Configuration du pare-feu PIX et des clients VPN à l'aide de PPTP, MPPE et IPSec

Contenu

Introduction

Dans cet exemple de configuration, quatre différents types de clients connectent et chiffrent le trafic en se servant du pare-feu Cisco Secure PIX comme terminal de tunnel :

- Utilisateurs qui exécutent Cisco Secure VPN Client 1.1 sous Microsoft Windows 95/98/NT
- Utilisateurs qui exécutent Cisco Secure VPN 3000 Client 2.5.x sous Windows 95/98/NT
- Utilisateurs qui exécutent des clients PPTP (Point-to-Point Tunneling Protocol) Windows 98/2000/XP natifs
- Utilisateurs qui exécutent le client VPN Cisco 3.x/4.x sous Windows 95/98/NT/2000/XP

Dans cet exemple, un pool unique pour IPsec et PPTP est configuré. En revanche, les piscines peuvent être séparées.

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 PIX version 6.3.3
- Client VPN sécurisé Cisco 1.1
- Client VPN Cisco 3000 version 2.5
- Client VPN Cisco 3.x et 4.x
- Clients Microsoft Windows 2000 et Windows 98

Note : Ceci a été testé sur le logiciel PIX version 6.3.3 mais devrait fonctionner sur les versions 5.2.x et 5.3.1. Le logiciel PIX version 6.x est requis pour les clients VPN Cisco 3.x et 4.x. (La prise en charge du client Cisco VPN 3000 2.5 est ajoutée dans le logiciel PIX version 5.2.x. La configuration fonctionne également pour le logiciel PIX version 5.1.x, à l'exception de la partie Client VPN Cisco 3000.) IPsec et PPTP/Microsoft Point-to-Point Encryption (MPPE) doivent fonctionner séparément en premier. S'ils ne travaillent pas séparément, ils ne travaillent pas ensemble.

Remarque : PIX 7.0 utilise la commande **inspect rpc** pour gérer les paquets RPC. La commande **inspect sunrpc** active ou désactive l'inspection d'application pour le protocole Sun RPC. Les services RPC Sun peuvent s'exécuter sur n'importe quel port du système. Lorsqu'un client tente d'accéder à un service RPC sur un serveur, il doit savoir sur quel port ce service particulier s'exécute. Pour ce faire, il interroge le processus portmapper sur le port bien connu numéro 111. Le client envoie le numéro de programme RPC du service et récupère le numéro de port. À partir de ce point, le programme client envoie ses requêtes RPC à ce nouveau port.

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.

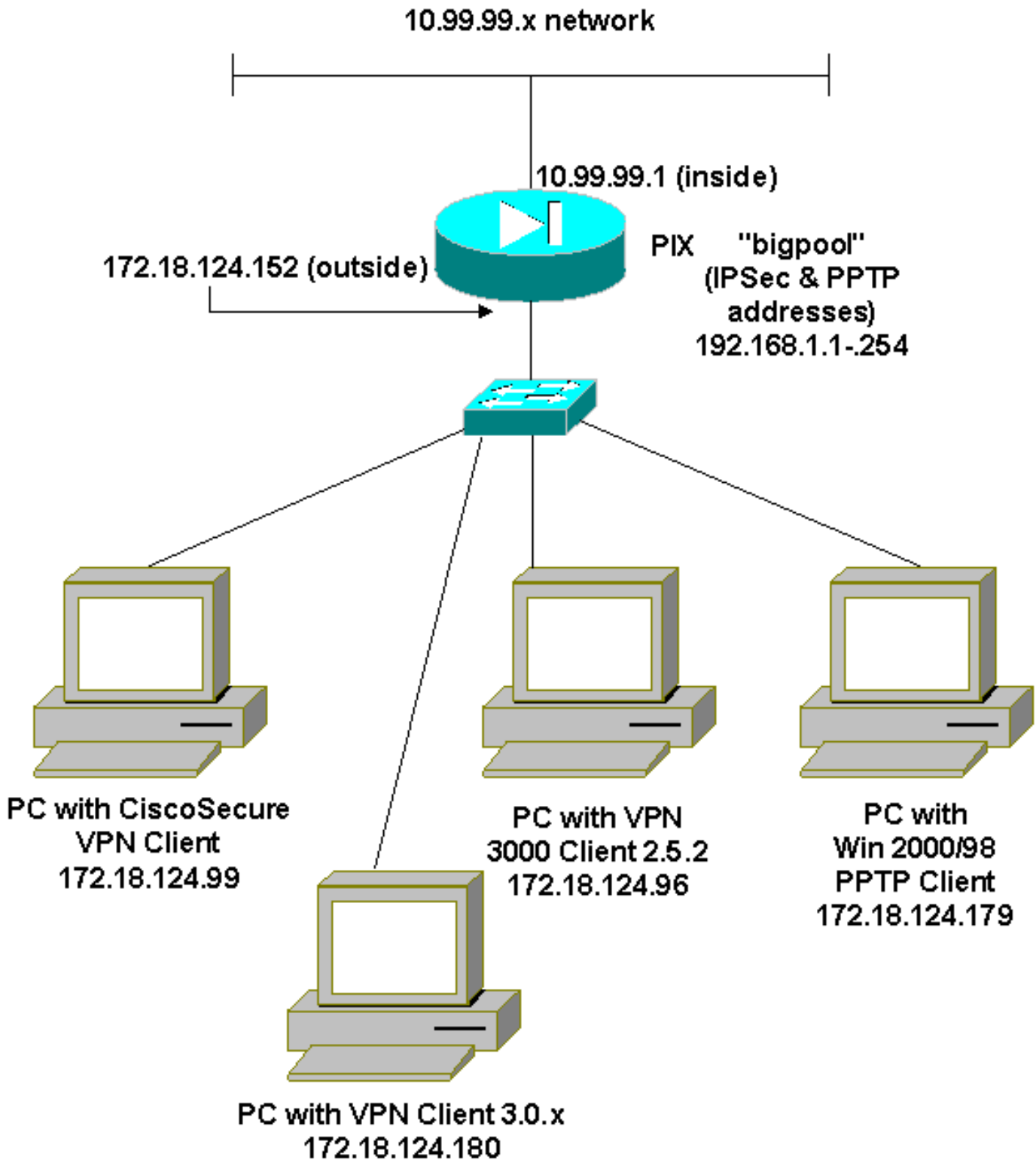
Configuration

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

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

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



Configurations

Ce document utilise les configurations suivantes.

- Pare-feu Cisco Secure PIX Firewall
- Client VPN sécurisé Cisco 1.1

Pare-feu Cisco Secure PIX Firewall
`PIX Version 6.3(3)` `interface ethernet0 auto`

```
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname goss-515A
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
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
names
access-list 101 permit ip 10.99.99.0 255.255.255.0
192.168.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.152 255.255.255.0
ip address inside 10.99.99.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool bigpool 192.168.1.1-192.168.1.254
pdm history enable
arp timeout 14400
nat (inside) 0 access-list 101
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
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
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
sysopt connection permit-pptp
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap interface outside
isakmp enable outside
!--- Cisco Secure_VPNClient_key. isakmp key ********
address 0.0.0.0 netmask 0.0.0.0
isakmp identity address
isakmp client configuration address-pool local bigpool
outside

!--- ISAKMP Policy for Cisco VPN Client 2.5 or !---
Cisco Secure VPN Client 1.1. isakmp policy 10
authentication pre-share
```

```
isakmp policy 10 encryption des
isakmp policy 10 hash md5

!--- The 1.1 and 2.5 VPN Clients use Diffie-Hellman (D-
H) !--- group 1 policy (PIX default). isakmp policy 10
group 1
isakmp policy 10 lifetime 86400

!--- ISAKMP Policy for VPN Client 3.0 and 4.0. isakmp
policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5

!--- The 3.0/4.0 VPN Clients use D-H group 2 policy !---
and PIX 6.0 code. isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
vpngroup vpn3000-all address-pool bigpool
vpngroup vpn3000-all dns-server 10.99.99.99
vpngroup vpn3000-all wins-server 10.99.99.99
vpngroup vpn3000-all default-domain password
vpngroup vpn3000-all idle-time 1800

!--- VPN 3000 group_name and group_password. vpngroup
vpn3000-all password ********
telnet timeout 5
ssh timeout 5
console timeout 0
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 ppp encryption mppe auto
vpdn group 1 client configuration address local bigpool
vpdn group 1 pptp echo 60
vpdn group 1 client authentication local

!--- PPTP username and password. vpdn username cisco
password *********
vpdn enable outside
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
goss-515A#
```

Client VPN sécurisé Cisco 1.1

```
1- TACconn
      My Identity
           Connection security: Secure
           Remote Party Identity and addressing
           ID Type: IP subnet
           10.99.99.0
            255.255.255.0
           Port all Protocol all

      Connect using secure tunnel
           ID Type: IP address
           172.18.124.152

      Pre-shared Key=CiscoSecure_VPNClient_key

      Authentication (Phase 1)
      Proposal 1
```

```
          Authentication method: pre-shared key
          Encryp Alg: DES
          Hash Alg: MD5
          SA life: Unspecified
          Key Group: DH 1

     Key exchange (Phase 2)
     Proposal 1
          Encapsulation ESP
          Encrypt Alg: DES
          Hash Alg: MD5
          Encap: tunnel
          SA life: Unspecified
          no AH

  2- Other Connections
        Connection security: Non-secure
        Local Network Interface
          Name: Any
          IP Addr: Any
          Port: All
```

Client VPN Cisco 3000 2.5.x ou Client VPN Cisco 3.x et 4.x

Sélectionnez **Options** > **Propriétés** > **Authentification**. Le nom de groupe et le mot de passe de groupe correspondent au nom de groupe et au mot de passe de groupe sur le PIX comme dans :

```
vpngroup vpn3000-all password ********
Host-name = 172.18.124.152
```

Configuration du client PPTP Windows 98/2000/XP

Vous pouvez contacter le fournisseur qui crée le client PPTP. Référez-vous à Comment configurer le pare-feu Cisco Secure PIX Firewall pour utiliser PPTP pour plus d'informations sur la façon de configurer ceci.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

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

Dépannage des commandes

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

Débogage IPsec PIX

- **debug crypto ipsec — affiche les négociations IPsec de la Phase 2.**
- **debug crypto isakmp** - Affiche les négociations ISAKMP (Internet Security Association and Key Management Protocol) de la phase 1.
- **debug crypto engine : Cette commande affiche le trafic chiffré.**

Débogage PPTP PIX

- **debug ppp io** : affiche les informations de paquet pour l'interface virtuelle PPP PPTP.
- **debug ppp error** - Affiche les messages d'erreur de l'interface virtuelle PPP PPTP.
- **debug vpdn error** - Affiche les messages d'erreur du protocole PPTP.
- **debug vpdn packets** —Affiche les informations de paquet PPTP sur le trafic PPTP.
- **debug vpdn events** - Affiche les informations de modification d'événement de tunnel PPTP.
- **debug ppp uauth** - Affiche les messages de débogage de l'authentification utilisateur AAA de l'interface virtuelle PPP PPTP.

Problèmes liés à Microsoft

- Comment maintenir des connexions RAS actives après fermeture de session : lorsque vous vous déconnectez d'un client Windows Remote Access Service (RAS), toutes les connexions RAS sont automatiquement déconnectées. Afin de rester connecté après votre déconnexion, activez la clé KeepRasConnections dans le Registre sur le client RAS.
- L'utilisateur n'est pas alerté en ouvrant une session avec les informations d'identification mises en cache —Symptômes : lorsque vous tentez de vous connecter à un domaine à partir d'une station de travail Windows ou d'un serveur membre et qu'un contrôleur de domaine est introuvable, aucun message d'erreur ne s'affiche. 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 noms —Il peut y avoir des cas où vous rencontrez des problèmes de résolution de noms sur votre réseau TCP/IP et que vous devez utiliser des fichiers Lmhosts pour résoudre des noms NetBIOS. Cet article traite de la méthode appropriée de création d'un fichier Lmhosts pour faciliter la résolution de noms et la validation de domaine.

Informations connexes

- Pages de support des protocoles IPsec Negotiation/IKE
- Référence des commandes PIX
- Page de support pour serveurs de sécurité de la gamme Cisco PIX 500
- Demandes de commentaires (RFC)
- Configuration de la sécurité des réseaux IPSec
- Configuration du protocole IKE (Internet Key Exchange)
- Support et documentation techniques - Cisco Systems