

Cisco

*400-251
CCIE Security Written*

**For More Information – Visit link below:
<http://www.certsgrade.com/>**

Version = Product



Question: 1

Which two statements about SCEP are true? (Choose two)

- A. CA Servers must support GetCACaps response messages in order to implement extended functionality.
- B. The GetCRL exchange is signed and encrypted only in the response direction.
- C. It is vulnerable to downgrade attacks on its cryptographic capabilities.
- D. The GetCert exchange is signed and encrypted only in the response direction.
- E. The GetCACaps response message supports DES encryption and the SHA-128 hashing algorithm.

Answer: A C

Question: 2

Which two events can cause a failover event on an active/standby setup? (Choose two)

- A. The active unit experiences interface failure above the threshold.
- B. The unit that was previously active recovers.
- C. The stateful failover link fails.
- D. The failover link fails
- E. The active unit fails.

Answer: A E

Question: 3

Which two statements about the MACsec security protocol are true? (Choose two)

- A. Stations broadcast an MKA heartbeat the contains the key server priority.
- B. The SAK is secured by 128-bit AES-GCM by default.
- C. When switch-to-switch link security is configured in manual mode, the SAP operation mode must be set to GCM.
- D. MACsec is not supported in MDA mode.
- E. MKA heartbeats are sent at a default interval of 3 seconds.

Answer: A B

Question: 4

Which two options are benefits of network summarization? (Choose two)

- A. It can summarize discontinuous IP addresses.
- B. It can easily be added to existing networks.
- C. It can increase the convergence of the network.
- D. It prevents unnecessary routing updates at the summarization boundary if one of the routes in the summary is unstable
- E. It reduces the number of routes.

Answer: D E

Question: 5

Refer to the exhibit.

```
%ASA-6-110001: No route to <dest_address> from <source_address>
```

Which meaning of this error message on a Cisco ASA is true?

- A. The route map redistribution is configured incorrectly.
- B. The default route is undefined.
- C. A packet was denied and dropped by an ACL.
- D. The host is connected directly to the firewall.

Answer: B

Question: 6

Which two statements about uRPF are true?(Choose two)

- A. The administrator can configure the allow-default command to force the routing table to use only the default .
- B. It is not supported on the Cisco ASA security appliance.
- C. The administrator can configure the ip verify unicast source reachable-via any command to enable the RPF check to work through HSRP touting groups.
- D. The administrator can use these how cef interface command to determine whether uRPF is enabled.
- E. In strict mode, only one routing path can be available to reach network devices on a subnet..

Answer: D E

Question: 7

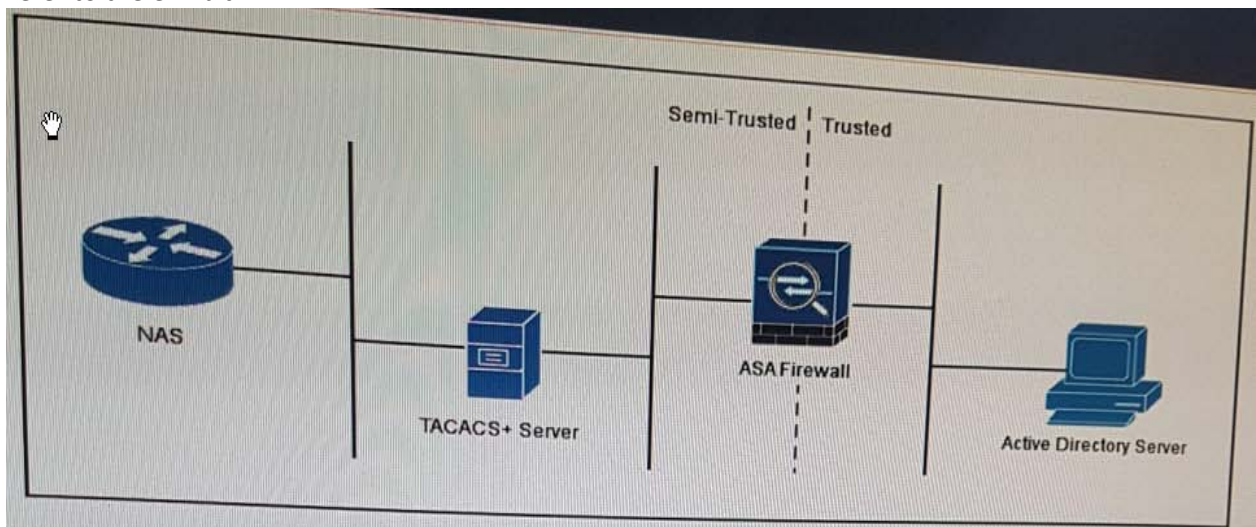
Which type of header attack is detected by Cisco ASA basic threat detection?

