



	<div data-bbox="523 320 1002 1137"> <p>LDAP Distinguished Name Query</p> <ul style="list-style-type: none"> <li>dc=trainingAD,dc=training,dc=lab           <ul style="list-style-type: none"> <li>CN=Users</li> <li>CN=Computers</li> <li>OU=Domain Controllers</li> <li>CN=System               <ul style="list-style-type: none"> <li>CN=WinsockServices</li> <li>CN=RpcServices</li> <li>CN=Meetings</li> <li>CN=Policies                   <ul style="list-style-type: none"> <li>CN={31B2F340-016D-11D2-945F-00C04FB984F9}                       <ul style="list-style-type: none"> <li>CN=User</li> <li>CN=Machine</li> </ul> </li> <li>CN={6AC1786C-016F-11D2-945F-00C04FB984F9}                       <ul style="list-style-type: none"> <li>CN=User</li> <li>CN=Machine</li> </ul> </li> </ul> </li> <li>CN=RAS and IAS Servers Access Check</li> <li>CN=IP Security</li> <li>CN=AdminSDHolder</li> <li>CN=ComPartitions</li> <li>CN=ComPartitionSets</li> <li>CN=WMIPolicy                   <ul style="list-style-type: none"> <li>CN=PolicyTemplate</li> <li>CN=SOM</li> <li>CN=PolicyType</li> <li>CN=WMIGPO</li> </ul> </li> <li>CN=DomainUpdates                   <ul style="list-style-type: none"> <li>CN=Operations                       <ul style="list-style-type: none"> <li>CN=ab402345-d3c3-455d-9ff7-40268a1099b6</li> <li>CN=bab5f54d-06c8-48de-9b87-d78b796564e4</li> <li>CN=f3dd09dd-25e8-4f9c-85df-12d6d2f2f2f5</li> <li>CN=2416c60a-fe15-4d7a-a61e-dffd5df864d3</li> <li>CN=7868d4c8-ac41-4e05-b401-776280e8e9f1</li> <li>CN=860c36ed-5241-4c62-a18b-cf6ff9994173</li> <li>CN=0e660ea3-8a5e-4495-9ad7-ca1bd4638f9e</li> <li>CN=a86fe12a-0f62-4e2a-b271-d27f601f8182</li> <li>CN=40f50bf4-0046-4a2d-a2b5-002e00404754</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> <p>OK Cancel</p> </div> <div data-bbox="523 1176 1353 1592"> <p>Dashboard</p> <ul style="list-style-type: none"> <li>Network</li> <li>Policy &amp; Objects</li> <li>Security Profiles</li> <li>VPN</li> <li>User &amp; Authentication           <ul style="list-style-type: none"> <li>User Definition               <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Two-factor Authentication</th> <th>Groups</th> </tr> </thead> <tbody> <tr> <td>flavio</td> <td>LDAP</td> <td>○</td> <td></td> </tr> <tr> <td>fulano</td> <td>LDAP</td> <td>○</td> <td></td> </tr> <tr> <td>quest</td> <td>LOCAL</td> <td>○</td> <td>Grupo_Guest_SEDUC Guest-group</td> </tr> <tr> <td>guilherme.reis</td> <td>LDAP</td> <td>○</td> <td></td> </tr> <tr> <td>jayr</td> <td>LDAP</td> <td>○</td> <td></td> </tr> <tr> <td>rodrigo</td> <td>LOCAL</td> <td>○</td> <td>Grupo_Guest_SEDUC</td> </tr> <tr> <td>rodrigo.andrade</td> <td>LDAP</td> <td>○</td> <td></td> </tr> <tr> <td>victor.merli</td> <td>LDAP</td> <td>○</td> <td></td> </tr> <tr> <td>victor.nika</td> <td>LOCAL</td> <td>○</td> <td>Grupo_Guest_SEDUC</td> </tr> </tbody> </table> </li> </ul> </li> </ul> </div>	Name	Type	Two-factor Authentication	Groups	flavio	LDAP	○		fulano	LDAP	○		quest	LOCAL	○	Grupo_Guest_SEDUC Guest-group	guilherme.reis	LDAP	○		jayr	LDAP	○		rodrigo	LOCAL	○	Grupo_Guest_SEDUC	rodrigo.andrade	LDAP	○		victor.merli	LDAP	○		victor.nika	LOCAL	○	Grupo_Guest_SEDUC
Name	Type	Two-factor Authentication	Groups																																						
flavio	LDAP	○																																							
fulano	LDAP	○																																							
quest	LOCAL	○	Grupo_Guest_SEDUC Guest-group																																						
guilherme.reis	LDAP	○																																							
jayr	LDAP	○																																							
rodrigo	LOCAL	○	Grupo_Guest_SEDUC																																						
rodrigo.andrade	LDAP	○																																							
victor.merli	LDAP	○																																							
victor.nika	LOCAL	○	Grupo_Guest_SEDUC																																						
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**

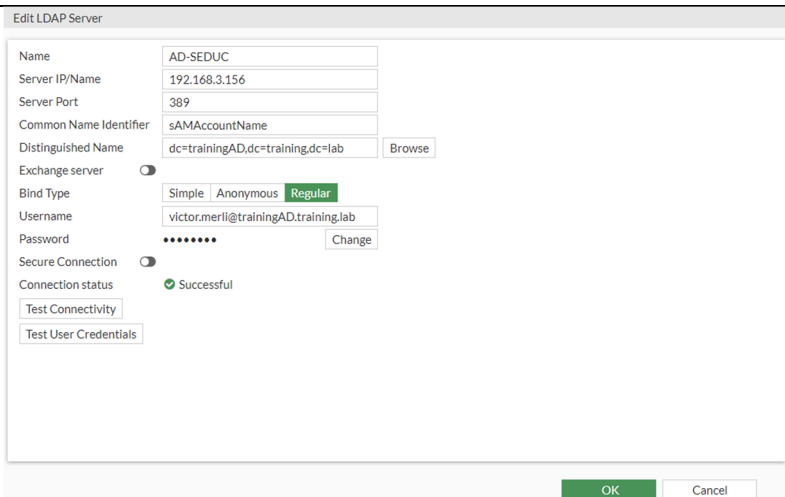
Name	Category	Technology	Popularity	Risk
1koun	Video/Audio	Client-Server	★★★★☆	Medium
1und1.Mail	Email	Browser-Based	★★★★☆	Medium
2Safe	Storage.Backup	Browser-Based	★★★★☆	Medium
2Safe_File.Download	Storage.Backup	Browser-Based	★★★★☆	Medium
2Safe_File.Upload	Storage.Backup	Browser-Based	★★★★☆	Medium
2ch	Social.Media	Browser-Based	★★★★☆	Medium
2ch_Post	Social.Media	Browser-Based	★★★★☆	Medium
2shared_File.Download	Storage.Backup	Browser-Based	★★★★☆	Medium
2shared_File.Upload	Storage.Backup	Browser-Based	★★★★☆	Medium
3PC	Network.Service	Network-Protocol	★★★★☆	Medium
45ync	Storage.Backup	Browser-Based	★★★★☆	Medium
45ync_File.Upload	Storage.Backup	Browser-Based	★★★★☆	Medium



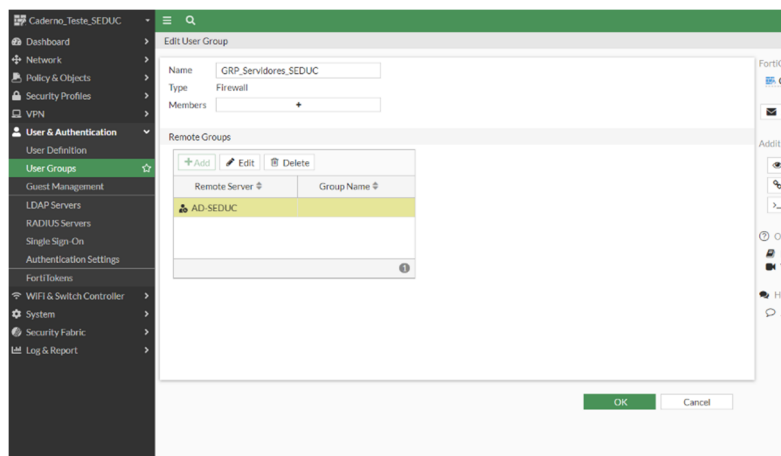
Comentário	

### 5.3.6 IDENTIFICAÇÃO DE USUÁRIOS:

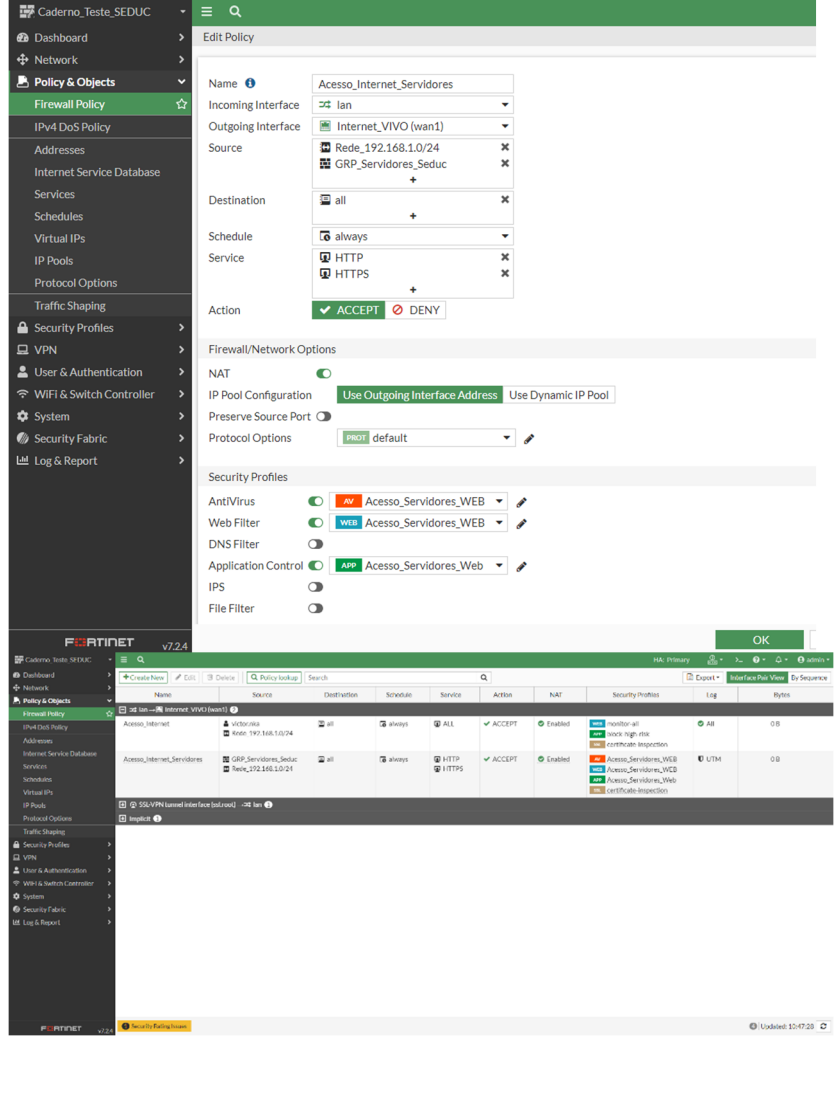
Item de Teste - 5.3.6.1	Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório;
Objetivo do Teste	Validar se a ferramenta tem a capacidade de realizar o controle de qual usuário está utilizando determinada aplicação, por meio de integração com serviços de diretório
Configuração do Teste	Demonstrar capacidade de integração com o AD.
Procedimento do Teste	<p>Navegando por <b>User and Authentication &gt; LDAP Servers &gt; Create New</b> é possível realizar a integração com os serviços de diretório</p> <p>Navegando por <b>User and Authentication &gt; User Group &gt; Create New</b> podemos criar um novo grupo de usuários linkado com o grupo do AD</p> <p>Navegando por <b>Policy &amp; Objects &gt; Firewall Policy</b> é possível realizar a criação de regras utilizando como origem o grupo criado com a integração do AD;</p> <p>Navegando por <b>Policy &amp; Objects &gt; Firewall Policy</b> podemos criar uma nova política utilizando o grupo do firewall no campo "source".</p> <p>Na mesma política podemos incluir perfis de segurança específicos para os grupos.</p>
Evidências	1 - Integração com AD via LDAP



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



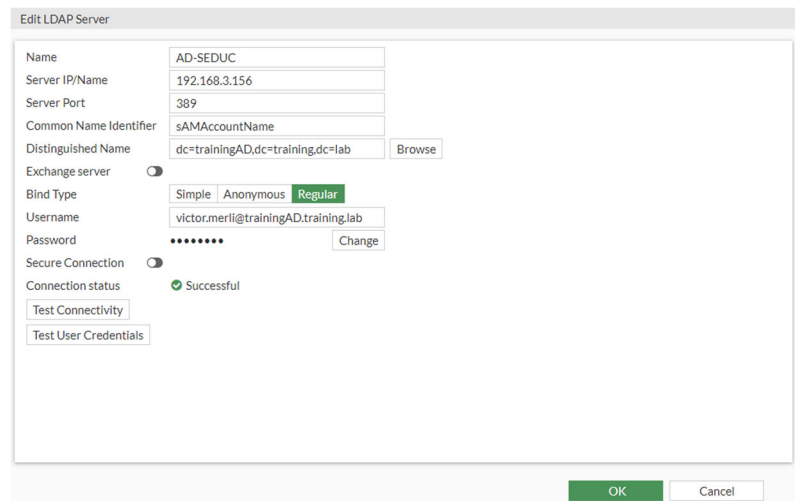
3- Criação de uma política com filtro de aplicação e web

	 <table border="1" data-bbox="515 1025 1353 1144"> <thead> <tr> <th>Name</th> <th>Source</th> <th>Destination</th> <th>Schedule</th> <th>Service</th> <th>Action</th> <th>NAT</th> <th>Security Profiles</th> <th>Log</th> <th>Filter</th> </tr> </thead> <tbody> <tr> <td>Acesso_Internet</td> <td>Rede_192.168.1.0/24</td> <td>all</td> <td>always</td> <td>ALL</td> <td>ACCEPT</td> <td>Enabled</td> <td>AV: monitor all, WEB: blocking dns, Application Inspection</td> <td>All</td> <td>0.0</td> </tr> <tr> <td>Acesso_Internet_Servidores</td> <td>GRP_Servidores_Seduc</td> <td>all</td> <td>always</td> <td>HTTP, HTTPS</td> <td>ACCEPT</td> <td>Enabled</td> <td>AV: monitor all, WEB: blocking dns, Application Inspection, UTM</td> <td>0.0</td> <td>0.0</td> </tr> </tbody> </table>	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Filter	Acesso_Internet	Rede_192.168.1.0/24	all	always	ALL	ACCEPT	Enabled	AV: monitor all, WEB: blocking dns, Application Inspection	All	0.0	Acesso_Internet_Servidores	GRP_Servidores_Seduc	all	always	HTTP, HTTPS	ACCEPT	Enabled	AV: monitor all, WEB: blocking dns, Application Inspection, UTM	0.0	0.0
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Filter																						
Acesso_Internet	Rede_192.168.1.0/24	all	always	ALL	ACCEPT	Enabled	AV: monitor all, WEB: blocking dns, Application Inspection	All	0.0																						
Acesso_Internet_Servidores	GRP_Servidores_Seduc	all	always	HTTP, HTTPS	ACCEPT	Enabled	AV: monitor all, WEB: blocking dns, Application Inspection, UTM	0.0	0.0																						
<b>Comentário</b>	Fonte: <a href="https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/656084/firewall-policy">https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/656084/firewall-policy</a>																														

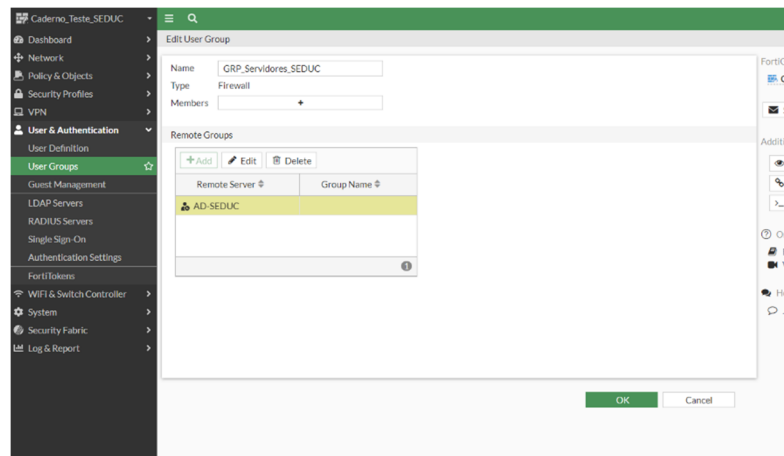
<b>Item de Teste - 5.3.6.2</b>	Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
<b>Objetivo do Teste</b>	Validar se a ferramenta possibilita integração com Microsoft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

**Evidências**

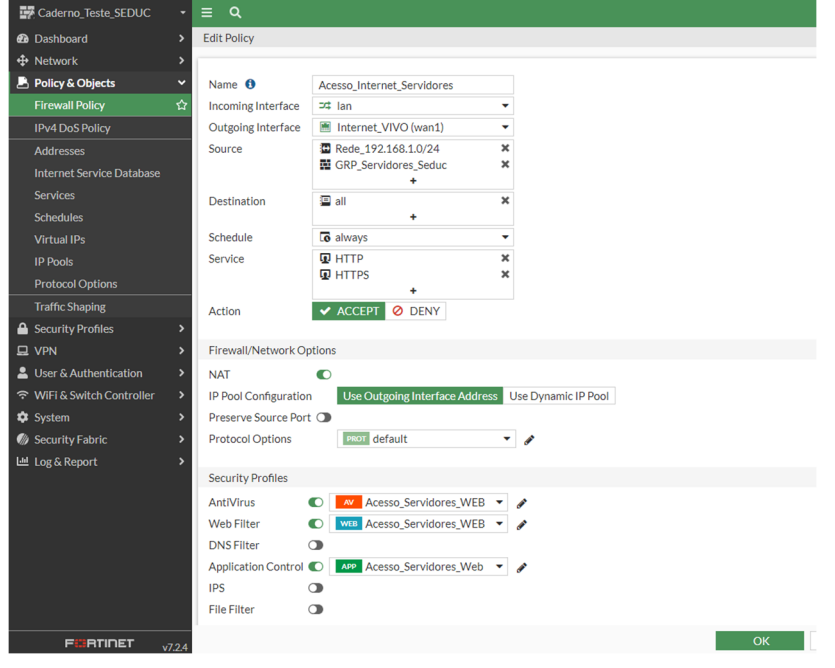
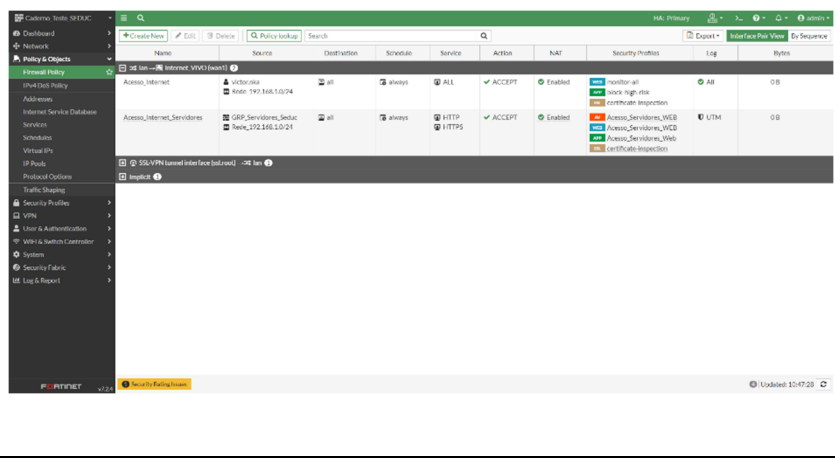
**1 - Integração com AD via LDAP**



**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**

<p><b>Comentário</b></p>	
	

<p><b>Item de Teste - 5.3.6.3</b></p>	<p>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;</p>
<p><b>Objetivo do Teste</b></p>	<p>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</p>
<p><b>Configuração do Teste</b></p>	<p>Demonstrar integração via WMI sem instalação de agente no cliente e no servidor AD.</p>
<p><b>Procedimento do Teste</b></p>	<p>Para realizar a integração dos serviços do Active Directory com o FortiGate, basta navegar por <b>User and Authentication &gt; LDAP Servers &gt; Create New</b>.</p>



A integração não necessita da instalação de nenhum software no Active Directory e nem nas estações dos usuários.

### Evidências

### Conectando o FortiGate ao Active Directory

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

Exchange server

Bind Type:  Simple  Anonymous  Regular

Username: victor.merli@trainingAD.training.lab

Password: ••••••••

Secure Connection

Connection status: ✔ Successful

Buttons: Test Connectivity, Test User Credentials, OK, Cancel

LDAP Distinguished Name Query

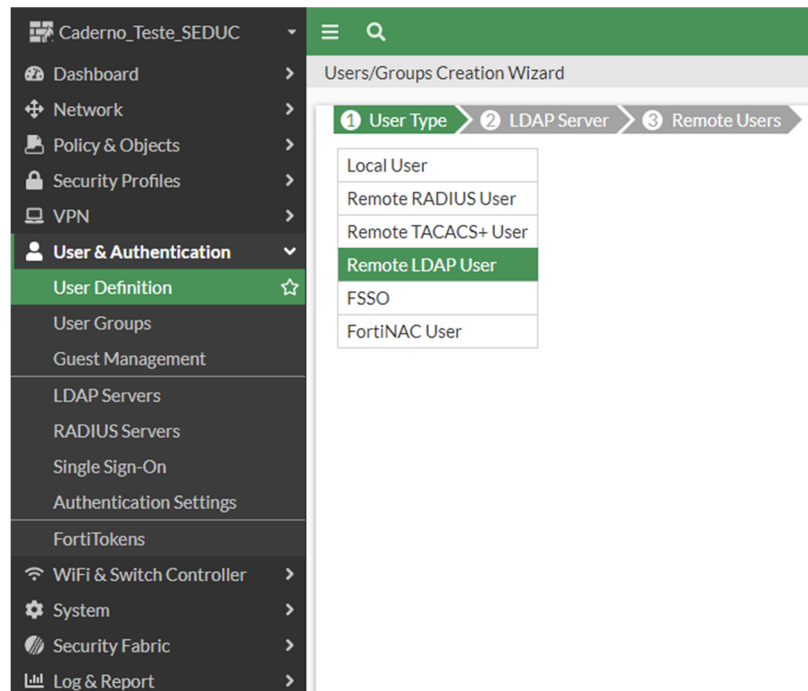
- dc=trainingAD,dc=training,dc=lab
  - CN=Users
  - CN=Computers
  - OU=Domain Controllers
  - CN=System
    - CN=WinsocServices
    - CN=RpcServices
    - CN=Meetings
  - CN=Policies
    - CN={31B2F340-016D-11D2-945F-00C04FB984F9}
      - CN=User
      - CN=Machine
    - CN={6AC1786C-016F-11D2-945F-00C04FB984F9}
      - CN=User
      - CN=Machine
  - CN=RAS and IAS Servers Access Check
  - CN=IP Security
  - CN=AdminSDHolder
  - CN=ComPartitions
  - CN=ComPartitionSets
  - CN=WMI Policy
    - CN=PolicyTemplate
    - CN=SOM
    - CN=PolicyType
    - CN=WMI GPO
  - 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
      - CN=405c06d4-0046-46d4-c2b5-02c0260475d4

Buttons: OK, Cancel



Name	Server	Port	Common Name/Identifier	Distinguished Name	Exchange Server	Sec.
AD-SEJUC	192.168.3.156	389	sAMAccountName	dc=trainingAD,dc=training,dc=lab		7

2 – Criando grupo no Firewall utilizando grupos do AD.



The screenshot shows the FortiGate web interface for configuring a user group. The left sidebar is expanded to 'User & Authentication' > 'User Definition'. The main area is the 'Users/Groups Creation Wizard' with three steps: 1. User Type, 2. LDAP Server, and 3. Remote Users. Under 'User Type', a list of options is shown, with 'Remote LDAP User' selected.

- Local User
- Remote RADIUS User
- Remote TACACS+ User
- Remote LDAP User**
- FSSO
- FortiNAC User



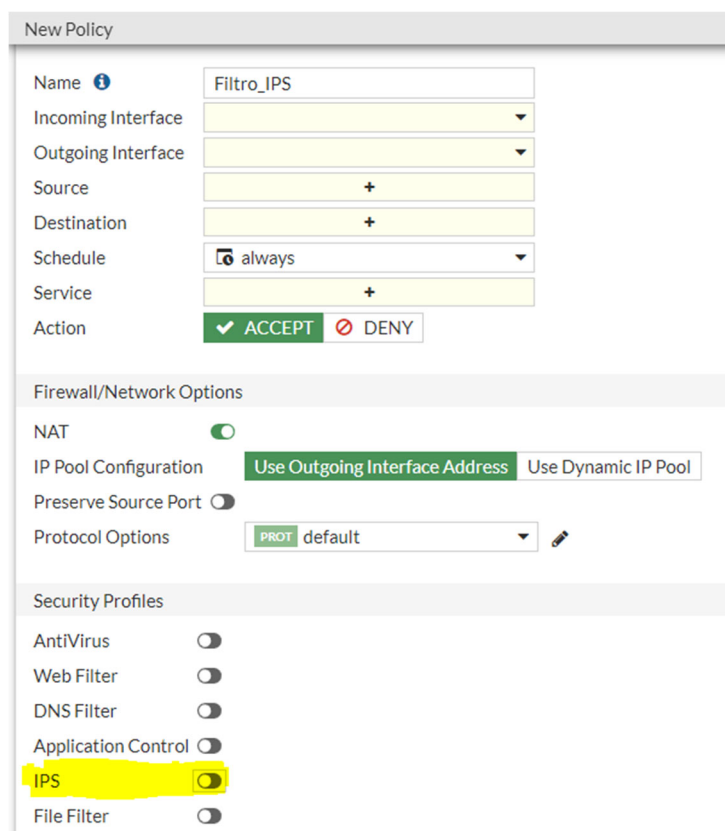
<b>Comentário</b>	

5.3.7 SISTEMA DE PREVENÇÃO DE INTRUSÃO - IPS:

<b>Item de Teste - 5.3.7.1</b>	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;
<b>Objetivo do Teste</b>	Verificar se a appliance possui módulo IPS integrado sem a necessidade de uso de quaisquer interfaces externas.
<b>Configuração do Teste</b>	Demonstrar configuração de IPS.
<b>Procedimento do Teste</b>	Demonstrar configuração de IPS.

**Evidências**

Dentro de uma política de segurança podemos notar a presença do Filtro IPS.



The screenshot shows the configuration for a new security policy named "Filtro\_IPS". The configuration is divided into three sections: "New Policy", "Firewall/Network Options", and "Security Profiles".

- New Policy:**
  - Name: Filtro\_IPS
  - Incoming Interface: (empty dropdown)
  - Outgoing Interface: (empty dropdown)
  - Source: (+)
  - Destination: (+)
  - Schedule: always
  - Service: (+)
  - Action: ACCEPT (checked), DENY
- Firewall/Network Options:**
  - NAT: (checked)
  - IP Pool Configuration: Use Outgoing Interface Address (selected), Use Dynamic IP Pool
  - Preserve Source Port: (unchecked)
  - Protocol Options: default
- Security Profiles:**
  - AntiVirus: (unchecked)
  - Web Filter: (unchecked)
  - DNS Filter: (unchecked)
  - Application Control: (unchecked)
  - IPS: (checked) - This row is highlighted in yellow.
  - File Filter: (unchecked)

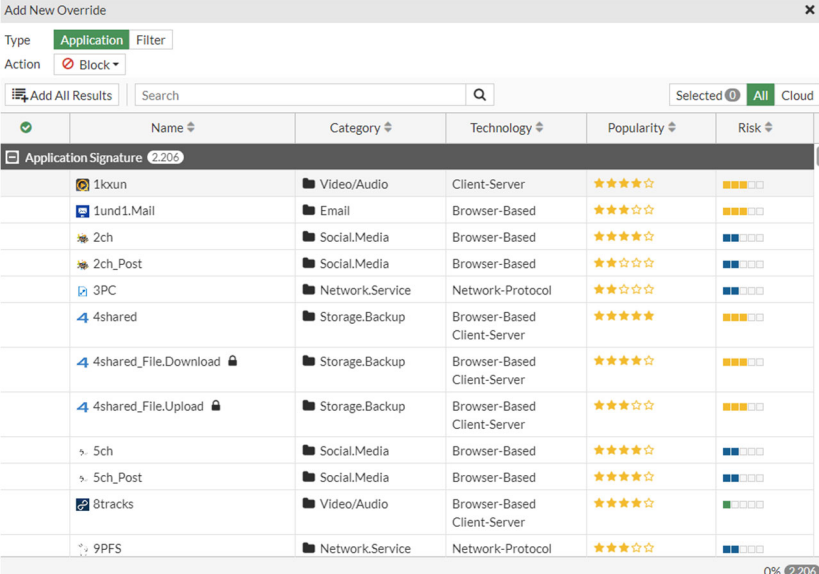
E dentro desse perfil de segurança podemos ter acesso a todas as assinaturas que ele conhece, como também o CVE daquela vulnerabilidade, a ação padrão e por fim o grau de severidade dela.

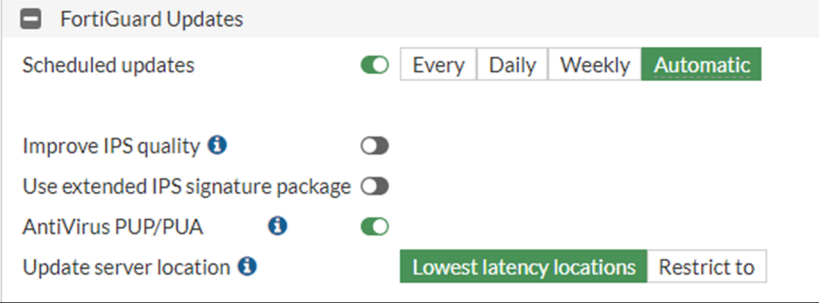


Comentário	

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 possui os seguintes mecanismos de detecção: assinaturas, anomalias de protocolos, controle de aplicações.
Configuração do Teste	Demonstrar na configuração de regra NGFW de IPS contendo: assinaturas, anomalias de protocolos, controle de aplicações;
Procedimento do Teste	Demonstrar na configuração de regra NGFW de IPS contendo: assinaturas, anomalias de protocolos, controle de aplicações;
Evidências	<p>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.</p>



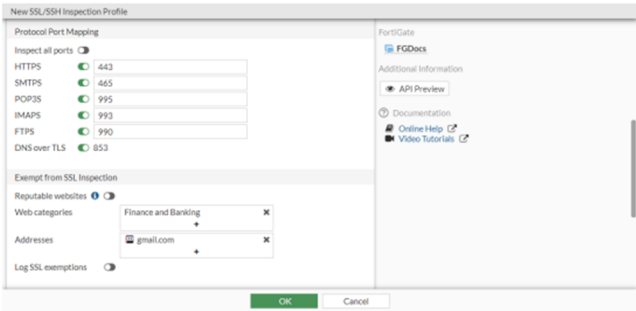
	<p>Vale ressaltar que a solução de IPS já faz uma decodificação de protocolo, ou seja, ela já faz a validação de anomalia de protocolo, caso este esteja com algum problema, ele é então descartado.</p> <p>Já o mecanismo de controle de aplicação é feito pelo Application Control.</p> 
<p><b>Comentário</b></p>	<p>Fonte: “How does the IPS engine determine if a packet contains an attack or anomaly” acessado em <a href="https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-does-the-IPS-engine-determine-if-a-packet/ta-p/199692">https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-does-the-IPS-engine-determine-if-a-packet/ta-p/199692</a></p>

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

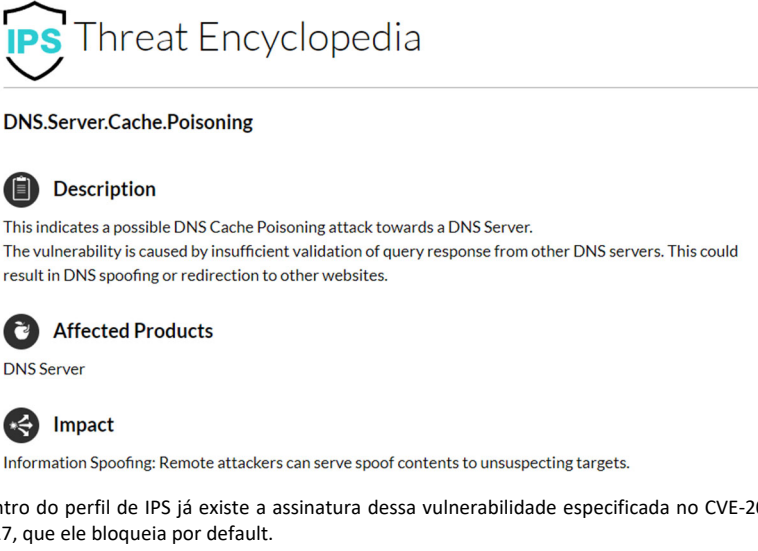
<p><b>Item de Teste - 5.3.7.4</b></p>	<p>Possuir proteções de segurança, informações como: código CVE, severidade, e tipo de ação que a mesma irá executar;</p>
---------------------------------------	---



<b>Objetivo do Teste</b>	Verificar se o sistema de proteção de segurança possui as informações de código CVE, severidade, e tipo de ação que a mesma irá executar;																																																						
<b>Configuração do Teste</b>	Demonstrar lista de assinaturas e suas características																																																						
<b>Procedimento do Teste</b>	Demonstrar lista de assinaturas e suas características																																																						
<b>Evidências</b>	<p>Podemos ver na imagem abaixo retirada de um perfil de IPS do FortiGate, que ele apresenta as seguintes informações:</p> <p>Grau de Severidade, Ação a ser tomada e como também o código CVE daquela vulnerabilidade.</p> <table border="1"> <tr> <td>3Com.3CDaemon.FTP.Server.Buffer.Over...</td> <td>■■■■■</td> <td>Server</td> <td>Windows</td> <td>⊘ Block</td> <td>CVE-2005-0277</td> </tr> <tr> <td>3Com.3CDaemon.FTP.Server.Information...</td> <td>■■■■■</td> <td>Client</td> <td>Windows</td> <td>✔ Pass</td> <td>CVE-2005-0278</td> </tr> <tr> <td>3Com.Intelligent.Management.Center.Info...</td> <td>■■■■■</td> <td>Server</td> <td>Windows</td> <td>⊘ Block</td> <td></td> </tr> <tr> <td>3Com.OfficeConnect.ADSL.Wireless.Fire...</td> <td>■■■■■</td> <td>Server</td> <td>Linux</td> <td>⊘ Block</td> <td></td> </tr> <tr> <td>3S.Pocket.VMS.ActiveX.Control.Buffer.O...</td> <td>■■■■■</td> <td>Client</td> <td>Windows</td> <td>⊘ Block</td> <td>CVE-2014-9263</td> </tr> <tr> <td>3ivx.MPEG4.File.Processing.Buffer.Overfl...</td> <td>■■■■■</td> <td>Client</td> <td>Windows</td> <td>⊘ Block</td> <td>CVE-2007-6401</td> </tr> <tr> <td>427BB.Cookie.Based.Authentication.Bypass</td> <td>■■■■■</td> <td>Server</td> <td>Other</td> <td>⊘ Block</td> <td>CVE-2006-0153</td> </tr> <tr> <td>427BB.Showthread.PHP.ForumID.Parame...</td> <td>■■■■■</td> <td>Server</td> <td>Other</td> <td>⊘ Block</td> <td>CVE-2006-0154</td> </tr> <tr> <td>A32S.Botnet</td> <td>■■■■■</td> <td>Server Client</td> <td>All</td> <td>⊘ Block</td> <td></td> </tr> </table>	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.Pocket.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	
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.Pocket.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																																																			
<b>Comentário</b>																																																							

<b>Item de Teste - 5.3.7.18</b>	A solução deve possuir inspeção de tráfego HTTPS sendo possível criar bypass para sites evitando qualquer tipo de quebra de sigilo de informações pessoais;
<b>Objetivo do Teste</b>	Verificar se a solução possui uma forma de dar bypass na inspeção de tráfego HTTPS.
<b>Configuração do Teste</b>	Demonstrar by-pass de https
<b>Procedimento do Teste</b>	Demonstrar by-pass de https
<b>Evidências</b>	<p><b>Exempt web sites from deep inspection</b></p> <p>If you do not want to apply deep inspection for privacy or other reasons, you can exempt the session by address, category, or allowlist.</p> <p>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.</p> <p>If you want to exempt all bank web sites, an easy way is to exempt the <i>Finance and Banking</i> category, which includes all finance and bank web sites identified in FortiGuard. For information about creating and using custom local and remote categories, see <a href="#">Web rating override on page 1419</a> and <a href="#">Threat feeds on page 2693</a>.</p>  <p>If you want to exempt commonly trusted web sites, you can bypass the SSL allowlist in the SSL/SSH profile by enabling <i>Reputable websites</i>. The allowlist includes common web sites trusted by FortiGuard.</p> <p>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.</p>

	<p><b>Exempt from SSL Inspection</b></p> <p>Reputable websites <input type="checkbox"/></p> <p>Web categories</p> <ul style="list-style-type: none"> <li>Finance and Banking <input checked="" type="checkbox"/></li> <li>Health and Wellness <input checked="" type="checkbox"/></li> <li>Personal Privacy <input checked="" type="checkbox"/></li> <li style="text-align: center;">+</li> </ul> <p>Addresses <input type="text" value=""/></p> <p>Log SSL exemptions <input type="checkbox"/></p> <p><b>SSH Inspection Options</b></p> <p>SSH deep scan <input type="checkbox"/></p>
<p><b>Comentário</b></p>	<p>Fonte: FortiOS Administration Guide acessado em <a href="https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a06117ca-5fbf-11ed-96f0-fa163e15d75b/FortiOS-7.2.3-Administration_Guide.pdf">https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a06117ca-5fbf-11ed-96f0-fa163e15d75b/FortiOS-7.2.3-Administration_Guide.pdf</a></p>

<p><b>Item de Teste - 5.3.7.22</b></p>	<p>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;</p>
<p><b>Objetivo do Teste</b></p>	<p>Verificar se a solução protege contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning), e impedir que os usuários acessem endereços de domínios bloqueados ou maliciosos.</p>
<p><b>Configuração do Teste</b></p>	<p>Demonstrar assinatura DNS.Server.Cache.Poisoning</p>
<p><b>Procedimento do Teste</b></p>	<p>Demonstrar assinatura DNS.Server.Cache.Poisoning</p>
<p><b>Evidências</b></p>	 <p><b>IPS Threat Encyclopedia</b></p> <p><b>DNS.Server.Cache.Poisoning</b></p> <p><b>Description</b></p> <p>This indicates a possible DNS Cache Poisoning attack towards a DNS Server. The vulnerability is caused by insufficient validation of query response from other DNS servers. This could result in DNS spoofing or redirection to other websites.</p> <p><b>Affected Products</b></p> <p>DNS Server</p> <p><b>Impact</b></p> <p>Information Spoofing: Remote attackers can serve spoof contents to unsuspecting targets.</p> <p>Dentro do perfil de IPS já existe a assinatura dessa vulnerabilidade especificada no CVE-2005-0817, que ele bloqueia por default.</p>



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

5.3.8 ANTI-MALWARE:

Item de Teste - 5.3.8.1	Possuir módulo de Antivírus, Antispyware e Antibot integrado no próprio appliance de segurança e integrado à gerência centralizada de administração, monitoração e logs;
Objetivo do Teste	Verificar se a solução possui módulo de Antivírus, Antispyware e Antibot integrado no próprio appliance de segurança e integrado à gerência centralizada de administração, monitoração e logs;
Configuração do Teste	Demonstrar regra com funcionalidades: Antivírus, Antispyware e Antibot
Procedimento do Teste	Demonstrar regra com funcionalidades: Antivírus, Antispyware e Antibot
Evidências	<p>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.</p> <p>Para isso, basta ir na aba de de “Security Profiles” e lá estará os perfis de Antivírus e IPS.</p>





### Edit AntiVirus Profile

HTTP	<input checked="" type="checkbox"/>
SMTP	<input checked="" type="checkbox"/>
POP3	<input checked="" type="checkbox"/>
IMAP	<input checked="" type="checkbox"/>
FTP	<input checked="" type="checkbox"/>
CIFS	<input type="checkbox"/>

#### APT Protection Options

Treat Windows Executables in Email Attachments as Viruses	<input checked="" type="checkbox"/>
Use FortiSandbox Database	<input type="checkbox"/>
Include Mobile Malware Protection	<input checked="" type="checkbox"/>
Quarantine	<input type="checkbox"/>
Send files to FortiSandbox for inspection	<input checked="" type="checkbox"/>

Scan strategy

File types

Do not submit files types and name patterns included in

Send files to FortiNDR for inspection

Inline **Post Transfer**

Suspicious Files Only **All Supported Files**

Click to select

Send files to FortiNDR for inspection

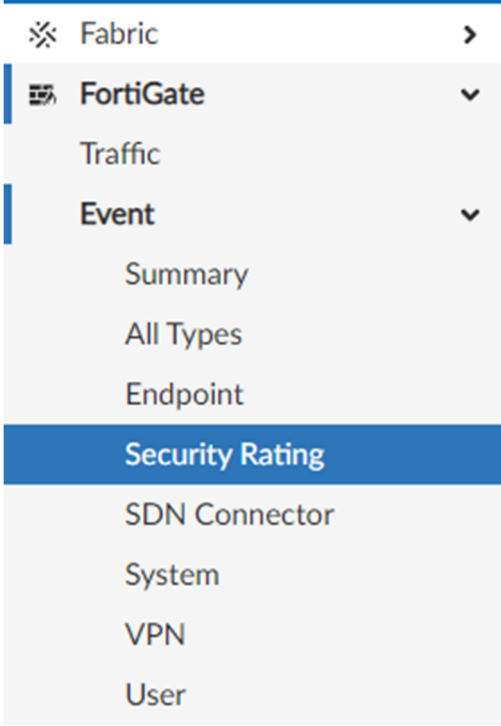
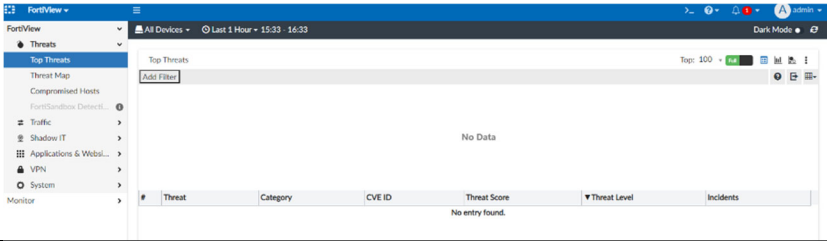
### Botnet C&C

Scan Outgoing Connections to Botnet Sites

**Block** Disable Monitor

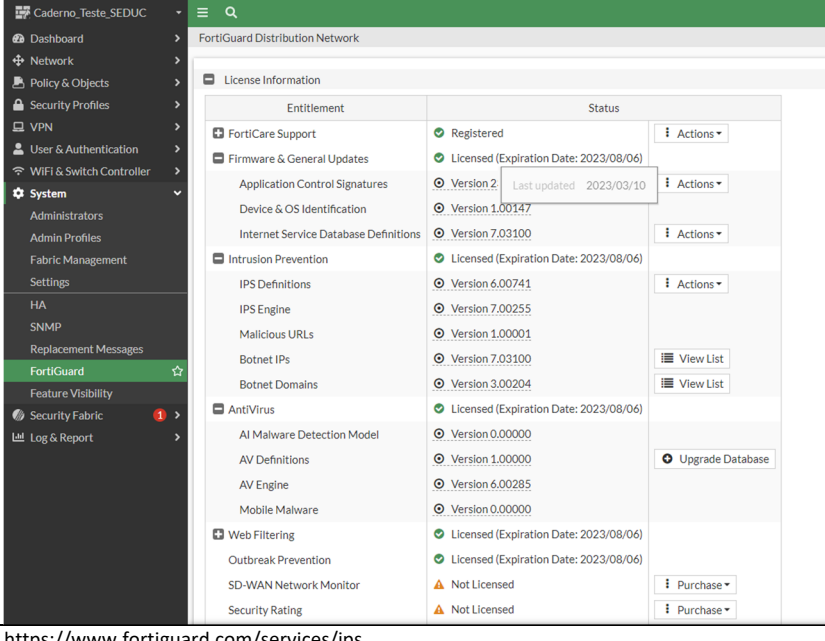
Na parte de logs podemos ver na seguinte forma:

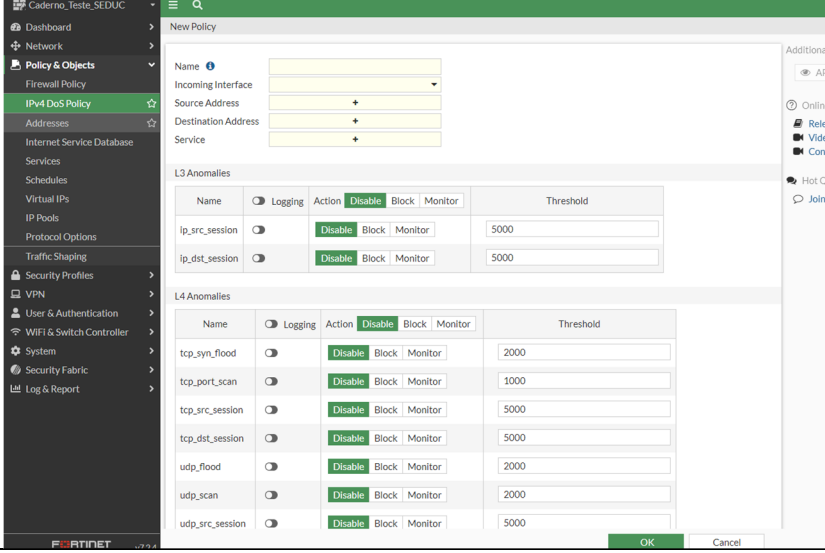


	 <p>E na de monitoração:</p> 
<b>Comentário</b>	

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



<p><b>Evidências</b></p>	
<p><b>Comentário</b></p>	<p><a href="https://www.fortiguard.com/services/ips">https://www.fortiguard.com/services/ips</a></p>

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

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

[www.nct.com.br](http://www.nct.com.br)



<b>Item de Teste - 5.3.8.6</b>	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;																																																																												
<b>Objetivo do Teste</b>	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;																																																																												
<b>Configuração do Teste</b>	Demonstrar regra NGFW																																																																												
<b>Procedimento do Teste</b>	Demonstrar regra NGFW																																																																												
<b>Evidências</b>	<p>A solução de Antibot feita pelo IPS Filter, consiste em reputação de endereços IP, com descrição do protocolo e a porta utilizada.</p> <div data-bbox="518 656 1348 1227"><p>Botnet C&amp;C IP Definitions <span style="float: right;">x</span></p><p>Search <input type="text"/> <input type="button" value="Q"/></p><table border="1"><thead><tr><th>IP</th><th>Port</th><th>Protocol</th><th>Name</th></tr></thead><tbody><tr><td>1.9.167.36</td><td>60.489</td><td>TCP</td><td>KillNet</td></tr><tr><td>1.10.189.133</td><td>50.855</td><td>TCP</td><td>KillNet</td></tr><tr><td>1.20.96.156</td><td>4.153</td><td>TCP</td><td>KillNet</td></tr><tr><td>1.20.97.181</td><td>34.102</td><td>TCP</td><td>KillNet</td></tr><tr><td>1.20.100.45</td><td>43.943</td><td>TCP</td><td>KillNet</td></tr><tr><td>1.20.100.111</td><td>41.480</td><td>TCP</td><td>KillNet</td></tr><tr><td>1.53.137.92</td><td>4.145</td><td>TCP</td><td>KillNet</td></tr><tr><td>1.62.2.147</td><td>18.186</td><td>TCP</td><td>KillNet</td></tr><tr><td>1.123.37.68</td><td>80</td><td>TCP</td><td>NanoCore</td></tr><tr><td>1.168.31.173</td><td>8.088</td><td>TCP</td><td>KillNet</td></tr><tr><td>1.169.224.221</td><td>16.464</td><td>UDP</td><td>ZeroAccess</td></tr><tr><td>1.169.224.228</td><td>16.464</td><td>UDP</td><td>ZeroAccess</td></tr><tr><td>1.171.19.54</td><td>3.128</td><td>TCP</td><td>KillNet</td></tr><tr><td>1.171.145.107</td><td>16.471</td><td>UDP</td><td>ZeroAccess</td></tr><tr><td>1.171.207.238</td><td>16.464</td><td>UDP</td><td>ZeroAccess</td></tr><tr><td>1.171.223.174</td><td>16.464</td><td>UDP</td><td>ZeroAccess</td></tr><tr><td>1.174.132.214</td><td>16.464</td><td>UDP</td><td>ZeroAccess</td></tr><tr><td>1.174.163.191</td><td>16.464</td><td>UDP</td><td>ZeroAccess</td></tr></tbody></table></div> <p>Já a parte de detecção de endereços DNS e URLs é feita pelo DNS Filter.</p>	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
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																																																																										



Botnet C&C Domain Definitions

Search

FQDN	Name
moduleconnector.at	Netwire
fonades.com	Ramnit
briancrabs.cm	Tofsee
defeatwax.ru	Tofsee
hugersl.com	Tofsee
lakeflex.ru	Tofsee
lazystax.ru	Tofsee
mubrikych.top	Tofsee
ovicrush.cn	Tofsee
oxyfx.xyz	Tofsee
parubey.info	Tofsee
quadol.ru	Tofsee
boombom.at	Gameover-zeus
donios.at	Gameover-zeus
doplertool.com	Gameover-zeus
hipohook.cn	Gameover-zeus
lujdhsndjfsk.com	Gameover-zeus
karlor.at	Gameover-zeus
liloptyp.at	Gameover-zeus

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

New Policy

Name

Incoming Interface

Outgoing Interface

Source

Destination

Schedule

Service

Action  ACCEPT  DENY

Firewall/Network Options

NAT

IP Pool Configuration  Use Outgoing Interface Address  Use Dynamic IP Pool

Preserve Source Port

Protocol Options

Security Profiles

AntiVirus

Web Filter

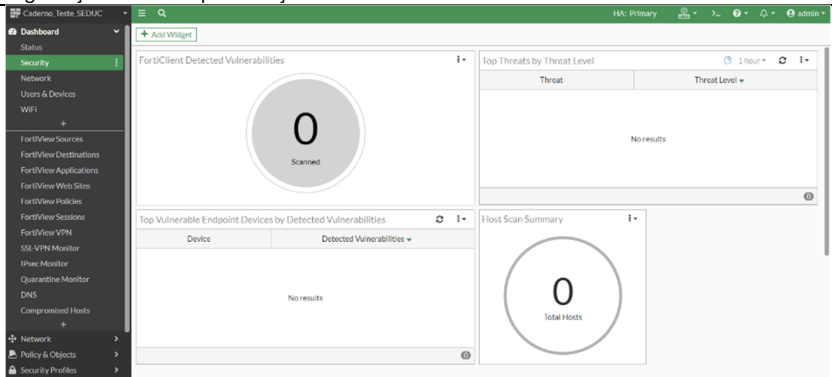
DNS Filter

Application Control

IPS

File Filter

Comentário

<b>Item de Teste - 5.3.8.9</b>	A solução deve possuir na própria interface de gerência, gráfico contendo informações em tempo real sobre as atividades recentes de malwares detectados na solução;
<b>Objetivo do Teste</b>	Verificar se a solução possui na própria interface de gerência gráfico contendo informações em tempo real sobre as atividades recentes de malwares detectados na solução;
<b>Configuração do Teste</b>	Demonstrar dashboards de detecção de malwares
<b>Procedimento do Teste</b>	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.
<b>Evidências</b>	 <p>The screenshot shows the FortiGate Security Dashboard. The 'FortiClient Detected Vulnerabilities' widget displays a large '0' and 'Scanned'. The 'Top Threats by Threat Level' widget shows 'No results'. The 'Top Vulnerable Endpoint Devices by Detected Vulnerabilities' widget also shows 'No results'. The 'Host Scan Summary' widget displays a large '0' and 'Total Hosts'.</p>
<b>Comentário</b>	

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



Comentário	<p>Edit DNS Filter Profile</p> <p>Name: default</p> <p>Comments: Default dns filtering. 22/255</p> <p>Redirect botnet C&amp;C requests to Block Portal: <input checked="" type="checkbox"/></p> <p>Enforce 'Safe Search' on Google, Bing, YouTube: <input type="checkbox"/></p> <p><input checked="" type="checkbox"/> FortiGuard Category Based Filter</p> <p>Pre-configured filters: Custom G PG-13 <b>R</b></p> <table border="1"><tr><td><input checked="" type="checkbox"/> Allow</td><td><input type="checkbox"/> Monitor</td><td><input checked="" type="checkbox"/> Redirect to Block Portal</td></tr><tr><th>Name</th><th>Action</th></tr><tr><td>Secondary Unwanted Program</td><td><input checked="" type="checkbox"/> Allow</td></tr><tr><td><b>Security Risk 6</b>   <input checked="" type="checkbox"/> 6</td><td></td></tr><tr><td>Malicious Websites</td><td><input checked="" type="checkbox"/> Redirect to Bloc...</td></tr><tr><td>Phishing</td><td><input checked="" type="checkbox"/> Redirect to Bloc...</td></tr><tr><td>Spam URLs</td><td><input checked="" type="checkbox"/> Redirect to Bloc...</td></tr><tr><td>Dynamic DNS</td><td><input checked="" type="checkbox"/> Redirect to Bloc...</td></tr><tr><td>Newly Observed Domain</td><td><input checked="" type="checkbox"/> Redirect to Bloc...</td></tr><tr><td>Newly Registered Domain</td><td><input checked="" type="checkbox"/> Redirect to Bloc...</td></tr><tr><td><b>Unrated 1</b>   <input checked="" type="checkbox"/> 1</td><td></td></tr><tr><td>Unrated</td><td><input checked="" type="checkbox"/> Allow</td></tr></table>	<input checked="" type="checkbox"/> Allow	<input type="checkbox"/> Monitor	<input checked="" type="checkbox"/> Redirect to Block Portal	Name	Action	Secondary Unwanted Program	<input checked="" type="checkbox"/> Allow	<b>Security Risk 6</b>   <input checked="" type="checkbox"/> 6		Malicious Websites	<input checked="" type="checkbox"/> Redirect to Bloc...	Phishing	<input checked="" type="checkbox"/> Redirect to Bloc...	Spam URLs	<input checked="" type="checkbox"/> Redirect to Bloc...	Dynamic DNS	<input checked="" type="checkbox"/> Redirect to Bloc...	Newly Observed Domain	<input checked="" type="checkbox"/> Redirect to Bloc...	Newly Registered Domain	<input checked="" type="checkbox"/> Redirect to Bloc...	<b>Unrated 1</b>   <input checked="" type="checkbox"/> 1		Unrated	<input checked="" type="checkbox"/> Allow
	<input checked="" type="checkbox"/> Allow	<input type="checkbox"/> Monitor	<input checked="" type="checkbox"/> Redirect to Block Portal																							
Name	Action																									
Secondary Unwanted Program	<input checked="" type="checkbox"/> Allow																									
<b>Security Risk 6</b>   <input checked="" type="checkbox"/> 6																										
Malicious Websites	<input checked="" type="checkbox"/> Redirect to Bloc...																									
Phishing	<input checked="" type="checkbox"/> Redirect to Bloc...																									
Spam URLs	<input checked="" type="checkbox"/> Redirect to Bloc...																									
Dynamic DNS	<input checked="" type="checkbox"/> Redirect to Bloc...																									
Newly Observed Domain	<input checked="" type="checkbox"/> Redirect to Bloc...																									
Newly Registered Domain	<input checked="" type="checkbox"/> Redirect to Bloc...																									
<b>Unrated 1</b>   <input checked="" type="checkbox"/> 1																										
Unrated	<input checked="" type="checkbox"/> Allow																									

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 <b>Policy &amp; Objects &gt; Firewall Policy &gt; Security Profiles</b> e no campo SSL Inspection selecionar Deep-Inspection, no fluxo da política selecionada o firewall irá realizar a inspeção de pacotes.



<b>Evidências</b>	<p><b>Security Profiles</b></p> <p>AntiVirus <input type="radio"/></p> <p>Web Filter <input type="radio"/></p> <p>DNS Filter <input type="radio"/></p> <p>Application Control <input type="radio"/></p> <p>IPS <input type="radio"/></p> <p>File Filter <input type="radio"/></p> <p><b>SSL Inspection</b> <span style="color: yellow;">⚠</span> <span style="border: 1px solid gray; padding: 2px;">SSL deep-inspection</span></p> <p>Decrypted Traffic Mirror <input type="radio"/></p> <hr/> <p><b>Edit SSL/SSH Inspection Profile</b></p> <p>SSL Inspection Options</p> <p>Enable SSL inspection of <span style="border: 1px solid green; padding: 2px;">Multiple Clients Connecting to Multiple Servers</span></p> <p>Inspection method <span style="border: 1px solid green; padding: 2px;">Protecting SSL Server</span></p> <p>CA certificate <span style="color: yellow;">⚠</span> <span style="border: 1px solid gray; padding: 2px;">Fortinet_CA_SSL</span> <span style="font-size: small;">Download</span></p> <p>Blocked certificates <span style="font-size: small;">i</span> <span style="border: 1px solid green; padding: 2px;">Allow</span> <span style="border: 1px solid green; padding: 2px;">Block</span> <span style="font-size: small;">View Blocked Certificates</span></p> <p>Untrusted SSL certificates <span style="border: 1px solid green; padding: 2px;">Allow</span> <span style="border: 1px solid green; padding: 2px;">Block</span> <span style="border: 1px solid green; padding: 2px;">Ignore</span> <span style="font-size: small;">View Trusted CAs List</span></p> <p>Server certificate SNI check <span style="font-size: small;">i</span> <span style="border: 1px solid green; padding: 2px;">Enable</span> <span style="border: 1px solid green; padding: 2px;">Strict</span> <span style="border: 1px solid green; padding: 2px;">Disable</span></p> <p>Enforce SSL cipher compliance <input type="radio"/></p> <p>Enforce SSL negotiation compliance <input type="radio"/></p> <p>RPC over HTTPS <input type="radio"/></p> <hr/> <p><b>Protocol Port Mapping</b></p> <p>Inspect all ports <input type="radio"/></p> <p>HTTPS <input checked="" type="radio"/> 443</p> <p>SMTPS <input checked="" type="radio"/> 465</p> <p>POP3S <input checked="" type="radio"/> 995</p> <p>IMAPS <input checked="" type="radio"/> 993</p> <p>FTPS <input checked="" type="radio"/> 990</p> <p>DNS over TLS <input type="radio"/> 853</p> <hr/> <p><b>Exempt from SSL Inspection</b></p> <p>Reputable websites <span style="font-size: small;">i</span> <input type="radio"/></p> <p>Web categories <span style="border: 1px solid gray; padding: 2px;">Finance and Banking</span> <span style="float: right;">✕</span> <span style="border: 1px solid gray; padding: 2px;">Health and Wellness</span> <span style="float: right;">✕</span> <span style="float: right;">+</span></p> <p>Addresses <span style="border: 1px solid gray; padding: 2px;">adobe</span> <span style="float: right;">✕</span> <span style="border: 1px solid gray; padding: 2px;">Adobe Login</span> <span style="float: right;">✕</span></p> <p style="text-align: right;"><span style="border: 1px solid gray; padding: 2px;">Return</span></p>
<b>Comentário</b>	

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

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

[www.nct.com.br](http://www.nct.com.br)



segunda forma é utilizando SSL Deep Inspection onde é possível realizar a inspeção de protocolos seguros.

**Evidências**

The screenshot displays the FortiGate configuration interface. On the left is a navigation menu with categories like Dashboard, Network, Policy & Objects, Security Profiles, AntiVirus, Web Filter, DNS Filter, Application Control, File Filter, SSL/SSH Inspection, Application Signatures, Web Rating Overrides, Web Profile Overrides, VPN, User & Authentication, WIFI & Switch Controller, System, Security Fabric, and Log & Report. The main area shows the configuration for a 'New AntiVirus Profile' named 'SEDUC\_AV'. The 'AntiVirus scan' is set to 'Block'. Under 'Inspected Protocols', HTTP, SMTP, POP3, IMAP, FTP, and CIFS are all checked. Under 'APT Protection Options', 'Treat Windows executables in email attachments as viruses' is unchecked, 'Send files to FortiSandbox for inspection' is unchecked, 'Include mobile malware protection' is checked, and 'Quarantine' is unchecked. Under 'Virus Outbreak Prevention', 'Use FortiGuard outbreak prevention database', 'Use external malware block list', and 'Use EMS threat feed' are all unchecked. Below this, the 'Security Profiles' section lists various security features with toggle switches: AntiVirus, Web Filter, DNS Filter, Application Control, IPS, File Filter, SSL Inspection (highlighted in yellow), and Decrypted Traffic Mirror. The 'SSL Inspection' dropdown menu is set to 'deep-inspection'.



<p><b>Comentário</b></p>	<p>Edit SSL/SSH Inspection Profile</p> <p>SSL Inspection Options</p> <p>Enable SSL inspection of <b>Multiple Clients Connecting to Multiple Servers</b> Protecting SSL Server</p> <p>Inspection method <b>SSL Certificate Inspection</b> <b>Full SSL Inspection</b></p> <p>CA certificate  Fortinet_CA_SSL  Download</p> <p>Blocked certificates  <b>Allow</b> <b>Block</b>  View Blocked Certificates</p> <p>Untrusted SSL certificates <b>Allow</b> <b>Block</b> <b>Ignore</b>  View Trusted CAs List</p> <p>Server certificate SNI check  <b>Enable</b> <b>Strict</b> <b>Disable</b></p> <p>Enforce SSL cipher compliance <input type="radio"/></p> <p>Enforce SSL negotiation compliance <input type="radio"/></p> <p>RPC over HTTPS <input type="radio"/></p> <p>Protocol Port Mapping</p> <p>Inspect all ports <input type="radio"/></p> <p>HTTPS <input checked="" type="radio"/> 443</p> <p>SMTPTS <input checked="" type="radio"/> 465</p> <p>POP3S <input checked="" type="radio"/> 995</p> <p>IMAPS <input checked="" type="radio"/> 993</p> <p>FTPS <input checked="" type="radio"/> 990</p> <p>DNS over TLS <input type="radio"/> 853</p> <p>Exempt from SSL Inspection</p> <p>Reputable websites  <input type="radio"/></p> <p>Web categories</p> <table border="1"> <tr><td>Finance and Banking</td><td></td></tr> <tr><td>Health and Wellness</td><td></td></tr> <tr><td colspan="2" style="text-align: center;">+</td></tr> </table> <p>Addresses</p> <table border="1"> <tr><td>adobe</td><td></td></tr> <tr><td>Adobe Login</td><td></td></tr> </table> <p style="text-align: right;"><a href="#">Return</a></p>	Finance and Banking		Health and Wellness		+		adobe		Adobe Login	
Finance and Banking											
Health and Wellness											
+											
adobe											
Adobe Login											

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



	<div style="border: 1px solid #ccc; padding: 10px;"> <h3>Edit AntiVirus Profile</h3> <p>Name <input type="text" value="default"/></p> <p>Comments <input type="text" value="Scan files and block viruses."/> 29/255</p> <p>AntiVirus scan <span style="color: blue;">i</span> <input type="checkbox"/></p> <hr/> <h4>Inspected Protocols</h4> <p>HTTP <input type="checkbox"/></p> <p>SMTP <input type="checkbox"/></p> <p>POP3 <input type="checkbox"/></p> <p>IMAP <input type="checkbox"/></p> <p>FTP <input type="checkbox"/></p> <p>CIFS <input type="checkbox"/></p> <hr/> <h4>APT Protection Options</h4> <p>Treat Windows executables in email attachments as viruses <span style="color: blue;">i</span> <input type="checkbox"/></p> <p>Send files to FortiSandbox for inspection <span style="color: blue;">i</span> <span style="color: orange;">⚠</span> <input type="checkbox"/></p> <p>Include mobile malware protection <input checked="" type="checkbox"/></p> <p>Quarantine <span style="color: blue;">i</span> <input type="checkbox"/></p> <hr/> <h4>Virus Outbreak Prevention <span style="color: blue;">i</span></h4> <p>Use FortiGuard outbreak prevention database <input type="checkbox"/></p> <p>Use external malware block list <input type="checkbox"/></p> <p>Use EMS threat feed <span style="color: blue;">i</span> <input type="checkbox"/></p> <hr/> <h4>External malware block list</h4> <p>The external malware block list allows users to add their own malware signatures in the form of MD5, SHA1, and SHA256 hashes. The FortiGate's antivirus database retrieves an external malware hash list from a remote server and polls the hash list every <i>n</i> minutes for updates. Enabling the AV engine scan is not required to use this feature.</p> <p>The external malware block list can be used in both proxy-based and flow-based policy inspections, but it is not supported in AV quick scan mode.</p> <p>Note that using different types of hashes simultaneously may slow down the performance of malware scanning. It is recommended to use one type of hash.</p> </div>
<b>Comentário</b>	<a href="https://docs.fortinet.com/document/fortigate/7.2.0/administration-guide/254346">https://docs.fortinet.com/document/fortigate/7.2.0/administration-guide/254346</a>

### 5.3.9 AMEAÇAS AVANÇADAS PERSISTENTES - APT:

<b>Item de Teste - 5.3.9.1</b>	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;
<b>Objetivo do Teste</b>	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.
<b>Configuração do Teste</b>	Realizar uma inspeção de tráfego de malwares.



<b>Procedimento do Teste</b>	<p>Primeiro é necessário configurar a funcionalidade “FortiGate Cloud Sandbox” no FortiGate.</p> <p>Após realizar as configurações para habilitar o Sandbox basta navegar por Security Profiles &gt; AntiVirus &gt; Create New &gt; APT Protection Options e habilitar o envio de arquivos para a inspeção do Sandbox.</p> <p>Por último basta incluir o perfil criado no fluxo da política em que deseja realizar a inspeção.</p>
------------------------------	--

7.2.4 ↓

Copy Link

Download PDF

## Configuring sandboxing

The Security Fabric supports the following FortiSandbox deployments.

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

7.2.4 ↓

Copy Link

Download PDF

## Using FortiSandbox post-transfer scanning with antivirus

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

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

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

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

To enable FortiSandbox inspection in an antivirus profile:

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



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

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



Evidências

The screenshot displays the Fortinet FortiGate GUI. On the left is a navigation menu with categories like Dashboard, Network, Policy & Objects, and Security Profiles. The main area is titled 'New Policy' and contains several configuration sections: 'Name', 'Outgoing Interface', 'Source', 'Destination', 'Schedule' (set to 'always'), 'Service', and 'Action' (set to 'ACCEPT'). Below this is the 'Firewall/Network Options' section, including 'NAT', 'IP Pool Configuration', 'Preserve Source Port', and 'Protocol Options'. The 'Security Profiles' section lists various filters: AntiVirus, Web Filter, DNS Filter, Application Control, IPS, File Filter, and SSL Inspection (set to 'deep-inspection'). At the bottom, a 'Security Profiles' summary shows all filters disabled except for 'SSL Inspection', which is highlighted in yellow and set to 'deep-inspection'. A 'Decrypted Traffic Mirror' toggle is also visible.



	<p>Edit SSL/SSH Inspection Profile</p> <p>SSL Inspection Options</p> <p>Enable SSL inspection of <b>Multiple Clients Connecting to Multiple Servers</b> Protecting SSL Server</p> <p>Inspection method <b>SSL Certificate Inspection</b> <b>Full SSL Inspection</b></p> <p>CA certificate  Fortinet_CA_SSL  Download</p> <p>Blocked certificates  <b>Allow</b> <b>Block</b>  View Blocked Certificates</p> <p>Untrusted SSL certificates <b>Allow</b> <b>Block</b> <b>Ignore</b>  View Trusted CAs List</p> <p>Server certificate SNI check  <b>Enable</b> <b>Strict</b> <b>Disable</b></p> <p>Enforce SSL cipher compliance <input type="radio"/></p> <p>Enforce SSL negotiation compliance <input type="radio"/></p> <p>RPC over HTTPS <input type="radio"/></p> <p>Protocol Port Mapping</p> <p>Inspect all ports <input type="radio"/></p> <p>HTTPS <input checked="" type="radio"/> 443</p> <p>SMTPTS <input checked="" type="radio"/> 465</p> <p>POP3S <input checked="" type="radio"/> 995</p> <p>IMAPS <input checked="" type="radio"/> 993</p> <p>FTPS <input checked="" type="radio"/> 990</p> <p>DNS over TLS <input type="radio"/> 853</p> <p>Exempt from SSL Inspection</p> <p>Reputable websites  <input type="radio"/></p> <p>Web categories</p> <table border="1"> <tr><td>Finance and Banking</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Health and Wellness</td><td><input checked="" type="checkbox"/></td></tr> <tr><td colspan="2" style="text-align: center;">+</td></tr> </table> <p>Addresses</p> <table border="1"> <tr><td>adobe</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Adobe Login</td><td><input checked="" type="checkbox"/></td></tr> </table> <p style="text-align: right;"><a href="#">Return</a></p>	Finance and Banking	<input checked="" type="checkbox"/>	Health and Wellness	<input checked="" type="checkbox"/>	+		adobe	<input checked="" type="checkbox"/>	Adobe Login	<input checked="" type="checkbox"/>
Finance and Banking	<input checked="" type="checkbox"/>										
Health and Wellness	<input checked="" type="checkbox"/>										
+											
adobe	<input checked="" type="checkbox"/>										
Adobe Login	<input checked="" type="checkbox"/>										
<b>Comentário</b>											

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





<p><b>Evidências</b></p>	
<p><b>Comentário</b></p>	

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



	<div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;"> <p><b>APT Protection Options</b></p> <p>Treat Windows executables in email attachments as viruses <span style="float: right;">i <input type="checkbox"/></span></p> <p><b>Send files to FortiSandbox for inspection</b> <span style="float: right;">i ⚠ <input type="checkbox"/></span></p> <p>Include mobile malware protection <span style="float: right;"><input checked="" type="checkbox"/></span></p> <p>Quarantine <span style="float: right;">i <input type="checkbox"/></span></p> </div>
Comentário	

<b>Item de Teste - 5.3.9.7</b>	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;												
<b>Objetivo do Teste</b>	Demonstrar que a solução possui estrutura interna ou na nuvem do fabricante para solução Sandbox.												
<b>Configuração do Teste</b>	Demonstrar relatórios na nuvem do fabricante Fortinet.												
<b>Procedimento do Teste</b>	Demonstrar relatórios na nuvem do fabricante Fortinet.												
<b>Evidências</b>	<p>O Antivírus do FortiGate faz o envio de códigos maliciosas para o FortiGate Cloud Sandbox, um ambiente na nuvem que faz a emulação desses códigos e retorna para o FortiGate a decisão tomada</p> <p><b>Configuring Sandboxing</b></p> <p>The Security Fabric supports the following FortiSandbox deployments.</p> <table border="1" data-bbox="539 1227 1345 1619"> <thead> <tr> <th>Type</th> <th>Description</th> <th>Requirements</th> </tr> </thead> <tbody> <tr> <td>FortiGate Cloud Sandbox</td> <td>Files are sent to Fortinet's Cloud Sandbox cluster for processing.</td> <td> <ul style="list-style-type: none"> <li>The FortiGate must have a valid AV license.</li> <li>The FortiCloud account provides access to a portal to view submissions. This is not required for the Security Fabric.</li> </ul> </td> </tr> <tr> <td>FortiSandbox Cloud</td> <td>Files are sent to a dedicated FortiCloud hosted instance of FortiSandbox for processing.</td> <td> <ul style="list-style-type: none"> <li>FortiCloud premium license</li> <li>FortiSandbox Cloud entitlement</li> <li>The FortiGate and FortiCloud license are registered to the same account.</li> </ul> </td> </tr> <tr> <td>FortiSandbox appliance</td> <td>Files are sent to a physical appliance or VM, typically residing on premise, for processing.</td> <td> <ul style="list-style-type: none"> <li>None</li> </ul> </td> </tr> </tbody> </table>	Type	Description	Requirements	FortiGate Cloud Sandbox	Files are sent to Fortinet's Cloud Sandbox cluster for processing.	<ul style="list-style-type: none"> <li>The FortiGate must have a valid AV license.</li> <li>The FortiCloud account provides access to a portal to view submissions. This is not required for the Security Fabric.</li> </ul>	FortiSandbox Cloud	Files are sent to a dedicated FortiCloud hosted instance of FortiSandbox for processing.	<ul style="list-style-type: none"> <li>FortiCloud premium license</li> <li>FortiSandbox Cloud entitlement</li> <li>The FortiGate and FortiCloud license are registered to the same account.</li> </ul>	FortiSandbox appliance	Files are sent to a physical appliance or VM, typically residing on premise, for processing.	<ul style="list-style-type: none"> <li>None</li> </ul>
Type	Description	Requirements											
FortiGate Cloud Sandbox	Files are sent to Fortinet's Cloud Sandbox cluster for processing.	<ul style="list-style-type: none"> <li>The FortiGate must have a valid AV license.</li> <li>The FortiCloud account provides access to a portal to view submissions. This is not required for the Security Fabric.</li> </ul>											
FortiSandbox Cloud	Files are sent to a dedicated FortiCloud hosted instance of FortiSandbox for processing.	<ul style="list-style-type: none"> <li>FortiCloud premium license</li> <li>FortiSandbox Cloud entitlement</li> <li>The FortiGate and FortiCloud license are registered to the same account.</li> </ul>											
FortiSandbox appliance	Files are sent to a physical appliance or VM, typically residing on premise, for processing.	<ul style="list-style-type: none"> <li>None</li> </ul>											

	<div style="border: 1px solid #ccc; padding: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span>7.2.4 ↓</span> <div style="text-align: right;"> <a href="#">Copy Link</a> <a href="#">Download PDF</a> </div> </div> <h3>Using FortiSandbox post-transfer scanning with antivirus</h3> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• <i>All Supported Files</i>: all files matching the file types defined in the scan profile of the FortiSandbox are forwarded.</li> <li>• <i>Suspicious Files Only</i>: 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.</li> <li>• <i>None</i>: files are not forwarded to FortiSandbox.</li> </ul> <p>For more information, see <a href="#">Configuring sandboxing</a>.</p> <p>To enable FortiSandbox inspection in an antivirus profile:</p> <ol style="list-style-type: none"> <li>1. Go to <i>Security Profiles &gt; AntiVirus</i>.</li> <li>2. Create, edit, or clone an antivirus profile.</li> <li>3. In the <i>APT Protection Options</i> section, set <i>Send Files to FortiSandbox for Inspection</i> to either <i>Suspicious Files Only</i> or <i>All Supported</i>.</li> </ol> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <h4>APT Protection Options</h4> <div style="display: flex; justify-content: space-between; align-items: center; margin-bottom: 10px;"> <div>Treat Windows executables in email attachments as viruses</div> <div style="text-align: right;"> <span>ⓘ</span> <input type="checkbox"/> </div> </div> <div style="display: flex; justify-content: space-between; align-items: center; margin-bottom: 10px;"> <div style="background-color: yellow;">Send files to FortiSandbox for inspection</div> <div style="text-align: right;"> <span>ⓘ</span> <span>⚠</span> <input type="checkbox"/> </div> </div> <div style="display: flex; justify-content: space-between; align-items: center; margin-bottom: 10px;"> <div>Include mobile malware protection</div> <div style="text-align: right;"> <input checked="" type="checkbox"/> </div> </div> <div style="display: flex; justify-content: space-between; align-items: center;"> <div>Quarantine</div> <div style="text-align: right;"> <span>ⓘ</span> <input type="checkbox"/> </div> </div> </div> </div>
Comentário	

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

## 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.

The screenshot shows the FortiGate GUI configuration for an Antivirus profile. The profile name is AV\_SEDJC\_GO. The scan strategy is set to Post Transfer, and the file types are set to All Supported Files. The 'Send files to FortiSandbox for inspection' option is enabled. The interface also shows various other settings like Inspected Protocols (HTTP, SMTP, POP3, IMAP, FTP, CIFS) and APT Protection Options.



	<p><b>APT Protection Options</b></p> <p>Treat Windows executables in email attachments as viruses <span style="float: right;">i <input type="checkbox"/></span></p> <p><b>Send files to FortiSandbox for inspection</b> <span style="float: right;">i ⚠ <input type="checkbox"/></span></p> <p>Include mobile malware protection <span style="float: right;"><input checked="" type="checkbox"/></span></p> <p>Quarantine <span style="float: right;">i <input type="checkbox"/></span></p>
<b>Comentário</b>	<p><a href="https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/481589">https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/481589</a></p> <p><a href="https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/660221/configuring-sandboxing">https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/660221/configuring-sandboxing</a></p>

<b>Item de Teste - 5.3.9.11</b>	Toda a análise ou bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real;															
<b>Objetivo do Teste</b>	Validar que a aplicação faz a análise ou bloqueio de malwares e/ou códigos maliciosos em tempo real															
<b>Configuração do Teste</b>	Possuir 1(um) FortiGate com uma regra de firewall contendo um Perfil de Antivírus configurado.															
<b>Procedimento do Teste</b>	Demonstrar relatórios no site do Fabricante.															
<b>Evidências</b>	<p>Quando uma política é configurada para incluir um perfil de antivírus, todo o tráfego que corresponde a essa regra será submetido à filtragem desse perfil. Conseqüentemente, todo o tráfego que transita nessa regra no momento da sua aplicação será submetido a um processo de bloqueio em tempo real de malwares e códigos maliciosos.</p> <table border="1" data-bbox="523 1254 1348 1395"> <thead> <tr> <th>Name</th> <th>Source</th> <th>Destination</th> <th>Security Profiles</th> <th>Hit Count</th> </tr> </thead> <tbody> <tr> <td colspan="5">Internet_VIVO (wan1)</td> </tr> <tr> <td>Acesso_Internet</td> <td>Rede_192.168.10/24</td> <td>all</td> <td>AV: Acesso_Servidores_WEB WEB: monitor:all APP: block-high-risk SSL: certificate-inspection</td> <td>199</td> </tr> </tbody> </table>	Name	Source	Destination	Security Profiles	Hit Count	Internet_VIVO (wan1)					Acesso_Internet	Rede_192.168.10/24	all	AV: Acesso_Servidores_WEB WEB: monitor:all APP: block-high-risk SSL: certificate-inspection	199
Name	Source	Destination	Security Profiles	Hit Count												
Internet_VIVO (wan1)																
Acesso_Internet	Rede_192.168.10/24	all	AV: Acesso_Servidores_WEB WEB: monitor:all APP: block-high-risk SSL: certificate-inspection	199												
<b>Comentário</b>																

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



Evidências

1 - Criação dos objetos

Caderno\_Testes\_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

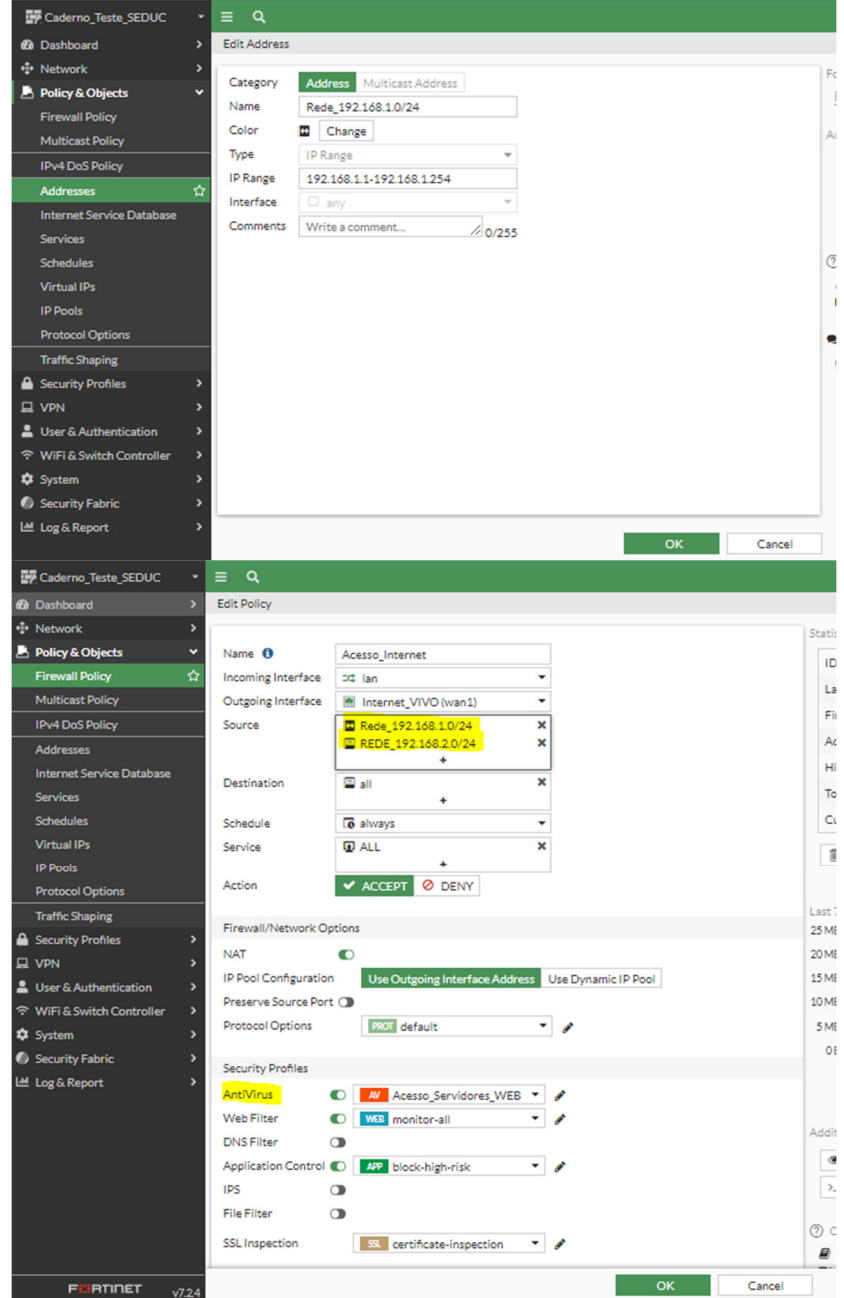
IP/Netmask: 192.168.2.0 255.255.255.0

Interface: any

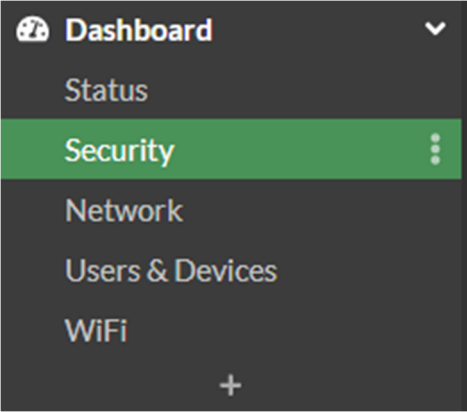
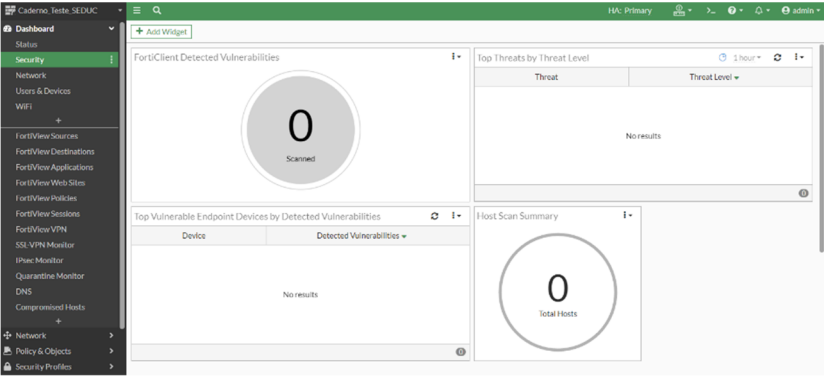

Static route configuration:

Comments: Write a comment... 0/255

OK Cancel

	 <p>The screenshot displays two windows from the FortiGate management interface. The top window is 'Edit Address' for an address named 'Rede_192.168.1.0/24'. The bottom window is 'Edit Policy' for a policy named 'Acesso_Internet'. The policy configuration includes: Incoming Interface: lan; Outgoing Interface: Internet_VIVO (wan1); Source: Rede_192.168.1.0/24 and REDE_192.168.2.0/24; Destination: all; Schedule: always; Service: ALL; Action: ACCEPT; Firewall/Network Options: NAT (disabled), IP Pool Configuration (Use Outgoing Interface Address, Use Dynamic IP Pool), Preserve Source Port (disabled), Protocol Options (PROT default); Security Profiles: AntiVirus (AV Acesso_Servidores_WEB), Web Filter (WEB monitor-all), Application Control (APP block-high-risk), IPS (disabled), File Filter (disabled), and SSL Inspection (SSL certificate-inspection).</p>
<b>Comentário</b>	<a href="https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/656084/firewall-policy#FirewallPolicyParameters">https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/656084/firewall-policy#FirewallPolicyParameters</a>


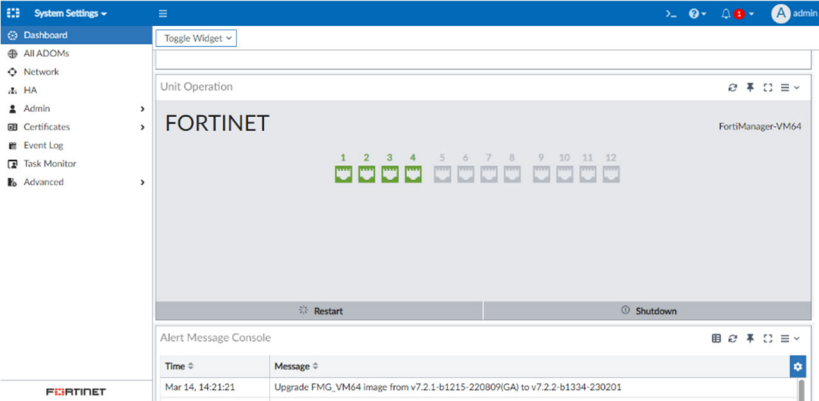
<b>Item de Teste - 5.3.9.13</b>	Implementar através da interface gráfica mecanismo de painel de controle onde seja possível a visualização de estatísticas das ameaças;
<b>Objetivo do Teste</b>	Verificar se a ferramenta possui uma interface gráfica com um painel de controle onde seja possível a visualização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

<p><b>Procedimento do Teste</b></p>	<p>Demonstrar dashboards de estatísticas de ameaças.</p>
<p><b>Evidências</b></p>	<p>Na aba "Dashboard" temos a opção de selecionar "Security".</p>  <p>Lá podemos ter acesso a diversas funcionalidades referentes a visualização de eventos de segurança detectados pela solução.</p>  <p>Em conjunto com isso temos outra aba de "Top Threats" que separa as ameaças que apareceram rede por nível de periculosidade.</p> 



Comentário	
------------	--

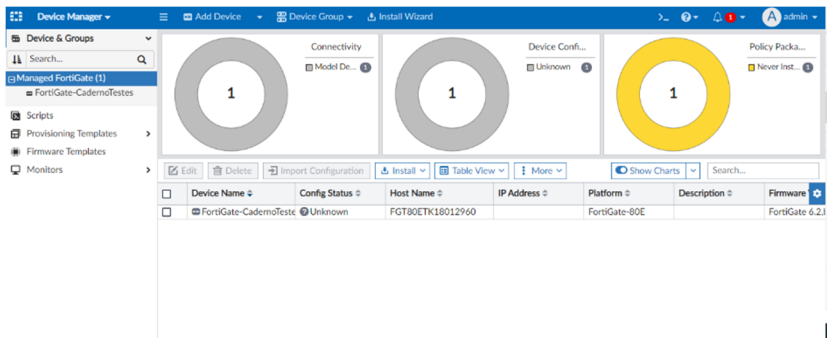
5.4 Solução de Gerenciamento e Controle do Firewall

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	 <p>The image shows a Fortinet Data Sheet for FortiManager. It features the Fortinet logo at the top, followed by 'DATA SHEET' and 'FortiManager' in large bold letters. Below this, it states 'Available in:' and shows three icons: Appliance (a server rack), Virtual Machine (a laptop), and Cloud (a cloud icon). The text describes FortiManager as providing automation-driven centralized management of Fortinet devices from a single console, enabling full administration and visibility through streamlined provisioning and innovative automation tools. It also mentions integration with the Fortinet Security Fabric advanced security architecture and automation driven network operations capabilities to secure and optimize network security.</p>  <p>The screenshot shows the FortiManager web interface. The left sidebar contains navigation options: Dashboard, All ADOMs, Network, HA, Admin, Certificates, Event Log, Task Monitor, and Advanced. The main content area displays 'Unit Operation' for 'FORTINET FortiManager-VM64'. It features a progress bar with 12 steps, all of which are completed (indicated by green checkmarks). Below the progress bar, there are buttons for 'Restart' and 'Shutdown'. At the bottom, an 'Alert Message Console' shows a message from 'Mar 14, 14:21:21' regarding an upgrade of the FMG, VM64 image from v7.2.1-b1215-220809(GA) to v7.2.2-b1334-230201.</p>



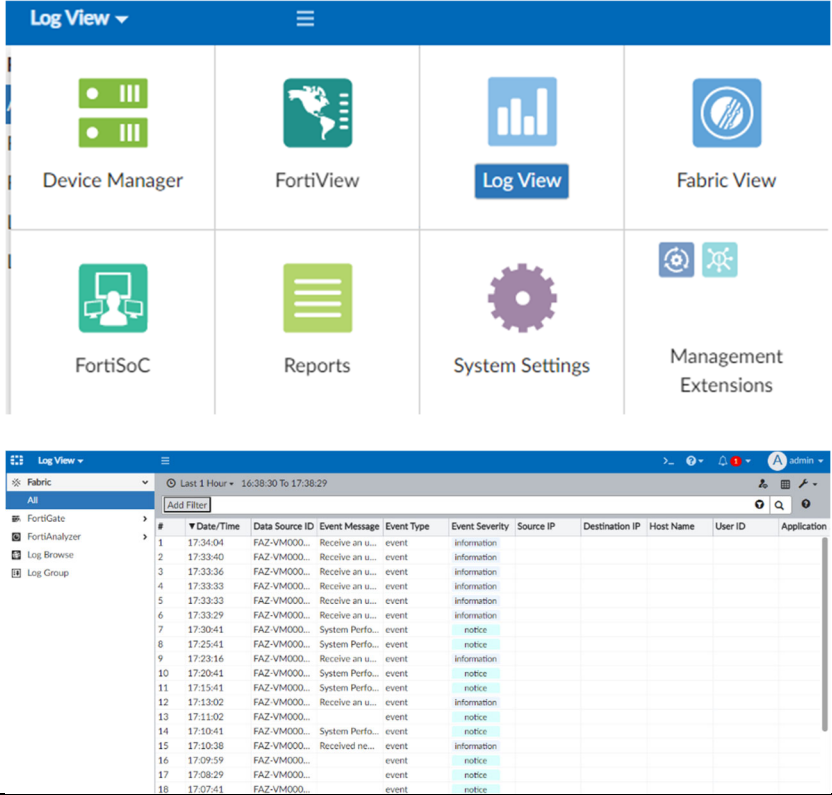
<b>Comentário</b>	Fonte: FortiManager Data Sheet acessado em <a href="https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf">https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf</a>
-------------------	--

<b>Item de Teste - 5.4.2</b>	A solução deve ser capaz de gerenciar todos os equipamentos de Segurança de forma centralizada;
<b>Objetivo do Teste</b>	Comprovar que a solução consegue gerenciar todos os equipamentos de segurança de forma centralizada.
<b>Configuração do Teste</b>	Demonstrar que o FortiManager suporta gerenciar o FG-1801F e FG-81F
<b>Procedimento do Teste</b>	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.

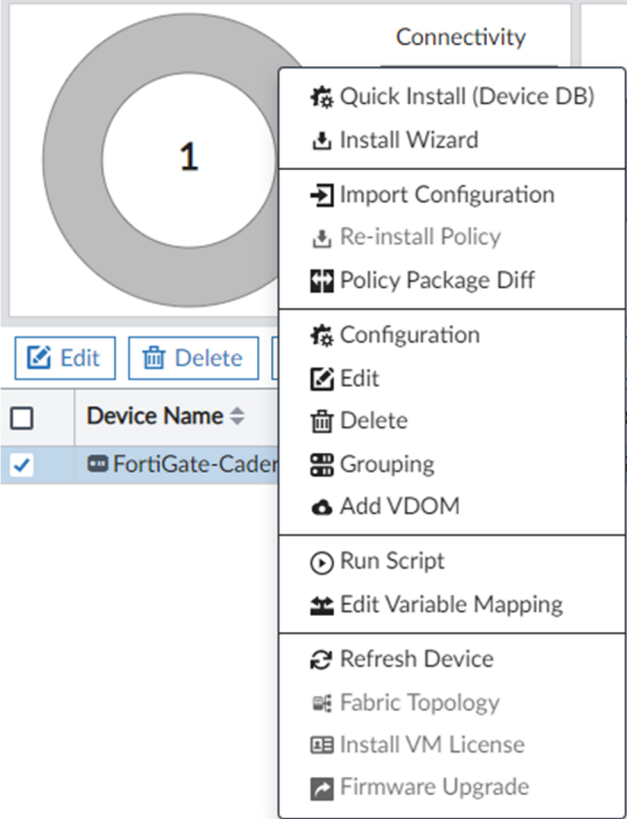
<b>Evidências</b>	 <p style="text-align: center;"><b>DATA SHEET   FortiManager</b></p> <h2 style="text-align: center;">FEATURE HIGHLIGHTS</h2> <h3 style="text-align: center;">Monitoring and Visibility</h3> <p><b>Manage and Monitor with Deep Visibility</b></p> <p>The FortiManager Device Manager provides full visibility, access, and management of Fortinet managed devices, interfaces, scripts, templates, automation, users, settings, and more. Install, edit, and delete policies. Monitor the health of FortiGate devices through customizable dashboards and widgets to see resource usage, network status of DHCP, IPsec and SSL VPN, routing, traffic shapers, and more. Easily navigate the hierarchical tree with categories for managed devices, logging devices, unauthorized devices, and customize to display as a table, folder, or a map view.</p>
-------------------	--

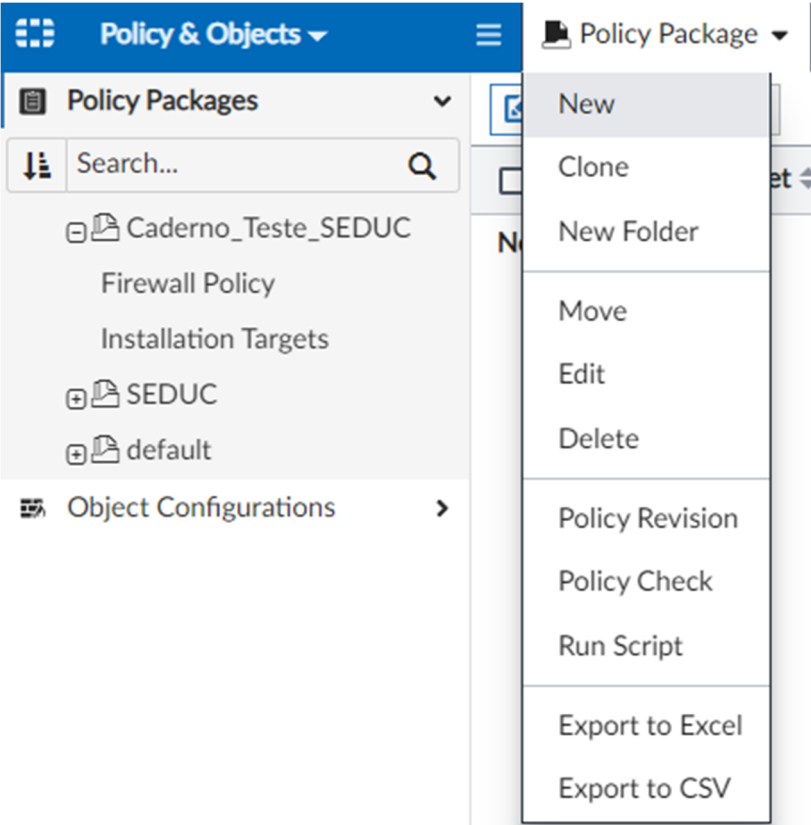


<b>Comentário</b>	Fonte: FortiManager Data Sheet acessado em <a href="https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf">https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf</a>
-------------------	--

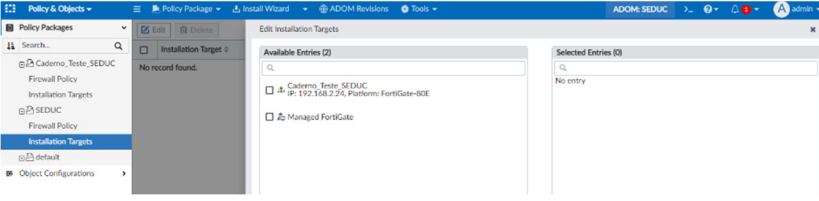
<b>Item de Teste - 5.4.3</b>	A solução deve ser responsável pela concentração dos logs e emissão de relatórios;
<b>Objetivo do Teste</b>	Comprovar que a solução é responsável pela concentração dos logs e emissão de relatórios.
<b>Configuração do Teste</b>	Acesso a um FortiAnalyzer com a conexão entre os equipamentos estabelecida.
<b>Procedimento do Teste</b>	Demonstrar configuração e ativação do FortiAnalyzer nos FortiGates.
<b>Evidências</b>	<p>Para acessar essa funcionalidade basta acessar o “Log View”.</p> 
<b>Comentário</b>	

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

<p><b>Evidências</b></p>	 <p>The screenshot shows the FortiGate web interface. A context menu is open over a device named 'FortiGate-Cader'. The menu items are:</p> <ul style="list-style-type: none"> <li>Quick Install (Device DB)</li> <li>Install Wizard</li> <li>Import Configuration</li> <li>Re-install Policy</li> <li>Policy Package Diff</li> <li>Configuration</li> <li>Edit</li> <li>Delete</li> <li>Grouping</li> <li>Add VDOM</li> <li>Run Script</li> <li>Edit Variable Mapping</li> <li>Refresh Device</li> <li>Fabric Topology</li> <li>Install VM License</li> <li>Firmware Upgrade</li> </ul> <p>Below the menu, the main dashboard is visible with various management tiles: Device Manager, Policy &amp; Objects (selected), AP Manager, VPN Manager, Fabric View, FortiGuard, FortiSwitch Manager, Extender Manager, and System Settings.</p> <p>At the bottom, a table of Policy Packages is shown:</p> <table border="1"> <thead> <tr> <th>#</th> <th>Name</th> <th>From</th> <th>To</th> <th>Source</th> <th>Destination</th> <th>Schedule</th> <th>Service</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>lan</td> <td>lan</td> <td>wan1</td> <td>all</td> <td>all</td> <td>always</td> <td>ALL</td> </tr> <tr> <td colspan="8">Implicit (2-2 / Total: 1)</td> </tr> <tr> <td>2</td> <td>Implicit Deny</td> <td>any</td> <td>any</td> <td>all</td> <td>all</td> <td>always</td> <td>ALL</td> </tr> </tbody> </table>	#	Name	From	To	Source	Destination	Schedule	Service	1	lan	lan	wan1	all	all	always	ALL	Implicit (2-2 / Total: 1)								2	Implicit Deny	any	any	all	all	always	ALL
#	Name	From	To	Source	Destination	Schedule	Service																										
1	lan	lan	wan1	all	all	always	ALL																										
Implicit (2-2 / Total: 1)																																	
2	Implicit Deny	any	any	all	all	always	ALL																										
<p><b>Comentário</b></p>																																	

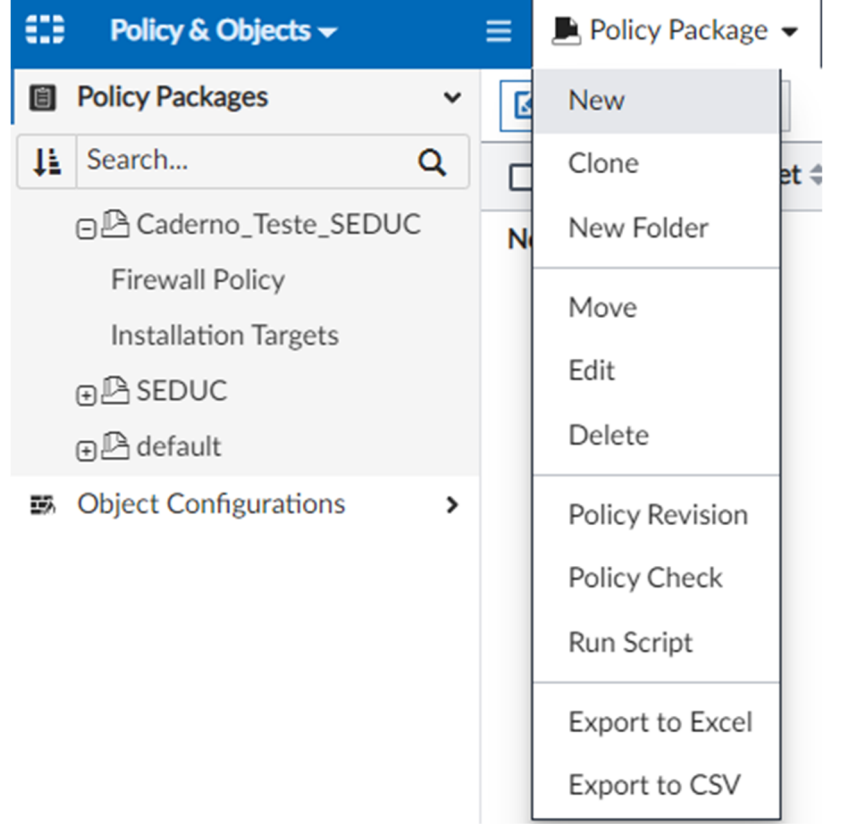
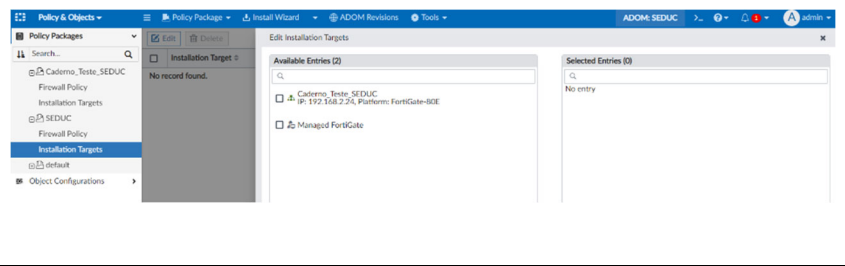
Item de Teste - 5.4.6	Permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os equipamentos;
Objetivo do Teste	Validar se o equipamento de gerência centralizada possui a funcionalidade de criação e distribuição de políticas 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	<p><b>About policies</b></p> <p>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.</p> <p>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.</p> <p>FortiManager can help simplify provisioning of new devices, ADOMs, or VDOMs by allowing you to copy or clone existing policy packages.</p> <p>Na aba de “Policy &amp; Objects “é possível criar um novo pacote de políticas.</p> 



	<p>Como também, selecionar quais equipamentos receberão esse pacote recém-criado. Para isto, basta acessar a guia "Installation Targets", em seguida ir em "Edit" e selecionar os equipamentos desejados.</p> 
<p><b>Comentário</b></p>	<p>Fonte: FortiManager Administration Guide acessado em <a href="https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/04f80bb3-e03c-11ec-bb32-fa163e15d75b/FortiManager-7.2.1-Administration_Guide.pdf">https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/04f80bb3-e03c-11ec-bb32-fa163e15d75b/FortiManager-7.2.1-Administration_Guide.pdf</a></p>

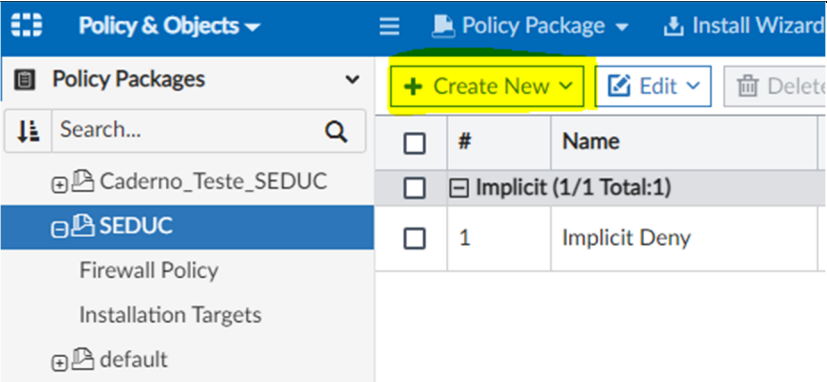
<p><b>Item de Teste - 5.4.8</b></p>	<p>Caso a Solução de Gerenciamento Centralizada torne-se indisponível, todos os seus gateways gerenciados devem continuar funcionando normalmente, permitindo a administração, operação e total controle sobre cada gateway enquanto a gerência continuar indisponível;</p>
<p><b>Objetivo do Teste</b></p>	<p>Demonstrar que o gateway independe da gerência para funcionar plenamente.</p>
<p><b>Configuração do Teste</b></p>	<p>Tornar indisponível a gerência e demonstrar o Firewall</p>
<p><b>Procedimento do Teste</b></p>	<p>Tornar indisponível a gerência e demonstrar o Firewall</p>
<p><b>Evidências</b></p>	<p>Imagens durante indisponibilidade</p>
<p><b>Comentário</b></p>	

<p><b>Item de Teste - 5.4.9</b></p>	<p>A Solução de Gerenciamento Centralizada deve permitir a instalação de políticas individuais (somente para 1 gateway), para um grupo de gateways e para todos os seus gateways gerenciados, não sendo aceito soluções com aplicações de apenas uma das opções;</p>
<p><b>Objetivo do Teste</b></p>	<p>Validar se a ferramenta permite a instalação de políticas individuais (somente para 1 gateway), para um grupo de gateways e para todos os seus gateways gerenciados.</p>
<p><b>Configuração do Teste</b></p>	<p>Demonstrar distribuição de política por gateway.</p>
<p><b>Procedimento do Teste</b></p>	<p>Na aba de "Policy &amp; Objects "é possível criar um novo pacote de políticas.</p> <p>Como também, selecionar quais equipamentos receberão esse pacote recém-criado. Para isto, basta acessar a guia "Installation Targets", em seguida ir em "Edit" e selecionar os equipamentos desejados.</p>

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

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



	e filtro de URL; monitoração de logs; ferramentas de investigação de logs; debugging; troubleshooting; visualização de eventos; dashboards; captura de pacotes;									
<b>Configuração do Teste</b> <b>Procedimento do Teste</b>	<p>Demonstrar operação do FortiManager</p> <p>Dentro de um pacote de políticas podemos adicionar uma nova regra e dentro dela colocar todos os filtros necessários.</p> <p>Entre eles, controle de aplicação (Applicatin Control), IPS, antivírus e anti-spyware(Antivírus), conteúdo Web e filtro de URL's(Web Filter Profile).</p> <p>Para realização de debugging e troubleshooting deve se usar do seguinte caminho para se acessar qualquer FortiGate gerenciado pelo FortiManager.</p> <p>Em "Device Manager" selecionar o FortiGate desejado e clicar duas vezes nele, assim aparecerá uma aba de informações sobre aquele ativo.</p> <p>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:</p> <p><a href="https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/244292/troubleshooting">https://docs.fortinet.com/document/FortiGate/7.2.4/administration-guide/244292/troubleshooting</a></p>									
<b>Evidências</b>	 <p>The screenshot shows the 'Policy &amp; Objects' configuration page in FortiManager. The 'Policy Packages' section is expanded, showing a search bar and a list of packages: 'Caderno_Testes_SEDUC', 'SEDUC', 'Firewall Policy', 'Installation Targets', and 'default'. The 'SEDUC' package is selected. To the right, a table lists the policies under 'SEDUC':</p> <table border="1"><thead><tr><th></th><th>#</th><th>Name</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td></td><td>Implicit (1/1 Total:1)</td></tr><tr><td><input type="checkbox"/></td><td>1</td><td>Implicit Deny</td></tr></tbody></table> <p>The '+ Create New' button is highlighted in yellow.</p>		#	Name	<input type="checkbox"/>		Implicit (1/1 Total:1)	<input type="checkbox"/>	1	Implicit Deny
	#	Name								
<input type="checkbox"/>		Implicit (1/1 Total:1)								
<input type="checkbox"/>	1	Implicit Deny								



The image displays three screenshots from the FortiGate management interface. The top screenshot, titled "Create New Firewall Policy", shows a list of security profiles on the left and a configuration table on the right. The table has two columns: "Use Standard Security Profiles" and "Use Security Profile Group". The profiles listed are AntiVirus Profile, Web Filter Profile, DNS Filter, Application Control, IPS, File Filter, Email Filter, DLP Profile, VOIP, ICAP, SSH Filter, and SSL/SSH Inspection. The "SSL no-inspection" profile is highlighted in the "Use Security Profile Group" column. The middle screenshot shows the "Device Manager" dashboard for a device named "Caderno\_Testes\_SEDUC". It displays system information such as Host Name, Serial Number, IP Address, System Time, Uptime, Firmware Version, Hardware Status, Operation Mode, VDOM, and Operation. The "Operation" status is highlighted in yellow. The bottom screenshot shows the "CLI Console of Caderno\_Testes\_SEDUC" with a terminal window displaying the command "diag debug application onvpn 1".

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



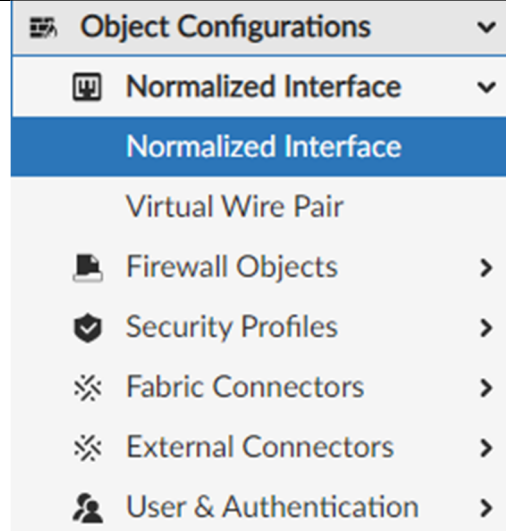
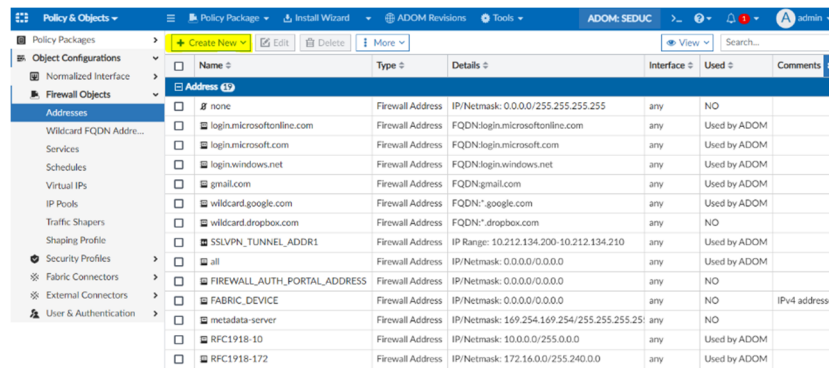
<b>Comentário</b>	

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

<b>Item de Teste - 5.4.12</b>	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;
<b>Objetivo do Teste</b>	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.
<b>Configuração do Teste</b>	Demonstrar caixa de pesquisa para filtro de objetos da base de regras
<b>Procedimento do Teste</b>	Em "Policy & Objects" podemos ter acesso a todos os tipos de objetos gerenciado por aquele equipamento.

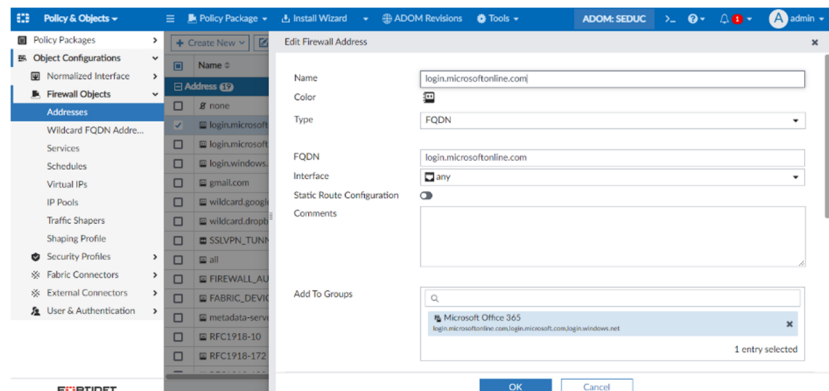
Dentro de cada aba, o FortiManager lhe dá a opção de criação de um novo objeto.

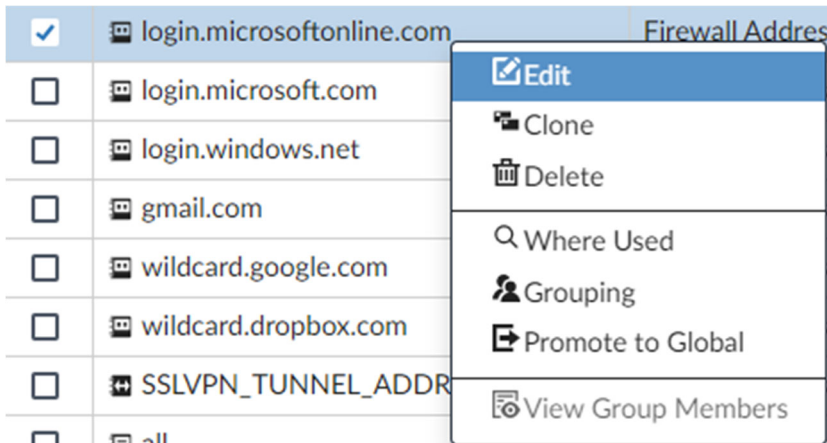
**Evidências**

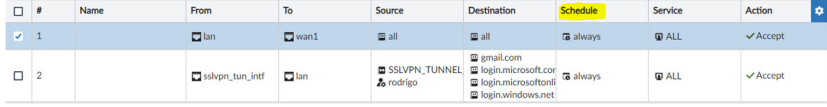
Name	Type	Details	Interface	Used	Comments
# none	Firewall Address	IP/Netmask: 0.0.0.0/255.255.255.255	any	NO	
login.microsoftonline.com	Firewall Address	FQDN:login.microsoftonline.com	any	Used by ADOM	
login.microsoft.com	Firewall Address	FQDN:login.microsoft.com	any	Used by ADOM	
login.windows.net	Firewall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

Edição de um já existente



Comentário	<p>Como também exclusão e visualização de onde está sendo usado.</p>  <p>The screenshot shows a list of Firewall Addresses with a context menu open over the first entry, 'login.microsoftonline.com'. The menu options are: Edit, Clone, Delete, Where Used, Grouping, Promote to Global, and View Group Members.</p>
------------	--

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

<b>Item de Teste - 5.4.14</b>	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);																											
<b>Objetivo do Teste</b>	Validar se a ferramenta possui a funcionalidade de atribuir tempo à uma política.																											
<b>Configuração do Teste</b>	Necessita ter um FortiManager e uma conta de administrador com acesso para escrita e visualização.																											
<b>Procedimento do Teste</b>	<p>Na aba de "Policy and Objects", é possível visualizar todas as regras presentes no dispositivo.</p> <p>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.</p>																											
<b>Evidências</b>	 <p>The screenshot shows a table with columns: #, Name, From, To, Source, Destination, Schedule, Service, and Action. Two rows are visible:</p> <table border="1"> <thead> <tr> <th>#</th> <th>Name</th> <th>From</th> <th>To</th> <th>Source</th> <th>Destination</th> <th>Schedule</th> <th>Service</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>1</td> <td></td> <td>lan</td> <td>wan1</td> <td>all</td> <td>all</td> <td>always</td> <td>ALL</td> <td>Accept</td> </tr> <tr> <td>2</td> <td></td> <td>sslvpn_tun_intf</td> <td>lan</td> <td>SSLVPN_TUNNEL, rodrigo</td> <td>gmail.com, login.microsoft.com, login.microsoftonline.com, login.windows.net</td> <td>always</td> <td>ALL</td> <td>Accept</td> </tr> </tbody> </table> <p>Para criação de regras para um período de tempo:</p>	#	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.microsoftonline.com, login.windows.net	always	ALL	Accept
#	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.microsoftonline.com, login.windows.net	always	ALL	Accept																				



**Create New One-Time Schedule**

Name:

Color: L

Start Time:

End Time:

Pre-expiration Event Log:

Number of Days Before:

Add To Groups:   
Click to select

Para regras recorrentes:

**Create New Recurring Schedule**

Name:

Color: L

Day:  Monday  Tuesday  Wednesday  
 Thursday  Friday  Saturday  
 Sunday

Time:  All day  Specify

Add To Groups:   
Click to select

**Comentário**

<b>Item de Teste - 5.4.15</b>	Deve registrar logs de auditoria referente as ações dos usuários administradores;																																																																								
<b>Objetivo do Teste</b>	Validar se a solução é capaz de registrar de auditoria referente as ações dos usuários administradores.																																																																								
<b>Configuração do Teste</b>	Demonstrar logs de rastreamento de ações locais dos administradores.																																																																								
<b>Procedimento do Teste</b>	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.																																																																								
<b>Evidências</b>	<p style="color: #0070C0; font-weight: bold; margin-top: 0;">Event Log</p> <p>The <i>Event Log</i> 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.</p> <p>See the <a href="#">FortiManager Log Message Reference</a>, available from the <a href="#">Fortinet Document Library</a>, for more information about the log messages.</p> <p>Go to <i>System Settings &gt; Event Log</i> to view the local log list.</p> <table border="1" style="width: 100%; border-collapse: collapse; font-size: 8px;"> <thead> <tr> <th>#</th> <th>Date Time</th> <th>Level</th> <th>User</th> <th>Sub-Type</th> <th>Description</th> <th>Operation</th> <th>Performed On</th> <th>Changes</th> </tr> </thead> <tbody> <tr> <td>7</td> <td>2023-04-26 12:27:39</td> <td>notice</td> <td>admin</td> <td>objcfg</td> <td>cds event log for object changed</td> <td>edit</td> <td>dtw-globul.adm...</td> <td>Superfap_manage 3ley-5358EVC1 Apr 24 09:12:07</td> </tr> <tr> <td>8</td> <td>2023-04-26 12:24:07</td> <td>notice</td> <td>admin</td> <td>objcfg</td> <td>cds event log for object changed</td> <td>edit</td> <td>dtw-globul.adm...</td> <td>Superfap_manage 3ley-5358EVC1 Apr 24 09:12:48</td> </tr> <tr> <td>9</td> <td>2023-04-26 12:24:07</td> <td>notice</td> <td>admin</td> <td>objcfg</td> <td>cds event log for object changed</td> <td>edit</td> <td>dtw-globul.adm...</td> <td>Superfap_manage 3ley-5358EVC1 Apr 24 09:12:07</td> </tr> <tr> <td>10</td> <td>2023-04-26 12:24:07</td> <td>notice</td> <td>admin</td> <td>objcfg</td> <td>cds event log for object changed</td> <td>edit</td> <td>dtw-globul.adm...</td> <td>Superfap_manage 3ley-5358EVC1 Apr 24 09:12:48</td> </tr> <tr> <td>11</td> <td>2023-04-26 12:21:55</td> <td>notice</td> <td>admin</td> <td>objcfg</td> <td>cds event log for object changed</td> <td>edit</td> <td>dtw-globul.adm...</td> <td>Superfap_manage 3ley-5358EVC1 Apr 24 09:12:48</td> </tr> <tr> <td>12</td> <td>2023-04-26 12:19:55</td> <td>information</td> <td>update_manager</td> <td>fgd</td> <td>Package update response from FortiGuard server received</td> <td>Update Response</td> <td>12.34.97.16</td> <td>Receive an update 8a000000:0000C 05000000:ALCID0 version=0000:0X</td> </tr> <tr> <td>13</td> <td>2023-04-26 12:09:41</td> <td>information</td> <td>update_manager</td> <td>fgd</td> <td>Package update response from FortiGuard server received</td> <td>Update Response</td> <td>12.34.97.16</td> <td>Receive an update 8a000000:0000C 05000000:ALCID0 version=0000:0X</td> </tr> </tbody> </table>	#	Date Time	Level	User	Sub-Type	Description	Operation	Performed On	Changes	7	2023-04-26 12:27:39	notice	admin	objcfg	cds event log for object changed	edit	dtw-globul.adm...	Superfap_manage 3ley-5358EVC1 Apr 24 09:12:07	8	2023-04-26 12:24:07	notice	admin	objcfg	cds event log for object changed	edit	dtw-globul.adm...	Superfap_manage 3ley-5358EVC1 Apr 24 09:12:48	9	2023-04-26 12:24:07	notice	admin	objcfg	cds event log for object changed	edit	dtw-globul.adm...	Superfap_manage 3ley-5358EVC1 Apr 24 09:12:07	10	2023-04-26 12:24:07	notice	admin	objcfg	cds event log for object changed	edit	dtw-globul.adm...	Superfap_manage 3ley-5358EVC1 Apr 24 09:12:48	11	2023-04-26 12:21:55	notice	admin	objcfg	cds event log for object changed	edit	dtw-globul.adm...	Superfap_manage 3ley-5358EVC1 Apr 24 09:12:48	12	2023-04-26 12:19:55	information	update_manager	fgd	Package update response from FortiGuard server received	Update Response	12.34.97.16	Receive an update 8a000000:0000C 05000000:ALCID0 version=0000:0X	13	2023-04-26 12:09:41	information	update_manager	fgd	Package update response from FortiGuard server received	Update Response	12.34.97.16	Receive an update 8a000000:0000C 05000000:ALCID0 version=0000:0X
#	Date Time	Level	User	Sub-Type	Description	Operation	Performed On	Changes																																																																	
7	2023-04-26 12:27:39	notice	admin	objcfg	cds event log for object changed	edit	dtw-globul.adm...	Superfap_manage 3ley-5358EVC1 Apr 24 09:12:07																																																																	
8	2023-04-26 12:24:07	notice	admin	objcfg	cds event log for object changed	edit	dtw-globul.adm...	Superfap_manage 3ley-5358EVC1 Apr 24 09:12:48																																																																	
9	2023-04-26 12:24:07	notice	admin	objcfg	cds event log for object changed	edit	dtw-globul.adm...	Superfap_manage 3ley-5358EVC1 Apr 24 09:12:07																																																																	
10	2023-04-26 12:24:07	notice	admin	objcfg	cds event log for object changed	edit	dtw-globul.adm...	Superfap_manage 3ley-5358EVC1 Apr 24 09:12:48																																																																	
11	2023-04-26 12:21:55	notice	admin	objcfg	cds event log for object changed	edit	dtw-globul.adm...	Superfap_manage 3ley-5358EVC1 Apr 24 09:12:48																																																																	
12	2023-04-26 12:19:55	information	update_manager	fgd	Package update response from FortiGuard server received	Update Response	12.34.97.16	Receive an update 8a000000:0000C 05000000:ALCID0 version=0000:0X																																																																	
13	2023-04-26 12:09:41	information	update_manager	fgd	Package update response from FortiGuard server received	Update Response	12.34.97.16	Receive an update 8a000000:0000C 05000000:ALCID0 version=0000:0X																																																																	



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

<b>Item de Teste - 5.4.16</b>	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;																																																																								
<b>Objetivo do Teste</b>	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.																																																																								
<b>Configuração do Teste</b>	Demonstrar logs de rastreamento de ações locais dos administradores.																																																																								
<b>Procedimento do Teste</b>	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.																																																																								
<b>Evidências</b>	<p><b>Event Log</b></p> <p>The <i>Event Log</i> 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.</p> <p>See the <i>FortiManager Log Message Reference</i>, available from the <i>Fortinet Document Library</i>, for more information about the log messages.</p> <p>Go to <i>System Settings &gt; Event Log</i> to view the local log list.</p> <table border="1"> <thead> <tr> <th>#</th> <th>Date Time</th> <th>Level</th> <th>User</th> <th>Sub Type</th> <th>Description</th> <th>Operation</th> <th>Performed On</th> <th>Changes</th> </tr> </thead> <tbody> <tr> <td>7</td> <td>2021-04-26 12:27:39</td> <td>notice</td> <td>admin</td> <td>objcfg</td> <td>obj event log for object changed</td> <td>edit</td> <td>dev-globalLads...</td> <td>typer-fp_manag... 2021-04-26 12:27:39 Apr 14 09:12:07</td> </tr> <tr> <td>8</td> <td>2021-04-26 12:24:07</td> <td>notice</td> <td>admin</td> <td>objcfg</td> <td>obj event log for object changed</td> <td>edit</td> <td>dev-globalLads...</td> <td>typer-fp_manag... 2021-04-26 12:24:07 Apr 14 09:12:48</td> </tr> <tr> <td>9</td> <td>2021-04-26 12:24:07</td> <td>notice</td> <td>admin</td> <td>objcfg</td> <td>obj event log for object changed</td> <td>edit</td> <td>dev-globalLads...</td> <td>typer-fp_manag... 2021-04-26 12:24:07 Apr 14 16:12:07</td> </tr> <tr> <td>10</td> <td>2021-04-26 12:24:07</td> <td>notice</td> <td>admin</td> <td>objcfg</td> <td>obj event log for object changed</td> <td>edit</td> <td>dev-globalLads...</td> <td>typer-fp_manag... 2021-04-26 12:24:07 Apr 14 16:27:32</td> </tr> <tr> <td>11</td> <td>2021-04-26 12:21:10</td> <td>notice</td> <td>admin</td> <td>objcfg</td> <td>obj event log for object changed</td> <td>edit</td> <td>dev-globalLads...</td> <td>typer-fp_manag... 2021-04-26 12:21:10 Apr 14 16:12:48</td> </tr> <tr> <td>12</td> <td>2021-04-26 12:19:55</td> <td>information</td> <td>update_manager</td> <td>fgpl</td> <td>Package update response from FortiGuard server received</td> <td>Update Response</td> <td>12:34:97:16</td> <td>Receive an update from FortiGuard server received</td> </tr> <tr> <td>13</td> <td>2021-04-26 12:09:41</td> <td>information</td> <td>update_manager</td> <td>fgpl</td> <td>Package update response from FortiGuard server received</td> <td>Update Response</td> <td>12:34:97:16</td> <td>Receive an update from FortiGuard server received</td> </tr> </tbody> </table>	#	Date Time	Level	User	Sub Type	Description	Operation	Performed On	Changes	7	2021-04-26 12:27:39	notice	admin	objcfg	obj event log for object changed	edit	dev-globalLads...	typer-fp_manag... 2021-04-26 12:27:39 Apr 14 09:12:07	8	2021-04-26 12:24:07	notice	admin	objcfg	obj event log for object changed	edit	dev-globalLads...	typer-fp_manag... 2021-04-26 12:24:07 Apr 14 09:12:48	9	2021-04-26 12:24:07	notice	admin	objcfg	obj event log for object changed	edit	dev-globalLads...	typer-fp_manag... 2021-04-26 12:24:07 Apr 14 16:12:07	10	2021-04-26 12:24:07	notice	admin	objcfg	obj event log for object changed	edit	dev-globalLads...	typer-fp_manag... 2021-04-26 12:24:07 Apr 14 16:27:32	11	2021-04-26 12:21:10	notice	admin	objcfg	obj event log for object changed	edit	dev-globalLads...	typer-fp_manag... 2021-04-26 12:21:10 Apr 14 16:12:48	12	2021-04-26 12:19:55	information	update_manager	fgpl	Package update response from FortiGuard server received	Update Response	12:34:97:16	Receive an update from FortiGuard server received	13	2021-04-26 12:09:41	information	update_manager	fgpl	Package update response from FortiGuard server received	Update Response	12:34:97:16	Receive an update from FortiGuard server received
#	Date Time	Level	User	Sub Type	Description	Operation	Performed On	Changes																																																																	
7	2021-04-26 12:27:39	notice	admin	objcfg	obj event log for object changed	edit	dev-globalLads...	typer-fp_manag... 2021-04-26 12:27:39 Apr 14 09:12:07																																																																	
8	2021-04-26 12:24:07	notice	admin	objcfg	obj event log for object changed	edit	dev-globalLads...	typer-fp_manag... 2021-04-26 12:24:07 Apr 14 09:12:48																																																																	
9	2021-04-26 12:24:07	notice	admin	objcfg	obj event log for object changed	edit	dev-globalLads...	typer-fp_manag... 2021-04-26 12:24:07 Apr 14 16:12:07																																																																	
10	2021-04-26 12:24:07	notice	admin	objcfg	obj event log for object changed	edit	dev-globalLads...	typer-fp_manag... 2021-04-26 12:24:07 Apr 14 16:27:32																																																																	
11	2021-04-26 12:21:10	notice	admin	objcfg	obj event log for object changed	edit	dev-globalLads...	typer-fp_manag... 2021-04-26 12:21:10 Apr 14 16:12:48																																																																	
12	2021-04-26 12:19:55	information	update_manager	fgpl	Package update response from FortiGuard server received	Update Response	12:34:97:16	Receive an update from FortiGuard server received																																																																	
13	2021-04-26 12:09:41	information	update_manager	fgpl	Package update response from FortiGuard server received	Update Response	12:34:97:16	Receive an update from FortiGuard server received																																																																	



The screenshot displays the FortiManager System Settings interface. At the top, there is a navigation bar with 'System Settings' and a menu icon. Below this is a grid of management tools: Device Manager, Policy & Objects, AP Manager, VPN Manager, Fabric View, FortiGuard, FortiSwitch Manager, Extender Manager, System Settings (highlighted with a blue box), and Management Extensions. Below the grid is an event log table with the following columns: #, Date Time, Level, User, Sub Type, Operation, Changes, Description, and Performed On.

#	Date Time	Level	User	Sub Type	Operation	Changes	Description	Performed On
7	2023-03-15 15:05:08	information	update_manager	FortiGuard service event	Update Resu...	Send new version object to device (snFGVM010000015354, ip=127.0.0.1) objid...	Object update re...	127.0.0.1.0
8	2023-03-15 15:05:51	information	update_manager	FortiGuard service event	Update Respo...	Receive an update package from f6b00002.10115-2303151745: 07000000AV...	Package update r...	208.184.237.67
9	2023-03-15 15:01:51	information	update_manager	FortiGuard service event	Update Respo...	Receive an update package from f6b00002.10115-2303151745: 07000000AV...	Package update r...	208.184.237.67
10	2023-03-15 15:01:48	information	update_manager	FortiGuard service event	Update Respo...	Receive an update package from f6b00000.00000-2303151801: 01000000ALCL...	Package update r...	208.184.237.67
11	2023-03-15 15:01:18	notice	A admin	Deployment manager event	Device conf...	Config install preview successfully (status=not modified configstatus=insync...	Install preview su...	Caderno_Teste_SEDUC
12	2023-03-15 15:00:49	information	A admin	Policy console event	package/tem...	Caderno_Teste_SEDUC[root] policy package 'Caderno_Teste_SEDUC' status upda...	Security console ...	Caderno_Teste_SEDUC
13	2023-03-15 15:00:49	notice	A admin-GUI192.168.3.254	Configuration change event	edit	type-policy_package_setting.pkgname=Caderno_Teste_SEDUC;checksum=2023...	cdtb event log for ...	dev-global.adom-SEDUC
14	2023-03-15 15:00:49	notice	A admin-GUI192.168.3.254	Configuration change event	add	type-dynamic_cert_mapping.key=Fortinet_CA_SSL;dynamiclocal-cert=Fortinet...	cdtb event log for ...	dev-Caderno_Teste_SEDU
15	2023-03-15 15:00:49	notice	A admin-GUI192.168.3.254	Configuration change event	edit	type-dynamic_cert_localkey=Fortinet_CA_SSL	cdtb event log for ...	dev-global.adom-SEDUC
16	2023-03-15 15:00:49	notice	A admin-GUI192.168.3.254	Configuration change event	add	type-authentication_set.pkgname=Caderno_Teste_SEDUC;auth=https-enable.ca...	cdtb event log for ...	dev-global.adom-SEDUC
17	2023-03-15 15:00:49	notice	A admin-GUI192.168.3.254	Configuration change event	add	[ ] : schedule-always:schedule-timeout-disable;send-deny-packet-disable;service...	cdtb event log for ...	dev-global.adom-SEDUC
18	2023-03-15 15:00:49	notice	A admin-GUI192.168.3.254	Configuration change event	add	type-fv_policy.pkgname=Caderno_Teste_SEDUC;key=2;uuid=2402297c-c345-5...	cdtb event log for ...	dev-global.adom-SEDUC
19	2023-03-15 15:00:49	notice	A admin-GUI192.168.3.254	Configuration change event	add	[ ] : on-ALL;service-regex-disable;session-@-0;age-check-disable;arcadd=all;tr...	cdtb event log for ...	dev-global.adom-SEDUC
20	2023-03-15 15:00:49	notice	A admin-GUI192.168.3.254	Configuration change event	add	type-fv_policy.pkgname=Caderno_Teste_SEDUC;key=1;uuid=f0e1-f0e1-f456-5...	cdtb event log for ...	dev-global.adom-SEDUC

**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](https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/04f80bb3-e03c-11ec-bb32-fa163e15d75b/FortiManager-7.2.1-Administration_Guide.pdf)

<b>Item de Teste - 5.4.17</b>	Prover funcionalidade para análise e auditoria de regras com capacidade de detectar regras conflitantes ou não conformes;
<b>Objetivo do Teste</b>	Verificar se o equipamento faz uma validação de políticas que estão conflitantes entre si ou em não conformação.
<b>Configuração do Teste</b>	Demonstrar a sobreposição de regras que se anulam ou se repetem.
<b>Procedimento do Teste</b>	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**

**Perform a policy consistency check**

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

The check will verify:

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

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

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

**Import Device - Caderno\_Testes\_SEDUC - Interface Mapping & Policy (2/5)**

Create a new policy package for import.

Policy Package Name:

Folder:

Policy Selection:

Object Selection:

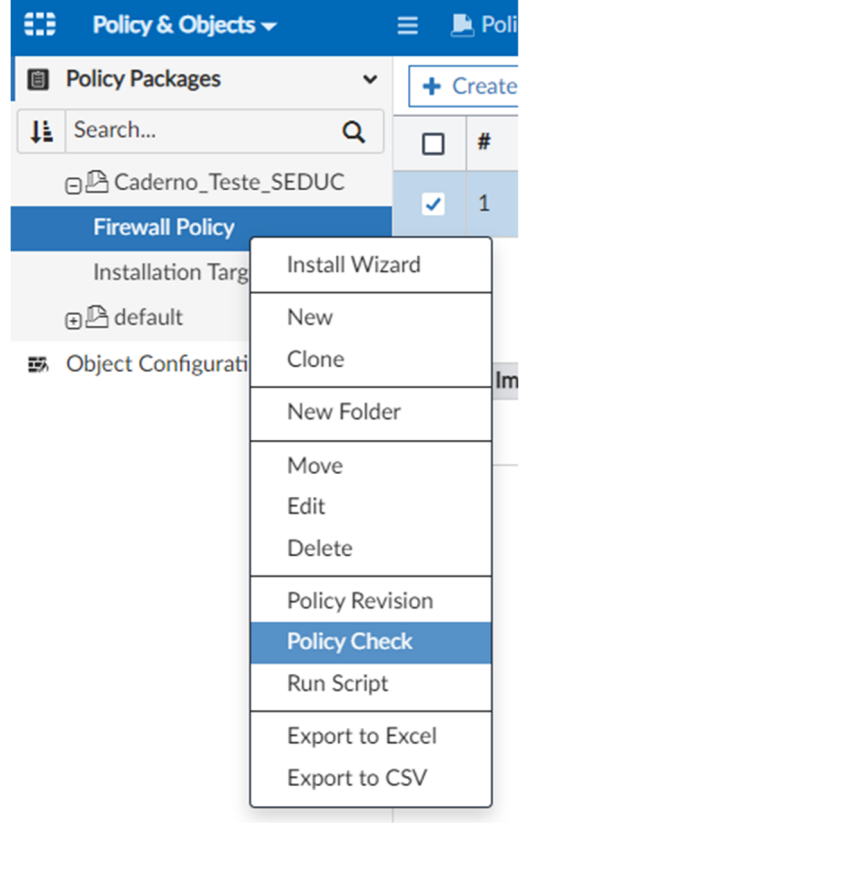
**i** When importing configuration from this device, all enabled interfaces require a mapping to an ADOM Level interface. Note, the same ADOM Level interface can map to different interfaces on the each device.

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

3

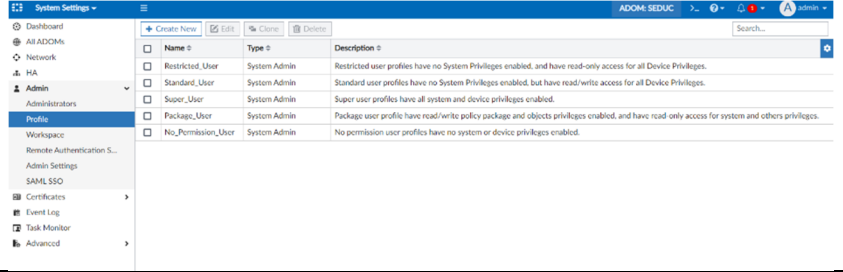
Add mappings for all unused



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

<b>Item de Teste - 5.4.18</b>	Suportar acesso baseado em perfil de usuário com as permissões de visualizar e modificar;								
<b>Objetivo do Teste</b>	Verificar se o equipamento de gerência centralizada suporta o Suportar acesso baseado em perfil de usuário com as permissões de visualizar e modificar;								
<b>Configuração do Teste</b>	Demonstrar os perfis de acesso ao FortiManager								
<b>Procedimento do Teste</b>	Demonstrar os perfis de acesso ao FortiManager								
<b>Evidências</b>	<p>Por padrão, o FortiManager já vem com os seguintes perfis:</p> <table border="1" data-bbox="526 1585 1348 1796"> <tr> <td><b>Restricted_User</b></td> <td>Restricted user profiles have no system privileges enabled, and have read-only access for all device privileges.</td> </tr> <tr> <td><b>Standard_User</b></td> <td>Standard user profiles have no system privileges enabled, and have read/write access for all device privileges.</td> </tr> <tr> <td><b>Super_User</b></td> <td>Super user profiles have all system and device privileges enabled. It cannot be edited.</td> </tr> <tr> <td><b>Package_User</b></td> <td>Package user profile have read/write policy and objects privileges enabled, and have read-only access for system and other privileges.</td> </tr> </table> <p>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</p>	<b>Restricted_User</b>	Restricted user profiles have no system privileges enabled, and have read-only access for all device privileges.	<b>Standard_User</b>	Standard user profiles have no system privileges enabled, and have read/write access for all device privileges.	<b>Super_User</b>	Super user profiles have all system and device privileges enabled. It cannot be edited.	<b>Package_User</b>	Package user profile have read/write policy and objects privileges enabled, and have read-only access for system and other privileges.
<b>Restricted_User</b>	Restricted user profiles have no system privileges enabled, and have read-only access for all device privileges.								
<b>Standard_User</b>	Standard user profiles have no system privileges enabled, and have read/write access for all device privileges.								
<b>Super_User</b>	Super user profiles have all system and device privileges enabled. It cannot be edited.								
<b>Package_User</b>	Package user profile have read/write policy and objects privileges enabled, and have read-only access for system and other privileges.								



	<p>possível visualizar todos os perfis já criados, bem como editar os perfis que foram fornecidos como padrão.</p> 
<p><b>Comentário</b></p>	<p>Fonte: FortiManager Administration Guide acessado em <a href="https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/04f80bb3-e03c-11ec-bb32-fa163e15d75b/FortiManager-7.2.1-Administration_Guide.pdf">https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/04f80bb3-e03c-11ec-bb32-fa163e15d75b/FortiManager-7.2.1-Administration_Guide.pdf</a></p>

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



**Import Device - Caderno\_Testes\_SEDUC - Interface Mapping & Policy (2/5)**

Create a new policy package for import.

Policy Package Name: Caderno\_Testes\_SEDUC  
Folder: root  
Policy Selection: Import All (3) | Select Policies to Import  
Object Selection: Import only policy dependent objects | Import all objects

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

Search...

Device Interface	Mapping Type	Normalized Interface
lan	Per-Device   Per-Platform	lan
ssl.root	Per-Device   Per-Platform	ssl.root
wan1	Per-Device   Per-Platform	wan1

3

Add mappings for all unused

Next > | Cancel

**Policy & Objects**

Policy Packages

Search...

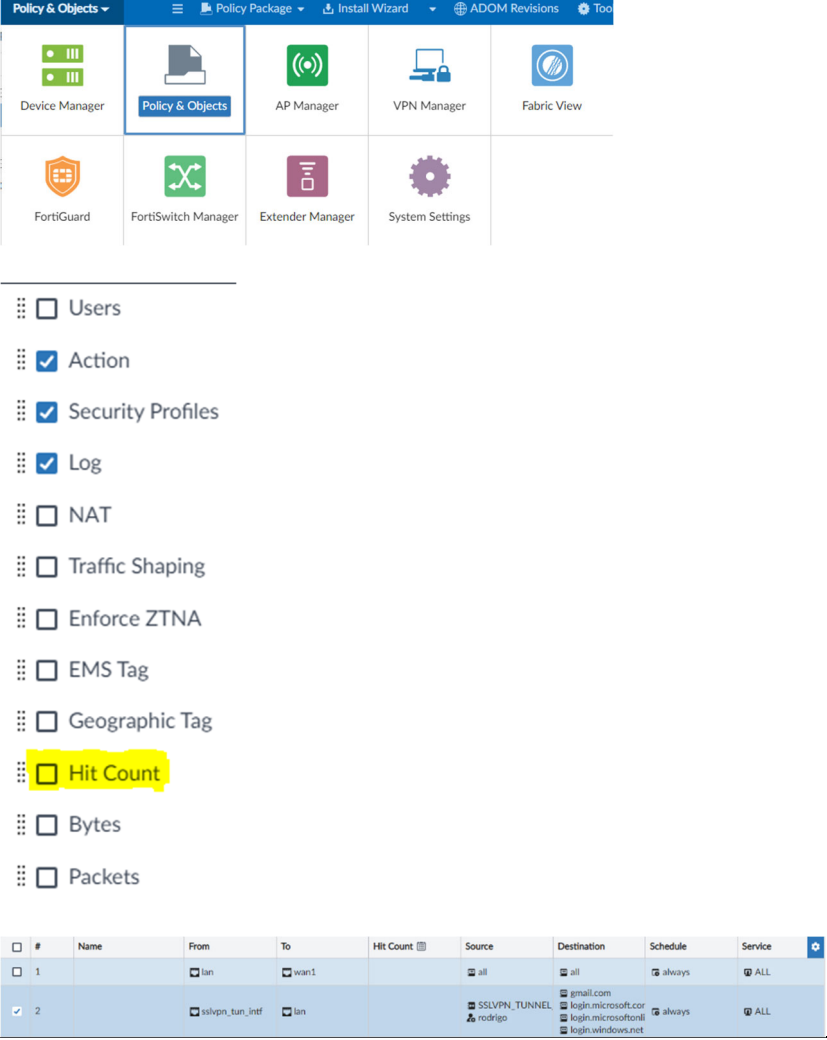
Caderno\_Testes\_SEDUC

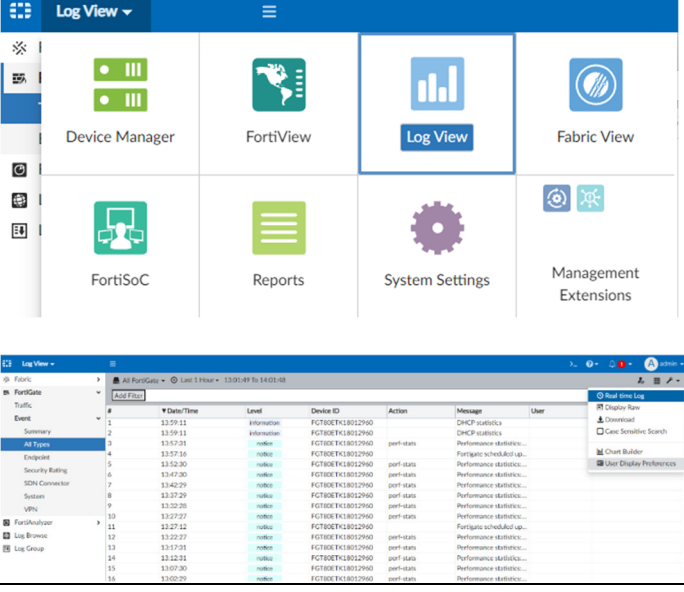
**Firewall Policy** | 1

- Install Wizard
- New
- Clone
- New Folder
- Move
- Edit
- Delete
- Policy Revision
- Policy Check**
- Run Script
- Export to Excel
- Export to CSV

**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](https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/04f80bb3-e03c-11ec-bb32-fa163e15d75b/FortiManager-7.2.1-Administration_Guide.pdf)



<b>Item de Teste -5.4.20</b>	A solução deve possuir “hit”/volume de regras para identificar possíveis melhorias na performance reordenando as mesmas;																											
<b>Objetivo do Teste</b>	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;																											
<b>Configuração do Teste</b>	Demonstrar hit counts de regras em uso.																											
<b>Procedimento do Teste</b>	<p>Para isto, é necessário acessar a aba de “Policy &amp; Objects”.</p> <p>Em seguida, é necessário selecionar um pacote de políticas. Depois, caso não esteja habilitado a opção de visualização de “Hit Counts”, basta ir ao canto superior direito e clicar no símbolo de engrenagem. Lá aparecerá várias informações referentes às políticas, entre elas, “Hit Count”.</p>																											
<b>Evidências</b>	 <p>The screenshot shows the 'Policy &amp; Objects' configuration page in FortiGate. The 'Hit Count' checkbox is highlighted in yellow. Below the configuration list, a table shows rule details for rule 2, including source, destination, and schedule.</p> <table border="1" data-bbox="523 1753 1353 1854"><thead><tr><th>#</th><th>Name</th><th>From</th><th>To</th><th>Hit Count</th><th>Source</th><th>Destination</th><th>Schedule</th><th>Service</th></tr></thead><tbody><tr><td>1</td><td></td><td>lan</td><td>wan1</td><td></td><td>all</td><td></td><td>always</td><td>ALL</td></tr><tr><td>2</td><td></td><td>sslvpn_tun_intf</td><td>lan</td><td></td><td>SSLVPN_TUNNEL rodrigo</td><td>gmail.com login.microsoft.com login.microsoftonl login.windows.net</td><td>always</td><td>ALL</td></tr></tbody></table>	#	Name	From	To	Hit Count	Source	Destination	Schedule	Service	1		lan	wan1		all		always	ALL	2		sslvpn_tun_intf	lan		SSLVPN_TUNNEL rodrigo	gmail.com login.microsoft.com login.microsoftonl login.windows.net	always	ALL
#	Name	From	To	Hit Count	Source	Destination	Schedule	Service																				
1		lan	wan1		all		always	ALL																				
2		sslvpn_tun_intf	lan		SSLVPN_TUNNEL rodrigo	gmail.com login.microsoft.com login.microsoftonl login.windows.net	always	ALL																				
<b>Comentário</b>																												

<b>Item de Teste - 5.4.21</b>	Deve possuir visualização de log em tempo próximo ao real;																																																																																																																
<b>Objetivo do Teste</b>	Verificar se o equipamento possui a funcionalidade de visualização de logs em tempo próximo ao real.																																																																																																																
<b>Configuração do Teste</b>	Demonstrar a sobreposição de regras que se anulam ou se repetem.																																																																																																																
<b>Procedimento do Teste</b>	<p>Para acessar a funcionalidade de visualização dos registros em tempo real, é necessário acessar a seção "Visualização de Logs".</p> <p>A seguir, é necessário selecionar o equipamento desejado, pressionar o ícone de chave de fenda localizado no canto superior direito e, em seguida, selecionar a opção "Registro em Tempo Real".</p>																																																																																																																
<b>Evidências</b>	 <table border="1" data-bbox="523 1120 1209 1352"> <thead> <tr> <th>#</th> <th>Date/Time</th> <th>Level</th> <th>Device ID</th> <th>Action</th> <th>Message</th> <th>User</th> </tr> </thead> <tbody> <tr><td>1</td><td>13:59:11</td><td>Information</td><td>FGT06TC18012960</td><td></td><td>DHCP statistics</td><td></td></tr> <tr><td>2</td><td>13:59:11</td><td>Information</td><td>FGT06TC18012960</td><td></td><td>DHCP statistics</td><td></td></tr> <tr><td>3</td><td>13:57:01</td><td>notice</td><td>FGT06TC18012960</td><td>port-status</td><td>Performance statistics...</td><td></td></tr> <tr><td>4</td><td>13:57:16</td><td>notice</td><td>FGT06TC18012960</td><td>port-status</td><td>Performance statistics...</td><td></td></tr> <tr><td>5</td><td>13:52:30</td><td>notice</td><td>FGT06TC18012960</td><td>port-status</td><td>Performance statistics...</td><td></td></tr> <tr><td>6</td><td>13:47:30</td><td>notice</td><td>FGT06TC18012960</td><td>port-status</td><td>Performance statistics...</td><td></td></tr> <tr><td>7</td><td>13:42:29</td><td>notice</td><td>FGT06TC18012960</td><td>port-status</td><td>Performance statistics...</td><td></td></tr> <tr><td>8</td><td>13:37:29</td><td>notice</td><td>FGT06TC18012960</td><td>port-status</td><td>Performance statistics...</td><td></td></tr> <tr><td>9</td><td>13:32:28</td><td>notice</td><td>FGT06TC18012960</td><td>port-status</td><td>Performance statistics...</td><td></td></tr> <tr><td>10</td><td>13:27:27</td><td>notice</td><td>FGT06TC18012960</td><td>port-status</td><td>Performance statistics...</td><td></td></tr> <tr><td>11</td><td>13:22:12</td><td>notice</td><td>FGT06TC18012960</td><td>port-status</td><td>Performance statistics...</td><td></td></tr> <tr><td>12</td><td>13:17:11</td><td>notice</td><td>FGT06TC18012960</td><td>port-status</td><td>Performance statistics...</td><td></td></tr> <tr><td>13</td><td>13:12:11</td><td>notice</td><td>FGT06TC18012960</td><td>port-status</td><td>Performance statistics...</td><td></td></tr> <tr><td>14</td><td>13:07:10</td><td>notice</td><td>FGT06TC18012960</td><td>port-status</td><td>Performance statistics...</td><td></td></tr> <tr><td>15</td><td>13:02:09</td><td>notice</td><td>FGT06TC18012960</td><td>port-status</td><td>Performance statistics...</td><td></td></tr> </tbody> </table>	#	Date/Time	Level	Device ID	Action	Message	User	1	13:59:11	Information	FGT06TC18012960		DHCP statistics		2	13:59:11	Information	FGT06TC18012960		DHCP statistics		3	13:57:01	notice	FGT06TC18012960	port-status	Performance statistics...		4	13:57:16	notice	FGT06TC18012960	port-status	Performance statistics...		5	13:52:30	notice	FGT06TC18012960	port-status	Performance statistics...		6	13:47:30	notice	FGT06TC18012960	port-status	Performance statistics...		7	13:42:29	notice	FGT06TC18012960	port-status	Performance statistics...		8	13:37:29	notice	FGT06TC18012960	port-status	Performance statistics...		9	13:32:28	notice	FGT06TC18012960	port-status	Performance statistics...		10	13:27:27	notice	FGT06TC18012960	port-status	Performance statistics...		11	13:22:12	notice	FGT06TC18012960	port-status	Performance statistics...		12	13:17:11	notice	FGT06TC18012960	port-status	Performance statistics...		13	13:12:11	notice	FGT06TC18012960	port-status	Performance statistics...		14	13:07:10	notice	FGT06TC18012960	port-status	Performance statistics...		15	13:02:09	notice	FGT06TC18012960	port-status	Performance statistics...	
#	Date/Time	Level	Device ID	Action	Message	User																																																																																																											
1	13:59:11	Information	FGT06TC18012960		DHCP statistics																																																																																																												
2	13:59:11	Information	FGT06TC18012960		DHCP statistics																																																																																																												
3	13:57:01	notice	FGT06TC18012960	port-status	Performance statistics...																																																																																																												
4	13:57:16	notice	FGT06TC18012960	port-status	Performance statistics...																																																																																																												
5	13:52:30	notice	FGT06TC18012960	port-status	Performance statistics...																																																																																																												
6	13:47:30	notice	FGT06TC18012960	port-status	Performance statistics...																																																																																																												
7	13:42:29	notice	FGT06TC18012960	port-status	Performance statistics...																																																																																																												
8	13:37:29	notice	FGT06TC18012960	port-status	Performance statistics...																																																																																																												
9	13:32:28	notice	FGT06TC18012960	port-status	Performance statistics...																																																																																																												
10	13:27:27	notice	FGT06TC18012960	port-status	Performance statistics...																																																																																																												
11	13:22:12	notice	FGT06TC18012960	port-status	Performance statistics...																																																																																																												
12	13:17:11	notice	FGT06TC18012960	port-status	Performance statistics...																																																																																																												
13	13:12:11	notice	FGT06TC18012960	port-status	Performance statistics...																																																																																																												
14	13:07:10	notice	FGT06TC18012960	port-status	Performance statistics...																																																																																																												
15	13:02:09	notice	FGT06TC18012960	port-status	Performance statistics...																																																																																																												
<b>Comentário</b>																																																																																																																	

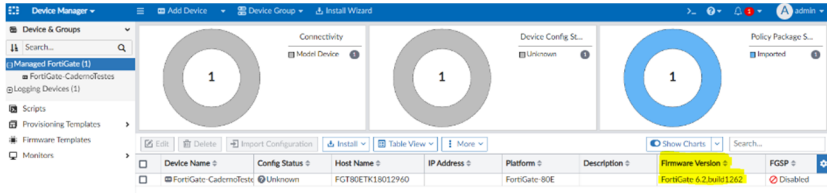
<b>Item de Teste - 5.4.22</b>	A solução deve possuir mecanismo de indexação de logs para permitir uma busca acelerada dos eventos sem a necessidade de abertura de arquivos de logs mais antigos;
<b>Objetivo do Teste</b>	Validar se a solução possui um mecanismo de indexação de logs para permitir uma busca acelerada dos eventos sem a necessidade de abertura de arquivos de logs mais antigos.
<b>Configuração do Teste</b>	Navegar no dashboard analíticos e demonstrar drill down de logs.
<b>Procedimento do Teste</b>	Navegar no dashboard analíticos e demonstrar drill down de logs.
<b>Evidências</b>	O FortiAnalyzer faz uma distinção dos logs de duas formas, uma são os logs arquivados e outras são de logs analíticos, os logs arquivados são os logs de tempo real que são arquivados e comprimidos e considerados offline, já os logs analíticos são indexados em um banco de dados SQL e considerados online.



	<h3>Analytics and Archive logs</h3> <p>Logs in FortiAnalyzer are in one of the following phases.</p> <ul style="list-style-type: none"> <li>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.</li> <li>Archive logs: When a real-time log file in Archive has been completely inserted, that file is compressed and considered to be offline.</li> <li>Analytics logs or historical logs: Indexed in the SQL database and online.</li> </ul> <p>Use a data policy to control how long to retain Analytics and Archive logs.</p> <ul style="list-style-type: none"> <li>Archive logs</li> <li>Analytic logs</li> </ul>
<b>Comentário</b>	Fonte: "Analytics and Archive logs" acessado em <a href="https://docs.fortinet.com/document/fortianalyzer/7.2.2/administration-guide/761825/analytics-and-archive-logs">https://docs.fortinet.com/document/fortianalyzer/7.2.2/administration-guide/761825/analytics-and-archive-logs</a>

5.4.39 Solução deve incluir monitoramento gráfico que fornece uma maneira fácil

monitorar o status de gateways, apresentando os seguintes status:

<b>Item de Teste - 5.4.39.1</b>	Versão do sistema operacional;
<b>Objetivo do Teste</b>	Verificar se a solução de gerenciamento possui visualização das versões do sistema operacional dos equipamentos gerenciados.
<b>Configuração do Teste</b>	Demonstrar versões de sistemas operacionais gerenciados.
<b>Procedimento do Teste</b>	Demonstrar versões de sistemas operacionais gerenciados.
<b>Evidências</b>	Na aba de "Device Manager" podemos ter acesso a algumas informações dos equipamentos gerenciados, entre elas, a versão do sistema operacional. 
<b>Comentário</b>	

<b>Item de Teste - 5.4.39.2</b>	Informações de utilização de CPU dos gateways gerenciados;
<b>Objetivo do Teste</b>	Verificar se a solução de gerenciamento possui visualização da utilização de CPU dos gateways gerenciados.
<b>Configuração do Teste</b>	Demonstrar consumo de CPU dos gateways gerenciados.
<b>Procedimento do Teste</b>	Demonstrar consumo de CPU dos gateways gerenciados.
<b>Evidências</b>	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.

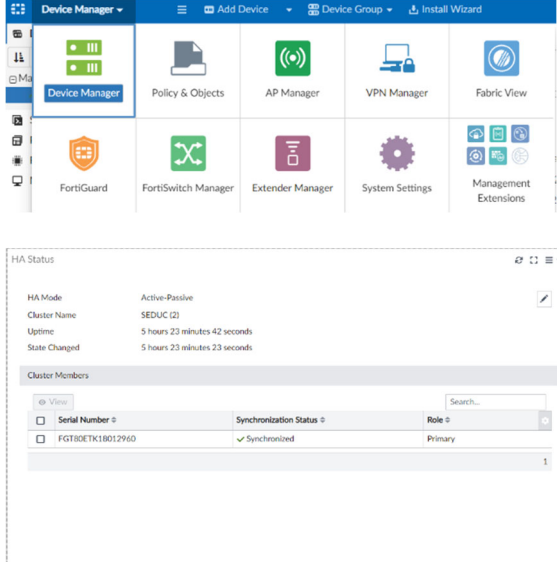


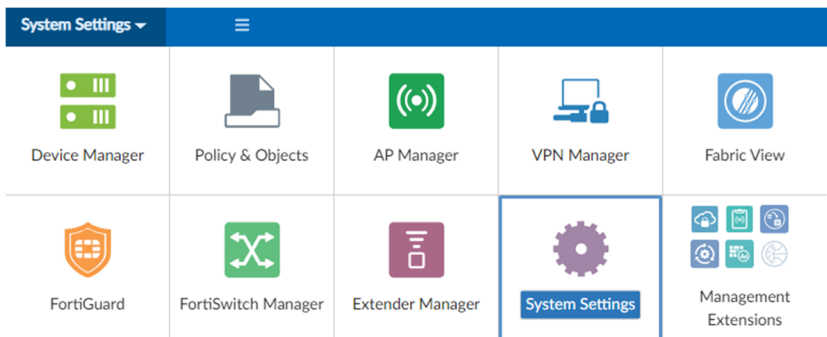
<b>Comentário</b>	

<b>Item de Teste - 5.4.39.3</b>	Informações de conexões concorrentes dos gateways gerenciados;
<b>Objetivo do Teste</b>	Verificar se a solução de gerenciamento possui visualização da quantidade de conexões concorrentes dos gateways gerenciados.
<b>Configuração do Teste</b>	Demonstrar consumo de conexões concorrentes por gateways gerenciados.
<b>Procedimento do Teste</b>	Demonstrar consumo de conexões concorrentes por gateways gerenciados.
<b>Evidências</b>	<p>Na aba de “Device Manager” podemos selecionar qualquer um dos equipamentos gerenciados. Quando fazemos isso, podemos ter visualização de diversas informações daquele equipamento, entre elas, a quantidade de conexões concorrentes.</p>
<b>Comentário</b>	

<b>Item de Teste - 5.4.40</b>	Alertar quando um membro estiver desconectado do cluster;
<b>Objetivo do Teste</b>	Verificar se o equipamento de gerência alerta quando um membro estiver desconectado do cluster.



<b>Configuração do Teste</b>	Demonstrar alerta de equipamento indisponível.
<b>Procedimento do Teste</b>	Demonstrar alerta de equipamento indisponível.
<b>Evidências</b>	<p>Na aba de "Device Manager" podemos selecionar qualquer um dos equipamentos gerenciados. Quando fazemos isso, podemos ter visualização de diversas informações daquele equipamento, entre elas, o estado dos clusters.</p> 
<b>Comentário</b>	

<b>Item de Teste - 5.4.42</b>	Suportar rollback de configuração para a última configuração salva e do sistema operacional para a última versão local;
<b>Objetivo do Teste</b>	Verificar se o equipamento de gerência suporta rollback de configuração.
<b>Configuração do Teste</b>	Demonstrar rollback de configuração.
<b>Procedimento do Teste</b>	Demonstrar rollback de configuração.
<b>Evidências</b>	<p>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</p> 





	<div data-bbox="523 331 1070 577"><p>System Information</p><table><tr><td>Host Name</td><td>FMG-VM64</td></tr><tr><td>Serial Number</td><td>FMG-VM0A17001174</td></tr><tr><td>Platform Type</td><td>FMG-VM64</td></tr><tr><td>HA Status</td><td>Standalone</td></tr><tr><td>System Time</td><td>Thu Mar 16 16:41:20 2023 GMT-3</td></tr><tr><td>Firmware Version</td><td>v7.2.2-build1334 230201 (GA)</td></tr><tr><td>System Configuration</td><td>Last Backup: Tue Mar 14 14:21:00 2023</td></tr><tr><td>Current Administrators</td><td>admin / 1 in total</td></tr><tr><td>Up Time</td><td>2 days 2 hours 11 minutes 58 seconds</td></tr><tr><td>Administrative Domain</td><td></td></tr><tr><td>FortiAnalyzer Features</td><td></td></tr></table></div> <p data-bbox="523 618 1353 645">Caso haja a necessidade basta apertar a tecla de "Restore" e importar a configuração desejada.</p> <div data-bbox="523 680 1353 1189"><p>System Configuration      Last Backup : Tue Mar 14 14:21:00 2023</p><p><b>Restore System</b></p><p>Upload file by drag &amp; drop here or <b>Browse</b></p><p>Password <input type="password"/> Maximum password length: 63</p><p><input checked="" type="checkbox"/> Overwrite current IP, routing and HA settings</p><p><input checked="" type="checkbox"/> Restore in Offline Mode</p><p><b>OK</b>      Cancel</p></div>	Host Name	FMG-VM64	Serial Number	FMG-VM0A17001174	Platform Type	FMG-VM64	HA Status	Standalone	System Time	Thu Mar 16 16:41:20 2023 GMT-3	Firmware Version	v7.2.2-build1334 230201 (GA)	System Configuration	Last Backup: Tue Mar 14 14:21:00 2023	Current Administrators	admin / 1 in total	Up Time	2 days 2 hours 11 minutes 58 seconds	Administrative Domain		FortiAnalyzer Features	
Host Name	FMG-VM64																						
Serial Number	FMG-VM0A17001174																						
Platform Type	FMG-VM64																						
HA Status	Standalone																						
System Time	Thu Mar 16 16:41:20 2023 GMT-3																						
Firmware Version	v7.2.2-build1334 230201 (GA)																						
System Configuration	Last Backup: Tue Mar 14 14:21:00 2023																						
Current Administrators	admin / 1 in total																						
Up Time	2 days 2 hours 11 minutes 58 seconds																						
Administrative Domain																							
FortiAnalyzer Features																							
<b>Comentário</b>																							

## 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);

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

[www.nct.com.br](http://www.nct.com.br)



### 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 throughput 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;

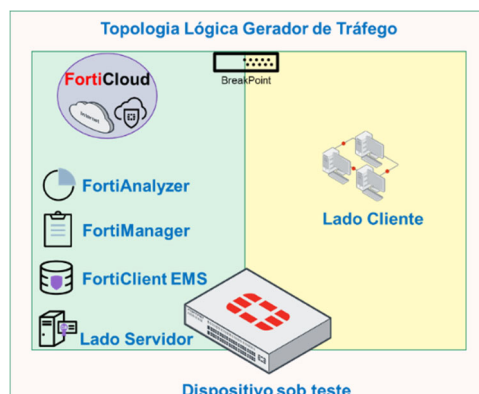
### 8.1.4. CONEXÕES CONCORRENTES:

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)

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

[www.nct.com.br](http://www.nct.com.br)



- Todas as assinaturas de: IPS, antivírus e aplicações ativas com base atualizada no momento do teste
- Funcionalidades de bypass desativadas, sendo apresentada no momento do teste as saídas dos seguintes comandos:
  - Antivirus
  - config system global
  - get | grep av-failopen
  - >> resultado esperado:
  - av-failopen: off
  - av-failopen-session : disable
- IPS
  - config ips global
  - get | grep fail-open
  - resultado esperado
  - fail-open : disable
  - get |grep database
  - resultado esperado
  - database : extended
- Mecanismos de alívio de fila desativados
- Envio de malware e tráfegos de ataque
- Evidências utilizadas na comprovação de pleno atendimento editalício:
  - Telas dos appliances sob teste
  - Telas do gerador
  - Logs de bloqueio visando demonstrar o bloqueio de conteúdo malicioso nas funcionalidades de Antivírus e IPS durante o período de curso do teste

#### 8.2.1.2. TESTE 02 – IPSEC VPN

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

#### 8.2.1.3. TESTE 03 – NOVAS CONEXÕES POR SEGUNDO

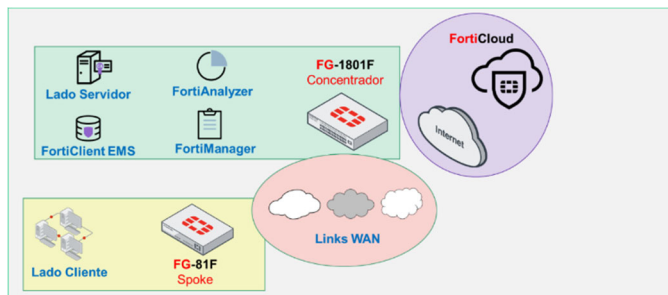
- Fluxo em HTTP 64 bytes
- Janela de teste composta por duas fases sendo:
  - Rampa de subida com tempo inferior a 1 minuto que não será considerada para aferição;
  - Curso após estabilização com tempo de 5 minutos, sendo considerado para aferição.
- Foco em abrir e fechar conexões
- Conexões TCP encerradas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

#### 8.2.1.4. TESTE 04 – CONEXÕES SIMULTÂNEAS

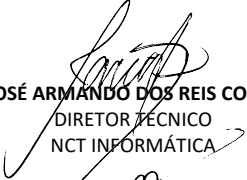
- Fluxo em HTTP 64 bytes
- Janela de teste composta por duas fases sendo:
  - Rampa de subida com tempo inferior a 1 minuto que não será considerada para aferição;
  - Curso após estabilização com tempo de 5 minutos, sendo considerado para aferição.
- Conexões TCP serão mantidas abertas como requisitado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

#### 8.2.1.5. TESTE DE FUNCIONALIDADES

#### 8.2.2. TOPOLOGIA



Brasília/DF, 23 de junho de 2023

  
JOSÉ ARMANDO DOS REIS COSTA  
DIRETOR TÉCNICO  
NCT INFORMÁTICA

  
CRYSTINE JÓRANHEZON RODRIGUES  
GERENTE DE DESENVOLVIMENTO DE NEGÓCIOS  
NCT INFORMÁTICA

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

[www.nct.com.br](http://www.nct.com.br)