IOS Router : Easy VPN (EzVPN) in Network−Extension Mode (NEM) with Split tunnelling Configuration Example

Document ID: 63098

Contents

Introduction

This configuration details the new feature in Cisco IOS® Software Release 12.3(11)T that enables you to configure a router as an EzVPN Client and server on the same interface. Traffic can be routed from a VPN Client to the EzVPN server, then back out to another remote EzVPN server.

Refer to Configuring an IPsec Router Dynamic LAN−to−LAN Peer and VPN Clients in order to learn more about the scenario where there is a LAN−to−LAN configuration between two routers in a hub−spoke environment with Cisco VPN Clients also connect to the hub and Extended Authentication (XAUTH) is used.

For a sample configuration on EzVPN between a Cisco 871 router and a Cisco 7200VXR Router with NEM Mode, refer to 7200 Easy VPN Server to 871 Easy VPN Remote Configuration Example.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS Software Release 12.3(11)T on the EzVPN Client and server router.
- Cisco IOS Software Release 12.3(6) on the remote EzVPN server router (this can be any crypto version that supports the EzVPN server feature).
- Cisco VPN Client Version 4.x

Note: This document was recertified with a Cisco 3640 Router with Cisco IOS Software Release 12.4(8).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

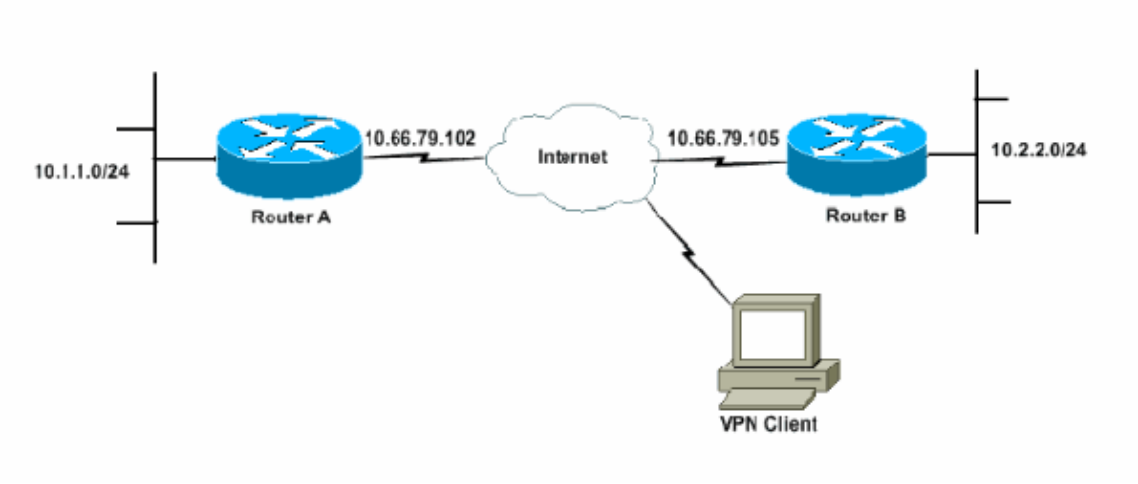
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

In this network diagram, RouterA is configured as both an EzVPN Client and server. This allows it to accept connections from VPN Clients, and to act as an EzVPN Client when it connects to RouterB. Traffic from the VPN Client can be routed to the networks behind RouterA and RouterB.



Configurations

RouterA has to be configured with IPsec profiles for the VPN Client connections. The use of a standard EzVPN server configuration on this router along with the EzVPN Client configuration does not work. The router fails Phase 1 negotiation.

In this sample configuration, RouterB sends a 10.0.0.0/8 split−tunnel list to RouterA. With this configuration, the VPN Client pool cannot be anything in the 10.x.x.x supernet. What happens is that RouterA builds an SA to RouterB for traffic from 10.1.1.0/24 to 10.0.0.0/8. As an example, assume you have a VPN Client connect and get an IP address out of a local pool of 10.3.3.1. RouterA successfully builds another SA for traffic from 10.1.1.0/24 to 10.3.3.1/32. However, when packets from the VPN Client are replied to and then hit RouterA, RouterA sends them over the tunnel to RouterB. This is because they match its SA of 10.1.1.0/24 to 10.0.0.0/8 instead of the more specific match of 10.3.3.1/32.

You must also configure split tunnelling on RouterB. Otherwise, VPN Client traffic never works. If you do not have split tunnelling defined (acl 150 on RouterB in this example), RouterA builds an SA for traffic from 10.1.1.0/24 to 0.0.0.0/0 (all traffic). When a VPN Client connects and receives any IP address out of any pool,

the return traffic to it is always sent over the tunnel to RouterB. This is because it gets matched on first. Since this SA defines "all traffic", it does not matter what your VPN Client address pool is, the traffic never gets back to it.

In summary, you must use split−tunnelling, and your VPN address pool must be a different supernet than any network in the split−tunnel list.

This document uses these configurations:

- 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

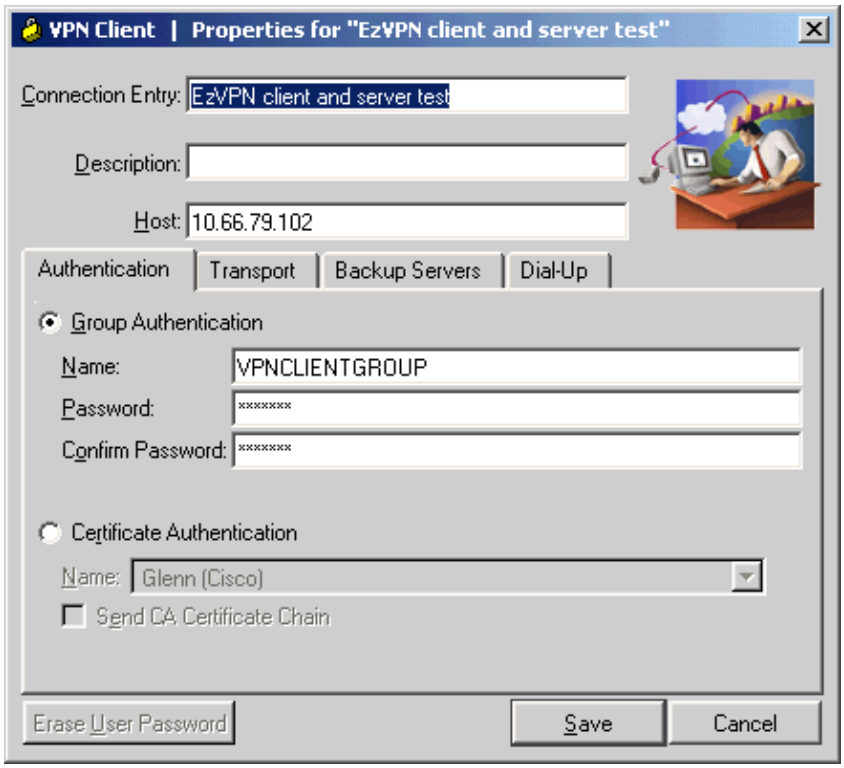
```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterB
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
!
```

```
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 Configuration

Create a new connection entry that references the IP address of router RouterA. The group name in this example is "VPNCLIENTGROUP" and the password is "mnbvcxz" as can be seen in the router configuration.



Verify and Troubleshoot

This section provides information you can use to confirm your configuration works properly. Refer to IP Security Troubleshooting − Understanding and Using debug Commands for additional verification/troubleshooting information. If you encounter any VPN Client issues or errors, refer to the VPN Client GUI Error Lookup Tool.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Related Information

- **IPsec Profile Configuration**
- **Cisco VPN Client Support Page**
- **IPsec Negotiation/IKE Protocols Support Page**
- **Technical Support & Documentation − Cisco Systems**

Updated: Mar 08, 2007 Document ID: 63098