Utilisation de SNMP avec les dispositifs de sécurité PIX/ASA

Contenu

Introduction

Vous pouvez contrôler des événements système sur le PIX en utilisant le Protocole de gestion de réseau simple (SNMP). Ce document décrit comment utiliser SNMP avec le PIX, notamment :

- Les commandes pour exécuter SNMP *par le* PIX ou *vers* le PIX
- Exemple de sortie PIX
- Prise en charge de la Management Information Base (MIB) dans le logiciel PIX Versions 4.0 et ultérieures
- Niveaux d'interception
- exemples de niveau de gravité Syslog
- Problèmes de détection des périphériques PIX et SNMP

Remarque: Le port pour snmpget/snmpwalk est UDP/161. Le port pour des interceptions SNMP est UDP/162.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations de ce document sont basées sur le Logiciel pare-feu Cisco Secure PIX Versions 4.0 et ultérieures.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Cette configuration peut également être utilisée avec la version 7.x de l'appliance de sécurité adaptable Cisco (ASA).

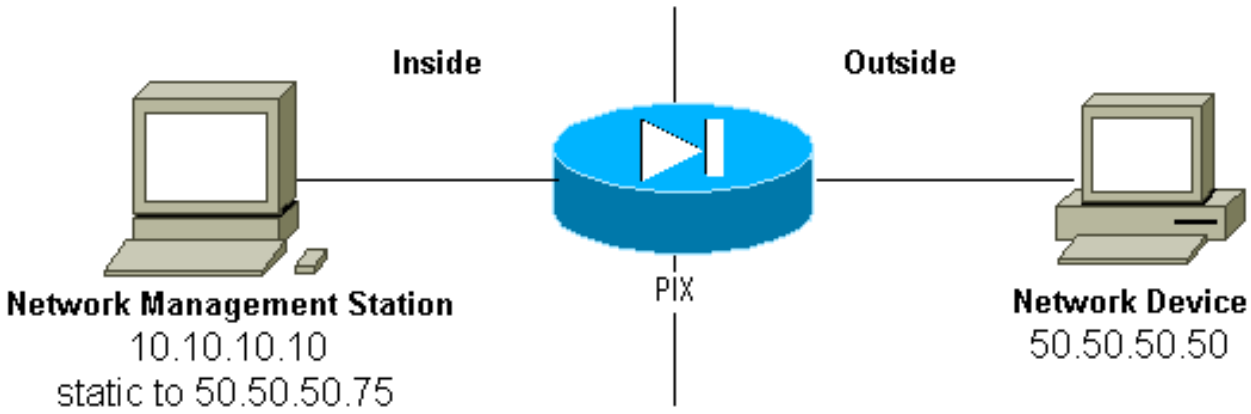
Conventions

Quelques lignes de résultat et de données de journal dans ce document ont été renvoyées à la ligne pour des raisons d'espace.

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

SNMP par le PIX/ASA

Interceptions de l'extérieur vers l'intérieur



Afin de permettre des interceptions de 50.50.50.50 à 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
```

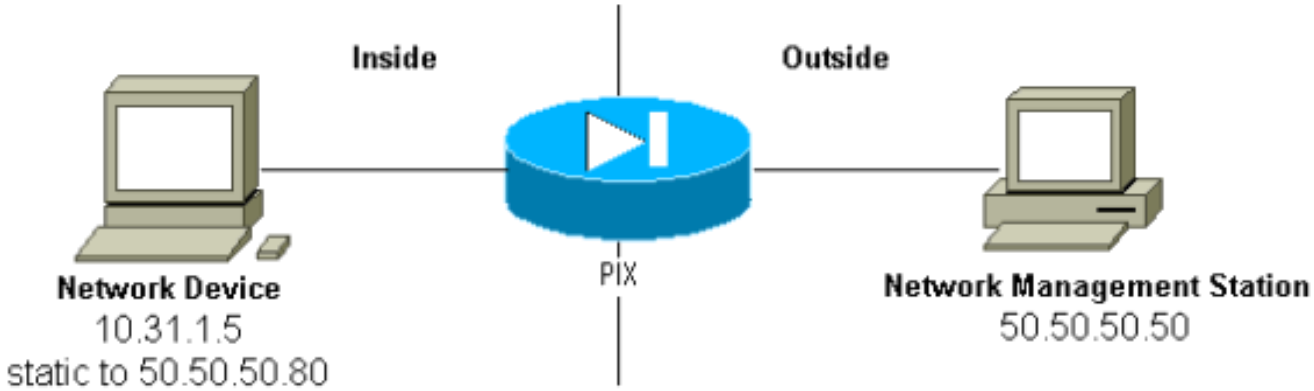
Si vous utilisez des listes de contrôle d'accès (ACL), disponibles dans PIX versions 5.0 et ultérieures, au lieu de conduits :

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

Le PIX affiche :

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

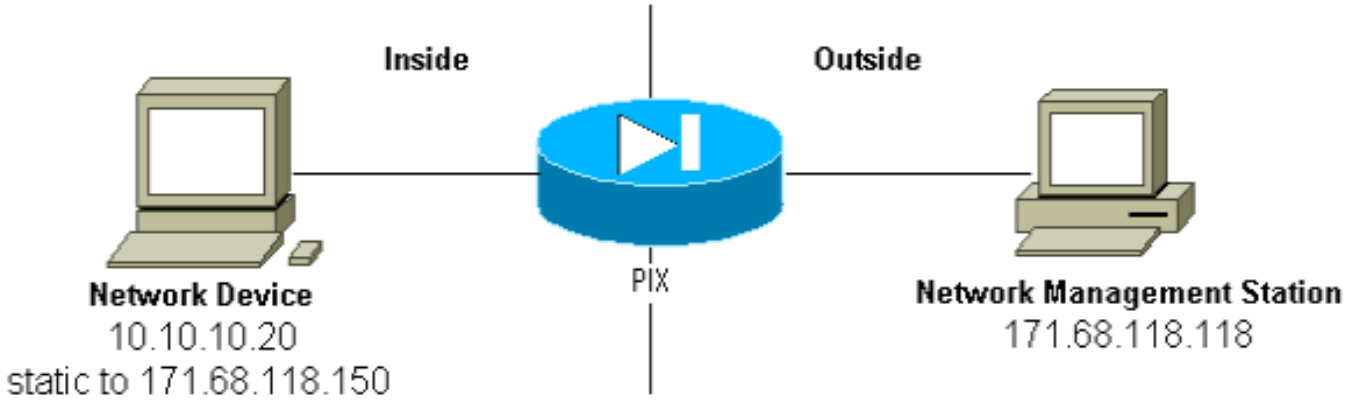
Interceptions de l'intérieur vers l'extérieur



Le trafic sortant est autorisé par défaut (faute de listes sortantes) et le PIX affiche :

```
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
```

Interrogation de l'extérieur vers l'intérieur



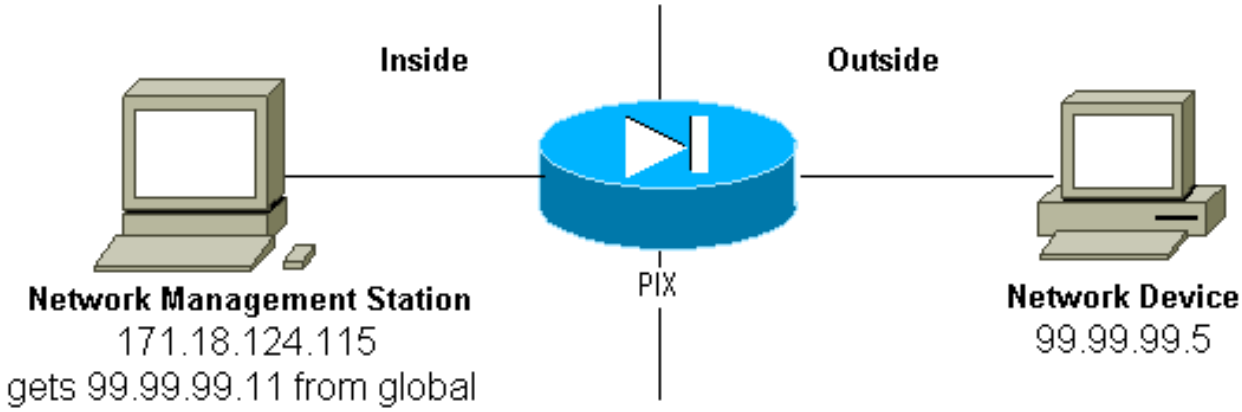
Pour permettre l'interrogation de 171.68.118.118 à 10.10.10.20 :

```
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 vous utilisez des ACL, disponibles dans PIX Versions 5.0 et ultérieures, au lieu de conduits :

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

Interrogation de l'intérieur vers l'extérieur



Le trafic sortant est autorisé par défaut (faute de listes sortantes) et le PIX affiche :

```
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 vers le PIX/ASA

Prise en charge MIB par la version

Voici les versions de MIB pris en charge dans le PIX :

- Logiciel pare-feu PIX Versions 4.0 à 5.1 — Groupes de système et d'interface de MIB-II (se référer à RFC 1213) mais non les groupes AT, ICMP, TCP, UDP, EGP, transmission, IP ou SNMP CISCO-SYSLOG-MIB-V1SMI.my.
- Logiciel pare-feu PIX Versions 5.1.x et ultérieures — MIB ultérieurs et CISCO-MEMORY-POOL-MIB.my et la branche cfwSystem de CISCO-FIREWALL-MIB.my.
- Logiciel pare-feu PIX Versions 5.2.x et ultérieures - MIB ultérieurs et l'ipAddrTable du groupe IP.
- Logiciel pare-feu PIX Versions 6.0.x et ultérieures - MIB ultérieurs et modifications du MIB-II OID pour identifier PIX par le modèle (et activer la prise en charge de CiscoView 5.2). Les nouveaux identificateurs d'objet (OID) sont disponibles dans le CISCO-PRODUCTS-MIB ; par exemple, le PIX 515 a l'OID 1.3.6.1.4.1.9.1.390.
- Logiciel pare-feu PIX Versions 6.2.x et ultérieures - MIB ultérieurs et CISCO-PROCESS-MIB-V1SMI.my.
- Logiciel PIX/ASA Version 7.x — MIB ultérieurs et IF-MIB, SNMPv2-MIB, ENTITY-MIB, CISCO-REMOTE-ACCESS-MONITOR-MIB, CISCO-CRYPTO-ACCELERATOR-MIB, ALTIGA-GLOBAL-REG.

Remarque: La section de PROCESS MIB prise en charge est la branche cpmCPUTotalTable de la branche cpmCPU de la branche ciscoProcessMIBObjects. Il n'y a aucun support pour la branche ciscoProcessMIBNotifications, la branche ciscoProcessMIBconformance ou les deux tables cpmProcessTable et cpmProcessExtTable, dans la branche cpmProcess de la branche ciscoProcessMIBObjects du MIB.

Activer le SNMP dans le PIX/ASA

Émettez ces commandes de autoriser l'interrogation/les requêtes et les interceptions dans le 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
```

Le logiciel PIX Versions 6.0.x et ultérieures permettent davantage de granularité en ce qui concerne les interceptions et les requêtes.

```
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.
```

Le logiciel PIX/ASA Versions 7.x permettent davantage de granularité en ce qui concerne les interceptions et les requêtes.

```
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.
```

Remarque: Spécifiez **trap** or **poll** si vous voulez limiter les NMS à la réception d'interceptions uniquement ou à la navigation (interrogation) uniquement. Par défaut, les NMS peuvent utiliser les deux fonctions.

Des interceptions SNMP sont envoyés sur le port UDP 162 par défaut. Vous pouvez modifier le numéro de port avec le mot clé **udp-port**.

SNMP au PIX/ASA - Interrogation

Les variables que le PIX renvoie dépendent de la prise en charge MIB dans la version. Un exemple de résultat d'un snmpwalk d'un PIX qu'exécute la version 6.2.1 est illustré à la fin de ce document. Les versions ultérieures du logiciel retournent uniquement les valeurs mib notées précédemment.

SNMP au PIX/ASA - Interceptions

Remarque: Un SNMP OID pour le pare-feu PIX s'affiche dans des interceptions d'événements SNMP envoyés depuis le pare-feu PIX. OID 1.3.6.1.4.1.9.1.227 était utilisé comme système pare-feu PIX OID avant le logiciel PIX Version 6.0. Les nouveaux modèles OID spécifiques sont disponibles dans le CISCO-PRODUCTS-MIB.

Émettez ces commandes pour activer des interceptions dans le 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
```

Interceptions dans le logiciel Version 4.0 jusqu'à 5.1

Quand vous utilisez le logiciel PIX Versions 4.0 et ultérieures, vous pouvez générer ces interruptions :

```
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
```

Modification d'interruption (PIX 5.1)

Dans le logiciel PIX Versions 5.1.1 et ultérieures, les niveaux d'interception sont séparés des niveaux Syslog pour les interceptions Syslog. Le PIX envoie toujours des interceptions Syslog, mais plus de granularité peut être configurée. Cet exemple montre le fichier trapd.log brut (et c'est le même pour HP OpenView [HPOV] ou Netview) y compris 3 interceptions link_up et 9 interceptions Syslog, avec 7 id Syslog différents : 101003, 104001, 111005, 111007, 199002, 302005, 305002.

Exemple 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
```

Description de chaque interception - 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
```

Exemples de niveau de gravité Syslog

Ceux-ci sont reproduits depuis la documentation pour illustrer les sept messages.

```
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.
```

Interpréter les niveau de gravité Syslog

Niveau	Signification
0	Système inutilisable - urgence
1	Agir immédiatement - alerte
2	État critique - critique
3	Message d'erreur - erreur
4	Message d'avertissement - avertissement
5	État normal mais significatif - notification
6	Informationnel - informationnel
7	Message de débogage - débogage

Configurer PIX Versions 5.1 et ultérieures pour un sous-ensemble d'interceptions

Si la configuration PIX a :

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

les seules interceptions qui sont générées sont les interceptions standards : démarrage à froid, liaison active et liaison inactive (pas Syslog).

Si la configuration PIX a :

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

alors toutes les interceptions standards et Syslog sont générées. Dans notre exemple, ce sont les entrées Syslog 101003, 104001, 111005, 111007, 199002, 302005 et 305002, et tous les autres résultats Syslog que le PIX a généré. Puisque l'historique d'événements défini pour le débogage et que ces numéros d'interception sont dans les niveaux notification, alerte et niveaux informationnels, le débogage de niveau inclut :

Si la configuration PIX a :

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

alors toutes les interceptions standards au niveau au-dessous du débogage sont générés. Si la commande **logging history notification** est utilisée, ceci inclurait toutes les interceptions Syslog aux niveaux urgence, alerte, critique, erreur, avertissement et notification (mais non aux niveaux informationnel ou débogage). Dans notre cas, 111005, 111007, 101003 et 104001 (et tous ceux que le PIX génère dans un réseau en activité) seraient inclus.

Si la configuration PIX a :

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

alors les messages 305002, 302005, 111005 ne sont pas produits. Lorsque PIX est défini sur **logging history debug**, vous voyez les messages 104001, 101003, 111007, 199002 et tous autres messages PIX, mais pas les 3 listés (305002, 302005, 111005).

Configurer PIX/ASA 7.x pour un sous-ensemble d'interceptions

Si la configuration PIX a :

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

les seules interceptions qui sont générées sont les interceptions standards : authentification, démarrage à froid, liaison active et liaison inactive (pas Syslog).

La configuration restante est semblable car le logiciel PIX Versions 5.1 et ultérieures, sauf dans PIX/ASA version 7.x, la commande **snmp-server enable traps** a des options supplémentaires telles que **ipsec**, **remote-access** et **entity**

Remarque: Consultez la section Activer SNMP de Contrôler l'appliance de sécurité pour en savoir plus sur les interceptions SNMP dans PIX/ASA

Problèmes SNMP

Détection PIX

Si le PIX réagit à une requête SNMP et signale son OID comme 1.3.6.1.4.1.9.1.227, ou dans le logiciel pare-feu PIX Versions 6.0 ou ultérieures, comme ID listé dans le CISCO-PRODUCTS-MIB pour ce modèle, alors le PIX fonctionne comme indiqué.

Dans les versions du code PIX ultérieures à 5.2.x, quand un support était ajouté pour l'ipAddrTable du groupe IP, les stations de gestion de réseau peuvent ne pas dessiner le PIX sur la carte comme un PIX. Une station de gestion de réseau doit toujours pouvoir détecter le fait que le PIX existe s'il peut envoyer un ping au PIX, mais il est possible qu'il ne puisse pas le dessiner comme PIX - une boîte noire avec 2 lumières. Outre la nécessité de prise en charge de l'ipAddrTable du groupe IP, HPOV, Netview et la plupart des autres stations de gestion de réseau doivent comprendre que l'OID retourné par le PIX est celui d'un PIX pour que l'icône appropriée apparaisse.

La prise en charge de la gestion PIX par CiscoView a été ajouté dans CiscoView 5,2 ; la version PIX 6.0.x est également requise. Dans les versions PIX ultérieures, une application de gestion tierce permet au Network Node Manager HPOV d'identifier les pare-feux PIX et les systèmes qui exécutent le manager du pare-feu PIX.

Détecter les périphériques à l'intérieur du PIX

Si le PIX est correctement configuré, il passe des requêtes et des interceptions SNMP de l'extérieur vers l'intérieur. Puisque la traduction d'adresses de réseau (NAT) est habituellement

configurée sur le PIX, des adresses statiques sont requis pour faire cela. Le problème se pose quand la station de gestion de réseau fait un snmpwalk de l'adresse publique, statique à une adresse privée à l'intérieur du réseau, l'en-tête extérieur du paquet n'est pas d'accord avec les informations dans l'ipAddrTable. Ici 171.68.118.150 est parcouru et est statique à 10.10.10.20 à l'intérieur du PIX, et vous pouvez voir où le périphérique 171.68.118.150 signale qu'il a deux 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
```

Est-ce que ceci aura du sens pour une station de gestion de réseau ? Probablement pas. Le même problème se présentera pour les interceptions : si l'interface 10.31.1.50 devait descendre, le périphérique 171.68.118.150 signalerait que l'interface 10.31.1.50 était en bas.

Un autre problème qui se pose lorsque vous essayez de gérer un réseau interne de l'extérieur est de « dessiner » le réseau. Si la station de gestion est Netview ou HPOV, ces Produits utilisent un daemon « netmon » pour lire les tables de routage à partir des périphériques. La table de routage est utilisée dans discovery. Le PIX ne prend en charge pas assez de RFC 1213 pour renvoyer une table de routage à une station de gestion de réseau, et pour des raisons de sécurité, ce n'est pas une bonne idée de toute façon. Tandis que les périphériques à l'intérieur du PIX signalent leurs tables de routage quand le routage statique est interrogé, tous les périphériques d'IP publiques (statiques) signalent toutes les interfaces privées. Si les autres adresses privées à l'intérieur du PIX n'ont pas de routages statiques, elles ne peuvent pas être interrogées. Si elles ont des routages statiques, la station de gestion de réseau n'a aucune façon de savoir quels sont les routages statiques.

Détecter les périphériques en dehors du PIX

Puisqu'une station de gestion de réseau à l'intérieur du PIX questionne une adresse publique qui signale les interfaces « publiques », les problèmes de détection de l'extérieur vers l'intérieur ne s'appliquent pas.

Ici, 171.68.118.118 était à l'intérieur et 10.10.10.25 à l'extérieur. Quand 171.68.118.118 a parcouru 10.10.10.25, la case a correctement signalé ses interfaces, c'est-à-dire que l'en-tête est identique à celui à l'intérieur du paquet :

```
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 version 6.2 de PIX

La commande **snmpwalk -c public <pix_ip_address>** a été utilisée sur une station de gestion HPOV pour effectuer le snmpwalk. Tous les MIB disponibles pour PIX 6.2 ont été chargés avant d'effectuer le 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.
```

Informations à collecter si vous ouvrez un dossier TAC

Si vous avez encore besoin d'assistance après avoir complété les étapes de dépannage dans ce document et que vous voulez ouvrir un dossier avec le Cisco TAC, veillez à inclure ces informations pour dépanner votre pare-feu PIX.

- Description du problème et des détails topologiques pertinents
- Dépannage réalisé avant l'ouverture du dossier
- Sortie de la commande **show tech-support**
- Sortie de la commande **show log** après l'exécution avec la commande **logging buffered debugging** , ou les captures de console qui expliquent le problème (si disponible)

Attachez les données rassemblées à votre dossier dans un format de texte brut (.txt) non compressé. Vous pouvez joindre des informations à votre cas en les téléchargeant à l'aide de TAC Service Request Tool (clients enregistrés uniquement). Si vous ne pouvez pas accéder au Case Query Tool, vous pouvez envoyer les informations en pièce-jointe dans un e-mail à attach@cisco.com avec votre numéro de dossier dans l'objet du message.

Informations connexes

- Références des commandes du pare-feu Cisco Secure PIX
- Support produit de Logiciels pare-feu Cisco PIX
- Request For Comments (RFC)
- Support et documentation techniques - Cisco Systems