Cisco IOS Intrusion Prevention System

Alex Yeung

Technical Marketing Engineer

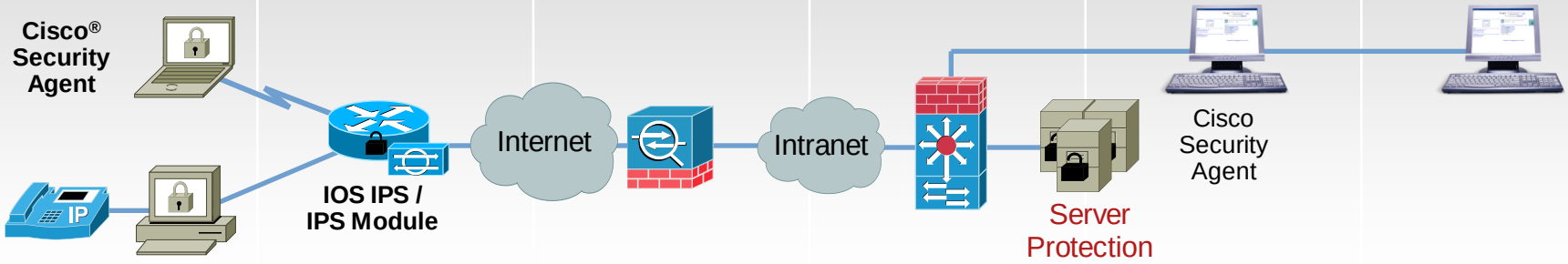
October 2008

Agenda

- IOS IPS Overview
- Technical Review
  - Architecture
  - Packet Flow
  - Configuration
  - Troubleshooting
- Use Cases
- Management
- Best Practices
- Resources

Cisco Intrusion Prevention Solution
Comprehensive Threat Protection for the SDN

Cisco Security Agent	Cisco Integrated Services Routers	Cisco ASA 5500 Adaptive Security Appliance	Cisco Catalyst ® Service Modules Cisco IPS 4200 Series Sensors	Cisco Security MARS	Cisco Security Manager



Day Zero Endpoint Protection	Branch Protection	Converged Perimeter Protection	Integrated Data Center Protection	Monitoring, Correlation, and Response	Policy-Based Solution Management

Integrated

- Multivector protections at all points in the network and desktop and server endpoints

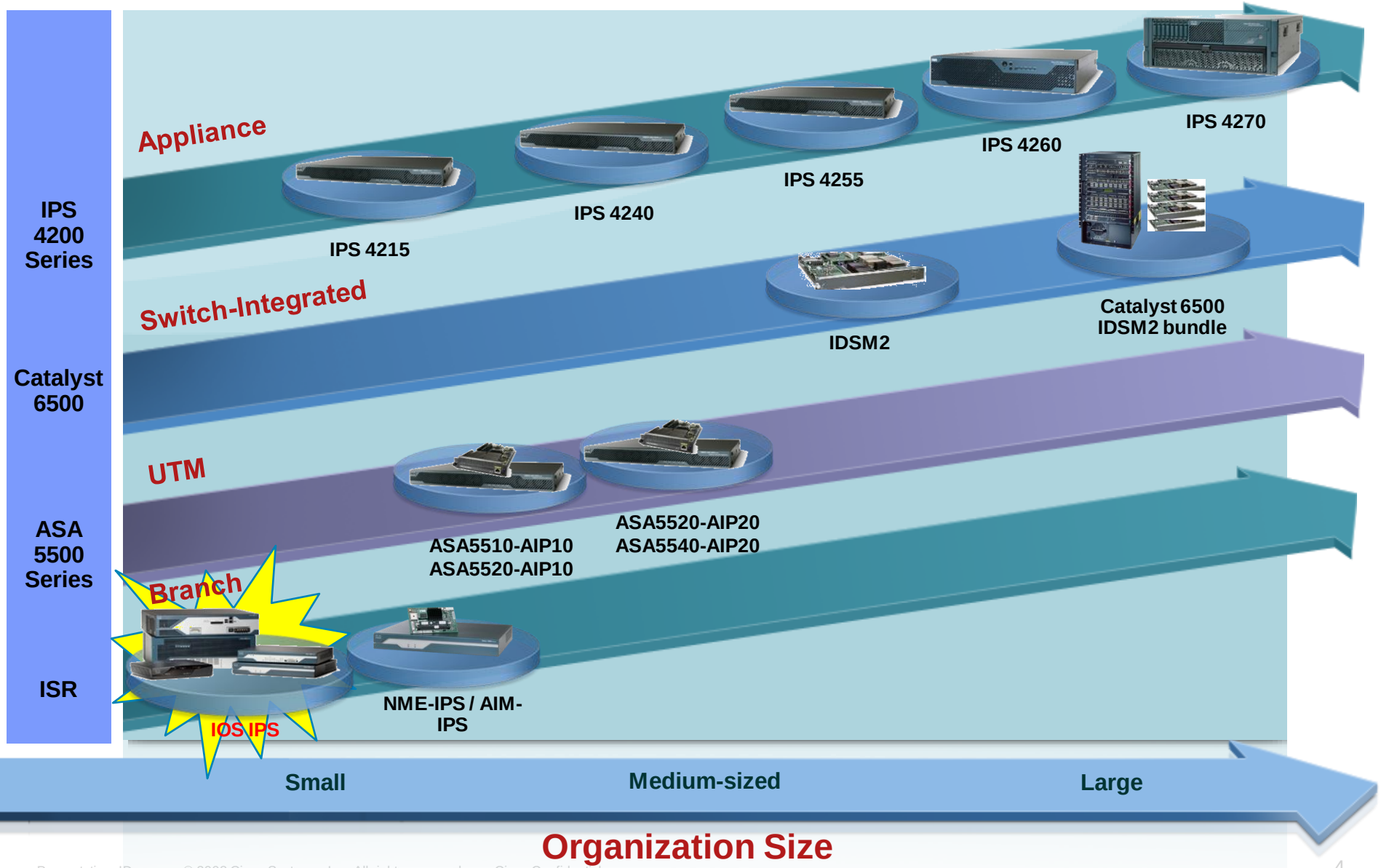
Collaborative

- Cross-solution feedback linkages
- Common policy management
- Multivendor event correlation
- Attack path identification
- Passive and active fingerprinting
- Cisco Security Agent-IPS Collaboration

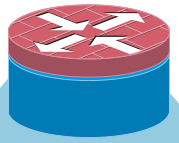
Adaptive

- Anomaly detection with in-production learning
- Network behavioral analysis
- On-device and network event correlation
- Real-time security posture adjustment

Cisco IPS Product Portfolio



All-in-One Security for the WAN



Only Cisco® Security Routers Deliver All of This

Secure Network Solutions


Business Continuity

Secure Voice


Secure Mobility


Compliance

Integrated Threat Control


Advanced Firewall


URL Filtering


Intrusion Prevention

Flexible Packet Matching


Network Admission Control


802.1x


Network Foundation Protection

Secure Connectivity


GET VPN


DMVPN


Easy VPN


SSL VPN

Management and Instrumentation


SDM


Role-Based Access

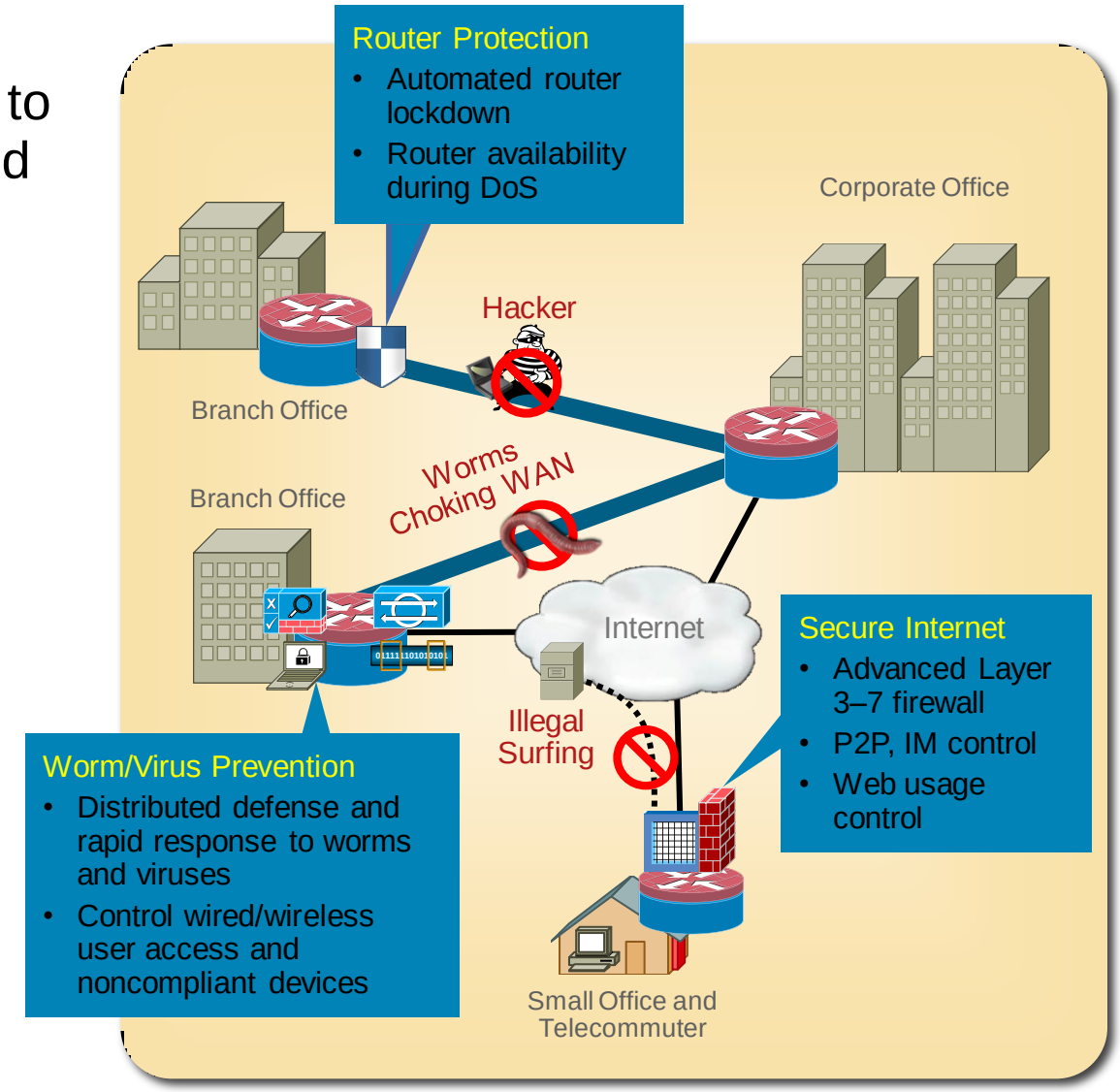

NetFlow


IP SLA

Integrated Threat Control Overview

Industry Certified Security Embedded within the Network

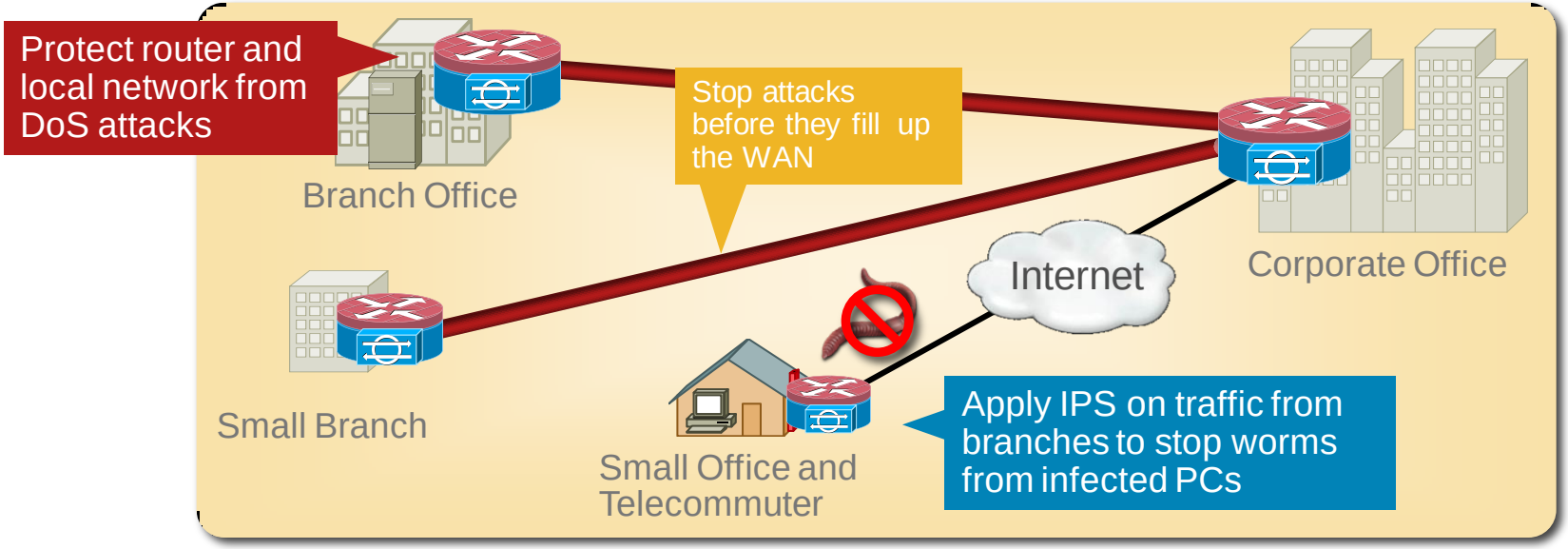
- Secure Internet access to branch, without the need for additional devices
- Control worms, viruses and adware/spyware right at the remote site; conserve WAN bandwidth
- Protect the router itself from hacking and DoS attacks
- Protects data, voice and video, wired and wireless, and WAN acceleration services



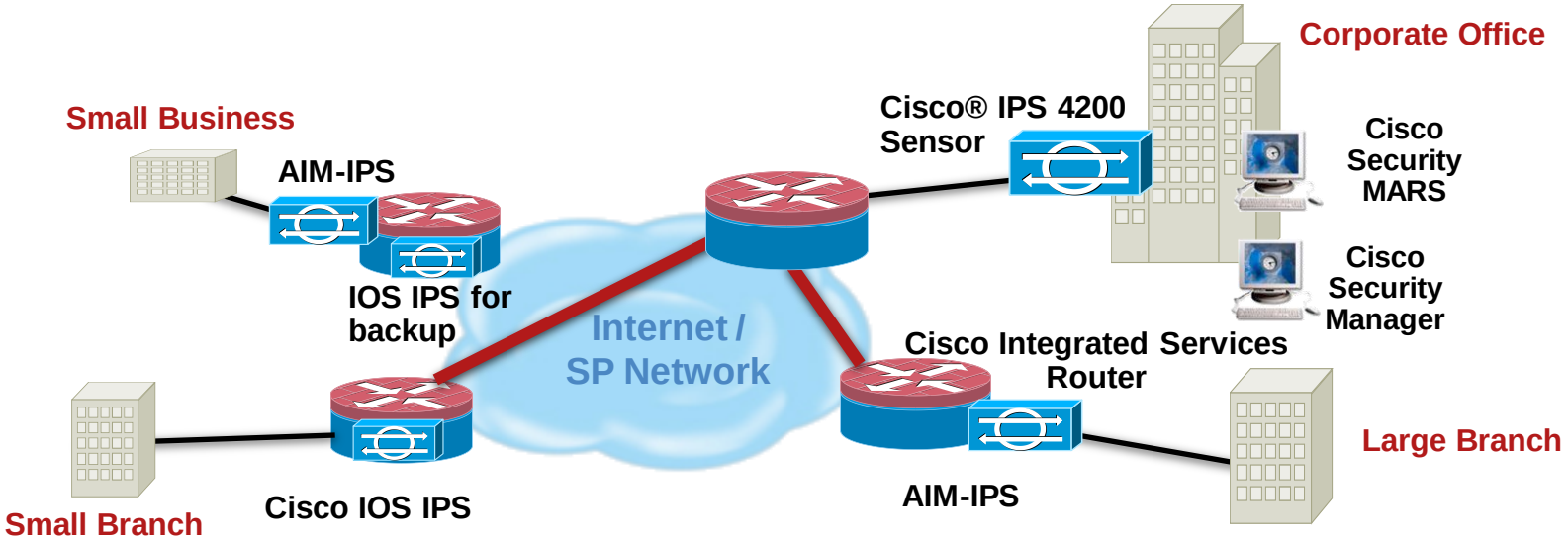
Cisco IOS Intrusion Prevention (IPS)

Distributed Defense Against Worms and Attacks

- Cisco® IOS® IPS stops attacks at the entry point, conserves WAN bandwidth, and protects the router and remote network from DoS attacks
- Integrated form factor makes it cost-effective and viable to deploy IPS in small and medium business and enterprise branch/telecommuter sites
- Supports a fully customizable subset of 2300+ signatures sharing the same signature database available with Cisco IPS sensors and modules
- Allows custom signature sets and actions to react quickly to new threats

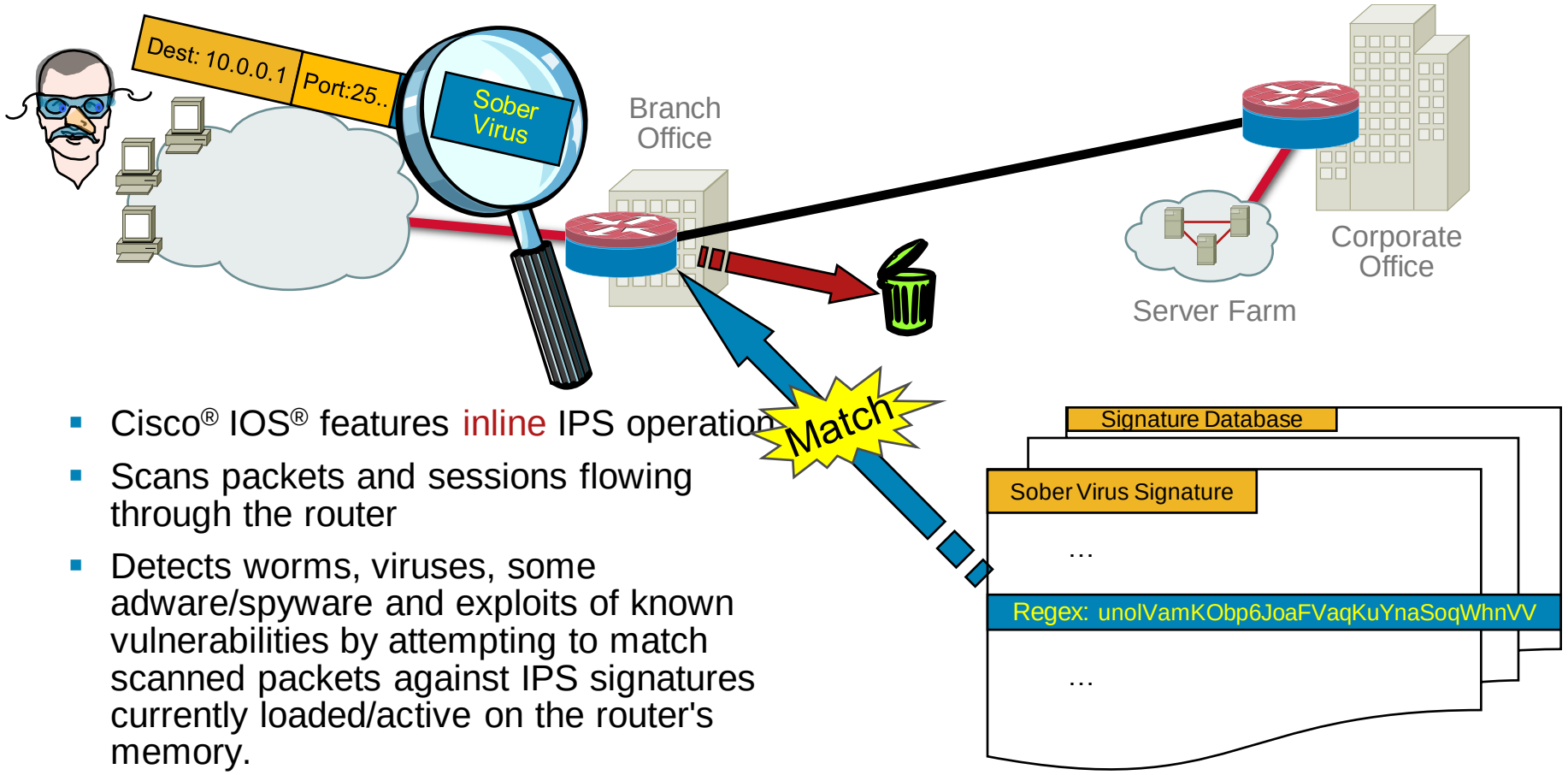


Benefits of Integrated IPS on Cisco ISRs



- Provides network-wide, protection from many worms, viruses, and vulnerabilities
- Eliminates the need for a standalone IPS device at branch and small offices
- Works with Cisco IOS® Firewall, control-plane policing, and other Cisco IOS Software security features to protect the router and networks behind the router
- Supports any routed WAN link; transport agnostic: T1/E1, T3/E3, Ethernet, xDSL, Multiprotocol Label Switching (MPLS), and third-generation (3G) wireless WAN (WWAN), LAN and WLAN links
- Provides defense-in-depth to the perimeter of the network: ICSA-certified Cisco IOS® Firewall, IP Security (IPsec) and Secure Sockets Layer (SSL) VPN, Cisco Network Admission Control (NAC), and URL filtering
- Integrates with data, security, and voice features on Cisco Integrated Services Router

Cisco IOS IPS Overview – How it Works



- Cisco® IOS® features inline IPS operation
- Scans packets and sessions flowing through the router
- Detects worms, viruses, some adware/spyware and exploits of known vulnerabilities by attempting to match scanned packets against IPS signatures currently loaded/active on the router's memory.
- Responds in real time through any of the following actions:

  ALARM, DROP, RESET, DENY-ATTACKER-INLINE, DENY-CONNECTION-INLINE

Cisco IOS IPS – History

Release	Changes
12.4(20)T	**Virtual IPS (VRF-aware – IPS on a VRF interface)**
12.4(15)T	**Support MSRPC engine and Microsoft SMB Advanced engine**
12.4(11)T	**Support Cisco IPS version 5.x signature format**
12.4(9)T2	Fix IOS IPS to work with packets arriving at the router out of order.
12.4(6)T	Session setup rate performance improvements
12.4(3)a/12.4(4)T	String engine memory optimization ▪ MULTI-STRING engine support for Trend Labs and Cisco Incident Control System ▪ Performance improvement
12.4(2)T	Layer 2 (Transparent IPS) support
12.3(14)T	▪ Support for three string engines (STRING.TCP, STRING.UDP and STRING.ICMP) ▪ Support for two new local shunning event actions: denyAttackerInline and denyFlowInline
12.3(8)T	First release

What's New in 12.4(11)T & 12.4(15)T Releases

Feature	Benefit
Same signature format as Cisco IPS 5.x/6.0 appliances/modules	Common operations for Cisco IPS appliances and Cisco IOS IPS
Native support for MSRPC and SMB signatures in12.4(15)T2 and later releases	Protection against vulnerabilities in MS applications before public release
***Risk Rating* value in IPS alarms based on Signature Severity, Fidelity and Target Value Rating**	Enables accurate and efficient IPS event correlation and monitoring
Individual and category based signature provisioning via IOS CLI	Granular customization and tuning of signatures through custom scripts
IDCONF (XML) signature provisioning mechanism	Secure provisioning over HTTPS via CSM 3.2 and CCP 1.0
Signature Event Action Processor (SEAP)	Quick and automated adjustment of signature event actions

Important End-of-Life Announcement for: IOS IPS Signatures written in Cisco IPS version 4.x Format

- IOS-S351.zip file posted on August 20, 2008 is the final signature release in 4.x format.

- Version 10 of the recommended Basic and Advanced signature sets (128MB.sdf and 256MB.sdf files) posted on August 11, 2008 are the final recommended sets in 4.x format for IOS IPS.

- Customers using IOS IPS feature with **IOS Mainline and T-Train Releases prior to 12.4(11)T Release** that work only with 4.x format IPS signatures are strongly encouraged to upgrade their routers to run IOS 12.4(15)T7 or 12.4(20)T release as soon as possible.

Recent Improvements in Cisco IOS IPS

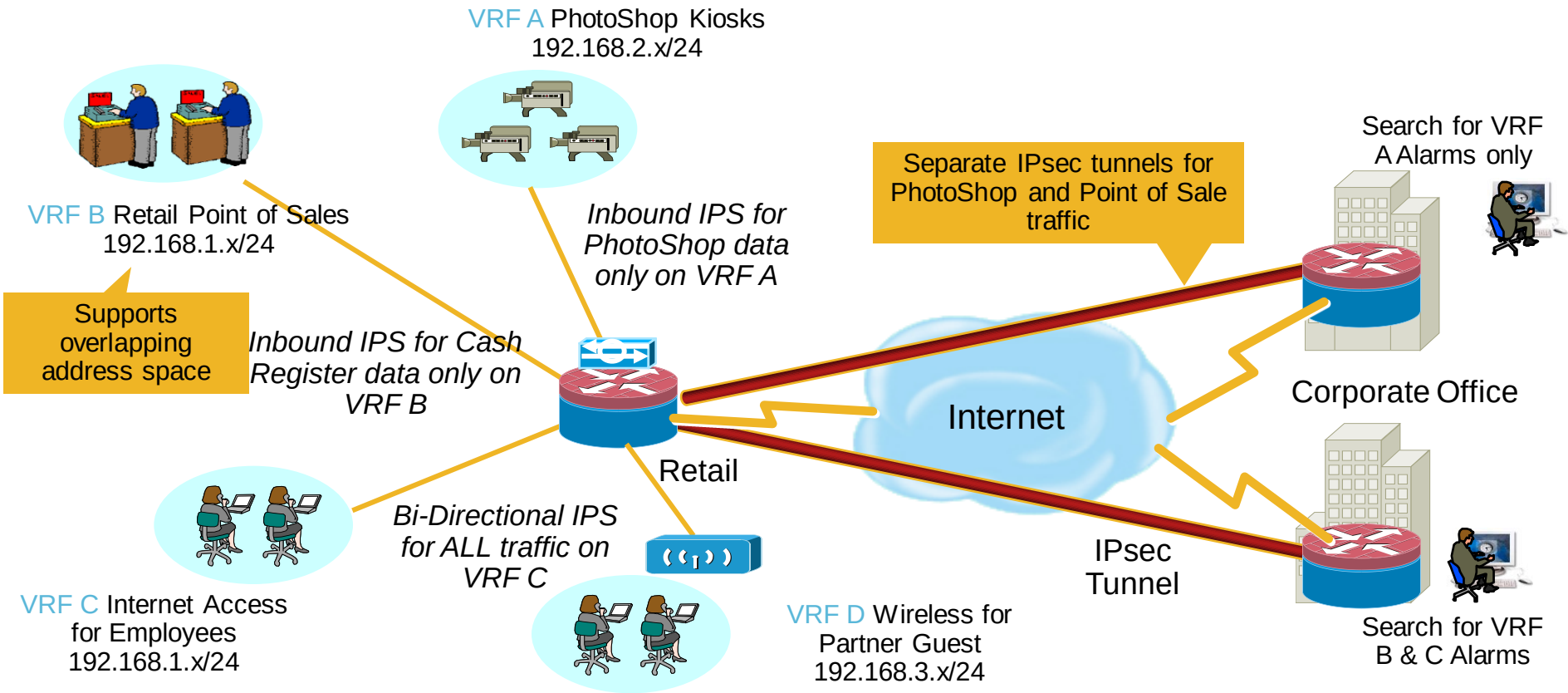
Cisco IOS 12.4(15)T2 and Later

Customer Pain Points	Features	Benefits
Quick Response Reduce Timeline from Vulnerability to Signature Deployment	▪NDA (encrypted) signature support and native support for MSRPC and Microsoft SMB signatures ▪Automated signature updates from a local TFTP or HTTP(S) server	▪Efficient protection against many new Microsoft and other vulnerabilities, some even before their public release ▪Protection from latest threats with minimal user intervention
Improved Accuracy Reduced False Positives	▪Risk Rating value in IPS alarms based on signature severity, fidelity, and target value rating ▪Supports Signature Event Action Processor (SEAP)	▪Enables accurate and efficient IPS event correlation and monitoring ▪Quick and automated adjustment of signature event actions based on Risk Rating
Manageability Secure and Simpler Signature Provisioning	▪Individual and category-based signature provisioning through Cisco IOS CLI ▪IDCONF (XML) signature provisioning mechanism ▪VRF aware IPS (from 12.4(20)T)	▪Offers granular customization and tuning of signatures through custom scripts ▪Secure provisioning through CSM 3.1 and CCP 1.x over HTTPS ▪ Apply/Monitor IPS on a VRF basis
Common Operations From HQ to Branch	▪ Same signature format as the latest Cisco® IPS appliances and modules	▪ Common operations for Cisco IPS appliances and Cisco IOS® IPS

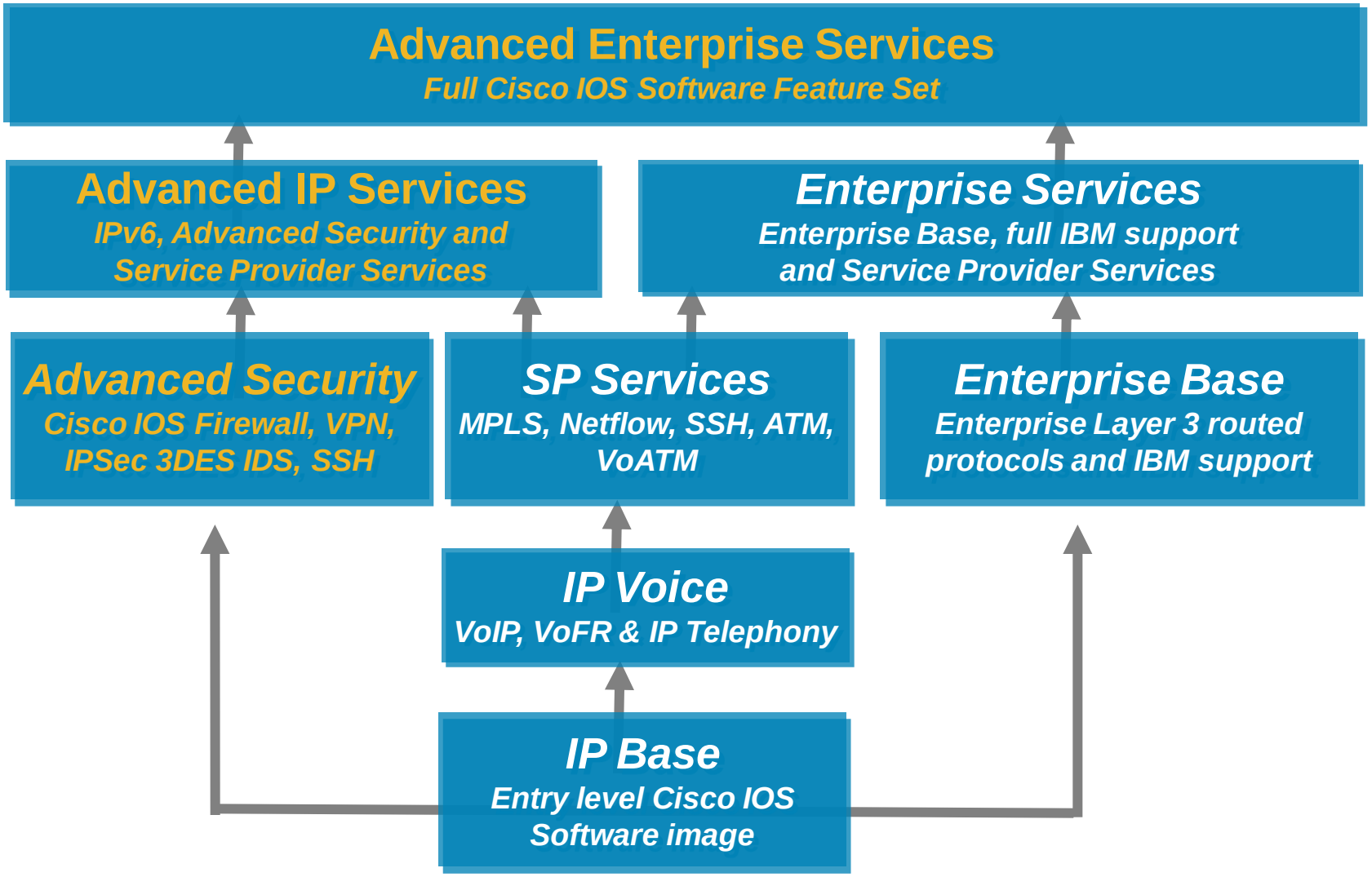
New IOS IPS Feature

New in 12.4(20)T

- Virtual IPS—Virtual Route Forwarding (VRF) Aware
  Similar to IOS Firewall/NAT and VPN. VRF aware supports overlapping addresses and granular IPS event alarms with VRF ID



Images that Supports IOS IPS



Cisco IOS IPS Platform Support

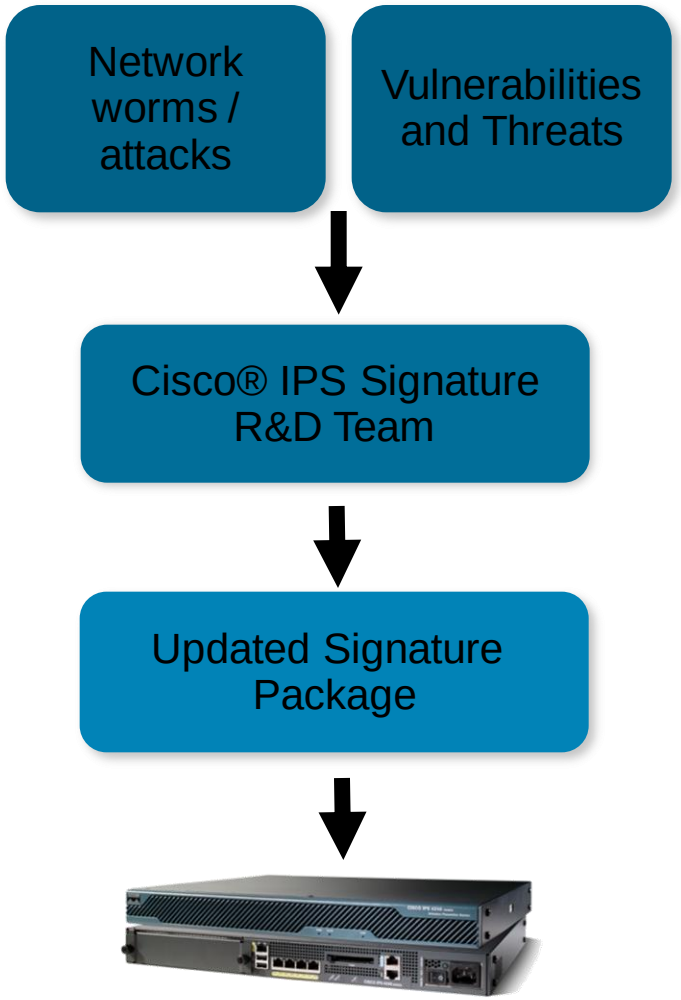
Cisco IOS IPS is supported on the following Platforms

ISR platforms: 87x/88x, 18xx, 28xx, 38xx

72xxVXR/7301

Cisco Services for IPS

Rapid Signature Updates for Emerging Threats



- Extensive 24-hour research capability gathers, identifies, and classifies vulnerabilities and threats
- Signatures are created to mitigate the vulnerabilities within hours of classification
- Signature updates are available to customers at Cisco.com

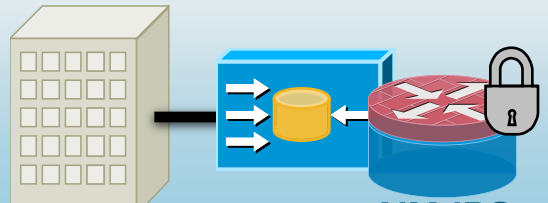
Intrusion Prevention System (IPS) Advanced Integration Module and Network Module

Q4CY08

NME-IPS-K9
Cisco 2811, 2821, 2851, 3800

AIM-IPS-K9
Cisco 1841, 2800, 3800

IOS Advanced Security or above
AIM – 12.4(15)XY, 12.4(20)T
NME – 12.4(20)YA



Accelerated Threat Control for Cisco ISR

- Enables Inline and promiscuous Intrusion Prevention (IPS)
- Runs same software (CIPS 6.1) and enables same features as Cisco IPS 4200
- Performance Improvement by Hardware Acceleration. Dedicated CPU and DRAM to offload host CPU
  - AIM – Up to 45 Mbps
  - NME – Up to 75 Mbps
- Device management through Cisco IPS Device Manager (IDM), Cisco Configuration Professional (CCP); Network wide management through Cisco Security Manager (CSM)
- Supported by IPS Manager Express (IME) and CS-MARS on event monitoring and correlation

Cisco IOS IPS, AIM-IPS and NME-IPS

Capability	IOS IPS	AIM-IPS, NME-IPS
CPU & DRAM Dedicated to IPS	No	Yes
Signature support	Subset of Cisco signatures based on available memory	All Cisco signatures that are not retired by default
Signature Updates & Tuning	CLI, File copy, IDCONF transactions	CLI, IDCONF transactions
Management Applications	SDM 2.5, CCP 1.x and CSM 3.2	IDM, CCP 1.1, IME, CSM 3.2
Event Notification	Syslog and SDEE	SDEE and SNMPv2
Event Monitoring Applications	SDM/CCP, IME and CS-MARS	IME and CS-MARS
Sig. Update Download from CCO	No (will be available in Dec. 2009)	Yes
Behavioral Anomaly Detection	No	Yes
Rate Limiting	No	Yes
IPv6 Detection	No	Yes
Risk Rating (RR) & Signature Event Action Proc. based on RR	Yes	Yes
Meta Engine & Signatures	No	Yes
Voice, Sweep & Flood Engines	No	Yes

Note: Only one IPS service may be active in the router. All others must be removed or disabled.

Agenda

- IOS IPS Overview
- Technical Review
  - Architecture
  - Packet Flow
  - Configuration
  - Troubleshooting
- Use Cases
- Management
- Best Practices
- Resources

Cisco IOS IPS—System Components

- Signature Micro-Engines (SMEs)

  A SME defines parameters for signatures in a specific protocol category, e.g. HTTP

- Signature Files

  Contains signature engine, parameter information such as signature name, signature ID and signature actions etc.

- Signature categories*

  A signature category contains pre-selected signature sets for a specific vulnerability

- SEAP (Signature Event Action Processor)

  SEAP allows for advanced event action filtering and overrides on the basis of the Event Risk Rating (ERR) feedback

- Event Monitoring

  Syslog messages and/or SDEE** alerts for events generated by IOS IPS

* Version 5.x Signature Format Only (i.e. 12.4(11)T2 or later)

** SDEE = Security Device Event Exchange

Cisco IOS IPS Signature Micro-Engines

- Total 13 signature engines
- Regular Expression Scanning Tables for each Signature Engine are compiled and loaded into the router's memory in the following order:

```
multi-string
service-http
string-tcp
string-udp
state
atomic-ip
string-icmp
service-ftp
service-rpc
service-dns
normalizer
service-smb-advanced
service-msrpc
```


Signature Files Explained

- IPS version 5.x/6.x signature package on CCO: IOS-Sxxx-CLI.pkg
- where xxx is the IPS signature update release, e.g. IOS-S320-CLI.pkg
- Copied to the router using the '**copy <sig pkg> idconf**' command

```
c2811#sh flash:
-#- --length-- -----date/time------ path
1     51054864 Feb 9 2008 05:30:18 +00:00 c2800nm-advipservicesk9-mz.12
2          660 Feb 11 2008 03:28:46 +00:00 vlan.dat
3            0 Mar 6 2008 08:34:04 +00:00 ips
4       212355 Mar 7 2008 18:24:24 +00:00 ips/c2811-sigdef-default.xml
5          271 Mar 7 2008 18:24:24 +00:00 ips/c2811-sigdef-delta.xml
6         6159 Mar 7 2008 18:24:24 +00:00 ips/c2811-sigdef-typedef.xml
7        23484 Mar 7 2008 18:24:26 +00:00 ips/c2811-sigdef-category.xml
8          304 Mar 7 2008 18:24:26 +00:00 ips/c2811-seap-delta.xml
9          491 Mar 7 2008 18:24:26 +00:00 ips/c2811-seap-typedef.xml
```

- 6 files
- File names begin with router's name

Signature Files Explained – Cont.

- <router-name>-sigdef-default.xml
  Default signature definition details. All signature parameters are defined here.
- <router-name>-sigdef-delta.xml
  Signature definitions that have been changed from the default.
- <router-name>-sigdef-typedef.xml
  Signature type definition file, such as engine definition, parameter type etc.
- <router-name>-sigdef-category.xml
  Signature category information.
- <router-name>-seap-delta.xml
  Signature SEAP configuration other than default.
- <router-name>-seap-typedef.xml
  Signature SEAP type definition file.

Signature Categories

- IOS IPS with Cisco 5.x/6.x format signatures operate with signature categories
- Signature category is a group of relevant signatures represented by a meaningful name
- All signatures are pre-grouped into categories
- An individual signature can belong to more than one category

```
Router#sh ip ips category ?

  adware/spyware          Adware/Spyware (more sub-categories)
  attack                  Attack (more sub-categories)
  ddos                    DDoS (more sub-categories)
  dos                     DoS (more sub-categories)
  email                   Email (more sub-categories)
  instant_messaging       Instant Messaging (more sub-categories)
  ios_ips                 IOS IPS (more sub-categories)
  l2/l3/l4_protocol       L2/L3/L4 Protocol (more sub-categories)
  network_services        Network Services (more sub-categories)
  os                      OS (more sub-categories)
  other_services          Other Services (more sub-categories)
  p2p                     P2P (more sub-categories)
  reconnaissance          Reconnaissance (more sub-categories)
  releases                Releases (more sub-categories)
  viruses/worms/trojans   Viruses/Worms/Trojans (more sub-categories)
  web_server              Web Server (more sub-categories)
```


Signature Event Action Processor (SEAP)

- Dynamically control actions taken by a signature event on the basis of signature risk rating.
- SEAP consists of two components:
  - Signature Event Action Overrides (SEAO)
  - Signature Event Action Filters (SEAF)

Risk Rating

Risk rating is a function of the following parameters:

- ASR: Attack Severity Rating
- SFR: Signature Fidelity Rating
- TVR: Target Value Rating
- ARR: Attack Relevance Rating*

These parameters have default values but can also be configured via CLI.

RR = F (ASR,SFR,TVR,ARR)

* In IOS IPS, ARR is hard-coded with default value 100 because it is only supported by Cisco stand-alone IPS appliances/modules.

Risk Rating – Cont.

- Risk Rating is a numerical quantification of the risk associated with a particular event on the network.
- The value is a number between 0 and 100. The higher the value, the greater the security risk of the trigger event for the associated alert.
- What is the benefit of using Risk Rating?

  IPS sensors generate a lot of alarms and we need some way to prioritize them better than simply by signature severity.

  The severity alone does not take into account the possibility of false positives, how important it is to protect the specific device being attacked, or whether or not the attack could have succeeded.

  By using Risk Rating a user should be able to better prioritize which alarms need attention first.

Attack Severity Rating (ASR)

- ASR is a rating associated with how severe the results of a successful exploit of the vulnerability is.
- ASR is an integer between 0 and 100
- 4 severity levels with pre-defined severity rating

ASR Level	Value Range
Information	25
Low	50
Medium	75
High	100

Signature Fidelity Rating (SFR)

- SFR is a rating associated with how confident the signature designer was of detecting true positives (or how well this signature might perform in the absence of specific knowledge of the target).
- SFR is an integer between 0 and 100. The higher the number the more accurate it is.
- If the signature was written with a very specific regex then it's SFR will be higher than one written with a more generic regex.
- If the program being attacked is fairly common and almost every version of the program is vulnerable, then the SFR will be higher than a signature for a program where only older versions are vulnerable or the program is rarely used at customer sites.
- Can be change by CLI per category or per signature

Target Value Rating (TVR)

- TVR is a rating associated with the user's perceived value of the target host.
- A host can be a single or range of IP addresses with and associated TVR value.
- TVR values are low, medium, high, mission critical.

TVR Level	Value Range
Low	75
Medium	100
High	150
Mission Critical	200

Cisco IOS IPS Event Monitoring

- IOS IPS supports two event reporting methods

  SYSLOG: Enabled by default

  SDEE: Disabled by default

- SDEE - a XML based IPS event logging format used by all Cisco IPS products, Cisco and 3rd party IPS event monitoring applications.
- SDEE event logs can be collected from IPS detectors only via HTTPS connections to guarantee secure reporting and monitoring
- Security Device Event Exchange (SDEE) is required by management applications—CCP, IME*, and CS-MARS

* IME = IPS Manager Express

Signature Actions

- produce-alert

  Sends alarms via syslog messages and/or SDEE alerts

- reset-tcp-connection

  Sends reset to both peers of a TCP connection

- deny-packet-inline

  Drops the packet

- deny-attacker-inline

  Blocks the attacker's source IP address by using dynamic ACL. No connection can be established from the attacker until the shun time expires (this is set by the user).

- deny-connection-inline

  Blocks the specific TCP flow from the attacker by using dynamic ACL. Other connections from the attacker can be established.

DoS Protection

- DoS Protection and Prevention is a common function shared between IOS FireWall and IOS IPS.
- Whenever IOS IPS is enabled on an interface, DoS protection will be turned on.
- Cisco IOS Firewall / IOS IPS inspection provides several adjustable parameters to protect against DoS attacks.
- These parameters allow you to configure the points at which your router's DoS protection begins to take effect.

DoS Protection – Cont.

There are five default parameters to protect against DoS attacks:

- The total number of half-open TCP or UDP sessions

```
ip inspect max-incomplete high value
ip inspect max-incomplete low value
```

- The number of new sessions based upon time (1 minute rate)

```
ip inspect one-minute high value
ip inspect one-minute low value
```

- Host session counter

```
ip inspect tcp max-incomplete host <half-open session> block-time
<block-time>
```

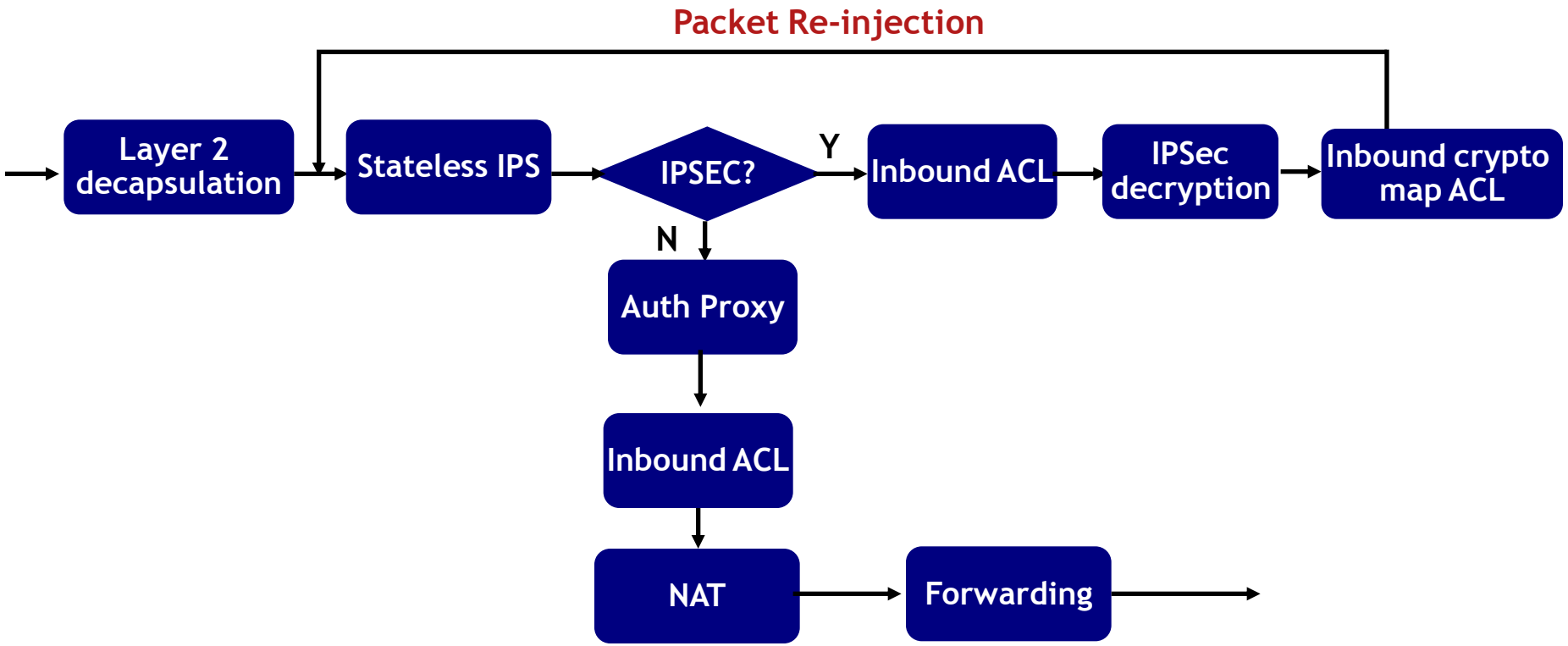
- Refer to the following guide for tuning these parameters:

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5708/ps5710/ps1018/prod_white_paper0900aecd8055e6ac.html

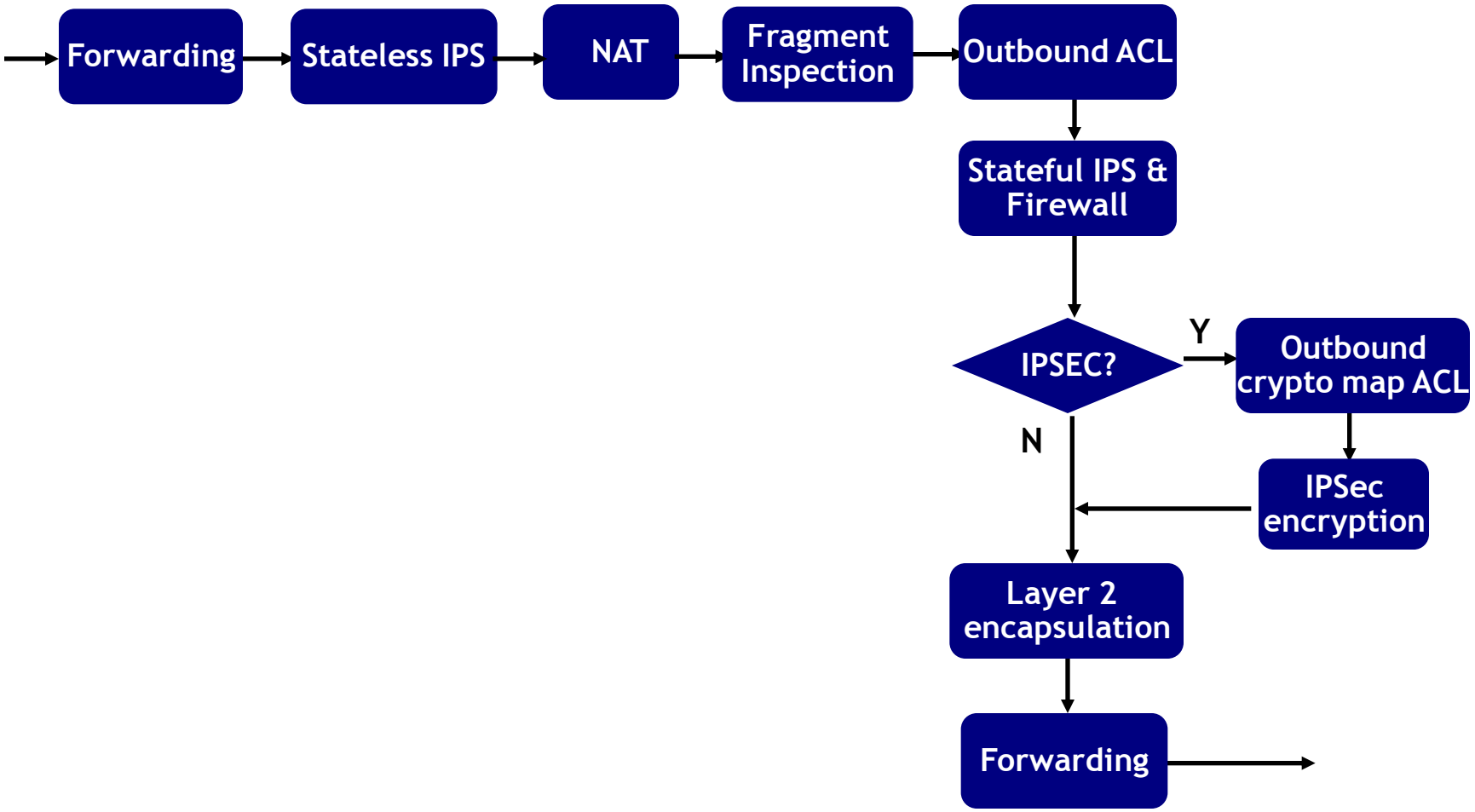
Agenda

- IOS IPS Overview
- Technical Review
  - Architecture
  - Packet Flow
  - Configuration
  - Troubleshooting
- Use Cases
- Management
- Best Practices
- Resources

Cisco IOS IPS Packet Flow—Inbound



IPSec/IPS Packet Flow - Outbound

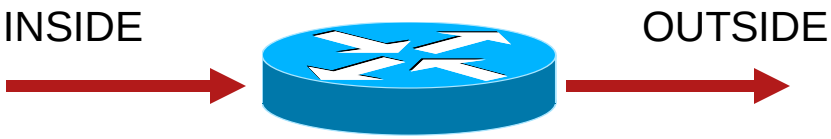


IOS IPS Packet Flow: Inside to Outside

Scenario 1: IPS applied in ‘inbound’ direction on INSIDE interface

```
interface ethernet1
 ip access-group 100 in
 ip nat inside
 ip ips myips in
```

```
interface ethernet0
 ip access-group 100 out
 ip nat outside
 ip inspect fw-policy out
 crypto map ipsec-policy
```



INSIDE interface

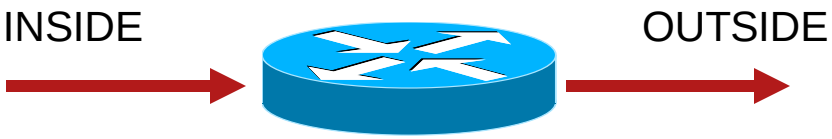
OUTSIDE interface

IOS IPS Packet Flow: Inside to Outside

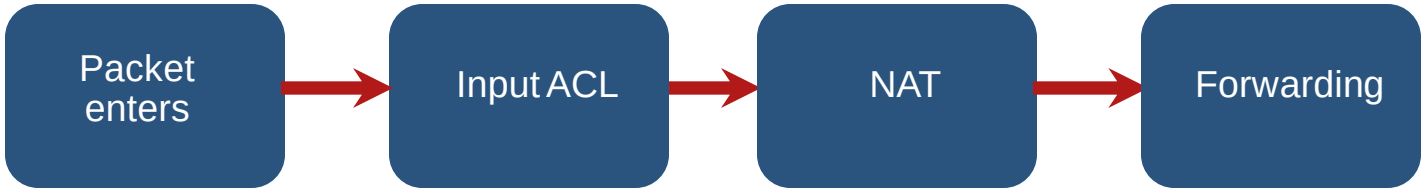
Scenario 2: IPS applied in 'outbound' direction on OUTSIDE interface

```
interface ethernet1
 ip access-group 100 in
 ip nat inside
```

```
interface ethernet0
 ip access-group 100 out
 ip nat outside
 ip inspect fw-policy out
 crypto map ipsec-policy
 ip ips myips out
```



INSIDE interface



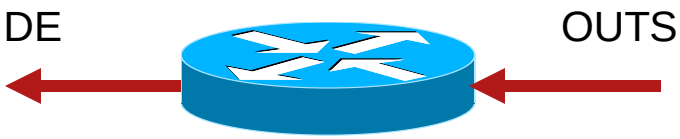
OUTSIDE interface

IOS IPS Packet Flow: Outside to Inside

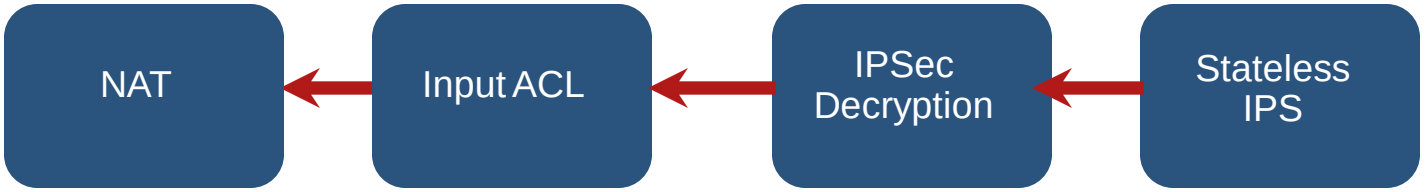
Scenario 3: IPS applied in ‘inbound’ direction on OUTSIDE interface

```
interface ethernet1
 ip access-group 100 out
 ip nat inside
```

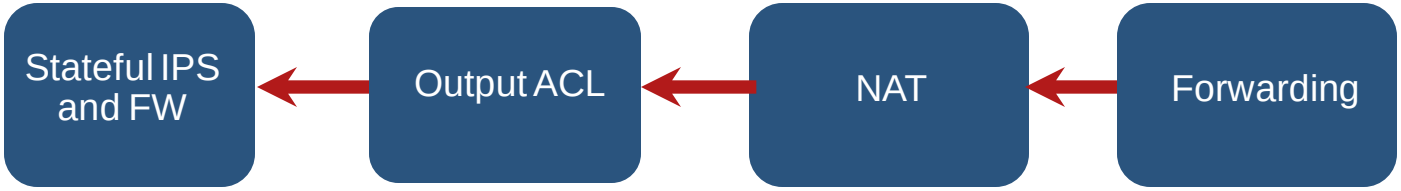
```
interface ethernet0
 ip access-group 100 in
 ip nat outside
 ip inspect fw-policy out
 crypto map ipsec-policy
 ip ips myips in
```



OUTSIDE interface



INSIDE interface

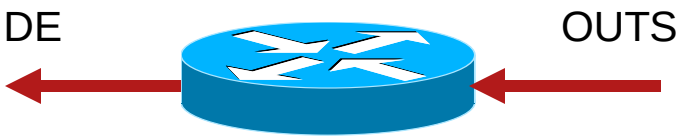


IOS IPS Packet Flow: Outside to Inside

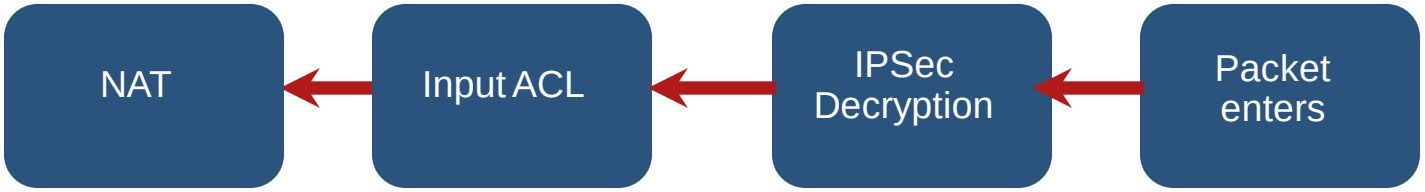
Scenario 4: IPS applied in 'outbound' direction on INSIDE interface

```
interface ethernet1
 ip access-group 100 out
 ip nat inside
 ip ips myips out
```

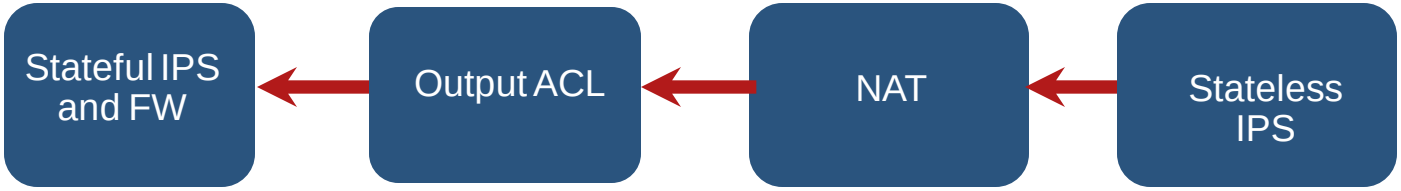
```
interface ethernet0
 ip access-group 100 in
 ip nat outside
 ip inspect fw-policy out
 crypto map ipsec-policy
```



OUTSIDE interface



INSIDE interface



Agenda

- IOS IPS Overview
- Technical Review
  - Architecture
  - Packet Flow
  - Configuration
  - Troubleshooting
- Use Cases
- Management
- Best Practices
- Resources

IOS IPS Configuration

Getting Started Config Steps

1. Download IPS Files
2. Create Directory on Flash
3. Configure IOS IPS Crypto Key
4. Enable IOS IPS
5. Load IOS IPS signatures

Advanced Config Options

- Signature Tuning & Customization
- Configure SEAP
- Signature Package Update

Terminology

- Retire/unretire is to select/de-select which signatures are being used by IOS IPS to scan traffic.

  Retiring a signature means IOS IPS will NOT compile that signature into memory for scanning.

  Unretiring a signature instructs IOS IPS to compile the signature into memory and use the signature to scan traffic.

- Enable/disable does NOT select/de-select signatures to be used by IOS IPS.

  Enabling a signature means that when triggered by a matching packet (or packet flow), the signature takes the appropriate action associated with it. However, only unretired AND successfully compiled signatures will take the action when they are enabled. In other words, if a signature is retired, even though it is enabled, it will not be compiled (because it is retired) and it will not take the action associated with it.

  Disabling a signature means that when triggered by a matching packet (or packet flow), the signature DOES NOT take the appropriate action associated with it. In other words, when a signature is disabled, even though it is unretired and successfully compiled, it will not take the action associated with it.

Step 1: Download IPS Files

Download latest signature package and crypto key:

http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup

IOS-Sxxx-CLI.pkg

Signature package – download the latest release

realm-cisco.pub.key.txt

Public Crypto key – crypto key used by IOS IPS

Step 2: Create Directory on Flash

To create a directory, use CLI

```
router#mkdir <directory name>

router#mkdir ips
    Create directory filename [ips]?
    Created dir flash:ips
```

Additional commands:

To rename a directory, use CLI

```
Router#rename <directory name>
```

To remove a directory, use CLI

```
Router#rmdir <directory name>
```

Step 3: Configure IOS IPS Crypto Key

Copy and paste public crypto key at global config mode:

```
router(config)#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
 Quit
```

Additional command:
Remove previous key if encounter crypto key error:

```
router(config)#no crypto key pubkey-chain rsa
router(config-pubkey-chain)#no named-key realm-cisco.pub signature
router(config-pubkey-chain)#exit
router(config)#exit
router#
```

Step 4: Enable IOS IPS

Step 4.1: Configure IPS Rule Name

```
router(config)#ip ips name iosips [list acl]*
```

Step 4.2: Configure IPS Signature Storage Location

```
router(config)#ip ips config location flash:ips
```

Step 4.3: Configure SDEE Event Notification

```
router(config)#ip ips notify sdee
```

* [list *acl*] – (Optional) Specifies an extended or standard access control list (ACL) to filter the traffic that will be scanned. All traffic that is permitted by the ACL is subject to inspection by the IPS. Traffic that is denied by the ACL is not inspected by the IPS.

Step 4: Enable IOS IPS - Continue

Step 4.4: Configure IPS Signature Category

```
router(config)#ip ips signature-category
router(config-ips-category)# category all
router(config-ips-category-action)# retired true
router(config-ips-category-action)# exit
router(config-ips-category)# category ios_ips basic *
router(config-ips-category-action)# retired false
router(config-ips-category-action)# exit
router(config-ips-category)# exit
Do you want to accept these changes? [confirm] yes
```

* Cisco recommends to start with either the IOS IPS Basic or Advanced signature category. Basic category is a subset of Advanced category.

Step 4.5: Enable IPS Rule on Interface

```
router(config)#int vlan 1
router(config-if)#ip ips iosips in
```

Step 5: Load Signatures

The last step is to load signature package

```
router#copy tftp://10.10.10.2/IOS-S310-CLI.pkg idconf
Loading IOS-S310-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7608873/4096 bytes]
```

Immediately after the signature package is loaded to the router, signature compiling begins. You can see the logs on the router with logging level 6 or above enabled.

```
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_BUILDS_STARTED:  16:44:47 PST Feb 14 2008
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_BUILDING: multi-string - 8 signatures - 1 of 13
engines
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_READY: multi-string - build time 4 ms - packets for
this engine will be scanned
|
output snipped
|
*Feb 14 16:45:18 PST: %IPS-6-ENGINE_BUILDING: service-msrpc - 25 signatures - 13 of 13
engines
*Feb 14 16:45:18 PST: %IPS-6-ENGINE_READY: service-msrpc - build time 32 ms - packets
for this engine will be scanned
*Feb 14 16:45:18 PST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 31628 ms
```

Step 5: Load Signatures – Cont.

Verify the signature package is properly compiled

```
router#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
|
outpt snipped
|
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
   Total Signatures with invalid parameters: 6
   Total Obsoleted Signatures: 11
```

Basic Configuration Example

```
ip ips config location flash:ips/ retries 1
ip ips notify SDEE
ip ips name iosips
```

```
ip ips signature-category
  category all
   retired true
  category ios_ips advanced
   retired false
```

ALWAYS remember first select category “all” AND retire all signatures

```
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   |
   snip
   |
   F3020301 0001
  quit
```

IOS IPS crypto key

```
interface GigabitEthernet0/1
 ip address 10.1.1.6 255.255.255.0
 ip ips iosips in
 ip virtual-reassembly
 duplex auto
 speed auto
```

enable IOS IPS policy on interface

Configure Event Notification Using SDEE

- SDEE messages are transported over HTTP/HTTPS
- You must enable HTTP/HTTPS in order to use SDEE

```
Router(config)#username cisco privilege 15 password cisco
Router(config)#ip ips notify sdee

Router(config)#ip http server
or
Router(config)#ip http secure-server
Router(config)#ip http authentication local
```

- Recommend to set the number of concurrent subscriptions to three when using IME

```
Router(config)#ip sdee subscriptions ?
      <1-3>  Number of concurrent SDEE subscriptions
```

- IOS IPS log message format:

```
*Mar 22 03:53:13.827: %IPS-4-SIGNATURE: Sig:5114 Subsig:1 Sev:75 WWW IIS
  Unicode Attack [10.1.1.252:4150 -> 192.168.1.249:80] RiskRating:75

*Mar 22 03:53:13.827: %IPS-4-SIGNATURE: Sig:5081 Subsig:0 Sev:100
 WWW WinNT cmd.exe Access [10.1.1.252:4150 -> 192.168.1.249:80]
  RiskRating:100
```

Advanced Config Options – Signature Tuning & Customization

- IOS IPS allows granular tuning on individual signature basis and / or signature category basis
- Using CLI, customer can:
  - select / de-select / retire / un-retire signatures
  - modify signature's action / severity
  - modify SEAP parameters
- Using CCP, in addition to what customer can do in CLI, customer also can:
  - tune all parameters of any individual signature
  - clone an existing signature and modify all its parameters
  - Create custom signatures for all protocols supported by IOS IPS in almost any way customers like

Advanced Config Options – Signature Tuning & Customization using CLI

Tune by individual signature: enable/disable/retire/unretire

```
router(config)#ip ips signature-definition
router(config-sigdef)#signature 6130 10
router(config-sigdef-sig)#status
router(config-sigdef-sig-status)#?
Status options for signatures:
  enabled  Enable Category Signatures
  exit     Exit from status submode
  no       Negate or set default values of a command
  retired  Retire Category Signatures
router(config-sigdef-sig-status)#retired false
router(config-sigdef-sig-status)#exit
router(config-sigdef-sig)#exit
router(config-sigdef)#exit
Do you want to accept these changes? [confirm]
```

e.g. retired false: the above example shows to un-retire a signature – instruct router to compile this signature

Advanced Config Options – Signature Tuning & Customization using CLI

Tune by individual signature: event action

```
router(config)#ip ips signature-definition
router(config-sigdef)#signature 5118 0
router(config-sigdef-sig)#engine
router(config-sigdef-sig-engine)#?
Engine options for signatures:
  event-action  Action
  exit          Exit from engine submode
  no            Negate or set default values of a command

router(config-sigdef-sig-engine)#event-action ?
  deny-attacker-inline    Deny Attacker
  deny-connection-inline  Deny Connection
  deny-packet-inline      Deny Packet
  produce-alert           Produce Alert
  reset-tcp-connection    Reset TCP Connection
  <cr>
router(config-sigdef-sig-engine)#event-action deny-attacker-inline
router(config-sigdef-sig-engine)#end
Do you want to accept these changes? [confirm]
```

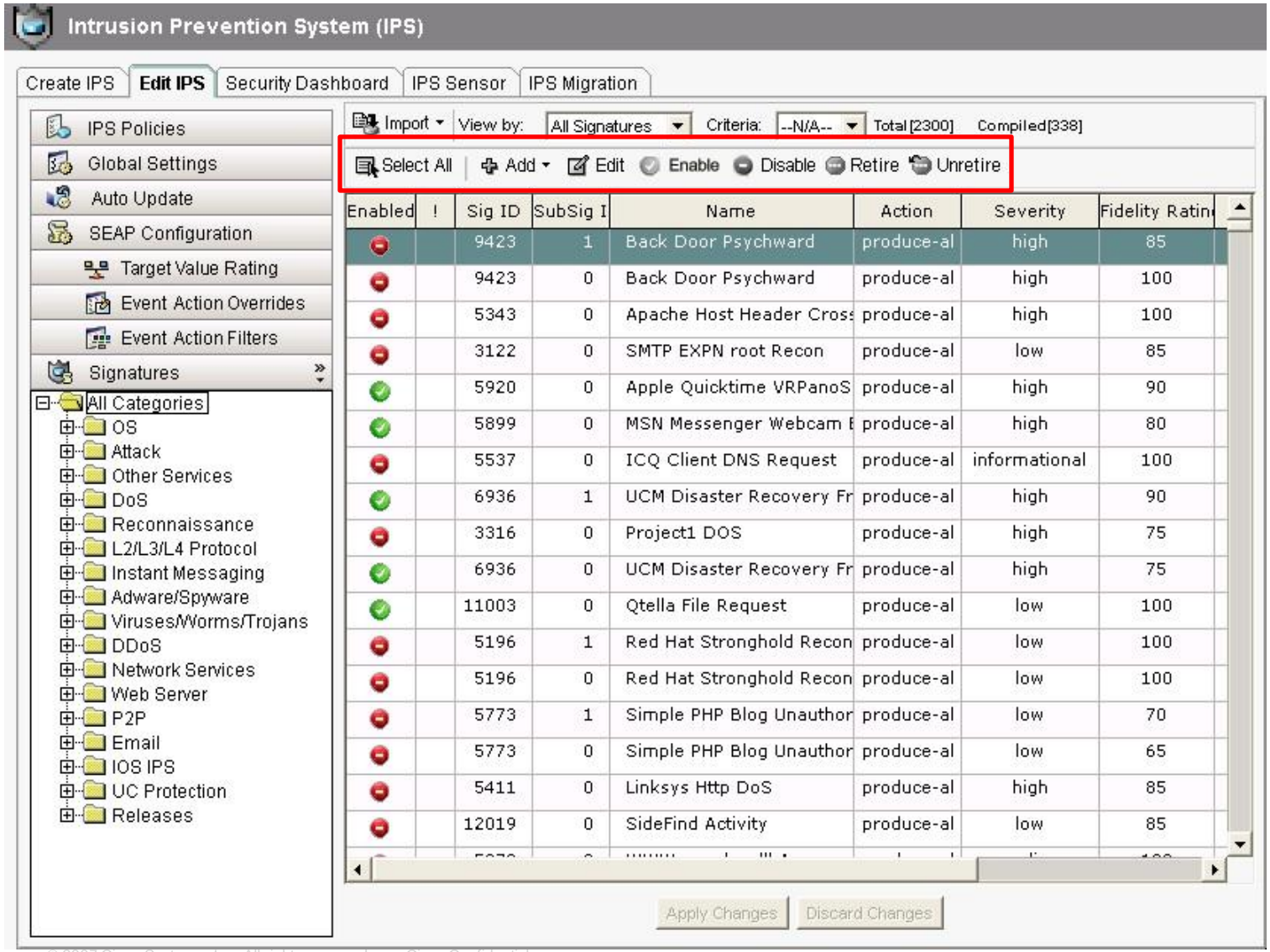
Advanced Config Options – Signature Tuning & Customization using CLI

Tune by signature category: enable/disable/retire/unretire/event action

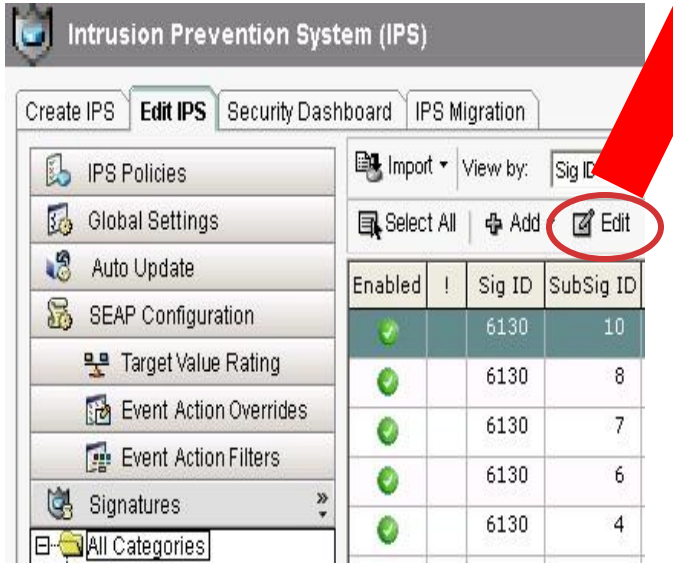
```
router(config)#ip ips signature-category
router(config-ips-category)# category web_server
router(config-ips-category-action)#?
Category Options for configuration:
  alert-severity   Alarm Severity Rating
  enabled          Enable Category Signatures
  event-action     Action
  exit             Exit from Category Actions Mode
  fidelity-rating  Signature Fidelity Rating
  no               Negate or set default values of a command
  retired          Retire Category Signatures
router(config-ips-category-action)#retired false
router(config-ips-category-action)#exit
router(config-ips-category)#exit
Do you want to accept these changes? [confirm]
```

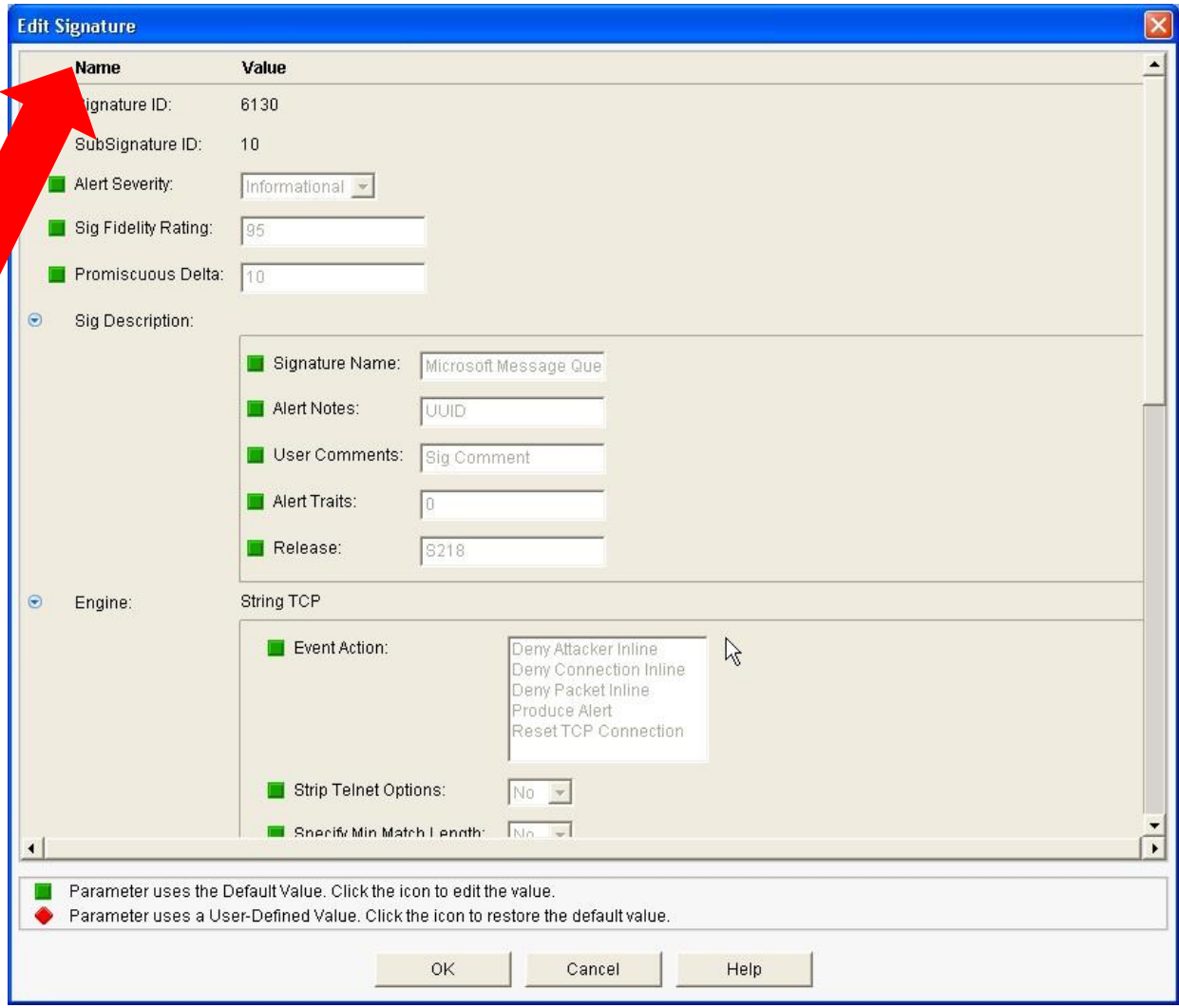
e.g. retired false: the above example shows unretire an entire signature category – instruct router to compile all signatures in this category

Advanced Config Options – Signature Tuning & Customization using CCP



Advanced Config Options – Signature Tuning & Customization using CCP





Advanced Config Options – Configure SEAP using CLI

Target Value Rating (TVR): applies to both individual signature and signature category

```
router(config)#ip ips event-action-rules
router(config-rul)#?
IPS event action rules (SEAP) commands:
  exit           Exit from Event Action Rules (SEAP) Mode
  no             Negate or set default values of a command
  target-value   Target value keyword
router(config-rul)#target-value ?
  high                high
  low                 low
  medium              medium
  mission-critical    mission-critical
  zero-value          zero-value
router(config-rul)#target-value mission-critical target-address ?
  A.B.C.D                       Target IP address
  A.B.C.D  {/nn || A.B.C.D}     Target IP address/mask
router(config-rul)#target-value mission-critical target-address
192.168.1.240 to 192.168.1.253
router(config-rul)#exit
Do you want to accept these changes? [confirm]
```

Advanced Config Options – Configure SEAP using CLI

Attack Severity Rating (ASR) and Signature Fidelity Rating (SFR): Tune by individual signature

```
router#sh ip ips sig sigid 6130 sub 10

 SigID:SubID En  Cmp   Action Sev   Trait   EC   AI   GST   SI  SM SW SFR Rel
 ----------- --  ----  ------ ---   -----  ---- ---- -----  --- -- -- --- ---
  6130:10    Y*  Nr       H  INFO     0     1    0      0    0  FA  N 95  S218


router(config)#ip ips signature-definition
router(config-sigdef)#signature 6130 10
router(config-sigdef-sig)#alert-severity ?
  high           high
  informational  informational
  low            low
  medium         medium
router(config-sigdef-sig)#alert-severity medium
router(config-sigdef-sig)#fidelity-rating ?
  <0-100>  SFR value
router(config-sigdef-sig)#fidelity-rating 100
router(config-sigdef-sig)#end
Do you want to accept these changes? [confirm]


router#sh ip ips signature sigid 6130 sub 10

 SigID:SubID En  Cmp   Action Sev   Trait   EC   AI   GST   SI  SM SW SFR Rel
 ----------- --  ----  ------ ---   -----  ---- ---- -----  --- -- -- --- ---
  6130:10    Y*  Nr       H   MED     0     1    0      0    0  FA  N 100 S218
```

Advanced Config Options – Configure SEAP using CLI

Attack Severity Rating (ASR) and Signature Fidelity Rating (SFR): Tune by entire signature category

```
router(config)#ip ips signature-category
router(config-ips-category)# category ios_ips basic
router(config-ips-category-action)#?
Category Options for configuration:
  alert-severity   Alarm Severity Rating
  enabled          Enable Category Signatures
  event-action     Action
  exit             Exit from Category Actions Mode
  fidelity-rating  Signature Fidelity Rating
  no               Negate or set default values of a command
  retired          Retire Category Signatures
```

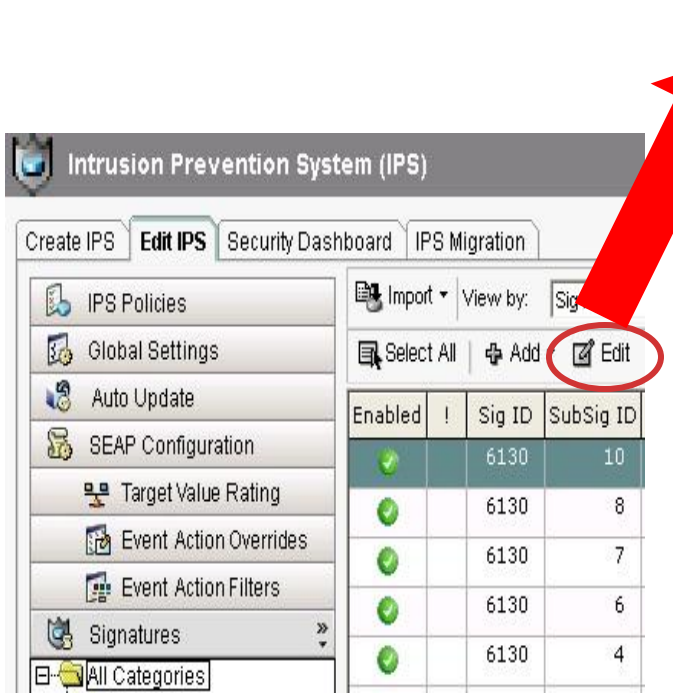
Advanced Config Options – Configure SEAP using CLI

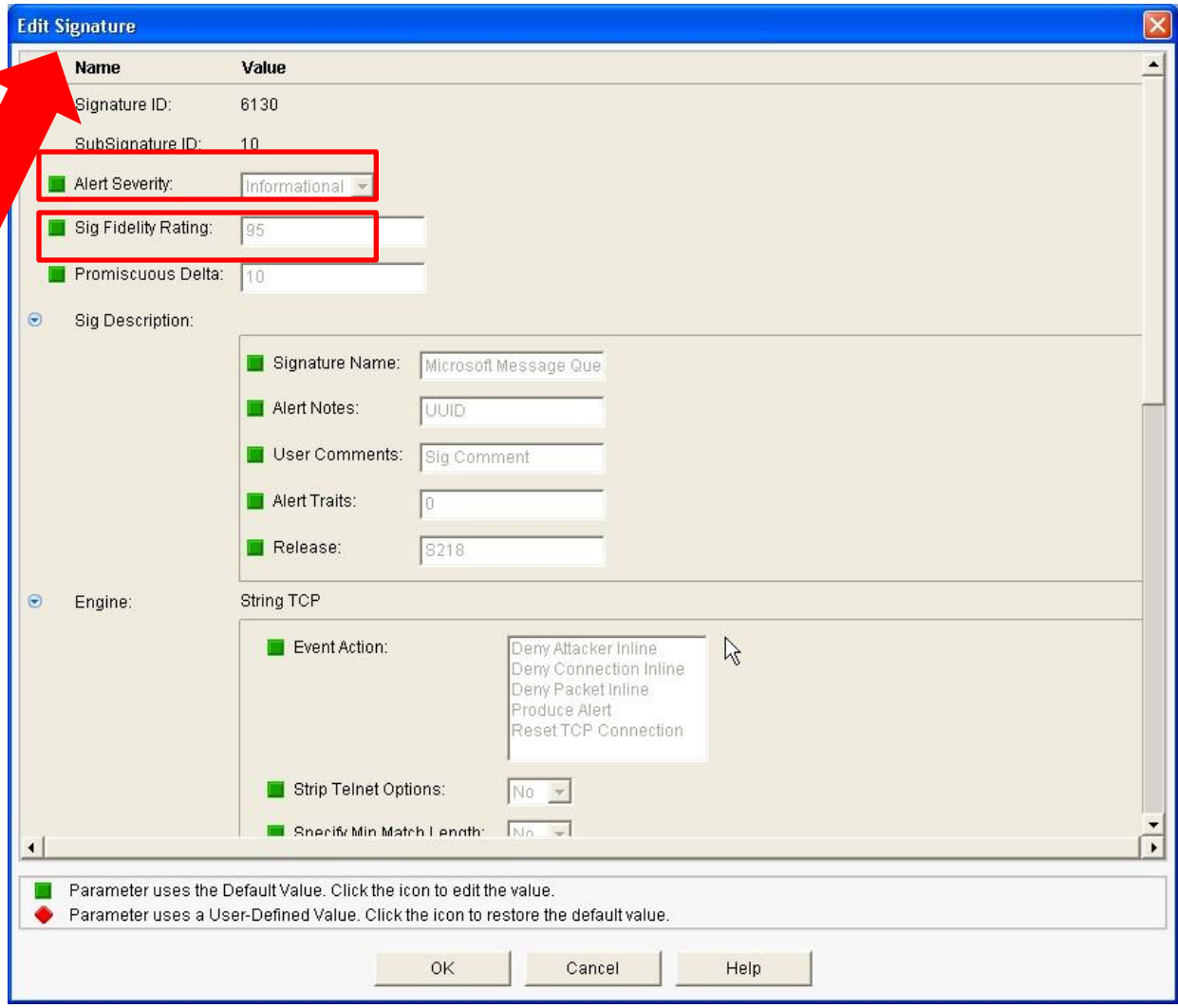
```
router#sh ip ips event-action-rules target-value-rating
Target Value Ratings
Target Value Setting   IP range
mission-critical       192.168.1.240-192.168.1.253
```

```
router#sh ip ips event-action-rules overrides
Overrides
Global Overrides Status: Enabled
Action to Add                      Enabled  Risk Rating
deny-attacker-inline                  Y     75-100
```

```
router#sh ip ips event-action-rules filters
Filters
Global Filters Status: Enabled
 Name - sig-6130
 Sig ID range - 6130
 Subsig ID range - 10
 Attacker address range - 0.0.0.0-255.255.255.255
 Victim address range - 192.168.1.240-192.168.1.253
 Attacker port list - 0-65535
 Victim port list - 0-65535
 Risk rating range - 0-100
 Actions to remove - produce-alert
 Filter status - Enabled
 Stop on match - False
```

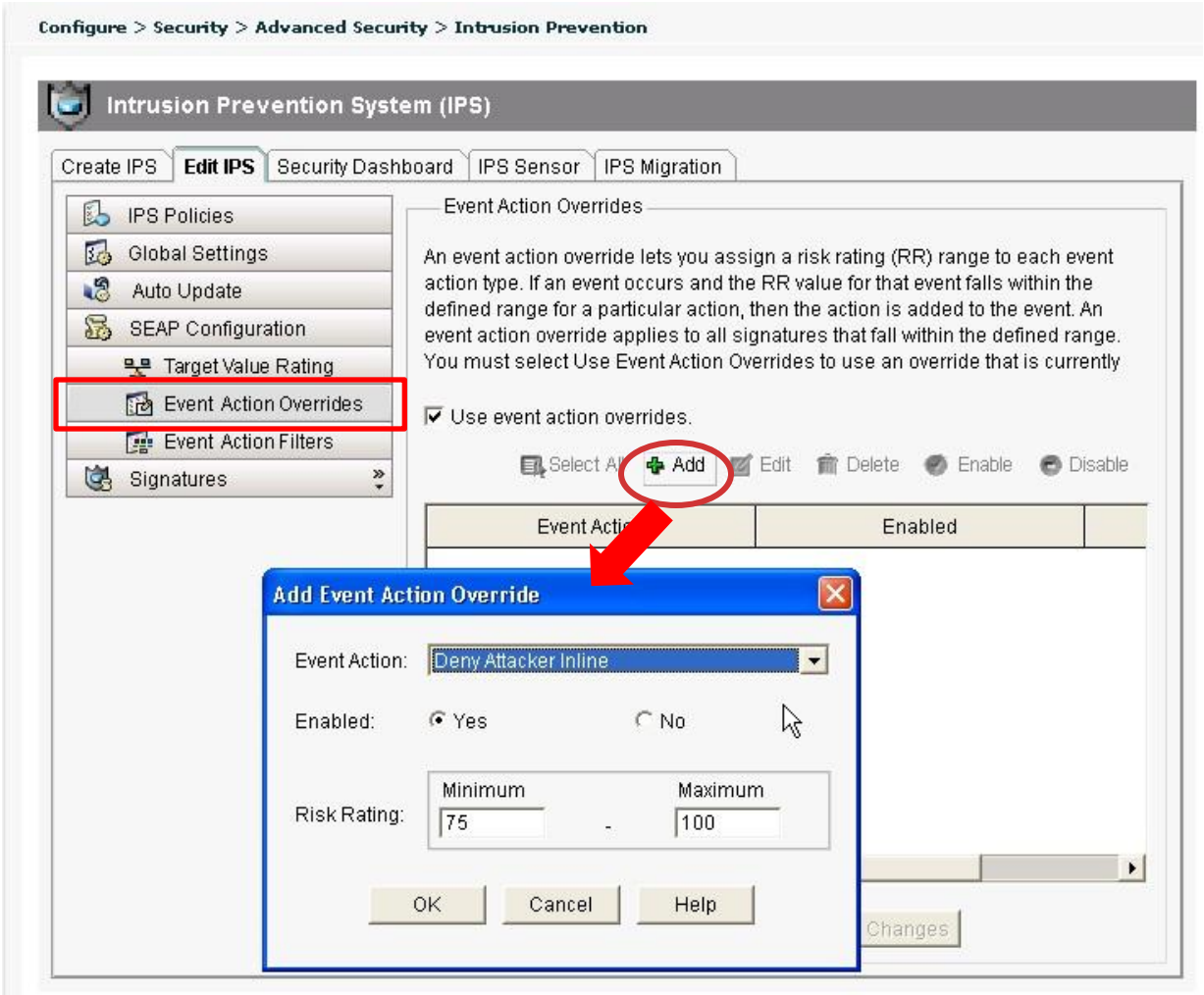
Advanced Config Options – Configure SEAP using CCP





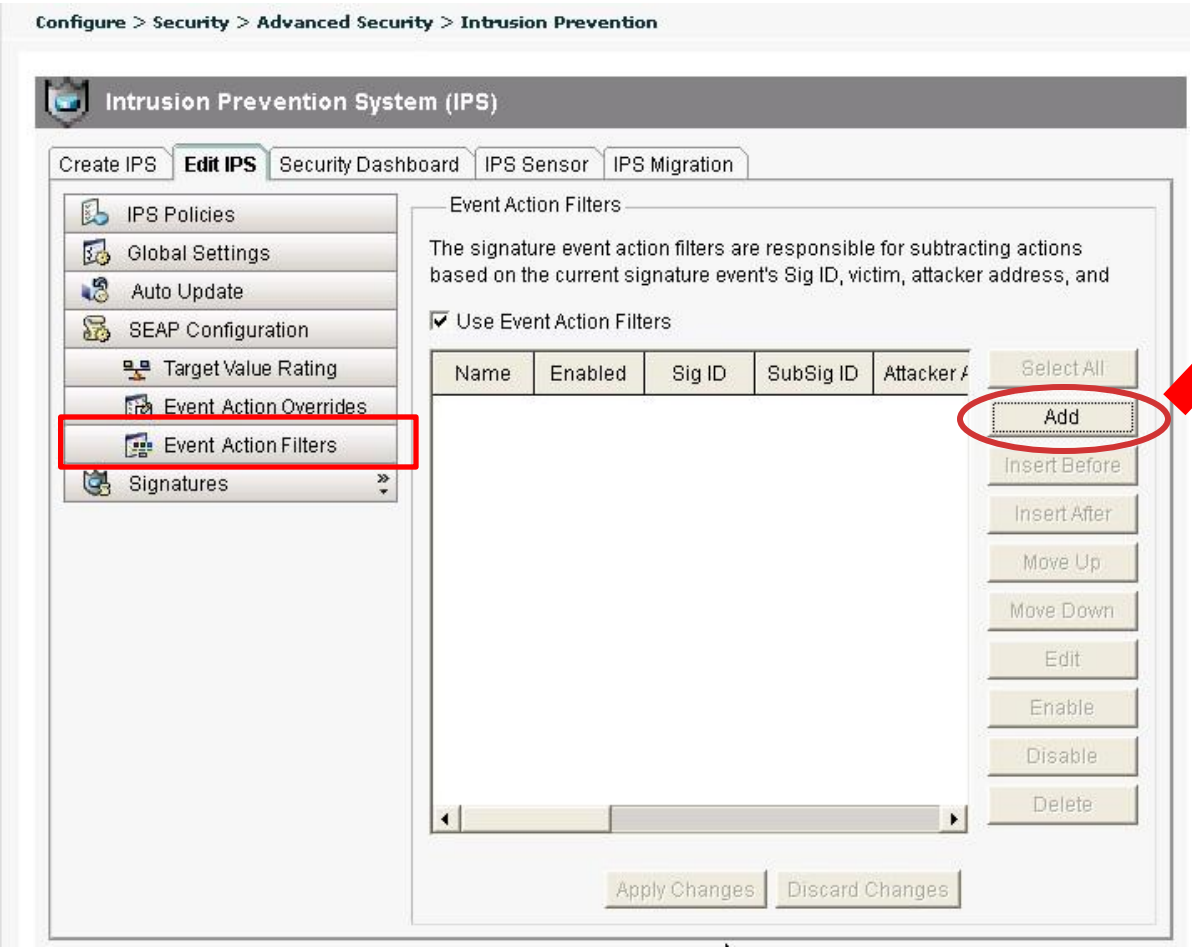
Advanced Config Options – Configure SEAP using CCP

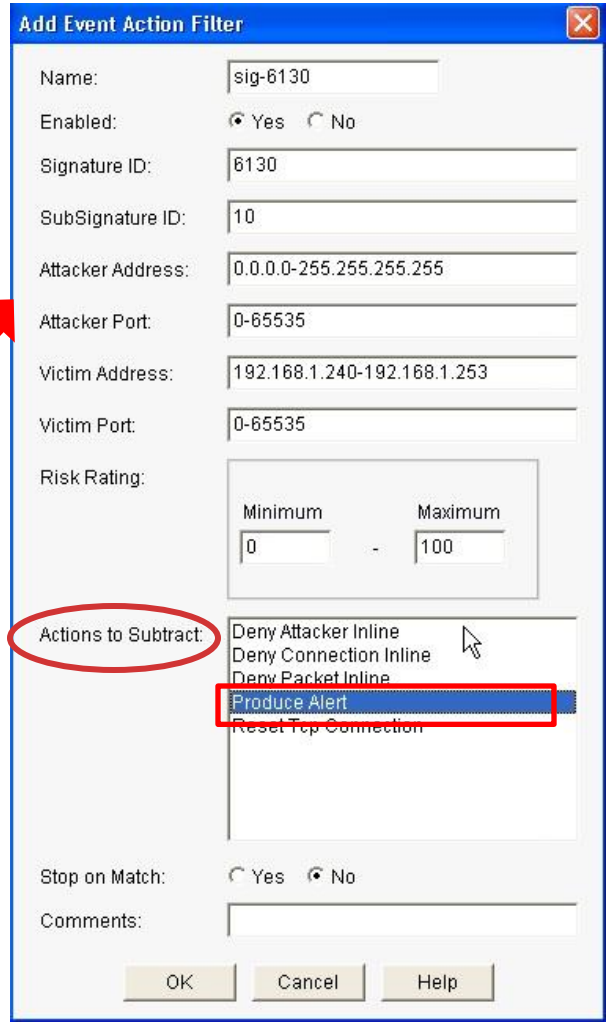
Signature Event Action Overrides (SEAO)



Advanced Config Options – Configure SEAP using CCP

Signature Event Action Filters (SEAF)





Advanced Config Options – Signature Package Update using CLI

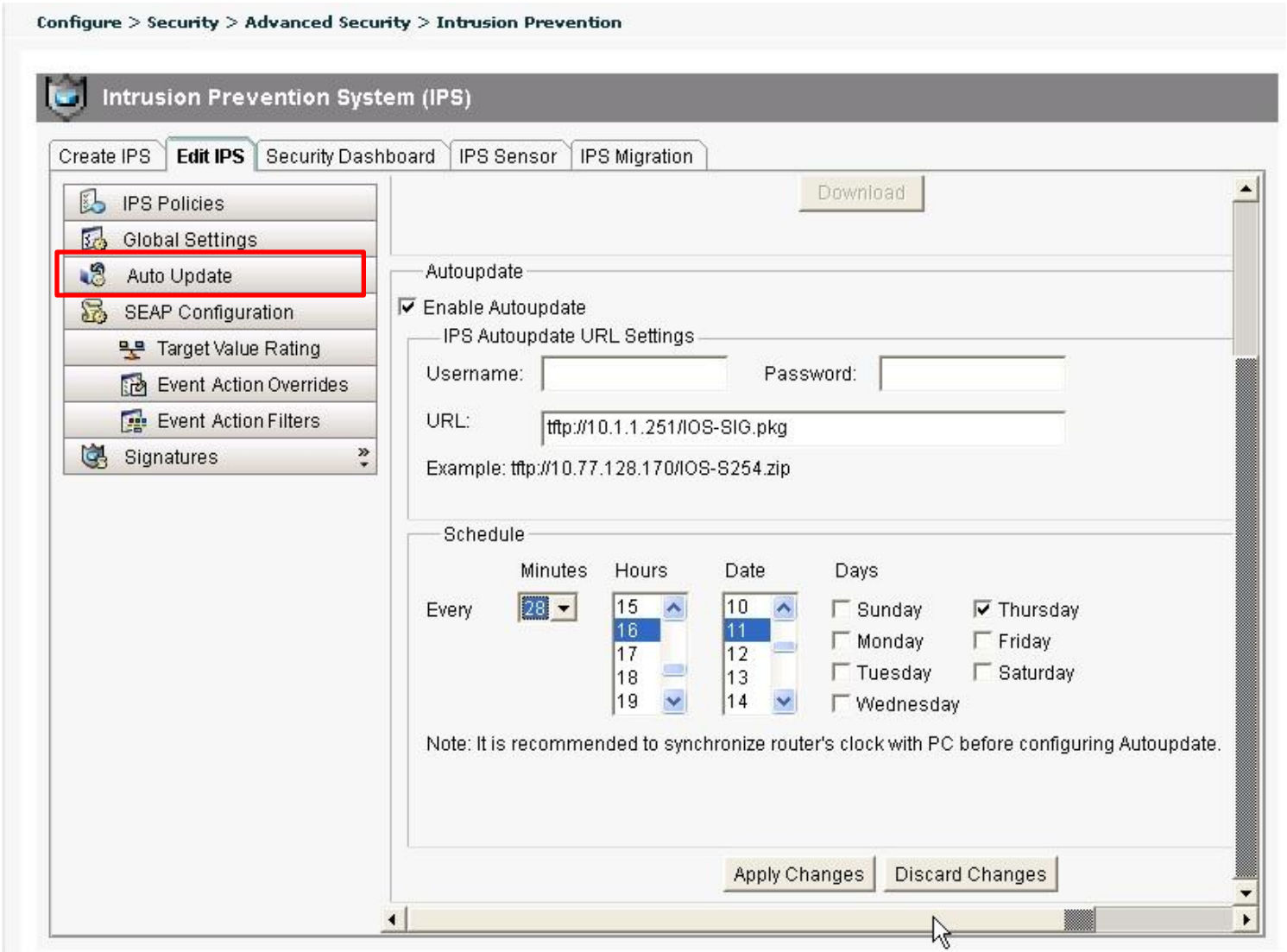
- **Automatically update signature package**
- **Retrieve update from local tftp, http, etc**
- **CLI command: ip ips auto-update**
- **Set router clock or use NTP**
- **You can also use CCP to configure auto update**

```
router(config)# ip ips auto-update
router(config-ips-auto-update)#?
IPS Auto Update Configuration:
  exit      Exit from Auto Update Mode
  occur-at  Specify occurence by calendar time
  url       Specify url to access the files on the server
  username  Specify username to access the files on the server
router(config-ips-auto-update)# occur-at 25 9 11 4
router(config-ips-auto-update)# url tftp://10.1.1.251/IOS-SIG.pkg
router(config-ips-auto-update)#end
```

Advanced Config Options – Signature Package Update using CLI

```
router#sh ip ips auto-update
IPS Auto Update Configuration
  URL                 : tftp://10.1.1.251/IOS-SIG.pkg
  Username            : not configured
  Password            : not configured
  Auto Update Intervals
    minutes (0-59)              : 28
    hours (0-23)                : 16
    days of month (1-31)        : 11
    days of week: (0-6)         : 4
    Last successful load time: 16:28:41 UTC Sep 11 2008
    Last failed load time     : 15:28:53 UTC Sep 11 2008
    Next scheduled load time : to be scheduled in 7 hours 27 minutes
```

Advanced Config Options – Signature Package Update using CCP



Agenda

- IOS IPS Overview
- Technical Review
  - Architecture
  - Packet Flow
  - Configuration
  - Troubleshooting
- Use Cases
- Management
- Best Practices
- Resources

Common Troubleshooting Steps

1. Check IOS IPS configuration, to confirm policy is applied to the right interface in the right direction

```
show run
```

2. Check signatures status, to confirm signatures are compiled

```
show ip ips config
```

```
show ip ips signatures count
```

3. Check flows inspected by IOS IPS, to verify IOS IPS is inspecting traffic

```
show ip ips sessions detail
```

4. Check SDEE alerts / syslog messages, to verify attacks are being detected

```
show ip sdee alerts
```

```
show logging
```

5. Use appropriate debug commands

IOS IPS Troubleshooting Commands

Step 1: Check IOS IPS configuration

```
Router#sh run
Building configuration...


-- output skipped --
!
ip ips config location flash:ips/ retries 1
ip ips notify SDEE
ip ips name iosips
!
ip ips signature-category
  category all
   retired true
  category ios_ips advanced
   retired false
!
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003…

  -- output skipped --

   F3020301 0001
  quit
!
interface GigabitEthernet0/1
 ip address 10.1.1.6 255.255.255.0
 ip ips iosips in
 ip virtual-reassembly
```

Verify IOS IPS policy name and signature storage location

Verify that the “all” signature category is retired

Verify IOS IPS crypto key is configured

Verify that the “all” signature category is retired

IOS IPS Troubleshooting Commands

Step 2: Check IOS IPS Configuration and Signatures Status

```
Router#sh ip ips all

IPS Signature File Configuration Status
    Configured Config Locations: flash:ips/
    Last signature default load time: 16:42:08 PST Mar 1 2008
    Last signature delta load time: 22:59:57 PST Mar 3 2008
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 581
    Total Inactive Signatures: 1623

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name iosips
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
    Quick run mode is enabled
    Interface Configuration
      Interface GigabitEthernet0/1
        Inbound IPS rule is iosips
        Outgoing IPS rule is not set

IPS Category CLI Configuration:
    Category all:
        Retire: True
    Category ios_ips advanced:
        Retire: False
```

Determine the # of active signatures

Verify the IOS IPS policy is applied to the right interface in the right direction

Verify the signature categories being used

IOS IPS Troubleshooting Commands

Step2: Check Signatures Status

```
Router#show ip ips signatures count

Cisco SDF release version S318.0
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 27
      service-msrpc enabled signatures: 27
      service-msrpc retired signatures: 19
      service-msrpc compiled signatures: 1
      service-msrpc inactive signatures - invalid params: 7

Total Signatures: 2204
   Total Enabled Signatures: 873
   Total Retired Signatures: 1617
   Total Compiled Signatures: 580
   Total Signatures with invalid parameters: 7
   Total Obsoleted Signatures: 11
```

Check signature release version, if version is V0.0, then signature package is not loaded properly

Check there are signatures being compiled, if the number is 0, then signatures are not loaded properly

IOS IPS Troubleshooting Commands

Step 3: Check Flows Inspected by IOS IPS

Verify that IOS IPS is indeed inspecting traffic at the right interface in the right direction by looking at the IP source and destination addresses

```
Router#show ip ips sessions detail
Established Sessions

 Session 47506A34 (10.1.1.252:3959)=>(192.168.1.249:21) tcp SIS_OPEN
  Created 00:02:49, Last heard 00:02:44
  Bytes sent (initiator:responder) [25:95]
  sig cand list ID 14272
  sig cand list ID 14273
```

src. address/port and dest. address/port

bytes sent and received

IOS IPS Troubleshooting Commands

Step 4: Check alert messages

Verify that the router is seeing IOS IPS related event and alert messages.

```
Router#sh logging
   Syslog logging: enabled (12 messages dropped, 7 messages rate-limited,
                    0 flushes, 0 overruns, xml disabled, filtering disabled)

   -- output skipped --

   Log Buffer (4096 bytes):

   *Mar 22 03:53:13.827: %IPS-4-SIGNATURE: Sig:5114 Subsig:1 Sev:75 WWW IIS Unicode
   Attack [10.1.1.252:4150 -> 192.168.1.249:80] RiskRating:75
   *Mar 22 03:53:13.827: %IPS-4-SIGNATURE: Sig:5081 Subsig:0 Sev:100 WWW WinNT cmd.exe
   Access [10.1.1.252:4150 -> 192.168.1.249:80] RiskRating:100
```

```
Router#sh ip sdee alerts
   Alert storage: 200 alerts using 75200 bytes of memory
                                    SDEE Alerts
         SigID    Sig Name                      SrcIP:SrcPort          DstIP:DstPort
                                                    or Summary Info
      1:  5114:1  WWW IIS Unicode Attack        10.1.1.252:4150      192.168.1.249:80
      2:  5081:0  WWW WinNT cmd.exe Access      10.1.1.252:4150      192.168.1.249:80
```

Cisco IOS IPS Debugging Commands

Step 5: Use debug commands

- Enable debugs on specified IOS IPS engines

```
Router# debug ip ips timers
Router# debug ip ips [object-creation | object-deletion]
Router# debug ip ips function trace
Router# debug ip ips detail
```


Not recommended in production network

- L3/L4 debug commands:

```
Router# debug ip ips [ip | icmp | tcp | udp]
```

- Application-level debug commands:

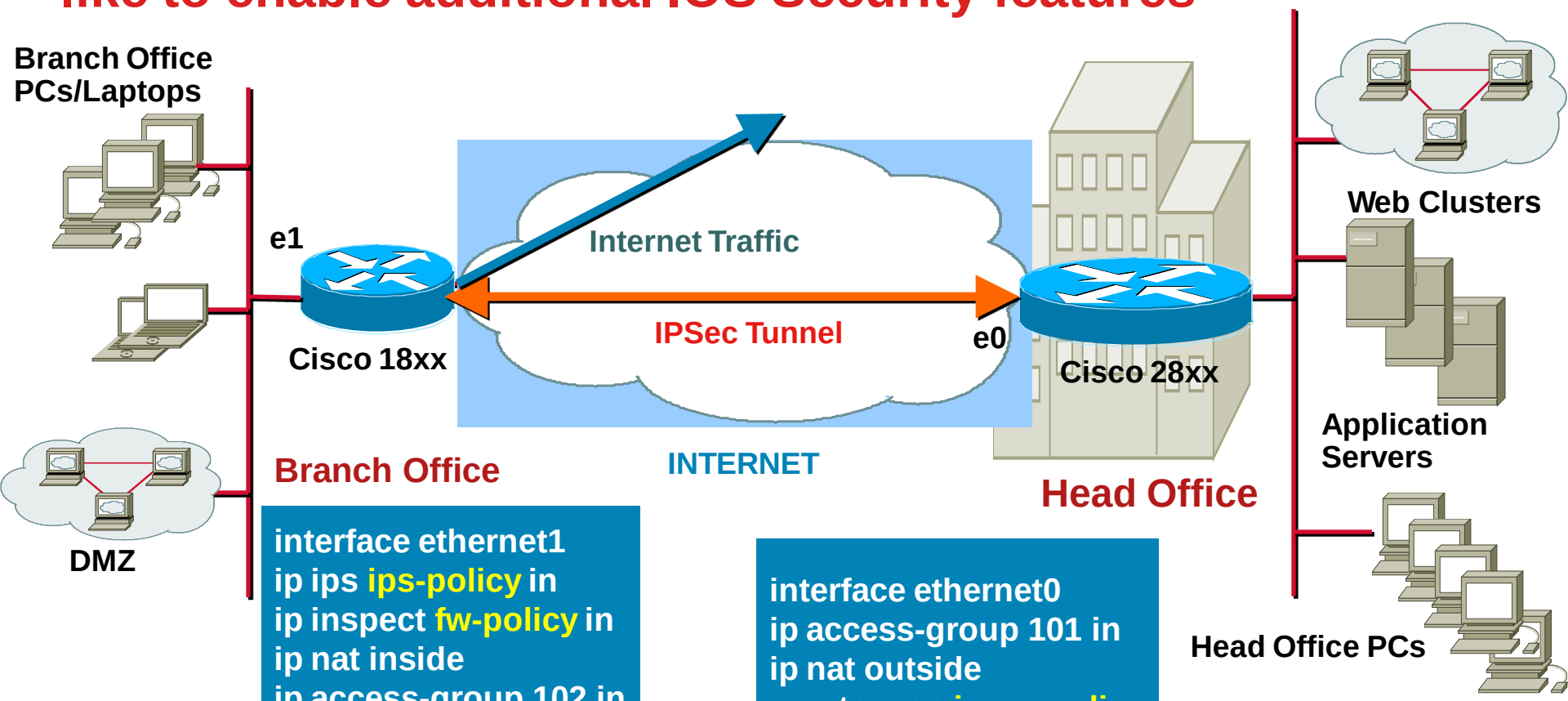
```
Router# debug ip ips [tftp | smtp | ftp-cmd | ftp-token]
```

- Enable debug on specified SDEE attributes

```
Router# debug ip sdee [alerts | details | messages | requests | subscriptions ]
```

Case Study: Enterprise Customer Deploys IOS Security Features

Customer has an existing IPSec VPN running and would like to enable additional IOS Security features



Troubleshooting

Customer Cannot Ping to Any of the Servers at Headquarter

```
C:\Documents and Settings\Administrator.SECURITY-COMP3>ping 19.1.1.1

Pinging 19.1.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 19.1.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\Documents and Settings\Administrator.SECURITY-COMP3>_
```

- Step 1: Check if the ACLs are not blocking legitimate ICMP packets using “show access-list” and verify the counters

  Extended IP access list 102

  10 permit icmp any any

  20 permit tcp any any (51 matches)

  30 permit udp any any (3 matches)

Troubleshooting

- Step 2: Create an access-list 180

  "**access-list 180 permit icmp any any** "

  enable debug "**debug ip packet detail 180**"

  Show logging doesn't show anything

- Step 3: Check if the FW session table has any information about this using "show ip inspect session details"

  Router# show ip inspect sessions detail

  Established Sessions

  Session 44350B7C (106.0.0.15:3404)=>(19.1.1.1:23) tcp SIS_OPEN

Troubleshooting

- Step 4: Check if the SDEE messages are enabled

  "**show ip sdee alerts**"

  Router# show ip sdee events

  Alert storage: 30 alerts using 8160 bytes of memory

  Message storage: 500 messages using 212000 bytes of memory

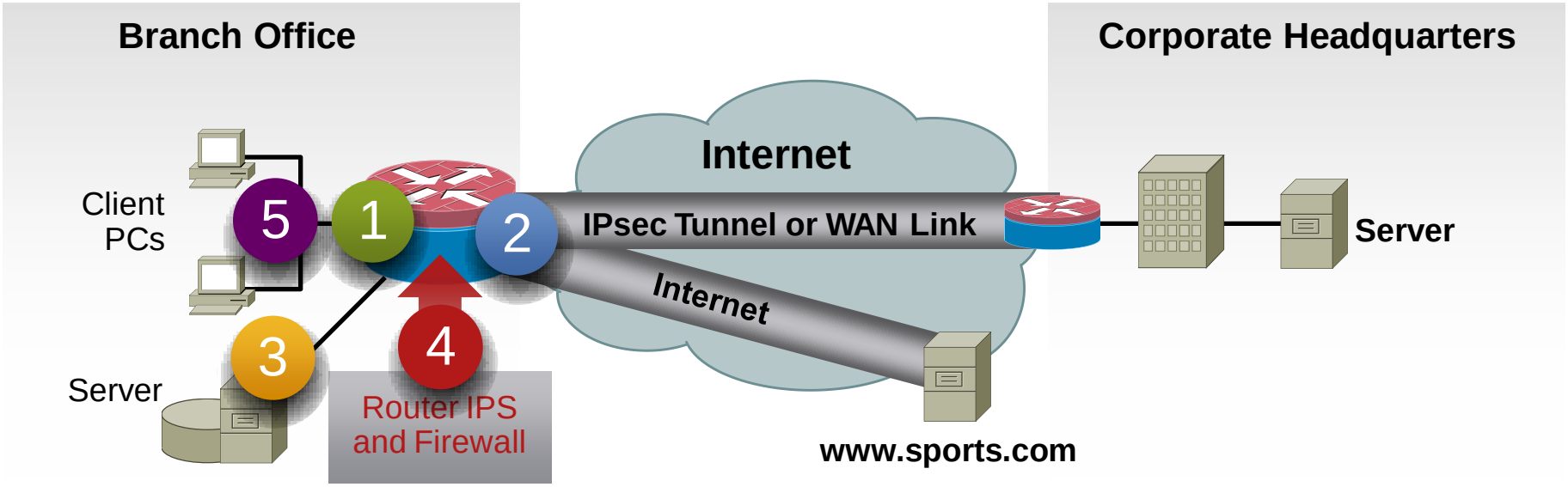
SDEE Events

	Time		Type	Description
1:	01:26:42 UTC Jun 21 2005	ALERT	Sig ID	2004:0 ICMP Echo Req
2:	01:26:43 UTC Jun 21 2005	ALERT	Sig ID	2004:0 ICMP Echo Req
3:	01:26:44 UTC Jun 21 2005	ALERT	Sig ID	2004:0 ICMP Echo Req

Agenda

- IOS IPS Overview
- Technical Review
  - Architecture
  - Packet Flow
  - Configuration
  - Troubleshooting
- Use Cases
- Management
- Best Practices
- Resources

Cisco IOS IPS Common Use Cases



1 **Protect Branch PCs from Internet Worms**

Use IPS and Firewall on a Cisco Router for Worm Protection

2 **Move Worm Protection to the Network Edge**

Apply IPS on Traffic From Branch to HQ to Stop Worms and Attacks From Infected Branch PCs

3 **Protect Branch-Office Servers**

Apply IPS and Firewall on Branch Router to Protect Local Servers at the Branch From Attacks

Avoid Need for a Separate Device to Protect Servers

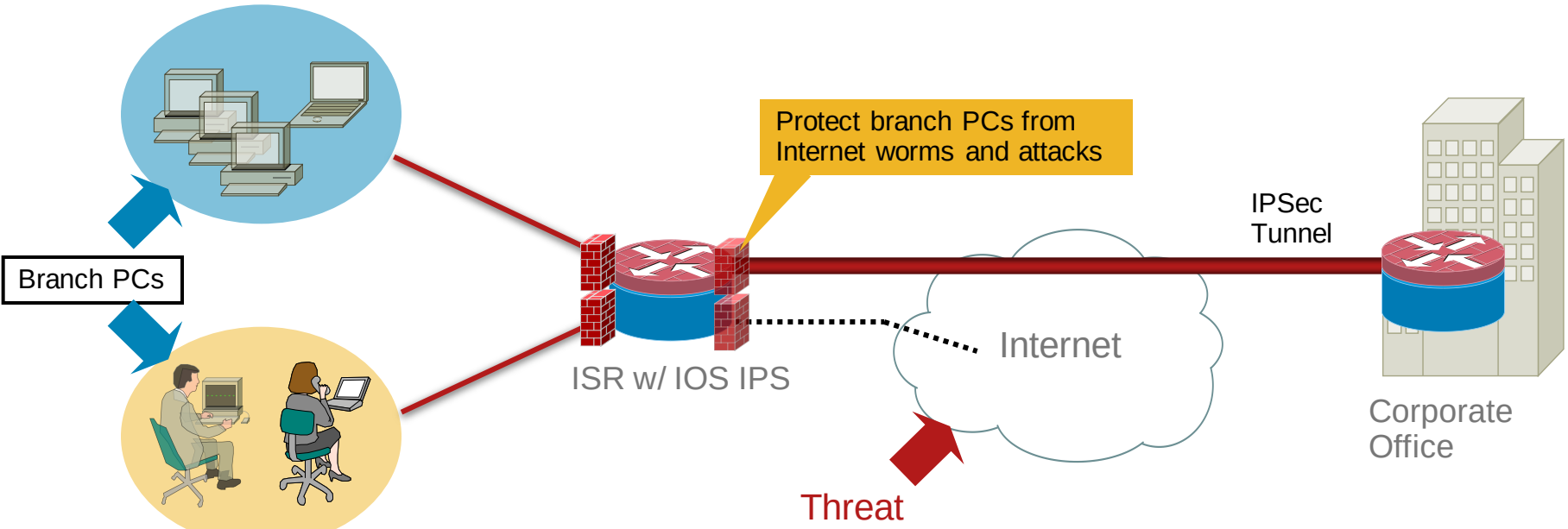
4 **Satisfy PCI Compliance Requirements**

5 **Transparent (layer 2) IPS**

Cisco IOS IPS Use Case 1

Protect Branch PCs from Internet Worms

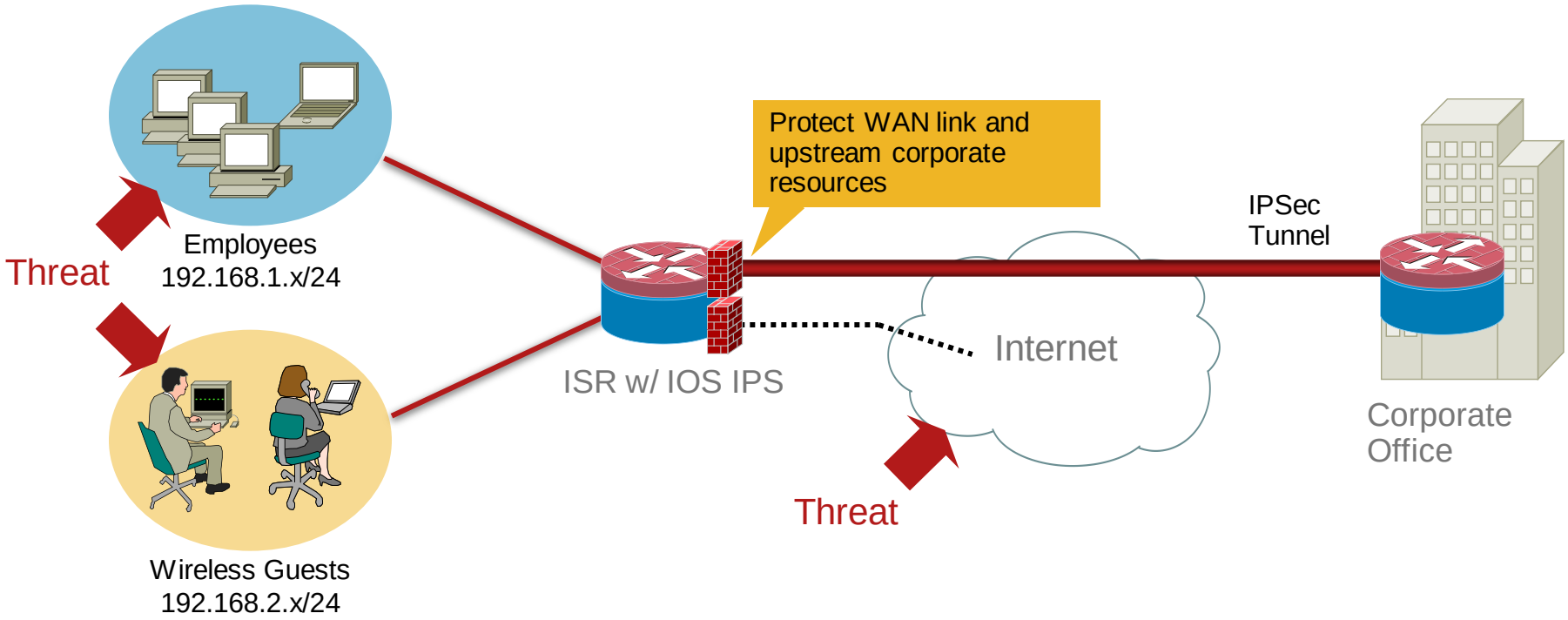
- Branch office LAN are prone to attacks from Internet, contaminated laptops and rogue wireless access points



Cisco IOS IPS Use Case 2

Protect WAN Link and Head Office

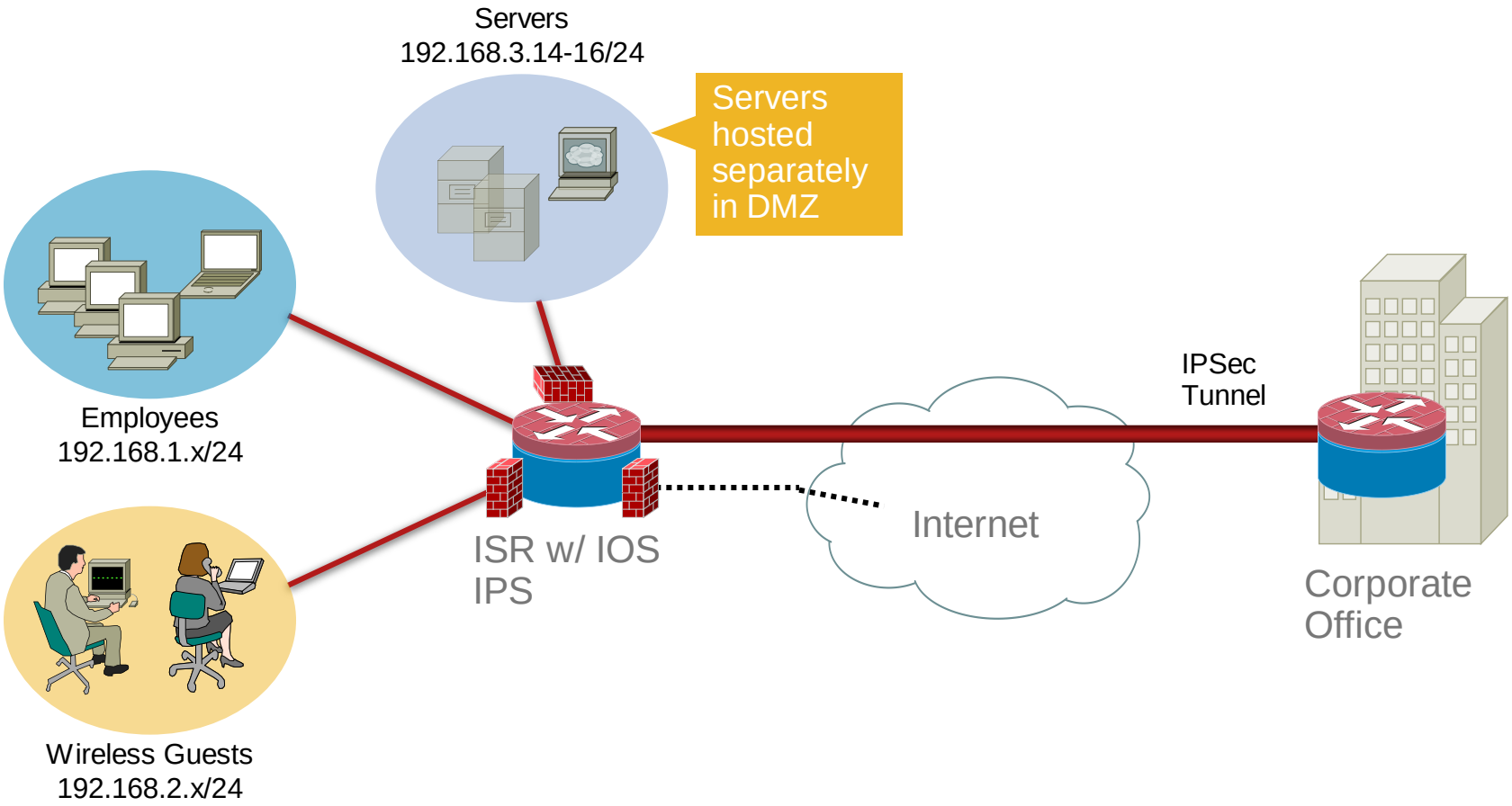
- Branch office contaminated PCs, laptops and rogue wireless access points
- Stops worms and attacks *before* they enter corporate or SP network
- Moves attack protection to the network edge



Cisco IOS IPS Use Case 3

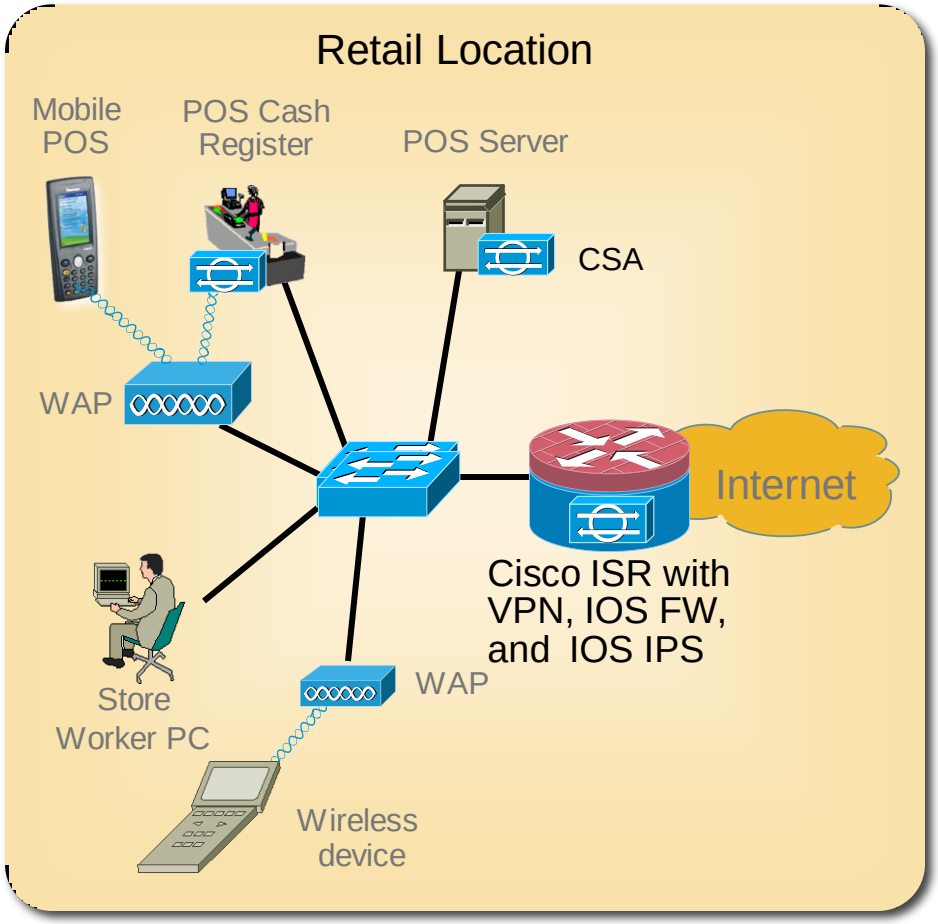
Protect Servers at Remote Sites

- Protect distributed application servers and web servers hosted at remote sites



Cisco IOS IPS Use Case 4

Enhanced PCI Compliance, Requirement 11



- Provides Intrusion Prevention in depth, as part of PCI Compliant Self Defending Network
- Event correlation provides audit trail for tests and validation exercises
- Integrates with IOS FW, IPSEC, SSL VPN and other IOS security technologies for complete solution
- Filters inspected traffic via ACLs

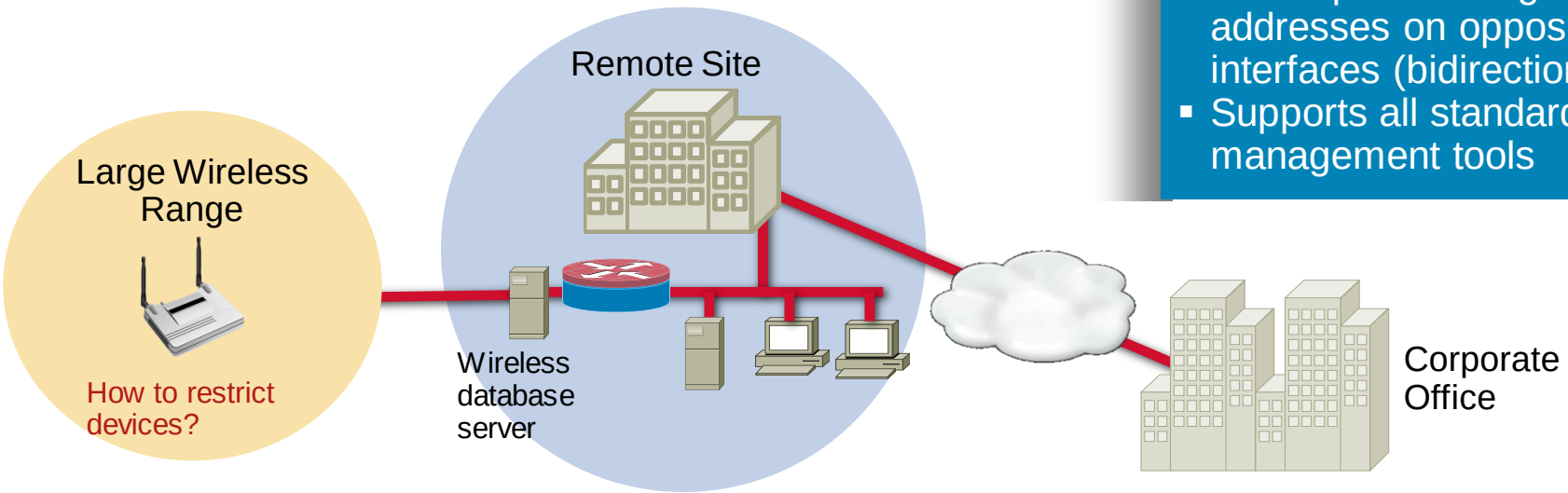
Cisco IOS IPS Use Case 5

Transparent IPS

- Provides Layer 2 connectivity with Layer 3 IPS support
- Easily add IPS to existing networks—no IP subnet renumbering required
- Operates on bridged packets; Layer 3 IPS continues to operate on routed packets

Features Supported

- Sub-interfaces and VLAN trunks
- Spanning Tree protocol
  - Handles PBDU packets correctly per 802.1d, not just “pass/drop”
- Mix Layer 2 and Layer 3 IPS on the same router
- No need for IP addresses on the interfaces
- DHCP pass-through assigns addresses on opposite interfaces (bidirectional)
- Supports all standard management tools



Agenda

- IOS IPS Overview
- Technical Review
  - Architecture
  - Packet Flow
  - Configuration
  - Troubleshooting
- Use Cases
- Management
- Best Practices
- Resources

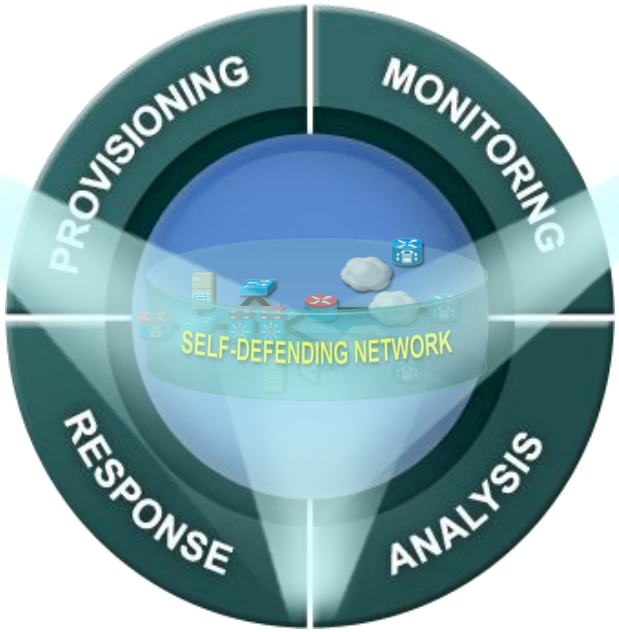
Cisco IOS IPS
Provisioning and Monitoring Options

IPS Signature Provisioning		IPS Event Monitoring		
Up to 5 devices	**More Than 5 devices**	**1 device**	**Up to 5 devices**	**More Than 5 devices**
Cisco Configuration Professional (CCP)	**Same Signature Set:** Option 1: Cisco Security Manager 3.2.1 Option 2: Cisco Configuration Professional (CCP) and Cisco Configuration Engine (CNS) **Otherwise:** Single or multiple Cisco Security Manager 3.2.1 instances	IPS Manager Express (IME) or Cisco Configuration Professional (CCP) or syslog server	IPS Manager Express (IME) or syslog server	Cisco Security MARS or syslog server

Cisco Security Management Suite

Cisco Configuration Professional

- Quickest way to setup a device
- Wizards to configure firewall, IPS, VPN, QoS, and wireless
- Ships with device



Cisco Security Manager

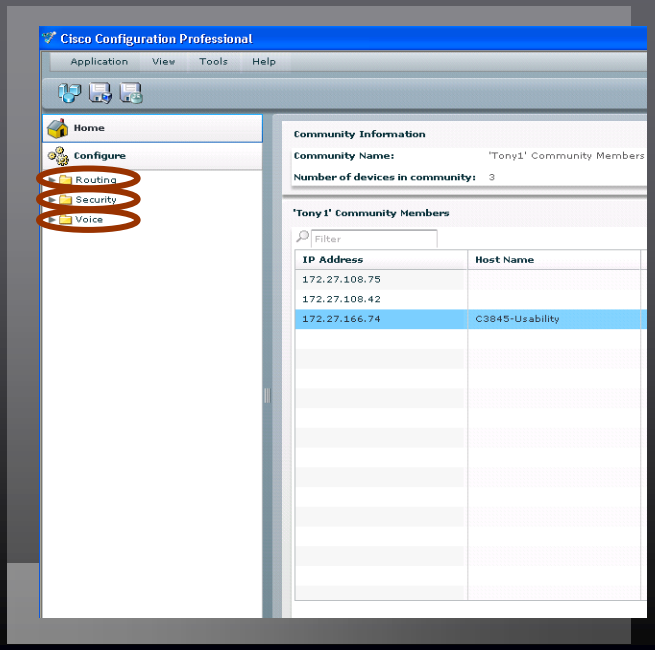
- New solution for configuring routers, appliances, switches
- New user-centered design
- New levels of scalability

Cisco Security MARS

- Solution for monitoring and mitigation
- Uses control capabilities within infrastructure to eliminate attacks
- Visualizes attack paths

Cisco Configuration Professional (CCP)

Intuitive device management GUI for easily configuring Cisco's Integrated Services Routers



- Easy to use with smart wizards and built-in tutorials
- Results in Cisco recommended IOS configurations
- Features:
  - Routing, Interfaces, QoS, Wireless
  - Security (firewall, IPS, IPSec VPN, etc)
  - Voice (CUCME and CUCE)
- CCP is the replacement for SDM

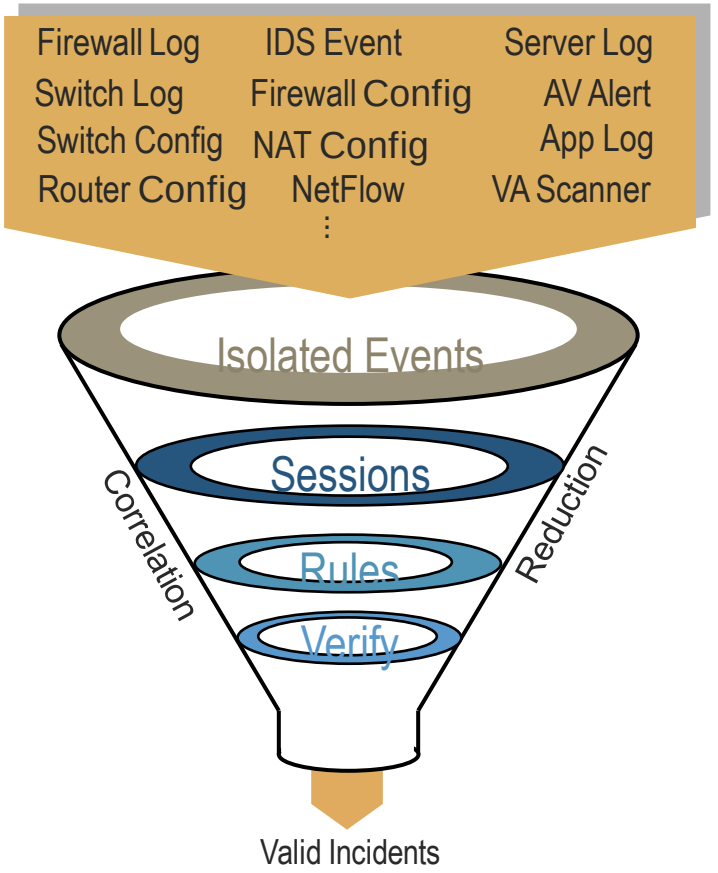
Cisco Configuration Professional

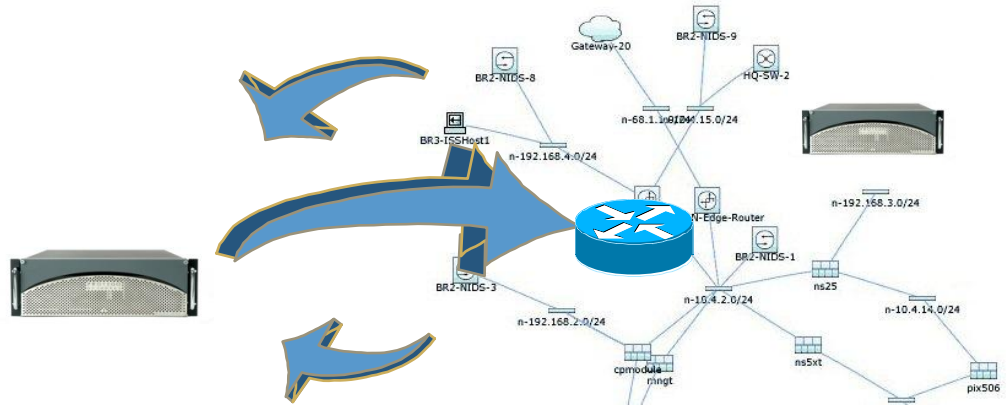
Cisco Security Manager (CSM) 3.2.1
Cisco IOS IPS Network-wide Configuration

- **Supports Cisco IOS® Software 12.4(11)T2 and later**
- **Signature file auto update**
- **Custom signature templates**
- **Wizards to Create and Update Signatures**
- **Rollback to previous Signature release and policy configuration**
- **Filtering based on signature category, release, fidelity or severity**
- **Copying IPS policies from one device to others**
- **Cloning signatures to create custom signatures**
- **Secure provisioning via IDCONF transactions over HTTPS**
- **Configuration of risk-based automated event action filters and overrides**

Cisco Security Monitoring, Analysis and Response System (CS-MARS)

- Cisco® CS-MARS "Know the battlefield": Mitigation and response turnkey system
- Gain network intelligence
  - Use the network you have, correlate router's NetFlow (WAN data) with firewall, IDS, switch data
  - Build topology and traffic-flow model
  - Know device configuration, enforcement abilities
- ContextCorrelation™
  - Correlates, reduces, categorizes events, validates incidents
- Allows for response





Agenda

- IOS IPS Overview
- Technical Review
  - Architecture
  - Packet Flow
  - Configuration
  - Troubleshooting
- Use Cases
- Management
- Best Practices
- Resources

IOS IPS Best Practices

- Understanding of terms used for signature status
- Dealing with memory allocation errors when compiling signatures
- Total number of signatures can be compiled
- Dealing with signature failing to compile
- Configuration steps
- Dealing with IOS IPS policy applied at the wrong direction and/or interface
- Dealing with signature that do not fire with matching traffic
- Dealing with Packet/Connections dropped due to packets arriving out of order

Understanding of Terms Used for Signature Status

- Retire vs. unretire
- Enable vs. disable
- Compiled vs. loaded
- Cisco IOS IPS inherited these terms from IPS 4200 series appliance
- Due to memory constraints, most of the signatures on router are retired by default
- IOS IPS users need to worry about enable/disable as well as retire/unretire

Understanding of Terms Used for Signature Status (Cont.)

- Retire vs. unretire

  Select/de-select which signatures are being used by IOS IPS to scan traffic

  Retiring a signature means IOS IPS will NOT compile that signature into memory for scanning

  Unretiring a signature instructs IOS IPS to compile the signature into memory and use the signature to scan traffic

  You can use IOS command-line interface (CLI) or SDM/CCP to retire or unretire individual signatures or a signature category

Understanding of Terms Used for Signature Status (Cont.)

- Enable vs. disable

  Enable/disable is NOT used to select/de-select signatures to be used by IOS IPS

  Enabling a signature means that when triggered by a matching packet (or packet flow), the signature takes the appropriate action associated with it

    However, only unretired AND successfully compiled signatures will take the action when they are enabled. In other words, if a signature is retired, even though it is enabled, it will not be compiled (because it is retired) and it will not take the action associated with it

  Disabling a signature means that when triggered by a matching packet (or packet flow), the signature DOES NOT take the appropriate action associated with it

    In other words, when a signature is disabled, even though it is unretired and successfully compiled, it will not take the action associated with it

  You can use IOS command-line interface (CLI) or SDM/CCP to enable or disable individual signatures or a signature category

Understanding of Terms Used for Signature Status (Cont.)

- Compiled vs. loaded

  Loading refers to the process where IOS IPS parse the signature files (XML files in the config location) and fill in the signature database

    This happens when signatures are loaded via “copy <sig file> idconf” or the router reboots with IOS IPS already configured

  Compiling refers to the process where the parameter values from unretired signatures are compiled into a regular expression table

    This happens when signatures are unretired or when other parameters of signatures belonging to that regular expression table changes

    Once signatures are compiled, traffic is scanned against the compiled signatures

Dealing with Memory Allocation Errors When Compiling Signatures

- The number of signatures that can be compiled depends on the free memory available on the router
- When router does not have enough memory to compile signatures, memory allocation failure messages are logged
- Already compiled signatures will still be used to scan traffic. No additional signatures will be compiled for that engine during the compiling process. IOS IPS will proceed with compiling signatures for the next engine

```
*Mar 18 07:09:36.887: %SYS-2-MALLOCFAIL: Memory allocation of 65536 bytes failed from 0x400C1024, alignment 0

Pool: Processor  Free: 673268  Cause: Memory fragmentation

Alternate Pool: None  Free: 0  Cause: No Alternate pool

 -Process= "Exec", ipl= 0, pid= 3,  -Traceback= 0x4164F41C 0x400AEF1C 0x400B4D58 0x400B52C4 0x400C102C
0x400C0820 0x400C23EC 0x400C0484 0x424C1DEC 0x424C2A4C 0x424C2FF0 0x424C31A0 0x430D6ECC 0x430D7864 0x430F0210
0x430FA0E8

*Mar 18 07:09:36.911: %SYS-2-CHUNKEXPANDFAIL: Could not expand chunk pool for regex. No memory available -
Process= "Chunk Manager", ipl= 3, pid= 1,  -Traceback= 0x4164F41C 0x400C06FC

*Mar 18 07:09:37.115: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 12024:0 - compilation of regular
expression failed

*Mar 18 07:09:41.535: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 5280:0 - compilation of regular
expression failed
*Mar 18 07:09:44.955: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 5284:0 - compilation of regular
expression failed
*Mar 18 07:09:44.979: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 12023:0 - compiles discontinued for this
engine
```

Dealing with Memory Allocation Errors When Compiling Signatures – Best Practice

- The pre-defined IOS IPS Basic and Advanced signature categories contain optimum combination of signatures for all standard memory configurations, providing a good starting point
- Never unretire the “all” category
- For routers with 128MB memory, start with the IOS IPS Basic category
- For routers with 256MB memory, start with the IOS IPS Advanced category
- Then customize the signature set by unretiring/retiring few signatures at a time according to your network needs
- Pay attention to the free memory every time after you unretiring/retiring signatures

Total Number of Signatures that Can Be Compiled

- There is no magic number!
- Many factors can have impact:

  Available free memory on router

  Type of signatures being unretired, e.g. signatures in the complex STRING.TCP engine

- When router free memory drops below 10% of the total installed memory, then stop unretiring signatures

Dealing with Signatures Failing to Compile

- There are mainly three reasons that could cause a signature fail to compile

  Memory constraint, running out of memory

  Signatures are not supported in IOS IPS: META signatures

  Regular Expression table for a particular engine exceeds 32MB entries

- Check the list of supported signatures in IOS IPS at:

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd8062ac75.html

- Retire signatures not supported by IOS IPS and signatures not applicable to your network to save memory

Configuration Steps

- Follow the steps in the following order for initial Cisco IOS IPS configuration:

  Step 1: Download IOS IPS signature package to PC

  Step 2: Create IOS IPS configuration directory

  Step 3: Configure IOS IPS crypto key

  Step 4: Create IOS IPS policy and apply to interface(s)

  Remember to FIRST retire the “all” category

  Step 5: Load IOS IPS signature package

- Next verify the configuration and signatures are compiled:

  show ip ips configuration

  show ip ips signatures count

Configuration Steps – Cont.

- Next you can start to tune the signature set with the following options:

  Retire/unretire signatures (i.e. add/remove signatures to/from the compiled list)

  Enable/disable signatures (i.e. enforce/disregard actions)

  Change actions associated with signatures

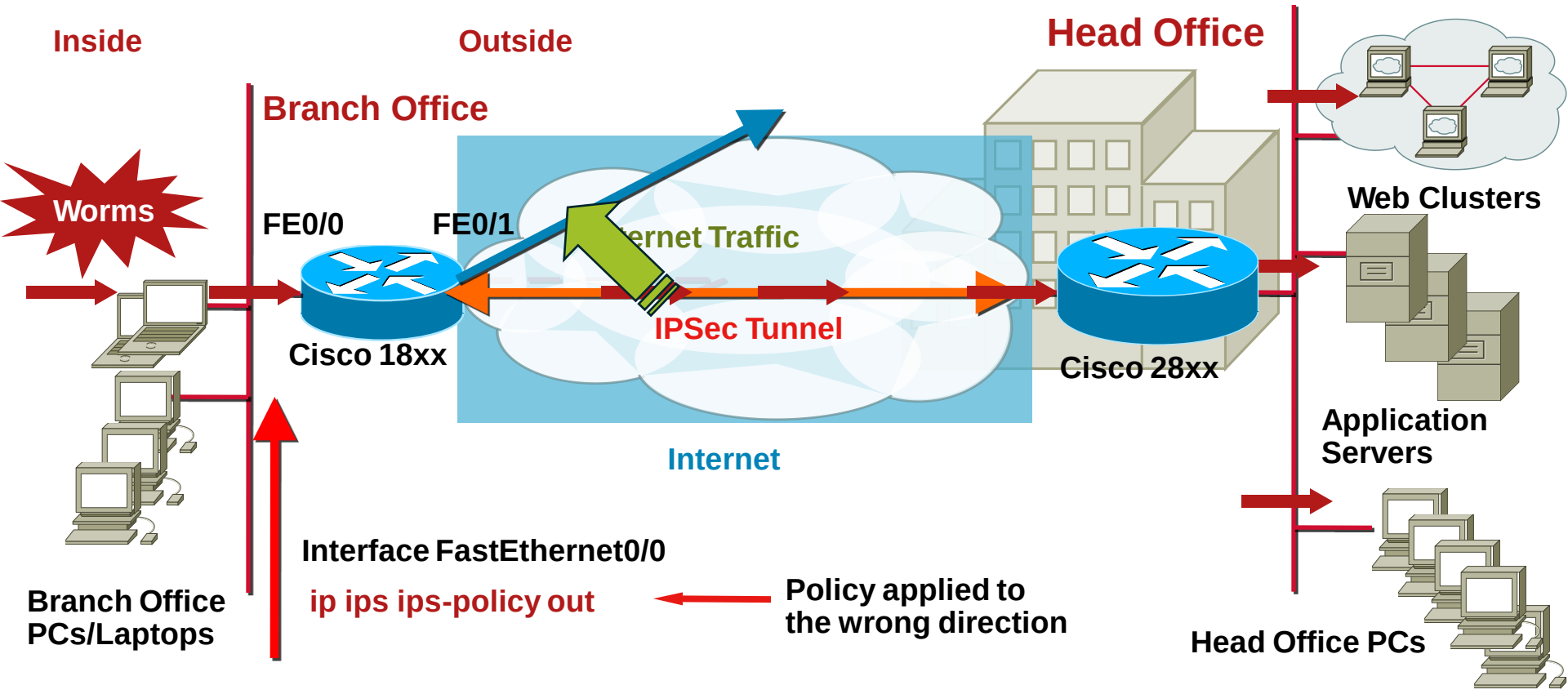
- Refer to Getting Started Guide at:

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd805c4ea8.html

Dealing with IOS IPS Policy Applied at the Wrong Direction/Interface—Incorrect Configuration

Case A: Issue

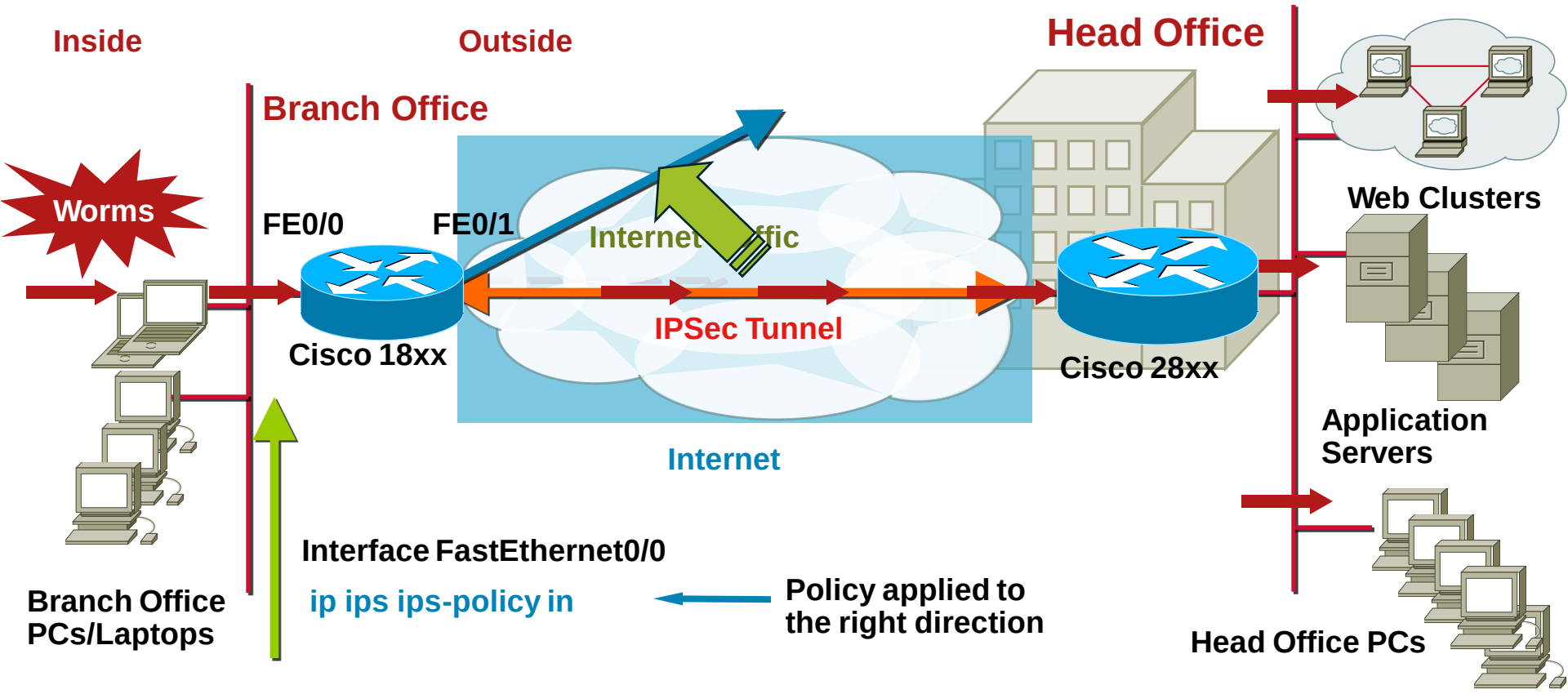
Protecting Attacks from Inside



Dealing with IOS IPS Policy Applied at the Wrong Direction/Interface—Resolution

Case A: Solution

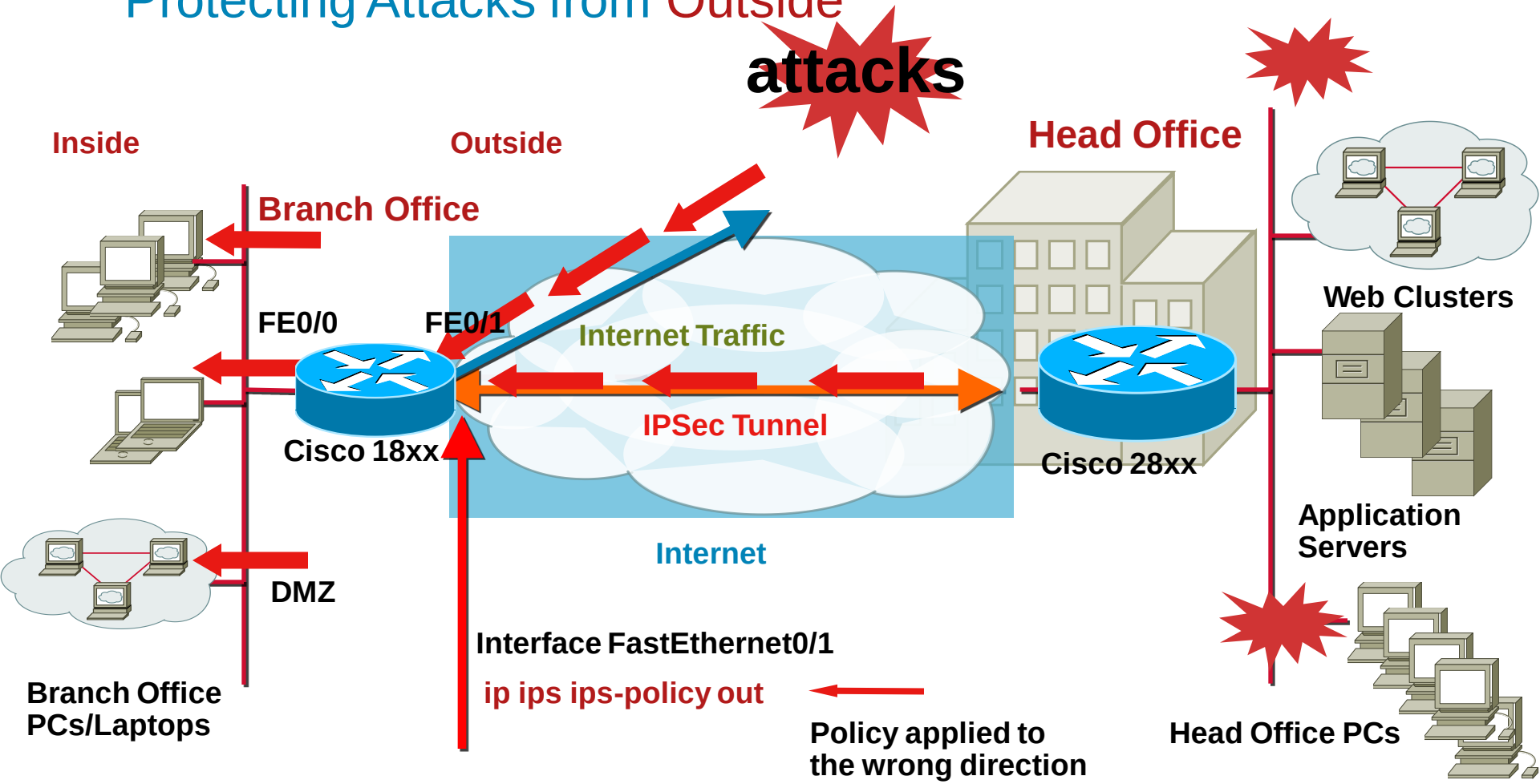
Protecting Attacks from Inside



Dealing with IOS IPS Policy Applied at the Wrong Direction/Interface—Incorrect Configuration

Case B: Issue

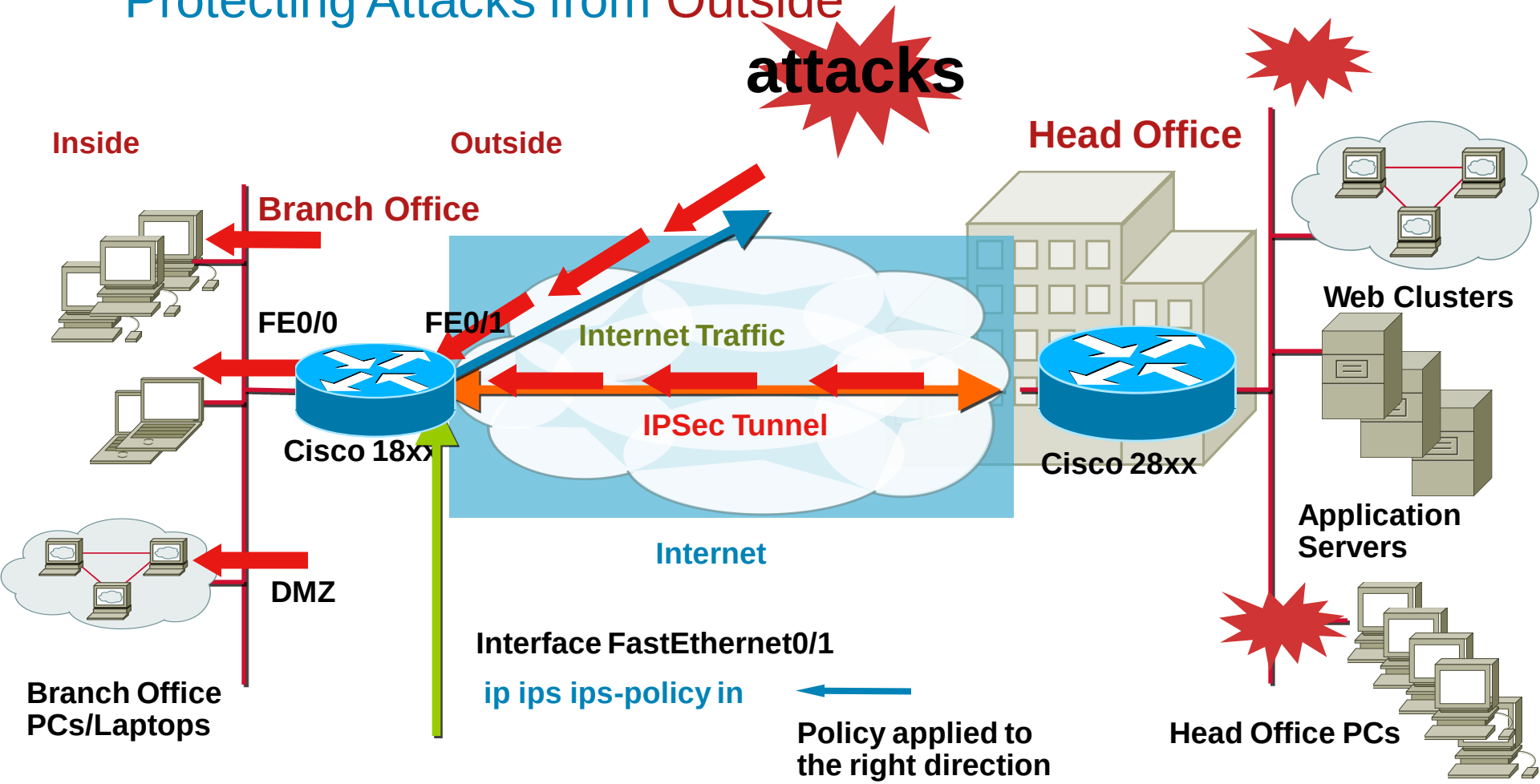
Protecting Attacks from Outside



Dealing with IOS IPS Policy Applied at the Wrong Direction/Interface—Resolution

Case B: Solution

Protecting Attacks from Outside



Dealing with Signature that Do Not Fire with Matching Traffic

1. Are all signatures not firing or only a specific signature not firing?
2. If a specific signature is not firing
   i) Check signature status – enabled/disabled/deleted?
   ii) Is IOS IPS event notification enabled? i.e. syslog/SDEE
3. If all signature are not firing
   i) Check whether signature package is loaded or not
   ii) Verify IOS IPS is applied in the right direction (inbound/outbound) and on the right interface
   iii) Is IOS IPS event notification enabled? i.e. syslog/SDEE
   iv) Do you see alarms/alerts showing signature matching?
   v) Use “show ip ips sessions detail” make sure traffic is going through IOS IPS
   vi) Use “show ip ips signatures statistics | i <sig id>” to see signature hits

Dealing with Packet/Connections dropped due to packets arriving out of order

FW Drops Out-of-Order Packet Slows Down Network Traffic

After turn on IPS, web traffic response time slows down. Go to the router and find out there are syslog messages dropping out of order packets.

```
*Jan  6 19:08:45.507: %FW-6-DROP_PKT: Dropping tcp pkt10.10.10.2:1090 => 199.200.9.1:443
*Jan  6 19:09:47.303: %FW-6-DROP_PKT: Dropping tcp pkt10.10.10.2:1091 => 199.200.9.1:443
*Jan  6 19:13:38.223: %FW-6-DROP_PKT: Dropping tcp pkt66.102.7.99:80 =>
192.168.18.21:1100
```

debug ip inspect detail shows Out-Of-Order packet

```
*Jan  6 19:15:28.931: CBAC* sis 84062FEC L4 inspectresult: SKIP packet 83A6F83C (199.200.9.1:443)
(192.168.18.21:1118) bytes 174 ErrStr = Out-Of-OrderSegment tcp
*Jan  6 19:15:28.931: CBAC* sis 84062FEC pak 83A6FF64SIS_OPEN/ESTAB TCP ACK 842755785 SEQ
2748926608 LEN 0 (10.10.10.2:1118) => (199.200.9.1:443)
*Jan  6 19:15:28.931: CBAC* sis 84062FEC pak 83A6F83CSIS_OPEN/ESTAB TCP ACK 2748926608 SEQ
842755785 LEN 1317 (199.200.9.1:443) <= (192.168.18.21:1118)
*Jan  6 19:15:28.931: CBAC* sis 84062FEC L4 inspectresult: SKIP packet 83A6F83C (199.200.9.1:443)
(192.168.18.21:1118) bytes 1317 ErrStr = RetransmittedSegment tcp
*Jan  6 19:15:28.935: CBAC* sis 84062FEC pak 83A6F83CSIS_OPEN/ESTAB TCP PSH ACK 2748926608
SEQ 842758636 LEN 137 (199.200.9.1:443) <=(192.168.18.21:1118)
*Jan  6 19:15:28.935: CBAC* sis 84062FEC L4 inspectresult: SKIP packet 83A6F83C (199.200.9.1:443)
(192.168.18.21:1118) bytes 137 ErrStr = Out-Of-OrderSegment tcp
```

Dealing with Packet/Connections dropped due to packets arriving out of order – Resolution

FW Drops Out-of-Order Packet Slows Down Network Traffic

- IPS requires packets arrive in order to perform signature scanning, thus drops out-of-order packet; this is one of the reasons for slow response and longer latency in network traffic
- IOS IPS supports Out-of-Order packet starting from 12.4(9)T2 and later 12.4T releases
- Not fixed in 12.4 mainline releases
- Out-of-Order fix also applies to application firewall
- Out-of-order fix DOES NOT work when IOS IPS interface is included in a Zone-Based FW zone
- Out-of-order fix works between IOS IPS and Classic IOS FW (ip inspect)
- If using a release that does not have the fix, workaround is to use ACL to bypass IOS IPS inspection for the traffic flow in question

```
router(config)#access-list 120 deny ip any host 199.200.9.1
router(config)#access-list 120 deny ip host 199.200.9.1 any
router(config)#access-list 120 permit ip any any
router(config)#ip ips name myips list 120
```

- In the example, ACL 120 denies traffic and remove the traffic from IPS scanning; the network traffic between the two site do not experience slow response

IOS IPS Best Practices – Summary

- First time users, follow **Getting Started with Cisco IOS IPS Guide**

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd805c4ea8.html

- **Always remember to RETIRE ALL signatures first**

```
router(config)#ip ips signature-category
router(config-ips-category)#category all
router(config-ips-category-action)#retired true
router(config-ips-category-action)#end
Do you want to accept these changes? [confirm]
```

- **Never unretire the "all" signature category**
- For routers with 128MB memory, start with the IOS IPS Basic category
- For routers with 256MB or more memory, start with the IOS IPS Advanced category

IOS IPS Best Practices – Summary

- Then use CCP/CSM to customize the signature set by unretiring/retiring few signatures at a time according to your network needs
- Pay attention to the free memory every time after you unretiring/retiring signatures
- When router free memory drops below 10% of the total installed memory, then stop unretiring signatures. Adding more memory will not necessarily increase the number of signatures that can be loaded significantly
- You must **unretire** and **enable** a signature to have it loaded and take configured actions when triggered. Enabling it does not load a signature
- If using IOS IPS in a network with a lot of *out-of-order* packets, note:

  You must use 12.4(9)T2 or 12.4(11)T or later T-Train releases. You may not use Mainline image. If Firewall will be also configured, you must configure Classic IOS Firewall. Zone Based Firewall will not work with out-of-order packets

Agenda

- IOS IPS Overview
- Technical Review
  - Architecture
  - Packet Flow
  - Configuration
  - Troubleshooting
- Use Cases
- Management
- Best Practices
- Resources

Contacts

- Product Manager: Kemal Akozer
- Technical Marketing Engineer: Alex Yeung

Documentation for Cisco IOS Security

- Cisco IOS IPS

  http://www.cisco.com/go/iosips

- Cisco IPS Modules for ISRs

  http://www.cisco.com/go/ipsaim

- Cisco Configuration Professional (CCP)

  http://www.cisco.com/go/ccp

- Router Security

  www.cisco.com/go/routersecurity

- Cisco IOS Security Commands Reference

  http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a7f84.html#wp1187286


CISCO