SDM: Konfigurationsbeispiel für ein standortübergreifendes IPsec-VPN zwischen ASA/PIX und einem IOS-Router

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Zugehörige Produkte Konventionen Konfiguration Netzwerkdiagramm **ASDM-Konfiguration für VPN-Tunnel Router-SDM-Konfiguration ASA CLI-Konfiguration Router-CLI-Konfiguration** Überprüfen ASA/PIX Security Appliance - Befehle anzeigen Remote-IOS-Router - Anzeigen von Befehlen Fehlerbehebung Zugehörige Informationen

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für den LAN-to-LAN (Site-to-Site) IPsec-Tunnel zwischen Cisco Security Appliances (ASA/PIX) und einem Cisco IOS-Router. Zur Vereinfachung werden statische Routen verwendet.

Weitere Informationen zum Szenario, in dem die PIX/ASA Security Appliance die Softwareversion *7.x* ausführt, finden Sie unter <u>PIX/ASA 7.x Security Appliance für einen IOS-Router, LAN-zu-LAN-IPsec-Tunnel</u>, in <u>Konfigurationsbeispiel</u>.

Voraussetzungen

<u>Anforderungen</u>

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Vor Beginn dieser Konfiguration muss eine End-to-End-IP-Verbindung eingerichtet werden.
- Die Security Appliance-Lizenz muss für die DES-Verschlüsselung (Data Encryption Standard) aktiviert werden (mindestens auf Verschlüsselungsebene).

Verwendete Komponenten

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

- Cisco Adaptive Security Appliance (ASA) ab Version 8.x
- ASDM ab Version 6.x
- Cisco 1812-Router mit Cisco IOS® Softwareversion 12.3
- Cisco Security Device Manager (SDM) Version 2.5

Hinweis: Informationen zur Konfiguration der ASA durch den ASDM finden Sie unter <u>Zulassen von</u> <u>HTTPS-Zugriff für ASDM</u>.

Hinweis: Informationen zur Konfiguration des Routers mithilfe von SDM finden Sie unter <u>Basic</u> <u>Router Configuration</u> (Basiskonfiguration des Routers).

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.

Hinweis: Weitere Informationen finden Sie unter <u>Configuration Professional: Site-to-Site-IPsec-</u> <u>VPN zwischen ASA/PIX und einem IOS-Router - Konfigurationsbeispiel</u> für eine ähnliche Konfiguration mit Cisco Configuration Professional auf dem Router.

Zugehörige Produkte

Diese Konfiguration kann auch mit der Cisco Security Appliance der Serie PIX 500 verwendet werden, die Version 7.x und höher ausführt.

Konventionen

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

Konfiguration

Netzwerkdiagramm

In diesem Dokument wird die in diesem Diagramm dargestellte Netzwerkeinrichtung verwendet.



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind <u>RFC 1918</u> -Adressen, die in einer Laborumgebung verwendet werden.

- ASDM-Konfiguration für VPN-Tunnel
- Router-SDM-Konfiguration
- ASA CLI-Konfiguration
- Router-CLI-Konfiguration

ASDM-Konfiguration für VPN-Tunnel

Gehen Sie wie folgt vor, um den VPN-Tunnel zu erstellen:

1. Öffnen Sie Ihren Browser, und geben Sie https://<IP_Adresse der ASA-Schnittstelle ein, die für ASDM Access konfiguriert wurde>, um auf das ASDM auf der ASA zuzugreifen.Achten Sie darauf, alle Warnungen zu autorisieren, die Ihr Browser bezüglich der Authentizität von SSL-Zertifikaten ausgibt. Standardmäßig sind Benutzername und Kennwort leer.Die ASA präsentiert dieses Fenster, um den Download der ASDM-Anwendung zu ermöglichen. In diesem Beispiel wird die Anwendung auf den lokalen Computer geladen und nicht in einem Java-Applet ausgeführt.



- 2. Klicken Sie auf **ASDM Launcher herunterladen und ASDM starten**, um das Installationsprogramm für die ASDM-Anwendung herunterzuladen.
- 3. Wenn der ASDM Launcher heruntergeladen wurde, führen Sie die Schritte aus, die von den Aufforderungen zur Installation der Software und Ausführung des Cisco ASDM Launchers ausgeführt werden.
- 4. Geben Sie die IP-Adresse für die Schnittstelle ein, die Sie mit dem Befehl http konfiguriert haben, sowie einen Benutzernamen und ein Kennwort, wenn Sie einen Befehl angegeben haben. In diesem Beispiel wird cisco123 als Benutzername und cisco123 als Kennwort

	Cisco ASDM Launch	er v1.5(30)	
		cisco	
	Device IP Address / Name:	10.77.241.111	v
	Username:	cisco123	
	Password:	* * * * * * *	
	📃 Run in Demo Mode		
		OK Close	
verwendet.		. 0	1 🗐 🗐

5. Führen Sie den IPsec VPN Wizard aus, sobald die ASDM-Anwendung eine Verbindung mit der ASA herstellt

nerstent.										
🖆 Cisco ASDM 6.	1 for AS	k - 10.77.3	841.111							
File View Tools	Wizards	Window H	telp	L	ook Fo	re-		Go		du.
Home % Cor	Sta	tup Wizard				Back 🌔 F	orward ? He	slp als	CIS	co
	IPse	ac VPN Wizard	i	N			0			
nome	SSL	VPN Wizard.		W5		1				
E Device Dasi	High	n Availability a	and Scalability W	Azard	ncion					
Device Informa	Pac	ket Capture V	Vizard			Interface Sta	tus			
General Licens	e					Interface	IP Address/	Mask	Line	Li
Hast Barray		defende de	and the second of			dmz	10.77.241.1	11/26	🕤 up	0
Host Name:	ciscoasa	.derault.do	main.invalid			inside	10.10.10.1/2	24	😧 up	0
ASA version:	8.0(2)	Device Upt	me: 14d 3h 1	m 515		outside	172.16.1.1/2	24	😧 up	0
ASDM Version:	6.1(3)	Device Typ	e: ASA 551	D						
Firewall Mode:	Routed	Context M	ode: Single							
Total Flash:	64 MB	Total Memo	ry: 256 MB			Select an interfe	aca to view input	and output	Khoc	
· · · · · · · · · · · · · · · · · · ·					, 	Select an intern	ace to view input	and output	Nups	
VPN Tunnels						Traffic Status				
IKE: 0 IPSec: 0	Clientle:	ss SSL VPN: O	SSL VPN Clier	nt: O <u>Details</u>		Connections P	er Second Usage			
System Resour	ces Statu	5								
CPU CPU	Usage (per	cent)								
100) <u> </u>									
0% 50	,					20:41	20:42	20:43	20	:44
						UDP: 0	TCP: 0	Total: 0		×
				cisco123	15		🛃 🔼	4	/6/09 8:45:4	12 PM UTC

6. Wählen Sie den Site-to-Site-IPsec VPN-Tunneltyp aus, und klicken Sie auf Weiter, wie hier gezeigt.

🖆 VPN Wizard	
VPN Wizard	VPN Tunnel Type (Step 1 of)
Branch Branch Freidig	Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM.
Corporate	VPN Tunnel Type: Site-to-Site VPN
THE REAL	⊙ <u>SRe-to-Site</u>
	Remote Access Remote Remote
	VPN Tunnel Interface:
	Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.
	< Back Next > Finish Cancel Help

7. Geben Sie die externe IP-Adresse des Remote-Peers an. Geben Sie die zu verwendenden Authentifizierungsinformationen ein, d. h. den vorinstallierten Schlüssel in diesem Beispiel. Der in diesem Beispiel verwendete vorinstallierte Schlüssel ist cisco123. Der Tunnelgruppenname ist standardmäßig Ihre externe IP-Adresse, wenn Sie L2L VPN konfigurieren. Klicken Sie auf Weiter.

🖆 VPN Wizard		×
VPN Wizard	Remote Site Peer (Step 2 of 6)	
VPN VVIZAIO	Remote Site Peer (Step 2 of 6) Configure the IP address of the peer device, authentication method and the tunnel group for this site-to-site tunnel. Peer IP Address: 172.17.1.1 Authentication Method • Pre-shared key Pre-Shared Key: clsco123 • Certificate Certificate Certificate Signing Algorithm: rsa-sig Certificate Name: • • Challenge/response authentication (CRACK) For site-to-site connections with pre-shared key authentication, the tunnel group name must be the same as either the peer IP address or the peer hostname, whichever is used as the peer's identity. Tunnel Group Name: 172.17.1.1	
	< Back Next > Finish Cancel Help)

8. Geben Sie die Attribute für IKE an, die auch als Phase 1 bezeichnet werden. Diese Attribute müssen auf dem ASA-Router und dem IOS-Router identisch sein. Klicken Sie auf **Weiter**.

🖆 VPN Wizard		×			
VPN Wizard	IKE Policy (Step 3 of 6)				
Branch Branch ISP Horeve Corporate	Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.				
Notwork he	Encryption: DES				
A A A A A A A A A A A A A A A A A A A	Authentication: SHA				
	DH Group:				
	< Back Next Finish Cancel He	P			

 Geben Sie die Attribute an, die f
ür IPsec verwendet werden sollen, auch als Phase 2 bezeichnet. Diese Attribute m
üssen auf dem ASA- und dem IOS-Router
übereinstimmen. Klicken Sie auf Weiter.

🖆 VPN Wizard		×
VPN Wizard	IPsec Encryption and Authentication (Step 4 of 6)	
Proventier of the second secon	Select the encryption and authentication algorithms for this IPsec VPN tunnel. Configurations on both sides of the connection must match exactly.	
	< Back Next > Finish Cancel Help]

10. Geben Sie die Hosts an, deren Datenverkehr den VPN-Tunnel passieren darf. In diesem Schritt müssen Sie die **lokalen** und **Remote-Netzwerke** für den VPN-Tunnel bereitstellen. Klicken Sie auf die Schaltfläche neben **Lokale Netzwerke** wie hier gezeigt, um die lokale Netzwerkadresse aus der Dropdown-Liste auszuwählen.

🖆 VPN Wizard		×
VPN Wizard	Hosts and Networks (Step 5 of 6)	
Branch Franch ISP	An IPsec tunnel protects data exchanged by selected hosts and networks at the local and remote sites. Please identify hosts and networks to be used in the IPsec tunnel.	
	Action: Protect Do not Protect	
Home	Local Networks: any	
Network	Remote Networks: any	
	Exempt ASA side host/network from address translation:	
	< Back Next > Finish Cancel Help]

11. Wählen Sie die Adresse des **lokalen Netzwerks aus**, und klicken Sie dann auf **OK**, wie hier gezeigt.

📬 Browse Local Netw	vorks			
💠 Add 🝷 📝 Edit 🗊	Delete Q			
Filter:				Filter Clear
Name	1 IP Address	Netmask	Description	
Network Objects				
iny 👋 any	0.0.0	0.0.0		
🚽 📑 dmz-network	10.77.241.64	255.255.255.192		
nside-network	10.10.10.0	255.255.255.0		
i	rk 172.16.1.0	255.255.255.0		
Selected Local Networks				
Local Networks ->	any			
			0	Cancel

12. Klicken Sie auf die Schaltfläche neben **Remote Networks (Remote-Netzwerke)** wie hier gezeigt, um die Remote-Netzwerkadresse aus der Dropdown-Liste auszuwählen.

🖆 VPN Wizard		
VPN Wizard	Hosts and Networks	(Step 5 of 6)
Branch	An IPsec tunnel protects remote sites. Please iden	data exchanged by selected hosts and networks at the local and htify hosts and networks to be used in the IPsec tunnel.
	Action:	Protect O Do not Protect
Home	Local Networks: in	nside-network/24 📖
Corporte	Remote Networks: a	ny R
	Event ASA side bo	rt/network from address translation:
	Compension side no	
		< Back Next > Finish Cancel Help

13. Wählen Sie die **Remote Network**-Adresse aus, und klicken Sie dann auf **OK**, wie hier gezeigt.**Hinweis:** Wenn das Remote-Netzwerk nicht in der Liste enthalten ist, muss das Netzwerk der Liste durch Klicken auf **Hinzufügen** hinzugefügt werden.

🖆 Browse Remote Netv	vorks			
🗣 Add 🝷 📝 Edit 👔 (Delete 🔍			
Filter:				Filter Clear
Name ^1	IP Address	Netmask	Description	
Network Objects				
	0.0.0.0	0.0.0.0		
🔤 🚽 🔤 🔤 🔤	10.77.241.64	255.255.255.192		
🙀 inside-network	10.10.10.0	255.255.255.0		
👰 outside-network	172.16.1.0	255.255.255.0		
i- 🔂 10.20.10.0	10.20.10.0	255.255.255.0		
Remote Networks				
Remote Networks ->				
			<u> </u>	Cancel

14. Aktivieren Sie das Kontrollkästchen **ASA-seitigen Host/Netzwerk von Adressenumwandlung ausnehmen**, um zu verhindern, dass der Tunnelverkehr Network Address Translation durchläuft. Klicken Sie anschließend auf **Weiter**.

🖆 VPN Wizard		
VPN Wizard	Hosts and Networks	(Step 5 of 6)
Branch	An IPsec tunnel protec remote sites. Please id	cts data exchanged by selected hosts and networks at the local and ientify hosts and networks to be used in the IPsec tunnel.
	Action:	Protect: O Do not Protect
Home	Local Networks:	inside-network/24
Corporate Network	Remote Networks:	10.20.10.0/24
	✓ Exempt ASA side	host/network from address translation:
		Cancel Hate

15. Die vom VPN-Assistenten definierten Attribute werden in dieser Zusammenfassung angezeigt. Überprüfen Sie die Konfiguration erneut, und klicken Sie auf **Fertig stellen**, wenn die Einstellungen korrekt sind.



Router-SDM-Konfiguration

Gehen Sie wie folgt vor, um den Site-to-Site-VPN-Tunnel auf dem Cisco IOS-Router zu konfigurieren:

 Öffnen Sie Ihren Browser, und geben Sie https://<IP_Address der Schnittstelle des Routers ein, der für SDM Access konfiguriert wurde>, um auf das SDM auf dem Router zuzugreifen.Achten Sie darauf, alle Warnungen zu autorisieren, die Ihr Browser bezüglich der Authentizität von SSL-Zertifikaten ausgibt. Standardmäßig sind Benutzername und Kennwort leer.Der Router zeigt dieses Fenster an, um das Herunterladen der SDM-Anwendung zu ermöglichen. In diesem Beispiel wird die Anwendung auf den lokalen Computer geladen und nicht in einem Java-Applet ausgeführt.



- 2. Der SDM-Download beginnt jetzt. Wenn der SDM-Launcher heruntergeladen wurde, führen Sie die Schritte aus, die von den Aufforderungen angewiesen werden, um die Software zu installieren und den Cisco SDM Launcher auszuführen.
- 3. Geben Sie den **Benutzernamen** und das **Passwort ein**, wenn Sie diesen eingegeben haben, und klicken Sie auf **OK**.In diesem Beispiel wird **cisco123** als Benutzername und **cisco123** als

A	uthenticati	on Required	×
	ن Java		
	Enter login det /10.77.241.10	ails to access level_15 or view_access on 9:	
	User name:	cisco123	
	Password:	•••••	
	Save this p	assword in your password list	
		OK Cancel	
	Authentication	scheme: Basic	

Kennwort verwendet.

4. Wählen Sie Konfiguration > VPN > Site-to-Site VPN, und klicken Sie auf das Optionsfeld

neben Create a Site-to-Site VPN (Site-to-Site-VPN erstellen) auf der SDM-Startseite. Klicken Sie anschließend auf Ausgewählten Task starten, wie hier

gezeigt:



5. Wählen Sie **Schritt-für-Schritt-Assistent**, um mit der Konfiguration fortzufahren:



6. Geben Sie im nächsten Fenster die VPN-Verbindungsinformationen in den entsprechenden Räumen an. Wählen Sie die Schnittstelle des VPN-Tunnels aus der Dropdown-Liste aus. Hier wird FastEthernet0 ausgewählt. Wählen Sie im Abschnitt Peer Identity (Peer-Identität) die Option Peer with static IP address (Peer mit statischer IP-Adresse) aus, und geben Sie die IP-Adresse des Remote-Peers an. Geben Sie dann den Pre-shared Key (cisco123 in diesem Beispiel) im Authentifizierungsbereich wie gezeigt ein. Klicken Sie anschließend auf Weiter.

Site-to-Site VPN Wizard	
VPN Wizard	VPN Connection Information Select the interface for this VPN connection: FastEthernet0
	Peer Identity Select the type of peer(s) used for this VPN connection: Enter the IP address of the remote peer: 172.16.1.1
	Authentication Authentication ensures that each end of the VPN connection uses the same secret key.
NA	Pre-shared Keys Digital Certificates Re-enter Key:
	<back next=""> Finish Cancel Help</back>

7. Klicken Sie auf **Hinzufügen**, um IKE-Vorschläge hinzuzufügen, die den Verschlüsselungsalgorithmus, den Authentifizierungsalgorithmus und die Key Exchange-Methode

angeben.

Site-to-Site VPN Wizard	
VPN Wizard	IKE Proposals IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below. Click the Add button to add more policies and the Edit button to edit an existing policy.
	Priority Encryption Hash D-H Group Authentication Type
	Add Edit
	Back Next > Finish Cancel Help

8. Stellen Sie Verschlüsselungsalgorithmus, Authentifizierungsalgorithmus und die Exchange-Methode wie hier gezeigt bereit, und klicken Sie dann auf OK. Die Werte Encryption Algorithm, Authentication Algorithm und Key Exchange sollten mit den in der ASA bereitgestellten Daten

ubere	einstimmen.	

Add IKE Policy	
Configure IKE Policy	
Priority:	Authentication:
1	PRE_SHARE
Encryption:	D-H Group:
DES 🔽	group2
Hash:	Lifetime:
SHA_1	24 0 0 HH:MM:SS
QK	Cancel Help

9. Klicken Sie auf Weiter, wie hier

gezeigt.							
Site-to-Site VPN Wizard							×
VPN Wizard	IKE Proposals IKE proposals method that is device. For the device should I Click the Add	specify the enc used by this ro VPN connectio be configured v . button to add	ryption algorith uter when nego n to be establis vith at least one more policies a	m, authenticati otiating a VPN o shed with the re a of the policies and the Edit b	on algorithm an connection with t emote device, the elisted below. outton to edit an e	d key exchange he remote e remote existing policy.	
	Priority 1 2	Encryption 3DES DES	Hash SHA_1 SHA_1	D-H Group group2 group1	Authentication PRE_SHARE PRE_SHARE	Type User Defined User Defined	
1)							
	Add	Edit					
				r Back Nord	Tinich		

10. In diesem neuen Fenster sollten die Details zum Konfigurationssatz angegeben werden. Das Transform Set legt die Verschlüsselungs- und Authentifizierungsalgorithmen fest, die zum Schutz von Daten im VPN-Tunnel verwendet werden. Klicken Sie anschließend auf Hinzufügen, um diese Details anzugeben. Sie können nach Bedarf eine beliebige Anzahl Transform Sets hinzufügen, indem Sie auf Hinzufügen klicken und die Details angeben.

Site-to-Site VPN Wizard					×
VPN Wizard	Transform Set A transform set specifies the data in the VPN tunnel. Since communicate, the remote de one selected below. Click the Add button to add transform set. Select Transform Set SDM Default Transform Details of the specified tra	encryption and aut the two devices m vice must be config a new transform se n Set snsform set	hentication algorithm ust use the same alg ured with the same t et and the Edit butto	ns used to protect the gorithms to transform set as the on to edit the specified	1
	Select Transform Set	n Set 💽 Insform set ESP Encryption ESP_3DES	ESP Integrity ESP_SHA_HMAC	AH Integrity	
	Ada			•	
		< [Back Next > Fini	ish Cancel He	lp

11. Geben Sie die Details zum **Transform Set (Verschlüsselungs- und Authentifizierungsalgorithmus)** an, und klicken Sie wie gezeigt auf

Ad	d Transform Set 🛛 🛛 🔀
Na	ame: ASA-IPSEC
	✓ Data integrity with encryption (ESP)
	Integrity Algorithm: ESP_SHA_HMAC 💌
	Encryption Algorithm: ESP_DES
	Show Advanced >>
	OK Cancel Hein

12. Wählen Sie den erforderlichen **Transform Set** aus der Dropdown-Liste aus, wie gezeigt.

13. Klicken Sie auf Weiter.

Site-to-Site VPN Wizard					×
VPN Wizard	Transform Set A transform set specifies the e data in the VPN tunnel. Since the communicate, the remote deviation one selected below. Click the Add button to add a transform set. Select Transform Set ASA-IPSEC Details of the specified training	ncryption and auth he two devices mo ice must be config new transform se	hentication algorithm ust use the same alg ured with the same t It and the Edit butto	is used to protect the porithms to transform set as the in to edit the specified	8
	AsA-IPSEC	Isform set	ESP Integrity ESP_SHA_HMAC	AH Integrity	
		« [Back Next > Fini	sh Cancel He	lp

14. Geben Sie im folgenden Fenster die Details zum Datenverkehr an, der über den VPN-Tunnel geschützt werden soll. Geben Sie die Quell- und Zielnetzwerke des zu schützenden Datenverkehrs an, sodass der Datenverkehr zwischen den angegebenen Quell- und Zielnetzwerken geschützt ist. In diesem Beispiel ist das Quellnetzwerk 10.20.10.0 und das Zielnetzwerk 10.10.10.0. Klicken Sie anschließend auf Weiter.

Site-to-Site VPN Wizard					
Site-to-Site VPN Wizard VPN Wizard	Traffic to protect IPSec rules define the traffic, such as file transfers (FTP) and e-mail (SMTP) that will be protected by this VPN connection. Other data traffic will be sent unprotected to the remote device. You can protect all traffic between a particular source and destination subnet, or specify an IPSec rule that defines the traffic types to be protected. Protect all traffic between the following subnets Local Network Enter the IP address and subnet mask of the network where IPSec traffic originates. IP Address: 10.20.10.0 Subnet Mask: 255.255.255.0 or 24 Create/Select an access-list for IPSec traffic				
		Back Next > Finish Cancel Heln			
		Back Net > Finish Cancel Help			

15. In diesem Fenster wird die Zusammenfassung der fertig gestellten Site-to-Site-VPN-Konfiguration angezeigt. Aktivieren Sie das Kontrollkästchen VPN-Verbindung testen nach der Konfiguration, wenn Sie die VPN-Verbindung testen möchten. Hier ist das Kontrollkästchen aktiviert, da die Verbindung aktiviert werden muss. Klicken Sie anschließend auf Fertig stellen.

Site-to-Site VPN Wizard						
VPN Wizard	Summary of the	Configuration				
	Click Finish to de Interface:FastEt Peer Device:17: Authentication T pre-shared key: IKE Policies: Hash SHA_1 SHA_1 Transform Sets Name: ESP Er ESP In Mode:T	eliver the configuration to hernet0 2.16.1.1 Type : Pre-shared key DH Group group1 group2 : ASA-IPSEC ncryption:ESP_DES tegrity:ESP_SHA_HMAC TUNNEL	Authentication PRE_SHARE PRE_SHARE	Encryption DES 3DES		
	Test VPN con	inectivity after configuring	LÎ.			
			< Back Next >	Finish	Cancel	Help

16. Klicken Sie auf **Start**, um die VPN-Verbindung zu überprüfen.

VPN Troubleshooting		
Tunnel Details		
Interface: FastEthernet0	Peer: 172.16.1.1	
	🔳 Summary	😰 Details
Activity		Status
	Decomposed of the (a)	
Failure Reason(s)	Recommended Action(s)	
Start Save Report	Close	Help

17. Im nächsten Fenster wird das Ergebnis des VPN-Verbindungstests bereitgestellt. Hier können Sie sehen, ob der Tunnel oben oder unten ist. In dieser Beispielkonfiguration ist der Tunnel nach oben wie in grün dargestellt.

VPN Troubleshooting		
Tunnel Details		
Interface: FastEthernet0	Peer: 172.16.1.1	
1		
	🔲 Summary	🕰 Details
Activity		Status
Checking the tunnel status		⊖Up
Failure Reason(s)	Recommended Action(s)	
Start Core Banait	Close	Holp
Start Save Report		Help

Damit ist die Konfiguration auf dem Cisco IOS-Router abgeschlossen.

ASA CLI-Konfiguration



encrypted ftp mode passive dns server-group DefaultDNS domain-name default.domain.invalid access-list 100 extended permit ip any any access-list inside_nat0_outbound extended permit ip 10.10.10.0 255.255.255.0 10.20.10.0 255.255.255.0 !--- This access list (inside_nat0_outbound) is used !--- with the **nat zero** command. This prevents traffic which !--- matches the access list from undergoing network address translation (NAT). !--- The traffic specified by this ACL is traffic that is to be encrypted and !--sent across the VPN tunnel. This ACL is intentionally !--- the same as (outside_1_cryptomap). !--- Two separate access lists should always be used in this configuration. access-list outside_1_cryptomap extended permit ip 10.10.10.0 255.255.255.0 10.20.10.0 255.255.255.0 !--- This access list (outside_cryptomap) is used !--with the crypto map **outside_map** !--- to determine which traffic should be encrypted and sent !--- across the tunnel. !--- This ACL is intentionally the same as (inside_nat0_outbound). !--- Two separate access lists should always be used in this configuration. pager lines 24 mtu inside 1500 mtu outside 1500 no failover asdm image disk0:/asdm-613.bin asdm history enable arp timeout 14400 global (outside) 1 interface nat (inside) 1 10.10.10.0 255.255.255.0 nat (inside) 0 access-list inside_nat0_outbound !--- NAT 0 prevents NAT for networks specified in !--the ACL inside_nat0_outbound. access-group 100 in interface outside route outside 0.0.0.0 0.0.0.0 172.16.1.2 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute http server enable http 0.0.0.0 0.0.0.0 dmz no snmp-server location no snmp-server contact !--- PHASE 2 CONFIGURATION ---! !--- The encryption types for Phase 2 are defined here. crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac !--- Define the transform set for Phase 2. crypto map outside_map 1 match address outside_1_cryptomap !--- Define which traffic should be sent to the IPsec peer. crypto map outside_map 1 set peer 172.17.1.1 !--- Sets the IPsec peer crypto map outside_map 1 set



Router-CLI-Konfiguration

Router
Puilding configuration
Current configuration : 2403 bytes
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!

boot-start-marker boot-end-marker no logging buffered 1 username cisco123 privilege 15 password 7 1511021F07257A767B no aaa new-model ip subnet-zero 1 ! ip cef ip ips po max-events 100 no ftp-server write-enable !--- Configuration for IKE policies. !--- Enables the IKE policy configuration (config-isakmp) !--- command mode, where you can specify the parameters that !--- are used during an IKE negotiation. Encryption and Policy details are hidden as the default values are chosen. crypto isakmp policy 2 authentication pre-share !--- Specifies the pre-shared key "cisco123" which should !--- be identical at both peers. This is a global !--- configuration mode command. crypto isakmp key cisco123 address 172.16.1.1 !--- Configuration for IPsec policies. !--- Enables the crypto transform configuration mode, !--- where you can specify the transform sets that are used !--- during an IPsec negotiation. crypto ipsec transform-set ASA-IPSEC esp-des esp-sha-hmac !--- !--- Indicates that IKE is used to establish !--the IPsec Security Association for protecting the !--traffic specified by this crypto map entry. crypto map SDM_CMAP_1 1 ipsec-isakmp description Tunnel to172.16.1.1 !--- !--- Sets the IP address of the remote end. set peer 172.16.1.1 !--- !--- Configures IPsec to use the transform-set !---"ASA-IPSEC" defined earlier in this configuration. set transform-set ASA-IPSEC !--- !--- Specifies the interesting traffic to be encrypted. match address 100 1 1 !--- Configures the interface to use the !--- crypto map "SDM_CMAP_1" for IPsec. interface FastEthernet0 ip address 172.17.1.1 255.255.255.0 duplex auto speed auto crypto map SDM_CMAP_1 1 interface FastEthernet1 ip address 10.20.10.2 255.255.255.0

```
duplex auto
 speed auto
interface FastEthernet2
no ip address
!
interface Vlan1
ip address 10.77.241.109 255.255.255.192
1
ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.233.0 255.255.255.0 10.77.241.65
ip route 172.16.1.0 255.255.255.0 172.17.1.2
1
ip nat inside source route-map nonat interface
FastEthernet0 overload
ip http server
ip http authentication local
ip http secure-server
1
!--- Configure the access-lists and map them to the
Crypto map configured. access-list 100 remark SDM_ACL
Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
!--- This ACL 110 identifies the traffic flows using
route map access-list 110 deny ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 110 permit ip 10.20.10.0 0.0.0.255 any
route-map nonat permit 10
match ip address 110
1
control-plane
!
1
line con 0
login local
line aux 0
line vty 0 4
privilege level 15
 login local
 transport input telnet ssh
1
end
```

<u>Überprüfen</u>

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**.

- PIX Security Appliance show Commands
- Remote-IOS-Router Anzeigen von Befehlen

ASA/PIX Security Appliance - Befehle anzeigen

• show crypto isakmp sa - Zeigt alle aktuellen IKE-SAs in einem Peer an. ASA#show crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 172.17.1.1 Type : L2L Role : initiator Rekey State : MM_ACTIVE : no show crypto ipsec sa - Zeigt alle aktuellen IPsec-SAs in einem Peer an. ASA#show crypto ipsec sa interface: outside Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1 local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0) current_peer: 172.17.1.1 #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9 #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.1.1 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: 434C4A7F inbound esp sas: spi: 0xB7C1948E (3082917006) transform: esp-des esp-sha-hmac none in use settings ={L2L, Tunnel, PFS Group 2, } slot: 0, conn_id: 12288, crypto-map: outside_map sa timing: remaining key lifetime (kB/sec): (4274999/3588) IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0x434C4A7F (1129073279) transform: esp-des esp-sha-hmac none in use settings ={L2L, Tunnel, PFS Group 2, } slot: 0, conn_id: 12288, crypto-map: outside_map sa timing: remaining key lifetime (kB/sec): (4274999/3588) IV size: 8 bytes replay detection support: Y

Remote-IOS-Router - Anzeigen von Befehlen

• show crypto isakmp sa - Zeigt alle aktuellen IKE-SAs in einem Peer an. Router#show crypto isakmp sa

dst	src	state	conn-id	slot	status
172.17.1.1	172.16.1.1	QM_IDLE	3	0	ACTIVE

• show crypto ipsec sa - Zeigt alle aktuellen IPsec-SAs in einem Peer an.

```
Router#show crypto ipsec sa
interface: FastEthernet0
   Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1
  protected vrf: (none)
  local ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
  current peer 172.16.1.1 port 500
     PERMIT, flags={origin_is_acl,}
  #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68
    #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
     path mtu 1500, ip mtu 1500
     current outbound spi: 0xB7C1948E(3082917006)
     inbound esp sas:
      spi: 0x434C4A7F(1129073279)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
       conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3004)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0xB7C1948E(3082917006)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3002)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
     outbound ah sas:
```

outbound pcp sas:

 show crypto engine connections active - Zeigt aktuelle Verbindungen und Informationen über verschlüsselte und entschlüsselte Pakete (nur Router).
 Router#show crypto engine connections active

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
3	FastEthernet0	172.17.1.1	set	HMAC_SHA+DES_56_CB	0	0
2001	FastEthernet0	172.17.1.1	set	DES+SHA	0	59
2002	FastEthernet0	172.17.1.1	set	DES+SHA	59	0

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

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**.

Hinweis: Lesen Sie die <u>wichtigen Informationen zu Debug-Befehlen</u> und <u>IP-</u> <u>Sicherheitsfehlerbehebung - Verwenden von Debugbefehlen</u>, bevor Sie **Debug-**Befehle verwenden.

- debug crypto ipsec 7: Zeigt die IPsec-Aushandlungen für Phase 2 an. debug crypto isakmp 7: Zeigt die ISAKMP-Verhandlungen für Phase 1 an.
- debug crypto ipsec: Zeigt die IPsec-Aushandlungen für Phase 2 an. debug crypto isakmp: Zeigt die ISAKMP-Verhandlungen für Phase 1 an.

Weitere Informationen zur Fehlerbehebung für Site-VPNs finden Sie unter <u>Häufigste L2L- und</u> <u>Remote Access IPSec VPN-Problemlösung</u>.

Zugehörige Informationen

- <u>Cisco PIX Firewall-Software</u>
- <u>Cisco Adaptive Security Device Manager</u>
- <u>Cisco Adaptive Security Appliances der Serie ASA 5500</u>
- <u>Configuration Professional: Konfigurationsbeispiel für ein standortübergreifendes IPsec-VPN</u>
 <u>zwischen ASA/PIX und einem IOS-Router</u>
- <u>Cisco Secure PIX Firewall Befehlsreferenzen</u>
- <u>Cisco Router- und Security Device Manager</u>
- Anforderungen für Kommentare (RFCs)
- <u>Technischer Support und Dokumentation Cisco Systems</u>