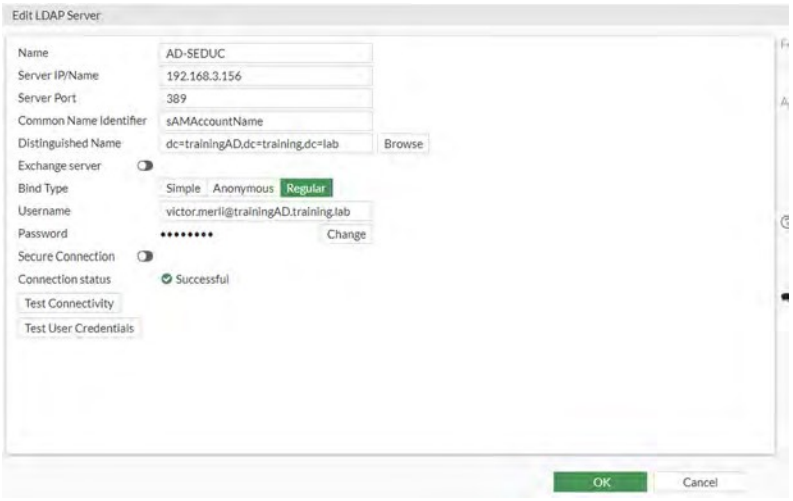
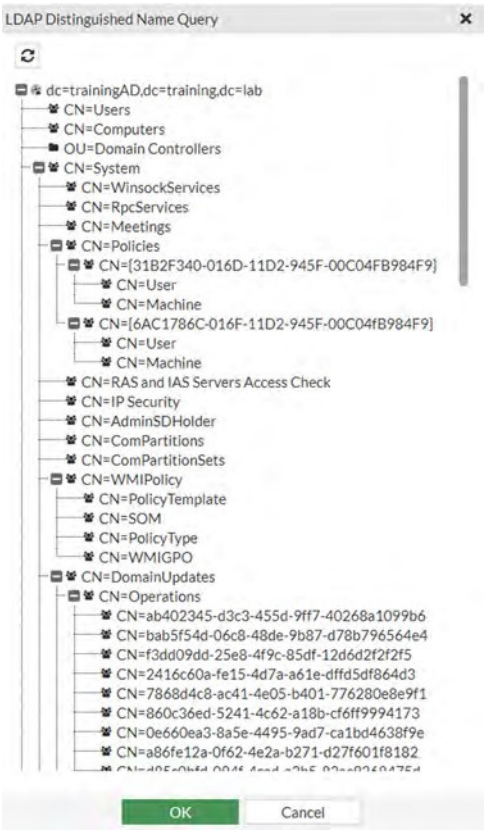
2 - Criação de um novo grupo no Firewall que utilizando a integração com o AD.

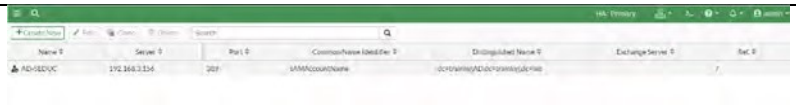


3 – Navegando por Policy & Objects > Firewall Policy é possível realizar a criação de regras utilizando como origem o grupo criado com a integração do AD

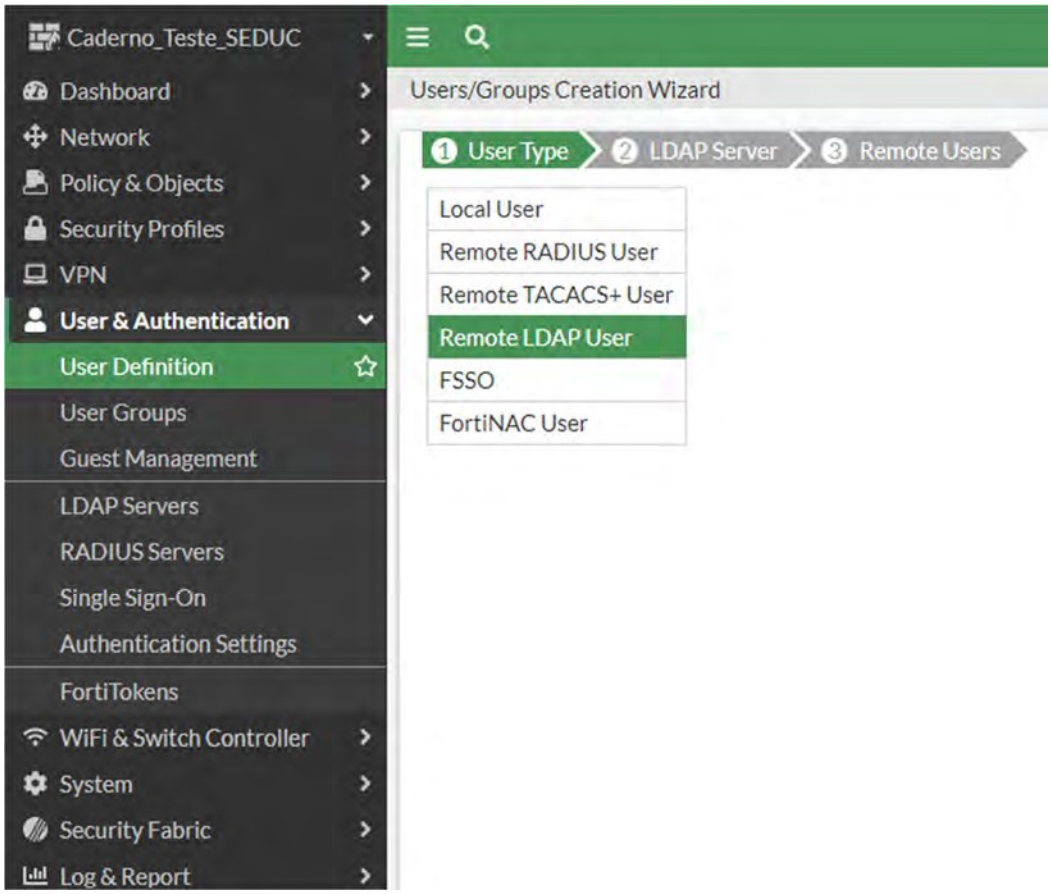
	 
Comentário	

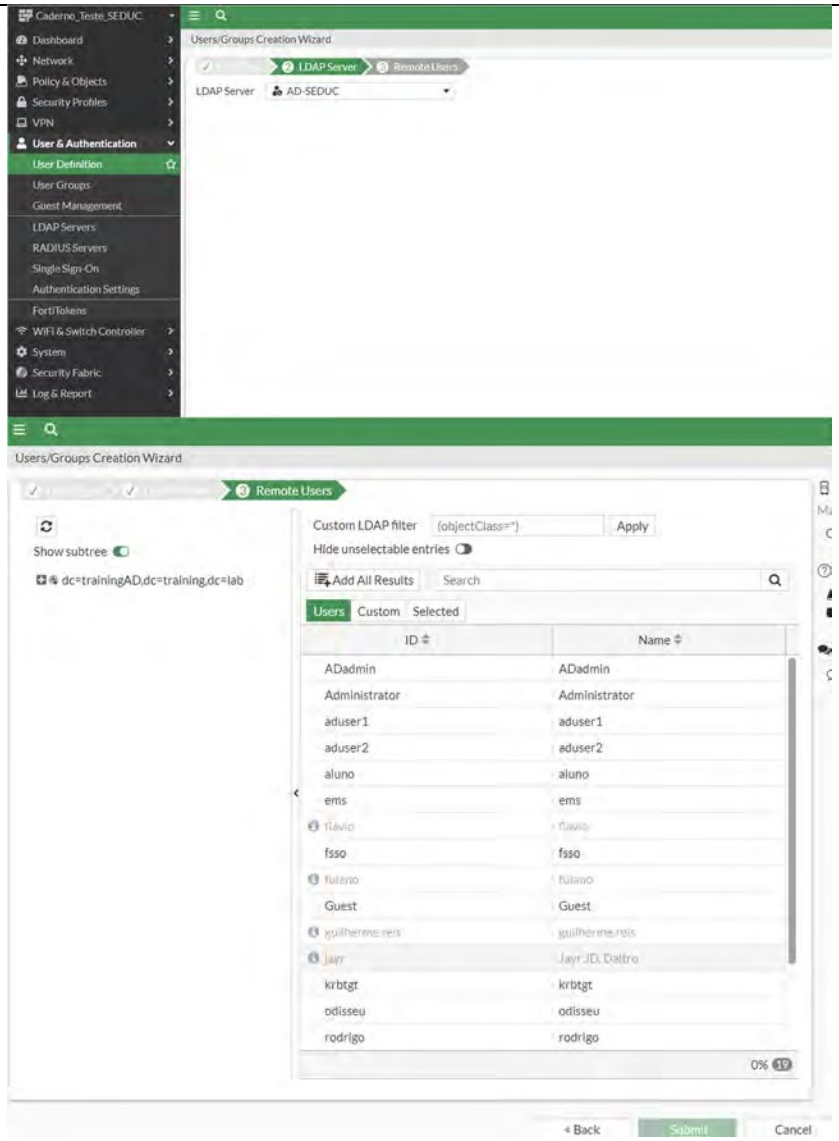
Item de Teste - 5.3.6.3	A identificação do usuário registrado no Microsoft Active Directory deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;
Objetivo do Teste	Validar se a identificação do usuário registrado no Microsoft Active Directory ocorre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

Evidências	ITEM COMPROVADO CONFORME SUBITEM 5.3.5.14 **TESTE OK** Conectando o FortiGate ao Active Directory  



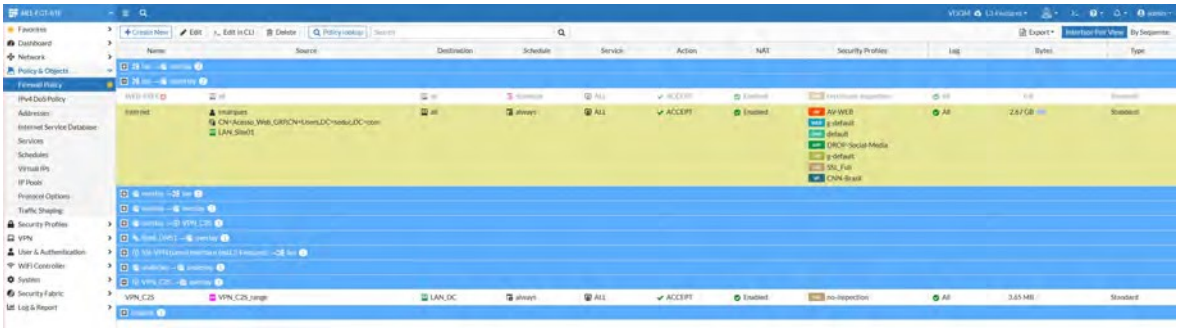
2 – Criando grupo no Firewall utilizando grupos do AD.

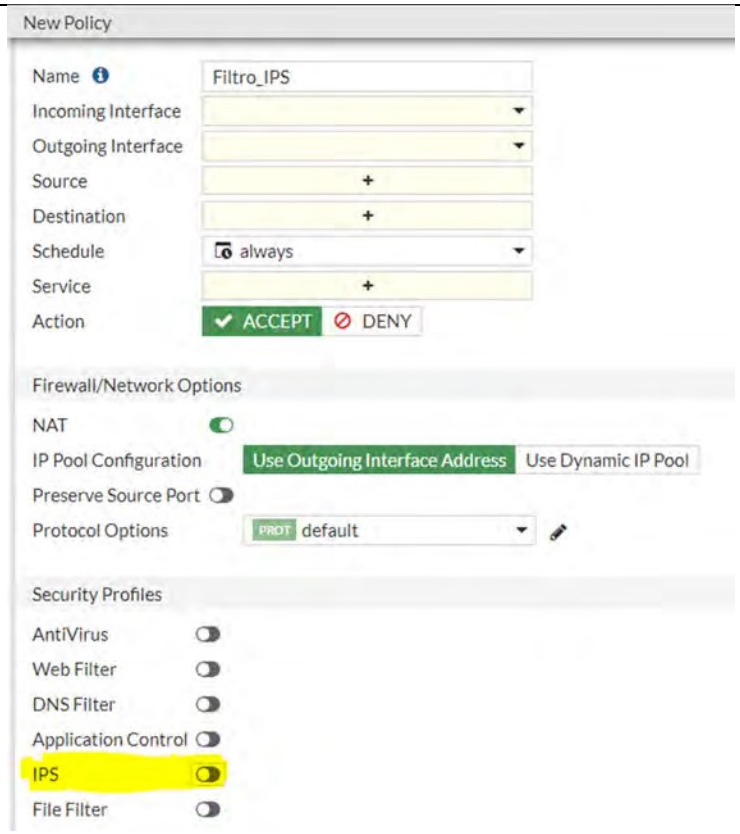


	
Comentário	

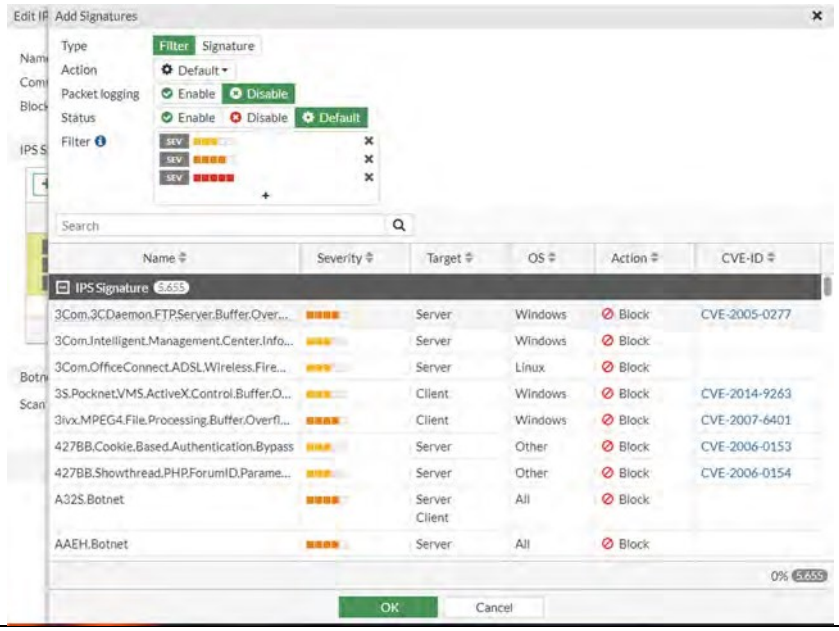
5.3.7 SISTEMA DE PREVENÇÃO DE INTRUSÃO - IPS:

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.

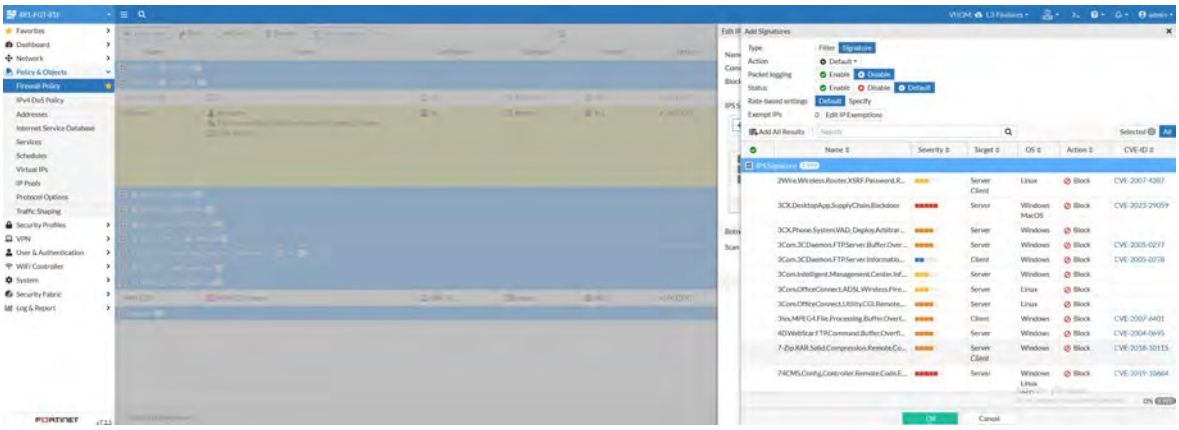
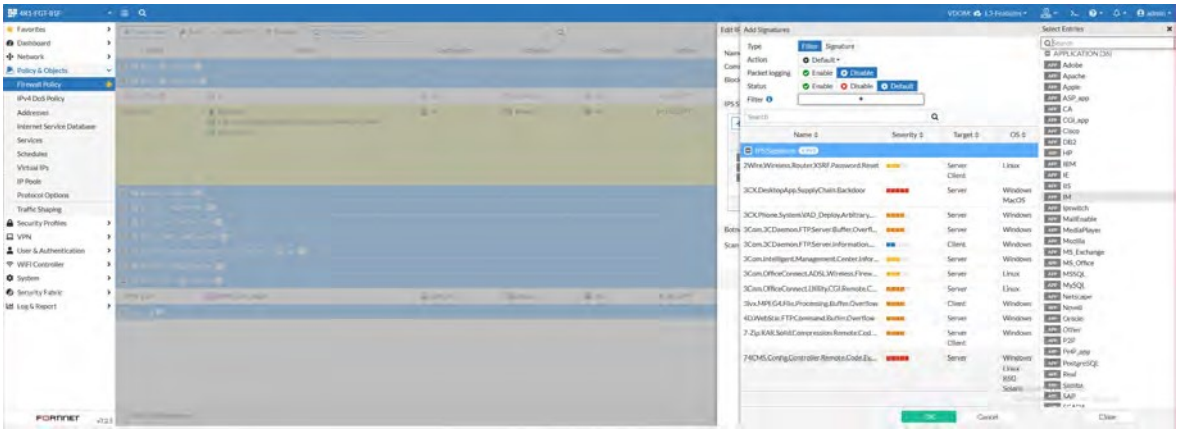
Evidências	  **TESTE OK** Dentro de uma política de segurança podemos notar a presença do Filtro IPS.

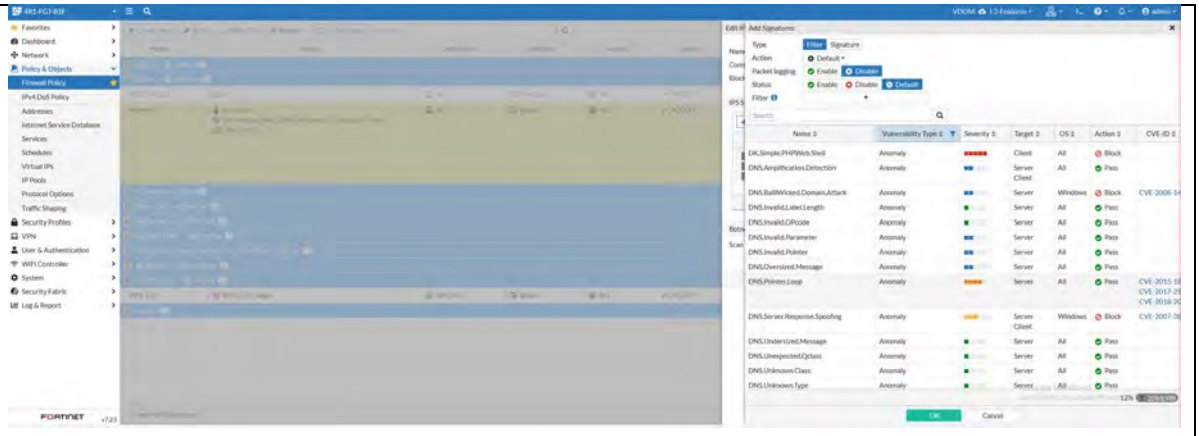


E dentro desse perfil de segurança podemos ter acesso a todas as assinaturas que ele conhece, como também o CVE daquela vulnerabilidade, a ação padrão e por fim o grau de severidade dela.



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 possuí 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	 

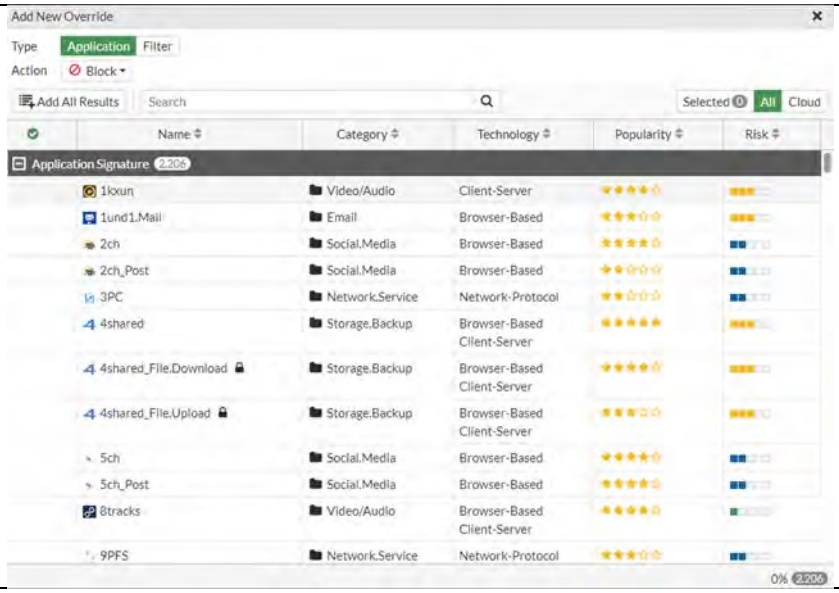


TESTE OK

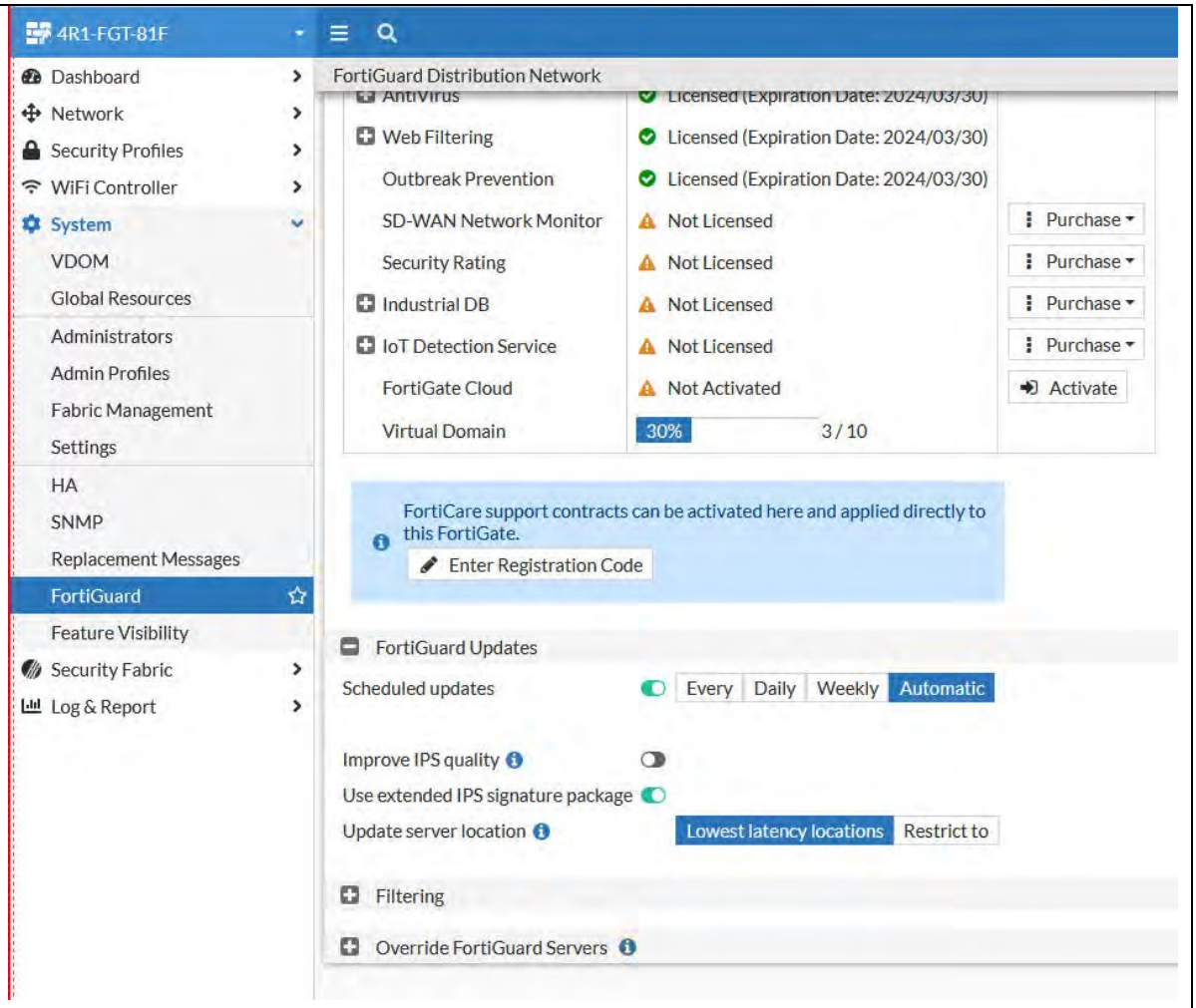
Nessa parte podemos ter visibilidade de todas as assinaturas que o filtro IPS possui naquele momento, sendo possível adicionar assinaturas novas sem contar as que são adicionadas frequentemente pelo FortiGuard.

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.

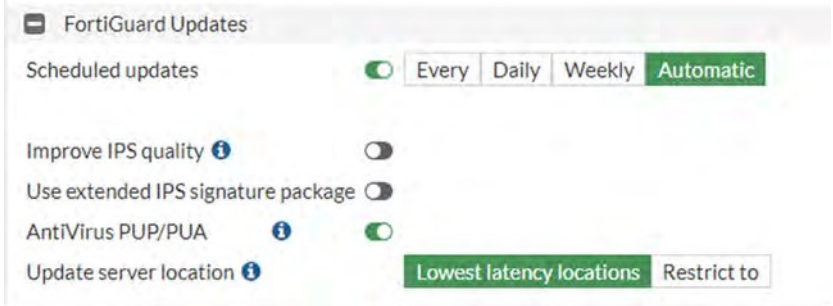
Já o mecanismo de controle de aplicação é feito pelo Application Control.

	
Comentário	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

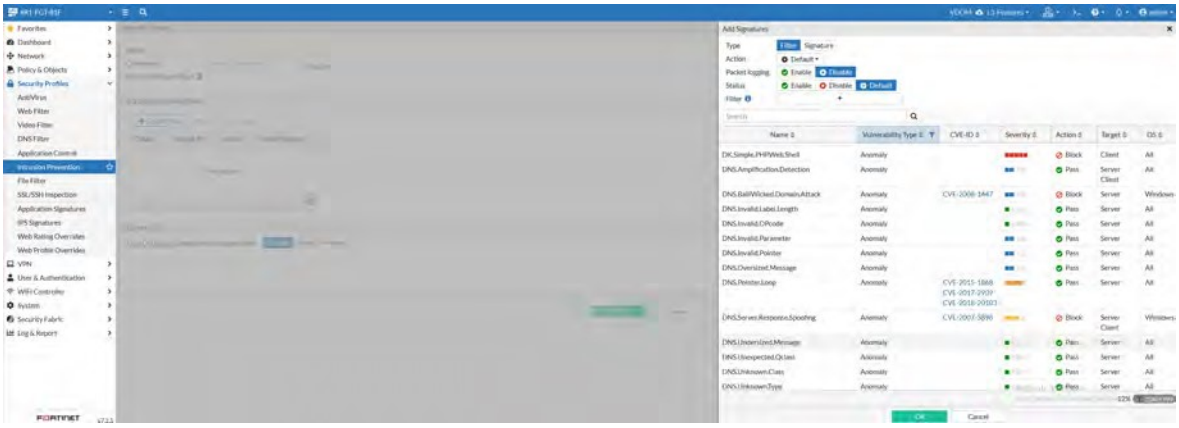
Item de Teste - 5.3.7.3	O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;
Objetivo do Teste	Verificar se a ferramenta recebe e implementa em tempo real atualizações para os ataques emergentes sem a necessidade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



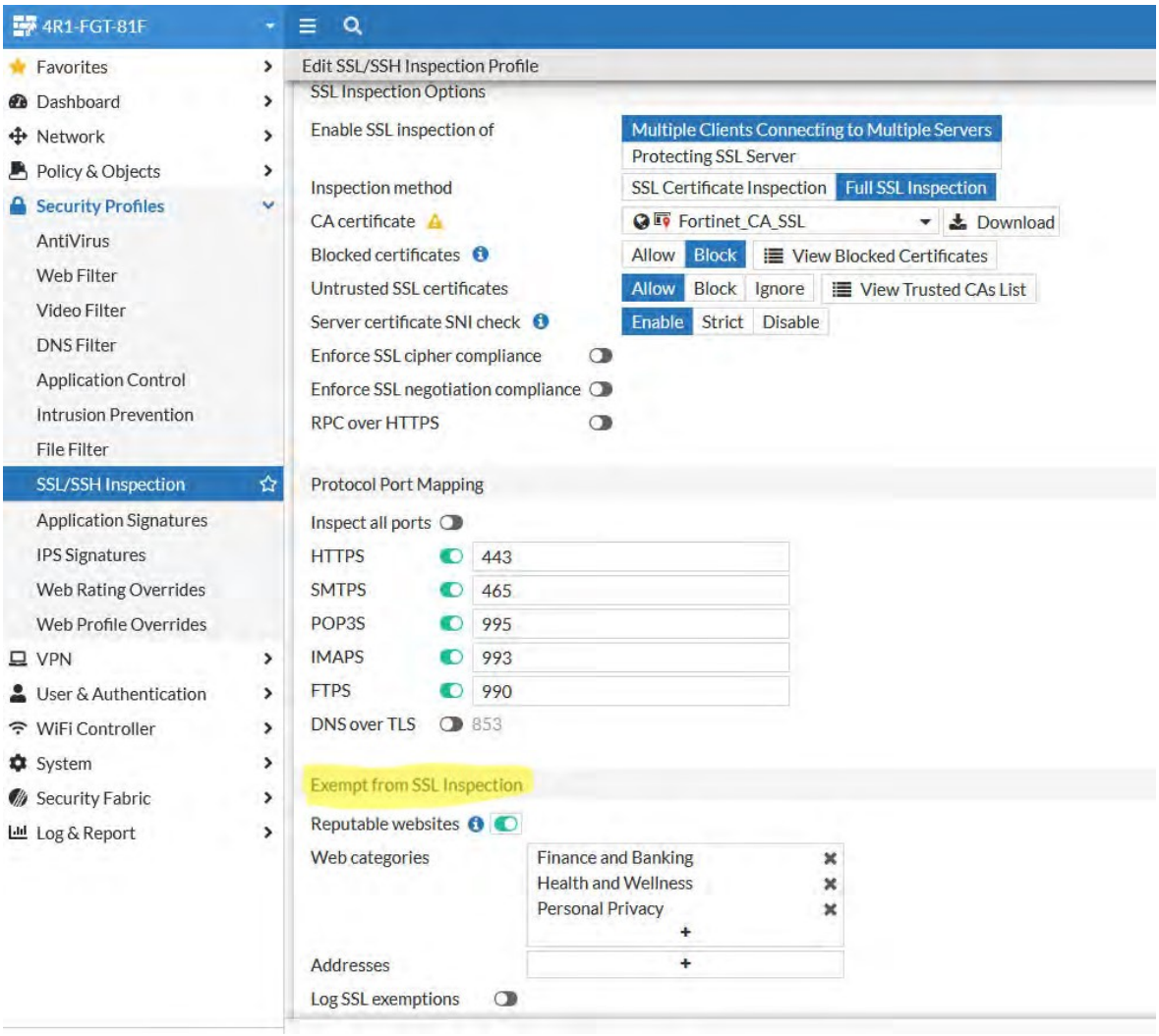
TESTE OK

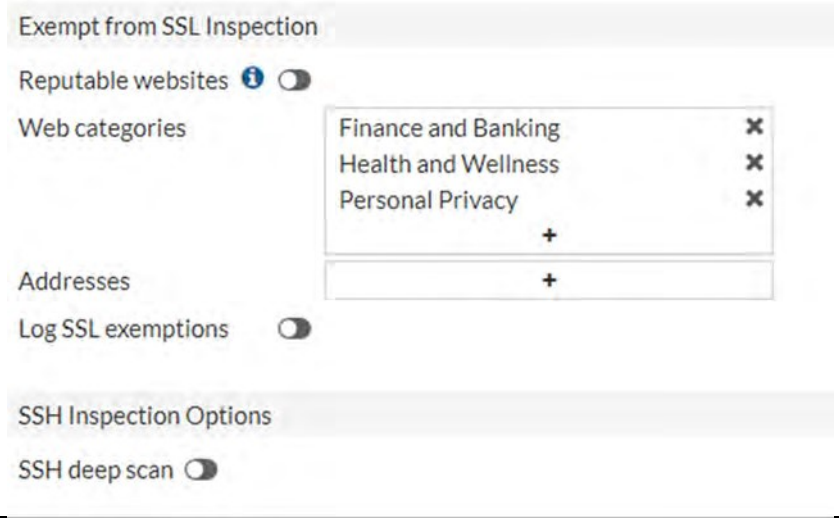


Comentário	

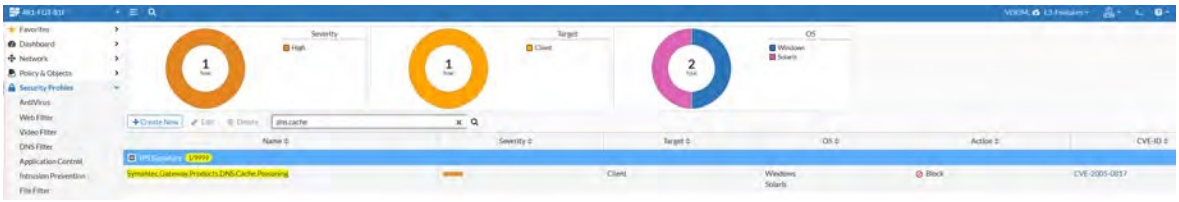
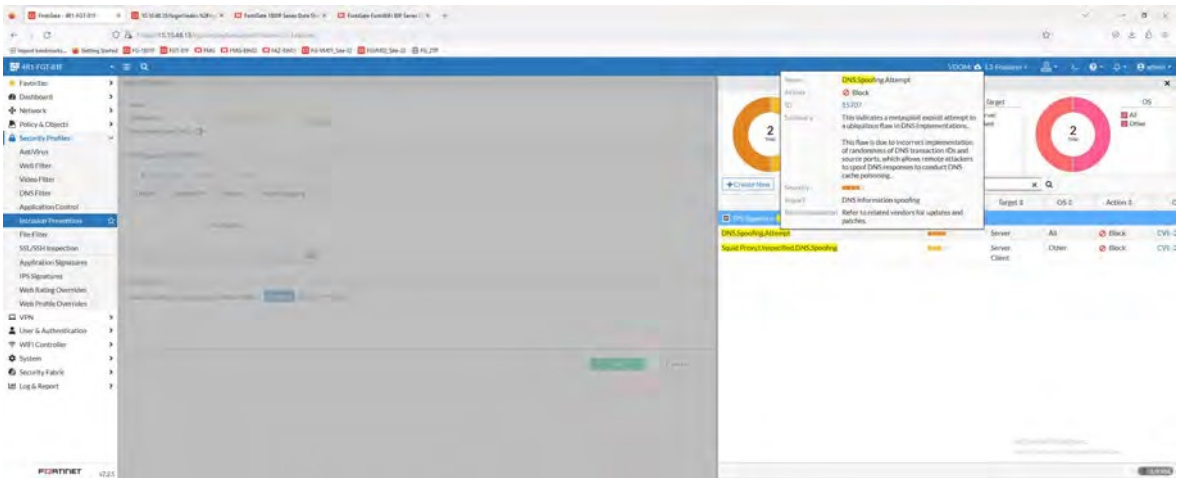
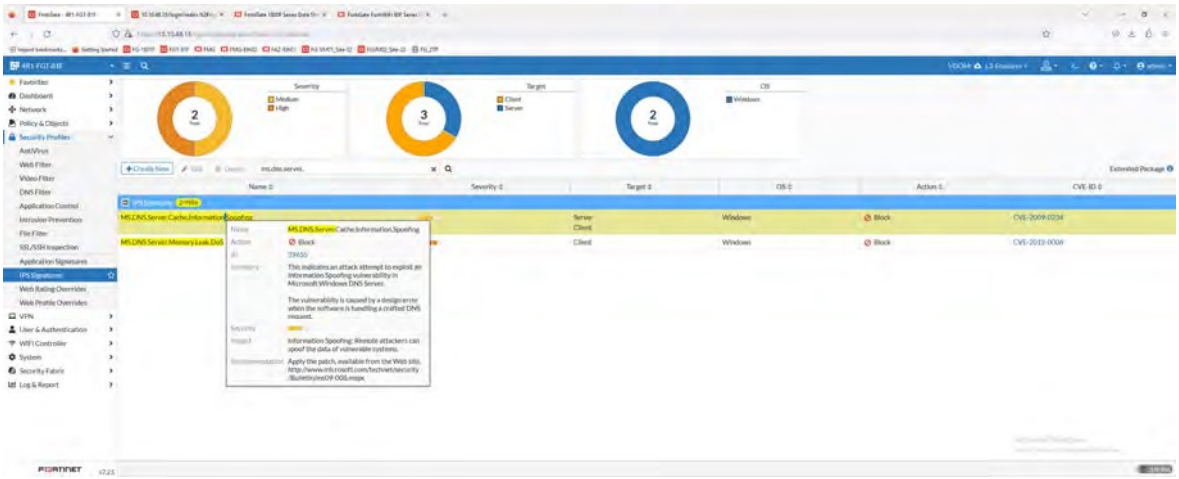
Item de Teste - 5.3.7.4	Possuir proteções de segurança, informações como: código CVE, severidade, e tipo de ação que a mesma irá executar;
Objetivo do Teste	Verificar se o sistema de proteção de segurança possui as informações de código CVE, severidade, e tipo de ação que a mesma irá executar;
Configuração do Teste	Demonstrar lista de assinaturas e suas características
Procedimento do Teste	Demonstrar lista de assinaturas e suas características
Evidências	 **TESTE OK** Podemos ver na imagem abaixo retirada de um perfil de IPS do FortiGate, que ele apresenta as seguintes informações: Grau de Severidade, Ação a ser tomada e como também o código CVE daquela vulnerabilidade. 3Com.3CDaemon.FTP.Server.Buffer.Over... Server Windows Block CVE-2005-0277 3Com.3CDaemon.FTP.Server.Information.... Client Windows Pass CVE-2005-0278 3Com.Intelligent.Management.Center.Info... Server Windows Block 3Com.OfficeConnect.ADSL.Wireless.Fire... Server Linux Block 3S.Pocknet.VMS.ActiveX.Control.Buffer.O... Client Windows Block CVE-2014-9263 3ivx.MPEG4.File.Processing.Buffer.Overfl... Client Windows Block CVE-2007-6401 427BB.Cookie.Based.Authentication.Bypass Server Other Block CVE-2006-0153 427BB.Showthread.PHP.ForumID.Parame... Server Other Block CVE-2006-0154 A32S.Botnet Server Client All Block
Comentário	

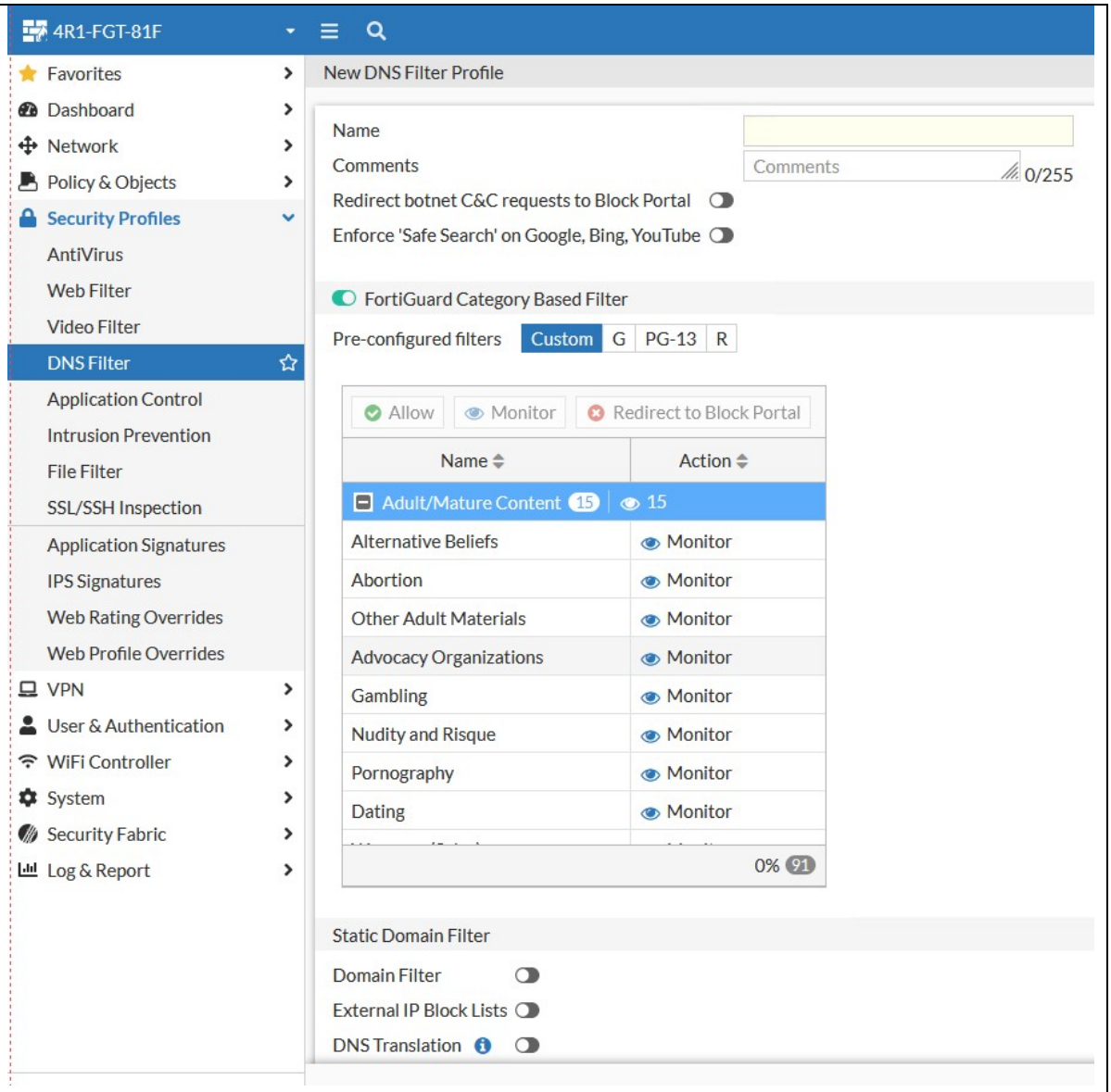
Item de Teste - 5.3.7.18	A solução deve possuir inspeção de tráfego HTTPS sendo possível criar bypass para sites evitando qualquer tipo de quebra de sigilo de informações pessoais;
Objetivo do Teste	Verificar se a solução possui uma forma de dar bypass na inspeção de tráfego HTTPS.

Configuração do Teste	Demonstrar by-pass de https
Procedimento do Teste	Demonstrar by-pass de https
Evidências	 **TESTE OK**

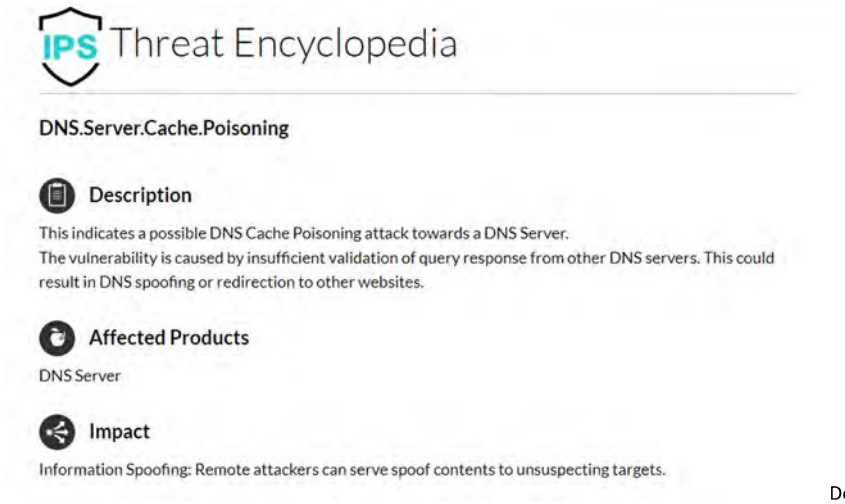
	Exempt web sites from deep inspection If you do not want to apply deep inspection for privacy or other reasons, you can exempt the session by address, category, or allowlist. If you know the address of the server you want to exempt, you can exempt that address. You can exempt specific address type including 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. 
Comentário	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

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.

Configuração do Teste	Demonstrar assinatura DNS.Server.Cache.Poisoning
Procedimento do Teste	Demonstrar assinatura DNS.Server.Cache.Poisoning
Evidências	  

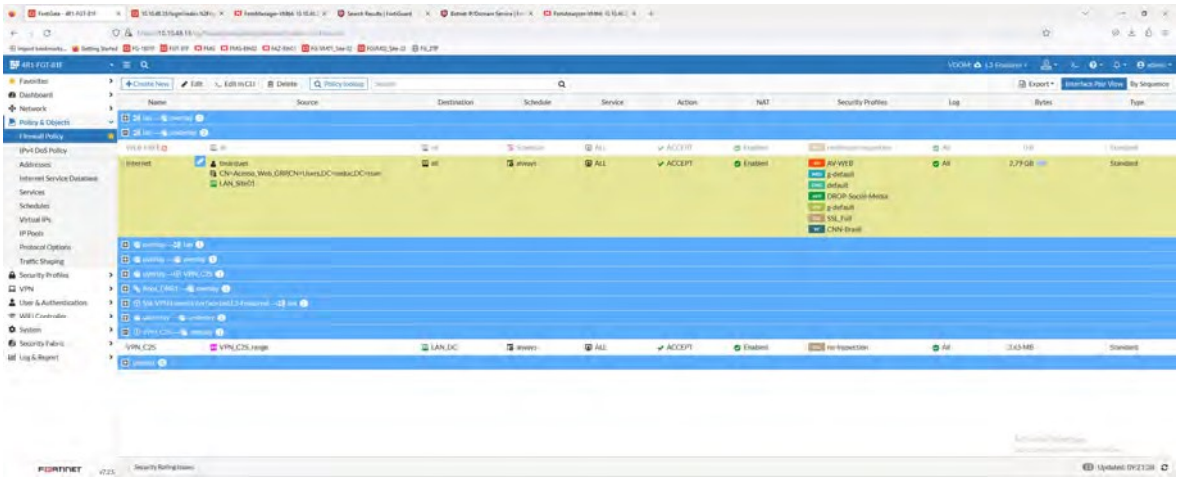

4R1-FGT-81F
Favorites
Dashboard
Network
Policy & Objects
Security Profiles
AntiVirus
Web Filter
Video Filter
DNS Filter
Application Control
Intrusion Prevention
File Filter
SSL/SSH Inspection
Application Signatures
IPS Signatures
Web Rating Overrides
Web Profile Overrides
VPN
User & Authentication
WiFi Controller
System
Security Fabric
Log & Report
New DNS Filter Profile
Name
Comments
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
Allow
Monitor
Redirect to Block Portal
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
0% 91
Static Domain Filter
Domain Filter
External IP Block Lists
DNS Translation

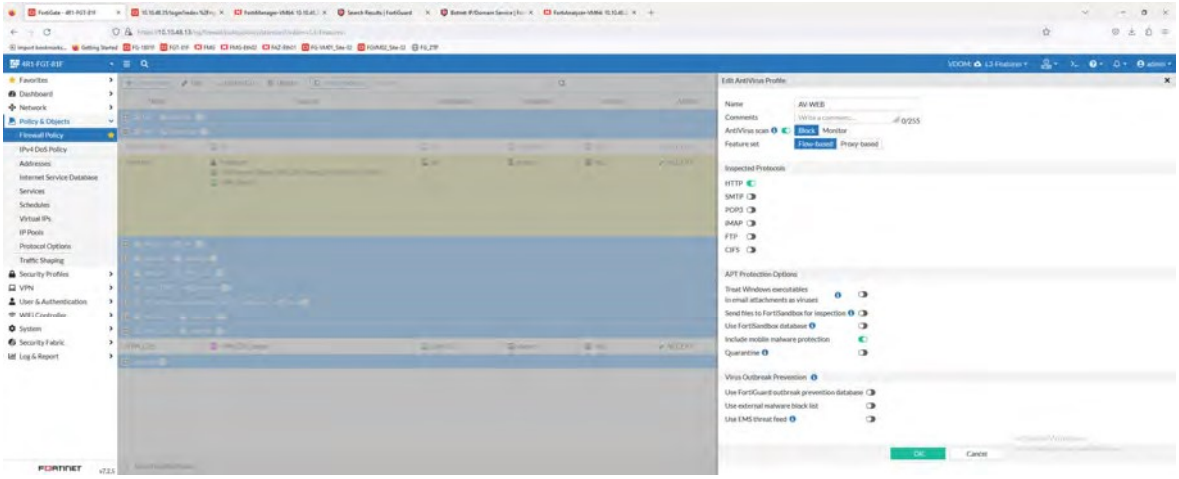
TESTE OK

	 Dentro do perfil de IPS já existe a assinatura dessa vulnerabilidade especificada no CVE-2005-0817, que ele bloqueia por default. 
Comentário	Fonte: IPS Threat Encyclopedia acessado em https://www.fortiguard.com/encyclopedia/ips/43827/dns-server-cache-poisoning

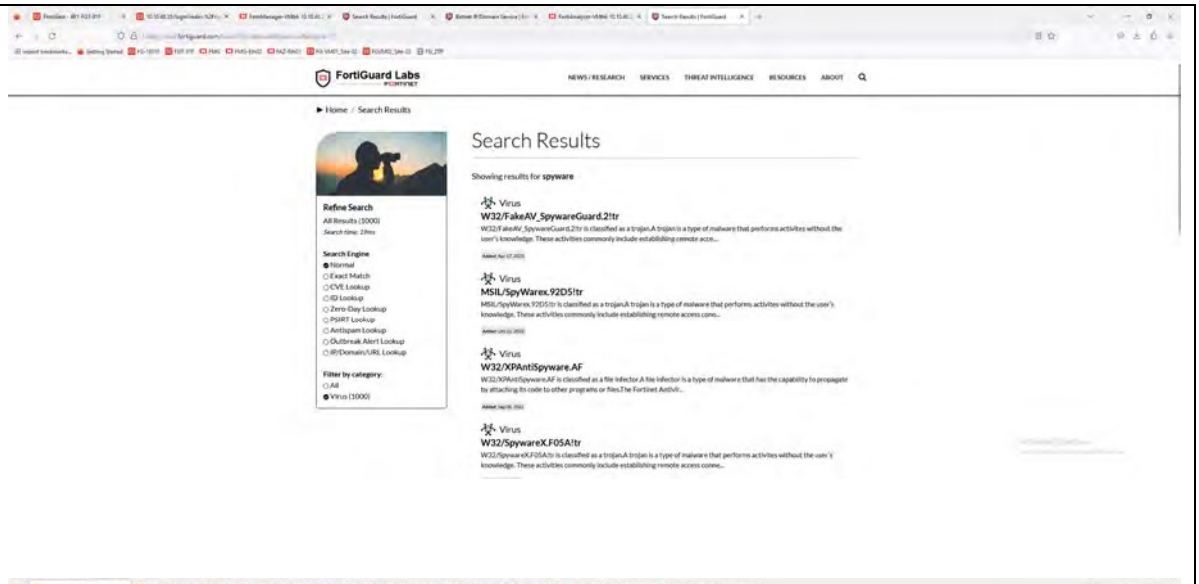
5.3.8 ANTI-MALWARE:

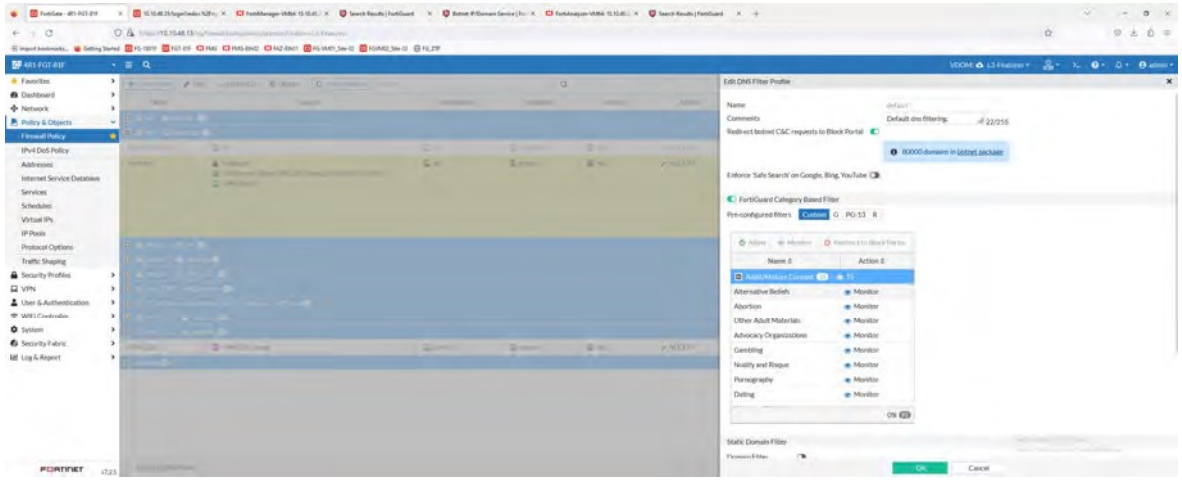
Item de Teste - 5.3.8.1	Possuir módulo de Antivírus, Antispyware e Antibot integrado no próprio appliance de segurança e integrado à gerência centralizada de administração, monitoração e logs;
Objetivo do Teste	Verificar se a solução possuí módulo de Antivírus, Antispyware e Antibot integrado no próprio 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.

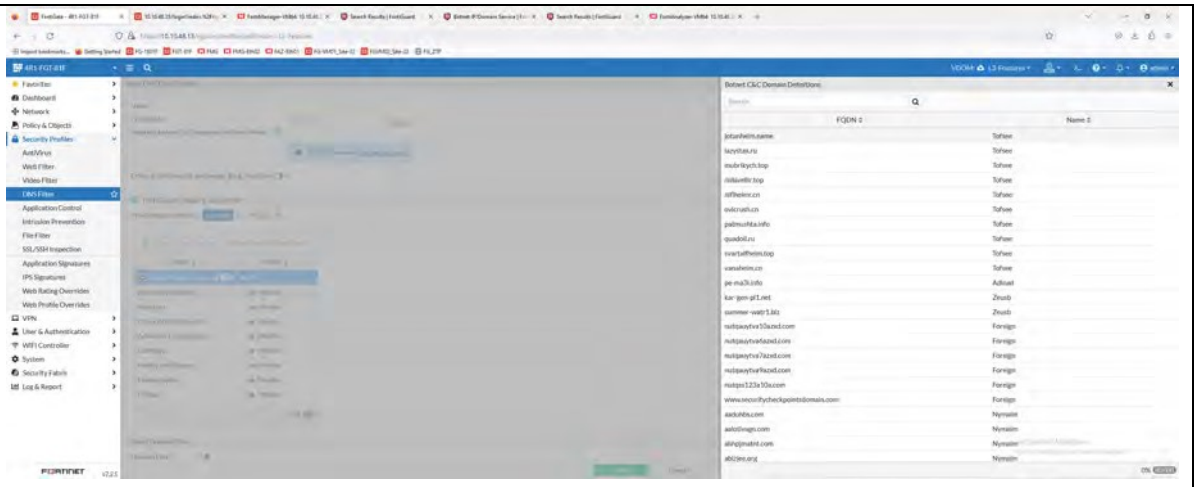




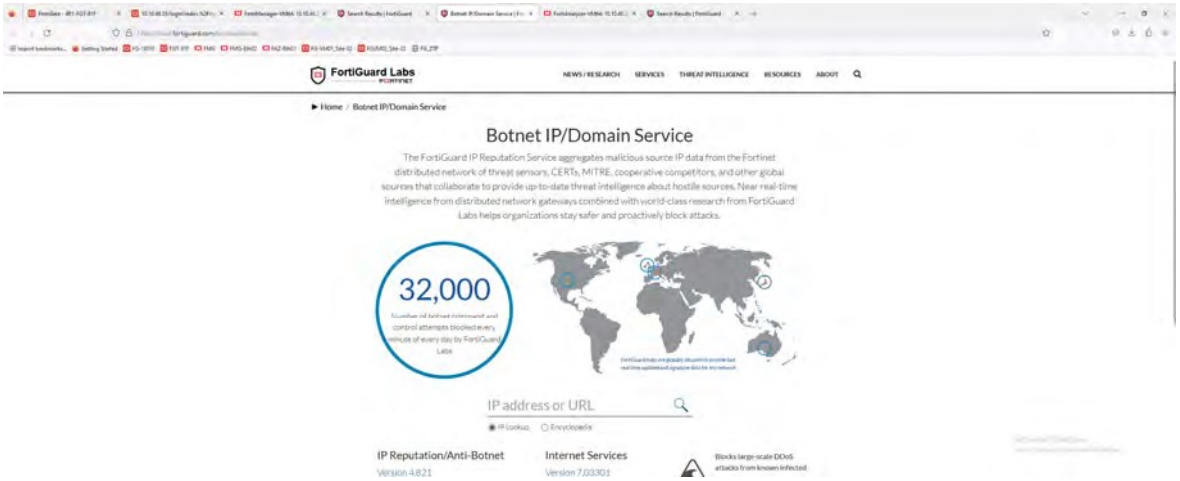
https://www.fortiguard.com/search?q=spyware&type=av&engine=1

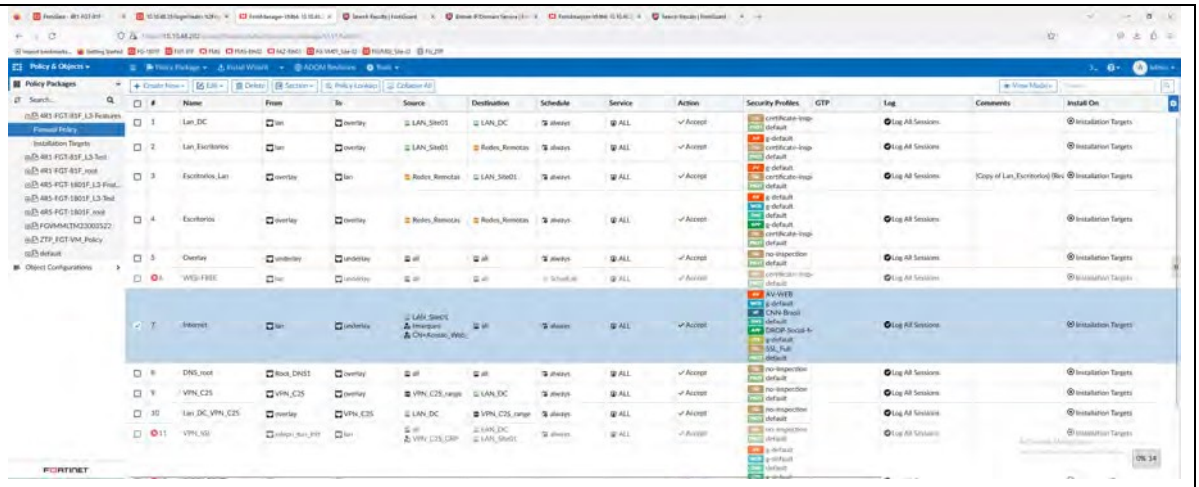

FortiGuard Labs
NEWS / RESEARCH
SERVICES
THREAT INTELLIGENCE
RESOURCES
ABOUT
Home / Search Results
Search Results
Showing results for spyware
Refine Search
Search Engine
Filter by category:
Virus
W32/FakeAV_SpywareGuard.2!tr
Virus
MSIL/SpyWarex.92D5!tr
Virus
W32/XPAntiSpyware.AF
Virus
W32/SpywareX.F05A!tr

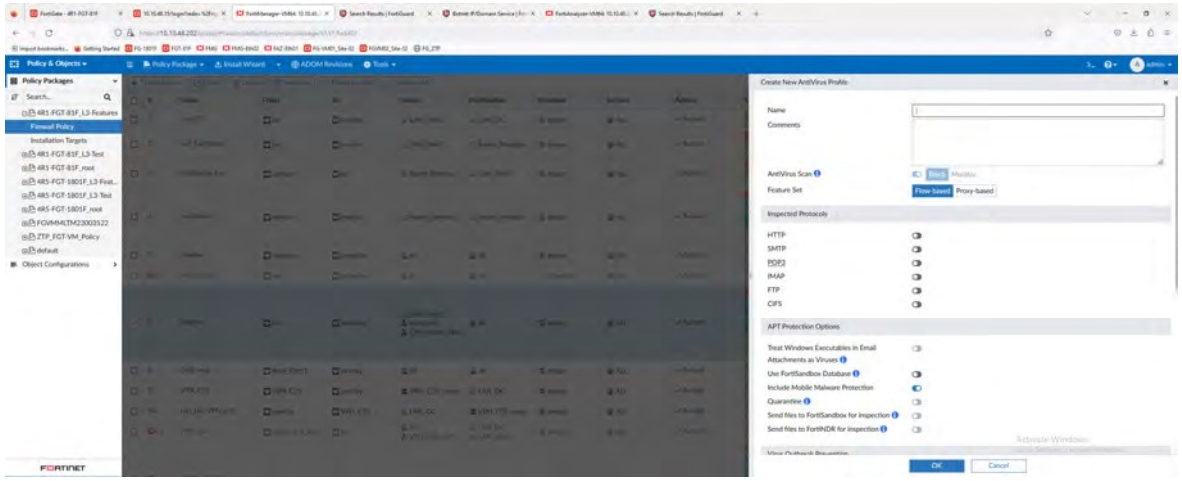

Edit DNS Filter Profile
FortiGuard Category Based Filter
Static Domain Filter
OK
Cancel

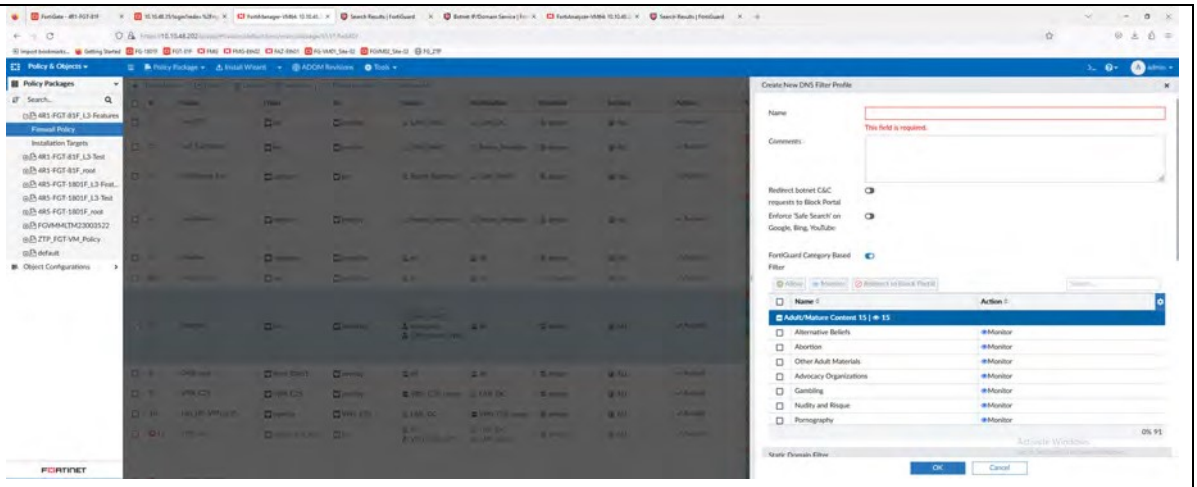


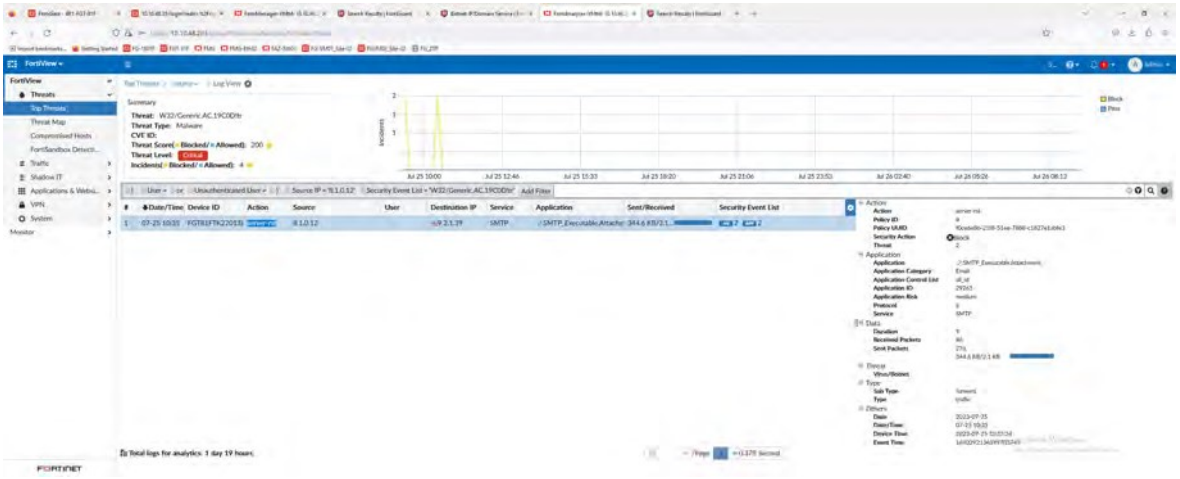
https://www.fortiguard.com/services/botnet



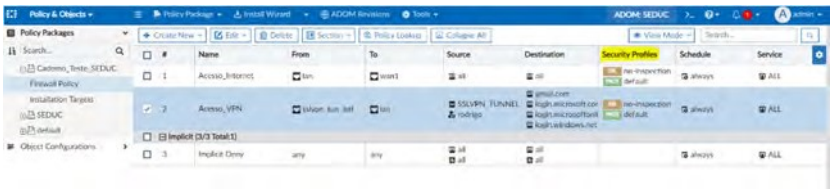




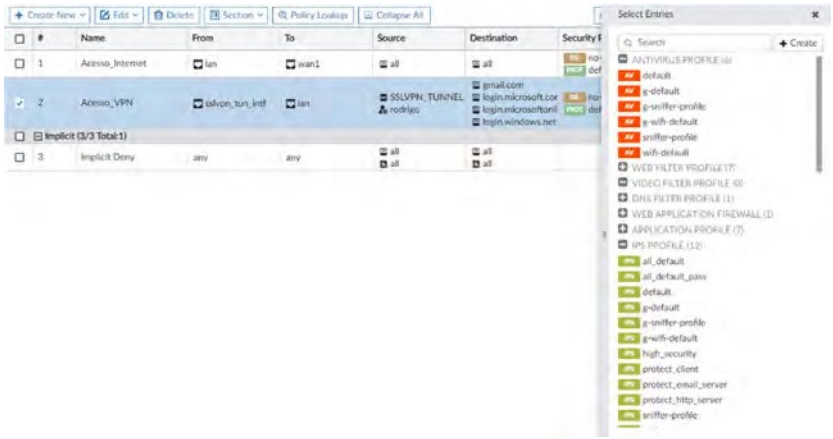


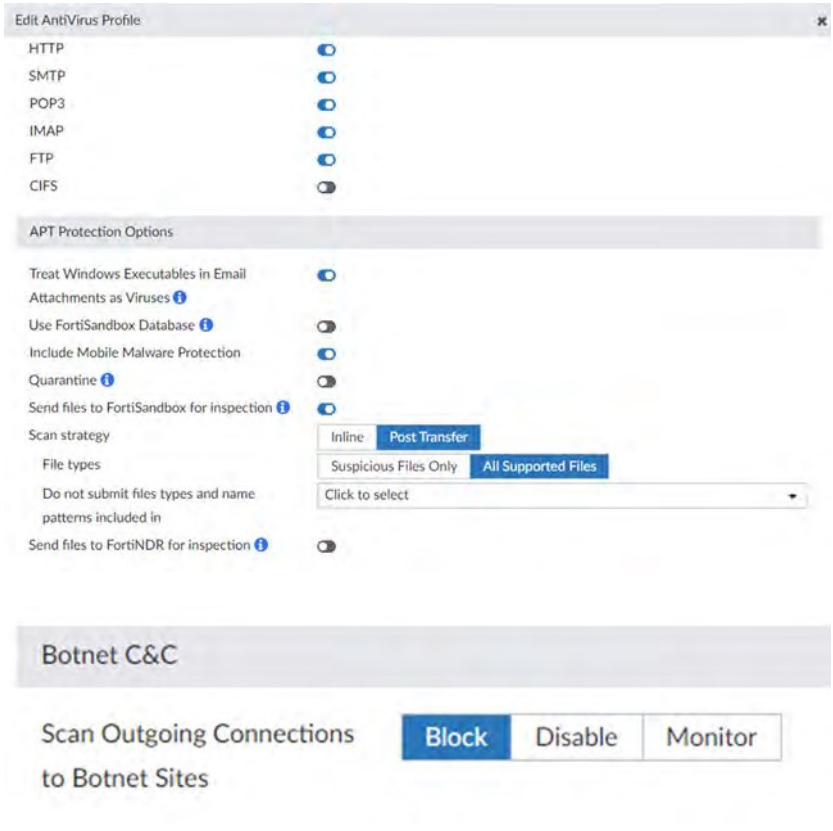


TESTE OK

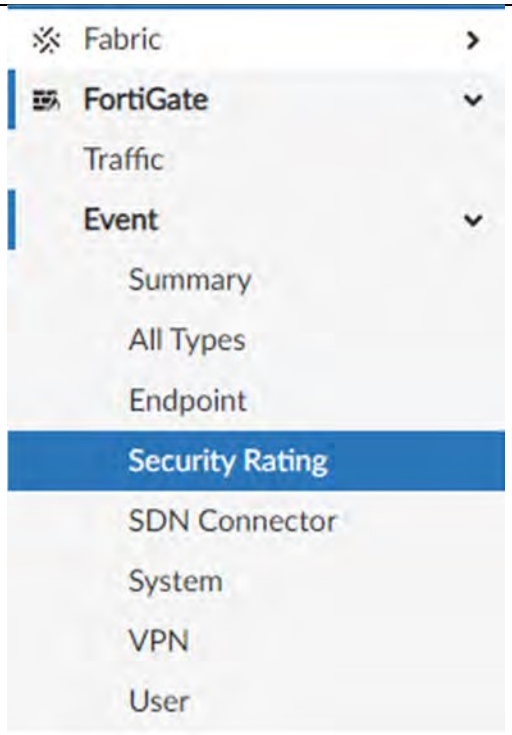
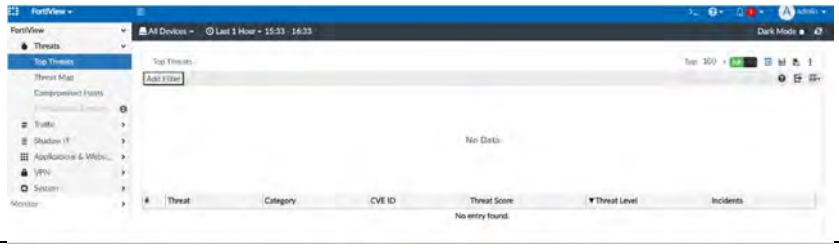


Para isso, basta ir na aba de de “Security Profiles” e lá estará os perfis de Antivírus e IPS.

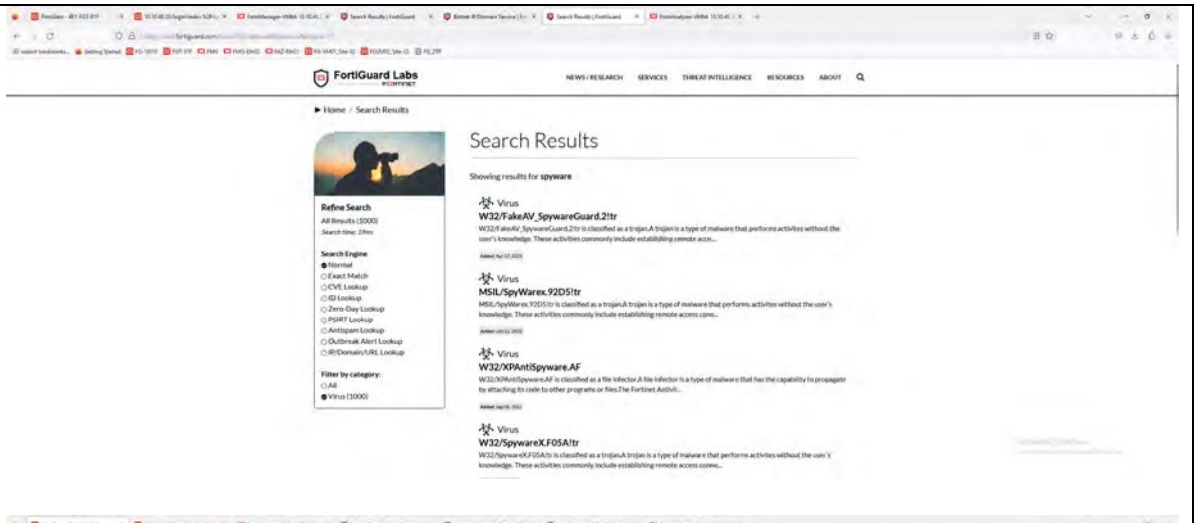


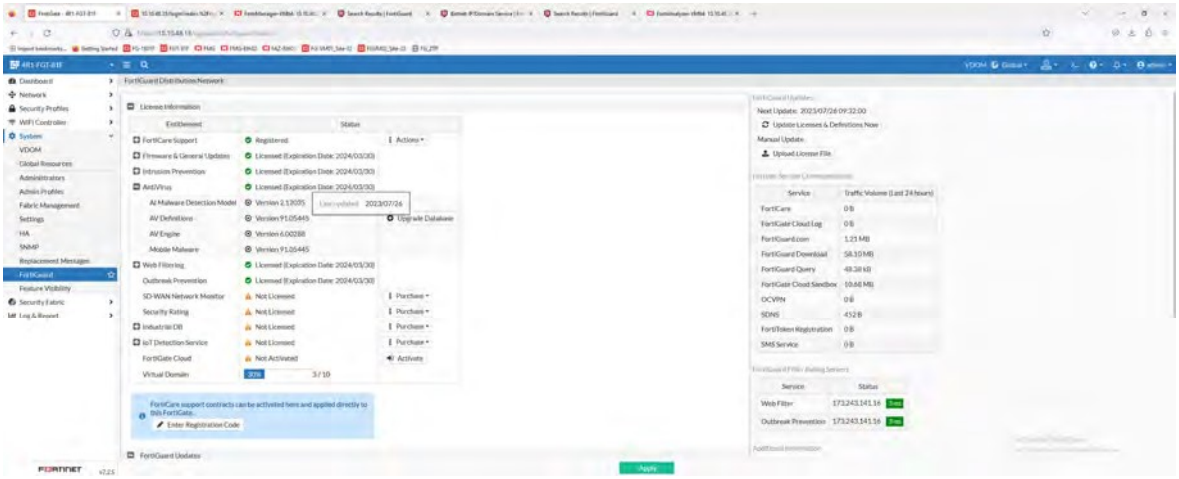


Na parte de logs podemos ver na seguinte forma:

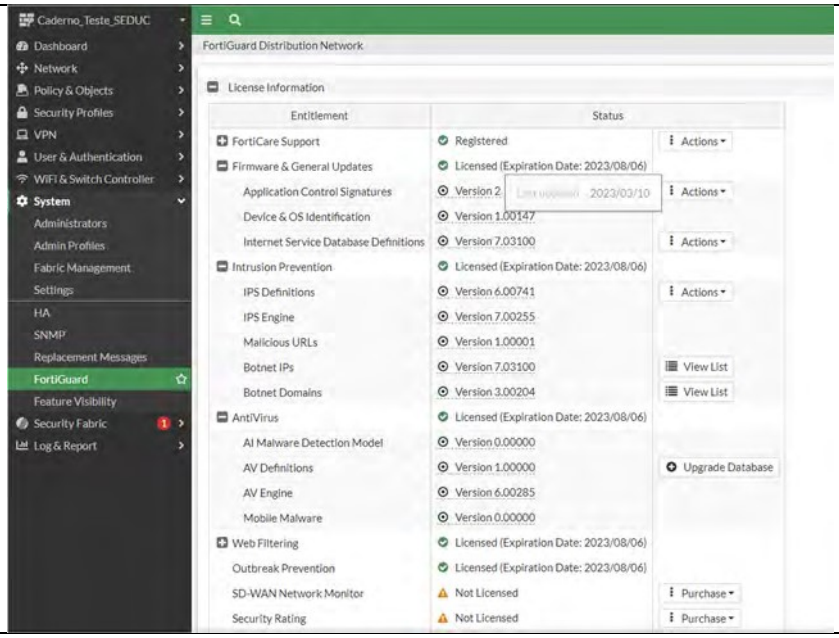
	 E na de monitoração: 
Comentário	

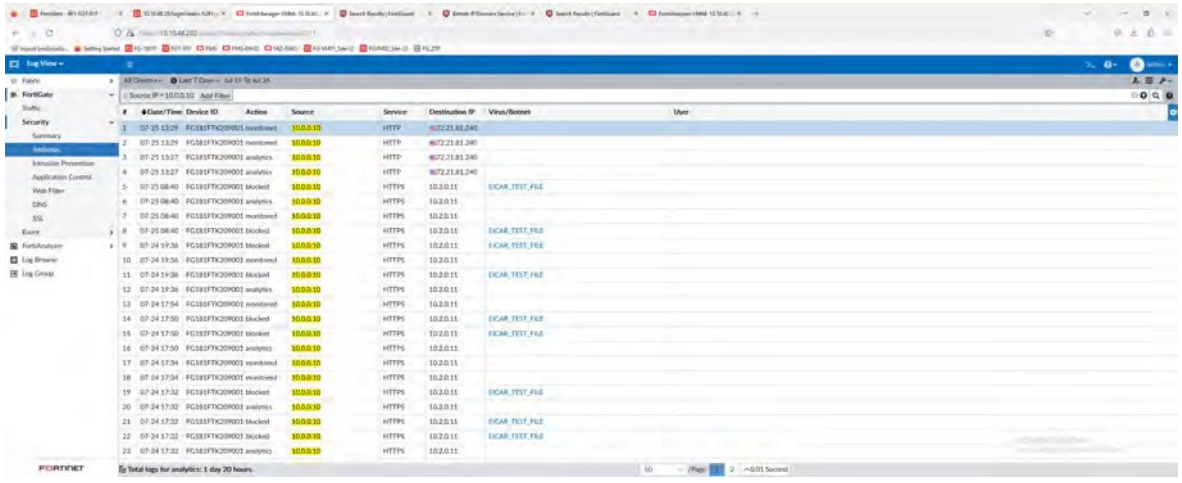
Item de Teste - 5.3.8.2	A solução deve possuir nuvem proprietária inteligente do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas;
Objetivo do Teste	Validar se a solução possui nuvem proprietária e inteligente do mesmo fabricante e se é possível 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	

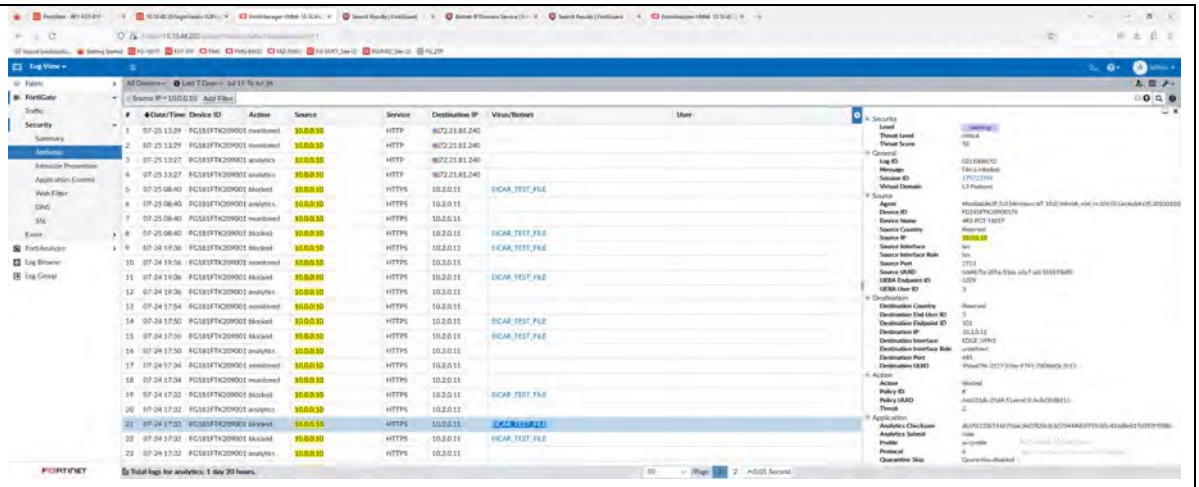
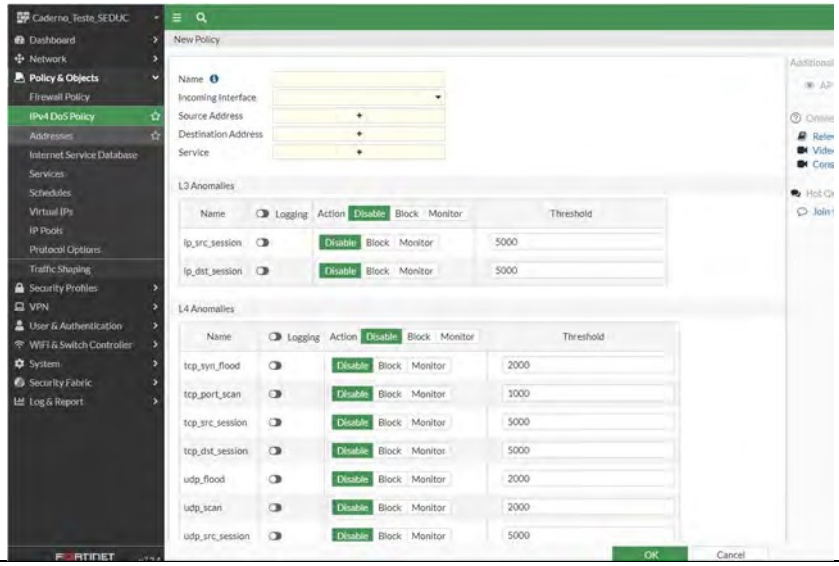

FortiGuard Labs
Search Results
Showing results for spyware
Virus
W32/FakeAV_SpywareGuard.2!tr
Virus
MSIL/SpyWarex.92D5!tr
Virus
W32/XPAntiSpyware.AF
Virus
W32/SpywareX.F05A!tr



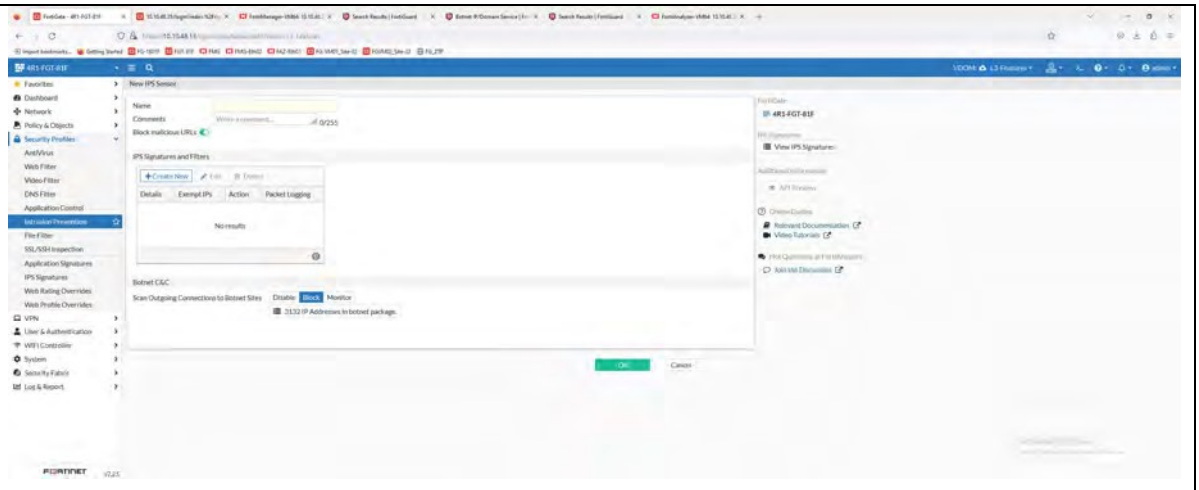
TESTE OK

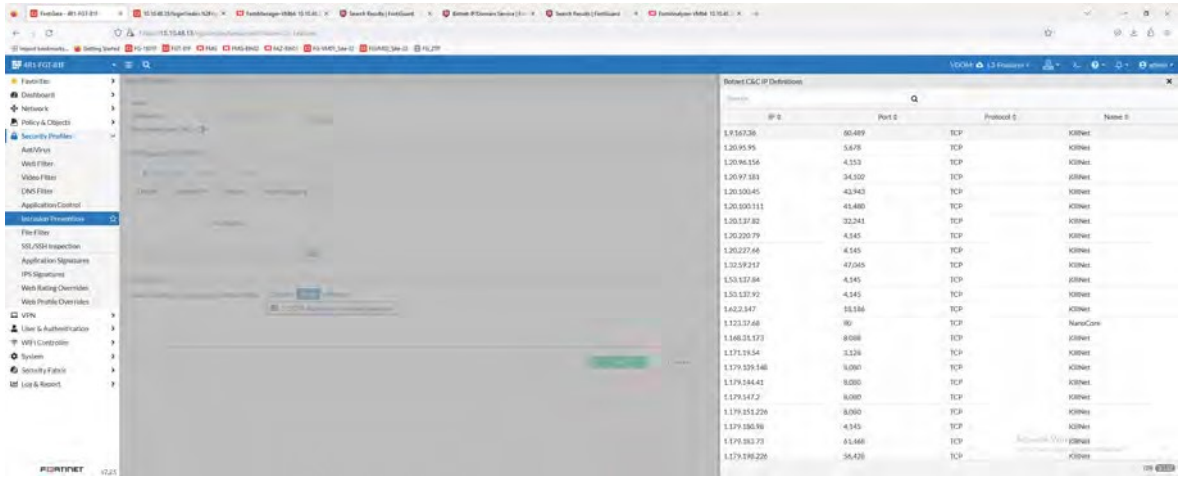
	
Comentário	https://www.fortiguard.com/services/ips

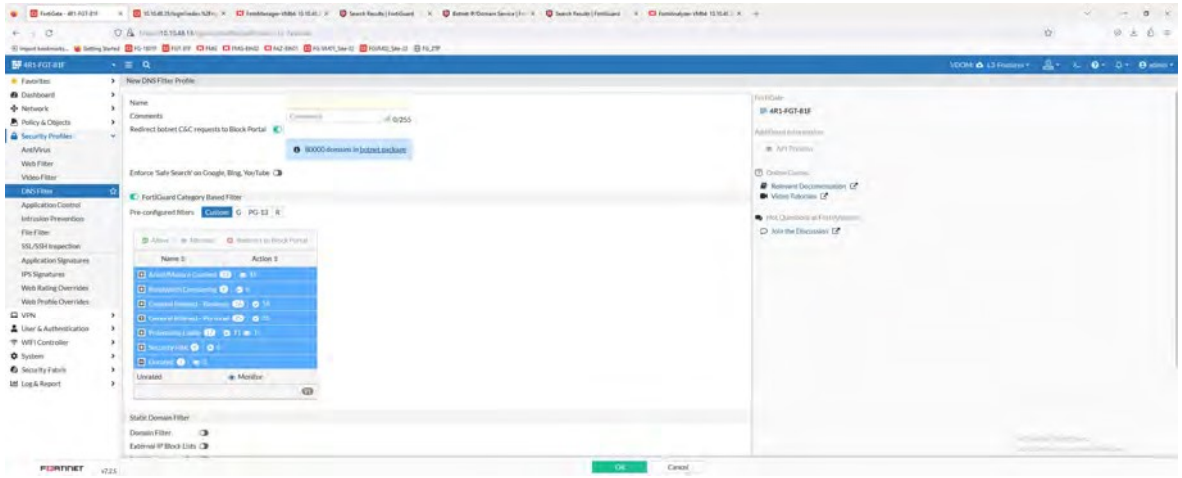
Item de Teste - 5.3.8.4	A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;
Objetivo do Teste	Validar se a solução detecta e bloqueia comportamentos suspeitos ou anormais da rede
Configuração do Teste	Criar regra de acesso NGFW de anomalia
Procedimento do Teste	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.
Evidências	

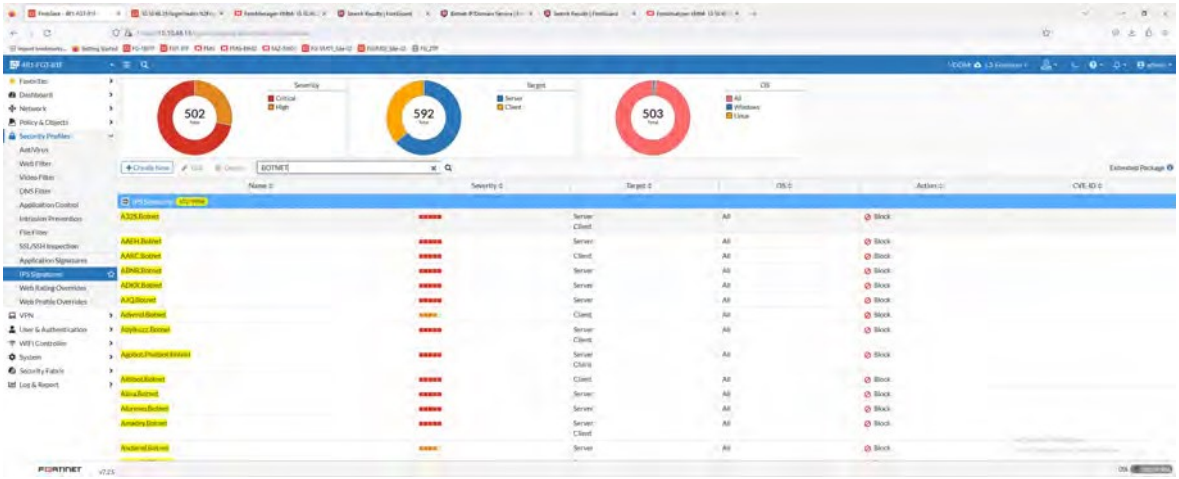
	 **TESTE OK** 
Comentário	

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	









TESTE OK

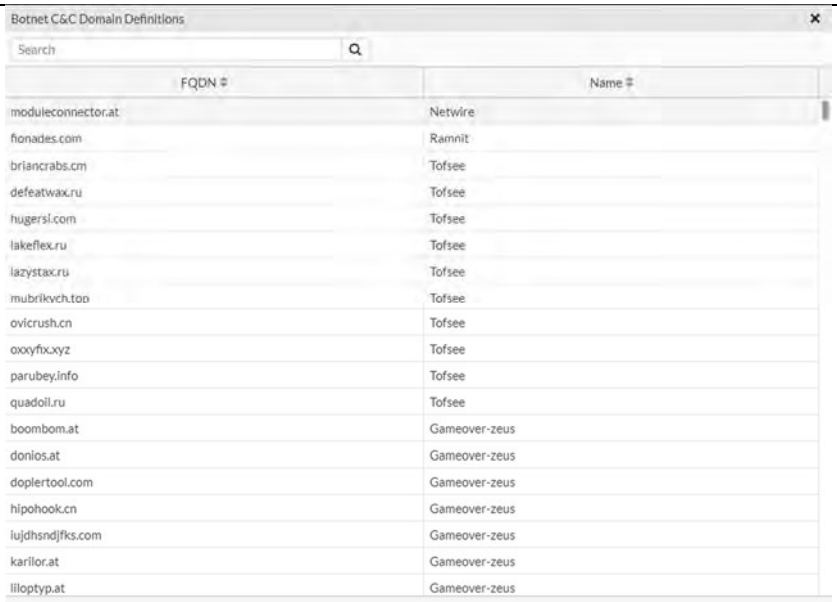
A solução de Antibot feita pelo IPS Filter, consiste em reputação de endereços IP, com descrição do protocolo e a porta utilizada.

Botnet C&C IP Definitions

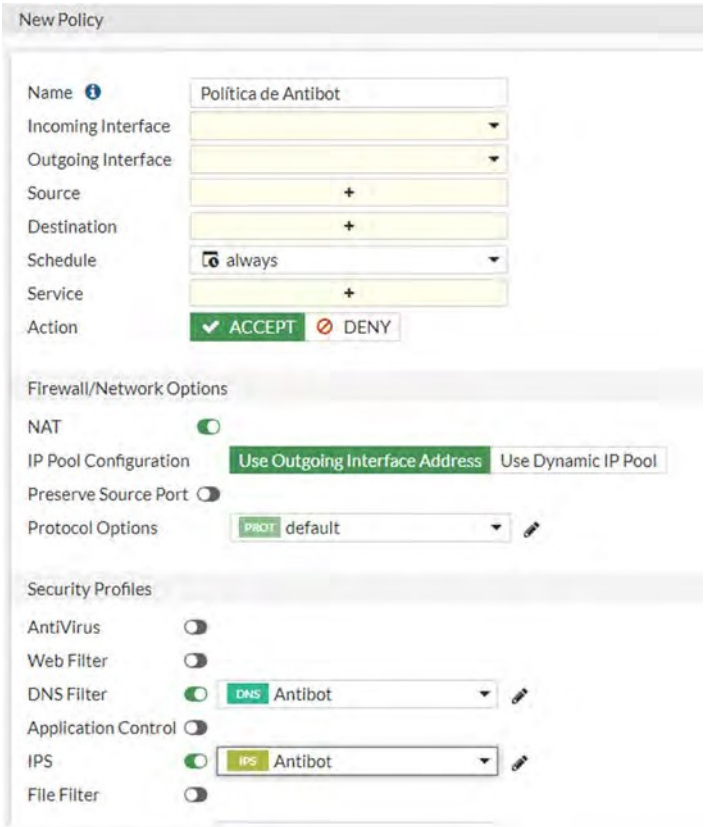
Search

IP	Port	Protocol	Name
1.9.167.36	60.489	TCP	KillNet
1.10.189.133	50.855	TCP	KillNet
1.20.96.156	4.153	TCP	KillNet
1.20.97.181	34.102	TCP	KillNet
1.20.100.45	43.943	TCP	KillNet
1.20.100.111	41.480	TCP	KillNet
1.53.137.92	4.145	TCP	KillNet
1.62.2.147	18.186	TCP	KillNet
1.123.37.68	80	TCP	NanoCore
1.168.31.173	8.088	TCP	KillNet
1.169.224.221	16.464	UDP	ZeroAccess
1.169.224.228	16.464	UDP	ZeroAccess
1.171.19.54	3.128	TCP	KillNet
1.171.145.107	16.471	UDP	ZeroAccess
1.171.207.238	16.464	UDP	ZeroAccess
1.171.223.174	16.464	UDP	ZeroAccess
1.174.132.214	16.464	UDP	ZeroAccess
1.174.163.191	16.464	UDP	ZeroAccess

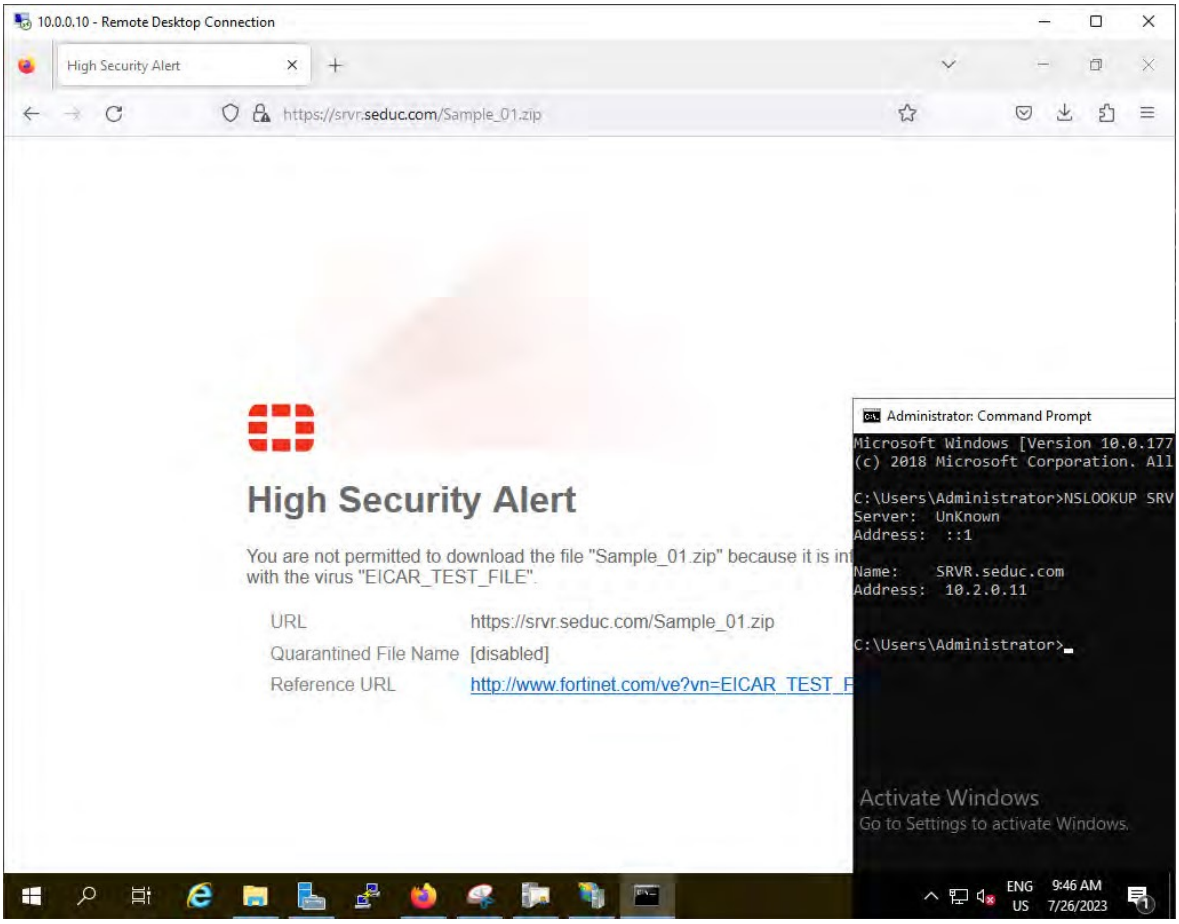
Já a parte de detecção de endereços DNS e URLs é feita pelo DNS Filter.

