Designing and Deploying Intrusion Detection Systems

Mike Peeters

Security Specialist SE

Cisco Systems Canada

CISSP, CCIE, CSSP,CCDA

The Challenge: Security in Modern Networks

The **Number** of Security Incidents Continues to Rise Exponentially

The **Complexity** and **Sophistication** of Attacks and Vulnerabilities Continues to Rise

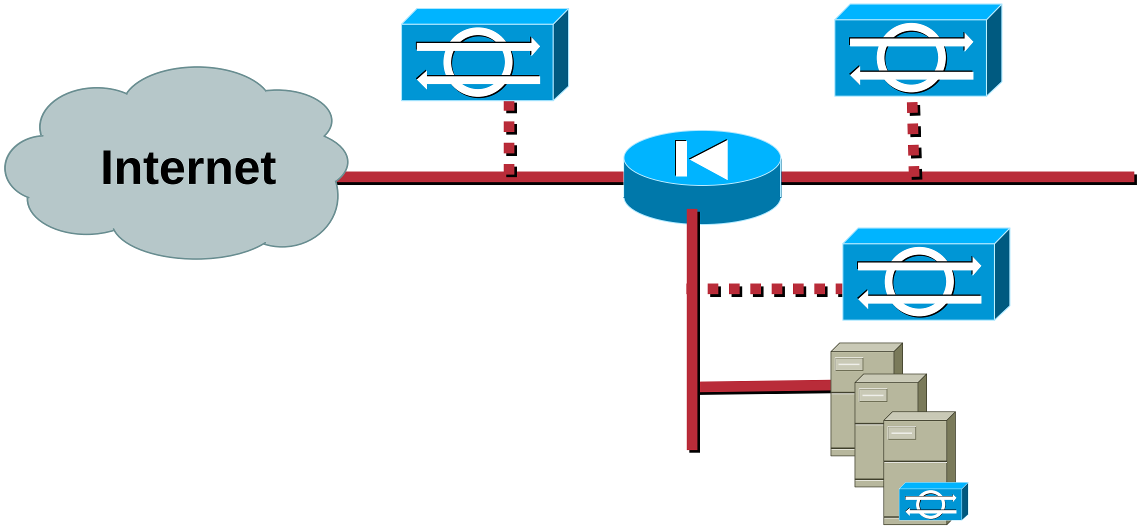
The Potential **Impact** to the Bottom Line Is Significant

Mitigating the Risk: Defense in Depth

- **Comprehensive security policy**
- **Pervasive security—end to end**
- **Security in layers**
- **Multiple technologies, working together**

Defense in Depth:
The Role of Intrusion Detection

- Complementary technology to firewalls
- Been around for more than a decade, started coming into prominence in the late ’90s
- Performs deep packet inspection, gaining visibility into detail often missed by firewalls



Designing and Deploying Intrusion Detection Systems: Agenda

- Intrusion Protection Systems
- Network Sensors
- Host Agents
- Cisco Security Agent Demonstration

Intrusion Protection Systems

Intrusion Protection Agenda

- Terminology and Technologies
- Complete Architecture:

  Sensors, Agents, Management Consoles
- Placement Strategies

  Where to Place Your Sensors, what Traffic to Watch, How to Get Traffic to Them
- Organization-Level Concerns

  Responding to Intrusions, Ownership and Organization, Outsourcing
- Cisco Security Agent Demonstration

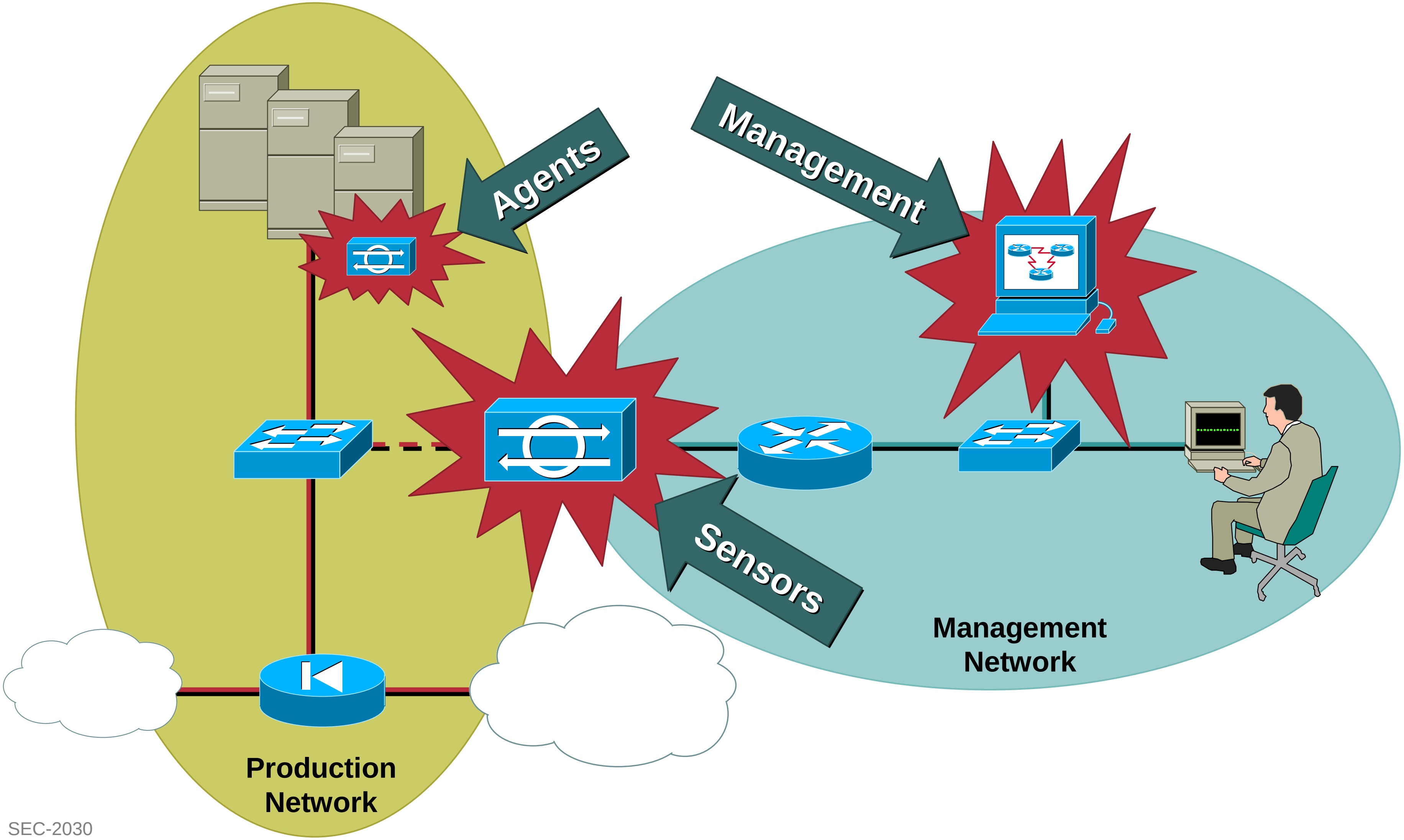
IDS Terminology:
False Positives and False Negatives

- **False Positives:** **Benign activity that the system mistakenly reports as malicious**
- **False Negatives:** **Malicious activity that the system does not detect or report**

IDS Terminology: Signatures and Anomalies

- Signatures explicitly define what activity should be considered malicious
  - Simple pattern matching
  - Stateful pattern matching
  - Protocol decode-based analysis
  - Heuristic-based analysis
- Anomaly detection involves defining “normal” activity and looking for deviations from this baseline

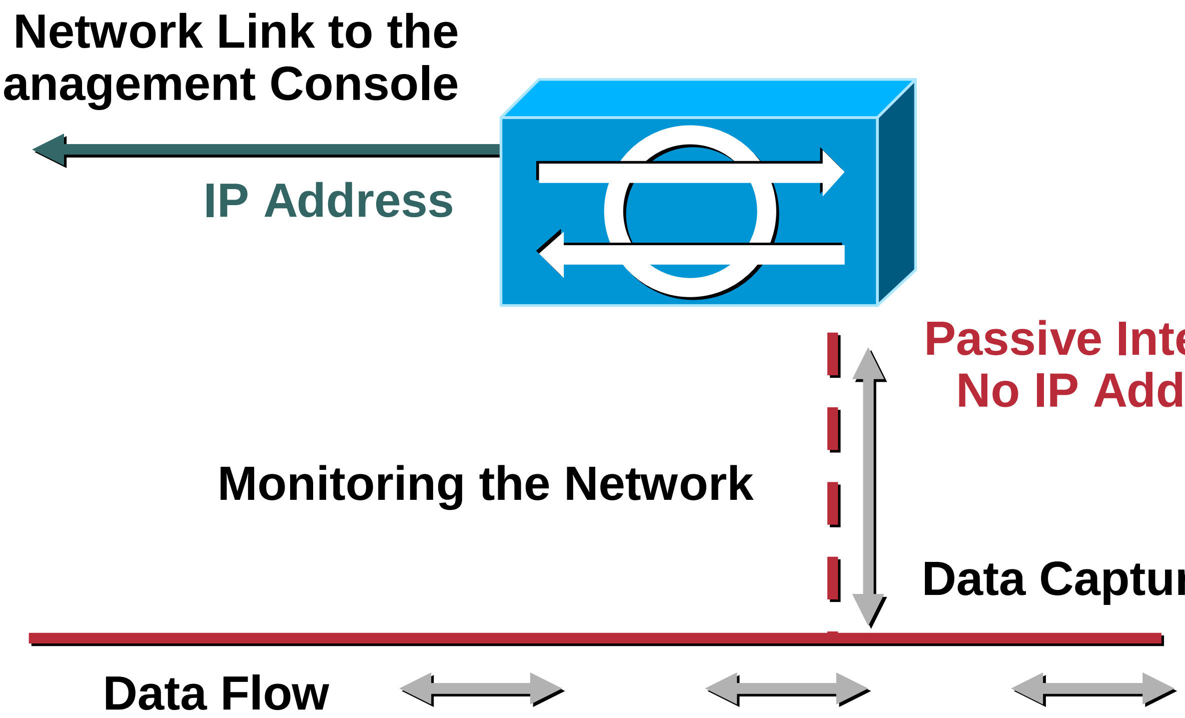
IDS Architecture: Sensors, Agents, and Management



IDS Components

- **Network-Based Sensors**
  - Specialized software and/or hardware used to collect and analyze network traffic
  - Appliances, modules, embedded in network infrastructure
- **Host-Based Agents**
  - Server-Specific Agent
  - Provides both packet- and system-level monitoring, and active response
- **Security Management and Monitoring**
  - Performs configuration and deployment services
  - Alert collection and aggregation for monitoring

Network-Based IDS: The Sensor



Network Link to the Management Console

IP Address

Passive Interface
No IP Address

Monitoring the Network

Data Capture

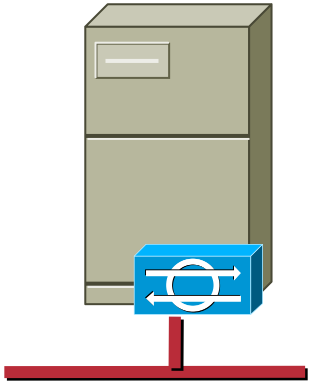
Data Flow

Network-Based IDS: Functions and Capabilities

- Monitors all traffic on a given segment
- Compare traffic against well known attack patterns (signatures); also look for heuristic attack patterns (i.e. multi-host scans, DoS)
- Includes fragmentation and stream reassembly logic for de-obfuscation of attacks
- Primarily an alarming and visibility tool, but also allows active response: IP session logging, TCP reset, shunning (blocking)

Host Agents: Functions and Capabilities

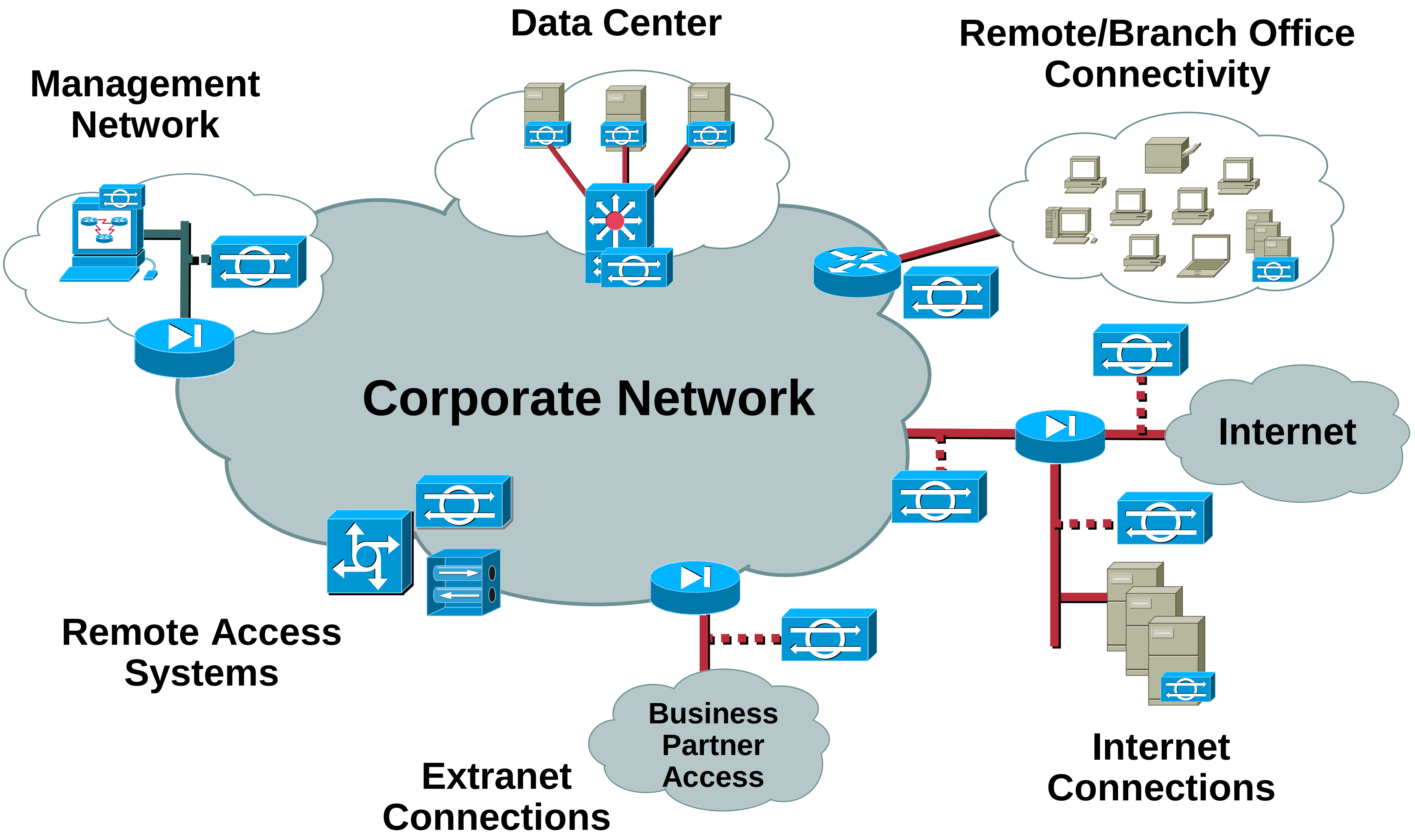
- Distributed Agent residing on each server to be protected
- Intimately tied to underlying operating system
  - Can allow very detailed analysis
  - Can allow some degree of Intrusion Protection
- Allows analysis of data encrypted for transport
- Monitors kernel-level application behavior, to mitigate attacks such as buffer-overflow and privilege escalation



Placement Strategies

- Monitor your critical traffic
- Deploy network sensors at security policy enforcement points throughout the network
- Deploy host sensors on business critical servers
- Beware of sensor overload—sensors must be able to handle peak traffic loads

Intrusion Detection Deployment
What Areas of the Network Are Candidates?



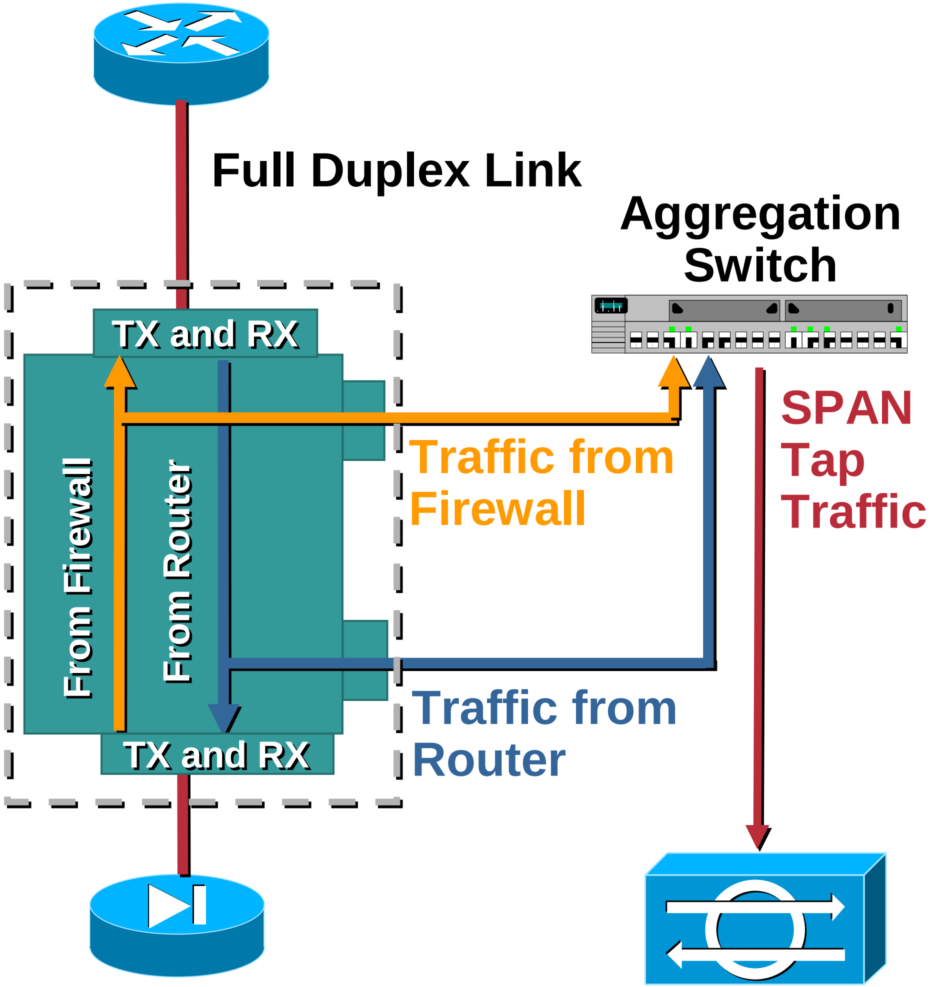
Next Steps: Getting Traffic to your Network Sensors

- Traffic must be mirrored to network sensors (replicated)
- Choices:
  - Shared media (hubs)
  - Network taps
  - Switch-based traffic mirroring (SPAN)
  - Selective mirroring (traffic capture—VACLs)

Using a Network Tap

- Tap splits full duplex link into two streams
- For sensors with only one sniffing interface, need to aggregate traffic to one interface
- Be careful of aggregate bandwidth of two tapped streams

  Don’t exceed SPAN port or sensor capacity



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't handle multi-VLAN traffic
    - http://www.cisco.com/warp/public/473/41.html
- **Rule-Based Capture: VLAN 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
    - http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/idsm/idsm_2/13074_03.htm

Switch-Based Traffic Capture Example

Using SPAN

```
switch>(enable) set span 4/5 6/1 rx create
switch>(enable) set span 401 6/1 rx create
```

- Sets port 5 on module 4 and VLAN 401 to span to the monitoring port on the IDS Module in slot 6

Using VACL

```
switch>(enable) set security acl ip WEBONLY
                 permit tcp any any eq 80 capture
switch>(enable) set security acl ip WEBONLY
                 permit tcp any eq 80 any capture
switch>(enable) commit security acl WEBONLY
switch>(enable) set security acl map WEBONLY 401
switch>(enable) set security acl capture-ports 6/1
```

- Captures web traffic on VLAN 401 only, and sends the captured traffic to the monitoring port on the IDS Module in slot 6

Additional Deployment Considerations: Organizational Issues

- **As with all security technologies, it is critical to have a robust security policy**
- **Intrusion Detection technologies cross many different business functions:**
  - **IT Security—Policy, deployment, monitoring**
  - **Networking—Traffic direction, active response**
  - **Server Admins—installation, maintenance**
    - **Who determines how/where to connect sensors on the network? Install new agents?**
    - **Switch configuration considerations, tap considerations, management considerations**

Incident Response: Policies and Procedures

- Security policy must also address incident response
  - Must be approved by senior management
- Must address containment/recovery procedures
  - Which areas do you respond to first?
  - When do you start severing connections?
  - Under what circumstances do you notify senior management?
  - Under what circumstances do you engage law enforcement (if ever)?

Incident Response: Responding to an Intrusion

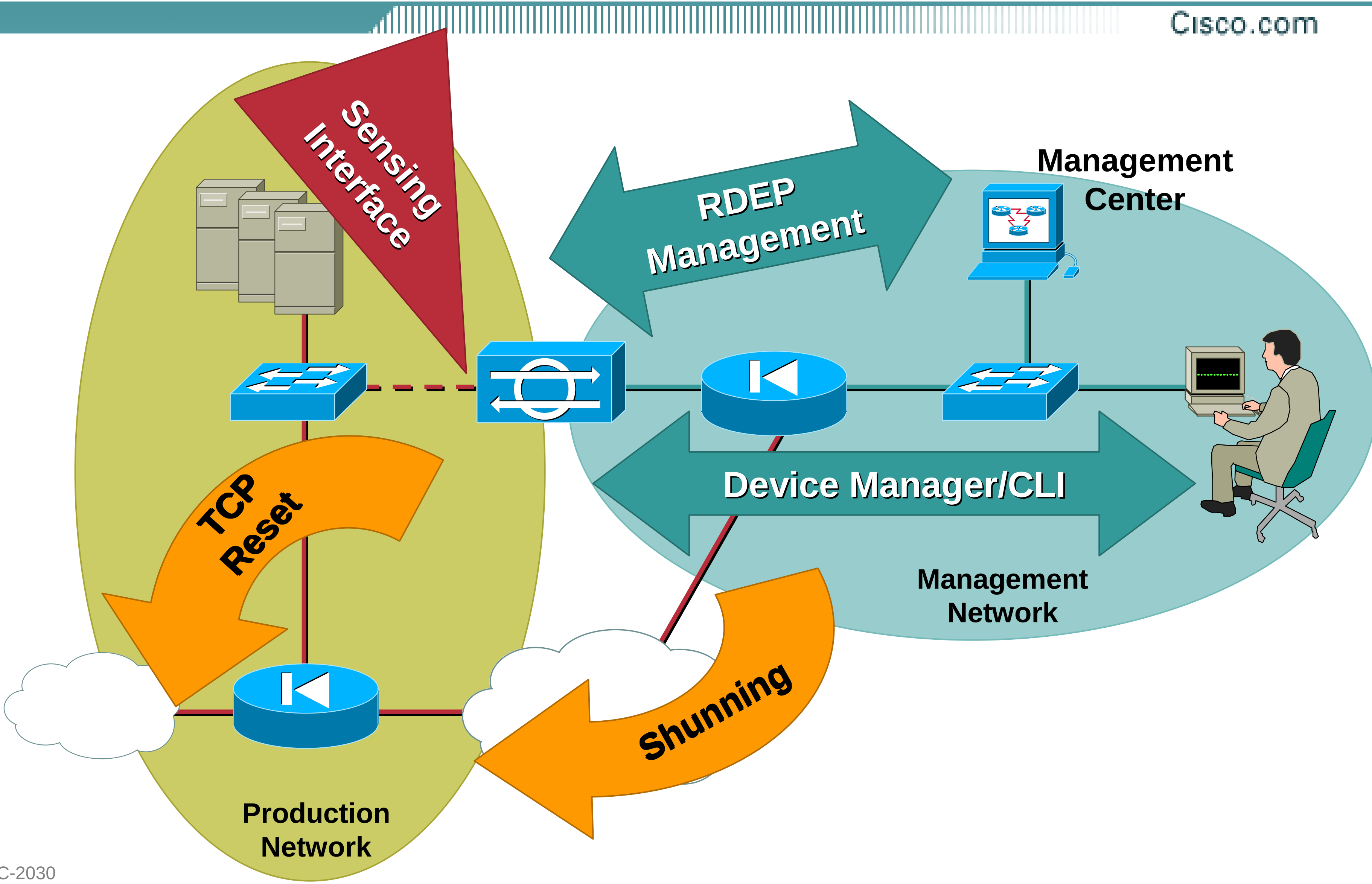
- Following investigation and alarm validation, an appropriate triage solution is put in place
- It is important to understand that this is not the end of the incident life cycle
  - A root cause analysis must be performed
  - A long term fix must be implemented
  - The IDS policy and security policy in general must be updated as appropriate

Network Sensors

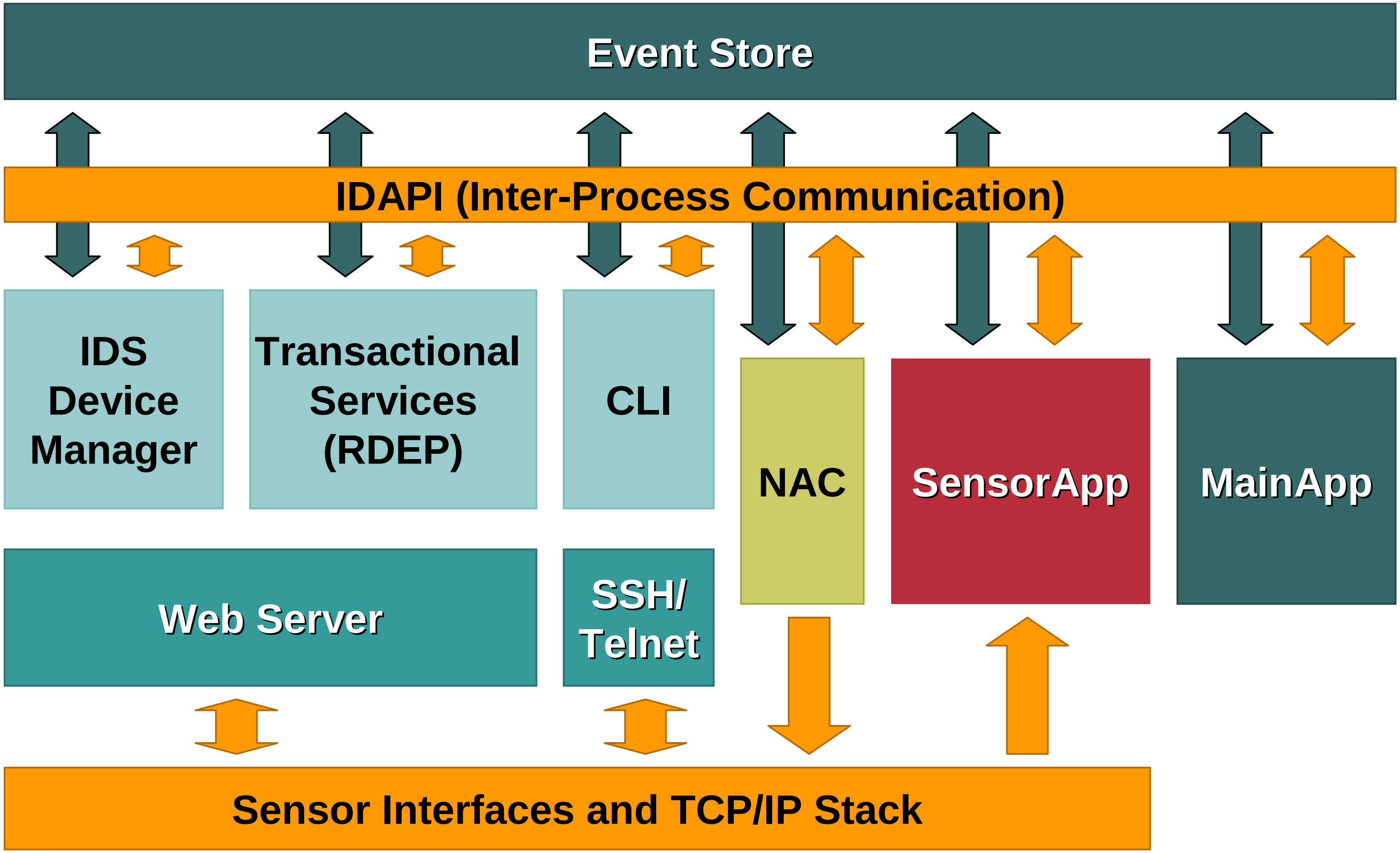
Agenda

- Sensor Architecture
- RDEP
- Sensor App and Micro-Engines
- Signature Analysis
- Environment-Based Tuning
- Active Response
- Cisco Threat Response

Sensor Architecture: The Big Picture



Sensor Architecture: The Details


Event Store
IDAPI (Inter-Process Communication)
IDS Device Manager
Transactional Services (RDEP)
CLI
NAC
SensorApp
MainApp
Web Server
SSH/ Telnet
Sensor Interfaces and TCP/IP Stack

Sensor Architecture: The Components

- **Sensor Interfaces:**

  Traffic inspection points

- **SensorApp:**

  “Sniffing” application

- **MainApp:**

  Core IDS application

- **Event Store:**

  Storage for all events (system and alarm)

- **IDAPI:**

  Communication channel between applications

- **Web Server:**

  Services all web and SSL requirements, including the IDS Device Manager (the integrated GUI), and transactional services such as remote management and monitoring through RDEP

- **SSH/Telnet:**

  Services SSH and telnet requirements, for the CLI application

- **NAC:**

  Application for active response (shunning)

Event and Alarm Communication: RDEP

- RDEP: Remote Data Exchange Protocol

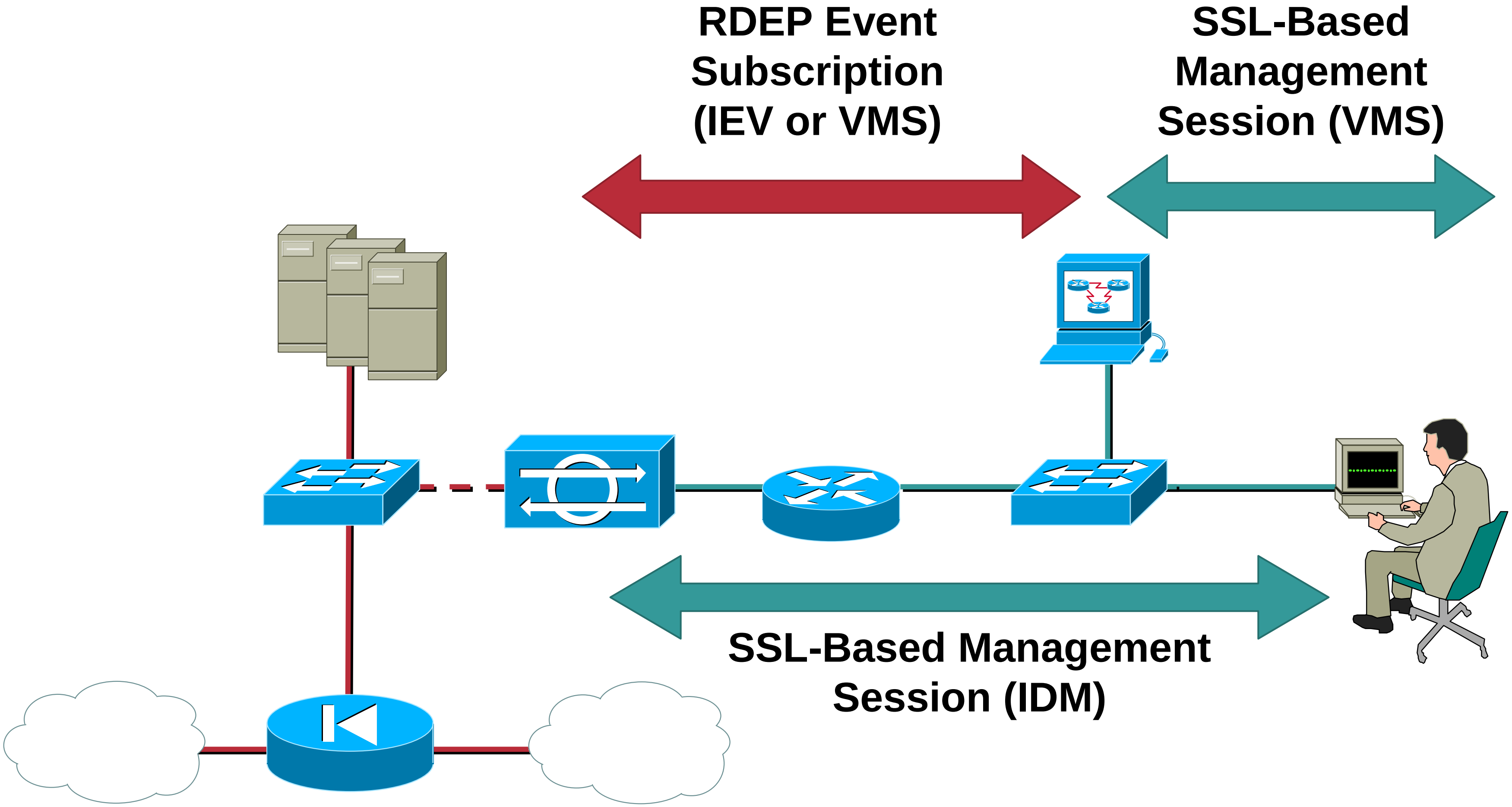
  XML-based communications protocol between sensors and management apps

  Encrypted using SSL

  Event and transaction message entity bodies consist of XML documents

- Used by both IDS Event Viewer (small IDS deployments) and VMS/Security Monitor (large IDS deployments)

RDEP in Action

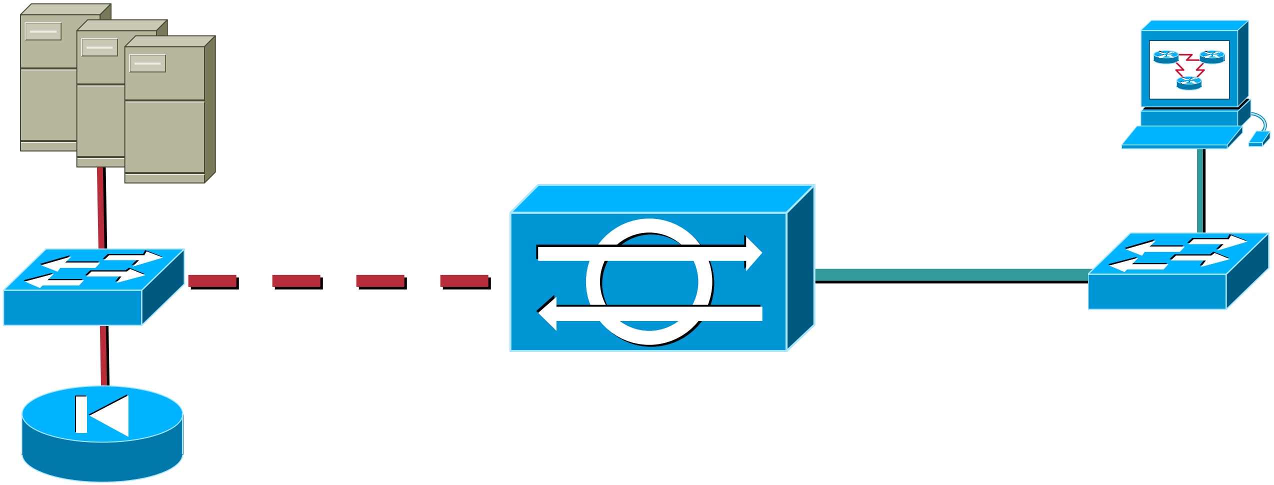


RDEP Event Subscription (IEV or VMS)

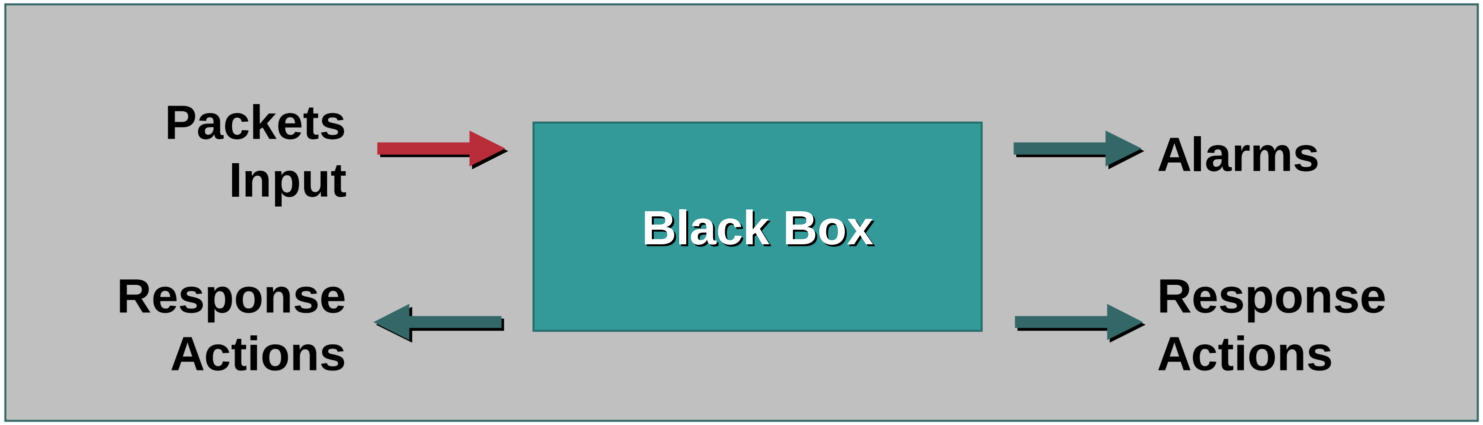
SSL-Based Management Session (VMS)

SSL-Based Management Session (IDM)

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



Inputs and Outputs:



Packets Input

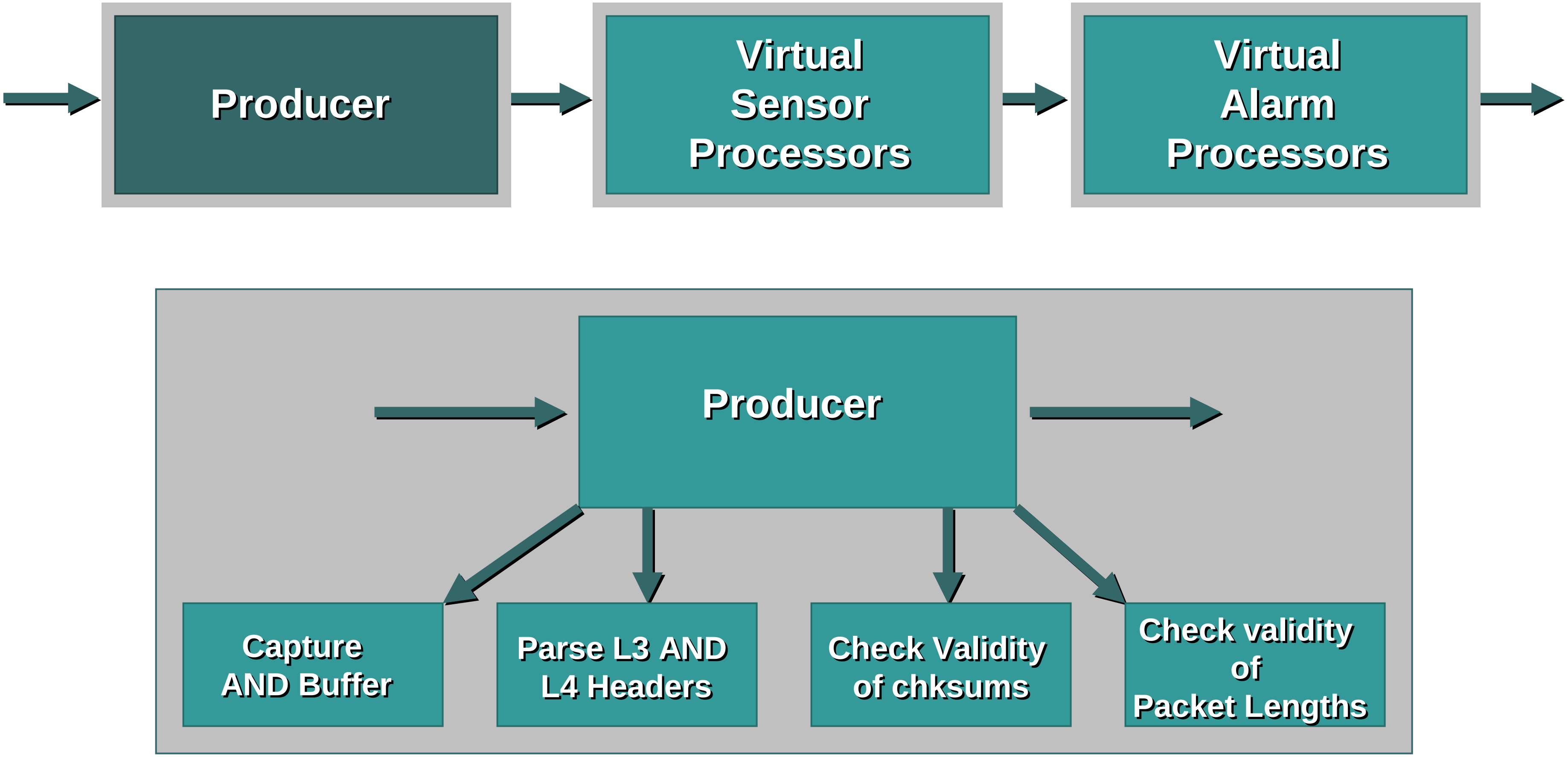
Response Actions

Black Box

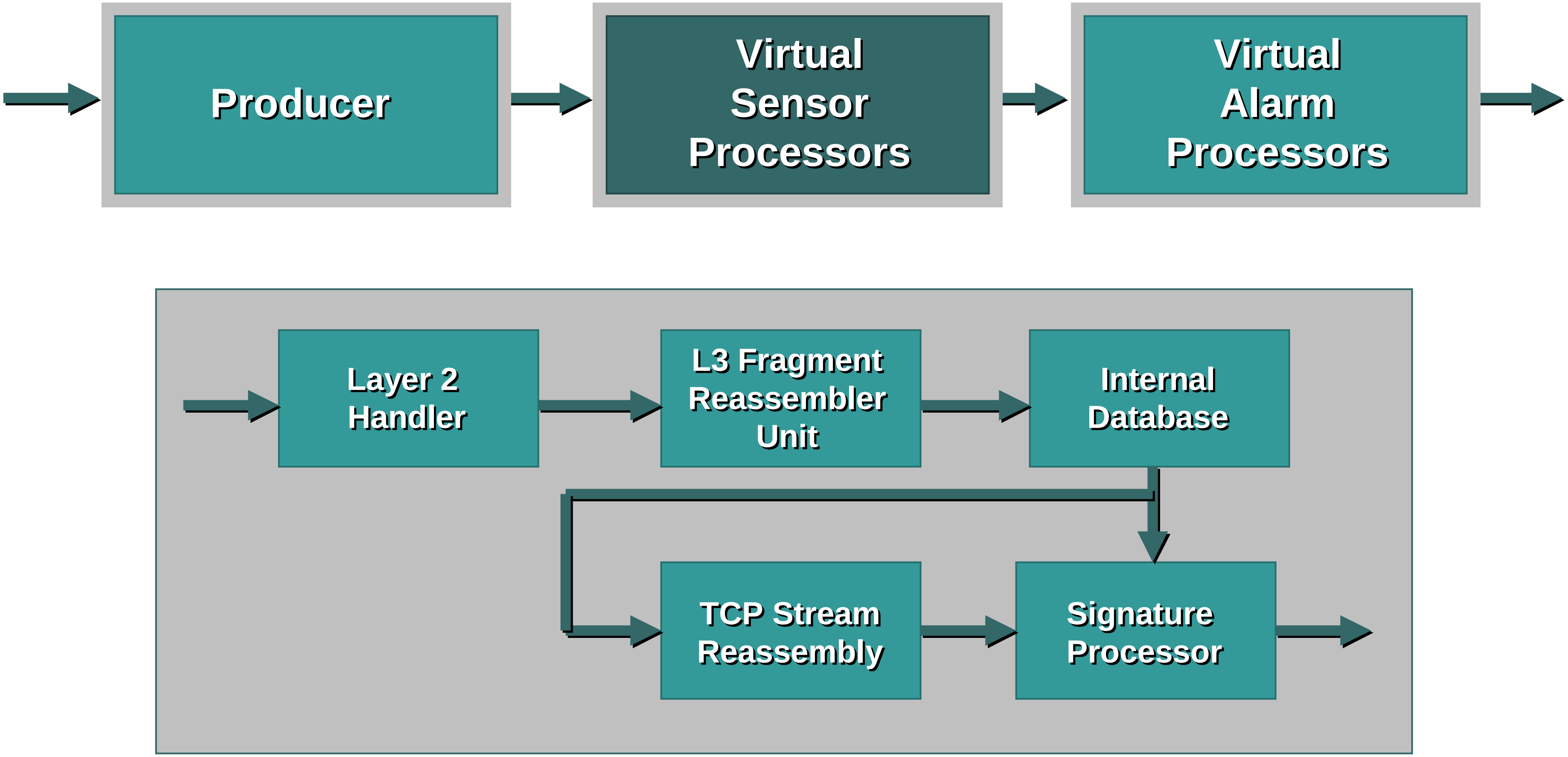
Alarms

Response Actions

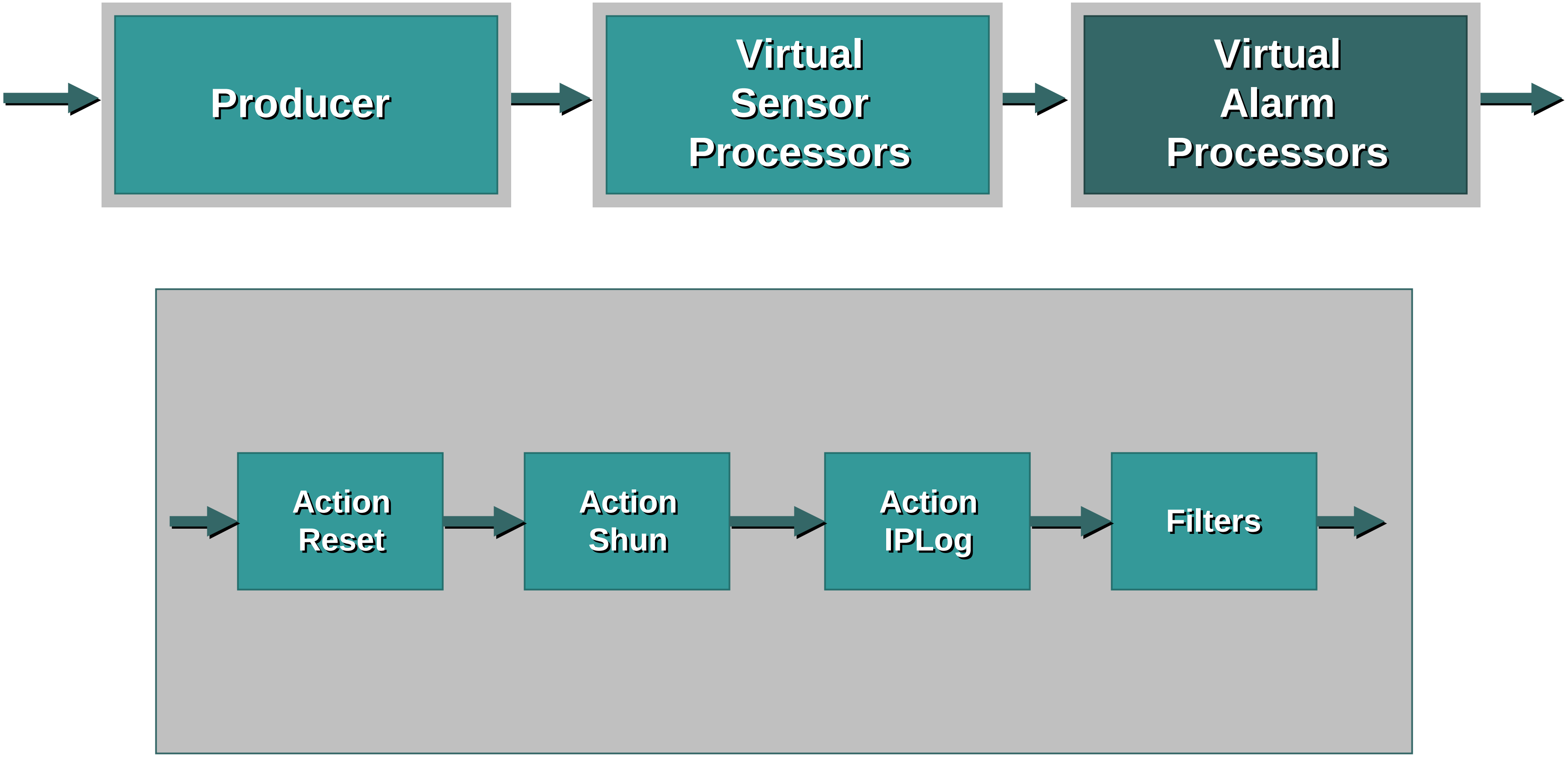
Network Sensor Packet Analysis: The Producer


Producer
Virtual Sensor Processors
Virtual Alarm Processors
Producer
Capture AND Buffer
Parse L3 AND L4 Headers
Check Validity of chksums
Check validity of Packet Lengths

Network Sensor Packet Analysis: Virtual Sensor Processors



Network Sensor Packet Analysis: Virtual Alarm Processors



Signatures Redux

- 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

- Heuristics

  e.g. Rate of inbound SYNs—SYN flood?

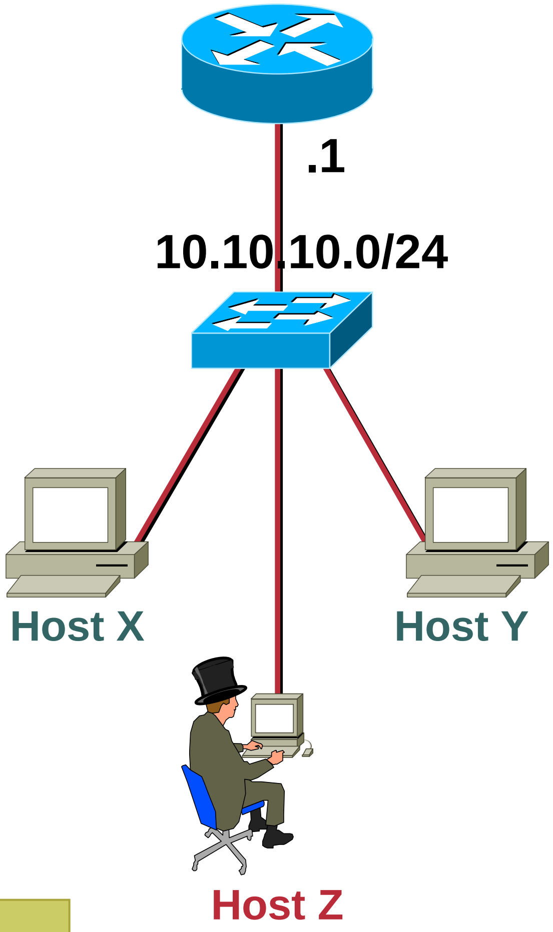
Scaling Analysis: Sensor Micro-Engines

- Traffic analysis is incredibly computationally intensive with large numbers of signatures
- Cisco IDS analysis implemented with a series of micro-engines
- Micro-Engine Types:

  ATOMIC
  FLOOD
  OTHER
  SERVICE
  STATE.STRING
  STRING
  SWEEP
  SYSLOG
  TROJAN

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

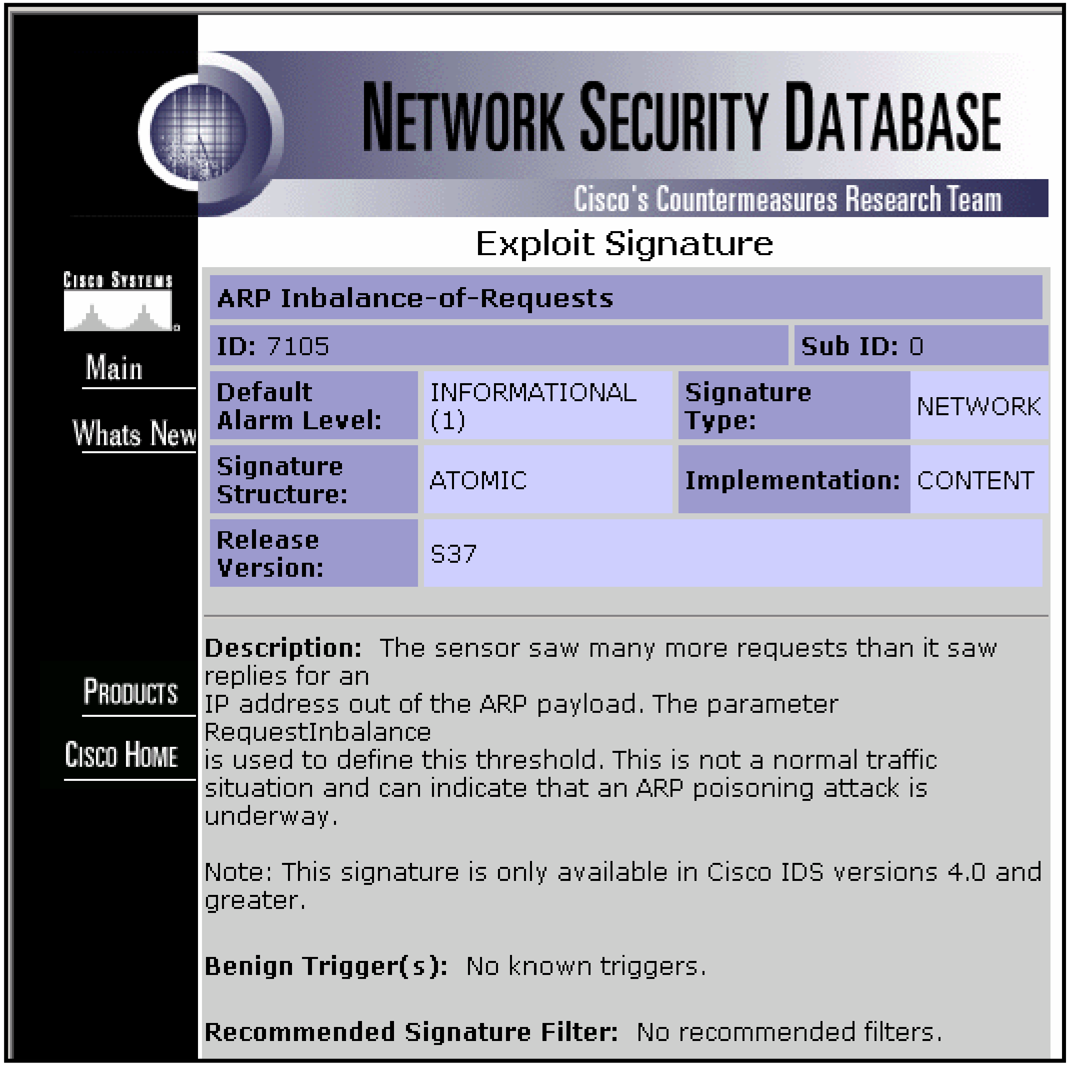
- **Host Z is a malicious user, attempting to gain access to traffic from Hosts X and Y**
- **Host Z sends gratuitous ARP replies, telling all that he is 10.10.10.1 (router), with his MAC address**
- **Since ARP replies are broadcast, all hosts on the same L2 subnet see and accept the gratuitous ARP**
- **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**


Network Security Database
Cisco's Countermeasures Research Team
Cisco Systems
Main
Whats New
Products
Cisco Home

Exploit Signature

ARP Inbalance-of-Requests			
ID: 7105		**Sub ID:** 0	
Default Alarm Level:	INFORMATIONAL (1)	**Signature Type:**	NETWORK
Signature Structure:	ATOMIC	**Implementation:**	CONTENT
Release Version:	S37		

Description: The sensor saw many more requests than it saw replies for an IP address out of the ARP payload. The parameter RequestInbalance is used to define this threshold. This is not a normal traffic situation and can indicate that an ARP poisoning attack is underway.

Note: This signature is only available in Cisco IDS versions 4.0 and greater.

Benign Trigger(s): No known triggers.

Recommended Signature Filter: No recommended filters.

Signature Updates

- Much like anti-virus, network IDS's must be kept up to date
- Process must be developed to rapidly update new signatures as released
- Cisco releases regular updates, along with critical updates for major events (e.g. Slammer)

http://www.cisco.com/warp/public/779/largeent/it/ids_news/subscribe.html

Tuning Your Sensors

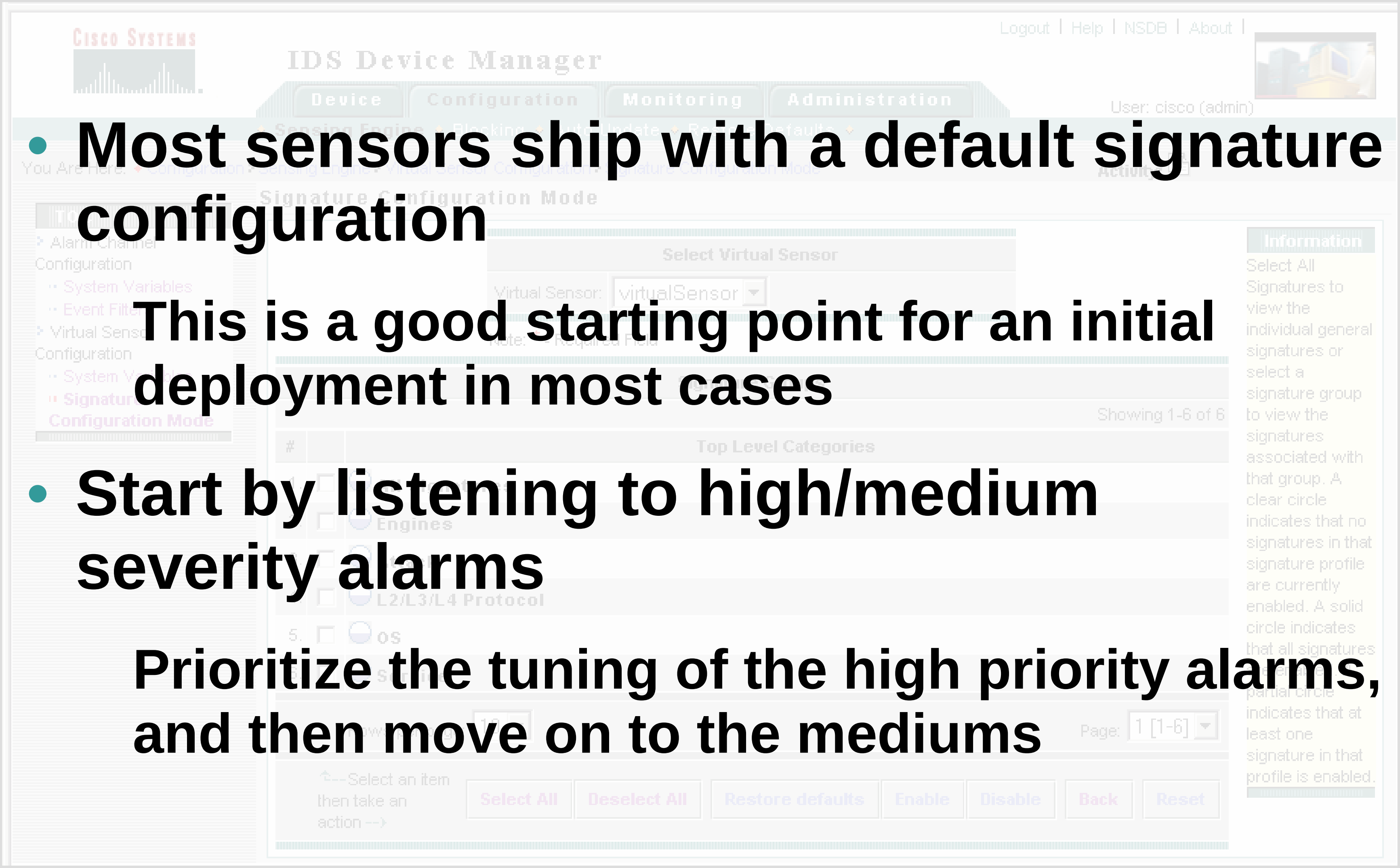
- Tuning is the most important part of intrusion detection deployment

  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



Select All Signatures to view the individual general signatures or select a signature group to view the signatures associated with that group. A clear circle indicates that no signatures in that signature profile are currently enabled. A solid circle indicates that all signatures are enabled. A partial circle indicates that at least one signature in that profile is enabled.

- **Most sensors ship with a default signature configuration**

  This is a good starting point for an initial deployment in most cases

- **Start by listening to high/medium severity alarms**

  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
- MinHits: number of events to see before alarm
- Severity: what level of alarm to send
- Alarm Aggregation: how many alarms to send
  - Alarm Throttle: Summarization characteristics
  - Alarm Interval: Summarization window
  - Choke Threshold: High water mark to force summary
- Actions: what to do following an alarm

Customizing Your Signatures

- 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

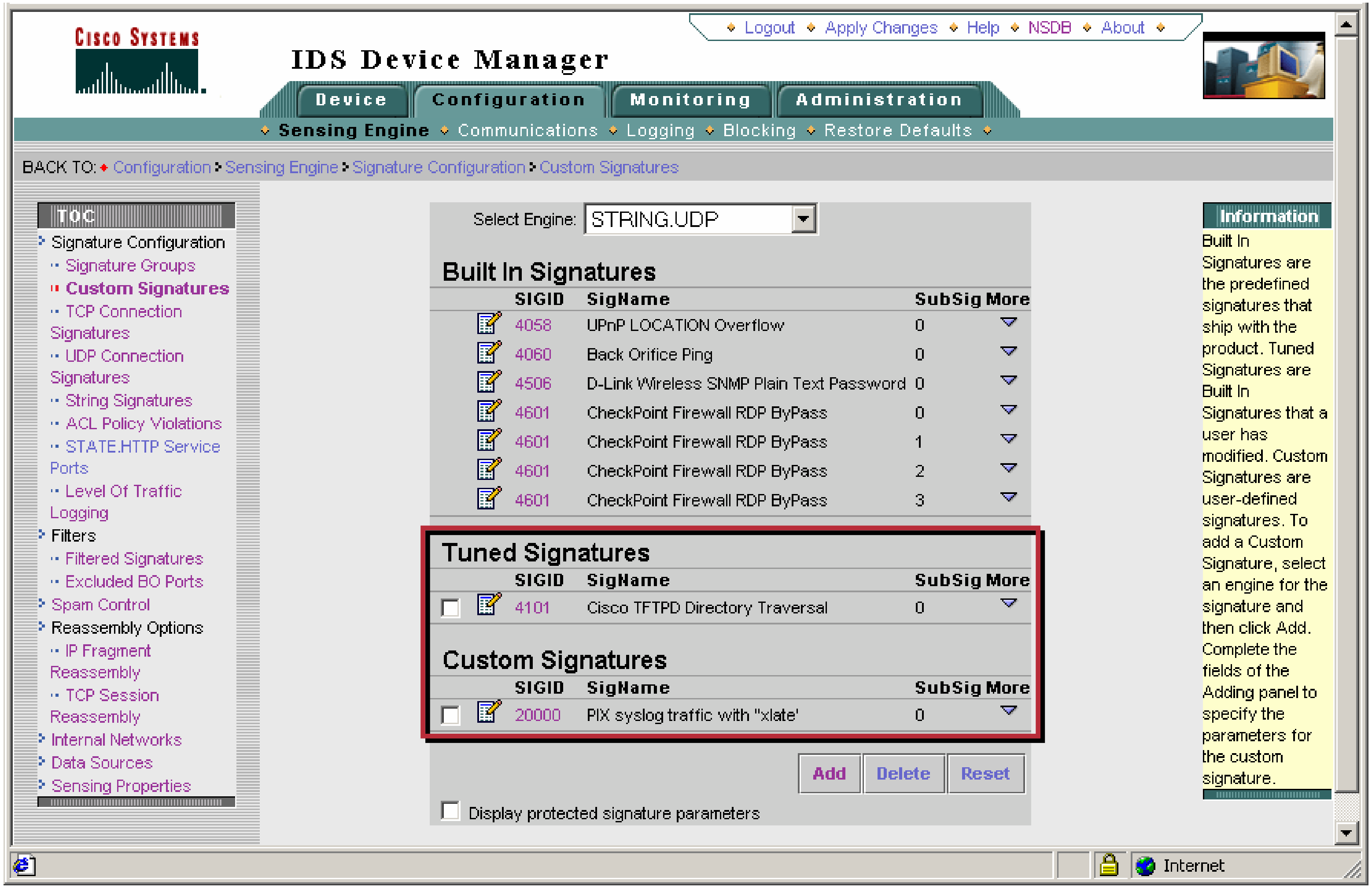
- Signature customization is not trivial

  Writing signatures requires detailed knowledge of attack "loose" signatures will generate false positives and mistakes might result in false negatives

  Test, test and test again before you deploy

Custom Signatures

Choose Configuration> Sensing Engine> Signature Configuration> Custom Signatures



Select Engine: STRING.UDP

Built In Signatures

SIGID	SigName	SubSig	More
4058	UPnP LOCATION Overflow	0	▽
4060	Back Orifice Ping	0	▽
4506	D-Link Wireless SNMP Plain Text Password	0	▽
4601	CheckPoint Firewall RDP ByPass	0	▽
4601	CheckPoint Firewall RDP ByPass	1	▽
4601	CheckPoint Firewall RDP ByPass	2	▽
4601	CheckPoint Firewall RDP ByPass	3	▽

Tuned Signatures

	SIGID	SigName	SubSig	More
□	4101	Cisco TFTPD Directory Traversal	0	▽

Custom Signatures

	SIGID	SigName	SubSig	More
□	20000	PIX syslog traffic with "xlate'	0	▽

Add | Delete | Reset

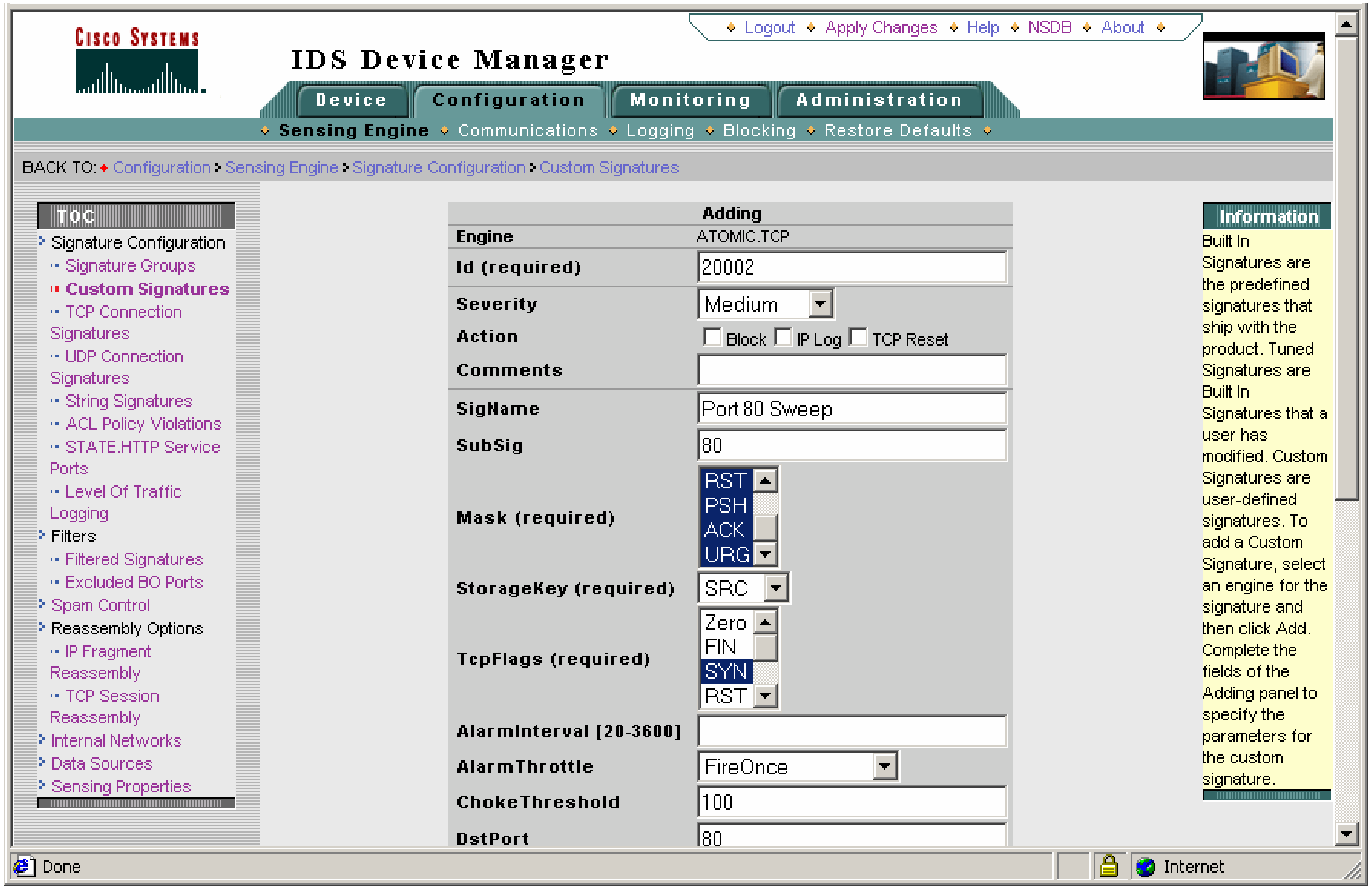
□ Display protected signature parameters

Information

Built In Signatures are the predefined signatures that ship with the product. Tuned Signatures are Built In Signatures that a user has modified. Custom Signatures are user-defined signatures. To add a Custom Signature, select an engine for the signature and then click Add. Complete the fields of the Adding panel to specify the parameters for the custom signature.

