# PIX 6.x : Exemple de configuration de tunnel IPSec à travers un pare-feu PIX avec utilisation de liste d'accès et NAT

## Contenu



## Introduction

Ce document fournit un exemple de configuration pour un tunnel IPsec par un pare-feu qui effectue la traduction d'adresses de réseau (NAT). **Cette configuration ne fonctionne pas avec la traduction d'adresse de port (PAT) si vous utilisez une version du logiciel de Cisco IOS® antérieure à 12.2(13)T.** Ce genre de configuration peut être utilisé pour percer un tunnel de trafic IP. Il ne peut pas être utilisé pour crypter le trafic qui ne passe pas par un pare-feu, tel qu'IPX ou les mises à jour du routage. L'encapsulation générique de routage (GRE) perçant un tunnel est appropriée pour ce type de configuration. Dans l'exemple de ce document, les routeurs Cisco 2621 et 3660 sont points finaux de tunnel IPsec et se connectent à deux réseaux privés, avec des conduits ou des listes de contrôle d'accès (ACL) sur le PIX intermédiaire pour permettre le trafic IPSec.

**Remarque :** NAT est une traduction d'adresses un-à-un, à ne pas confondre avec PAT, qui est une traduction plusieurs-à-un (à l'intérieur du pare-feu). Consultez la section Pour examiner l'opération NAT et le dépannage NAT de base ou Comment fonctionne NAT pour plus d'informations sur l'opération NAT et la configuration.

**Remarque :** IPSec avec PAT peut ne pas fonctionner correctement, car le périphérique de point de terminaison du tunnel externe ne peut pas gérer plusieurs tunnels à partir d'une adresse IP. Vous devez contacter votre fournisseur pour déterminer si les périphériques d'extrémité du tunnel fonctionnent avec PAT. En outre, dans les versions 12.2(13)T et ultérieures, la fonctionnalité de transparence NAT peut également être utilisée pour PAT. Référez-vous à Transparence NAT

IPSec pour plus d'informations. Consultez la section Prise en charge de l'ESP d'IPSec par NAT pour plus d'informations sur ces fonctionnalités dans les versions 12.2(13)T et ultérieures. Et, avant que vous ouvriez une valise avec le TAC, consultez les Foires aux questions NAT, où vous trouverez beaucoup de réponses aux questions courantes.

Consultez le Passage de tunnel IPsec à travers un dispositif de sécurité avec l'utilisation de la liste d'accès et MPF avec l'exemple de configuration NAT pour plus d'informations sur la façon configurer un tunnel IPsec moyennant un pare-feu avec NAT sur la version 7.x PIX/ASA.

# 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 12.0.7.T [jusqu'à la limite de 12.2(13)T]Consultez Transparence NAT d'IPSec pour des versions et plus récentes.
- Routeur Cisco 2621 exécutant le logiciel Cisco IOS Version 12.4
- Routeur Cisco 3660 exécutant le logiciel Cisco IOS Version 12.4
- Pare-feu PIX exécutant 6.x

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.

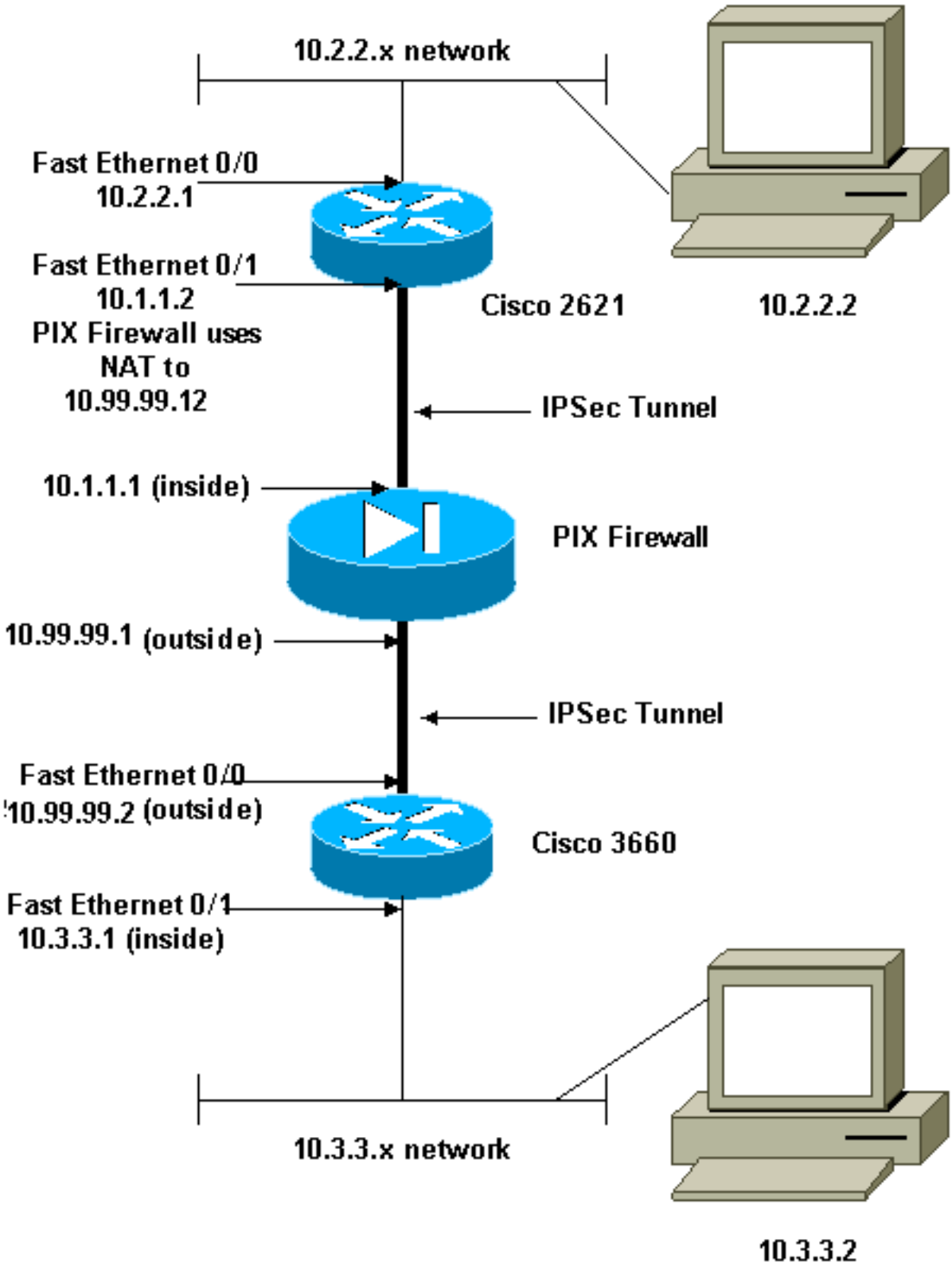
# Configuration

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

**Remarque :** Utilisez l'outil de recherche de commandes (clients inscrits seulement) pour en savoir plus sur les commandes figurant dans le présent document.

## Diagramme du réseau

Ce document utilise la configuration réseau suivante :




**Remarque :** les schémas d'adressage IP utilisés dans cette configuration ne sont pas routables légalement sur Internet. Ce sont des adresses RFC 1918qui ont été utilisées dans un environnement de laboratoire.

## Configurations

Ce document utilise les configurations suivantes :

- Configuration de Cisco 2621
- Configuration partielle du pare-feu PIX de Cisco

- Configuration de Cisco 3660

## Configuration de Cisco 2621

```
Current configuration:
 !
 version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-2621
 !
 ip subnet-zero
 !
 ip audit notify log
 ip audit po max-events 100
 isdn voice-call-failure 0
 cns event-service server
 !
 !--- IKE Policy 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
 !--- IPSec Policy crypto map mymap 10 ipsec-isakmp
  set peer 10.99.99.2
  set transform-set myset
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
 !
 controller T1 1/0
 !
 interface FastEthernet0/0
  ip address 10.2.2.1 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto
 !
 interface FastEthernet0/1
  ip address 10.1.1.2 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto
 !--- Apply to interface. crypto map mymap
 !
 ip classless
 ip route 0.0.0.0 0.0.0.0 10.1.1.1
 no ip http server
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255
 line con 0
  transport input none
 line aux 0
 line vty 0 4
 !
 no scheduler allocate
```

```
 end
```

### Configuration partielle du pare-feu PIX de Cisco

```
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
!--- The fixup protocol esp-ike command is disabled by
default.

fixup protocol esp-ike

ip address outside 10.99.99.1 255.255.255.0
 ip address inside 10.1.1.1 255.255.255.0
 !--- Range of registered IP addresses for use. global
(outside) 1 10.99.99.50-10.99.99.60 !--- Translate any
internal source address when !--- going out to the
Internet. 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

 !--- or access-list acl-out permit esp host 10.99.99.2
host 10.99.99.12
 access-list acl-out permit udp host 10.99.99.2 host
10.99.99.12 eq isakmp
 access-list acl-out permit udp host 10.99.99.2 host
10.99.99.12 eq 4500
!--- It is important to permit UDP port 4500 for NAT-T
because the PIX is acting !--- as a NAT device between
the routers. access-group acl-out in interface outside
isakmp enable outside isakmp enable inside Command
configured in order to enable NAT-T isakmp nat-traversal
20 route outside 0.0.0.0 0.0.0.0 99.99.99.2 1 route
inside 10.2.2.0 255.255.255.0 10.1.1.2 1
```

**Remarque :** La commande **fixup protocol esp-ike** est désactivée par défaut. Si une commande d'ESP-**IKE de protocole de fixup est émise, le fixup est activé, et le pare-feu PIX préserve la source port de l'échange de clés Internet (IKE).** Il crée également une traduction PAT pour le trafic de l'ESP. En outre, si le fixup d'ESP-IKE est actif, l'Internet Security Association and Key Management Protocol (ISAKMP) ne peut pas n'être activé sur aucune interface.

### Configuration de Cisco 3660

```
version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-3660
 !
 ip subnet-zero
```

```
 !
 cns event-service server
 !
 !--- IKE Policy 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
 !--- IPSec Policy crypto map mymap 10 ipsec-isakmp
  set peer 10.99.99.12
  set transform-set myset
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
 !
 interface FastEthernet0/0
  ip address 10.99.99.2 255.255.255.0
  no ip directed-broadcast
  ip nat outside
  duplex auto
  speed auto
 !--- Apply to interface. 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
 !
 interface Ethernet3/0
  no ip address
  no ip directed-broadcast
  shutdown
 !
 interface Serial3/0
  no ip address
  no ip directed-broadcast
  no ip mroute-cache
  shutdown
 !
 interface Ethernet3/1
  no ip address
  no ip directed-broadcast
 interface Ethernet4/0
  no ip address
  no ip directed-broadcast
  shutdown
 !
 interface TokenRing4/0
  no ip address
  no ip directed-broadcast
  shutdown
  ring-speed 16
 !
 !--- Pool from which inside hosts translate to !--- the
globally unique 10.99.99.0/24 network. ip nat pool
OUTSIDE 10.99.99.70 10.99.99.80 netmask 255.255.255.0
 !--- Except the private network from the NAT process.
ip nat inside source route-map nonat pool OUTSIDE
 ip classless
```

```
 ip route 0.0.0.0 0.0.0.0 10.99.99.1
 no ip http server
 !
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
 access-list 101 deny   ip 10.3.3.0 0.0.0.255 any
 !--- Except the private network from the NAT process.
access-list 110 deny   ip 10.3.3.0 0.0.0.255 10.2.2.0
0.0.0.255
 access-list 110 permit ip 10.3.3.0 0.0.0.255 any
 route-map nonat permit 10
  match ip address 110
 !
 line con 0
  transport input none
 line aux 0
 line vty 0 4
 !
 end
```

# Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

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** .

- **show crypto ipsec sa - Montre les associations de sécurisation de phase 2.**
- **show crypto isakmp sa - Montre les associations de sécurisation de phase 1.**
- **show crypto engine connections active - Permet de consulter les paquets cryptés et décryptés.**

# Dépannage

Utilisez cette section pour dépanner votre configuration.

## Dépannage des commandes

**Remarque :** Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug crypto engine - Montre le trafic crypté.**
- **debug crypto ipsec - Permet de consulter les négociations d'IPSec de la phase 2.**
- **debug crypto isakmp SA « Permet de consulter les négociations ISAKMP de la phase 1.**

## Effacer les associations de sécurité.

- **clear crypto isakmp - Efface les associations de sécurisation d'IKE.**
- **clear crypto ipsec sa - Efface les associations de sécurisation d'IPSec.**

## Informations connexes

- Dispositifs de sécurité de la gamme Cisco PIX 500
- Références des commandes du pare-feu Cisco Secure PIX
- Page de support NAT
- Request For Comments (RFC)
- Support et documentation techniques - Cisco Systems