Cisco 400-251 Exam

Volume: 402 Questions

Question No: 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: AC

Question No: 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 No: 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: AB

Question No: 4
Which two options are benefits of network summarization? (Choose two)

A. It can summarize discontiguous IP addresses.

B. It can easily be added to existing networks.

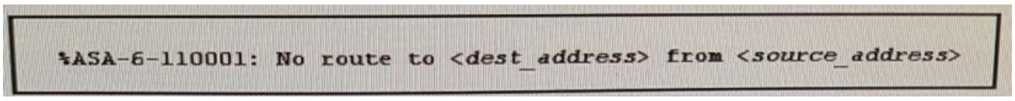
C. It can increase the convergence of the network.

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: DE

Question No: 5
Refer to the exhibit.
Which meaning of this error message on a Cisco ASA is true?



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

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 No: 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 thes 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: DE

Question No: 7
Which type of header attack is detected by Cisco ASA basic threat detection?

A. Connection limit exceeded.

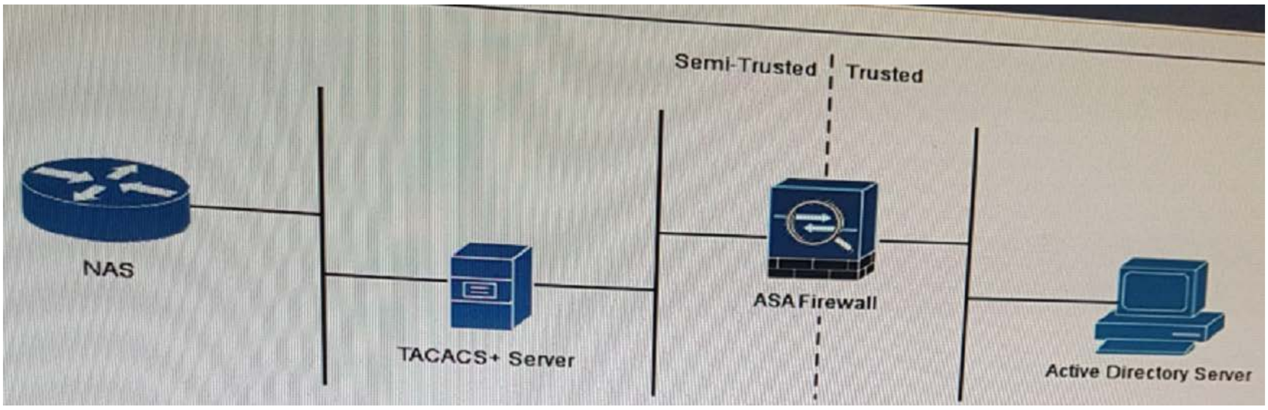
B. Denial by access list.

C. Failed application inspection.

D. Bad packet format.

Answer: D

Question No: 8
Refer to the exhibit.



A user authenticates to the NAS, which communicates to the VACAS+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 455.

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 No: 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 No: 10

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

A. It requires DNS packet inspection to be enabled to filter domain names in the dynamic database.

B. It requires the Cisco ASA DNS server to perform DNS lookups.

C. It can inspect both IPV4 and IPV6 traffic.

D. It can log and block suspicious connections from previously unknown bad domains and IP addresses.

E. It checks inbound traffic only.

F. It checks inbound and outbound traffic.

Answer: AF

Question No: 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. Separate VRFs require different CTS-SXP peers, but they can use the same source IP addresses.

Answer: ABC

Question No: 12
Which file extensions are supported on the Firesight Management Center 6.1(3.l)file policies that can be analyzed dynamically using the Threat Grid Sandbox integration?

A. MSEXE, MSOLE2, NEW-OFFICE, PDF;

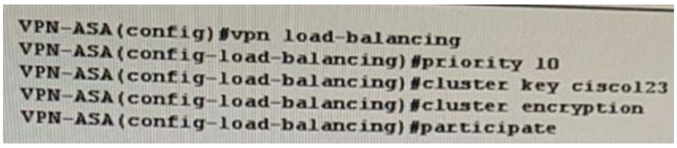
B. DOCX, WAV, XLS, TXT

C. TXT, MSOLE2, WAV, PDF.

D. DOC, MSOLE2, XML, PF.

Answer: A

Question No: 13
Refer to exhibit
You applied this CPN cluster configuration to n a Cisco ASA and the cluster failed to form. How do you edit the configuration to correct the problem?



```
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
```

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 No: 14
Which effect of the crypto pki authenticate commend is true?

A. It sets the certificate enrollment method.

B. It retrievers and authentication a CA certificate.

C. It configures a CA trust point.

D. It displays the current CA certificate.

Answer: B

Question No: 15
Which effect of the ip 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 No: 16
Which statement about VRF-aware GDOI group members is true?

A. IPsec is used only to secure data traffic.

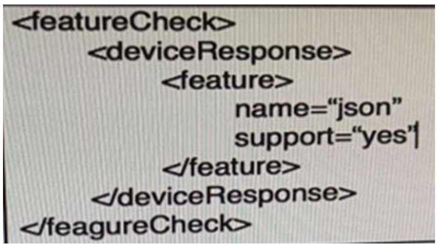
B. The GM cannot route control traffic through the same VRF as data traffic.

C. Multiple VRFs are used to separate control traffic and data traffic.

D. Registration traffic and re key traffic must operate on different on different VRFs.

Answer: A

Question No: 17
Refer to the exhibit.
Which data format is used in this script?



```
<featureCheck>
        <deviceResponse>
                <feature>
                        name=“json”
                        support=“yes’|
                </feature>
        </deviceResponse>
 </feagureCheck>
```

A. API

B. JavaScript

C. JSON

D. YANG

E. XML

Answer: E

Question No: 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 HTTP traffic.

E. By default, it allows all URLs when the connection to the filtering server is down.

F. It requires minimal CPU time.

Answer: AB

Question No: 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: CD

Question No: 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.

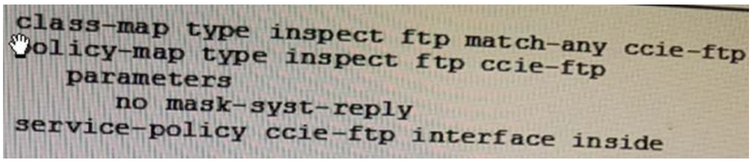
B. It matches traffic from individual hosts against the specific network characteristics of known attack types.

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 No: 21
Refer to the exhibit.
What are two effects of the given configuration?(Choose two)



```
class-map type inspect ftp match-any ccie-ftp
policy-map type inspect ftp ccie-ftp
  parameters
     no mask-syst-reply
service-policy ccie-ftp interface inside
```

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 S commas.

Answer: BE

Question No: 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: BCD

Question No: 23
Which two statement about the Cisco Any Connect VPN Client are true?(Choose two)

A. To improve security, keep a lives 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: BC

Question No: 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.

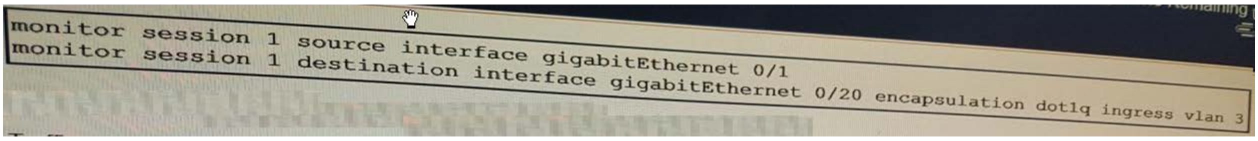
D. Public Mode.

E. Could Mode.

F. Proxy Mode.

Answer: A E

Question No: 25
Refer to the exhibit,
What are two functionalities of this configuration?(Choose two)



```
monitor session 1 source interface gigabitEthernet 0/1
monitor session 1 destination interface gigabitEthernet 0/20 encapsulation dotlq ingress vlan 3
```

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 dotlq encapsulated traffic.

E. Traffic will only be send to gigabit Ethernet 0/20

Answer: B E

Question No: 26
You are considering using RSPAN to capture traffic between several switches. Which two configuration aspects do you need to consider?(Choose two)

A. The RSPAN need to be blocked on all trunk interfaces leading to the destination RSPAN switch.

B. Not all switches need to support RSPAN for it to work.

C. The RSPAN VLAN need to be allow on all trunk interfaces leading to the destination RSPAN switch.

D. All distribution switches need to support RSPAN.

E. All switches need to be running the same IOS version.

Answer: BC

Question No: 27
Which two statements about the TIL value in an IPv4 header are true?(Choose two)

A. It is a 4-bit value.

B. It can be used for trace route operations.

C. When it reaches 0,the router sends an ICMP Type 11 message to the originator.

D. Its maximum value is 128.

E. It is a 16-bit value.

Answer: BC

Question No: 28
Which three ESMTP extensions are supported by the Cisco ASA?(Choose three)

A. Noop

B. PIPELINING

C. SAML

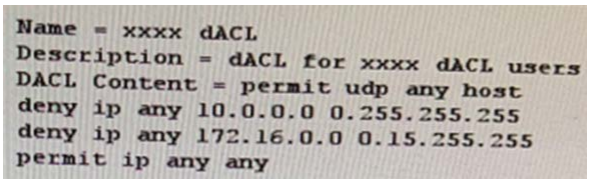
D. 8BITMIME

E. STARTTLS

F. ATRN

Answer: ACE

Question No: 29
Refer to exhibit.
For which type of user is this downloadable ACL appropriate?



```
Name = xxxx dACL
Description = dACL for xxxx dACL users
DACL Content = permit udp any host
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.15.255.255
permit ip any any
```

A. Management

B. Employees

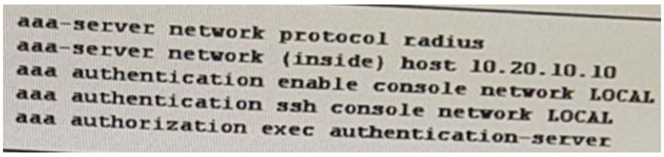
C. Guest users

D. Network administrators

E. Onsite contractors.

Answer: C

Question No: 30
Refer to the exhibit.
Which effect of this configuration is true?



```
aaa-server network protocol radius
aaa-server network (inside) host 10.20.10.10
aaa authentication enable console network LOCAL
aaa authentication ssh console network LOCAL
aaa authorization exec authentication-server
```

A. If the RADIUS server is unreachable, SSH users cannot authenticate.

B. All commands are validated by the RADIUS server before the device executes them.

C. Only SSH users are authenticated against the RADIUS server.

D. Users must be in the RADIUS server to access the serial console.

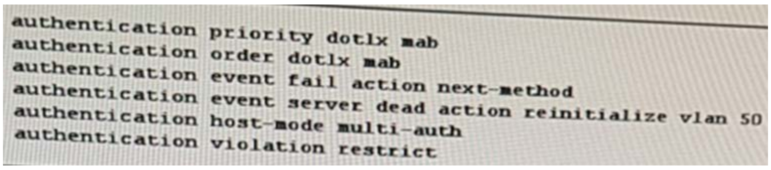
E. Users accessing the device via SSH and those assessing enable mode are authenticated against the RADIUS server.

Answer: E

Question No: 31

Refer to the exhibit.

Which two effects if this configuration are true?(Choose two)



```
authentication priority dot1x mab
authentication order dot1x mab
authentication event fail action next-method
authentication event server dead action reinitialize vlan 50
authentication host-mode multi-auth
authentication violation restrict
```

A. If the TACACS+ server is unreachable, the switch places hosts on critical ports in VLAN 50.

B. If the authentication priority is changed, the order in switch authentication is performed also changes.

C. If multiple hosts have authenticated to the same port, each can be in their own assigned VLAN

D. The port attempts 802.1x authentication first, and. then falls back to MAC authentication bypass.

E. The device allows multiple authenticated sessions for a single MAC address in the voice domain.

F. The switch periodically sends an EAP-ldentity-Request to the endpoint supplicant.

Answer: DE

Question No: 32

In OpenStack, which two statements about the NOVA component are true?(Choose two)

A. It launches virtual machine instances.

B. It provides the authentication and authorization services.

C. It tracks cloud usage statistics for billing purposes.

D. It is considered the cloud computing fabric controller.

E. It provides persistent block storage to running instances of virtual machines.

Answer: CE

Question No: 33
Which three authorization technologies does Cisco Trust Sec support?(Choose three)

A. 802.1x.

B. SGACL.

C. DACL.

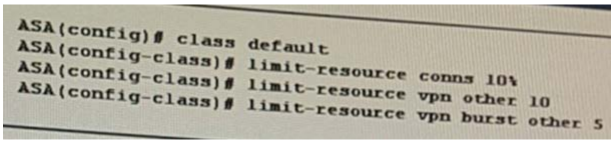
D. MAB.

E. SGT.

F. VLAN.

Answer: AD F

Question No: 34
Refer to the exhibit.
What is the maximum number if site-to-site VPNs allowed by this configuration?



```
ASA(config)# class default
ASA(config-class)# limit-resource conns 10%
ASA(config-class)# limit-resource vpn other 10
ASA(config-class)# limit-resource vpn burst other 5
```

A. 0

B. 1

C. 10

D. 5

E. 15

F. Unlimited

Answer: E

Question No: 35
Which three messages are part of the SSL protocol?(Choose three)

A. Alert.

B. Handshake.

C. Record.

D. CipherSpec.

E. Message Authorization.

F. Change CipherSpec.

Answer: AB F

Question No: 36
Which two statements about SPAN sessions are true?(Choose two)

A. Local SPAN and RSPAN can be mixed in the same session.

B. They can monitor sent and received packets in the same session.

C. Source ports and source VLANs can be mixed in the same session.

D. They can be configured on ports in the disabled state before enabling the port.

E. A single switch stack can support up to 32 source and RSPAN destination sessions.

F. Multiple SPAN sessions can use the same destination port.

Answer: B D

Question No: 37
When TCP Intercept in its default mode, how does it react to a SYN request?

A. It monitors the sequence of SYN, SYN-ACK, and ACK messages until the connection is fully established.

B. It drops the connection.

C. It monitors the attempted connection and drops it if it fails to establish within 30 seconds.

D. It allows the connection without inspection.

E. It intercepts the SYN before it reaches the server and responds with a SYN-ACK.

Answer: E

Question No: 38
Which OpenStack project has orchestration capabilities?

A. Cinder.

B. Heat.

C. Horizon.

D. Sahara

Answer: B

Question No: 39
Which three options are fields in a COA Request Response code packet?(Choose three)

A. State.

B. Acct-session-ID

C. Length.

D. Authenticator.

E. Calling-Station-ID.

F. Identifier.

Answer: ABE

Question No: 40
Which two statements about 802.1x components are true?(Choose two)

A. The access layer switch is the policy enforcement point.

B. The certificates that are used in the client-server authentication process are stored on the access switch.

C. The RADIUS server is the policy enforcement point.

D. The RADIUS server is the policy informant point.

E. The RADIUS server is the policy decision point.

F. An LADP server can server as the policy enforcement point.

Answer: A E

Question No: 41
A client computer at 10.10.7.4 is trying to access a Linux server (11.0.1.9) that is running a Tomcat Server application. What TCP dump filter would best to verify that traffic is reaching the Linux Server Eth0 interface?

A. Tcpdump-ieth0 host 10.10.7.4 and host 11.0.1.9 and port 8080.

B. Tcpump-ieth0 host 10.10.7.4 and 11.0.1.9.

C. Tcpdump-ieth0 dst 11.0.1.9 and dst port 8080.

D. Tcpdump-ieth0 src 10.10.7.4 and dst 11.0.1.9 and dst port 8080.

Answer: D

Question No: 42
Within Platform as a Service, which two components are managed by the customer?(Choose two)

A. Data.

B. Networking.

C. Middleware.

D. Applications.

E. Operating system

Answer: AD

Question No: 43
Which two options are important considerations when you use netflow to obtain the full picture of network traffic?(Choose two)

A. It monitors only TCP connections.

B. It monitors only routed traffic.

C. It monitors all traffic on the interface on which it is deployed.

D. It monitors only ingress traffic on the interface on which it is deployed.

E. It is unable to monitor over time.

Answer: BE

Question No: 44
Which option is a data modeling language used to model configuration and state data of network elements?

A. RESTCONF

B. YANG.

C. SNMPv4.

D. BETCONF.

Answer: B

Question No: 45
Which encryption type is used by ESA for implementing the Email Encryption?

A. PKI.

B. S/MMIE Encryption.

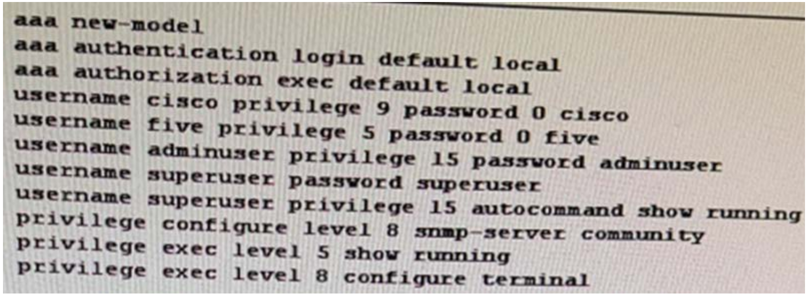
C. Identity Based Encryption(IBE).

D. TLS.

E. SSL Encryption.

Answer: B

Question No: 46
Refer to the exhibit.
Which two effects of this configuration are true?(Choose two)



```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
username cisco privilege 9 password 0 cisco
username five privilege 5 password 0 five
username adminuser privilege 15 password adminuser
username superuser password superuser
username superuser privilege 15 autocommand show running
privilege configure level 8 snmp-server community
privilege exec level 5 show running
privilege exec level 8 configure terminal
```

A. User five can execute the show run command.

B. User five can view usernames and passwords.

C. User superuser can change usernames and passwords.

D. User superuser can view the configuration.

E. User superuser can view usernames and password.

F. User cisco can view usernames and password.

Answer: AD

Question No: 47
Which three commands can you use to configure VXLAN on a Cisco ASA firewall?(Choose three).

A. Sysopt connection tcpmss.

B. Nve-only.