使用带有PIX/ASA的SNMP

目录

简介

您可以使用 Simple Network Management Protocol (SNMP) 来监控 PIX 上的系统事件。本文档描述如何将 SNMP 与 PIX 结合使用，包括：

- 用于*通过* PIX 或*对* PIX 运行 SNMP 的命令
- 示例 PIX 输出
- PIX 软件版本 4.0 及更高版本中的管理信息库 (MIB) 支持
- 陷阱级别
- syslog 严重级别示例
- PIX 和 SNMP 设备发现问题

注意： 用于 snmpget/snmpwalk 的端口是 UDP/161。用于 SNMP 陷阱的端口是 UDP/162。

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 Cisco Secure PIX 防火墙软件版本 4.0 及更高版本。

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。

相关产品

此配置可能也与Cisco可适应安全工具(ASA)版本7.x一起使用。

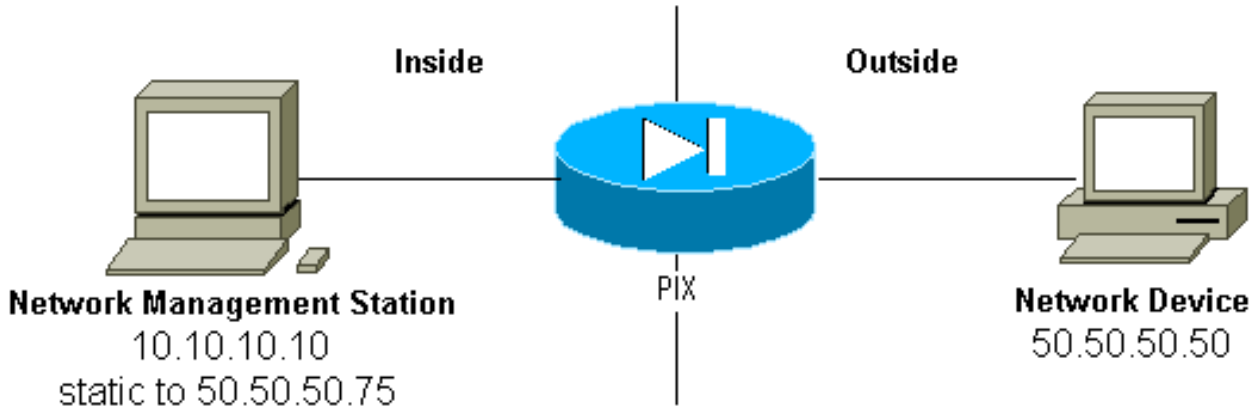
规则

本文的部分输出和日志数据线路已经包装用于间距注意事项。

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

通过 PIX/ASA 的 SNMP

由外到内的陷阱



为了允许从 50.50.50.50 到 10.10.10.10 的陷阱：

```
conduit permit udp host 50.50.50.75 eq snmptrap host 50.50.50.50 static (inside,outside)
50.50.50.75 10.10.10.10 netmask 255.255.255.255 0 0
```

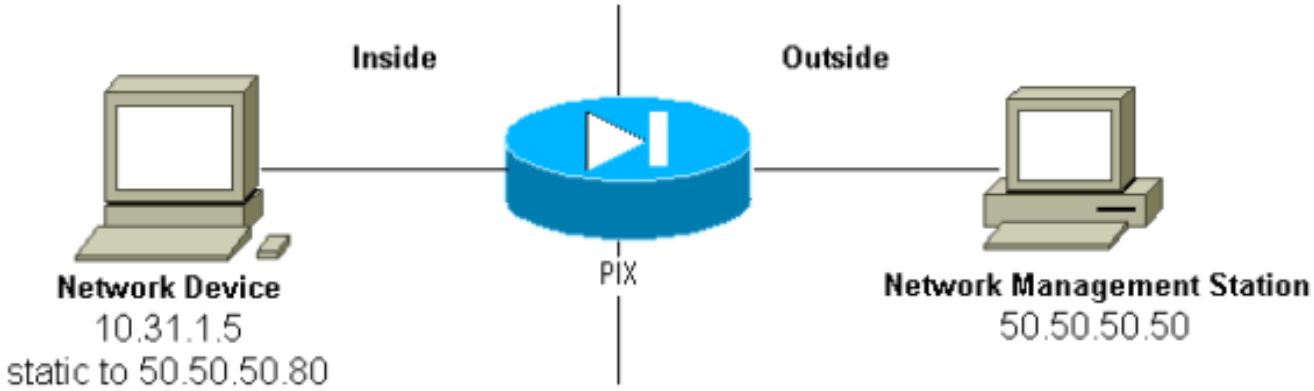
如果您使用 PIX 5.0 及更高版本提供的访问控制列表 (ACL) 来代替 conduit：

```
access-list Inbound permit udp host 50.50.50.50 host 50.50.50.75 eq snmptrap access-group
Inbound in interface outside
```

PIX 显示：

```
302005: Built UDP connection for faddr 50.50.50.50/2388
   gaddr 50.50.50.75/162 laddr 10.10.10.10/162
```

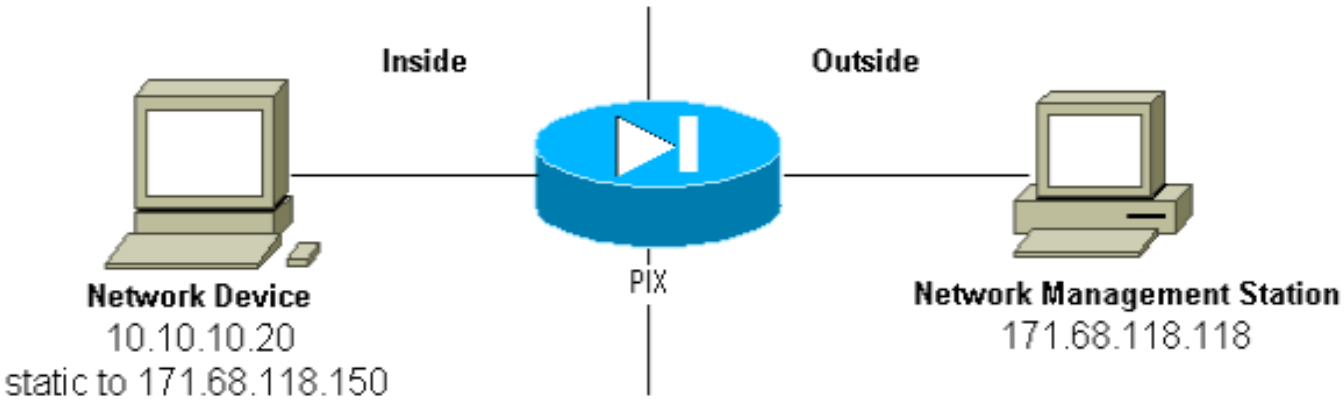
由内到外的陷阱



默认情况下允许出站流量（没有出站列表时），并且 PIX 显示：

```
305002: Translation built for gaddr 50.50.50.80 to laddr 10.31.1.5
302005: Built UDP connection for faddr 50.50.50.50/162
   gaddr 50.50.50.80/2982 laddr 10.31.1.5/2982
```

由外到内轮询



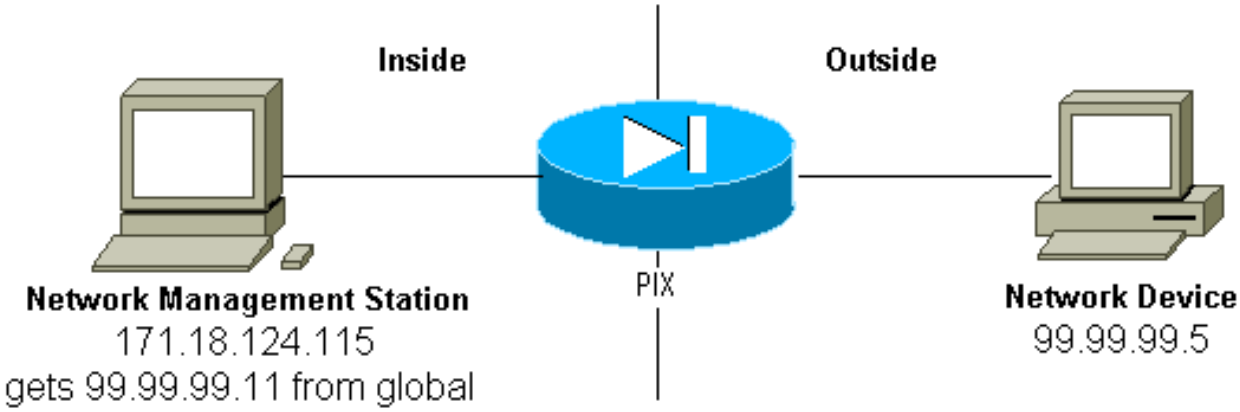
为了允许从 171.68.118.118 到 10.10.10.20 的轮询：

```
static (inside,outside) 171.68.118.150 10.10.10.20 netmask 255.255.255.255 0 0 conduit permit
udp host 171.68.118.150 eq snmp host 171.68.118.118
```

如果您使用 PIX 5.0 及更高版本支持的 ACL 来代替 conduit：

```
access-list Inbound permit udp host 171.68.118.118 host 171.68.118.150 eq snmp access-group
Inbound in interface outside
```

由内到外轮询



默认情况下允许出站流量（没有出站列表时），并且 PIX 显示：

```
305002: Translation built for gaddr 99.99.99.11 to laddr 172.18.124.115
302005: Built UDP connection for faddr 99.99.99.5/161
   gaddr 99.99.99.11/36086 laddr 172.18.124.115/36086
```

对 PIX/ASA 的 SNMP

MIB 版本支持

这些是 PIX 中支持的 MIB 版本：

- PIX 防火墙软件版本 4.0 到版本 5.1 — MIB-II 系统和接口组（参考 RFC 1213 ）而不是 AT、ICMP、TCP、UDP、EGP、传输、IP 或 SNMP 组 CISCO-SYSLOG-MIB-V1SMI.my。
- PIX 防火墙软件版本 5.1.x 及更高版本 — 早先的 MIB 和 CISCO-MEMORY-POOL-MIB.my 以及 CISCO-FIREWALL-MIB.my 的 cfwSystem 分支。
- PIX 防火墙软件版本 5.2.x 和更高版本 — 早先的 MIB 以及 IP 组的 ipAddrTable。
- PIX 防火墙软件版本 6.0.x 及更高版本 — 早先的 MIB 以及 MIB-II OID 的修改版本，通过型号来识别 PIX（并启用 CiscoView 5.2 支持）。在 CISCO-PRODUCTS-MIB 中找到新的对象标识符 (OIDs)；例如，PIX 515 具备 OID 1.3.6.1.4.1.9.1.390。
- PIX 防火墙软件版本 6.2.x 及更高版本 — 早先的 MIB 以及 CISCO-PROCESS-MIB-V1SMI.my。
- PIX/ASA 软件版本 7.x — 早先的 MIBs 以及 IF-MIB、SNMPv2-MIB、ENTITY-MIB、CISCO-REMOTE-ACCESS-MONITOR-MIB、CISCO-CRYPTO-ACCELERATOR-MIB、ALTIGA-GLOBAL-REG。

注意： PROCESS MIB的支持部分是ciscoProcessMIBObjects分组下的cpmCPU分组的cpmCPUTotalTable分组。在 MIB 中的 ciscoProcessMIBObjects 分支的 cpmProcess 分支中，不支持 ciscoProcessMIBNotifications 分支、ciscoProcessMIBconformance 分支和两个表：cpmProcessTable 和 cpmProcessExtTable。

在 PIX/ASA 中启用 SNMP

在 PIX 中发出以下命令，允许轮询/查询和陷阱：

```
snmp-server host #.#.#.# !--- IP address of the host allowed to poll !--- and where to send traps. snmp-server community <whatever> snmp-server enable traps
```

PIX 软件版本 6.0.x 及更高版本允许对陷阱和查询进行更精细的控制。

```
snmp-server host #.#.#.# !--- The host is to be sent traps and can query. snmp-server host
#.#.#.# trap !--- The host is to be sent traps and cannot query. snmp-server host #.#.#.# poll
!--- The host can query but is not to be sent traps.
```

PIX/ASA 软件版本 7.x 允许对陷阱和查询进行更精细的控制。

```
hostname(config)#snmp-server host <interface_name> <ip_address> trap community <community
string> !--- The host is to be sent traps and cannot query !--- with community string specified.
hostname(config)#snmp-server host <interface_name> <ip_address> poll community <community
string> !--- The host can query but is not to be sent traps !--- with community string
specified.
```

注意： 如果要将 NMS 限制为只接收陷阱或浏览（轮询），请指定 **trap** 或 **poll**。默认情况下，NMS 能使用这两种功能。

默认情况下，SNMP 陷阱是在 UDP 端口 162 上发送的。您可以使用 **udp-port** 关键字来更改端口号。

对 PIX/ASA 的 SNMP - 轮询

PIX 返回的变量取决于版本中的 MIB 支持。本文档末尾处展示了关于运行版本 6.2.1 的 PIX 的 snmpwalk 的示例输出。更早的软件版本只返回以前说明的 MIB 值。

对 PIX/ASA 的 SNMP - 陷阱

注意： PIX防火墙的SNMP OID显示在PIX防火墙发出的事件陷阱中。OID 1.3.6.1.4.1.9.1.227 被用作 PIX 防火墙系统 OID，直到 PIX 软件版本 6.0 为止。在 CISCO-PRODUCTS-MIB 中找到新的特定型号的 OID。

发出以下命令，以便在 PIX 中启用陷阱：

```
snmp-server host #.#.#.# !--- IP address of the host allowed to do queries !--- and where to
send traps. snmp-server community <whatever> snmp-server enable traps
```

陷阱版本 4.0 到 5.1

当您使用 PIX 软件 4.0 及更高版本时，能够生成以下陷阱：

```
cold start = 1.3.6.1.6.3.1.1.5.1
link_up = 1.3.6.1.6.3.1.1.5.4
link_down = 1.3.6.1.6.3.1.1.5.3
syslog trap (clogMessageGenerated) = 1.3.6.1.4.1.9.9.41.2.0.1
```

陷阱更改 (PIX 5.1)

在 PIX 软件版本 5.1.1 及更高版本中，陷阱级别与 syslog 陷阱的 syslog 级别分离。PIX 仍然发送 syslog 陷阱，但可以进行更精细的配置。此示例的原始 trapd.log 文件（对于 HP OpenView [HPOV] 和 Netview 均相同）中所包括的 3 个 link_up 陷阱和 9 个 syslog 陷阱，具有 7 个不同的 syslog ID：101003、104001、111005、111007、199002、302005、305002。

trapd.log 的示例

```
952376318 1 Mon Mar 06 15:58:38 2000 10.31.1.150 - 1=20 2=7
   3=Syslog Trap 4=199002:
PIX startup completed. Beginning operation. 5=0;1 .1.3.6.1.4.1.9.9.4 1.2.0.1 0
```

```
952376318 1 Mon Mar 06 15:58:38 [10.31.1.150.2.2] %PIX-1-104001: (Secondary)
Switching to ACTIVE - no failover cable.

952376332 1 Mon Mar 06 15:58:52 2000 10.31.1.150 - 1=20 2=2
   3=Syslog Trap 4=101003: (Secondary) Failover cable not connected (this unit)
   5=1400;1 .1.3.6.1.4.1.9.9.41.2.0.1 0

952376332 1 Mon Mar 06 15:58:52 [10.31.1.150.2.2] %PIX-1-101003: (Secondary)
Failover cable not connected (this unit)

952376345 1 Mon Mar 06 15:59:05 2000 10.31.1.150 - 1=20 2=7
   3=Syslog Trap 4=305002:
Translation built for gaddr 50.50.50.75 to laddr 171.68.118.118 5=2800;1
.1.3.6.1.4.1.9.9.41.2.0.1 0

952376345 1 Mon Mar 06 15:59:05 2000 10.31.1.150 - 1=20 2=7
   3=Syslog Trap 4=302005: Built UDP connection for faddr 50.50.50.50/2388
   gaddr 50.50.50.75/162 laddr 171.68.118.118/162
   5=2800;1 .1.3.6.1.4.1.9.9.41.2.0.1 0

952376347 1 Mon Mar 06 15:59:07 2000 10.31.1.150 - Agent Interface Up (linkUp
Trap) enterprise:ENTERPRISES.9.1.227 (.1.3.6.1.4.1.9.1.227) on interface 1;1
.1.3.6.1.6.3.1.1.5.4.1.3.6.1.4.1.9.1.227 0

952376347 1 Mon Mar 06 15:59:07 2000 10.31.1.150 - Agent Interface Up (linkUp
Trap) enterprise:ENTERPRISES.9.1.227 (.1.3.6.1.4.1.9.1.227) on interface 2;1
.1.3.6.1.6.3.1.1.5.4.1.3.6.1.4.1.9.1.227 0

952376347 1 Mon Mar 06 15:59:07 2000 10.31.1.150 - Agent Interface Up (linkUp
Trap) enterprise:ENTERPRISES.9.1.227 (.1.3.6.1.4.1.9.1.227) on interface 3;1
.1.3.6.1.6.3.1.1.5.4.1.3.6.1.4.1.9.1.227 0

952376360 1 Mon Mar 06 15:59:20 2000 10.31.1.150 - 1=20 2=6
   3=Syslog Trap 4=111007: Begin configuration: console reading from terminal
   5=4200;1 .1.3.6.1.4.1.9.9.41.2.0.1 0

952376365 1 Mon Mar 06 15:59:25 2000 10.31.1.150 - 1=20 2=6
   3=Syslog Trap 4=111005: console end configuration: OK
   5=4700;1 .1.3.6.1.4.1.9.9.41.2.0.1 0
```

每个陷阱的说明 - trapd.log

```
199002 (syslog)
4=199002: PIX startup completed. Beginning operation.
5=0;1 .1.3.6.1.4.1.9.9.41.2.0.1 0



104001 (syslog)
Mar 6 15:58:38 [10.31.1.150.2.2] %PIX-1-104001: (Secondary)
Switching to ACTIVE - no failover cable.


101003 (syslog)
952376332 1 Mon Mar 06 15:58:52 2000 10.31.1.150 - 1=20 2=2
   3=Syslog Trap 4=101003: (Secondary) Failover cable not connected (this unit)
   5=1400;1 .1.3.6.1.4.1.9.9.41.2.0.1 0


101003 (syslog)
Mar 6 15:58:52 [10.31.1.150.2.2] %PIX-1-101003: (Secondary) Failover cable not
connected (this unit)
```

```
305002 (syslog)
952376345 1 Mon Mar 06 15:59:05 2000 10.31.1.150 - 1=20 2=7
   3=Syslog Trap 4=305002: Translation built for gaddr 50.50.50.75
   to laddr 171.68.118.118 5=2800;1 .1.3.6.1.4.1.9.9.41.2.0.1 0


302005 (syslog)
952376345 1 Mon Mar 06 15:59:05 2000 10.31.1.150 - 1=20 2=7
   3=Syslog Trap 4=302005: Built UDP connection for faddr 50.50.50.50/2388
   gaddr 50.50.50.75/162 laddr 171.68.118.118/162
   5=2800;1 .1.3.6.1.4.1.9.9.41.2.0.1 0


Linkup (linkup)
952376347 1 Mon Mar 06 15:59:07 2000 10.31.1.150 - Agent Interface Up (linkUp
Trap) enterprise:ENTERPRISES.9.1.227 (.1.3.6.1.4.1.9.1.227) on interface 1;1
.1.3.6.1.6.3.1.1.5.4.1.3.6.1.4.1.9.1.227 0


Linkup (linkup)
952376347 1 Mon Mar 06 15:59:07 2000 10.31.1.150 - Agent Interface Up (linkUp
Trap) enterprise:ENTERPRISES.9.1.227 (.1.3.6.1.4.1.9.1.227) on interface 2;1
.1.3.6.1.6.3.1.1.5.4.1.3.6.1.4.1.9.1.227 0


Linkup (linkup)
952376347 1 Mon Mar 06 15:59:07 2000 10.31.1.150 - Agent Interface Up (linkUp
Trap) enterprise:ENTERPRISES.9.1.227 (.1.3.6.1.4.1.9.1.227) on interface 3;1
.1.3.6.1.6.3.1.1.5.4.1.3.6.1.4.1.9.1.227 0


Linkup (syslog)
952376360 1 Mon Mar 06 15:59:20 2000 10.31.1.150 - 1=20 2=6
   3=Syslog Trap 4=111007: Begin configuration: console reading from terminal
   5=4200;1 .1.3.6.1.4.1.9.9.41.2.0.1 0


111007 (syslog)
952376360 1 Mon Mar 06 15:59:20 2000 10.31.1.150 - 1=20 2=6
   3=Syslog Trap 4=111007: Begin configuration: console reading from terminal
   5=4200;1 .1.3.6.1.4.1.9.9.41.2.0.1 0


111005 (syslog)
952376365 1 Mon Mar 06 15:59:25 2000 10.31.1.150 - 1=20 2=6
   3=Syslog Trap 4=111005: console end configuration: OK
   5=4700;1 .1.3.6.1.4.1.9.9.41.2.0.1 0
```

syslog 严重级别示例

文档中重现的这些内容是为了说明七个消息。

Alert: %PIX-1-101003:(Primary) failover cable not connected (this unit) %PIX-1-104001:(Primary) Switching to ACTIVE (cause:reason) **Notification:** %PIX-5-111005:IP_addr end configuration: OK %PIX-5-111007:Begin configuration: IP_addr reading from device. **Informational**: %PIX-6-305002:Translation built for gaddr IP_addr to laddr IP_addr %PIX-6-302005:Built UDP connection for faddr faddr/fport gaddr gaddr/gport laddr laddr/lport %PIX-6-199002:Auth from laddr/lport to faddr/fport failed (server IP addr failed) in interface int name.

解释 syslog 严重级别

级别	含义

0	系统无法可用 - 紧急
1	立即采取动作 - 警报
2	严重情况 - 重要
3	错误消息 - 错误
4	警告消息 - 警告
5	正常但重要的情况 - 通知
6	参考性 - 信息
7	调试消息 - 调试

在 PIX 5.1 及更高版本上配置陷阱子集

如果 PIX 配置具有：

```
snmp-server host inside #.#.#.#
```

生成的唯一陷阱是标准陷阱：冷启动、链路打开和链路关闭（不是 syslog）。

如果 PIX 配置具有：

```
snmp-server enable traps logging history debug
```

然后生成所有标准陷阱和 syslog 陷阱。在我们的示例中，这些是 syslog 条目 101003、104001、111005、111007、199002、302005 和 305002，以及 PIX 生成的其他任何 syslog 输出。由于为调试设置的日志历史记录以及这些陷阱编号处于通知、警告和信息级别，调试级别将包括：

如果 PIX 配置具有：

```
snmp-server enable traps logging history (a_level_below_debugging)
```

然后生成低于调试级别的所有标准和陷阱。如果使用 **logging history notification** 命令，将包括所有关于紧急、警报、重要、错误、警告和通知级别的 syslog 陷阱（但是不包括信息或调试级别）。在我们的例子中，将包括 111005、111007、101003 和 104001（以及 PIX 在真实网络中可能生成的其他任何编号）。

如果 PIX 配置具有：

```
snmp-server enable traps logging history whatever_level no logging message 305002 no logging message 302005 no logging message 111005
```

然后没有生成消息 305002、302005、111005。通过 **logging history debug** PIX 设置，您会看到消息 104001、101003、111007、199002 和其他所有 PIX 消息，但不包括列出的 3 个（305002、302005、111005）。

在 PIX/ASA 7.x 上配置陷阱子集

如果 PIX 配置具有：

```
snmp-server host <interface name> <ip address> community <community string>
```

生成的唯一陷阱是标准陷阱：身份验证、冷启动、链路打开和链路关闭（不是 syslog）。

剩余的配置与 PIX 软件版本 5.1 及更高版本类似，除了在 PIX/ASA 版本 7.x 中，**snmp-server enable traps** 命令还有其他选项，如 **ipsec**、**remote-access** 和 **entity**

注意： 有关 PIX/ASA 中的 SNMP 陷阱的详细信息，请参阅监控安全设备的启用 SNMP 部分

SNMP 问题

PIX 发现

如果PIX响应SNMP咨询，并且报告OID为1.3.6.1.4.1.9.1.227，在PIX防火墙软件6.0版本或更高版本中，它以CISCO-PRODUCTS-MIB中列出的ID的形式报告，PIX正常运行。

在 5.2.x 之前的 PIX 代码版本中，如果为 IP 组的 ipAddrTable 添加支持，网络管理站可能无法在地图上正确标出 PIX。如果网络管理站能够 ping PIX，则它应该始终可以检测出 PIX 存在的情况，但可能无法将其标为 PIX - 带有 2 盏灯的黑盒子。除需要IP组的IP地址表、HPOV和Netview的支持以外，其他大部分网络管理站需要了解一点：PIX返回的OID是PIX的OID，以显示正确的图标。

CiscoView 对 PIX 管理的支持已添加到 CiscoView 5.2 中；还需要 PIX 版本 6.0.x。在早期的 PIX 版本中，第三方管理应用程序允许 HPOV 网络节点管理器识别运行 PIX 防火墙管理器的 PIX 防火墙和系统。

发现 PIX 内部的设备

如果已经正确配置了 PIX，将从外向内传递 SNMP 查询和陷阱。因为 PIX 上通常会配置网络地址转换 (NAT)，所以执行此操作要求静态状态。问题是，当网络管理站没有进行公共地址(对网络内部的专用地址是静态的)的snmpwalk时，信息包的外部头与ipAddrTable中的信息不一致。此处 171.68.118.150 是流动的，静态转换到 PIX 内的 10.10.10.20，并且您能看到设备 171.68.118.150 报告它有两个接口：10.10.10.20 和 10.31.1.50：

```
ip.ipAddrTable.ipAddrEntry.ipAdEntAddr.10.10.10.20 : IpAddress: 10.10.10.20
ip.ipAddrTable.ipAddrEntry.ipAdEntAddr.10.31.1.50 : IpAddress: 10.31.1.50
```

这对网络管理站会起作用吗？可能不会。陷阱也存在相同的问题：如果10.31.1.50接口断开，设备171.68.118.150将报告接口10.31.1.50发生了故障。

从外部尝试管理内部网络的另一个问题是“发现”网络。如果管理站是 Netview 或 HPOV，这些产品将使用“netmon”后台程序从设备上阅读路由表。路由表用于发现。PIX 不能充分支持 RFC 1213，以便将路由表返回给网络管理站，而且出于安全原因，这也不是一个好主意。 当PIX中的设备报告他们的路由表时，当静态被查询，所有共享IP设备(静态)报告所有专用接口。如果 PIX 内部的其他专用地址没有静态状态，则不能进行查询。如果它们有静态状态，网络管理站无法了解其静态情况。

发现 PIX 外部的设备

由于PIX内部的网络管理站查询报告"公共"接口的公共地址，外部发现到内部问题都不适用。

在这里，171.68.118.118 为内部，10.10.10.25 为外部。当171.68.118.118流到10.10.10.25时，机箱正确报告接口，即报头与信息包里面的相同：

```
ip.ipAddrTable.ipAddrEntry.ipAdEntAddr.10.10.10.25 : IpAddress: 10.10.10.25
ip.ipAddrTable.ipAddrEntry.ipAdEntAddr.10.31.1.50 : IpAddress: 10.31.1.50
```

PIX 的 6.2 版 snmpwalk

snmpwalk-c public<pix_ip_address> 命令，用在 HPOV 管理站上，执行 snmpwalk。在执行 snmpwalk 之前，已经加载了可由 PIX 6.2 使用的所有 MIB。

```
system.sysDescr.0 : DISPLAY STRING- (ascii):
Cisco PIX Firewall Version 6.2(1)
system.sysObjectID.0 : OBJECT IDENTIFIER:
.iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.390
system.sysUpTime.0 : Timeticks: (6630200) 18:25:02.00
system.sysContact.0 : DISPLAY STRING- (ascii):
system.sysName.0 : DISPLAY STRING- (ascii):  satan
system.sysLocation.0 : DISPLAY STRING- (ascii):
system.sysServices.0 : INTEGER: 4
interfaces.ifNumber.0 : INTEGER: 3
interfaces.ifTable.ifEntry.ifIndex.1 : INTEGER: 1
interfaces.ifTable.ifEntry.ifIndex.2 : INTEGER: 2
interfaces.ifTable.ifEntry.ifIndex.3 : INTEGER: 3
interfaces.ifTable.ifEntry.ifDescr.1 : DISPLAY STRING- (ascii):
PIX Firewall 'outside' interface
interfaces.ifTable.ifEntry.ifDescr.2 : DISPLAY STRING- (ascii):
PIX Firewall 'inside' interface
interfaces.ifTable.ifEntry.ifDescr.3 : DISPLAY STRING- (ascii):
PIX Firewall 'intf2' interface
interfaces.ifTable.ifEntry.ifType.1 : INTEGER: ethernet-csmacd
interfaces.ifTable.ifEntry.ifType.2 : INTEGER: ethernet-csmacd
interfaces.ifTable.ifEntry.ifType.3 : INTEGER: ethernet-csmacd
interfaces.ifTable.ifEntry.ifMtu.1 : INTEGER: 1500
interfaces.ifTable.ifEntry.ifMtu.2 : INTEGER: 1500
interfaces.ifTable.ifEntry.ifMtu.3 : INTEGER: 1500
interfaces.ifTable.ifEntry.ifSpeed.1 : Gauge32: 10000000
interfaces.ifTable.ifEntry.ifSpeed.2 : Gauge32: 10000000
interfaces.ifTable.ifEntry.ifSpeed.3 : Gauge32: 10000000
interfaces.ifTable.ifEntry.ifPhysAddress.1 : OCTET STRING-
(hex): length = 6
     0:  00 50 54 fe ea 30 -- -- -- -- -- -- -- -- -- --
.PT..0..........

interfaces.ifTable.ifEntry.ifPhysAddress.2 : OCTET STRING-   (hex): length = 6
     0:  00 50 54 fe ea 31 -- -- -- -- -- -- -- -- -- --
.PT..1..........

interfaces.ifTable.ifEntry.ifPhysAddress.3 : OCTET STRING-   (hex): length = 6
     0:  00 90 27 42 fb be -- -- -- -- -- -- -- -- -- --
..'B............

interfaces.ifTable.ifEntry.ifAdminStatus.1 : INTEGER: up
interfaces.ifTable.ifEntry.ifAdminStatus.2 : INTEGER: up
interfaces.ifTable.ifEntry.ifAdminStatus.3 : INTEGER: down
interfaces.ifTable.ifEntry.ifOperStatus.1 : INTEGER: up
interfaces.ifTable.ifEntry.ifOperStatus.2 : INTEGER: up
interfaces.ifTable.ifEntry.ifOperStatus.3 : INTEGER: down
interfaces.ifTable.ifEntry.ifLastChange.1 : Timeticks: (6630200) 18:25:02.00
interfaces.ifTable.ifEntry.ifLastChange.2 : Timeticks: (6630200) 18:25:02.00
interfaces.ifTable.ifEntry.ifLastChange.3 : Timeticks: (6630200) 18:25:02.00
interfaces.ifTable.ifEntry.ifInOctets.1 : Counter: 0
interfaces.ifTable.ifEntry.ifInOctets.2 : Counter: 19120151
interfaces.ifTable.ifEntry.ifInOctets.3 : Counter: 0
interfaces.ifTable.ifEntry.ifInUcastPkts.1 : Counter: 0
interfaces.ifTable.ifEntry.ifInUcastPkts.2 : Counter: 1180
interfaces.ifTable.ifEntry.ifInUcastPkts.3 : Counter: 0
interfaces.ifTable.ifEntry.ifInNUcastPkts.1 : Counter: 0
```

```
interfaces.ifTable.ifEntry.ifInNUcastPkts.2 : Counter: 246915
interfaces.ifTable.ifEntry.ifInNUcastPkts.3 : Counter: 0
interfaces.ifTable.ifEntry.ifInDiscards.1 : Counter: 0
interfaces.ifTable.ifEntry.ifInDiscards.2 : Counter: 0
interfaces.ifTable.ifEntry.ifInDiscards.3 : Counter: 0
interfaces.ifTable.ifEntry.ifInErrors.1 : Counter: 0
interfaces.ifTable.ifEntry.ifInErrors.2 : Counter: 0
interfaces.ifTable.ifEntry.ifInErrors.3 : Counter: 0
interfaces.ifTable.ifEntry.ifOutOctets.1 : Counter: 60
interfaces.ifTable.ifEntry.ifOutOctets.2 : Counter: 187929
interfaces.ifTable.ifEntry.ifOutOctets.3 : Counter: 0
interfaces.ifTable.ifEntry.ifOutUcastPkts.1 : Counter: 1
interfaces.ifTable.ifEntry.ifOutUcastPkts.2 : Counter: 2382
interfaces.ifTable.ifEntry.ifOutUcastPkts.3 : Counter: 0
interfaces.ifTable.ifEntry.ifOutNUcastPkts.1 : Counter: 0
interfaces.ifTable.ifEntry.ifOutNUcastPkts.2 : Counter: 0
interfaces.ifTable.ifEntry.ifOutNUcastPkts.3 : Counter: 0
interfaces.ifTable.ifEntry.ifOutDiscards.1 : Counter: 0
interfaces.ifTable.ifEntry.ifOutDiscards.2 : Counter: 0
interfaces.ifTable.ifEntry.ifOutDiscards.3 : Counter: 0
interfaces.ifTable.ifEntry.ifOutErrors.1 : Counter: 0
interfaces.ifTable.ifEntry.ifOutErrors.2 : Counter: 0
interfaces.ifTable.ifEntry.ifOutErrors.3 : Counter: 0
interfaces.ifTable.ifEntry.ifSpecific.1 : OBJECT IDENTIFIER:
.ccitt.zeroDotZero
interfaces.ifTable.ifEntry.ifSpecific.2 : OBJECT IDENTIFIER:
.ccitt.zeroDotZero
interfaces.ifTable.ifEntry.ifSpecific.3 : OBJECT IDENTIFIER:
.ccitt.zeroDotZero
ip.ipAddrTable.ipAddrEntry.ipAdEntAddr.212.3.3.1 : IpAddress:
212.3.3.1
ip.ipAddrTable.ipAddrEntry.ipAdEntAddr.10.48.66.47 : IpAddress:
10.48.66.47
ip.ipAddrTable.ipAddrEntry.ipAdEntAddr.127.0.0.1 : IpAddress:
127.0.0.1
ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex.212.3.3.1 : INTEGER: 1
ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex.10.48.66.47 : INTEGER: 2
ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex.127.0.0.1 : INTEGER: 3
ip.ipAddrTable.ipAddrEntry.ipAdEntNetMask.212.3.3.1 : IpAddress:
255.255.255.0
ip.ipAddrTable.ipAddrEntry.ipAdEntNetMask.10.48.66.47 : IpAddress:
255.255.254.0
ip.ipAddrTable.ipAddrEntry.ipAdEntNetMask.127.0.0.1 : IpAddress:
255.255.255.255
ip.ipAddrTable.ipAddrEntry.ipAdEntBcastAddr.212.3.3.1 : INTEGER: 0
ip.ipAddrTable.ipAddrEntry.ipAdEntBcastAddr.10.48.66.47 : INTEGER: 0
ip.ipAddrTable.ipAddrEntry.ipAdEntBcastAddr.127.0.0.1 : INTEGER: 0
ip.ipAddrTable.ipAddrEntry.ipAdEntReasmMaxSize.212.3.3.1 : INTEGER:
65535
ip.ipAddrTable.ipAddrEntry.ipAdEntReasmMaxSize.10.48.66.47 : INTEGER:
65535
ip.ipAddrTable.ipAddrEntry.ipAdEntReasmMaxSize.127.0.0.1 : INTEGER:
65535
cisco.ciscoMgmt.ciscoMemoryPoolMIB.ciscoMemoryPoolObjects.
ciscoMemoryPoolTable.ciscoMemoryPoolEntry.ciscoMemoryPoolName.1 :
DISPLAY STRING- (ascii):  PIX system memory
cisco.ciscoMgmt.ciscoMemoryPoolMIB.ciscoMemoryPoolObjects.
ciscoMemoryPoolTable.ciscoMemoryPoolEntry.ciscoMemoryPoolAlternate.1 :
INTEGER: 0
cisco.ciscoMgmt.ciscoMemoryPoolMIB.ciscoMemoryPoolObjects.
ciscoMemoryPoolTable.ciscoMemoryPoolEntry.ciscoMemoryPoolValid.1 :
INTEGER: true
cisco.ciscoMgmt.ciscoMemoryPoolMIB.ciscoMemoryPoolObjects.
ciscoMemoryPoolTable.ciscoMemoryPoolEntry.ciscoMemoryPoolUsed.1 :
```

```
Gauge32: 21430272
cisco.ciscoMgmt.ciscoMemoryPoolMIB.ciscoMemoryPoolObjects.
ciscoMemoryPoolTable.ciscoMemoryPoolEntry.ciscoMemoryPoolFree.1 :
Gauge32: 12124160
cisco.ciscoMgmt.ciscoMemoryPoolMIB.ciscoMemoryPoolObjects.
ciscoMemoryPoolTable.ciscoMemoryPoolEntry.ciscoMemoryPoolLargestFree.1 :
   Gauge32: 0
cisco.ciscoMgmt.ciscoProcessMIB.ciscoProcessMIBObjects.cpmCPU.
cpmCPUTotalTable.cpmCPUTotalEntry.cpmCPUTotalPhysicalIndex.1 : INTEGER: 0
cisco.ciscoMgmt.ciscoProcessMIB.ciscoProcessMIBObjects.cpmCPU.
cpmCPUTotalTable.cpmCPUTotalEntry.cpmCPUTotal5sec.1 : Gauge32: 0
cisco.ciscoMgmt.ciscoProcessMIB.ciscoProcessMIBObjects.cpmCPU.
cpmCPUTotalTable.cpmCPUTotalEntry.cpmCPUTotal1min.1 : Gauge32: 0
cisco.ciscoMgmt.ciscoProcessMIB.ciscoProcessMIBObjects.cpmCPU.
cpmCPUTotalTable.cpmCPUTotalEntry.cpmCPUTotal5min.1 : Gauge32: 0
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatus.cfwHardwareStatusTable.cfwHardwareStatusEntry.cfwHardwareInformation.
6 : OCTET STRING- (ascii):
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatus.cfwHardwareStatusTable.cfwHardwareStatusEntry.cfwHardwareInformation.
7 : OCTET STRING- (ascii):
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatus.cfwHardwareStatusTable.cfwHardwareStatusEntry.cfwHardwareStatusValue.
6 : INTEGER: 0
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatus.cfwHardwareStatusTable.cfwHardwareStatusEntry.cfwHardwareStatusValue.
7 : INTEGER: 0
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatus.cfwHardwareStatusTable.cfwHardwareStatusEntry.cfwHardwareStatusDetail.
6 : OCTET STRING- (ascii):   Failover Off
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatus.cfwHardwareStatusTable.cfwHardwareStatusEntry.cfwHardwareStatusDetail.
7 : OCTET STRING- (ascii):   Failover Off
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatInformation.
4.3 : OCTET STRING- (ascii):  maximum number of allocated 4 byte blocks
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatInformation.
4.5 : OCTET STRING- (ascii):  fewest 4 byte blocks available
   since system startup
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatInformation.
4.8 : OCTET STRING- (ascii):  current number of available 4 byte blocks
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatInformation.
80.3 : OCTET STRING- (ascii): maximum number of allocated 80 byte blocks
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatInformation.
80.5 : OCTET STRING- (ascii): fewest 80 byte blocks available
   since system startup
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatInformation.
80.8 : OCTET STRING- (ascii): current number of available 80 byte blocks
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatInformation.
256.3 : OCTET STRING- (ascii): maximum number of allocated 256 byte blocks
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatInformation.
256.5 : OCTET STRING- (ascii): fewest 256 byte blocks available
   since system startup
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatInformation.
   256.8 : OCTET STRING- (ascii): current number of available 256 byte blocks
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
```

```
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatInformation.
1550.3 : OCTET STRING- (ascii):  maximum number of allocated 1550 byte blocks
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatInformation.
1550.5 : OCTET STRING- (ascii): fewest 1550 byte blocks available
   since system startup
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatInformation.
1550.8 : OCTET STRING- (ascii): current number of available 1550 byte blocks
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatValue.
4.3 : Gauge32: 1600
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatValue.
4.5 : Gauge32: 1599
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatValue.
4.8 : Gauge32: 1600
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatValue.
80.3 : Gauge32: 400
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatValue.
80.5 : Gauge32: 374
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatValue.
80.8 : Gauge32: 400
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatValue.
256.3 : Gauge32: 500
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatValue.
256.5 : Gauge32: 498
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatValue.
256.8 : Gauge32: 500
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatValue.
1550.3 : Gauge32: 1252
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatValue.
1550.5 : Gauge32: 865
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.cfwBufferStatValue.
1550.8 : Gauge32: 867
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwConnectionStatTable.cfwConnectionStatEntry.
   cfwConnectionStatDescription.40.6 :
OCTET STRING- (ascii):       number of connections currently in use
   by the entire firewall
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwConnectionStatTable.cfwConnectionStatEntry.
   cfwConnectionStatDescription.40.7 :
OCTET STRING- (ascii):       highest number of connections in use
   at any one time since system startup
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwConnectionStatTable.cfwConnectionStatEntry.
   cfwConnectionStatCount.40.6 :
Counter: 0
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwConnectionStatTable.cfwConnectionStatEntry.
   cfwConnectionStatCount.40.7 :
Counter: 0
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
```

```
cfwStatistics.cfwConnectionStatTable.cfwConnectionStatEntry.
   cfwConnectionStatValue.40.6 :
Gauge32: 0
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwConnectionStatTable.cfwConnectionStatEntry.
   cfwConnectionStatValue.40.7 :
Gauge32: 0
End of MIB View.
```

报告TAC案例应收集的信息

在完成本文档中的故障排除步骤之后，如果您仍然需要帮助，并且希望建立 Cisco TAC 案例，请确保附上此信息，以便进行 PIX 防火墙故障排除。
• 问题说明和相关拓扑详细信息 • 在建立请求前执行的故障排除操作 • **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） 请以非压缩的纯文本格式 (.txt) 将收集的数据附加到请求中。您可以使用 TAC 服务请求工具（仅限注册用户），通过上载信息来将信息附加到案例中。如果您不能使用案例查询工具，请将信息以电子邮件附件的形式发送到 attach@cisco.com，并在标题栏中注明您的案例编号。

相关信息

- Cisco Secure PIX 防火墙命令参考
- 思科PIX防火墙软件产品支持
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems