ASA/PIX: Statische IP-adressering voor IPSec VPN-client met CLI en ASDMconfiguratievoorbeeld

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Verwante producten **Conventies** Configureren Netwerkdiagram Externe toegang instellen (IPSec) ASA/PIX met CLI configureren **Cisco VPN-clientconfiguratie** Verifiëren Opdrachten tonen Problemen oplossen Beveiligingsassociaties wissen Opdrachten voor probleemoplossing Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u de Cisco 5500 Series adaptieve security applicatie (ASA) moet configureren om het statische IP-adres naar de VPN-client te geven met de Adaptieve Security Devices Manager (ASDM) of CLI. De ASDM levert veiligheidsbeheer en controle van wereldklasse door middel van een intuïtieve, makkelijk te gebruiken web-gebaseerde beheerinterface. Nadat de Cisco ASA-configuratie is voltooid, kan deze met de Cisco VPN-client worden geverifieerd.

Raadpleeg <u>PIX/ASA 7.x en Cisco VPN-client 4.x met Windows 2003 IAS RADIUS (Against Active Directory) verificatievoorbeeld</u> voor het instellen van de VPN-verbinding op afstand tussen een Cisco VPN-client (4.x voor Windows) en de PIX 500 Series security applicatie 7.x. De externe VPN-clientgebruiker authenticeert de actieve map aan de hand van een Microsoft Windows 2003-server voor internetverificatie (IAS) RADIUS.

Raadpleeg <u>PIX/ASA 7.x en Cisco VPN-client 4.x voor Cisco Secure ACS-verificatie</u> <u>Configuratievoorbeeld</u> om een VPN-verbinding op afstand in te stellen tussen een Cisco VPNclient (4.x voor Windows) en PIX 500 Series security applicatie 7.x met een Cisco Secure Access Control Server (ACS versie 3.2) voor uitgebreide verificatie (Xauth).

Voorwaarden

Vereisten

Dit document gaat ervan uit dat de ASA volledig operationeel en geconfigureerd is om Cisco ASDM of CLI in staat te stellen configuratiewijzigingen door te voeren.

Opmerking: Raadpleeg <u>HTTPS-toegang voor ASDM</u> of <u>PIX/ASA 7.x: SSH in het Voorbeeld van de</u> <u>configuratie van binnen en buiten</u> om het apparaat extern te kunnen configureren door de ASDM of Secure Shell (SSH).

Gebruikte componenten

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

- Software voor Cisco adaptieve security applicatie, versie 7.x en hoger
- Adaptieve Security Office Manager versie 5.x en hoger
- Cisco VPN-clientversie 4.x en hoger

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.

Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco PIX security applicatie versie 7.x en hoger.

Conventies

Raadpleeg <u>Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor</u> meer informatie over documentconventies.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het <u>Opdrachtupgereedschap</u> (alleen <u>geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



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

Externe toegang instellen (IPSec)

ASDM-procedure

Voltooi deze stappen om de externe VPN-toegang te configureren:

 Kies Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE-beleid > Add om een ISAKMP-beleid te maken.

Home Configuration	Monitoring 🕞 Sa Configuration > Configure speci	ve 💽 Refresh 🚺 Remote Access V fic Internet Key Exch	Back O Forw	ard ? He Client) Acc	elp :ess > Advance
Remote Access P + × P Introduction Network (Client) Access	Configuration > Configure speci	Remote Access V fic Internet Key Exch	PN > Network ((Client) Acc	ess > Advance
AnyConnect Connection	Princity #	t 📋 Delete	ange (ike) algorit	hms and par	ameters, within t
Address Assignment Advanced Advanced Grant Security Grant					
. Geef de ISAKMP-					

🗲 Add IKE Polic	у				
Priority:	2	Authentication:	pre-share 🗸		
Encryption:	des 💙	D-H Group:	2 🗸		
Hash:	sha 💙	Lifetime:	Unlimited86400	seconds 💌	
Cancel Help					

Klik op OK en Toepassen.

3. Kies Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE-parameters om IKE op de buiteninterface mogelijk te

IIIakeii.						
🚰 Cisco ASDM 6.1 for ASA - 10.77.241.111						
File View Tools Wizards Wind	File View Tools Wizards Window Help					
😚 Home 🔏 Configuration 📴 M	🔥 Home 😘 Configuration 📴 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🦻 Help					
Remote Access d P ×	Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Parameters					
-? Introduction	Enable IKE NAT Transparency					
AnyConnect Connection	Interface IKE Enabled Enable IPsec over NAT-T					
Psec Connection Profit Group Policies	draz No NAT Keepalive: 20 seconds					
- Dynamic Access Policie	nside No Disable					
B-B Advanced	outside Yes Enable IPsec over TCP					
B-Ga Endpoint Security	values (1- 65535):					
P-IB IPsec	10000					
The Crypto Maps						
IN DEPENDENTS	Indentity to Be Sent to Paer					
Psec Transform						
Gertificate to Co	Identity: Automa Y Key Id String:					
-+2+ Zone Labs Integ						
System Options	Disable inbound aggressive mode connections					
Clientless SSL VPN Access	Alert peers before disconnecting					
AAA/Local Users	Wait for all active sessions to uninstantly terminate before reporting					
Certificate Manager	war for an active sessions to volumently terminate before rebuilding					

4. Kies Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IPSec Transformatiesets > Add om de ESP-DES-SHA transformatieset te maken, zoals

📧 Add	Transform Set			
	Set Name:	ESP-DES-SHA		
	Properties			
	Mode:			
	Mode.	Uniter .		
	ESP Encryptio	n: DES	×	
	ESP Authentic	ation: SHA	×	
	<u> </u>	Cancel	Help	

Klik op **OK** en **Toepassen**.

5. Kies Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > Crypto Maps > Add om een crypto-kaart te maken met dynamisch beleid van prioriteit 1, zoals

getoond.

🖆 Create IPsec Rule	
Tunnel Policy (Crypto Map) - Basic Tunnel Policy (Crypto Map) - Advanced Traffic Selection	
Interface: outside 💌 Policy Type: dynamic 💌	Priority: 1
Transform Sets	
Transform Set to Be Added:	Move Up
Remove	Move Down
Peer Settings - Optional for Dynamic Crypto Map Entries The Connection Type is applicable to static type! policies only. Uni-directional connection	n type policies are used
for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may redundant peers.	specify up to 10
OK Cancel Help	

Klik op OK en Toepassen.

6. Kies Configuration > Remote Access VPN > AAA-instelling > Local Gebruikers > Add om de gebruikersaccount te maken (bijvoorbeeld gebruikersnaam - cisco123 en Wachtwoord cisco123) voor VPN-

clienttoegang.

🕵 Add	User Account					
Ider	itiky					
	Policy	Username:	cisco123			
		Password:	*****			
		Confirm Password:	****			
		User authentica	ated using MSCHAP			
		Access Restriction				
		Select one of the	options below to restrict ASDM, SSH, Telnet and Console	access.		
		Note: All users ha	ave network access, regardless of these settings.			
		 Full access(ASDM, SSH, Telnet and Console) 				
		Privilege level is used with command authorization.				
		Privilege Level: 2				
		🚫 CLI login pron	npt for SSH, Telnet and console (no ASDM access)			
		This setting	g is effective only if AAA authenticate console command it	s configured.		
		🚫 No ASDM, SSI	H, Telnet or Console access			
		This setting	is effective only if AAA authenticate console command is	s configured.		
Find:			🔘 Next 🛛 🔘 Previous			
		ĺ	OK Cancel Help			

7. Ga naar **VPN-beleid** en voeg het **statische/speciale IP-adres** voor gebruiker "cisco123" toe, namelijk:

🖆 Cisco ASDM 6.1 for ASA	- 10.77.	241.111				
File View Tools Wizards W	indow H	elp				
Home 🆓 Configuration 👩	Monitorinç	a 🔚 Save 🔇 Refresh	🔇 Back 🚫 Forward 🧳 Help 🖉			
Remote Access 🗗 🖗 ×	Configu	ration > Remote Access	s VPN > AAA/Local Users > Local	Users		
-? Introduction	Crea	🖆 Add User Accoun	•			
AnyConnect Connection P						<u> </u>
Psec Connection Profiles	Corr	identity	Check an Inherit checkbox to let the	ne correspondi	ng setting take its value	from the
Group Policies	AAA	C-VEN Policy		_		
Address Assignment			Group Policy:	🗹 Inherit	L	
Assignment Policy	Use		Tunneling Protocols:	Inherit	Clientless SSL VPN	SSL.
Address Pools	enat		Filmer			
			Finter:	V unnerit		
AAA/Local Users			Tunnel Group Lock:	🗹 Inherit		
AAA Server Groups			Store Password on Client System:	V Inherit	O Yes ONo	
a Local users			Sere rassred or client System.		0.00 0.00	
- A Secure Desktop Manager			Connection Settings			
Certificate Management			Access Hours:	Inherit		
-Se Load Balancing					L	
- P DHCP Server			Simultaneous Logins:	Minherit		
			Maximum Connect Time:	🖌 Inherit	Unlimited	Minute
r-103 Advanced			Min Timon tr	Minharit	Unlimited	Afrento
			sue mieduc.	The second		
			Dedicated IP Address (Optional)			
			IP Address: 192,168.5.1	Subnet Mask	255.255.255.0	
	1000					

8. Kies Configuration > Remote Access VPN > Network (Client) Access > Address Asmission > Adres Pools en klik op Add om de VPN-client voor VPN-gebruikers toe te

voegen.

Cisco ASDM 6.1 for ASA	- 10.77.241.111
ile View Tools Wizards W	ndow Help
🔥 Home 🕞 Configuration 📴	Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help
Remote Access D 4 × Introduction Network (Client) Access AnyConnect Connection Pr IPsec Connection Profiles Group Policies Dynamic Access Policies Address Assignment Address Assignment Address SSL VPN Access Address SSL VPN Access	Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools Configure named IP Address pools. This parameter is enforced in either a VPN IPsec Connection Profiles, AnvConnect Connection Profiles or Group Policies • Add • Edit • Delete Pool Name Star Name: vpnclient1 Starting IP Address: 192.168.5.100 Subnet Mask: Subnet Mask:
Address Assignment Policy Address Assignment Policy Address SSL VPN Access AdA/Local Users AAA/Local Users AAA/Local Users Certificate Management Load Balancing DHCP Server DNS Advanced	Pool Name Star Name: vpnclient1 Starting IP Address: 192.168.5.10 Ending IP Address: 192.168.5.100 Subnet Mask: 55.255.00 OK Cancel Help

 Kies Configuration > Remote Access VPN > Network (Client) Access > IPSec Connection Profile > Add om een tunnelgroep toe te voegen (bijvoorbeeld TunnelGroup1 en de PreShared key as cisco123), zoals wordt

getoond.

File View Tools Wizards Window He	lp.		Look For:	
🔥 Home 🦓 Configuration 🔯 Monitorin	ng 🔲 Save 🔇 Refresh 🤇	Back 🔘 Forward 🧖 He	dp.	
Remote Access VPN P Inbroduction Network (Client) Access AnyConnect Connection Profiles Scoup Policies Particle Advanced Clientless SSL VPN Access AAA/Local Users Secure Desktop Manager Certificate Management Carguage Localization Language Localization DHCP Server	Configuration > Remote Acces Access Interfaces Enable interfaces for IPsec ac Uniterface Outside dmz inside Connection Profiles Connection profile (tunnel gro Add 2 Edit 10 Del	up) specifies how user is authentia	cese > IPsec Connection Prof	ikes.
	Name	IPsec Enabled	L2TP/IPsec Enabled	Autentication
H-GO Havanced	DefaultWEBVPNGroup			LOCAL
	DefaultRAGroup	N N	Ā	LOCAL
Remote Access VPN Ste-to-Site VPN IPS Device Management				
»			Apply Reset	

Kies onder het tabblad **Basic** de servergroep als **LOCAL** voor het veld Gebruikersverificatie.Kies **VPN-client1** als de clientadrespools voor de VPNclientgebruikers.

Home & Configuration	🗿 Monitoring 🔚 Save 📿	🕨 Refresh 🚱 Back 🜔	Forward ? Help	
Remote Access 🗗 🔍 🗵	Configuration > Rem	ote Access VPN > Net	work (Client) Access > IPsec Connection Pro	ofiles
	· · · · · · · · · · · · · · · · · · ·			
Network (Client) Access	🌃 Add IPsec Remote	Access Connection	n Profile	
Psec Connection Profile	r-Basic	Name:	TunnelGroup1	
Group Policies	Advanced			
Dynamic Access Policies		IKE Peer Authentication		
B-Sp Address Assignment				
Address Pools		Pre-shared Key:	*****	
Address Pools		Identity Contification	Aleen	Managar
Clientiess SSI VPN Access		toendry Certificate:	None	manage
AAA/Local Users		11		
- AAA Server Groups		User Authentication		
		Server Group:	LOCAL	Manage
- 🕼 Local Users				9/8/88226/0
🗜 🚮 Secure Desktop Manager		Fallback:	Use LOCAL if Server Group fails	
- Certificate Management				
Englage Localization		Client Address Assignme	ent	
- St Load Balancing		DHCP Servers:		
B DHCP Server				000000000000000000000000000000000000000
Advanced		Client Address Pools	vpnclient1	Select.
o Bo Movanced				
		Default Group Policy —		
		Group Policy:	DfltGrpPolicy Y	Manage
			(Following fields are attributed of the group policy	selected a
			Lenable (Psec protocol	
			Enable L2TP over IPsec protocol	

Klik op **OK**.

10. Kies Geavanceerd > Clientadressering en controleer het aankruisvakje Adres gebruiken om het IP-adres aan de VPN-clients toe te wijzen.Opmerking: Schakel de selectievakjes in om de verificatieserver te gebruiken en DHCP te gebruiken.

🚰 Add IPsec Remote Access Connection Profile
Basic General General Authentication Authorization Accounting G=Psec ppp G deal Client Address Assignment Policy This policy affects all Network (Client) Access connections. The following are tried in order until an address is found. Use authentication server Use address pool Interface-Specific Address Pools Add I Edit I Delete Interface Address Pools
Find:

Klik op **OK**.

11. Schakel de interface **Outside** voor IPSec Access in. Klik op **Toepassen** om verder te gaan.

🚰 Cisco ASDM 6.1 for ASA - 10.77.241.111					
File View Tools Wizards Window Help					
🔥 Home 🎭 Configuration 📝	Monitoring 🔚 Save 🔇 Refresh	Sack Serward ? Help			
Remote Access P × Introduction Network (Client) Access AnyConnect Connection Profiles Connection Profiles Connection Profiles Connection Profiles Address Policies Address Policies Address Policy Address Policy Address Pools Address Pools Address SSL VPN Access AAA/Local Users AAA/Local Users AAA/Local Users AAA Server Groups Local Users Certificate Management Local Users Certificate Management Load Balancing DHCP Server NS Advanced	Configuration > Remote Access Access Interfaces Enable interfaces for IPsec acces Interface outside dmz hside Connection Profiles Connection profile (tunnel group) ● Add @ Edit @ Delete Name TunnelGroup1 DefaultWEBVPNGroup DefaultRAGroup	s VPN > Network (Client) Access > IPsec Conners.			

ASA/PIX met CLI configureren

Voltooi deze stappen om de DHCP-server te configureren om IP-adressen te geven aan de VPNclients vanuit de opdrachtregel. Raadpleeg <u>Beelden voor externe toegang VPN's</u> of <u>Cisco ASA</u> <u>5500 Series adaptieve security applicaties-commando-referenties</u> voor meer informatie over elke opdracht die wordt gebruikt.

Configuratie op het ASA-apparaat uitvoeren
ASA# sh run
ASA Version 8.0(2)
!
<i>! Specify the hostname for the Security Appliance.</i>
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! ! Configure the outside and inside
<i>interfaces.</i> interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 50 ip address
192.168.10.2 255.255.255.0 ! Output is suppressed.
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa802-k8.bin ftp mode passive access-list 101
extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0
255.255.255.0 pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 ip local pool vpnclient1 192.168.5.10-192.168.5.100
mask 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1

--- Specify the location of the ASDM image for ASA to fetch the image for ASDM access. asdm image disk0:/asdm-613.bin no asdm history enable arp timeout 14400 global (outside) 1 192.168.1.5 nat (inside) 0 access-list 101 nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0 192.168.1.2 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 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute dynamic-access-policyrecord DfltAccessPolicy http server enable http 0.0.0.0 0.0.0.0 inside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto dynamic-map outside_dyn_map 1 set transform-set ESP-DES-SHA crypto map outside_map 1 ipsec-isakmp dynamic outside_dyn_map !--- Specifies the interface to be used with !--- the settings defined in this configuration. crypto map outside_map interface outside !--- PHASE 1 CONFIGURATION ---! !--- This configuration uses ISAKMP policy 2. !---The configuration commands here define the Phase !--- 1 policy parameters that are used. crypto isakmp enable outside crypto isakmp policy 2 authentication pre-share encryption des hash sha group 2 lifetime 86400 no crypto isakmp nat-traversal !--- Specifies that the IP address to the vpn clients are assigned by the local and not by AAA or dhcp. The CLI vpn-addr-assign local for VPN address assignment through ASA is hidden in the CLI provided by show run command. no vpn-addr-assign aaa no vpn-addr-assign dhcp telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list 1 class-map inspection_default match default-inspection-traffic 1 policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map 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
service-policy global_policy global
1
group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol IPSec webvpn
group-policy GroupPolicy1 internal
!--- In order to identify remote access users to the
Security Appliance, !--- you can also configure
usernames and passwords on the device. !--- specify the
IP address to assign to a particular user, use the vpn-
framed-ip-address command !--- in username mode
username cisco123 password ffIRPGpDSOJh9YLq encrypted
username cisco123 attributes
 vpn-framed-ip-address 192.168.5.1 255.255.255.0
!--- Create a new tunnel group and set the connection !-
-- type to remote-access. tunnel-group TunnelGroup1 type
remote-access tunnel-group TunnelGroup1 general-
attributes address-pool vpnclient1 !--- Enter the pre-
shared-key to configure the authentication method.
tunnel-group TunnelGroup1 ipsec-attributes pre-shared-
key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#
```

Cisco VPN-clientconfiguratie

Probeer met de Cisco ASA te verbinden met de Cisco VPN-client om te verifiëren dat de ASA met succes is geconfigureerd.

- 1. Kies Start > Programma's > Cisco Systems VPN-client > VPN-client.
- 2. Klik op **New** om het venster Nieuwe VPN-verbinding maken te

Status: Disconnected VPN Client - Version 5.0.03.0530					
Connection Entries Status Certificates Log Options Help					
Connect	New	F all	a (Aodify) Delete
Connection Entr	ries (Certificates	Log		
Con	nection	Entry /			Host

starten.

3. Vul de gegevens in van uw nieuwe aansluiting. Voer de naam van de verbindingsbocht in samen met een beschrijving. Voer het externe IP-adres van de ASA in het hostvak in. Voer vervolgens de naam van de VPN Tunnel Group (TunnelGroup1) en het wachtwoord in (Voorgedeelde sleutel - Cisco123) zoals ingesteld in ASA. Klik op

VPN Client Create New VPN Connect	tion Entry				
Connection Entry: ASA					
Description: vpntunnel		alada			
Host: 192.168.1.1		CISCO			
Authentication Transport Backup Servers Dial-Up					
Group Authentication					
Name: TunnelGroup1					
Password: ******					
Confirm Password: *******					
Certificate Authentication Name: Send CA Certificate Chain					
Erase User Password	Save	Cancel			

Opslaan.

4. Klik op de verbinding die u wilt gebruiken en klik op **Connect** vanuit het hoofdvenster van VPN-

client.			
🥥 status: Connected VPN Client - Versio	n 5.0.03.0530		
Connection Entries Status Certificates Log Optic	ons Help	en de la constante de la compo	
Connect New Import Modify Connection Entries Certificates Log	Delete	cito Cis	ili. co
Connection Entry /	Host	Transport	
ASA	192.168.1.1	IPSec/UDP	
Not connected.	C	onnected Time: 0 day(s), 00:01.18	T

5. Voer desgevraagd de **gebruikersnaam** in : **Cisco123** en **Wachtwoord: cisco123** zoals ingesteld in de ASA for Xauth en klik op **OK** om verbinding te maken met het externe

The server has reques authentication.	sted the following information to complete the user
Username:	cisco123
CISCO Password:	******

netwerk.

6. De VPN-client is verbonden met de ASA op de centrale

site.				
🥔 stat	us: Connected VPN Client - Versio	n 5.0.03.0530		
Connect	tion Entries Status Certificates Log Optio	ns Help		
Discon	nect New Import Modify	Delete		diada cisco
Connec	stion Entries Certificates Log			
	Connection Entry	Host	Transport	
0	ASA	192.168.1.1	IPSec/UDP	
Coppect	ad bo *650"			

7. Zodra de verbinding met succes is tot stand gebracht, kiest u **Statistieken** uit het menu Status om de details van de tunnel te controleren.

🥔 status: (Connected VPN Client - Version 5.0	.03.0530	
Connection Er	ntries Status Certificates Log Options He	lp	
Disconnect Connection E	Statistics Ctrl+S Notifications Ctrl+N N Reset Stats	elete	cisco
	Connection Entry	Host	Transport
٥	ASA	192.168.1.1	IPSec/UDP
Connected to	"ASA".	Con	nected Time: 0 day(s), 00:00.16 🛛 🔻

Verifiëren

Opdrachten tonen

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.

- toon crypto isakmp sa-toont alle huidige IKE Security Associations (SAs) bij een peer.
- toon crypto ipsec sa-Toont de instellingen die worden gebruikt door huidige SA's.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen. Ook wordt een voorbeelduitvoer van debug-uitvoer weergegeven.

Opmerking: Voor meer informatie over de oplossing van problemen met betrekking tot IPSec VPN <u>verwijst</u> u naar de <u>meest gebruikelijke oplossingen voor probleemoplossing in L2L en externe</u> <u>access IPSec VPN</u>.

Beveiligingsassociaties wissen

Wanneer u problemen oplossen, zorg er dan voor dat de bestaande veiligheidsassociaties worden gewist nadat u een wijziging hebt aangebracht. In de bevoorrechte modus van de PIX, gebruik deze opdrachten:

- duidelijk [crypto] ipsec sa-Delete de actieve IPSec SA's. Het sleutelwoord crypto is optioneel.
- Schakel [crypto] isakmp sa—Verwijdert de actieve IKE SA's. Het sleutelwoord crypto is optioneel.

Opdrachten voor probleemoplossing

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> 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.

Gerelateerde informatie

- <u>Cisco ASA 5500 Series ondersteuningspagina voor adaptieve security applicaties</u>
- <u>Cisco ASA 5500 Series Opdrachten voor adaptieve security applicaties</u>
- Ondersteuning van Cisco PIX 500 Series security applicaties
- <u>Cisco PIX 500 Series security applicaties, opdracht</u>

- <u>Cisco adaptieve security apparaatbeheer</u>
- Ondersteuning van IPSec-onderhandeling/IKE-protocollen
- <u>Cisco VPN-clientondersteuningspagina</u>
- <u>Cisco PIX-firewallsoftware</u>
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Security meldingen uit het veld (inclusief PIX)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie Cisco Systems