# Split-Tunneling für VPN-Clients auf der ASA konfigurieren

## Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Netzwerkdiagramm
Verwandte Produkte
Konventionen
Hintergrundinformationen
Split-Tunneling auf der ASA konfigurieren
ASA 7.x mit Adaptive Security Device Manager (ASDM) 5.x konfigurieren
Konfigurieren von ASA 8.x mit ASDM6.x
Konfigurieren von ASA 7.x oder höher über CLI
Konfigurieren von PIX 6.x über die CLI
Überprüfung
Mit dem VPN-Client verbinden
VPN-Client-Protokoll anzeigen
Testen des lokalen LAN-Zugriffs mit Ping
Fehlerbehebung
Beschränkung mit der Anzahl der Einträge in einer Split-Tunnel-ACL
Zugehörige Informationen

# Einleitung

In diesem Dokument wird der Prozess beschrieben, mit dem VPN-Clients auf das Internet zugreifen können, während sie sich über eine Cisco Sicherheitslösung der Serie ASA 5500 anmelden.

# Voraussetzungen

## Anforderungen

In diesem Dokument wird davon ausgegangen, dass auf der ASA bereits eine funktionierende VPN-Konfiguration für den Remote-Zugriff vorhanden ist. Weitere Informationen finden Sie unter <u>PIX/ASA 7.x als Remote-VPN-Server mit ASDM-Konfigurationsbeispiel</u>, falls noch kein Server konfiguriert ist.

#### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Security Appliances der Serie ASA 5500, Software-Version 7.x und höher
- Cisco Systems VPN Client Version 4.0.5
- Adaptive Security Device Manager (ASDM)



Hinweis: Dieses Dokument enthält auch die PIX 6.x CLI-Konfiguration, die mit dem Cisco VPN Client 3.x kompatibel ist.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

### Netzwerkdiagramm

Der VPN-Client befindet sich in einem typischen SOHO-Netzwerk und wird über das Internet mit der Hauptniederlassung verbunden.



Netzwerkdiagramm

## Verwandte Produkte

Diese Konfiguration kann auch mit der Software der Cisco Security Appliance der Serie PIX 500, Version 7.x, verwendet werden.

#### Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

## Hintergrundinformationen

Dieses Dokument enthält schrittweise Anleitungen, wie VPN-Clients der Zugriff auf das Internet gewährt wird, während sie über eine Cisco Adaptive Security Appliance (ASA) Security Appliance der Serie 5500 getunnelt werden. Diese Konfiguration ermöglicht VPN-Clients den sicheren Zugriff auf Unternehmensressourcen über IPsec und gewährt gleichzeitig ungesicherten Zugriff auf das Internet.



Hinweis: Vollständiges Tunneling gilt als sicherste Konfiguration, da es nicht den gleichzeitigen Gerätezugriff auf das Internet und das Firmen-LAN ermöglicht. Bei einem Kompromiss zwischen vollständigem Tunneling und Split-Tunneling ist nur der lokale LAN-Zugriff von VPN-Clients zulässig. Weitere Informationen finden Sie unter <u>PIX/ASA</u> 7.x: Allow Local LAN Access for VPN Clients Configuration Example (Konfigurationsbeispiel für lokalen LAN-Zugriff für VPN-Clients zulassen).

In einem grundlegenden Szenario von VPN-Client zu ASA wird der gesamte Datenverkehr vom VPN-Client verschlüsselt und an die ASA gesendet, unabhängig vom Ziel. Je nach Konfiguration und Anzahl der unterstützten Benutzer kann eine solche Einrichtung sehr bandbreitenintensiv sein. Split-Tunneling kann dieses Problem beheben, da Benutzer nur den Datenverkehr über den Tunnel senden können, der für das Unternehmensnetzwerk bestimmt ist. Der restliche Datenverkehr, wie Instant Messaging, E-Mail oder gelegentliches Surfen, wird über das lokale LAN des VPN Clients an das Internet gesendet.

## Split-Tunneling auf der ASA konfigurieren

#### ASA 7.x mit Adaptive Security Device Manager (ASDM) 5.x konfigurieren

Führen Sie diese Schritte aus, um Ihre Tunnelgruppe so zu konfigurieren, dass Split-Tunneling für die Benutzer in der Gruppe zugelassen wird.

 Wählen Sie Configuration > VPN > General > Group Policy aus, und wählen Sie die Gruppenrichtlinie aus, in der Sie den lokalen LAN-Zugriff aktivieren möchten. Klicken Sie dann auf Edit (Bearbeiten).



2. Wechseln Sie zur Registerkarte Client-Konfiguration.

Name: hilvalleyvpn			
General PSec Client Configuration Client Firewall	Hardware Client NAC	WebVPN	
Check an Inherit checkbox to let the corresponding	etting take its value from	the default group policy.	
General Client Parameters Cisco Client Parameters	Microsoft Client Parame	sters	
Banner:	Inherit	Edit Banner	
Default Domain:	🗹 Inherit		
Split Tunnel DNS Names (space delimited):	🔽 Inherit		
Split Tunnel Policy:	🔽 Inherit		¥
Split Tunnel Network List:	🔽 Inherit	▼ Manage.	
Address pools			
🔽 Inherit			
Available Pools	Assi	gned Pools (up to 6 entries)	
	Add≈>		
	< <remove< td=""><td></td><td></td></remove<>		
1			

3. Deaktivieren Sie das Kontrollkästchen Vererben für die Split Tunnel Policy, und wählen Sie Tunnel Network List Below ..

Iame:       Initialleyopn         Ineral       IPSec       Client Contiguration       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       Clicco Client Parameters       Microsoft Client Parameters         Banner:       Inherit       Edit Benner         Default Domain:       Inherit       Edit Benner         Split Tunnel DNS Names (space delimited):       Inherit       Tunnel All Networks         Split Tunnel Policy:       Inherit       Tunnel All Networks         Split Tunnel Network List       Inherit       Tunnel All Network List Below         Address pools       Address pools       Address         Imherit       Address       Address         Address pools       Address       Address			
neral PSec Client Configuration Client Firewall Hardware Client NAC VVebVPN   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: Image: Client Configuration Microsoft Client Parameters   Banner: Image: Client Parameters Microsoft Client Parameters   Banner: Image: Client Parameters Microsoft Client Parameters   Default Domain: Immerit Edit Banner   Spit Tunnel DNS Names (space definited): Immerit Tunnel All Networks   Spit Tunnel Policy: Inherit Tunnel All Networks   Spit Tunnel Network List: Immerit Tunnel All Network List Below   Address pools Address pools Address   Immerit Address Address   Address pools Address	Name: hillvalleyvpn		
Inherit       Edit Banner:         Default Domain:       Inherit         Split Tunnel DNS Names (space definited):       Inherit         Split Tunnel Policy:       Inherit         Split Tunnel Network List:       Inherit         Address pools       Address pools         Address pools       Address	unit Down Client Configuration Client Success	Lundowe cont	
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:       Inherit       Edit Banner         Default Domain:       Inherit       Edit Banner         Split Tunnel DNS Names (space delimited):       Inherit       Tunnel All Networks         Split Tunnel Policy:       Inherit       Tunnel All Networks         Split Tunnel Network List:       Inherit       Exclude Network List Below         Address pools       Address       Assigned Pools (up to 6 entries)         Address       Address       Assigned Pools (up to 6 entries)	eneral   IPSec Client Configuration   Client Firewall	Hardware Client	NAC   WebYPN
General Client Parameters Cisco Client Parameters   Banner: Inherit   Default Domain: Inherit   Split Tunnel DNS Names (space delimited): Inherit   Split Tunnel Policy: Inherit   Split Tunnel Network List: Inherit   Address pools Inherit   Varieble Pools Address   Address pools Inherit	Check an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.
General Client Parameters       Clisco Client Parameters       Microsoft Client Parameters         Banner:       Inherit       Edit Banner         Default Domain:       Inherit       Edit Banner         Split Tunnel DNS Names (space delimited):       Inherit       Inherit         Split Tunnel Policy:       Inherit       Tunnel All Networks         Split Tunnel Network List:       Inherit       Tunnel Network List Below         Address pools       Address pools       Address         Inherit       Avaïebre Pools       Address         Address       Address       Assigned Pools (up to 6 entries)		1	
Banner:       Inherit       Edit Banner         Default Domain:       Inherit       Inherit         Spit Tunnel DNS Names (space delimited):       Inherit       Tunnel All Networks         Spit Tunnel Policy:       Inherit       Tunnel All Networks         Spit Tunnel Network List:       Inherit       Tunnel All Networks         Spit Tunnel Network List:       Inherit       Tunnel Network List Below         Address pools       Address Pools (up to 6 entries)         Address pools       Address       Assigned Pools (up to 6 entries)	General Client Parameters   Cisco Client Parameter:	s   Microsoft Client	Parameters
Banner: Inherit     Default Domain:     Spit Tunnel DNS Names (space delimited):     Inherit     Spit Tunnel Policy:     Inherit     Tunnel All Networks     Spit Tunnel Network List:     Address pools		-	
Default Domain: Inherit   Spit Tunnel DNS Names (space definited): Inherit   Spit Tunnel Policy: Inherit   Tunnel All Networks Tunnel All Networks   Spit Tunnel Network List: Inherit   Address pools Exclude Network List Below   Address pools Address pools	Banner:	I≁ Inherit	Edit Banner
Spit Tunnel DNS Names (space delimited):   Spit Tunnel Policy:   Inherit   Tunnel All Networks   Tunnel Network List:   Inherit   Address pools    Adds>  Adds  Adds Adds Adds  Adds Adds Adds  Adds Adds Adds Adds Adds Ad	Defer it Domaio	Juberit	
Spit Tunnel DNS Names (space delimited):   Spit Tunnel Policy:   Inherit   Tunnel All Networks   Tunnel All Network List:   Inherit   Address pools   Inherit   Address pools   Address pools   Address pools   Address pools (see a construction of the second of	Dorous Dorrow.	It in the fit	1
Split Tunnel Policy: Inherit   Tunnel All Networks   Split Tunnel Network List:     Inherit     Address pools     Address	Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Spit Tunnel Policy: Inherit     Tunnel All Networks     Tunnel Network List Below     Address     Address     Address     Address     Address     Address     Tunnel All Networks     Address     Address     Address     Address   <			
Split Tunnel Network List:       Image: Image	Split Tunnel Policy:	🗌 Inherit	Tunnel All Networks
Split Tunnel Network List:     Address pools     Address pools     Address pools     Available Pools     Addi>>			Tunnel All Networks
Address pools           Address pools           Inherit           Avaïable Pools           Add>>           Add>>           KRemove	Split Tunnel Network List:	🔽 Inherit	Tunnel Network List Below
Address pools          Inherit       Avaïable Pools       Assigned Pools (up to 6 entries)         Add>>			
Available Pools     Assigned Pools (up to 6 entries)       Add>>	Address pools		
Avarable Pools Addex Assigned Pools (up to 6 entries)	Inherit		
Add>> < <remove< td=""><td>Avarable Pools</td><td></td><td>Assigned Pools (up to 6 entries)</td></remove<>	Avarable Pools		Assigned Pools (up to 6 entries)
<=Remove		Add>>	1
			1
		**nemove	1
	1		,

Deaktivieren Sie für Split Tunnel Network List das Kontrollkästchen **Inherit (Vererben**), und klicken Sie dann auf **Manage** (**Verwalten**), um den ACL Manager zu starten.

Name: hillvalleyvpn	
sparal IPSac Client Configuration Client Firewall Hardware Client N&C Web//PN	1
	1
Check an Inherit checkbox to let the corresponding setting take its value from the default	t group policy.
General Client Parameters Cisco Client Parameters Microsoft Client Parameters	
Banner: 🔽 Inherit Ed	it Banner
Default Domain: I Inherit	
Split Tunnel DNS Names (space delimited):	
Split Tunnel Policy:	List Below 🔻
Split Tunnel Network List:  None	Manage
Address pools	
🔽 Inherit	
Available Pools Assigned Pools	: (up to 6 entries)
Add>>	
< <remove< td=""><td></td></remove<>	

Wählen Sie in ACL Manager Add (Hinzufügen) > Add ACL ... (ACL hinzufügen ...) aus, um eine neue Zugriffsliste zu erstellen.

	ACL Manager					( ) I	L I		X
l (	Standard AGL Edender	I AGL							
	◆ Add → 🗐 5dt 🎁	D-Mrr -	F 4   X 4	h 18					
	Add AGL	dress	.A_6	05	Description				
	<ul> <li>Astron. **</li> <li>Astront</li> </ul>								
	Topert Atter.								
		-							

Geben Sie einen Namen für die ACL ein, und klicken Sie auf OK.

ACL Manager			<u>×</u>
Stendard ACL Extended ACL			
♣ Add → 필요한 홈 RODA 분 →	X % 8 -		
No Address	Adon Description		
	🖆 Add ACL	×	
	AG, Nenet: Splt_Turnel_List		
	OK N Cancal	Help	
Pula Pow Disgram			×
	s inside a cutatife		
	dorw		
	OK Cancel	14p	

Nachdem die ACL erstellt wurde, wählen Sie **Hinzufügen > ACE hinzufügen.** .um einen Access Control Entry (ACE) hinzuzufügen.



Definieren Sie den ACE, der dem LAN hinter der ASA entspricht. In diesem Fall ist das Netzwerk 10.0.1.0/24.

a.

Wählen Sie Permit (Zulassen) aus.

b.

Wählen Sie als IP-Adresse 10.0.1.0 aus.

c.

Wählen Sie die Netzmaske 255.255.255.0 aus.

#### d.

(Optional)Geben Sie eine Beschreibung an.

Klicken Sie auf > **OK**.

No	Address	Action	Description			
Spit_Turnet_Li	et					
	di Add AD				X	
	- Action -					
	Actor	Poret 💌				
	Horihie	twork				
	IP Add	HEAR 10.0.1.0			¥	
	Netwo	sk: 255 255 255 0			*	
	Descriptio	n.				
	The corp.	rate network behind the	ASA.			
		OK .	Cancel	Holp	1	
		Q			1	
in Flow Discover						
an ser sagar	-	a	neide al Contration	sido jug		
					-	

Klicken Sie auf OK, um ACL Manager zu beenden.

•

e.



Vergewissern Sie sich, dass die soeben erstellte ACL für "Split Tunnel Network List" ausgewählt ist.

ame: hilvalleyvpn		
and Draw Clart Configuration Class Descent	Libertuara Clarit	Luc Junior
eral PSec Control of Cart Preva	IT Hardware Clerk	I NOL I NED YAN I
heck an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.
Seneral Client Parameters Cisco Client Parameter	s Microsoft Client	Parametera
Barner.	🔽 Inherit	Edit Barrier
Default Domain:	₽ intert	
Split Tunnel DNS Names (space delimited):	I inherit	1
Split Tunnel Policy:	Inherit	Tunnel Network List Below
Split Tunnel Network List:	Inhert	Spit_Turnel_L Manage
- Address pade		None Solt Turnel List
inbert		cutside_cryptome5 <sup>4</sup>
Avaiblie Poolo		Assigned Pools (up to 6 entries)
	Addres	
	- Commun	
	STATES INTO	

Klicken Sie auf **OK**, um zur Konfiguration der Gruppenrichtlinie zurückzukehren.

🔂 Edit	t Internal C	Group Policy: hillvalleyvpn			X
	Nome:	hilvsleyvpn			
þ	General   IPS	Sec Client Configuration Client Firev	vail   Hardware Client	NAC WebVPN	_
	Check an	Inherit checkbox to let the correspond	ing setting take its valu	e from the default group policy.	
	General C	lient Parameters Cisco Client Parame	ters Microsoft Client	Parameters	
	Banne	n	🖓 inhert	Edit Earster	
	Defaul	t Donvein:	P interit		
	Split Tu	nnei DNS Names (space delmited):	17 Inhert		
	Split To	unnel Policy:	□ inherit	Tunnel Network List Below	
	Split Tu	nnel Network List:	[ Inhert	Spit_Tunnel_L * Menage	
	Addre	ss pools			

Klicken Sie auf Apply (Übernehmen) und dann ggf. auf Send (Senden), um die Befehle an die ASA zu senden.

٠



Konfigurieren von ASA 8.x mit ASDM 6.x

•

Führen Sie diese Schritte aus, um Ihre Tunnelgruppe so zu konfigurieren, dass Split-Tunneling für die Benutzer in der Gruppe zugelassen wird.

Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > Group Policies (Konfiguration > Remotezugriff-VPN > Netzwerkzugriff (Client) > Group Policies (Gruppenrichtlinien) und dann die Gruppenrichtlinie aus, in der Sie den lokalen LAN-Zugriff aktivieren möchten. Klicken Sie dann auf Edit (Bearbeiten).** 

Configuration > Remote Access VPN > Net	twork (Client) Acce	ss > Group Policies					
Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored inter externally on a RADBUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.							
🗣 Add 🔹 📝 Edit 👔 Delete	🗣 Add 🔹 📝 Edit 👔 Delete						
Name	Туре	Tunneling Protocol	4				
DfltGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webvpn	N/A				
Defaultgroup	Interna	Inherited	N/A				
hivaleyvpn	Internal	svc,IPSec	N/A				
and the second se	*						

1	Edit Internal Group Policy:	y: hivalleyvpn	
	General Servers B-Advanced	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and thos require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, ACL that consists of list of addresses on the private network.	n that do no which is an
	-IE Browser Procy	DNS Names: 🖾 Inherit	
	E-SSL VPN Client     Psec Client	Policy: 🖓 Inherit	
	- Clent Access Rule Clent Firewal	Network List: 🖂 Scherit	Martage
	-Hardware Clent	Intercept DHCP Configuration Message from Micosoft Clients	·
		DHCP Intercept lets Microsoft XP clerits use split tunneling with the security appliance. For Windows prior to XP, DHCP Intercept provides the domain name and subnet mask.	clients
		Intercept: 🔽 Inhert C 🕬 C 🕬	
		Subnet Mesk (Optione): 0.0.0.0	7
	1 2		
-			

Deaktivieren Sie das Kontrollkästchen Vererben für Split Tunnel Policy, und wählen Sie Tunnel Network List (Tunnelnetzliste unten) aus.

ſ	Edit Internal Group Policy:	: hivalleyvpn	
	General Servers Advanced Soit Tunneling I.I.B. Bröwser Proxy (E.S2, VPN Client Client Access Rule	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and the require tunneling. The security appliance makes split tunneling decisions on the basis of a network in AQL that consists of list of addresses on the private network.         DNS Names:       Image: Inherit         Folicy:       Inherit         Tunnel Network List Below       Image: Ima	see thet do no 4, which is an Mensor
	Clerk Firewal	Tunnel Network List Below	
	- Hardware Client	Internet DUCE Configuration Manager From Microsoft Clarate	
		DHCP Intercept lets Microsoft XP clients use split tunneling with the security appliance. For Window prior to XP, DHCP Intercept provides the domain name and subnet mask.	as clients
		Intercept: 🖓 Inherit C Yos C No	

Deaktivieren Sie das Kontrollkästchen Inherit für Split Tunnel Network List, und klicken Sie dann auf Manage (Verwalten), um den ACL Manager zu starten.

<b>f</b>	Edit Internal Group Policy:	i hiralleyvpn
	General Servers Ə. 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.
	- 22 Browser Prozy - 35, VPN Client	DNS Names: 🖓 Inherit
		Pokcy:         Inherit         Turnel Network List Berow         *           Network List:         Enherit         None         *         Manage)
	Hardware Clenk	Intercept DHCP Configuration Message from Micosoft Clients
		DHCP Intercept lets Microsoft XP clents use split tunneling with the security appliance. For Windows clents prior to XP, DHCP Intercept provides the domain name and subnet mask.
		Intercept: 🔽 Inherit - C No - C No
		Subret Mask (Optiona): 0.0.0.0

Wählen Sie in ACL Manager Add (Hinzufügen) > Add ACL ... (ACL hinzufügen ...) aus, um eine neue Zugriffsliste zu erstellen.



Geben Sie einen Namen für die ACL an, und klicken Sie auf OK.

•

No Address Action Description	Randard ACL   Exte	nded ACL   t 🏦 Delete   🛧	4 [ X Pa 10	. +	
No Address Action Description	🗣 Add 🔹 🧾 Edi	t 🔟 Delete   🕈	+ 5 10 10	7	
ACL Name: Split_Turnel_List OK Cancel Help	No	Address	Action	Description	
		Add A	ACL ne: Split_Tunnel_List OK Cancel	Help	

Wählen Sie nach Erstellung der ACL Add (Hinzufügen) > Add ACE ... (ACE hinzufügen ...) aus, um einen Zugriffskontrolleintrag (Access Control Entry, ACE) hinzuzufügen.

CL Manager	HACI I		
Add - 🔤 Edit	👔 Delete 👌	4 % Ba	18. ·
+ Add ACL	55	Action	Description
Add ACE			
Insert			

Definieren Sie den ACE, der dem LAN hinter der ASA entspricht. In diesem Fall ist das Netzwerk 10.0.1.0/24.

a.

•

Klicken Sie auf das Optionsfeld Zulassen.

b.

Wählen Sie die Netzwerkadresse mit der Maske 10.0.1.0/24 aus.

c.

(Optional) Geben Sie eine Beschreibung ein.

d.

Klicken Sie auf OK.

📫 AEL Manager					
Standard ACL Extended Ad	1				
🗣 Add 🔹 🔡 Edt 📋	Deloto 🛧 🗲 👗	Ra III			
No Addr	ess Action		Description		
Split_Tunnel_List					
	Add ACE				×
	Action: (+ Permit (	" Deny			
	Address: 10.0.1.0/24				
	Parminting				
	The Corporate network b	whind the ASA			
					-1
		OK.	Cancel	Help	
			en l	II-la I	

Klicken Sie auf OK, um ACL Manager zu beenden.

ACL Manager		<u></u>			
Observational ACL Devices	a a weed in				
Scandard Act   Exteni	DEO ACL				
🍄 Add 🔹 💽 Edit	🚺 Delete 🧳 🕈	÷ %			
No	Address	Action		Description	
Split_Tunnel_List					
1 10.0.	1.0/24	🥜 Permit	The Corporate	e network behind the At	5A
			41		
			C OF 1	Canad 3	tala.

Vergewissern Sie sich, dass die soeben erstellte ACL für "Split Tunnel Network List" ausgewählt ist.

٠

5	Edit Internal Group Policy: General Servers Advanced - Selt Turneing - E Growser Prozy (i) - SS, VPN Clent	Initiality upon         Split tunneling retwork lists distinguish networks that require traffic to go through the tunnel and those that do nor 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:       Image: Im
	⊡Psec Client. —Client Access Rule —Client Floewall —Hardware Client.	Network List:       Intercept DHCP Config         Intercept Ides Microsoft XP clients use split turneling with the security appliance. For Windows clients prior to XP, DHCP Intercept provides the domain name and subnet mask.
		Intercept: 🖓 Inherit (C. Yos) (C. No

Klicken Sie auf OK, um zur Konfiguration der Gruppenrichtlinie zurückzukehren.

•

General Servers Advanced	Split tunneling network lists distinguish networks that require traffic to go through require tunneling. The security appliance makes split tunneling decisions on the be ACL that consists of list of addresses on the private network.	the tunnel and those that do not asis of a network list, which is an
IE Browser Praxy	DNS Names: 🔽 Inherit	
G-SSL VPN Clent G-IPsec Clent	Policy: Tunnel Network List Below	*
	Network List: Tinhert Solk_Tunnel_List	* Manage
	Intercept DHCP Configuration Message from Micosoft Clients	8
	DHCP Intercept lets Microsoft XP clients use split tunneling with the security app prior to XP, DHCP Intercept provides the domain name and subnet mask.	oliance. For Windows clients
	Internet Extends Chief Chief	
	Turescebc: M. Tuuleur, K. 1993, K. 193	

Klicken Sie auf Apply (Übernehmen) und dann ggf. auf Send (Senden), um die Befehle an die ASA zu senden.

#### 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 intermexternally on a RADIUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.

fibGipPolicy (System Default) Internal L2TP-IPSec, IPSec, webvpn N Iefaultgroup Internal Inherited N Ivalityvpn Internal svc, IPSec N	Name	Туре	Tunneling Protocol	
efaultgroup Internal Inherited N ivalley.vpn Internal svc, IPSec N	tGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webvpn	N(A
ivalleyvpn Internal svc, IPSec N	sfaultgroup	Internal	Inherited	N/A
	valleyvpn	Internal	syc, IPSec	N/A

Apply Reset

Konfigurieren von ASA 7.x oder höher über CLI

Anstatt den ASDM zu verwenden, können Sie die folgenden Schritte in der ASA-CLI ausführen, um Split-Tunneling auf der ASA zu ermöglichen:



Hinweis: Die CLI Split Tunneling-Konfiguration ist für ASA 7.x und 8.x identisch.

Wechseln Sie in den Konfigurationsmodus.

<#root>

٠

ciscoasa>

enable

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

configure terminal

ciscoasa(config)#

Erstellen Sie die Zugriffsliste, die das Netzwerk hinter der ASA definiert.

<#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

Wechseln Sie in den Gruppenrichtlinienkonfigurationsmodus für die Richtlinie, die Sie ändern möchten.

<#root>

ciscoasa(config)#

group-policy hillvalleyvpn attributes

ciscoasa(config-group-policy)#

Geben Sie die Split-Tunnel-Richtlinie an. In diesem Fall ist die Richtlinie tunnelspecified.

<#root>

•

ciscoasa(config-group-policy)#

split-tunnel-policy tunnelspecified

Geben Sie die Split-Tunnel-Zugriffsliste an. In diesem Fall lautet die Liste Split\_Tunnel\_List.

<#root>

٠

٠

ciscoasa(config-group-policy)#

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

Führen Sie folgenden Befehl aus,

<#root>

#### ciscoasa(config)#

tunnel-group hillvalleyvpn general-attributes

Ordnen Sie die Gruppenrichtlinie der Tunnelgruppe zu

<#root>

•

ciscoasa(config-tunnel-ipsec)#

default-group-policy hillvalleyvpn

Beenden Sie die beiden Konfigurationsmodi.

<#root>

٠

ciscoasa(config-group-policy)#

exit

ciscoasa(config)#

exit

ciscoasa#

٠

Speichern Sie die Konfiguration im nichtflüchtigen RAM (NVRAM), und drücken Sie die Eingabetaste, wenn Sie aufgefordert werden, den Quelldateinamen anzugeben.

<#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#

Konfigurieren von PIX 6.x über die CLI

Führen Sie diese Schritte aus:

٠

Erstellen Sie die Zugriffsliste, die das Netzwerk hinter dem PIX definiert.

<#root>

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

• Erstellen Sie eine VPN-Gruppe "vpn3000", und geben Sie die ACL des Split-Tunnels wie folgt an:

<#root>

PIX(config)#

vpngroup vpn3000 split-tunnel Split\_Tunnel\_List



**Hinweis:** Weitere Informationen zur Remotezugriff-VPN-Konfiguration für PIX 6.x finden Sie unter <u>Cisco Secure PIX Firewall 6.x</u> und Cisco VPN Client 3.5 für Windows mit Microsoft Windows 2000 und 2003 IAS RADIUS Authentication.

Überprüfung

Gehen Sie wie in diesem Abschnitt beschrieben vor, um Ihre Konfiguration zu überprüfen.

Mit dem VPN-Client verbinden

VPN-Client-Protokoll anzeigen

Testen des lokalen LAN-Zugriffs mit Ping

Mit dem VPN-Client verbinden

•

•

•

•

Verbinden Sie den VPN-Client mit dem VPN Concentrator, um die Konfiguration zu überprüfen.

🍐 VPN Client - Version 4.0.5 (Rel)		
Connection Entries Status Certificates Log	Options Help	
Connect New Import M	odily Delete	Cisco Systems
Connection Entries Certificates Log		
Connection Entry	Host	Transport
hilvaleyvpn	172.22.1.160	IPSec/UDP

Wählen Sie Ihren Verbindungseintrag aus der Liste aus, und klicken Sie auf Verbinden.

Geben Sie Ihre Anmeldeinformationen ein.

👌 VPN Client   Use	r Authentica	tion for "hil	valleyvpn"	×
CISCO SYSTEMS	Jsername: ma Password: 🔤	rty ××××	OK	Cancel

Wählen Sie **Status > Statistics...** (**Status > Statistik**), um das Fenster "Tunnel Details" anzuzeigen, in dem Sie die Details des Tunnels überprüfen und den Verkehrsfluss sehen können.

Tunnel Details	Route Details	Firewal	
Address Info Client: Server	mation 10.0.1.50 172.22.1.160	Connection Information Entry: Time:	hilvalley2 9. dau(s): 00:00:25
Bytes Received Sent	0 1494	Crypto Encryption: Authentication:	168-bit 3-DES HMAC-SHA1
Packets Encrypted Decrypted Discarded Bypassed	9 0 0 159	Transport Transparent Tunneling Local LAN: Compression:	Inactive Disabled None
			Reset

•

•

Rufen Sie die Registerkarte Route Details (Routendetails) auf, um die Routen anzuzeigen, die der VPN-Client mit der ASA sichert.

In diesem Beispiel sichert der VPN-Client den Zugriff auf 10.0.1.0/24, während der gesamte andere Datenverkehr nicht verschlüsselt wird und nicht über den Tunnel gesendet wird.

👌 VPN Client   Sta	tistics			×
Tunnel Details	oute Details Frewa			
Local LAN Routes	, k	Secured Routes		
Network	Subnet Mask	Network	Subnet Mask	
		10.0.1.0	255.255.255.0	

VPN-Client-Protokoll anzeigen

Wenn Sie das Protokoll des VPN-Clients überprüfen, können Sie bestimmen, ob der Parameter, der Split-Tunneling angibt, festgelegt ist. Um das Protokoll anzuzeigen, gehen Sie zur Registerkarte Log (Protokoll) im VPN Client. Klicken Sie dann auf **Log Settings**, um anzupassen, was protokolliert wird. In diesem Beispiel ist IKE auf **3 - Hoch** festgelegt, während alle anderen Protokollelemente auf **1 - Niedrig** festgelegt sind.

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 = 255.255.255.0protocol = 0src port = 0dest port=0 !--- Output is supressed.

Testen des lokalen LAN-Zugriffs mit Ping

Eine weitere Möglichkeit, zu testen, ob der VPN-Client für Split-Tunneling konfiguriert ist, während er an die ASA getunnelt wird, besteht darin, den Befehl **ping** in der Windows-Befehlszeile zu verwenden. Das lokale LAN des VPN-Clients ist 192.168.0.0/24, und ein anderer Host ist im Netzwerk mit der IP-Adresse 192.168.0.3 vorhanden.

<#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>
```

Fehlerbehebung

Beschränkung mit der Anzahl der Einträge in einer Split-Tunnel-ACL

Die Anzahl der Einträge in einer ACL für Split-Tunnel ist begrenzt. Es wird empfohlen, nicht mehr als 50-60 ACE-Einträge zu verwenden, um eine zufriedenstellende Funktionalität sicherzustellen. Es wird empfohlen, die Subnetzfunktion zu implementieren, um einen Bereich von IP-Adressen abzudecken.

Zugehörige Informationen

- <u>PIX/ASA 7.x als Remote-VPN-Server mit ASDM-Konfigurationsbeispiel</u>
- <u>Cisco Adaptive Security Appliances der Serie ASA 5500</u>
- <u>Technischer Support und Downloads von Cisco</u>

#### Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.