# IOS路由器作为Easy VPN服务器使用 Configuration Professional 配置示例

## 目录

简介 先决条件 使用的组件 安装Cisco CP 运行 Cisco CP 的路由器配置 要求 规则 配置 网络图 Cisco CP - Easy VPN服务器配置 CLI 配置 验证 Easy VPN服务器 — show命令 故障排除 相关信息

## <u>简介</u>

本文档介绍如何使用Cisco Configuration Professional<sup>(</sup>Cisco CP)和CLI将Cisco IOS®路由<u>器配置为</u> <u>Easy VPN(EzVPN)</u>服务器。Easy VPN服务器功能允许远程最终用户使用IP安全(IPsec)与任何 Cisco IOS虚拟专用网络(VPN)网关进行通信。集中管理的IPsec策略由服务器"推送"到客户端设备 ,从而最大限度地减少最终用户的配置。

有关Easy VPN服务器的详细信息,请参阅<u>Cisco IOS版本12.4T</u>安全连<u>接配置指南库的Easy VPN服</u> <u>务器部分</u>。

## <u>先决条件</u>

### 使用的组件

本文档中的信息基于以下软件和硬件版本:

- 配备 Cisco IOS 软件版本 12.4(15T) 的 Cisco 1841 路由器
- Cisco CP 版本 2.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

### <u>安装Cisco CP</u>

要安装Cisco CP,请执行以下步骤:

- 1. 从思科软件中心下载Cisco CP V2.1(仅限注册客户),并将其安装到您的本地PC上。Cisco CP的最新版本可在Cisco CP网<u>站上找到</u>。
- 2. 从本地PC通过**开始 > 程序 > Cisco Configuration Professional(CCP)**启动Cisco CP,然后选择 具有要配置的路由器的**Community**。

Application Help		
Home Configure	Monitor 😽	🙆 🥘 Cisco
Select Community Memberi	ec Home > Community V	fiew
the move as inscrivened)	Cisco Configuratio	n 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
		and the second
	Community Informat	ion
	Selected Community	New Community Select a device from t
	Pittar	
	IP address / Hostn	ame Router Hostname
1		
	N	
	Hanage Devices	Delete Discover



3. 要发现要配置的设备,请突出显示路由器,然后单击Discover。

Appacadon neip			
Aome 👸 Configure	Monitor 8	🙆 🙆 🛛 c	isc
Select Community Memberi	Home > Community	View	
	🚺 Cisco Configuratio	on Professional News	
Community View	Date	Title	
	24-May-2010	Cisco Configuration Professi	onal s
	24-May-2010	Simplify ISR & ISR G2 deplo	ymen
	24-May-2010	Provide CCP Feedback	
I	Community Informa Selected Community Printer IP address / Hosto Router	ntion 1: New Community -Select a device name Router Hostname	e from

**注:有**关与Cisco CP v2.1兼容的Cisco路由器型号和IOS版本的信息,请参阅兼容的<u>Cisco IOS版本</u> 部分。

**注:有**关运行Cisco CP v2.1的PC要求的信息,请参阅"系统要<u>求"</u>部分。

运行 Cisco CP 的路由器配置

要在 Cisco 路由器上运行 Cisco CP,请执行以下配置步骤:

- 1. 使用 Telnet、SSH 或控制台连接路由器。使用以下命令进入全局配置模式: Router(config)#**enable** Router(config)#
- 2. 如果启用了 HTTP 和 HTTPS 并将其配置为使用非标准端口号,则可跳过此步骤并直接使用已 配置的端口号。使用以下 Cisco IOS 软件命令启用路由器 HTTP 或 HTTPS 服务器: Router(config)# ip http server Router(config)# ip http secure-server Router(config)# ip http authentication local
- 3. 创建一个权限级别为 15 的用户: Router(config)# username privilege 15 password 0

注意:将<username>和<password>替换为要配置的用户名和密码。

- 4. 为本地登录和权限级别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. (可选)启用本地登录以支持日志监控功能: Router(config)# logging buffered 51200 warning

### <u>要求</u>

本文档假设思科路由器完全运行且已配置为允许思科CP进行配置更改。

有关如何开始使用Cisco CP的完整信息,请参阅<u>Cisco Configuration Professional入门</u>。

#### <u>规则</u>

有关文档约定的更多信息,请参考 <u>Cisco 技术提示约定。</u>

### 配置

在本部分中,您将了解有关网络中路由器基本设置的配置信息。

**注意:**使用命<u>令查找工</u>具(<u>仅</u>限注册客户)可获取有关本节中使用的命令的详细信息。

#### 网络图

本文档使用以下网络设置:



**注意:**此配置中使用的IP编址方案在Internet上不可合法路由。这些地址是在实验室环境中使用的 <u>RFC 1918 地址。</u>

<u>Cisco CP - Easy VPN服务器配置</u>

要将Cisco IOS路由器配置为Easy VPN服务器,请执行以下步骤:

1. 选择Configure > Security > VPN > Easy VPN Server > Create Easy VPN Server ,然后单击 Launch Easy VPN Server Wizard,以将Cisco IOS路由器配置为Easy VPN服务器



2. 单击Next以继续Easy VPN服务器配置。



- 3. 在生成的窗口中,**虚拟接**口符配直为Easy VPN服务器配直的一部分。提供虚**拟隧道接口的** IP地址,并选择用于**验证**VPN客户端的身份验证方法。此处,**预共享密钥**是使用的身份验证方 法。单击"下一步
  - ":

Easy VPN Server Wizard -	10% Complete		N 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997	
VPN Wizard	Interface and Authentication Interface A virtual template interface will b	oe proated ad part of this Eady v	/PN Berver configuration.	
Any Cisco IOS feature that should be applied before encryption to the traffit the VPIN tunnel can be configured on this Interface.				
		10101010		
		15.10.10.10		
	Subnet Mask.	255.255 255.0	cr 24	
	C Urmumbered to	FastEthemet0/0	V Details	
11)a	Authentication Select the method used for auth VPN Gerver.	nenticating VPIN clients connect	ing to this Easy	
	Pre-shared Keys	C Digital Certificates	C Bull	
		< Back Next > P	inish Cancel Help	

4. 指定此**路由器在与远程设备协商时**要使用的加密算法、身份验证算法和密钥交换方法。路由器 上存在默认IKE策略,如果需要,可使用该策略。如果要添加新的IKE策略,请点击Add。

#### 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.

A STATEMENT	P1	ority Encryptic	on Hash	E-H Group	Authentication	Түре
Real Property in	1 🔮	3DES	SHA 1	group2	PRE SHARE	Cisco CP Defau
Sec. March						
Constant of						
and the second second second	bhA	Edit				
1		<u> </u>				
Sect. Said						
				e Back Mer	da Finica (	Cancal Holp
				S DHCK DIE		Help

5. 提供加密算法、验证算法和密钥交换方法(如图所示),然后单击确定

Add Inc Policy
Configure IKE Policy
Priority: Authentication:
₽ RSA_SIG ✓
Encryption: D-H Group:
DES 💙 group1 💙
Hash: Lifetime:
SHA_1 24 0 0 HH:MM:SS
OK Cancel Help

6. 本例**中使用**默认IKE策略。因此,选择默认IKE策略并单击**Next**。

Easy VPN Server Wizard -	20% Complete					
VPN Wizard	IKE Proposale IKE proposals method that is device. Click the Add	specify the en used by this ru putton to add	eryption algorit cuter when nea more policies :	hm, authenticai Iotlating a VPN and the Edit - b	ion algorithm ar cornection with withn to ecitian :	nd key exchange the remote existing policy
	Plority	Encomption	Hash	E-HiGroup	Authentication	Type
		3DES	SHA 1	group2	PRE SHARE	Cisco CP Defau
RA						
	Add	Edit				
				< Back Nex	Finish (	ancel Help

7. 在新窗口中,应提供转换集详细信息。"转换集"指定用于保护 VPN 隧道中的数据的加密算法 和验证算法。单击Add提供这些详细信息。单击"添加"并提供详细信息时,可根据需要添加任 意数量的转换集。注意:使用Cisco CP配置时,路由器上默认存在CP默认转换集。

Easy VPN Server Wizard	- 35% Complete				×
VPN Wizard	T <b>raneform Set</b> A transform set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel.				
	Click the Add button to add a transform set.	a new transform se	t and the Edil buto	on to eait the sp∋arte:	ł
	Select Transform Set Gisco CP Default Tran Details of the specified tra	sform Get 🛛 🔽 - Insform set			
	Name	EBP Encryption	ESP Integrity	A-Hrtegrity	
RA	SE ESP-3DES-SHA	ESF_3DES	ESP_SHA_HMAC		
E	<			2	
	And Enit				
		< 6	9ack N∈xl> Fini	sh Cancel He	Ip

8. 提供转换**集详细**信息(**加密和验证算法**),然后单**击确定**。

dd Transform Set		
Name:		
🔽 Data integrity with e	ncryption (ESP)	
Integrity Algorithm:	<none></none>	<b>~</b>
Encryption Algorithm:	<none></none>	*
		Show Advanced >>
ок	Cancel	Help
	+수 4= 65 m과 2 / ++ +수 4	

9. 本示**例中使**用名**为CP默认转**换集的默认转换集。因此,选择默认的转换集,然后单击"下**一步**"。

Easy VPN Server Wizard -	35% Complete				$\mathbf{X}$
VPN Wizard	Transform Set A transform set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel.				
	Click the Add button to add a transform set.	new transform se	t and the Edil Euto	in to eait the speart e:	ł
	Select Transform Set	form Get 🛛 🛩 —	]		
	Details of the specified trai	nsform set			
	Name	EBP Encryption	ESP Integrity	A-Hirtegrity	L .
RA	ESP-3DES-SHA	ESF 3DES	ESP SHA HMAC		
	And Ecit			<u> </u>	
		< 8	Back Next >	sn Cancel He	lp

10. 在新窗口中,选择将在其上配置组策略的服务器,该服务器可以是Local或RADIUS,也可以 是Local和RADIUS。在本例中,我们使用**本地服**务器配置组策略。选择"Local",然后单击 "Next"。

Easy VPN Server Wizard	- 50% Complete
VPN Wizard	Group Authorization and Group Policy Lookup An ISAKMP client 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 clients. 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 server's used for configuring group policies. Problec RADIUC RADIUS 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

11. 在此新窗口中选择要用于用户身份验证的服务器,该窗口可以是**仅本地**或**RADIUS**或**仅本地 和RADIUS**。在本示例中,我们使用**本地服**务器来配置用户身份验证凭据。确保选中Enable User Authentication旁**的复选**框。选择"**仅本地"**,然后单**击"下一步**"。

Easy VPN Server Wizard -	65% Complete 🛛 🔀
VPN Wizard	<b>User Authentication (XAuth)</b> User Authentication (XAuth) provides additional security by authenticating the user of a device ofter the device has undergone. KE authentication. User credentials XAuth can be configured locally on this to uter, on an external server, or on both
	✓ Enable User Authentication Select 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. (* Local Only)
	C RADIUS C RADIUS and Local Only
RA	Summary
	< Back Next >\ Finish Cancel Help

12. 单击Add以创建新组策略并在此组中添加远程用户。

Easy VPN Server	Wizard - 80%	Complete
-----------------	--------------	----------

VPN Wizard	Gro
	I he
	clier
	the
	Clor
	80
	<
	C C
E Carlos And	cle
	Id
A THE A	

#### Group Authorization and User Group Policies

The Easy VPN Server allows you to group remote users who are using Cisco VPN clients or other Easy VPN Remote client products. The group attributes will be downloaded through the clients or device that is part of a given group. The same group name should be configured on the remote client or device to ensure that appropriate group attributes are downloaded. Click the Add... buttor to add more groups. The Edit ... button to edit an existing group, or the Cline... buttor to create a new group from an existing group.

				1	1	
Select	Group Name	Pool	DNB	WN8	Domain Name	
<						>
Adc	Ecit	Clone.	Delet	e		
	figure die Timer					
Configur cleared.	e a timeoul value af	ter which	VPN tunnəls fi	rom idle clierts	should be	
ld e Tim	er:		HH:MM:SS	3		
			< Back	Next > Finis	n Cancel	Help

13. 在"添加组策略"窗口中,在空格中提供组名称,以提供"此组的名称"(本例中为cisco)以及预共 享密钥,并提供如图所示的IP池(起始IP地址和结束IP地址)信息,然后单击"确定"。**注意** :您可以创建新IP池或使用现有IP池(如果存在)。

Ad	d Group Policy	×					
ſ	ieneral DNS/WINS Split Tunneling Client Settings XAuth Options Client Update						
	Name of This Group: cisco						
	Pre-shared Keys						
	Specify the key that will be used to authenticate the clients associated with this group.						
	Current Key <none></none>						
	Enter new pre-shared 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 © 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.						
	Subnet Mask: (Optional)						
Maximum Connections Allowed:							
	OK Cancel Help						

14. 现在,选择名**为cisco**的新组策**略,然后按**需单击**配置空闲计时器**旁的复选框以配置空闲计时 器。单击 Next。

Easy VPN Server Wizard -	80% Comp	lete					
VPN Wizard	Group Authorization and User Group Policies The Easy VPN Server allows you to group remote users who are using Cisco VPN clients or other Easy VPN Remote all ent products. The group attributes will be downloaded through the clients or device that is part of a given group. The same group name should be configured or the remote client or device to ensure that appropriate group attributes are downloaded Click the Add buttor to add more groups the Edit buttor to edit an existing group, or the Clone buttor to create a new group from an existing group.						
	Scice:	Grcup Name	Pool SDM_FO	DNB	WN8	Domain Nam	c
	<						>
K A	Adc	Ecit	Clone.	. Liele	te		
	Configur Configur Cleared.	nfigure die Timer re a timeout value a	f.er which '	VPN tunnels f	from idle clierts	should be	
	ld e Tim	er: 24	00 00	HH:MM:S	S		
				< Back	Next > Fini	ish Cancel	Help

15. 如果需**要,请启**用思科隧道控制协议(cTCP)。否则,单击**Next**。

Easy VPN Server Wizard -	85% Complete
VPN Wizard	Cisco Tunneling Control Protocol(cTCP) The cTCP allows Easy VPN clients to fur clich transparently without modifying firewall rules.You must enable cTCF on the server in order to accept connections from remote clients using cTCP Chabe 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 portinumkers.
	< Back Next > Finish Cancel Help

16. 查看**配置摘要**。单击 **完成**。

Easy VPN Server Wizard -	90% Complete			X
VPN Wizard	Summary of the Configuration			
	Click Finish to deliver the configuration I Tunnel Interface Details Interface: Virtual Template1 Type Tunnel Mode: IFSec- Py4	lu the router.		^
	IP Address: Linnumbered to Lo IKE Folicies: Hash DH Oroup	cophackC Authentication	Encryption	-
	SHA_1 grcup2	PRE_SHARE	3DES	
	Fransform Sec Name: EOP-CDEO-OLIA ESP Encryption: ESP_3DES ESP Integrity, ESP_SHA_HMA/ Mode: TUNNEL	c		
	Oreus Dallau Leolaun Method Liet	(Lovel		>
	Test VPN connectivity after configurin	g.		
		< Back Mext	Finish	Cancel Help

17. 在将配**置传送到路由器**窗口中,单**击**传送将配置传送到路由器。您可以单击"**保存到文**件",将 配置另存为PC上的文件。

Deliver Configurat	ion to Router	×
Deliver delta comman	as to the router's running config.	
Preview commands t	hat will be delivered to the router's running configuration.	
aaa authentication lo	gin ciscocp_vpn_xauth_ml_1 local	~
aaa authorization net	work ciscocp_vpn_group_ml_1 local	
ip local pool SDM_PO	OL_1 192.168.1.1 192.168.1.254	
mode tunnel	ni-set ESP-SDES-SHA esp-sna-nniac esp-sdes	
exit		
crypto isakmp profile	ciscocp-ike-profile-1	
isakmp authorization	list ciscocp_vpn_group_ml_1	
match identity group	cisco	
client configuration s	idraee reenond	<u> </u>
		2
The differences be the router is turne	tween the running configuration and the startup configuration ar d off.	e lost whenever
🗖 Save running co	nfig. to router's startup config.	
This operation ca	n take several minutes.	
Γ	Deliver Cancel Save to file Help	1

18. 命令**传送状态窗口**显示命令传送到路由器的状态。它显示为"Configuration delivered to

router(配置传送到路由器)"。Click

Com	nands Delive	ery Status				×
Com	mand Delivery S	Status:				
Prep Subi Cont 	aring command nitting 47 comm figuration delive	s for delivery ands, please wait red to router.				~
						~
<					3	
		0	ĸ			
」 丁以看到	」 新创建的Easy	/ VPN服务器。通过	选择Edit Easy	/ VPN Ser	ver(编辑	Easy
ver),	可 <b>以编辑现有</b>	<b>服务器</b> 。Cisco IOS	路由器上的Ea	sy VPN服	务器配置	完成。
nfigure > S	econty > VPN > Eas	y VPN Server				
VPN						
VPN						
VPN eate Essyl	VPN Server Little	sy VPN Server	2104		Ldd Fair	De
VPN Pate Easy	VPN Server Edit Ea	sy VPN Server		a Cettings	Add Edi	: Del

Tool VEN Server



#### 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>验证</u>

### Easy VPN服务器 — show命令

使用本部分可确认配置能否正常运行。

• show crypto isakmp sa - 显示对等体上的所有当前 IKE SA。 Router#show crypto isakmp sa

dat	gro	state	conn-id	glot	gtatus
10.77.241.111	172.16.1.1	QM_IDLE	1003	0 2	ACTIVE

• show crypto ipsec sa - 显示对等体上的所有当前 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>故障排除</u>

<u>命令输出解释程序(仅限注册用户)(OIT) 支持某些 show 命令。</u>使用 OIT 可查看对 show 命令输 出的分析。

**注意:在**发出debug<u>命令之前,请参</u>阅有关debug命令的重要信息。

## 相关信息

- IPsec 协商/IKE 协议
- Cisco Configuration Professional 快速入门指南
- 思科产品支持页 路由器
- <u>技术支持和文档 Cisco Systems</u>