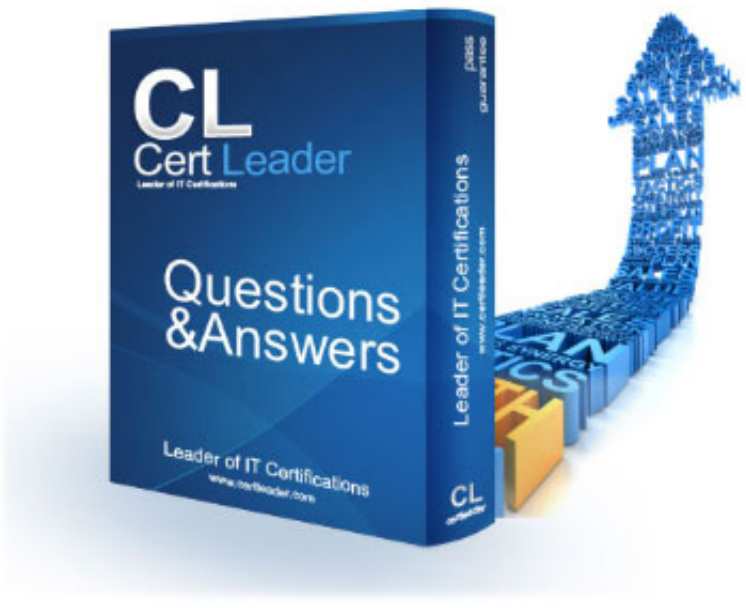
400-251 Dumps

CCIE Security Written Exam

https://www.certleader.com/400-251-dumps.html



NEW QUESTION 1
- (Exam Topic 1)
Which two statements about uRPF are true? (Choose two)

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

Answer: BC

Explanation:
Reverse Path Forwarding
http://www.cisco.com/c/en/us/about/security-center/unicast-reverse-path-forwarding.html

NEW QUESTION 2
- (Exam Topic 1)
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
- (Exam Topic 1)
Which three options are fields in a CoA Request Response code packet? (Choose three.)

A. Length
B. Acct-session-ID
C. Calling-station-ID
D. Identifier
E. Authenticator
F. State

Answer: BCF

NEW QUESTION 4
- (Exam Topic 1)
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 5
- (Exam Topic 1)
Which two options are unicast address types for IPv6 addressing? (Choose two.)

A. static
B. link-local
C. established
D. dynamic
E. global

Answer: BE

NEW QUESTION 6
- (Exam Topic 1)
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 7
- (Exam Topic 1)
Which effect of the crypto key encrypt write rsa command on a router is true?

A. The device locks the encrypted key, but the key is lost when the router is reloaded.
B. The device encrypts and locks the key before authenticating it with an external CA server.
C. The device unlocks the encrypted key, but the key is lost when the router is reloaded.
D. The device locks the encrypted key and saves it to the NVRAM.
E. The device saves the unlocked encrypted key to the NVRAM.

Answer: E

NEW QUESTION 8
- (Exam Topic 1)
Which three statements about Cisco AnyConnect SSL VPN with the ASA are true? (Choose three)

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

Answer: CDE

NEW QUESTION 9
- (Exam Topic 1)
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 10
- (Exam Topic 1)
What is an example of a stream cipher?

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

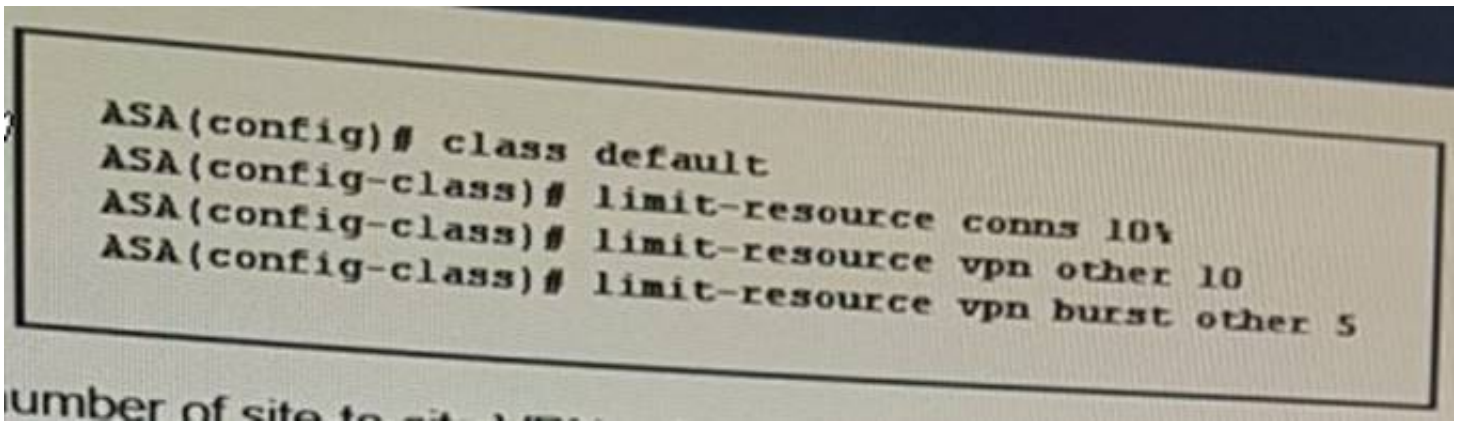
Answer: A

NEW QUESTION 10
- (Exam Topic 1)
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 13
- (Exam Topic 1)
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: F

NEW QUESTION 16
- (Exam Topic 1)
Which three statements about 802.1x multiauthentication mode are true? (Choose three.)

A. It is recommended for guest VLANs.
B. On non-802.1x devices, it can support only one authentication method on a single port.
C. Each multiauthentication port can support only one voice VLAN.
D. It is recommended for auth-fall VLANs.
E. It requires each connected client to authenticate individually.
F. It can be deployed in conjunction with MDA functionality on voice VLANs.

Answer: CEF

NEW QUESTION 21
- (Exam Topic 1)
Which three statements about WCCP are true? (Choose three.)

A. The minimum WCCP-Fast Timers messages interval is 500 ms
B. Is a specific capability is missing from the Capabilities Info component, the router is assumed to support the default capability
C. If the packet return method is missing from a packet return method advertisement, the web cache uses the Layer 2 rewrite method
D. The router must receive a valid receive ID before it negotiates capabilities
E. The assignment method supports GRE encapsulation for sending traffic
F. The web cache transmits its capabilities as soon as it receives a receive ID from router

Answer: ACE

Explanation:
Web Cache Communication Protocol (WCCP) http://www.cisco.com/c/en/us/td/docs/security/asa/special/wccp/guide/asa-wccp.html

NEW QUESTION 24
- (Exam Topic 1)
Which file extensions are supported on the Firesight Management Center 6.1 file policies that can be analyzed dynamically using the Threat Grid Sandbox integration?

A. MSEXEMSOLE2NEW-OFFICEPDF
B. DOCXWAVXLSTXT
C. TXTMSOLE2WAVPDF
D. DOCMSOLE2XMLPDF

Answer: A

NEW QUESTION 29
- (Exam Topic 1)
Which two statements about SPAN sessions are true? (Choose two.)

A. A single switch stack can support up to 32 source and RSPAN destination sessions.
B. Source ports and source VLANs can be mixed in the same session
C. They can monitor sent and received packets in the same session.
D. Multiple SPAN sessions can use the same destination port.
E. Local SPAN and RSPAN can be mixed in the same session.
F. They can be configured on ports in the disabled state before enabling the port.

Answer: CF

NEW QUESTION 33

- (Exam Topic 1)
Which four task items need to be performed for an effective nsk assessment and to envaluate network posture? (Choose four.)

A. discovery
B. baselining
C. scanning
D. notification
E. validation
F. escalation
G. mitigation
H. profiling

Answer: ACEH

NEW QUESTION 38
- (Exam Topic 1)
Which three statements about SCEP are true? (Choose three.)

A. It supports online certification revocation.
B. Cryptographically signed and encrypted messages are conveyed using PKCS#7
C. It supports multiple cryptographic algorithms including RSA.
D. The certificate request format uses PKCS#10.
E. CRL retrieval is supported through CDP(Certificate Distribution Point) queries.
F. It supports synchronous granting.

Answer: BDE

Explanation:
Simple Certificate Enrollment Protocol
http://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/116167-technotescep-00.html

NEW QUESTION 41
- (Exam Topic 1)
Which statement about deploying policies with the Firepower Management Center is true?

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

Answer: B

NEW QUESTION 42
- (Exam Topic 1)
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 43
- (Exam Topic 1)
Which two options are benefits of network summarization? (Choose two.)

