IOS ルータのスプリット トンネリングの NEM モードでの EzVPN 設定例

目次

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[設定](#)
[ネットワーク図](#)
[設定](#)
[VPN Client の設定](#)
[確認とトラブルシューティング](#)
[関連情報](#)

概要

この設定では、同じインターフェイス上でルータを EzVPN Client およびサーバとして設定可能な Cisco IOS® ソフトウェア リリース 12.3(11)T の新機能を詳細に示します。 トラフィックは、VPN Client から EzVPN サーバにルーティングした後、別のリモート EzVPN サーバにルーティングできます。

Cisco VPN Client がハブに接続され、拡張認証（Xauth）が使用されるハブ スポーク環境の 2 台のルータ間に LAN 間設定が存在するシナリオの詳細については、「IPSec ルータの動的な LAN 間ピアと VPN Client の設定」を参照してください。

Cisco 871 ルータと NEM モードの Cisco 7200VXR ルータ間の EzVPN 上の設定例については、「7200 Easy VPN Server と 871 Easy VPN Remote 間の設定例」を参照してください。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- EzVPN クライアントおよびサーバ ルータ上の Cisco IOS ソフトウェア リリース

12.3(11)T。
- リモート EzVPN サーバ ルータ上の Cisco IOS ソフトウェア リリース 12.3(6)（これは EzVPN サーバ機能をサポートする任意の暗号バージョンにすることができます）。
- Cisco VPN Client バージョン 4.x

注: このドキュメントは、Cisco IOS ソフトウェア リリース 12.4(8) がインストールされた Cisco 3640 ルータを使用して検証されました。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

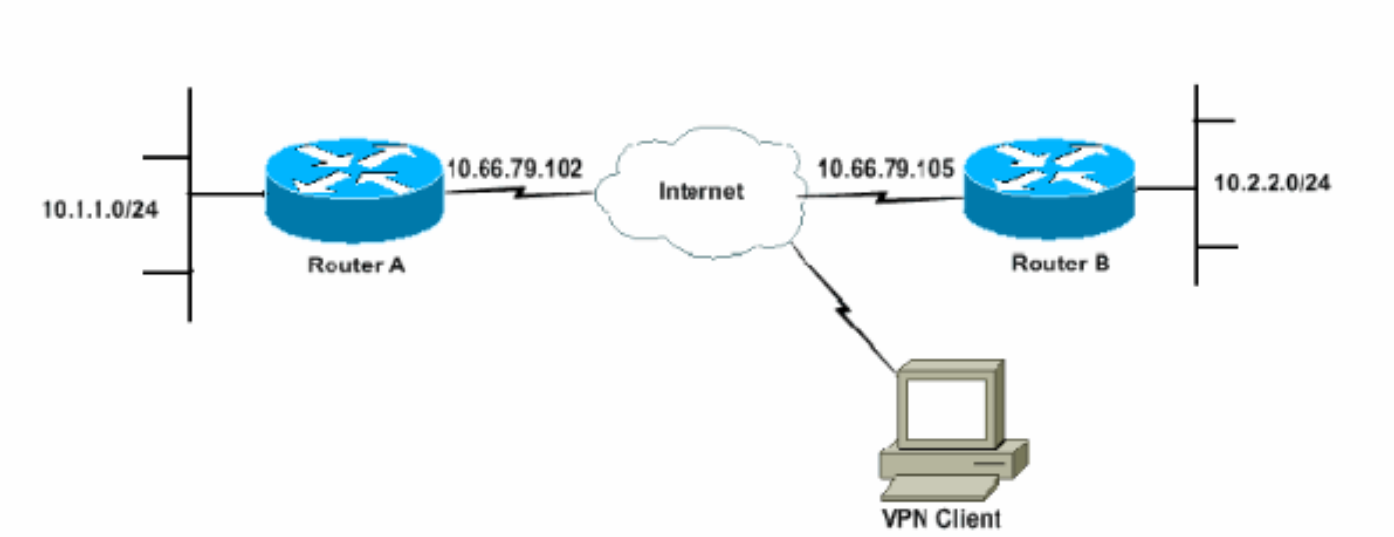
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このネットワーク図では、RouterA が EzVPN クライアントとサーバの両方として設定されています。 これにより、RouterA は VPN Client からの接続を受け入れ、RouterB への接続時に EzVPN Client として動作することが可能になります。 VPN Client からのトラフィックは、RouterA および RouterB の背後でネットワークにルーティングできます。



設定

RouterA は、VPN Client 接続用の IPsec プロファイルを使用して設定する必要があります。 このルータ上の標準の EzVPN サーバ設定と EzVPN クライアント設定を一緒に使用した場合は機能し

ません。 ルータは Phase 1 ネゴシエーションに失敗します。

この設定例では、RouterB が 10.0.0.0/8 スプリット トンネル リストを RouterA に送信します。 この設定では、VPN Client プールを 10.x.x.x スーパーネットのいずれにすることもできません。 この場合、RouterA は、10.1.1.0/24 から 10.0.0.0/8 へのトラフィックに対して、RouterB への SA を構築します。 例として、VPN Client を接続して、10.3.3.1 のローカル プールから IP アドレスを取得する場合を考えます。 RouterA は、10.1.1.0/24 から 10.3.3.1/32 へのトラフィックに対して別の SA を正常に構築します。 ただし、VPN Client からパケットが返信され、RouterA に到着すると、RouterA はそれらをトンネル経由で RouterB に送信します。 これは、これらのパケットが 10.3.3.1/32 のより限定的な一致ではなく、10.1.1.0/24 から 10.0.0.0/8 の SA に一致するためです。

また、RouterB でスプリット トンネリングを設定する必要もあります。 そうしなければ、VPN Client のトラフィックが機能しません。 スプリット トンネリング（この例では RouterB 上の acl 150）が定義されていない場合は、RouterA が 10.1.1.0/24 から 0.0.0.0/0 へのトラフィック（すべてのトラフィック）用の SA を構築します。 VPN Client が任意のプールからの任意の IP アドレスに接続し、その IP アドレスを受信した場合、リターン トラフィックは常に RouterB へのトンネルを介して送信されます。 これは、その IP アドレスが最初に一致するためです。 この SA は「すべてのトラフィック」を定義するため、VPN Client アドレス プールが何であるかにかかわらず、トラフィックがそこに戻ることはありません。

要するに、スプリット トンネリングを使用し、VPN アドレス プールをスプリット トンネル リスト内のどのネットワークとも違うスーパーネットにする必要があります。

このドキュメントでは、次の設定を使用します。

- 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
```

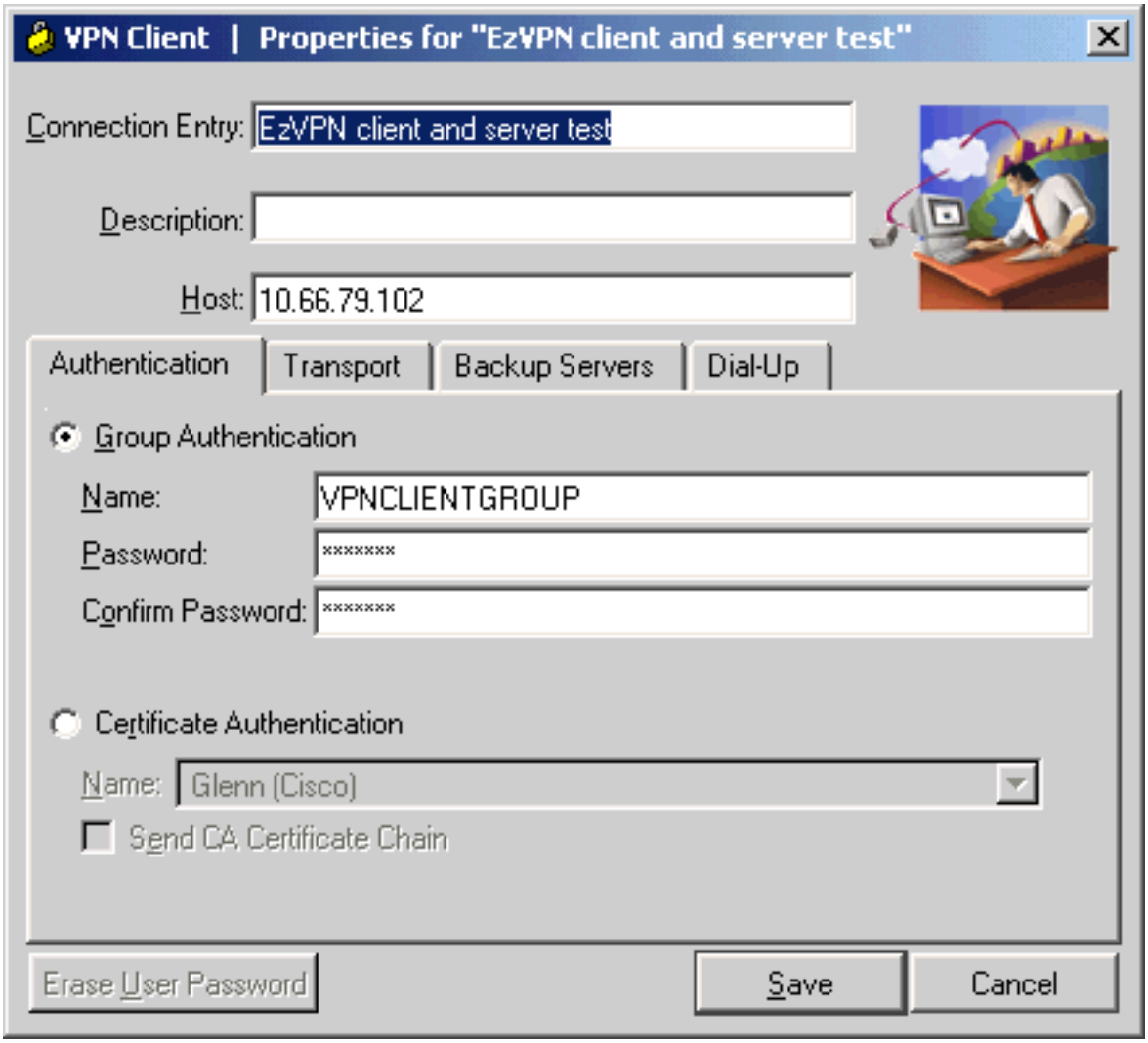
RouterB

```
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 の設定

ルータ RouterA の IP アドレスを参照する新しい接続エントリを作成します。 この例では、グループ名は「VPNCLIENTGROUP」、パスワードは「mnbvcxz」です（ルータの設定に示されています）。



確認とトラブルシューティング

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を示しています。 その他の確認/トラブルシューティング情報については、『IP セキュリティのトラブルシューティング - debug コマンドの理解と使用』を参照してください。 VPN Client の問題または エラーが発生した場合は、「VPN Client GUI エラー検索ツール」を参照してください。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

関連情報

- IPsec プロファイル設定
- Cisco VPN Client に関するサポート ページ
- IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems