Contenido

Introducción

Este documento proporciona las instrucciones graduales en cómo permitir el acceso de clientes VPN al Internet mientras que son tunneled en un router de Cisco IOS®. Esta configuración es necesaria para permitir a los clientes VPN un acceso seguro a los recursos corporativos a través de IPsec y, al mismo tiempo, permitir un acceso no seguro a Internet. Esta configuración se denomina tunelización dividida.

Nota: El Túnel dividido puede plantear un riesgo de seguridad cuando está configurado. Puesto que los clientes VPN tienen acceso sin garantía a Internet, pueden ser comprometidos por un atacante. Ese atacante puede entonces acceder el LAN corporativo vía el túnel IPsec. Un compromiso entre el Tunelización y el Túnel dividido llenos puede ser no prohibir a los clientes VPN el acceso del LAN local solamente. Consulte PIX/ASA 7.x: Permita el acceso del LAN local para el ejemplo de configuración de los clientes VPN para más información.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Router Cisco 3640 con el Cisco IOS Software Release 12.4
- Cliente Cisco VPN 4.8

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Antecedentes

Los VPN de accesos remotos dirigen el requisito del equipo de trabajo móvil de conectar con seguridad con la red de la organización. Los usuarios ambulantes pueden configurar una conexión segura usando el software cliente VPN instalado en sus PC. El cliente VPN inicia una conexión a un dispositivo del sitio central configurado para validar estas peticiones. En este ejemplo, el dispositivo del sitio central es un router del Cisco IOS que utiliza las correspondencias cifradas dinámicas.

Cuando usted habilita el Túnel dividido para las conexiones VPN, requiere la configuración de un Access Control List (ACL) en el router. En este ejemplo, asocian al **comando access-list 101 al** grupo para los propósitos del Túnel dividido, y el túnel se forma a la red 10.10.10.x/24. Los flujos del tráfico no encriptado (por ejemplo, Internet) a los dispositivos se excluyen de las redes configuradas en el ACL 101.

```
access-list 101 permit ip 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Aplicar ACL en las propiedades del grupo.

```
crypto isakmp client configuration group vpngroup key cisco123 dns 10.10.10.10 wins 10.10.10.20 domain cisco.com pool ippool acl 101
```

En este ejemplo de configuración, un túnel IPsec se configura con estos elementos:

- Correspondencias de criptografía aplicadas a las interfaces exteriores en el PIX
- Autenticación ampliada (Xauth) de los clientes VPN contra una autenticación local
- Asignación dinámica de un IP Address privado de un pool a los clientes VPN
- Las funciones del **comando nat 0 access-list**, que permite que los host en un LAN utilicen los IP Address privados con un usuario remoto y todavía que consigan un direccionamiento del Network Address Translation (NAT) del PIX para visitar una red no confiable.

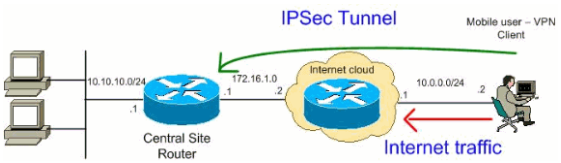
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

Configuraciones

En este documento, se utilizan estas configuraciones:

- Router
- Cliente de Cisco VPN

Router

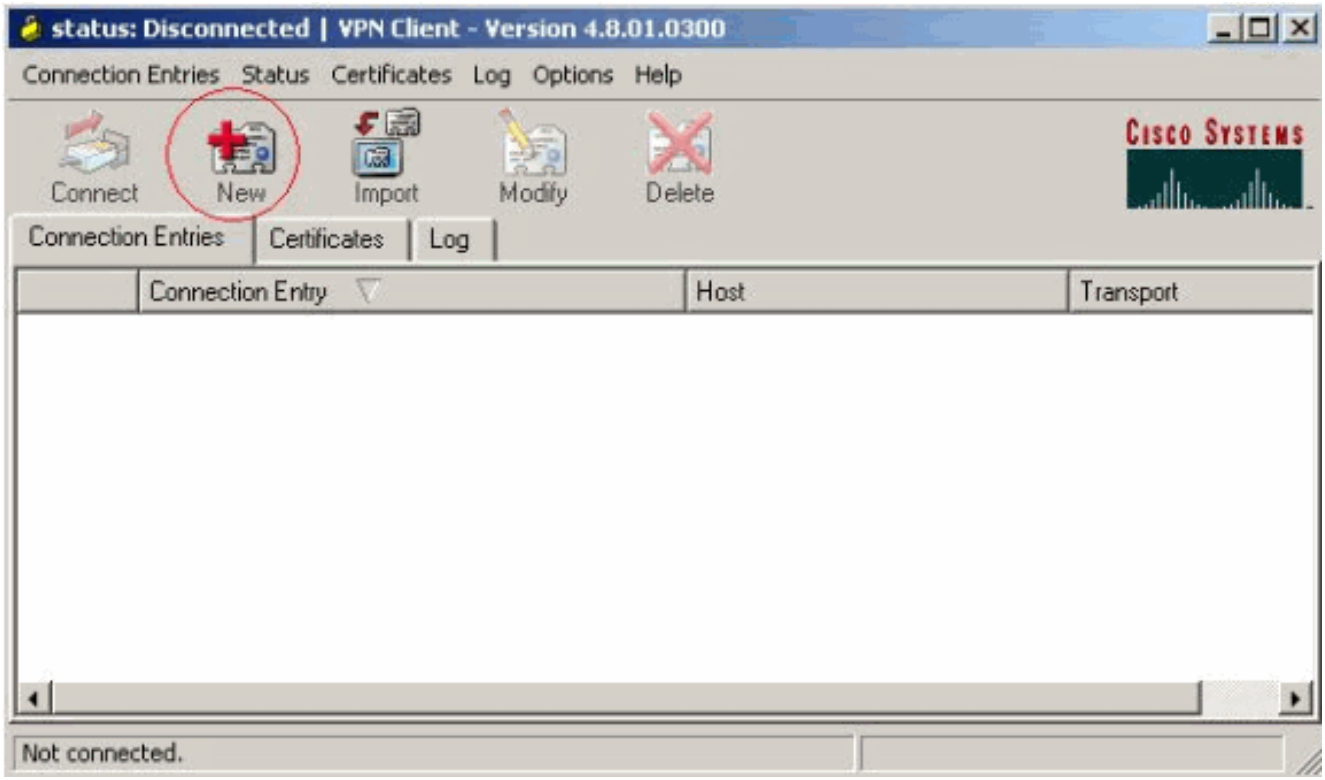
```
VPN#show runBuilding configuration...Current configuration :
2170 bytes!version 12.4service timestamps debug datetime
msecservice timestamps log datetime msecno service password-
encryption!hostname VPN!boot-start-markerboot-end-marker!!!--
- Enable authentication, authorization and accounting (AAA)
!--- for user authentication and group authorization.aaa new-
model!!--- In order to enable Xauth for user authentication,
!--- enable the aaa authentication commands.aaa
authentication login userauthen local!--- In order to enable
group authorization, enable !--- the aaa authorization
commands.aaa authorization network groupauthor local!aaa
session-id common!resource policy!!!--- For local
authentication of the IPsec user, !--- create the user with a
password.username user password 0 cisco!!!!--- Create an
Internet Security Association and !--- Key Management
Protocol (ISAKMP) policy for Phase 1 negotiations.crypto
isakmp policy 3 encr 3des authentication pre-share group 2!--
- Create a group that is used to specify the !--- WINS and
DNS server addresses to the VPN Client, !--- along with the
pre-shared key for authentication. Use ACL 101 used for !---
the Split tunneling in the VPN Clinet end.crypto isakmp
client configuration group vpnclient key cisco123 dns
10.10.10.10 wins 10.10.10.20 domain cisco.com pool ippool acl
101!!--- Create the Phase 2 Policy for actual data
encryption.crypto ipsec transform-set myset esp-3des esp-md5-
hmac!!--- Create a dynamic map and apply !--- the transform
set that was created earlier.crypto dynamic-map dynmap 10 set
transform-set myset reverse-route!!--- Create the actual
crypto map, !--- and apply the AAA lists that were created
earlier.crypto map clientmap client authentication list
userauthencrypto map clientmap isakmp authorization list
groupauthorcrypto map clientmap client configuration address
respondcrypto map clientmap 10 ipsec-isakmp dynamic
dynmap!!!!interface Ethernet0/0 ip address 10.10.10.1
255.255.255.0 half-duplex ip nat inside!--- Apply the crypto
map on the outbound interface.interface FastEthernet1/0 ip
address 172.16.1.1 255.255.255.0 ip nat outside ip virtual-
reassembly duplex auto speed auto crypto map
clientmap!interface Serial2/0 no ip address!interface
Serial2/1 no ip address shutdown!interface Serial2/2 no ip
address shutdown!interface Serial2/3 no ip address shutdown!-
-- Create a pool of addresses to be !--- assigned to the VPN
Clients. !ip local pool ippool 192.168.1.1 192.168.1.2ip http
serverno ip http secure-server!ip route 0.0.0.0 0.0.0.0
172.16.1.2!--- Enables Network Address Translation (NAT) !---
of the inside source address that matches access list 111 !--
- and gets PATed with the FastEthernet IP address.ip nat
inside source list 111 interface FastEthernet1/0 overload!!--
```

```
- The access list is used to specify which traffic !--- is to
be translated for the outside Internet. access-list 111 deny
ip 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255access-list 111
permit ip any any!--- Configure the interesting traffic to be
encrypted from the VPN Client !--- to the central site router
(access list 101). !--- Apply this ACL in the ISAKMP
configuration.access-list 101 permit ip 10.10.10.0 0.0.0.255
192.168.1.0 0.0.0.255control-plane!line con 0line aux 0line
vty 0 4!end
```

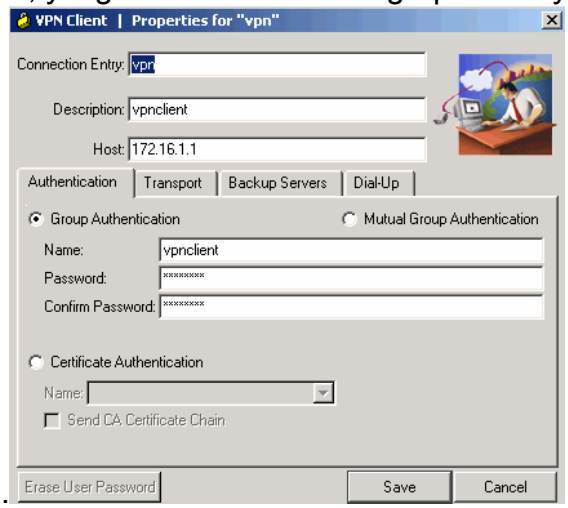
Configuración del cliente VPN 4.8

Complete estos pasos para configurar al cliente VPN 4.8.

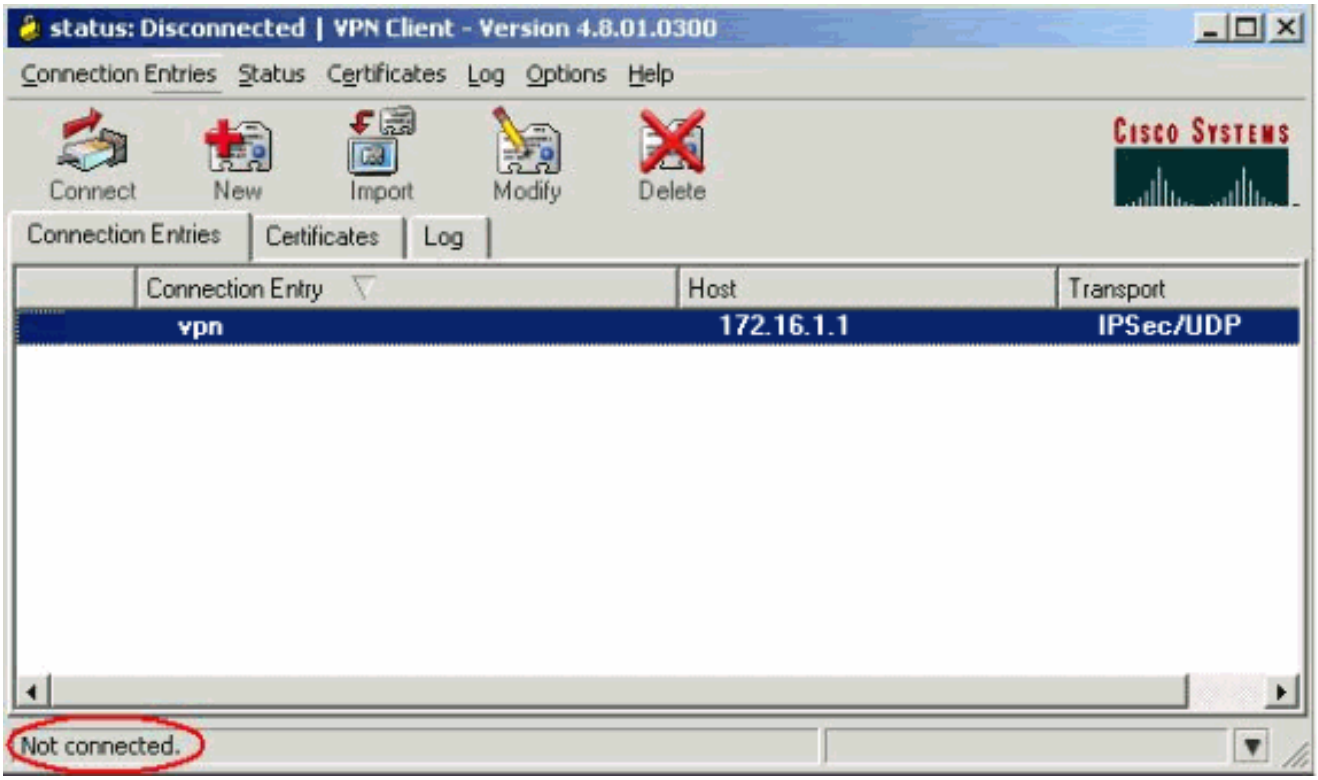
1. Elija el **Start (Inicio) > Programs (Programas) > Cisco Systems VPN Client (VPN Client de Cisco Systems) > al cliente VPN**.
2. Haga clic **nuevo** para iniciar la nueva ventana de entrada de la conexión VPN del crear.



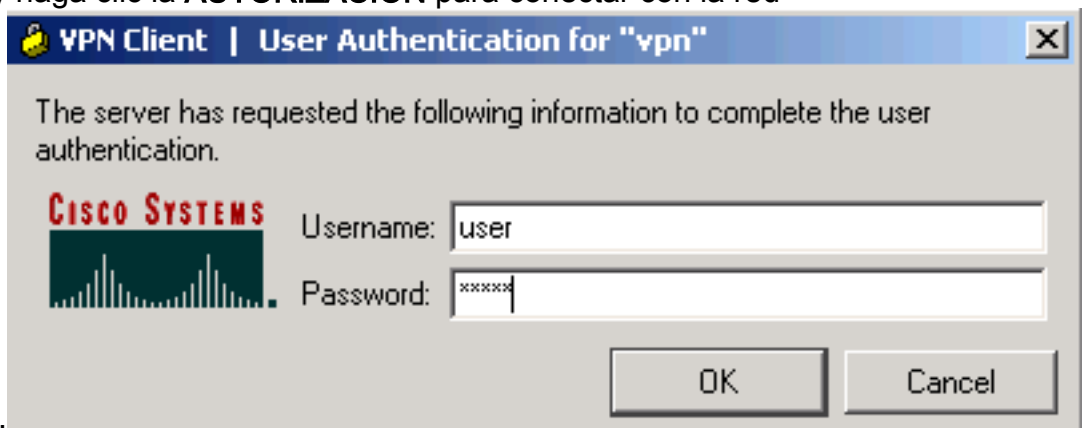
3. Ingrese el nombre del Entrada de conexión junto con una descripción, ingrese el IP Address externo del router en el rectángulo del host, y ingrese el nombre del grupo VPN y la contraseña. Haga clic en Save (Guardar).



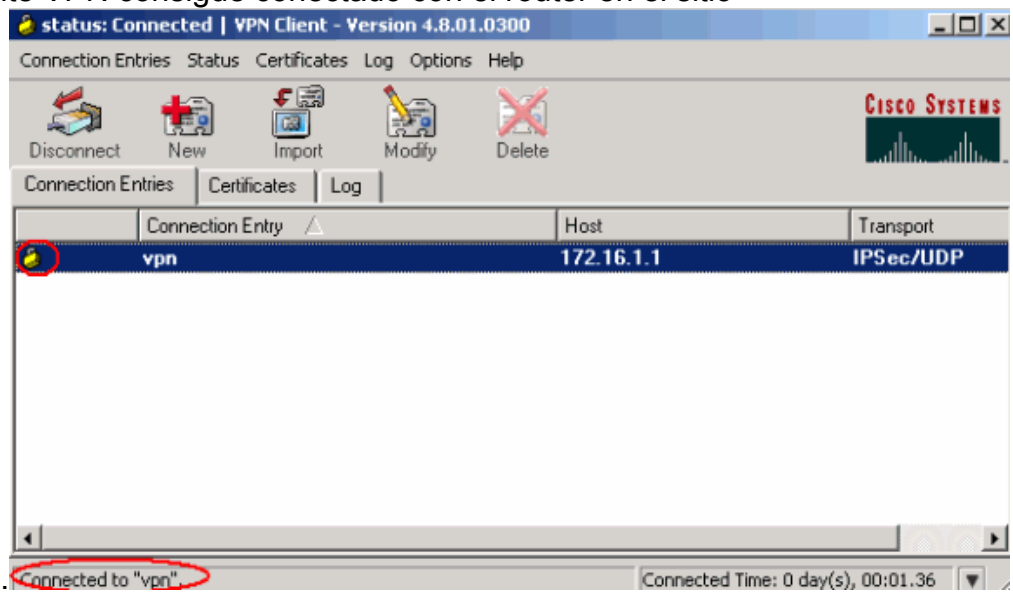
4. Haga clic en la conexión que usted quisiera utilizar y el tecleo **conecta de la** ventana principal del cliente
   VPN.



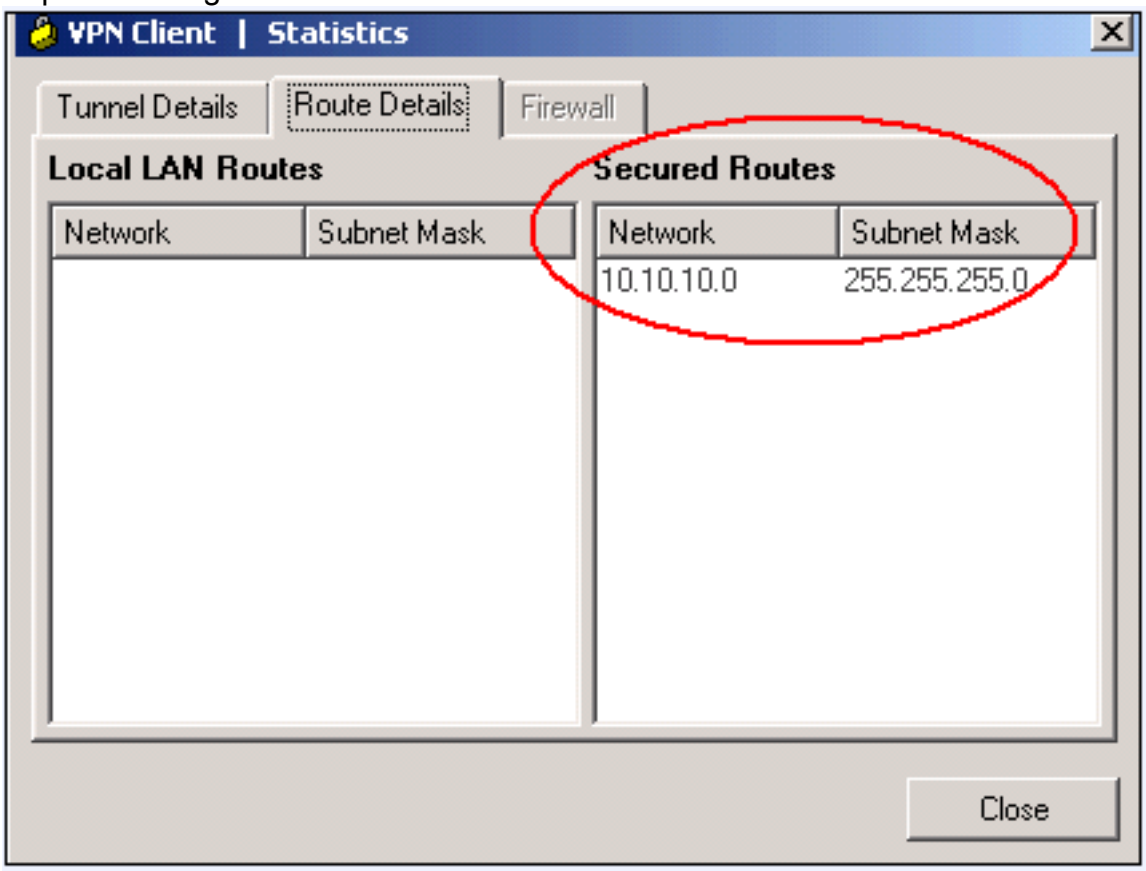
5. Cuando se le pregunte, ingrese la información del nombre de usuario y contraseña para el Xauth y haga clic la **AUTORIZACIÓN** para conectar con la red
   remota.



6. El cliente VPN consigue conectado con el router en el sitio
   central.



7. Elija el **estatus > las estadísticas** para marcar las estadísticas del túnel del cliente VPN.
8. Vaya a la lengueta de los detalles de la ruta para ver las rutas que el cliente VPN asegura al router.En este ejemplo, el cliente VPN asegura el acceso a 10.10.10.0/24 mientras que el resto del tráfico no se cifra y no se envía a través del túnel. La red segura se descarga del ACL 101 que se configura en el router del sitio central.



Verificación

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

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.

- **¿muestre isakmp crypto sa**? Muestra todas las asociaciones de seguridad actuales IKE (SA) en un par.VPN#**show crypto ipsec sa**interface: FastEthernet1/0 Crypto map tag: clientmap, local addr 172.16.1.1 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): (192.168.1.1/255.255.255.255/0/0) current_peer 10.0.0.2 port 500 PERMIT, flags={} **#pkts encaps: 270, #pkts encrypt: 270, #pkts digest: 270 #pkts decaps: 270, #pkts decrypt: 270, #pkts verify: 270** #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 0 **local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.0.0.2** path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0 current outbound spi: 0xEF7C20EA(4017889514) inbound esp sas: spi: 0x17E0CBEC(400608236) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } conn id: 2001, flow_id: SW:1, crypto map: clientmap sa timing: remaining key lifetime (k/sec): (4530341/3288) IV size: 8 bytes replay detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xEF7C20EA(4017889514) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } conn id: 2002, flow_id: SW:2, crypto map: clientmap sa timing: remaining key lifetime (k/sec): (4530354/3287) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound ah sas: outbound pcp sas:

- ¿**muestre IPSec crypto sa**? Muestra las configuraciones usadas por los SA actuales.
```
VPN#show crypto isakmp sa
dst             src             state          conn-id slot status
172.16.1.1      10.0.0.2        QM_IDLE           15    0 ACTIVE
```

Troubleshooting

Comandos para resolución de problemas

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 Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- ¿**IPSec del debug crypto**? Visualiza los IPSec Negotiations de la fase 2.
- ¿**isakmp del debug crypto**? Visualiza negociaciones ISAKMP de la fase 1.

Información Relacionada

- Negociación IPSec/Protocolos IKE
- Cliente Cisco VPN - Soporte de productos
- Router Cisco - Soporte de productos
- Soporte Técnico y Documentación - Cisco Systems