UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

Chapter 5:
Implementing Intrusion Prevention

CCNA Security v2.0 / Network Security v1.0
Chapter 5 / Modules 11 – 1x

KATEDRA INFORMAČNÝCH SIETÍ * FAKULTA RIADENIA A INFORMATIKY ŽU *

cisco
Networking
Academy

Bezpečnosť informačných sietí – KIS FRI UNIZA
Aktualizované v rámci projektu KEGA 026TUKE-4/2021.

Chapter Outline

- Introduction
- IPS Technologies
- IPS Signatures
- Implement IPS
- Summary

IPS Technologies

Upon completion of this section, you should be able to:

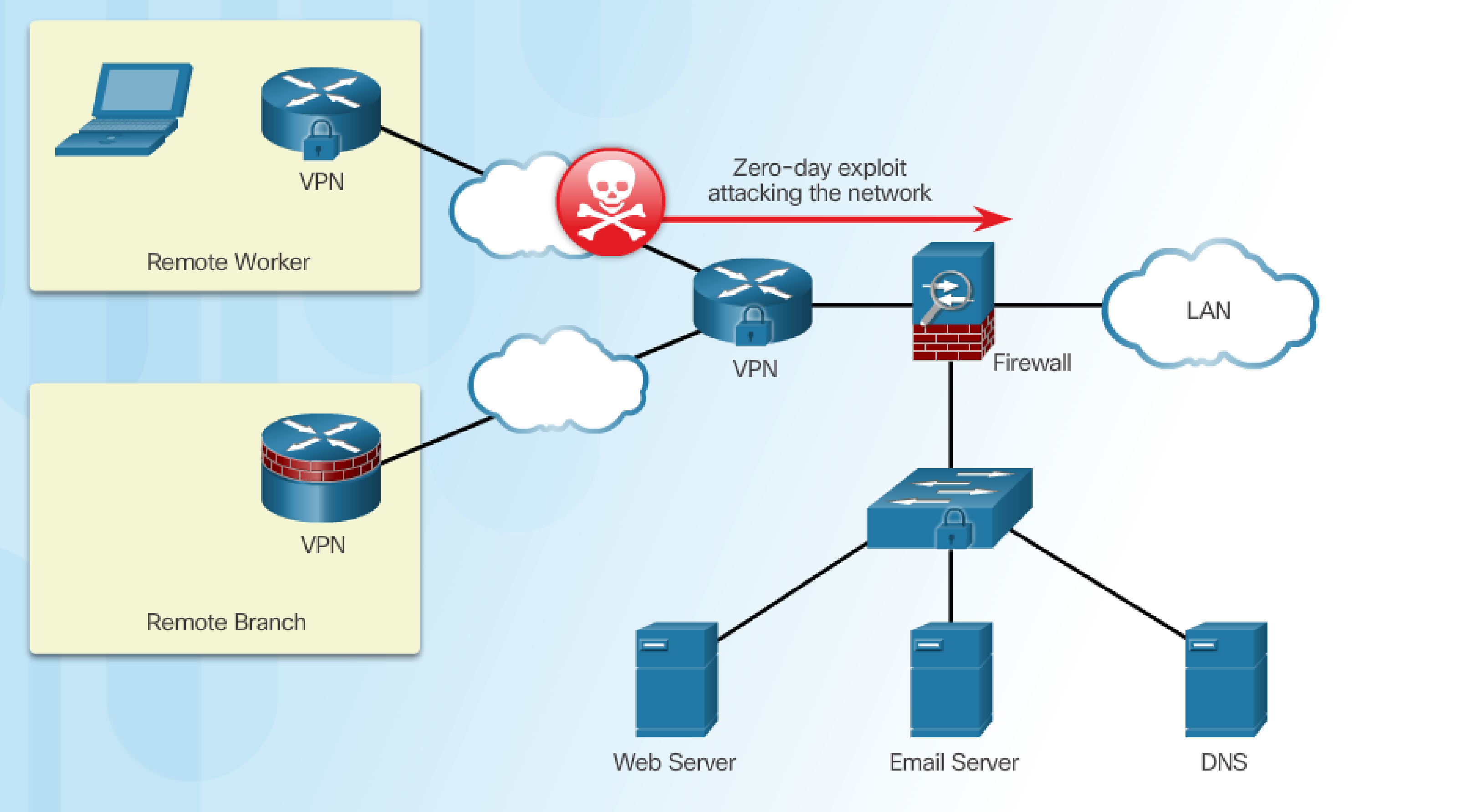
- Explain zero-day attacks.
- Understand how to monitor, detect and stop attacks.
- Describe the advantages and disadvantages of IDS and IPS.

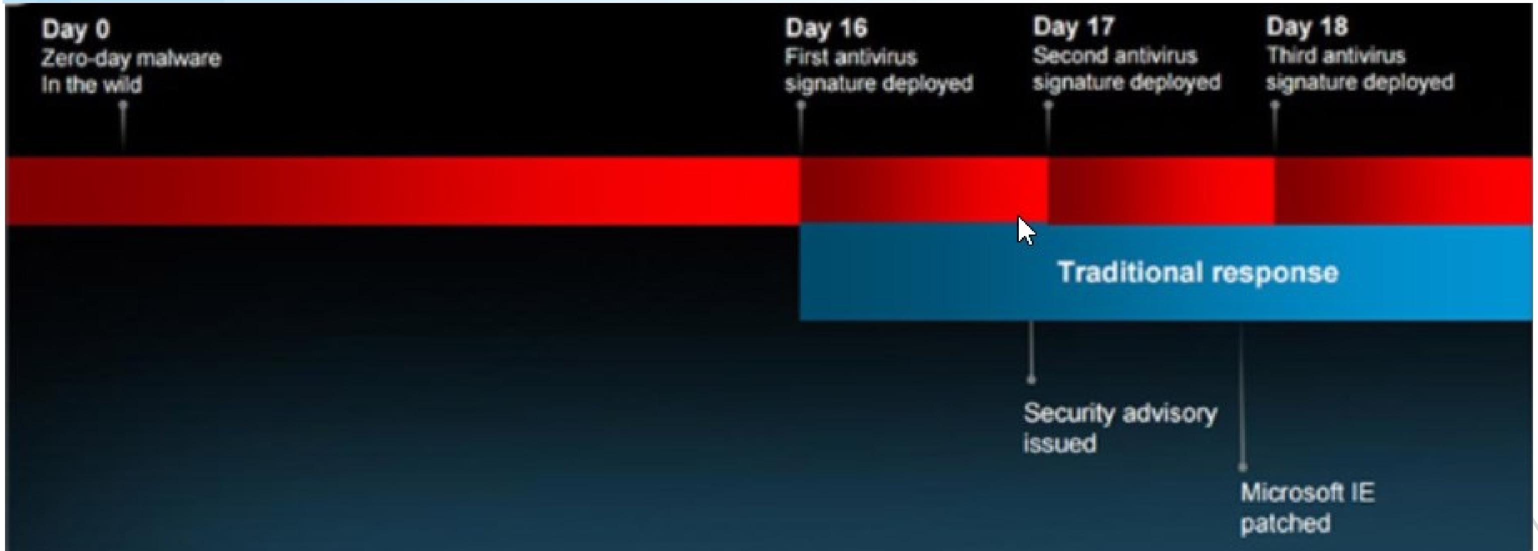
Net security

- Is not the question of a single application
- Requires
  - Device hardening,
  - Authentication, authorization, and accounting (AAA) access control,
  - Firewall features
- Problem, some attack are not still recognized
  - Zero-days attack
  - New malware
  - …

Zero-Day Attacks

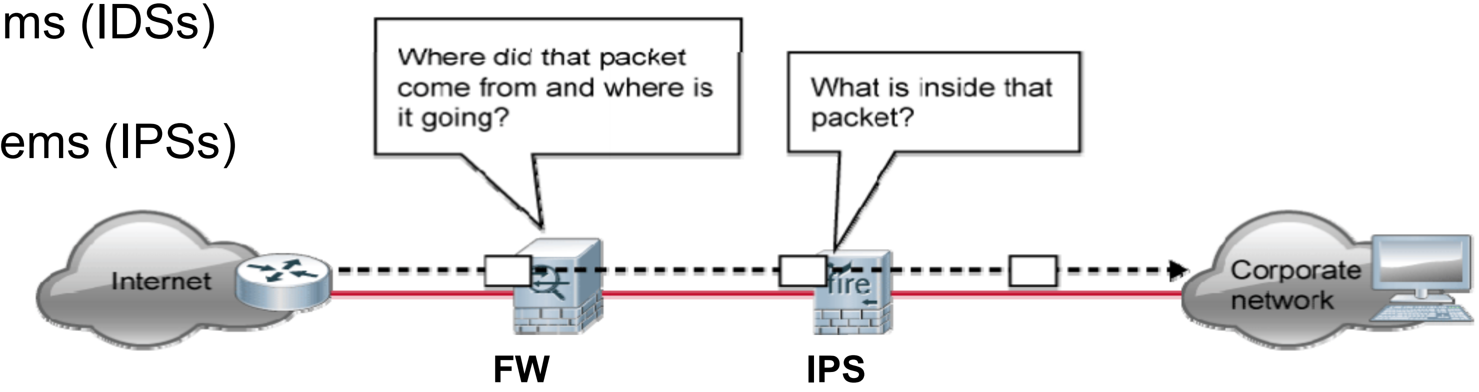
- Or zero-day threats
- An attack never known/seen before
  - Exploits some new software vulnerabilities
  - A zero-hour
    - The moment when the attack was discovered
  - Mitigation:
    - Requires to develop and release a patch by a sw vendor
    - Better view of a net infrastructure
    - Add new approaches





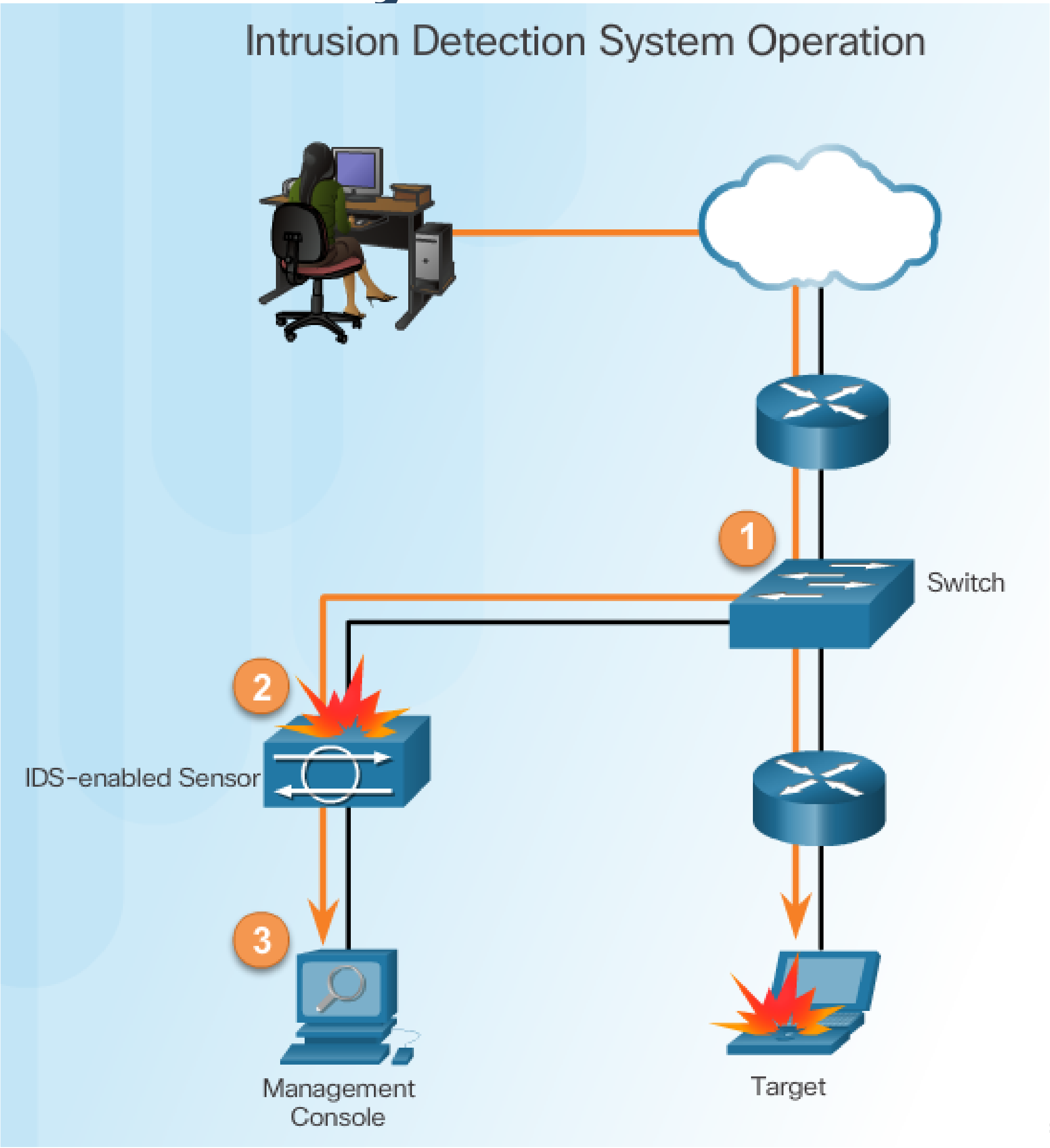
Detecting for Attacks

- + additional recognition is required throughout the entire network, every in/out port
- Several approaches
  - **Monitor and log analysis**
    - Time consuming, not very scalable
    - ***Note***: *SIEM may help*
  - **Intrusion systems (used for traffic monitoring)**
    - A system that detect activity that can compromise the confidentiality, integrity, and availability of information resources, processing, or systems
    - Two types
      - IDS – Intrusion Detection Systems (IDSs)
        - The first developed technology
      - IPS – Intrusion Prevention Systems (IPSs)
        - An IDS evolution


Where did that packet come from and where is it going?
What is inside that packet?
Internet
fire
Corporate network
FW
IPS

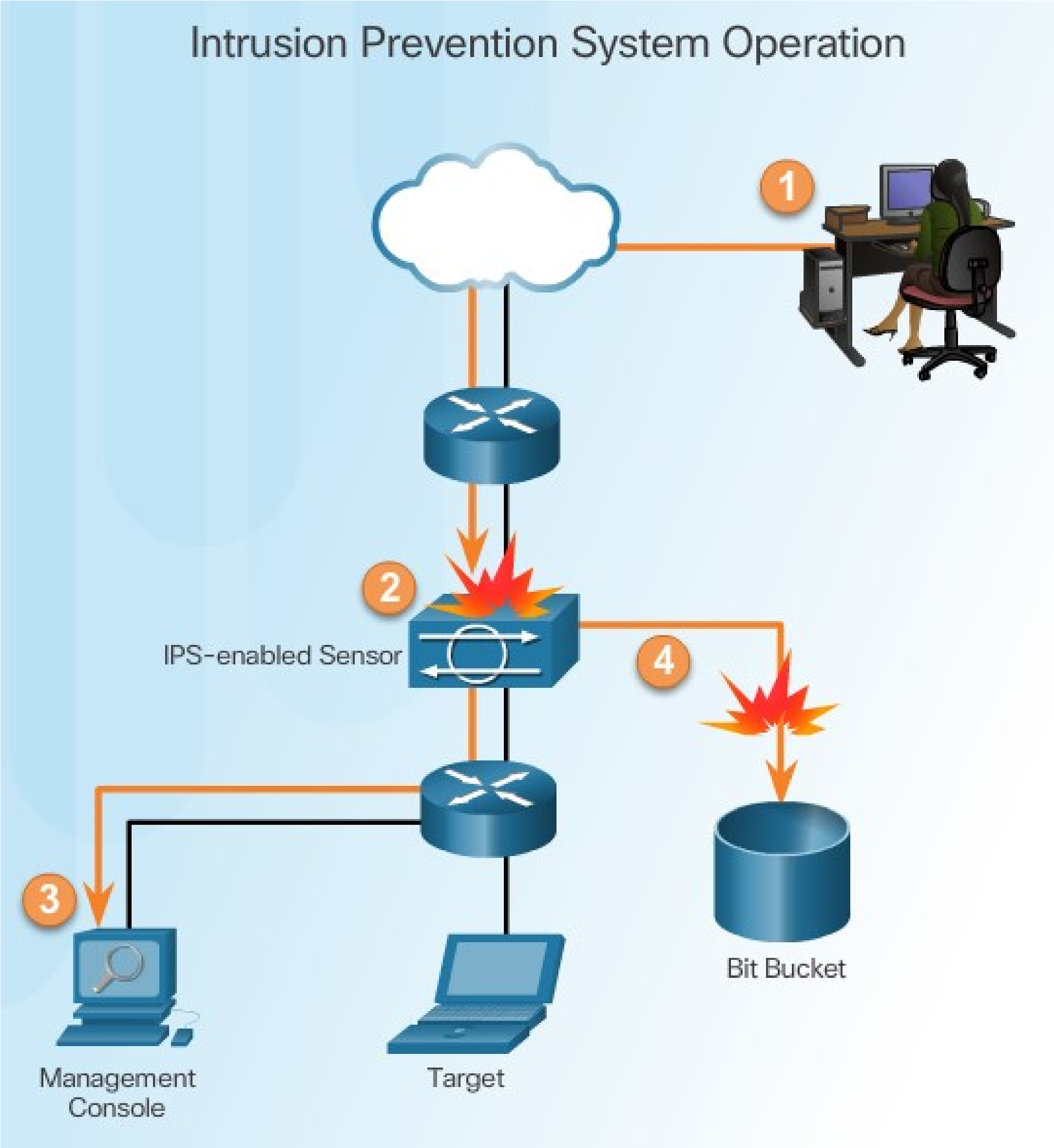
Detect Attacks - Intrusion Detection Systems

- Features of an IDS:
  - Primarily focused on identifying possible incidents, logging information about the incidents, and reporting the incidents
  - Works passively
    - Always deployed as passive sensor (offline)
    - Network traffic does not pass through
  - Requires copy of traffic packets
    - Port mirror
  - Do not perform an action on packets
    - **Cannot stop the attack**
    - However, may instruct router/fw
      - i.e. to apply policy



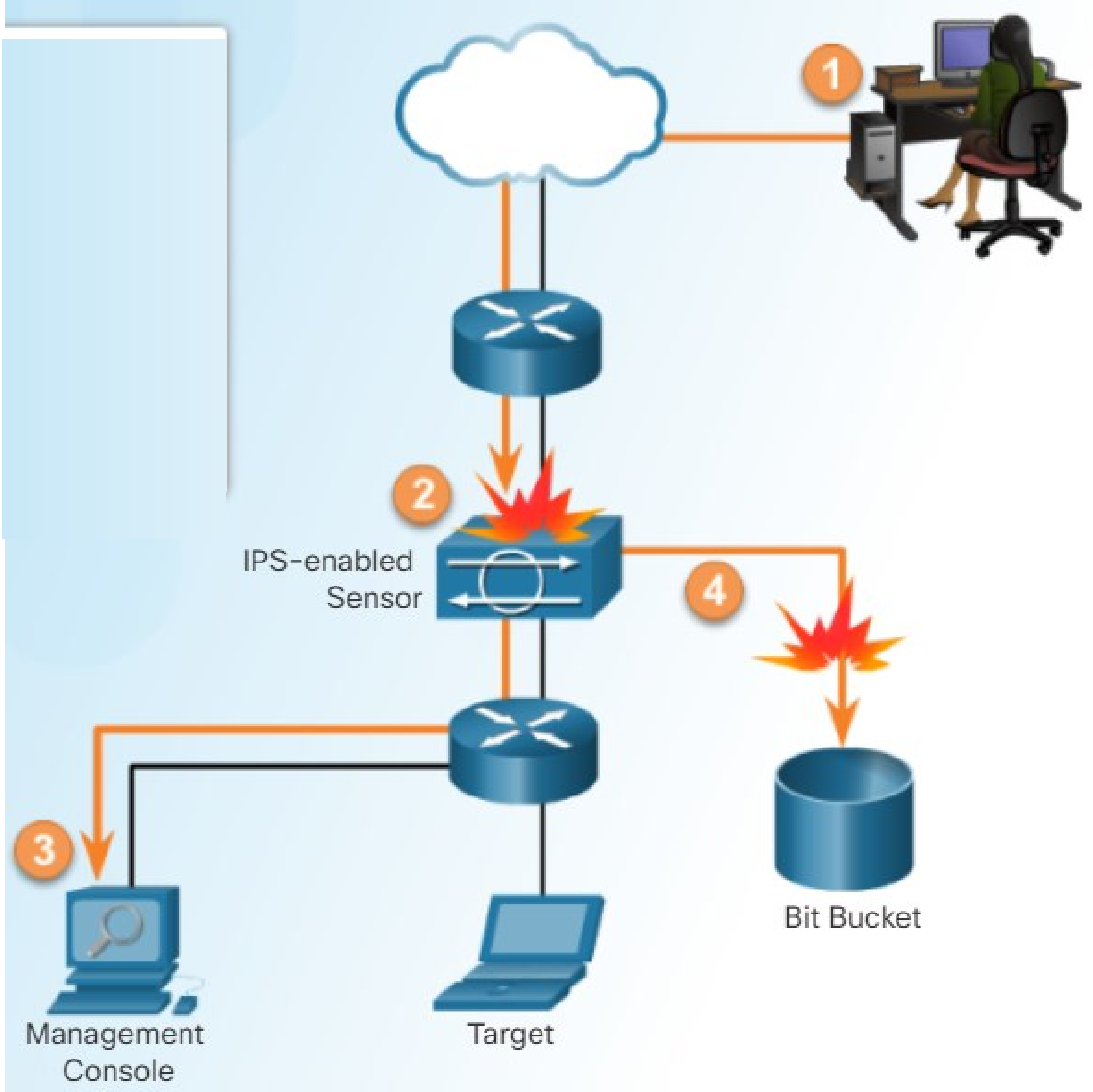
Detect and Stop Attacks - Intrusion Prevention System

- IPS – Intrusion Prevention System:
  - Better solution as IDS
    - Build upon IDS
  - Is able to
    - Analyze traffic from Layer 2 up to Layer 7 traffic
      - Deeper packet and application inspection
    - Detect
    - And Immediately **Stop/block** attacks from reaching a target
      - Including single packet
      - Or packet flow
  - Implemented in an **inline** mode
  - Detection techniques
    - Signature-based, profile-based (anomaly), and protocol analysis-based intrusion detection
    - Responds immediately, not allowing any malicious traffic to pass
  - Problems
    - With poorly configured or un-proportionally dimensioned



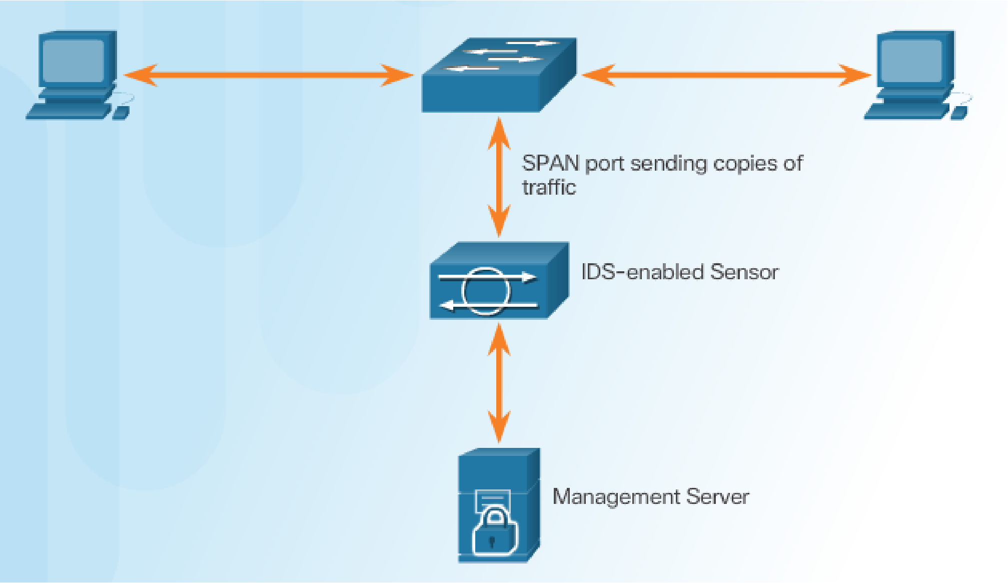
Similarities Between IDS and IPS

- Similarities
  - Both use signatures to detect patterns of misuse inside of the net traffic
  - Are deployed as **sensors**
  - Both can detect malformed packet (atomic patterns) or packet flow (composite patterns)
- Cisco deployment
  - Router with required sw feature
  - Standalone dedicated appliance
  - Network module
    - Installed in ASA FW, switch or router

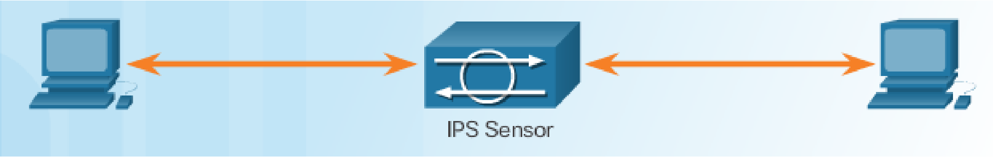


Modes of Deployment

Promiscuous (passive) Mode (requires SPAN, TAP)



Inline (inline interface pair) Mode



Note: Using one of these technologies does not negate the use of the other

Advantages and Disadvantages of IDS and IPS

Advantages IDS:

- No impact on network performance and latency (no inline)
- No network impact if there is a sensor **failure**
- No network impact if there is a sensor **overload**

Disadvantages IDS:

- Response action cannot stop trigger packet
- Response requires assistance from other devices (FW, router)
- Correct tuning required for response actions
- More vulnerable to network security evasion techniques

Advantages IPS:

- Stops trigger packets (inline)
- Reacts immediatelly
- Can use stream normalization techniques

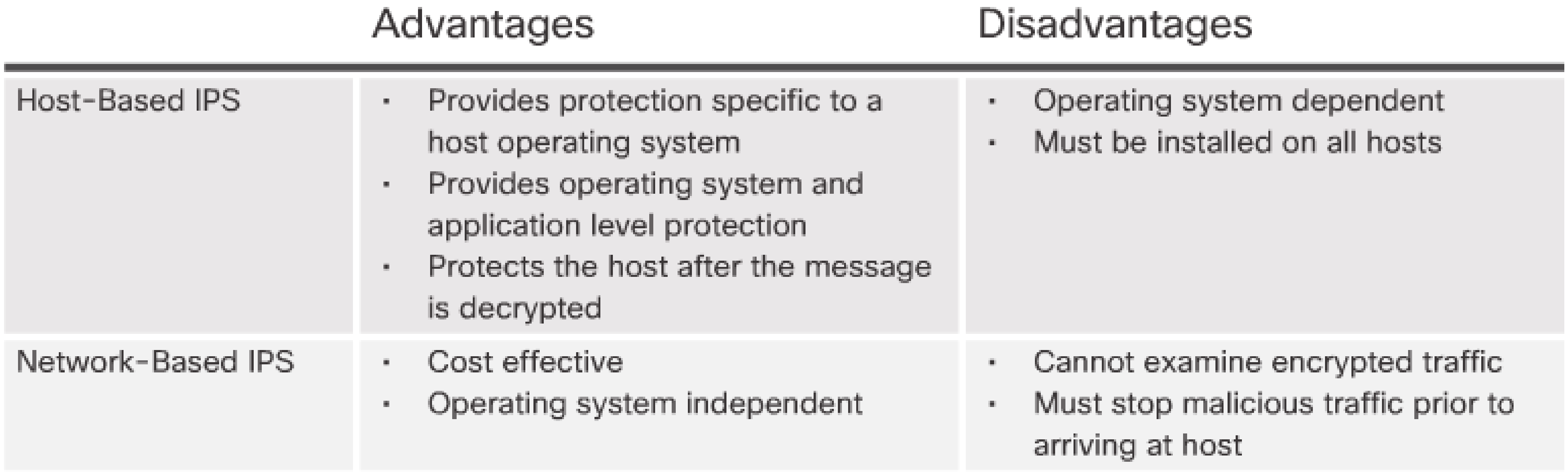
Disadvantages IPS:

- Sensor issues might affect network traffic
- Sensor overloading impacts the network
- Some impact on network

IPS types:
Host-Based and Network-Based IPS Implementations

Host-Based and Network-Based IPS

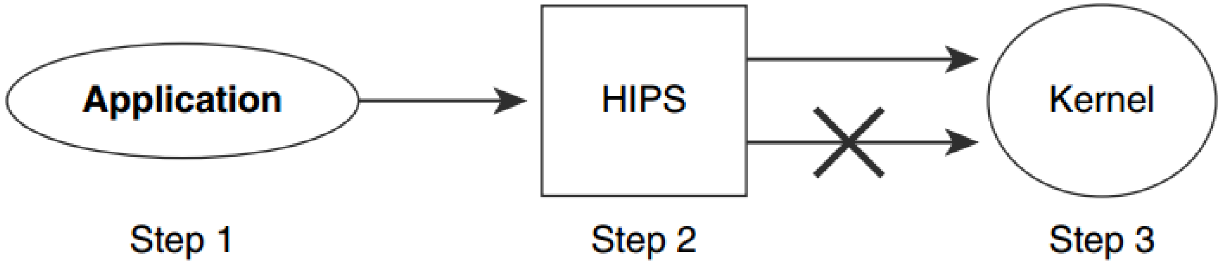
- Two IPS types
  - Host-based IPS
    - Installed on hosts (as an agent)
    - Should be able to cooperate with network based IPS
  - Network-based IPS
    - Network hw/sw appliance



	Advantages	Disadvantages
Host-Based IPS	• Provides protection specific to a host operating system • Provides operating system and application level protection • Protects the host after the message is decrypted	• Operating system dependent • Must be installed on all hosts
Network-Based IPS	• Cost effective • Operating system independent	• Cannot examine encrypted traffic • Must stop malicious traffic prior to arriving at host

Host-Based IPS (HIPS)

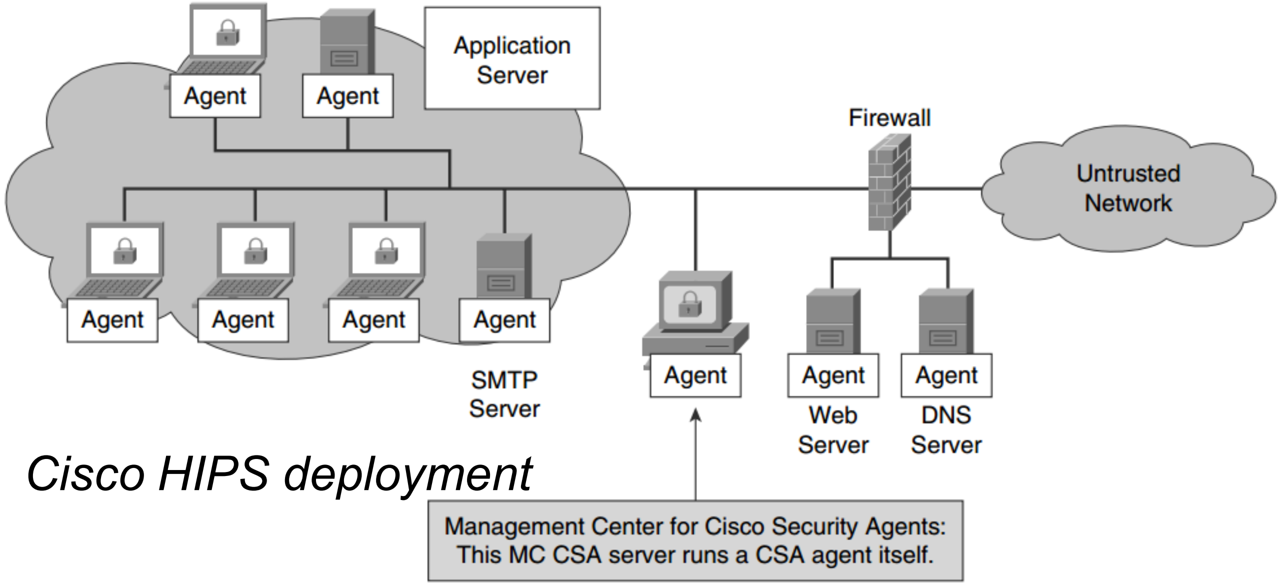
- Host-based IPS
  - Installed on hosts (crucial end-points) as an agent
    - Should cooperate with network based
    - Would report detection to local event log or central management console
  - Intercept app call to OS kernel
  - Monitor abnormal activity and/or network flow, prevent executing some commands or applications start within OS



- Activities include
  - Unauthorized registry updates
  - Changes to the system directory
  - Executing installation programs
  - and activities that cause buffer overflows
- Compare activities
  - To know attack characteristics
  - Specified by rules, policy or signatures
  - Out-of-bound activities are blocked

Host-Based IPS (HIPS)

- Can be a combination of antivirus software, antimalware software, and firewall
  - IBM ISS, TripWire, Verisys
  - Open Source: OSSEC, Wazuh

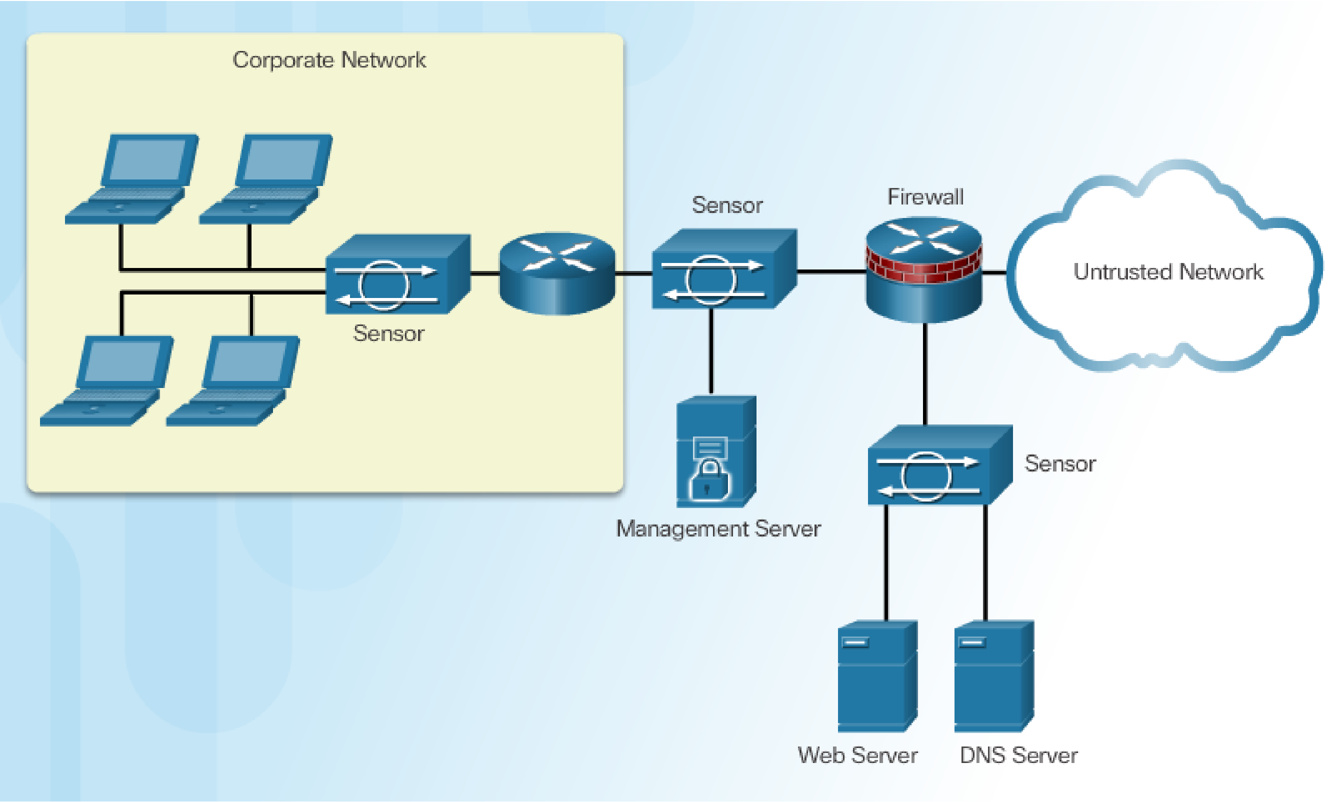


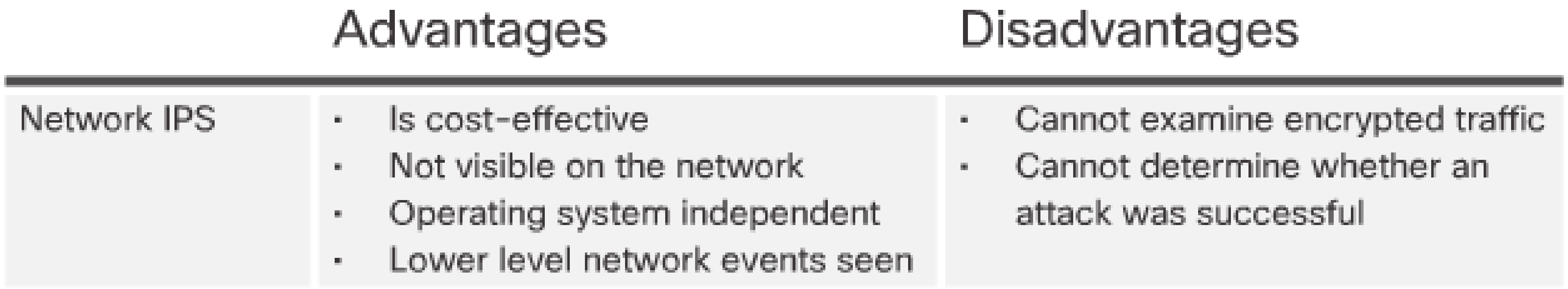
Cisco HIPS deployment

- Advantage:
  - Detection of activity that does not generate network traffic
  - Monitor OS networking stack behavior
  - Improve
- Disadvantage:
  - Operates locally on a single host
  - Requires agents on every single host
  - Operation processing load
  - Agent must be available for multiple OSs

Network-Based IPS (Sensors)

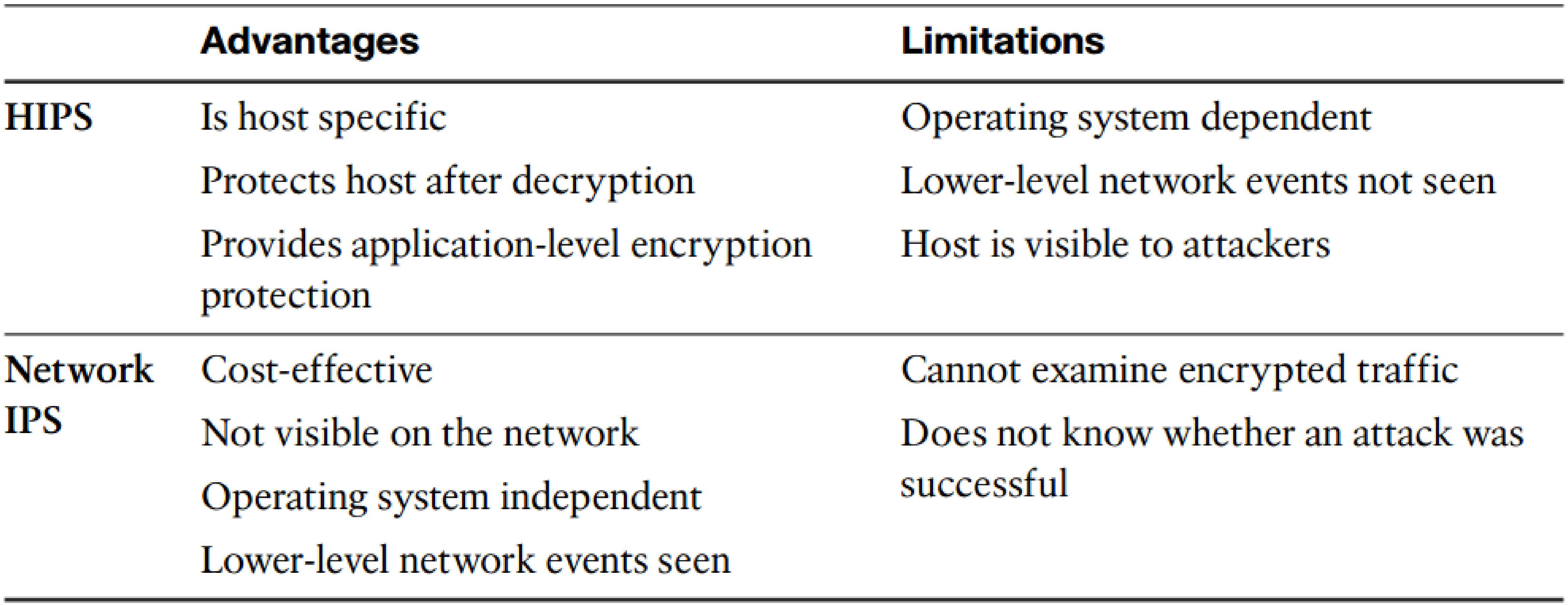
- Multi sensor deployment model
- Capture and analyze network traffic
- Works in real-time
- Protects network even end-points
- Have to be tunned for IPS analysis
- Device have to be hardenned
  - Optimized for perfomance and security
- Deployed as
  - Dedicated IPS hw appliance (similar to a server)
  - Non-dedicated hw





	Advantages	Disadvantages
Network IPS	· Is cost-effective · Not visible on the network · Operating system independent · Lower level network events seen	· Cannot examine encrypted traffic · Cannot determine whether an attack was successful

Comparison of HIPS and Network IPS



	Advantages	Limitations
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	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

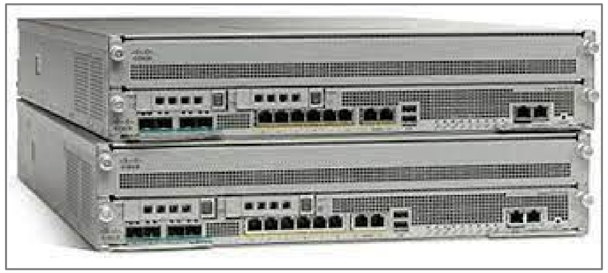
Non dedicated hw

Cisco's Modular and Appliance-Based IPS Solutions

- Cisco IPS AIM and Network Module Enhanced (IPS NME)
  - ISR G2 routers: 19xx, 2900, 3900

- Cisco ASA AIP-SSM (Advanced Inspection and Prevention Security Services Module)
  - ASA 5500 models: 5505, 5510, 5520
  - ASA-X models: next gen firewalls
    - May run FirePower services aka sourcefire threat detection

- Cisco Catalyst 6500 Series IDSM-2 (Intrusion Detection System Services Module)



- Cisco IPS 4300 Series Sensors (dedicated appliance)

Choose an IPS Solution

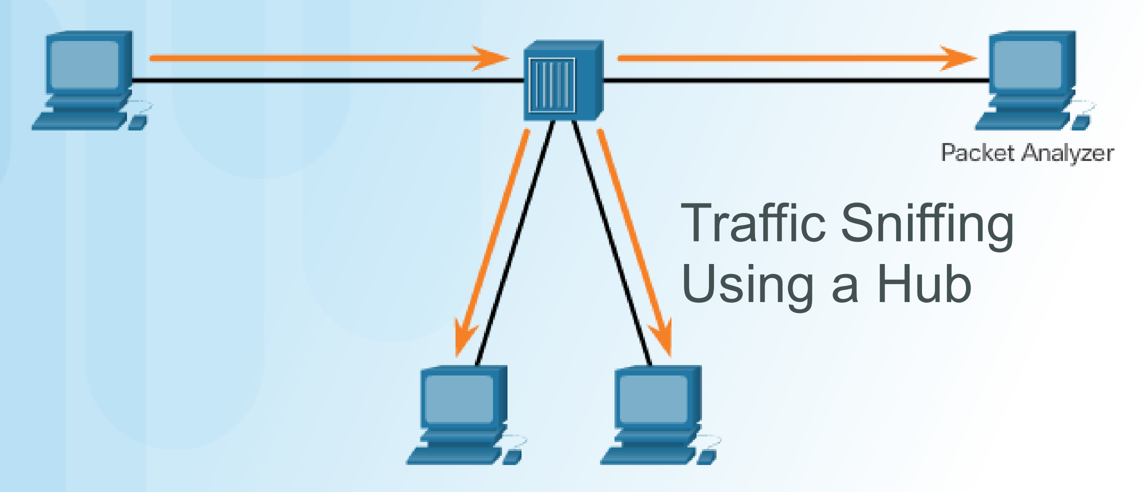
- Factors affecting the IPS sensor selection and deployment:
  - Amount of network traffic
  - Network topology
  - Security budget
  - Available security staff to manage IPS
- For example
  - SOHO => Cisco IOS with IPS enabled ISR
  - Large installation => 5500-X
  - Enterprise/SP => IPS and Catalyst 6500 IDSM

Specialized Security Appliances

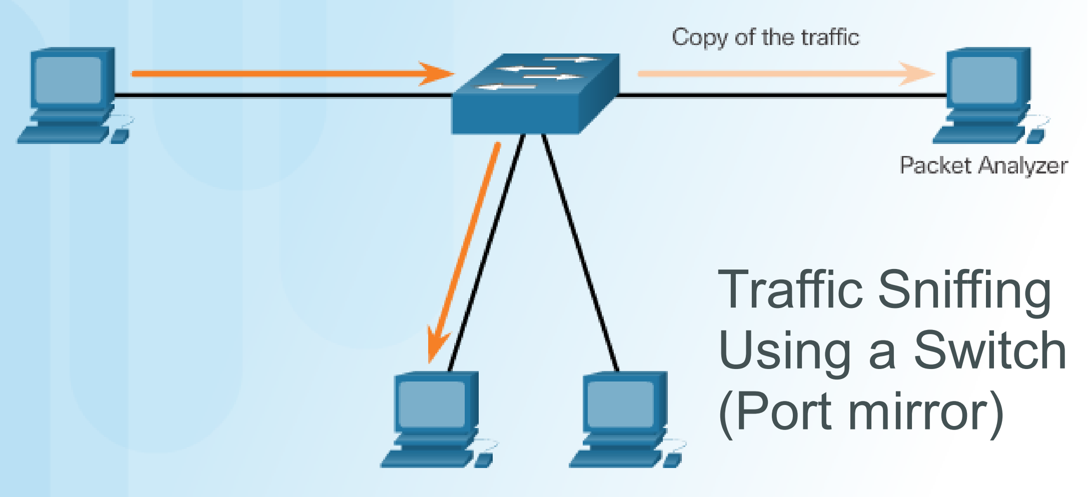
- Cisco has a variety of other specialized security appliances
  - Cisco Advanced Malware Protection (AMP)
    - Uses Cisco Talos security intelligence
  - Cisco Advanced Web Security Appliance (WSA)
  - Cisco Advanced Email Security Appliance (ESA)

Promiscuous deployment - connecting IDS/IPS

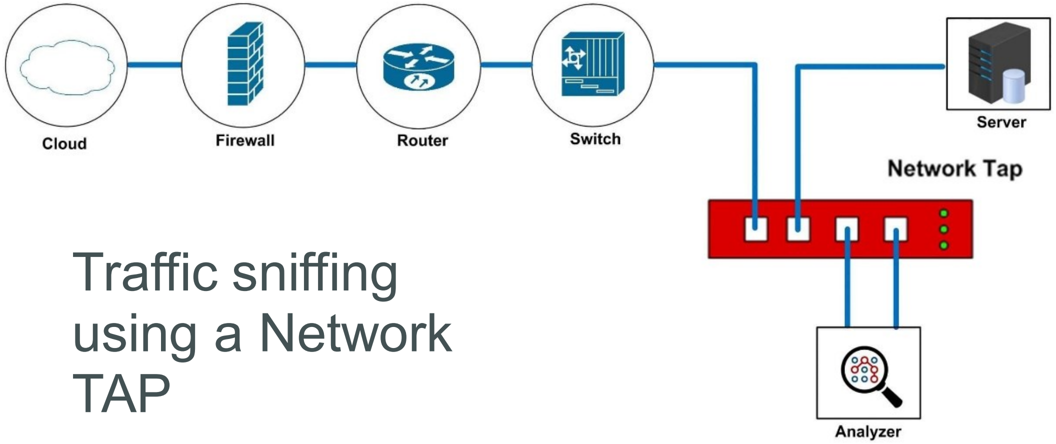
Traffic sniffing techniques



Traffic Sniffing Using a Hub

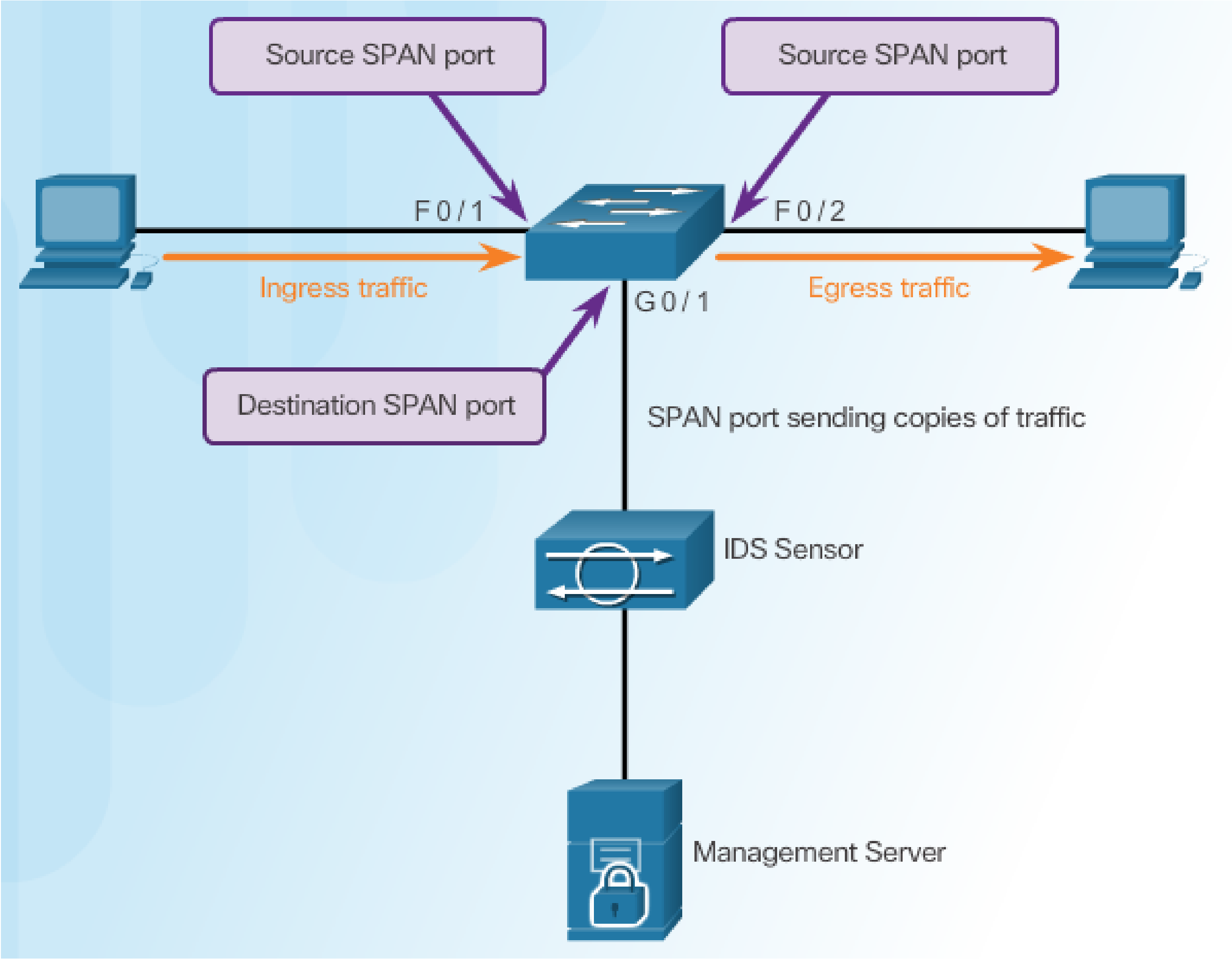


Traffic Sniffing Using a Switch (Port mirror)



Traffic sniffing using a Network TAP

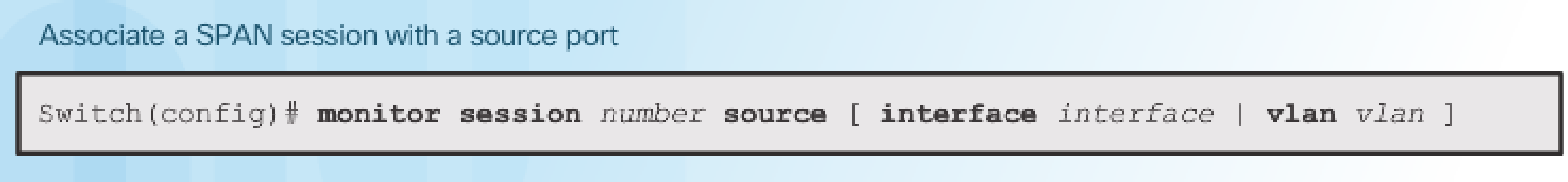
Cisco SPAN


Source SPAN port
Source SPAN port
F0/1
F0/2
Ingress traffic
Egress traffic
G0/1
Destination SPAN port
SPAN port sending copies of traffic
IDS Sensor
Management Server

Configuring Cisco SPAN

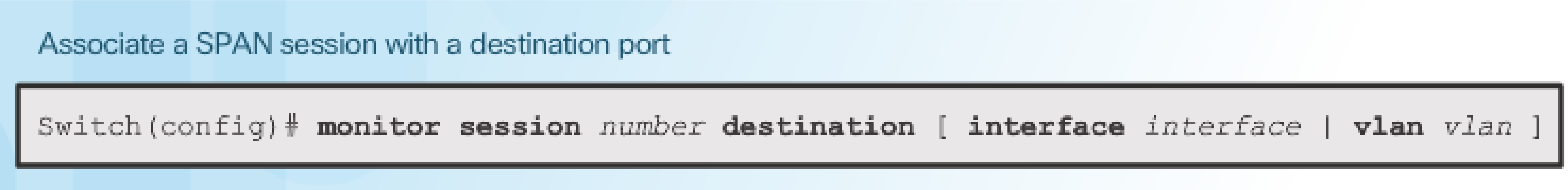
Cisco SPAN Commands:

- Monitor session command – used to associate a source port and a destination port with a SPAN session.



Associate a SPAN session with a source port

```
Switch(config)# monitor session number source [ interface interface | vlan vlan ]
```



Associate a SPAN session with a destination port

```
Switch(config)# monitor session number destination [ interface interface | vlan vlan ]
```

- Show monitor command – used to verify the SPAN session.

Example

Configuring a local SPAN

- SPAN je relácia, v ktorej sa prevádzka z lokálnych portov alebo VLAN odosiela na zvolený lokálny port

```
Switch(config)# monitor session 1 source interface Gi0/1
Switch(config)# monitor session 1 destination interface Gi0/3
```

- Cieľový port nie je viac použiteľný pre bežnú komunikáciu (vstupujúce rámce zahadzuje)
  - Je možné dovoliť spracovať aj bežné vstupujúce rámce príkazom

```
Switch(config)# monitor session 1 dest int Gi0/3 ingress vlan 1
```

- Aby bolo možné vidieť aj Layer2 obslužné protokoly (CDP, DTP, VTP, STP, PAgP, LACP, ...) a aby rámce odchádzali s pôvodným VLAN tagom, je potrebné výstupný port nakonfigurovať príkazom

```
Switch(config)# monitor session 1 dest int Gi0/3 encap replicate
```

  - Bez tohto príkazu zachytené rámce budú všetky „untagged“ a servisné protokoly nebudú odchytávané

Verifying a local SPAN

```
switch(config)# end
siwtch# show monitor session 1
Session 1
-----
Type                   : Local Session
Source Ports           :
Both                   : Gi0/1
Destination Ports      : Gi0/3
Encapsulation          : Native
Ingress                : Disable
```

Monitor filter

- If we want to filter traffic over a specific source port (for example a trunk) for a specific vlan (otherwise all VLANs are monitored)

```
Switch(config)# monitor session 1 filter vlan V_ID
```

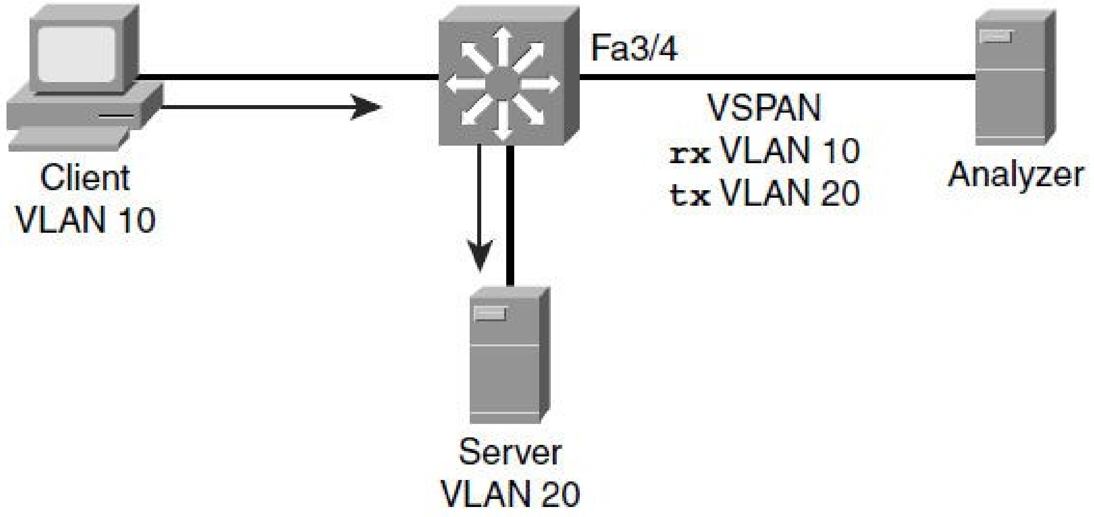
- Example

```
! Monitoruj na trunk porte len vlan 10,20,30,55-60
Switch(config)# int fa0/1
Switch(config)# sw mode trunk
Switch(config)# monitor session 1 source interface Fa0/1
Switch(config)# monitor session 1 filter vlan 10,20,30,55-60
Switch(config)# monitor session 1 destination interface Gi0/1
```

Local SPAN rules

- As source and destination ports we may use switched and even routed ports
- The port can be used as a destination but only for one SPAN session
- A port cannot be used as a destination if it is configured as a source
- The port channel interface (EtherChannel) can be a source but not a destination port for SPAN
- Source ports may belong to different VLANs
- The destination port must not participate in the STP
  - Do not connect to another switch to avoid the loop!

VLAN SPAN



- Suitable if we want to monitor the flow between specific VLANs
- Example
  - The Flow diagnostic flowing between a server in VLAN 20 and a client placed in VLAN 10

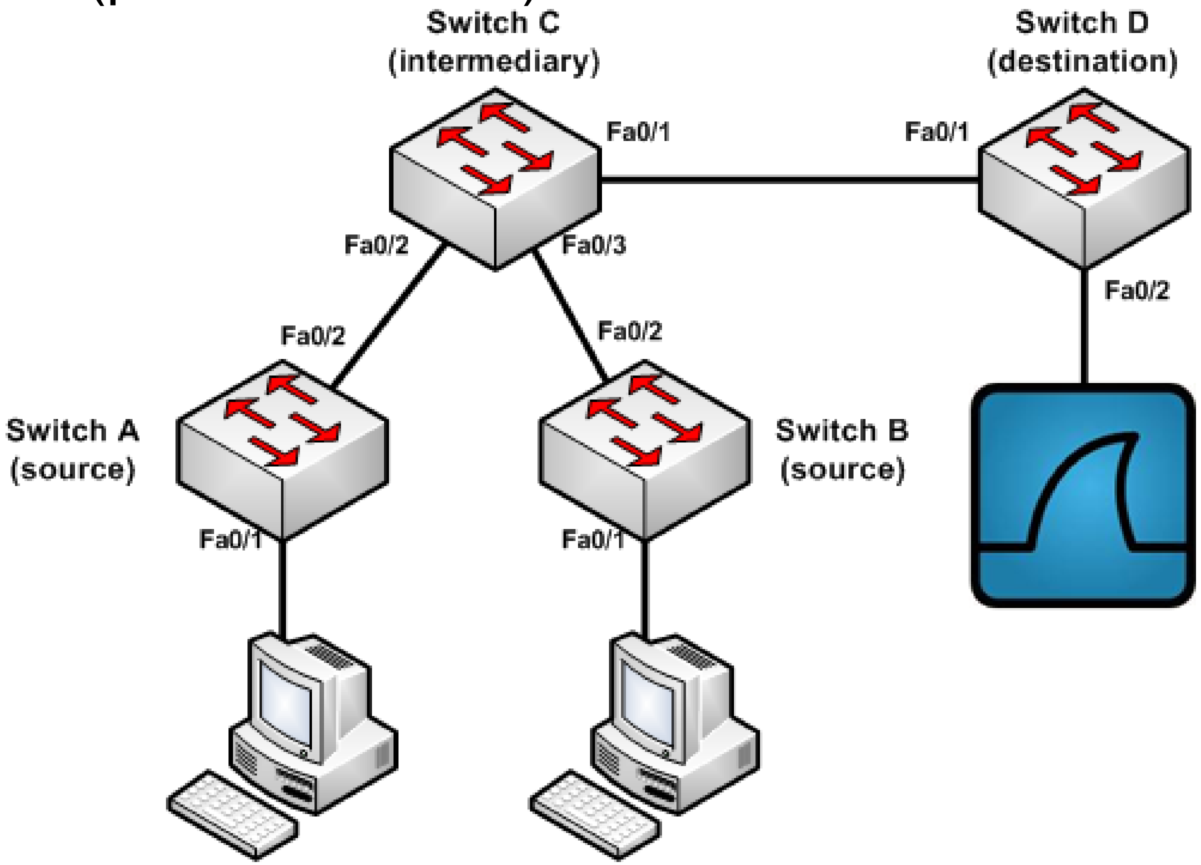
```
Switch(config)# monitor session 1 source vlan 10 rx
Switch(config)# monitor session 1 source vlan 20 tx
Switch(config)# monitor session 1 destination interface FastEthernet
  3 /4
Switch # show monitor session 1
Session 1
-----
Type                    : Local Session
Source VLANs  :
       RX Only          : 10
       TX Only          : 20
       Destination Ports : Fa3/4
       Encapsulation : Native
       Ingress          : Disabled
```

VSPAN rules

- VSPAN sessions, with both ingress and egress options configured, forward duplicate packets from the source port only if the packets get switched in the same VLAN.
- One copy of the packet is from the ingress traffic on the ingress port, and the other copy of the packet is from the egress traffic on the egress port.
- VSPAN monitors only traffic that leaves or enters Layer 2 ports in the VLAN:
  - Routed traffic that enters a monitored VLAN is not captured if the SPAN session is configured with that VLAN as an ingress source because traffic never appears as ingress traffic entering a Layer 2 port in the VLAN.
  - Traffic that is routed out of a monitored VLAN, which is configured as an egress source in a SPAN session, is not captured because the traffic never appears as egress traffic leaving a Layer 2 port in that VLAN.

Remote traffic monitoring with RSPAN

- Remote SPAN (RSPAN)
  - Is very similar to a local SPAN
  - But support a situation where a source (port even VLAN) and a destination can be on different switches



Configuring RSPAN

- RSPAN je dvojica relácií
  - Na zdrojovom switchi sa zachytáva prevádzka na lokálnych portoch alebo VLAN a odosiela sa do špeciálnej RSPAN VLAN
  - Na cieľovom switchi sa zachytená prevádzka z RSPAN VLAN odosiela na zvolený lokálny port
  - RSPAN VLAN je vyhradená len na účely RSPAN

```
Source(config)# vlan 999
Source(config-vlan)# remote-span
Source(config-vlan)# exit
Source(config)# monitor session 1 source interface Fa0/1
Source(config)# monitor session 1 source vlan 123
Source(config)# monitor session 1 destination remote vlan 999
```

```
Dest(config)# vlan 999
Dest(config-vlan)# remote-span
Dest(config-vlan)# exit
Dest(config)# monitor session 1 source remote vlan 999
Dest(config)# monitor session 1 destination interface Gi0/1
```

Types of IDS/IPS sensors (Signature)

Upon completion of the section, you should be able to:

- Understand IPS signature characteristics
- Explain IPS signature alarms
- Manage and monitor IPS
- Understand the global correlation of Cisco IPS devices

Signature Attributes

- Attack signatures = attack characteristics and activities
- A signature is a set of rules that IDS/IPS uses to detect a typical intrusion activity
  - Uniquely identify specific worms, viruses, protocol anomalies, or malicious traffic
  - Sensor scan packets and compare them to specific signature characteristics
- Typical detection method
  - Even other are supported
- Signatures have three distinct attributes (Cisco IOS):
  - Type (search for in (detect) …)
  - Trigger (alarm) (warn …)
  - Action (do something …)

Signature Types - Atomic

- Consists of a single packet, activity, or event that is examined to determine if it matches a configured signature
- Simplest signature type
  - The entire inspection can be accomplished in an atomic operation
  - Does not support state (for example TCP TWH)
  - Does not require any knowledge of past or future activities
  - Signatures are easy to identify and understand
    - for example, packet has the same source and destination IP address
    - one packet identifies an attack
- Consumes minimal system resources
  - traffic analysis is usually performed very quickly and efficiently
- If there is a signature match
  - An alarm is triggered
  - and a signature action is performed

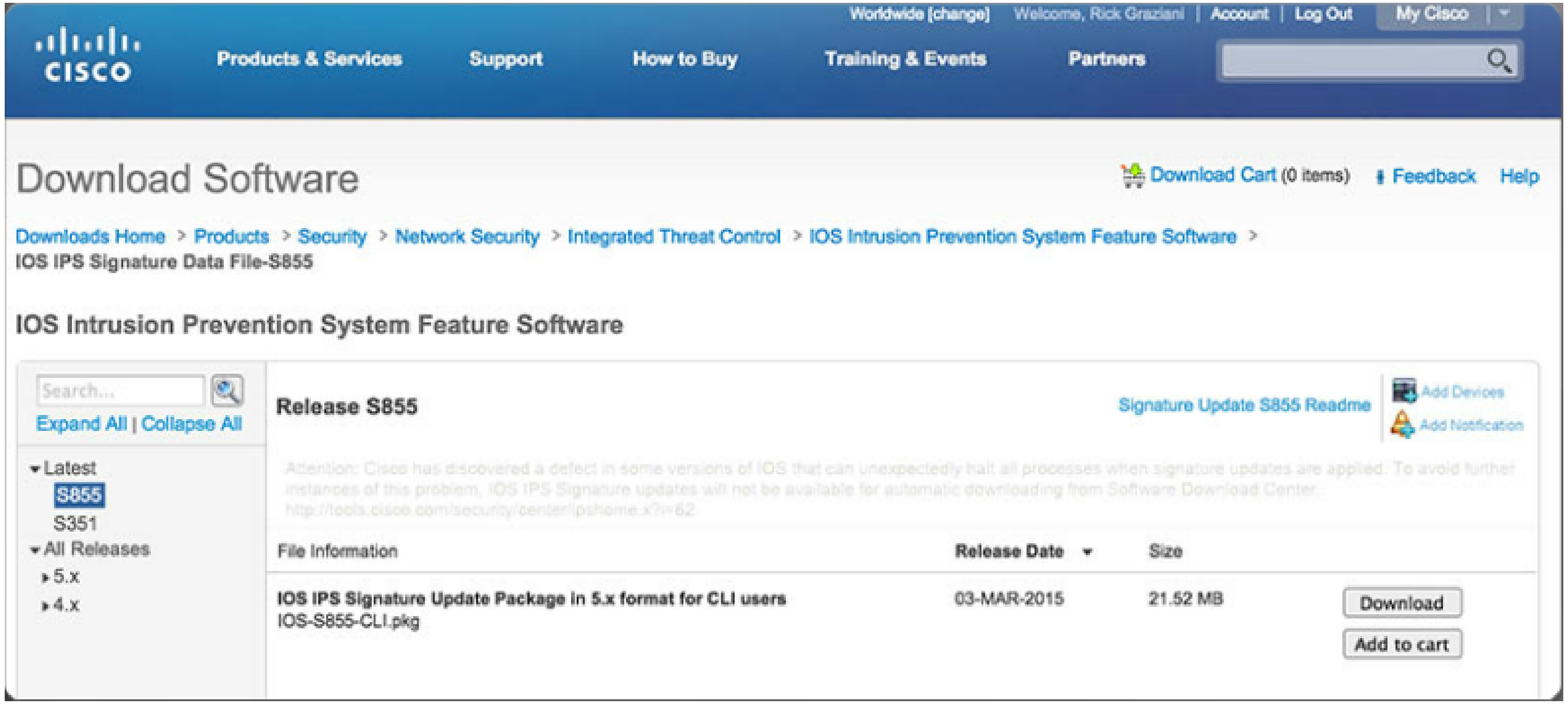
Signature Types - Composite

- Stateful signature
- Identifies a sequence of operations distributed across multiple hosts over an arbitrary period of time
  - Match an attack signature => requires several pieces of data for a time period
    - Length of time => known as the event horizon
    - Varies per signature

- Usually need to have configured the event horizon
  - Can not run out of resources
  - Trade-off between consuming system resources and being able to detect an attack

Signature File

- Contains a package of network signatures
- Updated once a new threats are identified
- Have to be uploaded to an IPS/IDS on regular basis
  - Newer and newer definitions
- Commercial signatures are not usually provided for free
  - Open source ?



Download Software

Downloads Home > Products > Security > Network Security > Integrated Threat Control > IOS Intrusion Prevention System Feature Software > IOS IPS Signature Data File-S855

IOS Intrusion Prevention System Feature Software

Release S855

Signature Update S855 Readme

Attention: Cisco has discovered a defect in some versions of IOS that can unexpectedly halt all processes when signature updates are applied. To avoid further instances of this problem, IOS IPS Signature updates will not be available for automatic downloading from Software Download Center. http://tools.cisco.com/security/center/ipshome.x?i=62

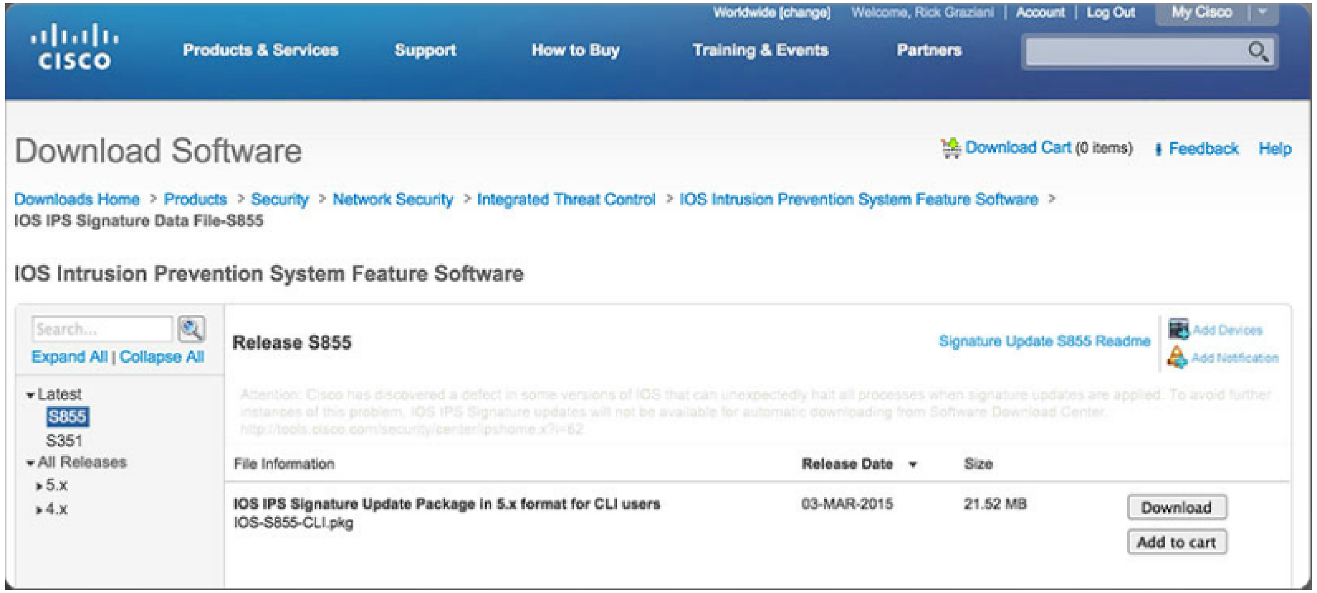
File Information	Release Date	Size
IOS IPS Signature Update Package in 5.x format for CLI users IOS-S855-CLI.pkg	03-MAR-2015	21.52 MB

Signature Micro-Engines - SMEs

- SMEs
  - Optimize attack detection => make search more efficient
  - They define for what the SME will search => define patterns
  - Contains set of parameters with allowable ranges or sets of values and fields what SME will inspects
    - Allows to define the signature too
- Cisco IOS defines five micro-engines (availability depends on the hw platform):
  - Atomic
    - Signatures that examine simple packets of specific protocol (ICP, UDP, TCP)
  - Service
    - Signatures that examine many services that are attacked (DNS, HTTP, FTP, SMTP …)
  - 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.
- SME definition file requires to be regularly updated

Signature Micro-Engines - SMEs

- Consider
  - Compiling a regular expression requires more memory than the final storage of the regular expression
  - Determine the final memory requirements of the finished signature before loading and merging signatures.
  - Assess how many signatures the various router platforms can actually support
    - The number depends on the memory available
  - Equipe a router with the maximum amount of memory possible



Download Software

Downloads Home > Products > Security > Network Security > Integrated Threat Control > IOS Intrusion Prevention System Feature Software > IOS IPS Signature Data File-S855

IOS Intrusion Prevention System Feature Software

Release S855

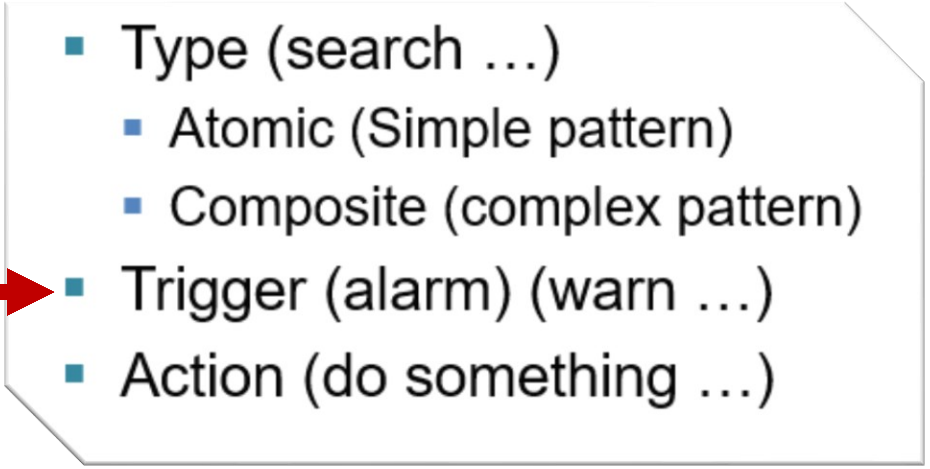
Signature Update S855 Readme

Attention: Cisco has discovered a defect in some versions of IOS that can unexpectedly halt all processes when signature updates are applied. To avoid further instances of this problem, IOS IPS Signature updates will not be available for automatic downloading from Software Download Center. http://tools.cisco.com/security/center/ipshome.x?i=62

File Information	Release Date	Size
IOS IPS Signature Update Package in 5.x format for CLI users IOS-S855-CLI.pkg	03-MAR-2015	21.52 MB

- Acquire the signature file
  - Signatures for lower priority threats published biweekly.
  - Serious threats – published within hours of identification.
  - Each update includes new signatures and all of the signatures in the previous version.

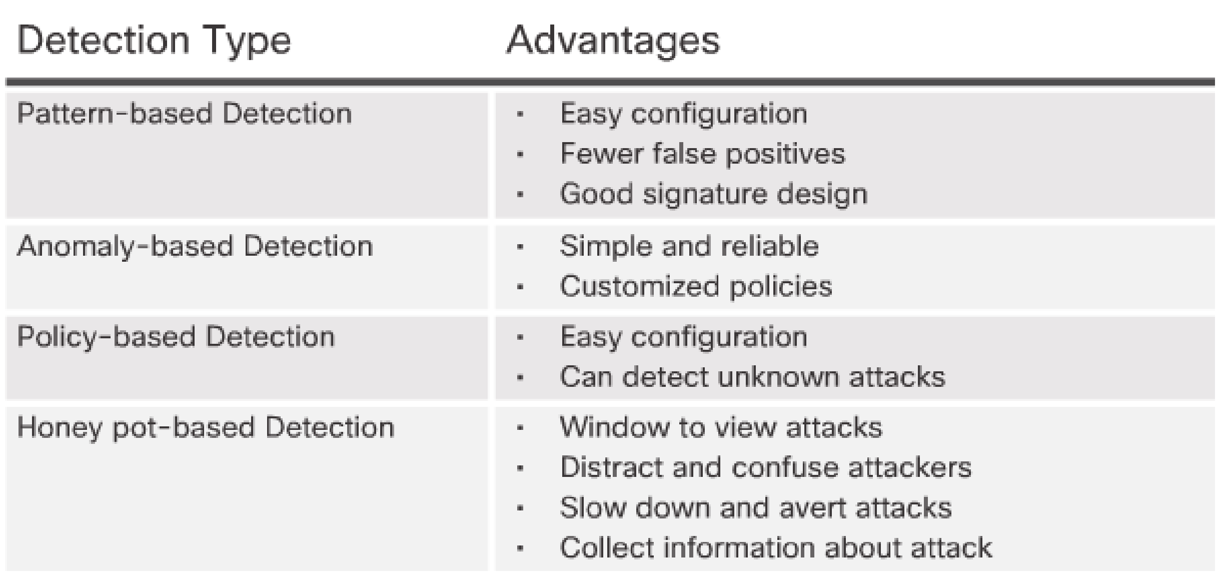
IPS Signature Alarms



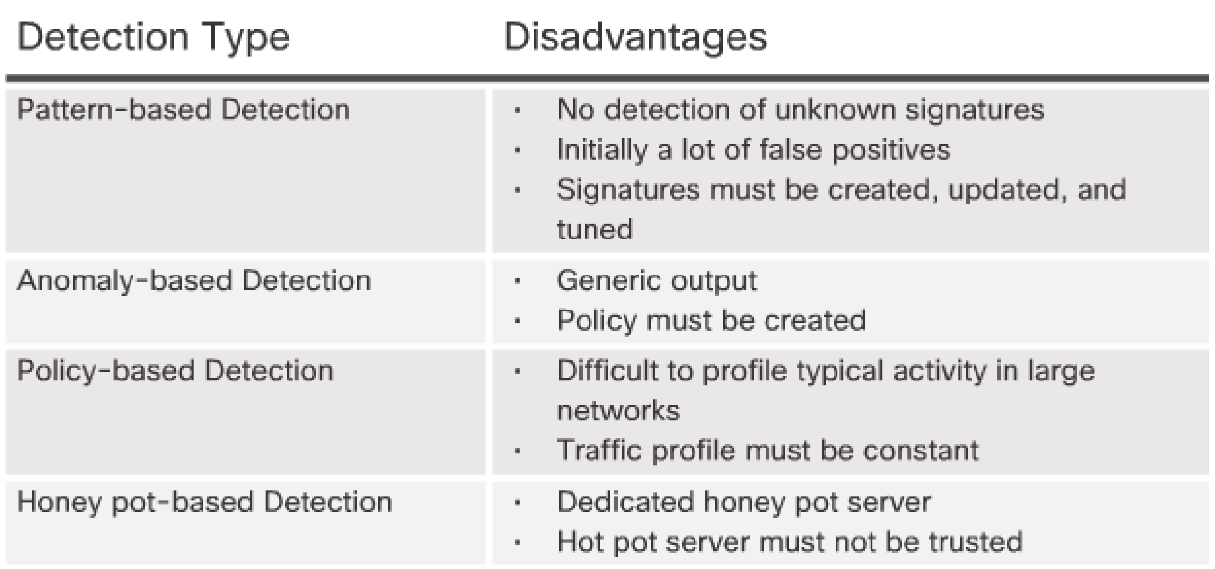
- Type (search …)
  - Atomic (Simple pattern)
  - Composite (complex pattern)
- Trigger (alarm) (warn …)
- Action (do something …)

Signature Alarm

- Signature alarm = signature trigger
  - It signal the intrusion or security policy violation
- Cisco solutions usually use four types of triggers (detection methods)
  - Pattern-based detection (Signature-based)
  - Anomaly-based detection (Profile-based)
  - Policy-based detection
  - HoneyPot-based detection



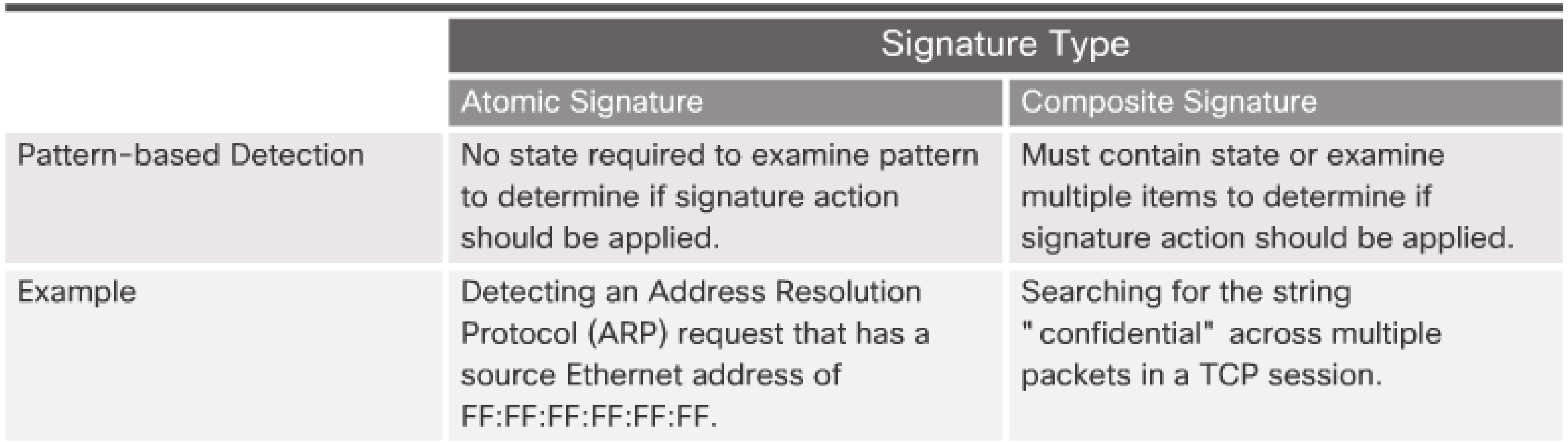
Detection Type	Advantages
Pattern-based Detection	Easy configuration Fewer false positives Good signature design
Anomaly-based Detection	Simple and reliable Customized policies
Policy-based Detection	Easy configuration Can detect unknown attacks
Honey pot-based Detection	Window to view attacks Distract and confuse attackers Slow down and avert attacks Collect information about attack



Detection Type	Disadvantages
Pattern-based Detection	No detection of unknown signatures Initially a lot of false positives Signatures must be created, updated, and tuned
Anomaly-based Detection	Generic output Policy must be created
Policy-based Detection	Difficult to profile typical activity in large networks Traffic profile must be constant
Honey pot-based Detection	Dedicated honey pot server Hot pot server must not be trusted

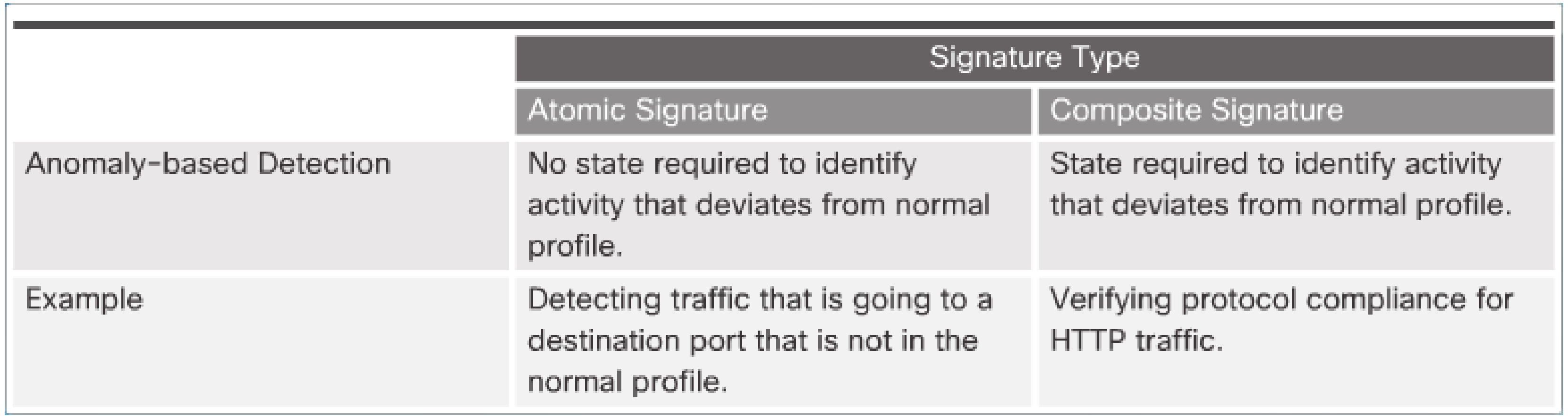
Pattern-Based Detection

- Also known as **signature-based detection**
- Simplest trigger
  - Might be textual, binary, or a series of function calls
  - Search for a specific and pre-defined pattern in network traffic (match)
    - Defined within of a database of known attacks
    - Database need to be periodically updated
- Can be detected in a single packet (atomic) or in a sequence of packets (composite)
- Requires tuning, as by default produce many false positives
- Difficult deals with protocols not running on well known ports
- Gartner recommends behavioral-based NDR tools (Network detection and response)
  - https://fidelissecurity.com/resource/report/2020-gartner-ndr-market-guide/
    - Cisco StealthWatch, Flowmon



	Signature Type	
	Atomic Signature	Composite Signature
Pattern-based Detection	No state required to examine pattern to determine if signature action should be applied.	Must contain state or examine multiple items to determine if signature action should be applied.
Example	Detecting 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.

Anomaly-Based Detection

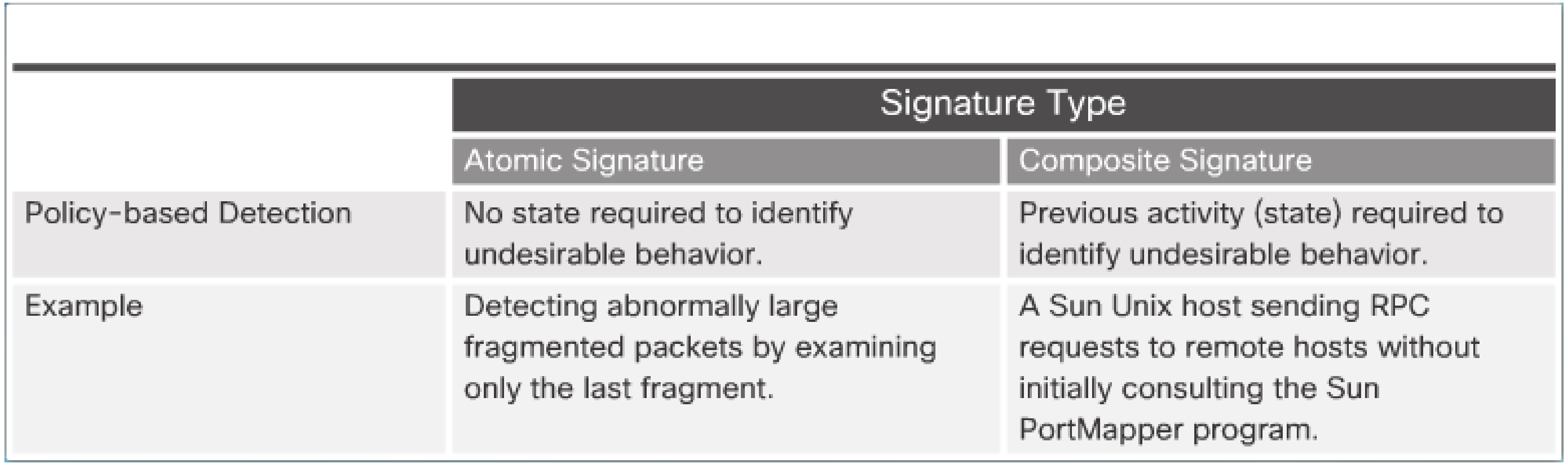


	Signature Type	
	Atomic Signature	Composite Signature
Anomaly-based Detection	No state required to identify activity that deviates from normal profile.	State required to identify activity that deviates from normal profile.
Example	Detecting traffic that is going to a destination port that is not in the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

- Also known as **profile-based detection or network behavior analysis or heuristic analysis**
- Look for traffic that deviates from “**normal**”
- First what must be defined => a profile of a normal behavior (so called as **Base line**)
  - Learned by monitoring the network activity (learning phase)
  - Or defined by specification (RFC)
  - Biggest issue
- Triggers are activated if excessive activity occurs beyond a specified threshold defined by a normal profile
- Pros:
  - May detect unknown attacks
- Cons:
  - Deviation of a normal traffic may by indicated as an attack
  - Can be difficult to define normal behavior (how do I know if a network is without attacks?)
  - Difficult to find specific attack, detection just indicates an anomaly (non normal)

Policy-Based Detection

- Policy-based detection = rule-based detection
  - Detection based on defined policies
    - Any traffic outside of the policy will generate an alarm
    - Creating a policy
      - Requires detailed knowledge of the network andtraffic
      - Is very time-cosuming
  - May use historical analysis (statistical evaluation of flows) and thresholds
    - An example, the number of scanned ports on a machine
  - Single signature may cover an entire class of similar activities



	Signature Type	
	Atomic Signature	Composite 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.

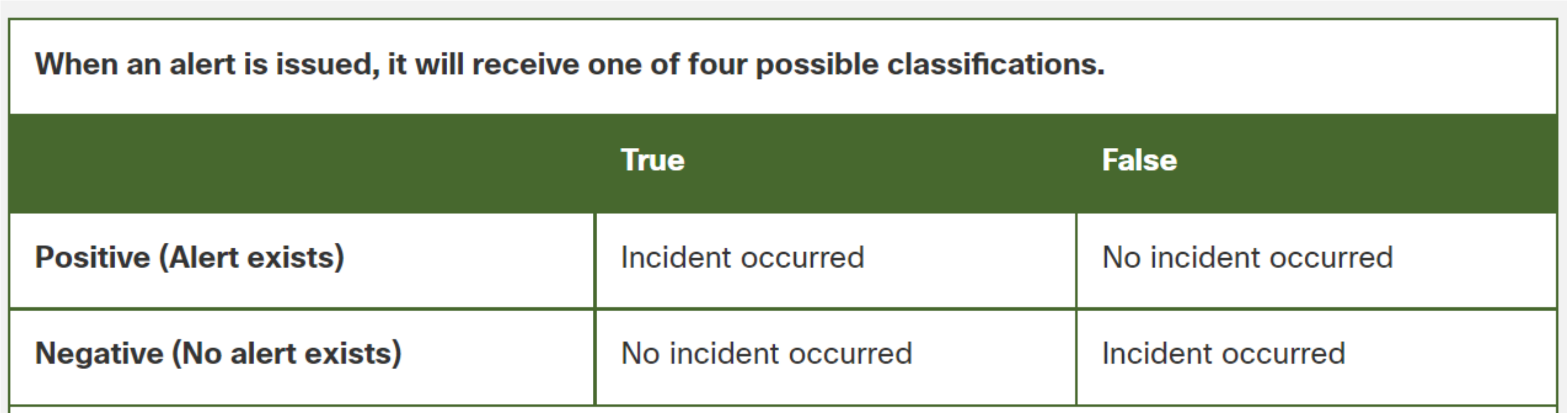
Honey-Pot Based Detection

- Honey Pot
  - A dummy server to attract attacks pretending to be vulnerable
  - Purpose is
    - Distract attacks away from real network devices
    - Allows administrators to analyze incoming types of attacks and malicious traffic patterns
    - Rarely used in production, more in research
  - The Honeynet Project – Honeypot research

Alarm Triggering Mechanisms – decision strategy

- **False positive**
  - Undesired, sensor generates an alarm on normal traffic, that should not to
  - Requires tuning
- **False negative**
  - Sensor should generate an alarm on configured attack, but it did not do
  - It is imperative that the IDS should not generate false negatives
    - Because that means that known attacks are not being detected
    - The goal is for these alarm types to generate true positive alarms.

- **True positive**
  - Expected behavior, generates an alarm in response to known attack traffic.
- **True negative**
  - Expected behavior, normal network traffic does not generate an alarm.

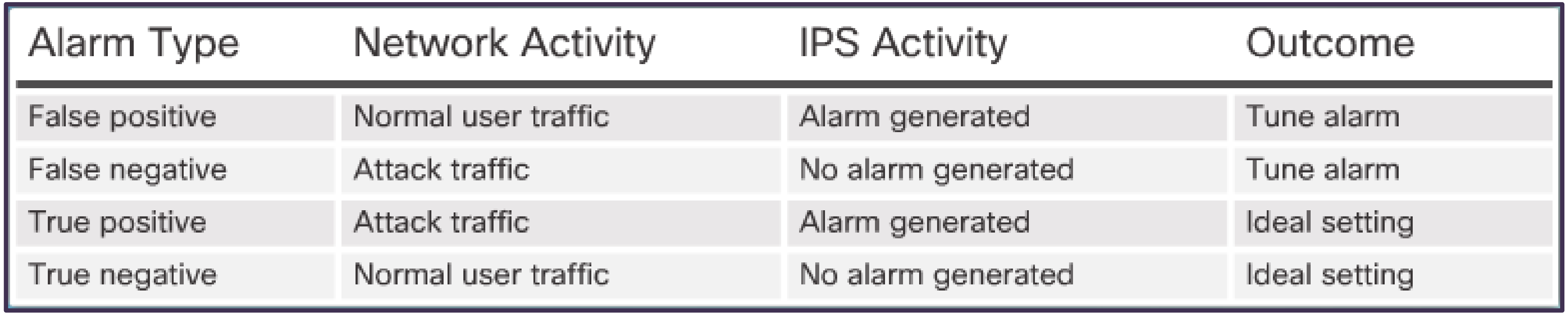


When an alert is issued, it will receive one of four possible classifications.

	True	False
Positive (Alert exists)	Incident occurred	No incident occurred
Negative (No alert exists)	No incident occurred	Incident occurred

IDS alarm actions

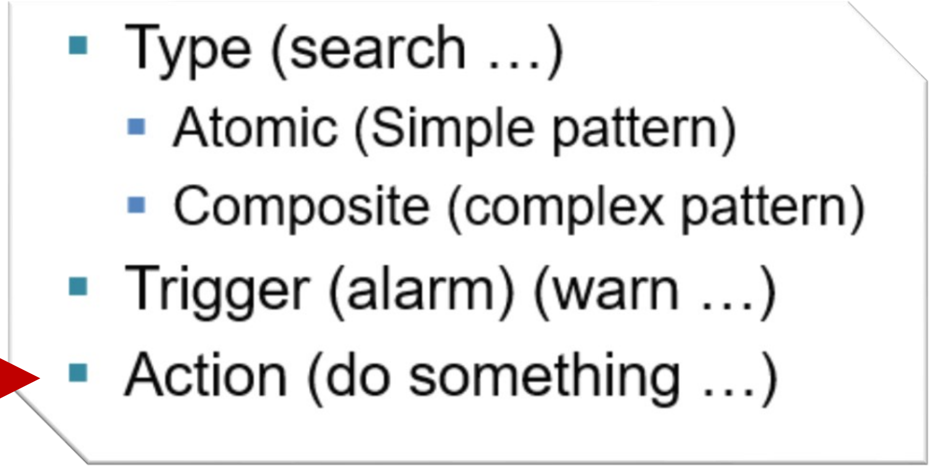
- What to do if



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

- Severity levels
  - Informational: Not intermediate threat
  - Low: abnormal activity but an immediate threat is not likely
  - Medium: abnormal activity but an immediate threat is likely
  - High: abnormal activity but an immediate threat is extremely likely

IPS Signature Actions

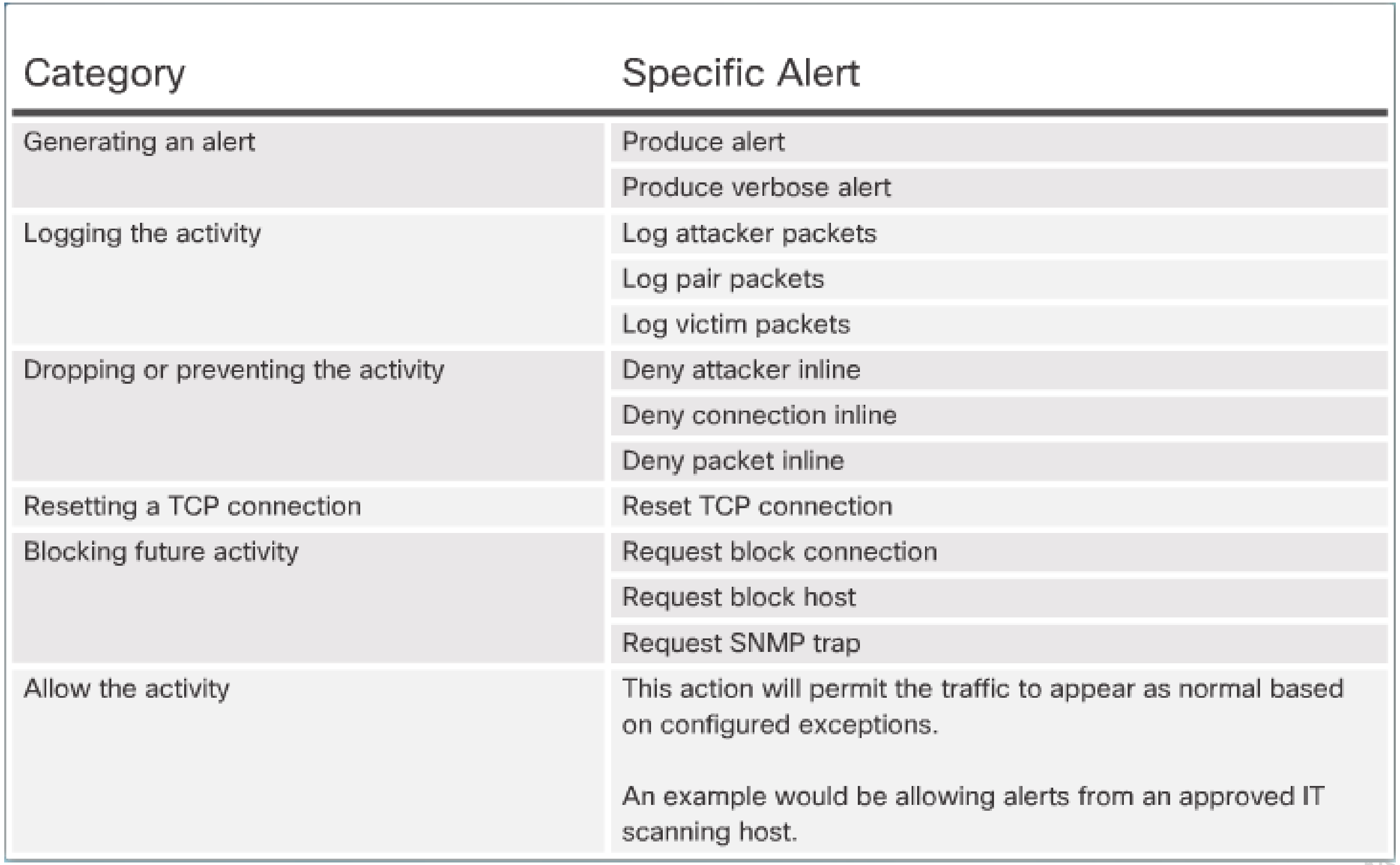


- Type (search …)
  - Atomic (Simple pattern)
  - Composite (complex pattern)
- Trigger (alarm) (warn …)
- Action (do something …)

Signature Actions

- What to do when the activity is detected

Summary of Action Categories:

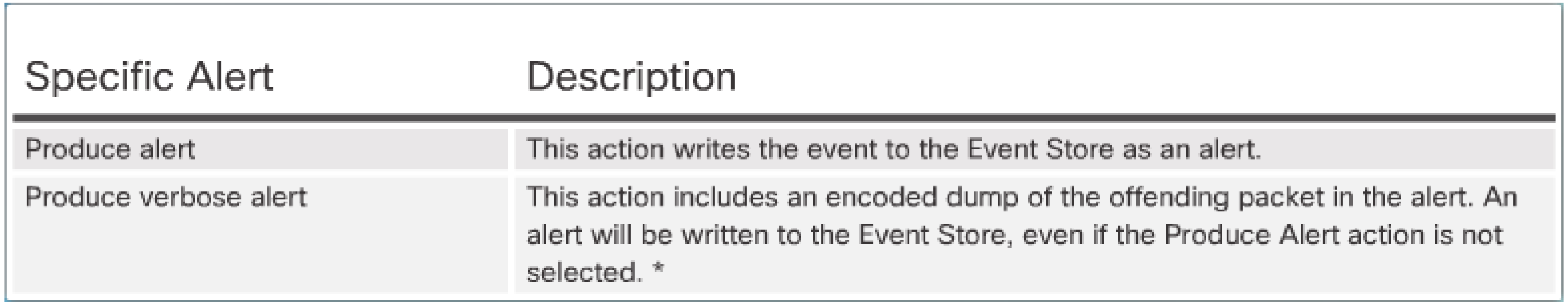


Category	Specific Alert
Generating an alert	Produce alert
	Produce verbose alert
Logging the activity	Log attacker packets
	Log pair packets
	Log victim packets
Dropping or preventing the activity	Deny attacker inline
	Deny connection inline
	Deny packet inline
Resetting a TCP connection	Reset TCP connection
Blocking future activity	Request block connection
	Request block host
	Request SNMP trap
Allow the activity	This action will permit the traffic to appear as normal based on configured exceptions. An example would be allowing alerts from an approved IT scanning host.

Action Categories

1) Generate Alert

- Monitoring and examining the alerts is a prerequisite to understand the attacks
- Type of alerts
  - Atomic
  - Verbose
- Generation of alerts
  - **Atomic alerts**
    - generated every time a signature triggers
    - indicates all occurrences of a specific attack,
    - Lot of information => attacker might be able to flood the monitor console with alerts by generating thousands of bogus alert
  - **Summary alerts**
    - Single alert that indicates multiple occurrences of the same signature from the same source address or port.
    - Produced for defined summary interval or for the number of atomic alerts



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. An alert will be written to the Event Store, even if the Produce Alert action is not selected. *

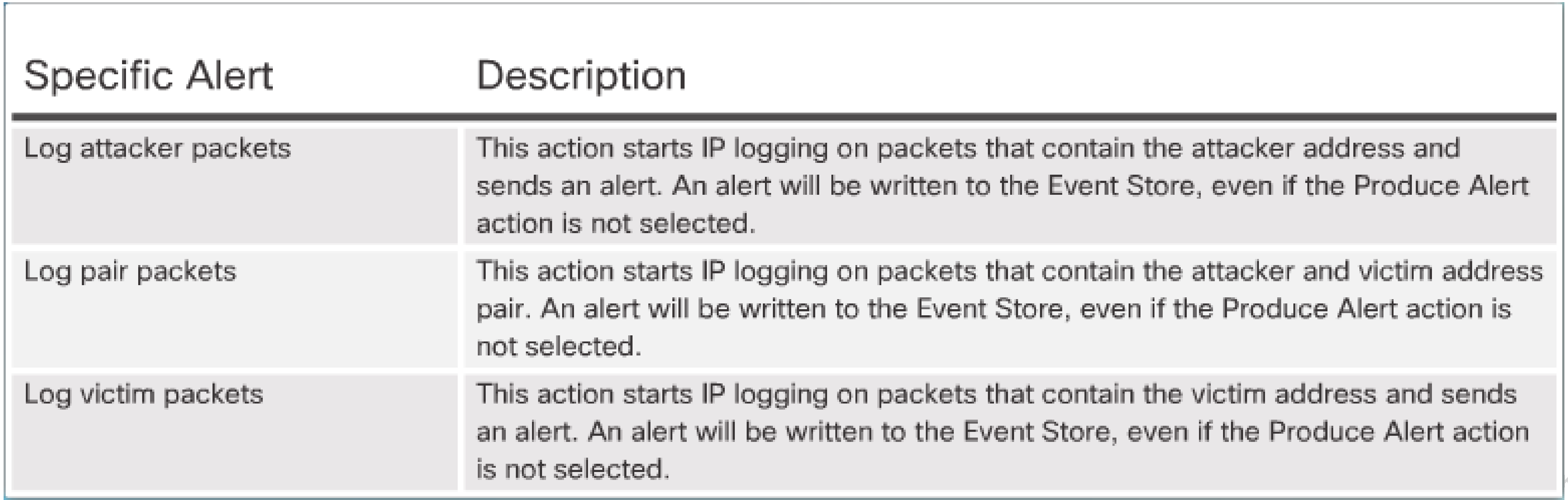
Generating an Alert:

Action Categories

2) Log Activities for Later Analysis

- Log information = stored in a specific file on IPS, log server (database) or SIEM
  - Depend on organization deployment
- Important for later detail attack analysis by
  - NOC (Network Operating Center)
  - SOC (Security Operating Center)

Logging the Activity:

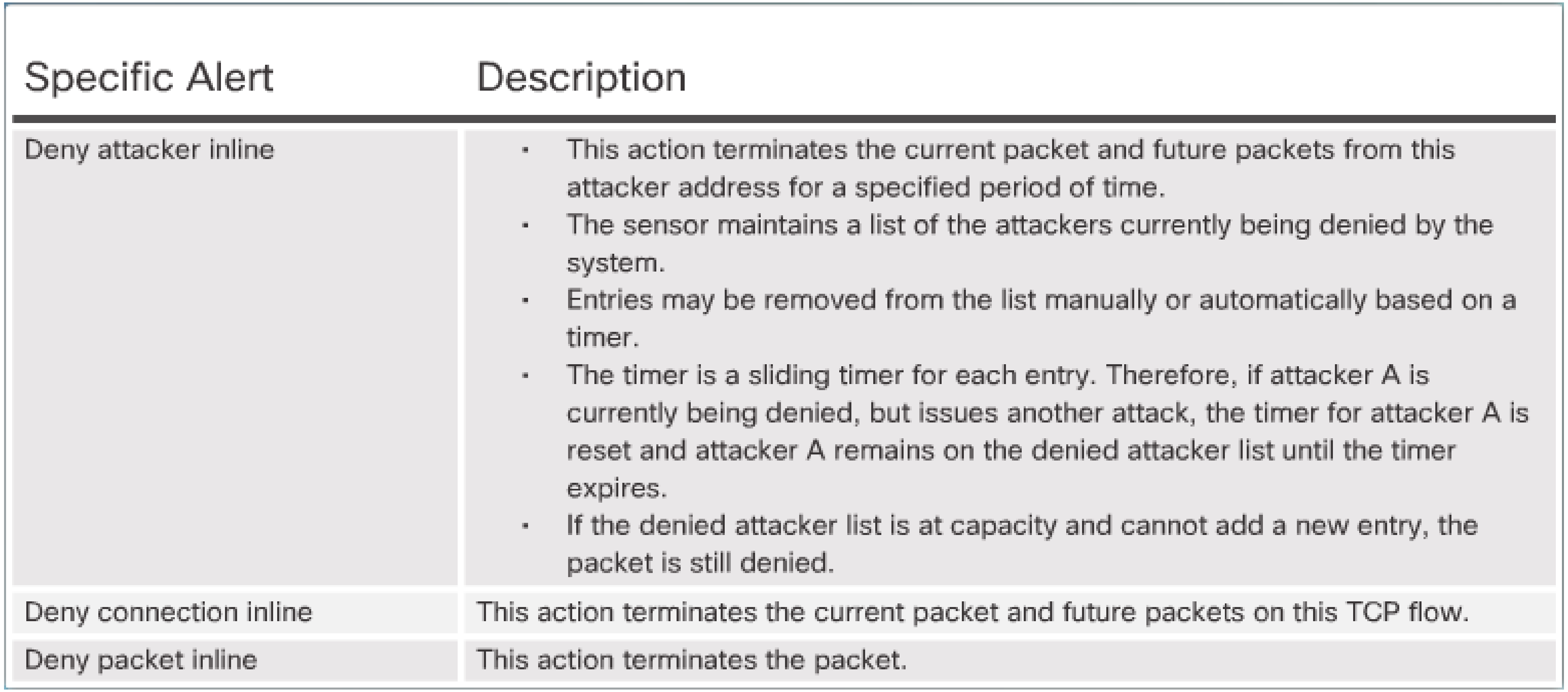


Specific Alert	Description
Log attacker packets	This action starts IP logging on packets that contain the attacker address and sends an alert. An alert will be written to the Event Store, even if the Produce Alert action is not selected.
Log pair packets	This action starts IP logging on packets that contain the attacker and victim address pair. An alert will be written to the Event Store, even if the Produce Alert action is not selected.
Log victim packets	This action starts IP logging on packets that contain the victim address and sends an alert. An alert will be written to the Event Store, even if the Produce Alert action is not selected.

Action Categories

3) Dropping or Preventing the Activity

- One of the most powerful actions
- Three types of deny activities



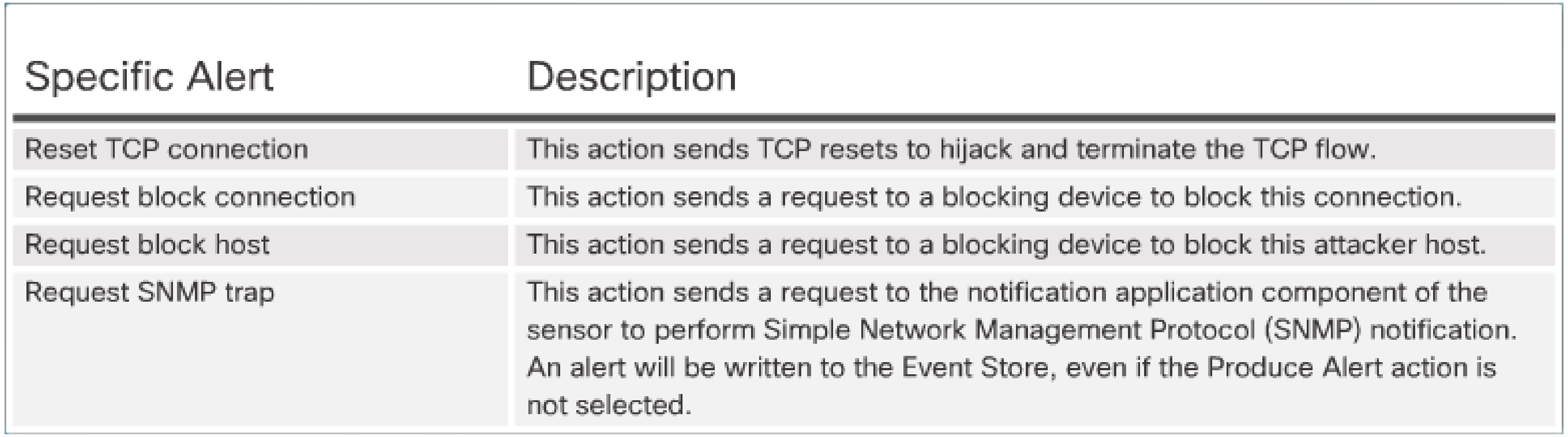
Specific Alert	Description
Deny attacker inline	▪ This action terminates the current packet and future packets from this attacker address for a specified period of time. ▪ The sensor maintains a list of the attackers currently being denied by the system. ▪ Entries may be removed from the list manually or automatically based on a timer. ▪ The timer is a sliding timer for each entry. Therefore, if attacker A is currently being denied, but issues another attack, the timer for attacker A is reset and attacker A remains on the denied attacker list until the timer expires. ▪ If the denied attacker list is at capacity and cannot add a new entry, the packet is still denied.
Deny connection inline	This action terminates the current packet and future packets on this TCP flow.
Deny packet inline	This action terminates the packet.

Action Categories

4) Reset, Block, and Allow Traffic

- Reset
  - Uses TCP RST flag to close a TCP session
- Drop
  - Drop the packet with suspicious payload
- Block further activity
  - For example, place an ACL to stop traffic from an attacking system for a period of time
  - Protect IPS system resources
- Shun
  - Request other devices to block the traffic
- Allowing the activity (Permit)
  - Allow admins define for a few systems or users to be exceptions to the configured rule on an IPS
    - Example: pentest scanning

Resetting the Connection and Blocking the Activity:



Specific Alert	Description
Reset TCP connection	This action sends TCP resets to hijack and terminate the TCP flow.
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	This action sends a request to the notification application component of the sensor to perform Simple Network Management Protocol (SNMP) notification. An alert will be written to the Event Store, even if the Produce Alert action is not selected.

Event monitoring and management - Manage and Monitor IPS

Monitor Activity

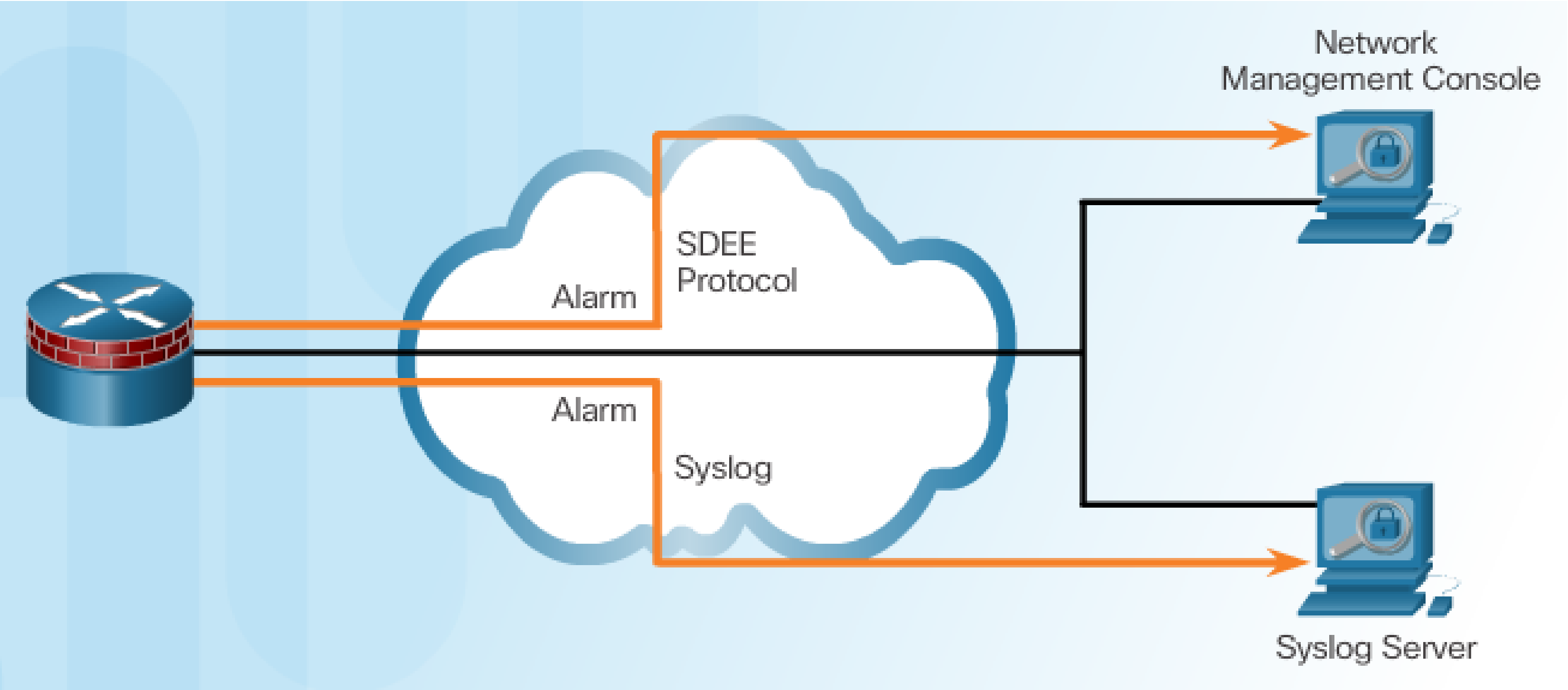
- Monitoring activities
  - A crucial aspect of protecting a network from attack
  - Helps understand attackers, attacks and the strength of protection
  - Helps to identify the attacks and security policy violations
- Support following needs
  - Need for real-time event monitoring and management
  - Need to perform analysis on archived information

Monitor Activity - strategy

- Four factors to consider when planning monitoring strategy:
  - **Management method**
    - How to manage IPS/IDS
      - Individually: for simple deployment scenarios only
      - Centrally: for larger sensor deployments
  - **Event correlation**
    - Correlates attacks happening simultaneously at different points across a network
    - Requires correct time set-up (NTP)
    - SIEM (Security Information and Event Management)?
  - **Security staff**
    - Appropriate security staff to analyze the activity and determine how well the IPS is protecting the network
  - **Incident response plan**
    - What to do if my network is compromised and how to restore the normal state

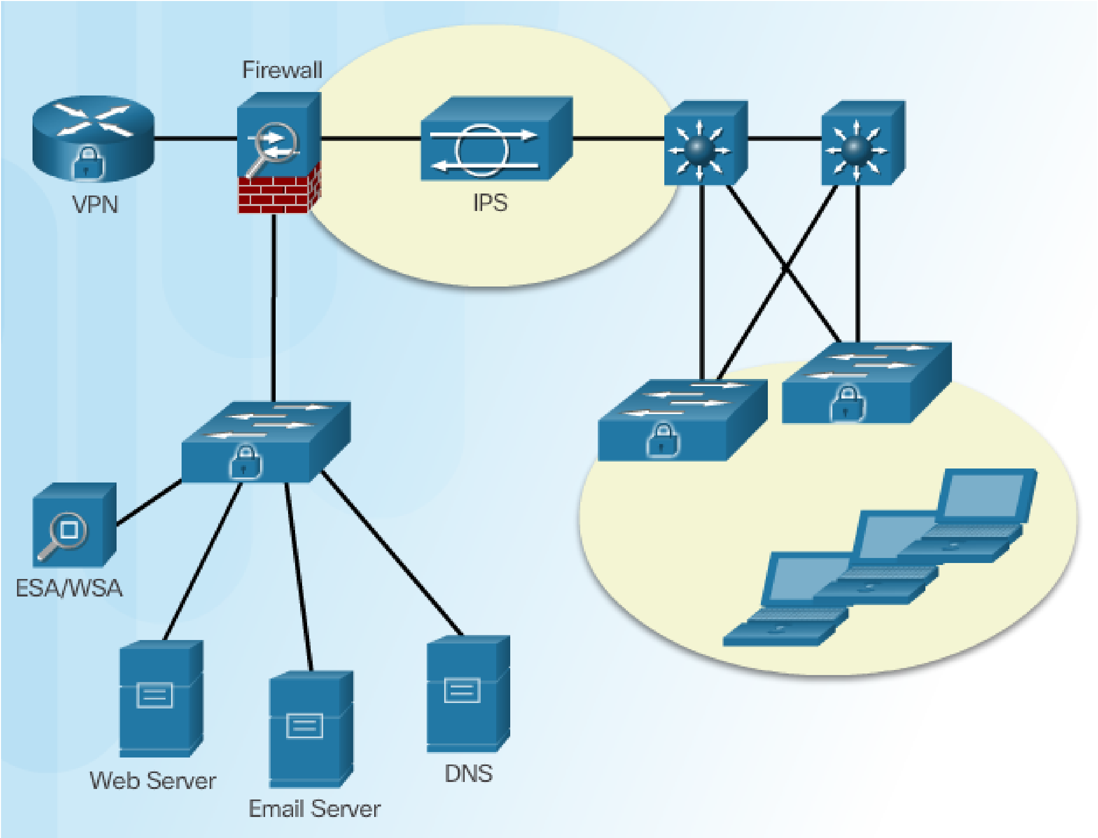
Secure Device Event Exchange - SDEE

- SDEE protocol
  - For the communication of security events generated by security devices
  - Uses a syslog message format
    - `%IPS-4-SIGNATURE:Sig:1107 Subsig:0 Sev:2 RFC1918 address [192.168.121.1:137 ->192.168.121.255:137]`



IPS Configuration Best Practices

- Balance the need to upgrade signatures against downtime
- Update signatures automatically rather than manually upgrading each sensor
- Download 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 signature packs on a dedicated SFTP 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.
- Configure the sensors to regularly check the SFTP server for new signature packs. Stagger the time of day for each sensor to check the SFTP server for new signature packs, perhaps through a predetermined change window. This prevents multiple sensors from overwhelming the SFTP server by asking for the same file at the same time.



- Keep the signature levels that are supported on the management console synchronized with the signature packs on the sensors.

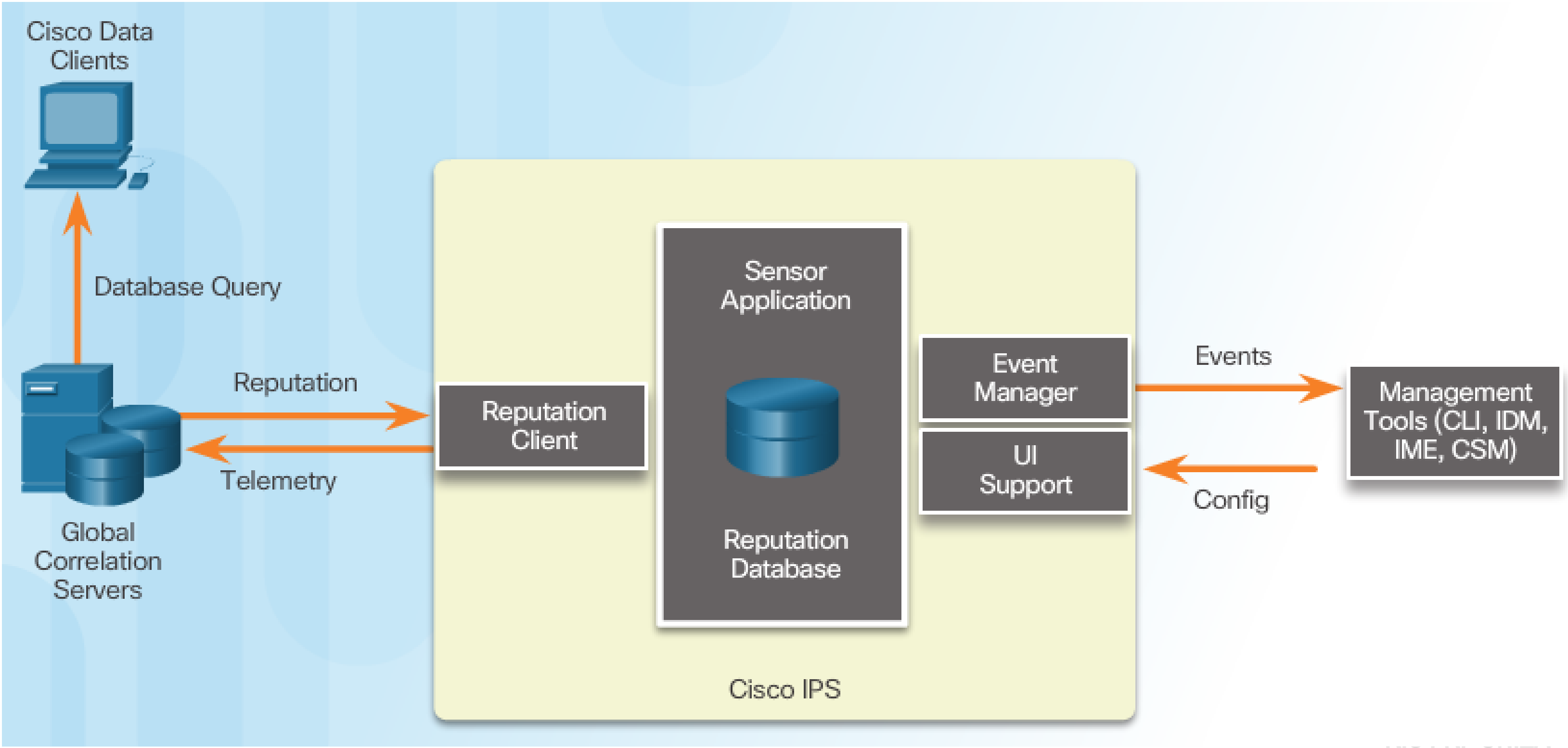
IPS Global Correlation

Cisco Global Correlation

- Cisco Global Correlation
  - Security feature
  - Enables IPS receive regular updates from central Cisco threat database
    - Cisco SensorBase Network
    - Available for Cisco IPS 4300 and 4500 Series appliances, Cisco ASA 5500-X and ISR G2 IPS modules
    - Part of larger Cisco Security Intelligence Operation (SIO)
- Goals of global correlation:
  - Dealing intelligently with alerts to improve effectiveness
  - Improving protection against known malicious sites (IP reputation)
  - Sharing telemetry data with the SensorBase Network to improve visibility of alerts and sensor actions on a global scale
  - Simplifying configuration settings
  - Automatic handling of security information uploads and downloads

Cisco SensorBase Network

- Allows sensor updates correlation data and send its telemetry data
  - Good if performed periodically
- Correlation data informs about the IP address reputation score
  - Helps to sensor determine the action on traffic from these IP addresses
- Mods of operation:
  - Off
  - Partial participation
  - Full participation



Cisco Security Intelligence Operation (SIO)

- Cisco Security Intelligence Operation
  - Large back-end security ecosystem
  - Cisco SensorBase Network is a part of it
  - Purpose is to detect threat activity, research and analyze threats,
  - Provide real-time updates and best practices to keep organizations informed and protected
- Is now **TALOS** (**https://www.talosintelligence.com/**)
  - = Cisco Security Intelligence Operation (SIO) + Sourcefire Vulnerability Research Team (VRT)

- Network participation gathers the following data:
  - Signature ID
  - Attacker IP address
  - Attacker port
  - Maximum segment size
  - Victim IP address
  - Victim port
  - Signature version
  - TCP options string
  - Reputation score
  - Risk rating

Protection before an attack

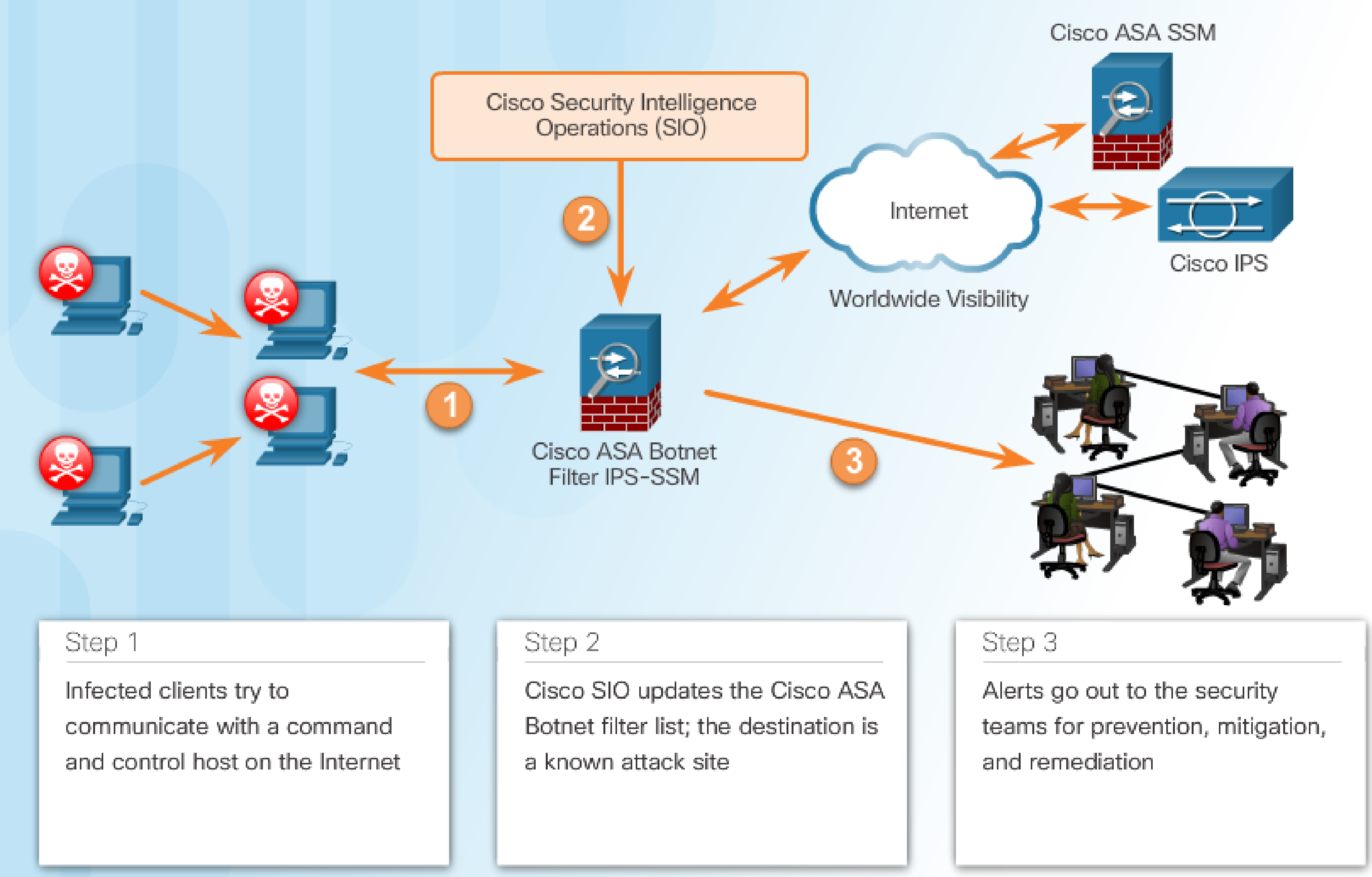
Reputations, Blacklists, and Traffic Filters

- Reputation
  - Apply to networks, IP addresses, mail servers, URLs …
  - An opinion or rating which help to build trust
  - Reputation filters offer the first level of defense by denying traffic based on IP addresses in the blacklist
- Blacklists
  - The list of **bad** IP addresses
    - Whitelist is an opposite
    - Traffic from blacklisted sources is blocked
  - For example in snmp antispam the list of identified spamming servers

Cisco SenderBase is now Talos: https://talosintelligence.com/

Protection before an attack

Reputations, Blacklists, and Traffic Filters


Cisco Security Intelligence Operations (SIO)
Cisco ASA SSM
Internet
Cisco IPS
Worldwide Visibility
2
1
Cisco ASA Botnet Filter IPS-SSM
3

Step 1

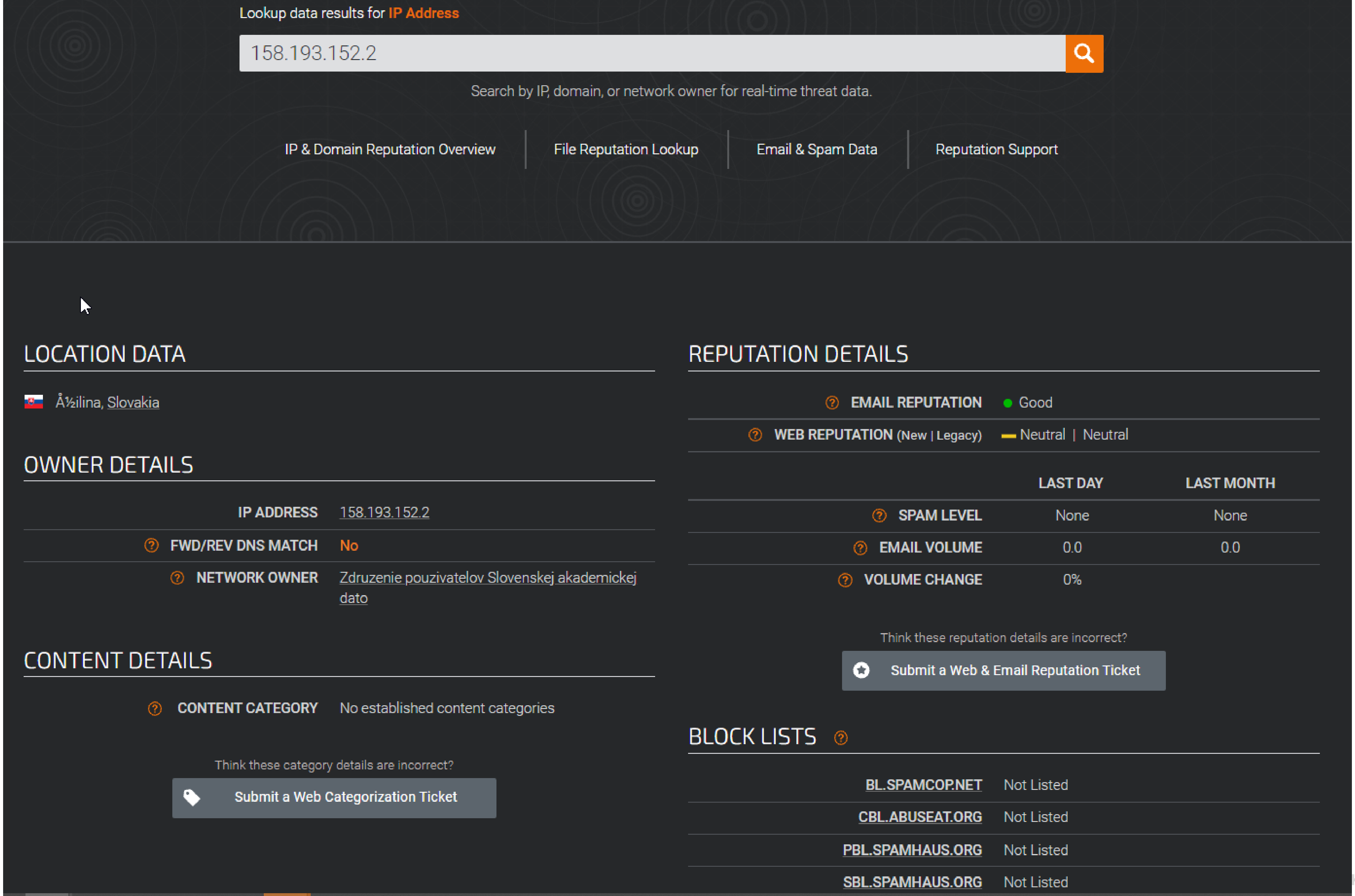
Infected clients try to communicate with a command and control host on the Internet

Step 2

Cisco SIO updates the Cisco ASA Botnet filter list; the destination is a known attack site

Step 3

Alerts go out to the security teams for prevention, mitigation, and remediation



Lookup data results for IP Address

158.193.152.2

Search by IP, domain, or network owner for real-time threat data.

LOCATION DATA

Å½ilina, Slovakia

OWNER DETAILS

IP ADDRESS	158.193.152.2
? FWD/REV DNS MATCH	No
? NETWORK OWNER	Zdruzenie pouzivatelov Slovenskej akademickej dato

CONTENT DETAILS

? CONTENT CATEGORY	No established content categories

Think these category details are incorrect?

Submit a Web Categorization Ticket

REPUTATION DETAILS

? EMAIL REPUTATION	● Good
? WEB REPUTATION (New | Legacy)	▬ Neutral | Neutral

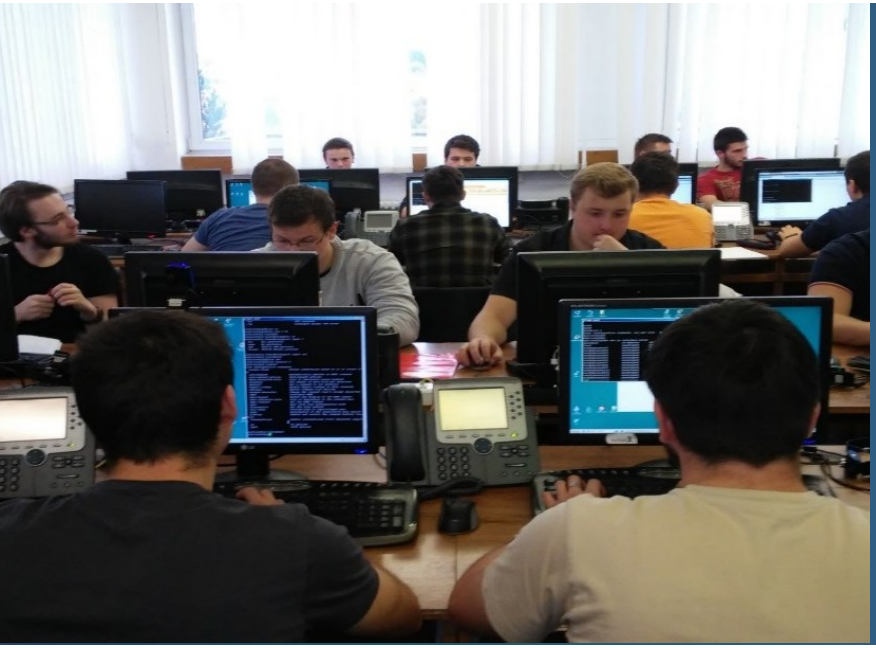
	LAST DAY	LAST MONTH
? SPAM LEVEL	None	None
? EMAIL VOLUME	0.0	0.0
? VOLUME CHANGE	0%	

Think these reputation details are incorrect?

Submit a Web & Email Reputation Ticket

BLOCK LISTS ?

BL.SPAMCOP.NET	Not Listed
CBL.ABUSEAT.ORG	Not Listed
PBL.SPAMHAUS.ORG	Not Listed
SBL.SPAMHAUS.ORG	Not Listed



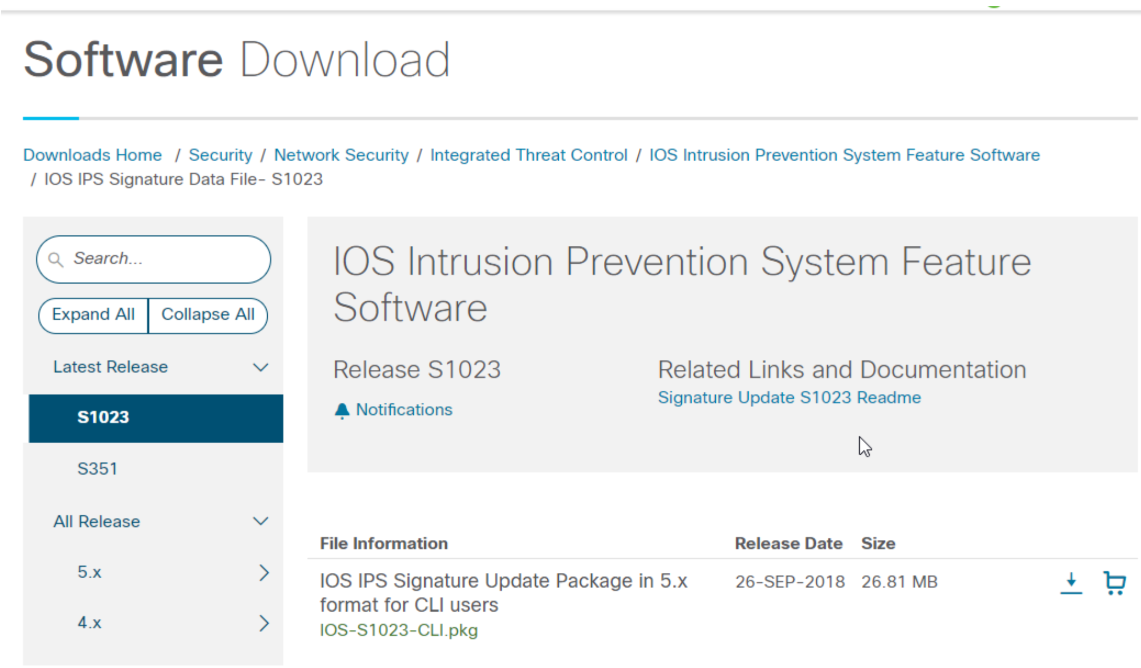
Configure Cisco IOS IPS with CLI

Implement IOS IPS feature

- IOS IPS
  - enables to manage intrusion prevention on routers
  - 12.4(10)T and earlier - 4.x format
    - Has built in signatures and support the import of signatures
  - Newer IOS versions - 5.x format
    - No build-in signatures
    - All signatures in separated file that have to be downloaded and imported
      - CCO required
    - support for encrypted signature parameters and addition of a signature risk rating
- How to implement IOS IPS (IOS IPS 5.x for IOS12.7 and later):
  - 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 IOS IPS

- Free Cisco Connection Online (CCO) account is required
  - Package file IOS-Sxxx-CLI.pkg
    - [Downloads Home - Security - Network Security - Integrated Threat Control - IOS Intrusion Prevention System Feature Software - IOS IPS Signature Data File- S1023]
  - **realm-cisco.pub.key.txt** - public crypto key used by IOS IPS



Software Download

Downloads Home / Security / Network Security / Integrated Threat Control / IOS Intrusion Prevention System Feature Software / IOS IPS Signature Data File- S1023

IOS Intrusion Prevention System Feature Software

Release S1023

Notifications

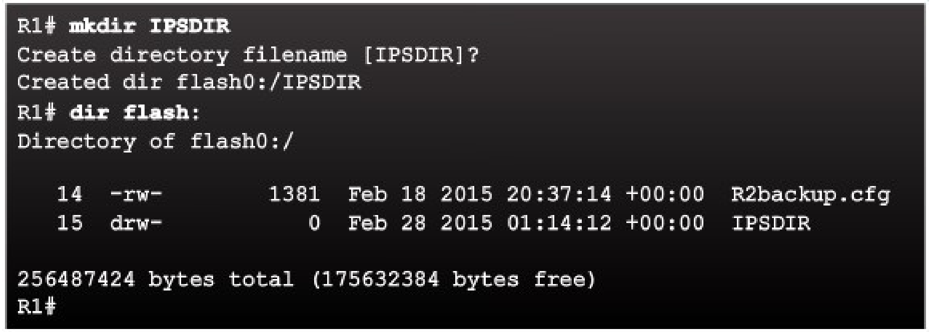
Related Links and Documentation

Signature Update S1023 Readme

File Information	Release Date	Size
IOS IPS Signature Update Package in 5.x format for CLI users IOS-S1023-CLI.pkg	26-SEP-2018	26.81 MB

Step 2) Create an IOS IPS configuration directory in Flash/USB:

```
! Make a directory in flash for sig and key file
Router# mkdir DIRECTORYY-NAME

! Other cmd
Router# rename CURRENT-DIRECTORYY-NAME NEW-NAME

! Display directories
Router# dir [/all] [filesystem: ][file-url]
```



```
R1# mkdir IPSDIR
Create directory filename [IPSDIR]?
Created dir flash0:/IPSDIR
R1# dir flash:
Directory of flash0:/

  14  -rw-        1381  Feb 18 2015 20:37:14 +00:00  R2backup.cfg
  15  drw-           0  Feb 28 2015 01:14:12 +00:00  IPSDIR

256487424 bytes total (175632384 bytes free)
R1#
```

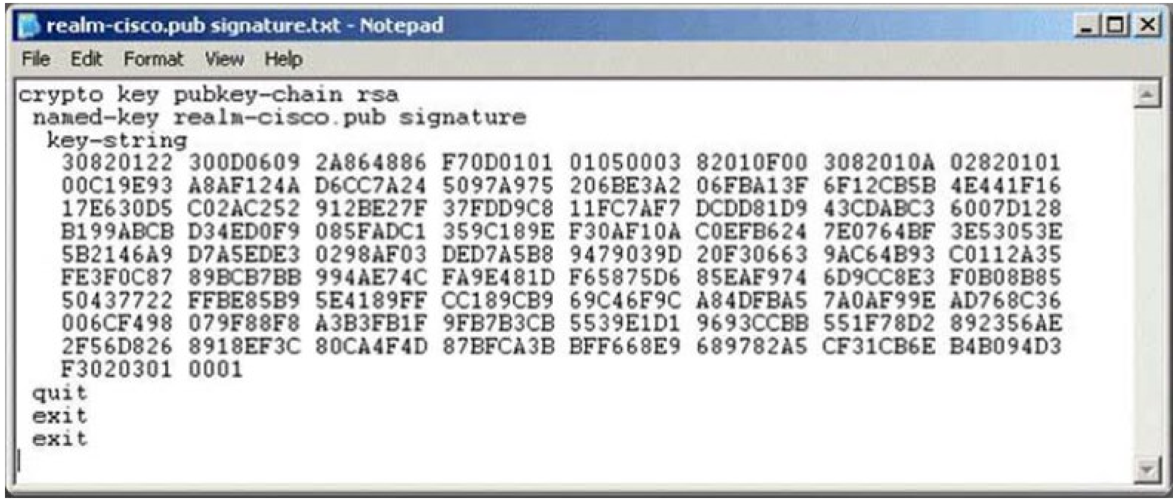
Step 3) Configure IPS Crypto Key

- The crypto key verifies the digital signature for the master signature file
- 1) open the file in a text editor
- 2) select the content and copy to Global Config mode
  - File contains commands to execute
- 3) If the key is configured incorrectly

```
%IPS-3-INVALID_DIGITAL_SIGNATURE:
Invalid Digital Signature found (key
not found)
```

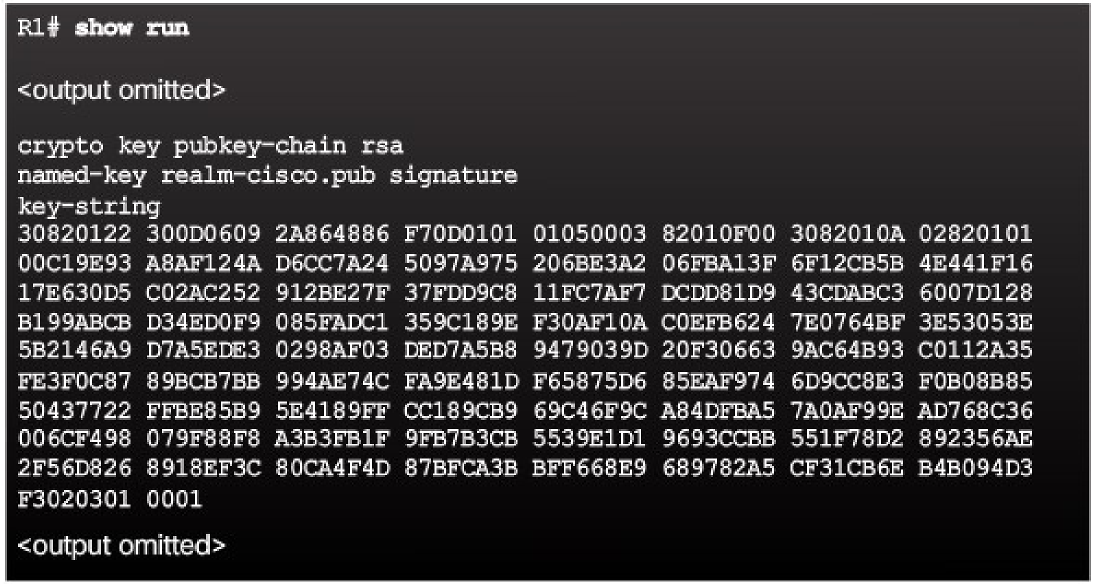
  - Remove it and repeat

```
no crypto key pubkey-chain rsa
no named-key realm-cisco.pub signature
```



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
```



```
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>
```

Step 4) Enable IOS IPS (1.)

- Process consist of four sub-steps
  - A) Create the IP Rule and Location
    - Create a rule name

```
R1(config)# ip ips name [RULE-NAME]
!R1(config)# ip ips name IOSIPS
```

- An optional ACL can be used to filter traffic
  - Permit: traffic is inspected
  - Deny: traffic is not suspected by IPS

```
R1(config)# ip ips config location filesystem:DIR-NAME
!R1(config)# ip ips config location flash:IPSDIR
```

Step 4) Enable IOS IPS (2.)

- B) Enable SDEE and logging event notification

```
R1(config)# ip ips notify [sdee | log]
```

  - Sdee: send messages in sdee format
  - log: send messages in syslog format. Default option.

```
!example
! HTTP server have to be started
R1(config)# ip http server
R1(config)# ip ips notify sdee
R1(config)# ip ips notify log
```

- C) Configure the signature category
  - Signatures are grouped into hierarchical categories
    - Three most common: all, basic, advanced
  - Signatures can be
    - Retired: not compiled and not used
    - unretired: compiled and used

Step 4) Enable IOS IPS (3.)

- C) … Configure the signature category ….
  - When IOS IPS is first configured
    - all signatures in the **all** category should be retired
      - Cmd: retired true
    - Then should be unretired in a less memory-intensive category
      - Cmd: retired false
- Note:
  - The **all** signature category contains all signatures in a signature release
  - Do not unretire the all category
    - Box will run out of memory

```
! Enter IPS category mode
R1(config)# ip ips signature-category
! Change the directory
R1(config-ips-category)# category all
! retire
R1(config-ips-category-action)# retired true
R1(config-ips-category-action)# exit

R1(config-ips-category)# category ios_ips ?
  advanced  Advanced
  basic     Basic
  <cr>

R1(config-ips-category)# category ios_ips basic
! unretire
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# end
Do you want to accept these changes? [confirm]
R1#
*Oct  1 12:45:54.851: Applying Category
configuration to signatures ...
R1#
```

Step 4) Enable IOS IPS (4.)

- d) apply an IPS rule to an interface

```
Router(config-if)# ip ips IPS-NAME {in | out}
```

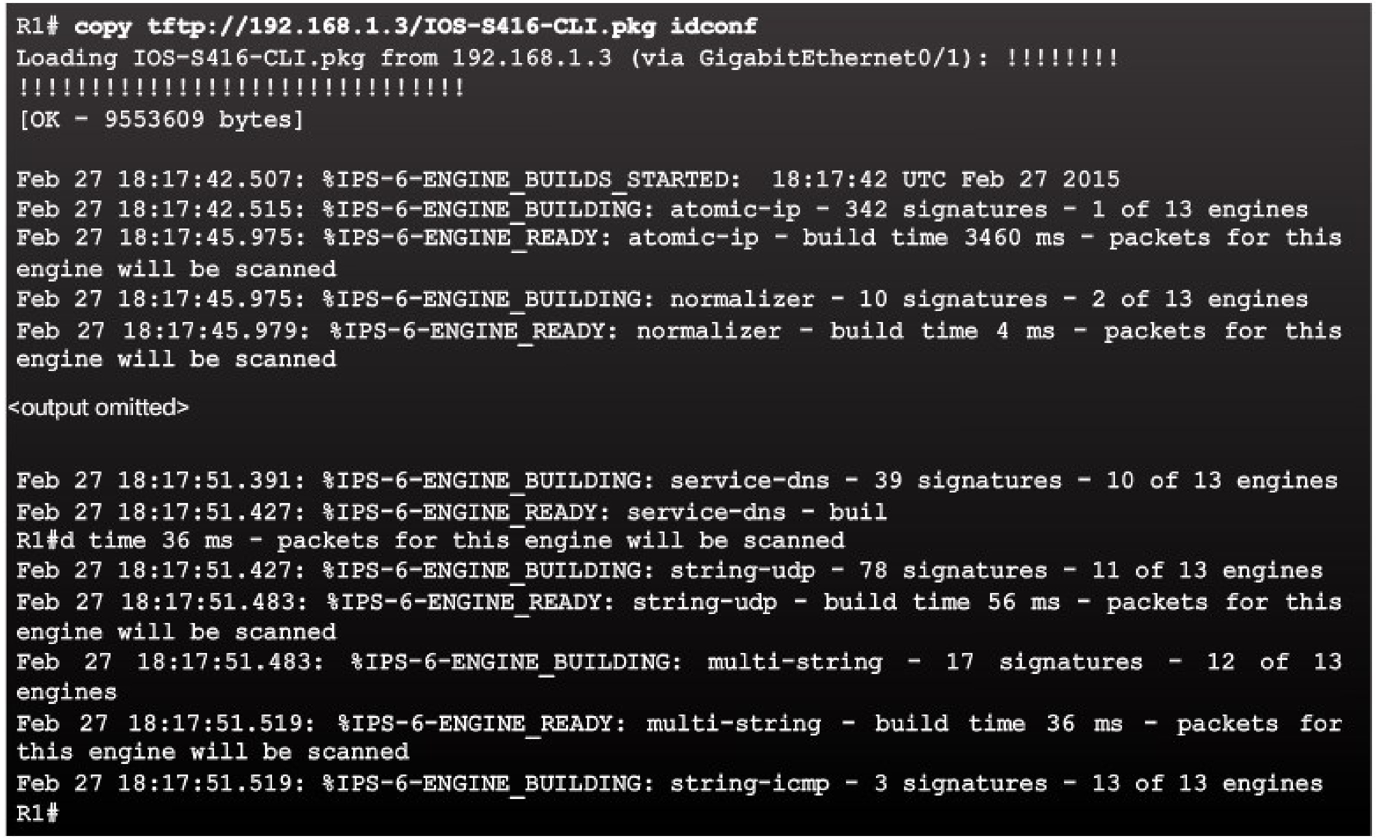
  - In: Apply IPS to inbound interface
  - Out: Apply IPS to inbound interface

```
!example
R1(config)# int g0/0
R1(config-if)# ip ips IOSIPS in
R1(config-if)# exit
R1(config)# int g0/1
R1(config-if)# ip ips IOSIPS in
R1(config-if)# ip ips IOSIPS out
R1(config-if)# end
```

Step 5) Load the IPS Signature Package in RAM

- Use ftp or tftp with idconf parameter

```
Router # copy ftp://gtp_user:paswswd@SERVER_IP/sig_package idconf
```

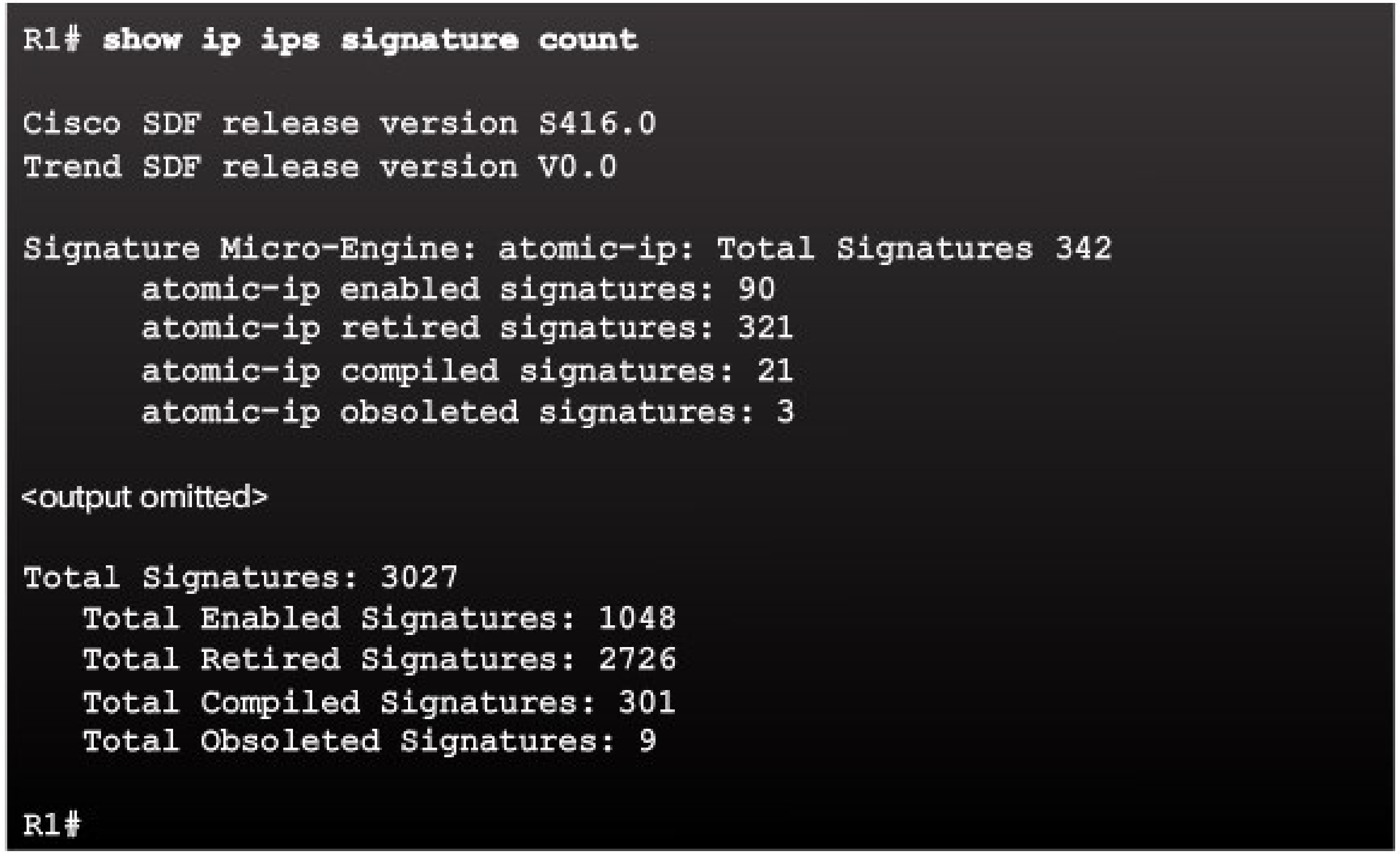


```
R1# copy tftp://192.168.1.3/IOS-S416-CLI.pkg idconf
Loading IOS-S416-CLI.pkg from 192.168.1.3 (via GigabitEthernet0/1): !!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 9553609 bytes]

Feb 27 18:17:42.507: %IPS-6-ENGINE_BUILDS_STARTED:  18:17:42 UTC Feb 27 2015
Feb 27 18:17:42.515: %IPS-6-ENGINE_BUILDING: atomic-ip - 342 signatures - 1 of 13 engines
Feb 27 18:17:45.975: %IPS-6-ENGINE_READY: atomic-ip - build time 3460 ms - packets for this
engine will be scanned
Feb 27 18:17:45.975: %IPS-6-ENGINE_BUILDING: normalizer - 10 signatures - 2 of 13 engines
Feb 27 18:17:45.979: %IPS-6-ENGINE_READY: normalizer - build time 4 ms - packets for this
engine will be scanned
<output omitted>

Feb 27 18:17:51.391: %IPS-6-ENGINE_BUILDING: service-dns - 39 signatures - 10 of 13 engines
Feb 27 18:17:51.427: %IPS-6-ENGINE_READY: service-dns - buil
R1#d time 36 ms - packets for this engine will be scanned
Feb 27 18:17:51.427: %IPS-6-ENGINE_BUILDING: string-udp - 78 signatures - 11 of 13 engines
Feb 27 18:17:51.483: %IPS-6-ENGINE_READY: string-udp - build time 56 ms - packets for this
engine will be scanned
Feb 27 18:17:51.483: %IPS-6-ENGINE_BUILDING: multi-string - 17 signatures - 12 of 13
engines
Feb 27 18:17:51.519: %IPS-6-ENGINE_READY: multi-string - build time 36 ms - packets for
this engine will be scanned
Feb 27 18:17:51.519: %IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 13 of 13 engines
R1#
```

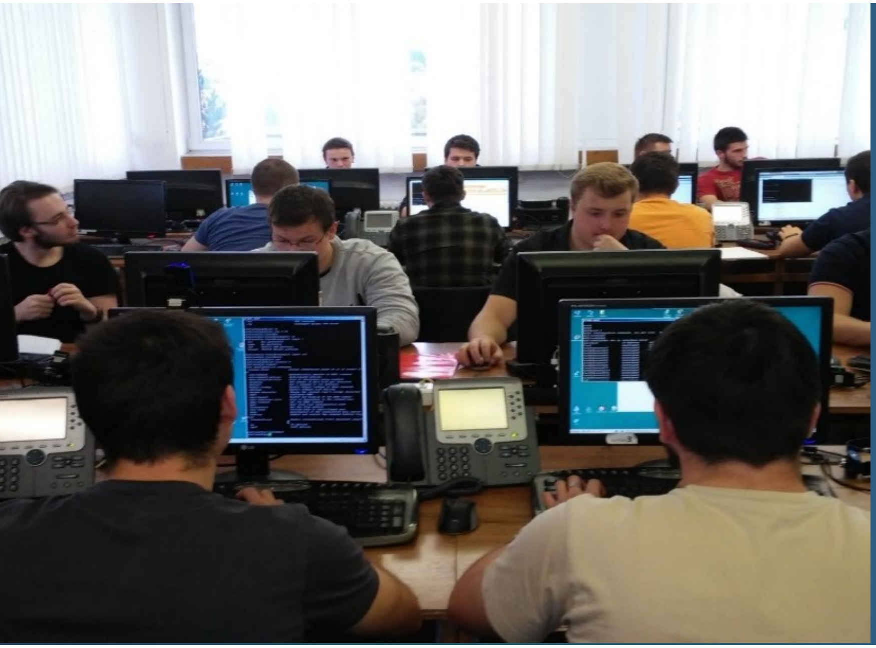
Step 5) Load the IPS Signature Package in RAM

- Verification

```
Router # show ip ips signature count
```



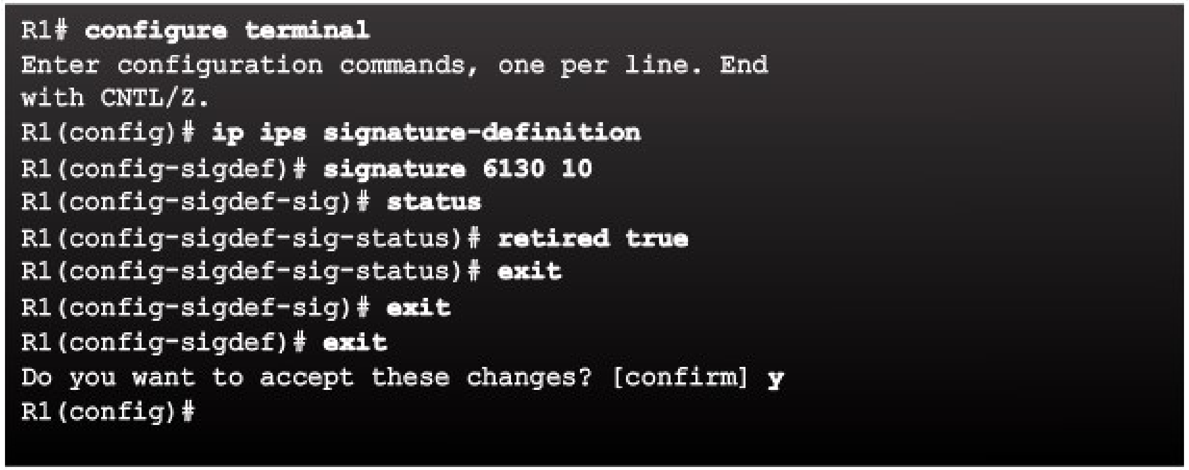
```
R1# show ip ips signature count

Cisco SDF release version S416.0
Trend SDF release version V0.0

Signature Micro-Engine: atomic-ip: Total Signatures 342
      atomic-ip enabled signatures: 90
      atomic-ip retired signatures: 321
      atomic-ip compiled signatures: 21
      atomic-ip obsoleted signatures: 3

<output omitted>

Total Signatures: 3027
   Total Enabled Signatures: 1048
   Total Retired Signatures: 2726
   Total Compiled Signatures: 301
   Total Obsoleted Signatures: 9

R1#
```



Modifying Cisco IOS IPS Signatures

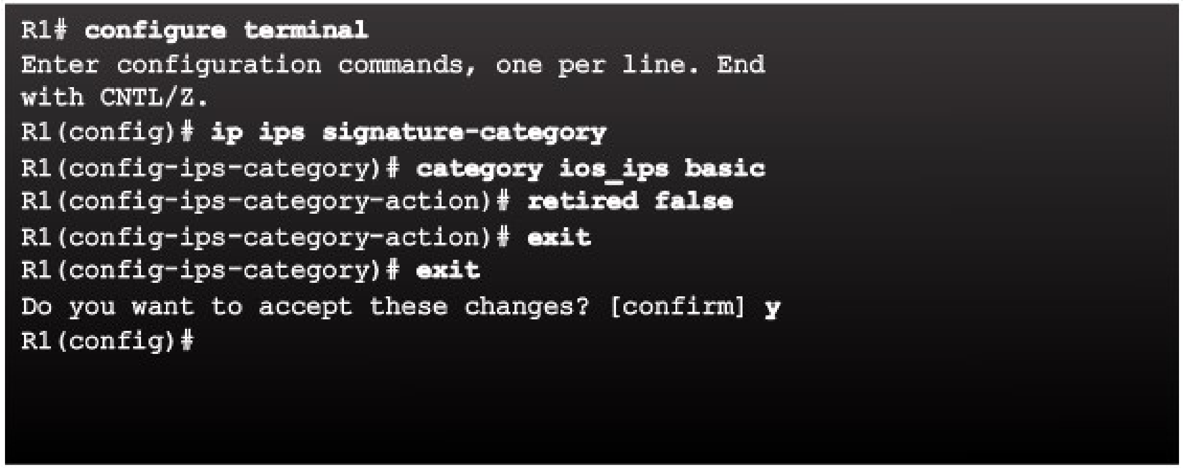
Retire and Unretire Individual Signature

Retiring an Individual Signature:



```
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)#
```

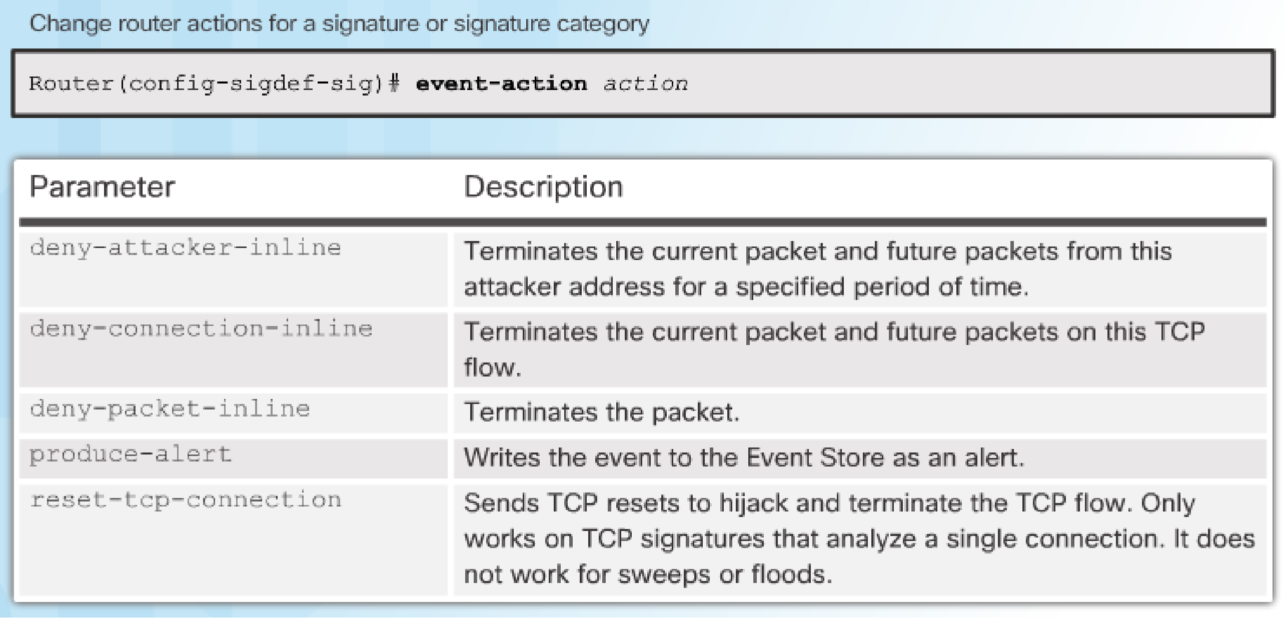
Retiring a Signature Category:



```
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)#
```

Change Signature Actions

- Allows individually per signature to change the action
  - Cmd: event-action

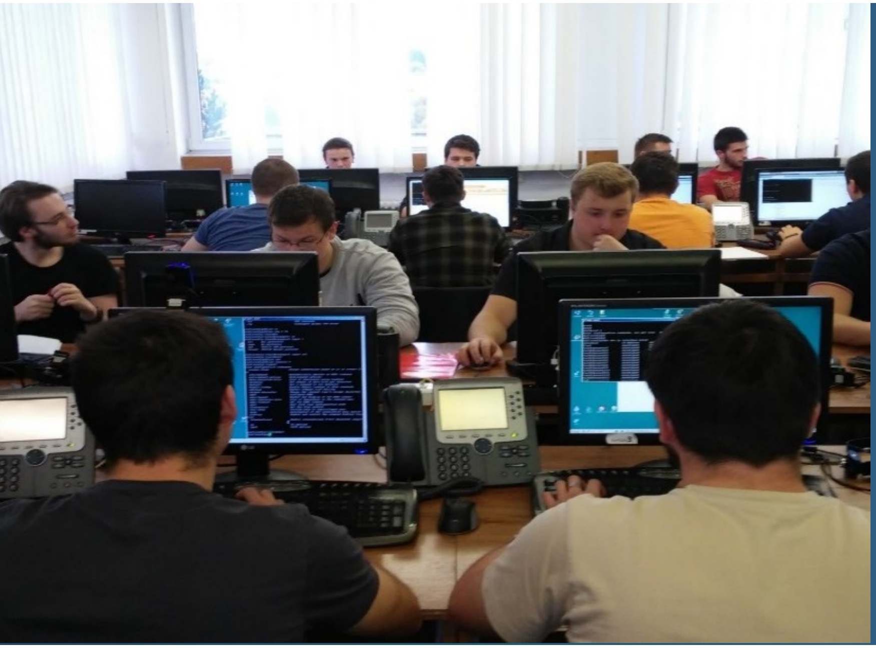


Change router actions for a signature or signature category

```
Router(config-sigdef-sig)# event-action action
```

Parameter	Description
`deny-attacker-inline`	Terminates the current packet and future packets from this attacker address for a specified period of time.
`deny-connection-inline`	Terminates the current packet and future packets on this TCP flow.
`deny-packet-inline`	Terminates the packet.
`produce-alert`	Writes the event to the Event Store as an alert.
`reset-tcp-connection`	Sends TCP resets to hijack and terminate the TCP flow. Only works on TCP signatures that analyze a single connection. It does not work for sweeps or floods.

```
R1#conf t
R1(config)#ip ips signature-category
R1(config-ips-category)#signature 6130 10
R1(config-sigdef-sig-engine)#event-action produce-alert
R1(config-sigdef-sig-engine)#event-action produce-alert
R1(config-sigdef-sig-engine)#event-action produce-alert
R1(config-sigdef-sig-engine)#exit
```



Verify and Monitor IPS

Verify IOS IPS

Show commands to verify the IOS IPS configuration:

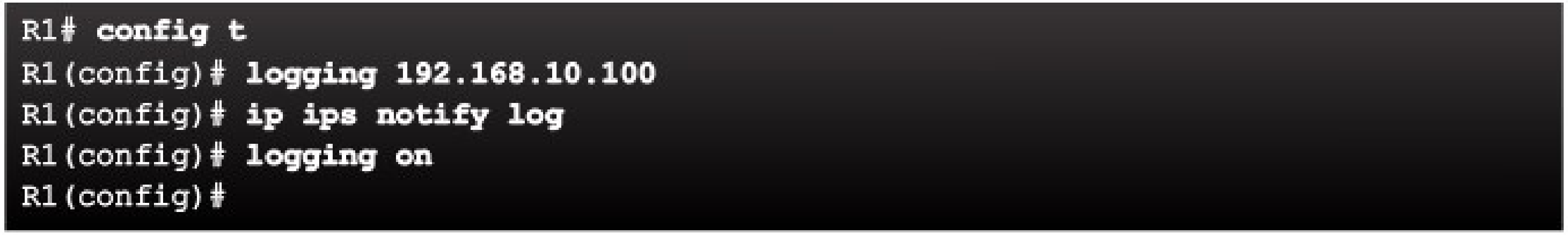
- **`show ip ips`**
  - Provides specific IPS info
- **`show ip ips all`**
  - displays all IPS configuration data
- **`show ip ips configuration`**
  - displays additional configuration data that is not displayed with the **show running-config**
- **`show ip ips interfaces`**
  - displays interface configuration data,
- **`show ip ips signatures`**
  - verifies the signature configuration,
- **`show ip ips statistics`**
  - displays the number of packets audited, and the number of alarms sent,

Clear commands to disable IPS:

- **`clear ip ips configuration`**
- **`clear ip ips statistics`**

Report IPS Alerts

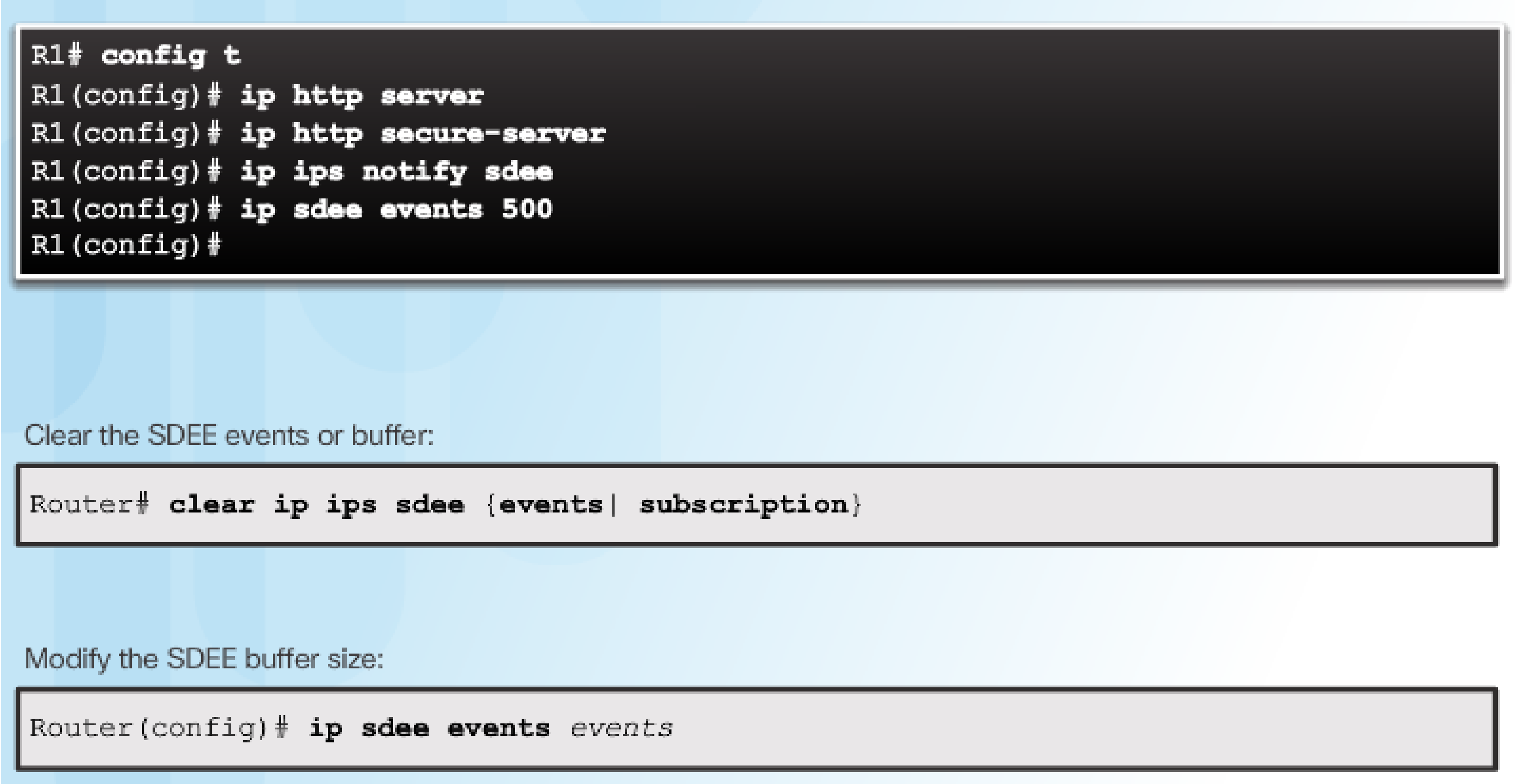
- Specify the method of event notification
  - **`ip ips notify sdee | log`**



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

Enable SDEE

- HTTP/S have to be enabled
- Buffer stores up to 200 SDEE events by default
  - Possible to change up to 1000
    - **ip sdee events**
- Decrease a buffer size
  - all messages are lost
- Increase
  - No problem
- Clear SDEE events
  - **clear ip ips sdee**



```
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)#
```

Clear the SDEE events or buffer:

```
Router# clear ip ips sdee {events| subscription}
```

Modify the SDEE buffer size:

```
Router(config)# ip sdee events events
```

UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

KATEDRA INFORMAČNÝCH SIETÍ * FAKULTA RIADENIA A INFORMATIKY ŽU *

CISCO
Networking
Academy

MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Aktualizované v rámci projektu KEGA 026TUKE-4/2021.