為安全防火牆威脅防禦和ASA配置控制平面訪問 控制策略

目錄
· · · · · · · · · · · · · · · · · · ·
<u>必要條件</u>
<u>採用元件</u>
<u>背景資訊</u>
<u>設定</u>
為FMC管理的FTD設定控制平面ACL
為FDM管理的FTD配置控制平面ACL
使用CLI為ASA配置控制平面ACL
<u>使用「shun」命令阻止安全防火牆攻擊的備用配置</u>
<u>驗證</u> (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)

<u>相關錯誤</u>

簡介

本文檔介紹為安全防火牆威脅防禦和自適應安全裝置(ASA)配置控制平面訪問規則的過程。

必要條件

需求

思科建議您瞭解以下主題:

- 安全防火牆威脅防禦(FTD)
- 安全防火牆裝置管理員(FDM)
- 安全防火牆管理中心(FMC)
- 安全防火牆ASA
- 存取控制清單(ACL)
- FlexConfig

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 安全防火牆威脅防禦版本7.2.5
- 安全防火牆管理器中心版本7.2.5
- 安全防火牆裝置管理員版本7.2.5

• 安全防火牆ASA版本9.18.3

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

流量通常通過防火牆,並在資料介面之間路由;在某些情況下,拒絕發往「到」安全防火牆的流量 是有益的。思科安全防火牆可以使用控制平面訪問控制清單(ACL)來限制「機箱內」流量。控制平 面ACL何時有用的示例是控制哪些對等體可以建立到安全防火牆的VPN(站點到站點或遠端訪問 VPN)隧道。

安全防火牆「機箱內」流量

流量通常從一個介面(入站)穿過防火牆到達另一個介面(出站),這稱為「通過機箱式」流量 ,由訪問控制策略(ACP)和預過濾器規則共同管理。



圖1.通過機箱的流量示例

安全防火牆的「機箱內」流量

在其他情況下,流量直接目的地為FTD介面(站對站或遠端存取VPN),這稱為「到箱」流量,由 該特定介面的控制平面管理。



圖2.即插即用流量示例

有關控制平面ACL的重要注意事項

 自FMC/FTD 7.0版起,必須使用FlexConfig使用ASA上使用的相同命令語法配置控制平面 ACL。

- 關鍵字control-plane被附加到訪問組配置中,該配置會將流量「強制」到安全防火牆介面。如 果沒有在命令後附加控制平面字,ACL將限制通過「安全」防火牆的流量。
- 控制平面ACL不會限制安全防火牆介面的SSH、ICMP或TELNET入站。根據平台設定策略處 理(允許/拒絕),並且具有更高的優先順序。
- 控制平面ACL將流量限製為「進入」安全防火牆本身,而FTD的訪問控制策略或ASA的正常 ACL則控制流量「通過」安全防火牆。
- 與普通ACL不同,ACL的結尾沒有隱含的「deny」。
- 建立本檔案時,FTD地理定位功能無法用於限制「訪問」FTD。

設定

在下一個範例中,來自特定國家的一組IP位址嘗試登入FTD RAVPN,從而VPN強行進入網路。保 護FTD免受這些VPN暴力攻擊的最佳選項是設定控制平面ACL,以阻擋這些連線到外部FTD介面。

組態

為FMC管理的FTD設定控制平面ACL

您可以在FMC中按照以下步驟操作,以設定控制平面ACL來阻止傳入VPN暴力攻擊到外部FTD介面 :

步驟 1.通過HTTPS開啟FMC圖形使用者介面(GUI)並使用您的憑證登入。

cisco SECURE	
Secure Firewall	
Management	
Center	
Username	
Password	
Log In	

圖3.FMC登入頁

步驟 2.您需要建立延伸型ACL。為此,請導航到Objects > Object Management。

Firewall Management Center Overview / Dashboards / Dashboard	Overview Analy	ysis Policies Devices	Objects Integration	Deploy Q 🥐 🌣 🕢 admin 🔻 🗄	SECURE
Summary Dashboard (switch.dashboard)			Object Management Intrusion Rules		Reporting
Network × Threats Intrusion Events	Status Geolocat	ion QoS +		Show the Last 1 hour	• II
Unique Applications over Time No Data		► Top Web Applications Seen	— X No Data	Top Client Applications Seen No Data	
		Last updated 2 minutes ago			
Traffic by Application Risk		► Top Server Applications See	m -×	► Top Operating Systems Seen	

圖4.物件管理

步驟 2.1.從左側面板導航到Access List > Extended以建立擴展ACL。

Chiects / Object Manageme	ent Center Overview Analy	sis Policies	Devices	Objects	Integration	De	eploy Q 🧬 🌣 (admin - distante SE	ECURE
> AAA Server	Network					Add Network	▼ Q Filter		
 Access List Extended Standard 	A network object represents one or n network discovery rules, event search	ore IP addresses. es, reports, and se	Network object	ts are used in	various places, in	cluding access control policies,	network variables, intrusi	Unused Objects on rules, identity rules,	
> Address Pools	Name				v	/alue	Туре	Override	
Application Filters AS Path	any				(:	0.0.0/0 :/0	Group	۹ 🗎	a an
Cipher Suite List	any-ipv4				0	0.0.0.0/0	Network	Q	66
Community List	any-ipv6					:/0	Host	۹ 🗎	8
 Distinguished Name DNS Server Group 	IPv4-Benchmark-Tests				1	198.18.0.0/15	Network	۹ 🗎	8
> External Attributes	IPv4-Link-Local				1	169.254.0.0/16	Network	۹ 🗎	8
File List	IPv4-Multicast				2	224.0.0.0/4	Network	۹ 🗌	68
Geolocation	IPv4-Private-10.0.0.0-8				1	10.0.0/8	Network	۹ 🗎	A.
Interface	IPv4-Private-172.16.0.0-12				1	172.16.0.0/12	Network	٩	8
Key Chain	IPv4-Private-192.168.0.0-16				1	192.168.0.0/16	Network	۹ 🗎	8
> ркі	IPv4-Private-All-RFC1918					10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Group	٩	8
Policy List Port						Displa	ying 1 - 14 of 14 rows	< Page 1 of 1 >	ЯC

圖5.擴展ACL選單

步驟 2.2.然後,選擇Add Extended Access List。

Firewall Managemen Objects / Object Managemen	nt Center _{Overv}	riew Analysis	Policies	Devices	Objects	Integration	Deploy	५ 🌓 ¢	8 🕜 admin 🕶 🗌	cisco SECURE
> AAA Server	Extended						Add Extended Acce	ss List ् ९ F	ilter	
✓ Access List										
Extended	An access list object, traffic based on source	also known as an acc and destination adv	cess control list (/	ACL), selects	s the traffic to 4 and IPv6 ad	which a service will apply.	Standard-Identifies traffic t ects when configuring parti	ased on destin	ation address only.	dentifies
Standard			inclusion and portal of	oupports in v	4 und il Vo ud		eeta when contiguing para	colar reactives, t	acti us route maps.	
> Address Pools	Name						Value		Override	
Application Filters										
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							N	o data to display	I I Page 1	of 1 > > C
Drafiv List										

圖6.新增擴展ACL

步驟 2.3.鍵入擴展ACL的名稱,然後按一下Add按鈕建立訪問控制條目(ACE):

Firewall Mana Objects / Object M	agement Center	Overview	Analysis Policies	Devices Objects	Integration	Deploy Q	🥙 🌣 🔞 :	admin 🕶 🔤 🕬 secure
> AAA Server	New Extended A	ccess List Objec	ct					
Extended Standard	Name ACL-UNWANTED-C	OUNTRY						dress only. Identifies oute maps.
 Address Pools Application Filters AS Path 	Entries (0)						Add	Override
Cipher Suite List Community List	Sequence Action	Source	Source Port	Destination	Destination Port	Application		
 Distinguished Name DNS Server Group External Attributes 								
File List FlexConfig								
Geolocation Interface Key Chain	Allow Overrides							
Network							Save	
Policy List Port						No data te	o display I < <	Page 1 of $1 > > C$

圖7.延伸型ACL專案

步驟 2.4.將ACE操作更改為Block,然後新增源網路以匹配需要拒絕到FTD的流量,將目標網路保留 為Any,然後按一下Add按鈕完成ACE條目:

— 在本示例中,配置的ACE條目將阻止來自192.168.1.0/24子網的VPN暴力攻擊。

Firewa Objects /	Action: Block			cisco SECURE
> AAA Server	Logging: Default v			
Extended	Log Level:			Identifies ;.
Standard				
 Address Pools Application Filt 	300 Sec.			
AS Path	Network Part Application			∕∎&
Cipher Suite Lit				
> Community List	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 Gr	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	of1>>C
> Prefix List			Cancer Add	

圖8.拒絕的網路

步驟 2.5.如果需要新增更多ACE條目,請再次按一下Add按鈕並重複步驟2.4。完成後,點選Save按 鈕完成ACL配置。

Firewall Managemen Objects / Object Management	Edit Exten	nded Acc	ess List Object						
> AAA Server ~ Access List	Name ACL-UNW	ANTED-CO	UNTRY						
	Entries (1)								Identifies
Standard								Add	
> Address Pools								_	
Application Filters	Sequence	Action	Source	Source Port	Destination	Destination Port	Application		/ = A
AS Path	1	Block	192.168.1.0/24					11	
Cipher Suite List									
> Community List									
> Distinguished Name									
DNS Server Group									
> External Attributes									
	Allow Ov	verrides							
> FlexConfig									
Geolocation								Save	
Interface									
Key Chain									
Network									
> ркі									
Policy List									
Port							Displaying 1 - 1 of 1 rows	K < Page 1	of 1 > > C

圖9.完成的擴展ACL條目

步驟 3.接下來,您需要設定Flex-Config對象,以將控制平面ACL套用到外部FTD介面。為此,導航 到左側面板,然後選擇選項FlexConfig > FlexConfig Object。



圖10.FlexConfig對象選單

步驟 3.1.按一下新增FlexConfig對象。

Firewall Managemen	nt Center _{Overview}	Analysis Policies	Devices	Objects	Integration		Deploy Q	e *	🎗 🕜 admin	Cisco SECURE
 > AAA Server > Access List Extended Standard 	FlexConfig Object	t	ands, variables, a	ind scripting la	nguage instruction	s. It is used in FlexCo	dd FlexConfig Objec	ः व	Filter	
> Address Pools	Name						Description			
Application Filters	Default_DNS_Configure						Configure Default	DNS with	the help of TextC	bj 🖬 🤇 🗑
AS Path Cipher Suite List	Default_Inspection_Protocol_Di	isable					Disable Default In	spection.		¶∎ Q
> Community List	Default_Inspection_Protocol_Er	nable					Enable Default Ins	pection.		¶a q 📄
> Distinguished Name	DHCPv6_Prefix_Delegation_Co	nfigure					Configure one out	side (PD o	lient) and one ins	sid 📲 🤇 🗑
External Attributes	DHCPv6_Prefix_Delegation_Un	Configure					Remove configura	tion of on	e outside (PD clie	nt 🖥 Q 🗎
File List	DNS_Configure						Configure DNS wi	th the help	of TextObjects	in P∎ Q 🗑
✓ FlexConfig	DNS_UnConfigure						Remove the DNS	configurat	ions.	F q 🗎
Text Object	Eigrp_Configure						Configures eigrp.	1. Configu	res next hop. 2.	co 📲 q 🗑
Geolocation	Eigrp_Interface_Configure						Configures interfa	ce parame	ters for eigrp. 1.	c 🛍 q 🗎
Interface Key Chain	Eigrp_UnConfigure						Clears eigrp confi	guration fo	or an AS	¶a q
Network	Eigrp_Unconfigure_All						Clears eigrp confi	guration.		Β α =
> ркі							Displaying 1 - 20	of 48 row	s I< < Page 1	of 3 > > C

圖11.新增Flexconfig對象

步驟 3.2.為FlexConfig對象新增名稱,然後插入ACL策略對象。為此,請選擇Insert > Insert Policy Object > Extended ACL Object。

Firewall Manageme	Name: OBJ-FC-CONTROL-PLANE						≵ 🕑 admin ▾ 🖓	seller SECURE
> AAA Server	Description:						Filter	
✓ Access List								
Extended	A Copy-pasting any rich text m	ight introduce line break	s while generating CLI.	Please verify the	CLI before deployr	nent.		
Standard	Innert - Danie	umanti Oraca		The second second	A			
> Address Pools	Insert V B Depic	once		• Type:	Appena			
Application Filters	insert Policy Object F Te:	tt Object					the help of TextObi	B o =
AS Path	Insert System Variable Ne	twork					ule help of fextooj	
Cipher Suite List	Insert Secret Key Se	curity Zones						¶∎ Q
> Community List	Sta	ndard ACL Object						¶a q =
> Distinguished Name	Ext	ended ACL Object					Read and end held	B o E
DNS Server Group	Ro	ute Map					tilent) and one insid	-11 × 1
> External Attributes							e outside (PD client	¶a < ≣
File List							of TextObjects dn	₽ Q =
✓ FlexConfig	▼ Variables							Bo =
FlexConfig Object	Name	Dimension	Default Value	Property	Override	Description	Ons.	
Text Object				(Type:wame)			ires next hop. 2. co	¶∎ Q
Geolocation			No records to di	splay			sters for eigrp. 1. C	F a ⊂ _
Interface								
Key Chain							or an AS	Ч а (
Network								Π α =
> ркі							s IK < Page 1	of 3 > > I C
Policy List						Cancel Save		

步驟 3.3.為ACL對象變數新增名稱,然後選擇在步驟2.3中建立的擴展ACL,然後點選Save按鈕。

Firewall Managemer	Name: OBJ-FC-CONTROL-PLANE				🌫 🕜 admin 🕶 🗄	
	Description:					
AAA Server Access List		Insert Extended Access List Object \	/ariable 🛛 🕘		Filter	
Extended Standard	Copy-pasting any rich	Variable Name: VAR-ACL-UNWANTED-COUNTRY				
> Address Pools Application Filters	access-group	Description:			the help of TextObi	Fa Q ⊒
AS Path Cipher Suite List		Available Objects	Selected Object			Π α.≣
Community List		Q Search	RACL-UNWANTED-COUNTRY			¶∎ Q]]
 Distinguished Name DNS Server Group 		-BACL-UNWANTED-COUNTRY			lient) and one insid	¶∎ Q =
> External Attributes		Add			a outside (PD client	¶a q
 Flie List ✓ FlexConfig 	▼ Variables				> of TextObjects dn	
FlexConfig Object	Name			ription	ions.	• a <
Text Object					ires next hop. 2. co	η α
Geolocation					sters for eigrp. 1. C	¶∎ Q 📄
Interface Key Chain			Cancel		or an AS	¶∎ Q
Network						Β α
> PKI					s K < Page 1	of 3 > > C

圖13.FlexConfig對象變數ACL分配

步驟 3.4.然後,將控制平面ACL配置為外部介面的入站流量,如下所示。

命令列語法:

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

圖12.FlexConfig對象變數

此命令轉換為下一個命令示例,該示例使用在以上步驟2.3「VAR-ACL-UNWANTED-COUNTRY」 中建立的ACL變數,如下所示:

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

這是必須配置到FlexConfig對象視窗中的方法,之後,選擇「儲存」按鈕完成FlexConfig對象。

Firewall Manageme	Name:							de este
U Objects / Object Manageme	OBJ-FC-CONTROL-PLANE						⊁ 🕲 admin v '	CISCO SECURE
> AAA Server	Description:						Filter	
✓ Access List								
Extended	Copy-pasting any rich text m	ight introduce line break	s while generating CLI.	Please verify the	CLI before deploy	ment.		
Standard	Incert - Depis	umanti Onco		- Trans	Annend			
> Address Pools	insert 🕶 🔛 Depio	yment: Once		• Type:	Append	_		
Application Filters	access-group \$VAR-ACL-UNWANTED-	COUNTRY in interface outsid	le control-plane				the help of TextObi	Fa q ⊒
AS Path								
Cipher Suite List								¶∎ < ⊤
> Community List								ि
> Distinguished Name							lient) and one insid	Fac 📄
DNS Server Group								
> External Attributes							e outside (PD client	¶∎ Q
File List							of TextObjects dn	F a Q ()
✓ FlexConfig	▼ Variables						0.05	Ba a ⊇
FlexConfig Object	Name	Dimension	Default Value	Property (Type:Name)	Override	Description	res sent hap 2 as	B O F
Text Object	VAR-ACL-UNWANTED-COUNTRY	SINGLE	ACL-UNWANTED	EXD_ACL:A	false		ires next hop. z. co	
Geolocation							aters for eigrp. 1. C	¶∎ Q
Interface							or an AS	Fi Q
Key Chain								
Network								
> PKI						Cancel	Pick Page	013 / // C
Policy List						ouncel oure		

圖14.Flexconfig Object complete命令列

步驟 4.您需要將FlexConfig對象配置應用於FTD,為此,請轉至Devices > FlexConfig。

Firewall Managemen	t Center _{Overview} Analysis Policies	Devices Objects	Integration	Deploy Q 🧬 🕻	✿ ø admin • │ :[see SECURE	
 > AAA Server > Access List Extended Standard > Address Pools Application Filters 10 Server 	FlexConfig Object FlexConfig Object include device configuration command Name Defa	Device Management Device Upgrade d: NAT QoS Platform Settings FlexConfig U 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	E ¹ α =	
AS Path Cipher Suite List > Community List	Default_ins	Default_Inspection_Protocol_Disable Default_Inspection_Protocol_Enable					
> Distinguished Name DNS Server Group	DHCPv6_Pr		Configure one outside (PD client) and one insid 📴 Q				
External Attributes File List ElevCente	DHCPv6_Prei	fix_Delegation_UnConfigure		Remove configuration of one outside (PD client 🖷 🔍			
FlexConfig Object	D	NS_UnConfigure		Remove the DNS configurati	ions.	R Q 🗎	
Text Object Geolocation		Eigrp_Configure					
Interface	Eigrp	Configures interface parame	aters for eigrp. 1. C				
Key Chain Network	Eigr	Clears eigrp configuration.					
> PKI Policy List				Displaying 1 - 20 of 49 row	s K < Page 1	of3 > > C'	

圖15.FlexConfig Policy選單

步驟 4.1.然後,如果沒有為FTD建立的FlexConfig,則點選New Policy,或編輯現有的FlexConfig策略。

P	Firewall Management Center Devices / FlexConfig	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ 🕯	¢ 9	🕜 admin -	cisco SECURE
												[New Policy
	FlexConfig Policy			Status				Last Modified					
						created. Add	a new policy						

圖16.FlexConfig策略建立

步驟 4.2.為新的FlexConfig策略新增名稱,並選擇要應用建立的控制平面ACL的FTD。

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

圖17.FlexConfig策略裝置分配

步驟 4.3.在左側面板中,搜尋在上面的步驟3.2中建立的FlexConfig對象,然後通過按一下位於視窗 中間的右箭頭將其新增到FlexConfig策略中,然後點選Save按鈕。

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q 🥩 🌣 🕢 admin 🛛 🖓 🚓 ECUR	E
FLEXCONFIG-POLICY							You have unsaved changes Preview Config	
							Policy Assignments (1)
	3 Selecte	d Prenend F	levConfigs					
Available FlexConfig C FlexConfig Object	# Nam	18	ic.comigs		Description			
Vuser Defined								
BOBJ-FC-CONTROL-PLANE								
System Defined								
Default_DNS_Configure								
Default_Inspection_Protocol_Disable								
Protocol_Enable	Selecte	d Append Fl	exConfigs					
☐ DHCPv6_Prefix_Delegation_Configure								
DHCPv6_Prefix_Delegation_UnConfigure	# Nam	10			Description			
DNS_Configure	1 OBJ	-FC-CONTROL	-PLANE				٩ 🖬	
DNS_UnConfigure	Ч							
B Eigrp_Configure								
Bigrp_Interface_Configure								
_9 Eigrp_UnConfigure								
.9 Eigrp_Unconfigure_All								

圖18.FlexConfig策略對象分配

步驟 5.繼續將組態變更部署到FTD,並為此請導覽至Deploy > Advanced Deploy。

Firewall Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy Q	e 🕹	🕑 admin -	cisco SE	CURE
FLEXCONFIG-POLICY								Advance	d Deploy	eploy All	ncel
Enter Description						FTD-CONTROL-PLANE		Ready for	Deployment	÷	:s (1)
Available FlexConfig	"à Selecte	ed Prepend F	lexConfigs								
×	# Nan	ne			Description						
V User Defined											
OBJ-FC-CONTROL-PLANE	-										
✓ System Defined											
Topfault_DNS_Configure											
Default_Inspection_Protocol_Disable						1 device is available for deployment				₽ 1 9	
Default_Inspection_Protocol_Enable	Selecte	ed Append F	lexConfigs								
DHCPv6_Prefix_Delegation_Configure	# Nan	ne			Description						
DHCPv6_Prenx_Delegation_UnConfigure DNS_Configure	1 08		-DI ANE								0
	- 000		- F LPANE								~
Fiarn Configure											
"i Eigrp_ostinguto											

圖19.FTD進階部署

步驟 5.1.然後,選擇要應用FlexConfig策略的FTD。如果一切正常,則按一下「部署」。

þ	Fir	ewall Management Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ 🇳	🔅 🕑 admin 🔻	cisco SECURE
1 devi	ce sele	cted Search using device name, user name, type,	group or statu	15								Deploy time: Estim	ate 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 Deploym	ent
\$1 •		Flex Configuration Template Policy: FLEXCONFIG-POLICY											
https://10.	.88.243.	58:43013/ddd/#ContextExplorer											

圖20.FTD部署驗證

步驟 5.2.之後,將彈出一個「部署確認」視窗,新增註釋以跟蹤部署並繼續進行「部署」。

Firewall Management Cente		Analysis Policies Devices Objects Integration Deploy Q 🧬 🌣 🕜 admin 🔻 🖓 SECURE					
1 device selected Y Q Search using device name, user name							
	Modified by						
V FTD-CONTROL-PLANE	admin			Sep 5, 2023 12	:05 PM 🗒	Ready for Deployment	
Flex Configuration Template Policy: FLEXCONFIG-POLI	CY	ployment Confirmation		×			
	You	have selected 1 device to depl	loy				
	Yo	a can optionally add notes abou	ut the configuration changes				
				Deploy			

圖21.FTD部署註釋

步驟 5.3.部署FlexConfig更改時可能會出現警告消息。只有完全確定策略配置正確時,才按一下 Deploy。



圖22.FTD部署Flexconfig警告

步驟 5.4.確認FTD的原則部署成功。

Firewall Management Center	Overview Analysis	Policies Devices Objec	ts Integration	Deploy Q 🤞	🗘 🕜 admin 🕶 🔤 🖓 🖓 🕹
Q Search using device name, user name, typ	e, group or status				Deploy
Device	Modified by	Inspect Interruption Type	Group	Last Deploy Time Preview	Status
V FTD-CONTROL-PLANE	admin	FTD		Sep 5, 2023 12:05 PM	Completed

圖23.FTD部署成功

步驟 6. 如果您為FTD建立新控制平面ACL,或編輯現有控制平面ACL且現有控制平面ACL處於使用 中,則務必強調所作的組態變更不適用於已建立與FTD的連線,因此,您需要手動清除與FTD的連 線嘗試。為此,請連線到FTD的CLI並清除作用中連線,如下所示。

要清除特定主機IP地址的活動連線:

> clear conn address 192.168.1.10 all

要清除整個子網網路的活動連線,請執行以下操作:

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

要清除IP地址範圍的活動連線,請執行以下操作:

> clear conn address 192.168.1.1-192.168.1.10 all

✤ 注意:強烈建議在clear conn address命令末尾使用關鍵字「all」,強制清除對安全防火牆的 活動的VPN暴力連線嘗試,主要在VPN暴力攻擊的性質正在引發大量持續連線嘗試時。

為FDM管理的FTD配置控制平面ACL

在FDM中,需要遵循以下步驟來配置控制平面ACL,以阻止傳入VPN暴力攻擊到外部FTD介面: 步驟 1.通過HTTPS開啟FDM GUI並使用您的憑據登入。



This product contains some software licensed under the "GNU Lesser General Public License, versions: 2, 2.1 and 3" provided with ABSOLUTELY NO WARRANTY under the terms of "GNU Lesser General Public License, version 2 🕻 version 2.1 🖒 and version 3 🕼

圖24.「FDM登入」頁

步驟 2.您需要建立對象網路。為此,請導航到Objects:



```
圖25.FDM主儀表板
```

步驟 2.1.在左側面板中選擇Networks,然後按一下「+」按鈕建立新的網路對象。

Firewall Device Manager	Monitoring Policies Objects Device: firepow	ver (>)	admin Administrator
Object Types ←	Network Objects and Groups		
C Networks	6 objects		▼ Filter + 🗐
S Ports			Preset filters: System defined, User defined
8 Security Zones	# NAME	TYPE VALUE	ACTIONS
🐬 Application Filters	1 IPv4-Private-10.0.0-8	NETWORK 10.0.0/8	
⊘ URLs	2 IPv4-Private-172.16.0.0-12	NETWORK 172.16.0.0/12	
Geolocations	3 IPv4-Private-192.168.0.0-16	NETWORK 192.168.0.0/16	
	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-10.0 192.168.0.0-16	0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private-
👍 IPSec Proposals			
Secure Client Profiles			
Sources			
1 Users			
🞗 Certificates			
Secret Keys			

圖26.對象建立

步驟 2.2.為網路物件新增名稱,為物件選取網路型別,並新增IP位址、網路位址或IP範圍,以與需要拒絕到FTD的流量相符。然後,按一下「確定」(Ok)按鈕完成對象網路。

— 在本示例中,配置的對象網路旨在阻止來自192.168.1.0/24子網的VPN暴力攻擊。

Firewall Device Manager	Monitoring Polici	Add Network Object
Object Types ←	Network Obje	Name
C Networks	6 objects	OBJ-NET-UNWANTED-COUNTRY +
S Ports	_	defined. User defined
8 Security Zones	N NAME	Description
P Application Filters	1 IPv4-Private-Al	e-172.16.0.0-12, IPv4-Private-
🤣 URLS	2 IPv4-Private-10	Туре
Geolocations	3 IPv4-Private-13	Network Host FQDN Range
Syslog Servers	4 IPv4-Private-19	Network
R IKE Policies	5 any-ipv4	192.168.1.0/24
	6 any-ipv6	
eg IPSec Proposais		CANCEL
Secure Client Profiles		
Sa Identity Sources		
L Users		
🙊 Certificates		
Secret Keys		

圖27.新增網路對象

步驟 3.然後,您需要建立一個延伸型ACL,為此,請導航到頂部選單的「Device(裝置)」頁籤。

Firewall Device Manager	Monitoring Policies Objects Device: firepow	ver	cisco SECURE
Object Types ←	Network Objects and Groups		
C Networks	7 objects	T Filter	+ 🔍
S Ports		Preset filters: System.defined, User.defined	
Security Zones	# NAME	TYPE VALUE	ACTIONS
🐬 Application Filters	1 IPv4-Private-All-RFC1918	Group IPv4-Private-10.0.08, 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	
IKE Policies	5 any-ipv4	NETWORK 0.0.0.0/0	
	6 any-ipv6	NETWORK ::/0	
	7 OBJ-NET-UNWANTED-COUNTRY	NETWORK 192.168.1.0/24	
Secure Client Profiles			
Salarity Sources			
1 Users			
😫 Certificates			
🔒 Secret Keys			

圖28.「裝置設定」頁

步驟 3.1.向下滾動,從Advanced Configuration(高級配置)方塊中選擇View Configuration(檢視 配置),如下所示。

Firewall Device Manager Monitoring	Policies Objects Device: firepower	> 🚔 🙆 ?	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 DNS Server
Smart License	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

圖29.FDM高級配置

步驟 3.2.然後,從左側面板導航到Smart CLI > Objects,然後點選CREATE SMART CLI OBJECT。

Firewall Device Manager	Monitoring Policie	s Objects	Device: firepower	o 🚑 🔅) ? :	admin Administrator	cisco SECURE
Advanced ← Configuration	Device Summary Objects						
Smart CLI							+
Objects	# NAME		түре	DESCRIPTION		ACTIONS	
FlexConfig				There are no Smart CLI objects yet.			
FlexConfig Objects			5	CREATE SMART CLI OR JECT			
FlexConfig Policy							

圖30.智慧CLI對象

步驟 3.3.為要建立的擴展ACL新增名稱,從CLI模板下拉選單中選擇Extended Access List,並使用 在上面的步驟2.2中建立的網路對象配置所需的ACE,然後按一下OK按鈕完成ACL。

Firewall Device		admin "Itali" SECURE			
Advanced Configuration	Name	Description			
Smart CLI	ACL-UNWANTED-COUNTRY CLI Template	+			
Objects	Extended Access List ~	A:1085			
FlexConfig	Template				
FlexConfig Objects	1 access-list ACL-UMMANTED-COUNTRY extended 2 configure access-list-entry deny ~ 3 deny network source [(00):htt=UMMANTED-COUNTRY ~] destination [http://pvd X ~] 4 configure deny port any ~ 5 deny port source ANY destination NNY 6 configure logging default ~ 7 default log set log-level INFORMATIONAL log-interval 300				
l					

圖31.擴展ACL建立

✤ 注意:如果需要為ACL新增更多ACE,可以將滑鼠懸停在當前ACE的左側,這樣就會出現三個 可點選的點。按一下它們並選擇「複製」以新增更多ACE。

步驟 4.然後,您需要建立FlexConfig對象,為此,請導航到左側面板並選擇FlexConfig > FlexConfig對象,然後按一下CREATE FLEXCONFIG OBJECT。

Firewall Device Manage	r Monitoring Policies Objects	Device: firepower	 second SECURE
Advanced ← Configuration	Device Summary FlexConfig Objects		
Smart CLI		Tilter	+
Objects	# NAME	DESCRIPTION ACTIONS	
FlexConfig FlexConfig Objects FlexConfig Policy		There are no FlexConfig objects yet. Start by creating the first FlexConfig object.	

圖32.FlexConfig對象

步驟 4.1.為FlexConfig對象新增名稱,以建立控制平面ACL並將其配置為外部介面的入站流量,如 下所示。

命令列語法:

這轉換為下一個命令示例,該示例使用在以上步驟3.3「ACL-UNWANTED-COUNTRY」中建立的 擴展ACL,如下所示:

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

這是將其配置到FlexConfig對象視窗的方式,之後,選擇「確定」(OK)按鈕完成FlexConfig對象。

Firewall Device Mar	nager Monitoring	Ø #	$\bigcirc \bigcirc \bigcirc \bigcirc$		admin Administrator	
	Device Sur	Create FlexConfig Object			Pauliningulator	
Advanced ← Configuration	FlexCo	Name				
Smart CI I		OBJ-FC-CONTROL-PLANE			+	
Objects		Description			CTIONS	
				h.		
FlexConfig		Variables				
FlexConfig Objects		Start with adding a new variable.				
FlexConfig Policy		+ ADD VARIABLE				
		Template	🗘 Expand	C Reset		
		1 access-group ACL-UNMANTED-COUN	TRY in interface outside control-plane			
		Negate Template 🛆	Expand	🗘 Reset		
		1 no access-group ACL-UNMANTED-CO	DUNTRY in interface outside control-plan	e		
			CANCEL	ОК		

圖33.FlexConfig對象建立

步驟 5.繼續建立FlexConfig策略,為此,請導航到Flexconfig > FlexConfig Policy,按一下「+」按 鈕,然後選擇在上面的步驟4.1中建立的FlexConfig對象。



圖34.FlexConfig策略

步驟 5.1.驗證FlexConfig預覽是否顯示所建立的控制平面ACL的正確配置,然後按一下「Save(儲存)」按鈕。

Firewall Device Manager	Monitoring Policies Objects Device: firepower	S→ (admin Administrator) × the second second second se
Advanced ← Configuration	Device Summary FlexConfig Policy	
Smart CLI	Group List	Preview
Objects	T OBJ-FC-CONTROL-PLANE	1 access-group ACL-UMMANTED-COUNTRY in interface outside control-plane
FlexConfig		
FlexConfig Objects		
FlexConfig Policy		
	SAVE	

圖35.FlexConfig策略預覽

步驟 6.將配置更改部署到要防禦VPN暴力攻擊的FTD,為此,按一下頂部選單上的Deployment按鈕 ,驗證要部署的配置更改是否正確,然後按一下DEPLOY NOW。



圖36.掛起的部署

步驟 6.1.驗證策略部署是否成功。

Firewall Device Ma	nager Pending Changes	admin istrator ~ "title" SECURE
Advanced ← Configuration ← Smart CLI Objects	There are no Pending Changes yet. Nothing to deploy.	← Expand
FlexConfig 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	in interface outside
Hexconfig Policy	SAVE	CK

圖37.部署成功

步驟 7. 如果您為FTD建立新控制平面ACL,或編輯現有控制平面ACL且現有控制平面ACL處於使用 中,則務必強調所作的組態變更不適用於已建立與FTD的連線,因此,您需要手動清除與FTD的連 線嘗試。為此,請連線到FTD的CLI並清除作用中連線,如下所示。

要清除特定主機IP地址的活動連線:

要清除整個子網網路的活動連線,請執行以下操作:

> clear conn address 192.168.1.0 netmask 255.255.255.0 all

要清除IP地址範圍的活動連線,請執行以下操作:

> clear conn address 192.168.1.1-192.168.1.10 all

✤ 注意:強烈建議在clear conn address命令末尾使用關鍵字「all」,強制清除對安全防火牆的 活動的VPN暴力連線嘗試,主要在VPN暴力攻擊的性質正在引發大量持續連線嘗試時。

使用CLI為ASA配置控制平面ACL

您需要在ASA CLI中按照以下步驟配置控制平面ACL以阻止傳入的VPN暴力攻擊到外部介面:

步驟 1.通過CLI登入安全防火牆ASA並訪問「配置終端」,如下所示。

asa# configure terminal

步驟 2.使用next命令配置擴展ACL,以阻止需要阻止到ASA的流量的主機IP地址或網路地址。

— 在本示例中,您將建立一個名為「ACL-WANTED-COUNTRY」的新ACL,並且配置的ACE條目 將阻止來自192.168.1.0/24子網的VPN暴力攻擊。

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

步驟 3.使用next access-group命令將「ACL-UNWANTED-COUNTRY」ACL配置為外部ASA介面的 控制平面ACL。

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

步驟 4. 如果建立新的控制平面ACL或編輯了正在使用的現有控制平面ACL,則必須強調所做的配置

更改不適用於已建立到ASA的連線,因此,您需要手動清除對ASA的活動連線嘗試。為此,請按如 下所示清除活動連線。

要清除特定主機IP地址的活動連線:

asa# clear conn address 192.168.1.10 all

要清除整個子網網路的活動連線,請執行以下操作:

asa# clear conn address 192.168.1.0 netmask 255.255.255.0 all

要清除IP地址範圍的活動連線,請執行以下操作:

asa# clear conn address 192.168.1.1-192.168.1.10 all



使用「shun」命令阻止安全防火牆攻擊的備用配置

如果存在阻止安全防火牆攻擊的立即選項,則可以使用「shun」命令。使用Thhuncommand可以阻止來自攻擊主機的連線。

— 迴避IP地址後,源IP地址的所有未來連線都會被丟棄並記錄,直到手動刪除阻止功能為止。

— 無論具有指定主機地址的連線當前是否處於活動狀態,都會應用thhuncommand的阻止功能。

— 如果指定目的地位址、來源和目的地連線埠和通訊協定,則會捨棄相符的連線,並對來自來源 IP的所有未來連線設定迴避

地址;將來所有連線都將被迴避,而不僅僅是那些匹配這些特定連線引數的連線。

— 每個源IP地址只能使用oneshuncommand。

— 由於thhuncommand用於動態阻止攻擊,因此它不會顯示在威脅防御設備配置中。

— 每當刪除介面配置時,也會刪除連線到該介面的所有分路。

- Shun命令語法:

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

— 要禁用shun,請使用此命令的no形式:

no shun source_ip [vlan vlan_id]

要避開主機IP地址,請按照以下步驟處理安全防火牆。 在本示例中,「shun」命令用於阻止來自源 IP地址192.168.1.10的VPN暴力攻擊。

FTD的組態範例。

步驟 1.透過CLI登入FTD, 然後按以下方式套用shun指令。

<#root>

>

shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf

Shun 192.168.1.10 successful

步驟 2. 您可以使用以下show命令確認FTD中的shun IP位址,並監控每個IP位址的shun命中次數:

<#root>

>

show shun

shun (outside) 192.168.1.10 0.0.0.0 0 0

>

show shun statistics

diagnostic=OFF, cnt=0
outside=ON, cnt=0

Shun 192.168.1.10 cnt=0, time=(0:00:28)

ASA配置示例

步驟 1.通過CLI登入到ASA並按如下方式應用shun命令。

<#root>

asa#

shun 192.168.1.10

Shun 192.168.1.10 added in context: single_vf

Shun 192.168.1.10 successful

步驟 2. 您可以使用以下show命令確認ASA中的shun IP地址並監控每個IP地址的shun命中數:

<#root>

asa#

show shun

shun (outside) 192.168.1.10 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)

≫ 注意:有關secure firewall shun命令的詳細資訊,請檢視<u>思科安全防火牆威脅防禦命令參考</u>

驗證

要確認安全防火牆的控制平面ACL配置已就緒,請按照以下步驟操作:

步驟 1.通過CLI登入安全防火牆,並運行以下命令以確認已應用控制平面ACL配置。

FMC管理的FTD的輸出示例:

<#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

FDM管理的FTD的輸出示例:

<#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

ASA的輸出示例:

<#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

步驟 2. 要確認控制平面ACL正在阻止所需的流量,請使用packet-tracer命令模擬到安全防火牆外部 介面的傳入TCP 443連線,然後使用show access-list <acl-name> 命令,每當到安全防火牆的 VPN暴力連線被控制平面ACL阻止時,ACL命中計數都會增加:

— 在本例中,packet Tracer命令模擬從主機192.168.1.10發往安全防火牆外部IP地址的傳入TCP 443連線。「packet Tracer」輸出確認流量被丟棄,而「show access-list」輸出則顯示現有控制平 面ACL的命中計數增量:

FTD的輸出範例

<#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

<#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) 0x9b4d26ac

✤ 注意:如果在安全防火牆中實施類似Cisco安全客戶端VPN的RAVPN解決方案,則可能會執行 到安全防火牆的真實連線嘗試,以確認控制平面ACL是否按預期工作,從而阻止所需的流量。

相關錯誤

• ENH | 基於地理位置的AnyConnect客戶端連線:思科錯誤<u>ID CSCvs65322</u>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。