PIX/ASA als een Remote VPN-server met uitgebreide verificatie met behulp van CLI en ASDM-configuratievoorbeeld

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Verwante producten **Conventies** Achtergrondinformatie Configuraties ASA/PIX configureren als een externe VPN-server met ASDM ASA/PIX configureren als externe VPN-server met CLI Configuratie van Cisco VPN-clientwachtwoord Uitgebreide verificatie uitschakelen Verifiëren Problemen oplossen **Onjuiste encryptie-ACL** Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u de Cisco 5500 Series adaptieve security applicatie (ASA) moet configureren om op te treden als een externe VPN-server met behulp van 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 worden geverifieerd met behulp van de Cisco VPN-client.

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 met 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.

Achtergrondinformatie

Remote-toegangsconfiguraties bieden beveiligde externe toegang voor Cisco VPN-clients, zoals mobiele gebruikers. Een VPN-toegang op afstand stelt externe gebruikers in staat om veilig toegang te krijgen tot gecentraliseerde netwerkbronnen. De Cisco VPN-client voldoet aan het IPSec-protocol en is specifiek ontworpen om met het security apparaat te werken. Het security apparaat kan echter wel IPSec-verbindingen maken met veel klanten die aan het protocol voldoen. Raadpleeg de <u>ASA Configuration Guides</u> voor meer informatie over IPSec.

Groepen en gebruikers zijn kernconcepten in het beheer van de beveiliging van VPN's en in de configuratie van het security apparaat. Ze specificeren eigenschappen die de toegang van gebruikers tot en het gebruik van VPN bepalen. Een groep is een verzameling gebruikers die als één entiteit worden behandeld. Gebruikers krijgen hun eigenschappen van groepsbeleid. Tunnelgroepen identificeren het groepsbeleid voor specifieke verbindingen. Als u geen bepaald groepsbeleid aan een gebruikers toewijst, is het standaard groepsbeleid voor de verbinding van toepassing.

Een tunnelgroep bestaat uit een reeks records die tunnelverbindingsbeleid bepalen. In deze registers worden de servers geïdentificeerd waarop de servers waarop de tunnelgebruikers zijn geauthentiseerd, evenals de eventuele boekhoudservers waarop de aansluitingsinformatie wordt verzonden. Ze identificeren ook een standaardgroepsbeleid voor de verbindingen, en ze bevatten protocol-specifieke verbindingsparameters. Tunnelgroepen omvatten een klein aantal eigenschappen die betrekking hebben op de totstandbrenging van de tunnel zelf. Tunnelgroepen bevatten een muiswijzer op een groepsbeleid dat gebruikersgeoriënteerde eigenschappen definieert.

Opmerking: In de steekproefconfiguratie in dit document worden lokale gebruikersrekeningen gebruikt voor authenticatie. Als u een andere service wilt gebruiken, zoals LDAP en RADIUS, raadpleegt u <u>Een externe RADIUS-server configureren voor autorisatie en verificatie</u>.

De Internet Security Association en het Key Management Protocol (ISAKMP), ook IKE genoemd, is het onderhandelingsprotocol dat hosts overeenstemming bereikt over de manier waarop een IPSec Security Association moet worden gebouwd. Elke ISAKMP-onderhandeling is verdeeld in twee delen, fase1 en fase2. Fase1 creëert de eerste tunnel om latere ISAKMP onderhandelingsberichten te beschermen. Phase2 creëert de tunnel die gegevens beschermt die over de veilige verbinding reiken. Raadpleeg <u>ISAKMP-beleidstrefwoorden voor CLI-opdrachten</u> voor meer informatie over ISAKMP.

Configuraties

ASA/PIX configureren als een externe VPN-server met ASDM

Voltooi deze stappen om Cisco ASA als een externe VPN-server te configureren met behulp van ASDM:

1. Selecteer **Wizard > VPN** vanuit het venster Start.

🚰 Cisco ASDM 5.0 for ASA - 172.10	5.1.2				_ O ×
File Rules Search Options T	ools Wizards Help				
Home Configuration (Monitor	arch Refresh	Save Help		CISCO SYSTEMS
-Device Information		Interface Sta	tus		
General License		Interface	IP Address/Mask	Line Link	Current Kbps
Host Name: ciecosea e	ieco com	inside	172.16.1.2/24	Oup Oup	1
ACA Manajor: 7.0(4)	Davias Listino: 04 06 43m 25a	outside	10.10.10.2/24	😏 up 😲 up	0
ADDM (content 5.0(4)	Device Optime: do un 12m 355				
AsDM Version: 5.0(4)	Device Type: ASA5520				
Firewall Mode: Routed	Context Mode: Single				
Total Flash: 64 MB	Total Memory: 512 MB	Select an inter	face to view input and	output Kbps	
-VPN Status		Traffic Status	8		
IKE Tunnels: 0	IPSec Tunnels: 0	Connections	Per Second Usage		
-System Resources Status -		1			
CPU CPU Usage (per	roent)	0.5			
90******		2 mont			
0% 84		10.02.20	700.0	Total: D	
12.02.45		- 00PE 0		Tetat: 0	
15.02.20		outside' Inte	rface Traffic Usage (Kbps	0	
Memory Memory Usage	(MB)	1			
512 384		0.5			
60M9 200 128		13:02:20			
13.02.49 13:02:28		Input Kb	ps: 0 📕	Output Kbps: 0	
Latest ASDM Syslog Messa	jes			Configure At	SDM Syslog Filters
	Syslog Disabled				
Device configuration loaded succes	ssfully.	admin N	A (15)	12/22	2/05 1:02:46 PM UTC

2. Selecteer het tunneltype **Remote Access** VPN en zorg ervoor dat de VPN-tunnelinterface naar wens wordt ingesteld.

📸 VPN Wizard		X
VPN Wizard	VPN Tunnel Type (Step 1 of)	
Branch Branch Dorporate Network	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. VPN Tunnel Type:	
	Site-to-Site VPN Remote Access Remote Access VPN Tunnel Interface: outside	
	< Back Next Finish Cancel Hel	p

3. Het enige beschikbare VPN-clienttype is al geselecteerd. Klik op **Volgende**.



4. Voer een naam in voor de naam van de tunnelgroep. Verstrek de te gebruiken authenticatie informatie. **Vooraf gedeelde sleutel** is geselecteerd in dit voorbeeld.

📸 VPN Wizard	
VPN Wizard	VPN Client Tunnel Group Name and Authentication Method (Step 3 of)
Branch Branch	The ASA allows you to group remote access tunnel users based on common connection parameters and client attributes configured in the following screens. Use the same tunnel group name for the device and the remote client. Select the type of authentication: shared secret or certificate. If certificate, select the certificate name and the certificate signing algorithm.
Corporate Natwork	Tunnel Group Name: hillvalleyvpn
THE REAL	Authentication Pre-shared Key
	Pre-shared Key: cisco123
	C Certificate
-6-	Certificate Signing Algorithm:
	Trustpoint Name:
	< Back Next > Finish Cancel Help

N.B.: Er is geen manier om de voorgedeelde toets op de ASDM te verbergen of te versleutelen. De reden is dat ASDM alleen gebruikt mag worden door mensen die de ASA configureren of door mensen die de klant bijstaan met deze configuratie.

5. Kies of u externe gebruikers wilt geauthentiseerd worden naar de lokale gebruikersdatabase of naar een externe AAA server groep. Opmerking: U voegt in stap 6 gebruikers toe aan de lokale gebruikersdatabase. Opmerking: Raadpleeg <u>PIX/ASA 7.x-groepen voor VPN-</u> <u>gebruikers via ASDM Configuration Voorbeeld</u> voor informatie over de configuratie van een externe AAA-servergroep via ASDM.

💼 VPN Wizard	
VPN Wizard	Client Authentication (Step 4 of)
Branch Branch ISP Home Network	To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next screen. To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below. To manage all other AAA settings, use Configuration > Features > Properties > AAA Setup category in the main ASDM window.
	 Authenticate using the local user database Authenticate using an AAA server group AAA Server Group
	< Back Next > Finish Cancel Help

6. Voeg indien nodig gebruikers toe aan de lokale database.N.B.: Verwijder bestaande gebruikers niet uit dit venster. Selecteer Configuratie > Apparaatbeheer > Administratie > Gebruikersrekeningen in het hoofdvenster van ASDM om bestaande items in de database te bewerken of deze uit de database te verwijderen.

🔂 VPN Wizard			×
VPN Wizard	User Accounts (Step 5 of 11)		
Brankdh Dialaithe Dialaithe Homm	Enter a new username/password in existing entries in the database or to Configuration > Device Administration ASDM window.	to the user authent) remove them from on > Administration	ication database. To edit the database, go to > User Accounts in the main
Corporate	Username:	Add >>	Username admin einstein marty
	Password (optional):	Delete	docbrown jennifer biff
	Confirm Password (optional):		
		< Back Next >	Finish Cancel Help

7. Defineert een pool van lokale adressen die dynamisch aan externe VPN-clients moeten worden toegewezen wanneer ze verbinding maken.

🔂 VPN Wizard		×
VPN Wizard	Address Pool (Step 6 of 11)	
Brench Fr	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.	
Corporato Network	Tunnel Group Name: hillvalleyvpn	
111 - I + M	Pool Name: vpnpool	
	Range Start Address: 172.16.1.100	
TTT	Range End Address: 172.16.1.199	
	Subnet Mask (Optional): 255.255.255.0	
	Sack Next > Finish Cancel Help	

8. *Optioneel:* Specificeer de DNS- en WINS-serverinformatie en een standaardnaam voor domeinen die naar externe VPN-clients moet worden geduwd.

💼 VPN Wizard	×
VPN Wizard	Attributes Pushed to Client (Optional) (Step 7 of 11)
Brendt Brendt	Attributes you configure below are pushed to the VPN client when the client connects to the ASA. If you do not want an attribute pushed to the client, leave the corresponding field blank.
(Corporate)	Tunnel Group: hillvalleyvpn
Network	Primary DNS Server:
	Secondary DNS Server:
- Terulli	Primary WINS Server:
	Secondary WINS Server:
	Default Domain Name:
	< Back Next > Finish Cancel Help

 Specificeer de parameters voor IKE, ook bekend als IKE Fase 1.De configuraties aan beide zijden van de tunnel moeten precies overeenkomen. Maar de Cisco VPN-client selecteert automatisch de juiste configuratie voor zichzelf. Daarom is geen IKE-configuratie nodig op de client-

pc.

薩 VPN Wizard		×
VPN Wizard	IKE Policy (Step 8 of 11)	
Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch	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.	
Corporate Network	Encryption: 3DES	
	Authentication: SHA	
5144	DH Group: 2	
		,

10. Specificeer de parameters voor IPSec, ook bekend als IKE fase 2.De configuraties aan beide zijden van de tunnel moeten precies overeenkomen. Maar de Cisco VPN-client selecteert automatisch de juiste configuratie voor zichzelf. Daarom is geen IKE-configuratie nodig op de clientpc.

🚰 VPN Wizard	
VPN Wizard	IPSec Encryption and Authentication (Step 9 of 11)
Branch	Select the encryption and authentication algorithms for this IPSec VPN tunnel. Configurations on both sides of the connection must match exactly.
Corporate Network	Encryption: 3DES
	Authentication:
	< Back Next > Finish Cancel Help

11. Specificeer welke, als om het even welke, interne hosts of netwerken zouden moeten worden blootgesteld aan externe VPN-gebruikers.Als u deze lijst leeg laat, staat het externe VPN-gebruikers toe om toegang te krijgen tot het gehele binnennetwerk van de ASA.U kunt ook gesplitste tunneling in dit venster inschakelen. Split-tunneling versleutelt het verkeer naar de bronnen die eerder in deze procedure zijn gedefinieerd en geeft onversleutelde toegang tot internet in het algemeen door dat verkeer niet uit te schakelen. Als gesplitste tunneling *niet* ingeschakeld is, wordt al het verkeer van externe VPN-gebruikers naar de ASA gekanaliseerd. Dit kan zeer bandbreedte en processor intensief worden, gebaseerd op uw

configuratie.

🔯 VPN Wizard		×
VPN Wizard	Address Translation Exemption and Split Tunneling	g (Optional) (Step 10 of 11)
Bronch Distriction Distriction Hormon	Network Address Translation (NAT) is used to hid users. You can make exceptions to NAT to expose network to authenticated remote users protected b To expose the entire network behind the most sec without NAT, leave the selection list blank.	e the internal network from outside e the entire or part of the internal by VPN. :ure interface to remote VPN users
Corporate Network	Host/Network to Be Added	Selected Hosts/Networks:
- com	● IP Address ○ Name ○ Group	
1 State	Interface: inside	Add >>
THUM	IP address: 0.0.0.0	Delete
	Mask: 0.0.0 💌	
	Enable split tunneling to let remote users have resources defined above, and unencrypted ac	e simultaneous encrypted access to the cess to the internet.
	< Back	Next > Finish Cancel Help

12. Dit venster geeft een samenvatting van de maatregelen die u hebt genomen. Klik op **Voltooien** als u tevreden bent met de configuratie.



ASA/PIX configureren als externe VPN-server met CLI

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

1. Voer het ip lokale pool opdracht in in de mondiale configuratiemodus om IP adrespools te configureren om te gebruiken voor VPN-tunnels in de externe toegang. Voer de geen vorm van deze opdracht in om adrepools te verwijderen. Het beveiligingsapparaat gebruikt adrestoestellen op basis van de tunnelgroep voor de aansluiting. Als u meer dan één adrespool voor een tunnelgroep vormt, gebruikt het security apparaat deze in de volgorde waarin ze zijn geconfigureerd. Geef deze opdracht uit om een pool van lokale adressen te maken die kan worden gebruikt om dynamische adressen toe te wijzen aan VPN-clients met externe toegang:

ASA-AIP-CLI(config)#ip local pool vpnpool 172.16.1.100-172.16.1.199 mask 255.255.255.0

- 2. Deze opdracht geven: ASA-AIP-CLI(config)#username marty password 12345678
- 3. Geef deze reeks opdrachten uit om de specifieke tunnel te configureren:ASA-AIP-CLI (configuratie)#isakmp beleid 1 verificatie vooraf delenASA-AIP-CLI (Config)#isakmp beleid 1encryptie 3desASA-AIP-CLI (configuratie)#isakmp beleid 1 hashshaASA-AIP-CLI (configuratie)#isakmp beleid 1 groep 2ASA-AIP-CLI (configuratie)#isakmp beleid 1 leven

43200ASA 5500-AIP-CLI (configuratie)#isakmp maakt toegang tot buiten mogelijkASA 5500-AIP-CLI (configuratie)#crypto ipsec transformatie-set ESP-3DES-SHA esp-3des esp-shahmacASA-AIP-CLI (configuratie)#crypto dynamisch-kaart buiten_dyn_map 10 set transformatie-set ESP-3DES-SHAASA-AIP-CLI (configuratie)#crypto dynamisch-kaart buiten_dyn_map 10 set reverse-routeASA-AIP-CLI (configuratie)#crypto dynamisch-kaart buiten_dyn_map 10 ingestelde security-associatie levensduur seconden 288000ASA-AIP-CLI (configuratie)#crypto kaart buiten_map 10 ipsec-isakmp dynamisch buiten_dyn_mapASA-AIP-CLI (configuratie)#crypto kaart buiten_map interfaceASA 5500-AIP-CLI (configuratie)#crypto nucleaire traversal

4. *Optioneel:* Als u wilt dat de verbinding de toegangslijst overschrijdt die op de interface wordt toegepast, geeft u deze opdracht uit:

ASA-AIP-CLI(config)#sysopt connection permit-ipsec

Opmerking: deze opdracht werkt vóór 7.2(2) op 7.x-afbeeldingen. Als u afbeelding 7.2(2) gebruikt, geeft u de ASA-AIP-CLI (configuratie)#sysopt verbinding vergunning-vpn opdracht uit.

5. Deze opdracht geven: ASA-AIP-CLI(config)#group-policy hillvalleyvpn internal

- 6. Geef deze opdrachten uit om de instellingen voor de clientverbinding te configureren:ASA-AIP-CLI (configuratie)#group-policy hillvalleyvpn-eigenschappenASA-AIP-CLI (configuratie)# (configuratie-groep-beleid)#dns-server waarde 172.16.1.11ASA 5500-AIP-CLI (configuratie)# (configuratie-groep-beleid)#vpn-tunnel-protocol IPSecASA-AIP-CLI (configuratie)# (configuratie-groep-beleid)#default-domeinwaarde test.com
- 7. Deze opdracht geven: ASA-AIP-CLI(config)#tunnel-group hillvalleyvpn ipsec-ra
- 8. Deze opdracht geven:

ASA-AIP-CLI(config)#tunnel-group hillvalleyvpn ipsec-attributes

9. Deze opdracht geven:

ASA-AIP-CLI(config-tunnel-ipsec)#pre-shared-key cisco123

10. Deze opdracht geven:

ASA-AIP-CLI(config)#tunnel-group hillvalleyvpn general-attributes

- 11. Geef deze opdracht uit om de lokale gebruikersdatabase voor authenticatie te raadplegen. ASA-AIP-CLI(config-tunnel-general)#authentication-server-group LOCAL
- 12. Associeer het groepsbeleid met de tunnelgroep ASA-AIP-CLI(config-tunnel-ipsec)# default-group-policy hillvalleyvpn
- 13. Geef deze opdracht uit in de algemene-attributenmodus van de hillvalleyvpn-tunnelgroep om de vpnpool die in stap 1 is gemaakt, aan de hillvalleyvpn-groep toe te wijzen. ASA-AIP-CLI(config-tunnel-general)#address-pool vpnpool

Config op het ASA-apparaat uitvoeren

ASA-AIP-CLI(config)#**show running-config** ASA Version 7.2(2)

hostname ASAwAIP-CLI

!

```
domain-name corp.com
enable password WwXYvtKrnjXqGbul encrypted
names
1
interface Ethernet0/0
nameif outside
security-level 0
ip address 10.10.10.2 255.255.255.0
1
interface Ethernet0/1
nameif inside
security-level 100
ip address 172.16.1.2 255.255.255.0
1
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
1
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
1
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name corp.com
pager lines 24
mtu outside 1500
mtu inside 1500
ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
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
group-policy hillvalleyvpn1 internal
group-policy hillvalleyvpn1 attributes
dns-server value 172.16.1.11
vpn-tunnel-protocol IPSec
default-domain value test.com
username marty password 6XmYwQ009tiYnUDN encrypted
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
```

```
sha-hmac
crypto dynamic-map outside_dyn_map 10 set transform-set
ESP-3DES-SHA
crypto dynamic-map outside_dyn_map 10 set security-
association lifetime seconds 288000
crypto map outside_map 10 ipsec-isakmp dynamic
outside_dyn_map
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
crypto isakmp nat-traversal 20
tunnel-group hillvalleyvpn type ipsec-ra
tunnel-group hillvalleyvpn general-attributes
address-pool vpnpool
default-group-policy hillvalleyvpn
tunnel-group hillvalleyvpn ipsec-attributes
pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
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
prompt hostname context
Cryptochecksum:0f78ee7ef3c196a683ae7a4804ce1192
: end
ASA-AIP-CLI(config)#
```

Configuratie van Cisco VPN-clientwachtwoord

Als u meerdere Cisco VPN-clients hebt, is het heel moeilijk om alle VPN-clientnamen en wachtwoorden te onthouden. Om de wachtwoorden in de VPN-clientmachine op te slaan, moet u de ASA/PIX- en de VPN-client configureren zoals in dit gedeelte wordt beschreven.

ASA/PIX

Gebruik de opdracht groepsbeleid eigenschappen in mondiale configuratiemodus:

```
group-policy VPNusers attributes
password-storage enable
Cisco VPN-client
```

Bewerk het .pcf-bestand en wijzig deze parameters:

SaveUserPassword=1 UserPassword=

Uitgebreide verificatie uitschakelen

In tunnelgroepsmodus, voer deze opdracht in om de uitgebreide authenticatie uit te schakelen, die standaard ingeschakeld is op PIX/ASA 7.x:

```
asa(config)#tunnel-group client ipsec-attributes
asa(config-tunnel-ipsec)#isakmp ikev1-user-authentication none
```

Nadat u de uitgebreide authenticatie uitschakelt, zetten de VPN-clients geen gebruikersnaam/wachtwoord voor een verificatie (Xauth) op. Daarom heeft de ASA/PIX niet de gebruikersnaam en de wachtwoordconfiguratie nodig om de VPN-clients te authenticeren.

Verifiëren

Probeer met de Cisco ASA te verbinden aan het gebruik van de Cisco VPN-client om te controleren of de ASA met succes is geconfigureerd.

1. Selecteer Connection Vermeldingen > New.

¥PN Client - Version 4.0.5 (Rel)			
Connection Entries Status Certificates	Log Options	Help	
Connect to my_remote_vpn Ctrl+O Disconnect Ctrl+D	adifu		CISCO SYSTEMS
Create Shortcut			
Modry		Host	Transport 🔺
D <u>e</u> lete			
Dyplicate			
Set as Default Connection Entry			
<u>N</u> ew			
Import	12		
Exit VPN Client Ctrl+Q			
•			
Not connected.			

2. Vul de gegevens in van uw nieuwe aansluiting.Het veld Host moet het IP-adres of de hostnaam van de eerder geconfigureerd Cisco ASA bevatten. De informatie over de groepsverificatie dient overeen te komen met de informatie die in <u>stap 4</u> wordt gebruikt. Klik op **Opslaan** als u klaar

-	👶 VPN Client Create New VPN Connection Entry
	Connection Entry: my_remote_vpn
	Host: 10.10.10.2
	Authentication Transport Backup Servers Dial-Up
	<u>G</u> roup Authentication <u>M</u> utual Group Authentication
	Name: hillvalleyvpn
	Password:
	Confirm Password: ******
	C Certificate Authentication
	Name:
	Send CA Certificate Chain
bent.	Erase User Password Cancel

3. Selecteer de nieuwe verbinding en klik op **Connect**.

VPN Client - Version 4.0.5 (Rel)		
Connection Entries Status Certificate	s Log Options Help	
Connect New Import	Modify Delete	CISCO SYSTEMS
Connection Entries Celuicates		
Connection Entry	Host	Transport 🔺
my_remote_vpn	10.10.10.2	IPSec/UDP
Not connected.		

4. Voer een gebruikersnaam en wachtwoord in voor uitgebreide verificatie. Deze informatie moet overeenkomen met de informatie die in <u>stap 5 en 6</u> is

👌 ¥PN Client User Authenticat	ion for "my_remote_vpn"
Enter Username and Password.	
Username: mar	ty ****
	OK Cancel

gespecificeerd.

5. Zodra de verbinding met succes is ingesteld selecteert u **Statistieken** uit het menu Status om de details van de tunnel te controleren.Dit venster toont informatie over verkeer en

👌 VPN Client	Statistics		×
Tunnel Details	Route Details	Firewall	
Address In Client: Server:	formation 172.16.1.100 10.10.10.2	Connection Informa Entry: Time:	a tion my_remote_vpn 0 day(s), 00:01.31
Bytes Receive Sent:	± 240 46816	Crypto Encryption: Authentication:	168-bit 3-DES HMAC-SHA1
Packets Encrypte Decrypte Discarde Bypasse	d: 332 d: 4 d: 137 d: 61	Transport Transparent Tunne Local LAN: Compression:	eling: Inactive Disabled None
			Reset
			<u>C</u> lose

dit venster wordt informatie over gesplitste tunneling weergegeven:

👌 VPN Client Sta	tistics		x		
Tunnel Details	oute Details Firew	ali			
Local LAN Route	Local LAN Routes		Secured Routes		
Network	Subnet Mask	Network 0.0.0.0	Subnet Mask 0.0.0.0		

Problemen oplossen

Gebruik dit gedeelte om de configuratie van het probleem op te lossen.

Onjuiste encryptie-ACL

ASDM 5.0(2) is bekend om een crypto toegangscontrolelijst (ACL) te maken en toe te passen die problemen kan veroorzaken voor VPN-clients die gesplitste tunneling gebruiken, evenals voor hardwareclients in netwerk-extensiemodus. Gebruik ASDM versie 5.0(4.3) of hoger om dit probleem te voorkomen. Raadpleeg Cisco bug-ID <u>CSCsc10806</u> (alleen <u>geregistreerde</u> klanten) voor meer informatie.

Gerelateerde informatie

- Cisco ASA 5500 Series adaptieve security applicaties
- Populairste oplossingen voor IPsec gemeenschappelijk L2L en Remote Access IPsec VPNprobleemoplossing
- Cisco ASA 5500 Series adaptieve security applicaties, probleemoplossing en meldingen
- Technische ondersteuning en documentatie Cisco Systems