



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 criaçã	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.					criar novas hecidas.
	1 – Navegando por já conhecidas pela I	Security Profiles Fabricante.	> Application sign	<b>atures</b> é possív	el visualizar as	assinaturas
	2 – Navegando por s assinaturas para ap	Security Profiles > licações não conf	> Application signa necidas pela fabric	<b>tures &gt; Create</b> ante.	<b>New</b> é possíve	l criar novas
Evidências	Dashboard     Dashboard     Network     Network     Policy & Objects     Security Profiles     AnthVirus     Web Filter	2414 Test	Category Network.Servi Storage.Backup Collaboration General.Inter Video/Audio Business	4 Technology Browser-Based Client-Server Network-Prot. Peer-to-Peer	4 2414 Tetal	Risk Low Medium Information High Critical
	DNS Filter	+ Create New - 🖋 Edit	Delete Search		Q	Signature Group
	Application Control	Name 🎙	Category 0	Technology 0	Popularity 0	Risk 0
	File Filter	Application Signature 2414				
	SSL/SSH Inspection	© 1kxun	Video/Audio	Client-Server	***	
	Application Signatures ☆	2Safe	Storage.Backup	Browser-Based Browser-Based	*****	
	Web Rating Overrides	2Safe_File.Download	Storage.Backup	Browser-Based	***	
	Web Profile Overrides	2Safe_File.Upload	Storage.Backup	Browser-Based	****	
	VPN	2ch	Social.Media	Browser-Based Browser-Based	****	
	☆ WiFi & Switch Controller >	2shared_File.Download	Storage.Backup	Browser-Based	****	
	System >	2shared_File.Upload	Storage.Backup	Browser-Based	***	
	Security Fabric	⊘ 3PC	Network.Service	Network-Protocol	****	
		V Hoyne	- Storage.backup	Client-Server		
		ASync_File.Upload	Storage.Backup	Browser-Based	****	



	🙆 Dashboard 🔷 🔸	New Application Signature	
	Image: Solubarid     >       Image: Network     >	NewApplication Signature  Name Comment: 0/63  Signature  OK Cance	FortiGate  Caderno_Teste_SEDUC  Additional Information  C Online Guides  Relevant Documentation  Hot Questions at FortiAnswers  Join the Discussion
Comentário			

#### 5.3.6 IDENTIFICAÇÃO DE USUÁRIOS:

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

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





	Caderno_Teste_SEDUC •	≡ <b>Q</b>					
	Dashboard	Edit Policy					
		-					
	Policy & Objects 🗸 🗸	Name 🚯	Acesso_Internet_Servidore	es .			
	Firewall Policy ☆	Incoming Interface	⊐⊄ lan	-			
	IPv4 DoS Policy	Outgoing Interface	Internet_VIVO (wan1)	•			
	Addresses	Source	Rede_192.168.1.0/24	×			
	Internet Service Database		GRP_Servidores_Seduc	×			
	Services Schedules	Destination	🗐 all 🕇	×			
	Virtual IPs	Schedule	Co always	•			
	IP Pools	Service	HTTP	×			
	Protocol Options		HTTPS	×			
	Traffic Shaping	Action					
	Security Profiles	Action	ACCEPT & DENY				
	⊒ VPN >	Firewall/Network C	Options				
	Leser & Authentication	NAT	•				
	☆ WiFi & Switch Controller >	IP Pool Configuration	Use Outgoing Interfac	ce Address Use Dyna	mic IP Pool		
	System >	Preserve Source Po	rt 🛈				
	Security Fabric	Protocol Options	PROT default	▼ 6 <sup>4</sup>			
	Log & Report >	Security Profiles					
		AntiVirus	Acesso_Servidor	es_WEB 🔻 🖋			
		Web Filter	C WEB Acesso_Servidor	es_WEB 🔻 🖋			
		DNS Filter					
		Application Control	APP Acesso_Servidor	es_Web 🔻 🖋			
		IPS					
		File Filter					
		4				OF	<
	Cademo_Teste_SEDUC			•	HA: Prim	iry <u>≗</u> •≻_0•	- <b>θ</b> admin •
	Network     Name	Source	Destination Schedule Se	rvice Action N	AT Security Profiles	La Export* Interface Pa	Bytes
	Particy & Cojects           Pirewall Policy           IPv4 Dos Policy           Accesso_Internet	t. VIVO (want) 🕗	🖸 all 🗔 always 😡 A	ALL 🗸 ACCEPT 💿 Eni	abled was monitor-all	© All	08
	Addresses Internet Service Database Services Acesso_Internet_Service	idores @ GRP_Servidores_Seduc	🖻 all 🐻 always 😡 H	TTP VACCEPT © End	abled Acesso_Servidores_WEB	U UTM	0.8
	Schedules Virtual IPs		Q1		Are Acesso_Servidores_WEB Are Acesso_Servidores_Web an certificate-inspection		
	IP Pools   Protocol Ontinee  Rentocol Ontinee  R	interface (sst.root)34 kan 🚯					
	Traffic Shaping						
	User & Authentication     WIFL& Switch Controller						
	♦ System >						
	L≝ Log & Report →						
	EXISTING AND South Relations					Giu	pdated: 10:47:28 C
	v)24					2010	
Comentário	Fonte:	https://a	docs fortinet con	n/document/	/FortiGate/7 2	4/adminis	stration-
concentario	guide/656084/firow	all-nolicy		i, accument,	10110010/7.2.	i, aunini	
	guide/050004/IIIeWa	an-policy					

Item de Teste - 5.3.6.2Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;Objetivo do TesteValidar se a ferramenta possibilita integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticasConfiguração do TesteCriar duas regras NGFW com filtros distintos de grupos do ADProcedimento do TestePara realizar esse teste é necessário primeiro realizar a integração do AD com o FortiGate da forma que está descrita no item "5.3.5.14" deste documento.Após ter realizado a integração, basta incluir os usuários e grupos LDAP nas políticas, para		
Objetivo do Teste       Validar se a ferramenta possibilita integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas         Configuração do Teste       Criar duas regras NGFW com filtros distintos de grupos do AD         Procedimento do Teste       Para realizar esse teste é necessário primeiro realizar a integração do AD com o FortiGate da forma que está descrita no item "5.3.5.14" deste documento.         Após ter realizado a integração, basta incluir os usuários e grupos LDAP nas políticas, para	Item de Teste - 5.3.6.2	Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
de usuários e grupos permitindo granularidade de controle/políticas         Configuração do Teste       Criar duas regras NGFW com filtros distintos de grupos do AD         Procedimento do Teste       Para realizar esse teste é necessário primeiro realizar a integração do AD com o FortiGate da forma que está descrita no item "5.3.5.14" deste documento.         Após ter realizado a integração, basta incluir os usuários e grupos LDAP nas políticas, para	Obietivo do Teste	Validar se a ferramenta possibilita integração com Microsoft Active Directory para identificação
Configuração do Teste       Criar duas regras NGFW com filtros distintos de grupos do AD         Procedimento do Teste       Para realizar esse teste é necessário primeiro realizar a integração do AD com o FortiGate da forma que está descrita no item "5.3.5.14" deste documento.         Após ter realizado a integração, basta incluir os usuários e grupos LDAP nas políticas, para		de usuários e grupos permitindo granularidade de controle/políticas
Configuração do Teste       Criar duas regras NGFW com filtros distintos de grupos do AD         Procedimento do Teste       Para realizar esse teste é necessário primeiro realizar a integração do AD com o FortiGate da forma que está descrita no item "5.3.5.14" deste documento.         Após ter realizado a integração, basta incluir os usuários e grupos LDAP nas políticas, para		de usuarios e grupos permitinuo granularidade de controle/ponticas
Procedimento do Teste       Para realizar esse teste é necessário primeiro realizar a integração do AD com o FortiGate da forma que está descrita no item "5.3.5.14" deste documento.         Após ter realizado a integração, basta incluir os usuários e grupos LDAP nas políticas, para	Configuração do Teste	Criar duas regras NGFW com filtros distintos de grupos do AD
Procedimento do Teste       Para realizar esse teste é necessário primeiro realizar a integração do AD com o FortiGate da forma que está descrita no item "5.3.5.14" deste documento.         Após ter realizado a integração, basta incluir os usuários e grupos LDAP nas políticas, para		
Procedimento do Teste       Para realizar esse teste é necessário primeiro realizar a integração do AD com o FortiGate da forma que está descrita no item "5.3.5.14" deste documento.         Após ter realizado a integração, basta incluir os usuários e grupos LDAP nas políticas, para		
Procedimento do Teste       Para realizar esse teste é necessário primeiro realizar a integração do AD com o FortiGate da forma que está descrita no item "5.3.5.14" deste documento.         Após ter realizado a integração, basta incluir os usuários e grupos LDAP nas políticas, para		
forma que está descrita no item "5.3.5.14" deste documento. Após ter realizado a integração, basta incluir os usuários e grupos LDAP nas políticas, para	Procedimento do Teste	Para realizar esse teste é necessário primeiro realizar a integração do AD com o FortiGate da
forma que está descrita no item "5.3.5.14" deste documento. Após ter realizado a integração, basta incluir os usuários e grupos LDAP nas políticas, para		
Após ter realizado a integração, basta incluir os usuários e grupos LDAP nas políticas, para		forma que está descrita no item "5.3.5.14" deste documento.
Após ter realizado a integração, basta incluir os usuários e grupos LDAP nas políticas, para		
Após ter realizado a integração, basta incluir os usuários e grupos LDAP nas políticas, para		
		Após ter realizado a integração, basta incluir os usuários e grupos LDAP nas políticas, para
l regular o controlo de queis golicações corão liberadas para esso grupo ou usuário		realizar o controlo do quais anlicações serão liberadas para esse grupo ou usuário
Tealizar o controle de quais aplicações serao liberadas para esse grupo ou usuario.		realizar o controle de quais aplicações serao liberadas para esse grupo ou usuario.



Evidências	1 - Integração com AD via LDAP	
	Edit LDAP Server	1.1
	Name     AD-SEDUC       Server IP/Name     192.168.3.156       Server Port     389       Common Name Identifier     sAMAccountName       Distinguished Name     dc=trainingAD,dc=trainingAD,dc=lab       Exchange server     Image: Simple Anonymous Regular       Username     victor.merli@trainingAD.training.lab       Password     Change       Secure Connection     Successful       Test Connectivity     Successful	Fr A
	OK Cancel 2 - Criação de um novo grupo no Firewall que utilizando a integração com o AD.	
	Writi & Switch Controller       >          Writi & Switch Controller        >          Writi & Switch Controller        >          Writi & Switch Controller        >          Writi & Switch Controller        >          Writi & Switch Controller        >          Writi & Switch Controller        >          Writi & Switch Controller        >          Writi & Switch Controller        >          Socurity Fabric:        >          Writi & Seport        >	
	3 – Navegando por Policy & Objects > Firewall Policy é possível realizar a criação de re utilizando como origem o grupo criado com a integração do AD	egras



	Caderno_Teste_SEDUC •	≣ Q.					
	Dashboard	Edit Policy					
	✤ Network >						
	🖹 Policy & Objects 🛛 🗸	Name 🚯	Acesso_Internet_Servidores				
	Firewall Policy ☆	Incoming Interface	⊐‡ lan	-			
	IPv4 DoS Policy	Outgoing Interface	Internet_VIVO (wan1)	-			
	Addresses	Source	Rede_192.168.1.0/24	×			
	Internet Service Database		GRP_Servidores_Seduc	×			
	Services	Destination	🔲 all	×			
	Schedules		+				
	Virtual IPs	Schedule	o always	•			
	IP Pools	Service	HTTP HTTPS	×			
	Protocol Options		+				
	Traffic Shaping	Action	✓ ACCEPT Ø DENY				
	Security Profiles						
	₩ VPN >	Firewall/Network O	ptions				
	Ser & Authentication >	NAT	•				
	☆ WiFi & Switch Controller >	IP Pool Configuratio	n Use Outgoing Interface A	Address Use Dynamic	IP Pool		
	System >	Preserve Source Por					
	Security Fabric	Protocol Options	PROT default	- Ø			
	Log & Report >	Security Profiles					
		AntiVirus	Acesso Servidores	WEB 🔻 🖋			
		Web Filter	C WEB Acesso_Servidores	WEB 🔻 🖋			
		DNS Filter	0				
		Application Control	C APP Acesso_Servidores_	Web 🔻 🖋			
		IPS					
		File Filter					
	FUBTIDET					ОК	
	v/.2.4						
	Cademo Teste SEDUC  Cademo Teste SEDUC  Cademo Teste Set  Cademo	B 3 Delete Q. Policy lookup	Search	9	HA: Prima	ry	Q • ⊕ admin •
	Network     Nime     Nime	Source	Destination Schodule Service	Action NAT	Security Profiles	Log B	lytes
	Firewall Policy ☆ 🖸 od lan → 🖄 Internet	VTVD (wan1) 🥑	Dall Galways GALL	✓ ACCEPT Senabled	monitor-all	O All 00	8
	Addresses	Rote_192.168.1.0/24			hinck high risk		
	Internet Service Database Acesso_Internet,Service	ores GRP_Servidores_Seduc Rede_192.160.1.0/24	all  all  blueys  blu	ACCEPT © Enabled	Acesso_Servidores_WEB	U UTM 08	8
	Schedules Virtual IPs				Ave Acesso_Servidores_Web		
	IP Pools   Protocol Onlines  Protocol Onlines  II Interface	ierface (ssl.rool) -24 lan 🕤					
	Traffic Shaping						
	User & Authentication     WIFL& Switch Controller						
	\$ System →						
	Les & Report						
	FERTINET v7.24					C Updat	led: 10:47:28 C
Comentário							

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



	A integração não necessita da instalação de nenhum software no Active Directory e nem nas			
Evidências	Conectando o FortiGate ao Active Directory			
	Edit LDAP Server			
	Name AD-SEDUC	FC		
	Server Port 389	A		
	Common Name Identifier sAMAccountName			
	Exchange server			
	Bind Type Simple Anonymous Regular			
	Username victor.merli@trainingAD.training.lab Password Change	C		
	Secure Connection			
	Connection status Successful			
	Test User Credentials			
	OK Cance	I		
	LDAP Distinguished Name Query			
	0			
	Image: Characterization         Image: Characterization			







	Gaderno_Teste_SEDUC      ✓		
	Dashboard > Users/Groups Creati	on Wizard	
	Network     Vser Type	2 LDAP Server > 3 Remote Users	
	Policy & Objects     LDAP Server	AD-SEDUC -	
	Security Profiles		
	Luser & Authentication ∽		
	User Definition 🏠		
	User Groups		
	Guest Management		
	EDAP Servers		
	Single Sign-On		
	Authentication Settings		
	FortiTokens		
	☆ WiFi & Switch Controller >		
	System		
	Lid Log & Report >		
	<u>≡ Q</u>		
	Users/Groups Creation Wizard		
	🗸 User Type 🔪 🗸 LDAP Server 🔪 3 Remo	ote Users	8
	2	Custom I DAD filter (abiast Classes)	Ma
	Show autotraa	Hide unselectable entries	С
	Show subtree		0
	dc=trainingAD,dc=training,dc=lab	Add All Results Search	Q
		Users Custom Selected	
		ID \$	Name 🗘 😞
		ADadmin	ADadmin S
		Administrator	Administrator
		aduser1	aduser1
		aduser2	aduser2
		aluno	aluno
		< ems	ems
		<ol> <li>flavio</li> </ol>	flavio
		fsso	fsso
		<ol> <li>fulano</li> </ol>	fulano
		Guest	Guest
		<ol> <li>guilherme.reis</li> </ol>	guilherme.reis
		<ol> <li>jayr</li> </ol>	Jayr JD. Daltro
		krbtgt	krbtgt
		odisseu	odisseu
		rodrigo	rodrigo
			0% 19
		_	
			< Back Submit Cancel
Comentário			

#### 5.3.7 SISTEMA DE PREVENÇÃO DE INTRUSÃO - IPS:

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

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



Evidências	Dentro de uma polític	a de segurança podemos notar a presença do Filtro IPS.
	New Policy	
	Name	Filtro_IPS
	Incoming Interface	▼
	Outgoing Interface	▼
	Source	+
	Destination	+
	Schedule	To always
	Service	+
	Action	✓ ACCEPT Ø DENY
	Firewall/Network O	ptions
	NAT	C
	IP Pool Configuration	Use Outgoing Interface Address Use Dynamic IP Pool
	Preserve Source Por	t 🛈
	Protocol Options	PROT default 🔻 🖋
	Security Profiles	
	AntiVirus	
	Web Filter	
	DNS Filter	0
	Application Control	
	IPS	
	File Filter	
	E dentro desse perfil como também o CVE dela.	de segurança podemos ter acesso a todas as assinaturas que ele conhece, daquela vulnerabilidade, a ação padrão e por fim o grau de severidade



Edit	P Add Signatures						×
Nar Cor Bio	Type Action Packet logging Status Filter <b>3</b>	Filter Signature Default Enable Disable Finable Disable Sty	Default				
	Search			Q			
	Ν	lame ≑	Severity 🖨	Target 🗘	OS ≑	Action 🗘	CVE-ID \$
	IPS Signature	5.655					0
	3Com.3CDaemor	h.FTP.Server.Buffer.Over		Server	Windows	Ø Block	CVE-2005-0277
	3Com.Intelligent.	Management.Center.Info		Server	Windows	Ø Block	
Bot	3Com.OfficeConr	nect.ADSL.Wireless.Fire		Server	Linux	Ø Block	
Sca	3S.Pocknet.VMS./	ActiveX.Control.Buffer.O		Client	Windows	Ø Block	CVE-2014-9263
	3ivx.MPEG4.File.	Processing.Buffer.Overfl		Client	Windows	Ø Block	CVE-2007-6401
	427BB.Cookie.Ba	sed.Authentication.Bypass		Server	Other	Ø Block	CVE-2006-0153
	427BB.Showthree	ad.PHP.ForumID.Parame		Server	Other	Ø Block	CVE-2006-0154
	A32S.Botnet			Server Client	All	Ø Block	
	AAEH.Botnet			Server	All	Ø Block	
							0% 5.655
			OF	Car	ncel		
Comentário							

Item de Teste - 5.3.7.2	A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas, anomalias de protocolos, controle de aplicações;								
Objetivo do Teste	Validar se a solução de IPS possuí os seguintes mecanismos de detecção: assinaturas, anomalias de protocolos, controle de aplicações.								
Configuração do Teste	Demonstrar na configuração de regra NGFW de IPS contendo: assinaturas, anomalias de protocolos, controle de aplicações;								
Procedimento do Teste	Demonstrar na configuração de regra NGFW de IPS contendo: assinaturas, anomalias de protocolos, controle de aplicações;								
Evidências	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.								
	E Q HA Primary Provide Administration Provide								
	+ Create New & Edit 🗇 Delete Search		۹			Standard Package 🕚			
	Name \$	Severity \$	Target \$	OS \$	Action \$	CVE-ID \$			
	IPS Signature (5.864)		Secure	Wadows	O Block	CHE 2005 0277			
	3Com 3C Daemon ETP Server Information Disclosure		Client	Windows	Diock     Diock	CVE-2005-0277			
	3Com Intelligent Management Center Information Disclosure		Server	Windows	Pass     Block	CVC-2003-0270			
	3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS		Server	Linux	Ø Block				
	3S.Pocknet.VMS.ActiveX.Control.Buffer.Overflow		Client	Windows	Ø Block	CVE-2014-9263			
	3ivx.MPEG4.File.Processing.Buffer.Overflow		Client	Windows	Ø Block	CVE-2007-6401			
	427BB.Cookie.Based.Authentication.Bypass		Server	Other	Ø Block	CVE-2006-0153			
	427BB.Showthread.PHP.ForumID.Parameter.SQL.Injection		Server	Other	Ø Block	CVE-2006-0154			
	A325.Botnet		Server Client	All	Ø Block				
	AAEH.Botnet		Server	All	Ø Block				
	AARC.Botnet		Server Client	All	Ø Block				
	ABBS.Audio.Media.Player.LST.Buffer.Overflow		Server	Windows	Ø Block				



lá o mecanismo	o de controle de anli	ração é feito n	olo Application (	ontrol	
Ju o meeamsme				John Off.	
Add New Override					
Type Application	Filter				
Action 🖉 Block 🕶					
Add All Results	Search		Q	Sele	ected 1 All Clo
•	Name ≑	Category 🖨	Technology 🗘	Popularity 🗘	Risk 🗘
Application Signatu	re <b>2.206</b>				
👩 1kxun		Video/Audio	Client-Server	****	
👳 1und1.	Mail	Email	Browser-Based	含含含合合	
🐞 2ch		Social.Media	Browser-Based	***	
₩ 2ch_Po	st	Social.Media	Browser-Based	黄黄合合合	
3PC	1	Network.Service	Network-Protocol	***	
4 4share	d I	Storage.Backup	Browser-Based Client-Server	****	
4 4share	d_File.Download	Storage.Backup	Browser-Based Client-Server	****	
4 4share	d_File.Upload	Storage.Backup	Browser-Based Client-Server	***	
⇒ 5ch		Social.Media	Browser-Based	***	
5- 5ch_Po	st	Social.Media	Browser-Based	***	
2 8tracks	•	Video/Audio	Browser-Based Client-Server	***	
S 9PFS	1	Network.Service	Network-Protocol	黄黄黄合合	

Item de Teste - 5.3.7.3	O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os					
	ataques emergentes sem a necessidade de reiniciar o appliance;					
Objetivo do Teste	Verificar se a ferramenta recebe e implementa em tempo real atualizações para os ataques					
	emergentes sem a necessidade de reiniciar o appliance.					
Configuração do Teste	Demonstrar tela de atualização de funcionalidades					
Procedimento do Teste	Demonstrar tela de atualização de funcionalidades					
Evidências	FortiGuard Updates					
	Scheduled updates C Every Daily Weekly Automatic					
	Improve IPS quality 1					
	Use extended IPS signature package 🕥					
	AntiVirus PUP/PUA 🚯 💽					
	Update server location ① Lowest latency locations Restrict to					
Comentário						

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



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

Item de Teste - 5.3.7.18	A solução deve possuir inspeção de tráfego HTTPS sendo possível criar bypass para sites evitando qualquer tipo de quebra de sigilo de informações pessoais:					
Objetivo do Teste	Verificar se a solução possui uma forma de dar hypass na inspeção de tráfego HTTPS					
Configuração do Testo	Vernical se a solução possul una forma de dal bypass na inspeção de tratego mirro.					
Comiguração do reste	Demonstral by-pass de littps					
Procedimento do Teste	Demonstrar by-pass de nttps					
Evidências	Exempt web sites from deep inspection					
	If you do not want to apply deep inspection for privacy or other reasons, you can exempt the session by address, category, or allowlist.					
	If you know the address of the server you want to exempt, you can exempt that address. You can exempt specific address type including IP address, IP address range, IP subnet, FQDN, wildcard-FQDN, and geography.					
	If you want to exempt all bank web sites, an easy way is to exempt the <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 Web rating override on page 1419 and Threat feeds on page 2693.					
	New SSL/SSH Inspection Profile					
	Protocol Port Mapping	FortiGate				
	Inspect all ports O	G FGDocs				
	HTTPS C 443	Additional Information				
	SMIPS C 465 POP35 C 995	API Preview				
	IMAPS C 993	(2) Documentation				
	FTPS 🔘 990	Online Help C     Video Tutorials C				
	DNS over TLS C 853					
	Exempt from SSL Inspection					
	Reputable websites 0 🕥					
	Web categories Finance and Banking ¥					
	Addresses gmail.com ×					
	Log SSL exemptions (3)					
	OK Cancel					
	If you want to exempt commonly trusted web sites, you ca Reputable websites. The allowlist includes common web	in bypass the SSL allowlist in the SSL/SSH profile by enabling sites trusted by FortiGuard.				
	Há uma funcionalidade no perfil de SSL Insp	ection chamada de "Exempt from SSL Inspection"				
	que faz esse bypass. Basta colocar os ende	reços dos sites desejados ou então por categoria,				
	como Finanças e Bancário.					



	Exempt from SSL Inspection							
	Reputable websites 🟮 🕥							
	Web categories	Finance and Banking Health and Wellness Personal Privacy	× × ×					
	Addresses	+						
	Log SSL exemptions							
	SSH Inspection Options							
	SSH deep scan 🕥							
Comentário	Fonte: FortiOS Ad https://fortinetweb.s3.amazonaws.c 11ed-96f0-fa163e15d75b/FortiOS-7	ministration Guide com/docs.fortinet.com/v2/attachn .2.3-Administration_Guide.pdf	acessado em nents/a06117ca-5fbf-					

Item de Teste - 5.3.7.22	A solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning), e impedir que os usuários acessem enderecos de domínios bloqueados ou
	maliciosos;
Objetivo do Teste	Verificar se a solução protege contra ataques do tipo envenenamento de cache DNS (DNS Cache
	Poisoning), e impedir que os usuários acessem endereços de domínios bloqueados ou
	maliciosos.
Configuração do Teste	Demonstrar assinatura DNS.Server.Cache.Poisoning
Procedimento do Teste	Demonstrar assinatura DNS.Server.Cache.Poisoning
Evidências	Threat Encyclopedia
	DNS.Server.Cache.Poisoning         Description         This indicates a possible DNS Cache Poisoning attack towards a DNS Server.         The vulnerability is caused by insufficient validation of query response from other DNS servers. This could result in DNS spoofing or redirection to other websites.         Image: Compact Comparison of the product



	Add Signatures						×
	Туре	Filter Signature					
	Action	🌣 Default 🕶					
	Packet logging	Senable Senable					
	Status	🛇 Enable 🕴 Disable 🄅 Defa	ult				
	Filter 🕚	+					
	poisoning		×Q				
		Name ≑	Severity 🖨	Target ≑	OS \$	Action ≑	CVE-ID \$
	IPS Signature	1/5864					
	Symantec.Gatewa	y,Products.DNS.Cache.Poisoning		Client	Windows Solaris	O Block	CVE-2005-0817
Comentário	Fonte:	IPS Thi	eat	Encycloped	dia	acessado	em
	https://ww	w.fortiguard.com/ency	clopedia/ips/	43827/dns-	server-cach	ne-poisoning	

#### 5.3.8 ANTI-MALWARE:

Item de Teste - 5.3.8.1	Possuir módulo de Antivírus, Antispyware e Antibot integrado no próprio appliance de											
Objetivo do Teste	Verificar se a solução possuí módulo de Antivírus, Antispyware e Antibot integrado no próprio											
	appliance de segurança e integrado à gerência centralizada de administração, monitoração e											
	logs;											
Configuração do Teste	Demor	Demonstrar regra com funcionalidades: Antivírus, Antispyware e Antibot										
Procedimento do Teste	Demor	nstrar re	egra co	m funciona	alidades: A	Antivírus, A	Antispyw	vare e An	tibot			
Evidências	Na inte	erface d	le ger	enciament	o, é possí	vel config	urar o p	erfil de l	Antivírus,	respon	isável pe	ela
	proteç	ão cont	ra víru:	s e malwar	es, bem co	omo o perf	il de IPS,	que atua	i como ur	na medi	da Antib	ot
	e aplica	á-los en	n qualo	quer polític	a selecion	ada.						
	•											
	Policy & C	Objects -		Parksen a	inter a BADOMI	Pevisions 🍙 Tools =			ADOM: SEDUC	\ <b>9</b> - (	a. Andre	nin #
	Policy Packa	iges v	+ Create N	ای کے اور دور میں اور میں	Pelete Section ~	Q. Policy Lookup	Collapse All		View M	ode - Search		a
	It Search	٩		Name	From	То	Source	Destination	Security Profiles	Schedule	Service	٠
	Eleval Firewall F	o_Teste_SEDUC Policy	1	Acesso_Internet	🖬 lan	wan1	🖀 all	🖾 all	ss. no-inspection mor default	Ta always	@ ALL	
	Installatio	on Targets	¥ 2	Acesso_VPN	sslvpn_tun_intf	🗖 lan		gmail.com	or standard no-inspection	G always	@ ALL	
	⊕ E SEDUC ⊕ P default			Ecit (2/2 Total-1)			Ze rodnigo	login.microsofton	t default			
	B Object Conf	igurations >		Implicit Deny	any	any	골 all 코 all	🖾 all 🖾 all		tā always	@ ALL	п.
	+ Create N	lew 🗸 🔀 Edit	× ∎ Del	ete 🛛 🖽 Section 🗸	Policy Lookup	Collapse All			<ul> <li>Select Entries</li> </ul>			×
	. *	Name		From	То	Source	Destination	Security	F Q Search		+ Crea	ate
	1	Acesso_Inte	rnet	🗖 lan	wan1	🗉 all	🖻 əll	550 n		S PROFILE (6)		
							gmail.com	m	AV default AV g-defau	/It		
	2	Acesso_VPI	N	sslvpn_tun_intf	🗖 lan	a rodrigo	INEL @ login.mic	rosoftonli 1801 d	ef AV g-sniffe	r-profile		
		icit (3/3 Total:1)					iogin.win	loows.net	AV sniffer-	profile		
	3	Implicit Der	ıy	any	any	🖸 all 15 all	🖻 all 🗈 all		wifi-del	ault FR PROFILE (7)		
									VIDEO FI	TER PROFILE (0	1)	
									WEB APP	R PROFILE (1)	WALL (1)	
										ION PROFILE (7	0	
									all_defa	ult		
									PS all_defa	ult_pass		
									🕫 g-defau	lt		
									g-sniffe	r-profile Jefault		
									PS high_se	curity		
									protect	_email_server		
									PS protect	http_server		
									and anner			

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



Edit AntiVirus Profile	×
НТТР	٥
SMTP	
POP3	
IMAP	
FTP	
CIFS	
APT Protection Options	
Treat Windows Executables in Email Attachments as Viruses <b>1</b>	٥
Use FortiSandbox Database 🜖	0
Include Mobile Malware Protection	
Quarantine 🚯	
Send files to FortiSandbox for inspection 🚺	
Scan strategy	Inline Post Transfer
File types	Suspicious Files Only All Supported Files
Do not submit files types and name	Click to select 🔹
patterns included in	
Send files to FortiNDR for inspection ()	0
Botnet C&C	
Scan Outgoing Connect to Botnet Sites	tions Block Disable Monitor
Na parte de logs podemos ver na s	seguinte forma:



	🔆 Fabric	>
	FortiGate	~
	Traffic	
	Event	~
	Summary	
	All Types	
	Endpoint	
	Security Rating	
	SDN Connector	
	System	
	VPN	
	User	
	E na de monitoração:	
	113         FortNew →         ■           FortNew →         ■ All Devices →         © Last 1 Hour → 15:33 - 16:33 <ul> <li>Threads →</li> <li>Threads →</li> </ul>	>_ @+ Ω(§+ A) adm Dark Mode e
	Agrificials inplification     Threat Map     Compromised Hosts     FortSandhas Detecti.	100:200 · (2018) (0 H A 5
	II: Traffic > # Shadow IT > III: Applications & Websil > & VPN >	No Data
	System     Monitor     Threat     Category     CVE ID	Threat Score  Threat Level Incidents No entry found.
Comentário		

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



Evidências	Caderno_Teste_SEDUC •	≡ Q.		
	Dashboard      FortiGuard Distribution Network			
	✤ Network >			
	Policy & Objects	License Information		
	Security Profiles	Entitlement	Status	
	₽ VPN >	FortiCare Support	Registered	Actions -
	Les & Authentication	Firmware & General Updates	<ul> <li>Licensed (Expiration Date: 2023/08/06)</li> </ul>	
		Application Control Signatures	● Version 2 Last updated 2023/03/10	Actions -
	System V	Device & OS Identification	• Version 1.00147	
	Administrators Admin Profiles	Internet Service Database Definitions	• Version 7.03100	: Actions -
	Fabric Management	Intrusion Prevention	<ul> <li>Licensed (Expiration Date: 2023/08/06)</li> </ul>	
	Settings	IPS Definitions	O Version 6.00741	Actions
	HA	IPS Engine	• Version 7.00255	
	SNMP	Malicious URLs	O Version 1.00001	
	Replacement Messages	Botnet IPs	• Version 7.03100	🔳 View List
	Feature Visibility	Botnet Domains	O Version 3.00204	🔳 View List
	Security Fabric	AntiVirus	<ul> <li>Licensed (Expiration Date: 2023/08/06)</li> </ul>	
	Log & Report >	Al Malware Detection Model	O Version 0.00000	
		AV Definitions	• Version 1.00000	O Upgrade Database
		AV Engine	• Version 6.00285	
		Mobile Malware	• Version 0.00000	
		Web Filtering	<ul> <li>Licensed (Expiration Date: 2023/08/06)</li> </ul>	
		Outbreak Prevention	Licensed (Expiration Date: 2023/08/06)	
		SD-WAN Network Monitor	A Not Licensed	Purchase -
		Security Rating	A Not Licensed	E Purchase -
Comentário	https://www.fortigua	rd.com/services/ips		

Item de Teste - 5.3.8.4	A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anorm	A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;				
Objetivo do Teste	Validar se a solução detecta e bloqueia comportamentos suspeitos ou anormais da rede					
Configuração do Teste	Criar regra de acesso NGFW de anomalia					
Procedimento do Teste	Navegando por Policy & Objects > IPv4 Dos Policy > Create New é possível criar n analisando o tráfego e detectam ou bloqueiam anomalias suspeitos da rede.	regras que				
Evidências	Streetere       The set of SEDUC       E       Q         Image: Set of Security Products       New Policy       New Policy         Image: Set of Security Products       New Policy       New Policy         Image: Set of Security Products       Set of Security Products       Security Products         Image: Security Products       Name       Disable Block Monitor       Threshold         Image: Security Products       Name       Disable Block Monitor       Security Products         Image: Security Products       Name       Lagging Action Disable Block Monitor       Threshold         Image: Security Products       Name       Lagging Action Disable Block Monitor       Threshold         Image: Security Products       Name       Lagging Action Disable Block Monitor       Threshold         Image: Security Fradric       Name       Lagging Action Disable Block Monitor       Threshold         Image: Security Fradric       Name       Lagging Action Disable Block Monitor       Threshold         Image: Security Fradric       Name       Lagging Action Disable Block Monitor       Threshold         Image: Security Fradric       Name       Lagging Action Disable Block Monitor       10000       Itp.grc.session         Image: Security Fradric       Name       Lagging Action Disable Block Monitor       10000	Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additional Additi				
Comentário						



Item de Teste - 5.3.8.6	A solução Antibot	A solução Antibot deve possuir mecanismo de detecção em multicamadas que inclui, reputação de anderece IR LIRIS e andereces DNS e detector padrãos de comunicação e assingturas:					
Objetivo do Teste	Verificar se a soluc	Verificar se a solução Antibot deve possuir mecanismo de detecção em multicamadas que inclui.					
	reputação de end	reputação de endereço IP, URLs e endereços DNS e detectar padrões de comunicação					
	assinaturas;						
Configuração do Teste	Demonstrar regra	NGFW					
Procedimento do Teste	Demonstrar regra	NGFW					
Evidências	A solução de Antib do protocolo e a p	A solução de Antibot feita pelo IPS Filter, consiste em reputação de endereços IP, com do protocolo e a porta utilizada.					
	Botnet C&C IP Definitions			×			
	Search	Q					
	IP \$	Port 🗢	Protocol 🗢	Name ≑			
	1.9.167.36	60.489	ТСР	KillNet			
	1.10.189.133	50.855	TCP	KillNet			
	1.20.96.156	4.153	TCP	KillNet			
	1.20.97.181	34.102	TCP	KillNet			
	1.20.100.45	43.943	TCP	KillNet			
	1.20.100.111	41.480	TCP	KillNet			
	1.53.137.92	4.145	TCP	KillNet			
	1.62.2.147	18.186	TCP	KillNet			
	1.123.37.68	80	TCP	NanoCore			
	1.168.31.173	8.088	TCP	KillNet			
	1.169.224.221	16.464	UDP	ZeroAccess			
	1.169.224.228	16.464	UDP	ZeroAccess			
	1.171.19.54	3.128	TCP	KillNet			
	1.171.145.107	16.471	UDP	ZeroAccess			
	1.171.207.238	16.464	UDP	ZeroAccess			
	1.171.223.174	16.464	UDP	ZeroAccess			
	1.174.132.214	16.464	UDP	ZeroAccess			
	1.174.163.191	16.464	UDP	ZeroAccess			
	Já a parte de detec	ção de endereços DNS	e URLs é feita pelo DNS F	-ilter.			



	Botnet C&C Domain Definitions		>	<
	Search	Q		
	F	QDN \$	Name 🗢	
	moduleconnector.at		Netwire	
	fionades.com		Ramnit	
	briancrabs.cm		Tofsee	
	defeatwax.ru		Tofsee	
	hugersi.com		Tofsee	_
	lakeflex.ru		Tofsee	-
	lazystax.ru		Tofsee	-
	ovicrush.cn		Tofsee	-
	oxxyfix.xyz		Tofsee	-
	parubey.info		Tofsee	
	quadoil.ru		Tofsee	
	boombom.at		Gameover-zeus	
	donios.at		Gameover-zeus	_
	doplertool.com		Gameover-zeus	-
	hipohook.cn		Gameover-zeus	-
	lujdhsndjfks.com		Gameover-zeus	-
	lilontyp.at		Gameover-zeus	
	Πορτγρ.ατ		Galileover-zeus	_
	Name () Incoming Interface Outgoing Interface Source Destination Schedule Service Action	Política de Antibot  Política de Antibot    Accept ODENY		
	Firewaii/Network Op	DUIDINS		
	NAT			
	IP Pool Configuration	Use Outgoing Interface	Address Use Dynamic IP Pool	
	Preserve Source Port	t 🛈		
	Protocol Options	PROT default	- <i>d</i>	
	Security Profiles			
	AntiVirus			
	Web Filter			
	DNIS Eilter		~ ^	
	DNS Filter	Antibot	a da	
	Application Control	•		
	IPS	C Antibot	▼ 6 <sup>*</sup>	
	File Filter			
Comentário				



Item de Teste - 5.3.8.9	A solução deve possu	uir na própria interface	de gerên	cia, gráfico conte	endo informações em		
	tempo real sobre as a	tempo real sobre as atividades recentes de malwares detectados na solução;					
Objetivo do Teste	Verificar se a solução	possuí na própria interfa	ce de ger	ência gráfico cont	endo informações em		
-	tempo real sobre as at	ividades recentes de ma	alwares de	etectados na soluç	:ão;		
Configuração do Teste	Demonstrar dashboar	ds de detecção de malw	ares				
Procedimento do Teste	Na aba "Dashboard" t	emos a opção de selecio	nar "Secu	rity".			
	Lá podemos ter aces	so a diversas funcional	idades re	ferentes a visuali	zação de eventos de		
	seguranca detectados	nela solução.	idddes ie				
Fvidências	₩ Caderno,Teste,SEDUC = Q	pela selaguel		HA: Prin	nary 👜 • >_ 🕢 • 🗘 • 😝 admin •		
	Dashboard						
	Security : FortiClient De	tected Vulnerabilities	i • Te	op Threats by Threat Level	🖲 ihour* 🖸 🗜		
	Users & Devices			Threat	Threat Level 🛩		
	WiFi +	$\bigcirc$		No results			
	FortiView Sources FortiView Destinations						
	FortiView Applications	Scanned					
	ForthView Policies				0		
	FortiView Sessions Top Vulnerable	Fort/Wav Sestions         Top Vulnerable Endpoint Devices by Detected Vulnerabilities         © I •         Host Scan Summary         I •           SSL VPM Monitor         Device         Detected Vulnerabilities •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •         I •					
	SSL-VPN Monitor						
	Quarantine Monitor	$\left( \begin{array}{c} 0 \end{array} \right)$					
	Compromised Hosts	Comprovided Hosts					
	+ + Network >						
	Policy & Objects     Security Profiles		0	<u> </u>			
Comentário							

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



Edit DNS Filter Profile	
Name Comments	default Default dns filtering. 22/255
Redirect botnet C&C requests to Blo	80000 domains in <u>botnet package</u>
Enforce 'Safe Search' on Google, Bing	g, YouTube 🗨
Pre-configured filters Custom C	G PG-13 R
Name 🖨	Action 🗢
<ul> <li>Security Risk 6 9 6</li> <li>Malicious Websites</li> </ul>	Redirect to Bloc
Phishing Spam URLs	<ul><li>Redirect to Bloc</li><li>Redirect to Bloc</li></ul>
Dynamic DNS Newly Observed Domain	<ul><li>Redirect to Bloc</li><li>Redirect to Bloc</li></ul>
Newly Registered Domain	C Redirect to Bloc
 Unrated	⊘ 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 Policy & Objects > Firewall Policy > Security
	Profiles e no campo SSL Inspection selecionar Deep-Inspection, no fluxo da política selecionada
	o firewall irá realizar a inspeção de pacotes.



Evidências	Security Profiles		
	AntiVirus		
	Web Filter	0	
	DNS Filter		
	Application Control	3	
	Application Control		
	IPS		
	File Filter		
	SSL Inspection	SSL deep-inspection 💌 🖋	
	Decrypted Traffic N	Mirror 🔘	
	Edit SSL/SSH Inspection Profile	e	
	Sachia CCL inspection Options	Multiple Oliverte Comerchine to Multiple Commercia	
	Enable SSL inspection of	Multiple Clients Connecting to Multiple Servers Protecting SSL Server	
	Inspection method	SSL Certificate Inspection Full SSL Inspection	
	CA certificate 🔺	📭 Fortinet_CA_SSL 🔹 🕹 Download	
	Blocked certificates 🟮	Allow Block 🗮 View Blocked Certificates	
	Untrusted SSL certificates	Allow Block Ignore 🗮 View Trusted CAs List	
	Server certificate SNI check 🤅	Enable Strict Disable	
	Enforce SSL cipher compliance	e 🛈	
	Enforce SSL negotiation compl	pliance 🕥	
	RPC over HTTPS	0	
	Protocol Port Mapping		
	Inspect all ports 🕥		
	HTTPS 💽 443		
	SMTPS 💽 465		
	POP3S 🔘 995		
	IMAPS 🔘 993		
	FTPS 💽 990		
	DNS over TLS 🕥 853		
	Exempt from SSL Inspection		
	Reputable websites 🟮 🕥		
	Web categories	Finance and Banking X Health and Wellness X	
	Addresses	adobe     ×       Adobe Login     ×	
		Return	
Comentário			

Item de Teste - 5.3.8.12	Deve ser capaz de inspecionar protocolos SMB/CIFS, SMTP, HTTP e HTTPS;	
Objetivo do Teste	Validar se a ferramenta é capaz de inspecionar protocolos SMB/CIFS, SMTP, HTTP e HTTPS;	
Configuração do Teste	Demonstrar inspeção: SMB/CIFS, SMTP, HTTP e HTTPS	
Procedimento do Teste	A inspeção de protocolos é feita de duas formas. A primeira é utilizando o Security Profile c	
	Antivírus, onde é possível inspecionar os protocolos HTTP, SMTP, POP3, IMAP, FTP, CIFS. A	



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



	Edit SSL/SSH Inspect	tion Profi	le			
	SSL Inspection Opti	ons				
	Enable SSL inspection	on of	Multiple Clients Co Protecting SSL Serv	Multiple Clients Connecting to Multiple Servers Protecting SSL Server		
	Inspection method		SSL Certificate Insp	SSL Certificate Inspection Full SSL Inspection		
	CA certificate 🔺		Fortinet_CA_SSL		<ul> <li>Lownload</li> </ul>	
	Blocked certificates	0	Allow Block	View Blocked Ce	ertificates	
	Untrusted SSL certi	ficates	Allow Block Ign	ore 🔳 View Tr	usted CAs List	
	Server certificate Si	NI check	Enable Strict Di	sable		
	Enforce SSL cipher	complian	ce 🛈			
	Enforce SSL negotia	ation com	pliance 🕕			
	RPC over HTTPS					
	Protocol Port Mapp	oing				
	Inspect all ports 🔾					
	HTTPS	443				
	SMTPS	465				
	POP3S	995				
	IMAPS C	993				
	FTPS C	990				
	DNS over TLS	853				
	Exempt from SSL In	spection				
	Reputable websites	i 🛈 🕕				
	Web categories		Finance and Banking Health and Wellness +	× ×		
	Addresses		<ul><li>adobe</li><li>Adobe Login</li></ul>	××		
				Return		
Comentário						-

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



	Fdit AntiVirus Profile			
	Name default			
	Comments Scan files and block viruses. 29/255			
	AntiVirus scan 🚯 🕥			
	Inspected Protocols			
	HTTP 🕥			
	SMTP 🕥			
	РОРЗ 🕥			
	IMAP 🕥			
	FTP 🕥			
	CIFS 🕥			
	APT Protection Options			
	Treat Windows executables in email attachments as viruses			
	Send files to FortiSandbox for inspection 🚯 🛕 🕥			
	Include mobile malware protection			
	Quarantine 🕄 🔹 🕕			
	Virus Outbreak Prevention 😈			
	Use FortiGuard outbreak prevention database			
	Use external malware block list			
	Use EMS threat feed 🚯 🔹			
	External malware block list			
	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.			
	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			
	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.			
Comentário	https://docs.fortinet.com/document/fortigate/7.2.0/administration-guide/254346			

#### 5.3.9 AMEAÇAS AVANÇADAS PERSISTENTES - APT:

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

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



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



7.2.4 <b>↓</b>	<b>О</b> Сору	Link 🕹 Download PDF
Configu	ring sandboxing	
The Security	/ Fabric supports the following FortiSandb	pox deployments.
Туре	Description	Requirements
FortiGate Cloud Sandbox	Files are sent to Fortinet's Cloud Sandbox cluster for processing.	<ul> <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 \u2224		Copy Link
Using Forti Antivirus profiles can supplement This augments ti FortiSandbox ca any known virus EortiSandbox i	Sandbox post-transfer scanning with antivin can submit potential zero-day viruses to FortiSandbox for inspec its own antivirus database with FortiSandbox's threat intelligence he FortiGate antivirus with zero-day detection. In be used with antivirus in both proxy-based and flow-based insp es. When a match is found, the file is tagged as known malware. Just the following options:	US tion. Based on FortiSandbox's analysis, the FortiGate to detect files determined as malicious or suspicious, pection modes. The FortiGate first examines the file for if no match is found, the files are forwarded to
All Support     Suspicious     When using     None: files a     For more inform	ed Files: all files matching the file types defined in the scan profile of Files Only: files classified by the antivirus as having any possibility FortiGate Cloud Sandbox, we recommend selecting this option of are not forwarded to FortiSandbox. ation, see Configuring sandboxing.	of the FortiSandbox are forwarded. of active content are forwarded to FortiSandbox. due to its submission limits.
To enable FortiS 1. Go to Secur 2. Create, edit 3. In the APT F	andbox inspection in an antivirus profile: ity Profiles > AntiVirus. , or clone an antivirus profile. Protection Options section, set Send Files to FortiSandbox for Ins;	pection to either Suspicious Files Only or All Supporte



	🛧 Favorites 🔹 🔸	Edit AntiVirus Profile
	A Favorites     Deshoard     Deshoard	Edit AntWirds Profile       Name     AV SEDUC_GO       Comments     Write a comment.       Or255       JantUMis son ©     Block Monitor       Feature set     Frow-based       Inspected Protocols       HTTP ©       SMTP ©       POP3 ©       IMAP ©
	File Filter Email Filter VoIP	FTP C CIFS C
	SSL/SSH Inspection	APT Protection Options
	Application Signatures IPS Signatures Web Rating Overrides Web Profile Overrides UPPN UPPNile Overrides UPPN UPF & Switch Controller  System System System Log & Report	Treat Windows executables In email attachments as viruses <ul> <li>Construction of the second se</li></ul>
Comontário	https://docs.fortin	at com/document/EartiGate/7.2.4/administration guide/481589
Contentario	https://docs.fortin guide/660221/con	et.com/document/FortiGate/7.2.4/administration- figuring-sandboxing

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



Evidências	Dashboard      New Policy		
Evidencias	✤ Network >		Additional Information
	Policy & Objects Vame 0		API Preview
	Firewall Policy Add Favorite hterface	•	
	Addresses 🕸 Outgoing Interface	•	(2) Online Guides
	Service Database Source	+	Video Tutorials
	Schedules Schedule		Consolidated Policy Configuration
	Virtual IPs Service	+	<ul> <li>Hot Questions at FortiAnswers</li> </ul>
	IP Pools Action	✓ ACCEPT Ø DENY	Is Web Cache on the GUI?
	Protocol Options		1 Answers # 0 Votes @ 262 Views  See More
	Traffic Shaping Firewall/Network Op	ptions	Sectore of
	Security Profiles > NAT	C	
	VPN      IP Pool Configuration	Use Outgoing Interface Address Use Dynamic IP Pool	
	Luser & Authentication > Preserve Source Por	t 🗇	
	WIFI & Switch Controller  Protocol Options	PROF default	
	Security Pabric Security Profiles		
	Let Log & Report > AntiVirus	0	
	WebFilter	•	
	DNS Filter	3	
	Application Control	3	
	IPS	0	
	File Filter	0	
	SSL Inspection 🛆	🚾 deep-inspection 👻 🖋	
		OK Cancel	
	Security Profiles		
	become, monico		
	AptiVirus		
	Antivirus		
	Mah Eilter		
	webFilter		
	DNIS Eiltor		
	DISFILE		
	Application Control		
	Application Control		
	IDC		
	IPS		
	File Filter		
	FileFilter		
		Г <u> </u>	
	SSL Inspection	SSL deep-inspection	▼ A <sup>2</sup>
	Decrypted Traffic Mirro	or 🕥	



Edit SSL/SSH Ins	spection Prof	ile		
SSL Inspection	Options			
Enable SSL insp	ection of	Multiple Clients Com Protecting SSL Serve	necting to Multiple Servers	
Inspection met	hod	SSL Certificate Inspe	ction Full SSL Inspection	
CA certificate	A	Fortinet_CA_SSL	🔻 📥 Downl	oad
Blocked certific	cates 📵	Allow Block	View Blocked Certificates	
Untrusted SSL	certificates	Allow Block Igno	re 🔳 View Trusted CAs List	
Server certifica	te SNI check	Enable Strict Disa	able	
Enforce SSL cip	her complian	nce 🛈		
Enforce SSL ne	gotiation com	npliance 🛈		
RPC over HTTP	PS			
Protocol Port N	/apping			
Inspect all port	s 🔿			
HTTPS	443			
SMTPS	465			
POP3S	• 995			
IMAPS	• 993			
FTPS	• 990			
DNS over TLS	853			
Event from S	SI Inspection			
Exemptition 3.				
Reputable web	sites 🔮 🌒	Finance and Danking	~	
Web categorie	S	Health and Wellness	×	
		+		
Addresses		adobe	×	
		Manne Fogui		
			Return	
Comentario				

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





Item de Teste - 5.3.9.6	A solução deve implementar a emulação, detecção ou bloqueio de qualquer malware e/ou código malicioso detectado;
Objetivo do Teste	Verificar se a solução implementa a emulação, detecção ou bloqueio de qualquer malware e/ou código malicioso detectado.
Configuração do Teste	Demonstrar configuração da regra com sandbox.
Procedimento do Teste	É necessário habilitar essa funcionalidade em "Security Profile" e "Antivírus".
Evidências	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.



	APT Protection Options	
	Treat Windows executables (1) in email attachments as viruses	
	Send files to FortiSandbox for inspection 🕄 🗚	
	Include mobile malware protection	
	Quarantine 🕄	
Comentário		

Item de Teste - 5.3.9.7	Toda análise dever nuvem do próprio	á ser realizada de forma interna em Appliar fabricante, não sendo aceitas soluções que i	nce do próprio fabricante ou necessitem de módulos e/ou
	servidores externos	para a implementação de máquinas virtuais;	
Objetivo do Teste	Demonstrar que a	solução possui estrutura interna ou na nuver	n do fabricante para solução
	Sandbox.		
Configuração do Teste	Demonstrar relatór	ios na nuvem do fabricante Fortinet.	
Procedimento do Teste	Demonstrar relatór	ios na nuvem do fabricante Fortinet.	
Evidências	O Antivírus do Forti ambiente na nuver tomada	iGate faz o envio de códigos maliciosas para o n que faz a emulação desses códigos e retorr	FortiGate Cloud Sandbox, um na para o FortiGate a decisão
	Configuring Sand	boxing	
	The Security Fabric suppo	rts the following FortiSandbox deployments.	
	Туре	Description	Requirements
	FortiGate Cloud Sandbox	Files are sent to Fortinet's Cloud Sandbox cluster for processing.	The FortiGate must have a valid AV license.
			<ul> <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.	The FortICloud account provides access to a portal to view submissions. This is not required for the Security Fabric.     FortiCloud premium license     FortiSandbox Cloud entitlement The FortiGate and FortICloud license are registered to the same account.
	FortiSandbox Cloud FortiSandbox appliance	Files are sent to a dedicated FortiCloud hosted instance of FortiSandbox for processing. Files are sent to a physical appliance or VM, typically residing on premise, for processing.	<ul> <li>The FortICloud account provides access to a portal to view submissions. This is not required for the Security Fabric.</li> <li>FortICloud premium license</li> <li>FortISandbox Cloud entitlement</li> <li>The FortIGate and FortICloud license are registered to the same account.</li> <li>None</li> </ul>



	72.4 ↓
	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.
	<ul> <li>Suspicious Files Only: files classified by the antivirus as having any possibility of active content are forwarded to FortiSandbox.</li> <li>When using FortiGate Cloud Sandbox, we recommend selecting this option due to its submission limits.</li> </ul>
	None: files are not forwarded to FortiSandbox.
	For more information, see Configuring sandboxing.
	To enable FortiSandbox inspection in an antivirus profile:
	1. Go to Security Profiles > AntiVirus.
	2. Create, edit, or clone an antivirus profile.
	3. In the APT Protection Options section, set Send Files to FortiSandbox for Inspection to either Suspicious Files Only or All Supported
	APT Protection Options
	Treat Windows executables (1) In email attachments as viruses
	Send files to FortiSandbox for inspection 🚯 🛕 🕥
	Include mobile malware protection
	Quarantine 🕄 🛛 🕥
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	Primeiro é necessário configurar a funcionalidade "FortiGate Cloud Sandbox" no FortiGate.
	Após realizar as configurações para habilitar o Sandbox basta navegar por <b>Security Profiles</b> > <b>AntiVírus &gt; Create New &gt; APT Protection Options</b> e habilitar o envio de arquivos para a inspeção do Sandbox.
	Por último basta incluir o perfil criado no fluxo da política em que deseja realizar a inspeção.



Evidências	7.2.3 ↓	
	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.	n.
	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 match is found, the file is tagged as known malware. If no match is found, the files ar forwarded to FortiSandbox using the following options:	a re
	<ul> <li>All Supported Files: all files matching the file types defined in the scan profile of the FortiSandbox are forwarded.</li> </ul>	
	<ul> <li>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.</li> </ul>	
	Favorites       Edit AntiWink Profile         Doubboard       Name         Network       Comments         Policy & Objects       With Subsect         Security Profiles       Inspected Protocols         Web Filter       Inspected Protocols         NTTP ©       Security Provides         Security Provides       Inspected Protocols         Intrusion Prevention       Inspected Protocols         Vial Supported Time       Inspected Protocols         Veb Profile Overrides       Inspected Protocols Inspectial         Ver Profile Overrides       Son strategy Inspection         Ver Profile Overrides       Son strategy Inspection         Ver Profile Overrides       Inspected Protocol on ot submit file smatching types	
	Fig RTIDET 1/224	el



	APT Protection Options	
	Treat Windows executables (3) in email attachments as viruses	
	Send files to FortiSandbox for inspection 🚯 🖌	
	Include mobile malware protection	
	Quarantine 🚯	
Comentário	https://docs.fortinet.com/document/FortiGate/7.2.4/administration-g	uide/481589
	https://docs.fortinet.com/document/FortiGate/7.2.4/administration- guide/660221/configuring-sandboxing	

Item de Teste - 5.3.9.11	Toda a análise ou b	oloqueio de malwar	es e/ou códigos m	aliciosos deve ocorrer e	em tempo real;
Objetivo do Teste	Validar que a aplica	ação faz a análise ou	bloqueio de malw	ares e/ou códigos malio	ciosos em tempo
	real				
Configuração do Teste	Possuir 1(um) Forti	iGate com uma regr	a de firewall conte	ndo um Perfil de Antiví	rus configurado.
Procedimento do Teste	Demonstrar relató	rios no site do Fabri	icante.		
Evidências	Quando uma política é configurada para incluir um perfil de antivírus, todo o tráfego que corresponde a essa regra será submetido à filtragem desse perfil. Consequentemente, todo o tráfego que transita nessa regra no momento da sua aplicação será submetido a um processo de bloqueio em tempo real de malwares e códigos maliciosos.				
	Name	Source	Destination	Security Profiles	Hit Count
	⊐     □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □      □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □     □	D (wan1) (2)			
	Acesso_Internet	2 Rede_192.168.1.0/24	💷 all	Average         Servidores_WEB           weal         monitor-all           Average         block-high-risk           sst         certificate-inspection	199
Comentário					

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







Bashboard > Edit Address     Category Address Multicast Address     Firewall Policy     Firewall Policy     Color      Color
Network      Network      Odects      Firewall Policy      Color      The Change Color      Color      The Change Color      Color      The Change Color      Color      The Change Color      Th
Policy & Objects      Firewall Policy      Category      Address      Muticast Address      Name      Rede_192.168.10/24      Color      The Change      Color      Color      The Change      Color      C
Firewall Policy Color TO Change
Color The Change
Multicast Policy Charge Ad
IPv4 DoS Policy Type IP Range 👻
Addresses () IP Range 192.168.12-54
Interface any *
Services Comments Write a comment
Schedules (7
VirtualIts
IP Pools
Protocol Options
Traffic Sharing
A Security Profiles >
Luser & Authentication >
─     ─     ♥ WiFi & Switch Controller
✿ System >
Security Fabric >
Lag & Report >
OK Cancel
₩ Caderno Teste SEDUC
Dastboard > Edit Policy
⊕ Network     →
Policy & Objects Viane 0 Areaso Internet
Firewall Policy & Incoming Interface 21 Incoming Interface 11
Multicast Dicy Outpoint Interface U/U/O (wan1) V
IPv4 DoS Policy Source To Read 192 146 11/24 X
Addresses ECE 192168.2.0/24 × Ac
Internet Service Database Hi
Services Destination all X
Schedules Schedule always C
Virtual IPs Service Q ALL ×
IP Pools
Protocol Options Action CEPT O DENY
Traffic Shaping Last
Security Profiles Firewall/Network Options 23 Mi
L VPN NAT C 20M
LIP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool 15 Mi
Security Fabric     Security Profiles
Let Log & Report →
Web Elize
DNS Filter
Application Control C 425 Nork-Michaelik
FileFilter O
⊙ c
SSL inspection
ESIBILITET STALL OK Cancel
https://docs.fortingst.com/document/EortiGate/7.2.4/administration_guida/655094/firswall
notry#firewallPolicyBarameters

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



Evidências	Na aba "Dashboard" temos a opção de selecionar "Security".
	Dashboard
	Status Security Network Users & Devices WiFi +
	Lá podemos ter acesso a diversas funcionalidades referentes a visualização de eventos de segurança detectados pela solução.
	∰ Cademo Insta 5000 • E Q. HK Primary • >_ 0 • Q. • ⊕ admin.• 0 Dabbourd • ↓ ◆ Astronome
	State       Important State         State       Import
	rede por nível de periculosidade.
	Top Threats by Threat Level
	0 Threat Score         09:45         09:55         10:00         10:05         10:10         10:15         10:20         10:25         10:30         10:40           Threat         Threat Category         Threat Level +         Threat Score +         Sessions +
	No results



Comentário

5.4 Solução de Gerenciamento e Controle do Firewall

Item de Teste - 5.4.1	A solução deve se	er do mesmo l	abricante dos demais itens ofertados no Lote 01;	
Objetivo do Teste	Comprovar que a	solução ofert	ada é da mesma fabricante que os demais itens ofertados	i.
Configuração do Teste	Demonstrar o For	tiGate, FortiN	1anager e FortiAnalyzer que são do fabricante Fortinet.	
Procedimento do Teste	Demonstrar o F Demonstrar o For	ortiGate, For tiGate, FortiN	tiManager e FortiAnalyzer que são do fabricante Fo Janager e FortiAnalyzer que são do fabricante Fortinet.	ortinet.
Evidências	DATA SHEET Forti Available in: Appliance	TINE Mana Mana Cloud ager provinent of yo cess enable vork device e automation d with the ure and au es provide vork secu	Ides automation-driven centralized ur Fortinet devices from a single console. les full administration and visibility of ces through streamlined provisioning and tion tools. e Fortinet Security Fabric advanced securi utomation driven network operations e a solid foundation to secure and optimiz rity.	ity e
	🕄 System Settings –	≡	>_ 0+ 0 <mark>-</mark> -	A admin
	Dashboard     All ADOMs	Toggle Widget 🗸		
	Network			
	a. HA	Unit Operation	0 ¥ (	3 = ~
	Admin     Certificates	FORTINET	FortiManage	er-VM64
	Event Log			
	Task Monitor Advanced			
			Č Burlat	
			Nesurs	
		Aiert Message Console		3 = ~
		Time ©	Message ©	•
	FURTIDET		ongrae rinor tinor mage itili Yriti	

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



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



Comentário	Fonte:	FortiManager	Data	Sheet	acessado	em
	https://www.fo	ortinet.com/content/dar	n/fortinet/asse	ts/data-sheets/fe	ortimanager.pdf	

Item de Teste - 5.4.3	A solução deve s	er respons	ável pela	concentracã	o dos log	s e emis	são de r	elatório	os:	
Objetivo do Teste	Comprovar que a	Comprovar que a solução é responsável pela concentração dos logs e emissão de relatórios.						rios.		
Configuração do Teste	Acesso a um EortiAnalyzer com a conexão entre os equipamentos estabelecida.									
Procedimento do Teste	Demonstrar conf	, iguração e	ativação	o do FortiAnal	lyzer nos l	FortiGa	tes.			
Evidências	Para acessar essa funcionalidade basta acessar o "Log View".									
	· · · · · · · · · · · · · · · · · · ·									
	Log view -		=							
	1									
	• 111			a -						
	• •								$\sim$	
	L Device Mana	ger	Forti	View	1.08	View		Fab	ric Vie	~
	Device Mana	igei	1010	VICVV	LOE	view		100		••
	L									
								6	<u>x</u>	
	FortiSoC		Rep	orts	System	n Settin	gs	Mar	lageme	ent
								Ext	ension	S
	11 Log View w	=						> 0-	A	A admin 👻
	≪ Fabric v	O Last 1 Hour -	16:38:30 To 17:38:	29					2	6 II + -
	All	Add Filter							0	Q O
	FortiGate     FortiAnalyzer	# Tate/Time	Data Source ID	Event Message Event Type	Event Severity	Source IP	Destination IP	Host Name	User ID	Application
	Log Browse	1 17:34:04 2 17:33:40	FAZ-VM000	Receive an u event	information					
	Log Group	3 17:33:36	FAZ-VM000	Receive an u event	information					
		5 17:33:33	FAZ-VM000	Receive an u event	information					
		6 17:33:29	FAZ-VM000	Receive an u event	information					
		8 17:25:41	FAZ-VM000	System Perfo event	notice					
		9 17:23:16	FAZ-VM000	Receive an u event	information					
		10 17:20:41	FAZ-VM000	System Perfo event	notice					
		12 17:13:02	FAZ-VM000	Receive an u event	information					
		13 17:11:02	FAZ-VM000	event	notice					
		15 17:10:38	FAZ-VM000	Received ne event	information					
		16 17:09:59	FAZ-VM000	event	notice					
		17 17:08:29 18 17:07:41	FAZ-VM000 FAZ-VM000	event	notice					
Comentário										

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







	1					
Item de Teste - 5.4.6	Permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando					
Objetive de Teste	organização hierarquica de regras em todos os equipa	amento	S;			
Objetivo do Teste	distribuição de políticas de seguranca 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	About policies FortiManager provides administrators the ability to customize poli administrators may want to customize access and policies based requirements, or legal requirements. Within a single ADOM, administrators can create multiple policy po- customize policy packages per device or VDOM within a specific / devices within an ADOM. These policy packages can be targeted single VDOM, multiple VDOMs, or all devices within a single ADO administrator can modify or edit the policies within that package a FortiManager can help simplify provisioning of new devices, ADO existing policy packages. Na aba de "Policy & Objects "é possível criar um novo	icies within on factors ackages. ADOM, or at a single M. By defi nd keep of Ms, or VD	a their organization as they see fit. Typically, such as geography, specific security FortiManager provides you the ability to to apply a single policy package for all a device, multiple devices, all devices, a ning the scope of a policy package, an ther policy packages unchanged. OMs by allowing you to copy or clone			
	El Policy & Objects - E Policy Package -					
	Policy Packages	۷	New			
	Li Search Q	N	Clone et 🖨			
	Caderno_Teste_SEDUC		New Folder			
	Firewall Policy		Move			
	⊕ L SEDUC Edit					
	⊕					
	Object Configurations >		Policy Revision			
			Policy Check			
			Run Script			
			Export to Excel			
			Export to CSV			



	Como também, selecionar o basta acessar a guia "Install desejados.	quais equipamentos receberão ation Targets", em seguida ir er	o esse pacote recém-cria n "Edit" e selecionar os e	do. Para isto, quipamentos
	Contract modeling     Contract modeling	Lett multanoon trigets Available Entries (2)	Selected Entries (0) (2, No entry	×
Comentário	Fonte: FortiManage https://fortinetweb.s3.ama 11ec-bb32-fa163e15d75b/f	r Administration zonaws.com/docs.fortinet.con ortiManager-7.2.1-Administra	Guide acessad n/v2/attachments/04f80 tion Guide.pdf	lo em Ibb3-e03c-

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

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





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



	e filtro de URL; monitoração de logs;	ferramentas de investigação de logs; debugging;					
Configuração do Tosto	troubleshooting; visualização de eventos; o	dashboards; captura de pacotes;					
Procedimento do Teste	Demonstrar operação do FortiManager Dentro de um pacote de políticas podemos os filtros necessários.	adicionar uma nova regra e dentro dela colocar todos					
	Entre eles, controle de aplicação (Applica conteúdo Web e filtro de URL's(Web Filter	tin Control), IPS, antivírus e anti-spyware(Antivírus), Profile).					
	Para realização de debugging e troubles acessar qualquer FortiGate gerenciado pel	nooting deve se usar do seguinte caminho para se o FortiManager.					
	Em "Device Manager" selecionar o FortiGa uma aba de informações sobre aquele ativ	te desejado e clicar duas vezes nele, assim aparecerá o.					
	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: <u>https://docs.fortinet.com/document/FortiGate/7.2.4/administration-</u> guide/244292/troubleshooting						
Evidências	Policy & Objects -	😑 🔎 Policy Package 👻 🛃 Install Wizard					
	Policy Packages	+ Create New ∽ 🗹 Edit ∽ 🛗 Delete					
	LE Search Q	# Name					
	⊕ Laderno_Teste_SEDUC	□ □ Implicit (1/1 Total:1)					
	⊖ <sup>[</sup> A SEDUC	1 Implicit Deny					
	Firewall Policy						
	Installation Targets						
	⊕ 🕒 default						







※ Fabric									>_ @•		A admin
	~ G	Last 1 Hour + 10:	:53:12 To 11:53	11						1	ね 🖩 チー
All	A	dd Filter								•	Q 0
➡ FortiGate	-> #	▼Date/Time	Data Source ID	Event Message	Event Type	Event Severity	Source IP	Destination IP	Host Name	User ID	Applicatio
FortiAnalyzer	> 1	11:49:53	FAZ-VM000	user 'admin'	event	information					
Log Browse	2	11:48:03	FGT80ETK1	Configuratio	event	alert				admin	
Log Group	3	11:48:03	FGT80ETK1	Admin logou	event	information	192.168.3.254	192.168.2.24		admin	
	4	11:47:37	FGT80ETK1	System perfo	event	notice					
	5	11:45:44	FAZ-VM000	System Perfo	event	notice					
	6	11:43:24	FAZ-VM000	Receive an u	event	information					
	7	11:42:41	FGT80ETK1	Security Rati	event	notice					
	8	11:42:41	FGT80ETK1	System perfo	event	notice					
	9	11:42:36	FGT80ETK1	Security Rati	event	notice					
	10	11:42:36	FGT80ETK1	Security Rati	event	notice					
	11	11:42:36	FGT80ETK1	Security Rati	event	notice					
	12	11:40:44	FAZ-VM000	System Perfo	event	notice					
	13	11:40:38	FAZ-VM000	Received ne	event	information					
	14	11:37:41	FGT80ETK1	System perfo	event	notice					
	15	11:35:44	FAZ-VM000	System Perfo	event	notice					
	16	11:34:44	FAZ-VM000	User 'admin'	event	information					
	17	11:33:10	FAZ-VM000	Receive an u	event	information					
Fabric     FortiGate	> Tot	loggle Widgets ~ tal Events	All_FortiGate	<ul> <li>O Last 1 H</li> </ul>	our ~ 2023-0	3-17 11:19:00 - 2	2023-03-17 12:19	9:00			
Traffic					-0-1	notice 🐟 informati	on 🔶 alert				
Security	>										
Event	~	5			$\sim$						
Summary		4			·····/ ··· \						
All Types		3									
Fadaciat					1		$\cap$				
Endpoint		2	-			1					
		1	/			N					
Security Rating											
Security Rating SDN Connector		0					-				
Security Rating SDN Connector System		0 2023/03/1	17 11:20 20	23/03/17 11:30	2023/03/17 1	1:40 2023/03/	/17 11:50 202	3/03/17 12:00	2023/03/17 12	:10	
Security Rating SDN Connector System VPN		0 2023/03/1	7 11:20 20	23/03/17 11:30	2023/03/17 1	1:40 2023/03/	/17 11:50 202	3/03/17 12:00	2023/03/17 12	:10	
Security Rating SDN Connector System VPN		02023/03/1	17 11:20 20	23/03/17 11:30	2023/03/17 1	1:40 2023/03/	/17 11:50 202	3/03/17 12:00	2023/03/17 12	210	
Security Rating SDN Connector System VPN User		0 2023/03/1	17 11:20 20	23/03/17 11:30	2023/03/17 1	1:40 2023/03/	77 11:50 202	3/03/17 12:00	2023/03/17 12	£10	
Security Rating SDN Connector System VPN User User	•	0 2023/03/1 System Events View general syste	17 11:20 20.	23/03/17 11:30	2023/03/17 1	1,40 2023/03/	Router Event View events rel	3/03/17 12:00 ts lating to layer-3 roo	2023/03/17 12	h10	×
Security Rating SDN Connector System VPN User SectiAnalyzer Log Browse Ing Browse	> (	0 2023/03/1 System Events View general syste vent Name ≎	17 11:20 20 ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;	23/03/17 11:30 C	2023/03/17 1	× 2023/03/	Router Event     View events rel ent Name \$	3/03/17 12:00 ts lating to layer-3 roo	2023/03/17 12 uting.	£10 Count ≎	×
Security Rating SDN Connector System VPN User S FortiAnalyzer Cog Browse Log Browse Log Group	> E	0 2023/03/1 View general syste vent Name ≎ ystem performance s	i7 11:20 20. iem events. Level \$	23/03/17 11:30 C	2023/03/17 1 Count ¢ 2	× 7	Router Event           View events rel           ent Name \$           ko record found.	ts Level	2023/03/17 12 uting.	Count ¢	×
Sccurity Rating SDN Connector System VPN User SFortiAnalyzer Log Browse Log Group	> (	0 2023/03/1 View general syste vent Name ≎ ystem performance s HCP statistics	i7 11:20 20 iem events. Level ¢ informa	23/03/17 11:30 c xe 1 ttion 2	2023/03/17 1 Count ¢ .2	× 2023/03/	Router Event View events rel view contained we contained view contain	ts lating to layer-3 roo Level	2023/03/17 12 uting. \$	Count ¢	×
Scurity Rating SDN Connector System VPN User FortiAnalyzer El Log Growp El Log Group	> E S D	System Events View general system vent Name © stem performance so HCP statistics ortiGate update succ	1711:20 20 iem events. Level ≎ information interest iem events information interest iem events interest information interest iem events interest ie	23/03/17 11:30 223/03/17 11:30 223/03/	2023/03/17 1 Count ¢ .2	× 2023/03/	Router Event View events rel ent Name ¢ No record found.	ts ating to layer-3 roo Level	2023/03/17 12 uting. ↓¢	Count \$	×

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

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







	Como tan	nbém exclusão e visualização de onde está	sendo usado.
	×	login.microsoftonline.com	Firewall Addres
		login.microsoft.com	Edit
		login.windows.net	■ Clone
	🔲 📟 gmail.com		
		wildcard.google.com	Crouping
		wildcard.dropbox.com	Promote to Global
		SSLVPN_TUNNEL_ADDR	View Group Members
Comentário	Ľ	周 all	

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

Deve nossibilita	r a especificaçã	ia de nalíti	ica nor tom		normiti	r a definid	na de rec	arac
Deve possibilità	i a específicaçã			po, ou seje	a, perinti			5103
para um determ	inado norario (	bu periodo	(dia, mes, a	ano, dia da	semana	e nora);		
Validar se a ferra	amenta possui	a funciona	lidade de at	tribuir tem	po à uma	política.		
Necessita ter u	m FortiManag	er e uma	conta de a	administrad	dor com	acesso p	ara escrit	ta e
visualização.	-							
Na aba de "Polic	y and Objects"	, é possíve	l visualizar t	todas as re	gras pres	entes no o	lispositivo	э.
					. ,	, .	<i>.</i> .	
Para cada regra,	há um campo	denomina	do "Agenda	imento", oi	nde é pos	ssível prog	ramá-la p	bara
um período espe	ecífico ou torná	i-la recorre	ente durant	e um deter	minado i	ntervalo d	e tempo.	
# Name	From	То	Source	Destination	Schedule	Service	Action	٠
✓ 1	🖾 lan	wan1	🖾 all	🖾 all	🖬 always	@ ALL	✓Accept	
				gmail.com				
2	sslvpn_tun_intf	🗖 lan	& rodrigo	<ul> <li>login.microsoftcoli</li> <li>login.windows.net</li> </ul>	G always	@ ALL	✓ Accept	
Dava suis são da		ام مار مار						
Para críação de	regras para um	periodo d	e tempo:					
	Deve possibilita para um determ Validar se a ferri Necessita ter u visualização. Na aba de "Polic Para cada regra, um período espe Para criação de	Deve possibilitar a especificaçã para um determinado horário o Validar se a ferramenta possui Necessita ter um FortiManag visualização. Na aba de "Policy and Objects" Para cada regra, há um campo um período específico ou torná	Deve possibilitar a especificação de polít para um determinado horário ou período Validar se a ferramenta possui a funciona Necessita ter um FortiManager e uma visualização. Na aba de "Policy and Objects", é possíve Para cada regra, há um campo denomina um período específico ou torná-la recorre	Deve possibilitar a especificação de política por tem para um determinado horário ou período (dia, mês, a Validar se a ferramenta possui a funcionalidade de ar Necessita ter um FortiManager e uma conta de a visualização. Na aba de "Policy and Objects", é possível visualizar f Para cada regra, há um campo denominado "Agenda um período específico ou torná-la recorrente durante e normal e an o superíodo específico a u torná-la recorrente durante Para criação de regras para um período de tempo:	Deve possibilitar a especificação de política por tempo, ou seja para um determinado horário ou período (dia, mês, ano, dia da Validar se a ferramenta possui a funcionalidade de atribuir tem Necessita ter um FortiManager e uma conta de administrat visualização. Na aba de "Policy and Objects", é possível visualizar todas as re Para cada regra, há um campo denominado "Agendamento", o um período específico ou torná-la recorrente durante um deter	Deve possibilitar a especificação de política por tempo, ou seja, permitipara um determinado horário ou período (dia, mês, ano, dia da semana o Validar se a ferramenta possui a funcionalidade de atribuir tempo à uma Necessita ter um FortiManager e uma conta de administrador com visualização. Na aba de "Policy and Objects", é possível visualizar todas as regras pres Para cada regra, há um campo denominado "Agendamento", onde é pos um período específico ou torná-la recorrente durante um determinado i 2 Name From To Source Destination Schedule 2 Stupp.tun.tet I al Stupp.TUNEL Emploidemento Schedule 2 Stupp.tun.tet I al Stupp.tun.tet I al Stupp.tun.tet I al Avays Para criação de regras para um período de tempo:	Deve possibilitar a especificação de política por tempo, ou seja, permitir a definiç para um determinado horário ou período (dia, mês, ano, dia da semana e hora); Validar se a ferramenta possui a funcionalidade de atribuir tempo à uma política. Necessita ter um FortiManager e uma conta de administrador com acesso pr visualização. Na aba de "Policy and Objects", é possível visualizar todas as regras presentes no c Para cada regra, há um campo denominado "Agendamento", onde é possível prog um período específico ou torná-la recorrente durante um determinado intervalo d 2 Name From To Source Destination Sondule Service 2 1 Cana Quanta at Cana Service Cana Service Cana Service 2 2 Cana Super, tan, inf Cana Source Cana Service C	Deve possibilitar a especificação de política por tempo, ou seja, permitir a definição de regara um determinado horário ou período (dia, mês, ano, dia da semana e hora);         Validar se a ferramenta possui a funcionalidade de atribuir tempo à uma política.         Necessita ter um FortiManager e uma conta de administrador com acesso para escritivisualização.         Na aba de "Policy and Objects", é possível visualizar todas as regras presentes no dispositivo         Para cada regra, há um campo denominado "Agendamento", onde é possível programá-la pum período específico ou torná-la recorrente durante um determinado intervalo de tempo.         Image: Pom       To       Source       Destination       Service       Action         Image: Pom       To       Source       Destination       Service       Action



	Create New One-Time Schedule	
	Name	Agendamento- <u>Sedud</u>
	Color	0
	Start Time	15/03/2023 🗖 14:58 <b>O</b>
	End Time	15/03/2023
	Pre-expiration Event Log	0
	Number of Days Before	3
	Add To Groups	٩
		Click to select
	Para regras recorrentes: Create New Recurring Schedule	
	Name	Agendamento-Seduc
	Color	ົ
	Day	Monday     Tuesday     Wednesday       Thursday     Friday     Saturday       Sunday     Sunday     Saturday
	Time	All day Specify
	Add To Groups	٩
		Click to select
Comentário		

Item de Teste - 5.4.15	Deve reg	gistrar log	gs de a	auditoria re	eferente as açõ	ões dos usuá	rios	admini	stradores;	
Objetivo do Teste	Validar	se a sol	ução	é capaz c	de registrar d	e auditoria	refe	erente	as ações	dos usuários
	administ	radores.								
Configuração do Teste	Demons	trar logs (	de ras	streamento	de ações loca	is dos admir	nistra	dores.		
Procedimento do Teste	Para isso	, é neces	ssário	acessar a	aba de "Syster	n Settings" e	e, en	1 segui	da, a seção	o "Event Log",
	onde sei	ão exibic	las to	das as alte	racões efetuad	das por dete	rmin	ado ad	Iministrado	or iuntamente
	com a da	com a data e a origem correspondentes.								
Fvidências			0-							
Evidencias	Ever	it Log								
		-								
	The	e Event Loa r	oane pro	ovides an audit	log of actions made	by users on Forti	Manao	er. It allo	ws you to view	log messages
	tha	t are stored in	n memo	ry or on the inte	ernal hard disk drive	You can use filte	ers to s	earch the	messages and	d download
	the	messages to	o the ma	anagement com	nputer.					
	Se	e the FortiMa	nager L	.og Message R	eference, available f	rom the Fortinet I	Docum	ent Libra	ry, for more infe	ormation
	abo	out the log me	essages	3.						
	Go	to System S	ettings	> Event Log to v	view the local log list					
	0	ast 1 Day • Add Filter			Apr 25 To Apr 26		≜ Dow	food 🖸 Raw Log	Historical Log	
		Date Time	Level	User	Sub Type	Description	Operation	Performed On	Changes	
	7	2021-04-26 12:27:39	notice	💽 admin	objetg	cdb event log for object changed	edit	dev~global,ado	type+fsp_manage 3Jkey=\$108DVCI Aver 14.09.12:07	
	8	2021-04-26 12:24:07	notice	💽 admin	objetg	cdb event log for object changed	edit	dev-global.ado	type+fsp_manage 3,key=\$108DVW	
	9	2021-04-26 12:24:07	notice	💽 admin	objefg	cdb event log for object changed	edit	dev-global,ado	type+fsp_mexage 3,key=S108DVCI Apr 14 16:12:07	
	10	2021-04-26 12:24:07	notice	💽 admin	objetg	cdb event log for object changed	edit	dev-global,ado	type=fsp_managi 3,key=5108DVM Apr 14 16:27:32	
	11	2021-04-26 12:21:10	notice	💽 admin	objefg	cdb event log for object changed	edit	dev-global,ado	type+fsp_manage 3,key+S108DVW Apr 14 16:12:48	
	12	2021-04-26 12:19:55	information	update_manager	fød	Package update response from FortiGuard server received	Update Response	12.34.97.16	Receive an updat fdw(00000.0000C 01000000ALCI0 version:00000.0K	
	13	2021-04-26 12:09:41	information	update_manager	fgd	Package update response from FortiGuard server received	Update Response	12.34.97.16	Receive an updat fdw(00000.0000C 01000000ALCI0 version:00000.0K	



	0	System Settings 🗸	≡				
	ا ۞						
	<del>ب</del> ،	• 111		((•))			
	• I	• 111					
	.a.	Device Manager	Policy & Objects	AP Manager	VPN Manager	Fabric View	
	± /						
		Ê	<b>*\</b>	Ŧ			1
			<b>≁^</b> →			<b>e e</b>	t -
	lio /	FortiGuard	FortiSwitch Manager	Extender Manager	System Settings	Management Extensions	
							1
Comentário	Font	e: FortiM	anager Adr	ministration	Guide a	cessado em	٦
	http	s://fortinetweb.s	3.amazonaws.com	/docs.fortinet.com	n/v2/attachments,	/04f80bb3-e03c-	
	1160	:-bb32-ta163e150	1/50/FortIManager	-7.2.1-Administra	tion_Guide.pdf		

Item de Teste - 5.	4.16	A solu admin	ição deve Distrador	e possui nermiti	ir registro ( indo a iden	de todas as al tificação do re	terações real	izada ela m	as em u	uma política de segurança, por um determinado ca contendo registros de autoria, data e origem:
Objetivo do Teste	2	Verific deteri data e	car se a minado a e origem.	solução administ	consegue	e registrar to mitindo a idei	das as altera ntificação do	açõe resp	s realiz oonsáve	zação em uma política de segurança, por un el pela mudança, contendo registros de autoria
Configuração Teste	do	Demo	nstrar lo	gs de ra	streament	o de ações loc	ais dos admir	nistra	adores.	
Procedimento	do	Para is	sso. é ne	cessário	acessar a a	aba de "Syster	n Settings" e.	em	seguida	a, a seção "Event Log", onde serão exibidas toda
Tosto		as alte	araçõos c	fotuada	s nor doto	rminado indiv	íduo iuntam	onto	com o	data o a origom correspondentes
Teste		as alle	el ações e	fetuaua	is por dete		iuuo, juntaine	ente	com a	uata e a ongeni correspondentes.
Evidências		Ev	The Event L that are stor the messag See the For about the lo Go to Syste	g Log pane pri red in memory jes to the m ttiManager in gg message em Settings	rovides an audi ory or on the ini anagement con Log Message F es. > Event Log to	t log of actions mad ternal hard disk driv mputer. Reference, available view the local log lit	e by users on Forti e. You can use filte from the Fortinet I st.	Manag ers to s Docun	ger. It allor search the nent Libra	ows you to view log messages e messages and download ary, for more information
			Color Ton	d Pitter	lbar	Colo Time	Description	Operation	Performed Co	
			7 2021-04-26 12	2.27:39 notice	edmin	objectg	cdb event log for object changed	edR	dev-global,ado	bae-tho, movag Jawy 5300/WC1 Awy 14 091207
			8 2021-04-26 12	2:24:07 notice	edmin	objefg	cdb event log for object changed	edit	dev-global,ado	hype-fug_manage 33ey-53007VX Aey 14.0912-68
			9 2021-04-26 12	2:24:07 notice	💽 admin	objefg	edb event lag for object changed	edit	dev-global,ado	- hpp=hg_mmap 3hey=5100KCl Ag+14.14.0207
			10 2021-04-26 12	2.24:07 notice	💽 admin	objetg	cdb event log for object changed	edR	dev-global,ado	- Ipor-Ng, minagi Jany-S1002VA Agi 14 16/2752
			11 2021-04-26 12	2:21:10 notice	edmin 🕢	objefg	edb event log for object changed	edit	dev-global,ado	- hpp=hg_mmapi 3.hey=5108D/W Agr 14.16.248
			12 2021-04-26 12	219:55 Information	update_manager	fgd	Package update response from FortiGuard server received	Update Response	12.34.97.16	Reverse as spatial inductional conduct of secondocal LCIo version-050000.0.0
		1	13 2021-04-26 12	209:41 Information	update_manager	fed	Package update response from	Update	12.34.97.16	Receive an updat
							FortiGuard server received	Rasponse		200000044.C0 version.00000.00



	E.E System	Settings -		≡						
	⊕ 1									
	⊕ / C				((•))					
	A Device	e Manager	Policy	& Objects	AP Manager		VPN Manager	Fabric View		
	<b>1</b>								_]	
				X	Ē		•	(*) (*) (*) (*) (*) (*)		
	For	tiGuard	FortiSwi	itch Manager E	xtender Mana	ger	System Settings	Management Extensions		
	513 System Settings +	-						4004-55	DUC ≻ Ω.	An • A admin •
	Dashboard	Add Filter		9 14	t 1 Hour 🗸 14:25:45 T	0 15:25:44		ADOM: 34	. Download	Rawlos O Historical Los
	All ADOMs	# Date Time	Level	User	Sub Type	Operation	Changes		Description	Performed On
	Network									
	Admin	7 2023-03-15 15:05:0	08 information	update_manager	FortiGuard service event	Update Requ	Send new version object to device (sn:FG	VM010000015354, ip=127.0.0.1): objid	Object update re	127.0.0.1:0
				undate manager	FortiGuard service event	Update Resp	Departure and under an end over factor (de 1000)			000 10 100 F
	Certificates	<b>,</b> 8 2023-03-15 15:01:5	anformation	oboose Junualist			Porceive an update package from rostoook	02.10115-2303151745): 07000000AV	Package update r	208.184.237.67
	Certificates  Event Log  Task Monitor	<ul> <li>8 2023-03-15 15:01:5</li> <li>9 2023-03-15 15:01:5</li> </ul>	51 information	update_manager	FortiGuard service event	Update Resp	Receive an update package from fds(0000	02.10115-2303151745): 07000000AV	Package update r Package update r	208.184.237.67
	Certificates     Event Log     Task Monitor     Bo Advanced	<ul> <li>8 2023-03-15 15:01:5</li> <li>9 2023-03-15 15:01:5</li> <li>10 2023-03-15 15:01:4</li> </ul>	51 information 51 information 48 information	update_manager update_manager	FortiGuard service event	Update Resp	Receive an update package from fds(0000 Receive an update package from fds(0000	0700000004V 02.10115-2303151745): 070000004V 00.0000-2303151801): 01000000AU	Package update r Package update r Package update r	208.184.237.67 208.184.237.67 208.184.237.67
	Certificates  Event Log  Task Monitor  Advanced	<ul> <li>8 2023-03-15 15:01:5</li> <li>9 2023-03-15 15:01:5</li> <li>10 2023-03-15 15:01:4</li> <li>11 2023-03-15 15:01:4</li> </ul>	1 information 1 information 18 information 18 notice	update_manager update_manager A admin	FortiGuard service event FortiGuard service event Deployment manager event	Update Resp Update Resp Device confi	Receive an update package from fds(0000 Receive an update package from fds(0000 Receive an update package from fds(0000 Config install preview successfully dbstate	22.10115-2303151745; 070000004V 22.10115-2303151745; 070000004V 20.00000-2303151801; 01000000ALCI us=not modified confstatus=insync	Package update r Package update r Package update r Install preview su	208.184.237.67 208.184.237.67 208.184.237.67 Cademo_Teste_SEDUC
	Certificates  Event Log  C Task Monitor  Advanced	<ul> <li>8 2023-03-15 15:01:3</li> <li>9 2023-03-15 15:01:3</li> <li>10 2023-03-15 15:01:4</li> <li>11 2023-03-15 15:01:4</li> <li>12 2023-03-15 15:00:4</li> </ul>	1 information 1 information 18 information 18 notice 19 information	update_manager update_manager A admin A admin	FortiGuard service event FortiGuard service event Deployment manager event Policy console event	Update Resp Update Resp Device confi package/tem	Receive an update package from residoo Receive an update package from fds(0000 Receive an update package from fds(0000 Config install preview successfully dostati Caderno_Teste_SEDUC(root) policy packa	22.10115-2303351745; 070000004V 22.10115-2303151745; 070000004V 20.00000-2303151801; 010000004LCI us=not modified confstatus=insync age 'Caderno_Teste_SEDUC' status upda	Package update r Package update r Package update r Install preview su Security console	208.184.237.67 208.184.237.67 208.184.237.67 Cademo_Teste_SEDUC Cademo_Teste_SEDUC
	Certificates  Event Log  To Event Log  Advanced  Advanced	<ul> <li>8 2023-03-15 15:01:1</li> <li>9 2023-03-15 15:01:4</li> <li>10 2023-03-15 15:01:4</li> <li>11 2023-03-15 15:01:4</li> <li>12 2023-03-15 15:00:4</li> <li>13 2023-03-15 15:00:4</li> </ul>	11 information 13 information 18 information 18 notice 19 information 19 notice	update_manager update_manager A admin A admin A admin A admin-GUI(192.168.3.254)	FortiGuard service event FortiGuard service event Deployment manager event Policy console event Configuration change event	Update Resp Update Resp Device confi package/tem edit	Receive an update package from folk000 Receive an update package from folk000 Receive an update package from folk000 Config install preview successfully dostate Caderno_Teste_SEDUC[root] policy packa type-policy_package_setting.pkgname-C	22.10115-2200353/4%) 070000004V 22.10115-230315174\$): 070000004V 20.00000-2303151801): 01000000ALCI us-not modified confitatus-innync age "Coderno, Teste, SEDUC status upda iaderno, Teste, SEDUC shedsum-2023	Package update r Package update r Package update r Install preview su Security console cdb event log for	208.184.237.67 208.184.237.67 208.184.237.67 Caderno_Teste_SEDUC Caderno_Teste_SEDUC devrsglobal.adom-SEDUC
	Certificates      Event Log      Tools Monitor      Advanced	<ul> <li>8 2022-03-15 15:01:1</li> <li>9 2023-03-15 15:01:1</li> <li>9 2023-03-15 15:01:1</li> <li>10 2023-03-15 15:01:4</li> <li>11 2023-03-15 15:01:4</li> <li>12 2023-03-15 15:00:4</li> <li>13 2023-03-15 15:00:4</li> <li>14 2023-03-15 15:00:4</li> </ul>	information information information information information information information information information information	update_manager update_manager A admin A admin A admin-GUI(192.168.3.254) A admin-GUI(192.168.3.254)	FortiGuard service event FortiGuard service event Deployment manager event Dolicy console event Configuration change event Configuration change event	Update Resp Update Resp Device confi package/tem edit add	Network an update package from foculo Receive an update package from foculo Receive an update package from foculo Receive an update package network of Config install preview successfully dotate Config install preview successfully dotate tope-policy_cakage_setting_akgument tope-dynamic_cert_mapping.key=Forther	22,20115-2800151749;070000000V 20,20115-2800151749;07000000AV 00.00000-2800151801;01000000ALCI us-not modified confutus-insync age Caderno, Teste, SEDUC stahu suda aderno, Teste, SEDUC stahu suda aderno, Teste, SEDUC stahu suda	Package update r Package update r Install preview su Security console cdb event log for cdb event log for	208.184.237.67 208.184.237.67 208.184.237.67 Caderno_Teste_SEDUC Caderno_Teste_SEDUC dev~global.adom~SEDUC dev~Caderno_Teste_SEDUC
	Certificates   Certificates   Catholic Certificates   Catholic Certificates   Advanced	> 8         2023-03-15 15:01:1           > 9         2023-03-15 15:01:1           > 10         2023-03-15 15:01:4           11         2023-03-15 15:01:4           12         2023-03-15 15:00:4           13         2023-03-15 15:00:4           14         2023-03-15 15:00:4           15         2023-03-15 15:00:4           16         2023-03-15 15:00:4           17         2023-03-15 15:00:4           18         2023-03-15 15:00:4           19         2023-03-15 15:00:4           10         2023-03-15 15:00:4           11         2023-03-15 15:00:4           12         2023-03-15 15:00:4           13         2023-03-15 15:00:4           14         2023-03-15 15:00:4           15         2023-03-15 15:00:4	information information information is information is notice information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information infor	update_manager update_manager A admin A admin A admin A admin A admin- CU(192.168.3.254) A admin-CU(192.168.3.254)	FortiGuard service event FortiGuard service event Deployment manager event Policy console event Configuration change event Configuration change event	Update Resp Update Resp Device confi package/tem edit add edit	Heterve an update package from findicide Receive an update package from findicide Receive an update package from findicide Config install preview successfully datate Coderno, Teste, SEDUC(root) pathy packa Coderno, Teste, SEDUC(root) pathy packa Dependicide, cert, mapping, Jay-Fortine Tope-dynamic, cert, Jocal Ley-Fortinet, C.	22.2015-2200151/96/07000000V 22.2015-2200151745), 07000000V 20.00000-2300151801), 01000000ALCI uso-not-modified confuture-insyne gap Caderno, Teste, SEDUC-status upda 20.0000, Teste, SEDUC-status upda 21.CA_SSLBymmic].local-cert-fortimet A_SSL	Package update r Package update r Package update r Install preview su Security console cdb event log for cdb event log for cdb event log for	208.194.237.67 208.184.237.67 208.184.237.67 Cademo_Teste_SEDUC Cademo_Teste_SEDUC devr_global.adom-SEDUC devr_Gademo_Teste_SEDUC
	Contributes  Control Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control  Control	> 8         2023-03-15 15:01:1           >         9         2023-03-15 15:01:1           >         10         2023-03-15 15:01:1           11         2023-03-15 15:01:1         12           12         2023-03-15 15:00:4         13         2023-03-15 15:00:4           14         2023-03-15 15:00:4         14         2023-03-15 15:00:4           15         2023-03-15 15:00:4         15         2023-03-15 15:00:4           16         2023-03-15 15:00:4         16         2023-03-15 15:00:4	information information information information information information information information information information information information information information information	update, mangar update, mangar update, mangar A admin A admin A admin-GU(192168.3254) A admin-GU(192168.3254) A admin-GU(192168.3254)	FortiGuard service event FortiGuard service event Deployment manager event Policy console event Configuration change event Configuration change event Configuration change event	Update Resp Update Resp Device confi package/tem edit add edit add	Henner an update package from Mission Receive an update package from Mission Receive an update package from Mission Config Install preview successfully obstat Caderno, Tester, SEDUC (noci) palicy pack type=package, package, jetting jagvame-C type=dynamic_cert_package, jetting jagvame-C type=dynamic_cert_package.pathing jagvame-Col pape-dynamic_cert_package.pathing jagvame-Col pape-dynamic_cert_package.pathing jagvame-Col pape-dynamic_cert_package.pathing jagvame-Col pape-subheticitation_strat_pagrame-Cole	22.013-22.01317.4%) 01000000V 22.013-22.01317.4%) 07000000V 22.013-22.01317.4%) 07000000V us-not modified contributio-imyric gige Caderno, Teste, SEDUC status upda ademo, Teste, SEDUC, status upda ademo, Teste, SEDUC, adek-sum-2022 4, CA, SSL(My,mink), local-cet-Fortinet A, SSL	Package update r Package update r Package update r Install preview su Security console cdb event log for cdb event log for cdb event log for cdb event log for	208.194.237.67 208.184.237.67 208.184.237.67 Cademo_Teste_SEDUC Cademo_Teste_SEDUC devrCademo_Teste_SEDUC devrCademo_Teste_SEDUC devrglobal.adom-SEDUC devrglobal.adom-SEDUC
	Certificates  Certificates  Catholic Certificates  Catholic Certificates  Advanced  Advanced	<ul> <li>a 2023-08-15 15:08:1</li> <li>y 2023-08-15 15:08:1</li> <li>y 2023-09-15 15:08:1</li> <li>y 10 2023-09-15 15:08.4</li> <li>y 10 2023-09-15 15:08.4</li> <li>y 2023-09-15 15:08.4</li> </ul>	information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information information inform	update, magar update, marager A admin A admin A admin A admin GU[192168.3254] A admin GU[192168.3254] A admin GU[192168.3254] A admin GU[192168.3254]	FortiGuard service event FortiGuard service event Deployment manager event Policy console event Configuration change event Configuration change event Configuration change event	Update Resp Update Resp Device confi package/tem edit add edit add add	Internet an update package non-tensioner Receive an update package non-fabilition Config install previous successfully obtain Confirms, Terle SEDUC(not) parks; package hope-replanatio, cert, package, setting aligname: Cat trape-replanatio, cert, package, setting aligname: Cat pape-admentication, set abadeser-fortime trape-relations, cert, backer-fortime, trape- admentations, cert, backer-fortime, trape- relations, cert, backer-fortime, trape- admentations, settebale thereach of	22.2013-2201311/kg) 0000004V 22.2013-2201311/kg) 0000004V usinot modified confutusi-inspic uge Calerno, Teste, SEDUC status upda dotron, Teste, SEDUC status upda 4,C, SSLdhynamic Jocal-cert-forthet A,SSL	Package update r Package update r Package update r Install preview su Security console cdb event log for cdb event log for cdb event log for cdb event log for cdb event log for	208.194.237.67 208.194.237.67 208.194.237.67 Caderno_Teste_SEDUC Caderno_Teste_SEDUC dev-global.adom-SEDUC dev-global.adom-SEDUC dev-global.adom-SEDUC
	Cettificates  Cettificates  Accuracy  Accurac	<ul> <li>2023-00-15 15:00:1</li> <li>2023-00-15 15:01:1</li> <li>2023-00-15 15:01:1</li> <li>2023-00-15 15:01:1</li> <li>2023-00-15 15:00:4</li> </ul>	information           infortice           infortint	varantij, undelar, manger updelar, manger A admin A admin A admin A admin-GU(192,168,3254) A admin-GU(192,168,3254) A admin-GU(192,168,3254) A admin-GU(192,168,3254) A admin-GU(192,168,3254) A admin-GU(192,168,3254)	Forstaurd service event ForstGaard service event Deployment manager event Deployment manager event Configuration change event Configuration change event Configuration change event Configuration change event	Update Resp Update Resp Device confi package/tem edit add add add add add	Internar and update package from fishcoord Receive an update package from fishcoord Receive an update package from fishcoord Config Intell preview successful dy data tages splitz, package, setting adjustment Compensational Configuration of the splitz hype-shytemic cont. Successful adjustment tages endowed and the splitz adjustment of the splitz adjustment of the splitz adjustment of the splitz adjustment of the splitz adjustment of the hype-shytemic cont. Successful adjustment of the splitz adjustment of the splitz adjustment of the splitz adjustment of the splitz adjustment of the splitz adjustment of the splitz adjustment of the splitz adjustment of the splitz adjustment of the splitz adjustment of the splitz adjustment of the splitz	22.2012-20131314/si 0000004/- 22.20115-20131514/si 0000004/- us rot modified confutura-impre up Colorno, Teste, SEDUC statu spitu. ademo, Teste, SEDUC statu spitu. C.C. SSL0/pumic/locil-cent-former, - A.SSL mo, Teste, SEDUC auth-https-molec.co. Itable.send-dmv; pocket-disable.service	Package update r Package update r Package update r Install preview su Security console cdb event log for cdb event log for	208.194.237.67 208.194.237.67 208.194.237.67 Cademo, Teste, SEDUC Cademo, Teste, SEDUC dev-global.adom-SEDUC dev-global.adom-SEDUC dev-global.adom-SEDUC dev-global.adom-SEDUC
	Contributes  Control of the second s	iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	information           infore           infore	varance, unpair, update, manger update, manger A admin A admin GU(192168.3254) A admin-GU(192168.3254) A admin-GU(192168.3254) A admin-GU(192168.3254) A admin-GU(192168.3254) A admin-GU(192168.3254)	TerritQuard service event ForttQuard service event Deployment manager event Configuration change event Configuration change event Configuration change event Configuration change event Configuration change event	Update Resp Update Resp Device confi edit add edit add add add add add	Receive an update package from findboom Receive an update package from findboom Config install preview successfully distall Config install preview successfully distall type=ropidity_package_setting_alpume=Co type=rhymic_color_should set-fortime_C type=rhymic_color_should set-fortime_C type=	22.2113-2201113/143) (VVXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Package update r Package update r Package update r Install preview su Security console cdb event log for cdb event log for	2013/94-237.67 2018/14/237.67 2018/14/237.67 2018/14/237.67 Cademo_Teste_SLDUC Cademo_Teste_SLDUC dev-global.tadom-SEDUC dev-global.tadom-SEDUC dev-global.tadom-SEDUC dev-global.tadom-SEDUC
	Contributes  Control of the second s	•         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •	information           infore           infore	Adamic, Jungari update, nunger update, nunger A admin A admin A admin GU(1921683254) A admin-GU(1921683254) A admin-GU(1921683254) A admin-GU(1921683254) A admin-GU(1921683254) A admin-GU(1921683254) A admin-GU(1921683254) A admin-GU(1921683254) A admin-GU(1921683254)	Terribland service event Fortibland service event Deployment manager event Deployment manager event Configuration change event Configuration change event Configuration change event Configuration change event Configuration change event Configuration change event	Update Resp Update Resp Device confi package/tem edit add add add add add add add add	Receive an update package into mission Receive an update package from fisitions Config install preview successfully distant Conferma, Tetra SERDEC/profit package https://preview.successfully.explored toppe-shynamic, cort, supplices/preview. Toppe-shynamic, cort, supplices/preview. T	22 2113-2201311/kg) 0000004/c. 22 2013-2201311/kg) 0000004/c. 22 2013-2201311/kg) 0000004/c. 20000-22013101(kg) 0000004/c. 20000-2201310(kg) 000004/c. 20000-2201310(kg) 000004/c. 20000-2201310(kg) 000004/c. 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000-20000- 20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-2000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-20000-2000000	Package update r Package update r Package update r Install preview su Security console cdb event log for cdb event log for rith event log for	2003.194.227.67 2003.194.227.67 2003.194.227.67 Codemo, Teste, SEDUC Codemo, Teste, SEDUC derr, global.adom-SEDUC derr, global.adom-SEDUC derr, global.adom-SEDUC derr, global.adom-SEDUC derr, global.adom-SEDUC derr, global.adom-SEDUC derr, global.adom-SEDUC derr, global.adom-SEDUC
	Contributes  Control of the second s	0         2023-00-15 51:00:1           7         2023-00-15 50:01           10         2023-00-15 50:01           11         2023-00-15 50:01           12         2023-00-15 50:01           12         2023-00-15 50:01           12         2023-00-15 50:01           12         2023-00-15 50:00           14         2023-00-15 50:00           15         2023-00-15 50:00           16         2023-00-15 50:00           18         2023-00-15 50:00           19         2023-00-15 50:00           19         2023-00-15 50:00           19         2023-00-15 50:00           19         2023-00-15 15:00           19         2023-00-15 15:00           19         2023-00-15 15:00           10         2023-00-15 15:00           11         2023-00-15 15:00           12         2023-00-15 15:00           13         2023-00-15 15:00           14         2023-00-15 15:00           15         2023-00-15 15:00           16         2023-00-15 15:00           17         2023-00-15 15:00           18         2023-00-15 15:00           19         2023-00-15 15:00	andormation       andormation <t< td=""><td>Adamic, Jungari update, nunger update, nunger A admin A admin A admin GU(1921683254) A admin-GU(1921683254) A admin-GU(1921683254) A admin-GU(1921683254) A admin-GU(1921683254) A admin-GU(1921683254) A admin-GU(1921683254)</td><td>Tertifiuard service event Fortfluard service event Deployment manager event Deployment manager event Configuration change event</td><td>Update Resp. Update Resp. Device confi. package/rem. edit add add add add add add add add add</td><td>Receive an update package monocologi Receive an update package from fishiotox Config install preview successfully distant Conferma, Tent SEDUCIONEL policy pack- three-policy, package, setting all parmor pape-sharinis, cryst Duckaler-Forties, CJ type-sharinis, cryst Duckaler-Forties</td><td>22 2013-220131748) 07000004/- 22 2013-220131748) 07000004/- 22 2013-220131748) 07000004/- curront modified confutura-impre ge Colema, Tente, SEDUC: Anton upda. 2000-2013181(0) 0000-0001/- ge Colema, Tente, SEDUC: Anton upda. 2, CA SSI (0) Canth-Rapo-enable Col- table and damy packet-disable sarvise. _SEDUC: Jan-SeDUC: Anton Happ-enable Col- table and damy packet-disable sarvise. _SEDUC: Jan-SeDUC: Anton Happ-enable Col- set of Colema and SeDUC: Anton Happ-enable Colema and SeDUC: Anton _SEDUC: Anton Happ-enable Col- _SEDUC: Anton Happ-enable Col- _SEDUC: Anton Happ-enable Col- _SEDUC: Anton Happ-enable Col _SEDUC: Anton Happ-enable Col _SED</td><td>Pickage update r Package update r Package update r Instalt preview usu- security consel cdb event log for cdb event log for rith event log for</td><td>2013/94/21/07/ 2013/14/22767 2010.194/22767 2010.194/22767 Codemo,Tente, SEDUC derro, Belan, Jacomos SEDUC derro, Belan, Sector, SEDUC derro, Sector, Sector,</td></t<>	Adamic, Jungari update, nunger update, nunger A admin A admin A admin GU(1921683254) A admin-GU(1921683254) A admin-GU(1921683254) A admin-GU(1921683254) A admin-GU(1921683254) A admin-GU(1921683254) A admin-GU(1921683254)	Tertifiuard service event Fortfluard service event Deployment manager event Deployment manager event Configuration change event	Update Resp. Update Resp. Device confi. package/rem. edit add add add add add add add add add	Receive an update package monocologi Receive an update package from fishiotox Config install preview successfully distant Conferma, Tent SEDUCIONEL policy pack- three-policy, package, setting all parmor pape-sharinis, cryst Duckaler-Forties, CJ type-sharinis, cryst Duckaler-Forties	22 2013-220131748) 07000004/- 22 2013-220131748) 07000004/- 22 2013-220131748) 07000004/- curront modified confutura-impre ge Colema, Tente, SEDUC: Anton upda. 2000-2013181(0) 0000-0001/- ge Colema, Tente, SEDUC: Anton upda. 2, CA SSI (0) Canth-Rapo-enable Col- table and damy packet-disable sarvise. _SEDUC: Jan-SeDUC: Anton Happ-enable Col- table and damy packet-disable sarvise. _SEDUC: Jan-SeDUC: Anton Happ-enable Col- set of Colema and SeDUC: Anton Happ-enable Colema and SeDUC: Anton _SEDUC: Anton Happ-enable Col- _SEDUC: Anton Happ-enable Col- _SEDUC: Anton Happ-enable Col- _SEDUC: Anton Happ-enable Col _SEDUC: Anton Happ-enable Col _SED	Pickage update r Package update r Package update r Instalt preview usu- security consel cdb event log for cdb event log for rith event log for	2013/94/21/07/ 2013/14/22767 2010.194/22767 2010.194/22767 Codemo,Tente, SEDUC derro, Belan, Jacomos SEDUC derro, Belan, Sector, SEDUC derro, Sector,
tário	Centicate  Catalogue  Advanced  Fonte:	<ul> <li>accession</li> <li>accession</li></ul>	tiManatan ti alormation alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore alore	update, manger update, manger update, manger A admin A admin A admin A admin-GU[192168.3254 A admin-GU[192168.3254 A admin-GU[192168.3254 A admin-GU[192168.3254 A admin-GU[192168.3254 A admin-GU[192168.3254 A admin-GU[192168.3254 A admin-GU[192168.3254 A admin-GU[192168.3254	Fortflaurd service event Fortflaurd service event Deployment murager event Deployment murager event Configuration charge event	Update Resp. Update Resp. Device confi pockage/tem edit add add add add add add add add state stratio	Internar na logata podra podra mini misoso Receitar an ugidata podragi mini misoso Config insuli preview successful de data Calemo, Pere SLEUCCIONE podra yeak taper oplica, unakaya, etiti guaraner. Cale Taper-dramitic, certi, bucklar-fortinet, C. Taper-dramitic, certi, bucklar-fortinet, C.	22.0115-220115-30100000004- 22.0115-20115-3010000004- 20.00000-220115180) 00000004- 20.00000-220115180) 00000004- 20.00000-220115180) 00000004- 20.00000-220115180) 0000004- 20.0000-220115180) 0000004- 20.0000-220115180) 0000004- 20.0000-220115180 20.0000-2000-2000-2000-2000-2000-2000- 2000-2000-	Pickage update Pickage update Pickage update Install preview su Security console cib event log for cib event	200.1942/2077 200.1942/207 200.1942/2077 200.1942/2077 200.1942/2077 200.1942/2077 200.1942/2077 200.1942/2077 200.1942/2077 dev-global.com-SEDUC dev-global.com-SEDUC dev-global.com-SEDUC dev-global.com-SEDUC dev-global.com-SEDUC dev-global.com-SEDUC dev-global.com-SEDUC dev-global.com-SEDUC dev-global.com-SEDUC
tário	Fonte: https://fort/	Course 15 15 15 15 15 15 15 15 15 15 15 15 15	tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiManaa tiMana	Addite, marger update, marger update, marger A admin A admin A admin A admin CU(1921643254) A admin-CU(1921643254) A a	Fortflaurd service event Fortflaurd service event Deployment manager event Deployment manager event Configuration change event	Update Resp Update Resp Device confi package/tem edit add edit add add add add add add add add sol sol sol com/	Energia an update package from fieldoor Receive an update package from fieldoor Config result preview successfully distant Config result preview successfully distant trace-robustic configurations of the successfully distant trace-robustic configurations of the successfully distant trace-robustic configurations of the successfully distant trace-robustic configura	22113-2213131430 0000004- 222113-220131340 0000004- corot modified confuture impact get Coloren, Felte, SEDUC Instances adorma, Teste, SEDUC Instances ASSA Market SEDUC Instances SEDUC I	Pickage update r Pickage update r Pickage update r Install preview su Security consule cith event log for cith event log for cit	200.194.227.67 200.194.227.67 200.194.227.67 Codema, Teste, SEDUC Codema, Teste, SEDUC Codema, Teste, SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC derrugbalt.adom-SEDUC de

Item de Teste - 5.4.17	Prover funcionalidade para análise e auditoria de regras com capacidade de detectar regras
	conflitantes ou não conformes;
Objetivo do Teste	Verificar se o equipamento faz uma validação de políticas que estão conflitantes entre si ou em
	não conformação.
Configuração do Teste	Demonstrar a sobreposição de regras que se anulam ou se repetem.
Procedimento do Teste	Primeiramente, é necessário importar as políticas presentes no dispositivo.
	Posteriormente, deve-se acessar a guia "Políticas e Objetos" e, utilizando o botão direito do mouse, selecionar a opção "Política de Firewall" e, em seguida, "Verificação de Política" para realizar a referida verificação.



Evidências						
	Perform a policy c	onsistency che	ck			
	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			
	<ul><li>Object shadowing:</li><li>Object overlap: on</li></ul>	a higher priority object e object partially overla	t completely encompasses aps another object of the s	s another object o ame type	of the same type	
	<ul> <li>Object orphaning:</li> </ul>	an object has been det	fined but has not been use	ed anywhere.		
	The policy check uses	an algorithm to evalua	te policy objects, based or	n the following att	ributes:	
	<ul> <li>The source and de</li> <li>The source and de</li> </ul>	estination interface policestination address policestination	cy objects			
	The service and se	chedule policy objects.	,, 00,0010			
		T & CEDUC LA		(0 (5)	_	
	Import Device - Caderno	_leste_SEDUC - Inte	rface Mapping & Policy	(2/5)		
	Create a new policy package	e for import.				
	Policy Package Name	Caderno_Teste_SEI	DUC			
	Folder	root			-	
	Policy Selection	Import All (3) S	elect Policies to Import			
	Object Selection	Import only policy	dependent objects Impo	rt all objects		
	When importing cor Note, the same ADC	nfiguration from this devi OM Level interface can ma	ce, all enabled interfaces require to different interfaces on	uire a mapping to a the each device.	n ADOM Level interface.	
					Search	
	Device Interface ≑	Mapping Type	÷	Normalized In	nterface 🗢 🔹	
	🖾 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	d 💽				
					Next > Cancel	
	1					





Item de Teste - 5.4.18	Suportar acesso baseado em perfil de usuário com as permissões de visualizar e modificar;					
Objetivo do Teste	Verificar se o equipamento de gerência centralizada suporta o Suportar acesso baseado em					
	perfil de usuário com as permissões de visualizar e modificar;					
Configuração do Teste	Demonstrar os perfis de ac	esso ao FortiManager				
Procedimento do Teste	Demonstrar os perfis de ac	esso ao FortiManager				
Evidências	Por padrão, o FortiManage	r já vem com os seguintes perfis:				
	Restricted User	Restricted user profiles have no system privileges enabled, and have read-only				
	access for all device privileges.					
	Standard User Standard user profiles have no system privileges enabled, and have read/write					
	access for all device privileges.					
	Super_User Super user profiles have all system and device privileges enabled. It cannot be					
		edited.				
	Package_User	Package user profile have read/write policy and objects privileges enabled, and				
		have read-only access for system and other privileges.				
	Caso haja a necessidade de	criação de outro tipo de perfil, é possível fazê-lo acessando a seção				
	"System Settings" e, em s	eguida, navegando até "Administração" e "Profile". Nessa área, é				



	possível visual como padrão.	lizar	todos os	s perfis já	criados, bem como editar os per	fis que foram fornecidos			
	System Settings -	≡				ADOM: SEDUC >_ @ + 4 G + (A) admin +			
	Dashboard		eate New 🛛 🖾 Edit	Se Clone		Search			
	All ADOMs		Name 0	Type 0	Description ©	•			
	• Network		Restricted_User	System Admin	Restricted user profiles have no System Privileges enabled, and have read-only acce	ss for all Device Privileges.			
	1 Admin Y		Standard_User	System Admin	Standard user profiles have no System Privileges enabled, but have read/write acce	ss for all Device Privileges.			
	Administrators		Super_User	System Admin	Super user profiles have all system and device privileges enabled.				
	Profile		Package_User	System Admin	Package user profile have read/write policy package and objects privileges enabled, and have read-only access for system and others privileges.				
	Workspace		No_Permission_User	System Admin	No permission user profiles have no system or device privileges enabled.				
	Remote Authentication S								
	Admin Settings								
	SAML SSO								
	Certificates								
	Task Monitor								
	Advanced >								
Comentário	Fonte:	For	tiManage	er	Administration Guide	acessado em			
	https://fortine	etwe	eb.s3.ama	azonaws.co	om/docs.fortinet.com/v2/attachr	nents/04f80bb3-e03c-			
	11 - c bb 22 f=1C2=1EdZEb /E=rtiNeneerr 7 2 1 Administration Cuide adf					, df			
	TTEC-0035-191	.036	5120/2D/	roruiviana	iger-7.2.1-Aurninistration_Guide.	Jui			

Item de Teste - 5.	4.19	Deverá possuir validação da política avisando quando houver regras que ofusquem ou conflitem com outras regras;
Objetivo do Teste	5	Verificar se o equipamento faz uma validação de políticas que estão sendo ofuscados ou em conflitos com outras regras.
Configuração	do	Demonstrar a sobreposição de regras que se anulam ou se repetem.
Teste		
Procedimento	do	Primeiramente, é necessário importar as políticas presentes no dispositivo.
Teste		
		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:
		<ul> <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>
		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 source and desumation address policy objects     The service and schedule policy objects.



Create a new policy package for import.						
Policy Package Name Cade	rno_Teste_SEDUC					
Folder root						-
Policy Selection Impo	ort All (3) Select	Policies to Imp	ort			
Object Selection     Impo     When importing configuration     Note, the same ADOM Level in	prt only policy dependent only policy dependent of the second sec	dent objects enabled interfa lifferent interfa	Import al aces require aces on the	I objects a mapping to an AD each device.	OM Level inte	erface.
				Se	earch	
Device Interface 🗢 🛛 M	1apping Type ≑			Normalized Interf	ace ≑	*
🗳 lan	Per-Device Per-	Platform		lan		
Ssl.root	Per-Device Per-	Platform		ssl.root		
wan1	Per-Device Per-	Platform		wan1		
Policy & Objects	•	≡ .	🖹 Poli			
Policy Packages	~	+ (	Create			
Search	Q		#			
Caderno_Teste	_SEDUC	~	1			
Firewall Policy						
Installation Targ	Install Wi	zard				
⊕ 🕒 default	New					
Object Configurati	Clone		Im			
	New Fold	ler				
	Move					
	Edit					
	Luit					
	Delete					
	Policy Re	vision				
	Policy Ch	eck				
	Run Scrip	t				
	Export to	Excel				
	Export to	CSV				



Item de Teste -5.4.20	A solução deve po	ssuir "hit'	/volume d	de regras	para iden	itificar po	ssíveis me	lhorias	na
Objetivo do Teste	Verificar se o equipamento de gerência centralizada possui uma forma de verificar a quantidade de "hit"/volume de regras para identificar possíveis melhorias na performance reordenando as mesmas;								
Configuração do Teste	Demonstrar hit coun	ts de regra	s em uso.						
Procedimento do Teste	Para isto, é necessário acessar a aba de "Policy & Objects".							loa	
F.: Jânsian	opção de visualizaçã engrenagem. Lá apar	o de "Hit C recerá vária	ounts", bas as informaç	sta ir ao car :ões referer	ito superio ites às pol	or direito e íticas, entr	e clicar no e elas, "Hit	símbolo t Count"	de ′.
Evidencias	Policy & Objects -	Policy Pack	age 👻 🔥 Install	Wizard 👻 🌐	ADOM Revision	ns 🥶 Too			
	III     Device Manager     Policy 6	Objects	((•)) AP Manager	VPN Manager	Fabric	View			
	FortiGuard FortiSwite	ch Manager Ex	tender Manager	System Setting	s				
	🗄 🗖 Users								
	🗄 🗹 Action								
	🎚 🗹 Security Pro	files							
	🎚 🗹 Log								
	🗄 🗖 NAT								
	🗄 🔲 Traffic Shapi	ng							
	Enforce ZTN	A							
	🎚 🔲 EMS Tag								
	🎚 🔲 Geographic	Tag							
	🗄 🔲 Hit Count								
	🗄 🗖 Bytes								
	🗄 🗖 Packets								
	□ # Name	From	То	Hit Count @	Source	Destination	Schedule	Service	0
		□ lan	wan1		🗉 all	🖾 all	G always	@ ALL	
	₹ 2	sslvpn_tun_intf	🗖 lan		SSLVPN_TUNNEL K rodrigo	gmail.com login.microsoft.co login.microsofton login.windows.ne	🕞 always	@ ALL	
Comentário									



Item de Teste - 5 4 21	Deve possuir visualizad	ão de log em tempo	nróximo ao real:				
Objetivo do Teste	Verificar se o equipam	ento nossui a funcio	nalidade de visua	lização de logs en	tempo próvimo		
objetivo do reste	ao real						
Configuração do Tosto	ao real.						
Comguração do Teste		sição de regras que s		epetern.			
Procedimento do Teste	Para acessar a funcionalidade de visualização dos registros em tempo real, é necessário acessar a seção "Visualização de Logs". A seguir, é necessário selecionar o equipamento desejado, pressionar o ícone de chave de fenda localizado no canto superior direito e, em seguida, selecionar a opção "Registro em Tempo Real".						
Evidências	🔛 Log View 🗸	≡					
	Device Manager	FortiView	Log View	Fabric View			
			٠	<b>(a)</b> 🔆			
	FortiSoC	Reports	System Settings	Management Extensions			
	Lig Verw +         Image: Constraint of the constrai	Hour + 13.01:47 To 14.01:48	Action Message	>_ @ (A) votnin			
	Dent         1         135911           Summary         2         135911           All Frien         3         135731           Enspeide         4         135716           Security Rating         6         134229           SDN Convector         7         134229	Hommotion FG180EFK18022900 information FG180EFK18022900 notice FG180EFK18022900 notice FG180EFK18022900 notice FG180EFK18022900 notice FG180EFK18022900 notice FG180EFK18022900	O     OHCP stabilities     OHCP stabilities     OHCP stabilities     Performance stabilities     Performance stabilities     performance stabilities     performance stabilities	Losenicad     Case Sensitive Search     Lose Sensitive Search     Lour Builder     User Display Preferences			
	System         0         13.0729           VPN         9         13.0226           SF entibulyzer         10         132727           St fortibulyzer         11         132727           St lag Browse         12         132227           St lag Browse         12         132227           St lag Browse         13         132727           St lag Browse         14         131231	robu FGTBEFKL892290 noten FGTBEFKL8922900 noten FGTBEFKL8922900 noten FGTBEFKL8922900 noten FGTBEFKL8922900 noten FGTBEFKL8922900 noten FGTBEFKL8922900 noten FGTBEFKL8922900	porf-stats Performance statistics.     perf-stats Performance statistics.     perf-stats Performance statistics.     porf-stats Performance statistics.     porf-stats Performance statistics.     perf-stats Performance statistics.     porf-stats Performance statistics.				
Comentário	15 130730 16 130229	notice FGTE0ETK18012960	0 perf-stats Performance statistics 0 perf-stats Performance statistics				

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



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

5.4.39 Solução deve incluir monitoramento gráfico que fornece uma maneira fácil

monitorar o status de gateways, apresentando os seguintes status:

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

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

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





Item de Teste - 5.4.39.3	Informações de conexões concorrentes dos gateways gerenciados;			
Objetivo do Teste	Verificar se a solução de gerenciamento possui visualização da quantidade de conexões			
	concorrentes dos gateways gerenciados.			
Configuração do Teste	Demonstrar consume de conexões concorrentes por gateways gerenciados.			
Procedimento do Teste	Demonstrar consume de conexões concorrentes por gateways gerenciados.			
Evidências	Na aba de "Device Manager" podemos selecionar qualquer um dos equipamentos gerenciados.			
	Quando fazemos isso, podemos ter visualização de diversas informações daquele equipament	о,		
	entre elas, a quantidade de conexões concorrentes.			
	🗱 Device Manager 🗸 🗮 📼 Add Device 🔹 🎬 Device Group 🔹 🗄 Install Wizard			
	Ma     Device Manager     Policy & Objects     AP Manager     VPN Manager     Fabric View			
	FortiGuard FortiSwitch Manager Extender Manager System Settings Management			
	Extensions			
	12       Device Manager →       ≣       B Add Device Amp +       ≥       benz Amp +       ≥       0 +       App + </th <th></th>			
	Is loads         Q.         Security Horizon         05.1           (Magazi Forcilian II)         Security Horizon         13.25         11.25         11.45           Convert Horizon V(D)         Security Horizon         Convert Horizon         Convert Horizon         11.45			
	Outgoing Devices (1)     A Fateroid       a Collemo, Selle SCDUC     D Statutori       b System     Sections			
	B Soros E Fenue Vabity  C Provisive Deptites → 20			
	Transe Reputes     Difference in the second se			
	10			
	10			
	30			
	120 11.53 11.53 11.55 11.65			
	Careet feature \$4			
Comentário				
		-		

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



Configuração do Teste	Demonstrar alerta de equipamento indisponível.			
Procedimento do Teste	Demonstrar alerta de equipamento indisponível.			
Evidências	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.         Image: Porter Manager v       E Orde Device Group v         Image: Noter Manager v       E Orde Device Group v			
	Image: Device Manager     Policy & Objects     AP Manager     VPN Manager     Fabric View			
	FortiGuard       FortiSwitch Manager       Extender Manager       System Settings       Management Extensions			
	HA Status C 🖸 🖸 = -			
	HA Mode Active-Pasilve Cluter Name SEDUC C2 Uptime 5 hours 23 minutes 42 seconds State Changed 5 hours 23 minutes 32 seconds			
	Cluster Members			
	Serial Number ≎         Serial Number ≎         Serial Status ≎         Role ≑			
	FGT80CTK18012960 FGT80CTK18012960 Finany FGT80CTK18012960 Finany			
Comentário				

Suportar rollback	do configuração no	ra a viltima configu		
Suportar rollback de configuração para a última configuração salva e do sistema operacional para a última versão local;				
Verificar se o equipamento de gerência suporta rollback de configuração.				
Demonstrar rollba	ck de configuração.	·		
Demonstrar rollback de configuração.				
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				
System Settings 🗸	≡			
• III • III		((•))		
Device Manager	Policy & Objects	AP Manager	VPN Manager	Fabric View
FortiGuard	FortiSwitch Manager	Extender Manager	System Settings	Image: Second se
	para a última versá Verificar se o equip Demonstrar rollba Demonstrar rollba Na parte de "Sy FortiManager, entr foi tirado System Settings • © III © III Device Manager FortiGuard	para a última versão local; Verificar se o equipamento de gerênci Demonstrar rollback de configuração. Demonstrar rollback de configuração. Na parte de "System Settings pod FortiManager, entre elas a configuraçã foi tirado <u>System Settings – E</u> <u>e III e III Device Manager</u> Policy & Objects FortiGuard	para a última versão local;         Verificar se o equipamento de gerência suporta rollback         Demonstrar rollback de configuração.         Demonstrar rollback de configuração.         Na parte de "System Settings podemos ter uma ta         FortiManager, entre elas a configuração atual do sistema         foi tirado         System Settings           Policy & Objects         AP Manager         FortiGuard         FortiSwitch Manager         Extender Manager	para a última versão local; Verificar se o equipamento de gerência suporta rollback de configuração. Demonstrar rollback de configuração. Demonstrar rollback de configuração. Na parte de "System Settings podemos ter uma tabela com diversa FortiManager, entre elas a configuração atual do sistema e qual foi a última foi tirado System Settings → E Policy & Objects AP Manager FortiGuard Policy & Objects Configuração FortiSwitch Manager Extender Manager



	Г	
	System Information	Ø ¥ Ω ≡ ~
	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	0
	FortiAnalyzer Features	0
	System Configural	tion Last Backup : Tue Mar 14 14:21:00 2023
		Upload file by drag & drop here or Browse
	Password	Maximum password length: 63
	rassword	
		Overwrite current IP, routing and HA settings
		🗹 Restore in Offline Mode 🍳
		OK Cancel
Comentário		A

#### 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 - 8° ANDAR - CEP 70.070-120 - ASA SUL-BRASÍLIA/DF



#### 8.1.2. IPSEC VPN CONFORME OS SUBITENS DO ANEXO VII:

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

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

#### 8.1.3. NOVAS CONEXÕES POR SEGUNDO:

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

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

#### 8.1.4. CONEXÕES CONCORRENTES:

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

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

8.2. TESTES DE CAPACIDADE 8.2.1. TOPOLOGIA



#### 8.2.1.1. • TESTE 01 – THROUGHPUT

- Tráfego Enterprise Mix
- Base de Regras com funcionalidades:
  - Firewall, IPS, Controle de Aplicação, Proteção Contra Malware;
  - Logging habilitado para todas as sessões e conexões;
  - Capacidade mínima considerada para aferimento sendo acima do requisitado conforme itens supracitados;
- Janela de teste composta por duas fases sendo:
  - <u>Rampa de subida</u> 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 - 8° ANDAR - CEP 70.070-120 - ASA SUL-BRASÍLIA/DF



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

#### 8.2.1.2. TESTE 02 - IPSEC VPN

- Criptografia AES256-SHA256
- Janela de teste composta por duas fases sendo:
  - <u>Rampa de subida</u> com tempo inferior a 1 minuto que não será considerada para aferição;
  - <u>Curso após estabilização</u> 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:
  - <u>Rampa de subida</u> 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:
  - <u>Rampa de subida</u> com tempo inferior a 1 minuto que não será considerada para aferição;
  - <u>Curso após estabilização</u> 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

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





Brasília/DF, 23 de junho de 2023

JOSÉ ARMANDO DOS REIS COSTA DIRETOR FECNICO

CRYSTINE JÓRANHEZON RODRIGUES GERENTE DE DESENVOLVIMENTO DE NEGÓCIOS NCT-HYFORMÁTICA

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