Autoriser les connexions PPTP/L2TP via PIX/ASA/FWSM

Contenu

Introduction

Ce document traite de la configuration requise sur le dispositif de sécurité Cisco/FWSM pour permettre à un client de protocole de tunnellisation point à point (PPTP)/Layer 2 Tunneling Protocol (L2TP) de se connecter à un serveur PPTP via la traduction d'adresses réseau (NAT).

FWSM 3.1.x et versions ultérieures prend en charge PPTP direct avec PAT. Employez l'inspection PPTP afin d'activer cette fonctionnalité.

Remarque: Utilisez la même configuration de PIX pour FWSM.

Référez-vous à Configuration de Cisco Secure PIX Firewall pour utiliser PPTP afin de configurer un dispositif de sécurité pour accepter les connexions PPTP.

Afin de configurer L2TP sur IPsec (IP Security) à partir de clients Microsoft Windows 2000/2003 et Windows XP distants d'un bureau principal de dispositifs de sécurité PIX/ASA utilisant des clés prépartagées avec Microsoft Windows 2003 Internet, référez-vous à Exemple de configuration de L2TP sur IPsec entre Windows 2000/XP PC et PIX/ASA 7.2 avec une clé prépartagée.

Conditions préalables

Conditions requises

Afin d'essayer cette configuration, vous devez avoir un serveur PPTP actif et un client avant d'impliquer PIX/ASA/FWSM.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Logiciels pare-feu Cisco PIX versions 6.x et ultérieures
- Dispositif de sécurité dédié de la gamme Cisco ASA 5500 qui exécute la version 7.x ou ultérieure
- FWSM qui exécute la version 3.1.x ou ultérieure

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.

Théorie générale

PPTP est décrit dans RFC 2637 . Ce protocole utilise une connexion TCP qui utilise le port 1723 et une extension d'encapsulation de routage générique (GRE) [protocole 47] pour transporter les données réelles (trame PPP). La connexion TCP est lancée par le client, suivie de la connexion GRE qui est lancée par le serveur.

Informations sur les versions 6.2 et antérieures

Puisque la connexion PPTP est lancée comme TCP sur un port et la réponse est le protocole GRE, l'algorithme PIX ASA (Adaptive Security Algorithm) ne sait pas que les flux de trafic sont connexes. En conséquence, il est nécessaire de configurer les listes ACL pour permettre le trafic de retour dans PIX. PPTP via PIX avec NAT (mappage d'adresses une à une) fonctionne car PIX utilise les informations sur le port dans l'en-tête TCP ou du protocole de datagramme utilisateur (UDP) pour assurer le suivi de la traduction. PPTP via PIX avec la traduction d'adresses de port (PAT) ne fonctionne pas parce qu'il n'y a aucun concept de ports dans GRE.

Informations sur la version 6.3

La caractéristique de fixup PPTP dans la version 6.3 permet au trafic PPTP pour traverser le PIX une fois configurée pour PAT. Stateful PPTP que l'inspection de paquet est également exécutée dans le processus. La commande **fixup protocol pptp** inspecte les paquets PPTP et crée

dynamiquement les traductions et connexions GRE nécessaires pour permettre le trafic PPTP. Spécifiquement, le pare-feu inspecte les annonces de version PPTP et la séquence de demandes/réponses des appels sortants. Seulement PPTP version 1, comme défini dans RFC 2637, est inspecté. Davantage d'inspection sur le canal de contrôle de TCP est désactivée si la version annoncée par l'un ou l'autre de côté n'est pas la version 1. en outre, la demande d'appel sortant et l'ordre de réponse est dépisté. Les connexions et/ou traductions sont dynamiquement allouées selon les besoins pour permettre le trafic de données GRE secondaire ultérieur. La fonctionnalité de correction PPTP doit être activée pour que le trafic PPTP soit traduit par PAT.

Informations sur la version 7.x

Le moteur d'inspection des applications PPTP dans la version 7.x fonctionne de la même manière que **fixup protocol pptp** dans la version 6.3.

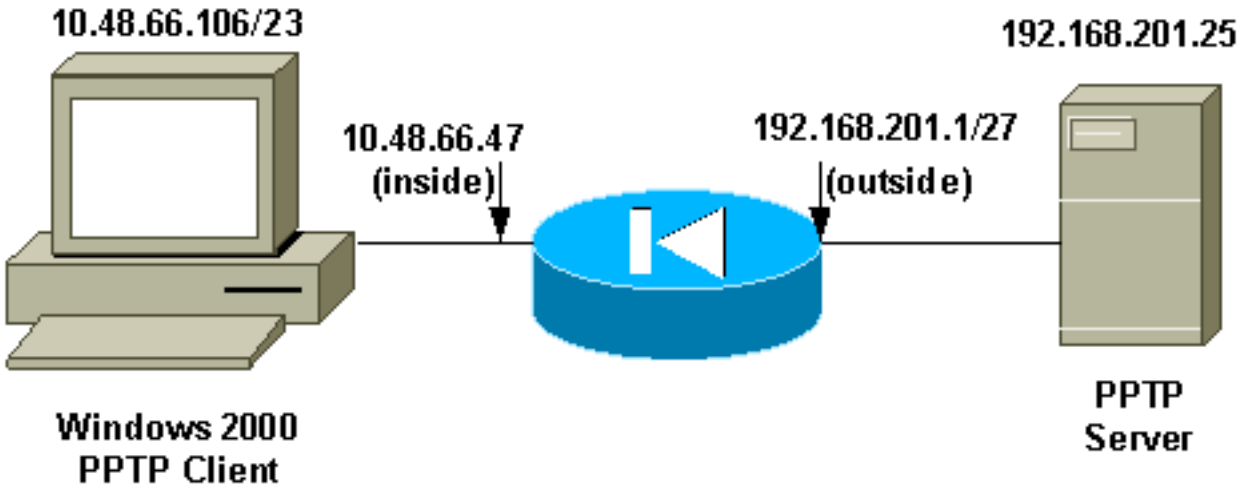
Conventions

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

PPTP avec client à l'intérieur et serveur à l'extérieur

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Remarque: Les schémas d'adressage d'IP utilisés 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.

Commandes à ajouter pour les versions 6.2 et antérieures

Complétez ces étapes pour ajouter des commandes pour la version 6.2 :

1. Définissez le mappage statique pour le PC intérieur. L'adresse vue sur l'extérieur est 192.168.201.5.`pixfirewall(config)#`**`static (inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0`**

2. Configurez et appliquez l'ACL pour permettre le trafic de retour GRE du serveur PPTP au client PPTP.`pixfirewall(config)#`**`access-list acl-out permit gre host 192.168.201.25 host 192.168.201.5`**
3. Appliquez l'ACL.`pixfirewall(config)#`**`access-group acl-out in interface outside`**

Commandes à ajouter pour la version 6.3

Complétez ces étapes pour ajouter des commandes pour la version 6.3 :

1. Activez le protocole de correction pptp 1723 à l'aide de cette commande.`pixfirewall(config)#`**`fixup protocol pptp 1723`**
2. Vous n'avez pas besoin de définir de mappage statique parce que le protocole de correction PPTP est activé. Vous pouvez utiliser PAT.`pixfirewall(config)#`**`nat (inside) 1 0.0.0.0 0.0.0.0 0 0`** `pixfirewall(config)#`**`global (outside) 1 interface`**

Commandes à ajouter pour les versions 7.x et 8.0 utilisant l'inspection

Complétez ces étapes pour ajouter des commandes pour les versions 7.x et 8.0 utilisant la commande **inspect** :

1. Ajoutez l'inspection PPTP à l'élément policy-map par défaut à l'aide de l'élément class-map par défaut.`pixfirewall(config)#`**`policy-map global_policy`** `pixfirewall(config-pmap)#`**`class inspection_default`** `pixfirewall(config-pmap-c)#`**`inspect pptp`**
2. Vous n'avez pas besoin de définir de mappage statique parce que PIX inspecte maintenant le trafic PPTP. Vous pouvez utiliser PAT.`pixfirewall(config)#`**`nat (inside) 1 0.0.0.0 0.0.0.0 0 0`** `pixfirewall(config)#`**`global (outside) 1 interface`** OU

Commandes à ajouter pour les versions 7.x et 8.0 utilisant ACL

Complétez ces étapes pour ajouter des commandes pour les versions 7.x et 8.0 utilisant ACL.

1. Définissez le mappage statique pour le PC intérieur. L'adresse vue sur l'extérieur est 192.168.201.5.`pixfirewall(config)#`**`static (inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0`**
2. Configurez et appliquez l'ACL pour permettre le trafic de retour GRE du serveur PPTP au client PPTP.`pixfirewall(config)#`**`access-list acl-out permit gre host 192.168.201.25 host 192.168.201.5`** `pixfirewall(config)#`**`access-list acl-out permit tcp host 192.168.201.25 host 192.168.201.5 eq 1723`**
3. Appliquez l'ACL.`pixfirewall(config)#`**`access-group acl-out in interface outside`**

Configuration pour les versions 6.2 et antérieures

Configuration PIX - Client à l'intérieur, serveur à l'extérieur
`pixfirewall(config)#`**`write terminal`** `Building configuration... : Saved : PIX Version 6.2(1) nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 intf2 security10 enable password Ujkil6aDv2yp6suI encrypted passwd OnTrBUG1Tp0edmkr encrypted hostname pixfirewall domain-name cisco.com fixup protocol ftp 21 fixup protocol http`

```
80 fixup protocol h323 h225 1720 fixup protocol h323 ras
1718-1719 fixup protocol ils 389 fixup protocol rsh 514
fixup protocol rtsp 554 fixup protocol smtp 25 fixup
protocol sqlnet 1521 fixup protocol sip 5060 fixup
protocol skinny 2000 no names !--- This line allows GRE
traffic from the !--- PPTP server to the client. access-
list acl-out permit gre host 192.168.201.25 host
192.168.201.5 pager lines 24 logging on logging console
debugging logging trap debugging interface ethernet0
auto interface ethernet1 auto interface ethernet2 auto
shutdown mtu outside 1500 mtu inside 1500 mtu intf2 1500
ip address outside 209.165.201.1 255.255.255.224 ip
address inside 10.48.66.47 255.255.254.0 ip address
intf2 127.0.0.1 255.255.255.255 ip audit info action
alarm ip audit attack action alarm no failover failover
timeout 0:00:00 failover poll 15 failover ip address
outside 0.0.0.0 failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0 pdm history enable arp
timeout 14400 !--- This allows traffic from a low
security interface to !--- a high security interface.
static (inside,outside) 192.168.201.5 10.48.66.106
netmask 255.255.255.255 0 0 !--- This applies the ACL to
the outside interface. access-group acl-out in interface
outside timeout xlate 3:00:00 timeout conn 1:00:00 half-
closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip
0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute
uauth 0:04:00 inactivity aaa-server TACACS+ protocol
tacacs+ aaa-server RADIUS protocol radius aaa-server
LOCAL protocol local no snmp-server location no snmp-
server contact snmp-server community public snmp-server
enable traps no floodguard enable no sysopt route dnat
telnet timeout 5 ssh timeout 5 terminal width 80
Cryptochecksum:18bdf8e21bd72ec0533795549165ecf5 : end
[OK]
```

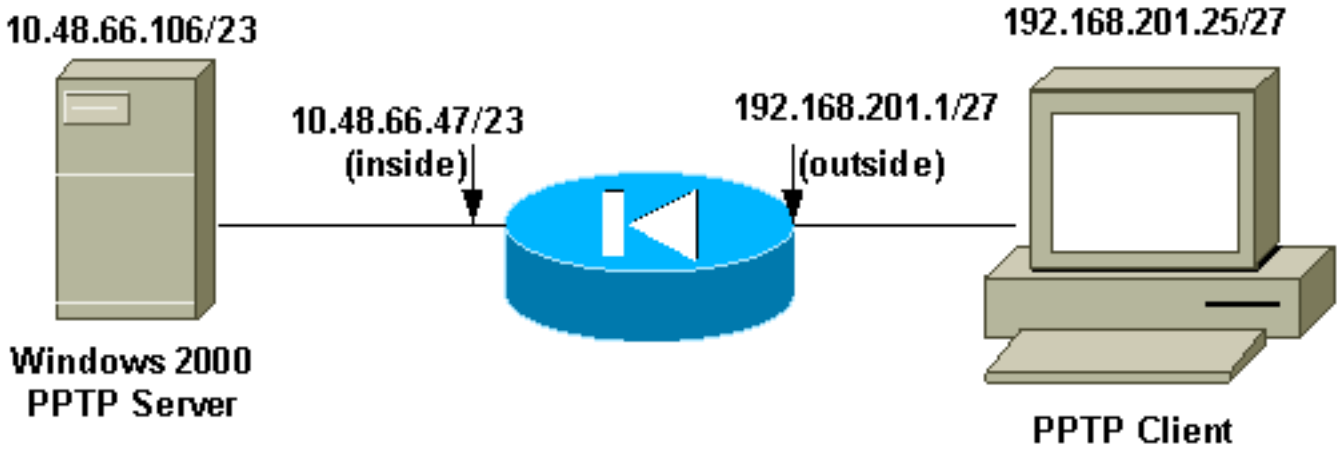
L2TP avec client à l'intérieur et serveur à l'extérieur

Complétez ces étapes afin d'ajouter des commandes pour les versions 7.x et 8.x qui utilisent ACL. (Cette configuration suppose que les adresses IP du serveur et du client PPTP sont les mêmes que pour le serveur et le client L2TP.)

1. Définissez le mappage statique pour le PC intérieur. L'adresse vue sur l'extérieur est 192.168.201.5.`pixfirewall(config)#`**`static (inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0`**
2. Configurez et appliquez l'ACL pour permettre le trafic de retour L2TP du serveur L2TP au client L2TP.`pixfirewall(config)#`
   `pixfirewall(config)#`**`access-list acl-out permit udp host 192.168.201.25 host 192.168.201.5 eq 1701`**
3. Appliquez l'ACL.`pixfirewall(config)#`**`access-group acl-out in interface outside`**

PPTP avec client à l'extérieur et serveur à l'intérieur

Diagramme du réseau



Remarque: Les schémas d'adressage d'IP utilisés 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.

Commandes à ajouter à toutes les versions

Dans cet exemple de configuration, le serveur PPTP est 192.168.201.5 (statique à 10.48.66.106 à l'intérieur) et le client PPTP est 192.168.201.25.

```
access-list acl-out permit gre host 192.168.201.25 host 192.168.201.5 access-list acl-out permit
tcp host 192.168.201.25 host 192.168.201.5 eq 1723 static (inside,outside) 192.168.201.5
10.48.66.106 netmask 255.255.255.255 0 0 access-group acl-out in interface outside
```

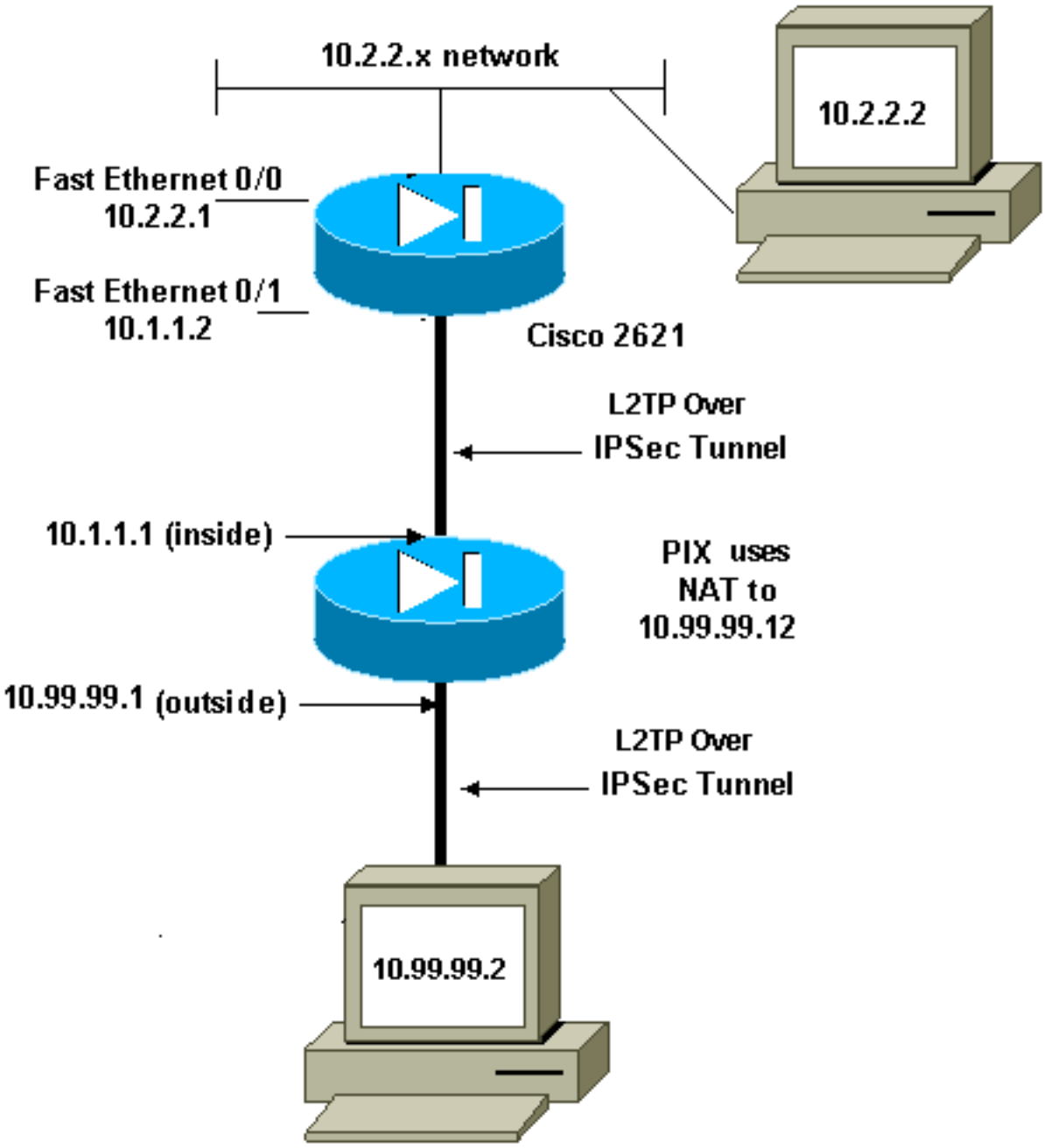
L2TP avec client à l'extérieur et serveur à l'intérieur

Dans cet exemple de configuration, le serveur L2TP est 192.168.201.5 (statique à 10.48.66.106 à l'intérieur) et le client L2TP est 192.168.201.25. (Cette configuration suppose que les adresses IP du serveur et du client PPTP sont les mêmes que pour le serveur et le client L2TP.)

```
access-list acl-out permit udp host 192.168.201.25 host 192.168.201.5 eq 1701 static
(inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0 access-group acl-out in
interface outside
```

Autoriser L2TP sur IPsec via PIX/ASA 7.x et versions ultérieures

Le client L2TP extérieur essaye d'établir la connexion VPN L2TP sur IPsec avec le serveur L2TP intérieur. Afin d'autoriser les paquets L2TP sur IPsec via PIX/ASA intermédiaire, vous devez permettre à ESP, ISAKMP(500), NAT-T et au port L2TP 1701 d'établir le tunnel. Les paquets L2TP sont traduits dans PIX et envoyés via le tunnel VPN.




```
global (outside) 1 interface
nat (inside) 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
access-group outside_access_in in interface outside

access-list outside_access_in remark Access Rule to Allow ESP traffic
access-list outside_access_in extended permit esp host 10.99.99.2
            host 10.99.99.12

access-list outside_access_in remark Access Rule to allow ISAKMP to
            host 10.99.99.12
access-list outside_access_in extended permit udp host 10.99.99.2 eq isakmp
            host 10.99.99.12

access-list outside_access_in remark Access Rule to allow port 4500 (NAT-T) to
            host 10.99.99.12
access-list outside_access_in extended permit udp host 10.99.99.2 eq 4500
            host 10.99.99.12

access-list outside_access_in remark Access Rule to allow port 1701 (L2TP) to
            host 10.99.99.12
```

```
access-list outside_access_in extended permit udp host 10.99.99.2 eq 1701
            host 10.99.99.12
```

Vérifiez

Aucune procédure de vérification n'est disponible pour ce document.

Dépannez

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

Les connexions multiples PPTP/L2TP échouent en utilisant PAT

Vous pouvez seulement avoir une connexion PPTP/L2TP via le dispositif de sécurité PIX quand vous utilisez PAT. C'est parce que la connexion GRE nécessaire est établie sur le port 0 et le dispositif de sécurité PIX ne mappe le port 0 qu'à un hôte. La solution de contournement est d'activer l'inspection PPTP sur le dispositif de sécurité.

Erreur 800 en essayant de se connecter à PPTP VPN d'arrivée

Quand vous essayez de se connecter à PPTP VPN d'arrivée, ce message d'erreur apparaît :

```
Error 800: The remote connection was not made because the attempted VPN tunnels failed. The VPN
server might be unreachable. If this connection is attempting to use an L2TP/IPsec tunnel, the
security parameters required for IPsec negotiation might not be configured properly.
```

Cette question se produit habituellement quand la fonction émulation PPTP ou L2TP n'est pas activée sur l'intermédiaire ASA entre le client et le périphérique de headend. Activez la fonction émulation PPTP ou L2TP et vérifiez la configuration afin de résoudre le problème.

Commandes de débogage

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** .

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Cet exemple montre un client PPTP à l'intérieur de PIX qui lance une connexion à un serveur PPTP en dehors de PIX quand il n'y a aucune ACL configurée pour permettre le trafic GRE. Avec le débogage de journalisation sur PIX, vous pouvez voir l'initiation de trafic du port TCP 1723 du client et le rejet du trafic de retour de protocole 47 GRE.

```
pixfirewall(config)#loggin on pixfirewall(config)#loggin console 7 pixfirewall(config)#302013:
Built outbound TCP connection 4 for outside: 192.168.201.25 /1723 (192.168.201.25 /1723) to
inside:10.48.66.106/4644 (192.168.201.5 /4644) 106010: Deny inbound protocol 47 src
outside:192.168.201.25 dst inside:192.168.201.5 106010: Deny inbound protocol 47 src
outside:192.168.201.25 dst inside:192.168.201.5
```

Informations à collecter si vous ouvrez une demande de service TAC

Si vous avez toujours besoin d'aide après avoir suivi les étapes de dépannage ci-dessus et voulez ouvrir une demande de service avec Cisco TAC, veillez à inclure les informations suivantes.
• Description du problème et des détails topologiques pertinents • Dépannage exécuté avant d'ouvrir la demande de service • Sortie de la commande **show tech-support** • Sortie de la commande **show log** après l'exécution avec la commande **logging buffered debugging** , ou les captures de console qui expliquent le problème (si disponible) Veuillez joindre les données rassemblées à votre demande de service en format non compressé et texte clair (.txt). Vous pouvez joindre des informations à votre demande de service en la téléchargeant à l'aide de l'outil de requête de demande de service (clients enregistrés uniquement). Si vous ne pouvez pas accéder à l'outil de requête de demande de service, vous pouvez envoyer l'information en pièce jointe dans un e-mail à attach@cisco.com avec votre numéro de demande de service dans le sujet du message.

Informations connexes

- Page de support PPTP
- Exemple de configuration du passage d'un tunnel IPSec PIX/ASA 7.x et versions ultérieures via un dispositif de sécurité avec utilisation de liste d'accès et MPF avec NAT
- Configuration d'un tunnel IPSec par un pare-feu avec NAT
- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems