CHAPTER 5

Implementing Intrusion Prevention

5.0 Introduction

5.0.1.1 Implementing Intrusion Prevention

The security challenges that face today's network administrators cannot be successfully managed by any single application. Although implementing device hardening, authentication, authorization, and accounting (AAA) access control, and firewall features are all part of a properly secured network, these features still cannot defend the network against fast-moving Internet worms and viruses. A network must be able to instantly recognize and mitigate worm and virus threats.

It is no longer possible to contain intrusions at a few points in the network. Intrusion prevention is required throughout the entire network to sucessfully detect and stop an attack at every inbound and outbound point.

A networking architecture paradigm shift is required to defend against fast-moving and evolving attacks. This must include cost-effective detection and prevention systems, such as intrusion detection systems (IDS) or the more scalable intrusion prevention systems (IPS). The network architecture integrates these solutions into the entry and exit points of the network.

When implementing IDS or IPS, it is important to be familiar with the types of systems available, host-based and network-based approaches, the placement of these systems, the role of signature categories, and possible actions that a Cisco IOS router can take when an attack is detected.

Refer to Online Course for Illustration

5.1 IPS Technologies

5.1.1 IDS and IPS Characteristics

5.1.1.1 Zero-Day Attacks

Internet worms and viruses can spread across the world in a matter of minutes. A network must instantly recognize and mitigate worm and virus threats. Firewalls can only do so much and cannot protect against malware and zero-day attacks.

A zero-day attack, sometimes referred to as a zero-day threat, is a computer attack that tries to exploit software vulnerabilities that are unknown or undisclosed by the software vendor, as shown in Figure 1. The term zero-hour describes the moment when the exploit is discovered. During the time it takes the software vendor to develop and release a patch, the network is vulnerable to these exploits, as shown in Figure 2. Defending against these fast-moving attacks

requires network security professionals to adopt a more sophisticated view of the network architecture. It is no longer possible to contain intrusions at a few points in the network.

Refer to Online Course for Illustration

5.1.1.2 Monitor for Attacks

One approach to prevent worms and viruses from entering a network is for an administrator to continuously monitor the network and analyze the log files generated by the network devices. This solution is not very scalable. Manually analyzing log file information is a time-consuming task and provides a limited view of the attacks being launched against a network. By the time the logs are analyzed, the attack may have already been successful.

Intrusion Detection Systems (IDSs) were implemented to passively monitor the traffic on a network. The figure shows that an IDS-enabled device copies the traffic stream and analyzes the copied traffic rather than the actual forwarded packets. Working offline, it compares the captured traffic stream with known malicious signatures, similar to software that checks for viruses. Working offline means several things:

- IDS works passively
- IDS device is physically positioned in the network so that traffic must be mirrored in order to reach it
- Network traffic does not pass through the IDS unless it is mirrored

Although the traffic is monitored and perhaps reported, no action is taken on packets by the IDS. This offline IDS implementation is referred to as promiscuous mode.

The advantage of operating with a copy of the traffic is that the IDS does not negatively affect the packet flow of the forwarded traffic. The disadvantage of operating on a copy of the traffic is that the IDS cannot stop malicious single-packet attacks from reaching the target before responding to the attack. An IDS often requires assistance from other networking devices, such as routers and firewalls, to respond to an attack.

A better solution is to use a device that can immediately detect and stop an attack. An Intrusion Prevention System (IPS) performs this function.

Refer to Online Course for Illustration

5.1.1.3 Detect and Stop Attacks

An IPS builds upon IDS technology. However, an IPS device is implemented in inline mode. This means that all ingress and egress traffic must flow through it for processing. As shown in the figure, an IPS does not allow packets to enter the trusted side of the network without first being analyzed. It can detect and immediately address a network problem.

An IPS monitors Layer 3 and Layer 4 traffic. It analyzes the contents and the payload of the packets for more sophisticated embedded attacks that might include malicious data at Layers 2 to 7. Cisco IPS platforms use a blend of detection technologies, including signature-based, profile-based, and protocol analysis-based intrusion detection. This deeper analysis enables the IPS to identify, stop, and block attacks that would pass through a traditional firewall device. When a packet comes in through an interface on an IPS, that packet is not sent to the outbound or trusted interface until the packet has been analyzed.

The advantage of operating in inline mode is that the IPS can stop single-packet attacks from reaching the target system. The disadvantage is that a poorly configured IPS, or a non-proportional IPS solution, can negatively affect the packet flow of the forwarded traffic.

The biggest difference between IDS and IPS is that an IPS responds immediately and does not allow any malicious traffic to pass, whereas an IDS allows malicious traffic to pass before it is addressed.

Refer to Online Course for Illustration

5.1.1.4 Similarities Between IDS and IPS

IDS and IPS technologies share several characteristics, as shown in the figure. IDS and IPS technologies are both deployed as sensors. An IDS or IPS sensor can be in the form of several different devices:

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

IDS and IPS technologies use signatures to detect patterns in network traffic. A signature is a set of rules that an IDS or IPS uses to detect malicious activity. Signatures can be used to detect severe breaches of security, to detect common network attacks, and to gather information. IDS and IPS technologies can detect atomic signature patterns (single-packet) or composite signature patterns (multi-packet).

Refer to Online Course for Illustration

5.1.1.5 Advantages and Disadvantages of IDS and IPS

IDS Advantages and Disadvantages

A list of the advantages and disadvantages of IDS and IPS is shown in the figure.

A primary advantage of an IDS platform is that it is deployed in offline mode. Since the IDS sensor is not inline, it has no impact on network performance. It does not introduce latency, jitter, or other traffic flow issues. In addition, if a sensor fails it does not affect network functionality. It only affects the ability of the IDS to analyze the data.

However, there are many disadvantages of deploying an IDS platform. An IDS sensor is primarily focused on identifying possible incidents, logging information about the incidents, and reporting the incidents. The IDS sensor cannot stop the trigger packet and is not guaranteed to stop a connection. The trigger packet alerts the IDS to a potential threat. IDS sensors are also less helpful in stopping email viruses and automated attacks, such as worms.

Users deploying IDS sensor response actions must have a well-designed security policy and a good operational understanding of their IDS deployments. Users must spend time tuning IDS sensors to achieve expected levels of intrusion detection.

Finally, because IDS sensors are not inline, an IDS implementation is more vulnerable to network security evasion techniques in the form of various network attack methods.

IPS Advantages and Disadvantages

An IPS sensor can be configured to perform a packet drop to stop the trigger packet, the packets associated with a connection, or packets from a source IP address. Additionally, because IPS sensors are inline, they can use stream normalization. Stream normalization is a technique used to reconstruct the data stream when the attack occurs over multiple data segments.

A disadvantage of IPS is that (because it is deployed inline) errors, failure, and overwhelming the IPS sensor with too much traffic can have a negative effect on network

performance. An IPS sensor can affect network performance by introducing latency and jitter. An IPS sensor must be appropriately sized and implemented so that time-sensitive applications, such as VoIP, are not adversely affected.

Deployment Considerations

Using one of these technologies does not negate the use of the other. In fact, IDS and IPS technologies can complement each other. For example, an IDS can be implemented to validate IPS operation because the IDS can be configured for deeper packet inspection offline. This allows the IPS to focus on fewer but more critical traffic patterns inline.

Deciding which implementation to use is based on the security goals of the organization as stated in their network security policy.

Refer to Interactive Graphic in online course

5.1.1.6 Activity - Compare IDS and IPS Characteristics

Refer to Online Course for Illustration

5.1.2 Network-Based IPS Implementations

5.1.2.1 Host-Based IPS

There are two primary kinds of IPSs available: host-based and network-based.

Host-based IPS (HIPS) is software installed on a single host to monitor and analyze suspicious activity. A significant advantage of HIPS is that it can monitor and protect operating system and critical system processes that are specific to that host. With detailed knowledge of the operating system, HIPS can monitor abnormal activity and prevent the host from executing commands that do not match typical behavior. This suspicious or malicious behavior might include unauthorized registry updates, changes to the system directory, executing installation programs, and activities that cause buffer overflows. Network traffic can also be monitored to prevent the host from participating in a denial-of-service (DoS) attack or being part of an illicit FTP session.

