EzVPN in NEM-modus met splitter-tunneling op het IOS-routerconfiguratievoorbeeld

Inhoud

Inleiding

Deze configuratie details de nieuwe functie in Cisco IOS® softwarerelease 12.3(11)T die u in staat stelt om een router als EzVPN-client en server op dezelfde interface te configureren. Het verkeer kan van een VPN-client naar de EzVPN-server worden verstuurd en dan terug naar een andere externe EzVPN-server.

Raadpleeg een IPsec-routerclient configureren met dynamisch LAN-to-LAN peer en VPN-clients om meer te weten te komen over het scenario waarin er een LAN-to-LAN configuratie is tussen twee routers in een op een hub gebaseerde omgeving met Cisco VPN-clients. U sluit ook een verbinding aan met de hub en de uitgebreide verificatie (XAUTH) wordt gebruikt.

Voor een voorbeeldconfiguratie op EzVPN tussen een Cisco 871 router en een Cisco 7200VXR router met NEM-modus, raadpleeg de 7200 Easy VPN-server aan 871 Easy VPN Remote Configuration-voorbeeld.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS-softwarerelease 12.3(11)T op de EzVPN-client- en serverrouter.
- Cisco IOS-softwarerelease 12.3(6) op de externe EzVPN-serverrouter (dit kan een crypto-versie zijn die de EzVPN-serverfunctie ondersteunt).
- Cisco VPN-client versie 4.x

N.B.: Dit document is herkend met een Cisco 3640 router met Cisco IOS-softwarerelease 12.4(8).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

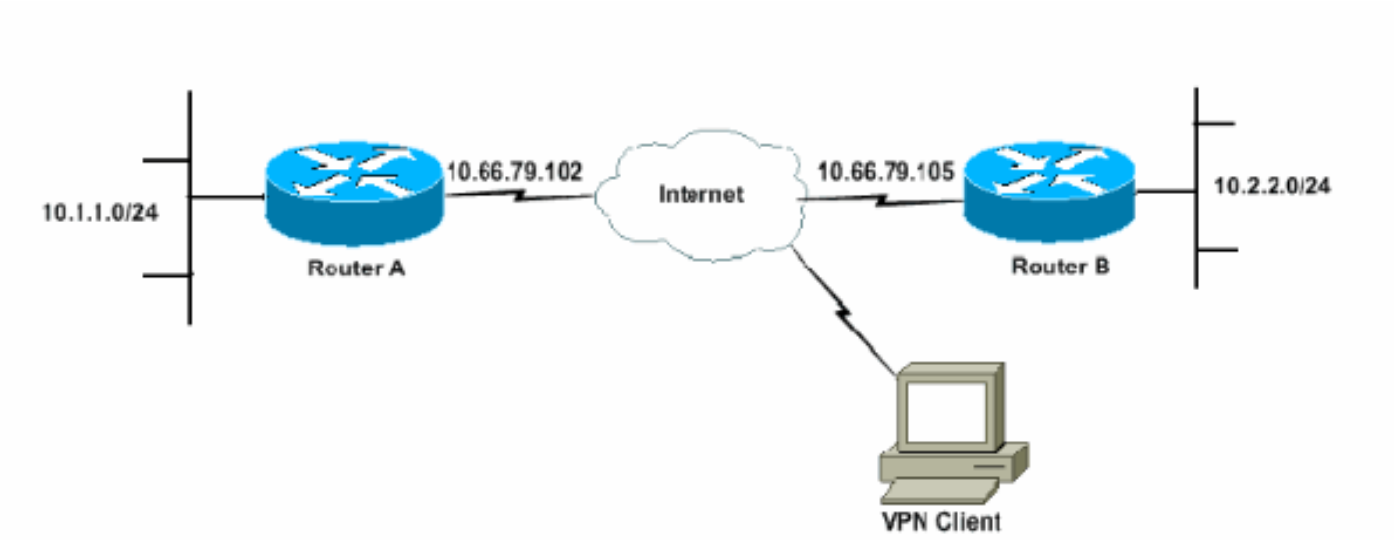
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

In dit netwerkdiagram wordt RouterA ingesteld als zowel een EzVPN-client als een server. Dit staat het toe om verbindingen van de Clients van VPN te accepteren en om als client voor EzVPN te handelen wanneer het verbonden is met RouterB. Het verkeer van de client van VPN kan naar de netwerken achter RouterA en RouterB worden verstuurd.



Configuraties

RouterA moet met IPsec-profielen worden geconfigureerd voor de VPN-clientverbindingen. Het gebruik van een standaard EzVPN-serverconfiguratie op deze router samen met de EzVPN-

clientconfiguratie werkt niet. De router faalt fase 1 onderhandeling.

In deze voorbeeldconfiguratie, verstuurt RouterB een 10.0.0.0/8 splitsing-tunnellijst naar RouterA. Bij deze configuratie kan de VPN-clientpool niet in de 10.x.x.x-supernet worden geplaatst. Wat er gebeurt is dat RouterA een SA aan RouterB voor verkeer van 10.1.1.0/24 aan 10.0.0.0/8 bouwt. Als voorbeeld, veronderstel dat u een client heeft en een IP adres uit een lokale pool van 10.3.3.1 krijgt. RouterA bouwt met succes een andere SA voor verkeer van 10.1.1.0/24 aan 10.3.3.1/32. Maar wanneer pakketten van de VPN client worden geantwoord op en dan router A, RouterA stuurt ze over de tunnel naar RouterB. Dit komt doordat ze overeenkomen met hun SA van 10.1.1.0/24 naar 10.0.0.0/8 in plaats van de specifiekere match van 10.3.3.1/32.

U moet ook gesplitste tunneling op RouterB configureren. Anders werkt VPN-clientverkeer nooit. Als u geen gesplitste tunneling gedefinieerd hebt (vraag 150 op RouterB in dit voorbeeld), bouwt RouterA een SA voor verkeer van 10.1.1.0/24 tot 0.0.0.0/0 (al verkeer). Wanneer een VPN-client een IP-adres uit een pool verbindt en ontvangt, wordt het retourverkeer via de tunnel naar RouterB verzonden. Dat komt omdat het eerst wordt aangepast. Aangezien deze SA "al verkeer" definieert, maakt het niet uit wat uw VPN-adrespool is, het verkeer komt er nooit meer terug.

Samengevat, moet u een gesplitste tunneling gebruiken, en uw VPN-adrespool moet een ander supernet zijn dan een netwerk in de lijst met gesplitste tunnels.

Dit document gebruikt deze configuraties:

- 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
```

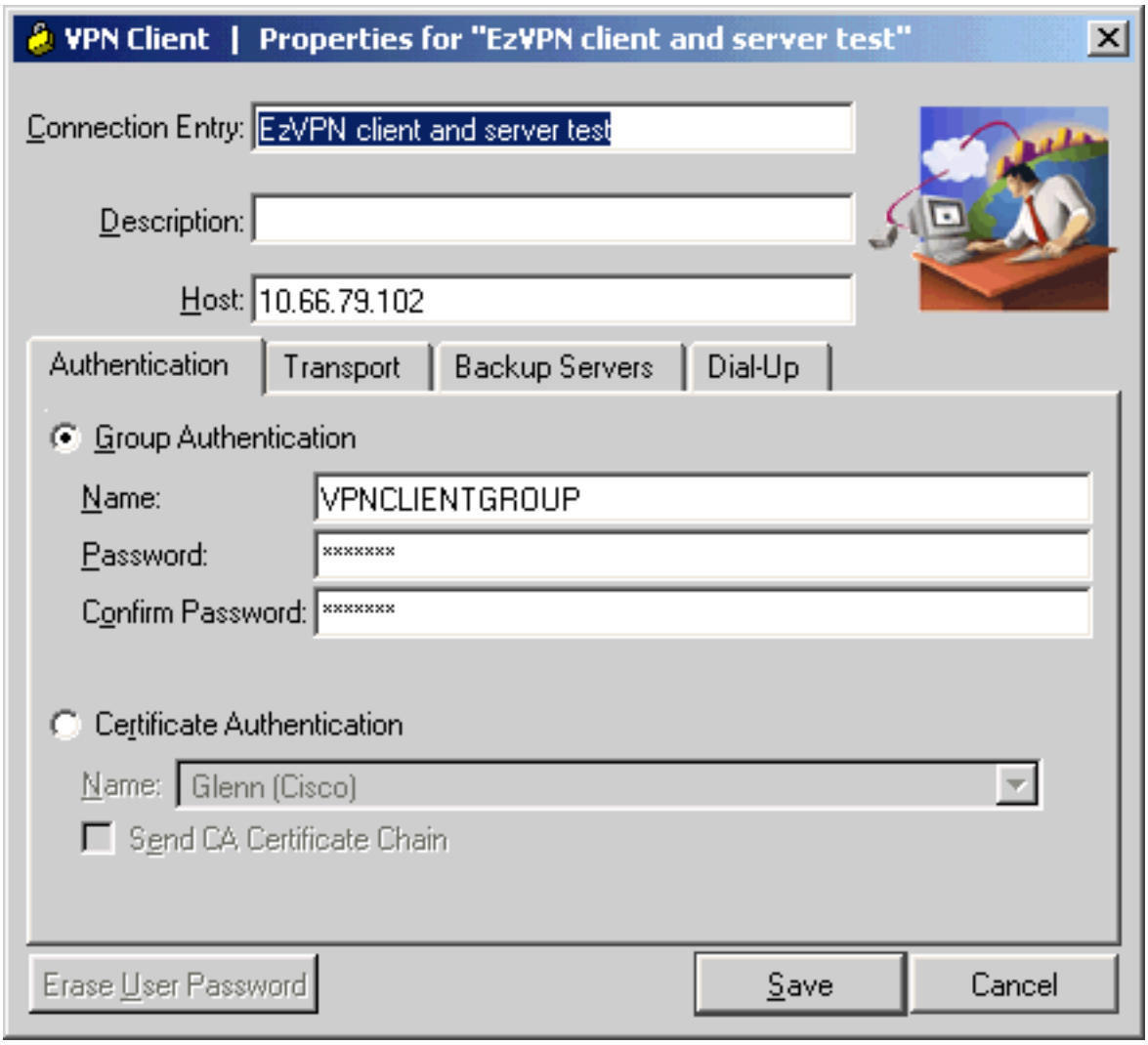
routerB

```
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
```

VPN-clientconfiguratie

Maak een nieuwe verbinding die verwijzingen het IP adres van routerA. De groepsnaam in dit voorbeeld is "VPNCLIENTGROUP" en het wachtwoord is "mnbvcxz" zoals in de routerconfiguratie kan worden gezien.



Probleemoplossing controleren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt. Raadpleeg het gedeelte IP-beveiligingsprobleemoplossing - Oplossingen begrijpen en gebruiken voor extra informatie over verificatie/probleemoplossing. Als u problemen of fouten met VPN-client hebt, raadpleegt u het VPN-clientgereedschap GUI-fout in de bijlage.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Gerelateerde informatie

- Configuratie van IPsec-profiel
- Cisco VPN-clientondersteuningspagina
- Ondersteuning van IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems