使用SDM配置作為遠端VPN伺服器的Cisco路由器 示例

目錄

<u>簡企業採慣設網設驗相</u> <u>必需採用例定路定證關</u> <u>個</u>定路定證關 <u>資</u>

<u>簡介</u>

本文檔介紹如何使用<u>Cisco安全裝置管理器(SDM</u>)將Cisco路由器配置為充當<u>Easy VPN伺服器</u>。 Cisco SDM允許您使用易於使用的基於Web的管理介面將路由器配置為Cisco VPN客戶端的VPN伺 服器。Cisco路由器配置完成後,可以使用Cisco VPN客戶端進行驗證。

<u>必要條件</u>

<u>需求</u>

本檔案假設Cisco路由器已完全運行並配置為允許Cisco SDM進行配置更改。

注意:請參閱<u>允許SDM進行HTTPS訪問</u>,以便允許SDM配置路由器。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- •採用Cisco IOS®軟體版本12.3(14T)的Cisco 3640路由器
- 安全裝置管理員版本2.31
- Cisco VPN使用者端版本4.8

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。

慣例

```
<mark>請參閱<u>思科技術提示慣例以瞭解更多有關文件慣例的資訊。</u></mark>
```

<u>設定</u>

本節提供配置Easy VPN伺服器功能的資訊,該功能允許遠端終端使用者使用IPsec與任何Cisco IOS® VPN網關通訊。

註:使用Command Lookup Tool(僅供已註冊客戶使用)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:



設定程式

完成以下步驟,使用SDM將Cisco路由器配置為遠端VPN伺服器。

1. 從主視窗中選擇Configure > VPN > Easy VPN Server,然後按一下Launch Easy VPN Server Wizard。



2. 啟動Easy VPN伺服器配置之前,必須在路由器上啟用AAA。按一下「**Yes**」以繼續設定。視窗中顯示「AAA has been successfully enabled on the router」消息。按一下**OK**以啟動Easy VPN伺服器配置。

Enable AAA	×
	AAA is disabled on the router. AAA must be enabled to configure Easy VPN Server.SDM will perform the following precautionary tasks while enabling AAA to prevent loss of access to the router.
	* Configure authentication and authorization for vty lines. The local database will be used for both authentication and authorization. * Configure authentication for the console line. The local database will be used for authentication.
	Do you want to enable AAA?
	Yes No

3. 按一下下一步啟動Easy VPN伺服器嚮導。



4. 選擇客戶端連線終止的介面和身份驗證型別。

Cancel

Help

VPN Wizard	Interface and Authentication
	Interface
	Please select the interface on which the Easy VPN Server should be configured. Easy VPN clients will connect to the server through this interface.
	Interface for this Easy VPN Server: Serial2/0 Details
	Authentication
P rod	Select the method used for authenticating VPN clients connecting to this Easy VPN Server.
	Pre-shared keys C Digital Certificates C Both
	Interface connected to Internet. This is the interface where the VPN connections from the VPN clients will terminate. Internet

5. 按一下**下一步**以配置Internet金鑰交換(IKE)策略,並使用**Add**按鈕建立新策略。通道兩端的設 定必須完全相符。但是,Cisco VPN客戶端會自動為自己選擇正確的配置。因此,客戶端PC上 無需進行IKE配置。

Easy VPN Server Wizard - 20	% Complete		11 mar 1			
VPN Wizard	IKE Proposals IKE proposals method that is device. Click the Add.	specify the er used by this . button to add	ncryption alg router when I more polici	orithm, authentica negotiating a VPN es and the Edit I	tion algorithm ar I connection with outton to edit an e	nd key exchange the remote existing policy.
	Priority	Encryption	Hash	D-H Group	Authentication	Type
	1	3DES	SHA_1	group2	PRE_SHARE	User Defined
RA			1			
	Add	Edit]			

 按一下下一步選擇預設轉換集或新增新的轉換集以指定加密和身份驗證演算法。在這種情況下 ,將使用預設轉換集。

VPN Wizard Transform Set A transform set specifies the encryption and authentication algorithms used to prote data in the VPN tunnel.					ns used to protect the
	Click the transform Select T	a Add button to add m set. Fransform Set. IDM Default Transfor	a new transform se n Set	t and the Edit butt	on to edit the specified
	Deta	IIs of the specified tr Name ESP-3DES-SHA1	ESP Encryption ESP_3DES	ESP Integrity ESP_SHA_HMAC	AH Integrity
	- -	Add Edit			Þ

7. 按一下**下一步**,為組策略查詢建立新的身份驗證、授權和記帳(AAA)授權網路方法清單,或選 擇用於組授權的現有網路方法清單。

An ISAKMP client configuration group (or VPN group) is a group of VPN clients that share the same authentication and configuration information. Group policies can be configured locally on this router, an external server, or both. Easy VPN Server will use these group policies to authenticate VPN clients. Method List for Group Policy Lookup Select the servers on which group policies will be configured, or select an existing AAA policy that defines the servers used for configuring group policies. • Local • RADIUS • RADIUS and local • Select an existing AAA method list • Select an existing AAA method list • Select an entry • Local • Select an existing AAA method list • Select an entry • The local database will be used for group authorization. This option is recommended if you do not have a RADIUS or TACACS+ server in your network.	VPN Wizard	Group Authorization and Group Policy Lookup	
C RADIUS and local Select an existing AAA method list Add RADIUS Server Summary The local database will be used for group authorization. This option is recommended if you do not have a RADIUS or TACACS+ server in your network.	VPN WIZalu	An ISAKMP client configuration group (or VPN grous same authentication and configuration informatio on this router, an external server, or both. Easy VP authenticate VPN clients. Method List for Group Policy Lookup Select the servers on which group policies will be policy that defines the servers used for configurin C Local C RADIUS	up) is a group of VPN clients that share the n. Group policies can be configured locally 'N Server will use these group policies to e configured, or select an existing AAA ig group policies.
Add RADIUS Server Summary The local database will be used for group authorization. This option is recommended if you do not have a RADIUS or TACACS+ server in your network.		C RADIUS and local	-Select an entry
	DA	Summary The local database will be used for group authorit you do not have a RADIUS or TACACS+ server in t	add RADIUS Server

8. 在Easy VPN伺服器上配置使用者身份驗證。您可以將使用者驗證詳細資訊儲存到外部伺服器 (例如RADIUS伺服器或本機資料庫,或兩者均有)上。AAA登入身份驗證方法清單用於確定 搜尋使用者身份驗證詳細資訊的順序。

Easy VPN Server Wizard -	65% Complete	×
VPN Wizard	User Authentication (XAuth) User authentication (KAuth) provides additional se after the device has undergone IKE authentication. locally on this router, on an external server, or both	curity by authenticating the user of a device User credentials XAuth can be configured
	Enable User Authentication Select the servers that will be used for configuring AAA policy that defines the servers used for config	user credentials, or select an existing wring user credentials.
	C RADIUS and Local Only	Add RADIUS Server
	Summary Local database will be used for user authenticatio	Add User Credentials
	< Ba	ck Next > Finish Cancel Help

9. 此視窗允許您在本地資料庫上新增、編輯、克隆或刪除使用者組策略。

Easy VPN Server Wizard - 80	% Complete				×
VPN Wizard	Group Authorizat The Easy VPN Se other Easy VPN R clients or device th the remote client of Click the Add bu Clone button to	ion and User G rver allows you emote client pr nat is part of a g or device to ens tton to add mor create a new gr	roup Policies to group remote oducts. The grou given group. The ure that appropri e groups, the Ed oup from an exis	users who are u p attributes will t same group nan ate group attribu it button to edit ting group.	sing Cisco VPN clients or be downloaded through the ne should be configured on tes are downloaded. an existing group, or the
	Group Name Group Name Add Configure a time cleared. Idle Timer:	Pool Edit	DNS	Iete	Domain Name
			< Ba	ack Next > F	inish Cancel Help

10. 輸入隧道組名稱的名稱。提供用於身份驗證資訊的預共用金鑰。建立新池或選擇用於將IP地 址分配給VPN客戶端的現有池。

Jama of This Group:		
varne of this Group.	Vpn	
Pre-shared keys		
Specify the key that will be us	ed to authenticate the clients associated with this group	
Current Key:	<none></none>	
Enter new pre-shared key:		
Reenter new pre-shared key:	c	
Specify a local pool containin internal IP address to a client	ng a range of addresses that will be used to allocate an .t.	
Specify a local pool containin internal IP address to a client © Create a new pool	ng a range of addresses that will be used to allocate an it. C Select from an existing pool	
 Specify a local pool containin internal IP address to a client Create a new pool Starting IP address: 192. 	ng a range of addresses that will be used to allocate an it. C Select from an existing pool 168.2.1	Is
 Specify a local pool containin internal IP address to a client Create a new pool Starting IP address: 192. 	ng a range of addresses that will be used to allocate an it. C Select from an existing pool .168.2.1 	IS
Specify a local pool containin internal IP address to a client Create a new pool Starting IP address: 192. Ending IP address: 192.1	ng a range of addresses that will be used to allocate an it. C Select from an existing pool .168.2.1 168.2.5	IS
Specify a local pool containin internal IP address to a client Create a new pool Starting IP address: 192. Ending IP address: 192.1 Enter the subnet mask that st	ng a range of addresses that will be used to allocate an C Select from an existing pool .168.2.1 168.2.5 should be sent to the client along with the IP address.	IS
Specify a local pool containin internal IP address to a client Create a new pool Starting IP address: 192.1 Ending IP address: 192.1 Enter the subnet mask that si Subnet Mask: 255.2	ng a range of addresses that will be used to allocate an C Select from an existing pool .168.2.1 168.2.5 should be sent to the client along with the IP address. .255.255.0 (Optional)	IS
Specify a local pool containin internal IP address to a client Create a new pool Starting IP address: 192.1 Ending IP address: 192.1 Enter the subnet mask that sl Subnet Mask: 255.2	ng a range of addresses that will be used to allocate an C Select from an existing pool .168.2.1 168.2.5 should be sent to the client along with the IP address. .255.255.0 (Optional)	IS

11. 此視窗顯示您已採取的操作的摘要。如果對配置滿意,請按一下Finish。

VPN Wizard Summary of the Configuration Click finish to deliver the configuration to the router. Image: Click finish to deliver the configuration to the router. Image: Click finish to deliver the configuration to the router. Image: Click finish to deliver the configuration to the router. Image: Click finish to deliver the configuration to the router. Image: Click finish to deliver the configuration to the router. Image: Click finish to deliver the configuration to the router. Image: Click finish to deliver the configuration to the router. Image: Click finish to deliver the configuration to the router. Image: Click finish to deliver the configuration to the router. Image: Click finish to deliver the configuration to the router. Image: Click finish to deliver the configuration to the router. Image: Click finish to deliver the configuration to the router. Image: Click finish to deliver the configuration to the router. Image: Click finish to deliver the configuration. Image: Click finish to deliver. Image: Click fi	Easy VPN Server Wizard - 90	% Complete			X
Click finish to deliver the configuration to the router.	VPN Wizard	Summary of the Configuration			
IKE Policies: Hash DH Group Authentication Encryption SHA_1 group2 PRE_SHARE 3DES Transform Set Name: ESP-3DES-SHA1 ESP Encryption: ESP_3DES ESP Integrity: ESP_SHA_HMAC Mode: TUNNEL Group Policy Lookup Method List : Local User Authentication Method List : Local Idle Timer : <none> Number of Group Policies : 1 Group Policy Name : vancilent T Test VPN connectivity after configuring.</none>		Click finish to deliver the configuration to th	e router.		
Hash DH Group Authentication Encryption SHA_1 group2 PRE_SHARE 3DES Transform Set Name: ESP-3DES-SHA1 ESP Encryption: ESP_3DES ESP Integrity: ESP_SHA_HMAC Mode: TUNNEL Group Policy Lookup Method List : Local User Authentication Method List : Local Idle Timer : «NONE> Number of Group Policies :1 Group Policy Name : wonclient Test VPN connectivity after configuring.		IKE Policies:			-
SHA_1 group2 PRE_SHARE 3DES Transform Set Name: ESP-3DES-SHA1 ESP Encryption: ESP_3DES ESP Integrity: ESP_SHA_HMAC Mode: TUNNEL Group Policy Lookup Method List : Local User Authentication Method List : Local Idle Timer : <none> Number of Group Policies :1 Group Policy Name :vonclient Image: Test VPN connectivity after configuring.</none>		Hash DH Group	Authentication	Encryption	
Transform Set Name: ESP-3DES-SHA1 ESP Encryption: ESP_3DES ESP Integrity: ESP_SHA_HMAC Mode: TUNNEL Group Policy Lookup Method List : Local User Authentication Method List : Local Idle Timer : <none> Number of Group Policies : 1 Group Policy Name : venciont Test VPN connectivity after configuring.</none>		SHA_1 group2	PRE_SHARE	3DES	
Image: Stream Policy Name : 1 Image: Stream Policy Name : vnnclient Image: Stream Policy N		Transform Set Name: ESP-3DES-SHA1 ESP Encryption: ESP_3DES ESP Integrity: ESP_SHA_HMAC Mode: TUNNEL Group Policy Lookup Method List User Authentication Method List Idle Timer	: Local : Local : <none></none>		
Test VPN connectivity after configuring.		Group Policies	: 1 		×.
< Back Next > Finish Cancel Help		Test VPN connectivity after configuring.	< Back Next	Finish [Ĉ	2

12. SDM將組態傳送到路由器以更新執行組態。按一下「OK」以完成。

ommands Delivery Status	×
Command Delivery Status:	
Preparing commands for delivery Submitting 27 commands, please wait Configuration delivered to router.	*
I	
OK	

13. 完成後,您可以根據需要編輯和修改配置中的更改。



<u>驗證</u>

嘗試使用Cisco VPN Client連線到Cisco路由器,以驗證Cisco路由器是否配置成功。

1. 選擇Connection Entries > New。

👶 status: Disconnected	VPN Client - Version 4.8.0)1.0300	
Connection Entries Status	Certificates Log Options	Help	
Connect New	Import Modify) Delete	CISCO SYSTEMS
Connection Entries Certific	cates Log		
Connection Entry	∇	Host	Transport
•			•
Not connected.			

2. 填寫新連線的詳細資訊。Host(主機)欄位應包含Easy VPN伺服器(Cisco路由器)的隧道終 點的IP<u>地址或主機名。 Group Authentication</u>資訊應對應於步驟9中使用的資訊。完成後按一下

Description:			50
Host	10.1.1.1		
Authentication	Transport Backu	pServers Dial-Up	
Group Authen	tication	C Mutual Gr	oup Authentic
Name:	vpn		
Password:	*****		
Confirm Passw	ord: [******		
C Certificate Aut	hentication		
Name:		Y	
C Send CA C	ertificate Chain		

3. 選擇新建立的連線,然後按一下Connect。

Connection En	tries Status	Certificates	Log Options	Help				
Connect	tew New	F R	Modify	X Delete				Cisco Syste
Connection Er	ntries Cer	tificates Lo	g					
	Connection	Entry 🛆		ł	Host			Transport
	vpn			1	0.1.1.1			IPSec/UDP
•								
Not connected	131-							
入用於延伯	伸驗證(Xa	auth)的使用	者名稱和密	密碼。 此資	資訊取決	於步驟7	′中的Xai	uth引數。
〕 〕 〕	伸驗證(Xa	auth)的使用	者名稱和密	招碼。 此道 Help	資訊取決	於步驟7	′中的Xai	uth引數。
前入用於延付 う status: Di Connection En Cancel Conne Connection E	伸驗證(Xa sconnecter htries Statu ct New ntries Cer	auth)的使用 d VPN Client s Certificates 『『 Import ttificates Lo	者名稱和密 Coversion do Log Options Modify	종碼。此 9 601.0300 5 Help Delete	資訊取決	於步驟7	'中的Xai	uth引數。 IC Cisco Srst
前入用於延伯 う status: Die Connection En Cancel Conne Connection E	伸驗證(Xa sconnected atries Statu ect New ntries Cer	auth)的使用 d VPN Clien s Certificates 『『 Import rtificates Lo	者名稱和密 Cog Options Log Options Modify	容碼。此 8.01.0300 5 Help Delete	資訊取決 Host	於步驟7	'中的Xai	uth引數。 — IC Cisco Syst
前入用於延(2) status: Di Connection En Cancel Conne Connection E	伸驗證(Xa sconnector htries Statu ect New ntries Cer Connection vpn	auth)的使用 d VPN Clien s Certificates 『記』 Import rtificates Lo n Entry /	者名稱和密 Log Options Modify	聲碼。此 9.01.0300 5 Help ∑elete	資訊取決 Host 10.1.1.1	<u>於步驟7</u>	'中的Xai	uth引數。 Lisco Sysy Transport IPSec/UDP
前入用於延(2) status: Di Connection En Cancel Conne Connection E	伸驗證(Xa sconnector itries Statu ect New ntries Cer Connection vpn	auth)的使用 d VPN Clien s Certificates 『副 Import rtificates Lo n Entry 人	者名稱和密 Log Options Modify	容碼。此會 6.01.0300 5 Help Delete	資訊取決 Host I0.1.1.1 ntication	於步驟7 for "vpn"	'中的Xai	uth引數。 Lisco Syst Lisco Sys
前入用於延([●] status: Di [●] connection Er [●] Connection E [●] Connection E	伸驗證(Xa sconnector htries Statu ect New ntries Cer Connection vpn	auth)的使用 d VPN Clien s Certificates 『『 Import rtificates Lo n Entry /	者名稱和密 Ce Version 4.3 Log Options Modify g	容碼。此會 6.01.0300 5 Help Delete	資訊取決 Host I0.1.1.1 ntication	於步驟7 for "vpn" ormation to	'中的Xau complete t	uth引數。 Cisco Srsr Cisco Srsr Transport IPSec/UDP X he user
前入用於延 の status: Di Connection Er Cancel Conne Connection E	伸驗證(Xa sconnector htries Statu ect New ntries Cer Connection vpn	auth)的使用 d VPN Clien s Certificates 『『 Import rtificates Lo n Entry /	a 名 稱 和 密 Log Options Modify PN Client L server has requestion. SCO SYSTEMS	容碼。此道 9.01.0300 5 Help Delete Delete	資訊取決 Host I0.1.1.1 ntication ollowing info	於步驟7 for "vpn" xmation to	で中的Xai	uth引數。 Cisco Syst Cisco Syst Transport IPSec/UDP X he user
前入用於延付 a status: Di Connection Er Cancel Conne Connection E	伸驗證(Xa sconnector ntries Statu ect New ntries Cer Connection vpn	auth)的使用 d VPN Clien s Certificates 『』 Import rtificates Lo n Entry /	される 古名和和密 Log Options Modify PN Client L server has requestion. SCO SYSTEMS	A碼。此道 Biol 1 0 3 0 0 S Help Delete User Auther Username Password	資訊取決 資訊取決 Host IO.1.1.1 ntication ollowing info	for "vpn"	r中的Xau	uth引數。 IC CISCO STST Luilliu
前入用於延 a status: Di Connection Er Cancel Conne Connection E	伸驗證(Xa sconnecter htries Statu ect New ntries Cer Connection ypn	auth)的使用 d VPN Clien s Certificates 『『』 Import ntificates Lo n Entry /	日本名稱和密 Log Options Log Options Modify PN Client L server has requestion. SEC SYSTEMS	4. 明子 Auther Biol 1 0 3 0 0 Si Help Delete Delete Username Username Password	資訊取決 資訊取決 Host IO.1.1.1 ntication ollowing info	於步驟7 for "vpn" xmation to	r中的Xau	uth引數。 if Cisco Syst iiiiiii Transport IPSec/UDP he user
前入用於延([●] status: Di Connection Er Cancel Conne Connection E	伸驗證(Xa sconnector htries Statu ect New ntries Cer Connection vpn	auth)的使用 d VPN Clien s Certificates 『『 Import rtificates Lo n Entry /	古名和和密 た Version (Log Options Modify 9 PN Client L server has requestication. SCO SYSTEMS 1111000000000000000000000000000000000	4. Fassword:	資訊取決 資訊取決 Host IO.1.1.1 ntication ollowing info	於步驟7 for "vpn" armation to	で中的Xau complete t	uth引數。 Cisco Syst Cisco Syst Transport IPSec/UDP X he user

5. 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。此視窗顯示流量和加



6. 選擇Log > Log Settings以啟用Cisco VPN客戶端中的日誌級別。

) :



7. 選擇Log > Log Windows以檢視Cisco VPN客戶端中的日誌條目。

Cisco Systems VPN Dient Version 4.8.01.0300 Copyright (C) 1998-2005 Disco Systems, Inc. All Rights Reserved. Client Type(s): Windows, WinNT Running on: 50.2195 Service Pack 4. 227 10:39.32.150 05/31/06 Sev=Info/6 IKE/0x6300003B Attempting to establish a connection with 10.1.1.1. 228 10:39.32.156 05/31/06 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP 0AK A6 [SA, KE, NON, ID, VID(Xauth), VID(dpd), VID(Frag), VID(Nat-T), VID(Unity)) to 10.1.1.1 10:39.32.156 05/31/06 Sev=Info/4 IPSEC/0x63700008 IPSec driver successfully started 230 10:39.32.156 05/31/06 Sev=Info/4 IPSEC/0x6370002C Sent 120 packets, 0 were fragmented. 232 10:39.33.921 05/31/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet peer = 10.1.1.1 233 10:39.33.921 05/31/06 Sev=Info/5 IKE/0x63000014 RECEIVING <<< ISAKMP packet peer = 10.1.1.1 234 10:39.33.921 05/31/06 Sev=Info/5 IKE/0x63000001 235 10:39.33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer is a Cisco-Unity compliant peer 235 10:39.33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer supports DVM Code and DVM Text 237 10:39.33.921 05/31/06 Sev=Info/5 IKE/0	VPN Client Log Window	×
227 10.39.32.140 05/31/06 Sev=Info/6 IKE/0x63000038 Attempting to establish a connection with 10.1.1.1 228 10.39.32.156 05/31/06 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP DAK AG (SA, KE, NON, ID, VID(Kauth), VID(dpd), VID(Frag), VID(Nat-T), VID(Unity)) to 10.1.1.1 19582/00008 229 10.39.32.156 05/31/06 Sev=Info/4 IPSEC/0x63700008 IPSec driver successfully started 230 10.39.32.156 05/31/06 Sev=Info/6 IPSEC/0x6370002C Sent 120 packets, 0 were fragmented. 101.1.1 232 10.39.32.156 05/31/06 Sev=Info/6 IPSEC/0x6370002C Sent 120 packets, 0 were fragmented. 102.32 10.39.33.921 05/31/06 Sev=Info/5 IKE/0x63000014 RECEIVING <<	Cisco Systems VPN Client Version 4.8.01.0300 Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Windows, WinNT Running on: 5.0.2195 Service Pack 4	•
228 10:39:32:156 05/31/06 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP 0AK AG [SA, KE, NON, ID, VID(Kauth), VID(dpd), VID(Frag), VID(Nat-T), VID(Unity)) to 10.1.1.1 229 10:39:32:156 05/31/06 Sev=Info/4 IPSEC/0x63700008 IPSec driver successfully started IPSEC/0x63700014 Deleted all keys 231 10:39:32:156 05/31/06 Sev=Info/6 IPSEC/0x6370002C Sent 120 packets, 0 were fragmented. IPSEC/0x6300002F Received ISAKMP packet: peer = 10.1.1.1 233 10:39:33:921 05/31/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 10.1.1.1 IKE/0x63000014 RECEMING <<	227 10:39:32.140 05/31/06 Sev=Info/6 IKE/0x6300003B Attempting to establish a connection with 10.1.1.1.	
229 10:39:32:156 05/31/06 Sev=Info/4 IPSEC/0x63700008 IPSec driver successfully started 230 10:39:32:156 05/31/06 Sev=Info/4 IPSEC/0x63700014 Deleted all keys 231 10:39:32:156 05/31/06 Sev=Info/6 IPSEC/0x6370002C Sent 120 packets, 0 were fragmented. IPSEC/0x6300002F 232 10:39:33:921 05/31/06 Sev=Info/5 IKE/0x63000014 Received ISAKMP packet peer = 10:1.1.1 IEE/0x63000014 RECEIVING <<<	228 10:39:32.156 05/31/06 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID(Kauth), VID(dpd), VID(Frag), VID(Nat-T), VID(Unity)) to 10.1.1.1	
230 10:39:32:156 05/31/06 Sev=Info/4 IPSEC/0x63700014 231 10:39:32:156 05/31/06 Sev=Info/6 IPSEC/0x6370002C Sent 120 packets, 0 were fragmented. IPSEC/0x6370002F 232 10:39:33:921 05/31/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 10:1.1.1 IKE/0x63000014 233 10:39:33:921 05/31/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<	229 10:39:32.156 05/31/06 Sev=Info/4 IPSEC/0x63700008 IPSec driver successfully started	
231 10:39:32:156 05/31/06 Sev=Info/6 IPSEC/0x6370002C Sent 120 packets, 0 were fragmented. 232 10:39:33:921 05/31/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet peer = 10.1.1.1 233 10:39:33:921 05/31/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<	230 10:39:32.156 05/31/06 Sev=Info/4 IPSEC/0x63700014 Deleted all keys	
232 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x6300002F Preceived ISAKMP packet peer = 10.1.1.1 233 10:39:33.921 05/31/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP 0AK AG (SA, VID(Unity), VID(dpd), VID(?), VID(Xauth), VID(Nat-T), KE, ID, NDN, HASH, NAT-D, NAT-D) from 10.1.1.1	231 10:39:32.156 05/31/06 Sev=Info/6 IPSEC/0x6370002C Sent 120 packets, 0 were fragmented.	
233 10.39.33.921 05/31/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP 0AK AG (SA, VID(Unity), VID(dpd), VID(?), VID(Xauth), VID(Nat-T), KE, ID, NON, HASH, NAT-D, NAT-D) from 10.1.1.1	232 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 10.1.1.1	
234 10.39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 235 10.39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 236 10.39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 236 10.39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 236 10.39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 237 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 238 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 238 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 239 10:39:33.937 05/31/06 Sev=Info/6 IKE/0x63000001	233 10:39:33.921 05/31/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP 0AK AG (SA, VID(Unity), VID(dpd), VID(?), VID(Xauth), VID(Nat-T), KE, ID, NON, HASH, NAT-D, NAT-D) from 10.1.1.1	
235 10.39.33.921 05/31/06 Sev=Info/5 IKE/0x63000001 236 10.39.33.921 05/31/06 Sev=Info/5 IKE/0x63000001 236 10.39.33.921 05/31/06 Sev=Info/5 IKE/0x63000001 237 10.39.33.921 05/31/06 Sev=Info/5 IKE/0x63000001 238 10.39.33.921 05/31/06 Sev=Info/5 IKE/0x63000001 238 10.39.33.921 05/31/06 Sev=Info/5 IKE/0x63000001 239 10.39.33.937 05/31/06 Sev=Info/6 IKE/0x63000001	234 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer is a Cisco-Unity compliant peer	
236 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer supports DWR Code and DWR Text 237 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 237 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer supports XAUTH 238 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 238 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer supports NAT-T 239 10:39:33.937 05/31/06 Sev=Info/6 IKE/0x63000001	235 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer supports DPD	
237 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer supports XAUTH 238 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 238 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer supports NAT-T 239 10:39:33.937 05/31/06 Sev=Info/6 IKE/0x63000001	236 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer supports DWR Code and DWR Text	
238 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer supports NAT-T 239 10:39:33.937 05/31/06 Sev=Info/6 IKE/0x63000001	237 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer supports XAUTH	
239 10:39:33.937 05/31/06 Sev=Info/6 IKE/0x63000001	238 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001 Peer supports NAT-T	
IDS Vendor ID Contruction successful	239 10:39:33.937 05/31/06 Sev=Info/6 IKE/0x63000001 IDS Vendor ID Contruction successful	•
Save Log Settings Clear Close	Save Log Settings Clear Close	1

相關資訊

- <u>下載和安裝思科路由器和安全裝置管理器</u>
- Cisco VPN使用者端支援頁面
- IPSec 協商/IKE 通訊協定
- 技術支援與文件 Cisco Systems