Exemplo de Configuração do IOS Router as Easy VPN Server Utilizando Configuration Professional

Contents

Introduction Prerequisites Componentes Utilizados Instalar o Cisco CP Configuração do roteador para executar o Cisco CP Requirements Conventions Configurar Diagrama de Rede Cisco CP - Configuração fácil do servidor VPN Configuração de CLI Verificar Easy VPN Server - Comandos show Troubleshoot Informações Relacionadas

Introduction

Este documento descreve como configurar um Cisco IOS[®] Router como um Easy VPN (EzVPN) Server usando o <u>Cisco Configuration Professional (Cisco CP</u>) e a CLI. A característica Easy VPN Server permite que um usuário final remoto comunique-se usando a Segurança IP (IPsec) com qualquer gateway da Rede Privada Virtual (VPN) do Cisco IOS. As políticas de IPsec centralmente gerenciadas são "empurradas" ao dispositivo de cliente pelo servidor, minimizando a configuração pelo usuário final.

Para obter mais informações sobre o Easy VPN Server, consulte a seção <u>Easy VPN Server</u> da <u>Secure Connectivity Configuration Guide Library, Cisco IOS versão 12.4T</u>.

Prerequisites

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

Roteador Cisco 1841 com Software Cisco IOS versão 12.4(15T)

Cisco CP Versão 2.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Instalar o Cisco CP

Execute estas etapas para instalar o Cisco CP:

- Baixe o Cisco CP V2.1 do <u>Cisco Software Center</u> (somente clientes<u>registrados</u>) e instale-o em seu PC local.A versão mais recente do Cisco CP pode ser encontrada no <u>site do Cisco</u> <u>CP</u>.
- 2. Inicie o Cisco CP no seu PC local através de Iniciar > Programas > Cisco Configuration Professional (CCP) e escolha a Comunidade que tem o roteador que deseja

Select Community Memberi	Home > Community (View
	📴 Cisco Configuratio	n Professional News
Ocommunity View	Date	Title
	24-May-2010	Cisco Configuration Professional
	24-May-2010	Simplify ISR & ISR 62 deployment
	24-May-2010	Provide CCP Feedback
		and have a second second second
	Community Information	tion
	Selected Community	New Community Select a desice from
	Piltar	
10	IP address / Hostn	ame Router Hostname
\mathbf{X}		
	2	
	1	



3. Para descobrir o dispositivo que deseja configurar, realce o roteador e clique em

Application Help	1000 CO. 100	
Home 👸 Configure	Monitor 66	🖄 🥘 Cisco
Select Community Memberi	Home > Community V	iew
Carried and a second se	🚺 Cisco Configuration	n Professional News
Community View	Date	Title
	24-May-2010	Cisco Configuration Professional v2
	24-May-2010	Simplify ISR & ISR 62 deployments
	24-May-2010	Provide CCP Feedback
	Community Informat	ton
	Selected Community:	New Community .Select a device from t
	Piltar	
	IP address / Hostna	me Router Hostname
	Router	
	-	
		200
	present and a second se	

Observação: para obter informações sobre os modelos de roteador Cisco e as versões do IOS compatíveis com o Cisco CP v2.1, consulte a seção <u>Compatível com as versões do Cisco IOS</u>.

Observação: para obter informações sobre os requisitos do PC que executa o Cisco CP v2.1, consulte a seção <u>Requisitos do sistema</u>.

Configuração do roteador para executar o Cisco CP

Siga estas etapas de configuração para executar o Cisco CP em um roteador da Cisco:

- Conecte-se ao roteador usando Telnet, SSH ou por meio do console.Entre no modo de configurações globais usando este comando: Router(config)#enable Router(config)#
- 2. Se HTTP e HTTPS estiverem habilitados e configurados para usar números de porta fora do padrão, pule essa etapa e use o número da porta já configurado.Habilite o servidor HTTP ou HTTPS do roteador usando estes comandos do Software Cisco IOS:

Router(config)# ip http server
Router(config)# ip http secure-server
Router(config)# ip http authentication local

3. Crie um usuário com nível de privilégio 15: Router(config)# username privilege 15 password 0

Observação: substitua *<nome de usuário>* e *<senha>* pelo nome de usuário e senha que você deseja configurar.

4. Configure SSH e Telnet para o nível de privilégio e login local 15.

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)# exit

 Opcional) Habilite o logon local para oferecer suporte à função de monitoramento de registro:

Router(config) # logging buffered 51200 warning

Requirements

Este documento pressupõe que o roteador Cisco está totalmente operacional e configurado para permitir que o Cisco CP faça alterações na configuração.

Para obter informações completas sobre como começar a usar o Cisco CP, consulte <u>Introdução</u> <u>ao Cisco Configuration Professional</u>.

Conventions

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

Configurar

Nesta seção, você recebe informações para definir as configurações básicas de um roteador em uma rede.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Easy VPN Client

Observação: os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São endereços <u>RFC 1918</u> que foram usados em um ambiente de laboratório.

Cisco CP - Configuração fácil do servidor VPN

Execute estas etapas para configurar o roteador Cisco IOS como um Easy VPN Server:

 Escolha Configure > Security > VPN > Easy VPN Server > Create Easy VPN Server e clique em Launch Easy VPN Server Wizard para configurar o roteador Cisco IOS como um Easy VPN

Server:
Configure > Security > VPN > Easy VPN Server
MARK VPN
Create Easy VPN Server Edit Easy VPN Server
Cisco CP can guide you through Easy VPN Server configuration tasks.
Use Case Scenario
Configure Easy VPN Server Client 1 Client 2 Client 2 Use this option to configure this router as an Easy VPN Server. To complete the configuration, you must know the different group policies to which the clients can connect and their attributes. Launch Easy VPN Server Wizard

2. Clique em **Next** para continuar com a configuração **Easy VPN Server**.

Easy VPN Server Wizard	
VPN Wizard	Welcome to the Easy VPH Server Wizard
	This wizard will guide you through configuring of an Easy VPN Server on this router. An Easy VPN Server allows a remote end user to use IP Security (IPSec) when communicating with a Cisco IOS Virtual Private Network (VPN) gateway. Centrally managed IPSec policies are "bushed" to the client by the server, minimizing configuration by the end user. This wizard will guide you in performing the following tasks to successfully configure an Easy VPN Server on this router: * Configuring virtual temp ate interface and authentications. * Configuring IKE policies. * Configuring an IPSec transform set. * Configuring a group policy lookup method. * Configuring user authent itation. * Configuring user authent itation. * Configuring user authent itation. * Configuring command RADIUS converted tailo. * Configuring cisco tunne ing control protocol («TCP) optionally.
	< Back Next > Finish Cancel Help

3. Na janela resultante, uma Interface Virtual será configurada como parte da configuração do Easy VPN Server. Forneça o endereço IP da Virtual Tunnel Interface e também escolha o método de autenticação usado para autenticar os clientes VPN. Aqui, Pre-shared Keys é o método de autenticação usado. Clique em Next:

Easy VPN Server Wizard -	10% Complete (×
VPN Wizard	Interface and Authentication Interface Avirtual template interface will be preated as part of this Easy VPN Berver configuration.	
	Any classo for leading that should be applied before encryption to the traine going into the VPIN tunnel can be configured on this interface.	
	IP Address 10.10.10.10	
×-	Subriel Mask. 255.265.255.0 cr 24	
	C Umumbered to FastEthernet0/0 Cetails	
A	Authentication	
	Pre-shared Keys O Digital Certificates O Both	
	< Back Next > Finish Cancel Help	

4. Especifique o algoritmo de criptografia, o algoritmo de autenticação e o método de troca de chaves a serem usados por este roteador ao negociar com o dispositivo remoto. Uma política IKE padrão está presente no roteador, que pode ser usada se necessário. Para adicionar uma nova política de IKE, clique em Adicionar.

Easy VPN Server Wizard	- 20% Complete				
VPN Wizard	IKE Proposale IKE proposals specify the e method that is used by this device. Click the Add – putton to ad	ncryption algorit router when neo dimore policies :	hm, authenlica Iotlating a VPN and the Edil - t	lion algorithm ar connection with withn to ecitian :	id key exchange the remote existing policy
	Priority Encryption	Hash	E-H Group	Authentication	Түре
	Add		4roup2	PRE DHARE	
			< Back Nex	1> Finish (ancəl Help

5. Forneça o algoritmo de criptografia, o algoritmo de autenticação e o método de troca de chaves como mostrado aqui e clique em

dd IKE Policy	
Configure IKE Policy	
Priority:	Authentication:
þ	RSA_SIG 🔽 🔽
Encryption:	D-H Group:
DES 🗸	group1 🗸 🗸
Hash:	Lifetime:
SHA_1 💌	24 0 0 HH:MM:SS
OK D	Cancel Help

 A política IKE padrão é usada neste exemplo. Como resultado, escolha a política IKE padrão e clique em Avançar.

Easy VPN Server Wizard -	20% Complete				
VPN Wizard	IKE Proposale IKE proposals specify the el method that is used by this device. Click the Add L putton to add	neryption algorit router when neo I more policies :	hm, authenlica Iotlating a VPN and the Edil - t	tion algorithm ar connection with nutten to ecitian :	nd key exchange the remote existing policy
		Hash	E-H Group	Authentication	Туре
		1			
	Add Edit		e Back Nov	The Finical (Cancal Holp

7. Na nova janela, os detalhes do conjunto de transformações devem ser fornecidos. O conjunto de transformação especifica os algoritmos de criptografia e autenticação usados para proteger dados em túnel VPN. Clique em Adicionar para fornecer estes detalhes. Você pode adicionar qualquer número de Conjuntos de transformação conforme necessário quando clicar em Adicionar e fornecer os detalhes.Observação: CP Default Transform Set está presente por padrão no roteador quando configurado usando o Cisco CP.

Easy VPN Server Wizard	35% Complete				X
VPN Wizard	Transform Set A transform set specifies the data in the VPN tunnel.	encryption and auth	nentication algorthm	is used to protect the	
	Click the Add button to acd a transform set. Select Transform Sot	a new transform se	tand Ihə =dıl ku:to	n to ecit the specifie:	1
	Cisco CP Default Trans	sform Cet 🛛 🔽			
, ``	Details of the specified that				
	SP-3DES-SHA	ESF_3DES	ESP_SHA_HMAC	A-Integrity	
	Ard Ecit.			>	
		< E	Back Next > Finit	sn Cancel He	Ip

8. Forneça os detalhes **do conjunto de transformações** (algoritmo de criptografia e autenticação) e clique em

dd Transform Set		
Name:		
✓ Data integrity with er	ncryption (ESP)	
Integrity Algorithm:	<none></none>	✓
Encryption Algorithm:	<none></none>	~
		Show Advanced >>
ок	Cancel	Help
	dd Transform Set Jame: ✓ Data integrity with e Integrity Algorithm: Encryption Algorithm:	dd Transform Set Jame: ✓ Data integrity with encryption (ESP) Integrity Algorithm: ≤None> Encryption Algorithm: OK Cancel

9. O **conjunto de transformações padrão** chamado **CP Default Transform Set** é usado neste exemplo. Como resultado, escolha o conjunto de transformações padrão e clique em **Avançar**.

Easy VPN Server Wizard -	35% Complete				×
VPN Wizard	T raneform Set A transform set specifies the data in the VPN tunnel.	encryption and aut	hentication algorthm	is used to protect the	:
	Click the Add button to add a transform set.	a new transform se	et and the Edil butto	in to ecit the specifie	r
	Cisco CP Default Tran	sform Get 🛛 🛩 – insform set]		
	Name	EBP Encryption	ESP Integrity	AH Integrity	1
RA	ESP-3DES-SHA	ESF 3DES	ESP SHA HMAC	>	
	Ard Ecit				
		< 8	9ack Next≯ <mark>,</mark> Fini	sh Cancel He	elp

10. Na nova janela, escolha o servidor no qual as políticas de grupo serão configuradas, que pode ser Local ou RADIUS ou Local e RADIUS. Neste exemplo, usamos o servidor local para configurar políticas de grupo. Escolha Local e clique em Avançar.

Easy VPN Server Wizard -	50% Complete	×
VPN Wizard	Group Authorization and Group Policy Lookup An ISAKMP disent configuration group (or VPN group) is a group of VPN disents 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 Server will use these group policies to authenticate VPN disents. Mothod Lipt 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. Problem Coal C RADIUE RADIUE and Local) (es
	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.	
	S Back MEXT A PIRIST Cancel Help	

11. Escolha o servidor a ser usado para Autenticação de usuário nesta nova janela que pode ser Somente local ou RADIUS ou Somente local e RADIUS. Neste exemplo, usamos o servidor local para configurar as credenciais do usuário para autenticação. Verifique se a caixa de seleção ao lado de Enable User Authentication está marcada. Escolha Somente local e clique em

Avançar.

Easy VPN Server Wizard -	65% Complete 🛛 🔀
VPN Wizard	User Authentication (XAuth) User Authentication (XAuth) 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 for ally on this to uter, on an external server, or on both IV 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.
	Image: Construction of the second
	Local database will be used for user authertication. < Back Next > Finish Cancel Help

12. Clique em **Adicionar** para criar uma nova política de grupo e adicionar os usuários remotos neste

grupo.

Easy VPN Server Wizard -	80% Comp	lete					
VPN Wizard	Group Aut The Easy Cther Easy clients or o the remote Click the A Clonc bu	thorization and Use VPN Server allows (VPN Remote then device that is part of client or device to dd butter to acd r dd butter to a new	r Group Po /Du to grou t products 'a giver <u>c</u> ensure th: nore grou v <u>c</u> roup fr:	Dictes up remote use . The group at roup The sam at sporopriate ; ps: the Ecit t om an existing	rs who are using tributes will be d be group name s group atributes pullon to edit an group.	g Cisco VPN clier lownloaded throu should be configu are dhwnloaded existing group, or	ntscr gitte redion Une
	Scice:	Grcup Name	Pool	DN3	WNS	Domain Name	
	<						>
KA	Adc	figure die Timer	Clone.	Uelet	E		
	Configure a timeoul value after which VPN tunnels from idle clients should be cleared.						
	ld e Tim	er:		HH:MM:SS	3		
				< Back	Next > Finis	n Cancel	Help

13. Na janela Adicionar política de grupo, forneça o nome do grupo no espaço fornecido para o Nome deste grupo (cisco neste exemplo) junto com a chave pré-compartilhada, e as informações do Pool IP (o endereço IP inicial e o endereço IP final), como mostrado, e clique em OK.Observação: você pode criar um novo pool de IPs ou usar um pool de IPs existente, se houver.

Ad	d Group Policy 🛛 🛛 🔀					
G	General 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 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.						
Subnet Mask: (Optional)						
Maximum Connections Allowed:						
	OK Cancel Help					

14. Agora escolha a nova Política de Grupo criada com o nome cisco e clique na caixa de seleção ao lado de Configurar temporizador de ociosidade conforme necessário para configurar o temporizador de ociosidade. Clique em Next.

Easy VPN Server Wizard	80% Complete 🛛 🔀
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 their 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 buttor to edit an existing group, or the Clone buttor to create a new group from an existing group.
	Scice: Grcup Namo Pool DNG WINS Domain Name Cisco SDM_FO
A	Adc Ecit Clone Lielete
	I✓ Configure a timeoul value after which VPN tunnels from idle clients should be cleared. Idle Timer: 24 0C 00 HH:MM:SS
	< Back Next > Finish Cancel Help

15. Ative o **Cisco Tunneling Control Protocol** (cTCP), se necessário. Caso contrário, clique em **Avançar**.

Easy VPN Server Wizard -	85% Complete 🔀							
VPN Wizard	PN Wizard The cTCP allows Easy VPN clients to furction transparently without modifying firewall rules.You must enable cTCF on the server in order to accept connections from remote cl							
	Lising cTCP Chabe cTCP Specify the port numbers on which the Easy VPIN Server needs to listen for cTCP request from clients.You can add a maximum of 10 port numbers.							
	Usc comma ' ' to separate entries.							
	< Back Next > Finish Cancel Help							

16. Revise o **Resumo da configuração**. Clique em Finish.

Easy VPN Server Wizard -	90% Complete				×
VPN Wizard	Summary of th e Configuration				
	Click Finish to deliver the configuration to Tunnel Interface Details Interface: Virtual Template1 Type Tunnel Mode: IFSec-Pv4 IP Address: Unnumbered to Loo	he rouler.			
	IKE Folicies: Hash DH Group	Authentication	Encryption	-	
	SHA_1 grcup2	PRE_SHARE	3DES		
11 A	Fransform Set: Name: EOP-CDEO-OFA ESP Encryption: ESP_3DES ESP Integrity, ESP_SHA_HMAC Mode: TUNNEL				
	Orgue Del au Lookue Method Liet	- Lovel		>	
	□ Test VPN connectivity after configuring.				
		< Back Mext >	Finish	Cancel H	elp

17. Na janela **Deliver Configuration to Router**, clique em **Deliver** para fornecer a configuração ao roteador. Você pode clicar em **Salvar em arquivo** para salvar a configuração como um arquivo no PC.

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 ciscoop_vpn_xauth_ml_1 local aaa authentization network ciscoop_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 ciscoop-ike-profile-1 isakmp authorization list ciscoop_vpn_group_ml_1 client authentication list ciscoop_vpn_group_ml_1 match identity group cisco	
The differences between the running configuration and the startup configuration a the router is turned off.	are lost whenever
Save running config. to router's startup config. This operation can take several minutes. Deliver Cancel Save to file Help	

18. A janela **Command Delivery Status** mostra o status de entrega dos comandos ao roteador. Ele aparece como **Configuração entregue ao roteador**. Click

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

 Você pode ver o Easy VPN Server recém-criado. Você pode editar o servidor existente escolhendo Editar Easy VPN Server. Isso conclui a configuração do Easy VPN Server no Cisco IOS Router.

ate Easy VP	N Server Edit Easj	/ VPN Server				
Cloba Cettings., Add., Edit., Delete						
ше	Interface	Group Authorization	User Ault entication	Mode Configuration.		
CCF Profi	or Virtual Templater	cibecop ven group mil 1	biscoop ypri xauth imilir	REEPOND		
		ht				

Configuração de CLI

Configuração do roteador				
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				
!				
!				
aaa authentication login ciscocp_vpn_xauth_ml_1 local				
aaa authorization network ciscocp_vpn_group_ml_1 local				
! !				
aaa session-id common				
ip cef				
:				
!				
1				
ip domain name cisco.com !				

```
multilink bundle-name authenticated
!--- 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
!--- 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
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
!--- 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

Verificar

Easy VPN Server - Comandos show

Use esta seção para confirmar se a sua configuração funciona corretamente.

• **show crypto isakmp sa** — Mostra todas as SAs IKE atuais em um peer. 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** — Mostra todas as SAs IPsec atuais em um peer. 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)
```

Troubleshoot

A <u>Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados</u> <u>comandos show.</u> Use a OIT para exibir uma análise da saída do comando show.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar os comandos debug.

Informações Relacionadas

transform: esp-3des esp-sha-hmac

- <u>Negociação IPsec/Protocolos IKE</u>
- Guia de início rápido do Cisco Configuration Professional (CCP)
- Página de suporte de produto da Cisco Roteadores
- <u>Suporte Técnico e Documentação Cisco Systems</u>