

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

Contenu

[Introduction](#)

[Avant de commencer](#)

[Conventions](#)

[Conditions préalables](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Suppression des associations de sécurité \(SA\)](#)

[Informations connexes](#)

[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 type de configuration pourrait être utilisé pour tunnel et chiffrer le trafic qui normalement ne passerait pas par un pare-feu, tel qu'IPX (comme dans notre exemple ici) ou les mises à jour de routage. Dans cet exemple, le tunnel entre le 2621 et le 3660 ne fonctionne que lorsque le trafic est généré à partir de périphériques sur les segments LAN (et non pas à partir d'une requête ping IP/IPX étendue des routeurs IPSec). La connectivité IP/IPX a été testée avec une requête ping IP/IPX entre les périphériques 2513A et 2513B.

Remarque : cela ne fonctionne pas avec la traduction d'adresses de port (PAT).

Components Used

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
- Logiciel Cisco PIX Firewall Version 7.x et ultérieure

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Configuration

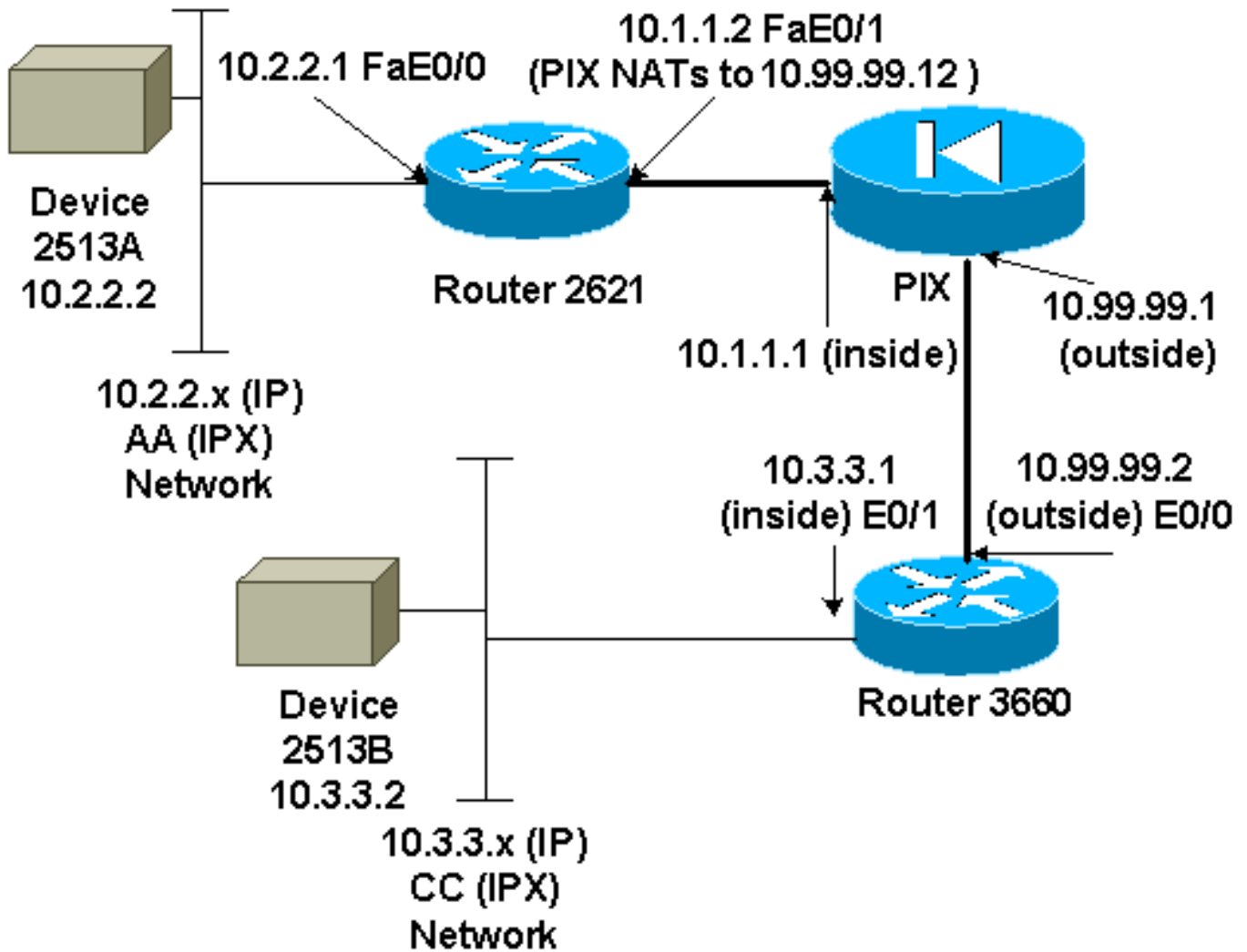
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez [l'outil de recherche de commandes](#) (clients [inscrits](#) seulement).

Remarque sur la configuration IOS : Avec la plate-forme logicielle Cisco IOS 12.2(13)T et les codes ultérieurs (codes de train T numérotés plus élevés, 12.3 et les codes ultérieurs), la carte de chiffrement IPSEC configurée ne doit être appliquée qu'à l'interface physique et n'est plus nécessaire à l'interface de tunnel GRE. La « crypto map » sur l'interface physique et tunnel lors de l'utilisation des codes 12.2.(13)T et ultérieurs fonctionne toujours. Cependant, il est fortement recommandé de l'appliquer uniquement 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 routables légalement sur Internet. Ce sont des adresses [RFC 1918 qui ont été utilisées dans un environnement de laboratoire.](#)

Notes de diagramme de réseau

- Tunnel GRE de 10.2.2.1 à 10.3.3.1 (réseau IPX BB)
- Tunnel IPsec de 10.1.1.2 (10.99.99.12) à 10.99.99.2

Configurations

Périphérique 2513A
<pre> 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 !---</pre>
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
```

Vérification

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 les associations de sécurité de phase 2.
- [show crypto isakmp sa](#) - Affiche les connexions de session chiffrées actives actuelles pour tous les moteurs de chiffrement.
- *Éventuellement* : [show interfaces tunnel number](#) - Affiche les informations d'interface de tunnel.
- [show ip route](#) - Affiche toutes les routes IP statiques, ou celles installées à l'aide de la fonction de téléchargement de route AAA (authentification, autorisation et comptabilité).
- [show ipx route](#) - Affiche le contenu de la table de routage IPX.

Dépannage

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.

Note : Avant d'émettre des commandes **debug**, consultez [Informations importantes sur les commandes de débogage](#).

- [debug crypto engine](#) - Affiche le trafic chiffré.
- [debug crypto ipsec](#) - Affiche les négociations IPsec de la phase 2.
- [debug crypto isakmp](#) - Affiche les négociations de la phase 1 de l'ISAKMP (Internet Security Association and Key Management Protocol).
- *Éventuellement* : [debug ip routing](#) - Affiche des informations sur les mises à jour de la table de routage RIP (Routing Information Protocol) et les mises à jour de la mémoire cache de route.
- [debug ipx routing {activité | events}](#) - debug ipx routing {activité | events} - Affiche des informations sur les paquets de routage IPX que le routeur envoie et reçoit.

Suppression des associations de sécurité (SA)

- [clear crypto ipsec sa](#) - Efface toutes les associations de sécurité IPsec.
- [clear crypto isakmp](#) - Efface les associations de sécurité IKE.
- *Éventuellement* : [clear ipx route *](#) - Supprime toutes les routes de la table de routage IPX.

Informations connexes

- [Pages d'assistance produit IPSec \(IP Security\)](#)
- [Pages d'assistance GRE](#)
- [Support technique - Cisco Systems](#)