Cisco

Exam Questions 400-251

CCIE Security Written Exam

NEW QUESTION 1
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

NEW QUESTION 2
Which two options are benefits of the Cisco ASA Identity Firewall? (Choose two.)

A. It can identify threats quickly based on their URLs.
B. It can operate completely independently of their services.
C. It can apply security policies on an individual user or user-group basis.
D. It decouples security policies from the network topology.
E. It supports an AD server module to verify identity data.

Answer: CD

NEW QUESTION 3
Which three statements about VRF-Aware Cisco Firewall are true? (Choose three.)

A. It supports both global and per-VRF commands and DoS parameters.
B. It enables service providers to deploy firewalls on customer devices.
C. It can generate syslog messages that are visible only to individual VPNs.
D. It can support VPN networks with overlapping address ranges without NAT.
E. It enables service providers to implement firewalls on PE devices.
F. It can run as more than one instance.

Answer: CEF

NEW QUESTION 4
Which two commands would enable secure logging on a Cisco ASA to a syslog server at 10.0.0.1? (Choose two.)

A. logging host inside 10.0.0.1 UDP/500 secure
B. logging host inside 10.0.0.1 TCP/1470 secure
C. logging host inside 10.0.0.1 UDP/447 secure
D. logging host inside 10.0.0.1 UDP/514 secure
E. logging host inside 10.0.0.1 TCP/1500 secure

Answer: BE

NEW QUESTION 5
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: BF

NEW QUESTION 6
Which statement about VRF-aware GDOI group members is true?

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

Answer: B

NEW QUESTION 7
What is an example of a stream cipher?

A. RC4
B. RC5
C. DES
D. Blowfish

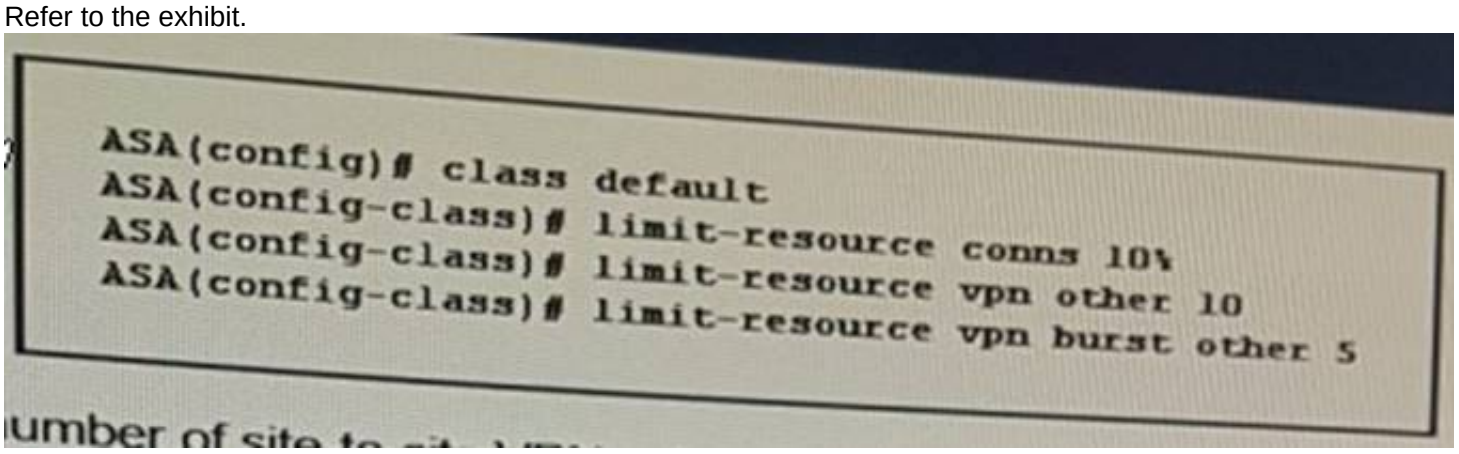
Answer: A

NEW QUESTION 8
Which two options are benefits of global ACLs? (Choose two)

A. They save memory because they work without being replicated on each interface.
B. They are more efficient because they are processed before interface access rules.
C. They are flexible because they match source and destination IP addresses for packets that arrive on any interface.
D. They only operate on logical interfaces.
E. They can be applied to multiple interfaces.

Answer: AC

NEW QUESTION 9
Refer to the exhibit.



What is the maximum number of site-to-site VPNs allowed by this configuration?

A. 10
B. unlimited
C. 5
D. 1
E. 15

Answer:

NEW QUESTION 10
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. Cloud Mode
F. Cloud Proxy Mode

Answer: AF

NEW QUESTION 10
Which two statements about Botnet Traffic Filter snooping are true? (Choose two.)

A. It can log and block suspicious connections from previously unknown bad domains and IP addresses.
B. It requires the Cisco ASADNS 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

NEW QUESTION 14
In OpenStack, which two statements about the NOVA component are true? (Choose two.)

A. It provides the authentication and authorization services.
B. It launches virtual machine instances.
C. It is considered the cloud computing fabric controller.
D. It provides persistent block storage to running instances of virtual machines.
E. It tracks cloud usage statistics for billing purposes.

Answer: BC

NEW QUESTION 18
Refer to the exhibit:

```
aaa-server networkprotocol 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 authenticaation server
```

Which effect of this configuration is true?

A. If the RADIUS server is unreachable, SSH users cannot authenticate.
B. Users must be in the RADIUS server to access the serial console.
C. Users accessing the device via SSH and those accessing enable mode are authenticated against the RADIUS server
D. All commands are validated by the RADIUS server before the device executes them.
E. Only SSH users are authenticated against the RADIUS server.

Answer: C

NEW QUESTION 20
What are three features that are enabled by generating Change of Authorization (CoA) requests in a push model? (Choose three.)

A. session reauthentication
B. session identification
C. host reauthentication
D. MAC identification
E. session termination
F. host termination

Answer: BCE

NEW QUESTION 23
Which three statement 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 support 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 ZBFW 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: BCE

NEW QUESTION 27
When TCP Intercept is enabled 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 monitors the attempted connection and drops it if it fails to establish within 30 seconds.
C. It allows the connection without inspection.
D. It intercepts the SYN before it reaches the server and responds with a SYN-ACK.
E. It drops the connection.

Answer: D

NEW QUESTION 28
Refer to the exhibit.

```
r1#telnet 209.165.200.225 19
Trying 209.165.200.225, 19 ...
Open
abcdefghijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHI
bcdefghijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJ
cdefghijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJK
defghijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKL
efghijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLM
fghijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMN
ghijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNO
hijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOP
ijklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQ
jklmnopqrstuvwxyz{|}~ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQR
```

Which service of feature must be enabled on 209.165.200.255 to produce the given output?

A. the Finger service
B. a BOOTP server
C. a TCP small server
D. the PAD service

Answer: C

NEW QUESTION 33
Which two statements about NVGRE are true? (Choose two.)

A. It supports up to 32 million virtual segments per instance.
B. The network switch handles the addition and removal of NVGRE encapsulation.
C. NVGRE endpoints can reside within a virtual machine.
D. It allows a virtual machine to retain its MAC and IP addresses when it is moved to a different hypervisor on a different L3 network.
E. The virtual machines reside on a single virtual network regardless of their physical location.

Answer: CE

NEW QUESTION 35
A server with IP address 209.165.202.150 is protected behind the inside interface of a Cisco ASA and the Internet on the outside interface. User on the Internet need to access the server ay any time, but the firewall
administrator does not want to apply NAT to the address of the server because it is currently a public address. Which three of the following commands can be used to accomplish this? (Choose three.)

A. static (outside, inside) 209.165.202.150.209.165.202.150 netmask 255.255.255.255
B. nat (inside) 1 209.165.202.150 255.255.255.255
C. static (inside, outside) 209.165.202.150.209.165.202.150 netmask 255.255.255.255
D. no nat-control
E. access-list no-nat permit ip host 209.165.202.150 any nat (inside) 0 access-list no-nat
F. nat (inside) 0 209.165.202.150 255.255.255.255

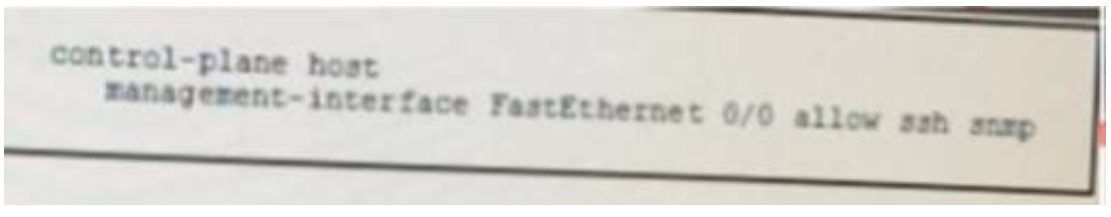
Answer: CEF

NEW QUESTION 37
Which three statements about the keying methods used by MACSec are true? (Choose three.)

A. SAP is not supported on switch SVIs.
B. SAP is supported on SPAN destination ports.
C. MKA is implemented as an EAPoL packet exchange.
D. Key management for host-to-switch and switch-to-switch MACSec sessions is provided by MKA.
E. SAP is enabled by default for Cisco TrustSec in manual configuration mode.
F. A valid mode for SAP is NULL.

Answer: ACF

NEW QUESTION 38
Refer to the exhibit.



What is the effect of the given command?
control-plane host
management-interface FastEhternet 0/0 allow ssh snmp

A. It enables CoPP on the FastEthernet 0/0 interface for SSH and SNMP management traffic.
B. It enables QoS policing on the control plane of the FastEthernet 0/0 interface.
C. It enables MPP on the FastEthernet 0/0 interface, allowing only SSH and SNMP management traffic.
D. It enables MPP on the FastEthernet 0/0 interface by enforcing rate-limiting for SSH and SNMP management traffic.
E. It enables MPP on the FastEthernet 0/0 interface for SNMP management traffic and CoPP for all other protocols.

Answer: C

NEW QUESTION 42
In a Cisco ASA multiple-context mode of operation configuration, what three session types are resourcelimited
by default when their context is a member of the default class? (Choose three.)

A. SSL VPN sessions
B. Telnet sessions
C. TCP session
D. IPSec sessions
E. ASDM sessions
F. SSH sessions

Answer: BDF

NEW QUESTION 47
Which OpenStack project has orchestration capabilities?

A. Cinder

B. Horizon
C. Sahara
D. Heat

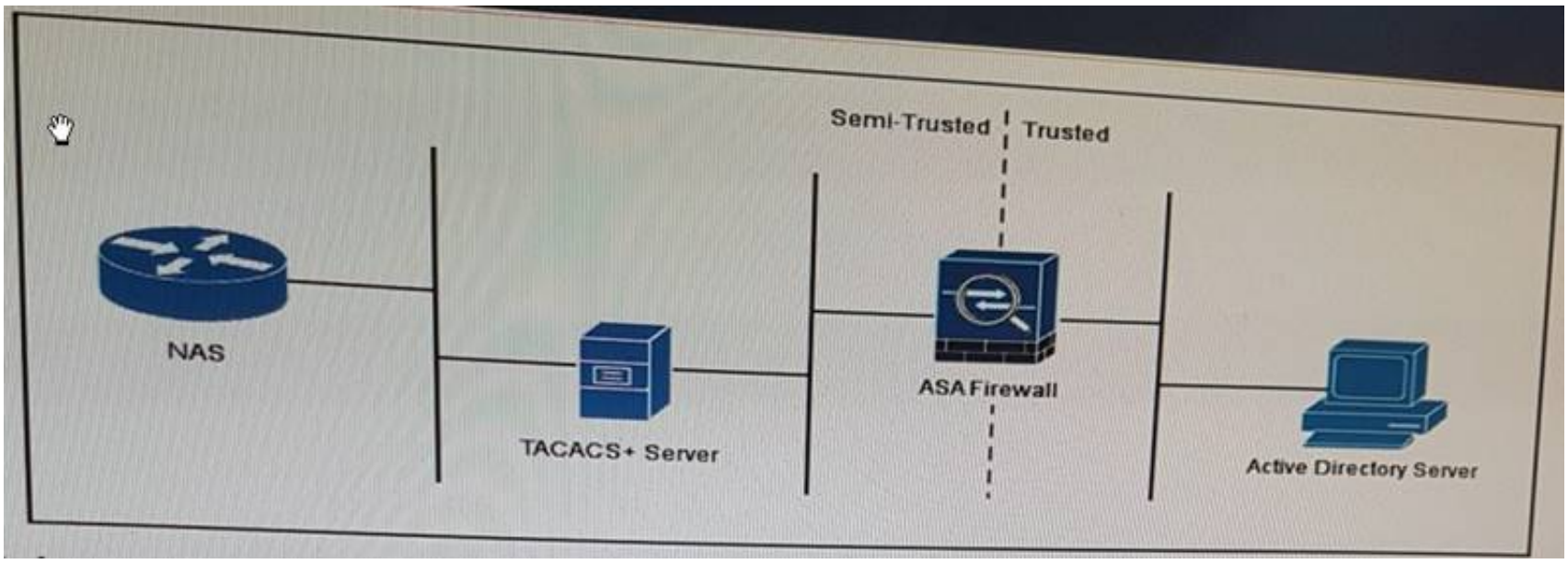
Answer: D

NEW QUESTION 51
What is the purpose of the BGP TTL security check?

A. to check for a TTL value in packet header of less than or equal to for successful peering
B. to protect against routing table corruption
C. to use for iBGP session
D. to protect against CPU utilization-based attacks
E. to authenticate a peer

Answer: D

NEW QUESTION 52
Refer to the exhibit.



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

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

NEW QUESTION 57
Refer to the exhibit.

Which effect of this command is true?

A. The route immediately deletes its current public key from the cache and generates a new one.
B. The public key of the remote peer is deleted from the router cache.
C. The CA revokes the public key certificate of the router.
D. The current public key of the router is deleted from the cache when the router reboots, and the router generates a new one.
E. The router sends a request to the CA to delete the router certificate from its configuration.

Answer: B

NEW QUESTION 60
What are two features that helps to mitigate man-in-the-middle attacks? (Choose two.)

A. DHCP snooping
B. ARP spoofing
C. destination MAC ACLs
D. dynamic ARP inspection
E. ARP sniffing on specific ports

Answer: AD

NEW QUESTION 64
Which two statements about Cisco AMP for Web Security are true? (Choose two.)

A. It can prevent malicious data exfiltration by blocking critical files from exiting through the Web gateway.
B. It can perform reputation-based evaluation and blocking by uploading the fingerprint of incoming files to a cloud-based threat intelligence network.
C. It can detect and block malware and other anomalous traffic before it passes through the Web gateway.
D. It can perform file analysis by sandboxing known malware and comparing unknown files to a local repository of the threats.
E. It can identify anomalous traffic passing through the Web gateway by comparing it to an established of expected activity.
F. It continues monitoring files after they pass the Web gateway.

Answer: BF

NEW QUESTION 65
What are the most common methods that security auditors use to access an organization's security processes? (Choose two.)

A. physical observation
B. social engineering attempts
C. penetration testing
D. policy assessment
E. document review
F. interviews

Answer: AF

NEW QUESTION 68
Which type of header attack is detected by Cisco ASA basic threat detection?

A. denial by access list
B. bad packet format
C. failed application inspection
D. connection limit exceeded

Answer: B

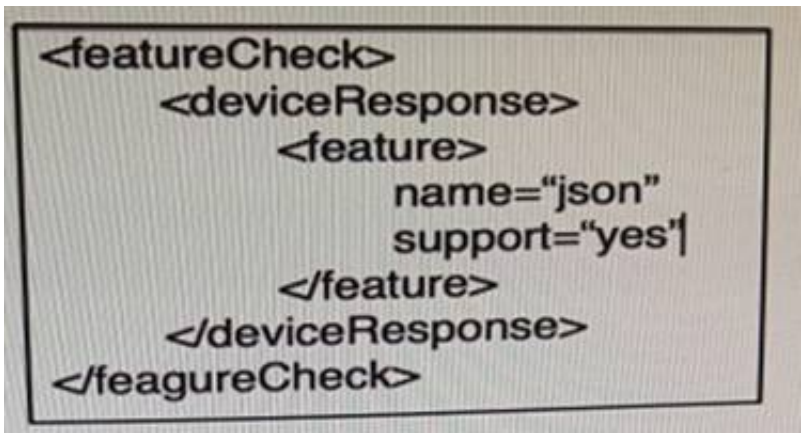
NEW QUESTION 71
Which three statements about RLDP are true? (Choose three.)

A. It detects rogue access points that are connected to the wired network.
B. It can detect rogue APs that use WPA encryption.
C. It can detect rogue APs operating only on 5 GHz.
D. It can detect rogue APs that use WEP encryption.
E. The AP is unable to serve clients while the RLDP process is active.
F. Active Rogue Containment can be initiated manually against rogue devices detected on the wired network.

Answer: AEF

Explanation: Rogue Location Discovery Protocol (RLDP)
http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70987-rogue-detect.html

NEW QUESTION 72
Refer to the exhibit.



Which data format is used in this script?

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

Answer: D

NEW QUESTION 74
Which command sequence do you enter to add the host 10.2.1.0 to the CISCO object group?

A. object-group network CISCO group-object 10.2.1.0
B. object network CISCO network-object object 10.2.1.0
C. object-group network CISCO network-object host 10.2.1.0
D. object network CISCO group-object 10.2.1.0

Answer: C

NEW QUESTION 75
Which two statements about Cisco ASA authentication using LDAP are true? (Choose two.)

A. It is a closed standard that manages directory-information services over distributed networks.
B. It can combine AD attributes and LDAP attributes to configure group policies on the Cisco ASA.
C. It uses attribute maps to map the AD memberOf attribute to the Cisco ASAGroup-Policy attribute.
D. It can assign a group policy to a user based on access credentials.
E. It uses AD attribute maps to assign users to group policies configured under the WebVPN context.
F. The Cisco ASA can use more than one AD memberOf attribute to match a user to multiple group policies.

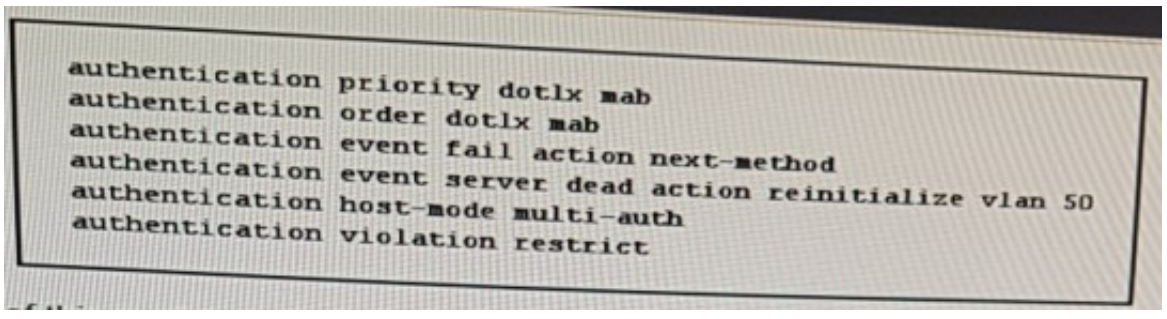
Answer: CE

NEW QUESTION 76
Which two design options are best to reduce security concerns when adopting IoT into an organization? (Choose two.)

A. Segment the Field Area Network from the Data Center network.
B. Encrypt sensor data in transit.
C. Ensure that application can gather and analyze data at the edge.
D. Implement video analytics on IP cameras.
E. Encrypt data at rest on all devices in the IoT network.

Answer: AB

NEW QUESTION 77
Refer to the exhibit.



Which two effects of this configuration are true? (Choose two.)

A. The switch periodically sends an EAP-Identity-Request to the endpoint supplicant.
B. The device allows multiple authenticated sessions for a single MAC address in the voice domain.
C. If the TACACS+ server is unreachable, the switch places hosts on critical ports in VLAN 50.
D. If the authentication priority is changed, the order in which authentication is performed also changes.
E. If multiple hosts have authenticated to the same port, each can be in their own assigned VLAN.
F. The port attempts 802.1x authentication first, and then falls back to MAC authentication bypass.

Answer: CF

NEW QUESTION 80
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

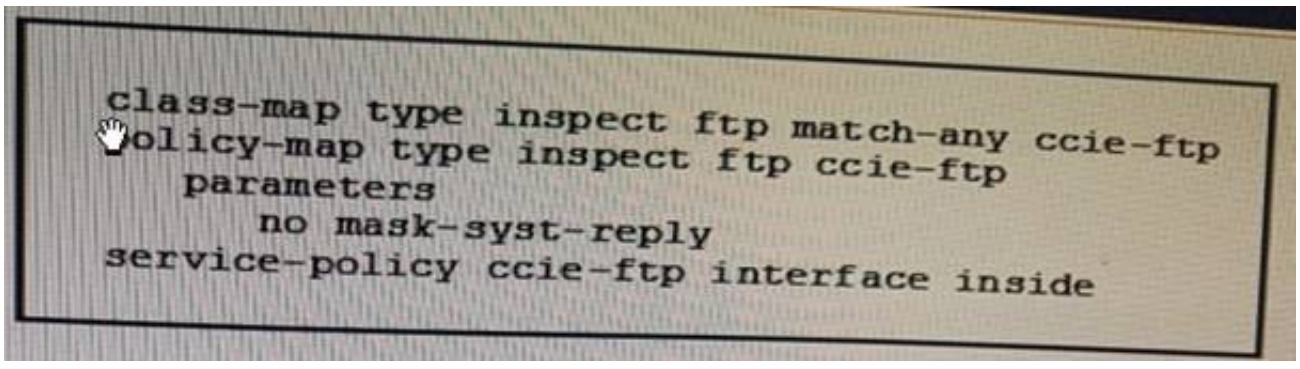
NEW QUESTION 82
Which statement about MDM with the Cisco ISE is true?

A. The MDM’s server certificate must be imported into the Cisco ISE Certificate Store before the MDM andISE can establish a connection.
B. MDM servers can generate custom ACLs for the Cisco ISE to apply to network devices.
C. The Cisco ISE supports a built-in list of MDM dictionary attributes it can use in authorization policies.
D. The Cisco ISE supports limited built-in MDM functionality.
E. If a mobile endpoint fails posture compliance, both the user and the administrator are notified immediately.
F. When a mobile endpoint becomes compliant the Cisco ISE records the updated device status in its internal database.

Answer: A

Explanation: Mobile Device Management https://meraki.cisco.com/blog/tag/mobile-device-management/

NEW QUESTION 85
Refer to the exhibit.



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

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

Answer: AE

NEW QUESTION 89
Which two statements about ICMP redirect messages are true? (Choose two.)

A. Redirects are only punted to the CPU if the packets are also source-routed.
B. The messages contain an ICMP Type 3 and ICMP code 7.
C. By default, configuring HSRP on the interface disables ICMP redirect functionality.
D. They are generated when a packet enters and exits the same route interface.
E. They are generated by the host to inform the router of an temate route to the destination.

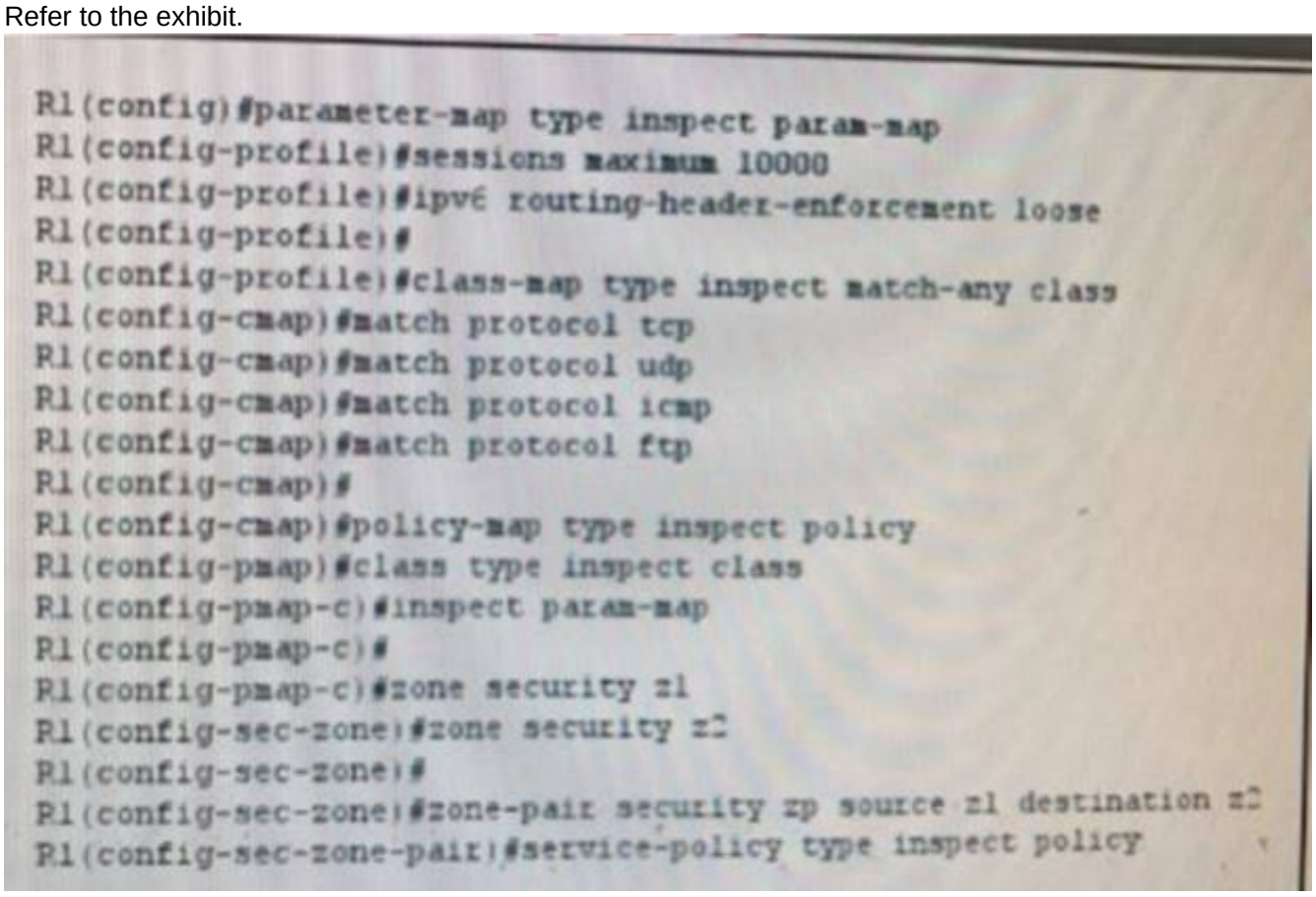
Answer: CD

NEW QUESTION 90
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 to lower security interfaces.
E. It provides SSL VPN support.

Answer: CD

NEW QUESTION 93
Refer to the exhibit.



Which two statements about the given IPv6 ZBF configuration are true? (Choose two.)

A. It inspects TCP, UDP, ICMP, and FTP traffic from z1 to z2.
B. It provides backward compatibility with legacy IPv4 inspection.
C. It inspects TCP, UDP, ICMP, and FTP traffic from z2 to z1.
D. It passes TCP, UDP, ICMP, and FTP traffic in both directions between z1 and z2.
E. It provides backward compatibility with legacy IPv6 inspection.

F. It passes TCP, UDP, ICMP, and FTP traffic from z1 to z2.

Answer: AE

NEW QUESTION 98
Which statement about the Cisco AMP Virtual Private Cloud Appliance is true for deployments in air-gap mode?

A. The amp-sync tool syncs the threat-intelligence repository on the appliance directly with the AMP public cloud.
B. The appliance can perform disposition lookup against either the Protect DB or the AMP public cloud.
C. The appliance can perform disposition lookups against the Protect DB without an Internet connection.
D. The appliance evaluates files against the threat intelligence and disposition information residing on the Update Host.
E. The Update Host automatically downloads updates and deploys them to the Protect DB on a daily basis.

Answer: C

NEW QUESTION 103
What are the major components of a Firepower health monitor alert?

A. The severity level, one or more alert responses, and a remediation policy.
B. A health monitor, one or more alert responses, and a remediation policy.
C. One of more health modules, the severity level, and an alert response.
D. One of more health modules, one or more alert responses, and one or more alert actions.
E. One health modules and one or more alert responses.

Answer: C

Explanation: Topic 2, Exam Pool B

NEW QUESTION 106
Which command is used to enable 802.1x authorization on an interface?

A. authentication open
B. aaa authorization auth-proxy default
C. authentication control-direction both
D. aaa authorization network default group tacacs+
E. authentication port-control auto

Answer: D

NEW QUESTION 108
Which statement about deploying policies with the Firepower Management Center is true?

A. Deploy tasks can be scheduled to deploy policies automatically.
B. All policies are deployed on-demand when the administration triggers them.
C. Policies are deployed automatically when the administration saves them.
D. The leaf domain can deploy change store all sub domains simultaneously.
E. The global domain can deploy changes to individual subdomains.

Answer: A

NEW QUESTION 111
A customer is developing a strategy to deal with Wanna Cry variants that defect sandboxing attempts and mask their present analyzed. Which four mechanisms can be used in this strategy?

A. Employ a DNS forwarder that responds to unknown domain names with a reachable IP (honey pot) that can mimic sandboxing containment responses and alert when a possible threat is detected.
B. Apply route maps at the access layer that prevent all RPC and SMB communication throughout the network.
C. Ensure that the standard desktop image used in the organization is an actively supported operating system and that security patches are applied.
D. Run antimalware software on user endpoints and servers as well as ensure regular signature updates.
E. Ensure that vulnerable services used for propagation of malware such as SMB are blocked on publicfacing segments.
F. Employ URL/DNS inspection mechanisms that blackhole the reques
G. This action prevents malware from communicating with unknown domains and thus prevents the WannaCry malware from becoming active.
H. Apply ACLs at the access layer that prevents all RPC and SMP communication throughout the network..

Answer: DEFG

NEW QUESTION 116
Which policy action allows to a pass without any further inspection by the intrusion when implementing Cisco Firepower access control policy?

A. Pass
B. Interactive block
C. Allow
D. Monitor
E. Block
F. Trust

Answer:

F

NEW QUESTION 121
Which action must happen before you enroll a device to a mobile device management service fro a different vendor?

A. wipe the entire device and start from scratch
B. Allow both vendor profiles remain on the device.
C. Remove the profiles form the previous vendor from the device
D. Alter the administrator so that they can remove this device form the network

Answer: C

NEW QUESTION 126
Which statement about Health Monitoring on the Firepower System is true?

A. When you delete a health policy that is applied to a device, the device reverts to the default health policy.
B. If you apply a policy without active modules to a device, the previous health policy remains in effect unless you delete it.
C. Health events are generated even when the health monitoring status is disabled.
D. Descendant domains in a multi-domain deployment can view, edit, and apply policies from ancestor domains.
E. The administrator of a descendant domain is unable to edit or delete blacklists applied by the administrator of an ancestor domain.
F. The default health policy is automatically applied to all managed devices.

Answer: C

NEW QUESTION 128
Which option is a benefit of VRF Selection Using Policy-Based Routing for routing for packets to different VPNs?

A. It suppprts more than one VPN per interface
B. It allows bidirectional traffic flow between the service provider and the CEs
C. It automatically enables fast switching on all directly connected interfaces
D. It can use global routing tables to forward packets if the destination address matches the VRF configure on the interface
E. Every PE router in the service provider MPLS cloud can reach every customer network
F. It inreases the router performance when longer subnet masks are in use

Answer: D

NEW QUESTION 132
Which two statements about DTLS are true? (Choose two.)

A. If DPD is enabled.DTLS can fall back to a TLS connection.
B. It is disabled by default if you enable SSL VPN on the interface.
C. It uses two simultaneous IPSec tunnels to carry traffic.
D. If DTLS is disabled on an interface, then SSL VPN connections must use SSL/TLS tunnels.
E. Because if requires two tunnels, it may experience more latency issues than SSL connections.

Answer: AD

NEW QUESTION 137
What technique can an attacker use to obfuscate a malware application payload, allowing it to bypass standard security mechanisms?

A. Teredo tunneling
B. A PE32 header
C. Steganography
D. BASE64
E. Decryption

Answer: D

NEW QUESTION 141
In a Cisco ISR with cloud Web Security Connector deployment, which command can you enter on the Cisco ISR G2 to verify connectivity to the CWS tower?

A. Show policy-map
B. Show service-policy
C. Show ip nbar
D. Show sw-module
E. Mtrace
F. Show content-scan summary

Answer: A

NEW QUESTION 145
Which command on Cisco ASA you can enter to send debug messages to a syslog server?

A. logging debug-trace
B. logging host
C. logging traps

D. logging syslog

Answer: A

NEW QUESTION 147
Which command on Cisco ASA you can enter to send debug messages to a syslog server?

A. logging debug-trace
B. logging host
C. logging traps
D. logging syslog

Answer: A

NEW QUESTION 152
Which three statements are true after a successful IPsec negotiation has taken place? (Choose three)

A. After IPsec tunnel is established data is encrypted using one set of DH-generated keying material
B. After the IPsec tunnel is established, data is encrypted using two sets of DH-generated keyring material
C. Two tunnels were established, the first one is for ISAKMP and IPsec negotiation and the second one is for data encryption as a result of IPsec negotiation
D. The ISAKMP tunnel was established to authenticate the peer and discreetly negotiate the IPsec parameters
E. One secure channel and one tunnel were established, the secure channel was established by ISAKMP negotiation followed by an IPsec tunnel for encrypting user data
F. The ISAKMP secure channel was established to authenticate the peer and discretely negotiate the IPsec parameters

Answer: BEF

NEW QUESTION 156
What are the three configurations in which SSL VPN can be Implemented? (Choose three)

A. WebVPN
B. PVC Tunnel Mode
C. Interactive mode
D. L2TP over IPSec
E. Thin-Client
F. AnyConnect Tunnel Mode
G. Clientless
H. CHAP

Answer: EFG

NEW QUESTION 158
Which statement about SMTP authentication in a Cisco ESA deployment is true?

A. It enables users at remote sites to retrieve their email messages via a secure client.
B. When SMTP authentication with forwarding is performed by a second SMTP server, the second server also performs the transfer of queued messages.
C. It enables user at remote sites to release email messages for spam quarantine.
D. If an authentication user belongs to more one LDAP group, each with different user roles.AsyncOs grants permissions in accordance with the least restrictive user role.
E. Clients can be authenticated with an LDAP bind or by fetching a passphrase attribute

Answer: E

NEW QUESTION 160
Which three types of addresses can the Botnet Traffic Filter feature of the Cisco ASA monitor? (Choose three)

A. dynamic address
B. known malware addresses
C. known allowed addresses
D. ambiguous addresses
E. internal addresses
F. listed addresses

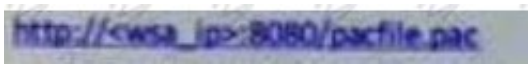
Answer: BCD

NEW QUESTION 165
Which location for the PAC file on Cisco IronPort WSA in the default?
A)


B)


C)


D)



A. Option A
B. Option B
C. Option C
D. Option D

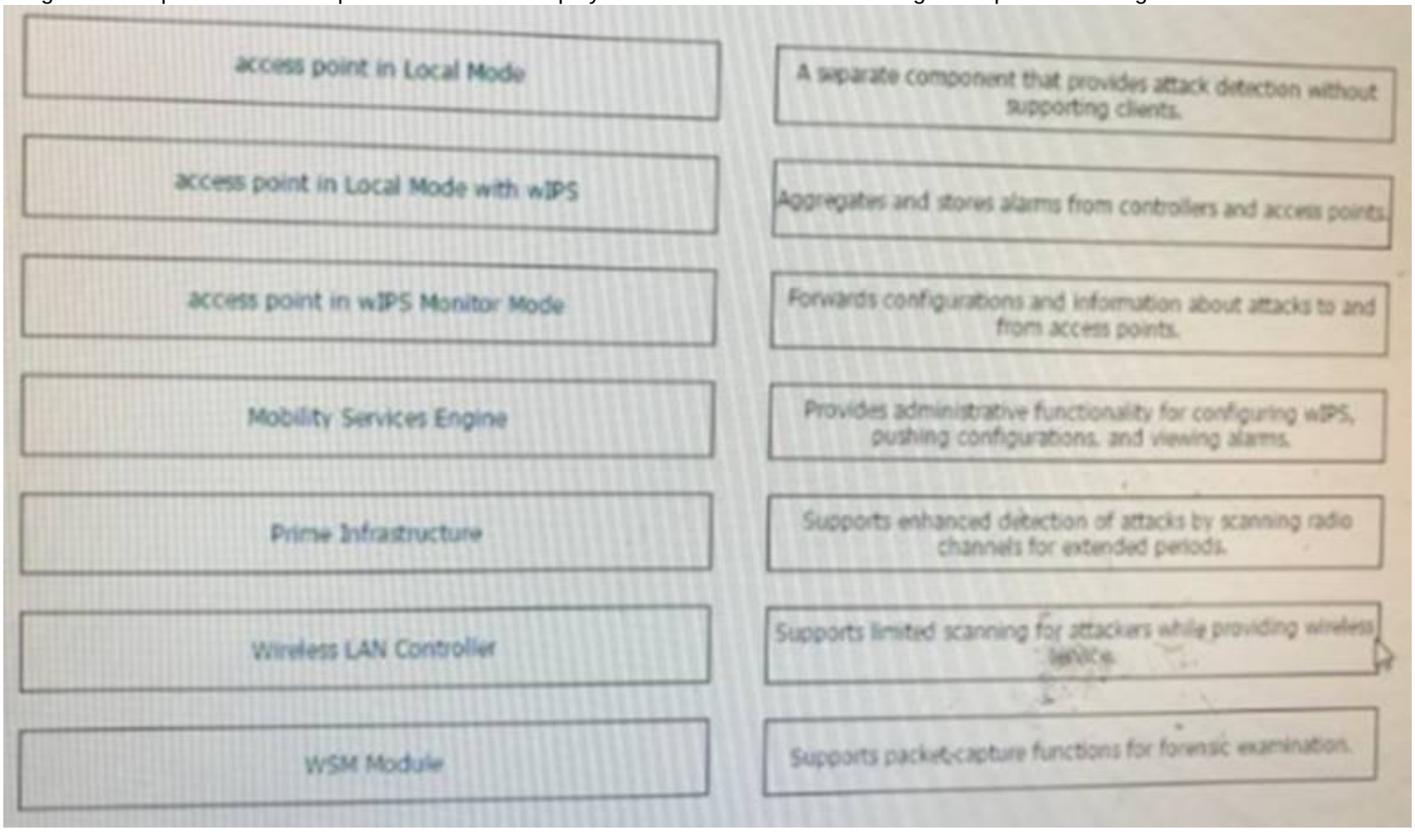
Answer: A

NEW QUESTION 166
In TLS Implementation on the Cisco Email Security Appliance cluster, the machine is removed from the cluster and then added back. Which description of what happens to the machine-level certificate true?

A. ESA cannot provider privacy for point-to point transmission of emails through encryption
B. The machine-level certificates are lost
C. The machine-level certificates are rebuilt by RAID 5
D. The cluster goes down.

Answer: C

NEW QUESTION 170
Drag each component of an Adaptive Wireless IPS deployment on the left to the matching description on the right



Answer:

Explanation: 1-F, 2-E, 3-B, 4-G, 5-D, 6-C, 7-A

NEW QUESTION 171
Which IPS deployment mode can blacklist traffic?

A. Transparent
B. Strict
C. Inline
D. Passive
E. Tap
F. Switched

Answer: C

NEW QUESTION 174
Which two statements about MACsec are true? (Choose two)

A. It maintains network intelligence as it applied to router uplinks and downlinks.
B. It works in conjunction with IEEE 802.1X -2010 port-based access control.
C. It uses symmetric-key encryption to protect data confidentiality.

D. It encrypts packets at Layer 3, which allows devices to handle packets in accordance with network polices.
E. It can be enabled on individual port at Layer 3 to allow MACsec devices to access the network.
F. It can use IEEE 802.1x master keys to encrypt wired and wireless links

Answer: BC

NEW QUESTION 175
What are two characteristics of RPL, used in IoT environments?(Choose two)

A. It is an Exterior Gateway Protocol
B. It is a Interior Gateway Protocol
C. It is a hybrid protocol
D. It is link-state protocol
E. It is a distance-vector protocol

Answer: BE

NEW QUESTION 178
How does a Cisco ISE server determine whether a client supports EAP chaining?

A. It sends an identity-type TLV to the client and analyzes the response.
B. It analyzes the options field in the TCP header of the first packet it receives from the client.
C. It analyzes the X.509 certificate it receives from the client through the TLS tunnel.
D. It send an MD5 challenge to the client and analyzes the response.
E. It analyzes the EAPoL message the client sends during the initial handshake.

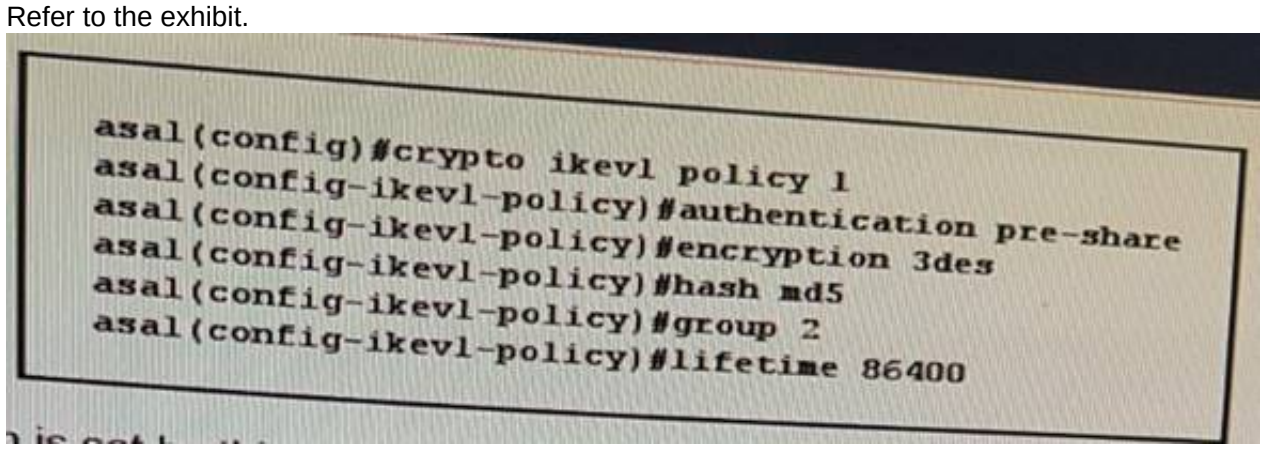
Answer: A

NEW QUESTION 180
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 be best to verify that traffic is reaching the Linux Server eth0 interface?

A. tcpdump -I eth0 host 10.10.7.4 and host 11.0.1.9 and port 8080.
B. tcpdump -l eth0 host 10.10.7.4 and 11.0.1.9.
C. tcpdump -I eth0 dst 11.0.1.9 and dst port 8080.
D. tcpdump -I eth0 scr 10.10.7.4 and dst 11.0.1.9 and dst port 8080

Answer: D

NEW QUESTION 182
Refer to the exhibit.



Which level of encryption is set by this configurations?

A. 1024-bit
B. 192-bit
C. 56-bit
D. 168-bit

Answer: D

NEW QUESTION 185
Refer to the exhibit.
Which effect of this configuration is true?

A. The minimum size of TCP SYN+AK packets passing the router is set to 1452 bytes and the IP MTU of the interface is set to 1492 bytes.
B. The minimum size of TCP SYN+AK packets passing the transient host is set to 1452 bytes and the IP MTU of the interface is set to 1492 bytes.
C. The MSS of TCP SYN packets is set to 1452 bytes and the IP MTU of the interface is set to 1492 bytes.
D. The PMTUD value sets itself to 1452 bytes when the interface MTU is set to 1492 bytes.
E. SYN packets carry 1452 bytes in the payload when the Ethernet MTU of the interface is set to 1492 bytes.

Answer: C

NEW QUESTION 187
Which statement about SenderBase sender-reputation filtering approaches on the Cisco

A. The conservative approach provides near zero false positives at the cost lower performance
B. The aggressive approach provides near zero false positives at the cost of lower performance
C. The aggressive approach provides maximum performance at the cost of numerous
D. The moderate approach provides maximum performance with some false positives
E. The conservative approach provides good performance with near zero false positives
F. The moderate approach combines high performance with some false positives

Answer: F

NEW QUESTION 189
Which two statement about RADIUS VSAs are true?(Choose two)

A. They allow the RADIUS server to exchange vendor-specific information with the network access server
B. They allow product form the other vendors to Interoperate with Cisco routers that support RADIUS
C. They VSA Implementation supports multiple VSAs, including cisco-avpair
D. They can be used for both authentication and authentication on Cisco routers
E. Cisco's unique vendor-ID is 26
F. Cisco VSA Implementation allow TACACS+ authorization features to be used with a RADIUS server

Answer: AF

NEW QUESTION 190
Which Cisco Firepower intrusion Event Impact level indicates the vulnerable to the attack, and requires the most immediate urgent.

A. Impact Level 3
B. Impact Level 4
C. Impact Level 2
D. Impact Level 0
E. Impact Level 1

Answer: E

NEW QUESTION 193
Which definition of Machine Access Restriction is true?

A. MAR offer security information and event management
B. MAR provides detailed malware analysis reports
C. MAR identifies threats on the cisco network by "learning" the topology, configuration and behavior you environment
D. MAR is feature introduced into ISE and ACS as a way to verify a successful machine authenticated
E. MAR provides user authentication

Answer: D

NEW QUESTION 195
Which of the following is AMP Endpoint offline engine for windows?

A. ClamAV
B. ClamAMP
C. TETRAAMP
D. TETRA

Answer: D

NEW QUESTION 200
Which three authorization technologies does Cisco TrustSec support? (Choose three)

A. 802.1X
B. SGACL
C. DACL
D. MAB
E. SGT
F. VLAN

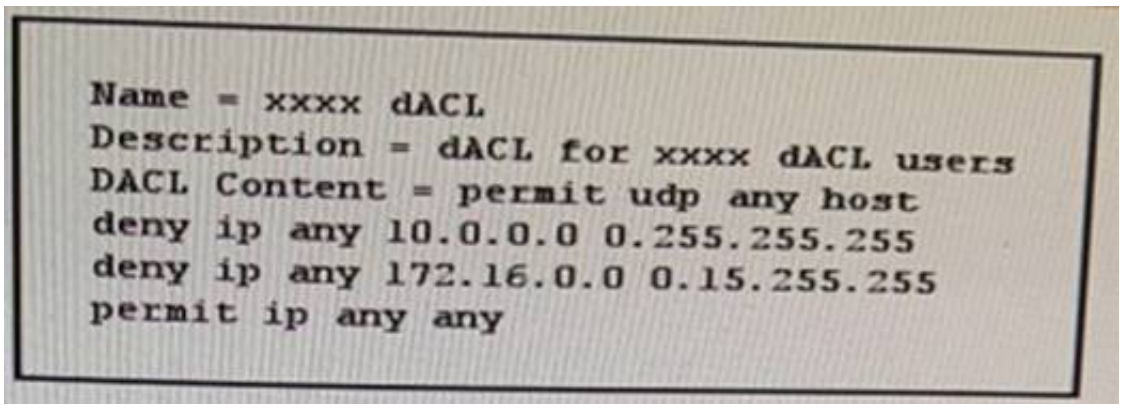
Answer: CEF

NEW QUESTION 201
Which three ISAKMP SA Message States can be output from the device that initiated an IPSec tunnel? (Choose three)

A. MM_WAIT_MSG4
B. MM_WAIT_MSG2
C. MM_WAIT_MSG5
D. MM_WAIT_MSG6
E. MM_WAIT_MSG1
F. MM_WAIT_MSG3

Answer: ABD

NEW QUESTION 205
Refer to the exhibit.



For which type of user is this downloadable ACL appropriate?

A. management
B. employees
C. guest users
D. network administrator
E. onside contractors

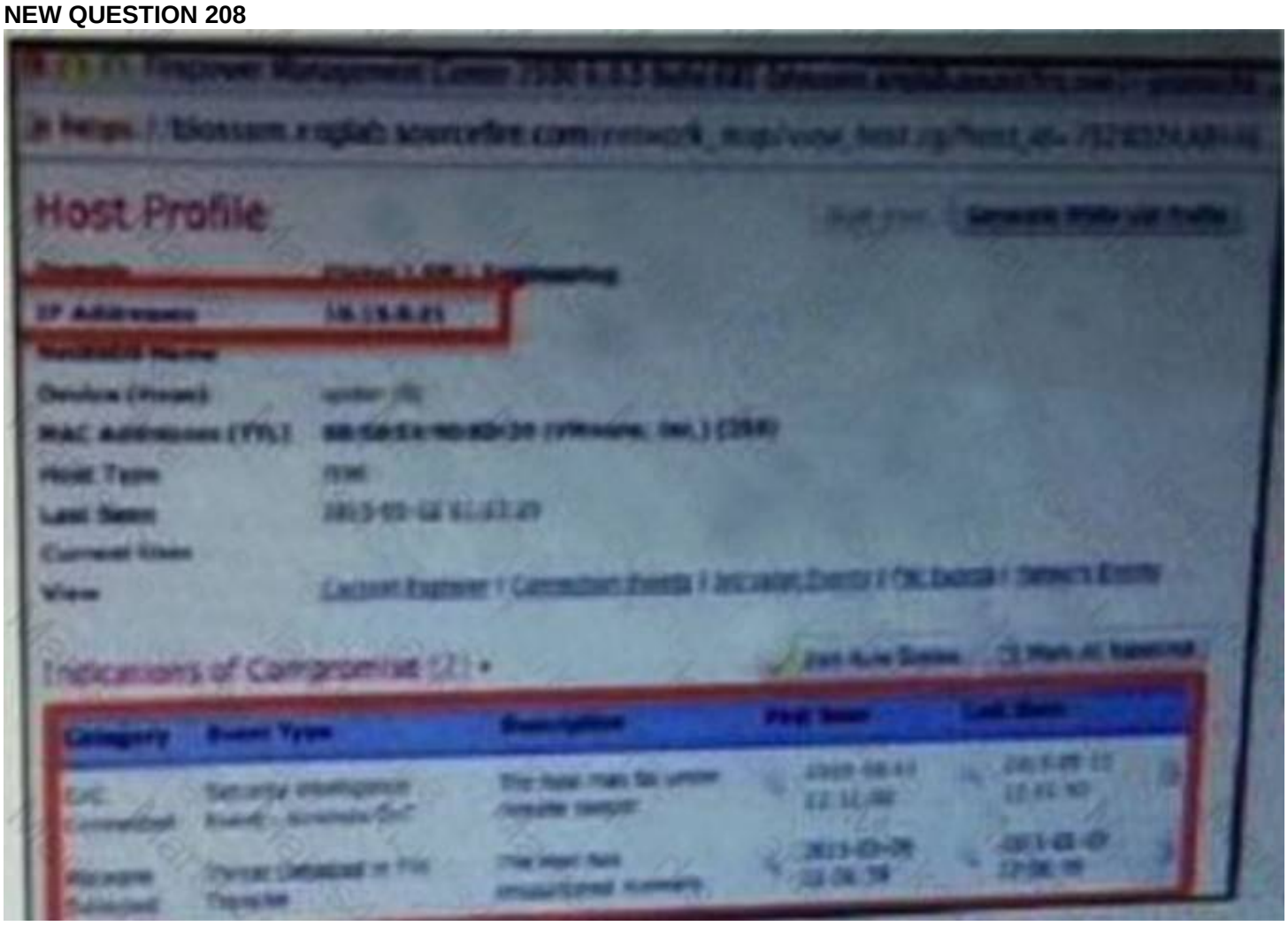
Answer: C

NEW QUESTION 207
Which two functions of Cisco Content Security Management Appliance are true?(Choose two)

A. SMA is used for on-box management of WSAs
B. SMA is used to configure NSAMP on the router
C. SMA is a centralized system used to collectively mange and report the WSAs that are deployed in a network
D. SMA is used for sandboxing functionality to perform malware analysis
E. SMA is unified management platform that manages web security, performs troubleshooting and maintains space for data storage.

Answer: CE

NEW QUESTION 208

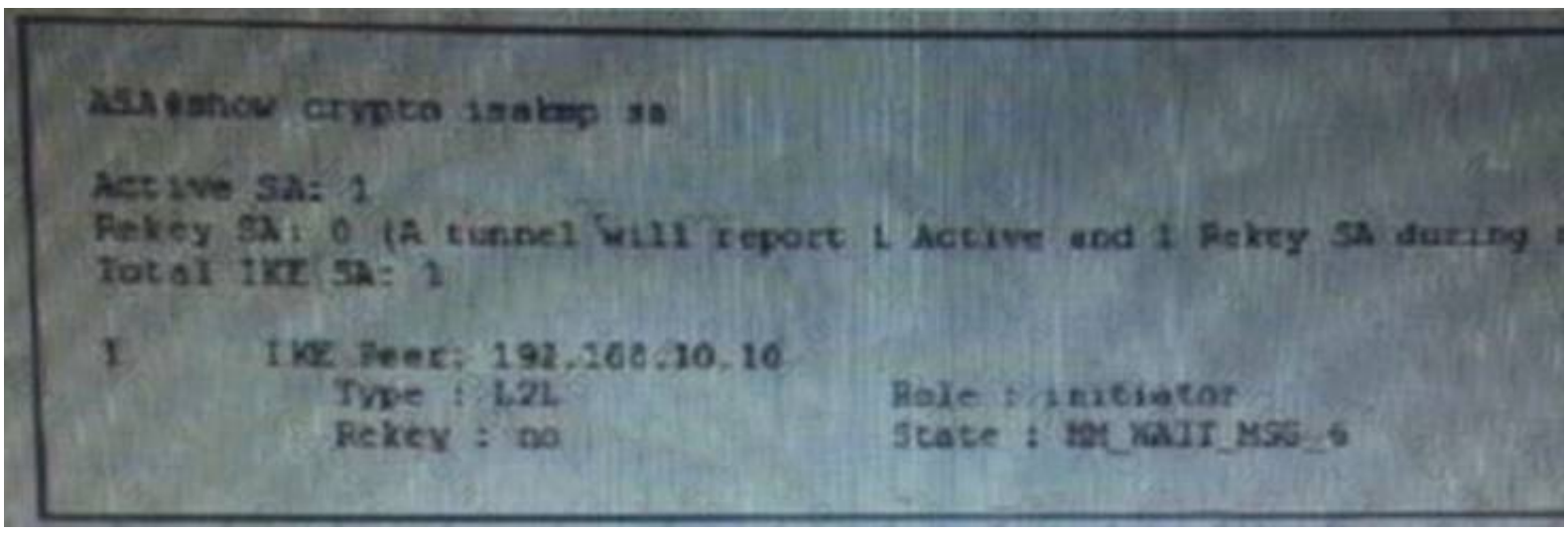


Refer the exhibit, Which Cisco firepower policy has detected a “CnC Connector” of comp event?

A. DNS policy
B. Network analysis policy
C. Identity policy
D. SSL policy
E. File policy
F. Intrusion policy

Answer: F

NEW QUESTION 210
Refer to the exhibit,



you issued the show crypto isakmp sa command to troubleshot of IPsec VPN. What possible issue does the given output indicate?

A. The peer is failing to respond
B. The crypto ACU are mismatched
C. The pre-shared keys ire mismatched
D. The transform sets are mismatched

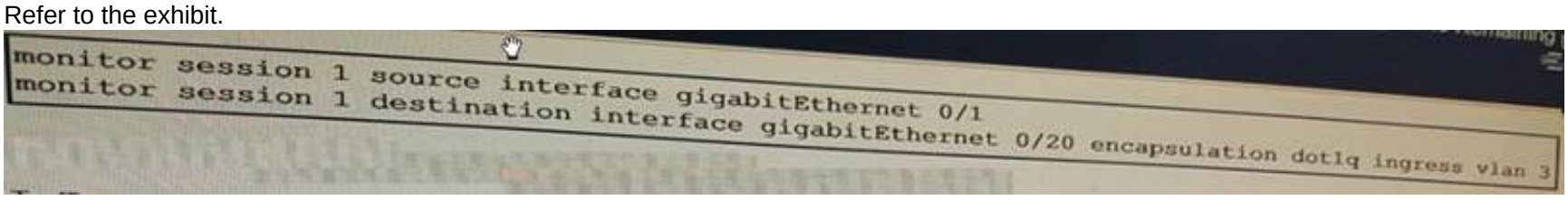
Answer: C

NEW QUESTION 212
Which ports is used by ISE pxGrid service for inter-node communication?

A. UDP port 161 and 162
B. TCP port 443
C. TCP port 5222
D. UPD port 9995

Answer: C

NEW QUESTION 214
Refer to the exhibit.

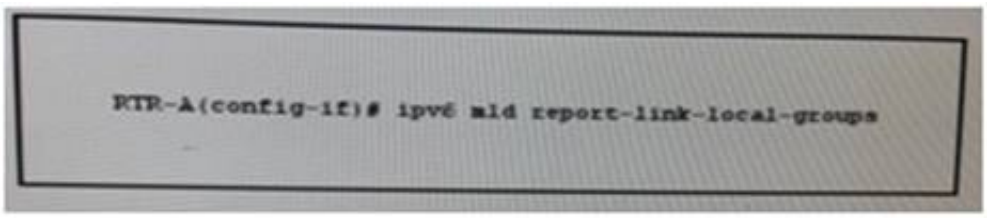


What are two functionalities of this configuration? (Choose two)

A. Traffic will not be able to pass on gigabitEthernet0/1.
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 do deep scan on dot1q encapsulation traffic
E. Traffic will only be sent to gigabitEthernet 0/20

Answer: BE

NEW QUESTION 215
Refer to the exhibit.

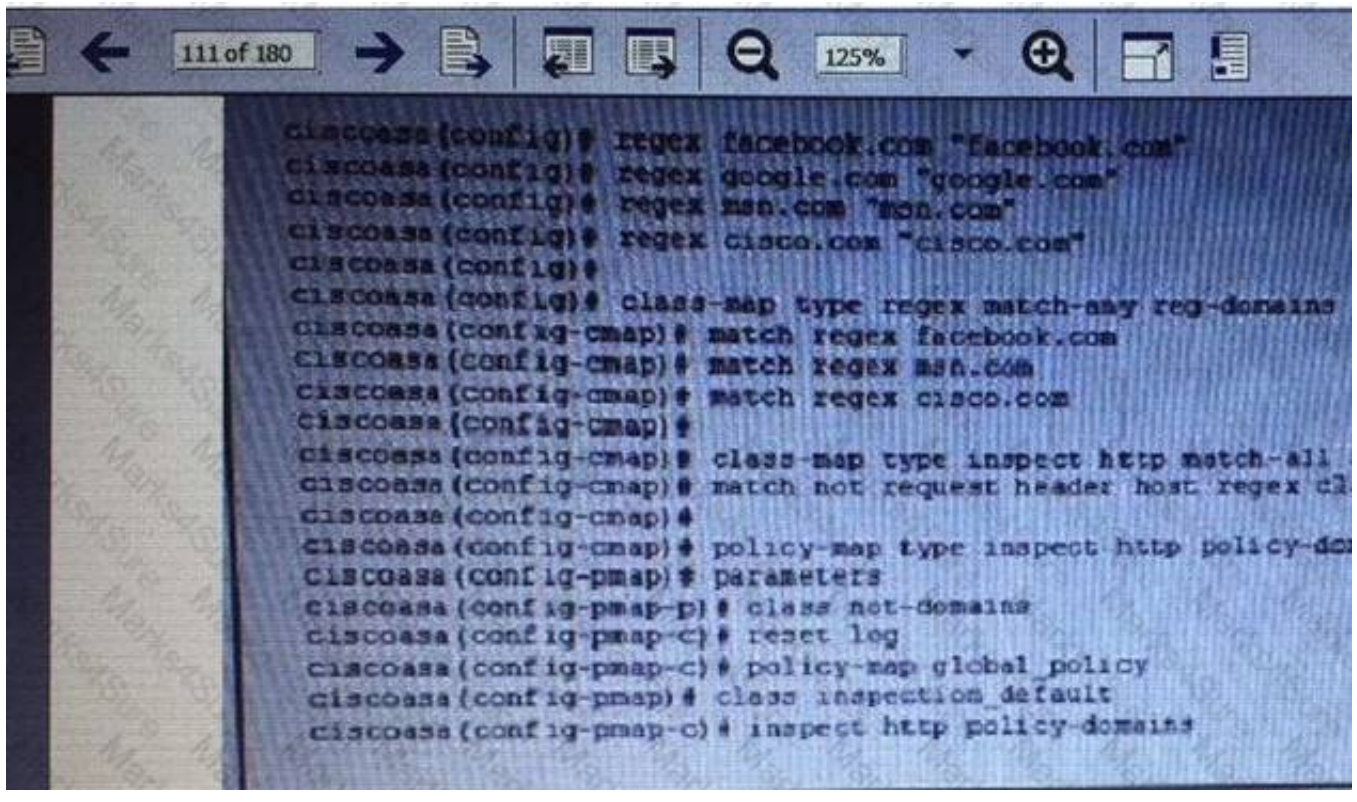


RTR-A(config-if)# ipv6 mld report-link local-groups
Which effect of this configuration is true?

A. It enables MLD query messages for all link-local groups.
B. It enables local group membership for MLDv1 and MLDv2.
C. It enabled hosts to send MLD report messages for groups in 224.0.0.0/24.
D. It enables the host to send MLD report messages for nonlink local groups.
E. It configures the node to generate a link-local group report when it joins the solicited-node multicast group.

Answer: C

NEW QUESTION 220
Exhibit:



Refer to the exhibit, what is the effect of the given service policy

A. It blockscisco.com, msn.com, and facebct3k.com and permanant
B. It blocks facebook.com, msn.com, cisco.com and google.com
C. It blocks all domains except facebook.eom, msn.com, cisco
D. It blocks all domains except cisco.com, msn, com; and facebook.com

Answer: D

NEW QUESTION 223
An organization is deploying FTD in the data center. Products applications have been connected; however, ping tests to resources firewall has two interfaces, INSIDE and OUTSIDE. The problem might testing scenario is from the OUTSIDE. Which two commands can be the situation and determine where the issue might be? (Choose two)

A. Packet-tracer input Outside <Protocol> < Destination IP> <Source
B. Packet-tracer input Outside <Protocol> <Source IP> <Source Port
C. Packet-tracer input Inside <Protocol> < Destination IP> <Source
D. Packet-tracer input Inside <Protocol>< Destination IP> < Destination
E. Packet-tracer input Outside <Protocol>< Destination IP> < Destination
F. Packet-tracer input Inside<Protocol> < Source IP> < Source Port:

Answer: BF

NEW QUESTION 228
Which statement about MDM is true?

A. If can support endpoints without requiring them to register
B. if an authorized user refreshes the web browser, the session must be reauthorized with the LDAP server
C. Cisco iSE communication with the MDM server by way of REST API calls
D. MDM policies can be configured with as few as two attributes
E. it reports the IP address of the endpoint to the Cisco ISE as the input parameter of the endpoint
F. Each cisco ISE node requires its own MDM server

Answer: C

NEW QUESTION 229
Which three Cisco attributes for LDAP authorization are supported on the ASA? (Choose three)

A. Web-VPN-ACL-Filters
B. IPsec-Default-Domain
C. IPsec-Client-Firewall-Name
D. Authorization-Type
E. L2TP-Encryption
F. Authenticated-User-idle-Timeout

Answer: ABF

NEW QUESTION 230
Which Cisco ASA firewall mode supports ASDM one-time-password authentication using RSA SecurID?

A. network translation mode
B. transparent mode
C. single-context routed mode
D. multiple-context mode

Answer: C

NEW QUESTION 232
Which two statements about application protocol detectors in the Cisco Fire? (Choose two)

A. They can analyze network traffic for specific application fingerprints
B. Port-based application protocol detectors can be modified for use as custom
C. Port-based and Firepower-based application protocol detectors can be import
D. firepower-based application protocol detectors are built in to the Firepower deactivated only by the system
E. They can be activated by VDB updates, but must be deactivated manually
F. They can detect web-based application activity in HTTP traffic

Answer: BE

NEW QUESTION 236
Which feature of WEP was intended to prevent an attacker from altering and resending data packets over a WEP connection ?

A. The RC4 cipher
B. Transport Layer Security
C. Message Intergrity checks
D. MD5 hashing
E. The cyclic redundancy check

Answer: E

NEW QUESTION 241
Refer to the exhibit.

```
class Partner-Class
limit-resource routers 50
limit-resource ASDM 4
limit-resource VPN other 400
limit-resource xlates 18000
```

Which effect of this configuration is true?

A. It allows each context to user all available resources.
B. It oversubscribes VPN sessions for the given class.
C. It creates a default class.
D. It creates a resource class.

Answer: D

NEW QUESTION 244
Which two statements about internal detectors in the Cisco Firepower System are true? (Choose two)

A. They are built in to the Firepower system and delivered automatically with firepower updates
B. They can be activated manually or configured to activate automatically under specific conditions
C. They can be modified for use as custom detectors
D. They can detect client and application traffic
E. They can detect only web-based application activity in FTTP traffic.
F. They can be deactivated manually or by VDB updates

Answer: AE

NEW QUESTION 247
Which two methods can be used to remove the previous vendor profiles the mobile device?

A. Disable the ISE profiling feature
B. Vendor profiles cannot be remove
C. Go to My Devices portal in ISE and click corporate wipe
D. Use the “full wipe” option and reset the device to factory setting
E. Use the “corporate wipe” option offered by the vendor

Answer: CE

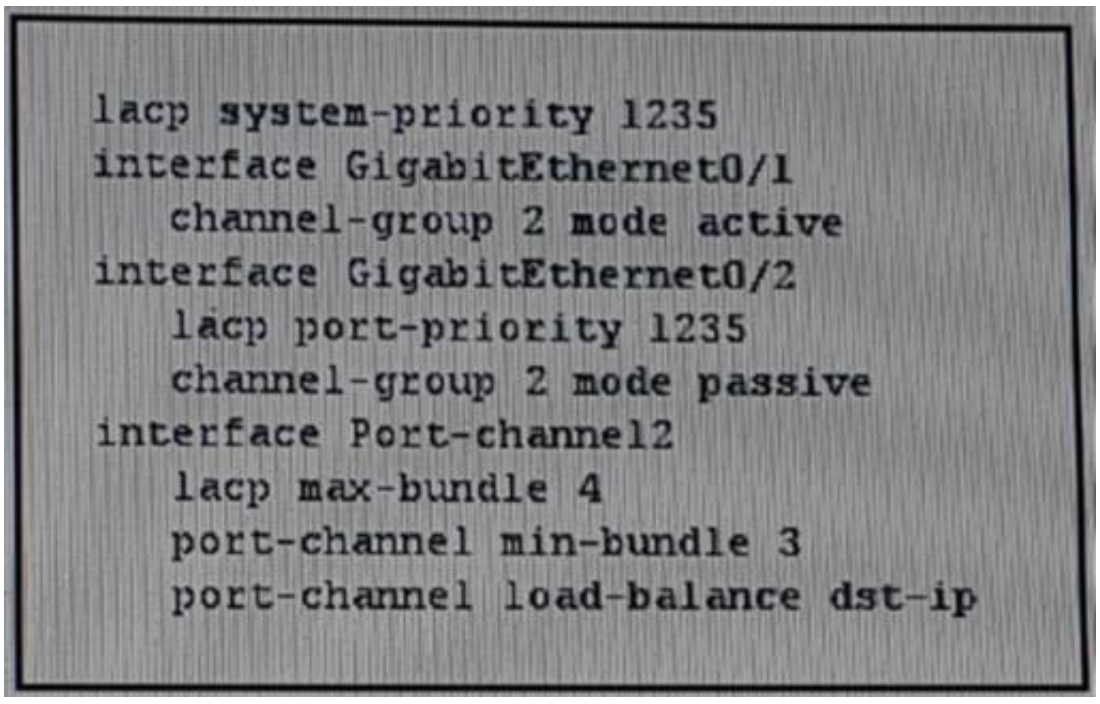
NEW QUESTION 250
Refer to the exhibit:
1d00h: IPSec (validate transform proposal): proxy identities not supported 1d00h: ISAKMP: IPSec policy invalid proposal
1d00h: ISAKMP (0:2): SA not acceptable

This error message is displayed while troubleshooting a newly set up IPsec VPN tunnel. Which cause is the most probable?

A. Peer information is incorrectly configured on the remote IPsec router.
B. the Phase 1 policies are not compatible
C. the Phase 2 policies are not compatible
D. Crypto ACLs are not correctly mirrored on both ends of the tunnel.
E. Peer information is incorrectly configured on both sides of the tunnel.

Answer: C

NEW QUESTION 251
Refer to the exhibit.



After you applied this EtherChannel configuration to a Cisco ASA, the EtherChannel Failed to come up.
Which reason for the problem is the most likely?

A. The lacp system-priority and lacp port-priority values are the same.
B. The EtherChannel requires three ports, and only two are configured.
C. The Ehterchannel is disabled.
D. The channel-group modes are mismatched.

Answer: B

NEW QUESTION 253
Which two statements about MAB are true? (Choose two)

A. It requires the administrator to create and maintain an accurate database of MAC addresses.
B. It server at the primary authentication mechanism when deployed in conjunction with 802.1x.
C. It operates at Layer 2 and Layer 3 of the OSI protocol stack.
D. It can be used to authenticate network devices and users.
E. MAC addresses stored in the MAB database can be spoofed.
F. It is a strong authentication method.

Answer: AE

NEW QUESTION 257
Which two statements about NetFlow Secure Event Logging on a Cisco ASA are true? (Choose two)

A. It tracks configured collectors over TCP.
B. It is supported only in single-context mode.
C. It can export templates through NetFlow.
D. It can be used without collectors.
E. It supports one event type per collector.
F. It can log different event types on the same device to different collectors.

Answer: CF

NEW QUESTION 258
Which two parameters must be identical per interface while configuring virtual port channels (Choose two)

A. network access control
B. IP sourcegard
C. Prrotocol independent multicast
D. Bridge Assurance setting
E. maximum transmission unit

Answer: DE

NEW QUESTION 262
Which statement about Cisco Firepower Advanced Malware

A. With dynamic analysis, the system pre classifies suspicious files a them to the AMP Threat Grid for analysis
B. If the system determines a file inside an archive to be malware, blocking the archive
C. The SHA-256 value of a file is calculated only if you configure a Lookup action
D. If the system pre classifies a file potential malware, it automatic; administrator to take further action
E. When local malware analysis is complete, it produces a threat s details of the analysis
F. The AMP for Firepower network-based solution supports malware files types than AMP for endpointsThe system can analyze up to two layers of nested files in ZIP are block files with more layers

Answer: A

NEW QUESTION 263
Which statement about the Cisco AMP Virtual Private Cloud Appliance is true for deployments in cloudproxy mode?

A. The appliance can perform disposition lookups against the Protect DB without an internet connection
B. The amp-sync tool syncs the threat-intelligence repository on the appliance on the AMP public cloud through the Update Host
C. The appliance can automatically download threat-intelligence updates directly from the AMP public cloud
D. The updates Host automatically downloads updates and deploys them to the Protect DB on a daily basis
E. The appliance communicates directly with the endpoint connectors only

Answer: C

NEW QUESTION 267
Which statement about the TLS security protocol is true?

A. TLS version 1.0 is less secure then SSL version 3.0
B. The TLS and SSL versions can interoperate in the client-server handshake
C. It is always recommended to disable TLS version 1.0 in the browser so that it only supports SSL for better security
D. You need to replace SSL certificate with TLS certificate for successful TLS operation
E. There are differences between TLS and SSL version 2 and 3
F. It only supports data authentication for the client-server session using a browser

Answer: E

NEW QUESTION 271
In your network, you require all guests to authenticate to the network before getting access. However, you don't want to be stuck creating or approving accounts. It is preferred that this is all taken care by the user, as long as their device is registered. Which two mechanisms can be used to provide this functionality? (Choose two.)

A. Social media login, with device registration
B. Guest's own organization authentication service, with device registration
C. PAP based authentication, with device registration
D. Active Directory, with device registration
E. 802.1x based user registration, with device registration
F. Self-registration of user, with device registration

Answer: AF

NEW QUESTION 273
Which of the following could be an evasion technique used by the attacker?

A. Port access using Dot1x
B. ACL implementation to drop unwanted traffic
C. TELNET to launch device administration session
D. Traffic encryption to bypass IPS detection
E. URL filtering to block malicious sites
F. NAT translations on routers and switches

Answer: D

NEW QUESTION 276
There is no ICMP connectivity from VPN_PC to Server1 and Server2. What could be the possible cause?

A. The action is incorrect in the access rule
B. The destination port configuration is missing in the access rule
C. The server network has incorrect mask in the access rule
D. The VLAN tags configuration is missing in the access rule
E. The source network is incorrect in the access rule
F. The zone configuration is missing in the access rule

Answer: E

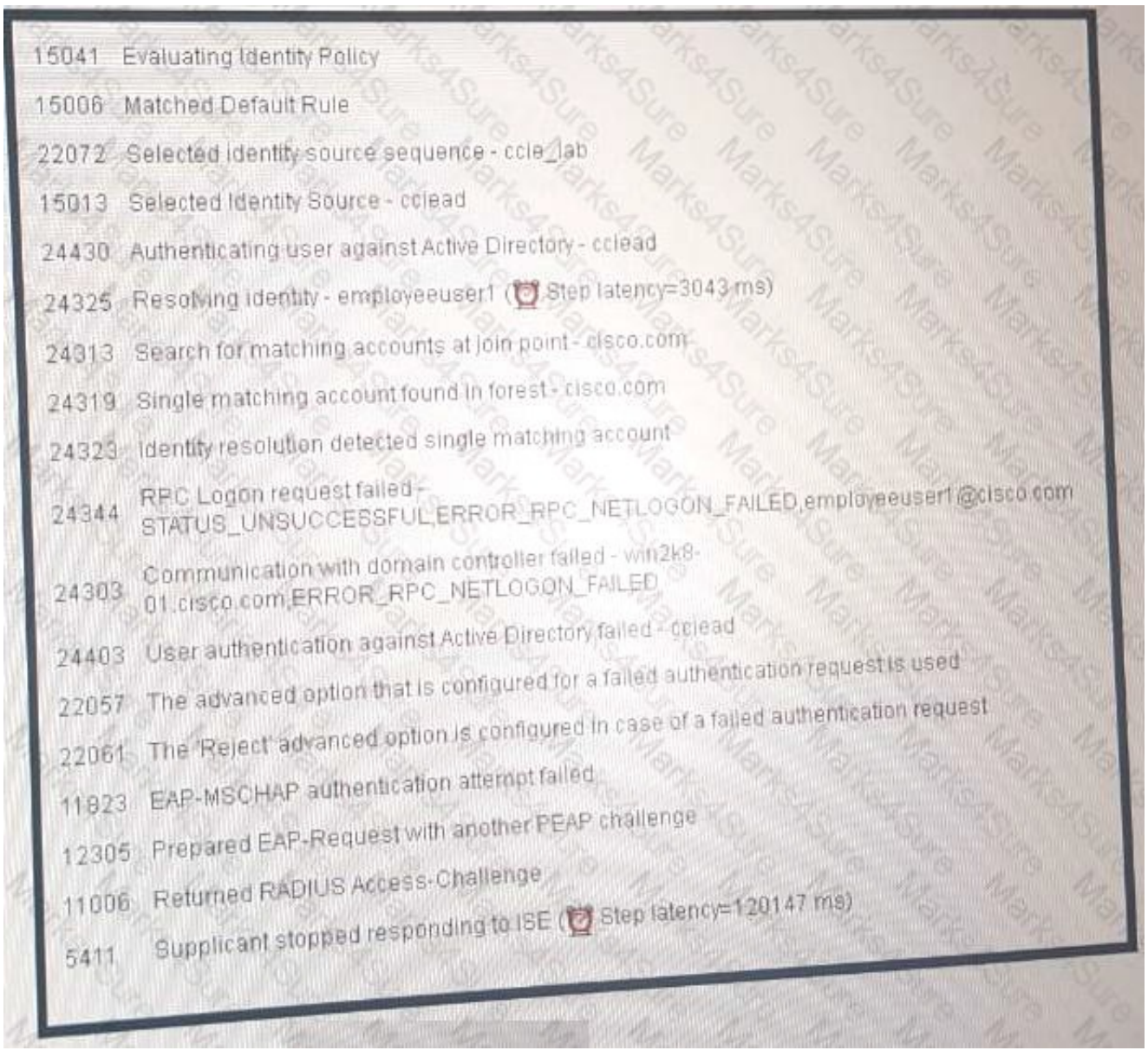
NEW QUESTION 278
Which of the following is the correct rule with regards to Zone-Based Firewall implementation?

A. Interface can be a member of only one zone.
B. All the interfaces of the device cannot be the part of the same zone.
C. If interface belongs to a zone then the traffic to and from the interface is always allowed.

D. By default traffic between the interfaces in the same zone is dropped.
E. Zone pair cannot have a zone as both source and destination.
F. If default zone is enabled then traffic from zone interface to non-zone interface will be dropped.

Answer: A

NEW QUESTION 280
Refer to the exhibit. Refer to the Exhibit.

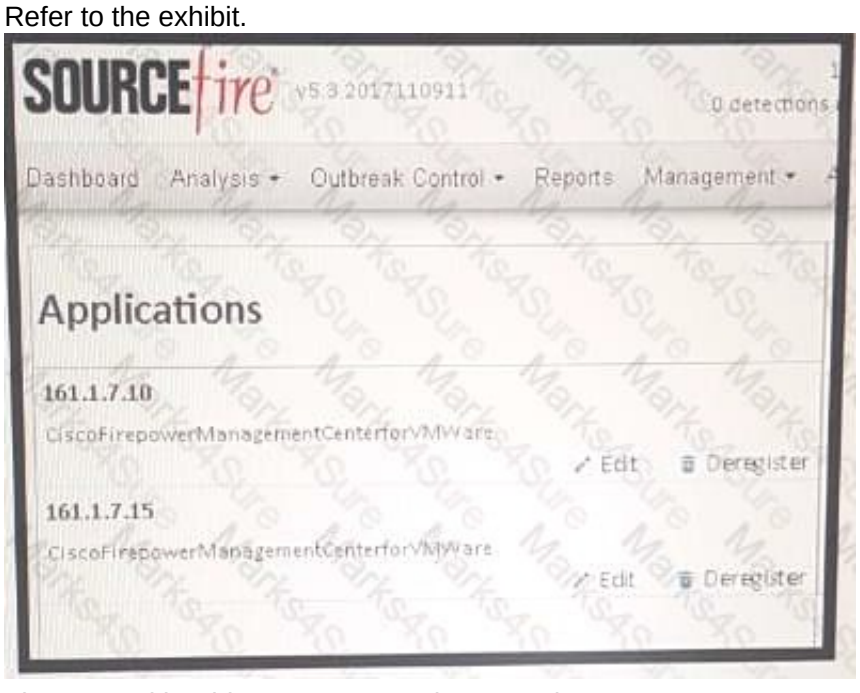


What could be the reason for Dot1x session failure?

A. Incorrect identity source referenced
B. Incorrect authorization permission
C. Incorrect authentication rule
D. Identity source has the user present but not enabled
E. Incorrect authorization condition
F. Incorrect user group
G. Incorrect user string

Answer: D

NEW QUESTION 285
Refer to the exhibit.



The FMC with address 161 1 7 16 is not seeing AMP Connector scan events that are reported to the AMP cloud from the test-pc Windows machine that belongs to "protect" group. Which cause of the issue is true?

A. The Windows machine belongs to an incorrect group in the AMP cloud policy.
B. The FMC was not added in the AMP cloud.

C. The incorrect group is selected for the events export in the AMP cloud for the FMC.
D. The Event must be viewed as a Connection event in the FMC.
E. The AMP cloud was not added in the FMC.
F. The Windows machine is not reporting scan events to the AMP cloud.
G. The Windows machine is not reporting events to the FMC.

Answer: A

NEW QUESTION 286
Which two events can cause a failover event on an active/standby setup? (Choose two.) E . The unit that was previously active recovers

A. The stateful failover link fails
B. The failover link fails
C. The active unit experiences interface failure above the threshold
D. The active unit fails

Answer: CD

NEW QUESTION 289
In your ISE design, there are two TACACS profiles that are created for device administration: IOS_HelpDesk_Profile, and IOS_Admin_Profile. The HelpDesk profile should login the user with privilege 1, with ability to change privilege level to 15. The Admin profile should login the user with privilege 15 by default. Which two commands must the HelpDesk enter on the IOS device to access privilege level 15? (Choose two)

A. enable secret
B. enable 15
C. privilege level 15
D. enable privilege 15
E. enable
F. enable IOS_Admin_Profile
G. enable password

Answer: BE

NEW QUESTION 291
Which criteria does ASA use for packet classification if multiple contexts share an ingress interlace MAC address?

A. ASA ingress interface IP address
B. policy-based routing on ASA
C. destination IP address
D. destination MAC address
E. ASA ingress interface MAC address
F. ASA NAT configuration
G. ASA egress interface IP address

Answer: E

NEW QUESTION 293
The SAML Single Sign-on ISE is supported by which four portals? (Choose four.)

A. Sponsor Portal
B. BYOD Portal
C. Employee Portal
D. Contractor Portal
E. Guest Portal (sponsored and self-registered)
F. My devices Portal
G. Wireless Client Portal
H. Certificate Provisioning Portal

Answer: AEFH

NEW QUESTION 297
Which statement is an advantage of network segmentation?

A. It enables efficient network monitoring due to a flat network
B. It takes less time to design a complex network with segmentation as one of the critical requirements
C. It allows flat network design for better security implementation
D. It allows efficient containment of a security incident as the effect will be limited to local subnet
E. It improves network performance by having broadcast traffic not limited to local subnets
F. It allows users to access the resource even though they won't need to for better visibility

Answer: D

NEW QUESTION 302
Aclientcomputerat10.10.7.14istryingtoaccessaLinuxserver(11.0.1.9)thatisrunninga TomcatServer application. What TCP dump filter would be the best to verify that traffic is reaching the Linux Server eth0 interface?

A. tcpdump -i eth0 host 10.10.7.2 and host 11.0.1.9 and port8080

B. tcpdump -i eth0 host 10.10.7.2 and11.0.1.9
C. tcpdump -i eth0 host dst 11.0.1.9 and dst port8080
D. tcpdump -i eth0 host 10.10.7.2 and dst 11.0.1.9 and dst port 8080

Answer: A

NEW QUESTION 303
Refer the exhibit.
Missing Exhibit
ASA at 150.1.7.43 is configured to receive IP address to SGT mapping from ISE at 161.1.7.14. Which of the following is true regarding packet capture from wireshark?

A. SXP keepalive message using TCP originated from ISE
B. ISE keepalive message for NDAC connection using TCP originated from ASA
C. TACACS connection keepalive using UDP originated from ASA
D. RADIUS connection keepalive using TCP originated from ISE
E. NTP keepalive message using UDP originated from ISE
F. SXP keepalive message for SXP connection using UDP originated from ASA

Answer: A

NEW QUESTION 304
Which statement is true regarding x.509 certificate?

A. The version number in the certificate is the OS version of CA
B. The Subject Distinguished Name in the certificate is of the entity who issued the certificate
C. The algorithm in the certificate is used by the issuer to sign the certificate
D. The serial number in the certificate is common across the certificates issued by the same CA
E. The algorithm in the certificate is used by the subject to encrypt the traffic
F. The Issuer Distinguished Name in the certificate is of the entity to which the certificate is issued

Answer: C

NEW QUESTION 306
Which statement is correct regarding Cisco VSG functionality?

A. It allows Active-Active failover operation mode when deployed as HA pair.
B. It applies security profile only after VM instantiation.
C. It allows third-party orchestration tool to interact with XML API's for its provisioning.
D. It does not allow to extend Zone-based firewall capabilities to VMs on VXLAN.
E. It allows administrative segregation due to which Security Administration can author and manage port profiles.
F. It does not provide trusted access to VMs in an enterprise data center.

Answer: C

NEW QUESTION 308
Refer to the exhibit. Which two effects of this configuration are true? (Choose two.) Case Study Title (Case Study):
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. The device allows multiple authenticated sessions for a single MAC address in the voice domain
C. If multiple hosts have authenticated to the sameport, each can bein their own assigned VLAN
D. If the authentication priority is changed the order in which authentication is performed also changes
E. The switch periodically sends an EAP-Identity-Request to the endpoint supplicant
F. The port attempts 802.1x authentication first, and then falls back to MAC authentication bypass

Answer: A

NEW QUESTION 309
Which statement is true regarding TLS security protocol?

A. It only supports data authentication for the client-server session using a browser
B. TLS and SSL versions can interoperate in the client-server handshake
C. There is no difference between TLS and SSL versions 2 and 3
D. TLS versoin 1.0 ismore secure then SSL version 3.0
E. It is always recommended to disable TLS version 1.0 in the browser so that it only supports SSL for better security
F. You need to replace SSL certificate with TLS certificate for successful TLS operation

Answer: D

NEW QUESTION 310
Refer to the exhibit. aaa new-model
aaa authentication login default group radius aaa authentication login NO_AUTH none aaa authentication login vty local
aaa authentication dot1x default group radius aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius

!u
sername cisco privilege 15 password 0 cisco dot1x system-auth-control
!i
nterface GigabitEthernet0/2 switchport mode access
ip access-group Pre-Auth in authentication host-mode multi-auth authentication open
authentication port-control auto
!v
lan 50
interface Vlan50
ip address 50.1.1.1 255.255.255.0
!i
p dhcp excluded-address 5.1.1.1 ip dhcp pool pc-pool
network 50.1.1.0 255.255.255.0
default-router 50.1.1.1
!i
p access-list extended Pre-Auth
permit udp any eq bootpc any eq bootps deny ip any any
!r
adius server ccie
address ipv4 161.1.7.14 auth-port 1645 acct-port 1646 key cisco
!l
ine con 0
login authentication NO_AUTH lien vty 0 4
login authentication vty
One of the Windows machines in your network is having connectivity issues using
802.1 x. Windows machines are set up to acquire an IP address from the DHCP server configured on the switch, which is supposed to hand over IP addresses from the 50.1.1.0/24 network, and forward AAA requests to the radius server at 161.1.7.14 using shared key "cisco". Knowing that interface Gi0/2 on SW1 may receive authentication requests from other devices and looking at the provided switch configuration, what could be the possible cause of this failure?

A. There is a RADIUS key mismatch
B. Authentication for multiple hosts is not configured on interface Gi0/2
C. 802.1x authentication is not enabled on interface Gi0/2.
D. An incorrect IP address is configured for SVI 50.
E. aaa network authorization is not configured.
F. 802.1x is disabled on the switch.
G. An incorrect default route is pushed on supplicant form SW1.

Answer: C

NEW QUESTION 311
Which statement about Remote Triggered Black Hole Filtering feature is true?

A. It works in conjunction with QoS to drop the traffic that has a lower priority.
B. The Null0 interface used for filtering able to receive the traffic but never forwards it.
C. In RTBH filtering, the trigger device redistributes dynamic routes to the eBGP peers.
D. It helps mitigate DDoS attack based only on destination address.
E. It drops malicious traffic at the customer edge router by forwarding it to a Null0 interface.
F. In RTBH filtering, the trigger device is always an ISP edge router.

Answer: C

NEW QUESTION 315
Refer to the exhibit.
R3
ip vrf mgmt
!c
rypto keyring CCIE vrf mgmt
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco
!c
rypto isakmp policy 33 encr 3des authentication pre-share group 2
lifetime 600
!c
rypto ipsec transform-set site_ab esp-aes-256 esp-sha-hmac mode tunnel
!c
rypto ipsec profile site_a
set security-association lifetime seconds 600 set transform-set site_ab
!c
rypto gdoi group group_a identity number 100 server local
rekey algorithm aes 256 rekey lifetime seconds 300 rekey retransmit 10 number 3
rekey authentication mypubkey rsa cciekey rekey transport unicast
sa ipsec 1 profile site_a
match address ipv4 site_a replay counter window-size 64 no tag
address ipv4 10.1.20.3
!i
nterface GigabitEthernet3
ip address 10.1.20.3 255.255.255.0
!i
p access-list extended site_a
permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
R3 is the Key Server in GETVPN VRF-Aware implementation. The Group Members for the site_a register with Key Server via interface address 10.1.20.3/24 in the management VRF “mgmt.”.

The Group ID for the siste_a is 100 to retrieve group policy and keys from the key server.
The traffic to be encrypted by the site_a Group Members is between 1921.68.4.0/24 and 192.168.5.0/24. Preshared-key used by the Group Members to authenticate with Key Server is “cissco”. It has been reported that Group Members are unable to perform encryption for the traffic defined in the group policy of site_a. What could be the issue?

A. Incorrect encryption traffic defined in the group policy
B. Incorrect mode configuration in the transform set
C. Incorrect password in the keyring configuration
D. Incorrect security-association time in the IPsec profile
E. Incorrect encryption in ISAKMP policy
F. The GDOI group has incorrect local server address
G. The registration interface is not part of management VRF “mgmt.”

Answer: G

NEW QUESTION 316
Refer to the exhibit.
R1
ntp authentication-key 12 md5 cisco ntp authenticate
ntp trusted-key 12
ntp source GigabitEthernet ntp master 1
!i
nterface GigabitEthernet1
ip address 171.1.7.21 255.255.255.0 R2
ntp authentication-key 12 md5 cisco ntp authentication-key 102 md5 cisco ntp authenticate
ntp trusted-key 12
ntp trusted-key 102
ntp server 171.1.7.21 key 102
R2# ping 172.1.7.21
Type escape sequence to abort
Sending 5 100-byte ICMP Echos to 171.1.7.21, timeout is 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/5 ms R2# sh ntp asso detail
171.1.7.21 configured ipv4, authenticated instance invalid, unsynced, stratum 6 ref ID INIT, time 00000000 0000000 (17:00:00.000 ccie Wed Dec 31, 2017)
R2 is getting time synchronized from NTP server R1. It has been reported that clock on R2 Is not able to associate with the NTP server R1. What could be the possible cause?

A. R2 has incorrect NTP server address
B. R1 has incorrect NTP source interface defined
C. R2 has incorrect trusted key binded with the NTP server
D. R2 does not support NTP authentication
E. R2 should not have two trusted keys for the NTP authentication
F. R2 has connectivity issue with the NTP server

Answer: C

NEW QUESTION 319
In which three configurations can SSL VPN be implemented? (Choose three)

A. CHAP
B. WebVPN
C. thin-client .
D. L2TP over IPsec
E. PVC tunnel mode
F. interactive mode
G. Cisco AnyConnect tunnel mode
H. clientless

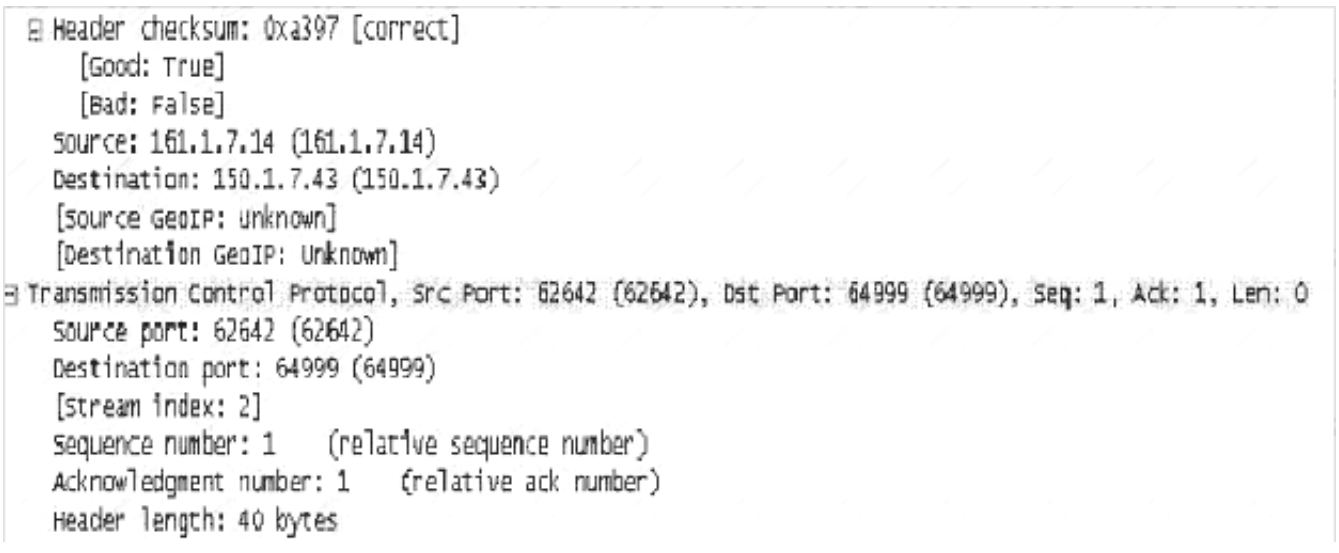
Answer: CGH

NEW QUESTION 324
Nexus 9000 Platform supports which of the following configuration management tools?

A. Ansible
B. Chef
C. Jenkins
D. Pupet
E. Salt

Answer: D

NEW QUESTION 326
Transmission control protocol, src port: 649999(64999), Dst Port:49086(49086),Seq:2,Ack:2,Len: Refer to the exhibit.



Refer to the exhibit. The ASA at 150.1.7.43 is configured to receive the IP address to SGT mapping from ISE at 161.1.7.14. Which statement about this packet capture from Wireshark is true?

A. The TACACS connection keep alive using UDP originated from ASA
B. The SXP message uses TCP port 64999 for connection termination
C. The RADIUS connection keep alive using TCP originated from ISE
D. The SXP message uses MD5 for authentication and integrity check.
E. The ISE keep alive message for NDAC connection using TCP originated from ASA
F. The NTP keep alive message using UDP originated from ISE
G. The SXP keep alive message for SXP connection using UDP originated from ASA

Answer: D

NEW QUESTION 330
Refer to the exhibit.
aaa authentication login default group radius aaa authentication login NO_AUTH none aaa authentication login vty local
aaa authentication dot1x default group radius aaa authorization network default group radius aaa accounting update newinfo
aaa accounting dot1x default start-stop group radius
!i
p dhcp excluded-address 60.1.1.11 ip dhcp excluded-address 60.1.1.2
!i
p dhcp pool mabpc-pool network 60.1.1.0 255.255.255.0
default-router 60.1.1.2
!c
ts sxp enable
cts sxp default source-ip 10.9.31.22 cts sxp default password ccie
cts sxp connection peer 10.9.31.1 password default mode peer listener hold-time 0!d
ot1x system-auth-control
!i
nterface GigabitEthernet1/0/9 switchport mode access
ip device tracking maximum 10 authentication host-mode multi-auth authentication port-control auto mab
!r
adius-server host 161.1.7.14 key cisco radius-server timeout 60
!
interface VLAN10
ip address 10.9.31.22 255.255.255.0
!i
nterface Vlan50 no ip address
!i
nterface Vlan60
ip address 60.1.1.2 255.255.255.0
!i
nterface Vlan150
ip address 150.1.7.2.255.255.255.0
Looking at the configuration what may cause the MAB authentication to fail for a supplicant?

A. There is an issue with the DHCP pool configuration
B. The VLAN configuration is missing on the authentication port
C. Incorrect CTS configuration on the switch
D. AAA authorization is incorrectly configured on the switch
E. CoA configuration is missing
F. Dot1x should be globally disabled for MAB to work
G. Switch configuration is properly configured and the issue is on the RADIUS server

Answer: E

NEW QUESTION 331
Which statement about ASA clustering requirements is true?

A. Only routed mode is allowed in the single context mode
B. Units in the cluster can be running different software version as long as they have identical hardware configuration
C. Units in the cluster can have different hardware configuration as long as they are running same software version
D. Units in the cluster can be in different geographical locations
E. Units in the cluster can be in different security context modes
F. Units in the cluster cannot have different software version even though they have identical hardware configuration.

Answer: F

NEW QUESTION 333
Which statement describes a pure SDN framework environment?

A. The control plane and data plane is pulled from the networking element and put in a SDN controller and SDN agent
B. The control plane function is split between a SDN controller and the networking element
C. The data plane is pulled from the networking element and put in a SDN controller
D. The data plane is controlled by a centralized SDN element
E. The control plane is pulled from the networking element and put in a SDN controller

Answer: E

NEW QUESTION 334
You have an ISE deployment with 2 nodes that are configured as PAN and MnT (Primary and Secondary), and 4 Policy Services Nodes. How many additional PSNs can you add to this deployment?

A. 3
B. 5
C. 1
D. 4
E. 2

Answer: D

NEW QUESTION 335
Which statement is true regarding securing connection using MACsec?

A. It secures connection between two supplicant clients
B. Switch uses session keys to calculate decrypted packet ICV value for the frame integrity check
C. Switch configured for MACSec can only accept MACSec frames from the MACSec client
D. It is implemented after a successful MAB authentication of supplicant
E. It provides network layer encryption on a wireless network
F. ISAKMP protocol is used to manage MACSec encryption keys

Answer: B

NEW QUESTION 337
In FMC, which two elements can the correlation rule be based on? (Choose two.)

A. authorization rule
B. Security Group Tag mapping
C. discovery event
D. user activity
E. database type
F. authentication condition
G. Change of Authorization
H. Network Device Admission Control

Answer: CD

NEW QUESTION 339
Which of the following Cisco products gives ability to interact with malware for its behavior analysis?

A. NGIPS
B. FMC
C. ASA
D. DNA
E. Threat Grid
F. pxGrid

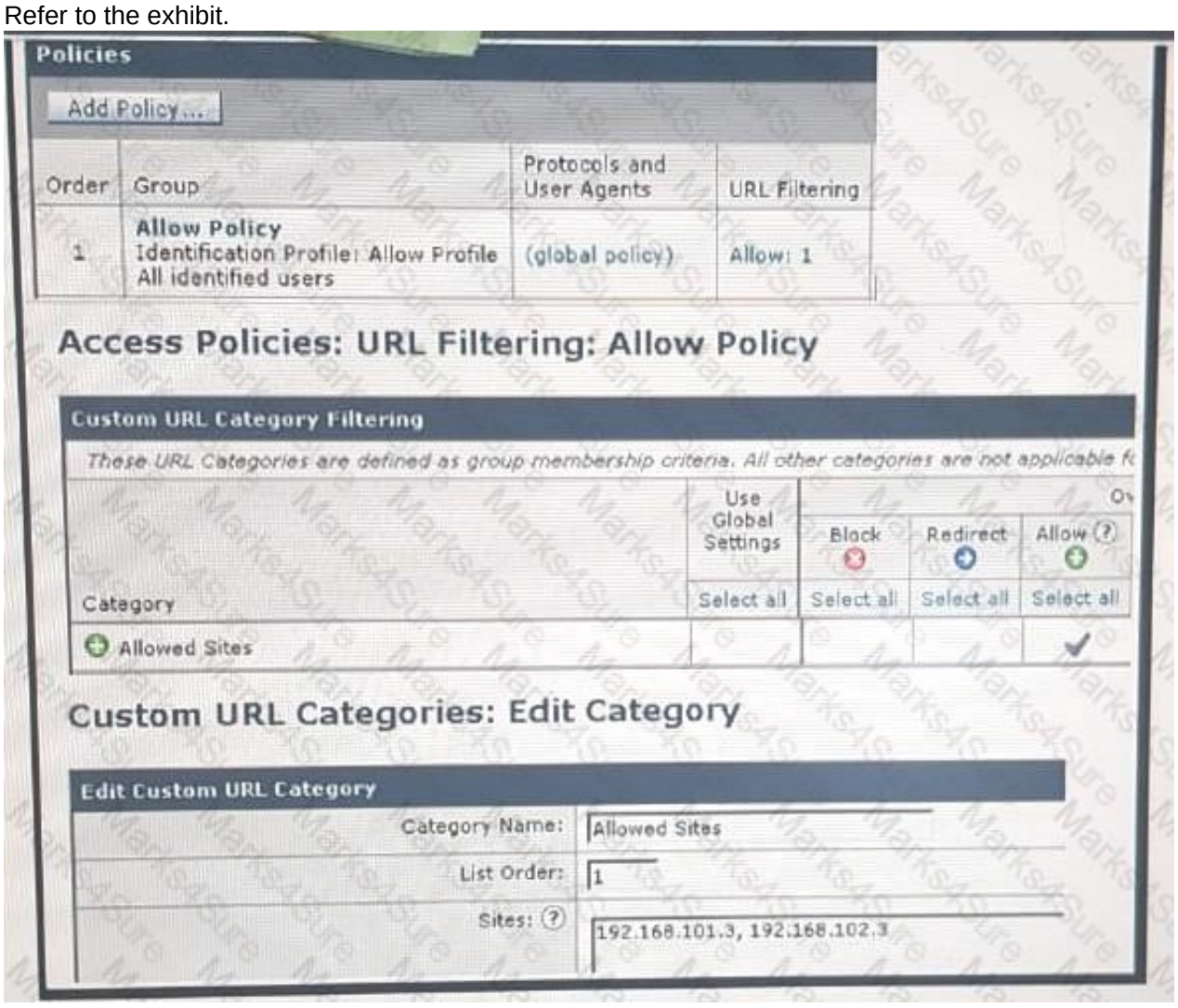
Answer: E

NEW QUESTION 344
For which of the four portals is the SAML Single Sign-On on ISE supported? (Choose four)

A. Wireless Client portal
B. Certificate Provisioning portal
C. Guest portal (sponsored and self-registered)
D. My Devices portal
E. Employee portal
F. Sponsor portal
G. Contractor portal
H. BYOD portal

Answer: BCDF

NEW QUESTION 347
Refer to the exhibit.



Users cannot access web servers 192.168.101.3/24 and 192.168 102.3/24 using Firefox web browser when 172.6V1.0/24 network. Which possible cause is true?

A. The identification profile "Allowed Profile" has a misconfigured user agent.
B. The access policy "Allow policy" is pointing to an incorrect identification profile.
C. The access policy "Allow Policy" has an incorrect action set for the custom URL category.
D. The custom URL category "Allowed Sites" has an incorrect server address listed.
E. The identification profile "Allow Profile" has an incorrect protocol.
F. The identification profile "Allow Profile" has an incorrect source network.

Answer: AF

NEW QUESTION 349
An employee using an Android phone on your network has disabled DHCP, enabled it's firewall, modified it's HTTP User-Agent header, to tool ISE into profiling it as a Windows 10 machine connected to the wireless network. This user is now able to get authorization for unrestricted network access using his Active Directory credentials, as your policy states that a Windows device using AD credentials should be able to get full network access. Whereas, an Android device should only get access to the Web proxy. Which two steps can you take to avoid this sort of rogue behavior? (Choose two.)

A. Create an authentication rule that should only allow session with a specific HTTP User-Agent header
B. Modify the authorization policy to only allow windows machines that have passed Machine Authentication to get full network access
C. Add an authorization policy before the Windows authorization policy that redirects a user with a static IPto a web portal for authentication
D. Chain an authorization policy to the Windows authorization policy that performs additional NMAP scansto verify the machine type, before allowing access
E. Only allow certificate-based authentication from Windows endpoints, such as EAP-TLS, or PEAP-TL
F. Should the endpoint use MSCHAPv2 (EAP or PEAP) the user shoujld be only given restricted access.
G. Perform CoA to push a restricted access when the machine is acquiring address using DHCP

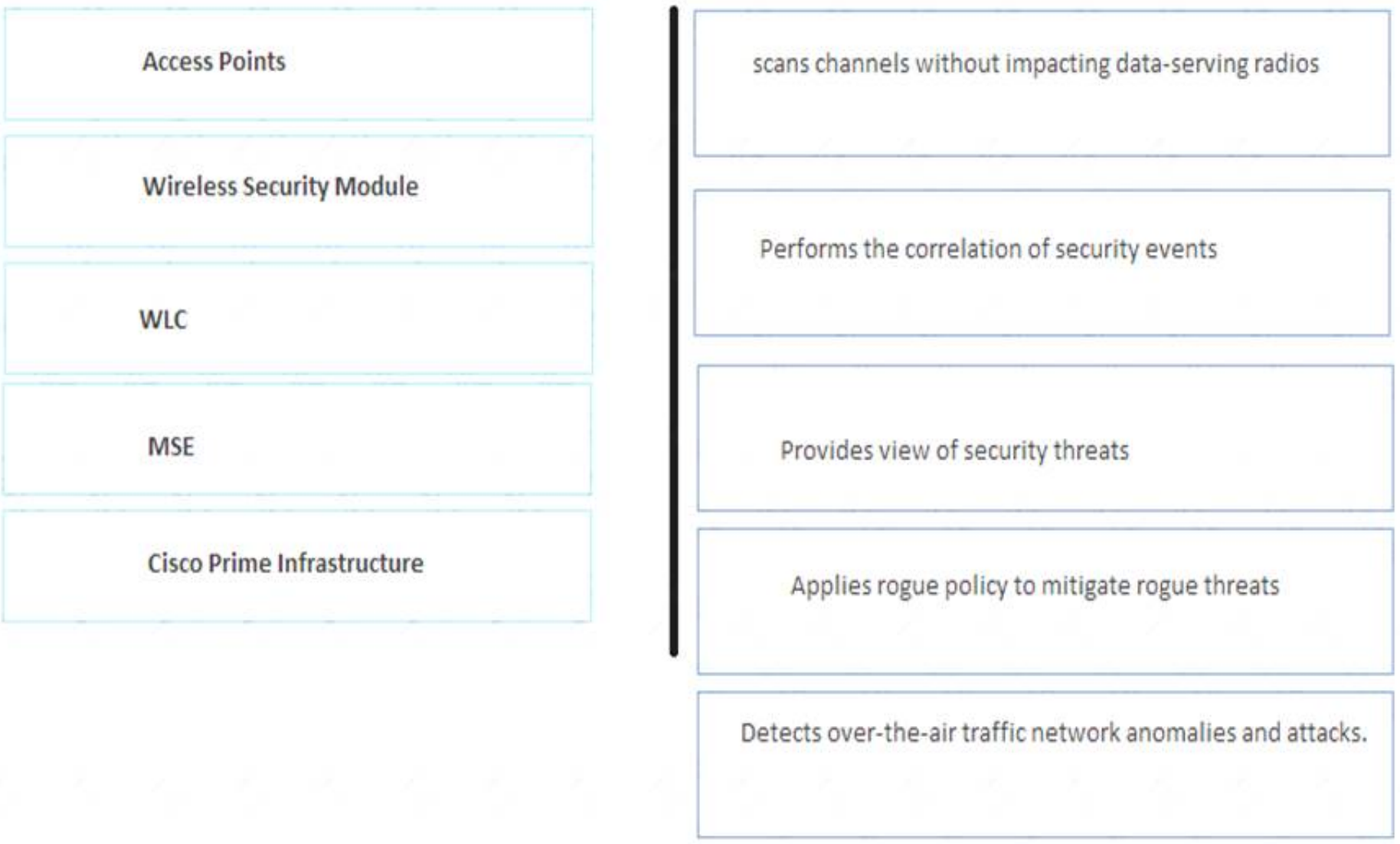
Answer: BC

NEW QUESTION 352
Which statement is true about a SMURF attack?

A. The attacker uses spoofed destination address to launch the attack
B. It sends ICMP Echo Requests to a broadcast address of a subnet
C. In order to mitigate the attack you need to enable IP directed broadcast on the router interface
D. It sends ICMP Echo Replies to known IP addresses in a subnet
E. It is used by the attackers to check if destination addresses are alive
F. It exhausts the victim machine resources with large number of ICMP Echo Requests from a subnet

Answer: B

NEW QUESTION 355
Drag the components of WIPS architecture on the left to their respective functionalities on the right.



Answer:

Explanation: 1-5, 2-1, 3-4, 4-2, 5-3

NEW QUESTION 357
Refer to the exhibit.
R9
crypto ikev2 keyring ccier10 peer r10
address 20.1.4.11
pre-shared-key local ccier10 pre-shared-key remote ccier10
!c
rypto ikev2 profile ccier10
match identity remote address 20.1.4.10 255.255.255.255 authentication local pre-share
authentication remote pre-share keyring local ccier10
!c
rypto ipsec profile ccier10 set ikev2-profile ccier10
!i
nterface Loopback1
ip address 192.168.9.9 255.255.255.0
!i
nterface Tunnel34
ip address 172.16.2.9 255.255.255.0
tunnel source GigabitEthernet1 tunnel destination 20.1.4.10
tunnel protection ipsec profile ccier10
!i
nterface GigabitEthernet1
ip address 20.1.3.9 255.255.255.0 negotiation auto
!r
outer eigrp 34
network 172.16.2.0 0.0.0.255
network 192.168.9.0
!r
outer bgp 3
bgp log-neighbor-changes
network 20.1.3.0 mask 255.255.255.0
neighbour 20.1.3.12 remote-as 345 netighbor 20.1.3.12 password cisco
R9 is running FLEXVPN with peer R10 at 20.1.4.10 using a pre-shared key "ccier10".
The IPSec tunnel is sourced from 172.16.2.0/24 network and is included in EIGRP routing process.
BGP nexthop is AS345 with address 20.1.3.12. It has been reported that FLEXVPN is down. What could be the issue?

A. Incorrect IPSec profile configuration
B. Incorrect tunnel network address in EIGRP routing process
C. Incorrect tunnel source for the tunnel interface
D. Incorrect keyring configuration
E. Incorrect IKEv2 profile configuration
F. Incorrect local network address in BGP routing process

Answer: D

NEW QUESTION 360
Which of the following four traffic flows should be allowed during an unknow posture state? (Choose four)

A. Traffic from AnyConnect client, with posture module, to ASA
B. Traffic to FireAMP cloud for AMP for endpoint scan results
C. Traffic to public search engines
D. Traffic to remediation servers, if needed
E. DHCP traffic
F. DNS traffic
G. SSH traffic for network device administration
H. Traffic to ISE PSNs to which Client Provisioning Protocol FQDN points

Answer: DEFH

NEW QUESTION 365
Which statement is correct regarding the SenderBase functionality?

A. ESA sees a high negative score from SenderBase as very unlikely that sender is sending spam.
B. SenderBase uses DNS/based blacklist as one of the sources of information to define reputation score of sender's IP address.
C. WSA uses SenderBase information to confiugre URL filtering policies.
D. ESA uses destination address reputation information from SenderBase to configure mail policies.
E. SenderBase uses spam complaints as one of the sources of information of defined reputation score of receiver IP address.
F. ESA sees a high positive score from SenderBase as very likely that sender is sending spam.

Answer: B

NEW QUESTION 368
What are the three configurations in which SSL VPN can be implemented? (Choose three.)

A. WebVPN
B. PVC TunnelMode
C. Interactivemode
D. L2TP overIPSec
E. Thin-Client
F. AnyConnect TunnelMode
G. Clientless
H. CHAP

Answer: EFG

NEW QUESTION 373
For your enterprise ISE deployment, you want to use certificate-based authentication for all your Windows machines. You have already pushed the machine and user certificates out to all the machines using GPO. by default, certificate-based authentication-does not check the certificate against Active Directory, or requires credentials from the user. This essentially means that no groups are returned as part of the authentication request. In which way can the user be authorized based on Active Directory group membership?

A. Configure the Windows supplicant to used saved credentials as well as certificate-based authentication
B. Enable Change of Authorization on the deployment to perform double authentication
C. Use ISE as the Certificate Authority, which will then allow for automatic group retrieval from Active Directory to perform the required authorization
D. The certificate must be configured with the appropriate attributes that contain appropriate group information, which can be used in Authorization policies
E. Configure Network Access Device to bypass certificate-based authentication and push configured user credentials as a proxy to ISE
F. Use EAP authorization to retrieve group information from Active Directory

Answer: C

NEW QUESTION 375
Which statement about the Traffic Substitution and Insertion attack is true?

A. It substitutes by performing action slower than normal not exceeding threshol
B. It is used for reconnaissance
C. It substitutes payload data in a different format but has the same meaning
D. It is form of a DoS attack
E. It substitutes payload data in the same format but has different meaning
F. It substitutes by performing action faster than normal not exceeding threshold
G. It is a from pivoting in the network

Answer: C

NEW QUESTION 377
Refer to the exhibit.
Exhibit Missing
Users are unable to access web server 192.168.101.3/24 and 1921.68.102.3/24 using
Firefox web browser when initiated from 172.16.1.0/24 network. What could be the possible cause?

A. Identification profile “allow Profile” has incorrect source subnet
B. Access policy “allow policy” is pointing to incorrect identification profile
C. Identification profile “alow Profile” has incorrect protocol
D. Access policy “allow policy” has incorrect action set for the custom URL category
E. Custom URL category “allowed sites” has incorrect server addresses listed
F. Identification profile “allowed Profile” has misconfigured user agent

Answer: F

NEW QUESTION 378
Which statement about Nmap scanning on the Cisco Firepower System is true?

A. It can leverage multiple proxy devices to increase scan speed
B. It can scan TCP and UDP ports, but TCP ports require significantly more resources
C. The Fast Port Scan scans only the TCP ports that are lited in the nmap-service file
D. It can scan IP addresses, address blocks, and address ranges on IPv4 and IPv6 networks
E. It supports custom fingerprinting to identify malware by its unique characteristics in your specific environment
F. It performs host discovery before each scan to identify hosts that are online and skips the full scan for hosts that are offline

Answer: C

NEW QUESTION 381
In a large organization, with thousands of employees scattered across the globe, it is difficult to provision and onboard new employee device with the correct profiles and certificates. With ISE, it is possible to do that with client provided device. Which four conditions must be met? (Choose four.)

A. Endpoint operating system should be supported
B. Client provisioning is enabled on ISE
C. The pxGrid controller should be enabled on ISE
D. Device MAC addresses are added to the Endpoint Identity Group
E. Profiling is enabled on ISE
F. SCEP Proxy is enabled on ISE
G. Microsoft windows server is configured with certificate services
H. ISE should be configured as SXP listener to push SGT-to-IP mapping to network access devices
I. Network access device and ISE should have the PAC provisioning for CTS environment authentication

Answer: BDEF

NEW QUESTION 384
Which statement about the pxGrid connection agent is true?

A. It manages the sharing of contextual information between partner platforms
B. It can fetch user information from Active Directory on behalf of a WSA or Cisco ISE
C. It enables communication from the partner platform to the pxGrid controller
D. It supports an agentless solution for Cisco ISE
E. It leverages Cisco ISE control functions to manage connections and share information between partners
F. It fetches user information from Active Directory and transmits it to the pxGrid controller

Answer: A

NEW QUESTION 386
Refer to the exhibit. ASA# sh nat detail
Auto NAT Policies (Section 1)
1 (inside) to (outside) source static servers server1_t translate_hits = 0 untranslate_hits = 5
Source = Origin 192.168.1.3/32. Translated 19.16.1.3/32 2 (inside) to (outside) source static servers server2_t translate_hits = 0 untranslate_hits = 24
Source = Origin 192.168.2.3/32. Translated 19.16.2.3/32 ASA# sh access-list
access-list trustsec line 1 extended permit tcp security-group name employee (tag=16) any security-group name engineering_int(tag=20) any eq 8080 (hitcnt=1)
access-list trustsec line 2 extended permit tcp security-group name guest
(tag=17) any security-group name intranet_int(tag=10) any eq 8080 (hitcnt=1) ASA# sh cts exp sge-map
SGT 17
IPv4 60.1.1.1
PeerIP 161.1.7.14
InsNum 1 Status Active SGT 18
IPv4 19.16.1.1
PeerIP 161.1.7.14
InsNum 1 Status Active SGT 20
IPv4 192.168.1.3
PeerIP 161.1.7.14
InsNum 1 Status Active SGT 19
IPv4 19.16.2.3
PeerIP 161.1.7.14
InsNum 1 Status Active SGT 15
IPv4 192.168.2.3
PeerIP 161.1.7.14

InsNum 1 Status Active SGT 16
IPv4 50.1.3.4
PeerIP 161.1.7.14
InsNum 1 Status Active
Destination address with name "engineering_int" is visible to the outside as which of the following addresses?

A. 19.16.1.3
B. 192.168.1.3
C. 50.1.1.1
D. 161.1.7.14
E. 60.1.1.1
F. 19.16.2.3
G. 192.168.2.3

Answer: A

NEW QUESTION 391
A device on your internal network is hard-coded with two DNS servers on the Internet (1.1.1.53, 2.2.2.53). However, you want to send all requests to your OpenDNS server (208.67.222.222). Which set of commands do you run on the ASA to achieve this goal?

A. static (inside,outside) source any 1.1.1.53 destination 208.61.222.222 eqdomain static (inside,outside) source any 2.2.2.53 destination 208.67.222.222 eq domain
B. static (inside,outside) source any 208.67.222.222 destination 1.1.1.53 eqdomain static (inside,outside) source any 208.67.222.222 destination 2.2.2.53 eq domain
C. static (inside,outside) source any destination 208.61.222.222 eq domain
D. static (outside,inside) source any 208.67.222.222 destination 1.1.1.53 eqdomain static (outside,inside) source any 208.67.222.222 destination 2.2.2.53 eq domain
E. net (inside,outside) source any 1.1.1.53 destination 208.61.222.222 eq domainnet (inside,outside) source any 2.2.2.53 destination 208.67.222.222 eq domain
F. object network OpenDNS host 208.67.222.222!object network Rogue1-DNS host 1.1.1.53object network Rogue2-DNS host 2.2.2.53!object-group network Rogue-DNS network-object object Rogue1-DNS network-object object Rogue2-DNS!object service udp-DNSservice udp destination eq domain!object service tcp-DNSservice tcp destination eq domain!nat (inside,outside) source static any interface destination static Rogue-DNS OpenDNS service udp-DNS udp-DNSnat (inside,outside) source static any interface destination static Rogue- DNS OpenDNS service tcp-DNS tcp-DNS
G. nat (inside,outside) source static any interface destination static Rogue-DNS OpenDNS service udp-DNS udp-DNSnat (inside,outside) source static any interface destination static Rogue- DNS OpenDNS service tcp-DNS tcp-DNS
H. object network OpenDNS host 208.67.222.222!object network Rogue1-DNS host 1.1.1.53object network Rogue2-DNS host 2.2.2.53!object-group network Rogue-DNS network-object object Rogue1-DNS network-object object Rogue2-DNS!object service udp-DNSservice udp destination eq domain!object service tcp-DNSservice tcp destination eq domain!nat (inside,outside) source static any interface destination static OpenDNS Rogue-DNS service udp-DNS udp-DNSnat (inside,outside) source static any interface destination static OpenDNS Rogue-DNS service tcp-DNS tcp-DNS

Answer: F

NEW QUESTION 396
What would describe Cisco Virtual Topology System?

A. Package that contains an entire runtime environment
B. An agent that resides on physical devices
C. Web server hosting for NX-OS
D. Overlay provisioning and management solution

Answer: D

NEW QUESTION 400
In an effort to secure your enterprise campus network, any endpoint that connects to the network should authenticate before being granted access. For all corporate-owned endpoints, such as laptops, mobile phones and tablets, you would like to enable 802.1x and once authenticated allow full access to the network. For all employee owned personal devices, you would like to use web authentication, and only allow limited access to the network. Which two authentication methods can ensure that an employee on a personal device can't use his or her Active Directory credentials to log on to the network by simply re configuring their supplicant to use 802.1x and getting unfettered access? (Choose two.)

A. Use PEAP-EAP-MSCHAPv2
B. Use EAP-FAST
C. Use EAP-TLS or EAP-TTLS
D. Use EAP-MSCHAPv2
E. Use PAP-CHAP-MSCHAP
F. Use PEAP-EAP-TLS

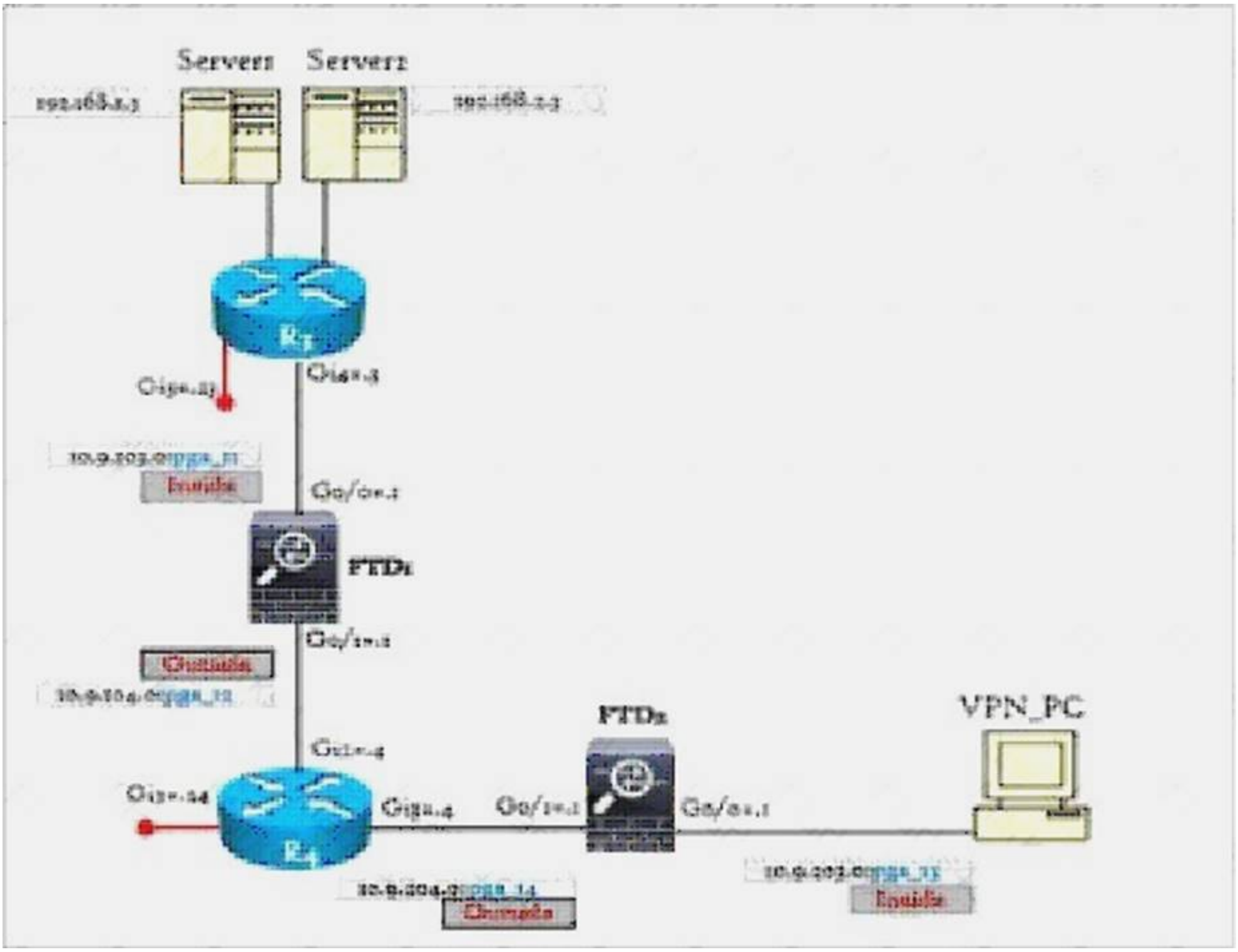
Answer: AB

NEW QUESTION 402
Which statement correctly describes 3DES encryption algorithm?

A. It uses a set of three keys for encryption and a different set of three keys for decryption.
B. It is a block Cipher algorithm but weaker than DES due to smaller key size.
C. It is an asymmetric algorithm with a key size of 168 bits.
D. It does decryption in reverse order with the same set of keys used during encryption.
E. It is a block cipher algorithm with a key size of 56 bits.
F. It is a stream cipher algorithm with a key size of 168 bits.

Answer: D

NEW QUESTION 406
Refer to the exhibit.



There is no ICMP connectivity from VPN PC to Server 1 and Server2. What could be the possible cause?

A. The destination port configuration missing in the access rule
B. The server network has incorrect mask in the access rule
C. The VLAN tags configuration missing in the access rule
D. The action is incorrect in the access rule
E. The source network is incorrect in the access rule
F. The zone configuration missing in the access rule

Answer: E

NEW QUESTION 410
Which statement about EAP chaining is true?

A. It supports RADIUS and TACACS+ authentication
B. It performs authentication on a device-only basis
C. It locks a unique certificate to BYOD devices to differentiate them from corporate-owned devices
D. It requires EAP-FAST authentication
E. By default devices on which EAP chaining is not supported are immediately denied access to the network
F. It can be deployed in an agentless environment

Answer: D

NEW QUESTION 414
Various methods are available for load-balancing across WSA deployment. Which method requires the least effort for all types of endpoints (campus and data center) across the enterprise?

A. Push out proxy settings to endpoints through Windows GPO settings
B. Host a PAC file on the WSA or an intranet web server and point all endpoints to it for auto-configuration
C. Configure an SRV DNS record to point to the WSA for all WAN services
D. Use transparent Layer 4 redirection with multiple WSAs behind a load-balancer
E. Use WPAD that uses the IP addresses of the WSAs

Answer: D

NEW QUESTION 418
An organization plans to upgrade its Internet-facing ASA running version 8.2 on an older HW platform to 5585/X version 9.6. The configuration was backed up and submitted for review before the migration takes
place. Which three changes must be made before the configuration is applied to the new ASA firewall?
(Choose three.)

A. Static NAT statements are changed to xlate statements
B. NAT control must be disabled so that traffic is allowed through the ASA
C. Inbound ACLs must contain the pre-NAT IP instead the post-NAT IP
D. NAT Control must be enabled so that traffic is allowed through the ASA
E. Static NAT statements are changed to NAT statements
F. Inbound ACLs must contain the post-NAT IP instead of the pre-NAT IP

Answer: ACD

NEW QUESTION 421
Which three statements about EAP-Chaining are true? (Choose three.)

A. lt allows user and machine authentication with one RADIUS / EAP session.
B. It is supported on the Windows 802.1x supplicant.
C. It is enabled on NAM automatically when EAP-TLS user and machine authentication is enabled.
D. lt is enabled on Cisco AnyConnect NAM automatically when EAP-FAST user and machine authentication is enabled.
E. lt can use only EAP-FAST, and it requires the use of Cisco AnyConnect NAM.
F. EAP-FAST does not allow multiple authentication binding, and this limitation is used for mutual authentication in EAP-Chaining.
G. The EAP-FAST PAC provisioning phase is responsible to establish SSH tunnel between supplicant and ISE to perform EAP-Chaining.

Answer: ADE

NEW QUESTION 423
An sneaky employee using an Android phone on your network has disabled DHCP, enabled it's firewall, modified it's HTTP User-Agent header, to fool ISE into profiling it as a Windows 10 machine connected to the wireless network. This user can now get authorization for unrestricted network access using his Active Directory credentials, because your policy states that a Windows device using AD credentials should be able to get full network access. However, an Android device should only get access to the Web Proxy. Which two steps can you take to avoid this sort of rogue behavior? (Choose two.)

A. Add an authorization policy before the Windows authorization policy that redirects a user with a static IP to a web portal for authentication
B. Perform CoA to push a restricted access when the machine is acquiring address using DHCP.
C. Chain an authorization policy to the Windows authorization policy that performs additional NMAP scans to verify the machine type before access is allowed
D. Create an authentication rule that allows only a session with a specific HTTP User-Agent header
E. Allow only certificate based authentication from Windows endpoints such as EAP-TLS or PEAP-TLS.If the endpoint uses MSCHAPv2 (EAP or PEAP), the useris given only restricted access
F. Modify the authorization policy to allow only Windows machines that have passed Machine Authentication to get full network access

Answer: EF

NEW QUESTION 425
Which statement is true regarding the wireless security technologies?

A. WPA provides message integrity using AES
B. WPA2-PSK mode allows passphrase to store locally on the device
C. WEP is more secure than WPA2 because it uses AES for encryption
D. WPA-ENT mode does not require RADIUS for authentication
E. WPÁ2-PSK mode provides better security by having same passphrase across the network
F. WPA2 is more secure than WPA because it uses TKIP for encryption

Answer: A

NEW QUESTION 426
Your organization is deploying an ESA for email security for inbound and outbound email. To receive inbound emails from external organizations, you must set up your DNS servers with the appropriate records so that the sending email server can determine which email gateway to send to. Assume that you have two ESAs deployed and the hostnames and IP addresses are as follows:
esa1.myesa.com: 5.5.5.25 (Preferred)
esa2.myesa.com: 5.5.5.26
Which two options must you include in your DNS server to receive email from all external senders? (Choose two.)

A. Forward Lookup Zone:@ 3600 IN A 10 esa1.myesa.com@ 3600 IN A 20 esa2.myesa.com
B. Forward Lookup Zone: esa1 IN 3600 A 5.5.5.25esa2 IN 3600 A 5.5.5.26
C. Forward Lookup Zone:mail1.myesa.com 120 CNAME esa1.myesa.com mail2.myesa.com 120 CNAME esa2.myesa.com
D. Forward Lookup Zone:@ 3600 IN MX 10 mail1.myesa.com@ 3600 IN MX 20 mail1.myesa.com
E. Reverse Lookup Zone for 5.5.5.: 25 3600 IN PTR esa1.myesa.com26 3600 IN PTR esa2.myesa.com

Answer: CE

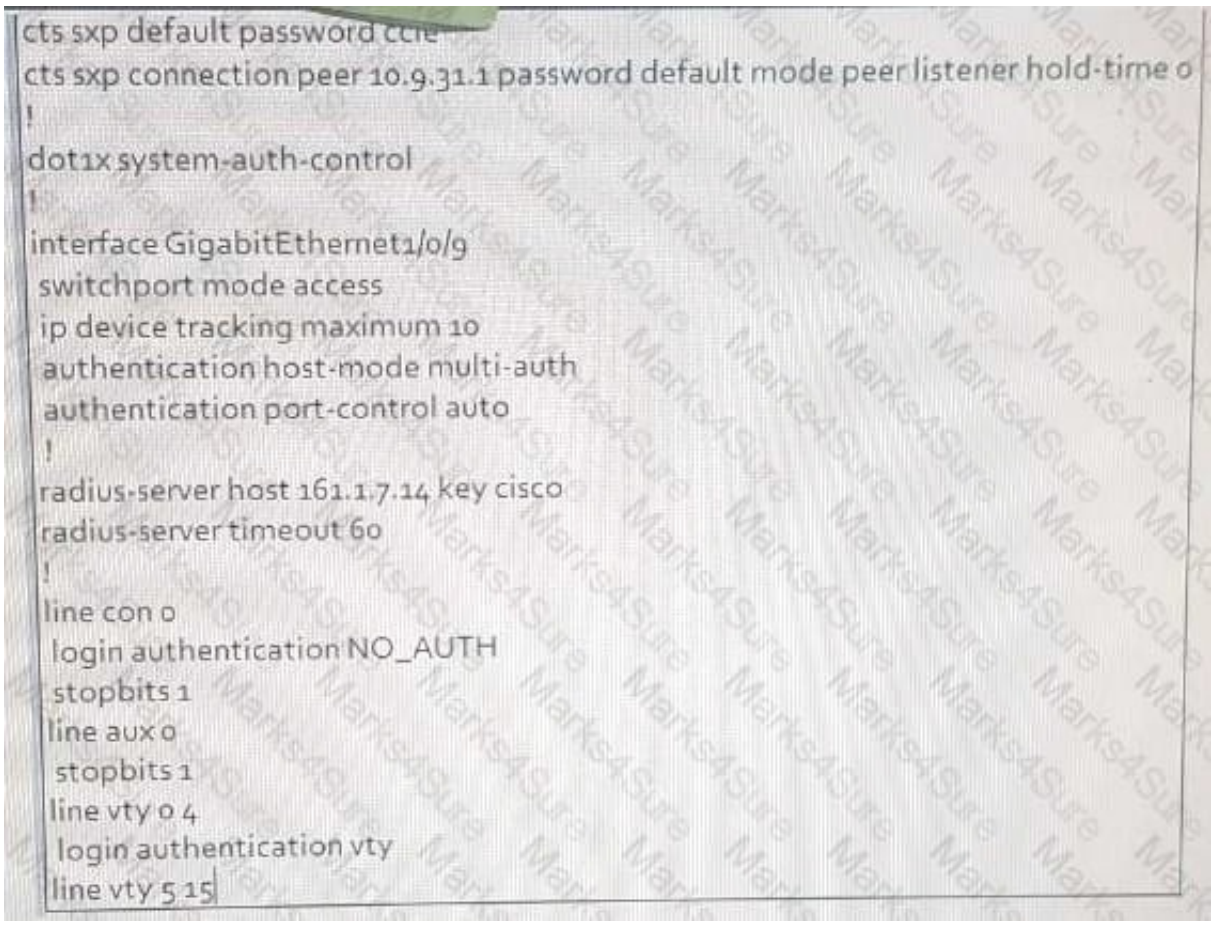
NEW QUESTION 427
You have an ISE deployment with two nodes that re configured as PAN and MnT (Primary and Secondary), and four Policy Service Nodes. How many additional PSNs can you add to this deployment?

A. 1
B. 3

C. 5
D. 4
E. 2

Answer: B

NEW QUESTION 430
Refer to the exhibit.



A customer reports to Cisco TAC that one of the Windows clients that is supposed to log in to the network using MAB can no longer access any allowed resources. Which possible cause of the MAB failure is true?

A. MAB is disabled on port Gi1/0/9.
B. AAA authorization is incorrectly configured on the switch.
C. CTS is configured incorrectly on the switch.

Answer: A

NEW QUESTION 431
A network architect has been tasked to migrate a customer's legacy infrastructure switches from Nexus 9000 platform. Which peers will help him achieve his milestone?

A. Create a container providing separate execution space
B. Manage software upgrades via guest shell
C. Setup a Web-based interface for configuration management.
D. Allow guests temporary access to the CLI without logging in.

Answer: A

NEW QUESTION 433
Which statement description of the Strobe scan is true?

A. It never opens a full TCP connection.
B. It relies on ICMP "port unreachable" message to determine if the port is open.
C. It is used to find the ports that already have an existing vulnerability to exploit.
D. It checks the firewall deployment in the path.
E. It is a directed scan to a known TCP/UDP port.
F. It evades network auditing tools.

Answer: C

NEW QUESTION 435
Which of the following is one of the requirements for the FTD high availability setup?

A. Units should not have any uncommitted changes of FMC and should be fully deployed
B. Units should have DHCP configured for the interfaces
C. Units should be configured in transparent mode
D. Units should not synchronize using the same NTP source
E. Units should be configured in routed mode
F. Units should be in different domains in FMC
G. Units should have the same major software version running on them, minor and maintenance version could be different

Answer: A

NEW QUESTION 439
Which statement is true regarding Private VLAN?

A. A private VLAN domain can have multiple primary VLANs
B. Each secondary VLAN in a private VLAN domain needs to have a separate associated primary VLAN
C. Each port in a private VLAN domain is a member of all the secondary VLANs in the domain
D. A subdomain in a primary VLAN domain consists of a primary and secondary VLAN pair
E. In a private VLAN domain a secondary VLAN port needs to be an isolated port for it to be able to communicate with a layer-3 device
F. In a private VLAN domain a secondary VLAN can have only one promiscuous port

Answer: F

NEW QUESTION 440
The purpose of an authentication proxy is to force the user to authenticate to a network device before users are allowed access through the device. This is primarily used for HTTP based services, but also can be used for other services. In the case of an ASA, what does ISE have to send to enforce this access policy?

A. LDAP attribute with ACL
B. Group Policy enabled for proxy-auth
C. Downloadable ACL
D. Not possible on the ASA
E. VLAN
F. Redirect URL to ISE

Answer: C

NEW QUESTION 445
Which description of a Dockers file is true?

A. repository for Docker images
B. software used to manage containers
C. message daemon files
D. text document used to build an image

Answer: D

NEW QUESTION 449
Which statement is true about Social Engineering attack?

A. It uses the reconnaissance method for exploitation.
B. It is a method of extracting a non-confidential information.
C. The "Phishing" technique is one of the ways to launch the attack.
D. It is always performed through an email from a person that you know.
E. It is always done by having malicious ads on untrusted websites for the users to browse.
F. It can be only done by a person who is not part of the organization.

Answer: A

NEW QUESTION 454
For your enterprise ISE deployment, you are looking to use certificate-based authentication for all your Windows machines. You have already gone through the exercise of pushing the machine and user certificates out to all the machines using GPO. Since certificate based authentication, by default, doesn't check the certificate against Active Directory or requires credentials from the user, this essentially means that no groups are returned as a part of the authentication request. What are the possible ways to authorize the user based on Active Directory group membership?

A. Configure the Windows supplicant to use saved credentials as well as certificate-based authentication
B. Enable Change of Authorization on the deployment to perform double authentication
C. Use EAP authorization to retrieve group information from Active Directory
D. The certificate should be configured with the appropriate attributes which contain appropriate group information, which can be used in Authorization policies
E. Use ISE as the Certificate Authority, which will then allow automatic group retrieval from Active Directoryto perform the required authorization
F. Configure Network Access Device (NAD) to bypass certificate-based authentication and push configured user credentials as a proxy to ISE

Answer: F

NEW QUESTION 459
Whic statement about Dynamic ARP inspection is true?

A. It is supported only in DHCP environments to detect invalid ARP requests and response
B. It requires that DHCP snooping be enabled to build valid binding databas
C. It validates ARP requests and responses on untrusted ports using MAC address table
D. It validates ARP requests and responses on trusted ports using IP-to-MAC address binding
E. It forwards invalid ARP responses and requests on switch untrusted ports
F. It drops invalid ARP responses and requests on the switch trusted ports

Answer: B

NEW QUESTION 464
Which statement correctly describes AES encryption algorithm?

A. It works on substitution and permutation principle
B. It uses three encryption keys of length 168, 112 and 56 bits
C. Reapplying same encryption key three times makes it less vulnerable then 3DES
D. It only provides data integrity
E. Theoretically 3DES is more secure then AES

Answer: A

NEW QUESTION 467
Which of the following is a correct operational statement of DKIM signing in ESA?

A. The signing public key is required by the receiving server
B. The ESA does not allow to create signing key pair
C. The receiving server gets the signing public key from DNS
D. The domain profile in ESA is configured with signing public key
E. The outgoing profile in ESA is configured with signing private key
F. The signing private key is required by the sending server

Answer: C

NEW QUESTION 469
Which description of the AES encryption algorithm is true?

A. Reapplying the same encryption key three times makes it less vulnerable than 3DES
B. Theoretically 3DES is more secure than AES
C. It uses the block of 64 bits
D. It provides only data integrity
E. It does not use the substitution and permutation principle
F. It uses three encryption keys of lengths 128, 192, and 256

Answer: F

NEW QUESTION 470
Which statement about Local Web Authentication is true?

A. It supports Change of Authorization and VLAN enforcement
B. It can use VLANs and ACLs to enforce authorization
C. The network device handles guest authentication
D. The ISE servers web pages
E. It supports posture and profiling services
F. The web portal can be customized locally or managed by the ISE

Answer: C

NEW QUESTION 475
Which description of a Botnet attack is true?

A. It can be used to participate in DDoS.
B. It is form a wireless attack where the attacker installs an access point to create backdoor to a network.
C. It is launched by a collection of noncompromised machines controlled by the Command and Control system.
D. It is launched by a single machine controlled by the Command and Control system.
E. It is form of a fragmentation attack to evade an intrusion prevention security device.
F. It is a form of a man-in-the-middle attack where the compromised machine is controlled remotely.

Answer: AD

NEW QUESTION 477
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

400-251 Practice Exam Features:

* 400-251 Questions and Answers Updated Frequently

* 400-251 Practice Questions Verified by Expert Senior Certified Staff

* 400-251 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 400-251 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year