Использование SNMP с устройствами защиты PIX/ASA

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Родственные продукты
Условные обозначения
Протокол SNMP через PIX/ASA
Прерывания входящего трафика
Ловушки исходящего трафика
Внешние опросы (внутрь)
Опрос для исходящего трафика
SNMP к PIX/ASA
Поддержка MIB по версиям
Включение протокола SNMP в PIX/ASA
Опрос с использованием протокола SNMP к PIX/ASA
SNMP к PIX/ASA - прерывания
Проблемы SNMP
Обнаружение PIX
Обнаружение устройств внутри PIX
Обнаружение устройств вне PIX
Версия 6.2 snmpwalk PIX
Информация, обязательная для сбора в случае обращения в Центр технической поддержки
Дополнительные сведения

Введение

Осуществлять контроль системных событий на PIX можно с помощью простого протокола сетевого управления (SNMP). В этом документе описывается использование SNMP с PIX, в том числе:

- *Команды для запуска SNMP через PIX или к PIX*
- Пример выходных данных PIX
- Поддержка базы управляющей информации (MIB) в ПО PIX версии 4.0 и выше
- Уровни прерываний
- примеры степени серьезности событий, регистрируемых в системном журнале
- Проблемы обнаружения устройства PIX и SNMP

Примечание: Порт для snmpget/snmpwalk -UDP/161. Порт для trap-сообщений SNMP является UDP/162.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основаны на Cisco Secure PIX Firewall Software Release 4.0 и выше.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Родственные продукты

Данную конфигурацию также можно использовать с адаптивным устройством обеспечения безопасности Cisco ASA версии 7.x.

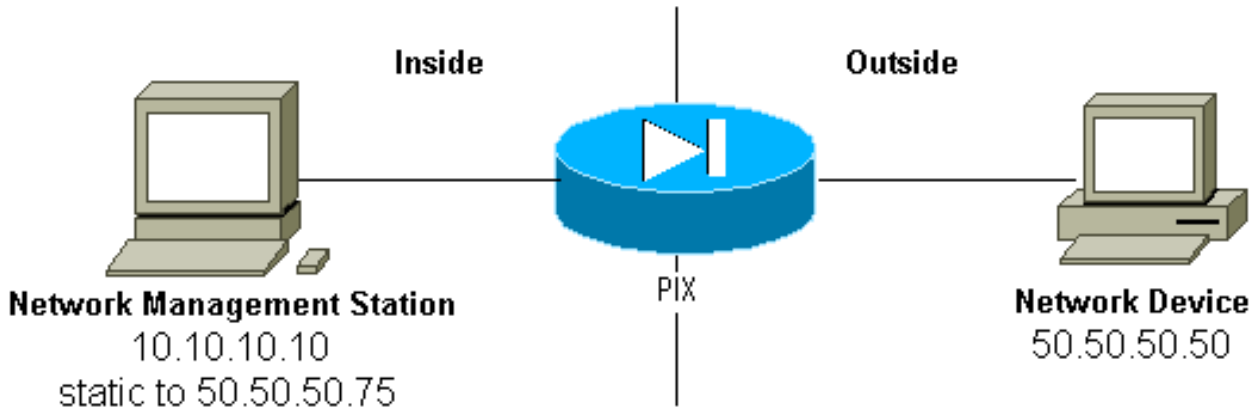
Условные обозначения

Некоторые строки выходных данных и данных журнала в этом документе были свернуты из соображений размещения.

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Протокол SNMP через PIX/ASA

Прерывания входящего трафика



Чтобы разрешить передачу прерывания с адреса 50.50.50.50 по адресу 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
```

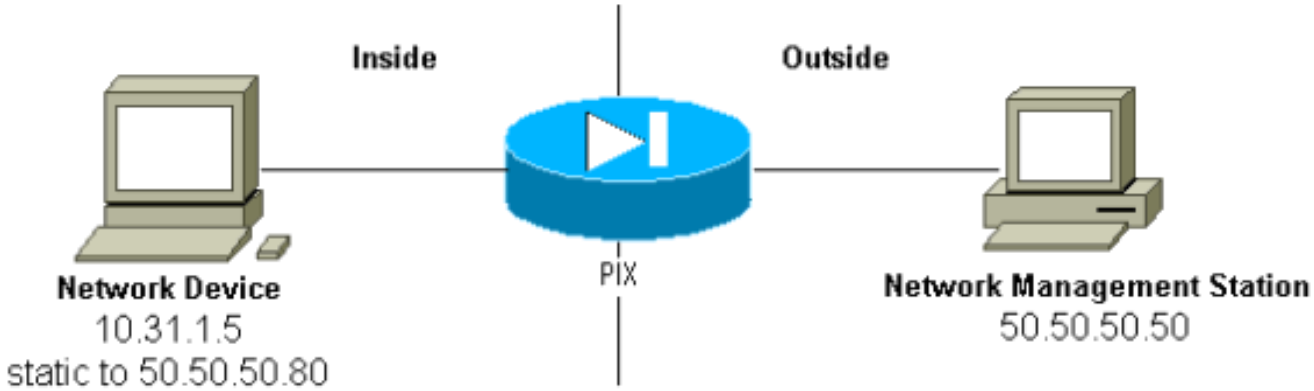
Если использовать списки управления доступом (ACL), доступные в PIX версии 5.0 и выше, вместо каналов:

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

PIX отображает:

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

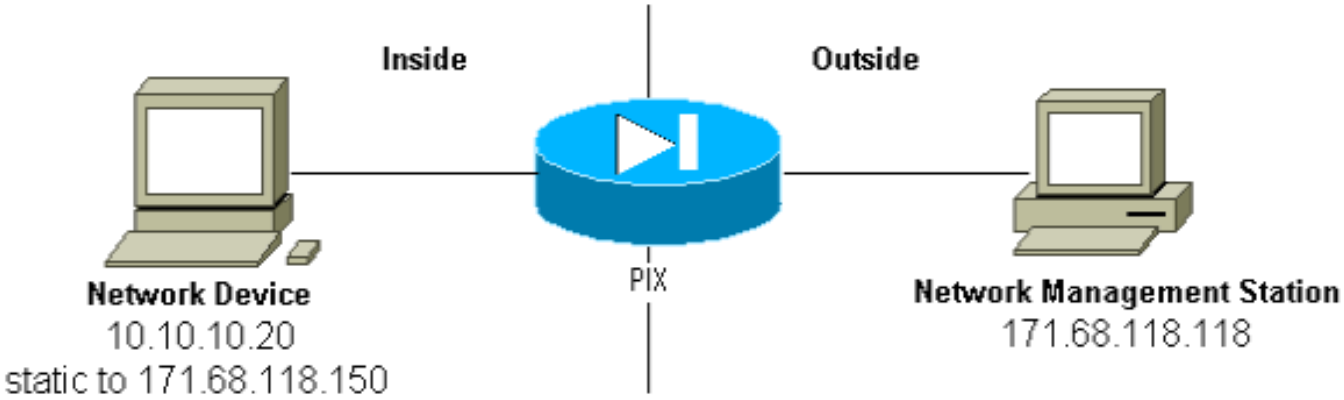
Ловушки исходящего трафика



Исходящий трафик разрешен по умолчанию (в отсутствие исходящих списков), и PIX показывает:

```
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
```

Внешние опросы (внутрь)



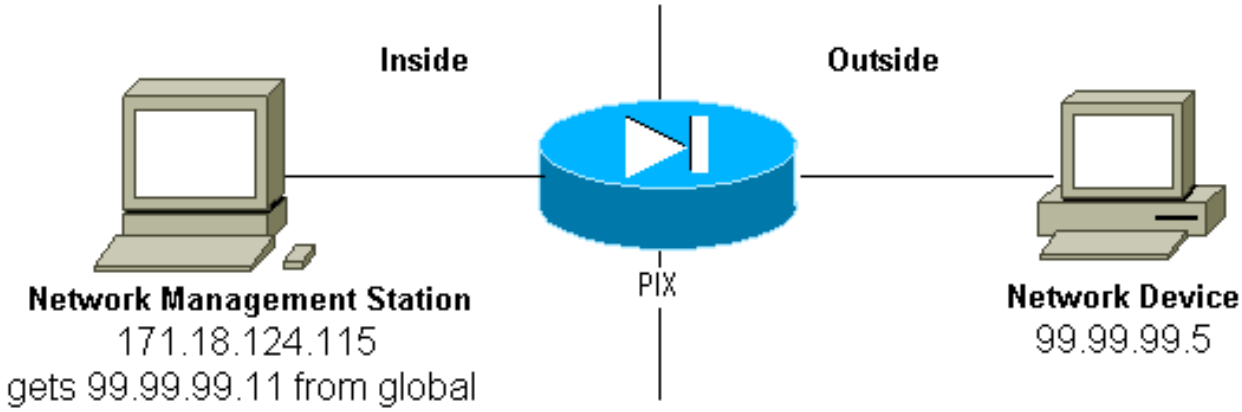
Чтобы разрешить упорядоченный опрос от 171.68.118.118 к 10.10.10.20:

```
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
```

Если использовать списки ACL, доступные в PIX версии 5.0 и в более поздних версиях, вместо каналов:

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

Опрос для исходящего трафика



Исходящий трафик разрешен по умолчанию (в отсутствие исходящих списков), и PIX показывает:

```
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 к PIX/ASA

Поддержка MIB по версиям

Ниже приведены версии поддержки MIB в PIX:

- Версии ПО межсетевого экрана PIX от 4.0 до 5.1 – это группы систем и интерфейсов MIB-II (см. раздел RFC 1213), но не AT, ICMP, TCP, UDP, EGP, передача, IP или группы SNMP CISCO-SYSLOG-MIB-V1SMI.my.
- Версии ПО межсетевого экрана PIX 5.1.x и более поздние – это предыдущие базы MIB и CISCO-MEMORY-POOL-MIB.my, а также ветвь cfwSystem CISCO-FIREWALL-MIB.my.
- Версии ПО межсетевого экрана PIX 5.2.x и более поздние – это предыдущие базы MIB и ipAddrTable IP-группы.
- Версии ПО межсетевого экрана PIX 6.0.x и более поздние – это предыдущие базы MIB и изменение MIB-II OID, чтобы определить PIX по модели (и включить поддержку CiscoView 5.2). Новые идентификаторы объекта (OID) можно найти в CISCO-PRODUCTS-MIB; например, в PIX 515 есть OID 1.3.6.1.4.1.9.1.390.
- Версии ПО межсетевого экрана PIX 6.2.x и более поздние – это предыдущие базы MIB и CISCO-PROCESS-MIB-V1SMI.my.
- ПО PIX/ASA версии 7.x – это предыдущие базы MIB и IF-MIB, SNMPv2-MIB, ENTITY-MIB, CISCO-REMOTE-ACCESS-MONITOR-MIB, CISCO-CRYPTO-ACCELERATOR-MIB, ALTIGA-GLOBAL-REG.

Примечание: Поддерживаемый раздел PROCESS MIB является ветвью cpmCPUTotalTable ветви cpmCPU ветви ciscoProcessMIBObjects. Не поддерживаются ветвь ciscoProcessMIBNotifications, ветвь ciscoProcessMIBconformance или две таблицы, cpmProcessTable и cpmProcessExtTable, в ветви cpmProcess для ветви ciscoProcessMIBObjects MIB.

Включение протокола SNMP в PIX/ASA

Выполните следующие команды, чтобы разрешить опросы/запросы и прерывания в 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
```

Программное обеспечение PIX версий 6.0.x и более поздних позволяют большую степень детализации в отношении прерываний и запросов.

```
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.
```

ПО PIX/ASA версии 7.x позволяет использовать большую степень детализации в отношении прерываний и запросов.

```
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.
```

Примечание: Задайте **trap-сообщение** или **опрос**, если вы хотите ограничить NMS получением trap-сообщений только или просмотром (опроса) только. По умолчанию NMS может использовать обе функции.

По умолчанию прерывания SNMP посылаются на порт UDP 162. **Для изменения номера порта необходимо ввести ключевое слово udp-port.**

Опрос с использованием протокола SNMP к PIX/ASA

Переменные, которые возвращает PIX, зависят от поддержки mib в версии. Пример выходных данных snmpwalk для PIX под управлением 6.2.1 приведен в конце документа. Более ранние версии ПО возвращают лишь ранее указанные значения mib.

SNMP к PIX/ASA - прерывания

Примечание: OID SNMP для Межсетевого экрана PIX отображается в trap-сообщениях события SNMP, передаваемых от Межсетевого экрана PIX. До появления ПО PIX версии 6.0 OID 1.3.6.1.4.1.9.1.227 использовался в качестве системного OID межсетевого экрана PIX. Новые модельные специализированные OID найдены в CISCO-PRODUCTS-MIB.

Чтобы включить прерывания в PIX, выполните следующие команды:

```
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
```

Версии прерываний с 4.0 по 5.1

При использовании ПО PIX версии 4.0 и более поздних версий возможно генерирование следующих прерываний:

```
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
```

Изменения прерываний (PIX 5.1)

В ПО PIX версии 5.1.1 и более поздних версий уровни прерываний отделены от уровней системного журнала для прерываний системного журнала. PIX продолжает посылать прерывания системного журнала, но возможно повысить степень детализации. Данный пример необработанного файла trapd.log (как и для HP OpenView [HPOV] или Netview) включает 3 link_up-прерывания и 9 syslog-прерываний с 7 различными syslog ids: 101003, 104001, 111005, 111007, 199002, 302005, 305002.

Пример файла 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
```

Описание каждого прерывания – файл 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
```

[примеры степени серьезности событий, регистрируемых в системном журнале]

Это примеры семи сообщений из документации.

```
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.
```

[Интерпретация степени серьезности ошибок журнала syslog]

Уровень	Значение
0	Система неработоспособна - критическая ситуация
1	Take immediate action – сигнал тревоги
2	Критическое состояние, критическое
3	Сообщение об ошибке – ошибка
4	Предупреждающее сообщение, предупреждение
5	Нормальное, но важное состояние – уведомление
6	Информационное сообщение – информация
7	Сообщение об отладке – отладка

[Конфигурация PIX версии 5.1 и более поздних версий для подмножества прерываний]

Если в конфигурации PIX задана команда:

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

то единственными генерируемыми прерываниями являются стандартные прерывания: начальный запуск, включение и отключение канала (не системный журнал).

Если в конфигурации PIX задана команда:

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

формируются все стандартные ловушки и все ловушки системного журнала. В данном примере отображены записи системного журнала 101003, 104001, 111005, 111007, 199002, 302005 и 305002 и все остальные выходные данные системного журнала, формируемые PIX. Так как журнал регистрации настроен на отладку и эти номера прерываний находятся в уведомлении, сигнале тревоги и информационных уровнях, уровень отладки предполагает следующее:

Если в конфигурации PIX задана команда:

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

затем создаются все стандарты и все прерывания на уровне ниже отладки. **При выполнении команды logging history notification будут включены все прерывания системного журнала на уровне аварийной ситуации, сигнала тревоги, критическом уровне, ошибки, предупреждения и уведомления (но это не относится к информационному уровню и уровню отладки).** В данном случае будут включены прерывания 111005, 111007, 101003 и 104001 (и любые другие, которые PIX будет генерировать в рабочей сети).

Если в конфигурации PIX задана команда:

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

после этого сообщения 305002, 302005 и 111005 перестанут поступать. **С помощью установки PIX для logging history debug можно увидеть сообщения 104001, 101003, 111007, 199002 и все другие сообщения PIX, но не перечисленные выше три (305002, 302005, 111005).**

Конфигурация PIX/ASA версии 7.x и более поздних версий для подмножества прерываний

Если в конфигурации PIX задана команда:

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

то единственными генерируемыми прерываниями являются стандартные прерывания: аутентификация, начальный запуск, включение и отключение канала (не системный журнал).

Оставшаяся конфигурация похожа на ПО PIX версии 5.1 и более поздних версий, за исключением того, что в PIX/ASA версии 7.x команда snmp-server enable traps имеет дополнительные параметры, такие как ipsec, remote-access и entity

Примечание: См. раздел SNMP Включения Мониторинга Устройства безопасности для узнавания больше о trap-сообщениях SNMP в PIX/ASA

Проблемы SNMP

Обнаружение PIX

Если PIX отвечает на запрос SNMP и сообщает его OID как 1.3.6.1.4.1.9.1.227 или в ПО межсетевого экрана PIX версии 6.0 или более поздних версий — как идентификатор, указанный в CISCO-PRODUCTS-MIB для данной модели, тогда PIX функционирует, как предполагалось разработчиками.

В версиях кода PIX до 5.2.x, когда существовала поддержка, добавленная для ipAddrTable IP-группы, станции управления сетями могли не указывать PIX на схеме как PIX. Станция управления сетями всегда должна определять факт существования PIX, если от нее можно отправить запрос "ICMP-эхо" на PIX, но она может не отображать это устройство в виде PIX – черного прямоугольника с двумя индикаторами. Помимо необходимости поддержки

ipAddrTable IP-группы, станциям HPOV, Netview и большинству других станций управления сетями необходимо для правильного отображения значка распознавать, что OID, возвращаемый с помощью PIX, представляет собой OID устройства PIX.

Поддержка CiscoView для управления PIX была добавлена в CiscoView 5.2; устройство PIX версии 6.0.x также необходимо. В более ранних версиях PIX приложение управления сторонних производителей позволяет HPOV Network Node Manager определять PIX и системы, которые используют диспетчер межсетевых экранов PIX.

Обнаружение устройств внутри PIX

Если настройка PIX выполнена верно, входящие запросы и прерывания SNMP передаются. Поскольку трансляция сетевых адресов (NAT) обычно настраивается в среде PIX, для этого потребуются правила статической адресации. Проблема в том, что когда станция управления сетью делает snmpwalk общедоступного адреса, который является статичным для частного адреса внутри сети, внешний заголовок пакета не согласуется со сведениями в таблице ipAddrTable. Здесь адрес 171.68.118.150, возвращаемый функцией snmpwalk, является статичным для 10.10.10.20 внутри PIX, поэтому можно увидеть, куда устройство 171.68.118.150 отправляет отчеты о двух интерфейсах: 10.10.10.20 и 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
```

Имеет ли это смысл для станции управления сетью? Возможно, нет. Подобный аспект характерен и для прерываний: если интерфейс 10.31.1.50 выходит из строя, устройство 171.68.118.150 отошлет отчет о том, что интерфейс 10.31.1.50 был выведен из строя.

Другая проблема состоит в попытке внешнего управления внутренней сети, что приводит к "вытягиванию" сети. Если управляющей станцией является Netview или HPOV, данные продукты используют демон "netmon", чтобы прочитать таблицы маршрутов из устройств. Таблица маршрутов используется при обнаружении. PIX не поддерживает достаточное количество RFC 1213, чтобы вернуть таблицу маршрутов на станцию управления сетью, и с точки зрения безопасности это считается не очень удачной идеей. Пока устройства внутри PIX отчитываются о своих таблицах маршрутов при запросе статического адреса, все общедоступные IP-устройства (статические)отчитываются обо всех частных интерфейсах. Если другие частные адреса внутри PIX не являются статичными, их нельзя запросить. Если они статичны, станция управления сетью не знает ничего о статике.

Обнаружение устройств вне PIX

Поскольку станция управления сетью внутри PIX выполняет запросы об общедоступных адресах, которые присылают отчеты на "общие" интерфейсы, проблемы обнаружения входящего трафика не возникает.

Здесь 171.68.118.118 – входящий адрес, а 10.10.10.25 – исходящий. Когда 171.68.118.118 обнаруживает 10.10.10.25, устройство верно оповещает свои интерфейсы, это значит, что заголовок такой же как и внутри пакета:

```
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
```

Версия 6.2 snmpwalk PIX

Команда snmpwalk -c public <pix_ip_address> была использована на управляющей станции HPOV, чтобы выполнить команду snmpwalk. Все доступные MIB для PIX 6.2 были загружены до выполнения команды 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.
```

Информация, обязательная для сбора в случае обращения в Центр технической поддержки

Если после того, как шаги по устранению неполадок, описанные в данном документе выполнены, но все еще требуется помощь, обратитесь в TAC Cisco. Убедитесь, что были упомянуты следующие сведения для устранения неполадок в межсетевом экране PIX.
• Описание проблемы и соответствующие сведения о топологии • Выполнен ли процесс устранения неполадок перед созданием обращения • **Выходные данные команды show tech-support** • **Выходные данные команды show log после выполнения команды logging buffered debugging или снимки консоли, демонстрирующие проблему (при их наличии)** Присоедините собранные данные к запросу в простом текстовом формате (.txt), не архивируя файл. Информацию можно приложить к запросу путем загрузки с помощью программы подготовки запросов в Центр технической поддержки (только для зарегистрированных заказчиков). Если средство Case Query недоступно, необходимые данные можно отправить как вложение в электронное сообщение по адресу attach@cisco.com, указав в теме сообщения номер обращения.

Дополнительные сведения

- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Поддержка продуктов программного обеспечения Cisco PIX Firewall
- Запрос на комментарии (RFC)
- Cisco Systems – техническая поддержка и документация