# Configuration de la transmission tunnel partagée pour les clients VPN sur l'ASA

# Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Diagramme du réseau
Produits connexes
Conventions
Informations générales
Configurer la transmission tunnel partagée sur ASA
Configurer ASA 7.x avec l'Adaptive Security Device Manager (ASDM) 5.x
Configurer ASA 8.x avec ASDM6.x
Configurer ASA 7.x et ultérieures via l'interface de ligne de commande (CLI)
Configurer PIX 6.x via l'interface de ligne de commande (CLI)
Vérifier
Se connecter avec le client VPN
Afficher le journal du client VPN
Tester l'accès local au LAN avec un ping
Dépannage
Limitation avec le nombre d'entrées dans une ACL de tunnel partagé
Informations connexes

# Introduction

Ce document décrit le processus permettant aux clients VPN d'accéder à Internet tout en effectuant une tunnellisation vers un dispositif de sécurité de la gamme Cisco ASA 5500.

# Conditions préalables

## Exigences

Ce document suppose qu'une configuration de VPN d'accès à distance opérationnelle existe déjà sur l'ASA. Référez-vous à <u>Exemple de configuration de PIX/ASA 7.x comme serveur VPN distant</u> avec l'ASDM si cette configuration n'est pas encore effectuée.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel du dispositif de sécurité de la gamme Cisco ASA 5500 version 7.x et ultérieures
- Client VPN version 4.0.5 de Cisco Systems
- Adaptive Security Device Manager (ASDM)



Remarque : ce document contient également la configuration CLI PIX 6.x qui est compatible avec le client VPN Cisco 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Diagramme du réseau

Le client VPN est situé sur un réseau SOHO standard et se connecte à travers l'Internet au bureau central.





## Produits connexes

Cette configuration peut également être utilisée avec le logiciel du dispositif de sécurité de la gamme Cisco PIX 500 version 7.x et ultérieures.

## Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

## Informations générales

Ce document fournit des instructions pas à pas sur la façon d'autoriser l'accès des clients VPN à l'Internet tandis qu'ils sont reliés par tunnel à un dispositif de sécurité adaptatif dédié de la gamme Cisco ASA 5500. Cette configuration offre aux clients VPN un accès sécurisé aux ressources de l'entreprise par l'intermédiaire d'IPsec tout en bénéficiant d'un accès non sécurisé à 'Internet.



Remarque : la transmission tunnel complète est considérée comme la configuration la plus sécurisée, car elle n'autorise pas l'accès simultané des périphériques à Internet et au réseau local de l'entreprise. Un compromis entre tunnellisation complète et split tunneling permet aux clients VPN d'accéder au LAN local uniquement. Référez-vous à <u>Exemple de configuration de PIX/ASA 7.x : Allow Local LAN Access for VPN Clients</u> pour plus d'informations.

Dans un scénario de connexion de base d'un client VPN à ASA, tout le trafic provenant du client VPN est crypté et envoyé à ASA quelle que soit sa destination. En fonction de votre configuration et du nombre d'utilisateurs pris en charge, une telle configuration peut devenir gourmande en bande passante. La transmission tunnel partagée peut aider à résoudre ce problème puisqu'elle permet aux utilisateurs de n'envoyer que le trafic qui est destiné au réseau de l'entreprise à travers le tunnel. Tout autre trafic, comme la messagerie instantanée, l'email, ou la navigation occasionnelle, est envoyé à l'Internet par l'intermédiaire du LAN local du client VPN.

# Configurer la transmission tunnel partagée sur ASA

## Configurer ASA 7.x avec l'Adaptive Security Device Manager (ASDM) 5.x

Complétez ces étapes afin de configurer votre groupe de tunnels de façon à permettre la transmission tunnel partagée pour les utilisateurs du groupe.

1. Choisissez Configuration > VPN > General > Group Policy et sélectionnez la stratégie de groupe dans laquelle vous souhaitez activer l'accès au LAN local. Cliquez alors sur Edit.



2. Accédez à l'onglet Client Configuration.

General IPSec Client Configuration Client Firewall	Hardware Client NAC WebVPN
لرج 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. Décochez la case Inherit pour Split Tunnel Policy et choisissez Tunnel Network List Below ..

Name: hillvalleyvpn		
Client Configuration Client Success	Lundone con	
eneral   PSec Clerk Comgunation   Clerk Pirewall	Hardware Client	NAC   WebYPN
Check an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.
Ceneral Clert Perspetere	1	
General Client Parameters   Cisco Client Parameters	s   Microsoft Client	Parameters
Banner	V Inharit	Edit Banner
Danner.	14 HILIGH	Luc Durine
Default Domain:	🔽 Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
	<b>-</b>	
Split Tunnel Policy:	I_ Innert	Turnel All Networks
Colli Turned Methodal Lint	The last and	Tunnel Network List Below
Spir Furner Network List.	iv mient	Exclude Network List Below
Address pools		
l⊽ Inherit		
Avaïable Pools		Assigned Pools (up to 6 entries)
	A state of	
	Addee	1
	< <remove< td=""><td>]</td></remove<>	]
		1

Désactivez la case Inherit pour la liste Split Tunnel Network List, puis cliquez sur Manage pour lancer l'ACL Manager.

ternal Group Policy: hillvalleyvpn		
ame: hillvalleyvpn		
neral IPSec Client Configuration Client Firewal	Hardware Client	
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	Parameters
Banner:	🔽 Inherit	Edit Banner
Dodeu di Devuelori	-	
Derault Domain.	i∾ innent	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Split Tunnel Policy:	🗌 Inherit	Tunnel Network List Below
Split Tunnel Network List:		None Manage
Address pools		
🔽 Inherit		Assistant Danie (un la Combine)
Avenable Pools		Assigned Pools (up to 6 entries)
	Add≽≻	
	< <remove< td=""><td>]</td></remove<>	]
		,

Dans le gestionnaire de listes de contrôle d'accès (ACL), choisissez « Add > Add ACL... » (ajouter > ajouter une ACL...) pour créer une nouvelle liste d'accès.

Standard ACL Extended ACL	
◆Add • 留 GB 官 PHON 于 4 — 茶 釉 臨 +	
Add ACL dress Action Description	
♠ Addiace. **	
The insert Attor	

Fournissez un nom pour l'ACL et cliquez sur OK.

ACI. Manager		
Standard ACL Extended ACL		
◆ Add → () ESC () DSSS () + 4	X 16 10 -	
No Address	Adon Desortation	
	S Add ACL	×
	AG, Nanet: Splt_Turnel_List	
	OK Cancel	Holp
Rule Flow Disgreen		×
	Maide a cutatie	
	🔶 🖌 dony	• · · · · · · · · · · · · · · · · · · ·
	OK Cancel	196

Une fois la liste de contrôle d'accès créée, choisissez Add > Add ACE. .afin d'ajouter une entrée de contrôle d'accès (ACE).

٠



Définissez l'ACE qui correspond au LAN derrière l'ASA. Dans ce cas, le réseau est 10.0.1.0/24.

a.

Choisissez Permit.

b.

Choisissez une adresse IP 10.0.1.0

c.

Choisissez un masque de réseau 255.255.255.0.

#### d.

(Facultatif) Fournissez une description.

Cliquez sur > **OK**.

tenderd ACL Edend		
Add = Ⅲ ESC		
Solt Turnel List	Address Action Description	
	Adian	
	Action V Porvet	
	HortMetwork	
	P Addess: 10.0.1.0	
	Netwask: 255 255 255 0	
	The corporate network behind the ASA.	
	OK Cancel Holp	
Rule Flow Diegram	and method La	

Cliquez sur OK afin de quitter l'ACL Manager.

•

e.



Assurez-vous que l'ACL que vous venez de créer est sélectionné pour la liste Split Tunnel Network List.

neering of days roles, his value, your		
lame: hilvsleyvpn		
event Diser Client Configuration Client Disease	Lineturara Clarit	NAC WARNEN
renal poet construction of Clerc Previa	IT Hardware Client	[ Note ] independ
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
Processo -	17 Internet	Ett Davage
parner.	iv men	EB. DOVICE
Default Domain:	P Inherit	
Split Tunnel DNS Names (space delimited);		
Split Tunnel Policy:	Inherit	Turnel Network List Below
Split Tunnel Network List:	[ Intert	Solt Turnel L., * Menage.,
		None
-Address pools		Splt_Tunnet_List outside_cryptome5
Avaiatie Pacia		Assigned Pools (up to 5 entries)
	A031**	
	ciditettione	J

Cliquez sur OK afin de retourner à la configuration de la stratégie de groupe.

🔂 Ed	it Inter	nal Grou	p Policy: hillvalk	yvpn				×
	Nome	h	Ivalleyvpn	_				
	Genera	IPSec	Client Configuration	n Client Firewall Ha	rdware Client	NAC WebVPN		_
	Chec	k an Inha	nt checkbox to let t	he corresponding setti	ng taka its valu	e from the default group	policy.	
	Gene	erai Client	Parameters Cisc	o Client Parameters   N	lorosoft Client	Parametera		
	6	enter:			🖂 inherit	Esit Bory	761	
	D	efault Don	nain:		P Interit			
	S	pitt Tunnel	DNS Names (spac	e delivited):	I⊽ inhert			
	9	plit Tunnel	Policy:		□ inherit	Tunnel Network List B	ielow 💌	
	9	pitt Tunnel	Network List:		linhert	Splt_Turnet_L *	Manage	
	E.	lddress p	ools					

Cliquez sur Apply puis sur Send (s'il y a lieu) afin d'envoyer les commandes à l'ASA.

٠



#### Configurer ASA 8.x avec ASDM 6.x

Complétez ces étapes afin de configurer votre groupe de tunnels de façon à permettre la transmission tunnel partagée pour les utilisateurs du groupe.



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 interna externally on a RADIUS/LDAP server. The group policy information is referenced by VPN bunnel groups and user accounts. Add * Collection Collecti						
Name	Туре	Tunneling Protocol	A			
OfftGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webvpn	N/A			
Defaultgroup	Interna	Inherited	N/A			
hivalleyvpn	Internal	svc, IPSec	N/A			

Cliquez sur Split Tunneling.

•

📫 Edit Internal Group Policy:	hivalleyvpn		
General Servers B-Advanced	Split tunneling network lists require tunneling. The secur ACI, that consists of list of a	distinguish networks that require traffic to ity appliance makes split tunneling decision didresses on the private network.	go through the tunnel and those that do no is on the basis of a network list, which is an
-IE Browser Proxy	DNS Names: 🕫 Inherit	[	
B-SSL WIN Client	Policy: 🖂 Inherit		×
Clent Access Rule Clent Firewal	Network List: 🖓 [nheit]		Managat
Thoroward Group	Intercept DHCP Config	uration Message from Micosoft Clier	és (8)
	prior to XP, DHCP Intercept	t provides the domain name and subnet n	and.
	5.	bhet Mesk (Optionel): 0.0.0.0	<u>×</u>
1 I I I			
<u> </u>			

Désactivez la case Inherit pour la stratégie Split Tunnel Policy et choisissez Tunnel Network List Below.

1	Edit Internal Group Policy	y: hivalleyvpn	
	General Servers	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those the require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which AQ, that consists of list of addresses on the private network.	t don e hiis an
		DNS Names: IF Inherit Turnel Network List Below	
	<ul> <li>Olent Access Rule</li> <li>Clent Firewal</li> </ul>	Network Liet: IF Inherit	ge
	- Hardware Clienk	Interrent NHCD Configuration Manager from Microsoft Clients	
		DHCP Intercept lets Microsoft XP clerits use split tunneling with the security appliance. For Windows cleri prior to XP, DHCP Intercept provides the domain name and subnet mask. Intercept: IF Inherit. C Yes. C No.	3

Désactivez la case Inherit pour la liste Split Tunnel Network List, puis cliquez sur Manage pour lancer l'ACL Manager.

f Edit Internal Group Policy:	i hivalleyypn
General Servins Advanced - 2E Browser Proxy B-SS, VPN Client B-3Post Client - Client Access Rulie - Client Risevall Hardware Client	Spit tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The security applance 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 Nemes:
	Scient Muk (Grenny): 0.000
	Sector and Sector Secto

Dans le gestionnaire de listes de contrôle d'accès (ACL), choisissez « Add > Add ACL... » (ajouter > ajouter une ACL...) pour créer une nouvelle liste d'accès.



Fournissez un nom pour l'ACL et cliquez sur OK.

•

🜈 ACL Manager			
Standard ACL Extended ACL			
♣ Add •  Edt 🏢 Delete 🛧	4 X Ba th	เป	
No. 1 Address	- or	Prescription	F
NO ADDRESS	-44Ction)	Description	
🔂 Add A	VCL	×	
ACL Nov	er Solt Turoel List		
mul non	er [ppic_runio_cod		
	OK Carice	Help	
			war î

Une fois que l'ACL est créé, choisissez Add > Add ACE... afin d'ajouter une Entrée de contrôle d'accès (ACE).



Définissez l'ACE qui correspond au LAN derrière l'ASA. Dans ce cas, le réseau est 10.0.1.0/24.

a.

Cliquez sur la case d'option Permit.

b.

Choisissez l'adresse réseau avec le masque 10.0.1.0/24.

c.

(Facultatif) Fournissez une description.

d.

Click OK.

💼 AEL Manager				
Standard ACL Extended AC	1			
🗣 Add 👻 🖬 Edt 📫 D	belete + - € X Ra	60		
	are fatter f	Party interes		
Solt_Turnel_List	100 AC000	Description		
	standd ACE			×
	Action: @ Permit C De	any		
	Address: 10.0.1.0/24			
	Description:			
	The Corporate network behin	d the ASA		
				_
		OK Cancel	Help	
			· ·	

Cliquez sur OK afin de quitter l'ACL Manager.

ACL Manager					
Observational ArCI. Longitudes	a secol				
standard Act.   Extend	ied ACL				
🜩 Add 🔹 💽 Edit	T Delete	4 X	un 111 -		
No	Address	Action		Description	
E Split_Tunnel_List					
1 12,2 10.0.1	.0/24	🥜 Permit	The Corporate	e network behind th	e ASA
			COX /	Cancel	Hain

Assurez-vous que l'ACL que vous venez de créer est sélectionné pour la liste Split Tunnel Network List.

5	General General Servers Advanced - E Browser Prozy B SS, VPN Clerk - Roser / Lerk	hivalleyvpn         Spik tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The security appliance makes spik 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: I
	-Clent Access Rule -Clent Pressal -Hardware Clent	Network List: Drherk Spik_Tunnel_List.  Manage Intercept DHCP Config Spik_Tunnel_List DHCP Intercept lets Microsoft XP clients use spik tunneling with the security appliance. For Windows clients prior to XP, DHCP Intercept provides the domain name and subnet mask.

Cliquez sur OK afin de retourner à la configuration de la stratégie de groupe.

٠

General Servers Advanced	Split tunneling network lists distinguish networks that require traffic to go through the require tunneling. The security appliance makes split tunneling decisions on the basis ACL that consists of list of addresses on the private network.	e tunnel and those that do no of a network list, which is an
- E Browser Proxy	DNS Names: 🗁 Inherit	
⊕-SSL VPN Clent ⊕-IPsec Clent	Policy: Tunnel Network List Below	*
	NetworkList: Therit Splk_Tunnel_List	* Manage
	Intercept DHCP Configuration Message from Micosoft Clients	
	DHCP Intercept lets Microsoft XP clients use split tunneling with the security applian prior to XP, DHCP Intercept provides the domain name and subnet mask.	ce. For Windows clients
	Intercept: 🖓 Inherit - C Vice - C Vice	
	Subnet Mesk (Optional): 0.0.0.0	÷

Cliquez sur Apply puis sur Send (s'il y a lieu) afin d'envoyer les commandes à l'ASA.

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

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

Name	Туре	Tunneling Protocol	
fltGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webvpn	N/A
efaultgroup	Internal	InherRed	N(A
ivalleyvpn	Internal	svc,IPSec	N/A

Configurer ASA 7.x et ultérieures via l'interface de ligne de commande (CLI)

Au lieu d'utiliser l'ASDM, vous pouvez compléter ces étapes dans l'interface de ligne de commande CLI d'ASA afin d'autoriser la transmission tunnel partagée sur ASA :



**Remarque** : la configuration CLI Split Tunneling est la même pour ASA 7.x et 8.x.

Passez en mode de configuration.

<#root>

٠

ciscoasa>

#### enable

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

configure terminal

ciscoasa(config)#

Créez la liste d'accès qui définit le réseau derrière 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

Entrez le mode de configuration Group Policy pour la stratégie que vous souhaitez modifier.

<#root>

•

ciscoasa(config)#

group-policy hillvalleyvpn attributes

ciscoasa(config-group-policy)#

Spécifiez la stratégie de transmission tunnel partagée. Dans ce cas, la stratégie est tunnelspecified.

<#root>

•

ciscoasa(config-group-policy)#

split-tunnel-policy tunnelspecified

Spécifiez la liste d'accès de transmission tunnel partagée. Dans ce cas, la liste est Split\_Tunnel\_List.

<#root>

•

•

ciscoasa(config-group-policy)#

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

Émettez la commande suivante :

<#root>

### ciscoasa(config)#

tunnel-group hillvalleyvpn general-attributes

Associez la stratégie de groupe au groupe de tunnels

<#root>

•

ciscoasa(config-tunnel-ipsec)#

default-group-policy hillvalleyvpn

Quittez les deux modes de configuration.

<#root>

٠

ciscoasa(config-group-policy)#

exit

ciscoasa(config)#

exit

ciscoasa#

٠

Sauvegardez la configuration dans une mémoire vive non volatile (NVRAM) et appuyez Enter lorsqu'on vous invite à spécifier le nom de fichier source.

<#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#

Configurer PIX 6.x via l'interface de ligne de commande (CLI)

Procédez comme suit :

٠

Créez la liste d'accès qui définit le réseau derrière PIX.

<#root>

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

• Créez un groupe vpn vpn3000 et spécifiez l'ACL de transmission tunnel partagée pour ce groupe comme illustré :

<#root>

PIX(config)#

vpngroup vpn3000 split-tunnel Split\_Tunnel\_List



**Remarque** : référez-vous à <u>Cisco Secure PIX Firewall 6.x et Cisco VPN Client 3.5 pour Windows avec authentification RADIUS</u> <u>IAS Microsoft Windows 2000 et 2003</u> pour plus d'informations sur la configuration VPN d'accès à distance pour PIX 6.x.

Vérifier

Exécutez les étapes décrites dans ces parties afin de vérifier votre configuration.

Se connecter avec le client VPN

Afficher le journal du client VPN

Tester l'accès local au LAN avec un ping

Se connecter avec le client VPN

•

Connectez votre client VPN au concentrateur VPN afin de vérifier votre configuration.

- 0 × VPN Client - Version 4.0.5 (Rel) Connection Entries Status Certificates Log Options Help Import Connect New Modify **Connection Entries** Certificates Log Host Transport **Connection Entry** 4 IPSec/UDP 172.221.160 hilvaleyvpn 4

Choisissez votre entrée de connexion dans la liste et cliquez sur Connect.

Entrez dans vos informations d'identification.

👌 VPN Client   U	er Authen	tication fo	or "hillvalley	yvpn"	×
Cisco Systems	<u>U</u> sername: <u>P</u> assword:	marty	OK		Cancel

Choisissez Status > Statistics... afin d'afficher la fenêtre de détails de tunnel où vous pouvez inspecter les conditions particulières du tunnel et consulter le flux du trafic.

•

•

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

Accédez à l'onglet Route Details pour afficher les routes que le client VPN sécurise vers ASA.

Dans cet exemple, le client VPN sécurise l'accès à 10.0.1.0/24, tandis que tout autre trafic n'est pas crypté et n'est pas envoyé à travers le tunnel.

👌 VPN Client   Sta	tistics			x
Tunnel Details R	oute Details Firewal			
Local LAN Routes	1	Secured Routes		
Network	Subnet Mask	Network	Subnet Mask	
		10.0.1.0	255.255.255.0	

Afficher le journal du client VPN

Quand vous examinez le journal du client VPN, vous pouvez déterminer si le paramètre qui spécifie la transmission tunnel partagée est défini. Afin d'afficher le journal, accédez à l'onglet Log dans le client VPN. Cliquez alors sur **Log Settings afin d'ajuster ce qui est enregistré.** Dans cet exemple, IKE est défini sur **3 - High** tandis que tous les autres éléments du journal sont définis sur **1 -** Low.

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

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 14:20:14.208 07/27/06 Sev=Info/5 25 IKE/0x63000010 MODE\_CFG\_REPLY: Attribute = INTERNAL\_IPV4\_NETMASK: , value = 255.255.255.0 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x630000D 26 MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_SAVEPWD: , value = 0x00000000 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x630000D 27 MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_PFS: , value = 0x00000000 28 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300000E MODE\_CFG\_REPLY: Attribute = APPLICATION\_VERSION, value = Cisco Systems, Inc ASA5510 Version 7.2(1) built by root on Wed 31-May-06 14:45 !--- Split tunneling is permitted and the remote LAN is defined. 29 14:20:14.238 07/27/06 Sev=Info/5 IKE/0x630000D MODE\_CFG\_REPLY: Attribute = MODECFG\_UNITY\_SPLIT\_INCLUDE (# of split\_nets), value = 0x000000130 14:20:14.238 07/27/06 Sev=Info/5 IKE/0x6300000F SPLIT\_NET #1 subnet = 10.0.1.0mask = 255.255.255.0 protocol = 0src port = 0dest port=0 !--- Output is supressed.

Tester l'accès local au LAN avec un ping

Un moyen supplémentaire de tester si le client VPN est configuré pour la transmission tunnel partagée, tout en étant relié par tunnel à ASA, est d'utiliser la commande ping sur la ligne de commande Windows. Le réseau local du client VPN est 192.168.0.0/24 et un autre hôte est présent sur le réseau avec une adresse IP 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>
```

#### Dépannage

Limitation avec le nombre d'entrées dans une ACL de tunnel partagé

Il existe une restriction avec le nombre d'entrées dans une liste de contrôle d'accès utilisée pour le split tunnel. Il est recommandé de ne pas utiliser plus de 50-60 entrées ACE pour une fonctionnalité satisfaisante. Il est conseillé de mettre en oeuvre la fonction de création de sousréseaux pour couvrir une plage d'adresses IP.

Informations connexes

- Exemple de configuration de PIX/ASA 7.x comme serveur de VPN distant avec l'ASDM
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- <u>Assistance technique de Cisco et téléchargements</u>

## À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.