IOS 라우터 컨피그레이션에서 스플릿 터널링을 사용하는 NEM 모드의 EzVPN 컨피그레이션 예

목차

소개

이 컨피그레이션에서는 라우터를 EzVPN 클라이언트로 구성하고 동일한 인터페이스에서 서버를 구성할 수 있는 Cisco IOS® Software Release 12.3(11)T의 새로운 기능에 대해 자세히 설명합니다 .트래픽은 VPN 클라이언트에서 EzVPN 서버로 라우팅된 다음 다른 원격 EzVPN 서버로 다시 라우팅될 수 있습니다.

Cisco VPN 클라이언트가 허브에 연결되고 XAUTH(Extended Authentication)가 사용되는 허브 스포크 환경의 두 라우터 간에 LAN-to-LAN 구성이 있는 시나리오에 대한 자세한 내용은 IPsec 라우터 동적 LAN-to-LAN 피어 및 VPN 클라이언트 구성을 참조하십시오.

Cisco 871 라우터와 Cisco 7200VXR Router with NEM Mode 사이의 EzVPN에 대한 샘플 컨피그레이션은 7200 Easy VPN Server to 871 Easy VPN Remote Configuration Example을 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- EzVPN 클라이언트 및 서버 라우터의 Cisco IOS Software 릴리스 12.3(11)T

- 원격 EzVPN 서버 라우터의 Cisco IOS Software 릴리스 12.3(6)(EzVPN 서버 기능을 지원하는 모든 암호화 버전일 수 있음).
- Cisco VPN Client 버전 4.x

참고: 이 문서는 Cisco IOS Software 릴리스 12.4(8)가 포함된 Cisco 3640 라우터로 수정되었습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

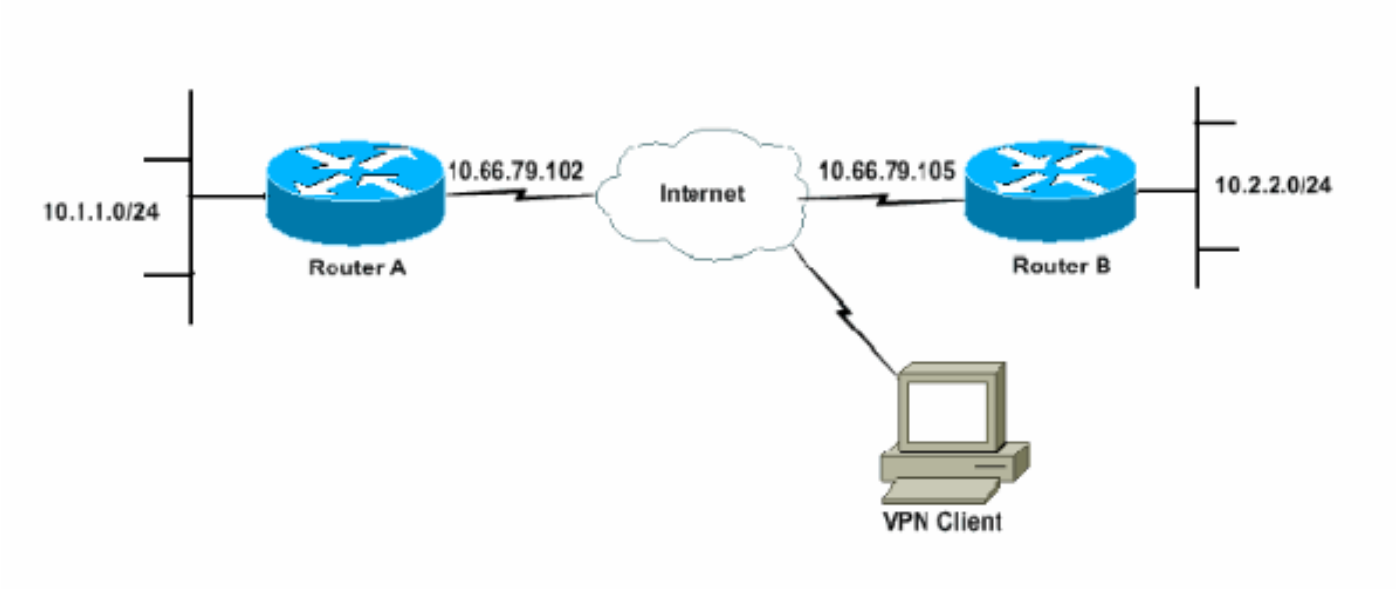
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 네트워크 다이어그램에서 RouterA는 EzVPN 클라이언트 및 서버로 구성됩니다.이를 통해 VPN 클라이언트의 연결을 수락하고 RouterB에 연결할 때 EzVPN 클라이언트 역할을 수행할 수 있습니다.VPN 클라이언트의 트래픽은 RouterA 및 RouterB 뒤의 네트워크로 라우팅될 수 있습니다.



구성

RouterA는 VPN 클라이언트 연결을 위해 IPsec 프로필을 사용하여 구성해야 합니다.이 라우터에서 표준 EzVPN 서버 컨피그레이션과 EzVPN 클라이언트 컨피그레이션을 함께 사용해도 작동하지 않습니다.라우터가 1단계 협상에 실패합니다.

이 샘플 컨피그레이션에서는 RouterB가 10.0.0.0/8 스플릿 터널 목록을 RouterA로 전송합니다.이

컨피그레이션에서는 VPN 클라이언트 풀이 10.x.x.x 슈퍼넷에서 아무것도 될 수 없습니다 .RouterA는 10.1.1.0/24에서 10.0.0.0/8로의 트래픽에 대해 RouterB에 SA를 구축합니다. 예를 들어, VPN Client가 연결되어 있고 로컬 풀 10.3.3.1에서 IP 주소를 얻는다고 가정합니다. RouterA는 10.1.1.0/24에서 10.3.3.1/32으로 트래픽에 대해 다른 SA를 성공적으로 구축합니다. 그러나 VPN 클라이언트에서 패킷을 수신한 다음 RouterA를 통해 RouterA를 실행하면 RouterA를 통해 해당 패킷을 전송합니다. RouterB에 터널링합니다.이는 10.3.3.1/32의 보다 구체적인 일치 대신 10.1.1.0/24의 SA를 10.0.0.0/8과 일치시키기 때문입니다.

또한 RouterB에서 스플릿 터널링을 구성해야 합니다.그렇지 않으면 VPN 클라이언트 트래픽이 작동하지 않습니다.스플릿 터널링이 정의되지 않은 경우(이 예에서는 RouterB에서 acl 150), RouterA는 10.1.1.0/24에서 0.0.0.0/0(모든 트래픽)으로 트래픽에 대한 SA를 구축합니다. VPN Client가 어떤 풀에서도 IP 주소를 연결 및 수신하면 반환 트래픽은 항상 터널을 통해 RouterB로 전송됩니다.처음에는 매치되기 때문입니다.이 SA는 "모든 트래픽"을 정의하므로 VPN 클라이언트 주소 풀이 무엇인지는 중요하지 않으므로 트래픽은 다시 수신되지 않습니다.

요약하자면 스플릿 터널링을 사용해야 하며, VPN 주소 풀은 스플릿 터널 목록의 어떤 네트워크와는 다른 수퍼넷이어야 합니다.

이 문서에서는 다음 구성을 사용합니다.

- 라우터A
- 라우터B

라우터A

```
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
```

라우터B

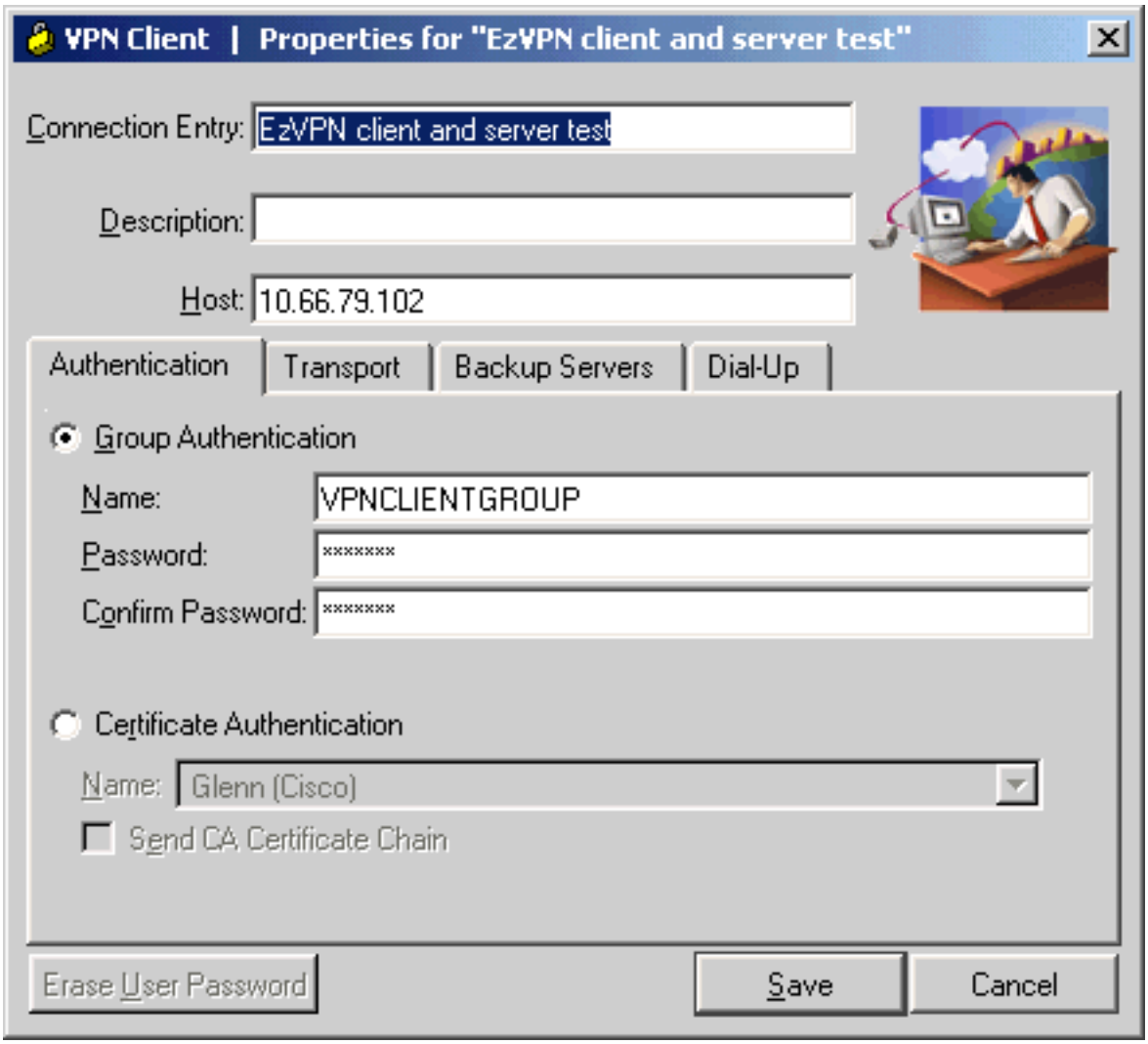
```
version 12.4
```

```
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 클라이언트 컨피그레이션

라우터 RouterA의 IP 주소를 참조하는 새 연결 항목을 만듭니다.이 예에서 그룹 이름은 "VPNCLIENTGROUP"이고 암호는 "mnbvcxz"이며 라우터 컨피그레이션에서 볼 수 있습니다.



확인 및 문제 해결

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다 .추가 확인/문제 해결 정보는 IP 보안 문제 해결 - 디버그 명령 이해 및 사용을 참조하십시오.VPN 클

라이언트 문제 또는 오류가 발생한 경우 VPN 클라이언트 GUI 오류 조회 도구를 참조하십시오.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

관련 정보

- IPsec 프로파일 컨피그레이션
- Cisco VPN 클라이언트 지원 페이지
- IPsec 협상/IKE 프로토콜 지원 페이지
- 기술 지원 및 문서 – Cisco Systems