Chapters 25 – 26: Access Control and Infrastructure Security Exam (Answers)

itexamanswers.net/chapters-25-26-access-control-and-infrastructure-security-exam-answers.html

December 20, 2020

CCNPv8 ENCOR (Version 8.0) – Access Control and Infrastructure Security Exam

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. Which place in the network (PIN) is considered to be the highest-risk, as it is the ingress and egress point for internet traffic?

- cloud
- data center
- WAN
- **edge**

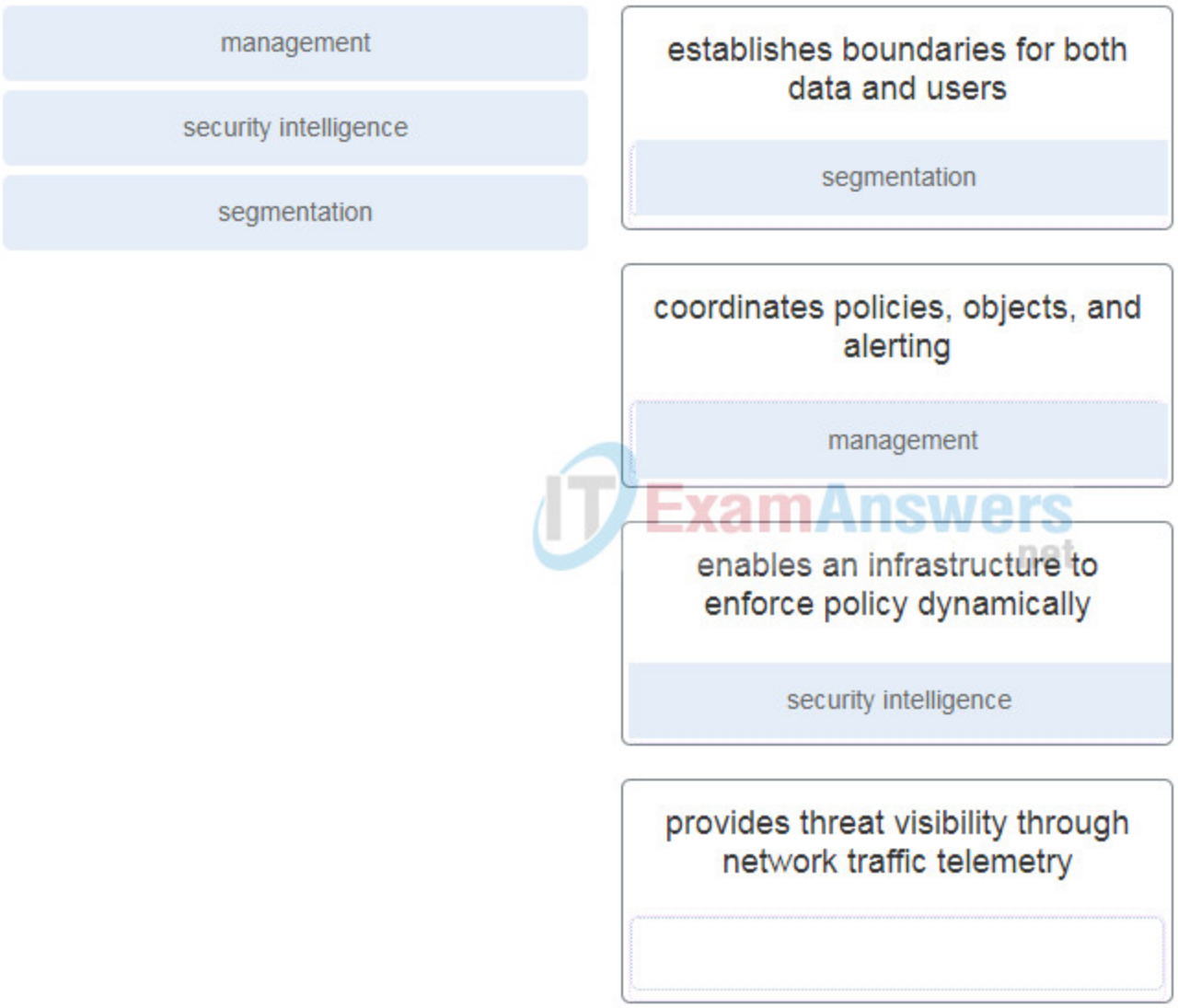
Explanation: The network edge is the ingress and egress point for traffic to and from the internet. It is the most important place in the network (PIN) for e-commerce and is also the highest-risk PIN.

2. What threat protection actions are involved in the "before" phase of the attack continuum?

- defining the abilities and actions that are required when an attack gets through
- **establishing policies and implementing prevention measures to reduce risks**
- detecting, containing, and remediating attacks
- conducting threat analysis and incident response

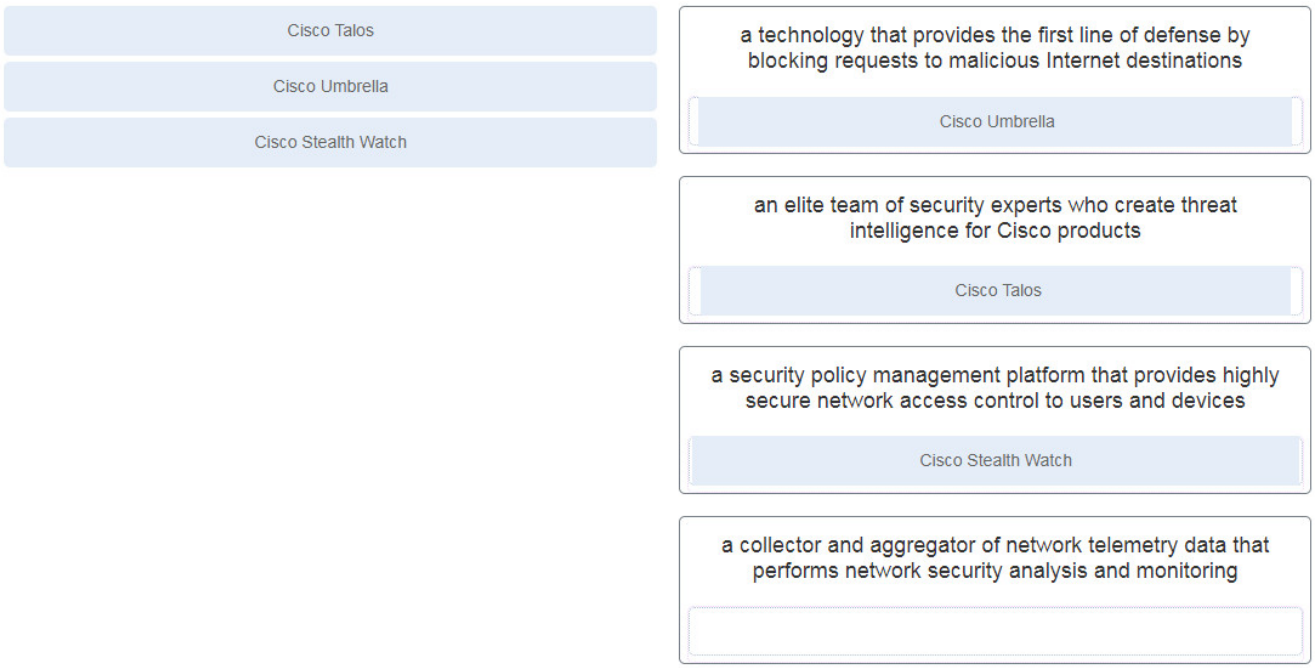
Explanation: Threat protection activities before a network attack include establishing the policies and implementing prevention solutions that can reduce risk.

3. Question as presented: Match the Cisco Safe security concepts to the description. (Not all options are used.)



- segmentation – establishes boundaries for both data and users
- management – coordinates policies, objects, and alerting
- security intelligence – enables an infrastructure to enforce policy dynamically
- provides threat visibility through network traffic telemetry

4. Question as presented: Match the Cisco SAFE component with the description. (Not all options are used.)



- a technology that provides the first line of defense by blocking requests to malicious Internet destinations
- an elite team of security experts who create threat intelligence for Cisco products
- a security policy management platform that provides highly secure network access control to users and devices
- a collector and aggregator of network telemetry data that performs network security analysis and monitoring

5. Which solution provides comprehensive network and data protection for organizations before, during, and after a malware attack?

- Cisco Umbrella
- Cisco ISE
- **Cisco AMP**
- Cisco Stealthwatch

Explanation: Cisco Advanced Malware Protection (AMP) is a malware analysis and protection solution that provides comprehensive protection for organizations across the full attack continuum: before, during, and after.

6. Which solution provides VPN access for clients and performs an assessment of the VPN client security posture compliance?

- Cisco Umbrella
- Cisco AMP
- Cisco Talos
- **Cisco AnyConnect**

Explanation: Cisco AnyConnect is a client software product that provides VPN access to clients and also is capable of assessing endpoint compliance with antivirus, antispyware, and firewall software installed on the host.

7. What security capability is provided by applying Cisco WSA web reputation filters before an attack?

- **prevents client devices from accessing dangerous websites containing malware or phishing links**
- uses URL filtering to shut down access to websites known to host malware
- provides administrators with granular control over web and mobile application usage behavior
- inspects the network continuously for instances of undetected malware and breaches

Explanation: Cisco Web Security Appliance (WSA) provides a variety of protections across the attack continuum before, during, and after an attack. Before an attack Cisco WSA uses web reputation filters to prevent client devices from accessing dangerous websites containing malware or phishing links and to block those that fall below a defined security threshold.

8. Which security appliance passively monitors and analyzes network traffic for potential network intrusion attacks and logs the attacks for analysis?

- next-generation firewall
- web security appliance
- **intrusion detection system**
- intrusion prevention system

Explanation: An intrusion detection system (IDS) is a system that passively monitors and analyzes network traffic for potential network intrusion attacks and logs the intrusion attack data for security analysis.

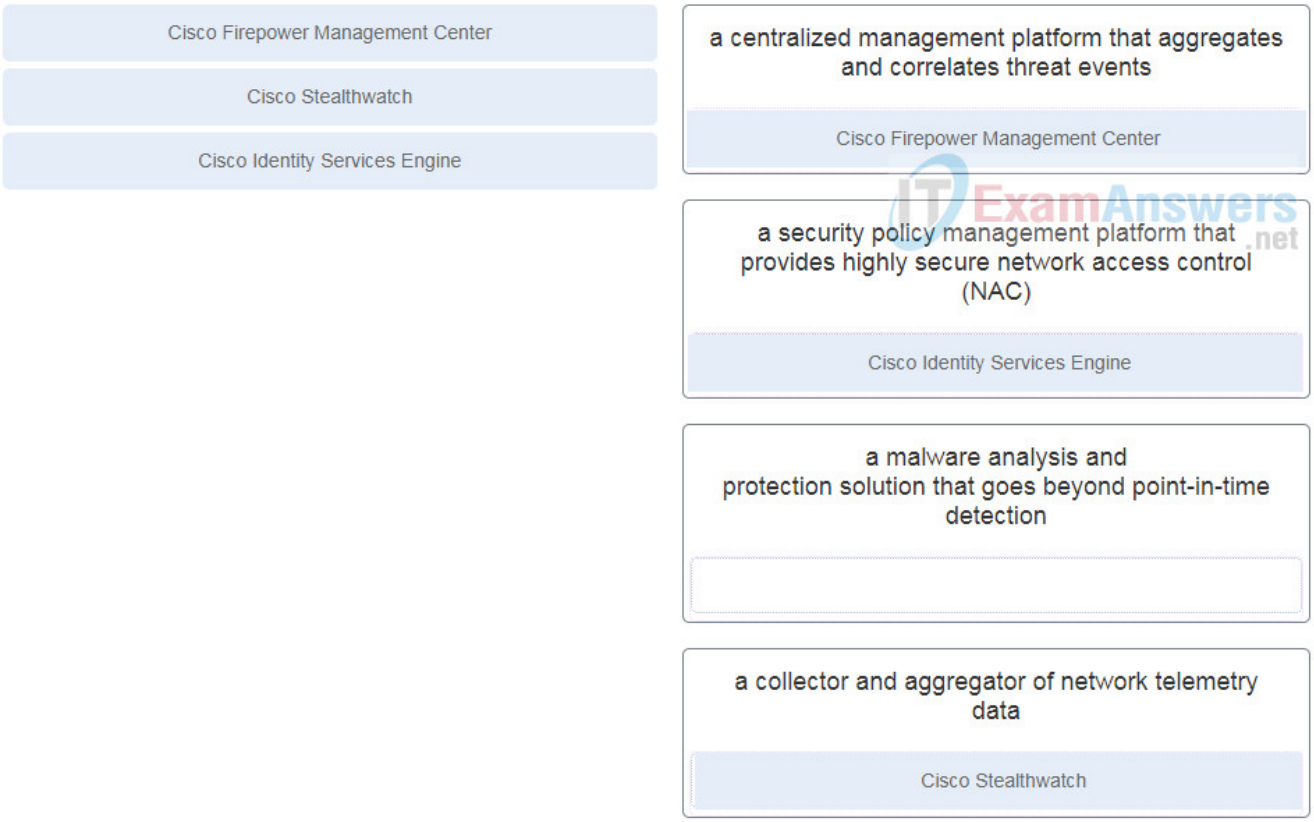
9. According to Gartner, Inc. what three capabilities must a next-generation firewall (NGFW) provide in addition to standard firewall features? (Choose three.)

- **the ability to perform application-level inspection**
- real-time contextual awareness
- incident response and forensics
- **the ability to leverage external security intelligence**
- **an integrated IPS**
- the ability to identify users who click malicious URLs

Explanation: In addition to IPS functionality, Gartner Inc. states a next-generation firewall (NGFW) should include the following capabilities:

- An integrated IPS
- Application-level inspection
- The ability to leverage external security intelligence to address evolving security threats

10. Question as presented: Match the security platform to the description. (Not all options are used.)



- a centralized management platform that aggregates and correlates threat events
- a security policy management platform that provides highly secure network access control (NAC)
- a malware analysis and protection solution that goes beyond point-in-time detection
- a collector and aggregator of network telemetry data

11. Which secure access solution can be implemented to authenticate endpoints that do not support 802.1x or MAB?

- Cisco TrustSec
- Cisco Identity-Based Network Services
- **web authentication**
- Enhanced Flexible Authentication

Explanation: Some endpoints that need access to the network may not have 802.1x supplicants and may not know the MAC address to perform MAB. This can be a problem for contractors or visitors that need internet access. In such cases web authentication can be

implemented to present a user with web portal requesting a username and password.

12. Which EAP method makes use of the Protected Extensible Authentication Protocol (PEAP)?

- EAP challenge-based authentication method
- **EAP tunneled TLS authentication method**
- EAP TLS authentication method
- EAP inner authentication method

Explanation: PEAP is used in EAP tunneled TLS authentication methods. PEAP forms an encrypted TLS tunnel between the supplicant and the authentication server and uses an EAP authentication inner method to authenticate the supplicant through the outer PEAP TLS tunnel.

13. What message is sent every 30 seconds by the 802.1x authenticator to an endpoint to initiate the MAB authentication process?

- RADIUS access-accept
- **EAPoL identity request**
- RADIUS access-request
- EAPoL start

Explanation: The authenticator initiates the 802.1x MAB authentication process by sending an EAPoL identity request message to the endpoint every 30 seconds to determine if it has a supplicant.

14. What are the three phases of TrustSec configuration? (Choose three.)

- access-request
- start
- **ingress classification**
- **propagation**
- access-accept
- **egress enforcement**

Explanation: TrustSec configuration occurs in three phases:
Ingress classification – where SGT tags are assigned to users and resources
Propagation – where mappings to the TrustSec devices are made based on SGT tags
Egress enforcement – where policies are enforced at the egress point of the TrustSec network

15. Which set of access control entries would allow all users on the 192.168.10.0/24 network to access a web server that is located at 172.17.80.1, but would not allow them to use Telnet?

access-list 103 permit tcp 192.168.10.0 0.0.0.255 host 172.17.80.1 eq 80
access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq 23

access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq 23

access-list 103 deny tcp host 192.168.10.0 any eq 23
access-list 103 permit tcp host 192.168.10.1 eq 80

access-list 103 permit 192.168.10.0 0.0.0.255 host 172.17.80.1
access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq telnet

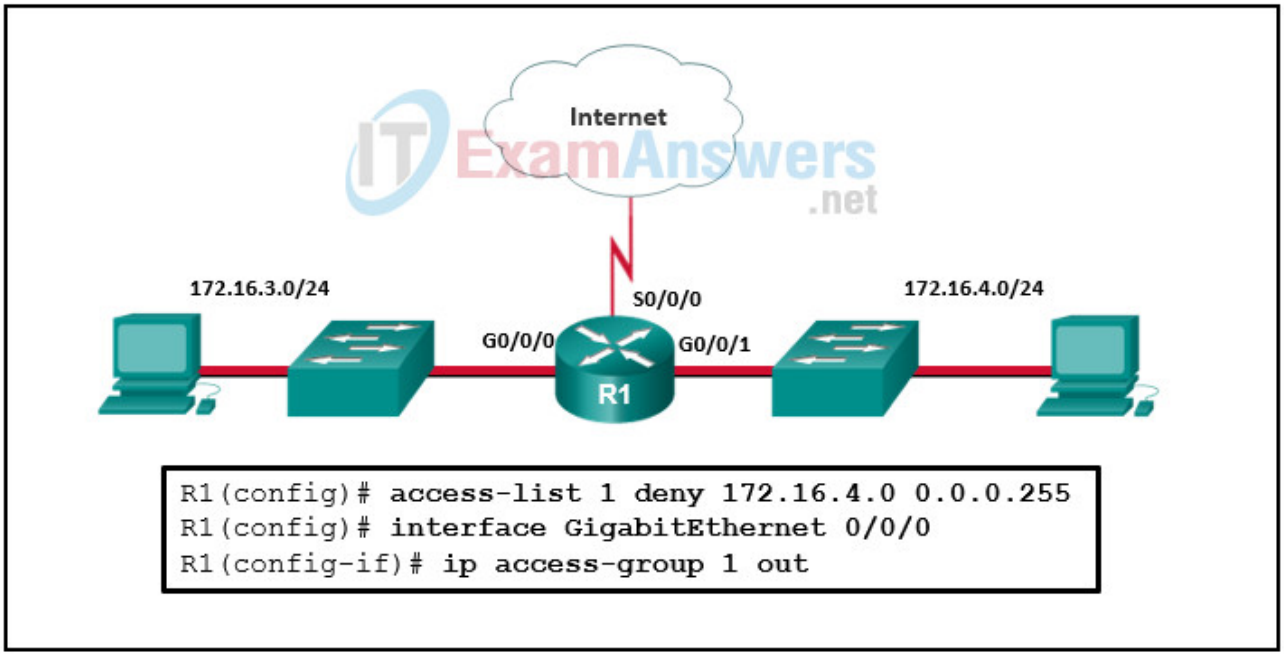
Explanation: For an extended ACL to meet these requirements the following need to be included in the access control entries:
identification number in the range 100-199 or 2000-2699
permit or deny parameter
protocol
source address and wildcard
destination address and wildcard
port number or name

16. Which three statements describe ACL processing of packets? (Choose three.)

- A packet that has been denied by one ACE can be permitted by a subsequent ACE.
- **An implicit deny any rejects any packet that does not match any ACE.**
- A packet that does not match the conditions of any ACE will be forwarded by default.
- **Each statement is checked only until a match is detected or until the end of the ACE list.**
- Each packet is compared to the conditions of every ACE in the ACL before a forwarding decision is made.
- **A packet can either be rejected or forwarded as directed by the ACE that is matched.**

Explanation: When packets are checked against an access list, each ACE in the access list is checked in sequence until a match is detected. At the end of all access lists is an implicit deny any ACE. Packets will be dropped or forwarded as directed by the matching ACE.

17. Refer to the exhibit. An ACL was configured on R1 with the intention of denying traffic from subnet 172.16.4.0/24 into subnet 172.16.3.0/24. All other traffic into subnet 172.16.3.0/24 should be permitted. This standard ACL was then applied outbound on interface G0/0/0. Which conclusion can be drawn from this configuration?



- An extended ACL must be used in this situation.
- Only traffic from the 172.16.4.0/24 subnet is blocked, and all other traffic is allowed.
- The ACL should be applied outbound on all interfaces of R1.
- **All traffic will be blocked, not just traffic from the 172.16.4.0/24 subnet.**
- The ACL should be applied to the GigabitEthernet 0/0/0 interface of R1 inbound to accomplish the requirements.

Explanation: Because of the implicit deny at the end of all ACLs, the access-list 1 permit any command must be included to ensure that only traffic from the 172.16.4.0/24 subnet is blocked and that all other traffic is allowed.

18. What are two limitations of PACLs? (Choose two.)

- only support numbered ACLs
- only support extended ACLs
- can only filter Layer 2 traffic
- **no support of ACLs that filter IPv6 packets**
- **no filtering of outbound traffic**

Explanation: PACLs have some limitations and restrictions. PACLs do not support filtering of outbound traffic on an interface and they do not support ACLs filtering IPv6. Also, PACLs do not support Layer 2 control packets like STP, CDP, or VTP and are only supported in hardware.

19. An administrator defined a local user account with a secret password on router R1 for use with SSH. Which three additional steps are required to configure R1 to accept only encrypted SSH connections? (Choose three.)

- Configure DNS on the router.
- Enable inbound vty Telnet sessions.
- **Configure the IP domain name on the router.**
- **Configure a host name other than "Router".**
- Generate two-way pre-shared keys.
- **Generate crypto keys.**

Explanation: There are three steps to configure SSH support on a Cisco router:
Step 1: Configure a hostname.
Step 2: Configure a domain name.
Step 3: Generate crypto keys.

20. Which command produces an encrypted password that is easily reversible?

- username {username} secret {password}
- username {username} algorithm-type sha256 {password}
- enable secret {password}
- **service password-encryption**

Explanation: The service password-encryption command uses a Cisco proprietary Vignere cypher algorithm which is weak and easily reversible. The enable secret and the username secret commands encrypt passwords using the MD5 hashing algorithm and the username algorithm-type sha 256 command uses a SHA-256 hashed secret and is considered uncrackable.

21. Which is the preferred method for securing device terminal lines?

- a password configured directly on the terminal lines
- username-based authentication
- **AAA authentication**
- username-based authentication restricted with an ACL

Explanation: The preferred method for securing device terminal lines is to use an AAA server. Username-based authentication is recommended as a backup. Configuring a password directly on the line is not recommended.

22. What protocol is used to encapsulate the EAP data between the authenticator and authentication server performing 802.1X authentication?

- SSH
- TACACS+
- **RADIUS**
- MD5

Explanation: Encapsulation of EAP data between the authenticator and the authentication server is performed using RADIUS.

23. Which statement describes a difference between RADIUS and TACACS+?

- RADIUS separates authentication and authorization, whereas TACACS+ combines them as one process.
- RADIUS does not support EAP for 802.1x, whereas TACACS+ does.
- **RADIUS encrypts only the password, whereas TACACS+ encrypts all communication.**
- RADIUS uses TCP, whereas TACACS+ uses UDP.

Explanation: TACACS+ uses TCP, encrypts the entire packet (not just the password), and separates authentication and authorization into two distinct processes. Both protocols are supported by the Cisco Secure ACS software.

24. What is a feature of a Cisco IOS Zone-Based Policy Firewall?

- Router management interfaces must be manually assigned to the self zone.
- **A router interface can belong to only one zone at a time.**
- Service policies are applied in interface configuration mode.
- The pass action works in multiple directions.

Explanation: The pass action allows traffic in only one direction. Interfaces automatically become members of the self zone. Interfaces are assigned to a zone in interface configuration mode, but most configuration takes place in global configuration mode and associated submodes. An interface can belong to only one zone at a time.

25. Which statement describes Cisco IOS Zone-Based Policy Firewall operation?

- **The pass action works in only one direction.**
- Router management interfaces must be manually assigned to the self zone.
- A router interface can belong to multiple zones.
- Service policies are applied in interface configuration mode.

Explanation: The pass action allows traffic only in one direction. Interfaces automatically become members of the self zone. Interfaces are assigned to zones in interface configuration mode, but most configuration takes place in global configuration mode and associated submodes. Interfaces can belong to only one zone at any time.

26. What are two characteristics of the ZBFW default zone? (Choose two.)

- By default, all IP addresses on a router are included in the default zone.
- **It is a system built zone.**

- By default, interfaces in the default zone are permitted to communicate with interfaces in other zones.
- All traffic is permitted by default to and from the default zone.
- **Interfaces that are not members of other zones are placed in this zone by default.**

Explanation: The default zone is a system-level zone. If an interface is not configured as part of another security zone, it is placed in the default zone automatically. Interfaces in different zones are not permitted to communicate by default.

27. What is the Control Plane Policing (CoPP) feature designed to accomplish?

- disable control plane services to reduce overall traffic
- manage services provided by the control plane
- direct all excess traffic away from the route processor
- **prevent unnecessary traffic from overwhelming the route processor**

Explanation: Control Plane Policing (CoPP) does not manage or disable any services. It does not direct traffic away from the route processor, but rather it prevents unnecessary traffic from getting to the route processor.

28. Which command can be issued to protect a Cisco router from unauthorized automatic remote configuration?

- no cdp enable
- no service pad
- **no service config**
- no ip proxy-arp

Explanation: Service configuration allows Cisco devices to be configured automatically from remote devices using TFTP. By disabling this service with the no service config command, the threat of an unauthorized automatic device configuration can be mitigated.

29. Which vulnerability can be mitigated by disabling CDP and LLDP on a Cisco device?

- **advertising detailed information about a device**
- automatic remote configuration
- half-open or orphaned TCP connections
- answering APR requests intended for other devices

Explanation: Both CDP and LLDP are topology discovery tools and can advertise detailed information about a device. To prevent a Cisco device from sending CDP and LLDP packets onto the network, both protocols should be disabled.

30. Which type of threat defense is provided by Cisco Umbrella?

- **blocking requests to malicious Internet destinations**
- monitoring and analyzing network traffic for potential network intrusion attacks
- identifying and blocking zero-day threats that manage to infiltrate the network
- blocking hidden malware from both suspicious and legitimate websites

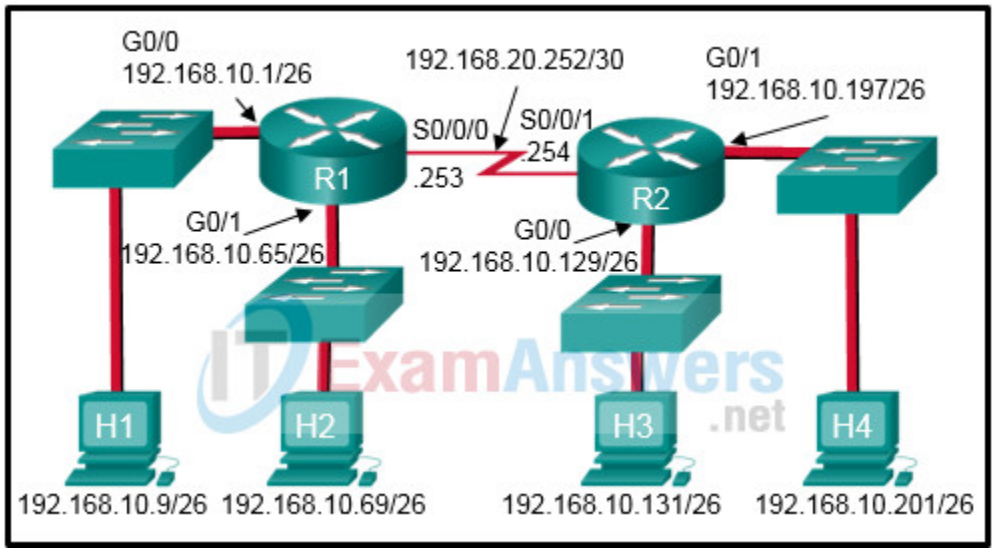
Explanation: Cisco Umbrella serves as a first line of defense for an organization by blocking requests to malicious internet destinations.

31. Which Cisco solution is used by Cisco Web Security Appliance to detect and correlate threats in real time?

- Cisco Umbrella
- **Cisco Talos**
- Cisco Threat Grid
- Cisco ISE

Explanation: Cisco Web Security Appliance (WSA) is a web gateway that offers a wide range of security protection. It leverages Cisco Talos for real-time intelligence so that is can stay ahead of the evolving threat landscape and protect against the latest exploits.

32. Refer to the exhibit. Which two ACLs, if applied to the G0/1 interface of R2, would permit only the two LAN networks attached to R1 to access the network that connects to R2 G0/1 interface? (Choose two.)



access-list 4 permit 192.168.10.0 0.0.0.255

access-list 5 permit 192.168.10.0 0.0.0.63
access-list 5 permit 192.168.10.64 0.0.0.63

access-list 3 permit 192.168.10.128 0.0.0.63

access-list 1 permit 192.168.10.0 0.0.0.127

access-list 2 permit host 192.168.10.9
access-list 2 permit host 192.168.10.69

Explanation: The permit 192.168.10.0 0.0.0.127 command ignores bit positions 1 through 7, which means that addresses 192.168.10.0 through 192.168.10.127 are allowed through. The two ACEs of permit 192.168.10.0 0.0.0.63 and permit 192.168.10.64 0.0.0.63 allow the same address range through the router.