Configurar Políticas de Controle de Acesso de Plano de Controle para Secure Firewall Threat Defense e ASA

Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Configurar
Configurações
Configurar uma ACL de plano de controle para o FTD gerenciado pelo FMC
Configurar uma ACL de plano de controle para FTD gerenciado pelo FDM
Configurar uma ACL de plano de controle para ASA usando CLI
Configuração alternativa para bloquear ataques para um firewall seguro usando o comando <u>'shun'</u>
Verificar
Bugs relacionados

Introdução

Este documento descreve o processo para configurar as regras de acesso ao plano de controle para Secure Firewall Threat Defense e Adaptive Security Appliance (ASA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Defesa contra ameaças de firewall (FTD) segura
- Gerenciador de Dispositivos de Firewall Seguro (FDM)
- Centro de gerenciamento seguro de firewall (FMC)
- ASA com firewall seguro
- Lista de controle de acesso (ACL)
- FlexConfig

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Secure Firewall Threat Defense versão 7.2.5
- Secure Firewall Manager Center versão 7.2.5
- Secure Firewall Device Manager versão 7.2.5
- Secure Firewall ASA versão 9.18.3

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O tráfego geralmente atravessa um firewall e é roteado entre interfaces de dados; em algumas circunstâncias, é benéfico negar o tráfego destinado 'para' o firewall seguro. O firewall seguro da Cisco pode usar uma lista de controle de acesso (ACL) do plano de controle para restringir o tráfego "para a caixa". Um exemplo de quando uma ACL de plano de controle pode ser útil seria controlar quais pares podem estabelecer um túnel VPN (Site-to-Site ou VPN de Acesso Remoto) para o firewall seguro.

Tráfego "pronto para usar" do Secure Firewall

O tráfego normalmente atravessa firewalls de uma interface (de entrada) para outra interface (de saída), o que é conhecido como tráfego "através da caixa" e é gerenciado por ambas, as Políticas de Controle de Acesso (ACP) e as regras de Pré-filtro.



Imagem 1. Exemplo de tráfego por meio da caixa

Tráfego "pronto para usar" do firewall seguro

Há outros casos em que o tráfego é diretamente destinado a uma interface FTD (Site-to-Site ou Remote Access VPN), isso é conhecido como tráfego "to-the-box" e é gerenciado pelo plano de controle dessa interface específica.



Imagem 2. Exemplo de tráfego pronto para usar

Considerações importantes sobre ACLs de plano de controle

- A partir do FMC/FTD versão 7.0, uma ACL de plano de controle deve ser configurada usando FlexConfig, usando a mesma sintaxe de comando usada no ASA.
- A palavra-chave control-plane é anexada à configuração do grupo de acesso, que aplicará o tráfego 'para' a interface de firewall segura. Sem a palavra de plano de controle anexada ao comando, a ACL restringiria o tráfego "através" do firewall seguro.
- Uma ACL de plano de controle não restringirá a entrada SSH, ICMP ou TELNET a uma interface de firewall segura. Eles são processados (permitidos/negados) de acordo com as políticas de configurações de plataforma e têm uma precedência mais alta.
- Uma ACL de plano de controle restringe o tráfego 'para' o próprio firewall seguro, enquanto a Política de controle de acesso para o FTD ou as ACLs normais para o ASA, controla o tráfego 'através' do firewall seguro.
- Diferentemente de uma ACL normal, não há um 'deny' implícito no final da ACL.
- No momento em que este documento está sendo criado, o recurso Geolocalização do FTD não pode ser usado para restringir o acesso 'ao' FTD.

Configurar

No próximo exemplo, um conjunto de endereços IP de um determinado país tenta forçar a VPN na rede tentando fazer login no FTD RAVPN. A melhor opção para proteger o FTD contra esses ataques de força bruta de VPN é configurar uma ACL de plano de controle para bloquear essas conexões à interface externa do FTD.

Configurações

Configurar uma ACL de plano de controle para o FTD gerenciado pelo FMC

Este é o procedimento que você precisa seguir em um FMC para configurar uma ACL de plano de controle para bloquear ataques de força bruta de VPN de entrada para a interface FTD externa:

Etapa 1. Abra a interface gráfica do usuário (GUI) do FMC via HTTPS e faça login com suas

credenciais.



Imagem 3. Página de início de sessão do FMC

Etapa 2. Você precisa criar uma ACL estendida. Para isso, navegue até Objetos > Gerenciamento de objetos.

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy Q 🤞	📍 🔅 🕜 admir	t▼ distin SECURE
Summary Dashboard (switch dashboard) Provides a summary of activity on the appliance					Object M Intrusion	lanagement Rules				Reporting
Network × Threats Intrusion Events	Status 0	Geolocation	QoS					Show the Last	1 hour	• 11
Unique Applications over Time	-	- × 🕨	Top Web App	lications Seen				Top Client Applications Seen		
No Data Last updated 2 minutes ago				utes ago	No Data			N Last updated 2 minutes ago	lo Data	
Traffic by Application Risk	-	- ×	Top Conver Ar	onlightions Cos				Top Operating Systems Sage		
			TOP Server Ap	диканны See			- ×	Top operating systems seen		

Imagem 4. Gerenciamento de objetos

Etapa 2.1. No painel esquerdo, navegue até Lista de acesso > Estendida para criar uma ACL estendida.

Firewall Managemen	t Center _{Overview}	Analysis Policies	Devices	Objects	Integration		Deploy Q 🤞	📍 🌣 🕝 admin •	cisco SECURE
> AAA Server Access List Extended Standard 	A network object represents network discovery rules, eve	s one or more IP addresses ent searches, reports, and s	. Network objects o on.	s are used in v	arious places, ir	Add Network	▼ icies, network variab	Filter Show Unused Objectes, intrusion rules, identified	ts y rules,
> Address Pools	Name				1	Value	Туре	Override	
Application Filters AS Path	any					0.0.0/0 ::/0	Group		ବ ≣ #
Cipher Suite List	any-ipv4				(0.0.0/0	Network		Q ≣ ₿
> Community List	any-ipv6					::/0	Host		۵ 🗑 👪
 Distinguished Name DNS Server Group 	IPv4-Benchmark-Tests					198.18.0.0/15	Network		Q ≣ ₿
> External Attributes	IPv4-Link-Local					169.254.0.0/16	Network		९ च ₩
File List	IPv4-Multicast				:	224.0.0.0/4	Network		ୟ 🗑 👪
Geolocation	IPv4-Private-10.0.0.0-8					10.0.0.0/8	Network		Q ≣ ₿
Interface	IPv4-Private-172.16.0.0-12					172.16.0.0/12	Network		९ ≣ ₿
Key Chain	IPv4-Private-192.168.0.0-16	5				192.168.0.0/16	Network		ର ≣ ଲ
> PKI	IPv4-Private-All-RFC1918					10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Group		ବ 🗑 👪
Policy List Port							Displaying 1 - 14 of 14	4 rows K < Page 1	of 1 > > C

Imagem 5. Menu da ACL estendida

Etapa 2.2. Em seguida, selecione Adicionar lista de acesso estendida.

Firewall Management	t Center _{Overview}	Analysis	Policies De	vices Objects	Integration	Deploy	९ 🤩 🗘 📀	admin 🕶 🏻 🗧	SECURE
> AAA Server	Extended					Add Extended Access	List Q. Filter		
✓ Access List	An access list chiest also	known as an acces	e control liet (AC) celects the traffic	to which a cancice will apply Str	ndard-Idantifiae traffic bas	ad on destination of	ldrees only k	lantifica
Extended	traffic based on source and	d destination addres	ss and ports. Sup	ports IPv4 and IPv6	addresses. You use these object	s when configuring particula	ar features, such as	route maps.	Jenunes
Standard									
> Address Pools	Name					Value		Override	
Application Filters					No records to display				
AS Path									
Cipher Suite List									
> Community List									
> Distinguished Name									
DNS Server Group									
> External Attributes									
File List									
> FlexConfig									
Geolocation									
Interface									
Key Chain									
Network									
> ркі									
Policy List									
Port						No d	ata to display I< <	Page 1	of 1 > > C
> Prefix List									

Imagem 6. Adicionar ACL estendida

Etapa 2.3. Digite um nome para a ACL estendida e clique no botão Adicionar para criar uma entrada de controle de acesso (ACE):

Firewall Mana Objects / Object M	agement Ce anagement	nter	Overview	Analysis	Policies	Devices	o Objects	Integ	ration		Deploy	۹	e 🔹	🕜 admin '	• altalia cisco	SECURE
> AAA Server	New Exte	nded Acc	cess List Ob	ject												
Extended	Name ACL-UNW	ANTED-CO	UNTRY											dress o oute m	nly. Identi aps.	ifies
Address Pools Application Eiltere	Entries (0)													Overri	de	
AS Path													Add			
Cipher Suite List Community List	Sequence No record	Action s to display	Source		Source Port		Destination		Destination Port	Application	n					
 Distinguished Name DNS Server Group 																
 External Attributes File List 																
> FlexConfig Geolocation	Allow Ov	errides														
Key Chain Network													Save			
> PKI Policy List																
Port											No	o data to	o display ∣<	< Page 1	of 1	

Imagem 7. Entradas de ACL estendida

Etapa 2.4. Altere a ação ACE para Block (Bloquear), adicione a rede de origem para corresponder ao tráfego que precisa ser negado para o FTD, mantenha a rede de destino como Any (Qualquer) e clique no botão Add (Adicionar) para concluir a entrada ACE:

- Neste exemplo, a entrada ACE configurada bloqueará ataques de força bruta de VPN provenientes da sub-rede 192.168.1.0/24.

Firewa Objects /	Action: Block			cisco SECURE
> AAA Server	Logging: Default			
Extended	Log Level:			Identifies 3.
Standard Address Pools	Log Interval:			
Application Filt AS Path	300 Sec. Network Port () Application			/ ≣ 88
Cipher Suite Lis	Available Networks C +	Source Networks (1)	Destination Networks (0)	
> Distinguished N	Q Search by name or value	192.168.1.0/24	any	
DNS Server Gro	any Add to Source			
> External Attribu	any-ipv4 Add to Destination			
File List	any-ipv6			
> FlexConfig	IPv4-Benchmark-Tests			
Geolocation	IPv4-Link-Local			
Interface	IPv4-Multicast			
Key Chain	IPv4-Private-10.0.0.0-8			
Network	IPv4-Private-172.16.0.0-12	Enter an IP address Add	Enter an IP address Add	
> ркі				
Policy List				
Port			Cancel	
> Prefix List			Calleer	

Imagem 8. Redes negadas

Etapa 2.5. Caso precise adicionar mais entradas ACE, clique no botão Add novamente e repita a etapa 2.4. Depois disso, clique no botão Save (Salvar) para concluir a configuração da ACL.

Firewall Managemen Objects / Object Management	Edit Exten	Edit Extended Access List Object										
➢ AAA Server ✓ Access List	Name ACL-UNW	ANTED-CC	DUNTRY									
Extended	Entries (1)											
Standard								Add				
> Address Pools								_				
Application Filters	Sequence	Action	Source	Source Port	Destination	Destination Port	Application		人主体			
AS Path	1	Block	192.168.1.0/24					11				
Cipher Suite List												
> Community List												
> Distinguished Name												
DNS Server Group												
> External Attributes												
File List	Allow Ov	verrides										
> FlexConfig												
Geolocation								Four				
Interface								Jave				
Key Chain												
Network												
> ркі												
Policy List												
Port							Displaying 1 - 1 of 1 rows	I< < Page 1	of 1 > > C			
> Prefix List												

Imagem 9. Entradas de ACL estendida concluídas

Etapa 3. Em seguida, você precisa configurar um Objeto de configuração flexível para aplicar a ACL do plano de controle à interface FTD externa. Para isso, navegue até o painel esquerdo e selecione a opção FlexConfig > Objeto FlexConfig.

Firewall Managemen	t Center _{Overvie}	w Analysis	Policies	Devices	Objects	Integration		Deploy	۹ 🤞	° 0	admin 🕶 🛛	cisco SECURE
> AAA Server	Extended						Add Ext	tended Acces	s List	Q Filter		
✓ Access List												
Extended	An access list object, al traffic based on source	so known as an ac and destination ad	cess control list dress and port	st (ACL), select s. Supports IPv	ts the traffic to /4 and IPv6 ad	which a service will ap dresses. You use these	pply. Standard-Iden e objects when con	ntifies traffic ba ifiguring partic	ased on de ular featu	estination a res. such a	address only. Is route map:	. Identifies s.
Standard												
> Address Pools	Name						Value				Override	
Application Filters	ACL-UNWANTED-COUN	ITRY										1 🖬 🕅
AS Path												
Cipher Suite List												
> Community List												
> Distinguished Name												
DNS Server Group												
> External Attributes												
File List												
✓ FlexConfig												
FlexConfig Object												
Text Object												
Geolocation												
Interface												
Key Chain												
Network												
> ркі								Displaying	1 - 1 of 1	rows K <	Page 1	of 1 > > C
Deline List												



Etapa 3.1. Clique em Adicionar objeto FlexConfig.

Firewall Manageme	nt Center Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ 🍨 ۹	🗘 🕜 admi	in 🕶 🛛 🗄 cisco SECURE
> AAA Server ~ Access List Extended Standard	FlexConfig Object include o	Ct levice configurat	ion command	s, variables, a	nd scripting la	nguage instruction	ns. It is used in FlexCon	d FlexConfig Ot	əject Q	Filter	
> Address Pools	Name							Description			
Application Filters AS Path	Default_DNS_Configure							Configure Defa	ault DNS with	the help of Tex	ktObj 🖥 🤉 🗑
Cipher Suite List	Default_Inspection_Protocol	_Disable						Disable Defaul	t Inspection.		¶∎ <.]
> Community List	Default_Inspection_Protocol	_Enable						Enable Default	Inspection.		¶∎ Q 🗑
Distinguished Name	DHCPv6_Prefix_Delegation_	Configure						Configure one	outside (PD	client) and one	insid 🖪 🤇 🗑
External Attributes	DHCPv6_Prefix_Delegation_	UnConfigure						Remove config	guration of on	e outside (PD o	client 🐴 Q 🗎
File List	DNS_Configure							Configure DNS	s with the hel	p of TextObject	ts dn 📲 🔍 🗑
 FlexConfig ElexConfig Object 	DNS_UnConfigure							Remove the D	NS configural	tions.	Pa Q 🗑
Text Object	Eigrp_Configure							Configures eig	rp. 1. Config	ures next hop. :	2. co 📲 🤍 🗑
Geolocation	Eigrp_Interface_Configure							Configures inte	erface param	eters for eigrp.	1. C 📲 Q 🗑
Interface	Eigro UnConfigure							Clears eigro c	onfiguration f	or an AS	¶a, jj
Key Chain								01			E o T
> PKI	Eigrp_Unconfigure_All							Displaying 1 -	20 of 48 row	s I< < Page	1of3 > >) C

Imagem 11. Adicionar Objeto Flexconfig

Etapa 3.2. Adicione um nome para o objeto FlexConfig e insira um objeto de política de ACL. Para isso, selecione Inserir > Inserir objeto de política > Objeto de ACL estendida.

Firewall Manageme	Name:						⊱ 🙆 admin 🕶	abala SECURE
Objects / Object Manageme	OBJ-FC-CONTROL-PLANE							
> AAA Server	Description:						Filter	
✓ Access List								
Extended	Copy-pasting any rich te	ext might introduce line break	s while generating CLI.	Please verify the	CLI before deploy	ment.		
Standard	Insert - Bi D	Deployment: Once		Type:	Append			
> Address Pools	Insert Policy Object	Text Object			reported			
Application Filters	Insert System Variable >	Network					the help of TextObj	- ¶∎ Q =
AS Path	Insert Secret Key	Security Zones						Ra a ⊒
Cipher Suite List		Standard ACL Object						
Community List Distinguished Name		Extended ACL Object						¶a ⊂ ⊤
DNS Server Group		Route Map					lient) and one insid	. ¶∎ Q 🗑
> External Attributes							e outside (PD client	F a ⊂
							of TextObjects dn.,	ମ୍ କୁ ର୍ କି
✓ FlexConfig	▼ Variables							Bo E
	Name	Dimension	Default Value	Property (Typerblame)	Override	Description	ions.	
Text Object			No records to de	(Type.Name)			res next hop. 2. co	- ¶∎ ⊂,
Geolocation			No records to de	spiay			eters for eigrp. 1. C	⊑ < <u></u>
Interface							ar an AS	Fa 0, 🗑
Key Chain								
Network								
2 PKI							Save	

Imagem 12. Variável de objeto FlexConfig

Etapa 3.3. Adicione um nome para a variável de objeto ACL e, em seguida, selecione a ACL estendida que foi criada na Etapa 2.3, depois disso, clique no botão Salvar.

Firewall Managemen	Name: OBJ-FC-CONTROL-PLANE	:			⊁ 🕑 admin ▾ 🏻 🖞	SECURE
> AAA Server ~ Access List	Description:	Insert Extended Access List Object Va	riable 🛛 🕥		Filter	
Extended Standard > Address Pools Application Filters AS Path Cipher Suite List > Community List > Distinguished Name DND Common Comm	Copy-pasting any rich	Variable Name: VAR-ACL-UNWANTED-COUNTRY Description: Available Objects C Q Search	Selected Object		the help of TextObj	日 日 へ 日日 へ 日日 へ 日日 へ 日日 へ
External Attributes File List FlexConfig	▼ Variables	Add			 outside (PD client of TextObjects dn ions. 	1
Text Object Geolocation Interface Key Chain	Name		Cancet	ription	res next hop. 2. co hters for eigrp. 1. C or an AS	Γ 3 α = Γ3 α = Γ3 α =
Network > PKI Policy List				Cancel Save	s I< < Page 1	ng Q of 3 > > C

Imagem 13. Atribuição de ACL variável de objeto FlexConfig

Etapa 3.4. Em seguida, configure a ACL do plano de controle como entrada para a interface externa da seguinte maneira.

Sintaxe da linha de comando:

```
access-group "variable name starting with $ symbol" in interface "interface-name" control-plane
```

Isso se traduz no próximo exemplo de comando, que usa a variável ACL criada na Etapa 2.3 acima 'VAR-ACL-UNWANTED-COUNTRY' da seguinte maneira:

access-group \$VAR-ACL-UNWANTED-COUNTRY in interface outside control-plane

É assim que ele deve ser configurado na janela do objeto FlexConfig. Depois disso, selecione o botão Salvar para concluir o objeto FlexConfig.

Firewall Manageme	Name: OBJ-FC-CONTROL-PLANE						≵ 🥝 admin v "≵	secure
> AAA Server	Description:						Filter	
✓ Access List								
Extended	A Copy-pasting any rich text might in	troduce line breaks	s while generating CLI.	Please verify the	CLI before deploy	ment.		
Standard								
> Address Pools	Insert V 🔢 Deployment	Once		Type:	Append	•		
Application Filters	access-group \$VAR-ACL-UNWANTED-COUN	TRY in interface outsid	e control-plane				the help of TextObj	₽ _ 0,]
AS Path								Bo =
Cipher Suite List								
> Community List								¶∎ Q
> Distinguished Name							lient) and one insid	Ela Q ≣
DNS Server Group								
> External Attributes							e outside (PD client	Г а ()
							of TextObjects dn	₽ a ⊂
✓ FlexConfig	▼ Variables							B. A. E
	Name	Dimension	Default Value	Property	Override	Description	lons.	
Text Object				(Type:Name)			ires next hop. 2. co	¶∎ Q
Geolocation	VAR-ACL-UNWANTED-COUNTRY	SINGLE	ACL-UNWANTED	EXD_ACL:A	false		eters for eigro. 1. C	En α ⊒
Interface								
Key Chain							or an AS	Fi Q 📄
Network								¶a q =
> ркі							s IK < Page 1	of 3 > > C
Policy List						Cancel Save		

Imagem 14. Linha de comando completa do Objeto Flexconfig

Etapa 4. Você precisa aplicar a configuração do Objeto FlexConfig ao FTD; para isso, vá para Dispositivos > FlexConfig.

Firewall Management Objects / Object Management	Center _{Overview} Analysis Policies	Devices Objects	Integration	Deploy Q 🧬 🗧	🔅 🎯 admin 🕇 🏻	SECURE
AAA Server Access List Extended Standard Address Pools Application Filters AS Path	FlexConfig Object FlexConfig Object include device configuration commands Name Defaul	Device Management Device Upgrade NAT QoS Platform Settings FlexConfig Certificates	VPN Site To Site Remote Access Dynamic Access Policy Troubleshooting Site to Site Monitoring	Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture	ilter	₽ Q
Cipher Suite List	Default_Inspe	ction_Protocol_Disable		Disable Default Inspection.		¶a Q
> Community List	Default_Inspe	ection_Protocol_Enable		Enable Default Inspection.		¶∎ Q
> Distinguished Name DNS Server Group	DHCPv6_Preft	x_Delegation_Configure		Configure one outside (PD	client) and one insid	₽ 0, ``
> External Attributes	DHCPv6_Prefix	_Delegation_UnConfigure		Remove configuration of on	e outside (PD client	₽ 0,
File List	DN	IS_Configure		Configure DNS with the help	p of TextObjects dn	Pa Q 🗎
✓ FlexConfig	DNS	_UnConfigure		Remove the DNS configurat	tions.	Γ α]
FlexConfig Object	Fig	ro Configure		Configures sigm 1 Config	urge part hop 2 co	E o =
Geolocation		ip_conigue		Conligues eigip, 1, Conlig	ares next nop. z. co	
Interface	Eigrp_In	iterface_Configure		Configures interface param	eters for eigrp. 1. C	а (
Key Chain	Eigr	p_UnConfigure		Clears eigrp configuration f	or an AS	Pa Q 📄
Network	Eigrp_	Unconfigure_All		Clears eigrp configuration.		¶a q
> ркі				Displaying 1 - 20 of 49 row	vs K < Page 1	of 3 > > C

Imagem 15. Menu Política do FlexConfig

Etapa 4.1. Em seguida, clique em Nova política se ainda não houver um FlexConfig criado para o FTD ou edite a política FlexConfig existente.

Ę	Firewall Management Center Devices / FlexConfig	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	م	e 🕹	🕜 admin -	cisco SECURE
													New Policy
	FlexConfig Policy			Status				Last Modified					
						created. Add	a new policy						

Imagem 16. Criação de política FlexConfig

Etapa 4.2. Adicione um nome para a nova política FlexConfig e selecione o FTD ao qual deseja aplicar a ACL de plano de controle criada.

Firewall Management Center	Overview Analysis Policies Devices Objects Integration	Deploy Q 🤩 🌣 🎯 admin 🗸 🗄
FlexConfig Policy	New Policy	0
	Name: FLEXCONFIG-POLICY Description: Targeted Devices Select devices to which you want to apply this policy. Available Devices Q. Search by name or value FTD-CONTROL-PLANE Add to Policy	
	Cancel	Save

Imagem 17. Atribuição de dispositivo de Política FlexConfig

Etapa 4.3. No painel esquerdo, procure o objeto FlexConfig criado na etapa 3.2 acima e, em seguida, adicione-o à política FlexConfig clicando na seta para a direita localizada no meio da janela. Depois disso, clique no botão Salvar.

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	م	🥐 🌣	❷ admin • ;	SECURE
FLEXCONFIG-POLICY										v Config Save	Cancel
										Policy As	ssignments (1)
	"3 Solooto	d Dropond F	lovConfigs								
Available FlexConfig	Selecte	a Prepena P	lexconligs								
	# Nan	10		C	Description						
V User Defined											
OBJ-FC-CONTROL-PLANE											
✓ System Defined											
Topfault_DNS_Configure											
Default_Inspection_Protocol_Disable											
Contemporary Conte	_ Selecte	d Append F	lexConfigs								
Therefix_Delegation_Configure											
DHCPv6_Prefix_Delegation_UnConfigure	# Nan	ne		C	Description						
TDNS_Configure	1 овј	-FC-CONTROL	-PLANE								۹ 🖥
DNS_UnConfigure	ц										
"B Eigrp_Configure											
B Eigrp_Interface_Configure											
_9 Eigrp_UnConfigure											

Imagem 18. Atribuição de objeto de Política FlexConfig

Etapa 5. Continue a implantar a alteração de configuração no FTD, para isso, navegue até Implantar > Implantação avançada.

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q	. 🤗 🌣	🍘 admin •	cisco SE	CURE
FLEXCONFIG-POLICY								Advanced	Deploy De	ploy All	ncel
Enter Description						FTD-CONTROL-PLANE		Ready for D	eployment	4	.s (1)
Available FlexConfig A FlexConfig Object	n Selecte	ed Prepend F	lexConfigs								
×	# Nar	ne			Description						
✓ User Defined											
OBJ-FC-CONTROL-PLANE											
✓ System Defined											
Configure						• • • • • • • • • • • • • • • • • • •					
Default_Inspection_Protocol_Disable						1 device is available for deployment				12 49	
Default_Inspection_Protocol_Enable	Selecte	ed Append Fl	exConfigs								
DHCPv6_Prefix_Delegation_Configure	# Nar	ne			Description						
DNS Configure	1 OB	J-FC-CONTROL	-PLANE								۹.
DNS_UnConfigure											

Imagem 19. Implantação Avançada de FTD

Etapa 5.1. Em seguida, selecione o FTD ao qual deseja aplicar a política FlexConfig. Se tudo estiver correto, clique em Implantar.

P	Fi	rewall Management Center ploy / Deployment	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ 🇳	🔅 🕜 admin 🕶 🏻	elsee SECURE
1 devic	ce sele	ected Search using device name, user name, type,	, group or statu	15								Deploy time: Estimat	Deploy
	Z	Device	Modified by		Inspect Inte	rruption	Туре	Group	Last Deploy Time		Preview	Status	
×		FTD-CONTROL-PLANE	admin				FTD		Sep 5, 2023 12:0	5 PM	B	Ready for Deployme	nt
*= •		Flex Configuration Template Policy; FLEXCONFIG-POLICY											
https://10.	88.243	3.58:43013/ddd/#ContextExplorer											

Imagem 20. Validação da implantação do FTD

Etapa 5.2. Depois disso, uma janela de confirmação da implantação será exibida, adicionará um comentário para rastrear a implantação e continuará a implantação.

Firewall Management Center Deploy / Deployment						🕻 🧬 🌣 🔞 admin v	
1 device selected							
	Modified by						
V FTD-CONTROL-PLANE	admin			Sep 5, 2023 1	2:05 PM	Ready for Deployme	
Flex Configuration Template Policy: FLEXCONFIG-POLICY		Deployment Confirmation		×			
—		Deployment Notes:					
		You can optionally add notes about t	the configuration changes				
				Deploy			

Imagem 21. Comentários de implantação do FTD

Etapa 5.3. Uma mensagem de aviso pode ser exibida durante a implantação de alterações de FlexConfig. Clique em Implantar somente se tiver certeza completa de que a configuração de política está correta.



Imagem 22. Aviso do Flexconfig de Implantação do FTD

Etapa 5.4. Confirme se a implantação da política foi bem-sucedida para o FTD.

Ð	Fi De	rewall Management Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy Q	🧬 🌣 🕜 adn	nin ▼
Ţ	۹	Search using device name, user name, type,	group or statu	is								Deploy
		Device	Modified by		Inspect Inte	rruption 1	Гуре	Group	Last Deploy Time	Preview	Status	
~		FTD-CONTROL-PLANE	admin			F	TD		Sep 5, 2023 12:05	рм 🖪	Completed	
:: •		 Flex Configuration Template Policy: FLEXCONFIG-POLICY 										



Etapa 6. Se você criar uma nova ACL de plano de controle para o FTD ou se editou uma ACL existente que esteja ativamente em uso, é importante destacar que as alterações de configuração feitas não se aplicam a conexões já estabelecidas com o FTD, portanto, você precisa limpar manualmente as tentativas de conexão ativas ao FTD. Para isso, conecte-se ao CLI do FTD e limpe as conexões ativas da seguinte maneira.

Para limpar a conexão ativa para um endereço IP de host específico:

> clear conn address 192.168.1.10 all

Para limpar as conexões ativas de toda uma rede de sub-rede:

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

Para limpar as conexões ativas para um intervalo de endereços IP:

> clear conn address 192.168.1.1-192.168.1.10 all

Observação: é altamente recomendável usar a palavra-chave 'all' no final do comando clear conn address para forçar a limpeza das tentativas de conexão de força bruta de VPN ativas para o firewall seguro, principalmente quando a natureza do ataque de força bruta de VPN está iniciando uma explosão de tentativas de conexão constantes.

Configurar uma ACL de plano de controle para FTD gerenciado pelo FDM

Este é o procedimento que você precisa seguir em um FDM para configurar uma ACL de plano de controle para bloquear ataques de força bruta de VPN recebidos para a interface FTD externa:

Etapa 1. Abra a GUI do FDM via HTTPS e Efetue login com suas credenciais.



cisco SECURE

Cisco Secure Firewall Device Manager

Username	
Password	
Password	O
	LOG IN

© 2015-2023 Clisco Systems, Inc. Clisco, Clisco Systems and Clisco Systems logo are registered trademarks of Clisco Systems, Inc. This product contains some software licensed under the "GNU Lesser General Public License, versions: 2, 2, 1 and 3" provided with ASSULTEY INO WARRANTY under the terms of "GNU Lesser General Public License, versions 2, 2, 1 and 4" provided with

Firewall Device Manager	500 Monitoring	⑦ Policies Objects	Device: firepowe	er	>		•	admin Administrator	
Model Cisco Firepo	ower Threat Defense	for VMwa Software	VDB Intrusion 353.0 202205	n Rule Update Cloud Se 11-1540 🛞 Not I	ervices Registered Re	High A	vailability 🧑	CONFIGURE	
	Finide Netwo	Cisco Firepower Thr	0/1 eat Defense for VMwar 0/0 0/1 1 0/0 0/0		ISP/WA	N/Gateway (DNS Ser	et iver License	
Interfaces Connected Enabled 3 of 3 View All Interfaces	>	Routing There are no static rout View Configuration	tes yet	Updates Geolocation, R Security Intellig View Configur	ule, VDB, Syst jence Feeds ration	em Upgrade, >	S) M La Di	iystem Settings lanagement Access ogging Settings HCP Servic / Relay DNS Service	
Smart License Evaluation expires in 89 days	89 DAYS	Backup and Rest	ore	Troublesho	ot d yet		- Di M Ho Ti	NS Server lanagement Interface ostname ime Services	

Etapa 2. Você precisa criar uma rede de objetos. Para isso, navegue até Objetos:

Imagem 25. Painel principal do FDM

Etapa 2.1. No painel esquerdo, selecione Redes e clique no botão '+' para criar um novo objeto de rede.

Firewall Device Manager	Monitoring Policies Objects Device: firepov	ar () admin
Object Types ←	Network Objects and Groups	
C Networks	6 objects	▼ Filter + 💭
S Ports		Preset filters: System defined, User defined
Security Zones	# NAME	TYPE VALUE ACTIONS
🐬 Application Filters	1 IPv4-Private-10.0.0-8	NETWORK 10.0.0/8
A URLs	2 IPv4-Private-172.16.0.0-12	NETWORK 172.16.0.0/12
	3 IPv4-Private-192.168.0.0-16	NETWORK 192.168.0.0/16
Geolocations	4 any-ipv4	NETWORK 0.0.0.0/0
Syslog Servers	5 any-ipv6	NETWORK ::/0
🔏 IKE Policies	6 IPv4-Private-All-RFC1918	Group IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private- 192.168.0.0-16
🐴 IPSec Proposals		
Secure Client Profiles		
St. Identity Sources		
1 Users		
🞗 Certificates		
🔒 Secret Keys		

Imagem 26. Criação de objeto

Etapa 2.2. Adicione um nome para o objeto de rede, selecione o tipo de rede do objeto, adicione o endereço IP, o endereço de rede ou o intervalo de IPs para corresponder ao tráfego que precisa ser negado para o FTD. Em seguida, clique no botão Ok para concluir a rede de objetos.

- Neste exemplo, a rede de objetos configurada destina-se a bloquear ataques de força bruta de VPN provenientes da sub-rede 192.168.1.0/24.

Firewall Device Manager	Monitoring Police			(?) : admin Administrator · ··································
Object Types ←	Network Obje		V ×	
C Networks	6 objects	OBJ-NET-UNWANTED-COUNTRY		+ 6
S Ports				defined, User defined
G Security Zones	N NAME	Description		ACTIONS
F Application Filters	1 IPv4-Private-A		1.	e-172.16.0.0-12, IPv4-Private-
🖉 URLs	2 IPv4-Private-10	Туре		
Geolocations	3 IPv4-Private-1	Network Host FQDN Rang	l6	
Syslog Servers	4 IPv4-Private-19	Network		
	5 any-ipv4	192.168.1.0/24		
IPSec Proposals	6 any-ipv6	e.g. rat.rot.to/ze of zoor.boo.cobac.roo		
Secure Client Profiles			CANCEL OK	
🚉 Identity Sources				
1 Users				
🙊 Certificates				
🔒 Secret Keys				

Imagem 27. Adicionar objeto de rede

Etapa 3. Em seguida, você precisa criar uma ACL estendida; para isso, navegue até a guia Device (Dispositivo) no menu superior.

Firewall Device Manager	Monitoring Policies Objects Device: firepow	ver	cisco SECURE
Object Types ←	Network Objects and Groups		
C Networks	7 objects	F ilter	+ 📖
S Ports		Preset filters: System defined, User defined	
Security Zones	# NAME	TYPE VALUE	ACTIONS
🐬 Application Filters	1 IPv4-Private-All-RFC1918	Group IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private- 192.168.0.0-16	
C URLs	2 IPv4-Private-10.0.0-8	NETWORK 10.0.0/8	
Geolocations	3 IPv4-Private-172.16.0.0-12	NETWORK 172.16.0.0/12	
Syslog Servers	4 IPv4-Private-192.168.0.0-16	NETWORK 192.168.0.0/16	
	5 any-ipv4	NETWORK 0.0.0.0/0	
	6 any-ipv6	NETWORK ::/0	
IPSec Proposals	7 OBJ-NET-UNWANTED-COUNTRY	NETWORK 192.168.1.0/24	
Secure Client Profiles			
Sources			
👤 Users			
Q Certificates			
Secret Keys			

Imagem 28. Página de configurações do dispositivo

Etapa 3.1. Role para baixo e selecione Exibir configuração no quadrado Configuração avançada da seguinte maneira.

Firewall Device Manager Monitoring	Policies Objects Device: firepower	(). (). (). (). (). (). (). (). (). ().	admin Administrator Cisco SECURE
	0/0		
Interfaces Connected Enabled 3 of 3 View All Interfaces	Routing There are no static routes yet View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server / Relay DDNS Service DNS Service
Smart License Evaluation expires in 89 days Tier: Not selected (Threat Defense Virtual - Variable) View Configuration	Backup and Restore View Configuration	Troubleshoot No files created yet REQUEST FILE TO BE CREATED	Management Interface Hostname Time Services See more
Site-to-Site VPN There are no connections yet View Configuration	Remote Access VPN Requires RA VPN license No connections 1 Group Policy Configure	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration	Device Administration Audit Events, Deployment History, Download Configuration View Configuration

Imagem 29. Configuração Avançada do FDM

Etapa 3.2. Em seguida, no painel esquerdo, navegue até Smart CLI > Objects e clique em CREATE SMART CLI OBJECT.

SECURE
+

Imagem 30. Objetos Smart CLI

Etapa 3.3. Adicione um nome para a ACL estendida a ser criada, selecione Lista de acesso estendida no menu suspenso de modelos de CLI e configure as ACEs necessárias usando o objeto de rede criado na etapa 2.2 acima e clique no botão OK para concluir a ACL.

Firewall Devic		A A A Admin thult SECURE	
Advanced Configuration	Name	Description	
Smart CLI	ACL-UNWANTED-COUNTRY CLI Template		
FlexConfig	Extended Access List ~	Show disabled Reset	
FlexConfig Objects	1 access-list ACL-UMANITED-COUNTRY extended 2 configure access-list-entry deny ~ 3 deny network source [003:HET-UMANITED-COUNTRY × ~] destin 4 configure deny port any ~ 5 deny port source NNY destination NNY 6 configure logging default ~	ation [<u>my-lpvix</u> ~]	
	⊙ 7 default log set log-level INFORMATIONAL log-interval	CANCEL OK	

Imagem 31. Criação de ACL estendida

Observação: se precisar adicionar mais ACEs para a ACL, você poderá fazê-lo passando o mouse sobre a esquerda da ACE atual; em seguida, aparecerão três pontos clicáveis. Clique neles e selecione Duplicar para adicionar mais ACEs.

Etapa 4. Em seguida, você precisa criar um objeto FlexConfig, para isso, navegue até o painel esquerdo e selecione FlexConfig > Objetos FlexConfig e clique em CRIAR OBJETO FLEXCONFIG.

Firewall Device N	lanager Monitoring	Policies Object	s Device: firepower	o. 🚔 🗐 ?	admin Administrator	 diale SECURE
Advanced ← Configuration	<mark>Device Sum</mark> r FlexCor	nary nfig Objects				
Smart CLI				Filter		+
Objects	1. Sec. 1	NAME	DESCRIPTION		ACTIONS	
FlexConfig Objects FlexConfig Policy			There as Start by cre	e no FlexConfig objects yet. ating the first FlexConfig object.		

Imagem 32. Objetos FlexConfig

Etapa 4.1. Adicione um nome para o objeto FlexConfig para criar e configurar a ACL do plano de controle como entrada para a interface externa da seguinte maneira.

```
Sintaxe da linha de comando:
```

```
access-group "ACL-name" in interface "interface-name" control-plane
```

Isso se traduz no próximo exemplo de comando, que usa a ACL estendida criada na Etapa 3.3 "ACL-UNWANTED-COUNTRY" acima, da seguinte maneira:

```
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

É assim que ele deve ser configurado na janela do objeto FlexConfig. Depois disso, selecione o botão OK para concluir o objeto FlexConfig.

Firewall Device Manage	er Monitoring	Ø #=			<u></u>	admin Administrator V cisco SECURE
	montoning	Create FlexConfig Obje	ect			Planninguator
Advanced ←	FlexCo	Name				
Configuration		OBJ-FC-CONTROL-PLANE				
Smart CLI	_					
Objects	1 - C	Description				CTIONS
					lin	
FlexConfig		Variables				
FlexConfig Objects		Start with adding a new variable.				
FlexConfig Policy		+ ADD VARIABLE				
		Template		Expand	🗘 Reset	
		1 access-group ACL-UNHANT	TED-COUNTRY in interface outsid	e control-plane		
		Negate Template 🛆		C Expand	🗘 Reset	
		1 no access-group ACL-UNM	WANTED-COUNTRY in interface out	side control-plane		
			[CANCEL	ок	

Imagem 3. Criação de Objeto FlexConfig

Etapa 5. Prossiga para criar uma Política FlexConfig, para isso, navegue até Flexconfig > Política FlexConfig, clique no botão '+' e selecione o objeto FlexConfig que foi criado na etapa 4.1 acima.



Imagem 34. Política FlexConfig

Etapa 5.1. Verifique se a visualização FlexConfig mostra a configuração correta da ACL do plano de controle criada e clique no botão Save (Salvar).

Firewall Device Manager	Monitoring Policies Objects Device: firepower	() () () () () () () () () () () () () (
Advanced ← Configuration	Device Summary FlexConfig Policy	
Smart CLI	Group List	Preview
Objects	→ OBJ-FC-CONTROL-PLANE	<pre>1 access-group ACL-UNWAVITED-COUNTRY in interface outside control-plane</pre>
FlexConfig		· · · · · · · · · · · · · · · · · · ·
FlexConfig Objects		
FlexConfig Policy		
	SAVE	

Imagem 35. Visualização da Política FlexConfig

Etapa 6. Implante as alterações de configuração no FTD que você deseja proteger contra os ataques de força bruta da VPN. Para isso, clique no botão Implantação no menu superior, confirme se as alterações de configuração a serem implantadas estão corretas e clique em IMPLANTAR AGORA.

Firewall Device Manager	er 🗰 🞯 🌐 🧰 💼 🔿 🖓 🖓 🖓 admin v diudh s	SECURE
Advanced ← Configuration	Pending Changes Image: Change Chang	
Smart CLI	Deployed Version (05 Sep 2023 02:27 PM) Pending Version O LEGEND	
Objects	Network Object Added: OBJ-NET-UNWANTED-COUNTRY	Evened
FlexConfig	- subType: Network - value: 2.2.2.0/24 - is\$ystemDefined: false - dnsResolution: IPV4_AND_IPV6 in interface outside	EXpand
FlexConfig Objects	- description: - name: 087-NET-UNWANTED-COUNTRY	
FlexConfig Policy	FlexConfig Policy Edited: default-aroup	
	flexConfigObjects: - 083-FC-CONTROL-PLANE	
	Extended Access List Added: ACL-UNWANTED-COUNTRY	
	- entries[0].logging: DEFAULT - entries[0].action: DENY - name: ACL-UNEANTED-COUNTRY entries[0].sourceNetworks: OPI NET IMANTED CONTRY	
	MORE ACTIONS V CANCEL V	

Imagem 36. Implantação Pendente

Etapa 6.1. Valide se a implantação da política foi bem-sucedid
--

Firewall Device Ma	nager Pending Changes OX	n vitige SECURE
Advanced ← Configuration Smart CLI	÷	
Objects	There are no Pending Changes yet. Nothing to deploy.	<> Expand
FlexConfig		in interface outside
FlexConfig Objects	You can see what was deployed in previous jobs in the Deployment History	
FlexConfig Policy		
	ок	
	SAVE	

Imagem 37. Implantação bem-sucedida

Passo 7. Se você criar uma nova ACL de plano de controle para o FTD ou se editou uma ACL existente que esteja ativamente em uso, é importante destacar que as alterações de configuração feitas não se aplicam a conexões já estabelecidas com o FTD, portanto, você precisa limpar manualmente as tentativas de conexão ativas ao FTD. Para isso, conecte-se ao CLI do FTD e limpe as conexões ativas da seguinte maneira.

Para limpar a conexão ativa para um endereço IP de host específico:

> clear conn address 192.168.1.10 all

Para limpar as conexões ativas de toda uma rede de sub-rede:

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

Para limpar as conexões ativas para um intervalo de endereços IP:

> clear conn address 192.168.1.1-192.168.1.10 all

Observação: é altamente recomendável usar a palavra-chave 'all' no final do comando clear conn address para forçar a limpeza das tentativas de conexão de força bruta de VPN ativas para o firewall seguro, principalmente quando a natureza do ataque de força bruta de VPN está iniciando uma explosão de tentativas de conexão constantes.

Configurar uma ACL de plano de controle para ASA usando CLI

Este é o procedimento que você precisa seguir em uma CLI do ASA para configurar uma ACL de plano de controle para bloquear ataques de força bruta de VPN recebidos para a interface externa:

Etapa 1. Faça login no firewall seguro ASA via CLI e obtenha acesso ao "configure terminal" da seguinte maneira.

asa# configure terminal

Etapa 2. Use o próximo comando para configurar uma ACL estendida para bloquear um endereço IP de host ou um endereço de rede para o tráfego que precisa ser bloqueado para o ASA.

 Neste exemplo, você cria uma nova ACL chamada 'ACL-UNWANTED-COUNTRY' e a entrada ACE configurada bloqueará ataques de força bruta de VPN provenientes da sub-rede 192.168.1.0/24.

asa(config)# access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any

Etapa 3. Use o próximo comando access-group para configurar a ACL 'ACL-UNWANTED-COUNTRY' como uma ACL de plano de controle para a interface ASA externa.

```
asa(config)# access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Etapa 4. Se você criar uma nova ACL de plano de controle ou se editou uma ACL existente que esteja ativamente em uso, é importante destacar que as alterações de configuração feitas não se aplicam a conexões já estabelecidas com o ASA, portanto, você precisa limpar manualmente as tentativas de conexão ativas com o ASA. Para isso, limpe as conexões ativas da seguinte maneira.

Para limpar a conexão ativa para um endereço IP de host específico:

```
asa# clear conn address 192.168.1.10 all
```

Para limpar as conexões ativas de toda uma rede de sub-rede:

asa# clear conn address 192.168.1.0 netmask 255.255.255.0 all

Para limpar as conexões ativas para um intervalo de endereços IP:

asa# clear conn address 192.168.1.1-192.168.1.10 all

Observação: é altamente recomendável usar a palavra-chave 'all' no final do comando clear conn address para forçar a limpeza das tentativas de conexão de força bruta de VPN ativas para o firewall seguro, principalmente quando a natureza do ataque de força bruta de VPN está iniciando uma explosão de tentativas de conexão constantes.

Configuração alternativa para bloquear ataques para um firewall seguro usando o comando 'shun'

No caso de uma opção imediata para bloquear ataques para o firewall seguro, você pode usar o comando 'shun'. O comando hunter permite bloquear conexões de um host de ataque.

- Depois de evitar um endereço IP, todas as conexões futuras do endereço IP de origem serão canceladas e registradas até que a função de bloqueio seja removida manualmente.

- A função de bloqueio do comando de bloqueio é aplicada independentemente de uma conexão com o endereço de host especificado estar ou não ativa no momento.

- Se você especificar o endereço de destino, as portas de origem e de destino e o protocolo, então você desconectará a conexão correspondente, bem como colocará um shun em todas as conexões futuras do IP de origem

todas as conexões futuras são evitadas, não apenas aquelas que correspondem a esses parâmetros de conexão específicos.

- Você pode ter apenas um comando uneshuncommand por endereço IP de origem.

- Como o comando hunter é usado para bloquear ataques dinamicamente, ele não é exibido na configuração do dispositivo de defesa contra ameaças.

- Sempre que uma configuração de interface é removida, todos os shuns conectados a essa interface também são removidos.

- Sintaxe do comando Shun:

```
shun source_ip [ dest_ip source_port dest_port [ protocol]] [ vlan vlan_id]
```

- Para desativar um shun, use a forma no desse comando:

no shun source_ip [vlan vlan_id]

Para evitar um endereço IP de host, siga as etapas abaixo para obter o firewall seguro. Neste exemplo, o comando 'shun' é usado para bloquear ataques de força bruta de VPN provenientes do endereço IP de origem 192.168.1.10.

Exemplo de configuração para FTD.

Etapa 1. Faça login no FTD via CLI e aplique o comando shun da seguinte maneira.

<#root>

>

shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf

Shun 192.168.1.10 successful

Etapa 2. Você pode usar os seguintes comandos show para confirmar os endereços IP shun no FTD e para monitorar as contagens de ocorrências shun por endereço IP:

<#root> > show shun shun (outside) 192.168.1.10 0.0.0 0 0 0 > show shun statistics diagnostic=0FF, cnt=0 outside=ON, cnt=0 Shun 192.168.1.10 cnt=0, time=(0:00:28)

Exemplo de configuração para ASA

Etapa 1. Faça login no ASA via CLI e aplique o comando shun da seguinte maneira.

<#root>
asa#
shun 192.168.1.10
Shun 192.168.1.10 added in context: single_vf

Shun 192.168.1.10 successful

Etapa 2. Você pode usar os seguintes comandos show para confirmar os endereços IP shun no ASA e para monitorar as contagens de ocorrências shun por endereço IP:

<#root>

asa#

show shun

shun (outside) 192.168.1.10 0.0.0.0 0 0 0
asa#
show shun statistics
outside=ON, cnt=0
inside=OFF, cnt=0
dmz=OFF, cnt=0
outside1=OFF, cnt=0
mgmt=OFF, cnt=0
Shun 192.168.1.10 cnt=0, time=(0:01:39)

Observação: para obter mais informações sobre o comando secure firewall shun, consulte a <u>Referência de Comandos do Cisco Secure Firewall Threat Defense</u>

Verificar

Para confirmar se a configuração da ACL do plano de controle está estabelecida para o firewall seguro, siga este procedimento:

Etapa 1. Faça login no firewall seguro via CLI e execute os próximos comandos para confirmar se a configuração da ACL do plano de controle foi aplicada.

Exemplo de saída para o DTF gerido pelo CVP:

<#root>
>
show running-config access-list ACL-UNWANTED-COUNTRY
access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any

>

show running-config access-group

OUTPUT OMITTED FOR BREVITY access-group ACL-UNWANTED-COUNTRY in interface outside control-plane

Exemplo de saída para o FTD gerenciado pelo FDM:

<#root>

> show running-config object id OBJ-NET-UNWANTED-COUNTRY

object network OBJ-NET-UNWANTED-COUNTRY subnet 192.168.1.0 255.255.255.0

>

show running-config access-list ACL-UNWANTED-COUNTRY

```
access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any4 log default
```

> show running-config access-group

```
***OUTPUT OMITTED FOR BREVITY***
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

Exemplo de saída do ASA:

<#root>

asa#

show running-config access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any

asa#

show running-config access-group

OUTPUT OMITTED FOR BREVITY access-group ACL-UNWANTED-COUNTRY in interface outside control-plane

Etapa 2. Para confirmar se a ACL do plano de controle está bloqueando o tráfego necessário, use o comando packet-tracer para simular uma conexão TCP 443 de entrada para a interface externa do firewall seguro e, em seguida, use o comando show access-list <acl-name> , a contagem de ocorrências da ACL deve ser incrementada toda vez que uma conexão de força bruta de VPN para o firewall seguro for bloqueada pela ACL do plano de controle:

 Neste exemplo, o comando packet-tracer simula uma conexão TCP 443 de entrada originada do host 192.168.1.10 e destinada ao endereço IP externo de nosso firewall seguro. A saída do "packet-tracer" confirma que o tráfego está sendo descartado e a saída do "show access-list" exibe os incrementos da contagem de ocorrências para nossa ACL de plano de controle:

Exemplo de saída para FTD

<#root>

packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.251 443 Phase: 1 Type: ACCESS-LIST Subtype: log Result: DROP Elapsed time: 21700 ns Config: Additional Information: Result: input-interface: outside(vrfid:0) input-status: up input-line-status: up Action: drop Time Taken: 21700 ns Drop-reason: (acl-drop) Flow is denied by configured rule , Drop-location: frame 0x00005623c7f324e7 flow (NA)/NA > show access-list ACL-UNWANTED-COUNTRY

```
access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f
access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any (
```

hitcnt=1

) 0x142f69bf

Exemplo de saída do ASA

<#root>

asa#

packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.5 443

Phase: 1 Type: ACCESS-LIST Subtype: Result: ALLOW Elapsed time: 19688 ns Config: Implicit Rule Additional Information: MAC Access list

Phase: 2 Type:

```
ACCESS-LIST
Subtype: log
Result: DROP
Elapsed time: 17833 ns
Config:
Additional Information:
Result:
input-interface: outside
input-status: up
input-line-status: up
Action: drop
Time Taken: 37521 ns
Drop-reason: (acl-drop) Flow is denied by configured rule
, Drop-location: frame 0x0000556e6808cac8 flow (NA)/NA
asa#
show access-list ACL-UNWANTED-COUNTRY
access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f
access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any
(hitcnt=1)
```





Norma Servação: se uma solução RAVPN como o Cisco Secure Client VPN for implementada no firewall seguro, uma tentativa real de conexão com o firewall seguro poderá ser realizada para confirmar se a ACL do plano de controle está funcionando conforme esperado para bloquear o tráfego necessário.

Bugs relacionados

 ENH | Conexões do AnyConnect Client baseadas em localização geográfica: ID de bug da Cisco CSCvs65322

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.