在ASA上為VPN客戶端配置分割隧道

目錄 簡介 必要條件 需求 <u>採用元件</u> 網路圖表 相關產品 <u>慣例</u> 背景資訊 <u>在ASA上配置分割隧道</u> 使用自適應安全裝置管理器(ASDM) 5.x配置ASA 7.x 使用ASDM6.x配置ASA 8.x 透過CLI配置ASA 7.x及更高版本 透過CLI配置PIX 6.x 驗證 連線VPN客戶端 <u>檢視VPN客戶端日誌</u> 使用Ping測試本地LAN訪問 疑難排解 <u>分割通道ACL中的專案數限制</u> 相關資訊

簡介

本文檔介紹在將VPN客戶端透過隧道連線到Cisco ASA 5500系列安全裝置時允許VPN客戶端訪問網 際網路的過程。

必要條件

需求

本文檔假設ASA上已存在有效的遠端訪問VPN配置。如果尚未配置PIX/ASA 7.x,請參閱<u>使用</u> ASDM將其配置為遠端VPN伺服器的配置示例。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

• Cisco ASA 5500系列安全裝置軟體版本7.x及更高版本

- Cisco系統VPN使用者端4.0.5版
- 調適型安全裝置管理員(ASDM)



注意:本文檔還包含與Cisco VPN Client 3.x相容的PIX 6.x CLI配置。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

網路圖表

VPN客戶端位於典型的SOHO網路中,透過Internet連線到總部。



網路圖表

相關產品

此配置還可用於Cisco PIX 500系列安全裝置軟體版本7.x。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

本文檔提供有關如何允許VPN客戶端在透過隧道連線到Cisco自適應安全裝置(ASA) 5500系列安全 裝置時訪問網際網路的分步說明。此配置允許VPN Client透過IPsec安全地訪問公司資源,同時提供 對Internet的不安全訪問。



注意:完全隧道配置被視為最安全的配置,因為它不支援同時裝置訪問Internet和公司 LAN。全隧道和分割隧道之間的折衷方案僅允許VPN客戶端訪問本地LAN。有關詳細資訊 ,請參閱<u>PIX/ASA 7.x:允許VPN Client訪問本地LAN的配置示例</u>。

在從VPN客戶端到ASA的基本場景中,來自VPN客戶端的所有流量都會被加密並傳送到ASA,無論 其目標是什麼。根據您的配置和支援的使用者數量,此類設定會成為頻寬密集型設定。分割隧道可 以緩解此問題,因為它允許使用者透過隧道僅傳送發往企業網路的流量。所有其他流量(如即時消 息、電子郵件或臨時瀏覽)透過VPN客戶端的本地LAN傳送到網際網路。

在ASA上配置分割隧道

使用自適應安全裝置管理器(ASDM) 5.x配置ASA 7.x

完成以下步驟以配置您的隧道組,以允許對該組中的使用者使用分割隧道。

1. 選擇Configuration > VPN > General > Group Policy,並選擇您希望在其中啟用本地LAN訪問 的組策略。然後按一下Edit。



2. 轉到Client Configuration頁籤。

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 Parameters	Microsoft Client Parameters
	F
Banner:	Minherit Edit Banner
Default Domain:	l Inherit
Solt Tunnel DNS Names (space delimited):	
opia rum el prio rumes (apace delimaco).	in the second se
Split Tunnel Policy:	V Inherit
Split Funnel Network List:	Manage
Address pools	
🔽 Inherit	
Available Pools	Assigned Pools (up to 6 entries)
	Add>>
	<=Remove

3. 取消選中分割隧道策略的Inherit框,然後選擇Tunnel Network List Below...

