

Ejemplo de Configuración de EzVPN en el Modo NEM con Tunnelización Dividida en el Router IOS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración de cliente VPN](#)

[Verificación y resolución de problemas](#)

[Información Relacionada](#)

[Introducción](#)

Esta configuración detalla la nueva función de Cisco IOS® Software Release 12.3(11)T que permite configurar un router como cliente y servidor EzVPN en la misma interfaz. El tráfico se puede rutear de un cliente VPN al servidor EzVPN, y después a otro servidor EzVPN remoto.

Consulte [Configuración de un Peer LAN a LAN Dinámico de Router IPsec y Clientes VPN](#) para obtener más información sobre el escenario donde hay una configuración de LAN a LAN entre dos routers en un entorno de radio hub con Cisco VPN Clients que también se conectan al hub y se utiliza la autenticación extendida (XAUTH).

Para ver un ejemplo de configuración en EzVPN entre un router Cisco 871 y un router Cisco 7200VXR con modo NEM, refiérase al [Ejemplo de Configuración de Easy VPN Server 7200 a 871 Easy VPN Remote](#).

[Prerequisites](#)

[Requirements](#)

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.

- Cisco IOS Software Release 12.3(11)T en EzVPN Client y el router del servidor.
- Cisco IOS Software Release 12.3(6) en el router del servidor EzVPN remoto (puede ser cualquier versión criptográfica que admita la función de servidor EzVPN).
- Cisco VPN Client versión 4.x

Nota: Este documento se rectificó con un Cisco 3640 Router con Cisco IOS Software Release 12.4(8).

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.

Convenciones

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

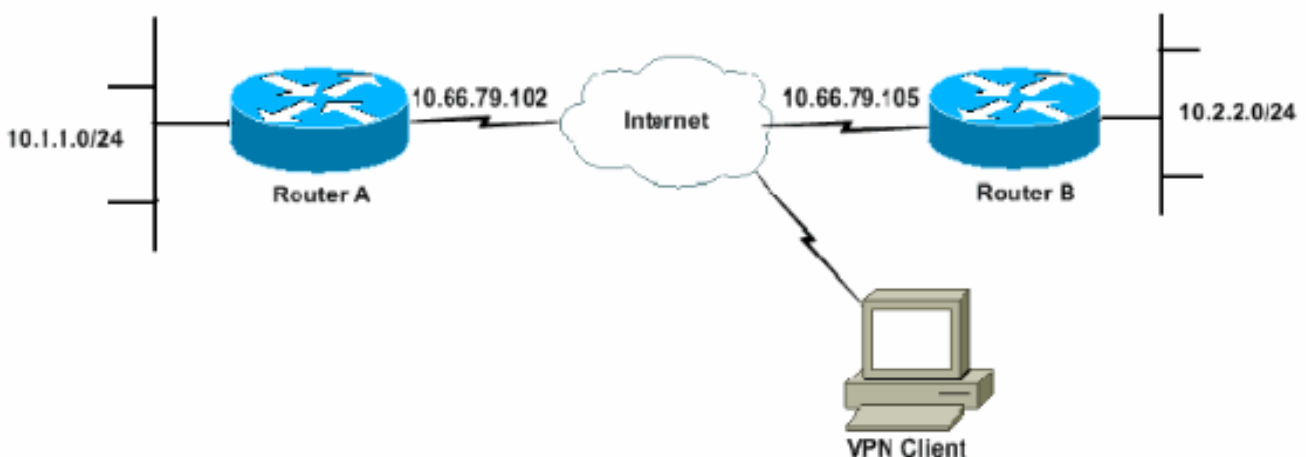
Configurar

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

Nota: Utilice la herramienta [Command Lookup](#) (sólo para clientes [registrados](#)) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este diagrama de red, el RouterA se configura como cliente EzVPN y como servidor. Esto le permite aceptar las conexiones provenientes de los clientes VPN y actuar como cliente EzVPN cuando se conecta al router B. El tráfico desde el cliente VPN puede ser enrutado a las redes detrás del RouterA y del RouterB.



Configuraciones

El RouterA debe configurarse con perfiles IPsec para las conexiones de VPN Client. El uso de

una configuración de servidor EzVPN estándar en este router junto con la configuración de EzVPN Client no funciona. El router no puede llevar a cabo la negociación de la Fase 1.

En esta configuración de ejemplo, el RouterB envía una lista de túnel dividido 10.0.0.0/8 al RouterA. Con esta configuración, el grupo de clientes VPN no puede ser nada dentro de la superred 10.x.x.x. Lo que ocurre es que si el RouterA crea una SA al RouterB para el tráfico desde 10.1.1.0/24 hacia 10.0.0.0/8. Como ejemplo, asuma que tiene una conexión de VPN Client y obtiene una dirección IP de un conjunto local de 10.3.3.1. RouterA genera correctamente otra SA para el tráfico de 10.1.1.0/24 a 10.3.3.1/32. Sin embargo, cuando los paquetes del VPN Client son respondidos y luego llegan al RouterA, el RouterA los envía a través del túnel al RouterB. Esto se debe a que hacen coincidir sus SA de 10.1.1.0/24 con 10.0.0.0/8, en lugar de hacerlo con la coincidencia más específica de 10.3.3.1/32.

También debe configurar la tunelización dividida en el Router B. De lo contrario, el tráfico de VPN Client nunca funciona. Si no tiene definida la tunelización dividida (acl 150 en el Router B en este ejemplo), el RouterA genera una SA para el tráfico de 10.1.1.0/24 a 0.0.0.0/0 (todo el tráfico). Cuando un Cliente VPN conecta y recibe cualquier dirección IP de cualquier agrupación, el tráfico de retorno a él se envía siempre por el túnel al RouterB. Esto se debe a que se hace coincidir primero. Dado que esta SA define "todo el tráfico", cualquiera sea la dirección del agrupamiento de direcciones de su cliente VPN, el tráfico nunca regresa a él.

En resumen, debe utilizar la tunelización dividida y su conjunto de direcciones VPN debe ser una superred diferente a cualquier red de la lista de túnel dividido.

En este documento, se utilizan estas configuraciones:

- [RouterA](#)
- [RouterB](#)

RouterA

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterA
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
enable password cisco
!
username glenn password 0 cisco123
no network-clock-participate slot 1
no network-clock-participate wic 0
aaa new-model
!
!
aaa authentication login userlist local
aaa authorization network groupauthor local
aaa session-id common
ip subnet-zero
ip cef
!
ip dhcp-server 172.17.81.127
```

```

!
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
!
crypto isakmp keepalive 20 10
!
!--- Group definition for the EzVPN server feature. !---
VPN Clients that connect in need to be defined with this
!--- group name/password and are allocated these
attributes. crypto isakmp client configuration group
VPNCLIENTGROUP
  key mnbvcxz
  domain nuplex.com.au
  pool vpn1
  acl 150
!
!
!--- IPsec profile for VPN Clients. crypto isakmp
profile VPNclient
  description VPN clients profile
  match identity group VPNCLIENTGROUP
  client authentication list userlist
  isakmp authorization list groupauthor
  client configuration address respond
!
!
crypto ipsec transform-set 3des esp-3des esp-sha-hmac
!
!
!--- Configuration for EzVPN Client configuration. These
parameters !--- are configured on RouterB. ACL 120 is
the new "multiple-subnet" !--- feature of EzVPN. This
allows the router to build an additional !--- SA for
traffic that matches the line in ACL 120 so that traffic
!--- from VPN Clients are routed over the EzVPN Client
tunnel !--- to RouterB. Without this, VPN Clients are
only able to !--- connect to subnets behind RouterA, and
not RouterB.
crypto ipsec client ezvpn china
  connect auto
  group china key mnbvcxz
  mode network-extension
  peer 10.66.79.105
  acl 120
!
!

crypto dynamic-map SDM_CMAP_1 99
  set transform-set 3des
  set isakmp-profile VPNclient
  reverse-route
!
!
crypto map SDM_CMAP_1 99 ipsec-isakmp dynamic SDM_CMAP_1
!
!
!
interface FastEthernet0/0
  description Outside interface
  ip address 10.66.79.102 255.255.255.224
  ip nat outside

```

```

ip virtual-reassembly
duplex auto
speed auto
crypto map SDM_CMAP_1
crypto ipsec client ezvpn china
!
!
interface FastEthernet1/0
description Inside interface
ip address 10.1.1.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
crypto ipsec client ezvpn china inside
!
!  

!--- IP pool of addresses. Note that this pool must be
!--- a different supernet to any of the split tunnel !--
- networks sent down from RouterB. ip local pool vpn1
192.168.1.1 192.168.1.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.66.79.97
!
no ip http server
no ip http secure-server
ip nat inside source list 100 interface FastEthernet0/0
overload
!
access-list 100 deny ip 10.1.1.0 0.0.0.255 192.168.1.0
0.0.0.255
access-list 100 permit ip 10.1.1.0 0.0.0.255 any

!--- Access-list that defines additional SAs for this !-
-- router to create to the head-end EzVPN server
(RouterB). !--- Without this, RouterA only builds an SA
for traffic !--- from 10.1.1.0 to 10.2.2.0. VPN Clients
!--- that connect (and get a 192.168.1.0 address) !---
are not able to get to 10.2.2.0. access-list 120 permit
ip 192.168.1.0 0.0.0.255 10.0.0.0 0.255.255.255

!--- Split tunnel access-list for VPN Clients. access-
list 150 permit ip 10.1.1.0 0.0.0.255 any
access-list 150 permit ip 10.2.2.0 0.0.0.255 any
dialer-list 1 protocol ip permit
!
!
control-plane
!
!
!
!
line con 0
exec-timeout 0 0
login authentication nada
line aux 0
modem InOut
modem autoconfigure type usr_courier
transport input all
speed 38400
line vty 0 4
transport preferred all
transport input all
!

```

```
!  
end
```

RouterB

```
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname RouterB  
!  
boot-start-marker  
boot-end-marker  
!  
logging buffered 4096 debugging  
!  
aaa new-model  
!  
!  
!--- No XAuth is defined but can be if needed. aaa  
authorization network groupauthor local  
aaa session-id common  
ip subnet-zero  
ip cef  
!  
!  
!  
crypto isakmp policy 1  
  encr 3des  
  authentication pre-share  
  group 2  
crypto isakmp keepalive 10  
!  
!  
!--- Standard EzVPN server configuration, !--- matching  
parameters defined on RouterA. crypto isakmp client  
configuration group china  
  key mnbvcxz  
  acl 150  
!  
!  
crypto ipsec transform-set 3des esp-3des esp-sha-hmac  
!  
crypto dynamic-map dynmap 1  
  set transform-set 3des  
  reverse-route  
!  
!  
!  
crypto map mymap isakmp authorization list groupauthor  
crypto map mymap client configuration address respond  
crypto map mymap 10 ipsec-isakmp dynamic dynmap  
!  
!  
!  
!  
interface Ethernet0/0  
  description Outside interface  
  ip address 10.66.79.105 255.255.255.224  
  half-duplex  
  crypto map mymap  
!
```

```
!  
interface Ethernet0/1  
  description Inside interface  
  ip address 10.2.2.1 255.255.255.0  
  half-duplex  
!  
no ip http server  
no ip http secure-server  
ip classless  
ip route 0.0.0.0 0.0.0.0 10.66.79.97  
!  
!  
access-list 150 permit ip 10.0.0.0 0.255.255.255 any  
!  
!  
line con 0  
  exec-timeout 0 0  
line aux 0  
line vty 0 4  
!  
!  
!  
end
```

Configuración de cliente VPN

Cree una nueva entrada de conexión que haga referencia a la dirección IP del router RouterA. El nombre de grupo en este ejemplo es "VPNCLIENTGROUP" y la contraseña es "mnbvcxz" como se puede ver en la configuración del router.

The screenshot shows the 'VPN Client | Properties for "EzVPN client and server test"' dialog box. It features a title bar with a close button. The main area contains several input fields: 'Connection Entry' (EzVPN client and server test), 'Description' (empty), and 'Host' (10.66.79.102). To the right is an illustration of a person at a computer. Below these fields are four tabs: 'Authentication' (selected), 'Transport', 'Backup Servers', and 'Dial-Up'. The 'Authentication' tab is active, showing two radio button options: 'Group Authentication' (selected) and 'Certificate Authentication'. Under 'Group Authentication', there are fields for 'Name' (VPNCLIENTGROUP), 'Password' (masked with asterisks), and 'Confirm Password' (masked with asterisks). Under 'Certificate Authentication', there is a 'Name' dropdown menu (Glenn (Cisco)) and a checkbox for 'Send CA Certificate Chain' which is unchecked. At the bottom, there are three buttons: 'Erase User Password', 'Save', and 'Cancel'.

[Verificación y resolución de problemas](#)

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente. Refiérase a [Troubleshooting de Seguridad IP - Comprensión y Uso de los Comandos de debug](#) para obtener información adicional de verificación/Troubleshooting. Si encuentra algún problema o error de VPN Client, refiérase a la [Herramienta de Búsqueda de Error GUI de VPN Client](#).

[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.

[Información Relacionada](#)

- [Configuración del Perfil IPsec](#)
- [Página de soporte para cliente Cisco VPN](#)
- [Página de Soporte de IPsec Negotiation/IKE Protocols](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)