通过PIX/ASA/FWSM允许PPTP/L2TP连接

目录

简介

本文档讨论 Cisco 安全设备/FWSM 所需的配置，以允许点对点隧道协议 (PPTP)/第二层隧道协议 (L2TP) 客户机通过网络地址转换 (NAT) 连接到 PPTP 服务器。

FWSM 3.1.x 和更高版本通过 PAT 支持 PPTP 穿透功能。使用 PPTP 检查以启用此功能。

注意： 为 FWSM 使用相同的 PIX 配置。

请参阅配置 Cisco 安全 PIX 防火墙以使用 PPTP，配置安全设备以接受 PPTP 连接。

对于通过 Microsoft Windows 2003 Internet 使用预共享密钥的 PIX/ASA 安全设备企业办公室，要配

置从远程 Microsoft Windows 2000/2003 和 Windows XP 客户机到该办公室的 L2TP over IP Security (IPsec)，请参阅 Windows 2000/XP PC 和使用预共享密钥的 PIX/ASA 7.2 之间的 L2TP Over IPsec 配置示例。

先决条件

要求

为尝试此配置，首先必须有正常工作的 PPTP 服务器和客户机，然后才可以处理 PIX/ASA/FWSM。

使用的组件

本文档中的信息基于以下软件版本：

- Cisco PIX 防火墙版本 6.x 和更高版本
- 运行版本 7.x 或更高版本的 Cisco ASA 5500 系列安全设备
- 运行版本 3.1.x 或更高版本的 FWSM

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。

背景理论

RFC 2637 中介绍了 PPTP。 此协议使用 TCP 连接传输实际数据（PPP 帧），TCP 连接使用的是端口 1723 和通用路由封装 (GRE) [协议 47] 扩展。客户机首次启动 TCP 连接后，由服务器启动 GRE 连接。

版本 6.2 和更低版本的信息

由于 PPTP 连接作为某个端口上的 TCP 启动，且响应为 GRE 协议，因此，PIX 自适应安全算法 (ASA) 无法确定数据流是否相关。因此，必须配置 ACL 以允许返回数据流进入 PIX。PPTP（一对一地址映射）通过使用 NAT 的 PIX 可有效工作，这是因为 PIX 使用 TCP 中的端口信息或用户数据报协议 (UDP) 包头保持对转换的跟踪。PPTP 通过使用端口地址转换协议 (PAT) 的 PIX 无法工作，这是因为 GRE 中不存在端口概念。

版本 6.3 的信息

版本 6.3 中的 PPTP 修正功能允许 PPTP 数据流通过 PIX（配置 PAT 时）。在进程中还会执行 PPTP 数据包状态检查。**fixup protocol pptp** 命令可检查 PPTP 数据包，并动态创建允许 PPTP 数据流所必需的 GRE 连接和转换。具体而言，防火墙会检查 PPTP 版本声明和呼出请求/响应顺序。如 RFC 2637 中所定义的，仅检查 PPTP 版本 1。如果任意一端声明的版本不是版本 1，则禁用 TCP 控制通道上的进一步检查。此外，还将跟踪呼出请求和响应顺序。连接和/或转换根据需要动态分配，以允许随后的辅助 GRE 数据流。为使 PAT 转换 PPTP 数据流，必须启用 PPTP 修正功能。

版本 7.x 的信息

版本 7.x 中的 PPTP 应用程序检查引擎与版本 6.3 中 **fixup protocol pptp** 的运行方式相同。

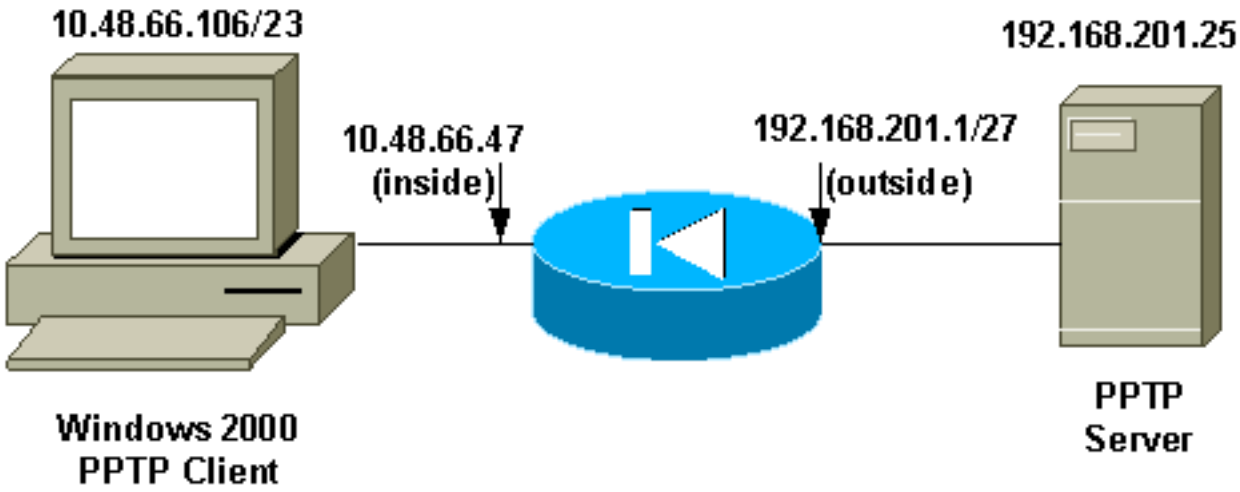
规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

客户机在内部服务器在外部的 PPTP

网络图

本文档使用以下网络设置：



注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

为版本 6.2 和更低版本添加命令

完成以下步骤，为版本 6.2 添加命令：

1. 为内部 PC 定义静态映射。在外部看到的地址为 192.168.201.5。`pixfirewall(config)#`**`static (inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0`**
2. 配置并应用 ACL，以允许 GRE 数据流从 PPTP 服务器返回 PPTP 客户机。`pixfirewall(config)#`**`access-list acl-out permit gre host 192.168.201.25 host 192.168.201.5`**
3. 应用 ACL。`pixfirewall(config)#`**`access-group acl-out in interface outside`**

为版本 6.3 添加命令

完成以下步骤，为版本 6.3 添加命令：

1. 使用此命令启用修正协议 pptp 1723。`pixfirewall(config)#`**`fixup protocol pptp 1723`**
2. 由于已启用 PPTP 修正协议，因此无需定义静态映射。可使用 PAT。`pixfirewall(config)#`**`nat (inside) 1 0.0.0.0 0.0.0.0 0 0`** `pixfirewall(config)#`**`global (outside) 1 interface`**

使用检查为版本 7.x 和 8.0 添加命令

完成以下步骤，使用 **Inspect** 命令为版本 7.x 和 8.0 添加命令：

1. 使用默认的类别映射将 PPTP 检查添加到默认策略映射中。`pixfirewall(config)#`**`policy-map global_policy`** `pixfirewall(config-pmap)#`**`class inspection_default`** `pixfirewall(config-pmap-c)#`**`inspect pptp`**

2. 由于现在由 PIX 检查 PPTP 数据流，因此无需定义静态映射。可使用 PAT。
   pixfirewall(config)#**nat (inside) 1 0.0.0.0 0.0.0.0 0 0** pixfirewall(config)#**global (outside) 1 interface** **或者**

使用 ACL 为版本 7.x 和 8.0 添加命令

完成以下步骤，使用 ACL 为版本 7.x 和 8.0 添加命令。

1. 为内部 PC 定义静态映射。在外部看到的地址为 192.168.201.5。pixfirewall(config)#**static (inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0**
2. 配置并应用 ACL，以允许 GRE 数据流从 PPTP 服务器返回 PPTP 客户机。
   pixfirewall(config)#**access-list acl-out permit gre host 192.168.201.25 host 192.168.201.5**
   pixfirewall(config)#**access-list acl-out permit tcp host 192.168.201.25 host 192.168.201.5 eq 1723**
3. 应用 ACL。pixfirewall(config)#**access-group acl-out in interface outside**

为版本 6.2 和更低版本添加命令

PIX 配置 - 内部客户机，外部服务器

```
pixfirewall(config)#write terminal Building
configuration... : Saved : PIX Version 6.2(1) nameif
ethernet0 outside security0 nameif ethernet1 inside
security100 nameif ethernet2 intf2 security10 enable
password Ujkil6aDv2yp6suI encrypted passwd
OnTrBUG1Tp0edmkr encrypted hostname pixfirewall domain-
name cisco.com fixup protocol ftp 21 fixup protocol http
80 fixup protocol h323 h225 1720 fixup protocol h323 ras
1718-1719 fixup protocol ils 389 fixup protocol rsh 514
fixup protocol rtsp 554 fixup protocol smtp 25 fixup
protocol sqlnet 1521 fixup protocol sip 5060 fixup
protocol skinny 2000 no names !--- This line allows GRE
traffic from the !--- PPTP server to the client. access-
list acl-out permit gre host 192.168.201.25 host
192.168.201.5 pager lines 24 logging on logging console
debugging logging trap debugging interface ethernet0
auto interface ethernet1 auto interface ethernet2 auto
shutdown mtu outside 1500 mtu inside 1500 mtu intf2 1500
ip address outside 209.165.201.1 255.255.255.224 ip
address inside 10.48.66.47 255.255.254.0 ip address
intf2 127.0.0.1 255.255.255.255 ip audit info action
alarm ip audit attack action alarm no failover failover
timeout 0:00:00 failover poll 15 failover ip address
outside 0.0.0.0 failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0 pdm history enable arp
timeout 14400 !--- This allows traffic from a low
security interface to !--- a high security interface.
static (inside,outside) 192.168.201.5 10.48.66.106
netmask 255.255.255.255 0 0 !--- This applies the ACL to
the outside interface. access-group acl-out in interface
outside timeout xlate 3:00:00 timeout conn 1:00:00 half-
closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip
0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute
uauth 0:04:00 inactivity 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 snmp-server
enable traps no floodguard enable no sysopt route dnat
telnet timeout 5 ssh timeout 5 terminal width 80
Cryptochecksum:18bdf8e21bd72ec0533795549165ecf5 : end
```

```
[OK]
```

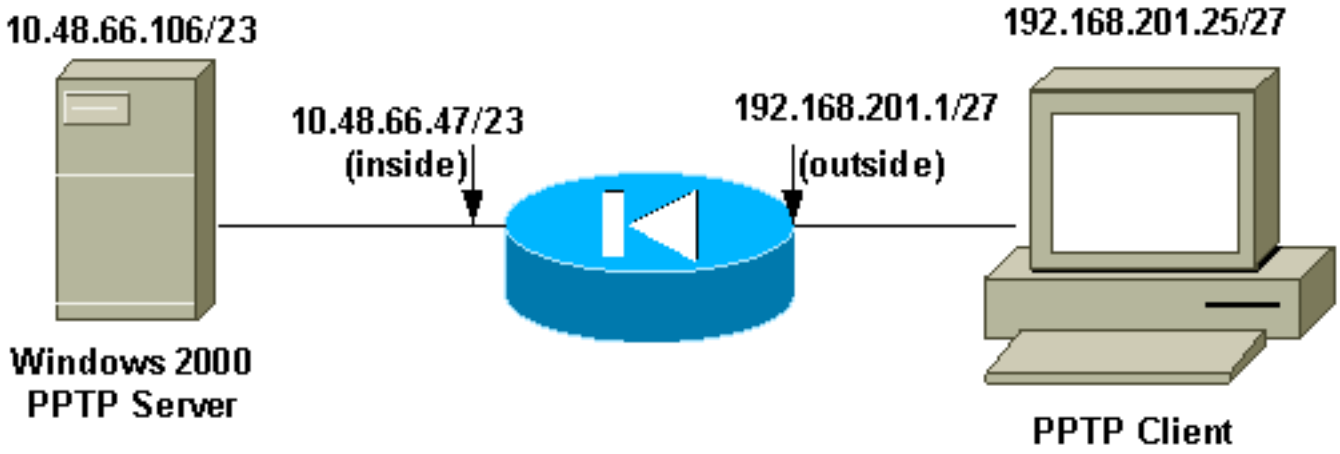
客户机在内部服务器在外部的 L2TP

完成以下步骤，使用 ACL 为版本 7.x 和 8.x 添加命令。（此配置假设 PPTP 客户机和服务器与 L2TP 客户机和服务器的 IP 地址相同。）

1. 为内部 PC 定义静态映射。在外部看到的地址为 192.168.201.5。`pixfirewall(config)#`**`static (inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0`**
2. 配置并应用 ACL，以允许 L2TP 数据流从 L2TP 服务器返回 L2TP 客户机。
   `pixfirewall(config)#`
   `pixfirewall(config)#`**`access-list acl-out permit udp host 192.168.201.25 host 192.168.201.5 eq 1701`**
3. 应用 ACL。`pixfirewall(config)#`**`access-group acl-out in interface outside`**

客户机在外部服务器在内部的 PPTP

网络图



注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

为所有版本添加命令

在此配置示例中，PPTP 服务器地址为 192.168.201.5（对内部 10.48.66.106 是静态的），PPTP 客户机地址为 192.168.201.25。

```
access-list acl-out permit gre host 192.168.201.25 host 192.168.201.5 access-list acl-out permit tcp host 192.168.201.25 host 192.168.201.5 eq 1723 static (inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0 access-group acl-out in interface outside
```

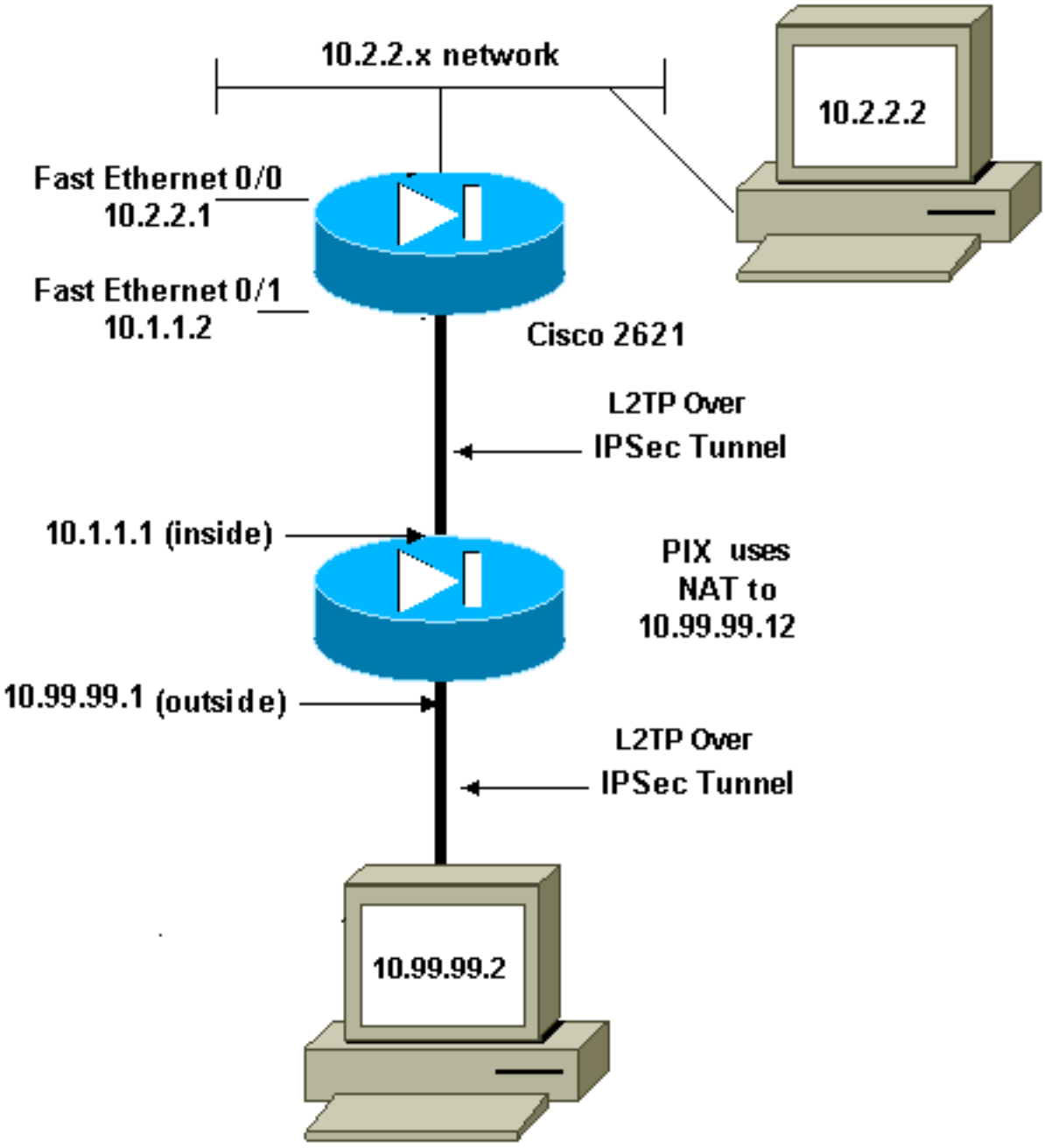
客户机在外部服务器在内部的 L2TP

在此配置示例中，L2TP 服务器地址为 192.168.201.5（对内部 10.48.66.106 是静态的），L2TP 客户机地址为 192.168.201.25。（此配置假设 PPTP 客户机和服务器与 L2TP 客户机和服务器的 IP 地址相同。）

```
access-list acl-out permit udp host 192.168.201.25 host 192.168.201.5 eq 1701 static
(inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0 access-group acl-out in
interface outside
```

