IDS-APP1# sh ver
Application Partition:

Cisco Systems Intrusion Detection Sensor, Version 4.0(1)S37

OS Version 2.4.18-5smpbigphys
Platform: IDS-4210
Sensor up-time is 4 days.
Using 257024000 out of 261312512 bytes of available memory (98% usage)
Using 528M out of 17G bytes of available disk space (4% usage)

MainApp	2003_Jan_23_02.00	(Release)	2003-01-23T02:00:25-0600	Running
AnalysisEngine	2003_Jan_23_02.00	(Release)	2003-01-23T02:00:25-0600	Running
Authentication	2003_Jan_23_02.00	(Release)	2003-01-23T02:00:25-0600	Running
Logger	2003_Jan_23_02.00	(Release)	2003-01-23T02:00:25-0600	Running
NetworkAccess	2003_Jan_23_02.00	(Release)	2003-01-23T02:00:25-0600	Running
TransactionSource	2003_Jan_23_02.00	(Release)	2003-01-23T02:00:25-0600	Running
WebServer	2003_Jan_23_02.00	(Release)	2003-01-23T02:00:25-0600	Running
CLI	2003_Jan_17_18.33	(Release)	2003-01-17T18:33:18-0600	

Upgrade History:

  IDS-K9-maj-4.0-1-S36   00:04:22 UTC Sun Nov 09 2003

Recovery Partition Version 1.1 - 4.0(1)S37

IDS-APP1#?

clear	Clear system settings or devices
clock	Set system clock settings
configure	Enter configuration mode
copy	Copy iplog or configuration files
erase	Erase a logical file
exit	Terminate current CLI login session
iplog	Control ip logging on the interface group
iplog-status	Display a list of IP Logs currently existing in the system
more	Display a logical file
no	Remove or disable system settings
ping	Send echo messages to destination
remove-xl	Indicate that the hardware accelerator card has been removed from the system
reset	Shutdown the sensor applications and reboot
setup	Perform basic sensor configuration
show	Display system settings and/or history information
ssh	Secure Shell Settings
terminal	Change terminal configuration parameters
tls	Configure TLS settings
trace	Display the route an IP packet takes to a destination

IDS-APP1# show ?

clock	Display system clock
events	Display local event log contents
history	Display commands entered in current menu
interfaces	Display statistics and information about system interfaces
privilege	Display current user access role
ssh	Display Secure Shell information

```
statistics       Display application statistics
tech-support     Generate report of current system status
tls              Display tls certificate information
users            Show all users currently logged into the system
version          Display product version information
```

IDS-APP1# show interface ?

```
<cr>
clear               Clear statistics after read
command-control     Display statistics and information about the command-control
interface
group               Display statistics and information about the interface
groups
sensing             Display statistics and information about the sensing
interfaces
```

IDS-APP1# show interface group

```
Group 0 is up
  Sensing ports int0
  Logical virtual sensor configuration: virtualSensor
  Logical alarm channel configuration:  virtualAlarm

VirtualSensor0
   General Statistics for this Virtual Sensor
      Number of seconds since a reset of the statistics = 2017
      Total number of packets processed since reset = 58
      Total number of IP packets processed since reset = 0
      Total number of packets that were not IP processed since reset = 58
      Total number of TCP packets processed since reset = 0
      Total number of UDP packets processed since reset = 0
      Total number of ICMP packets processed since reset = 0
      Total number of packets that were not TCP, UDP, or ICMP processed since
reset = 0
      Total number of ARP packets processed since reset = 0
      Total number of ISL encapsulated packets processed since reset = 0
      Total number of 802.1q encapsulated packets processed since reset = 0
      Total number of packets with bad IP checksums processed since reset = 0
      Total number of packets with bad layer 4 checksums processed since reset =
0
      Total number of bytes processed since reset = 6813
      The rate of packets per second since reset = 0
      The rate of bytes per second since reset = 3
      The average bytes per packet since reset = 117
   Fragment Reassembly Unit Statistics for this Virtual Sensor
      Number of fragments currently in FRU = 0
      Number of datagrams currently in FRU = 0
      Number of fragments received since reset = 0
      Number of complete datagrams reassembled since reset = 0
      Number of incomplete datagrams abandoned since reset = 0
      Number of fragments discarded since reset = 0
   Statistics for the TCP Stream Reassembly Unit
      Current Statistics for the TCP Stream Reassembly Unit
         TCP streams currently in the embryonic state = 0
         TCP streams currently in the established state = 0
         TCP streams currently in the closing state = 0
         TCP streams currently in the system = 0
         TCP Packets currently queued for reassembly = 0
```

```
      Cumulative Statistics for the TCP Stream Reassembly Unit since reset
         TCP streams that have been tracked since last reset = 0
         TCP streams that had a gap in the sequence jumped = 0
         TCP streams that was abandoned due to a gap in the sequence = 0
         TCP packets that arrived out of sequence order for their stream = 0
         TCP packets that arrived out of state order for their stream = 0
         The rate of TCP connections tracked per second since reset = 0
   The Signature Database Statistics.
      The Number of each type of node active in the system (can not be reset)
         Total nodes active = 0
         TCP nodes keyed on both IP addresses and both ports = 0
         UDP nodes keyed on both IP addresses and both ports = 0
         IP nodes keyed on both IP addresses = 0
      The number of each type of node inserted since reset
         Total nodes inserted = 0
         TCP nodes keyed on both IP addresses and both ports = 0
         UDP nodes keyed on both IP addresses and both ports = 0
         IP nodes keyed on both IP addresses = 0
      The rate of nodes per second for each time since reset
         Nodes per second = 0
         TCP nodes keyed on both IP addresses and both ports per second = 0
         UDP nodes keyed on both IP addresses and both ports per second = 0
         IP nodes keyed on both IP addresses per second = 0
      The number of root nodes forced to expire because of memory constraints
         TCP nodes keyed on both IP addresses and both ports = 0
   Alarm Statistics for this Virtual Sensor
      Number of alarms triggered by events = 1
      Number of alarms excluded by filters = 0
      Number of alarms removed by summarizer = 0
      Number of alarms sent to the Event Store = 1

IDS-APP1# show interface sensing
Sensing int0 is up
  Hardware is eth0, TX
  Reset port

MAC statistics from the IntelPro interface
   Link = up
   Speed = 10
   Duplex = half
   State = up
   Rx_Packets = 59
   Tx_Packets = 0
   Rx_Bytes = 6047
   Tx_Bytes = 0
   Rx_Errors = 0
   Tx_Errors = 0
   Rx_Dropped = 0
   Tx_Dropped = 0
   Multicast = N/A
   Collisions = 0
   Rx_Length_Errors = 0
   Rx_Over_Errors = 0
   Rx_CRC_Errors = 0
   Rx_Frame_Errors = 0
   Rx_FIFO_Errors = 0
   Rx_Missed_Errors = 0
```

```
   Tx_Aborted_Errors = 0
   Tx_Carrier_Errors = 0
   Tx_FIFO_Errors = 0
   Tx_Heartbeat_Errors = 0
   Tx_Window_Errors = 0
   Rx_TCP_Checksum_Good = 0
   Rx_TCP_Checksum_Bad = 0
   Tx_TCP_Checksum_Good = 0
   Tx_TCP_Checksum_Bad = 0
   Tx_Abort_Late_Coll = 0
   Tx_Deferred_Ok = 0
   Tx_Single_Coll_Ok = 0
   Tx_Multi_Coll_Ok = 0
   Rx_Long_Length_Errors = 0
   Rx_Align_Errors = 0
   Tx_Flow_Control_Pause = 0
   Rx_Flow_Control_Pause = 0
   Rx_Flow_Control_Unsup = 0
   Tx_TCO_Packets = 0
   Rx_TCO_Packets = 0
   Rx_Interrupt_Packets = 59
   MDIX_Status = MDI
   Cable_Status = Cable
   OK = Cable
   Dropped Packet Percent = 0

Sensing int1 is up
  Hardware is eth1, TX
  Reset port
  Command control port
```

IDS-APP1# show interface command-control

```
command-control is up
  Internet address is 10.1.5.2, subnet mask is 255.255.255.0, telnet is enabled.
  Hardware is eth1, tx

Network Statistics
   eth1      Link encap:Ethernet  HWaddr 00:02:B3:A4:93:CD
             inet addr:10.1.5.2  Bcast:10.1.5.255  Mask:255.255.255.0
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:1539 errors:0 dropped:0 overruns:0 frame:0
             TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:100
             RX bytes:90505 (88.3 Kb)  TX bytes:336 (336.0 b)
             Interrupt:5 Base address:0xee80 Memory:febfa000-febfa038
```

IDS-APP1# show statistics ?

```
Authentication        Display authentication statistics
EventServer           Display event server statistics
EventStore            Display event store statistics
Host                  Display host statistics
Logger                Display logger statistics
NetworkAccess         Display network access controller statistics
TransactionServer     Display transaction server statistics
TransactionSource     Display transaction source statistics
WebServer             Display web server statistics
```

```
IDS-APP1# show statistics eventstore
Event store statistics
   General information about the event store
      The current number of open subscriptions = 1
      The number of events lost by subscriptions and queries = 0
      The number of queries issued = 0
      The number of times the event store circular buffer has wrapped = 0
   Number of events of each type currently stored
      Debug events = 0
      Status events = 6
      Log transaction events = 17
      Shun request events = 0
      Error events, warning = 1
      Error events, error = 0
      Error events, fatal = 0
      Alert events, informational = 1
      Alert events, low = 0
      Alert events, medium = 0
      Alert events, high = 0

IDS-APP1# show statistics authentication
General
   totalAuthenticationAttempts = 0
   failedAuthenticationAttempts = 0

IDS-APP1# show events ?
<cr>
alert          Display local system alerts
error          Display error events
hh:mm[:ss]     Display start time
log            Display log events
nac            Display NAC shun events
status         Display status events

IDS-APP1# show events alert ?
<cr>
hh:mm[:ss]        Display start time
high              Display local high system alerts
informational     Display local informational system alerts
low               Display local system low alerts
medium            Display local medium system alerts
sig-attribute     Display local alerts matching the specified attribute.

IDS-APP1# show events alert informational

IDS-APP1# more ?
backup-config      Display the saved backup system configuration
current-config     Display the current system configuration

IDS-APP1# copy ?
/erase           Erase the destination file before copying
<source-url>     Location of source file to be copied
iplog            IP log

IDS-APP1# erase ?
backup-config      Delete the backup-configuration file
```

```
current-config     Delete the current-configuration file


IDS-APP1# conf t
IDS-APP1(config)# ?
display-serial     Re-direct all terminal output to the serial port
downgrade          Remove the last applied upgrade
end                Exit configuration mode and return to exec mode
exit               Exit configuration mode and return to exec mode
hostname           Set the sensor's hostname
interface          Enter configuration mode for system interfaces
no                 Remove configuration
password           Modify current user password on the local sensor
privilege          Modify user privilege
recover            Re-image the application partition from the recovery
partition
service            Enter configuration mode for node services
show               Display system settings and/or history information
ssh                Secure Shell Settings
telnet-server      Modify telnet-server settings
tls                Configure TLS settings
upgrade            Upgrade system software and signatures
username           Add a user to the local sensor

IDS-APP1(config)# interface ?
command-control     Enter configuration mode for the command control interface
group               Enter configuration mode for a sensing interface group
sensing             Enter configuration mode for a sensing interface

IDS-APP1(config)# interface command-control
IDS-APP1(config-if)#?
end      Exit interface configuration mode and return to exec mode
exit     Exit interface configuration mode and return to global configuration
mode
ip       Configure IP information for interface
show     Display system settings and/or history information
IDS-APP1(config-if)# ip ?
address             Set the IP address and subnet mask for the interface
default-gateway     Set the default gateway for the interface

IDS-APP1(config-if)# ip address 10.1.5.2 255.255.255.0

IDS-APP1(config-if)# ip default-gateway 10.1.5.1

IDS-APP1(config)# interface sensing int0
IDS-APP1(config-ifs)#?
end          Exit interface sensing configuration mode and return to exec mode
exit         Exit interface sensing configuration mode and return to global
configuration mode
no           Remove configuration
show         Display system settings and/or history information
shutdown     Disable the sensing interface

IDS-APP1(config)# interface group 0
IDS-APP1(config-ifg)#?
end                   Exit interface group configuration mode and return to exec
mode
```

```
exit                    Exit interface group configuration mode and return to
global configuration mode
no                      Remove configuration
sensing-interface       Add a sensing interface to the interface group
show                    Display system settings and/or history information
shutdown                Disable the interface group
```

