# ASA/PIX: Split-tunneling voor VPN-clients toestaan in het ASA Configuration-voorbeeld

# Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Netwerkdiagram Verwante producten **Conventies** Achtergrondinformatie Split-tunneling op ASA configureren ASA 7.550x configureren met adaptieve security applicatie Manager (ASDM) 5.x ASA 8.500x configureren met adaptieve security applicatie Manager (ASDM) 6.x ASA 7.x en hoger configureren via CLI PIX 6.x configureren via CLI Verifiëren Connect met VPN-client Bekijk het VPN-clientlogboek Lokale LAN-toegang testen met Ping Problemen oplossen Beperking met aantal ingangen in een splitter-tunnelleiding Gerelateerde informatie

# **Inleiding**

Dit document bevat stap-voor-stap instructies over hoe u VPN-clients toegang tot het internet kunt geven terwijl ze in een Cisco adaptieve security applicatie (ASA) 5500 Series security applicatie zijn verbonden. Deze configuratie maakt VPN-clients veilig toegang tot bedrijfsmiddelen via IPsec mogelijk terwijl u onbeveiligde toegang tot het internet hebt.

**Opmerking:** Een volledige tunneling wordt gezien als de meest beveiligde configuratie omdat geen gelijktijdige toegang tot zowel internet als LAN door het apparaat mogelijk is. Een compromis tussen een volledige tunneling en een gesplitste tunneling maakt de lokale LAN-toegang van VPN-clients alleen mogelijk. Raadpleeg <u>PIX/ASA 7.x: Lokaal LAN-toegang voor VPN-clients</u> toestaan. Configuratievoorbeeld voor meer informatie.

# **Voorwaarden**

### **Vereisten**

Dit document gaat ervan uit dat er al een werkende VPN-configuratie voor externe toegang op de ASA bestaat. Raadpleeg <u>PIX/ASA 7.x als een externe VPN-server met ASDM Configuration</u> <u>Voorbeeld</u> als deze niet al is geconfigureerd.

#### Gebruikte componenten

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

- Cisco ASA 5500 Series security applicatie, versie 7.x en hoger
- Cisco Systems VPN-clientversie 4.0.5

**Opmerking:** Dit document bevat ook de PIX 6.x CLI-configuratie die compatibel is voor Cisco VPNclient 3.x.

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.

#### **Netwerkdiagram**

De VPN-client is gevestigd op een typisch SOHO-netwerk en sluit zich via het internet aan op het hoofdkantoor.



#### Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco PIX 500 Series security applicatie, versie 7.x.

#### **Conventies**

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

# **Achtergrondinformatie**

In een basisscenario van VPN-client naar ASA wordt al het verkeer van de VPN-client versleuteld en naar de ASA verzonden, ongeacht de bestemming ervan. Op basis van uw configuratie en het aantal ondersteunde gebruikers kan een dergelijke installatie bandbreedte-intensief worden. Splittunneling kan dit probleem helpen verminderen aangezien het gebruikers alleen dat verkeer dat voor het bedrijfsnetwerk over de tunnel bestemd is, laat verzenden. Al het andere verkeer, zoals onmiddelijk overseinen, e-mail of willekeurig bladeren, wordt naar het internet verzonden via het lokale LAN van de VPN-client.

# Split-tunneling op ASA configureren

## ASA 7.550x configureren met adaptieve security applicatie Manager (ASDM) 5.x

Voltooi deze stappen om uw tunnelgroep te configureren om een gesplitste tunneling voor de gebruikers in de groep toe te staan.

1. Kies **Configuratie > VPN > Algemeen > Groepsbeleid** en selecteer het groepsbeleid dat u lokale LAN-toegang in wilt schakelen. Klik vervolgens op



2. Ga naar het tabblad Clientconfiguratie.

eneral IPSec Client Configuration Client Firewall	Hardware Client	[NAC WebVPN]
Çi alı bila ile		
Check an inherit checkbox to let the corresponding	setting take its van	ue from the default group policy.
General Client Parameters   Cisco Client Parameter	s   Microsoft Client	Parameters
Banner:	🔽 Inherit	Edit Banner
Default Domain:	🔽 inherit	
Split Tunnel DNS Names (space delimited):	I⊻ Inherit	
Split Tunnel Policy:	🔽 Inherit	Y
Split Tunnel Network List:	🔽 Inherit	Manage
Address pools		
Available Pools		Assigned Pools (up to 6 entries)
	Add>>	1
	< <remove< td=""><td>il</td></remove<>	il

3. Schakel het vakje **Inherit** voor Split Tunnel Policy uit en kies **de onderstaande** lijst **met tunnelnetwerken**.

General Client Parameters Cisco Client Parameter	ers   Microsoft Client	Parameters
Banner:	Inherit	Edit Banner
Default Domain:	🔽 Inherit	
Spit Tunnel DNS Names (space delimited):	🔽 Inherit	
Split Tunnel Policy:	🗌 Inherit	Tunnel All Networks
Split Tunnel Network List:	🔽 Inherit	Tunnel All Networks Tunnel Network List Below Exclude Network List Below
Address pools		
Avaïable Pools	Add>> < <remove< th=""><th>Assigned Pools (up to 6 entries)</th></remove<>	Assigned Pools (up to 6 entries)

4. Schakel het vakje Inherit uit voor de netwerklijst met splitter en klik vervolgens op **Bewerken** om de ACL-Manager te starten.

eneral IPSec Client Configuration Client Firewall	Hardware Client	NAC WebVPN
Check an Inherit checkbox to let the corresponding	setting take its val	ue from the default group policy.
General Client Parameters Cisco Client Parameters	s Microsoft Client	Parameters
Banner:	🔽 Inherit	Edit Banner
Default Domain:	🔽 Inherit	
Call Tunnal PAIC blancas (anona delimited):		
Spiit Tunnel DNS Names (space delimited).	I≁ innent	1
Split Tunnel Policy:	linherit	Tunnel Network List Below
Solt Tunnal Network List:		None X Manage
Spin Former Verwork List.	1 Fillene	manage
Address pools		
Available Pools		Assigned Pools (up to 6 entries)
		1
	Add>>	
	< <remove< td=""><td></td></remove<>	

5. Kies in de ACL Manager Add > Add ACL... om een nieuwe toegangslijst te maken.

Add       Image: Edit       Image: Edit <t< th=""><th>andard ACL Extend</th><th>ed ACL</th><th></th><th></th><th></th><th></th></t<>	andard ACL Extend	ed ACL				
Add ACL. Action Description Add ACE. Action Description Action Action Description Action Action Action Description Action Action Action Description Action Act	Add 🔹 📑 Edit	î Delete 🔶	4 品面面。	·		
Add ACE	😔 Add ACL	dress	Action	Description		
Lie Flow Diegrem	Add ACE	15				
Aufe Flow Diegram	💼 Inseri					
ule Flow Disgram	Pinsen Andr					
ule Flow Diegram						
inside deny						
aufe Flow Diegrem						
tule Flow Disgram						
aule Flow Diagram						
aule Flow Diagram						
aule Flow Diegrem						
aule Flow Diagram						
aule Flow Diagram						
Rule Flow Diagram						
aule Flow Diagram						
aule Flow Diagram						
	tule Flow Diagram			in the second se		
			프		<u></u> - <u></u>	
				env env	•	
				• • •		

6. Typ een naam voor ACL en klik op

Oł	<b>K</b> .					
1	ACL Mana	ger				×
	Standard A	ICL Extended ACL				
	💠 Add	• 🗃 Edit 📋 Delete 🎓 🖣				
	No	Address	Action	Description	[	
			🔬 Add ACL		×	
			ACL Name: Sp	it_Tunnel_List		
			ок	Cancel	Help	
				-12		
						_
	Rule Flow	/ Diagram	al	inside_,, outside	L a	×
			2			
				💶 🔶 🖌 deny 💷 🔶		
			ОК	Cancel	Help	

7. Zodra ACL wordt gecreëerd, kies Add > Add ACE... om een Access Control Entry (ACE) toe

te

voegen.

ACL Manager					( )		
Standard ACL Extende	d ACL						
🗣 Add 🕞 📑 Edi: 🥤	Delete 🛧 🗸	4 2 座 画 -					
🍄 Add ACL	dress	Action	Description				
Add ACE							
insert After							
	_						
Rule Flow Diagram			neide	outeide	1		×
				oatolao			
			🔶 🖌 deny				
		OK	Cancel	Hel	p		

 Defineer de ACE die overeenkomt met het LAN achter de ASA. In dit geval is het netwerk 10.0.1.0/24.Kies Toestemming.Kies een IP-adres van 10.0.1.0Kies een netwerkmasker van 255.255.255.0.(Optioneel) Geef een beschrijving.Klik op OK.

No .	Address	Action	Description			
Splt_Tunnel_List						
	🕵 Add ACE				×	1
	Action					
	Action	🖌 Permit 💌				
	HostNetwo	ark				
	IP Addres	8: 10.0.1.0			¥	
	Netmask:	256.255.255.0			·	
	Description					
	The corporat	e network behind the A	ISA.		_	
		ок	Cancel	Help	1	
					_	
le Flow Diagram						
-		🖳 in	side of the side	utside	3	

9. Klik op **OK** om de ACL-Manager te



10. Verzeker u dat ACL die u zojuist hebt gemaakt, is geselecteerd voor Split Tunnel Network

Contract Decay Client Configuration	Lucido ana Clara	Lung Lung and
General IPSec Client Configuration   Client Firewall	Hardware Client	NAC   WEDVHN
Check an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.
General Client Parameters Cisco Client Parameters	s   Microsoft Client	Parameters
	_	1
Banner:	M Inherit	Edit Banner
Default Domain:	🔽 Inherit	
Solit Tunnel DNS Nemes (energy delimited):	V Inharit	
Spill runner pris Names (space delimited).	iv mient	]]
Split Tunnel Policy:	🗌 Inherit	Tunnel Network List Below
	_	
Split Tunnel Network List:	l Inherit	Splt_Tunnel_L Manage
Address pools		Split_Tunnel_List
🔽 Inherit		outside_cryptomap <sup>®</sup>
Available Pools		Assigned Pools (up to 6 entries)
	Add⊳⊳	1
	< <remove< td=""><td>i</td></remove<>	i

11. Klik op **OK** om naar de configuratie van het groepsbeleid terug te keren.

Name: hillvalleyvpn		
eneral IPSec Client Configuration Client Firev	vall Hardware Client	NAC WebVPN
Check an Inherit checkbox to let the correspondi	ing setting take its val	ue from the default group policy.
General Client Parameters Cisco Client Parame	ters   Microsoft Client	Parameters
T shoe old at a shoe		
Banner:	🗹 Inherit	Edit Banner
Default Domain:	🔽 Inherit	
Split Tunnel DNS Names (space delimited):	☑ Inherit	
Split Tunnel Policy:	🗖 Inherit	Tunnel Network List Below
Split Tunnel Network List:	🗖 Inherit	Spit_Tunnel_L Manage
- Address node		
Inherit		
Available Pools		Assigned Pools (up to 6 entries)
	Add⊳⊳	1
	< <remove< td=""><td></td></remove<>	

12. Klik op **Toepassen** en **Verzend** (indien nodig) om de opdrachten naar de ASA te sturen.

File Options To	als VVizerds	Help							Search:		Find +
G Home	or Sonfiguration	Monitoring	C Back	Forward	्र् Packet Tracer	Refr	esh Save	? Help			CISCO SYSTEMS
Interfaces Security Policy NAT Security Policy NAT Security Policy NAT Security Properties	Configuration VPN Configuration Configuratio	on > VFN > Gene Wizard eral VPN System Option Clent Update Turnel Group Group Policy Users Default Turnel Gete Zone Labs Integrity c dates Managemen c WPN al Proxy	al - O -Gr	roup Policy Manage VPN may be stored referenced by Name NUVELEYOPA DittorpPolicy (Sy	group policies . 3 internally on the 4 VPN funnel gr a stem Defa	A VPN gro e device o cups and u Type Internal	up policy is a cole x externelly on a f iser accounts. Turneling f Posc L2TP-IPSec JPSec	ection of use RADIUS serv Protocol c	er-oriented ethis ver. The group AAA Serv - N/A - N/A	bute/value po policy inform /er Group	iks that ation is Add <b>v</b> Edit Delete
						cisco	2		<u>i</u>	👌 7	/26/06 1:33:20 PM UTC

# ASA 8.500x configureren met adaptieve security applicatie Manager (ASDM) 6.x

Voltooi deze stappen om uw tunnelgroep te configureren om een gesplitste tunneling voor de gebruikers in de groep toe te staan.

1. Kies Configuration > Remote Access VPN > Network (Client) Access > Group Policy en kies het groepsbeleid waarin u lokale LAN-toegang wilt inschakelen. Klik vervolgens op Bewerken.

Configuration > Remote Access VPN > N	letwork (Client) Acce	ss > Group Policies	
Manage VPN group policies. A VPN group p externally on a RADIUS/LDAP server. The Add V C Edit Delete	policy is a collection of us group policy information	er-oriented attribute/value pairs that may n is referenced by VPN tunnel groups and u	be stored interna ser accounts.
Name	Туре	Tunneling Protocol	A
DfltGroPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webvpn	N/A
Drica proncy (Dyscon Dordary			
Defaultgroup	Internal	Inherited	N/A

2. Klik op **Tunneling** splitsen.

🥵 Edit Internal Group Policy:	hivalleyvpn	
General Servers	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, whice ACL that consists of list of addresses on the private network.	t do nol h is an
Splt Tunneling     E Browser Proxy     SSL VPN Client     IPsec Client     Client Access Rule     Client Firewal     Hardware Client	DNS Names:     Inherit       Policy:     ✓ Inherit       Network List:     ✓ Inherit	ige
	Intercept DHCP Configuration Message from Micosoft Clients	*
	Intercept: I Inherit C Yes C No	
	Subnet Mask (Optional): 0.0.0.0	¥
	OK Cancel Help	

3. Schakel het vakje **Inherit** voor Split Tunnel Policy uit en kies **de onderstaande lijst met tunnelnetwerken**.

🚰 Edit Internal Group Policy:	hivalleyvpn				
General Servers	Split tunneling network list: require tunneling. The sec ACL that consists of list of	s distinquish networks th urity appliance makes sp addresses on the prival	at require traffic to go th lit tunneling decisions on l e network.	rough the tunnel and th the basis of a network lis	ose that do no t, which is an
E Browser Proxy E Browser Proxy SSL VPN Client Psec Client Client Access Rule Client Firewall Hardware Client	DN5 Names: V Inherit Policy: Inherit Network List: V Inherit Intercept DHCP Confid DHCP Intercept lets Micr prior to XP, DHCP Interce	Tunnel Network List E Tunnel All Networks Tunnel All Network List B Exclude Network List I guration Message fro osoft XP clients use split ept provides the domain	elow elow Selow om Micosoft Clients tunneling with the securi name and subnet mask.	y appliance. For Window	Manage s clients
	Intercept: 🔽 Inherit	C Yes C No			
	3	Subnet Mask (Optional):	0.0.0.0		Y
×>					
	OK	Cancel	Help		

4. Schakel het vakje **Inherit** uit voor de netwerklijst Split Tunnel en klik vervolgens op **Bewerken** om de ACL Manager te starten.

Edit Internal Group Policy:	hivalleyvpn
General Servers EAdvanced	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network.
Split Tunneling IE Browser Proxy	DNS Names: 🔽 Inherit
<ul> <li>SSL VPN Client</li> <li>IPsec Client</li> </ul>	Policy: Inherit Tunnel Network List Below
Client Access Rule Client Firewall	Network List: None
Hardware Client	Intercept DHCP Configuration Message from Micosoft Clients
	Intercept: 🔽 Inherit C Yos C No
	Subnet Mask (Optional): 0.0.0.0
	OK Cancel Help

5. Kies in de ACL Manager Add > Add ACL... om een nieuwe toegangslijst te maken.



6. Typ een naam voor ACL en klik op **OK**.

	1000	1 1 1		
140	Audress	Action	Description	
	🔂 Add	ACL	×	
	ACL N	ame: Split_Tunnel_List		
		OK Cancel		



8. Defineer de ACE die overeenkomt met het LAN achter de ASA. In dit geval is het netwerk

10.0.1.0/24.Klik op de radioknop **Toestemming**.Kies het netwerkadres met masker **10.0.1.0/24**.(Optioneel) Geef een beschrijving.Klik op

Split_Tunnel_List					
	2 ALL ACT				
	Je Add ALE	and a second			
	Action: 📀 P	ermit C Deny			
	Address: 10.0	1.0/24			
	Houress, [10.0	.1.0/2.4			
	Description:				
	The Corporate	network behind the ASA	A		
		OK		ous T	
		OK		Help	

9. Klik op **OK** om de ACL-Manager te verlaten.

he ASA
ne ASA
ACA 91

10. Verzeker u dat ACL die u zojuist hebt gemaakt, is geselecteerd voor Split Tunnel Network List.

General Servers - Advanced	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which ACL that consists of list of addresses on the private network.	: do no n is an
E Browser Proxy	DN5 Names: 🔽 Inherit	
SSL VPN Client	Policy: 🗆 Inherit Tunnel Network List Below 💌	
Client Access Rule Client Firewall	Network List: Inherit Split_Tunnel_List Mana	ge
Hardware Client	Intercept DHCP Config Split_Tunnel_List	*
	DHCP Intercept lets Microsoft XP clients use split tunneling with the security appliance. For Windows client prior to XP, DHCP Intercept provides the domain name and subnet mask.	s
	Intercept: 🔽 Inherit C Yes C No	
	Subnet Mask (Optional): 0.0.0.0	-

11. Klik op **OK** om naar de configuratie van het groepsbeleid terug te

General	Split tunneling network list require tunneling. The set ACL that consists of list of	ts distinguish networks that require traffic to go through the tur curity appliance makes split tunneling decisions on the basis of a f addresses on the private network.	nel and those that do network list, which is
IE Browser Proxy	DNS Names: 🖾 Inherit		
SSL VPN Client     IPsec Client	Policy: 🕅 Inherit	Tunnel Network List Below	¥
	Network List: 🥅 Inherit	Split_Tunnel_List	▼ Manage.
	Intercept DHCP Conf	iguration Message from Micosoft Clients	
	DHCP Intercept lets Mic prior to XP, DHCP Interc	rosoft XP clients use split tunneling with the security appliance. cept provides the domain name and subnet mask.	For Windows clients
	Intercept: 🔽 Inherit	C Yes C No	
		Subnet Mask (Optional): 0.0.0.0	

12. Klik op **Toepassen** en **Verzend** (indien nodig) om de opdrachten naar de ASA te sturen.

Ninor	Turne	Turneline Dustavel	1
Name DfltGroBolicy (System Default)	Internal	12TB-TDSec TDSec webyop	N//
Defaultaroup	Internal	Inberited	N/4
hivalleyvon	Internal	svc.TPSec	N/A

## ASA 7.x en hoger configureren via CLI

In plaats van de ASDM te gebruiken, kunt u deze stappen in de ASA CLI voltooien om gesplitste tunneling op de ASA toe te staan:

**Opmerking:** De CLI Split Tunneling-configuratie is hetzelfde voor zowel ASA 7.x als 8.x.

1. Geef de configuratie op.

```
ciscoasa>enable
Password: *******
ciscoasa#configure terminal
ciscoasa(config)#
```

- 2. Maak de toegangslijst die het netwerk achter de ASA definieert. ciscoasa(config)#access-list Split\_Tunnel\_List remark The corporate network behind the ASA. ciscoasa(config)#access-list Split\_Tunnel\_List standard permit 10.0.1.0 255.255.255.0
- 3. Geef de configuratiemodus voor het groepsbeleid op voor het beleid dat u wilt wijzigen. ciscoasa(config)#group-policy hillvalleyvpn attributes ciscoasa(config-group-policy)#
- 4. Specificeer het gesplitste tunnelbeleid. In dit geval wordt het beleid **aangegeven**. ciscoasa(config-group-policy)#**split-tunnel-policy tunnelspecified**

- 5. Specificeer de gesplitste tunneltoegangslijst. In dit geval is de lijst **Split\_Tunnel\_List**. ciscoasa(config-group-policy)#split-tunnel-network-list value Split\_Tunnel\_List
- 6. Deze opdracht geven:

ciscoasa(config)#tunnel-group hillvalleyvpn general-attributes

- 7. Associeer het groepsbeleid met de tunnelgroep ciscoasa(config-tunnel-ipsec)# default-group-policy hillvalleyvpn
- 8. Sluit de twee configuratie-modi. ciscoasa(config-group-policy)#exit ciscoasa(config)#exit ciscoasa#
- 9. Sla de configuratie op in niet-vluchtige RAM (NVRAM) en druk op **ENTER** wanneer u wordt gevraagd om de bronbestandsnaam te specificeren.

Source filename [running-config]? Cryptochecksum: 93bb3217 0f60bfa4 c36bbb29 75cf714a 3847 bytes copied in 3.470 secs (1282 bytes/sec) ciscoasa#

#### PIX 6.x configureren via CLI

Voer de volgende stappen uit:

1. Maak de toegangslijst die het netwerk achter de PIX definieert.

```
PIX(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0
```

2. Maak een VPN groep *vpn3000* en specificeer de gesplitste tunnel ACL naar deze zoals wordt weergegeven: PIX(config)#vpngroup vpn3000 split-tunnel Split\_Tunnel\_List

**Opmerking:** Raadpleeg <u>Cisco Secure PIX Firewall 6.x en Cisco VPN-client 3.5 voor Windows</u> <u>met Microsoft Windows 2000 en 2003 IAS RADIUS-verificatie</u> voor meer informatie over VPN-configuratie voor externe toegang voor PIX 6.x.

# **Verifiëren**

Volg de stappen in deze secties om uw configuratie te controleren.

- <u>Connect met VPN-client</u>
- Bekijk het VPN-clientlogboek
- Lokale LAN-toegang testen met Ping

## Connect met VPN-client

Sluit uw VPN-client aan op de VPN-centrator om uw configuratie te controleren.

1. Kies uw verbindingsingang van de lijst en klik op **Connect**.

👶 VPN Client - Version 4.0.5 (Rel)		
Connection Entries Status Certificates Log Opt	ions <u>H</u> elp	
Connect New Import Modify	) XA V Delete	CISCO SYSTEMS
Connection Entry	Host	Transport
hilvalleyvpn	172.22.1.160	IPSec/UDP
<u>•</u>		
Not connected		

2. Voer je geloofsbrieven

👌 ¥PN Client   User	Authentication for "hillvalleyvpn"	×
CISCO SYSTEMS US	ername: marty issword: ****** OK	Cancel

3. Kies **Status > Statistieken...** om het venster met tunneldetails weer te geven, waar u de gegevens van de tunnel kunt inspecteren en verkeer kunt zien stromen.

👌 VPN Client 📋	Statistics			×
Tunnel Details	Route Details	Firewall		
Address Info	rmation	Connection Information	i.	
Client:	10.0.1.50	Entry:	hillvalley2	
Server:	172.22.1.160	Time:	0 day(s), 00:00.25	
Bytes		Crypto		
Received:	0	Encryption:	168-bit 3-DES	
Sent:	1494	Authentication:	HMAC-SHA1	
Packets		Transport		
Encrypted:	9	Transparent Tunneling:	Inactive	
Decrypted:	0	Local LAN:	Disabled	
Discarded:	0	Compression:	None	
Bypassed:	159			
			Reset	
			Close	

4. Ga naar het tabblad Route Details om de routes te zien die de VPN-client aan de ASA heeft beveiligd. In dit voorbeeld, waarborgt de client van VPN toegang tot 10.0.1.0/24 terwijl al het andere verkeer niet versleuteld en niet verzonden wordt over de

👌 ¥PN Client	Statistics		
Tunnel Details	Route Details Fire	wall	
Local LAN Ro	outes 🗟	Secured Rou	ites
Network	Subnet Mask	Network	Subnet Mask
		10.0.1.0	255.255.255.0
			<u>C</u> lose

## Bekijk het VPN-clientlogboek

Wanneer u het logbestand van VPN-client onderzoekt, kunt u bepalen of de parameter die

gesplitste tunneling specificeert, al dan niet is ingesteld. Ga naar het tabblad Log in de VPN-client om het logbestand te bekijken. Klik vervolgens op **loginstellingen** om aan te passen wat is vastgelegd. In dit voorbeeld is IKE ingesteld op **3 - Hoog** terwijl alle andere logelementen zijn ingesteld op **1 - Laag**.

👶 VPN Client - Version 4.0.5 (Rel)	
Connection Entries Status Certificates Log Options Help	
Disable Clear Log Settings Log Window	CISCO SYSTEMS
Connection Entries Certificates Log	
Cisco Systems VPN Client Version 4.0.5 (Ref) Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Windows, WinNT Running on: 5.1.2600 Service Pack 2	
Not connected.	11.

Cisco Systems VPN Client Version 4.0.5 (Rel) Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Windows, WinNT Running on: 5.1.2600 Service Pack 2

1 14:20:09.532 07/27/06 Sev=Info/6IKE/0x6300003B Attempting to establish a connection with 172.22.1.160.

!--- Output is supressed 18 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005D Client sending a firewall request to concentrator 19 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Systems Integrated Client, Capability= (Centralized Protection Policy). 20 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Intrusion Prevention Security Agent, Capability= (Are you There?). 21 14:20:14.208 07/27/06 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS \*(HASH, ATTR) to 172.22.1.160 22 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.22.1.160 23 14:20:14.208 07/27/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS \*(HASH, ATTR) from 172.22.1.160 24 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x63000010 MODE CFG REPLY: Attribute = INTERNAL\_IPV4\_ADDRESS: , value = 10.0.1.50 25 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x63000010 MODE\_CFG\_REPLY: Attribute = INTERNAL\_IPV4\_NETMASK: , value = 255.255.255.0 26 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300000 MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_SAVEPWD: , value = 0x0000000 27 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300000D MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_PFS: , value = 0x00000000 28 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300000E MODE\_CFG\_REPLY: Attribute = APPLICATION\_VERSION, value = Cisco Systems, Inc ASA5510 Version 7.2(1) built by root on Wed 31-May-06 14:45 !--- Split tunneling is permitted and the remote LAN is defined. 29 14:20:14.238 07/27/06 Sev=Info/5 IKE/0x6300000D MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_SPLIT\_INCLUDE (# of split\_nets), value = 0x00000001 30 14:20:14.238 07/27/06 Sev=Info/5 IKE/0x6300000F SPLIT\_NET #1 subnet = 10.0.1.0 mask = 255.255.255.0 protocol = 0 src port = 0 dest port=0 !--- Output is supressed.

#### Lokale LAN-toegang testen met Ping

Een extra manier om te testen dat de VPN-client is geconfigureerd voor gesplitste tunneling terwijl deze is aangesloten op de ASA, is door de ping-opdracht in de Windows-opdrachtregel te gebruiken. Het lokale LAN van de VPN-client is 192.168.0.0/24 en er is een andere host op het netwerk aanwezig met een IP-adres van 192.168.0.3.

```
C:\>ping 192.168.0.3
Pinging 192.168.0.3 with 32 bytes of data:
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre>
```

# Problemen oplossen

#### Beperking met aantal ingangen in een splitter-tunnelleiding

Er is een beperking met het aantal ingangen in een ACL die voor splitsingen tunnel wordt gebruikt. Aanbevolen wordt niet meer dan 50-60 ACE-items te gebruiken voor een bevredigende functionaliteit. U wordt geadviseerd om de subnetting optie uit te voeren om een bereik van IP adressen te bestrijken.

# Gerelateerde informatie

- PIX/ASA 750x als externe VPN-server met ASDM-configuratievoorbeeld
- <u>Cisco ASA 5500 Series adaptieve security applicaties</u>
- Technische ondersteuning en documentatie Cisco Systems