ASA/PIX - Konfigurieren eines Cisco IOS-Router-LAN-to-LAN-IPsec-Tunnels

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Hintergrundinformationen Konfigurieren Netzwerkdiagramm Konfigurationen Konfigurationen Konfiguration mit ASDM Überprüfung Fehlerbehebung Befehle zur Fehlerbehebung Zugehörige Informationen

Einleitung

In diesem Dokument wird veranschaulicht, wie ein IPsec-Tunnel von der PIX Security Appliance 7.x und höher oder der Adaptive Security Appliance (ASA) mit einem internen Netzwerk zu einem 2611-Router konfiguriert wird, der ein Krypto-Image ausführt. Zur Vereinfachung werden statische Routen verwendet.

Weitere Informationen über eine LAN-zu-LAN-Tunnelkonfiguration zwischen einem Router und dem PIX finden Sie unter Konfigurieren von IPSec - Router zu PIX.

Weitere Informationen zur Konfiguration eines LAN-to-LAN-Tunnels zwischen dem Cisco VPN 3000 Concentrator und der PIX-Firewall-Konfiguration zwischen der PIX-Firewall und dem Cisco VPN 3000-Concentrator finden Sie im Konfigurationsbeispiel für einen LAN-zu-LAN-Tunnel.

Weitere Informationen zum Szenario, in dem sich der LAN-zu-LAN-Tunnel zwischen dem PIX<u>7.x</u> <u>und dem VPN</u> 3000 Concentrator befindet, finden Sie im Konfigurationsbeispiel für den<u>IPsec-</u> <u>Tunnel zwischen PIX und VPN Concentrator</u>.

Unter Konfigurationsbeispiel für PIX/ASA 7.x Enhanced Spoke-to-Client VPN mit TACACS+-Authentifizierung erfahren Sie mehr über das Szenario, in dem der LAN-zu-LAN-Tunnel zwischen den PIXs auch einem VPN-Client den Zugriff auf die Spoke-PIX über den Hub-PIX ermöglicht.

Weitere Informationen finden Sie unter <u>SDM: Site-to-Site-IPsec-VPN zwischen ASA/PIX und</u> <u>einem IOS-Router - Konfigurationsbeispiel</u>, um mehr über dasselbe Szenario zu erfahren, in dem die PIX/ASA Security Appliance die Softwareversion 8.x ausführt.

Weitere Informationen finden Sie unter <u>Configuration Professional: Standortübergreifendes IPsec-</u><u>VPN zwischen ASA/PIX und einem IOS-Router - Konfigurationsbeispiel</u>, um mehr über dasselbe Szenario zu erfahren, in dem die ASA-bezogene Konfiguration mithilfe der ASDM-GUI angezeigt wird und die Router-bezogene Konfiguration mithilfe der Cisco CP-GUI angezeigt wird.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- PIX-525 mit PIX Software Version 7.0
- Cisco 2611 Router mit Cisco IOS® Software, Version 12.2(15)T13

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen 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).

Hintergrundinformationen

Auf dem PIX arbeiten die Befehle **access-list** und **nat 0** zusammen. Wenn ein Benutzer im 10.1.1.0-Netzwerk zum 10.2.2.0-Netzwerk geht, wird die Zugriffsliste verwendet, um die Verschlüsselung des 10.1.1.0-Netzwerkverkehrs ohne Network Address Translation (NAT) zu ermöglichen. Auf dem Router werden die Befehle **route-map** und **access-list** verwendet, um die Verschlüsselung des 10.2.2.0-Netzwerkverkehrs ohne NAT zu ermöglichen. Wenn jedoch dieselben Benutzer an einen anderen Ort reisen, werden sie mithilfe von Port Address Translation (PAT) in die Adresse 172.17.63.230 übersetzt.

Dies sind die Konfigurationsbefehle, die auf der PIX Security Appliance erforderlich sind, damit Datenverkehr *nicht* über PAT über den Tunnel läuft und Datenverkehr zum Internet über PAT fließt.

access-list nonat permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 nat (inside) 0 access-list nonat nat (inside) 1 10.1.1.0 255.255.255.0 0 0

Konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Hinweis: Verwenden Sie das <u>Command Lookup Tool</u> (nur <u>registrierte</u> Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

Diese Konfigurationsbeispiele gelten für die Befehlszeilenschnittstelle. Wenn Sie <u>ASDM</u> verwenden möchten, lesen Sie den Abschnitt<u>"Konfiguration mithilfe</u> des <u>Adaptive Security Device</u> <u>Manager (ASDM)</u> dieses Dokuments.

- Hauptsitz PIX
- <u>Zweigstellen-Router</u>

Hauptsitz PIX

HQPIX(config)# show run	
PIX Version 7.0(0)102	
names	
!	
interface Ethernet0	

```
description WAN interface
nameif outside
security-level 0
ip address 172.17.63.229 255.255.255.240
!
interface Ethernet1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
interface Ethernet2
shutdown
no nameif
no security-level
no ip address
interface Ethernet3
shutdown
no nameif
no security-level
no ip address
1
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
1
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname HQPIX
domain-name cisco.com
ftp mode passive
clock timezone AEST 10
access-list Ipsec-conn extended permit ip 10.1.1.0
255.255.255.0 10.2.2.0 255.255.255.0
access-list nonat extended permit ip 10.1.1.0
255.255.255.0 10.2.2.0 255.255.255.0
pager lines 24
logging enable
logging buffered debugging
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 access-list nonat
nat (inside) 1 10.1.1.0 255.255.255.0
access-group 100 in interface inside
route outside 0.0.0.0 0.0.0.0 172.17.63.230 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
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server partner protocol tacacs+
username cisco password 3USUcOPFUiMCO4Jk encrypted
http server enable
http 10.1.1.2 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp
crypto ipsec transform-set avalanche esp-des esp-md5-
hmac
crypto ipsec security-association lifetime seconds 3600
crypto ipsec df-bit clear-df outside
crypto map forsberg 21 match address Ipsec-conn
crypto map forsberg 21 set peer 172.17.63.230
crypto map forsberg 21 set transform-set avalanche
crypto map forsberg interface outside
isakmp identity address
isakmp enable outside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash sha
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
tunnel-group 172.17.63.230 type ipsec-121
tunnel-group 172.17.63.230 ipsec-attributes
pre-shared-key *
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
inspect http
```

```
service-policy asa_global_fw_policy global
Cryptochecksum:3a5851f7310d14e82bdf17e64d638738
: end
SV-2-8#
Zweigstellen-Router
```

```
BranchRouter#show run
Building configuration...
Current configuration : 1719 bytes
1
! Last configuration change at 13:03:25 AEST Tue Apr 5
2005
! NVRAM config last updated at 13:03:44 AEST Tue Apr 5
2005
1
version 12.2
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
1
hostname BranchRouter
1
logging queue-limit 100
logging buffered 4096 debugging
1
username cisco privilege 15 password 0 cisco
memory-size iomem 15
clock timezone AEST 10
ip subnet-zero
!
!
ip audit notify log
ip audit po max-events 100
!
!
crypto isakmp policy 11
encr 3des
authentication pre-share
group 2
crypto isakmp key cisco123 address 172.17.63.229
1
1
crypto ipsec transform-set sharks esp-des esp-md5-hmac
!
crypto map nolan 11 ipsec-isakmp
set peer 172.17.63.229
set transform-set sharks
match address 120
1
1
no voice hpi capture buffer
```

```
no voice hpi capture destination
1
!
mta receive maximum-recipients 0
1
!
!
1
interface Ethernet0/0
ip address 172.17.63.230 255.255.255.240
ip nat outside
no ip route-cache
no ip mroute-cache
half-duplex
crypto map nolan
interface Ethernet0/1
ip address 10.2.2.1 255.255.255.0
ip nat inside
half-duplex
ip nat pool branch 172.17.63.230 172.17.63.230 netmask
255.255.255.0
ip nat inside source route-map nonat pool branch
overload
no ip http server
no ip http secure-server
ip classless
ip route 10.1.1.0 255.255.255.0 172.17.63.229
1
access-list 120 permit ip 10.2.2.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 130 deny ip 10.2.2.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 130 permit ip 10.2.2.0 0.0.0.255 any
!
route-map nonat permit 10
match ip address 130
1
call rsvp-sync
1
1
mgcp profile default
1
dial-peer cor custom
1
!
!
!
1
line con 0
line aux 0
line vty 0 4
login
!
!
end
```

Konfiguration mit ASDM

In diesem Beispiel wird die Konfiguration des PIX mithilfe der ASDM-GUI veranschaulicht. Ein PC mit Browser und IP-Adresse 10.1.1.2 ist mit der internen Schnittstelle e1 des PIX verbunden. Stellen Sie sicher, dass http auf dem PIX aktiviert ist.

Dieses Verfahren veranschaulicht die ASDM-Konfiguration des PIX-Systems am Hauptsitz.

1. Verbinden Sie den PC mit dem PIX, und wählen Sie eine Download-Methode

Cisco ASDM 5.0	
Cisco ASDM 5.0 provides an intuitive graphical user inte configure and manage your Cisco Security Appliances.	erface that makes it easy to set up,
Cisco ASDM runs as either a local application or a Java	Applet.
Running Cisco ASDM as a local Application	
 Upgrades of the local application are performe You can invoke ASDM from desktop shortcuts 	ed automatically.
 Upgrades of the local application are performe You can invoke ASDM from desktop shortcuts One desktop shortcut allows you to connect to Download ASDM Launcher a	ed automatically. . No browser is required. . <i>multiple</i> Security Appliances. nd Start ASDM
 Upgrades of the local application are performe You can invoke ASDM from desktop shortcuts One desktop shortcut allows you to connect to Download ASDM Launcher a	ed automatically. . No browser is required. . <i>multiple</i> Security Appliances. .nd Start ASDM
Upgrades of the local application are performe You can invoke ASDM from desktop shortcuts. One desktop shortcut allows you to connect to Download ASDM Launcher a	ed automatically. . No browser is required. . <i>multiple</i> Security Appliances.
 Upgrades of the local application are performe You can invoke ASDM from desktop shortcuts. One desktop shortcut allows you to connect to Download ASDM Launcher a Running Cisco ASDM as a Java Applet You can run Cisco ASDM as a Java applet that is dynwhich you connect.	ed automatically. No browser is required. <i>multiple</i> Security Appliances. and Start ASDM

ASDM lädt die vorhandene Konfiguration aus dem PIX.

			Interface Sta	tus		
General License			Interface	IP Address/Mask	Line Lini	k Current Kops
Host Name:						
PDCVersion:	Device	Uptime:				
ASDM Version:	Device	Type:				
Firewall Mode.	🚮 Status				×	
	a second s					
VPN Status	50	Please wait while ASDM is I	oading the curren	t configuration from yo	ur	
E de la companya de la compa	<u> </u>	Gence.				
System Resources Status		_		1		
cro cro onyrt	×.	62	296	J		
		Initializing Monitor modules	ar.,		Total:	
Memory Memory Usa	s					
			imput HD	· · · ·	rasput integat.	

Dieses Fenster bietet Überwachungsinstrumente und Menüs.

Home Cor	ofiguration Monit	oring Back	Forward Searc	h Refresh	Save Help			dbdb
Device Inform	ation			-Interface Sta	tus			
General Lic	ense			Interface	IP Address/Mas	k Line	Link	Current Kbps
Host Name:	SV-2-8.cisco.co	m		inside	10.1.1.1/24	💿 up	😧 up	1
PC Version:	7.0(0)102	Device Uptime:	0d 0h 24m 50s					
ASDM Version	5.0(0)73	Device Type:	PIX 525					
Firewall Mode	Routed	Context Mode:	Single					
Total Flash:	16 MB	Total Memory:	256 MB	Colect on inter	face to view innut ar	d output kits	ne	
VPN Status	-			Traffic Statu	s	ia ostiput ros	hè	
IKE Tunnels:	0	IPSec Tunnels:	0	Connections	Per Second Usage			
CPU 0% 04:57:46 Memory 67M9 04:57:46	CPU Usage (percent) 90 04 32 04 36 36 Memory Usage (MB) 250 102 122 122 04 04 50 30 102 102 102 102 102 102 102 10			0.5 0.5 UDP: 0 'inside' leter 24 16 03:50:20 Input Kb	TCP: 0 face Traffic Urage (Ktp pr: 0	i) Output Hop	Fotal: 0	
Latest ASDM	Syslog Messages	Syslog Disable	-			2	nfigure AS	DM System Filler

2. Wählen Sie **Konfiguration > Funktionen > Schnittstellen** aus, und wählen Sie **Add** für neue Schnittstellen oder **Edit** für eine vorhandene Konfiguration aus.

ares (Configuration = Features = th 수 옷 좋! 딸! 🏦 🐰	nataces Por IBS IBS R	5 3 1				-	-			
aces	Interface	Name	Enabled	Security	IP Address	Subnet Mask	Management	MTU		D	Ad
Policy	Ethernetl	Inside	Yes	100	10.1.1.1	255 255 255 0	No	1500			Ed
k	Ethernet0	outside	Yes	0	172.17.63.229	255 255 255 240	No	1500	WAN interface		Dete
ut 🖉	Ethernet2		No				No				
5	Ethernet3		No				No				
	Ethernet4		No				No				
5 ting	Ethernet5		No				No				
Blocks											
tration											

3. Wählen Sie die Sicherheitsoptionen für die interne Schnittstelle

aus.	0 fer PIX - 10.1.1.1			and the second second				
Home C	Configuration Monitoring	zards Help Back Ferward	Search Refresh	Save Help			Cis	te States
Hone C Features Interfaces Security Policy NAT Security Policy	Configuration Monitoring Configuration & Fristures Configuration & Fristures	Back Forward	Search Refresh Rules es C Service Policy Ru Show All Destination HostNetwork	Save Help les Rule Applied To Traffic	Interface	Service	Log Level Interval	Add Edit Delete
Wizards /	✓ Allow traffic	Deny traffic Apply	Reset	Advance	ıd	Show Summary	C Show Detail	
				cisco	NA (2)	14 de 1	A 16/05 3 25 21	S PM AEST

4. In der NAT-Konfiguration ist der verschlüsselte Datenverkehr von der NAT ausgenommen, und der gesamte andere Datenverkehr ist NAT/PAT zur externen Schnittstelle

Cisco ASDM 5. Tile Rules Se	o for PEX - 10.1.1.1 arch Options Tools Wiz	ards Help					- [2]
Horse	Configuration Monitoring	Dack Forward	Q @ Search Refresh	Sove Help	b G	Cis	co Statu
Features	Configuration + Features +	NAT = Translation Rules		_		-	
internaces	C Enable traffic throug Translation Rules Show Rules for Interfac	C Translation Exem	s translation ption Rules				
NAT	Rule	Original			Translated		Add
8	Type Interface	Source Network	Destination Network	Interface	Address	DNS Rewrite	Edit
Routing Building Blocks Device Administration Properties							
	-						
	2. CHARLENET 3	Dunamic NAT A Sta	fic Policy NAT	mamic Policy N	4AT	Managa Regis	

5. Wählen Sie **VPN >Allgemein > Tunnelgruppe** aus, und aktivieren Sie eine Tunnelgruppe.



 Wählen Sie VPN > IKE > Globale Parameter aus, und aktivieren Sie IKE auf der externen Schnittstelle.

Cisco ASOM S	Conc.		
Home	Configuration Montoring Back	O Q Q Retresh Save Help	Cisco Statias
Features	Configuration & Features + VPN > KE Configuration + Features + VPN > KE Configuration + Features + VPN > KE Configuration + Clean Update Tunnel Group Control Policy Conficate Oroup Matching Conficate Oroup Matching Policies Policy Policy Policy Policy Policy Policy Policy Policy Policy Policy Policy Policy Policy Policy Pre-Fragmentation Policy Policy Policy Policy Pre-Fragmentation Policy Policy Policy Policy Pre-Fragmentation Policy Policy Policy Policy Policy Policy Policy Pre-Pragmentation Policy P	Otobal Parameters Enable IKE Interface Interface	

7. Wählen Sie VPN > IKE > Policies (VPN > IKE > Richtlinien) und wählen Sie die IKE-

Richtlinien

aus.

Home	Configuration Monitoring Back	Forward	Search Re	ofreah	Save He	sip			alburgh
Features	Configuration > Features > VFN > IKE >	Policies	_		_				
Interfaces	Client Update	Policies Configure s Security Ass protocols	pecific Interne sociation Key f	t Key Exch danagem	ange (KE) alg ent Protocol (IS	orithms and paran AKMP) framework	neters, within the IPS for the AH and ESP	lec Internet IPSec	
乱	Default Tunnel Gateway	Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime(secs)	Add	
NAT	- Global Parameters	1	3des	sha	2	pre-share	86400	Edit	
VPN	Certificate Group Matching							Cun	
Routing Routing Biocks Bevice hereitration	Padres Rules	-17							
					,App)	/ F	teset		

 Wählen Sie VPN > IPsec > IPsec > IPsec Rules und wählen Sie IPsec f
ür die lokale Tunnelund Remote-Adressierung aus.

Cisco ASDM 5.	0 for PEX - 10.1.1.1	E				*D×
Home C	Configuration Montoring Back	Porward Sea	ch Retresh Save	? Help		Cisco Sestens
Features	Configuration + Features + VPN + IPSec +	IPSec Rules				
interfaces		IPSec Rules Use the Rules	menu, the toolbar, or the right n	nouse button to add, edit or d	telete roles.	
Security Policy	- Tunnel Group - Group Policy	# Acti	on PDC Side	Remote Side	Service	Tunnel Po Add
品	-+-Default Tunnel Gateway	1 prot	ect 🖾 10.1.1.0/24	E 10.2.2.0/24	💌 ip 🛛 out	side.static-
NAT	- Global Parameters					Delete
	Certificate Group Matching					
Routing Building Blocks Device Administration Properties	Policy PRules Provide			(ኛ 8	how Summary 🔿 S	* how Detail
Wizards 🖉			Apply	Reset		
			ci	isco NA (2)	6 B	4/6/05 3:33:35 PM AEST

9. Wählen Sie VPN > IPsec > Tunnel Policy aus, und wählen Sie die Tunnelrichtlinie



10. Wählen Sie VPN > IPsec > Transform Sets und wählen Sie einen Transform Set

aus.

Nere Nordorn Bat Perved Sach Refer Seve Perved Seve Seve Seve Seve Seve Seve Seve </th <th>Cisco ASDM 5. No Rules Se</th> <th>O for PIX-10.1.1.1 Arch Options Tools Wizards Help</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>_10</th>	Cisco ASDM 5. No Rules Se	O for PIX-10.1.1.1 Arch Options Tools Wizards Help						_10
Features Configuration > Flashungs > VFN > Place > Transform Sets Imprint Construction > Flashungs > VFN > Place > Transform Sets Imprint Construction > Flashungs > VFN > Place > Transform Sets Imprint Construction > Flashungs > VFN > Place > Transform Sets Imprint Construction > Flashungs > VFN > Place > Transform Sets Imprint Construction > Flashungs > VFN > Place > Transform Sets Imprint Construction > Flashungs > VFN > Place > Transform Sets Imprint Construction > Flashungs > VFN > Place > Transform Sets Imprint Construction > Flashungs > VFN > Place > Transform Sets Imprint Place > Place > Transform Sets Imprint Place > Place > Transform Sets Imprint Place > Place > Place > Transform Sets Imprint Place > Place > Place > Place > Transform Sets Imprint Place > Place > Place > Place > Transform Sets > Place >	Homo C	Configuration Monitoring Back	Forward Search	Refresh	Save Help			Casco System
/cs/y Reset	Features Interfaces Security Policy NAT Security Policy NAT VPN & Routing Building Elocts Building Elocts Building Elocts Properties	Configuration > Footures > VFN = Place Client Update Client Upda	Transform Sets Transform Sets Specify Transform Sets Specify Transform Sets Name avalanche ESP-DES-SHA ESP-DES-SHA ESP-JDES-MD5 ESP-AES-128-SHA ESP-JDES-MD5 ESP-AES-128-SHA ESP-AES-128-SHA ESP-AES-128-SHA ESP-AES-256-SHA ESP-AES-256-SHA ESP-AES-256-MD5	Node Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel	ESP Encryption DES DES JDES JDES AES-128 AES-128 AES-129 AES-192 AES-192 AES-192 AES-256 AES-256	ESP Authentication MD5 SHA MD5 SHA MD5 SHA MD5 SHA MD5 SHA MD5	AH Aufhentication None None None None None None None No	Add Edt Delete
Without a	Wittenie /		1		/dply	Reset		

11. Wählen Sie **Routing > Routing > Statische Route aus**, und wählen Sie eine statische Route zum Gateway-Router aus. In diesem Beispiel verweist die statische Route aus Gründen der Einfachheit auf den Remote-VPN-Peer.

Cisco ASDM SJ	0 for PIX - 10.1.1.1	te Holo						
Home C	Sonfiguration Montoring	Back Forward	Q C Search Ret	esh Save	? Help			Cisco Systems
Features	Configuration > Features > R	Routing > Routing > Static	Route					
Interfaces	GROUTING GROUTING	Static Route Specify static routes	10 Malance	Notes and	Outroaciti	Mahir	Terrented	
NAT ST	B SMUTCast B S IGMP B S PIM MRoute	autside 0.	0.0.0 0	100.0	172.17.63.230	Methic 1	No	Edit
Routing								
Building Blocks								
Properties								
Wizands /				Açı	W F	leset		
					cisco NA	7) 😡	4/6	05 3:39:35 PM AEST

Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- show crypto ipsec sa Zeigt die Sicherheitszuordnungen für Phase 2 an.
- show crypto isakmp sa Zeigt die Sicherheitszuordnungen für Phase 1 an.

Fehlerbehebung

Sie können ASDM verwenden, um die Protokollierung zu aktivieren und die Protokolle anzuzeigen.

- Wählen Sie Konfiguration > Eigenschaften > Protokollierung > Protokollierung Setup, wählen Sie Protokollierung aktivieren aus, und klicken Sie auf Übernehmen, um die Protokollierung zu aktivieren.
- Wählen Sie **Monitoring > Logging > Log Buffer > On Logging Level aus**, wählen Sie **Logging Buffer aus**, und klicken Sie auf **View**, um die Protokolle anzuzeigen.

Befehle zur Fehlerbehebung

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte show-Befehle.

Verwenden Sie das OIT, um eine Analyse der Ausgabe des Befehls show anzuzeigen.

Hinweis: Beachten Sie <u>vor der</u> Verwendung von **Debug-**Befehlen die <u>Informationen</u> zu <u>Debug-</u><u>Befehlen</u>.

- debug crypto ipsec Zeigt die IPsec-Aushandlungen für Phase 2.
- debug crypto isakmp Zeigt die ISAKMP-Verhandlungen für Phase 1.
- debug crypto engine Zeigt den verschlüsselten Datenverkehr an.
- clear crypto isakmp: Löscht die Sicherheitszuordnungen für Phase 1.
- clear crypto sa: Löscht die Sicherheitszuordnungen für Phase 2.
- debug icmp trace Zeigt, ob ICMP-Anfragen von den Hosts den PIX erreichen. Sie müssen den Befehl access-list hinzufügen, um ICMP in der Konfiguration zuzulassen, damit dieses Debuggen ausgeführt werden kann.
- 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 wird mit dem Befehl show log angezeigt.

Zugehörige Informationen

- Häufigste L2L- und Remote Access IPSec VPN-Lösungen zur Fehlerbehebung
- <u>Cisco PIX Firewall-Software</u>
- <u>Cisco Secure PIX Firewall Befehlsreferenzen</u>
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Anforderungen für Kommentare (RFCs)