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

目录

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
- 运行本地窗口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： 在 PIX 软件版本 6.3.3 上进行了测试，但在版本 5.2.x 和 5.3.1 上应该也能正常工作。PIX软件版本6.x为Cisco VPN Client 3.x和4.x要求。(Cisco VPN 3000客户端的2.5支持在PIX软件版本5.2.x被添加。该配置也适用于 PIX 软件版本 5.1.x，但 Cisco VPN 3000 客户端部分除外。）首先，应该使 IPsec 与 PPTP/Microsoft 点到点加密 (MPPE) 分开。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** 命令来处理 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。为此，它在著名端口 111 上查询端口映射进程。客户端发送该服务的 RPC 程序编号，并获得端口号。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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

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（仅限注册用户）可获取有关本部分所使用命令的详细信息。

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： 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

- **如何保持RAS连接活动在注销以后** —，当您从Windows远程访问服务(RAS)客户端注销，所有RAS连接自动切断。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。
- **在使用缓存的凭证登录时，用户不会收到警报**—症状 - 当您尝试从基于 Windows 的工作站或成员服务器登录域，并且找不到域控制器时，不会显示任何错误消息。 而是使用缓存的凭证登录到本地计算机。
- **如何写入 LMHOSTS 文件以便进行域验证以及其他名称解析问题**—有时您会在 TCP/IP 网络上遇到名称解析问题，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&说明文件Cisco系统