

# Troubleshooting Cisco Secure Intrusion Detection Systems

## Session 2503

# Agenda

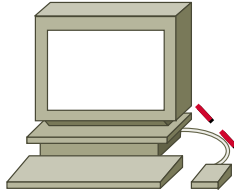
- **Introduction and Overview of IDS**
- **Director Issues**
- **Troubleshooting the Sensor**
- **The Integrated Software Router**
- **And the Netsonar**
- **Case Study 1**
- **Case Study 2**

# Agenda

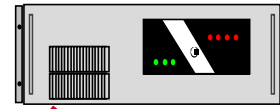
- **Introduction and Overview of IDS**
- **Director Issues**
- **Troubleshooting the Sensor**
- **The Integrated Software Router**
- **And the Netsonar**
- **Case Study 1**
- **Case Study 2**

# NetRanger Components

NetRanger Director



NetRanger Sensor



Communications

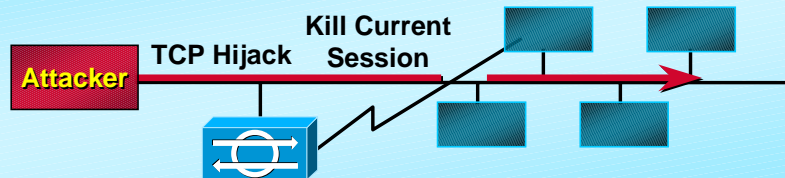


# Event Actions: Response

## Session Termination and Shunning

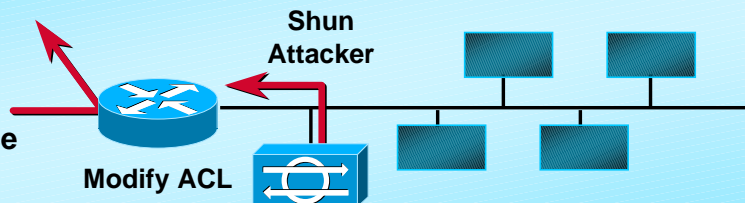
### Session Termination

Terminates an Active TCP Session



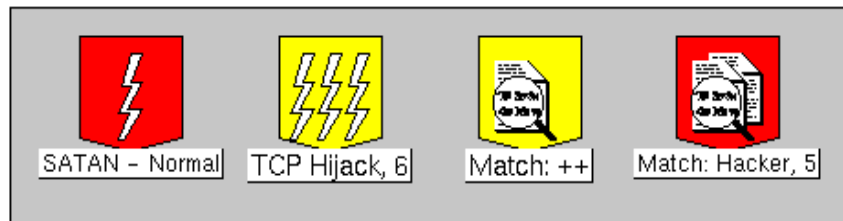
### Shunning

Reconfigure Filters  
This Requires the Device Management Option



# Event Actions: Alarm Notification

- Alarms are transmitted as soon as they are detected. This generally occurs within a second
- The PostOffice protocol relies upon a positive acknowledgement scheme over UDP to make sure that a director receives the alarm

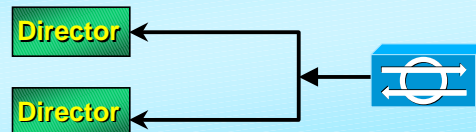


# NetRanger Communications

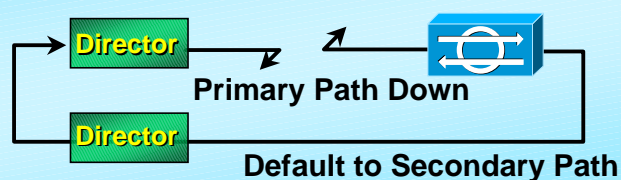
**Reliability:** Sensor waits for an acknowledgment of every alarm sent to the director



**Redundancy:** The sensor can send alarms to multiple directors



**Fault Tolerance:** The sensor supports multiple routes to a single destination. If the primary route is down the sensor defaults to secondary route



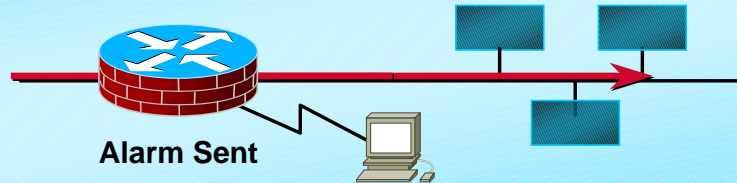
# Event Actions

Attack

Info

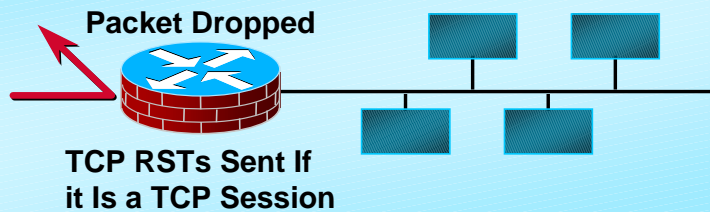
## Alarm

Console Messages  
syslog  
PostOffice



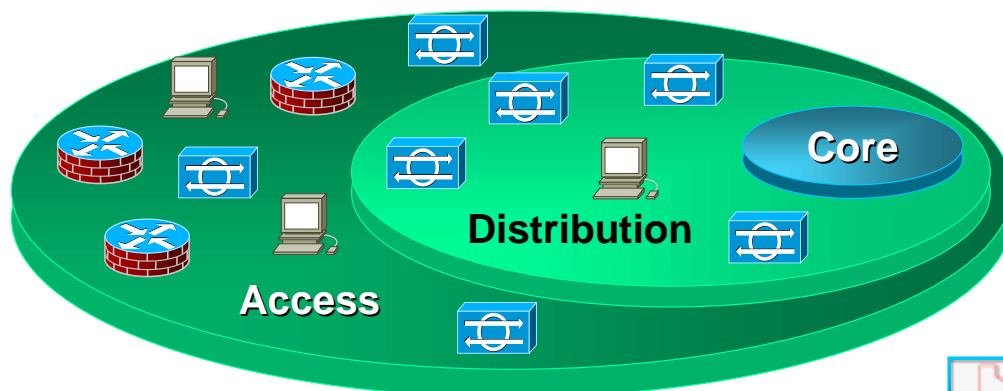
## Drop Reset

These Are Expected  
to Be Used Together  
but Can Be Individually  
Configured



# Implementation

- The Cisco IOS Firewall with Intrusion Detection can be used to supplement an Intrusion Detection System



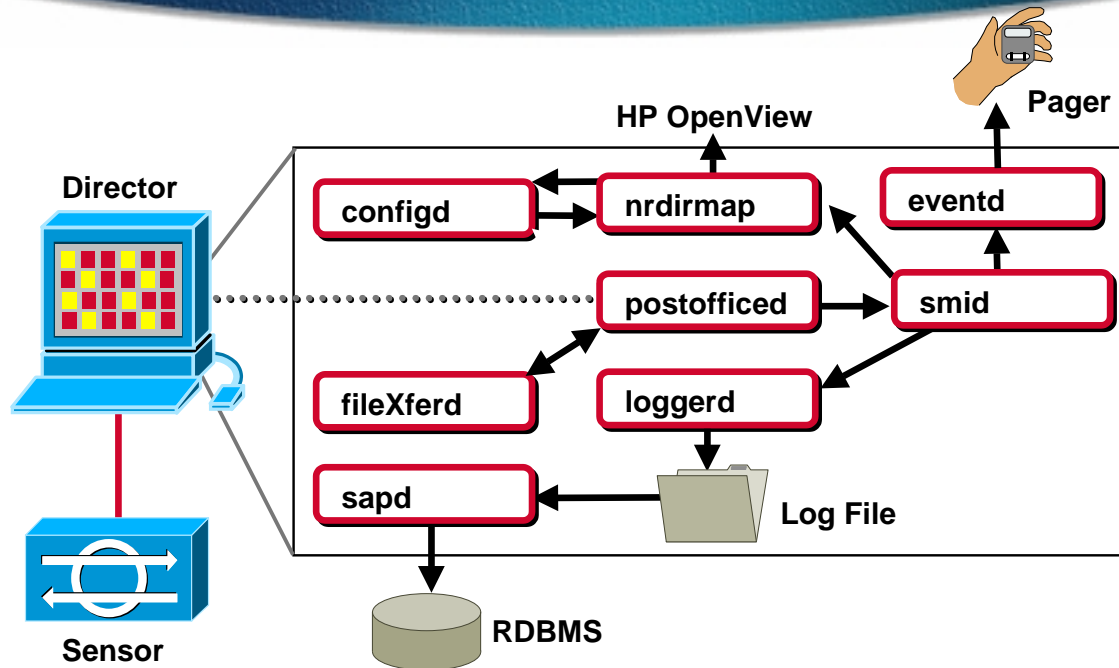
# Agenda

- Introduction and Overview of IDS
- **Director Issues**
- Troubleshooting the Sensor
- The Integrated Software Router
- And the Netsonar
- Case Study 1
- Case Study 2

# Common Director Problems

- SMID issues
- Alarming problems
- OVW issues

# Director Architecture



# Smid Associated Problems

- The **smid** daemon's primary function is to populate the alarm icons on the Director's HPOV maps
- It interacts with the **postofficed**, **eventd** and the **loggerd** daemons
- Most common problem is:  
    **“Cannot write message to Director”**

# Troubleshooting Smid Problems

- Make sure smid and all the daemons it interacts with are running (**nrstatus**)  
If not then do an **nrstart**
- Smid writes to a socket created in **/usr/nr/tmp**. Make sure that the socket is created as “**socket.dircomm=**”  
If not then **(stop and re) start Open View (ovw)**

# Troubleshooting Smid Problems (Cont.)

- The socket smid writes to, can overflow. This means that the messages are not getting removed fast enough to OV. Check to see if OV is running  
If not then start OV (**ovw**)
- Smid and nrdirmap need to have adequate permissions to communicate. Make sure that smid is owned by netranger and nrdirmap is SUID netranger  
If not, **logout and login back in as netranger and restart all processes**

# Alarms and Associated Problems

- Alarms are reported based on the severity level and destination
- Alarms are sent to the director through the postofficed, passed to the smid and then displayed by the nrdirmap utility graphically
- Most common problem, of course, is

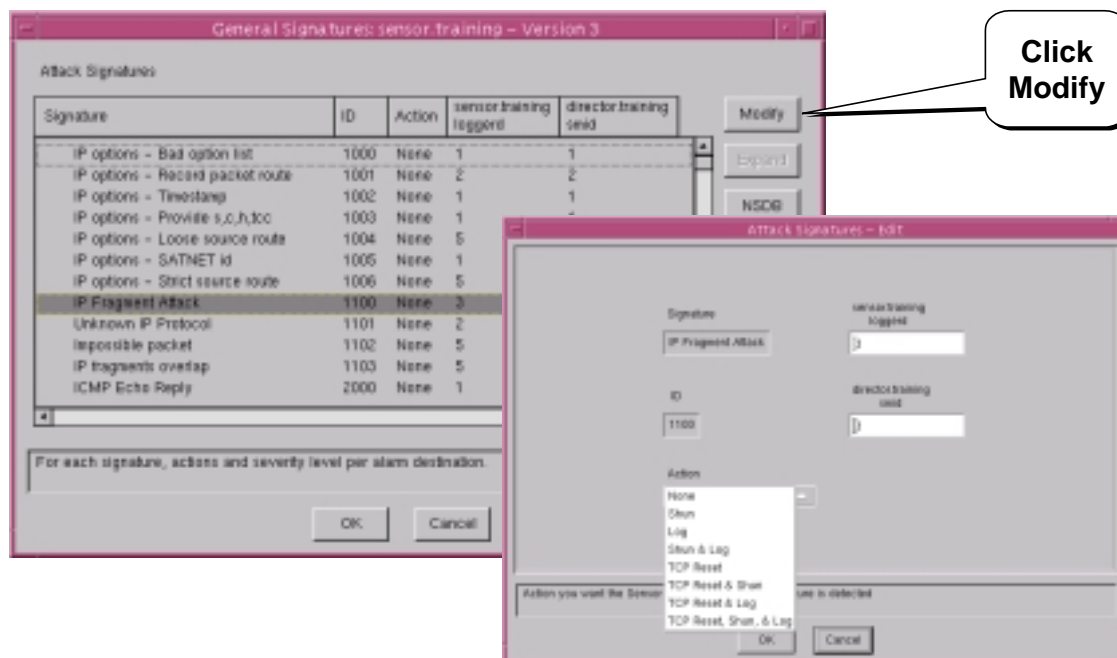
**no alarms reported**

# Troubleshooting Alarming Problems

- Alarms on the director are only reported if they are above the configured minimum limit. Confirm that the sensor is generating alarms higher than the lower limits

If not then **adjust the minimum critical and/or the minimum marginal level** on the director for the sensor in question

# Changing Signature Settings



2503  
1214\_05\_2000\_c1 © 2000, Cisco Systems, Inc.

cisco.com

19

# Troubleshooting Alarming Problems (Cont.)

- **Alarm data is thrown to the director log files by either the smid or the sensor itself. If there are no logs being created, make sure that an entry for the loggerd exists either in the sensor destinations file or a dupdestination entry exists in the [smid.conf](#) file**

**If not then make either of the two changes**

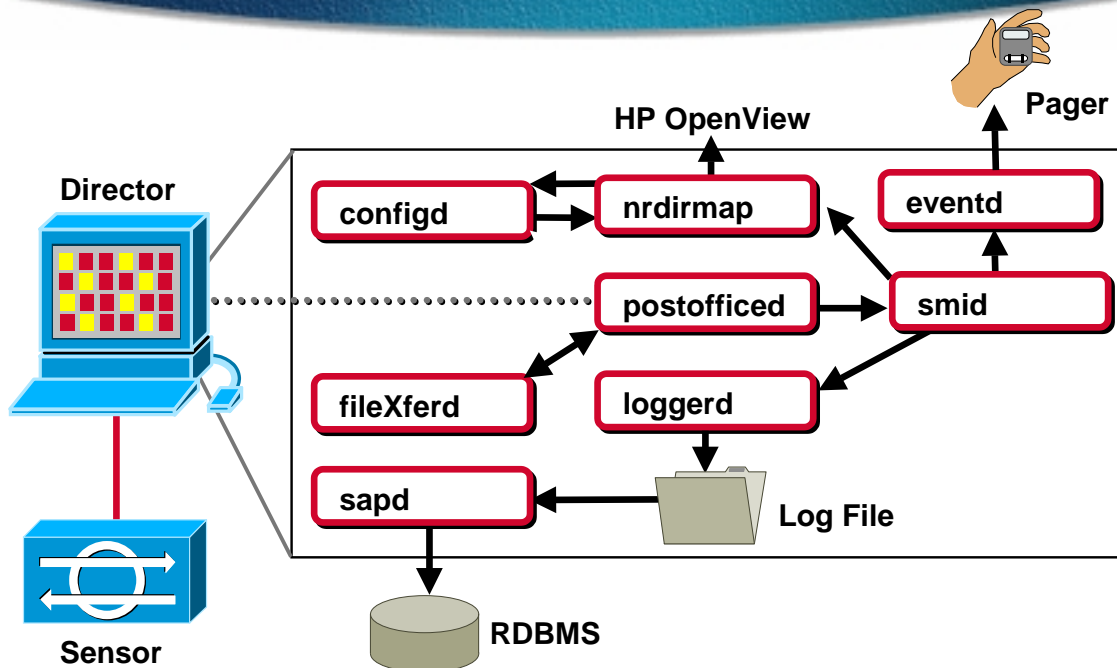
**DupDestination director.training loggerd 1  
EVENTS,ERRORS,COMMANDS**

2503  
1214\_05\_2000\_c1 © 2000, Cisco Systems, Inc.

cisco.com

20

# Director Architecture



## Troubleshooting Alarming Problems (Cont.)

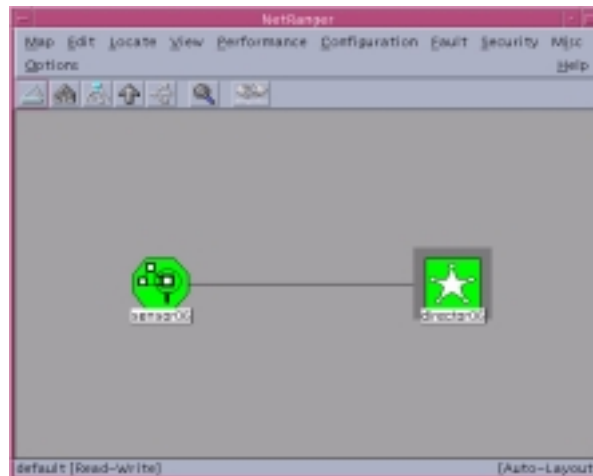
- The sensor postofficed only communicates the alarms to the director smid which are specified in the **destinations** file. Make sure that the destinations file contains the correct level of alarms

If not then adjust the destinations file entry, for example to propagate level 2 and above alarms to the director.training, use:

**1 director.training smid 2**  
**EVENTS,ERRORS,COMMANDS**

# OVW Problems

- **Open View is the medium used to display the NetRanger alarms and objects**



# Troubleshooting OVW Problems

- **Open View compatibility matrix:** It is important to know which versions of OVW will work with NetRanger and which won't

	<u>4.10</u>	<u>4.11</u>	<u>5.0.0</u>	<u>5.0.1</u>
• NetRanger 1.2.2	Patch	Y	N	N
• NetRanger 1.3.1	Patch	Y	N	N
• NetRanger 2.0.1	Patch	Y	N	N
• NetRanger 2.1.1	Patch	Y	N	Y

# Troubleshooting OVW Problems

- **Problems with nrdirmap core dumping when staring ovw. Confirm that the license file in `/usr/nr/etc` does not contain more than one entry for nrdirmap**

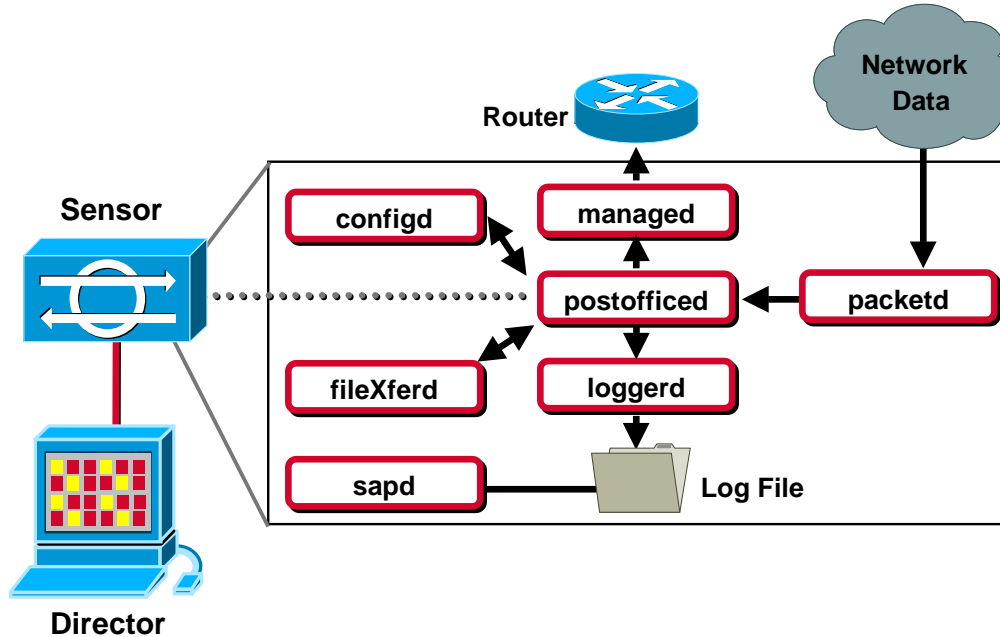
**If it does, then delete the extra entry**

**If there are more than one .lic files, keep only the one which is correct**

## Agenda

- **Introduction and Overview of IDS**
- **Director Issues**
- **Troubleshooting the Sensor**
- **The Integrated Software Router**
- **And the Netsonar**
- **Case Study 1**
- **Case Study 2**

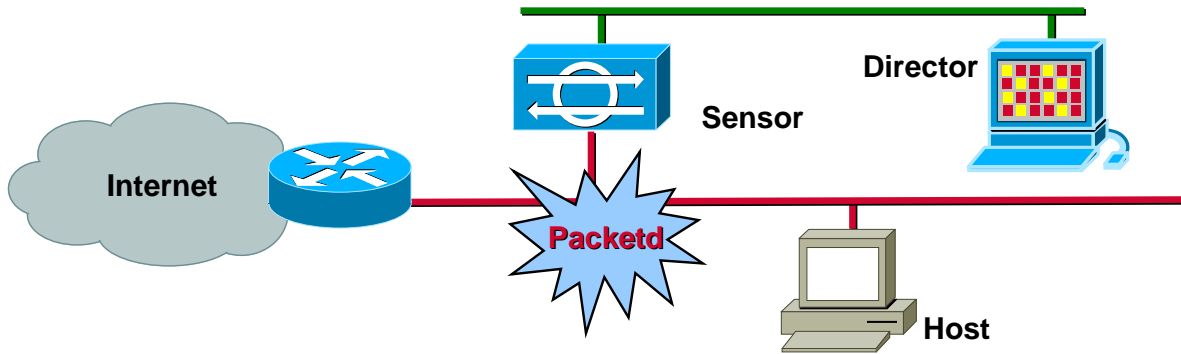
# Sensor Architecture



# Sniffing Issues

- The sensor sniffs the network on one of its interfaces, generally the **spwr0** interface
- The most common issue is that of the **sniffing not occurring**

# Packetd Sniffing Issues



# Troubleshooting Sniffing Issues

- The sensor sniffs the network only when its sniffing daemon, packetd is running. Make sure that the packetd is running (**nrstatus**)
  - If not then restart the daemon (**nrstart**)
  - If the daemon still does not come up, check the **daemons** file to make sure it is one of the listed daemons. If it is not, then **vi the daemons file** to include it

## Troubleshooting Sniffing Issues

- The sensor sniffs the network on the interface which is considered by the packetd to be interesting. Check the packetd.conf to see if the sniffing interface is indeed configured

(**grep nameOfPacketDevice /usr/nr/etc/packetd.conf**)

If not then on the director, **change the data sources tab in intrusion detection** and download the configurations to the sensor again

## Troubleshooting Sniffing Issues

- The sensor wraps the FDDI ring on which it is sniffing. The reason for this is that the sniffing interface on the sensor does not have an IP address by default

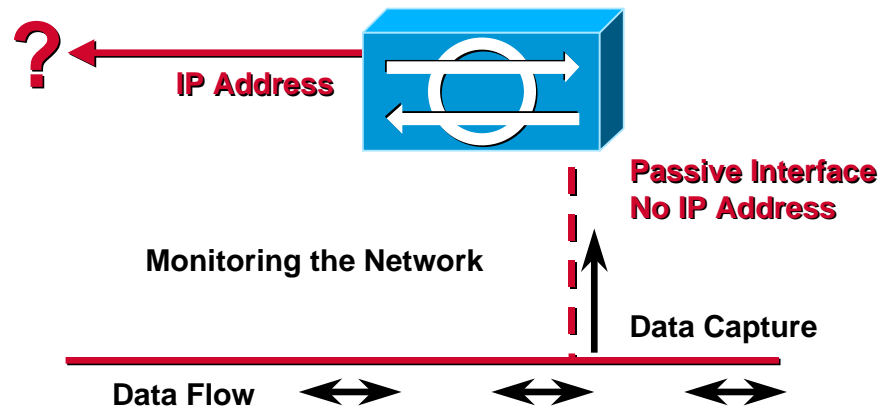
**vi the etc/hostname.ptpci0** file, and add a name, e.g. sensor-fddi. Then modify the /etc/hosts file, and add an entry for the IP address with a name 'sensor-fddi'.

# Communication Issues

- The sensor communicates with the director in order to feed it information for alarms. In addition it also needs to send resets to offensive devices
- The most prevalent issue is a break down of communications (**nrconns**)

# Routing Issues

Network Link to the Director



# Troubleshooting Communication Issues

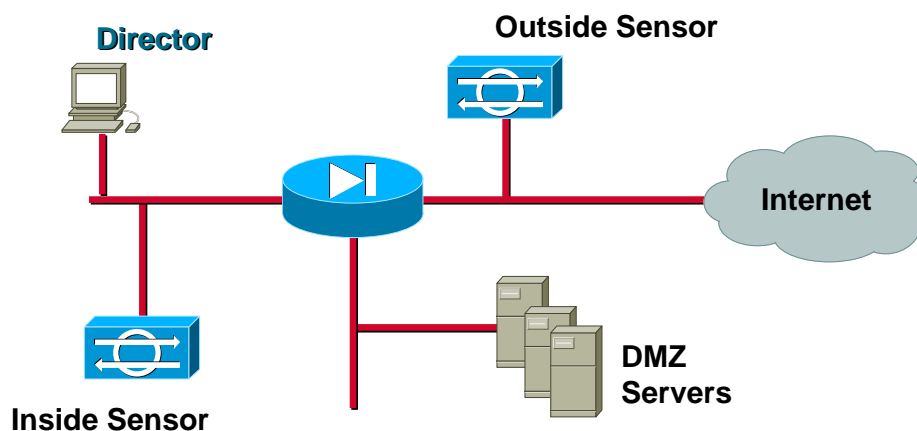
- The sensor uses the information in the routes file to reach the director. Confirm that the routes file has a correct entry for the director

```
sensor.cisco 1 10.1.9.201 45000 1
```

```
director.cisco 1 10.1.9.200 45000 1
```

If not then **modify the sensor configuration** on the director and download files to the sensor again

# Communication Through a Firewall



# Troubleshooting Communication Issues

- A firewall sitting between the sensor and the director can disrupt the communications between them. Make sure that the firewall allows the two to communicate

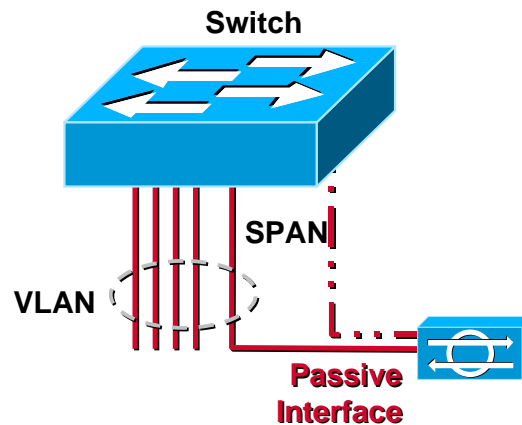
If not then

Open a hole for port 45000

Create necessary Network address translation e.g. on a PIX firewall,

```
static (inside,outside) 172.16.1.2 10.1.1.2 netmask 255.255.255.255  
conduit permit udp host 172.16.1.2 eq 45000 host 192.168.1.2
```

# Sensor Issues with a Switch



# Troubleshooting Communication Issues

- A sensor uses tcp resets to drop particularly offensive connections. If the sensor is hanging off a switch, the switch can stop these resets from going through. Make sure that the switch is configured to allow the resets through

If not then

Make sure that the switch can receive packets from the sensor (**inpmts on cat5k**)

The switch does not learn the mac address of the sensor and use it to discard spoofed mac addresses (**learning on cat5k**)

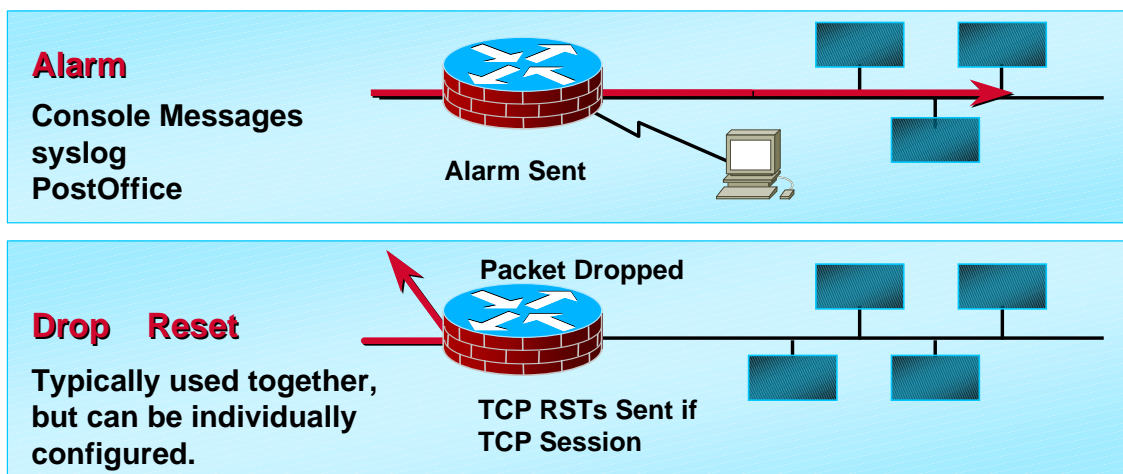
## Agenda

- Introduction and Overview of IDS
- Director Issues
- Troubleshooting the Sensor
- **The Integrated Software Router**
- And the Netsonar
- Case Study 1
- Case Study 2

# Cisco Secure Integrated Software

**Attack**

**Info**



## Determining Correct Router Behavior: The Show Commands

- The following show commands are available on the router for IDS:
- **sh ip audit ?**
  - all** IDS all available information
  - configuration** IDS configuration
  - interfaces** IDS interfaces
  - name** IDS name
  - sessions** IDS sessions
  - statistics** IDS statistics

# sh ip audit all

- A **good** 'sh ip audit all'

Event notification through syslog is enabled

Event notification through Net Director is enabled

Default action(s) for info signatures is alarm

Default action(s) for attack signatures is alarm

Default threshold of recipients for spam signature is 250

**PostOffice:HostID:10 OrgID:5500 Msg dropped:228**

**:Curr Event Buf Size:100 Configured:100**

**HID:1 OID:5500 S:15 A:4 H:603 HA:309 DA:0 R:98 Q:0**

**ID:1 Dest:172.16.171.18:45000 Loc:172.16.171.27:45000 T:5 S:ESTAB \***

# sh ip audit all

- A **bad** 'sh ip audit all'

Event notification through syslog is enabled

Event notification through Net Director is enabled

Default action(s) for info signatures is alarm

Default action(s) for attack signatures is alarm

Default threshold of recipients for spam signature is 250

**PostOffice:HostID:10 OrgID:5500 Msg dropped:328**

**:Curr Event Buf Size:100 Configured:100**

**HID:1 OID:5500 S:13296 A:5 H:1259 HA:650 DA:0 R:210 Q:16**

**ID:1 Dest:172.16.171.18:45000 Loc:172.16.171.27:45000 T:5 S:SYN  
SENT**

## sh ip audit all

- A **bad** 'sh ip audit all'

r7100#sh ip audit all

Event notification through syslog is enabled

Event notification through Net Director is disabled

Default action(s) for info signatures is alarm

Default action(s) for attack signatures is alarm

Default threshold of recipients for spam signature is 250

PostOffice:HostID:0 OrgID:0 Msg dropped:0

:Curr Event Buf Size:0 Configured:100

**Post Office is not enabled—No connections are active**

## sh ip audit interfaces

- A **good** 'sh ip audit interfaces'

Interface Configuratio

Interface FastEthernet0/

Inbound IDS audit rule is test

info actions alarm

attack actions alarm

Outgoing IDS audit rule is not set

# sh ip audit statistics

- A **good** 'sh ip audit statistics'

Signature audit statistics [process switch:fast switch]

Signature 2150 packets audited: [27741:28153]

Interfaces configured for audit 1

Session creations since subsystem startup or last reset 0

Current session counts (estab/half-open/terminating) [0:0:0]

Maxever session counts (estab/half-open/terminating) [0:0:0]

Last session created never

Last statistic reset never

HID:1 OID:5500 S:15 A:4 H:712 HA:368 DA:0 R:123 Q:0

# Debug Commands

- **Debug ip audit ?**

detailed	Audit Detailed debug records
ftp-cmd	Audit FTP commands and responses
ftp-token	Audit FTP tokens
function-trace	Audit function trace
icmp	Audit ICMP packets
ip	Audit IP packets
object-creation	Audit Object Creations
object-deletion	Audit Object Deletions
rpc	Audit RPC
smtp	Audit SMTP
tcp	Audit TCP
tftp	Audit TFTP
timers	Audit Timer related events
udp	Audit UDP

# Error Messages

**"Connection to HostID:%u OrgID:%u"**

- **Check connectivity between the director and the router**
- **Check PO configuration on both the director and the router**
- **If you have just changed the org or host id on either systems, you need to reboot the router**

# Common Problems

- **Unable to 'add host'**
- **No alarms being reported to the director**
- **Memory impact too high, performance tuning**

## Unable to 'Add Host'

- Remember you **cannot use the 'add host' wizard to add the IOS sensor**
- **Must add it to the director properties in the 'hosts' section**
- **Also need to add an entry to the routes entry for the router**

## No Alarms Being Reported

- **Mis configured PO** on router or director
- **No route** for router on director
- **Firewall** blocking communication between router and director
- **Router not configured to report to the director**

## No Alarms Being Reported

- Correct **audit rule not applied** to the correct interface
- Audit rule **applied in the wrong direction**
- **Router not rebooted** after change to PO configuration

## Performance Tuning

- It is recommended not to change the **max-queue size** from 100. A higher queue size can impact performance. (Each event in the queue requires 32 KB of memory)
- Consider **removing some of the IP addresses from generating alarms or disabling a signature altogether**

# Limiting Audit Activity

```
ip audit name AUDIT.1 info list 90 action alarm
ip audit name AUDIT.1 attack list 90 action alarm drop
reset

interface e0

    ip address 10.1.1.1 255.0.0.0
    ip audit AUDIT.1 in

interface e1

    ip address 172.16.57.1 255.255.255.0
    ip audit AUDIT.1 in

access-list 90 deny 172.16.59.16
access-list 90 permit any
```

# Limiting Signature Activity

```
ip audit signature 1234 disable
ip audit signature 2345 list 91
ip audit signature 3456 list 91

ip audit name AUDIT.1 info action alarm
ip audit name AUDIT.1 attack action alarm drop reset

interface e1

    ip address 172.16.57.1 255.255.255.0
    ip audit AUDIT.1 in

access-list 91 deny host 10.4.1.1
access-list 91 deny host 10.4.1.2
access-list 91 deny 172.16.58.0 0.0.0.255
access-list 91 permit any
```

# Agenda

- Introduction and Overview of IDS
- Director Issues
- Troubleshooting the Sensor
- The Integrated Software Router
- **And the Netsonar**
- Case Study 1
- Case Study 2

# Common Problems

- Licensing issues
- Scan too slow
- Graphing problems

# Licensing Issues

- The demo license is for only a single host scan. Make sure you have a **valid license**. A demo license has an expiry date in it
- Make sure that the **host name specified in the .lic file** is correct, otherwise the license will not be used

# Slow Scan

- If machines on the network do not reply to Netsonar pings, it takes Netsonar 50 seconds by default to declare a machine dead. Either **exclude the dead addresses or reduce the time out and retry count**
- **Do not force scan** if there are dead addresses in the network

## Slow Scan (Cont.)

- Consider **not scanning for password vulnerabilities**, they tend to take the longest
- Make sure that all **machines send resets** and don't silently discard Netsonar packets
- Finally make sure **all system requirements are met**, especially paging space

## GUI Problems

- Most common GUI problems are due to running an older version of the Java environment
- Open a DOS window, type **jview**. What is the version? **5.00.3167 or greater?**

# Agenda

- Introduction and Overview of IDS
- Director Issues
- Troubleshooting the Sensor
- The Integrated Software Router
- And the Netsonar
- **Case Study 1**
- **Case Study 2**

## The Case of a Netranger Which Would Not Alarm!

- **Original issue:** The NetRanger was not alarming
- **Initial Diagnosis:** All the software seemed to be installed correctly. All devices were up and running

## A Troubleshooting Guide

- **Rule # 1:** Don't troubleshoot a problem which does not exist!
- **Rule # 2:** It won't alarm unless it sees something
- **Rule # 3:** The sniffer is what it is because of packetd
- **Rule # 4:** The packetd will only sniff on what it is told to sniff on

## A Troubleshooting Guide

- **Rule # 5:** It won't do for the director what it can't do for itself
- **Rule # 7:** The sensor may be talking to the director but who on the director is it chatting with?
- **Rule # 8:** The sensor can do everything right but the smid has to talk to nrdirmap!

## Generate Some Alarms!

- **Rule # 1: Don't troubleshoot a problem which does not exist!**
- The first thing that should be done under such cases is to generate some high severity alarms on the sniffed network
- Use **'ping -l 20000 dest\_host\_IP'** from a windows machine to generate frag. Icmp alarm
- Check to see if the director ovw is reporting alarms

**Result: No alarms were seen**

## Is the Sniffing Interface Getting Any Traffic?

- **Rule # 2: It won't alarm unless it sees something**
- Su to root and run the snoop command
- **snoop -d spwr0**
- If there were no traffic, we would have tried to troubleshoot hardware issues but,

**Result: Traffic was seen on the interface**

## Is the Packetd Running?

- **Rule # 3: The sniffer is what it is because of packetd**
- **Nrstatus** showed that packetd was indeed running
- If it were not running, we would have restarted it after checking the daemons file but,

**Result: packetd was up and running**

## Is the Packetd Correctly Configured?

- **Rule # 4: The packetd will only sniff on what it is told to sniff on**
- A **grep for spwr0 in packetd.conf** to see if the correct sniffing interface was configured
- If it were not then, we would have reconfigured the director but,

**Result: packetd was correctly configured**

**The Plot Thickens...**

## Is the Sensor Generating Alarms for Itself?

- **Rule # 5: It won't do for the director what it can't do for itself**
- **A tail -f log\*** on the log files in the **/usr/nr/var** directory while we generated alarming attacks
- **If the file were not increasing in size, we would have checked the alarms severity levels, however the**

**Result: The log file was increasing in size**

## Is the Sensor Talking to the Director?

- **Rule # 6: The director will display only what it receives**
- **Nrconns** to see if the connection between the director and sensor was working
- **Had it not been working we would have looked at connectivity issues, but the**

**Result: The director and sensor were communicating**

## Is the Sensor Talking to the Director Smid?

- **Rule # 7: The sensor may be talking to the director but who on the director is it chatting with?**
- A look at the **destinations** file showed that the director smid was one of the destinations with an appropriate level
  - 2 **director.cisco smid 2 EVENTS,ERRORS,COMMANDS**
- Had it not been we would have changed the config on the director and downloaded to the sensor again, but the

**Result: The sensor was talking to the correct process on the director**

## What Is the Smid Doing About It?

- **Rule # 8: The sensor can do everything right but the smid has to talk to nrdirmap!**
- **Nrstatus** showed that the smid was up but not owned by netranger!
- **Stopped the daemons, logged in as netranger, started the services again.**

**Result: Alarms of all colors in the OV map!**

# Agenda

- Introduction and Overview of IDS
- Director Issues
- Troubleshooting the Sensor
- The Integrated Software Router
- And the Netsonar
- Case Study 1
- **Case Study 2**

## The Case of a Cisco IOS IDS Router Not Generating Alarms!

- **Original issue:** The Cisco IOS not reporting alarms to the director
- **Initial diagnosis:** All the software seemed to be installed correctly. All devices were up and running

# Generate Some Alarms!

- **Rule # 1: Don't troubleshoot a problem which does not exist!**

**Generated large packet pings**

# Are Alarms Being Generated and Reported?

- **Rule # 2: It won't alarm unless it see something**

**r7100#sh log**

2d19h: %IDS-4-ICMP\_FRAGMENT\_SIG: Sig:2150:Fragmented ICMP Traffic—from 172.16.171.5 to 172.16.171.27

2d19h: %IDS-4-ICMP\_FRAGMENT\_SIG: Sig:2150:Fragmented ICMP Traffic—from 172.16.171.5 to 172.16.171.27

2d19h: %IDS-4-ICMP\_FRAGMENT\_SIG: Sig:2150:Fragmented ICMP Traffic—from 172.16.171.5 to 172.16.171.27

2d19h: %IDS-4-ICMP\_FRAGMENT\_SIG: Sig:2150:Fragmented ICMP Traffic—from 172.16.171.5 to 172.16.171.27

2d19h: %IDS-4-ICMP\_FRAGMENT\_SIG: Sig:2150:Fragmented ICMP Traffic—from 172.16.171.5 to 172.16.171.27

# Is the Router PO Configured Correctly?

- **Rule # 6:** The director will display only what it receives

```
ip audit notify nr-director
```

```
ip audit notify log
```

```
ip audit po max-events 100
```

```
ip audit po protected 172.16.171.1 to 172.16.171.254
```

```
ip audit po remote hostid 1 orgid 5500 rmtaddress 172.16.171.18 localaddress  
172
```

```
.16.171.27 port 45000 preference 1 timeout 5 application director
```

```
ip audit po local hostid 10 orgid 5500
```

```
ip audit name test info action alarm
```

```
ip audit name test attack action alarm
```

# What Is Being Sent to the Director?

```
r7100#sh ip audit sta
```

```
Signature audit statistics [process switch:fast switch]
```

```
signature 2005 packets audited: [3:10]
```

```
signature 2150 packets audited: [2471:3057]
```

```
Interfaces configured for audit 0
```

```
Session creations since subsystem startup or last reset 0
```

```
Current session counts (estab/half-open/terminating) [0:0:0]
```

```
Maxever session counts (estab/half-open/terminating) [0:0:0]
```

```
Last session created never
```

```
Last statistic reset never
```

```
HID:1 OID:5500 S:89 A:7 H:48597 HA:24942 DA:0 R:2 Q:100
```

## Are the Director and the Router Communicating?

**r7100#sh ip audit all**

Event notification through syslog is enabled

Event notification through Net Director is enabled

Default action(s) for info signatures is alarm

Default action(s) for attack signatures is alarm

Default threshold of recipients for spam signature is 250

PostOffice:HostID:10 OrgID:5500 Msg dropped:101

:Curr Event Buf Size:100 Configured:100

HID:1 OID:5500 S:89 A:7 H:48597 HA:24942 DA:0 R:2 Q:100

ID:1 Dest:172.16.171.18:45000 Loc:172.16.171.27:45000 T:5 S:**SYN SENT**

## Are the Director and the Router Communicating?

- **If org id or other similar configs are changed the box needs to be rebooted**
- **Rebooted the box, but PO still did not go to established**

## Are the Director and the Router Communicating?

```
interface FastEthernet0/0
ip address 172.16.171.27 255.255.255.240
ip access-group 101 in
ip audit test in
duplex auto
speed auto
```

## Are the Director and the Router Communicating?

```
access-list 101 permit tcp any host 172.16.171.27 eq telnet
access-list 101 permit tcp any host 172.16.171.30 eq www
```

**Added:**

```
access-list 101 permit udp host 172.16.171.18 eq 45000 host
172.16.171.27 eq 45000
```

# Are the Director and the Router Communicating?

```
r7100#sh ip audit all
```

```
Event notification through syslog is enabled
```

```
Event notification through Net Director is enabled
```

```
Default action(s) for info signatures is alarm
```

```
Default action(s) for attack signatures is alarm
```


```
Default threshold of recipients for spam signature is 250
```

```
PostOffice:HostID:10 OrgID:5500 Msg dropped:1899
```

```
  :Curr Event Buf Size:100 Configured:100
```

```
HID:1 OID:5500 S:93 A:9 H:48603 HA:24942 DA:0 R:7 Q:0
```

```
ID:1 Dest:172.16.171.18:45000 Loc:172.16.171.27:45000 T:5 S:ESTAB *
```



## Troubleshooting Cisco Secure Intrusion Detection Systems

### Session 2503



# Please Complete Your Evaluation Form

## Session 2503

2503  
1214\_05\_2000\_c1 © 2000, Cisco Systems, Inc.

[cisco.com](http://cisco.com)

87

# CISCO SYSTEMS



## EMPOWERING THE INTERNET GENERATION<sup>SM</sup>

2503  
1214\_05\_2000\_c1 © 2000, Cisco Systems, Inc.

[cisco.com](http://cisco.com)

88