IR-1201 Network Project Report: Intrusion Prevention System (IPS)

Authors:

- Muhammed Arif EREN
- Syed Basit ALI
- Aleksandre CHKAIDZE
- Orlando KODJO

Table Of Contents

1. Introduction

1.1 Project Description

This project comprehends application and testing of an Intrusion Prevention System (IPS) configuration in Cisco Packet Tracer on a network topology. The main objective of this project is to monitor the network traffic, identify potential threats, and intervene with these threats in a proactive manner.

To achieve these goals, Cisco Packet Tracer allows the usage of a router as an Intrusion Prevention System (IPS) with specific configurations. So, we introduced a router called R1 to be an Intrusion Prevention System (IPS) to monitor traffic on its network in the Cisco Packet Tracer. This router R1 follows the signature-pattern matching to monitor network traffic, and these signatures are stored and managed in R1's flash memory. To optimize device resources and retire irrelevant rule sets, router R1 uses "IOS IPS Basic" category. Moreover, to ensure accurate monitoring, the router sends its real-time events to a centralized syslog server. Using explicit server provides accurate chronological analysis by synchronizing the router R1's clock and enables timestamp services for log messages. Furthermore, outbound traffic is inspected from GigabitEthernet 0/1 interface in which IPS rules are applied.

Finally, to verify these configurations in the router R1, we will conduct a specific test case by modifying Signature 2004 (ICMP Echo Request) to alert IPS and observe how R1 prevents unauthorized or suspicious ping activities.

1.2 Definition of IPS

In today's world, IPS is widely used in almost every cyber-conscious organization, and individuals. IPS is a cybersecurity tool that mainly monitors network traffic or host as well as prevents suspicious and malicious intrusions proactively. An IPS is a proactive device designed to prevent attacks against network devices. The IPS is unlike the traditional Intrusion Detection System which allow initial attack. An IPS acts as a layer 2 forwarding device. By virtue of it being a layer 2 device, it is able to drop intrusive attacks in real-time before it reaches its target.

The IPS was designed to accommodate the evolutions of security threats that made older mitigation tools insufficient. The adoption of client-server systems and mobile computing significantly increase the number of targets and pathways available to attackers. The evolution of the internet also extended the reach of these attackers shifting their focus from hardware focused attacked to attacks designed to obtain essential information. These rendered the use of older mitigation systems almost useless as an initial attack is all that is required.

1.3 How an IPS works

Like a firewall, IPS acts as an obstacle between a network and internet, but typical firewalls only inspect header of a packet and filters traffic according to their source and destination IP addresses in Network Layer (Layer 3 in OSI model). In Transport Layer (Layer 4 in OSI model), firewalls inspect header of a segment and filters traffic according to segment's port number. For instance, it matches port 80 for HTTP, and port 22 for SSH, which is not properly sufficient to defeat malicious or suspicious activity because firewalls cannot audit the content of the payload.

On the other hand, Intrusion Prevention Systems (IPSs) can go deeper. It mostly operates from Data Link Layer (Layer 2 in OSI model) until Application Layer (Layer 7 in OSI model). IPS does not look for the header only, but it inspects payload of the PDUs. Also, IPS is designed to detect potential threats before it causes any security breach in a proactive manner.

1.4 Types of IPS

There are generally four types of IPS:

Network-based IPS (NIPS): NIPS, which is the main objective of our project, is deployed entry of the network and can be used with firewall as well as NIPS can be deployed center of the LAN. NIPS that is placed to the entry of the LAN analyzes inbound and outbound traffic which flows in the network, and it responds to the traffic if it detects, and prevents anything suspicious to enter the internal network. The NIPS that is placed inside of the LAN, monitors the internal network to prevent threats to infect other hosts/servers inside of the LAN.

Host-based IPS (HIPS): HIPS is deployed on endpoint devices like hosts and servers. It monitors OS logs, inbound and outbound traffic from the device that is installed, and it interferes to the system according to monitored data. Using Host-based IPS with Network-based IPS builds solid and secure structure against threats that bypassed Network-based IPS.

Wireless Intrusion Prevention System (WIPS): WIPS scans RF signals to protect Wi-Fi structure. It monitors access points and removes unauthorized devices. WIPS also prevents wireless-orientated attacks.

1.5 Types of IPS Alarms

IPS alarms are categorized in 4 parts:

True-positive: This alarm is triggered when the case that IPS flags a real threat and prevents it.

False-positive: False-positive means IPS detects harmless PDU as malicious and triggers an alarm.

True-negative: This is the situation that everything normally operates. There is neither an attack nor an alert.

False-negative: This case is the most dangerous case, which there is an attack on the network and IPS cannot understand it and get alarmed from it.

1.6 Types of IPS Detection Methods

There are three common detection methods used by IPS to detect malicious activity in network traffic.

Signature-Based Detection: Signature-Based IPS stores known cyber-attacks digital fingerprints (signatures) in their database. As network traffic flows, every PDU in the network is compared with these signatures to decide whether to filter or not the PDU. The advantage of this approach is that it detects and prevents known cyber-attack patterns quickly with low false positive rate. Besides its quick approach, it is ineffective to detect zero-day attacks which are unknown cyber-attacks. We used “IOS IPS Basic” signatures in the following project configurations.

Anomaly-Based Detection: Anomaly-Based IPS learns network’s ordinary traffic density, used protocols and hourly habits. This is called baseline of the network. If IPS detects anormal network traffic behavior other than baseline, it treats this network traffic as malicious activity and prevents it. The advantage of Anomaly-Based Detection is that it can detect Zero-Day attacks unlike Signature-Based Detection, but as a downside it has high false positive rate detection.

1.7 IPS Signatures

In Cisco IOS, it is necessary to understand how the IPS is managed in the router in order to have optimized system performance and intrusion detection. Signatures can be managed to optimize device resources.

The signatures are grouped into a hierarchical structure, and also a signature can belong to multiple categories. So, not all of the signatures can be enabled at the same time. This is because the router's memory will be overloaded.

In the Signature-based IPS, Signature Event Action Processor (SEAP) is responsible for managing the actions based on the IPS matching the network traffic patterns with specific signature. SEAP uses parameters like fidelity, severity, or the target value rating. It helps the system to prioritize threats and reduce false positives. So, harmless network traffic is not blocked.

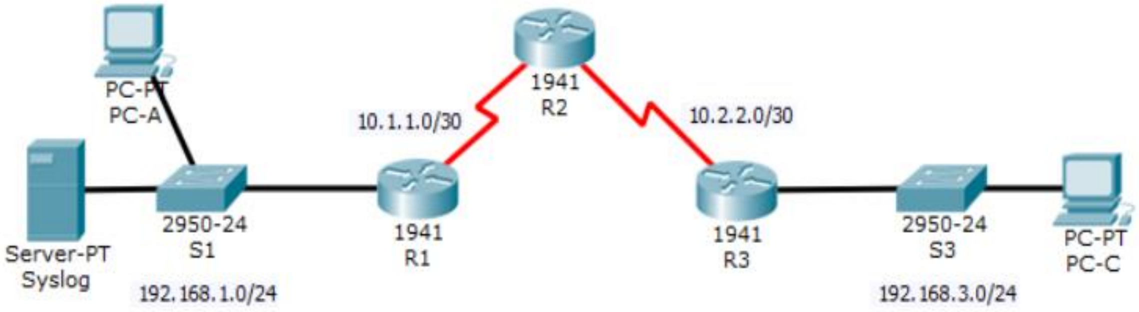
When IPS matches the signature with the network traffic, SEAP can generate various actions, which include transmission of the alert to the syslog server or centralized management interface, packet drop and resetting the connection. In addition, IPS can also block the attacker's source IP address or the connection where the signature was identified for a specific time duration.

2. Network Infrastructure

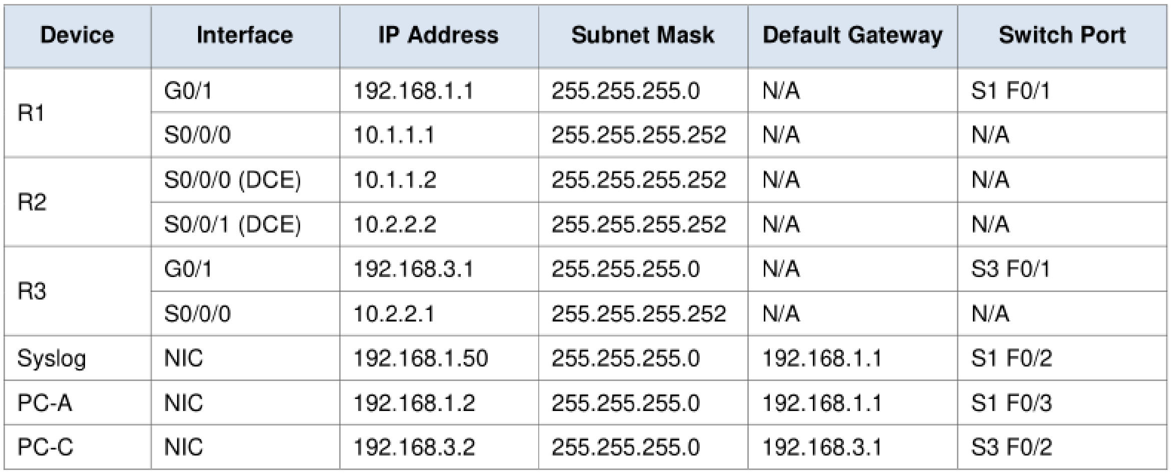
2.1 Network Topology & Addressing

In implementing our project, we used two hosts, PC-A and PC-C, three (3) routers R1, R2 and R3, two switches and a Server where our logs were being stored.

Topology



Addressing Table



Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/1
	S0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
Syslog	NIC	192.168.1.50	255.255.255.0	192.168.1.1	S1 F0/2
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1	S1 F0/3
PC-C	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/2

2.2 Network Scenario

The network is designed as a linear, multi-site topology consisting of three primary routing nodes and two Local Area Network (LAN) segments.

Core Transit Node (R2): A Cisco 1941 Integrated Services Router (ISR) serves as the central hub of the network, simulating an ISP or a corporate WAN core. It provides a link between the two LANs

Security Edge Gateway (R1): This Cisco 1941 router serves as the primary enforcement point for the IPS. It connects the trusted internal LAN to the WAN core via a Serial 0/0/0 interface.

Remote Site Router (R3): This Cisco 1941 router facilitates connectivity for the untrusted remote segment.

Switching Infrastructure: Cisco 2950-24 switches (S1 and S3) are deployed at each site to provide Layer 2 connectivity for end-user devices and servers.

2.3 Logical Addressing and Segmentation

The network is partitioned into three distinct subnets to facilitate routing and security inspection:

The Trusted Internal LAN (192.168.1.0/24): This segment is protected by the IPS on R1. It contains assumed high-value assets including PC-A and the centralized Syslog Server.

The WAN Core Segments: High-efficiency point-to-point subnets are used for inter-router communication, specifically the 10.1.1.0/30 network (R1-R2) and the 10.2.2.0/30 network (R2-R3).

The Remote Untrusted LAN (192.168.3.0/24): This segment houses PC-C and represents the external source of traffic that must be scrutinized by the security policy.

2.4 Management and Connectivity Requirements

For the IPS to function within this topology, several infrastructure prerequisites were met:

Dynamic Routing: End-to-end reachability across all five subnets is maintained via OSPF Process 101, ensuring that traffic from the untrusted zone can reach the trusted zone for inspection.

Logging Infrastructure: A dedicated Syslog Server at 192.168.1.50 is configured to receive real-time security alerts from the R1 IPS engine.

Temporal Synchronization: To ensure forensic accuracy in the logs, the system clock on R1 is synchronized, and the service timestamps log datetime msec command is enabled to provide millisecond-accurate event reporting.

2.5 Strategic IPS Placement Logic

The IPS rule, identified as iosips, is strategically applied to the GigabitEthernet 0/1 interface of R1. The rule is applied in the outbound direction. This specific placement ensures that any traffic arriving from the untrusted WAN (R3/R2) is inspected by the Cisco IOS security engine after the routing decision is made, but before the packets are delivered to the local hosts in the 192.168.1.0/24 network.

3. Configuration & Application of IPS

3.1 Configuration

Explain what the difference between an IPS is and an IDS (Intrusion Prevention System):

IPS (Intrusion Prevention System): IPS is a cybersecurity tool that mainly monitors network traffic or host as well as prevents suspicious and malicious intrusions proactively. An IPS is a proactive device designed to prevent attacks against network devices

IDS (Intrusion detection system): IDS also monitors traffic for threats or suspicious activities, and it also alerts if any of the suspicious activity got detected by any chance. The focus of IDS is to look for anomalies and to report. IDS works by looking for signs that looks unusual and also for attempts made by hackers. All the anomalies detected are then send in the upper stack in the system and they also pass through for credibility check via protocol and application layer. It can also explain the quantity and type of the attack. There are different types of IDS systems that are available. Network based, Host based, Signature based, and Anomaly based intrusion detection systems.

Difference between IDS and IPS
In a nutshell, IPS can configure to stop serious threats or more advanced suspicious activities without system administrator intervention. IPS are located between firewall and the rest of the network. False positives is one of its drawbacks. IDS just simply alerts the if it detects any suspicious activities, it is unable to block it without any intervention. IDS false positive is less harmful the IPS false positive because of their blocking capability on there own can block legitimate traffic as well. Organizations can use both for better security.

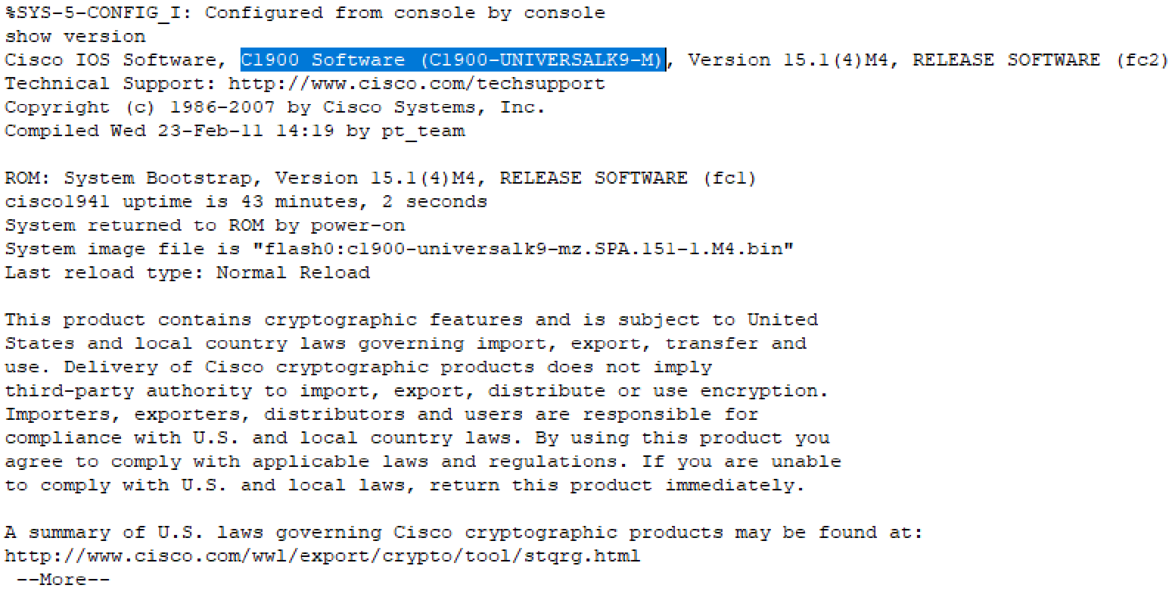
Do you think that an IPS and an IDS are using different signatures files to detect attacks? Explain why.
No, they both use same signature files to detect attacks. They use the same files because in the end they must detect the same suspicious threats and suspicious patterns in the network traffic. Those files have dictionary of known attacks, vulnerabilities, and suspicious patterns. The system operates in any of them IDS or IPS

the job remains the same. IDS operates as a detective it compares the traffic with a signature and if it's found anything unusual it reports and let rest of the traffic passes. However, IPS reports and block the traffic at the same time. It makes more sense to keep the same signature database for administrators rather to have two different ones. Modern systems can switch between these two, acting accordingly with the situation.

Part 1:

Step 1: Enable the Security Technology package.

A. On R1, issue the show version command to view the Technology Package license information. We have used the show version command and security package was already enabled below is the screenshot.

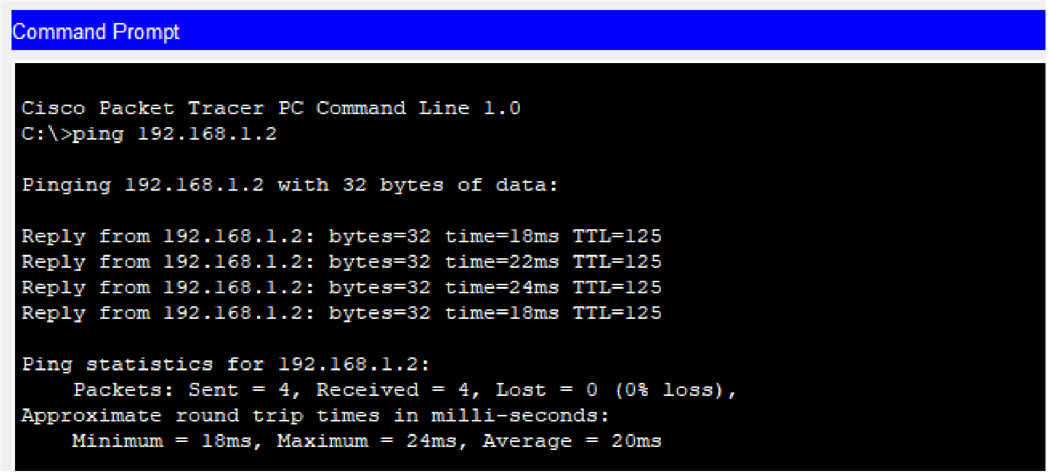


```
%SYS-5-CONFIG_I: Configured from console by console
show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 43 minutes, 2 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
 --More--
```

Step 2: Verify network connectivity.

C:\> ping 192.168.1.2

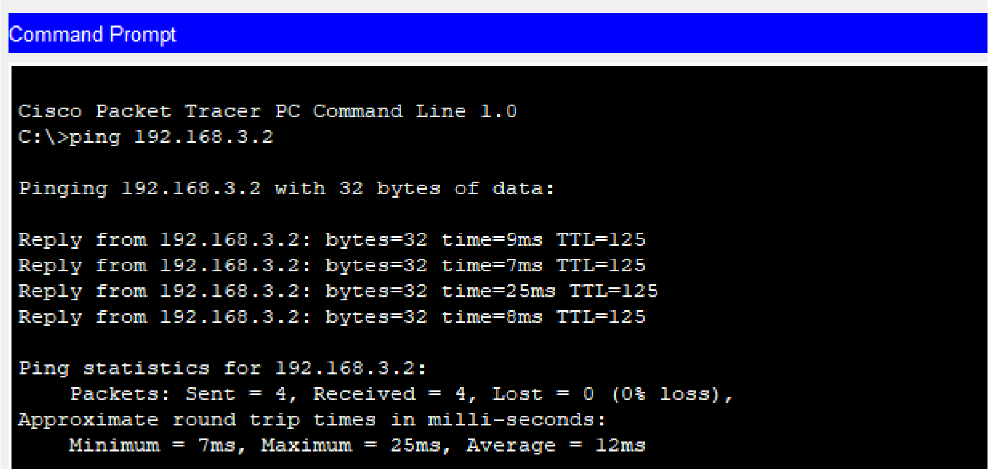
A. Ping from PC-C to PC-A. Ping from PC-C to PC-A is successful.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=18ms TTL=125
Reply from 192.168.1.2: bytes=32 time=22ms TTL=125
Reply from 192.168.1.2: bytes=32 time=24ms TTL=125
Reply from 192.168.1.2: bytes=32 time=18ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 18ms, Maximum = 24ms, Average = 20ms
```

B. Ping from PC-A to PC-C.

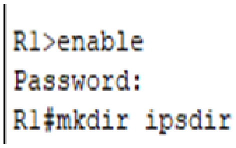
C:\> 192.168.3.2
Ping from PC-A to PC-C is successful.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=9ms TTL=125
Reply from 192.168.3.2: bytes=32 time=7ms TTL=125
Reply from 192.168.3.2: bytes=32 time=25ms TTL=125
Reply from 192.168.3.2: bytes=32 time=8ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 25ms, Average = 12ms
```

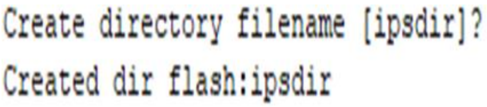
Step 3: Create an IOS IPS configuration directory in flash.

On R1, create a directory in flash using the mkdir command. Name the directory ipsdir.



```
R1>enable
Password:
R1#mkdir ipsdir
```

Create directory filename [ipsdir]? Created dir flash: ipsdir



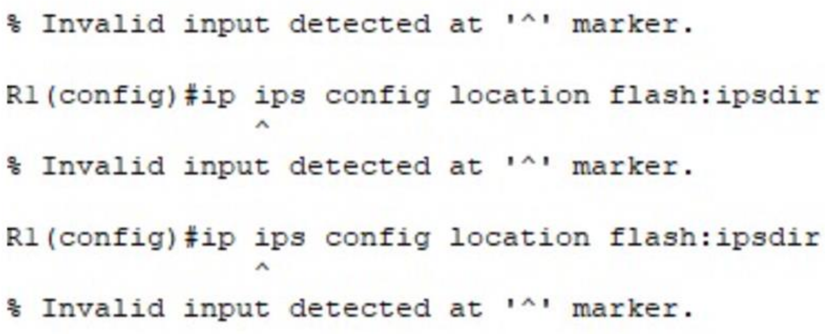
```
Create directory filename [ipsdir]?
Created dir flash:ipsdir
```

We have created the directory ipsdir by following the instructions given in the lab.

Step 4: Configure the IPS signature storage location.

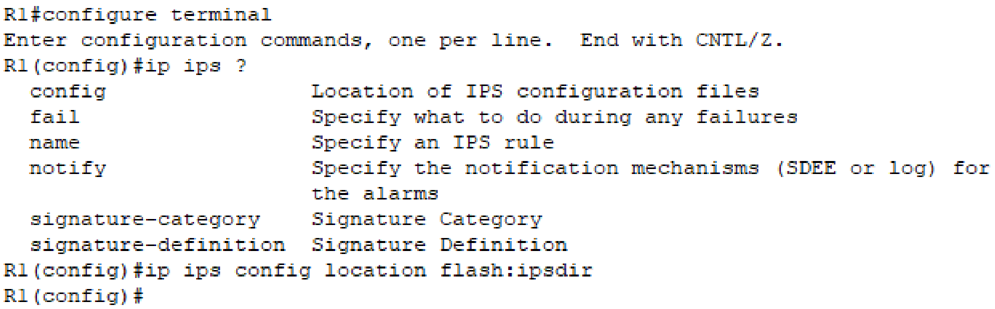
There was a trouble doing this step because IOS and IPS was not enable. Security Technology package was not loaded and not activated so it was showing the following errors mentioned below.

Configure terminal
 ip ips config location flash:ipsdir



```
% Invalid input detected at '^' marker.

R1(config)#ip ips config location flash:ipsdir
              ^
% Invalid input detected at '^' marker.

R1(config)#ip ips config location flash:ipsdir
              ^
% Invalid input detected at '^' marker.
```

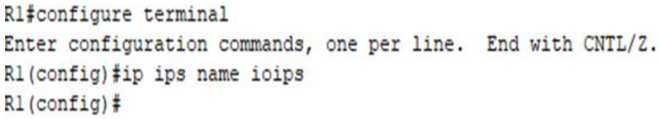
Once the issue being resolved IOS and IPS are working now perfectly.



```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip ips ?
  config                  Location of IPS configuration files
  fail                    Specify what to do during any failures
  name                    Specify an IPS rule
  notify                  Specify the notification mechanisms (SDEE or log) for
                          the alarms
  signature-category      Signature Category
  signature-definition    Signature Definition
R1(config)#ip ips config location flash:ipsdir
R1(config)#
```

Step 5: Create an IPS rule.

IPS rule is created by following the commands given. And, below is the output.
 ip ips name iosips

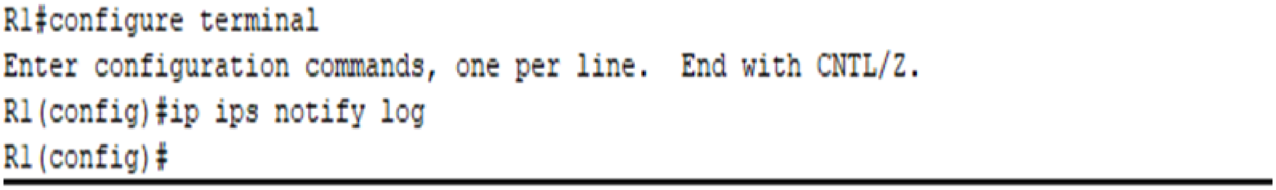


```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip ips name ioips
R1(config)#
```

Step 6: Enable logging.

Enable syslog if it is not enabled.

IPS logging was enabled successfully to send alerts.

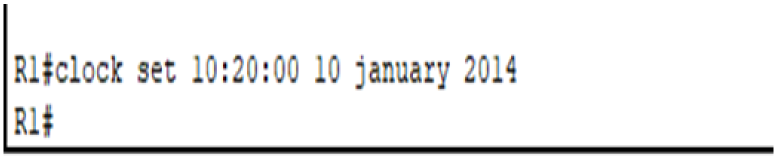


```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip ips notify log
R1(config)#
```

If necessary, use the clock set command from privileged EXEC mode to reset the clock.

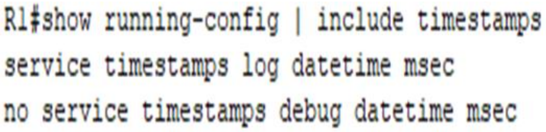
Clock is set to the given time as mentioned in the instructions to ensure

timestamps without errors.



```
R1#clock set 10:20:00 10 january 2014
R1#
```

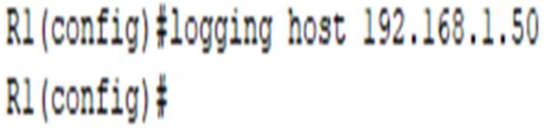
Verify that the timestamp service for logging is enabled on the router using the show run command. Enable the timestamp service if it is not enabled.
The timestamp service was not enabled. We have enabled the service and verified the configuration again.
service timestamps log datetime msec



```
R1#show running-config | include timestamps
service timestamps log datetime msec
no service timestamps debug datetime msec
```

Send log messages to the syslog server at IP address 192.168.1.50.

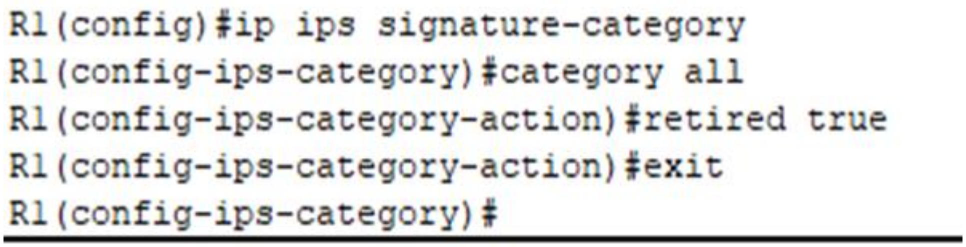
The router was configured successfully.
logging host 192.168.1.50



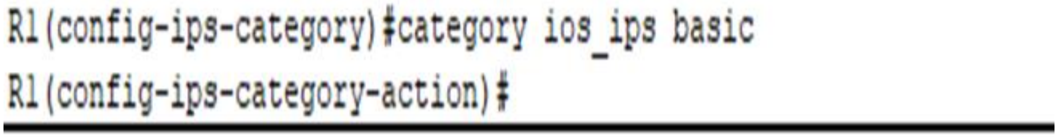
```
R1(config)#logging host 192.168.1.50
R1(config)#
```

Step 7: Configure IOS IPS to use the signature categories.

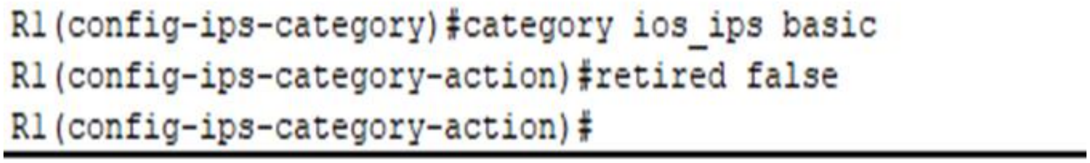
Firstly, all previous IPS signatures were retired and then the basic signature category of IOS IPS was enabled. The purpose to enable is to detect important intrusions and to reduce unnecessary alerts at the same time. All the commands and results are shown in the screenshots below.



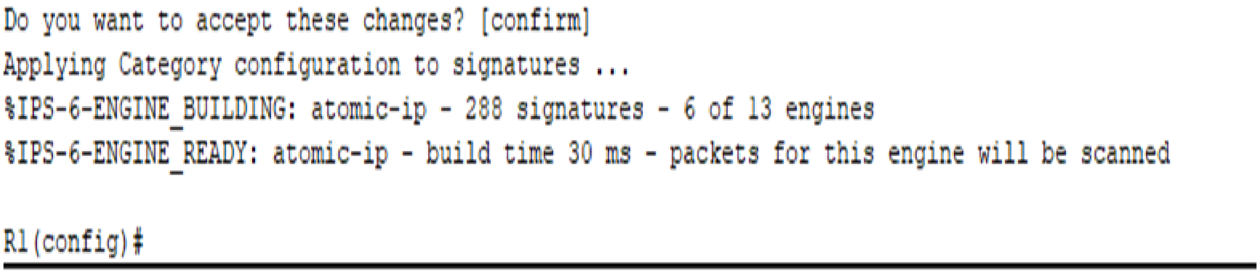
```
R1(config)#ip ips signature-category
R1(config-ips-category)#category all
R1(config-ips-category-action)#retired true
R1(config-ips-category-action)#exit
R1(config-ips-category)#
```



```
R1(config-ips-category)#category ios_ips basic
R1(config-ips-category-action)#
```



```
R1(config-ips-category)#category ios_ips basic
R1(config-ips-category-action)#retired false
R1(config-ips-category-action)#
```

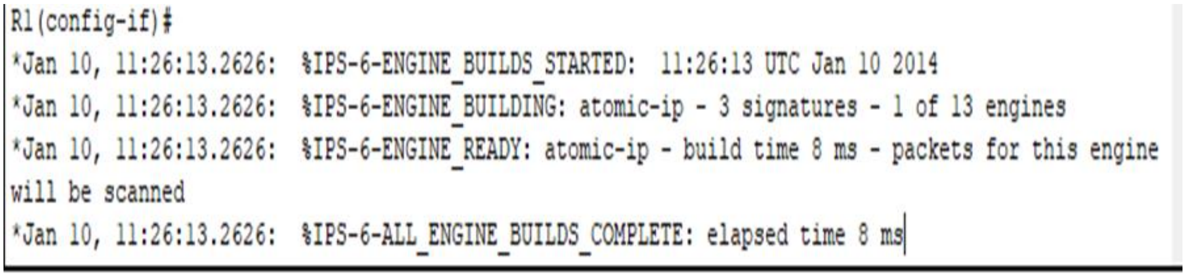


```
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine will be scanned

R1(config)#
```

Step 8: Apply the IPS rule to an interface.

As been told in the instruction all commands are successfully completed and below is the screenshot.

Interface g0/1
ip ips iosips out



```
R1(config-if)#
*Jan 10, 11:26:13.2626:  %IPS-6-ENGINE_BUILDS_STARTED:  11:26:13 UTC Jan 10 2014
*Jan 10, 11:26:13.2626:  %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
*Jan 10, 11:26:13.2626:  %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine
will be scanned
*Jan 10, 11:26:13.2626:  %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
```

3.2 Application of IPS

Part 2: Modify the signature

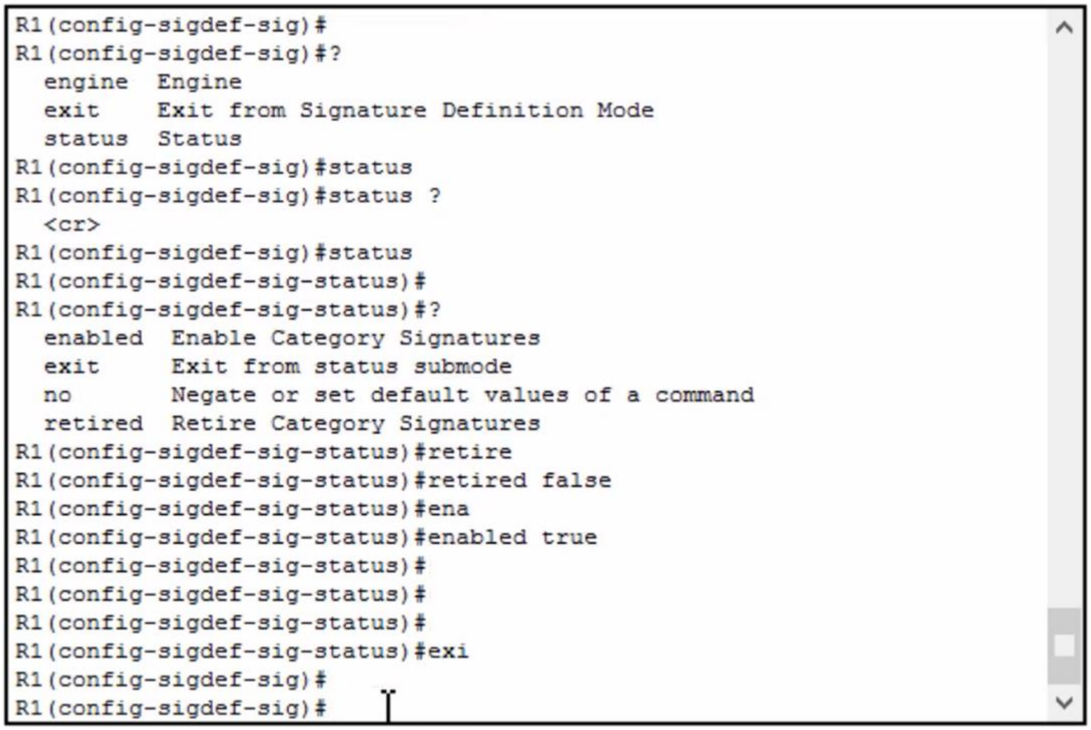
Step 1: Change the event-action of a signature. We activated signature 2004 to demonstrate advanced thereat mitigation. This required to switch the signature form from retired (stored in flash) to unretired (active in RAM) allowing scanning engines to process real-time traffic.

Question:

- What is the protocol that uses Echo Request packets? You can mention the usual command used for that.

Answer:

-The protocol is ICMP (internet Control Message Protocol), and the standard diagnostic command used is ping.



```
R1(config-sigdef-sig)#
R1(config-sigdef-sig)#?
  engine  Engine
  exit    Exit from Signature Definition Mode
  status  Status
R1(config-sigdef-sig)#status
R1(config-sigdef-sig)#status ?
  <cr>
R1(config-sigdef-sig)#status
R1(config-sigdef-sig-status)#
R1(config-sigdef-sig-status)#?
  enabled  Enable Category Signatures
  exit     Exit from status submode
  no       Negate or set default values of a command
  retired  Retire Category Signatures
R1(config-sigdef-sig-status)#retire
R1(config-sigdef-sig-status)#retired false
R1(config-sigdef-sig-status)#ena
R1(config-sigdef-sig-status)#enabled true
R1(config-sigdef-sig-status)#
R1(config-sigdef-sig-status)#
R1(config-sigdef-sig-status)#
R1(config-sigdef-sig-status)#exi
R1(config-sigdef-sig)#
R1(config-sigdef-sig)#
```

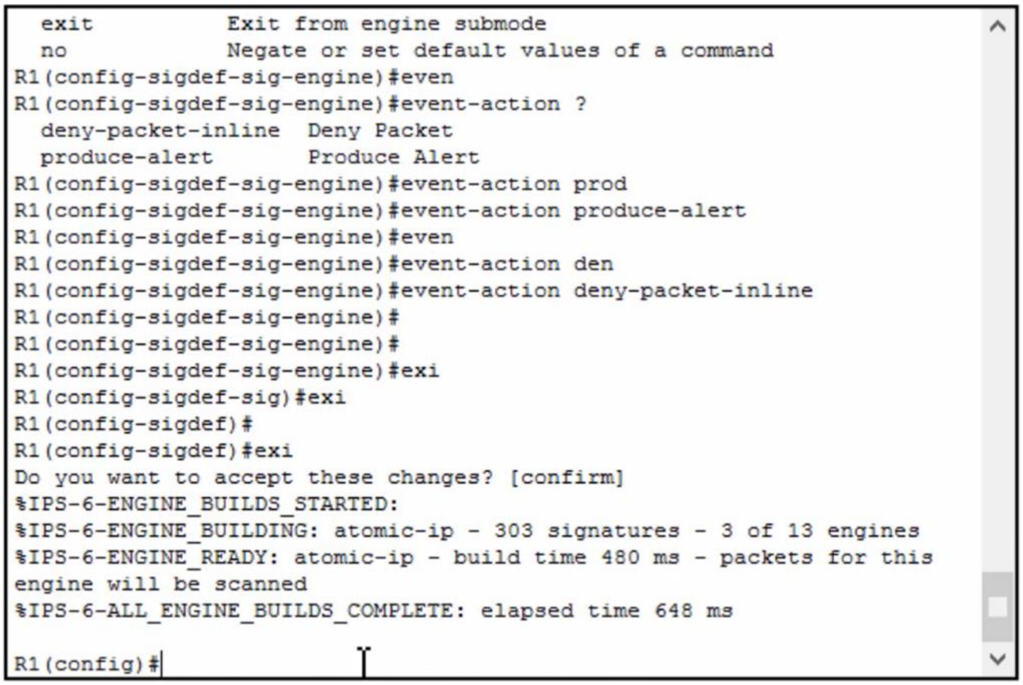
Step 2: Use show commands to verify IPS. Verification of the IPS policy is essential to ensure the engine has successfully compiled the new signature rules.

Question:

-To which interfaces and in which direction is the iosips rule applied?

Answer:

-Based on the configuration, iosips rule is applied to interface Gigabit Ethernet in the outbound direction.



```
  exit          Exit from engine submode
  no            Negate or set default values of a command
R1(config-sigdef-sig-engine)#even
R1(config-sigdef-sig-engine)#event-action ?
  deny-packet-inline  Deny Packet
  produce-alert       Produce Alert
R1(config-sigdef-sig-engine)#event-action prod
R1(config-sigdef-sig-engine)#event-action produce-alert
R1(config-sigdef-sig-engine)#even
R1(config-sigdef-sig-engine)#event-action den
R1(config-sigdef-sig-engine)#event-action deny-packet-inline
R1(config-sigdef-sig-engine)#
R1(config-sigdef-sig-engine)#
R1(config-sigdef-sig-engine)#exi
R1(config-sigdef-sig)#exi
R1(config-sigdef)#
R1(config-sigdef)#exi
Do you want to accept these changes? [confirm]
%IPS-6-ENGINE_BUILDS_STARTED:
%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets for this
engine will be scanned
%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 648 ms

R1(config)#
```

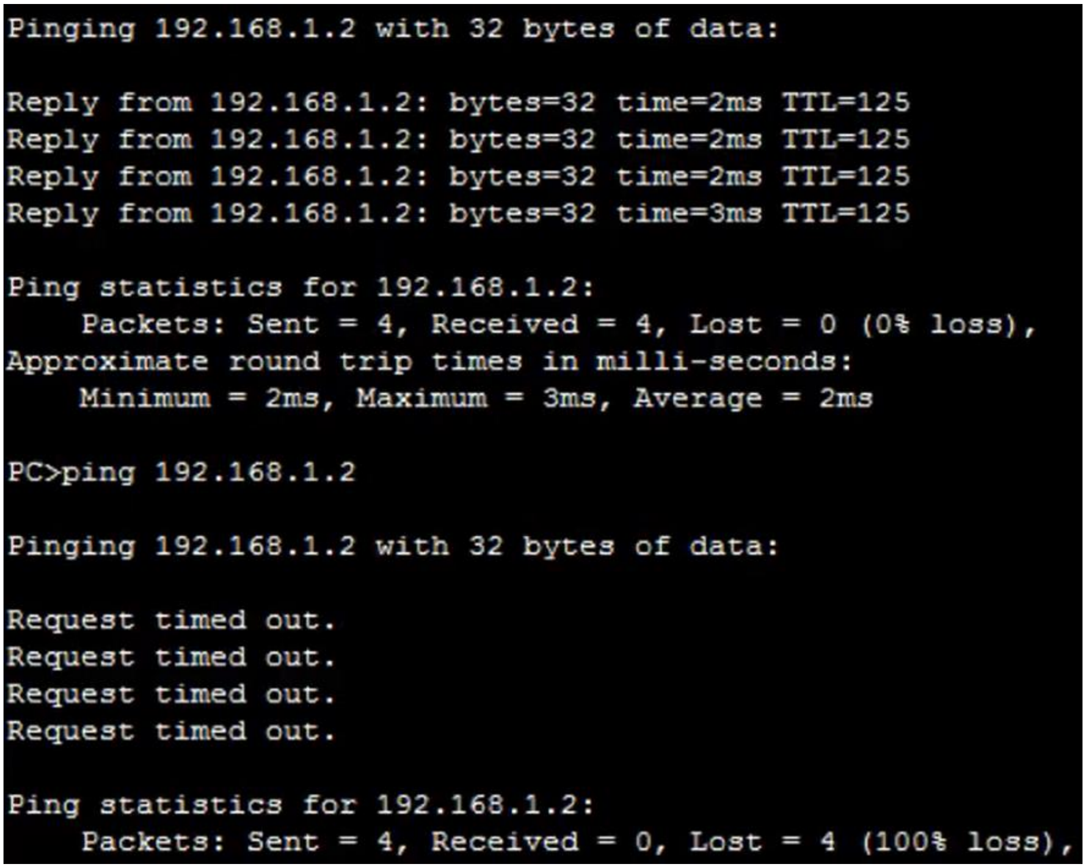
Step 3: IPS working verification. We made connectivity tests from PC-C and PC-A, to validate the Signature Event Action Processor (SEAP).

-PC-C, attempt to ping PC-A.

Ping was unsuccessful, because R1 identified ICMP traffic as a match for signature 2004 and dropped all packets.

-PC-A, attempt to ping PC-C

Ping was unsuccessful, the IPS engine on the R1 interface blocked the echo request as they tried to leave the gateway, causing request to time out.



```
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

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

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

The produce-alert action makes blocked threats administratively visible.

Observation:

The syslog server (192.168.1.2) recorded IPS-4-Signature: sig:2004 subsig:0, including the timestamp and source and destination information for the blocked attack.

Step 5: Result checking

Final status: The configuration has been confirmed.

4. Conclusion

This project was to simulate and test a network-based IPS on CISCO router (R1). On the router, we set up real-time network traffic monitoring to protect an “trusted” internal network from any potential external threat. By using a signature-based approach, we made the system capable of recognizing known malicious signatures for such unauthorized communication events. The configuration was confirmed by testing that the system would automatically block and log (and therefore avoid human intervention) of inappropriate activity, in response to malicious traffic (specifically ICMP ping requests).

The Importance of IPS in the Digital Era When you look at the current digital environment, traditional security tools that include basic firewalls no longer cut it, as they also only tend to "read" labels (or headers) of data packets and not really analyze their contents. With the increasing complexity of cyber-attacks that focus on indirect access to critical information, a strong offense is necessary. An IPS is vital because it:

- **Proactive:** While detection systems tell you an attack is happening, an IPS. PREVENTS attacks in real-time before they reach their intended victim.
- **Goes Beyond the Surface:** It examines data payload more extensively to identify clandestine threats other implementations fail to detect.
- **Secure at Scale:** Automatically block malicious traffic automatically without added burden on IT personnel.
- **Adjusts to the Evolution of Threats:** It keeps up with new cyber-threat and eliminates them using current signature databases and anomaly detection.

REFERENCES

https://www.splunk.com/en_us/blog/learn/ips-intrusion-prevention-systems.html

https://www.ibm.com/think/topics/intrusion-prevention-system

https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/ips-vs-firewall-differences/

https://www.networkacademy.io/ccna/network-fundamentals/firewalls

https://serverfault.com/questions/792572/what-does-a-layer-3-4-firewall-do-that-a-layer-7-does-not

https://www.stamus-networks.com/ids-detection-types

https://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-4/user/guide/CSMUserGuide_wrapper/ipsios.pdf

https://powerdmarc.com/what-is-ips/

www.zenarmor.com/docs/network-security-tutorials/what-is-ips

E. Carter and J. Hogue, *Intrusion Prevention Fundamentals: An Introduction to Network Attack Mitigation with IPS*. Cisco Press, n.d.