De PIX-firewall en VPN-clients configureren met PPTP, MPPE en IPSec

Inhoud

Inleiding

In deze voorbeeldconfiguratie, verbinden vier verschillende soorten cliënten en versleutelen verkeer met de Cisco Secure PIX-firewall als tunneleindpunt:

- Gebruikers die Cisco Secure VPN-client 1.1 uitvoeren op Microsoft Windows 95/98/NT
- Gebruikers die de Cisco Secure VPN 3000 Client 2.5.x op Windows 95/98/NT uitvoeren
- Gebruikers die native Windows 98/2000/XP Point-to-Point Tunneling Protocol (PPTP)-clients gebruiken
- Gebruikers die de Cisco VPN-client 3.x/4.x uitvoeren op Windows 95/98/NT/2000/XP

In dit voorbeeld wordt één pool voor IPsec en PPTP geconfigureerd. De pools kunnen echter ook afzonderlijk worden gemaakt.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- PIX-softwarerelease 6.3.3
- Cisco Secure VPN-client 12.1
- Cisco VPN 3000 clientversie 2.5
- Cisco VPN-client 3.x en 4.x
- Microsoft Windows 2000 en Windows 98-clients

Opmerking: Dit is getest op PIX-softwarerelease 6.3.3 maar moet werken aan release 5.2.x en 5.3.1. PIX-softwarerelease 6.x is vereist voor Cisco VPN-client 3.x en 4.x. (Ondersteuning voor Cisco VPN 3000 Client 2.5 wordt toegevoegd aan PIX-softwarerelease 5.2.x. De configuratie werkt ook voor PIX-softwarerelease 5.1.x, behalve voor het Cisco VPN 3000-clientdeel.) IPsec en PPTP/Microsoft Point-to-Point Encryption (MPPE) moeten eerst afzonderlijk worden uitgevoerd. Als ze niet afzonderlijk werken, werken ze niet samen.

Opmerking: PIX 7.0 gebruikt de opdracht **rpc**-pakketten **controleren** om RPC-pakketten te verwerken. De opdracht **zonnepc** controleren stelt een toepassingsinspectie voor het Sun RPC-protocol in of uit. De RPC-services van de zon kunnen op elke poort van het systeem draaien. Wanneer een client probeert om toegang te krijgen tot een RPC-service op een server, moet hij uitzoeken welke poort op die bepaalde service wordt ingeschakeld. Dit gebeurt door het portopenproces te bevragen op het bekende havennummer 111. De cliënt verstuurt het RPC-programmanummer van de dienst en krijgt het poortnummer terug. Vanaf dit punt stuurt het clientprogramma zijn RPC-vragen naar die nieuwe poort.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

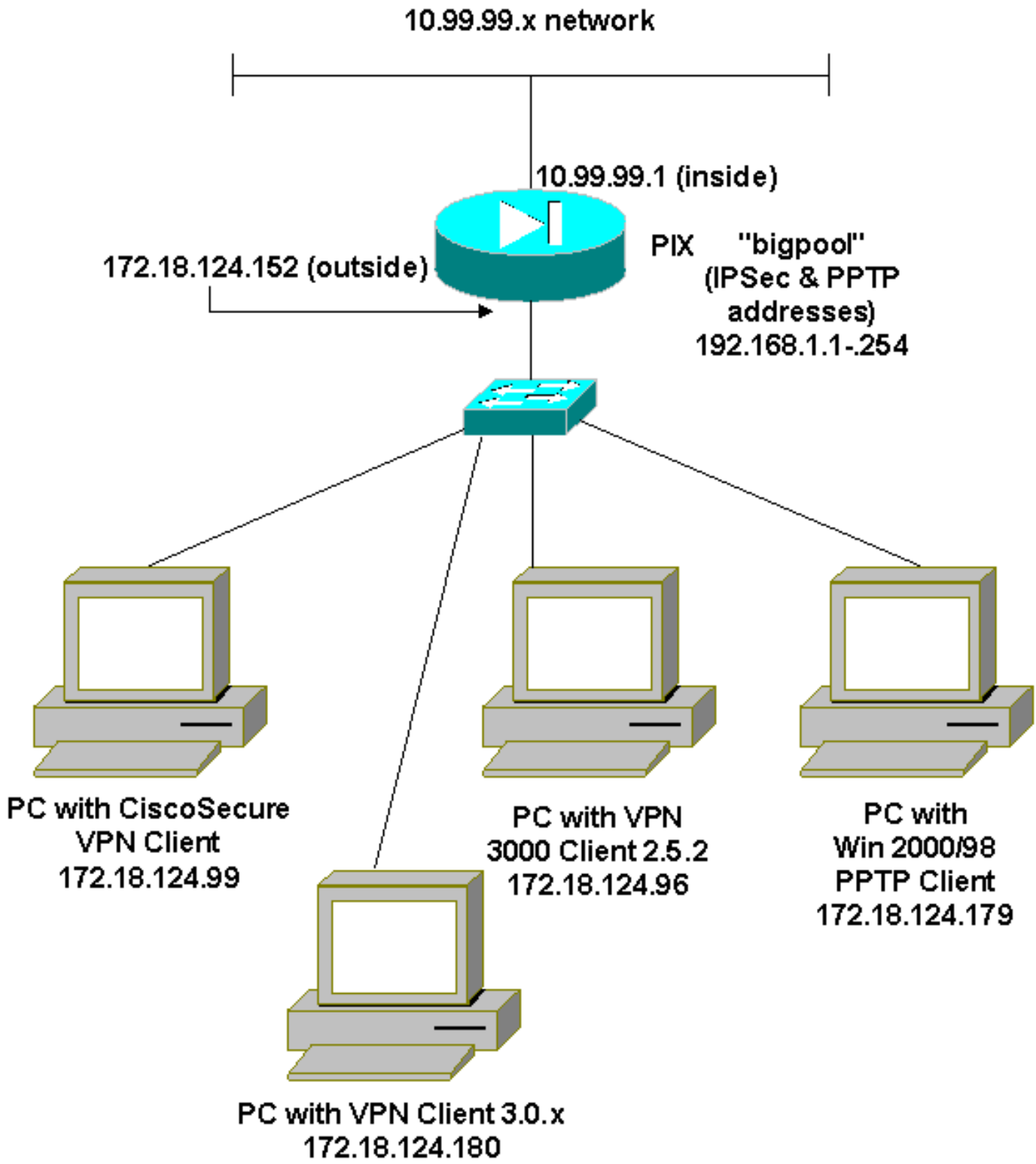
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Dit document gebruikt de netwerkinstellingen die in dit diagram worden weergegeven.



Configuraties

Dit document gebruikt deze configuraties.

- Cisco Secure PIX-firewall
- Cisco Secure VPN-client 12.1

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#
```

Cisco Secure VPN-client 12.1

```
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 voor Cisco VPN-client 3.x en 4.x

Selecteer **Opties > Eigenschappen > Verificatie**. Groepsnaam en groepswachtwoord komen overeen met group_name en group_password op de PIX zoals in:

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

Windows 98/2000/XP PPTP-clientinstelling

U kunt contact opnemen met de verkoper die de PPTP-client maakt. Raadpleeg Hoe u de Cisco Secure PIX-firewall configureren als u PPTP wilt gebruiken voor informatie over het instellen van deze firewall.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor troubleshooting

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

PIX IPsec debug

- **debug crypto ipsec**-displays de IPsec onderhandelingen van fase 2.
- **debug van crypto isakmp** — Hiermee geeft u de onderhandelingen over fase 1 weer van de Internet Security Association en Key Management Protocol (ISAKMP).
- **debug van crypto motor**-displays het verkeer dat versleuteld wordt.

PIX PPTP-debug

- **debug ppo io**-displays de pakketinformatie voor de PPTP PPP virtuele interface.
- **debug van PPP-fout**-displays PPTP PPP virtuele interfacefoutmeldingen.
- **debug van fout**-displays PPTP-protocolfoutmeldingen.
- **debug VPDN-pakketten**—displays PPTP-pakketinformatie over PPTP-verkeer.
- **debug VPDN gebeurtenissen**—displays PTP-tunnelgebeurtenissen veranderingsinformatie.
- **debug van PPP auth**-displays de PPTP PPP virtuele interface AAA gebruiker authenticatie-berichten.

Verwante Microsoft-problemen

- RAS-verbindingen actief houden na het uitloggen —Wanneer u zich uit een Windows Remote Access Service-client (RAS) logt, worden alle RAS-verbindingen automatisch losgekoppeld. Om verbinding te blijven maken nadat u bent uitgeschakeld, schakelt u de toets BebRasConnections in het register op de RAS-client in.
- Gebruiker is niet gewaarschuwd bij inloggen met gedeponeerde crediteuren —Symptomen - Wanneer u probeert in te loggen op een domein van een Windows-gebaseerde werkstation of ledenserver en er geen domeincontroller kan worden gevonden, wordt er geen foutmelding weergegeven. In plaats daarvan, wordt u met gecachede geloofsbrieven op de lokale computer ingelogd.
- Schrijf een LMHOSTS-bestand voor domeinvalidatie en andere problemen met naamresolutie —Er kunnen ook gevallen zijn waarin u problemen ondervindt bij het oplossen van namen op uw TCP/IP-netwerk en u probeert LAN-bestanden te gebruiken om Netgeblokkeerde namen op te lossen. In dit artikel wordt de juiste methode besproken om een LMD-bestand te maken om te helpen bij het oplossen van namen en het valideren van domein.

Gerelateerde informatie

- Ondersteuning van IPsec-onderhandeling/IKE-protocollen
- PIX-opdracht
- Ondersteuning van Cisco PIX 500 Series security applicaties
- Verzoeken om opmerkingen (RFC's)
- IPsec-netwerkbeveiliging configureren
- Het configureren van Internet Key Exchange-beveiligingsprotocol
- Technische ondersteuning en documentatie – Cisco Systems