Configure Split Tunneling for VPN Clients on the ASA

Contents

Introduction
Prerequisites
Requirements
Components Used
Network Diagram
Related Products
Conventions
Background Information
Configure Split Tunneling on the ASA
Configure the ASA 7.x with Adaptive Security Device Manager (ASDM) 5.x
Configure the ASA 8.x with ASDM6.x
Configure the ASA 7.x and later via CLI
Configure PIX 6.x through the CLI
<u>Verify</u>
Connect with the VPN Client
View the VPN Client Log
Test Local LAN Access with Ping
Troubleshoot
Limitation with Number of Entries in a Split Tunnel ACL
Related Information

Introduction

This document describes the process to allow VPN Clients access to the Internet while tunneling into a Cisco ASA 5500 Series Security Appliance.

Prerequisites

Requirements

This document assumes that a working remote access VPN configuration already exists on the ASA. Refer to <u>PIX/ASA 7.x as a Remote VPN Server using ASDM Configuration Example</u> if one is not already configured.

Components Used

The information in this document is based on these software and hardware versions:

• Cisco ASA 5500 Series Security Appliance Software version 7.x and later

- Cisco Systems VPN Client version 4.0.5
- Adaptive Security Device Manager (ASDM)



Note: This document also contains the PIX 6.x CLI configuration that is compatible for the Cisco VPN client 3.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Network Diagram

The VPN Client is located on a typical SOHO network and connects across the Internet to the main office.



Network Diagram

Related Products

This configuration can also be used with Cisco PIX 500 Series Security Appliance Software version 7.x.

Conventions

Refer to the <u>Cisco Technical Tips Conventions</u> for more information on document conventions.

Background Information

This document provides step-by-step instructions on how to allow VPN Clients access to the Internet while they are tunneled into a Cisco Adaptive Security Appliance (ASA) 5500 Series Security Appliance. This configuration allows VPN Clients secure access to corporate resources via IPsec while giving unsecured access to the Internet.



Note: Full tunneling is considered the most secure configuration because it does not enable simultaneous device access to both the Internet and the corporate LAN. A compromise between full tunneling and split tunneling allows VPN Clients local LAN access only. Refer to <u>PIX/ASA</u> 7.x: Allow Local LAN Access for VPN Clients Configuration Example for more information.

In a basic VPN Client to ASA scenario, all traffic from the VPN Client is encrypted and sent to the ASA no matter what its destination is. Based on your configuration and the number of users supported, such a set up can become bandwidth intensive. Split tunneling can work to alleviate this problem since it allows users to send only that traffic which is destined for the corporate network across the tunnel. All other traffic such as instant messaging, email, or casual browsing is sent out to the Internet via the local LAN of the VPN Client.

Configure Split Tunneling on the ASA

Configure the ASA 7.x with Adaptive Security Device Manager (ASDM) 5.x

Complete these steps in order to configure your tunnel group to allow split tunneling for the users in the group.

1. Choose **Configuration > VPN > General > Group Policy** and select the Group Policy that you wish

to enable local LAN access in. Then click Edit .



2. Go to the Client Configuration tab.

General IPSec Client Configuration Client Firewall	Hardware Client NAC WebVPN
لح Check an Inherit checkbox to let the corresponding	setting take its value from the default group policy.
General Client Parameters Cisco Client Parameter	Microsoft Client Parameters
Banner:	Edit Banner
Default Domain:	I Inherit
	E trans
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>>
	<≤Remove

3. Uncheck the Inherit box for Split Tunnel Policy and chose Tunnel Network List Below ..

Name: hillvalleyvpn		
and the Cient Configuration Large to		[
General IPSec Client Configuration Client Firewa	II Hardware Client	NAC WebYPN
Check an Inherit checkbox to let the corresponding	g setting take its valu	e from the default group policy.
Ceneral Clant Decemeters	1	
General Client Parameters Cisco Client Paramete	rs Microsoft Client	Parameters
Banner	V Inherit	Edit Banner
During.	1. Autom	Leading and Million star
Default Domain:	🔽 Inherit	
	_	
Split Tunnel DNS Names (space delimited):	Minherit	I
Soft Tunnel Policy:	🗆 Inherit	Turppel All Networks
opic runner oney.		Tunnel All Networks
Split Tunnel Network List	🔽 Inherit	Tunnel Network List Below
		Exclude Network List Below
Address pools		
linherit		
Avaïable Pools		Assigned Pools (up to 6 entries)
	Add>>	1
	DELCOTIONE /	
		1

4. Uncheck the **Inherit** box for Split Tunnel Network List and then click **Manage** in order to launch the ACL Manager.

ame: hilvalleyvpn neral IPSec 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:			
IPSec 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 Manage Address pools Address Assigned Pools (up to 5 entries) Imment Address Address	Name: hillvalleyvpn		
Integrate of the corresponding setting take its value from the defauit group policy. 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 Address pools Image: Address Address pools Address Address pools Address	nexe Direct Configuration Client Stressel	Literature Clear	
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: Image: Cisco Client Parameters Microsoft Client Parameters Default Domain: Image: Cisco Client Parameters Microsoft Client Parameters Split Tunnel DNS Names (space delimited): Image: Cisco Client Parameters Manage: Cisco Client Parameters Split Tunnel Policy: Imment Tunnel Network List Below Imment Split Tunnel Network List: Imment Manage: Cisco Client Parameters Manage: Cisco Client Parameters Address pools Imment Address pools Address Client Parameters Address (op to 6 entries) Address pools Imment Address (op to 6 entries) Imment Imment	neral IPSec Clent Configuration Clent Pirewall	I Hardware Client	NAC WEDVHN
General Client Parameters Cisco Client Parameters Microsoft Client Parameters Banner: Inherit Edit Benner Default Domain: Inherit Edit Benner Spit Tunnel DNS Names (space delimited): Inherit Tunnel Network List Below Spit Tunnel Policy: Inherit Tunnel Network List Below Spit Tunnel Network List: Inherit None Address pools Address pools Imherit Address Address pools Imherit Address	Check an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.
Banner: Image: Default Domain: Image: Spit Tunnel DNS Names (space delimited): Image: Spit Tunnel Policy: Image: Spit Tunnel Network List: Image: Address pools Image: Address pools Image: Address pools	General Client Parameters Cisco Client Parameter	s Microsoft Client	Parameters
Banner: Image: Edit Benner, Default Domain: Image: Imag			
Default Domain: Image: Control of the set of t	Banner:	🗹 Inherit	Edit Benner
Spit Tunnel DNS Names (space delimited):	Default Domain:	🔽 Inherit	
Spit Tunnel DNS Names (space delimited): Pint Spit Tunnel Network List Spit Tunnel Network List: Inherit Address pools Add>>		_	
Spit Tunnel Policy:	Split Tunnel DNS Names (space delimited):	I⊻ Inherit	
Spit Tunnel Network List: Address pools I Inherit Available Pools Address Address pools (up to 6 entries) Address Address Address Address Address Areanove	Split Tunnel Policy:	🗖 Inherit	Tunnel Network List Below
Spit Tunnel Network List:			
Address pools Inherit Available Pools Assigned Pools (up to 6 entries) Add>>	Split Tunnel Network List:	☐ inherit	None Manage
Inherit Available Pools Assigned Pools (up to 6 entries) Add>>	Address pools		~~
Available Pools (up to 6 entries) Add>> Add>>	Inherit		
Add>>	Available Pools		Assigned Pools (up to 6 entries)
<-Remove		Add⊳⊳	1
		<-Remove	1

5. Within the ACL Manager, choose **Add** > **Add** ACL... in order to create a new access list.

ALL Manager					<u> </u>
Standard AG. Edende	I ACL				
💠 Add 🔹 📑 548. 🎁	2007 🕈 🤞	3. Ro 85			
🔶 Add ACL.	dress	Action	Description		
⊕ ASLACE. N					
The inset of the					
aproperty context.					

6. Provide a name for the ACL and click **OK**.

📫 ACL Manager			X
Stendard ACL Extended ACL			
◆Add + Ⅲ DCT Ⅲ DCTTO	F 苦胎胞 -		
No Address	Addon Description		
	ACI, Name: Splt_Turnel_List	Holp	
Flue Plow Degrees			×
	OK Cancel	THE	

7. Once the ACL is created, choose Add > Add ACE.. .in order to add an Access Control Entry (ACE).



- 8. Define the ACE that corresponds to the LAN behind the ASA. In this case, the network is 10.0.1.0/24.
 - a. Choose Permit .
 - b. Choose an IP Address of 10.0.1.0
 - c. Choose a Netmask of **255.255.255.0**.
 - d. (Optional)Provide a description.
 - e. Click > **OK**.

10		olitor
Splt_Turnet_Lie	Part New Door	
	di Add ACE	
	- Action	
	Action 📌 Poret 💌	
	thorthertwork	
	P Address: 100.1.0	
	Netwask: 255 255 255 0	
	Description: The correction performed the la S.A.	
		Careed Hore
Je Flow Diegner	au meide.	outside La
		· · · · · · · · · · · · · · · · · · ·

9. Click **OK** in order to exit the ACL Manager.

	KCL Manage					
I	Senderd AC	Extended ACL				
	🗣 Add 🕞	🖬 Ese 🏥 Delete 🏼 🕈	4 3 階間			
	No	A391050	Action	Description		
	E-spt_tw	wel_List				
	1	10.03.024	Y Pernit	The corporate network behind the ASA.		

10. Be sure that the ACL you just created is selected for Split Tunnel Network List.

Internal Group Policy: hillvalleyvpn		
Nome: Initvalleyvpn		
General 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 Parameter	s Microsoft Client	Parametera
Provent Sector 201	E have	C di Davana
barner:	P intert	ED-DOVAT
Default Domain:	P Inherit	
Spit Tunnel DNS Names (space delimited):	17 Inherit	
Split Tunnel Policy:	E intert	Turnel Network List Below
Spit Tunnel Network List:	inhert	Spit_Turnet_L Manage
Address pools		Splt_Turnel_List
F interit		outside_oryptomap%
Avolatie Poola		Assigned Peolo (up to 6 entries)
	Addre	1
	colientove	i l

11. Click **OK** in order to return to the Group Policy configuration.

Neme Nitralegypn General IPSec Clert Configuration Clert Pinewall Hardware Clert NAC WebVPN Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. General Clert Parameters Cloco Clert Parameters Morosoft Clert Parameters Berner: IP Inherit Edt.Borner IP Inherit Edt.Borner Default Domain IP Inherit Immediate State St	t Internal Group Policy: hillvalleyvpn	$1 \rightarrow 1$	
General PSec Gent Configuration Cleart Finewall Hardware Cleart NAC WebVPN Check an Inhert checkbox to let the corresponding setting take its value from the default group policy. General Cleart Parameters Cloco Cleart Parameters Microsoft Cleart Parameters Berner: Inhert Edf: Berner Default Domain: Inhert Edf: Berner Split Tunnel DNS Nerves (space delimited): Inhert Inhert Split Tunnel Policy: Inhert Inhert Inhert Split Tunnel Network List Inhert Inhert Manage Address pools Inhert Inhert Manage	Name: hilvalleyvpn		
Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. General Client Parameters Cloco Client Parameters Microsoft Client Parameters Banner: Inherit Edit Domain: Default Domain: Inherit Inherit Spit Tunnel DNS Names (space delimited): Inherit Tunnel Network List Below Spit Tunnel Network List: Inherit Inherit Address pools Minnest Menage	General IPSec Client Configuration Client Firewall	Hardware Client	NAC WEDVPN
General Client Parameters Cloco Client Parameters Microsoft Client Parameters Banner: Imment Edit Eormen Default Donvain Imment Edit Eormen Spit Tunnel DMS Names (space delimited) Imment Tunnel Network List Below Spit Tunnel Policy: Imment Tunnel Network List Manage Addresse pools Addresse pools Imment Manage	Check an Inherit checkbox to let the corresponding	setting take its vak	ue from the detault group policy.
Barner: Image: Imag	General Client Parameters Cisco Client Parameters	s Microsoft Client	Parametora
Barner: Immediate Edr. Borner Default Domain: Immediate Immediate Spit Tunnel DNS Names (space delimited): Immediate Immediate Spit Tunnel Policy: Immediate Immediate Spit Tunnel Network List: Immediate Manage Address pools Immediate Immediate		-	
Detault Domain: Image: Comparison of the comparison of t	Barner:	🖂 Inhert	Edt Borner
Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Spit Tunnel Network List: Address pools	Default Domain:	P intert	
Spit Tunnel Policy:	Split Tunnel DNS Names (space delimited):	I inhert	
Spit Tunnel Network List: Inherit Spit_Tunnel, L* Manage	Split Tunnel Policy:	□ inherit	Turnel Network List Below
-Address pods	Spilt Tunnei Network List:	F Intert	Spit_Tunnel_L Manage
	-Address pools		

12. Click **Apply** and then **Send** (if required) in order to send the commands to the ASA.



Configure the ASA 8.x with ASDM 6.x

Complete these steps in order to configure your tunnel group to allow split tunneling for the users in the group.

1. Choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, and choose the Group Policy in which you want to enable local LAN access. Then click **Edit**.

Co	nfiguration > Remote Access VPN > Network (Client) Access > Group Policies								
	Manage VPN group policies. A VPN group poli externally on a RADIUS/LDAP server. The gro	cy is a collection of use oup policy information	er-oriented attribute/value pairs that may b is referenced by VPN tunnel groups and use	e stored internal er accounts.					
	Add - CE Edit Delete								
	Name	Туре	Tunneling Protocol	A					
	OfftGrpPolicy (System Default)	Internal	L2TP-JPSec, IPSec, webvpn	N/A					
	Defaultgroup	Internal	Inherited	N/A					
	hivaleyvpn	- Internal	svc,IPSec	N/A)					

2. Click Split Tunneling.

General Servers - Advanced - Et browser Procy - SEL WPN Client	Split turnwing n require turnwing ACL that consist DNS Names: F	etwork list g. The sec is of list of	ts distingu curity appl f addresse	esh networks the lance makes split es on the private	t require traffic to tunneling decision pelvenik.	go through the tur is on the basis of a	mel and the network lis	ose that do no 8. which is an
	DNS Names: F							
E-1Psec Clienc	Policy: F	7 Inherit 7 Inherit					×	
Clent Access Rule Clent Firewal	Network List: F	7 liferii					×	Martege
There was a	Intercept Dr	ICP Confi	iguration	n Message from	n Micosoft Clier	da .		
	Intercept: 🔽	Inherit	C Yes	C ho	0.0.0.0			-
			10110.15	ar(0,001d);	0.0.00			

3. Uncheck the Inherit box for Split Tunnel Policy, and chose Tunnel Network List Below.

ſ	Edit Internal Group Policy	: hivalleyvpn
	General Servers E Advanced	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do in 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.
	Electrometro III Browser Procy El-52L VPN Clent	ENS Names: 🖓 Inhent Policy: Turnel Network List Below
	Clerit Access Rule	Network Let: IZ Inherit Tunnel Al Networks Ist Below Tunnel Network List Below Tunnel Network List Below
	·····Haroware Clenc	Intercept DHCP Configuration Message from Micosoft Clients
		DHCP Intercept lets Microsoft XP clerits use split tunneling with the security appliance. For Windows clerits prior to XP, DHCP Intercept provides the domain name and subnet mask.

4. Uncheck the **Inherit** box for Split Tunnel Network List, and then click **Manage** in order to launch the ACL Manager.

f	Edit Internal Group Policy	i hivalleyvpn
	General Servers E-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-Pise: Client	Policy: Dinherit Turnel Network List Below +
	- Client Access Rule - Client Firewall	Network List: Note
	-Hardware Clienk	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 Vos - C No
		Subret Mark (Optiona): 0.0.0.0

5. Within the ACL Manager, choose **Add** > **Add ACL...** in order to create a new access list.

ACL	Manager		and the second s		
Stand	dard ACL Extended	ACL			
* A	vdd 🔹 🎯 EdR 🥤	Delete	★ ↓ 3. № 8	<u>B.</u> +	
4	Add ACL		Action	Description	
*	Add ACE	-			
4	Insert				
-	Insert After				

6. Provide a name for the ACL, and click **OK**.

🚰 ACL Menager			
Standard ACL Extended ACL			
4 Add • El Edt The Delete	4 X Ba (8)		
	- 00	Bernelikien	
No Address	Action	Description	
🔂 Add A		X	
ACI Nas	ne: Solt Turcel List		
	en http://www.bod		
	OK Caricel	Help	
	-		

7. Once the ACL is created, choose Add > Add ACE... in order to add an Access Control Entry (ACE).



- 8. Define the ACE that corresponds to the LAN behind the ASA. In this case, the network is 10.0.1.0/24.
 - a. Click the **Permit** radio button.
 - b. Choose the network address with mask 10.0.1.0/24.
 - c. (Optional) Provide a description.
 - d. Click OK.

ACL Manager
Sandard ACL International
No Address Addon Description
Stradd Arts
Action: @ Permit C Deny
Address: 10.0.1.0/24
Description:
The Corporate network behind the ASA
OK Cancel Help

9. Click **OK** in order to exit the ACL Manager.

ACL Manager	<u>, , , , , , , , , , , , , , , , , , , </u>	<u> </u>	
Standard ACL Extended ACL			
A ALL - TO EAL O PALL		nin -	
🗣 Haa 🔹 🔄 Eat 🚺 Delete	7 4 6 93	105 T	
No Address	Action	Descriptio	n
Splt_Tunnel_List		he Connecte network h	abind the ACA
1 <u>10</u> + 10.0.1.0/24	ermit.	ne corporate network c	ening the Mon
1			
	K	OK Canra	Help

10. Be sure that the ACL you just created is selected for Split Tunnel Network List.

E	Edit Internal Group Policy: General Servers Advanced	c hivalleyvpn Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, ACI, that consists of list of addresses on the private network.	e that do no which is an
	IE Browser Praxy (ii)-SSL VPN (client (iii)-SSL VPN (client)	DNS Names: 🖓 Inherit Policy: 🗇 Inherit Tunnel Network List Below 💌	
	Clent Access Rule Clent Firewal Hardware Clent	Network List: Differit Spit_Tunnel_List Intercept DHCP Config Spit_Tunnel_List	Manage
		DHCP Intercept lets Microsoft XP clients use split tunneling with the security appliance. For Windows prior to XP, DHCP Intercept provides the domain name and subnet mask.	clients

11. Click **OK** in order to return to the Group Policy configuration.

General General Servers Advanced Spit Tunneling E Browser Proxy	 Split tunneling network list require tunneling. The sec ACL that consists of list of DNS Names: 17 Inherit 	s distinguish networks that require traffic to go through the tun wity appliance makes split tunneling decisions on the basis of a addresses on the private network.	mel and those that do not network let, which is an
⊞-SSLWN Clent ⊞-IPsec Clent	Policy: There Network List: There Intercent DHCP Confi	Tunnel Network List Below Split_Tunnel_List	× Manage
	DHCP Intercept lets Micr prior to 3P, DHCP Intero Intercept: 🔽 Inherit	osoft XP clients use split tunneling with the security appliance. I apt provides the domain name and subnet mask. C. You. C. Yu: Subnet Mask (Options7): 0.0.0.0	For Windows clients

12. Click Apply and then Send (if required) in order to send the commands to the ASA.

Contributation / Remote Access OFM / Network (Citeria) Access / Oroup (

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

mal L2TP mal Inf mal svc, I	-IPSec, IPSec, we writed PSec	bvpn	N/4 N/4 N/4
rnal Ini mal svc, I	nerked PSec		14/4 N/4
mal svc, J	PSec		N/J

Configure the ASA 7.x and later via CLI

Rather than use the ASDM, you can complete these steps in the ASA CLI in order to allow split tunneling on the ASA:

Acoly Reset



Note: The CLI Split Tunneling configuration is the same for both ASA 7.x and 8.x.

1. Enter configuration mode.

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

2. Create the access list that defines the network behind the ASA.

```
<#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
```

3. Enter Group Policy configuration mode for the policy that you wish to modify.

```
<#root>
ciscoasa(config)#
group-policy hillvalleyvpn attributes
ciscoasa(config-group-policy)#
```

4. Specify the split tunnel policy. In this case the policy is **tunnelspecified**.

```
<#root>
ciscoasa(config-group-policy)#
split-tunnel-policy tunnelspecified
```

5. Specify the split tunnel access list. In this case, the list is Split_Tunnel_List.

```
<#root>
ciscoasa(config-group-policy)#
split-tunnel-network-list value Split_Tunnel_List
```

6. Issue this command:

```
<#root>
ciscoasa(config)#
tunnel-group hillvalleyvpn general-attributes
```

7. Associate the group policy with the tunnel group

<#root>

```
ciscoasa(config-tunnel-ipsec)#
default-group-policy hillvalleyvpn
```

8. Exit the two configuration modes.

```
<#root>
ciscoasa(config-group-policy)#
exit
ciscoasa(config)#
exit
ciscoasa#
```

9. Save the configuration to non-volatile RAM (NVRAM) and press **Enter** when prompted to specify the source filename.

```
<#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#
```

Configure PIX 6.x through the CLI

Complete these steps:

1. Create the access list that defines the network behind the PIX.

<#root>

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

2. Create a vpn group **vpn3000** and specify the split tunnel ACL to it as shown:

```
<#root>
PIX(config)#
vpngroup vpn3000 split-tunnel Split_Tunnel_List
```



Note: Refer to <u>Cisco Secure PIX Firewall 6.x and Cisco VPN Client 3.5 for Windows with</u> <u>Microsoft Windows 2000 and 2003 IAS RADIUS Authentication</u> for more information on remote access VPN configuration for PIX 6.x.

Verify

Complete the steps in these sections in order to verify your configuration.

- Connect with the VPN Client
- <u>View the VPN Client Log</u>
- Test Local LAN Access with Ping

Connect with the VPN Client

Connect your VPN Client to the VPN Concentrator in order to verify your configuration.

1. Choose your connection entry from the list and click **Connect**.

Connection Entries Status Certificates Log Log Entries Entries	
Import	
Connection Entry Log Connection Entry Host Transport Initivaleyvpm 172.221.160 IPSec/UDP	STSTENS
Connection Entry V Host Transport	
hilveleyvpn 172.22.1.160 IPSec/UDP	
<u></u>	

2. Enter your credentials.

👌 VPN Client U	ser Authen	ntication for "hillvalleyvpn" 🛛 🗙
Cisco Systems	<mark>∐sername:</mark> <u>P</u> assword:	marty Cancel

3. Choose **Status > Statistics...** in order to display the Tunnel Details window where you can inspect the particulars of the tunnel and see traffic flowing.



4. Go to the Route Details tab in order to see the routes that the VPN Client is securing to the ASA.

In this example, the VPN Client is securing access to 10.0.1.0/24 while all other traffic is not encrypted and not sent across the tunnel.

8	VPN Client Sta	tistics			×
1	Tunnel Details Route Details Firewall				
	Local LAN Routes		Secured Routes		
	Network	Subnet Mask	Network	Subnet Mask	וונ
			10.0.1.0	255.255.255.0	

View the VPN Client Log

When you examine the VPN Client log, you can determine whether or not the parameter that specifies split tunneling is set. In order to view the log, go to the Log tab in the VPN Client. Then click on **Log Settings** in order to adjust what is logged. In this example, IKE is set to **3 - High** while all other log elements are set to **1 - Low**.

VPN Client - Version 4.0.5 (Rel)	_ 🗆 🗵
Connection Entries Status Certificates Log Options Help	
Disable Clear Log Settings Log Window Connection Entries Certificates Log	Cisco Systems
Cisco Systems VPN Dient Version 4.0.5 (Ref) Copyright (C) 1998-2003 Disco Systems, Inc. All Rights Reserved. Dient 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
27
      14:20:14.208 07/27/06 Sev=Info/5
                                            IKE/0x630000D
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 = 0x0000001
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.
```

Test Local LAN Access with Ping

An additional way to test that the VPN Client is configured for split tunneling while tunneled to the ASA is to use the **ping** command at the Windows command line. The local LAN of the VPN Client is 192.168.0.0/24 and another host is present on the network with an IP address of 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>
```

Troubleshoot

Limitation with Number of Entries in a Split Tunnel ACL

There is a restriction with the number of entries in an ACL used for split tunnel. It is recommended not to use more than 50-60 ACE entries for satisfactory functionality. You are advised to implement the subnetting feature to cover a range of IP addresses.

Related Information

- <u>PIX/ASA 7.x as a Remote VPN Server using ASDM Configuration Example</u>
- <u>Cisco ASA 5500 Series Adaptive Security Appliances</u>
- <u>Cisco Technical Support & Downloads</u>