允许 L2TP Over IPsec 通过 PIX/ASA 7.x 和更高版本

外部 L2TP 客户机尝试与内部 L2TP 服务器建立 L2TP over IPsec VPN 连接。为允许 L2TP over IPsec 数据包通过中间 PIX/ASA，必须允许 ESP、ISAKMP(500)、NAT-T 和 L2TP 端口 1701 建立隧道。L2TP 数据包在 PIX 中转换，并通过 VPN 隧道发送。




```
global (outside) 1 interface
nat (inside) 0 0.0.0.0 0.0.0.0
static (inside,outside) 10.99.99.12 10.1.1.2 netmask 255.255.255.255
access-group outside_access_in in interface outside

access-list outside_access_in remark Access Rule to Allow ESP traffic
access-list outside_access_in extended permit esp host 10.99.99.2
            host 10.99.99.12
```

```
access-list outside_access_in remark Access Rule to allow ISAKMP to
            host 10.99.99.12
access-list outside_access_in extended permit udp host 10.99.99.2 eq isakmp
            host 10.99.99.12

access-list outside_access_in remark Access Rule to allow port 4500 (NAT-T) to
            host 10.99.99.12
access-list outside_access_in extended permit udp host 10.99.99.2 eq 4500
            host 10.99.99.12

access-list outside_access_in remark Access Rule to allow port 1701 (L2TP) to
            host 10.99.99.12
access-list outside_access_in extended permit udp host 10.99.99.2 eq 1701
            host 10.99.99.12
```

验证

当前没有可用于此文档的验证程序。

故障排除

本部分提供的信息可用于对配置进行故障排除。

使用 PAT 时，多个 PPTP/L2TP 连接失败

使用 PAT 时，仅可有一条 PPTP/L2TP 连接通过 PIX 安全设备。这是因为，必要的 GRE 连接建立在端口 0 上，而 PIX 安全设备仅将端口 0 映射到一台主机。应急方案是启用在安全工具的PPTP检查。

错误800，当尝试连接到入站时的PPTP VPN

当您设法连接到入站时的PPTP VPN，此错误消息出现：

```
Error 800: The remote connection was not made because the attempted VPN tunnels failed. The VPN
server might be unreachable. If this connection is attempting to use an L2TP/IPsec tunnel, the
security parameters required for IPsec negotiation might not be configured properly.
```

当PPTP或L2TP转接在客户端和数据转发设备之间时的中间ASA没有启用此问题通常出现。Enable (event) PPTP或L2TP转接和检查配置为了解决问题。

debug 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。

此示例显示了未配置 ACL 以允许 GRE 数据流的情况下，PIX 内部的 PPTP 客户机启动与 PIX 外部的 PPTP 服务器的连接。如果记录对 PIX 的调试，可看到 TCP 端口 1723 数据流从客户机启动，以及 GRE 协议 47 返回数据流遭到拒绝。

```
pixfirewall(config)#loggin on pixfirewall(config)#loggin console 7 pixfirewall(config)#302013:
Built outbound TCP connection 4 for outside: 192.168.201.25 /1723 (192.168.201.25 /1723) to
inside:10.48.66.106/4644 (192.168.201.5 /4644) 106010: Deny inbound protocol 47 src
outside:192.168.201.25 dst inside:192.168.201.5 106010: Deny inbound protocol 47 src
```

```
outside:192.168.201.25 dst inside:192.168.201.5
```

建立 TAC 服务请求时应收集的信息

执行以上故障排除步骤后，如果仍需帮助，并且要使用 Cisco TAC 打开服务请求，请确保包括以下信息。
• 问题说明和相关拓扑详细信息 • 在开立服务请求之前执行的故障排除 • **show tech-support** 命令的输出 • 运行 **logging buffered debugging** 命令后 **show log** 命令的输出，或演示问题的控制台捕获信息（如果可用） 请将收集到的数据以未压缩的纯文本格式 (.txt) 附加到服务请求中。通过使用服务请求查询工具（仅限注册用户）上载信息，可以将信息附加到服务请求中。如果无法访问服务请求查询工具，可以将信息以电子邮件附件的形式发送到 attach@cisco.com，并在邮件的主题行中注明服务请求号。

相关信息

- PPTP 支持页
- PIX/ASA 7.x 和更高版本 IPsec 隧道使用访问列表和 MPF 通过执行 NAT 的安全设备配置示例
- 配置 IPSec 隧道通过执行 NAT 的防火墙
- Cisco PIX 防火墙软件
- Cisco Secure PIX 防火墙命令参考
- 安全产品 Field Notices（包括 PIX）
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems