Configurazione dei criteri di controllo di accesso del Control Plane per la difesa dalle minacce del firewall protetto e l'appliance ASA

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Configurazione
Configurazioni
Configurazione di un ACL del control plane per FTD gestito da FMC
Configurare un ACL del control plane per FTD gestito da FDM
Configurazione di un ACL del control plane per un'ASA tramite CLI
Configurazione alternativa per bloccare gli attacchi per un firewall protetto tramite il comando <u>'shun'</u>
<u>Verifica</u>
Bug correlati

Introduzione

In questo documento viene descritto il processo di configurazione delle regole di accesso al control plane per Secure Firewall Threat Defense e Adaptive Security Appliance (ASA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Secure Firewall Threat Defense (FTD)
- Secure Firewall Device Manager (FDM)
- Centro gestione firewall protetto (FMC)
- Secure Firewall ASA
- Access Control List (ACL)
- FlexConfiguration

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il traffico in genere attraversa un firewall e viene instradato tra le interfacce dati; in alcune circostanze, è utile impedire il traffico destinato al firewall sicuro. Il firewall sicuro Cisco può utilizzare un ACL (Control-Plane Access Control List) per limitare il traffico "diretto". Un esempio di quando un ACL control-plane può essere utile è controllare quali peer possono stabilire un tunnel VPN (da sito a sito o VPN ad accesso remoto) per il firewall sicuro.

Protezione del traffico "through-the-box" del firewall

Il traffico in genere attraversa i firewall da un'interfaccia (in entrata) a un'altra interfaccia (in uscita). Questo tipo di traffico è noto come traffico "through-the-box" ed è gestito da entrambe le regole, ACP (Access Control Policies) e Pre-filter.



Immagine 1. Esempio di traffico integrato

Protezione del traffico "diretto" del firewall

In altri casi, il traffico è destinato direttamente a un'interfaccia FTD (da sito a sito o VPN ad accesso remoto), ovvero al traffico "diretto", ed è gestito dal control plane dell'interfaccia specifica.



Immagine 2. Esempio di traffico diretto

Considerazioni importanti sugli ACL dei Control Plane

- A partire dalla versione 7.0 di FMC/FTD, un ACL del control plane deve essere configurato utilizzando FlexConfig, utilizzando la stessa sintassi del comando utilizzata sull'appliance ASA.
- La parola chiave control-plane viene aggiunta alla configurazione del gruppo di accesso, che attiverà il traffico 'verso' l'interfaccia protetta del firewall. Senza la parola control-plane aggiunta al comando, l'ACL limiterebbe il traffico 'attraverso' il firewall protetto.
- Un ACL control-plane non limita il protocollo SSH, ICMP o TELNET in entrata a un'interfaccia firewall sicura. Questi vengono elaborati (consentiti/negati) in base ai criteri di impostazioni della piattaforma e hanno una precedenza più alta.
- Un ACL control-plane restringe il traffico 'verso' il firewall sicuro stesso, mentre i criteri di controllo dell'accesso per l'FTD o gli ACL normali per l'ASA controllano il traffico 'attraverso' il firewall sicuro.
- A differenza di un ACL normale, alla fine dell'ACL non è presente un 'rifiuto' implicito.
- Al momento della creazione del documento, la funzione di georilevazione FTD non può essere utilizzata per limitare l'accesso 'a' FTD.

Configurazione

Nell'esempio successivo, un gruppo di indirizzi IP di un determinato paese cerca di forzare la VPN nella rete tentando di accedere all'FTD RAVPN. L'opzione migliore per proteggere l'FTD da questi attacchi VPN con forza bruta è configurare un ACL del control plane in modo da bloccare queste connessioni all'interfaccia FTD esterna.

Configurazioni

Configurazione di un ACL del control plane per FTD gestito da FMC

Questa è la procedura da seguire in un FMC per configurare un ACL del control plane in modo da bloccare gli attacchi VPN con forza bruta in arrivo sull'interfaccia FTD esterna:

Passaggio 1. Aprire l'interfaccia grafica utente (GUI) di FMC tramite HTTPS ed eseguire l'accesso con le credenziali dell'utente.



Immagine 3. Pagina Log In di FMC

Passaggio 2. È necessario creare un ACL esteso. A tale scopo, selezionare Oggetti > Gestione oggetti.

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy Q 🤩 🌣 🕜	admin - cisco SECURE
Summary Dashboard (switch dashboard) Provides a summary of activity on the applance					Object N Intrusion	lanagement Rules			Reporting
Network × Threats Intrusion Events	Status	Geolocation	QoS					Show the Last 1 hour	• 11
Unique Applications over Time		-× •	Top Web Appl	lications Seen				Top Client Applications Seen	
No Data				,	No Data			No Data	
Traffic by Application Risk		- ×	Top Server Ap	plications See	n		- ×	► Top Operating Systems Seen	- ×

Immagine 4. Gestione oggetti

Passaggio 2.1. Dal pannello di sinistra, selezionare Access List > Extended (Elenco accessi > Esteso) per creare un ACL esteso.

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	C 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

Immagine 5. Menu ACL esteso

Passaggio 2.2. Quindi, selezionare Aggiungi elenco accessi esteso.

Firewall Managemen Objects / Object Management	t Center o	verview Analys	s Policies	Devices	Objects	Integration	Deploy	Q 🧬	🔅 🕜 admir	n▼
> AAA Server	Extended						Add Extended Acce	ss List	Filter	
✓ Access List	•					which a sector will sector for				
Extended	traffic based on so	ect, also known as an surce and destination	address and por	ts. Supports IP	v4 and IPv6 ad	dresses. You use these obje	cts when configuring part	cular feature	s, such as route	maps.
Standard										
> Address Pools	Name						Value		Over	rride
Application Filters										
AS Path						o records to display				
Cipher Suite List										
> Community List										
> Distinguished Name										
DNS Server Group										
> External Attributes										
File List										
> FlexConfig										
Geolocation										
Interface										
Key Chain										
Network										
> ркі										
Policy List										
Port							N	lo data to disp	lay I< < Page	1 of 1 > > C
> Prefix List										

Immagine 6. Aggiungi ACL esteso

Passaggio 2.3. Digitare un nome per l'ACL esteso e quindi fare clic sul pulsante Aggiungi per creare una voce di controllo di accesso (ACE):

AAA Server Access List Object	Firewall Man Objects / Object N	agement Cer Management	nter	Overview	Analysis	Policies	Device	s Objects	Integ	ration		Deploy	٩	e 🕈	🕜 admin 🔻	cisco SECURE	
Access List Extended Name Standard ACL-UNWANTED-COUNTRY Address Pools ACL-UNWANTED-COUNTRY Address Pools ACL-UNWANTED-COUNTRY Address Pools Action Source Application Filters AS Path Cipher Suite List Sequence Action Source Source Port Destination Port Application No records to display No records to display No records to display Pietural Attributes File List Pietural Attributes File List Pietural Attributes	> AAA Server	New Exter	nded Acc	ess List Ob	ject												
Standard ACL-UNWANTED-COUNTRY A Address Pools Application Filters AS Path Cipher Suite List Sequence Action Source Port Source Port Destination Port Add Source Port Add No records to display No records to display Piet List Piet List	 Access List Extended 	Name													dress on oute ma	y. Identifies os.	
Application Filters Application Filters As Path Cipher Suite List Source Management Action Source Port Destination Port Application No records to display Vorecords File List Peternal Attributes File List Geolocation Interface	Standard Address Pools	ACL-UNWA	ANTED-CO	UNTRY											Override		
Sequence Action Source Port Destination Destination Port Application > Community List No records to display No records to display Image: Community List Image: Community List	Application Filters	Entries (0)												Add			
> Community List No records to display > Distinguished Name DNS Server Group > External Attributes File List > FlexConfig Allow Overrides Interface Allow Overrides	Cipher Suite List	Sequence	Action	Source		Source Port		Destination		Destination Port	Applicatio	'n					
DNS Server Group > External Attributes File List > FlexConfig Geolocation Interface	Distinguished Name																
File List > FlexConfig Geolocation Interface	DNS Server Group > External Attributes																
Geolocation Allow Overrides	File List																
	Geolocation	Allow Ove	errides														
Key Chain	Key Chain													Save			
	> ркі																
Policy List Port No data to display I of 1	Policy List Port											No	o data to	o display	< Page 1	of 1 $>$ > C	

Immagine 7. Voci ACL estese

Passaggio 2.4. Modificare l'azione ACE in Blocca, quindi aggiungere la rete di origine in modo che corrisponda al traffico che deve essere rifiutato all'FTD, mantenere la rete di destinazione come Qualsiasi e fare clic sul pulsante Aggiungi per completare la voce ACE:

- Nell'esempio, la voce ACE configurata bloccherà gli attacchi di forza bruta VPN provenienti dalla subnet 192.168.1.0/24.

Firewa Objects /	Action: Block			cisco SECURE
> AAA Server	Logging: Default			
Extended	Log Level:			Identifies ;.
> Address Pools	Log Interval:			
Application Filt AS Path	300 Sec. Network Port () Application			18
Cipher Suite Li	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 Gre	any Add to Source any any-ipv4 Add to Destination			
File List	any-ipv6			
Geolocation	IPv4-Benchmark-Tests IPv4-Link-Local			
Interface Key Chain	IPv4-Multicast			
Network	IPv4-Private-172.16.0.0-12	Enter an IP address Add	Enter an IP address Add	
> PKI Policy List				
Port			Cancel	of1>>\C

Immagine 8. Reti negate

Passaggio 2.5. Se è necessario aggiungere altre voci ACE, fare di nuovo clic sul pulsante Aggiungi e ripetere il passaggio 2.4. Quindi, fare clic sul pulsante Save (Salva) per completare la configurazione dell'ACL.

Firewall Managemen Objects / Object Management	Edit Exten	nded Acc	ess List Object					0	cisco SECURE
> AAA Server ~ Access List	Name ACL-UNW	ANTED-CC	DUNTRY						
Extended	Entries (1)								Identifies
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	× • 00
Cipher Suite List									
> Community List									
> Distinguished Name									
DNS Server Group									
> External Attributes									
File List	Allow Ov	verrides							
> FlexConfig									
Geolocation								Save	
Interface									
Key Chain									
Network									
> ркі									
Policy List									
Port							Displaying 1 - 1 of 1 rows	IC < Page 1	of1>>IC
> Prefix Liet									

Immagine 9. Voci ACL estese completate

Passaggio 3. Quindi, è necessario configurare un oggetto Flex-Config per applicare l'ACL del piano di controllo all'interfaccia FTD esterna. A tale scopo, spostarsi nel pannello sinistro e selezionare l'opzione FlexConfig > Oggetto FlexConfig.

Ð	Firewall Management Objects / Object Management	Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy Q	¢ 🗘	🕜 admin 🕶 🏻	cisco SECURE
> AAA	Server	Extended	d						Add Extende	ed Access Lis	it Q Filte	r	
✓ Acc	ess List					. (
	Extended	An access list of traffic based or	object, also kno n source and d	own as an acce estination addr	ess control list ess and ports	t (ACL), select s. Supports IPv	ts the traffic to 4 and IPv6 ad	which a service will apply.	Standard-Identifies ects when configuri	ng particular	on destination features, suc	h as route maps	. Identifies s.
	Standard												
> Add	ress Pools	Name							Value			Override	
Арр	lication Filters	ACL-UNWANT	ED-COUNTRY										1 1 8
AS F	Path												
Ciph	ner Suite List												
> Com	nmunity List												
> Disti	inguished Name												
DNS	Server Group												
> Exte	rnal Attributes												
File	List												
~ Flex	Config												
	FlexConfig Object												
	Text Object												
Geo	location												
Inter	face												
Key	Chain												
Netv	work												
> ркі									C	Displaying 1 - 1	lof1 rows 🕸	C < Page 1	of 1 > > C
Polic	nv Liet												

Immagine 10. Menu Oggetto FlexConfig

Passaggio 3.1. Fare clic su Aggiungi oggetto FlexConfig.

Firewall Manageme	t Center _{Overview} Analysis Polici	ies Devices Objects Integration	Deploy Q 🗳 🌣 🍞 admin 🕶 🖓	🖑 SECURE
 AAA Server Access List Extended Standard 	FlexConfig Object FlexConfig Object include device configuration com	mands, variables, and scripting language instructions. I	Add FlexConfig Object Q. Filter	
> Address Pools	Name		Description	
Application Filters AS Path	Default_DNS_Configure		Configure Default DNS with the help of TextObj	¶∎ q 🗎
Cipher Suite List	Default_Inspection_Protocol_Disable		Disable Default Inspection.	α []
> Community List	Default_Inspection_Protocol_Enable		Enable Default Inspection.	β α
> Distinguished Name	DHCPv6_Prefix_Delegation_Configure		Configure one outside (PD client) and one insid	α ()
DNS Server Group	DHCPv6 Prefix Delegation LInConfigure		Remove configuration of one outside (PD client	R a
 External Attributes File List 				
✓ FlexConfig	DNS_Configure		Configure DNS with the help of TextObjects dn	a d
FlexConfig Object	DNS_UnConfigure		Remove the DNS configurations.	α []
Text Object	Eigrp_Configure		Configures eigrp. 1. Configures next hop. 2. co	α ()
Geolocation	Eigrp_Interface_Configure		Configures interface parameters for eigrp. 1. C	¶∎ Q 🗎
Interface	Fiaro UnConfigure		Clears eigro configuration for an AS	¶a a ∋
Key Chain				
> PKI	Eigrp_Unconfigure_All		Clears eigrp configuration. Displaying 1 - 20 of 48 rows K < Page 1 o	af3>>IC

Immagine 11. Aggiungi oggetto Flexconfig

Passaggio 3.2. Aggiungere un nome per l'oggetto FlexConfig, quindi inserire un oggetto criterio ACL. A tale scopo, selezionare Inserisci > Inserisci oggetto criterio > Oggetto ACL esteso.

Firewall Managemer	Name: OBJ-FC-CONTROL-PLANE							🎗 🕜 admin 🕶	
> AAA Server	Description:							Filter	
Extended Standard	Copy-pasting any rich to	ext might introduce line break	s while generating CLI.	Please verify the	CLI before deploy	ment.			
> Address Pools		Deployment: Once		Type:	Append		• I		
Application Filters AS Path	Insert Policy Object	Text Object Network						the help of TextObj	¶_ Q
Cipher Suite List	Insert Secret Key	Security Zones							¶∎ Q 🗎
> Community List		Standard ACL Object							R Q
> Distinguished Name		Extended ACL Object						fight) and one insid	En o E
DNS Server Group		Route Map						alenty and one insid	
> External Attributes								e outside (PD client	唱 < 🗍
File List								of TextObjects dn	Pa 0, 🗎
✓ FlexConfig	▼ Variables							0.00	E o ⊇
FlexConfig Object	Name	Dimension	Default Value	Property (Type:Name)	Override	Description			
Text Object			No records to di	enlav				ires next hop. 2. co	Ч (
Geolocation								sters for eigrp. 1. C	팀 Q 🔒
Interface								ar an AS	Fa Q
Key Chain									
Network									
> PKI							Save	s IC C Page 1	

Immagine 12. Variabile oggetto FlexConfig

Passaggio 3.3. Aggiungere un nome per la variabile oggetto ACL e quindi selezionare l'ACL esteso creato nel passaggio 2.3. Quindi, fare clic sul pulsante Save (Salva).

Firewall Managemen	Name: OBJ-FC-CONTROL-PLANE	:			⊁ 🛛 admin ▼ 🖓	SECURE
> AAA Server ~ Access List	Description:	Insert Extended Access List Object Var	iable Ø		Filter	
Extended Standard > Address Pools Application Filters AS Path Cipher Suite List > Community List > Distinguished Name DMS Examt Group	Copy-pasting any rich	Variable Name: VAR-ACL-UNWANTED-COUNTRY Description: Available Objects C Q Search	Selected Object		the help of TextObj	F a ⊂ 11 F a ⊂ 11
External Attributes File List FlexConfig	▼ Variables	Add			outside (PD client	₽a Q ₽a Q ₽a Q ₽a Q
FlexConfig Object Text Object Geolocation Interface Key Chain	Name		Cancel	ription	res next hop. 2. co sters for eigrp. 1. C	
Network > PKI Policy List				Cancel Save	s I< < Page 1	na 3 > > C

Immagine 13. Assegnazione ACL variabile oggetto FlexConfig

Passaggio 3.4. Quindi, configurare l'ACL del piano di controllo come in entrata per l'interfaccia esterna nel modo seguente.

Sintassi della riga di comando:

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

In questo esempio viene illustrato il comando successivo, che utilizza la variabile ACL creata nel passaggio 2.3 'VAR-ACL-UNWANTED-COUNTRY' come segue:

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

Per completare l'oggetto FlexConfig, selezionare il pulsante Save (Salva) nella finestra oggetto 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		

Immagine 14. Riga di comando per il completamento dell'oggetto Flexconfig

Passaggio 4. È necessario applicare la configurazione dell'oggetto FlexConfig all'FTD. A tale scopo, selezionare Dispositivi > FlexConfig.

Cipects / Object Management	Center Overview Analysis Policies	Devices Objects	Integration	Deploy Q 🤩	🔅 🥝 admin 🕶 🏻 🖞	secure
AAA Server Access List Extended Standard Address Pools Application Filters	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 he help of TextObj	Fa Q
AS Path Cipher Suite List > Community List	Default_Insp Default_Insp	ection_Protocol_Disable		Disable Default Inspection.		⊑α ⊑α
> Distinguished Name DNS Server Group	DHCPv6_Pref	fix_Delegation_Configure		Configure one outside (PD o	client) and one insid	Fa Q
External Attributes File List ElsyConfig	DHCPv6_Prefv	<_Delegation_UnConfigure		Remove configuration of on Configure DNS with the help	e outside (PD client	α Πα (
FlexConfig Object	DN	S_UnConfigure		Remove the DNS configurat	ions.	₽a () ₽a () ₽a ()
Geolocation	Eigrp_N	nterface_Configure		Configures interface parame	aters for eigrp. 1. C	₽ Q]
Key Chain Network	Eigr	p_UnConfigure _Unconfigure_All		Clears eigrp configuration fo	or an AS	₽∎ α `` ₽∎ α ``
> ркі				Displaying 1 - 20 of 49 row	s I< < Page 1	of 3 > > C

Immagine 15. Menu criteri di FlexConfig

Passaggio 4.1. Quindi, fare clic su Nuovo criterio se non è già stato creato un FlexConfig per il FTD o modificare il criterio FlexConfig esistente.

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

Immagine 16. Creazione criteri FlexConfig

Passaggio 4.2. Aggiungere un nome per il nuovo criterio FlexConfig e selezionare l'FTD a cui si desidera applicare l'ACL del control plane creato.

Firewall Management Center	Overview Analysis Policies Devi	ices Objects Integration	Deploy Q 🤩 🏞 🕜 admin 🔻 记
FlexConfig Policy	New Policy		0
	Name: FLEXCONFIG-POLICY Description: Targeted Devices Select devices to which you want to app Available Devices Q. Search by name or value FTD-CONTROL-PLANE	aly this policy. Selected Devices FTD-CONTROL-PLANE	
		Cancel	

Immagine 17. Assegnazione dispositivo criteri FlexConfig

Passaggio 4.3. Dal pannello sinistro, cercare l'oggetto FlexConfig creato nel passaggio precedente 3.2, quindi aggiungerlo al criterio FlexConfig facendo clic sulla freccia destra al centro della finestra, quindi fare clic sul pulsante Salva.

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q 🔮 🏠 🕢 admin 🕶 🖓	
FLEXCONFIG-POLICY							You have unsaved changes Preview Config Save Car	ncel
							Policy Assignment	ts (1)
	" Solooto	d Dropond F	lovConfigs					
Available FlexConfig	Selecte	a Prepena P	lexconligs					
X	# Nan	ne			Description			
V User Defined								
CBJ-FC-CONTROL-PLANE								
V System Defined								
Default_DNS_Configure								
Default_Inspection_Protocol_Disable								
Contemporary Conte		d Append Fl	lexConfigs					
Therefix_Delegation_Configure								
DHCPv6_Prefix_Delegation_UnConfigure	# Nan	ne			Description			
DNS_Configure	1 ОВЈ	-FC-CONTROL	-PLANE					۹ 🖬
DNS_UnConfigure	Ч——							
"B Eigrp_Configure								
* Eigrp_Interface_Configure								

Immagine 18. Assegnazione oggetto criteri FlexConfig

Passaggio 5. Continuare a distribuire la modifica della configurazione nell'FTD. Per questo, passare a Distribuisci > Distribuzione avanzata.

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q	\$	🕑 admin •	cisco SE	CURE
FLEXCONFIG-POLICY								Advanced	Deploy D	eploy All	ncel
Enter Description						FTD-CONTROL-PLANE		Ready for D	eployment	é	
Ausiable ElevConfig	" Select	ed Prepend F	FlexConfigs								
Available recording of Plexconing Object	# Nai	me			Description						
V Heer Defined											
Obj-FC-CONTROL-PLANE											
✓ System Defined											
"? Default_DNS_Configure											
Default_Inspection_Protocol_Disable						1 device is available for deployment				12 •9	
" Default_Inspection_Protocol_Enable		ed Append F	lexConfigs								
DHCPv6_Prefix_Delegation_Configure	# Na	me			Description						
DHCPv6_Prefix_Delegation_UnConfigure	1 00										<u> </u>
DNS_Configure	T OB.	J-FC-CONTROL	L-PLANE								~
DNS_UnConfigure											
"i Eigrp_Configure											
Eigrp_Interface_Configure											
? Eigrp_UnConfigure											
" ^{II} Eigrp_Unconfigure_All											
.9 Eigrp_Unconfigure_All											

Immagine 19. Distribuzione avanzata FTD

Passaggio 5.1. Quindi, selezionare l'FTD a cui si desidera applicare il criterio FlexConfig. Se tutto è corretto, fare clic su Distribuisci.

þ	Fi	rewall Management Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ 🇳	🌣 🕜 admin -	cisco SECURE
1 devic	e sek Q	ected Search using device name, user name, type,	, group or statu	15								Deploy time: Esti	nate Deploy
_		Device	Modified by		Inspect Inte	erruption	Туре	Group	Last Deploy Time		Preview	Status	
~		FTD-CONTROL-PLANE	admin				FTD		Sep 5, 2023 12:0	5 PM	B	Ready for Deploy	ment
:: •		Flex Configuration Template Policy: FLEXCONFIG-POLICY											
https://10	88 243	8.5843013/dd/#Context5mioner											

Immagine 20. Convalida distribuzione FTD

Passaggio 5.2. Al termine, verrà visualizzata una finestra di conferma della distribuzione, verrà aggiunto un commento per tenere traccia della distribuzione e si procederà alla distribuzione.

	Firewall Management Center Deploy / Deployment								🔅 🕜 admin 🕶 🛉	
1 devic	a selected Q Search using device name, user name, typ									
		Modified by								
~	FTD-CONTROL-PLANE	admin					Sep	5, 2023 12:05 PM	Ready for Deploymen	
÷.	 Flex Configuration Template Policy: FLEXCONFIG-POLICY 		Deployment Cont	irmation			×			
			You have selected 1 d	evice to deplo	y					
			Deployment Notes:							
			You can optionally ac	ld notes about	the configura	ation changes				
							Deploy			

Immagine 21. Commenti distribuzione FTD

Passaggio 5.3. Durante la distribuzione delle modifiche di FlexConfig potrebbe essere visualizzato un messaggio di avviso. Fare clic su Distribuisci solo se si è completamente certi che la configurazione dei criteri sia corretta.



Immagine 22. Avviso Flexconfig di distribuzione FTD

Passaggio 5.4. Confermare che la distribuzione dei criteri per l'FTD è riuscita.

Ð	Fi De	rewall Management Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	, q 🤞	🗘 🕜 adm	in ▼
T	۹	Search using device name, user name, type,	, group or statu	15									Deploy
		Device	Modified by		Inspect Inte	rruption	Туре	Group	Last Deploy Time		Preview	Status	
~		FTD-CONTROL-PLANE	admin				FTD		Sep 5, 2023 12:	05 PM		Completed	
*= •		 Flex Configuration Template Policy: FLEXCONFIG-POLICY 											

Immagine 23. Distribuzione FTD completata

Passaggio 6. Se si crea un nuovo ACL del piano di controllo per l'FTD o se ne è stato modificato uno esistente che è attivamente in uso, è importante sottolineare che le modifiche apportate alla configurazione non si applicano alle connessioni già stabilite all'FTD; pertanto, è necessario cancellare manualmente i tentativi di connessione attivi all'FTD. Per questo, collegarsi alla CLI dell'FTD e cancellare le connessioni attive come segue.

Per cancellare la connessione attiva per un indirizzo IP host specifico:

> clear conn address 192.168.1.10 all

Per cancellare le connessioni attive per un'intera rete di subnet:

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

Per cancellare le connessioni attive per un intervallo di indirizzi IP:

> clear conn address 192.168.1.1-192.168.1.10 all

Nota: si consiglia di usare la parola chiave 'all' alla fine del comando clear conn address per forzare la cancellazione dei tentativi di connessione VPN brute force attivi verso il firewall sicuro, soprattutto quando la natura dell'attacco VPN brute force sta lanciando un'esplosione di tentativi di connessione costanti.

Configurare un ACL del control plane per FTD gestito da FDM

Questa è la procedura che è necessario seguire in un FDM per configurare un ACL del control plane in modo da bloccare gli attacchi di forza bruta VPN in ingresso sull'interfaccia FTD esterna:

Passaggio 1. Aprire l'interfaccia utente grafica di FDM tramite HTTPS ed eseguire l'accesso con le credenziali.



cisco SECURE

Cisco Secure Firewall Device Manager

Username	
Password	
	•
	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 ABSOLUTEUX NO WARRANTV under the terms of "GNU Lesser General Public License, versions 2, 2, 2, 1 and 3" provided with

Firewall Device Manager Monitoring	Policies Objects Device: firepower	> 🖄 Ø ?	admin Administrator
Model Cisco Firepower Threat Defen	Software VDB Intrusion R se for VMwa 7.2.5-208 353.0 20220511	ule Update Cloud Services High Ava -1540 🛞 Not Registered Register Not Con	ailability CONFIGURE
reside Net	0/1 Cisco Firepower Threat Defense for VMware 0/0 0/1 Cisco Firepower Threat Defense for VMware 0/0 0/1 Cisco Firepower Threat Defense for VMware 0/0 0/1 Cisco Firepower Threat Defense for VMware		Internet CNS Server NTP Server Smart Liceme
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
Smart License Evaluation expires in 89 days	Backup and Restore	Troubleshoot No files created yet	DNS Server Management Interface Hostname Time Services

Passaggio 2. È necessario creare una rete di oggetti. A tale scopo, passare a Oggetti:

Immagine 25. Dashboard principale di FDM

Passaggio 2.1. Dal pannello sinistro, selezionare Reti, quindi fare clic sul pulsante '+' per creare un nuovo oggetto di rete.

Firewall Device Manager	Monitoring Policies Objects Device: fireport	wer (D_{a})
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-10.0.0.0-8	NETWORK 10.0.0/8
	2 IPv4-Private-172.16.0.0-12	NETWORK 172.16.0.0/12
C URLS	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-
🛖 IPSec Proposals		132.100.0.0-10
Secure Client Profiles		
Salidentity Sources		
1 Users		
Certificates		
e continuatos		
🔒 Secret Keys		

Immagine 26. Creazione di oggetti

Passaggio 2.2. Aggiungere un nome per l'oggetto di rete, selezionare il tipo di rete per l'oggetto, aggiungere l'indirizzo IP, l'indirizzo di rete o l'intervallo di IP in modo che corrisponda al traffico che deve essere negato all'FTD. Quindi, fare clic sul pulsante OK per completare la rete di oggetti.

- Nell'esempio, la rete di oggetti configurata ha lo scopo di bloccare gli attacchi di forza bruta VPN provenienti dalla subnet 192.168.1.0/24.

Firewall Device Manag	ger Monitoring Polici	Add Network Object	
Object Types ←	Network Obje		
C Networks	6 objects	OBJ-NET-UNWANTED-COUNTRY	
Security Zones	N NAME	defined. User defined Description Actions	
🖗 Application Filters	1 IPv4-Private-Al	re-172.16.0.0-12, IPv4-Private-	
🤣 URLS	2 IPv4-Private-10	Type	
Geolocations	3 IPv4-Private-1	Network	
Syslog Servers	4 IPv4-Private-19	192.168.1.0/24	
🔏 IKE Policies	6 any-ipv6	e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60	
IPSec Proposals		CANCEL	
Secure Client Profiles			
Identity Sources			
Certificates			
B Secret Keys			

Immagine 27. Aggiungi oggetto di rete

Passaggio 3. Quindi, è necessario creare un ACL esteso; a questo scopo, selezionare la scheda Device (Dispositivo) nel menu superiore.

Firewall Device Manager	Monitoring Policies Objects Device: firepow	er	disto SECURE
Object Types ←	Network Objects and Groups		
C Networks	7 objects	Y Filter	+ 👰
S Ports		Preset filters: System defined, User defined	
8 Security Zones	II 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	
🖉 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			
🙊 Certificates			
🔒 Secret Keys			

Immagine 28. Pagina Impostazioni dispositivo

Passaggio 3.1. Scorrere verso il basso e selezionare Visualizza configurazione dal riquadro Configurazione avanzata come indicato di seguito.

Firewall Device Manager Monitorin	g Policies Objects Device: firepower	ی کے کی د	admin Administrator
	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
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	DNS Server 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

Immagine 29. Configurazione avanzata FDM

Passaggio 3.2. Quindi, dal pannello sinistro, passare a Smart CLI > Oggetti e fare clic su CREA OGGETTO SMART CLI.

Firewall Device Manager	Monitoring	Ø Policies	ä. Dbjects	Device: firepower		6	0	?	•	admin Administrator	 diality SECURE 	
Advanced ← Configuration	Device Summ Objects	hary										
Smart CLI											+	
Objects	•	NAME		туре	DESCRIPTION					ACTIONS		
FlexConfig					There are no Smart	CLI objects y	et.					
FlexConfig Objects				1	Start by creating the firs	t Smart CLI	object.					
FlexConfig Policy					CREATE SMART (CLI OBJECT						

Immagine 30. Oggetti Smart CLI

Passaggio 3.3. Aggiungere un nome per l'ACL esteso da creare, selezionare Elenco accessi esteso dal menu a discesa del modello CLI, configurare le voci di controllo di accesso richieste dall'oggetto di rete creato nel passaggio precedente, 2.2, quindi fare clic sul pulsante OK per completare l'ACL.

Firewall Devic	Edit Smart CI I Object		sco SECURE
Advanced Configuration	Name ACL-UNWANTED-COUNTRY	Description	+
Smart CLI Objects	CLI Template Extended Access List ~		ACTIONS
FlexConfig	Template		Reset
FlexConfig Objects FlexConfig Policy	1 access-list ACL-UMANTED-COUNTRY extended 2 configure access-list-entry deny 3 deny network source [[003-hET-UMANTED-COUNTRY]] ~] destin	ation [any-lpu4 X v]	
	 4 configure deny port any ~ 5 deny port source AWY destination AWY 6 configure logging default ~ 		
	⊙ 7 default log set log-level INFORMATIONAL log-interval	300	-
		CANCEL	

Immagine 31. Creazione di ACL estesi

Nota: se è necessario aggiungere altre voci di controllo di accesso per l'ACL, è possibile farlo posizionando il mouse sulla sinistra della voce di controllo di accesso corrente. Verranno quindi visualizzati tre punti su cui è possibile fare clic. Fare clic su di esse e selezionare Duplica per aggiungere altre voci ACE.

Passaggio 4. Quindi, è necessario creare un oggetto FlexConfig. Per questo, spostarsi sul pannello sinistro e selezionare FlexConfig > Oggetti FlexConfig, quindi fare clic su CREATE FLEXCONFIG OBJECT.

Firewall Device Man	ager Monitoring P	olicies Objects	Device: firepower	(Σ_{-})) 🚔 💿 ?	• admin • Administrator	 dialis SECURE
Advanced ← Configuration	Device Summary FlexConfig	Objects					
Smart CLI					T Filter		+
Objects	•	NAME	DESCRIPTION			ACTIONS	
FlexConfig Objects FlexConfig Policy			Star	There are no FlexConfig o t by creating the first Flex CREATE FLEXCONFIG O	bjects yet. Config object. BJECT		

Immagine 32. Oggetti FlexConfig

Passaggio 4.1. Aggiungere un nome per l'oggetto FlexConfig per creare e configurare l'ACL del

piano di controllo come in entrata per l'interfaccia esterna, come indicato di seguito.

Sintassi della riga di comando:

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

Questo si traduce nell'esempio di comando successivo, che usa l'ACL esteso creato nel passaggio 3.3 'ACL-UNWANTED-COUNTRY' come segue:

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

Di seguito viene riportata la modalità di configurazione dell'oggetto FlexConfig nella finestra oggetto FlexConfig. A questo punto, selezionare il pulsante OK per completare l'oggetto FlexConfig.

Firewall Device Manager	Monitoring	Ø #2			<u></u>	admin Administrator
Advanced ←	Device Sur	Create FlexConfig Object			0 ×	
Configuration	FlexCo	Name				
		OBJ-FC-CONTROL-PLANE				+
Smart CLI		Description				OTTONIC
Objects					10	
ElevConfig		Variablee				
riexconing		There are no variables yet.				
FlexConfig Objects		Start with adding a new variable.				
FlexConfig Policy		+ ALU VARABLE				
		Template		C Expand	C Reset	
		1 access-group ACL-UNWANTED-C	COUNTRY in interface outside con	itrol-plane		
		Negate Template 🛕		Expand	Reset	
		1 no access-group ACL-UNMANTE	ED-COUNTRY in interface outside	control-plane		
				_		
			C/	ANCEL	ОК	

Immagine 33. Creazione oggetto FlexConfig

Passaggio 5. Procedere alla creazione di un criterio FlexConfig. A tale scopo, selezionare Flexconfig > Criterio FlexConfig, fare clic sul pulsante '+' e selezionare l'oggetto FlexConfig creato nel passaggio 4.1 precedente.



Immagine 34. Criteri FlexConfig

Passaggio 5.1. Verificare che nell'anteprima di FlexConfig sia visualizzata la configurazione corretta per l'ACL del piano di controllo creato e fare clic sul pulsante Save (Salva).

Firewall Device Ma	Inager Monitoring Policies Objects Device: firepower		ator ~ the SECURE
Advanced ← Configuration	Device Summary FlexConfig Policy		
Smart CLI	Group List	Preview	<> Expand
Objects	+ OBJ-FC-CONTROL-PLANE	<pre>access-group ACL-UNMANTED-COUNTRY in control-plane</pre>	interface outside
FlexConfig			
FlexConfig Objects			
FlexConfig Policy			
	SAVE		

Immagine 35. Anteprima criteri FlexConfig

Passaggio 6. Distribuire le modifiche della configurazione all'FTD che si desidera proteggere dagli attacchi di forza brute della VPN. A tale scopo, fare clic sul pulsante Deployment nel menu superiore, verificare che le modifiche della configurazione da distribuire siano corrette e quindi fare clic su DEPLOY NOW.

Firewall Device Manager		istrator v ulturle SECURE	
Advanced ← Configuration	Pending Changes Last Deployment Completed Successfully 05 Sep 2023 02:27 PM. <u>See Deployment History</u>	• ×	
Smart CLI	Deployed Version (05 Sep 2023 02:27 PM)	Pending Version C LEGEND	
Objects	Network Object Added: OBJ-NET-UNWANTED-COUNTRY		
FlexConfig		subType: Network CLAND value: 2.2.2.0/24 isSystemDefined: false dmsResolution: IPV4_ND_IPV6 description:	
FlexConfig Objects	-	name: 083-NET-UNMANTED-COUNTRY	
FlexConfig Policy	SelexConfig Policy Edited: default-group		
	flexConfigObjects: -	083-FC-CONTROL-PLANE	
	Extended Access List Added: ACL-UNWANTED-COUNTRY		
	- - - entries[0].sourceNetworks:	entries[0].logging: DEFAULT entries[0].action: DENY name: ACL-UNWANTED-COUNTRY	
	MORE ACTIONS V	CANCEL DEPLOY NOW	

Immagine 36. Distribuzione in sospeso

Passaggio 6.1. V	/erificare che la	a distribuzione dei	i criteri sia stata	a completata.
00				

Firewall Device Ma	nager Pending Changes Q X	
Advanced ← Configuration	*	
Smart CLI		
Objects	There are no Pending Changes yet. Nothing to deploy.	
FlexConfig	in interface outside	
FlexConfig Objects	Last successful deployment was on 05 Sep 2023 11:09 AM. You can see what was deployed in previous jobs in the Deployment History	
FlexConfig Policy		
	SAVE	

Immagine 37. Distribuzione completata

Passaggio 7. Se si crea un nuovo ACL del piano di controllo per l'FTD o se ne è stato modificato uno esistente che è attivamente in uso, è importante sottolineare che le modifiche apportate alla configurazione non si applicano alle connessioni già stabilite all'FTD; pertanto, è necessario cancellare manualmente i tentativi di connessione attivi all'FTD. Per questo, collegarsi alla CLI dell'FTD e cancellare le connessioni attive come segue.

Per cancellare la connessione attiva per un indirizzo IP host specifico:

> clear conn address 192.168.1.10 all

Per cancellare le connessioni attive per un'intera rete di subnet:

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

Per cancellare le connessioni attive per un intervallo di indirizzi IP:

> clear conn address 192.168.1.1-192.168.1.10 all

Nota: si consiglia di usare la parola chiave 'all' alla fine del comando clear conn address per forzare la cancellazione dei tentativi di connessione VPN brute force attivi verso il firewall sicuro, soprattutto quando la natura dell'attacco VPN brute force sta lanciando un'esplosione di tentativi di connessione costanti.

Configurazione di un ACL del control plane per un'ASA tramite CLI

Questa è la procedura da seguire in una CLI ASA per configurare un ACL del control plane in modo da bloccare gli attacchi VPN con forza bruta in arrivo sull'interfaccia esterna:

Passaggio 1. Accedere all'appliance ASA del firewall sicuro tramite la CLI e configurare il terminale come segue.

asa# configure terminal

Passaggio 2. Usare il comando successivo per configurare un ACL esteso in modo che blocchi un indirizzo IP host o un indirizzo di rete per il traffico che deve essere bloccato sull'appliance ASA.

- Nell'esempio, viene creato un nuovo ACL chiamato 'ACL-UNWANTED-COUNTRY' e la voce ACE configurata blocca gli attacchi della forza bruta VPN provenienti dalla subnet 192.168.1.0/24.

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

Passaggio 3. Usare il comando access-group successivo per configurare l'ACL 'ACL-

UNWANTED-COUNTRY' come ACL del piano di controllo per l'interfaccia ASA esterna.

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

Passaggio 4. Se si crea un nuovo ACL del piano di controllo o se ne è stato modificato uno esistente e in uso, è importante sottolineare che le modifiche apportate alla configurazione non si applicano alle connessioni già stabilite all'appliance ASA. Pertanto, è necessario cancellare manualmente i tentativi di connessione attiva all'appliance. A tale scopo, deselezionare le connessioni attive nel modo seguente.

Per cancellare la connessione attiva per un indirizzo IP host specifico:

asa# clear conn address 192.168.1.10 all

Per cancellare le connessioni attive per un'intera rete di subnet:

asa# clear conn address 192.168.1.0 netmask 255.255.255.0 all

Per cancellare le connessioni attive per un intervallo di indirizzi IP:

asa# clear conn address 192.168.1.1-192.168.1.10 all

Nota: si consiglia di usare la parola chiave 'all' alla fine del comando clear conn address per forzare la cancellazione dei tentativi di connessione VPN brute force attivi verso il firewall sicuro, soprattutto guando la natura dell'attacco VPN brute force sta lanciando un'esplosione di tentativi di connessione costanti.

Configurazione alternativa per bloccare gli attacchi per un firewall protetto tramite il comando 'shun'

In caso di un'opzione immediata per bloccare gli attacchi per il firewall protetto, è possibile utilizzare il comando 'shun'. Il comando theshunconsente di bloccare le connessioni da un host in attacco.

- Una volta evitato un indirizzo IP, tutte le connessioni future dall'indirizzo IP di origine vengono interrotte e registrate fino a quando la funzione di blocco non viene rimossa manualmente.

- La funzione di blocco del comando hunviene applicata indipendentemente dal fatto che sia attiva o meno una connessione con l'indirizzo host specificato.

- Se si specificano l'indirizzo di destinazione, le porte di origine e di destinazione e il protocollo, si elimina la connessione corrispondente e si rimuove l'indirizzo da tutte le connessioni future dell'IP di origine

indirizzo; verranno ignorate tutte le connessioni future, non solo quelle che corrispondono a questi parametri di connessione specifici.

- È possibile avere solo un comando per indirizzo IP di origine.

- Poiché viene utilizzato per bloccare gli attacchi in modo dinamico, il comando hunnon viene visualizzato nella configurazione del dispositivo di difesa delle minacce.

- Quando si rimuove la configurazione di un'interfaccia, vengono rimossi anche tutti gli shun collegati a quell'interfaccia.

- Sintassi del comando Shun:

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

- Per disabilitare un shun, utilizzare la forma no di questo comando:

no shun source_ip [vlan vlan_id]

Per evitare un indirizzo IP host, procedere come segue per il firewall protetto. Nell'esempio, il comando 'shun' viene usato per bloccare gli attacchi di forza bruta VPN provenienti dall'indirizzo IP di origine 192.168.1.10.

Esempio di configurazione per FTD.

Passaggio 1. Accedere al FTD tramite CLI e applicare il comando shun come indicato di seguito.

<#root>

>

shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf

Shun 192.168.1.10 successful

Passaggio 2. È possibile utilizzare i seguenti comandi show per confermare gli indirizzi IP di shun nel FTD e per monitorare il conteggio delle visite di shun per indirizzo IP:

<#root>

```
>
show shun
shun (outside) 192.168.1.10 0.0.0.0 0 0 0
>
show shun statistics
diagnostic=0FF, cnt=0
outside=0N, cnt=0
Shun 192.168.1.10 cnt=0, time=(0:00:28)
```

Esempio di configurazione dell'appliance ASA

Passaggio 1. Accedere all'ASA tramite la CLI e applicare il comando shun come indicato di seguito.

<#root>

asa#

```
shun 192.168.1.10
```

```
Shun 192.168.1.10 added in context: single_vf
```

```
Shun 192.168.1.10 successful
```

Passaggio 2. È possibile usare i seguenti comandi show per confermare gli indirizzi IP shun nell'appliance ASA e monitorare il numero di accessi shun per indirizzo 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
Shun 192.168.1.10 cnt=0, time=(0:01:39)
```

Nota: per ulteriori informazioni sul comando secure firewall shun, consultare la guida di riferimento dei comandi di Cisco Secure Firewall Threat Defense

Verifica

Per verificare che la configurazione dell'ACL del control plane sia attiva per il firewall protetto, procedere come segue:

Passaggio 1. Accedere al firewall protetto tramite CLI ed eseguire i comandi successivi per verificare che la configurazione dell'ACL del control plane sia stata applicata.

Esempio di output per l'FTD gestito da FMC:

<#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
```

Esempio di output per l'FTD gestito da 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
```

Esempio di output per l'appliance 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
```

Passaggio 2. Per verificare che l'ACL del control-plane stia bloccando il traffico richiesto, usare il comando packet-tracer per simulare una connessione TCP 443 in entrata all'interfaccia esterna del firewall protetto, quindi usare il comando show access-list <acl-name> per aumentare il numero di accessi all'ACL ogni volta che una connessione VPN con forza brute al firewall protetto viene bloccata dall'ACL del control-plane:

- Nell'esempio, il comando packet-tracer simula una connessione TCP 443 in entrata originata dall'host 192.168.1.10 e destinata all'indirizzo IP esterno del nostro firewall sicuro. L'output 'packet-tracer' conferma che il traffico viene interrotto e l'output 'show access-list' visualizza gli incrementi del numero di accessi per l'ACL del control plane sul posto:

Esempio di output per FTD

<#root>

Additional Information:

MAC Access list

>

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 Esempio di output per l'appliance 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

```
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)
```

0x9b4d26ac

Nota: se nel firewall sicuro è implementata una soluzione VPN come la VPN Cisco Secure Client, è possibile eseguire un reale tentativo di connessione al firewall sicuro per verificare che l'ACL del control plane stia funzionando come previsto per bloccare il traffico richiesto.

Bug correlati

 ENH | Connessioni client AnyConnect basate sulla località geografica: ID bug Cisco CSCvs65322

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).