ASAでのVPNクライアントのスプリットトンネ リングの設定

内容 <u>はじめに</u> 前提条件 要件 <u>使用するコンポーネント</u> <u>ネットワーク図</u> 関連製品 表記法 <u>背景説明</u> ASA にスプリット トンネリングを設定する Adaptive Security Device Manager (ASDM) 5.x で ASA 7.x を設定する <u>ASDM6.xによるASA 8.xの設定</u> <u>CLI で ASA 7.x 以降を設定する</u> <u>CLI で PIX 6.x を設定する</u> 確認 <u>VPN Client で接続する</u> <u>VPN Client ログの表示</u> Ping でローカル LAN アクセスをテストする トラブルシュート スプリット トンネル ACL でのエントリの数に関する制限 関連情報

はじめに

このドキュメントでは、Cisco ASA 5500シリーズセキュリティアプライアンスにトンネリングし ながら、VPN Clientがインターネットにアクセスできるようにするプロセスについて説明します 。

前提条件

要件

このドキュメントは、動作しているリモート アクセス VPN 設定が ASA にすでに存在しているこ とを前提としています。未設定の場合は、『<u>ASDMを使用したリモートVPNサーバとしての</u> <u>PIX/ASA 7.xの設定例</u>』を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ・ Cisco ASA 5500 シリーズ セキュリティ アプライアンス ソフトウェア バージョン 7.x 以降
- ・ Cisco Systems VPN Client バージョン 4.0.5
- Adaptive Security Device Manager (ASDM)



注:このドキュメントには、Cisco VPN Client 3.xと互換性のあるPIX 6.x CLI設定も含まれています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

ネットワーク図

VPN Client は一般的な SOHO ネットワーク上にあり、インターネット経由で本社に接続しています。



ネットワーク図

関連製品

この設定は、Cisco PIX 500 シリーズ セキュリティ アプライアンス ソフトウェア バージョン 7.x にも使用できます。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

このドキュメントでは、VPN Client が Cisco 適応型セキュリティ アプライアンス (ASA) 5500 シリーズ セキュリティ アプライアンスにトンネリングされている間に、それにインターネットへ のアクセスを許可する方法のステップごとの説明を提供します。この設定により、VPN Client は IPSec を使用した企業リソースへのセキュアなアクセスと、セキュリティ保護されていないイン ターネット アクセスの両方を実現できます。



注:フルトンネリングでは、インターネットと社内LANの両方へのデバイスアクセスが同 時にイネーブルにされないため、最も安全な設定と見なされます。フル トンネリングと スプリット トンネリングの折衷案として、VPN Client にローカル LAN アクセスだけを許 可することができます。詳細は、『<u>PIX/ASA 7.x:VPNクライアントでローカルLANアクセ</u> <u>スを許可するための設定例</u>』を参照してください。

VPN Client と ASA の基本的な接続シナリオでは、宛先に関係なく、VPN Client からのすべての トラフィックは暗号化されて ASA に送信されます。設定とサポートされるユーザ数によっては、 このような設定は帯域幅を大量に消費する可能性があります。スプリット トンネリングでは、ト ンネル接続で、企業ネットワーク向けトラフィックの送信だけがユーザに許可されるため、この 問題の軽減に役立ちます。インスタント メッセージ、電子メール、または通常の Web 閲覧など 、その他すべてのトラフィックは、VPN Client のローカル LAN 経由でインターネットに送出さ れます。

ASA にスプリット トンネリングを設定する

Adaptive Security Device Manager (ASDM) 5.x で ASA 7.x を設定する

次の手順を実施して、グループのユーザにスプリット トンネリングを許可するトンネル グループ を設定します。

1. [Configuration] > [VPN] > [General] > [Group Policy] の順に選択し、ローカル LAN アクセス を有効にするグループ ポリシーを選択します。次に [Edit] をクリックします。



2. [Client Configuration] タブに移動します。

General 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 Parameter	s Microsoft Client Parameters
Banner:	Edit Banner
Default Domain:	I Inherit
Collin Townel DNC Marrier (annual delivity de	
Split Tunnel DNS Names (space delimited):	l≪ innerit
Split Tunnel Policy:	V Inherit
Split Tunnel Network List:	Manage
Address pools	
Available Pools	Assigned Pools (up to 6 entries)
	Add>>
	<sremove< td=""></sremove<>

3. Split Tunnel PolicyのInheritボックスのチェックマークを外し、Tunnel Network List Belowを選択する。

Name: pillvalleyvpn sneral PSec Client Configuration Client Firewall Hardware Client NAC WebVPN Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. General Client Parameters Clisco Client Parameters Microsoft Client Parameters Banner: Inherit Edit Banner	Name: pillvalleyvpn sneral PSec Client Configuration Client Firewall Hardware Client NAC WebVPN Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. General Client Parameters Clisco Client Parameters Microsoft Client Parameters Banner: 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 pools Address Inherit Address Address Address pools Address Address	Name: pillvalleyvpn eneral 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 Clicco Client Parameters Microsoft Client Parameters Banner: Imment Edit Banner Default Domain: Imment Edit Banner Split Tunnel DNS Names (space delimited): Imment Tunnel All Networks Split Tunnel Policy: Inherit Tunnel All Networks Split Tunnel Network List: Imment Exclude Network List Below Address pools Address Address Imment Address Address Address Address Address			
Inversion 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 Banner Default Domain: Inherit Edit Banner Split Tunnel DNS Names (space definited): Inherit Tunnel All Networks Split Tunnel Policy: Inherit Tunnel All Networks Split Tunnel Network List: Inherit Tunnel All Network List Below Address pools Imherit Address Address	eneral PSec Client Configuration Client Firewall Hardware Client NAC WebVPN Check an Inherit checkbox to let the corresponding setting take its value from the defauit group policy. General Client Parameters Clisco Client Parameters Microsoft Client Parameters Banner: Inherit Edit Banner	Interval PSec Client Configuration Client Firewall Hardware Client NAC WebVPN Check an Inherit checkbox to let the corresponding setting take its value from the defauit group policy. General Client Parameters Clisco Client Parameters Microsoft Client Parameters Banner: Inherit Edit Banner Defauit 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 Tunnel All Network List Below Address pools Address pools Address Inherit Address Address	Name: hilvalleyvpn		
Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. General Client Parameters Banner: Default Domain: Default Domain: Split Tunnel DNS Names (space delimited): Split Tunnel DNS Names (space delimited): Split Tunnel Policy: Split Tunnel Network List: Vinnerit Address pools Address pool	Address pools Address Address pools Address	Address pools Address Address pools Address	energy [IPSec Client Configuration Client Firework	Hardwara Client	
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 Tunnel Network List Below Address pools Address Address Image: Address Address	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 Tunnel All Networks List Below Address pools Address Address Inherit Address Address Address pools Inherit Address Inherit Address Address	Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. General Client Parameters Clisco Client Parameters Banner: Inherit Default Domain: Inherit Split Tunnel DNS Names (space definited): Inherit Split Tunnel Policy: Inherit Tunnel All Networks Split Tunnel Network List: Address pools Inherit Address pools Inherit Address pools	eneral PSec Clerk configuration Clerk Preval	I Hardware Cieni	
General Client Parameters Cisco Client Parameters Microsoft Client Parameters Banner: Inherit Edit Banner Default Domain: Inherit Inherit Spit Tunnel DNS Names (space delimited): Inherit Inherit Spit Tunnel Policy: Inherit Inherit Spit Tunnel Network List: Inherit Inherit Address pools Address Address Inherit Address Address Address pools Address Address	General Client Parameters Cisco Client Parameters Banner: Inherit Default Domain: Inherit Spit Tunnel DNS Names (space delimited): Inherit Spit Tunnel Policy: Inherit Spit Tunnel Network List: Inherit Kddress pools Inherit Imherit Address Address pools	General Client Parameters Cisco Client Parameters Microsoft Client Parameters Banner: Inherit Edt Banner Default Domain: Inherit Edt Banner Spit Tunnel DNS Names (space delimited): Inherit Tunnel All Networks Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Tunnel All Network List Below Address pools Address Pools (up to 6 entries) Address Address pools Address Address Address	Check an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.
Centeral Client Parameters Microsoft Client Parameters Banner: Inherit Default Domain: Inherit Spit Tunnel DNS Names (space delimited): Inherit Spit Tunnel Policy: Inherit Spit Tunnel Policy: Inherit Spit Tunnel Network List: Inherit Address pools Address Address pools Address Address Address	Banner: Inherit Edit Banner Default Domain: Inherit Edit Banner Spit Tunnel DNS Names (space delimited): Inherit Inherit Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Tunnel All Networks Address pools Address Address Inherit Address Address Address pools Address	Banner: Inherit Edit Banner Default Domain: Inherit Edit Banner Spit Tunnel DNS Names (space delimited): Inherit Inherit Spit Tunnel Policy: Inherit Inherit Spit Tunnel Network List: Inherit Inherit Address pools Address Address Inherit Address Assigned Pools (up to 6 entries)		1	
Banner: Inherit Default Domain: Inherit Spit Tunnel DNS Names (space definited): Inherit Spit Tunnel Policy: Inherit Spit Tunnel Network List: Inherit Spit Tunnel Network List: Inherit Address pools Address pools Inherit Address pools Address pools Address Inherit Address pools	Banner: Inherit Edit Banner Default Domain: Inherit Inherit Spit Tunnel DNS Names (space definited): Inherit Inherit Spit Tunnel Policy: Inherit Iunnel All Networks Spit Tunnel Network List Inherit Iunnel Network List Below Address pools Address pools Address Inherit Available Pools Address Address pools Address Address	Banner: Inherit Default Domain: Inherit Spit Tunnel DNS Names (space delimited): Inherit Spit Tunnel Policy: Inherit Spit Tunnel Network List: Inherit Tunnel All Networks List Tunnel All Networks List Below Address pools Inherit Address pools Address Inherit Address Address pools Inherit	General Client Parameters Cisco Client Parameter	s Microsoft Client	Parameters
Default Domain: Default Domain: Split Tunnel DNS Names (space delimited): Inherit Split Tunnel Policy: Inherit Tunnel All Networks Tunnel All Network List: Vertices pools Address pools	Default Domain: Default Domain: Spit Tunnel DNS Names (space delimited): Inherit Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Address pools Address pools Inherit Address pools Image: Address pools Address pools	Default Domain: Default Domain: Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Address pools Inherit Address pools Inherit Address pools Address pools Inherit Address pools Address pools Inherit Address pools Address pools Inherit Address pools Address pools Inherit Address pools Address pools Inherit	D	The second	Cult Downey
Default Domain: Inherit Split Tunnel DNS Names (space delimited): Inherit Split Tunnel Policy: Inherit Split Tunnel Network List: Inherit Split Tunnel Network List: Inherit Address pools Address pools (up to 6 entries) Address Address	Default Domain: Inherit Spit Tunnel DNS Names (space delimited): Inherit Spit Tunnel Policy: Inherit Spit Tunnel Network List: Inherit Tunnel All Networks Tunnel Network List: Address pools Inherit Address pools	Default Domain: Inherit Spit Tunnel DNS Names (space delimited): Inherit Spit Tunnel Policy: Inherit Spit Tunnel Network List: Inherit Spit Tunnel Network List: Inherit Address pools Address pools Imherit Address pools Imherit Address pools Address pools Imherit Address pools Address pools Imherit Address pools Imherit Address pools Imherit Address pools Imherit Address Address Address Imherit Imherit Address Imherit I	Banner:	I¥ innent	Cat Danner
Split Tunnel DNS Names (space delimited): Split Tunnel Policy: Inherit Tunnel All Networks Tunnel Network List: Inherit Address pools Address </td <td>Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Address pools Address pools</td> <td>Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Inherit Spit Tunnel Network List: Inherit Tunnel Network List: Inherit Address pools Address pools Address pools Address pools Address pools Address pools Address Address Address Address Address</td> <td>Default Domain:</td> <td>🔽 Inherit</td> <td></td>	Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Address pools	Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Inherit Spit Tunnel Network List: Inherit Tunnel Network List: Inherit Address pools Address pools Address pools Address pools Address pools Address pools Address Address Address Address Address	Default Domain:	🔽 Inherit	
Spit Tunnel DNS Names (space definited): Inherit Spit Tunnel Policy: Inherit Spit Tunnel Network List: Spit Tunnel Network List: Address pools Address	Split Tunnel DNS Names (space delimited): Split Tunnel Policy: Inherit Tunnel All Networks Tunnel All Network List Split Tunnel Network List Inherit Address pools Address pools Addiss Addiss Addiss	Spit Tunnel DNS Names (space delimited): Inherit Spit Tunnel Policy: Inherit Tunnel All Networks Tunnel Network List Below Address pools Address Image: Address Image: Address Image: Address Image: Address Image: Address			1
Spit Tunnel Policy: Inherit Tunnel All Networks Tunnel All Networks Tunnel All Networks Tunnel All Networks Tunnel Network List Below Address pools	Spit Tunnel Policy: Inherit Spit Tunnel Network List: Spit Tunnel Network List: Address pools	Spit Tunnel Policy: Inherit Tunnel All Networks Tunnel All Networks Tunnel Network List Address pools Address pools Address Pools (up to 6 entries) Address Address Address Address Address Address Address Address Address Address Address Address Address Address Address A	Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Imherit Tunnel Network List Below Address pools Address pools Imherit Address pools Address pools Address pools Imherit Address (up to 6 entries) Image: Address (up to 6 entries)	Spit Tunnel Policy: Spit Tunnel Network List: Address pools Address Address Address A	Spit Tunnel Policy: Inherit Tunnel All Networks Tunnel All Networks Tunnel Network List Below Address pools A			
Spit Tunnel Network List Address pools Address Address Address Address Address Address Address	Spit Tunnel Network List: Image:	Split Tunnel Network List Immerit Tunnel All Network List Below Address pools Exclude Network List Below Immerit Avsitable Pools Assigned Pools (up to 6 entries) Address Address Immerit Address Address Address Address Address	Split Tunnel Policy:	🗌 Inherit	Tunnel All Networks
Spit Tunnel Network List Immerit Tunnel Network List Below Address pools ✓ Inherit Avaïable Pools Add>> Add>> Add>> Add>> Add>>	Split Tunnel Network List Immerit Immerit Exclude Network List Below Address pools Immerit Assigned Pools (up to 6 entries) Address Address Address Address pools Immerit Assigned Pools (up to 6 entries) Immerit Address Immerit Address Address Immerit Immerit Address Immerit Immerit Address Immerit Immerit Address Immerit	Spit Tunnel Network List Immerit Immerit Exclude Network List Below Address pools Immerit Assigned Pools (up to 6 entries) Add>> Add>> Assigned Pools (up to 6 entries) Immerit Add>> Immerit Add>> Add>> Immerit			Tunnel All Networks
Address pools Address pools Available Pools Available Pools Add>> Add>> <	Address pools Address pools Available Pools Add>> Add>> Add>>	Address pools Address pools Image: Address pools Available Pools Adds> Adds>	Split Tunnel Network List:	🔽 Inherit	Exclude Network List Below
Address pools Image: Address pools Available Pools Assigned Pools (up to 6 entries) Address Address Address Assigned Pools (up to 6 entries) Address Address	Address pools Inherit Avaïable Pools Assigned Pools (up to 6 entries) Add>> Add>> Add>> Add>>	Address pools Inherit Avaïable Pools Assigned Pools (up to 6 entries) Address Address Address Address			
Available Pools Add>> Ad	Available Pools Add>> Ad	Avaïable Pools Add>> Add	Address pools		
Add>> Add>> Add>>	Add>> Add>> Add>>	Add>> Add>> Add>	Minherit		Residented Deale (under Combine)
Add>> < <remove< td=""><td>Add>> <<remove< td=""><td>Add>> <<remove< td=""><td>Available Pools</td><td></td><td>Assigned Pools (up to 6 entries)</td></remove<></td></remove<></td></remove<>	Add>> < <remove< td=""><td>Add>> <<remove< td=""><td>Available Pools</td><td></td><td>Assigned Pools (up to 6 entries)</td></remove<></td></remove<>	Add>> < <remove< td=""><td>Available Pools</td><td></td><td>Assigned Pools (up to 6 entries)</td></remove<>	Available Pools		Assigned Pools (up to 6 entries)
<	<-Remove	<#Remove		Adde>	
				«Remove	i
					1

[Split Tunnel Network List] の [Inherit] ボックスをオフにし、[Manage] をクリックして ACL Manager を起動します。

nternal Group Policy: hillvalley v pn		
Name: hilvalleyvpn		
eneral IPSec Client Configuration Client Firewall	Hardware Client	
andrai (17360) andra den ingen andra (Calori, Filleyrai)	Thank ware client	
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:	I∕ Inherit	J
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Split Tunnel Policy:	Inherit	Tunnel Network List Below
Split Tunnel Network List:	🗖 İnherit	None Manage
Address pools		
🔽 Inherit		
Available Pools		Assigned Pools (up to 6 entries)
	Add≽⊳	
	< <remove< td=""><td>1</td></remove<>	1

[ACL Manager] で、[Add] > [Add ACL...] の順に選択して、新しいアクセス リストを作成します。

ACL Manager					L (X
Standard AG. Extended	ACL.					
🔶 Add 🕒 📰 0.0. 🏢	Dektr 🕐	4 美脂酸	-			
Add ACL	dress	Action	Description			
⊕LASTACEL №						
全 insert ● insert Attor						
	1					

ACL に名前を指定して [OK] をクリックします。

ACL Manager					2
◆ Add → III Estim III Distric +	F X % @ -				
No Address	Adlon	Description			
	AGL Henret: Spill_1 OK	umel_List	Holp		
- Brite Prove Discovery		2			~
Huld Prover Deligneen	<u>s</u> m	ide a contes	+de		×
	OK.	Cancel	Hep		

ACLを作成したら、Add > Add ACEの順に選択します。.コマンドを入力して、アクセスコントロールエントリ(ACE)を追加します。



ASA の背後にある LAN に対応する ACE を定義します。この場合、ネットワークは 10.0.1.0/24 です。

a.

[Permit] を選択します。

b.

[IP Address] で [10.0.1.0] を選択します。

c.

[Netmask] で [255.255.255.0] を選択します。

d.

(任意)説明を入力します。

>OKをクリックします。

No	Address	Action	Description			
Splt_Turnel_List						
	IN Add ALL				<u>×</u>	
	Action					
	Action	V Poort T				
	HordAleth	work				
	IP Add	na: 00.1.0			<u> </u>	
	Netwo	E 255.255.255.0			¥	
	Description					
	The corpor	ste network behind the A	ISA.			
		OK .	Canoti	Holp		
Lie Flow Disgram-						
		3- <u>I</u>	inter a constant	10		

[OK] をクリックして [ACL Manager] を終了します。

•

e.



Split Tunnel Network List で、作成した ACL が選択されていることを確認します。

Nome: hillvalleyvpn		
eneral IPSec Client Configuration Client Firewall	Hardware Client	NAC WebVPN
Check an inherit checkbox to let the corresponding a	setting take its valu	e from the default group policy.
General Client Parameters Cisco Client Parameters	Microsoft Client	Parametora
Barner.	M Inhert	EDF. E orvver
Default Domain:	Intert	
Split Tunnel DNS Names (space delimited):	🖂 inherit	
	_	
Split Tunnel Policy:	I inherit	Turnel Network List Below
	E unua	Total Description of the second
Spit Furner vervronk List.	1 Innerit	None
Address pools		Splt_Tunnel_List
🔽 interit		cutside_cryptome5%
Avoiblie Pools		Assigned Pools (up to 6 entries)
	Editor.	
	20165	
	collemane]

[OK] をクリックして、グループ ポリシー設定に戻ります。

Name: PHralleyrypn General PSac Clerit. Configuration Clerit Firewall Hardware Clerit NAC WebVPN Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. Clerit Parameters Cloco Clerit Parameters Microsoft Clerit Parameters General Clerit Parameters Cloco Clerit Parameters Microsoft Clerit Parameters Edit Porner. Banner: Imherit Edit Porner. Edit Porner. Default Domain: Imherit Imherit Edit Porner. Split Tunnel DNS Names (space definited): Imherit Tunnel Network List Imherit Tunnel Network List Below V Split Tunnel Network List: Imherit Tunnel Network List Menage Address pools Menage	Name: Name: <td< th=""><th>it Internal Group Policy: hillvalleyvpn</th><th></th><th></th><th>×</th></td<>	it Internal Group Policy: hillvalleyvpn			×
General IPSec Clerit Configuration Clerit Firewall Hardware Clerit NAC Web/PN Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. General Clerit Forometers Cloco Clerit Parameters Microsoft Clerit Parameters General Clerit Parameters Cloco Clerit Parameters Microsoft Clerit Parameters Edit Foromet. Banner: Imherit Edit Foromet. Edit Foromet. Default Domain Imherit Edit Foromet. Edit Foromet. Spit Tunnel DNS Names (space delimited): Imherit Tunnel Network List Below Imherit Spit Tunnel Network List Imherit Tunnel Network List Below Imherit Address pools Imherit Imherit Manage	General IPSec Clert Configuration Clert Firewail Hardware Clert NAC WebVPN Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. Ceneral Clert Parameters Cisco Clert Parameters Microsoft Clert Parameters Banner: IP Inherit Edit Former Default Domain: IP Inherit Edit Former Split Tunnel DNS Names (space delivited): IP Inherit Tunnel Network List Below IP Split Tunnel Network List: Inherit Split Tunnel Network List: Menage Address pools	Nome: hitvalleyvpn			
Check an Inhert checkbox to let the corresponding setting take its value from the default group policy. General Client Parameters Cloco Client Parameters Microsoft Client Parameters Banner: Default Donvaix Finhert Spit Tunnel DNS Names (space definited): Spit Tunnel DNS Names (space definited): Spit Tunnel Policy: Spit Tunnel Network List: Inhert Address packs	Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. General Client Parameters Banner: Default Donveix Default Donveix Spit Tunnel DNS Names (space delimited): Inherit Tunnel Network List: Inherit Spit Tunnel Network List:	General IPSec Client Configuration Client Firewall	Hardware Client	NAC WEDVPN	
General Clent Parameters Cloco Clent Parameters Microsoft Clent Parameters Banner: Imment Enhant Detsuit Donver: Imment Imment Spit Tunnel DNS Names (space delimited): Imment Tunnel Network List Below Spit Tunnel Policy: Imment Tunnel Network List Below Imment Spit Tunnel Network List: Imment Manage Address pools Imment Manage	General Clent Parameters Cloco Clent Parameters Banner: Image: Clent Parameters Detsuit Donvan: Image: Clent Parameters Spit Tunnel DNS Names (space delimited): Image: Clent Parameters Spit Tunnel Policy: Image: Clent Parameters Spit Tunnel Network List: Image: Clent Parameters	Check an Inherit checkbox to let the corresponding	setting take its valu	e from the default group policy.	
Barner: Image: Im	Barner: Image: Im	General Client Parameters Cisco Client Parameter	s Microsoft Client	Parameters	
Default Donvair: Immerit Spit Tunnel DNS Names (space delimited): Immerit Spit Tunnel Policy: Immerit Spit Tunnel Network List: Immerit Spit Tunnel Network List: Immerit Address pools	Default Domain: Image: I	Barner:	🔽 inherit	Edt Eororer	
Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Spit Tunnel Network List: Address pools	Spit Tunnel DNS Names (space delimites): Spit Tunnel Policy: Spit Tunnel Network List: Address pools	Default Domain:	Interit		
Spit Tunnel Policy: Intert Tunnel Network List Below Spit Tunnel Network List: Manage Address pools	Spit Tunnel Network List Spit Tunnel Network List Manage Address pools	Split Tunnel DNS Names (space delimited):	🖓 inherit		
Spit Tunnel Network List: Inhert Spit Tunnel L Manage	Spit Tunnel Network List: Inhert Spit Tunnel L. Manage Address pools	Split Tunnel Policy:	□ interit	Tunnel Network List Below	
-Address pools	Address pools	Split Tunnel Network List:	inhert	Spit_Tunnet_L * Manage	
		Address pools			

[Apply] をクリックしてから [Send](必要な場合)をクリックして、コマンドを ASA に送信します。



ASDM 6.xによるASA 8.xの設定

•

次の手順を実施して、グループのユーザにスプリット トンネリングを許可するトンネル グループを設定します。

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択し、ローカル LAN アクセスを有効 にするグループ ポリシーを選択します。次に [Edit] をクリックします。

nfiguration > Remote Access VPN > N	etwork (Client) Acces	ss > Group Policies	
Manage VPN group policies. A VPN group p externally on a RADIUS/LDAP server. The	plicy is a collection of us group policy information	er-oriented attribute/value pairs that may is referenced by VPN bunnel groups and u	be stored inte ser accounts.
🗣 Add 🔹 📝 Edit 📋 Delete			
Name	Type	Tunneling Protocol	
DfltGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webvpn	N/A
	Redenand I	Televited of the second s	
Defaultgroup	Incernal	unnerroed	i≃ N/A

🙀 Edit Internal Group Policy:	: hivalleyvpn	
General Servers Advanced - 201: Turneling - 12: Browser Procy B-551, VPN Client	Split tunneling network lats distinguish networks that require traffic to go through the to require tunneling. The security applance makes split tunneling decisions on the basis of ACL that consists of lat of addresses on the private network.	unnel and those that do no a network list, which is an
E-IPsec Client	Policy: 🖓 Inherit	-
Clent Access Rule Clent Firewal	Network List: 🖓 [inherit]	• Mariage
There was a case of	Intercept DHCP Configuration Message from Micosoft Clients	
	Intercept: IP Inherit C Yos C No	
	Subnet Plesk (Optional): 0.0.0.0	<u>×</u>
ŭ D		

[Split Tunnel Policy] の [Inherit] ボックスをオフにし、[Tunnel Network List Below] を選択します。

Edit Internal Group Policy:	hivalleyvpn		
General General Advanced	Split tunneling network lists distingu- require tunneling. The security app ACL that consists of list of address	ish networks that require traffic to go liance makes split turneling decisions o as on the private network.	through the tunnel and those that do no n the basis of a network list, which is an
	DNS Names: 🔽 Inherit		
⊕-53L VPN Client ⊖ (Prec Client	Policy: Tinherit Tunne	Network List Below	*
- Clerit Access Rule - Clerit Pirewal	NetworkList: IV Inherit	Al hietworks Network List Below	Managa
- Hardware Clenc	Intercept DHCP Configuratio	h Message from Micosoft Clients	\$
	Intercept: $\overline{\varphi}$ inherit $C^{\gamma_{(2)}}$	C fo	

[Split Tunnel Network List] の [Inherit] ボックスをオフにし、[Manage] をクリックして ACL Manager を起動します。

だ Edit Internal Group Policy	i hiralleyvpn
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.
-E provise Prany	DNS Names: 🖵 Inherit
B-Pise: Client	Policy: Dhherit Turnel Nebeork List Beices
- Client Access Rule - Client Firewall	Network List: Note
flandware Clienc	Intercept DHCP Configuration Message from Micosoft Clients (*)
	DHCP Intercept lets Microsoft XP clients use split tunneling with the security appliance. For Windows clients prior to XP, DHCP Intercept provides the domain name and subnet mask.
	Intercept: 🔽 Inherit C Yes C No
	Subret Hark (Options): 0.0.0.0

[ACL Manager] で、[Add] > [Add ACL...] の順に選択して、新しいアクセス リストを作成します。

ACL	Manager				
Stand	dard ACL Extended	ACL A			
* A	Add 🔸 📓 Edit 👔	Delete 1	► 4 % h	18. T	
4	Add ACL		Action	Description	
+	Add ACE				
	Insert				
Ŧ	Insert After				

ACL の名前を指定して [OK] をクリックします。

•

💼 ACL Manager		_				
Standard ACL Extended ACL	ù.					
♣ Add • III Edt 🏦 D	siete 🕂 🛧 🗣	X Ba	183			
No 1 Addre		Action		Description	F	
	🚮 Add ACL	1-21-2		×		
	ACL Name:	Split_Tunnel_L	list			
	OK	Ca	ncel	Help		
					-	
		2		i and l	11ala	- î

ACL が作成された後、[Add] > [Add ACE...] を選択して、アクセス コントロール エントリ(ACE)を追加します。



ASA の背後にある LAN に対応する ACE を定義します。この場合、ネットワークは 10.0.1.0/24 です。

a.

[Permit] オプション ボタンをクリックします。

b.

マスク 10.0.1.0/24 のネットワーク アドレスを選択します。

c.

(任意)説明を入力します。

d.

[OK] をクリックします。

💼 ACL Manager					
Standard ACL Extended A	aj				
🗣 Add 🔹 🎬 Edt 🁔	Delete 🛧 🐇	Ra 65			
No Add	ess Action	1	Description		
Split_Tunnel_List					
	G Add ACE				xI
	Action: 1+ Permit (Deny			
	Address: [10.0.1.0/24				
	Description:				
	The Corporate network b	whind the ASA			
		or	Carcel	Halo [
			Carco,	nop	
		2542	Sec. 1	1 Inda	

[OK] をクリックして [ACL Manager] を終了します。

ACL Manager			- <u></u>		
Standard ACL Science	feed and 1				
Action of Net 1 Excent	ieu Act	- 1			
🏶 Add 🔹 🧭 Edit	🔟 Delete 🕈	÷ % 40			
No	Address	Action		Description	
E Split_Tunnel_List					
1 2 10.0.1	.0/24	🥜 Permit —	The Corporate	network behind	the ASA
1					
		K	OK)	Cancel	Help

Split Tunnel Network List で、作成した ACL が選択されていることを確認します。

Edit Internal Group Policy	hivalleyvpn
General Servers Advanced -IE Browser Proxy B-SS, VPN Client -IPsec Client	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. DNS Names: Image: Imag
Client Access Rule Client Pirewall	Network List: Dinherit Spit_Tunnel_List Manage
Hardware Client	Intercept DHCP Config Spit, Turnel 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: V Inherit C Yos C Ho

[OK] をクリックして、グループ ポリシー設定に戻ります。

•

•

General General Servers Advanced Soft Turneling E Drowser Proxy	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those require tunneling. The security applance makes split tunneling decisions on the basis of a network list, + ACL that consists of list of addresses on the private network. DNS Names: Image: The security application of the private network.	that do not which is an
19-55, VPN Clent 19-3Psec Clent	Policy: Inherit Tunnel Network List Below Network List: Inherit Solk_Tunnel List	tanage
	Intercept DHCP Configuration Message from Micosoft Clients	\$
	DHCP Intercept lets Microsoft XP clients use split tunneling with the security appliance. For Windows o prior to XP, DHCP Intercept provides the domain name and subnet mask.	lients.
	Intercept: 🔽 Inherit C Yes C No Submet Mark (Optional): [0.0.0.0	×

[Apply] をクリックしてから [Send](必要な場合)をクリックして、コマンドを ASA に送信します。

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

🗣 Add	τ.	📝 Edit	📋 Delete	
-------	----	--------	----------	--

Name	Туре	Tunneling Protocol	
DfltGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webypn	N/A
Defaultgroup	Internal	Inherited	N(A
hivalleyvpn	Internal	svc,IPSec	N/A
I			
	· · ·		
	- P	oply / Reset	

CLI で ASA 7.x 以降を設定する

ASDM を使用する代わりに、ASA CLI で次の手順を実行して、ASA のスプリット トンネリングを許可することもできます。



注:CLIスプリットトンネリングの設定は、ASA 7.xと8.xの両方で同じです。

コンフィギュレーション モードに切り替えます。

<#root>

ciscoasa>

enable

Password: ******* ciscoasa#

configure terminal

ciscoasa(config)#

ASA の背後にあるネットワークを定義するアクセス リストを作成します。

<#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

修正するポリシーのグループ ポリシー コンフィギュレーション モードに入ります。

<#root>

٠

ciscoasa(config)#

group-policy hillvalleyvpn attributes

ciscoasa(config-group-policy)#

スプリット トンネル ポリシーを指定します。この例では、ポリシーは tunnelspecified です。

<#root>

•

ciscoasa(config-group-policy)#

split-tunnel-policy tunnelspecified

スプリット トンネル アクセス リストを指定します。この例では、リストは Split_Tunnel_List です。

<#root>

٠

ciscoasa(config-group-policy)#

split-tunnel-network-list value Split_Tunnel_List

次のコマンドを実行します。

<#root>

ciscoasa(config)#

tunnel-group hillvalleyvpn general-attributes

グループ ポリシーとトンネル グループを関連付けます。

<#root>

٠

ciscoasa(config-tunnel-ipsec)#

default-group-policy hillvalleyvpn

2つのコンフィギュレーション モードを終了します。

<#root>

•

ciscoasa(config-group-policy)#

exit

ciscoasa(config)#

exit

ciscoasa#

•

この設定を不揮発性 RAM(NVRAM)に保存して、ソース ファイル名を指定するようにプロンプトが表示されたら、Enter キーを押します。

<#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#

CLI で PIX 6.x を設定する

次のステップを実行します。

•

PIX の背後にあるネットワークを定義するアクセス リストを作成します。

<#root>

• VPN グループ vpn3000 を作成して、次のようにスプリット トンネル ACL を指定します。

<#root>

PIX(config)#

vpngroup vpn3000 split-tunnel Split_Tunnel_List



注: PIX 6.xのリモートアクセスVPN設定の詳細は、『<u>Cisco Secure PIX Firewall 6.xおよびCisco VPN Client 3.5 for</u> <u>WindowsでMicrosoft Windows 2000/2003 IAS RADIUS認証を使用するための設定</u>』を参照してください。

確認

次に示すセクションの手順を実行して、設定を確認します。

<u>VPN Client で接続する</u>

<u>VPN Client ログの表示</u>

Ping でローカル LAN アクセスをテストする

VPN Client で接続する

•

•

•

VPN Client を VPN コンセントレータに接続して、設定を確認します。

リストから接続エントリを選択して [Connect] をクリックします。

🎍 VPN Client - Version 4.0.5 (Rel)		
Connection Entries Status Certificates Log Options	jelp	
Connector Entries Certificates Log	Delete	Cisco Systems
Connection Entry	Host	Tiansport .
hilvaleyvpn	172.22.1.160	IPSec/UDP

認証情報を入力してください。



[Status] > [Statistics...] の順に選択して、[Tunnel Details] ウィンドウを表示します。ここでトンネルの詳細を調べ、トラフィックの流れを確認できます。

	Tilewol.	
mation	Connection Information	6
10.0.1.50	Entry:	hillvalley2
172.22.1.160	Time:	0 day(s), 00:00.25
	Crypto	
D	Encryption:	168-bit 3-DES
1494	Authentication:	HMAC-SHA1
	Transport	
9	Transparent Tunneling	Inactive
0	Local LAN:	Disabled
0	Compression:	None
159		
		Reset
	mation 10.0.1.50 172.22.1.160 0 1494 9 0	mationConnection Information10.0.1.50Entry: Time:172.22.1.160Time:0Encryption: Authentication:1494Authentication:9Transport0Local LAN: Compression:159

VPN Client が ASA に対して保護しているルートを確認するには、[Route Details] タブに移動します。

この例では、VPN Client は 10.0.1.0/24 へのアクセスを保護していますが、一方で、他のすべてのトラフィックは暗号化さ れず、トンネルを経由しては送信されません。

ł	VPN Client Sta	tistics			×
	Tunnel Details	oute Details Firewa			
	Local LAN Routes	N.	Secured Routes		
	Network	Subnet Mask	Network	Subnet Mask	
			10.0.1.0	255.255.255.0	

VPN Client ログの表示

VPN Client ログを調査すると、スプリット トンネリングを指定するパラメータが設定されているかどうかを確認できます。ログ を表示するには、VPN Client の [Log] タブに移動します。その後、[Log Settings] をクリックして、記録される内容を調整します。 この例では、IKE は 3- High に設定されており、他のすべてのログ要素は 1 - Low に設定されています。

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

Ping でローカル LAN アクセスをテストする

VPN Client が ASA へのトンネル時にスプリット トンネリングを使用するように設定されているかどうかは、Windows コマンド ラ インで ping コマンドを使用してテストすることもできます。VPN Client のローカル LAN は 192.168.0.0/24 で、もう一方のホスト は同じネットワーク上に IP アドレス 192.168.0.3 で存在しています。

<#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>

トラブルシュート

スプリット トンネル ACL でのエントリの数に関する制限

スプリット トンネルに使用される ACL のエントリの数には制限があります。機能を適切に動作させるためには、ACE のエントリを 50 ~ 60 以下にすることをお勧めします。サブネット化機能を実装して IP アドレスの範囲をカバーすることをお勧めします。

関連情報

- <u>ASDM の設定例を使用したリモート VPN サーバとしての PIX/ASA 7.x</u>
- <u>Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス</u>
- <u>シスコのテクニカルサポートとダウンロード</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。