Exemple de configuration d'EzVPN en mode NEM avec transmission tunnel partagée sur le routeur IOS

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Conventions
Configuration
Diagramme du réseau
Configurations
Configuration du client VPN
Vérifiez et dépannez
Informations connexes

Introduction

Cette configuration détaille la nouvelle fonction de la version 12.3(11)T du logiciel Cisco IOS® qui vous permet de configurer un routeur en tant que client et serveur EzVPN sur la même interface. Le trafic peut être acheminé d'un client VPN au serveur EzVPN, puis être renvoyé à un autre serveur EzVPN distant.

Référez-vous à Configuration d'un homologue LAN-à-LAN dynamique de routeur IPsec et de clients VPN afin d'en savoir plus sur le scénario où il y a une configuration LAN-à-LAN entre deux routeurs dans un environnement en étoile avec les clients VPN Cisco se connectent également au concentrateur et l'authentification étendue (XAUTH) est utilisée.

Pour un exemple de configuration sur EzVPN entre un routeur Cisco 871 et un routeur Cisco 7200VXR avec le mode NEM, reportez-vous à l'exemple de configuration Easy VPN Server vers 871 Easy VPN Remote du 7200.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco IOS Version 12.3(11)T sur le client et le routeur serveur EzVPN.
- Logiciel Cisco IOS Version 12.3(6) sur le routeur serveur EzVPN distant (il peut s'agir de n'importe quelle version de chiffrement prenant en charge la fonctionnalité serveur EzVPN).
- Client VPN Cisco Version 4.x

Remarque : Ce document a été recertifié avec un routeur Cisco 3640 avec le logiciel Cisco IOS Version 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

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

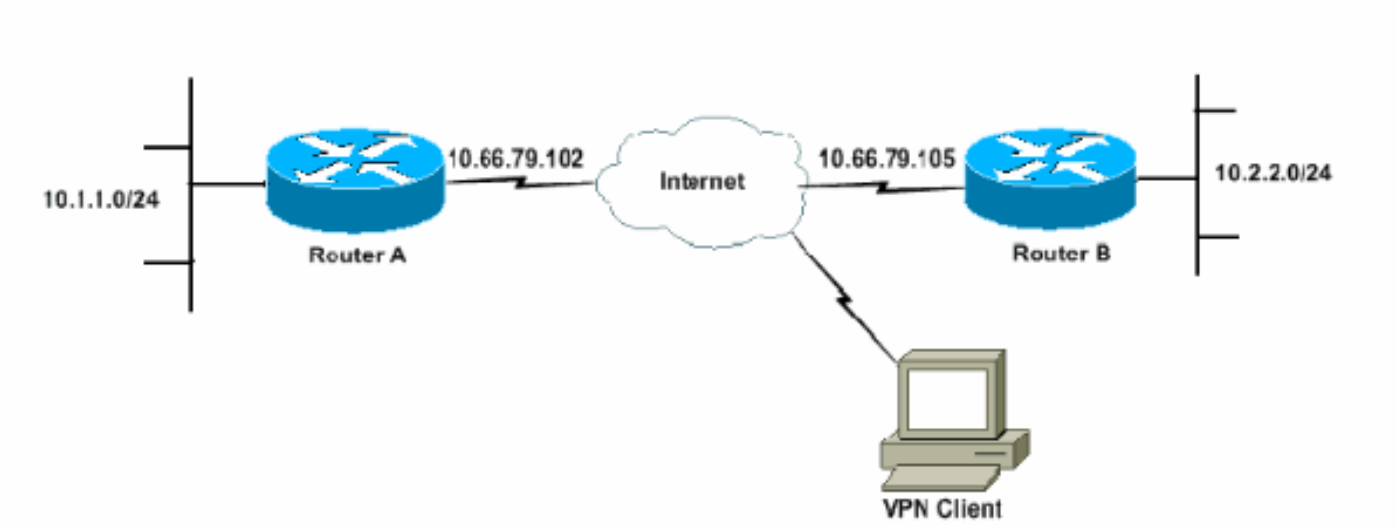
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Dans ce schéma de réseau, RouterA est configuré en tant que client et serveur EzVPN. Cela lui permet d'accepter les connexions des clients VPN et d'agir en tant que client EzVPN lorsqu'il se connecte au routeur B. Le trafic du client VPN peut être acheminé vers les réseaux derrière les routeurs A et B.



Configurations

Le routeur A doit être configuré avec des profils IPsec pour les connexions du client VPN. L'utilisation d'une configuration de serveur EzVPN standard sur ce routeur avec la configuration du client EzVPN ne fonctionne pas. Le routeur échoue la négociation de phase 1.

Dans cet exemple de configuration, RouterB envoie une liste de tunnels fractionnés 10.0.0.0/8 au RouterA. Avec cette configuration, le pool de clients VPN ne peut être rien dans le super-réseau 10.x.x.x. Ce qui se passe, c'est que RouterA crée une SA vers RouterB pour le trafic de 10.1.1.0/24 à 10.0.0.0/8. Par exemple, supposons que vous avez une connexion VPN Client et que vous obteniez une adresse IP à partir d'un pool local de 10.3.3.1. Le routeur A a réussi à créer une autre SA pour le trafic de 10.1.1.0/24 à 10.3.3.1/32. Cependant, lorsque des paquets provenant du client VPN reçoivent une réponse, puis qu'ils atteignent le routeur A, le routeur A les envoie par le tunnel au routeur B. C'est parce qu'ils correspondent à son SA de 10.1.1.0/24 à 10.0.0.0/8 au lieu de la correspondance plus spécifique de 10.3.3.1/32.

Vous devez également configurer la transmission tunnel partagée sur le routeur B. Sinon, le trafic du client VPN ne fonctionne jamais. Si la transmission tunnel partagée n'est pas définie (acl 150 sur RouterB dans cet exemple), RouterA crée une SA pour le trafic de 10.1.1.0/24 à 0.0.0.0/0 (tout le trafic). Lorsqu'un client VPN se connecte et reçoit une adresse IP de n'importe quel pool, le trafic de retour vers celui-ci est toujours envoyé par le tunnel vers le routeur B. C'est parce qu'il est mis en correspondance en premier. Puisque cette SA définit « tout le trafic », peu importe ce qu'est votre pool d'adresses de client VPN, le trafic n'y retourne jamais.

En résumé, vous devez utiliser la transmission tunnel partagée et votre pool d'adresses VPN doit être un super-réseau différent de n'importe quel réseau de la liste de tunnels partagés.

Ce document utilise les configurations suivantes :

- Routeur A
- Routeur B

Routeur A

```
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
```

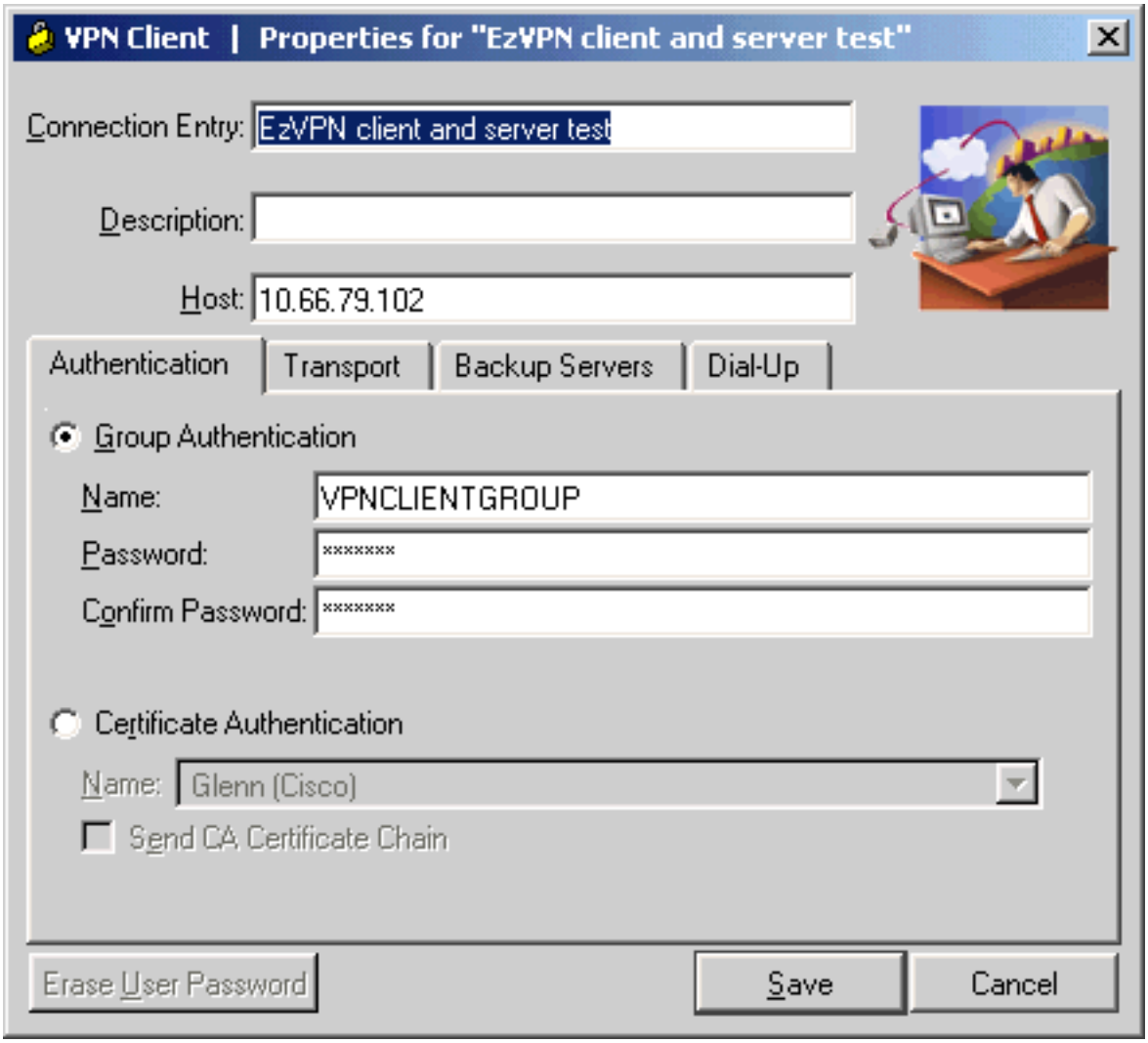
Routeur B

```
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
```

Configuration du client VPN

Créez une nouvelle entrée de connexion qui fait référence à l'adresse IP du routeur RouterA. Le nom du groupe dans cet exemple est « VPNCLIENTGROUP » et le mot de passe est « mnbvcxz », comme vous pouvez le voir dans la configuration du routeur.



Vérifiez et dépannez

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement. Référez-vous à Dépannage de la sécurité IP - Compréhension et utilisation des commandes de débogage pour plus d'informations de vérification/dépannage. Si vous rencontrez des problèmes ou des erreurs de client VPN, reportez-vous à l'outil de recherche d'erreurs de l'interface utilisateur graphique du client VPN.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Informations connexes

- Configuration de profil IPSec
- Cisco VPN Client Support Page
- Page de support de la négociation IPSec/des protocoles IKE
- Support et documentation techniques - Cisco Systems