PIX 6.x : Exemple de configuration de l'authentification de PPTP avec Radius

Contenu

Introduction

Le Protocole PPTP (Point-to-Point Tunneling Protocol) est un protocole de perçage d'un tunnel de la couche 2 qui permet à un client distant pour employer un réseau IP public afin de communiquer sécurisé avec des serveurs à un réseau d'entreprise. PPTP perce un tunnel l'IP. PPTP est décrit dans RFC 2637 . Le support PPTP sur le Pare-feu PIX a été ajouté dans la version du logiciel PIX 5.1. La documentation PIX fournit à plus d'informations sur PPTP et à son utilisation le PIX. Ce document décrit comment configurer le PIX pour utiliser PPTP avec des gens du pays,

l'authentification TACACS+, et de RAYON. Ce document fournit également des conseils et des exemples que vous pouvez employer pour vous aider à dépanner des problèmes courants.

Ce document affiche comment configurer des connexions PPTP au PIX. Afin de configurer un PIX ou une ASA pour permettre PPTP *par les* dispositifs de sécurité, référez-vous à permettre des connexions PPTP/L2TP par le PIX.

Référez-vous au pare-feu Cisco Secure PIX 6.x et au serveur 3.5 pour Windows avec le Microsoft Windows 2000 et l'authentification de RAYON de 2003 IAS afin de configurer le Pare-feu et le client vpn PIX pour l'usage avec le Windows 2000 et 2003 de Client VPN Cisco de Service d'authentification Internet (IAS) de RAYON.

Référez-vous à configurer le concentrateur VPN 3000 et le PPTP avec le Cisco Secure ACS pour l'authentification de RAYON de Windows afin de configurer PPTP sur un concentrateur VPN 3000 avec le Cisco Secure ACS pour Windows pour l'authentification de RAYON.

Référez-vous à configurer le Cisco Secure ACS pour l'authentification du routeur PPTP de Windows afin d'installer une connexion par PC au routeur, qui fournit alors l'authentification de l'utilisateur au Système de contrôle d'accès sécurisé Cisco (ACS) 3.2 pour des Windows Server, avant que vous permettiez l'utilisateur dans le réseau.

Remarque: En termes PPTP, par RFC, le PPTP Network Server (PNS) est le serveur (dans ce cas, le PIX, ou l'appelé) et le concentrateur PPTP Access (PAC) est le client (le PC, ou l'appelant).

Remarque: La Segmentation de tunnel n'est pas prise en charge sur PIX pour des clients PPTP.

Remarque: PIX 6.x a besoin de MS-CHAP v1.0 pour que PPTP fonctionne. Les Windows Vista ne prennent en charge pas MS-CHAP v1.0. Ainsi PPTP sur PIX 6.x ne fonctionnera pas pour des Windows Vista. PPTP n'est pas pris en charge dans la version de PIX 7.x et plus tard.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur la version de logiciel 6.3(3) de pare-feu Cisco Secure PIX.

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.

Conventions

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

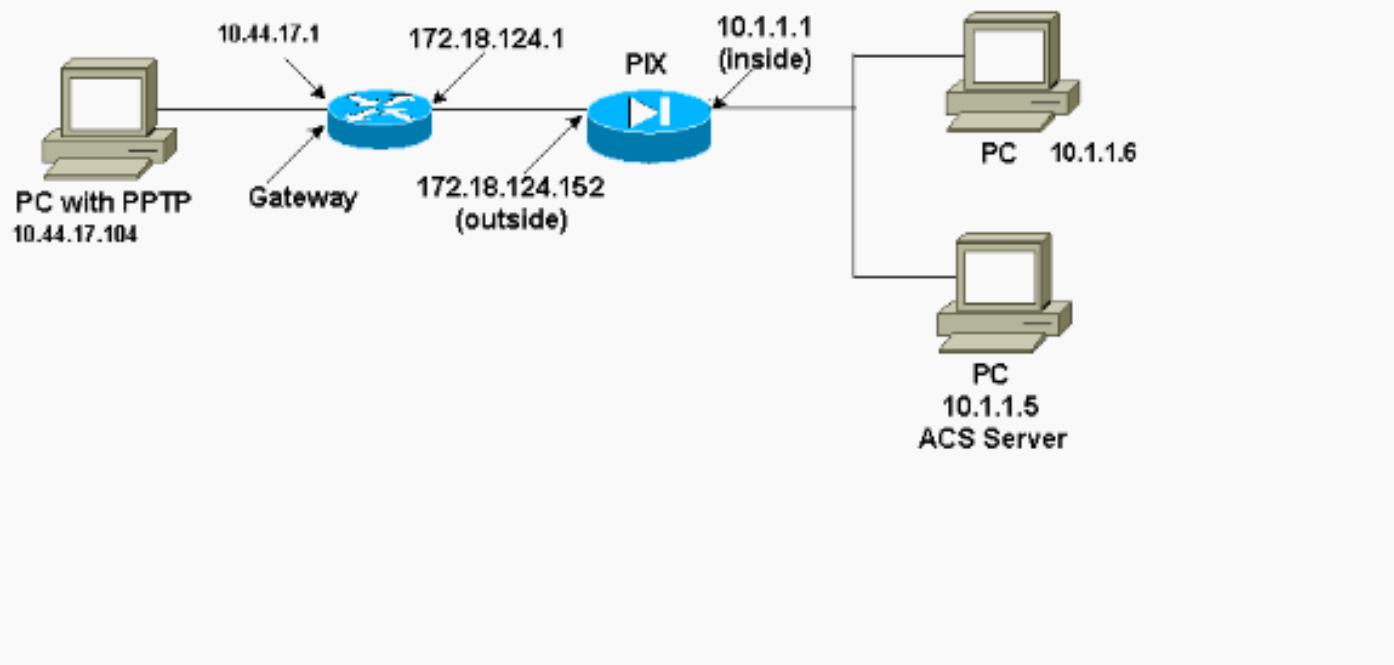
Configurez

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

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise cette configuration du réseau.



Conseils de configuration pour le Pare-feu PIX

Type d'authentification - CHAP, PAP, MS-CHAP

Le PIX configuré pour chacune des trois méthodes d'authentification (CHAP, PAP, MS-CHAP) fournit en même temps la meilleure occasion de connecter n'importe comment le PC est configuré. C'est une bonne idée pour dépanner des buts.

```
vpdn group 1 ppp authentication chap vpdn group 1 ppp authentication mschap vpdn group 1 ppp authentication pap
```

Cryptage point par point de Microsoft (MPPE)

Employez cette syntaxe de commande afin de configurer le chiffrement MPPE sur le Pare-feu PIX.

```
vpdn group 1 ppp encryption mppe 40|128|auto [required]
```

Dans cette commande, **exigée** est un mot clé facultatif. MS-CHAP doit être configuré.

Configurez la caractéristique PPTP sur des PC de client

Remarque: Les informations disponibles ici sur connexe à la configuration de logiciel Microsoft ne sont livré avec aucune garantie ou logiciel de support pour microsoft. Le logiciel de support pour microsoft est disponible de Microsoft et au site Web de support de Microsoft .

Windows 98

Suivez ces étapes afin d'installer la caractéristique PPTP sur le Windows 98.

1. **Start > Settings > Control Panel > Add New Hardware** choisi. Cliquez sur **Next** (Suivant).
2. Cliquez sur **choisi de la liste** et choisissez l'**adaptateur réseau**. Cliquez sur **Next** (Suivant).
3. Choisissez **Microsoft** dans le panneau et l'**adaptateur** gauches de **Microsoft VPN** sur le panneau de droite.

Suivez ces étapes afin de configurer la caractéristique PPTP.

1. **Start > Programs > Accessories > Communications > Dial Up Networking** choisi.
2. Le clic **établissent le nouveau rapport**. Pour **Select un périphérique**, se connectent à l'aide de l'**adaptateur de Microsoft VPN**. L'adresse IP de serveur VPN est le point d'extrémité de tunnel PIX.
3. L'authentification par défaut de Windows 98 utilise le cryptage de mot de passe (CHAP ou MS-CHAP). Afin de changer le PC pour permettre également le PAP, **Properties > Server types** choisi. Désactivez **Require encrypted password**. Vous pouvez configurer le chiffrement des données (MPPE ou pas de MPPE) dans cette zone.

Windows 2000

Suivez ces étapes afin de configurer la caractéristique PPTP sur le Windows 2000.

1. Sélectionnez le **début > les programmes > les accessoires > les transmissions > le réseau et les connexions d'accès par réseau commuté**.
2. Le clic **établissent le nouveau rapport**, puis cliquent sur Next.
3. Choisi **connectez à un réseau privé par l'Internet** et **composez une connexion antérieurement** (ou si RÉSEAU LOCAL). Cliquez sur **Next** (Suivant).
4. Écrivez l'adresse Internet ou l'adresse IP du périphérique du tunnel (PIX/router).
5. Si vous devez changer le type de mot de passe, **Properties > Security for the connection > Advanced** choisi. La valeur par défaut est MS-CHAP et MS-CHAP v2 (et non CHAP ou PAP). Vous pouvez configurer le chiffrement des données (MPPE ou pas de MPPE) dans cette zone.

Windows NT

Référez-vous à installer, à configurer, et à employer PPTP avec des clients et serveurs de Microsoft pour installer des clients de NT pour PPTP.

Configurez le PIX

Configuration PIX - Authentification locale, aucun cryptage
`PIX Version 6.3(3)`

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access-list 101 permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0 pager lines 24 logging on no
logging timestamp no logging standby no logging console
no logging monitor logging trap debugging no logging
history logging facility 20 logging queue 512 interface
ethernet0 10baset interface ethernet1 10baset interface
ethernet2 10baset mtu outside 1500 mtu inside 1500 mtu
pix/intf2 1500 ip address outside 172.18.124.152
255.255.255.0 ip address inside 10.1.1.1 255.255.255.0
ip address pix/intf2 127.0.0.1 255.255.255.255 ip local
pool pptp-pool 192.168.1.1-192.168.1.50 no failover
failover timeout 0:00:00 failover ip address outside
0.0.0.0 failover ip address inside 0.0.0.0 failover ip
address pix/intf2 0.0.0.0 arp timeout 14400 global
(outside) 1 172.18.124.201-172.18.124.202 nat (inside) 0
access-list 101 nat (inside) 1 10.1.1.0 255.255.255.0 0
0 conduit permit icmp any any route outside 0.0.0.0
0.0.0.0 172.18.124.1 1 timeout xlate 3:00:00 conn
1:00:00 half-closed 0:10:00 udp 0:02:00 timeout rpc
0:10:00 h323 0:05:00 timeout uauth 0:05:00 absolute aaa-
server TACACS+ protocol tacacs+ aaa-server RADIUS
protocol radius no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps floodguard enable sysopt connection permit-
pptp isakmp identity hostname telnet timeout 5 vpdn
group 1 accept dialin pptp vpdn group 1 ppp
authentication pap vpdn group 1 ppp authentication chap
vpdn group 1 ppp authentication mschap vpdn group 1
client configuration address local pptp-pool vpdn group
1 client authentication local vpdn username cisco
password cisco vpdn enable outside terminal width 80
Cryptochecksum:a72d9f71d1a31332307fcd348e02410d : end
```

Configuration PIX - Authentification locale avec le cryptage

Si vous ajoutez cette commande à la configuration PIX - l'authentification locale, aucune configuration de chiffrement, le PC et PIX n'en autonégocient le cryptage 40-bit ou aucun (basé sur des configurations PC).

vpdn group 1 ppp encryption mppe auto

Si le PIX a la fonction activée 3DES, la commande de **show version** affiche ce message.

- Versions 6.3 et ultérieures :`VPN-3DES-AES: Enabled`
- Versions 6.2 et antérieures :`VPN-3DES: Enabled`

le cryptage 128-bit est également possible. Cependant, si un de ces messages est affiché, puis le PIX n'est pas activé pour le cryptage 128-bit.

- Versions 6.3 et ultérieures :`Warning: VPN-3DES-AES license is required for 128 bits MPPE encryption`
- Versions 6.2 et antérieures :`Warning: VPN-3DES license is required for 128 bits MPPE encryption`

La syntaxe pour la commande MPPE est affichée ici.

vpdn group ppp encryption mppe 40|128|auto [required]

Le PC et le PIX doivent être configurés pour l'authentification MS-CHAP en même temps que le MPPE.

Configuration PIX - Authentification TACACS+/RADIUS sans cryptage

```
PIX Version 6.3(3)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname PIX
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access-list 101 permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0 pager lines 24 logging on
logging timestamp no logging standby logging console
debugging no logging monitor logging buffered debugging
logging trap debugging no logging history logging
facility 20 logging queue 512 interface ethernet0
10baset interface ethernet1 10baset interface ethernet2
10baset mtu outside 1500 mtu inside 1500 mtu pix/intf2
1500 ip address outside 172.18.124.152 255.255.255.0 ip
address inside 10.1.1.1 255.255.255.0 ip address
pix/intf2 127.0.0.1 255.255.255.255 ip local pool pptp-
pool 192.168.1.1-192.168.1.50 no failover failover
timeout 0:00:00 failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0 failover ip address
pix/intf2 0.0.0.0 arp timeout 14400 global (outside) 1
172.18.124.201-172.18.124.202 nat (inside) 0 access-list
101 nat (inside) 1 10.1.1.0 255.255.255.0 0 0 conduit
permit icmp any any route outside 0.0.0.0 0.0.0.0
172.18.124.1 1 timeout xlate 3:00:00 conn 1:00:00 half-
closed 0:10:00 udp 0:02:00 timeout rpc 0:10:00 h323
0:05:00 timeout uauth 0:05:00 absolute aaa-server
TACACS+ protocol tacacs+ aaa-server RADIUS protocol
radius !--- Use either RADIUS or TACACS+ in this
statement. aaa-server AuthInbound protocol radius |
tacacs+ aaa-server AuthInbound (outside) host
172.18.124.99 cisco timeout 5 no snmp-server location no
snmp-server contact snmp-server community public no
snmp-server enable traps floodguard enable sysopt
connection permit-pptp isakmp identity address telnet
10.1.1.5 255.255.255.255 inside telnet 10.1.1.5
255.255.255.255 pix/intf2 telnet timeout 5 vpdn group 1
accept dialin pptp vpdn group 1 ppp authentication pap
vpdn group 1 ppp authentication chap vpdn group 1 ppp
authentication mschap vpdn group 1 client configuration
```

```
address local pptp-pool vpdn group 1 client
authentication aaa AuthInbound vpdn enable outside
terminal width 80
Cryptochecksum:96e9c93cb0a6ad6f53581dd7b61ac763 : end
[OK]
```

Configuration PIX - Authentification de RAYON avec le cryptage

Si le RAYON est utilisé, et si le serveur de RAYON (attribut 26 de constructeur-particularité, Microsoft comme constructeur) prend en charge la génération de clés MPPE, le chiffrement MPPE peut être ajouté. L'authentification TACACS+ ne fonctionne pas avec le cryptage parce que les serveurs TACACS+ ne sont pas capables de renvoyer des clés MPPE spéciales. Le Cisco Secure ACS pour Windows 2.5 et le RAYON postérieur prend en charge le MPPE (tous les serveurs de RAYON ne prennent en charge pas le MPPE).

Avec la supposition que l'authentification de RAYON fonctionne sans cryptage, ajoutez le cryptage en incluant cette commande dans la configuration précédente :

vpdn group 1 ppp encryption mppe auto

Le PC et le PIX n'en autonégocie le cryptage 40-bit ou aucun (basé sur des configurations PC).

Si le PIX a la fonction activée 3DES, la commande de **show version** affiche ce message.

```
VPN-3DES: Enabled
```

le cryptage 128-bit est également possible. Cependant, si ce message est affiché, le PIX n'est pas activé pour le cryptage 128-bit.

```
Warning: VPN-3DES license is required
for 128 bits MPPE encryption
```

La syntaxe pour la commande MPPE est affichée dans cette sortie.

vpdn group ppp encryption mppe 40|128|auto [required]

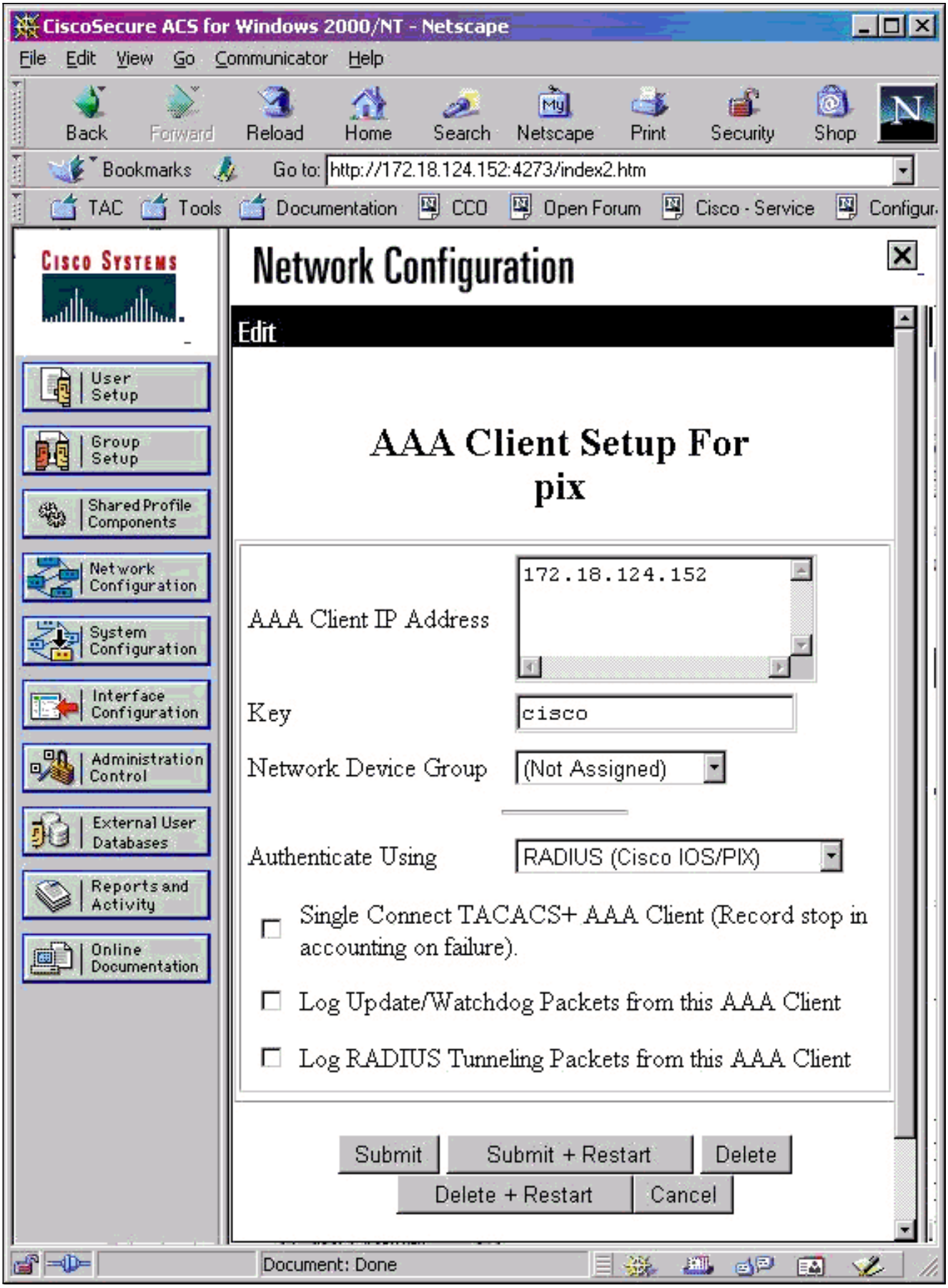
Le PC et le PIX doivent être configurés pour l'authentification MS-CHAP en même temps que le MPPE.

Configurez le Cisco Secure ACS pour Windows 3.0

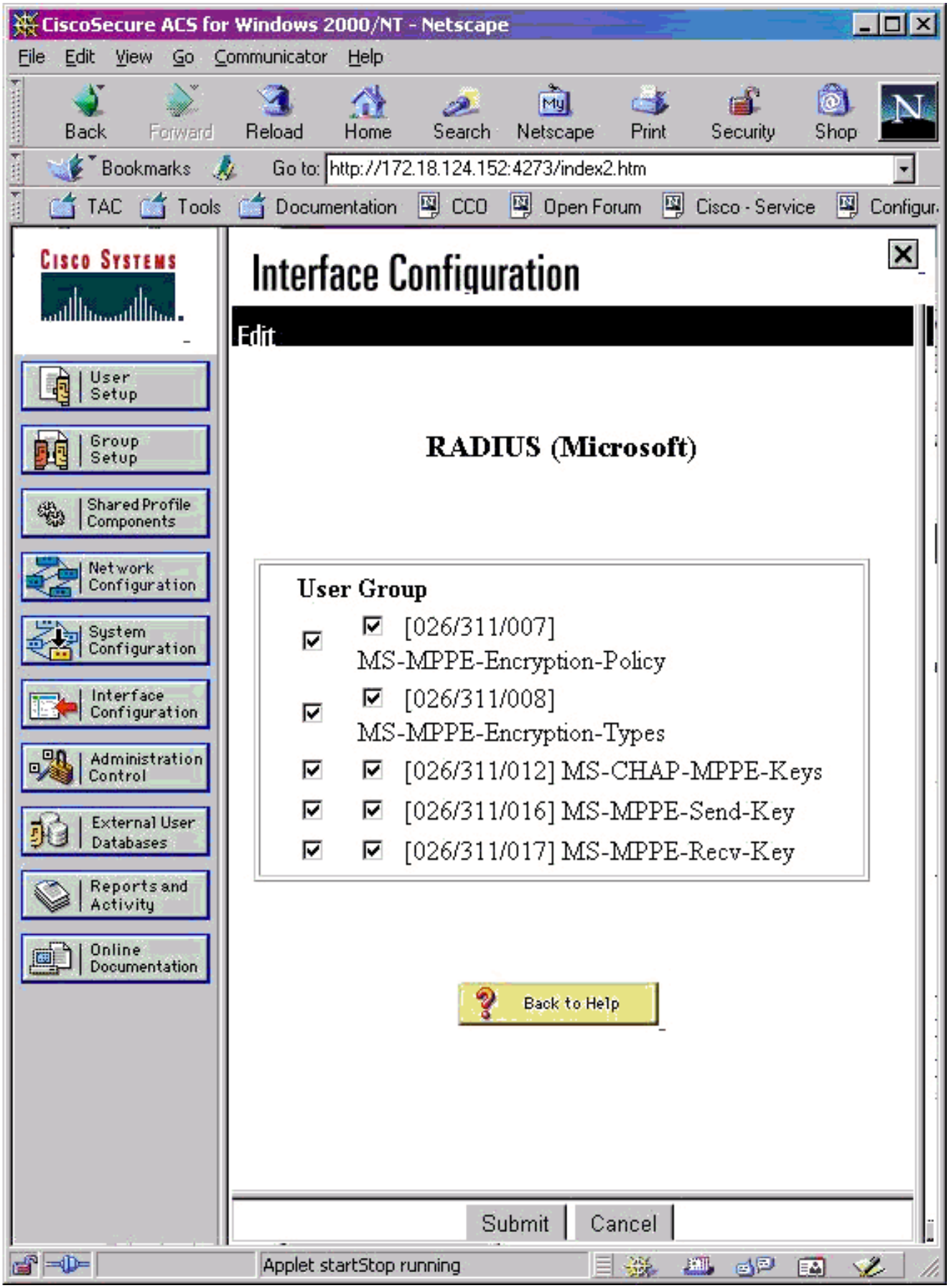
Authentification de RAYON avec le cryptage

Employez ces étapes afin de configurer le Cisco Secure ACS pour Windows 3.0. Les mêmes étapes de configuration s'appliquent aux versions 3.1 et 3.2 ACS.

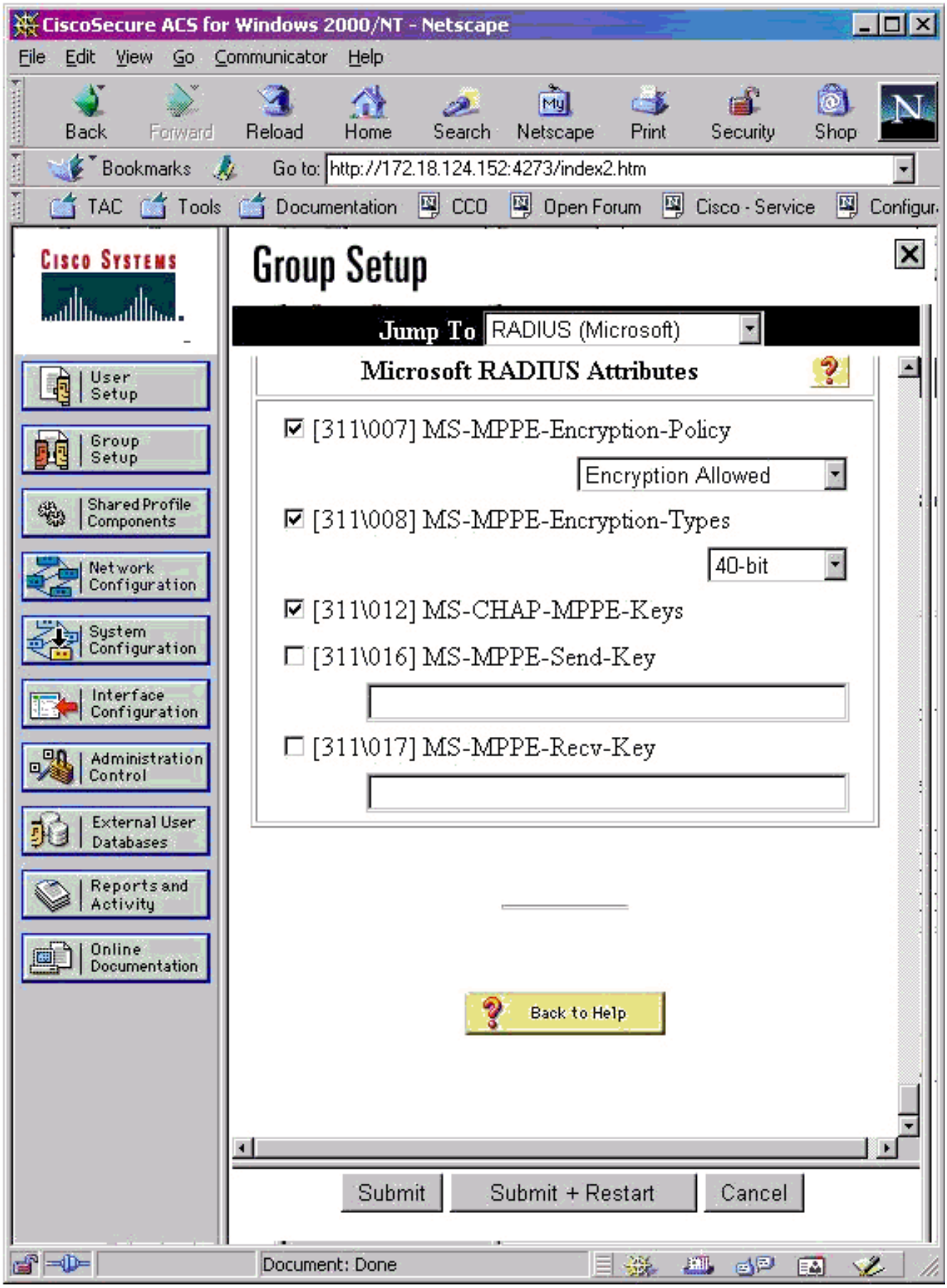
1. Ajoutez le PIX au Cisco Secure ACS pour la **configuration réseau de** Windows Server et identifiez le dictionnaire-type comme **RAYON (Cisco IOS/PIX)**.



2. Ouvrez la **configuration d'interface > le RAYON (Microsoft)** et vérifiez les attributs MPPE afin de les faire apparaître dans l'interface de groupe.



3. Ajoutez un utilisateur. Dans le Groupe d'utilisateurs, ajoutez MPPE [RAYON (Microsoft)] attributs. Vous devez activer ces attributs pour le cryptage et il est facultatif quand le PIX n'est pas configuré pour le
cryptage.



Vérifiez

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

Commandes show PIX (authentification de courrier)

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** .

Les listes de commandes de **show vpdn** tunnel et informations de session.

