Ejemplo de Configuración Profesional del Router IOS como Servidor Easy VPN Usando Configuración

Contenido

Introducción Prerequisites Componentes Utilizados Instalación de Cisco CP Configuración del router para ejecutar Cisco CP Requirements Convenciones Configurar Diagrama de la red Cisco CP - Configuración del servidor Easy VPN Configuración de CLI Verificación Servidor Easy VPN - Comandos show Troubleshoot Información Relacionada

Introducción

Este documento describe cómo configurar un router Cisco IOS[®] como servidor Easy VPN (EzVPN) usando <u>Cisco Configuration Professional (Cisco CP)</u> y la CLI. La función Easy VPN Server permite a un usuario final remoto comunicarse mediante IP Security (IPsec) con cualquier gateway de Red privada virtual (VPN) de Cisco IOS. Las políticas IPSec administradas de manera centralizada se envían al dispositivo cliente mediante el servidor, lo que minimiza la configuración que debe realizar el usuario final.

Para obtener más información sobre Easy VPN Server, consulte la sección <u>Easy VPN Server</u> de la <u>Biblioteca de la Guía de Configuración de Conectividad Segura, Cisco IOS Release 12.4T</u>.

Prerequisites

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Router Cisco 1841 con software Cisco IOS versión 12.4(15T)
- Cisco CP versión 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.

Instalación de Cisco CP

Realice estos pasos para instalar Cisco CP:

- 1. Descargue Cisco CP V2.1 desde el <u>Cisco Software Center</u> (<u>sólo</u> clientes registrados) e instálelo en su PC local.La última versión de Cisco CP se puede encontrar en el <u>sitio web de</u> <u>Cisco CP</u>.
- 2. Inicie Cisco CP desde su PC local a través de **Start > Programs > Cisco Configuration Professional (CCP)** y elija la **Comunidad** que tiene el router que desea

Home 👸 Configure	Monitor 8	0	Cisco
Select Community Memberi	Home > Community t	fiew	
	🐻 Cisco Configuratio	n Professional N	
Community View	Date	Title	
	24-May-2010	Cisco Confi	ouration Professional +2
	24-May-2010	Simplify 18	R & ISR 62 deployments
	24-May-2010	Provide CC	P Feedback
	-		
	Community Informa	tion .	
	Selected Community	New Community	Select a device from 1
	Pittar	Carl Accurate	
	IP address / Hostn	ame Rout	ter Hostname
	Hanage Devices	Delete	Discover
	Hanage Devices	Delete	Discover



3. Para descubrir el dispositivo que desea configurar, resalte el router y haga clic en

Application Help		
👔 Home 🖓 Configure	Monitor	🔄 🥹 Cisco
Select Community Memberi	Home > Community V	lew
The sector secto	🚺 Lisco 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 Informati Selected Community: Pinter IP address / Hostna Router	ion New Community .Select a device from t me Router Hostname
	Hanage Devices	Delete Discover

Nota: Para obtener información sobre los modelos de router de Cisco y las versiones de IOS compatibles con Cisco CP v2.1, consulte la sección <u>Versiones compatibles con Cisco IOS</u>.

Nota: Para obtener información sobre los requisitos de PC que ejecutan Cisco CP v2.1, consulte la sección <u>Requisitos del sistema</u>.

Configuración del router para ejecutar Cisco CP

Realice estos pasos de configuración para ejecutar Cisco CP en un router de Cisco:

- 1. Conecte el router mediante Telnet, SSH o a través de la consola.Ingrese al modo de configuración global usando este comando: Router(config)#enable Router(config)#
- 2. Si HTTP y HTTPS están habilitados y configurados para utilizar números de puerto no estándar, puede omitir este paso y utilizar simplemente el número de puerto ya configurado.Habilite el router HTTP o el servidor HTTPS con estos comandos de software Cisco IOS:

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

3. Cree un usuario con el nivel de privilegio 15: Router(config)# username privilege 15 password 0

Nota: Reemplace *<username>* y *<password>* por el nombre de usuario y la contraseña que desea configurar.

4. Configure SSH y Telnet para el inicio de sesión local y el nivel de privilegio 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

5. (Opcional) Habilite el registro local para admitir la función de monitoreo de registro: Router(config)# logging buffered 51200 warning

Requirements

Este documento asume que el router Cisco está completamente operativo y configurado para permitir que Cisco CP realice cambios en la configuración.

Para obtener información completa sobre cómo empezar a utilizar Cisco CP, refiérase a Introducción a Cisco Configuration Professional.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

En esta sección se ofrece información para configurar las configuraciones básicas para un router en una red.

Nota: Utilice la herramienta <u>Command Lookup (sólo para clientes</u> registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



```
Easy VPN Client
```

Nota: Los esquemas de direccionamiento IP utilizados en esta configuración no son legalmente enrutables en Internet. Son direcciones RFC 1918 que se han utilizado en un entorno de laboratorio.

Cisco CP - Configuración del servidor Easy VPN

Realice estos pasos para configurar el router Cisco IOS como servidor Easy VPN:

1. Elija Configure > Security > VPN > Easy VPN Server > Create Easy VPN Server y haga clic en Launch Easy VPN Server Wizard para configurar el router Cisco IOS como un Easy VPN Server:

Configure > Security > VPN > Easy VPN Server

2	🚰 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 Lient 1 Lient 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

Server.



3. En la ventana resultante, una interfaz virtual se configurará como parte de la configuración del servidor Easy VPN. Proporcione la dirección IP de la interfaz de túnel virtual y también elija el método de autenticación utilizado para autenticar los clientes VPN. Aquí, Pre-shared Keys es el método de autenticación utilizado. Haga clic en Next (Siguiente):

Easy VPN Server Wizard -	10% Complete		
VPN Wizard	Interface and Authentication Interface A virtual template interface will	be proated as part of this Easy v	/PN Server configuration.
	Any Cisco IOS teature that shou the VPIN tunnel can be configur IP Adcress of Virtual Tunnel in:	id be applied before encryption ed on this Interface. erface	to the traffic gcing into
	IP Address	10101010	
	Subnet Mask.	255.255 255.0	cr 24
	C Unnumbered to	FastEthemeto/o	Cetails
Ka	Aufhentication Select the method used for aut VPN Server.	henticating VPN clients connect	Ing to this Easy
	Pre-shared Keys	C Digital Certificates	C Bult
N/			
		< Back Next > P	inish Cancel Help

4. Especifique el algoritmo de cifrado, el algoritmo de autenticación y el método de intercambio de claves que utilizará este router al negociar con el dispositivo remoto. Hay una política IKE predeterminada en el router que se puede utilizar si es necesario. Si desea agregar una nueva política IKE, haga clic en Agregar.

Lasy VPN Server Wizard -	20% Complete					
VPN Wizard	IKE Proposale IKE proposals method that is device. Click the Add	specify the en used by this n putton to add	eryption algorit cuter when neo more policies :	hm, authentica Iotlating a VPN and the Edit i b	lion algorithm ar cornection with withn to ecit an :	id key exchange the remote existing policy
	Plorty	Econotion	Hash	E-HiGroup	Authentication	Type
		2059	SHA 1	20010 2	PRE SHARE	Claro CR Dofai
	Add	Edit				
				< Back Nex	l> Finish (ancel Help

5. Proporcione Algoritmo de Cifrado, Algoritmo de Autenticación y el Método de Intercambio de Claves como se muestra aquí, luego haga clic en

	Add IKE Policy	
	Configure IKE Policy	
	Priority: 2	Authentication:
	Encryption:	D-H Group: group1
	Hash: SHA_1	Lifetime: 24 0 0 HH:MM:SS
otar	ок	Cancel Help

 En este ejemplo se utiliza la política IKE predeterminada. Como resultado, elija la política IKE predeterminada y haga clic en Next.

Easy VPN Server Wizard -	20% Complete					Ľ
VPN Wizard	IKE Proposals IKE proposals method that is device. Click the Add	specify the en used by this n putton to add	eryption algorit cuter when nea more policies :	hm, authentica Iotlating a VPN and the Edit i b	lion algorithm ar cornection with withn to ecitian :	id key exchange the remote existing policy
	Pilorthy	Econotion	Hash	E-HIGroup	Authentication	Type
		3DES	SHA 1	3mun2	PRE SHARE	Cisro CP Defau
	Add	Edit				
				< Back Nex	Finis1 (Cancel Help

7. En la nueva ventana, se deben proporcionar los detalles del conjunto de transformación. El conjunto de transformación especifica los algoritmos Encryption y Authentication utilizados para proteger los datos en el túnel VPN. Haga clic en Agregar para proporcionar estos detalles. Puede agregar cualquier número de conjuntos de transformación según sea necesario al hacer clic en Agregar y proporcionar los detalles.Nota: CP Default Transform Set está presente de forma predeterminada en el router cuando se configura con Cisco CP.

Easy VPN Server Wizard	35% Complete				×	
VPN Wizard	T raneform Set A transform set specifies the data in the VPIN tunnel.	T raneform Set A transform set specifies the encryption and authentication algor thms used to protect the data in the VPN tunnel.				
	Click the Add button to acd transform set.	a new transtorm se	et and the Edil kutto	n to eart the speart e:	ł	
	Cisco CP Default Tran	Cisco CP Default Transform Set				
	Name	EBP Encryption	ESP Integrity	A-Hrtegrity		
	E ESP-3DES-SHA	ESF_3DES	ESP_SHA_HMAC			
	Acd Ecit			2		
		< 6	Back Next > Fini	sn Cancel He	/Ip	

8. Proporcione los detalles Transform Set (Encryption and Authentication Algorithm) y haga clic

Add Transfo	rm Set			×
Name:				
🔽 🔽 Data i	ntegrity with e	encryption (ESP)		
Integrity A	lgorithm:	<none></none>	×	
Encryption	n Algorithm:	<none></none>	*	
			Show Advanced >	•>
	ок	Cancel	Help	

9. En este ejemplo se utiliza el **Conjunto de transformación predeterminado** denominado **Conjunto de transformación predeterminada de CP**. Como resultado, elija el conjunto de transformación predeterminado y haga clic en **Siguiente**.

Easy VPN Server Wizard	35% Complete				×
VPN Wizard	Traneform Set A transform set specifies the data in the VPIN tunnel.	encryption and aut	hentication algorthm	ns used to protect the	I
	Click the Add button to acd transform set. Select Transform Set Cisco CP Default Tran	a new transform se sform Oet 🛛 🖌 –	et and the =dil kuto	in to ecit the specifie	t
, N (1997),	Details of the specified the	anetorm set			1
lin Nad		E3P Encryption	ESP Integrity	A-Integrity	Ы
ba	Acd Frit			>	
		< [Back Next > , Fini	sn Cancel He	elp

10. En la nueva ventana, elija el servidor en el que se configurarán las políticas de grupo que pueden ser Local o RADIUS o tanto Local como RADIUS. En este ejemplo, utilizamos el servidor local para configurar las políticas de grupo. Elija Local y haga clic en 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 dients 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 dients. 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. PADIUE C RADIUE and Local	⊋ V ies
	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. Elija el servidor que se utilizará para la autenticación de usuario en esta nueva ventana que puede ser Local Only o RADIUS o bien Local Only y RADIUS. En este ejemplo, utilizamos servidor local para configurar las credenciales de usuario para la autenticación. Asegúrese de que la casilla de verificación junto a Enable User Authentication esté marcada. Elija Local Only y haga clic en 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 offer the device has undergone. KE authentication. User credentials XAuth can be configured locally on this to dev, 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. Loca Only
	C RADIUS and Local Only
ba	Summary
	< Back Next >\ Finish Cancel Help

12. Haga clic en **Agregar** para crear una nueva política de grupo y agregar los usuarios remotos en este grupo.

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

VPN Wizard	G
	Th oth olio the Olio Olio
	8
	~

oup Authorization and User Group Policies

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

	Octoor Oreum	blassa	Deal		107 N O	Domain Homa	
	Scied: Group	Name	POOL	DINS	W1/8	Domain Name	
Contraction of the second seco							
	<						>
	Anc she	-cit	Clone	Lielet			
	noc de	- 5416.77	010110		-		
	Configure dle	Timer					
	Configure a timeo	ul value af	er which v	/PN tunnals fr	om idle clierts s	should be	
	cleared.						
				_			
	ld e Timer:			HH:MM:SS	3		
And the second second second							
				< Back	Next > Finis	n Cancel	Help

13. En la ventana Agregar política de grupo, proporcione el nombre de grupo en el espacio para proporcionar el nombre de este grupo (cisco en este ejemplo) junto con la clave previamente compartida, y la información sobre el conjunto IP (la dirección IP inicial y la dirección IP final) como se muestra y haga clic en Aceptar. Nota: Puede crear un nuevo conjunto IP o utilizar un conjunto IP existente si está presente.

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. Ahora elija la nueva Política de Grupo creada con el nombre cisco y luego haga clic en la casilla de verificación junto a Configure Idle Timer según sea necesario para configurar el Temporizador de Inactividad. Haga clic en Next (Siguiente).

Easy VPN Server Wizard -	80% Complete	$\mathbf{\times}$
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 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 of 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 Clone button to create a new group from an existing group.	r 1e Dn
	Scice: Grcup Name Pool DNB WINS Domain Name Cisco SDM_FO	
	Adc Ecit Clone Lielete	
	Configure de Timer Configure a timeoul value after which VPN tunnels from idle clients should be cleared.	
	Id e Timer: 24 0C 00 HH:MM:SS	
	< Back Next > Finish Cancel Help	

 Habilite Cisco Tunneling Control Protocol (cTCP) si es necesario. De lo contrario, haga clic en Siguiente.

Easy VPN Server Wizard	- 85% Complete
Easy VPN Server Wizard VPN Wizard	85% Complete Cisco Tunneling Curu of Protocol(cTCP) The cTCP allows Easy VPN clients to fur clich transparently without modifying firewall rules.You must enable cTCP on the server in order to accept connections from remote clients u.sing cTCP Deabe 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.
	Vec comma ' ' to separate entrice. < Back Next & Finish Cancel Help

16. Revise el **resumen de la configuración**. Haga clic en Finish (Finalizar).

Easy VPN Server Wizard -	90% Complete				×
VPN Wizard	Summary of the Configuration				
	Click Finish to deliver the configuration to .	he rouler.			
	Tunnel Interface Details Interface: Virtual Template1 Type Tunnel Mode: IFSec- Pv4 IP Address: Linnumbered to Loo	pbackC			
	IKE Folicies:				
	Hash CH Oroup	Authentication	Encryption		
	SHA_1 group2	PRE_SHARE	3DES		
A	Transform Set: Name: ESP-CDES-GLA ESP Encryption: ESP_3DES ESP Integrity, ESP_SHA_HMAC Mode: TUNNEL				
	Overue Dation Licelane Method Lief	-Lovel		- 5	
	⊨== ☐ Test VPN connectivity after configuring.				
		< Back Mext >	Finish	Cancel H	elp

17. En la ventana **Entregar configuración al router**, haga clic en **Entregar** para entregar la configuración al router. Puede hacer clic en **Guardar en archivo** para guardar la configuración como un archivo en el equipo.

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 authorization 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 ciscocp-ike-profile-1 isakmp authorization 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 the router is turned off.	n are lost whenever
Save running config. to router's startup config.	
This operation can take several minutes.	
Deliver Cancel Save to file Hel	q

18. La ventana **Estado de Entrega de Comandos** muestra el estado de entrega de los comandos al router. Aparece como **Configuración enviada al router**. Click

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

 Puede ver el servidor Easy VPN recién creado. Puede editar el servidor existente seleccionando Editar servidor Easy VPN. Esto completa la configuración del servidor Easy VPN en el router Cisco IOS.

nin Easy VP-N Server Cloba Cettings. Add. Edit. Delets Srouro Authunization User Authentication Mode Configuration. <u>rip ato: cisecop vpn group mi 1 siscoop vpr xauth mi : REEPOND</u> V	VPN					
Cloba Cettings Add Edit Delets Srouro Authonization User Authonization Mude Configuration. The alconization of the provide the provided of t	ate Easy VPr	4 Server 🗍 Edit Easy	VPN Server			
Sroup Authurization User Authentication Mude Configuration.				Cloba Cett	ngs. Add. Edit. Dele	ete
r <u>pator cisecep von group mild sessep vpr xauth mild SEEPOND</u>	m e	Interface	Group Authorization	User Ault entication	Mode Configuration.	
β	CCF Profit	r Virtual Templater	cipecto ven group ml 1	biscoop ypri xauth imilir	REEPOND	
			ν			

Configuración de CLI

Configuración del router
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
! !
aaa session-id common ip cef ! ! !
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

Verificación

Servidor Easy VPN - Comandos show

Use esta sección para confirmar que su configuración funciona correctamente.

• show crypto isakmp sa — Muestra todas las IKE SAs actuales en un par. 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**: muestra todas las SAs IPsec actuales en un par. 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
```

Troubleshoot

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte <u>Información Importante sobre Comandos Debug</u> antes de ejecutar los comandos debug.

Información Relacionada

- Negociación IPSec/Protocolos IKE
- Guía de inicio rápido de Cisco Configuration Professional
- Páginas de Soporte de Productos de Cisco Routers
- Soporte Técnico y Documentación Cisco Systems