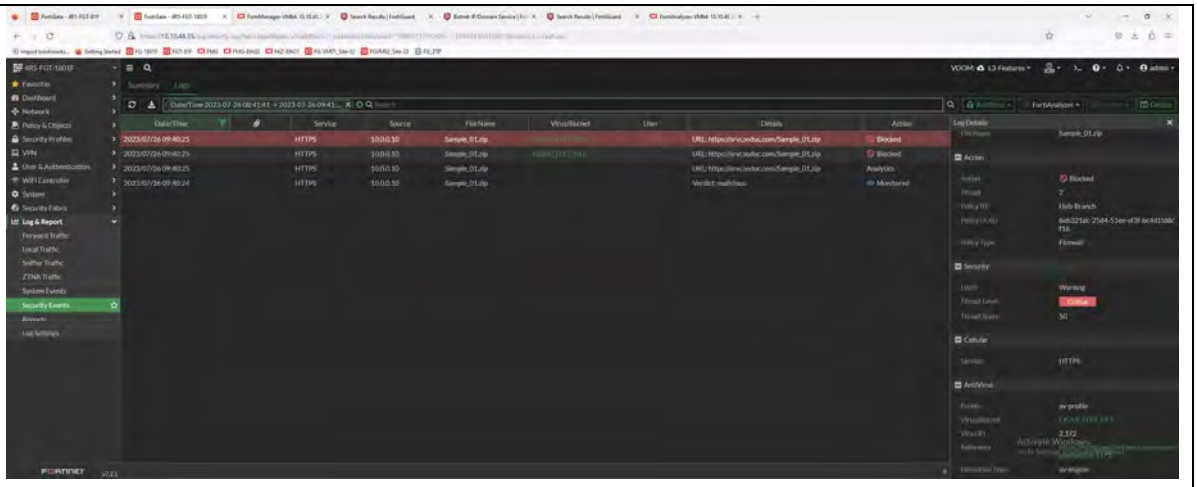


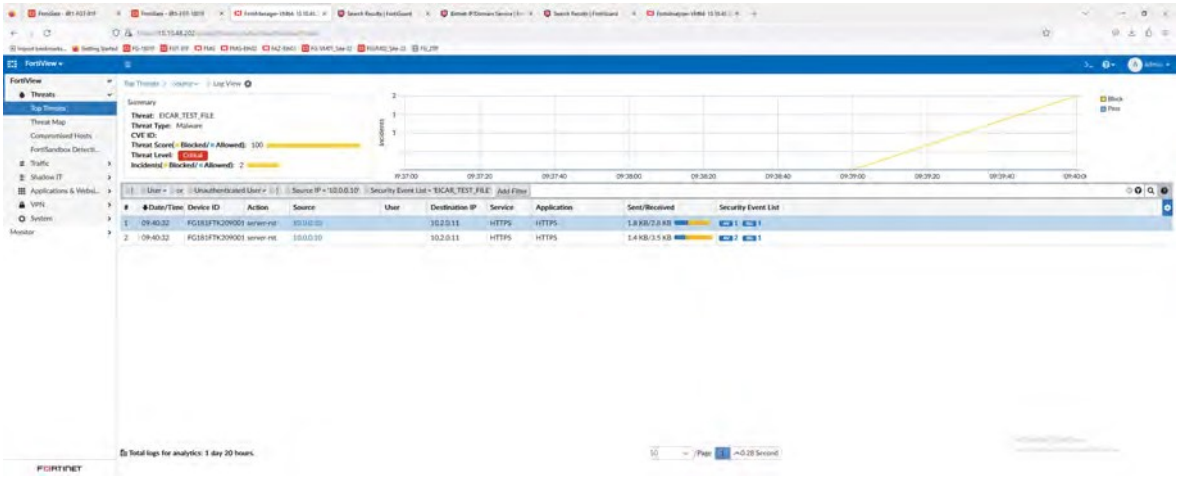
Ambas são perfis de segurança que podem ser aplicados juntamente em uma política específica.

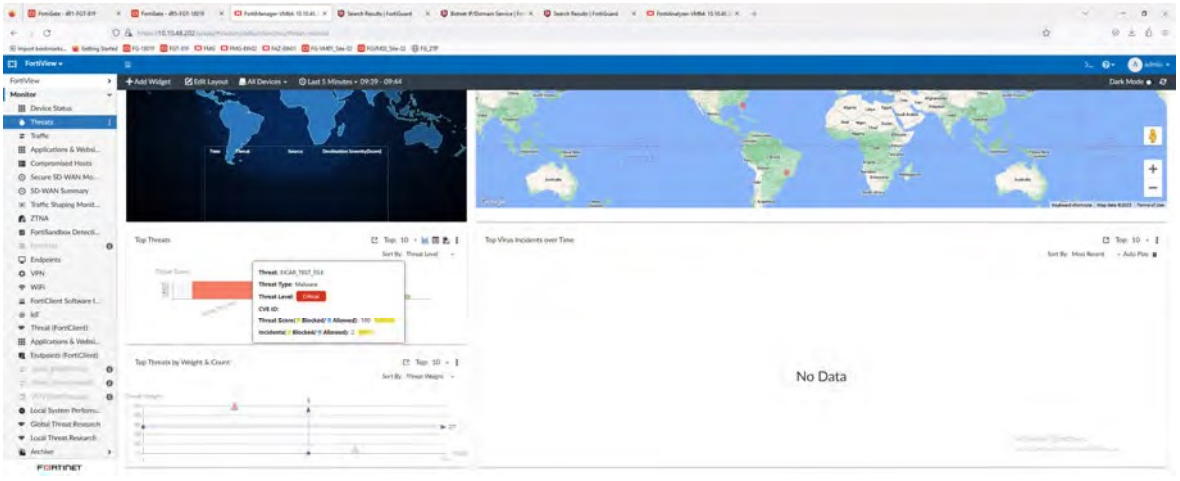


Comentário	

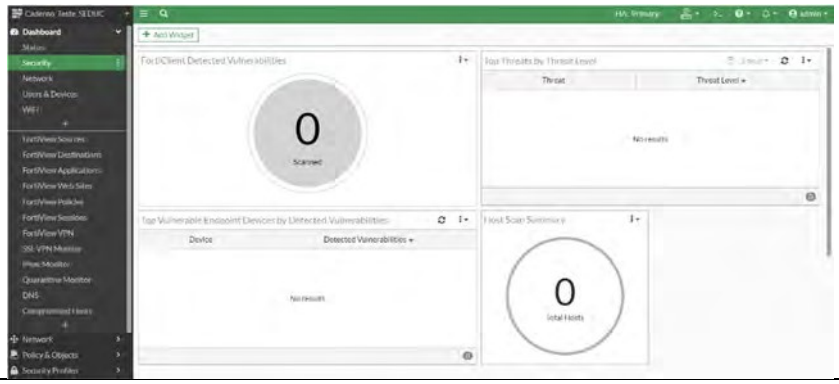
Item de Teste - 5.3.8.9	A solução deve possuir na própria interface de gerência, gráfico contendo informações em tempo real sobre as atividades recentes de malwares detectados na solução;
Objetivo do Teste	Verificar se a solução possuí na própria interface de gerência gráfico contendo informações em 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”. Lá podemos ter acesso a diversas funcionalidades referentes a visualização de eventos de segurança detectados pela solução.
Evidências	

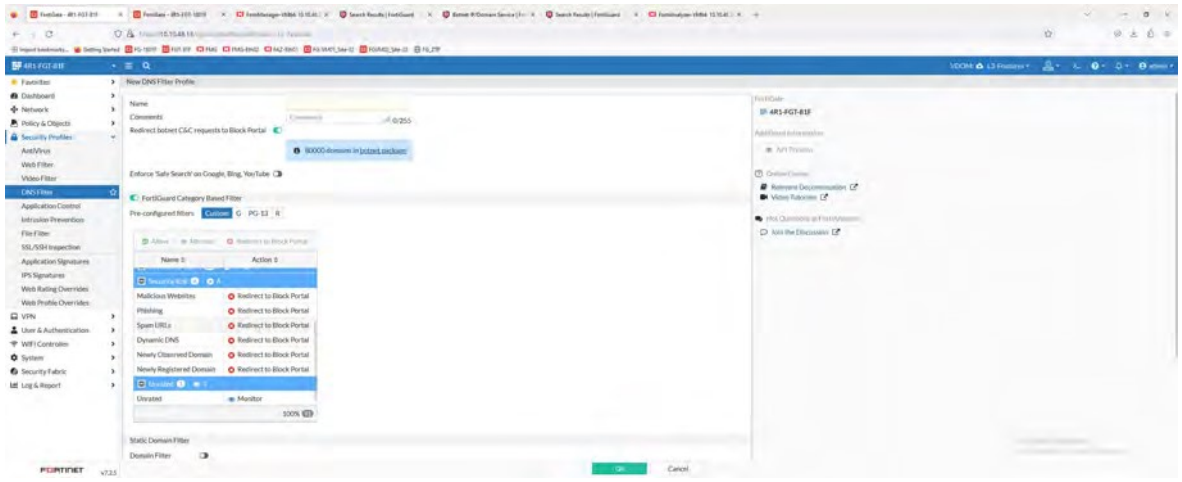


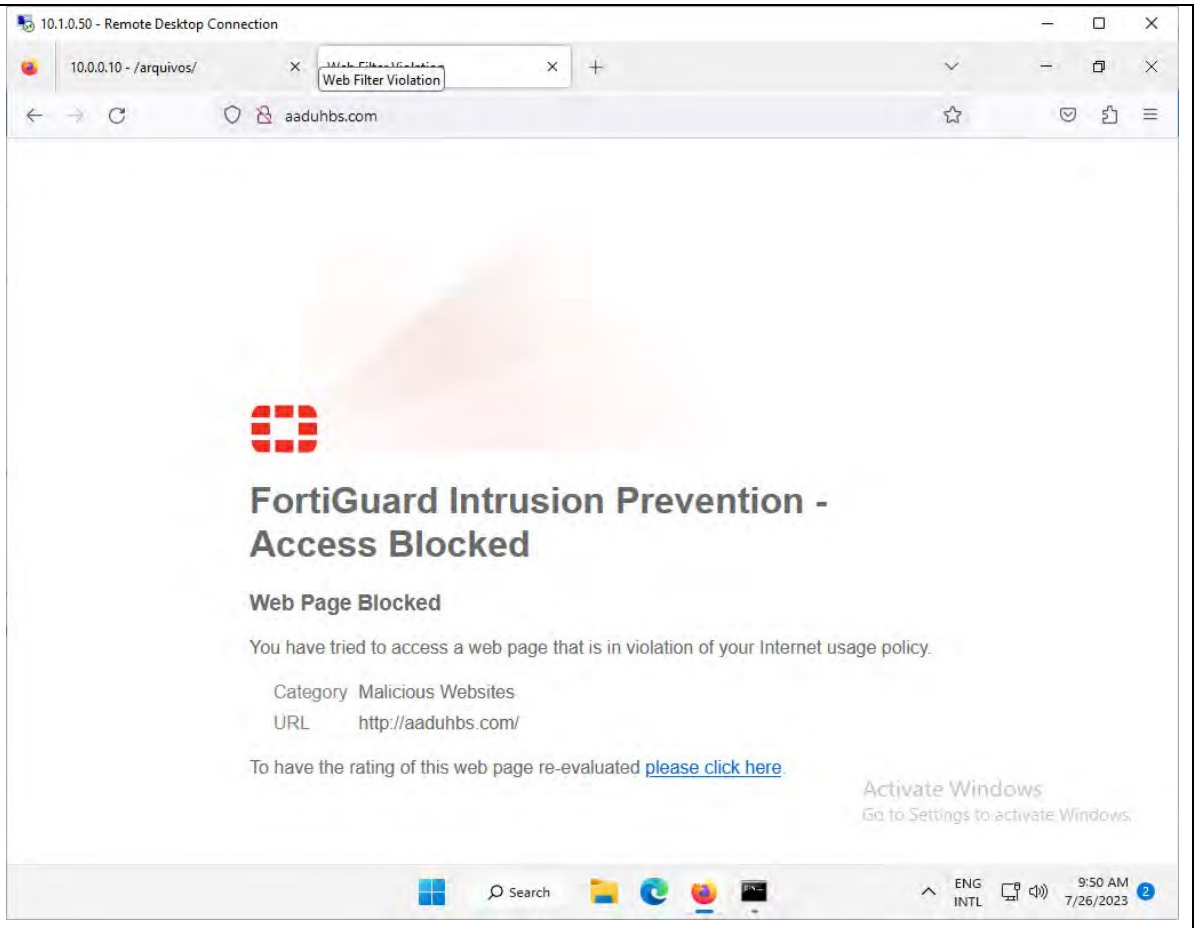


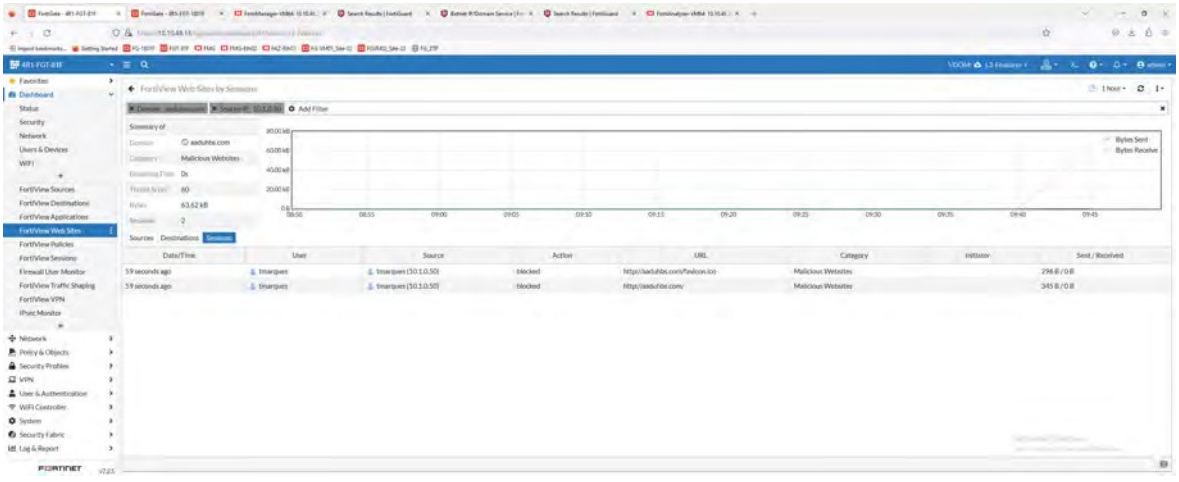


TESTE OK

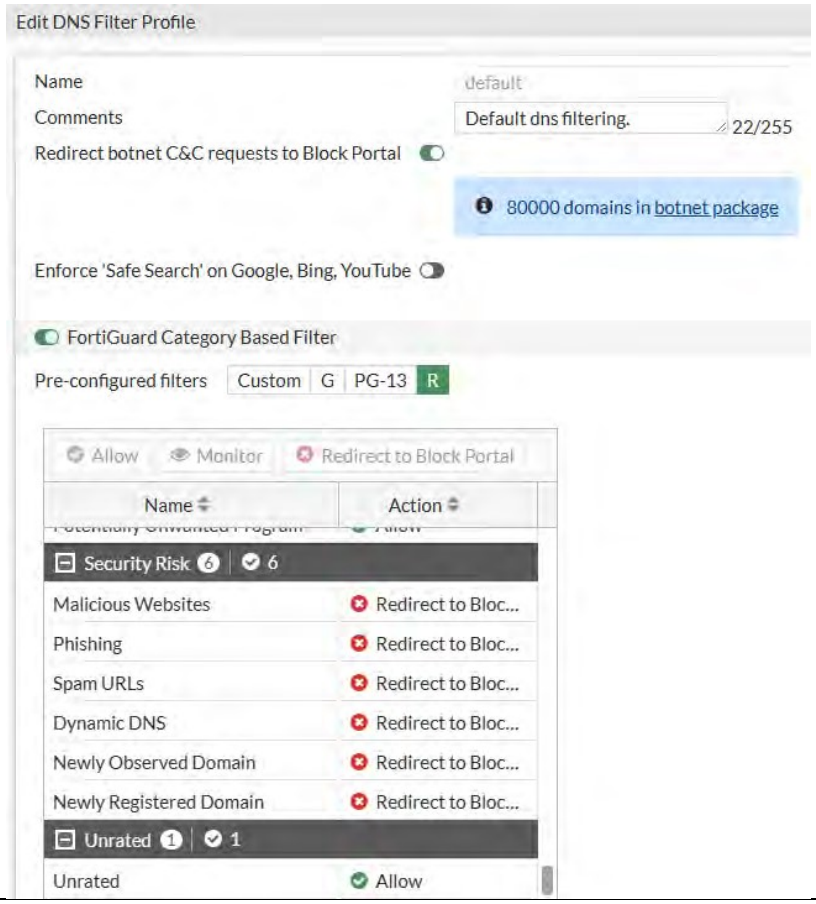
	
Comentário	

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

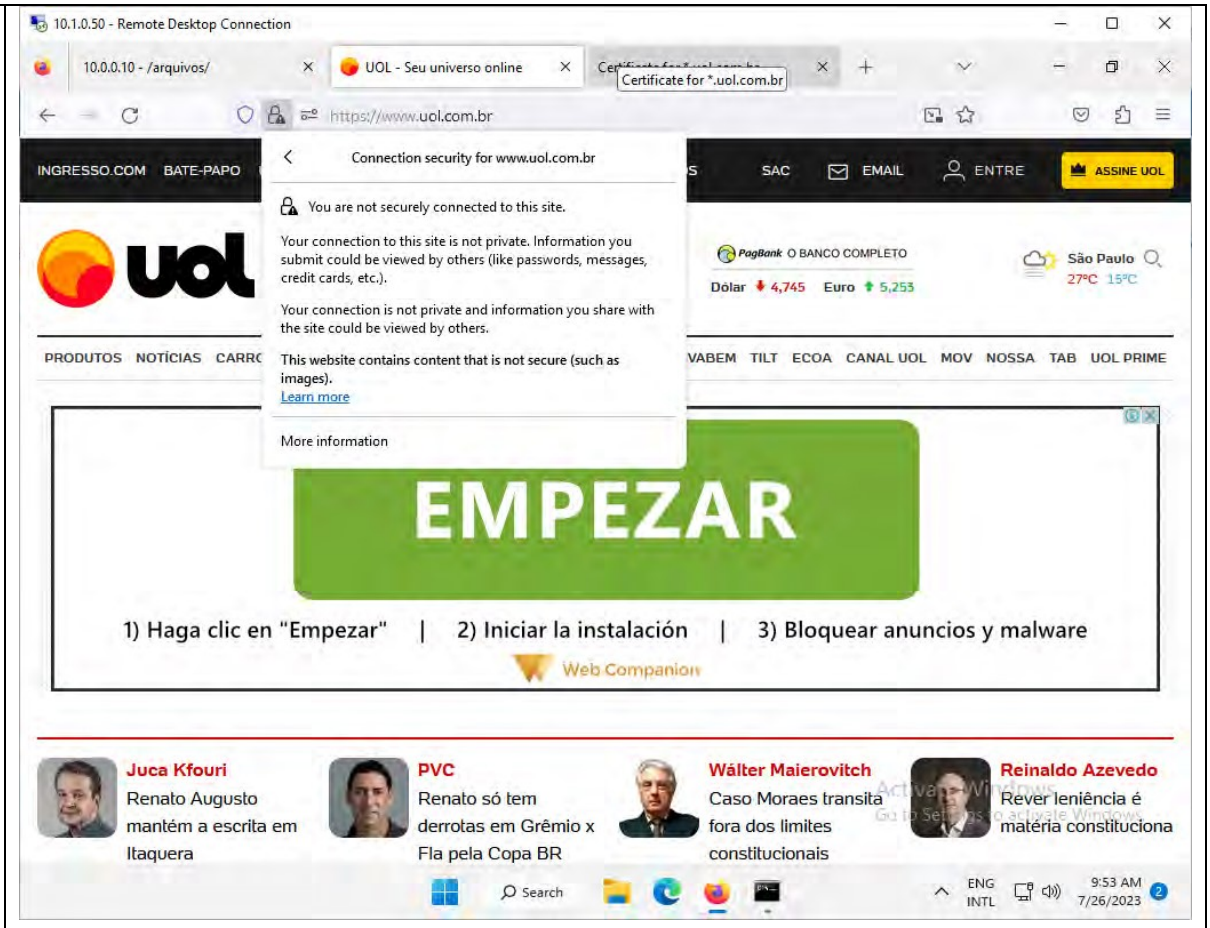

10.1.0.50 - Remote Desktop Connection
10.0.0.10 - /arquivos/
Web Filter Violation
aaduhbs.com
FortiGuard Intrusion Prevention - Access Blocked
Web Page Blocked
You have tried to access a web page that is in violation of your Internet usage policy.
Category Malicious Websites
URL http://aaduhbs.com/
To have the rating of this web page re-evaluated please click here.
Activate Windows
Go to Settings to activate Windows.
Search
ENG INTL
9:50 AM 7/26/2023

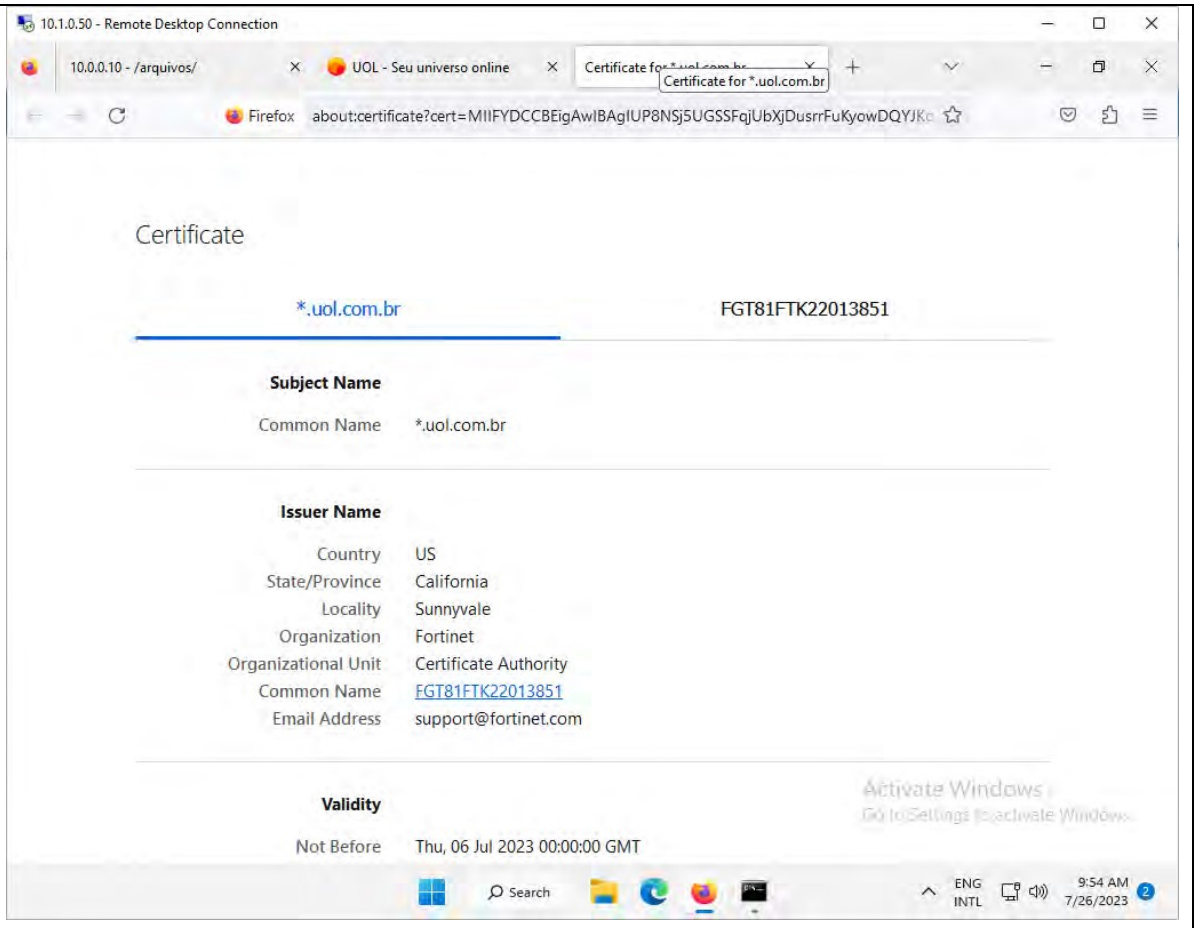


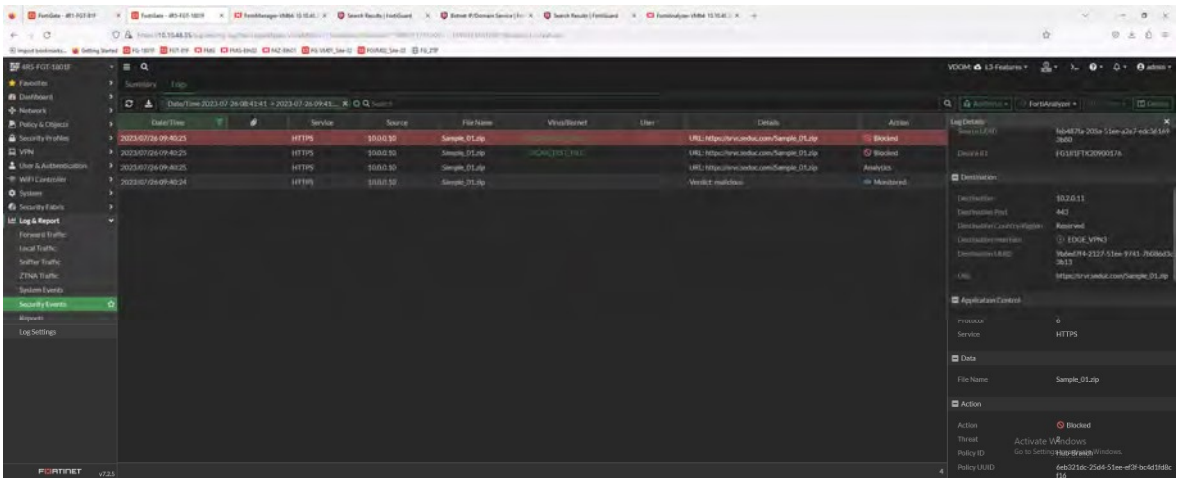
TESTE OK

	O FortiGate possui uma funcionalidade chamada de “DNS Filter” 
Comentário	

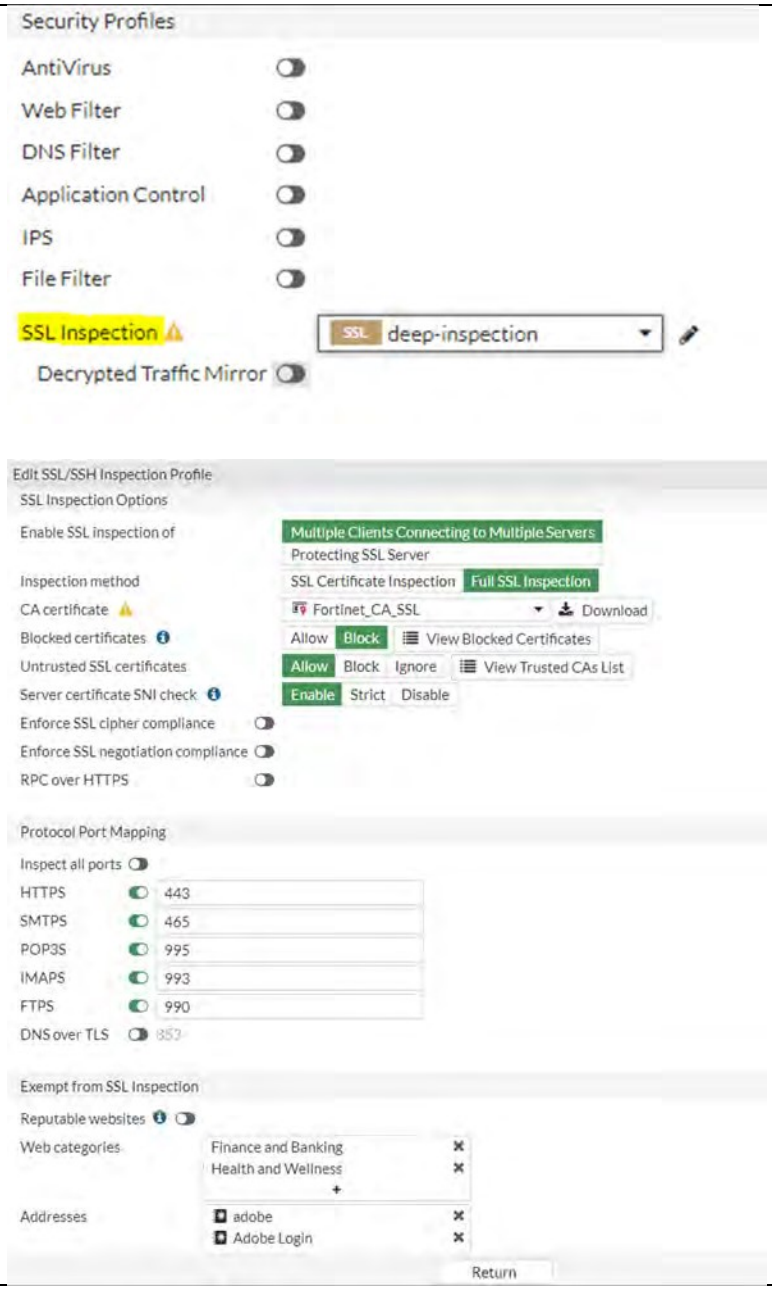
Item de Teste - 5.3.8.11	Deve ser capaz de inspecionar o tráfego criptografado SSL;
Objetivo do Teste	Validar se o FortiGate realiza inspeção SSL de pacotes de tráfego criptografado
Configuração do Teste	Demonstrar regra NGFW com inspeção SSL.
Procedimento do Teste	Para realizar SSL Inspection basta 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	


10.1.0.50 - Remote Desktop Connection
10.0.0.10 - /arquivos/
UOL - Seu universo online
Certificate for *.uol.com.br
https://www.uol.com.br
Connection security for www.uol.com.br
You are not securely connected to this site.
Your connection to this site is not private. Information you submit could be viewed by others (like passwords, messages, credit cards, etc.).
Your connection is not private and information you share with the site could be viewed by others.
This website contains content that is not secure (such as images).
Learn more
More information
INGRESSO.COM
BATE-PAPO
SAC
EMAIL
ENTRE
ASSINE UOL
uol
PagBank O BANCO COMPLETO
Dolar 4,745
Euro 5,253
São Paulo
27°C 15°C
PRODUTOS
NOTÍCIAS
TILT
ECOA
CANAL UOL
MOV
NOSSA
TAB
UOL PRIME
EMPEZAR
1) Haga clic en "Empezar" | 2) Iniciar la instalación | 3) Bloquear anuncios y malware
Web Companion
Juca Kfouri
Renato Augusto mantém a escrita em Itaquera
PVC
Renato só tem derrotas em Grêmio x Fla pela Copa BR
Wálter Maierovitch
Caso Moraes transita fora dos limites constitucionais
Reinaldo Azevedo
Rever leniência é matéria constituciona
Search
ENG
INTL
9:53 AM
7/26/2023

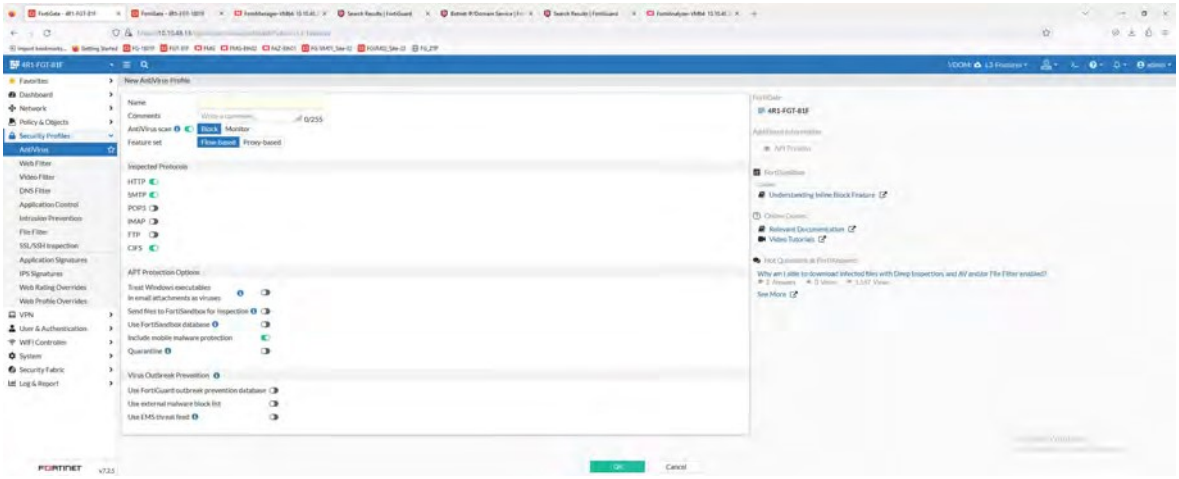
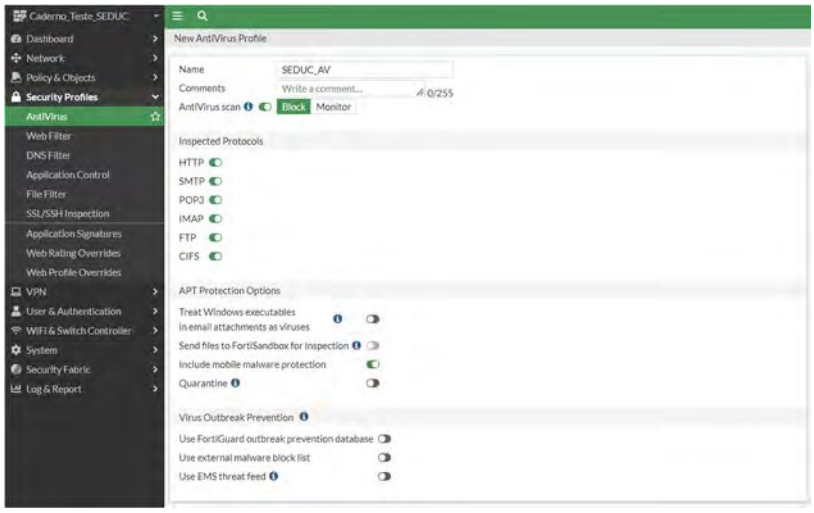

10.1.0.50 - Remote Desktop Connection
10.0.0.10 - /arquivos/
UOL - Seu universo online
Certificate for *.uol.com.br
Firefox
about:certificate?cert=MIIFYDCCBEigAwIBAgIUP8NSj5UGSSFqjUbXjDusrrFuKyowDQYJKo
Certificate
*.uol.com.br
FGT81FTK22013851
Subject Name
Common Name *.uol.com.br
Issuer Name
Country US
State/Province California
Locality Sunnyvale
Organization Fortinet
Organizational Unit Certificate Authority
Common Name FGT81FTK22013851
Email Address support@fortinet.com
Validity
Not Before Thu, 06 Jul 2023 00:00:00 GMT
Activate Windows
Search
ENG
INTL
9:54 AM
7/26/2023

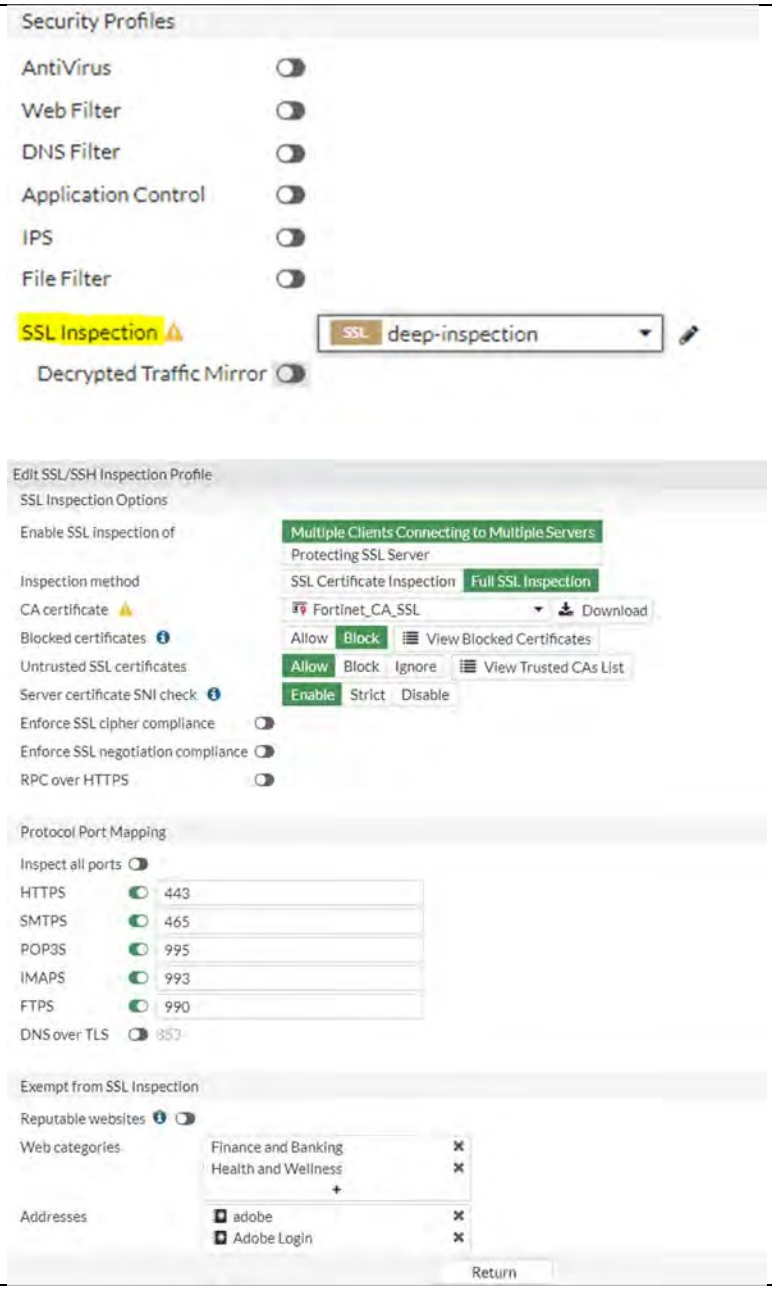


TESTE OK

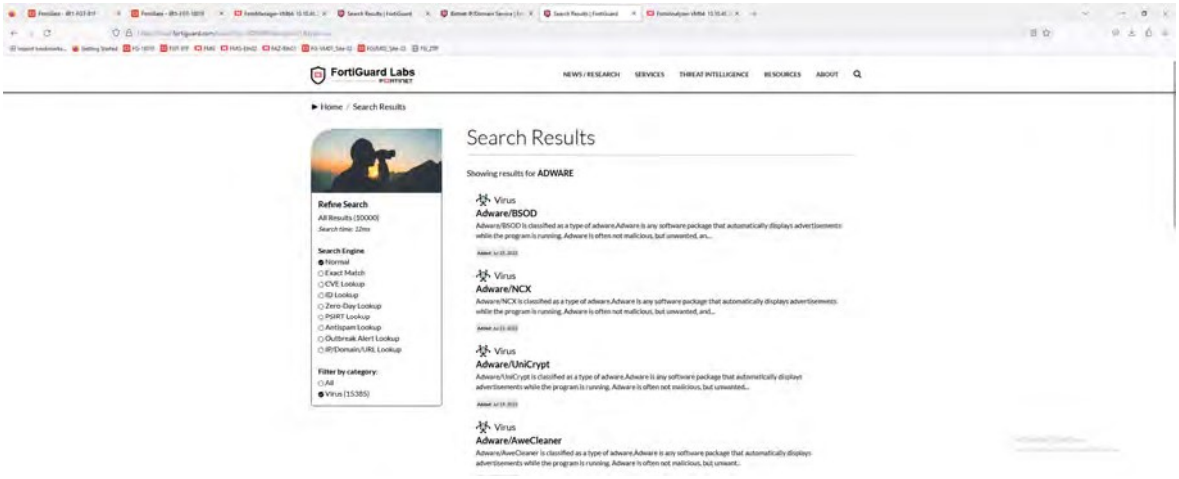
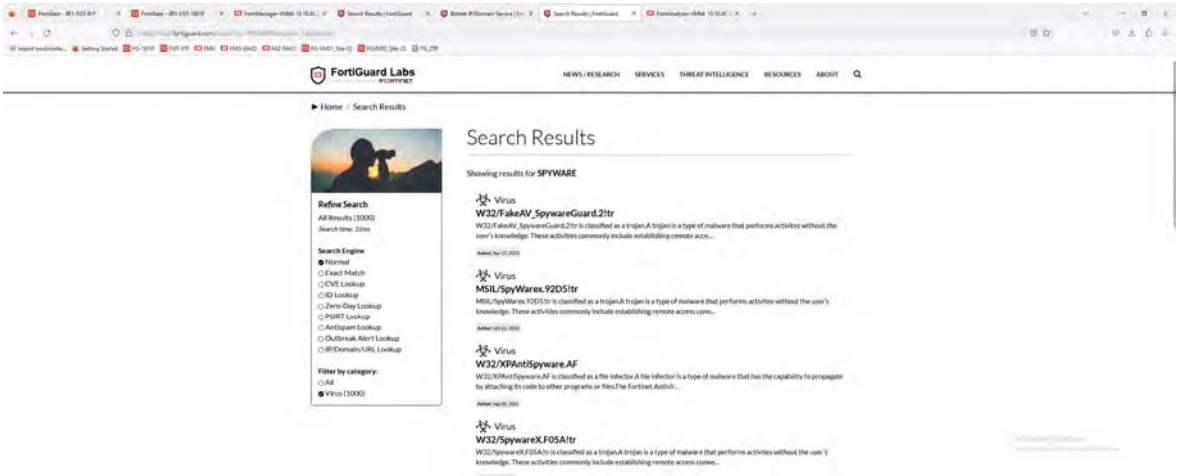
	
Comentário	

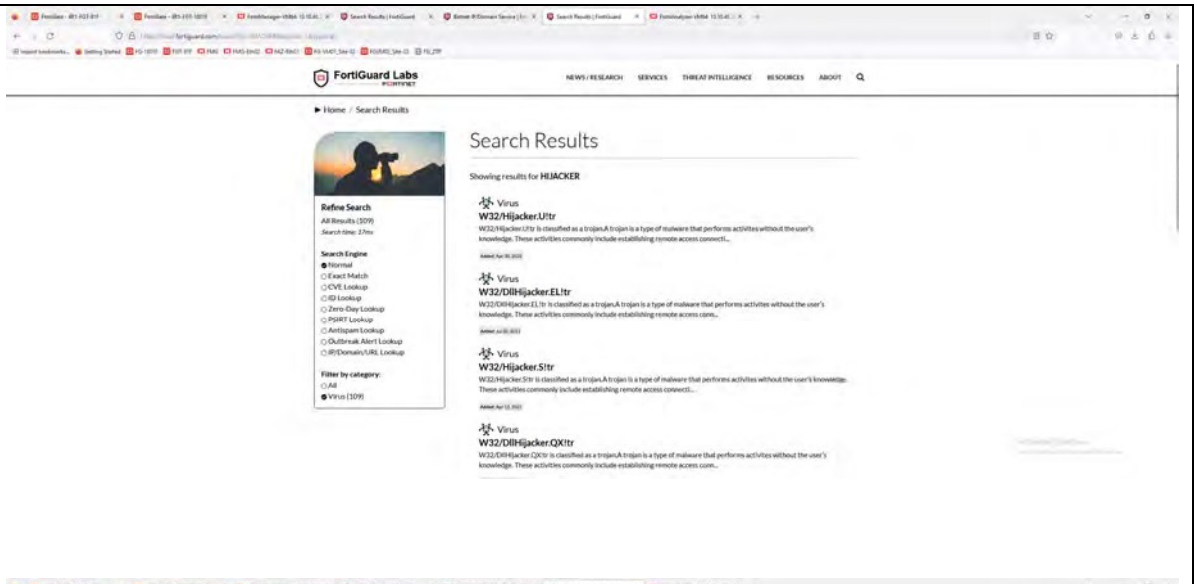
Item de Teste - 5.3.8.12	Deve ser capaz de inspecionar protocolos SMB/CIFS, SMTP, HTTP e HTTPS;
Objetivo do Teste	Validar se a ferramenta é capaz de inspecionar protocolos SMB/CIFS, SMTP, HTTP e HTTPS;
Configuração do Teste	Demonstrar inspeção: SMB/CIFS, SMTP, HTTP e HTTPS

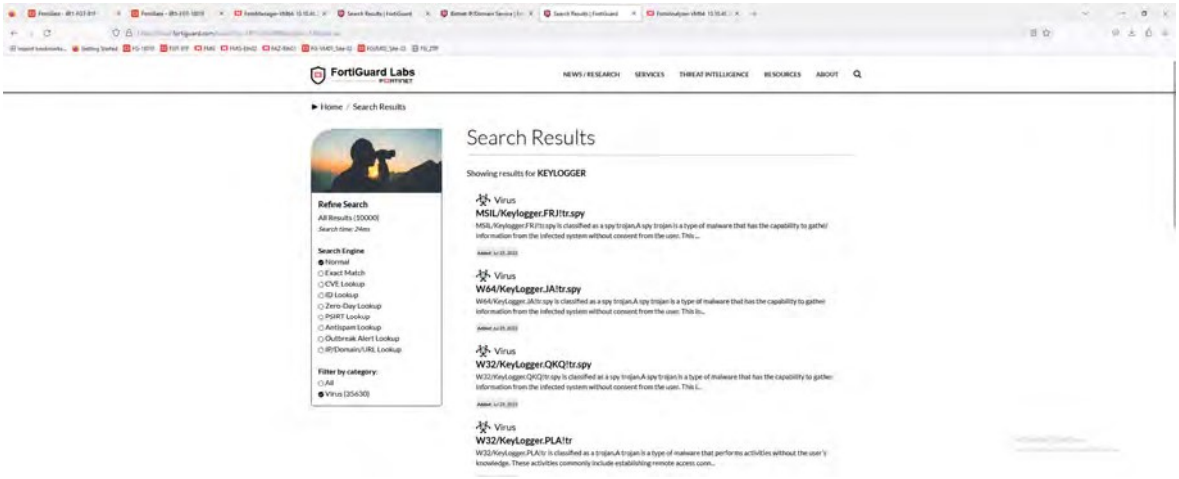
Procedimento do Teste	A inspeção de protocolos é feita de duas formas. A primeira é utilizando o Security Profile de Antivírus, onde é possível inspecionar os protocolos HTTP, SMTP, POP3, IMAP, FTP, CIFS. A segunda forma é utilizando SSL Deep Inspection onde é possível realizar a inspeção de protocolos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

	
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 Antívirus.

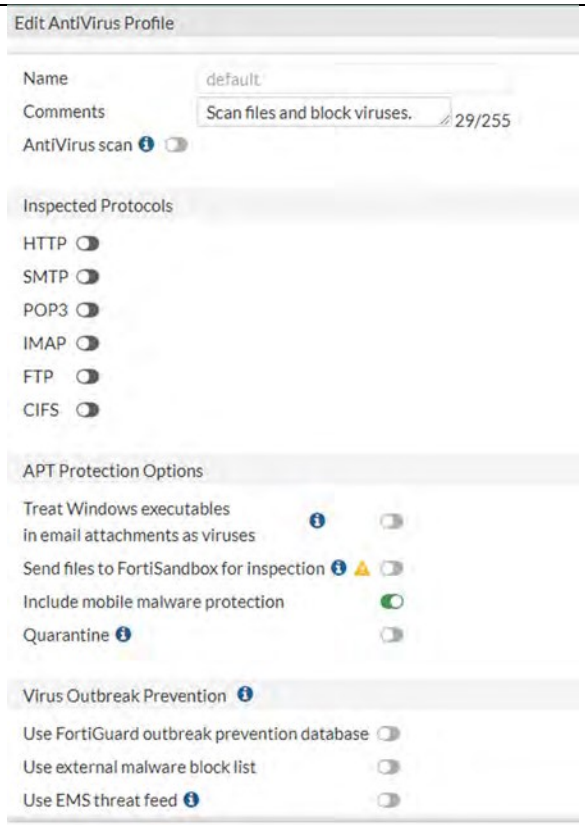
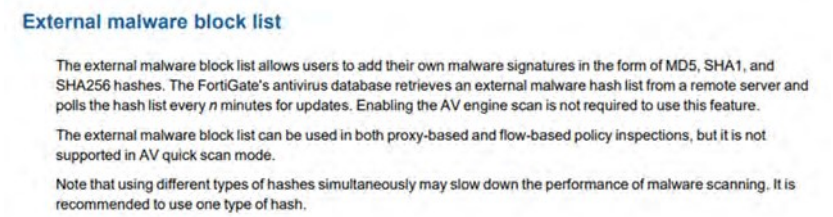
Procedimento do Teste	Demonstrar a configuração de regra com filtro de Antívirus.
Evidências	 





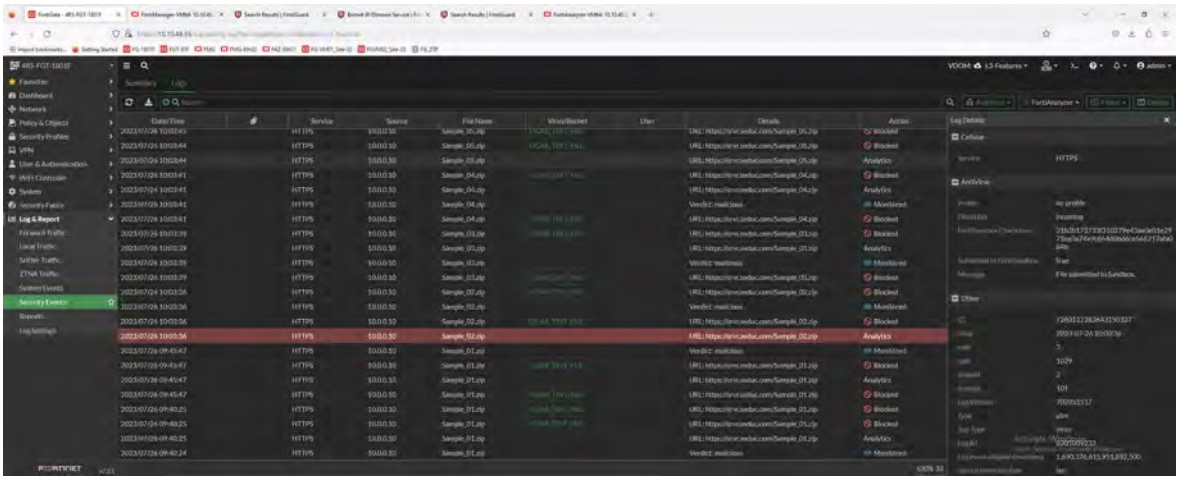
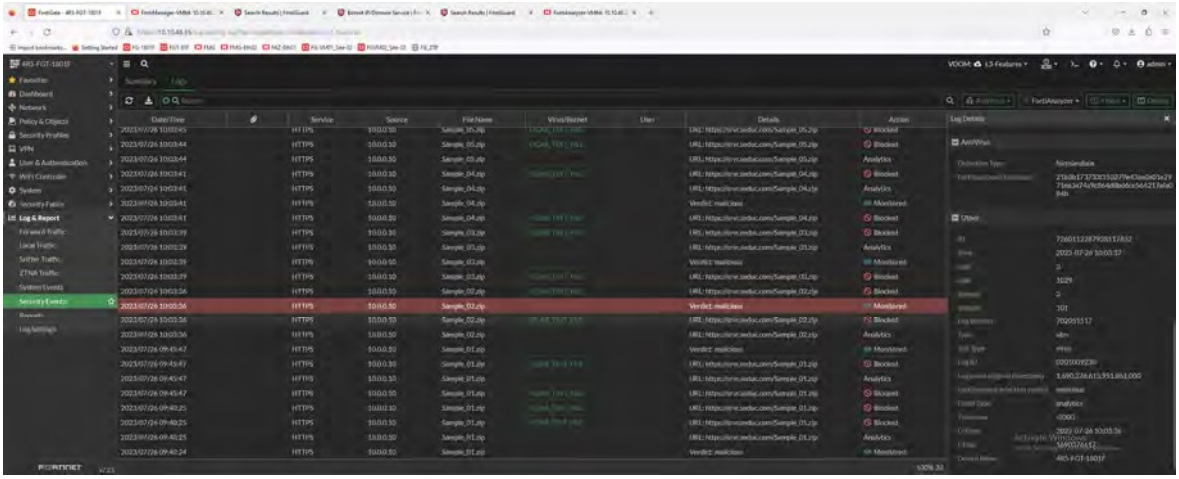
TESTE OK

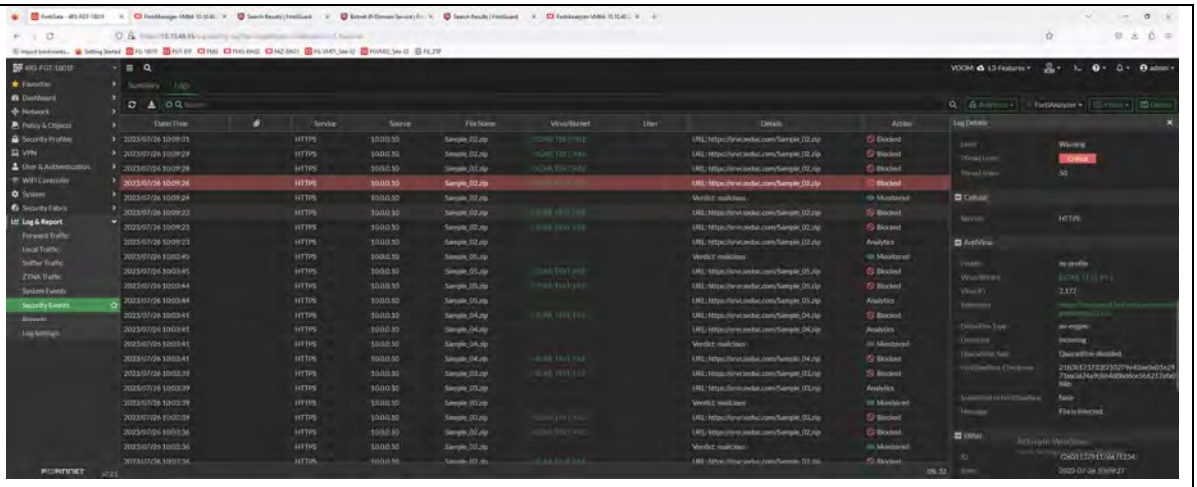
Todos os bloqueios de malwares são feitos pelo Antivírus do FortiGate, caso haja a necessidade de adicionar outras assinaturas além das que já são mapeadas pela FortiGuard, o FortiGate te dá a opção de adicioná-las à base de dados dele.

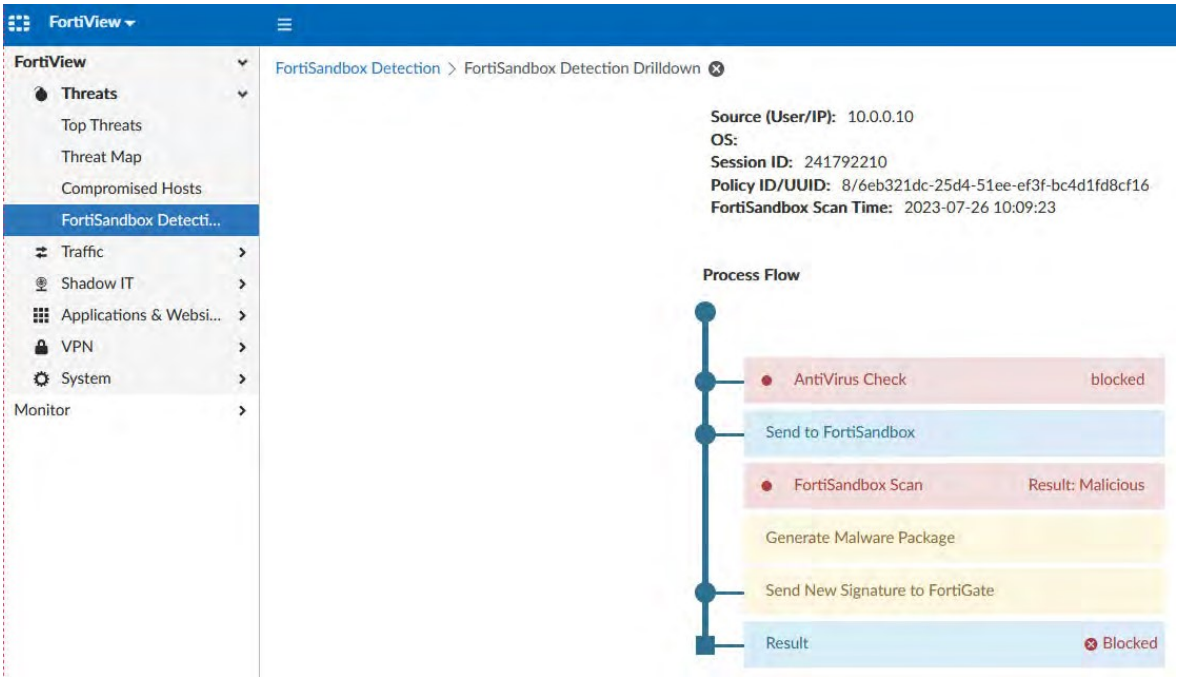
	 
Comentário	https://docs.fortinet.com/document/fortigate/7.2.0/administration-guide/254346

5.3.9 AMEAÇAS AVANÇADAS PERSISTENTES - APT:

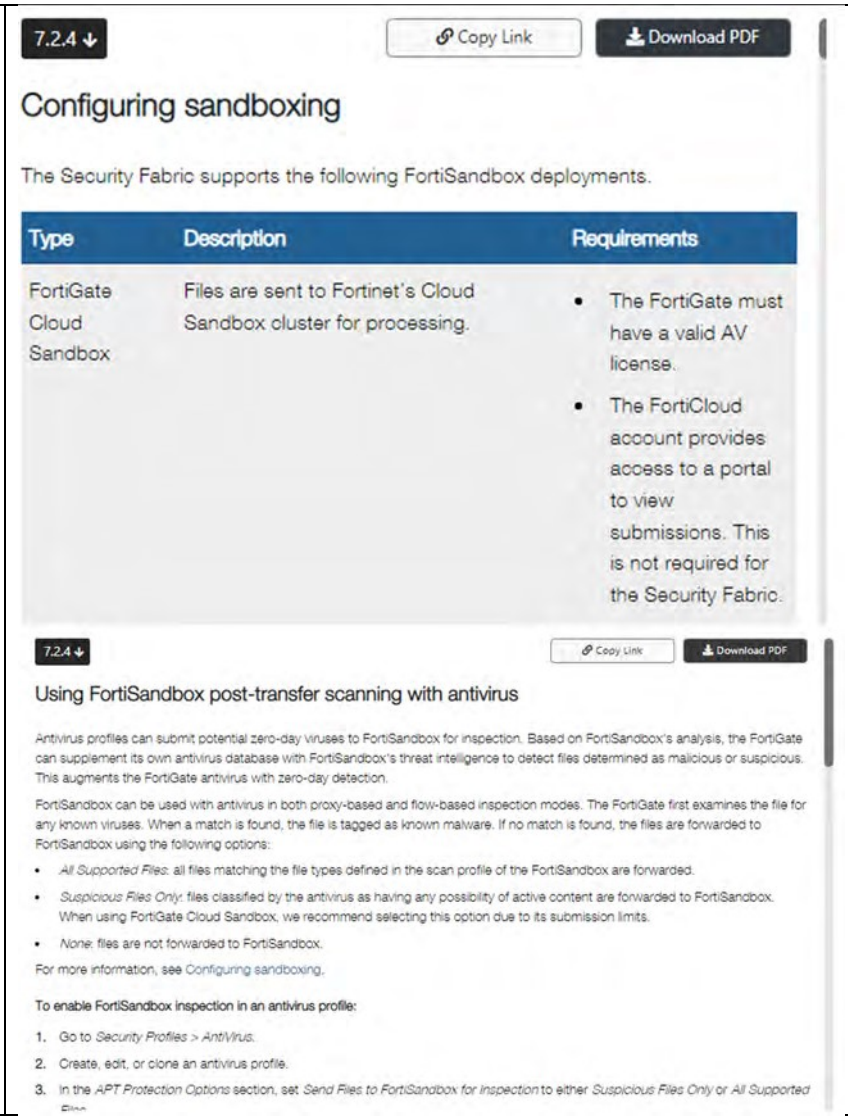
Item de Teste - 5.3.9.1	Deverá prover as funcionalidades de inspeção de tráfego de entrada de malwares não conhecidos (dia zero) ou do tipo APT (Advanced Persistent Threat) com filtro de ameaças avançadas e análise de execução em tempo real;
Objetivo do Teste	Validar se a solução promove a funcionalidade 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.

	Após realizar as configurações para habilitar o Sandbox basta navegar por Security Profiles > AntiVírus > Create New > APT Protection Options e habilitar o envio de arquivos para a inspeção do Sandbox. Por último basta incluir o perfil criado no fluxo da política em que deseja realizar a inspeção.
Evidências	 




FortiView
FortiView
Threats
Top Threats
Threat Map
Compromised Hosts
FortiSandbox Detecti...
Traffic
Shadow IT
Applications & Websi...
VPN
System
Monitor
FortiSandbox Detection > FortiSandbox Detection Drilldown
Source (User/IP): 10.0.0.10
OS:
Session ID: 241792210
Policy ID/UUID: 8/6eb321dc-25d4-51ee-ef3f-bc4d1fd8cf16
FortiSandbox Scan Time: 2023-07-26 10:09:23
Process Flow
AntiVirus Check
blocked
Send to FortiSandbox
FortiSandbox Scan
Result: Malicious
Generate Malware Package
Send New Signature to FortiGate
Result
Blocked

TESTE OK



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.	• 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.

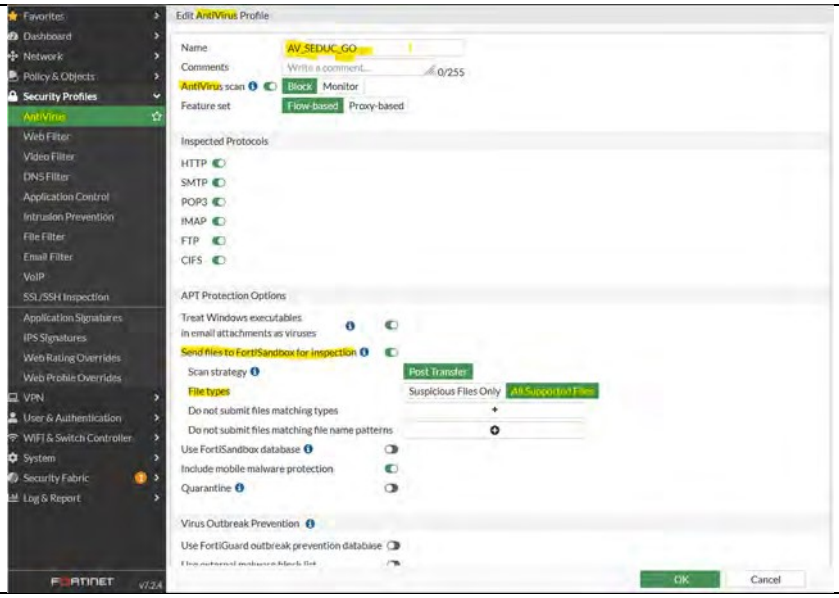
FortiSandbox can be used with antivirus in both proxy-based and flow-based inspection modes. The FortiGate first examines the file for any known viruses. When a match is found, the file is tagged as known malware. If no match is found, the files are forwarded to FortiSandbox using the following options:

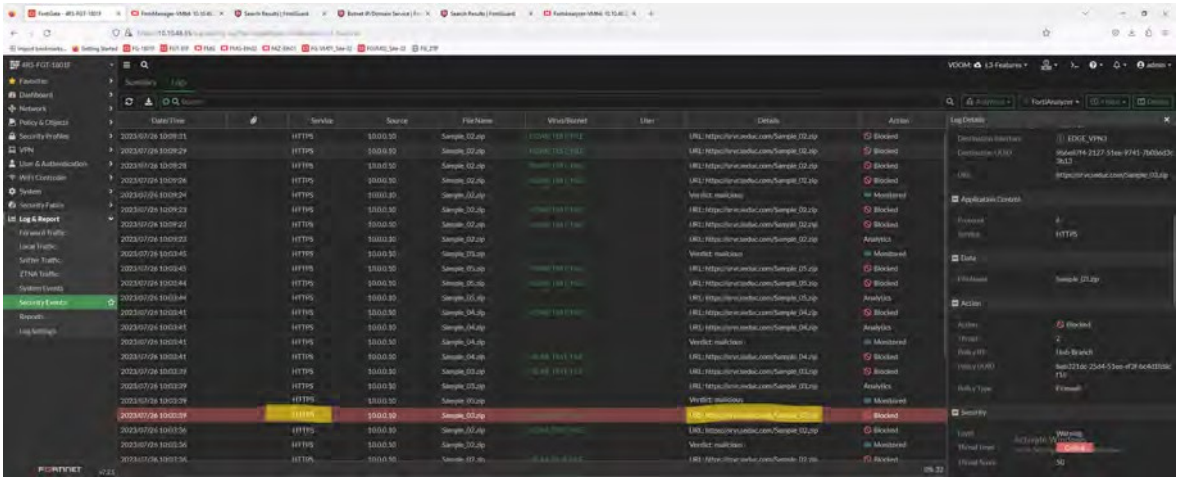
- *All Supported Files*: all files matching the file types defined in the scan profile of the FortiSandbox are forwarded.
- *Suspicious Files Only*: files classified by the antivirus as having any possibility of active content are forwarded to FortiSandbox. When using FortiGate Cloud Sandbox, we recommend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

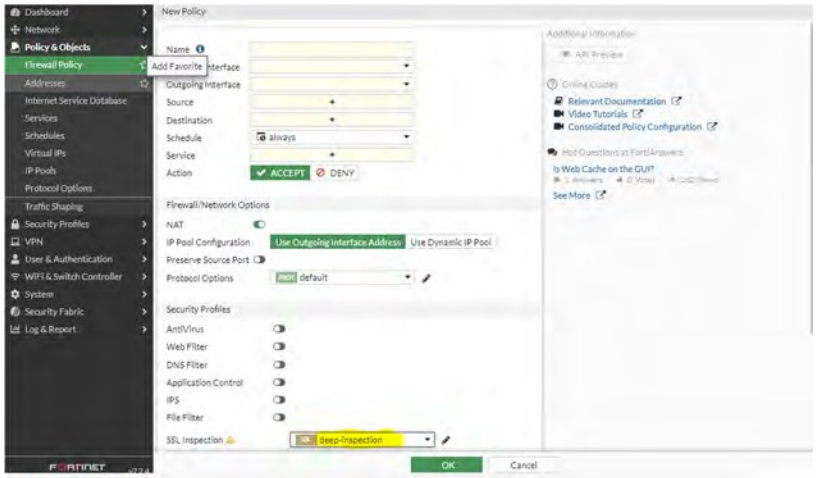
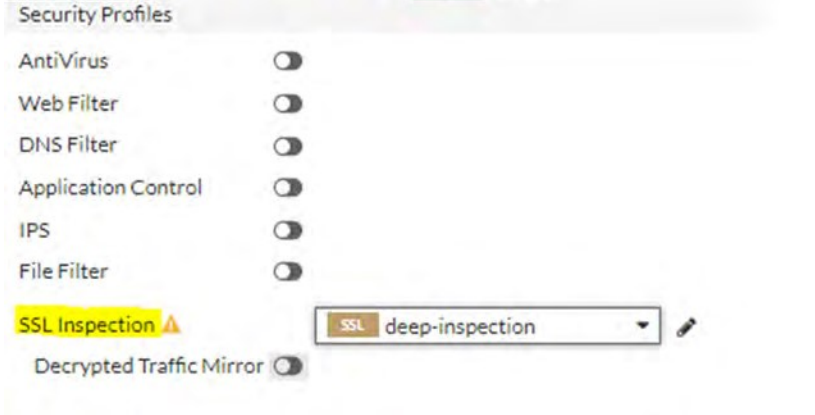
For more information, see Configuring sandboxing.

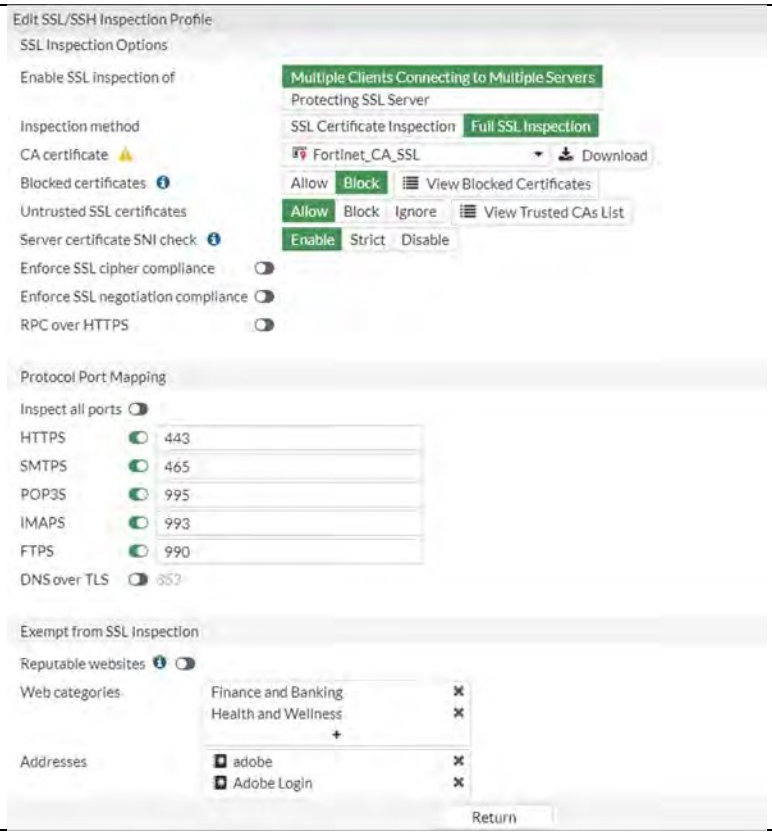
To enable FortiSandbox inspection in an antivirus profile:

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*

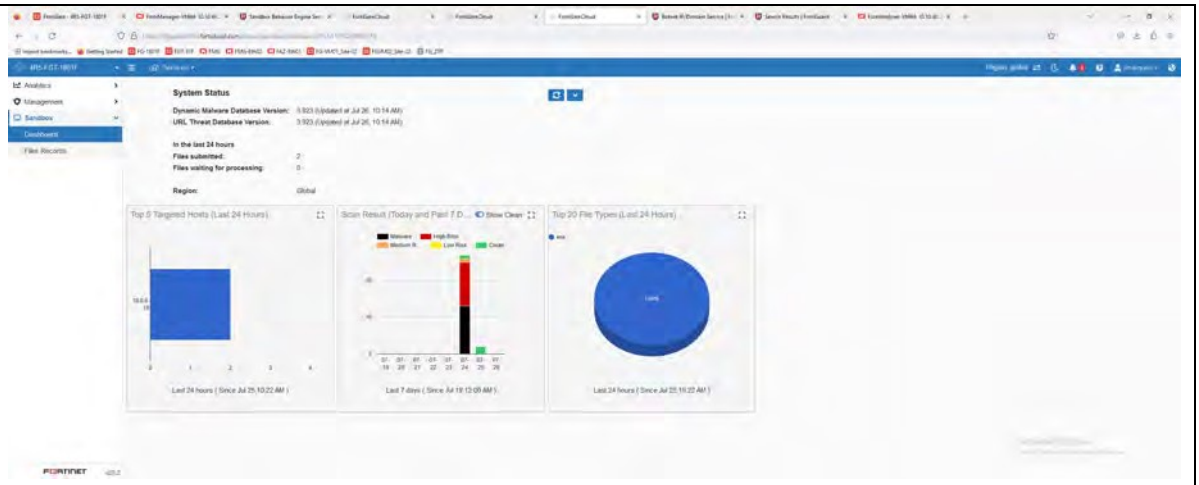
	
Comentário	https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/481589 https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/660221/configuring-sandboxing

Item de Teste - 5.3.9.2	A solução 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	Criar regra de 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	

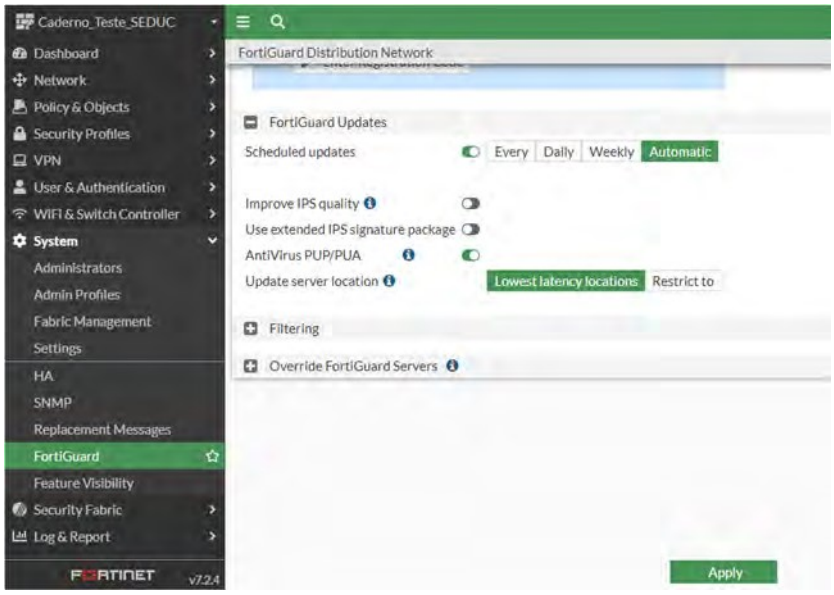
	TESTE OK  

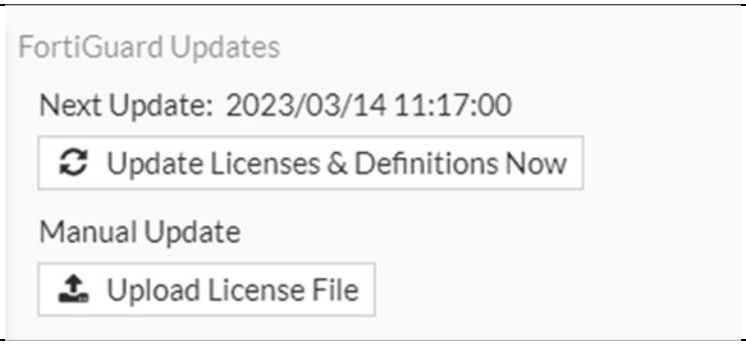
	
Comentário	

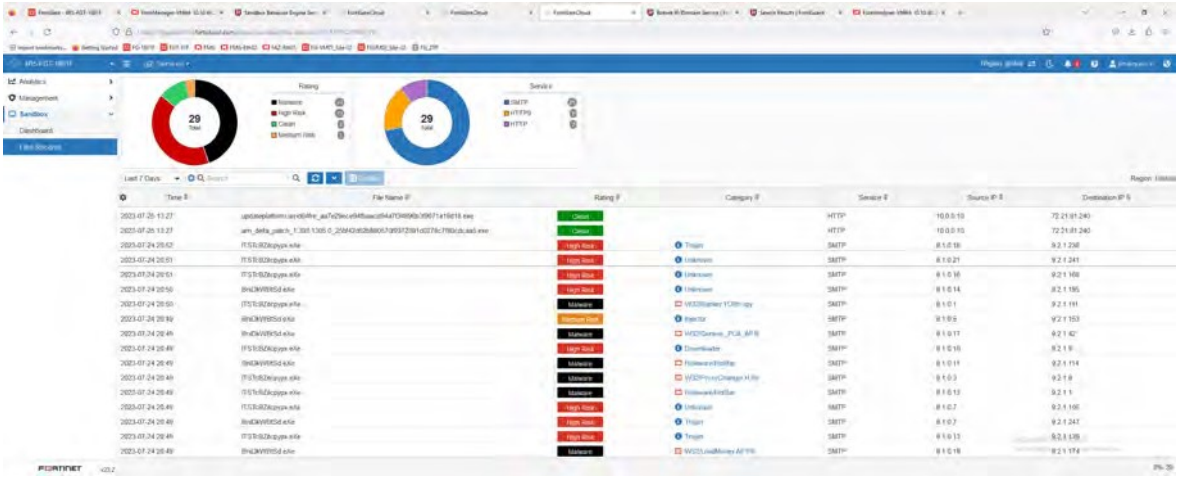
Item de Teste - 5.3.9.5	Implementar atualização da base de dados da rede de inteligência de forma automática;
Objetivo do Teste	Verificar se a base de dados da rede de inteligência atualiza de forma automatizada.
Configuração do Teste	Demonstrar tela de atualização
Procedimento do Teste	Para ter acesso 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
Evidências	


System Status
Dynamic Malware Database Version:
URL Threat Database Version:
In the last 24 hours
Files submitted:
Files waiting for processing:
Region:
Global

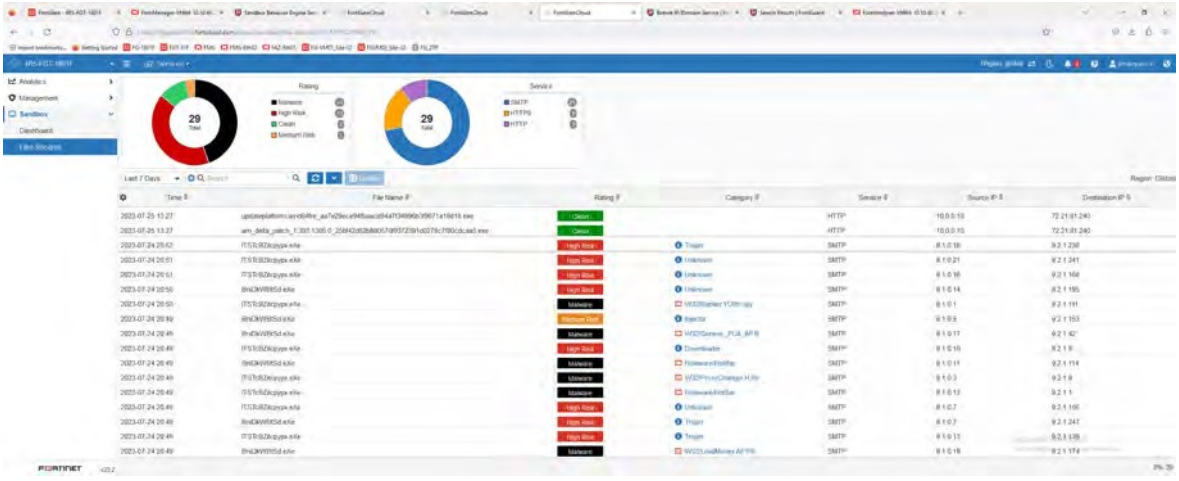
TESTE OK


Caderno_Teste_SEDUC
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi & Switch Controller
System
Administrators
Admin Profiles
Fabric Management
Settings
HA
SNMP
Replacement Messages
FortiGuard
Feature Visibility
Security Fabric
Log & Report
FORTINET
v7.2.4
FortiGuard Distribution Network
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
Filtering
Override FortiGuard Servers
Apply

	
Comentário	

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	 **TESTE OK** 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.

	
Comentário	

Item de Teste - 5.3.9.7	Toda análise deverá ser realizada de forma interna em Appliance do 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	 **TESTE OK**

	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.
Comentário	

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.	• 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.	• 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.	• 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.

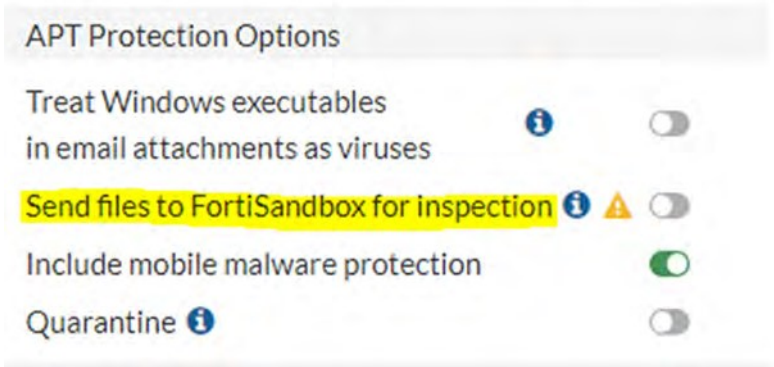
FortiSandbox can be used with antivirus in both proxy-based and flow-based inspection modes. The FortiGate first examines the file for any known viruses. When a match is found, the file is tagged as known malware. If no match is found, the files are forwarded to FortiSandbox using the following options:

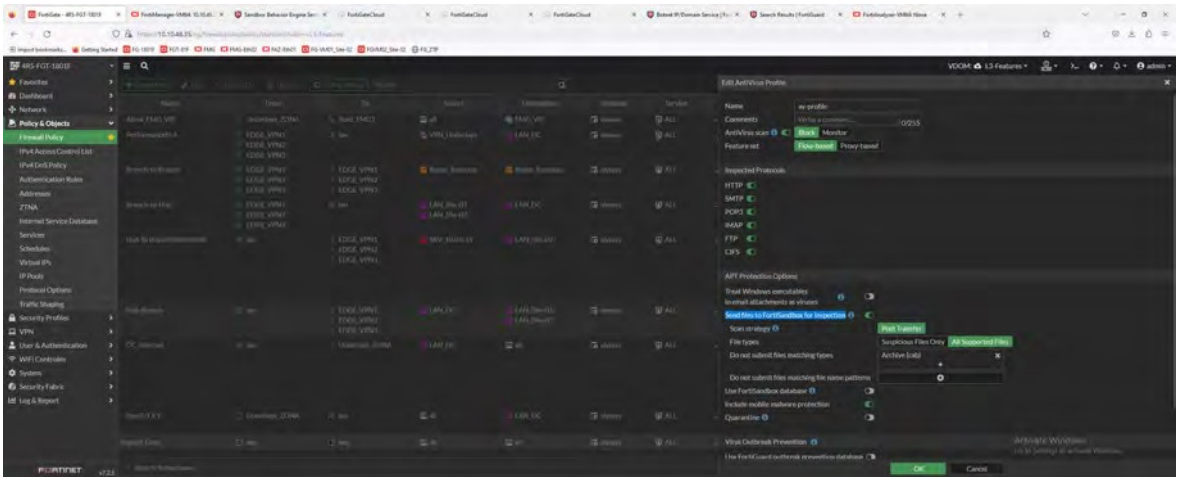
- *All Supported Files*: all files matching the file types defined in the scan profile of the FortiSandbox are forwarded.
- *Suspicious Files Only*: files classified by the antivirus as having any possibility of active content are forwarded to FortiSandbox. When using FortiGate Cloud Sandbox, we recommend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

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*.



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	Primeiro é necessário configurar a funcionalidade “FortiGate Cloud Sandbox” no FortiGate. Após realizar as configurações para habilitar o Sandbox basta navegar por **Security Profiles** > **AntiVírus** > **Create New** > **APT Protection Options** e habilitar o envio de arquivos para a inspeção do Sandbox. Por último basta incluir o perfil criado no fluxo da política em que deseja realizar a inspeção.
Evidências	 **TESTE OK**

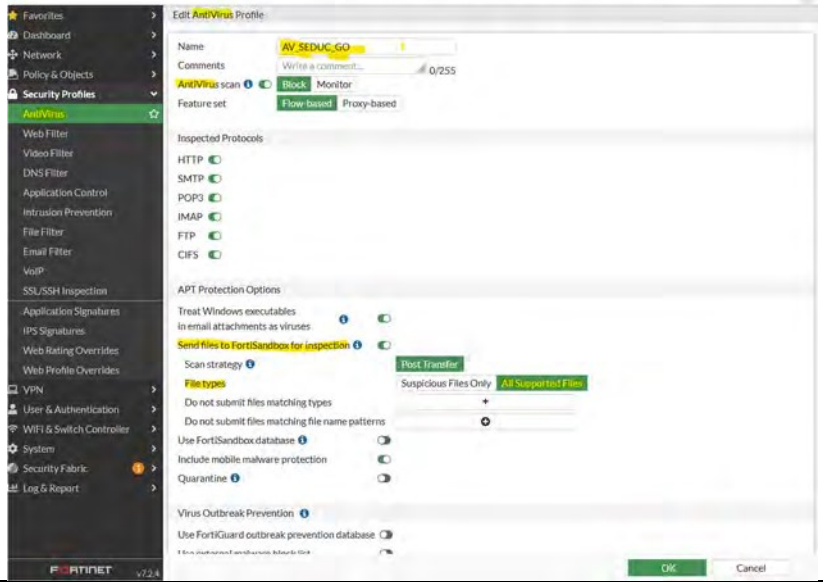
7.2.3 ↓ Copy Link Download PDF

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.

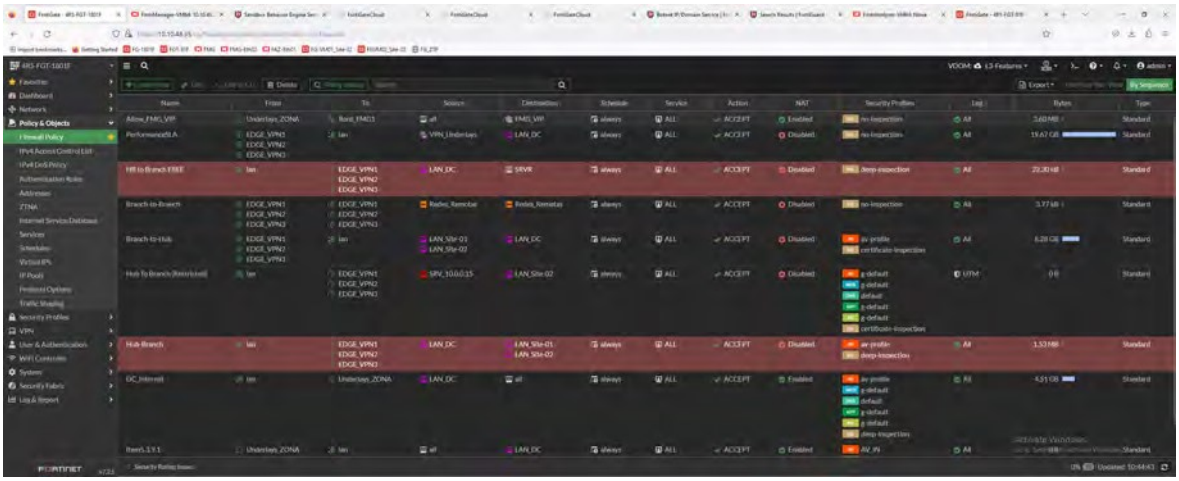
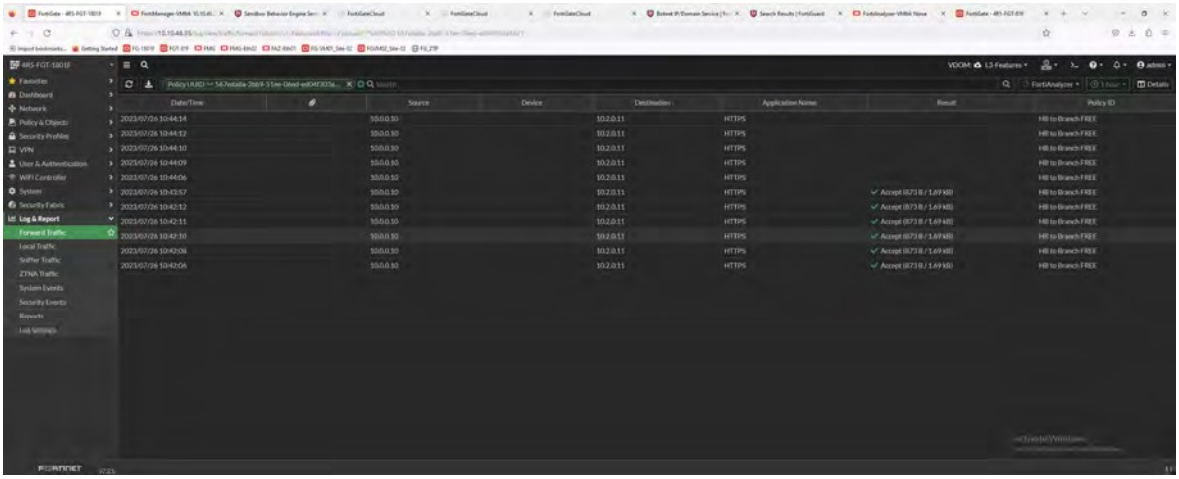
FortiSandbox can be used with antivirus in both proxy-based and flow-based inspection modes. The FortiGate first examines the file for any known viruses. When a match is found, the file is tagged as known malware. If no match is found, the files are forwarded to FortiSandbox using the following options:

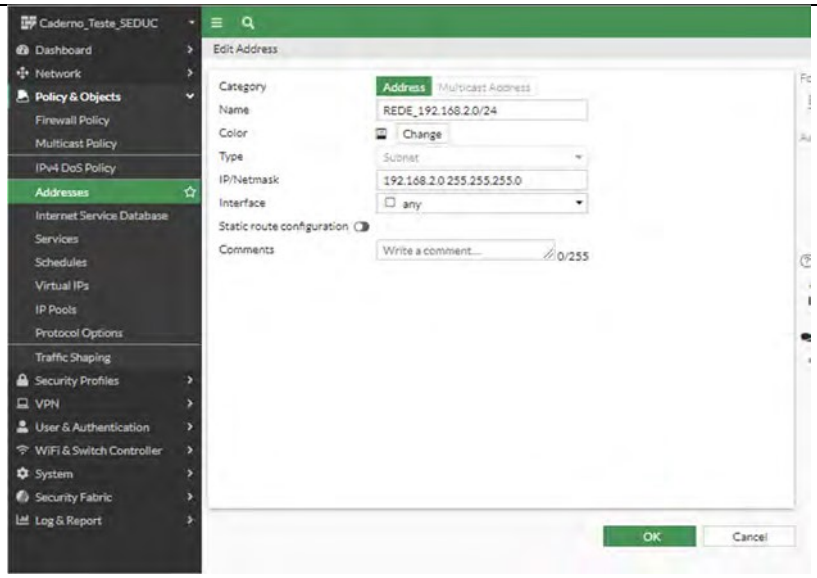
- *All Supported Files*: all files matching the file types defined in the scan profile of the FortiSandbox are forwarded.
- *Suspicious Files Only*: files classified by the antivirus as having any possibility of active content are forwarded to FortiSandbox. When using FortiGate Cloud Sandbox, we recommend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

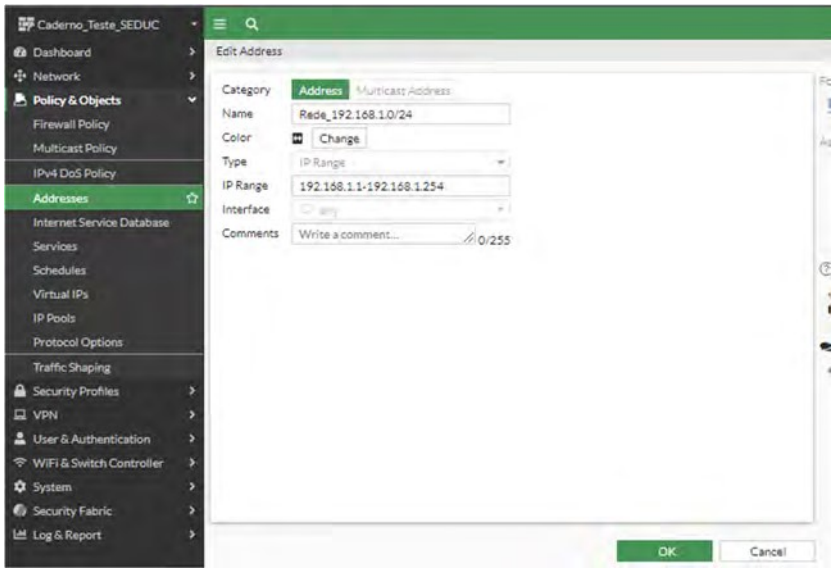


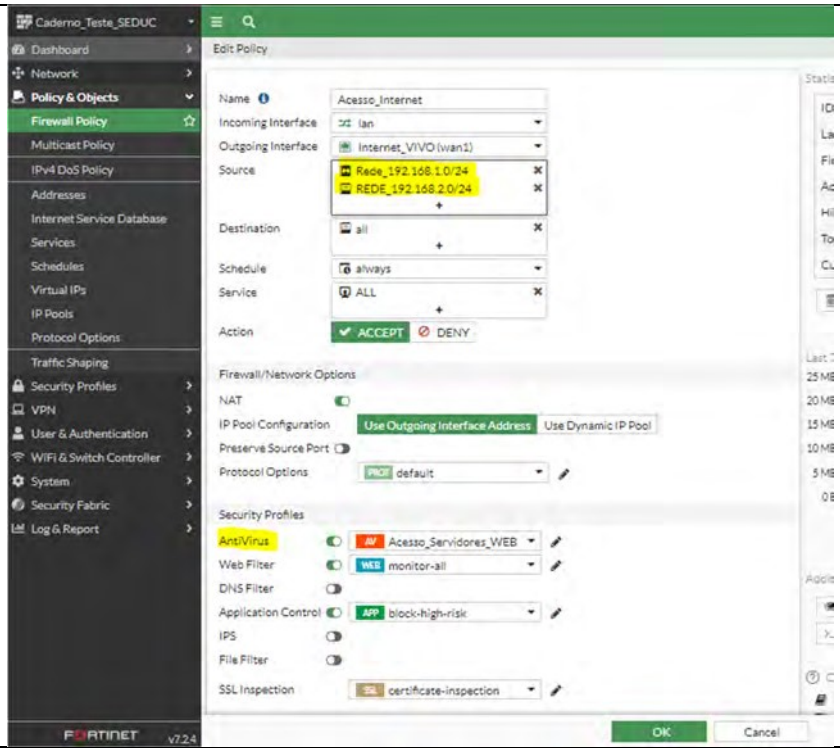
	
Comentário	https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/481589 https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/660221/configuring-sandboxing

Item de Teste - 5.3.9.11	Toda a análise ou bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real;
Objetivo do Teste	Validar que a aplicação faz a análise ou bloqueio de malwares e/ou códigos maliciosos em tempo real
Configuração do Teste	Possuir 1(um) FortiGate com uma regra de firewall contendo um Perfil de Antivírus configurado.
Procedimento do Teste	Demonstrar relatórios no site do Fabricante.
Evidências	Conforme subitem comprovado 5.3.9.1 **TESTE OK** 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. 
Comentário	

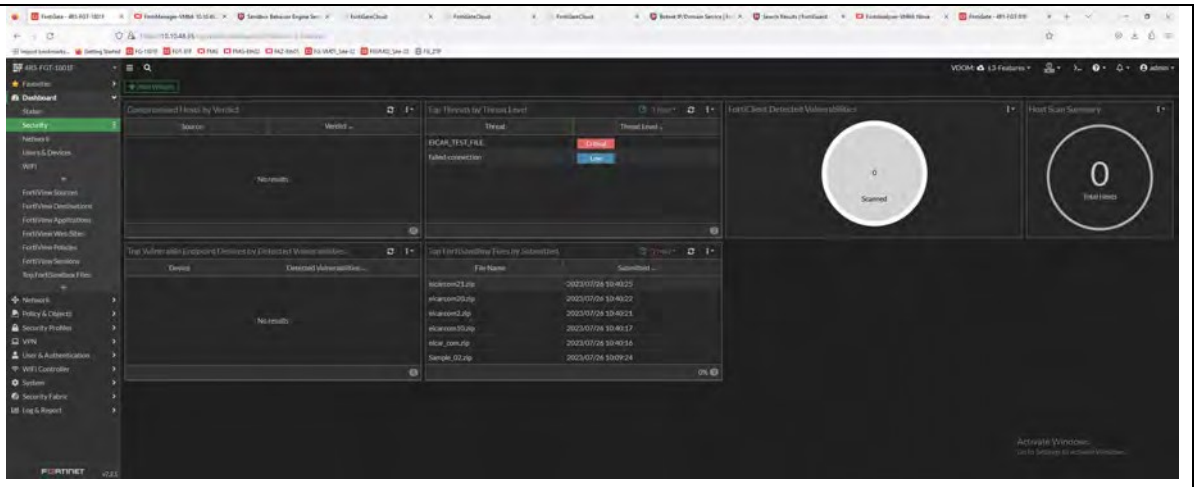
Item de Teste - 5.3.9.12	Implementar mecanismo de exceção, permitindo a criação de regras por sub-rede e endereço IP;
Objetivo do Teste	Validar se a solução implementa mecanismo de exceção, permitindo a criação de regras utilizando sub-redes e endereços de IP
Configuração do Teste	Demonstrar regras de exceção.
Procedimento do Teste	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 Navegando por **Security Profiles** > **Antivírus** > **Create New** é possível criar um novo profile de Antivírus onde é ativado a função de ATP (FortiGate Sandbox) Por último basta enquadrar os usuários e grupos criados no campo “source” da política.
Evidências	  **TESTE OK** 1 - Criação dos objetos


Caderno_Teste_SEDUC
Dashboard
Network
Policy & Objects
Firewall Policy
Multicast Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
WiFi & Switch Controller
System
Security Fabric
Log & Report
Edit Address
Category
Address
Multicast Address
Name
REDE_192.168.2.0/24
Color
Change
Type
Subnet
IP/Netmask
192.168.2.0 255.255.255.0
Interface
any
Static route configuration
Comments
Write a comment...
0/255
OK
Cancel


Caderno_Teste_SEDUC
Dashboard
Network
Policy & Objects
Firewall Policy
Multicast Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
WiFi & Switch Controller
System
Security Fabric
Log & Report
Edit Address
Category
Address
Multicast Address
Name
Rede_192.168.1.0/24
Color
Change
Type
IP Range
IP Range
192.168.1.1-192.168.1.254
Interface
Comments
Write a comment...
0/255
OK
Cancel

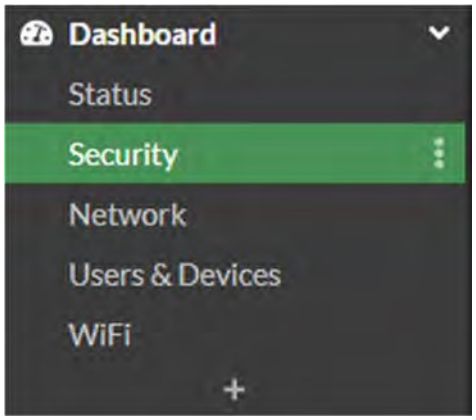
	
Comentário	https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/656084/firewall-policy#FirewallPolicyParameters

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	

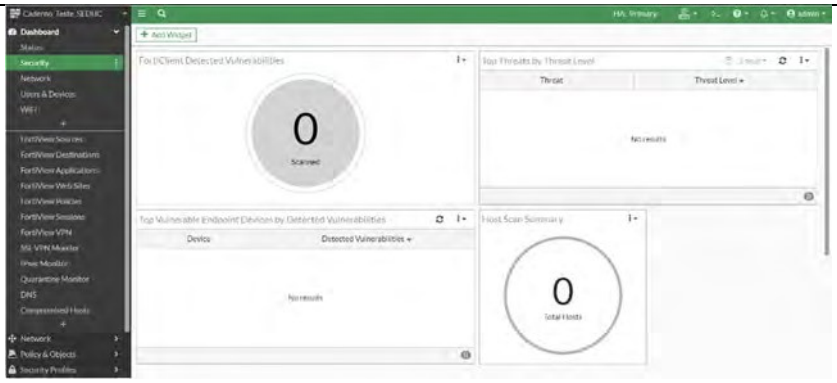
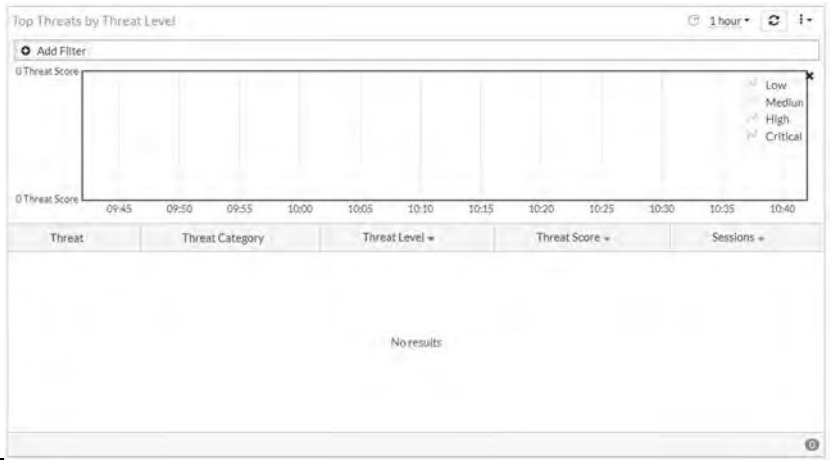


TESTE OK

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

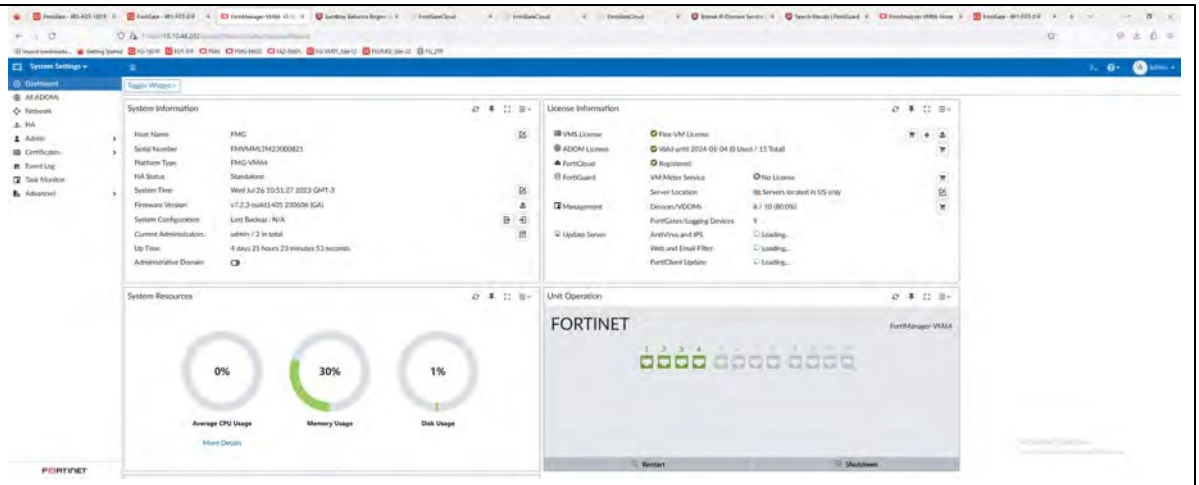


Lá podemos ter acesso a diversas funcionalidades referentes a visualização de eventos de segurança detectados pela solução.

	 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

FORTINET

DATA SHEET

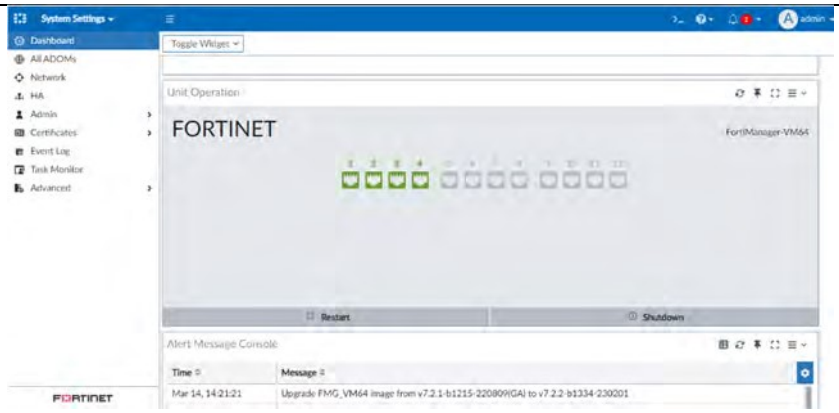
FortiManager

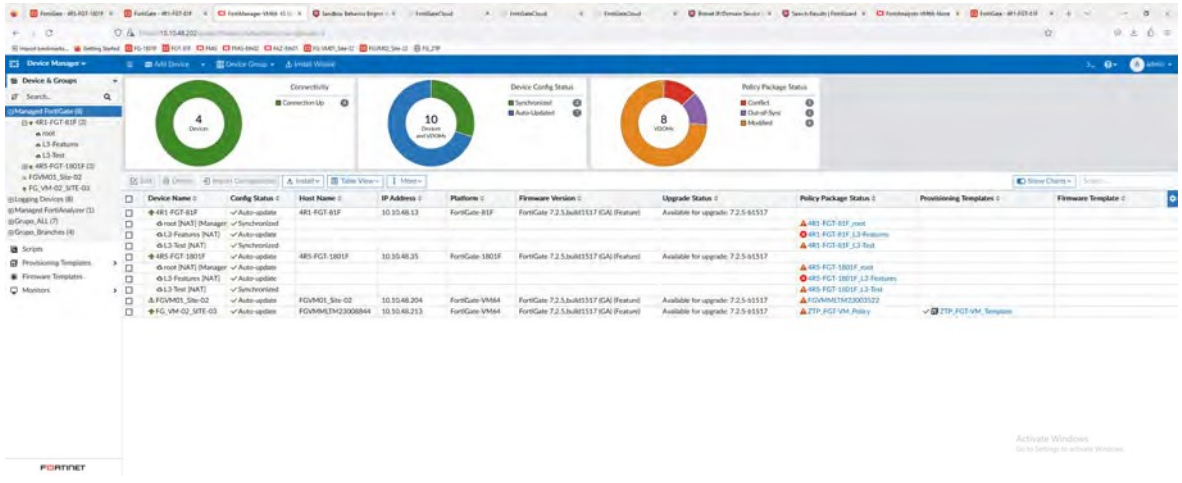
Available in:

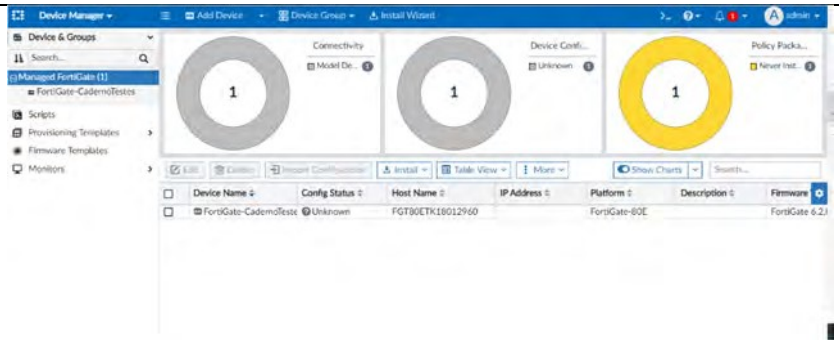
Appliance Virtual Machine Cloud

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.

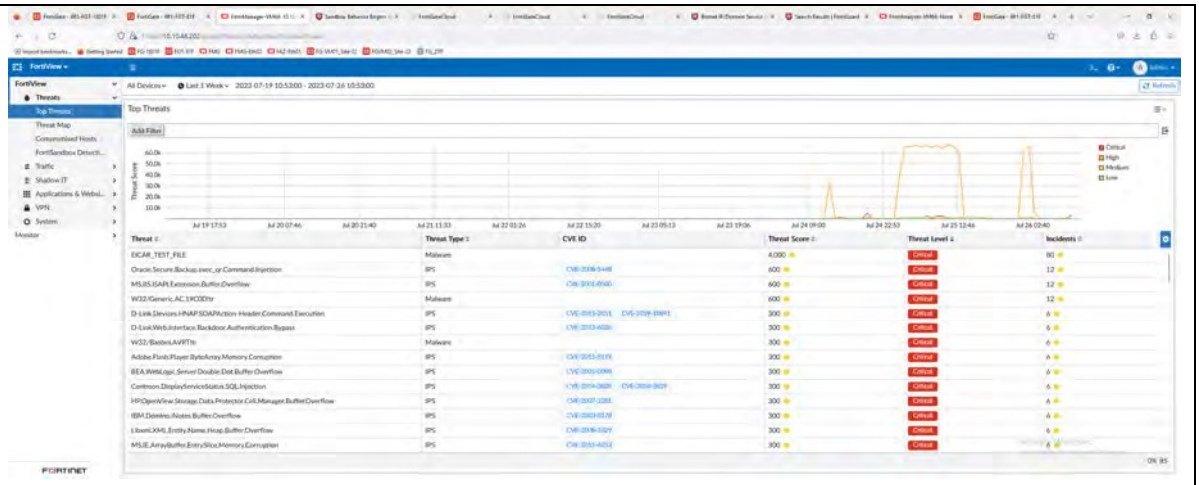
Integrated with the Fortinet Security Fabric advanced security architecture and automation driven network operations capabilities provide a solid foundation to secure and optimize your network security.

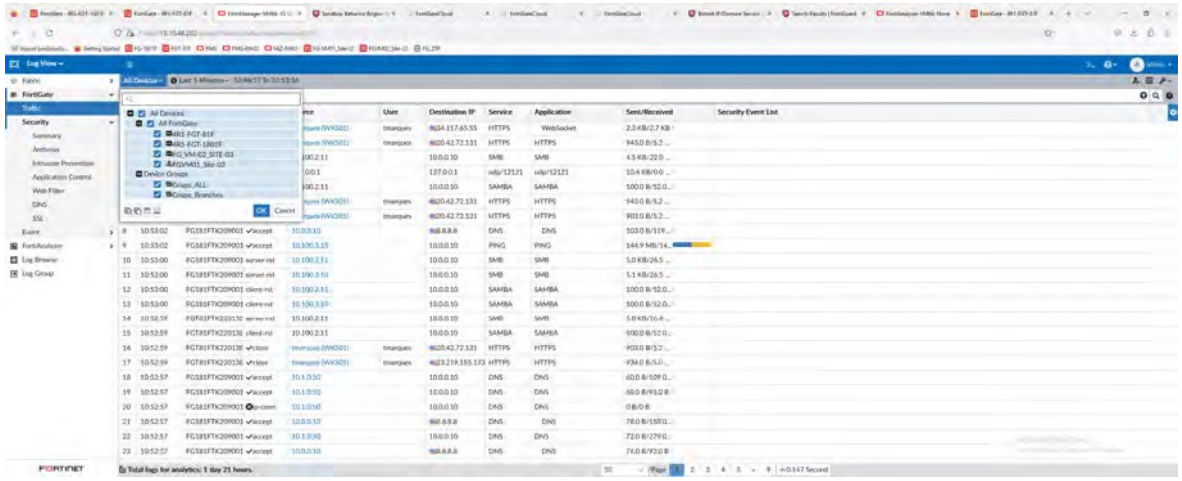
	
Comentário	Fonte: FortiManager Data Sheet acessado em https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf

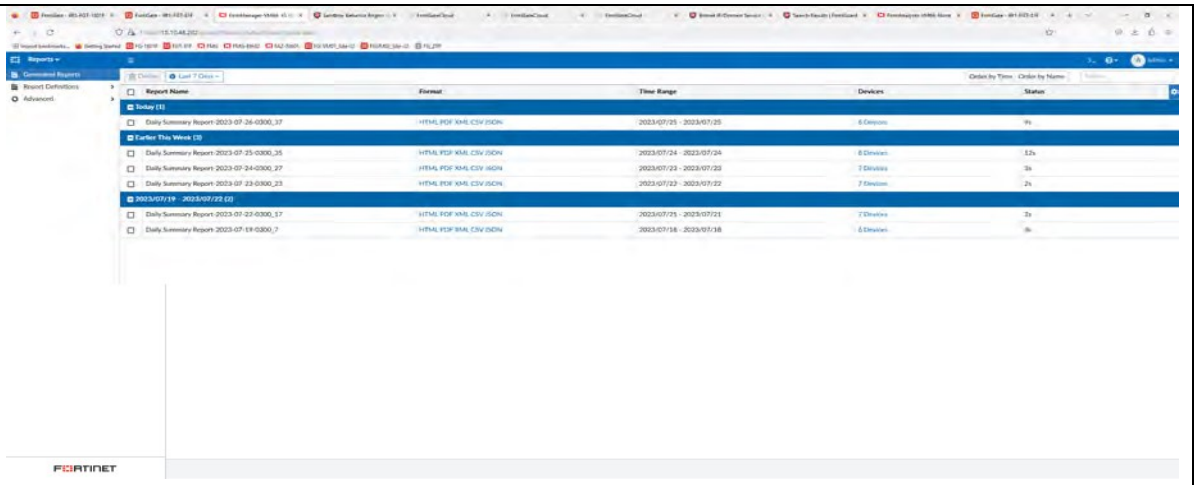
Item de Teste - 5.4.2	A solução deve ser capaz de gerenciar todos os equipamentos de Segurança de forma centralizada;
Objetivo do Teste	Comprovar que a solução consegue gerenciar todos os equipamentos de segurança de forma centralizada.
Configuração do Teste	Demonstrar que o FortiManager suporta gerenciar 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	 **TESTE OK**

	 
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	

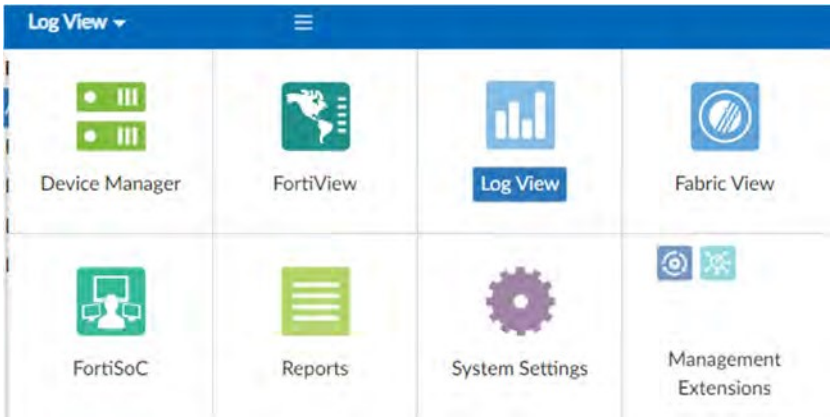


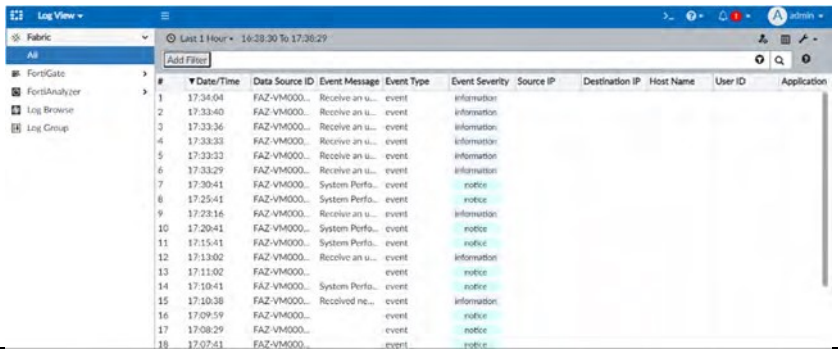




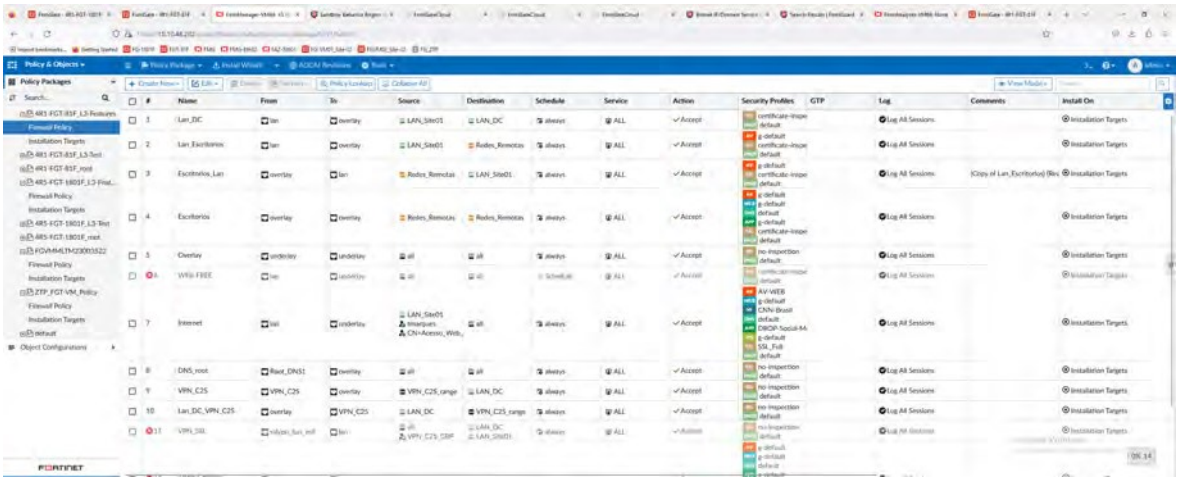
TESTE OK

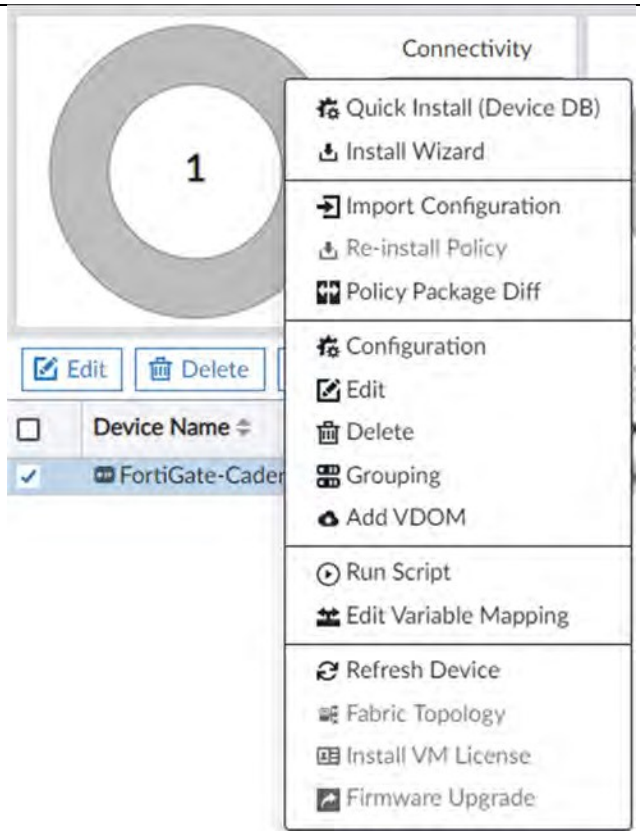
Para acessar essa funcionalidade basta acessar o “Log View”.

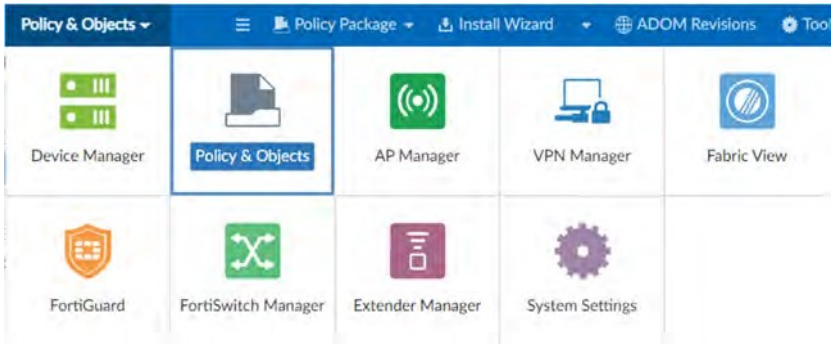


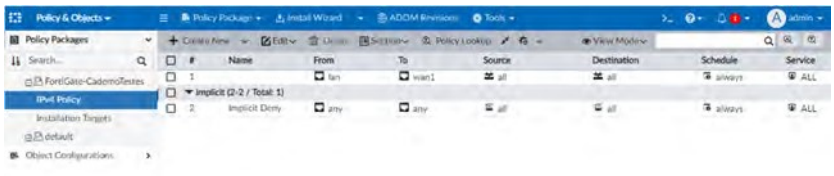


Comentário	

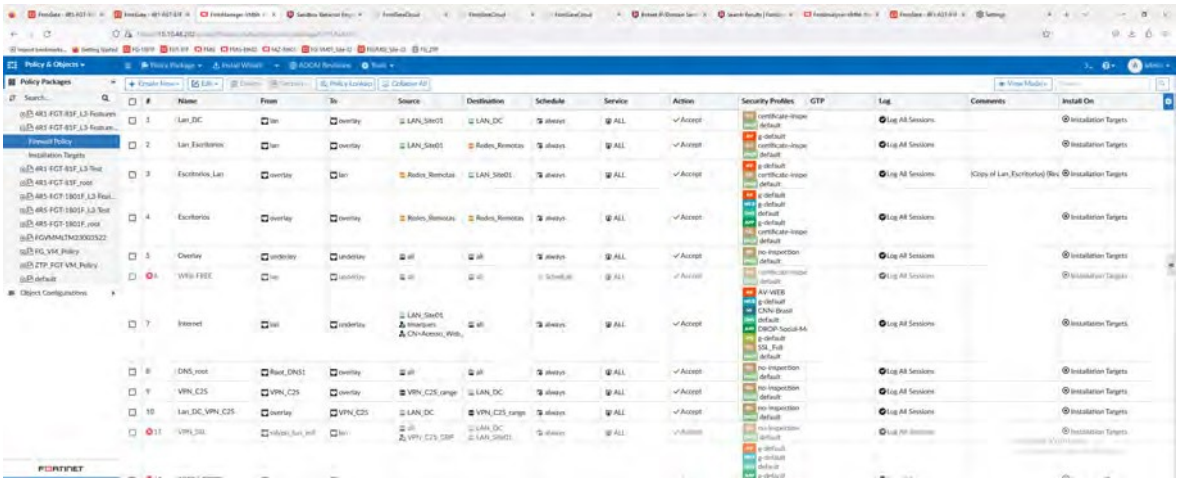
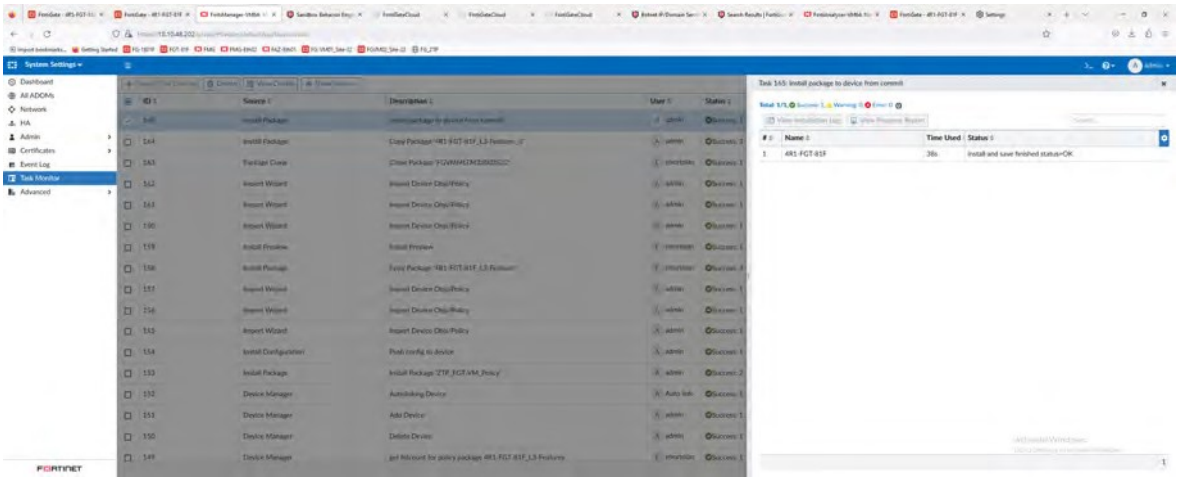
Item de Teste - 5.4.5	O gerenciamento de políticas será realizado em um único ponto centralizado;
Objetivo do Teste	Validar que o equipamento de gerência realiza esse gerenciamento das políticas em um só lugar.
Configuração do Teste	Demonstrar o FortiManager com os FortiGates integrados
Procedimento do Teste	Para ter acesso as políticas dos equipamentos gerenciados, primeiro tem de ser feita essa importação das políticas. 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.
Evidências	 **TESTE OK**

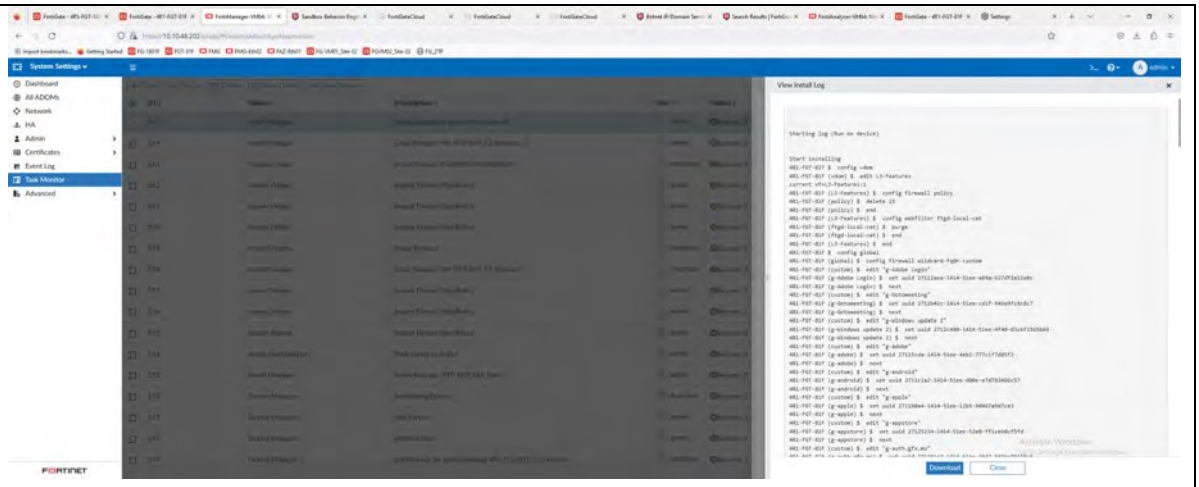

Connectivity
1
Quick Install (Device DB)
Install Wizard
Import Configuration
Re-install Policy
Policy Package Diff
Configuration
Edit
Delete
Grouping
Add VDOM
Run Script
Edit Variable Mapping
Refresh Device
Fabric Topology
Install VM License
Firmware Upgrade
Edit
Delete
Device Name
FortiGate-Cader

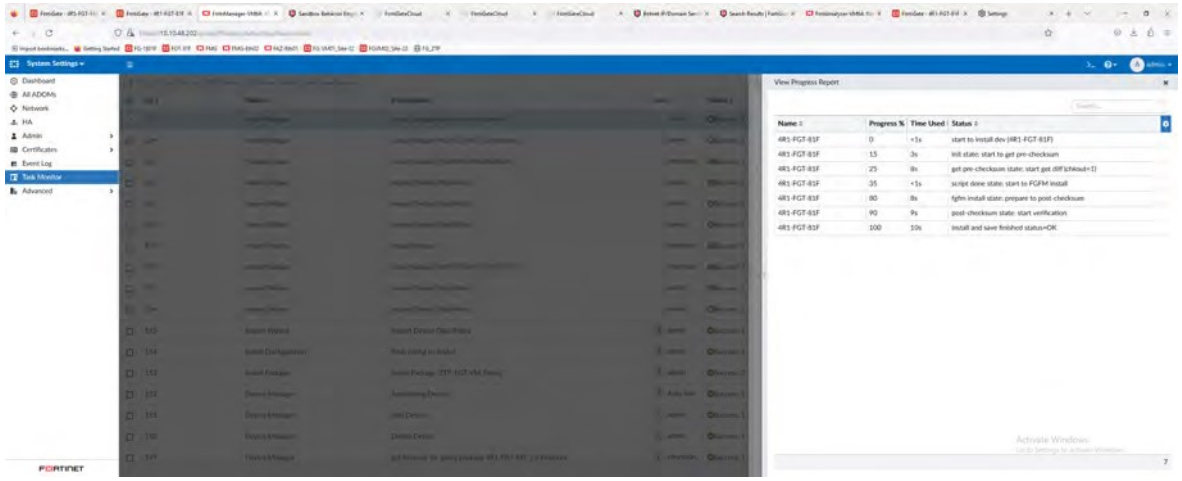

Policy & Objects
Policy Package
Install Wizard
ADOM Revisions
Device Manager
Policy & Objects
AP Manager
VPN Manager
Fabric View
FortiGuard
FortiSwitch Manager
Extender Manager
System Settings



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	 





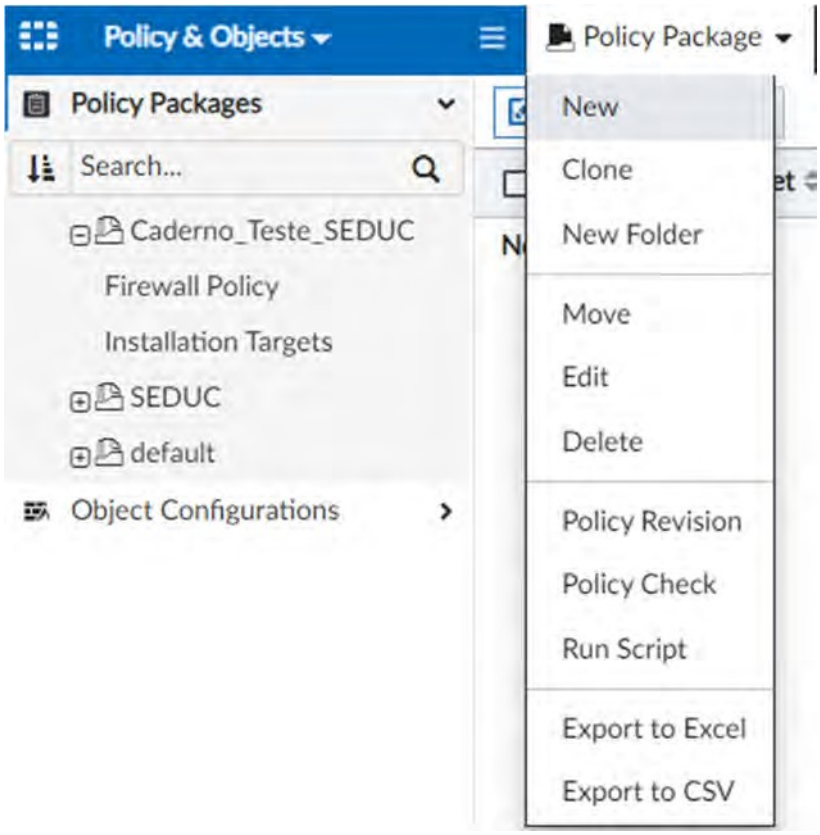
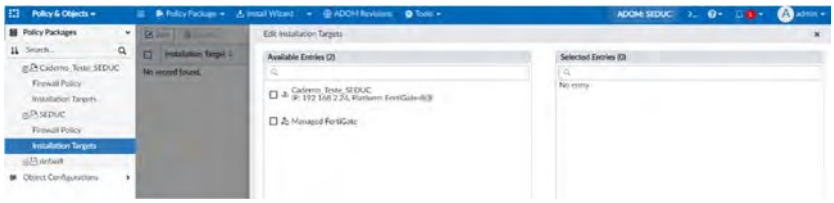
TESTE OK

About policies

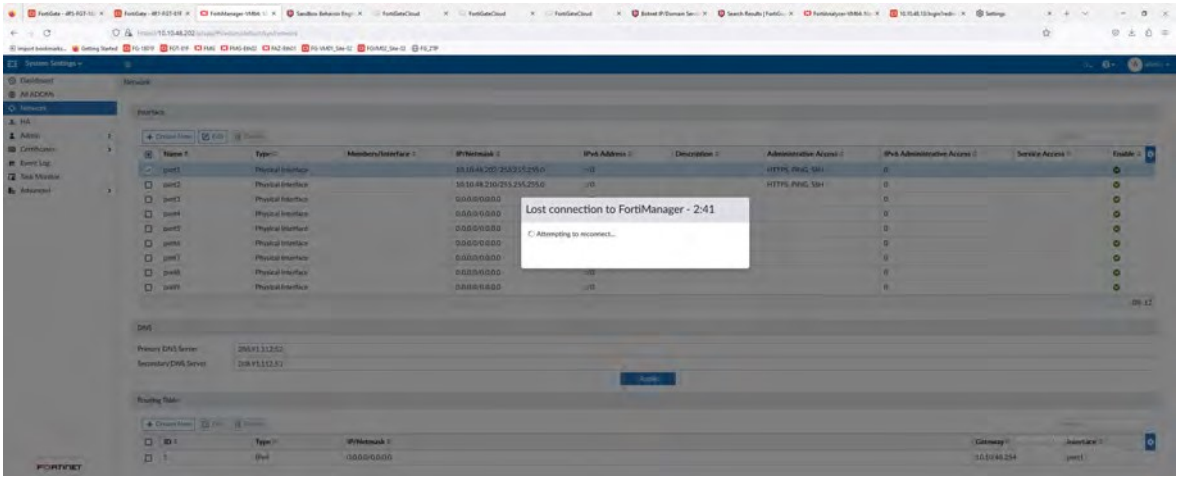
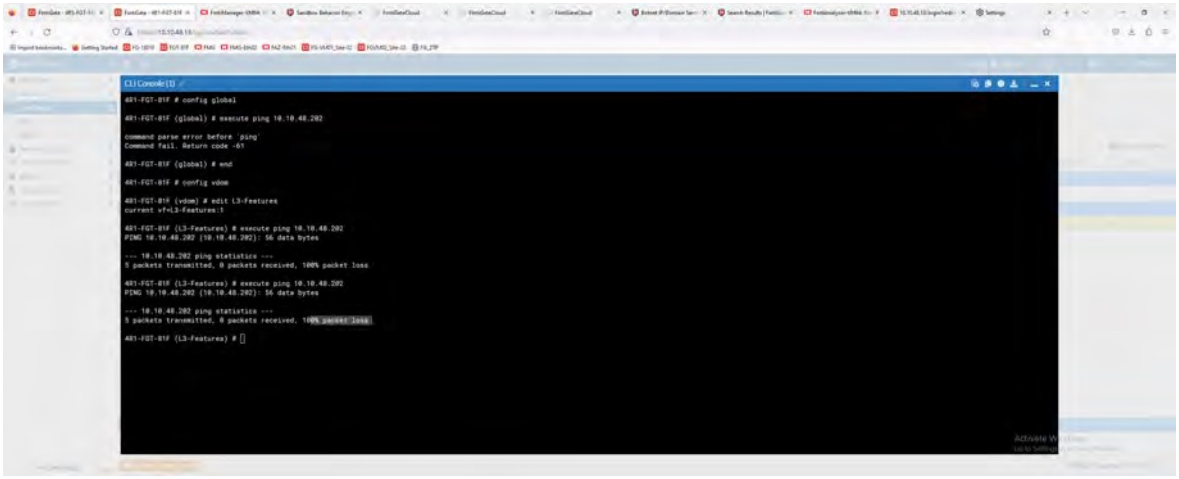
FortiManager provides administrators the ability to customize policies within their organization as they see fit. Typically, administrators may want to customize access and policies based on factors such as geography, specific security requirements, or legal requirements.

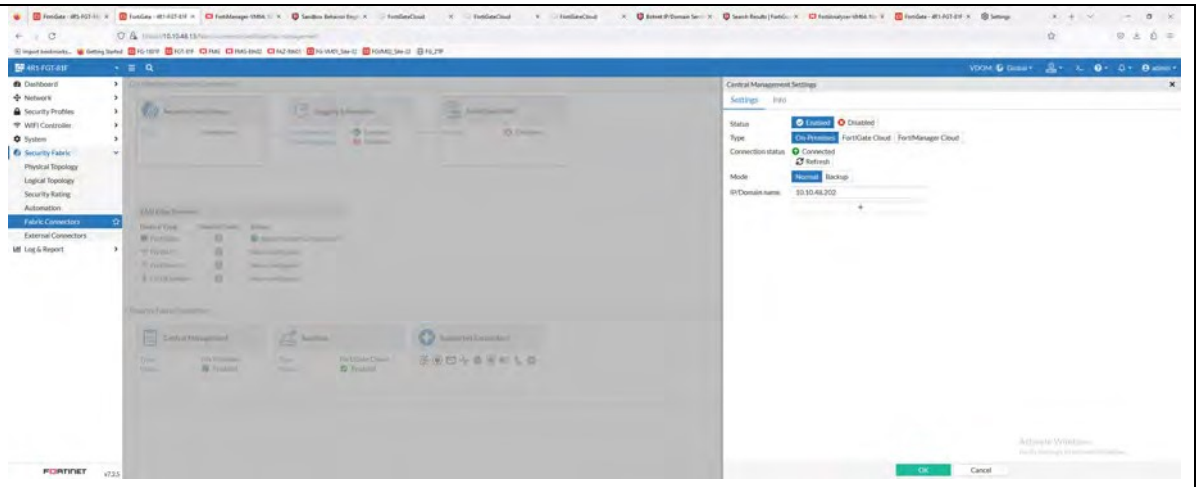
Within a single ADOM, administrators can create multiple policy packages. FortiManager provides you the ability to customize policy packages per device or VDOM within a specific ADOM, or to apply a single policy package for all devices within an ADOM. These policy packages can be targeted at a single device, multiple devices, all devices, a single VDOM, multiple VDOMs, or all devices within a single ADOM. By defining the scope of a policy package, an administrator can modify or edit the policies within that package and keep other policy packages unchanged.

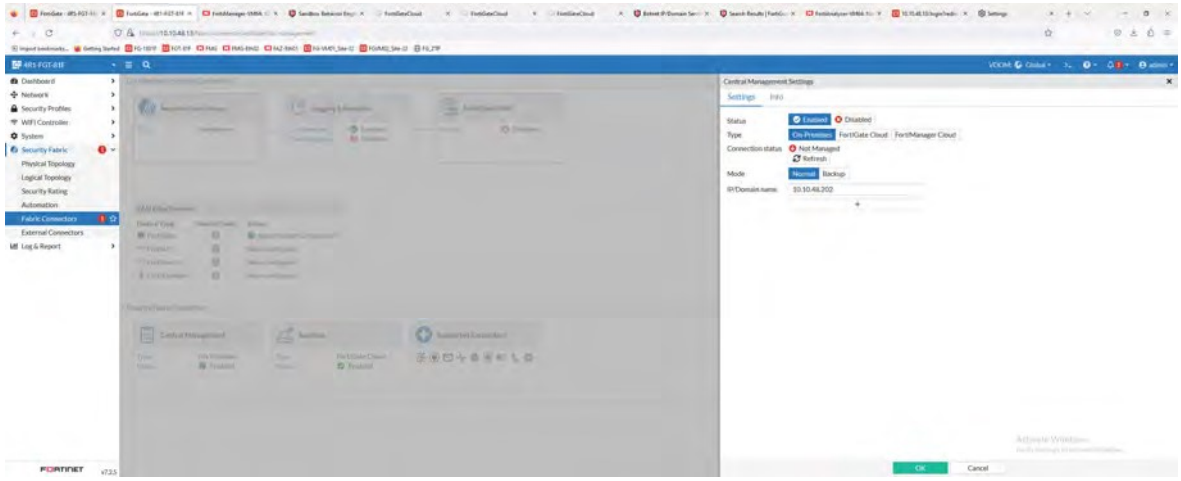
FortiManager can help simplify provisioning of new devices, ADOMs, or VDOMs by allowing you to copy or clone existing policy packages.

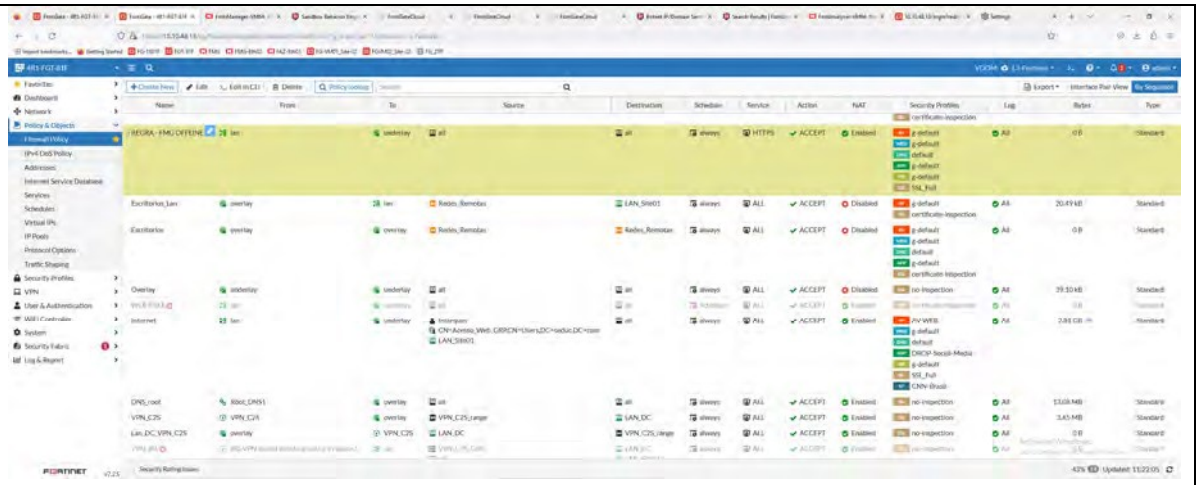
	Na aba de “Policy & Objects “é possível criar um novo pacote de políticas.  Como também, selecionar quais equipamentos receberão esse pacote recém-criado. Para isto, basta acessar a guia “Installation Targets”, em seguida ir em “Edit” e selecionar os equipamentos desejados. 
Comentário	Fonte: FortiManager 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

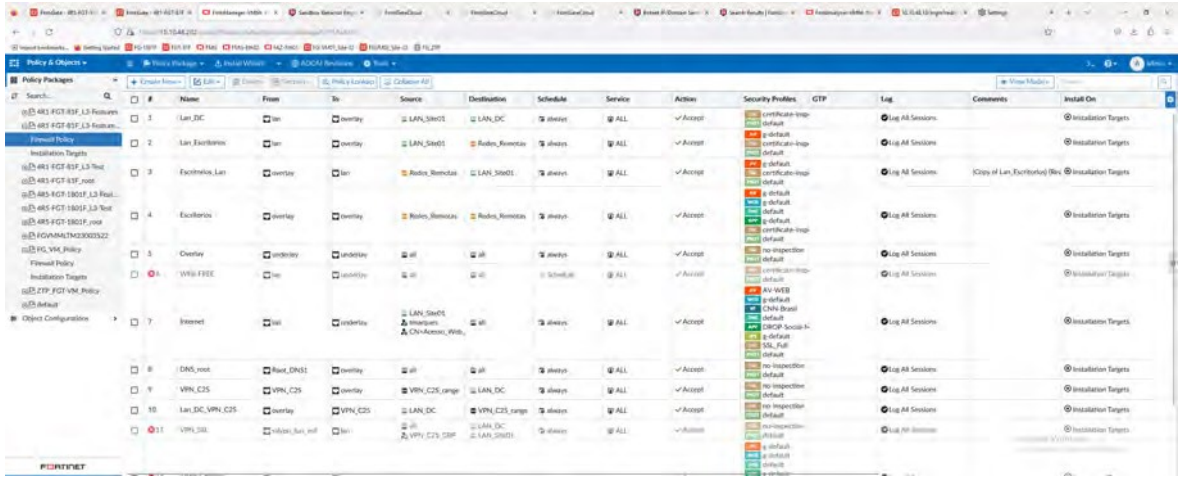
Item de Teste - 5.4.8	Caso a Solução de Gerenciamento Centralizada torne-se indisponível, todos os seus gateways gerenciados devem continuar funcionando normalmente, permitindo a administração, operação e total controle sobre cada gateway enquanto a gerência continuar indisponível;
Objetivo do Teste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

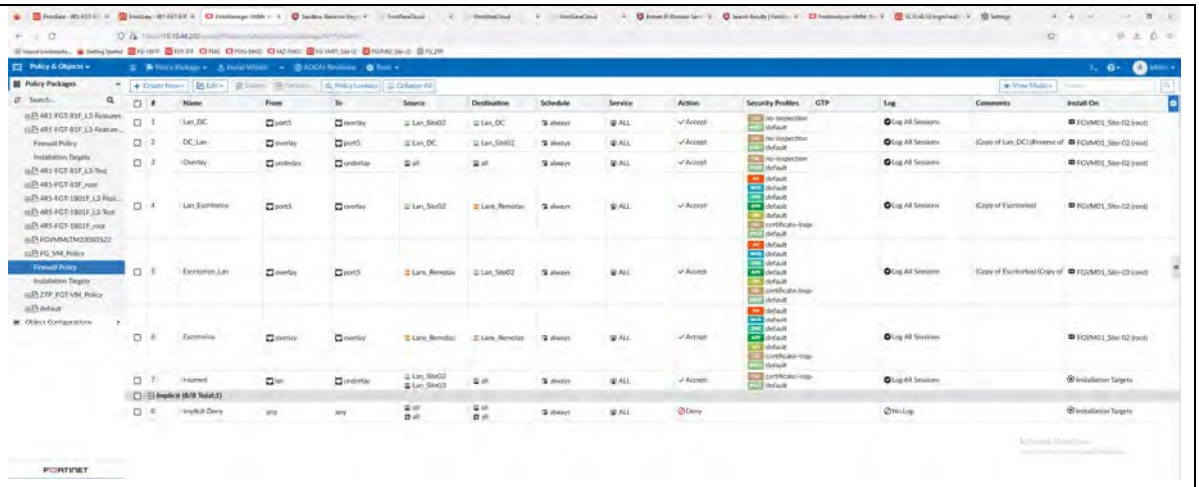
Configuração do Teste	Tornar indisponível a gerência e demonstrar o Firewall
Procedimento do Teste	Tornar indisponível a gerência e demonstrar o Firewall
Evidências	 

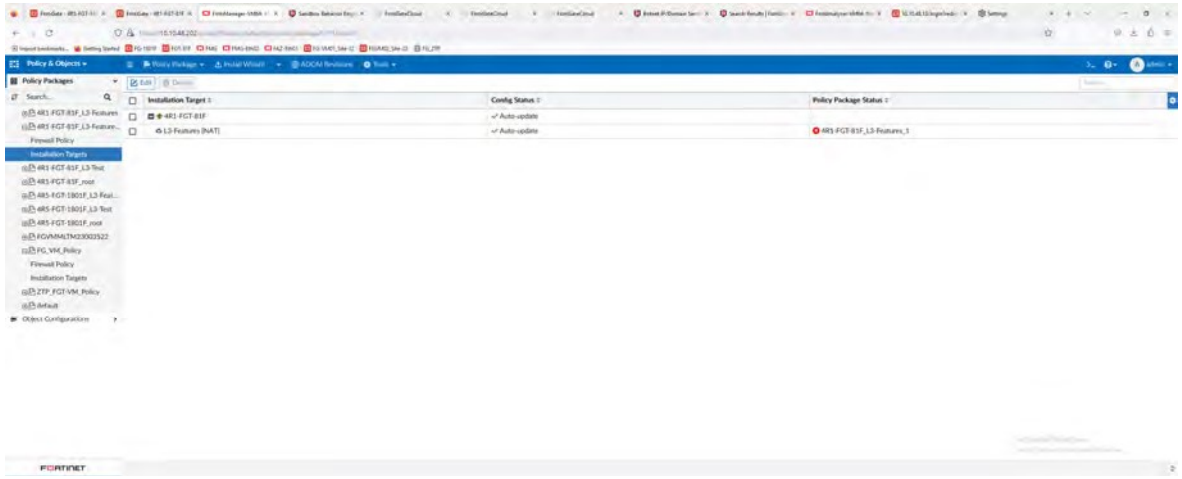


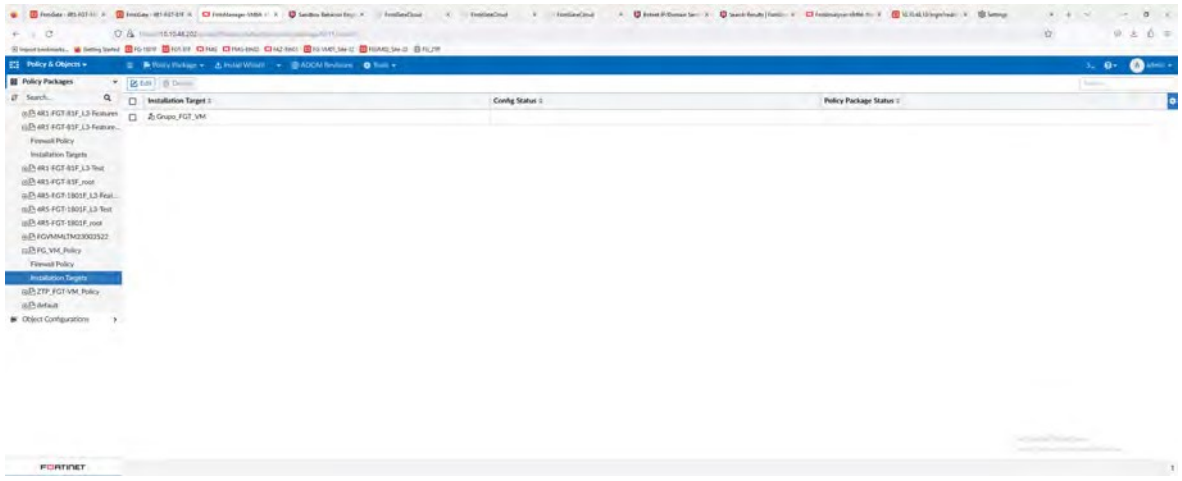


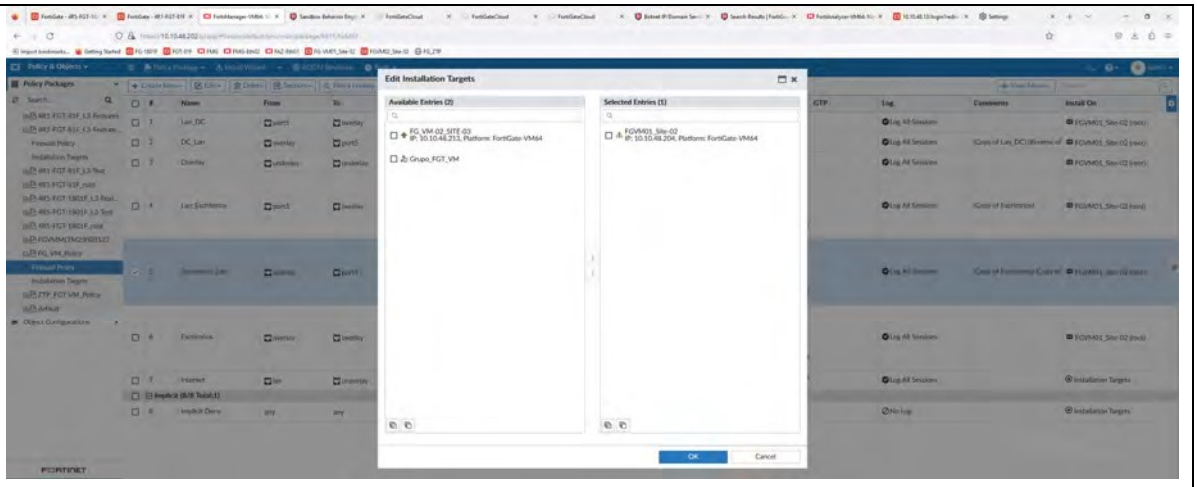
	 **TESTE OK**
Comentário	

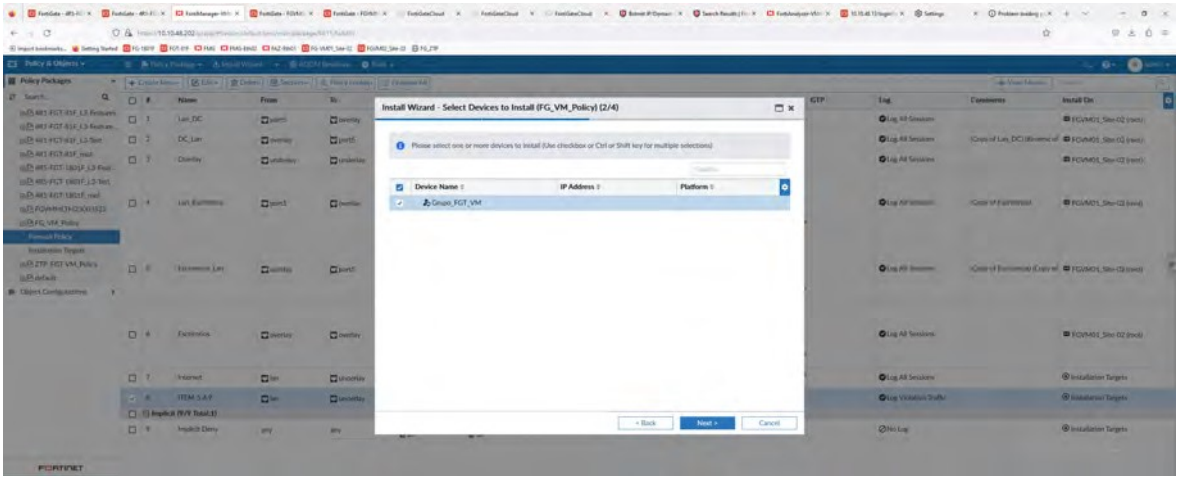
Item de Teste - 5.4.9	A Solução de Gerenciamento Centralizada deve permitir a instalação de políticas individuais (somente para 1 gateway), para um grupo de gateways e para todos os seus gateways gerenciados, não sendo aceito soluções com aplicações de apenas uma das opções;
Objetivo do Teste	Validar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

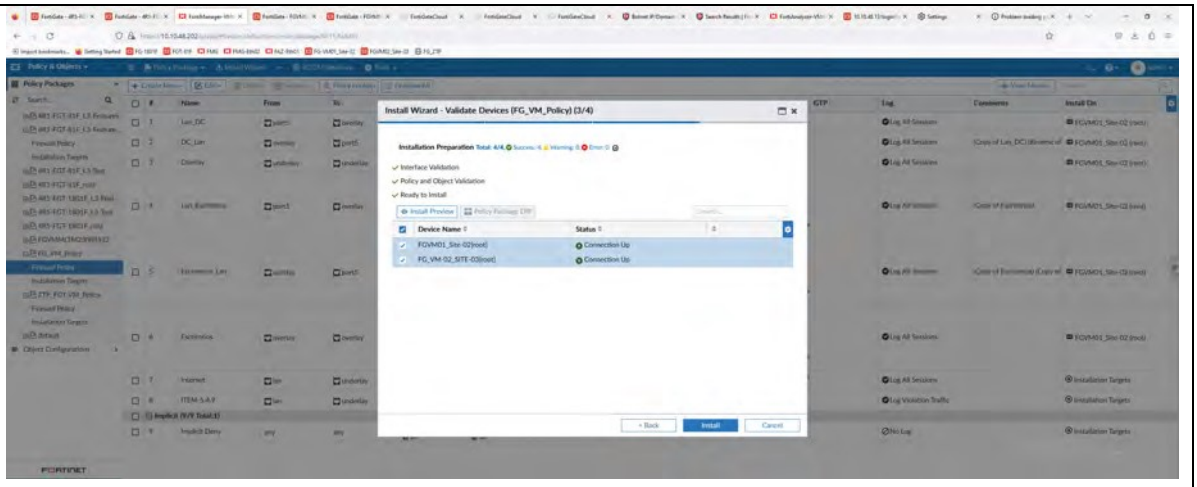


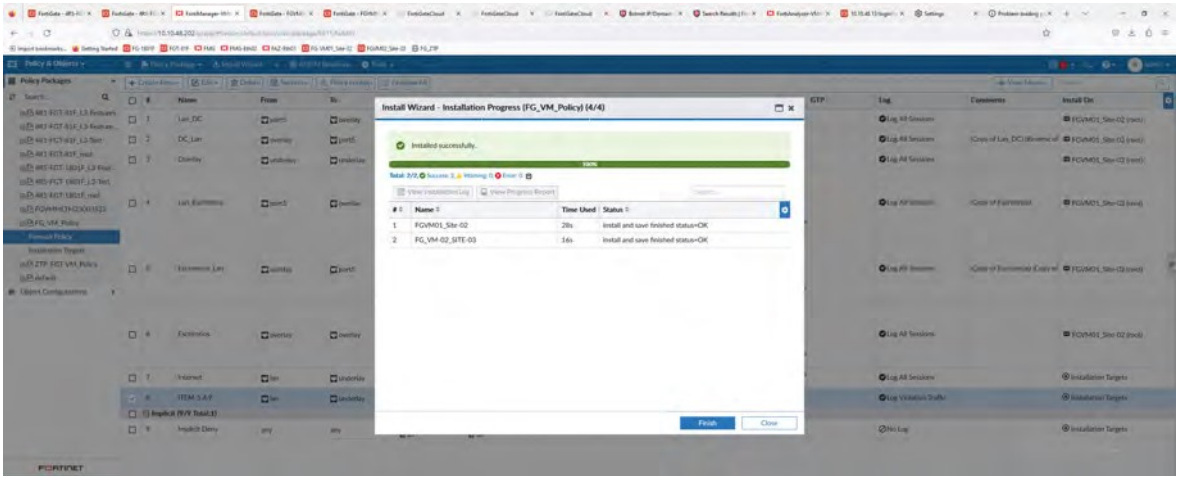





Edit Installation Targets
Available Entries (2)
Selected Entries (1)
OK
Cancel


Install Wizard - Select Devices to Install (FG_VM_Policy) (2/4)
Device Name
IP Address
Platform
Next
Cancel

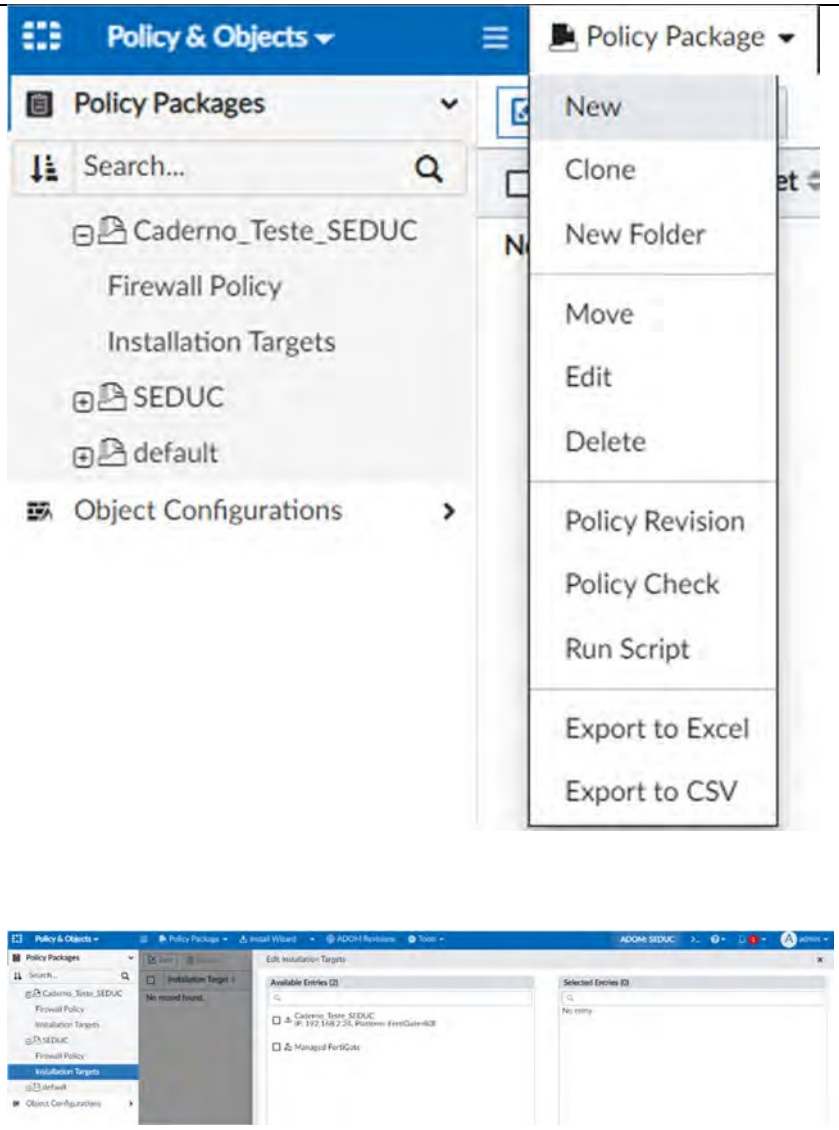




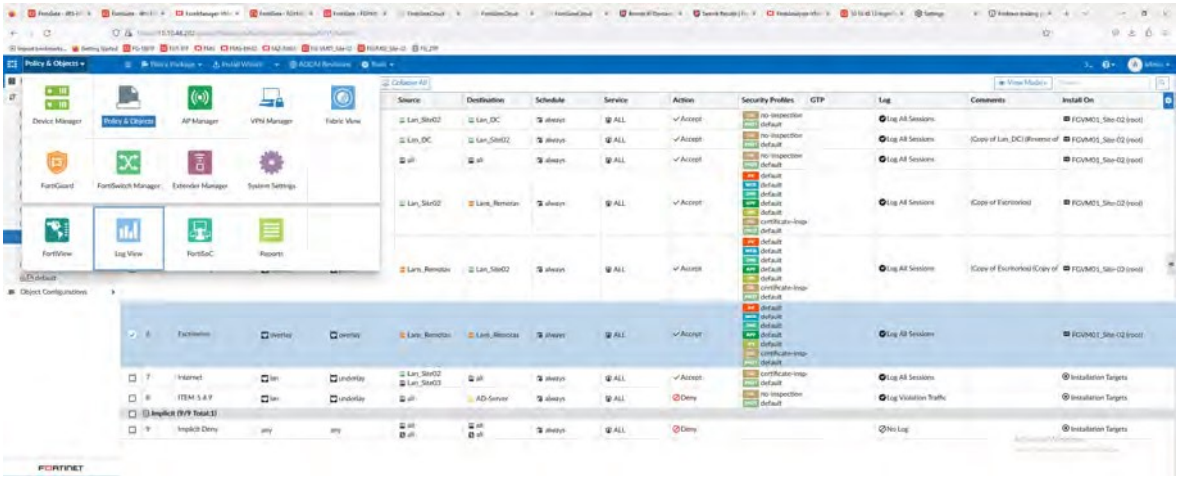
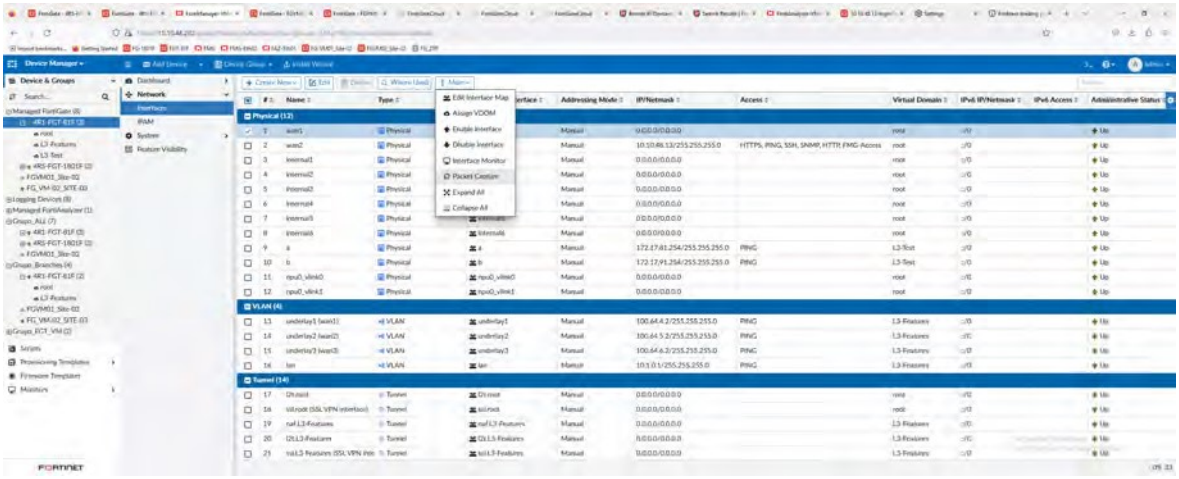
TESTE OK

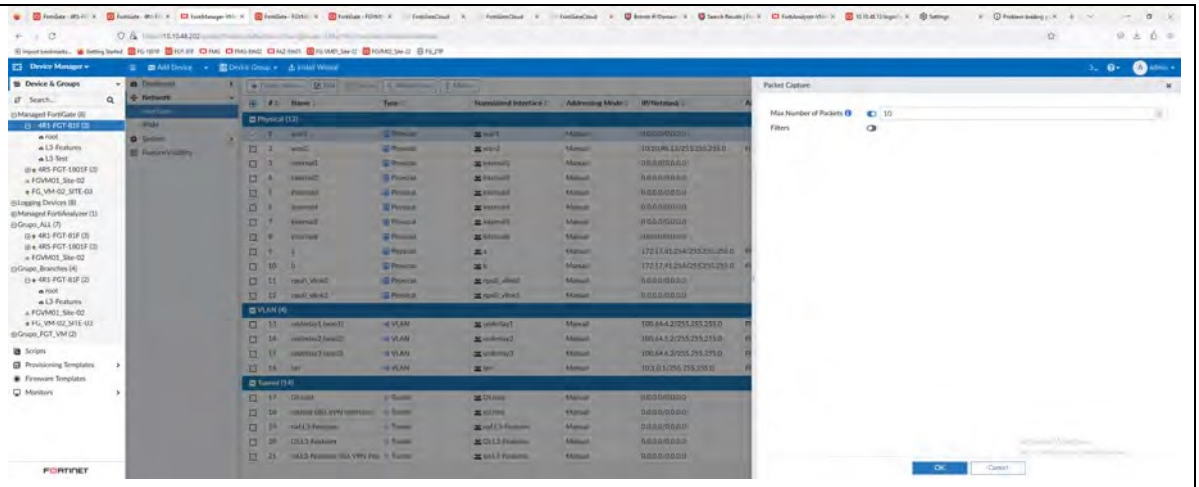
Na aba de “Policy & Objects “é possível criar um novo pacote de políticas.

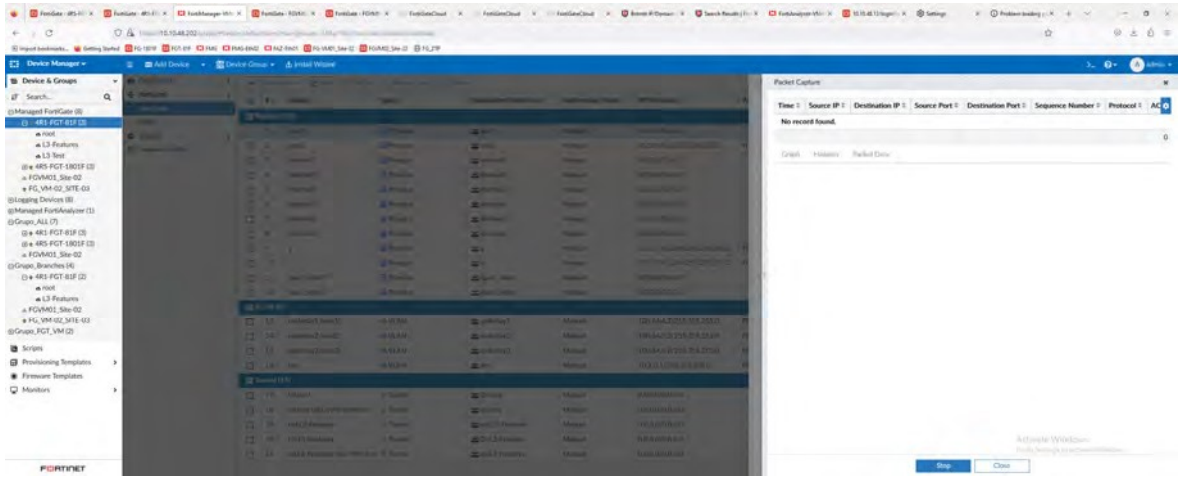
Como também, selecionar quais equipamentos receberão esse pacote recém-criado. Para isto, basta acessar a guia “Installation Targets”, em seguida ir em “Edit” e selecionar os equipamentos desejados.

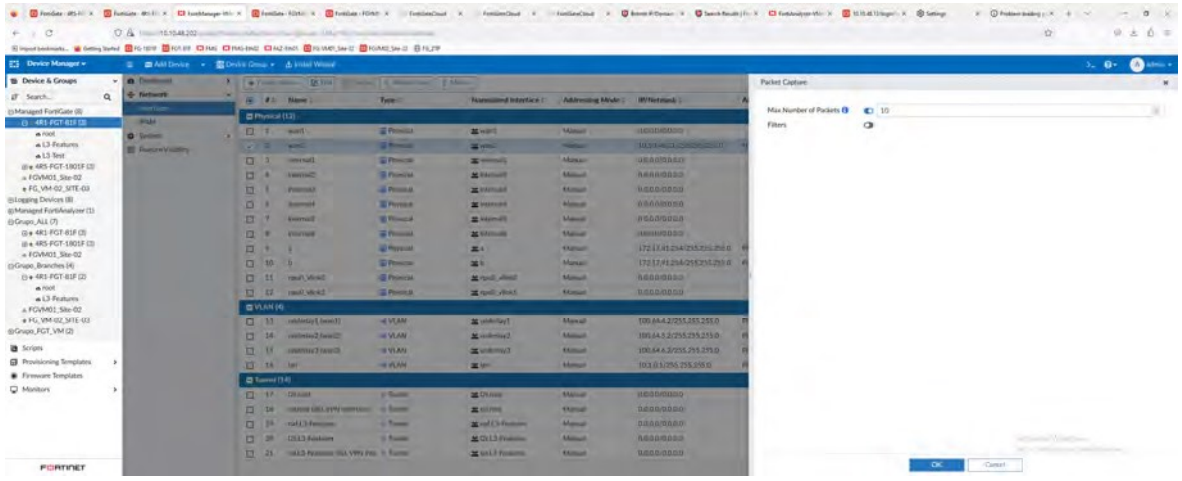
Evidências	
Comentário	Fonte: FortiManager Administration Guide acessado em: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/04f80bb3-e03c-11ec-bb32-fa163e15d75b/FortiManager-7.2.1-Administration_Guide.pdf

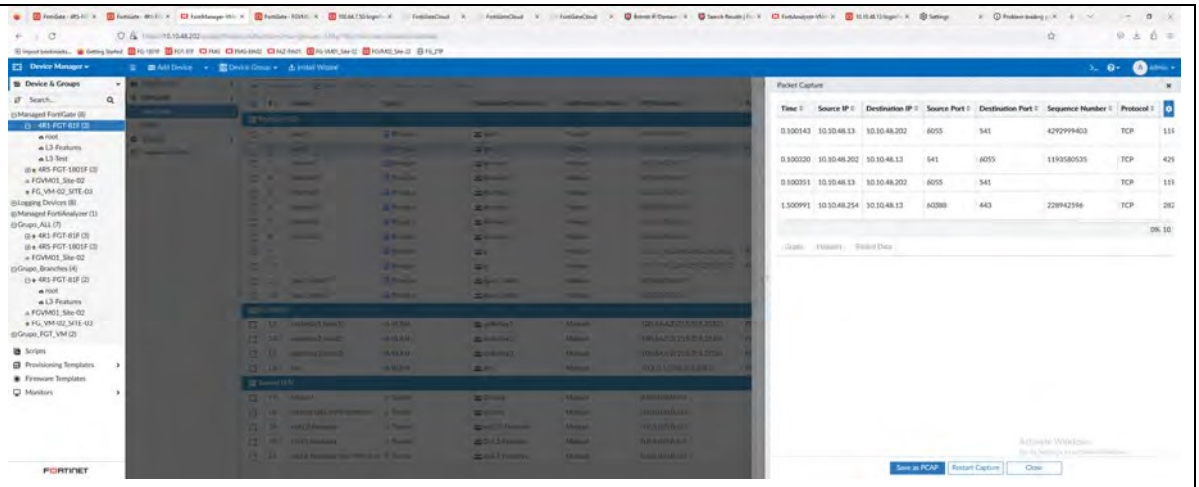
Item de Teste - 5.4.10	Possibilitar a execução das seguintes tarefas: criação e administração de políticas de firewall e controle de aplicação; criação e administração de políticas de IPS, antivírus e anti-spyware; criação e administração de políticas de conteúdo Web e filtro de URL; monitoração de logs; ferramentas de investigação de logs; debugging; troubleshooting; visualização de eventos; dashboards; captura de pacotes;
Objetivo do Teste	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;

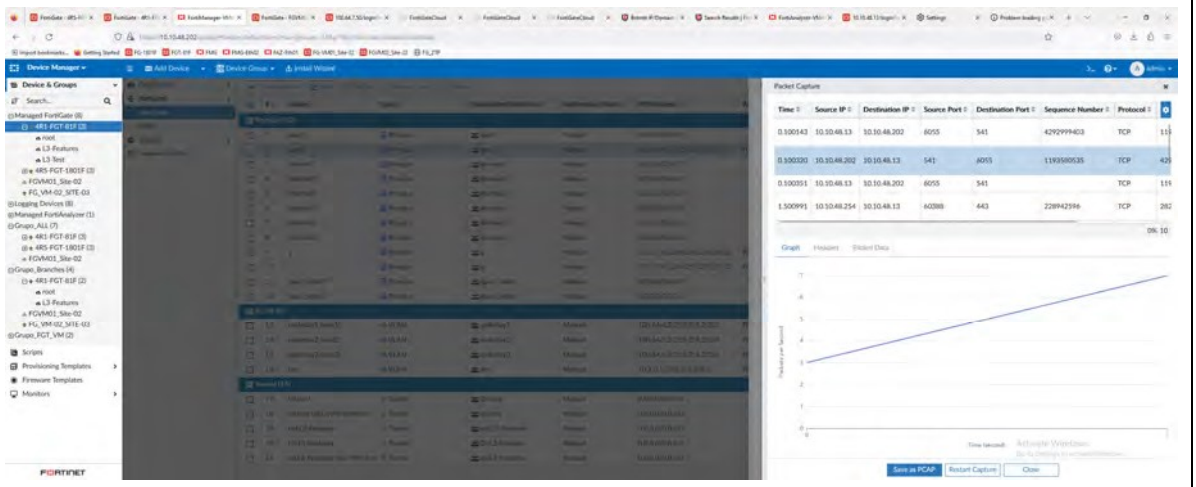
Configuração do Teste	Demonstrar operação do FortiManager
Procedimento do Teste	 

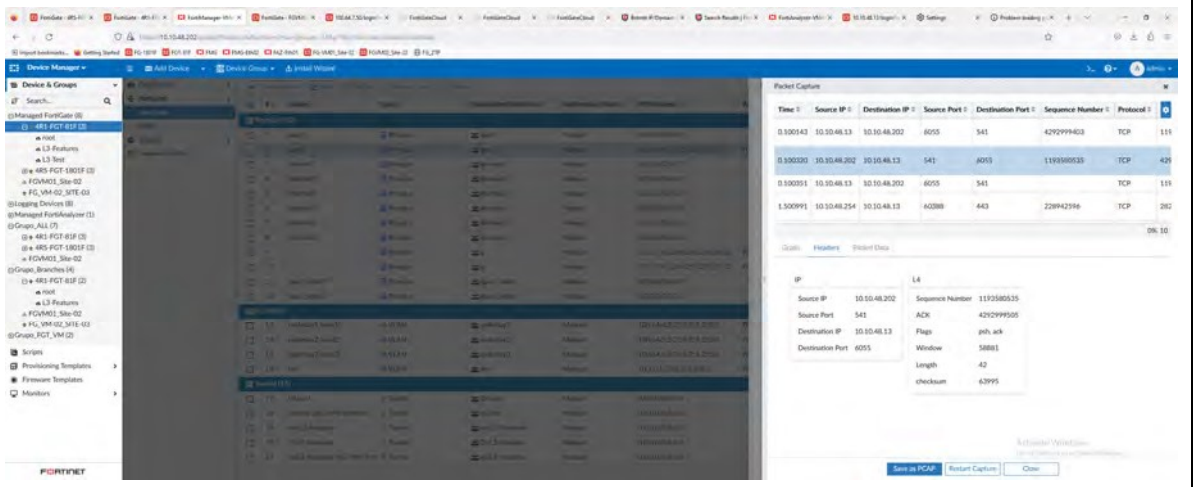


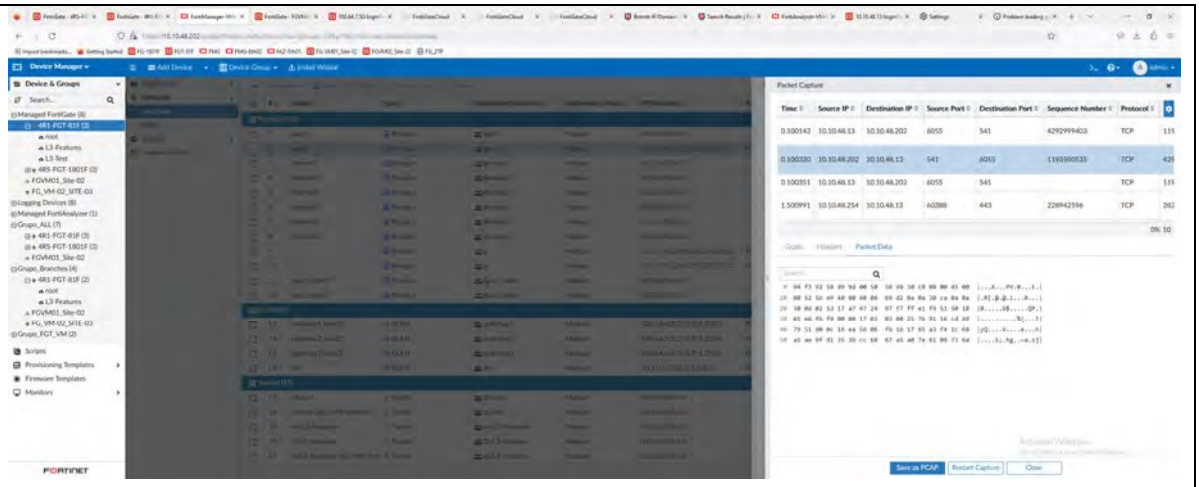












TESTE OK

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

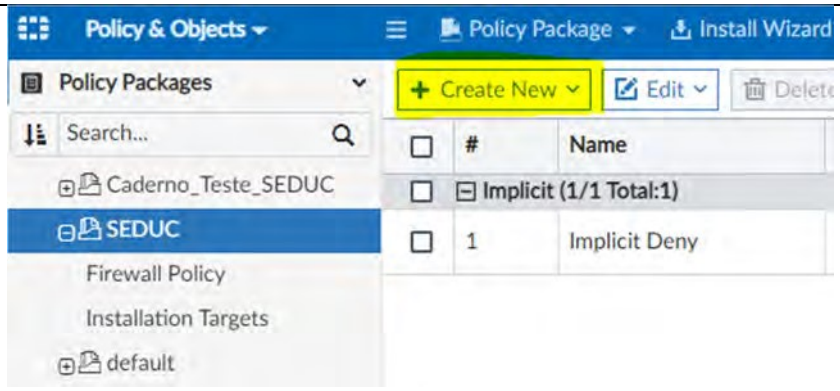
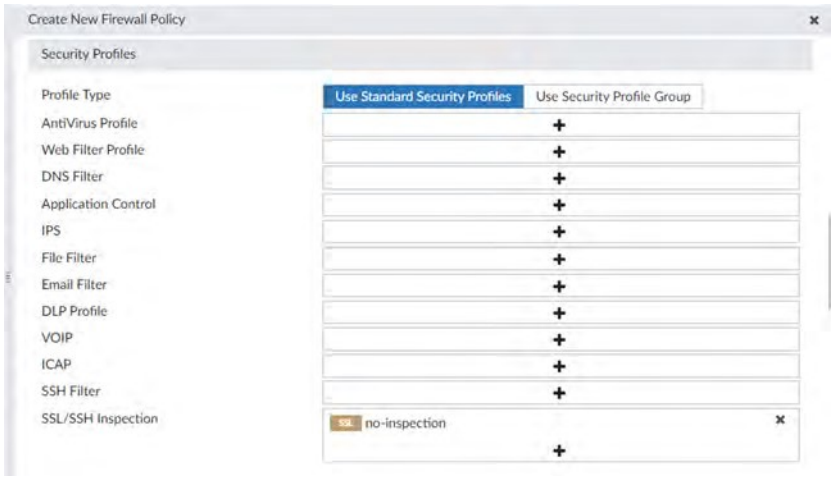
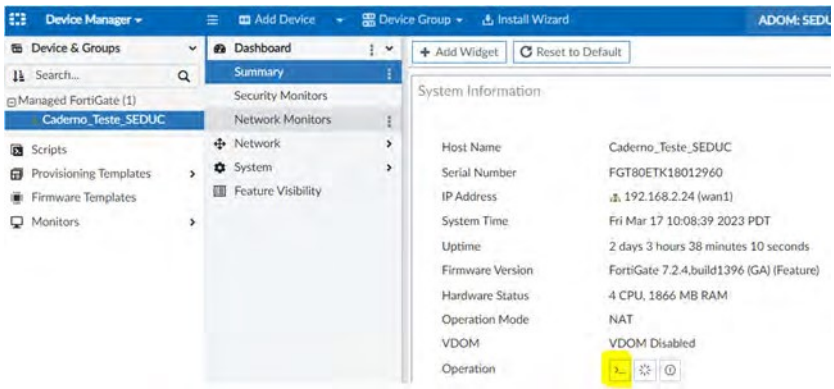
Entre eles, controle de aplicação (Applicatin Control), IPS, antivírus e anti-spyware(Antivírus), conteúdo Web e filtro de URL's(Web Filter Profile).

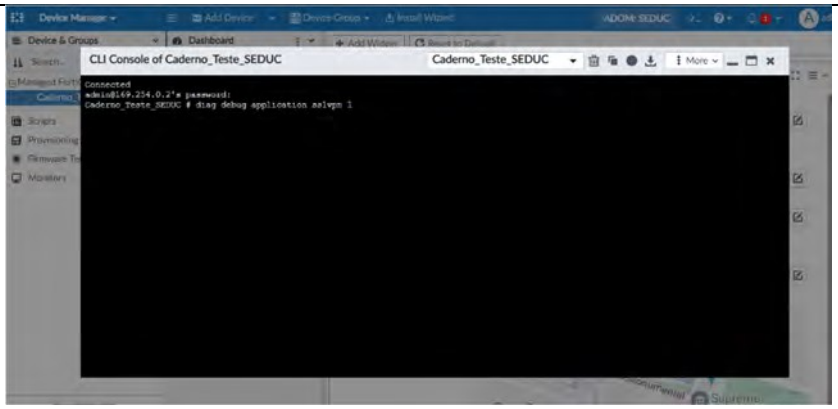
Para realização de debugging e troubleshooting deve se usar do seguinte caminho para se acessar qualquer FortiGate gerenciado pelo FortiManager.

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

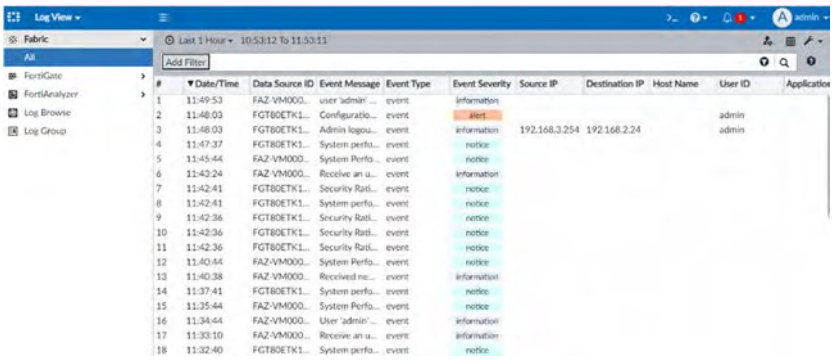
Clicando no ícone indicado, se tem acesso a interface cli daquele equipamento, te dando assim, a possibilidade de debuggar e dar troubleshooting no equipamento com o auxílio deste documento:

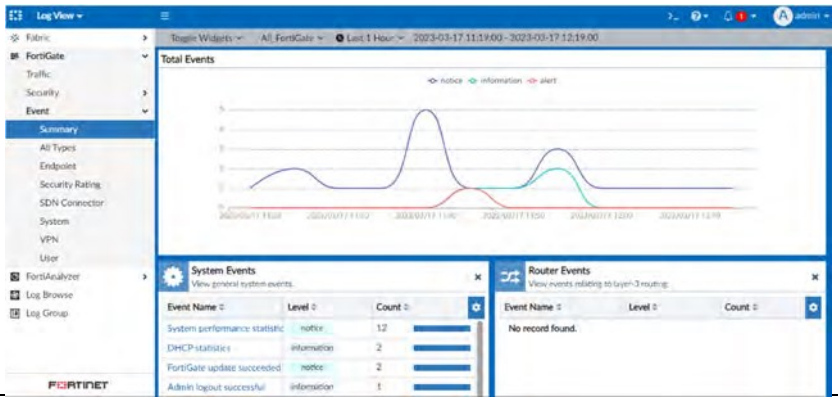
https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/244292/troubleshooting

Evidências	  

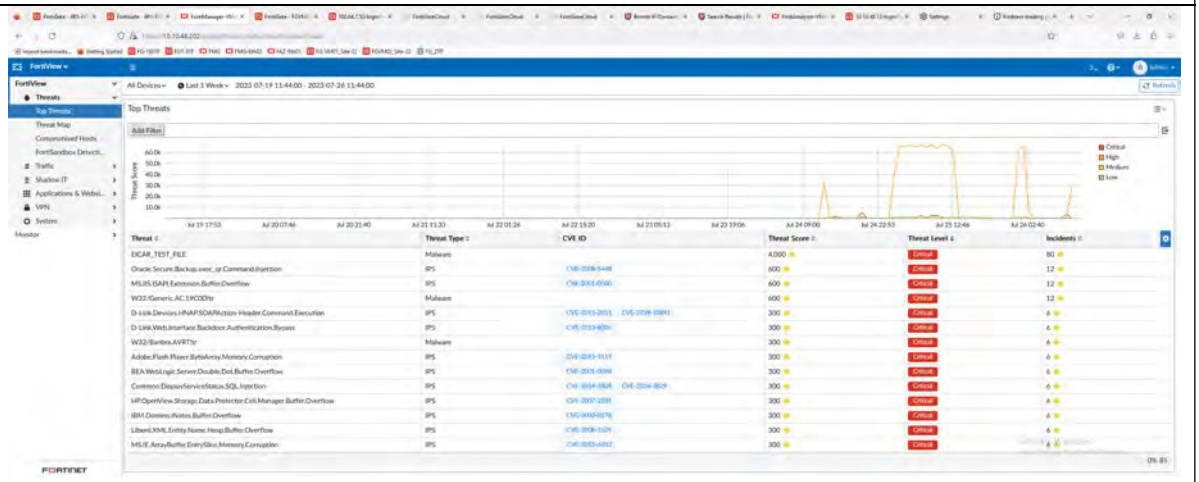
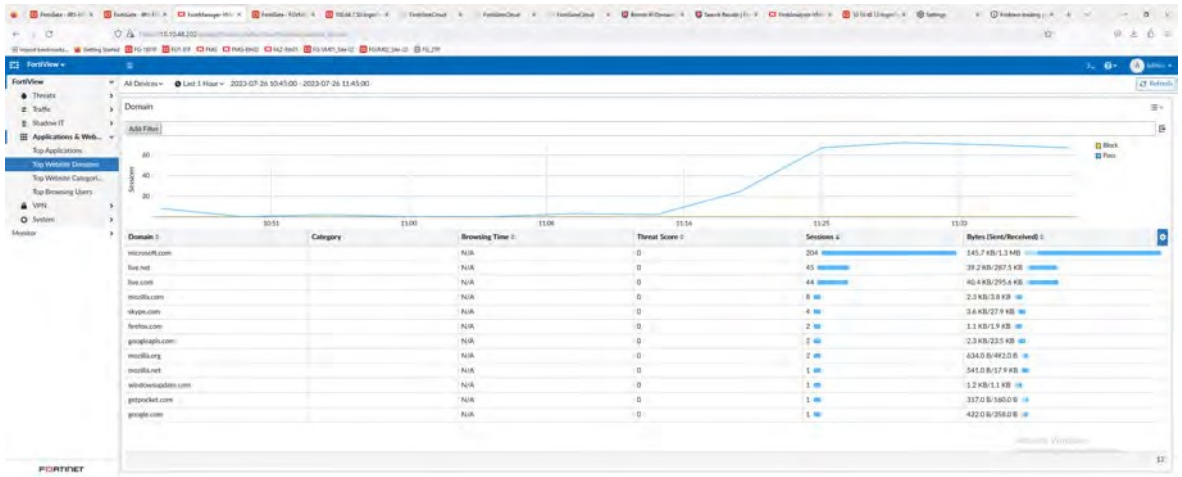


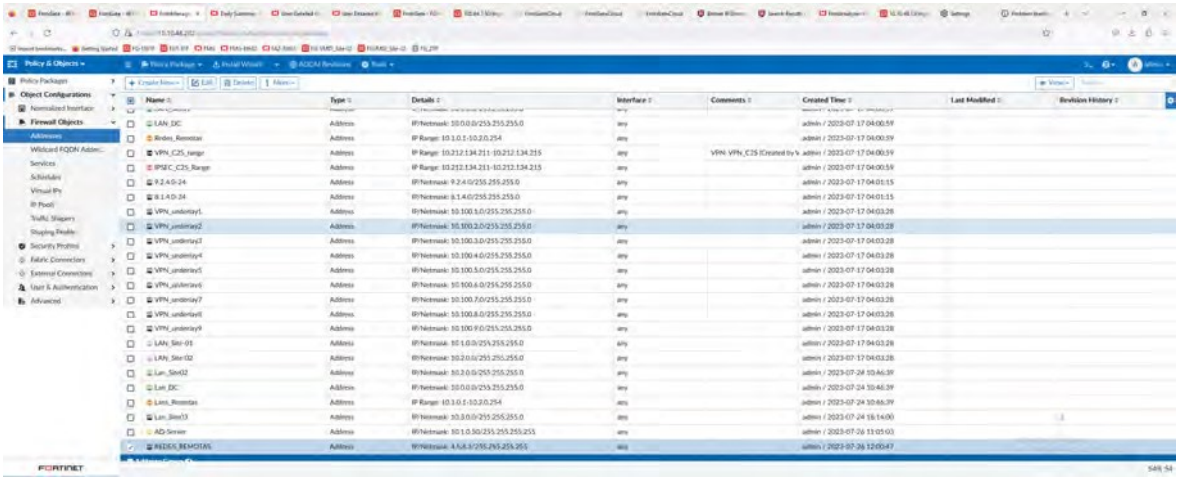
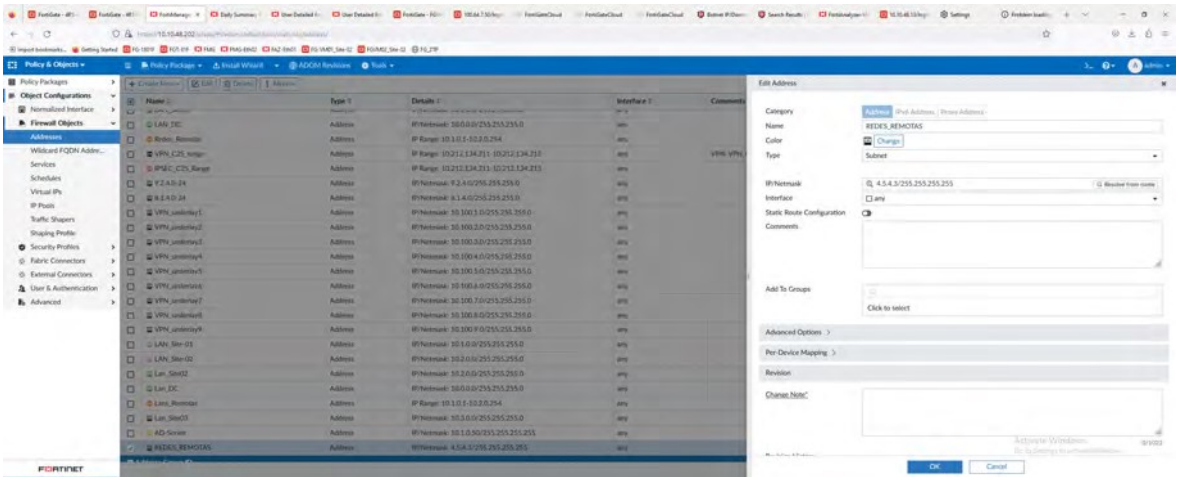
Para monitoração e investigação de logs deve-se utilizar o FortiAnalyzer, que é uma ferramenta própria para análise de logs, investigação de eventos.

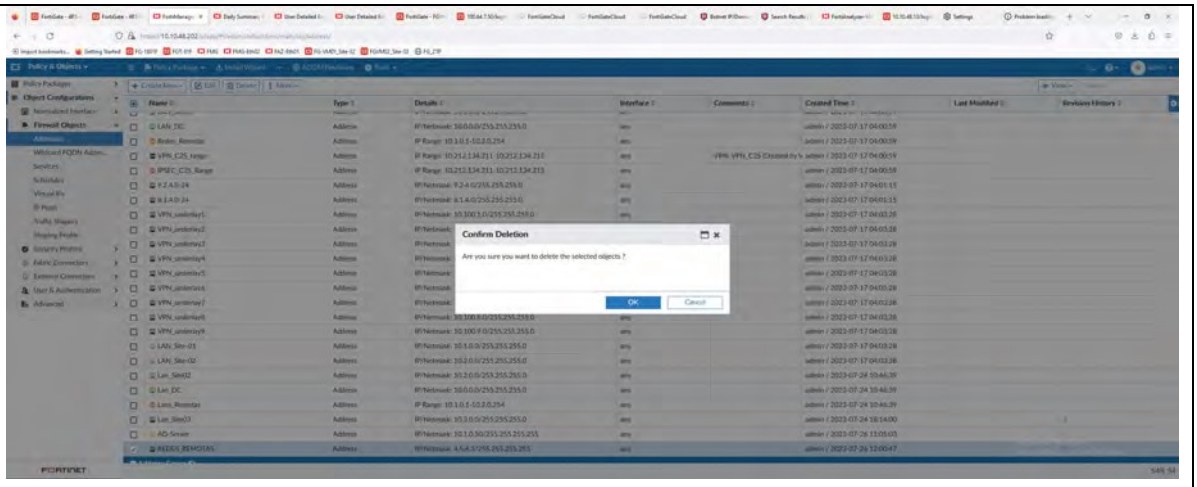


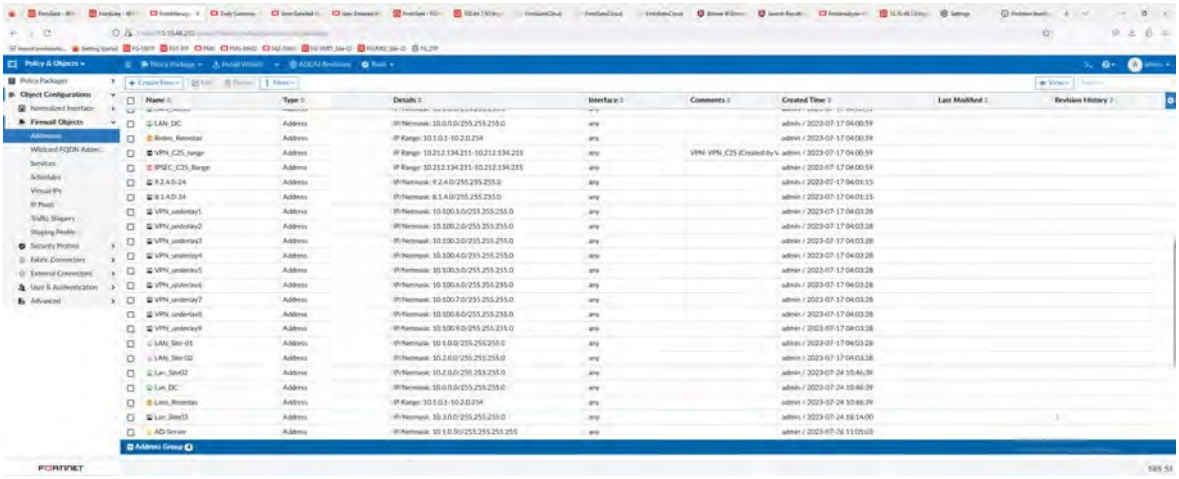


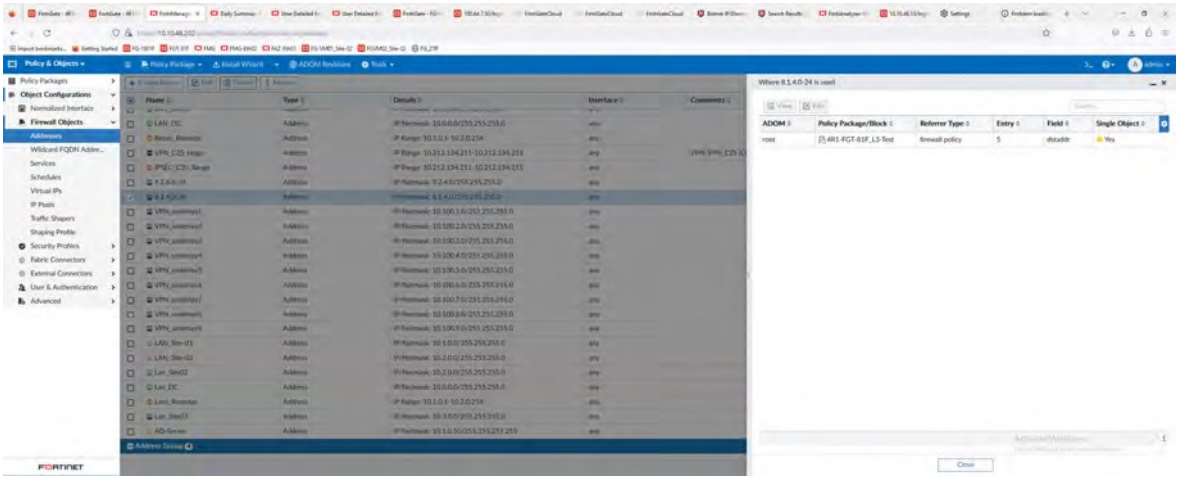
Comentário	

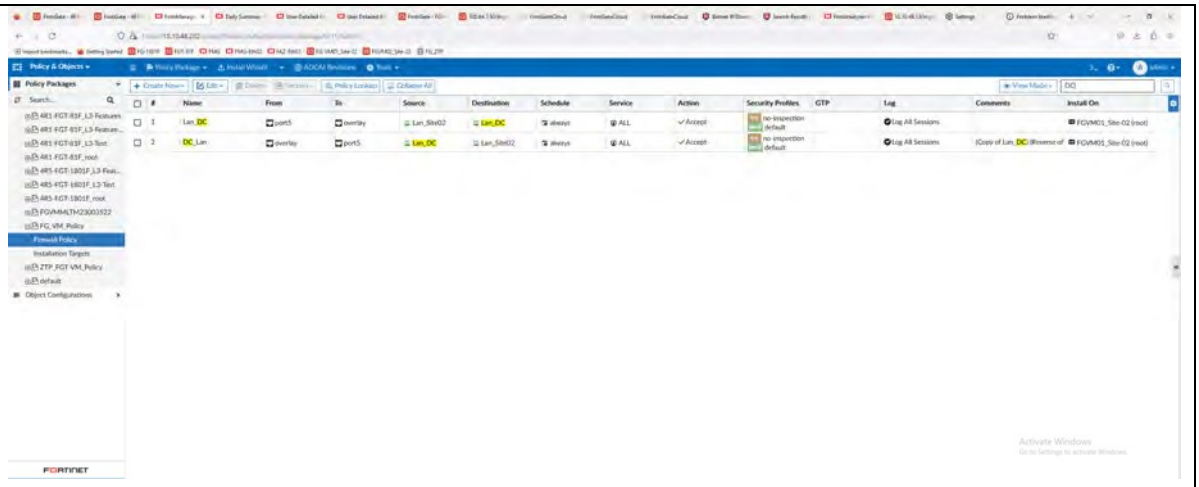
Item de Teste - 5.4.11	Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, antivírus, anti-malware) e URLs analisadas pelo firewall;
Objetivo do Teste	Demonstrar na gerência centralizada os dashboards de eventos.
Configuração do Teste	Demonstrar dashboards do FortiAnalyzer.
Procedimento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

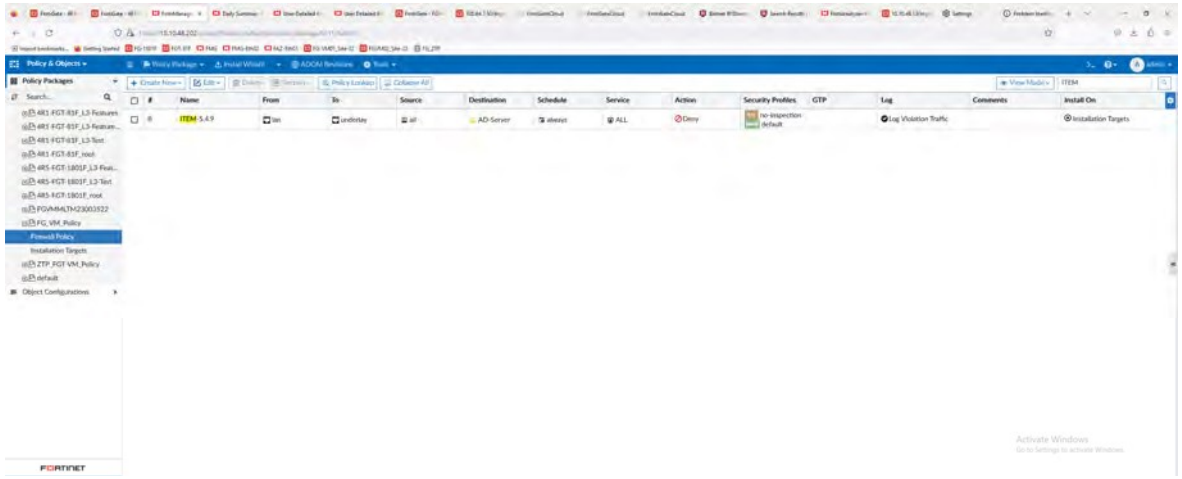
Item de Teste - 5.4.12	Possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deverá ainda permitir detectar onde, na base de regras, está sendo utilizado determinado objeto de rede;
Objetivo do Teste	Verificar se o equipamento de gerência realiza criação, 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	 

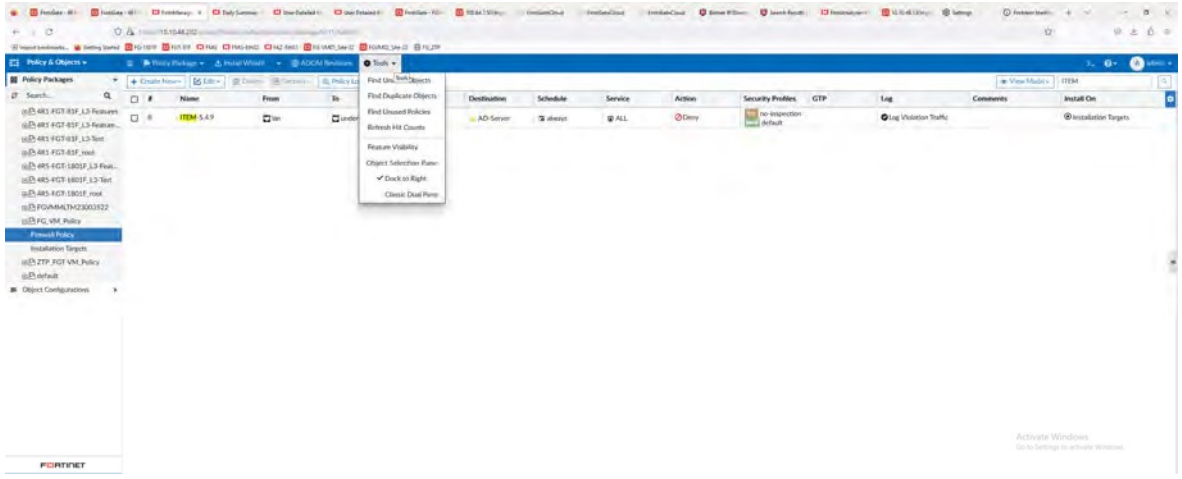

Confirm Deletion
Are you sure you want to delete the selected objects ?
OK
Cancel

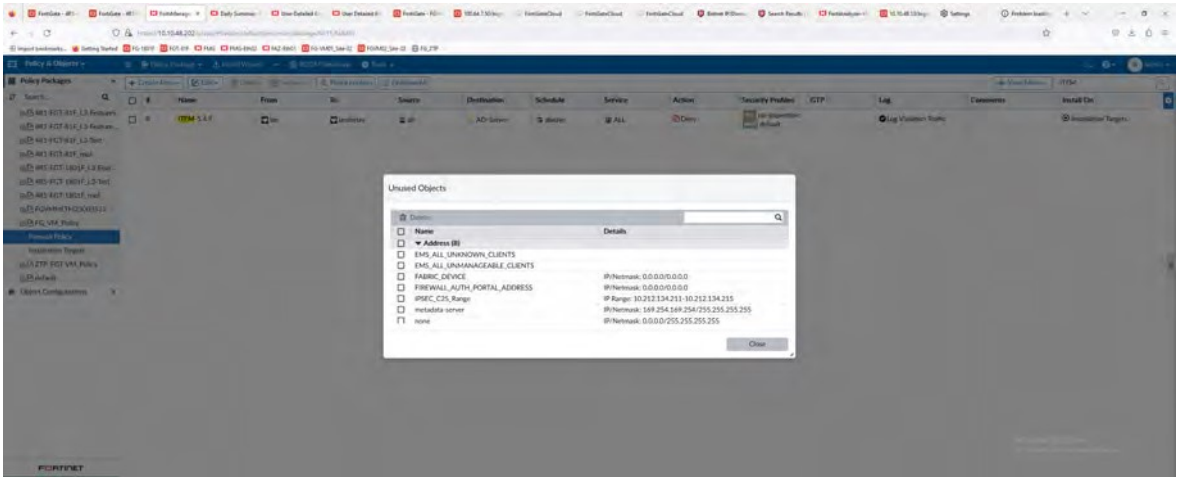




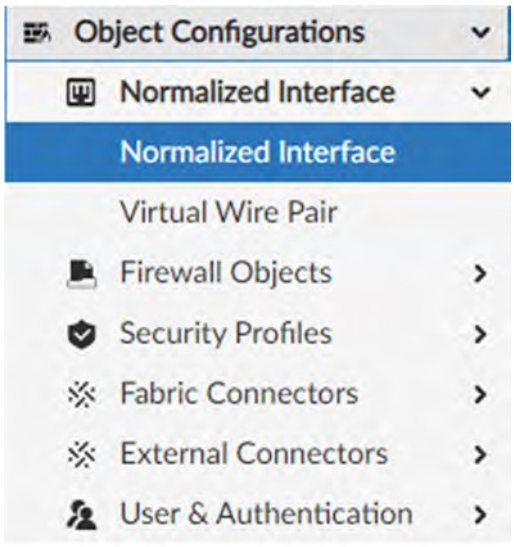


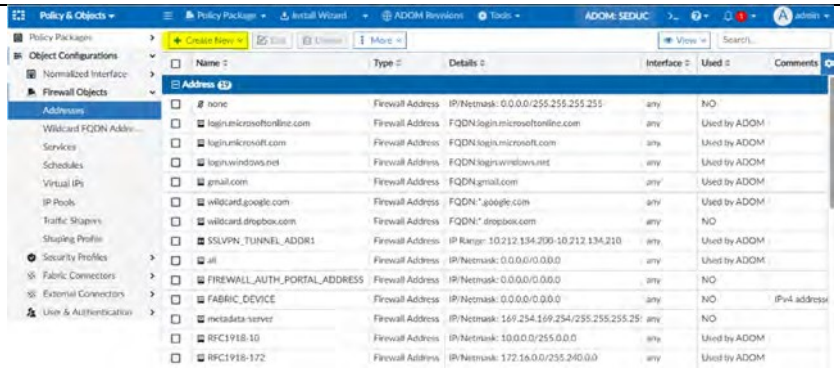




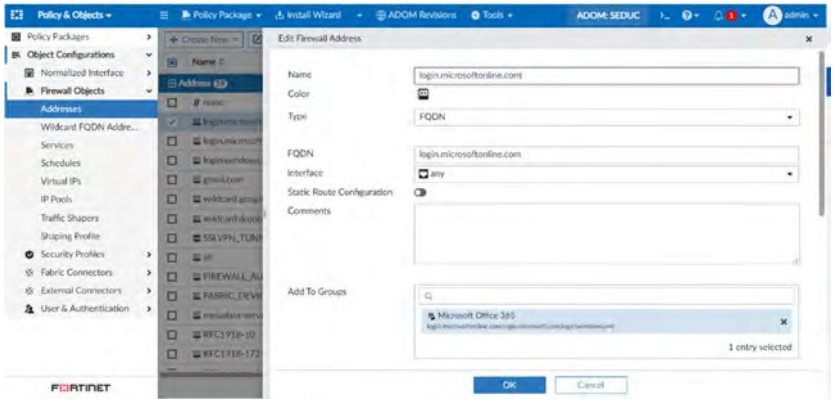

Unused Objects
Name
Details
Address (8)
EMS_ALL_UNKNOWN_CLIENTS
EMS_ALL_UNMANAGEABLE_CLIENTS
FABRIC_DEVICE
FIREWALL_AUTH_PORTAL_ADDRESS
IPSEC_C2S_Range
metadata server
none
Close

TESTE OK

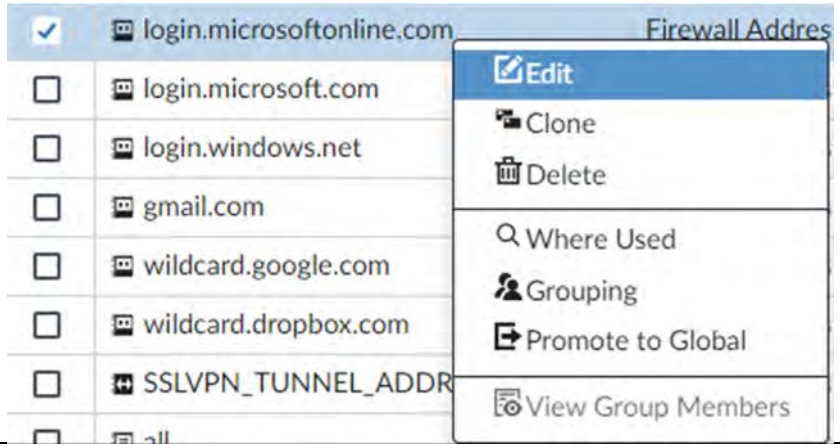

Object Configurations
Normalized Interface
Normalized Interface
Virtual Wire Pair
Firewall Objects
Security Profiles
Fabric Connectors
External Connectors
User & Authentication



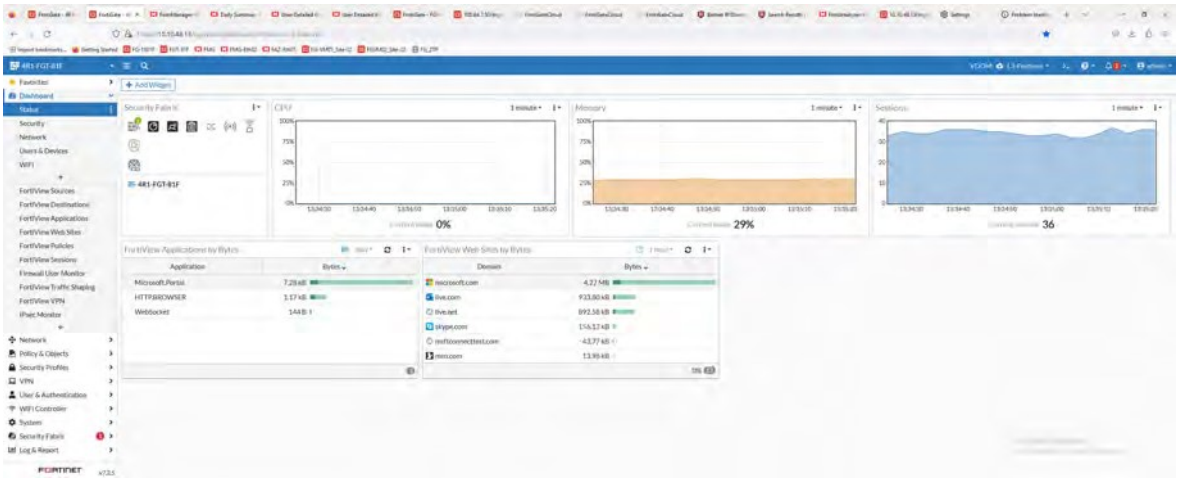
Edição de um já existente



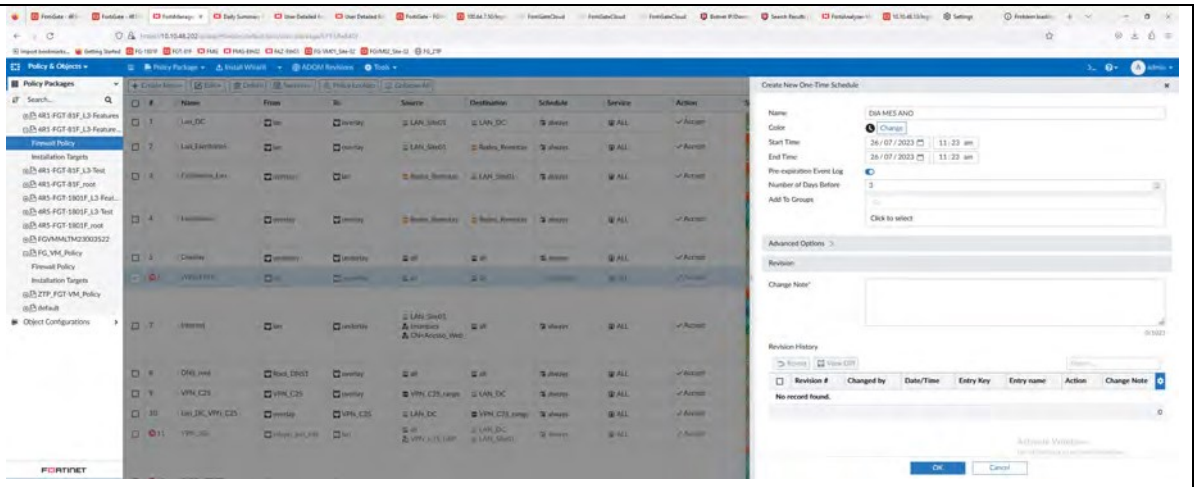
Como também exclusão e visualização de onde está sendo usado.

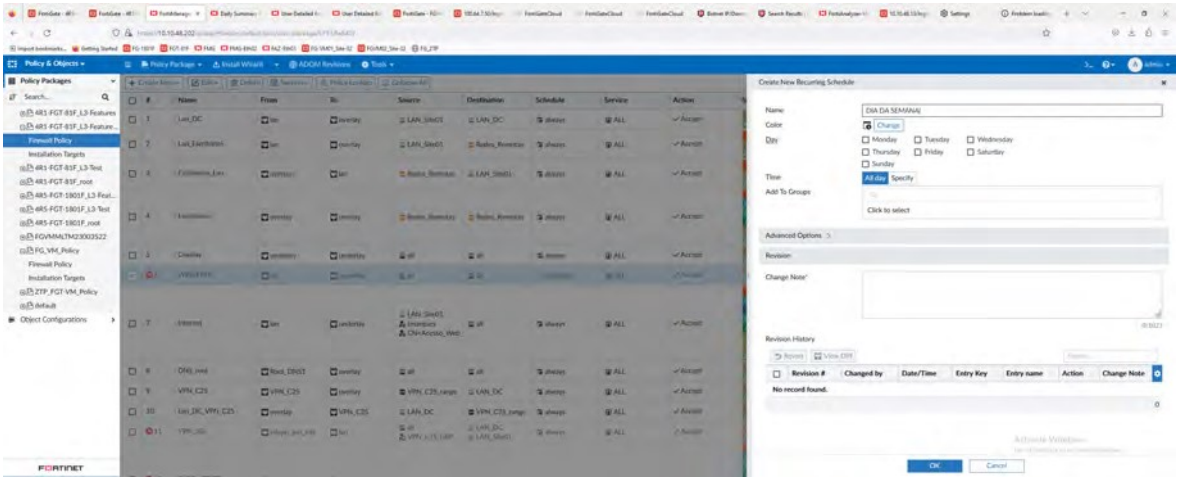


Comentário	

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	 **TESTE OK** Não existe a necessidade de instalar nenhum software para realizar a administração da solução, utilizando qualquer navegador web suportado.
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	

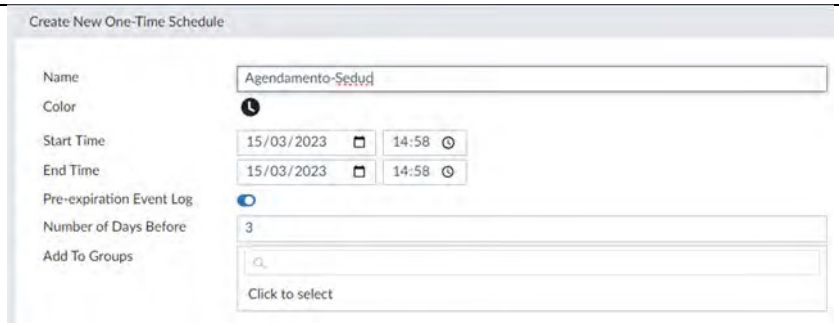
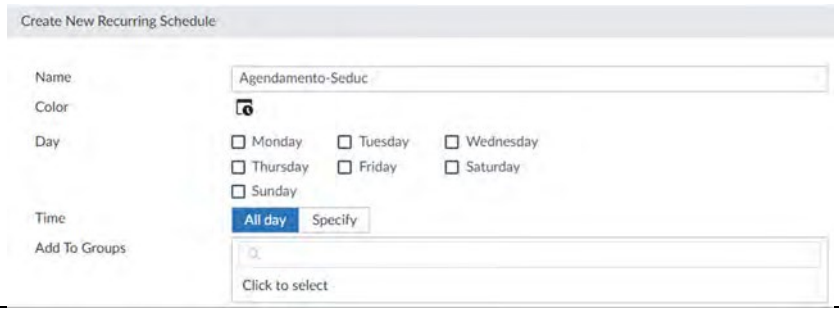




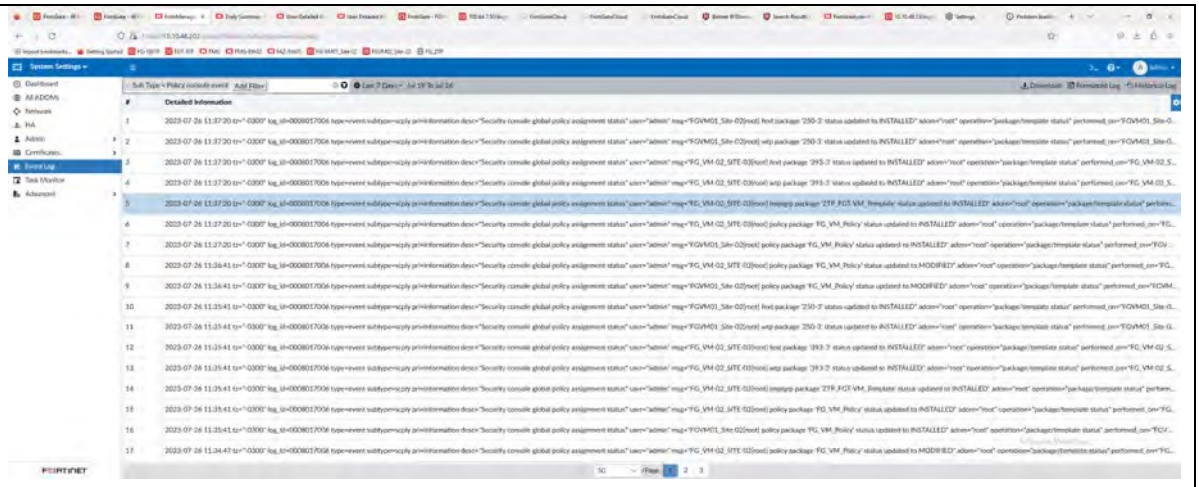
TESTE OK

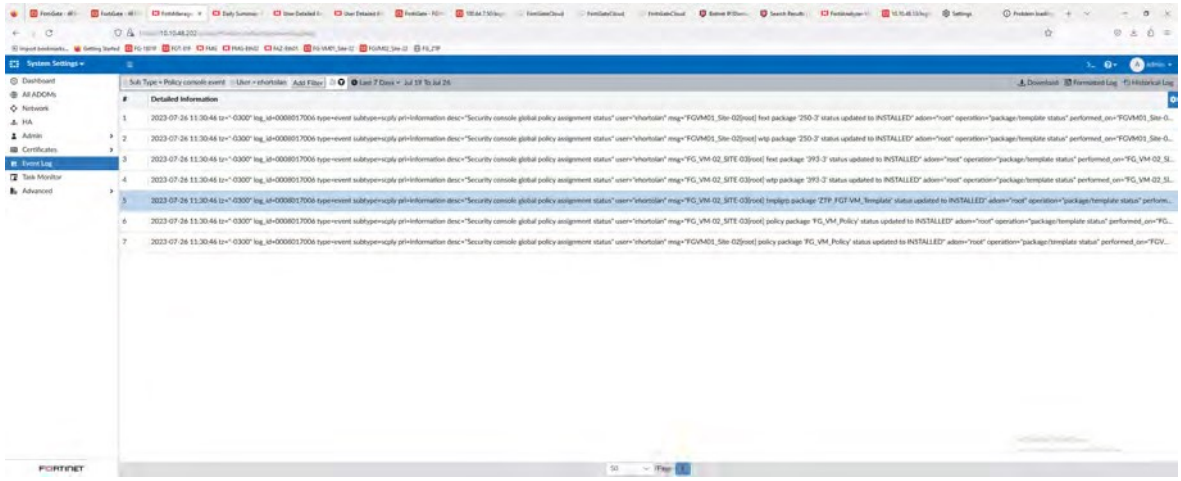
#	Name	From	To	Source	Destination	Schedule	Service	Action
1		lan	wan1	all	all	always	ALL	✓ Accept
2		sslvpn_tun_intf	lan	SSLVPN_TUNNEL rodrigo	gmail.com login.microsoft.com login.microsoftonli login.windows.net	always	ALL	✓ Accept

Para criação de regras para um período de tempo:

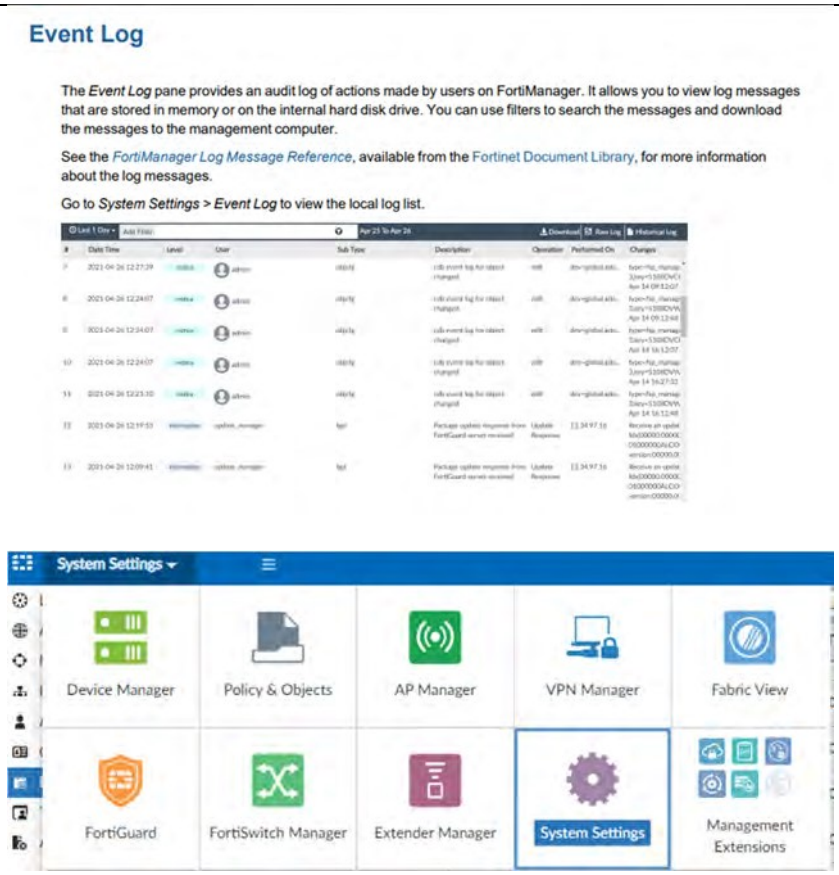
	 Para regras recorrentes: 
Comentário	

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	

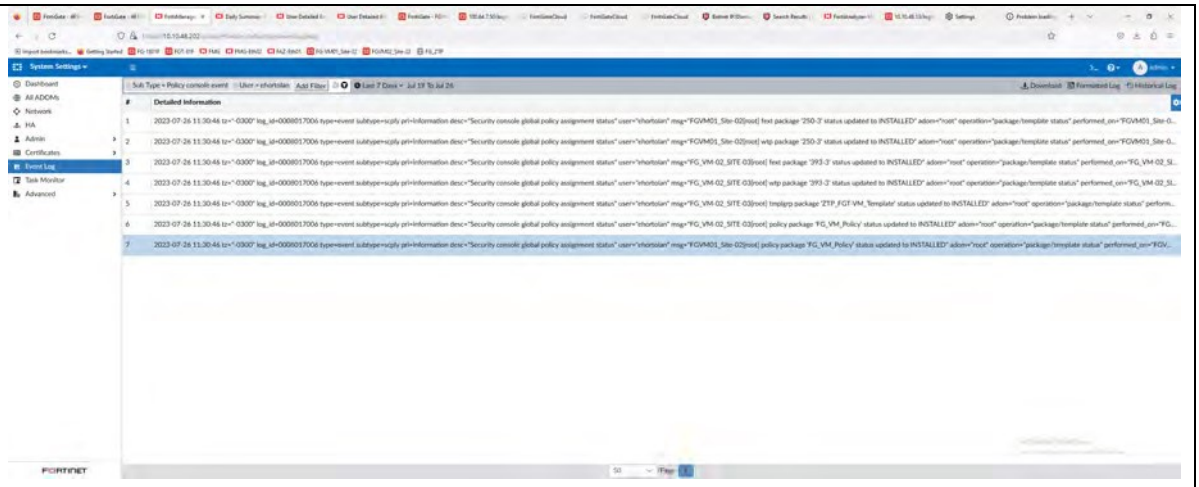


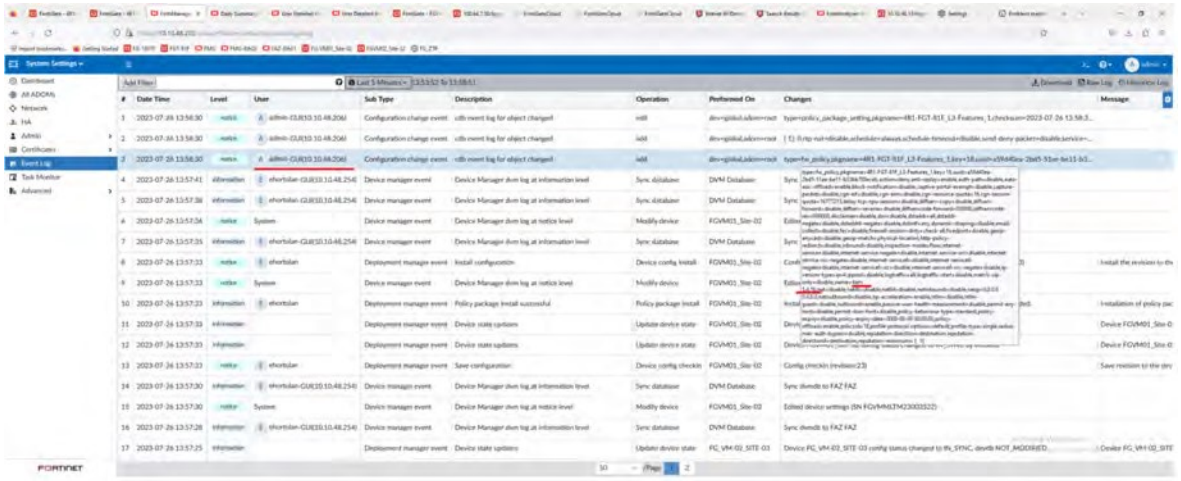


TESTE OK

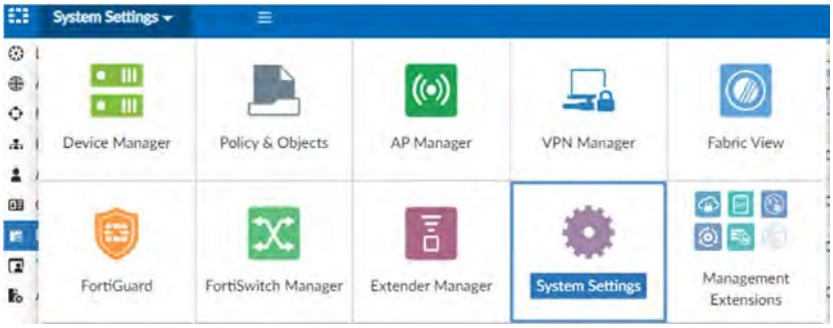
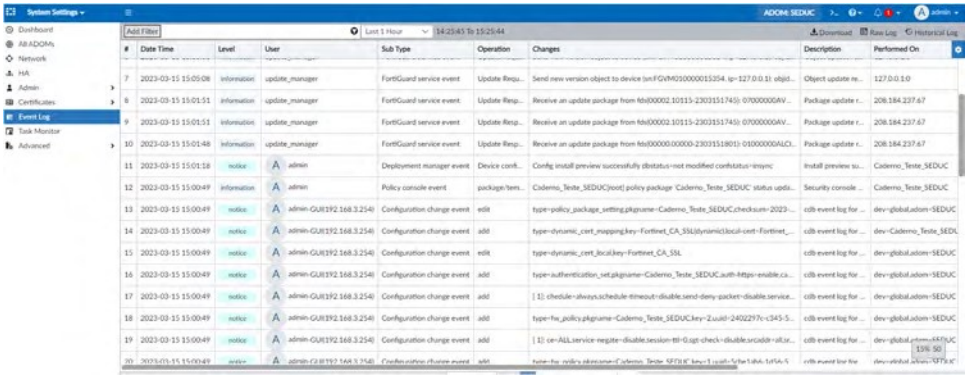
	
Comentário	Fonte: FortiManager Administration Guide acessado em: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/04f80bb3-e03c-11ec-bb32-fa163e15d75b/FortiManager-7.2.1-Administration_Guide.pdf

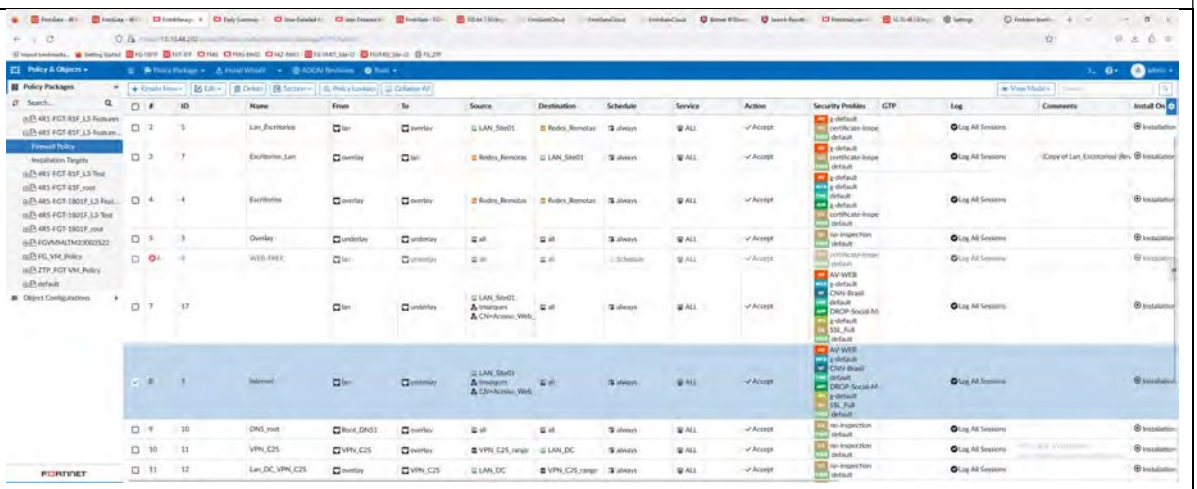
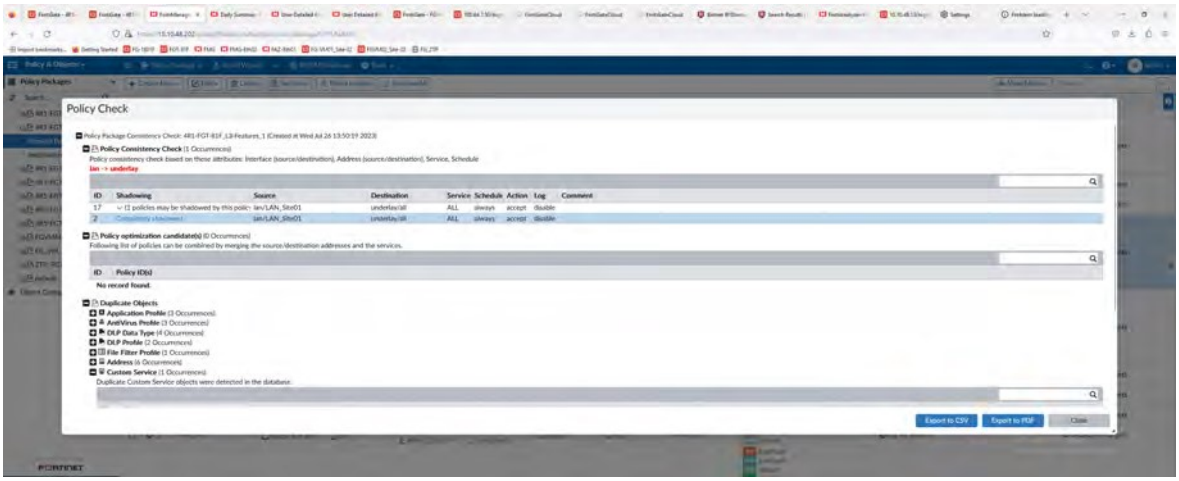
Item de Teste - 5.4.16	A solução deve possuir registro de todas as alterações realizadas em uma política de segurança, por um determinado administrador, permitindo a identificação do responsável pela mudança, contendo registros de autoria, data e origem;
Objetivo do Teste	Verificar se a solução consegue 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	





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.   
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 - 5.4.17	Prover funcionalidade para análise e auditoria de regras com capacidade de detectar regras conflitantes ou não conformes;
Objetivo do Teste	Verificar se o equipamento faz uma validação de políticas que estão conflitantes entre si ou em não conformação.
Configuração do Teste	Demonstrar a sobreposição de regras que se anulam ou se repetem.
Procedimento do Teste	Primeiramente, é necessário importar as políticas presentes no dispositivo. 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.
Evidências	  **TESTE OK**

Perform a policy consistency check

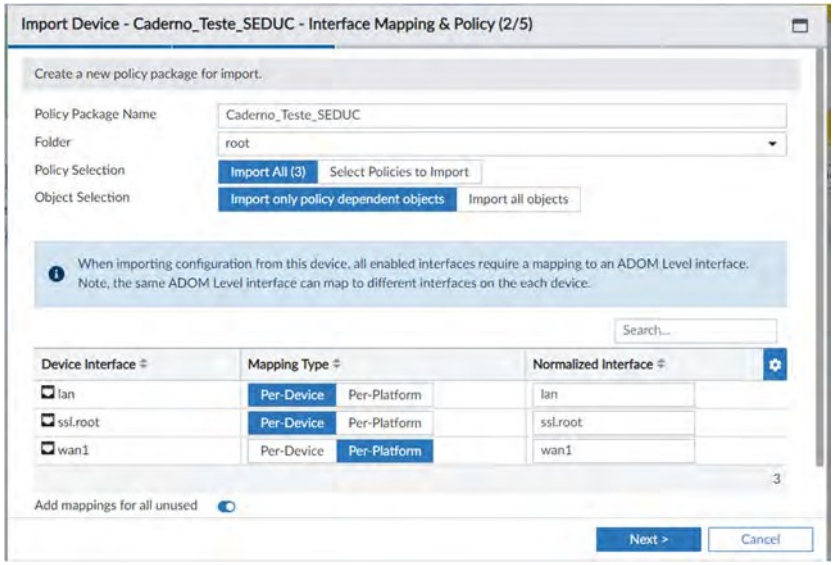
The policy check tool allows you to check all policy packages within an ADOM to ensure consistency and eliminate conflicts that may prevent your devices from passing traffic. This allows you to optimize your policy sets and potentially reduce the size of your databases.

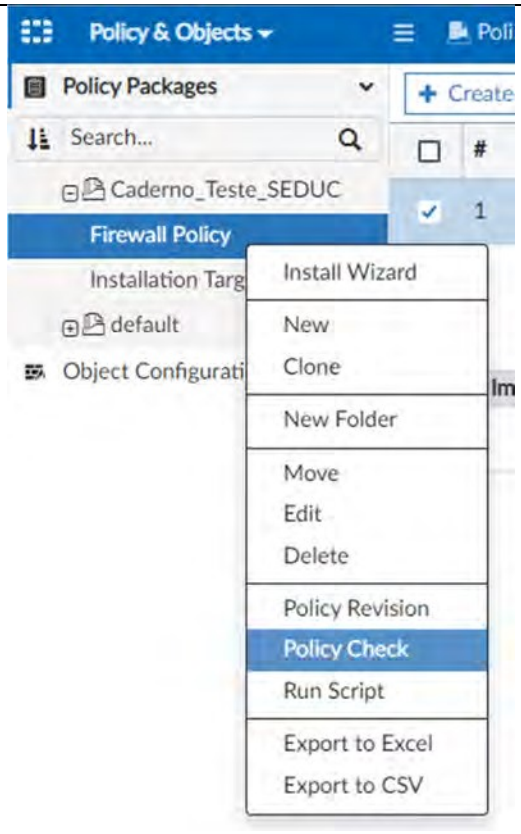
The check will verify:

- 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.

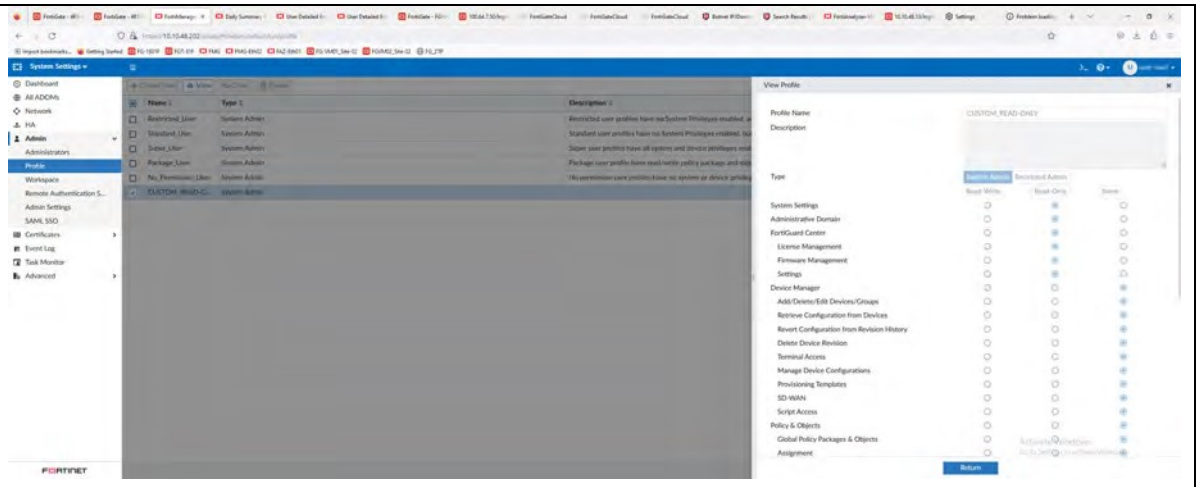
The policy check uses an algorithm to evaluate policy objects, based on the following attributes:

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



	
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 - 5.4.18	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	

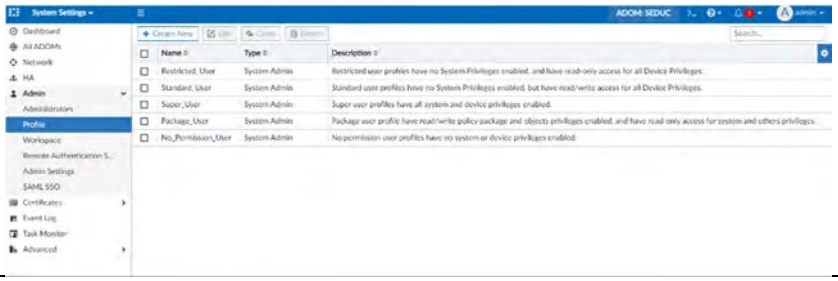


TESTE OK

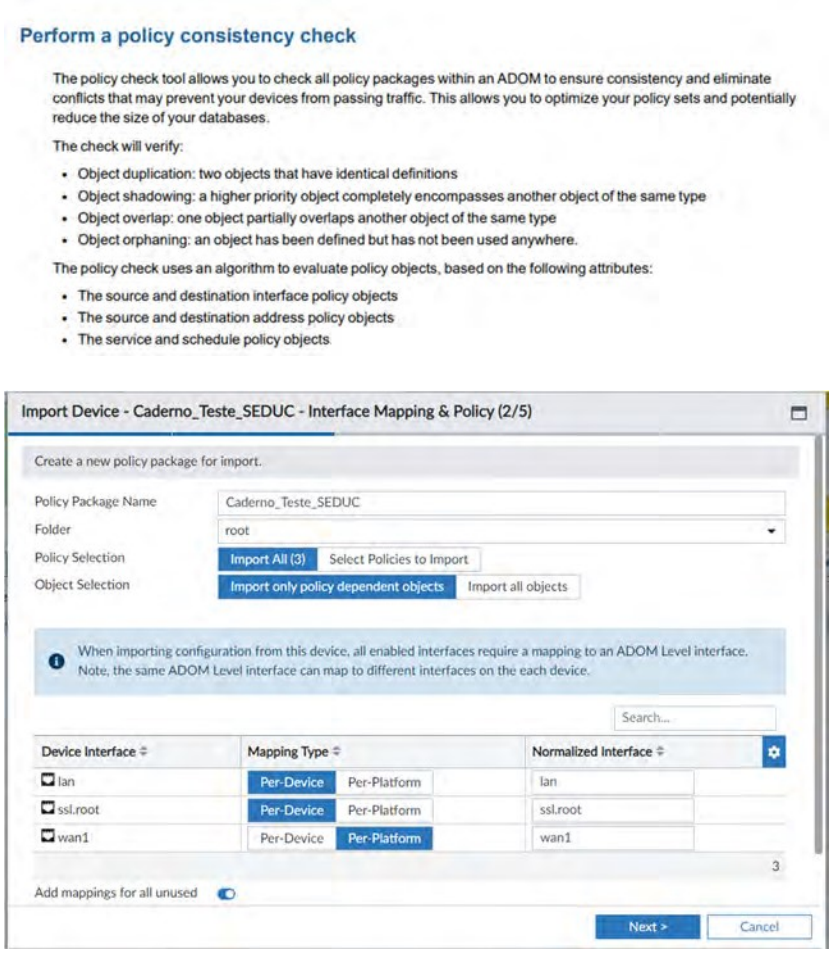
Por padrão, o FortiManager já vem com os seguintes perfis:

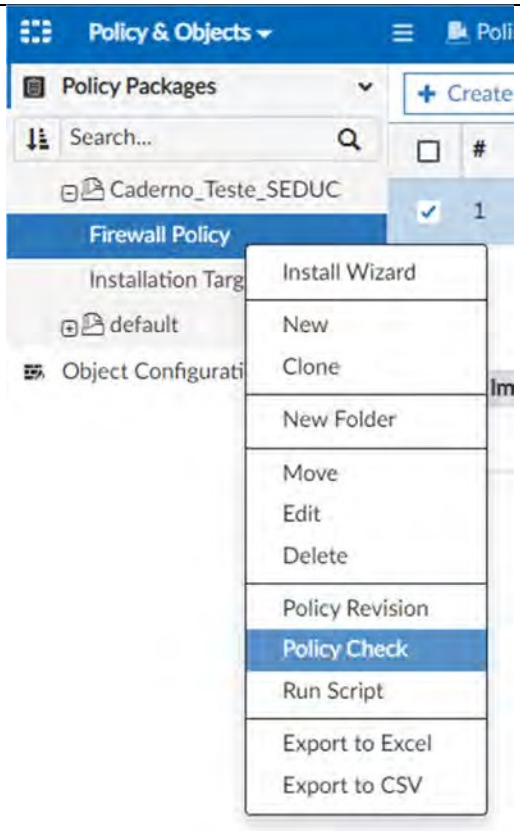
Restricted_User	Restricted user profiles have no system privileges enabled, and have read-only access for all device privileges.
Standard_User	Standard user profiles have no system privileges enabled, and have read/write access for all device privileges.
Super_User	Super user profiles have all system 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.

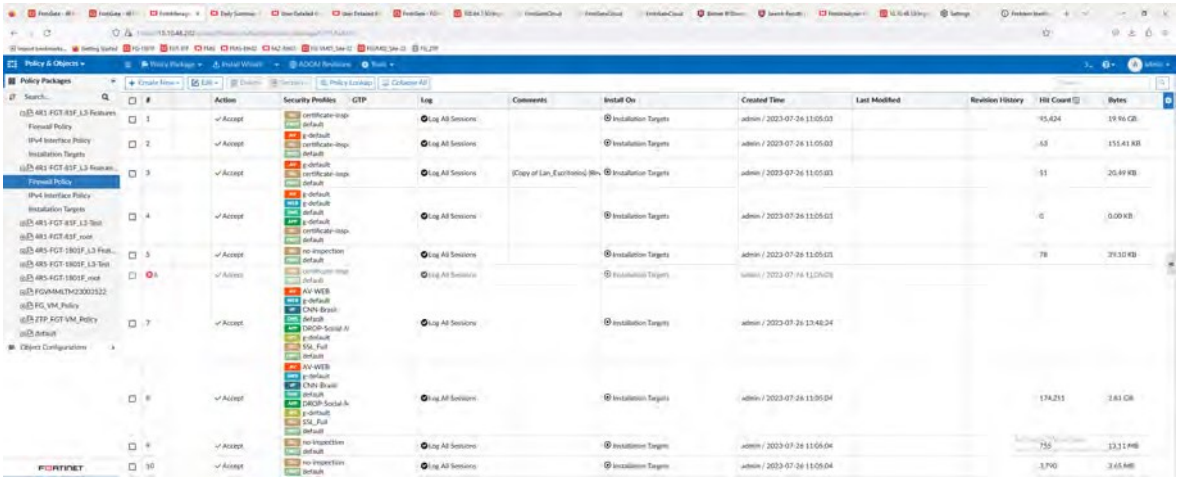


Comentário	Fonte: FortiManager Administration Guide acessado em: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/04f80bb3-e03c-11ec-bb32-fa163e15d75b/FortiManager-7.2.1-Administration_Guide.pdf

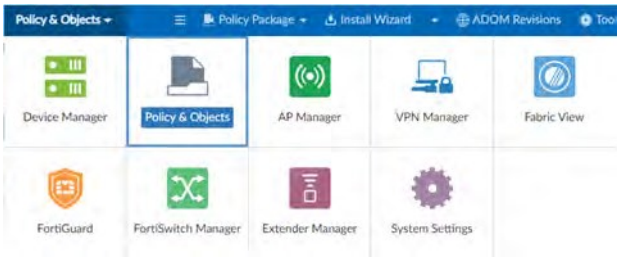
Item de Teste - 5.4.19	Deverá possuir validação da política avisando quando houver regras que ofusquem ou conflitem com outras regras;
Objetivo do Teste	Verificar se o equipamento faz uma validação de políticas que estão sendo ofuscados ou em conflitos com outras regras.
Configuração do Teste	Demonstrar a sobreposição de regras que se anulam ou se repetem.
Procedimento do Teste	Primeiramente, é necessário importar as políticas presentes no dispositivo. 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.
Evidências	Atendido conforme subitem 5.4.17 **TESTE OK** 

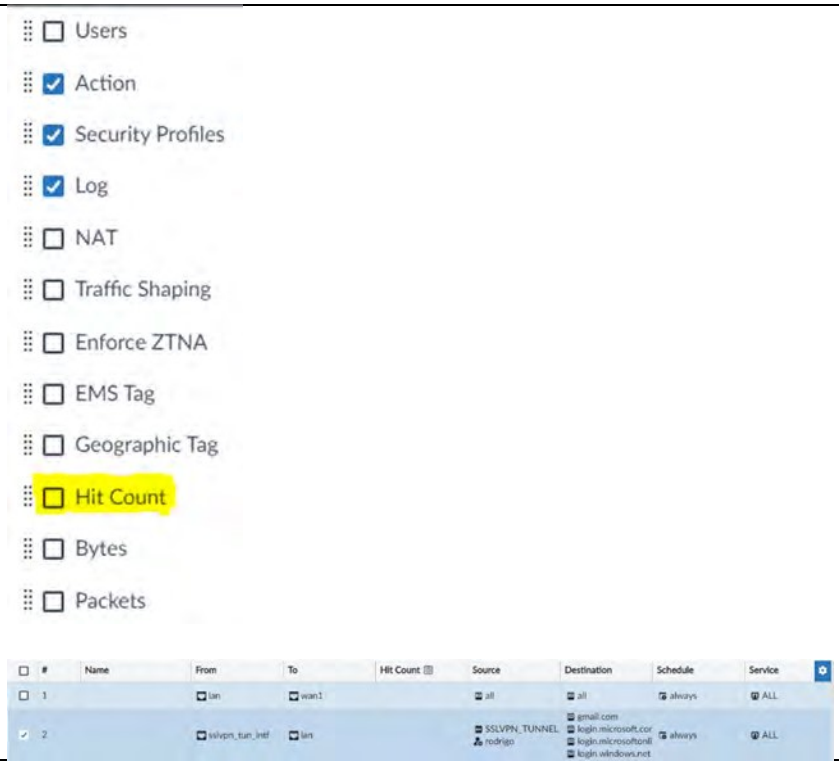
	
Comentário	Fonte: FortiManager Administration Guide acessado em: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/04f80bb3-e03c-11ec-bb32-fa163e15d75b/FortiManager-7.2.1-Administration_Guide.pdf

Item de Teste -5.4.20	A solução deve possuir “hit”/volume de regras para identificar possíveis melhorias na performance reordenando as mesmas;
Objetivo do Teste	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;
Configuração do Teste	Demonstrar hit counts de regras em uso.
Procedimento do Teste	Para isto, é necessário acessar a aba de “Policy & Objects”. 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”.
Evidências	

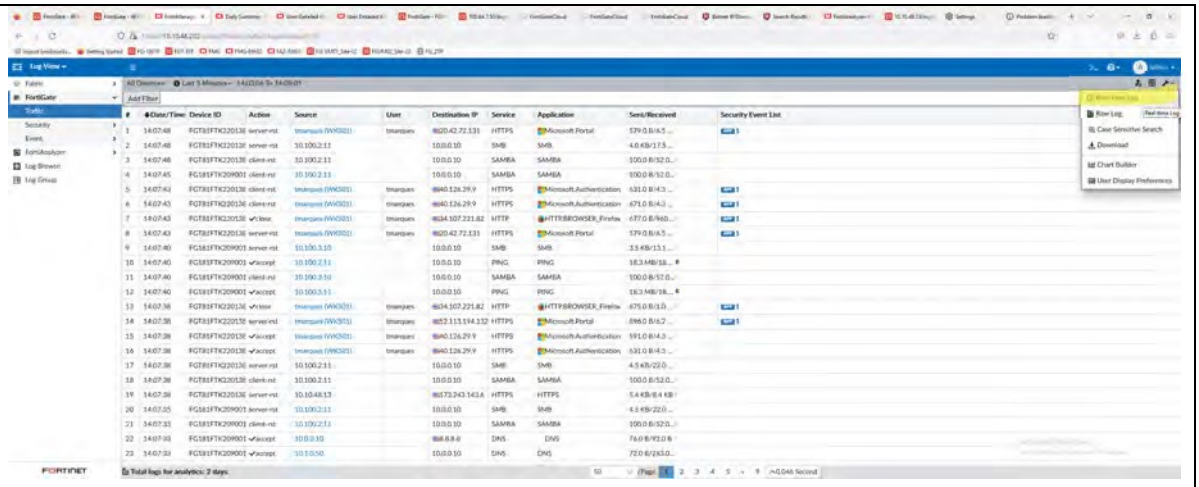
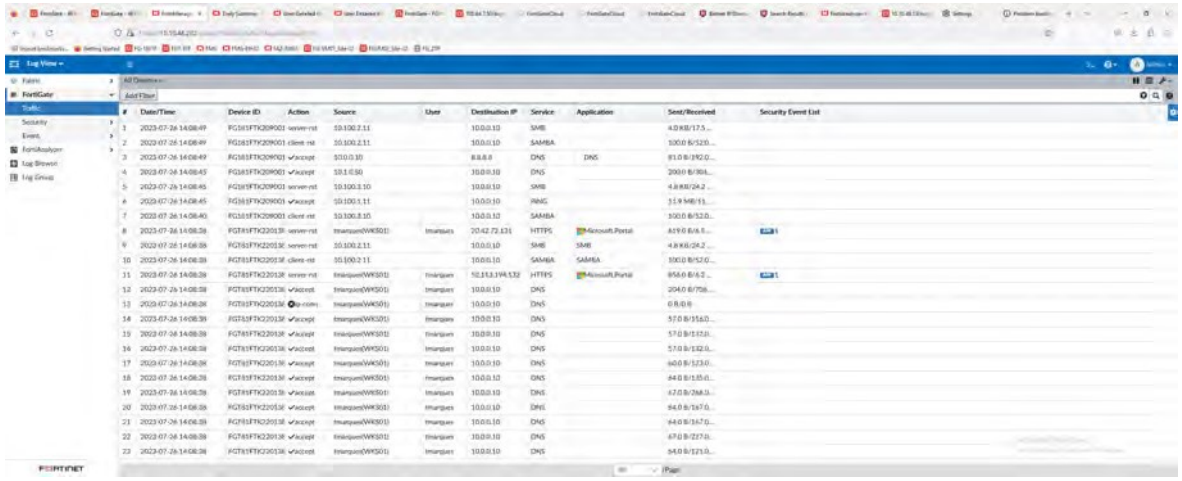


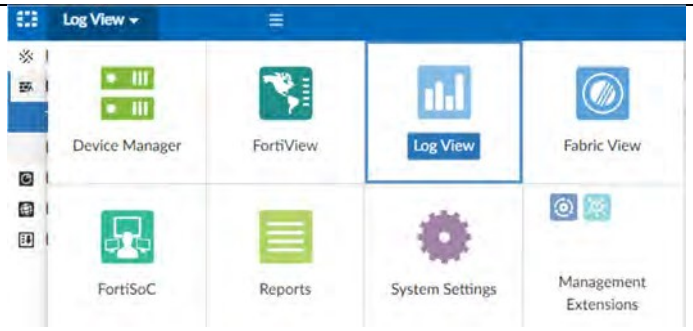
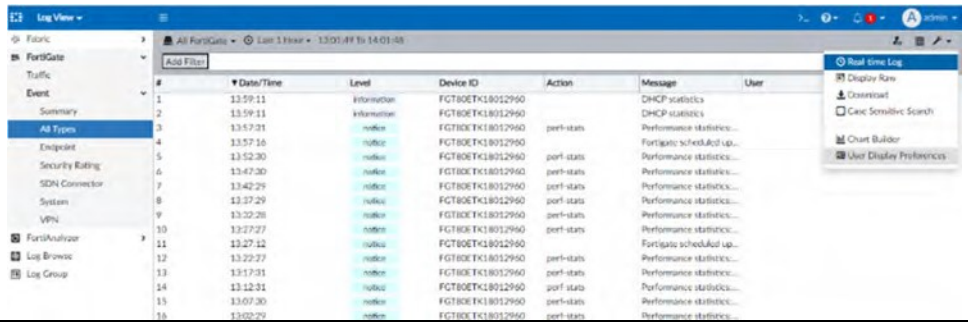
TESTE OK

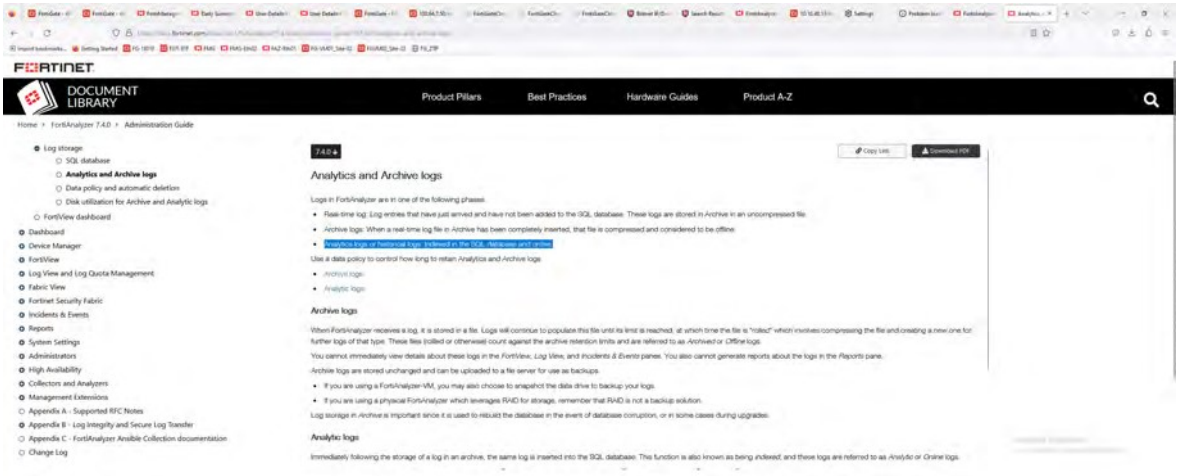

Policy & Objects
Policy Package
Install Wizard
ADOM Revisions
Device Manager
Policy & Objects
AP Manager
VPN Manager
Fabric View
FortiGuard
FortiSwitch Manager
Extender Manager
System Settings

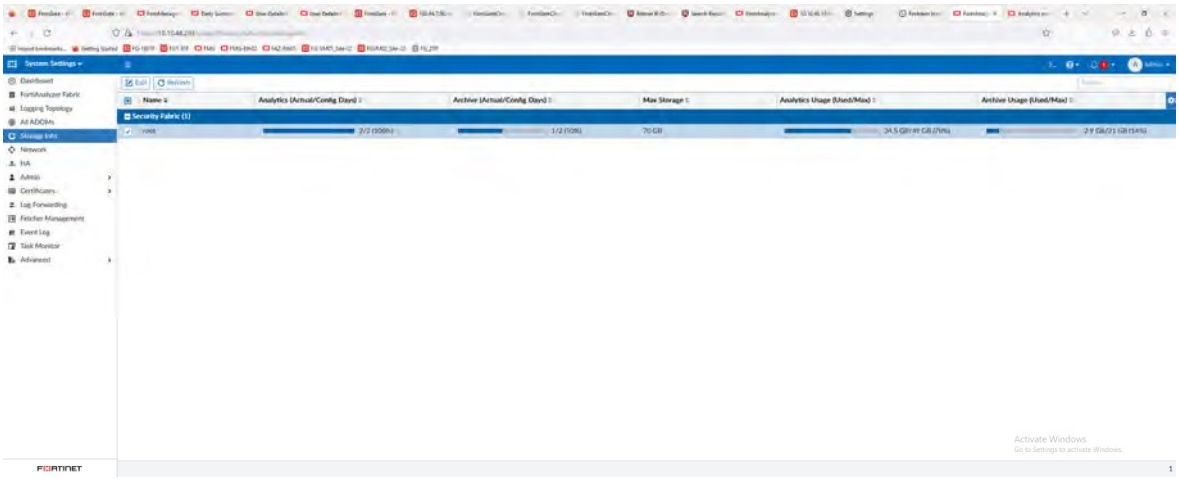
	
Comentário	

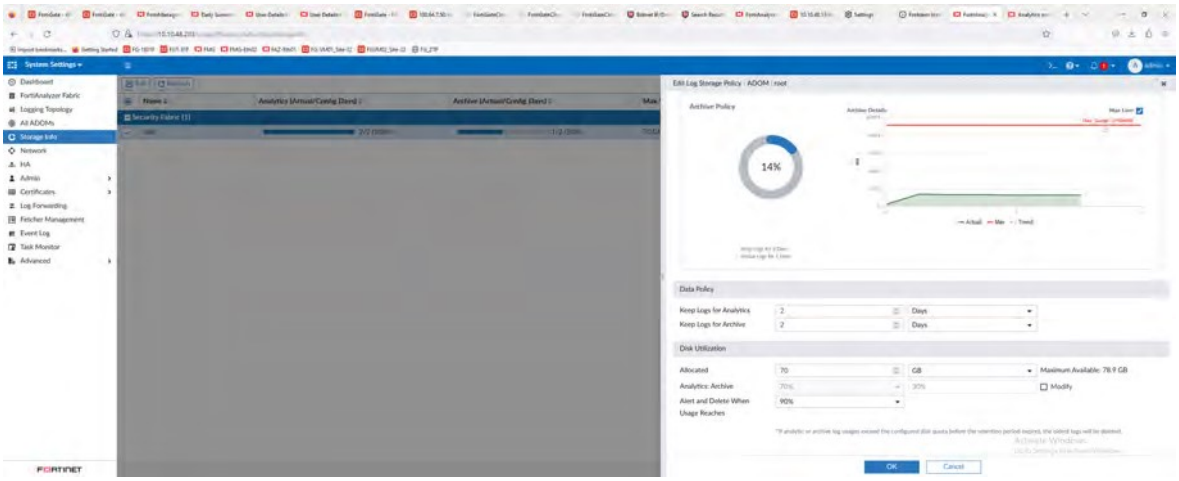
Item de Teste - 5.4.21	Deve possuir visualização de log em tempo próximo ao real;
Objetivo do Teste	Verificar se o equipamento possui a funcionalidade de visualização de logs em tempo próximo ao real.
Configuração do Teste	Demonstrar a sobreposição de regras que se anulam ou se repetem.
Procedimento do Teste	Para acessar a funcionalidade de visualização dos registros em tempo real, é necessário acessar a seção "Visualização de Logs". 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".
Evidências	

	  **TESTE OK**

	 
Comentário	

Item de Teste - 5.4.22	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;
Objetivo do Teste	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.
Configuração do Teste	Navegar no dashboard analíticos e demonstrar drill down de logs.
Procedimento do Teste	Navegar no dashboard analíticos e demonstrar drill down de logs.
Evidências	





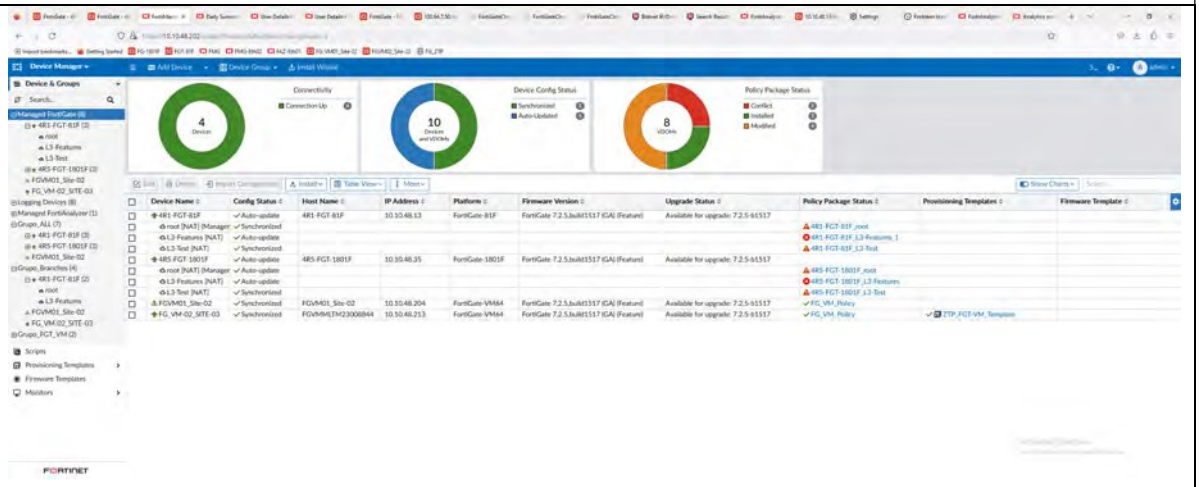
TESTE OK

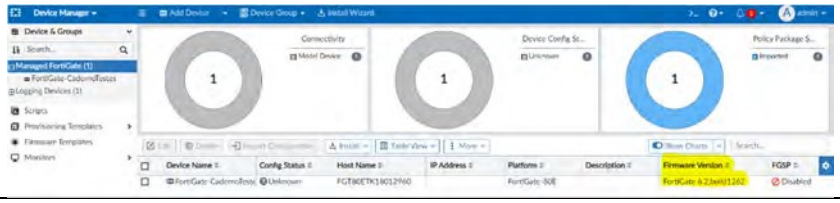
O FortiAnalyzer faz uma distinção dos logs de duas formas, uma são os logs arquivados e outras são de logs analíticos, os logs arquivados são os logs de tempo real que são arquivados e comprimidos e considerados offline, já os logs analíticos são indexados em um banco de dados SQL e considerados online.

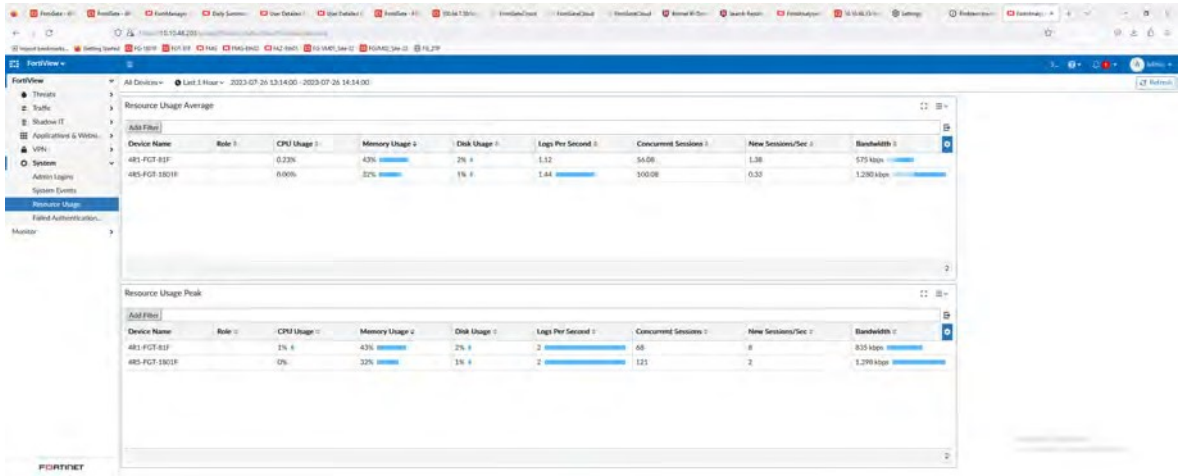
	Analytics and Archive logs Logs in FortiAnalyzer are in one of the following phases. • Real-time log: Log entries that have just arrived and have not been added to the SQL database. These logs are stored in Archive in an uncompressed file. • Archive logs: When a real-time log file in Archive has been completely inserted, that file is compressed and considered to be offline. • Analytics logs or historical logs: Indexed in the SQL database and online. Use a data policy to control how long to retain Analytics and Archive logs. • Archive logs • Analytic logs
Comentário	Fonte: "Analytics and Archive logs" acessado em: https://docs.fortinet.com/document/fortianalyzer/7.2.2/administration-guide/761825/analytics-and-archive-logs

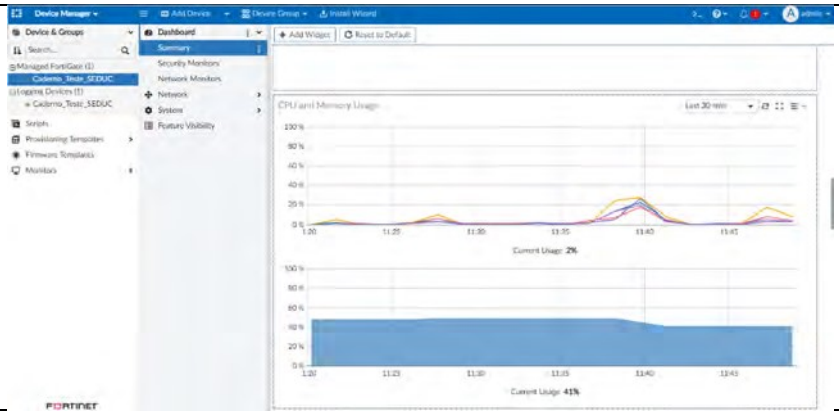
5.4.39 Solução deve incluir monitoramento gráfico que fornece uma maneira fácil

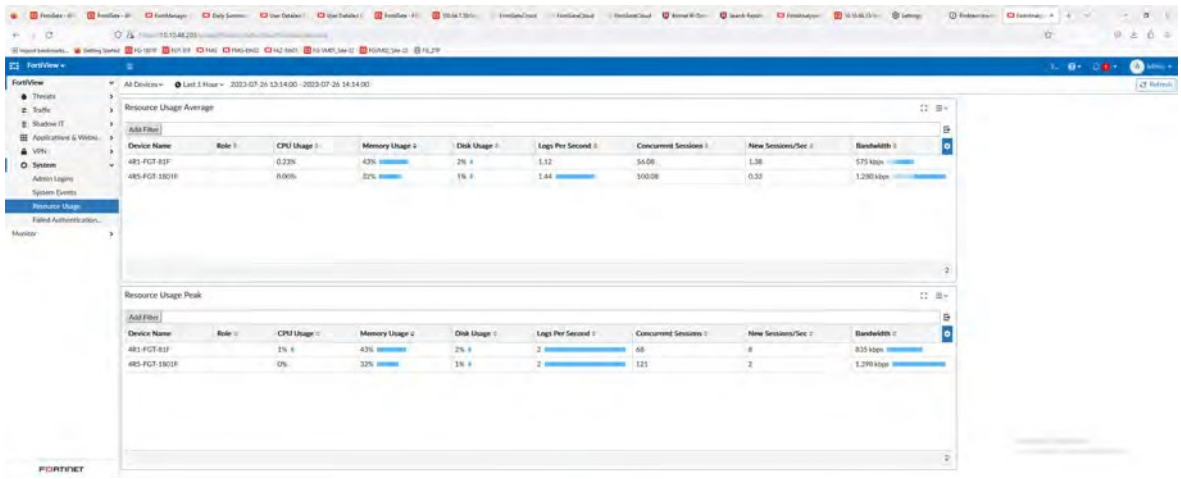
monitorar o status de gateways, apresentando os seguintes status:

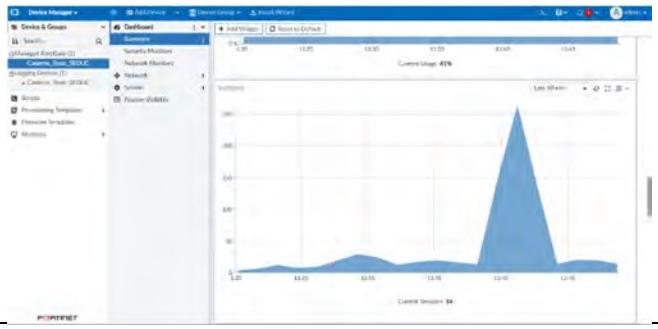
Item de Teste - 5.4.39.1	Versão do sistema operacional;
Objetivo do Teste	Verificar se a solução de gerenciamento possui visualização das versões do sistema operacional dos equipamentos gerenciados.
Configuração do Teste	Demonstrar versões de sistemas operacionais gerenciados.
Procedimento do Teste	Demonstrar versões de sistemas operacionais gerenciados.
Evidências	 **TESTE OK**

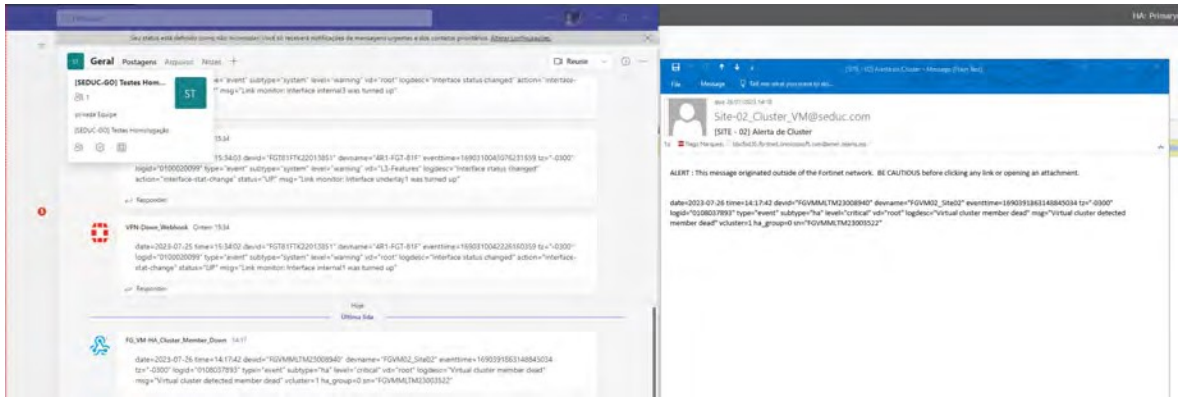
	Na aba de “Device Manager” podemos ter acesso a algumas informações dos equipamentos gerenciados, entre elas, a versão do sistema operacional. 
Comentário	

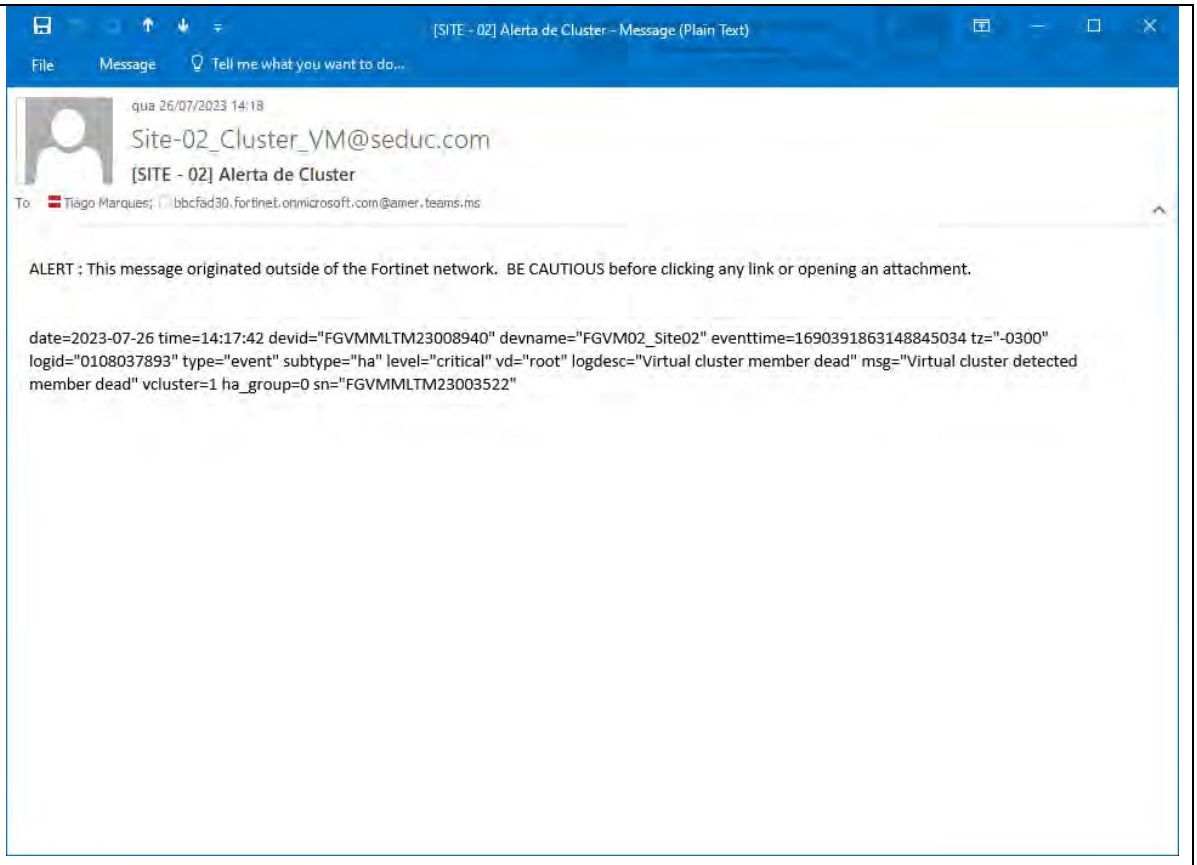
Item de Teste - 5.4.39.2	Informações de utilização de CPU dos gateways gerenciados;
Objetivo do Teste	Verificar se a solução de gerenciamento possui visualização da utilização de CPU dos gateways gerenciados.
Configuração do Teste	Demonstrar consumo de CPU dos gateways gerenciados.
Procedimento do Teste	Demonstrar consumo de CPU dos gateways gerenciados.
Evidências	 **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 consume de conexões concorrentes por gateways gerenciados.
Procedimento do Teste	Demonstrar consume de conexões concorrentes por gateways gerenciados.
Evidências	 **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 conexões concorrentes.

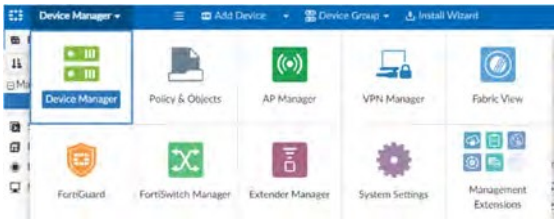
	 
Comentário	

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

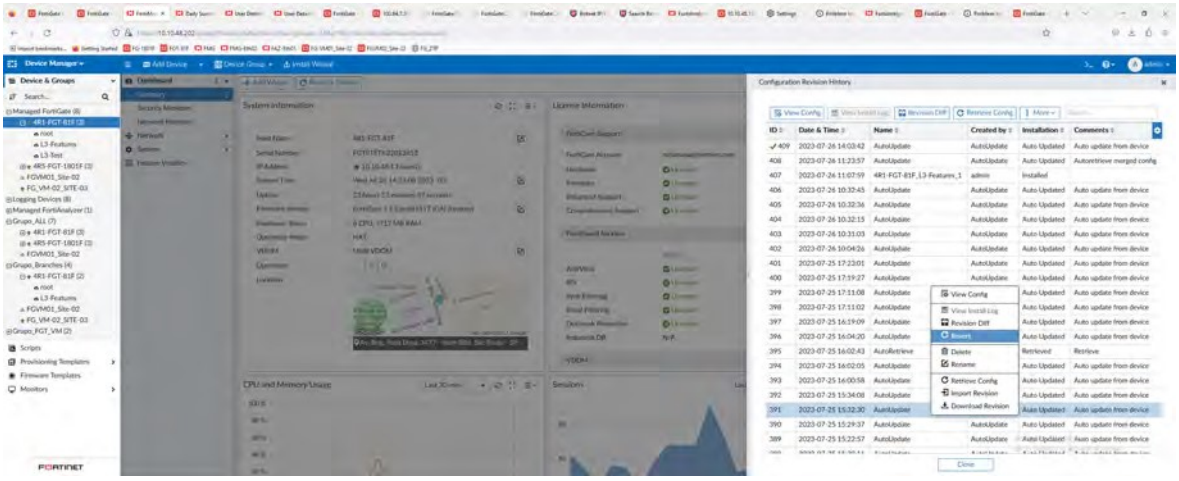
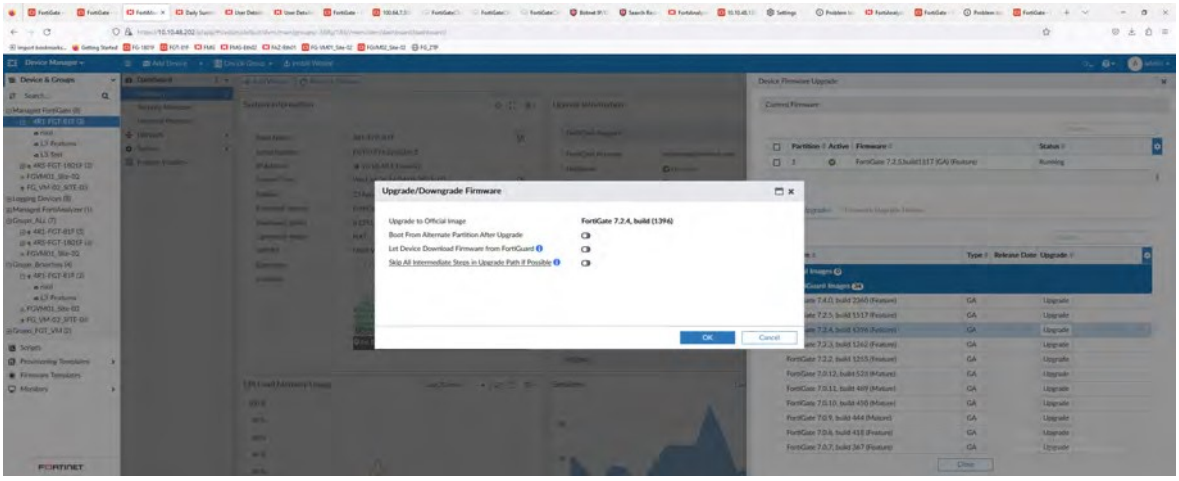


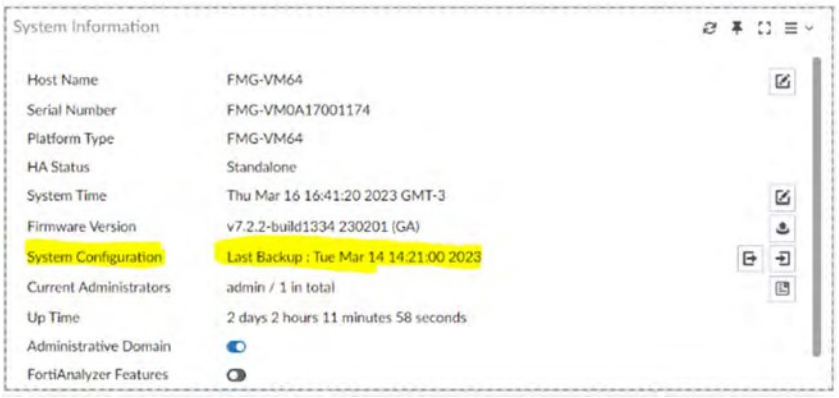
TESTE OK

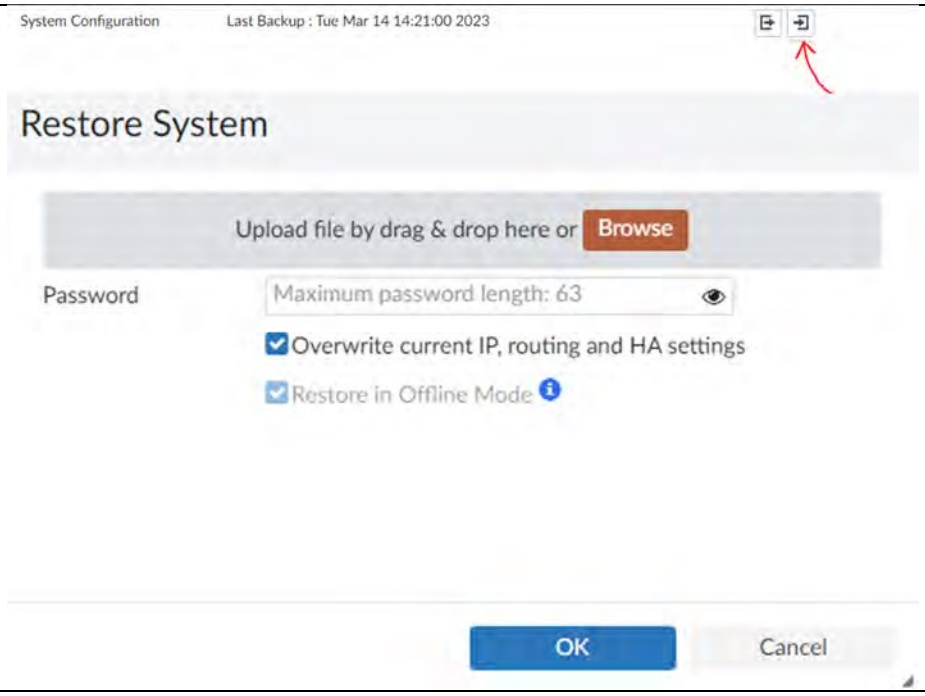
Na aba de “Device Manager” podemos selecionar qualquer um dos equipamentos gerenciados. Quando fazemos isso, podemos ter visualização de diversas informações daquele equipamento, entre elas, o estado dos clusters.



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	  **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	

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;

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;

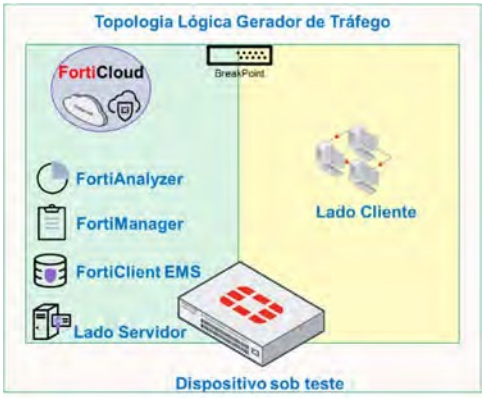
8.1.4. CONEXÕES CONCORRENTES:

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 editalíticio:
  - 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

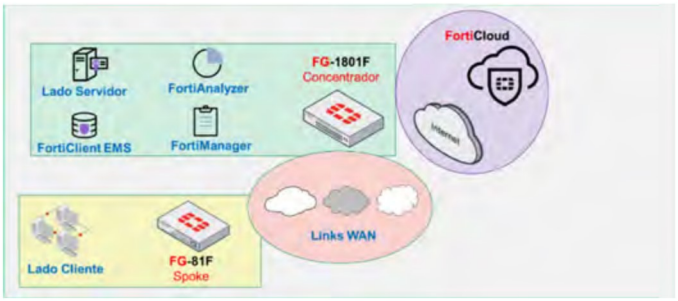
- Fluxo em HTTP 64 bytes
- Janela de teste composta por duas fases sendo:
  - Rampa de subida com tempo inferior a 1 minuto que não será considerada para aferição;
  - Curso após estabilização com tempo de 5 minutos, sendo considerado para aferição.
- Foco em abrir e fechar conexões
- Conexões TCP encerradas 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:63625032104

Digitally signed by JOSE ARMANDO DOS REIS COSTA:63625032104
DN: C=BR, O=ICP-Brasil, OU=00000101072545S, OU=Secretaria da Receita Federal do Brasil - RFB, OU=RFB e-CPF A3, OU=AC SERASA RFB, OU=26718487000136, OU=PRESENCIAL, CN=JOSE ARMANDO DOS REIS COSTA:63625032104
Reason: I am approving this document
Location:
Date: 2023.08.01 13:29:50-03'00'
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