PIX/ASA (Version 7.x und höher) IPsec-VPN-Tunnel mit Network Address Translation -Konfigurationsbeispiel

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Zugehörige Produkte Konfigurieren Netzwerkdiagramm Konfigurationen Konfiguration der PIX Security Appliance und Zugriffslisten PIX Security Appliance- und MPF-Konfiguration (Modular Policy Framework) Überprüfen Fehlerbehebung Befehle zur Fehlerbehebung für Router IPsec Löschen von Sicherheitszuordnungen Befehle zur Fehlerbehebung für PIX Zugehörige Informationen

Einführung

Diese Beispielkonfiguration veranschaulicht einen IPsec-VPN-Tunnel durch eine Firewall, die die Network Address Translation (NAT) durchführt. Diese Konfiguration funktioniert nicht mit Port Address Translation (PAT), wenn Sie Cisco IOS® Software Releases vor und ohne 12.2(13)T verwenden. Dieser Konfigurationstyp kann zum Tunnel von IP-Datenverkehr verwendet werden. Diese Konfiguration kann nicht zum Verschlüsseln von Datenverkehr verwendet werden, der nicht über eine Firewall geleitet wird, z. B. IPX oder Routing-Updates. Generic Routing Encapsulation (GRE)-Tunneling ist eine geeignetere Option. In diesem Beispiel sind die Cisco 2621- und 3660-Router die IPsec-Tunnel-Endpunkte, die zwei private Netzwerke miteinander verbinden, wobei dazwischen Leitungen oder Zugriffskontrolllisten (ACLs) auf dem PIX angeordnet sind, um den IPsec-Datenverkehr zuzulassen.

Hinweis: NAT ist eine Eins-zu-Eins-Adressenumwandlung, die nicht mit PAT verwechselt werden darf. Hierbei handelt es sich um eine viele (innerhalb der Firewall)-zu-Eins-Übersetzung. Weitere Informationen zum NAT-Betrieb und zur NAT-Konfiguration finden Sie unter <u>Verifying NAT</u> <u>Operation and Basic NAT Troubleshooting (NAT-Betrieb und grundlegende NAT-Fehlerbehebung)</u> oder <u>How NAT Works (Funktionsweise von NAT)</u>.

Hinweis: IPsec mit PAT funktioniert möglicherweise nicht ordnungsgemäß, da das Endgerät des externen Tunnels nicht mehrere Tunnel von einer IP-Adresse aus verarbeiten kann. Wenden Sie sich an Ihren Anbieter, um festzustellen, ob die Tunnel-Endgeräte mit PAT kompatibel sind. Darüber hinaus kann in der Cisco IOS-Softwareversion 12.2(13)T und höher die NAT-Transparenzfunktion für PAT verwendet werden. Weitere Informationen finden Sie unter <u>IPSec NAT Transparency</u>. Unter <u>Support für IPSec ESP Through NAT</u> finden Sie weitere Informationen zu diesen Funktionen in Cisco IOS Software Release 12.2(13)T und höher.

Hinweis: Bevor Sie ein Ticket beim technischen Support von Cisco eröffnen, lesen Sie die <u>FAT-</u> <u>Fragen</u>, die viele Antworten auf häufige Fragen enthält.

Unter Konfigurieren eines IPSec-Tunnels durch eine Firewall mit NAT finden Sie weitere Informationen zur Konfiguration eines IPsec-Tunnels durch Firewall mit NAT auf PIX, Version 6.x oder früher.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS Software Release 12.0.7.T (bis zu, aber nicht einschließlich Cisco IOS Software Release 12.2(13)T)Neuere Versionen finden Sie unter <u>IPSec NAT Transparency</u>.
- Cisco 2621-Router
- Cisco Router 3660
- Cisco Security Appliance der Serie PIX 500 mit 7.x und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Zugehörige Produkte

Dieses Dokument kann auch mit der Cisco Adaptive Security Appliance (ASA) der Serie 5500 mit der Softwareversion 7.x und höher verwendet werden.

Konfigurieren

In diesem Abschnitt finden Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Um weitere Informationen zu den Befehlen zu erhalten, die dieses Dokument verwendet, verwenden Sie das <u>Command Lookup Tool</u> (<u>nur registrierte</u> Kunden).

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:





Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Konfiguration des Cisco 2621
- Konfiguration des Cisco 3660
- Konfiguration der PIX Security Appliance und ZugriffslistenKonfiguration der Advanced Security Device Manager GUI (ASDM)CLI-Konfiguration (Command Line Interface)
- PIX Security Appliance- und MPF-Konfiguration (Modular Policy Framework)

Cisco 2621

```
Current configuration:
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
 I
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
 1
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
!
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
```

```
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
 !
hostname goss-3660
 1
ip subnet-zero
 !
cns event-service server
 1
!--- The IKE policy. crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 99.99.99.12
 1
crypto ipsec transform-set myset esp-des esp-md5-hmac
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
 1
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
interface FastEthernet0/1
 ip address 10.3.3.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
 duplex auto
 speed auto
 !
```

```
interface Ethernet3/0
 no ip address
 no ip directed-broadcast
 shutdown
 I
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
!
!--- 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
1
line con 0
 transport input none
line aux 0
line vty 0 4
!
end
```

Konfiguration der PIX Security Appliance und Zugriffslisten

ASDM 5.0-Konfiguration

Führen Sie diese Schritte aus, um PIX Firewall Version 7.0 mit ASDM zu konfigurieren.

- 1. In den PIX einstecken. Verwenden Sie nach einer gelöschten Konfiguration die interaktiven Aufforderungen, um die Advanced Security Device Manager GUI (ASDM) für die Verwaltung des PIX von der Workstation 10.1.1.3 zu aktivieren.
- 2. Öffnen Sie auf Workstation 10.1.1.3 einen Webbrowser, und verwenden Sie ADSM (in diesem Beispiel https://10.1.1.1).
- 3. Wählen Sie **Yes (Ja)** auf den Zertifikatsaufforderungen aus, und melden Sie sich mit dem aktivierten Kennwort an, wie in der <u>ASDM-Bootstrap-Konfiguration der PIX-Firewall</u> konfiguriert.
- 4. Wenn ASDM zum ersten Mal auf dem PC ausgeführt wird, werden Sie aufgefordert, ASDM Launcher zu verwenden oder ASDM als Java-Anwendung zu verwenden. In diesem Beispiel wird der ASDM Launcher ausgewählt und installiert.
- 5. Fahren Sie mit dem ASDM Home-Fenster fort, und wählen Sie die Registerkarte Configuration (Konfiguration)

aus.	
Sisce ASDM 5.0 for PIX - 10.1.1.1	
File Rules Search Options roots Wizards Help	
Home Configuration Monitoring Back Forward Sear	Ch Refresh Save Hap Cisco Systems
- Device Information	Interface Status
General License	Interface IP Address/Mask Line Link Current Kops
Host Name: pixfirewall.cisco.com	inside 10.1.1.1/24 O up O up 1
POCVersion: 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	
	Select an interface to view input and output Kbps
VPN Status	Traffic Status
IKE Tunnels: U IPSec Tunnels: U	Connections Per Second Usage
System Resources Status	1
CPU Usage (percent)	0.5
08	10 20 18
03 32	UDP: 0 TCP: 0 Total: 0
10 20 28	Particle Industry Territor Manual
	Inside Intenace Tranic Gage (Kops)
Memory Usage (MB)	1.5
48	1
2008 321	16/20:18
16:20:28 15:20:18	Input Kaps: 0 Output Kaps: 1
Latest ASDM System Messares	Configure ASDN Sudag Filters
Sysing Disabled	
oyong praktion	
Device configuration loaded successfully	sadmina N8 (15)
Device configuration loaded successionly.	

 Markieren Sie die Ethernet 0-Schnittstelle, und klicken Sie auf Bearbeiten, um die externe Schnittstelle zu konfigurieren.

Eisco ASDM 5 File Rules B	5.0 for earch	PIX - 10.1.1 Options	 Tools Wizards	Help								
G Home	Confi	Guration	Monitoring	Back F	orward	Q Search	Refresh	Seve	? Help			Cisco Systems
Features	Co	nfiguration =	Features > Inte	rfaces	- A -							
, Interfaces	- +	1 <u>.</u>	e i mi i k s		31991							
<u>6</u> ,		Ir	nteríace	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
in the second se		Ethernet0			No					No		Delete
423 Routing												
Building Blocks												
Device Administration												
Properties		•									•	
		🗆 Enable t	affic between tw	o or more inf	erfaces w	hich are c	onfigured with sa	ame secu	irity levels			
							_		1			
Wizards /						Apply	R	eset				
						ŀ	admin> N	A (15)	6		3/16/05	4:26:48 PM UTC

7. Klicken Sie an der Eingabeaufforderung Bearbeiten auf



8. Geben Sie die Schnittstellendetails ein, und klicken Sie abschließend auf **OK**.

🔂 Edit Interface		2	хI
Hardware Port:	EthernetO	Configure Hardware Properties	
🔽 Enable Interface	🗖 Dedicate this interface to manag	ement only	
Interface Name:	outside		
Security Level:	0		
- IP Address			
Ose Static IP	C Obtain Address via DHCP		
IP Address:	99.99.99.1		
Subnet Mask:	255.255.255.0		
MTU:	1500		
Description:			
	1		
	OK Cancel	Help	

9. Klicken Sie an der Eingabeaufforderung Schnittstellenänderung auf



10. Klicken Sie auf **Apply**, um die Schnittstellenkonfiguration zu akzeptieren. Die Konfiguration wird auch auf den PIX übertragen. In diesem Beispiel werden statische Routen verwendet.

File Rules B	.0 fo sarch	PTX - 10.1.1.1 Options Tools Wiza	rds Help							-	
G Home	Conf	🦓 [] iguration Monitoring	Back F	orward	Q Search	Refresh	Nave Save	? Helip			CISCO SYSTEMS
Features	C	infiguration > Features > I	Interfaces	. A.							
Interfaces		· 프 + IK I U I A	19 10 19 19 19	51691							
<u>6</u> ,		Interface	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	55.255.0	No	1500	Edit
1		Ethernetü	outside	Yes	0	99.99.99.1	265.2	55.255.0	No	1500	Delete
423 Routing											
Building Blocks											
Device Administration											
Froperties		×								×	
		Enable traffic between	n two or more int	erfaces w	hich are c	onfigured with s	ame sec	urity levels			
					Apply	R	eset	1			
Wizards 🕗								_			
					-	<admin> N</admin>	A (15)	1		3/16/05	4:29:18 PM UTC

11. Klicken Sie unter der Registerkarte Funktionen auf **Routing**, markieren Sie **Statische Route**, und klicken Sie auf **Hinzufügen**.

File Rules Be	.0 for PIX - 10.1.1.1 sarsh Options Tools Wizari	is Help				_ 🗆 X
G Home	Configuration Monitoring	Back Forward	Q Q Search Refrest	Save	? Help	Cisco Systems
Features	Configuration > Features > R	outing > Routing > Static R Static Route Specify static routes. Interface IP Addr	ess Netmask	Gateway IP	Metric Tunnele	d Add Edit Delete
			<admin></admin>	NA (15)	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	🔒 3/16/05 4:44:48 PM UTC

12. Konfigurieren Sie das Standard-Gateway, und klicken Sie auf

	🔂 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. Klicken Sie auf Hinzufügen, und fügen Sie die Routen zu den internen Netzwerken

	🗲 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 o	nly for default route)
hinzu	ок	Cancel Help

14. Bestätigen Sie, dass die richtigen Routen konfiguriert sind, und klicken Sie auf Übernehmen.

	<u> </u>		
Gisco ASDM 5.	0 for PIX - 10.1.1.1		_ 🗆 ×
File Rules Be	arch Options Tools Wizard	з нер	
Home C	Configuration Monitoring	O O Q O Q Back Forward Search Refresh Save Help	Cisco Systems
Features	Configuration > Features > Re	uting > Routing > Static Route	
	● 金 等 ■ 前 永 日本 Bourdian	2 単 影 昭 辛	
Interfaces	EF Vig Routing	- Static Route	
<u>i</u> ,		Specify static routes.	
Security Policy	E AOSPF	Interface IP Address Netmask Gateway IP Metric Tunneled	Add
24	🖻 🍓 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
	E PIM		
			Delete
*25 Routing			
- 83			
Building Blocks			
Bevice			
Administration			
3 .			
Properties			
		Apply Reset	
Wizards 🗠			
		admin> 🛛 🗛 付 ا 🛃 🖓 ا 😂 ا ۲۵ ما	/05 4:46:48 PM UTC

15. In diesem Beispiel wird NAT verwendet. Deaktivieren Sie das Kontrollkästchen Datenverkehr durch die Firewall ohne Adressübersetzung aktivieren, und klicken Sie auf Hinzufügen, um die NAT-Regel zu

konfiguriere	en.											
🔨 Cisco ASDM 5.0) for PIX - 10	.1.1.1					L X					
File Rules Sea	arch Option	is Tools Wizari	is Help									
Home C	onfiguration	Monitoring	Back Forward S	Q Q Search Refresh :	Save Help	C	ISCO SYSTEMS					
Features	Configurati	on > Features > N	AT > Translation Rules									
	🔶 🤤 🖗	「「「「」「「」」と	54 🛍 🕵 🛍 🕼 👘									
Interfaces	🗆 Enst	le traffic through t	he firewall without address	translation								
Δ,	Translation Rules O Translation Exemption Rules											
Security Policy	Show Rules for Interface: All Interfaces Show All											
NAT	Rule		Original			Translated	Add					
<u> </u>	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit					
VPN							Delete					
423 Routing												
<u>8</u>												
Building Blocks												
Device Administration												
Properties	•					•						
	nja Sta	tic NAT 🛛 📲 I	Dynamic NAT 🐘 🔂 Stati	c Policy NAT 👘 🖓 D	ynamic Policy NA	T Manage Pools						
				(aniv	Parat							
Wittendo				Abbiy	Reset							
wizarus ×	1			Leadering (k)	(45) L L		14 VO DM LITO					
				saurinis Ma	(10)	ar 📷 🔰 📄 ar 6/05 4	31.48 PM OTC					

16. Konfigurieren Sie das Quellnetzwerk (in diesem Beispiel verwenden Sie alle). Klicken Sie anschließend auf **Pools verwalten**, um die PAT zu definieren.

🙀 Add Address Tr	anslation R	ule						x
Use NAT	ΟU	se Policy NAT						
- Source Hos	t/Network-							1
		Interface:	inside		•			
		IP Address:	0.0.0.0					
		Mask:	0.0.0.0		Ŧ			
			Browse .					
							NAT Options	1
Translate Add	ress on Inter	rface: outsid	le 💌			_		_
Translate Ad	ddress To —							
C III S	Static	IP Address;			-			
	Redirect p	ort						
	C UDP	Original port:		Translated	port:			
• 🖷 (Dynamic	Address Pool:	same addr	ess 💌	Manage	Pools		
	Pool ID		Ado	dress				
	N/A	No address poo) defined					
		ок	Canc	el	Help			

17. Wählen Sie die **externe** Schnittstelle aus, und klicken Sie auf **Hinzufügen**.

lobal Address Po	ools			
obal Address Po dresses.	ols are used to con	figure Dynamic Network Ad	dress Translation (NAT)	
Interface	Pool ID	IP Address(es)		
nside outside			A	bb
			E	dit
			De	lete
			1	
	OK	Cancel	Help	

In diesem Beispiel wird eine PAT verwendet, die die IP-Adresse der Schnittstelle verwendet.

🕵 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. Klicken Sie bei der Konfiguration der PAT auf OK.

lobal Address P	'ools are used to con	figure Dynamic Network Address 1	Franslation (NAT)
idresses.			
Interface	Pool ID	IP Address(es)	
nside uteide	1 00 00	00 1/interface PAT)	Add
utoruc	1 33.33.	55.T(IntendeeTAT)	
			Edit
			Delete

19. Klicken Sie auf **Hinzufügen**, um die statische Übersetzung zu konfigurieren.

🔁 Add Address 1	Franslation R	ule				x
Use NAT	r cu	se Policy NAT				
Source Ho	st/Network—					
		Interface:	inside	•		
		IP Address:	0.0.0.0			
		Mask	0.0.0.0	T		
			Browse	_		
			DIONSC		NAT Options	
Translate åd	dress on inter	face: outein	10 1		INAT Options	
Translate		Joursie				
I ranslate /	Address Io—		-	_		
0 II	Static	IP Address:		<u>×</u>		
	C TOD	ion.				
	CUDP	Original port:	Translated	port.		
e 🚻	Dynamic	Address Pool:	same address 💌	Manage Pools		
	Pool ID		Address			
	1	99.99.99.1 (inter	face PAT)			
	1					
		OK	Consol	Holp		
	_	UK	Cancel	Help		

20. Wählen Sie drinnen im Dropdown-Menü Interface (Schnittstelle) aus, und geben Sie dann die IP-Adresse 10.1.1.2, Subnetzmaske 255.255.255, wählen Sie Statisch und den IP-Adresstyp außerhalb der Adresse 99.99.12 ein. Klicken Sie abschließend auf OK.

🕵 Add Address Tra	Inslation R	ule				x
O Use NAT	ΟU	se Policy NAT				
- Source Host/	Network-					
		Interface:	inside	•		
		IP Address:	10.1.1.2			
		Mask:	255 255 255 255	-		
			1200.200.200.200			
			Browse			
					NAT Options	
Translate Addre	ess on Inter	rface: outsid	le 💌			
— Translate Ad	dress To —	,				
G ili s	tatic	IP åddrass:	00.00.00.12	-		
	Redirect p	ort	33.33.33.12			
	C TOP	Original port:	Translate	ed port:		
с 🖞 р	ynamic	Address Pool:	same address 💌	Manage Pool	s	
	Pool ID		Address			
		014		11-1-		
	_	UK	Cancel	Help		

21. Klicken Sie auf **Apply**, um die Schnittstellenkonfiguration zu akzeptieren. Die Konfiguration wird auch auf den PIX übertragen.



22. Wählen Sie auf der Registerkarte Funktionen **Sicherheitsrichtlinie** aus, um die Sicherheitsrichtlinienregel zu konfigurieren.



23. Klicken Sie auf **Hinzufügen**, um Datenverkehr zuzulassen, und klicken Sie auf **OK**, um fortzufahren.

Add Access Rule	2
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	
CITCP CUDP CICMP CIP	Manage Service Groups
IP Protocol	
IP protocol: esp	
Please enter the description below (optional):	
Access Rule to Allow ESP traffic	A
OK Car	ncel Help

24. Klicken Sie auf **Hinzufügen**, um ISAKMP-Datenverkehr zuzulassen, und klicken Sie auf **OK**, um

fortzufahren.

📬 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: 255.255.255.255 💌	Mask: 255.255.255.255 💌
99.99.99.2	inside 99.99.99.12
Protocol and Service	
C TCP © UDP C ICMP C IP Source Port © Service = V 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	×
OK Can	cel Help

25. Klicken Sie auf **Hinzufügen**, um den UDP-Port 4500-Verkehr für NAT-T zuzulassen, und klicken Sie auf **OK**, um fortzufahren.

🖆 Edit Access Rule	x
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
	CIP 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 💌
Rule Flow Diagram Rule applied to traffic incoming to 99.99.99.2 Allow tr	source interface
Protocol and Service	
C TCP © UDP C ICMP C IP Source Port © Service = • 4500 © Service Group	Manage Service Groups Destination Port Service = any C Service Group
Please enter the description below (optional):	
Access Rule to allow 4500 to host 99.99.99.12	*
OK Car	ncel Help

26. Klicken Sie auf **Apply**, um die Schnittstellenkonfiguration zu akzeptieren. Die Konfiguration wird auch auf den PIX übertragen.

Elisco ASDM 5.0 File Rules Sea	for PIX arch Op	-10.1.1.1 tions Too)is Wiz	ards Help								_0×
Home C	onfigura	tion Mo) Notice	C) Back	O Forward	Q Search	Refresh	Seve	? Helip		Ces t	CO SYSTEMS
Features	Configu	ration > Fe	atures >	Security Policy	> Access R	ules						
	* *	¥ 🗹	1	6 🖻 🛍 🕵 i	ñ 🖇 🛛							
Nerfaces	Ac Ac Ac Ac	cess Rule	s CA	AA Rules C	Filter Rule:	s C Sen	vice Policy R	ules				
	Show	Rules for I	nteríace	All Interfaces	•	Show All						
Security Policy	#	Rule Enabled	Action	Source Hostilvet	work	Des Hos	tination bNetwork	Rule App To Traffic	lied	Interface	Service	Add
NAT		N	¥	🎱 any		🧼 any			ir Q	nside outbound)	™ ip	Edit
02	1	V	*	A 99.99.99.2 A 99.99.2		🗟 99.99.9	9.12	🥬 incom	ning o	utside	ır⁄esp	Delete
VPN	2		1	399.99.99.2		E 99.99.9	9.12	♣ incom	ning o	utside	Brc: isakmp	
423 Routing												
Administration												
Properties												
	-	Allow traffic	:	 Deny traffic 				(• Show	w Summary	C Show Detail	
Wizards - 4					Apply		Reset		Advanc	ed		
	,					<	admin>	NA (15)		2 N 1	3/16/05 4:54	4:58 PM UTC

27. Die Konfiguration ist nun abgeschlossen.Wählen Sie File (Datei) > Show Running Configuration (Konfiguration anzeigen) in New Window, um die CLI-Konfiguration

	File Rules Search Options Tools Wizards Help
	Refresh ASDM with the Running Configuration on the Device
	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
anzuzeigen	Exit
anzuzeigen.	

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
1
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 Security Appliance- und MPF-Konfiguration (Modular Policy Framework)

Verwenden Sie anstelle der Zugriffsliste den Befehl **inspect ipsec-pass-thru** in MPF (Modular Policy Framework), um den IPsec-Datenverkehr über die PIX/ASA Security Appliances weiterzuleiten.

Diese Prüfung ist so konfiguriert, dass sie Pinholes für ESP-Datenverkehr öffnet. Alle ESP-Datenflüsse sind zulässig, wenn ein Weiterleitungsfluss vorhanden ist, und es gibt keine Beschränkung für die maximale Anzahl an Verbindungen, die zulässig sein können. AH ist nicht zulässig. Das Timeout für Leerlaufzeiten für ESP-Datenflüsse ist standardmäßig auf 10 Minuten festgelegt. Diese Überprüfung kann an allen Standorten angewendet werden, an denen andere Überprüfungen durchgeführt werden können. Dazu gehören Befehlsmodi für Klassen und Übereinstimmung. Die IPSec-Passthrough-Anwendungsinspektion ermöglicht eine einfache Überbrückung des ESP-Datenverkehrs (IP Protocol 50), der mit einer Verbindung des IKE-UDP-Ports 500 verbunden ist. Sie vermeidet langwierige Zugriffslistenkonfigurationen, um ESP-Datenverkehr zuzulassen, und bietet außerdem Sicherheit mit Timeout und max. Verbindungen. Befehle für Klassenzuordnung, Richtlinienzuordnung und Dienstrichtlinien zum Definieren einer Datenverkehrsklasse, zum Anwenden des Befehls inspect auf die Klasse und zum Anwenden der Richtlinie auf eine oder mehrere Schnittstellen verwenden. Wenn der Befehl inspect IPSec-passthru aktiviert ist, kann unbegrenzter ESP-Datenverkehr mit einer Zeitüberschreitung von 10 Minuten zugelassen werden, die nicht konfigurierbar ist. NAT- und Nicht-NAT-Datenverkehr ist zulässig.

```
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
```

<u>Überprüfen</u>

Dieser Abschnitt enthält Informationen zur Bestätigung, dass Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom <u>Output Interpreter Tool</u> unterstützt (nur <u>registrierte</u> Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- show crypto ipsec sa Zeigt die Sicherheitszuordnungen für Phase 2 an.
- show crypto isakmp sa Zeigt die Sicherheitszuordnungen für Phase 1 an.
- show crypto engine connections active Zeigt die verschlüsselten und entschlüsselten Pakete an.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung für Router IPsec

Hinweis: Lesen Sie <u>vor dem</u> Ausgabe von **Debug-**Befehlen unter<u>Wichtige Informationen zu</u> <u>Debug-Befehlen nach</u>.

- debug crypto engine: Zeigt den verschlüsselten Datenverkehr an.
- debug crypto ipsec: Zeigt die IPsec-Aushandlungen für Phase 2 an.
- debug crypto isakmp: Zeigt die Aushandlungen der Internet Security Association und des Key Management Protocol (ISAKMP) für Phase 1 an.

Löschen von Sicherheitszuordnungen

- clear crypto isakmp Löscht die Sicherheitszuordnungen von Internet Key Exchange (IKE).
- clear crypto ipsec sa: Löscht IPsec-Sicherheitszuordnungen.

Befehle zur Fehlerbehebung für PIX

Bestimmte **show**-Befehle werden vom <u>Output Interpreter Tool</u> unterstützt (nur <u>registrierte</u> Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

Hinweis: Lesen Sie <u>vor dem</u> Ausgabe von **Debug-**Befehlen unter<u>Wichtige Informationen zu</u> <u>Debug-Befehlen nach</u>.

- **logging buffer debugging** Zeigt Verbindungen an, die hergestellt und Hosts verweigert werden, die den PIX durchlaufen. Die Informationen werden im PIX-Protokollpuffer gespeichert, und die Ausgabe kann mit dem Befehl **show log** angezeigt werden.
- ASDM kann verwendet werden, um die Protokollierung zu aktivieren und die Protokolle anzuzeigen, wie in diesen Schritten gezeigt.
- 1. Wählen Sie Konfiguration > Eigenschaften > Protokollierung > Protokollierung > Setup > Protokollierung aktivieren aus, und klicken Sie dann auf

Ubernenm	n.	
🔂 Eisco ASDM 5.	for PIX - 10.1.1.1	
File Rules Se	ch Options Tools Wizards Help	
💰 Ноте	nfiguration Monitoring Back Forward Search Refresh Save Help	EN S
Features	Configuration > Features > Properties > Logging > Logging Setup	
Interfaces Security Policy NAT Security Policy NAT Security NAT Security Recting Building Blocks Device Administration	Configure FTP Settings Save Buffer To: FTP Server Configure FTP Settings Configure FTP Settings Save Buffer To: FTP Server Configu	
Wizards /	Apply Reset	
	 sadmin> (NA (15) SA 8/05 5:03:38 PM 	orc

 Wählen Sie Monitoring > Logging > Log Buffer > On Logging Level > Logging Buffer aus, und klicken Sie dann auf View (Anzeigen).



Dies ist ein Beispiel für den Log-Puffer.

Log Buff	fer	
This scre	en shows syslog mess:	ages in ASDM logging buffer as of now.
	F	
Find text	in messages below:	Find Next
Severity	Time	
<u> 6</u> 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>i</u> 6	Mar 16 2005 17:05:47	609001: Built local-host inside:10.1.1.2
<u>i</u> 6	Mar 16 2005 17:05:47	609001: Built local-host outside:99.99.99.2
<u>i</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>î</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>i</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>î</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>i</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
<u>i</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>f</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
🔥 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>i</u> . 6	Mar 16 2005 17:05:47	609001: Built local-host inside:10.1.1.2
έ. 6	Mar 16 2005 17:05:47	609001: Built local-host outside:99.99.99.2
<u>i</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
ί. 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>i</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>î</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
i 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>i</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.
1.6	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>1</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
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.
1.6	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
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
<u>i</u> 6	Mar 16 2005 17:05:46	302014: Teardown TCP connection 44 for inside:10.1.1.3/1216 to NP Identity Ifc:10

6 🔥

4

Refresh

Save Log As...

Mar 16 2005 17:05:46

Clear

605005: Login permitted from 10.1.1.3/1219 to inside:10.1.1.1/https for user "enable

Close

Help

F

Zugehörige Informationen

- Support-Seite für IPsec-Aushandlung/IKE-Protokolle
- PIX-Support-Seite
- PIX-Befehlsreferenzen
- <u>NAT-Support-Seite</u>
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation Cisco Systems