Esempio di configurazione del tunnel VPN IPsec PIX/ASA (versione 7.x e successive) con Network Address Translation

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Prodotti correlati Configurazione Esempio di rete Configurazioni Configurazione di PIX Security Appliance e elenco accessi Configurazione di PIX Security Appliance e MPF (Modular Policy Framework) Verifica Risoluzione dei problemi Comandi per la risoluzione dei problemi di IPSec del router Cancellazione delle associazioni di protezione Comandi per la risoluzione dei problemi per PIX Informazioni correlate

Introduzione

In questa configurazione di esempio viene mostrato un tunnel VPN IPsec attraverso un firewall che esegue NAT (Network Address Translation). Questa configurazione non funziona con Port Address Translation (PAT) se si usa il software Cisco IOS® versioni precedenti a 12.2(13)T esclusa. Questo tipo di configurazione può essere utilizzata per eseguire il tunnel del traffico IP. Questa configurazione non può essere utilizzata per crittografare il traffico che non attraversa un firewall, ad esempio gli aggiornamenti di routing o IPX. Il tunneling GRE (Generic routing Encapsulation) è una scelta più appropriata. Nell'esempio, i router Cisco 2621 e 3660 sono gli endpoint del tunnel IPsec che si uniscono a due reti private, con condotti o elenchi di controllo di accesso (ACL) sul PIX nel mezzo per consentire il traffico IPsec.

Nota: NAT è una traduzione di indirizzi uno a uno, da non confondere con PAT, che è una traduzione molti (all'interno del firewall)-a-uno. Per ulteriori informazioni sul funzionamento e la configurazione NAT, fare riferimento a <u>Verifica del funzionamento NAT e risoluzione dei problemi</u> <u>NAT di base</u> o a <u>Come funziona NAT</u>.

Nota: IPsec con PAT potrebbe non funzionare correttamente perché il dispositivo endpoint del

tunnel esterno non è in grado di gestire più tunnel da un indirizzo IP. Contattare il fornitore per determinare se i dispositivi di endpoint del tunnel funzionano con PAT. Inoltre, nel software Cisco IOS versione 12.2(13)T e successive, la funzione di trasparenza NAT può essere utilizzata per PAT. Per ulteriori informazioni, vedere <u>Trasparenza NAT IPSec</u>. per ulteriori informazioni su queste funzionalità nel software Cisco IOS versione 12.2(13)T e successive. IOS versione 12.2(13)T e successive.

Nota: prima di aprire una richiesta di assistenza con il supporto tecnico Cisco, fare riferimento alle <u>domande frequenti NAT</u>, che contengono molte risposte alle domande frequenti.

Per ulteriori informazioni su come configurare il tunnel IPSec attraverso il firewall con NAT sulla versione 6.x e precedenti, fare riferimento a <u>Configurazione di un tunnel IPSec attraverso il firewall</u> <u>con NAT su PIX.</u>

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- Software Cisco IOS release 12.0.7.T (fino al software Cisco IOS release 12.2(13)T escluso)Per le versioni più recenti, fare riferimento a <u>Trasparenza NAT IPSec</u>.
- Cisco 2621 router
- Cisco 3660 router
- Cisco PIX serie 500 Security Appliance con versione 7.x e successive.

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.

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

Prodotti correlati

Questo documento può essere usato anche con Cisco serie 5500 Adaptive Security Appliance (ASA) con software versione 7.x e successive.

Configurazione

In questa sezione vengono presentate le informazioni che è possibile utilizzare per configurare le

funzionalità descritte nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo <u>strumento di</u> ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:





Nel documento vengono usate queste configurazioni:

- <u>Configurazione di Cisco 2621</u>
- Configurazione di Cisco 3660
- Configurazione di PIX Security Appliance e elenco accessiConfigurazione ASDM (Advanced Security Device Manager GUI)Configurazione CLI (Command Line Interface)
- <u>Configurazione di PIX Security Appliance e MPF (Modular Policy Framework)</u>

```
Cisco 2621
Current configuration:
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
 Т
hostname goss-2621
 !
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
isdn voice-call-failure 0
cns event-service server
!--- 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
 !
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
 Т
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
 !
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
crypto ipsec transform-set myset esp-des esp-md5-hmac
 I
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
 Т
 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
 !
 interface Ethernet3/1
 no ip address
 no ip directed-broadcast
 interface Ethernet4/0
 no ip address
 no ip directed-broadcast
 shutdown
 1
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
 !--- 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
```

Configurazione di PIX Security Appliance e elenco accessi

Configurazione di ASDM 5.0

Completare questa procedura per configurare PIX Firewall versione 7.0 con ASDM.

1. Collegare la console al PIX. Da una configurazione ripristinata ai valori predefiniti, usare le

istruzioni interattive per abilitare l'**interfaccia grafica di Advanced Security Device Manager (ASDM)** per la gestione dei PIX dalla workstation 10.1.1.3.

- 2. Da Workstation 10.1.1.3, aprire un browser Web e utilizzare ADSM (in questo esempio, https://10.1.1.1).
- 3. Selezionare **Yes** (Sì) nelle richieste del certificato e accedere con la password enable configurata nella <u>configurazione di bootstrap ASDM di PIX Firewall</u>.
- 4. Se è la prima volta che ASDM viene eseguito sul PC, viene richiesto se utilizzare ASDM Launcher o se utilizzare ASDM come app Java.Nell'esempio, l'Utilità di avvio ASDM è selezionata e installa questi prompt.
- 5. Passare alla finestra Home ASDM e selezionare la scheda

Configurazione.	
📬 Cisco ASDM 5.0 for PTX - 10.1.1.1	
File Roles Bearch Options Tools Wizards Help	
Home Configuration Monitoring Back Forward Search	Refresh Save Help
- Device Information	- Interface Status
General License	Interface IP Address/Mask Line Link Current Kops
Host Name: pivfirewall rise nom	inside 10.1.1.1/24 O up O up 1
P0(Version: 7.0(0)102 Device Uptime: 0d 0h 3m 53s	
ASDM Version: 5.0(0)73 Device Type: PIX 515E	
Firewall Mode: Routed Context Mode: Single	
Total Flash: 16 MB Total Nemory: 64 MB	Palast an interface to view input and output Vana
	- Traffic Status
IKE Tunnels: 0 IPSec Tunnels: 0	Connections Per Second Usage
System Resources Status	4
CPU CPU Usage (percent)	0.5
00	10/20:18
01 32	UDP: 0 TCP: 0 Total: 0
10 20.28 10.20.18	'inside' Interface Traffic Usage (Kbps)
Memory — Memory Usage (MB)	2
84	1.5
2016 32 ***	
10:20:28 10:20:18	Input Khos: 0 Output Khos: 1
Latest 4SDM System Messanes	Cordinare ASDM Suring Fillers
Syslog Disabled	
Device configuration loaded successfully.	<admin> NA (15) 🔡 🔐 🔓 3/16/05 4:26:28 PM UTC</admin>

6. Per configurare l'interfaccia esterna, evidenziare **Ethernet 0 Interface** e fare clic su **Edit** (Modifica).

Ella Prilas Ba	0 for PIX - 10.1.1.1 arch: Ontions: Tools: Wizard	is Hain					_0×
Home G	Configuration Monitoring	Back Forwa) Q ard Search	Refresh S			Cisco Systems
Features	Configuration > Features > In	terfaces					
Interfaces	● <u>♀</u> ¥ ⊠ ⅓ ⅔		9 1				
<u>b</u> ,	Interface	Name En	abled Security Level	IP Address	Subnet Mask	Management Only MTU	Add
Security Policy	Ethernet1	inside 1	Yes 100	10.1.1.1	255.255.255.0	No 1500	Edit
1	Ethernet0		No			No	Delete
VPN							
423 Routing							
Real Control of Contro							
Device Administration							
Properties						•	
	Enable traffic between	two or more interfa	ces which are co	onfigured with sar	me security levels		
			And and an				
Wizards - 4			Addb10	Re	set		
	,		*	admin> NA	(15)	🔒 3/1 6/05	4:26:48 PM UTC

7. Fare clic su OK al prompt dell'interfaccia di





8. Immettere i dettagli dell'interfaccia e al termine fare clic su OK.

🔂 Edit Interface		×
Hardware Port:	Ethernet0	Configure Hardware Properties
🔽 Enable Interface	🗖 Dedicate this interface to manag	gement 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:		
	OK Cancel	Help

9. Fare clic su **OK** al prompt Modifica di un'interfaccia.



10. Per accettare la configurazione dell'interfaccia, fare clic su **Apply** (Applica). La configurazione viene inoltre inserita nel PIX. In questo esempio vengono utilizzate route statiche.

Eisco ASDM 5 File Rules Bi	i.O fo sarch	PTX - 10.1.1.1 Options Tool	s Wizards	Help								_ 🗆 🛛
G Home	Conf	a Mont	toring	O Back Fi	Orward	Q Search	Refresh	Serve	? Help			CISCO SYSTEMS
Features	Ce	nfiguration > Fea	tures > Interf	aces	- A-		_			_		
, Interfaces		! <u>≗</u> # ⊠	TIY AN	10. 10. 10	51691							
<u>e</u> .		Interfa	ice	Name	Enabled	Security Level	IP Address	Su	bnet Mask	Management Only	MTU	Add
Security Policy		Ethernet1		Inside	Yes	100	10.1.1.1	255.2	255.255.0	No	1500	Edit
NAT.		Ethernetü		outside	Yes	0	99.99.99.1	265.2	255.255.0	No	1500	Delete
423 Routing												
Building Blocks												
Device Administration												
Properties		×[•	
		🗆 Enable traffic	between two	or more int	erfaces wi	hich are c	onfigured with s	ame ser	urity levels			
						Apply	R	eset	1			
Wizards - ^												
							<admin> N</admin>	A (15)			3/16/05	4:28:18 PM UTC

11. Fare clic su **Routing** nella scheda Features, evidenziare **Static Route**, quindi fare clic su **Add**.

Elsco ASDM 5. File Rules Be	0 for PTX - 10.1.1.1 arch Options Tools Wizari	ts Help				_0×
di Home	Configuration Monitoring	G O Back Forward	Q Q Search Refrest	Save He	?	CISCO SYSTEMS
Features	Configuration - Features - R	outing > Routing > Stati PA PA PA PA PA PA	c Route	Gateway IP Me	tric Tunneled	Add Edit Delete
Wizards /			A0;	ly R	eset	
			<admin></admin>	NA (15)	🍰 🔂 🛛 🖻	3/16/05 4:44:48 PM UTC

12. Configurare il gateway predefinito e fare clic su

	🗲 Add Static Route	×
	Interface Name:	outside
	IP Address:	0.0.0.0
	Mask:	0.0.0.0
	Gateway IP:	99.99.99.2
	Metric	1
	C Tunneled (Used	only for default route)
OK.	ок	Cancel Help

13. Fare clic su Add (Aggiungi) e aggiungere le route alle reti



14. Verificare che siano configurate le route corrette e fare clic su

Applica.



15. Nell'esempio viene utilizzato NAT. Rimuovere la casella di controllo Abilita traffico attraverso il firewall senza conversione degli indirizzi e fare clic su Add per configurare la regola



 Configurare la rete di origine (nell'esempio riportato viene utilizzato any). Quindi, fare clic su Gestisci pool per definire il percorso.

	ransiation R	ule	
O Use NAT	οu	se Policy NAT	
-Source Hos	t/Network		
		Interface: IP Address: Mask:	Inside 0.0.0 0.0.0 Browse
			NAT Options
Translate Add	iress on Inter	rface: outsid	de 🔽
-Translate A	ddress To —		
0 1	Static	IP Address:	
יוי ס ו	Static Redirect p	IP Address; ort	
ייי ס ו ן	Static Redirect p © TCP © UDP	IP Address: ort Original port:	Translated port:
• + •	Static Redirect p © TCP © UDP Dynamic	IP Address: ort Original port: Address Pool:	Translated port:
• + • [• ¶	Static Redirect p C TCP C UDP Dynamic Pool ID	IP Address: ort Original port: Address Pool:	Translated port: Same address Manage Pools Address
C +	Static Redirect p C TCP C UDP Dynamic Pool ID N/A	IP Address: ort Original port: Address Pool: No address poo	Translated port: Same address Manage Pools Address ol defined
с ф с ¶	Static Redirect p C TCP C UDP Dynamic Pool ID N/A	IP Address: ort Original port: Address Pool: No address poo	Translated port: Same address Manage Pools Address ol defined
с ф с	Static Redirect p TCP C UDP Dynamic Pool ID N/A	IP Address: ort Original port: Address Pool: No address poo	Translated port: same address Manage Pools Address ol defined
C +	Static Redirect p TCP C UDP Dynamic Pool ID N/A	IP Address: ort Original port: Address Pool: No address poo	Translated port: Same address Manage Pools Address

17. Selezionare l'interfaccia **esterna** e fare clic su **Aggiungi**.

🔂 Manage Global A	ddress Pools			×
Global Address	Pools			
Global Address addresses.	Pools are used	to configure Dynamic Net	work Address Transl	ation (NAT)
Interface	Pool ID	IP Addres	s(es)]
inside				Add
				Edit
				Delete
1				
	OK	Cancel	Help	

In questo esempio viene utilizzato un PAT con l'indirizzo IP dell'interfaccia.

🕵 Add Global Pool Item	×
Interface: outside Pool ID: 1	
C Range	
C Port Address Translation (PAT)	
Port Address Translation (PAT) using the IP address of the interface	
IP Address:	
Network Mask (optional):	
OK Cancel Help	

18. Fare clic su **OK** quando la parte è configurata.

🚰 Manage Global Ado	iress Pools					×
Global Address P	ools					
Global Address Po addresses.	ools are used	to config	jure Dynamic Netw	ork Address Trans	lation (NAT)	
Interface	Pool ID		IP Address(es)		
inside outside	1	99.99.99	3.1 (interface PAT)		Add	
					Edit	
					Delete	
	ок		Cancel	Help		

19. Per configurare la traduzione statica, fare clic su Add (Aggiungi).

🔂 Add Address 1	ranslation R	ule				x
Use NAT	. CU	se Policy NAT				
Source Ho	st/Network—					
		Interface:	inside	<u> </u>		
		IP Address:	0.0.0.0			
		Mask	0.0.0.0	v		
			Browse			
				[NAT Options	
Translate Ad	dress on Inte	rface: outsid	e 💌			
Translate /	Address To —					
⊂ ili	Static	IP Address: ort		*		
	C UDP	Original port:	Translated	port		
• 🚻	Dynamic	Address Pool:	same address 💌	Manage Pools.		
	Pool ID		Address			
	1	99.99.99.1 (inter	face PAT)			
	1					
	[ок	Cancel	Help		

20. Selezionare dall'interno dell'elenco a discesa Interfaccia, quindi immettere l'indirizzo IP 10.1.1.2, la subnet mask 255.255.255.255, scegliere Statico e nel campo Indirizzo IP digitare l'indirizzo esterno 99.99.12. Al termine, fare clic su OK.

👩 Add Address T	ranslation R	ule					
• Use NAT	· •	Jse Policy NAT					
Source Ho	st/Network-						
		Interface: IP Address:	inside 10.1.1.2		•		
		Mask:	255.255.255	5.255	*		
			Browse				
						NA	T Options
Translate Ad	dress on Inte	rface: outsic	ie 💌				
Translate #	Address To						
· · ·	Static	IP Address:	99.99.99.12	-]		
	🗖 Redirect p	oort					
	C UDP	Original port:		Translated p	oort:		
c 41	Dynamic	Address Pool:	same addr	ess 🔻	Manage P	Pools	
	Pool ID		Ado	iress		_	
		ОK	Canc	el	Help		

21. Fare clic su **Apply** (Applica) per accettare la configurazione dell'interfaccia. La configurazione viene inoltre inserita nel PIX.



 Per configurare la regola dei criteri di sicurezza, selezionare Criteri di sicurezza nella scheda Funzionalità.



23. Per continuare, fare clic su **Add** (Aggiungi) per consentire il traffico esp e fare clic su **OK**.

Add Access Rule	×
Action	Syslog
Select an action: permit	Default Syslog More Options
Apply to Traffic: incoming to src interface	Time Range New
Source Host/Network	Destination Host/Network
	C IP Address C Name C 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 Allow 1	99.99.99.12
Protocol and Service	
C TCP C UDP C ICMP @ IP	Manage Service Groups
IP protocol: esp	
Please enter the description below (optional):	
Access Rule to Allow ESP traffic	×
ок Са	ancel Help

24. Per autorizzare il traffico ISAKMP, fare clic su **Add** (Aggiungi), quindi su **OK**.

📬 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 I 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 💌
99.99.99.2 outside	99.99.99.12
Protocol and Service	
C TCP © UDP C ICMP C IP Source Port © Service = I isakmp C Service Group	Manage Service Groups Destination Port Service = any Service Group
Please enter the description below (optional):	
Access Rule to allow ISAKMP to host 99.99.99.12	A 7
OK Can	cel Help

25. Fare clic su **Add** (Aggiungi) per consentire il traffico UDP porta 4500 per NAT-T e fare clic su **OK** per continuare.

🚰 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 INew
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
99.99.99.2	source Interface
Protocol and Service	
C TCP © UDP C ICMP C IP Source Port © Service = • 4500 C Service Group	Manage Service Groups Destination Port Service = any Service Group
Please enter the description below (optional):	
Access Rule to allow 4500 to host 99.99.99.12	
OK Can	Help

26. Per accettare la configurazione dell'interfaccia, fare clic su **Apply** (Applica). La configurazione viene inoltre inserita nel PIX.

File Rules Sea	for PIX arch Op	-10.1.1.1 tions Too	is Wiz	ards Help								_ 🗆 X
Home C	anfigura	tion Mo	ji Nitoring	O Back	O Forward	Q Search	Q Refresh	Save	? Helip		Cas	CO SYSTEMS
Features	Configu	ration > Fe	atures >	Security Policy	y > Access R	lules						
	* *	¥ 🗹	1 3	i 🔁 🛍 🖺	iii 🎯 I							
Nerfaces	Ac Ac Ac Ac	cess Rule	s CA	AA Rules 🤇	Filter Rule	s C Ser	vice Policy R	ules				
	Show	Rules for I	nterrace	: All Interface	s 🔻	Show All						
Security Policy	*	Rule Enabled	Action	Source HostiNe	etwork	Des Hos	tination bNetwork	Rule App To Tra m	plied 1	nterface	Service	Add
NAT NAT		V	¥	🍅 any		🧼 any			insi (out	de baund)	™ ip	Edit
02	1	V	*	📕 99.99.99.2	2	📕 99.99.9	9.12	📌 incon	ning outs	side	<u>⊐r</u> ∕esp	Delete
VPN	2		1	S 99.99.99.2	2	🛋 99.99.1	9.12	루 incon	ning outs	side	≌udp Src: isakmp	
Routing Routing Building Blocks Device Administration Froperties												
	•								-		•	
	×	Allow traffic	2	O Deny traffi	c				Show 5	Summary	C Show Detail	
Wizards 🗠				_	Apply		Reset		Advanced			
						<	admin>	NA (15)	1 🍰		🔒 3/1 6/05 4:54	4:58 PM UTC

27. Configurazione completata.Per visualizzare la configurazione CLI, scegliere **File > Mostra configurazione corrente** in **una nuova**



PIX Firewall

```
pixfirewall# show run
: Saved
PIX Version 7.0(0)102
names
1
interface Ethernet0
nameif outside
 security-level 0
ip address 99.99.99.1 255.255.255.0
1
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
mqcp-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
1
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
```

Configurazione di PIX Security Appliance e MPF (Modular Policy Framework)

Anziché utilizzare l'elenco degli accessi, usare il comando **inspect ipsec-pass-thru** in MPF(Modular Policy Framework) per passare il traffico IPsec attraverso le appliance di sicurezza PIX/ASA.

Questa ispezione è configurata per aprire i fori per il traffico ESP. Tutti i flussi di dati ESP sono consentiti quando esiste un flusso in avanti e non esiste alcun limite al numero massimo di connessioni consentite. AH non è permesso. Il timeout di inattività predefinito per i flussi di dati ESP è impostato per impostazione predefinita su 10 minuti. Questa ispezione può essere applicata in tutti i punti in cui è possibile eseguire altre ispezioni, incluse le modalità di comando class e match. L'ispezione delle applicazioni pass-through IPSec consente di attraversare agevolmente il traffico ESP (protocollo IP 50) associato a una connessione con porta UDP IKE 500. Evita la configurazione di lunghi elenchi degli accessi per consentire il traffico ESP e fornisce anche la sicurezza con timeout e connessioni massime. Utilizzare i comando inspect alla classe e applicare il criterio a una o più interfacce. Se abilitato, il comando **inspect IPSec-pass-thru** consente un traffico ESP illimitato con un timeout di 10 minuti, che non è configurabile. È consentito il traffico NAT e non NAT.

```
hostname(config)#access-list test-udp-acl extended permit udp any any eq 500
hostname(config)#class-map test-udp-class
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
```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show sono supportati dallo** <u>strumento Output Interpreter (solo utenti registrati); lo</u> <u>strumento permette di visualizzare un'analisi dell'output del comando</u> **show**.

- show crypto ipsec sa: visualizza le associazioni di sicurezza della fase 2.
- show crypto isakmp sa: visualizza le associazioni di sicurezza della fase 1.
- show crypto engine connections active: visualizza i pacchetti crittografati e decrittografati.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi di IPSec del router

Nota: consultare le <u>informazioni importanti sui comandi di debug</u> prima di usare i comandi di **debug**.

- debug crypto engine: visualizza il traffico crittografato.
- debug crypto ipsec: visualizza le negoziazioni IPsec della fase 2.
- **debug crypto isakmp**: visualizza le negoziazioni ISAKMP (Internet Security Association and Key Management Protocol) della fase 1.

Cancellazione delle associazioni di protezione

- clear crypto isakmp: cancella le associazioni di protezione IKE (Internet Key Exchange).
- clear crypto ipsec sa: cancella le associazioni di sicurezza IPsec.

Comandi per la risoluzione dei problemi per PIX

Alcuni comandi **show sono supportati dallo** <u>strumento Output Interpreter (solo utenti registrati); lo</u> <u>strumento permette di visualizzare un'analisi dell'output del comando</u> **show**.

Nota: consultare le <u>informazioni importanti sui comandi di debug</u> prima di usare i comandi di **debug**.

• logging buffer debugging: visualizza le connessioni stabilite e negate agli host che passano

attraverso il PIX. Le informazioni vengono memorizzate nel buffer di registro PIX e l'output può essere visualizzato con il comando **show log**.

- ASDM può essere utilizzato per abilitare il log e anche per visualizzare i log, come mostrato in questa procedura.
- 1. Scegliete Configurazione > Proprietà > Log > Impostazione log > Abilita log e fate clic su Applica.

🔁 Cisco ASDM 5.0	D for PIX - 10.1.1.1	
File Rules Sea	arch Options Tools Wizards I	telp
G Home C	Configuration Monitoring E	Cisco Systems ack Forward Search Retriesh Save Help Cisco Systems
Features	Configuration > Features > Property	lies > Logging > Logging Setup
Electroces Security Policy NAT		Image: Section of the section of th
VRU VRU Routing	POHCP Server POHCP Relay POHCP Relay POHCP Relay Pohce Relay	Buffer Size: 4096 bytes You can choose to save the buffer contents before the buffer is overwritten. Save Buffer To: FTP Server Configure FTP Settings
Building Blocks Device Administration		ASDM Logging Specify the size of the queue for syslogs intended for viewing in ASDM. Queue Size: 100
Wizards /	RINEPC Repar	Apply Reset
Wizards /		admin> NA (15) 🖧 🔂 👌 3/1 8/05 5:03:38 PM UTC

2. Scegliere Controllo > Log > Buffer di log > Al livello di log > Buffer di log, quindi fare clic su Visualizza.



Questo è un esempio di buffer di registro.

🔂 Log Bufl	fer					
This scre	en shows syslog mess:	ages in ASDM logging buffer as of now.				
Find text	in messages below:	Find Next				
Severity	Time	<u> </u>				
4 6	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>4</u> 6	Mar 16 2005 17:05:47	609001: Built local-host inside:10.1.1.2				
▲ 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>▲</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>∔</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>1</u> 6	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				
<u>1</u> 6	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				
1.6	Mar 16 2005 17:05:47	302014: Teardown TCP connection 48 for inside:10.1.1.3/1220 to NP Identity Ifc:10.				
4 4 6	Mar 16 2005 17:05:47	106023: Deny uop src outside:99.99.99.2/4500 dst inside:99.99.99.12/4500 by acce 202015: Ruittinbound UDB connection 40 for outside:90.00.00.2/500 /00.00.2/50				
4 6	Mar 16 2005 17:05:47 Mar 16 2005 17:05:47	S02015. Built Insound ODP connection 49 for builside.99.99.99.2/500 (99.99.99.2/5)				
6	Mar 16 2005 17:05:47	609001: Built local-host rutside:99.99.99.2				
4.6	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				
A 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>1</u> 6	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				
▲ 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>4</u> 6	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> 6	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> </u>	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				
1.6	Mar 16 2005 17:05:46	302014: Teardown TCP connection 45 for inside:10.1.1.3/1217 to NP Identity Ifc:10.				
16	Mar 16 2005 17:05:46	505005: Login permitted from 10.1.1.3/1217 to inside:10.1.1.1/https for user "enable				
1.6	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				
10	Mar 16 2005 17:05:46 Mar 16 2005 17:05:46	302014: Learnown TCP connection 44 for inside:10.1.1.3/1216 to NP identity ffc:10.				
1	Mar 10 2005 17.05.46	Busbuss Login permitted from To.T.T.S/T219 to Inside.To.T.T.T/https for user "enable"				

Refresh

Clear

Close

Help

Informazioni correlate

• Pagina di supporto per la negoziazione IPsec/i protocolli IKE

Save Log As...

- Pagina di supporto PIX
- Riferimenti per i comandi PIX
- Pagina di supporto NAT
- RFC (Requests for Comments)
- Documentazione e supporto tecnico Cisco Systems