Usando o SNMP com PIX/ASA dos dispositivos de segurança

Contents

Introduction

Épossível monitorar os eventos do sistema no PIX usando o SNMP (Protocolo simples de gestão de rede). Este documento descreve como usar o SNMP com o PIX, que inclui:

- Comandos para executar o SNMP *através* do PIX ou *para* o PIX
- Amostra do PIX
- Suporte à Base de Informações de Gerenciamento (MIB - Management Information Base) no software PIX versão 4.0 e posterior
- Níveis de armadilhas
- exemplos de nível de gravidade syslog
- Problemas no descobrimento de dispositivos PIX e SNMP

Observação: a porta para snmpget/snmpwalk é UDP/161. A porta para interceptações SNMP é UDP/162.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Secure PIX Firewall Software Release 4.0 e posteriores.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produtos Relacionados

Essa configuração também pode ser usada com o Cisco Adaptive Security Appliance (ASA) versão 7.x.

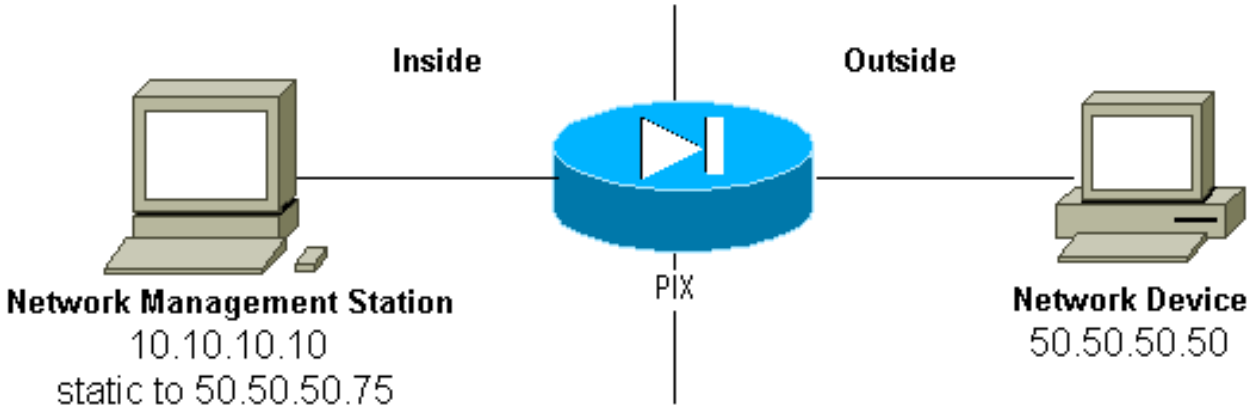
Conventions

Algumas linhas de saída e dados de registro deste documento foram retornadas por considerações de espaço.

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

SNMP através do PIX/ASA

Armadilhas de fora para dentro



Para permitir armadilhas de 50.50.50.50 a 10.10.10.10:

```
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
```

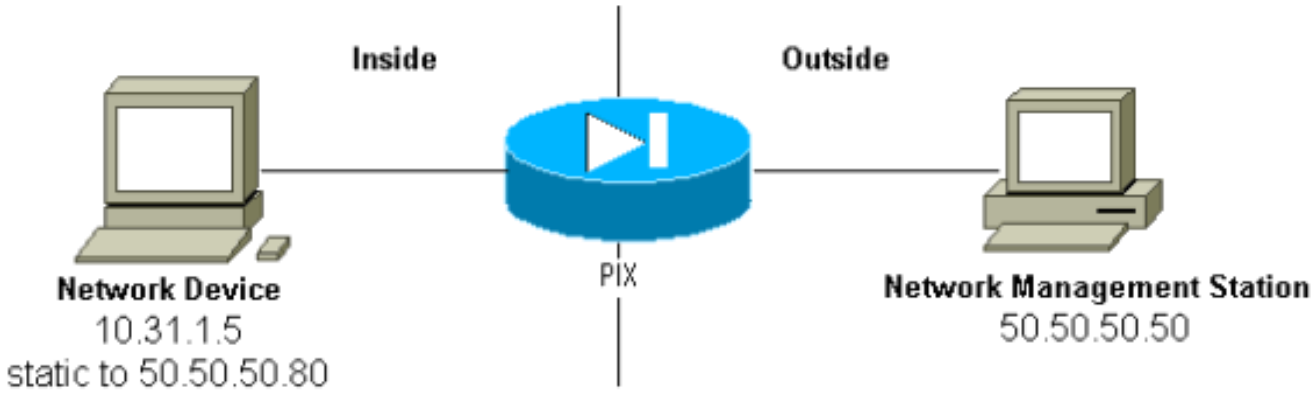
Se você usa listas de controle de acesso (ACLs), disponíveis no PIX 5.0 e posteriores, em vez de conduítes:

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

O PIX mostra:

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

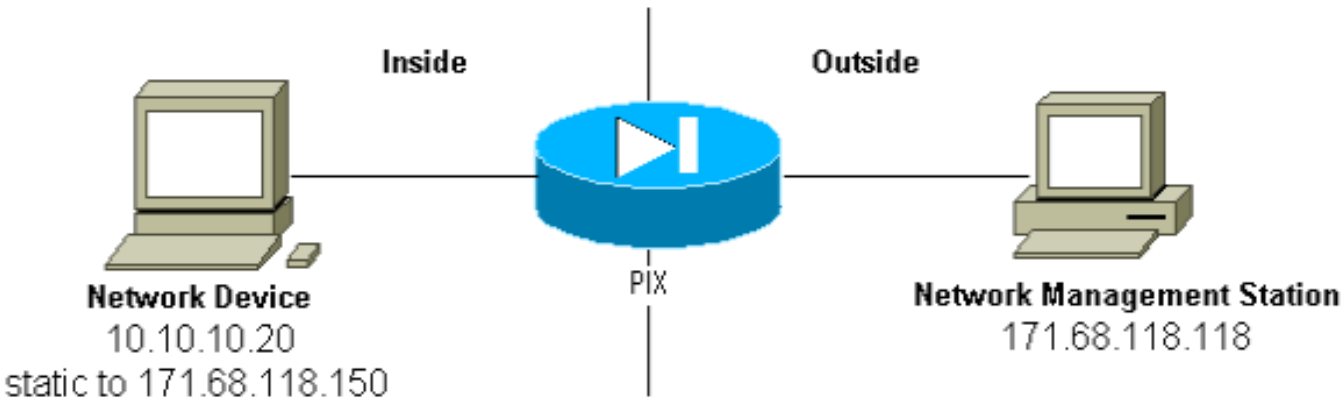
Armadilhas de dentro para fora



Por padrão, o tráfego de saída é permitido (na falta de listas de saída), e o PIX mostra:

```
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
```

Controlando de fora para dentro



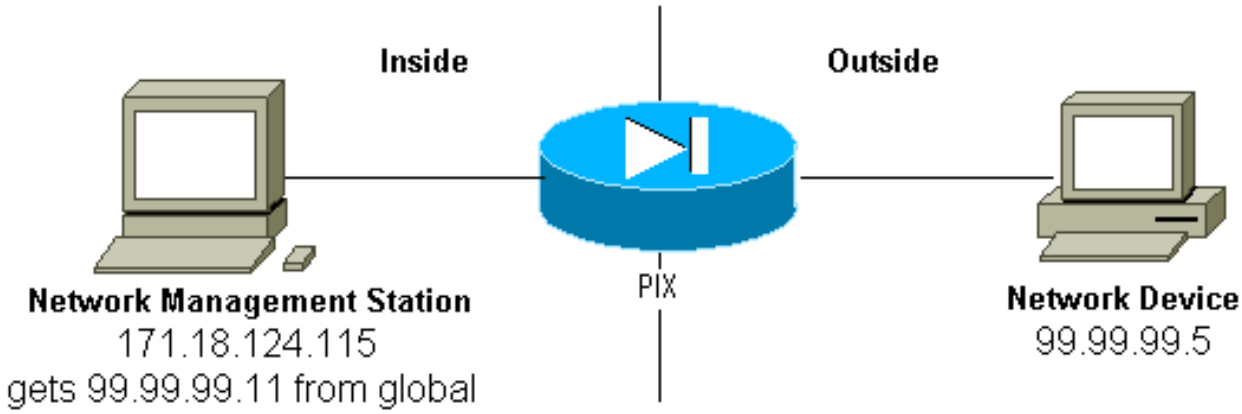
Para permitir a pesquisa de 171.68.118.118 para 10.10.10.20:

```
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
```

Se você usa ACLs, disponíveis no PIX 5.0 e posteriores, em vez de conduítes:

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

Controlando de dentro para fora



Por padrão, o tráfego de saída é permitido (na falta de listas de saída), e o PIX mostra:

```
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
```

SNMP para PIX/ASA

Suporte de MIB por versão

Estas são as versões do suporte MIB no PIX:

- Software PIX Firewall versões 4.0 a 5.1—Grupo de sistemas e interfaces de MIB-II (consulte RFC 1213) mas não os grupos AT, ICMP, TCP, UDP, EGP, transmissão, IP ou SNMP CISCO-SYSLOG-MIB-V1SMI.my.
- Software PIX Firewall versões 5.1.x e posteriores—MIBs anteriores e CISCO-MEMORY-POOL-MIB.my e a filial cfwSystem do CISCO-FIREWALL-MIB.my.
- Software PIX Firewall versões 5.2.x e posteriores — MIBs anteriores e a ipAddrTable do grupo IP.
- Software PIX Firewall versões 6.0.x e posteriores — MIBs anteriores e modificação do OID MIB-II para identificar PIX por modelo (e habilitar o suporte ao CiscoView 5.2). Os novos identificadores de objeto (OIDs) são encontrados no CISCO-PRODUC-MIB; por exemplo, o PIX 515 tem o OID 1.3.6.1.4.1.9.1.390.
- Software PIX Firewall versões 6.2.x e posteriores—MIBs anteriores e CISCO-PROCESS-MIB-V1SMI.my.
- Software PIX/ASA versão 7.x—MIBs e IF-MIB anteriores, SNMPv2-MIB, ENTITY-MIB,

CISCO-REMOTE-ACCESS-MONITOR-MIB, CISCO-CRYPTO-ACCELERATOR-MIB, ALTIGA-GLOBAL-REG .

Observação: a seção suportada do MIB PROCESS é a filial cpmCPUTotalTable da filial cpmCPU da filial ciscoProcessMIBObjects. Não há suporte para os produtos ciscoProcessMIBNotifications, ciscoProcessMIBconformance ou para as duas tabelas, cpmProcessTable e cpmProcessExtTable, no produto cpmProcess do produto ciscoProcessMIBObjects do MIB.

Ativando o SNMP no PIX/ASA

Emita estes comandos para permitir pesquisas/consultas e armadilhas no PIX:

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

As versões do software PIX 6.0.x e mais recentes permitem maior granularidade com relação a armadilhas e consultas.

```
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.
```

As versões 7.x do software PIX/ASA permitem mais granularidade em relação a armadilhas e consultas.

```
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.
```

Observação: especifique **interceptação** ou **pesquisa** se quiser limitar o NMS a receber apenas interceptações ou navegação (pesquisa). Por padrão, o NMS pode usar ambas as funções.

As interceptações SNMP (traps) são enviadas na porta UDP 162 por padrão. Você pode alterar o número da porta com a palavra-chave **udp-port**.

SNMP para PIX/ASA - Pesquisa

As variáveis que o PIX retorna dependem do suporte de mib na versão. Um exemplo de saída de um snmpwalk de um PIX executado6.2.1 está no final deste documento. As versões anteriores do software retornam somente os valores de mib anotados anteriormente.

SNMP para PIX/ASA - Armadilhas

Observação: um OID SNMP para PIX Firewall é exibido em interceptações de eventos SNMP enviadas do PIX Firewall. O OID 1.3.6.1.4.1.9.1.227 foi usado como o OID do sistema do PIX Firewall até a versão 6.0 do software PIX. Os novos OIDs específicos para o modelo são

encontrados no CISCO-PRODUCTS-MIB.

Emita estes comandos para ativar as interceptações no PIX:

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

Traps Versão 4.0 Até 5.1

Ao usar o PIX Software 4.0 e posterior, você pode gerar estas armadilhas:

```
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
```

Alterações de armadilha (PIX 5.1)

No software PIX versão 5.1.1 e posterior, os níveis de interceptação (trapping) são separados dos níveis de syslog para as interceptações de syslog. O PIX ainda envia armadilhas de syslog, mas mais granularidade pode ser configurada. Este exemplo de arquivo raw trapd.log (e este é o mesmo para o HP OpenView [HPOV] ou Netview) incluiu 3 armadilhas de link_up e 9 armadilhas de syslog, com 7 IDs de syslog diferentes: 101003, 104001, 111005, 111007, 199002, 302005, 305002.

Exemplo de trapd.log

```
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
```

Descrição de cada interceptação - 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
```

Exemplos de Nível de Gravidade syslog

Eles são reproduzidos com base na documentação para ilustrar as sete mensagens.

```
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.
```

Interpretar os níveis de gravidade do syslog

Nível	Significado
0	Sistema inutilizável - emergência
1	Tomar ações imediatas - alerta
2	Condição crítica - crítica
3	Mensagem de erro - erro
4	Mensagem de aviso - aviso
5	Condição normal, mas significativa -

	notificação
6	Informativo - informativo
7	Mensagem de depuração - debug

Configure o PIX 5.1 e posterior para um subconjunto de armadilhas

Se a configuração do PIX tiver:

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

as únicas armadilhas geradas são as armadilhas padrão: inicialização a frio, link ativo e link inativo (não syslog).

Se a configuração do PIX tiver:

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

em seguida, todos os desvios padrão e de syslog são gerados. Em nosso exemplo, essas são entradas de syslog 101003, 104001, 111005, 11007, 199002, 302005 e 305002, e qualquer outro syslog saída de log do PIX gerado. Como o histórico de registro definido para depuração e esses números de interceptação (trapping) estão nos níveis de notificação, alerta e informação, o nível de depuração inclui estes:

Se a configuração do PIX tiver:

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

Todos as padrão e todas as armadilhas no nível abaixo de depuração são geradas. Se o comando **logging history notification** for usado, isso incluirá todas as interceptações de syslog nos níveis de emergência, alerta, crítico, erro, aviso e notificação (mas não nos níveis informativos ou de depuração). No nosso caso, 11005, 111007, 101003 e 104001 (e quaisquer outros que o PIX gerasse em uma rede ativa) seriam incluídos.

Se a configuração do PIX tiver:

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

as mensagens 305002, 302005 e 111005 não serão geradas. Com o PIX definido para **depuração de histórico de registro**, você vê mensagens 104001, 101003, 111007, 199002 e todas as outras

mensagens PIX, mas não as 3 listadas (305002, 3020 05, 11005).

Configurar PIX/ASA 7.x para um subconjunto de armadilhas

Se a configuração do PIX tiver:

```
snmp-server host
```

as únicas armadilhas geradas são as armadilhas padrão: autenticação, inicialização a frio, link ativo e link inativo (não syslog).

A configuração restante é semelhante à versão do software PIX 5.1 e posterior, exceto no PIX/ASA versão 7.x , o comando **snmp-server enable traps** tem opções adicionais como **ipsec**, **acesso remoto** e **entidade**

Observação: consulte a seção Ativação do SNMP de Monitoramento do Security Appliance para saber mais sobre as interceptações SNMP no PIX/ASA

Problemas de SNMP

Descoberta PIX

Se o PIX responder a uma consulta SNMP e relatar seu OID como 1.3.6.1.4.1.9.1.227, ou no PIX Firewall Software versões 6.0 ou posterior, como um ID listado no CISCO-PRODUC-MIB para esse modelo, o PIX está funcionando como projetado.

Em versões do código PIX anteriores à 5.2.x quando havia suporte adicionado para ipAddrTable do grupo IP, as estações de gerenciamento de rede podem não conseguir desenhar o PIX no mapa como um PIX. Uma estação de gerenciamento de rede deve sempre ser capaz de detectar o fato de que o PIX existe se for capaz de fazer ping no PIX, mas pode não desenhá-lo como um PIX - uma caixa preta com 2 luzes. Além de precisar de suporte para ipAddrTable do grupo IP, HPOV, Netview e a maioria das outras estações de gerenciamento de rede, o OID que está sendo retornado pelo PIX é o de um PIX para que o ícone apropriado seja exibido.

O suporte do CiscoView para gerenciamento de PIX foi adicionado ao CiscoView 5.2; A versão 6.0.x do PIX também é necessária. Em versões anteriores do PIX, um aplicativo de gerenciamento de terceiros permite que o gerenciador de nó de rede do HPOV identifique os PIX Firewalls e sistemas que executam o PIX Firewall Manager.

Descubra os dispositivos dentro do PIX

Se o PIX estiver configurado corretamente, ele passará consultas SNMP e traps de fora para dentro. Como a Conversão de Endereço de Rede (NAT - Network Address Translation) é normalmente configurada no PIX, seria necessário estática para fazer isso. O problema ocorre

quando a estação de gerenciamento de rede faz um snmpwalk do endereço público, que fica estático em um endereço privado na rede, o cabeçalho externo do pacote não concorda com a informação do ipAddrTable. Aqui, 171.68.118.150 é caminhado, que é estático para 10.10.10.20 dentro do PIX e você pode ver onde o dispositivo 171.68.118.150 relata que ele tem duas interfaces: 10.10.10.20 e 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
```

Isso fará sentido para uma estação de gerenciamento de rede? Provavelmente não. O mesmo problema estará presente para armadilhas: se a interface 10.31.1.50 fosse desativada, o dispositivo 171.68.118.150 relataria que a interface 10.31.1.50 estava inativa.

Outro problema ao tentar gerenciar uma rede interna de fora é "desenhar" a rede. Se a estação de gerenciamento for Netview ou HPOV, esses produtos usarão um daemon "netmon" para ler as tabelas de rotas dos dispositivos. A tabela de rotas é usada na descoberta. O PIX não suporta o suficiente de RFC 1213 para devolver uma tabela de roteamento a uma estação de gerenciamento de rede e, por motivos de segurança, isso não é uma boa ideia de qualquer forma. Enquanto os dispositivos dentro do PIX informam suas tabelas de rota quando o estático é consultado, todos os dispositivos de IP público (estáticos) informam todas as interfaces privadas. Se os outros endereços privados dentro do PIX não tiverem estática, eles não poderão ser consultados. Se eles têm estática, a estação de gerenciamento de rede não tem como saber quais são as estatísticas.

Descobrir dispositivos fora do PIX

Como uma estação de gerenciamento de rede dentro do PIX consulta um endereço público que relata interfaces "públicas", a descoberta de fora para dentro não se aplica.

Aqui, 171.68.118.118 estava dentro e 10.10.10.25 estava lá fora. Quando 171.68.118.118 caminhou 10.10.10.25, a caixa relatou corretamente suas interfaces, ou seja, o cabeçalho é o mesmo que dentro do pacote:

```
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
```

snmpwalk de PIX versão 6.2

O **comando snmpwalk -c public <pix_ip_address>** foi usado em uma estação de gerenciamento HPOV para executar snmpwalk. Todos os MIBs disponíveis para o PIX 6.2 foram carregados antes da execução do snmpwalk.

```
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.
```

Informações a serem coletadas se você abrir um caso de TAC

Se você ainda precisar de assistência após concluir as etapas de solução de problemas neste documento e quiser abrir um caso no Cisco TAC, certifique-se de incluir essas informações para solucionar problemas do PIX Firewall.

- Descrição do problema e detalhes relevantes de topologia
- Solução de problemas executada antes de abrir o caso
- Saída do comando **show tech-support**
- Saída do comando show log após a execução com o comando de depuração de registro colocado em buffer ou capturas do console que demonstram o problema (se disponível)

Anexe os dados coletados à sua ocorrência em formato de texto simples descompactado (.txt). Você pode anexar informações ao seu caso fazendo o upload usando a TAC Service Request Tool (somente clientes registrados). Se não conseguir acessar a Case Query Tool, você poderá enviar as informações em um anexo de e-mail para attach@cisco.com com o número do caso na linha de assunto da sua mensagem.

Informações Relacionadas

- Referências do comando Cisco Secure PIX Firewall
- Suporte ao produto do software Cisco PIX Firewall
- Solicitação de comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems