使用預共用金鑰在Windows 2000/XP PC和 PIX/ASA 7.2之間通過IPsec的L2TP配置示例

目錄

簡介 必要條件 需求 採用元件 相關產品 慣例 背景資訊 設定 網路圖表 組態 Windows L2TP/IPsec客戶端配置 PIX配置中的L2TP伺服器 使用ASDM配置的L2TP 採用IAS配置的Microsoft Windows 2003 Server 使用Active Directory通過IPSec進行L2TP的擴展身份驗證 驗證 疑難排解 疑難排解指令 調試輸出示例 使用ASDM進行故障排除 問題:頻繁斷開 對Windows Vista進行故障排除 相關資訊

<u>簡介</u>

本文說明如何使用預共用金鑰和Microsoft Windows 2003 Internet Authentication Service(IAS)RADIUS Server進行使用者身份驗證,配置從Microsoft Windows 2000/2003和XP客戶 端到PIX安全裝置公司辦公室的IP安全(IPsec)第2層隧道協定(L2TP)。請參閱<u>Microsoft — 清單:配</u> 置IAS以進行撥號和VPN訪問,以瞭解有關IAS的更多資訊。

在遠端訪問情況下使用IPsec配置L2TP的主要優點是,遠端使用者可以通過公共IP網路訪問 VPN,而無需網關或專用線路。這樣,幾乎可以通過POTS從任何位置進行遠端訪問。另一個好處 是,VPN接入的唯一客戶端要求是使用Windows 2000和Microsoft撥號網路(DUN)。 不需要額外的 客戶端軟體,如Cisco VPN客戶端軟體。

本文檔還介紹了如何使用思科自適應安全裝置管理器(ASDM)來配置用於L2TP over IPsec的PIX

500系列安全裝置。

附註: Cisco Secure PIX防火牆軟體版本6.x及更高版本支持基於IPsec的第2層隧道協定(L2TP)。

要在PIX 6.x和Windows 2000之間配置L2TP Over IPsec,請參閱<u>使用證書在PIX防火牆和Windows</u> 2000 PC之間配置L2TP Over IPsec。

要使用加密方法配置從遠端Microsoft Windows 2000和XP客戶端到公司站點的L2TP over IPsec,請參閱<u>使用預共用金鑰配置L2TP over IPsec從Windows 2000或XP客戶端到Cisco VPN</u> 3000系列集中器。

<u>必要條件</u>

<u>需求</u>

在建立安全隧道之前,對等體之間需要存在IP連線。

確保UDP埠1701在連線路徑的任何位置都沒有被阻止。

僅使用Cisco PIX/ASA上的預設隧道組和預設組策略。使用者定義的策略和組無法工作。

注意:如果安裝了Cisco VPN Client 3.x或Cisco VPN 3000 Client 2.5,則安全裝置不會在Windows 2000中建立L2TP/IPsec隧道。從Windows 2000的「服務」面板中禁用適用於Cisco VPN客戶端 3.x的Cisco VPN服務,或適用於Cisco VPN 3000客戶端2.5的ANetIKE服務。為此,請選擇**開始>程 式>管理工具>服務**,從「服務」面板重新啟動IPsec策略代理服務,然後重新啟動電腦。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- PIX安全裝置515E,軟體版本7.2(1)或更高版本
- 自適應安全裝置管理器5.2(1)或更高版本
- Microsoft Windows 2000 Server
- Microsoft Windows XP Professional SP2
- 採用IAS的Windows 2003 Server

注意:如果將PIX 6.3升級到版本7.x,請確保已在Windows XP(L2TP客戶端)中安裝SP2。

注意: 文檔中的資訊對ASA安全裝置也是有效的。

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。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

<u>相關產品</u>

此配置還可以與Cisco ASA 5500系列安全裝置7.2(1)或更高版本配合使用。

慣例

如需文件慣例的詳細資訊,請參閱<u>思科技術提示慣例。</u>



完成以下步驟,即可設定使用IPsec的L2TP。

1. 配置IPsec傳輸模式,以便使用L2TP啟用IPsec。Windows 2000 L2TP/IPsec客戶端使用 IPsec傳輸模式 — 僅加密IP負載,並且原始IP報頭保持不變。此模式的優點在於它只給每個封 包增加幾個位元組,並允許公用網路上的裝置看到封包的最終來源和目的地。因此,要使 Windows 2000 L2TP/IPsec客戶端連線到安全裝置,必須為轉換配置IPsec傳輸模式(請參閱 <u>ASDM配置中的步驟2</u>)。 通過此功能(傳輸),您可以根據IP報頭中的資訊在中間網路上啟用 特殊處理(例如QoS)。但是,第4層報頭已加密,這限制了資料包的檢查。遺憾的是,IP報 頭以明文傳輸,傳輸模式允許攻擊者執行一些流量分析。

2. 使用虛擬專用撥號網路(VPDN)組配置L2TP。

使用IPsec配置L2TP支援使用預共用金鑰或RSA簽名方法的證書,並支援使用動態(而非靜態)加 密對映。預共用金鑰用作建立基於IPsec的L2TP隧道的身份驗證。

<u>設定</u>

本節提供用於設定本文件中所述功能的資訊。

註:使用Command Lookup Tool(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

注意:此配置中使用的IP編址方案在Internet上不能合法路由。這些地址是在實驗室環境中使用的 RFC 1918地址。

網路圖表

本檔案會使用以下網路設定:



<u>組態</u>

本檔案會使用以下設定:

