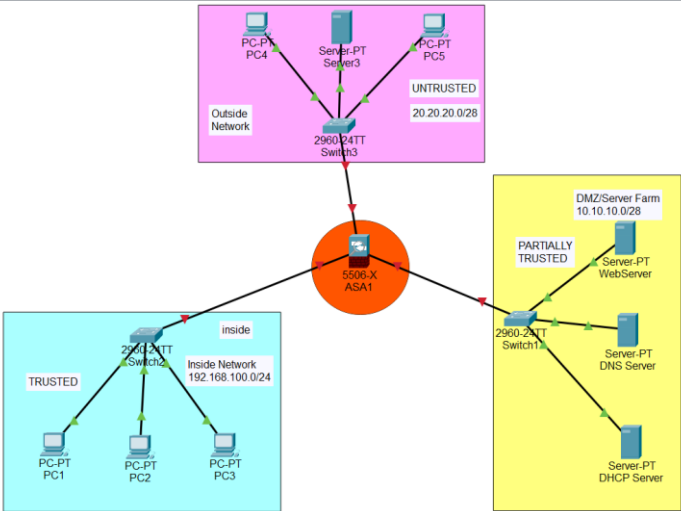


Q.No.	Question
1.	<p>You are the network security administrator for a medium-sized company that recently suffered a cyber attack due to unauthorized access to its internal network. The management has tasked you with enhancing the network security infrastructure. As part of this initiative, you need to configure a firewall to restrict incoming and outgoing traffic effectively. Based on the scenario provided, outline the steps you would take to configure the firewall to prevent unauthorized access to the internal network while ensuring legitimate traffic flow. Draw an architecture diagram for this scenario and discuss the importance of firewall rules, NAT (Network Address Translation), and stateful inspection in this configuration.</p>
Key-1	<p>Topic: Firewall</p> <p>1. Architecture diagram (2 Marks)</p>  <p>2. Configuration of firewall (5 Marks)</p> <p>Basic Configuration for each interface (3)</p> <p>Inside , DMZ, Outside</p> <pre> FIREWALL(config)#interface gig1/1 FIREWALL(config-if)#no shut FIREWALL(config-if)#ip add 192.168.100.1 255.255.255.0 FIREWALL(config-if)#nameif INSIDE INFO: Security level for "INSIDE" set to 0 by default. FIREWALL(config-if)#security-level 100 FIREWALL(config-if)# </pre> <p>Hostname, password, clock (1),</p> <pre> ciscoasa(config)#hostname FIREWALL FIREWALL(config)# FIREWALL(config)#enable password admin FIREWALL(config)# </pre>

	<pre> FIREWALL(config)#username usr1 password usr123 FIREWALL(config)#clock set 08:00:30 23 Feb 2024 FIREWALL(config)#  Saving and display(1) FIREWALL(config-if)#write mem Building configuration... [OK] FIREWALL(config-if)#show start : Saved </pre> <p><b>3. Importance of firewall rules, NAT, Stateful Inspection (3 Marks)</b></p> <p>Why Firewall (1)  Why NAT (1)  Why Stateful Inspection (1)</p>
2.	<p>ABC Corp., operates across several continents with numerous branch offices interconnected through a Wide Area Network (WAN). Recently, there have been concerns about the security of data transmitted between these offices, particularly sensitive financial information. ABC Corp.'s situation, describe, which methodology can be utilized to ensure secure communication between geographically dispersed offices over the WAN. Discuss the technical specifications and configuration parameters necessary to implement the solution effectively. Additionally, explain how that particular methodology contributes to maintaining the confidentiality, integrity, and authenticity of data transmissions in such a distributed environment.</p> <p>Topic: VPN</p> <p><b>which methodology? (2)</b></p> <p>Explanation of VPN Mythology</p> <p>Technical specifications and configuration parameters (5)</p> <p><b>Basic configuration on routers (1)</b></p> <p><b>Tunnel specific configuration (4 Marks) on both routers (R1 and R3)</b></p> <pre> r1#config t r1(config)#interface tunnel 10 r1(config-if)#ip address 172.16.1.1 255.255.0.0 r1(config-if)#tunnel source fa0/1 r1(config-if)#tunnel destination 2.0.0.2 r1(config-if)#no shut </pre> <p><b>Check the tunnel using traceroute (1 Mark)</b></p> <pre> C:\&gt;tracert 192.168.1.2 Tracing route to 192.168.1.2 over a maximum of 30 hops: </pre>

	<p>1 0 ms 0 ms 108 ms 192.168.2.1  2 0 ms 1 ms 0 ms 172.16.1.1  3 0 ms 0 ms 0 ms 192.168.1.2</p> <p>Trace complete.</p> <p>How CIA? (2)</p> <p>Confidentiality:  VPNs use encryption to create a secure connection over unsecured internet infrastructure. This means that all data transmitted over the VPN is scrambled and can only be understood by authorized parties. The encryption mechanism prevents data from being intercepted during transmission. Even if a criminal intercepts the data, all they can see is the encrypted version of the data.</p> <p>Integrity:  VPNs ensure the integrity of your data by employing a technique called tunnelling. Your VPN encrypted data is encapsulated within an additional layer of security, forming a secure tunnel between your device and the VPN server  A security authentication header or encapsulation security payload is used to encrypt and authenticate the data to ensure its integrity. This means that the data cannot be tampered with during transmission.</p> <p>Availability:  Availability refers to the data being accessible when it is required. All three of these security attributes are critical if we want to keep attackers out of our data, while still being able to access it when we need it. VPN helps in maintaining availability in several ways:</p> <p>Remote Access:  Reliability:  Performance:</p>
3.	<p>A financial institution has experienced multiple security breaches, resulting in significant financial losses and reputational damage. As part of the security enhancement strategy, the management has decided to deploy a System to monitor network traffic and detect malicious activities. Draw an architecture diagram for this scenario and discuss the role of the system in network security and its deployment strategies. Explain how the detection methods can be used to identify potential security threats in the network.</p> <p>Topic: IDS</p> <p>Draw an architecture diagram for this scenario and discuss the role of the system in network security and its deployment strategies (5)</p>

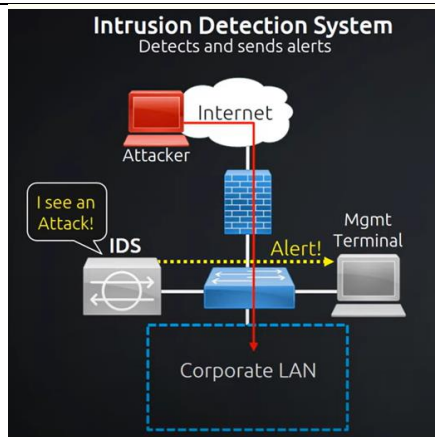
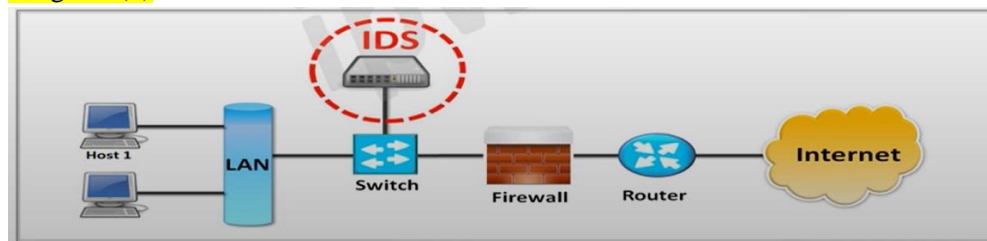


Diagram (3)



Explanation (2)

Explain how the detection methods can be used to identify potential security threats in the network. (5)

“IP Audit”

- ip audit info: Configures the IDS to audit informational level events
- ip audit attack: Configures the IDS to audit attack level events
- ip audit name: Defines an IDS audit rule and enters IDS audit configuration mode
- ip audit interface: Applies an IDS audit rule to an interface
- ip audit notify: Configures the IDS to send audit notifications
- ip audit smtp spam: Configures the IDS to detect and log Simple Mail Transfer Protocol (SMTP) spam

Router(config)# ip audit po max-events 100

Router(config)# ip audit smtp spam 100

Router(config)# ip audit notify log

Router(config)# ip audit notify director

Router(config)# logging console

Router(config)# logging console info

Router(config)# logging host 192.168.0.10

Router(config)# ip audit po local hostid host-id orgid org-id

Router(config)# ip audit po remote hostid host-id orgid org-id rmtaddress remote-address localaddress local-address port port-number preference preference timeout timeout application application

- Router(config)# ip audit info {action [alarm] [drop] [reset]}
- Router(config)# ip audit attack {action [alarm] [drop] [reset]}

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

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

#### Packet Tracer

Router(config)#show version

#### **Enable security technology**

Router(config)#license boot module c1900 technology-package securityk9

Router(config)#do reload

#### **Create a folder - ipsdir**

Router(config)#mkdir ipsdir

#### **Configure IPS signature location ipsdir**

Router(config)#ip ips config location ipsdir

#### **Configure IPS Rule**

Router(config)#ip ips name iosips

#### **Retire IPS Category**

Router(config)#ip ips signature-category

Router(config-ips-category)#category all

Router(config-ips-category-action)#retired true

#### **Enable IOS\_IPS Category , Basic signature**

Router(config-ips-category-action)#exit

Router(config-ips-category)#category ios\_ips basic

Router(config-ips-category-action)#retired false

#### **Install the IPS on interface, outbound traffic**

Router(config)#interface gigabitEthernet 0/1

Router(config-if)#ip ips iosips out

Router(config-if)#exit

#### **Configure log message to syslog server**

Router(config)#logging host 192.168.1.2

#### **Synchronize clocks on all devices**

Router(config)#service timestamps log datetime msec

**Signature definitions**

```
Router(config)#ip ips signature-definition
Router(config-sigdef)#signature 2004 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enabled true
```

**Signature alerts for packet drop**

```
Router(config-sigdef-sig)#engine
Router(config-sigdef-sig-engine)#event-action produce-alert
Router(config-sigdef-sig-engine)#event-action deny-packet-inline
```

Imagine you are the cybersecurity engineer tasked with safeguarding a financial institution grappling with a surge in targeted cyber attacks aimed at stealing sensitive customer data. Using a scenario-based approach, outline the configuration of an advanced security system to actively obstruct malicious traffic and prevent unauthorized access to critical systems. Detail the mechanisms that you would employ to customize the system according to your company's unique security requirements, placing emphasis on the creation of tailored policies or filters. Additionally, discuss strategies for ensuring the system remains adaptable and responsive to evolving cybersecurity threats.

Topic: IPS

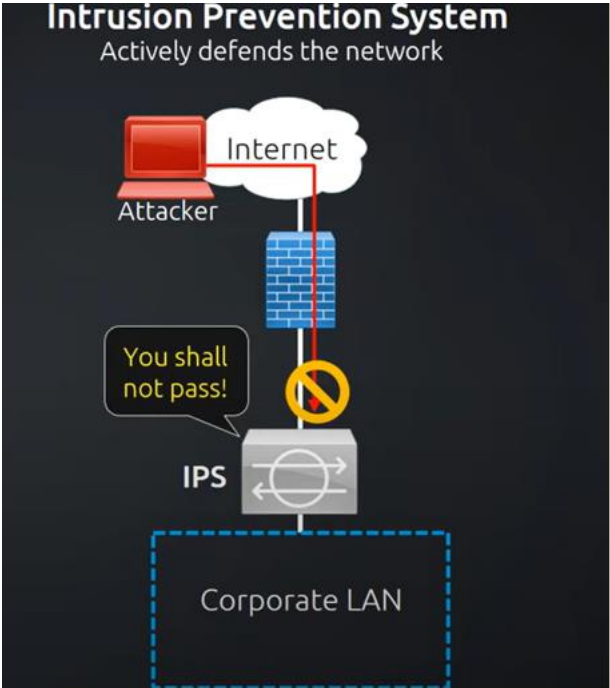
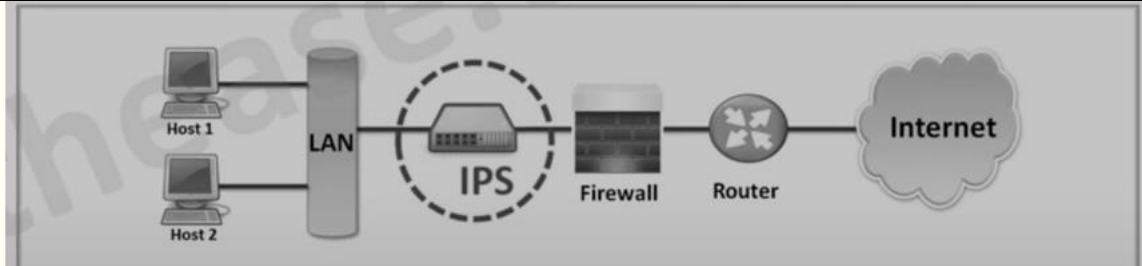


Diagram (3)



Explanation (3)

customize the system according to your company's unique security requirements, placing emphasis on the creation of tailored policies or filters (2 Marks)

**Signature-Based Detection:** Customize the IPS to recognize known threat signatures. Regularly update the signature database to keep up with new threats.

**Anomaly-Based Detection:** Configure the IPS to recognize normal network behavior. Any significant deviation could indicate a potential threat.

**Policy-Based Detection:** Create custom policies based on the company's security requirements. For example, block traffic from certain IP addresses or limit access to sensitive parts of the network

Strategies for ensuring the system remains adaptable and responsive to evolving cybersecurity threats.(2 Marks)

**Threat Intelligence Integration:** Integrate the IPS with threat intelligence services. This provides real-time information about emerging threats, allowing the IPS to adapt its defenses accordingly.

**Machine Learning:** Some modern IPSs use machine learning algorithms to identify new threats. This can help the system adapt to evolving cybersecurity threats.

**Regular Updates and Patches:** Keep the IPS software up-to-date to ensure it can protect against the latest known threats.

Discuss the installation, configuration methodologies, and troubleshooting procedures for router information security devices. Identifying common issues that may arise during installation or configuration, and explaining how to resolve these issues effectively.

Topic: installation, configuration methodologies, and troubleshooting procedures for router

Configuration (3 Marks)

5.

Router Basic configuration

Router Interfaces Configuration

Routing configuration

Access Control and other configuration

**Router problems and solutions (4 Marks)**

*Physical*

*Routing Table*

*Check the interfaces*

*Is there a Firewall?*

*Connectivity Issues*

*Any Access Lists*

*VPN enabled?*

*Protocols Match?*

**Troubleshooting (3 Marks) with examples**

*Show (2 examples)*

*Debug (2 examples)*

*Ping, Traceroute*