itoring Cisco Secure PIX Firewall Using SNMP and Syslog Thro

Table of Contents

Monitoring Cisco Secure PIX Firewall Using SNMP and Syslog Through VPN Tunnel

Introduction

.Cisco Secure PIX Firewalls are commonly used in site−to−site VPN deployment where the PIXs are used as IPSec VPN termination devices. In either the simple site−to−site design or the more complicated hub−and−spoke design, people sometimes want to monitor all the PIX Firewalls using the Simple Network Management Protocol (SNMP) server and syslog server located at a central site.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

This configuration was developed and tested using the software and hardware versions below.

- Cisco PIX Firewall Software Release 6.1(1)
- PIX Firewall 520 and 515
- A Solaris system running HPOV 6.1 as SNMP and syslog server

Background Theory

For general information regarding how to use SNMP to monitor Cisco Secure PIX Firewall, please refer to Using SNMP with the Cisco Secure PIX Firewall.

For general information regarding how to setup syslog on Cisco Secure PIX Firewall, please refer to Setting Up PIX Syslog.

The goals for this sample configuration were:

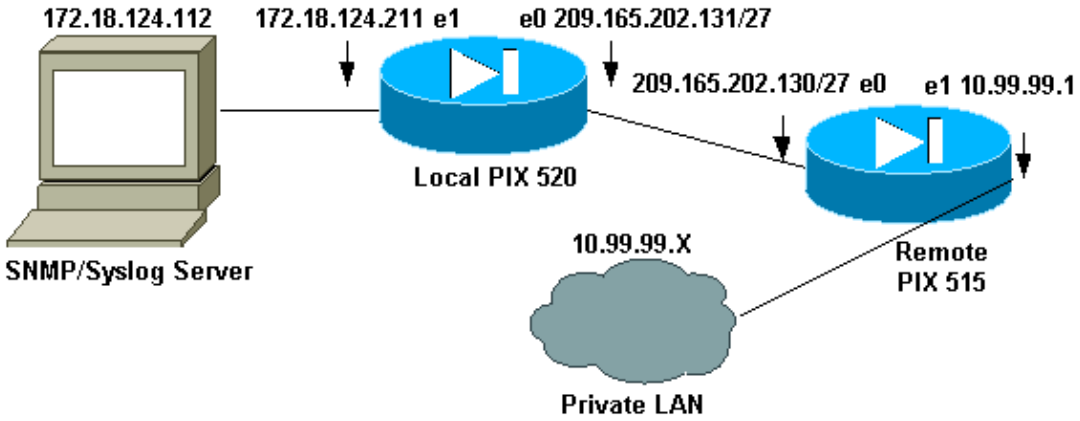
- To have data between the 10.99.99.X & 172.18.124.X networks encrypted. This includes syslog and SNMP between the 10.99.99.X network and the 172.18.124.112 SNMP/syslog server.
- To be able to have both PIXs send syslog to the SNMP/syslog server.
- To be able to do SNMP queries to and send traps from both PIXs to the SNMP/syslog server.

Configure

This sample configuration demonstrates how to monitor a Cisco Secure PIX Firewall using SNMP and syslog through the existing VPN tunnels.

Network Diagram

This document uses the network setup shown in the diagram below.



Configurations

Local PIX Firewall (PIX 520)

```
PIX Version 6.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
nameif ethernet3 intf3 security15
nameif ethernet4 intf4 security20
nameif ethernet5 intf5 security25
enable password OnTrBUG1Tp0edmkr encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix-520b
domain-name cisco.com
fixup protocol ftp 21
```

```
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names

!--- Define IPSec interesting traffic.
!--- This line covers traffic between the LAN segment behind two PIXs.
!--- It also covers the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind PIX 515.

access-list 101 permit ip 172.18.124.0 255.255.255.0 10.99.99.0 255.255.255.0

!--- This line covers SNMP and syslog traffic from SNMP/syslog server to remote
!--- PIX outside interface.

access-list 101 permit ip host 172.18.124.112 host 209.165.202.130
pager lines 24
logging on
logging trap debugging
logging history debugging

!--- Define logging host information.

logging facility 16
logging host inside 172.18.124.112
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
ip address outside 209.165.202.131 255.255.255.224
ip address inside 172.18.124.211 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
ip address intf3 127.0.0.1 255.255.255.255
ip address intf4 127.0.0.1 255.255.255.255
ip address intf5 127.0.0.1 255.255.255.255
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0
failover ip address intf3 0.0.0.0
failover ip address intf4 0.0.0.0
failover ip address intf5 0.0.0.0
pdm history enable
arp timeout 14400
global (outside) 1 209.165.202.132

!--- Bypass NAT for IPSec traffic.
```

```
nat (inside) 0 access-list 101
conduit permit udp any any
conduit permit tcp any any
conduit permit icmp any any
route outside 0.0.0.0 0.0.0.0 209.165.202.130 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323
0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
http server enable
http 172.18.124.112 255.255.255.255 inside

!--- Define SNMP configuration.

snmp-server host inside 172.18.124.112
no snmp-server location
no snmp-server contact
snmp-server community test
snmp-server enable traps
floodguard enable

!---IPSec configuration.

sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto map vpn 10 ipsec-isakmp
crypto map vpn 10 match address 101
crypto map vpn 10 set peer 209.165.202.130
crypto map vpn 10 set transform-set myset
crypto map vpn interface outside
isakmp enable outside
isakmp key ******** address 209.165.202.130 netmask 255.255.255.255
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:03b5bc406e18006616ffbaa32caeccd1
: end
```

Remote PIX Firewall (PIX 515)

```
PIX Version 6.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
nameif ethernet3 intf3 security15
nameif ethernet4 intf4 security20
nameif ethernet5 intf5 security25
enable password OnTrBUG1Tp0edmkr encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX515A
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
```

```
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names

!--- Define IPSec interesting traffic.
!--- This line covers traffic between the LAN segment behind two PIXs.
!--- It also covers the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind PIX 515.

access-list 101 permit ip 10.99.99.0 255.255.255.0 172.18.124.0 255.255.255.0

!--- This line covers the SNMP and syslog traffic sent from this PIX outside
!--- interface to the server.

access-list 101 permit ip host 209.165.202.130 host 172.18.124.112
pager lines 24
logging on
logging timestamp
logging monitor debugging
logging trap debugging
logging history debugging

!--- Define syslog server.

logging facility 23
logging host outside 172.18.124.112
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
ip address outside 209.165.202.130 255.255.255.224
ip address inside 10.99.99.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
ip address intf3 127.0.0.1 255.255.255.255
ip address intf4 127.0.0.1 255.255.255.255
ip address intf5 127.0.0.1 255.255.255.255
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0
failover ip address intf3 0.0.0.0
failover ip address intf4 0.0.0.0
failover ip address intf5 0.0.0.0
pdm history enable
arp timeout 14400
global (outside) 1 209.165.202.133

!--- Bypass NAT for IPSec traffic.
```

```
nat (inside) 0 access-list 101
route outside 0.0.0.0 0.0.0.0 209.165.202.131 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323
0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
http server enable
http 10.99.99.99 255.255.255.255 inside

!--- Define SNMP server.

snmp-server host outside 172.18.124.112
no snmp-server location
no snmp-server contact
snmp-server community test
snmp-server enable traps
floodguard enable

!--- IPSec configuration.

sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto map vpn 10 ipsec-isakmp
crypto map vpn 10 match address 101
crypto map vpn 10 set peer 209.165.202.131
crypto map vpn 10 set transform-set myset
crypto map vpn interface outside
isakmp enable outside
isakmp key ******** address 209.165.202.131 netmask 255.255.255.255
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:edb21b64ab79eeb6eaf99746c94a1e36
: end
```

SNMP and syslog Server Setup Information

HPOV 6.1 is used as the SNMP server application.

For syslog collection, the syslog daemon (syslogd) is used, and syslog information from the local PIX and the remote PIX are stored in different files based on the logging facility configured on the PIX Firewall.

The **/etc/syslog.conf** file has:

```
local0.debug /var/log/local.log
local7.debug /var/log/remote.log
```

On the local PIX configuration, **logging facility 16** corresponds to LOCAL0.

On the remote PIX configuration, **logging facility 23** corresponds to LOCAL7.

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: The **clear** commands must be performed in config mode.

- **clear crypto ipsec sa** − To reset the IPSec associations after failed attempts to negotiate a VPN tunnel.
- **clear crypto isakmp sa** − To reset the Internet Security Association and Key Management Protocol (ISAKMP) security associations after failed attempts to negotiate a VPN tunnel.
- **show crypto engine ipsec** − To display the encrypted sessions.

Troubleshoot

Troubleshooting Commands

Note: Before issuing **debug** commands, please see Important Information on Debug Commands.

- **debug crypto ipsec** − To see if a client is negotiating the IPSec portion of the VPN connection.
- **debug crypto isakmp** − To see if the peers are negotiating the ISAKMP portion of the VPN connection.

Sample Debug Output

SNMP Output

The following examples demonstrate how to use snmpwalk to monitor both PIX Firewalls' buffer utilization. The Object Identifier (OID) for buffer status is:

```
"cfwBufferStatsTable"     "1.3.6.1.4.1.9.9.147.1.2.2.1"
```

- Monitoring the remote PIX Firewall

```
Script started on Tue Oct 09 21:53:54 2001
# ./snmpwalk −c test 209.165.202.130 1.3.6.1.4.1.9.9.147.1.2.2.1
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.
cfwBufferStatInformation.2560.3 : OCTET STRING- (ascii):
maximum number of allocated 2560 byte blocks
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatInformation.2560.5 : OCTET STRING- (ascii):
fewest 2560 byte blocks available since system startup
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatInformation.2560.8 : OCTET STRING- (ascii):
current number of available 2560 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: 399
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: 750
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatValue.256.5 : Gauge32: 746
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatValue.256.8 : Gauge32: 749
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatValue.1550.3 : Gauge32: 1956
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatValue.1550.5 : Gauge32: 1166
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatValue.1550.8 : Gauge32: 1188
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatValue.2560.3 : Gauge32: 200
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatValue.2560.5 : Gauge32: 196
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatValue.2560.8 : Gauge32: 199
```

- Monitoring the local PIX Firewall

```
Script started on Tue Oct 09 21:54:53 2001
# ./snmpwalk -c test 172.18.124.211  1.3.6.1.4.1.9.9.147.1.2.2.1
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.
cfwBufferStatInformation.2560.3 : OCTET STRING- (ascii):
maximum number of allocated 2560 byte blocks
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatInformation.2560.5 : OCTET STRING- (ascii):
fewest 2560 byte blocks available since system startup
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatInformation.2560.8 : OCTET STRING- (ascii):
current number of available 2560 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: 397
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: 1500
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatValue.256.5 : Gauge32: 1497
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatValue.256.8 : Gauge32: 1499
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatValue.1550.3 : Gauge32: 2468
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatValue.1550.5 : Gauge32: 1686
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatValue.1550.8 : Gauge32: 1700
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
```

```
cfwBufferStatValue.2560.3 : Gauge32: 200
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatValue.2560.5 : Gauge32: 198
cisco.ciscoMgmt.ciscoFirewallMIB.ciscoFirewallMIBObjects.cfwSystem.
cfwStatistics.cfwBufferStatsTable.cfwBufferStatsEntry.
cfwBufferStatValue.2560.8 : Gauge32: 199
```

Show block Command

The output of the **snmpwalk** of the cfw Buffer Statistics Table corresponds to the following **show** command on the remote PIX.

```
PIX−515A# show block
```

SIZE	MAX	LOW	CNT
4	1600	1599	1600
80	400	399	400
256	750	746	749
1550	1956	1166	1188
2560	200	196	199

The output of the **snmpwalk** of the cfw Buffer Statistics Table corresponds to the following **show** command on the local PIX.

```
PIX−520B# show block
```

SIZE	MAX	LOW	CNT
4	1600	1599	1600
80	400	397	400
256	1500	1497	1499
1550	2468	1686	1700
2560	200	198	199

Verifying IPSec Tunnel

- Remote **show crypto ipsec sa**

```
PIX515A# show crypto ipsec sa


interface: outside
    Crypto map tag: vpn, local addr. 209.165.202.130

   local  ident (addr/mask/prot/port): (10.99.99.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (172.18.124.0/255.255.255.0/0/0)
   current_peer: 209.165.202.131
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1962, #pkts encrypt: 1962, #pkts digest 1962
    #pkts decaps: 1963, #pkts decrypt: 1963, #pkts verify 1963
```

```
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0,
 #pkts decompress failed: 0
 #send errors 0, #recv errors 0

  local crypto endpt.: 209.165.202.130, remote crypto endpt.:
     209.165.202.131
  path mtu 1500, ipsec overhead 56, media mtu 1500
  current outbound spi: 3411a392

  inbound esp sas:
   spi: 0x554ad733(1430968115)
     transform: esp-des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 4, crypto map: vpn
     sa timing: remaining key lifetime (k/sec): (4608000/28472)
     IV size: 8 bytes
     replay detection support: Y
   spi: 0x63a866ca(1671980746)
     transform: esp-des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 2, crypto map: vpn
     sa timing: remaining key lifetime (k/sec): (4607747/27373)
     IV size: 8 bytes
     replay detection support: Y


  inbound ah sas:


  inbound pcp sas:


  outbound esp sas:
   spi: 0x3411a392(873571218)
     transform: esp-des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 3, crypto map: vpn
     sa timing: remaining key lifetime (k/sec): (4608000/28463)
     IV size: 8 bytes
     replay detection support: Y
   spi: 0x7523ba4a(1965275722)
     transform: esp-des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 1, crypto map: vpn
     sa timing: remaining key lifetime (k/sec): (4607798/27366)
     IV size: 8 bytes
     replay detection support: Y


  outbound ah sas:


  outbound pcp sas:



local  ident (addr/mask/prot/port):
   (209.165.202.130/255.255.255.255/0/0)
remote ident (addr/mask/prot/port):
   (172.18.124.112/255.255.255.255/0/0)
current_peer: 209.165.202.131
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 26, #pkts encrypt: 26, #pkts digest 26
```

```
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify 7
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0
    #send errors 12, #recv errors 0

     local crypto endpt.: 209.165.202.130, remote crypto endpt.:
        209.165.202.131
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 326421ac

     inbound esp sas:
      spi: 0x6eeec108(1861140744)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 6, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4608000/28159)
        IV size: 8 bytes
        replay detection support: Y


     inbound ah sas:


     inbound pcp sas:

   outbound esp sas:
      spi: 0x326421ac(845423020)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4607994/28159)
        IV size: 8 bytes
        replay detection support: Y


     outbound ah sas:


     outbound pcp sas:
```

- Local **show crypto ipsec sa**

```
PIX-520B# show crypto ipsec sa

interface: outside
    Crypto map tag: vpn, local addr. 209.165.202.131

   local  ident (addr/mask/prot/port): (172.18.124.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.99.99.0/255.255.255.0/0/0)
   current_peer: 209.165.202.130
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4169, #pkts encrypt: 4169, #pkts digest 4169
    #pkts decaps: 4168, #pkts decrypt: 4168, #pkts verify 4168
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0
    #send errors 2, #recv errors 0

     local crypto endpt.: 209.165.202.131, remote crypto endpt.:
        209.165.202.130
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 63a866ca

     inbound esp sas:
```

```
   spi: 0x7523ba4a(1965275722)
     transform: esp-des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 4, crypto map: vpn
     sa timing: remaining key lifetime (k/sec): (4607560/28160)
     IV size: 8 bytes
     replay detection support: Y


  inbound ah sas:


  inbound pcp sas:


  outbound esp sas:
   spi: 0x63a866ca(1671980746)
     transform: esp-des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 3, crypto map: vpn
     sa timing: remaining key lifetime (k/sec): (4607705/28151)
     IV size: 8 bytes
     replay detection support: Y


  outbound ah sas:


  outbound pcp sas:



local  ident (addr/mask/prot/port):
   (172.18.124.112/255.255.255.255/0/0)
remote ident (addr/mask/prot/port):
   (209.165.202.130/255.255.255.255/0/0)
current_peer: 209.165.202.130
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 8, #pkts encrypt: 8, #pkts digest 8
 #pkts decaps: 32, #pkts decrypt: 32, #pkts verify 32
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0,
 #pkts decompress failed: 0
 #send errors 0, #recv errors 0

  local crypto endpt.: 209.165.202.131, remote crypto endpt.:
     209.165.202.130
  path mtu 1500, ipsec overhead 56, media mtu 1500
  current outbound spi: 6eeec108

  inbound esp sas:
   spi: 0x326421ac(845423020)
     transform: esp-des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 2, crypto map: vpn
     sa timing: remaining key lifetime (k/sec): (4607993/27715)
     IV size: 8 bytes
     replay detection support: Y


  inbound ah sas:


  inbound pcp sas:
```

```
outbound esp sas:
 spi: 0x6eeec108(1861140744)
   transform: esp-des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 1, crypto map: vpn
   sa timing: remaining key lifetime (k/sec): (4608000/27706)
   IV size: 8 bytes
   replay detection support: Y


outbound ah sas:


outbound pcp sas:
```

Syslog Output

- Remote Syslog Output

```
# more /var/log/remote.log

Oct 11 22:28:08 209.165.202.130 Oct 11 2001 18:08:01: %PIX-6-302010:
0 in use, 4 most used
Oct 11 22:28:08 209.165.202.130 Oct 11 2001 18:08:01: %PIX-6-302010:
0 in use, 4 most used
Oct 11 22:38:07 209.165.202.130 Oct 11 2001 18:18:01: %PIX-6-302010:
0 in use, 4 most used
Oct 11 22:38:07 209.165.202.130 Oct 11 2001 18:18:01: %PIX-6-302010:
0 in use, 4 most used
Oct 11 22:47:50 209.165.202.130 Oct 11 2001 18:27:44: %PIX-5-111007:
Begin configuration: console reading from terminal
Oct 11 22:47:50 209.165.202.130 Oct 11 2001 18:27:44: %PIX-5-111007:
Begin configuration: console reading from terminal
Oct 11 22:47:57 209.165.202.130 Oct 11 2001 18:27:51: %PIX-5-111005:
console end configuration: OK
Oct 11 22:47:57 209.165.202.130 Oct 11 2001 18:27:51: %PIX-5-111005:
console end configuration: OK
```

- Local Syslog Output

```
# more /var/log/local.log

Oct 11 22:54:03 [172.18.124.211.2.2] %PIX-5-111005:
console end configuration: OK
Oct 11 22:54:03 [172.18.124.211.2.2] %PIX-5-111005:
console end configuration: OK
Oct 11 22:54:07 [172.18.124.211.2.2] %PIX-5-111007: Begin configuration:
console reading from terminal
Oct 11 22:54:07 [172.18.124.211.2.2] %PIX-5-111007: Begin configuration:
console reading from terminal
Oct 11 22:54:11 [172.18.124.211.2.2] %PIX-5-111005:
console end configuration: OK
Oct 11 22:54:11 [172.18.124.211.2.2] %PIX-5-111005:
console end configuration: OK
Oct 11 22:54:26 [172.18.124.211.2.2] %PIX-6-302010:
   0 in use, 9 most used
Oct 11 22:54:26 [172.18.124.211.2.2] %PIX-6-302010:
   0 in use, 9 most used
```

Information to Collect if You Open a TAC Case

If you still need assistance after following the troubleshooting steps above and want to open a case with the Cisco TAC, be sure to include the following information for troubleshooting your PIX Firewall.
• Problem description and relevant topology details • Troubleshooting performed before opening the case • Output from the **show tech−support** command • Output from the **show log** command after running with the **logging buffered debugging** command, or console captures that demonstrate the problem (if available) Please attach the collected data to your case in non−zipped, plain text format (.txt). You can attach information to your case by uploading it using the Case Query Tool (registered customers only) . If you cannot access the Case Query Tool, you can send the information in an email attachment to attach@cisco.com with your case number in the subject line of your message.

Related Information

- **Using SNMP with the Cisco Secure PIX Firewall**
- **Cisco Security PIX Firewall Command Reference**
- **Setting Up PIX Syslog**
- **PIX Support Page**
- **Documentation for PIX Firewall**
- **PIX Command References**
- **Requests for Comments (RFCs)**
- **Technical Support − Cisco Systems**