HIPS can be thought of as a combination of antivirus software, antimalware software, and firewall. Combined with a network-based IPS, HIPS is an effective tool in providing additional protection for the host.

A disadvantage of HIPS is that it operates only at a local level. It does not have a complete view of the network, or coordinated events that might be happening across the network. To be effective in a network, HIPS must be installed on every host and have support for every operating system.

Refer to Online Course for Illustration

5.1.2.2 Network-Based IPS Sensors

A network-based IPS can be implemented using a dedicated or non-dedicated IPS device. Network-based IPS implementations are a critical component of intrusion prevention. There are host-based IDS/IPS solutions, but these must be integrated with a network-based IPS implementation to ensure a robust security architecture.

Sensors detect malicious and unauthorized activity in real time and can take action when required. Sensors are deployed at designated network points that enable security managers to monitor network activity while it is occurring, regardless of the location of the attack target.

Sensors can be implemented in several ways:

- On an ISR router with or without an IPS Advanced Integration Module (AIM), or an IPS Network Module Enhanced (NME)
- On an ASA firewall device with or without an ASA Advanced Inspection and Prevention Security Services Module (AIP-SSM)
- Added to a Catalyst 6500 switch using an Intrusion Detection System Services Module (IDSM-2)
- As a standalone device, such as a Cisco IPS 4300 Series Sensor

Network-based IPS sensors are usually tuned for intrusion prevention analysis. The underlying operating system of the platform on which the IPS module is mounted is stripped of unnecessary network services, and essential services are secured. This is known as hardening. The hardware includes three components:

- **NIC** - The network-based IPS must be able to connect to any network, such as Ethernet, Fast Ethernet, and Gigabit Ethernet.
- **Processor** - Intrusion prevention requires CPU power to perform intrusion detection analysis and pattern matching.
- **Memory** - Intrusion detection analysis is memory-intensive. Memory directly affects the ability of a network-based IPS to efficiently and accurately detect an attack.

Network-based IPS gives security managers real-time security insight into their networks regardless of growth. Additional hosts can be added to protected networks without requiring more sensors. Additional sensors are only required when their rated traffic capacity is exceeded, when their performance does not meet current needs, or when a revision in security policy or network design requires additional sensors to help enforce security boundaries. When new networks are added, additional sensors are easy to deploy. The figure shows an example IPS sensor deployment.

Refer to Online Course for Illustration

5.1.2.3 Cisco's Modular and Appliance-Based IPS Solutions

Cisco 1900, 2900, and 3900 ISR G2s can be configured, using command-line interface (CLI) to support IPS features using Cisco IOS IPS. The Cisco IOS IPS is part of the Cisco IOS Security Technology Package. This does not require the installation of an IPS module but does require downloading signature files and adequate memory to load the signatures. However, this deployment should be limited to a small organization with limited traffic patterns.

For larger volumes of traffic, Cisco IPS sensors can be implemented using standalone appliances or as modules added to network devices.

In addition to Cisco IOS IPS, Cisco offers a variety of modular and appliance-based IPS solutions:

- **Cisco IPS Advanced Integration Module and Network Module Enhanced** - Integrates IPS onto a Cisco ISR and is used for small and medium-sized business (SMB) and branch office environments to provide advanced IPS functions, as shown in Figure 1.

- **Cisco IPS Advanced Inspection and Prevention Security Services Module and Security Services Card** - Enhances IPS capabilities for Cisco ASA 5500 Series Adaptive Security Appliances. Figure 2 displays an AIP SSM-10 for Cisco ASA 5510 and 5520 models. The AIP SSC-5 is designed specifically for the Cisco ASA 5505.
- **Cisco ASA 5500-X Series and Cisco IPS Security Services Processor for the ASA 5585-X** - With the small office and branch office version of the Cisco ASA 5500-X Series extra hardware is not required for optimal IPS performance.
- **Cisco IPS 4300 and 4500 Series Sensors** - Combines inline IPS services with innovative technologies that improve accuracy in detecting, classifying, and stopping threats including worms, spyware, adware, and network viruses, as shown in Figure 3. As a result, more threats can be stopped without the risk of dropping legitimate network traffic.
- **Cisco Catalyst 6500 Series Intrusion Detection System Services Module** - As part of the Cisco IPS solution, it works in combination with the other components to efficiently protect the data infrastructure, as shown in Figure 4.

Refer to **Video** in online course

5.1.2.4 Cisco's Modular and Appliance-Based IPS Solutions (Cont.)

Cisco offers other modular and appliance-based solutions:

- **Cisco ASA 5500-X Series Next-Generation Firewalls** - Includes Cisco Application Visibility and Control (AVC), Web Security Essentials (WSE), and IPS. It is a stateful inspection firewall with next-generation firewall capabilities. It has network-based security controls for end-to-end network intelligence and streamlined security operations. Click Play in the figure to view a video about Cisco ASA 5500 X Series Next Generation Firewalls.
- **Cisco ASA with FirePOWER Services** – Brings an adaptive, threat-focused, next-generation security services to the ASA 5500-X Series and ASA 5585-X firewall products. The Cisco ASA with FirePOWER Services delivers integrated threat defense before, during, and after an attack. It combines the ASA firewall with Sourcefire threat and advanced malware protection in a single device. The Cisco ASA with FirePOWER Services provides comprehensive protection from known and advanced threats, including protection against targeted and persistent malware attacks.

Click here to read the transcript of this video.

Refer to **Video** in online course

5.1.2.5 Choose an IPS Solution

The choice of a sensor varies depending on the requirements of the organization. There are several factors that affect the IPS sensor selection and deployment:

- Amount of network traffic
- Network topology
- Security budget
- Available security staff to manage IPS

Small implementations such as branch offices might only require a Cisco IOS IPS-enabled ISR router. As traffic patterns increase, the ISR can be configured to offload IPS functions using an IPS NME or IPS AIM.

Larger installations can be deployed using an existing ASA 5500-X appliance.

Enterprises and service providers might require a dedicated IPS appliance or a Catalyst 6500 using an IDSM-2 network module.

Click Play in the figure to view the video about the fundamentals of an IPS.

Click here to read the transcript of this video.

Refer to Online Course for Illustration

5.1.2.6 Network-Based IPS

Network-based IPS has several advantages and disadvantages, as shown in the figure.

One advantage is that a network-based monitoring system can easily see attacks that are occurring across the entire network. This provides a clear indication of the extent to which the network is being attacked. In addition, because the monitoring system is examining traffic only from the network, it does not have to support every type of operating system that is used on the network.

There are also disadvantages to network-based IPS. If network data is encrypted, this can essentially blind network-based IPS, allowing attacks to go undetected. Another problem is that IPS has a difficult time reconstructing fragmented traffic for monitoring purposes. Finally, as networks grow in terms of bandwidth utilization, it becomes more difficult to place a network-based IPS device at a single location and successfully capture all traffic. Eliminating this problem requires using more sensors throughout the network, which increases costs.

Refer to Online Course for Illustration

5.1.2.7 Modes of Deployment

Cisco IDS and IPS sensors can operate in inline mode (also known as inline interface pair mode) or promiscuous mode (also known as passive mode).

As shown in Figure 1, packets do not flow through the sensor in promiscuous mode. The sensor analyzes a copy of the monitored traffic, not the actual forwarded packet. The advantage of operating in promiscuous mode is that the sensor does not affect the packet flow with the forwarded traffic. The disadvantage of operating in promiscuous mode is that the sensor cannot stop malicious traffic from reaching its intended target for certain types of attacks, such as atomic attacks (single-packet attacks). The response actions implemented by promiscuous sensor devices are post-event responses and often require assistance from other networking devices (for example, routers and firewalls) to respond to an attack. Such response actions can prevent some classes of attacks. However, in atomic attacks the single packet has the chance of reaching the target system before the promiscuous-based sensor can apply an ACL modification on a managed device (such as a firewall, switch, or router). In Figure 1, Switched Port Analyzer (SPAN) is used to mirror the traffic entering, going to, and coming from the host.

As shown in Figure 2, operating in inline mode puts the IPS directly into the traffic flow and makes packet-forwarding rates slower by adding latency. Inline mode allows the sensor to stop attacks by dropping malicious traffic before it reaches the intended target, thus providing a protective service. Not only is the inline device processing information on Layers 3 and 4, but it is also analyzing the contents and payload of the packets for more

sophisticated embedded attacks (Layers 3 to 7). This deeper analysis lets the system identify and stop or block attacks that would pass through a traditional firewall device. An IDS sensor could also be deployed inline. The IDS would be configured so that it only sends alerts and does not drop any packets.

Refer to Interactive Graphic in online course

5.1.2.8 Activity - Compare Network-Based and Host-Based IPS Devices

Refer to Online Course for Illustration

5.1.3 Cisco Switched Port Analyzer

5.1.3.1 Port Mirroring

A packet analyzer can be a valuable tool to help monitor and troubleshoot a network. The packet analyzer (also known as a packet sniffer or traffic sniffer) is typically software that captures packets entering and exiting the network interface card (NIC). It is not always possible or desirable to have the packet analyzer on the device that is being monitored. Sometimes it is better on a separate station designated to capture the packets.

When LANs were based on hubs, connecting a packet analyzer was simple, as shown in Figure 1. When a hub receives an Ethernet frame, the bits received on one port are sent out all other ports except the port that the frame came in on. The packet analyzer is simply connected to the hub and can receive all traffic connected to that hub.

Modern LANs are essentially switched networks. A Layer 2 switch populates its MAC address table, also known as a Layer 2 forwarding table, based on the source MAC address and the ingress port of the Ethernet frame. After this forwarding table is built, the switch forwards traffic destined for a MAC address directly to the corresponding port. This filtering prevents a packet analyzer, which is connected to another port, to receive the unicast traffic.

Port mirroring is a feature that allows a switch to make a duplicate copy of an incoming Ethernet frame, and then send it out a port with a packet analyzer attached for capture. The original frame is forwarded in the usual manner. An example of port mirroring is illustrated in Figure 2.

Refer to Online Course for Illustration

5.1.3.2 Cisco SPAN

The Switched Port Analyzer (SPAN) feature on Cisco switches sends copies of the frame entering a port, out another port on the same switch. A host running a packet analyzer or an IDS might be at the other end of that port.

SPAN terminology includes several specific items:

- Ingress traffic - Traffic that enters the switch.
- Egress traffic - Traffic that leaves the switch.
- Source (SPAN) port - A port that is monitored with use of the SPAN feature.
- Destination (SPAN) port - A port that monitors source ports, usually where a packet analyzer or IDS is connected.

The source port is a port that is monitored for traffic analysis. SPAN mirrors traffic that is received and/or sent on one or more source ports to a destination port for analysis. Layer 2 and Layer 3 ports can be configured as SPAN source ports. Traffic is copied to the destination (also called monitor) port. The figure shows the different types of SPAN ports.

The association between source ports and a destination port is called a SPAN session. In a single session, you can monitor one or multiple source ports. On some Cisco switches, you can copy session traffic to more than one destination port.

Alternatively you can specify a source VLAN in which all ports in the source VLAN become sources of SPAN traffic. Each SPAN session can have ports or VLANs as sources, but not both.

There are three important things to consider when configuring a SPAN:

- The destination port cannot be a source port, and the source port cannot be a destination port.
- The number of destination ports is platform-dependent. Some platforms allow for more than one destination port.

The destination port is no longer a normal switch port. Only monitored traffic passes through that port.

Refer to Online Course for Illustration

5.1.3.3 Configuring Cisco SPAN using Intrusion Detection

The SPAN feature on Cisco switches sends a copy of each frame entering the source port, out the destination port and toward the packet analyzer or IDS.

A session number is used to identify a SPAN session. Figure 1 shows the **monitor session** command, used to associate a source port and a destination port with a SPAN session. A separate **monitor session** command is used for each session. A VLAN can be specified instead of a physical port.

In Figure 2, PCA is connected to F0/1 and an IDS is connected to F0/2. The objective is to capture all the traffic that is sent or received by PCA on port F0/1 and send a copy of those frames to the IDS (or a packet analyzer) on port F0/2. The SPAN session on the switch will copy all the traffic that it sends and receives on source port F0/1 to the destination port F0/2.

The **show monitor** command is used to verify the SPAN session. The command displays the type of the session, the source ports for each traffic direction, and the destination port. In the example shown in Figure 3, the session number is 1, the source port for both traffic directions is F0/1, and the destination port is F0/2. The ingress SPAN is disabled on the destination port, so only traffic that leaves the destination port is copied to that port.

Use the Syntax Checker in Figure 4 to configure and verify SPAN.

Note Remote SPAN (RSPAN) can be used when the packet analyzer or IDS is on a different switch than the traffic being monitored. RSPAN extends SPAN by enabling remote monitoring of multiple switches across the network. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated (for that RSPAN session) in all participating switches.

Refer to Online Course for Illustration

5.2 IPS Signatures

5.2.1 IPS Signature Characteristics

5.2.1.1 Signature Attributes

The network must be able to identify incoming malicious traffic in order to stop it. Fortunately, malicious traffic displays distinct characteristics or "signatures". A signature is a set of rules that an IDS and an IPS use to detect typical intrusion activity, such as DoS attacks. These signatures uniquely identify specific worms, viruses, protocol anomalies, or malicious traffic, as shown in the figure. IPS sensors are tuned to look for matching signatures or abnormal traffic patterns. IPS signatures are conceptually similar to the virus.dat file used by virus scanners.

As sensors scan network packets, they use signatures to detect known attacks and respond with predefined actions. A malicious packet flow has a specific type of activity and signature. An IDS or IPS sensor examines the data flow using many different signatures. A sensor takes action when it matches a signature with a data flow, such as logging the event or sending an alarm to the IDS or IPS management software.

Signatures have three distinctive attributes:

- Type
- Trigger (alarm)
- Action

Refer to Online Course for Illustration

5.2.1.2 Signature Types

Signature types are generally categorized as atomic or composite.

Atomic Signature

An atomic signature is the simplest type of signature. It consists of a single packet, activity, or event that is examined to determine if it matches a configured signature. If it does, an alarm is triggered, and a signature action is performed. Because these signatures can be matched on a single event, they do not require an intrusion system to maintain state information. State refers to situations in which multiple packets of information are required, but the packets of information are not necessarily received at the same time. For example, if there was a requirement to maintain state, it would be necessary for the IDS or IPS to track the three-way handshake of established TCP connections. With atomic signatures, the entire inspection can be accomplished in an atomic operation that does not require any knowledge of past or future activities.

Detecting atomic signatures consumes minimal resources, such as memory, on the IPS or IDS device. These signatures are easy to identify and understand because they are compared to a specific event or packet. Traffic analysis for these atomic signatures can usually be performed very quickly and efficiently. For example, a LAND attack has an atomic signature because it sends a spoofed TCP SYN packet (connection initiation) with the same source and destination IP address of the target host and the same source and destination port as an open port on the target, as shown in the figure. The reason a LAND attack works is because it causes the machine to reply to itself continuously. One packet

is required to identify this type of attack. An IDS is particularly vulnerable to an atomic attack because malicious single packets are allowed into the network until it finds the attack. However, an IPS prevents these packets from entering the network altogether.

Composite Signature

A composite signature is also called a stateful signature. This type of signature identifies a sequence of operations distributed across multiple hosts over an arbitrary period of time. Unlike atomic signatures, the stateful properties of composite signatures usually require several pieces of data to match an attack signature, and an IPS device must maintain state. The length of time that the signatures must maintain state is known as the event horizon.

The length of an event horizon varies from one signature to the next. An IPS cannot maintain state information indefinitely without eventually running out of resources. Therefore, an IPS uses a configured event horizon to determine how long it will look for a specific attack signature when an initial signature component is detected. Configuring the length of the event horizon is a trade-off between consuming system resources and being able to detect an attack that occurs over an extended period of time.

Note The terms atomic and composite are analogous to the terms atom and compound used in chemistry.

Refer to Online Course for Illustration

5.2.1.3 Signature File

Network security threats are occurring more frequently and spreading more quickly. As new threats are identified, new signatures must be created and uploaded to an IPS. To make this process easier, all signatures are contained in a signature file and uploaded to an IPS on a regular basis.

The signature file contains a package of network signatures. These are intended as an update to the signature database resident in a Cisco product with IPS or IDS functions. This signature database is used by the IPS or IDS solution to compare network traffic against data patterns within the signature-file library. The IPS or IDS uses this comparison to detect suspected malicious network traffic behavior.

For example, the LAND attack is identified in the "Impossible IP Packet" signature (signature 1102.0). A signature file contains that signature and many more. Networks deploying the latest signature files are better protected against network intrusions. The figure displays a signature file being accessed from Cisco.com.

Automatic periodic retrieval of IPS signature updates from Cisco.com can be configured on an ISR G2 device after installing VeriSign SSL certificates on the device.

Refer to Online Course for Illustration

5.2.1.4 Signature Micro-Engines

To make the scanning of signatures more efficient, Cisco IOS software relies on signature micro-engines (SMEs), which categorize common signatures in groups. Cisco IOS software can then scan for multiple signatures based on group characteristics, instead of one at a time.

When IDS or IPS is enabled, an SME is loaded or built on the router. When an SME is built, the router might need to compile the regular expression found in a signature. A regular expression is a systematic way to specify a search for a pattern in a series of bytes.

The SME then looks for malicious activity in a specific protocol. Each engine defines a set of legal parameters with allowable ranges or sets of values for the protocols and the fields the engine inspects. Atomic and composite packets are scanned by the micro-engines that recognize the protocols contained in the packets. Signatures can be defined using the parameters offered by the SME.

Each SME extracts values from the packet and passes portions of the packet to the regular expression engine. The regular expression engine can search for multiple patterns at the same time.

The available SMEs vary depending on the platform, Cisco IOS version, and version of the signature file. Cisco IOS defines five micro-engines:

- **Atomic** - Signatures that examine simple packets, such as ICMP and UDP, as shown in Figure 1.
- **Service** - Signatures that examine the many services that are attacked, as shown in Figure 2.
- **String** - Signatures that use regular expression-based patterns to detect intrusions, as shown in Figure 3.
- **Multi-string** - Supports flexible pattern matching and Trend Labs signatures, as shown in Figure 3.
- **Other** - Internal engine that handles miscellaneous signatures, as shown in Figure 3.

SMEs are constantly being updated. For example, before Release 12.4(11)T, the Cisco IPS signature format used version 4.x. Since IOS 12.4(11)T, Cisco introduced version 5.x, which is an improved IPS signature format. The new version supports encrypted signature parameters and other features, such as signature risk rating, which rates the signature on security risk.

There are a few factors to consider when determining router requirements for maintaining signatures. 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 of signatures and engines that can be adequately supported depends on the memory available. For this reason, implement Cisco IOS IPS-enabled routers with the maximum amount of memory possible.

Refer to Online Course for Illustration

5.2.1.5 Acquire the Signature File

Cisco investigates and creates signatures for new threats and malicious behavior as they are discovered and publishes them regularly. Typically, lower priority IPS signature files are published biweekly. If the threat is severe, Cisco publishes signature files within hours of identification.

To protect a network, the signature file must be updated regularly. Each update includes new signatures and all of the signatures in the previous version. For example, signature file IOS-S855-CLI.pkg includes all signatures in file IOS-S854-CLI.pkg, plus signatures created for threats discovered subsequently.

Just as virus checkers must constantly update their virus database, network administrators must be vigilant and regularly update the IPS signature file. As shown in the figure, new

signatures are downloaded from cisco.com. A cisco.com account is required to retrieve signatures.

Note The automatic update option available for IPS signature definition files on ISR G2 routers saves time and ensures real-time threat defense.

Refer to Interactive Graphic in online course

5.2.1.6 Activity - Identify IPS Signature Type

Refer to Online Course for Illustration

5.2.2 IPS Signature Alarms

5.2.2.1 Signature Alarm

The heart of any IPS signature is the signature alarm, which is often referred to as the signature trigger. Consider a home security system. The triggering mechanism for a burglar alarm could be a motion detector that detects the movement of an individual entering a room protected by an alarm.

The signature trigger for an IPS sensor could be anything that can reliably signal an intrusion or security policy violation. A network-based IPS might trigger a signature action if it detects a packet with a payload containing a specific string going to a specific port. A host-based IPS might trigger a signature action when a specific function call is invoked. Anything that can reliably signal an intrusion or security policy violation can be used as a triggering mechanism.

Note A function call is an expression that passes control and arguments to a function.

Cisco IDS and IPS sensors, such as the Cisco IPS 4300 Series Sensors and Cisco Catalyst 6500 IDSM-2, can use four types of signature triggers:

- Pattern-based detection
- Anomaly-based detection
- Policy-based detection
- Honey pot-based detection

Figures 1 and 2 list the advantages and disadvantages of these four types of triggers.

These triggering mechanisms can be applied to atomic and composite signatures. The triggering mechanisms can be simple or complex. Every IPS incorporates signatures that use one or more of these basic triggering mechanisms to trigger signature actions.

Another common triggering mechanism is called protocol decodes. Instead of simply looking for a pattern anywhere in a packet, protocol decodes break down a packet into the fields of a protocol. Protocol decodes then search for specific patterns in a specific protocol field or some other malformed aspect of the protocol fields. The advantage of protocol decodes is that it enables a more granular inspection of traffic and reduces the number of false positives, such as traffic that generates an alert but is not a threat to the network.

Refer to Online Course for Illustration

5.2.2.2 Pattern-Based Detection

Pattern-based detection, also known as signature-based detection, is the simplest triggering mechanism. It searches for a specific and pre-defined pattern. A signature-based IDS or IPS sensor compares the network traffic to a database of known attacks, and triggers an alarm or prevents communication if a match is found. The figure provides examples of atomic signature and composite signature pattern-based attacks.

The signature trigger might be textual, binary, or a series of function calls. It can be detected in a single packet (atomic) or in a sequence of packets (composite). In most cases, the pattern is matched to the signature only if the suspect packet is associated with a particular service or destined to or from particular ports. This matching technique helps decrease the amount of inspection done on every packet. However, it makes it more difficult for systems to deal with protocols and attacks that do not use well-defined ports. For example, Trojan horses and their associated traffic can propagate indiscriminately.

At the initial stage of incorporating pattern-based IDS or IPS, before the signatures are tuned, there can be many false positives. After the system is tuned and adjusted to the specific network parameters, there are fewer false positives than with a policy-based approach.

Refer to Online Course for Illustration

5.2.2.3 Anomaly-Based Detection

Anomaly-based detection, also known as profile-based detection, involves first defining a profile of what is considered normal for the network or host. This normal profile can be learned by monitoring activity on the network or specific applications on the host over a period of time. It can also be based on a defined specification, such as an RFC. After defining normal activity, the signature triggers an action if excessive activity occurs beyond a specified threshold that is not included in the normal profile. Atomic signature and composite signature examples of anomaly-based attacks are described in the figure.

The advantage of anomaly-based detection is that new and previously unpublished attacks can be detected. Instead of having to define a large number of signatures for various attack scenarios, the administrator simply defines a profile for normal activity. Any activity that deviates from this profile is considered abnormal and triggers a signature action.

Despite this obvious advantage, several factors can make anomaly-based signatures hard to use. For example, an alert from an anomaly signature does not necessarily indicate an attack. It only indicates a deviation from the defined normal activity, which can sometimes occur as a result of valid user traffic. As the network evolves, the definition of normal usually changes, so the definition of normal must be redefined.

Another consideration is that the administrator must guarantee that the network is free of attack traffic during the learning phase. Otherwise, the attack activity will be considered normal traffic. Precautions should be taken to ensure that the network is free of attacks while establishing normal activity. However, it can be difficult to define normal traffic because most networks consist of a heterogeneous mixture of systems, devices, and applications that continually change.

When a signature generates an alert, it might be difficult to correlate that alert back to a specific attack because the alert indicates only that non-normal traffic has been detected. More analysis is required to determine whether the traffic represents an actual attack and what the attack actually accomplished. In addition, if the attack traffic happens to be similar to normal traffic, the attack might go undetected.

Refer to Online Course for Illustration

5.2.2.4 Policy-Based and Honey Pot-Based Detection

Policy-based detection, also known as behavior-based detection, is similar to pattern-based detection. However, instead of trying to define specific patterns, the administrator defines behaviors that are suspicious based on historical analysis. The figure lists examples of atomic signature and composite signature policy-based attacks.

The use of behaviors enables a single signature to cover an entire class of activities without having to specify each individual situation. For example, a signature that triggers an action when an email client invokes cmd.exe enables the administrator to apply the signature to any application whose behavior mimics the basic characteristics of an email client. The administrator will not have to apply the signature to each email client application individually. Therefore, if a user installs a new email application, the signature still applies.

Honey Pot-Based Detection

Honey pot-based detection uses a dummy server to attract attacks. The purpose of the honey pot approach is to distract attacks away from real network devices. By staging different types of vulnerabilities in the honey pot server, administrators can analyze incoming types of attacks and malicious traffic patterns. They can then use this analysis to tune their sensor signatures to detect new types of malicious network traffic. Honey pot systems are rarely used in production environments. Antivirus and other security vendors tend to use them for research.

Refer to Online Course for Illustration

5.2.2.5 Benefits of the Cisco IOS IPS Solution

Cisco has implemented IPS functions into its Cisco IOS software. Cisco IOS IPS uses technology from Cisco IDS and IPS sensor product lines, including the Cisco IPS 4300 Series Sensors and the Cisco Catalyst 6500 Series Intrusion Detection System Services Module. Cisco IPS 4300 models are shown in the figure.

There are many benefits to using the Cisco IOS IPS solution:

- It uses the underlying routing infrastructure to provide an additional layer of security.
- It is inline and is supported on a broad range of routing platforms. Attacks can be effectively mitigated by denying malicious traffic from both inside and outside the network.
- It provides threat protection at all entry points to the network when used in combination with Cisco IDS, Cisco IOS Firewall, VPN, and Network Admission Control (NAC) solutions.
- The size of the signature database used by the device can be adapted to the amount of available memory in the router.

Refer to Online Course for Illustration

5.2.2.6 Alarm Triggering Mechanisms

Triggering mechanisms can generate alarms that are false positives or false negatives. These alarms must be addressed when implementing an IPS sensor.

The figure summarizes the following four types of alarms:

- A false positive alarm is an expected but undesired result. A false positive occurs when an intrusion system generates an alarm after processing normal user traffic that should not have triggered an alarm. If this occurs, the administrator must be sure to

tune the IPS to change these alarm types to true negatives. Analyzing false positives limits the time that a security analyst has to examine actual intrusive activity on a network.

- A false negative is when an intrusion system fails to generate an alarm after processing attack traffic that the intrusion system is configured to detect. It is imperative that the intrusion system does 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.
- A true positive alarm describes a situation in which an intrusion system generates an alarm in response to known attack traffic.
- A true negative describes a situation in which normal network traffic does not generate an alarm.

Refer to Interactive Graphic in online course

5.2.2.7 Activity - IPS Signature Alarms

Refer to Online Course for Illustration

5.2.3 IPS Signature Actions

5.2.3.1 Signature Actions

When a signature detects the activity for which it is configured, the signature triggers one or more actions. Several categories of actions can be invoked, as shown in Figures 1, 2, and 3:

- Generate an alert.
- Log the activity.
- Drop or prevent the activity.
- Reset a TCP connection.
- Block future activity.
- Allow the activity.

The available actions depend on the signature type and the platform.

Refer to Online Course for Illustration

5.2.3.2 Manage Generated Alerts

Monitoring the alerts generated by network-based and host-based IPS systems is vital to understanding the attacks being launched against the network. As shown in the figure, an IPS can be enabled to produce an alert or a verbose alert.

Should an attacker cause a flood of bogus alerts, examining these alerts can overwhelm the security analysts. Network-based and host-based IPS solutions incorporate two types of alerts to enable an administrator to efficiently monitor the operation of the network: atomic alerts and summary alerts. Understanding these types of alerts is critical to providing the most effective protection for a network.

Atomic Alerts

Atomic alerts are generated every time a signature triggers. In some situations, this behavior is useful and indicates all occurrences of a specific attack. However, an attacker might be able to flood the monitor console with alerts by generating thousands of bogus alerts against the IPS device or applications.

Summary Alerts

Instead of generating alerts for each instance of a signature, some IPS solutions enable the administrator to generate summary alerts. A summary alert is a single alert that indicates multiple occurrences of the same signature from the same source address or port. Alert summary modes limit the number of alerts generated and make it difficult for an attacker to consume resources on the sensor.

With the summarization modes, the administrator also receives information on the number of times the activity that matches a signature's characteristics was observed during a specific period of time. When using alert summarization, the first instance of intrusive activity usually triggers a normal alert. Additional instances of the same activity or duplicate alerts are counted until the end of the signature's summary interval. When the length of time specified by the summary interval has elapsed, a summary alert is sent, which indicates the number of alerts that occurred during the time interval.

Some IPS solutions also enable automatic summarization, even though, the default behavior is to generate atomic alerts. In this situation, if the number of atomic alerts exceeds a configured threshold in a specified amount of time, the signature automatically switches to generating summary alerts instead of atomic alerts. After a defined period of time, the signature reverts to its original configuration. Automatic summarization enables the administrator to automatically regulate the number of alerts being generated.

Some IPS solutions also enable the generation of a single atomic alert and then disable alerts for that signature and source address for a specific period of time. This prevents an administrator from getting overwhelmed with alerts while still indicating that a specific system shows suspicious activity.

Refer to Online Course for Illustration

5.2.3.3 Log Activities for Later Analysis

In some situations, an administrator does not necessarily have enough information to stop an activity. Therefore, logging the actions or packets that are seen so that they can be analyzed later in more detail is very important. As shown in the figure, an IPS can be enabled to log the attacker packets, pair packets, or just the victim packets.

By performing a detailed analysis, an administrator can identify exactly what is taking place and make a decision as to whether it should be allowed or denied in the future.

For example, an administrator can configure a signature to look for the string **/etc/password** and to log the action with the attacker's IP address whenever the signature triggers. The IPS device begins logging the traffic from the attacker's IP address for a specified period of time or number of bytes. This log information is usually stored on the IPS device in a specific file. Because the signature also generates an alert, the administrator can observe the alert on the management console. Then the log data can be retrieved from the IPS device, and the activity that the attacker performed on the network after triggering the initial alarm can be analyzed.

Refer to Online Course for Illustration

5.2.3.4 Deny the Activity

One of the most powerful actions that an IPS device can perform is to drop packets or prevent an activity from occurring. As shown in the figure, an IPS can be enabled to deny the attacker packets, deny the connection, or deny the specific packet.

Dropping packets enables the device to stop an attack before it has the chance to perform malicious activity. Unlike a traditional IDS device, the IPS device actively forwards packets across two of its interfaces. The analysis engine determines which packets should be forwarded and which packets should be dropped.

Besides dropping individual packets, the drop action can be expanded to drop all packets for a specific connection or even all packets from a specific host for a certain amount of time. By dropping traffic for a connection or host, the IPS conserves resources without having to analyze each packet separately.

Refer to Online Course for Illustration

5.2.3.5 Reset, Block, and Allow Traffic

An IPS can be enabled to reset or block packets, as shown in the figure.

Resetting a TCP Connection

The TCP Reset Signature Action is a basic action that can be used to terminate TCP connections by generating a packet for the connection with the TCP RST flag set. Many IPS devices use the TCP reset action to abruptly end a TCP connection that is performing unwanted operations. The reset TCP connection action can be used in conjunction with deny packet and deny connection actions. Deny packet and deny flow actions do not automatically cause TCP reset actions to occur.

Blocking Future Activity

Most IPS devices have the capability to block future traffic by having the IPS device update the ACLs on one of the infrastructure devices. The ACL stops traffic from an attacking system without requiring the IPS to consume resources analyzing the traffic. After a configured period of time, the IPS device removes the ACL. Network-based IPS devices usually provide this blocking functionality along with other actions, such as dropping unwanted packets. One advantage of the blocking action is that a single IPS device can stop traffic at multiple locations throughout the network, regardless of the location of the IPS device. For example, an IPS device located deep within the network can apply ACLs at the perimeter router or firewall.

Allowing the Activity

The final action is the Allow Signature action. It might seem a little confusing because most IPS devices are designed to stop or prevent unwanted traffic on a network. The allow action is necessary so that an administrator can define exceptions to configured signatures. Sometimes there is a need to allow a few systems or users to be exceptions to the configured rule on an IPS. Configuring exceptions enables administrators to take a more restrictive approach to security because they can first deny everything and then allow only the activities that are needed.

For example, suppose that the IT department routinely scans its network using a common vulnerability scanner. This scanning causes the IPS to trigger various alerts. These are the same alerts that the IPS generates if an attacker scans the network. By allowing the alerts from the approved IT scanning host, an administrator can protect the network from intrusive scans while eliminating the false positives generated by the routine IT-approved scanning.

Some IPS devices provide the allow action indirectly through other mechanisms, such as signature filters. If an IPS does not provide the allow action directly through an action, such as permit or allow, the administrator needs to search the product documentation to find the mechanism used to enable exceptions to signatures.

Refer to Interactive Graphic in online course

5.2.3.6 Activity - Identify the IPS Signature Action

Refer to Online Course for Illustration

5.2.4 Manage and Monitor IPS

5.2.4.1 Monitor Activity

Monitoring the security-related events on a network is also a crucial aspect of protecting a network from attack. Understanding which attacks are being launched against the network enables an administrator to assess how strong the current protections are and what enhancements may be required as the network grows. Only by monitoring the security events on a network can an administrator accurately identify the attacks and security policy violations that are occurring.

As shown in the figure, there are four factors to consider when implementing an IPS solution.

Refer to Online Course for Illustration

5.2.4.2 Monitoring Considerations

The figure illustrates the four factors to consider when implementing a monitoring strategy.

Management Method

IPS sensors can be managed individually or centrally. Configuring each IPS device individually is the easiest process if there are only a couple of sensors. Managing many IPS routers and IPS sensors individually becomes difficult and time-consuming.

In a larger network, a centralized management system that allows the administrator to configure and manage all IPS devices from a single central system should be deployed. Using a centralized management approach for large sensor deployments reduces time and staffing requirements and enables greater visibility to all events occurring on a network.

Event Correlation

Event correlation refers to the process of correlating attacks and other events that are happening simultaneously at different points across a network. Having the devices derive their time from a Network Time Protocol (NTP) server enables all alerts generated by the IPS to be accurately time-stamped. A correlation tool can then correlate the alerts based on their time-stamps. The administrator should enable NTP on all network devices to time-stamp events with a common system time. These time-stamps can then be used to accurately assess when specific network events happened in relation to other events, regardless of which device detected the event.

Another factor that facilitates event correlation is deploying a centralized monitoring facility on a network. By monitoring all IPS events at a single location, an administrator greatly improves the accuracy of event correlation.

Security Staff

IPS devices tend to generate numerous alerts and other events during network traffic processing. Large enterprises require appropriate security staff to analyze this activity and determine how well the IPS is protecting the network. Examining these alerts also enables security operators to tune the IPS and optimize the IPS operation to the unique requirements of the network.

Incident Response Plan

If a system is compromised on a network, a response plan must be in place. The compromised system should be restored to the state it was in before the attack. It must be determined if the compromised system led to a loss of intellectual property or the compromise of other systems on the network.

Note Although the CLI can be used to configure an IPS deployment, it is sometimes simpler to use a GUI-based device manager. Several Cisco device management software solutions are available to help administrators manage an IPS solution. Some provide locally managed IPS solutions, and some provide more centrally managed solutions.

There are three GUI-based IPS device managers available:

- Cisco Configuration Professional
- Cisco IPS Manager Express (IME)
- Cisco Security Manager

Refer to Online Course for Illustration

5.2.4.3 Secure Device Event Exchange

IPS sensors and Cisco IOS IPS generate alarms when an enabled signature is triggered. These alarms are stored on the sensor and can be viewed locally, or through a management application, such as IPS Manager Express.

When an attack signature is detected, the Cisco IOS IPS feature can send a syslog message or an alarm in Secure Device Event Exchange (SDEE) format, as shown in the figure.

The SDEE protocol was developed to improve communication of events generated by security devices. It primarily communicates IDS events, but the protocol is intended to be extensible and allows additional event types to be included as they are defined.

Example SDEE system alarm message format:

%IPS-4-SIGNATURE:Sig:1107 Subsig:0 Sev:2 RFC1918 address [192.168.121.1:137 ->192.168.121.255:137]

Refer to Online Course for Illustration

5.2.4.4 IPS Configuration Best Practices

Managing signatures on many IPS devices can be difficult. To improve IPS efficiency in a network, consider using these recommended configuration best practices, as shown in the figure:

- Balance the need to upgrade sensors with the latest signature packs against the momentary downtime during which the network becomes vulnerable to attack.

- Update signature packs automatically when setting up a large deployment of sensors, rather than manually upgrading each sensor. This gives security operations personnel more time to analyze events.
- 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 SFTP server to allow read-only access to the files within the directory on which the signature packs are placed.
- 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.

Note Automatic download of updated IPS signature definition files is configurable on ISR G2 routers. This is an alternative to relying on an SFTP server.

Refer to Online Course for Illustration

5.2.5 IPS Global Correlation

5.2.5.1 Cisco Global Correlation

In addition to maintaining signature packs, Cisco IPS includes a security feature called Cisco Global Correlation. With global correlation, Cisco IPS devices receive regular threat updates from a centralized Cisco threat database called the Cisco SensorBase Network. The Cisco SensorBase Network contains real-time, detailed information about known threats on the Internet. The goals of the Cisco Global Correlation are shown in the figure.

Participating IPS devices are part of the Cisco SensorBase Network and receive global correlation updates that include information on network devices with a reputation for malicious activity. Similar to human social interaction, reputation is an opinion about a device on the Internet. A network device with a reputation is most likely either malicious or infected. The reputation analysis data contained in the global correlation updates is factored into the analysis of network traffic. This increases IPS effectiveness because traffic is denied or allowed based on the reputation of the source IP address.

Note Cisco Global Correlation is available for the Cisco IPS 4300 and 4500 Series appliances, as well as for the Cisco ASA 5500-X and ISR G2 IPS modules.

Refer to Online Course for Illustration

5.2.5.2 Cisco SensorBase Network

The IPS sensor can be configured to participate in the global correlation updates and in sending telemetry data. Both services can also be turned off.

When participating in global correlation, the Cisco SensorBase Network provides information to the IPS sensor about IP addresses with a reputation, as shown in the figure. The sensor uses this information to determine which actions, if any, to perform when potentially harmful traffic is received from a host with a known reputation. Since the global correlation database changes rapidly, the sensor must periodically download global correlation updates from the global correlation servers. It is possible to view reputation scores in events and see the reputation score of attackers. It is also possible to view statistics from the reputation filter.

Sensors installed at customer sites can also enable network participation, in which they send data to the SensorBase Network. This allows the SensorBase Network to collect nearly real-time data from sensors around the world. Communication between sensors and the SensorBase Network involves an HTTPS request and response over TCP/IP. Network participation requires a network connection to the Internet. There are three modes for network participation: off, partial participation, and full participation.

Refer to Online Course for Illustration

5.2.5.3 Cisco Security Intelligence Operation

In order for global correlation to occur, the raw information is first collected by the Cisco SensorBase Network, as shown in Figure 1. The SensorBase Network is part of a larger, back-end security ecosystem, known as the Cisco Security Intelligence Operation (SIO). As shown in Figure 2, the purpose of Cisco SIO is to detect threat activity, research and analyze threats, and provide real-time updates and best practices to keep organizations informed and protected. Cisco SIO consists of three elements:

- Threat intelligence from the Cisco SensorBase Network
- Threat Operations Center, which is the combination of automated and human processing and analysis
- Automated and best practices content that is pushed to network elements in the form of dynamic updates

Cisco SIO is a security intelligence ecosystem that baselines the current state of threats on a worldwide basis. It also provides network administrative systems with valuable information to detect, prevent, and react to threats. SIO acts as an early warning system by correlating threat information from the SensorBase, which has been analyzed by the Threat Operations Center. SIO then feeds this information to enforcement elements, such as an IPS device configured with global correlation. These enforcement elements provide live threat prevention based on malware outbreaks, current vulnerabilities, and zero-day attacks.

Refer to Online Course for Illustration

5.2.5.4 Reputations, Blacklists, and Traffic Filters

A reputation is based on a commonly held opinion. Reputations can be tarnished when there is a reason that causes others to become distrustful or suspicious. This also applies to networks. IP addresses, mail servers, URLs, and other entities can all have a reputation.

Many of today's network protection technologies and filtering systems depend on lists to determine if the information is good (whitelist) or bad (blacklist). Antispam technologies rely on these lists of bad email server IP addresses to prevent the continued deluge of emails coming from an identified spamming server.

Malware is malicious software that is installed on an unknowing host. A common characteristic of malware is the presence of a URL that a user must visit to be attacked. Spam, URL-based viruses, phishing attacks, and spyware all direct the user to a malicious URL. Accurately analyzing these URLs and associating a reputation with them helps stop attacks much more quickly and avoids the URL in whatever method it is disseminated.

By participating in Cisco's global correlation, IPS sensors can periodically receive regular threat updates from the centralized Cisco threat database called the Cisco SensorBase Network. This includes information about botnets, malware, spammers, and other threats. IPS sensors can use reputation filters to deny IP addresses that are blacklisted before the sensor does further analysis on the traffic. Reputation filters offer the first level of defense by denying traffic based on IP addresses in the blacklist. Cisco SenderBase web site, www.senderbase.org is shown in Figure 1. Figure 2 illustrates the Cisco ASA botnet traffic filter.

Refer to Video in online course

5.2.5.5 Reputations, Blacklists, and Traffic Filters (Cont.)

The video in the figure provides a thorough overview of Cisco IPS including threat intelligence, advance inspection protection, and reputation technology.

You can also supplement the Cisco dynamic database with blacklisted addresses of your choice by adding them to a static blacklist. If the dynamic database includes blacklisted addresses that you think should not be blacklisted, you can manually enter them into a static whitelist. Whitelisted addresses, those that are permitted on the network, still generate syslog messages. However, because you are only targeting blacklist syslog messages, they are only informational.

Today's organizations must consider what impact their security practices may have on the larger and increasingly complex and interconnected cybersecurity ecosystem. Not taking this "big picture" view could result in an organization earning a bad reputation score, which means no leading security provider will allow users to access the blacklisted site or forward their email. It is not easy for a company to come back from being blacklisted—and some may never fully recover.

Click here to read the transcript of this video.

Refer to Online Course for Illustration

5.3 Implement IPS

5.3.1 Configure Cisco IOS IPS with CLI

5.3.1.1 Implement IOS IPS

Cisco IOS IPS enables administrators to manage intrusion prevention on routers. Cisco IOS IPS monitors and prevents intrusions by comparing traffic against signatures of known threats and blocking the traffic when a threat is detected.

Several steps are necessary to use the Cisco IOS CLI to work with IOS IPS 5.x format signatures. Cisco IOS version 12.4(10) or earlier used IPS 4.x format signatures and some IPS commands have changed.

Implement IOS IPS:

Step 1. Download the IOS IPS files.

Step 2. Create an IOS IPS configuration directory in Flash.

Step 3. Configure an IOS IPS crypto key.

Step 4. Enable IOS IPS.

Step 5. Load the IOS IPS signature package to the router.

Refer to Online Course for Illustration

5.3.1.2 Download the IOS IPS Files

Cisco IOS release 12.4(10)T and earlier, provided built-in signatures in the Cisco IOS software image, as well as support for imported signatures. IPS signature selection involved loading an XML file onto the router. This file, called the signature definition file (SDF), contained a detailed description of each selected signature in Cisco IPS Sensor software 4.x signature format.

With newer IOS versions, there are no built-in (hard-coded) signatures within the Cisco IOS software. Instead, all signatures are stored in a separate signature file and must be imported. The IOS release 12.4(15)T4 or later, uses the newer 5.x format signature files. These files can be downloaded from cisco.com, which requires a user account.

Step 1. **Download the IOS IPS files.**Prior to configuring IPS, it is necessary to download the IOS IPS signature package files, as shown in Figure 1, and a public crypto key from cisco.com. The specific IPS files to download vary depending on the current release. Only registered customers can download the package files and key.

- **IOS-Sxxx-CLI.pkg** - The latest signature package.
- **realm-cisco.pub.key.txt** - The public crypto key used by IOS IPS.

Step 2. **Create an IOS IPS configuration directory in Flash.**

The second step is to create a directory in flash to store the signature files and configurations. The **mkdir** privileged EXEC command creates the directory in Flash, as shown in Figure 2. Other useful commands include **rename**, which allows the name of the directory to be changed. To verify the contents of Flash, enter the **dir flash:** privileged EXEC mode command. The syntax for both commands is shown in Figure 2.

Figure 3 shows an example of creating and verifying the directory IPSDIR.

Cisco IOS IPS supports any Cisco IOS file system as the configuration location, as long as it has proper write access. A Cisco USB flash drive connected to the USB port on the router can be used as an alternative location to store the signature files and configurations. The USB flash drive must remain connected to the USB port on the router if it is used as the IOS IPS configuration directory location.

Refer to Online Course for Illustration

5.3.1.3 IPS Crypto Key

Step 3. **Configure an IOS IPS Crypto Key**

The third step is to configure the crypto key used by IOS IPS. This key is located in the realm-cisco.pub.key.txt file that was obtained in Step 1.

The crypto key verifies the digital signature for the master signature file (sigdef-default.xml). The content of the file is signed by a Cisco private key to guarantee its authenticity and integrity.

Open the text file to configure the IOS IPS crypto key, as shown in Figure 1. Copy the contents of the file, and paste the contents to the router at the global configuration prompt. The text file issues the various commands to generate the RSA key.

At the time of signature compilation, an error message is generated if the public crypto key is invalid.

Example Error Message:

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

If the key is configured incorrectly, the key must be removed and then reconfigured. Use the **no crypto key pubkey-chain rsa** and the **no named-key realm-cisco.pub signature** commands. Then repeat the procedure in Step 3 to reconfigure the key.

Enter the **show run** command, as shown in Figure 2, to confirm that the crypto key is configured.

Refer to Online Course for Illustration

5.3.1.4 Enable IOS IPS

Step 4. Enable IOS IPS

The fourth step is to configure IOS IPS, which is a process that consists of four sub-steps.

a. Identify the IPS rule name and specify the location.

Create a rule name by using the command syntax shown in Figure 1, and the **ip ips name** command. In Figure 1, an IPS rule named IOSIPS is created. An optional extended or standard ACL can be configured to filter the scanned traffic. All traffic that is permitted by the ACL is subject to inspection by the IPS. Traffic that is denied by the ACL is not inspected by the IPS.

Configure the IPS signature storage location by using the command syntax in Figure 1 and the **ip ips config location flash** command. In the example in Figure 1, the IPS location in flash is identified as **flash:IPS**.

Note Prior to IOS 12.4(11)T, the **ip ips sdf location** command was used.

b. Enable SDEE and logging event notification.

To use SDEE, the HTTP or HTTPS server must first be enabled with the **ip http server** or **ip https server** command. If the HTTP server is not enabled, the router cannot respond to the SDEE clients because it cannot see the requests. SDEE notification is disabled by default and must be explicitly enabled. Enable IPS SDEE even notification by using the **ip ips notify sdee** command, as shown in Figure 2. IOS IPS also supports logging to send event notification. SDEE and logging can be used independently or enabled at the same time. Logging notification is enabled by default. If the logging console is enabled, IPS log messages are displayed on the console. Use the **ip ips notify log** command to enable logging. The IPS log messages are sent to a syslog server if one is configured.

In Figure 2, SDEE and Syslog notifications are enabled.

c. Configure the signature category.

All signatures are grouped into categories, and the categories are hierarchical. This helps classify signatures for easy grouping and tuning. The three most common categories are **all**, **basic**, and **advanced**.

The signatures that IOS IPS uses to scan traffic can be retired or unretired. Retiring a signature means that IOS IPS does not compile that signature into memory for scanning. Un-retiring a signature instructs IOS IPS to compile the signature into memory and use it to scan traffic. When IOS IPS is first configured, all signatures in the **all** category should be retired. Then, selected signatures should be unretired in a less memory-intensive category. To retire and unretire signatures, first enter IPS category mode using the **ip ips signature-category** command. Next use the **category** command to change a category. For example, use the **category all** command to enter IPS category **all** action mode. To retire a category, use the **retired true** command. To unretire a category, use the **retired false** command.

In the example in Figure 3, the **all** IPS category is retired, and the **basic** IPS category is unretired.

Caution Do not unretire the **all** category. The **all** signature category contains all signatures in a signature release. The IOS IPS cannot compile and use all the signatures at one time because it will run out of memory.

The order in which the signature categories are configured on the router is also important. IOS IPS processes the category commands in the order listed in the configuration. Some signatures belong to multiple categories. If multiple categories are configured and a signature belongs to more than one of them, IOS IPS uses the signature's properties in the last configured category, for example, retired, unretired, or actions.

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

Use the **ip ips** interface configuration command to apply the IPS rule, shown in Figure 4.

In the example in Figure 4, the IPS rule IOSIPS is applied to incoming traffic on the G0/0 interface. It is also applied to the incoming and outgoing traffic on the G0/1 interface.

Refer to Online Course for Illustration

5.3.1.5 Load the IPS Signature Package in RAM

Step 5. Loading IOS IPS Signature Package to the Router

The last step is for the administrator to upload the signature package to the router. The most common methods are FTP or TFTP. To copy the downloaded signature package from the TFTP server to the router, use the **copy tftp** command with the **idconf** parameter at the end of the command. An example is shown in Figure 1. The syntax for the **copy ftp** command is shown in Figure 2.

To verify that the signature package is properly compiled, the administrator uses the **show ip ips signature count** command, as shown in Figure 3.

Use the Syntax Checker in Figure 4 to configure Cisco IOS IPS on R2.

Refer to Interactive Graphic in online course

5.3.1.6 Activity - Implementing IPS

Refer to Online Course for Illustration

5.3.2 Modifying Cisco IOS IPS Signatures

5.3.2.1 Retire and Unretire Signatures

The Cisco IOS CLI can be used to retire or unretire individual signatures or a group of signatures that belong to a signature category. When a group of signatures is retired or unretired, all signatures in that category are retired or unretired.

Some unretired signatures, either unretired as an individual signature or within an unretired category, might not compile because of insufficient memory, invalid parameters, or if the signature is obsolete.

Figure 1 shows a sample of retiring a specific signature. In this example, the signature 6130 with subsig ID of 10 is retired.

Figure 2 shows an example of unretiring a signature category. In this example, all signatures that belong to the IOSIPS Basic category are unretired.

Refer to Online Course for Illustration

5.3.2.2 Change Signature Actions

You can also use the IOS CLI to change signature actions for one signature or a group of signatures based on signature categories. To change an action, the **event-action** command must be used in IPS Category Action mode or Signature Definition Engine mode.

The **event-action** command has several parameters, as shown in Figure 1.

Figure 2 shows an example of changing the action for signature 6130 with subsig ID of 10. Figure 3 shows an example of changing the event action for all signatures that belong to the signature IOS IPS Basic category.

Use the Syntax Checker in Figure 4 to configure IPS signature actions on R2.

Refer to Online Course for Illustration

5.3.3 Verify and Monitor IPS

5.3.3.1 Verify IOS IPS

After IPS is implemented, it is necessary to verify the configuration to ensure correct operation. There are several **show** commands that can be used to verify the IOS IPS configuration:

- The **show ip ips** privileged EXEC command can be used with other parameters to provide specific IPS information.
- The **show ip ips all** command displays all IPS configuration data, as shown in Figures 1 and 2. The output can be lengthy depending on the IPS configuration.

- The **show ip ips configuration** command displays additional configuration data that is not displayed with the **show running-config** command. Figure 3 displays example output of the command.
- The **show ip ips interfaces** command displays interface configuration data, as shown in Figure 4. The output shows inbound and outbound rules applied to specific interfaces.
- The **show ip ips signatures** command verifies the signature configuration, as shown in Figure 5. The command can also be used with the keyword **detail** to provide more explicit output.
- The **show ip ips statistics** command displays the number of packets audited, and the number of alarms sent, as shown in Figure 6. The optional **reset** keyword resets output to reflect the latest statistics.

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

Refer to Online Course for Illustration

5.3.3.2 Report IPS Alerts

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

The example in the figure enables syslog reporting.

Refer to Online Course for Illustration

5.3.3.3 Enable SDEE

SDEE is the preferred method of reporting IPS activity. SDEE uses HTTP and XML to provide a standardized approach. It can be enabled on an IOS IPS router using the **ip ips notify sdee** command. The Cisco IOS IPS router can still send IPS alerts via syslog.

The figure shows an example of enabling SDEE reporting.

Administrators must also enable HTTP or HTTPS on the router when enabling SDEE. The use of HTTPS ensures that data is secured as it traverses the network.

All stored events are lost when Cisco SDEE notification is disabled. A new buffer is allocated when the notifications are re-enabled. SDEE uses a pull mechanism. With a pull mechanism, requests come from the network management application and the IDS or IPS router responds. SDEE is the standard format for vendor devices to communicate events to a network management application.

The buffer stores up to 200 events by default. If a smaller buffer is requested, all stored events are lost. If a larger buffer is requested, all stored events are saved and additional space is allocated for entries beyond the previous buffer size. The default buffer size can be altered with the **ip sdee events** command. The maximum number of events is 1,000.

The **clear ip ips sdee** command clears SDEE events or subscriptions. The syntax for both commands is shown in the figure.

The **ip ips notify** command replaces the older **ip audit notify** command. If the **ip audit notify** command is part of an existing configuration, the IPS interprets it as the **ip ips notify** command.

5.4 Summary

5.4.1 Conclusion

Refer to Lab Activity for this chapter

5.4.1.1 Lab - Configure an IOS IPS Using CLI

In this lab, you will configure the Cisco IOS IPS, which is part of the Cisco IOS Firewall feature set. IPS examines certain attack patterns and alerts or mitigates when those patterns occur. IPS alone is not enough to make a router into a secure Internet firewall, but when added to other security features, it can be a powerful defense.

Refer to Packet Tracer Activity for this chapter

5.4.1.2 Packet Tracer - Configure an IOS IPS Using the CLI

In this Packet Tracer, you will complete the following objectives:

- Enable IOS IPS.
- Configure logging.
- Modify an IPS signature.
- Verify IPS.

Refer to Online Course for Illustration

5.4.1.3 Implementing Intrusion Prevention

A network must be able to instantly recognize and mitigate worm and virus threats. To defend the network against fast-moving Internet worms and viruses, a network-based IPS should be implemented inline while IDS is implemented offline.

IPS signatures are similar to antivirus .dat files because they provide an IPS with a list of identified problems. The IPS signatures are configured to use various triggers and actions. Security staff must continuously monitor an IPS solution to ensure that it provides an adequate level of protection. If not, then signatures may need to be tuned to a specific network.

Go to the online course to take the quiz and exam.

Chapter 5 Quiz

This quiz is designed to provide an additional opportunity to practice the skills and knowledge presented in the chapter and to prepare for the chapter exam. You will be allowed multiple attempts and the grade does not appear in the gradebook.

Chapter 5 Exam

The chapter exam assesses your knowledge of the chapter content.

Your Chapter Notes