Cisco 210-260 Exam

Volume: 310 Questions

Question: 1
which are two valid TCP connection states (pick 2) is the gist of the question?

A. SYN-RCVD

B. Closed

C. SYN-WAIT

D. RCVD

E. SENT

Answer: A,B

Question: 2
How does the Cisco ASA use Active Directory to authorize VPN users?

A. It queries the Active Directory server for a specific attribute for the specified user.

B. It sends the username and password to retrieve an ACCEPT or REJECT message from the Active Directory server.

C. It downloads and stores the Active Directory database to query for future authorization requests.

D. It redirects requests to the Active Directory server defined for the VPN group.

Answer: A

Question: 3
Which statements about smart tunnels on a Cisco firewall are true? (Choose two.)

A. Smart tunnels can be used by clients that do not have administrator privileges

B. Smart tunnels support all operating systems

C. Smart tunnels offer better performance than port forwarding

D. Smart tunnels require the client to have the application installed locally

Answer: A,C

Question: 4
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

Question: 5
Within an 802.1X enabled network with the Auth Fail feature configured, when does a switch port get placed into a restricted VLAN?

A. When 802.1X is not globally enabled on the Cisco catalyst switch

B. When AAA new-model is enabled

C. When a connected client fails to authenticate after a certain number of attempts

D. If a connected client does not support 802.1X

E. After a connected client exceeds a specific idle time

Answer: C

Question: 6
Which prevent the company data from modification even when the data is in transit?

A. Confidentiality

B. Integrity

C. Vailability

Answer: B

Question: 7
When is the best time to perform an anti-virus signature update?

A. Every time a new update is available.

B. When the local scanner has detected a new virus.

C. When a new virus is discovered in the wild.

D. When the system detects a browser hook.

Answer: A

Question: 8
How to verify that TACACS+ connectivity to a device?

A. You successfully log in to the device by using the local credentials.

B. You connect to the device using SSH and receive the login prompt.

C. You successfully log in to the device by using ACS credentials.

D. You connect via console port and receive the login prompt.

Answer: B

Question: 9
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 antimalware system.

D. Enable bypass mode.

Answer: A

Question: 10
What is the default timeout interval during which a router waits for responses from a TACACS server before declaring a timeout failure?

A. 5 seconds

B. 10 seconds

C. 15 seconds

D. 20 seconds

Answer: A

Question: 11
Which security zone is automatically defined by the system?

A. The source zone

B. The self zone

C. The destination zone

D. The inside zone

Answer: B

Question: 12
You have implemented a Sourcefire IPS and configured it to block certain addresses utilizing Security Intelligence IP Address Reputation. A user calls and is not able to access a certain IP address. What action can you take to allow the user access to the IP address?

A. Create a whitelist and add the appropriate IP address to allow the traffic.

B. Create a custom blacklist to allow the traffic.

C. Create a user based access control rule to allow the traffic.

D. Create a network based access control rule to allow the traffic.

E. Create a rule to bypass inspection to allow the traffic.

Answer: A

Question: 13
In which three cases does the ASA firewall permit inbound HTTP GET requests during normal operations? (Choose three).

A. when matching NAT entries are configured

B. when matching ACL entries are configured

C. when the firewall receives a SYN-ACK packet

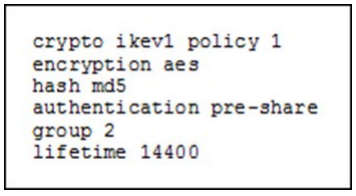
D. when the firewall receives a SYN packet

E. when the firewall requires HTTP inspection

F. when the firewall requires strict HTTP inspection

Answer: A,B,D

Question: 14
Refer to the exhibit.



What is the effect of the given command sequence?

A. It configures IKE Phase 1.

B. It configures a site-to-site VPN tunnel.

C. It configures a crypto policy with a key size of 14400.

D. It configures IPSec Phase 2.

Answer: A

Question: 15
By default, how does a zone-based firewall handle traffic to and from the self zone?

A. It permits all traffic without inspection.

B. It inspects all traffic to determine how it is handled.

C. it permits all traffic after inspection

D. it drops all traffic.

Answer: C

Question: 16
Refer to the exhibit.

```
crypto map mymap 20 match address 201
access-list 201 permit ip 10.10.10.0 255.255.255.0 10.100.100.0 255.255.255.0
```

What is the effect of the given command sequence?

A. It defines IPSec policy for traffic sourced from 10.10.10.0/24 with a destination of 10.100.100.0/24.

B. It defines IPSec policy for traffic sourced from 10.100.100.0/24 with a destination of 10.10.10.0/24.

C. It defines IKE policy for traffic sourced from 10.10.10.0/24 with a destination of 10.100.100.0/24.

D. It defines IKE policy for traffic sourced from 10.100.100.0/24 with a destination of 10.10.10.0/24.

Answer: A

Question: 17
By which kind of threat is the victim tricked into entering username and password information at a disguised website?

A. Spoofing

B. Malware

C. Spam

D. Phishing

Answer: D

Question: 18
Which countermeasures can mitigate ARP spoofing attacks? (Choose two.)

A. Port security

B. DHCP snooping

C. IP source guard

D. Dynamic ARP inspection

Answer: B,D

Question: 19
Which technology can be used to rate data fidelity and to provide an authenticated hash for data?

A. file reputation

B. file analysis

C. signature updates

D. network blocking

Answer: A

Question: 20
Refer to the exhibit.

```
dst          src         state          conn-id     slot
10.10.10.2   10.1.1.5    MM_NO_STATE    1           0
```

While troubleshooting site-to-site VPN, you issued the show crypto isakmp sa command. What does the given output show?

A. IKE Phase 1 main mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2.

B. IKE Phase 1 main mode has successfully negotiated between 10.1.1.5 and 10.10.10.2.

C. IKE Phase 1 aggressive mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2.

D. IKE Phase 1 aggressive mode has successfully negotiated between 10.1.1.5 and 10.10.10.2.

Answer: A

Question: 21
What configure mode you used for the command ip ospf authentication-key c1$c0?

A. global

B. privileged

C. in-line

D. Interface

Answer: D

Question: 22
Refer to the exhibit.

```
Oct 13 19:46:06.170: AAA/MEMORY: create_user (0x4C5E1F60) user='tecteam'
ruser='NULL' ds0=0 port='tty515' rem_addr='10.0.2.13' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0', vrf= (id=0)
Oct 13 19:46:06.170: AAA/AUTHEN/START (2600878790): port='tty515' list=''
action=LOGIN service=ENABLE
Oct 13 19:46:06.170: AAA/AUTHEN/START (2600878790): console enable - default to
enable password (if any)
Oct 13 19:46:06.170: AAA/AUTHEN/START (2600878790): Method=ENABLE
Oct 13 19:46:06.170: AAA/AUTHEN (2600878790): status = GETPASS
Oct 13 19:46:07.266: AAA/AUTHEN/CONT (2600878790): continue_login
(user='(undef)')
Oct 13 19:46:07.266: AAA/AUTHEN (2600878790): status = GETPASS
Oct 13 19:46:07.266: AAA/AUTHEN/CONT (2600878790): Method=ENABLE
Oct 13 19:46:07.266: AAA/AUTHEN(2600878790): password incorrect
Oct 13 19:46:07.266: AAA/AUTHEN (2600878790): status = FAIL
Oct 13 19:46:07.266: AAA/MEMORY: free_user (0x4C5E1F60) user='NULL'
ruser='NULL' port='tty515' rem_addr='10.0.2.13' authen_type=ASCII service=ENABLE
priv=15 vrf= (id=0)
```

Which statement about this output is true?

A. The user logged into the router with the incorrect username and password.

B. The login failed because there was no default enable password.

C. The login failed because the password entered was incorrect.

D. The user logged in and was given privilege level 15.

Answer: C

Question: 23
Which statement correctly describes the function of a private VLAN?

A. A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains

B. A private VLAN partitions the Layer 3 broadcast domain of a VLAN into subdomains

C. A private VLAN enables the creation of multiple VLANs using one broadcast domain

D. A private VLAN combines the Layer 2 broadcast domains of many VLANs into one major broadcast domain

Answer: A

Question: 24
Which type of encryption technology has the broadest platform support to protect operating systems?

A. software

B. hardware

C. middleware

D. file-level

Answer: A

Question: 25
What are two default Cisco IOS privilege levels? (Choose two.)

A. 0

B. 1

C. 5

D. 7

E. 10

F. 15

Answer: B,F

Question: 26
Which sensor mode can deny attackers inline?

A. IPS

B. fail-close

C. IDS

D. fail-open

Answer: A