me: hilvalleyvpn aral PSec Client Configuration Client Firewall Hardware Client NAC WebVPN eck an Inherit checkbox to let the corresponding setting take its value from the default group policy. eneral Client Parameters Cisco Client Parameters Microsoft Client Parameters Banner: Cisco Client Parameters Microsoft Client Parameters Banner: Inherit Edit Benner Default Domain: Inherit Edit Benner Split Tunnel DNS Names (space delimited): Inherit Split Tunnel Network List: Inherit Split Tunnel Network List: Inherit Address pools Address pools Address pools Address Pools (up to 6 entries)	me: hilvalleyvpn eral PSec Client Configuration Client Firewall Hardware Client NAC WebVPN heck an Inherit checkbox to let the corresponding setting take its value from the default group policy. ereral Client Parameters Cisco Client Parameters Microsoft Client Parameters Banner: Image: Cisco Client Parameters Microsoft Client Parameters Banner: Image: Cisco Client Parameters Microsoft Client Parameters Default Domain: Image: Cisco Client Parameters Microsoft Client Parameters Spit Tunnel DNS Names (space delimited): Image: Image: Cisco Client Parameters Image: Cisco Client Parameters Spit Tunnel Policy: Inherit Tunnel All Networks Image: Cisco Client Parameters Spit Tunnel Network List: Image: Cisco Client Parameters Image: Cisco Client Parameters Address pools Address Assigned Pools (up to 6 entries) Address Address Assigned Pools (up to 6 entries)	lame: hilvalleyvpn Ineral 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 Clisco Client Parameters Microsott Client Parameters Banner: Client Parameters Client Parameters Microsott Client Parameters Banner: Client Domain: Inherit Edit Banner Default Domain: Inherit Split Tunnel DNS Names (space delimited): Inherit Split Tunnel DNS Names (space delimited): Inherit Split Tunnel Policy: Inherit Tunnel All Networks Split Tunnel Network List Address pools (up to 6 entries)	ime: hilvalleyvpn ieral IPSec Client Configuration Client Firewall Hardware Client NAC WebVPN heck an Inherit checkbox to let the corresponding setting take its value from the default group policy. ieneral Client Parameters Cisco Client Parameters Microsoft Client Parameters Banner: Inherit Edit Banner Default Domain: Inherit Edit Banner Spit Tunnel DNS Names (space definited): Inherit Tunnel All Networks Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Tunnel All Networks Address pools Address Address Minert Address Address	me: hilvalleyypn eral PSec Client Configuration Client Firewall Hardware Client NAC WebVPN heck an Inherit checkbox to let the corresponding setting take its value from the defauit group policy. eneral Client Parameters Cisco Client Parameters Microsoft Client Parameters Banner: Clie	ne: hilvalleyvpn rat PSec Client Configuration Client Firewall Hardware Client NAC WebVPN eck an Inherit checkbox to let the corresponding setting take its value from the default group policy. eneral Client Parameters Cisco Client Parameters Microsott Client Parameters Banner: Cisco Client Parameters Banner: C			
aral PSec Client Configuration Client Firewall Hardware Client NAC WebVPN aeck an Inhert checkbox to let the corresponding setting take its value from the default group policy. eneral Client Parameters Clisco Client Parameters Microsoft Client Parameters Banner: Inherit Edt Banner Default Domain: Inherit Edt 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 Address Address Address Assigned Pools (up to 6 entries)	erral PSec Client Configuration Client Firewall Hardware Client NAC WebVPN heck an Inhert checkbox to let the corresponding setting take its value from the default group policy. ieneral Client Parameters Clicco Client Parameters Microsoft Client Parameters Banner: Inherit Edit Banner Default Domain: Inherit Edit Banner Spit Tunnel DNS Names (space delimited): Inherit Tunnel All Networks Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List Inherit Exclude Network List Below Address pools Address Assigned Pools (up to 6 entries)	neral 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: Clicco Client Parameters Microsoft Client Parameters Banner: Clicco Client Parameters Microsoft Client Parameters Default Domain: Clince Client Parameters Microsoft Client Parameters Split Tunnel DNS Names (space delimited): Inherit Split Tunnel DNS Names (space delimited): Inherit Split Tunnel Policy: Inherit Split Tunnel Network List: Imherit Address pools Microsoft Client Parameters Microsoft Client Parameters Address pools Address pools Address pools Address Pools (up to 6 entries) Address Pools (up to 6 entries)	erral PSec Client Configuration Client Firewall Hardware Client NAC WebVPN heck an Inherit checkbox to let the corresponding setting take its value from the defauit group policy. ieneral Client Parameters Cisco Client Parameters Microsoft Client Parameters Banner: Inherit Edit Banner Default Domain: Inherit Edit Banner Spit Tunnel DNS Names (space delimited): Inherit Tunnel All Networks Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Exclude Network List Below Address pools Address Address Imherit Address Address	erel IPSec Client Contiguration Client Firewall Hardware Client NAC WebVPN heck an Inherit checkbox to let the corresponding setting take its value from the defauit group policy. eneral Client Parameters Clisco Client Parameters Microsoft Client Parameters Banner: Clicco Client Parameters Microsoft Client Parameters Banner: Clinco Client Parameters Microsoft Client Parameters Banner: Client Parameters Microsoft Client Parameters Banner: Clinco Client Parameters Microsoft Client Parameters Banner: Client Parameters Spit Tunnel DNS Names (space delimited): Client Parameters Spit Tunnel Policy: Client Parameters Spit Tunnel Network List: Client Parameters Address pools Vinnert Address pools Solid Inherit Address Pools (up to 6 entries) Solid Inherit Address Spit Tunnel Policy: Client Parameters Address pools Solid Inherit Address Pools (up to 6 entries) Solid Inherit Address Pools (up to 6 entries) Solid Inherit Address Pools (up to 6 entries) Solid Inherit Solid Inherit Address Pools (up to 6 entries) Solid Inherit Solid Inh	ral PSec Clert Configuration Clert Firewal Hardware Clert NAC WebVPN eck an Inherit checkbox to let the corresponding setting take its value from the default group policy, eneral Clert Parameters Clsco Clert Parameters Microsoft Clert Parameters Banner: Clico Clert Parameters Microsoft Clert Parameters Spit Tunnel DNS Names (space delimited): Inherit Spit Tunnel All Networks List Bolow Exclude Network List Bolow Address pools Clinherit Address pools Addres	ame: hilvalleyvpn		
eral PSec Client Configuration Client Firewall Hardware Client NAC WebVPN eck an Inherit checkbox to let the corresponding setting take its value from the default group policy. eneral Client Parameters Cisco Client Parameters Microsott Client Parameters Banner: Default Domain: Default Domain: Split Tunnel DNS Names (space delimited): Split Tunnel Policy: Split Tunnel Policy: Split Tunnel Network List: Address pools Address pools Address	eral PSec Client Configuration Client Firewall Hardware Client NAC WebVPN heck an Inherit checkbox to let the corresponding setting take its value from the default group policy. ieneral Client Parameters Clisco Client Parameters Microsoft Client Parameters Banner: Inherit Edit Banner Default Domain: Inherit Edit Banner Spit Tunnel DNS Names (space delimited): Inherit Tunnel All Networks Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Exclude Network List Below Address pools Address Address Inherit Address Address	IPSec Client Configuration Client Firewal 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 Microsott Client Parameters Banner: Immerit Edit Banner Default Domain: Immerit Edit Banner Split Tunnel DNS Names (space delimited): Immerit Tunnel All Networks Split Tunnel Policy: Inherit Tunnel All Networks Split Tunnel Network List: Imherit Tunnel Network List Below Address pools Address pools Assigned Pools (up to 6 entries)	eral PSec Client Configuration Client Firewall Hardware Client NAC WebVPN heck an Inherit checkbox to let the corresponding setting take its value from the default group policy. ieneral Client Parameters Clisco Client Parameters Microsoft Client Parameters Banner: Inherit Edit Banner Default Domain: Inherit Edit Banner Spit Tunnel DNS Names (space delimited): Inherit Tunnel All Networks Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List Inherit Address pools Address pools Address Address Address Varieble Pools Address Address Address	eral PSec Client Configuration Client Firewall Hardware Client NAC WebVPN heck an Inherit checkbox to let the corresponding setting take its value from the default group policy. eneral Client Parameters Cisco Client Parameters Microsott Client Parameters Banner:	ral PSec Client Configuration Client Firewall Hardware Client NAC WebVPN eck an Inherit checkbox to let the corresponding setting take its value from the default group policy. meral Client Parameters Clieco Client Parameters Microsoft Client Parameters Banner:			
eek an Inherit checkbox to let the corresponding setting take its value from the default group policy. eneral Client Parameters Cisco Client Parameters Microsott Client Parameters Banner: Banner: Default Domain: Default Doma	heck an Inherit checkbox to let the corresponding setting take its value from the default group policy. eneral Client Parameters Cisco Client Parameters Microsoft Client Parameters Banner: Clit Banner Default Domain: Inherit Edit Banner Default Domain: Inherit Spit Tunnel DNS Names (space definited): Inherit Tunnel All Networks Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Eckle Below Exclude Network List Below Address pools Address pools Address pools Address pools Address pools	Check an Inherit checkbox to let the corresponding setting take its value from the default group policy. Seneral Client Parameters Clisco Client Parameters Microsott Client Parameters Banner: Inherit Edit Banner Default Domain: Split Tunnel DNS Names (space delimited): Inherit Split Tunnel Policy: Inherit Tunnel All Networks Split Tunnel Network List: Address pools Address pools Address pools Address pools Address pools	heck an Inherit checkbox to let the corresponding setting take its value from the default group policy. eneral Client Parameters Cisco Client Parameters Microsoft 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 pools Address pools Address Addres Address Address Address Address Addres Add	heck an Inherit checkbox to let the corresponding setting take its value from the default group policy. eneral Client Parameters Clisco Client Parameters Microsoft Client Parameters Banner: Clisco Client Parameters Microsoft Client Parameters Default Domain: Clinherit Edit Banner Spit Tunnel DNS Names (space delimited): Clinherit Tunnel All Networks Tunnel All Network List Below Exclude Network List Below Colude Network List Below Address pools Clinherit Avarietie Pools (up to 6 entries) Client Address Address Address Pools (up to 6 entries) Client Address Client Parameters Client Pools (up to 6 entries) Client Pools (up to 6 e	eck an Inherit checkbox to let the corresponding setting take its value from the default group policy. Inneral Client Parameters Cisco Client Parameters Microsoft Client Parameters Banner: Default Domain: Default Domain: Default Domain: Default Domain: Default Domain: Default Domain: Default Domain: Default Domain: Default Domain: Default Domain: Default Domain: Default Domain: Default Domain: Default Domain: Default Domain: Default Domain: Default Domain:	neral IPSec Client Configuration Client Firewall	Hardware Client	NAC WebVPN
eneral Client Parameters Cisco Client Parameters Microsott Client Parameters Banner: Default Domain: Default Domain: Split Tunnel DNS Names (space delimited): Split Tunnel DNS Names (space delimited): Split Tunnel Policy: Split Tunnel Policy: Split Tunnel Network List: Split Tunnel Network List: Split Tunnel Network List: Address pools Address pools Address Pools Address	eeneral Client Parameters Cisco Client Parameters Microsoft Client Parameters Banner: Default Domain: Default Domain: Spit Tunnel DNS Names (space delimited): Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Inherit Spit Tunnel Network List Spit Tunnel Network List Network List Address pools	General Client Parameters Cisco Client Parameters Microsott Client Parameters Banner: Inherit Edit Banner Default Domain: Inherit Inherit Spit Tunnel DNS Names (space delimited): Inherit Tunnel All Networks Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Tunnel Network List Below Address pools Addiss Acsigned Pools (up to 6 entries) Addiss Addiss Addiss	eeneral Client Parameters Cisco Client Parameters Microsoft Client Parameters Banner: Default Domain: Default Domain: Spit Tunnel DNS Names (space delimited): Spit Tunnel All Networks Spit Tunnel Policy: Spit Tunnel Network List: Spit Tunnel Network List: Address pools Address	eneral Client Parameters Cisco Client Parameters Microsoft Client Parameters Banner: Default Domain: Default Domain: Spit Tunnel DNS Names (space delimited): Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Spit Tunnel Policy: Spit Tunnel Network List: Spit Tunnel Network List Below Address pools Spit Inherit Available Pools Address Address Address	nerel Client Parameters Clisco Client Parameters Microsott Client Parameters Banner:	Check an Inherit checkbox to let the corresponding	setting take its valu	ue from the default group policy.
eneral Client Parameters Cisco Client Parameters Microsoft Client Parameters Banner: Default Domain: Default Domain: Split Tunnel DNS Names (space delimited): Split Tunnel DNS Names (space delimited): Split Tunnel Policy: Split Tunnel Policy: Inherit Address pools Address pools Adde> Adde> Assigned Pools (up to 6 entries) Adde>	Banner: Inherit Default Domain: Inherit Spit Tunnel DNS Names (space delimited): Inherit Spit Tunnel Policy: Inherit Spit Tunnel Network List: Inherit Address pools	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 Inherit Split Tunnel Policy: Inherit Tunnel All Networks Split Tunnel Network List: Inherit Tunnel All Network List Below Address pools Addi>> Addi>> Addi>> Addi>> Addi>>	Banner: Inherit Default Domain: Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Address pools Address pools Inherit Address pools	eneral Client Parameters Clisco Client Parameters Microsoft Client Parameters Banner: Default Domain: Default Domain: Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Spit Tunnel Network List: Address pools Address Addres Address Addres	eneral Client Parameters Cisco Client Parameters Microsoft Client Parameters Banner: Banner: Default Domain: Default Domain: Spit Tunnel DNS Names (space delimited): Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Spit Tunnel Network List: Spit Tunnel Network List: Spit Tunnel Network List: Address pools Address Address Pools Address A			
Banner: Inherit Edit Banner Default Domain: Inherit Inherit Spit Tunnel DNS Names (space delimited): Inherit Inherit 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) Adde> Adde>	Banner: Inherit Edit Banner Default Domain: Inherit Inherit Spit Tunnel DNS Names (space delimited): Inherit Tunnel All Networks Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Tunnel Network List Below Address pools Address pools (up to 6 entries) Addiese Addiese Inherit	Banner: Inherit Edit Banner Default Domain: Inherit Inherit Spit Tunnel DNS Names (space delimited): Inherit Tunnel All Networks Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Tunnel All Network List Below Address pools Address Pools (up to 6 entries) Address pools Address	Banner: Inherit Edit Banner Default Domain: Inherit Inherit Spit Tunnel DNS Names (space delimited): Inherit Tunnel All Networks Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Tunnel All Network List Below Address pools Address pools (up to 6 entries) Address pools Addi>> Addi>>	Banner: Image: Imag	Banner: Inherit Default Domain: Inherit Spit Tunnel DNS Names (space definited): Inherit Spit Tunnel Policy: Inherit Spit Tunnel Network List: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Address pools	General Client Parameters Cisco Client Parameters	s 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 Inherit Exclude Network List Below Address pools Address Assigned Pools (up to 6 entries)	Banner: Inherit Edit Banner Default Domain: Inherit Inherit 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 pools Assigned Pools (up to 6 entries) Add>> Add>> Assigned Pools (up to 6 entries)	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 pools Acsigned Pools (up to 6 entries) Address Address Address	Banner: Inherit Edit Banner Default Domain: Inherit Inherit 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 pools Adde>> Addi>> Addi>> Assigned Roots (up to 6 entries)	Banner: Inherit Edit Banner Default Domain: Inherit Inherit Spit Tunnel DNS Names (space delimited): Inherit Tunnel All Networks Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Tunnel All Networks Address pools Inherit Address Inherit Available Pools Assigned Pools (up to 6 entries) Address <	Banner: ✓ Inherit Edt Banner Default Domain: ✓ Inherit Split Tunnel DNS Names (space delimited): ✓ Inherit Split Tunnel Networks (space delimited): ✓ Inherit Tunnel All Networks Split Tunnel Network List: ✓ Inherit Address pools ✓ Inherit Avariable Pools Addess Addes		_	
Default Domain: Inherit Spit Tunnel DNS Names (space delimited): Inherit Spit Tunnel Policy: Inherit Spit Tunnel Network List: Inherit Tunnel Network List: Inherit Address pools Inherit Address pools Inherit Address pools	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 Immerit Available Pools Addless Addless Addless Addless	Default Domain: Inherit Spit Tunnel DNS Names (space delimited): Inherit Spit Tunnel Policy: Inherit Spit Tunnel Network List: Inherit Tunnel All Networks Spit Tunnel Network List: Address pools Inherit Available Pools Address	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 (up to 6 entries) Addless Addless Addless Addless	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 Inherit Address pools Inherit Address pools Address pools (up to 6 entries) (up to 6 entries) (up to 6 entries)	Default Domain: Image: Default Domain: Image: Default Domain: Split Tunnel DNS Names (space definited): Split Tunnel Policy: Inherit Tunnel All Networks Split Tunnel Network List: Image: Default Domain: Address pools Address pools Address pools (up to 6 entries) Address Set Tunnel Pools (up to 6 entries) Address	Banner:	l⊻ Inherit	Edit Banner
Spit Tunnel DNS Names (space delimited): Immerit Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Immerit Address pools Immerit Address pools Address	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 Inherit Available Pools Address pools Addess Inherit Addess	Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Spit Tunnel Policy: Inherit Spit Tunnel Network List: Address pools Address Add	Split Tunnel DNS Names (space delimited): Split Tunnel All Networks Split Tunnel Network List: Split Tunnel Network List: Address pools Address pools Address pools Address pools Address pools Address Pools (up to 6 entries) Address Pools (up to 6 entries) Address Pools (up to 6 entries)	Spit Tunnel DNS Names (space delimited): ✓ Inherit Spit Tunnel Policy: Inherit Spit Tunnel Network List: ✓ Inherit Address pools ✓ Inherit Address pools ✓ Inherit Address pools ✓ Address ✓ Inherit Address Address pools ✓ Address ✓ Inherit Address Address ✓ Inherit	Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Spit Tunnel Network List: Address pools Address Address pools Address Addres	Defer it Domain:	🔽 Inherit	
Split Tunnel DNS Names (space delimited): Immerit Split Tunnel Policy: Immerit Split Tunnel Network List: Immerit Split Tunnel Network List: Immerit Address pools Immerit Address pools Address Address pools Address Address Address Address Address	Spit Tunnel DNS Names (space delimited): Inherit Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Address pools Address pools Addiress pools Addiress pools Addiress pools	Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Inherit Tunnel All Networks Tunnel All Networks Tunnel Network List: Inherit Address pools Inherit Available Pools Address Address pools	Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Inherit Address pools Inherit Available Pools Addle> Addle>	Spit Tunnel DNS Names (space delimited): Inherit Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: ✓ Inherit Address pools Inherit Address pools Inherit Assigned Pools (up to 6 entries) Address Address Address Address	Spit Tunnel DNS Names (space delimited): Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List Address pools	Denoue Denoue.	14 million	1
Split Tunnel Policy: □ Inherit Tunnel All Networks Split Tunnel Network List: ☑ Inherit Tunnel Network List Below Address pools ☑ Inherit Exclude Network List Below Address pools ☑ Assigned Pools (up to 6 entries) Add>> ☑ Add>>	Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Imherit Address pools	Spit Tunnel Policy: Inherit Tunnel All Networks Tunnel All Network List Inherit Address pools Address pools Address pools Address pools Address pools Address pools Address pools Address pools Address pools Address pools Address pools	Spit Tunnel Policy: Spit Tunnel Network List: Address pools Add	Spit Tunnel Policy: Spit Tunnel Network List: Spit Tunnel Network List: Address pools Address pools Address pools Address pools Address Pools (up to 6 entries) Address Address	Spit Tunnel Policy:	Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Split Tunnel Policy: Inherit Tunnel All Networks Split Tunnel Network List: Imherit Tunnel Network List Below Address pools Imherit Exclude Network List Below Address pools Address (up to 6 entries) Address Address Address (up to 6 entries)	Split Tunnel Policy: Inherit Tunnel All Networks Split Tunnel Network List: Imherit Tunnel All Network List Below Address pools Exclude Network List Below Exclude Network List Below Address pools Address pools Address pools (up to 6 entries) Address pools Address (up to 6 entries) Address (up to 6 entries)	Spit Tunnel Policy: Inherit Tunnel All Networks Tunnel All Networks Tunnel All Networks Tunnel Network List Inherit Address pools Image: Address pools	Spit Tunnel Policy: Inherit Tunnel All Networks Spit Tunnel Network List: Imherit Address pools	Split Tunnel Policy: Inherit Tunnel All Networks Split Tunnel Network List: Inherit Tunnel Network List Below Address pools Exclude Network List Below Address pools Address pools Inherit Avaïable Pools Assigned Pools (up to 6 entries) Address Address	Spit Tunnel Policy: Inherit Iunnel All Networks Iunnel All Networks Iunnel Network List Below Address pools Address pools Address Pools Address Addre			
Split Tunnel Network List: Image: Tunnel All Network List Below Address pools Exclude Network List Below Address pools Assigned Pools (up to 6 entries) Add>> Add>>	Split Tunnel Network List: Immerit Tunnel All Network List Below Address pools Exclude Network List Below Exclude Network List Below Address pools Address pools Assigned Pools (up to 6 entries) Address pools Address Address Address pools Address Assigned Pools (up to 6 entries)	Split Tunnel Network List: Inherit Tunnel Network List Below Address pools Exclude Network List Below Address pools Assigned Pools (up to 6 entries) Address Address Address pools Assigned Pools (up to 6 entries) Address Address	Split Tunnel Network List:	Split Tunnel Network List: Address pools Address pools Available Pools Addl>>	Split Tunnel Network List Immerit Tunnel All Network List Below Address pools Address pools ✓ Inherit Available Pools Assigned Pools (up to 6 entries) Addi>> Addi>>	Split Tunnel Policy:	🗌 Inherit	Tunnel All Networks
Split Tunnel Network List: Inherit Address pools Inherit Avaïable Pools Add>>	Address pools Address pools Available Pools Address Address	Spit Tunnel Network List Inherit Exclude Network List Below Address pools Imherit Available Pools Available Pools Assigned Pools (up to 6 entries) Add>> Add>>	Address pools Address pools Address pools Address pools	Split Tunnel Network List:	Split Tunnel Network List:			Tunnel All Networks
Address pools Inherit Avaïable Pools Add>>	Address pools Address pools Avaïable Pools Avaïable Pools Add>> Add>> <	Address pools Address pools Image: Address pools Available Pools Add>> Add>> Add>> < <remove< td=""></remove<>	Address pools Address pools Avaïab/e Pools Assigned Pools (up to 6 entries) Add>> Add>>	Address pools Address pools Available Pools Add>> Add>> Add>> Add>>	Address pools Address pools Available Pools Assigned Pools (up to 6 entries) Add>>	Split Tunnel Network List	🔽 Inherit	Exclude Network List Below
Available Pools Assigned Pools (up to 6 entries)	Available Pools Assigned Pools (up to 6 entries) Add>> <	Image: Second	Avaïable Pools Assigned Pools (up to 6 entries) Add>>	Avaïable Pools Assigned Pools (up to 6 entries) Add>> <	Inherit Available Pools Assigned Pools (up to 6 entries) Add>>	- Address pools		
Avaïable Pools Assigned Pools (up to 6 entries) Add>>	Available Pools Assigned Pools (up to 6 entries) Add>>	Available Pools Assigned Pools (up to 6 entries) Add>> Add>>	Available Pools Assigned Pools (up to 6 entries) Add>>	Avaïabre Pooris Assigned Pools (up to 6 entries) Add>> < <remove< td=""></remove<>	Available Pools Assigned Pools (up to 6 entries) Add>> <			
Add>>	Add>> < <remove< td=""><td>Add>> <<remove< td=""><td>Add>> <<remove< td=""><td>Add>> <</td><td>Add>></td><td>Avaïable 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>Add>> <</td><td>Add>></td><td>Avaïable Pools</td><td></td><td>Assigned Pools (up to 6 entries)</td></remove<></td></remove<>	Add>> < <remove< td=""><td>Add>> <</td><td>Add>></td><td>Avaïable Pools</td><td></td><td>Assigned Pools (up to 6 entries)</td></remove<>	Add>> <	Add>>	Avaïable Pools		Assigned Pools (up to 6 entries)
Add>>	Add>> < <remove< td=""><td>Add>> <<remove< td=""><td>Add>></td><td>Add>></td><td>Add>></td><td></td><td></td><td></td></remove<></td></remove<>	Add>> < <remove< td=""><td>Add>></td><td>Add>></td><td>Add>></td><td></td><td></td><td></td></remove<>	Add>>	Add>>	Add>>			
	<=Remove	< <remove< td=""><td></td><td><#Remove</td><td><!-- Remove</td--><td></td><td>Add>></td><td>]</td></td></remove<>		<#Remove	Remove</td <td></td> <td>Add>></td> <td>]</td>		Add>>]
<=Remove							< <remove< td=""><td></td></remove<>	

取消選中Split Tunnel Network List所對應的Inherit框,然後按一下Manage啟動ACL Manager。

ame: hilvalleyvpn		
eral IPSec Client Configuration Client Firewall	Hardware Client	NAC WebVPN
heck an inherit checkbox to let the corresponding a	atting take its val	is from the default aroun policy
Incorder mineral checkbox to let the corresponding a	i	a non-the default group policy.
eneral Client Parameters Cisco Client Parameters	Microsoft Client	Parameters
Banner:	🔽 Inherit	Edit Benner
	E	
Default Domain:	I¥ Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Soit Tunnel Policy	Inherit	Tunnel Network List Below
Split Tunnel Network List:	inherit	None Manage
- Address pools		10
l Inherit		
Available Pools		Assigned Pools (up to 6 entries)
	Add⊳⊳	1
	< <remove< td=""><td>i</td></remove<>	i
		, I

在ACL Manager中,選擇Add > Add ACL...以建立新的訪問清單。

Bandard AGL Edan	ded ACL				
🗣 Add 🔹 🔡 Edit	1 2000 + 4	发胎圈子			
Add AGL	dress dress	Action	Description		
≜inset . Trisert atter					
approver server.					

為此ACL提供一個名稱,然後按一下**OK**。

ACL Manager			×
Add * Edended ACL Edended ACL # Add * Address	Adton Description		
	AGI, Name: Spit_Turnel_List	Holp	
Rule Row Disgram	sinside → dony	side -S	×
	OK Cancel	Hep	

建立ACL後,選擇Add > Add ACE。.以便增加訪問控制條目(ACE)。

ACL Manager					n i	×
Stendard ACL Extende	NI AGL					
◆ Add → 🔟 🗠 (Dekte + 4	X % @ -				
Add AG	dress	Action	Description			
🔸 Add AGE 📐		·				
A losed						
# R0912101						
						_

定義與ASA後面的LAN對應的ACE。在本例中,網路是10.0.1.0/24。

a.

٠

選擇Permit。

b.

選擇IP地址10.0.1.0

c.

選擇網路掩碼255.255.255.0。

d.

(可選)提供說明。

e.

按一下>「**確定**」。

Stereierd 442. Extended 442. • Add • Extended 442. • Add • Extended 442. • Addrees	M.L.Manager		
Add - M Adves Adve Adve Adve Adve Adve Adve Adve Adve	Stendard ACL Extender	AG.	
No Address Action Decorption SplL Turnet Lit Action	🗣 Add 🕞 📑 ESC 📋	Delete 9 6 3 Ra 88 -	
Selt_Turvel_List Selt_Turvel_List ActionAction	No A	alifeis Action Description	
Action Action Action P Action P Actions P Actions P Actions P Actions P Actions P Concel Methylastic Description Cencel Holp	Splt_Turnet_List		
Action ★ Action ▼ HostRietwork ▼ P Addemse: 10.0.1.0 Hetwase: 255.255.0 Description: ▼ Description: ▼ Off Cencel Holp			
Action Action ProceNetwork P Address: 0.0.1.0 Network: 055.255.255.0 Description Description Off Cancel Holp		Seadd Act	l l
Action Powel		Adion	
P Addetese: F0.0.1.0 Hetmask: 255.255.255.0 Description: The components network behind the ASA.		Action of Poerry T	
P Addemso: 10.0.1.0 Hetwask: 255.255.255.0 Description: Description: Off. Cencel Help		HortHetwork	
Netweak: 255.255.0		PAddemax F0.010	
Description: The corporate network behind the ASA.		Network 055,255,255,1	
Description: The corporate network behind the ASA.			
The corporate network terhind the ASA.		Description	
OK Cancel Holp		The corporate network behind the ASA.	
OK Cancel Holp			
		OK Cancel Holp	
		V	
Rule Row Disgram	Fluie Flow Disgram		
3- Welde at an outside		and invide	

按一下OK 以退出ACL Manager。



確保您剛剛建立的ACL已為Split Tunnel Network List選中。

lame: hitvalleyvpn		
neral IPSec Client Configuration Client Firewal	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	Parameters
Barren	17 kitarit	Erit Enver
Carles.	17 BERGIN	Lat. District.
Default Domain:	🖂 inherit	
Split Tunnel DNS Names (space delimited):	P Inherit	
Colli Terreni Dolove	C start	Turned blob work 1 let Daines
spill runnel Policy.	1. Press	
Spilt Tunnel Network List:	inherit	Spit_Turnet_L Manage
-Address page		None Spit. Turnet List
17 intent		cutside_cryptome
Available Pada		Assigned Pools (up to 5 entries)
	Addre	1
	offermowe	il
		·

按一下OK 以返回組策略配置。

it Internal Group Policy: hillvalleyvpn			X
Name: hitvaleyvpn			
General PSec Client Configuration Client Firewall	Hardware Client	NAC WebVPN	
Check an Inherit checkbox to let the corresponding a	setting take its val.	e from the default group policy.	
General Client Parameters Cisco Client Parameters	Microsoft Client	Parametera	
Barner:	🖂 inhert	Edt Borner	
Default Domain:	I⊽ inherit		
Split Tunnel DNS Names (space delimited):	17 Inhert		
Split Tunnel Policy:	□ interit	Tunnel Network List Below	
Split Tunnel Network List:	inhert	Spit_Tunnet_L * Manage	
Address pools			

按一下Apply,然後按一下Send(如果需要),以將命令傳送到ASA。



使用ASDM 6.x配置ASA 8.x

•

完成以下步驟以配置您的隧道組,以允許對該組中的使用者使用分割隧道。

選擇Configuration > Remote Access VPN > Network (Client) Access > Group Policies,並選擇您希望在其中啟用本地LAN訪問的組策略。然後按一下Edit。

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 internal externally on a RADIUS/LDAP server. The group policy information is referenced by VPN bunnel groups and user accounts.

🚸 Add 🔹 📝 Edit 👔 Delete			
Name	Туре	Tunneling Protocol	A
OfItGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webvpn	N/A
Defaultgroup	Interna	Inherited	N/A
(hivaleyvpn	Internal	svc,IPSec	N/A

1	Edit Internal Group Policy:	: hivalleyvpn	
	General Servers B-Advanced Golt Turneling - If Browser Procy B-SSL VPN Client B-IPsec Client	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and require tunneling. The security appliance makes split tunneling decisions on the basis of a network ACL that consists of list of addresses on the private network. DNS Names: 🖓 Inherit 📃	t those that do no k list, which is an
	Clent Firewal	Network List: 🔽 Inheriti	Manage
	Herdware Clent	Intercept DHCP Configuration Message from Micosoft Clients	
		prior to XP, DHCP Intercept provides the domain name and subnet mask. Intercept: ∇ Inherit $C \cong C$ is:	
		Subnet Mark (Optional): 0.0.0.0	<u>*</u>
	ž D		

取消選中Split Tunnel Policy所對應的Inherit框,然後選擇Tunnel Network List Below。

ſ	Edit Internal Group Policy	: hivalleyvpn	
	General Servers	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do n require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is a A/CL that consists of list of addresses on the private network.	nc
		DNS Names: 🖂 Inherit Policy: 🔲 Inherit Tunnel Network List Below	
	Clerit Access Rule	Network Let: V Inherit Tunnel Al Network List Below	
	- Hardware Clienc	Intercent DHCP Configuration Message from Microsoft Clients (1	81
		Intercept: IP Intercept into the cents use spit currency with the security appliance. For Windows clients prior to XP, DHCP Intercept provides the domain name and subnet mask.	

取消選中Split Tunnel Network List所對應的Inherit框,然後按一下Manage啟動ACL Manager。

🗯 Edit Internal Group Policy	n hivalleyvpn
General Servins 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 Browser Prazy	DNS Names: 🖂 Inherit 🗍
Clent Access RuleClent Rreval	Network Liet: Sthere None
Hardware Clienc	Intercept DHCP Configuration Message from Micosoft Clients (*)
	DHCP Intercept lets Microsoft 3P clients use split tunneling with the security appliance. For Windows clients prior to 3P, DHCP Intercept provides the domain name and subnet mask.
	Intercept: 🔽 Inhent - C Vos - C No
	Subret Heck (Options): 0.0.0.0 💌

在ACL Manager中,選擇Add > Add ACL...以建立新的訪問清單。

C ACL	Manager					
Stani	dard ACL Extended AC	i -				
*	vdd 🔹 📓 Edit 📋 D	elete 🕈 🔹	4 次 時	a 💼 🕴		
4	Add ACL		Action		Description	
+	Add ACE	2				
*	Insert					
Ŧ	Insert After					

為ACL提供一個名稱,然後按一下OK。

•

ACL Manage	er			
Standard ACL	Extended ACL		- 1	
🗣 Add 🔸	🗹 Edit 🎬 Delete 🕈	4 3, Ph 1	8. •	
No _	Address	Action	Description	
	🚮 Add A	a		×
	ACI Nor	e Solt Turcel Lid		-
	MCL NON	e. [pt+c_rome_bo		
		OK Cario	Help	
				1 Sec

建立ACL後,選擇Add > Add ACE...以增加訪問控制項(ACE)。



定義與ASA後面的LAN對應的ACE。在本例中,網路是10.0.1.0/24。

a.

按一下Permit單選按鈕。

b.

選擇掩碼為10.0.1.0/24的網路地址。

c.

(可選)提供說明。

d.

按一下「OK」(確定)。

💼 ALL Manager						
Standard ACL Extended AV	al					
🗣 Add 🔹 🎬 Edt 👔 I	Deloto 🕈 🗲 👗	Ri 10				
No Addr	ess Action		Description			
Split_Turnel_List	10.000					
	🖆 Add ACE					×
	Action: (? Permit (" Denv				
	Address: 10.0.1.024			-		
	man man (manual tra					
	Description:					
	The Corporate network t	behind the ASA				
			(t.	
		OK	Cancel	Help]	
					1	

按一下OK 以退出ACL Manager。

ACL Manager			×		
Standard ACL School	feed and 1				
available of Hote Extern	ieu Acc I				
🏶 Add 🔹 🧭 Edit	Telete 🕈	* \$ 4	8 III		
No	Address	Action		Description	
E Split_Tunnel_List					
1 10.0.	.0/24	Permit	The Corporate	network behind the AS	5A
					1
			OK	Cancel	tein

確保您剛剛建立的ACL已為Split Tunnel Network List選中。

📬 Edit Internal Group Policy	hivalleyvpn
General Servers Advanced	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 ACI, that consists of list of addresses on the private network.
	DNS Names: 🖓 Inherit
III-SS, WW Client ⊟-IFsec Client	Policy: Dinherit: Tunnel Network Ust Below *
Client Access Rule Client Firewal	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: 17 Inherit C Yos C /42

按一下OK 以返回組策略配置。

•

Split bunneling network lists require tunneling. The sec ACL that consists of list of	s distinguish networks that require traffic to go through the burry appliance makes split tunneling decisions on the basis of addresses on the private network.	nnel and those that do no a network list, which is an
DNS Names: 🖾 Inherit		
Policy: 🗂 Inherit	Tunnel Network List Below	Ŧ
Network List: 🕅 Inherit	Splk_Tunnel_List	* Manage
Intercept DHCP Confi DHCP Intercept lets Micr prior to 3P, DHCP Interc	puration Message from Micosoft Clients osoft XP clients use split tunneling with the security appliance apt provides the domain name and subnet mask.	Por Windows clients
Intercept: 🔽 Inherit	с»» сл.	
	Split tunneling receivers list require tunneling. The sec ACL that consists of list of DNS Names: IF Inherit Policy: IF Inherit Network List: IF Inherit Intercept DHCP Confil DHCP Intercept lets Nice prior to 3P, DHCP Interce Intercept: IF Inherit	Split tunneling retrieors lets distinguish networks that require transitions on the basis of ACL that consists of list of addresses on the private network. DNS Names: Import Policy: Inherit Tunnel Network List Below Network List: Inherit Split_Tunnel_List Intercept DHCP Configuration Message from Micosoft Clients DHCP Intercept lets Microsoft XP clients use split tunneling with the security appliance prior to XP, DHCP Intercept provides the domain name and subnet mask. Intercept: Inherit C You C You

按一下Apply,然後按一下Send(如果需要),以將命令傳送到ASA。

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

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

🗣 Add	Ŧ	Z	Edit	Û	Delete	
-------	---	---	------	---	--------	--

Name	Туре	Tunneling Protocol	
OfltGrpPolicy (System Default)	Internal	L2TP-IPSec, IPSec, webypn	N/A -
Defaultgroup	Internal	Inherited	N/A -
hivalleyvpn	Internal	svc, IP5ec	N/A -
	C ,	lock Decet	

透過CLI配置ASA 7.x及更高版本

您可以在ASA CLI中完成以下步驟,以便在ASA上允許分割隧道,而不是使用ASDM:



注意:CLI分割隧道配置對於ASA 7.x和8.x均相同。

進入配置模式。

•

<#root>

ciscoasa>

enable

Password: ******* ciscoasa#

configure terminal

ciscoasa(config)#

建立定義ASA後方的網路的訪問清單。

<#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

進入要修改的策略的組策略配置模式。

<#root>

ciscoasa(config)#

group-policy hillvalleyvpn attributes

ciscoasa(config-group-policy)#

指定拆分隧道策略。在本示例中,此策略為tunnelspecified。

<#root>

•

ciscoasa(config-group-policy)#

split-tunnel-policy tunnelspecified

指定拆分隧道訪問清單。在本示例中,此清單為Split_Tunnel_List。

<#root>

٠

ciscoasa(config-group-policy)#

split-tunnel-network-list value Split_Tunnel_List

<#root>

ciscoasa(config)#

tunnel-group hillvalleyvpn general-attributes

將組策略與隧道組關聯

<#root>

٠

ciscoasa(config-tunnel-ipsec)#

default-group-policy hillvalleyvpn

退出兩種配置模式。

•

<#root>

ciscoasa(config-group-policy)#

exit

ciscoasa(config)#

exit

ciscoasa#

將配置儲存到非易失性RAM (NVRAM),並在系統提示指定源檔名時按Enter。

<#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#

透過CLI配置PIX 6.x

請完成以下步驟:

٠

建立定義PIX後方的網路的訪問清單。

<#root>

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

• 建立一個vpn組**vpn3000**,並向其指定分割隧道ACL,如下所示:

<#root>

PIX(config)#

vpngroup vpn3000 split-tunnel Split_Tunnel_List



注意:有關PIX 6.x的遠端訪問VPN配置的詳細資訊,請參閱使用Microsoft Windows 2000和2003 IAS RADIUS身份驗證配 置適用於Windows的Cisco Secure PIX Firewall 6.x和Cisco VPN客戶端3.5。

驗證

完成以下部分中的步驟以驗證您的配置。

<u>連線VPN客戶端</u>

<u>檢視VPN客戶端日誌</u>

使用Ping測試本地LAN訪問

連線VPN客戶端

•

•

•

將您的VPN客戶端連線到VPN集中器以驗證您的配置。

從清單中選擇連線條目,並按一下Connect。

👌 VPN Client - Version 4.0.5 (Rel)		_IO X
Connection Entries Status Certificates Lo	g Options Help	
Connect New Import	Modily Delete	Cisco Systems
Connection Entries Certificates Log		
Connection Entry	Host	Tiansport _
hilvaleyvpn	172.221.160	IPSec/UDP
		-
<u>.</u>		×

輸入您的認證。

٠



1

選擇Status > Statistics...以便顯示Tunnel Details窗口,您可以在此窗口中檢查隧道特定資訊並檢視資料流。

unnel Details	Route Details	Frewal	
Address Info	rmation	Connection Information	É.
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
		·····	

轉至Route Details頁籤,檢視VPN客戶端保護到ASA的路由。

在本示例中,VPN客戶端保護對10.0.1.0/24的訪問,而所有其他流量均未加密,也未通過隧道傳送。

6	VPN Client Sta	tistics			x
	Tunnel Details	oute Details Frewa			
	Local LAN Routes	, ki	Secured Routes		
	Network	Subnet Mask	Network	Subnet Mask	
			10.0.1.0	255.255.255.0	

檢視VPN客戶端日誌

檢查VPN客戶端日誌時,您可以確定是否設定了指定分割隧道的引數。要檢視日誌,請轉到VPN Client中的Log頁籤。然後按一下Log Settings以調整記錄的內容。在本示例中,IKE設定為3 - High,而所有其他日誌元素設定為1 - Low。

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.

使用Ping測試本地LAN訪問

測試VPN客戶端在透過隧道連線到ASA時是否配置了分割隧道的另一種方法是:在Windows命令列中使用ping命令。VPN客戶端的本 地LAN是192.168.0.0/24,而網路中存在IP地址為192.168.0.3的另一台主機。

<#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 Reply from 192.168.0.3: bytes=32 time<1ms TTL=255

```
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
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>
```

疑難排解

分割通道ACL中的專案數限制

ACL中用於分割隧道的條目數量存在限制。建議不要使用50到60個以上的ACE條目以獲得滿意的功能。建議您實施子網劃分功能以 覆蓋一系列IP地址。

相關資訊

- 使用ASDM將PIX/ASA 7.x配置為遠端VPN伺服器的配置示例
- <u>Cisco ASA 5500系列調適型安全裝置</u>
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。