

配置 PIX 防火墙与 VPN 客户端，以使用 PPTP、MPPE 以及 IPSec

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[Cisco VPN 3000 客户端 2.5.x 或 Cisco VPN 客户端 3.x 和 4.x](#)

[Windows 98/2000/XP PPTP 客户端设置](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[Microsoft 相关问题](#)

[相关信息](#)

简介

在这个示例配置中，四个不同的客户端使用 Cisco 安全 PIX 防火墙作为隧道终点来连接并加密数据流

- 在 Microsoft Windows 95/98/NT 上运行 Cisco 安全 VPN 客户端 1.1 的用户
- 在 Windows 95/98/NT 上运行 Cisco 安全 VPN 3000 客户端 2.5.x 的用户
- 运行本地 Windows 98/2000/XP 点对点隧道协议(PPTP)客户端的用户
- 在 Windows 95/98/NT/2000/XP 上运行 Cisco VPN 客户端 3.x/4.x 的用户

本示例中为 IPsec 和 PPTP 配置一个池。但也可以将它们分开。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- PIX 软件 6.3.3 版本
- Cisco 安全 VPN 客户端 1.1
- Cisco VPN 3000 客户端版本 2.5
- Cisco VPN 客户端 3.x 和 4.x
- Microsoft Windows 2000 和 Windows 98 客户端

注意：此版本已在PIX软件版本6.3.3上测试，但应在版本5.2.x和5.3.1上运行。Cisco VPN客户端3.x和4.x需要PIX软件版本6.x。(在PIX软件版本5.2.x中增加了对Cisco VPN 3000 Client 2.5的支持。除Cisco VPN 3000客户端部分外，该配置也适用于PIX软件版本5.1.x。) IPsec和PPTP/Microsoft点对点加密(MPPE)应先单独工作。如果它们不分开，它们就不能配合使用。

注意：PIX 7.0使用inspect rpc命令处理RPC数据包。[inspect sunrpc 命令为 Sun RPC 协议启用或禁用应用程序检查](#)。Sun RPC 服务可运行在系统中的任何端口上。当客户端尝试访问服务器上的RPC 服务时，它必须找出该服务运行于哪个端口。它通过查询公认端口号111上的端口映射器进程来实现此目的。客户端发送服务的RPC程序号，并返回端口号。从此时起，客户端程序就会将其RPC 查询发送给那个新端口。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 [Cisco 技术提示约定](#)。

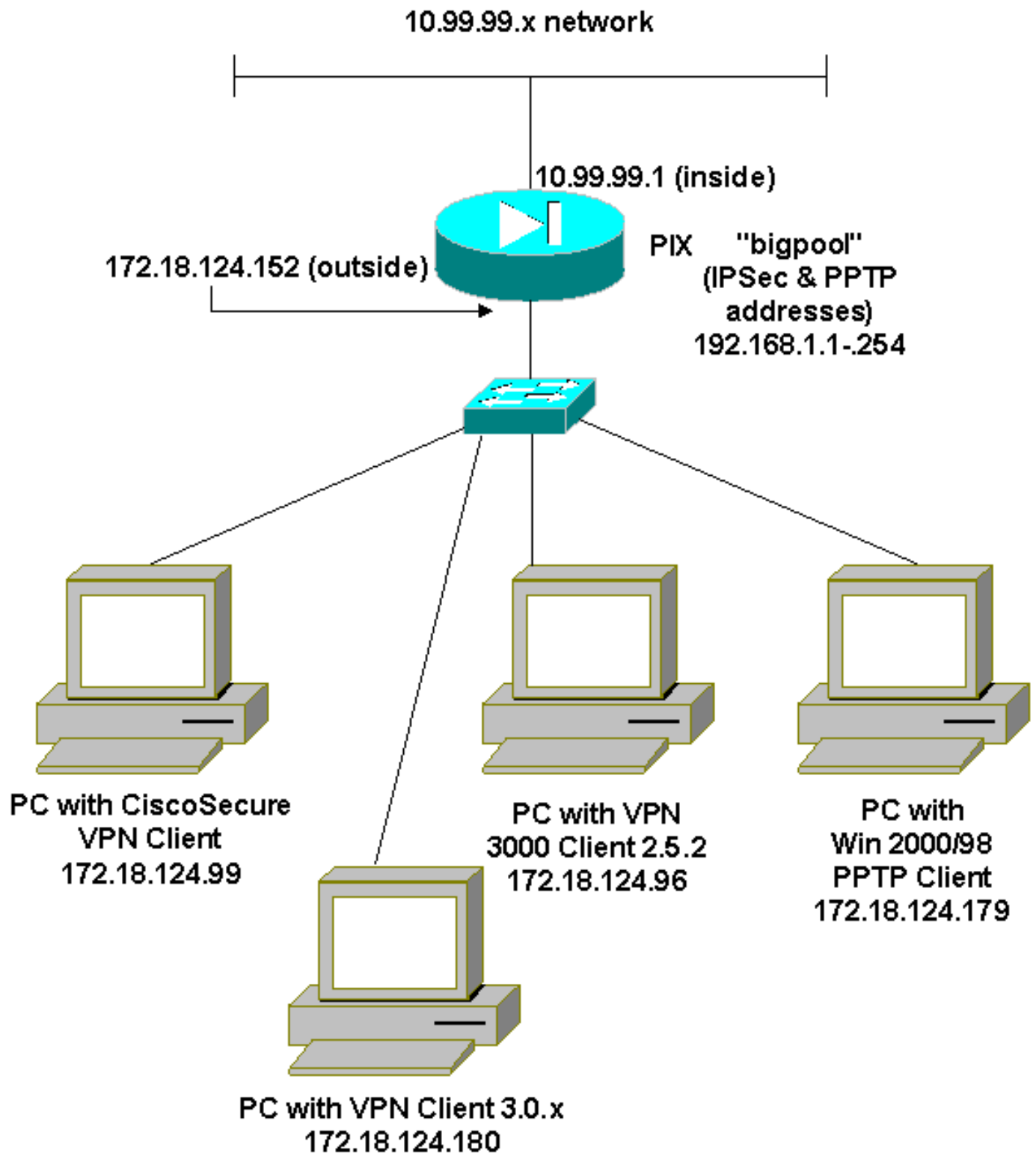
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用[命令查找工具](#)(仅限注册客户)可获取有关本节中使用的命令的详细信息。

网络图

本文档使用此图所示的网络设置。



配置

本文档使用以下配置。

- [Cisco Secure PIX 防火墙](#)
- [Cisco 安全 VPN 客户端 1.1](#)

Cisco Secure PIX 防火墙

```
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 客户端 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 客户端 2.5.x 或 Cisco VPN 客户端 3.x 和 4.x](#)

选择 **Options > Properties > Authentication**。组名和组密码与 PIX 上的组名和组密码匹配：

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

[Windows 98/2000/XP PPTP 客户端设置](#)

您可以与制造 PPTP 客户端的供应商联系。有关如何进行设置的信息，请参阅[如何配置 Cisco Secure PIX 防火墙以使用 PPTP](#)。

[验证](#)

当前没有可用于此配置的验证过程。

[故障排除](#)

本部分提供的信息可用于对配置进行故障排除。

[故障排除命令](#)

[命令输出解释程序 \(仅限注册用户\) \(OIT\) 支持某些 show 命令](#)。使用 OIT 可查看对 show 命令输出的分析。

注意：在使用 debug [命令之前](#)，请参[阅](#)有关 Debug 命令的重要信息。

[PIX IPsec 调试](#)

- debug crypto ipsec - 显示第 2 阶段的 IPsec 协商。

- debug crypto isakmp—显示第 1 阶段的 Internet 安全连接和密钥管理协议 (ISAKMP) 协商。
- debug crypto engine - 显示已加密的流量。

[PIX PPTP 调试](#)

- debug ppp io—显示 PPTP PPP 虚拟接口的数据包信息。
- debug ppp error—显示 PPTP PPP 虚拟接口的错误消息。
- debug vpdn error—显示 PPTP 协议的错误消息。
- debug vpdn packets—显示有关 PPTP 流量的 PPTP 数据包信息。
- debug vpdn events—显示 PPTP 隧道事件更改信息。
- debug ppp uauth—显示 PPTP PPP 虚拟接口 AAA 用户身份验证调试消息。

[Microsoft 相关问题](#)

- [如何在注销后使 RAS 连接保持活动状态](#) — 当您从 Windows 远程访问服务 (RAS) 客户端注销时，所有 RAS 连接都会自动断开。要在注销后保持连接，请在 RAS 客户端上的注册表中启用 KeepRasConnections 注册项。
- [使用缓存凭证登录时，用户没有收到警报](#) — 症状 — 当您尝试从基于 Windows 的工作站或成员服务器登录到域且找不到域控制器时，不显示错误消息。而是使用缓存的凭证登录到本地计算机。
- [如何为域验证和其他名称解析问题编写 LMHOSTS 文件](#) — 在 TCP/IP 网络上遇到名称解析问题时，可能会出现一些实例，并且需要使用 Lmhosts 文件来解析 NetBIOS 名称。本文讨论了创建 Lmhosts 文件的适当方法，以便进行名字解析和域确认。

[相关信息](#)

- [IPsec 协商/IKE 协议技术支持页](#)
- [PIX 命令参考](#)
- [Cisco PIX 500 系列安全设备支持页](#)
- [请求注解 \(RFC\)](#)
- [配置 IPsec 网络安全](#)
- [配置 Internet 密钥交换安全协议](#)
- [技术支持和文档 - Cisco Systems](#)