Example: Port 80 Sweeps

Choose Configuration> Sensing Engine> Signature Configuration> Custom Signatures



BACK TO: Configuration > Sensing Engine > Signature Configuration > Custom Signatures

Adding

Engine	ATOMIC.TCP
Id (required)	20002
Severity	Medium
Action	□ Block □ IP Log □ TCP Reset
Comments	
SigName	Port 80 Sweep
SubSig	80
Mask (required)	RST PSH ACK URG
StorageKey (required)	SRC
TcpFlags (required)	Zero FIN SYN RST
AlarmInterval [20-3600]	
AlarmThrottle	FireOnce
ChokeThreshold	100
DstPort	80

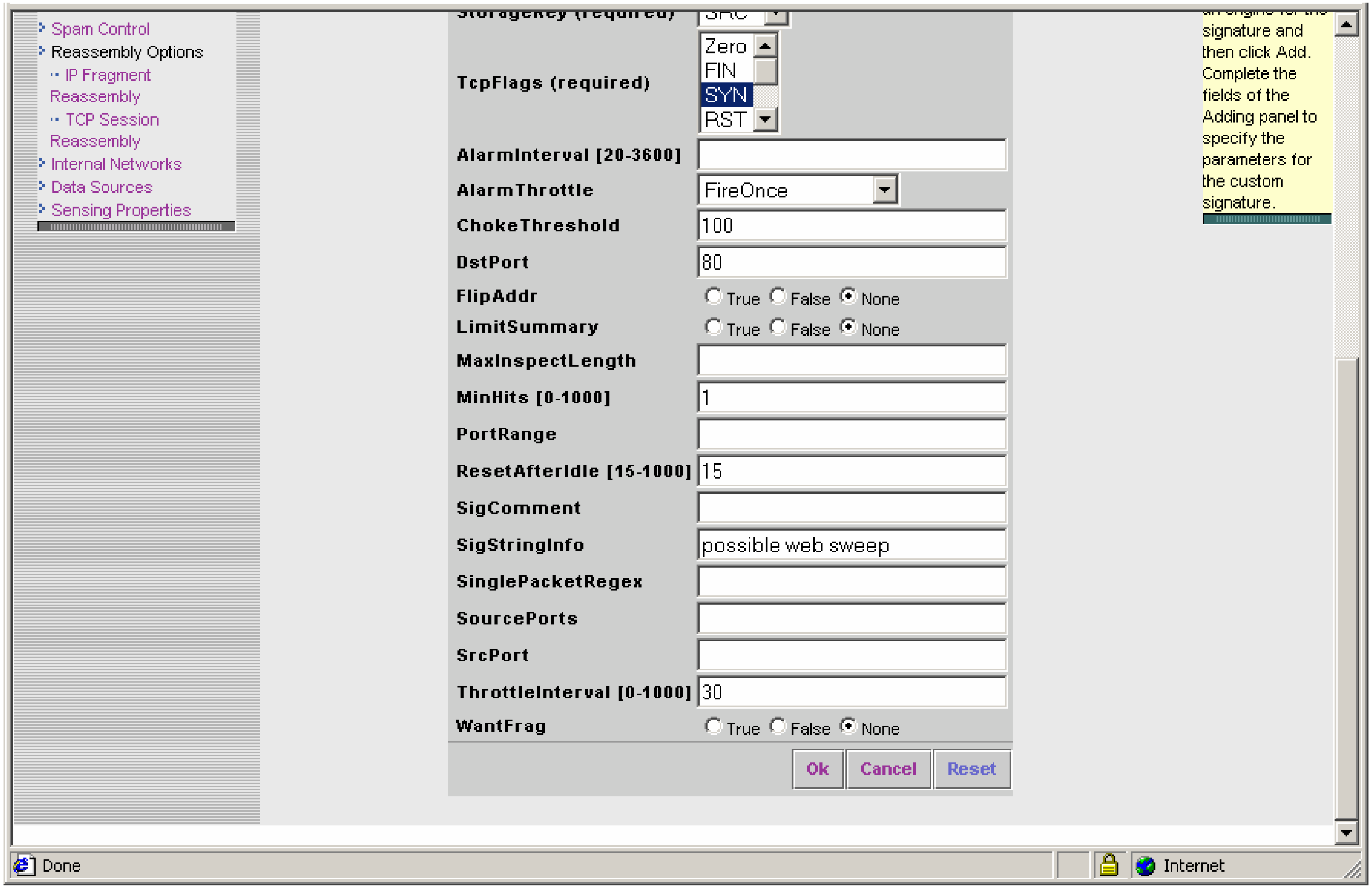
Information

Built In Signatures are the predefined signatures that ship with the product. Tuned Signatures are Built In Signatures that a user has modified. Custom Signatures are user-defined signatures. To add a Custom Signature, select an engine for the signature and then click Add. Complete the fields of the Adding panel to specify the parameters for the custom signature.

SEC-2030
8175_05_2003_c1

Port 80 Sweeps (Cont.)

Cisco.com



StorageKey (required)	SRC
TcpFlags (required)	Zero FIN SYN RST
AlarmInterval [20-3600]	
AlarmThrottle	FireOnce
ChokeThreshold	100
DstPort	80
FlipAddr	○ True ○ False ● None
LimitSummary	○ True ○ False ● None
MaxInspectLength	
MinHits [0-1000]	1
PortRange	
ResetAfterIdle [15-1000]	15
SigComment	
SigStringInfo	possible web sweep
SinglePacketRegex	
SourcePorts	
SrcPort	
ThrottleInterval [0-1000]	30
WantFrag	○ True ○ False ● None

signature and then click Add. Complete the fields of the Adding panel to specify the parameters for the custom signature.

Active Response

- **Promiscuous IDS’s allow a number of response actions to be taken when an alert is generated:**

  IP session logging

  TCP resets

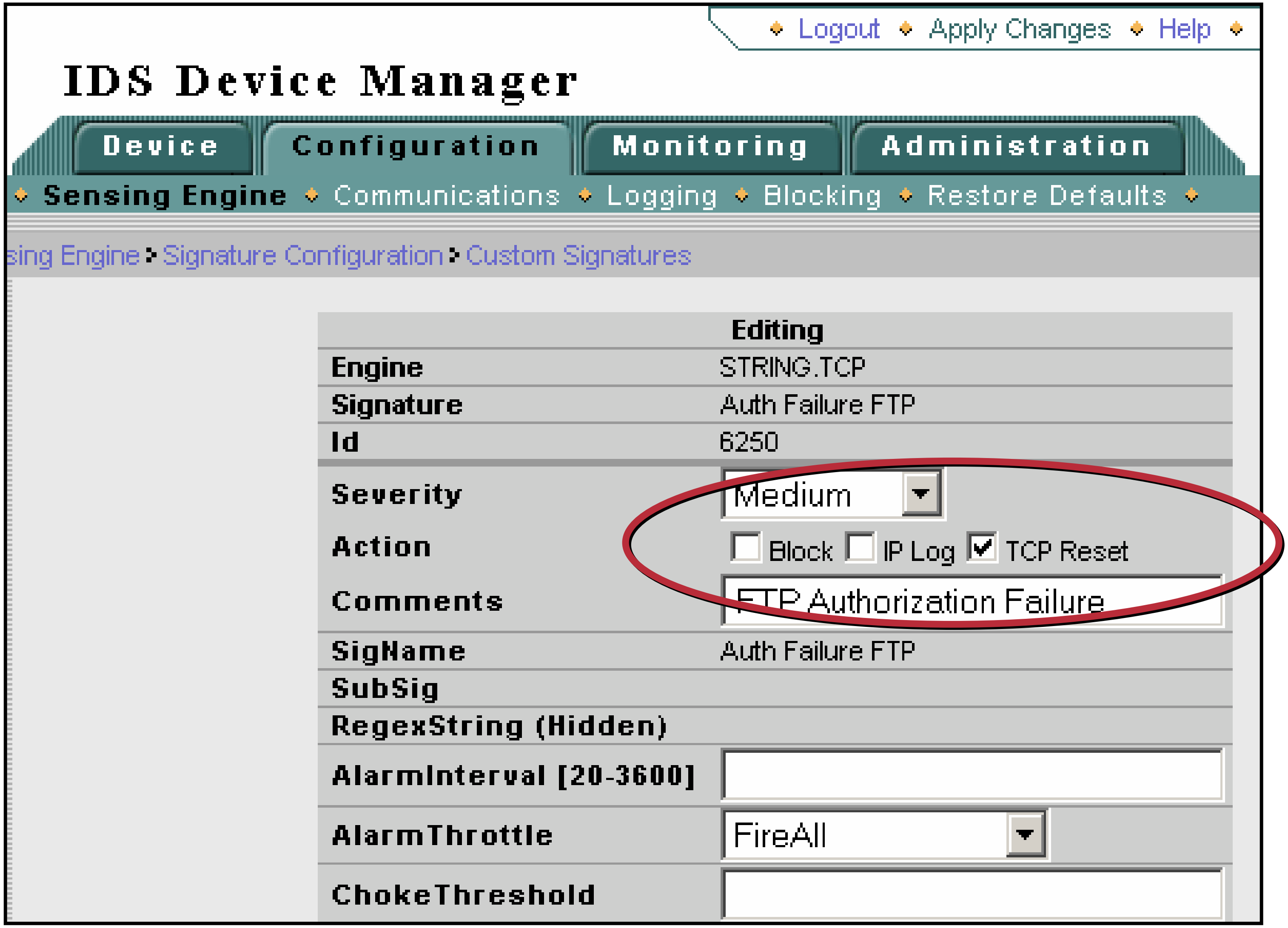
  Shunning/blocking

→ False Positives Can Be Problematic ←

→ Actions Configurable per Signature ←

Configuring Response Actions

Choose Configuration> Sensing Engine> Signature Configuration> Custom Signatures



Editing	
Engine	STRING.TCP
Signature	Auth Failure FTP
Id	6250
Severity	Medium
Action	□ Block □ IP Log ☑ TCP Reset
Comments	FTP Authorization Failure
SigName	Auth Failure FTP
SubSig	
RegexString (Hidden)	
AlarmInterval [20-3600]	
AlarmThrottle	FireAll
ChokeThreshold	

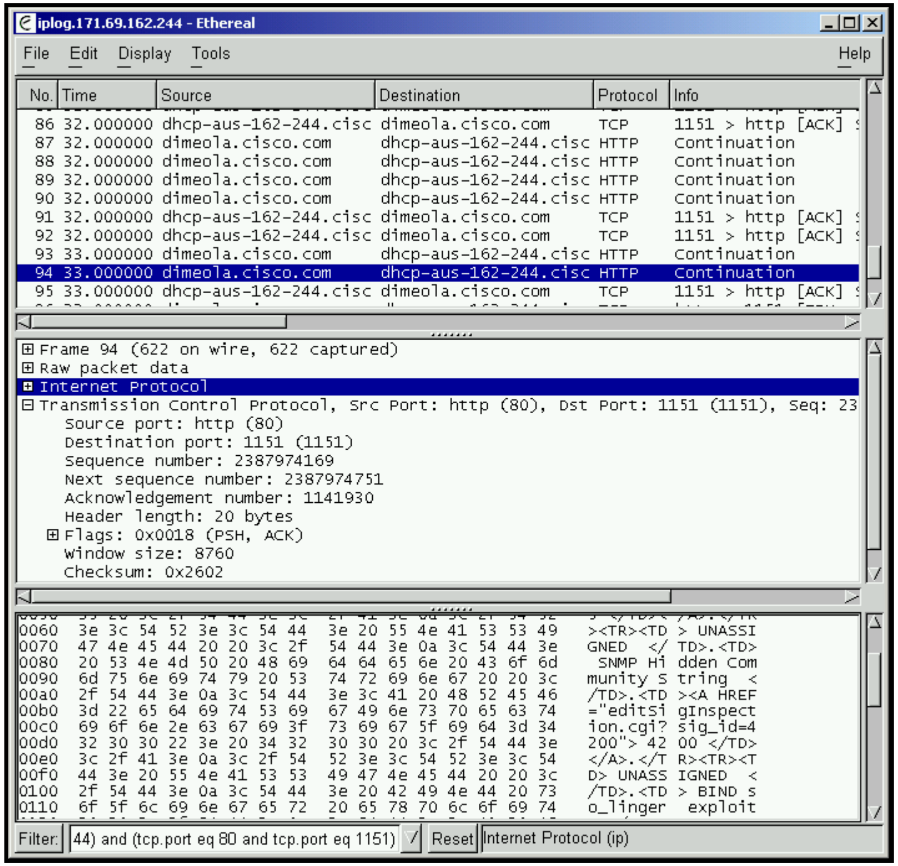
IP Session Logging

- **Logs traffic associated with a signature trigger (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



```
No. Time      Source                 Destination            Protocol Info
 86 32.000000 dhcp-aus-162-244.cisc dimeola.cisco.com      TCP      1151 > http [ACK]
 87 32.000000 dimeola.cisco.com     dhcp-aus-162-244.cisc HTTP     Continuation
 88 32.000000 dimeola.cisco.com     dhcp-aus-162-244.cisc HTTP     Continuation
 89 32.000000 dimeola.cisco.com     dhcp-aus-162-244.cisc HTTP     Continuation
 90 32.000000 dimeola.cisco.com     dhcp-aus-162-244.cisc HTTP     Continuation
 91 32.000000 dhcp-aus-162-244.cisc dimeola.cisco.com      TCP      1151 > http [ACK]
 92 32.000000 dhcp-aus-162-244.cisc dimeola.cisco.com      TCP      1151 > http [ACK]
 93 33.000000 dimeola.cisco.com     dhcp-aus-162-244.cisc HTTP     Continuation
 94 33.000000 dimeola.cisco.com     dhcp-aus-162-244.cisc HTTP     Continuation
 95 33.000000 dhcp-aus-162-244.cisc dimeola.cisco.com      TCP      1151 > http [ACK]
```

```
⊞ Frame 94 (622 on wire, 622 captured)
⊞ Raw packet data
⊞ Internet Protocol
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port: 1151 (1151), Seq: 23
    Source port: http (80)
    Destination port: 1151 (1151)
    Sequence number: 2387974169
    Next sequence number: 2387974751
    Acknowledgement number: 1141930
    Header length: 20 bytes
  ⊞ Flags: 0x0018 (PSH, ACK)
    Window size: 8760
    Checksum: 0x2602
```

```
0060  3e 3c 54 52 3e 3c 54 44  3e 20 55 4e 41 53 53 49   ><TR><TD > UNASSI
0070  47 4e 45 44 20 20 3c 2f  54 44 3e 0a 3c 54 44 3e   GNED  </ TD>.<TD>
0080  20 53 4e 4d 50 20 48 69  64 64 65 6e 20 43 6f 6d    SNMP Hi dden Com
0090  6d 75 6e 69 74 79 20 53  74 72 69 6e 67 20 20 3c   munity S tring  <
00a0  2f 54 44 3e 0a 3c 54 44  3e 3c 41 20 48 52 45 46   /TD>.<TD ><A HREF
00b0  3d 22 65 64 69 74 53 69  67 49 6e 73 70 65 63 74   ="editSi gInspect
00c0  69 6f 6e 2e 63 67 69 3f  73 69 67 5f 69 64 3d 34   ion.cgi? sig_id=4
00d0  32 30 30 22 3e 20 34 32  30 30 20 3c 2f 54 44 3e   200"> 42 00 </TD>
00e0  3c 2f 41 3e 0a 3c 2f 54  52 3e 3c 54 52 3e 3c 54   </A>.</T R><TR><T
00f0  44 3e 20 55 4e 41 53 53  49 47 4e 45 44 20 20 3c   D> UNASS IGNED  <
0100  2f 54 44 3e 0a 3c 54 44  3e 20 42 49 4e 44 20 73   /TD>.<TD > BIND s
0110  6f 5f 6c 69 6e 67 65 72  20 65 78 70 6c 6f 69 74   o_linger  exploit
```

Filter: 44) and (tcp.port eq 80 and tcp.port eq 1151)

Session Sniping: TCP Resets

- For TCP applications, connection is prematurely terminated by a RST sent from “sniffing” interface
- Must guess correct TCP sequence number and successfully insert RST into session

  Makes TCP Resets somewhat unreliable especially when source and destination are not “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
- 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 (Not Supported on All Switches)

```
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, the RST Will Only Be Sent on the Native VLAN

Shunning/Blocking

- When signature fires, sensor inserts ACL in firewall/ router
  - Deny subsequent traffic from that source IP address
  - Note that initial trigger packets will make it to its destination
- Sensor connects to firewall and/or router from management interface
  - Need to configure authentication credentials for firewall/router
- Conclusion: Use to “buy time” until you can respond
  - Don’t use as permanent countermeasure

Alarm Validation: Cisco Threat Response

- Emerging capability in the market—automated alarm validation
- Alarm validation:
  - Make intelligent decisions on the validity of an alarm
  - Increase or decrease the severity of the alarm appropriately

THREAT RESPONSE
ATTACKS
REAL THREAT
REAL
REAL THREAT
FALSE

How Threat Response Works

- **Was the attack successful? (eliminate and escalate)**
  - Target vulnerability check (Level 1)
    - OS detection (via NMAP)
    - Detect web servers
  - Detailed system investigation of Windows targets (Level 2)
    - Registry analysis (via Win32 system calls) (i.e. service pack check)
    - File system analysis (via SMB) (i.e. capture log files)
    - Level 2 investigation requires login to target box
- **What can de done about it? (remediate)**
  - Forensic evidence retrieval
    - Includes capture of impacted files and logs

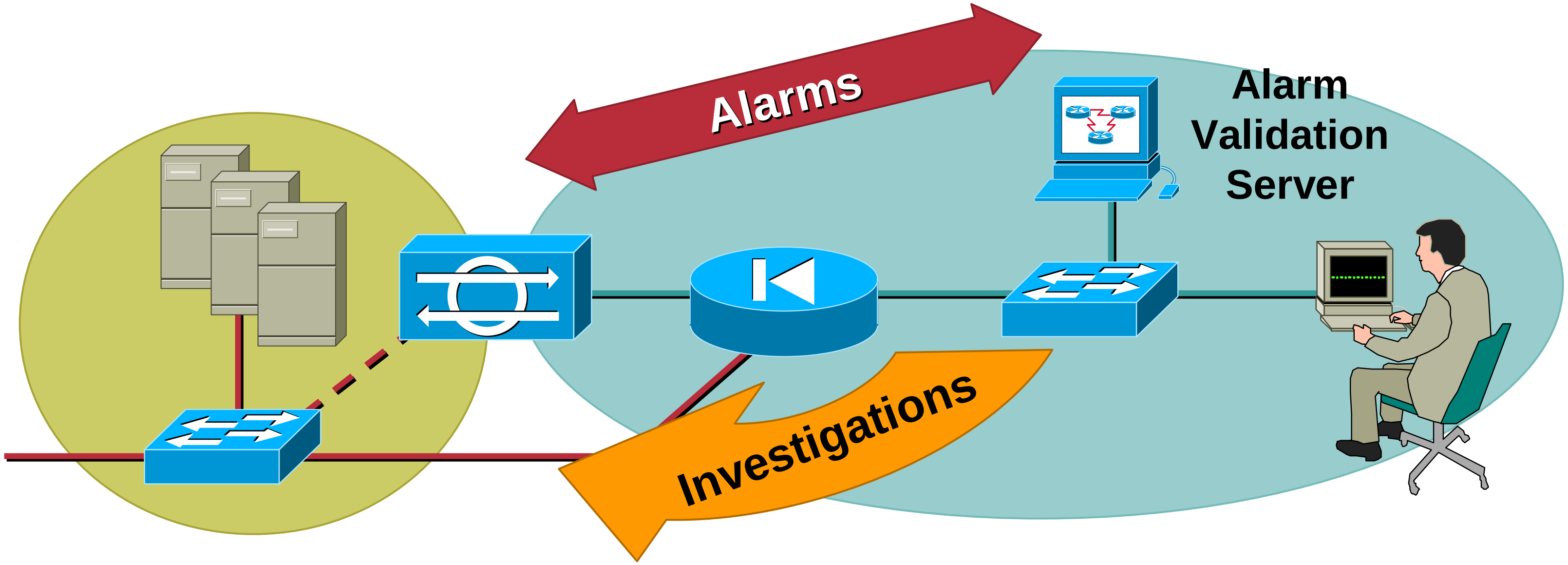
Threat Response Components

Server

- Receives alarms from monitored IDS
- Performs all investigations using agents
- Performs all storage

Client

- Browser access to the server for management and monitoring



Agents Defined

What is an agent?

- In Threat Response an agent is a built-in active or passive procedure used to investigate an attack
- Level 0 agents use rule-based analysis (preset upgrade/downgrade)
- Level 1 agents use minimum-impact methods to determine vulnerability and impact
- Level 2 agents connect to the targeted host and look for traces and indicators of a successful attack directly on the affected system

Why does this matter?

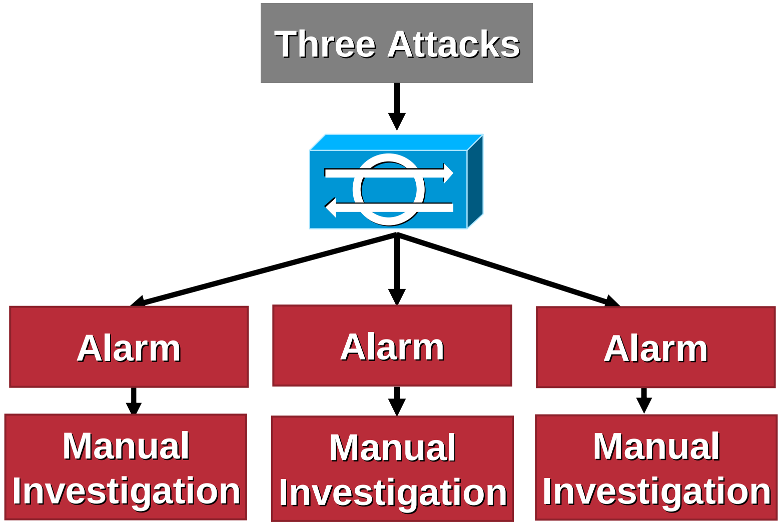
- Allows deployment with minimum install
- “Just in Time” analysis is always up to date
- Impact of the investigative agents is minimal on end hosts

Intrusion Protection w/o Validation

1. An Attacker Launches Auto-Scanner Script to Search for a Common Microsoft IIS Unicode Vulnerability

2. The IDS Sensor Reports a Number of Detected Attacks against the Servers on Your Network

3. The Security Administrator Sees Dozens of Real Attack Events on Their IDS and Correlation Screens; Time Is Wasted Investigating Each One



15 Minutes Manually Investigating Each Alarm

Total Elapsed Time = 45 Minutes

Intrusion Protection with Validation

1. An Attacker Launches Auto-Scanner Script to Search for a Common Microsoft IIS Unicode Vulnerability

2. The IDS Sensor Reports a Number of Detected Attacks against the Servers on Your Network

3. Threat Response Technology Quickly Assesses the Targeted in Real-Time without Prior Network Knowledge or Installed Remote Agent Software

Investigation Steps for Successful IIS Unicode Attack:

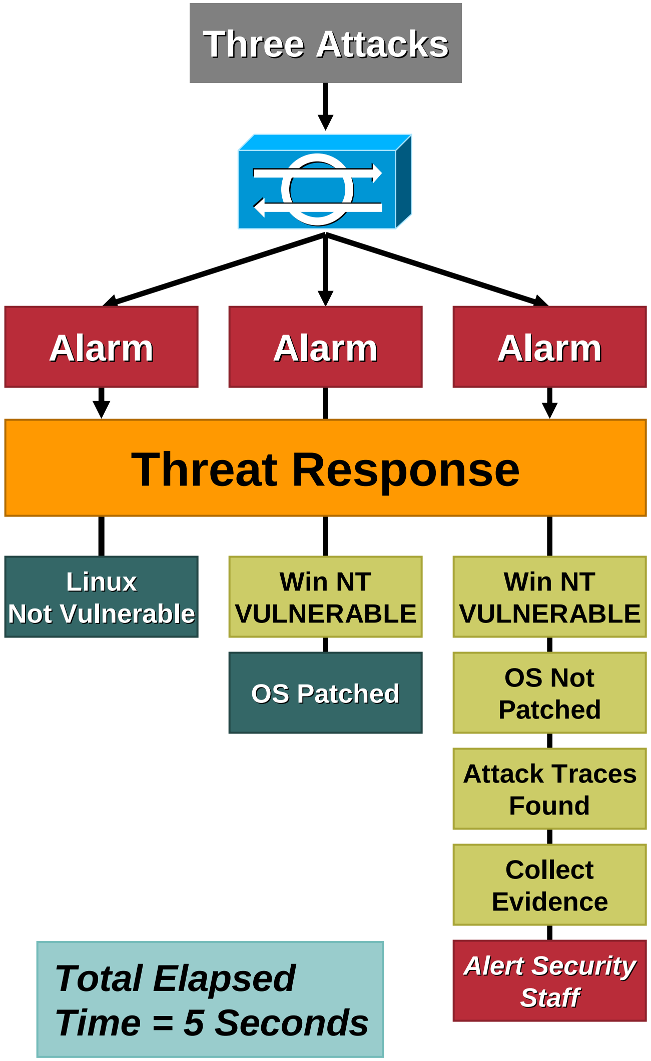
1. Does the attack target this OS type? (Level 1)

2. Is the OS vulnerable? (Level 1)

3. Are there traces of a successful attack? (Level 2)

4. Copy and secure forensic evidence (Level 2)

5. Administrator alerted to real and confirmed attack



Cisco.com

Host Agents

Agenda

- **Host Agents and the Security Architecture**

  Capabilities of a host agent

- **Cisco Security Agent Architecture**

  Policy, Rules, and Anomalies

- **Demonstration of Cisco Security Agent**

Host IDS in the Security Architecture

- Host-based agents installed on a specific host

  Can be based on behavioral/anomalies, signatures, file system integrity checking, and/or system event analysis

- Can provide:

  Event visibility and analysis

  Buffer overflow protection

  Malicious code protection

  OS lockdown

- Endpoint security: Host IDS and…

  Personal firewalls?

  Anti-virus?

Host IDS: System Level Architecture

- Agents

  Some products provide server-specific and desktop-specific agents

  Some products provide application-specific agents (such as web-server, or database)

  Agents are specific to a particular OS

- Management Console

  Required to communicate with and manage the agents

  Beginnings of correlation facilities appearing in the management stations

Cisco Security Agent Architecture

- Rules-based architecture; static and dynamic rules (behavioral)
- Composed of a set of “interceptors”

    COM Component Interceptor

    Network Application Interceptor

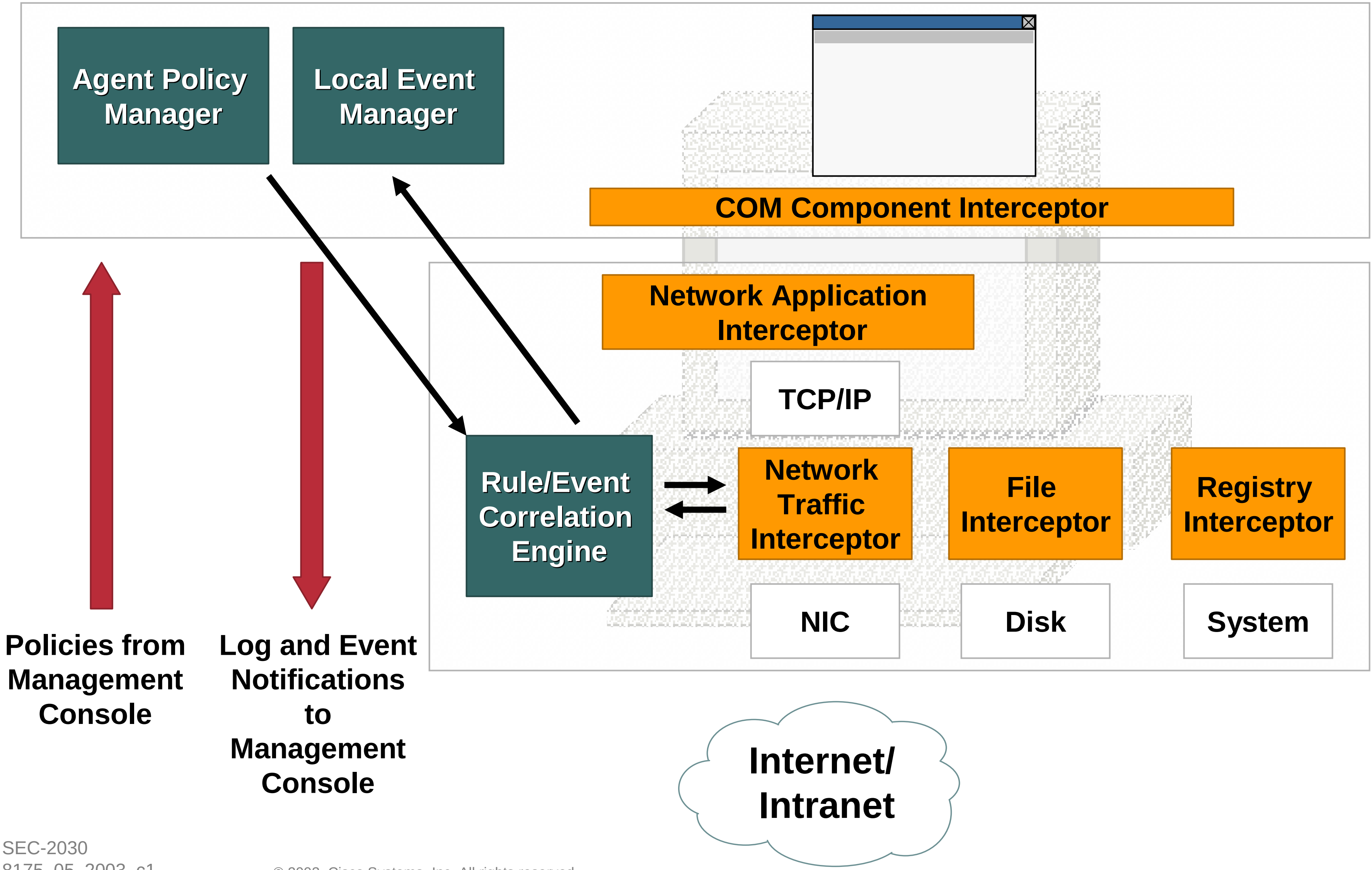
    Network Traffic Interceptor

    File Interceptor

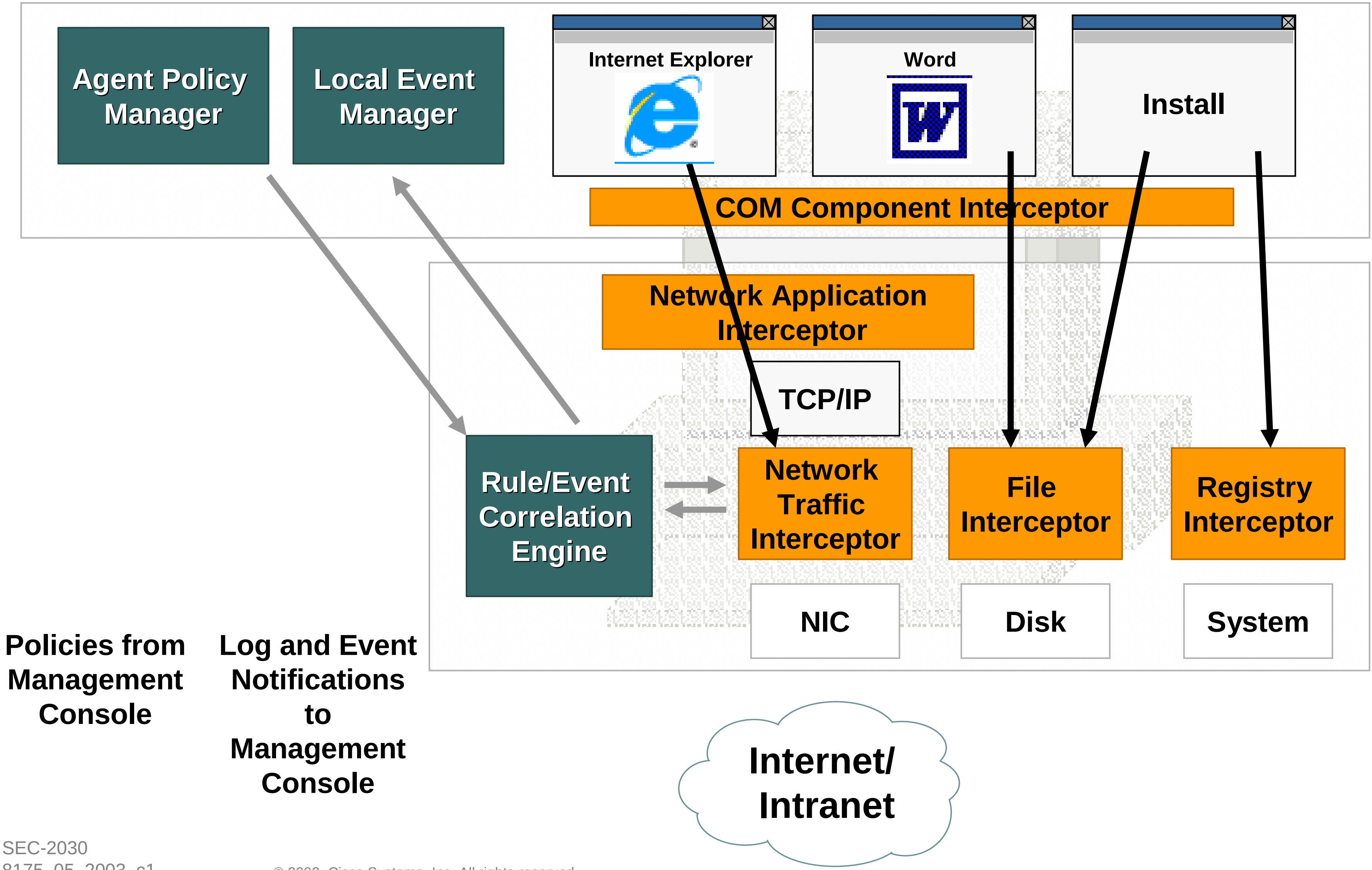
    Registry Interceptor

- Other components: Rule/Event Correlation Engine, Local Event Manager, Agent Policy Manager

Agent Architecture: Windows


Agent Policy Manager
Local Event Manager
COM Component Interceptor
Network Application Interceptor
TCP/IP
Rule/Event Correlation Engine
Network Traffic Interceptor
File Interceptor
Registry Interceptor
NIC
Disk
System
Policies from Management Console
Log and Event Notifications to Management Console
Internet/ Intranet

Agent Architecture: Windows



Policies from Management Console

Log and Event Notifications to Management Console

Agent Architecture: Rules

- Agent architecture based around a series of rules guiding behavior passing through an interceptor

  e.g. Internet Explorer is not allowed to access the memory space of Word (or any other application)—stops many buffer overflows

- A series of default rule profiles ship with the product

  90% of the time, these rule-sets are sufficient to meet a security policy requirement

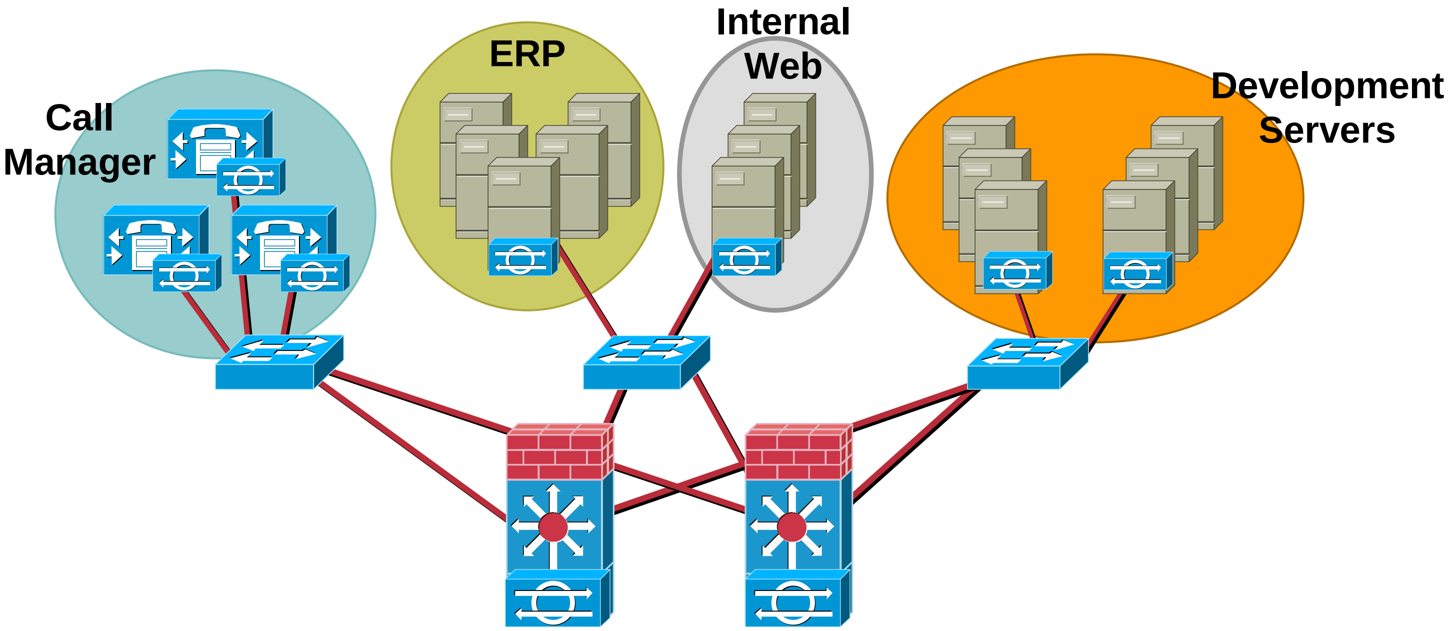
- Rules can be custom built on the management console, or “learned” through behavioral analysis

Policy Deployment on Agents: Grouping

- **Some products allow for host groupings**

  Simplifies policy deployment through grouping similar hosts into a larger policy group

- **For large scale deployments, this can be a significant benefit**



Initial Configuration and Tuning

- Initial configuration is very agent/vendor specific

  Most agents install with a default secure configuration, but check specifics

- Host agents can need tuning to specific environment, just like network sensors (particularly signature-based agents)

- Recommend using similar techniques as network sensors

  Install in environment

  Monitor for a week

  Tune signatures and responses based on results

Response Actions and Updates

- Agents can active alert on suspicious action
- In certain cases, agents can actually prevent intrusions before they occur by not allowing trigger action
- For signature-based agents: Signature response is only as current as database

  Ensure agent signature files are kept up to date

Cisco Security Agent Demonstration

Closing

Intrusion Detection in the Comfort of Your own Home…

Further Reading

- Cisco IDS product documentation
  http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/index.htm
- Cisco IDS Discussion Forum
  http://www.cisco.com/go/netpro
- Proactive Field Notices Tool for signature updates
  http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice
- Document describing SPAN functionality on Cisco switches
  http://www.cisco.com/warp/public/473/41.html
- Cisco SAFE Blueprint
  http://www.cisco.com/go/safe
- Cisco Security Advisories (includes a number of security documents)
  http://www.cisco.com/warp/public/707/advisory.html
- Vulnerability information
  http://www.cisco.com/go/csec http://www.cert.org/
  http://www.securityfocus.com http://whitehats.com
  http://www.incidents.org
- Ethereal tool to view IP Session Logs
  http://www.ethereal.com

CISCO SYSTEMS ®