EzVPN no modo NEM com tunelamento dividido no exemplo de configuração do roteador IOS

Contents

Introduction

Esta configuração detalha a nova característica no Cisco IOS® Software Release 12.3(11)T que permite a configuração de um roteador como um EzVPN Client e o servidor na mesma interface. O tráfego pode ser roteado de um Cliente VPN para o servidor de EzVPN e, então, de volta para outro servidor remoto de EzVPN.

Consulte Configurando um Ponto de LAN para LAN Dinâmico de um Roteador IPsec e Clientes VPN para saber mais sobre o cenário em que há uma configuração de LAN para LAN entre dois roteadores em um ambiente hub-spoke com Cisco VPN Clients também se conectam ao hub e a Autenticação Estendida (XAUTH) é usada.

Para obter um exemplo de configuração no EzVPN entre um roteador Cisco 871 e um roteador Cisco 7200VXR com modo NEM, consulte Exemplo de Configuração Remota do 7200 Easy VPN Server para 871 Easy VPN.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Software Cisco IOS versão 12.3(11)T no EzVPN Client e roteador de servidor.
- Software Cisco IOS versão 12.3(6) no roteador do servidor EzVPN remoto (pode ser qualquer versão de criptografia que suporte o recurso do servidor EzVPN).
- Cisco VPN Client versão 4.x

Observação: este documento foi recertificado com um Cisco 3640 Router com 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.

Conventions

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

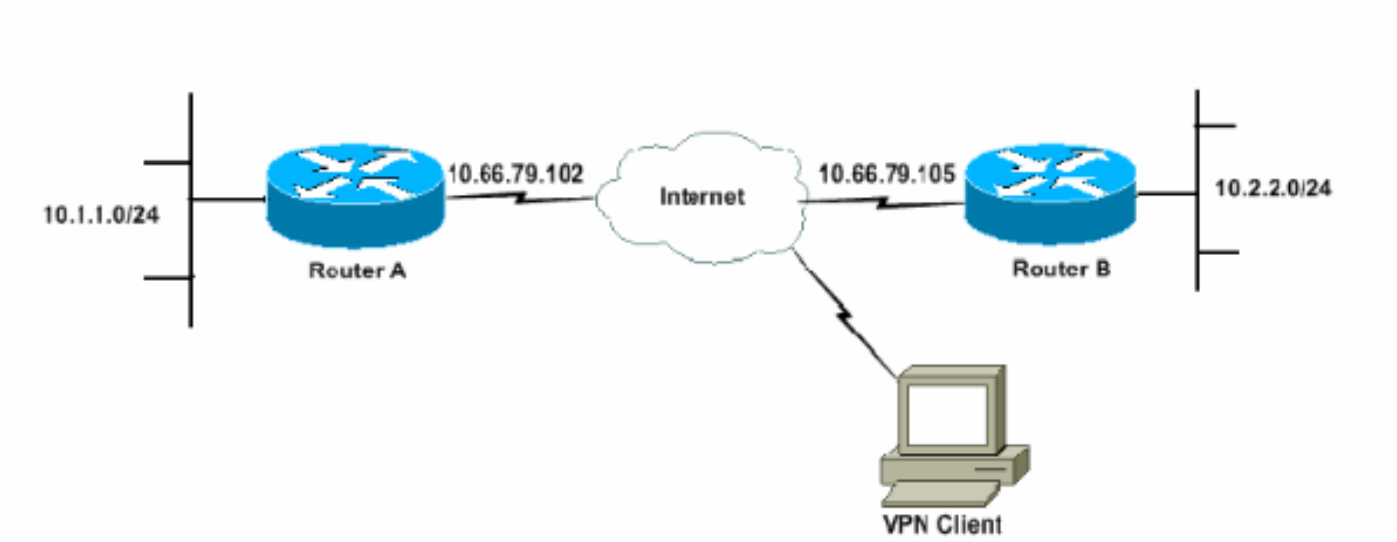
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

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

Diagrama de Rede

Neste diagrama de rede, o Roteador A é configurado como um EzVPN Client e um servidor. Isso permite que ele aceite conexões de clientes VPN e funcione como cliente EzVPN quando se conecta ao roteador B. O tráfego do cliente VPN pode ser roteado para as redes depois do roteador A e do roteador B.



Configurações

O RouterA deve ser configurado com perfis IPsec para as conexões do VPN Client. O uso de uma

configuração padrão de servidor EzVPN neste roteador junto com a configuração do EzVPN Client não funciona. O roteador falha na negociação da fase 1.

Nesta configuração de exemplo, o RouterB envia uma lista de túneis divididos 10.0.0.0/8 para o RouterA. Com esta configuração, o pool de VPN Client não pode ser nada além de 10.x.x.x supernet. O que ocorre é que o Roteador A cria um SA para o RoteadorB para o tráfego a partir de 10.1.1.0/24 para 10.0.0.0/8. Por exemplo, suponha que você tenha uma conexão de VPN Client e obtenha um endereço IP de um pool local de 10.3.3.1. O RoteadorA cria com êxito outro SA para tráfego de 10.1.1.0/24 para 10.3.3.1/32. No entanto, quando os pacotes do VPN Client são respondidos e, em seguida, acessam o RouterA, o RouterA os envia pelo túnel para o RouterB. Isso ocorre porque eles correspondem a seu SA de 10.1.1.0/24 a 10.0.0.0/8 em vez de uma correspondência mais específica de 10.3.3.1/32.

Você também deve configurar o tunelamento dividido no RouterB. Caso contrário, o tráfego do VPN Client nunca funcionará. Se você não tiver o tunelamento dividido definido (acl 150 no RouterB neste exemplo), o RouterA cria um SA para o tráfego de 10.1.1.0/24 para 0.0.0.0/0 (todo o tráfego). Quando um VPN Client se conectar e receber um endereço IP fora de qualquer pool, o tráfego de retorno para ele será sempre enviado sobre o túnel para o RoteadorB. Isso porque ele é comparado primeiro. Como esse SA define todo o tráfego, não importa qual é o conjunto de endereços do cliente de VPN: o tráfego nunca retorna a ele.

Em resumo, você deve usar o tunelamento dividido e seu pool de endereços VPN deve ser uma super-rede diferente de qualquer rede na lista de túneis divididos.

Este documento utiliza as seguintes configurações:

- RoteadorA
- RoteadorB

RoteadorA

```
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
```

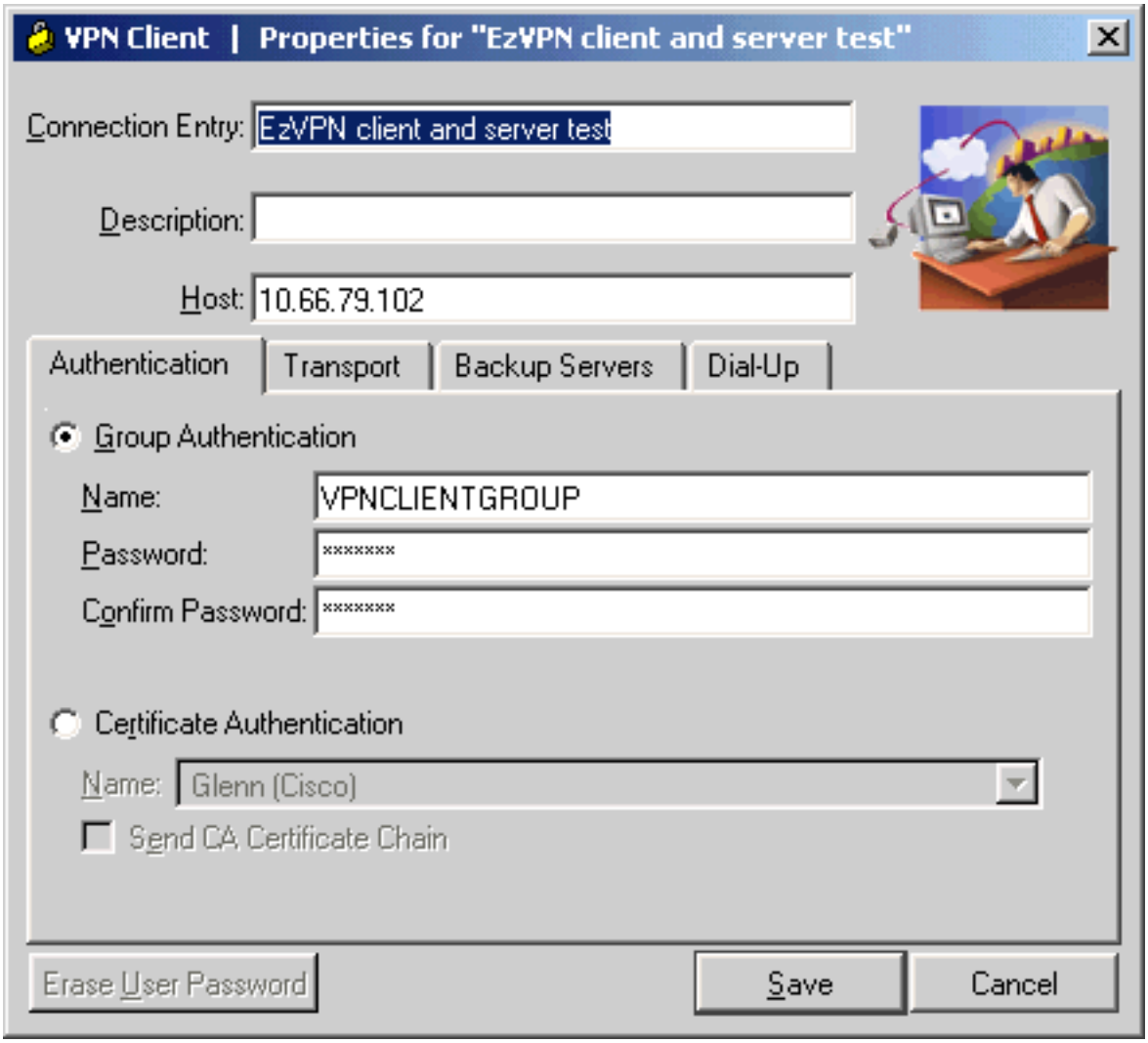
RoteadorB

```
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
```

Configuração de cliente de VPN

Crie uma nova entrada de conexão que faça referência ao endereço IP do roteador RouterA. O nome do grupo neste exemplo é VPNCLIENTGROUP e a senha é mnbvcxz, como pode ser visto na configuração do roteador.



Verificar e solucionar problemas

Esta seção fornece informações que você pode usar para confirmar se sua configuração funciona adequadamente. Consulte IP Security Troubleshooting - Understanding and Using debug Commands para obter informações adicionais sobre verificação/solução de problemas. Se você encontrar algum problema ou erro no VPN Client, consulte a Ferramenta de pesquisa de erros da GUI do VPN Client.

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

Informações Relacionadas

- Configuração do perfil IPsec
- Página de Suporte do Cisco VPN Client
- Página de Suporte de Negociação IPSec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems