Cisco

Exam Questions 210-260

IINS Implementing Cisco Network Security
NEW QUESTION 1
- (Exam Topic 1)

Refer to the exhibit.

```
authentication event fail action next-method
authentication event no-response action authorize vlan 101
authentication order mab dot1x webauth
authentication priority dot1x mab
authentication port-control auto
dot1x pae authenticator
```

If a supplicant supplies incorrect credentials for all authentication methods configured on the switch, how will the switch respond?

A. The supplicant will fail to advance beyond the webauth method.
B. The switch will cycle through the configured authentication methods indefinitely.
C. The authentication attempt will time out and the switch will place the port into the unauthorized state.
D. The authentication attempt will time out and the switch will place the port into VLAN 101.

Answer: A

Explanation:
Flexible authentication (FlexAuth) is a set of features that allows IT administrators to configure the sequence and priority of IEEE 802.1X, MAC authentication bypass (MAB), and switch-based web authentication (local WebAuth).

Case 2: Order MABDot1x and Priority Dot1x MAB
If you change the order so that MAB comes before IEEE 802.1X authentication and change the default priority so that IEEE 802.1X authentication precedes MAB, then every device in the network will still be subject to MAB, but devices that pass MAB can subsequently go through IEEE 802.1X authentication.

Special consideration must be paid to what happens if a device fails IEEE 802.1X authentication after successful MAB. First, the device will have temporary network access between the time MAB succeeds and IEEE 802.1X authentication fails. What happens next depends on the configured event-fail behavior.

If next-method is configured and a third authentication method (such as WebAuth) is not enabled, then the switch will return to the first method (MAB) after the held period. MAB will succeed, and the device will again have temporary access until and unless the supplicant tries to authenticate again.

If next-method failure handling and local WebAuth are both configured after IEEE 802.1X authentication fails, local WebAuth ignores EAPoL-Start commands from the supplicant.

MAB --> MAB Pass --> Port Authorized by MAB --> EAPoL-Start Received --> IEEE 802.1x MAB --> MABFail --> IEEE 802.1x

(config-if)#authentication order mab dot1x (config-if)#authentication priority dot1x mab


NEW QUESTION 2
- (Exam Topic 1)

Which type of mirroring does SPAN technology perform?

A. Remote mirroring over Layer 2
B. Remote mirroring over Layer 3
C. Local mirroring over Layer 2
D. Local mirroring over Layer 3

Answer: C

Explanation:
You can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to an analyzer or other monitoring or security device.

Local SPAN supports a SPAN session entirely within one switch; all source ports or source VLANs and destination ports are in the same switch or switch stack. Each local SPAN session or RSPAN destination session must have a destination port (also called a monitoring port) that receives a copy of traffic from the source ports or VLANs and sends the SPAN packets to the user, usually a network analyzer:

+ If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.

Source:

NEW QUESTION 3
- (Exam Topic 1)

According to Cisco best practices, which three protocols should the default ACL allow on an access port to enable wired BYOD devices to supply valid credentials and connect to the network? (Choose three.)

A. BOOTP
B. TFTP
C. DNS
D. MAB
E. HTTP
F. 802.1x

Answer: ABC

Explanation:
ACLs are the primary method through which policy enforcement is done at access layer switches for wired devices within the campus.

ACL-DEFAULT--This ACL is configured on the access layer switch and used as a default ACL on the port. Its purpose is to prevent un-authorized access.

An example of a default ACL on a campus access layer switch is shown below: Extended IP access list ACL-DEFAULT

```
10 permit udp any eq bootpc any eq bootps log (2604 matches) 20 permit udp any host 10.230.1.45 eq domain 30 permit icmp any any 40 permit udp any any eq tftp
50 deny ip any any log (40 matches)
```

As seen from the output above, ACL-DEFAULT allows DHCP, DNS, ICMP, and TFTP traffic and denies everything else.
MAB is an access control technique that Cisco provides and it is called MAC Authentication Bypass.

NEW QUESTION 4
- (Exam Topic 1)
When an IPS detects an attack, which action can the IPS take to prevent the attack from spreading?
A. Deny the connection inline.
B. Perform a Layer 6 reset.
C. Deploy an antisizare system.
D. Enable bypass mode.
Answer: A
Explanation:
Deny connection inline: This action terminates the packet that triggered the action and future packets that are part of the same TCP connection. The attacker could open up a new TCP session (using different port numbers), which could still be permitted through the inline IPS.
Available only if the sensor is configured as an IPS.
Source: Cisco Official Certification Guide, Table 17-4 Possible Sensor Responses to Detected Attacks, p.465

NEW QUESTION 5
- (Exam Topic 2)
In which three ways does the RADIUS protocol differ from TACACS? (Choose three.)
A. RADIUS uses UDP to communicate with the NAS.
B. RADIUS encrypts only the password field in an authentication packet.
C. RADIUS authenticates and authorizes simultaneously, causing fewer packets to be transmitted.
D. RADIUS uses TCP to communicate with the NAS.
E. RADIUS can encrypt the entire packet that is sent to the NAS.
F. RADIUS supports per-command authorization.
Answer: ABC
Explanation:
Cisco Official Certification Guide, Table 3-2 TACACS+ Versus RADIUS, p.40

NEW QUESTION 6
- (Exam Topic 2)
A proxy firewall protects against which type of attack?
A. cross-site scripting attack
B. worm traffic
C. port scanning
D. DDoS attacks
Answer: A
Explanation:
Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec as of 2007.
Source: https://en.wikipedia.org/wiki/Cross-site_scripting
A proxy firewall is a network security system that protects network resources by filtering messages at the application layer. A proxy firewall may also be called an application firewall or gateway firewall. Proxy firewalls are considered to be the most secure type of firewall because they prevent direct network contact with other systems.
Source: http://searchsecurity.techtarget.com/definition/proxy-firewall

NEW QUESTION 7
- (Exam Topic 2)
What is the best way to confirm that AAA authentication is working properly?
A. Use the test aaa command.
B. Ping the NAS to confirm connectivity.
C. Use the Cisco-recommended configuration for AAA authentication.
D. Log into and out of the router, and then check the NAS authentication log.
Answer: A
Explanation:
#test aaa group tacacs+ admin cisco123 legacy - Aillow verification of the authentication function working between the AAA client (the router) and the ACS server (the AAA server).
Source: Cisco Official Certification Guide, Table 3-6 Command Reference, p.68

NEW QUESTION 8
- (Exam Topic 2)
Which feature of the Cisco Email Security Appliance can mitigate the impact of snowshoe spam and sophisticated phishing attacks?

A. contextual analysis  
B. holistic understanding of threats  
C. graymail management and filtering  
D. signature-based IPS  

Answer: A

**Explanation:**
Snowshoe spamming is a strategy in which spam is propagated over several domains and IP addresses to weaken reputation metrics and avoid filters. The increasing number of IP addresses makes recognizing and capturing spam difficult, which means that a certain amount of spam reaches their destination email inboxes. Specialized spam trapping organizations are often hard pressed to identify and trap snowshoe spamming via conventional spam filters. The strategy of snowshoe spamming is similar to actual snowshoes that distribute the weight of an individual over a wide area to avoid sinking into the snow. Likewise, snowshoe spamming delivers its weight over a wide area to remain clear of filters.

Source: https://www.techopedia.com/definition/1713/snowshoe-spamming Snowshoe spam, as mentioned above, is a growing concern as spammers distribute spam attack origination across a broad range of IP addresses in order to evade IP reputation checks. The newest AsyncOS 9 for ESA enables enhanced anti-spam scanning through contextual analysis and enhanced automation, as well as automatic classification, to provide a stronger defense against snowshoe campaigns and phishing attacks.

NEW QUESTION 14
- (Exam Topic 3)
Which IPS mode is less secure than other options but allows optimal network throughput?

A. Promiscuous mode
B. inline mode
C. transparent mode
D. inline-bypass mode

Answer: A

Explanation:
The recommended IPS deployment mode depends on the goals and policies of the enterprise. IPS inline mode is more secure because of its ability to stop malicious traffic in real-time, however it may impact traffic throughput if not properly designed or sized. Conversely, IPS promiscuous mode has less impact on traffic throughput but is less secure because there may be a delay in reacting to the malicious traffic.

NEW QUESTION 15
- (Exam Topic 3)
The purpose of the certificate authority (CA) is to ensure what?

A. BYOD endpoints are posture checked
B. BYOD endpoints belong to the organization
C. BYOD endpoints have no malware installed
D. BYOD users exist in the corporate LDAP directory

Answer: B

NEW QUESTION 16
- (Exam Topic 3)
which port should (or would) be open if VPN NAT-T was enabled

A. port 500
B. port 500 outside interface
C. port 4500 outside interface
D. port 4500 ipsec

Answer: D

Explanation:
NAT traversal: The encapsulation of IKE and ESP in UDP port 4500 enables these protocols to pass through a device or firewall performing NAT. Source: https://en.wikipedia.org/wiki/Internet_Key_Exchange Also a good reference Source: https://supportforums.cisco.com/document/64281/how-does-nat-t-work-ipsec

NEW QUESTION 17
- (Exam Topic 3)
What is the effect of the ASA command crypto isakmp nat-traversal?

A. It opens port 4500 only on the outside interface.
B. It opens port 500 only on the inside interface.
C. It opens port 500 only on the outside interface.
D. It opens port 4500 on all interfaces that are IPSec enabled.

Answer: D

NEW QUESTION 18
- (Exam Topic 4)
Which statement about traffic inspection using the Cisco Modular Policy Framework on the ASA is true?

A. HTTP inspection is supported with Cloud Web Security inspection
B. QoS policing and QoS priority queuing can be configured for the same traffic
C. ASA with FirePOWER supports HTTP inspection
D. Traffic can be sent to multiple modules for inspection

Answer: A

NEW QUESTION 19
- (Exam Topic 4)
Which two types of VLANs using PVLANs are valid? (Choose two.)

A. secondary
B. community
C. isolated
D. promiscuous
E. backup

Answer:
Explanation:

- Promiscuous (P): Usually connects to a router—a type of a port which is allowed to send and receive frames from any other port on the VLAN.
- Isolated (I): This type of port is only allowed to communicate with P ports—they are "stub". This type of ports usually connects to hosts.

https://learningnetwork.cisco.com/docs/DOC-16110

NEW QUESTION 20
- (Exam Topic 4)
Which two options are primary deployment model for mobile device management (Choose two)

A. Cloud-based
B. Hybrid-cloud based
C. Multi-site
D. On-Perimeter
E. Single site

Answer: AD

NEW QUESTION 21

......
Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

210-260 Practice Exam Features:

* 210-260 Questions and Answers Updated Frequently
* 210-260 Practice Questions Verified by Expert Senior Certified Staff
* 210-260 Most Realistic Questions that Guarantee you a Pass on Your First Try
* 210-260 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 210-260 Practice Test Here