Catalyst 6500
IDSM-2 module

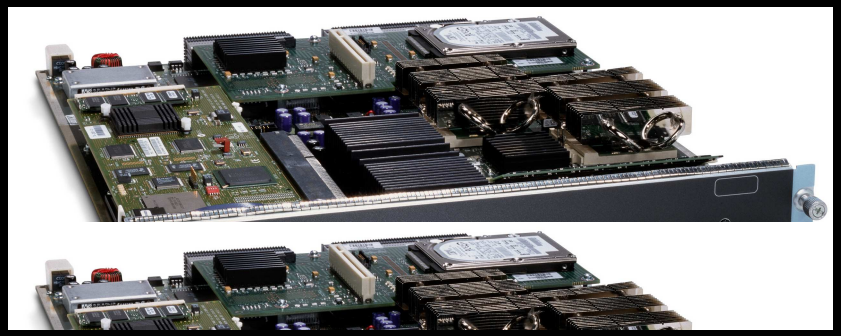
ÁCS GYÖRGY
GACS@CISCO.COM

TARTALOM

- IDSM-2 technikai leírás
- IDSM-2 alapkonfiguráció
- Capturing
- In-line
- IPS konfiguráció
- HA
- Összefoglalás

IDSM-2 TECHNIKAI LEÍRÁS

Intrusion Detection Module 2



•CLI, telnet, SSHv3, SSL (IDM),
•VMS 2.3, MARS, CTR, SNMP

• Catalyst performance not affected by additional VLANs or devices in the Cisco Catalyst chassis (IDS)
• Fabric Enabled, CEF256, 2.5A@42V
• Over-sampling alert generates "993 Bandwidth Exceeded" alert
• Unlimited VLAN support (IDS)
• Trend Micro collaboration: network based AV

THE WS-SVC-IDSM2 SUPPORTS THE FOLLOWING…

- Supports connection to 32-Gbps shared bus
- Supports single 8-Gbps fabric connection

- Comprehensive attack recognition
- Same code base as Cisco IDS/IPS appliances
- Monitors up to 600Mbps of traffic (IPS: 500Mbps)
- Supports up to 500,000 concurrent connections
- Passive monitoring + IPS (5.0) – 1 VLAN pair now- software failure bypass
- Extensive signature database
- Built in web-based management (IDM)
- Supports alarms, shunning and TCPresets, drop, …
- …

IDSM-2

Maximum Number of Modules per Chassis

- Eight per chassis
- No Slot Restriction

Traffic Capture Methods (Passive Mode)

- VACL capture
- SPAN
- RSPAN (2)
- ERSPAN (4) (Sup 720 Only)

Minimum Code Revision

- Release 4.x, S47
- Current release: 5.x Sxxx

Hot-Swap Requirements

- Module shutdown required before removal.
- Module insertion/removal never affects the Cisco Catalyst switch.

Processor

Dual Pentium P3 1.13 GHz on main board with 232 MHz IXP 32 bit StrongARM policy processor on the accelerator

Memory and Hard Drive

- 20 Gigabytes (not all used)
- 2 Gigabytes RAM
- 32 Megabytes Event Storage with IDSv5.0
- 64 MB Flash

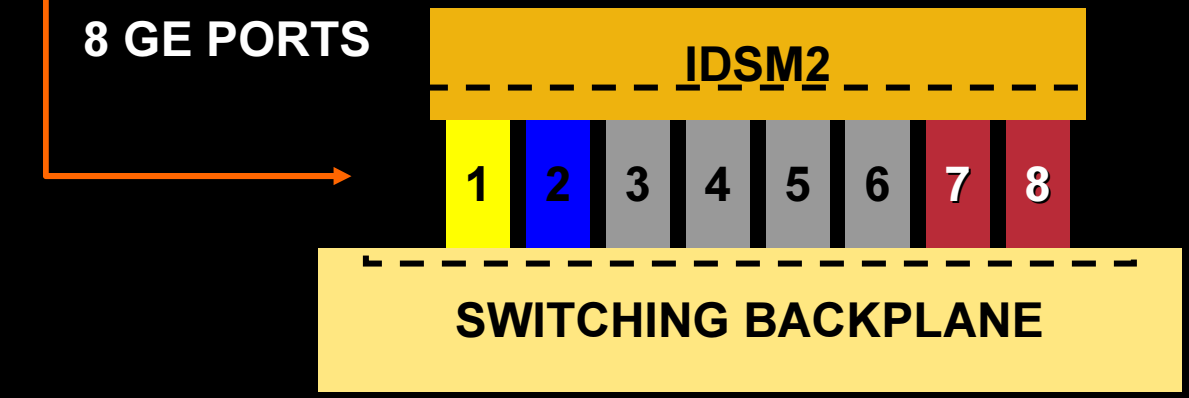
Operating System

GNU Linux kernel version 2.4.26

Intrusion Detection Module 2 Architecture…

```
C6509#show module
Mod Ports Card Type                                  Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  5     2  Supervisor Engine 720 (Active)         WS-SUP720-BASE     SAD07260096
  8     8  Intrusion Detection System             WS-SVC-IDSM-2      SAD072001DF
```

SIGNIFIES
8 GE PORTS



Port Role

1. Reset
2. Command and Control
3–6. IGNORE
7, 8. Sniffing – IPS pair

Only TWO PORTS in This Group Can Be Set up to Monitor Traffic via SPAN or VACL Capture THESE PORTS ARE PHYSICAL PORTS 7/8

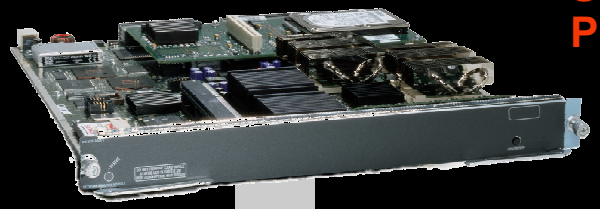
This Port Is Set up as a Trunk Port by Default and Should Be Used Whenever You Set up SPAN or VACL CAPTURE

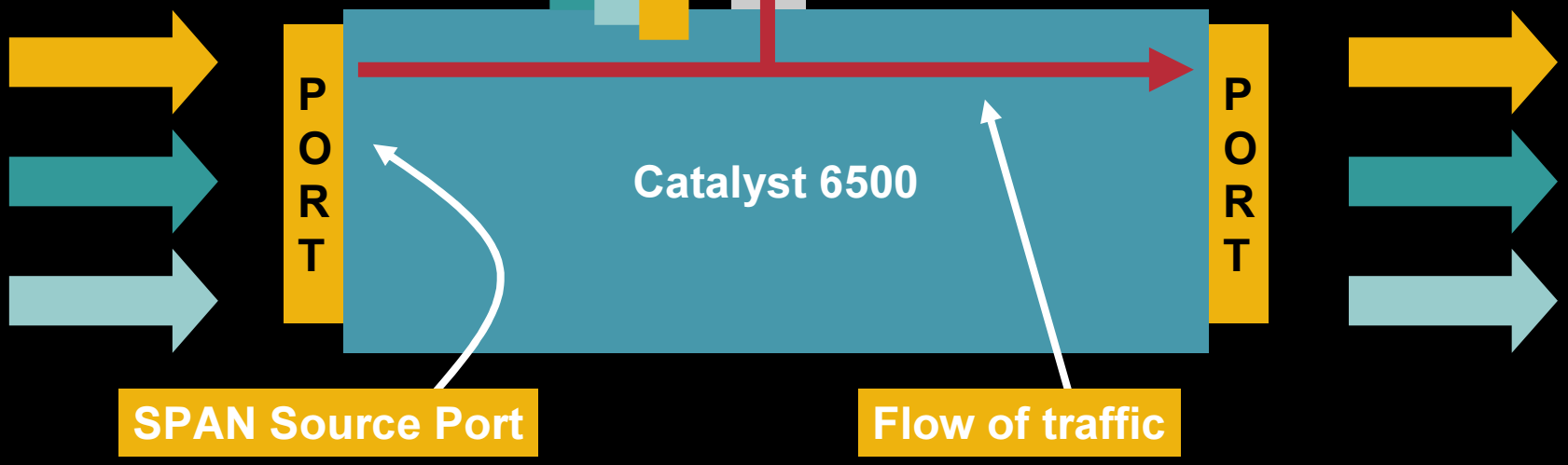
Intrusion Detection Module 2 Packet Flow

The Administrator Sets up a SPAN Source Port/VLAN and a SPAN Destination Port

SPAN Sends a Copy of Traffic to the SPAN Destination Port Which Is the IDSM in Our Case…

NOTE: ALL TRAFFIC from the SPAN Source Port/VLAN Is Sent to the SPAN Destination Port

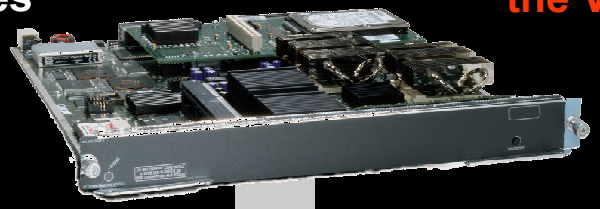


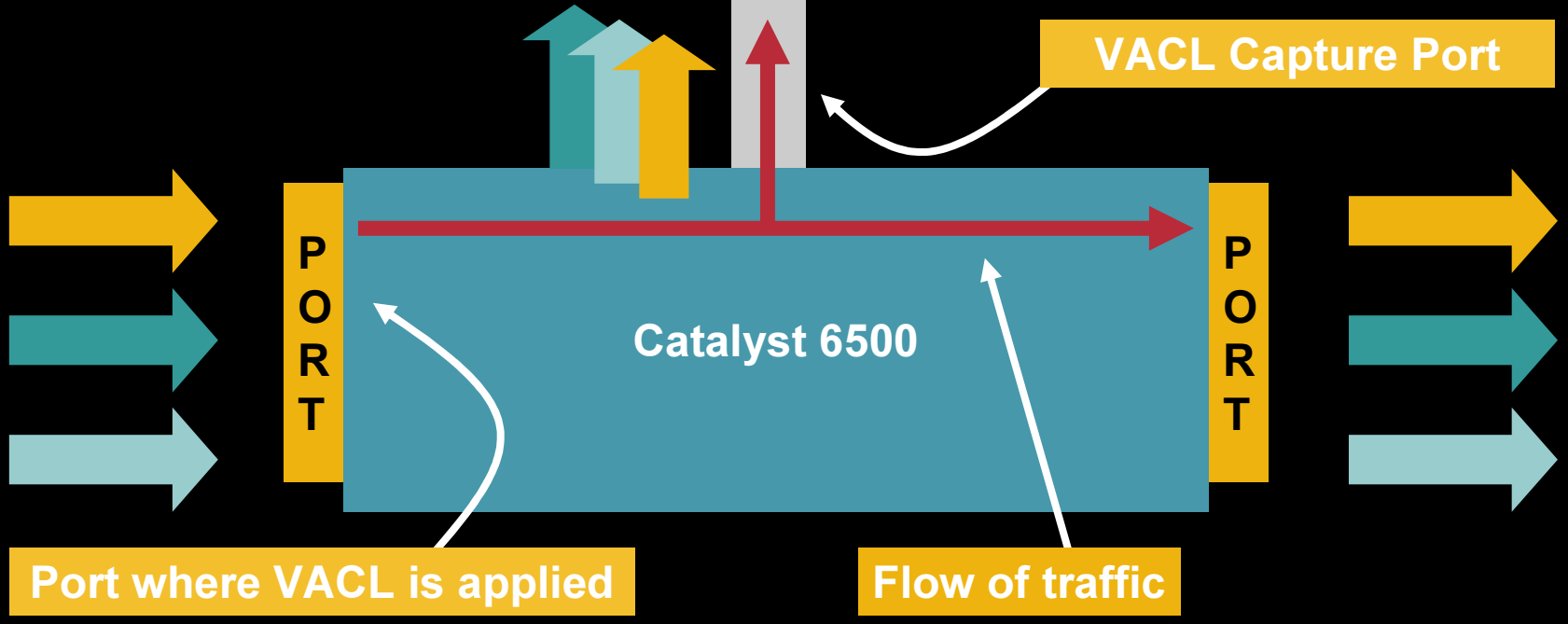


Intrusion Detection Module 2 Packet Flow

The Administrator Sets up a VACL Capture Filter and Applies It to the Source Port, then Defines IDSM Monitor Port as the VACL Capture Port

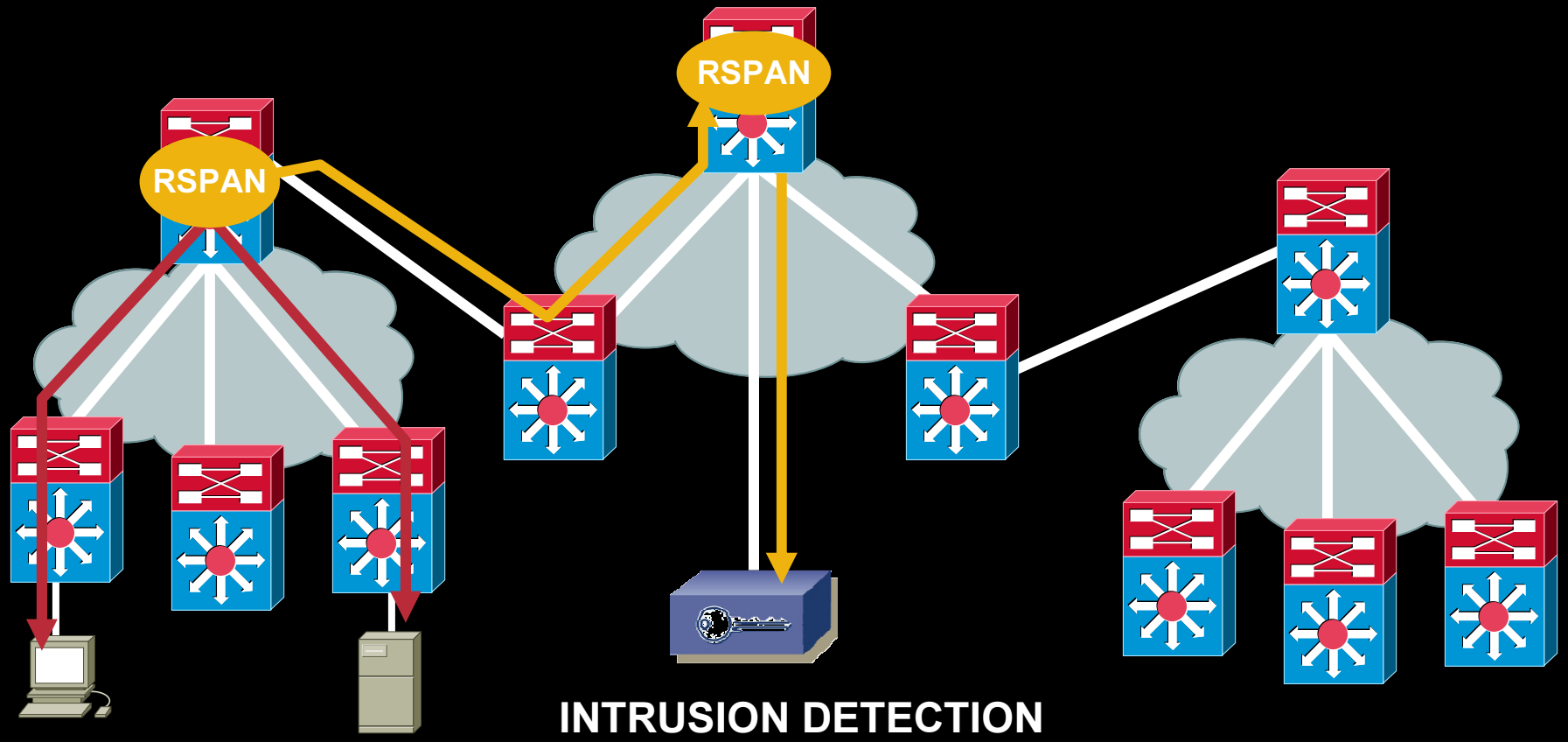
NOTE: Only TRAFFIC Matching the VACL Is Sent to the VACL Capture Port





Intrusion Detection Module 2 Design Consideration

The IDSM2 as a Promiscuous Device (<5.0) and with the Use of RSPAN Can Be Positioned Anywhere in the Network, as Long as There Is a Valid Contiguous RSPAN VLAN to Carry the Traffic from Source to Destination…



Cat OS – IOS support

Module	Supervisor 1A	Supervisor 2	Supervisor 32	Supervisor 720
IDSM2 - CatOS	7.6.1	7.6.1		8.2.1
IDSM2 - native IOS	No Support	12.2(17d)SXB	12.2(18)SXF	12.2(14)SX1

Module	Min. SupEngine	Recommended SupEngine
IDSM2 - CatOS	7.5.1	7.6.9

In-line support

Latency : ~1 µs/packet

Supervisor	Native IOS Branch with Inline Operation	Catalyst OS Branch with Inline Operation
Sup 720 (all versions)	12.2(18)SXE	8.4.1
Sup 1a (no PFC, with PFC and with MSFC2)	TBD	8.4.1
Sup 2 (no PFC, with PFC and with MSFC2)	TBD	8.4.1

Cisco IOS software 12.2(18)SXE with Supervisor Engine 720 supports only one IDSM-2 inline between two VLANs.

IDSM-2 – with IPS 5.0

Module	Interfaces Supporting Inline	Possible Port Combinations	Interfaces Not Supporting Inline
IDSM-2	port 7 and 8 GigabitEthernet0/7 GigabitEthernet0/8	0/7<->0/8	GigabitEthernet0/2

IDSM-2 ALAPKONFIGURÁCIÓ

0. Show Module

```
cat6k> (enable) show module
```

```
router# show module
```

```
Mod Ports Card Type                                   Model              Serial No.
--- ----- ------------------------------------------- ------------------ -----------
  1   16  16 mb RJ-45 ethernet                        WS-X6248-RJ-45     SAD0401012S
  3   48  48 mb RJ45                                  WS-X6348-RJ-45     SAL04483QBL
  4   48  48 port 10/100/1000mb RJ45                  WS-X6548-GE-TX     SAD073906GH
  6   16  SFM-capable 16 port 1000mb GBIC             WS-X6516A-GBIC     SAL0740MMYJ
  7    2  Supervisor Engine 720 (Active)              WS-SUP720-3BXL     SAD08320L2T
  9    1  1 port 10-Gigabit Ethernet Module           WS-X6502-10GE      SAD071903BT
 10    3  Anomaly Detector Module                     WS-SVC-ADM-1-K9    SAD084104JR
 11    8  Intrusion Detection System                  WS-SVC-IDSM2       SAD05380608
 13    8  Intrusion Detection System                  WS-SVC-IDSM-2      SAD072405D8

Mod MAC addresses                       Hw     Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  1  00d0.d328.e2ac to 00d0.d328.e2db   1.1    4.2(0.24)VAI 8.5(0.46)ROC Ok
  2  0003.6c14.e1d0 to 0003.6c14.e1ff   1.4    5.4(2)       8.5(0.46)ROC Ok
  3  000d.29f6.7a80 to 000d.29f6.7aaf   5.0    7.2(1)       8.5(0.46)ROC Ok
  6  000d.ed23.1658 to 000d.ed23.1667   1.0    7.2(1)       8.5(0.46)ROC Ok
  7  0011.21a1.1398 to 0011.21a1.139b   4.0    8.1(3)       12.2(PIKESPE Ok
  9  000d.29c1.41bc to 000d.29c1.41bc   1.3    Unknown      Unknown      PwrDown
 10  000b.fcf8.2ca8 to 000b.fcf8.2caf   0.101  7.2(1)       4.0(0.25)    Ok
 11  00e0.b0ff.3340 to 00e0.b0ff.3347   0.102  7.2(0.67)    5.0(1)       Ok
 13  0003.feab.c850 to 0003.feab.c857   4.0    7.2(1)       5.0(1)       Ok

Mod Sub-Module                  Model              Serial       Hw     Status
--- --------------------------- ------------------ ------------ ------- -------
  7 Policy Feature Card 3       WS-F6K-PFC3BXL     SAD083305A1  1.3    Ok
  7 MSFC3 Daughterboard         WS-SUP720          SAD083206JX  2.1    Ok
 11 IDS 2 accelerator board     WS-SVC-IDSUPG      .            2.0    Ok
 13 IDS 2 accelerator board     WS-SVC-IDSUPG      0347331976   2.0    Ok

Mod Online Diag Status
--- -------------------
  1 Pass
  2 Pass
  3 Pass
  6 Pass
  7 Pass
  9 Unknown
 10 Not Applicable
 11 Pass
 13 Pass
```

1. Command & Control i/f config + gw check

```
cat6k> enable

cat6k> (enable) set vlan c&c_vlan_number
idsm2_slot_number/c&c_port_number
cat6k> (enable) set vlan 10 6/2
cat6k> (enable) session slot_number
cat6k> (enable) session 6
…
idsm-2# ping 10.1.1.1
```

```
router# configure terminal

router (config)# intrusion-detection module module_number management-
port access-vlan vlan_number
router (config)# intrusion-detection module 6 management-port access-
vlan 10
router# session slot module_number processor 1
router# session slot 6 processor 1
…
idsm-2# ping 10.89.149.254
```

Service Module Reference Designs
IDSM2 Configuration

On setting up the IDSM2
Start with running the "setup" command to initialize the IDSM2

```
sensor(config)# setup
<snip>
Continue with configuration dialog?[yes]: yes
Enter host name[sensor]: IDSM2
Enter IP address[10.1.1.150]: 192.168.102.150
Enter netmask[255.255.255.0]: 255.255.255.0
Enter default gateway[10.1.1.1]: 192.168.102.1
Enter telnet-server status[enabled]: enabled
Enter web-server port[443]: 443

Use this configuration? [yes]: yes
Configuration Saved.
Warning: The node must be rebooted for the changes to go into effect.
```

IDSM2

```
IDSM2(config)# username idm-admin password idmadmin privilege administrator
Enter Login Password: *****
Re-enter Login Password: *****
```

Create the userid to be used when accessing IDSM2 IDM Web interface

CAPTURING

First Step:
Getting Traffic to Your Network IDS

- Traffic must be mirrored (replicated) to sensors in IDS mode
- Choices:

  Switch-based traffic mirroring (SPAN) directly or from aggregation switch

  Selective mirroring (traffic capture—VACLs)

Switch-Based Traffic Capture

- **Port mirroring: SPAN functionality and command syntax varies between product lines and switch vendors**
  - **Some limit the number of SPAN ports**
  - **Some allow you to monitor multi-VLAN traffic**
    - **Note that not all sensor vendors can handle multi-VLAN traffic**
  - **www.cisco.com/warp/public/473/41.html**
  - **www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/hwguide/hwclipr.htm#wp89697**
- **Rule-Based capture: VLAN ACL capture/MLS IP IDS**
  - **Policy Feature Card (PFC) required on Catalyst® 6500**
  - **Allows you to monitor multi-VLAN traffic**
  - **Use "mls ip ids" when using "router" interfaces or when interface is configured for Cisco IOS® FW**
  - **www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/hwguide/hwclipr.htm#wp89697**

Promiscous mode

If you configure both ports (7/8) as monitoring ports, make sure that they are configured to monitor different traffic.

You should not configure an IDSM-2 data port as both a SPAN destination port and a VACL capture port, because IDSM-2 will not receive traffic. This dual configuration (SPAN and VACL) causes problems on the switch and traffic is not sent properly.

Using the TCP Reset Interface
The IDSM-2 has a TCP reset interface—port 1. The IDSM-2 has a specific TCP reset interface because it cannot send TCP resets on its sensing ports.
If you have reset problems with the IDSM-2, try the following:

- If the sensing ports are access ports (a single VLAN), you need to configure the reset port to be in the same VLAN.
- If the sensing ports are dot1q trunk ports (multi-VLAN), the sensing ports and reset port all must have the same native VLAN, and the reset port must trunk all the VLANs being trunked by both the sensing ports.

Promiscous mode SPAN

filter keyword to monitor traffic on specific VLANs on source trunk ports.

```
cat6k> (enable) set span 3/3 13/7
Destination      : Port 13/7
Admin Source     : Port 3/3
Oper Source      : Port 3/3
Direction        : transmit/receive
Incoming Packets: disabled
Learning         : enabled
Multicast        : enabled
Filter           : -

Session Number   : 1
```

```
router (config)# monitor session (session_number) source interface
interface/port_number [, | - | rx | tx | both]
router (config)# monitor session 1 source interface
GigabitEthernet2/23 both
router (config)# monitor session (session_number) destination
intrusion-detection-module module_number data-port data_port_number
router (config)# monitor session 1 destination intrusion-detection-
module 6 data-port 1
router (config)# monitor session (session_number) {filter vlan
{vlan_ID} [, | - ]}
router (config)# monitor session 1 filter vlan 146
```

SPAN Parameters

disable—Disables port monitoring.

- *module/port*—Source module and port numbers.
- *vlan*—Source VLAN numbers.
- *module/port*—Destination module and port numbers.
- **both—Both receiving and transmitting traffic.**
- **filter—Applies filter to VLAN.**
- **inpkts—Enables/disables destination port incoming packets.**
- **learning—Enables/disables MAC address learning.**
- **multicast—Enables/disables multicast traffic.**
- **rx—Receiving traffic.**
- **session— Session number for SPAN session.**
- **tx —Transmitting traffic.**

interface—SPAN source interface

- **remote—SPAN source Remote**
- **vlan— SPAN source VLAN**
- **GigabitEthernet— GigabitEthernet IEEE 802.3z**
- **Port-channel— Ethernet Channel of interfaces**
- **,— Specify another range of interfaces**
- **-— Specify a range of interfaces**
- **both— Monitor received and transmitted traffic**
- **rx— Monitor received traffic only**
- **tx— Monitor transmitted traffic only**
- **intrusion-detection-module— SPAN destination intrusion detection module**
- **destination— SPAN destination interface or VLAN**
- **filter— SPAN filter VLAN**
- **source— SPAN source interface, VLAN**
- **type— Type of monitor session**

VACL

Permit = capture

```
cat6k> (enable) set security acl ip acl_name permit ip [permit (...) |
deny (...)] capture
console> (enable) set security acl ip CAPTUREALL permit ip any any
capture

console> (enable) commit security acl CAPTUREALL

console> (enable) set security acl map acl_name vlan_number
console> (enable) set security acl map CAPTUREALL 650

console> (enable) set security acl capture module_number/port_number
console> (enable) set security acl capture 6/7
```

VACL

```
router (config)# ip access-list [standard | extended] acl_name
router(config)# ip access-list standard CAPTUREALL

router(config)# vlan access-map map_name [0-65535]
router (config-access-map)# match [ip address {1-199 | 1300-2699 |
acl_name}]
router(config-access-map)# action forward capture

router (config)# vlan filter map_name vlan-list vlan_list

router (config)# intrusion-detection module module_number data-port
data_port_number
capture allowed-vlan vlan_list


router (config)# intrusion-detection module module_number data-port
data_port_number capture
```

mls ip ids

Cisco IOS Firewall on the MSFC, you cannot use VACLs to capture traffic, you can use the mls ip ids. Packets that are permitted by the ACL are captured. The permit/deny parameter does not affect whether a packet is forwarded to destination ports.

The mls ip ids command only captures incoming traffic.
You will need to use the mls ip ids command on both the client-side router interface and server-side router interface, so that both directions of the connection will be captured.
For IDSM-2 to capture all packets marked by the mls ip ids command, data port 1 or data port 2 of IDSM-2 must be a member of all VLANs to which those packets are routed.

```
router(config)# ip access-list extended word
router(config)# interface interface_name
router(config-if)# mls ip ids word
cat6k> (enable) set security acl capture module_number/port_number
```

```
router(config)# ip access-list extended word
router(config)# interface interface_name
router(config)# intrusion-detection module module_number data-port
data_port_number capture allowed-vlan capture_vlans
router(config-if)# mls ip ids word
```

IN-LINE

In-line CatOS

For IPS 5.0(1) you can only configure one IDSM-2 for inline mode between two VLANs. This restriction has been removed for IPS 5.0(2).

```
! Set the native VLAN for each IDSM-2 monitoring port:
set vlan vlan_number slot_number/port_number
cat6k (enable)> set vlan 651 9/7
cat6k (enable)> set vlan 652 9/8

; Clear all VLANs from each IDSM-2 monitoring port except for the
native VLAN
cat6k (enable)> clear trunk slot_number/port_number vlan_range
cat6k (enable)> clear trunk 9/7 1-650,652-4094
cat6k (enable)> clear trunk 9/8 1-651,653-4094

; For IPS 5.0(2), omit this step.
cat6k (enable)> set spantree bpdu-filter 6/7-8 enable
```

In-line - IOS

Cisco IOS software 12.2(18)SXE with Supervisor Engine 720 supports only one IDSM-2 inline between two VLANs.

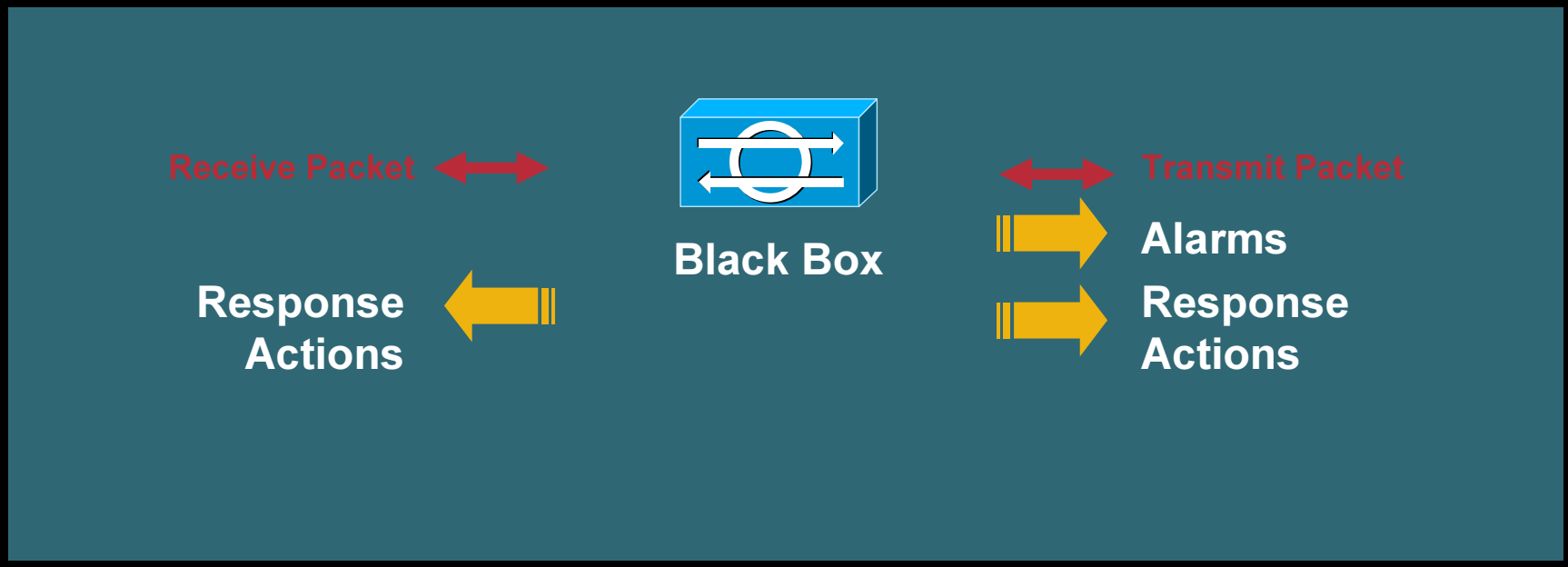
```
!Create two VLANs, one for each side of the inline IDSM-2:
router(config)# vlan vlan_number
router(config)# name vlan_name
router(config)# exit

! Configure an IOS access port for each interface on each inline VLAN
router(config)# interface interface_name
router(config-if)# description description
router(config-if)# switchport
router(config-if)# switchport access vlan vlan_number
router(config-if)# switchport mode access

!Configure one IDSM-2 data port to be on each of the two VLANs you
created
router(config)# intrusion-detection module slot_number data-port
data_port_number access-vlan vlan_number
```

Capturing Support

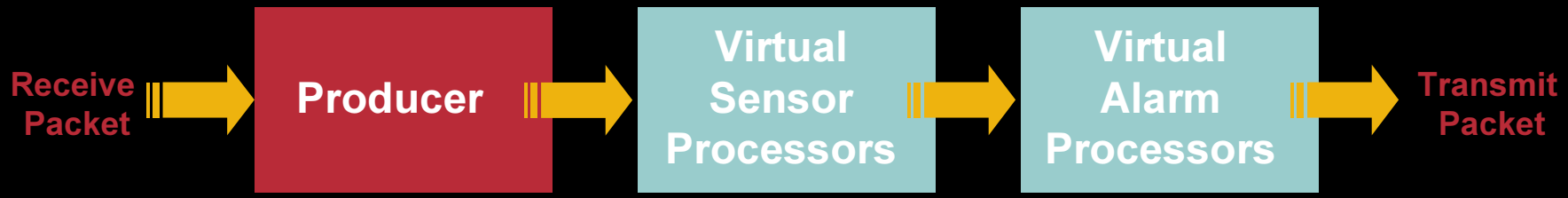
Config	SPAN/RSPAN	VACL capture
Sup 1A	X	-
Sup 1A w/PFC1	X	X
Sup 1A w/PFC1 or MFSC1	X	X
Sup 1A w/PFC2 or MFSC2	X	X
Sup2 w/ PFC2	X	X
Sup w/PFC2 or MSFC2	X	X
Sup720	X	X

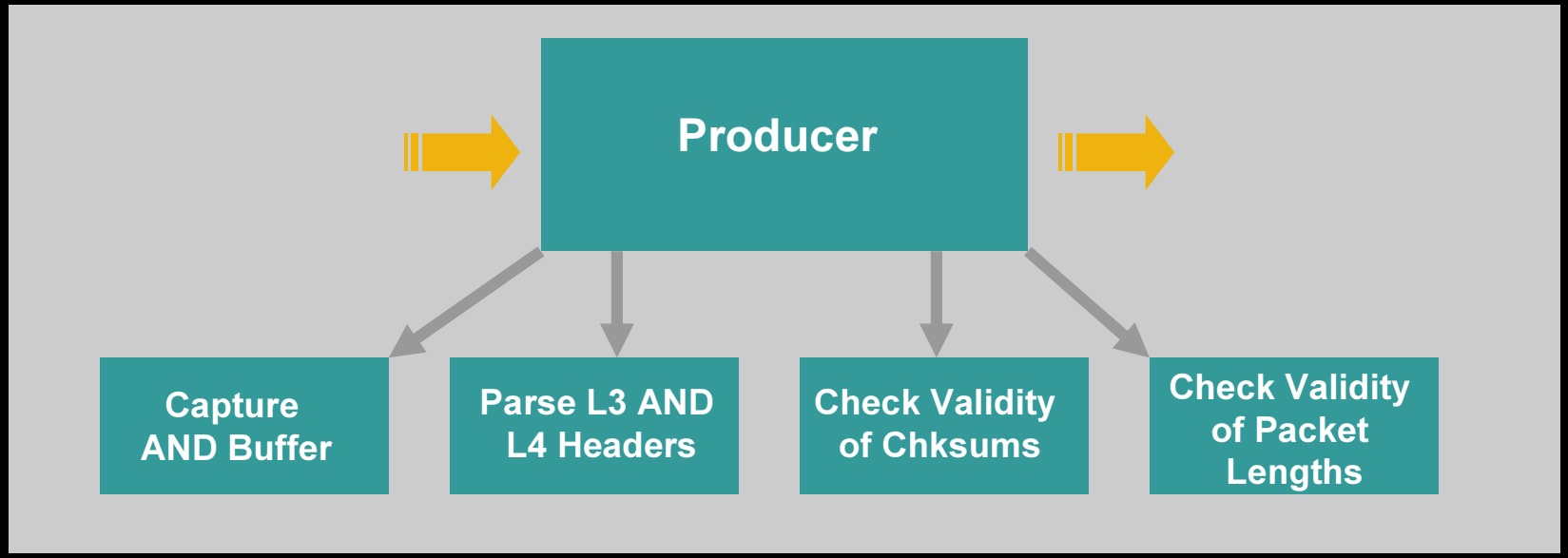
IPS KONFIGURÁCIÓ

IPS Sensor Packet Analysis:
A Day in the Life of a Packet



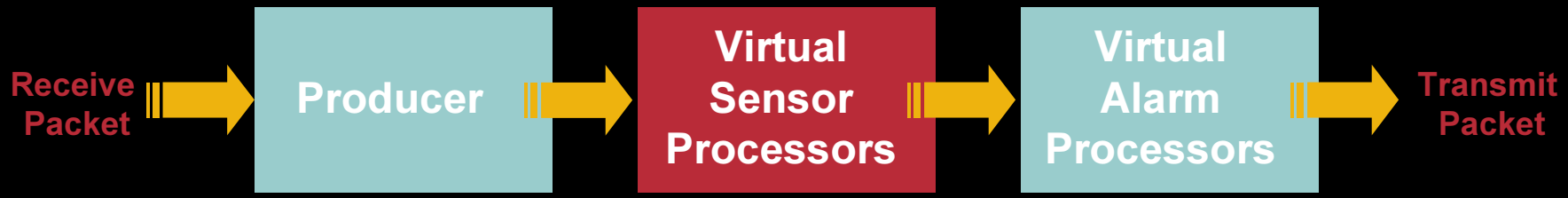
The Producer

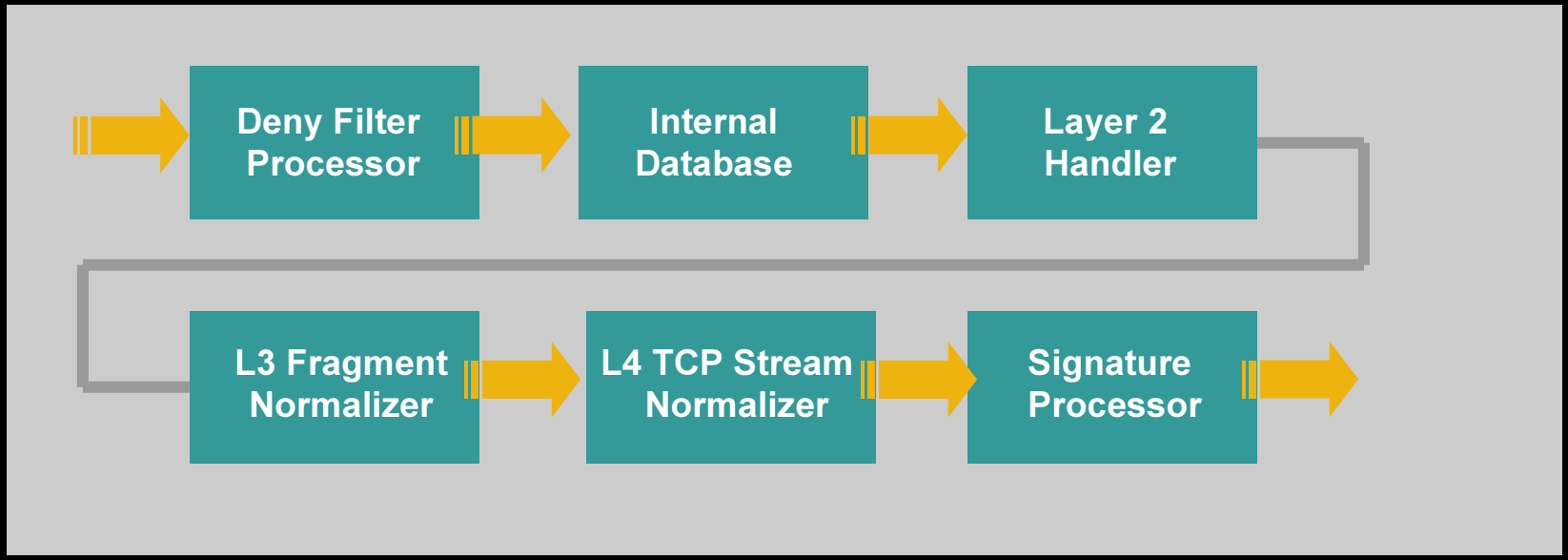




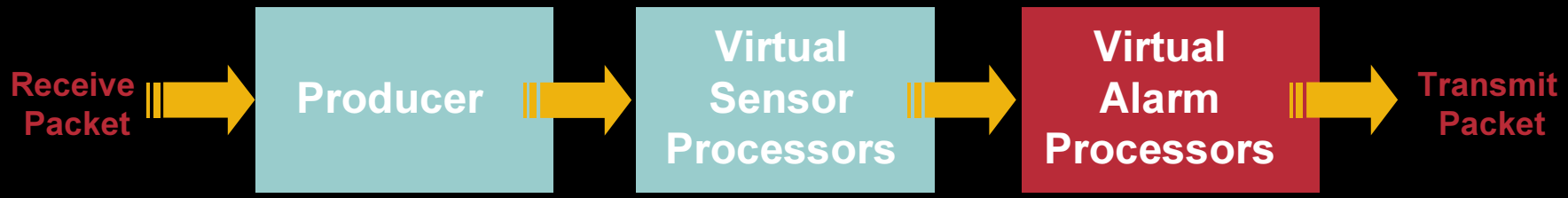
Based on IPS 5.x Sensor Code

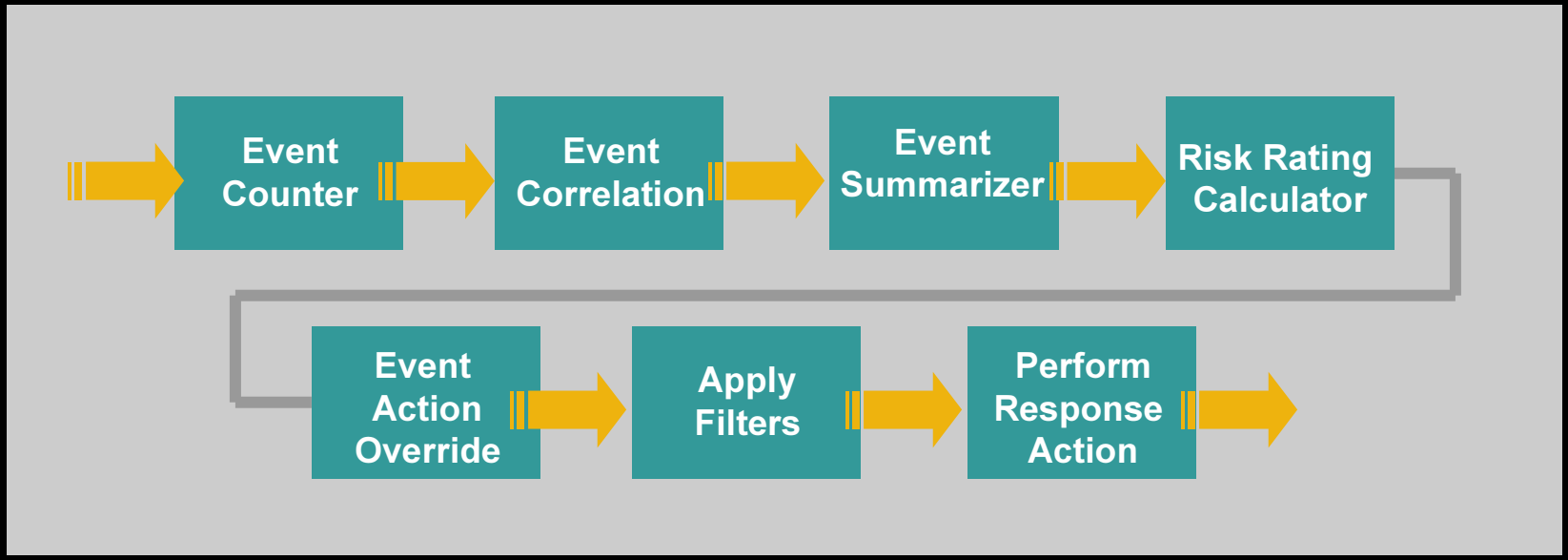
Virtual Sensor Processors





Virtual Alarm Processors





Scaling Analysis: Signature Engines

- Traffic analysis is incredibly computationally intensive with large numbers of signatures
- Cisco IPS analysis implemented with a series of engines that each inspect for a specific type of activity
- Signature engine types:

Atomic	Flood	Traffic
Meta	Service	Normalizer
State	String	AIC
Sweep	Trojan	Other

Signatures Revisited

Signatures Do Not Necessarily Mean String Matching

- Simple pattern matching

  E.g. look for “root”

- Stateful pattern matching

  E.g. decode a telnet session to look for “root”

- Protocol decode and anomaly detection

  E.g. RPC session decoding and analysis; SNMP protocol anomaly detected from use of protos tool

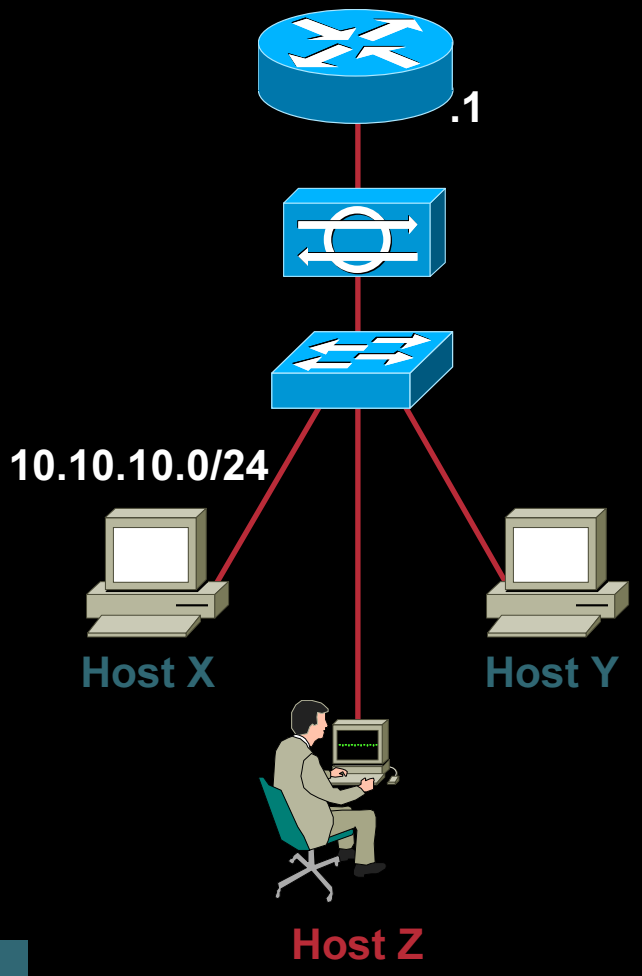
- Heuristics

  E.g. rate of inbound SYNs—SYN flood?

Signature Example: Protection at Layer 2 (Data Link Layer)

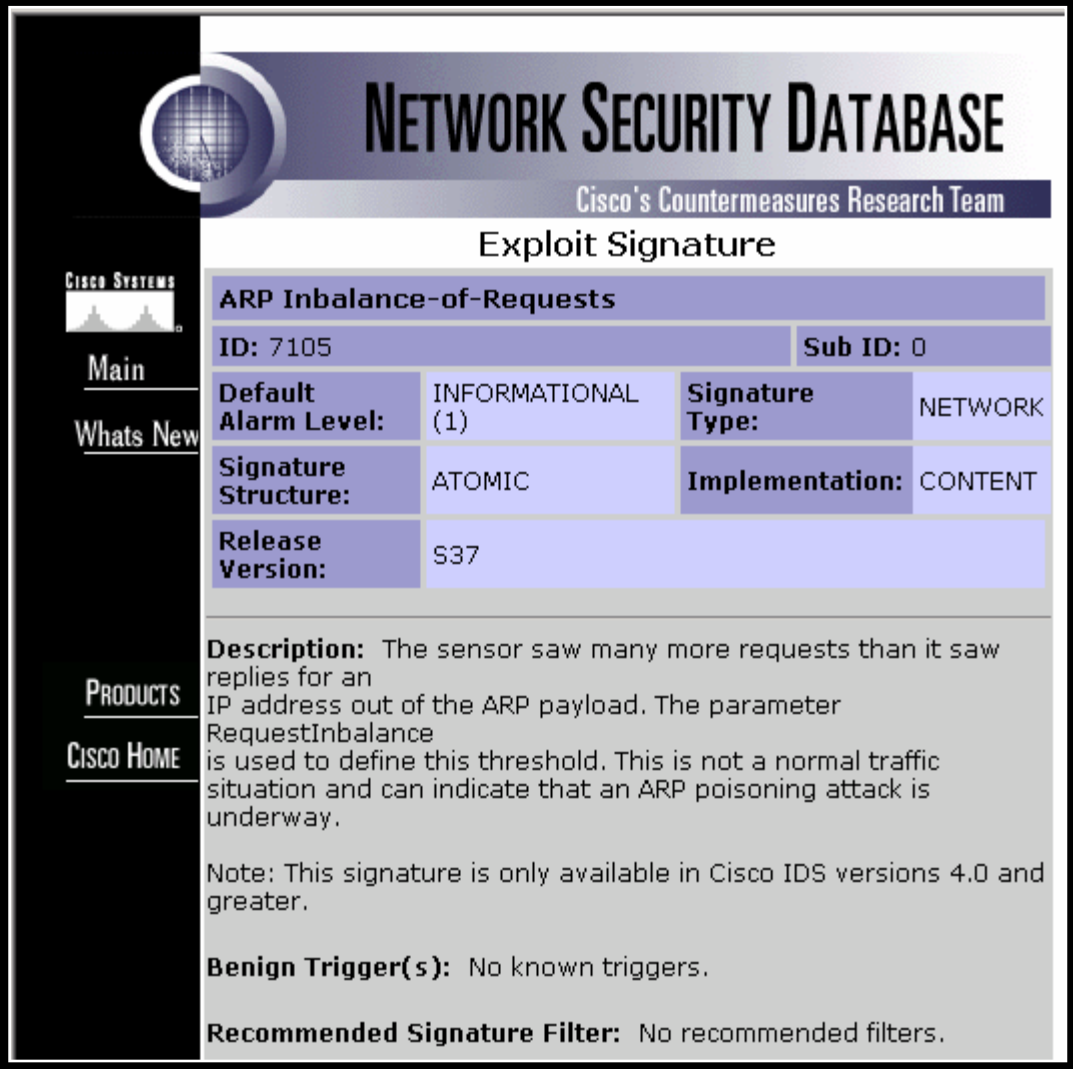
- Host Z is a malicious user, attempting to gain access to traffic from hosts X and Y
- Host Z sends gratuitous ARP replies, telling all that he is 10.10.10.1 (router), with his MAC address
- Since ARP replies are broadcast, all hosts on the same L2 subnet see and accept the gratuitous ARP
- If host Z is more persistent than the actual router in asserting its identity, host X and Y will believe that host Z is the router
- Host Z has effectively inserted himself as a man in the middle, since host X and Y will send it their IP traffic

Signature ID 7105 Detects the Above Attack



Alarm Guidance: NSDB

- Most products have an alarm database that provides guidance on alarms
- Web or text-based DBs can allow addition of custom information or directions for operations staff



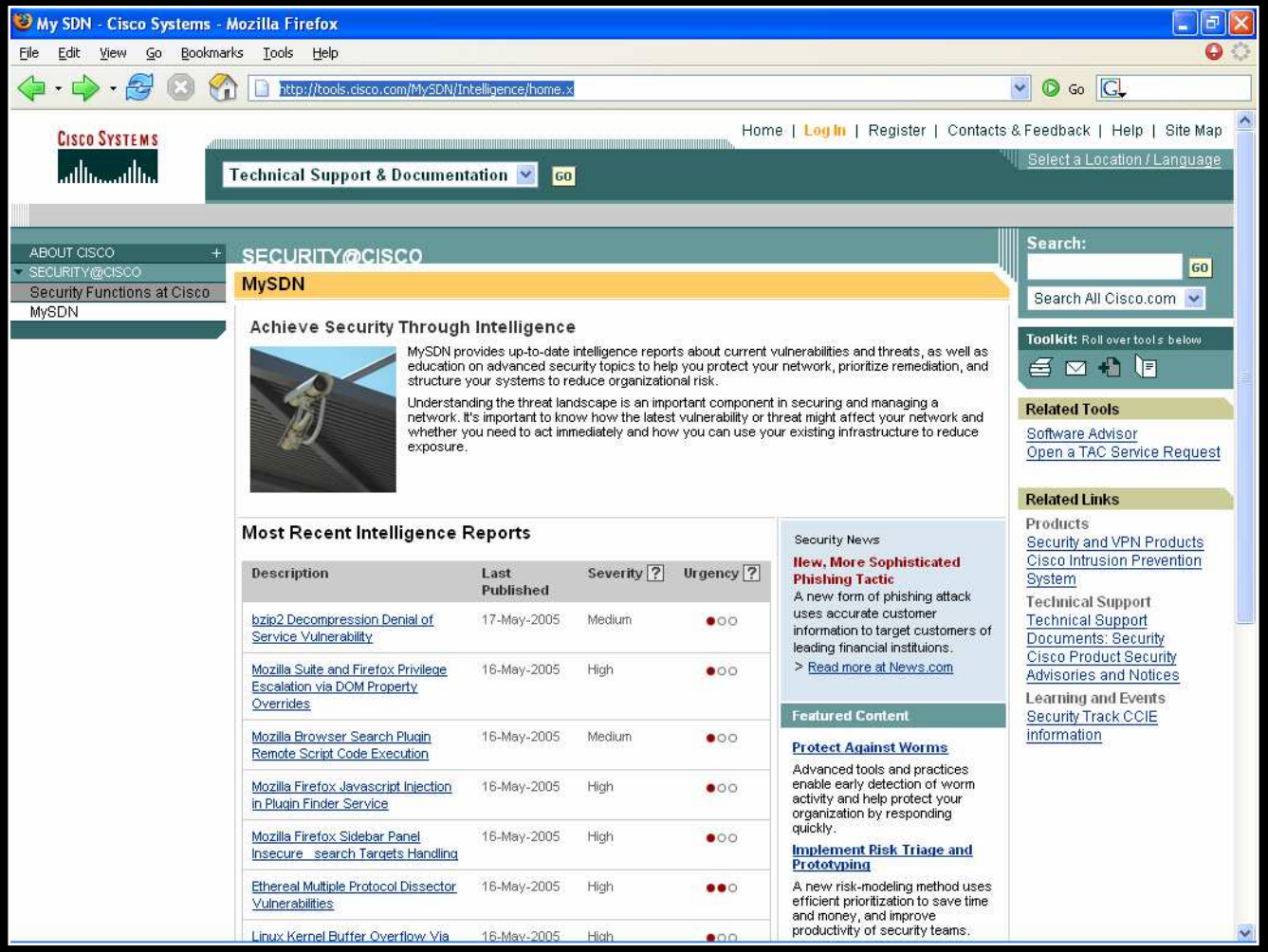
Signature Updates

- Much like anti-virus, network IPSs must be kept up to date
- Process must be developed to rapidly update new signatures as released
- Cisco has developed a new partnership with Trend Micro to provide enhanced virus and worm coverage as part of the normal IPS signature updates
- Cisco has a new home for security information in general:

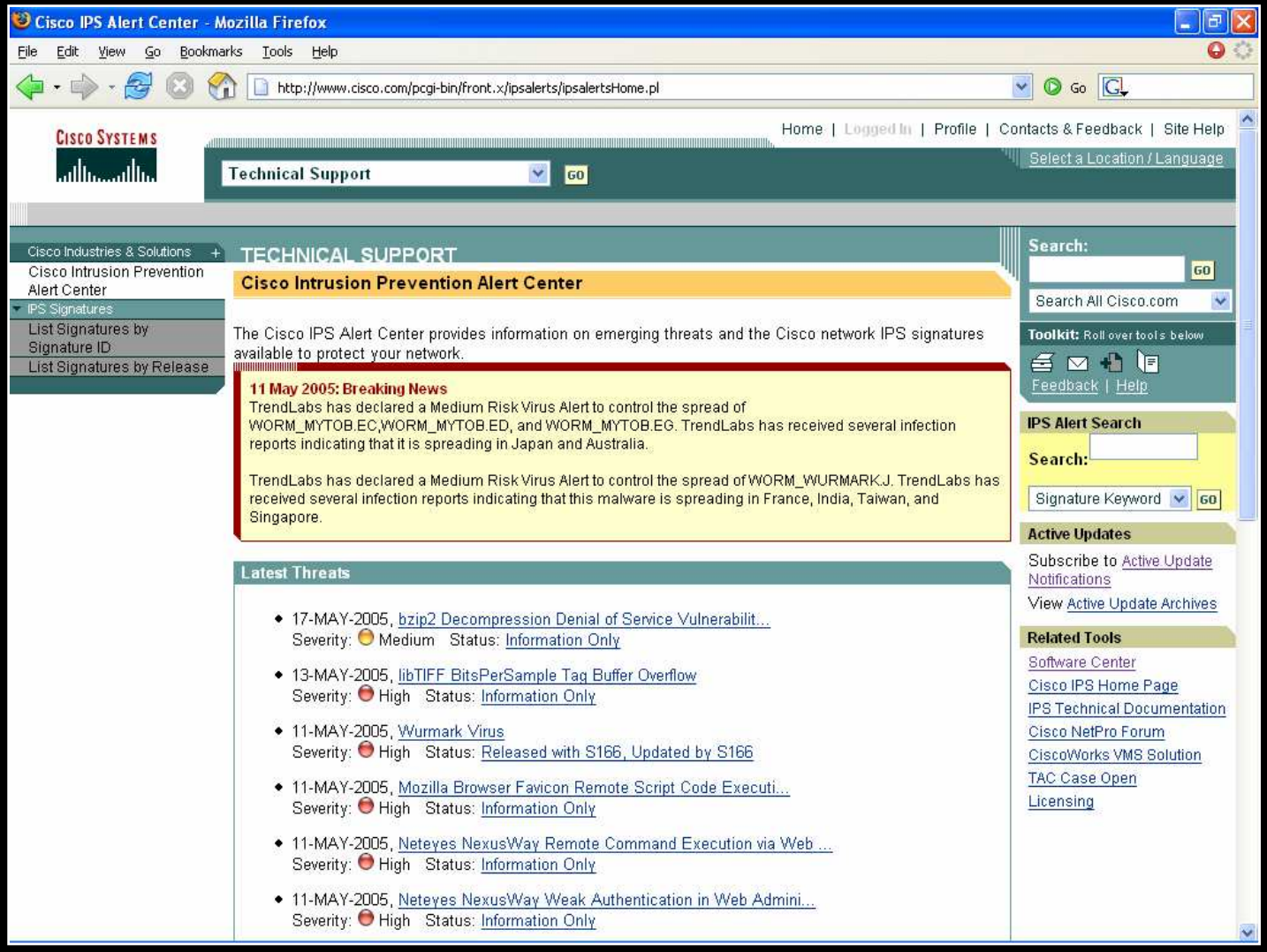
  tools.cisco.com/MySDN/Intelligence/home.x
- There is also a new home for all things IPS related:

  www.cisco.com/go/ipsalert

MySDN: Cisco's Security Portal



IPS Alert Center for All Things IPS Related



Tuning Your Sensors

- Tuning is the most important part of intrusion detection and prevention deployments
  - The data reduction that results from proper tuning is essential for a fully functional system
- Not every sensor needs to alert on every event
  - Implementing environment specific configurations increases scalability of the entire system

Tuning: Where to Start

- **Most sensors ship with a default signature configuration**
  - **This is a good starting point for an initial deployment in most cases**
- **Start by monitoring the default configuration**
  - **Prioritize the tuning of the high priority alarms, and then move on to the mediums**

How to Tune a Sensor: Techniques

- Understand the environment and traffic patterns
- List out potential false positives
  - Analyze each alert and classify stimulus and response
- Define policy, and policy exceptions
  - i.e. ping sweeps generate alarms, except when coming from the management network
- Turn down severity of signatures not applicable to that environment
- Iterative process: as traffic patterns change, sensors can require re-tuning

Example Tuning Features

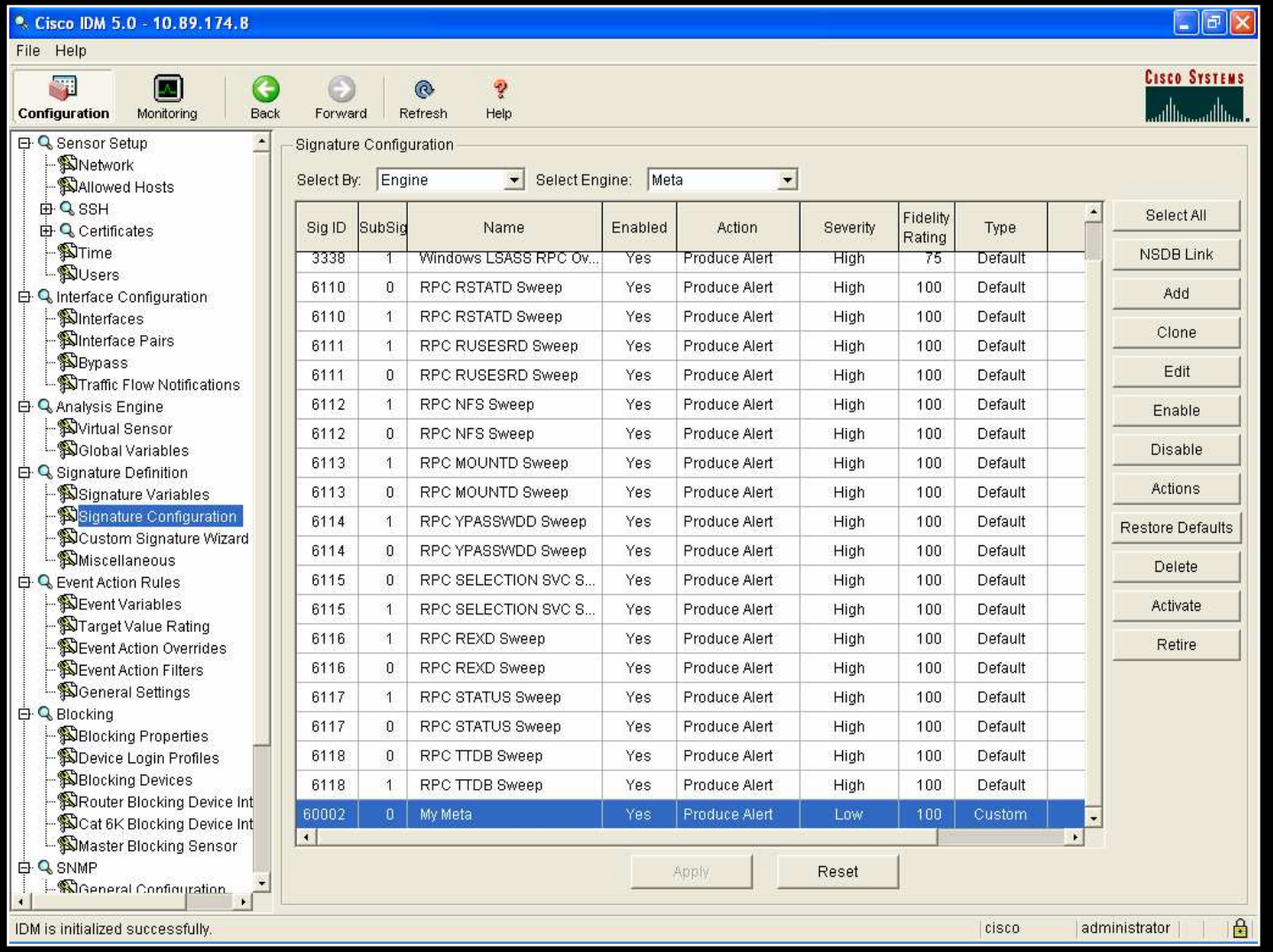
- **Signature specific:**
  - **Ports, protocols, services, analysis length, etc.**
- **Filtering: what networks to alarm on**
- **Event count: number of events to see before alarm**
- **Severity: what level of alarm to send**
- **Alarm aggregation: how many alarms to send**
  - **Summary mode: fire all, summarize, global summarize**
  - **Summary interval: summarization window**
  - **Summary threshold: high water mark to change summarization**
- **Event action: what to do following when the sig is triggered (includes producing an alert)**

Customizing Your Signature Set

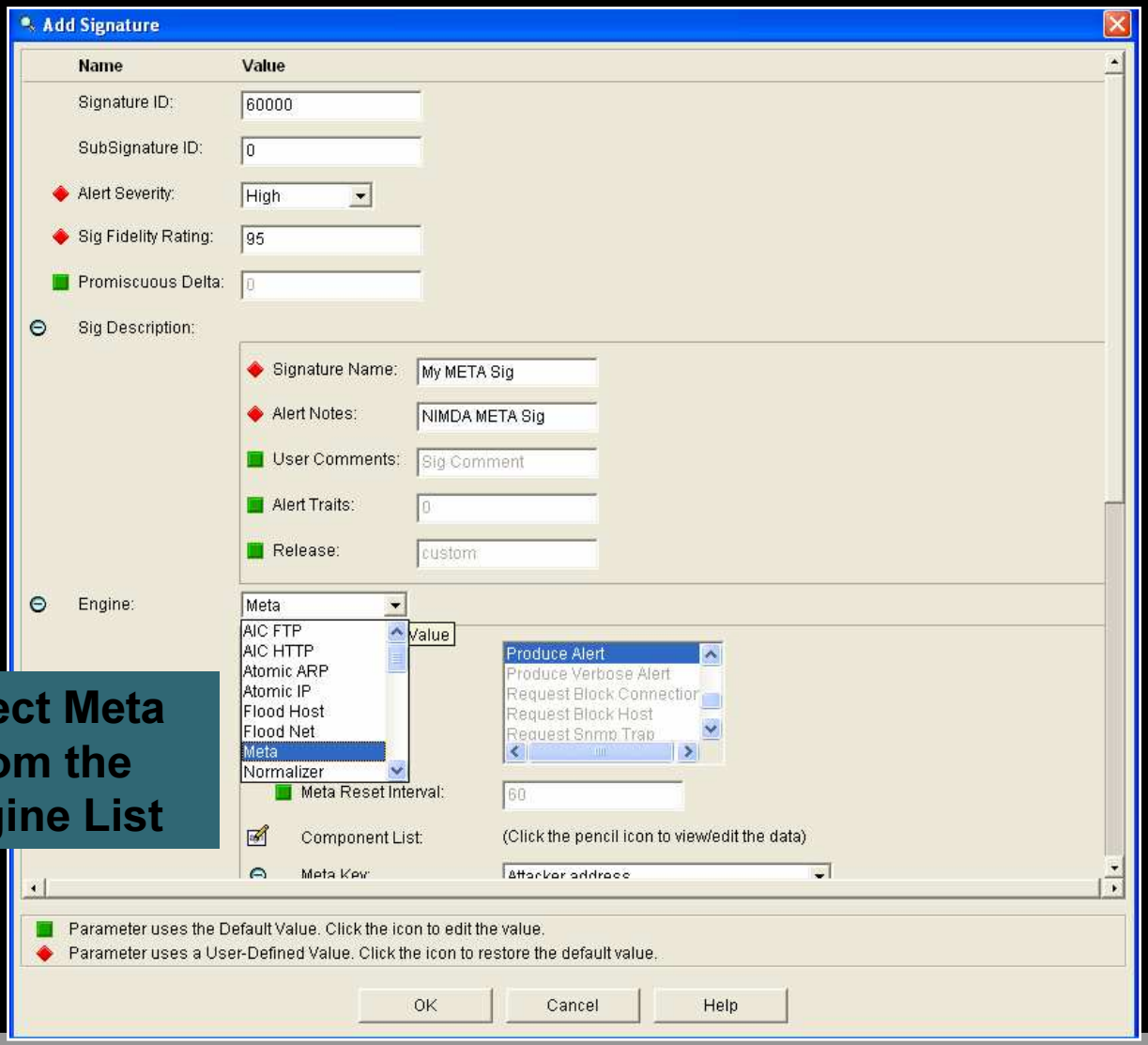
- Customize vendor-provided signatures
- New environment specific signatures can be created
- Cisco custom signature configuration tasks:
  - Select the signature micro-engine that best meets your requirements
  - Enter values for the signature parameters that are required and meet your requirements
  - Save and apply the custom signature to the sensor
- Signature customization is not trivial
  - Writing signatures requires detailed knowledge of the attack; poorly focused signatures will generate false positives and too narrowly focused or outright mistakes might result in false negatives
  - Test, test and test again before you deploy

Custom Signatures

Choose Configuration> Signature Configuration> Add

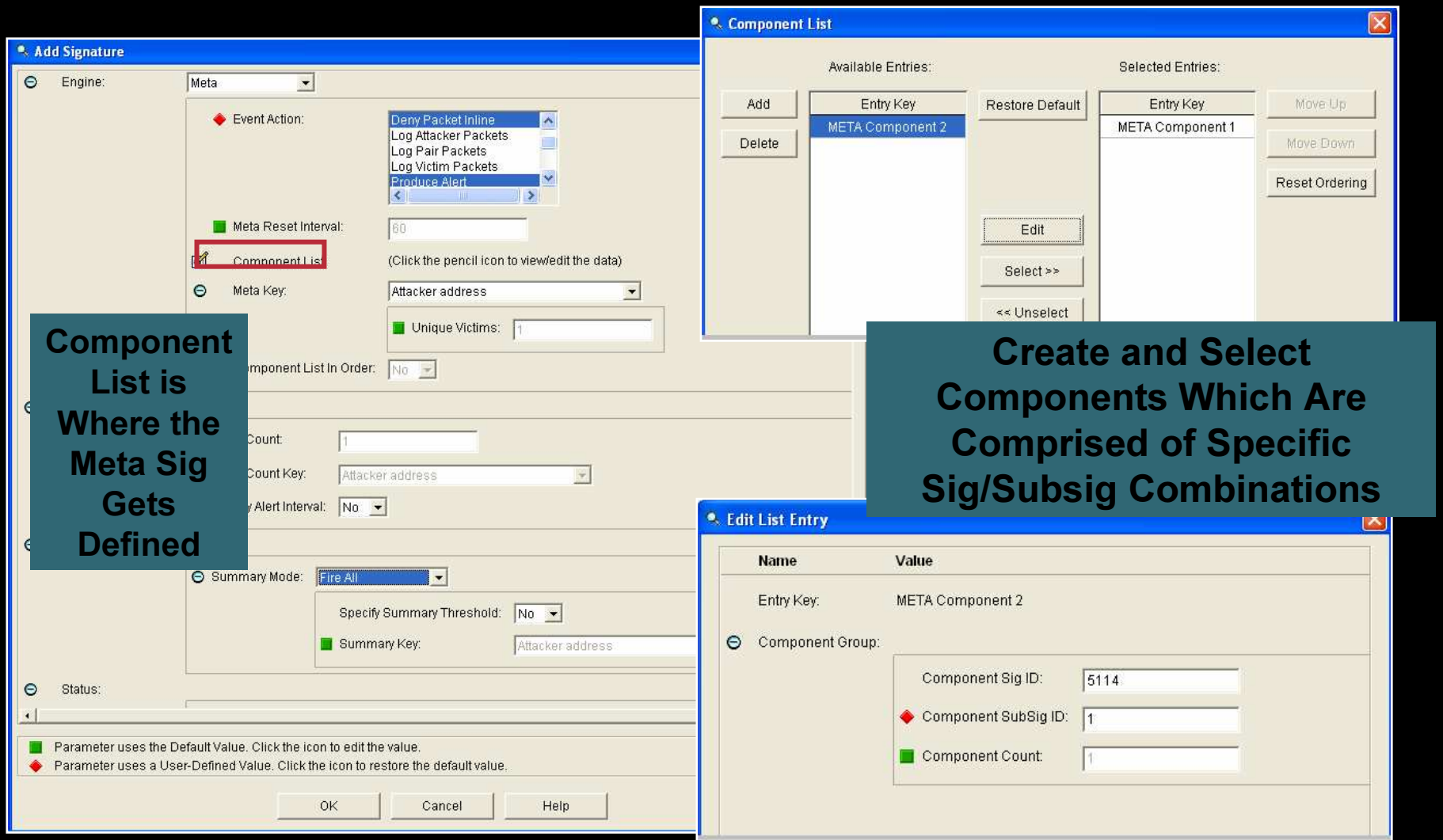


Example: Meta Signature (Local Correlation)



Select Meta from the Engine List

META (Cont.)



Component List is Where the Meta Sig Gets Defined

Create and Select Components Which Are Comprised of Specific Sig/Subsig Combinations

Active Response: IDS

- A sensor deployed in IDS mode allows a number of response actions to be taken when an alert is generated:
  - Log packets to a file in PCAP format
  - Blocking using an external device (router or firewall)
  - TCP resets—sends TCP reset packets to break a TCP connection
- Actions configurable per signature

→ False Positives Can Be Problematic ←

Active Response: IPS

- A sensor deployed in IPS mode operates on the actual network packets instead of copies
  - Multiple different deny actions are possible in addition to all actions supported in IDS mode
    - Deny attacker
    - Deny connection
    - Deny packet
- Actions configurable per signature

→ False Positives Are Still Problematic ←

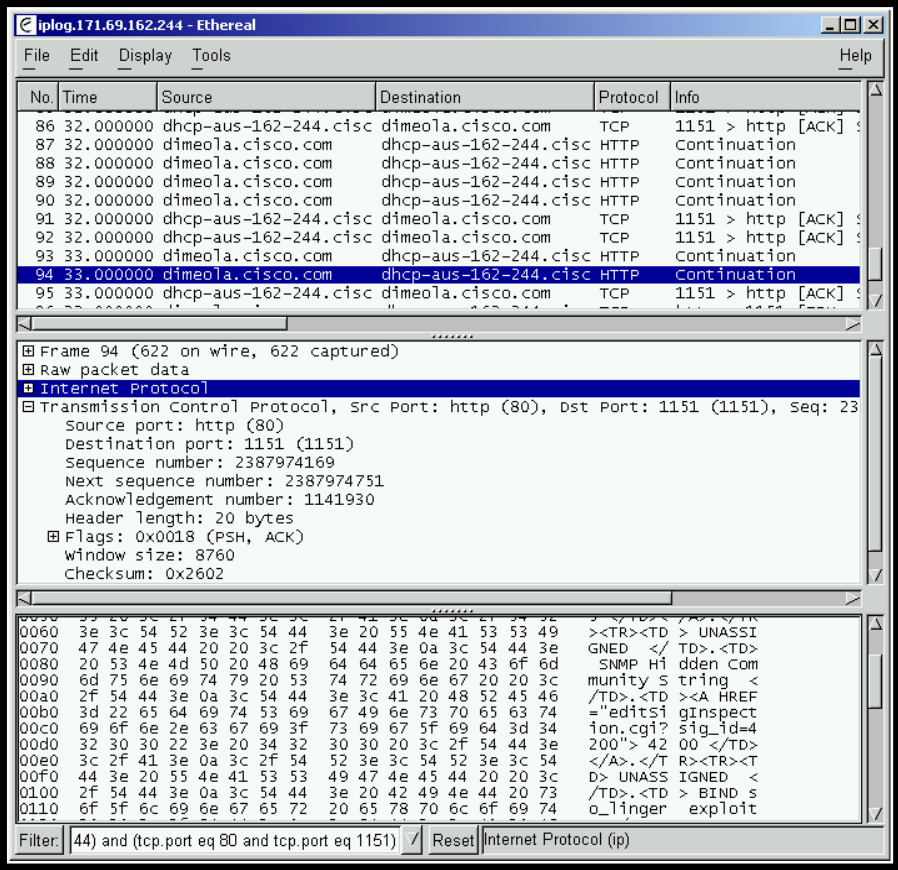
Deny Packet (Inline Only)

When Signature Fires, Sensor Discards the Packet That Triggered the Alarm

- Pros:
  - Stops the attack packet
  - Most useful for events that are triggered frequently (i.e. worms)
  - Lower chance of self-inflicted DoS if wrong (unless deny attacker is used)
- Cons:
  - Less useful to stop a determined attacker as he will move on to other attacks or victims that may not be protected (unless deny attacker is used)
  - Sensor must be inline to perform this action
- Limitation: Traffic that does not pass through the sensor cannot be scrubbed in this manner (must have full featured IPS everywhere to be most effective)

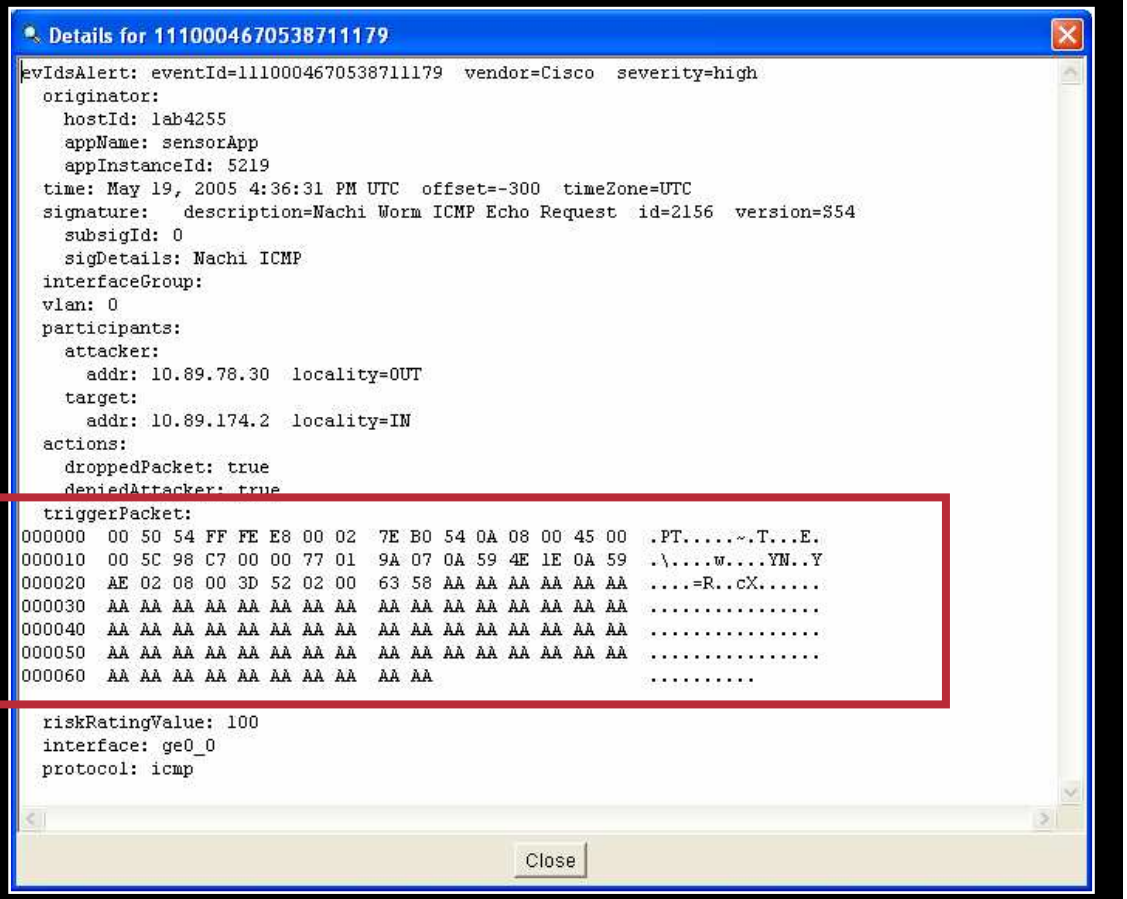
Logging: Session Capture

- Logs traffic associated with a signature trigger (in PCAP format)
- Generally, only trigger and subsequent packets logged
- Does impact sensor performance
- Usage guidelines:
  - Tuning: Use during sensor tuning for event analysis and subsequent signature tweaking
  - Forensics: Useful to monitor “critical” signatures/resources
  - Handy tip: Use with a custom signature to monitor a specific service/server/user
  - Do not log unless you know what you plan to use the log for



Logging (Alternative): Produce Verbose Alert

- Instead of creating a log file with many packets, capture and include as part of the alert just the packet that triggered the alert



TCP Resets

- For TCP applications, connection is prematurely terminated by a RST sent from “sensing” interface
- Must guess correct TCP sequence number and successfully insert RST into session
  - Makes TCP resets somewhat unreliable especially when source and destination are “close”
- Certain applications will automatically reconnect and resend (e.g., SMTP), making this less effective
- Note that initial trigger packet will make it to its destination, so can’t necessarily stop event
  - Code red 1 was a single packet attack and couldn’t be reset
- Conclusion: TCP resets are a temporary solution while you readjust your security posture

Gotchas: TCP Resets and SPAN

If You Use TCP Resets, You Must Enable Input Packets so Switch Will Accept RST Packets on SPAN Port (Check Your Switch to Determine Exact Support for IPS Reset Packets)

```
set span <src_mod/src_ports...|src_vlans...|sc0>
         <dest_mod/dest_port> [rx|tx|both]
          [inpkts <enable|disable>]
         [multicast <enable|disable>]
         [filter <vlans...>]
```

If Monitoring Multiple VLANs, Cisco IPS Sources the Resets into the Correct VLAN

Blocking (Shunning)

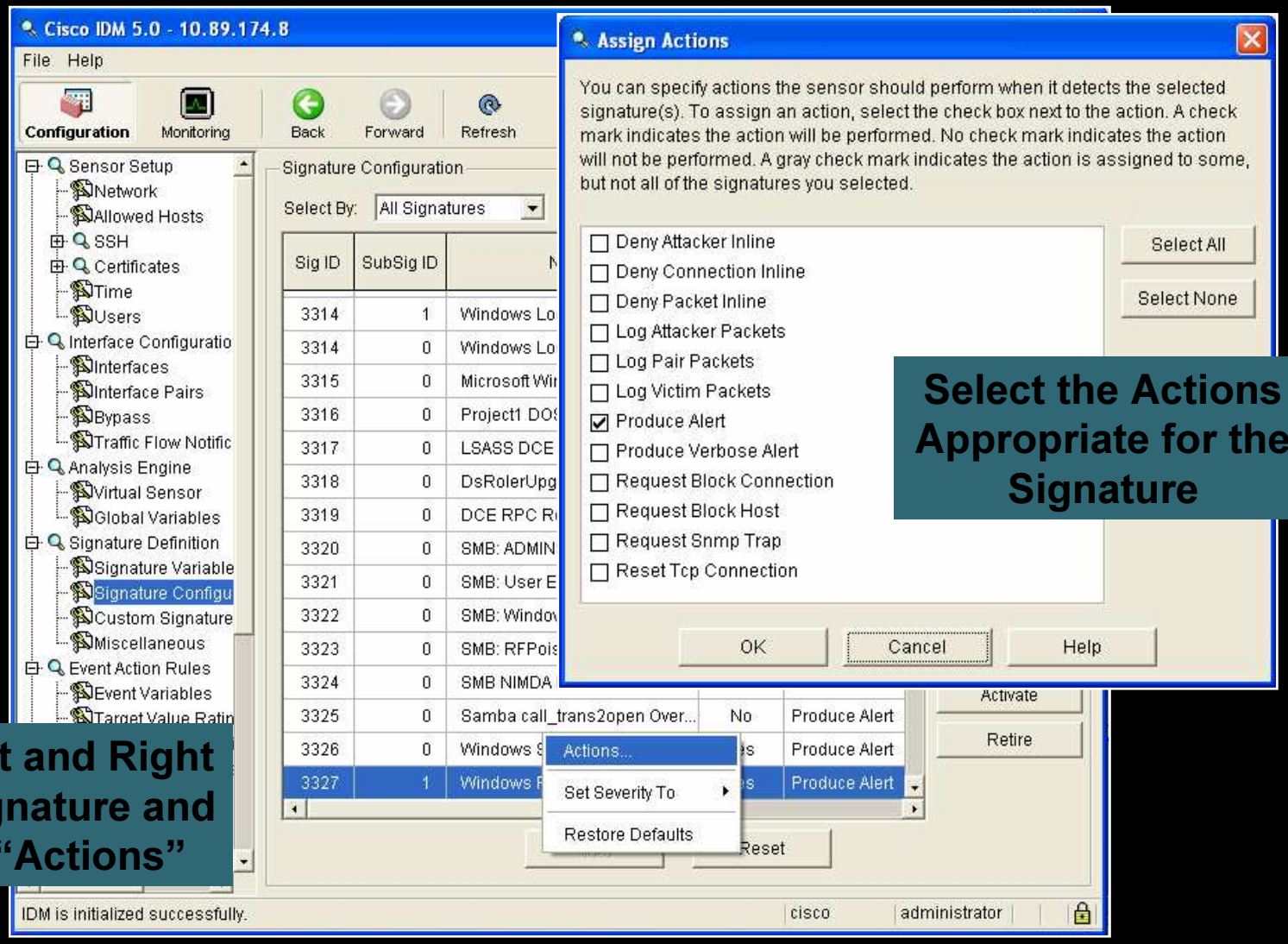
- When signature fires, sensor inserts ACL on router/issues shun command on PIX® firewall
  - Deny subsequent traffic from that source IP address or associated with that specific connection
  - Note that initial trigger packets will make it to the destination because of the time required to establish the block
- Sensor connects to firewall and/or router from management interface
  - Need to configure authentication credentials for firewall/router
- Conclusion: Blocking can be effective at stopping an infected host but can't stop first attack

Blocking

Can Be Very Successful in Helping to Implement a Security Policy

- Pros:
  - Best used to thwart an attacker at the first location possible
  - Can be used to block a source address at multiple locations
  - Sensor can be “out of band” (IDS)
- Cons:
  - Does not stop the attack packet or even the connection
  - Less useful in stopping thousands of automated attackers (i.e. worms), or for e-mail viruses
- Limitation: User must have a well thought out security policy combined with a good operational understanding of their IDS deployments (correctly tuned sensors are a must)

Configuring Response Actions



HA

High Availability for IPS

- Deploying an IPS sensor into the traffic stream introduces a new device to possibly fail and prevent traffic from flowing (It will be the first thing blamed for any problems)
- High availability is defined as building into the network, the ability to cope with the loss of a component of that network to ensure that network functionality is preserved

  Solutions:

  Failopen techniques: Hardware or software that functions to detect problems and pass packets through the device without inspection when required

  Failover: One or more paths through the network to allow packets, in the event of a device failure, to either go through a backup IPS sensor or through a plain wire

  Load balancing: Using devices or software features to split a traffic load up across multiple devices; this can achieve both higher data rates and redundant paths in case of failure

IPS Fail-Open

IPS Fail-Open Mechanisms

- Hardware based fail-open functions by closing a circuit when either power is removed, a link fails, or potentially when triggered by software
- Software based fail-open functions by building some software feature to pass packets when a failure is detected or packets are not flowing normally for any reason

→ Best Case Is Reliance on Fail-Open Strategies Leaves You with No Protection and, at Worst, Can Bring Down Your Entire Network ←

Failover

Network Failover Allows the Network to Recover from a Device or Physical Layer Failure

- **Layer three: Pix failover, Cisco IOS HSRP**
- **Later two: spanning tree**

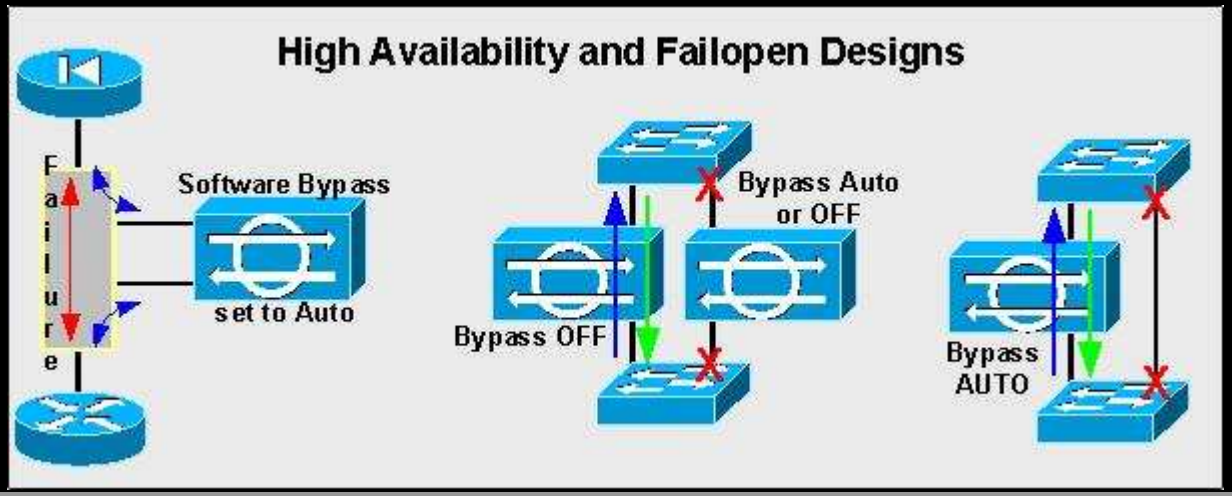
  Typical IPS sensors (non layer three) do not and cannot control network failover; they function like a wire and a failure of the sensor should look like a failure of a wire; the network will respond accordingly; fail-open capabilities help but do not truly solve the problem.

→ True High Availability Is Something Built into the Network, Never Built into a Single Piece of Hardware or Software ←

Fail-Open and Failover Deployments

IPS Appliance Sensor Solutions

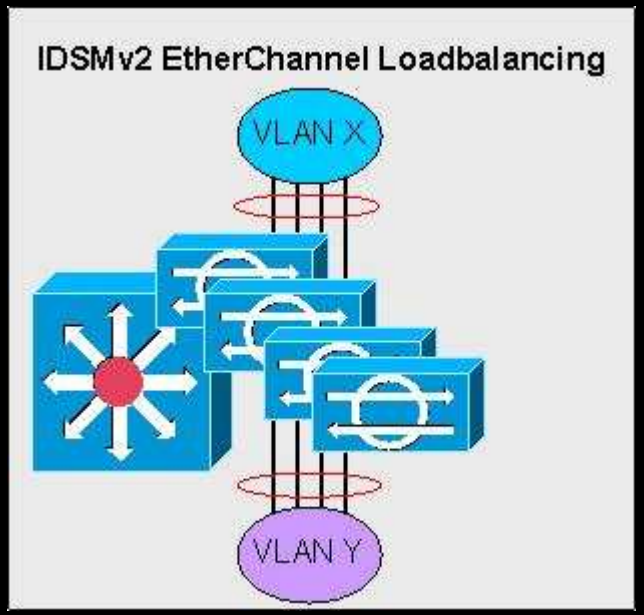
- Standalone sensor in hardware bypass deployment
- Redundant deployment using spanning tree for active/ passive failover
- Redundant deployment using spanning tree for high availability (along with plain wire)



EtherChannel Load Balancing

IPS Sensors Can Be Deployed Inline as Part of an EtherChannel® (EC) to Provide Redundancy

- Allows up to eight sensors deployed inspecting the same data set
- Relies on EC algorithm to split flows amongst the different blades (no guarantee of equal load)



Design Metrics for EC Load Balancing

	Designing for Performance		Designing for Redundancy			
Number of IDSM-2	Performance Design (Mbps)*	Perf. if 1 Unit Fails	Redundancy Design (Mbps)*	Perf. if 1 Unit Fails	Number of Units That Can Fail	Max Avg. Load per Device
1	1x Unit Performance	0				
2	2x Unit Performance	<1x**	1x	1x	1	.5x
3			2x	2x	1	.66x
4	4x Unit Performance	<3x**	2x	2x	2	.5x
5			4x	4x	1	.8x
6			4x	4x	2	.66x
7			4x	4x	3	.57x
8	8x Unit Performance	<7x**	4x	4x	4	.5x

*Maximum Attainable Performance in Mbps **Data Lost

KÉRDÉSEK ÉS VÁLASZOK

További információk

www.cisco.com/go/ips
Cisco IPS

www.cisco.com/go/srnd
Solution Reference Network Design
Includes Data-Center architectures with services modules

www.cisco.com/go/cvdm
Cisco View Device Manager

További információk

- Cisco IPS product documentation
  - www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/index.htm
- Cisco MySDN
  - tools.cisco.com/MySDN/Intelligence/home.x
- Cisco IPS alert center
  - www.cisco.com/pcgi-bin/front.x/ipsalerts/ipsalertsHome.pl
- Cisco IPS discussion forum
  - www.cisco.com/go/netpro
- Cisco security advisories (includes a number of security documents)
  - www.cisco.com/en/US/products/products_security_advisories_listing.html
- Vulnerability information
  - www.cert.org
  - www.incidents.org
  - www.securityfocus.com
  - whitehats.com
- Ethereal tool to view IP session logs
  - www.ethereal.com