# ASA/PIX: Split Tunneling für VPN-Clients im ASA-Konfigurationsbeispiel zulassen

## Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Netzwerkdiagramm Zugehörige Produkte Konventionen Hintergrundinformationen Konfigurieren von Split Tunneling auf der ASA Konfigurieren Sie die ASA 7.x mit dem Adaptive Security Device Manager (ASDM) 5.x Konfigurieren der ASA 8.x mit dem Adaptive Security Device Manager (ASDM) 6.x Konfigurieren der ASA 7.x und höher über die CLI Konfigurieren von PIX 6.x über die CLI Überprüfen Herstellen einer Verbindung mit dem VPN-Client VPN-Clientprotokoll anzeigen Testen des lokalen LAN-Zugriffs mit Ping Fehlerbehebung Beschränkung durch die Anzahl der Einträge in einer Split-Tunnel-ACL Zugehörige Informationen

# **Einführung**

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

**Hinweis:** Vollständiges Tunneling gilt als die sicherste Konfiguration, da es nicht den gleichzeitigen Gerätezugriff auf das Internet und das Firmen-LAN ermöglicht. Ein Kompromiss zwischen Voll-Tunneling und Split-Tunneling ermöglicht nur den lokalen LAN-Zugriff von VPN-Clients. Siehe <u>PIX/ASA 7.x: Konfigurationsbeispiel für VPN-Clients den lokalen LAN-Zugriff</u> für weitere Informationen <u>zulassen</u>.

## 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 unter Verwendung des ASDM-Konfigurationsbeispiels</u>, falls dieser noch nicht konfiguriert ist.

#### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Security Appliance der Serie ASA 5500 Softwareversion 7.x und höher
- Cisco Systems VPN Client Version 4.0.5

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

#### **Netzwerkdiagramm**

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



### Zugehörige Produkte

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

#### **Konventionen**

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips

## Hintergrundinformationen

In einem grundlegenden VPN Client-zu-ASA-Szenario wird der gesamte Datenverkehr vom VPN-Client verschlüsselt und an die ASA gesendet, unabhängig von dessen Ziel. Basierend auf Ihrer Konfiguration und der Anzahl der unterstützten Benutzer kann eine solche Einrichtung bandbreitenintensiv sein. Durch Split-Tunneling kann dieses Problem behoben werden, da die Benutzer nur den Datenverkehr senden können, der für das Unternehmensnetzwerk bestimmt ist. Sämtlicher anderer Datenverkehr wie Instant Messaging, E-Mail oder gelegentliches Surfen wird über das lokale LAN des VPN-Clients ins Internet gesendet.

# Konfigurieren von Split Tunneling auf der ASA

#### Konfigurieren Sie die ASA 7.x mit dem Adaptive Security Device Manager (ASDM) 5.x

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

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

Dearbolt	/11.						
File Options 1	iools VVizards	Help				Search:	Find 👻
Itome	ି Configuration	Manikaring	Back Forward	Packet Tracer   Re	💽 🛄 fresh Save	? Heto	Cisco Systems
Home	Configuration	Monitoring Network Monitoring Wizard and Wizard UPN System Option Client Update Furmel Group Stores Default Tunnel Geter Zone Labs Integrity c ktrease Management VPN il Proxy	Back Forward  > Group Policy  Group Policy  Manage VFN g may be stored referenced by  Name Nitveleyopn DthGrpPolicy (Sys	Packet Tracer Re roup policies. A VPN g internally on the devic VPN tunnel groups an Type tem Defa Internal	roup policy is a colle or externally on a R Juser accounts.	Help trion of user-oriented attribute. RADIUS server. The group polic Protocol AAA Server G N/A N/A	Add Coup Add Eol Delete
			1		Apply	Reset	
Configuration cha	nges saved suct	cesstully.		ciso	0 2		BM.06 7:28:38 PM UTC

2. Öffnen Sie die Registerkarte Client Configuration.

General Client Parameters Cisco Client Parameters	setting take its value from the default group policy. s   Microsoft Client Parameters
Banner:	Edit Banner
Default Domain:	I inherit
Split Tunnel DNS Names (space delimited):	l✓ Inherit
Split Tunnel Policy:	V Inherit
Split Tunnel Network List:	Manage
Address pools	
Available Pools	Assigned Pools (up to 6 entries) Add>> <

3. Deaktivieren Sie das Kontrollkästchen Inherit (Erben) für Split Tunnel Policy (Tunnelrichtlinie aufteilen), und wählen Sie unten Tunnel Network List (Tunnelnetzwerkliste).

Name:  hillvalleyvpn		
eneral PSec Client Configuration Client Firewall	Hardware Client	NAC WebVPN
Check an Inherit checkbox to let the corresponding	setting take its valu	ue from the default group policy.
General Client Parameters Cisco Client Parameters	s Microsoft Client	Parameters
Banner:	🔽 inherit	Edit Banner
Default Domain:	🔽 Inherit	
	_	
Split Tunnel DNS Names (space delimited):	I⊻ Inherit	
Split Tunnel Policy:	🗌 Inherit	Tunnel All Networks
	_	Tunnel All Networks Tunnel Network List Below
Split Tunnel Network List:	🗹 Inherit	Exclude Network List Below
Address pools		
I Inherit		
Avarabre Poors		Assigned Pools (up to 6 entries)
	Add>>	
	< <remove< td=""><td></td></remove<>	

4. Deaktivieren Sie das Feld **Erben** für "Tunnel-Netzwerkliste teilen", und klicken Sie dann auf **Verwalten**, um den ACL Manager zu starten.

Canaval Client Devenuetors	Inc. con a	
General Client Parameters   Cisco Client Parameter	s   Microsoft Client	Parameters
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	None Manage
Address pools		
Available Pools		Assigned Pools (up to 6 entries)
	a data a	1
-	Remove	1
	~~17510346	

5. Wählen Sie im ACL Manager Hinzufügen > ACL hinzufügen aus.. um eine neue Zugriffsliste zu

erstellen.

andard ACL Extende	d ACL				
Add - Edt 1	Delete 🛧	+ % m m	*		 
Add ACL	dress	Action	Description	[	 
🔹 🖶 Add ACE	5			_	
🚖 inseri					
🖶 Insert Atter					
	_				
Rule Flow Diagram					
		3-	inside outside		
		1		I.	
			🔶 🔥 geny		

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

VCL Manager					
tandard ACL	Extended ACL				
🕈 Add 👻 📝	Edt 💼 Delete 🕈 🖌	3 1 1 1			
No	Address	Action	Description		
		💰 Add ACL		×	
		ACL Name: Solt	Tunnel List		
				1	
		(	Cancel	Help	
			·		
Rule Flow Diag	ram				_
-		3- ins	side outside		
			2 denv		
			• worry		
		OK	Cancel	Heip	

7. Wenn die ACL erstellt wurde, wählen Sie Add > Add ACE.. (Hinzufügen > ACE hinzufügen)

**aus.** um einen Zugriffssteuerungseintrag (ACE) hinzuzufügen.

ACL Manager					i. († 1
Standard ACL Extended	ACL				
🗣 Add 🕞 📝 Edi: 🧻	Delete 🛧 🧃	- X == ==	*		
Add ACL	dress	Action	Description		
Add ACE					
The state of the second	1				
-Rule Flow Diagram		3-	inside v deny		×
		OH	Cancel	Help	 

 Definieren Sie den ACE, der dem LAN hinter der ASA entspricht. In diesem Fall ist das Netzwerk 10.0.1.0/24.Wählen Sie Zulassen aus.Wählen Sie eine IP-Adresse von 10.0.1.0 aus.Wählen Sie die Netzmaske 255.255.255.0 aus.(Optional) Geben Sie eine Beschreibung an.Klicken Sie auf OK.

🕵 ACL Manager						×
Standard ACL	Extended ACL					
🗣 Add 👻 📧	f Edit 📋 Delete 🛧 🕔	6 X B B -				
No	Address	Action	Description			
Splt_Tunne	l_List					
	📬 Add ACE				×	
	Action					
	Action	🖌 Permit 💌				
	HostNet	work				
	IP Add	ress: 10.0.1.0			×	
	Netma	sk: 255.255.255.0			*	
	Description	n				
	The corpo	rate network behind the	ASA.			
	1					
		ок	Cancel	Help		
			<u>}                                    </u>			
Rule Flow Diag	gram					×
		B	inside outside			
		· · · · · · · · · · · · · · · · · · ·	2 deny			
		ок	Cancel	Help		

9. Klicken Sie auf OK, um den ACL Manager zu



10. Stellen Sie sicher, dass die gerade erstellte ACL für die Split Tunnel Network List

(Netzwerkliste des Split-Tunnels) ausgewählt ist.

General Clenit Parameters   Cisco Client Parameters   Microso	oft Client Parameters
Banner: IV I	Inherit Edit Banner
Default Domain:	Inherit
Split Tunnel DNS Names (space delimited):	Inherit
Soit Tuppel Policy	kherit Tunnel Network List Below
oper termorroncy.	
Split Tunnel Network List:	Inherit Splt_Tunnel_L Manage
Address pools	None Splt_Tunnel_List
🔽 Inherit	outside_cryptomap <sup>%</sup>
Available Pools	Assigned Pools (up to 6 entries)
Adds	44
<-Rem	10VE

11. Klicken Sie auf **OK**, um zur Gruppenrichtlinienkonfiguration zurückzukehren.

Name: Ihillvalleyvpn		
eneral IPSec Client Configuration Client Firewall	Hardware Client	NAC WebVPN
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
Banner:	🗹 Inherit	Edit Banner
Default Domain:	🔽 inherit	
Split Tunnel DNS Names (space delimited);	I Inherit	
Split Tunnel Policy:	🖵 Inherit	Tunnel Network List Below
Split Tunnel Network List:	🗖 Inherit	Splt_Tunnel_L Manage
- Advess node		
Inherit		
Available Pools		Assigned Pools (up to 6 entries)
	Add≽≽	1
	< <remove< td=""><td></td></remove<>	

12. Klicken Sie auf **Apply** und dann **Send** (falls erforderlich), um die Befehle an die ASA zu senden.

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

#### Konfigurieren der ASA 8.x mit dem Adaptive Security Device Manager (ASDM) 6.x

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

 Wählen Sie Configuration > Remote Access VPN > Network (Client) Access > Group Policies (Konfiguration > Remote Access VPN > Netzwerk (Client) Access > Group Policies (Gruppenrichtlinien) aus, und wählen Sie die Gruppenrichtlinie aus, in der Sie den lokalen LAN-Zugriff aktivieren möchten. Klicken Sie anschließend auf

eardeneri.			
nfiguration > 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 - C Edit Delete	policy is a collection of us group policy information	er-oriented attribute/value pairs that may l is referenced by VPN tunnel groups and us	be stored interna ser accounts.
Name	Туре	Tunneling Protocol	A
Name DfltGrpPolicy (System Default)	Type	Tunneling Protocol L2TP-IPSec, IPSec, webvpn	N/A
Name DfltGrpPolicy (System Default) Defaultgroup	Type Internal Internal	Tunneling Protocol L2TP-IPSec, IPSec, webvpn Inherited	N/A N/A

2. Klicken Sie auf Getrenntes Tunneling aufteilen.

🥵 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 no 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.
IE Browser Proxy	DNS Names: 🔽 Inherit
SSL VPN Client     ⊡ IPsec Client	Policy: 🔽 Inherit
Clent Access Rule Clent Firewall	Network List: 🔽 Inherit Manage
- Hardhard Clork	Intercept DHCP Configuration Message from Micosoft Clients
	Intercept: Ves C No
	Subnet Mask (Optional): 0.0.0.0
<b>I</b>	
	OK Cancel Help

3. Deaktivieren Sie das Kontrollkästchen Inherit (Erben) für Split Tunnel Policy (Tunnelrichtlinie aufteilen), und wählen Sie unten Tunnel Network List (Tunnelnetzwerkliste).

💼 Edit Internal Group Policy:	hivalleyvpn			
General Servers Advanced	Split tunneling network lists distir require tunneling. The security a ACL that consists of list of addre	iquish networks that require trafi ppliance makes split tunneling de sses on the private network.	ic to go through the tunnel and cisions on the basis of a netwo	d those that do no rk list, which is an
IE Browser Proxy IE Browser Proxy SSL VPN Client IPsec Client Client Access Rule Client Firewall Hardware Client	DNS Names:  ☐ Inherit Policy: ☐ Inherit Tur Network List: ☐ Inherit ☐ Intercept DHCP Configurat DHCP Intercept lets Microsoft prior to XP, DHCP Intercept pr	nel Network List Below nel All Networks nel Network List Below ude Network List Below ion Message from Micosoft ( KP clients use split tunneling with ovides the domain name and subr	<b>Clients</b> the security appliance. For Wir net mask.	Manage Manage Adows clients
	Intercept: 🔽 Inherit 🔿 Ye	s C No		
	Subne	: Mask (Optional): 0.0.0.0		<b>Y</b>
x >				
	ок	Cancel Help	]	

4. Deaktivieren Sie das Feld **Erben** für "Tunnel-Netzwerkliste teilen", und klicken Sie dann auf **Verwalten**, um den ACL Manager zu starten.

💼 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 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
SSL VPN Client     ⊡-IPsec Client	Policy: Inherit Tunnel Network List Below
	Network List: None
Hardware Clienc	Intercept DHCP Configuration Message from Micosoft Clients
	prior to XP, DHCP Intercept provides the domain name and subnet mask. Intercept: I Inherit C Yes C No
	Subnet Mask (Optional): 0.0.0.0
×>	
	OK Cancel Help

5. Wählen Sie im ACL Manager **Hinzufügen > ACL hinzufügen aus..** um eine neue Zugriffsliste zu



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

		ana pari	00	- Ward	Description		2-
No	Addre	ISS	Action	<u>,                                     </u>	Description		8
		🙀 Add A	CL		×		
		ACL Nam	e: Split_Tunnel	_List			
				ancel	Help 1		
							_
			Г	~ 1		11-1-	
enn die AC	L erstellt wurd	e, wählen S	ie Add > Add	ACE (Hinzu	rfügen > ACE ł	ninzufüç	je
enn die AC I <b>s</b> . um eine nzuzufüger	:L erstellt wurd n Zugriffssteue ւ	e, wählen S erungseintra	ie <b>Add &gt; Add</b> g (ACE)	ACE (Hinzu	rfügen > ACE ł	 ninzufüç	je
enn die AC Is. um eine nzuzufüger	L erstellt wurd n Zugriffssteue 1. ager	e, wählen S erungseintra	ie <b>Add &gt; Add</b> g (ACE)	ACE (Hinzu	rfügen > ACE h	ninzufüç	je
enn die AC Is. um eine Dzuzufüger ACL Man Standard (	L erstellt wurde n Zugriffssteue ager	e, wählen S erungseintra	ie <b>Add &gt; Add</b> g (ACE)	ACE (Hinzu	rfügen > ACE h	ninzufüç	je
enn die AC s. um eine zuzufüger ACL Man Standard (	L erstellt wurde n Zugriffssteue ager CL Extended 4	e, wählen S erungseintra	ie <b>Add &gt; Add</b> ig (ACE)	ACE (Hinzu	ر المحدي Ifügen > ACE ا	ninzufüç	je
enn die AC s. um eine nzuzufüger ACL Man Standard / Standard /	L erstellt wurden n Zugriffssteue ager ACL Extended A	e, wählen S erungseintra ACL	ie Add > Add Ig (ACE)	ACE (Hinzu	, fügen > ACE ł	ninzufüç	je
enn die AC s. um eine nzuzufüger ACL Man Standard / Standard / Add	L erstellt wurden Zugriffssteue L ager ACL Extended A CL Extended A	e, wählen S erungseintra ACL   Delete   1	ie Add > Add ig (ACE)	ACE (Hinzu	Jifügen > ACE I	ninzufüç	je
enn die AC s. um eine nzuzufüger ACL Man Standard / Standard / Add Add	L erstellt wurden Zugriffssteue L ager ACL Extended A CL ACL	e, wählen S erungseintra ACL   Delete   1	ie Add > Add g (ACE)	ACE (Hinzu	Jifügen > ACE I	ninzufüç	je
enn die AC Is. um eine nzuzufüger ACL Man Standard / Standard / Add Add Add Add	L erstellt wurden Zugriffssteuen ager ACL Extended A CL Extended A ACL ACL ACL	e, wählen S erungseintra ACL   Delete   1	ie Add > Add g (ACE)	ACE (Hinzu	Jifügen > ACE I	ninzufüç	je

8. Definieren Sie den ACE, der dem LAN hinter der ASA entspricht. In diesem Fall ist das

Netzwerk 10.0.1.0/24.Klicken Sie auf das Optionsfeld Zulassen.Wählen Sie die Netzwerkadresse mit der Maske 10.0.1.0/24 aus.(Optional) Geben Sie eine Beschreibung an.Klicken Sie auf

ΟK

Split_Tunnel_List					<u> </u>		
	🔂 Add A	CE					
	Action		-				
	Action:	to permit to be	ліу				
	Address:	10.0.1.0/24					
	Descriptio	on:					
	The Corp	orate network behin	d the ASA				
			ок	Cancel	Help	T I	

9. Klicken Sie auf **OK**, um den ACL Manager zu verlassen.

Address List 10.0.1.0/24	Ai	rmit The Col	Description rporate network bel	hind the ASA
l_List	Pe	rmit The Col	rporate network bel	hind the ASA
10.0.1.0/24	✔ Pe	rmit The Col	rporate network bel	hind the ASA

ist.

General Servers Advanced	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do 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.
IE Browser Proxy	DN5 Names: 🔽 Inherit
SSL VPN Client	Policy: 🗆 Inherit Tunnel Network List Below 💌
Client Access Rule	Network List:  Inherit Split_Tunnel_List  Manage.
Hardware Clienc	Intercept DHCP Config Split_Tunnel_List
	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
	Subnet Mask (Optional): 0.0.0.0

11. Klicken Sie auf **OK**, um zur Gruppenrichtlinienkonfiguration

-General Servers -Advanced	Split tunneling network list require tunneling. The sec ACL that consists of list of	s distinguish networks that require traffic to go through the tunn- urity appliance makes split tunneling decisions on the basis of a n- addresses on the private network.	el and those that do n etwork list, which is an
IE Browser Proxy	DNS Names: 🔽 Inherit		
ie - SSL VPN Client ie - IPsec Client	Policy: 🗖 Inherit	Tunnel Network List Below	-
	Network List: 🥅 Inherit	Split_Tunnel_List	▼ Manage
	Intercept DHCP Confi	guration Message from Micosoft Clients	*
	DHCP Intercept lets Micr prior to XP, DHCP Interc	osoft XP clients use split tunneling with the security appliance. For opt provides the domain name and subnet mask.	or Windows dients
	Intercept: 🔽 Inherit	C Yes C No	
		Subnet Mask (Optional): 0.0.0.0	*

12. Klicken Sie auf **Apply** und dann **Send** (falls erforderlich), um die Befehle an die ASA zu senden.

Manag	Turne	Tunnalina Duata ad	1
Name Dfl:CroBolicy (System Default)	Internal	L 2TR-IDSec IDSec weburp	N//
Defaultaroup	Internal	Inberited	N/4
hivalleyvon	Internal	svc.IPSec	N/A

#### Konfigurieren der ASA 7.x und höher über die CLI

Anstatt das 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.

- 1. Wechseln in den Konfigurationsmodus ciscoasa>enable Password: \*\*\*\*\*\*\* ciscoasa#configure terminal ciscoasa(config)#
- 2. Erstellen Sie eine Zugriffsliste, die das Netzwerk hinter der ASA definiert. 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. Geben Sie den Konfigurationsmodus für Gruppenrichtlinien für die Richtlinie ein, die Sie ändern möchten.

ciscoasa(config)#group-policy hillvalleyvpn attributes
ciscoasa(config-group-policy)#

4. Geben Sie die Split-Tunnel-Richtlinie an. In diesem Fall wird die Richtlinie tunnelspezifiziert.

5. Geben Sie die Liste für den geteilten Tunnel-Zugriff an. In diesem Fall lautet die Liste **Split\_Tunnel\_List**.

ciscoasa(config-group-policy)#split-tunnel-network-list value Split\_Tunnel\_List

- 6. Geben Sie den folgenden Befehl ein: ciscoasa(config)#tunnel-group hillvalleyvpn general-attributes
- 7. Ordnen Sie die Gruppenrichtlinie der Tunnelgruppe zu. ciscoasa(config-tunnel-ipsec)# default-group-policy hillvalleyvpn
- 8. Schließen Sie die beiden Konfigurationsmodi. ciscoasa(config-group-policy)#exit ciscoasa(config)#exit ciscoasa#
- 9. Speichern Sie die Konfiguration im nichtflüchtigen RAM (NVRAM), und drücken Sie bei Aufforderung die Eingabetaste, um den Quelldateinamen anzugeben.

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

Gehen Sie wie folgt vor:

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

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

2. Erstellen Sie eine VPN-Gruppe *vpn3000*, und geben Sie die Split-Tunnel-ACL wie folgt an: PIX(config)#vpngroup vpn3000 split-tunnel split\_Tunnel\_List

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

## <u>Überprüfen</u>

Befolgen Sie die Schritte in diesen Abschnitten, um Ihre Konfiguration zu überprüfen.

- Herstellen einer Verbindung mit dem VPN-Client
- <u>VPN-Clientprotokoll anzeigen</u>
- Testen des lokalen LAN-Zugriffs mit Ping

#### Herstellen einer Verbindung mit dem VPN-Client

Verbinden Sie den VPN-Client mit dem VPN-Konzentrator, um Ihre Konfiguration zu überprüfen.

1. Wählen Sie den Eintrag für die Verbindung aus der Liste aus, und klicken Sie auf **Verbinden**.

Connection Entries       Status       Certificates       Log       Cisco       SYSTEM         Connection Entries       Certificates       Log       Connection Entry       Transport         Connection Entry        Host       Transport         hillwalleyvpn       172.22.1.160       IPSec/UDP	👌 VPN Client - Version 4.0.5 (Rel)		
Import       Import       Modity       Delete       Import       Import	Connection Entries Status Certificates Log O	otions Help	
Connection Entry V Host Transport hillvalleyvpn 172.22.1.160 IPSec/UDP	Connect New Import Mod	ify Delete	CISCO SYSTEMS
hillvalleyvpn 172.22.1.60 IPSec/UDP	Connection Entry	Host	Transport 🔺
	hillvalleyvpn	172.22.1.160	IPSec/UDP

2. Geben Sie Ihre Anmeldeinformationen

	VPN Client   Us	er Authen	ntication for "hillvalleyvpn"	
	CISCO SYSTEMS	<u>U</u> sername: <u>P</u> assword:	: marty	
ein.			OK Cancel	

3. Wählen Sie **Status > Statistics.. (Status > Statistik) aus.** um das Fenster Tunneldetails anzuzeigen, in dem Sie die Einzelheiten des Tunnels überprüfen und den Verkehrsfluss sehen

können.

👌 VPN Client 📔	5tatistics			×
Tunnel Details	Route Details	Firewall		
Address Info Client:	<b>rmation</b> 10.0.1.50	Connection Information Entry:	n hillvalley2	
Server:	172.22.1.160	Time:	0 day(s), 00:00.25	
Bytes Received: Sent:	0 1494	Encryption: Authentication:	168-bit 3-DES HMAC-SHA1	
Packets Encrypted: Decrypted: Discarded: Bypassed:	9 0 0 159	<b>Transport</b> Transparent Tunneling: Local LAN: Compression:	Inactive Disabled None	
			Reset	

4. Wechseln Sie zur Registerkarte Route Details (Routendetails), um die Routen anzuzeigen, die der VPN-Client für die ASA sichert. In diesem Beispiel sichert der VPN-Client den Zugriff auf 10.0.1.0/24, während der gesamte andere Datenverkehr nicht verschlüsselt und nicht über den Tunnel gesendet

🕽 VPN Client	Statistics		
Tunnel Details	Route Details Firev	vall	
Local LAN Rou	utes 🗟	Secured Rou	ites
Network	Subnet Mask	Network	Subnet Mask
		10.0.1.0	255.255.255.0
1		1	
			~
			Llose

VPN-Clientprotokoll anzeigen

Beim Überprüfen des VPN-Clientprotokolls können Sie bestimmen, ob der Parameter für das Split-Tunneling festgelegt ist. Um das Protokoll anzuzeigen, gehen Sie zur Registerkarte Log (Protokoll) im VPN-Client. Klicken Sie dann auf **Protokolleinstellungen**, um die protokollierten Einstellungen anzupassen. In diesem Beispiel ist IKE auf **3 - High (3 - Hoch)** festgelegt, während alle anderen Protokollelemente auf **1 - Low (1 - Niedrig)** festgelegt sind.



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 = 0x00000000 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.

#### Testen des lokalen LAN-Zugriffs mit Ping

Eine weitere Möglichkeit zum Testen, dass der VPN-Client für Split-Tunneling konfiguriert ist, während er für die ASA getunnelt wird, besteht in der Verwendung des **Ping-**Befehls in der Windows-Befehlszeile. 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.

```
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 durch die Anzahl der Einträge in einer Split-Tunnel-ACL

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

## Zugehörige Informationen

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