```
PIX#show vpdn PPTP Tunnel and Session Information (Total tunnels=1 sessions=1) Tunnel id 13,
remote id is 13, 1 active sessions Tunnel state is estabd, time since event change 24 secs
remote Internet Address 10.44.17.104, port 1723 Local Internet Address 172.18.124.152, port 1723
12 packets sent, 35 received, 394 bytes sent, 3469 received Call id 13 is up on tunnel id 13
Remote Internet Address is 10.44.17.104 Session username is cisco, state is estabd Time since
event change 24 secs, interface outside Remote call id is 32768 PPP interface id is 1 12 packets
sent, 35 received, 394 bytes sent, 3469 received Seq 13, Ack 34, Ack_Rcvd 12, peer RWS 64 0 out
of order packets
```

Vérification de PC client

Dans une fenêtre de MS-DOS, ou de la fenêtre de passage, **ipconfig /all de** type. La partie d'adaptateur de PPP affiche cette sortie.

```
PPP adapter pptp:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : WAN (PPP/SLIP) Interface
        Physical Address. . . . . . . . . : 00-53-45-00-00-00
        DHCP Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.1.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . :
```

Vous pouvez également cliquer sur des **détails** afin de visualiser les informations dans la connexion PPTP.

Dépannez

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

- Il doit y avoir Connectivité pour l'Encapsulation de routage générique (GRE) et de TCP 1723 du PC au point d'extrémité de tunnel PIX. S'il y a n'importe quelle occasion que ceci est bloqué par un Pare-feu ou une liste d'accès, déplacez le PC plus près du PIX.
- Il est le plus facile installer le Windows 98 et le Windows 2000 PPTP. En cas de doute, plusieurs PC d'essai et systèmes d'exploitation. Après une connexion réussie, **détails de** clic sur le PC afin d'afficher des informations sur la connexion. Par exemple, si vous utilisez le PAP, CHAP, IP, cryptage, et ainsi de suite.
- Si vous avez l'intention d'utiliser le RAYON et/ou le TACACS+, essayez d'installer (nom d'utilisateur et mot de passe sur le PIX) l'authentification locale d'abord. Si ceci ne fonctionne pas, authentifier avec un serveur de RAYON ou TACACS+ ne fonctionne pas.
- Au commencement, veillez les paramètres de sécurité sur le PC pour permettre autant de différents types d'authentification en tant que possible (PAP, CHAP, MS-CHAP) et pour décocher la case pour le **chiffrement de données Require** (rendez lui facultatifs chacun des deux sur le PIX et le PC).
- Puisque le type d'authentification est négocié, configurez le PIX avec le nombre maximal de

possibilités. Par exemple, si le PC est configuré pour seulement MS-CHAP et le routeur pour seulement le PAP, il n'y a jamais n'importe quel accord.
- Si le PIX agit en tant que serveur PPTP pour deux endroits différents et chaque emplacement a son propre serveur de RAYON sur l'intérieur, utilisant un PIX simple pour les deux emplacements entretenus par leur propre serveur de RAYON n'est pas pris en charge.
- Quelques serveurs de RAYON ne prennent en charge pas le MPPE. Si un serveur de RAYON ne prend en charge pas la génération de clés MPPE, l'authentification de RAYON fonctionne, mais le chiffrement MPPE ne fonctionne pas.
- Avec le Windows 98 ou plus tard, quand vous utilisez le PAP ou le CHAP, le nom d'utilisateur envoyé au PIX est identique à ce qui est présenté dans la connexion (BRUNE GRISÂTRE) commutée de réseau. Mais quand vous utilisez MS-CHAP, le nom de domaine peut être ajouté à l'avant du nom d'utilisateur, par exemple :Nom d'utilisateur écrit dans le DUN - « Cisco »Positionnement de domaine sur la case de Windows 98 - « DOMAINE »Le nom d'utilisateur MS-CHAP a envoyé à PIX - « DOMAINE \ Cisco »Nom d'utilisateur sur PIX - « Cisco »Résultat - Nom d'utilisateur/mot de passe non valideC'est une section du log de PPP d'un PC de Windows 98 qui affiche le comportement.
```
02-01-2001 08:32:06.78 - Data 0038: 49
53 4c 41 42 5c 63 69 | DOMAIN\ci
02-01-2001 08:32:06.78 - Data 0040: 73 63 6f 00 00 00 00 00 | sco.....
|
|
02-01-2001 08:32:06.80 - Data 0000: c2 23 04 01 00 1a 41 75 | .#...^ZAu
02-01-2001 08:32:06.80 - Data 0008: 74 68 65 6e 74 69 63 61 | thentica
02-01-2001 08:32:06.80 - Data 0010: 74 69 6f 6e 20 66 61 69 | tion fai
02-01-2001 08:32:06.80 - Data 0018: 6c 65 64 2e 00 00 00 00 | led.....
02-01-2001 08:32:06.80 - CHAP : Login failed: username, password,
   or domain was incorrect.
```
Si vous utilisez le Windows 98 et MS-CHAP au PIX, en plus de avoir le nom d'utilisateur hors domaine, vous pouvez ajouter le « DOMAINE \ nom d'utilisateur » au PIX :

vpdn username cisco password cisco vpdn username DOMAIN\cisco password cisco **Remarque:** Si vous exécutez l'authentification à distance sur un serveur d'AAA, le même s'applique.

Dépannage des commandes

Les informations sur l'ordre de l'ordre prévu des événements PPTP sont trouvées dans le RFC 2637 PPTP . Sur le PIX, les événements significatifs dans un bon ordre PPTP affichent :

SCCRQ (Start-Control-Connection-Request)
SCCRP (Start-Control-Connection-Reply)
OCRQ (Outgoing-Call-Request)
OCRP (Outgoing-Call-Reply)

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

Commandes de débogage PIX

- **debug ppp E/S** — Affiche les informations de paquet pour l'interface virtuelle de PPP PPTP.
- **debug ppp error** — Les erreurs de protocole et les statistiques sur les erreurs d'affichages ont associé avec la négociation et l'exécution de connexion PPP.
- **erreur de debug vpdn** — Affiche les erreurs qui empêchent un tunnel de PPP d'être établi ou les erreurs qui causent un tunnel établi d'être fermé.
- **paquet de debug vpdn** — Erreurs et événements des affichages L2TP qui sont une partie de

l'établissement normal d'un tunnel ou un arrêt pour VPDNs.
- **événements de debug vpdn** — Affiche des messages au sujet des événements qui font partie d'établissement normal de tunnel de PPP ou arrêt.
- **uauth de debug ppp** — Affiche les messages d'élimination des imperfections d'authentification de l'utilisateur d'AAA d'interface virtuelle de PPP PPTP.

Commandes claires PIX

Cette commande doit être émise en mode de config.

- **clear vpdn tunnel [tout |** *[tunnel_id d'id]***]** — Retire un ou plusieurs tunnels PPTP de la configuration.

Attention : N'émettez pas la commande **claire de vpdn**. Ceci élimine *toutes les* commandes de vpdn.

PPP d'enable ouvrant une session le PC client

Terminez-vous ces instructions afin d'activer l'élimination des imperfections de PPP pour différents systèmes de Windows et d'exploitation Microsoft.

Windows 95

Suivez ces étapes afin d'activer le PPP ouvrant une session un ordinateur de Windows 95.

1. Dans l'option Network au panneau de configuration, **adaptateur pour circuit téléphonique commuté de Microsoft de** double clic dans la liste de composants de réseau installés.
2. Cliquez sur l'onglet **Advanced**. Dans la liste des propriétés, cliquez sur l'option nommée l'**enregistrement un fichier journal**, et dans la liste de valeurs, clic **oui**. Cliquez ensuite sur **OK**.
3. Arrêtez et redémarrez l'ordinateur pour que cette option la prenne effet. Le log est enregistré dans un fichier appelé ppplog.txt.

Windows 98

Suivez ces étapes afin d'activer le PPP ouvrant une session un ordinateur de Windows 98.

1. Dans le **réseau commuté**, cliquez une fois une icône de connexion, et puis sélectionnez le **fichier > le Properties**.
2. Cliquez sur l'onglet de types de serveur.
3. Sélectionnez l'option nommée l'**enregistrement un fichier journal pour cette connexion**. Le fichier journal se trouve chez C:\Windows\ppplog.txt

Windows 2000

Afin d'activer ouvrir une session de PPP le Windows 2000 usine, va à Microsoft la page de support et recherche le « PPP d'enable ouvrant une session Windows. »

Windows NT

Suivez ces étapes afin d'activer le PPP ouvrant une session un système NT.

1. Localisez le **SYSTÈME** principal **\ CurrentControlSet \ services \ RasMan \ PPP** et changez **en se connectant** de 0 à **1.** Ceci crée un fichier appelé PPP.Login le répertoire du <winnt root>\SYSTEM32\RAS.
2. Afin de mettre au point une session PPP, un premier enable se connectant et puis initier la connexion PPP. Quand la connexion échoue ou des sorties, examinez PPP.LOG pour voir ce qui s'est produit.

Le pour en savoir plus, se rapportent à la page de support de Microsoft et recherchent « activer le PPP ouvrant une session Windows NT. »

Questions supplémentaires de Microsoft

Plusieurs questions liées à la Microsoft pour considérer le pour le dépannage PPTP sont répertoriées ici. Des informations détaillées sont disponibles dans la Base de connaissances Microsoft avec les liens fournis.

- Comment maintenir des connexions RAS actives après fermeture de sessionLes connexions Windows RAS (Remote Access Service) sont automatiquement déconnectées lorsque vous fermez la session d'un client RAS. Vous pouvez rester connecté en activant la clé de Registre **KeepRasConnections** sur le client RAS.
- L'utilisateur n'est pas alerté en ouvrant une session avec les informations d'identification mises en cacheSi vous ouvrez une session à un domaine d'un poste de travail basé sur Windows ou le serveur membre et le contrôleur de domaine ne peuvent pas se trouvent, vous ne recevez pas un message d'erreur qui indique cette question. Au lieu de cela, vous ouvrez une session sur l'ordinateur local à l'aide des informations d'identification mises en cache.
- Procédures pour écrire un fichier LMHOSTS pour la validation de domaine et autres problèmes de résolution de nomsSi vous éprouvez des questions de résolution de noms sur votre réseau TCP/IP, vous devez utiliser des fichiers lmhosts afin de résoudre des noms NetBIOS. Vous devez suivre une procédure spécifique afin de créer un fichier lmhosts pour utiliser dans la validation de résolution de noms et de domaine.

Exemple de sortie de débogage

Debug PIX - Authentification locale

Cette sortie de débogage affiche des événements significatifs en *italique*.

```
PPTP: new peer fd is 1

Tnl 42 PPTP: Tunnel created; peer initiated PPTP:
   created tunnel, id = 42

PPTP: cc rcvdata, socket fd=1, new_conn: 1
PPTP: cc rcv 156 bytes of data

SCCRQ = Start-Control-Connection-Request - message code bytes 9 & 10 = 0001 Tnl 42 PPTP: CC I
009c00011a2b3c4d000100000100000000000010000... Tnl 42 PPTP: CC I SCCRQ Tnl 42 PPTP: protocol
version 0x100 Tnl 42 PPTP: framing caps 0x1 Tnl 42 PPTP: bearer caps 0x1 Tnl 42 PPTP: max
channels 0 Tnl 42 PPTP: firmware rev 0x0 Tnl 42 PPTP: hostname "local" Tnl 42 PPTP: vendor "9x"
Tnl 42 PPTP: SCCRQ-ok -> state change wt-sccrq to estabd SCCRP = Start-Control-Connection-Reply
```

- message code bytes 9 & 10 = 0002 Tnl 42 PPTP: CC O SCCRP PPTP: cc snddata, socket fd=1, len=156, data: 009c00011a2b3c4d0002000001000100000000030000... PPTP: cc waiting for input, max soc FD = 1 PPTP: soc select returns rd mask = 0x2 PPTP: cc rcvdata, socket FD=1, new_conn: 0 PPTP: cc rcv 168 bytes of data *OCRQ = Outgoing-Call-Request - message code bytes 9 & 10 = 0007* Tnl 42 PPTP: CC I 00a800011a2b3c4d00070000000000000000dac00000... Tnl 42 PPTP: CC I OCRQ Tnl 42 PPTP: call id 0x0 Tnl 42 PPTP: serial num 0 Tnl 42 PPTP: min bps 56000:0xdac0 Tnl 42 PPTP: max bps 64000:0xfa00 Tnl 42 PPTP: bearer type 3 Tnl 42 PPTP: framing type 3 Tnl 42 PPTP: recv win size 16 Tnl 42 PPTP: ppd 0 Tnl 42 PPTP: phone num Len 0 Tnl 42 PPTP: phone num "" Tnl/Cl 42/42 PPTP: l2x store session: tunnel id 42, session id 42, hash_ix=42 PPP virtual access open, ifc = 0 Tnl/Cl 42/42 PPTP: vacc-ok -> state change wt-vacc to estabd *OCRP = Outgoing-Call-Reply - message code bytes 9 & 10 = 0008* Tnl/Cl 42/42 PPTP: CC O OCRP PPTP: cc snddata, socket FD=1, Len=32, data: 002000011a2b3c4d00080000002a00000100000000fa... *!--- Debug following this last event is flow of packets.* PPTP: cc waiting for input, max soc FD = 1 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 39, seq 1 PPP rcvd, ifc = 0, pppdev: 1, Len: 27, data: ff03c021010100170206000a00000506001137210702... PPP xmit, ifc = 0, Len: 23 data: ff03c021010100130305c22380050609894ab407020802 Interface outside - PPTP xGRE: Out paket, PPP Len 23 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 39, seq 1, ack 1, data: 3081880b00170000000000010000000 1ff03c0210101... PPP xmit, ifc = 0, Len: 17 data: ff03c0210401000d0206000a00000d0306 Interface outside - PPTP xGRE: Out paket, PPP Len 17 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 33, seq 2, ack 1, data: 3081880b00110000000000020000000 1ff03c0210401... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 39, seq 2, ack 1 PPP rcvd, ifc = 0, pppdev: 1, Len: 23, data: ff03c021020100130305c22380050609894ab407020802 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 34, seq 3, ack 2 PPP rcvd, ifc = 0, pppdev: 1, Len: 18, data: ff03c0210102000e05060011372107020802 PPP xmit, ifc = 0, Len: 18 data: ff03c0210202000e05060011372107020802 Interface outside - PPTP xGRE: Out paket, PPP Len 18 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 34, seq 3, ack 3, data: 3081880b00120000000000030000000 3ff03c0210202... PPP xmit, ifc = 0, Len: 17 data: ff03c2230101000d08d36602863630eca8 Interface outside - PPTP xGRE: Out paket, PPP Len 15 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 31, seq 4, ack 3, data: 3081880b000f0000000000400000003c2230101000d... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 76, seq 4, ack 4 PPP rcvd, ifc = 0, pppdev: 1, Len: 62, data: ff03c2230201003a31d4d0a397a064668bb00d954a85... PPP xmit, ifc = 0, Len: 8 data: ff03c22303010004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 22, seq 5, ack 4, data: 3081880b00060000000000005000000 04c22303010004 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 58, seq 5, ack 5 PPP rcvd, ifc = 0, pppdev: 1, Len: 44, data: ff038021010100280206002d0f010306000000008106... PPP xmit, ifc = 0, Len: 14 data: ff0380210101000a030663636302 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 28, seq 6, ack 5, data: 3081880b000c0000000000060000000 5802101010 00a... PPP xmit, ifc = 0, Len: 38 data: ff038021040100220206002d0f018106000000008206... Interface outside - PPTP xGRE: Out paket, PPP Len 36 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 52, seq 7, ack 5, data: 3081880b00240000000000070000000 5802104010022... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 29, seq 6 PPP rcvd, ifc = 0, pppdev: 1, Len: 19, data: ff0380fd0101000f1206010000011105000104 PPP xmit, ifc = 0, Len: 8 data: ff0380fd01010004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 22, seq 8, ack 6, data: 3081880b00060000000000008000000 0680fd01010004 PPP xmit, ifc = 0, Len: 19 data: ff0380fd0401000f1206010000011105000104 Interface outside - PPTP xGRE: Out paket, PPP Len 17 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 33, seq 9, ack 6, data: 3081880b00110000000000090000000 680fd0401000f... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 28, seq 7, ack 6 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210201000a030663636302 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 22, seq 8, ack 8 PPP rcvd, ifc = 0, pppdev: 1, Len: 8, data: ff0380fd02010004 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 22, seq 9, ack 9 PPP rcvd, ifc = 0, pppdev: 1, Len: 8, data: ff0380fd01020004 PPP xmit, ifc = 0, Len: 8 data: ff0380fd02020004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 22, seq 10, ack 9, data: 3081880b00060000000000000a0000000 980fd02020004 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 22, seq 10, ack 10 PPP rcvd, ifc = 0, pppdev: 1, Len: 8, data: ff0380fd05030004 PPP xmit, ifc = 0, Len: 8 data: ff0380fd06030004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 22, seq 11, ack 10, data: 3081880b00060000000000000b0000000 a80fd06030004 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 48, seq 11 PPP rcvd, ifc = 0, pppdev: 1, Len: 38, data: ff038021010200220306000000008106000000008206... PPP xmit, ifc = 0, Len: 32 data: ff0380210402001c810600000000820600000000 8306... Interface outside - PPTP xGRE: Out paket, PPP Len 30 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 46, seq 12, ack 11, data:

```
3081880b001e00000000000c0000000b80210402001c... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 28, seq 12, ack 12 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210103000a030600000000
PPP xmit, ifc = 0, Len: 14 data: ff0380210303000a0306ac100101 Interface outside - PPTP xGRE: Out
paket, PPP Len 12 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 28, seq 13, ack 12, data:
3081880b000c00000000000d0000000c80210303000a... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 28, seq 13, ack 13 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210104000a0306ac100101
PPP xmit, ifc = 0, Len: 14 data: ff0380210204000a0306ac100101 Interface outside - PPTP xGRE: Out
paket, PPP Len 12 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 28, seq 14, ack 13, data:
3081880b000c00000000000e0000000d80210204000a... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 41, seq 14 PPP rcvd, ifc = 0, pppdev: 1, Len: 32, data:
ff0300214500001cc80000008001e5ccac100101e000... PPP IP Pkt:
4500001cc80000008001e5ccac100101e00000020a00... 603104: PPTP Tunnel created, tunnel_id is 42,
remote_peer_ip is 99.99.99.5 ppp_virtual_interface_id is 1, client_dynamic_ip is 172.16.1.1
username is john, MPPE_key_strength is None outside PPTP: Recvd xGRE pak from 99.99.99.5, Len
109, seq 15 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060ca0000008011176bac100101ac10... PPP IP Pkt:
45000060ca0000008011176bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 16 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060cb0000008011166bac100101ac10... PPP IP Pkt:
45000060cb0000008011166bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 17 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060cc0000008011156bac100101ac10... PPP IP Pkt:
45000060cc0000008011156bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 18 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060d000000008011116bac100101ac10... PPP IP Pkt:
45000060d000000008011116bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 19 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060d200000080110f6bac100101ac10... PPP IP Pkt:
45000060d200000080110f6bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 20 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060d300000080110e6bac100101ac10... PPP IP Pkt:
45000060d300000080110e6bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 41, seq 21 PPP rcvd, ifc = 0, pppdev: 1, Len: 32, data:
ff0300214500001cd60000008001d7ccac100101e000... PPP IP Pkt:
4500001cd60000008001d7ccac100101e00000020a00... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 22 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060d800000008011096bac100101ac10... PPP IP Pkt:
45000060d800000008011096bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 23 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060da0000008011076bac100101ac10... PPP IP Pkt:
45000060da0000008011076bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 24 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060db0000008011066bac100101ac10... PPP IP Pkt:
45000060db0000008011066bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 25 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060de0000008011036bac100101ac10... PPP IP Pkt:
45000060de0000008011036bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 26 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060e000000008011016bac100101ac10... PPP IP Pkt:
45000060e000000008011016bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 27 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060e100000008011006bac100101ac10... PPP IP Pkt:
45000060e100000008011006bac100101ac10ffff0089... inside:172.16.255.255/137 outside PPTP: Recvd
xGRE pak from 99.99.99.5, Len 41, seq 28 PPP rcvd, ifc = 0, pppdev: 1, Len: 32, data:
ff0300214500001ce40000008001c9ccac100101e000... PPP IP Pkt:
4500001ce40000008001c9ccac100101e00000020a00...
```

Authentification de debug radius PIX

Cette sortie de débogage affiche des événements significatifs en *italique*.

```
PIX#terminal monitor PIX# 106011: Deny inbound (No xlate) icmp src outside:172.17.194.164 dst
outside:172.18.124.201 (type 8, code 0) 106011: Deny inbound (No xlate) icmp src
```

outside:172.17.194.164 DST outside:172.18.124.201 (type 8, code 0) PIX# PPTP: soc select returns rd mask = 0x1 PPTP: new peer FD is 1 Tnl 9 PPTP: Tunnel created; peer initiatedPPTP: created tunnel, id = 9 PPTP: cc rcvdata, socket FD=1, new_conn: 1 PPTP: cc rcv 156 bytes of data *SCCRQ = Start-Control-Connection-Request - message code bytes 9 & 10 = 0001* Tnl 9 PPTP: CC I 009c00011a2b3c4d000100000100000000000010000... Tnl 9 PPTP: CC I SCCRQ Tnl 9 PPTP: protocol version 0x100 Tnl 9 PPTP: framing caps 0x1 Tnl 9 PPTP: bearer caps 0x1 Tnl 9 PPTP: max channels 0 Tnl 9 PPTP: firmware rev 0x870 Tnl 9 PPTP: hostname "" Tnl 9 PPTP: vendor "Microsoft Windows NT" Tnl 9 PPTP: SCCRQ-ok -> state change wt-sccrq to estabd *SCCRP = Start-Control-Connection-Reply - message code bytes 9 & 10 = 0002* Tnl 9 PPTP: CC O SCCRP PPTP: cc snddata, socket FD=1, Len=156, data: 009c00011a2b3c4d000200000100010000000000030000... PPTP: cc waiting for input, max soc FD = 1 PPTP: soc select returns rd mask = 0x2 PPTP: cc rcvdata, socket FD=1, new_conn: 0 PPTP: cc rcv 168 bytes of data *OCRQ = Outgoing-Call-Request - message code bytes 9 & 10 = 0007* Tnl 9 PPTP: CC I 00a800011a2b3c4d000700004000e4f50000012c05f5... Tnl 9 PPTP: CC I OCRQ Tnl 9 PPTP: call id 0x4000 Tnl 9 PPTP: serial num 58613 Tnl 9 PPTP: min bps 300:0x12c Tnl 9 PPTP: max BPS 100000000:0x5f5e100 Tnl 9 PPTP: bearer type 3 Tnl 9 PPTP: framing type 3 Tnl 9 PPTP: recv win size 64 Tnl 9 PPTP: ppd 0 Tnl 9 PPTP: phone num Len 0 Tnl 9 PPTP: phone num "" Tnl/Cl 9/9 PPTP: l2x store session: tunnel id 9, session id 9, hash_ix=9 PPP virtual access open, ifc = 0 Tnl/CL 9/9 PPTP: vacc-ok -> state change wt-vacc to estabd *OCRP = Outgoing-Call-Reply - message code bytes 9 & 10 = 0008* Tnl/CL 9/9 PPTP: CC O OCRP PPTP: cc snddata, socket FD=1, Len=32, data: 002000011a2b3c4d000800000009400001000000000fa... PPTP: cc waiting for input, max soc FD = 1 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 60, seq 0 PPP rcvd, ifc = 0, pppdev: 1, Len: 48, data: ff03c0210100002c0506447e217e070208020d030611... PPP xmit, ifc = 0, Len: 23 data: ff03c021010100130305c2238005065a899b2307020802 Interface outside - PPTP xGRE: Out paket, PPP Len 23 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 39, seq 1, ack 0, data: 3081880b00174000000000010000000ff03c0210101... PPP xmit, ifc = 0, Len: 38 data: ff03c021040000220d03061104064e131701beb613cb.. . Interface outside - PPTP xGRE: Out paket, PPP Len 38 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 54, seq 2, ack 0, data: 3081880b00264000000000002000000000ff03c0210400... PPTP: soc select returns rd mask = 0x2 PPTP: cc rcvdata, socket FD=1, new_conn: 0 PPTP: cc rcv 24 bytes of data Tnl 9 PPTP: CC I 001800011a2b3c4d000f0000000900000fffffffffffff... Tnl/CL 9/9 PPTP: CC I SLI PPTP: cc waiting for input, max soc FD = 1 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 39, seq 1, ack 1 PPP rcvd, ifc = 0, pppdev: 1, Len: 23, data: ff03c021020100130305c2238005065a899b2307020802 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 34, seq 2, ack 2 PPP rcvd, ifc = 0, pppdev: 1, Len: 18, data: ff03c0210101000e0506447e217e07020802 PPP xmit, ifc = 0, Len: 18 data: ff03c0210201000e0506447e217e07020802 Interface outside - PPTP xGRE: Out paket, PPP Len 18 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 34, seq 3, ack 2, data: 3081880b00124000000000030000000 2ff03c0210201... PPP xmit, ifc = 0, Len: 17 data: ff03c2230101000d08f3686cc47e37ce67 Interface outside - PPTP xGRE: Out paket, PPP Len 15 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 31, seq 4, ack 2, data: 3081880b000f4000000000400000002c2230101000d... outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 36, seq 3, ack 3 PPP rcvd, ifc = 0, pppdev: 1, Len: 22, data: ff03c0210c020012447e217e4d5352415356352e3030 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 45, seq 4 PPP rcvd, ifc = 0, pppdev: 1, Len: 35, data: ff03c0210c03001f447e217e4d535241532d312d4349... PPTP: soc select returns rd mask = 0x2 PPTP: cc rcvdata, socket FD=1, new_conn: 0 PPTP: cc rcv 24 bytes of data Tnl 9 PPTP: CC I 001800011a2b3c4d000f0000000900000000000000000... Tnl/CL 9/9 PPTP: CC I SLI PPTP: cc waiting for input, max soc FD = 1 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 76, seq 5, ack 4 PPP rcvd, ifc = 0, pppdev: 1, Len: 62, data: ff03c2230201003a3100000000000000000000000000000... uauth_mschap_send_req: pppdev=1, ulen=4, user=john 6031 uauth_mschap_proc_reply: pppdev = 1, status = 1 PPP xmit, ifc = 0, Len: 8 data: ff03c22303010004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 22, seq 5, ack 5, data: 3081880b000640000000000500000005c22303010004 CHAP peer authentication succeeded for john outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 72, seq 6 PPP rcvd, ifc = 0, pppdev: 1, Len: 62, data: ff03c2230201003a3100000000000000000000000000000... PPP xmit, ifc = 0, Len: 8 data: ff03c22303010004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 22, seq 6, ack 6, data: 3081880b000640000000000600000006c22303010004 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 7, ack 5 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380fd0104000a120601000001 PPP xmit, ifc = 0, Len: 14 data: ff0380fd0101000a120601000020 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 7, ack 7, data: 3081880b000c4000000000070000000780fd0101000a... PPP xmit, ifc = 0, Len: 14 data: ff0380fd0304000a120601000020 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 8, ack 7, data: 3081880b000c4000000000080000000780fd0304000a... outside PPTP: Recvd xGRE pak from 10.44.17.104,

Len 48, seq 8 PPP rcvd, ifc = 0, pppdev: 1, Len: 38, data:
ff038021010500220306000000008106000000008206... PPP xmit, ifc = 0, Len: 14 data:
ff0380210101000a0306ac127c98 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP:
Sending xGRE pak to 10.44.17.104, Len 28, seq 9, ack 8, data:
3081880b000c40000000000900000080210101000a... PPP xmit, ifc = 0, Len: 32 data:
ff0380210405001c810600000000820600000000008306.. . Interface outside - PPTP xGRE: Out paket, PPP
Len 30 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 46, seq 10, ack 8, data:
3081880b001e40000000000a0000000880210405001c... outside PPTP: Recvd xGRE pak from 10.44.17.104,
Len 28, seq 9, ack 7 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380fd0201000a120601000020
outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 10, ack 8 PPP rcvd, ifc = 0, pppdev:
1, Len: 14, data: ff0380fd0106000a120601000020 PPP xmit, ifc = 0, Len: 14 data:
ff0380fd0206000a120601000020 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP:
Sending xGRE pak to 10.44.17.104, Len 28, seq 11, ack 10, data:
3081880b000c40000000000b0000000a80fd0206000a... outside PPTP: Recvd xGRE pak from 10.44.17.104,
Len 28, seq 11, ack 9 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210201000a0306ac127c98
outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 12, ack 10 PPP rcvd, ifc = 0,
pppdev: 1, Len: 14, data: ff0380210107000a030600000000 PPP xmit, ifc = 0, Len: 14 data:
ff0380210307000a0306c0a80101 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP:
Sending xGRE pak to 10.44.17.104, Len 28, seq 12, ack 12, data:
3081880b000c40000000000c0000000c80210307000a... outside PPTP: Recvd xGRE pak from 10.44.17.104,
Len 24, seq 13 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210108000a030600000000 PPP
xmit, ifc = 0, Len: 14 data: ff0380210308000a0306c0a80101 Interface outside - PPTP xGRE: Out
paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 13, ack 13, data:
3081880b000c40000000000d0000000d80210308000a... 0 outside PPTP: Recvd xGRE pak from
10.44.17.104, Len 28, seq 14, ack 13 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data:
ff0380210109000a0306c0a80101 PPP xmit, ifc = 0, Len: 14 data: ff0380210209000a0306c0a80101
Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to
10.44.17.104, Len 28, seq 14, ack 14, data: 3081880b000c40000000000e0000000e80210209000a... 2:
PPP virtual interface 1 - user: john aaa authentication started 603103: PPP virtual interface 1
- user: john aaa authentication succeed 109011: Authen Session Start: user 'joh outside PPTP:
Recvd xGRE pak from 10.44.17.104, Len 117, seq 15, ack 14 PPP rcvd, ifc = 0, pppdev: 1, Len:
104, data: ff0300fd9000bccf59b71755d9af7330dae3bbc94d28... PPP Encr/Comp Pkt:
9000bccf59b71755d9af7330dae3bbc94d28e431d057... PPP IP Pkt:
4500006002bb000080117629c0a80101ffffffff0089... n', sid 3 603104: PPTP Tunnel created, tunnel_id
is 9, remote_peer_ip is 10.44.17.104 ppp_virtual_interface_id is 1, client_dynamic_ip is
192.168.1.1 username is john, MPPE_key_strength is 40 bits outside PPTP: Recvd xGRE pak from
10.44.17.104, Len 113, seq 16 PPP rcvd, ifc = 0, pppdev: 1, Len: 104, data:
ff0300fd9001f8348351ef9024639ed113b43adfeb44... PPP Encr/Comp Pkt:
9001f8348351ef9024639ed113b43adfeb4489af5ab3... PPP IP Pkt:
4500006002bd000080117627c0a80101ffffffff0089... ide outside PPTP: Recvd xGRE pak from
10.44.17.104, Len 113, seq 17 PPP rcvd, ifc = 0, pppdev: 1, Len: 104, data:
ff0300fd9002cc73cd65941744a1cf30318cc4b4b783... PPP Encr/Comp Pkt:
9002cc73cd65941744a1cf30318cc4b4b783e825698a... PPP IP Pkt:
4500006002bf000080117625c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 18 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd9003aaa545eaeeda0f82b5999e2fa9ba3245... PPP Encr/Comp Pkt:
9003aaa545eaeeda0f82b5999e2fa9ba324585a1bc8d... PPP IP Pkt:
4500006002c1000080117623c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 19 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd90045b35d080900ab4581e64706180e3540e... PPP Encr/Comp Pkt:
90045b35d080900ab4581e64706180e3540ee15d664a... PPP IP Pkt:
4500006002c3000080117621c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 20 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd90052878b256edbd17b42f2cb672ba80b40a... PPP Encr/Comp Pkt:
90052878b256edbd17b42f2cb672ba80b40a79760cef... PPP IP Pkt:
4500006002c500080011761fc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 21 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900632359a2c07e79106c5e282e3892e60de... PPP Encr/Comp Pkt:
900632359a2c07e79106c5e282e3892e60ded6c6d4d1... PPP IP Pkt:
4500006002c700008011761dc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 22 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd90070ca6ea48b2ad26987d52a4e109ca68b6... PPP Encr/Comp Pkt:
90070ca6ea48b2ad26987d52a4e109ca68b6758569d3... PPP IP Pkt:
4500006002c900008011761bc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,

```
len 113, seq 23 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd90085aba60edf57e50eea4d523596cb9d690... PPP Encr/Comp Pkt:
90085aba60edf57e50eea4d523596cb9d69057715894... PPP IP Pkt:
4500006002cb000080117619c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 24 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd90094b73b6c962272b60d32f135b5f29f2a5... PPP Encr/Comp Pkt:
90094b73b6c962272b60d32f135b5f29f2a58bacd050... PPP IP Pkt:
4500006002cc000080117618c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 345, seq 25 PPP rcvd, ifc = 0, pppdev: 1, len: 336, data:
ff0300fd900a86307ed9537df5389ea09223d62c20fd... PPP Encr/Comp Pkt:
900a86307ed9537df5389ea09223d62c20fd9e34072f... PPP IP Pkt:
4500014802cf00008011752dc0a80101ffffffff0044... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 26 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900b45303a5fe7b2dc3f62db739b4bb1b802... PPP Encr/Comp Pkt:
900b45303a5fe7b2dc3f62db739b4bb1b80253278fad... PPP IP Pkt:
4500006002d1000080117613c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 27 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900ceb5aaaecc832df3c12bc6c519c25b4db... PPP Encr/Comp Pkt:
900ceb5aaaecc832df3c12bc6c519c25b4dba569d10... PPP IP Pkt:
4500006002d2000080117612c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 28 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900dbdaaf071c2bd1c92c1f56085813d1a77... PPP Encr/Comp Pkt:
900dbdaaf071c2bd1c92c1f56085813d1a778cc61c29... PPP IP Pkt:
4500006002d500008011760fc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 29 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900e97de47036d95a0721ef6b28479b8efde... PPP Encr/Comp Pkt:
900e97de47036d95a0721ef6b28479b8efde8e16b398... PPP IP Pkt:
4500006002d600008011760ec0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 30 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900f75bf4c8cbcf11464bf52bd7f6155c7d6... PPP Encr/Comp Pkt:
900f75bf4c8cbcf11464bf52bd7f6155c7d62ea2ca5e... PPP IP Pkt:
4500006002d900008011760bc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 31 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd9010f221e7ba169702765529e4ffa368dba5... PPP Encr/Comp Pkt:
9010f221e7ba169702765529e4ffa368dba5610921ae... PPP IP Pkt:
4500006002da00008011760ac0a80101ffffffff0089... from (192.168.1.1) to 255.255.255.255 on
interface outside outside PPTP: Recvd xGRE pak from 10.44.17.104, len 231, seq 32 PPP rcvd, ifc
= 0, pppdev: 1, len: 222, data: ff0300fd9011c23a03921c1e10ccc38847cb8056fa93... PPP Encr/Comp
Pkt: 9011c23a03921c1e10ccc38847cb8056fa9387018912... PPP IP Pkt:
450000d602dd000080117591c0a80101ffffffff008a... side outside PPTP: Recvd xGRE pak from
10.44.17.104, len 345, seq 33 PPP rcvd, ifc = 0, pppdev: 1, len: 336, data:
ff0300fd90127d7213f35cd1d82d8988e28e0930ecc1... PPP Encr/Comp Pkt:
90127d7213f35cd1d82d8988e28e0930ecc104a993f... PPP IP Pkt:
4500014802df00008011751dc0a80101ffffffff0044...
```

Causes de problèmes potentiels

Tunnel simultané PPTP

Vous ne pouvez pas connecter plus de 127 connexions à PIX 6.x, et ce message d'erreur apparaît :

%PIX-3-213001 : Le socket E/S de démon de contrôle PPTP reçoivent l'erreur, errno = 5

Solution :

Il y a une limitation matérielle de 128 sessions simultanées dans PIX 6.x. Si vous soustrayez un pour le socket de écoute PPTP, les connexions du nombre maximal is127.

PIX et PC ne peuvent pas négocier l'authentification

Les Protocoles d'authentification PC sont placés pour ceux que le PIX ne peut pas faire version 2 (MS-CHAP v.2) de CHAP protocole d'identification de mot de passe ((SPAP) et de Microsoft de Shiva au lieu de version 1). Le PC et les PIX ne peuvent pas convenir sur l'authentification. Le PC affiche ce message :

```
Disconnected - Error 732: Your computer and the remote computer
    could not agree on PPP control protocols
```

PIX et PC ne peuvent pas négocier le cryptage

Le PC est placé pour **Encrypted seulement** et le **groupe 1 de vpdn que le ppp encrypt mppe 40 a exigé la** commande est supprimé du PIX. Le PC et les PIX ne peuvent pas convenir sur le cryptage et le PC affiche ce message :

```
Error 742 : The remote computer does not support the required
    data encryption type.
```

PIX et PC ne peuvent pas négocier le cryptage

Le PIX est placé pour le **ppp encrypt mppe 40 exigé** et le PC du **groupe 1 de vpdn** pour aucun cryptage permis. Ceci ne produit aucun message sur le PC, mais les débranchements de session et les PIX mettent au point des expositions cette sortie :

```
PPTP: Call id 8, no session id protocol: 21,
    reason: mppe required but not active, tunnel terminated
603104: PPTP Tunnel created, tunnel_id is 8,
    remote_peer_ip is 10.44.17.104
ppp_virtual_interface_id is 1, client_dynamic_ip is 192.168.1.1
username is cisco, MPPE_key_strength is None
603105: PPTP Tunnel deleted, tunnel_id = 8,
    remote_peer_ip = 10.44.17.104
```

Problème de RAYON PIX MPPE

Le PIX est placé pour le **ppp encrypt mppe 40 du groupe 1 de vpdn exigé** et le PC pour le cryptage permis avec l'authentification à un serveur de RAYON ne renvoie pas la clé MPPE. Le PC affiche ce message :

```
Error 691: Access was denied because the username
    and/or password was invalid on the domain.
```

Les PIX mettent au point des expositions :

```
2: PPP virtual interface 1 -
   user: cisco  aaa authentication started
603103: PPP virtual interface 1 -
   user: cisco  aaa authentication failed
403110: PPP virtual interface 1,
   user: cisco missing MPPE key from aaa server
603104: PPTP Tunnel created,
   tunnel_id is 15,
   remote_peer_ip is 10.44.17.104
   ppp_virtual_interface_id is 1,
   client_dynamic_ip is 0.0.0.0
   username is Unknown,
   MPPE_key_strength is None
603105: PPTP Tunnel deleted,
   tunnel_id = 15,
   remote_peer_ip = 10.44.17.104
```

Le PC affiche ce message :

```
Error 691: Access was denied because the username
    and/or password was invalid on the domain.
```

Informations connexes

- 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)
- Solutions de dépannage les plus fréquentes concernant un VPN IPsec LAN à LAN et d'accès à distance
- Page de support PPTP
- RFC 2637 : Protocole de tunnellisation point à point (PPTP)
- Demandes de commentaires (RFC)
- Support technique - Cisco Systems