Router y cliente VPN para el Internet pública en un ejemplo de la configuración del palillo

Contenido

Introducción

Este documento describe cómo poner a un router del sitio central para realizar el tráfico IPSec en un palillo. Esta disposición se aplica a un caso específico donde el router, sin la activación del Túnel dividido, y de los usuarios ambulantes (Cliente Cisco VPN) puede tener acceso a Internet vía el router del sitio central. Para alcanzar esto, configure la correspondencia de la directiva en el router para señalar todo el tráfico VPN (Cliente Cisco VPN) a un interfaz del loopback. Esto permite que el tráfico de Internet sea dirección de puerto traducida (PATed) al mundo exterior.

Refiera al cliente del PIX/ASA 7.x y VPN para el Internet pública VPN en un ejemplo de la configuración del palillo para completar una configuración similar en un Firewall del sitio central PIX.

Nota: Para evitar solapar de los IP Addresses en la red, asigne el pool totalmente diverso de los IP Addresses al cliente VPN (por ejemplo, 10.x.x.x, 172.16.x.x, 192.168.x.x). Este esquema de dirección IP le ayuda a resolver problemas su red.

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 3640 de Cisco con el Software Release 12.4 de Cisco IOS®
- 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.

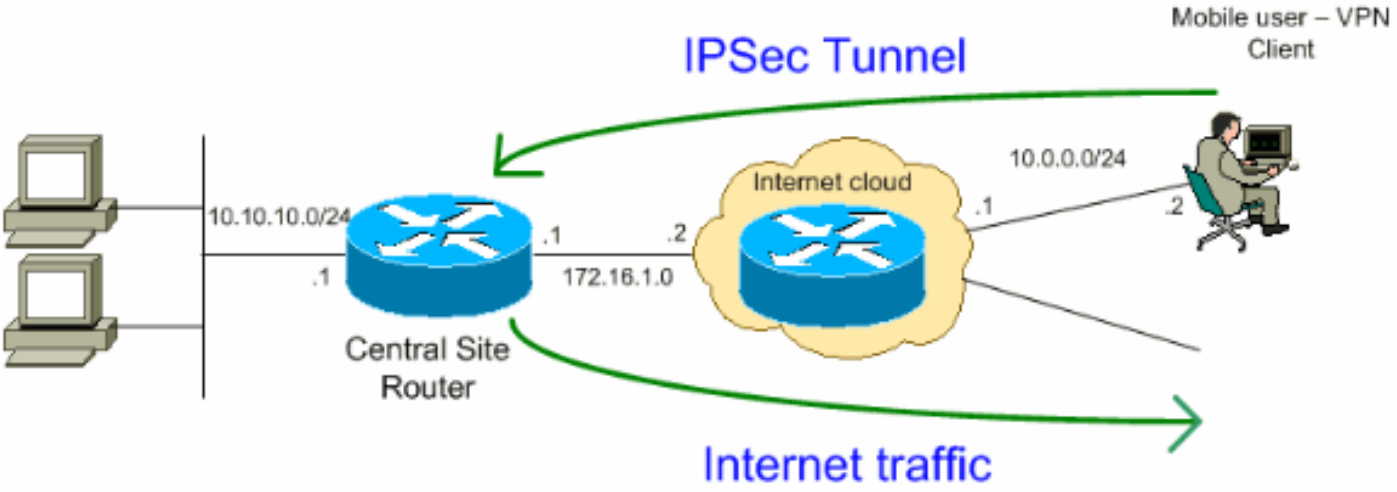
Configurar

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

Nota: Utilice la herramienta de búsqueda de comandos (clientes registrados solamente) para obtener más información sobre los comandos usados 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 los direccionamientos del RFC 1918 que se han utilizado en un entorno del laboratorio.

Configuraciones

Este documento utiliza estas configuraciones:

- Router
- Cliente de Cisco VPN

Router

```
 VPN#show run
Building configuration...

Current configuration : 2170 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN
!
boot-start-marker
boot-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. crypto
isakmp client configuration group vpnclient
 key cisco123
 dns 10.10.10.10
 wins 10.10.10.20
```

```
 domain cisco.com
 pool ippool
!
!--- 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 userauthen
crypto map clientmap isakmp authorization list
groupauthor
crypto map clientmap client configuration address
respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
!
!
!--- Create the loopback interface for the VPN user
traffic . interface Loopback0
 ip address 10.11.0.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 half-duplex
 ip nat inside

!--- Apply the crypto map on the interface. interface
FastEthernet1/0
 ip address 172.16.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 ip policy route-map VPN-Client
 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
```

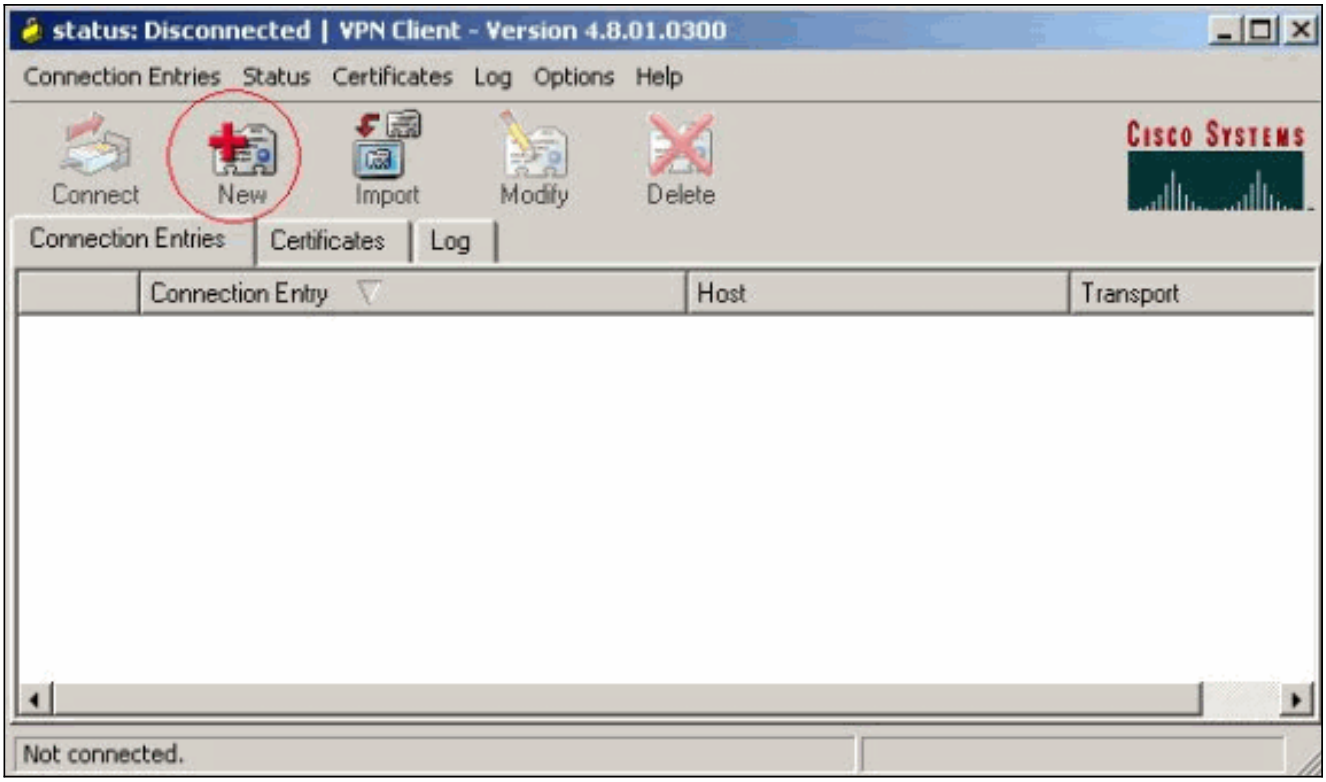
```
192.168.1.2
ip http server
no ip http secure-server
!
ip route 10.0.0.0 255.255.255.0 172.16.1.2
!--- Enables Network Address Translation (NAT) !--- of
the inside source address that matches access list 101
!--- and gets PATed with the FastEthernet IP address. ip
nat inside source list 101 interface FastEthernet1/0
overload
!
!--- The access list is used to specify which traffic is
to be translated for the !--- outside Internet. access-
list 101 permit ip any any

!--- Interesting traffic used for policy route. access-
list 144 permit ip 192.168.1.0 0.0.0.255 any
!--- Configures the route map to match the interesting
traffic (access list 144) !--- and routes the traffic to
next hop address 10.11.0.2. ! route-map VPN-Client
permit 10
 match ip address 144
 set ip next-hop 10.11.0.2
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
end
```

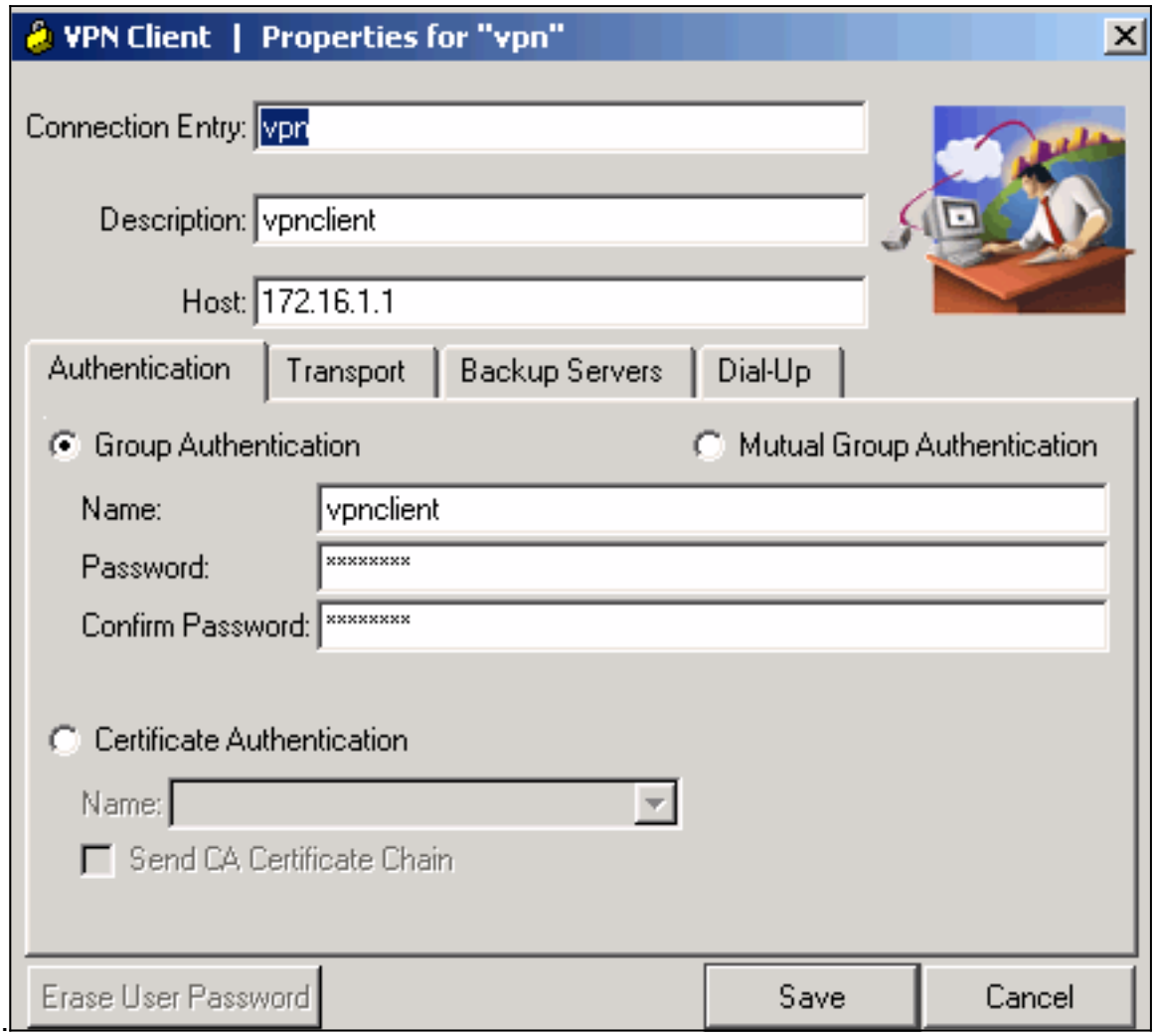
Configuración del cliente 4.8 VPN

Complete estos pasos para configurar al cliente 4.8 VPN.

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



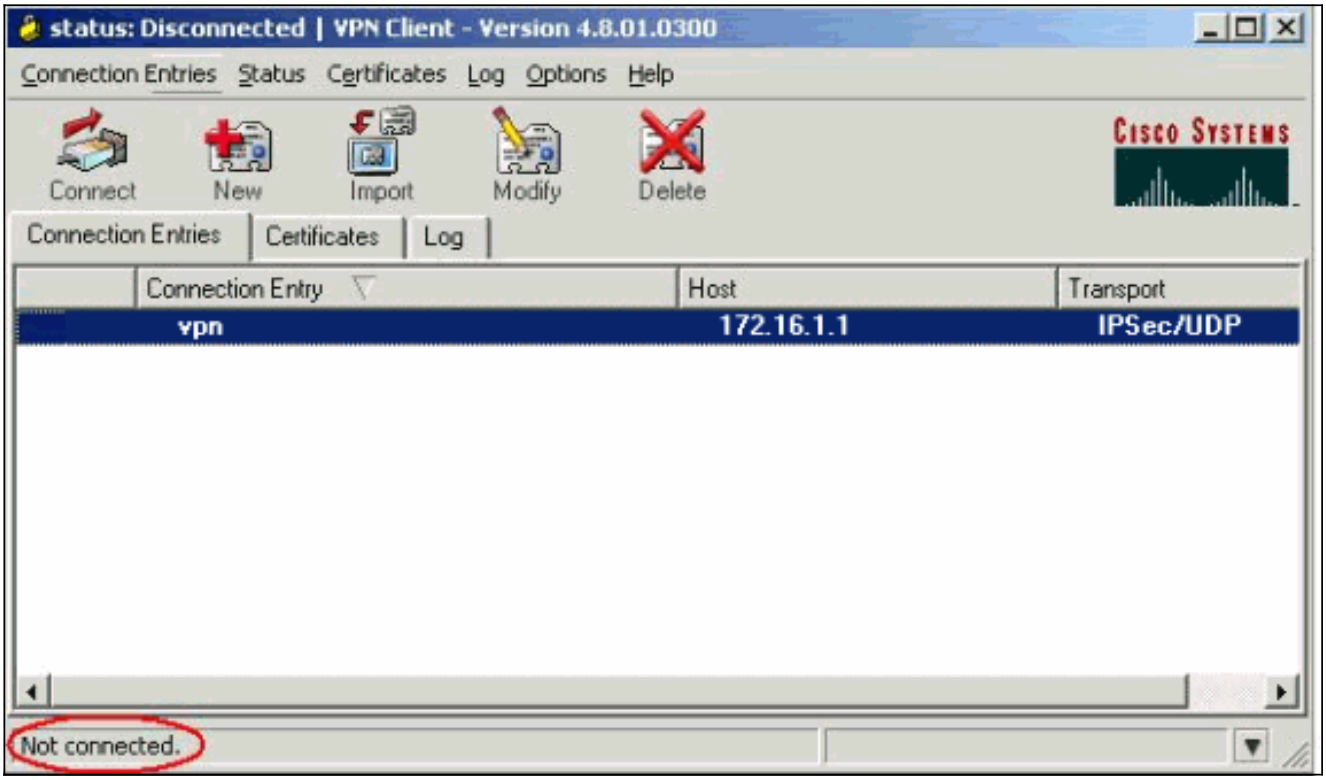
3. Ingrese el nombre del Entrada de conexión junto con una descripción, ingrese el IP address exterior del ranurador en el rectángulo del host, y ingrese el nombre del grupo VPN y la contraseña. Click



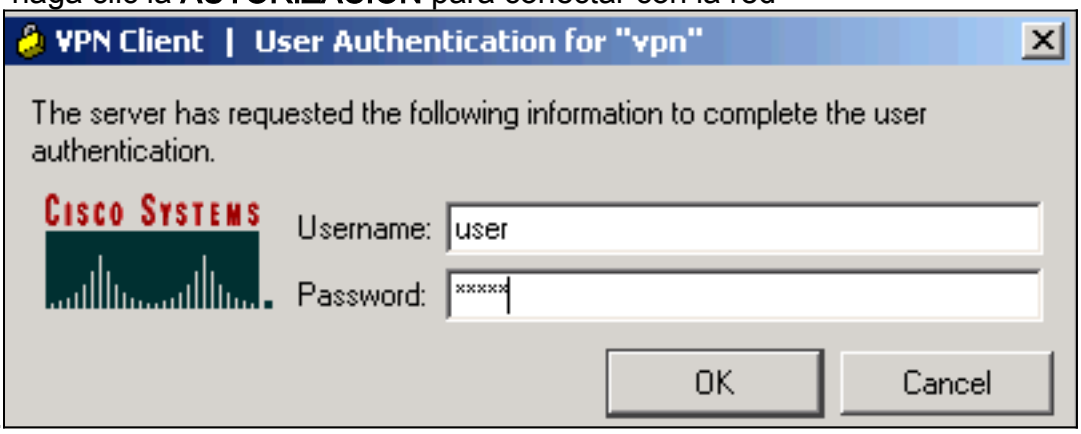
Save.

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

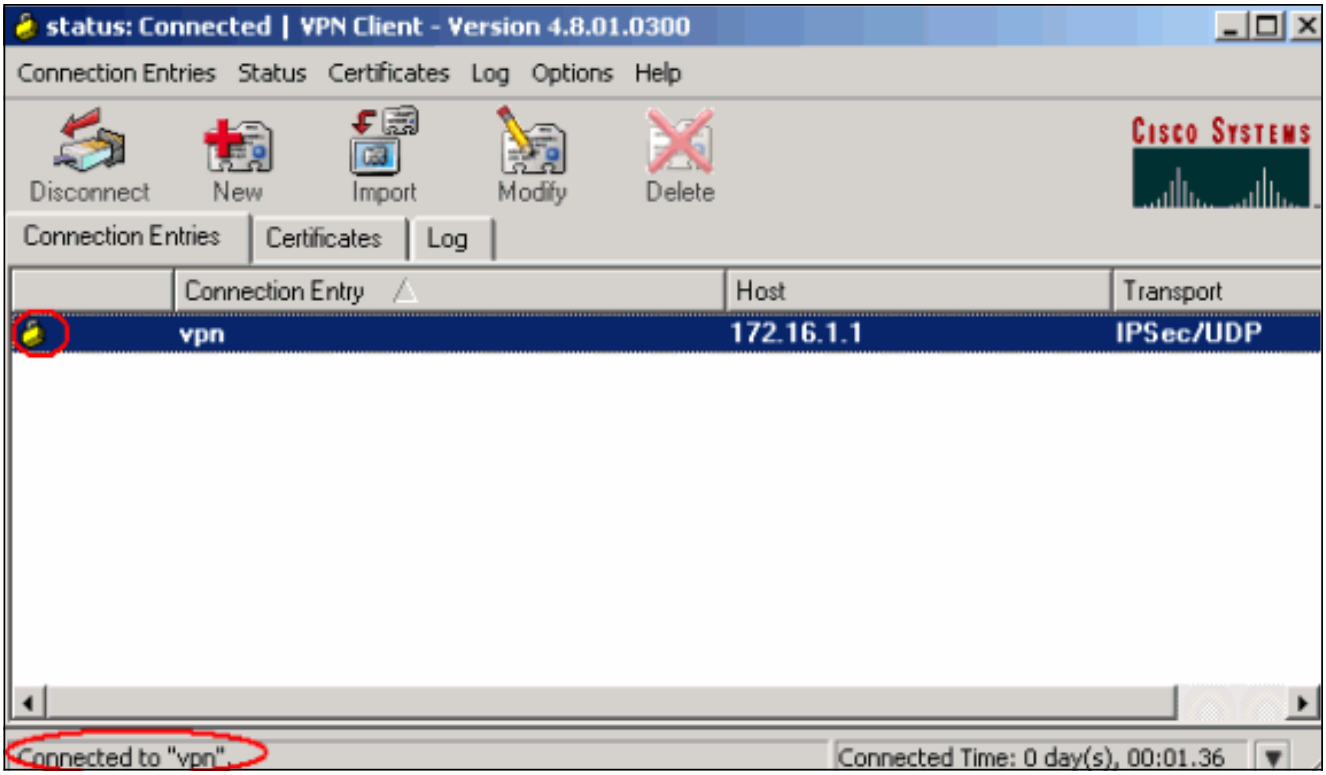
VPN.



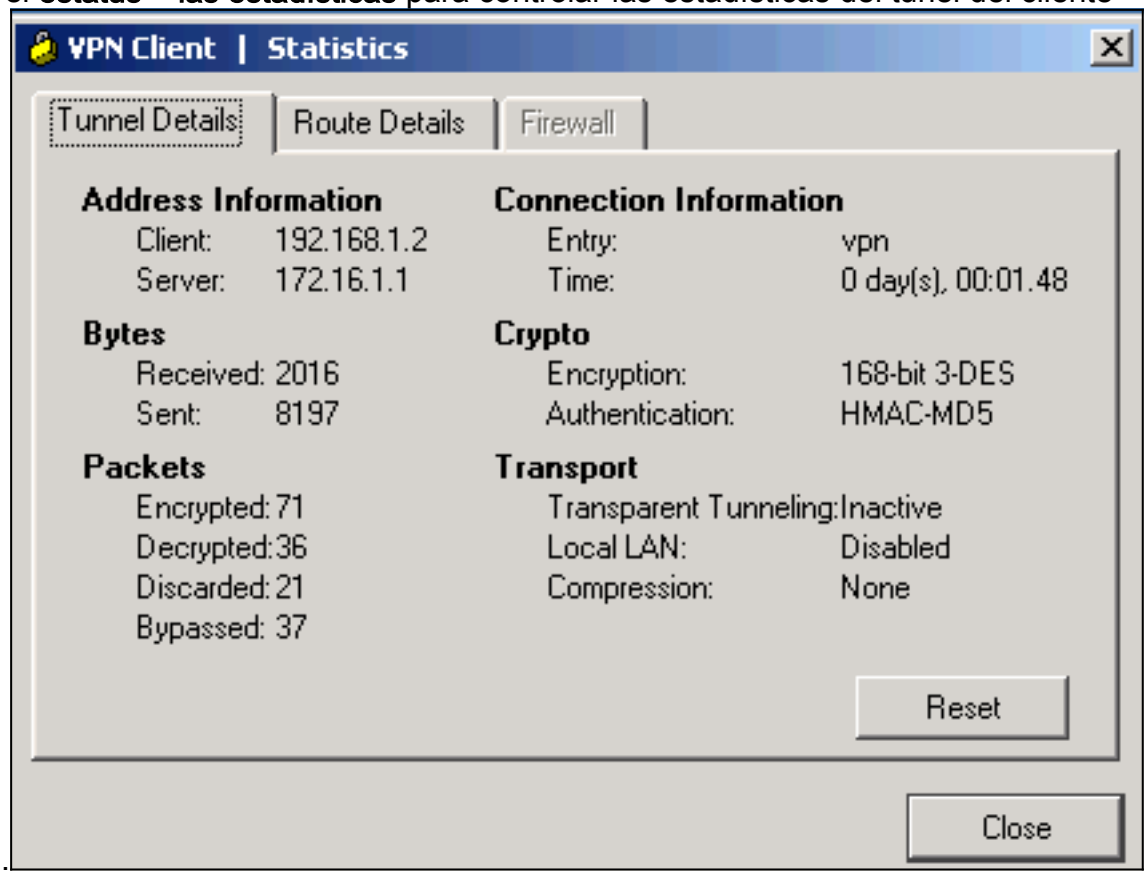
5. Cuando está incitado, ingrese la información del nombre de usuario y contraseña para el Xauth y haga clic la **AUTORIZACIÓN** para conectar con la red remota.



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



7. Elija el **estatus > las estadísticas** para controlar las estadísticas del túnel del cliente VPN.



Verificación

Esta sección proporciona a la información que usted puede utilizar para confirmar sus trabajos de la configuración correctamente.

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

- show crypto isakmp sa: muestra todas las asociaciones actuales de seguridad IKE (SA) de 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 el SAs actual.

```
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 el OIT para ver un análisis de la **salida del comando show**.

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

- **ponga a punto el ipsec crypto** — Visualiza los IPSec Negotiations de la fase 2.
- debug crypto isakmp — Muestra las negociaciones ISAKMP para la fase 1.

Información Relacionada

- Negociación IPSec/Protocolos IKE
- Cliente Cisco VPN - Asistencia técnica
- Soporte del producto de router de Cisco
- Soporte Técnico y Documentación - Cisco Systems