Konfigurieren der PIX-Firewall und der VPN-Clients mithilfe von PPTP, MPPE und IPSec

Inhalt

Einführung

In dieser Beispielkonfiguration verbinden vier verschiedene Arten von Clients den Datenverkehr mit der Cisco Secure PIX Firewall als Tunnelendpunkt und verschlüsseln ihn:

- Benutzer, die Cisco Secure VPN Client 1.1 unter Microsoft Windows 95/98/NT ausführen
- Benutzer, die Cisco Secure VPN 300 Client 2.5.x unter Windows 95/98/NT ausführen
- Benutzer, die native Windows 98/2000/XP Point-to-Point Tunneling Protocol (PPTP)-Clients ausführen
- Benutzer, die Cisco VPN Client 3.x/4.x unter Windows 95/98/NT/2000/XP ausführen

In diesem Beispiel wird ein einzelner Pool für IPsec und PPTP konfiguriert. Allerdings können die Pools auch separat angelegt werden.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- PIX Softwareversion 6.3.3
- Cisco Secure VPN Client 1.1
- Cisco VPN 3000 Client Version 2.5
- Cisco VPN Client 3.x und 4.x
- Microsoft Windows 2000- und Windows 98-Clients

Hinweis: Dies wurde mit Version 6.3.3 der PIX-Software getestet, sollte jedoch mit Version 5.2.x und 5.3.1 funktionieren. PIX Software Release 6.x ist für Cisco VPN Client 3.x und 4.x erforderlich. (Die Unterstützung für den Cisco VPN 300 Client 2.5 wird in Version 5.2.x der PIX-Software hinzugefügt. Die Konfiguration funktioniert auch für PIX Software Release 5.1.x, mit Ausnahme des Cisco VPN 3000 Client-Teils.) IPsec- und PPTP/Microsoft Point-to-Point Encryption (MPPE) sollten separat verwendet werden. Wenn sie nicht separat arbeiten, arbeiten sie nicht zusammen.

Hinweis: PIX 7.0 verwendet den Befehl **inspect rpc** zur Verarbeitung von RPC-Paketen. Der Befehl inspect sunrpc aktiviert oder deaktiviert die Anwendungsüberprüfung für das Sun-RPC-Protokoll. Sun RPC-Dienste können auf jedem beliebigen Port des Systems ausgeführt werden. Wenn ein Client versucht, auf einen RPC-Dienst auf einem Server zuzugreifen, muss er herausfinden, auf welchem Port dieser Dienst ausgeführt wird. Hierzu fragt er den Port-Mapper-Prozess unter der bekannten Portnummer 111 ab. Der Client sendet die RPC-Programmnummer des Diensts und erhält die Portnummer zurück. Von diesem Punkt an sendet das Clientprogramm seine RPC-Abfragen an diesen neuen Port.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

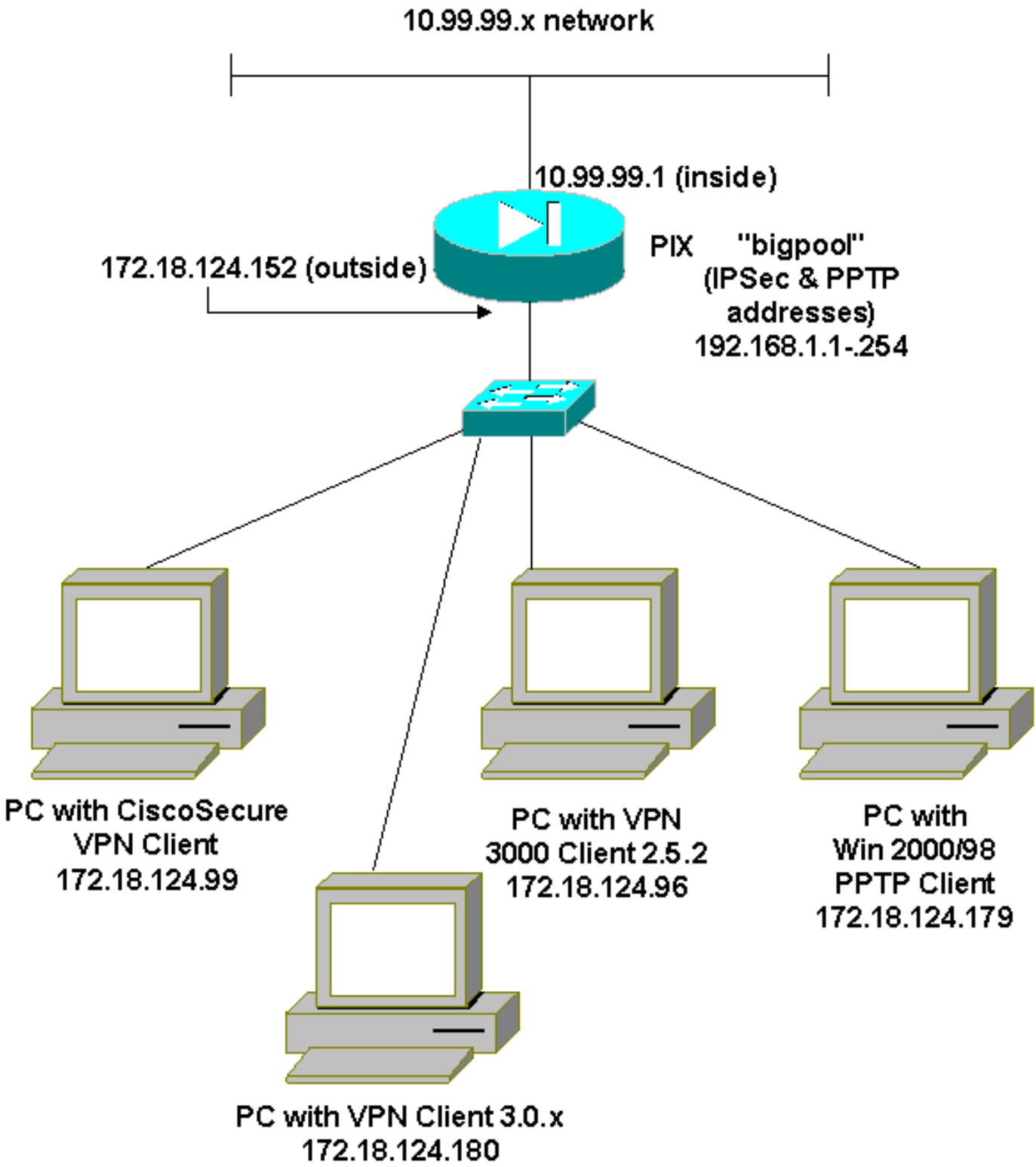
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die in diesem Diagramm dargestellte Netzwerkeinrichtung verwendet.



Konfigurationen

In diesem Dokument werden diese Konfigurationen verwendet.

- Cisco Secure PIX-Firewall
- Cisco Secure VPN Client 1.1

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 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 oder Cisco VPN Client 3.x und 4.x

Wählen Sie **Optionen > Eigenschaften > Authentifizierung aus**. Gruppenname und Gruppenkennwort stimmen mit der Gruppe_Name und dem Gruppenkennwort auf dem PIX wie in überein:

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

Windows 98/2000/XP PPTP Client Setup

Sie können sich an den Anbieter wenden, der den PPTP-Client herstellt. Weitere Informationen zur Einrichtung finden Sie unter Konfigurieren der Cisco Secure PIX Firewall zur Verwendung von PPTP.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

PIX-IPsec-Debug

- **debug crypto ipsec**: Zeigt die IPsec-Aushandlungen für Phase 2 an.
- **debug crypto isakmp**: Zeigt die Aushandlungen der Internet Security Association und des Key Management Protocol (ISAKMP) für Phase 1 an.
- **debug crypto engine**: Zeigt den verschlüsselten Datenverkehr an.

PIX PPTP-Debuggen

- **debug ppp io**: Zeigt die Paketinformationen für die virtuelle PPTP PPP-Schnittstelle an.
- **debug ppp error** (**ppp-Fehler debuggen**): Zeigt Fehlermeldungen zur virtuellen PPTP-PPP-Schnittstelle an.
- **debug vpdn error** (**vpdn-Fehler debuggen**): Zeigt Fehlermeldungen zum PPTP-Protokoll an.
- **debug vpdn pakets**: Zeigt PPTP-Paketinformationen über PPTP-Datenverkehr an.
- **debug vpdn events**: Zeigt Informationen über Änderungen von PPTP-Tunnelereignissen an.
- **debug ppp uauth**: Zeigt die Debug-Meldungen zur AAA-Benutzerauthentifizierung für die virtuelle PPTP PPP-Schnittstelle an.

Microsoft-bezogene Probleme

- So halten Sie RAS-Verbindungen nach der Abmeldung aktiv —Wenn Sie sich von einem RAS-Client (Windows Remote Access Service) abmelden, werden alle RAS-Verbindungen automatisch getrennt. Wenn Sie nach der Abmeldung eine Verbindung aufrechterhalten möchten, aktivieren Sie den KeepRasConnections-Schlüssel in der Registrierung auf dem RAS-Client.
- Der Benutzer wird nicht benachrichtigt, wenn er sich mit zwischengespeicherten Anmeldeinformationen anmeldet. —Symptome - Wenn Sie versuchen, sich von einem Windows-basierten Workstation- oder Mitgliedserver aus bei einer Domäne anzumelden, und ein Domänen-Controller nicht gefunden werden kann, wird keine Fehlermeldung angezeigt. Stattdessen sind Sie mit zwischengespeicherten Anmeldeinformationen am lokalen Computer angemeldet.
- Schreiben einer LMHOSTS-Datei für Probleme mit der Domänenvalidierung und anderen Namensauflösung —Es kann vorkommen, dass Probleme mit der Namensauflösung im TCP/IP-Netzwerk auftreten und Sie Lmhosts-Dateien verwenden müssen, um NetBIOS-Namen aufzulösen. In diesem Artikel wird die korrekte Methode zum Erstellen einer Lmhosts-Datei beschrieben, um bei der Namensauflösung und der Domänenvalidierung zu helfen.

Zugehörige Informationen

- Support-Seiten für IPsec-Aushandlung/IKE-Protokolle
- PIX-Befehlsreferenz
- Support-Seite für Cisco PIX Security Appliances der Serie 500
- Anforderungen für Kommentare (RFCs)
- Konfigurieren der IPsec-Netzwerksicherheit
- Konfigurieren des Internet Key Exchange Security Protocol
- Technischer Support und Dokumentation - Cisco Systems