- A. Connection limit exceeded.
- B. Denial by access list.
- C. Failed application inspection.
- D. Bad packet format.

Answer: D

Question: 8

Refer to the exhibit.



A user authenticates to the NAS, which communicates to the TACACS+ server authentication. The TACACS+ server then accesses the Active Directory Server through the ASA firewall to validate the user credentials. Which protocol-Port pair must be allowed access through the ASA firewall?

- A. SMB over TCP 445.
- B. DNS over UDP 53.
- C. LDAP over UDP 389.
- D. global catalog over UDP 3268.
- E. TACACS+ over TCP 49.
- F. DNS over TCP 53.

Answer: C

Question: 9

Which WEP configuration can be exploited by a weak IV attack?

- A. When the static WEP password has been stored without encryption.
- B. When a per-packet WEP key is in use.
- C. When a 64-bit key is in use.
- D. When the static WEP password has been given away.
- E. When a 40-bit key is in use.
- F. When the same WEP key is used to create every packet.

Answer: E

Question: 10

Which two statements about Botnet Traffic Filter snooping are true?(Choosetwo)

- A. It can log and block suspicious connections from previously unknown bad domains and IP addresses.
- B. It requires the Cisco ASA DNS server to perform DNS lookups.
- C. It requires DNS packet inspection to be enabled to filter domain names in the dynamic database.
- D. It checks inbound traffic only.
- E. It can inspect both IPv4 and IPv6 traffic.
- F. It checks inbound and outbound traffic.

Answer: CF

Question: 11

Which three statements about SXP are true?(Choose three)

- A. It resides in the control plane, where connections can be initiated from a listener.
- B. Packets can be tagged with SGTs only with hardware support.
- C. Each VRF supports only one CTS-SXP connection.
- D. To enable an access device to use IP device tracking to learn source device IP addresses,DHCP snooping must be configured.
- E. The SGA ZBPF uses the SGT to apply forwarding decisions.
- F. SeparateVRFs require different CTS-SXP peers, but they can use the same source IP addresses.

Answer: A B C

Question: 12

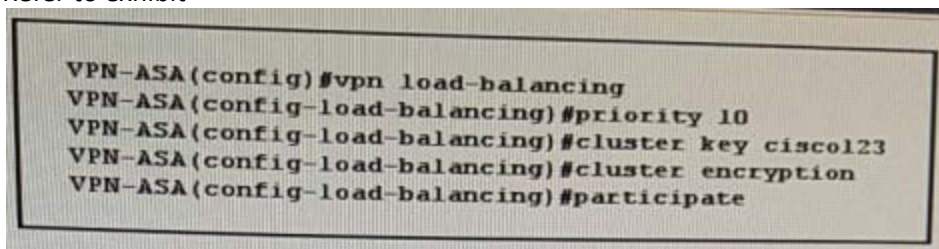
Which file extensions are supported on the Firesight Management Center 6.1(3.1)file policies that can be analyzed dynamically using the Threat Grid Sandbox integration?

- A. MSEX, MSOLE2, NEW-OFFICE,PDF;
- B. DOCX, WAV,XLS,TXT
- C. TXT, MSOLE2, WAV, PDF.
- D. DOC, MSOLE2, XML, PF.

Answer: A

Question: 13

Refer to exhibit



```
VPN-ASA(config)#vpn load-balancing
VPN-ASA(config-load-balancing)#priority 10
VPN-ASA(config-load-balancing)#cluster key cisco123
VPN-ASA(config-load-balancing)#cluster encryption
VPN-ASA(config-load-balancing)#participate
```

You applied this VPN cluster configuration to a Cisco ASA and the cluster failed to form. How do you edit the configuration to correct the problem?

- A. Define the maximum allowable number of VPN connections.
- B. Define the master/slave relationship.
- C. Configure the cluster IP address.
- D. Enable load balancing.

Answer: C

Question: 14

Which effect of the crypto pki authenticate command is true?

- A. It sets the certificate enrollment method.
- B. It retrieves and authenticates a CA certificate.
- C. It configures a CA trustpoint.
- D. It displays the current CA certificate.

Answer: B

Question: 15

Which effect of the nhrp map multicast dynamic command is true?

- A. It configures a hub router to automatically add spoke routers to multicast replication list of the hub.
- B. It enables a GRE tunnel to operate without the IPsec peer or crypto ACLs.
- C. It enables a GRE tunnel to dynamically update the routing tables on the devices at each end of the tunnel.
- D. It configures a hub router to reflect the routes it learns from a spoke back to other spoke back to other spokes through the same interface.

Answer: A

Question: 16

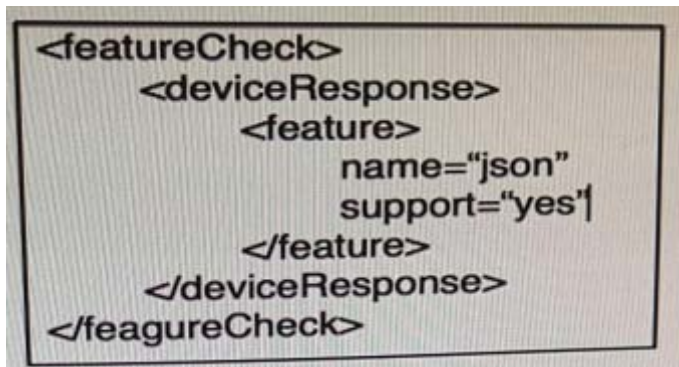
Which statement about VRF-aware GDOI group members is true?

- A. IPsec is used only to secure data traffic.
- B. The GM cannot route control traffic through the same VRF as data traffic.
- C. Multiple VRFs are used to separate control traffic and data traffic.
- D. Registration traffic and rekey traffic must operate on different on different VRFs.

Answer: C

Question: 17

Refer to the exhibit .



```
<featureCheck>
  <deviceResponse>
    <feature>
      name="json"
      support="yes"
    </feature>
  </deviceResponse>
</featureCheck>
```

Which data format is used in this script?

- A. API
- B. JavaScript
- C. JSON
- D. YANG
- E. XML

Answer: E

Question: 18

Which two statements about Cisco URL Filtering on Cisco IOS Software are true?(Choose two)

- A. It supports Websense and N2H2 filtering at the same time.
- B. It supports local URL lists and third-party URL filtering servers.
- C. By default, it uses ports 80 and 22.
- D. It supports HTTP and HTTPS traffic.
- E. By default, it allows all URLs when the connection to the filtering server is down.
- F. It requires minimal CPU time.

Answer: A B

Question: 19

Which two options are benefits of the Cisco ASA transparent firewall mode?(Choose two)

- A. It can establish routing adjacencies.
- B. It can perform dynamic routing.
- C. It can be added to an existing network without significant reconfiguration.
- D. It supports extended ACLs to allow Layer 3 traffic to pass from higher lower security interfaces.
- E. It provides SSL VPN support.

Answer: C D

Question: 20

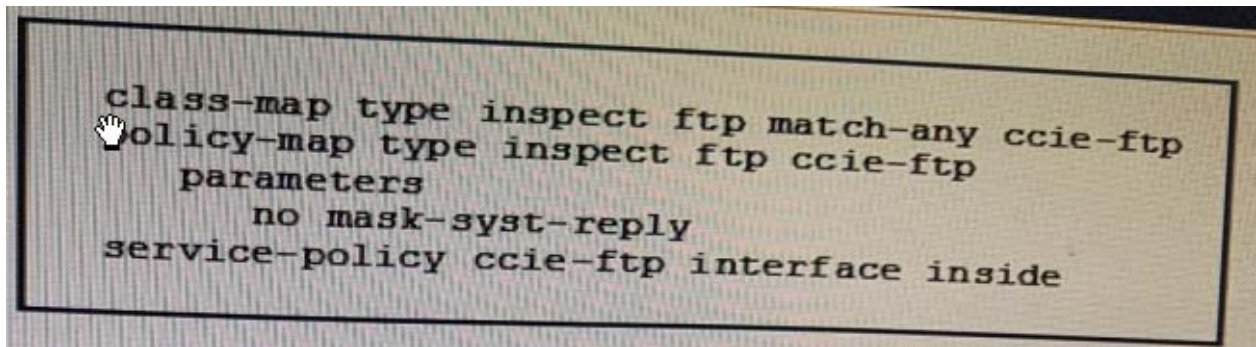
How does Scavenger-class QOS mitigate DOS and worm attacks?

- A. It monitors normal traffic flow and drops burst traffic above the normal rate for a single host.
- B. It matches traffic from individual hosts against the specific network characteristics of known attack types.
- C. It sets a specific intrusion detection mechanism and applies the appropriate ACL when matching traffic is detected.
- D. It monitors normal traffic flow and aggressively drops sustained abnormally high traffic streams from multiple hosts.

Answer: D

Question: 21

Refer to the exhibit.



What are two effects of the given configuration?(Choose two)

- A. TCP connections will be completed only to TCP ports from 1 to 1024.
- B. FTP clients will be able to determine the server's system type
- C. The client must always send the PASV reply.
- D. The connection will remain open if the size of the STOP command is greater than a fixed constant.
- E. The connection will remain open if the PASV reply command includes 5 commas.

Answer: B E

Question: 22

Which three statements about Cisco Any Connect SSL VPN with the ASA are true?(Choose three)

- A. DTLS can fail back to TLS without enabling dead peer detection.
- B. By default, the VPN connection connects with DTLS.
- C. Real-time application performance improves if DTLS is implemented.
- D. Cisco Any Connect connections use IKEv2 by default when it is configured as the primary protocol on the client.
- E. By default, the ASA uses the Cisco Any Connect Essentials license.
- F. The ASA will verify the remote HTTPS certificate.

Answer: B C D

Question: 23

Which two statement about the Cisco Any Connect VPN Client are true?(Choose two)

- A. To improve security, keep alives are disabled by default.
- B. It can be configured to download automatically without prompting the user.
- C. It can use an SSL tunnel and a DTLS tunnel simultaneously.
- D. By default, DTLS connections can fall back to TLS.

E. It enable users to manage their own profiles.

Answer: B C

Question: 24

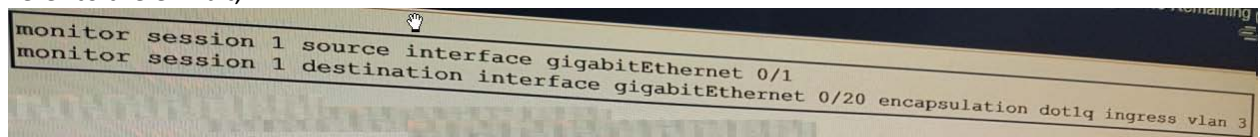
What are the two different modes in which Private AMP cloud can be deployed?(Choose two)

- A. Air Gap Mode.
- B. External Mode.
- C. Internal Mode.
- D. Public Mode.
- E. Could Mode.
- F. Proxy Mode.

Answer: A E

Question: 25

Refer to the exhibit,



What are two functionalities of this configuration?(Choose two)

- A. Traffic will not be able to pass on gigabit Ethernet 0/1.
- B. The ingress command is used for an IDS to send a reset on Vlan 3 only.
- C. The source interface should always be a VLAN.
- D. The encapsulation command is used to deep scan on dot1q encapsulated traffic.
- E. Traffic will only be send to gigabit Ethernet 0/20

Answer: B, E

For More Information – **Visit link below:**
<http://www.certsgrade.com/>

PRODUCT FEATURES

-  **100% Money Back Guarantee**
-  **90 Days Free updates**
-  **Special Discounts on Bulk Orders**
-  **Guaranteed Success**
-  **50,000 Satisfied Customers**
-  **100% Secure Shopping**
-  **Privacy Policy**
-  **Refund Policy**



WE ACCEPT

