EzVPN im NEM-Modus mit Split-Tunneling auf dem IOS-Router - Konfigurationsbeispiel

Inhalt

Einführung

In dieser Konfiguration wird die neue Funktion in der Cisco IOS® Softwareversion 12.3(11)T beschrieben, mit der Sie einen Router als EzVPN-Client und -Server auf derselben Schnittstelle konfigurieren können. Der Datenverkehr kann von einem VPN-Client zum EzVPN-Server und dann zurück zu einem anderen Remote-EzVPN-Server geroutet werden.

Unter Konfigurieren eines dynamischen IPsec-Routers für Peer- und VPN-Clients zwischen LAN und LAN erfahren Sie mehr über das Szenario, in dem eine LAN-zu-LAN-Konfiguration zwischen zwei Routern in einer Hub-Spoke-Umgebung mit Cisco VPN-Clients auch mit dem Hub verbunden ist und XAUTH (Extended Authentication) verwendet wird.

Eine Beispielkonfiguration für ein EzVPN zwischen einem Cisco 871-Router und einem Cisco 7200VXR-Router mit NEM-Modus finden Sie unter Easy VPN Server 7200 zu 871 Easy VPN Remote Configuration Example.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und

Hardwareversionen:

- Cisco IOS Software Release 12.3(11)T auf dem EzVPN-Client und Server-Router.
- Cisco IOS Softwareversion 12.3(6) auf dem Remote-EzVPN-Server-Router (dies kann eine beliebige Verschlüsselungsversion sein, die die EzVPN-Serverfunktion unterstützt).
- Cisco VPN-Client Version 4.x

Hinweis: Dieses Dokument wurde mit einem Cisco 3640 Router mit Cisco IOS Software Release 12.4(8) erneut zertifiziert.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

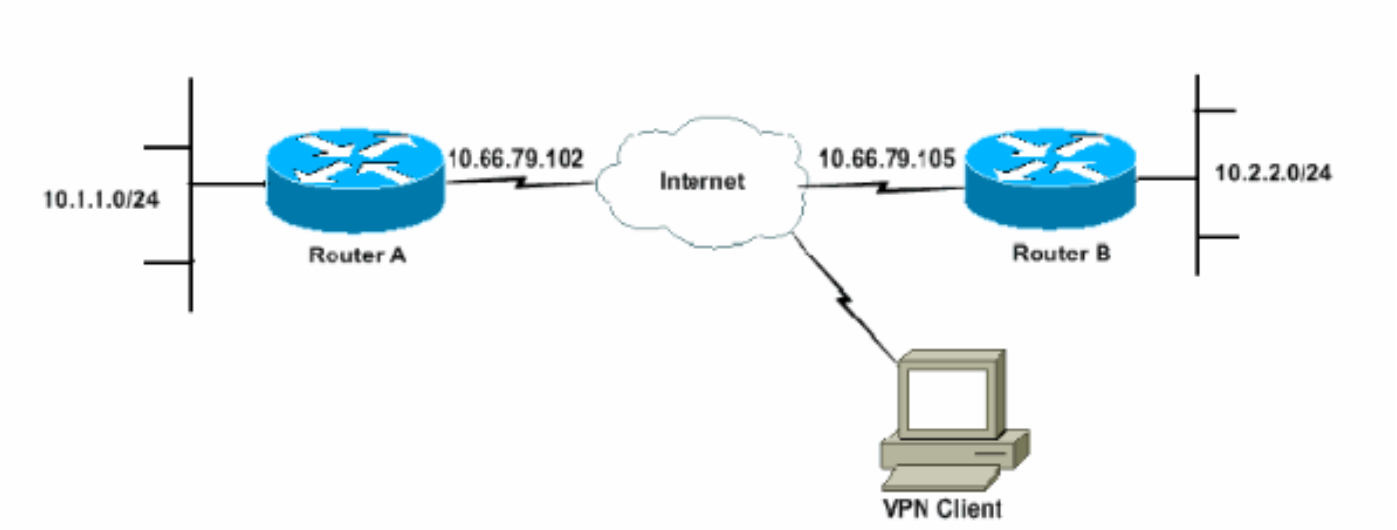
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Netzwerkdiagramm ist RouterA sowohl als EzVPN-Client als auch als Server konfiguriert. Dies ermöglicht es, Verbindungen von VPN-Clients zu akzeptieren und bei der Verbindung mit RouterB als EzVPN-Client zu fungieren. Datenverkehr vom VPN-Client kann an die Netzwerke hinter RouterA und RouterB weitergeleitet werden.



Konfigurationen

RouterA muss mit IPsec-Profilen für die VPN-Client-Verbindungen konfiguriert werden. Die Verwendung einer standardmäßigen EzVPN-Serverkonfiguration auf diesem Router zusammen mit der Konfiguration des EzVPN-Clients funktioniert nicht. Der Router verhandelt Phase 1 nicht.

In dieser Beispielkonfiguration sendet RouterB eine 10.0.0.0/8 Split-Tunnel-Liste an RouterA. Bei dieser Konfiguration darf der VPN-Client-Pool keine Komponente des Supernetzes 10.x.x.x sein. RouterA erstellt für den Datenverkehr von 10.1.1.0/24 bis 10.0.0.0/8 eine SA zu RouterB. Beispiel: Nehmen Sie an, Sie haben eine VPN Client-Verbindung und beziehen eine IP-Adresse aus einem lokalen Pool von 10.3.3.1. RouterA erstellt erfolgreich eine weitere SA für den Datenverkehr von 10.1.1.0/24 bis 10.3.3.1/32. Wenn jedoch Pakete vom VPN-Client beantwortet werden und dann auf RouterA drücken, sendet RouterA sie über den Tunnel an RouterB. Dies liegt daran, dass sie ihre SA von 10.1.1.0/24 auf 10.0.0.0/8 anstatt der spezifischeren Übereinstimmung von 10.3.3.1/32.

Sie müssen auch Split-Tunneling auf RouterB konfigurieren. Andernfalls funktioniert der VPN-Client-Datenverkehr nie. Wenn Sie kein Split-Tunneling definiert haben (in diesem Beispiel acl 150 auf RouterB), erstellt RouterA eine SA für den Datenverkehr von 10.1.1.0/24 bis 0.0.0.0/0 (der gesamte Datenverkehr). Wenn ein VPN-Client eine Verbindung herstellt und eine beliebige IP-Adresse aus einem Pool empfängt, wird der zurückkehrende Datenverkehr immer über den Tunnel an RouterB gesendet. Dies liegt daran, dass sie zuerst abgeglichen wird. Da diese SA den "gesamten Datenverkehr" definiert, spielt es keine Rolle, wie Ihr VPN-Client-Adresspool aussieht, der Datenverkehr wird nie wieder darauf zurückgeleitet.

Zusammenfassend müssen Sie Split-Tunneling verwenden, und Ihr VPN-Adresspool muss ein anderes Supernet sein als jedes andere Netzwerk in der Split-Tunnel-Liste.

In diesem Dokument werden folgende Konfigurationen verwendet:

- 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
```

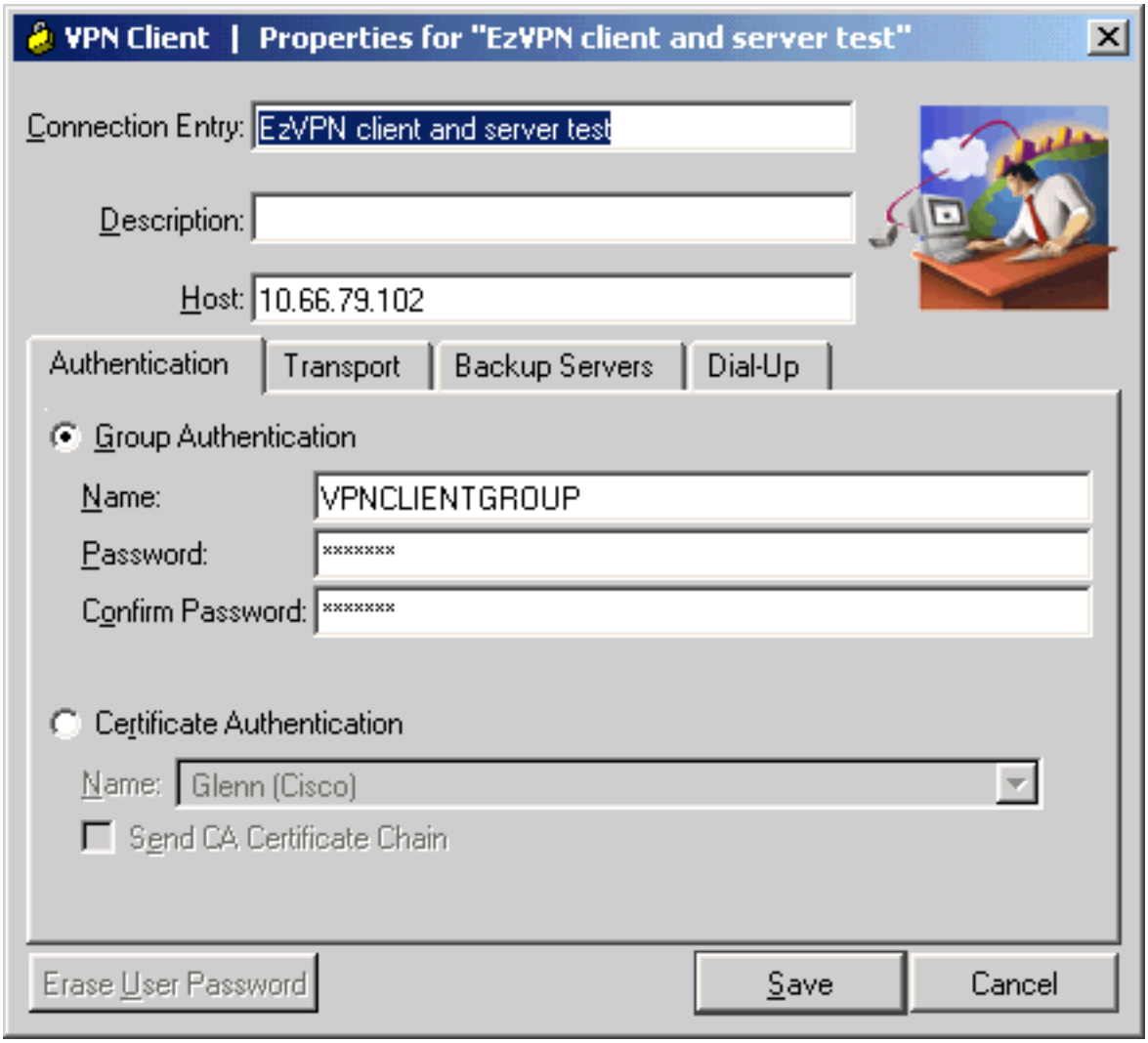
RouterB

```
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-Client-Konfiguration

Erstellen Sie einen neuen Verbindungseintrag, der auf die IP-Adresse von Router RouterA verweist. Der Gruppenname in diesem Beispiel lautet "VPNCLIENTGROUP", und das Kennwort lautet "mnbvcxz", wie in der Router-Konfiguration zu sehen ist.



Überprüfung und Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Bestätigung, dass Ihre Konfiguration ordnungsgemäß funktioniert. Weitere Informationen zur Überprüfung und Fehlerbehebung finden Sie unter IP Security Troubleshooting - Understanding and Using debug Commands (IP-Sicherheitsfehlerbehebung). Wenn bei Ihnen Probleme oder Fehler beim VPN-Client auftreten, verwenden Sie das Tool zur Fehlersuche bei der VPN-Client-GUI.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Zugehörige Informationen

- IPsec-Profilkonfiguration
- Support-Seite für Cisco VPN-Clients
- Support-Seite für IPsec-Aushandlung/IKE-Protokolle
- Technischer Support und Dokumentation - Cisco Systems