SNMP gebruiken met security applicaties PIX/ASA

Inhoud

Inleiding

U kunt systeemgebeurtenissen in de PIX bewaken met behulp van Simple Network Management Protocol (SNMP). In dit document wordt beschreven hoe SNMP met de PIX moet worden gebruikt.

- Opdrachten om SNMP *door* de PIX of *naar* de PIX te leiden
- PIX-uitvoer van monster
- Ondersteuning van Management Information Base (MIB) in PIX-softwarerelease 4.0 en hoger
- Trapingsniveaus
- syslog ernst voorbeelden
- Problemen met de ontdekking van PIX- en SNMP-apparaten

Opmerking: De poort voor snget/snwalk is UDP/161. De poort voor SNMP-traps is UDP/162.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Secure PIX-firewall softwarereleases 4.0 en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco adaptieve security applicatie (ASA) versie 7.x.

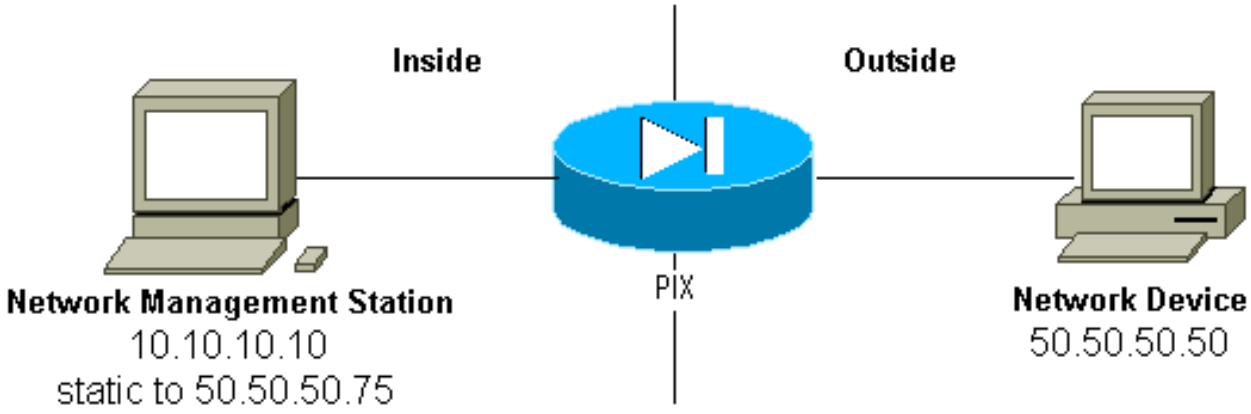
Conventies

Sommige regels uitvoer- en loggegevens in dit document zijn verpakt voor overwegingen met afstand.

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

SNMP via de PIX/ASA

Vouwen naar binnen



Om vallen toe te staan van 50.50.50.50 tot 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
```

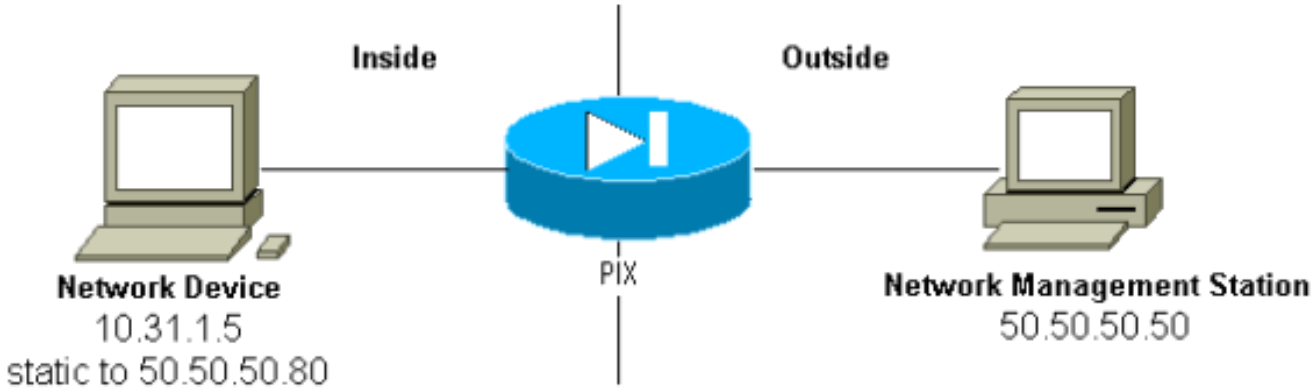
Als u toegangscontrolelijsten (ACL's) gebruikt, beschikbaar in PIX 5.0 en hoger, in plaats van circuits:

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

De PIX toont:

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

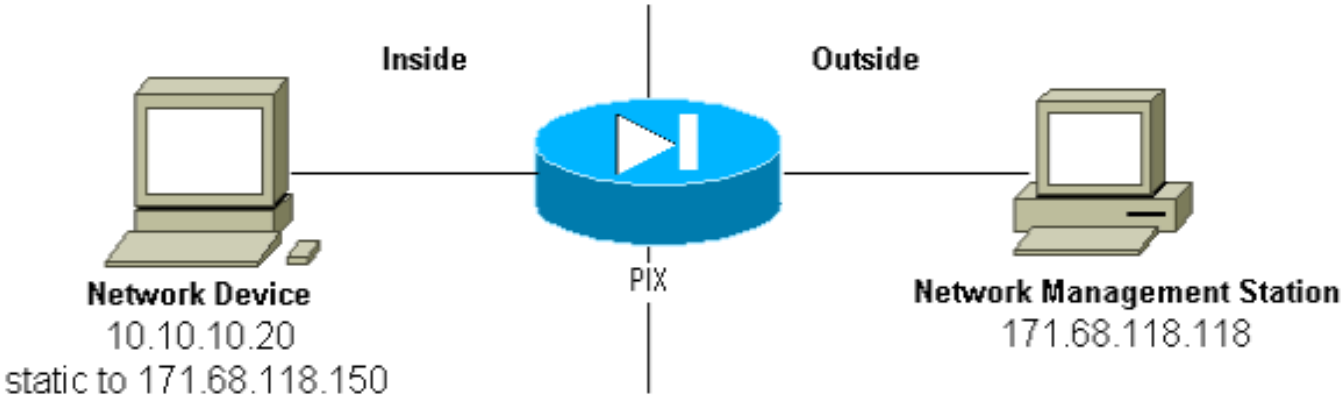
Vangen naar buiten



Het uitgaande verkeer is standaard toegestaan (bij ontstentenis van uitgaande lijsten) en de PIX toont:

```
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
```

Naar buiten kijken



Om de stemming mogelijk te maken van 17.68.118.118 tot 10.10.10.20:

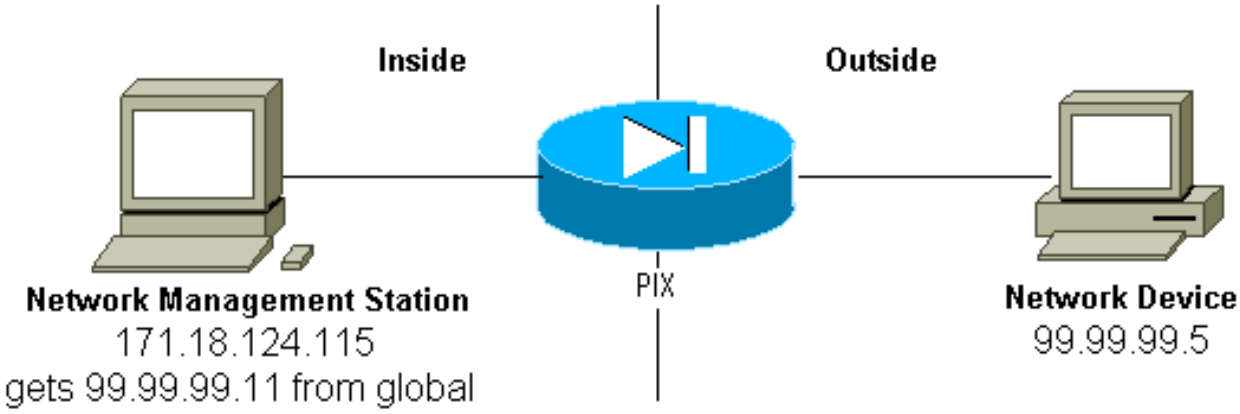
```
static (inside,outside) 171.68.118.150 10.10.10.20 netmask 255.255.255.255 0 0
```

```
conduit permit udp host 171.68.118.150 eq snmp host 171.68.118.118
```

Als u ACL's (ACL's) gebruikt, beschikbaar in PIX 5.0 en hoger, in plaats van conduits:

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

Naar buiten kijken



Het uitgaande verkeer is standaard toegestaan (bij ontstentenis van uitgaande lijsten) en de PIX toont:

```
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 aan de PIX/ASA

MIB-ondersteuning per versie

Dit zijn de versies van MIB ondersteuning in PIX:

- PIX-firewallsoftwareversies 4.0 tot 5.1 — Systeem en interfacegroepen van MIB-II (zie RFC 1213) maar niet de groepen AT, ICMP, TCP, UDP, EGP, transmissie, IP of SNMP CISCO-SYSLOG-MIB-V1SMI.my.
- PIX-firewallsoftwareversies 5.1.x en later — Vorige MIBs en CISCO-MEMORY-POOL-MIB.my en de cfwSystem-tak van de CISCO-FIREWALL-MIB.my.
- PIX-firewall-softwareversies 5.2.x en later-vorige MIB's en de ipAddressTable van de IP-groep.
- PIX-firewallsoftwareversies 6.0.x en later — Vorige MIB's en wijziging van de MIB-II OID om PIX door model te identificeren (en CiscoView 5.2 ondersteuning mogelijk te maken). De nieuwe doelidentificatoren (OID's) worden gevonden in de CISCO-PRODUCTS-MIB; de PIX 515 heeft bijvoorbeeld de OID 1.3.6.1.4.1.9.1.390.
- PIX-firewallsoftwareversies 6.2.x en later — Vorige MIB's en CISCO-PROCESS-MIB-V1SMI.my.
- PIX/ASA-software versie 7.x—Voorgaande MIB's en IF-MIB, SNMPv2-MIB, ENTITY-MIB, CISCO-REMOTE-ACCESS-MONITOR-MIB, CISCO-CRYPTO-ACCELERATOR-MIB,

ALTIGA-GG BAL-REG.

Opmerking: het ondersteunde gedeelte van het PROCES MIB is de cpmCPUTotalTable tak van de cpmCPU-tak van de ciscoProcesbalkMIBObjects-tak. Er is geen ondersteuning voor de ciscoProcentMIBNderhalve-routing, de ciscoProceMIBconformance tak of de twee tabellen, cpmProcestabel en cpmProceingsExtTable, in de cpmProcestak van de ciscoProcessingMIBObjects tak van de MIB.

SNMP inschakelen in de PIX/ASA

Geef deze opdrachten uit om opiniepeilingen/vragen en vallen in de PIX toe te staan:

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

PIX-softwarereleases 6.0.x en zorgen later voor meer granulariteit met betrekking tot vallen en vragen.

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

PIX/ASA-softwareversies 7.x maken meer granulariteit met betrekking tot vallen en vragen mogelijk.

```
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.
```

Opmerking: Specificeer de val of **enquête** als u de NMS alleen wilt beperken tot het ontvangen van vallen of het bladeren (opiniepeiling) alleen. NMS kan standaard beide functies gebruiken.

SNMP-traps worden standaard verzonden op UDP-poort 162. U kunt het poortnummer wijzigen met het **udp-poort** sleutelwoord.

SNMP op de PIX/ASA - Polling

De variabelen dat de PIX retourneert zijn afhankelijk van de ondersteuning van de mib in de versie. Een voorbeelduitvoer van een stok van een PIX die6.2.1 draait, is aan het eind van dit document. Eerdere versies van software geven alleen de eerder genoemde mib waarden terug.

SNMP op de PIX/ASA - Traps

Opmerking: Een SNMP OID voor PIX-firewall wordt weergegeven in SNMP-gebeurtenissen die vanuit de PIX-firewall zijn verstuurd. OID 1.3.6.1.4.1.9.1.27 werd gebruikt als het PIX-firewallsysteem OID tot PIX-softwareversie 6.0. De nieuwe model-specifieke OIDs zijn gevonden

in de CISCO-PRODUCTS-MIB.

Geef deze opdrachten uit om de vallen in de PIX in te schakelen:

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

Traps versie 4.0 tot 5.1

Wanneer u PIX-software 4.0 en hoger gebruikt, kunt u deze vallen genereren:

```
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
```

Wijzigingen van trap (PIX 5.1)

In PIX-softwarerelease 5.1.1 en hoger worden de val- en systeemniveaus voor de syslogvallen gescheiden. De PIX stuurt nog steeds syslogvallen, maar er kan meer granulariteit worden ingesteld. Dit voorbeeld rauw trapd.log bestand (en dit is hetzelfde voor HP OpenView [HPOV] of NetView) bevatte 3 link_up vallen en 9 syslog vallen, met 7 verschillende syslogbestanden: 101003, 104001, 111005, 11007, 199002, 302005, 305002.

Voorbeeld van een 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
```

Beschrijving van elke trap - trapd.log

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



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


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


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


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


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


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

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


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


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


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


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

syslog ernst-level-voorbeelden

Deze zijn opgenomen in de documentatie ter illustratie van de zeven berichten.

```
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.
```

Systeem interpreteren Ernstige Niveaus

Niveau	Betekenis
0	Systeem onbruikbaar - noodgeval
1	Neem onmiddellijk actie -
2	Kritieke conditie - kritisch
3	Fout in bericht - fout
4	Waarschuwingsbericht - waarschuwing
5	Normale maar significante voorwaarde -

	kennisgeving
6	Informatica - informatie
7	Debug bericht - debug

PIX 5.1 en hoger configureren voor een subset van trappen

Als de PIX-configuratie heeft:

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

de enige vallen die worden gegenereerd zijn de standaardvallen : koude start, verbinding omhoog en link omlaag (niet syslog).

Als de PIX-configuratie heeft:

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

vervolgens worden alle standaard - en syslogvallen gegenereerd . In ons voorbeeld zijn dit de syslog-ingangen 101003, 104001, 11005, 111007, 199002, 302005, 305002, en nog wat dan ook. g geeft de gegenereerde PIX uit. Omdat de houtkapgeschiedenis voor het debug en deze val getallen in het bericht, het alarm en de informatieniveaus zijn ingesteld, omvat niveau debug deze:

Als de PIX-configuratie heeft:

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

vervolgens worden alle standaard- en alle vallen op het onderstaande niveau gegenereerd. Als de opdracht **voor** het **melding van de houtkap** wordt gebruikt, omvat dit alle klemmen bij noodgevallen, alarm, kritisch, fout, waarschuwing en waarschuwing (maar geen informatie- of debug-niveaus). In ons geval zouden 11005, 11007, 101003 en 104001 (en alle andere dingen die de PIX in een levend netwerk zou genereren) inbegrepen zijn.

Als de PIX-configuratie heeft:

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

vervolgens worden 305002 , 302005 , 111005 niet verzonden . Als PIX is ingesteld voor **houtkapgeschiedenis debug**, dan zie je berichten 104001, 101003, 111007, 199002 en alle andere PIX-berichten, maar niet de 3 die zijn opgesomd (305002, 322 05, 111005).

PIX/ASA 7.x configureren voor een subset van trappen

Als de PIX-configuratie heeft:

```
snmp-server host
```

de enige vallen die worden gegenereerd zijn de standaardvallen : verificatie, koude start, link omhoog en omlaag (niet syslog).

De resterende configuratie is vergelijkbaar met PIX-softwareversie 5.1 en hoger, behalve in PIX/ASA versie 7.x, heeft de **snmp-server** voor **de** trap aanvullende opties zoals **ipsec**, **toegang op afstand** en **entiteit**

Opmerking: Raadpleeg het gedeelte SNMP-**ondersteuning** van het toezicht op de security applicatie om meer te weten te komen over de SNMP-trap in PIX/ASA

SNMP-problemen

PIX-ontdekking

Als de PIX op een SNMP-zoekopdracht reageert en zijn OID als 1.3.6.1.4.1.9.1.27 of in PIX-firewallversies 6.0 of hoger rapporteert als een ID die in CISCO-PRODUCTS-MIB is opgenomen voor dat model, dan werkt de PIX volgens zijn opzet.

In versies van PIX-code vóór 5.2.x toen er ondersteuning werd toegevoegd voor de ipAdresseerbare tabel van de IP-groep, kunnen netwerkbeheerstations de PIX niet als PIX op de kaart tekenen. Een netwerkbeheerstation zou altijd in staat moeten zijn om het feit te detecteren dat de PIX bestaat als het de PIX kan ping ping, maar het zou het niet als PIX kunnen tekenen - een zwarte doos met 2 lichten. Naast de ondersteuning van de ipAddrTable van de IP-groep, moeten HPOV, Netview en de meeste andere netwerkbeheerstations begrijpen dat de OID die door PIX wordt teruggegeven, de PIX is die van een PIX om het juiste pictogram te laten verschijnen.

CiscoView-ondersteuning voor PIX-beheer is toegevoegd in CiscoView 5.2. PIX, versie 6.0.x is ook vereist. In eerdere PIX-versies kan een beheertoepassing van derden het HPOV Network Node Manager toestaan om PIX-firewalls en systemen te identificeren die PIX-firewallbeheer uitvoeren.

Apparaten in de PIX ontdekken

Als de PIX goed is geconfigureerd, geeft hij SNMP-vragen door en valt hij van buiten naar binnen. Omdat NAT (Network Address Translation) doorgaans op de PIX wordt ingesteld, moeten statistieken dit doen. Het probleem is wanneer het netwerkbeheerstation een simpele weergave van het openbare adres uitvoert, dat op een privéadres in het netwerk aanstuurt, dan gaat de buitenste header van het pakket niet akkoord met de informatie in de ipAddressTable. Hier lopen

we 171.68.118.150, dat staat statisch tot 10.10.10.20 in de PIX en je kunt zien waar toestel 171.68.118.150 bericht dat het twee interfaces heeft: 10.10.10.20 en 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
```

Is dit zinvol voor een netwerkbeheerstation? Waarschijnlijk niet. Hetzelfde geldt voor vallen: als de 10.31.1.50-interface naar beneden zou gaan, zou machine 171.68.118.150 interface 10.31.1.50 moeten melden.

Een ander probleem bij het beheren van een binnennetwerk van buiten is het "tekenen" van het netwerk. Als het beheerstation Netview of HPOV is, gebruiken deze producten een "mon"daemon om de routetabellen van apparaten te lezen. De routekaart wordt bij ontdekking gebruikt. De PIX steunt niet genoeg van RFC 1213 om een routingtabel naar een netwerkbeheerstation terug te sturen, en om veiligheidsredenen is dit geen goed idee hoe dan ook. Terwijl apparaten binnen de PIX hun route-tafels rapporteren wanneer de statische vraag wordt gesteld, rapporteren alle openbare IP apparaten (statcs) alle privé interfaces. Als de andere privé adressen binnen de PIX geen statistieken hebben, kunnen zij niet worden betwist. Als ze statistieken hebben, heeft het netwerkbeheerstation geen enkele manier om te weten wat de statica zijn.

Apparaten buiten PIX ontdekken

Aangezien een netwerkbeheerstation binnen PIX een openbaar adres vraagt dat "openbare" interfaces meldt, is de ontdekking buiten om niet van toepassing op binnenproblemen.

Hier, 171.68.118.118 was binnen en 10.10.10.25 was buiten. Toen 171.68.118.118 10.10.10.25 liep, rapporteerde het vakje juist zijn interfaces, dat wil zeggen, de header is hetzelfde als binnen het pakje:

```
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
```

Versie 6.2.1.1.2 van PIX

De **simpwalk-c openbare <pix_ip_address>** opdracht werd gebruikt op een HPOV-beheerstation om sneltoetsen uit te voeren. Alle MIBs die beschikbaar waren voor PIX 6.2 werden geladen voordat de tussenstappen werden uitgevoerd.

```
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.
```

Te verzamelen informatie als u een TAC-case opent

Als u nog steeds assistentie nodig hebt nadat u de stappen voor het oplossen van problemen in dit document hebt voltooid en een case wilt openen met Cisco TAC, zorg er dan voor dat u deze informatie ook opgenomen hebt voor het oplossen van uw PIX-firewall.
• Probleembeschrijving en relevante topologgegevens • Probleemoplossing uitgevoerd voordat u de case opent

- Uitvoer vanuit de opdracht **Tech-support**
- Uitvoer van het bevel van het **showlogbestand** na het lopen met de **het registreren gebufferde** het bevel, of console vangt die het probleem (indien beschikbaar) aantoont

Hang de verzamelde gegevens aan uw case in een niet-zipped, onbewerkte tekstformaat (.txt). U kunt informatie aan uw case toevoegen door deze te uploaden via de TAC Service Application Tool (alleen geregistreerde klanten). Als u geen toegang hebt tot de Case Query Tool, kunt u de informatie in een e-mailbijlage naar attach@cisco.com met uw casenummer in de onderwerpregel of uw bericht verzenden.

Gerelateerde informatie

- Opdrachtreferenties van Cisco Secure PIX-firewall
- Productondersteuning voor Cisco PIX-firewall
- Verzoek om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems