Uso de SNMP con los Dispositivos de Seguridad PIX/ASA

Contenido

Introducción

Puede monitorear los eventos del sistema en el PIX utilizando el Protocolo de administración de red simple (SNMP). Este documento describe cómo utilizar SNMP con el PIX, lo que incluye:

- Comandos para ejecutar SNMP *a través* del PIX o *hacia* el PIX
- Resultado PIX de ejemplo
- Compatibilidad con Base de información de administración (MIB) en la versión 4.0 y posteriores del software PIX
- Niveles de trampa
- Ejemplos de nivel de gravedad de syslog
- Problemas de detección de dispositivos PIX y SNMP.

Nota: El puerto para snmpget/snmpwalk es UDP/161. El puerto para trampas SNMP es UDP/162.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Secure PIX Firewall Software Releases 4.0 y 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.

Productos Relacionados

Esta configuración también se puede utilizar con Cisco Adaptive Security Appliance (ASA) versión 7.x.

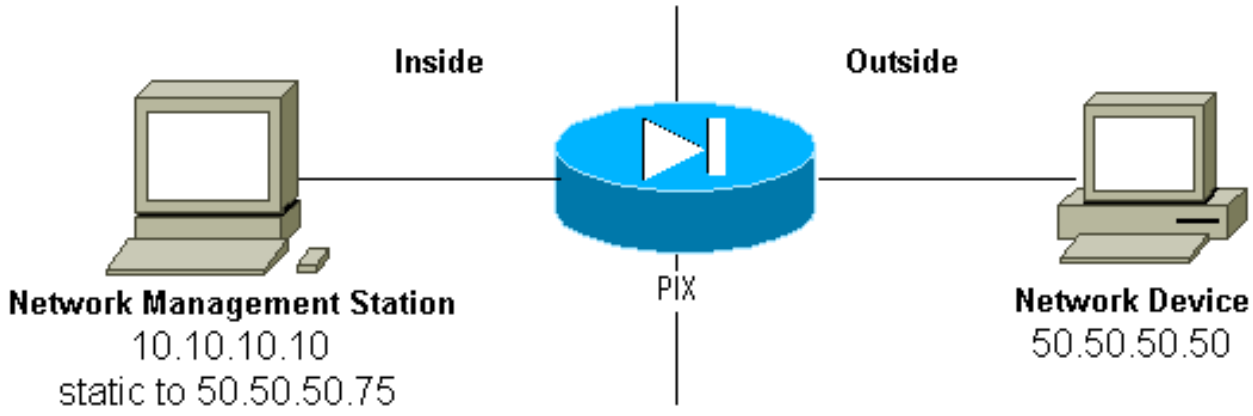
Convenciones

Se han replegado algunas de las líneas de resultado y datos de registro en este documento por razones de espacio.

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

SNMP a través de PIX/ASA

Trampas de afuera hacia adentro



Para permitir trampas desde 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
```

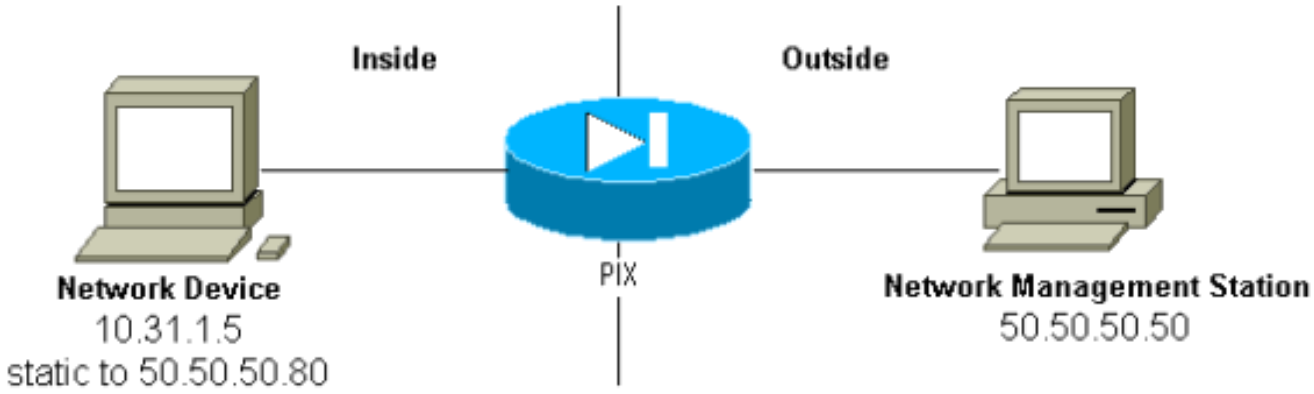
Si utiliza listas de control de acceso (ACL), disponibles en PIX 5.0 y posteriores, en lugar de conductos:

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

El PIX muestra:

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

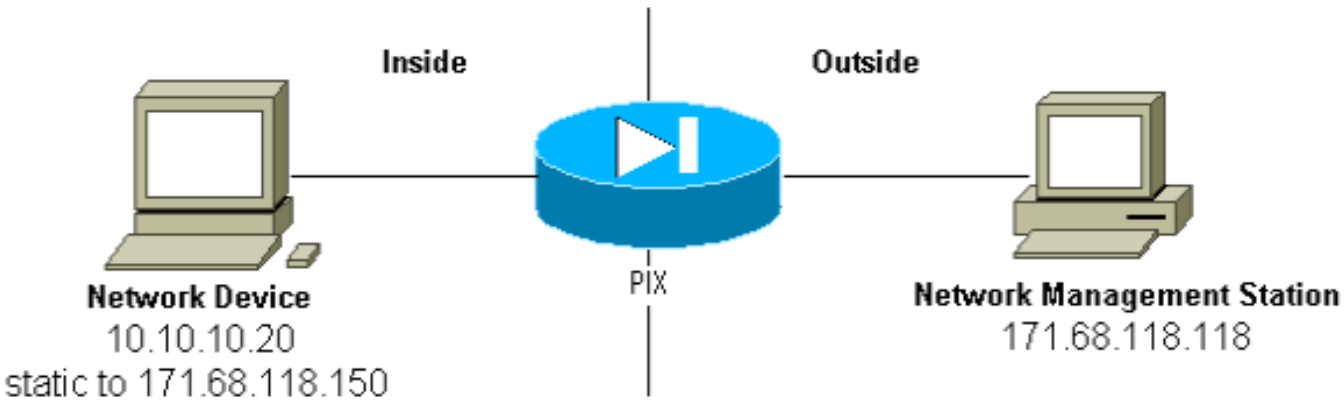
Trampas de adentro hacia afuera



El tráfico de salida se permite de forma predeterminada (en ausencia de listas de salida) y el PIX muestra:

```
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
```

Consulta de adentro hacia afuera



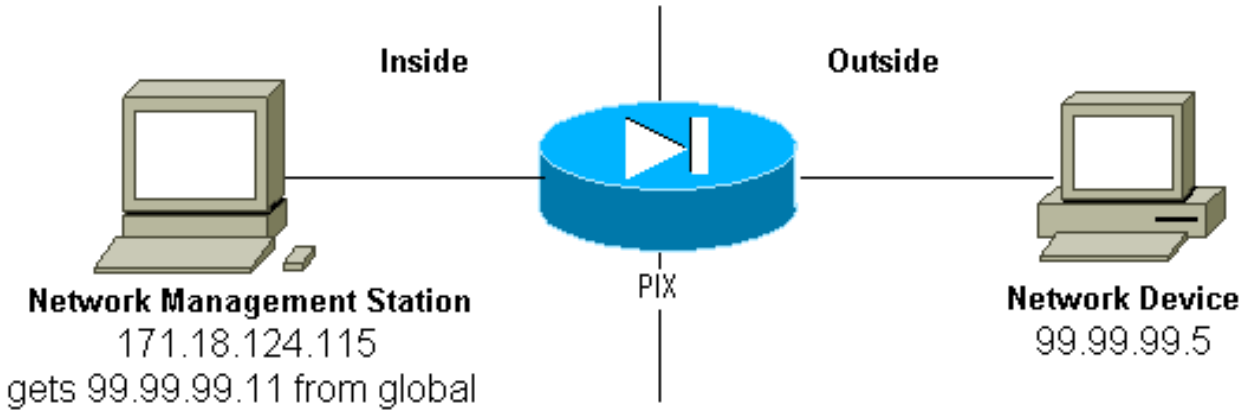
Para permitir el sondeo de 171.68.118.118 a 10.10.10.20:

```
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
```

Si utiliza ACL, disponibles en PIX 5.0 y posteriores, en lugar de conductos:

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

Consulta de adentro hacia afuera



El tráfico de salida se permite de forma predeterminada (en ausencia de listas de salida) y el PIX muestra:

```
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 a PIX/ASA

Soporte MIB por versión

Estas son las versiones del soporte MIB en el PIX:

- PIX Firewall Software Versiones 4.0 hasta 5.1—Grupos de Sistema e Interfaz de MIB-II (consulte RFC 1213) pero no los grupos AT, ICMP, TCP, UDP, EGP, transmisión, IP o SNMP CISCO-SYSLOG-MIB-V1SMI.my.
- Software PIX Firewall Versiones 5.1.x y posteriores: MIB anteriores y CISCO-MEMORY-POOL-MIB.my y la rama cfwSystem de CISCO-FIREWALL-MIB.my.
- Software PIX Firewall Versiones 5.2.x y posteriores: MIB anteriores y la ipAddrTable del grupo IP.
- Software PIX Firewall Versiones 6.0.x y posteriores: MIB anteriores y modificación del OID MIB-II para identificar el PIX por modelo (y habilitar el soporte de CiscoView 5.2). Los nuevos identificadores de objeto (OID) se encuentran en CISCO-PRODUCTS-MIB; por ejemplo, el PIX 515 tiene el OID 1.3.6.1.4.1.9.1.390.
- PIX Firewall Software Versiones 6.2.x y posteriores: MIB anteriores y CISCO-PROCESS-MIB-V1SMI.my.

- Software PIX/ASA versión 7.x: MIB anteriores y IF-MIB, SNMPv2-MIB, ENTITY-MIB, CISCO-REMOTE-ACCESS-MONITOR-MIB, CISCO-CRYPTO-ACCELERATOR-MIB, ALTIGA-GLOBAL-REG.

Nota: La sección soportada de PROCESS MIB es la rama cpmCPUTotalTable de la rama cpmCPU de la rama ciscoProcessMIBObjects. En la rama cpmProcess de la rama ciscoProcessMIBObjects de la MIB no existe soporte para las ramas ciscoProcessMIBNotifications y ciscoProcessMIBconformance ni para las dos tablas cpmProcessTable y cpmProcessExtTable.

Activación de SNMP en PIX/ASA

Ejecute estos comandos para permitir sondeos/consultas y trampas en el 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
```

Las versiones 6.0x y posteriores del software PIX permiten mayor granularidad con respecto a las notificaciones de trampa y a las 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.
```

Las versiones 7.x del software PIX/ASA permiten una mayor granularidad con respecto a las trampas y las 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.
```

Nota: Especifique **trampa** o **sondeo** si desea limitar el NMS a recibir sólo trampas o navegar (sondeo) solamente. De forma predeterminada, el NMS puede utilizar ambas funciones.

Las trampas SNMP se envían en el puerto UDP 162 de forma predeterminada. Puede cambiar el número de puerto con la palabra clave **udp-port**.

SNMP a PIX/ASA - Sondeo

Las variables que devuelve el PIX dependen del soporte mib en la versión. Al final de este documento se encuentra un ejemplo de salida de una snmpwalk de un PIX que ejecuta 6.2.1. Las versiones anteriores del software devuelven solamente los valores mib previamente mencionados.

SNMP a PIX/ASA - Trampas

Nota: Un OID SNMP para Firewall PIX se muestra en las trampas de eventos SNMP enviadas desde el Firewall PIX. OID 1.3.6.1.4.1.9.1.227 se utilizó como OID del sistema PIX Firewall hasta la versión 6.0 del software PIX. Las nuevas OID específicas del modelo se encuentran en CISCO-PRODUCTS-MIB.

Ejecute estos comandos para activar las trampas en el PIX:

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

Trampas Versión 4.0 Hasta 5.1

Cuando utiliza PIX Software 4.0 y posterior, puede generar estas trampas:

```
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
```

Cambios de trampas (PIX 5.1)

En la versión 5.1.1 y posteriores del software PIX, los niveles de trampa se separan de los niveles de syslog para las trampas de syslog. El PIX todavía envía trampas de syslog, pero se puede configurar más granularidad. Este ejemplo de archivo trapd.log sin procesar (y esto es lo mismo para HP OpenView [HPOV] o Netview) incluía 3 trampas link_up y 9 trampas syslog, con 7 identificadores syslog diferentes: 101003, 104001, 111005, 111007, 199002, 302005, 305002.

Ejemplo 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
```

Descripción de cada trampa - 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
```

Ejemplos de nivel de gravedad de syslog

Éstos se reproducen desde la documentación para ilustrar los siete mensajes.

```
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 los niveles de gravedad de syslog

'Nivel'	Significado
0	Sistema inutilizable, emergencia
1	Realizar una acción inmediatamente - alertar
2	Condición crítica: crítica
3	Mensaje de error - error

4	Mensaje de advertencia - advertencia
5	Condición normal pero significativa - notificación
6	Informativo - informativo
7	Mensaje de depuración - debug

Configuración de PIX 5.1 y posteriores para un subconjunto de trampas

Si la configuración de PIX tiene:

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

las únicas trampas que se generan son las trampas estándar: inicio en frío, enlace hacia arriba y enlace hacia abajo (no syslog).

Si la configuración de PIX tiene:

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

entonces se generan todas las trampas estándar y de syslog. En nuestro ejemplo, estas son entradas syslog 101003, 104001, 111005, 111007, 199002, 302005 y 305002, y cualquier otro sistema salida de registro del PIX generado. Debido a que el historial de registro establecido para la depuración y estos números de trampa están en los niveles de notificación, alerta e información, el nivel de depuración incluye lo siguiente:

Si la configuración de PIX tiene:

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

entonces se generan todos los estándares y todas las trampas en el nivel siguiente a la depuración. Si se utiliza el comando **logging history notification**, esto incluiría todas las trampas de syslog en los niveles de emergencia, alerta, crítica, error, advertencia y notificación (pero no en los niveles de información o depuración). En nuestro caso, se incluirían 111005, 111007, 101003 y 104001 (y cualquier otro que el PIX genere en una red en funcionamiento).

Si la configuración de PIX tiene:

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

entonces los mensajes 305002, 302005, 111005 no se producen. Con el PIX configurado para **logging history debug**, usted ve los mensajes 104001, 101003, 111007, 199002 y todos los demás mensajes PIX, pero no los 3 enumerados (305002, 30200000 111005).

Configuración de PIX/ASA 7.x para un subconjunto de trampas

Si la configuración de PIX tiene:

```
snmp-server host
```

las únicas trampas que se generan son las trampas estándar: autenticación, inicio en frío, enlace activo y enlace inactivo (no syslog).

La configuración restante es similar a la versión 5.1 y posterior del software PIX, excepto en la versión 7.x de PIX/ASA , el comando **snmp-server enable traps** tiene opciones adicionales como **ipsec**, **remote-access** y **entity**

Nota: Consulte la sección Habilitación de SNMP de Monitoreo del Dispositivo de Seguridad para obtener más información sobre las trampas SNMP en PIX/ASA

Problemas de SNMP

Detección de PIX

Si el PIX responde a una consulta SNMP e informa su OID como 1.3.6.1.4.1.9.1.227, o en las versiones 6.0 o posteriores del Software PIX Firewall, como un ID enumerado en el CISCO-PRODUCTS-MIB para ese modelo, entonces el PIX funciona como diseñado.

En las versiones del código PIX anteriores a 5.2.x cuando se agregó soporte para la ipAddrTable del grupo IP, las estaciones de administración de red podrían no ser capaces de dibujar el PIX en el mapa como un PIX. Una estación de administración de red siempre debería ser capaz de detectar el hecho de que el PIX existe si es capaz de hacer ping al PIX, pero podría no dibujarlo como un PIX - una caja negra con 2 luces. Además de necesitar soporte de ipAddrTable del grupo IP, HPOV, Netview y la mayoría de las otras estaciones de administración de red necesitan entender que el OID que devuelve el PIX es el de un PIX para que aparezca el icono adecuado.

El soporte de CiscoView para la administración de PIX se agregó en CiscoView 5.2; También se requiere la versión 6.0.x de PIX. En las versiones anteriores de PIX, una aplicación de administración de terceros permite al administrador de nodos de red HPOV identificar los firewalls PIX y los sistemas que ejecutan el PIX Firewall Manager.

Descubra los dispositivos dentro del PIX

Si el PIX está configurado correctamente, pasa las consultas SNMP y las trampas de afuera hacia

adentro. Debido a que la traducción de direcciones de red (NAT) suele configurarse en el PIX, se necesitarían estadísticas para hacerlo. El problema ocurre cuando la estación de administración de red realiza una snmpwalk de la dirección pública, que es estática a una dirección privada dentro de la red, el encabezado externo del paquete no coincide con la información en la ipAddrTable. Aquí se avanza 171.68.118.150, que es estática a 10.10.10.20 dentro del PIX y puede ver dónde el dispositivo 171.68.118.150 informa que tiene dos interfaces: 10.10.10.20 and 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
```

¿Tendrá sentido esto para una estación de administración de redes? Probablemente no. El mismo problema estará presente para las trampas: si la interfaz 10.31.1.50 se desactivara, el dispositivo 171.68.118.150 informaría que la interfaz 10.31.1.50 estaba inactiva.

Otro problema al intentar gestionar una red interna desde el exterior es "dibujar" la red. Si la estación de administración es Netview o HPOV, estos productos utilizan un daemon "netmon" para leer las tablas de ruta de los dispositivos. La tabla de rutas se utiliza en la detección. El PIX no soporta lo suficiente de RFC 1213 para devolver una tabla de ruteo a una estación de administración de red, y por razones de seguridad, esta no es una buena idea en cualquier caso. Mientras los dispositivos dentro del PIX informan sus tablas de rutas cuando se consulta la estática, todos los dispositivos IP públicos (estáticos) informan todas las interfaces privadas. Si las otras direcciones privadas dentro del PIX no tienen estática, no se pueden consultar. Si tienen estática, la estación de administración de red no tiene forma de saber cuáles son las estadísticas.

Descubra dispositivos fuera del PIX

Dado que una estación de administración de red dentro del PIX consulta una dirección pública que informa de interfaces "públicas", el descubrimiento fuera de los problemas internos no se aplica.

Aquí, 171.68.118.118 estaba adentro y 10.10.10.25 estaba afuera. Cuando 171.68.118.118 caminó 10.10.10.25, la caja informó correctamente de sus interfaces, es decir, el encabezado es el mismo que dentro del paquete:

```
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
```

Versión 6.2 snmpwalk of PIX

El comando **snmpwalk -c public <pix_ip_address>** se utilizó en una estación de administración de HPOV para realizar snmpwalk. Todas las MIB disponibles para PIX 6.2 se cargaron antes de realizar la 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.
```

Información para recopilar si abre un caso del TAC

Si todavía necesita ayuda después de completar los pasos de solución de problemas en este documento y

desea abrir un caso con el TAC de Cisco, asegúrese de incluir esta información para resolver el problema de su Firewall PIX.
• Descripción del problema y detalles relevantes de la topología • Resolución de problemas realizada antes de abrir el caso • Resultado del comando show tech-support • Resultado del comando show log después de la ejecución con el comando logging buffered debugging o capturas de consola que muestran el problema (si están disponibles) Adjunte los datos recopilados para su caso en un texto sin formato (.txt), sin compactar. Puede adjuntar información a su caso transfiriéndola mediante Herramienta de Solicitud de Servicio TAC (sólo clientes registrados). Si no puede acceder a la herramienta Case Query Tool, puede enviar la información en un archivo adjunto de correo electrónico a attach@cisco.com con su número de caso en el asunto del mensaje.

Información Relacionada

- Referencias de Comandos de Cisco Secure PIX Firewall
- Soporte de Productos del Software Cisco PIX Firewall
- Solicitud de comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems