# Uso di SNMP con le appliance di sicurezza PIX/ASA

## Sommario



## Introduzione

Èpossibile monitorare gli eventi di sistema sul PIX utilizzando il protocollo SNMP (Simple Network Management Protocol). Questo documento descrive come usare il protocollo SNMP con il protocollo PIX, che include:

- Comandi per eseguire *il protocollo* SNMP *attraverso* il PIX o *verso* il PIX
- Uscita PIX di esempio
- Supporto MIB (Management Information Base) nel software PIX versione 4.0 e successive
- Livelli di trapping
- esempi di livello di gravità syslog
- Problemi di rilevamento dei dispositivi PIX e SNMP

**Nota:** la porta per snmpget/snmpwalk è UDP/161. La porta per le trap SNMP è UDP/162.

# Prerequisiti

## Requisiti

Nessun requisito specifico previsto per questo documento.

## Componenti usati

Il riferimento delle informazioni contenute in questo documento è il software Cisco Secure PIX Firewall versione 4.0 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco Adaptive Security Appliance (ASA) versione 7.x.

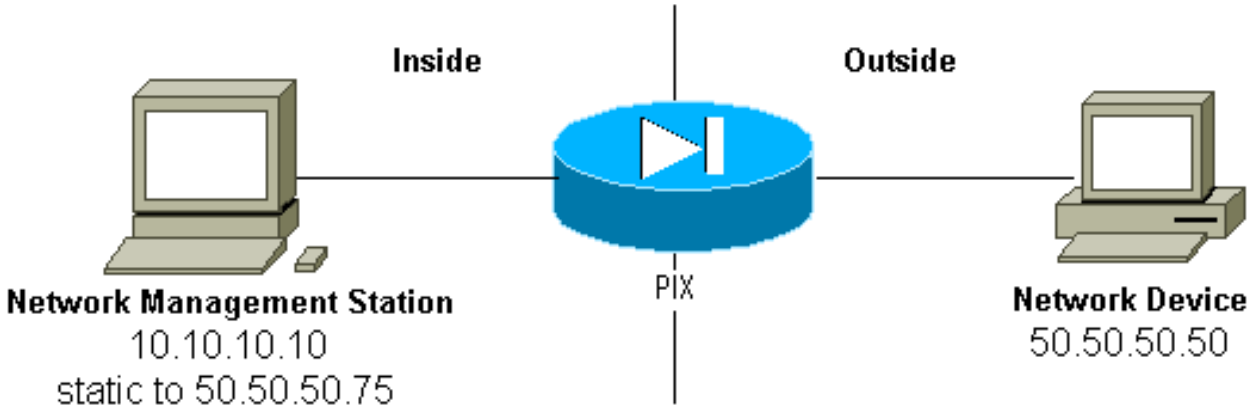
## Convenzioni

per motivi di spazio, alcune righe di output e dati di registro di questo documento sono state riportate a capo.

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

# SNMP tramite PIX/ASA

## Trap dall'esterno all'interno




Per consentire l'accesso delle trap da 50.50.50.50 a 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
```

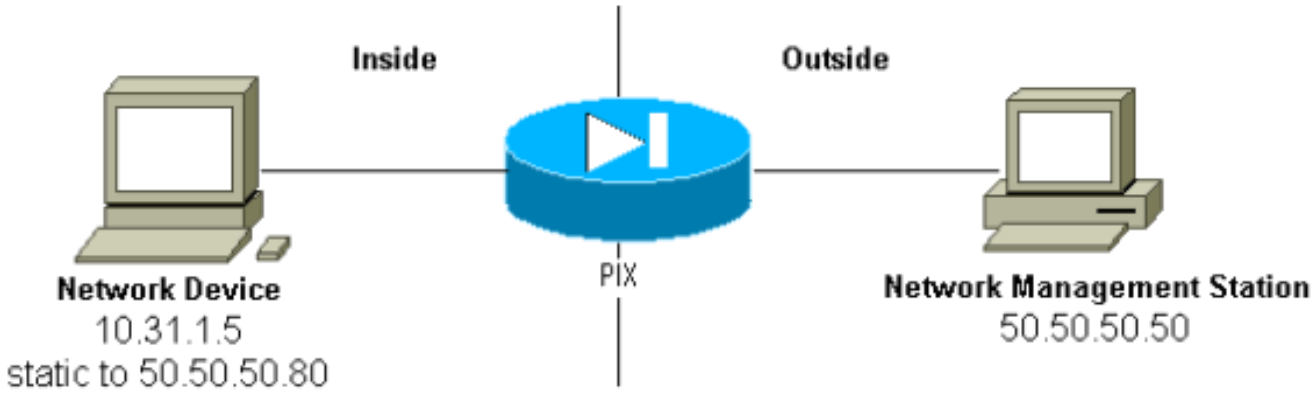
Se si utilizzano gli elenchi di controllo di accesso (ACL), disponibili in PIX 5.0 e versioni successive, anziché i condotti:

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

Il PIX mostra:

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

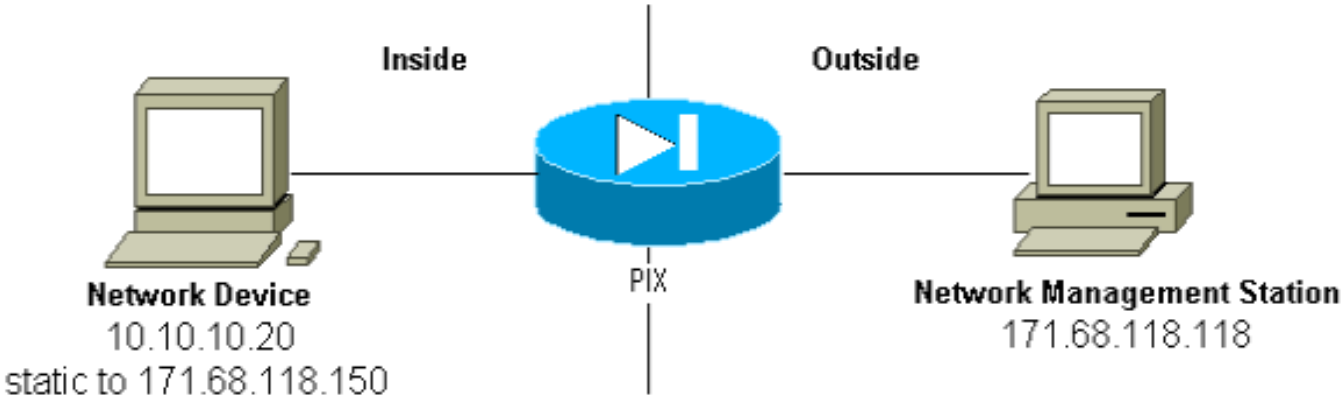
## Trap dall'interno all'esterno




Il traffico in uscita è consentito per impostazione predefinita (in assenza di elenchi in uscita) e il PIX mostra:

```
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
```

## Polling dall'esterno all'interno



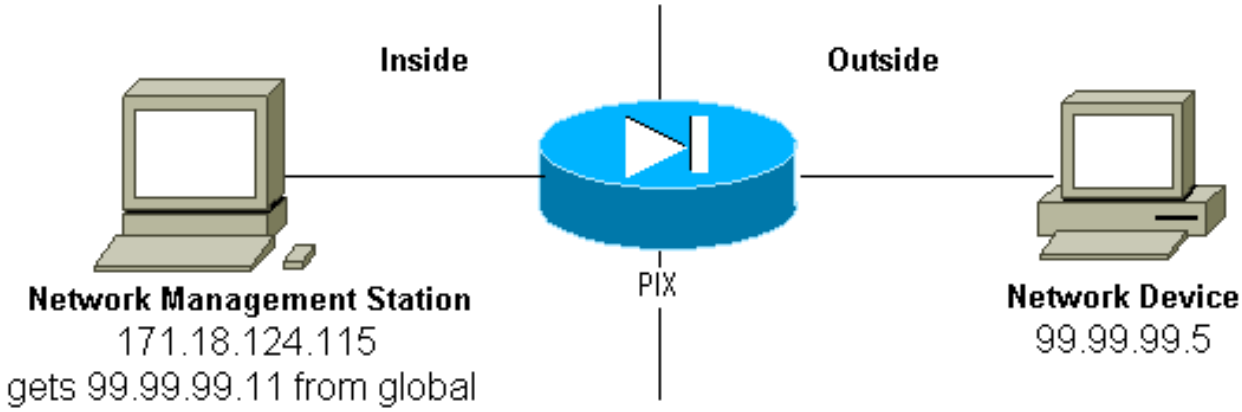

Per consentire lo scrutinio da 171.68.118.118 a 10.10.10.20:

```
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
```

Se si usano gli ACL, disponibili in PIX 5.0 e versioni successive, al posto dei condotti:

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

### Polling dall'interno all'esterno




Il traffico in uscita è consentito per impostazione predefinita (in assenza di elenchi in uscita) e il PIX mostra:

```
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 su PIX/ASA

### Supporto MIB per versione

Queste sono le versioni del supporto MIB in PIX:

- PIX Firewall Software versioni da 4.0 a 5.1 - Gruppi di sistema e di interfaccia di MIB-II (fare riferimento alla RFC 1213 ) ma non ai gruppi AT, ICMP, TCP, UDP, EGP, trasmissione, IP o SNMP CISCO-SYSLOG-MIB-V1SMI.my.
- Software PIX Firewall versione 5.1.x e successive—Precedenti MIB e CISCO-MEMORY-POOL-MIB.my e la sezione cfwSystem di CISCO-FIREWALL-MIB.my.
- PIX Firewall Software versioni 5.2.x e successive - MIB precedenti e ipAddrTable del gruppo IP.
- PIX Firewall Software versioni 6.0.x e successive - MIB precedenti e modifica di MIB-II OID per identificare PIX per modello (e abilitare il supporto di CiscoView 5.2). I nuovi identificatori di oggetto (OID) si trovano in CISCO-PRODUCTS-MIB; ad esempio, il PIX 515 ha l'OID 1.3.6.1.4.1.9.1.390.
- PIX Firewall Software versioni 6.2.x e successive—Previous MIBs and CISCO-PROCESS-

MIB-V1SMI.my.
- Software PIX/ASA versione 7.x - MIB e IF-MIB precedenti, SNMPv2-MIB, ENTITY-MIB, CISCO-REMOTE-ACCESS-MONITOR-MIB, CISCO-CRYPTO-ACCELERATOR-MIB, ALTIGA-GLOBAL-REG.

**Nota:** la sezione supportata del MIB PROCESS è la diramazione cpmCPUTotalTable della diramazione cpmCPU della diramazione ciscoProcessMIBObjects. Il ramo ciscoProcessMIBotifications, ciscoProcessMIBconformance o le due tabelle cpmProcessTable e cpmProcessExtTable non sono supportati nel ramo cpmProcessMIBbjects del ramo ciscoProcessMIBObjects del MIB.

## Attivazione di SNMP in PIX/ASA

Utilizzare questi comandi per consentire polling/query e trap nel 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
```

Il software PIX versione 6.0.x e successive consentono una maggiore granularità per quanto riguarda trap e query.

```
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.
```

Il software PIX/ASA versione 7.x consente una maggiore granularità per quanto riguarda trap e query.

```
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.
```

**Nota:** specificare **trap** o **polling** se si desidera limitare il sistema NMS alla sola ricezione di trap o alla sola navigazione (polling). Per impostazione predefinita, NMS può utilizzare entrambe le funzioni.

Le trap SNMP vengono inviate sulla porta UDP 162 per impostazione predefinita. Il numero di porta può essere modificato con la parola chiave **udp-port**.

## SNMP su PIX/ASA - Polling

Le variabili restituite dal PIX dipendono dal supporto mib nella versione. Alla fine di questo documento è riportato un esempio di output di uno snmpwalk di un PIX con esecuzione 6.2.1. Le versioni precedenti del software restituiscono solo i valori mib annotati in precedenza.

## SNMP su PIX/ASA - Trap

**Nota:** un OID SNMP per PIX Firewall viene visualizzato nelle trap di eventi SNMP inviate dal PIX Firewall. OID 1.3.6.1.4.1.9.1.227 è stato utilizzato come OID di sistema del firewall PIX fino alla versione 6.0 del software PIX. I nuovi OID specifici del modello si trovano in CISCO-PRODUCTS-MIB.

Utilizzare i seguenti comandi per attivare le trap in PIX:

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

## Trap Versione 4.0 Fino A 5.1

Quando si utilizza PIX Software 4.0 e versioni successive, è possibile generare le seguenti trap:

```
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
```

## Modifiche ai trap (PIX 5.1)

Nel software PIX versione 5.1.1 e successive, i livelli di trap sono separati dai livelli syslog per le trap syslog. Il PIX invia ancora trap syslog, ma è possibile configurare una maggiore granularità. Nell'esempio seguente, il file raw trapd.log (lo stesso per HP OpenView [HPOV] o Netview) include 3 trap link_up e 9 trap syslog, con 7 ID syslog diversi: 101003, 104001, 111005, 111007, 199002, 302005, 305002.

## Esempio di 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
```

## Descrizione di ogni trap - trapd.log

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



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


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


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


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


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

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


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


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


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


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


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

## Esempi di livello di gravità syslog

Questi sono riprodotti dalla documentazione per illustrare i sette messaggi.

```
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.
```

## Interpreta livelli di gravità syslog

| Livello | Significato |
|---|---|
| 0 | Sistema inutilizzabile - emergenza |
| 1 | Azione immediata - avviso |
| 2 | Condizione critica - critica |
| 3 | Messaggio di errore - errore |

| | |
|---|---|
| 4 | Messaggio di avviso - avviso |
| 5 | Condizione normale ma significativa - notifica |
| 6 | Informativo - Informativo |
| 7 | Messaggio di debug - debug |

## Configurazione di PIX 5.1 e versioni successive per un sottoinsieme di trap

Se la configurazione PIX ha:

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

le uniche trap generate sono quelle standard: cold start, link up e link down (non syslog).

Se la configurazione PIX ha:

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

vengono quindi generate tutte le trap standard e syslog. Nell'esempio, queste sono le voci syslog 101003, 104001, 111005, 111007, 199002, 302005 e 305002 e qualsiasi altro output syslog generato dal PIX. Poiché la cronologia di registrazione impostata per il debug e questi numeri di trap sono nei livelli di notifica, avviso e informazione, il debug del livello include quanto segue:

Se la configurazione PIX ha:

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

quindi vengono generati tutti i trap standard e tutti i trap al livello sottostante al debug. Se si usa il comando **logging history notification**, questo include tutte le trap syslog a livello di emergenza, di alert, critico, di errore, di avvertenza e di notifica (ma non a livello informativo o di debug). Nel nostro caso, i numeri 111005, 111007, 101003 e 104001 (e qualsiasi altra cosa il PIX genererebbe in una rete attiva) sarebbero inclusi.

Se la configurazione PIX ha:

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

i messaggi 305002, 302005, 111005 non vengono prodotti. Se PIX è impostato per il **debug della cronologia di registrazione**, verranno visualizzati i messaggi 104001, 101003, 111007, 19002 e

tutti gli altri messaggi PIX, ma non i 3 elencati (305002, 302005, 111005).

### Configurazione di PIX/ASA 7.x per un sottoinsieme di trap

Se la configurazione PIX ha:

```
snmp-server host
```

le uniche trap generate sono quelle standard: autenticazione, avvio a freddo, collegamento attivo e collegamento non attivo (non syslog).

La configurazione rimanente è simile a quella del software PIX versione 5.1 e successive, ad eccezione della versione 7.x di PIX/ASA, in cui il comando **snmp-server enable traps** dispone di opzioni aggiuntive come **ipsec**, **accesso remoto** ed **entità**

**Nota: per** ulteriori informazioni sulle trap SNMP in PIX/ASA, consultare la sezione Abilitazione del protocollo SNMP di Monitoraggio dell'appliance di sicurezza

# Problemi SNMP

## Rilevamento PIX

Se il PIX risponde a una query SNMP e segnala il suo OID come 1.3.6.1.4.1.9.1.227, o nelle versioni 6.0 o successive del software del firewall PIX, come ID elencato nel CISCO-PRODUCTS-MIB per tale modello, il PIX funziona come previsto.

Nelle versioni del codice PIX precedenti alla 5.2.x, quando era stato aggiunto il supporto per ipAddrTable del gruppo IP, le stazioni di gestione di rete potrebbero non essere in grado di disegnare il PIX sulla mappa come PIX. Una stazione di gestione di rete dovrebbe sempre essere in grado di rilevare il fatto che il PIX esiste se è in grado di eseguire il ping del PIX, ma potrebbe non disegnarlo come un PIX - una scatola nera con 2 luci. Oltre a richiedere il supporto della tabella ipAddrTable del gruppo IP, HPOV, Netview e la maggior parte delle altre stazioni di gestione di rete devono capire che l'OID restituito dal PIX è quello di un PIX affinché venga visualizzata l'icona corretta.

Il supporto CiscoView per la gestione PIX è stato aggiunto in CiscoView 5.2; È richiesta anche la versione PIX 6.0.x. Nelle versioni PIX precedenti, un'applicazione di gestione di terze parti consente a HPOV Network Node Manager di identificare i firewall PIX e i sistemi che eseguono PIX Firewall Manager.

## Individua dispositivi all'interno del PIX

Se il PIX è configurato correttamente, passa le query e le trap SNMP dall'esterno all'interno. Poiché Network Address Translation (NAT) è in genere configurato sul PIX, per eseguire questa

operazione sono necessarie statistiche. Il problema si verifica quando la stazione di gestione della rete esegue un'istantanea dell'indirizzo pubblico, che esegue la statica in un indirizzo privato all'interno della rete, l'intestazione esterna del pacchetto non concorda con le informazioni contenute nell'ipAddrTable. Qui viene camminato 171.68.118.150, che è statico a 10.10.10.20 all'interno del PIX ed è possibile vedere dove il dispositivo 171.68.118.150 segnala di avere due interfacce: 10.10.10.20 e 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
```

Per una stazione di gestione di rete, tutto questo è sensato? Probabilmente no. Lo stesso problema si presenterà per le trap: se l'interfaccia 10.31.1.50 non è operativa, il dispositivo 171.68.118.150 non è attivo.

Un altro problema nel tentativo di gestire una rete interna dall'esterno è quello di "disegnare" la rete. Se la stazione di gestione è Netview o HPOV, questi prodotti utilizzano un daemon "netmon" per leggere le tabelle di routing dai dispositivi. La tabella di route viene utilizzata nell'individuazione. Il PIX non supporta abbastanza la RFC 1213 per restituire una tabella di routing a una stazione di gestione di rete e, per motivi di sicurezza, questa non è comunque una buona idea. Mentre i dispositivi all'interno del PIX segnalano le tabelle di routing quando viene eseguita una query sull'immagine statica, tutti i dispositivi IP pubblici (statistiche) segnalano tutte le interfacce private. Se gli altri indirizzi privati all'interno del PIX non contengono statistiche, non è possibile eseguirne una query. Se hanno delle statistiche, la stazione di gestione della rete non ha modo di sapere quali siano le statistiche.

### Individua dispositivi esterni al PIX

Poiché una stazione di gestione di rete all'interno del PIX interroga un indirizzo pubblico che segnala le interfacce "pubbliche", il rilevamento dei problemi interni o esterni non è applicabile.

Qui, 171.68.118.118 era dentro e 10.10.10.25 era fuori. Quando la cassetta 171.68.118.118 ha camminato 10.10.10.25, ha segnalato correttamente le sue interfacce, ossia l'intestazione è la stessa del pacchetto:

```
ip.ipAddrTable.ipAddrEntry.ipAdEntAddr.10.10.10.25 : IpAddress: 10.10.10.25
ip.ipAddrTable.ipAddrEntry.ipAdEntAddr.10.31.1.50 : IpAddress: 10.31.1.50
```

## Snmpwalk versione 6.2 di PIX

Il comando **snmpwalk -c public <indirizzo_ip_ip>** è stato utilizzato su una stazione di gestione HPOV per eseguire snmpwalk. Tutti i MIB disponibili per PIX 6.2 sono stati caricati prima di eseguire la procedura guidata.

```
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.
```

## Informazioni da raccogliere se si apre una richiesta TAC

**Se dopo aver completato la procedura di risoluzione dei problemi descritta in questo documento si desidera ancora ricevere assistenza e si desidera aprire una richiesta di assistenza in Cisco TAC, includere queste**

| informazioni per risolvere i problemi relativi a PIX Firewall. |
| --- |
| • Descrizione del problema e dettagli sulla topologia<br>• Risoluzione dei problemi eseguita prima dell'apertura della richiesta<br>• Output del comando **show tech-support**<br>• Output del comando **show log** dopo l'esecuzione con il comando **logging buffered debugging** o acquisizioni della console che dimostrano il problema (se disponibili)<br>Allegare i dati raccolti alla richiesta in formato testo normale non compresso (txt). È possibile allegare informazioni alla richiesta caricandola tramite lo strumento TAC Service Request (solo utenti registrati). Se non è possibile accedere allo strumento Case Query, inviare le informazioni in un allegato e-mail a attach@cisco.com con il numero della richiesta in oggetto. |

## Informazioni correlate

- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Supporto dei prodotti software Cisco PIX Firewall
- RFC (Request for Comments)
- Documentazione e supporto tecnico – Cisco Systems