Usando el SNMP con el PIX/ASA de los dispositivos de seguridad

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 de ejecutar el SNMP *con el* PIX o al PIX
- Resultado PIX de ejemplo
- Soporte de Base de información de administración (MIB) en el software PIX versión 4.0 y posterior
- Niveles de trampa
- ejemplos llanos de la gravedad de Syslog
- Problemas de detección de dispositivos PIX y SNMP.

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

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en los Software Release 4.0 y Posterior del Cisco Secure PIX Firewall.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Esta configuración se puede también utilizar con la versión 7.x adaptante del dispositivo de seguridad de Cisco (ASA).

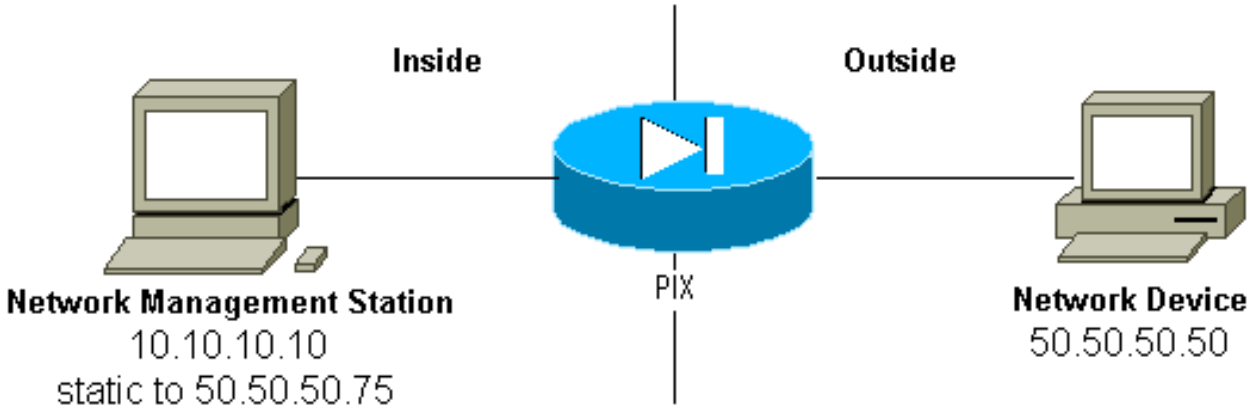
Convenciones

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 con el PIX/ASA

Trampas de afuera hacia adentro



Para permitir los desvíos adentro 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
```

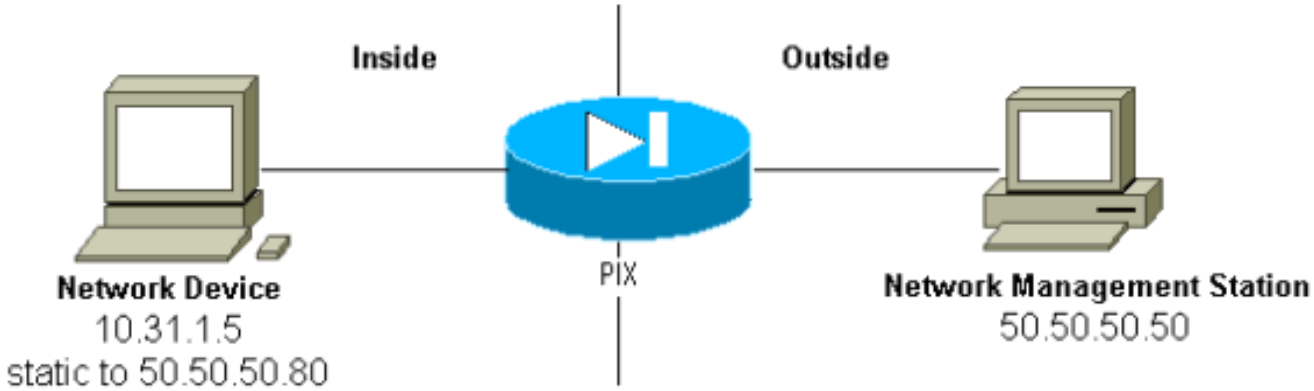
Si usted utiliza el Listas de control de acceso (ACL), disponible en PIX 5.0 y posterior, en vez de los conductos:

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

Las demostraciones PIX:

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

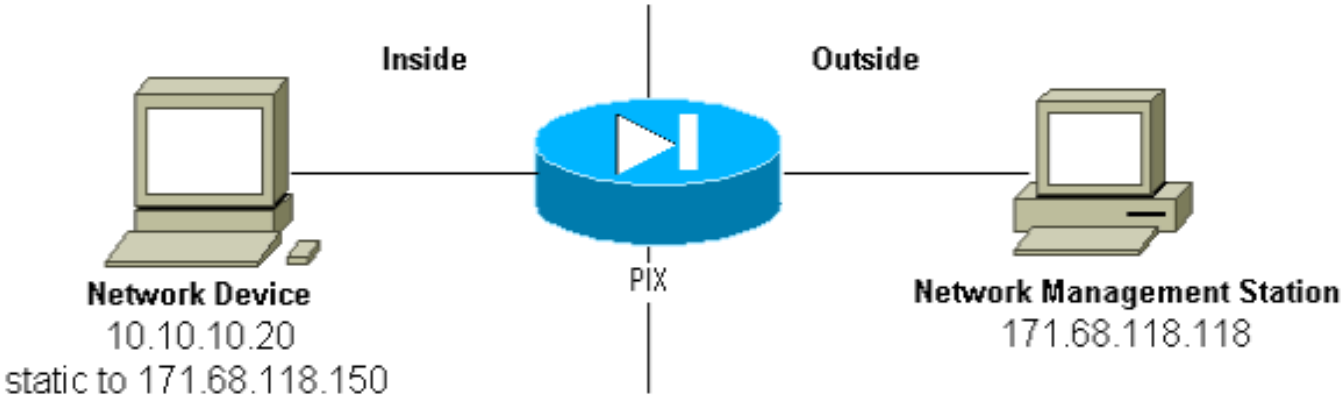
Trampas de adentro hacia afuera



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 sondear de 171.68.118.118 a 10.10.10.20:

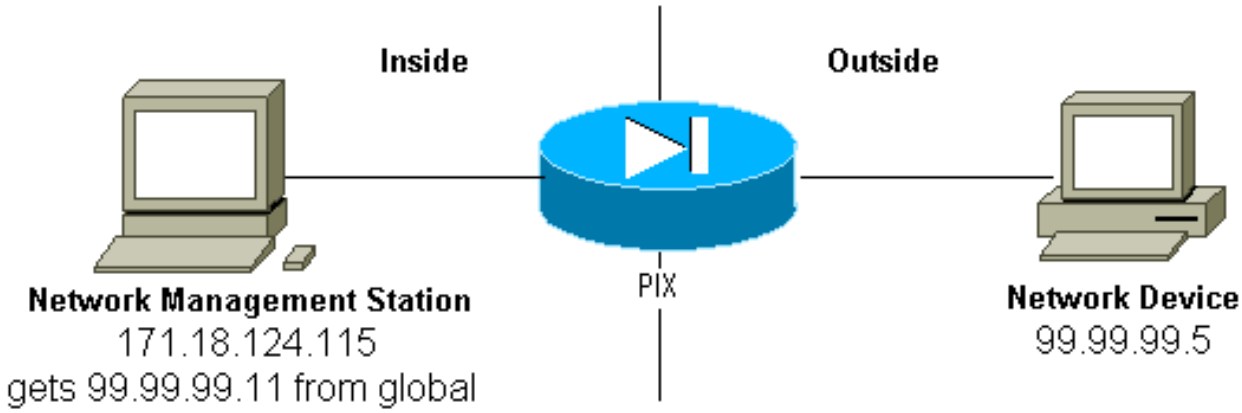
```
static (inside,outside) 171.68.118.150 10.10.10.20 netmask 255.255.255.255 0 0 conduit permit
udp host 171.68.118.150 eq snmp host 171.68.118.118
```

Si usted utiliza los ACL, disponibles en PIX 5.0 y posterior, en vez de los 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 al PIX/ASA

Soporte MIB por versión

Éstas son las versiones del soporte de MIB en el PIX:

- Versiones 4.0 del Software PIX Firewall hasta 5.1 — Sistema y grupos de interfaces de MIB-II (refiera al RFC 1213) pero no EN, de ICMP, de TCP, de UDP, de EGP, de transmisión, de los grupos CISCO-SYSLOG-MIB-V1SMI.my IP, o SNMP.
- Versiones 5.1.x del Software PIX Firewall y posterior — MIB y CISCO-MEMORY-POOL-MIB.my anterior y la bifurcación del cfwSystem del CISCO-FIREWALL-MIB.my.
- Versiones 5.2.x del Software PIX Firewall y posterior — MIB anterior y el ipAddrTable del grupo IP.
- Versiones 6.0.x del Software PIX Firewall y posterior — MIB y modificación anteriores del MIB-II OID para identificar el PIX por el modelo (y habilitar el soporte del CiscoView 5.2). Los nuevos identificadores de objeto (OID) se encuentran en el CISCO-PRODUCTS-MIB; por ejemplo, el PIX 515 tiene el OID 1.3.6.1.4.1.9.1.390.
- Versiones 6.2.x del Software PIX Firewall y posterior — MIB y CISCO-PROCESS-MIB-V1SMI.my anteriores.
- Versión de software 7.x del PIX/ASA — MIB y IF-MIB anteriores, SNMPv2-MIB, ENTITY-MIB, CISCO-REMOTE-ACCESS-MONITOR-MIB, CISCO-CRYPTO-ACCELERATOR-MIB, ALTIGA-GLOBAL-REG.

Nota: La sección admitida de PROCESS MIB es la rama cpmCPUTotalTable de la rama cpmCPU perteneciente a 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.

Girar el SNMP en el PIX/ASA

Publique estos comandos de permitir sondear/las interrogaciones y los desvíos 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 de software 7.x del PIX/ASA permiten más granularity con respecto a los desvíos y a las interrogaciones.

```
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 el **desvío** o **sondee** si usted quiere limitar el NMS a recibir los desvíos solamente o a la ojeada (interrogación) solamente. Por abandono, el NMS puede utilizar ambas funciones.

El SNMP traps se envía en el puerto 162 UDP por abandono. Usted puede cambiar el número del puerto con la palabra clave del UDP-**puerto**.

SNMP al PIX/ASA - El sondear

Las variables que las devoluciones PIX dependen del soporte de MIB en la versión. Una salida de ejemplo de un snmpwalk de un PIX que runs6.2.1 está en el extremo de este documento. Versiones anteriores de la vuelta del software solamente los valores previamente conocidos MIB.

SNMP al PIX/ASA - Desvíos

Nota: Un SNMP OID para las visualizaciones del firewall PIX en los desvíos del evento SNMP enviados del firewall PIX. El OID 1.3.6.1.4.1.9.1.227 fue utilizado como el sistema OID del firewall PIX hasta la versión de software PIX 6.0. Las nuevas OID específicas del modelo se encuentran en CISCO-PRODUCTS-MIB.

Publique estos comandos de girar los desvíos en el PIX:

```
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
```

Atrapa la versión 4.0 hasta 5.1

Cuando usted utiliza el software PIX 4.0 y posterior, usted puede generar estos desvíos:

```
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 de software PIX 5.1.1 y posterior, los niveles de trampa se separan de los niveles del Syslog para las trampas de Syslog. El PIX todavía envía las trampas de Syslog, pero más granularity puede ser configurado. Desvíos incluidos sin procesar de este del ejemplo de trapd.log link_up del archivo (y éste es lo mismo para el [HPOV] o el Netview del HP OpenView) 3 y 9 trampas de Syslog, con 7 diversos ID de syslogs: 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 desvío - 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.
```

Interprete los niveles de la 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	Normal pero estado significativo - notificación
6	Informativo - informativo
7	Mensaje del debug - debug

Configure PIX 5.1 y posterior para un subconjunto de desvíos

Si la configuración PIX tiene:

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

los únicos desvíos se generan que son los desvíos estándar: arranque en frío, link ascendente y link abajo (no Syslog).

Si la configuración PIX tiene:

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

entonces se generan todas las trampas estándar y de syslog. En nuestro ejemplo, éstas son las entradas de syslog 101003, 104001, 111005, 111007, 199002, 302005, y 305002, y sea cual sea la otra salida de Syslog el PIX generó. Porque el conjunto del historial del registro para el debug y estos números de trampa están en la notificación, la alerta, y los niveles informativos, el debug del nivel incluye éstos:

Si la configuración 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 utilizan al **comando logging history notification**, éste incluiría todas las trampas de Syslog en la emergencia, la alerta, crítico, error, advertencia, y los niveles de notificación (pero no

informativo o los niveles de debug). En nuestro caso, 111005, 111007, 101003, y 104001 (y sea cual sea otros el PIX generarían en una red en funcionamiento) serían incluidos.

Si la configuración 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 fijado para el **logging history debug**, usted ve los mensajes 104001, 101003, 111007, 199002, y el resto de los mensajes PIX, pero no los 3 enumerados (305002, 302005, 111005).

Configure el PIX/ASA 7.x para un subconjunto de desvíos

Si la configuración PIX tiene:

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

los únicos desvíos se generan que son los desvíos estándar: autenticación, arranque en frío, link ascendente y link abajo (no Syslog).

La Configuración restante es similar pues la versión de software PIX 5.1 y posterior, excepto en la versión 7.x del PIX/ASA, el **comando snmp-server enable traps** tiene opciones adcionales tales como **IPSec**, **acceso remoto** y **entidad**

Nota: Refiera a la sección SNMP que habilita de monitorear el dispositivo de seguridad para aprender más sobre el SNMP traps en el PIX/ASA

Problemas de SNMP

Detección de PIX

Si el PIX responde a una interrogación SNMP y señala su OID como 1.3.6.1.4.1.9.1.227, o en las versiones 6.0 del Software PIX Firewall o más adelante, como ID enumerado en el CISCO-PRODUCTS-MIB para ese modelo, después el PIX está trabajando según lo diseñado.

En las versiones del código de PIX antes de 5.2.x cuando había soporte agregado para el ipAddrTable del grupo IP, las estaciones de administración de red no pudieron poder drenar el PIX en la correspondencia como PIX. Una estación de administración de red debe siempre poder detectar el hecho de que existe el PIX si puede hacer ping el PIX, pero puede ser que no lo drene como PIX - un Black Box con 2 luces. Además de necesitar el soporte del ipAddrTable del grupo IP, el HPOV, el Netview, y la mayoría de las otras estaciones de administración de red necesitan entender que el OID que es vuelto por el PIX sea el de un PIX para que aparezca el icono apropiado.

El Soporte de CiscoView para la administración de PIX fue agregado en el CiscoView 5.2; La versión de PIX 6.0.x también se requiere. En versiones de PIX anteriores, una aplicación de administración de terceros permite que el Administrador de nodos de red del HPOV identifique los Firewall PIX y los sistemas que ejecuten el PIX Firewall Manager.

Descubra los dispositivos dentro del PIX

Si el PIX se configura correctamente, pasa las interrogaciones y los desvíos SNMP del exterior al interior. Porque el Network Address Translation (NAT) se configura generalmente en el PIX, el statics sería requerido para hacer esto. 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 171.68.118.150 se recorre, que es estático a 10.10.10.20 dentro del PIX y usted puede ver donde el dispositivo 171.68.118.150 señala que tiene dos interfaces: 10.10.10.20 y 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
```

¿Esto tendrá sentido a una estación de administración de red? Probablemente no. El mismo problema estará presente para los desvíos: si la interfaz de 10.31.1.50 fuera ir abajo, el dispositivo 171.68.118.150 señalaría que la interfaz 10.31.1.50 estaba abajo.

Otro problema en intentar manejar una red interna del exterior “está drenando” la red. Si la estación de administración es Netview o HPOV, estos Productos utilizan una daemon del “netmon” para leer las tablas de ruta de los dispositivos. La tabla de ruta se utiliza en la detección. El PIX no soporta bastante de RFC 1213 para devolver una tabla de ruteo a una estación de administración de red, y por razones de seguridad, esto no es una buena idea de todos modos. 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 statics, no pueden ser preguntadas. Si tienen statics, la estación de administración de red no tiene ninguna manera de conocer cuáles es el statics.

Descubra los dispositivos fuera del PIX

Puesto que una estación de administración de red dentro del PIX pregunta a una dirección pública que las interfaces “públicas” de los informes, la detección afuera a los problemas interiores no apliquen.

Aquí, 171.68.118.118 era interior y 10.10.10.25 estaba afuera. Cuando recorrió 171.68.118.118 10.10.10.25, el cuadro señaló correctamente sus interfaces, es decir, la encabezado es lo 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 snmpwalk - el comando **público del <pix_ip_address> c** fue utilizado en una estación de administración del HPOV de realizar el snmpwalk. Todo el MIB disponible para PIX 6.2 fue cargado antes de realizar el 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 usted todavía necesita la ayuda después de que usted complete los pasos de Troubleshooting en este documento y quiera abrir un caso con el TAC de Cisco, aseegurese incluir esta información para resolver

problemas su firewall PIX.
• Descripción del problema y detalles relevantes de la topología • El troubleshooting se realizó antes de que usted abriera 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 usted no puede acceder la herramienta del Case Query, usted puede enviar la información en un elemento adjunto de correo electrónico a attach@cisco.com con su número de caso en el asunto de su mensaje.

Información Relacionada

- Referencias de Comandos de Cisco Secure PIX Firewall
- Soporte de productos del Software Cisco PIX Firewall
- Request For Comments (RFC)
- Soporte Técnico y Documentación - Cisco Systems