使用PPTP、MPPE和IPSec配置PIX防火牆和VPN客戶端

目錄

簡介

在此示例配置中，四種不同型別的客戶端連線並加密流量並使用Cisco Secure PIX防火牆作為隧道端點：

- 在Microsoft Windows 95/98/NT上運行Cisco Secure VPN Client 1.1的使用者
- 在Windows 95/98/NT上運行Cisco Secure VPN 3000客戶端2.5.x的使用者
- 運行本地Windows 98/2000/XP點對點隧道協定(PPTP)客戶端的使用者
- 在Windows 95/98/NT/2000/XP上運行Cisco VPN Client 3.x/4.x的使用者

在本示例中，為IPsec和PPTP配置了單個池。但是，池也可以單獨設定。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- PIX軟體版本6.3.3
- Cisco安全VPN使用者端1.1
- Cisco VPN 3000使用者端版本2.5
- Cisco VPN客戶端3.x和4.x
- Microsoft Windows 2000和Windows 98客戶端

注意：在PIX軟體版本6.3.3上測試了此項，但應該在5.2.x和5.3.1版上運行。Cisco VPN客戶端3.x和4.x需要PIX軟體版本6.x。(PIX軟體版本5.2.x中新增了對Cisco VPN 3000客戶端2.5的支援。該配置也適用於PIX軟體版本5.1.x，Cisco VPN 3000客戶端部分除外。）首先應使IPsec和PPTP/Microsoft點對點加密(MPPE)單獨工作。如果他們不單獨工作，他們就不會一起工作。

注意：PIX 7.0使用**inspect rpc命令來處理RPC資料包。**inspect sunrpc 命令啟用或禁用Sun RPC協定的應用程式檢查。Sun RPC服務可以在系統上的任何埠上運行。當客戶端嘗試訪問伺服器上的RPC服務時，它必須找出運行該特定服務的埠。它通過在公認埠號111上查詢埠對映程式進程來完成此操作。客戶端傳送服務的RPC程式號，並返回埠號。從此時起，客戶端程式將其RPC查詢傳送到該新埠。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

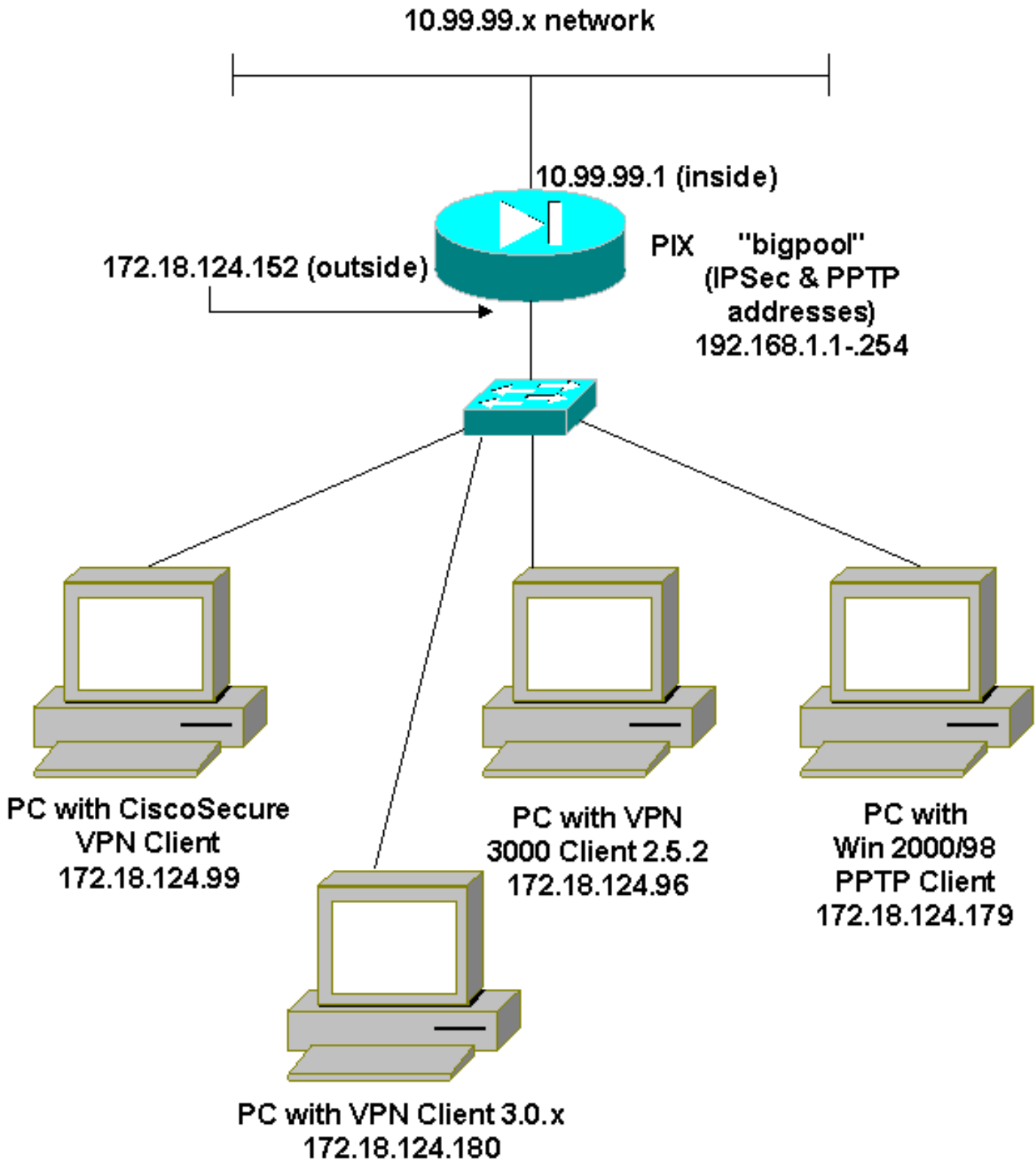
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用下圖中所示的網路設定。



組態

本檔案會使用這些設定。

- Cisco安全PIX防火牆
- Cisco安全VPN使用者端1.1

Cisco安全PIX防火牆
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安全VPN使用者端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客戶端2.5.x或Cisco VPN客戶端3.x和4.x

選擇**Options > Properties > Authentication**。Group-name和group password與PIX上的group_name和group_password匹配，如下所示：

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

Windows 98/2000/XP PPTP客戶端安裝程式

您可以聯絡製造PPTP客戶端的供應商。有關如何設定此命令的資訊，請參閱如何配置Cisco安全PIX防火牆以使用PPTP。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

PIX IPsec調試

- **debug crypto ipsec** — 顯示第2階段的IPsec協商。
- **debug crypto isakmp** — 顯示第1階段的網際網路安全關聯和金鑰管理協定(ISAKMP)協商。
- **debug crypto engine** — 顯示加密的流量。

PIX PPTP調試

- **debug ppp io** — 顯示PPTP PPP虛擬介面的資料包資訊。
- **debug ppp error** — 顯示PPTP PPP虛擬介面錯誤消息。
- **debug vpdn error** — 顯示PPTP協定錯誤消息。
- **debug vpdn packets** — 顯示有關PPTP流量的PPTP資料包資訊。
- **debug vpdn events** — 顯示PPTP隧道事件更改資訊。
- **debug ppp uauth** — 顯示PPTP PPP虛擬介面AAA使用者身份驗證調試消息。

Microsoft相關問題

- **如何在註銷後保持RAS連線處於活動狀態** — 從Windows遠端訪問服務(RAS)客戶端註銷時，所有RAS連線都會自動斷開連線。要在註銷後保持連線，請在RAS客戶端上的登錄檔中啟用KeepRasConnections項。
- **使用快取憑據登入時不會提示使用者** — 症狀 — 當您嘗試從基於Windows的工作站或成員伺服器登入到域時，如果找不到域控制器，則不會顯示錯誤消息。而是使用快取的憑據登入到本地電腦。
- **如何針對域驗證和其他名稱解析問題編寫LMHOSTS檔案** — 某些情況下，您的TCP/IP網路可能會遇到名稱解析問題，您需要使用Lmhosts檔案來解析NetBIOS名稱。本文討論建立Lmhosts檔案的正確方法，以幫助進行名稱解析和域驗證。

相關資訊

- IPsec協商/IKE通訊協定支援頁面
- PIX命令參考
- Cisco PIX 500系列安全裝置支援頁面
- 要求建議 (RFC)
- 配置IPsec網路安全
- 配置Internet金鑰交換安全協定
- 技術支援與文件 - Cisco Systems