Exemple de configuration de IPSec/GRE avec NAT sur routeur IOS

Contenu

Introduction

Cet exemple de configuration montre comment configurer la GRE (Generic Routing Encapsulation) sur la sécurité IP (IPSec) lorsque le tunnel GRE/IPSec passe à travers un pare-feu faisant la traduction d'adresses réseau (NAT).

Avant de commencer

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Conditions préalables

Ce genre de configuration pourrait être utilisé pour percer un tunnel et chiffrer le trafic qui normalement ne passerait pas par un Pare-feu, tel que l'IPX (comme dans notre exemple ici) ou les mises à jour de routage. Dans cet exemple, le tunnel entre les 2621 et les 3660 seulement travaux quand le trafic est généré des périphériques sur les segments de RÉSEAU LOCAL (pas un ping étendu IP/IPX des Routeurs d'IPSec). La Connectivité IP/IPX a été testée avec le ping IP/IPX entre les périphériques 2513A et 2513B.

Remarque: Ceci ne fonctionne pas avec la translation d'adresses d'adresse du port (PAT).

Composants utilisés

Les informations dans ce document sont basées sur les versions de logiciel et de matériel ci-dessous.

- Cisco IOS® 12.4
- Pare-feu Cisco PIX 535
- Version 7.x et ultérieures de Logiciels pare-feu Cisco PIX

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Configurez

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

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Note de configuration IOS : Avec le Cisco IOS 12.2(13)T et les codes postérieurs (des codes numérotés plus élevés de T-série, 12.3 et des codes postérieurs) l'IPSEC configuré « crypto map » doit seulement être appliqué à l'interface physique et n'est plus exigé pour être appliqué sur l'interface de tunnel GRE. Ayant le « crypto map » sur l'examen médical et l'interface de tunnel en utilisant toujours le 12.2.(13)T et les travaux postérieurs de codes. Cependant, il est fortement recommandé pour l'appliquer juste sur l'interface physique.

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :

Remarque: Les adresses IP utilisées dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Remarques sur les diagrammes de réseau

- Tunnel GRE de 10.2.2.1 à 10.3.3.1 (BB de réseau IPX)
- Tunnel d'IPSec de 10.1.1.2 (10.99.99.12) à 10.99.99.2

Configurations

Périphérique 2513A
ipx routing 00e0.b064.20c1 ! interface Ethernet0 **ip address 10.2.2.2 255.255.255.0** no ip directed-broadcast

```
 ipx network AA
!
ip route 0.0.0.0 0.0.0.0 10.2.2.1
!--- Output Suppressed
```

2621

```
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2621
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
ipx routing 0030.1977.8f80
isdn voice-call-failure 0
cns event-service server
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 10.99.99.2
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/1
crypto map mymap 10 ipsec-isakmp
 set peer 10.99.99.2
 set transform-set myset
 match address 101
!
controller T1 1/0
!
interface Tunnel0
 ip address 192.168.100.1 255.255.255.0
 no ip directed-broadcast
 ipx network BB
 tunnel source FastEthernet0/0
 tunnel destination 10.3.3.1
 crypto map mymap
!
interface FastEthernet0/0
 ip address 10.2.2.1 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
 ipx network AA
!
interface FastEthernet0/1
 ip address 10.1.1.2 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
 crypto map mymap
!
ip classless
ip route 10.3.3.0 255.255.255.0 Tunnel0
ip route 10.3.3.1 255.255.255.255 10.1.1.1
ip route 10.99.99.0 255.255.255.0 10.1.1.1
no ip http server
!
```

```
access-list 101 permit gre host 10.2.2.1 host 10.3.3.1
!
line con 0
 transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end

!--- Output Suppressed
```

PIX

```
pixfirewall# sh run
: Saved
:
PIX Version 7.0
!
hostname pixfirewall
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.99.99.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
global (outside) 1 10.99.99.50-10.99.99.60
nat (inside) 1 0.0.0.0 0.0.0.0 0 0

static (inside,outside) 10.99.99.12 10.1.1.2 netmask
255.255.255.255 0 0
access-list 102 permit esp host 10.99.99.12 host
10.99.99.2
access-list 102 permit udp host 10.99.99.12 host
10.99.99.2 eq isakmp


route outside 0.0.0.0 0.0.0.0 10.99.99.2 1
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1

!--- Output Suppressed
```

3660

```
version 12.4
service timestamps debug datetime
service timestamps log uptime
no service password-encryption
!
hostname 3660
!
memory-size iomem 30
ip subnet-zero
no ip domain-lookup
!
ipx routing 0030.80f2.2950
cns event-service server
!
crypto isakmp policy 10
```

```
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 10.99.99.12
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/0
crypto map mymap 10 ipsec-isakmp
 set peer 10.99.99.12
 set transform-set myset
 match address 101
!
interface Tunnel0
 ip address 192.168.100.2 255.255.255.0
 no ip directed-broadcast
 ipx network BB
 tunnel source FastEthernet0/1
 tunnel destination 10.2.2.1
 crypto map mymap
!
interface FastEthernet0/0
 ip address 10.99.99.2 255.255.255.0
 no ip directed-broadcast
 ip nat outside
 duplex auto
 speed auto
 crypto map mymap
!
interface FastEthernet0/1
 ip address 10.3.3.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
 duplex auto
 speed auto
 ipx network CC
!
ip nat pool 3660-nat 10.99.99.70 10.99.99.80 netmask
255.255.255.0
ip nat inside source list 1 pool 3660-nat
ip classless
ip route 0.0.0.0 0.0.0.0 Tunnel0
ip route 10.2.2.1 255.255.255.255 10.99.99.1
ip route 10.99.99.12 255.255.255.255 10.99.99.1
no ip http server
!
access-list 1 permit 10.3.3.0 0.0.0.255
access-list 101 permit gre host 10.3.3.1 host 10.2.2.1
!
line con 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
!--- Output Suppressed
```

Périphérique 2513B

```
ipx routing 00e0.b063.e811
!
interface Ethernet0
 ip address 10.3.3.2 255.255.255.0
 no ip directed-broadcast
 ipx network CC
```

```
!
ip route 0.0.0.0 0.0.0.0 10.3.3.1

!--- Output Suppressed
```

Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- show crypto ipsec sa - Affiche à la phase 2 associations de sécurité.
- show crypto isakmp sa - Affiche les connexions de session chiffrées par active en cours pour tous les moteurs de chiffrement.
- *Sur option : nombre de* show interfaces tunnel - Affiche les informations d'interface de tunnel.
- show ip route - Affiche toutes les artères statiques IP, ou ceux installées utilisant la fonction de téléchargement d'artère d'AAA (authentification, autorisation, et comptabilité).
- show ipx route - Affiche le contenu de la table de routage ipx.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Remarque: Avant d'exécuter les commandes **debug**, référez-vous à la section **Informations importantes sur les commandes Debug**.

- debug crypto engine - Affiche le trafic qui est chiffré.
- debug crypto ipsec - Affiche les négociations IPSecs de la phase 2.
- debug crypto isakmp - Affiche les négociations de Protocole ISAKMP (Internet Security Association and Key Management Protocol) de la phase 1.
- *Sur option :* mettez au point le Routage IP - Les informations d'expositions sur des mises à jour de table de routage de Protocole RIP (Routing Information Protocol) et des mises à jour de route-cache.
- mettez au point le routage ipx {activité | des événements} - mettez au point le routage ipx {activité | événements} - les informations d'expositions sur les paquets de routage ipx que le routeur envoie et reçoit.

Autorisation des associations de sécurité (SAS)

- effacez ipsec SA de crytpo - Autorise toutes les associations de sécurité d'IPSec.
- clear crypto isakmp - Autorise les associations de sécurité d'IKE.

- *Sur option :* le clear ipx route * - supprime toutes les artères de la table de routage ipx.

Informations connexes

- Pages de support produit de sécurité IP (IPSec)
- Pages d'assistance GRE
- Support technique - Cisco Systems