CCNA Security

Chapter Five

Implementing Intrusion Prevention

© 2009 Cisco Learning Institute.

Lesson Planning

- This lesson should take 3-6 hours to present
- The lesson should include lecture, demonstrations, discussion and assessments
- The lesson can be taught in person or using remote instruction

© 2009 Cisco Learning Institute.

Major Concepts

- Describe the purpose and operation of network-based and host-based Intrusion Prevention Systems (IPS)
- Describe how IDS and IPS signatures are used to detect malicious network traffic
- Implement Cisco IOS IPS operations using CLI and SDM
- Verify and monitor the Cisco IOS IPS operations using CLI and SDM

© 2009 Cisco Learning Institute.

Lesson Objectives

Upon completion of this lesson, the successful participant will be able to:

1. Describe the functions and operations of IDS and IPS systems
2. Introduce the two methods of implementing IPS and describe host based IPS
3. Describe network-based intrusion prevention
4. Describe the characteristics of IPS signatures
5. Describe the role of signature alarms (triggers) in Cisco IPS solutions
6. Describe the role of tuning signature alarms (triggers) in a Cisco IPS solution

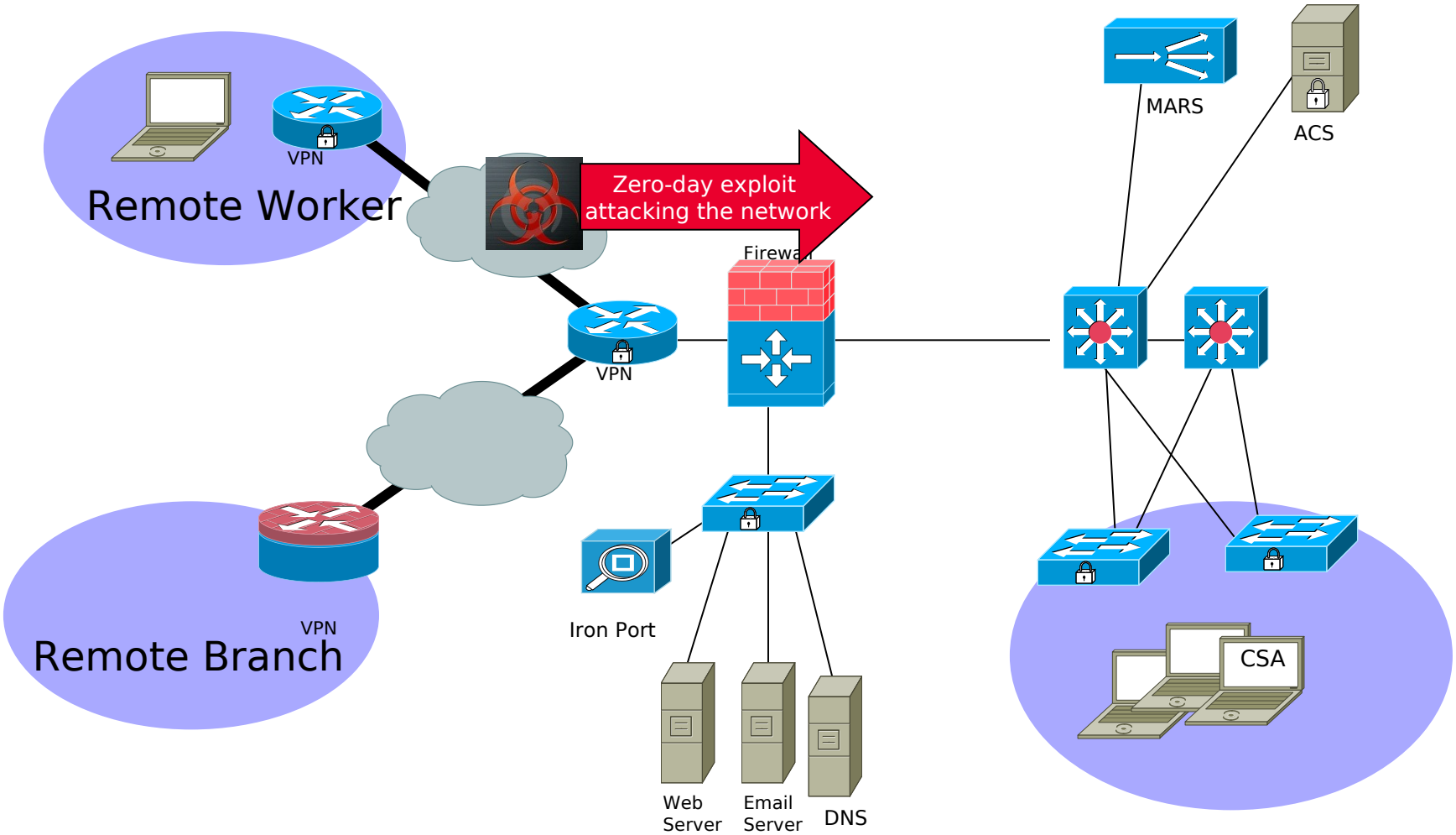
© 2009 Cisco Learning Institute.

Lesson Objectives

7. Describe the role of signature actions in a Cisco IPS solution
8. Describe the role of signature monitoring in a Cisco IPS solution
9. Describe how to configure Cisco IOS IPS Using CLI
10. Describe how to configure Cisco IOS IPS using Cisco SDM
11. Describe how to modify IPS signatures in CLI and SDM
12. Describe how to verify the Cisco IOS IPS configuration
13. Describe how to monitor the Cisco IOS IPS events
14. Describe how to troubleshoot the Cisco IOS IPS events

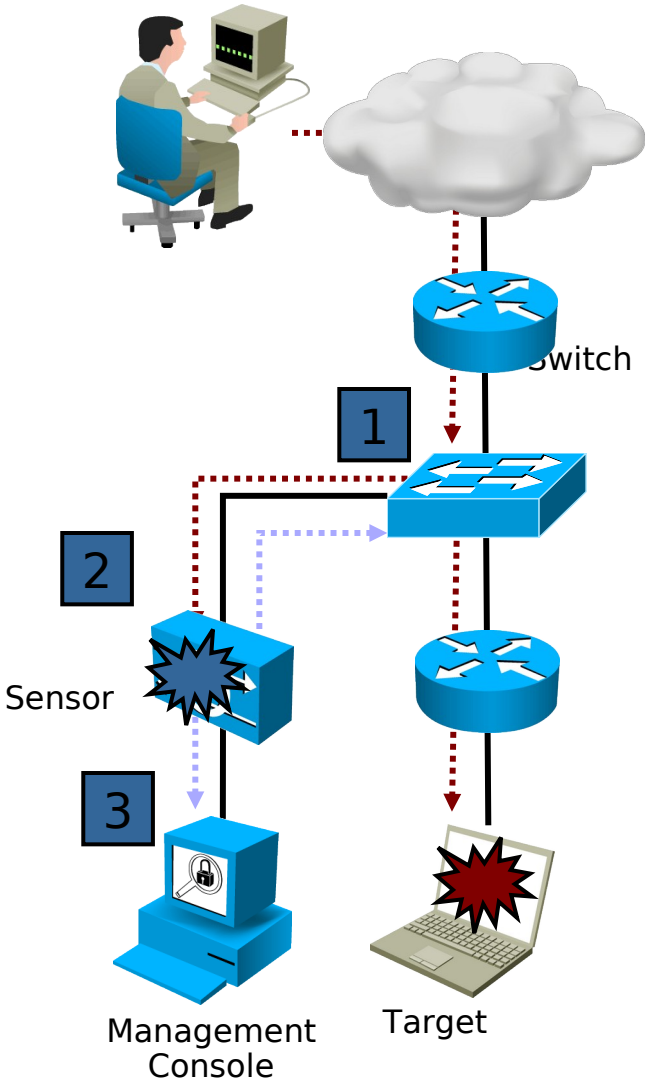
© 2009 Cisco Learning Institute.

Common Intrusions



Intrusion Detection Systems (IDSs)

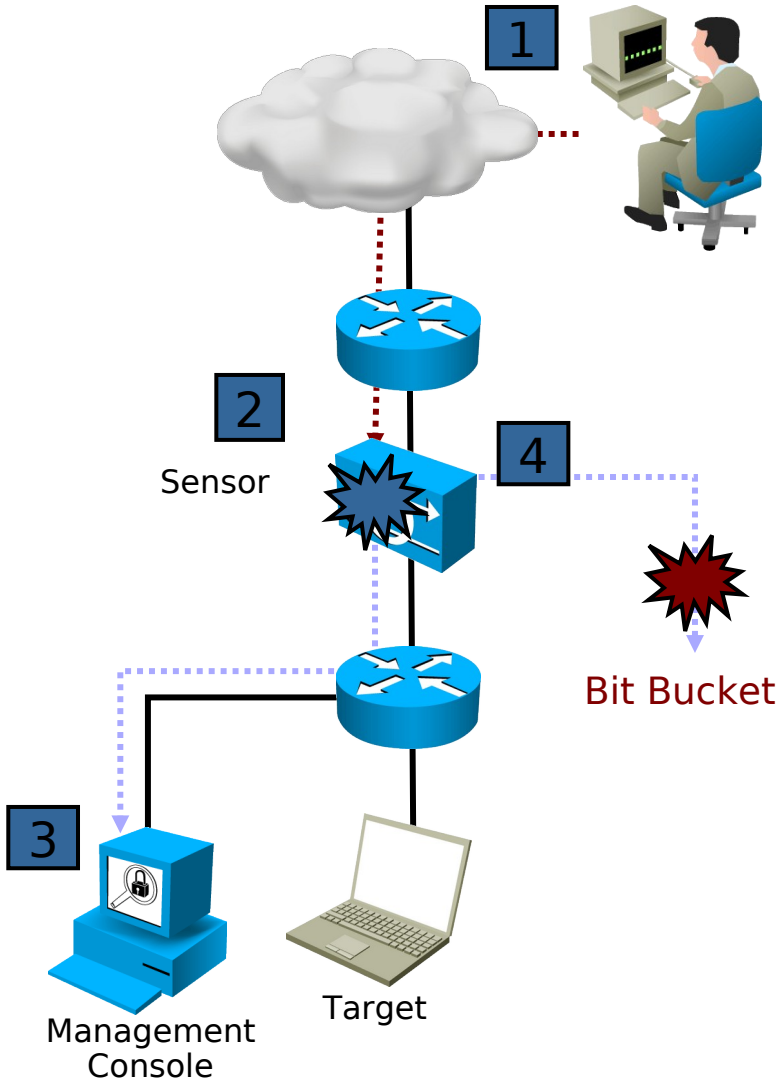
1. An attack is launched on a network that has a sensor deployed in promiscuous IDS mode; therefore copies of all packets are sent to the IDS sensor for packet analysis. However, the target machine will experience the malicious attack.
2. The IDS sensor, matches the malicious traffic to a signature and sends the switch a command to deny access to the source of the malicious traffic.
3. The IDS can also send an alarm to a management console for logging and other management purposes.



© 2009 Cisco Learning Institute.

Intrusion Prevention Systems (IPSs)

1. An attack is launched on a network that has a sensor deployed in IPS mode (inline mode).
2. The IPS sensor analyzes the packets as they enter the IPS sensor interface. The IPS sensor matches the malicious traffic to a signature and the attack is stopped immediately.
3. The IPS sensor can also send an alarm to a management console for logging and other management purposes.
4. Traffic in violation of policy can be dropped by an IPS sensor.



© 2009 Cisco Learning Institute.

Common characteristics of IDS and IPS

- ✓ Both technologies are deployed using sensors.
- ✓ Both technologies use signatures to detect patterns of misuse in network traffic.
- ✓ Both can detect atomic patterns (single-packet) or composite patterns (multi-packet).

© 2009 Cisco Learning Institute.

Comparing IDS and IPS Solutions

	Advantages	Disadvantages
IDS Promiscuous Mode	▪ No impact on network (latency, jitter) ▪ No network impact if there is a sensor failure ▪ No network impact if there is sensor overload	▪ Response action cannot stop trigger packets ▪ Correct tuning required for response actions ▪ Must have a well thought-out security policy ▪ More vulnerable to network evasion techniques

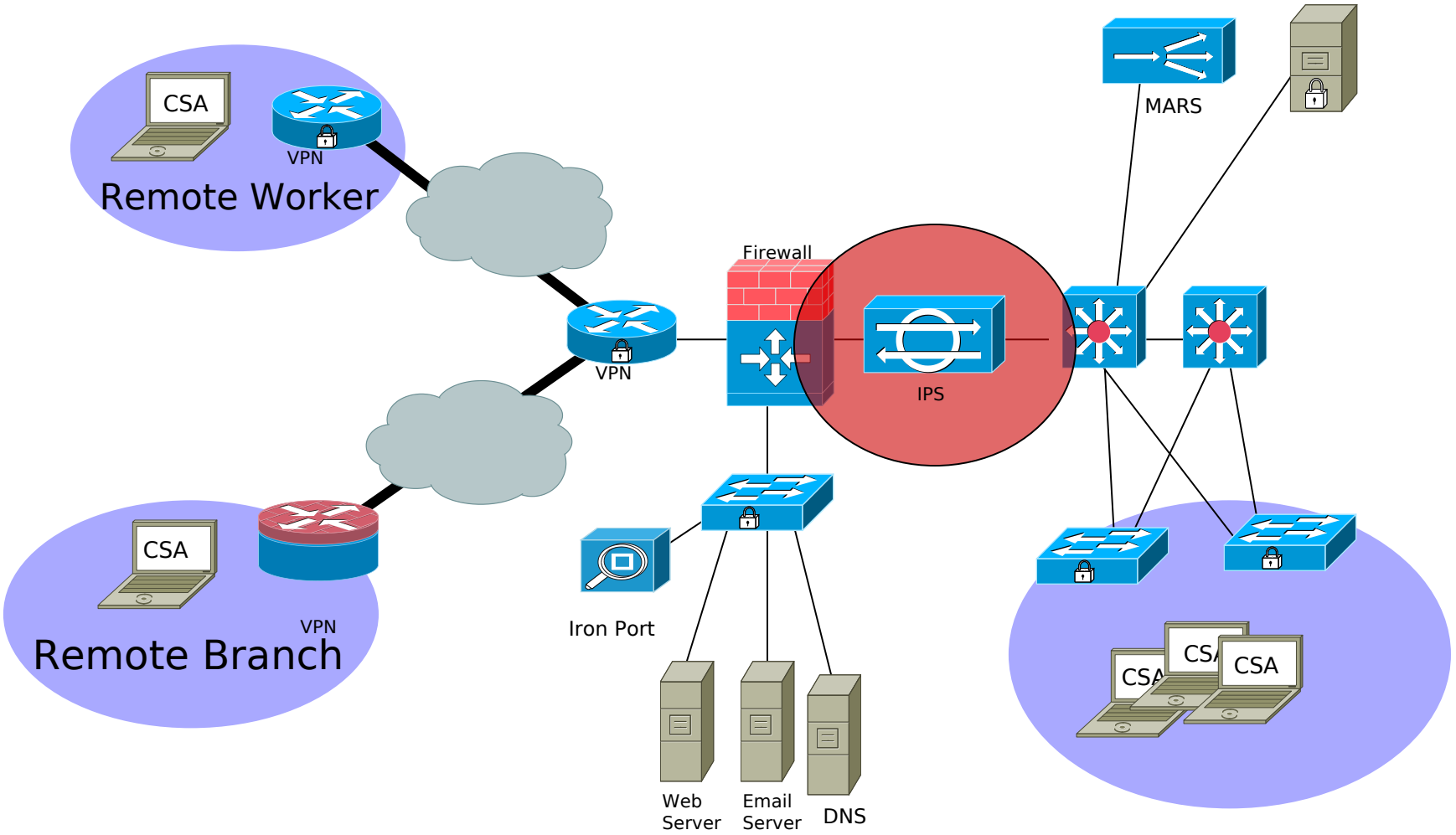
© 2009 Cisco Learning Institute.

Comparing IDS and IPS Solutions

	Advantages	Disadvantages
IPS Inline Mode	▪ Stops trigger packets ▪ Can use stream normalization techniques	▪ Sensor issues might affect network traffic ▪ Sensor overloading impacts the network ▪ Must have a well thought-out security policy ▪ Some impact on network (latency, jitter)

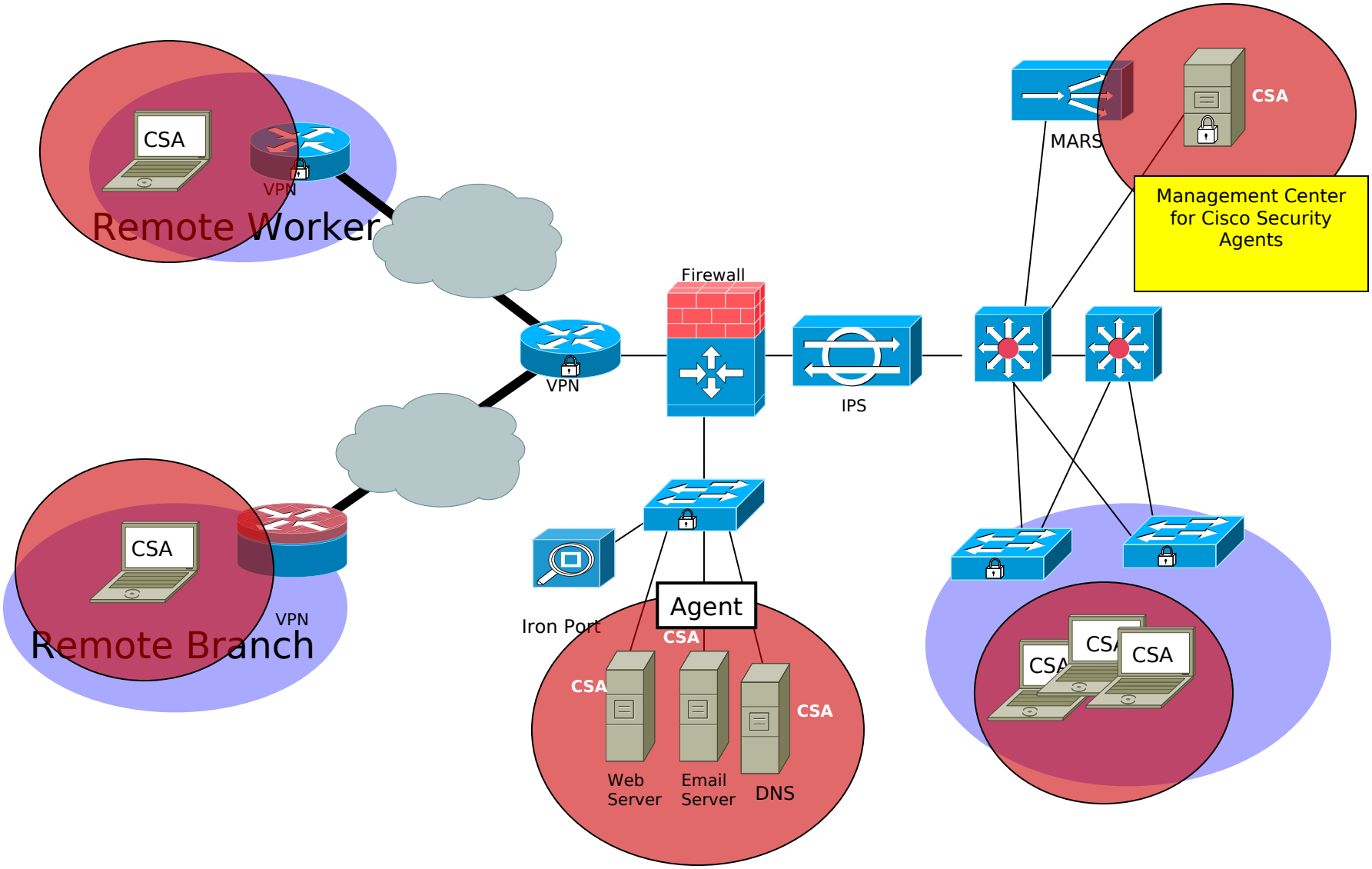
© 2009 Cisco Learning Institute.

Network-Based Implementation



© 2009 Cisco Learning Institute.

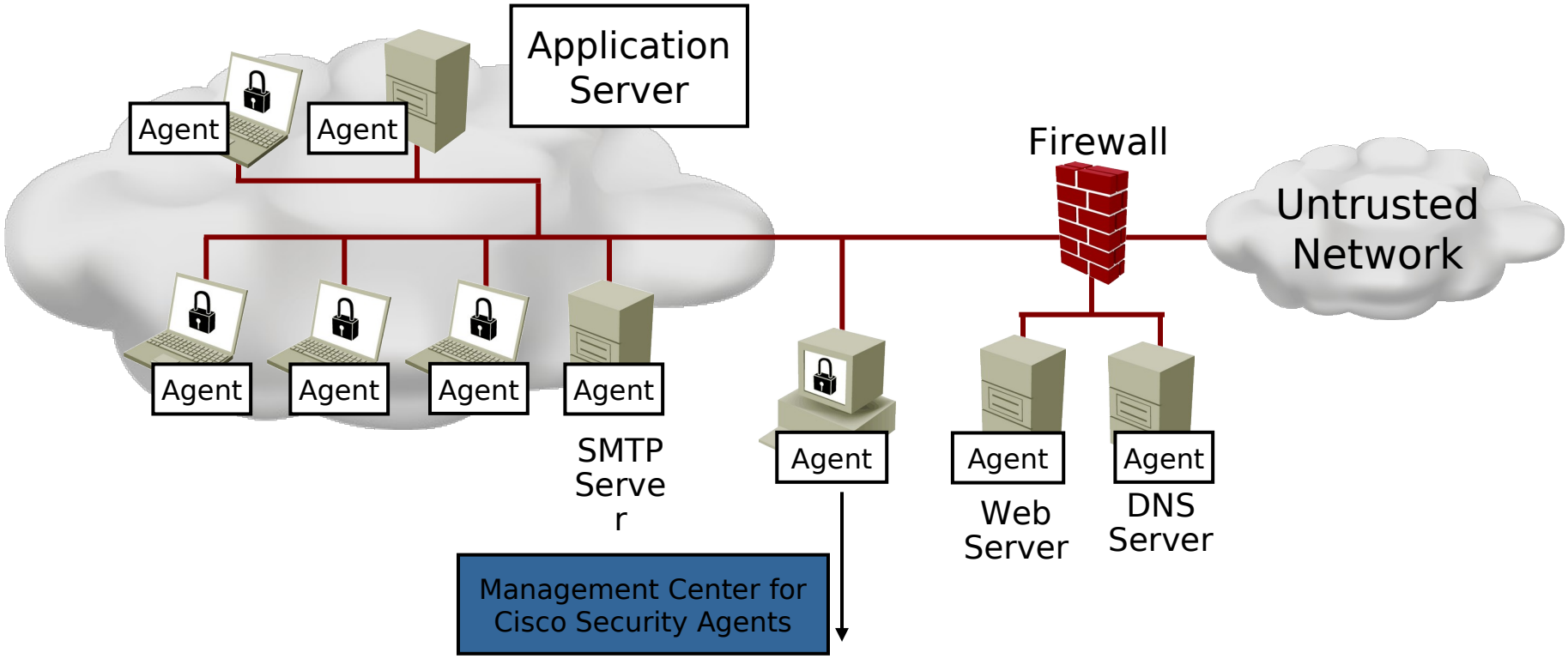
Host-Based Implementation



© 2009 Cisco Learning Institute.

Cisco Security Agent

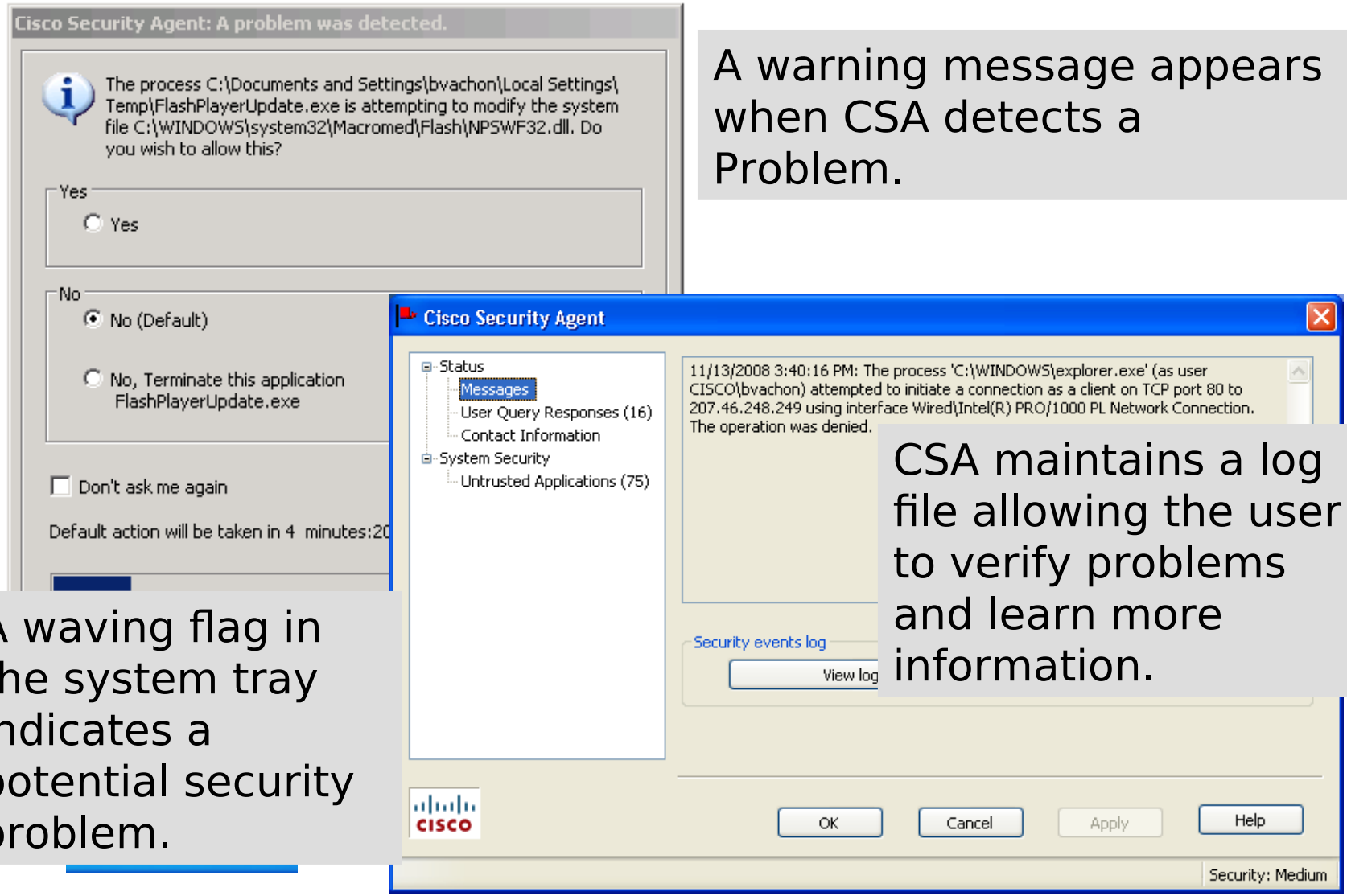
Corporate Network



video

© 2009 Cisco Learning Institute.

Cisco Security Agent Screens



A warning message appears when CSA detects a Problem.

CSA maintains a log file allowing the user to verify problems and learn more information.

A waving flag in the system tray indicates a potential security problem.

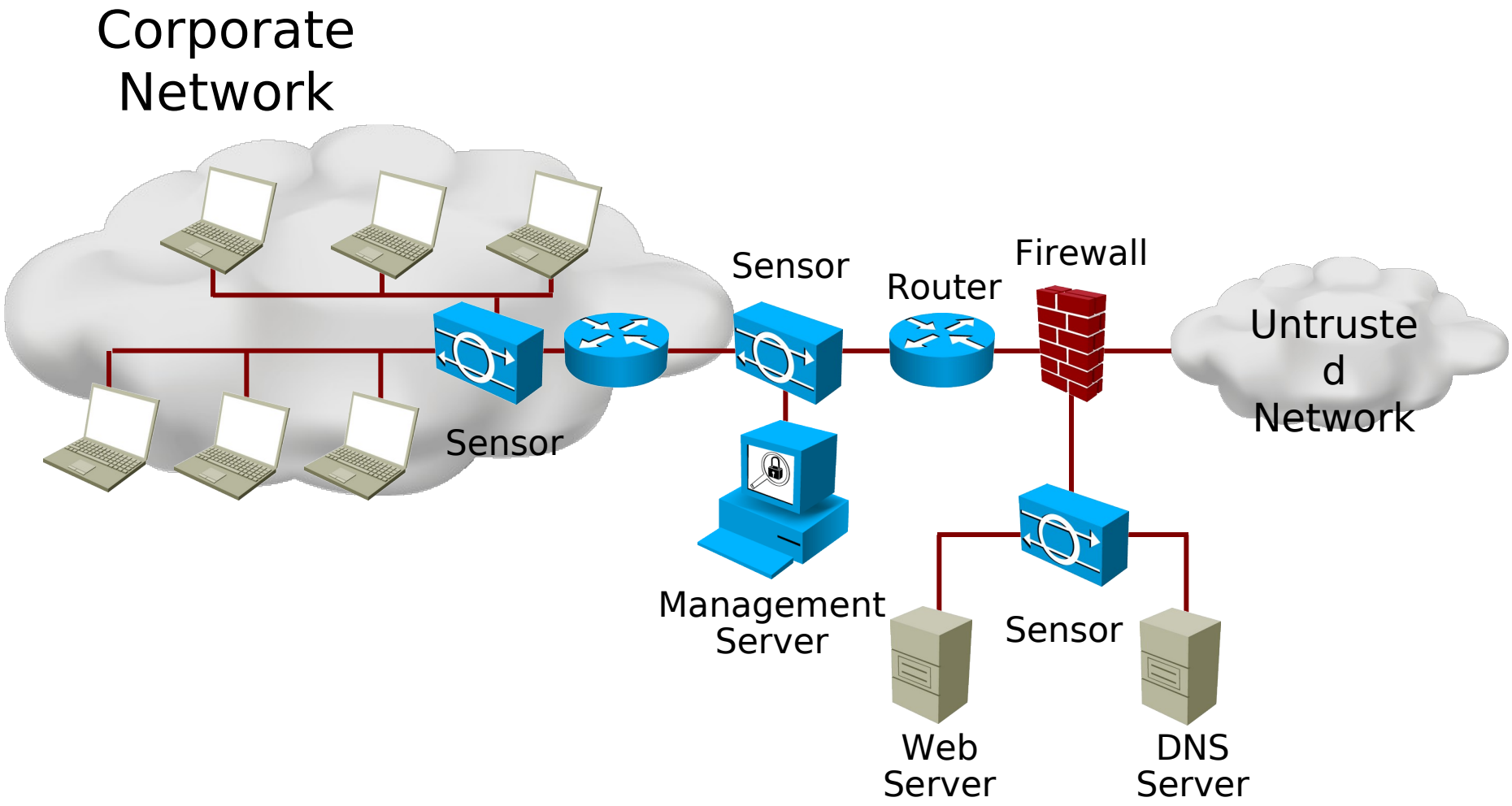
© 2009 Cisco Learning Institute.

Host-Based Solutions

Advantages	Disadvantages
▪ The success or failure of an attack can be readily determined. ▪ HIPS does not have to worry about fragmentation attacks or variable Time to Live (TTL) attacks. ▪ HIPS has access to the traffic in unencrypted form.	▪ HIPS does not provide a complete network picture. ▪ HIPS has a requirement to support multiple operating systems.

© 2009 Cisco Learning Institute.

Network-Based Solutions



© 2009 Cisco Learning Institute.

Cisco IPS Solutions
AIM and Network Module Enhanced

- Integrates IPS into the Cisco 1841 (IPS AIM only), 2800 and 3800 ISR routers
- IPS AIM occupies an internal AIM slot on router and has its own CPU and DRAM
- Monitors up to 45 Mb/s of traffic
- Provides full-featured intrusion protectior
- Is able to monitor traffic from all router interfaces
- Can inspect GRE and IPsec traffic that has been decrypted at the router
- Delivers comprehensive intrusion protection at branch offices, isolating threats from the corporate network
- Runs the same software image as Cisco IPS Sensor Appliances



© 2009 Cisco Learning Institute.

Cisco IPS Solutions
ASA AIP-SSM

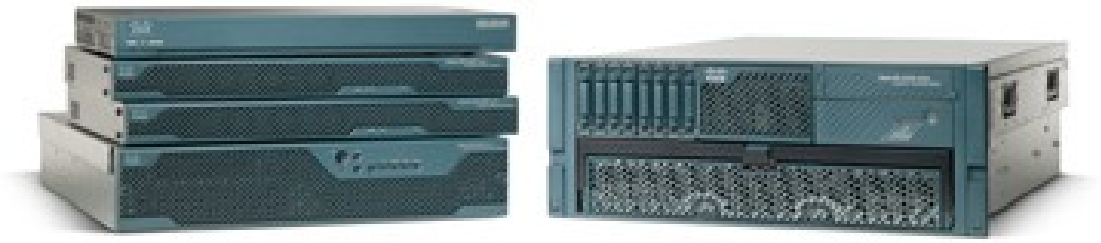
- High-performance module designed to provide additional security services to the Cisco ASA 5500 Series Adaptive Security Appliance
- Diskless design for improved reliability
- External 10/100/1000 Ethernet interface for management and software downloads
- Intrusion prevention capability
- Runs the same software image as the Cisco IPS Sensor appliances



© 2009 Cisco Learning Institute.

Cisco IPS Solutions
4200 Series Sensors

- Appliance solution focused on protecting network devices, services, and applications
- Sophisticated attack detection is provided.



© 2009 Cisco Learning Institute.

Cisco IPS Solutions
Cisco Catalyst 6500 Series IDSM-2

- Switch-integrated intrusion protection module delivering a high-value security service in the core network fabric device
- Support for an unlimited number of VLANs
- Intrusion prevention capability
- Runs the same software image as the Cisco IPS Sensor Appliances



© 2009 Cisco Learning Institute.

IPS Sensors

- Factors that impact IPS sensor selection and deployment:
  - Amount of network traffic
  - Network topology
  - Security budget
  - Available security staff
- Size of implementation
  - Small (branch offices)
  - Large
  - Enterprise

© 2009 Cisco Learning Institute.

Comparing HIPS and Network IPS

	Advantages	Disadvantages
HIPS	▪ Is host-specific ▪ Protects host after decryption ▪ Provides application-level encryption protection	▪ Operating system dependent ▪ Lower level network events not seen ▪ Host is visible to attackers
Network IPS	▪ Is cost-effective ▪ Not visible on the network ▪ Operating system independent ▪ Lower level network events seen	▪ Cannot examine encrypted traffic ▪ Does not know whether an attack was successful

© 2009 Cisco Learning Institute.

Signature Characteristics



- An IDS or IPS sensor matches a signature with a data flow
- The sensor takes action
- Signatures have three distinctive attributes
  - Signature type
  - Signature trigger
  - Signature action

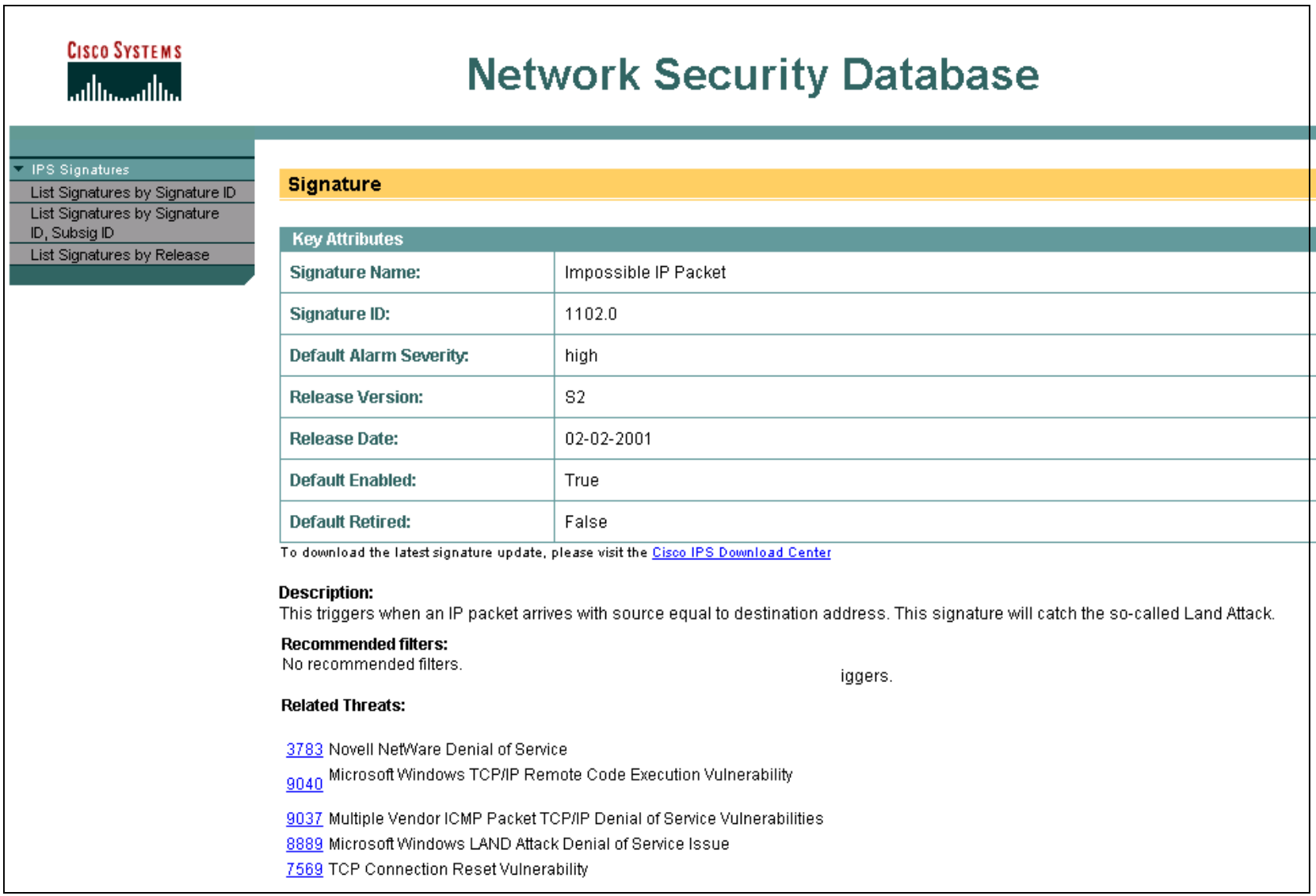
© 2009 Cisco Learning Institute.

Signature Types

- Atomic
  - Simplest form
  - Consists of a single packet, activity, or event
  - Does not require intrusion system to maintain state information
  - Easy to identify
- Composite
  - Also called a stateful signature
  - Identifies a sequence of operations distributed across multiple hosts
  - Signature must maintain a state known as the event horizon

© 2009 Cisco Learning Institute.

Signature File



© 2009 Cisco Learning Institute.

Signature Micro-Engines

Version 4.x SME Prior 12.4(11)T later		
ATOMIC.IP	ATOMIC.IP	Provides simple Layer 3 IP alarms
ATOMIC.ICMP	ATOMIC.IP	Provides simple Internet Control Message Protocol (ICMP) alarms based on the following parameters: type, code, sequence, and ID
ATOMIC.IPOPTIONS	ATOMIC.IP	Provides simple alarms based on the decoding of Layer 3 options
ATOMIC.UDP		Provides simple User Datagram Protocol (UDP) packet alarms based on the following parameters: port,
ATOMIC.TCP		
SERVICE.DNS		
SERVICE.RPC	SERVICE.RPC	Analyzes the remote-procedure call (RPC) service
SERVICE.SMTP	STATE	Inspects Simple Mail Transfer Protocol (SMTP)
SERVICE.HTTP		
SERVICE.FTP		
STRING.TCP		
STRING.UDP		
STRING.ICMP		
MULTI-STRING	MULTI-STRING	Supports flexible pattern matching and supports Trend Labs signatures
OTHER	NORMALIZER	Provides internal engine to handle miscellaneous signatures

Atomic – Examine simple packets

Service – Examine the many services that are attacked

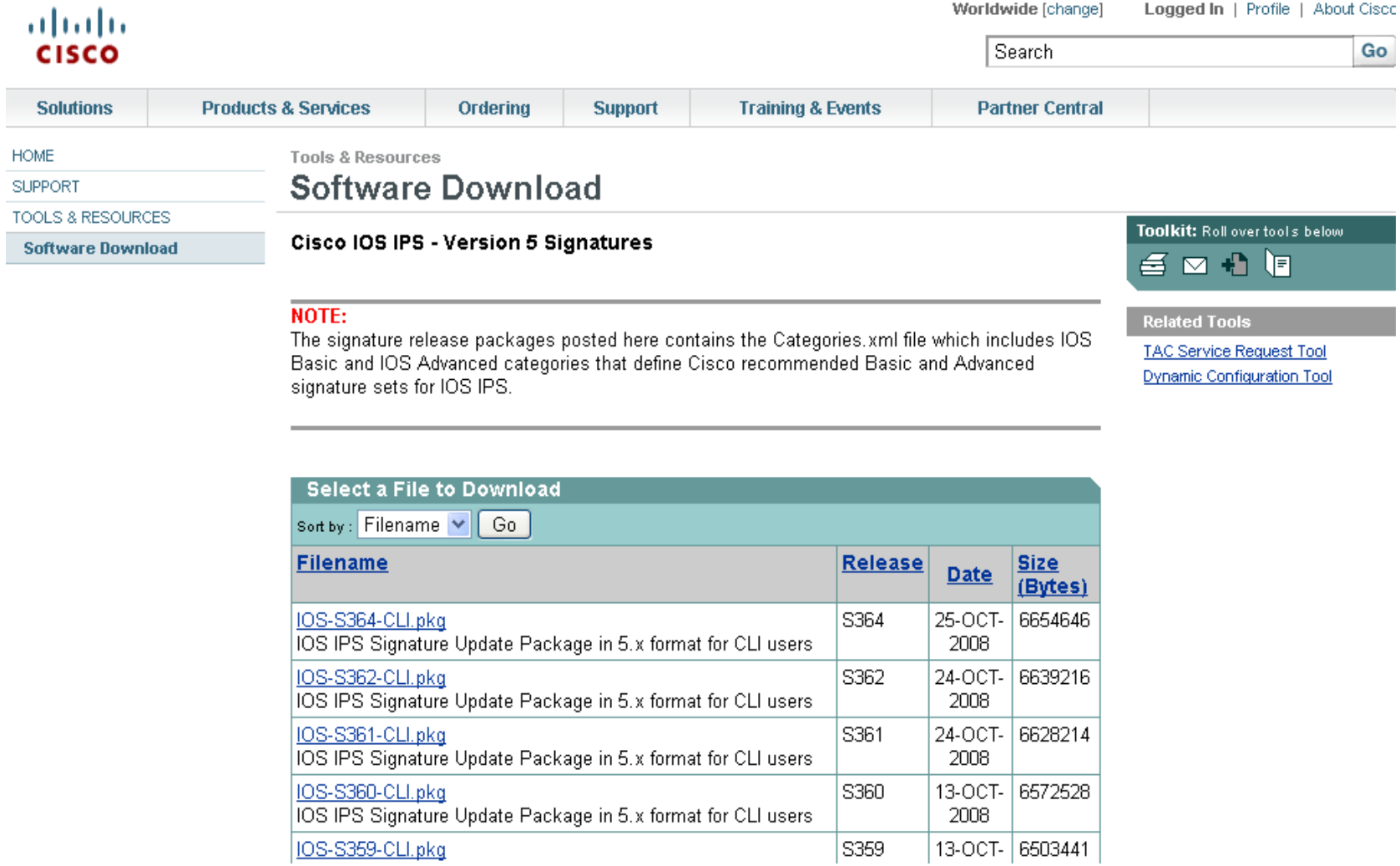
String – Use expression-based patterns to detect intrusions

Multi-String Supports flexible pattern matching

Other – Handles miscellaneous signatures

© 2009 Cisco Learning Institute.

Cisco Signature List



Worldwide [change] Logged In | Profile | About Cisco

Search Go

Solutions | Products & Services | Ordering | Support | Training & Events | Partner Central

HOME
SUPPORT
TOOLS & RESOURCES
Software Download

Tools & Resources

Software Download

Cisco IOS IPS - Version 5 Signatures

Toolkit: Roll over tools below

Related Tools

TAC Service Request Tool
Dynamic Configuration Tool

NOTE:
The signature release packages posted here contains the Categories.xml file which includes IOS Basic and IOS Advanced categories that define Cisco recommended Basic and Advanced signature sets for IOS IPS.

Select a File to Download

Sort by : Filename Go

Filename	Release	Date	Size (Bytes)
IOS-S364-CLI.pkg IOS IPS Signature Update Package in 5.x format for CLI users	S364	25-OCT-2008	6654646
IOS-S362-CLI.pkg IOS IPS Signature Update Package in 5.x format for CLI users	S362	24-OCT-2008	6639216
IOS-S361-CLI.pkg IOS IPS Signature Update Package in 5.x format for CLI users	S361	24-OCT-2008	6628214
IOS-S360-CLI.pkg IOS IPS Signature Update Package in 5.x format for CLI users	S360	13-OCT-2008	6572528
IOS-S359-CLI.pkg	S359	13-OCT-	6503441

© 2009 Cisco Learning Institute.

Signature Triggers

	Advantages	Disadvantages
Pattern-based Detection	• Easy configuration • Fewer false positives • Good signature design	• No detection of unknown signatures • Initially a lot of false positives • Signatures must be created, updated, and tuned
Anomaly-based Detection	• Simple and reliable • Customized policies • Can detect unknown attacks	• Generic output • Policy must be created
Policy-based Detection	• Easy configuration • Can detect unknown attacks	• Difficult to profile typical activity in large networks • Traffic profile must be constant
Honey Pot-Based Detection	• Window to view attacks • Distract and confuse attackers • Slow down and avert attacks • Collect information about attack	• Dedicated honey pot server • Honey pot server must not be trusted

© 2

Pattern-based Detection

Trigger	Signature Type	
	Atomic Signature	**Stateful Signature**
Pattern-based detection	No state required to examine pattern to determine if signature action should be applied	Must maintain state or examine multiple items to determine if signature action should be applied
Example	Detecting for an Address Resolution Protocol (ARP) request that has a source Ethernet address of FF:FF:FF:FF:FF:FF	Searching for the string confidential across multiple packets in a TCP session

© 2009 Cisco Learning Institute.

Anomaly-based Detection

Trigger	Signature Type	
	Atomic Signature	**Stateful Signature**
Anomaly-based detection	No state required to identify activity that deviates from normal profile	State required to identify activity that deviates from normal profile
Example	Detecting traffic that is going to a destination port that is not in the normal profile	Verifying protocol compliance for HTTP traffic

© 2009 Cisco Learning Institute.

Policy-based Detection

Signature Trigger	Signature Type	
	Atomic Signature	**Stateful Signature**
Policy-based detection	No state required to identify undesirable behavior	Previous activity (state) required to identify undesirable behavior
Example	Detecting abnormally large fragmented packets by examining only the last fragment	A SUN Unix host sending RPC requests to remote hosts without initially consulting the SUN PortMapper program.

© 2009 Cisco Learning Institute.

Honey Pot-based Detection

- Uses a dummy server to attract attacks
- Distracts attacks away from real network devices
- Provides a means to analyze incoming types of attacks and malicious traffic patterns

© 2009 Cisco Learning Institute.

Cisco IOS IPS Solution Benefits

- Uses the underlying routing infrastructure to provide an additional layer of security with investment protection
- Attacks can be effectively mitigated to deny malicious traffic from both inside and outside the network
- Provides threat protection at all entry points to the network when combined with other Cisco solutions
- Is supported by easy and effective management tools
- Offers pervasive intrusion prevention solutions that are designed to integrate smoothly into the network infrastructure and to proactively protect vital resources
- Supports approximately 2000 attack signatures from the same signature database that is available for Cisco IPS appliances

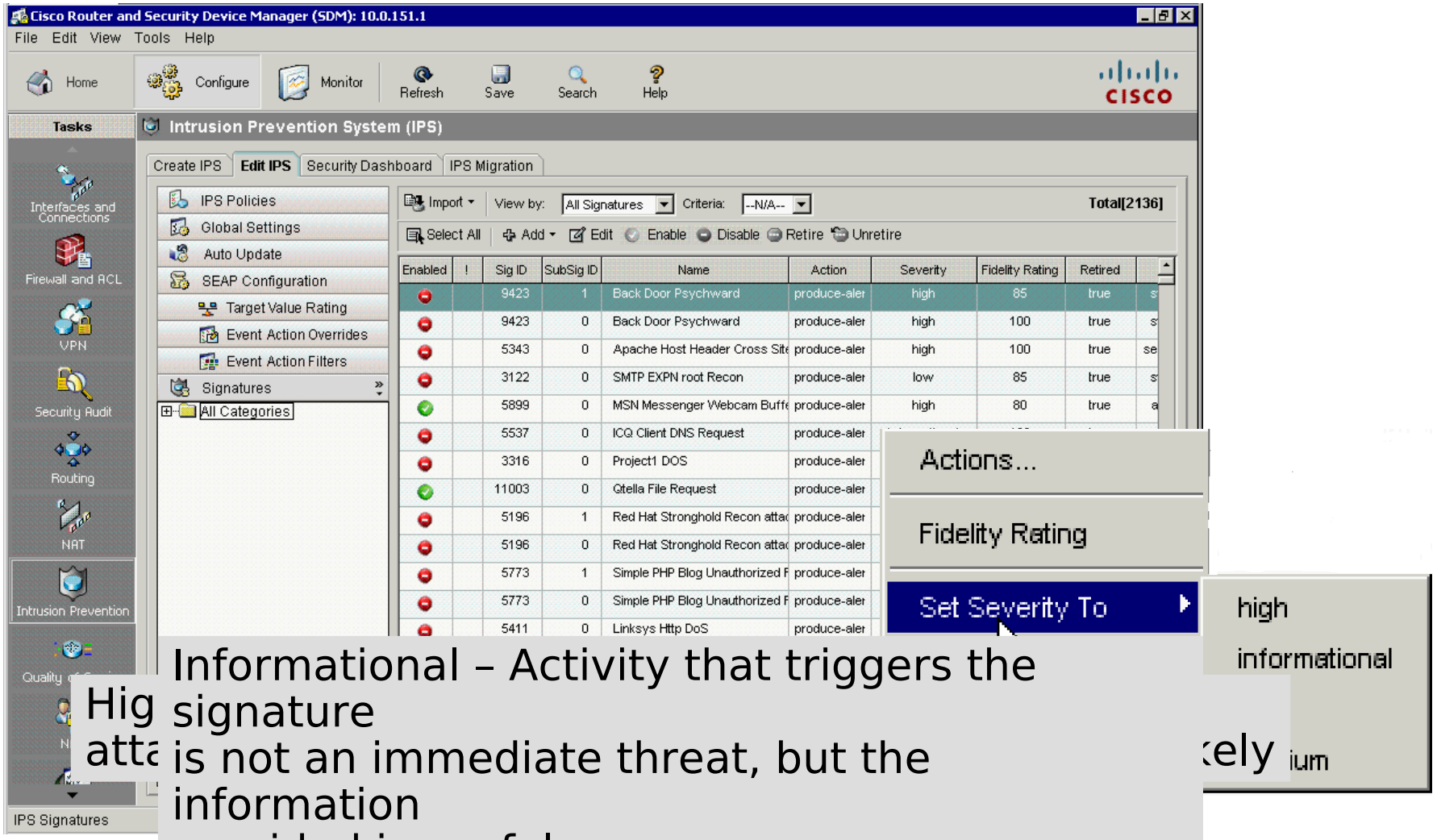
© 2009 Cisco Learning Institute.

Signature Alarms

Alarm Type	Network Activity	IPS Activity	Outcome
False positive	Normal user traffic	Alarm generated	Tune alarm
False negative	Attack traffic	No alarm generated	Tune alarm
True positive	Attack traffic	Alarm generated	Ideal setting
True negative	Normal user traffic	No alarm generated	Ideal setting

© 2009 Cisco Learning Institute.

Signature Tuning Levels



Informational – Activity that triggers the signature is not an immediate threat, but the information provided is useful

© 2009 Cisco Learning Institute.

Generating an Alert

Specific Alert	Description
Produce alert	This action writes the event to the Event Store as an alert.
Produce verbose alert	This action includes an encoded dump of the offending packet in the alert.

© 2009 Cisco Learning Institute.

Logging the Activity

Specific Alert	Description
Log attacker packets	This action starts IP logging on packets that contain the attacker address and sends an alert.
Log pair packets	This action starts IP logging on packets that contain the attacker and victim address pair.
Log victim packets	This action starts IP logging on packets that contain the victim address and sends an alert.

© 2009 Cisco Learning Institute.

Dropping/Preventing the Activity

Specific Alert	Description
Deny attacker inline	• Terminates the current packet and future packets from this attacker address for a period of time. • The sensor maintains a list of the attackers currently being denied by the system. • Entries may be removed from the list manually or wait for the timer to expire. • The timer is a sliding timer for each entry. • If the denied attacker list is at capacity and cannot add a new entry, the packet is still denied.
Deny connection inline	• Terminates the current packet and future packets on this TCP flow.

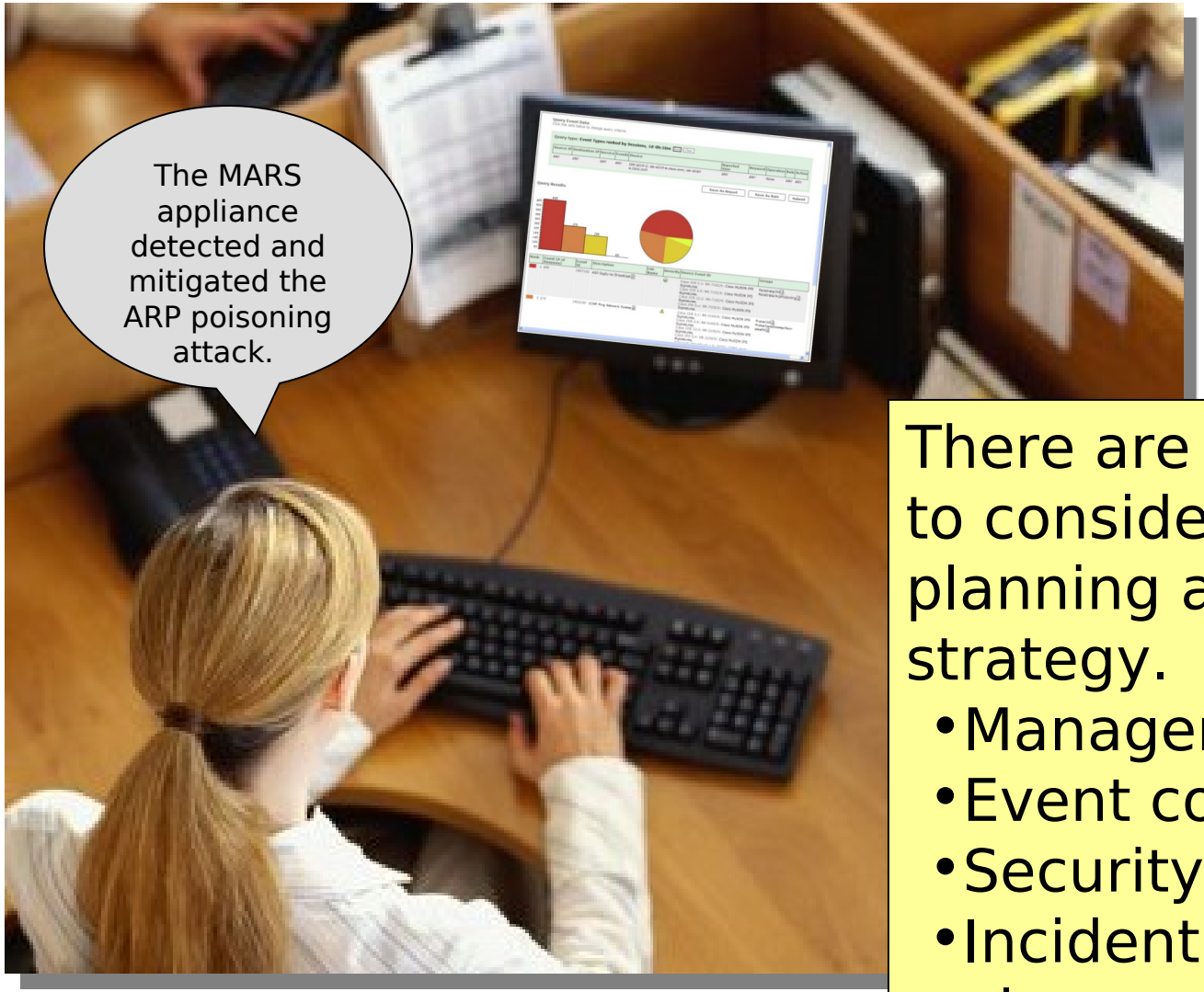
© 200

Resetting a TCP Connection/Blocking Activity/Allowing Activity

Category	Specific Alert	Description
Resetting a TCP connection	Reset TCP connection	• Sends TCP resets to hijack and terminate the TCP flow
Blocking future activity	Request block connection	• This action sends a request to a blocking device to block this connection.
	Request block host	• This action sends a request to a blocking device to block this attacker host.
	Request SNMP trap	• Sends a request to the notification application component of the sensor to perform SNMP notification.
Allowing		• Allows administrator to define

© 2

Planning a Monitoring Strategy

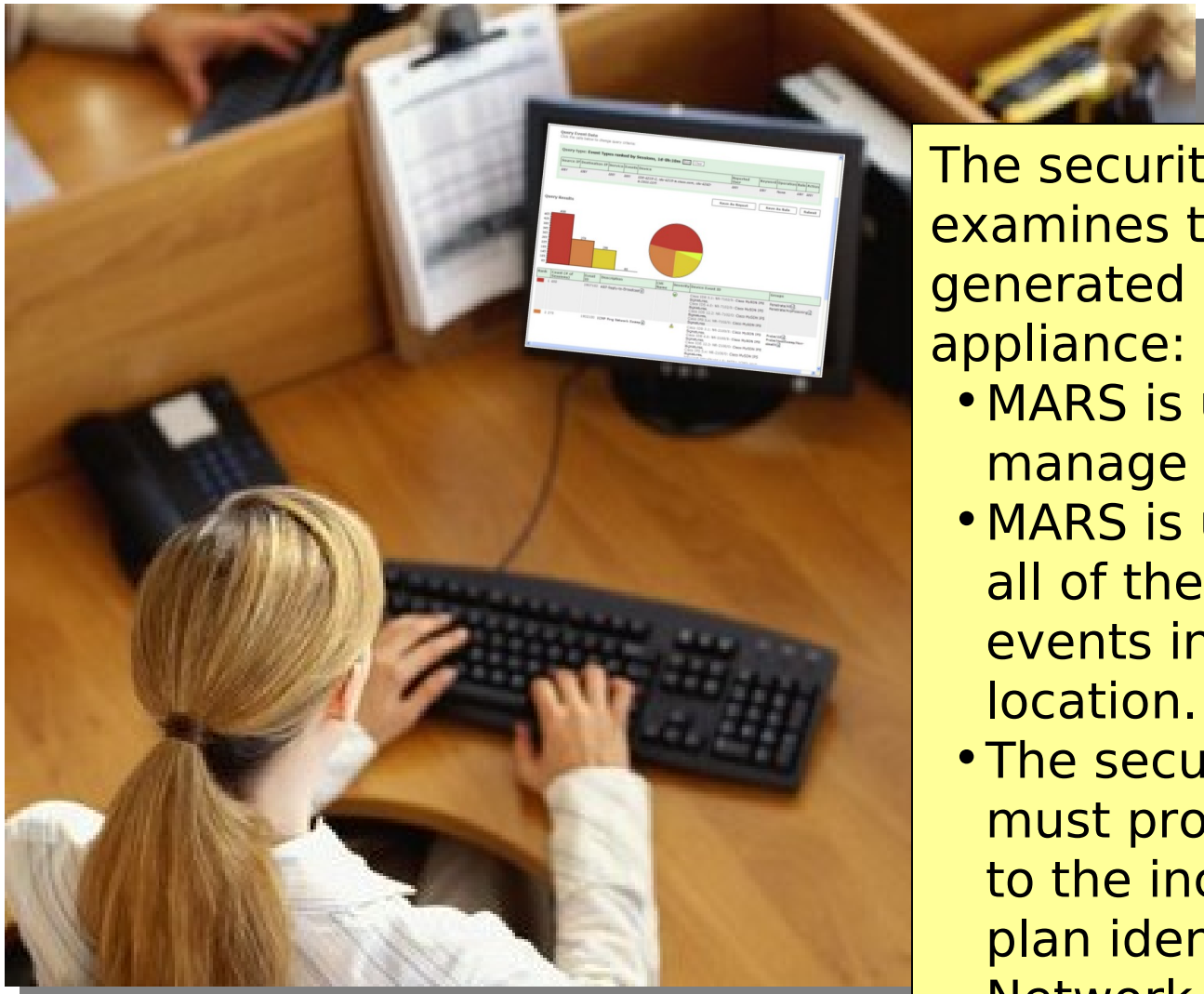


There are four factors to consider when planning a monitoring strategy.

- Management method
- Event correlation
- Security staff
- Incident response plan

© 2009 Cisco Learning Institute.

MARS



The security operator examines the output generated by the MARS appliance:

- MARS is used to centrally manage all IPS sensors.
- MARS is used to correlate all of the IPS and Syslog events in a central location.
- The security operator must proceed according to the incident response plan identified in the Network Security Policy.

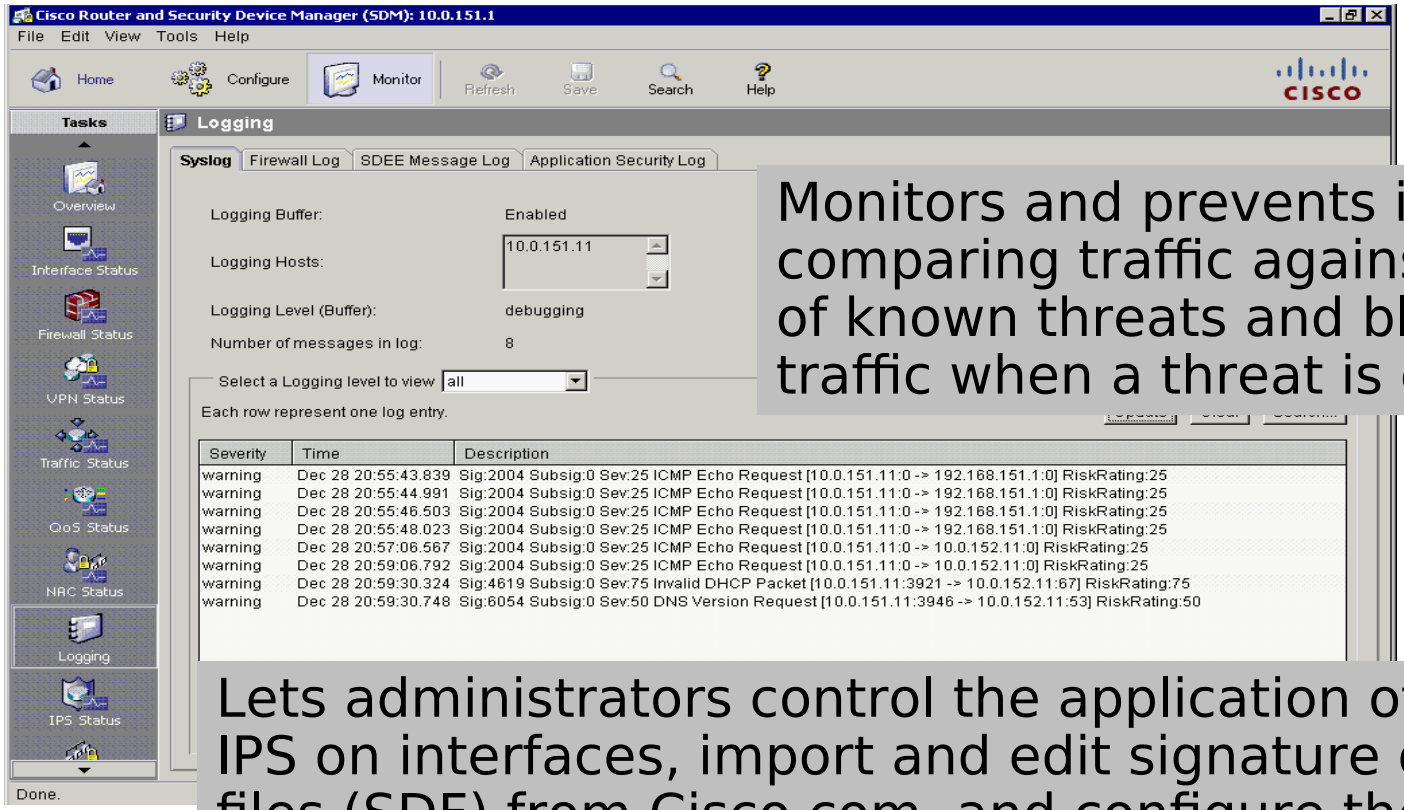
© 2009 Cisco Learning Institute.

Cisco IPS Solutions

- Locally Managed Solutions:
  - Cisco Router and Security Device Manager (SDM)
  - Cisco IPS Device Manager (IDM)
- Centrally Managed Solutions:
  - Cisco IDS Event Viewer (IEV)
  - Cisco Security Manager (CSM)
  - Cisco Security Monitoring, Analysis, and Response System (MARS)

© 2009 Cisco Learning Institute.

Cisco Router and Security Device Manager

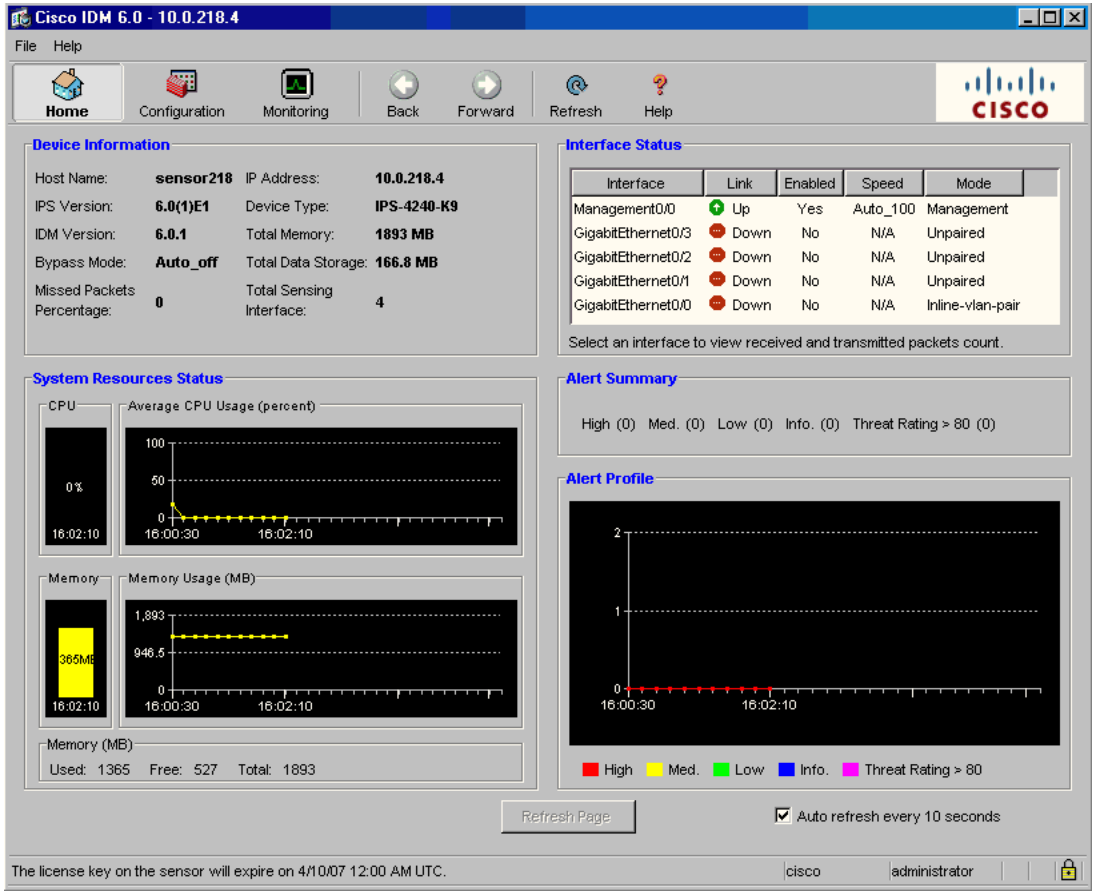


Monitors and prevents intrusions by comparing traffic against signatures of known threats and blocking the traffic when a threat is detected

Lets administrators control the application of Cisco IOS IPS on interfaces, import and edit signature definition files (SDF) from Cisco.com, and configure the action that Cisco IOS IPS is to take if a threat is detected

© 2009 Cisco Learning Institute.

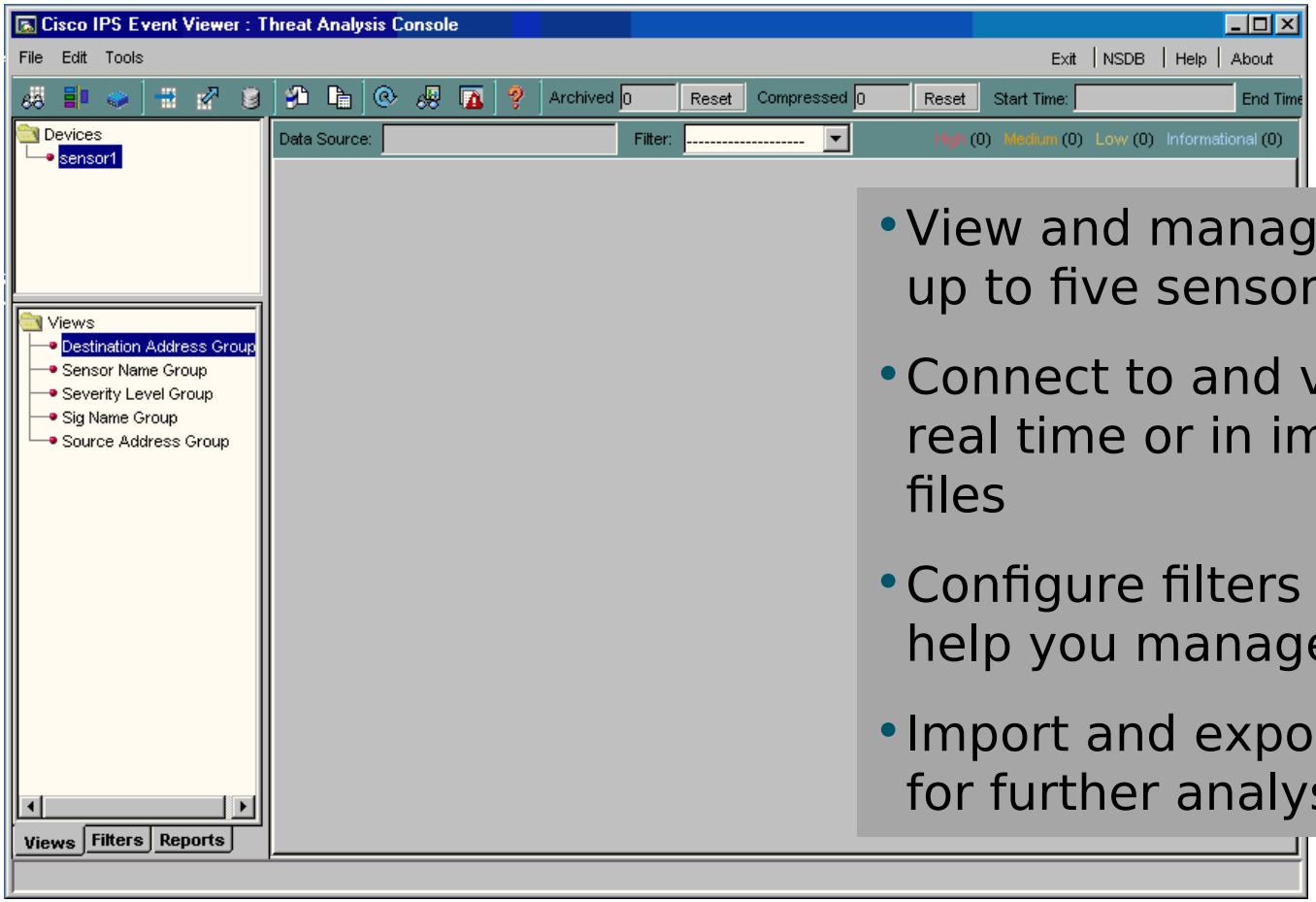
Cisco IPS Device Manager



- A web-based configuration tool
- Shipped at no additional cost with the Cisco IPS Sensor Software
- Enables an administrator to configure and manage a sensor
- The web server resides on the sensor and can be accessed through a web browser

© 2009 Cisco Learning Institute.

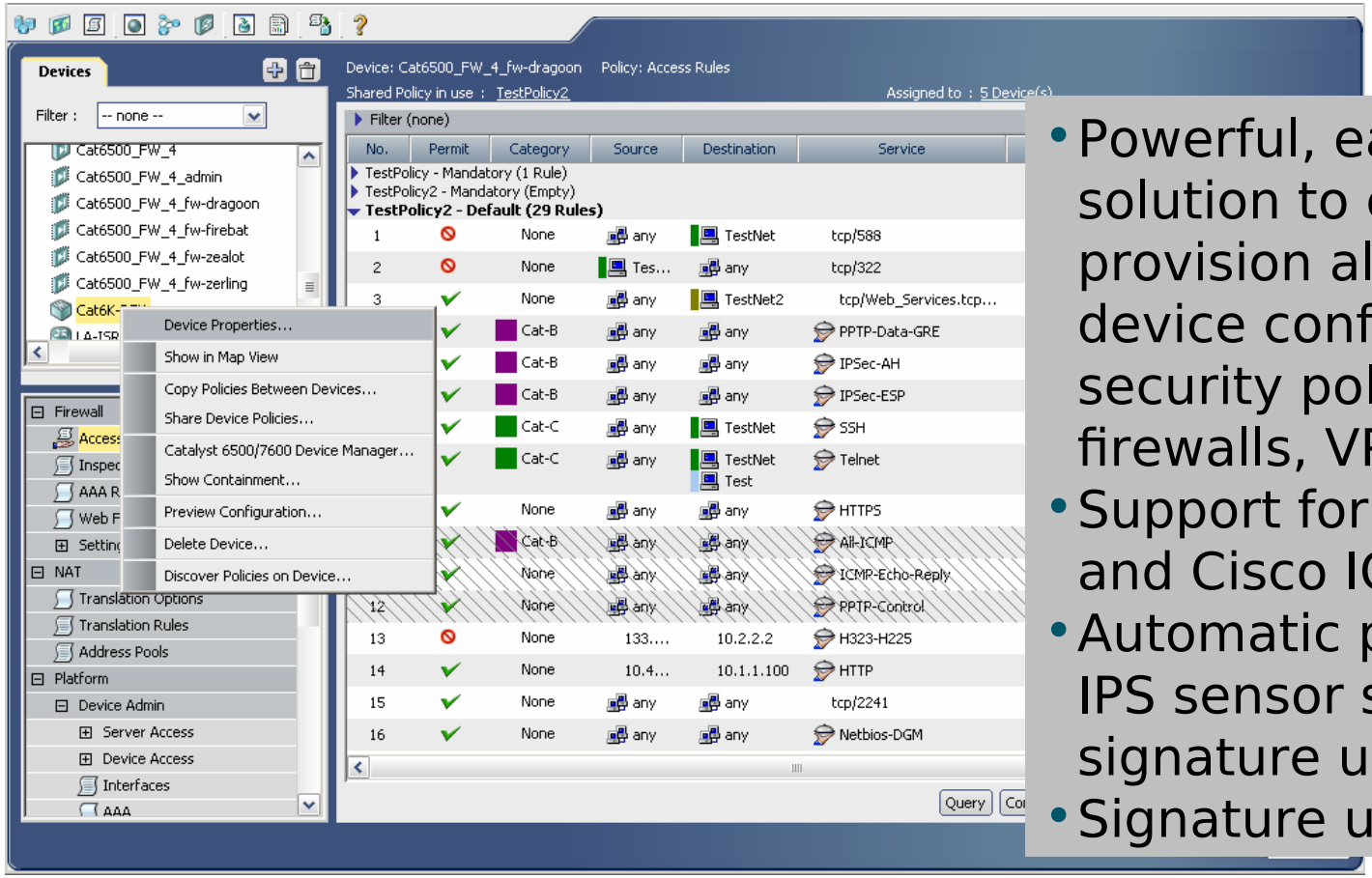
Cisco IPS Event Viewer



- View and manage alarms for up to five sensors
- Connect to and view alarms in real time or in imported log files
- Configure filters and views to help you manage the alarms.
- Import and export event data for further analysis.

© 2009 Cisco Learning Institute.

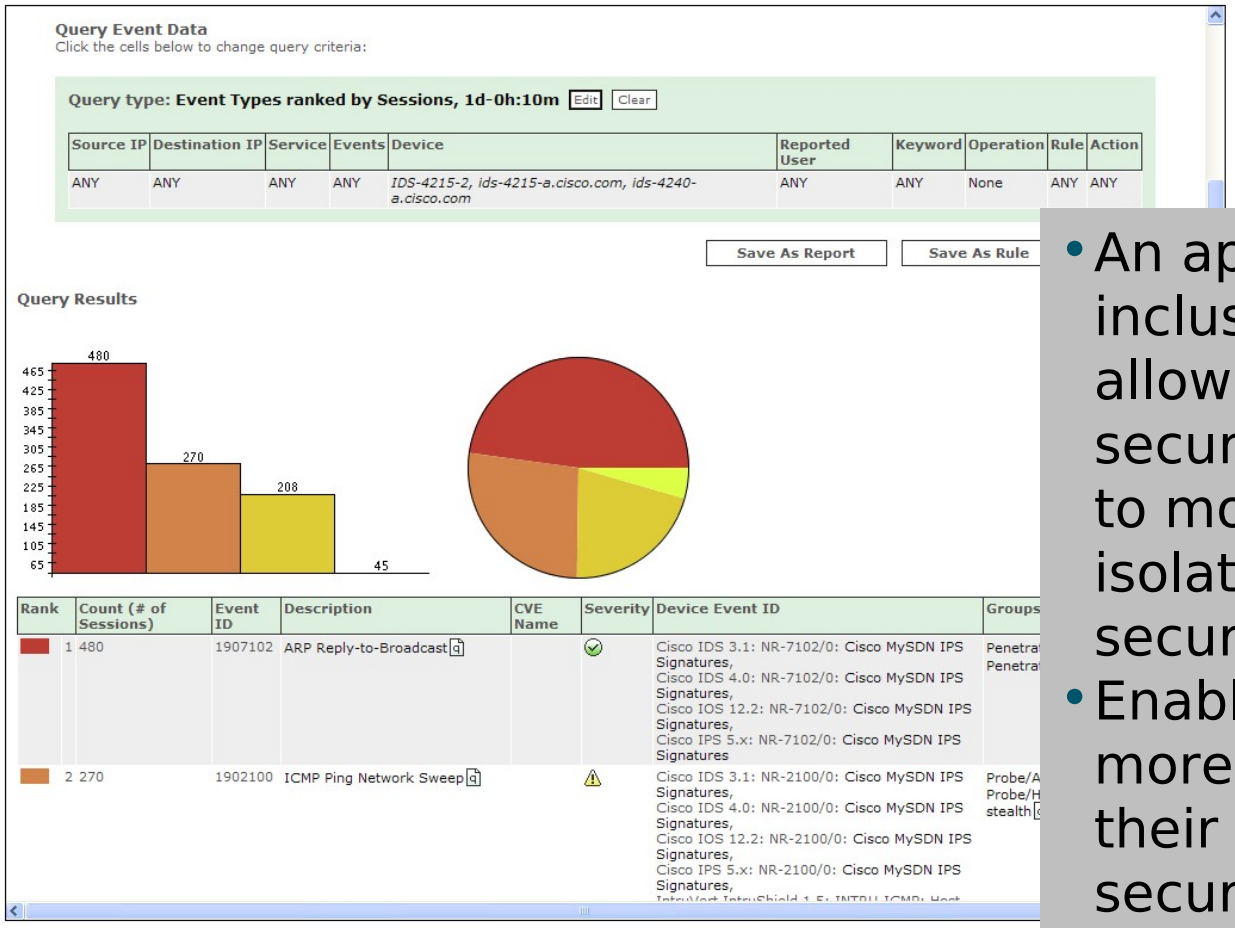
Cisco Security Manager



- Powerful, easy-to-use solution to centrally provision all aspects of device configurations and security policies for Cisco firewalls, VPNs, and IPS
- Support for IPS sensors and Cisco IOS IPS
- Automatic policy-based IPS sensor software and signature updates
- Signature update wizard

© 2009 Cisco Learning Institute.

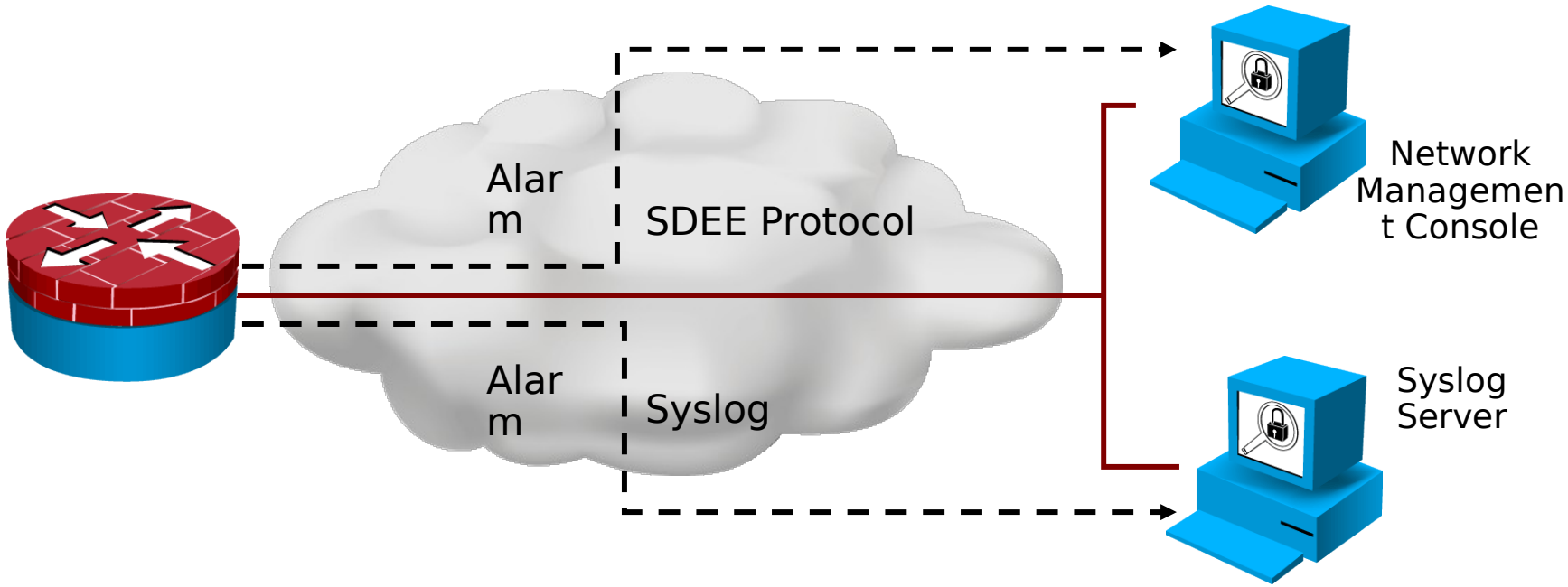
Cisco Security Monitoring Analytic and Response System



- An appliance-based, all-inclusive solution that allows network and security administrators to monitor, identify, isolate, and counter security threats
- Enables organizations to more effectively use their network and security resources.
- Works in conjunction with Cisco CSM.

© 2009 Cisco Learning Institute.

Secure Device Event Exchange



- The SDEE format was developed to improve communication of events generated by security devices
- Allows additional event types to be included as they are defined

© 2009 Cisco Learning Institute.

Best Practices

- The need to upgrade sensors with the latest signature packs must be balanced against the momentary downtime.
- When setting up a large deployment of sensors, automatically update signature packs rather than manually upgrading every sensor.
- When new signature packs are available, download the new signature packs to a secure server within the management network. Use another IPS to protect this server from attack by an outside party.
- Place the signature packs on a dedicated FTP server within the management network. If a signature update is not available, a custom signature can be created to detect and mitigate a specific attack.

© 2009 Cisco Learning Institute.

Best Practices

- Configure the FTP server to allow read-only access to the files within the directory on which the signature packs are placed only from the account that the sensors will use.
- Configure the sensors to automatically update the signatures by checking the FTP server for the new signature packs periodically. Stagger the time of day when the sensors check the FTP server for new signature packs.
- The signature levels that are supported on the management console must remain synchronized with the signature packs on the sensors themselves.

© 2009 Cisco Learning Institute.

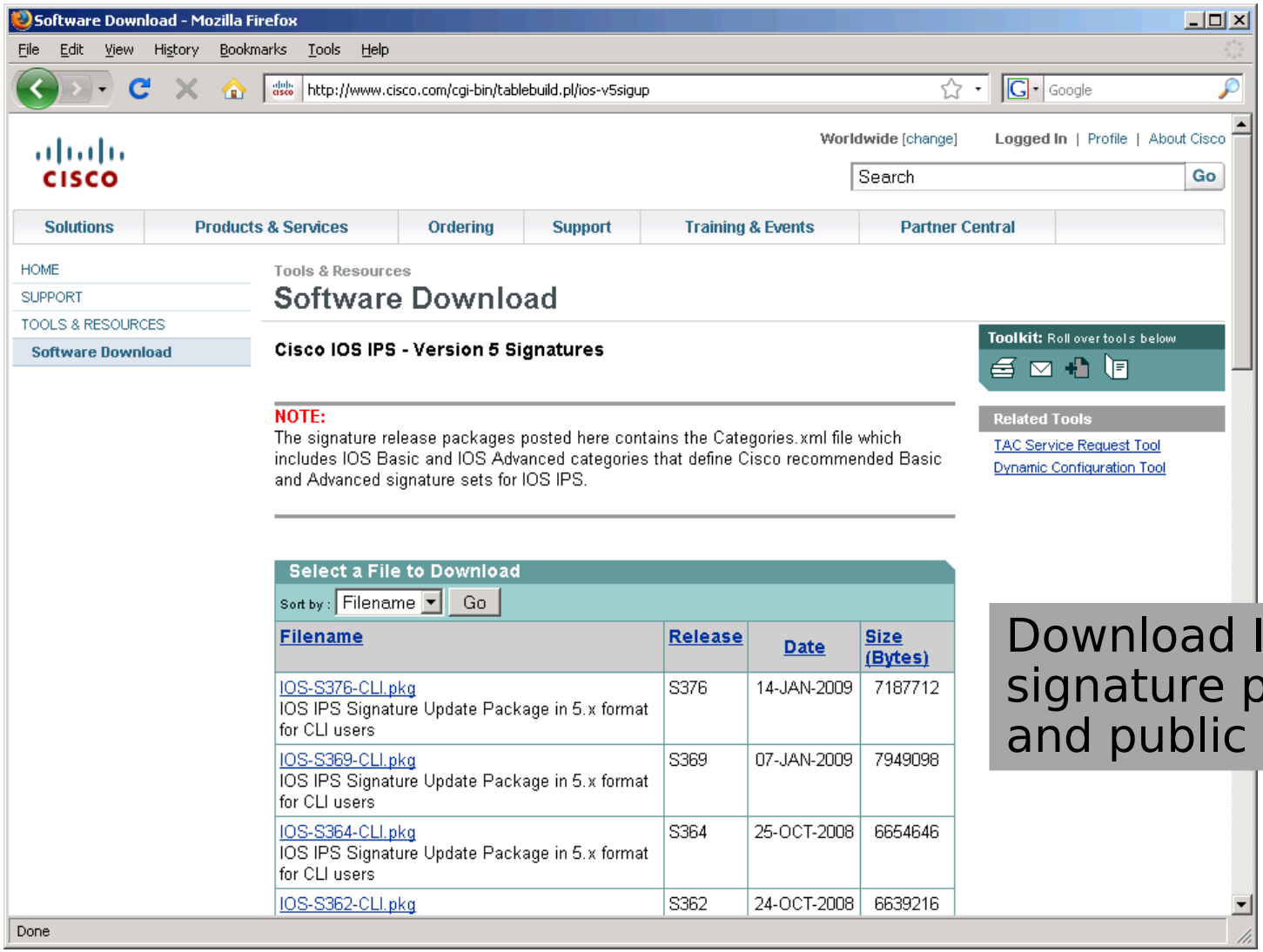
Overview of Implementing IOS IPS



1. Download the IOS IPS files
2. Create an IOS IPS configuration directory on Flash
3. Configure an IOS IPS crytpo key
4. Enable IOS IPS
5. Load the IOS IPS Signature Package to the router

© 2009 Cisco Learning Institute.

1. Download the Signature File



Download IOS IPS signature package files and public crypto key

© 2009 Cisco Learning Institute.

2. Create Directory

```
R1# mkdir ips
Create directory filename [ips]?
Created dir flash:ips
R1#
R1# dir flash:
Directory of flash:/
   5 -rw-   51054864 Jan 10 2009 15:46:14 -08:00
                     c2800nm-advipservicesk9-mz.124-20.T1.bin
   6 drw-          0 Jan 15 2009 11:36:36 -08:00 ips
64016384 bytes total (12693504 bytes free)
R1#
```

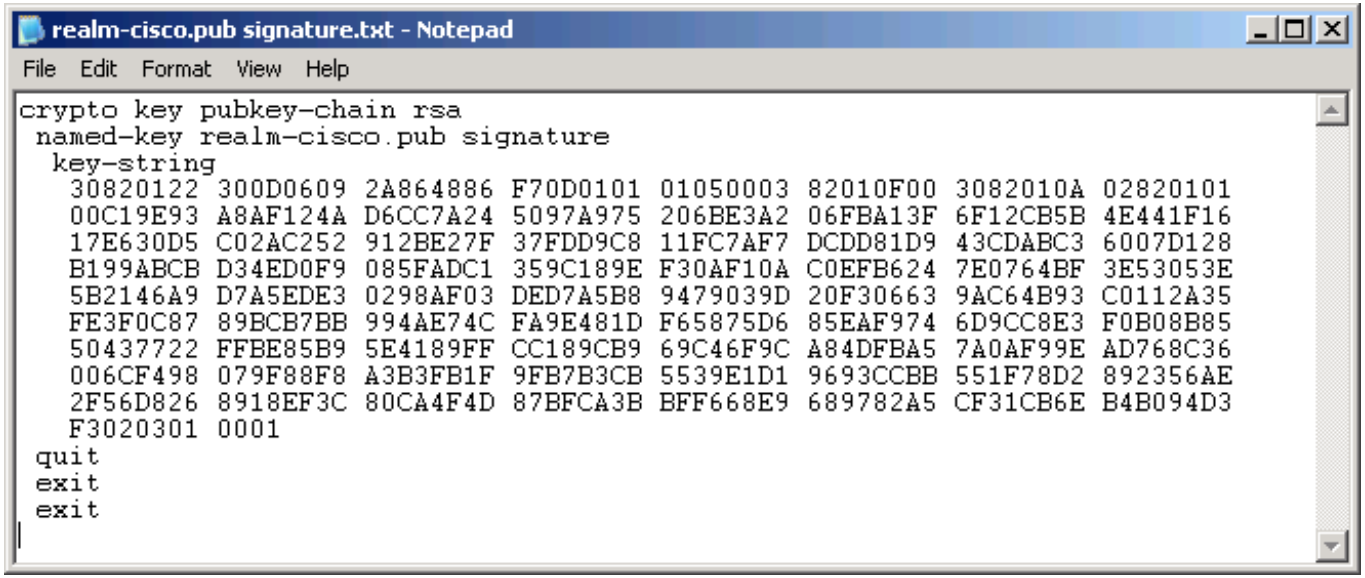
To rename a directory:

```
R1# rename ips ips_new
Destination filename [ips_new]?
R1#
```

© 2009 Cisco Learning Institute.

3. Configure the Crypto Key

1



2

```
R1# conf t
R1(config)#
```

1 – Highlight and copy the text contained in the public key file.

2 – Paste it in global configuration mode.

© 2009 Cisco Learning Institute.

Confirm the Crypto Key

```
R1# show run

<Output omitted>

crypto key pubkey-chain rsa
named-key realm-cisco.pub signature
key-string
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001

<Output omitted>
```

© 2009 Cisco Learning Institute.

4. Enable IOS IPS

1

2

```
R1(config)# ip ips name iosips
R1(config)# ip ips name ips list ?
<1-199> Numbered access list
WORD Named access list
R1(config)#
R1(config)# ip ips config loc
R1(config)#
```

1 – IPS rule is created

2 – IPS location in flash identified

3

```
R1(config)# ip http server
R1(config)# ip ips notify sdee
R1(config)# ip ips notify log
R1(config)#
```

3 – SDEE and Syslog notification are enabled

© 2009 Cisco Learning Institute.

4. Enable IOS IPS

1

```
R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# retired tru
R1(config-ips-category-action)# exit
R1(config-ips-category)#
```

1 – The IPS **all** category is retired

2

```
R1(config-ips-category)# category ios_
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit
Do you want to accept these changes? [confirm] y
R1(config)#
```

2 – The IPS **basic** category is unretired.

3

```
R1(config)# interface GigabitEthernet 0/1
R1(config-if)# ip ips iosips in
R1(config-if)# exit
R1(config)#exit
```

3 – The IPS rule is applied in a incoming direction

4

```
R1(config)# interface GigabitEthernet 0/1
R1(config-if)# ip ips iosips in
R1(config-if)# ip ips iosips out
R1(config-if)# exit
R1(config)# exit
```

4 – The IPS rule is applied in an incoming and outgoing direction.

© 2009 Cisco Learning Institute.

5. Load Signature Package

1 – Copy the signatures from the FTP server.

1

2

```
R1# copy ftp://cisco:cisco@10.1.1.1/IOS-S376-CLI.pkg idconf
Loading IOS-S310-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7608873/4096 bytes]
*Jan 15 16:44:47 PST: %IPS-6-ENGINE_BUILDS_STARTED: 16:44:47 PST Jan 15 2008
*Jan 15 16:44:47 PST: %IPS-6-ENGINE_BUILDING: multi-string - 8 signatures - 1 of 13 engines
*Jan 15 16:44:47 PST: %IPS-6-ENGINE_READY: multi-string - build time 4 ms - packets for this
                      engine will be scanned
*Jan 15 16:44:47 PST: %IPS-6-ENGINE_BUILDING: service-http - 622 signatures - 2 of 13 engines
*Jan 15 16:44:53 PST: %IPS-6-ENGINE_READY: service-http - build time 6024 ms - packets for this
                       engine will be scanned

<Output omitted>

*Jan 15 16:45:18 PST: %IPS-6-ENGINE_BUILDING: service-smb-advanced - 35 signatures - 12 of 13
engines
*Jan 15 16:45:18 PST: %IPS-6-ENGINE_READY: service-smb-advanced - build time 16 ms - packets
                       for this engine will be scanned
*Jan 15 16:45:18 PST: %IPS-6-ENGINE_BUILDING: service-msrpc - 25 signatures - 13 of 13 engines
*Jan 15 16:45:18 PST: %IPS-6-ENGINE_READY: service-msrpc - build time 32 ms - packets for this
                      engine will be scanned
*Jan 15 16:45:18 PST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 31628 ms
```

2 – Signature compiling begins immediately after the signature package is loaded to the router.

© 2009 Cisco Learning Institute.

Verify the Signature

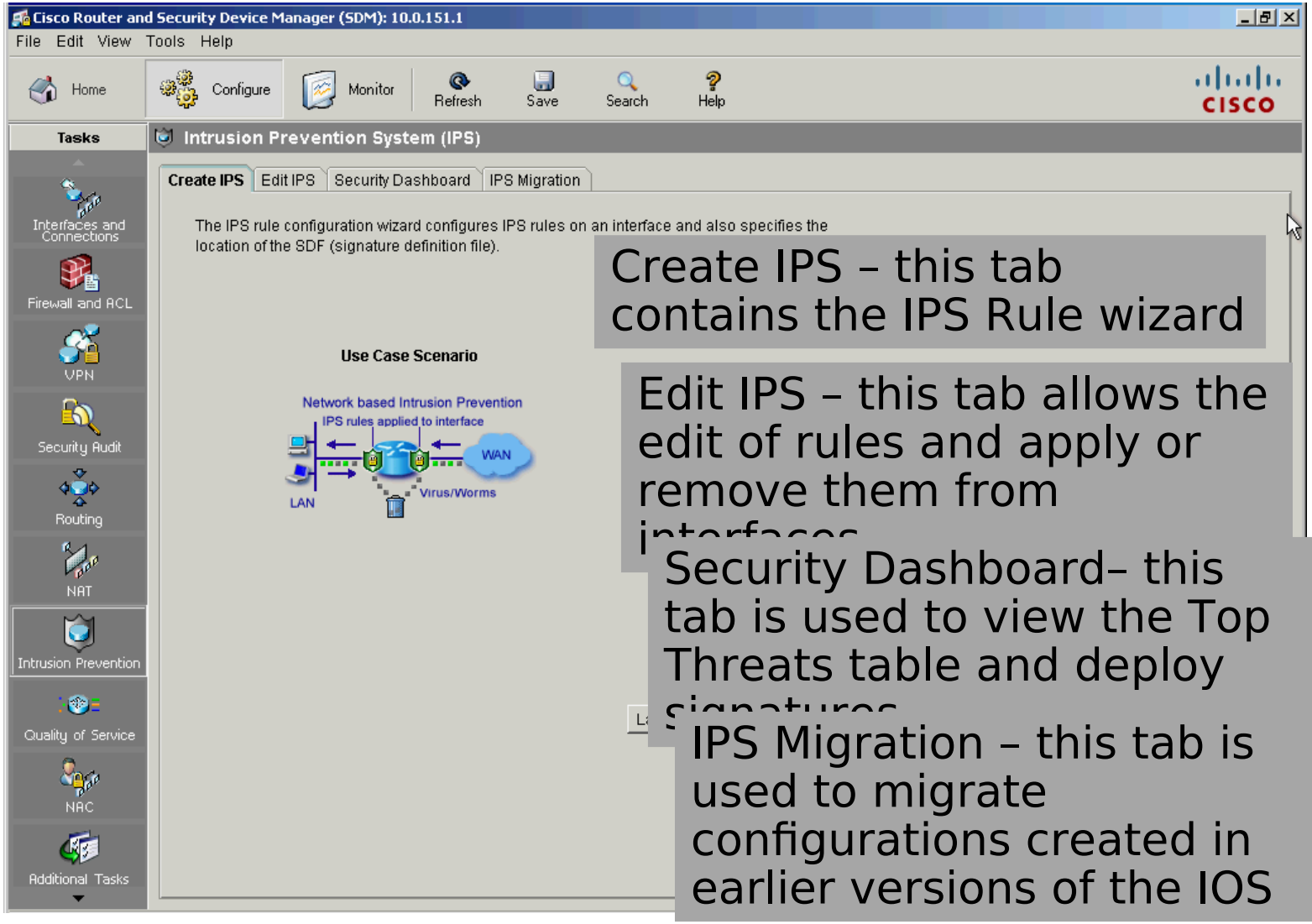
```
R1# show ip ips signature count
Cisco SDF release version S310.0 ← signature package release version
Trend SDF release version V0.0
Signature Micro-Engine: multi-string: Total Signatures 8
multi-string enabled signatures: 8
multi-string retired signatures: 8

<Output omitted>

Signature Micro-Engine: service-msrpc: Total Signatures 25
service-msrpc enabled signatures: 25
service-msrpc retired signatures: 18
service-msrpc compiled signatures: 1
service-msrpc inactive signatures - invalid params: 6
Total Signatures: 2136
Total Enabled Signatures: 807
Total Retired Signatures: 1779
Total Compiled Signatures:
      351 ← total compiled signatures for the IOS IPS Basic category
Total Signatures with invalid parameters: 6
Total Obsoleted Signatures: 11
R1#
```

© 2009 Cisco Learning Institute.

Configuring Cisco IOS IPS in SDM



Create IPS – this tab contains the IPS Rule wizard

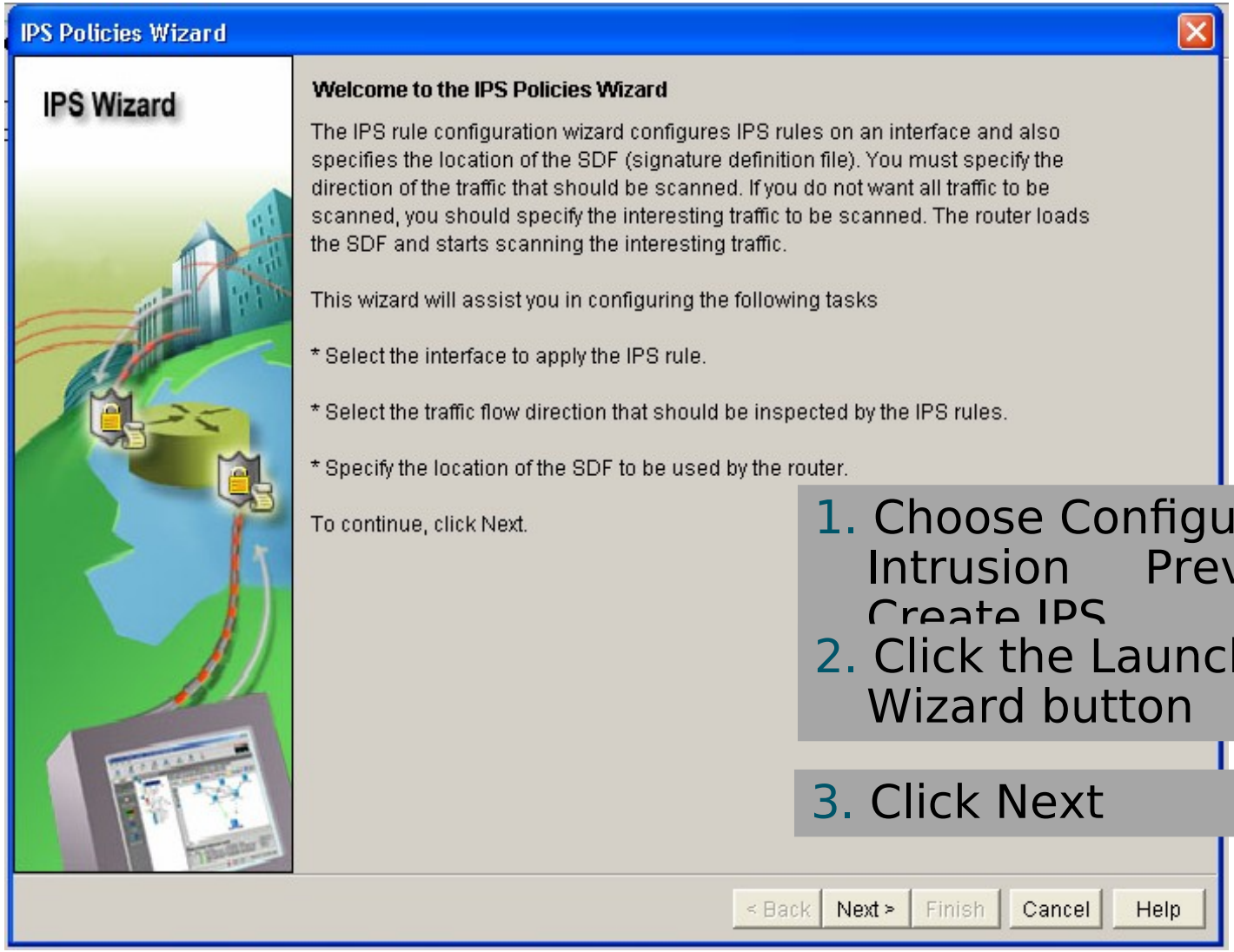
Edit IPS – this tab allows the edit of rules and apply or remove them from interfaces

Security Dashboard– this tab is used to view the Top Threats table and deploy signatures

IPS Migration – this tab is used to migrate configurations created in earlier versions of the IOS

© 2009 Cisco Learning Institute.

Using SDM

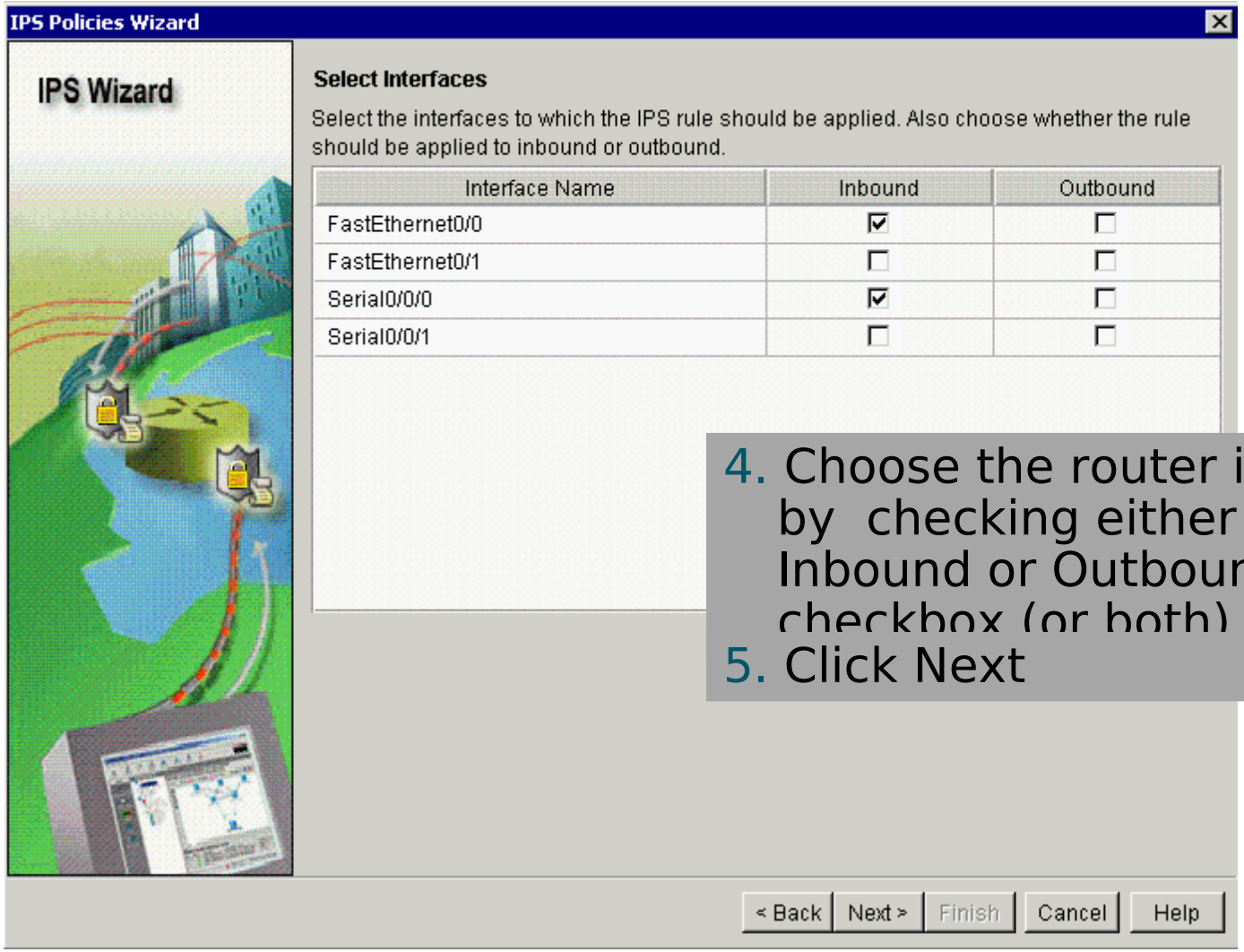


1. Choose Configure > Intrusion Prevention > Create IPS
2. Click the Launch IPS Rule Wizard button

3. Click Next

© 2009 Cisco Learning Institute.

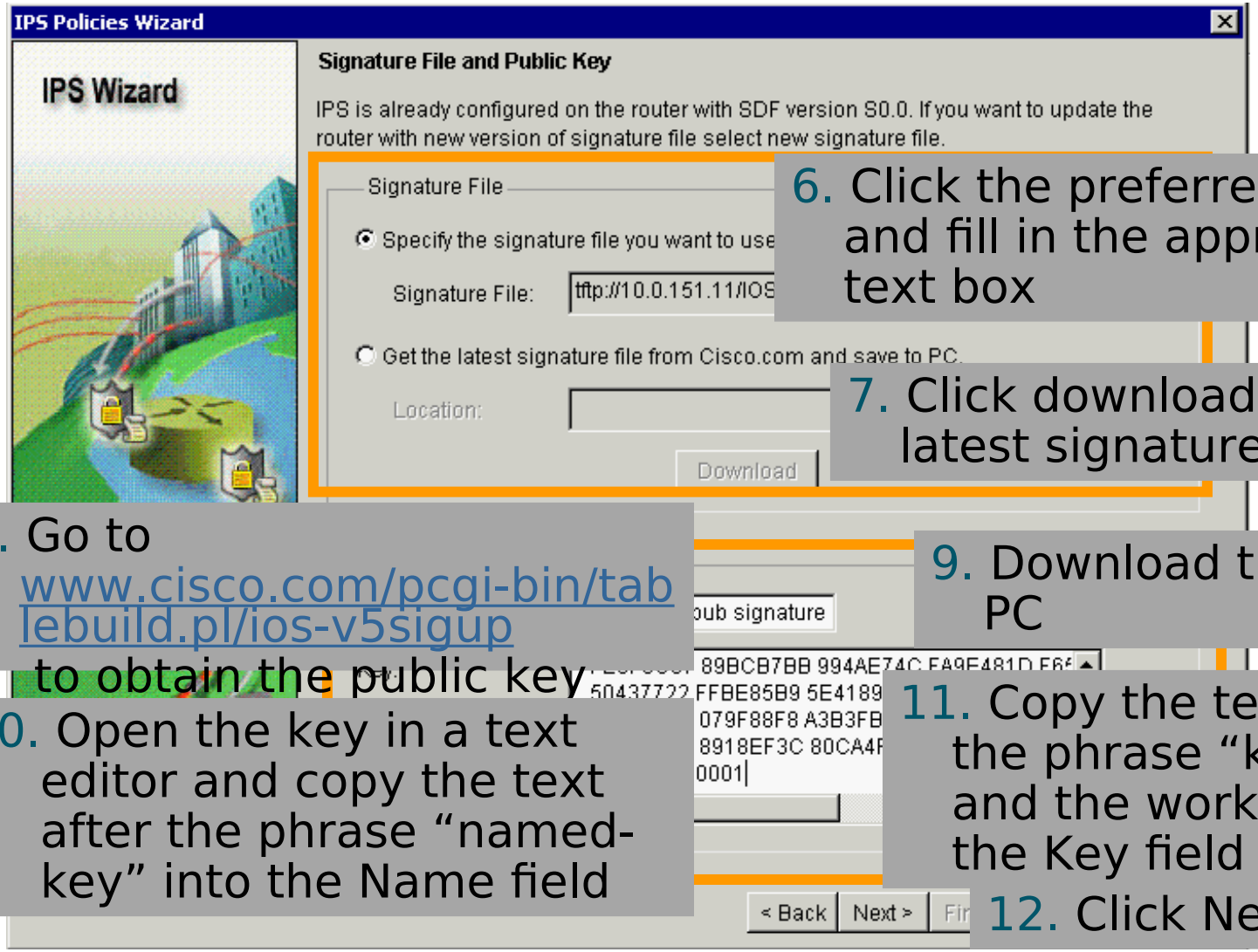
Using SDM



4. Choose the router interface by checking either the Inbound or Outbound checkbox (or both)
5. Click Next

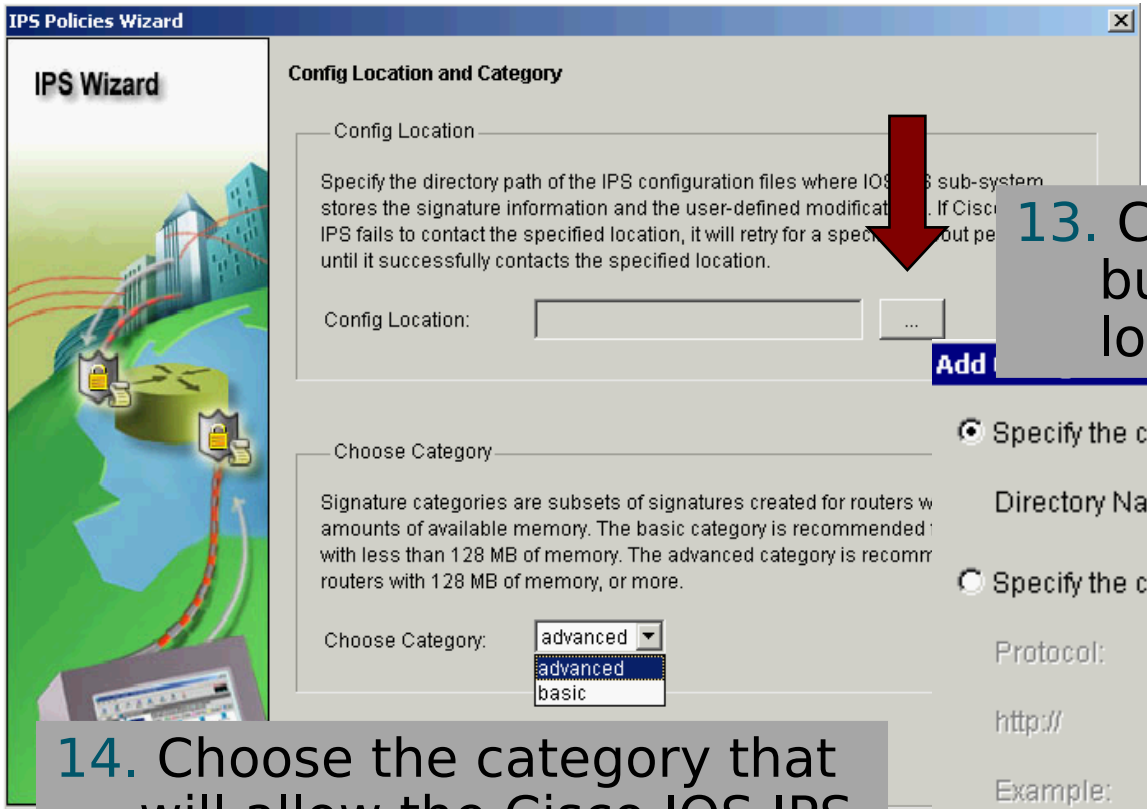
© 2009 Cisco Learning Institute.

Using SDM

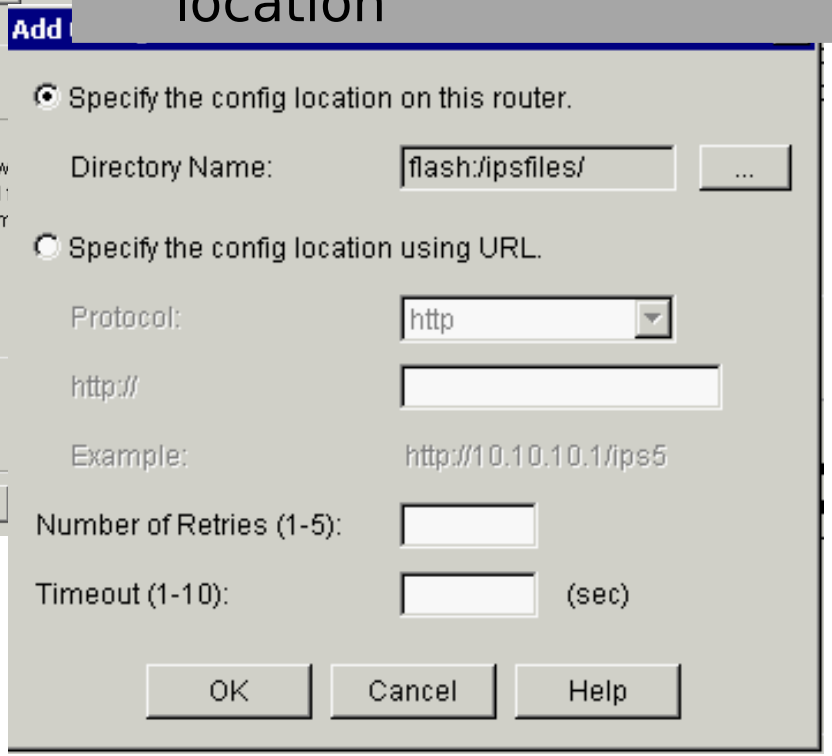


© 2009 Cisco Learning Institute.

Using SDM



13. Click the ellipsis (…) button and enter config location

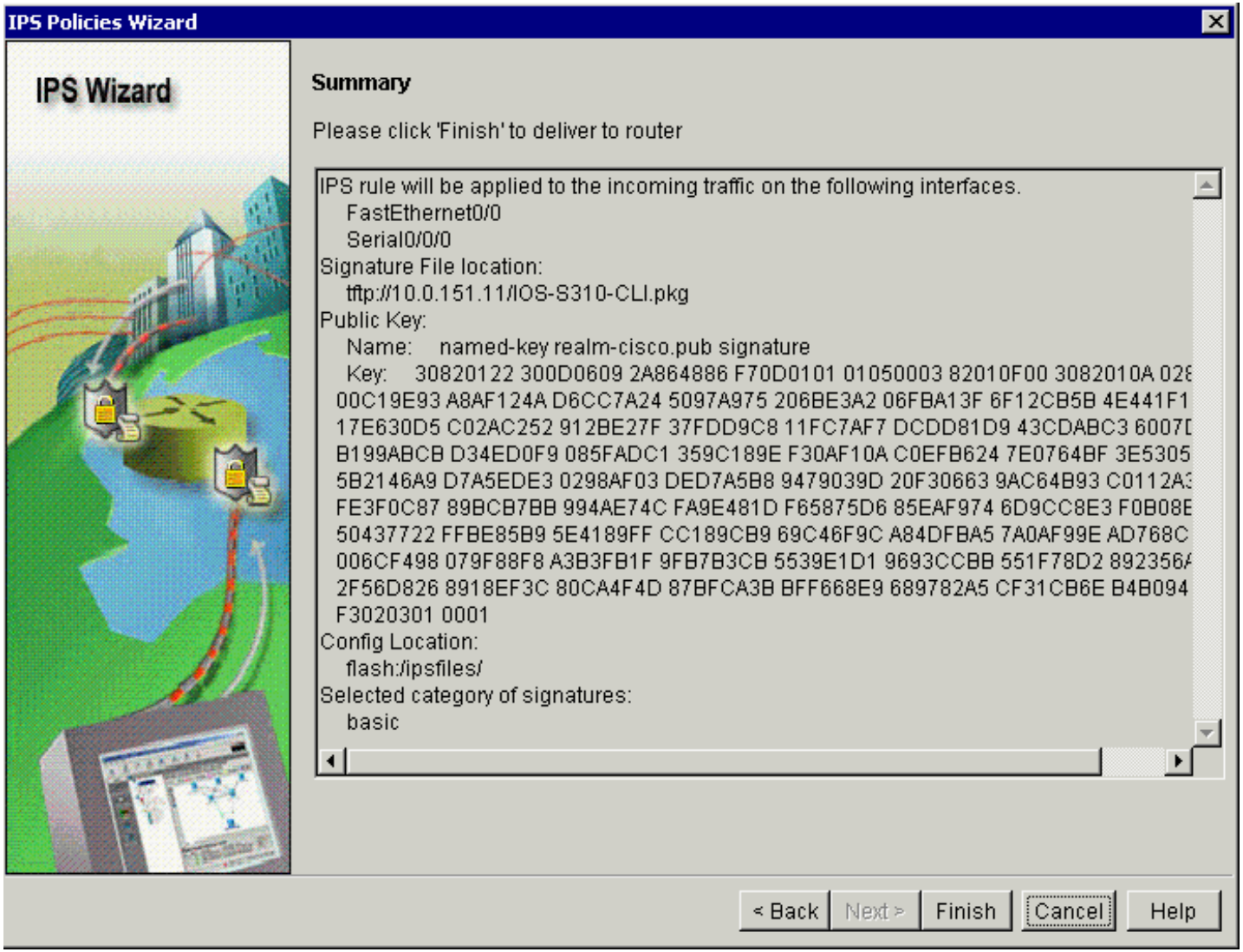


14. Choose the category that will allow the Cisco IOS IPS to function efficiently on the router

15. Click finish

© 2009 Cisco Learning Institute.

SDM IPS Wizard Summary



© 2009 Cisco Learning Institute.

Generated CLI Commands

```
R1# show run

<Output omitted>

ip ips name sdm_ips_rule
ip ips config location flash:/ipsdir/ retries 1
ip ips notify SDEE
!
ip ips signature-category
  category all
   retired true
  category ios_ips basic
   retired false
!
interface Serial0/0/0
 ip ips sdm_ips_rule in
 ip virtual-reassembly

<Output omitted>
```

© 2009 Cisco Learning Institute.

Using CLI Commands

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip ips signature-definition
R1(config-sigdef)# signature 6130 10
R1(config-sigdef-sig)# status
R1(config-sigdef-sig-status)# retired true
R1(config-sigdef-sig-status)# exit
R1(config-sigdef-sig)# exit
R1(config-sigdef)# exit
Do you want to accept these changes? [confirm] y
R1(config)#
```

This example shows how to retire individual signatures. In this case, signature 6130 with subsig ID of 10.

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip ips signature-category
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit
Do you want to accept these changes? [confirm] y
R1(config)#
```

This example shows how to unretire all signatures that belong to the IOS IPS Basic category.

© 2009 Cisco Learning Institute.

Using CLI Commands for Changes

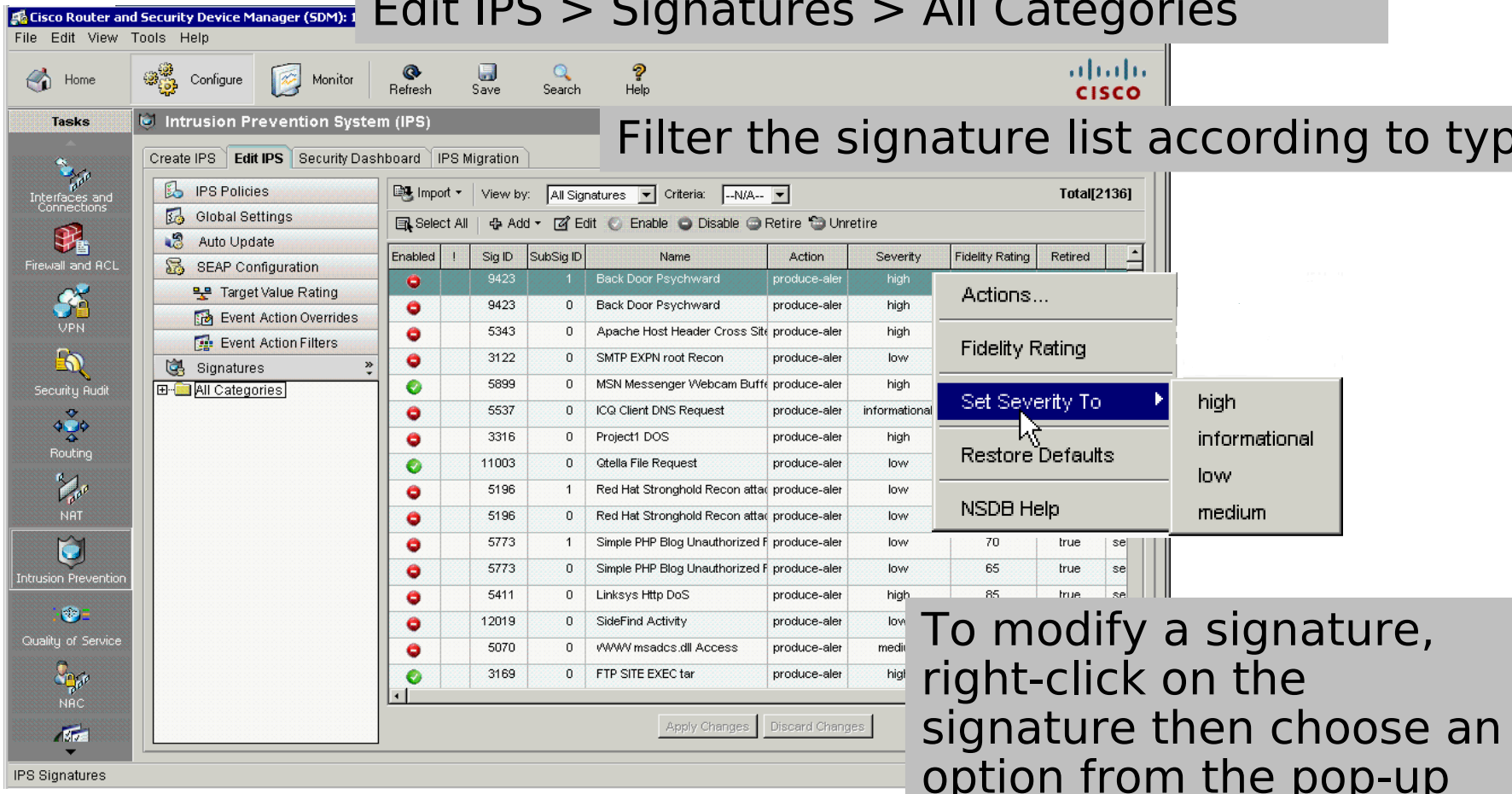
```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip ips signature-definition
R1(config-sigdef)# signature 6130 10
R1(config-sigdef-sig)# engine
R1(config-sigdef-sig-engine)# event-action produce-alert
R1(config-sigdef-sig-engine)# event-action deny-packet-inline
R1(config-sigdef-sig-engine)# event-action reset-tcp-connection
R1(config-sigdef-sig-engine)# exit
R1(config-sigdef-sig)# exit
R1(config-sigdef)# exit
Do you want to accept these changes? [confirm] y
R1(config)#
```

This example shows how to change signature actions to alert, drop, and reset for signature 6130 with subsig ID of 10.

© 2009 Cisco Learning Institute.

Viewing Configured Signatures

Choose Configure > Intrusion Prevention > Edit IPS > Signatures > All Categories



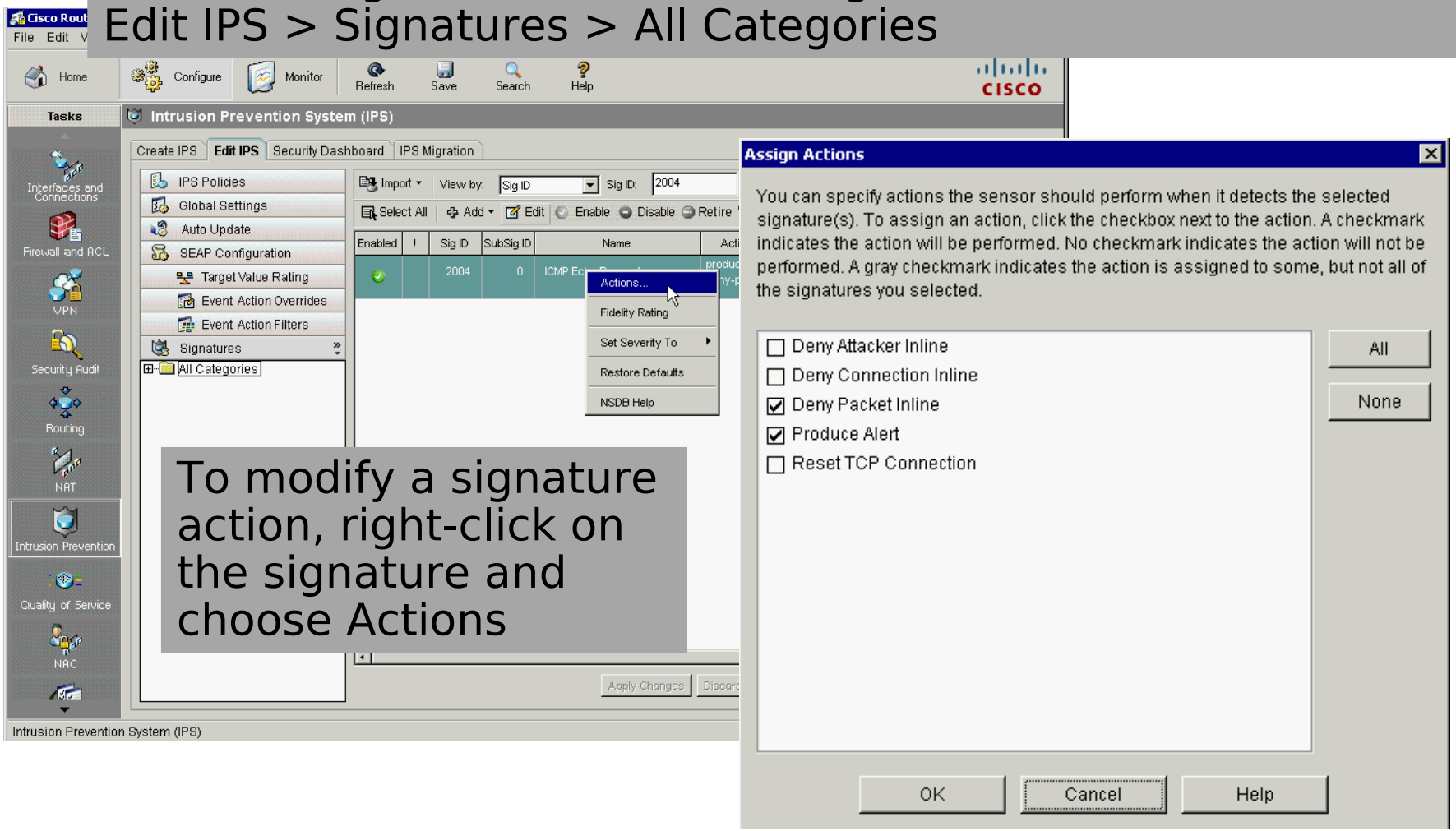
Filter the signature list according to type

To modify a signature, right-click on the signature then choose an option from the pop-up

© 2009 Cisco Learning Institute.

Modifying Signature Actions

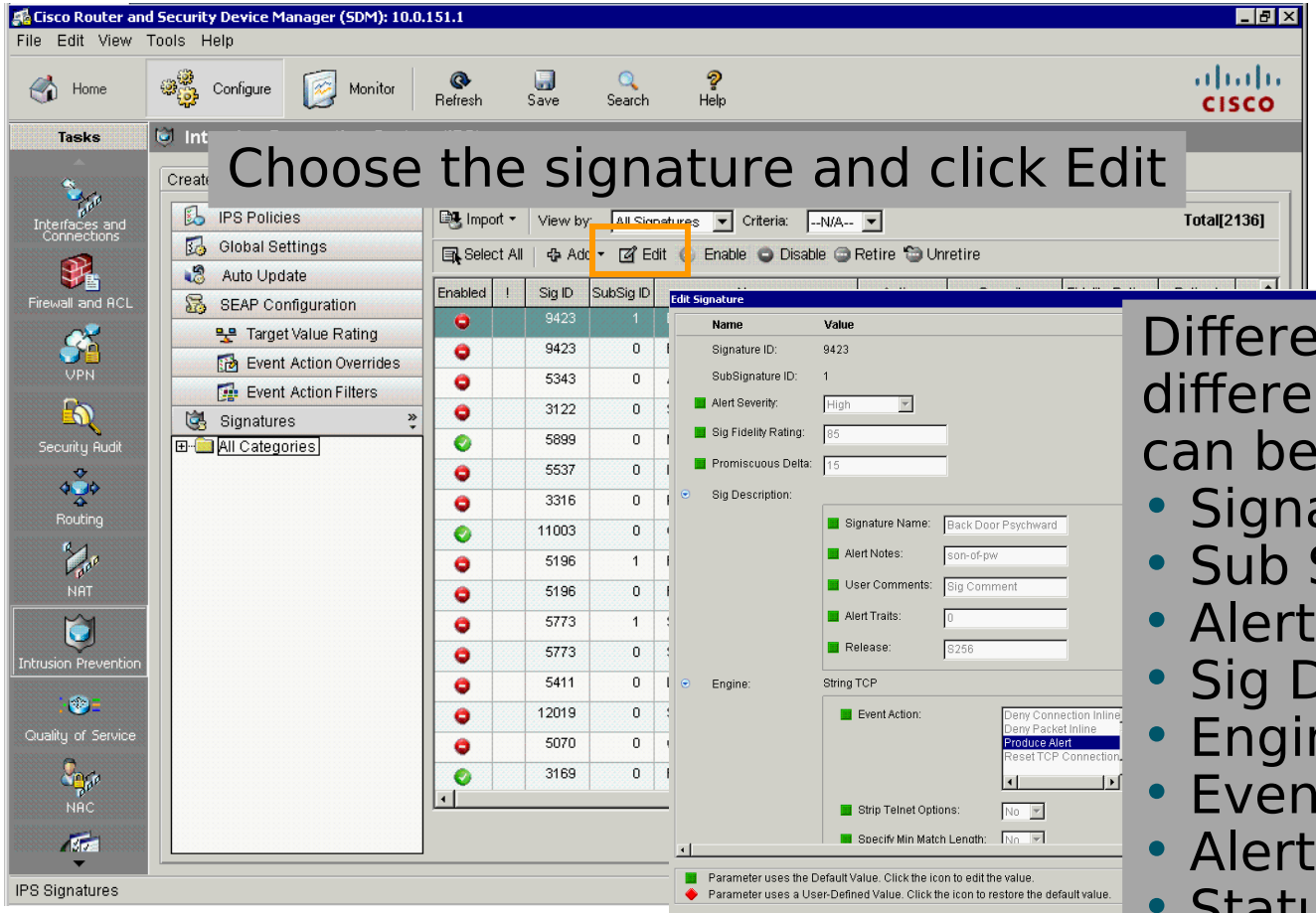
To tune a signature, choose Configure > Intrusion Prevention > Edit IPS > Signatures > All Categories



To modify a signature action, right-click on the signature and choose Actions

© 2009 Cisco Learning Institute.

Editing Signature Parameters



Choose the signature and click Edit

Different signatures have different parameters that can be modified:

- Signature ID
- Sub Signature ID
- Alert Severity
- Sig Description
- Engine
- Event Counter
- Alert Frequency
- Status

© 2009 Cisco Learning Institute.

Using CLI Commands

The **show ip ips** privileged EXEC command can be used with several other parameters to provide specific IPS information.

- The **show ip ips all** command displays all IPS configuration data.
- The **show ip ips configuration** command displays additional configuration data that is not displayed with the **show running-config** command.
- The **show ip ips interface** command displays interface configuration data. The output from this command shows inbound and outbound rules applied to specific interfaces.

© 2009 Cisco Learning Institute.

Using CLI Commands

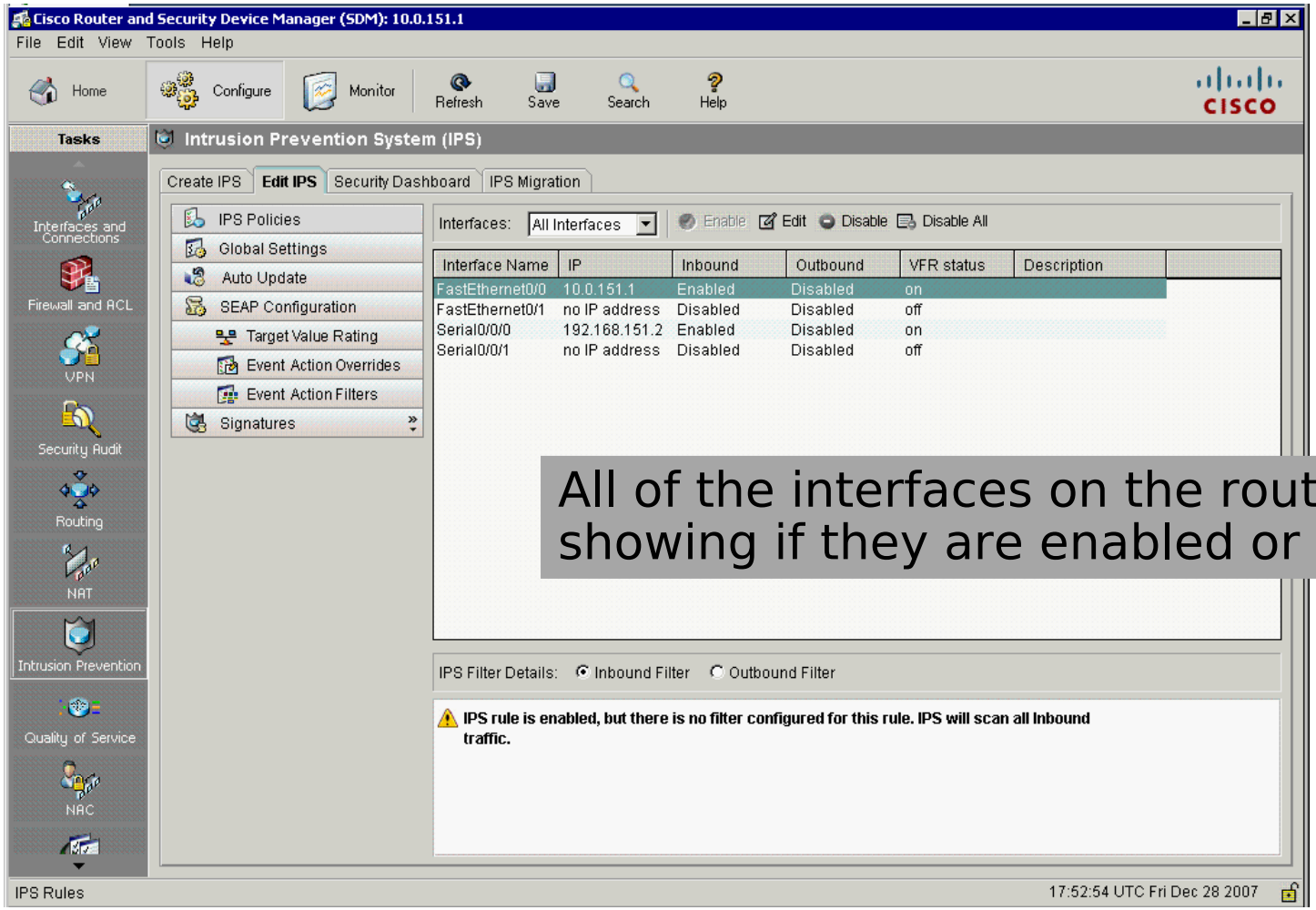
- The **`show ip ips signature`** verifies the signature configuration. The command can also be used with the key word **detail** to provide more explicit output
- The **`show ip ips statistics`** command displays the number of packets audited and the number of alarms sent. The optional **reset** keyword resets output to reflect the latest statistics.

  Use the **`clear ip ips configuration`** command to remove all IPS configuration entries, and release dynamic resources. The **`clear ip ips statistics`** command resets statistics on packets analyzed and alarms sent.

© 2009 Cisco Learning Institute.

Using SDM

Choose Configure > Intrusion Prevention > Edit IPS



All of the interfaces on the router display showing if they are enabled or disabled

© 2009 Cisco Learning Institute.

Reporting IPS Intrusion Alerts

- To specify the method of event notification, use the **ip ips notify [log | sdee]** global configuration command.
  - The **log** keyword sends messages in syslog format.
  - The **sdee** keyword sends messages in SDEE format.

```
R1# config t
R1(config)# logging 192.168.10.100
R1(config)# ip ips notify log
R1(config)# logging on
R1(config)#
```

© 2009 Cisco Learning Institute.

SDEE on an IOS IPS Router

- Enable SDEE on an IOS IPS router using the following command:

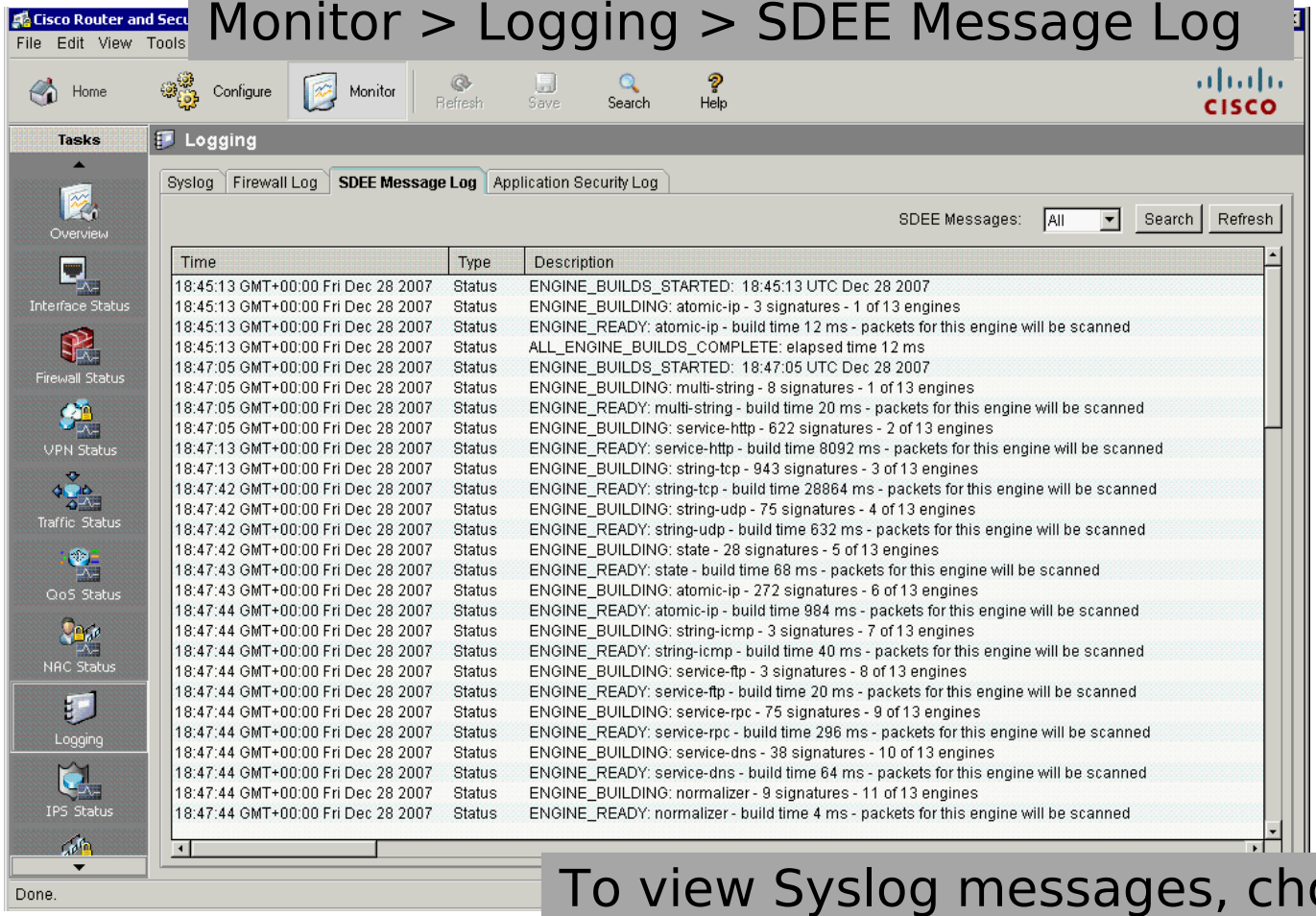
```
R1# config t
R1(config)# ip http server
R1(config)# ip http secure-server
R1(config)# ips notify sdee
R1(config)# ip sdee events 500
R1(config)#
```

- Enable HTTP or HTTPS on the router
- SDEE uses a pull mechanism
- Additional commands:
  - `ip sdee events` *events*
  - `Clear ip ips sdee {events|subscription}`
  - `ip ips notify`

© 2009 Cisco Learning Institute.

Using SDM to View Messages

To view SDEE alarm messages, choose Monitor > Logging > SDEE Message Log



To view Syslog messages, choose Monitor > Logging > Syslog

© 2009 Cisco Learning Institute.



© 2009 Cisco Learning Institute.