# Split-tunneling configureren voor VPN-clients op de ASA

## Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Netwerkdiagram
Verwante producten
Conventies
Achtergrondinformatie
Split-tunneling op de ASA configureren
De ASA 7.x configureren met Adaptieve Security Device Manager (ASDM) 5.x
De ASA 8.x configureren met ASDM6.x
De ASA 7.x en hoger via CLI configureren
PIX 6.x configureren via de CLI
Verifiëren
Verbinding maken met de VPN-client
Het VPN-clientlogboek bekijken
Lokale LAN-toegang testen met ping
Problemen oplossen
Beperking met aantal ingangen in een Split-tunnelACL
Gerelateerde informatie

# Inleiding

Dit document beschrijft het proces om VPN-clients toegang tot internet te geven terwijl u een tunneling maakt in een Cisco ASA 5500 Series security applicatie.

# 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 Remote VPN-server met ASDM Configuration</u> <u>Voorbeeld</u> als een nog niet is geconfigureerd.

Gebruikte componenten

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

- Software voor Cisco ASA 5500 Series security applicatie, versie 7.x en hoger
- Cisco Systems VPN-clientversie 4.0.5
- Adaptieve security apparaatbeheer (ASDM)



Opmerking: dit document bevat ook de PIX 6.x CLI-configuratie die compatibel is voor de Cisco VPN-client 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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Netwerkdiagram

De VPN-client bevindt zich op een typisch SOHO-netwerk en maakt via het internet verbinding met het hoofdkantoor.



Netwerkdiagram

#### Verwante producten

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

#### Conventies

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

## Achtergrondinformatie

Dit document bevat stap-voor-stap instructies hoe u VPN-clients toegang tot internet kunt geven terwijl ze een tunnel zijn gegraven in een Cisco adaptieve security applicatie (ASA) 5500 Series security applicatie. Deze configuratie biedt VPN-clients beveiligde toegang tot bedrijfsbronnen via IPsec terwijl ze onbeveiligde toegang tot het internet geven.



Opmerking: volledige tunneling wordt beschouwd als de best beveiligde configuratie omdat het apparaat geen gelijktijdige toegang tot zowel internet als het LAN van het bedrijf mogelijk maakt. Een compromis tussen volledige tunneling en gesplitste tunneling biedt alleen lokale LAN-toegang voor VPN-clients. Zie <u>PIX/ASA 7.x: Local LAN Access for</u> <u>VPN Clients Configuration Voorbeeld</u> voor meer informatie.

In een basis-VPN-client naar ASA-scenario wordt al het verkeer vanaf de VPN-client versleuteld en naar de ASA verzonden, ongeacht wat de bestemming is. Gebaseerd op uw configuratie en het aantal gebruikers dat wordt ondersteund, kan een dergelijke installatie bandbreedte-intensief worden. Split-tunneling kan werken om dit probleem te verlichten omdat het gebruikers in staat stelt alleen dat verkeer te verzenden dat is bestemd voor het bedrijfsnetwerk over de tunnel. Al het andere verkeer, zoals instant messaging, e-mail of willekeurig browsen, wordt via het lokale LAN van de VPN-client naar het internet verzonden.

# Split-tunneling op de ASA configureren

### De ASA 7.x configureren met Adaptieve Security Device Manager (ASDM) 5.x

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

1. Kies Configuratie > VPN > Algemeen > Groepsbeleid en selecteer het Groepsbeleid waarin u lokale LAN-toegang wilt inschakelen. Klik vervolgens op Edit (Bewerken).



2. Ga naar het tabblad Clientconfiguratie.

General IPSec Client Configuration Client Firewall	Hardware Client	NAC WebVPN
rی Check an Inherit checkbox to let the corresponding	setting take its value	e from the default group policy.
General Client Parameters Cisco Client Parameters	s   Microsoft Client P	Parameters
Banner:	🔽 Inherit	Edit Banner
Default Domain:	🔽 Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Split Tunnel Policy:	🔽 Inherit	<u>v</u>
Split Tunnel Network List:	🔽 Inherit	Manage
Address pools		
⊠ Inherit		Analyzed Davis (on the Combine)
Available Pools		Assigned Poors (up to 6 entries)
	Add>>	
	< <remove< td=""><td></td></remove<>	

3. Schakel het vakje Inherit voor het beleid voor de Split-tunnel uit en kies Tunnel Network List Below ..

Name: hillvalleyvpn		
meral IPSec Client Configuration Client Firewall	Hardware Client	
sherai   P360 chera configeration   Cilent Pirewaii	I naroware cienc	
Check an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.
General Client Parameters	L Margarett Clicut	Parameters I
General Client Parameters   Cisco Client Parameters	s   Microsoft Cilerit	Parameters
Banner'	V Inherit	Edit Banner
Danner.	14 In the second	LONG ROMITION ST
Default Domain:	🔽 Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
	_	
Split Tunnel Policy:	I Inherit	Tunnel All Networks
	_	Tunnel All Networks Tunnel Network List Below
Split Tunnel Network List	l⊻ Inherit	Exclude Network List Below
Address pools		
Avaïable Pools		Assigned Pools (up to 6 entries)
		(
	Addee	]
	< <remove< td=""><td></td></remove<>	

Schakel het vakje Inherit voor de netwerklijst van de Split-tunnel uit en klik vervolgens op Beheren om de ACL-beheer te starten.

Name:       hilvalleyvpn         eneral       PSec       Client Configuration       Client Firewall       Hardware Client       NAC       WebVPN         Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.         General Client Parameters       Cisco Client Parameters       Microsoft Client Parameters         Banner:       Imment       Edit.Berner         Default Domain:       Imment       Edit.Berner         Spit Tunnel DNS Names (space delimited):       Imment       Tunnel Network List Below         Spit Tunnel Policy:       Imment       Tunnel Network List Below         Spit Tunnel Network List:       Imment       Manage         Address pools       Address pools       Address pools         Imment       Address pools       Address         Variable Pools       Address       Address	Name: hillvalleyvpn	
eneral PSec Client Configuration Client Firewall Hardware Client NAC WebVPN Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. General Client Parameters Clisco Client Parameters Microsoft Client Parameters Banner:		
eneral [Page]       Clerk Configuration [Clerk Parameters]         Check an Inherit checkbox to let the corresponding setting take its value from the defauit group policy.         General Clerk Parameters       Cisco Clerk Parameters         Banner:       Inherit         Default Domain:       Inherit         Split Tunnel DNS Names (space delimited):       Inherit         Split Tunnel Policy:       Inherit         Split Tunnel Network List:       Inherit         Address pools       Address pools         Inherit       Address pools         Address pools       Address pools	annual Income Client Configuration Client Stressell Mandulane Client Mar	[ 10/444 (TA) ]
Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.          General Clent Parameters       Cisco Clent Parameters       Microsoft Clent Parameters         Banner:       Inherit       Edit Benner         Default Domain:       Inherit       Edit Benner         Split Tunnel DNS Names (space delimited):       Inherit       Tunnel Network List Below         Split Tunnel Policy:       Inherit       Tunnel Network List Below         Address pools       Address pools       Address pools         Image:       Address       Address	eneral   IPSec   Client Configuration   Client Pirewall   Hardware Client   NAC	WEDVHN
General Client Parameters Cisco Client Parameters   Banner: Inherit   Default Domain: Inherit   Spit Tunnel DNS Names (space delimited): Inherit   Spit Tunnel Policy: Inherit   Spit Tunnel Network List: Inherit   Address pools   Imherit   Address pools   Imherit   Address pools	Check an Inherit checkbox to let the corresponding setting take its value from	the default group policy.
Banner: Inherit   Default Domain: Inherit   Spit Tunnel DNS Names (space delimited): Inherit   Spit Tunnel Policy: Inherit   Spit Tunnel Network List: Inherit   Address pools Inherit   Address pools Address pools   Inherit Assigned Pools (up to B entries)   Address Address	General Client Parameters   Cisco Client Parameters   Microsoft Client Param	eters
Default Domain:   Default Domain:   Spit Tunnel DNS Names (space delimited):   Inherit   Spit Tunnel Policy:   Inherit   Spit Tunnel Network List:   Inherit   Address pools   Inherit   Address pools   Inherit   Address pools   Address pools (applied Pools (up to 6 entries)) (applied Pools (up to 6 entries)<	Banner: 🔽 Inherit	Edit Benner
Default Domain: Image: Construction   Spit Tunnel DNS Names (space delimited): Image: Construction   Spit Tunnel Policy: Immerit   Spit Tunnel Network List: Immerit   Address pools Immerit   Address pools Address   Immerit Assigned Pools (up to 6 entries)   Address Immerit		
Spit Tunnel DNS Names (space delimited):   Spit Tunnel Policy:   Inherit   Tunnel Network List:   Inherit   Address pools   Address pools </td <td>Default Domain: 🔽 Inherit</td> <td></td>	Default Domain: 🔽 Inherit	
Spit Tunnel Policy:     Spit Tunnel Network List:     Immention     Address pools     Address	Split Tunnel DNS Names (space delimited):	
Spit Tunnel Policy:		
Spit Tunnel Network List:     Address pools     Inherit        Available Pools        Add>>           Add>>           Add>>        Add>>	Split Tunnel Policy. I Inherit <u> Tun</u>	rel Network List Below
Address pools          Address pools         Inherit         Available Pools         Add>>         Add>>         < <remove< td=""></remove<>	Split Tunnel Network List:	me Manage N
Address pools       Inherit     Available Pools     Assigned Pools (up to 6 entries)       Add>>		
Available Pools Add>> Add>> Add>>	Address pools	
Add>>	Available Pools Ass	igned Pools (up to 6 entries)
<-Remove	AdbA	
	<-Remove	

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

Serviced ACL            • Add          • Example Action             • Add ACL            • Add ACL            • Proof:            • P	ACL Manager					( I)		X
● Add       ● Col: ● Col: ● ● Adie       ● Adie       Description         ● Add DCS:       ● Col: DCS:       ● Col: DCS:       ● Col: DCS:         ● Col: DCS:       ● Col: DCS:       ● Col: DCS:       ● Col: DCS:         ● Col: DCS:       ● Col: DCS:       ● Col: DCS:       ● Col: DCS:         ● Col: DCS:       ● Col: DCS:       ● Col: DCS:       ● Col: DCS:         ● Col: DCS:       ● Col: DCS:       ● Col: DCS:       ● Col: DCS:         ● Col: DCS:       ● Col: DCS:       ● Col: DCS:       ● Col: DCS:         ● Col: DCS:       ● Col: DCS:       ● Col: DCS:       ● Col: DCS:         ● Col: DCS:       ● Col: DCS:       ● Col: DCS:       ● Col: DCS:         ● Col: DCS:       ● Col: DCS:       ● Col: DCS:       ● Col: DCS:         ● Col: DCS:       ● Col: DCS:       ● Col: DCS:       ● Col: DCS:         ● Col: DCS:       ● Col: DCS:       ● Col: DCS:       ● Col: DCS:         ● Col: DCS:       ● Col: DCS:       ● Col: DCS:       ● Col: DCS:         ● Col: DCS:       ● Col: DCS:       ● Col: DCS:       ● Col: DCS:         ● Col: DCS:       ● Col: DCS:       ● Col: DCS:       ● Col: DCS:         ● Col: DCS:       ● Col: DCS:       ● Col: DCS:       ● Col: DCS:	Stenderd AG. Edended	I ACL						
Or And ACL     Action     Description       Image: Action of the second	💠 Add 🕞 🔤 🕬 🎁	Prior 9	4 X B	10				
Image: Control in the second secon	Add AGL.	dress	Action		Description			
	Constant							
	The losest After.							
		-						

Typ een naam voor de ACL en klik op OK.

Ki ACL Manager			X
Stendard ACL Extended ACL			
◆ Add → (() 100 () () () () () () () () () () () () ()	————————————————————————————————————		
No Address	Addon Description		
	🖆 Abl ACL	×	
	AG, Name: Splf_Turnel_List		
	OK N Cancel	Holp	
- Bule Flower Classes			
Hat For Dagram	uinside	10 - S	^ l
	OK Cancel	THE	

Zodra de ACL is gemaakt, kiest u **Toevoegen > ACE toevoegen.** .om een Access Control Entry (ACE) toe te voegen.

٠



Bepaal het ACE dat aan LAN achter ASA beantwoordt. In dit geval is het netwerk 10.0.1.0/24.

a.

•

Selecteer Permit (Toestaan).

b.

Kies IP-adres 10.0.1.0.

c.

Kies een Netmasker van 255.255.255.0.

d.

(Optioneel)Geef een beschrijving.

Klik op >  $\mathbf{OK}$ .

Add - Image: Delete + A B Image: Added - Added         No       Address         Address       Addres         Solt_Thereol Lid         Image: Address       Address         Address       Address         Address       Address         Address       Address         Address       Address         Address       Address         Address       Power Image: Ima	Stendard ACL Extern	er AG.		
No     Address     Address       Soll. Torrest Litt         Image: Address         Address         Address         Address         P Address      <	◆ Add → 圖* 6.00	1 Detes 9 6 X Ra 10		
Solt formet List	No	Address Action Description		
Action       Action       Image: Fourier in the second sec	Selt_Turnel_List			
Addam     Addam       Addam     Addam       Addam     Image: Concernege and the ASA.				
Action       Action       Image: Concerned on the second s		Bradd ALL	X	
Action:       ************************************		- Adian		
P Address       0010       IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		Action w Power *		
P Address:     100.1.0     W       Hetwask:     125.255.255.0     W       Description:     The corporate network behind the ASA.       DK     Cancel     Hop		Horthletwork		
Network     195-205-205-0       Description       The corporate network behind the ASA.		P Addess: 10010	¥	
		Netwask: 255.255.255.0	w	
Thue flow Diegram		Description		
OK         Carce         Hop           PLie Row Diagram         31         aveide         33		The corporate network behind the ASA.		
Thuếe Row Daigram				
Thuế Naw Diagram		OK OWNER HIMP		
Pule Now Diagram				
5- Invite outside -5				
	Rule Flow Disgram	au invide		3
		"Internet to the second s		

Klik op OK om ACL Manager af te sluiten.

•

e.



Zorg ervoor dat de ACL die u zojuist hebt gemaakt, is geselecteerd voor de netwerklijst van splitste tunnels.

t Internal Group Policy: hillvalleyvpn		
biener Filbusheuren		
Norme. prevanegraphi		
General IPSec Client Configuration Client Firewai	Hardware Client	NAC WebVPN
Check an interit checkbox to let the corresponding	setting take its valu	e from the default group policy.
	1	
General Client Parameters   Cisco Client Parameter	s Microsoft Client	Parameters
Barnar	☑ Interit	Edt Envier
Default Domain:	P intert	
Solit Tunnel DNS Names (space delimited);	☑ Inherit	
		1
Split Tunnel Policy:	Inherit	Tunnel Network List Below
	_	
Spilt Tunnel Network List:	l Inherit	Spit_Turnel_L Manage
Address pools		Spit_Turnet_List
🖂 inherit		cutside_cryptomap*
Avaiolife Poolo		Appigned Peolo (up to 6 entries)
	Addres	1
	collemova	il in the second se

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

٠

Name:       Nelseyupn         Seneral       IPSic       Clerit Configuration       Clerit Firewall       Hardware Clerit       NAC       WebVPN         Check an Interit checkbox to let the corresponding setting take its value from the default group policy.       General Clerit Parameters       Cloco Clerit Parameters       Microsoft Cliert Parameters         Banner:       Immet       Elf: Borner.       Immet       Elf: Borner.         Default Donvaix       Immet       Immet       Elf: Borner.         Spit Tunnel DNS Names (space delimited):       Immet       Immet Network List       Immet         Spit Tunnel Network List       Immet       Spit Tunnel Network List       Manage         Address pools       Immet       Spit Tunnel Network List       Manage	Nome:         Physicspan           Ceneral (PSac Client Configuration)         Client Prevent)         Hardware Client   NAC   WebVPN            Check an Inhert checkbox to let the corresponding setting take its value from the default group policy.         Ceneral Client Parameters         Cloco Client Parameters           Ceneral Client Parameters         Cloco Client Parameters         Microsoft Client Parameters         Edit Borner.           Default Domein:         Imherit         Edit Borner.         Edit Borner.           Default Domein:         Imherit         Edit Borner.           Spit Tunnel DNS Names (space definited):         Imherit         Tunnel Network List Below           Spit Tunnel Policy.         Imherit         Tunnel Network List         Menage           Address pools         Imherit         Spit Tunnel Network List         Menage	Neme:       Neme:       NetWork         General       IPSec       Clert Configuration       Clert Prevent       Hardware Clert       NAC       WebVPN         Check an Interit checkbox to let the corresponding setting take its value from the detauit group policy.       Clert Parameters       Cloco Clert Parameters       Morosoft Clert Parameters         Benner:       IP Interit       Edit Eonner.       IP Interit       Edit Eonner.         Detault Donveix       IP Interit       Edit Eonner.       Edit Eonner.         Spit Tunnel DNS Nenes (space delinited)       IP Interit       Immediate Setow       Immediate Setow         Spit Tunnel Network List       Interit       Immediate Setow       Immediate Setow       Immediate Setow         Address pools       Immediate Setow       Immediate Setow <t< th=""><th>Neme:       Pithaleyupn         General (PSec Clent Configuration Clent Firewall   Hardware Clent   NAC   WebVPN          Check an Inhert Checkbox to let the corresponding setting take its value from the default group policy.         General Clent Parameters       Cloco Clent Parameters   Morosoft Clent Parameters           Banner:       If Inherit         Default Donvair:       Inherit         Split Tunnel DNS Names (space definited):       Inherit         Split Tunnel Policy:       Inherit         Split Tunnel Network List:       Inherit         Address pools       Manage</th><th>t Internal Group Policy: hillvalleyvpn</th><th>1 1 1</th><th></th><th>X</th></t<>	Neme:       Pithaleyupn         General (PSec Clent Configuration Clent Firewall   Hardware Clent   NAC   WebVPN          Check an Inhert Checkbox to let the corresponding setting take its value from the default group policy.         General Clent Parameters       Cloco Clent Parameters   Morosoft Clent Parameters           Banner:       If Inherit         Default Donvair:       Inherit         Split Tunnel DNS Names (space definited):       Inherit         Split Tunnel Policy:       Inherit         Split Tunnel Network List:       Inherit         Address pools       Manage	t Internal Group Policy: hillvalleyvpn	1 1 1		X
General IPSec Clert Configuration Clert Firewall Hardware Clert NAC WebVPN   Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. Ceneral Clert Parameters   Clert Parameters Cloco Clerit Parameters Microsoft Clert Parameters  Edit Environ  Edit Environ Edit Environ  Edit Environ  Ed	General PSec Clent Contiguration Clent Finewaii Hardware Clent NAC WebVPN   Check an Inhert checkbox to let the corresponding setting take its value from the default group policy.   General Clent Parameters Cloco Clent Parameters Microsoft Clent Parameters   Banner: Image: Image: Image: Image item item item item item item item ite	General       PSec       Clert Configuration       Clert Firewall       Hardware Clert       NAC       WebVPN         Check as Inherit checkbox to let the corresponding setting take its value from the default group policy.       Ceneral Clert Parameters       Cisco Clerit Parameters       Microsoft Clerit Parameters         Barner:       Image: Clerit Domain       Image: Clerit Parameters       Microsoft Clerit Parameters       Edit Porver         Default Domain       Image: Clerit Parameters       Image: Clerit Parameters       Image: Clerit Parameters         Spit Tunnel DNS Names (space definited):       Image: Clerit Parameters       Image: Clerit Parameters         Spit Tunnel Policy:       Image: Clerit Parameters       Manage         Address pools       Address pools       Image: Clerit Parameters	General IPSec Clert Configuration Clert Preventi Hardware Clert NAC WebVPN   Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. Ceneral Clert Parameters   Cleret Parameters Cloco Clert Parameters Microsoft Clert Parameters Banner:  Default Domain  Spit Tunnel DNS Names (space definited):  Spit Tunnel Policy:  Address pools  Address pools	Nome: hilvsileyvpn			
Check an Inhert checkbox to let the corresponding setting take its value from the default group policy.   General Client Parameters   Banner:   Pinhert   Default Donvein:   Pinhert   Spit Tunnel DNS Names (space definited):   Pinhert   Spit Tunnel Policy:   Inhert   Spit Tunnel Network List:	Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.  Ceneral Client Parameters Cloco Client Parameters Microsoft Client Parameters  Default Domain:  Default Domain:  Pinherit  Spit Tunnel DNS Names (space definited):  Pinherit  Spit Tunnel Policy:  Nerror:  Address pods  Address pods	Check an Inhert checkbox to let the corresponding setting take its value from the default group policy.  General Clert Parameters Cisco Clerit Parameters Microsoft Clert Parameters Banner: Default Donwaix Finherit Spit Tunnel DNS Names (space definited) Finherit Spit Tunnel Policy: Spit Tunnel Network List Menage Address pools	Check an Inhert checkbour to let the corresponding setting take its value from the default group policy.   General Clerit Parameters Cloco Clerit Parameters   Barner: Image: Clerit Parameters   Default Donvaix Immerit   Spit Tunnel DNS Names (space delimited): Immerit   Spit Tunnel Policy: Immerit   Spit Tunnel Network List: Immerit   Address pools	Seneral IPSec Client Configuration Client Firewall	Hardware Client	NAC WEDVPN	
General Client Parameters       Cisco Client Parameters       Microsoft Client Parameters         Banner:       Image: Cisco Client Parameters       Edt Environ         Default Donvain:       Image: Cisco Client Parameters       Edt Environ         Spit Tunnel DNS Names (space delinited):       Image: Cisco Client Parameters       Image: Cisco Client Parameters         Spit Tunnel Policy:       Image: Cisco Client Parameters       Image: Cisco Client Parameters         Spit Tunnel Policy:       Image: Cisco Client Parameters       Image: Cisco Client Parameters         Spit Tunnel Policy:       Image: Cisco Client Parameters       Image: Cisco Client Parameters         Spit Tunnel Network List:       Image: Cisco Client Parameters       Manage         -Addresse pools       Cisco Client Parameters       Manage	General Clent Parameters       Cisco Clent Parameters       Microsoft Clent Parameters         Banner:       Image: List Edit Edit Parameters         Default Domain:       Image: List Edit Edit Parameters         Split Tunnel DNS Names (space delimites):       Image: List Below         Split Tunnel Policy:       Image: List Below         Split Tunnel Network List:       Image: List Below         Address pools       Image: List Below	General Client Parameters       Microsoft Client Parameters         Banner:       Image: Client Parameters         Default Donvain:       Image: Client Parameters         Spit Tunnel DNS Names (space delimited):       Image: Client Parameters         Spit Tunnel Policy:       Image: Client Parameters         Spit Tunnel Network List:       Image: Client Parameters         Address pools       Manage: Client Parameters	General Clent Parameters       Cisco Clent Parameters       Microsoft Clent Parameters         Benner:       Image: Cisco Clent Parameters       Edit Enviror         Default Donwin:       Image: Cisco Clent Parameters       Edit Enviror         Spit Tunnel DNS Names (space delimited):       Image: Cisco Clent Parameters       Image: Cisco Clent Parameters         Spit Tunnel Policy:       Image: Cisco Clent Parameters       Image: Cisco Clent Parameters         Spit Tunnel Network List:       Image: Cisco Clent Parameters       Image: Cisco Clent Parameters         Address pools       Address pools       Image: Cisco Clent Parameters       Image: Cisco Clent Parameters	Check an Inherit checkbox to let the corresponding a	setting take its valu	e from the detault group policy.	
Banner:       Image: Conversion         Default Donvair:       Image: Conversion         Spitt Tunnel DNS Names (space delimited):       Image: Conversion         Spitt Tunnel Policy:       Image: Conversion         Spitt Tunnel Network List:       Image: Conversion         Address paols       Image: Conversion	Banner: Image: Edf:Enver   Default Dowain: Image: Image: Edf:Enver   Spit Tunnel DNS Names (space delimited): Image: I	Barner: Image: Edt:Edt:   Detaut Donver: Image: Edt:   Spit Tunnel DNS Names (space delimited): Image:	Banner: Finherit Edit Borner Detaut Domain Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Spit Tunnel Network List: Inherit Spit Tunnel Network List: Manage Address pods	General Client Parameters Cisco Client Parameters	Microsoft Client	Parameters	
Detault Domain:     Spit Tunnel DNS Names (space delimited):     Spit Tunnel Policy:     Inherit     Spit Tunnel Network List:     Inherit     Spit Tunnel Network List:     Inherit     Spit Tunnel Network List:     Address pools	Detsut Domain: Image: Im	Default Domein:  Spit Tunnel DNS Names (space delimited):  Spit Tunnel Network List Below  Spit Tunnel Network List:  Inherit Spit Tunnel Network List Below Address pools	Default Donwin:   Spit Tunnel DNS Names (space delimited):  Spit Tunnel Policy:  Spit Tunnel Network List  Spit Tunnel Network List:  Address pools	Barner:	🔽 Inherit	Edt Borner	
Spit Tunnel DNS Names (space delimited):  Spit Tunnel Policy:  Spit Tunnel Network List  Address pools	Spit Tunnel DNS Names (space delimited):  Spit Tunnel Policy:  Spit Tunnel Network List:  Address pools	Spit Tunnel DNS Names (space delimited):  Spit Tunnel Policy:  Spit Tunnel Network List:  Address pools	Spit Tunnel DNS Names (space delimited):  Spit Tunnel Policy:  Spit Tunnel Network List:  Address pode	Default Domain:	P intert		
Spit Tunnel Policy:	Spit Tunnel Policy: Inherit Tunnel Network List Below   Spit Tunnel Network List: Inherit Spit Tunnel L.  Manage  Address pools	Spit Tunnel Policy: Inhert Tunnel Network List Below   Spit Tunnel Network List: Inhert Spit_Tunnel L.  Menage Address pools	Spit Tunnel Policy:   Spit Tunnel Network List  Spit Tunnel Network List  Address pools	Split Tunnel DNS Names (space delimited):	I⊽ inherit		
Spit Tunnel Network List: Inhert Spit Tunnel L. Manage	Spit Tunnel Network List: Inhert Spit Tunnel L. * Manage	Spit Tunnel Network List: Inhert Spit_Tunnel L. Manage Address pools	Spit Tunnel Network List: Inhert Spit Tunnel L. Manage	Split Tunnel Policy:	inherit	Turnel Network List Below	
-Address pools	Address pools	Address pools	Address pods	Split Tunnel Network List:	☐ inhert	Spit_Tunnel_L Manage	
				-Address pools			

Klik op Apply (Toepassen) en vervolgens op Send (Verzenden) (waar vereist) om de opdrachten naar de ASA te sturen.

٠



De ASA 8.x configureren met ASDM 6.x

•

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

Kies **Configuratie > Externe toegang VPN > Netwerktoegang (client) > Groepsbeleid** en kies het Groepsbeleid waarin u lokale LAN-toegang wilt inschakelen. Klik vervolgens op Edit (Bewerken).

A total ( Col ca) Contract			
A HOD COL Delete			
Name	Type	Tunneling Protocol	
DRtGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webvpn	N(A
OfftGrpPolicy (System Default) Defaultgroup	Internal	L2TP-IPSec, IPSec, webvpn Inherited	N/A

Klik op Split-tunneling.

🏂 Ed	it Internal Group Policy	hivalleyvpn				
	It Internal Group Policy General Sorvers Advanced Golt Turneling E Browser Procy E SSL VPN Client E IPsec Client Client Access Rule Client Access Rule Client Firewal Hardware Client	Spit tunneling retwork let require tunneling. The sec ACL that consists of list of DNS Names: IF Inherit Policy: IF Inherit Network List: IF Inherit Intercept DHCP Confi DHCP Intercept lets Nic prior to XP, OHCP Interce Intercept: IF Inherit	to distinguish networks the party appliance makes spl f addresses on the privato in the privato in the senge from rosoft XP clents use split from part provides the domain of cost provides the domain of	et require traffic to go through t t tunneling decisions on the bas a network. m Micosoft Clients tunneling with the security appli name and subnet mask.	the turnel and tho is of a network list	ee that do no , which is an Motoge s clients
l		Intercept: 🖓 Inherit	C Yes C No Subnet Mesk (Optional):	0.0.0.0		<u>×</u>
E.						

Schakel het vakje Inherit voor het Split-tunnelbeleid uit en kies hieronder de lijst met tunnelnetwerken.

ſ	Edit Internal Group Policy	: hivalleyvpn	
	General Servers	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do n require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is a A/CL that consists of list of addresses on the private network.	nc
		Policy: Dinherit Turnel Network List Below	
	Clerit Access Rule	Network Let: V Inherit Tunnel Al Network List Below	
	- Hardware Clienc	Intercent DHCP Configuration Message from Microsoft Clients (1	81
		Intercept: IP Intercept into the cents use spit currency with the security appliance. For Windows clients prior to XP, DHCP Intercept provides the domain name and subnet mask.	

Schakel het vakje Inherit voor de netwerklijst van de Split-tunnel uit en klik vervolgens op Beheren om de ACL-beheer te starten.

f Edit Internal Group Policy	: hiralleyvpn
Genéral Servins El Advanced	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.
	DNS Names: 🔽 Inherit
B-IPse: Clent	Policy: Dinherit Turnel Network List Below +
- Client Access Rule - Client Firewall	Network List: Street None
·maroware Cienc	Intercept DHCP Configuration Message from Micosoft Clients (*)
	DHCP Intercept lets Microsoft XP clients use split tunneling with the security appliance. For Windows clients prior to XP, DHCP Intercept provides the domain name and subnet mask.
	Intercept: 🔽 Inherit C Yes C No
	Subret Hask (Options): 0.0.0.0

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

i ACI	. Manager		1999			
Stan	idard ACL Extend	fed ACL				
*	Add 🔹 📓 Edit	💼 Delete 👌	4 × 1	B +		
4	Add ACL	<b>3</b>	Action	18	Description	
+	Add ACE					
1.2	Insert					
-	Insert After					

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

•

No _	Address	Action	Description	
				1
	Add Act N	ACL	×	
		OK Cano	el Help	
				]

Zodra de ACL is gemaakt, kiest u Add > Add ACE... om een Access Control Entry (ACE) toe te voegen.



Bepaal het ACE dat aan LAN achter ASA beantwoordt. In dit geval is het netwerk 10.0.1.0/24.

a.

.

Klik op de radioknop Toestaan.

b.

Kies het netwerkadres met masker 10.0.1.0/24.

c.

(Optioneel) Geef een beschrijving op.

d.

Klik op OK.

📫 ACL Manager						
Standard ACL Extended AC	1]					
🗢 Add 👻 🔟 Edt 🍈 E	belete ∲ ∉ 🐰	Ra Bla -				
No Addr	ess Action		Description			
Split_Tunnel_List						
	al	-		-	_	
	NOU HCC					
	Action: (* Permit C	Deny				
	Address: 10.0.1.0/24			-		
	Description:					
	The Corporate network b	ehind the ASA				
		OK	Cancel	Help		
					1	

Klik op OK om ACL Manager af te sluiten.

ACL Manager					
Standard ACL Printers	aa wa l				
Scandard Act   Extend	ed ACL				
🗣 Add 🔹 💽 Edit	T Delete	* <b>%</b>			
No	Address	Action		Description	
E Split_Tunnel_List					
1 10.0.1	.0/24	🥜 Permit	The Corporate	e network behind ti	IE ASA
			C or D	Cancel	Halp

Zorg ervoor dat de ACL die u zojuist hebt gemaakt, is geselecteerd voor de netwerklijst van splitste tunnels.

Clent Access Rule Clent Presail Hardware Clent Hardware Clent Intercept DHCP Config Spit_Turnel_List DHCP Intercept lets Microsoft XP clents use spit turneling with the security appliance. For Windows clents prior to XP, DHCP Intercept provides the domain name and subnet mask.	5	Colt Internal Group Policy General General Advanced Colt Turneling E Browser Proxy B-SS, VPN Client G-TEsec Client	hivelicyvpn         Spik tunneling retwork lists distinguish networks that require traffic to go through the tunnel and those that or require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is ACL that consists of list of addresses on the private network.         DNS Names:       Image: Image: Tunnel Network List Delow         Policy:       Image: Tunnel Network List Delow	lo ne s an
Intercept: 🔽 Inherit - C No.		- Clent Access Rule - Clent Freeval - Hardware Clent	Network List:       Splt_Turnel_List       Manage         Intercept OHCP Config Splt_Turnel_List       Intercept OHCP Config Splt_Turnel_List       Manage         DHCP Intercept lets Microsoft XP clients use split turneling with the security appliance. For Windows clients prior to XP, OHCP Intercept provides the domain name and subnet mask.       Intercept:       Intercept:       C //icities       C //icities	*

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

•

General Servers Advanced	Split tunneling network lists distinguish networks that require traffic to go through to require tunneling. The security appliance makes split tunneling decisions on the basi ACL that consists of list of addresses on the private network.	he tunnel and those that do no is of a network list, which is an
	DNS Names: 🔽 Inherit	
Gent     Gent     Gent	Policy: Tunnel Network List Below	*
	NetworkList: Tinhert Solk_Tunnel_List	* Manage
	Intercept DHCP Configuration Message from Micosoft Clients	*
	DHCP Intercept lets Microsoft 3P clients use split tunneling with the security applic prior to 3P, DHCP Intercept provides the domain name and subnet mask.	ance. For Windows dients
	Intercept: 🖓 Inherit - C 🕬 - C 🗤	

Klik op Apply (Toepassen) en vervolgens op Send (Verzenden) (waar vereist) om de opdrachten naar de ASA te sturen.

#### Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored interexternally on a RADIUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.

Name	Type	Tunneling Protocol	
fltGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webypn	N(A
efaultgroup	Internal	Inherited	N/A
valleyvpn	Internal	syc, IPSec	N/A

Apply Reset

De ASA 7.x en hoger via CLI configureren

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



**Opmerking**: de configuratie van de CLI Split-tunneling is hetzelfde voor zowel ASA 7.x als 8.x.

Geef de configuratiemodus op.

<#root>

٠

ciscoasa>

enable

Password: \*\*\*\*\*\*\* ciscoasa#

configure terminal

ciscoasa(config)#

Maak de toegangslijst die het netwerk achter de ASA definieert.

<#root>

•

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

Voer de configuratiemodus voor groepsbeleid in voor het beleid dat u wilt wijzigen.

<#root>

ciscoasa(config)#

group-policy hillvalleyvpn attributes

ciscoasa(config-group-policy)#

Geef het beleid voor split-tunneling op. In dit geval wordt het beleid tunnelgespecificeerd.

<#root>

•

ciscoasa(config-group-policy)#

split-tunnel-policy tunnelspecified

Geef de toegangslijst voor split-tunneling op. In dit geval is de lijst Split\_Tunnel\_List.

<#root>

٠

•

ciscoasa(config-group-policy)#

split-tunnel-network-list value Split\_Tunnel\_List

Voer de volgende opdracht uit:

<#root>

#### ciscoasa(config)#

tunnel-group hillvalleyvpn general-attributes

Koppel het groepsbeleid aan de tunnelgroep

<#root>

•

ciscoasa(config-tunnel-ipsec)#

default-group-policy hillvalleyvpn

Sluit de twee configuratiemodi af.

<#root>

٠

ciscoasa(config-group-policy)#

exit

ciscoasa(config)#

exit

ciscoasa#

•

Sla de configuratie op in niet-vluchtig RAM (NVRAM) en druk op Enter wanneer u wordt gevraagd om de naam van het bronbestand op te geven.

<#root>

ciscoasa#

copy running-config startup-config

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 de CLI

Voer de volgende stappen uit:

٠

Maak de toegangslijst die het netwerk achter de PIX definieert.

<#root>

PIX(config)#access-list Split\_Tunnel\_List standard permit 10.0.1.0 255.255.255.0

• Maak een VPN-groep **vpn3000** en specificeer de gesplitste tunnelACL zoals aangegeven:

<#root>

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 met Microsoft Windows 2000 en</u> 2003 IAS RADIUS-verificatie voor meer informatie over externe VPN-configuratie voor PIX 6.x.

Verifiëren

Volg de stappen in deze secties om de configuratie te verifiëren.

Verbinding maken met de VPN-client

Het VPN-clientlogboek bekijken

•

•

•

Lokale LAN-toegang testen met ping

Verbinding maken met de VPN-client

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

👌 VPN Client - Version 4.0.5 (Rel)		.IO X
Connection Entries Status Certificates Log Opti	ions Help	
Connect New Import Modify	) XA	Cisco Systems
Connection Entries Certificates Log		
Connection Entry	Host	Transport
hilvaleyvpn	172.22 1.160	IPSec/UDP

Kies uw verbindingsitem in de lijst en klik op Verbinden.

Voer uw referenties in.

👌 VPN Client   U	er Authent	ication	for "hillvalle	eyvpn"	X
Cisco Systems thiliti	<u>U</u> sername: <u>P</u> assword:	marty	OK		Cancel

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

•

•

Tunnel Details	Route Details	Frewal	
Address Info	rmation	Connection Information	1
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

Ga naar het tabblad Routedetails om de routes te zien die de VPN-client voor de ASA beveiligt.

In dit voorbeeld, de VPN-client is het beveiligen van toegang tot 10.0.1.0/24 terwijl al het andere verkeer niet is versleuteld en niet over de tunnel is verzonden.

👌 VPN Client   Sta	tistics			X
Tunnel Details Ro	oute Details Frewa			
Local LAN Routes	N.	Secured Routes		
Network	Subnet Mask	Network	Subnet Mask	
		10.0.1.0	255.255.255.0	

Het VPN-clientlogboek bekijken

Wanneer u het VPN-clientlogboek onderzoekt, kunt u bepalen of de parameter die gesplitste tunneling specificeert, is ingesteld. Als u het logbestand wilt weergeven, gaat u naar het tabblad Log in de VPN-client. Klik vervolgens op **Log Settings** om aan te passen wat er is vastgelegd. In dit voorbeeld is IKE ingesteld op **3 - High**, terwijl alle andere log elementen ingesteld zijn op **1 - Low**.

VPN Client - Version 4.0.5 (Rel)	
Connection Entries Status Certificates Log Options Help	
Disable Clear Log Settings Log Window	CISCO STATEMS
Connection Entries Certificates Log	
Cisco Systems VPN Client Version 4.0.5 [Ref/C Copyright (C) 1999-2003 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Windows, WinNT Running on: 5.1.2600 Service Pack 2	
Not connected.	

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/6 IKE/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 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x630000D 26 MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_SAVEPWD: , value = 0x00000000 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x630000D 27 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/0x630000D MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_SPLIT\_INCLUDE (# of split\_nets), value = 0x000000130 14:20:14.238 07/27/06 Sev=Info/5 IKE/0x6300000F SPLIT\_NET #1 subnet = 10.0.1.0mask = 255.255.255.0 protocol = 0src port = 0dest 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 er een tunnel wordt gegraven naar de ASA, is om de **ping-**opdracht op de opdrachtregel van Windows te gebruiken. Het lokale LAN van de VPN-client is 192.168.0.0/24 en er is een andere host aanwezig op het netwerk met een IP-adres van 192.168.0.3.

<#root>

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
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 Split-tunnelACL

Er is een beperking met het aantal ingangen in een ACL die voor gesplitste tunnel wordt gebruikt. Het wordt aanbevolen niet meer dan 50-60 ACE-waarden te gebruiken voor een bevredigende functionaliteit. U wordt geadviseerd om de subnetting eigenschap uit te voeren om een waaier van IP adressen te behandelen.

Gerelateerde informatie

- <u>PIX/ASA 7.x as a Remote VPN Server using ASDM Configuration Example (Configuratievoorbeeld van PIX/ASA 7.x als externe VPN-server via ASDM)</u>
- <u>Adaptieve security applicaties van Cisco ASA 5500 Series</u>
- <u>Cisco Technical Support en downloads</u>

#### Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.