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

Contenu

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 configurer un pair dynamique d'entre réseaux locaux de routeur d'IPsec et les clients vpn afin de se renseigner plus sur le scénario où il y a une configuration entre réseaux locaux entre deux Routeurs dans un environnement de hub-spoke avec des Clients VPN Cisco également se connectent au hub et à l'authentification étendue (XAUTH) est utilisés.

Pour une configuration d'échantillon sur l'EzVPN entre un routeur de Cisco 871 et un routeur de Cisco 7200VXR avec PAS MENTIONNÉ AILLEURS le mode, référez-vous au serveur Easy VPN 7200 à l'exemple de 871 configurations d'Easy VPN distant.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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 routeur de client et de serveur d'EzVPN.
- Logiciel Cisco IOS version 12.3(6) sur le routeur à distance de serveur d'EzVPN (ceci peut être n'importe quelle version crypto qui prend en charge la caractéristique de serveur d'EzVPN).
- Version 4.x de Client VPN Cisco

Remarque: Ce document recertified avec un routeur de Cisco 3640 avec la version du logiciel Cisco IOS 12.4(8).

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

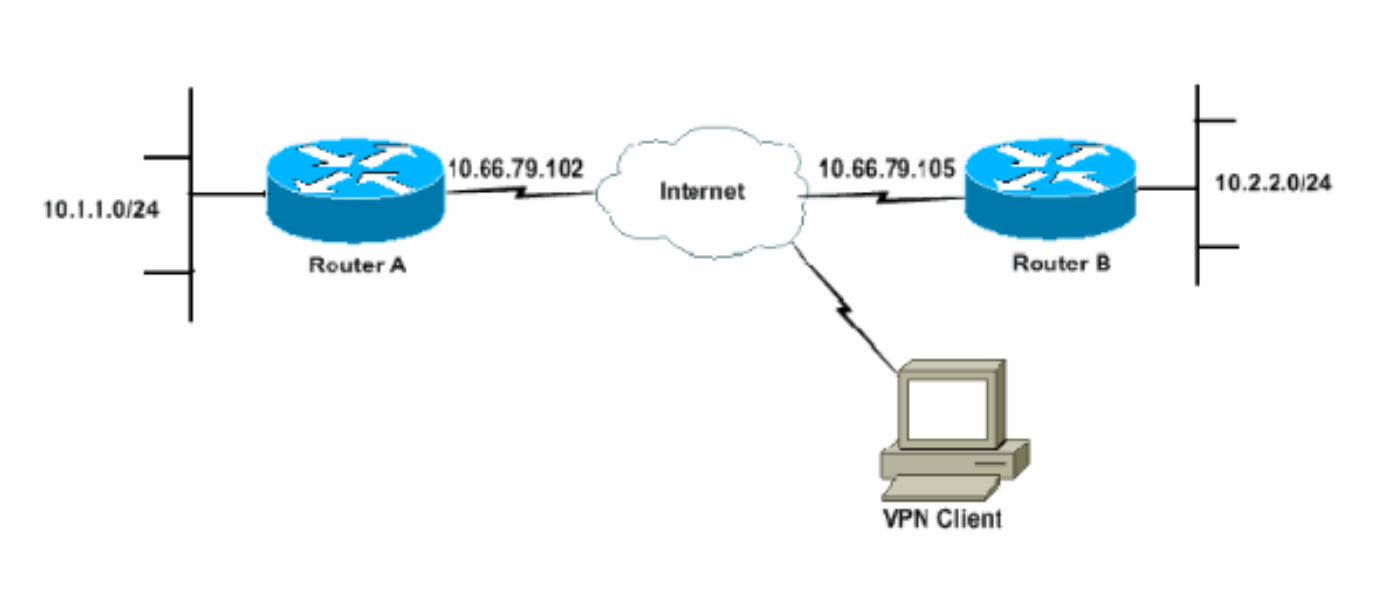
Configurez

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

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Dans ce schéma de réseau, le RouterA est configuré en tant que client et serveur d'EzVPN. Ceci lui permet pour recevoir des connexions des clients vpn, et pour agir en tant que client d'EzVPN quand il se connecte au RouterB. Le trafic du client vpn peut être conduit aux réseaux derrière le RouterA et le RouterB.



Configurations

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

Dans cette configuration d'échantillon, le RouterB envoie une liste de 10.0.0.0/8 tunnels partagés au RouterA. Avec cette configuration, le groupe de client vpn ne peut pas être quelque chose dans les super-réseaux 10.x.x.x. Ce qui se produit est ce RouterA construit SA au RouterB pour le trafic de 10.1.1.0/24 à 10.0.0.0/8. Comme exemple, supposez que vous faites obtenir à un client vpn connecter et une adresse IP hors d'un groupe local de 10.3.3.1. Le RouterA construit avec succès une autre SA pour le trafic de 10.1.1.0/24 à 10.3.3.1/32. Cependant, quand des paquets du client vpn sont répondus à et RouterA alors frappé, le RouterA les envoie au-dessus du tunnel au RouterB. C'est parce qu'ils concurrencent sa 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 le fractionnement perçant un tunnel sur le RouterB. Autrement, le trafic de client vpn ne fonctionne jamais. Si vous n'avez pas séparé le perçage d'un tunnel défini (acl 150 sur le RouterB dans cet exemple), le RouterA construit SA pour le trafic de 10.1.1.0/24 à 0.0.0.0/0 (tout le trafic). Quand un client vpn connecte et reçoit n'importe quelle adresse IP hors de n'importe quel groupe, le trafic de retour à lui est toujours envoyé au-dessus du tunnel au RouterB. C'est parce qu'il obtient apparié en fonction d'abord. Puisque cette SA définit « tout le trafic », elle n'importe pas ce qu'est votre pool d'adresses de client vpn, le trafic ne revient jamais à elle.

En résumé, vous devez utiliser le fractionnement-perçage d'un tunnel, et votre pool d'adresses VPN doit être un super-réseau différent que n'importe quel réseau dans la liste de tunnel partagé.

Ce document utilise les configurations suivantes :

- 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
```

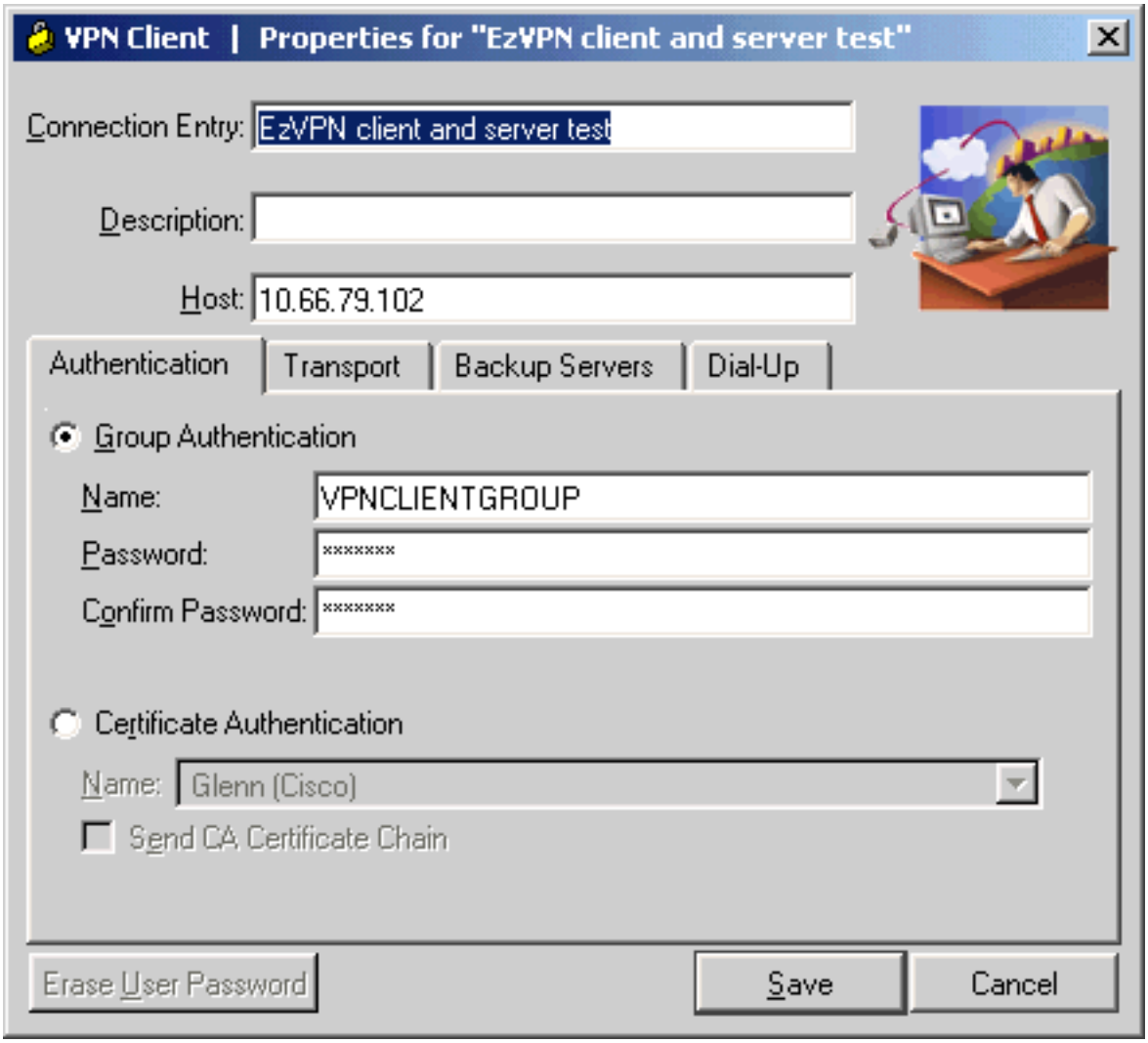
```
defines additional SAs for this !--- router to create to
the head-end EzVPN server (RouterB). !--- Without this,
RouterA only builds an SA for traffic !--- from 10.1.1.0
to 10.2.2.0. VPN Clients !--- that connect (and get a
192.168.1.0 address) !--- are not able to get to
10.2.2.0. access-list 120 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
```

Configuration du client VPN

Créez une nouvelle entrée de connexion qui met en référence l'adresse IP du RouterA de routeur. Le nom de groupe dans cet exemple est « VPNCLIENTGROUP » et le mot de passe est « mnbvcxz » comme peut être vu en configuration de routeur.



Vérifiez et dépannez

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement. Référez-vous au dépannage de sécurité IP - Comprenant et utilisant des commandes de débogage pour la vérification/information de dépannage supplémentaires. Si vous rencontrez n'importe quelles questions ou erreurs de client vpn, référez-vous à l'Outil VPN Client GUI Error Lookup.

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