BCSE354E - Information Security Management

Module 3a – Configuring IPS

Intrusion Prevention System

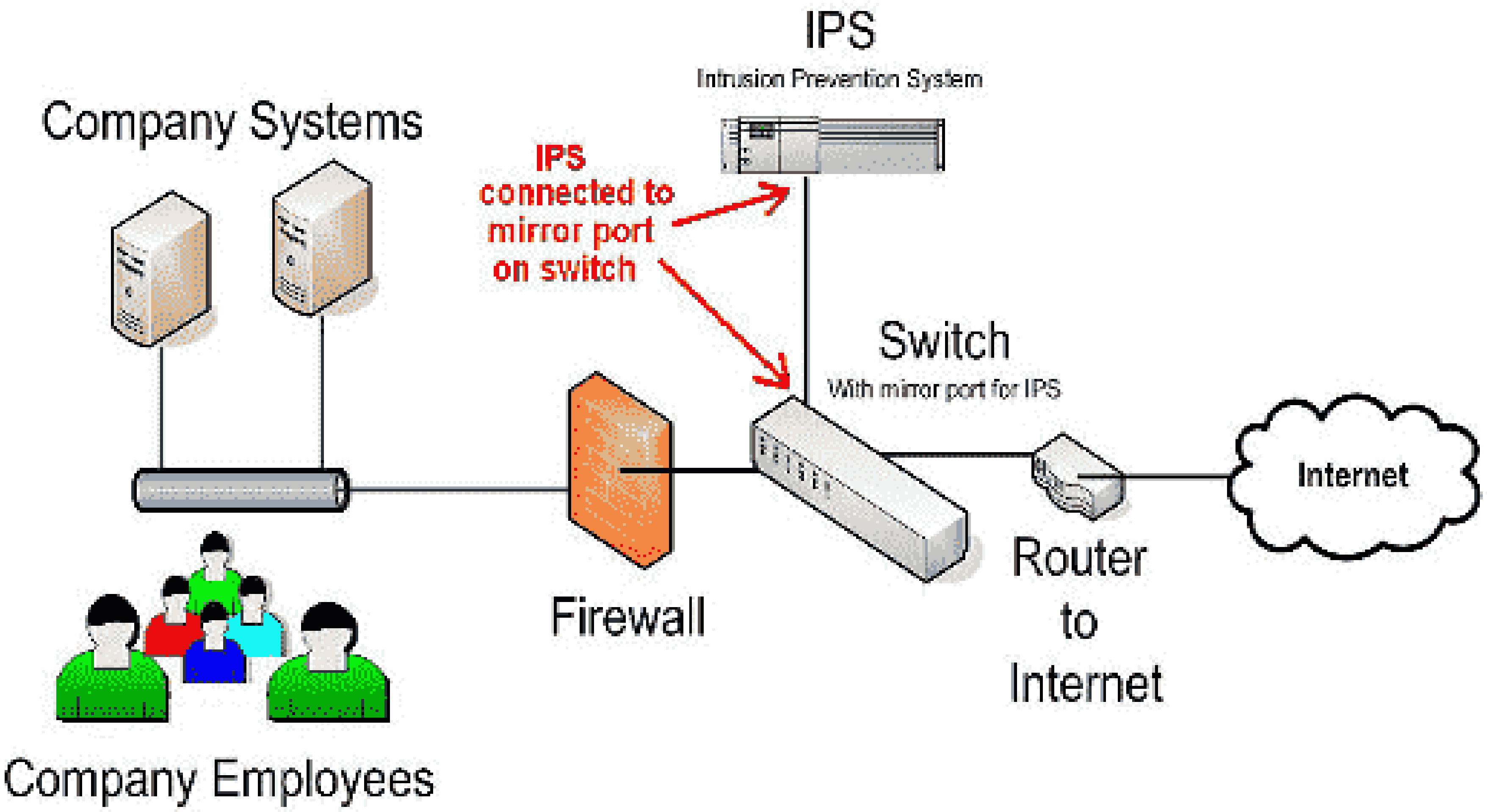
(IPS)

Intrusion Prevention System (IPS)

- Intrusion Prevention System (IPS) is a network-based platform that inspects **network traffic for malicious or unwanted activity** such as worms, spyware, and policy violations.
- When IPS detects a threat, it reacts in **real-time** by taking actions such as **blocking or dropping connections**, logging the detected activities, and sending notifications about these activities.
- You can use the **default actions for each signature*** or customize the actions to suit your requirements.

*unique characteristics or behaviors that are associated with a specific threat

Intrusion Prevention System



Intrusion Prevention System

- **Signature-based**
- **Anomaly-based**
- **Policy-based**

Intrusion Prevention System

- **Signature-based:**
- This method matches the activity to **signatures of well-known threats.**
- One drawback to this method is that it can only stop **previously identified attacks** and won’t be able to recognize new ones.

Intrusion Prevention System

- **Anomaly-based:**
- This method **monitors for abnormal behavior** by comparing random samples of network activity against a baseline standard.
- It is more **robust** than signature-based monitoring, but it can sometimes produce **false positives**.
- Some newer and more advanced intrusion prevention systems use **artificial intelligence and machine learning technology** to support anomaly-based monitoring.

Intrusion Prevention System

- **Policy-based:**
- This method is somewhat less common than signature-based or anomaly-based monitoring.
- It employs **security policies** defined by the enterprise and blocks activity that violates those policies.
- This requires an **administrator** to set up and configure security policies.

Configuring Intrusion Prevention System (IPS)

- IPS uses signatures to identify the attacks in progress.
  - You must update the IPS signatures frequently to keep the protection current.

- After setting up IPS, you have these options for monitoring the activity:
  - Enable the IPS report from the Security Services > Security Services Reports page or from the Status > Security Services Reports page to see the number of packets detected and the number of packets dropped by IPS.
  - Enable the IPS Alert feature to send an alert email to a specified email address if an attack is detected by IPS.
- **Note:** You must install licenses on the License Management page before you can configure IPS.

Configuring Intrusion Prevention System (IPS)

IPS Scan Modes - two scan modes

1. **Full Scan**
    - Scan all packets for policies that have IPS enabled.
    - Inspects a larger portion of the file and requires more time and resources to complete.
2. **Fast Scan**
    - Scan fewer packets within each connection to improve performance.
    - Inspects a smaller portion of each file that in most cases is enough to identify all threats, and provides much better IPS performance.

- It is recommended to use the Fast scan mode in most environments.

Configuring Intrusion Prevention System (IPS)

IPS Threat Levels

- IPS categorizes IPS signatures into five threat levels, based on the severity of the threat.
- The severity levels, from highest to lowest are:
  - **Critical**
  - **High**
  - **Medium**
  - **Low**
  - **Information**
- When you enable IPS, the **default setting is** to drop and log traffic that matches the **Critical, High, Medium, or Low threat levels**.
- Traffic that matches the Information threat level is allowed and **not logged by default.**

Configuring Intrusion Prevention System (IPS)

IPS Actions

For each threat level you can select one of these actions:

- **Allow** — Allows the connection.
- **Drop** — Denies the request and drops the connection. No information is sent to the source of the content.
- **Block** — Denies the request, drops the connection, and adds the IP address of the content source to the Blocked Sites list.
  - If the content that matches an IPS signature came from a *client*, the client IP address is added to the *Blocked Sites list*.
  - If the content came from a server, the server IP address is added to the *Blocked Sites list*.

Steps for Configuring Intrusion Prevention

1. Click **Security Services > Intrusion Prevention (IPS) > IPS Policy and Protocol Inspection**.
   - The IPS Policy and Protocol Inspection window opens.
2. At the top of the page, enable or disable IPS by clicking **On** or **Off**.
3. In the **Zone** area, chose the zones to be inspected. IPS inspects inter-zone traffic only.
   - **To add a zone:** In the Zones Available list, click a zone, and then click **Add** to move it to the Selected Zones list. All incoming and outgoing traffic for the selected zones is inspected.
   - **To remove a zone:** In the Selected Zones list, click a zone, and then click **Remove** to move it to the Zones Available list.

Steps for Configuring Intrusion Prevention

4. In the **IPS Signature** area, use the options below to filter the list of signatures in the Selected Signature table.

- The unfiltered list includes thousands of IPS signatures that are used to identify attacks.
- After selecting filters, click **Refresh** to redisplay the Selected Signature table showing only the matching signatures.
    - **Severity Level:** Choose a severity level, from highest to lowest: Critical, High, Medium, Low, and Information.
    - **Operating System Type:** Choose **All** to include all signatures regardless of the type of operating system, or choose **Selected OS Types Only** to include only the signatures that match the specified types of operation systems.
    - **Host Type:** Choose a host type.
    - **Category:** Choose **All** to include all signatures regardless of the category, or choose **Selected Categories Only** to include only the signatures that match the specified categories.

Steps for Configuring Intrusion Prevention

The Selected Signature table displays this information:

- **Name**: The name of the signature.
- **ID**: The unique identifier of the signature. To view complete details for a signature, click the link in the ID column.
- **Severity**: The severity level of the threat that the signature can identify.
- **Category**: The category that the signature belongs to.
- **Default Action**: The default preventive action for the signature.
  - Block and Log: Deny the request, drop the connection, and log the event when a signature is detected by the IPS engine.
  - Log Only: Only log the event when a signature is detected by the IPS engine.

Steps for Configuring Intrusion Prevention

Current Action: The current preventive action for the signature.

- **Edit Action:** Click the pencil icon to enable, disable, or set the preventive actions for a signature.

NOTE: For ease of use, you can edit the preventive actions for a group of signatures. Check the box for each signature that you want to change, or select all signatures by checking the box in the top left corner of the table. To edit the settings for the selected signatures, click the **Edit** (pencil) icon at the top of the table.

- **Block Threshold:** Specify a threshold at which blocking occurs; whether the Current Action is to block and log or to log only, traffic is blocked after the specified number of occurrences. Enter 0 to apply the Current Action immediately upon detection.

NOTE: The counter is reset to 0 whenever IPS settings are saved in the configuration utility or the security appliance is rebooted.

5. Click **Save** to apply your settings.

BCSE354E - Information Security Management

Module 3b – Data Loss Prevention

What is DLP and How Does it Work?

- Data Loss Prevention (DLP) is an approach that seeks to **improve information security and protect business information from data breaches.**
- It prevents end-users from moving key information outside the network.
- DLP also refers to tools that enable a network administrator to monitor data accessed and shared by end users.

What is DLP and How Does it Work?

- Other features common in DLP solutions include:

1. **Monitoring**—tools provide visibility into data and system access.
2. **Filtering**—tools can filter data streams to restrict suspicious or unidentified activity.
3. **Reporting**—tools provide logging and reports helpful for incident response and auditing.
4. **Analysis**—tools can identify vulnerabilities and suspicious behavior and provide forensic context to security teams.

What is DLP and How Does it Work?

- DLP solutions can be helpful in a variety of use cases, including:

1. **Security policy enforcement**—DLP tools can help you identify deviations from policy making it easier to correct misconfigurations.
2. **Meeting compliance standards**—DLP tools can compare current configurations to compliance standards and provide proof of measures taken.
3. **Increasing data visibility**—DLP tools can provide visibility across systems, helping you ensure that data is secure no matter where it's stored.

Reasons for Implementing a Data Loss Prevention Policy

1. Compliance

- Businesses are subject to mandatory compliance **standards imposed by governments (such as HIPAA, SOX, PCI DSS)**. These standards often stipulate how businesses should secure Personally Identifiable Information (PII), and other sensitive data A DLP policy is a basic first step to compliance, and most DLP tools are built to address the requirements of common standards.

Reasons for Implementing a Data Loss Prevention Policy

2. Intellectual property and intangible assets

- An organization may have trade secrets, other strategic **proprietary information, or intangible assets such as customer lists, business strategies, and so on.**
- Loss of this type of information can be **extremely damaging**, and accordingly, it is directly targeted by attackers and malicious insiders.
- A DLP policy can help **identify and safeguard** critical information assets.

Reasons for Implementing a Data Loss Prevention Policy

3. Data visibility

- Implementing a **DLP policy can provide insight into how stakeholders use data.**
- In order to protect sensitive information, organizations must first know whether it exists or not, where it exists, who uses it and for what purposes.

Creating a Successful DLP Policy

1. **Classifying and interpreting data**
   - Identify which information needs to be protected, by evaluating risk factors and how vulnerable it is. **Invest in classifying and interpreting data**, because this is the basis for implementing a suitable data protection policy.
2. **Allocate roles**
   - clearly define the **role of each individual** involved in the data loss prevention strategy.
3. **Begin by securing the most sensitive data**
   - start by selecting a **specific kind of information to protect**, which represents the biggest risk to the business.
4. **Automate as much as possible**
   - The more DLP processes are automated, the broader you'll be able to deploy them in the organization. **Manual DLP processes are inherently limited in its scope** and the amount of data they can cover.

Creating a Successful DLP Policy

5. **Use anomaly detection**
   - Some modern DLP tools use **machine learning** and **behavioral analytics**, instead of simple statistical analysis and correlation rules, **to identify abnormal user behavior.**
   - Each user and group of users is modeled with a behavioral baseline, allowing accurate detection of data actions that might represent malicious intent.

6. **Involve leaders in the organization**
   - management is key to making DLP work, because policies are **worthless if they cannot be enforced at the organizational level.**

7. **Educate stakeholder**
   - putting a DLP policy in place is not enough. Invest in **making stakeholders and users of data aware of the policy**, its significance and what they need to do to safeguard organizational data.

Creating a Successful DLP Policy

8. **Documenting DLP strategy**
    - **Documenting the DLP policy** is required by many compliance standards. It also **provides clarity**, both at the individual and organizational level, as to what is required and how the policy is enforced.

9. **Establish metrics**
    - Measure DLP effectiveness using **metrics like percentage of false positives**, number of incidents and Mean Time to Response.

10. Don’t save unnecessary data
    - A business should only use, save and store information that is essential. If information is **not needed, remove it;** data that was never stored cannot go missing.

What Type of DLP Solution is Right for Your Organization?

1. **Network DLP**

   - Protects an organization's network processes, such as **web application, email and FTP.**
   - Lives in the company's network, and monitors data as it moves throughout the network.
   - Maintains a database which provides details as to which data is being used and who is using the data.
   - Provides visibility into all data in transit on their network.

What Type of DLP Solution is Right for Your Organization?

2. Storage DLP

- Provides information about **files stored and shared by users of an organization's network.**
- Enables viewing sensitive files shared and stored on the network.
- Provides visibility into information stored via on-premise storage equipment and cloud-based storage.

What Type of DLP Solution is Right for Your Organization?

3. **Endpoint DLP**

   - **Monitors workstations, servers, and mobile devices such as laptops, mobile phones, external hard-drives and USB disks.**
   - Installed as an agent on endpoint equipment and prevents data leakage from the endpoints.
   - Provides visibility into data stored on endpoints physically located inside and outside the organization.

BCSE354E - Information Security Management

Module 3.c – Configuring IDS

Intrusion Detection System

IDS

Cisco IOS Firewall IDS feature

- The Cisco IOS Firewall IDS feature supports **intrusion detection technology for midrange and highend router platforms with firewall support.**
- It is ideal for **any network perimeter**, and especially for locations in which a **router is being deployed and additional security between network segments is required**.
- It also can **protect intranet and extranet connections** where additional security is mandated, and **branch-office sites connecting to the corporate office or Internet.**

The intrusion-detection signatures

- The Cisco IOS Firewall IDS feature identifies **59 of the most common attacks using "signatures" to detect patterns of misuse in network traffic.**
  - The intrusion-detection signatures included in the Cisco IOS Firewall were chosen from a broad cross-section of intrusion-detection signatures.
- The signatures represent **severe breaches of security** and the most common **network attacks and information-gathering scans**.
- The Cisco IOS Firewall IDS acts as an **in-line intrusion detection sensor, watching packets and sessions as they flow through the router, scanning each to match any of the IDS signatures.**
  - IDS monitors packets and send alarms when suspicious activity is detected.
  - IDS logs the event through Cisco IOS syslog or the Cisco Secure Intrusion Detection System (Cisco Secure IDS, formerly known as NetRanger) Post Office Protocol.

The intrusion-detection signatures

- The network administrator can configure the IDS system to choose the **appropriate response to various threats.**
- When packets in a session match a signature, the IDS system can be configured to take these actions:
  - **Send an alarm to a syslog server or a Cisco Secure IDS Director (centralized management interface)**
  - **Drop the packet**
  - **Reset the TCP connection**

Compatibility with Cisco Secure Intrusion Detection

- The Cisco Secure IDS is an **enterprise-scale, real-time, intrusion detection system designed to detect, report, and terminate unauthorized activity throughout a network.**
- The Cisco Secure IDS consists of three components:
  1. **Sensor**
  2. **Director**
  3. **Post Office**

IDS Components

1. **Cisco Secure IDS Sensors**
   - High-speed network appliances, **analyze the content and context of individual packets** to determine if traffic is authorized.
   - If a network's data stream exhibits unauthorized or suspicious activity, such as a SATAN attack, a ping sweep, or the transmission of a secret research project code word, Cisco Secure IDS Sensors can detect the policy violation in real time, forward alarms to a Cisco Secure IDS Director management console, and remove the offender from the network.
2. **The Cisco Secure IDS Director**
   - A high-performance, software-based management system that **centrally monitors the activity of multiple Cisco Secure IDS Senso**rs located on local or remote network segments.
3. **The Cisco Secure IDS Post Office**
   - The communication backbone that allows Cisco Secure IDS services and hosts to communicate with each other.
   - All communication is supported by a proprietary, connection-based protocol that can switch between alternate routes to maintain point-to-point connections.

Functional Description

- The Cisco IOS Firewall IDS acts as an in-line intrusion detection sensor, watching packets as they traverse the router's interfaces and acting upon them in a definable fashion.
- When a packet, or a number of packets in a session, match a signature, the Cisco IOS Firewall IDS may perform the following configurable actions:
    1. **Alarm—Sends an alarm to a syslog server or Cisco Secure IDS Director**
    2. **Drop—Drops the packet**
    3. **Reset—Resets the TCP connection**

Cisco IOS Firewall IDS - Packet auditing process

- You create an audit rule, **which specifies the signatures that should be applied to packet traffic and the actions to take when a match is found**. An audit rule can apply informational and attack signatures to network packets. You apply the audit rule to an interface on the router, specifying a traffic direction (in or out).
- **If the audit rule is applied to the *in* direction of the interface, packets passing through the interface are audited** before the inbound ACL has a chance to discard them. This allows an administrator to be alerted if an attack or information-gathering activity is underway even if the router would normally reject the activity.
- **If the audit rule is applied to the *out* direction on the interface**, **packets are audited after they enter the router through another interface.** In this case, the inbound ACL of the other interface may discard packets before they are audited. This may result in the loss of Cisco IOS Firewall IDS alarms even though the attack or information-gathering activity was thwarted.

Cisco IOS Firewall IDS - Packet auditing process

- Packets going through the interface that match the audit rule are audited by a series of modules, starting with IP; then either ICMP, TCP, or UDP (as appropriate); and finally, the Application level.
- If a signature match is found in a module, then the following user-configured action(s) occur:
  - **If the action is alarm, then the module completes its audit, sends an alarm, and passes the packet to the next module.**
  - **If the action is drop, then the packet is dropped from the module, discarded, and not sent to the next module.**
  - **If the action is reset, then the packets are forwarded to the next module, and packets with the reset flag set are sent to both participants of the session, if the session is TCP.**
- **Note**:
  - It is recommended that you use the drop and reset actions together.
  - If there are multiple signature matches in a module, only the first match fires an action. Additional matches in other modules fire additional alarms, but only one per module.

When to Use Firewall IDS

- The Firewall with intrusion detection is intended to satisfy the security goals of customers, and is particularly appropriate for the following scenarios:
  - **Enterprises that are interested in a cost-effective method of extending their perimeter security across all network boundaries, specifically branch-office, intranet, and extranet perimeters.**
  - **Small and medium-sized businesses that are looking for a cost-effective router that has an integrated firewall with intrusion-detection capabilities.**
  - **Service providers that want to set up managed services, providing firewalling and intrusion detection to their customers, all housed within the necessary function of a router.**

Memory and Performance Impact

- The **performance impact of intrusion detection will depend on the configuration of the signatures, the level of traffic on the router, the router platform, and other individual features enabled on the router such as encryption, source route bridging**, and so on.
  - Enabling or disabling individual signatures will not alter performance significantly, however, signatures that are configured to use **Access Control Lists** will have a significant performance impact.
- **For auditing atomic signatures, there is no traffic-dependent memory requirement.**
- **For auditing compound signatures, CBAC allocates memory to maintain the state of each session for each connection.**
- Memory is also allocated for the configuration database and for internal caching.

IOS Firewall IDS Signature List

- Cisco IOS Firewall IDS, signatures are categorized into four types:
  - Info Atomic
  - Info Compound
  - Attack Atomic
  - Attack Compound
- An info signature detects information-gathering activity, such as a port sweep.
- An attack signature detects attacks attempted into the protected network, such as denial-of-service attempts or the execution of illegal commands during an FTP session.
- Info and attack signatures can be either atomic or compound signatures.
  - Atomic signatures can detect patterns as simple as an attempt to access a specific port on a specific host.
  - Compound signatures can detect complex patterns, such as a sequence of operations distributed across multiple hosts over an arbitrary period of time.
- The intrusion-detection signatures included in the Cisco IOS Firewall were chosen from a broad cross-section of intrusion-detection signatures as representative of the most common network attacks and information-gathering scans that are not commonly found in an operational network.

Example – Signature List

Signature	Description
1000 IP options-Bad Option List (Info, Atomic)	Triggers on receipt of an IP datagram where the list of IP options in the IP datagram header is incomplete or malformed.
1001 IP options-Record Packet Route (Info, Atomic)	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 7 (Record Packet Route).
1002 IP options-Timestamp (Info, Atomic)	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 4 (Timestamp).
. . .	. . .
8000 FTP Retrieve Password File (Attack, Atomic*)	Triggers on string "passwd" issued during an FTP session. May indicate someone attempting to retrieve the password file from a machine in order to crack it and gain unauthorized access to system resources.

Configuring IDS

Step 1. Initialization configuration

Step 2. Logging or PostOffice configuration

Step 3. Audit rule configuration and activation

Configuring IDS

Step 1: Initialization Configuration

- Router(config)# ip audit po max-events #_of_events
- Router(config)# ip audit smtp spam #_of_recipients
- The ip audit po max-events command limits the number of IDS events that the Cisco IOS queues up to send to a remote device.
- By default, this is 250 events, but this can range from 1 to 65,535.
- This limit is used to ensure that if a hacker tried to flood a router with a lot of attacks, the router would not overload itself in trying to process all of them.
- Otherwise, this basically would allow the hacker to create a DoS attack against the router itself.

PO - The PostOffice protocol provides a critical communication link between your Director platform and your IDS sensors

Configuring IDS

Step 1: Initialization Configuration

- The ip audit smtp spam command is used to limit e-mail spamming that uses mass mailings.
- With this command, the default number of recipients allowed in an e-mail message is 250. If an e-mail message contains more than this value, the router takes the configured action
- The number of recipients can range from 1 to 65,535.

Configuring IDS

Step 2: Logging and PostOffice Configuration

- The Cisco IOS can use two methods when logging IDS events:
  - log the information using syslog or log the information using an IDS Director.
  - Using syslog, the Cisco IOS can log information locally (the console or the internal buffer) or remotely (a syslog server).
  - If you want to use the syslog method, you must configure the following IDS statement:

```
Router(config)# ip audit notify log
```

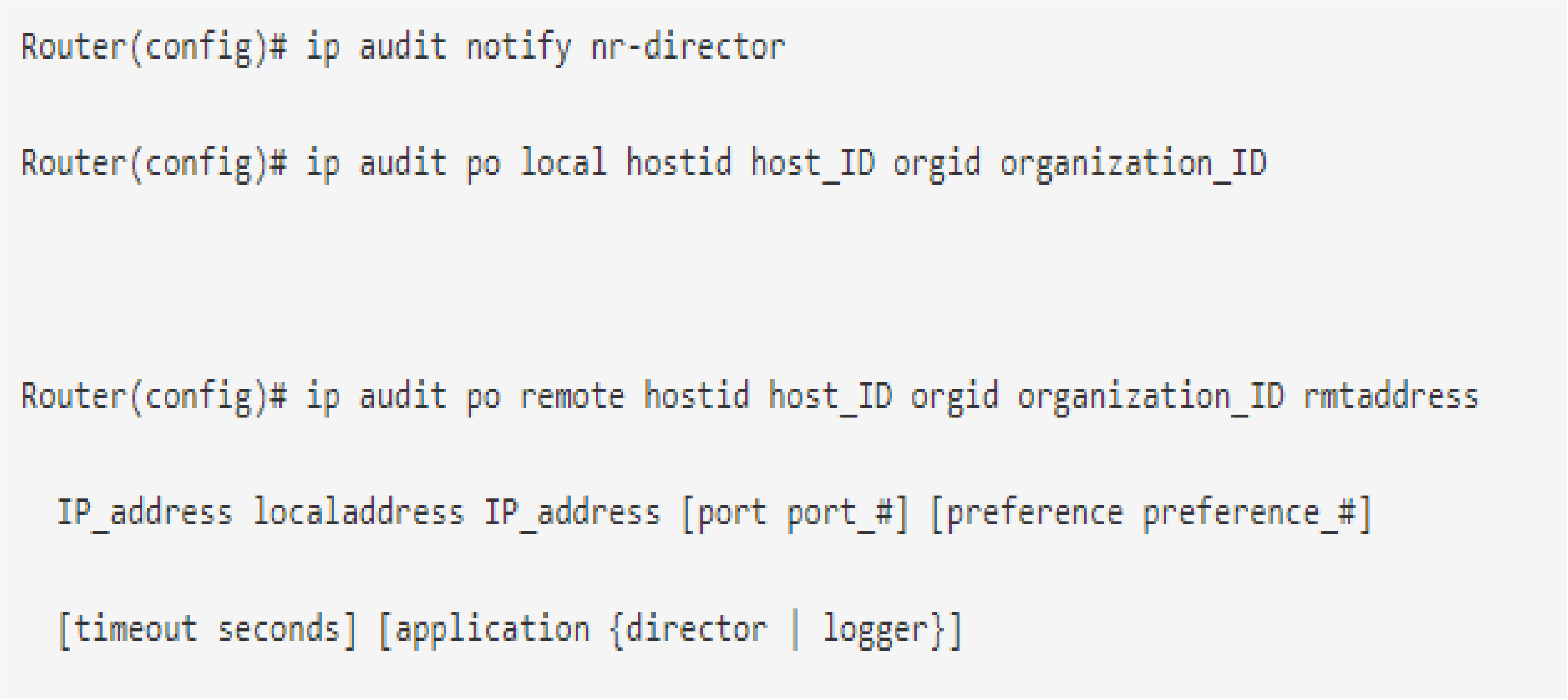
Configuring IDS

- When logging informational signatures to the router's console, you also need to execute the following command:

```
Router(config)# logging console info
```

Configuring IDS

- Second logging option is to log information to an IDS Director,



```
Router(config)# ip audit notify nr-director

Router(config)# ip audit po local hostid host_ID orgid organization_ID



Router(config)# ip audit po remote hostid host_ID orgid organization_ID rmtaddress

  IP_address localaddress IP_address [port port_#] [preference preference_#]

  [timeout seconds] [application {director | logger}]
```

Configuring IDS

- The ip audit notify nr-director command enables the logging of IDS events to an IDS Director product.
- The ip audit po local command specifies the PostOffice configuration for the router
- the ip audit po remote command specifies the configuration for the remote Director device.

Configuring IDS

- With PostOffice, each device needs a unique combination of a host ID and an organization ID.
- The organization ID is used to group sensors.
  - In smaller companies, normally only a single organization ID is necessary.
  - For enterprise companies, you might have different organization IDs for each division, allowing for easier management of your sensor products.
- Within each organization, a device needs a unique host ID. This concept is similar to IP addressing, in which you have network numbers and hosts within a network. Both of these IDs range from 1 to 65,535.

Configuring IDS

Step 3: Audit Rule Configuration and Activation

- When you have defined your logging method, you are ready to create your IDS auditing rules. Two sets of commands are used to configure audit rules: global (default actions) and specific.
- Global Policies
  - Global policies are used to take the appropriate actions for matching on signatures, unless a specific rule designates otherwise. To create your global policies, use these two commands:
    - Router(config)# ip audit info {action [alarm] [drop] [reset]}
    - Router(config)# ip audit attack {action [alarm] [drop] [reset]}

Configuring IDS

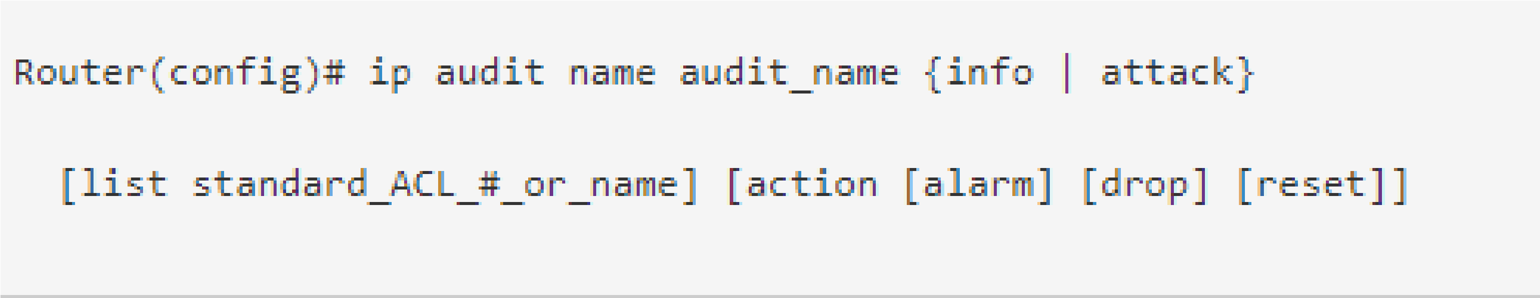
- As you can see, the two commands specify actions for informational and attack signatures. Each has three possible actions that the router can take:
  - alarm? Generate an alarm (log), where this is the default action
  - drop? Drop the packet
  - reset? For TCP connections, tear down the connection
- These commands need to be configured only if you want to change the default action (alarm) and you want the Cisco IOS IDS engine to use the same policy for all traffic of the same signature category.

Configuring IDS

- **Specific Policies**
  - Besides globally changing the behavior or IDS, you can create specific IDS auditing policies.
  - Typically, you do this if you have two interfaces on your router? perhaps one connected to the Internet and the other to a remote site? and you want to set up different IDS policies (actions to signature matches) for each interface.

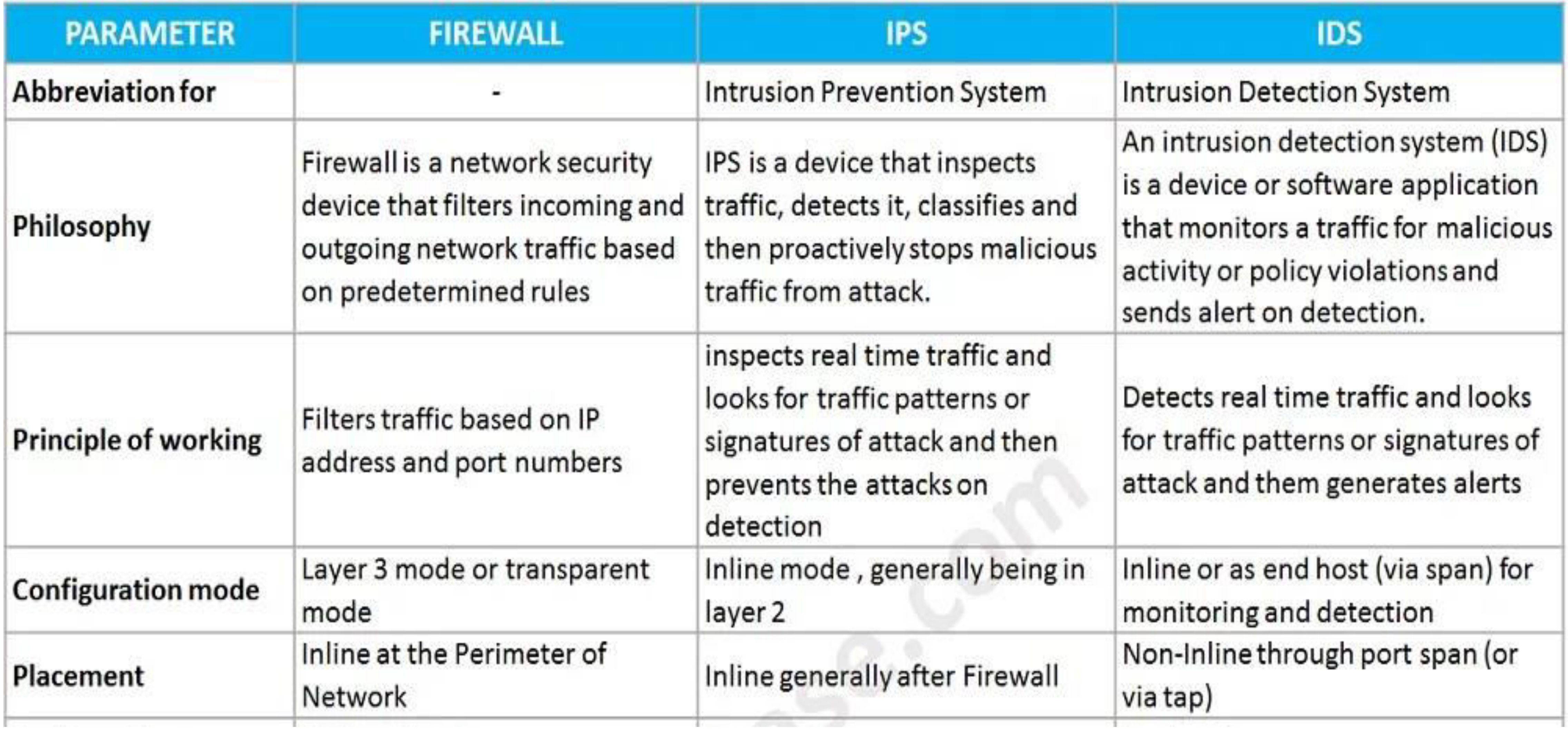
Configuring IDS

- **Specific Policies**
  - Here is the command syntax to set up your specific IDS auditing policies:



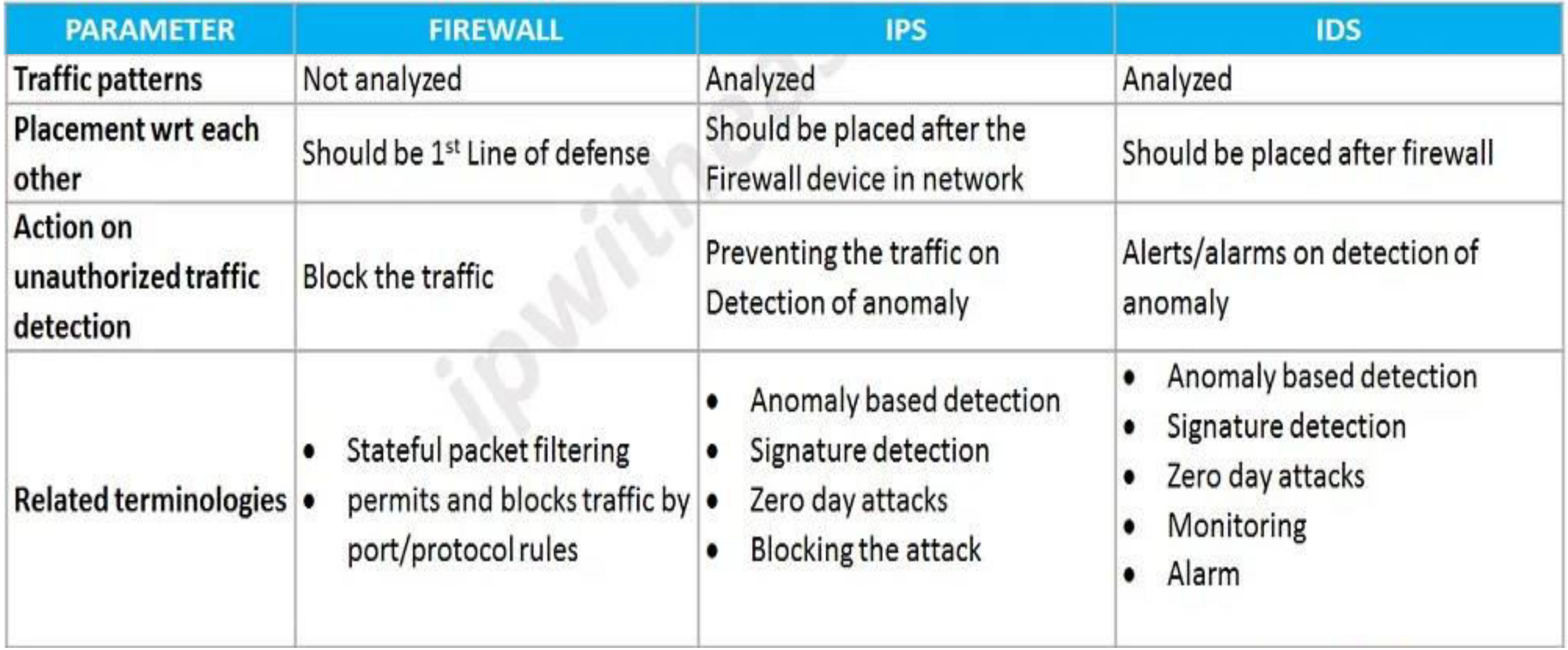
```
Router(config)# ip audit name audit_name {info | attack}

  [list standard_ACL_#_or_name] [action [alarm] [drop] [reset]]
```

Firewalls Vs IPS Vs IDS



PARAMETER	FIREWALL	IPS	IDS
Abbreviation for	-	Intrusion Prevention System	Intrusion Detection System
Philosophy	Firewall is a network security device that filters incoming and outgoing network traffic based on predetermined rules	IPS is a device that inspects traffic, detects it, classifies and then proactively stops malicious traffic from attack.	An intrusion detection system (IDS) is a device or software application that monitors a traffic for malicious activity or policy violations and sends alert on detection.
Principle of working	Filters traffic based on IP address and port numbers	inspects real time traffic and looks for traffic patterns or signatures of attack and then prevents the attacks on detection	Detects real time traffic and looks for traffic patterns or signatures of attack and them generates alerts
Configuration mode	Layer 3 mode or transparent mode	Inline mode , generally being in layer 2	Inline or as end host (via span) for monitoring and detection
Placement	Inline at the Perimeter of Network	Inline generally after Firewall	Non-Inline through port span (or via tap)

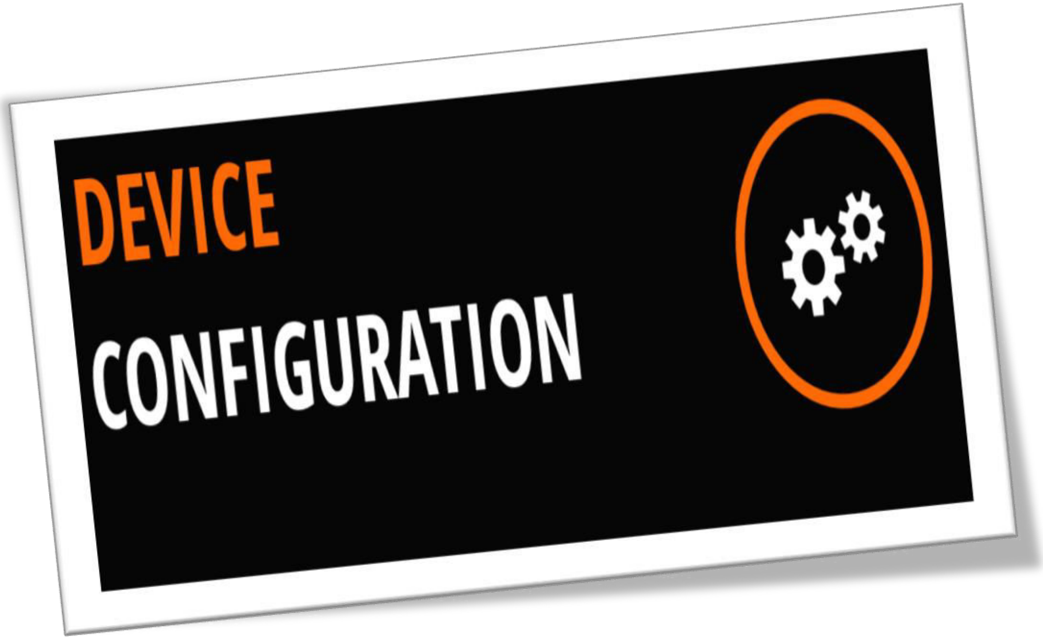
Firewalls Vs IPS Vs IDS



PARAMETER	FIREWALL	IPS	IDS
Traffic patterns	Not analyzed	Analyzed	Analyzed
Placement wrt each other	Should be 1st Line of defense	Should be placed after the Firewall device in network	Should be placed after firewall
Action on unauthorized traffic detection	Block the traffic	Preventing the traffic on Detection of anomaly	Alerts/alarms on detection of anomaly
Related terminologies	• Stateful packet filtering • permits and blocks traffic by port/protocol rules	• Anomaly based detection • Signature detection • Zero day attacks • Blocking the attack	• Anomaly based detection • Signature detection • Zero day attacks • Monitoring • Alarm

BCSE354E - Information Security Management

Module 3.c - Device Configuration



Contents

1. Common issues in installing or configuring information security devices

2. Methods to resolve these issues

3. Methods of testing installed/configured information security devices

Common Router problems and solutions

1. Correct your Wi-Fi Security Settings
2. Update your Hardware or Firmware
3. Fix Overheating or Overloading
4. Remove MAC Address Restrictions
5. Check Wireless Signal Limitations

Common Router problems and solutions

1. Correct your Wi-Fi Security Settings

   - **Network Mode:** The router must be allowed to accommodate all Wi-Fi models used by network clients. For example, routers designed to run in 802.11g mode only will not support 802.11n or old 802.11b devices. Adjust the router to run in mixed mode to remedy this kind of network failure.

   - **Security Mode:** Most Wi-Fi devices support several network security protocols (typically different variations of WPA and WEP). All Wi-Fi devices, including routers belonging to the same local network, shall use the same protection mode.

   - **Security key:** Wi-Fi security keys are phrases or sequences of letters and digits. All devices that enter the network must be configured to use the Wi-Fi key recognized by the router (or wireless access point).

Common Router problems and solutions

2. Update your Hardware or Firmware

- The reason for this step is twofold. You can take benefit of any additional features and improvements of the new version of the firmware. Also, your router will normally receive any critical security updates.

- Typically, you will have the choice of checking, evaluating, downloading, and installing the latest firmware on your router's administration tab. The exact steps depend on the make and model of your router, so check the specifics of the router manufacturer's support site.

Common Router problems and solutions

3. Fix Overheating or Overloading

- You can set up a different Wi-Fi router or allow the "Guest Network" option for your router.
- You can also set up a separate SSID and password for your host network to avoid issues with your main network.
- This segregation would also work with your smart appliances and secure your key devices from attacks on the Internet of Things.
- You can also use QoS (Quality of Service). QoS is a feature on some routers that lets you prioritize traffic according to the type of data being transmitted.

Common Router problems and solutions

4. Remove MAC Address Restrictions

- A number of network routers support a function called MAC address filtering.
- While disabled by default, router administrators can turn this function on and limit connections to only those devices by their MAC address number.
- Check the router to ensure that either the MAC address filtering is off or the MAC address of the computer is included in the list of allowed connections.

Common Router problems and solutions

5. Check Wireless Signal Limitations

- If you have a newer router, check if it supports the 5GHz band. Newer routers typically have dual-band capabilities.
- By allowing dual bands, you could hold older devices that only support slower G specification on the 2.4GHz band and newer devices on the beefier and faster 5GHz band.
- Essentially, this is like having two routers in one.

Common Router problems and solutions

- Basic Faults

  - Physical Layer Stuff
  - Check the Interfaces
  - Ping
  - Check the Routing Table
  - Is there a Firewall on the Computer?
  - Any Access Lists?
  - Is the VPN Up?
  - Do the Protocols Match?
  - Check for Human Error
  - Verify Settings

Common Router problems and solutions

- Physical Layer Stuff:
  - Check power issues. Look for power lights, check plugs, and circuit breakers.

- Check the Interfaces:
  - Use the command show ip interface brief or show ipv6 interface brief to ensure that desired interfaces are up and configured properly.

Common Router problems and solutions

- Ping:
  - Use the ping and trace commands to check for connectivity.
- Check the Routing Table:
  - Use the show ip route or show ipv6 route command to find out what the router knows. Is there either an explicit route to the remote network or a gateway of last resort?

Common Router problems and solutions

- Is there a Firewall on the Computer?
  - If the problem involves a computer, check to ensure that its firewall is not blocking packets.
  - Sometimes there are computers at client locations with firewalls in operation without the client's knowledge.

Common Router problems and solutions

- Any Access Lists?
  - If the above steps don’t resolve the issue, check for access-control lists that block traffic.
  - There is an implicit “deny any” at the end of every access-control list, so even if you don’t see a statement explicitly denying traffic, it might be blocked by an implicit “deny any.”

Common Router problems and solutions

- Is the VPN Up?
  - If a VPN is part of the connection, check to ensure that it is up. Use the show crypto family of commands to check VPN connections.
  - With VPN connections, each end of the connection must mirror the other.
  - For example, even something as seemingly inconsequential as a different timeout value or a different key lifetime can prevent a connection.

Common Router problems and solutions

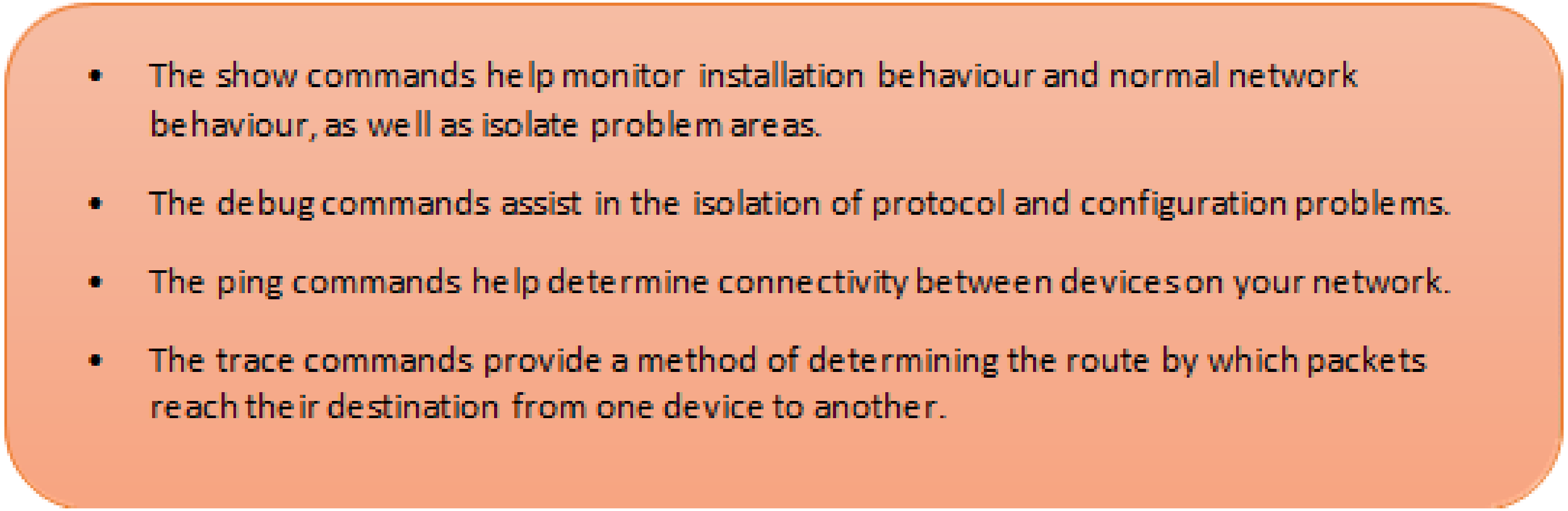
- Do the Protocols Match?
  - If you are trying to gain remote access to a server, ensure that it supports the protocol you’re attempting to use.
  - For example, if the router hasn’t been configured to support SSH and you use the default settings in PuTTY which call for SSH, you won’t be able to connect.
  - Also, some admins change the default port numbers, so you may expect to use port 22 with SSH, but the admin may have configured it to use a non-standard port.

Common Router problems and solutions

- Check for Human Error:
  - User errors can also be the source of errors. Check to ensure that correct usernames and passwords are being used, that you and the admin on the other end of the connection are using the same network addresses and matching subnet masks.
- Verify Settings:
  - Do not make assumptions. Verify everything!

Router Troubleshooting Tools

- **Using Router Diagnostic Commands**
  - Cisco routers provide numerous integrated commands to assist you in monitoring and troubleshooting your internetwork.



- The show commands help monitor installation behaviour and normal network behaviour, as well as isolate problem areas.
- The debug commands assist in the isolation of protocol and configuration problems.
- The ping commands help determine connectivity between devices on your network.
- The trace commands provide a method of determining the route by which packets reach their destination from one device to another.

Router Troubleshooting Tools

- **Using show Commands**
  - The **show** commands are powerful monitoring and troubleshooting tools.
    - Monitor router behaviour during initial installation
    - Monitor normal network operation
    - Isolate problem interfaces, nodes, media, or applications
    - Determine when a network is congested
    - Determine the status of servers, clients, or other neighbours

Router Troubleshooting Tools

- **Using debug Commands**
  - The **debug** privileged exec commands can provide a wealth of information about the traffic being seen (or *not* seen) on an interface, error messages generated by nodes on the network, protocol-specific diagnostic packets, and other useful troubleshooting data.
  - In many situations, using third-party diagnostic tools can be more useful and less intrusive than using **debug** commands.

Router Troubleshooting Tools

- **Using the ping Command**
    - To check host reachability and network connectivity, use the **ping** exec (user) or privileged exec command.
    - After you log in to the router or access server, you are automatically in user exec command mode. The exec commands available at the user level are a subset of those available at the privileged level.
    - In general, the user exec commands allow you to connect to remote devices, change terminal settings on a temporary basis, perform basic tests, and list system information.
    - The **ping** command can be used to confirm basic network connectivity on AppleTalk, ISO Connectionless Network Service (LNS), IP, Novell, Apollo, VINES, DECnet, or XNS networks.

Router Troubleshooting Tools

- **Using the trace Command**
  - The **trace user exec** command discovers the routes that a router's packets follow when traveling to their destinations.
  - The **trace privileged exec** command permits the supported IP header options to be specified, allowing the router to perform a more extensive range of test options.