IDS - IPS

- IDS – Intrusion Detection System
- IPS – Intrusion Protection System

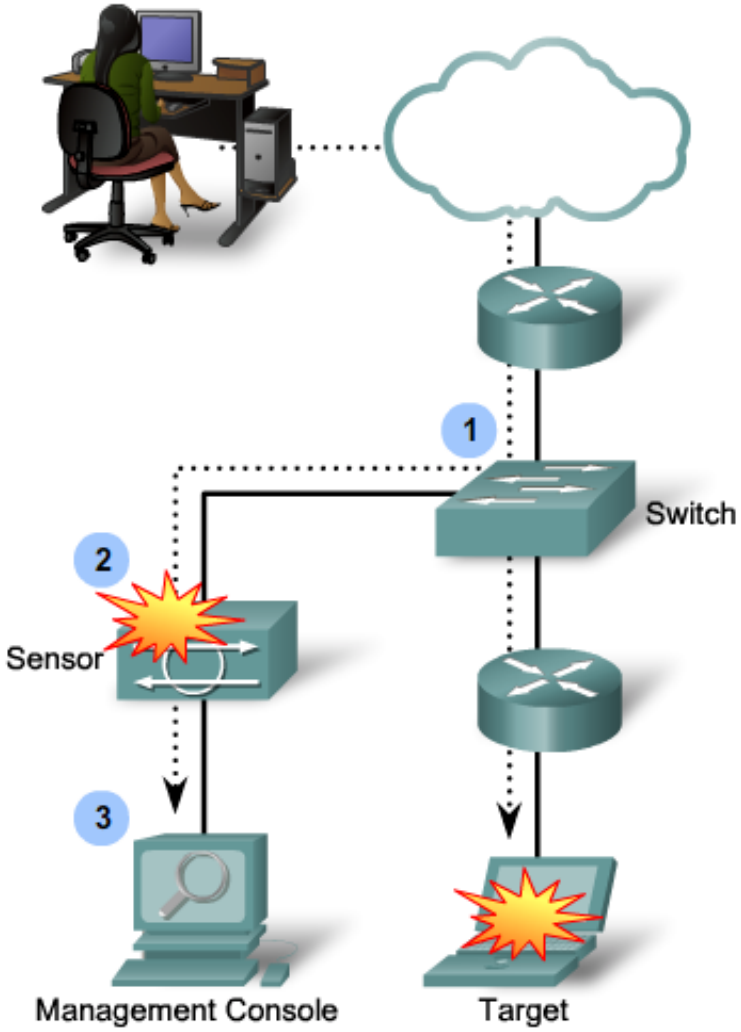
IDS

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 malicious traffic.

3. The IDS sends an alarm to a management console for logging and other management purposes.

IDS



IPS

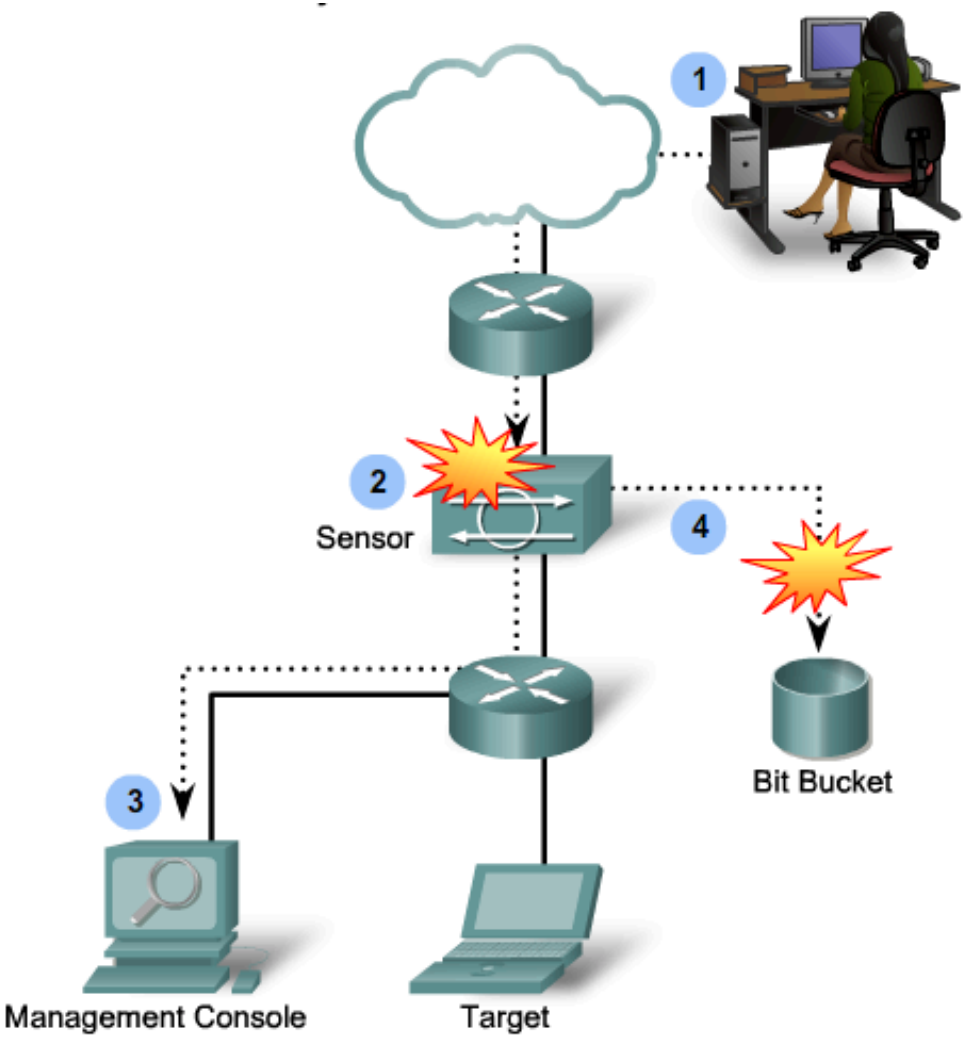
1. An attack is launched on a network that has a sensor deployed in IPS mode (inline mode).

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 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.

IPS



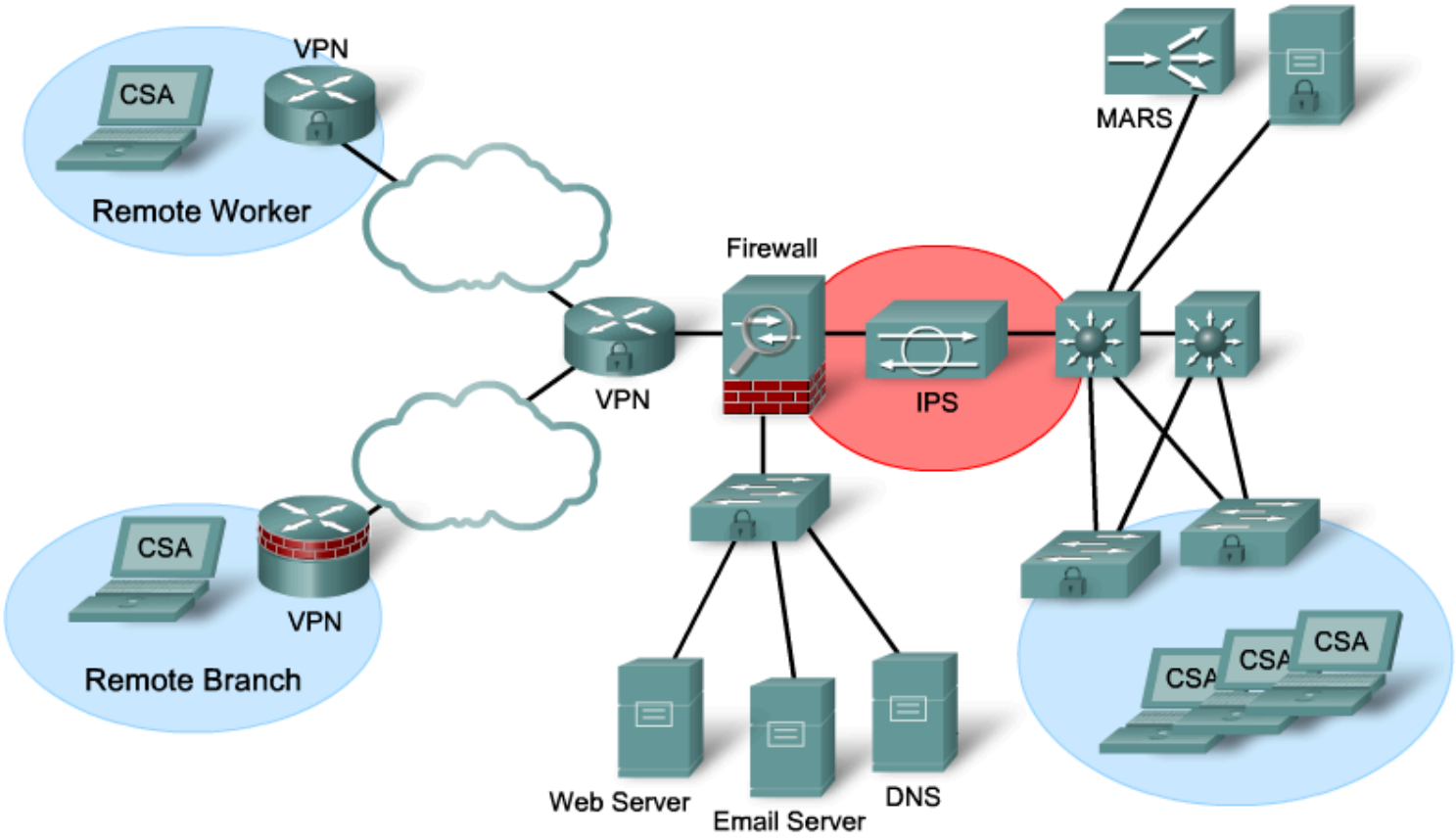
Devices

- Router configured with Cisco IOS IPS software
- Appliance specifically designed to provide dedicated IDS or IPS services
- Network module installed in an ASA (adaptive security appliance), switch or router

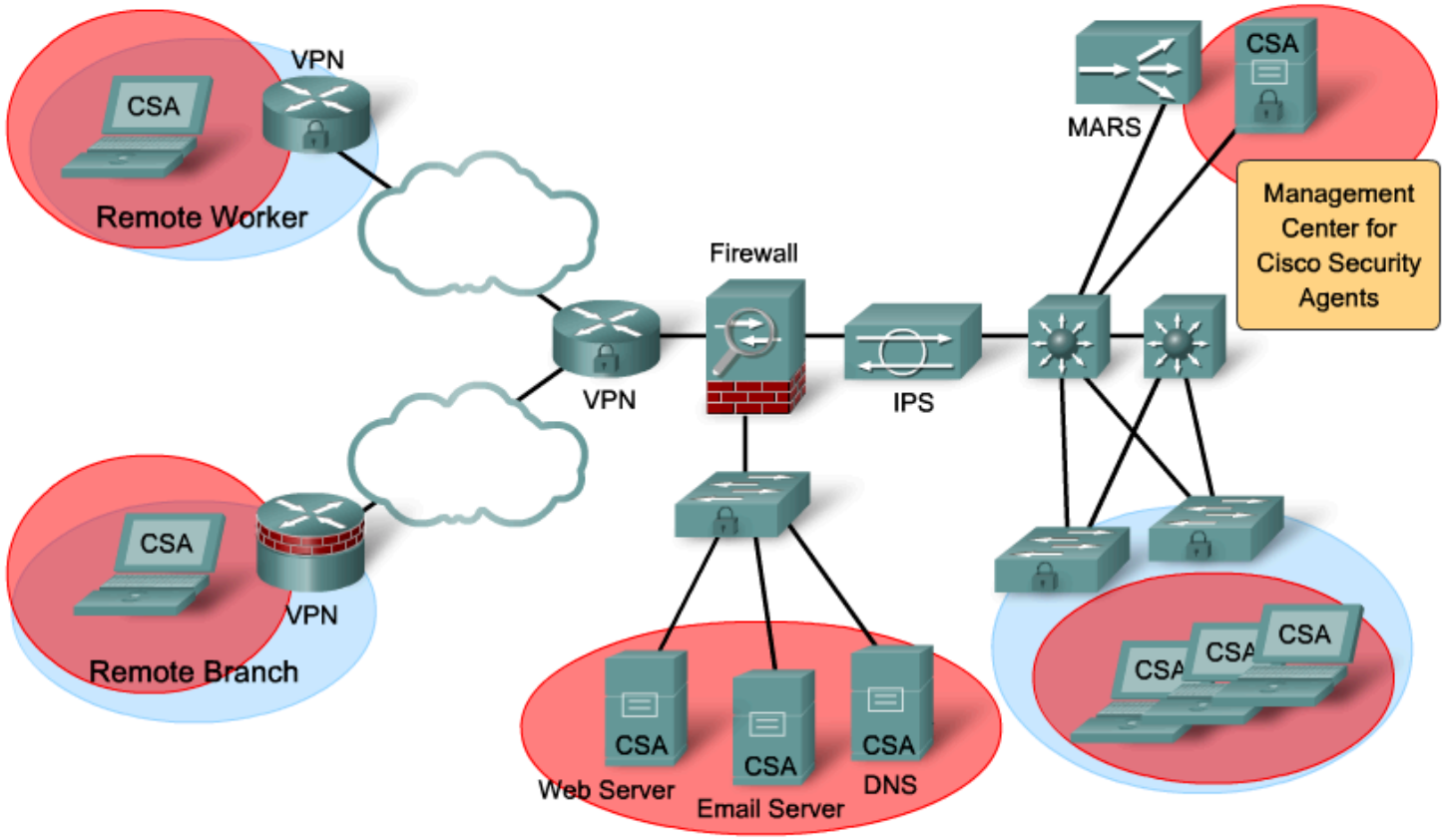
IDS - IPS

- Sensors
- Signatures of misuse
- Atomic(Single packet)-, Composite(Multi packet) Patterns
- IDS and IPS complement each other
  - IDS can validate IPS operation
    - IDS - deeper packet inspection offline
- IPS focus on fewer more critical traffic patterns

Network Based Implementation



Host Based Implementation



Host based

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

HIPS

- Advantages
  - Is host-specofic
  - Protects host after decryption
  - Proides application-level encryption protection
- Disadvantages
  - Operating system dependent
  - Lower level network events not seen
  - Host is visible to attackers

Network IPS

- Advantages
  - Cost-effective
  - Not visible on the network
  - Operating system independent
  - Lower-level network event seen
- Disadvantages
  - Cannot examine encrypted traffic
  - Does not know whether an attack was successful

Signatures

- Malicious traffic displays distinct characteristics or "signatures."
- Uniquely identify specific
  - Worms
  - Viruses
  - protocol anomalies
  - malicious traffic.
  - virus.dat file

Signature Types

- Atomic
  - LAND attack
  - one packet is required to identify this type of attack.
- Composite
  - a stateful signature
  - a sequence of operations distributed across multiple hosts over an arbitrary period of time
  - the event horizon.

Signature Micro-Engines SME

- Atomic - Signatures that examine simple packets, such as ICMP and UDP.
- Service - Signatures that examine the many services that are attacked.
- String - Signatures that use regular expression-based patterns to detect intrusions.
- Multi-string - Supports flexible pattern matching and Trend Labs signatures.
- Other - Internal engine that handles miscellaneous signatures.
- Maximum amount of memory possible.

Triggering mechanisms

- Pattern-Based Detection
- Anomaly-based Detection
- Policy-based Detection
- Honey pot-based Detection

Pattern-Based Detection

- Example
  - Detecting for an address resolution protocol (ARP) request that has a source address of FF:FF:FF:FF:FF:FF
  - Searching for the string ”confidential” across multiple packets in a TCP connection

Anomaly-based Detection

- Profile-based detection,
- What is considered normal for the network or host
- An alert from an anomaly signature does not necessarily indicate an attack. It indicates only a deviation from the defined normal activity
- The network is free of attack traffic during the learning phase. Otherwise, the attack activity will be considered normal traffic

Policy-based Detection

- The administrator defines behaviors that are suspicious based on historical analysis.

Honey pot-based Detection

- Honey pot-based detection uses a dummy server to attract attacks.
- Honey pot systems are rarely used in production environments. Anti-virus and other security vendors tend to use them for research.

Triggering False 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

Signature four levels

- A signature is tuned to one of four levels based on the perceived severity of the signature:
  - High - Attacks used to gain access or cause a DoS attack are detected, and an immediate threat is extremely likely.
  - Medium - Abnormal network activity is detected that could be perceived as malicious, and an immediate threat is likely.
  - Low - Abnormal network activity is detected that could be perceived as malicious, but an immediate threat is not likely.
  - Informational - Activity that triggers the signature is not considered an immediate threat, but the information provided is useful information.

Generating an alert

- Logging the Activity
- Dropping or Preventing the Activity the IPS device actively forwards packets across two of its interfaces
- Blocking Future Activity update the access control lists (ACLs)
- Allowing the Activity

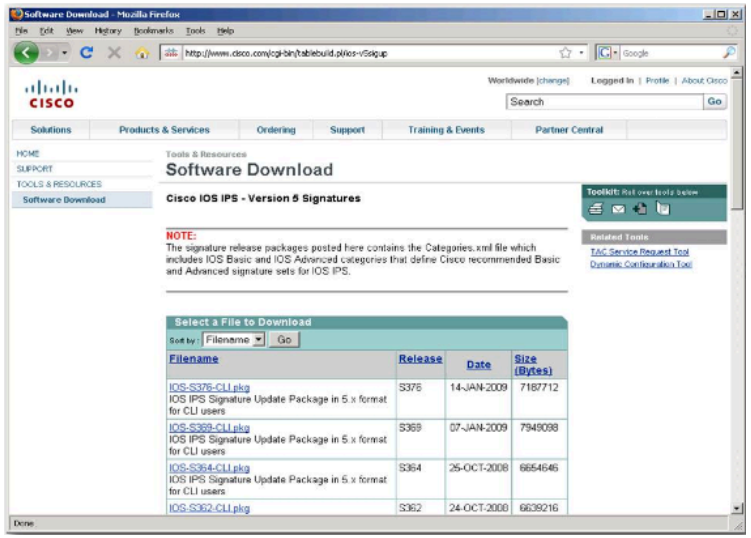
To implement IOS IPS:

- Step 1. Download the IOS IPS files.
- Step 2. Create an IOS IPS configuration directory in flash.
- Step 3. Configure an IOS IPS crypto key.
- Step 4. Enable IOS IPS.
- Step 5. Load the IOS IPS signature package to the router.

Step 1:Download the IOS IPS files.

Cisco.com

- IOS-Sxxx-CLI.pkg
  - This is the latest signature package.
- realm-cisco.pub.key.txt
  - This is the public crypto key used by IOS IPS.



Step2: Create an IOS IPS Configuration Directory in Flash


```
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#
```

Step 3: Configure an IOS IPS Crypto Key

- To configure the IOS IPS crypto key, open the text file, copy the contents of the file, and paste it in the global configuration prompt. The text file issues the various commands to generate the RSA key.

Step 3: Configure an IOS IPS Crypto Key

Cisco.com

realm-cisco.pub signature.txt - Notepad

File Edit Format View Help

```
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
 exit
 exit
```

Step 3: Configure an IOS IPS 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>
```

Step4: Enable IOS IPS #1

- Identify the IPS rule name and specify the location.

```
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 location flash:ips
R1(config)#
```

- IPS rule `iosips` is created.
- IPS location in flash is identified as `flash:ips`.

Step4: Enable IOS IPS #2

- Enable SDEE and logging event notification.

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

SDEE and logging notification are enabled.

- Secure Device Event Exchange (SDEE)

Step4: Enable IOS IPS # 3

- Configure the signature category.

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

- The IPS **all** category is retired.
- The IPS **basic** category is unretired.

Step4: Enable IOS IPS #4

- Apply the IPS rule to a desired interface, and specify the direction.

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

- The IPS rule is applied in a incoming direction.

```
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
```

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

Step5: Load the IOS IPS Signature Package to the Router.

Cisco.com

```
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


*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
```

Copy the signatures from the FTP server.

Monitoring Cisco IOS IPS

Cisco.com

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

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