EzVPN no modo NEM com a separação que escava um túnel no exemplo de configuração do IOS Router

Índice

Introdução

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.

Refira configurar um par dinâmico do LAN para LAN do roteador de IPSec e os clientes VPN a fim aprender mais sobre a encenação onde há uma configuração de LAN para LAN entre dois Roteadores em um ambiente do hub-spoke com Cisco VPN Client igualmente conectam ao hub e à autenticação extendida (XAUTH) são usados.

Para uma configuração de exemplo no EzVPN entre um Cisco 871 Router e um Cisco 7200VXR Router com modo NEM, refira 7200 Easy VPN Server ao exemplo de configuração do Easy VPN Remote 871.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco IOS Software Release 12.3(11)T no cliente ezvpn e no roteador de servidor.
- Cisco IOS Software Release 12.3(6) no roteador remoto do servidor de EzVPN (esta pode ser toda a versão de criptografia que apoiar a característica do servidor de EzVPN).
- Versão Cliente VPN Cisco 4.x

Nota: Este documento recertified com um Cisco 3640 Router com Cisco IOS Software Release 12.4(8).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

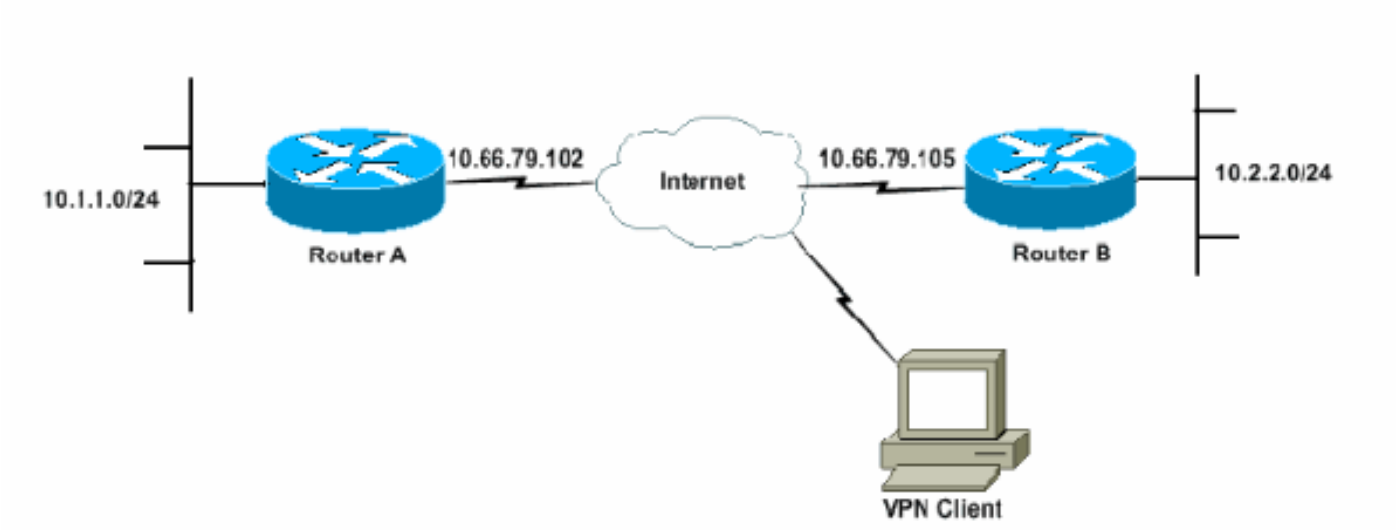
Configurar

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 da rede, o roteadorA é configurado como um cliente ezvpn e o server. 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 roteadorA tem que ser configurado com perfis IPSec para as conexões de cliente de VPN. O uso de uma configuração de servidor de EzVPN padrão neste roteador junto com a configuração de cliente ezvpn não trabalha. O roteador falha na negociação da fase 1.

Nesta configuração de exemplo, o roteadorB envia uma lista de túneis em divisão 10.0.0.0/8 ao roteadorA. 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. Como um exemplo, supõe que você manda um cliente VPN conectar e obter um endereço IP de Um ou Mais Servidores Cisco ICM NT fora de um conjunto local de 10.3.3.1. O roteadorA constrói com sucesso um outro SA para o tráfego de 10.1.1.0/24 a 10.3.3.1/32. Contudo, quando os pacotes do cliente VPN são respondidos a e roteadorA então batido, o roteadorA envia-os sobre o túnel ao roteadorB. 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 deve igualmente configurar a separação que escava um túnel no roteadorB. Se não, o tráfego do cliente VPN nunca trabalha. Se você não rachou a escavação de um túnel definida (acl 150 no roteadorB neste exemplo), o roteadorA constrói um SA para o tráfego de 10.1.1.0/24 a 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. Isto é porque obtém combinado sobre primeiramente. 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 a separação-escavação de um túnel, e seu conjunto de endereços VPN deve ser um super-rede diferente do que toda a rede na lista de túneis em divisão.

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
```

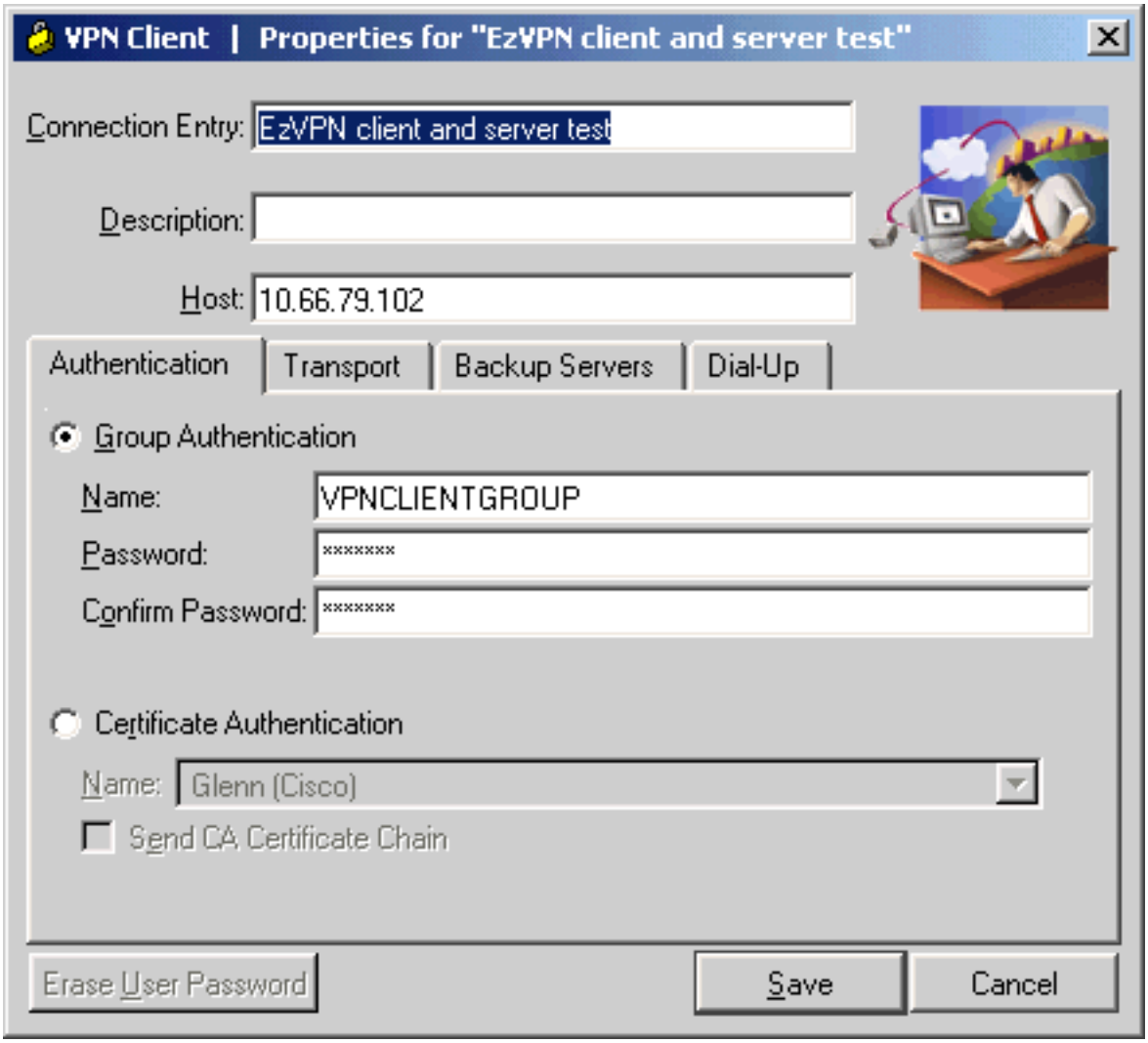
RoteadorB

```
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 entrada da nova conexão que proveja o roteadorA do endereço IP de roteador. 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. Refira o Troubleshooting de Segurança IP - Compreendendo e usando comandos debug para a verificação/informação de Troubleshooting adicionais. Se você encontra quaisquer edições ou erros do cliente VPN, refira a ferramenta da Consulta de Erro de GUI do cliente VPN.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta 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