セキュリティ アプライアンス PIX/ASA での SNMP の使用

内容

概要

Simple Network Management Protocol（SNMP）を使用して PIX 上のシステム イベントをモニタできます。 このドキュメントでは、次のような PIX での SNMP の使用方法について説明します。

- PIX *経由*または PIX *に対して* SNMP を実行するコマンド
- PIX の出力例
- PIX ソフトウェア リリース 4.0 以降の Management Information Base（MIB; 管理情報ベース）
- トラップ レベル
- syslog 重大度の例

- PIX および SNMP デバイス検出の問題

注：snmpget/snmpwalkのポートはUDP/161です。SNMPトラップのポートはUDP/162です。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Secure PIX Firewall ソフトウェア リリース 4.0 以降に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

関連製品

この設定は、Cisco Adaptive Security Appliance（ASA）バージョン 7.x でも使用できます。

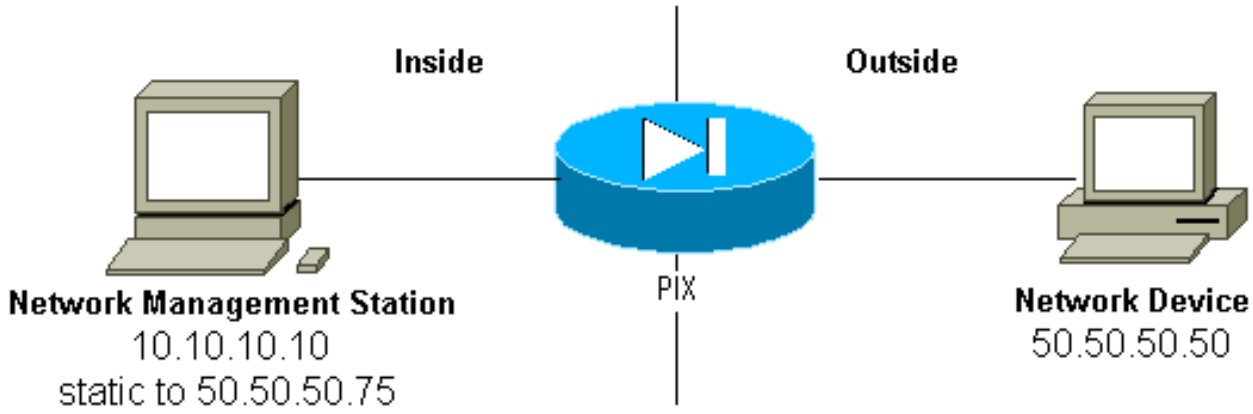
表記法

このドキュメントの出力と ログ データの行の一部は、スペースを節約するために折り返しています。

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

PIX/ASA を経由する SNMP

外部から内部へのトラップ



50.50.50.50 から 10.10.10.10 へのトラップを許可するには、次のように指定します。

```
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
```

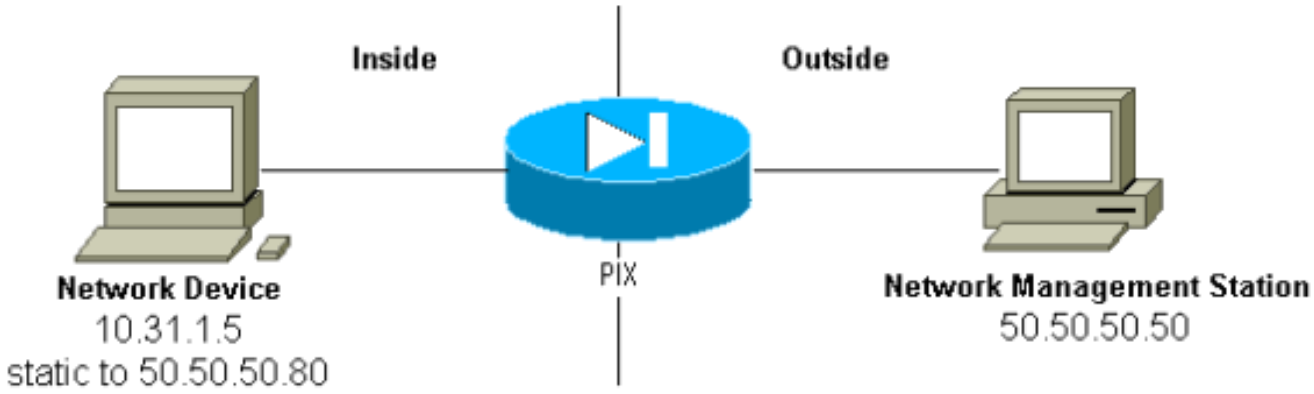
コンジットではなく、PIX 5.0 以降から利用できる Access Control List（ACL; アクセス コントロール リスト）を使用する場合は、次のように指定します。

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

PIXには次のように表示されます。

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

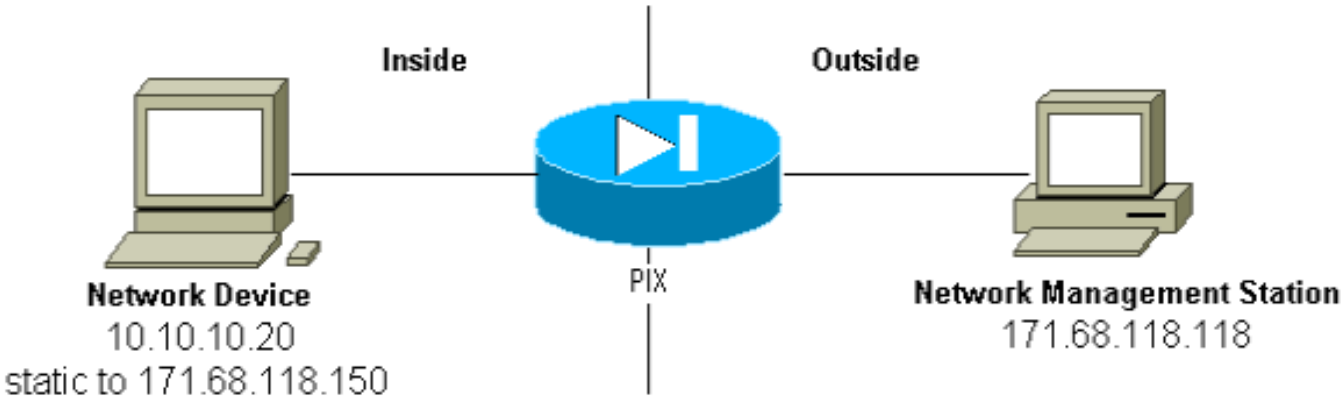
内部から外部へのトラップ



発信トラフィックはデフォルトで許可され（発信リストが存在しない場合）、PIX は次を示します。

```
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
```

外部から内部へのポーリング



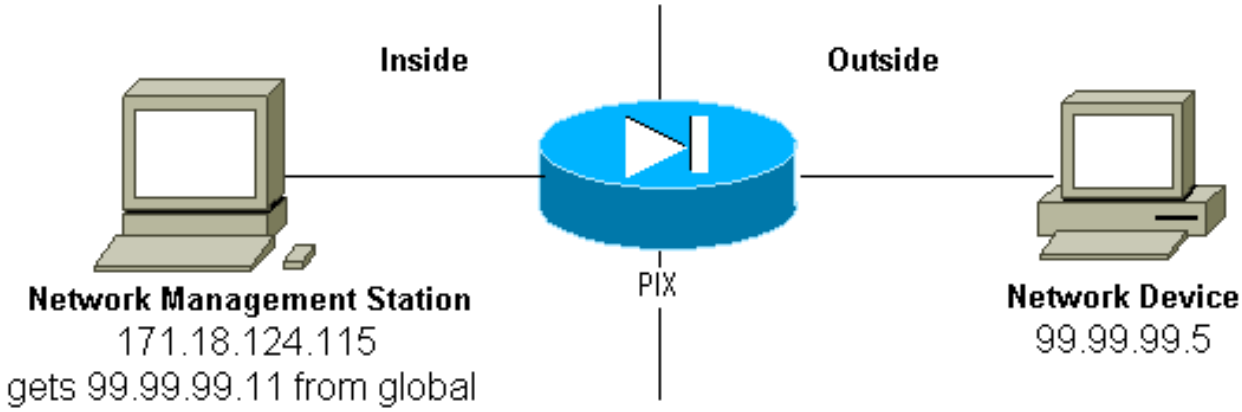
171.68.118.118 から 10.10.10.20 へのポーリングを許可するには、次のように指定します。

```
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
```

コンジットではなく、PIX 5.0 以降から利用できる ACL を使用する場合、次のように指定します。

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

Inside から Outside へのポーリング



発信トラフィックはデフォルトで許可され（発信リストが存在しない場合）、PIX は次を示します。

```
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 から PIX/ASA へ

バージョンごとの MIB サポート

次に示すのは、PIX における MIB サポートのバージョンです。

- PIX Firewallソフトウェアバージョン4.0 ~ 5.1:MIB-IIのシステムグループとインターフェイスグループ(RFC 1213を参照)。ただし、AT、ICMP、TCP、UDP、EGP、送信、IP、またはSNMPグループCISCO-SYSLOG-MIB V1SMI.my。
- PIX Firewall ソフトウェア バージョン 5.1.x 以降：以前の MIB と CISCO-MEMORY-POOL-MIB.my および CISCO-FIREWALL-MIB.my の cfwSystem ブランチ。
- PIX Firewall ソフトウェア バージョン 5.2.x 以降：以前の MIB と IP グループの ipAddrTable。
- PIX Firewall ソフトウェア バージョン 6.0.x 以降：モデルによって PIX を識別する（そして CiscoView 5.2 サポートをイネーブルにする）ための、以前の MIB と、MIB-II OID の変更。新しい Object IDentifier（OID; オブジェクト識別子）は CISCO-PRODUCTS-MIB にあります。たとえば、PIX 515 には OID 1.3.6.1.4.1.9.1.390 があります。
- PIX Firewall ソフトウェア バージョン 6.2.x 以降：以前の MIB と CISCO-PROCESS-MIB-

V1SMI.my。
- PIX/ASA ソフトウェア バージョン 7.x：以前の MIB と IF-MIB、SNMPv2-MIB、ENTITY-MIB、CISCO-REMOTE-ACCESS-MONITOR-MIB、CISCO-CRYPTO-ACCELERATOR-MIB、ALTIGA-GLOBAL-REG。

注：PROCESS MIBでサポートされているセクションは、ciscoProcessMIBObjectsブランチのcpmCPUブランチのcpmCPUTotalTableブランチです。ciscoProcessMIBNotifications ブランチ、ciscoProcessMIBconformance ブランチ、または MIB の ciscoProcessMIBObjects ブランチの cpmProcess ブランチにある 2 つのテーブル cpmProcessTable および cpmProcessExtTable はサポートされていません。

PIX/ASA での SNMP の有効化

次のコマンドを発行すると、PIX でポーリング/クエリおよびトラップを許可できます。

```
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 ソフトウェア バージョン 6.0.x 以降では、トラップとクエリに関してさらに細かく設定できます。

```
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 ソフトウェア バージョン 7.x では、トラップとクエリに関してさらに細かく設定できます。

```
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.
```

注：NMSをトラップの受信のみまたはブラウジング（ポーリング）だけに制限する場合は、trapまたはpollを指定します。デフォルトでは、NMS はどちらの機能も使用できます。

SNMP トラップは、デフォルトで UDP ポート 162 に送信されます。**udp-port** キーワードを使用すると、ポート番号を変更できます。

PIX/ASA への SNMP：ポーリング

PIX が返す変数は、そのバージョンの MIB サポートによって異なります。6.2.1 を稼動している PIX の snmpwalk の出力例が、このドキュメントの最後にあります。それよりも前のバージョンでは、前述した MIB 値だけが返されます。

PIX/ASA への SNMP：トラップ

注：PIX FirewallのSNMP OIDは、PIX Firewallから送信されたSNMPイベントトラップに表示されます。OID 1.3.6.1.4.1.9.1.227は、PIXソフトウェアバージョン6.0まではPIXファイアウォールシステムOIDとして使用されていました。新しいモデル固有のOIDはCISCO-PRODUCTS-MIBにあります。

次のコマンドを発行して、PIX 内のトラップをオンにします。

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

バージョン 4.0 から 5.1 までのトラップ

PIX ソフトウェア 4.0 以降を使用するときには、次のトラップを生成できます。

```
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
```

トラップの変更 (PIX 5.1)

PIX ソフトウェア バージョン 5.1.1 以降では、トラップ レベルは syslog トラップ用の syslog レベルとは別になっています。PIX は引き続き syslog トラップを送信できますが、さらに細かい設定が可能です。下の例で紹介する未加工の trapd.log ファイル (HP OpenView (HPOV) または Netview の場合も同様) には、3 つの link_up トラップと 9 つの syslog トラップが、次の 7 つの異なる syslog ID とともに含まれています：101003、104001、111005、111007、199002、302005、305002.

trapd.log の例

```
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
```

[各トラップの説明：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 重大度の例

次に示すメッセージは、7 つのメッセージを説明するため、マニュアルから複製されたものです。

```
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.
```

syslog 重大度の解釈

レベル	意味
0	システムが使用不能：緊急事態
1	ただちに措置が必要：警報

0	重大な状態：重大
3	エラー メッセージ：エラー
4	警告メッセージ：警告
5	通常の状態だが重要な状態：通知
6	情報：情報
7	デバッグ メッセージ：デバッグ

トラップのサブセット用の PIX 5.1 以降の設定

PIX 設定に次の値がある場合、

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

生成される唯一のトラップは、標準トラップである、コールド スタート、link up、および link down になります（syslog はない）。

PIX 設定に次の値がある場合、

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

すべての標準トラップおよびすべての syslog トラップが生成されます。ここで示す例では、これらが syslog エントリ、101003、104001、111005、111007、199002、302005、および 305002 と、PIX が生成した他のさまざまな出力になります。デバッグのために口ギング ヒストリが設定され、これらのトラップ番号が通知、警報、情報レベル内にあるので、レベル デバッグには次のものが含まれます。

PIX 設定に次の値がある場合、

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

標準およびデバッグより下のレベルにあるすべてのトラップが生成されます。**logging history notification** コマンドが使用されると、これは、緊急事態、警報、重大、エラー、警告、および通知レベル（ただし、情報レベルやデバッグ レベルではない）のすべての syslog トラップを含むことになります。 ここで示すものには、111005、111007、101003、および 104001（実稼動中のネットワークに PIX が生成する他のものすべて）が含まれます。

PIX 設定に次の値がある場合、

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

メッセージ 305002、302005、111005 は生成されません。**logging history debug** 用に PIX が設定される場合、先に示した 3 つ (305002、302005、111005) 以外の、メッセージ 104001、101003、111007、199002、および他のすべての PIX メッセージが表示されます。

トラップのサブセット用のPIX/ASA 7.xの設定

PIX 設定に次の値がある場合、

```
snmp-server host
```

生成される唯一のトラップは、標準トラップである、認証、コールド スタート、link up、link down になります (syslog はない) 。

残りの設定は、PIX/ASA バージョン 7.x を除く、PIX ソフトウェア バージョン 5.1 以降に似ており、**snmp-server enable traps** コマンドには、**ipsec**、**remote-access**、**entity などの追加のオプションがあります。**

注：PIX/ASAでのSNMPトラップの詳細は、『セキュリティアプライアンスの監視』の「SNMPの有効化」セクションを参照してください

SNMP の問題

PIX の検出

PIX が SNMP クエリに応答して、その OID を 1.3.6.1.4.1.9.1.227 として報告した場合、または PIX Firewall ソフトウェア バージョン 6.0 以降でそのモデルの CISCO-PRODUCTS-MIB に示された ID として報告した場合、PIX は設計したとおりに動作しています。

IP グループの ipAddrTable にサポートが追加されたときに、5.2.x よりも前の PIX コードのバージョンでは、ネットワーク管理ステーションがマップ上に PIX を PIX として引き出せない可能性があります。ネットワーク管理ステーションは、PIX を ping できる場合には PIX が存在することを常に検出できるはずですが、2 つのライトの付いたブラックボックスである PIX としてそれを引き出さない可能性もあります。IP グループの ipAddrTable をサポートする必要性に加えて、HPOV、Netview、および他のほとんどのネットワーク管理ステーションは、PIX によって戻される OID が、表示される適切なアイコン用の PIX であることを理解する必要があります。

PIX 管理用の CiscoView サポートは、CiscoView 5.2 で追加されました。PIX バージョン 6.0.x も必要です。以前の PIX バージョンでは、サードパーティ管理アプリケーションによって、HPOV Network Node Manager が PIX Firewall と PIX Firewall Manager を実行するシステムを識別できます。

PIX の Inside にあるデバイスの検出

PIX は、適切に設定されている場合、Outside から Inside に SNMP クエリとトラップを渡します。Network Address Translation（NAT; ネットワーク アドレス変換）は通常は PIX 上で設定されるので、これを行うにはスタティックであることが必要です。問題が生じるのは、ネットワーク管理ステーションが（静的にネットワーク内のプライベート アドレスになる）パブリック アドレスのsnmpwalk を実行する場合で、パケットの外部ヘッダーは ipAddrTable 内の情報と一致しません。ここでは 171.68.118.150 が走査され、これは、PIX の Inside の 10.10.10.20 に対してスタティックであり、デバイス 171.68.118.150 に 2 つのインターフェイス、10.10.10.20 および 10.31.1.50 が存在することが報告されているとわかります。

```
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
```

このことは、ネットワーク管理ステーションにとって意味のあることでしょうか。おそらくそのようなことはしないでしょう。同じ問題がトラップにも存在します。10.31.1.50 インターフェイスがダウンする場合、デバイス 171.68.118.150 はインターフェイス 10.31.1.50 がダウンしたと報告します。

Inside ネットワークを Outside から管理しようとするときの別の問題は、ネットワークを「引き出す」ことです。管理ステーションが Netview または HPOV である場合、これらの製品はデバイスからのルート テーブルを読み取るときに「netmon」デーモンを使用します。ルート テーブルは検出時に使用されます。PIXはRFC 1213を十分にサポートしていなく 、ルーティングテーブルをネットワーク管理ステーションに戻すことができず、セキュリティ上の理由から、これはまったく適切な考えではありません。スタティックがクエリされるときに PIX の Inside のデバイスが自身のルート テーブルを報告する一方で、すべてのパブリック IP デバイス（スタティック）はすべてのプライベート インターフェイスを報告します。PIX の Inside の他のプライベート アドレスは、スタティックでない場合、クエリの対象にはなれません。それらのアドレスが実際にはスタティックだとしても、ネットワーク管理ステーションには何がスタティックかを知る方法はありません。

PIX の Outside にあるデバイスの検出

PIX 内のネットワーク管理ステーションは「パブリック」インターフェイスを報告するパブリック アドレスを照会するため、外部から内部への検出の問題は該当しません。

ここでは、171.68.118.118 が Inside で、10.10.10.25 が Outside でした。171.68.118.118 が 10.10.10.25 を走査したとき、ボックスはそのインターフェイスを正確に報告しています。その内容は、ヘッダーがパケットの Inside と同じであるということです。

```
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
```

PIX のバージョン 6.2 snmpwalk

snmpwalk -c public <pix_ip_address> コマンドは、snmpwalk を実行するために HPOV 管理ステーションで使用されていました。PIX 6.2 で利用できるすべての MIB は、snmpwalk を実行する前にロードされました。

```
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.
```

TAC サービス リクエストをオープンする場合に収集する情報

このドキュメントで説明したトラブルシューティング手順を実行しても、なおサポートが必要で、Cisco TAC でサービス リクエストをオープンする場合には、ご使用の PIX Firewall のトラブルシューティングに必要な次の情報をご提供ください。
• 問題の説明と関連するトポロジの詳細 • サービス リクエストをオープンする前に実行したトラブルシューティング • show tech-support コマンドの出力 • **logging buffered debugging コマンド実行後の show log コマンドの出力、あるいは、問題を示すコンソール キャプチャ（採取されている場合）** 収集したデータは、圧縮しないプレーン テキスト形式（.txt）でサービス リクエストに添付してください。 サービスリクエストに情報を添付するには、TAC Service Request Tool（登録ユーザ専用）を使用してアップロードします。 Service Request Tool にアクセスできない場合は、電子メールへの添付で、attach@cisco.com に情報を送信できます。この場合は、メッセージの件名（Subject）行にサービス リクエスト番号を記入してください。

関連情報

- Cisco Secure PIX ファイアウォール コマンド リファレンス
- Cisco PIX Firewall Software に関する製品サポート
- Request for Comments（RFC）
- テクニカル サポートとドキュメント – Cisco Systems