dm: Site-to-Site IPsec VPN tussen ASA/PIX en een IOS routerconfiguratievoorbeeld

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Verwante producten Conventies Configuratie Netwerkdiagram VPN-tunnelconfiguratie ASDM Configuratie van routerdm ASA CLI-configuratie Configuratie van router CLI Verifiëren ASA/PIX security applicatie - show Opdrachten Remote IOS-router - toont opdrachten Problemen oplossen Gerelateerde informatie

Inleiding

Dit document biedt een voorbeeldconfiguratie voor de LAN-to-LAN (Site-to-Site) IPsec-tunnel tussen Cisco security applicaties (ASA/PIX) en een Cisco IOS-router. Statische routes worden gebruikt voor eenvoud.

Raadpleeg <u>PIX/ASA 7.x security applicatie voor een IOS Router LAN-to-LAN IPsec Tunnel</u> <u>Configuration Voorbeeld</u> om meer te weten te komen over hetzelfde scenario waarin PIX/ASA security applicatie softwareversie *7.x* uitvoert.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

• End-to-end IP connectiviteit moet vóór het beginnen van deze configuratie worden vastgesteld.

• De Security Appliance-licentie moet worden ingeschakeld voor Data Encryption Standard (DES) encryptie (op een minimaal coderingsniveau).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco adaptieve security applicatie (ASA) met versie 8.x en hoger
- ASDM versie 6.x en hoger
- Cisco 1812 router met Cisco IOS® softwarerelease 12.3
- Cisco Security apparaat Manager (DSM) versie 2.5

Opmerking: Raadpleeg <u>HTTPS-toegang voor ASDM</u> om de ASA te kunnen configureren door de ASDM.

Opmerking: Raadpleeg de <u>basisrouterconfiguratie met behulp van</u> een<u>dm</u> om de router door een dm te laten configureren.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Opmerking: Raadpleeg <u>Configuration Professional: Site-to-Site IPsec VPN tussen ASA/PIX en</u> <u>een IOS routerconfiguratievoorbeeld</u> voor een soortgelijke configuratie met Cisco Configuration Professional op de router.

Verwante producten

Deze configuratie kan ook worden gebruikt met de Cisco PIX 500 Series security applicatie, die versie 7.x en hoger uitvoert.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configuratie

Netwerkdiagram

Dit document gebruikt de netwerkinstellingen die in dit diagram worden weergegeven.



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn <u>RFC 1918</u> adressen, die in een labomgeving gebruikt zijn.

- VPN-tunnelconfiguratie ASDM
- <u>Configuratie van routerdm</u>
- ASA CLI-configuratie
- Configuratie van router CLI

VPN-tunnelconfiguratie ASDM

Voltooi deze stappen om de VPN-tunnel te maken:

 Open uw browser en voer https://<IP_Address van de interface van ASA in die is geconfigureerd voor ASDM Access>om toegang te krijgen tot de ASDM in de ASA.Controleer of alle waarschuwingen die uw browser u geeft, behoren tot de SSLcertificatie. De standaard gebruikersnaam en wachtwoord zijn beide leeg.De ASA presenteert dit venster om het downloaden van de ASDM-toepassing mogelijk te maken. Dit voorbeeld laadt de toepassing op de lokale computer en werkt niet in een Javaapplet.



- 2. Klik op **Download ASDM Launcher en Start ASDM** om de installateur voor de ASDMtoepassing te downloaden.
- 3. Voltooi na het downloaden van de ASDM Launcher de stappen die door de aanwijzingen zijn geleid om de software te installeren en de Cisco ASDM Launcher uit te voeren.
- 4. Voer het IP-adres in voor de interface die u met de http opdracht en een gebruikersnaam en wachtwoord hebt ingesteld als u er een hebt opgegeven.Dit voorbeeld gebruikt cisco123 voor de gebruikersnaam en cisco123 als het

🕵 Cisco ASDM Launch	er v1.5(30)	
		cisco
Device IP Address / Name:	10.77.241.111	•
Username:	cisco123	
Password:	* * * * * * *	
🔲 Run in Demo Mode		
	0	🗎 👙 🖯

- wachtwoord.
- 5. Start de **IPsec VPN-wizard** nadat de ASDM-toepassing is aangesloten op de ASA.

🖆 Cisco ASDM 6.1 for ASA - 10.77.241.111					(
File View Tools Wizards Window Help	Loc	ok Fo	r:		<u>م</u>	aha
Home 🖧 Cor Startup Wizard		6	Back 🌔 F	orward 🤣 Help 🚽	CI	sco
IPsec VPN Wizard				3		
SSL VPN Wizard	15		1			
High Availability and Scalabilit	y Wizard	icion				-
Device Informa Packet Capture Wizard			Interface Stal	tus		
General License			Interface	IP Address/Mask	Line	Li
Hort Name: circoaca default domain inval	id.		dmz	10.77.241.111/26	O up	0
A50 Version: 8-0(2) Device Untime: 14d 3	h 1m 51s		inside	10.10.10.1/24	O up	0
ASDM Version: 6.1(3) Device Type: ASA 5	510		outside	172.16.1.1/24	Up Up	
Firewall Mode: Routed Context Mode: Single	,					
Total Flash: 64 MB Total Memory: 256 M	в					
			Select an interfa	ace to view input and ou	itput Kbps	
VON Turpede			Tuaffic Shabue			
TVE 0 TDSec 0 Clanting SSI VDV 0 SSI VDV/	Boot: 0 Details		-Connections D	av Cassad Llavan		
INC. O IPSEL O CIENCESS SSE TPN. O SSE TPN.			Connections M	er second usage		
System Resources Status						
CPU CPU Usage (percent)						
100						
			20.41	20.42	0.49	20-44
096 50			UDP: 0	TCP: 0 Total	:0	.0.44
	:				2	<u> </u>
	cisco123	15		🖾 🔟 🛛	5] 4/6/09 8:45	5:42 PM UTC

6. Kies het tunneltype **Site-to-Site** IPsec VPN en klik op **Volgende** zoals hier wordt getoond.

🖆 VPN Wizard	
VPN Wizard	VPN Tunnel Type (Step 1 of)
Branch Pranch Provide	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	⊙ Site-to-Site
	Remote Access
	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. Specificeer het externe IP-adres van de externe peer. Voer de te gebruiken verificatieinformatie in, de vooraf gedeelde sleutel in dit voorbeeld. De pre-gedeelde sleutel die in dit voorbeeld wordt gebruikt is cisco123. De Naam van de Tunnel Groep zal uw buiten IP adres standaard zijn als u L2L VPN configureren. Klik op Volgende.

🖆 VPN Wizard		×
VPN Wizard	Remote Site Peer (Step 2 of 6)	
VPN Wizard	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: cisco123 • Certificate Certificate Signing Algorithm: rsa-sig Certificate Name: • Challenge/response authentication (CRACK)	
	Tunnel Group 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	
		J

8. Specificeer de eigenschappen die voor IKE moeten worden gebruikt, ook bekend als Fase 1. Deze eigenschappen moeten hetzelfde zijn op zowel de ASA als de IOS Router. Klik op **Volgende**.

🖆 VPN Wizard		×
VPN Wizard	IKE Policy (Step 3 of 6)	
Branch Branch Fisp Corporate Parks	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	Encryption: DES	
	Authentication: SHA	
	< Back Next Finish Cancel Help	0

Specificeer de eigenschappen die voor IPsec moeten worden gebruikt, ook bekend als Fase
 Deze eigenschappen moeten op zowel de ASA als de IOS router overeenkomen. Klik op Volgende.

🖆 VPN Wizard		
VPN Wizard	IPsec Encryption and Authentication (Step 4 of 6)	
Branch Branch ISP ISP Harwo Korporate Network	Select the encryption and authentication algorithms for this IPse on both sides of the connection must match exactly.	c VPN tunnel. Configurations
CINT I	Encryption: DES Y	
	Authentication: SHA 💌	
	< Back Next >	Finish Cancel Help
	N	

10. Specificeer de hosts waarvan het verkeer door de VPN-tunnel moet kunnen passeren. In deze stap moet u de lokale en afstandsnetwerken voor de VPN-tunnel beschikbaar stellen. Klik op de knop naast Local Networks zoals hier aangegeven om het lokale netwerkadres in de vervolgkeuzelijst te kiezen.

🖆 VPN Wizard		×
VPN Wizard	Hosts and Networks (Step 5 of 6)	
Branch Franch Franch Franch	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. Kies het adres Local Network en klik vervolgens op OK zoals hier wordt weergegeven.

📬 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		
	rk 172.16.1.0	255.255.255.0		
Selected Local Networks				
Local Networks ->	any			
			0	Cancel

12. Klik op de knop naast **Remote Networks** zoals hieronder aangegeven, om het externe netwerkadres in de vervolgkeuzelijst te kiezen.

🖆 VPN Wizard		
VPN Wizard	Hosts and Networks	(Step 5 of 6)
Branch	An IPsec tunnel protects remote sites. Please ider	s data exchanged by selected hosts and networks at the local and ntify hosts and networks to be used in the IPsec tunnel.
	Action: (Protect O Do not Protect
Home	Local Networks: in	nside-network/24
Corport	Remote Networks: a	any R
	🗹 Exempt ASA side ho	ost/network from address translation:
		< Back Next > Finish Cancel Help

13. Kies het adres van het Remote Network en klik vervolgens op OK zoals hieronder wordt weergegeven.N.B.: Als u het Remote Network niet in de lijst hebt staan, moet het netwerk aan de lijst worden toegevoegd door op Toevoegen te klikken.

🖆 Browse Remote Netv	vorks			
🗣 Add 🝷 📝 Edit 👔 I	Delete 🔍			
Filter:				Filter Clear
Name +1	IP Address	Netmask	Description	
⊡ Network Objects				
	0.0.0.0	0.0.0		
📑 📑 dmz-network	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		
L 🔂 10.20.10.0	10.20.10.0	255.255.255.0		
Demote Networks				
Kelliote Metworks ->				
			C PK	Cancel

14. Controleer de **vrijstellingsASA side host/network van adresomzetting** selectieteken om te voorkomen dat het tunnelverkeer **netwerkadresomzetting** ondergaat. Klik vervolgens op **Volgende**.

🖆 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 dentify hosts and networks to be used in the IPsec tunnel.
597 000	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:
		< Back Next > Finish Cancel Help

15. De eigenschappen die door de VPN Wizard worden gedefinieerd, worden in deze samenvatting weergegeven. Controleer de configuratie en klik op **Voltooien** wanneer u tevreden bent met de juiste instellingen.



Configuratie van routerdm

Voltooi deze stappen om site-to-Site VPN-tunnelheid op de Cisco IOS-router te configureren:

 Open uw browser en voer https://<IP_Address van de interface van de router in die voor de Toegang van het Sdm op de router is gevormd.Controleer of alle waarschuwingen die uw browser u geeft, behoren tot de SSL-certificatie. De standaard gebruikersnaam en wachtwoord zijn beide leeg.De router stelt dit venster voor om de download van de toepassing te toestaan. Dit voorbeeld laadt de toepassing op de lokale computer en werkt niet in een Java-



- 2. De download van het dm begint nu. Zodra de lantaarn van het Sdm wordt gedownload, voltooien de stappen die door de herinnering worden geregisseerd om de software te installeren en de Launcher van Cisco Sdm in werking te stellen.
- 3. Voer de **gebruikersnaam** en het **wachtwoord in** als u deze hebt ingesteld en klik op **OK**.Dit voorbeeld gebruikt **cisco123** voor de gebruikersnaam en **cisco123** als

Authenticati	on Required 🛛 🔀
چ) 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

wachtwoord.

4. Kies Configuration->VPN->Site-to-Site VPN en klik op de radioknop naast Een Site-to-Site

VPN-on-Site VPN maken op de startpagina met SDH. Klik vervolgens op De geselecteerde taak starten zoals hieronder wordt



5. Kies **Stap voor stap wizard** om verder te gaan met de configuratie:



6. Typ in het volgende venster de VPN-verbindingsinformatie in de betreffende ruimtes. Selecteer de interface van de VPN-tunnel in de vervolgkeuzelijst. Hier, FastEthernet0 wordt geselecteerd. Selecteer in het gedeelte Peer Identity de optie Peer met het statische IPadres en geef het externe IP-adres op. Typ vervolgens de Pre-Shared key (cisco123 in dit voorbeeld) in de sectie Verificatie zoals getoond. Klik vervolgens op Volgende.

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

7. Klik op Add om IKE-voorstellen toe te voegen die het Encryption Algorithm, Authentication Algorithm en de Key Exchange-methode specificeren.

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
Real Provide American Ame American American Amer	
DA	Add Edit
	< Back Next > Finish Cancel Help

8. Typ Encryption Algorithm, verificatie Algorithm en de Key Exchange-methode zoals hier aangegeven, en klik vervolgens op OK. De waarden Encryption Algorithm, Authentication Algorithm en de Key Exchange-methode moeten overeenkomen met de gegevens in de

	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
	<u> </u>	Cancel Help
ASA.	5	

9. Klik op **Volgende** zoals hier wordt weergegeven.

Site-to-Site VPN Wizard						
VPN Wizard	IKE Proposal IKE proposals method that is device. For the device should Click the Add	Is specify the en used by this ro VPN connection be configured button to add	cryption algorith outer when neg on to be establis with at least on I more policies	m, authentication otiating a VPN of shed with the re e of the policies and the Edit b	on algorithm and connection with t emote device, the elisted below. utton to edit an e	d key exchange he remote e remote existing policy.
	Priorit 1 2	3DES DES	Hash SHA_1 SHA_1	D-H Group group2 group1	Authentication PRE_SHARE PRE_SHARE	Type User Defined User Defined
	Add	Edit		< Back Ngx	t» Finish (Cancel Help

10. In dit nieuwe venster dienen de details voor het omzetten van de instellingen te worden verstrekt. Met de Instellen Omzetten wordt de Encryptie en verificatie-algoritmen gespecificeerd die worden gebruikt om gegevens in VPN-tunnels te beschermen. Klik vervolgens op Toevoegen om deze gegevens te verstrekken. U kunt indien nodig een aantal transformatiesets toevoegen door op Toevoegen te klikken en de gegevens te verstrekken.

11. Geef de Set-details op (Encryptie en verificatie-algoritme) en klik op OK zoals

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 Help

aangegever

12. Kies de gewenste **transformatie die ingesteld** wordt om gebruikt te worden in de vervolgkeuzelijst zoals weergegeven.

Site-to-Site VPN Wizard		×
	Transform Set A transform set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel. Since the two devices must use the same algorithms to communicate, the remote device must be configured with the same transform set as the one selected below. Click the Add button to add a new transform set and the Edit button to edit the specified transform set. Select Transform Set SDM Default Transform Set SDM Default Transform Set Name ESP Encryption ESP_SHA_HMAC Add Edit	
	Rack Next > Finish Cancel Helt	n

13. Klik op Volgende.

Site-to-Site VPN Wizard					×
VPN Wizard	Transform Set A transform set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel. Since the two devices must use the same algorithms to communicate, the remote device must be configured with the same transform set as the one selected below. Click the Add button to add a new transform set and the Edit button to edit the specified transform set. Select Transform Set				
	Details of the specified trans	sform set ESP Encryption ESP_DES	ESP Integrity ESP_SHA_HMAC	AH Integrity	
		< (Back Next > Fini	sh Cancel He	Ip

14. Typ in het volgende venster de informatie over het verkeer dat door de VPN-tunnelleiding beschermd moet worden. Verstrek de bron- en doelnetwerken van het te beschermen verkeer zodat het verkeer tussen de gespecificeerde bron- en doelnetwerken wordt beschermd. In dit voorbeeld is het Bron-netwerk 10.20.10.0 en het Bestemingsnetwerk is 10.10.10.0. Klik vervolgens op Volgende.

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	Remote Network Enter the IP Address and Subnet Mask of the destination Network. IP Address: 10.10.10.0 Subnet Mask 255.255.255.0 or 24			
		< Back Next > Finish Cancel Help			

15. Dit venster toont de samenvatting van de Site-to-Site VPN-configuratie uitgevoerd. Controleer de VPN-connectiviteit testen na het configureren van het vakje als u de VPNconnectiviteit wilt testen. Hier wordt het vakje ingeschakeld om de aansluitingen te controleren. Klik vervolgens op Voltooien.

Site-to-Site VPN Wizard						X
VPN Wizard	Summary of the (Configuration				
	Click Finish to del Interface:FastEth Peer Device:172. Authentication Ty pre-shared key:** IKE Policies: Hash SHA_1 SHA_1 Transform Sets: Name:A ESP End ESP Inte Mode:Tu	iver the configuration to the ernet0 16.1.1 pe : Pre-shared key DH Group group1 group2 SA-IPSEC cryption:ESP_DES egrity:ESP_SHA_HMAC JNNEL	Authentication PRE_SHARE PRE_SHARE	Encryption DES 3DES	· ·	
	Test VPN conn	ectivity after configuring.				
			<back next=""></back>	Finish	Cancel H	elp

16. Klik op **Start** zoals wordt getoond om de VPN-connectiviteit te controleren.

VPN Troubleshooting		×
Tunnel Details		1
Interface: FastEthernet0	Peer: 172.16.1.1	
	💷 Summary 🛛 🖳 Details	
Activity	Status	
Failure Reason(s)	Recommended Action(s)	
]
Start Save Report	Close Help	

 In het volgende venster wordt het resultaat van de VPN connectiviteit Test geleverd. Hier zie je of de tunnel omhoog of omlaag is. In deze voorbeeldconfiguratie, is de Tunnel Omhoog zoals in groen weergegeven.

VPN Troubleshooting			×
Tunnel Details			
Interface: FastEthernet0	Peer: 172.16.1.1		
	🗐 Summary	🕰 Details	
Activity		Status	
Checking the tunnel status		○ Up	
Failure Reason(s)	Recommended Action(s)		
Start Save Report	Close	Help	

Dit voltooit de configuratie op de Cisco IOS-router.

ASA CLI-configuratie



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



Configuratie van router CLI

router
Building configuration
Current configuration : 2403 bytes !
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
1

boot-start-marker boot-end-marker no logging buffered 1 username ciscol23 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 1 !--- !--- 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
!
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
!
!--- 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
!
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
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- PIX security applicatie toon opdrachten
- Remote IOS-router toont opdrachten

ASA/PIX security applicatie - show Opdrachten

• toon crypto isakmp sa-toont alle huidige IKE SAs bij een peer. 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 State : MM_ACTIVE Rekey : no toon crypto ipsec sa-Toont alle huidige IPsec SAs bij een peer. 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 - toont opdrachten

• toon crypto isakmp sa-toont alle huidige IKE SAs bij een peer. 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

• toon crypto ipsec sa-Toont alle huidige IPsec SAs bij een peer.

```
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:

• tonen de crypto motor verbindingen actief-toont huidige verbindingen en informatie over gecodeerde en gedecrypteerde pakketten (slechts 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

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg <u>Belangrijke informatie over debug Commands</u> en <u>IP security</u> <u>probleemoplossing - Bezig met begrijpen en gebruiken debug Commands</u> voordat u **debug**opdrachten gebruikt.

- debug crypto ipsec 7-displays de IPsec onderhandelingen van fase 2.debug crypto isakmp 7
 Hiermee geeft u de ISAKMP-onderhandelingen van fase 1 weer.
- debug crypto ipsec-displays de IPsec onderhandelingen van fase 2.debug crypto isakmp Hiermee geeft u de ISAKMP-onderhandelingen van fase 1 weer.

Raadpleeg de <u>meest gebruikelijke L2L- en IPSec VPN-oplossingen voor probleemoplossing</u> voor probleemoplossing bij site-site VPN.

Gerelateerde informatie

- <u>Cisco PIX-firewallsoftware</u>
- <u>Cisco adaptieve security apparaatbeheer</u>
- <u>Cisco ASA 5500 Series adaptieve security applicaties</u>
- <u>Configuration Professional: Site-to-Site IPsec VPN tussen ASA/PIX en een IOS</u> routerconfiguratie voorbeeld
- Opdrachtreferenties van Cisco Secure PIX-firewall
- <u>Cisco-router- en beveiligingsapparaatbeheer</u>
- Verzoeken om opmerkingen (RFC's)
- <u>Technische ondersteuning en documentatie Cisco Systems</u>