Esempio di configurazione di EzVPN in modalità NEM con split tunneling sul router IOS

Sommario

Introduzione

Questa configurazione descrive in dettaglio la nuova funzionalità del software Cisco IOS® versione 12.3(11)T che consente di configurare un router come client e server EzVPN sulla stessa interfaccia. Il traffico può essere indirizzato da un client VPN al server EzVPN, quindi indirizzato a un altro server EzVPN remoto.

Per ulteriori informazioni sullo scenario in cui si verifica una configurazione LAN-LAN tra due router in un ambiente hub-spoke e sui client VPN Cisco, fare riferimento alla configurazione di un router IPsec per un'autenticazione estesa (XAUTH).

Per un esempio di configurazione su EzVPN tra un router Cisco 871 e un router Cisco 7200VXR con modalità NEM, fare riferimento all'esempio di configurazione remota Easy VPN da 7200 a 871.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco IOS versione 12.3(11)T sul client e sul router server EzVPN.
- Software Cisco IOS versione 12.3(6) sul router del server EzVPN remoto (può essere una versione crittografica che supporta la funzionalità del server EzVPN).
- Cisco VPN Client versione 4.x

Nota: questo documento è stato ricertificato con un router Cisco 3640 e software Cisco IOS versione 12.4(8).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

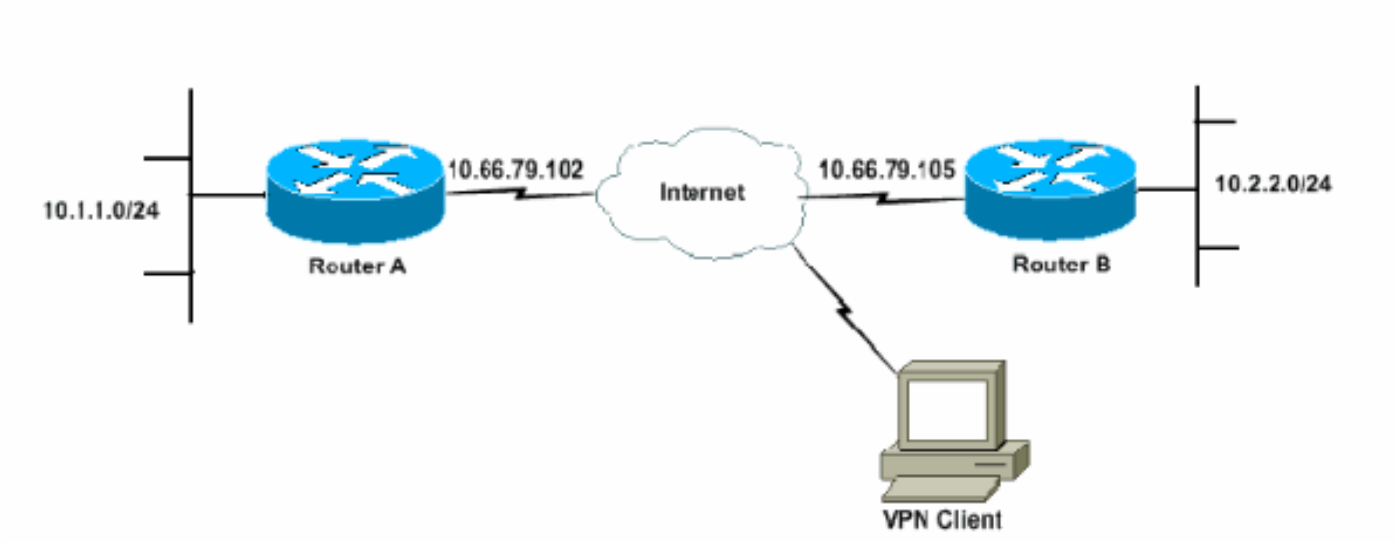
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

In questo diagramma di rete, il router A è configurato sia come client che come server EzVPN. In questo modo, può accettare connessioni da client VPN e agire come client EzVPN quando si connette a RouterB. Il traffico proveniente dal client VPN può essere indirizzato alle reti dietro il router A e il router B.



Configurazioni

Ènecessario configurare il router A con i profili IPsec per le connessioni client VPN. L'uso di una configurazione server EzVPN standard su questo router insieme alla configurazione client EzVPN non funziona. Il router non riesce la negoziazione di fase 1.

In questa configurazione di esempio, il router B invia un elenco di split-tunnel 10.0.0.0/8 al router A. Con questa configurazione, il pool di client VPN non può essere presente nella supernet 10.x.x.x. In questo caso, il router A crea un'associazione di sicurezza (SA) per il router B per il traffico compreso tra 10.1.1.0/24 e 10.0.0.0/8. Si supponga, ad esempio, di avere una connessione client VPN e di ottenere un indirizzo IP da un pool locale pari a 10.3.3.1. Il router A crea correttamente un'altra associazione di sicurezza per il traffico tra 10.1.1.0/24 e 10.3.3.1/32. Tuttavia, quando i pacchetti provenienti dal client VPN vengono risposte al router A e quindi raggiunti, il router A li invia tramite il tunnel a RouterB. Ciò è dovuto al fatto che l'associazione di sicurezza corrispondente è pari a 10.1.1.0/24 a 10.0.0.0/8 anziché alla corrispondenza più specifica di 10.3.3.1/32.

Ènecessario configurare anche il tunneling suddiviso sul router B. In caso contrario, il traffico del client VPN non funziona mai. Se non è stato definito il tunneling suddiviso (nell'esempio, ACL 150 sul router B), il router A costruisce un'associazione di sicurezza per il traffico tra 10.1.1.0/24 e 0.0.0.0/0 (tutto il traffico). Quando un client VPN si connette e riceve un indirizzo IP da un pool, il traffico di ritorno verso di esso viene sempre inviato al router B attraverso il tunnel. Questo perché viene confrontato prima. Poiché questa associazione di protezione definisce "tutto il traffico", non importa quale sia il pool di indirizzi del client VPN, il traffico non torna mai a tale pool.

In sintesi, è necessario utilizzare lo split-tunneling e il pool di indirizzi VPN deve essere una supernet diversa da qualsiasi rete nell'elenco dello split-tunnel.

Nel documento vengono usate queste configurazioni:

- 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
```

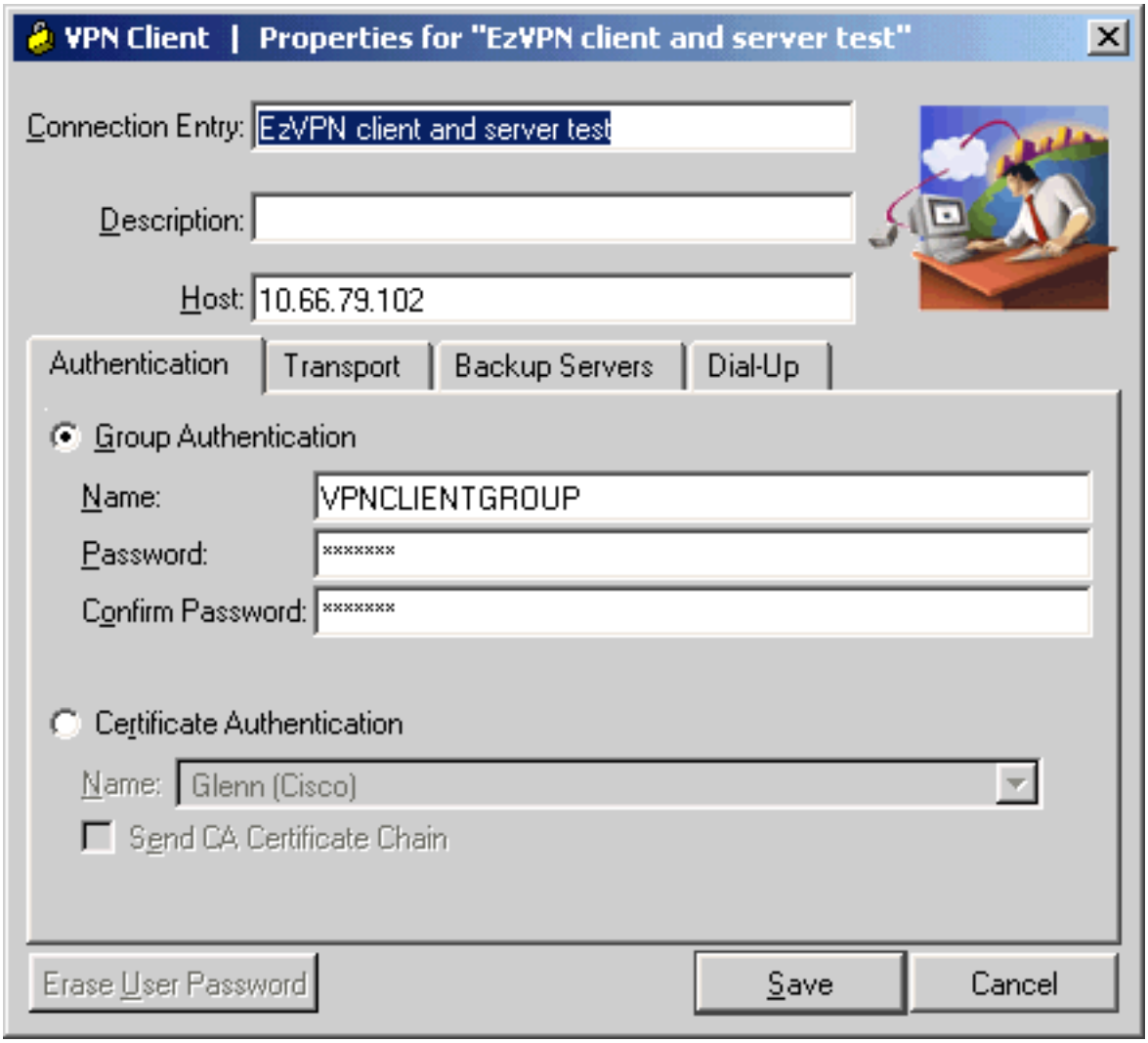
RouterB

```
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
```

Configurazione client VPN

Creare una nuova voce di connessione che faccia riferimento all'indirizzo IP del router A. Nell'esempio, il nome del gruppo è "VPNCLIENTGROUP" e la password è "mnbvcxz", come è possibile verificare nella configurazione del router.



Verifica e risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente. Per ulteriori informazioni sulla verifica e la risoluzione dei problemi, consultare il documento sulla risoluzione dei problemi di sicurezza IP - Comprensione e uso dei comandi di debug. In caso di problemi o errori del client VPN, fare riferimento allo strumento di ricerca degli errori della GUI del client VPN.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Informazioni correlate

- Configurazione profilo IPsec
- Pagina di supporto per Cisco VPN Client
- Pagina di supporto per la negoziazione IPsec/i protocolli IKE
- Documentazione e supporto tecnico – Cisco Systems