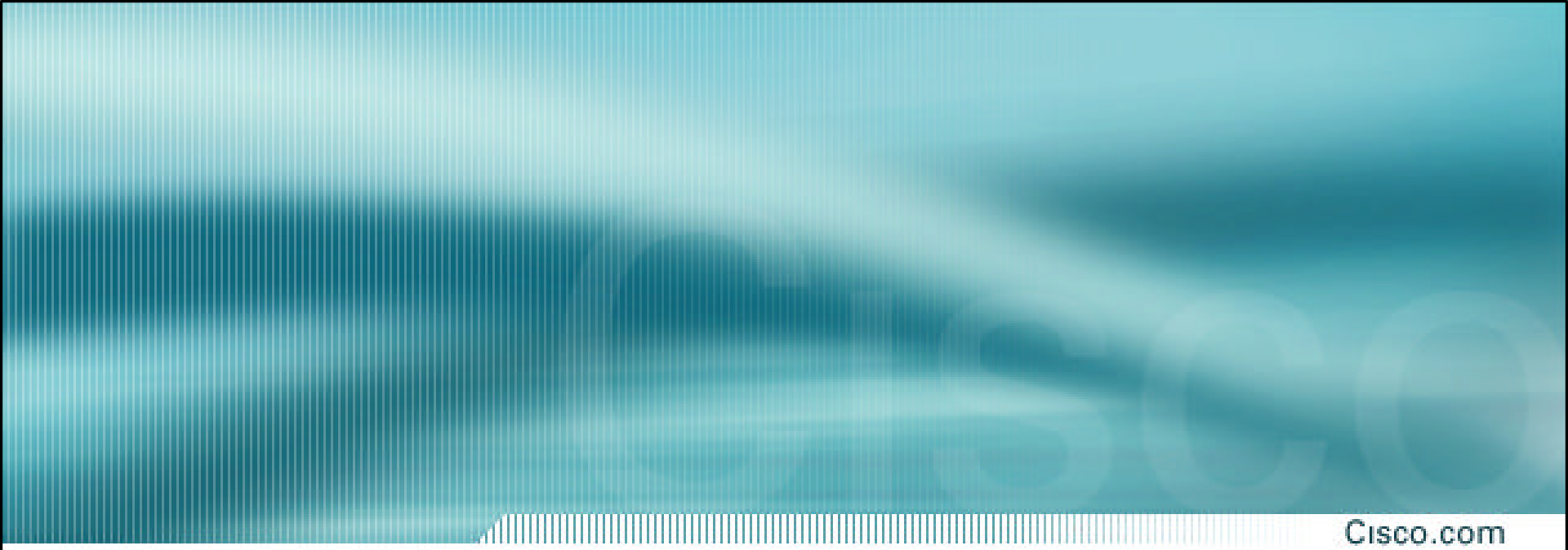


IDS 4.0 Roadshow

Module 2- Product Overview

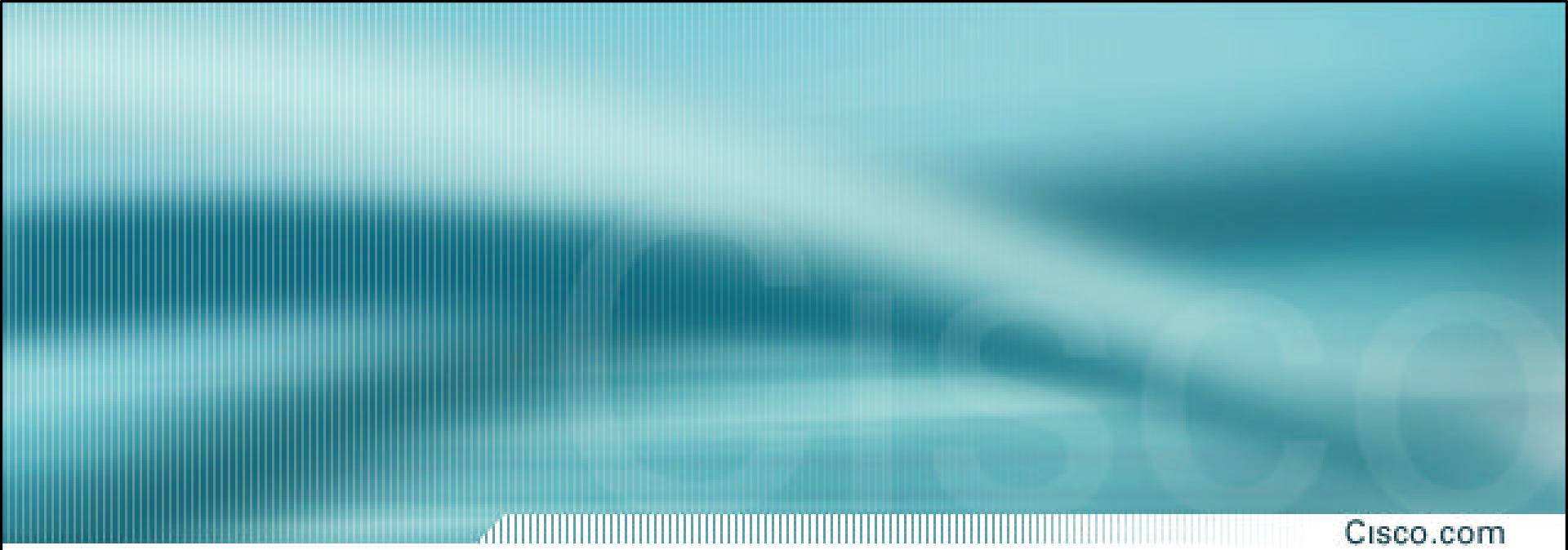
© 2003, Cisco Systems, Inc. All rights reserved.

Agenda

Cisco.com

- Network Sensor Platforms
- Host Based IDS
- Security Management
- Cisco Threat Response (CTR)
- IDS Communication
- User Accounts

© 2003, Cisco Systems, Inc. All rights reserved.



Network Sensor Platforms

© 2003, Cisco Systems, Inc. All rights reserved.

Network Sensor Features

- Active responses
  - TCP resets
  - IP session logging
  - Shunning/blocking
- Active updates
  - Regular, automated updates
  - Cisco Countermeasure's Research Team (C-CRT)
- Signature Language
  - Allowing customers to write their own signatures
- Analysis Support
  - Integrated Network Security Database

C-CRT

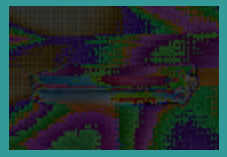
NSDB

© 2003, Cisco Systems, Inc. All rights reserved.

Cisco IDS Deployment Options

Cisco.com

Solution Breadth

Network Sensor		New 4215	4235	4250	4250-XL	
Switch Sensor		IDSM-2				
Network Module		New 2600XM	2691	3660	3725	3745
Router Sensor		800	1700	2600	3600	7x00
Firewall Sensor		501	506E	515E	525	535

© 2003, Cisco Systems, Inc. All rights reserved.

Router Sensor IOS-IDS

- Router and switch-integrated intrusion detection technology targeted at lower risk environments
- Software: IOS 12.0(5)T+
- Platforms: 1700, 2600, 3600, 7100, 7200, and 7500 routers; Catalyst 5000 RSM
- Signatures: 100
- Syslog or PostOffice alarming
- Responses: drop and reset

© 2003, Cisco Systems, Inc. All rights reserved.

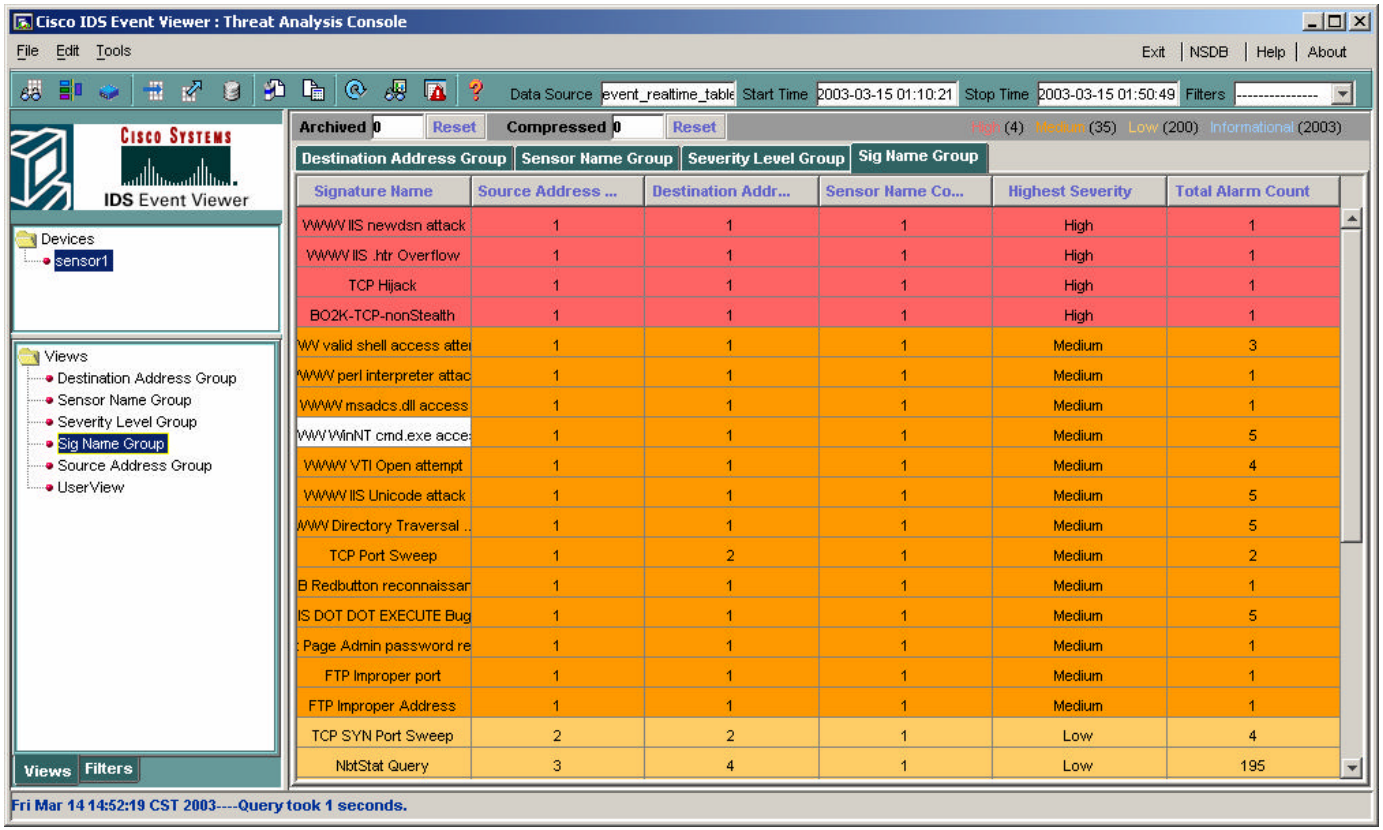
Firewall Sensor
Pix Firewall IDS

- Firewall integrated intrusion detection technology targeted at lower risk environments
- Software: PIX Firewall v5.2+
- Platforms: 506E, 515E, 525, and 535
- Signatures: 57
- Syslog alarming
- Responses: drop and reset

© 2003, Cisco Systems, Inc. All rights reserved.

Sensor Device Management Products (cont.)

IDS Event Viewer



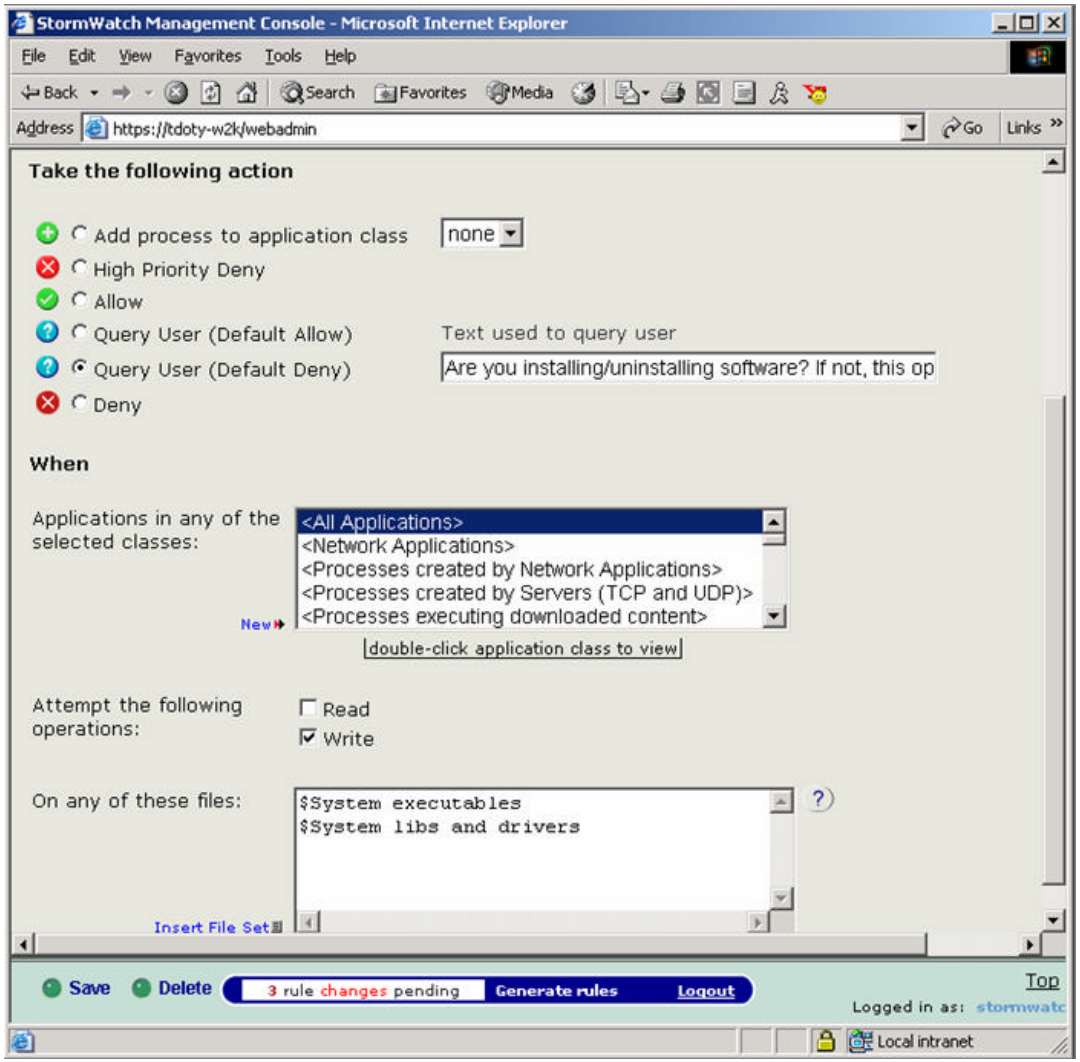
- Windows application: NT or 2000
- Can be downloaded from www.Cisco.com
- Event monitoring for up to three Sensors including IDSM

© 2003, Cisco Systems, Inc. All rights reserved.

HIP Management Product

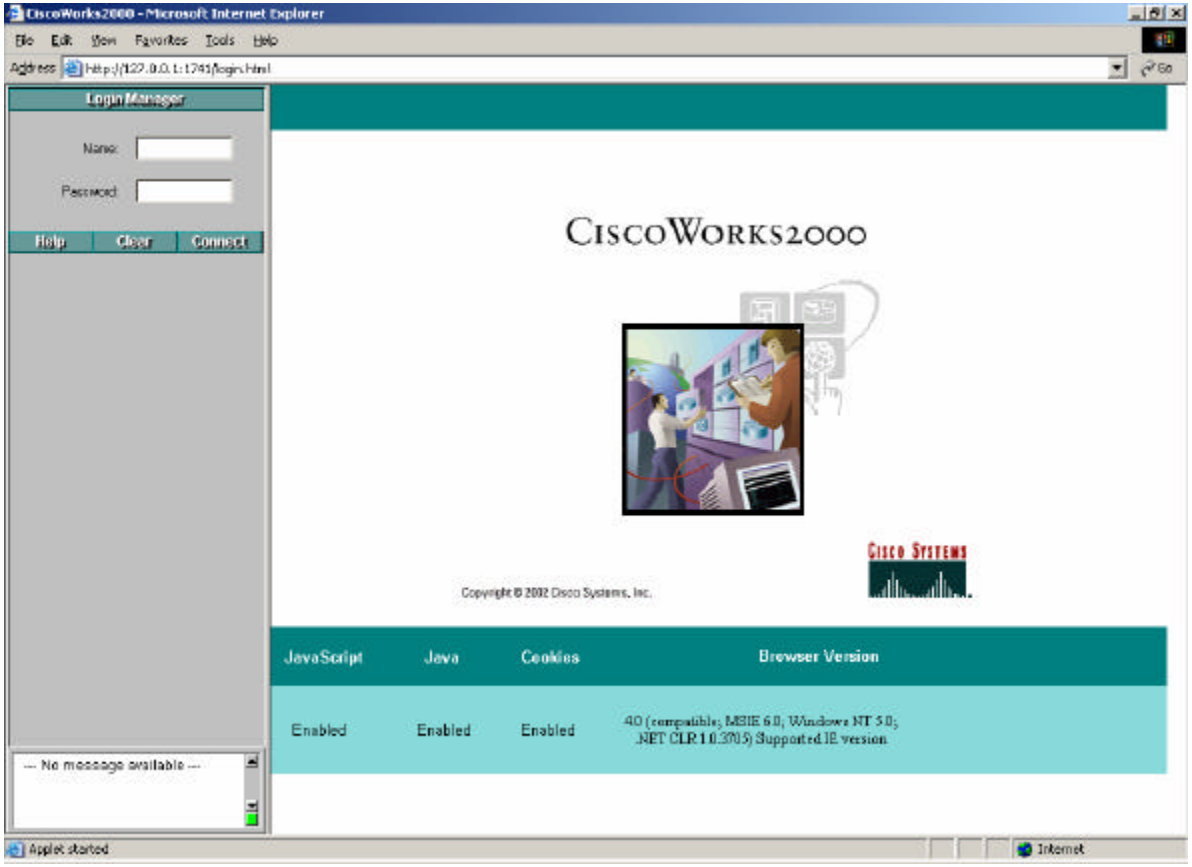
Cisco Security Agent Management Console

- Runs on Windows 2000
- Provides agent management including deployment, configuration, event monitoring, and reporting



© 2003, Cisco Systems, Inc. All rights reserved.

VMS



- **An integrated management solution**
- **Provides web-based applications for the following:**
  - **Monitoring and troubleshooting enterprise VPNs**
  - **VPN C3000, 7100, 7200, 2600, 3600, 1700, and 800**
- **Features for configuring and monitoring firewall and IDS security**
- **Used for large-scale deployment**

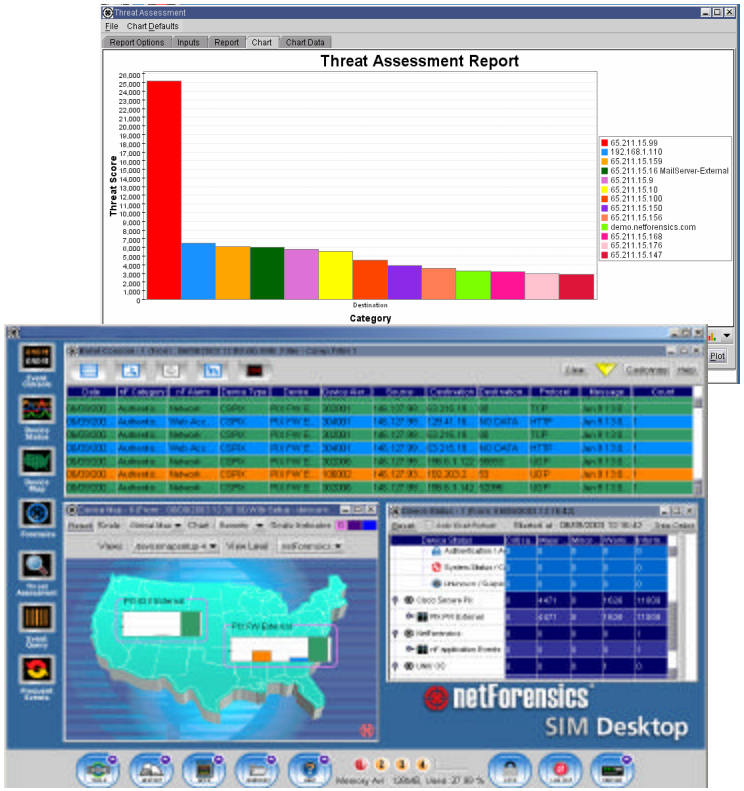
© 2003, Cisco Systems, Inc. All rights reserved.

CiscoWorks SIMS Overview

CiscoWorks IDS Advanced Monitoring and Reporting

Cisco.com

- Real-time monitoring & graphing
- Advanced reporting (250 reports)
  - Top intruders by source, top attack destinations, sensor summary by alarm level
  - Build custom reports
- Business impact for value/risk assessment
- Minimizes the time gap between detection and reaction
- Scalable distributed monitoring to support large Cisco IDS deployments
- Role-based administration



CWSIM-3.1-SS-K9 – Solaris ki
CWSIM-3.1-SL-K9 – Linux kit
CWSIME-1160-K9 – Appliance

© 2003, Cisco Systems, Inc. All rights reserved.

RDEP / 3rd Party Integration

Flexible Monitoring Options

Integration Completed:

netForensics

Micromuse

Arbor Networks

Arcsight

Network Intelligence

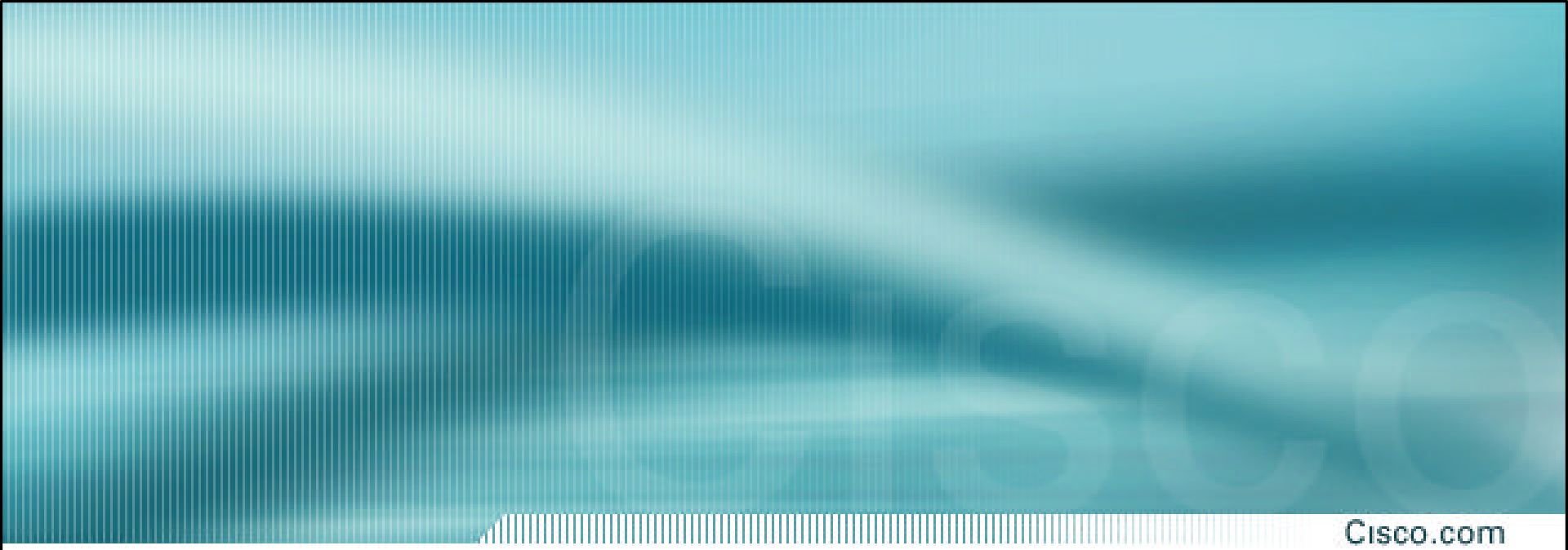
E-Security

Integration In Progress:

Tivoli RiskManager

© 2003, Cisco Systems, Inc. All rights reserved.

** RDEP = Remote Data Exchange Protocol*



Cisco Threat Response

© 2003, Cisco Systems, Inc. All rights reserved.

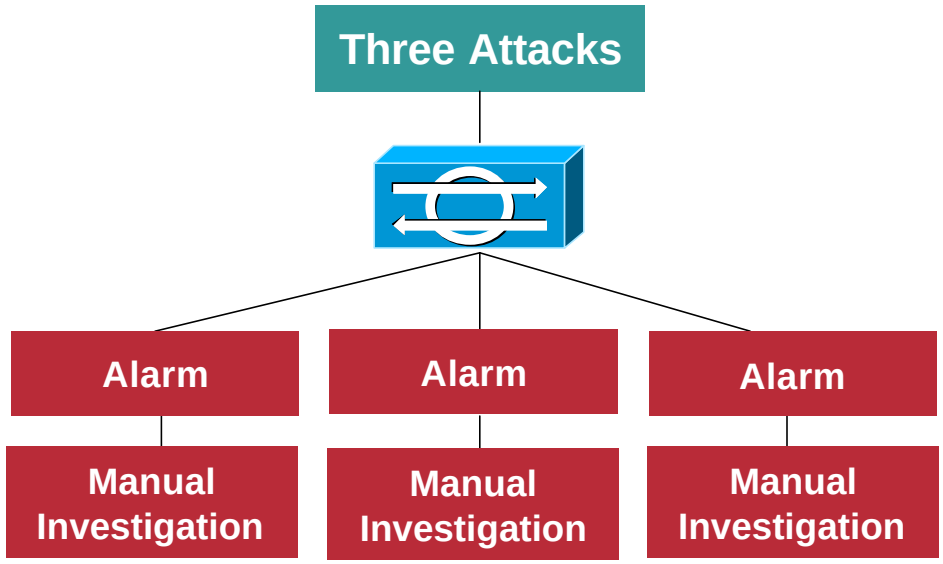
Cisco Threat Response

Threat Response has the following characteristics:

- Performs real-time investigation of every alert
- Discriminates between real and false alarms
- Downgrades inconsequential alerts
- Escalates critical alerts
- Performs just-in-time analysis of target hosts to assess damage
- Aids in remediation of intrusions
- Focuses exclusively on monitoring your Sensors and providing automated investigation of each attack
- Requires no prior knowledge of network
- Requires no remote agents
- Synergistic relationship with existing solutions
- Reduces false positives up to 95%

© 2003, Cisco Systems, Inc. All rights reserved.

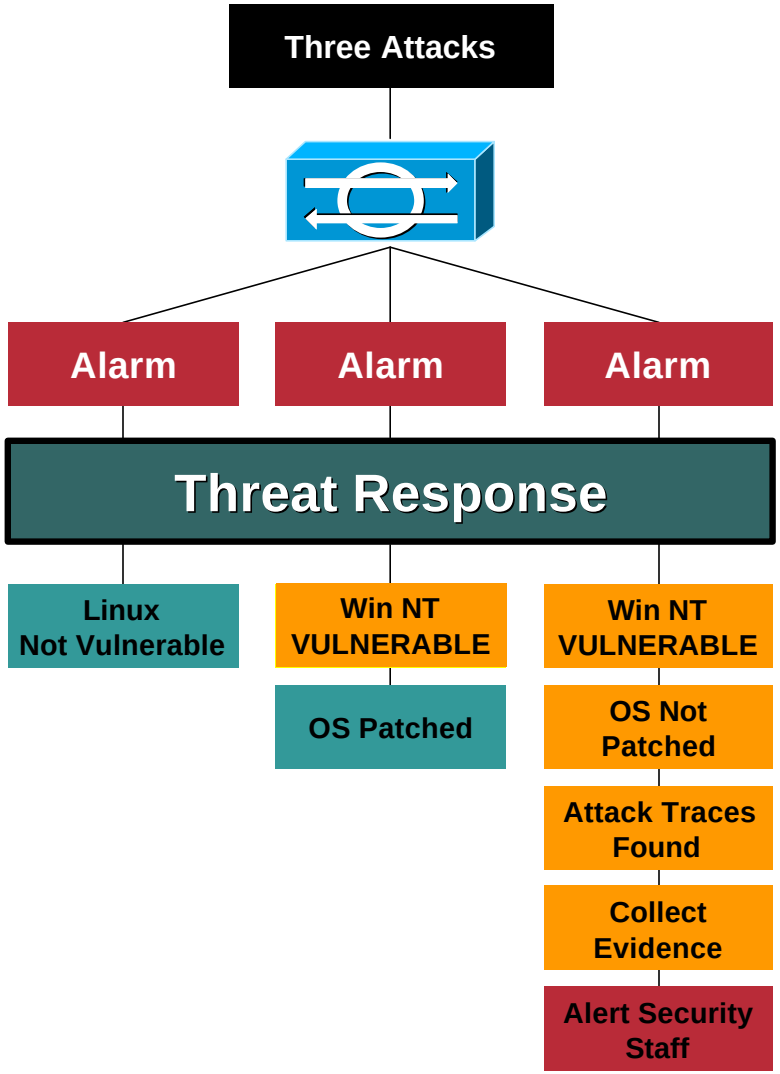
Intrusion Protection without Intelligent Investigation



1. An attacker launches an auto-scanner script to search for a common IIS unicode vulnerability.
2. The Sensor reports a number of detected attacks against hosts in the network.
3. The Event Viewer or Security Monitor displays several real attack events.

© 2003, Cisco Systems, Inc. All rights reserved.

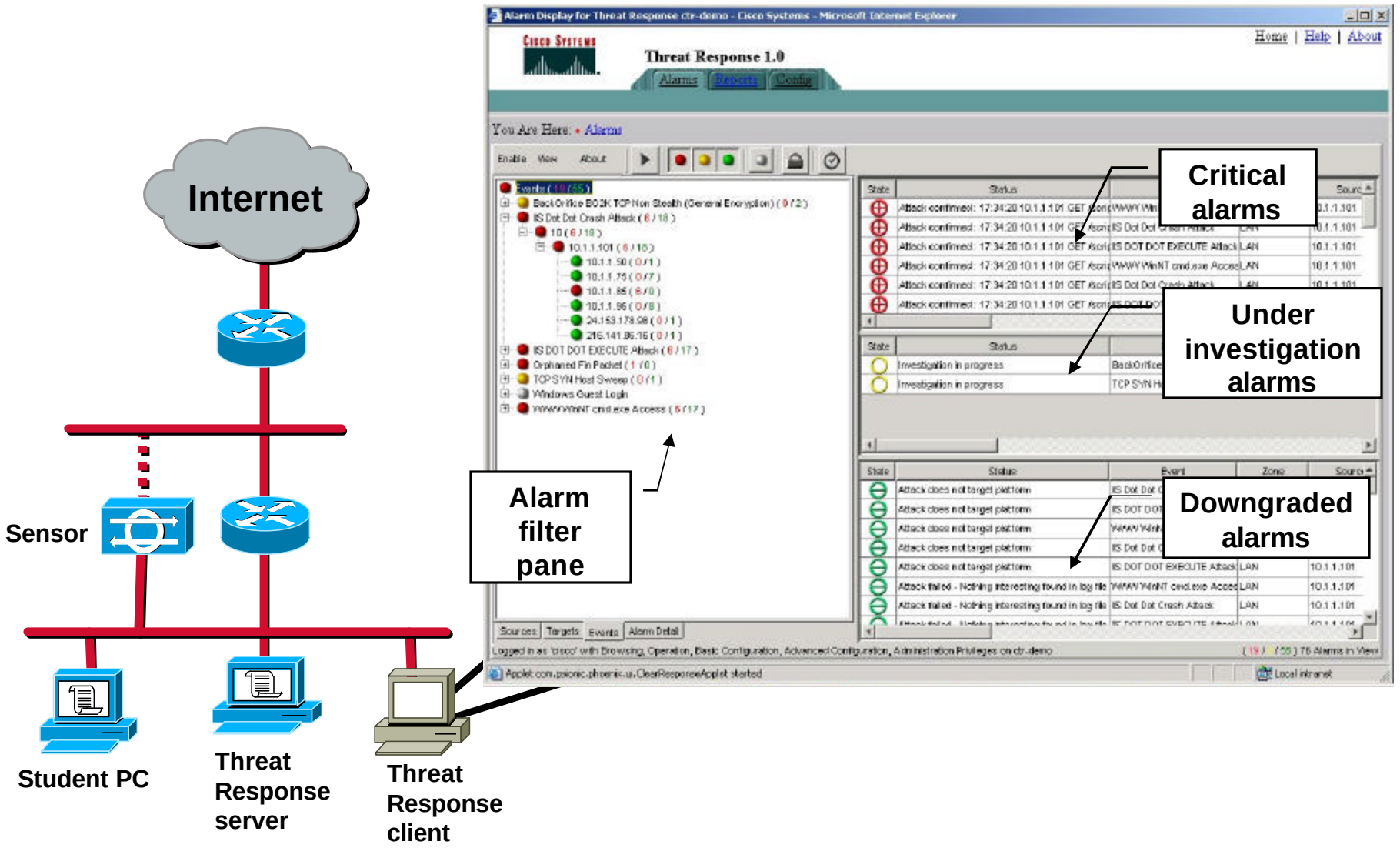
Intrusion Protection with Intelligent Investigation



1. An attacker launches an auto-scanner script to search for a common IIS unicode vulnerability.
2. The Sensor reports a number of detected attacks against hosts in the network.
3. Threat Response does the following:
   - Step 1) Determines whether the attack targets this OS type
   - Step 2) Determines whether the OS is vulnerable
   - Step 3) Determines whether there are traces of a successful attack
   - Step 4) Copies and secures forensic evidence
   - Step 5) Alerts you to a real and confirmed attack

© 2003, Cisco Systems, Inc. All rights reserved.

Threat Response Deployment



© 2003, Cisco Systems, Inc. All rights reserved.

Traffic Capture Overview

© 2003, Cisco Systems, Inc. All rights reserved.

Overview

Cisco.com

- **Network traffic must be visible to the Network IDS to perform analysis.**
- **The Sensor's monitoring port is connected to a network device that captures the traffic.**

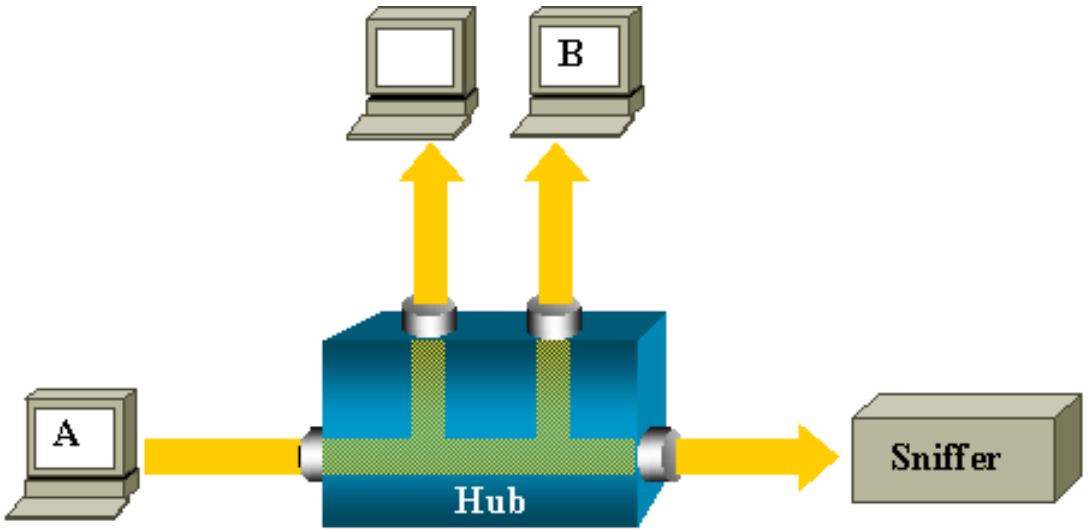
© 2003, Cisco Systems, Inc. All rights reserved.

Overview (Cont.)

- **The network devices that are used to capture network traffic are:**
  - **Hubs**
  - **Network Taps***
  - **Switches**
- **The methods that are used to capture network traffic are:**
  - **SPAN**
  - **RSPAN**
  - **VACLs**
  - **The** mls ip ids **command**

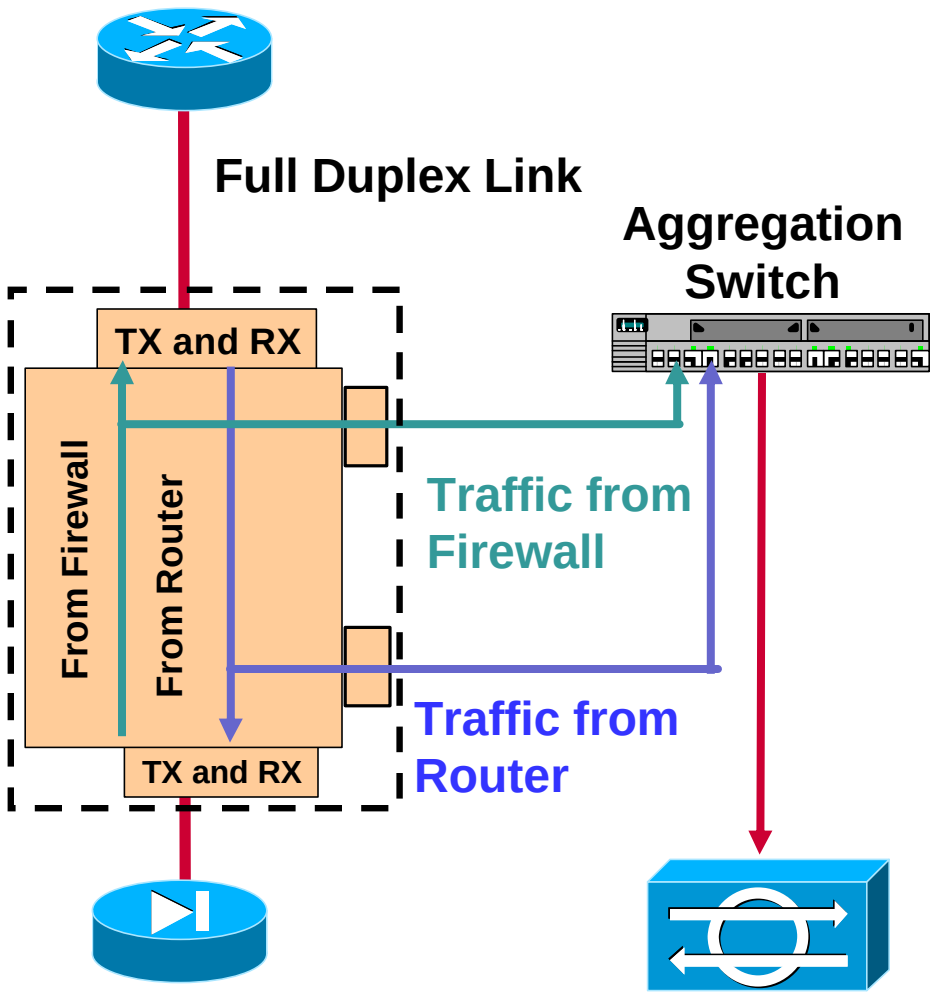
© 2003, Cisco Systems, Inc. All rights reserved.

Hub Traffic Flow



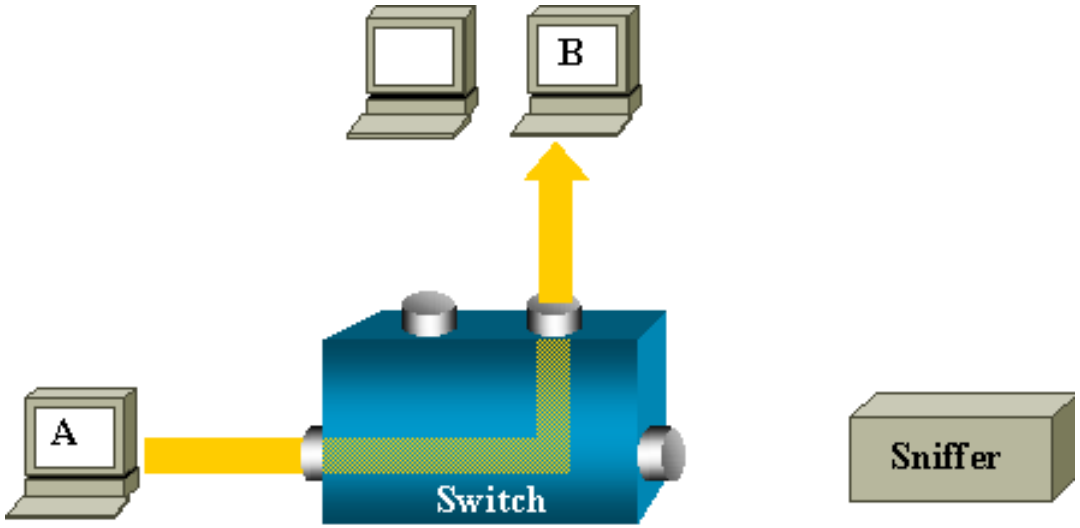
© 2003, Cisco Systems, Inc. All rights reserved.

Network Tap Traffic Flow



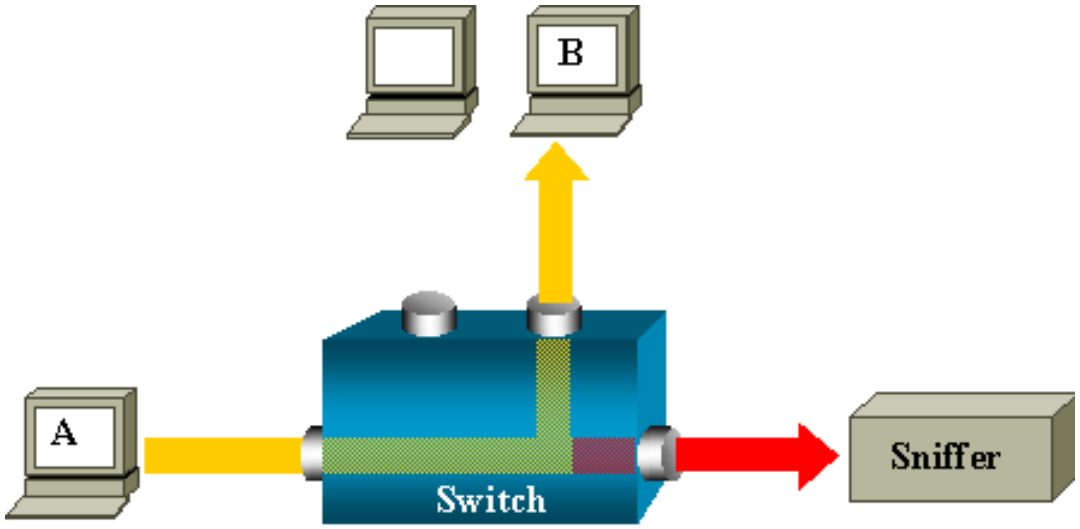
© 2003, Cisco Systems, Inc. All rights reserved.

Switch Traffic Flow



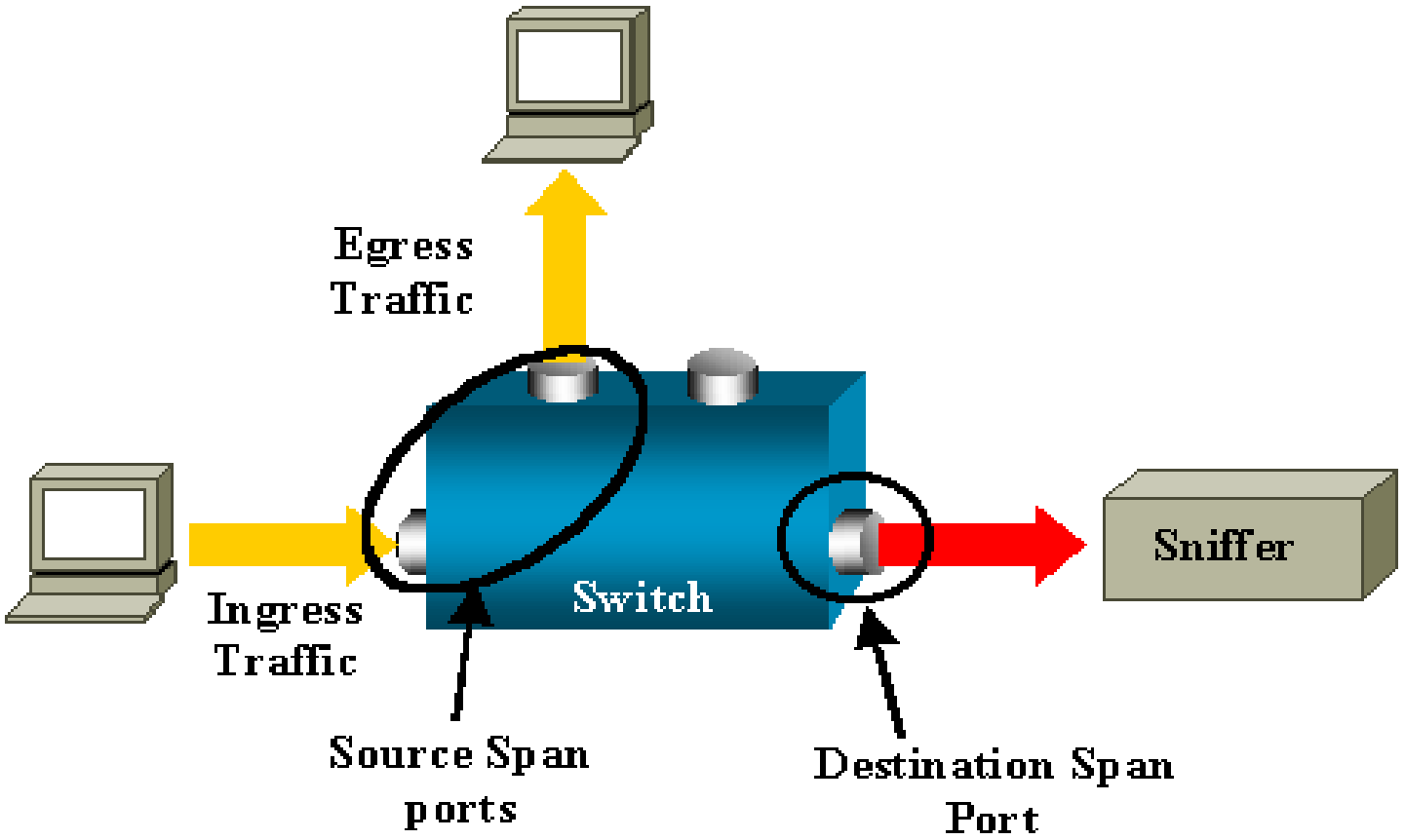
© 2003, Cisco Systems, Inc. All rights reserved.

SPAN Traffic Flow



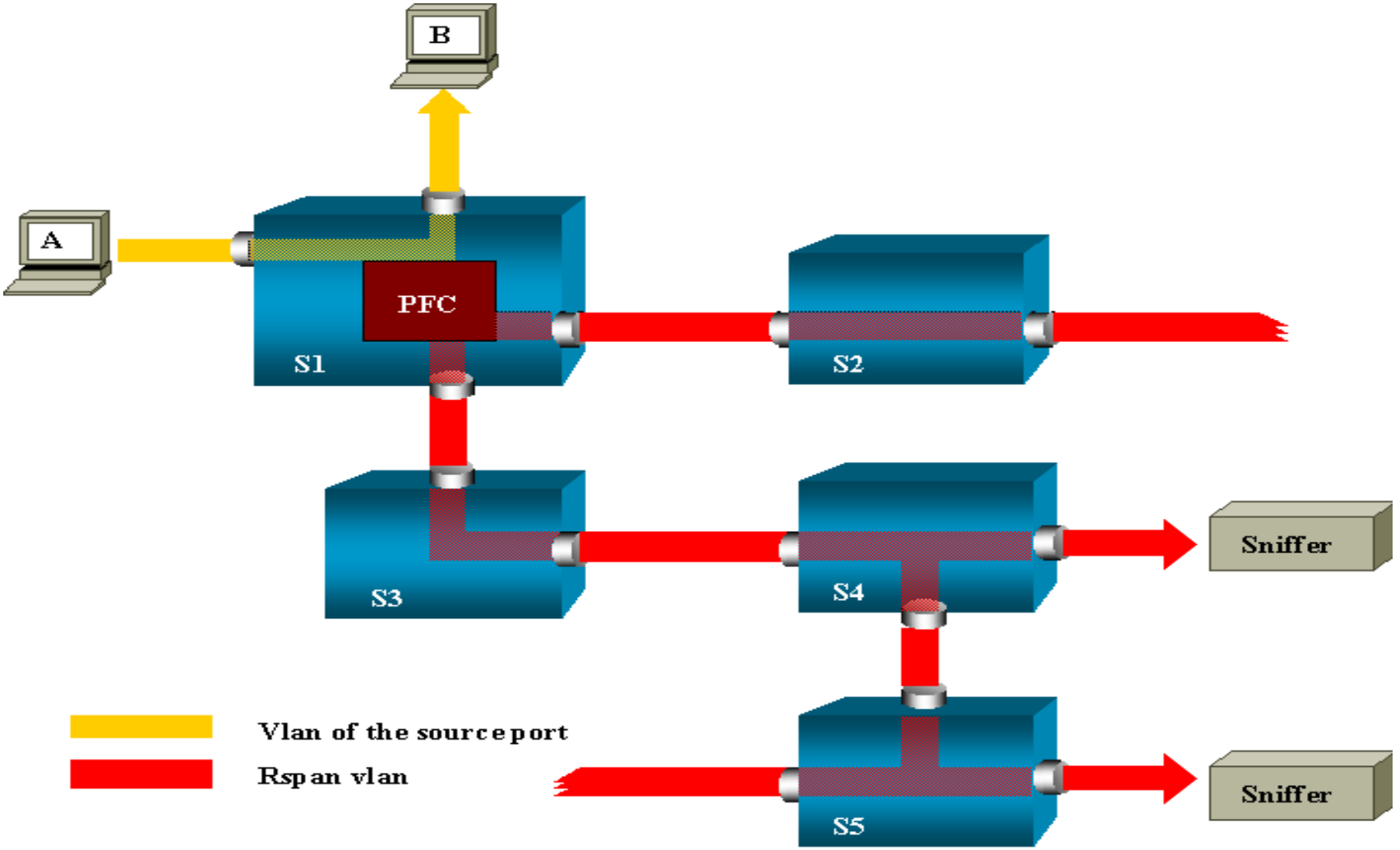
© 2003, Cisco Systems, Inc. All rights reserved.

SPAN Terminology



© 2003, Cisco Systems, Inc. All rights reserved.

RSPAN Traffic Flow



© 2003, Cisco Systems, Inc. All rights reserved.

TCP Resets and Switches

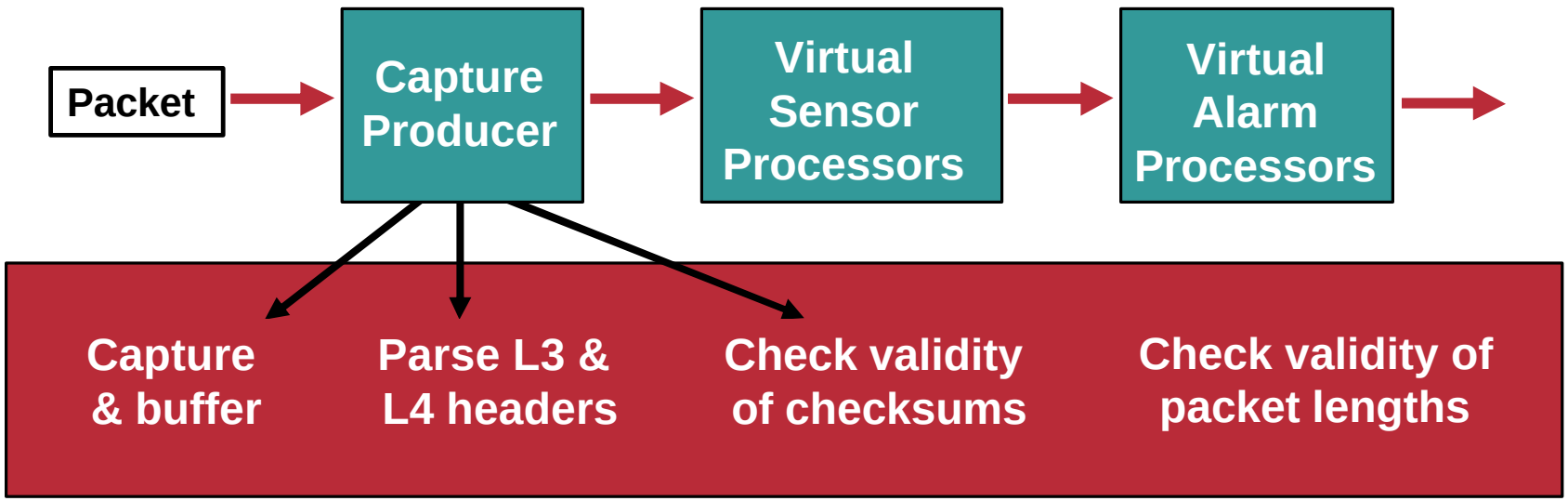
- The Sensor sends the TCP reset packets from the monitoring interface.
- The monitoring interface is typically the SPAN destination port.
- Not all switches allow SPAN destination ports to receive input packets.
- Cisco IDS Sensors use a randomly generated MAC address in the TCP reset packet.

© 2003, Cisco Systems, Inc. All rights reserved.

Cisco IDS Software Architecture

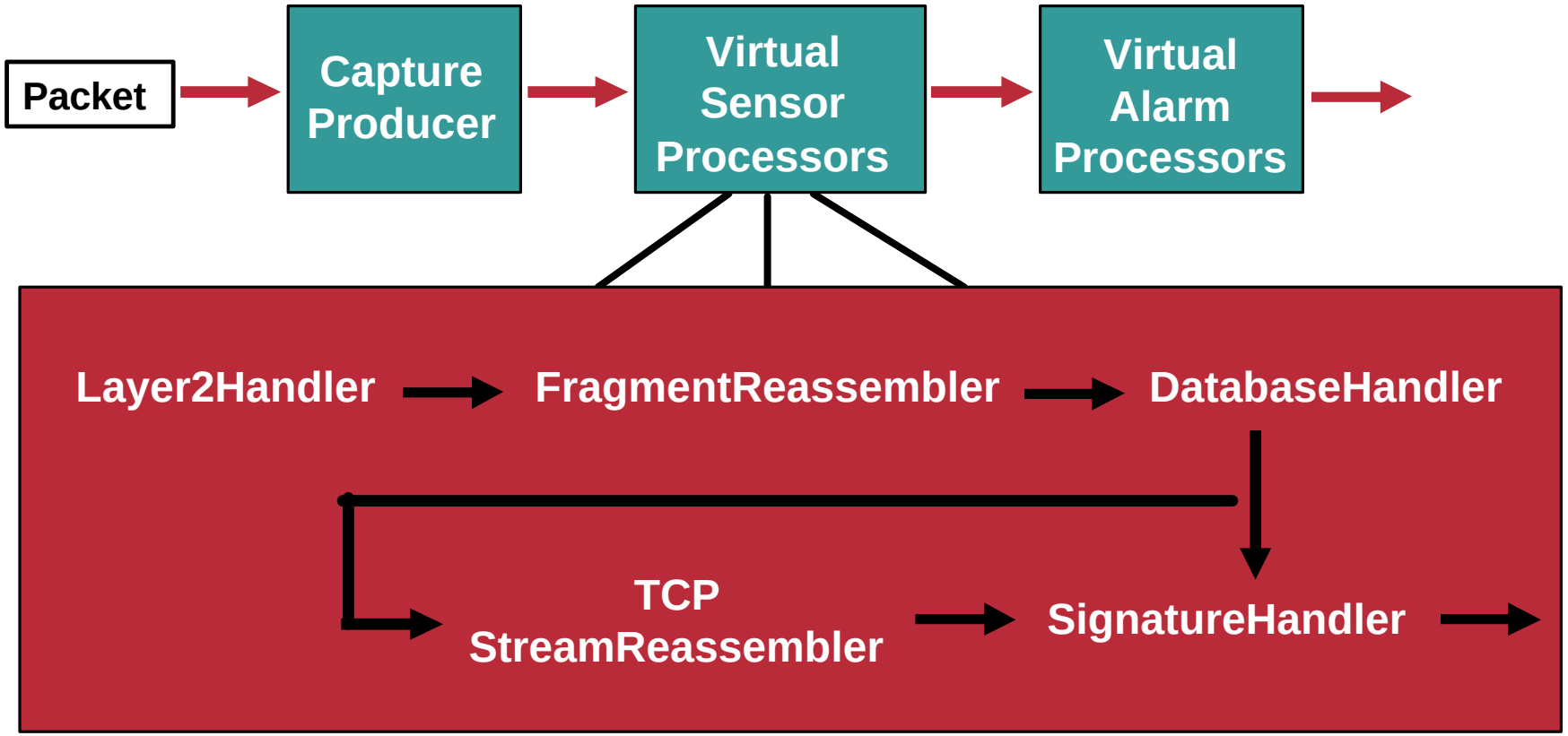
© 2003, Cisco Systems, Inc. All rights reserved.

Life of a Packet



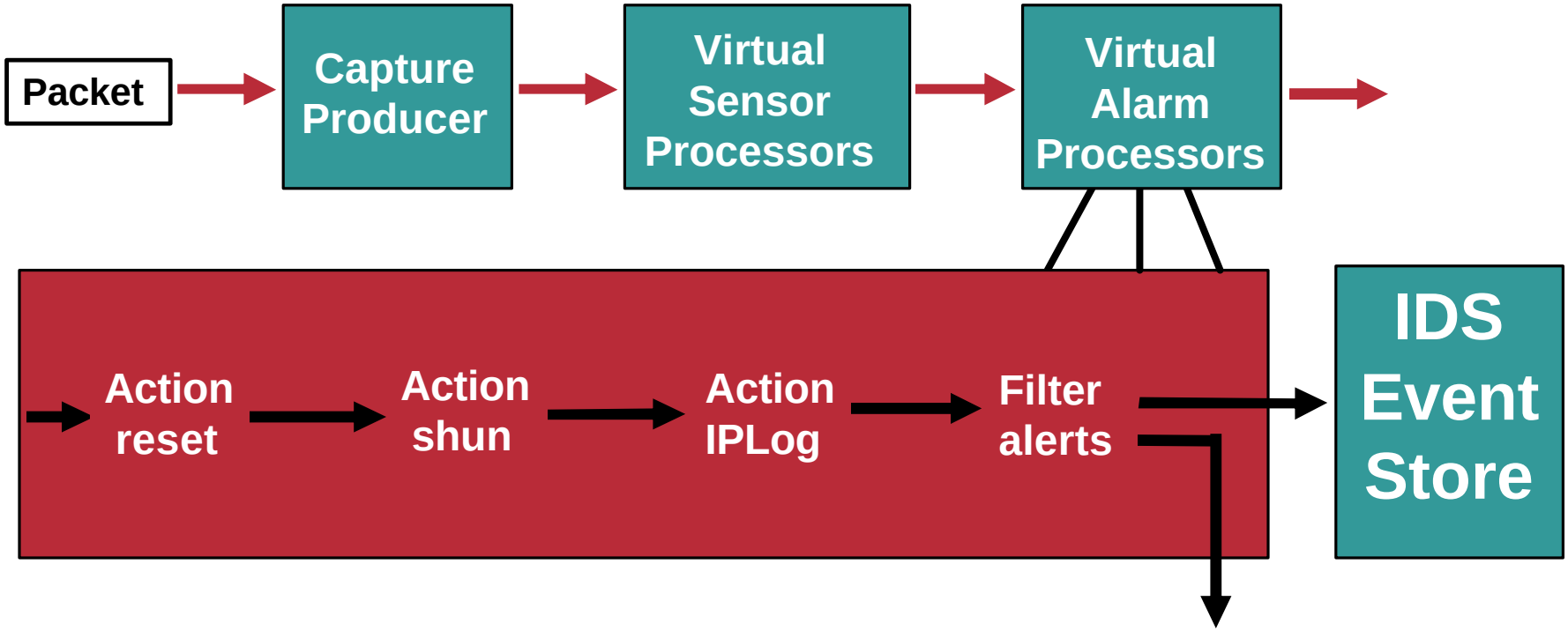
© 2003, Cisco Systems, Inc. All rights reserved.

Life of a Packet (Cont.)

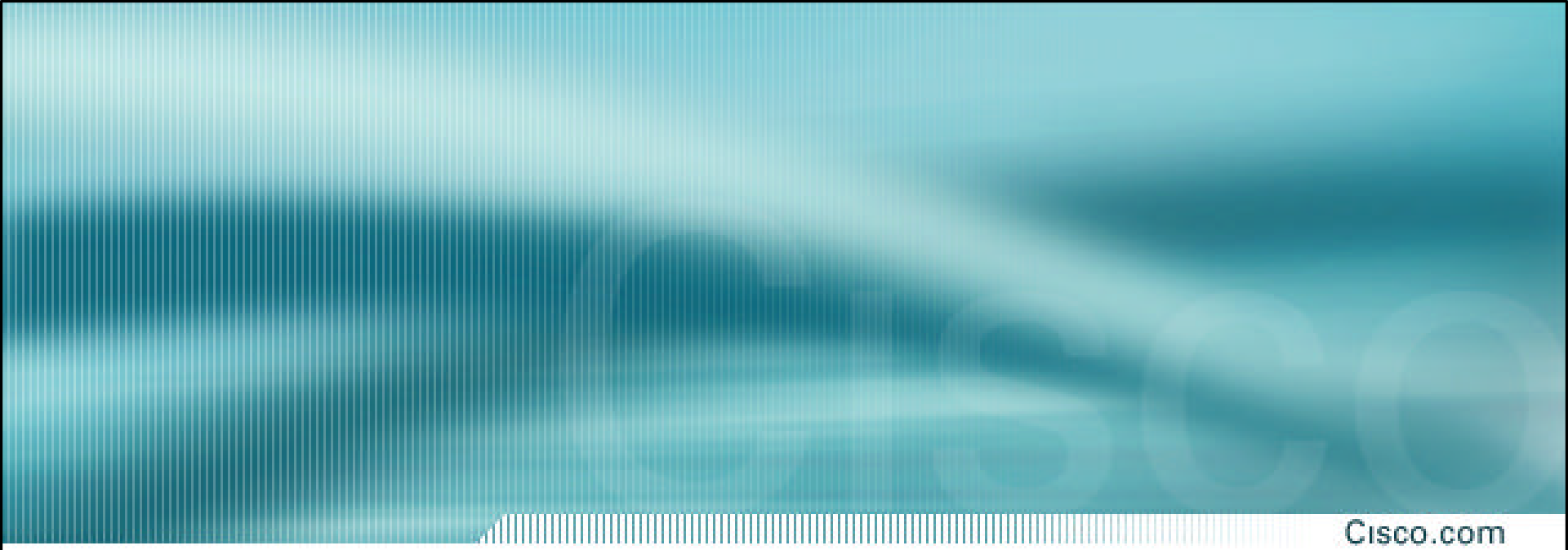


© 2003, Cisco Systems, Inc. All rights reserved.

Life of a Packet (Cont.)



© 2003, Cisco Systems, Inc. All rights reserved.



Cisco IDS Communication

© 2003, Cisco Systems, Inc. All rights reserved.

Communications Overview

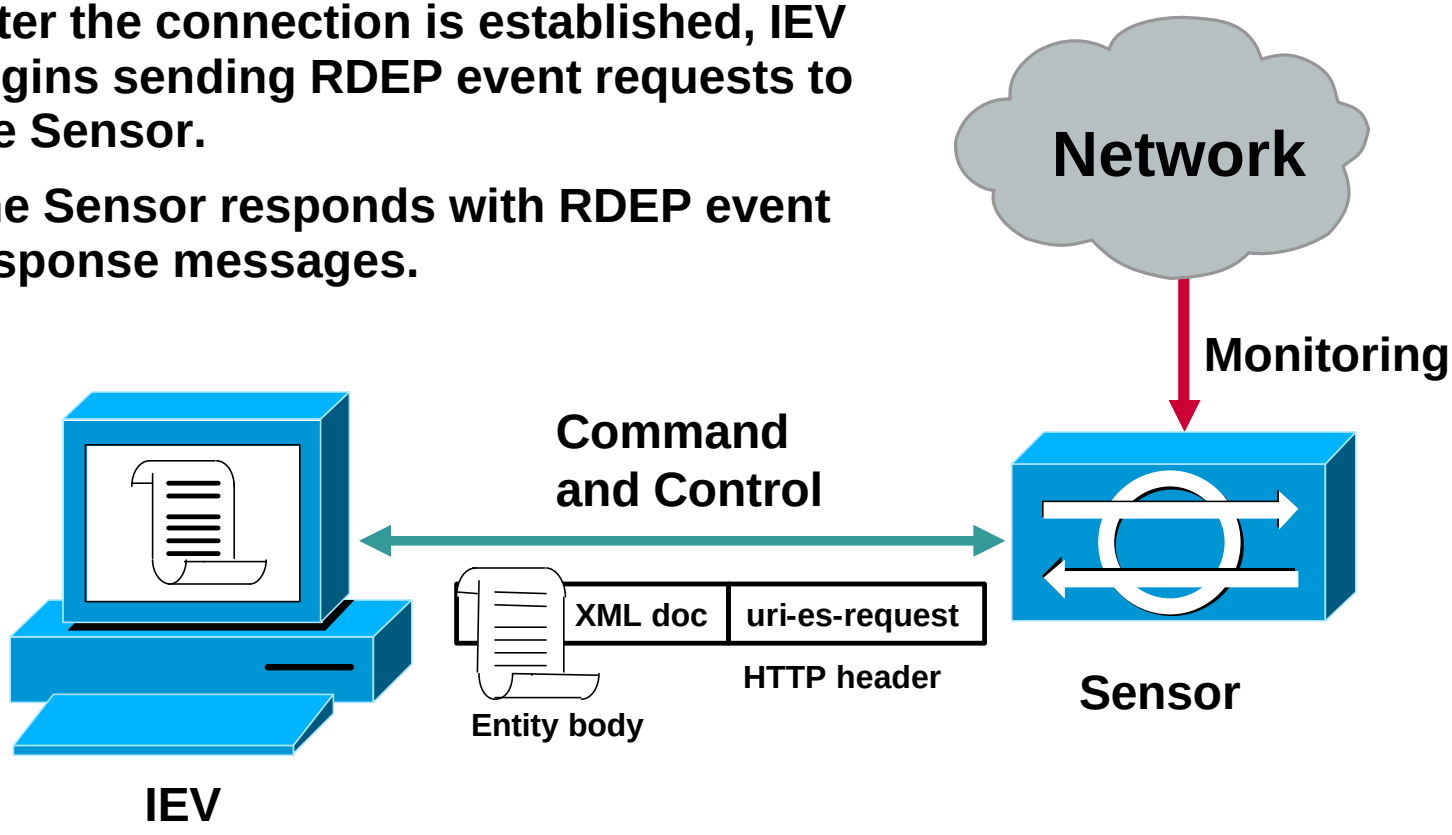
Cisco.com

- IDAPI handles internal communications.
- RDEP handles external communications.
  - RDEP uses HTTP/HTTPS to communicate XML documents between the Sensor and external systems.

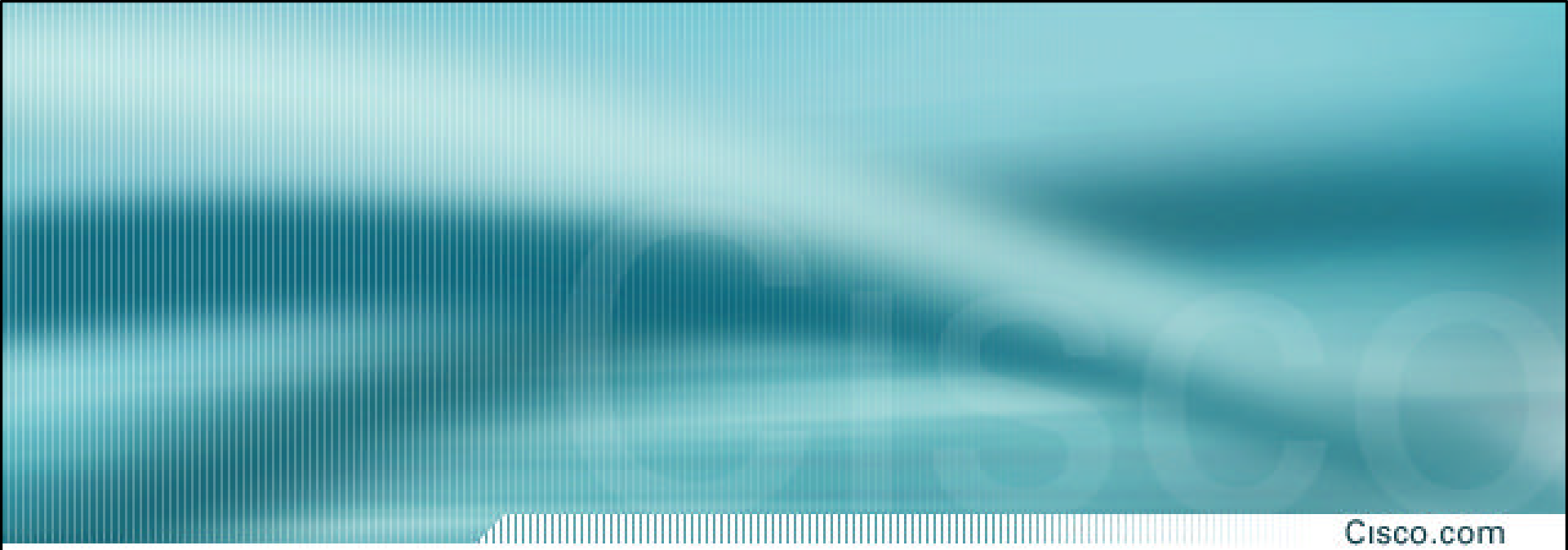
© 2003, Cisco Systems, Inc. All rights reserved.

RDEP Requests and Responses

- IEV has initiated an encrypted HTTP over TLS/SSL connection with the Sensor.
- After the connection is established, IEV begins sending RDEP event requests to the Sensor.
- The Sensor responds with RDEP event response messages.



© 2003, Cisco Systems, Inc. All rights reserved.



User Accounts and Roles

© 2003, Cisco Systems, Inc. All rights reserved.

User Accounts

- Users access a Sensor by logging into a user account.
- User accounts are created on the Sensor.
- Multiple accounts can be created.
- The authentication application configures and manages authentication.

© 2003, Cisco Systems, Inc. All rights reserved.

User Account Roles

- User accounts have roles.
- Roles determine the user's privileges.
- The following roles can be assigned to an account:
  - Administrator
  - Operator
  - Anonymous
  - Viewer
  - Service

© 2003, Cisco Systems, Inc. All rights reserved.

The Service Account

- Special account that enables root access
- Sensor allows only one service account
- Not created by default
- Should be created for troubleshooting

!Caution!

Do not make modifications to the Sensor through the service account except under the direction of TAC.

© 2003, Cisco Systems, Inc. All rights reserved.

© 2002, Cisco Systems, Inc. All rights reserved.