ASA/PIX:使用帶有ASDM的DHCP伺服器的IPsec VPN客戶端編址配置示例

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 設定遠端存取VPN(IPSec) 使用CLI配置ASA/PIX Cisco VPN客戶端配置 驗證 show命令 疑難排解 清除安全關聯 疑難排解指令 調試輸出示例 相關資訊

<u>簡介</u>

本文檔介紹如何配置Cisco 5500系列自適應安全裝置(ASA),以使DHCP伺服器使用自適應安全裝置 管理器(ASDM)或CLI為所有VPN客戶端提供客戶端IP地址。ASDM通過直觀易用的基於Web的管理 介面提供世界一流的安全管理和監控。Cisco ASA配置完成後,可以使用Cisco VPN客戶端進行驗 證。

請參閱<u>使用Windows 2003 IAS RADIUS(針對Active Directory)的PIX/ASA 7.x和Cisco VPN客戶 端4.x身份驗證配置示例</u>,以在Cisco VPN客戶端(4.x for Windows)和PIX 500系列安全裝置7.x之間 設定遠端訪問VPN連線。遠端VPN客戶端使用者使用Microsoft Windows 2003 Internet身份驗證服 務(IAS)RADIUS伺服器對Active Directory進行身份驗證。

請參閱<u>適用於Cisco安全ACS的PIX/ASA 7.x和Cisco VPN客戶端4.x身份驗證配置示例</u>,以使用思科 安全訪問控制伺服器(ACS版本3.2)進行擴展身份驗證(Xauth),在Cisco VPN客戶端(適用於 Windows的4.x)和PIX 500系列安全裝置7.x之間建立遠端訪問VPN連線。



本文檔假定ASA已完全正常運行並配置為允許Cisco ASDM或CLI進行配置更改。

註:請參閱<u>允許ASDM或PIX/ASA 7.x的HTTPS訪問</u>:<u>內部和外部介面上的SSH配</u>置示例,允許通過 ASDM或安全外殼(SSH)遠端配置裝置。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- •思科自適應安全裝置軟體版本7.x及更高版本
- 自適應安全裝置管理器5.x版及更高版本
- Cisco VPN客戶端4.x版及更高版本

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 PIX安全裝置7.x版及更高版本配合使用。

<u>慣例</u>

如需文件慣例的詳細資訊,請參閱思科技術提示慣例。

<u>背景資訊</u>

遠端訪問VPN滿足移動工作人員安全地連線到組織網路的要求。移動使用者可以使用其PC上安裝的 VPN客戶端軟體設定安全連線。VPN客戶端發起與配置為接受這些請求的中央站點裝置的連線。在 本示例中,中心站點裝置是使用動態加密對映的ASA 5500系列自適應安全裝置。

在安全裝置地址管理中,我們必須配置IP地址,通過隧道將客戶機與專用網路上的資源連線起來 ,並讓客戶機像直接連線到專用網路一樣工作。此外,我們只處理分配給客戶端的私有IP地址。分 配給專用網路上其他資源的IP地址是網路管理職責的一部分,而不是VPN管理的一部分。因此,此 處討論IP地址時,是指私有網路編址方案中允許客戶端用作隧道端點的IP地址。

<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<u>Command Lookup Tool</u>(僅限<u>註冊</u>客戶)可獲取本節中使用的命令的詳細資訊。

<u>網路圖表</u>

本檔案會使用以下網路設定:



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

設定遠端存取VPN(IPSec)

ASDM過程

完成以下步驟以配置遠端訪問VPN:

1. 選擇Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPSec > IKE Policies > Add以建立ISAKMP策略2,如下所示。

🚰 Add IKE Polic	у		
Priority:	2	Authentication:	pre-share 🔽
Encryption:	des 💌	D-H Group:	2 🛩
Hash:	sha 👻	Lifetime:	 Unlimited 86400 seconds
		Cancel	Help

按一下「OK」和「Apply」。

2. 選擇Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPSec > IPSec Transform Sets > Add以建立ESP-DES-SHA轉換集,如圖所示。

🖆 Add Transform Set				\mathbf{X}
Set Name:	ESP-DES-SHA]	
Properties				
Mode:	💿 Tunnel		ransport	
ESP Encryptio	n:	DES	~	
ESP Authentic	ation:	SHA	~	
		ncel	Help	
				按·

「OK」和「Apply」。

3. 選擇Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPSec > Crypto Maps > Add,以便使用優先順序為1的動態策略建立加密對映,如下所示。

📽 Create IPsec Rule
Tunnel Policy (Crypto Map) - Basic Tunnel Policy (Crypto Map) - Advanced Traffic Selection
Interface: outside V Policy Type: dynamic V Priority: 1
Transform Set to Be Added: ESP-DES-MD5 Remove Remove
Peer Settings - Optional for Dynamic Crypto Map Entries The Connection Type is applicable to static tunnel policies only. Uni-directional connection type policies are used for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may specify up to 10 redundant peers.
OK Cancel Help

按一下「OK」和「Apply」。

4. 選擇Configuration > Remote Access VPN > Network(Client)Access > Advanced > Group Policies > Add>Internal Group Policies以建立組策略(例如GroupPolicy1),如下所示。

🛍 Add Internal Group Policy 🛛 🔀						
Genera Servers ⊡Advanced	Name: Banner: Address Pools: More Option	GroupPolicy1 Inherit Inherit Select S				
Find: Next Previous Cancel Help						

按一下「OK」和「Apply」。

5. 選擇Configuration > Remote Access VPN > Network(Client)Access > Advanced > Group Policies > Add>Internal Group Policies>Servers>>,以便為要動態分配的VPN客戶端使用者 配置DHCP範圍。

🖆 Add Internal Group Po	licy 🔁	<
General Gervers ⊕-Advanced	DNS Servers: ✓ Inherit WINS Servers: ✓ Inherit More Options ② DHCP Scope: Inherit 192.168.5.0 ○ Default Domain: ✓ Inherit	
Find:	Next Previous OK Cancel Help	

按一下「**OK**」和「**Apply**」。**注意:**DHCP作用域配置是可選的。有關詳細資訊,請參閱<u>配置</u> <u>DHCP編址</u>。

6. 選擇Configuration > Remote Access VPN > AAA Setup > Local Users > Add,以便為VPN客 戶端訪問建立使用者帳戶(例如,使用者名稱 — cisco123和密碼 — cisco123)。

📬 Add User Account		×
Identity		
	Username: cisco123	
	Password: ******	
	Confirm Password: ******	
	User authenticated using MSCHAP	
	Access Restriction	
	Select one of the options below to restrict ASDM, SSH, Telnet and Console access.	
	Note: All users have network access, regardless of these settings.	
	 Full access(ASDM, SSH, Telnet and Console) 	
	Privilege level is used with command authorization.	
	Privilege Level: 2	
	CLI login prompt for SSH, Telnet and console (no ASDM access)	
	This setting is effective only if AAA authenticate console command is configured.	
	No ASDM, SSH, Telnet or Console access	
	This settion is effective only if AAA authenticate console command is configured	
	The second is chosened only in Here demonstrates consider command is configured.	
Find:	Next O Previous	
	Cancel Help	

7. 選擇Configuration > Remote Access VPN > Network(Client)Access > IPSec Connection Profiles > Add>以新增隧道組(例如,TunnelGroup1,並將Preshared key作為cisco123),如

卜所示。				
File View Tools Wizards Window He	dp.		Look For:	
Home 🆓 Configuration 🔯 Monitoria	ng 🔚 Save 🔇 Refresh 🔇	Back 🔘 Forward 🧳 He	dp	
Remote Access VPN Imposition Introduction Network (Clent) Access AnyConnect Connection Profiles Free Connection Profiles Group Policies Imposition Access Policies Imposition Profiles	Configuration > Remote Access Access Interfaces Enable interfaces for IPsec acce Interface outside dmz inside Connection Profiles Connection profile (tunnel group Add T2 Edit III Delet	VPH > Hetwork (Client) Ac ss. Allow Ac	cese > IPsec Connection Pro	0108
	Name	IPsec Enabled	L2TP/IPsec Enabled	Autentication
H-bo Hovanced	DefaultWEBVPNGroup			LOCAL
	DefaultRAGroup	Ā	M	LOCAL
Remote Access VPN Image: Ste-to-Site VPN <td></td> <td></td> <td></td> <td></td>				
» *			Apply Reset	

在Basic頁籤下,為User Authentication欄位選擇伺服器組作為LOCAL。選擇Grouppolicy1作

為Default Group Policy欄位的組策略。在為DHCP伺服器提供的空間中提供DHCP伺服器IP地 址。

🖆 Add IPsec Remote Acce	ess Connection Prof	ile 🛛 🔀
Basic	Name:	TunnelGroup1
±-Auvanceu	IKE Peer Authentication	
	Pre-shared Key:	* * * * * * *
	Identity Certificate:	None Manage
	User Authentication —	
	Server Group:	LOCAL Manage
	Fallback:	Use LOCAL if Server Group fails
	Client Address Assignme	ent
	DHCP Servers:	192.168.10.1
	Client Address Pools:	Select
	Default Group Policy	
	Group Policy:	GroupPolicy1 Manage
	•	(Following fields are attributed of the group policy selected above.)
		C Enable IPsec protocol
		Enable L2TP over IPsec protocol
Find:		💿 Next 🛛 🙆 Previous
		Cancel Help

按一下「OK」(確定)。

8. 選擇Advanced > Client Addressing >, 然後選中Use DHCP覈取方塊, DHCP伺服器可以將 IP地址分配給VPN客戶端。**注意:**確保取消選中Use authentication server和Use address pool**的覈取方塊。**

🖆 Add IPsec Remote Acc	ess Connection Profile	×
Basic Advanced General Client Addressing Authentication Authorization Accounting PPP	Global Client Address Assignment Policy This policy affects all Network (Client) Access connections. The following are tried in order until an address is found. Use authentication server ✓ Use DHCP Use address pool Interface-Specific Address Pools ▲ Add met Edit methed Interface Address Pools	
Find:	Next O Previous	
	Cancel Help	

ASDM 6.x的配置

同一個ASDM配置在ASDM 6.x版中運行良好,但對ASDM路徑進行了一些細微修改除外。到某些欄 位的ASDM路徑與ASDM 6.2版及更高版本有所不同。下面列出了這些修改以及現有的路徑。如果所 有主要ASDM版本中的圖形影象保持不變,則不會附加這些圖形。

- Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPSec > IKE Policies > Add
- 2. Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPSec > IPSec Transform Sets > Add
- Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPSec > Crypto Maps > Add
- 4. 選擇Configuration > Remote Access VPN > Network(Client)Access > Group Policies > Add > Internal Group Policies
- 5. 選擇Configuration > Remote Access VPN > Network(Client)Access > Group Policies > Add > Internal Group Policies > Servers
- 6. 選擇Configuration > Remote Access VPN > AAA Setup/Local Users > Local Users > Add
- 7. Configuration > Remote Access VPN > Network(Client)Access > IPSec Connection Profiles > Add
- 8. 選擇Configuration > Remote Access VPN > Network(Client)Access > Address Assignment > Assignment

Policy



預設情況下啟用這三個選項。Cisco ASA按照相同順序為VPN客戶端分配地址。取消選中其他兩個選項時,Cisco ASA不會驗證aaa伺服器和本地池選項。預設啟用的選項可通過**show run** all驗證 在vpn-add命令中|。以下是供您參考的輸出示例:

vpn-addr-assign aaa vpn-addr-assign dhcp vpn-addr-assign local reuse-delay 0 有關此命令的詳細資訊,請參閱vpn-addr-assign。

<u>使用CLI配置ASA/PIX</u>

完成這些步驟,以便配置DHCP伺服器從命令列向VPN客戶端提供IP地址。有關所使用的每個命令的詳細資訊,請參閱<u>配置遠端訪問VPN</u>或<u>Cisco ASA 5500系列自適應安全裝置 — 命令參考</u>。

在ASA裝置上運行配置
ASA# sh run
ASA Version 8.0(2)
!
! Specify the hostname for the Security Appliance.
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! ! Configure the outside and inside
interfaces. interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 50 ip address
192.168.10.2 255.255.255.0 ! Output is suppressed.
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa802-k8.bin ftp mode passive access-list 101
extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0
255.255.255.0 pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 no failover icmp unreachable rate-limit 1 burst-
size 1 ! Specify the location of the ASDM image for
ASA to fetch the image for ASDM access. asdm image
disk0:/asdm-613.bin no asdm history enable arp timeout
14400 global (outside) 1 192.168.1.5 nat (inside) 0
access-list 101 nat (inside) 1 0.0.0.0 0.0.0.0 route
outside 0.0.0.0 0.0.0.0 192.168.1.2 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 sipdisconnect 0:02:00 timeout uauth 0:05:00 absolute dynamic-access-policy-record DfltAccessPolicy 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 crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto dynamic-map outside_dyn_map 1 set transform-set ESP-DES-SHA crypto map outside_map 1 ipsec-isakmp dynamic outside_dyn_map !--- Specifies the interface to be used with !--- the settings defined in this configuration. crypto map outside_map interface outside !--- PHASE 1 CONFIGURATION ---! !--- This configuration uses ISAKMP policy 2. !--- The configuration commands here define the Phase !--- 1 policy parameters that are used. crypto isakmp enable outside crypto isakmp policy 2 authentication pre-share encryption des hash sha group 2 lifetime 86400 no crypto isakmp nat-traversal !---Specifies that the IP address to the vpn clients are assigned by the DHCP Server and now by AAA or the Local pool. The CLI vpn-addr-assign dhcp for VPN address assignment through DHCP Server is hidden in the CLI provided by **show run** command. no vpn-addr-assign aaa no vpn-addr-assign local

telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list ! class-map inspection_default match default-inspection-traffic ! 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 service-policy global_policy global 1 group-policy GroupPolicy1 internal group-policy GroupPolicy1 attributes !--- define the DHCP network scope in the group policy. This configuration is Optional dhcp-network-scope



Cisco VPN客戶端配置

嘗試使用Cisco VPN客戶端連線到Cisco ASA,以驗證ASA配置是否成功。

- 1. 選擇Start > Programs > Cisco Systems VPN Client > VPN Client。
- 2. 按一下New以啟動Create New VPN Connection Entry視窗。

status: Disconnected VPN Client - Version 5.0.03.0530						
Connection B	Entries S	itatus	Certificates	Log Option	s Help	
Connect New Import Modify Delete						
Connection Entries Certificates Log						
(Connectio	n Entry	r A		Host	

3. 填寫新連線的詳細資訊。輸入連線條目的名稱和說明。在Host**框中輸入ASA的**外部IP地址。然 後輸入ASA中配置的VPN隧道組名稱(TunnelGroup1)和密碼(預共用金鑰 — cisco123)。按 一下「**Save**」。

VPN Client Create New VPN Conner	ction Entry	
Connection Entry: ASA		
Description: vpntunnel		uluilu cisco
Host: 192.168.1.1		
Authentication Transport Backup Servers	Dial-Up	
Group Authentication	C Mutual Group	Authentication
Name: TunnelGroup1		
Password: ******		
Confirm Password:		
C Certificate Authentication		
Name:		
🗖 Send CA Certificate Chain		
Erase User Password	Save	Cancel

4. 點選要使用的連線,然後從VPN客戶端主視窗中點選Connect。

	us: Connected VPN Client - Ver	sion 5.0.03.0530	antona enclandan enclandan ence	
Connec	tion Entries Status Certificates Log O	ptions Help	en la sectione de sectione de la se	nin na
Con	nect New Import Mode	y Delete	alı ci	nilin sco
Connec	ction Entries Certificates Log			apoa
	Connection Entry /	Host	Transport	
8	ASA	192.168.1.1	IPSec/UDP	

5. 出現提示時,輸入Username:cisco123和密碼:cisco123(如上述ASA中配置的xauth),然後點 選OK(確定)以連線到遠端網路。

The	and the fallenting i		
authentication.	sted the following i	nrormation to complete	e the user
Username:	cisco123		
CISCO Passwor	******		
		OK	Court

6. VPN客戶端與中心站點的ASA連線。

🥔 stat	tus: Connected VPN Client	Version 5.0.03.0530	
Connec	tion Entries Status Certificates Log	Options Help	
Discor	nnect New Import	lodiy Delete	cisco
Connec	ction Entries Certificates Log		
	Connection Entry	Host	Transport
0	ASA	192.168.1.1	IPSec/UDP
Conner	La Regali		

7. 成功建立連線後,從Status選單中選擇**Statistics**以驗證隧道的詳細資訊。

🥔 status: Cor	nected VPN Client - Version 5	.0.03.0530	
Connection Entrie	es Status Certificates Log Options	Help	
Disconnect Connection Entri	Statistics Ctrl+S Notifications Ctrl+N Reset Stats	Delete	alialia cisco
C	Connection Entry	Host	Transport
<u>۵</u> ۸	SA	192.168.1.1	IPSec/UDP



<u>show命令</u>

使用本節內容,確認您的組態是否正常運作。

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析 。

• show crypto isakmp sa — 顯示對等體上的所有當前IKE安全關聯(SA)。

• show crypto ipsec sa — 顯示當前SA使用的設定。

```
ASA #show crypto ipsec sa
interface: outside
    Crypto map tag: dynmap, seq num: 10, local addr: 192.168.1.1
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.5.1/255.255.255.255/0/0)
      current_peer: 192.168.1.2, username: cisco123
      dynamic allocated peer ip: 192.168.5.1
      #pkts encaps: 55, #pkts encrypt: 55, #pkts digest: 55
      #pkts decaps: 55, #pkts decrypt: 55, #pkts verify: 55
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-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.: 192.168.1.1, remote crypto endpt.: 192.168.1.2
      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: C2C25E2B
    inbound esp sas:
      spi: 0x69F8C639 (1777911353)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 40960, crypto-map: dynmap
         sa timing: remaining key lifetime (sec): 28337
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xC2C25E2B (3267517995)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 40960, crypto-map: dynmap
         sa timing: remaining key lifetime (sec): 28337
         IV size: 8 bytes
         replay detection support: Y
ASA #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: 192.168.1.2 Type : user Role : responder Rekey : no State : AM_ACTIVE



本節提供的資訊可用於對組態進行疑難排解。還顯示了調試輸出示例。

註:有關遠端訪問IPsec VPN故障排除的詳細資訊,請參閱<u>最常見的L2L和遠端訪問IPSec VPN故障</u> 排除解決方案

<u>清除安全關聯</u>

進行故障排除時,請確保在進行更改後清除現有的安全關聯。在PIX的特權模式下,使用以下命令 :

- clear [crypto] ipsec sa 刪除活動的IPsec SA。關鍵字crypto是可選的。
- clear [crypto] isakmp sa 刪除活動的IKE SA。關鍵字crypto是可選的。

<u>疑難排解指令</u>

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析 。

附註:使用 debug 指令之前,請先參閱<u>有關 Debug 指令的重要資訊</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>ASA 8.0</u>
- <u>適用於Windows的VPN使用者端5.0</u>

<u>ASA 8.0</u>

ASA#debug crypto isakmp 7

```
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message
 (msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR
(13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total le
ngth : 856
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing SA payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ke payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ISA_KE payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing nonce payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received xauth V6 VID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received DPD VID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Fragmentation VID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, IKE Peer included IKE fragmenta
tion capability flags: Main Mode:
                                          True Aggressive Mode: False
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received NAT-Traversal ver 02 V
ID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Cisco Unity client VID
```

Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, Connection landed on tunnel_group Tun nelGroup1 Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g IKE SA payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, IKE SA Pr oposal # 1, Transform # 13 acceptable Matches global IKE entry # 2 Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing ISAKMP SA payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing ke payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing nonce payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Generatin g keys for Responder... Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing ID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing hash payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing hash for ISAKMP Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing Cisco Unity VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing xauth V6 VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing dpd vid payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing Fragmentation VID + extended capabilities payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Send Alti ga/Cisco VPN3000/Cisco ASA GW VID Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total le ngth : 368 Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE DECODE RECEIVED Message (msgid=0) with payloads : HDR + HASH (8) + NOTIFY (11) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 116 Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin q hash pavload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing hash for ISAKMP Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g notify payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processin g IOS/PIX Vendor ID payload (version: 1.0.0, capabilities: 00000408) Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Received Cisco Unity client VID Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing blank hash payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing qm hash payload Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=e8a 1816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 68 Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=e8 al816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 84 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, process_a ttr(): Enter! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processin

g MODE_CFG Reply attributes. Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: primary DNS = cleared Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: secondary DNS = cleared Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: primary WINS = cleared Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: secondary WINS = cleared Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: IP Compression = disabled Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: Split Tunneling Policy = Disabled Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: Browser Proxy Setting = no-modify Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: Browser Proxy Bypass Local = disable Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = ciscol23, IP = 192.168 .1.2, User (ciscol23) authenticated. Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing blank hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing qm hash payload Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=143 60de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 60 Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=14 360de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 56 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, process_attr(): Enter! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Processing cfg ACK attributes Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=26 63aldd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 193 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, process_attr(): Enter! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Processing cfg Request attributes Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for IPV4 address! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for IPV4 net mask! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for DNS server address! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for WINS server address! Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = ciscol23, IP = 192.168 .1.2, Received unsupported transaction mode attribute: 5 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Banner! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Save PW setting! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Default Domain Name! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = ciscol23, IP = 1 92.168.1.2, MODE_CFG: Received request for Split Tunnel List! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = ciscol23, IP = 1 92.168.1.2, MODE_CFG: Received request for Split DNS! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for PFS setting! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Client Browser Proxy Setting! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for backup ip-sec peer list! Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168

.1.2, Received unknown transaction mode attribute: 28684 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Application Version! Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Client Type: WinNT Client Application Version: 5.0.03.0530 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for FWTYPE! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for DHCP hostname for DDNS is: Wireless12 3! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for UDP Port! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Obtained IP addr (192.168.5.1) prior to initiating Mode Cfg (XAuth e nabled) Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Assigned private IP address 192.168.5.1 to remote user Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing blank hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Send Client Browser Proxy Attributes! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Browser Proxy set to No-Modify. Browser Proxy data will NOT be inclu ded in the mode-cfg reply Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing qm hash payload Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE DECODE SENDING Message (msqid=266 3aldd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 158 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = ciscol23, IP = 192.168 .1.2, PHASE 1 COMPLETED Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, Keep-alive type for this connection: DPD Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Starting P1 rekey timer: 950 seconds. Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, sending notify message Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing blank hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing qm hash payload Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=f44 35669) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 84 Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=54 1f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 1022 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = ciscol23, IP = 1 92.168.1.2, processing hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing SA payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = ciscol23, IP = 1 92.168.1.2, processing nonce payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing ID payload Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Received remote Proxy Host data in ID Payload: Address 192.168.5.1, Proto col 0, Port 0 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = ciscol23, IP = 1 92.168.1.2, processing ID payload Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = ciscol23, IP = 192.168 .1.2, Received local IP Proxy Subnet data in ID Payload: Address 0.0.0.0, Mask

0.0.0.0, Protocol 0, Port 0 Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = ciscol23, IP = 192.168 .1.2, QM IsRekeyed old sa not found by addr Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, IKE Remote Peer configured for crypto map: dynmap Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing IPSec SA payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IPSec SA Proposal # 14, Transform # 1 acceptable Matches global IPS ec SA entry # 10 Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = ciscol23, IP = 192.168 .1.2, IKE: requesting SPI! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKE got SPI from key engine: SPI = 0x31de01d8 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, oakley constucting quick mode Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing blank hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing IPSec SA payload Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = ciscol23, IP = 192.168 .1.2, Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 secon ds Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing IPSec nonce payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing proxy ID Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Transmitting Proxy Id: Remote host: 192.168.5.1 Protocol 0 Port 0 Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Sending RESPONDER LIFETIME notification to Initiator Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing qm hash payload Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=541 f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 176 Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=54 1f8e43) with payloads : HDR + HASH (8) + NONE (0) total length : 48 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, loading all IPSEC SAs Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Generating Quick Mode Key! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Generating Quick Mode Key! Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = ciscol23, IP = 192.168 .1.2, Security negotiation complete for User (cisco123) Responder, Inbound SPI = 0x31de01d8, Outbound SPI = 0x8b7597a9 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKE got a KEY_ADD msg for SA: SPI = 0x8b7597a9 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = ciscol23, IP = 1 92.168.1.2, Pitcher: received KEY_UPDATE, spi 0x31de01d8 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Starting P2 rekey timer: 27360 seconds. Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Adding static route for client address: 192.168.5.1 Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, PHASE 2 COMPLETED (msgid=541f8e43) Jan 22 22:21:41 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=78 f7d3ae) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 8 0

ASA#debug crypto ipsec 7

!--- Deletes the old SAS. ASA# IPSEC: Deleted inbound decrypt rule, SPI 0x7F3C985A Rule ID: 0xD5567DB0 IPSEC: Deleted inbound permit rule, SPI 0x7F3C985A Rule ID: 0xD4EF1DF0 IPSEC: Deleted inbound tunnel flow rule, SPI 0x7F3C985A Rule ID: 0xD556AF60 IPSEC: Deleted inbound VPN context, SPI 0x7F3C985A VPN handle: 0x0004678C IPSEC: Deleted outbound encrypt rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: Deleted outbound permit rule, SPI 0xC921E280 Rule ID: 0xD5123250 IPSEC: Deleted outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 !--- Creates new SAs. ASA# IPSEC: New embryonic SA created @ 0xD4EF2390, SCB: 0xD4EF22C0, Direction: inbound SPI : 0x7F3C985A Session ID: 0x0000F000 VPIF num : 0x00000002 Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: New embryonic SA created @ 0xD556B118, SCB: 0xD556B048, Direction: outbound SPI : 0xC921E280 Session ID: 0x0000F000 VPIF num : 0x00000002 Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0xC921E280 IPSEC: Creating outbound VPN context, SPI 0xC921E280 Flags: 0x00000005 SA : 0xD556B118 SPI : 0xC921E280 MTU : 1500 bytes VCID : 0x00000000 Peer : 0x00000000 SCB : 0x0133B741 Channel: 0xD4160FA8 IPSEC: Completed outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 IPSEC: New outbound encrypt rule, SPI 0xC921E280 Src addr: 0.0.0.0 Src mask: 0.0.0.0 Dst addr: 192.168.5.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false SPI: 0x0000000 Use SPI: false IPSEC: Completed outbound encrypt rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: New outbound permit rule, SPI 0xC921E280 Src addr: 192.168.1.1 Src mask: 255.255.255.255 Dst addr: 192.168.1.2 Dst mask: 255.255.255.255 Src ports Upper: O Lower: O Op : ignore Dst ports Upper: O Lower: O Op : ignore Protocol: 50 Use protocol: true SPI: 0xC921E280 Use SPI: true IPSEC: Completed outbound permit rule, SPI 0xC921E280 Rule ID: 0xD5123250 IPSEC: Completed host IBSA update, SPI 0x7F3C985A IPSEC: Creating inbound VPN context, SPI 0x7F3C985A Flags: 0x00000006 SA : 0xD4EF2390 SPI : 0x7F3C985A MTU : 0 bytes VCID : 0x00000000 Peer : 0x00040AB4 SCB : 0x0132B2C3 Channel: 0xD4160FA8 IPSEC: Completed inbound VPN context, SPI 0x7F3C985A VPN handle: 0x0004678C IPSEC: Updating outbound VPN context 0x00040AB4, SPI 0xC921E280 Flags: 0x00000005 SA : 0xD556B118 SPI : 0xC921E280 MTU : 1500 bytes VCID : 0x00000000 Peer : 0x0004678C SCB : 0x0133B741 Channel: 0xD4160FA8 IPSEC: Completed outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 IPSEC: Completed outbound inner rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: Completed outbound outer SPD rule, SPI 0xC921E280 Rule ID: 0xD5123250 IPSEC: New inbound tunnel flow rule, SPI 0x7F3C985A Src addr: 192.168.5.1 Src mask: 255.255.255.255 Dst addr: 0.0.0.0 Dst mask: 0.0.0.0 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false SPI: 0x00000000 Use SPI: false IPSEC: Completed inbound tunnel flow rule, SPI 0x7F3C985A Rule ID: 0xD556AF60 IPSEC: New inbound decrypt rule, SPI 0x7F3C985A Src addr: 192.168.1.2 Src mask: 255.255.255.255 Dst addr: 192.168.1.1 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: 0x7F3C985A Use SPI: true IPSEC: Completed inbound decrypt rule, SPI 0x7F3C985A Rule ID: 0xD5567DB0 IPSEC: New inbound permit rule, SPI 0x7F3C985A Src addr: 192.168.1.2 Src mask: 255.255.255.255 Dst addr: 192.168.1.1 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: 0x7F3C985A Use SPI: true IPSEC: Completed inbound permit rule, SPI 0x7F3C985A Rule ID: 0xD4EF1DF0 適用於Windows的VPN使用者端5.0

選擇Log > Log settings以啟用VPN客戶端中的日誌級別。



選擇Log > Log Window以檢視VPN客戶端中的日誌條目。

VPN Client Log Window			
Cisco Systems VPN Client Version 5.0.03.0530 Copyright (C) 1998-2007 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Windows, WinNT Running on: 5.1.2600 Service Pack 2	<u> </u>		
1 12:33:57.906 01/23/09 Sev=Info/4IKE/0x63000001 IKE received signal to terminate VPN connection			
2 12:33:57.906 01/23/09 Sev=Info/4IKE/0x63000013 SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 192.168.1.1			
3 12:33:57.906 01/23/09 Sev=Info/4IKE/0x63000049 Discarding IPsec SA negotiation, MsgID=9CB18482			
4 12:33:58.031 01/23/09 Sev=Info/4IKE/0x63000017 Marking IKE SA for deletion (I_Cookie=017A1BBFAA4B6C12 R_Cookie=0A18652E60468C00) reason = DEL_REASON_RESET_SADB			
5 12:33:58.031 01/23/09 Sev=Info/4IKE/0x63000013 SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 192.168.1.1			
6 12:34:00.500 01/23/09 Sev=Info/4IKE/0x6300004B Discarding IKE SA negotiation (I_Cookie=017A1BBFAA4B6C12 R_Cookie=0A18652E60468C00) reason = DEL_REASON_RESET_SADB			
7 12:34:00.546 01/23/09 Sev=Info/4IPSEC/0x63700013 Delete internal key with SPI=0x2b5ec2c2			
8 12:34:00.546_01/23/09_Sev=Info/4IPSEC/0x6370000C Key deleted by SPI 0x2b5ec2c2			
9 12:34:00.546 01/23/09 Sev=Info/4IPSEC/0x63700013			
Save Log Settings Clear	Close		

相關資訊

- Cisco ASA 5500系列自適應安全裝置支援頁
- Cisco ASA 5500系列自適應安全裝置命令參考
- Cisco PIX 500系列安全裝置支援頁面
- Cisco PIX 500系列安全裝置命令參考
- 思科調適型資安裝置管理員
- IPsec協商/IKE通訊協定支援頁面