IDS-APP1(config-ifg)# sensing-interface int0

IDS-APP1(config)# upgrade ?

```
<source-url>     Location of upgrade
```

IDS-APP1(config)# downgrade ?

```
<cr>
```

IDS-APP1(config)# downgrade

```
Error: No downgrade available
```

IDS-APP1(config)# recover ?

```
application-partition     Re-image the application partition from the recovery partition
```

IDS-APP1(config)# privilege user idsview operator

IDS-APP1(config)# service host
IDS-APP1(config-Host)#?

```
exit                      Exit service configuration mode
networkParams             Network configuration parameters
no                        Remove an entry or selection setting
optionalAutoUpgrade       Optional AutoUpgrade configuration
show                      Display system settings and/or history information
timeParams                Time configuration parameters
```

IDS-APP1(config-Host)# networkparams
IDS-APP1(config-Host-net)#?

```
accessList          list of trusted hosts
default             Set the value back to the system default setting
defaultGateway      Command and Control interface default gateway
exit                Exit networkParams configuration submode
hostname            Sensor hostname
ipAddress           Command and Control interface IP address
netmask             Command and Control interface netmask
no                  Remove an entry or selection setting
show                Display system settings and/or history information
telnetOption        option for turning off telnet service
```

IDS-APP1(config)# service ?

```
alarm-channel-configuration      Enter configuration mode for the alarm channel
Authentication                   Enter configuration mode for user authentication
options
Host                             Enter configuration mode for node configuration
Logger                           Enter configuration mode for debug logger
NetworkAccess                    Enter configuration mode for the network access
controller
SshKnownHosts                    Enter configuration mode for configuring SSH known
hosts
TrustedCertificates              Enter configuration mode for configuring trusted
certificates
virtual-sensor-configuration     Enter configuration mode for the virtual sensor
WebServer                        Enter configuration mode for the web server application
```

IDS-APP1(config)# username testuser privilege ?

```
administrator     Allows full system privileges
operator          May modify most configuration
service           Logs directly into a system shell
viewer            No modification allowed view only
```

IDS-APP1(config)# service virtual-sensor-configuration virtualsensor
Error: Cannot create a new virtual sensor configuration. "virtualSensor" is currently the only conf.
IDS-APP1(config)# service virtual-sensor-configuration virtualSensor
IDS-APP1(config-vsc)#?

```
end                   Exit configuration mode and return to exec mode
exit                  Exit configuration mode and return to global configuration mode
reset-signatures      Reset signatures settings back to the default configuration
show                  Display system settings and/or history information
tune-micro-engines    Enter micro-engine tuning mode
```

IDS-APP1(config-vsc)# tune-micro-engines
IDS-APP1(config-vsc-virtualSensor)#?

```
ATOMIC.ARP                        Layer 2 ARP signatures.
ATOMIC.ICMP                       Simple ICMP alarms based on Type, Code, Seq, Id, etc.
ATOMIC.IPOPTIONS                  Simple L3 Alarms based on Ip Options
ATOMIC.L3.IP                      Simple L3 IP Alarms.
ATOMIC.TCP                        Simple TCP packet alarms based on TCP Flags, ports
(both sides), a.
ATOMIC.UDP                        Simple UDP packet alarms based on Port, Direction and
DataLength.
exit                              Exit service configuration mode
FLOOD.HOST.ICMP                   Icmp Floods directed at a single host
FLOOD.HOST.UDP                    UDP Floods directed at a single host
FLOOD.NET                         Multi-protocol floods directed at a network segment.
Ip Addresses.
FragmentReassembly                Fragment Reassembly configuration tokens
IPLog                             Virtual Sensor IP log configuration tokens
OTHER                             This engine is used to group generic signatures so
common paramete.
SERVICE.DNS                       DNS SERVICE Analysis Engine
SERVICE.FTP                       FTP service special decode alarms
SERVICE.GENERIC                   Custom service/payload decode and analysis based on our
quartet tu.
SERVICE.HTTP                      HTTP protocol decode based string search Engine.
Includes anti-evan
SERVICE.IDENT                     Ident service (client and server) alarms.
SERVICE.MSSQL                     Microsoft (R) SQL service inspection engine
SERVICE.NTP                       Network Time Protocol based signature engine
SERVICE.RPC                       RPC SERVICE analysis engine
SERVICE.SMB                       SMB Service decode inspection.
SERVICE.SMTP                      SMTP Protocol Inspection Engine
SERVICE.SNMP                      Inspects SNMP traffic
SERVICE.SSH                       SSH header decode signatures.
SERVICE.SYSLOG                    Engine to process syslogs.
show                              Display system settings and/or history information
ShunEvent                         Shun Event configuration tokens
STATE.STRING.CISCOLOGIN           Telnet based Cisco Login Inspection Engine
STATE.STRING.LPRFORMATSTRING      LPR Protocol Inspection Engine
StreamReassembly                  Stream Reassembly configuration tokens
STRING.ICMP                       Generic ICMP based string search Engine
STRING.TCP                        Generic TCP based string search Engine.
STRING.UDP                        Generic UDP based string search Engine
SWEEP.HOST.ICMP                   ICMP host sweeps from a single attacker to many
victims.
SWEEP.HOST.TCP                    TCP-based Host Sweeps from a single attacker to
multiple victims.
```

```
SWEEP.MULTI                     UDP and TCP combined port sweeps.
SWEEP.OTHER.TCP                 Odd sweeps/scans such as nmap fingerprint scans.
SWEEP.PORT.TCP                  Detects port sweeps between two nodes.
SWEEP.PORT.UDP                  Detects UDP connections to multiple destination ports
between two .
systemVariables                 User modifiable system variables
TRAFFIC.ICMP                    Identifies ICMP traffic irregularities.
TROJAN.BO2K                     BackOrifice BO2K trojan traffic
TROJAN.TFN2K                    TFN2K trojan/ddos traffic
TROJAN.UDP                      Detects BO/BO2K UDP trojan traffic.
```

```
IDS-APP1(config)# service alarm-channel-configuration virtualAlarm
IDS-APP1(config-acc)#?
end                  Exit configuration mode and return to exec mode
exit                 Exit configuration mode and return to global configuration mode
show                 Display system settings and/or history information
tune-alarm-channel   Enter configuration mode for the alarm channel
```

```
IDS-APP1(config-acc)# tune-alarm-channel
IDS-APP1(config-acc-virtualAlarm)#?
EventFilter         Configuration for the Event Filters.
exit                Exit service configuration mode
show                Display system settings and/or history information
systemVariables     User modifiable system variables
```

```
IDS-APP1(config-acc-virtualAlarm)# EventFilter
IDS-APP1(config-acc-virtualAlarm-Eve)#?
default     Set the value back to the system default setting
exit        Exit EventFilter configuration submode
Filters     Defines the Filter Rules
no          Remove an entry or selection setting
show        Display system settings and/or history information
```

```
IDS-APP1(config-acc-virtualAlarm-Eve)# filters ?
<cr>
DestAddrs       Source Addresses of Events to which this filter should be
applied.
Exception       Does this filter describe an exception to an event filter?  This
allows creating 'General Case' exclusions then a.
SIGID           Signature ID's of Events to which this filter should be applied.
SourceAddrs     Source Addresses of Events to which this filter should be
applied.
SubSig          SubSigID's of Events to which this filter should be applied.
```