帶網路地址轉換的PIX/ASA(版本7.x和更高版本)IPsec VPN隧道配置示例

目錄

簡介 必要條件 需求 採用元件 慣例 相關產品 設定 網路圖表 組態 PIX安全裝置和訪問清單配置 PIX安全裝置和MPF(模組化策略框架)配置 驗證 疑難排解 路由器IPsec的故障排除命令 清除安全關聯 PIX故障排除命令 相關資訊

<u>簡介</u>

此示例配置演示了通過執行網路地址轉換(NAT)的防火牆的IPsec VPN隧道。 如果您使用早於 12.2(13)T且不包括12.2(13)T的Cisco IOS®軟體版本,則此配置不適用於埠地址轉換(PAT)。此型別 的配置可用於隧道IP流量。此組態不能用於加密沒有通過防火牆(例如IPX或路由更新)的流量。通 用路由封裝(GRE)通道是更合適的選擇。在本示例中,Cisco 2621和3660路由器是加入兩個專用網 路的IPsec隧道終端,其間的PIX上帶有管道或訪問控制清單(ACL),以便允許IPsec流量。

注意:NAT是一對一地址轉換,不要與PAT混淆,後者是許多(防火牆內部)對一轉換。有關 NAT操作和配置的詳細資訊,請參閱<u>驗證NAT操作和基本NAT故障排除</u>或<u>NAT的工作原理</u>。

注意:帶PAT的IPsec可能無法正常工作,因為外部隧道終結點裝置無法處理來自一個IP地址的多個 隧道。聯絡您的供應商,以確定隧道終端裝置是否與PAT配合使用。此外,在Cisco IOS軟體版本 12.2(13)T及更高版本中,NAT透明功能可用於PAT。有關詳細資訊,請參閱<u>IPSec NAT透明度</u>。請 參閱透過NAT的IPSec ESP支援,以詳細瞭解Cisco IOS軟體版本12.2(13)T和更新版本中的這些功 能。

注意:在使用Cisco技術支援開啟案例之前,請參閱<u>NAT常見問題</u>,該問題有許多常見問題的答案。

有關如何在PIX版本6.x及更低版本上使用NAT配置IPsec隧道穿過防火牆的詳細資訊,請參閱使用

<u>必要條件</u>

<u>需求</u>

本文件沒有特定需求。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- Cisco IOS軟體版本12.0.7.T(最高但不包括Cisco IOS軟體版本12.2(13)T)有關最新版本,請參閱 IPSec NAT透明度。
- 思科2621路由器
- 思科3660路由器
- 運行7.x及更高版本的Cisco PIX 500系列安全裝置。

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。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

<u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

相關產品

本檔案也適用於軟體版本7.x及更新版本的Cisco 5500系列調適型安全裝置(ASA)。

<u>設定</u>

本節提供可用於設定本檔案中所述功能的資訊。

注意:要查詢有關本文檔使用的命令的更多資訊,請使用<u>命令查詢工具</u>(僅限<u>註冊</u>客戶)。

<u>網路圖表</u>

本檔案會使用以下網路設定:



10.3.3.2

<u>組態</u>

本檔案會使用以下設定:

- <u>思科2621配置</u>
- <u>思科3660配置</u>
- PIX安全裝置和訪問清單配置高級安全裝置管理器GUI(ASDM)配置命令列介面(CLI)配置
- PIX安全裝置和MPF(模組化策略框架)配置

Cisco 2621

```
Current configuration:
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
 !
hostname goss-2621
 1
ip subnet-zero
 !
ip audit notify log
ip audit po max-events 100
isdn voice-call-failure 0
cns event-service server
 1
!--- The IKE policy. crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 99.99.99.2
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto map mymap local-address FastEthernet0/1
!--- IPsec policy. crypto map mymap 10 ipsec-isakmp
 set peer 99.99.99.2
 set transform-set myset
!--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
 1
controller T1 1/0
 1
interface FastEthernet0/0
 ip address 10.2.2.1 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
 1
interface FastEthernet0/1
 ip address 10.1.1.2 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
!--- Apply to the interface. crypto map mymap
1
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
no ip http server
!--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255
line con 0
 transport input none
line aux 0
line vty 0 4
```

```
no scheduler allocate
end
Cisco 3660
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
 1
hostname goss-3660
 1
ip subnet-zero
 1
cns event-service server
!--- The IKE policy. crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 99.99.99.12
 1
crypto ipsec transform-set myset esp-des esp-md5-hmac
 1
crypto map mymap local-address FastEthernet0/0
!--- The IPsec policy. crypto map mymap 10 ipsec-isakmp
 set peer 99.99.99.12
 set transform-set myset
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
 !
interface FastEthernet0/0
 ip address 99.99.99.2 255.255.255.0
 no ip directed-broadcast
 ip nat outside
 duplex auto
 speed auto
!--- Apply to the interface. crypto map mymap
 1
 interface FastEthernet0/1
 ip address 10.3.3.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
 duplex auto
 speed auto
 1
interface Ethernet3/0
 no ip address
 no ip directed-broadcast
 shutdown
 !
interface Serial3/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 I
 interface Ethernet3/1
 no ip address
```

```
no ip directed-broadcast
 interface Ethernet4/0
 no ip address
 no ip directed-broadcast
 shutdown
 I
interface TokenRing4/0
 no ip address
 no ip directed-broadcast
 shutdown
 ring-speed 16
1
!--- The pool from which inside hosts translate to !---
the globally unique 99.99.99.0/24 network. ip nat pool
OUTSIDE 99.99.99.70 99.99.99.80 netmask 255.255.255.0
!--- Except the private network from the NAT process. ip
nat inside source route-map nonat pool OUTSIDE
ip classless
ip route 0.0.0.0 0.0.0.0 99.99.99.1
no ip http server
1
!--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 101 deny ip 10.3.3.0 0.0.0.255 any
!--- Except the private network from the NAT process.
access-list 110 deny ip 10.3.3.0 0.0.0.255 10.2.2.0
0.0.0.255
access-list 110 permit ip 10.3.3.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 110
!
line con 0
 transport input none
line aux 0
line vty 0 4
1
end
```

PIX安全裝置和訪問清單配置

<u>ASDM 5.0配置</u>

完成以下步驟,以便使用ASDM配置PIX防火牆版本7.0。

- 通過控制檯連線到PIX。在清除的配置中,使用互動式提示啟用高級安全裝置管理器 GUI(ASDM),以便從工作站10.1.1.3管理PIX。
- 2. 在Workstation 10.1.1.3中開啟Web瀏覽器並使用ADSM(在本例中為https://10.1.1.1)。
- 3. 在證書提示上選擇Yes, 然後使用PIX防火牆ASDM載入程式配置中配置的啟用密碼登入。
- 4. 如果這是第一次在PC上運行ASDM,則會提示您使用ASDM啟動程式還是將ASDM用作Java應 用。在本示例中,ASDM啟動程式被選中並安裝這些提示。
- 5. 進入ASDM主視窗並選擇Configuration頁籤。



6. 選中Ethernet 0 Interface並按一下Edit以配置外部介面。

Eisco ASDM 3 File Rules B	5.0 fo Sanch	PIX - 10.1.1.1 Options Tools Wizar	ds Help							_ 🗆 ×
G Home	Conf	iguration Monitoring	Back F	orward	Q Search	Refresh	Seve	? Help		CISCO SYSTEMS
Features	Co	infiguration > Features > Ir	iterfaces	- A -						
, Interfaces		· 当 41 K 1 M 1 Y	19 IB 19 F	31991						
<u>6</u> ,	Т	Interface	Name	Enabled	Security Level	IP Address	Subne	et Mask	Management Only	mu Add
Security Policy		Ethernet1	inside	Yes	100	10.1.1.1	255.255.	255.0	No 150	Edit
1		Ethernet0		No					No	Defete
423 Routing										
Building Blocks										
Bevice Administration										
Froperties		×								
		🗆 Enable traffic between	two or more inf	erfaces w	hich are c	onfigured with sa	ame securit	y levels		
							[
Wizards /					schibility	R	esei			
					ŀ	admin> N	A (15)	6	ne 🔒 📋 📔	6/05 4:26:49 PM UTC

7. 在Editing interface提示符下按一下OK。

🐞 Warning		×
<u>^</u>	Editing interface Ethernet0 may cause temporary or permanent loss of connectivity.	
	OK	

8. 輸入介面詳細資訊,完成後按一下**OK**。

📬 Edit Interface		×
Hardware Port:	Ethernet0	Configure Hardware Properties
🔽 Enable Interface	Dedicate this interface to manage	jement only
Interface Name:	outside	
Security Level:	0	
- IP Address		
 Use Static IP 	🔿 Obtain Address via DHCP	
IP Address:	99.99.99.1	
Subnet Mask:	255.255.255.0	
MTU:	1500	
Description:		
Description.		
	1	
	OK Cancel	Help

9. 在Changing an Interface提示符下按一下OK。



10. 按一下「Apply」以接受介面組態。該配置也將推到PIX上。此示例使用靜態路由。

Eisco ASDM 3 File Rulas B	5.0 foi learch	PIX - 10.1 Options	.1.1 Tools Wizards	Help								_ 🗆 ×
C Home	Conf	of the second se	Monitoring	O Back F	Orward	Q Search	R efresh	Save	? Help			CISCO SYSTEMS
Features	Co	riguration	i > Features > Interf	aces	-							
Interfaces		· <u>R</u> +	INCI∏IX 59		51991							
Ъ.	Т		Interface	Name	Enabled	Security Level	IP Address	Sub	net Mask	Management Only	MTU	Add
Security Policy		Ethernet1		inside	Yes	100	10.1.1.1	255.25	5.255.0	No	1500	Edit
14		Ethernetü		outside	Yes	0	89.99.99.1	265.25	5.255.0	No	1500	Delete
NAT												
VPN												
* <u>2</u> }												
Routing												
Building Blocks												
Device												
Administration												
Properties		•									•	
		🗆 Enable	traffic between two	or more int	erfaces wi	hich are co	onfigured with s	ame secu	rity levels			
									1			
Wizards /						Apply	R	eset				
							admin> N	IA (15)	6		3/16/05	4:28:18 PM UTC
,											_	

11. 在Features(功能)頁籤下按一下Routing,選中Static Route,然後按一下Add。

File Rulas Be	0 for PTX - 10.1.1.1 arch Options Tools Wizari	ds Help						_ 🗆 X
di Home	Configuration Monitoring	Back Form	vard Searc	h Refrest	n Save	? Help		Cisco Systems
Features Interfaces Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT Security Policy Security Policy Security Policy Security Policy Security Policy Security Policy Security Policy Security Policy Security Policy Security Policy Security Security Policy Security Policy Security Policy Security Securi	Configuration - Features - R Realing	Static Routing Static Route Specify static Interface	 Static Route Toutes. IP Address 	Netmask	Gateway IP	Metric	Tunneled	Add Edit Delete
Wizards K				Agg	ly	Reset		
				<admin></admin>	NA (15)	- B	N 🔤 3	18/05 4:44:49 PM UTC

12. <u>設定預設閘道,然後按一下**OK**。</u>

🚰 Add Static Route	×
Interface Name:	outside
IP Address:	0.0.0
Mask:	0.0.0.0
Gateway IP:	99.99.99.2
Metric	1
C Tunneled (Use	d only for default route)
ок	Cancel Help

	📬 Add Static Route	×
	Interface Name:	inside
	IP Address:	10.2.2.0
	Mask:	255.255.255.0
	Gateway IP:	10.1.1.2
	 Metric 	1
	C Tunneled (Used or	nly for default route)
	ок	ancel Help
14.		 安一下Apply。
	Gisco ASDM 5.0 for PIX - 10.1.1.1 File Rules Bearch Options Tools Wizards	Help
	Home Configuration Monitoring	C C Q Refresh Save Halp
	Features Configuration > Features > Rout ⊕ ⊕ ♥ III ⊕ & Pa	ing > Routing > Static Route 巴 縣 范 华

	金澤美 ■ 風 氷	19 18 19 18 18	19					
.	E-*&Routing	- Static Route						
Interfaces	Static Route	Specify stat	c routes.					
Security Policy	E COSPF	Interface	IP Address	Netmask	Gateway IP	litetric	Tunneled	And
34.	🖬 🍓 Multicast	outside	0.0.0.0	0.0.0.0	99.99.99.2	1	No	
NAT NAT	E B IGMP	inside	10.2.2.0	255.255.2	10.1.1.2	1	N/A	Edit
	면-mo-PIM 노·석출MRoute							Delete
Routing								
Building Blocks								
Device Administration								
Froperties								
				Ap	ply	Reset		
Wizards 🗠								
				<admin></admin>	NA (15)			3/16/05 4:46:48 PM UTC

_0×

Cisco Systems

15. 本示例使用NAT。選中Enable traffic through the firewall without address translation覈取方

塊,然後打	安一下 Ad	d以配置N	IAT規則。				
🔂 Cisco ASDM !	5.0 for PIX - 10.	1.1.1					
File Rules S	earch Options	Tools Wizar	ds Help				
💰 Home	of Configuration	Monitoring	Back Forward S	Q Q Jearch Refresh	Save Help	C	ISCO SYSTEMS
Features	Configuratio	n > Features > N	AT > Translation Rules				
	🔶 👷 🌾	1213	24 🛍 🕵 🛍 🕼 🛛				
Interfaces	🗆 Enabl	e traffic through 1	he firewall without address	translation			
<u>,</u>	Trans	lation Rules	C Translation Exemp	tion Rules			
Security Policy	Show Ru	ules for Interface	All Interfaces	▼ Show All			
NAT	Rule		Ortginal			Translated	Add
<u> </u>	Type	Interface	Source Network	Destination Network	Interface	Address	Edit
VPN					1		Delete
* <u>*</u> }							
Rotang							
Building Blocks							
3.							
Device Administration							
5.							
Properties							
	1. 2146	MAT JU	Demannic MAT De Dive	a Policy NAT 🛛 🖓 D	Anamic Dalicy M	<u>ت</u>	
	-i- Stau	111	eynamic rest i qui blas	er oney room i digit b	what the money re-	Manage Pools	
				Apply	Reset		
Wizards /							
				<admin> N^A</admin>	4 (15)	🍰 🔂 📔 🗎 🔂 3/1 6/05 4	31:48 PM UTC

16. 配置源網路(本示例使用any)。 然後按一下**Manage Pools**以定義PAT。

📬 Add Address Translati	ion Rule			×
O Use NAT	C Use Policy NAT			
Source Host/Netwo	ork			
	Interface:	inside	•	
	IP Address:	0.0.0.0	_	
	Mask:	0.0.0.0	T	
		0.0.0.0		
		Browse		
L				NAT Options
Translate Address or	n Interface: outsid	e 🔹		
- Translate Address	То			
C 1 Static	IP Address:		T	
E Redi	rect port	1		
(°) (°)	ICP Original port:	Translate	ed port:	
💿 🚻 Dynami	ic Address Pool:	same address 💌	Manage Poo	Is
Pool	ID	Address		
N/A	No address po	ol defined		
				-
	OK	Cancel	Help	

17. 選擇outside介面,然後按一下Add。

	: Global Add	ress Pools											×
Global	Address Po	ols											
Olahal	Adduces De				i- bl		. O al al a	T	-1-4:				
addres	Address Po ses.	ois are used	to config	jure Dyn	amic N	etwork	adan	ess Iran	siatio	n (NAT)		
	la ufa ca	DeallD			D. A. al al an								
inside	terrace	Pool ID		1	P Addre	ess(es))						
outsid	le										Add	J	
											Edit		
											elete	1	
											01010	1	
		OK	(0	ancel			Help					
此云例使田	田庙田公西												
			ΔТ										
	时使用기值 lobal Pool	们P地址的P Item	PAT。							_		-	×I
此小时使用 「 Add Gl	h使用介值 lobal Pool	们P地址的P Item	<u>PAT。</u>					-					×
Add G	时使用기面 lobal Pool	IIP地址的F Item	<u>PAT。</u>	T		Pool	ID:	1					×
Add Gl	前使用기值 lobal Pool face:	IIP地址的F Item outside	2ΑΤ。	•		Pool	ID:	1					×
Add Gl	前使用기值 lobal Pool face:	IIP地址的F Item outside	<u>PAT。</u>	•		Pool	ID:	1					×
Add Gi	前使用기區 lobal Pool face: Range	Item	<u>PAT。</u>	•		Pool	ID:	1					X
Add Gi Interf	前使用기面 lobal Pool face: Range Port Addre	Item Item outside ess Transla	Ntion (P/	T)		Pool	ID:	1					×
Add Gi Interf	Fig:H)Tig Tace: Range Port Addre Port Addre	Item Item outside ess Transla	tion (P/	T) AT) usi	ng the	Pool IP ad	ID:	1 s of the	inter	face			×
	iobal Pool face: Range Port Addre Port Addre	Item Item outside ess Transla	tion (P)	T) AT) usi	ng the	Pool IP ad	ID:	1 s of the	inter	face			×
Add Gi Interf	Fig:H) (G lobal Pool face: Range Port Addre Port Addre	Item Item outside ess Transla	tion (P)	T) AT) usi	ng the	Pool IP ad	ID:	1 s of the	inter	face			×
Add Gi Interf	iobal Pool face: Range Port Addre Port Addre	Item Item outside ess Transla ess Transla	tion (P/	T) AT) usi	ng the	Pool IP ad	ID: Idres	1 s of the	inter	face			×
	iobal Pool face: Range Port Addre Port Addre	Item Item outside ess Transla ess Transla	tion (P/	T) AT) usi	ng the	Pool	ID: Idres	1 s of the	inter	face			×
	iobal Pool face: Range Port Addre Port Addre	Item Item outside ess Transla ess Transla ess:	ition (P/	AT) AT) usi	ng the	Pool	ID:	1 s of the	inter	face			×
	iobal Pool face: Range Port Addre Port Addre	Item Item outside ess Transla ess Transla ess:	tion (P/	T) AT) usin	ng the	Pool	ID: Idres	1 s of the	inter	face			×
	iobal Pool face: Range Port Addre Port Addre	Item Item outside ess Transla ess Transla ess:	ition (P/	T) AT) usi	ng the	Pool	ID: Idres	1 s of the	inter	face			×
Add Gi Interf	iobal Pool	Item Item outside ess Transla ess Transla ess:	tion (P/	T) AT) usi	ng the	Pool IP ad	ID:	1 s of the	inter	face			×
	iobal Pool face: Range Port Addre Port Addre IP Addre	Item Item outside ess Transla ess Transla ess: Mask (opt	ition (P/	AT) AT) usir	ng the	Pool IP ad	ID:	1 s of the	inter	face			×

18. **配置PAT**時,按一下**OK**。

dresses.		ingure Dynamic Network A	duress franslation (NAT)
Interface	Pool ID	IP Address(es)	
nside utoido	1 00 00) 00 1/interface DATA	Add
uiside	1 99.99	.99.T(Intenace PAT)	
			Edit
			Delete

19. 按一下Add以設定靜態轉譯。

👩 Add Address 1	ranslation R	ule						x
Use NAT	. CU	se Policy NAT						
Source Ho	st/Network—							-
		Interface:	inside		-			
		IP Address:	0.0.0					
		Mask	0.0.0.0		T			
			1		_			
			Browse					
-							NAT Options	1
Translate Ad	dress on Inte	rface: outsid	ie 💌			_		_
- Translate /	Address To —							
0.1	Static	IP Address:		~	1			
	🗖 Redirect p	ort	1		_			
	C UDP	Original port:	Т	ranslated p	port:			
e 📲	Dynamic	Address Pool:	same addres	ss 💌	Manage	Pools		
	Pool ID		Addro	ess				
	1	99.99.99.1 (inter	face PAT)			-		
	1							
		014	1		Linin	1		
	_	UK	Cancel	<u> </u>	нер			

20. 在Interface(介面)下拉選單中選擇inside,然後輸入IP地址10.1.1.2,子網掩碼 255.255.255.255,選擇**Static**,然後在IP Address(IP地址)欄位中鍵入outside address **99.99.12**。完成後,按一下**OK**。

G Lloo MR					
Ose NA	т сц	Jse Policy NAT			
-Source He	ost/Network-				
		Interface:	inside	•	
		IP Address:	10.1.1.2		
		Mask:	255.255.255.255	-	
			Browse	_	
					NAT Options
Translate	0 datas a Ta				
Translate	Address To Static Redirect (IP Address:	99.99.99.12]	
Translate	Address To – Static Redirect (C UDP	IP Address: port Original port	99.99.99.12	port:	
Translate	Address To – Static Redirect (TCP C UDP Dynamic	IP Address: oort Original port Address Pool:	99.99.99.12 Translated p same address	port: Manage F	
Translate	Address To – Static Redirect (C UDP Dynamic Pool ID	IP Address: oort Original port Address Pool:	99.99.99.12 Translated ; same address Address	port: Manage F	2001s
Translate	Address To – Static Redirect (C UDP Dynamic	IP Address: port Original port Address Pool:	99.99.99.12 Translated same address Address	oort: Manage F	2001s

21. 按一下「Apply」以接受介面組態。該配置也將推到PIX上。



22. 在Features(功能)頁籤下選擇**Security Policy**(安全策略)以配置Security Policy(安全策略)規則。



23. 按一下「Add」以允許esp流量,然後按一下「OK」以繼續。

Action	Syslog
Select an action: permit	Default Syslog More Options
Apply to Traffic: incoming to src interface	Time Range Time Range: Not Applied 💌 New
Source Host/Network	Destination Host/Network
Interface: outside 💌	Interface: inside 💌
IP address: 99.99.99.2	IP address: 99.99.99.12
Mask: 255.255.255.255	Mask: 255.255.255.255
a a a a a a a a a a a a a a a a a a a	inside
99.99.99.2 Allo	inside 99.99.99.12 w traffic
99.99.99.2 Protocol and Service	99.99.99.12
Protocol and Service C TCP C UDP C ICMP © IP IP Protocol IP protocol: esp	Manage Service Groups
Protocol and Service C TCP C UDP C ICMP C IP IP Protocol IP protocol: esp Please enter the description below (optional):	Manage Service Groups
Protocol and Service C TCP C UDP C ICMP C IP IP Protocol IP protocol: Please enter the description below (optional): Access Rule to Allow ESP traffic	Manage Service Groups

24. 按一下「Add」以允許ISAKMP流量,然後按一下「OK」以繼續。

Edit Access Rule	×
Action	Syslog
Select an action: permit	Default Syslog More Options
Apply to Traffic: incoming to src interface	Time Range Time Range: Not Applied 💌 New
Source Host/Network	Destination Host/Network
	⑦ IP Address ○ Name ○ Group
Interface: outside	Interface: inside
IP address: 99.99.99.2	IP address: 99.99.99.12
Mask: 255.255.255.255 💌	Mask: 255.255.255.255 💌
99.99.99.2 outside	99.99.99.12
Protocol and Service	
C TCP C UDP C ICMP C IP Source Port	Manage Service Groups
• Service = 💌 isakmp	🕫 Service 😑 💌 any
C Service Group	C Service Group
Please enter the description below (optional);	
Access Rule to allow ISAKMP to host 99.99.99.12	×
OK Ca	ncel Help

25. 按一下Add以允許NAT-T的UDP埠4500流量,然後按一下OK以繼續。

Edit Access Rule	×
Action	Syslog
Select an action: permit	Default Syslog More Options
Apply to Traffic: incoming to src interface	Time Range
,	Time Range: Not Applied New
Source Host/Network	Destination Host/Network
Interface: outside	Interface: inside
IP address: 99.99.99.2	IP address: 99.99.99.12
Mask: 255.255.255 💌	Mask: 255.255.255.255 💌
99.99.99.2 Allow tr	99.99.99.12
Protocol and Service	
CICP CUDP CICMP CIP	Manage Service Groups
Source Port	Destination Port
• Service = 💌 4500	• Service = • any
C Service Group	C Service Group
Please enter the description below (optional):	
Access Rule to allow 4500 to host 99.99.99.12	A
	<u>_</u>
OK Can	Help

26. 按一下「Apply」以接受介面組態。該配置也將推到PIX上。

File Rules Se	.0 for PIX - earch Op	- 10.1.1.1 tons Toe	ols Wiza	ards Help							_ 🗆 X
S Home	original Configurat	ion Mo	itoring	Back	O Forward	Q Search	Q Refresh	Serve	? Help	Cts l	CO SYSTEMS
Features	Configu	ration > Fe	atures >	Security Polic	y > Access F	Rules					
Interfaces	Ac Show	🍯 🗹 cess Rule Rules for I	i 👔 i 🐰 s — C A Interface:	AA Rules (Al Interface	C Filter Rule	s C Ser Show All	vice Policy R	ules			
Security Policy	*	Rule Enabled	Action	Source HostiN	e letwork	Des Hos	tination bNetwork	Rule Applie To Traffic	ad Interface	Service	Add
NAT		2	~	🎱 any		🧼 any			inside (outbound)	<u>™</u> ip	Edit
1000 C	1	V	4	📕 99.99.99.	2	89.99. الع	99.12	🥬 incomin	g outside	æ≻esp	Delete
VPN	2		1	2 , 99,99,99,	2	S 99.991	99.12	🐥 incomir	g outside	III udp Src: isakmp	
Routing Building Blocks Device											
Properties											
		f House boo 🕾		Domited	5.0			0	Dhave Durate	<u>)</u>	
	1	MIOWIPam	2	o Denytran	inc .		-	•	snow Summary	O Show Detail	
Wizards 🕗				_	Арріу		Reset	A0	wanced		
						4	admin>	NA (15)	- 🛃 🔂	📩 3/1 6/05 4:54	4:58 PM UTC

27. <u>配置現在已完成。選擇File > Show Running Configuration in New Window</u>以檢視CLI配置。

 File
 Rules
 Search
 Options
 Tools
 Wizards
 Help

 Refresh ASDM with the Running Configuration on the Device
 Reset Device to the Factory Default Configuration...
 Reset Device to the Factory Default Configuration...

 Show Running Configuration in New Window...
 Save Running Configuration to Flash
 Save Running Configuration to TFTP Server...

 Save Running Configuration to Standby Unit
 Save Internal Log Buffer to Flash
 Print...

 Clear ASDM Cache
 Clear Internal Log Buffer
 Exit

<u>PIX防火牆配置</u>

PIX防火牆

```
pixfirewall# show run
: Saved
:
PIX Version 7.0(0)102
names
!
interface Ethernet0
nameif outside
 security-level 0
ip address 99.99.99.1 255.255.255.0
interface Ethernet1
nameif inside
 security-level 100
ip address 10.1.1.1 255.255.255.0
1
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
domain-name cisco.com
ftp mode passive
access-list outside_access_in remark Access Rule to
Allow ESP traffic
access-list outside_access_in
            extended permit esp host 99.99.99.2 host
99.99.99.12
access-list outside_access_in
           remark Access Rule to allow ISAKMP to host
99.99.99.12
access-list outside_access_in
            extended permit udp host 99.99.99.2 eq
isakmp host 99.99.99.12
access-list outside_access_in
           remark Access Rule to allow port 4500 (NAT-
T) to host 99.99.99.12
access-list outside_access_in
                    extended permit udp host 99.99.99.2
eq 4500 host 99.99.99.12
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
monitor-interface inside
monitor-interface outside
asdm image flash:/asdmfile.50073
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 0 0.0.0.0 0.0.0.0
static (inside,outside) 99.99.99.12 10.1.1.2 netmask
255.255.255.255
access-group outside_access_in in interface outside
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1
route outside 0.0.0.0 0.0.0.0 99.99.99.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
```

```
sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat
0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 10.1.1.3 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
telnet timeout 5
ssh timeout 5
console timeout 0
class-map inspection_default
match default-inspection-traffic
policy-map asa_global_fw_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
1
service-policy asa_global_fw_policy global
Cryptochecksum: 0a12956036ce4e7a97f351cde61fba7e
: end
```

PIX安全裝置和MPF(模組化策略框架)配置

使用命令**inspect ipsec-pass-thru** in MPF(Modular Policy Framework)而不是訪問清單,以便通過 PIX/ASA安全裝置傳遞IPsec流量。

此檢測配置為開啟ESP流量的針孔。如果存在轉發流,則允許所有ESP資料流,並且允許的最大連 線數沒有限制。不允許使用AH。預設情況下,ESP資料流的預設空閒超時設定為10分鐘。此檢查可 應用於可以應用其他檢查的所有位置,包括類和match命令模式。IPSec直通應用檢測提供了與IKE UDP埠500連線關聯的ESP(IP協定50)流量的便捷遍歷。它可避免冗長的訪問清單配置來允許 ESP流量,還可通過超時和最大連線提供安全性。使用class-map、policy-map和service-policy命令 可定義流量類、將inspect命令應用於該類,以及將策略應用於一個或多個介面。啟用時,inspect IPSec-pass-thru命令允許無限制ESP流量,超時為10分鐘,這是不可配置的。允許NAT和非NAT流 量。

```
hostname(config)#access-list test-udp-acl extended permit udp any any eq 500
hostname(config)#class-map test-udp-class
hostname(config-cmap)#match access-list test-udp-acl
hostname(config)#policy-map test-udp-policy
hostname(config-pmap)#class test-udp-class
hostname(config-pmap-c)#inspect ipsec-pass-thru
hostname(config)#service-policy test-udp-policy interface outside
```



本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供<u>註冊</u>客戶使用)支援某些show命令,此工具可讓您檢視<u>show</u>命令輸出的分析。

- show crypto ipsec sa 顯示第2階段安全關聯。
- show crypto isakmp sa 顯示第1階段安全關聯。
- show crypto engine connections active 顯示加密和解密的資料包。

<u>疑難排解</u>

本節提供的資訊可用於對組態進行疑難排解。

<u>路由器IPsec的故障排除命令</u>

- 註:發出debug<u>指令之前,請先參閱</u>有關Debug指令的重要資訊。
 - debug crypto engine 顯示加密的流量。
 - debug crypto ipsec 顯示第2階段的IPsec協商。
 - debug crypto isakmp 顯示第1階段的網際網路安全關聯和金鑰管理協定(ISAKMP)協商。

<u>清除安全關聯</u>

- clear crypto isakmp 清除網際網路金鑰交換(IKE)安全關聯。
- clear crypto ipsec sa 清除IPsec安全關聯。

PIX故障排除命令

<u>輸出直譯器工具(</u>僅供<u>註冊</u>客戶使用)支援某些**show**命令,此工具可讓您檢視<u>show</u>命令輸出的分析。

- 註:發出debug<u>指令之前,請先參閱</u>有關Debug指令的**重要**資訊。
 - logging buffer debugging 顯示正在建立並拒絕到通過PIX的主機的連線。資訊儲存在PIX日 誌緩衝區中,可以使用show log命令檢視輸出。
 - ASDM可用於啟用日誌記錄以及檢視日誌,如以下步驟所示。
 - 1. 選擇Configuration > Properties > Logging > Logging Setup > Enable Logging,然後按一下 Apply。

Elsco ASDM 5. File Rules Se	D for PTX - 10.1.1.1 arch Options Tools Wizards	Help	_ 🗆 X
Home C	onfiguration Montoring	O O Q O Q Back Forward Search Refiresh Save Help	CISCO SYSTEMS
Features	Configuration > Features > Prope	erties > Logging > Logging Setup	
Interfaces		ILE 용 행 역 Logging Setup F Enable logging on the faile	over standby unit
Security Policy	Options Options Options Options Options Options Options Options Options	Send debug messages as systogs Logging to Internal Buffer Specify the size of the internal buffer to which systogs will be saved. When the b	format oufferfills up, it will
STRN VPN	POHCP Services POHCP Services POHCP Server POHCP Relay POHCP Relay	Buffer Size: 4095 bytes You can choose to save the buffer contents before the buffer is overwritten.	
Routing Building Blocks	· @Failover - 일History Metrics 다면, IP Audit - 내일IP Audit Policy	Save Buffer To: FTP Server Configure FTP Settings F Flash Configure Flash Usage	
Device Administration	Event Lists	ASDM Logging Specify the size of the queue for syslogs intended for viewing in ASDM.	
Properties	- E-Logging Filters - E-Syslog Setup - E-Syslog Servers - SE-Mail Setup	Queue Size: 100	
Wizards X	RUNDPC Report	Apply Reset	24 805 5:02:20 DM I TO
			analog plastag FM OTC

2. 選擇Monitoring > Log Buffer > On Logging Level > Logging Buffer,然後按一下 View。



以下是日誌緩衝區的示例。

E	👌 Log Buf	fer	
	This scre	een shows syslog mess	ages in ASDM logging buffer as of now.
	Find text	in messages below:	Find Next
	Severity	Time	
	<u> </u>	Mar 16 2005 17:06:11	605005: Login permitted from 10.1.1.3/1247 to inside:10.1.1.1/https for user "enable
	<u>1</u> 6	Mar 16 2005 17:05:47	609001: Built local-host inside:10.1.1.2
	1.6	Mar 16 2005 17:05:47	609001: Built local-host outside:99.99.99.2
	<u>1</u> 6	Mar 16 2005 17:05:47	605005: Login permitted from 10.1.1.3/1220 to inside:10.1.1.1/https for user "enable
	1.6	Mar 16 2005 17:05:47	302013: Built inbound TCP connection 48 for inside:10.1.1.3/1220 (10.1.1.3/1220) t
	▲ 6	Mar 16 2005 17:05:47	302014: Teardown TCP connection 47 for inside:10.1.1.3/1219 to NP Identity Ifc:10.

Mar 16 2005 17:05:47 605005: Login permitted from 10.1.1.3/1221 to inside:10.1.1.1/https for user "enable"
 Mar 16 2005 17:05:47 302013: Built inbound TCP connection 50 for inside:10.1.1.3/1221 (10.1.1.3/1221) t

<u>4</u> 6	Mar 16 2005 17:05:47	302014: Teardown TCP connection 48 for inside:10.1.1.3/1220 to NP Identity Ifc:10.	
<u>*</u> 4	Mar 16 2005 17:05:47	106023: Deny udp src outside:99.99.99.2/4500 dst inside:99.99.99.12/4500 by acce	
<u>4</u> 6	Mar 16 2005 17:05:47	302015: Built inbound UDP connection 49 for outside:99.99.99.2/500 (99.99.99.2/5)	
<u>4</u> 6	Mar 16 2005 17:05:47	609001: Built local-host inside:10.1.1.2	
<u>4</u> 6	Mar 16 2005 17:05:47	609001: Built local-host outside:99.99.99.2	
<u>4</u> 6	Mar 16 2005 17:05:47	605005: Login permitted from 10.1.1.3/1220 to inside:10.1.1.1/https for user "enable	
<u>4</u> 6	Mar 16 2005 17:05:47	302013: Built inbound TCP connection 48 for inside:10.1.1.3/1220 (10.1.1.3/1220) t	
<u>4</u> 6	Mar 16 2005 17:05:47	302014: Teardown TCP connection 47 for inside:10.1.1.3/1219 to NP Identity Ifc:10.	
<u> </u>	Mar 16 2005 17:05:46	605005: Login permitted from 10.1.1.3/1219 to inside:10.1.1.1/https for user "enable	
<u>4</u> 6	Mar 16 2005 17:05:46	302013: Built inbound TCP connection 47 for inside:10.1.1.3/1219 (10.1.1.3/1219) t	
<u> </u>	Mar 16 2005 17:05:46	302014: Teardown TCP connection 46 for inside:10.1.1.3/1218 to NP Identity Ifc:10.	
<u> </u>	Mar 16 2005 17:05:46	605005: Login permitted from 10.1.1.3/1218 to inside:10.1.1.1/https for user "enable	
<u>4</u> 6	Mar 16 2005 17:05:46	302013: Built inbound TCP connection 46 for inside:10.1.1.3/1218 (10.1.1.3/1218) t	
<u> </u>	Mar 16 2005 17:05:46	302014: Teardown TCP connection 45 for inside:10.1.1.3/1217 to NP Identity Ifc:10.	
<u> </u>	Mar 16 2005 17:05:46	605005: Login permitted from 10.1.1.3/1217 to inside:10.1.1.1/https for user "enable	
<u> </u>	Mar 16 2005 17:05:46	302013: Built inbound TCP connection 45 for inside:10.1.1.3/1217 (10.1.1.3/1217) t	
<u> </u>	Mar 16 2005 17:05:46	302014: Teardown TCP connection 44 for inside:10.1.1.3/1216 to NP Identity Ifc:10.	
<u> </u>	Mar 16 2005 17:05:46	605005: Login permitted from 10.1.1.3/1219 to inside:10.1.1.1/https for user "enable	¥
•			
	Refresh Save	Log As Clear Close Help	

相關資訊

- IPsec協商/IKE通訊協定支援頁面
- <u>PIX支援頁</u>
- <u>PIX命令參考</u>
- <u>NAT支援頁面</u>
- <u>要求建議 (RFC)</u>
- 技術支援與文件 Cisco Systems