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

Dans cet exemple, un seul pool pour IPsec et PPTP est configuré. Cependant, les groupes peuvent également être rendus distincts.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Version du logiciel PIX 6.3.3
- Cisco Secure VPN Client 1.1
- Version 2.5 de Cisco VPN 3000 Client
- Client VPN Cisco 3.x et 4.x
- Clients de Microsoft Windows 2000 et de Windows 98

Remarque: Ceci a été testé sur la version du logiciel PIX 6.3.3 mais devrait travailler à la version 5.2.x et 5.3.1. La version du logiciel PIX 6.x est exigée pour le Client VPN Cisco 3.x et 4.x. (Le soutien du Cisco VPN 3000 Client 2.5 est ajouté dans la version du logiciel PIX 5.2.x. La configuration fonctionne également pour la version du logiciel PIX 5.1.x, excepté la cloison de Cisco VPN 3000 Client) IPsec et le chiffrement point par point PPTP/Microsoft (MPPE) devrait être fait fonctionner séparément d'abord. S'ils ne fonctionnent pas séparément, ils ne fonctionnent pas ensemble.

Remarque: PIX 7.0 utilise la commande **RPC d'examiner** de manipuler des paquets RPC. Les commandes enables de **sunrpc d'examiner** ou l'inspection d'application de débronchements pour le protocole RPC de Sun. Les services RPC de Sun peuvent fonctionner sur n'importe quel port sur le système. Quand les tentatives d'un client d'accéder à un service RPC sur un serveur, il doivent découvrir qui mettent en communication des passages de ce service particulier en fonction. Il fait ceci en questionnant le processus de portmapper sur le port connu le numéro 111. Le client envoie le nombre de programme RPC du service, et récupère le numéro de port. À partir de là, le programme client envoie ses requêtes RPC à ce nouveau port.

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.

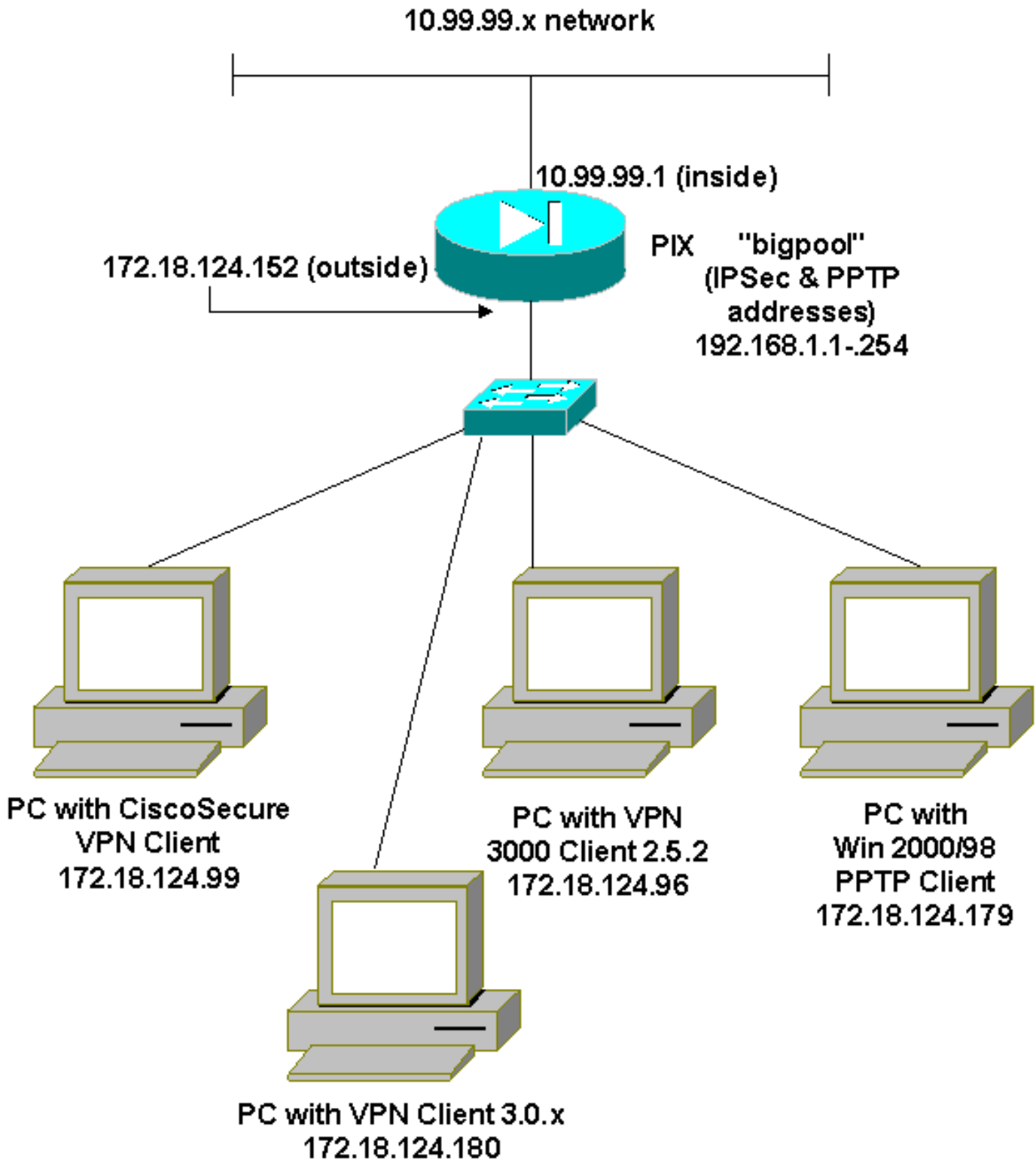
Configurez

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 la configuration réseau indiquée dans le diagramme suivant.



Configurations

Ce document utilise les configurations suivantes.

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

Pare-feu Cisco Secure PIX

`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#
```

Cisco Secure VPN Client 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
```

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

Options choisies > **Properties** > **authentification**. le Groupe-nom et le mot de passe de groupe apparient le group_name et le group_password sur le PIX comme dans :

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

Installation de client de Windows 98/2000/XP PPTP

Vous pouvez contacter le constructeur qui fait le client PPTP. Référez-vous à comment configurer le pare-feu Cisco Secure PIX pour utiliser PPTP pour les informations sur la façon dont établir ceci.

Vérifiez

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

Dépannez

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

Debug PIX IPsec

- **debug crypto ipsec** — Affiche les négociations IPsec de la phase 2.
- **debug crypto isakmp** — Affiche les négociations de Protocole ISAKMP (Internet Security Association and Key Management Protocol) de la phase 1.
- **debug crypto engine** — Affiche le trafic qui est chiffré.

Debug PIX PPTP

- **debug ppp E/S** — Affiche les informations de paquet pour l'interface virtuelle de PPP PPTP.
- **debug ppp error** — Messages d'erreur d'interface virtuelle de PPP des affichages PPTP.
- **erreur de debug vpdn** — Messages d'erreur de protocole des affichages PPTP.
- **paquets de debug vpdn** — Les informations de paquet des affichages PPTP au sujet du trafic PPTP.
- **événements de debug vpdn** — Les informations de modification d'événement de tunnel des affichages PPTP.
- **uauth de debug ppp** — Affiche les messages d'élimination des imperfections d'authentification de l'utilisateur d'AAA d'interface virtuelle de PPP PPTP.

Questions connexes de Microsoft

- Comment maintenir des connexions RAS actives après s'être fermé une session — quand vous vous fermez une session d'un client de Windows Remote Access Service (RAS), toutes les connexions RAS sont automatiquement déconnectées. Afin de rester a connecté après que vous vous fermiez une session, active la clé de KeepRasConnections dans le registre sur le client RAS.
- L'utilisateur n'est pas alerté en ouvrant une session avec les qualifications cachées — des symptômes - quand vous tentez d'ouvrir une session à un domaine d'un poste de travail basé sur Windows ou le serveur membre et un contrôleur de domaine ne peuvent pas se trouvent, aucun message d'erreur n'est affiché. Au lieu de cela, vous ouvrez une session sur

l'ordinateur local à l'aide des informations d'identification mises en cache.
- Comment écrire un fichier lmhosts pour la validation de domaine et d'autres questions de résolution de noms — il peut y avoir des exemples quand vous éprouvent des questions de résolution de noms sur votre réseau TCP/IP et vous devez utiliser des fichiers lmhosts pour résoudre des noms NetBIOS. Cet article discute la méthode appropriée de créer un fichier lmhosts pour faciliter la validation de résolution de noms et de domaine.

Informations connexes

- Pages de support de Négociation IPSec/protocoles IKE
- Référence des commandes PIX
- Page de support pour serveurs de sécurité de la gamme Cisco PIX 500
- Demandes de commentaires (RFC)
- Sécurité des réseaux de configuration d'IPSec
- Configurer le protocole de sécurité IKE
- Soutien technique et documentation Cisco Systems