Verwendung von SNMP mit den Security Appliances PIX/ASA

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Zugehörige Produkte
Konventionen
SNMP über PIX/ASA
Traps von außen nach innen
Traps innen nach außen
Umfragen von außen nach innen
Umfragen von innen nach außen
SNMP für PIX/ASA
MIB-Unterstützung nach Version
SNMP in PIX/ASA aktivieren
SNMP an PIX/ASA - Polling
SNMP an PIX/ASA - Traps
SNMP-Probleme
PIX-Erkennung
Entdecken Sie Geräte im PIX
Erkennung von Geräten außerhalb des PIX
Version 6.2 SNMPwalk von PIX
Informationen, die beim Öffnen eines TAC-Tickets gesammelt werden müssen
Zugehörige Informationen

Einführung

Sie können Systemereignisse auf dem PIX mithilfe des Simple Network Management Protocol (SNMP) überwachen. In diesem Dokument wird beschrieben, wie SNMP mit dem PIX verwendet wird. Dazu gehören:

- Befehle zum Ausführen von SNMP *über* den PIX oder *auf* den PIX
- PIX-Beispielausgabe
- Management Information Base (MIB)-Unterstützung in PIX Software Version 4.0 und höher
- Trap-Level
- Beispiele für Syslog-Schweregrad
- Probleme bei der PIX- und SNMP-Geräteerkennung

Hinweis: Der Port für snmpget/snmpwalk ist UDP/161. Der Port für SNMP-Traps ist UDP/162.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Secure PIX Firewall Software Releases 4.0 und höher.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Diese Konfiguration kann auch mit der Cisco Adaptive Security Appliance (ASA) Version 7.x verwendet werden.

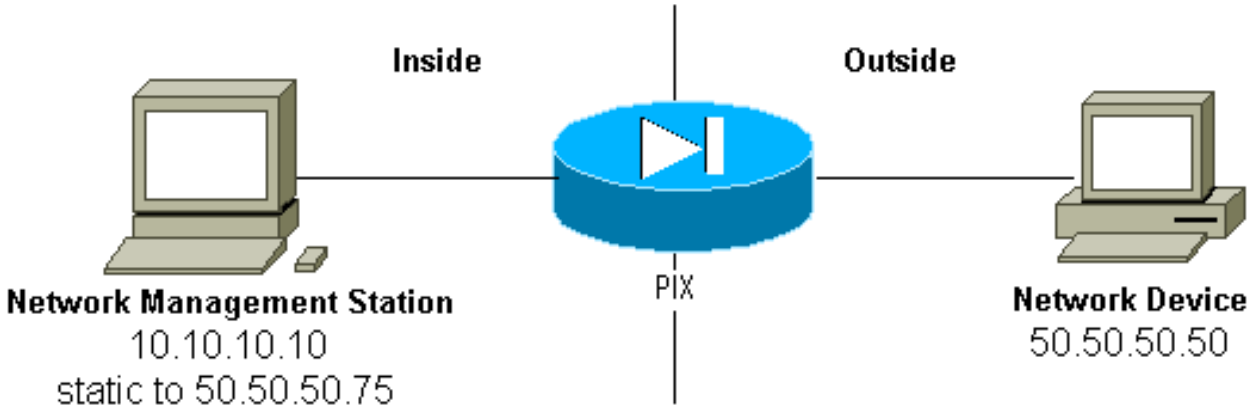
Konventionen

Einige Zeilen mit Ausgabe- und Protokolldaten in diesem Dokument wurden aus Platzhaltergründen eingeschlossen.

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

SNMP über PIX/ASA

Traps von außen nach innen



So lassen Sie Traps von 50.50.50.50 bis 10.10.10.10 ein:

```
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
```

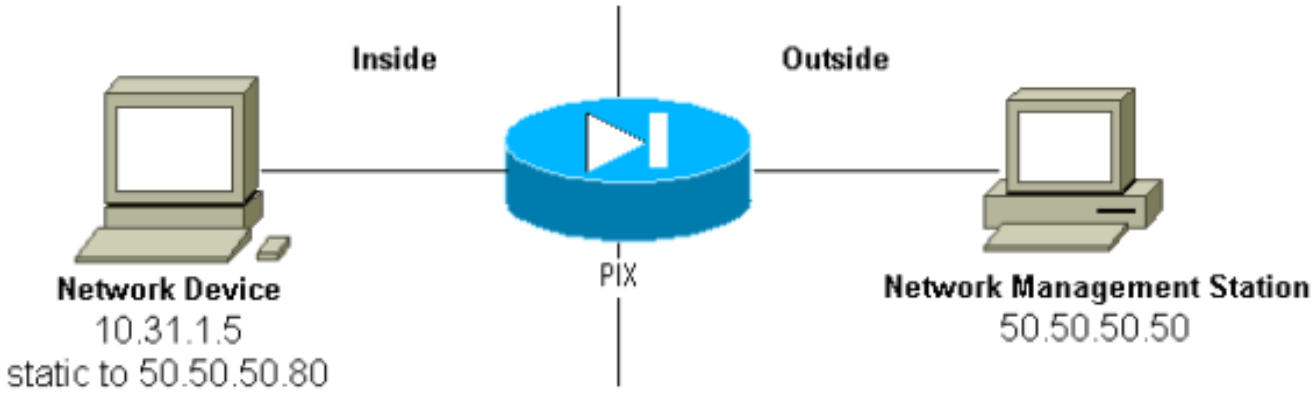
Wenn Sie anstelle von Leitungen Zugriffskontrolllisten (ACLs) verwenden, die in PIX 5.0 und höher verfügbar sind:

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

Der PIX zeigt Folgendes:

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

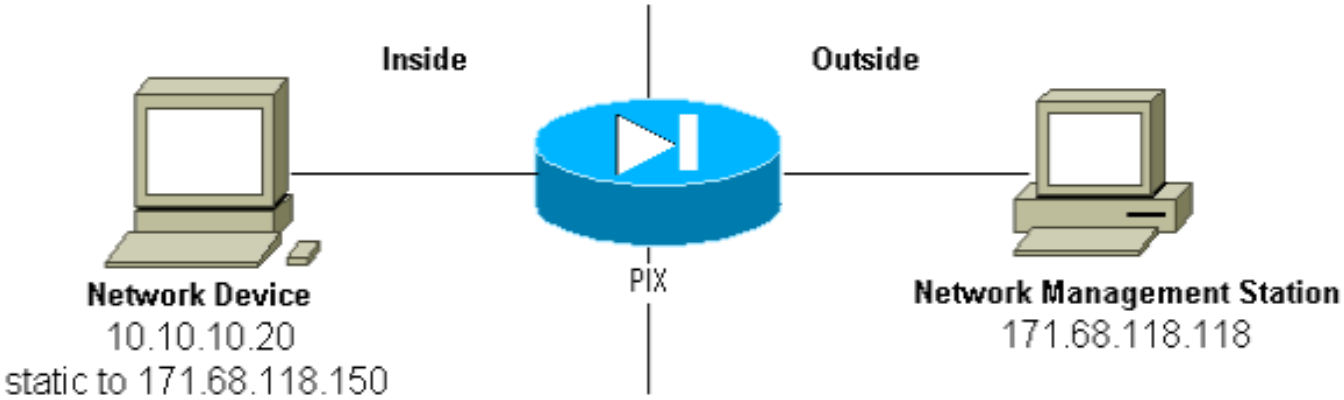
Traps innen nach außen



Ausgehender Datenverkehr ist standardmäßig zulässig (sofern keine ausgehenden Listen vorhanden sind), und der PIX zeigt Folgendes an:

```
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
```

Umfragen von außen nach innen



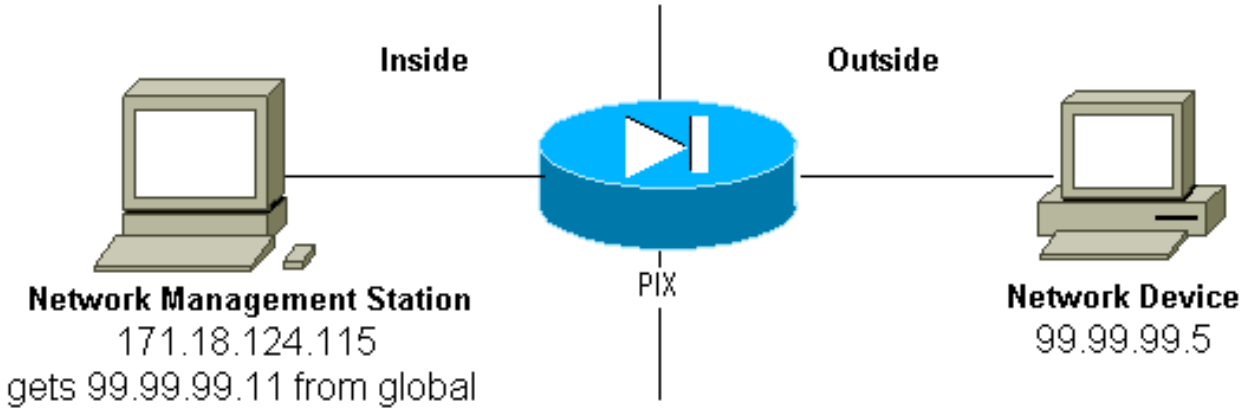
So ermöglichen Sie die Abfrage von 171.68.118.118 bis 10.10.10.20:

```
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
```

Wenn Sie ACLs verwenden, die in PIX 5.0 und höher verfügbar sind, anstelle von Kanälen:

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

Umfragen von innen nach außen



Ausgehender Datenverkehr ist standardmäßig zulässig (sofern keine ausgehenden Listen vorhanden sind), und der PIX zeigt Folgendes an:

```
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 für PIX/ASA

MIB-Unterstützung nach Version

Dies sind die Versionen der MIB-Unterstützung in PIX:

- PIX Firewall Software Version 4.0 bis 5.1 - System- und Schnittstellengruppen von MIB-II (siehe RFC 1213), jedoch nicht die AT-, ICMP-, TCP-, UDP-, EGP-, Übertragungs-, IP- oder SNMP-Gruppen CISCO-SYSLOG-MIB-V1SMI.my.
- PIX Firewall Software Version 5.1.x und höher - frühere MIBs und CISCO-MEMORY-POOL-MIB.my und die cfwSystem-Zweigstelle der CISCO-FIREWALL-MIB.my.
- PIX Firewall Software Version 5.2.x und höher - vorherige MIBs und die ipAddrTable der IP-Gruppe.
- PIX Firewall Software Version 6.0.x und höher - vorherige MIBs und Änderung der MIB-II OID zur modellbasierten Identifikation von PIX (und Aktivierung der Unterstützung für CiscoView 5.2). Die neuen Objekt-IDs (OIDs) finden Sie in der CISCO-PRODUCTS-MIB. Beispiel: PIX 515 hat die OID 1.3.6.1.4.1.9.1.390.
- PIX Firewall Software Version 6.2.x und höher - frühere MIBs und CISCO-PROCESS-MIB-

V1SMI.my.
- PIX/ASA Software Version 7.x - frühere MIBs und IF-MIB, SNMPv2-MIB, ENTITY-MIB, CISCO-REMOTE-ACCESS-MONITOR-MIB, CISCO-CRYPTO-ACCELERATOR-MIB, ALTIGA-GLOBBAL-REG.

Hinweis: Der unterstützte Abschnitt der PROZESS-MIB ist der cpmCPUTotalTable-Zweig der cpmCPU-Verzweigung des ciscoProcessMIBObjects-Zweiges. Im cpmProcess-Zweig der ciscoProcessMIBObjects-Zweigstelle der MIB-MIBonformance-Verzweigung oder den beiden Tabellen cpmProcessTable und cpmProcessExtTable gibt es keine Unterstützung für die cpmProcess-Verzweigung der ciscoProcessMIBObjects-Verzweigung der MIB.

SNMP in PIX/ASA aktivieren

Führen Sie die folgenden Befehle aus, um Abfragen und Traps in PIX zuzulassen:

```
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 Software Versionen 6.0.x und höher bieten mehr Präzision bei Traps und Abfragen.

```
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 Software Version 7.x bietet mehr Präzision bei Traps und Abfragen.

```
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.
```

Hinweis: Geben Sie **Trap** oder **Polling** an, wenn das NMS nur Traps empfangen oder nur durchsuchen (Polling) soll. Standardmäßig kann das NMS beide Funktionen verwenden.

SNMP-Traps werden standardmäßig auf dem UDP-Port 162 gesendet. Sie können die Portnummer mit dem **udp-port**-Schlüsselwort ändern.

SNMP an PIX/ASA - Polling

Die Variablen, die vom PIX zurückgegeben werden, hängen von der MIB-Unterstützung in der Version ab. Eine Beispielausgabe eines Snapwalk eines PIX, der 6.2.1 ausführt, befindet sich am Ende dieses Dokuments. Frühere Versionen der Software geben nur die zuvor angegebenen MIB-Werte zurück.

SNMP an PIX/ASA - Traps

Hinweis: Eine SNMP-OID für die PIX-Firewall wird in SNMP-Ereignistraps angezeigt, die von der

PIX-Firewall gesendet werden. Die OID 1.3.6.1.4.1.9.1.227 wurde bis zur Version 6.0 der PIX-Software als PIX-Firewall-System-OID verwendet. Die neuen modellspezifischen OIDs finden Sie in der CISCO-PRODUCTS-MIB.

Geben Sie folgende Befehle ein, um Traps in PIX zu aktivieren:

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

Traps Version 4.0 bis 5.1

Wenn Sie PIX Software 4.0 oder höher verwenden, können Sie folgende Traps generieren:

```
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
```

Trap Changes (PIX 5.1)

In PIX Software Version 5.1.1 und höher werden die Trap-Level von den Syslog-Ebenen für die Syslog-Traps getrennt. Der PIX sendet weiterhin Syslog-Traps, es kann jedoch eine größere Detailgenauigkeit konfiguriert werden. In diesem Beispiel wurde die Datei "trapd.log" (und dies ist die gleiche Datei für HP OpenView [HPOV] oder Netview) mit 3 link_up-Traps und 9 Syslog-Traps mit 7 verschiedenen Syslog-IDs angezeigt: 101003, 104001, 111005, 111007, 199002, 302005, 305002.

Beispiel für ein 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
```

Beschreibung der einzelnen Traps - 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-Schweregrad - Beispiele

Diese werden aus der Dokumentation reproduziert, um die sieben Meldungen zu veranschaulichen.

```
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.
```

Interpretieren der Syslog-Schweregrade

Stufe	Bedeutung
0	System unbrauchbar - Notfall
1	Sofortige Maßnahmen - Alarm
2	Kritische Bedingung - kritisch

1	Fehlermeldung - Fehler
4	Warnmeldung - Warnung
5	Normale, aber wesentliche Bedingung - Benachrichtigung
6	Information - Information
7	Debug-Meldung - Debuggen

Konfigurieren von PIX 5.1 und höher für eine Teilmenge von Traps

Wenn die PIX-Konfiguration:

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

Die einzigen generierten Traps sind die Standard-Traps: Kaltstart, Link auf und Link down (kein Syslog).

Wenn die PIX-Konfiguration:

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

dann werden alle Standard- und alle Syslog-Traps generiert. Im vorliegenden Beispiel sind dies die Syslog-Einträge 101003, 104001, 111005, 11007, 199002, 302005 und 305002 sowie alles andere Syslog Protokollausgabe des generierten PIX. Da der Protokollierungsverlauf für das Debuggen festgelegt wurde und sich diese Trap-Nummern in der Benachrichtigungs-, Warn- und Informationsstufe befinden, umfasst das Level-Debugging Folgendes:

Wenn die PIX-Konfiguration:

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

dann werden alle Standard-Traps und alle Traps auf der Ebene unter debug generiert. Wenn der Befehl **zur Meldung des Protokollierungsverlaufs** verwendet wird, umfasst dies alle Syslog-Traps bei Notfall-, Alarm-, kritische, Fehler-, Warn- und Benachrichtigungsebenen (jedoch nicht Informations- oder Debugging-Ebenen). In unserem Fall werden 11005, 11007, 101003 und 104001 (und alle anderen, die der PIX in einem Live-Netzwerk generieren würde) einbezogen.

Wenn die PIX-Konfiguration:

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

dann werden die Nachrichten 305002, 302005, 111005 nicht erstellt. Wenn PIX für die **Protokollierung** des **Verlaufsdebuggens** festgelegt ist, werden die Meldungen 104001, 101003, 11007, 199002 und alle anderen PIX-Nachrichten angezeigt, jedoch nicht die 3 aufgeführten (305000020 05, 111005).

Konfigurieren von PIX/ASA 7.x für eine Teilmenge von Traps

Wenn die PIX-Konfiguration:

```
snmp-server host
```

Die einzigen generierten Traps sind die Standard-Traps: Authentifizierung, Kaltstart, Link Up und Link Down (kein Syslog).

Die restliche Konfiguration ähnelt der PIX Software Version 5.1 und höher, mit Ausnahme von PIX/ASA Version 7.x, verfügt der Befehl **snmp-server enable traps** über zusätzliche Optionen wie **ipsec**, **Remote-Zugriff** und **Entität.**

Hinweis: Weitere Informationen zu SNMP-Traps in PIX/ASA finden Sie im Abschnitt SNMP aktivieren unter Überwachen der Sicherheits-Appliance.

SNMP-Probleme

PIX-Erkennung

Wenn der PIX auf eine SNMP-Abfrage reagiert und seine OID als 1.3.6.1.4.1.9.1.227 oder in der PIX-Firewall-Softwareversion 6.0 oder höher als eine ID meldet, die in der CISCO-PRODUCTS-MIB für dieses Modell aufgeführt ist, funktioniert das PIX wie vorgesehen.

In Versionen von PIX-Code, die vor 5.2.x installiert wurden, als Unterstützung für die ipAddrTable der IP-Gruppe hinzugefügt wurde, können Netzwerkmanagementstationen den PIX möglicherweise nicht als PIX auf der Karte zeichnen. Eine Netzwerkmanagementstation sollte immer erkennen können, dass der PIX vorhanden ist, wenn er den PIX pingen kann, ihn aber möglicherweise nicht als PIX zeichnen kann - eine Blackbox mit zwei Leuchten. Neben der Unterstützung der ipAddrTable der IP-Gruppe müssen HPOV, Netview und die meisten anderen Netzwerkmanagement-Stationen auch verstehen, dass die vom PIX zurückgegebene OID die eines PIX ist, damit das entsprechende Symbol angezeigt wird.

CiscoView-Unterstützung für das PIX-Management wurde in CiscoView 5.2 hinzugefügt. PIX Version 6.0.x ist ebenfalls erforderlich. In früheren PIX-Versionen kann der HPOV Network Node Manager mit einer Management-Anwendung eines Drittanbieters PIX-Firewalls und -Systeme identifizieren, auf denen der PIX Firewall Manager ausgeführt wird.

Entdecken Sie Geräte im PIX

Wenn das PIX ordnungsgemäß konfiguriert ist, leitet es SNMP-Abfragen und Traps von außen an interne Geräte weiter. Da Network Address Translation (NAT) normalerweise auf dem PIX konfiguriert wird, sind hierfür Statistiken erforderlich. Das Problem besteht darin, dass der externe Header des Pakets nicht mit den Informationen in der ipAddrTable übereinstimmt, wenn die Netzwerkmanagementstation einen Snapshot der öffentlichen Adresse ausführt, die einer privaten Adresse im Netzwerk entspricht. Hier ist 171.68.118.150, statisch zu 10.10.10.20 im PIX, und Sie können sehen, wo Gerät 171.68.118.150 meldet, dass es zwei Schnittstellen hat: 10.10.10.20 und 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
```

Ist dies für eine Netzwerkmanagement-Station sinnvoll? Wahrscheinlich nicht. Das gleiche Problem tritt auch bei Traps auf: Wenn die Schnittstelle 10.31.1.50 ausfallen sollte, meldet das Gerät 171.68.118.150, dass die Schnittstelle 10.31.1.50 ausgefallen ist.

Ein weiteres Problem bei der Verwaltung eines internen Netzwerks von außen besteht darin, das Netzwerk zu "zeichnen". Wenn die Managementstation Netview oder HPOV ist, verwenden diese Produkte einen "netmon"-Daemon, um die Routing-Tabellen von Geräten zu lesen. Die Routing-Tabelle wird bei der Erkennung verwendet. Das PIX unterstützt nicht genügend RFC 1213 , um eine Routing-Tabelle an eine Netzwerkmanagementstation zurückzusenden. Aus Sicherheitsgründen ist dies in jedem Fall keine gute Idee. Während Geräte innerhalb des PIX ihre Routing-Tabellen melden, wenn eine Abfrage für die statische Abfrage durchgeführt wird, melden alle öffentlichen IP-Geräte (Statistiken) alle privaten Schnittstellen. Wenn die anderen privaten Adressen innerhalb des PIX keine Statistiken aufweisen, können sie nicht abgefragt werden. Wenn sie über Statistiken verfügen, kann die Netzwerkmanagement-Station nicht wissen, was die Statistiken sind.

Erkennung von Geräten außerhalb des PIX

Da eine Netzwerkmanagementstation innerhalb des PIX eine öffentliche Adresse abfragt, die "öffentliche" Schnittstellen meldet, gilt die Erkennung außerhalb interner Probleme nicht.

Hier war der 171.68.118.118 innen und der 10.10.10.25 war draußen. Wenn 171.68.118.118 10.10.10.25 ging, meldete das Feld seine Schnittstellen korrekt, das heißt, der Header ist der gleiche wie im Paket:

```
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
```

Version 6.2 SNMPwalk von PIX

Der Befehl **snmpwalk -c public <pix_ip_address>** wurde auf einer HPOV-Managementkonsole verwendet, um snmpwalk auszuführen. Alle für PIX 6.2 verfügbaren MIBs wurden vor der Durchführung des snmpwalk geladen.

```
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.
```

Informationen, die beim Öffnen eines TAC-Tickets gesammelt

werden müssen

Wenn Sie nach Abschluss der Schritte zur Fehlerbehebung in diesem Dokument weiterhin Hilfe benötigen und ein Ticket beim Cisco TAC erstellen möchten, stellen Sie sicher, dass Sie diese Informationen zur Fehlerbehebung für Ihre PIX-Firewall angeben.
• Problembeschreibung und relevante Topologiedetails • Fehlerbehebung durchgeführt, bevor Sie das Ticket geöffnet haben • Ausgabe des Befehls **show tech-support** • Ausgabe des Befehls **show log** nach der Ausführung mit dem Befehl **logging puffered debugging** oder Konsolenerfassungen, die das Problem veranschaulichen (falls verfügbar) Hängen Sie die erfassten Daten im unverzippten Textformat (.txt) an Ihren Fall an. Sie können Informationen zu Ihrem Ticket hinzufügen, indem Sie es mit dem TAC Service Request Tool hochladen (nur registrierte Kunden). Wenn Sie nicht auf das Fallabfrage-Tool zugreifen können, können Sie die Informationen in einem E-Mail-Anhang an attach@cisco.com senden, der Ihre Fallnummer in der Betreffzeile Ihrer Nachricht enthält.

Zugehörige Informationen

- Cisco Secure PIX Firewall - Befehlsreferenzen
- Produkt-Support für die Cisco PIX Firewall
- Request for Comments (RFCs)
- Technischer Support und Dokumentation - Cisco Systems