使用Configuration Professional將IOS路由器作為 Easy VPN伺服器配置示例

目錄

簡介 必要條件 採用元件 安裝Cisco CP 運行Cisco CP的路由器配置 需求 慣例 設定 網路圖表 Cisco CP - Easy VPN伺服器配置 CLI組態 驗證 Easy VPN伺服器 — show命令 疑難排解 相關資訊

<u>簡介</u>

本檔案介紹如何使用<u>Cisco Configuration Professional(Cisco CP)和CLI將Cisco IOS</u>[®]路由器設定為 Easy VPN(EzVPN)伺服器。Easy VPN Server功能允許遠端終端使用者使用IP安全(IPsec)與任何 Cisco IOS虛擬專用網路(VPN)網關通訊。伺服器將集中管理的IPsec策略「推送」到客戶端裝置 ,從而最大限度地減少了終端使用者的配置。

有關Easy VPN伺服器的詳細資訊,請參閱<u>安全連線配置指南庫Cisco IOS版本12.4T</u>的<u>Easy VPN伺</u> <u>服器</u>部分。

<u>必要條件</u>

<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12.4(15T)的Cisco 1841路由器
- Cisco CP版本2.1

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。

安裝Cisco CP

執行以下步驟以安裝Cisco CP:

- 1. 從<u>Cisco Software Center</u>(僅供<u>註冊</u>客戶使用)下載Cisco CP V2.1,然後將其安裝在本地PC上 。最新版本的Cisco CP可在<u>Cisco CP網站上找到</u>。
- 2. 從本地PC通過**開始 > 程式 > Cisco Configuration Professional(CCP)**啟動Cisco CP,然後選擇 具有您要配置的路由器的**Community**。

Application Help		
Home 👸 Configure	Monitor 😽	📄 🥹 Cisco
Select Community Members	K Home > Community	View
Company and a second second	🐻 Cisco Configuratio	on Professional News
Community View	Date	Title
	24-May-2010	Cisco Configuration Professional #2
	24-May-2010	Simplify ISR & ISR 62 deployments
	24-May-2010	Provide CCP Feedback
	formunity Informa	-time.
	Selected Community	New Community .Select a device from t
	Ø	
	IP address / Hostn	name Router Hostname
<pre></pre>	IP address / Hostr	name Router Hostname
1	IP address / Hostr	name Router Hostname
1	IP address / Hostn	name Router Hostname
	IP address / Hostr	name Router Hostname
1	IP address / Hostr	name Router Hostname
	IP address / Hostr	name Router Hostname
	IP address / Hostr	name Router Hostname
	IP address / Hostr	name Router Hostname
	IP address / Hostr	name Router Hostname
	IP address / Hostr	Delete Discovor



3. 若要探索您想要設定的裝置,請突出顯示路由器,然後按一下「Discover」。

Application Help		
Home & Configure	Monitor 8	📄 🙆 Cisco
Select Community Memberi	Home > Community 1	View
	🚺 Cisco Configuratio	on Professional News
Community View	Date	Title
	24-May-2010	Cisco Configuration Professional •
	24-May-2010	Simplify ISR & ISR 62 deployment
	24-May-2010	Provide CCP Feedback
	Community Informa	tion
	Community Informa	tion : New Community .Select a device from
	Community Informa Selected Community Printer	tion : New Community .Select a device from
	Community Informa Selected Community Pitter IP address / Hostn	tion : New Community .Select a device from ame Router Hostname
	Community Informa Selected Community Pifiter IP address / Hostn Router	tion : New Community .Select a desice from name Router Hostname
	Community Information Selected Community Piffitar IP address / Hostin Router	tion : New Community .Select a device from ame Router Hostname

注意:有關與Cisco CP v2.1相容的Cisco路由器型號和IOS版本的資訊,請參閱<u>相容Cisco IOS版本</u> 部分。

註:有關運行Cisco CP v2.1的PC要求的資訊,請參閱<u>系統要求</u>部分。

運行Cisco CP的路由器配置

要在Cisco路由器上運行Cisco CP,請執行以下步驟:

- 1. 使用Telnet、SSH或通過控制檯連線到路由器。使用以下命令進入全域性配置模式: Router(config)#**enable** Router(config)#
- 2. 如果啟用了HTTP和HTTPS並將其配置為使用非標準埠號,則可以跳過此步驟,只使用已配置 的埠號。使用以下Cisco IOS軟體命令啟用路由器HTTP或HTTPS伺服器: Router(config)# ip http server Router(config)# ip http secure-server Router(config)# ip http secure-server Router(config)# ip http authentication local
- 3. 建立許可權級別為15的使用者: Router(config)# username privilege 15 password 0

注意:將<username> 和<password>替換為要配置的使用者名稱和密碼。

- 4. 為本地登入和許可權級別15配置SSH和Telnet。 Router(config)# line vty 0 4 Router(config-line)# privilege level 15 Router(config-line)# login local Router(config-line)# transport input telnet Router(config-line)# transport input telnet ssh Router(config-line)# transport input telnet ssh
- 5. (可選) 啟用本地日誌記錄以支援日誌監控功能: Router(config)# logging buffered 51200 warning

<u>需求</u>

本文檔假定Cisco路由器已完全運行並配置為允許Cisco CP更改配置。

有關如何開始使用Cisco CP的完整資訊,請參閱Cisco Configuration Professional入門。

<u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

<u>設定</u>

本節提供為網路中的路由器配置基本設定的相關資訊。

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。

網路圖表

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<u>RFC 1918</u>,已在實驗室環境 中使用。

<u>Cisco CP - Easy VPN伺服器配置</u>

執行以下步驟,將Cisco IOS路由器配置為Easy VPN伺服器:

1. 選擇Configure > Security > VPN > Easy VPN Server > Create Easy VPN Server,然後點選 Launch Easy VPN Server Wizard,將Cisco IOS路由器配置為Easy VPN伺服器



2. 按一下Next以繼續Easy VPN Server配置。



3. 在出現的視箇中,**虛預介面**將配直為Easy VPN伺服器配直的一部分。提供虛**預通道介面的** IP**位址**,並選擇用於驗證VPN使用者端的驗證方法。此處,**預共用金鑰**是使用的身份驗證方法 。按一下「Next」

Easy VPN Server Wizard -	10% Complete		
VPN Wizard	Interface and Authentication Interface A virtual template interface will & Any Cisco IOS feature that shou the VPIN tunnel can be configure	oc proated as part of this Easy IId be applied before encryptio ed on this Interface.	√PN Berver configuration. n to the traffic gcing into
	IP Address of Virtual Tunnel in:	erface	
	IP Address	Loophack Interface	
	Subnet Mask.	255.255.255.0	cr 24
	C Urmumbered to	FastEthernet0/0	Cetails
A	Authentication Select the method used for auth VPN Server.	nenticating VPIN clients connec	tin <u>c</u> to this Easy
	Pre-shared Keys	C Digital Certificates	C Bult
		< Back Mext >	Finish Cancel Help

4. 指定此**路由器在與遠端裝置協商時**要使用的加密演算法、身份驗證演算法和金鑰交換方法。路 由器上存在預設IKE策略,如果需要,可以使用它。如果要新增新的IKE策略,請按一下Add。

Easy VPN Server Wizard -	20% C	omplete					
VPN Wizard	IKE Proposals IKE proposals specify the encryption algorithm, authentication algorithm and key exc method that is used by this router when negotiating a VPN connection with the remo- device. Click the Add – button to add more policies and the Edit – button to edit an existing pu					id key exchange the remote existing policy	
		Priority	Encryption	Hash	E-H Group	Authentication	Туре
	1	1	3DES	SHA 1	group2	PRE SHARE	Cisco CP Defau
		\dd	Edit				
					< Back Nex	l> Finish (ancel Help

- 5. 提供Encryption Algorithm、Authentication Algorithm和Key Exchange method(如此處所示),然後按一下

Add IKE Policy	
Configure IKE Policy	
Priority:	Authentication:
Encryption:	D-H Group: group1
Hash:	Lifetime: 24 0 0 HH:MM:SS
	Cancel Heip

6. 本示例中使用的是**預設IKE策略**。因此,選擇預設IKE策略並按一下**Next**。

Easy VPN Server Wizard	20% Complete

VPN Wizard

IKE Proposale

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device.

Click the Add - button to add more policies and the Edit - button to edit an existing policy.

P1ority	Encryption 3DES	Hash SHA 1	E-H Group group 2	Authentication	TYpe Claco CP Defau	
Add	Edit					
			< Back Nex	Finish 0	ancel Help	

7. 在新視窗中,應提供轉換集詳細資訊。轉換集指定用於保護VPN隧道中的資料的加密和身份驗 證演算法。按一下「Add」以提供這些詳細資訊。按一下Add並提供詳細資訊時,可以根據需 要新增任意數量的轉換集。附註: 使用Cisco CP配置時,預設情況下路由器上會顯示CP默認 轉換集。

Easy VPN Server Wizard -	35% Complete				×
VPN Wizard	Traneform Set A transform set specifies the e data in the VPN tunnel.	ncryption and aul	hentication algorthm	is used to protect the	
	Click the Add button to acd a transform set.	new transform se	et and the Edil kuto	n to ecit the specified	
	Select Transform Set — Cisco CP Default Trans Details of the specified tran	form Get 🛛 🔽 –			
	Name	EBP Encryption	ESP Integrity	AH Integrity	
RA	ESP-3DES-SHA	ESF_3DES	ESP_SHA_HMAC		
	<u> </u>	III		>	
	And Frit.				
		< [9ack N∈xl≻ Fini	sh Cancel Hel	р
提供 轉換集詳細資訊 (加	加密和身份驗證演算法)	,然後按一下	OK.		

Add Transform Set 🛛 🔀
Name:
✓ Data integrity with encryption (ESP)
Integrity Algorithm: <a>None>
Encryption Algorithm: <none></none>
Show Advanced >>
OK Cancel Help

9. 本示例中使用的是名為CP Default Transform Set的Default Transform Set。因此,選擇預設轉 換集並按一下**下一步**。

Easy VPN Server Wizard -	35% Complete				×
VPN Wizard	Transform Set A transform set specifies the data in the VPN tunnel.	encryption and aut	hantication algorthm	ns used to protect the	i
	Click the Add button to acd transform set.	a new transform se	et and the Edil buto	in to ecit the specifie	r
	Select Transform Set ————————————————————————————————————	sform Get 🛛 🛩 –]		
	Details of the specified tra	ansform set			_
	Name	EBP Encryption	ESP Integrity	AH Integrity	L
RA	ESP-3DES-SHA	ESF 3DES	ESP SHA HMAC		
	Ard Enit			<u> </u>	y
		< [9ack Next≯ <mark>,</mark> Fini	sn Cancel H	elp

10. 在新視窗中,選擇將在其上配置組策略的伺服器,該伺服器可以是Local或RADIUS,或者同時是Local和RADIUS。在本示例中,我們使用Local server來配置組策略。選擇Local,然後按一下Next。

Easy VPN Server Wizard	- 50% Complete 🛛 🔀
VPN Wizard	Group Authorization and Group Policy Lookup An ISAKMP dient configuration group (or VPN group) is a group of VPN clients that share the same authentibation and configuration information. Group policies can be configured locally on this router, on an external server, or on both. Easy VPN Gerver will use these group policies to authenticate VPN dients. Mothod List for Group Folicy Lookup Gelect the servers on which group policies will be configured, or select an existing AAA policy that defines the servers used for configuring group policies. Prabluc C PADIUC C PADIUS and Local
	Summary The local database will be used for group authorization. This option is recommended if you do not have a RADIUS or TACACE- server in your network.
	< Back Next > Finish Cancel Help
在此新想窗中選擇更明	B於使用者身份驗證的伺服器 可以是Local Only或RADIUS 也可以是

- 11. 在此新視窗中選擇要用於使用者身份驗證的伺服器,可以是Local Only或RADIUS,也可以是 Local Only和RADIUS。在本示例中,我們使用Local server配置用於身份驗證的使用者憑據
 - 。確保選中Enable User Authentication旁邊的覈取方塊。選擇「Local Only」,然後按一下 「Next」。

Easy VPN Server Wizard -	- 65% Complete 🛛 🔀
VPN Wizard	User Authentication (XAuth) User Authentication (XAuth) provides additional security by authenticating the user of a device after the device has undergone. KE authentication. User credentials XAuth can be configured locally on this touter, on an external server, or on both
	Enable User Authentication Belact the servers that will be used for configuring user credentials, or select an existing AAA policy that defines the servers used for configuring user credentials.
	© RADIUS © RADIUS and Local Only
RA	Add User Crodentials Summary Local database will be used for user authertication.
	< Back Next > Finish Cancel Help

12. 按一下Add以建立新的組策略,並在此組中新增遠端使用者。

Easy VPN Server Wizard -	80% Comp	lete					×
VPN Wizard	Group Auti The Easy V other Easy clients or d the remote Click the Au Clonc but	horization and User PN Server allows) VPN Remote the shert of evice that is part of client or device to r Id butten to acd r Iten to create a new	r Group Poll /ou to group t products. T 'a giver gro ensure that nure group v group from	ctes Fremote use The group at up The sam appropriate sithe Ecitt non existing	rs who are usin tributes will be o e group name o group atributes putton to edit an group.	g Cisco VPN clients downloaded throug should be configure are downloaded existing group, or th	SCr Intre action Ne
	Scice:	Grcup Namo	Pool	DN3	WN8	Domain Name	
	Adc Configura cleared. Id e Time	igure dle Timer e a timeout value at	fer which V	PN tunnals fi HH:MM:SS	e rom idle clierts	should be	
				< Back	Next > Finis	n Cancel H	lelp

13. 在Add Group Policy視窗中,在Space中提供Name for Name of This Group(在本例中為 cisco)以及Pre-shared key,以及IP Pool(起始IP地址和結束IP地址)資訊,如圖所示,然後按 一下**OK**。**注意:**您可以建立新的IP池,或使用現有的IP池(如果存在)。

Ad	d Group	Policy				X	
G	eneral	DNS/WINS	Split Tunneling	Client Setting	s XAuth Options	Client Update	
	Name o	of This Group			cisco		
	Pre	eshared Keys	3				
	Specify the key that will be used to authenticate the clients associated with this group.						
	Curre	ent Key			<none></none>		
	Enter	new pre-sha	red key:		*****		
	Reenter new pre-shared key:						
Pool Information							
Specify a local pool containing a range of addresses that will be used to allocate an internal IP address to a client.							
	Create a new pool C Select from an existing pool						
	Starting IP address: 192.168.1.1 -Select an entry 🕑 Details						
Ending IP address: 192.168.1.254							
Enter the subnet mask that should be sent to the client along with the IP address.							
	Su	bnet Mask:		(Optic	inal)		
Maximum Connections Allowed:							
			ок	Cancel	Help		

14. 現在,選擇使用**cisco**名稱建立的新**組策略**,然後根據需要按一下**配置空閒計時器**旁邊的覈取 方塊以配置**空閒計時器**。按「Next」(下一步)。

VPN Wizard Group Authorization and User Group Policies The Easy VPN Server allows you to group remote users who are using Cisco VPN clients other Easy VPN Remote blient products. The group attributes will be downloaded through clients or device that is part of a given group. The same group name should be configure: the remote client or device the ensure that apartopriate group attributes are drawnloaded Click the Add butten to and more groups the Ecil butten to edit an existing group, or the Clone butten to create a new group from an existing group. Sciec: Group Name Pol DN3 WN8 Domain Name Image: Cisco SDM_FO Made Lett Clone Lette
Scice: Grcup Nama Scice: Grcup Nama Cisco SDM_FO Adc Lett Clone Lielete Configure de Timer Configure de Timer
Adc Ecit Clone Lielete
Adc Ecit Clone Lielete
Configure dle Timer
cleared.
Id e Timer: 24 0C 00 HH:MM:SS
< Back Next > Finish Cancel He

Easy VPN Server Wizard -	85% Complete
Easy VPN Server Wizard - VPN Wizard	85% Complete Cisco Tunneling Control Protocol(cTCP) The cTCP allows Easy VPN clients to fur during transparently without modifying frewall rules.You must enable cTCP on the server in order to accept connections from remote clients using cTCP Specify the portinumpers on which the Easy VPN Server needs to listen for cTCP request from clients.You can add a maximum of 10 portinumbers. Use comma' ' to separate entrips.
	< Back Next > Finish Cancel Help

16. 檢查**配置摘要**。按一下「Finish」(結束)。

Easy VPN Server Wizard -	90% Complete				
VPN Wizard	Summary of the Configuration				
	Click Finish to deliver the configuration b	u the router.			
	Tunnel Interface Details Interface: Virtual Template1 Type Tunnel Mode: IFSec-Py4 IP Address: Linnumbered to Lo	ophackC		=	
	IKE Folicies:			-	
	Hash CH Oroup	Authentication	=noryption	-	
	SHA_1 grcup2	PRE_SHARE	3DES	-	
	Fransform Set: Name: EGP-CDEC-OFA ESP Encryption: ESP_3DES ESP Integrity, ESP_SHA_HMAC Mode: TUNNEL				
	Oreus Dallaut colour Matkaalt int	-Lovel		>	
	Test VPN connectivity after configuring	J.			
		< Back Next >	Finish	Cancel	Help

17. 在「Deliver Configuration to Router」視窗中,按一下Deliver將配置傳送到路由器。您可以 按一下Save to file,將配置儲存為PC上的檔案。

Deliver Configuration to Router	×
Deliver delta commands to the router's running config.	
Preview commands that will be delivered to the router's running configuration.	
aaa authentication login ciscocp_vpn_xauth_ml_1 local aaa authorization network ciscocp_vpn_group_ml_1 local ip local pool SDM_POOL_1 192.168.1.1 192.168.1.254 crypto ipsec transform-set ESP-3DES-SHA esp-sha-hmac esp-3des mode tunnel exit crypto isakmp profile ciscocp-ike-profile-1 isakmp authorization list ciscocp_vpn_group_ml_1 client authentication list ciscocp_vpn_group_ml_1 client authentication list ciscocp_vpn_xauth_ml_1 match identity group cisco	
The differences between the running configuration and the startup configuration are lost whenev the router is turned off.	er
Save running config. to router's startup config. This operation can take several minutes. Deliver Cancel Save to file	

18. 命令傳遞狀態視窗顯示命令到路由器的傳遞狀態。它顯示為Configuration delivered to

rouler。按一下「UN」(唯止)	ter 。按一下	「OK」 ((確定)) 。
--------------------	-----------------	--------	------	-----

Commands Delivery Status	
Command Delivery Status:	
Preparing commands for delivery Submitting 47 commands, please wait Configuration delivered to router. 	
<	>
ок	

19. 您可以看到新建立的Easy VPN伺服器。您可以通過選擇**編輯Easy VPN伺服器**來編輯現有伺 服器。這將完成Cisco IOS路由器上的Easy VPN伺服器配置。

onfigure .> Se	CUNTY > VPN > Easy '	VPN Server			3
🖥 VPN					
reate Easy Vi	PN Server ∐Edit Easy	VPN Server			
			Cloba Cett	ngs Add Edit D	elete
Nerr e	Interface	Group Authorization	User Ault entication	Mode Configuration.	
iscoCF Prof	Tor Virtual Templater	cipecop vicin group mil 1	ic scoop ypri xauth imilir	REEPOND	
		νç			
				Toot VEN 8	CIVICI
				ICOTVEN 8	

<u>CLI組態</u>

路由器配置

```
Router#show run
Building configuration...
Current configuration : 2069 bytes
! version 12.4 service timestamps debug datetime msec
service timestamps log datetime msec no service
password-encryption hostname Router boot-start-marker
boot-end-marker no logging buffered enable password
cisco !---AAA enabled using aaa newmodel command. Also
AAA Authentication and Authorization are enabled ---! aaa
new-model
1
aaa authentication login ciscocp_vpn_xauth_ml_1 local
aaa authorization network ciscocp_vpn_group_ml_1 local
1
aaa session-id common
ip cef
1
!
1
ip domain name cisco.com
multilink bundle-name authenticated
1
!--- Configuration for IKE policies. !--- Enables the
IKE policy configuration (config-isakmp) !--- command
mode, where you can specify the parameters that !--- are
used during an IKE negotiation. Encryption and Policy
details are hidden as the default values are chosen.
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp keepalive 10
crypto isakmp client configuration group cisco
key cisco123
pool SDM_POOL_1
crypto isakmp profile ciscocp-ike-profile-1
  match identity group cisco
  client authentication list ciscocp_vpn_xauth_ml_1
  isakmp authorization list ciscocp_vpn_group_ml_1
  client configuration address respond
  virtual-template 1
1
!--- Configuration for IPsec policies. !--- Enables the
crypto transform configuration mode, !--- where you can
specify the transform sets that are used !--- during an
IPsec negotiation. crypto ipsec transform-set ESP-3DES-
SHA esp-3des esp-sha-hmac
1
crypto ipsec profile CiscoCP_Profile1
set security-association idle-time 86400
set transform-set ESP-3DES-SHA
set isakmp-profile ciscocp-ike-profile-1
```

```
-- RSA certificate generated after you enable the !--
ip http secure-server command.
crypto pki trustpoint TP-self-signed-1742995674
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-1742995674
revocation-check none
rsakeypair TP-self-signed-1742995674
!--- Create a user account named cisco123 with all
privileges.
username cisco123 privilege 15 password 0 cisco123
archive
log config
 hidekeys
1
1
!--- Interface configurations are done as shown below---
! interface Loopback0 ip address 10.10.10.10
255.255.255.0 ! interface FastEthernet0/0 ip address
10.77.241.111 255.255.255.192 duplex auto speed auto !
interface Virtual-Template1 type tunnel ip unnumbered
Loopback0 tunnel mode ipsec ipv4 tunnel protection ipsec
profile CiscoCP_Profile1 ! !--- VPN pool named
SDM_POOL_1 has been defined in the below command---! ip
local pool SDM_POOL_1 192.168.1.1 192.168.1.254
!--- This is where the commands to enable HTTP and HTTPS
are configured. ip http server ip http authentication
local ip http secure-server ! ! ! ! control-plane ! line
con 0 line aux 0 !--- Telnet enabled with password as
cisco. line vty 0 4 password cisco transport input all
scheduler allocate 20000 1000 ! ! ! ! end
```

<u>驗證</u>

Easy VPN伺服器 — show命令

使用本節內容,確認您的組態是否正常運作。

• show crypto isakmp sa — 顯示對等體上的所有當前IKE SA。 Router#show crypto isakmp sa

IPv4 Crypto ISA	KMP SA			
dst	src	state	conn-id	slot status
10.77.241.111	172.16.1.1	QM_IDLE	1003	0 ACTIVE

• show crypto ipsec sa — 顯示對等體上的所有當前IPsec SA。

Router#**show crypto ipsec sa** interface: Virtual-Access2 Crypto map tag: Virtual-Access2-head-0, local addr 10.77.241.111

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.3/255.255.255.255/0/0)
current_peer 172.16.1.1 port 1086
 PERMIT, flags={origin_is_acl,}

```
#pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28
#pkts decaps: 36, #pkts decrypt: 36, #pkts verify: 36
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 2

local crypto endpt.: 10.77.241.111, remote crypto endpt.: 172.16.1.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x186C05EF(409732591)

inbound esp sas:
spi: 0x42FC8173(1123844467)
transform: esp-3des esp-sha-hmac
```

<u>疑難排解</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 。

註:在發出debug命令前<u>,請先參閱</u>有關Debug命令的重要資訊。

相關資訊

- IPSec 協商/IKE 通訊協定
- 思科配置專業版快速入門手冊
- 思科產品支援頁面 路由器
- 技術支援與文件 Cisco Systems