- Windows L2TP/IPsec客戶端配置
- PIX配置中的L2TP伺服器
- <u>使用ASDM配置的L2TP</u>
- 採用IAS配置的Microsoft Windows 2003 Server

<u>Windows L2TP/IPsec客戶端配置</u>

完成以下步驟,以便在Windows 2000上配置通過IPsec的L2TP。對於Windows XP,請跳過步驟 1和步驟2,然後從步驟3開始:

- 1. 將此登錄檔值新增到Windows 2000電腦: HKEY LOCAL MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
- 2. 將此登錄檔值新增到此項: Value Name: ProhibitIpSec Data Type: REG_DWORD

Value: 1

注意:在某些情況下(Windows XP Sp2),新增此項(值:1)顯示斷開連線,因為它使XP框僅協商L2TP而不是具有IPsec連線的L2TP。必須將IPsec策略與該登錄檔項一起新增。如果在嘗試建立連線時收到800,請移除金鑰(值:1)以使連線正常工作。注意:要使更改生效,必須重新啟動Windows 2000/2003或XP電腦。預設情況下,Windows客戶端會嘗試對證書頒發機構(CA)使用IPsec。 配置此登錄檔項可防止出現這種情況。現在,您可以在Windows工作站上配置IPsec策略以匹配您想要在PIX/ASA上的引數。有關Windows IPsec策略的逐步配置,請參閱如何使用預共用金鑰身份驗證(Q240262)配置L2TP/IPSec連線。如需詳細資訊,請參閱在Windows XP(Q281555)中設定用於第2層通道通訊協定連線的預先共用金鑰\。

- 3. 建立連線。
- 4. 在Network and Dial-up Connections(網路和撥號連線)下,按一下右鍵連線並選擇 **Properties**。轉到「安全」頁籤,然後按一下**高級**。選擇如下圖所示的協定。

Advanced Security Settings 🛛 💽 🔀
Data encryption:
Require encryption (disconnect if server declines)
C Logon security
O Use Extensible Authentication Protocol (EAP)
Properties
 Allow these protocols
Unencrypted password (PAP)
Shiva Password Authentication Protocol (SPAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP (MS-CHAP)
Allow older MS-CHAP version for Windows 95 servers
Microsoft CHAP Version 2 (MS-CHAP v2)
For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)
OK Cancel

5. **附註:**此步驟僅適用於Windows XP。按一下**IPSec Settings**,選中**Use pre-shared key for** authentication,然後鍵入預共用金鑰以設定預共用金鑰。在本示例中,測試用作預共用金鑰。



PIX配置中的L2TP伺服器

PIX 7.2
pixfirewall# show run
PIX Version 7.2(1) !
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
<pre>! Configures the outside and inside interfaces.</pre>
interface Ethernet0 nameif outside security-level 0 ip
address 172.16.1.1 255.255.255.0 ! interface Ethernet1
nameif inside security-level 100 ip address 10.4.4.1
255.255.255.0 ! passwd 2KFQnbNIdI.2KYOU encrypted ftp
mode passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list nonat extended permit
ip 10.4.4.0 255.255.255.0 10.4.5.0 255.255.255.0
nat (inside) 0 access-list nonat
pager lines 24

logging console debugging mtu outside 1500 mtu inside 1500 !--- Creates a pool of addresses from which IP addresses are assigned !--- dynamically to the remote VPN Clients. ip local pool clientVPNpool 10.4.5.10-10.4.5.20 mask 255.255.255.0 no failover asdm image flash:/asdm-521.bin no asdm history enable arp timeout 14400 !--- The global and nat command enable !--- the Port Address Translation (PAT) using an outside interface IP !--- address for all outgoing traffic. global (outside) 1 interface nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0 172.16.1.2 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute !--- Create the AAA server group "vpn" and specify its protocol as RADIUS. !--- Specify the IAS server as a member of the "vpn" group and provide its !--- location and key. aaa-server vpn protocol radius aaa-server vpn host 10.4.4.2 key radiuskey !--- Identifies the group policy as internal. grouppolicy DefaultRAGroup internal !--- Instructs the security appliance to send DNS and !--- WINS server IP addresses to the client. group-policy DefaultRAGroup attributes wins-server value 10.4.4.99 dns-server value 10.4.4.99 *!--- Configures L2TP over IPsec as a valid VPN tunneling* protocol for a group. vpn-tunnel-protocol IPSec 12tpipsec default-domain value cisco.com !--- Configure usernames and passwords on the device !--- in addition to using AAA. !--- If the user is an L2TP client that uses Microsoft CHAP version 1 or !--version 2, and the security appliance is configured !--to authenticate against the local !--- database, you must include the mschap keyword. !--- For example, username username test password DLaUiAX3178qgoB5c7iVNw== nt-

encrypted
vpn-tunnel-protocol 12tp-ipsec
<pre>http server enable http 0.0.0.0 0.0.0.0 inside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart</pre>
<pre>! Identifies the IPsec encryption and hash algorithms ! to be used by the transform set. crypto ipsec transform-set TRANS_ESP_3DES_MD5 esp-3des esp-md5-hmac</pre>
<pre>! Since the Windows 2000 L2TP/IPsec client uses IPsec transport mode, ! set the mode to transport. ! The default is tunnel mode. crypto ipsec transform-set TRANS_ESP_3DES_MD5 mode transport</pre>
<pre>! Specifies the transform sets to use in a dynamic crypto map entry. crypto dynamic-map outside_dyn_map 20 set transform-set TRANS_ESP_3DES_MD5</pre>
<pre>! Requires a given crypto map entry to refer to a pre-existing ! dynamic crypto map. crypto map outside_map 20 ipsec-isakmp dynamic outside_dyn_map</pre>
<pre>! Applies a previously defined crypto map set to an outside interface. crypto map outside_map interface outside</pre>
crypto isakmp enable outside crypto isakmp nat-traversal 20
<pre>! Specifies the IKE Phase I policy parameters. crypto isakmp policy 10 authentication pre-share encryption 3des hash md5 group 2 lifetime 86400</pre>
<pre>! Creates a tunnel group with the tunnel-group command, and specifies the local ! address pool name used to allocate the IP address to the client. ! Associate the AAA server group (VPN) with the tunnel group.</pre>
tunnel-group DefaultRAGroup general-attributes address-pool clientVPNpool authentication-server-group vpn
<pre>! Link the name of the group policy to the default tunnel ! group from tunnel group general-attributes mode. default-group-policy DefaultRAGroup</pre>

!--- Use the tunnel-group ipsec-attributes command !--in order to enter the ipsec-attribute configuration

```
mode. !--- Set the pre-shared key. !--- This key should
be the same as the key configured on the Windows
machine.
tunnel-group DefaultRAGroup ipsec-attributes
pre-shared-key *
!--- Configures the PPP authentication protocol with the
authentication type !--- command from tunnel group ppp-
attributes mode.
tunnel-group DefaultRAGroup ppp-attributes
no authentication chap
authentication ms-chap-v2
telnet timeout 5
ssh timeout 5
console timeout 0
1
class-map inspection_default
match default-inspection-traffic
1
1
policy-map type inspect dns preset_dns_map
parameters
 message-length maximum 512
policy-map global_policy
class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
1
service-policy global_policy global
prompt hostname context
Cryptochecksum:e1e0730fa260244caa2e2784f632accd
: end
```

使用ASDM配置的L2TP

完成以下步驟,將安全裝置配置為接受L2TP over IPsec連線:

1. 新增IPsec轉換集並指定IPsec以使用傳輸模式而不是隧道模式。為此,請選擇Configuration > VPN > IPSec > Transform Sets,然後按一下Add。將顯示「轉換集」窗格。

🙀 Cisco ASDM 5	.2 for PIX - 10.4.4.1					_1
File Options To	ols Wizards Help				Search:	Fir
ổ Home	Configuration Monitoring Bac	* Forward Pac	ket Tracer Refresh	🔒 🦓 Save Help		Cisco Syst
Mterfaces	Configuration × VPN × IP Sec × Tr VPN Wizard General VPN System Options	ansform Sets Transform Sets Specify Transform Set	8			T
L.,	Turnel Group	Name	Mode	ESP Encryption	ESP Authentication	0.444
Security Policy	Group Policy Users	ESP-DES-MD5 ESP-3DES-MD5 ESP-3DES-SHA ESP-3DES-MD5	Tunnel Tunnel Tunnel	DES DES 3DES 3DES	MD5 SHA MD5	Ealt
	Control Daramaters	ESP-AES-128-SHA ESP-AES-128-MD5	Tunnel	AES-128 AES-128	SHA MD5	
VPN	Policies	ESP-AES-192-SHA ESP-AES-192-MD5	Tunnel Tunnel	AES-192 AES-192	SHA MD5	Delete
4 3 6	PSec	ESP-AES-256-SHA	Tunnel	AES-256	SHA	
Routing	IPSec Rules Transform Sets Pre-Fragmentation Address Management	ESP-AES-256-MD6	Tunnel	AES-256	MD5	

2. 完成以下步驟以新增轉換集:輸入轉換集的名稱。選擇ESP加密和ESP身份驗證方法。選擇 Transport模式。按一下「OK」(確定)。

	\geq
Set Name: TRANS_ESP_3DES_MD5	
Properties	
Mode: O Tunnel O Transport	
ESP Encryption: 3DES	
ESP Authentication: MD5	
OK Cancel Help	

3. 完成這些步驟,設定位址指派方法。此示例使用IP地址池。選擇Configuration > VPN > IP Address Management > IP Pools。按一下「Add」。系統將顯示Add IP Pool對話方塊。輸入 新IP地址池的名稱。輸入起始和結束IP地址。輸入子網掩碼,然後按一下OK。

薩 Add IP Pool	×
Name:	clientVPNpool
Starting IP Address:	10.4.5.10
Ending IP Address:	10.4.5.20
Subnet Mask:	255.255.255.0
ок	Cancel Help

4. 選擇**Configuration > VPN > General > Group Policy**,將L2TP over IPsec配置為組策略的有效 VPN隧道協定。將顯示「組策略」窗格。

🔂 Cisco ASDM 5.2 for PIX - 10.4.4.1					_
File Options Tools Wizards Help				Search	Fi
Home Configuration Monitoring Ex	ack Forward Packet Tracer	Q Refresh	Save Help		Cisco Sys
Configuration > VPN > General VPN Wizerd Ceneral VPN System Options Clent Update Cent Update Clent Update Clent Update Clent Update Clent System Options	 Group Policy Group Policy Manage VPN group policies: A may be stored internally on the referenced by VPN tunnel group 	VPN group po device or ext as and user a	alicy is a collection of use temaly on a RADIUS ser accounts.	er-oriented attribute/value p ver. The group policy infor	wirs that mation is
NAT	Name	Туре	Tunneling Protocol 🗠	AAA Server Group	Add 🔻
	DittGrpPolicy (System Default)	Internal	L2TP-PSec JPSec	N/A	
Global Parameters	DefaultRAGroup	Internal	L2TP-PSec JPSec	N/A	Edit
VPN Policies UPN E-20 Certificate Group Mat					Delete
🖧 📴 🏪 PSec					

5. 選擇一個組策略(DiffGrpPolicy),然後按一下Edit。將顯示「編輯組策略」對話方塊。選中 L2TP over IPSec以為組策略啟用協定,然後按一下OK。

Internal Group Policy: Drite	rpPolicy
Name: DfttGrpPolicy	
eneral DRec Client Configur	ation Client Einswall Handware Client NAC
citeria (insec citeria contigui	ation Client Firewair Hardware Client NAC
Tunneling Protocols:	PSec V L2TP over IPSec
Filter:	None Manage
Connection Settings	
Access Hours:	Unrestricted Manage
Simultaneous Logins:	3
Maximum Connect Time:	Unlimited minutes
Idle Timeout:	Unlimited 30 minutes
Servers	
DNS Servers:	Primary: Secondary:
WINS Servers:	Primary: Secondary:
DHCP Scope:	
Servers DNS Servers: WINS Servers: DHCP Scope:	Primary: Secondary: Primary: Secondary:

6. 完成以下步驟,以便將IP地址池分配給隧道組:選擇Configuration > VPN > General > Tunnel Group。出現Tunnel Group窗格後,在表中選擇一個隧道組(DefaultRAGroup)。按一下「

Eait」。					
Cisco ASDM 5.	2 for PIX - 10.4.4.1				
File Options Too	ols VVIzards Help			Search	
G Home C	Configuration Monitoring Bac	k Forward Packet Trace	r Refresh Save	? Halp	Cisc
	Configuration > VPN > General > 1	Tunnel Group			
Interfaces	VPN Wixerd General VPN System Options Crient Update Tunnel Group Croup Paticy	Manage VPN tunnel groups. or Web/VPN connection.	A VPN tunnel group represe	nts a connection specific reco	rd for a IPSec
	Users	Name	Туре	Group Policy	Add 🔫
64	Default Tunnel Gatev	DefaultRAGroup	ipsec-ra	DefaultRAGroup	í
NAT		DefaultL2LGroup	ipsec-I2I	DttGrpPolicy	Edit
SK VPN	KE Global Parameters Policias Certificate Group Mal				Delete
423 Routing	B-1 PSec				

7. 出現「Edit Tunnel Group(編輯隧道組)」視窗時,請完成以下步驟:從General頁籤轉到 Client Address Assignment頁籤。在Address Pools區域中,選擇要分配給隧道組的地址池。

按一	下「Add」。	,地址池將顯	頁示在「分配的	为池」	框中。		
🚺 Eo	lit Tunnel Gr	oup					
	Name:	DefautRAGr	pup		Туре:	ipsec-ra	
	General IP:	Sec PPP					
	Configure	general access	attributes from th	e follov	ving sub-	tabs.	
	Basic Au	thentication A	thorization Acc	ounting	Client	Address A	Assignment Advanced
	To s > IP	pecify whether Address Manag	to use DHCP or a gement > Assignm	address nent.	pools fo	r address	assignment, go to Confi
	C.	HCP Servers					
		P Address:			Add >> Delete		
	<u>م</u>	ddress Pools To configure inte	erface-specific ad	dress	pools, go	to the Ad	vanced tab.
		Available Pools					Assigned pools
		client∀PNpool			Add :	ave	

8. 若要設定預共用金鑰,請轉到IPSec頁籤,輸入**預共用金鑰**,然後按一下**確定**。

撞 Edit Tunnel Group		
Name: DefaultRAGroup	Type: ipsec-ra	
General IPSec ppp		
Pre-shared Key: [lest]	Trustpoint Name:	None
Authentication Mode: xauth	IKE Peer ID Validation:	Required
Enable sending certificate chain		
ISAKMP Keepalive		
C Disable keepalives		
Monitor keepalives		
Confidence Interval:	300 (seconds) Retry Inter	val: 2 (seconds)
C Head end will never initiate k	eepalive monitoring	
Interface-Specific Authentication M	lode	
Interface:	Interfac	e Authentication Mode
inside	Add >>	
Authentication Mode:	<< Remove	
none		

9. L2TP over IPsec使用PPP身份驗證協定。在隧道組的PPP頁籤上指定允許PPP連線的協定。 選擇**MS-CHAP-V1協定進**行身份驗證。

Edit Tunnel G	roup			
Name:	DefaultRAGroup	Туре:	ipsec-ra	
General IP	Sec PPP			
(and the second				
Specify	y the authentication protocols perm	nitted for a PPP	connection.	
	Г СНАР			
	MS-CHAP-V	1		
	MS-CHAP-V	2		
	П РАР			
	EAP-PROXY			

10. 指定對嘗試通過IPsec進行L2TP連線的使用者進行身份驗證的方法。您可以將安全裝置配置為使用身份驗證伺服器或它自己的本地資料庫。若要執行此操作,請轉至隧道組的Authentication頁籤。預設情況下,安全裝置使用其本地資料庫。Authentication ServerGroup下拉選單顯示LOCAL。要使用身份驗證伺服器,請從清單中選擇一個伺服器。注意:安全裝置僅支援本地資料庫上的PPP身份驗證PAP和Microsoft CHAP版本1和2。EAP和CHAP由代理身份驗證伺服器執行。因此,如果遠端使用者屬於使用EAP或CHAP配置的隧道組,並且安全裝置配置為使用本地資料庫,則該使用者無法連線。

🧊 Ed	lit Tunnel Gro	up					
	Name:	DefaultRAGroup		Type:	ipsec-ra		
					·		
	General IPS	ec PPP					
	Configure g	eneral access attributes f	from the follow	ving sub)-tabs.		
	Basic Auth			Client	Address Assid	nment A	dvanced
	To set au	thentication server group	per interface,	, go to th	ne Advanced ta	b.	
			-			-	
	Authenti	cation Server Group:			-	$\mathbf{\mathcal{D}}$	
	Г	Use LOCAL if Server Gr	oup fails	_			
			,				
	NAC Aut	hentication Server Group	None		_		
	141101164		. [

注意:選擇Configuration > VPN > General > Tunnel Group以返回隧道組配置,以便您可以 將組策略連結到隧道組並啟用隧道組交換(可選)。 顯示Tunnel Group窗格時,選擇隧道組 並按一下Edit。注意:通道組交換使安全裝置能夠將建立L2TP over IPsec連線的不同使用者 與不同的隧道組相關聯。由於每個隧道組都有自己的AAA伺服器組和IP地址池,因此使用者 可以通過特定於其隧道組的方法進行身份驗證。通過此功能,使用者不再僅傳送使用者名稱 ,而是以username@group_name格式傳送使用者名稱和組名,其中「@」表示您可以配置 的分隔符,組名是在安全裝置上配置的隧道組的名稱。注意:通道組交換通過剝離組處理啟 用,通過剝離組處理,安全裝置能夠通過從VPN客戶端提供的使用者名稱獲取組名來為使用 者連線選擇隧道組。然後,安全裝置僅傳送使用者名稱的使用者部分以進行授權和身份驗證 。否則(如果禁用),安全裝置將傳送整個使用者名稱,包括領域。要啟用隧道組交換,請 選中Strip the realm from username before passing to the AAA server,選中Strip the group from username before passing to the AAA server。然後按一下OK。

11. 完成以下步驟,在本地資料庫中建立使用者:選擇Configuration >Properties >裝置管理>使 用者帳戶。按一下「Add」。如果使用者是使用Microsoft CHAP版本1或2的L2TP客戶端,並 且安全裝置配置為針對本地資料庫進行身份驗證,則必須選中User Authenticated using MSCHAP以啟用MSCHAP。按一下「OK」(確定)。

付 Add User Account		
Identity VPN Policy		
	Username:	test
	Password:	****
	Confirm Password:	****
<	l User authenticat	ed using MSCHAP
	Privilege level is used wit	h command authorization.
	Privilege Level:	2 💌

12. 選擇Configuration > VPN > IKE > Policies,然後按一下Add以為階段I建立IKE策略。按一下 OK繼續。

Add IKE Policy			×
Priority:	10	Authentication:	pre-share
Encryption:	3des 💌	D-H Group:	2 💌
Hash:	md5	Lifetime:	Unlimited Seconds
	ок	Cancel	Help

13. (可選)如果您希望一個NAT裝置後面有多個L2TP客戶端嘗試通過IPsec連線到安全裝置 ,則必須啟用NAT遍歷,以便ESP資料包可以經過一個或多個NAT裝置。完成以下步驟即可 完成此操作:選擇Configuration > VPN > IKE > Global Parameters。確保在介面上啟用 ISAKMP。選中Enable IPSec over NAT-T。按一下「OK」(確定)。

採用IAS配置的Microsoft Windows 2003 Server

完成以下步驟,以便使用IAS配置Microsoft Windows 2003伺服器。

注意:這些步驟假設IAS已安裝在本地電腦上。如果不是,請通過**控制面板>新增/刪除程式**新增此項 。

 選擇Administrative Tools > Internet Authentication Service,然後按一下右鍵RADIUS Client以新增新的RADIUS客戶端。鍵入客戶端資訊後,按一下OK。此示例顯示一個名為「 Pix」的客戶端,其IP地址為10.4.4.1。客戶端供應商設定為RADIUS Standard,而共用金鑰為

Treather Which a	tx:	[Protocol
RADIUS CH	nts Eliendy name	RADBUS
Renote Act	ess	
E 🙆 Connection	Ret Address (IP or DNS)	100
	10.4.4.1	
	Vede	
		and the second
	attribute, specify the vendor of the RADRUS client.	cent vendors
	Cleret-Vendor RADIUS Studyland	
	Bequest must contain the Message Authenticator	atribule
	Changed accept	
	graeu seuer.	
	Cgnim shared secret	

- 2. 選擇Remote Access Policies,按一下右鍵Connections to Other Access Servers,然後選擇 Properties。
- 3. 確保選擇了**授予遠端訪問許可權**選項。
- 4. 按一下Edit Profile並檢查以下設定:在Authentication頁籤上,選中Unencrypted authentication(PAP, SPAP)。在加密頁籤上,確保選中No Encryption選項。完成後按一下



- OK₀
- 5. 選擇Administrative Tools > Computer Management > System Tools > Local Users and Groups,按一下右鍵Users並選擇New Users,以便將使用者新增到本地電腦帳戶中。
- 6. 使用思科密碼password1新增使用者並檢查此配置檔案資訊:在「General(常規)」頁籤上 ,確保選中Password Never Expired選項,而不是「User Must Change Password(使用者必 須更改密碼)」選項。在「撥入」頁籤上,選擇允許訪問(或保留通過遠端訪問策略控制訪問)的選項。完成後按一下OK。

Ble Action ye Image: Second Secon

使用Active Directory通過IPSec進行L2TP的擴展身份驗證

在ASA上使用此配置允許從Active Directory對L2tp連線進行身份驗證:

此外,在L2tp客戶端上,轉到Advanced Security Settings(Custom),然後僅選擇未加密密碼 (PAP)選項。



本節提供的資訊可用於確認您的組態是否正常運作。

<u>Output Interpreter Tool</u> (僅供<u>註冊</u>客戶使用)支援某些**show**命令,這允許您檢視<u>show</u>命令輸出的分 析。

• show crypto ipsec sa — 顯示對等體上的所有當前IKE安全關聯(SA)。 pixfirewall#show crypto ipsec sa interface: outside Crypto map tag: outside_dyn_map, seq num: 20, local addr: 172.16.1.1 access-list 105 permit ip host 172.16.1.1 host 192.168.0.2 local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/17/0) remote ident (addr/mask/prot/port): (192.168.0.2/255.255.255.255/17/1701) current_peer: 192.168.0.2, username: test dynamic allocated peer ip: 10.4.5.15 #pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 23 #pkts decaps: 93, #pkts decrypt: 93, #pkts verify: 93 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 23, #pkts comp failed: 0, #pkts decomp failed: 0 #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 172.16.1.1, remote crypto endpt.: 192.168.0.2 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: C16F05B8 inbound esp sas: spi: 0xEC06344D (3959829581) transform: esp-3des esp-md5-hmac in use settings ={RA, Transport, } slot: 0, conn_id: 3, crypto-map: outside_dyn_map sa timing: remaining key lifetime (sec): 3335 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xC16F05B8 (3245278648) transform: esp-3des esp-md5-hmac in use settings ={RA, Transport, } slot: 0, conn_id: 3, crypto-map: outside_dyn_map sa timing: remaining key lifetime (sec): 3335 IV size: 8 bytes replay detection support: Y show crypto isakmp sa — 顯示對等體上的所有當前IKE SA。 pixfirewall#show crypto isakmp sa

Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1

- 1 IKE Peer: 192.168.0.2 Type : user Role : responder Rekey : no State : MM_ACTIVE
- show vpn-sessiondb 包括可用於檢視有關L2TP over IPsec連線的詳細資訊的協定過濾器。
 全域性配置模式的完整命令是show vpn-sessoindb detailed remote filter protocol
 I2tpOverIpsec。此示例顯示單個L2TP over IPsec連線的詳細資訊:

pixfirewall#show vpn-sessiondb detail remote filter protocol L2TPOverIPSec

```
Session Type: Remote Detailed
Username : test
Index
           : 1
Assigned IP : 10.4.5.15
                                 Public IP : 192.168.0.2
Protocol : L2TPOverIPSec
                                 Encryption : 3DES
Hashing
           : MD5
Bytes Tx : 1336
                                 Bytes Rx : 14605
                                  Client Ver :
Client Type :
Group Policy : DefaultRAGroup
Tunnel Group : DefaultRAGroup
Login Time : 18:06:08 UTC Fri Jan 1 1993
Duration : 0h:04m:25s
Filter Name :
NAC Result : N/A
Posture Token:
IKE Sessions: 1
IPSec Sessions: 1
L2TPOverIPSec Sessions: 1
TKE:
 Session ID : 1
 UDP Src Port : 500
                                   UDP Dst Port : 500
 IKE Neg Mode : Main
                                    Auth Mode : preSharedKeys
 Encryption : 3DES
                                    Hashing
                                                : MD5
 Rekey Int (T): 28800 Seconds
                                   Rekey Left(T): 28536 Seconds
 D/H Group : 2
TPSec:
 Session ID : 2
 Local Addr
             : 172.16.1.1/255.255.255.255/17/1701
 Remote Addr : 192.168.0.2/255.255.255.255/17/1701
 Encryption : 3DES
                                   Hashing : MD5
 Encapsulation: Transport
                                  Rekey Left(T): 3333 Seconds
 Rekey Int (T): 3600 Seconds
 Idle Time Out: 30 Minutes
                                   Idle TO Left : 30 Minutes
 Bytes Tx : 1336
                                   Bytes Rx : 14922
  Pkts Tx
            : 25
                                    Pkts Rx
                                               : 156
L2TPOverIPSec:
 Session ID : 3
 Username : test
 Assigned IP : 10.4.5.15
                                   Auth Mode : msCHAPV1
  Encryption : none
                                Idle TO Left : 30 Minutes
Bytes Rx : 13431
  Idle Time Out: 30 Minutes
 Bytes Tx : 378
```

Pkts Rx

: 146



Pkts Tx

: 16

本節提供的資訊用於對組態進行疑難排解。還顯示了調試輸出示例。

<u>疑難排解指令</u>

輸出直譯器工具(僅供註冊客戶使用)支援特定命令,此工具允許您檢視show命令輸出的分析。

注意:使用debug命令之前,請先參閱<u>有關Debug命令</u>和<u>IP安全性故障排除的重要資訊 — 瞭解和使</u> <u>用debug命令</u>。

- debug crypto ipsec 7 顯示第2階段的IPsec協商。
- debug crypto isakmp 7 顯示第1階段的ISAKMP協商。

<u> 調試輸出示例</u>

<u>PIX防火牆</u>

PIX#debug crypto isakmp 7 pixfirewall# Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Mess age (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 256 Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Oakley proposal is acceptable Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received Fragmentation VID Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received NAT-Traversal ver 02 V ΤD Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing IKE SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, IKE SA Proposal # 1, Transform # 2 acceptable Matches global IKE entry # 2 Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ISAKMP SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Fragmentation VID + extended capabilities payload Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 104 Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) total length : 184 Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ke payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ISA_KE payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing nonce payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ke payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing nonce payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Cisco Unity VID pa yload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing xauth V6 VID paylo ad Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send IOS VID Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Constructing ASA spoofing IOS V endor ID payload (version: 1.0.0, capabilities: 20000001) Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing VID payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group Def aultRAGroup Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat ing keys for Responder...

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 256 Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) total length : 60 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing ID payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computi ng hash for ISAKMP Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group Def aultRAGroup Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Freeing previ ously allocated memory for authorization-dn-attributes Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting ID payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computi ng hash for ISAKMP Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting dpd vid payload Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 80 !--- Phase 1 completed succesfully. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, PHASE 1 COMPL ETED Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alive type for this connection: None Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alives configured on but peer do es not support keep-alives (type = None) Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Startin g P1 rekey timer: 21600 seconds. Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE DECODE RECEIVED Message (msgid=e1 b84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 164 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing nonce payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing ID payload Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received remo te Proxy Host data in ID Payload: Address 192.168.0.2, Protocol 17, Port 1701 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing ID payload Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received loca 1 Proxy Host data in ID Payload: Address 172.16.1.1, Protocol 17, Port 1701 !--- PIX identifies the L2TP/IPsec session. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, **L2TP/IPSec se** ssion detected. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, QM IsRekeyed old sa not found by addr

Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE Remote Pe er configured for crypto map: outside_dyn_map Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing IPSec SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IPSec S

A Proposal # 1, Transform # 1 acceptable Matches global IPSec SA entry # 20 Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE: requesti ng SPI! Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got SPI from key engine: SPI = 0xce9f6e19 !--- Constructs Quick mode in Phase 2. Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, **oakley** constucting quick mode Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting blank hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting IPSec SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting IPSec nonce payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting proxv ID Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Transmi tting Proxy Id: Remote host: 192.168.0.2 Protocol 17 Port 1701 Local host: 172.16.1.1 Protocol 17 Port 1701 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting qm hash payload Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=elb 84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + N ONE (0) total length : 144 Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE DECODE RECEIVED Message (msgid=e1 b84b0) with payloads : HDR + HASH (8) + NONE (0) total length : 48 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, loading all IPSEC SAs Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat ing Ouick Mode Kev! Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat ing Quick Mode Key! Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Security nego tiation complete for User () Responder, Inbound SPI = 0xce9f6e19, Outbound SPI $= 0 \times d08 f711 b$ Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got a KEY_ADD msg for SA: SPI = 0xd08f711b Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Pitcher : received KEY_UPDATE, spi 0xce9f6e19 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Startin g P2 rekey timer: 3059 seconds. !--- Phase 2 completes succesfully. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, PHASE 2 COMPL ETED (msgid=0e1b84b0) Jan 02 18:26:44 [IKEv1]: IKEQM Active() Add L2TP classification rules: ip <192.1 68.0.2> mask <0xFFFFFFF> port <1701> PIX#debug crypto ipsec 7 pixfirewall# IPSEC: Deleted inbound decrypt rule, SPI 0x71933D09 Rule ID: 0x028D78D8 IPSEC: Deleted inbound permit rule, SPI 0x71933D09 Rule ID: 0x02831838 IPSEC: Deleted inbound tunnel flow rule, SPI 0x71933D09 Rule ID: 0x029134D8 IPSEC: Deleted inbound VPN context, SPI 0x71933D09 VPN handle: 0x0048B284 IPSEC: Deleted outbound encrypt rule, SPI 0xAF4DA5FA Rule ID: 0x028DAC90 IPSEC: Deleted outbound permit rule, SPI 0xAF4DA5FA Rule ID: 0x02912AF8 IPSEC: Deleted outbound VPN context, SPI 0xAF4DA5FA VPN handle: 0x0048468C

```
IPSEC: New embryonic SA created @ 0x01BFCF80,
   SCB: 0x01C262D0,
   Direction: inbound
   SPI : 0x45C3306F
   Session ID: 0x000000C
   VPIF num : 0x0000001
   Tunnel type: ra
   Protocol : esp
   Lifetime : 240 seconds
IPSEC: New embryonic SA created @ 0x0283A3A8,
   SCB: 0x028D1B38,
   Direction: outbound
   SPI : 0x370E8DD1
   Session ID: 0x000000C
   VPIF num : 0x0000001
   Tunnel type: ra
   Protocol : esp
   Lifetime : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x370E8DD1
IPSEC: Creating outbound VPN context, SPI 0x370E8DD1
   Flags: 0x0000205
   SA : 0x0283A3A8
   SPI : 0x370E8DD1
   MTU : 1500 bytes
   VCID : 0x0000000
   Peer : 0x0000000
   SCB : 0x028D1B38
   Channel: 0x01693F08
IPSEC: Completed outbound VPN context, SPI 0x370E8DD1
   VPN handle: 0x0048C164
IPSEC: New outbound encrypt rule, SPI 0x370E8DD1
   Src addr: 172.16.1.1
   Src mask: 255.255.255.255
   Dst addr: 192.168.0.2
   Dst mask: 255.255.255.255
   Src ports
     Upper: 1701
     Lower: 1701
     Op : equal
   Dst ports
     Upper: 1701
     Lower: 1701
     Op : equal
   Protocol: 17
   Use protocol: true
   SPI: 0x0000000
   Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x370E8DD1
   Rule ID: 0x02826540
IPSEC: New outbound permit rule, SPI 0x370E8DD1
   Src addr: 172.16.1.1
   Src mask: 255.255.255.255
   Dst addr: 192.168.0.2
   Dst mask: 255.255.255.255
   Src ports
     Upper: 0
     Lower: 0
     Op : ignore
   Dst ports
     Upper: 0
     Lower: 0
     Op : ignore
    Protocol: 50
   Use protocol: true
```

SPI: 0x370E8DD1 Use SPI: true IPSEC: Completed outbound permit rule, SPI 0x370E8DD1 Rule ID: 0x028D78D8 IPSEC: Completed host IBSA update, SPI 0x45C3306F IPSEC: Creating inbound VPN context, SPI 0x45C3306F Flags: 0x0000206 SA : 0x01BFCF80 SPI : 0x45C3306F MTU : 0 bytes VCID : 0x0000000 Peer : 0x0048C164 SCB : 0x01C262D0 Channel: 0x01693F08 IPSEC: Completed inbound VPN context, SPI 0x45C3306F VPN handle: 0x0049107C IPSEC: Updating outbound VPN context 0x0048C164, SPI 0x370E8DD1 Flags: 0x00000205 SA : 0x0283A3A8 SPI : 0x370E8DD1 MTU : 1500 bytes VCID : 0x0000000 Peer : 0x0049107C SCB : 0x028D1B38 Channel: 0x01693F08 IPSEC: Completed outbound VPN context, SPI 0x370E8DD1 VPN handle: 0x0048C164 IPSEC: Completed outbound inner rule, SPI 0x370E8DD1 Rule ID: 0x02826540 IPSEC: Completed outbound outer SPD rule, SPI 0x370E8DD1 Rule ID: 0x028D78D8 IPSEC: New inbound tunnel flow rule, SPI 0x45C3306F Src addr: 192.168.0.2 Src mask: 255.255.255.255 Dst addr: 172.16.1.1 Dst mask: 255.255.255.255 Src ports Upper: 1701 Lower: 1701 Op : equal Dst ports Upper: 1701 Lower: 1701 Op : equal Protocol: 17 Use protocol: true SPI: 0x0000000 Use SPI: false IPSEC: Completed inbound tunnel flow rule, SPI 0x45C3306F Rule ID: 0x02831838 IPSEC: New inbound decrypt rule, SPI 0x45C3306F Src addr: 192.168.0.2 Src mask: 255.255.255.255 Dst addr: 172.16.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50

```
Use protocol: true
   SPI: 0x45C3306F
   Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x45C3306F
   Rule ID: 0x028DAC90
IPSEC: New inbound permit rule, SPI 0x45C3306F
   Src addr: 192.168.0.2
   Src mask: 255.255.255.255
   Dst addr: 172.16.1.1
   Dst mask: 255.255.255.255
   Src ports
     Upper: 0
     Lower: 0
     Op : ignore
   Dst ports
     Upper: 0
     Lower: 0
     Op : ignore
   Protocol: 50
   Use protocol: true
   SPI: 0x45C3306F
   Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x45C3306F
    Rule ID: 0x02912E50
```

使用ASDM進行故障排除

您可以使用ASDM啟用日誌記錄並檢視日誌。

- 選擇Configuration > Properties > Logging > Logging Setup,選擇Enable Logging,然後按一 下Apply以啟用日誌記錄。
- 2. 選擇Monitoring > Log Buffer > On Logging Level, 選擇Logging Buffer, 然後按一下View以檢視日誌。

<u>問題:頻繁斷開</u>

空閒/會話超時

如果閒置超時設定為30分鐘(預設值),則表示在30分鐘內沒有流量通過隧道後丟棄該隧道。無論 空閒超時設定如何,VPN客戶端都會在30分鐘後斷開連線,並且會遇到PEER_DELETE-IKE_DELETE_UNSPECIFIED錯誤消息。

將閒置逾時和作業階段逾時設定為none,讓通道一直處於開啟狀態且永遠不會捨棄通道。

在組策略配置模式或使用者名稱配置模式下輸入vpn-idle-timeout命令以配置使用者超時時間:

hostname(config)#group-policy DfltGrpPolicy attributes hostname(config-group-policy)#vpn-idle-timeout none

在組策略配置模式或使用者名稱配置模式下使用**vpn-session-timeout**命令配置VPN連線的最大時間 :

hostname(config)#group-policy DfltGrpPolicy attributes hostname(config-group-policy)#vpn-session-timeout none

對Windows Vista進行故障排除

同時使用者

Windows Vista L2TP/IPsec引入了一些架構更改,禁止多個同時使用者連線到頭端PIX/ASA。此行 為在Windows 2K/XP上不會發生。自版本7.2(3)及更高版本起,思科已實施此變更的解決方法。

Vista PC無法連線

如果Windows Vista電腦無法連線L2TP伺服器,則驗證您是否在DefaultRAGroup上的pppattributes下僅配置了mschap-v2。

相關資訊

- 最常見的L2L和遠端訪問IPSec VPN故障排除解決方案
- Cisco PIX 500系列安全裝置
- <u>Cisco ASA 5500系列調適型安全裝置</u>
- Cisco PIX防火牆軟體產品支援
- <u>Cisco Secure PIX防火牆命令參考</u>
- <u>RADIUS 支援頁面</u>
- IPSec協商/IKE通訊協定支援頁面
- <u>要求建議 (RFC)</u>
- <u>第二層通道通訊協定(L2TP)</u>
- <u>技術支援與文件 Cisco Systems</u>