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

Answer: AE

NEW QUESTION 47
- (Exam Topic 1)
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 51
- (Exam Topic 1)
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 55
- (Exam Topic 1)
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 60
- (Exam Topic 1)
Which two statements SCEP are true? (Choose two)

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

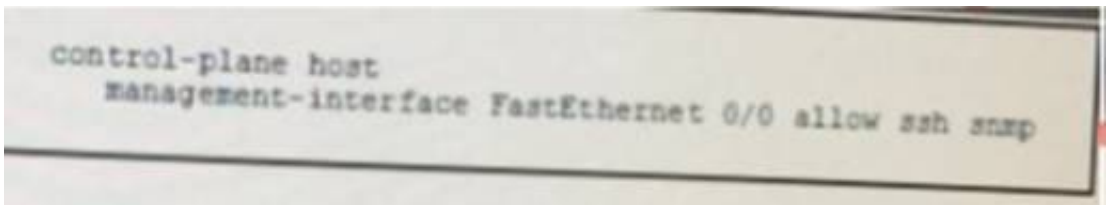
Answer: AC

NEW QUESTION 65
- (Exam Topic 1)
Which description of SaaS is true?

A. a service offering on-demand licensed applications for end users
B. a service offering that allowing developers to build their own applications
C. a service offering on-demand software downloads
D. a service offering a software environment in which applications can be build and deployed.

Answer: A

NEW QUESTION 69
- (Exam Topic 1)
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 74

- (Exam Topic 1)
Which two statements about a wireless access point configured with the guest-mode command are true? (Choose two.)

A. It can support more than one guest-mode SSID.
B. It supports associations by clients that perform passive scans.
C. It allows clients configured without SSIDs to associate.
D. It allows associated clients to transmit packets using its SSID.
E. If one device on a network is configure in guest-mode, clients can use the guest-mode SSID to connect to any device in the same network.

Answer: BC

NEW QUESTION 76
- (Exam Topic 1)
Which two statements about 6to4 tunneling are true? (Choose two.)

A. It provides a /128 address block.
B. It supports static and BGPV4 routing.
C. It provides a /48 address block.
D. It supports managed NAT along the path of the tunnel.
E. The prefix address of the tunnel is determined by the IPv6 configuration of the interface.
F. It supports multihoming.

Answer: BC

NEW QUESTION 78
- (Exam Topic 1)
Refer to the exhibit.

```
ASA(config)# dynamic-filter updater-client enable
ASA(config)# changeto context context1
ASA/context1(config)# dynamic-filter use-database
ASA/context1(config)# changeto context context2
ASA/context2(config)# dynamic-filter use-database
```

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

A. It enables the ASA to download the static botnet filter database.
B. It enables the ASA to download the dynamic botnet filter database.
C. It enables botnet filtering in single context mode.
D. It enables botnet filtering in mutiple context mode.
E. It enables multiple context mode.
F. It enables single context mode.

Answer: BD

NEW QUESTION 81
- (Exam Topic 1)
Which OpenStack project has orchestration capabilities?

A. Cinder
B. Horizon
C. Sahara
D. Heat

Answer: D

NEW QUESTION 84
- (Exam Topic 1)
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 88
- (Exam Topic 1)
Which two statements about EVPN are true? (Choose two.)

A. EVPN route exchange enables PEs to discover one another and elect a DF.
B. EVPN routes can advertise backbone MAC reachability.
C. EVLs allow you to map traffic on one or more VLANs or ports to a Bridge Domain.

D. EVPN routes can advertise VLAN membership and verify the reachability of Ethernet segments.
E. It is a next-generation Ethernet L2VPN solution that supports load balancing at the individual flow leveland provider advanced access redundancy.
F. It is a next-generation Ethernet L3VPN solution that simplifies control-plane operations and enhances scalability.

Answer: AB

NEW QUESTION 93
- (Exam Topic 1)
Which three statements about Dynamic ARP inspection on Cisco switches are true? (Choose three)

A. The trusted database can be manually configured using the CLI
B. Dynamic ARP inspection is supported only on access ports
C. Dynamic ARP inspection does no perform ingress security checking
D. DHCP snooping is used to dynamically build the trusted database
E. Dynamic ARP inspection checks ARP packets against the trusted database
F. Dynamic ARP inspection checks ARP packets on trusted and untrusted ports

Answer: ADE

NEW QUESTION 98
- (Exam Topic 1)
Which two statements about ping flood attacks are true? (Choose two.)

A. They attack by sending ping requests to the broadcast address of the network.
B. They use SYN packets.
C. The attack is intended to overwhelm the CPU of the target victim.
D. They use UDP packets.
E. They use ICMP packets.
F. They attack by sending ping requests to the return address of the network.

Answer: CE

NEW QUESTION 100
- (Exam Topic 1)
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 104
- (Exam Topic 1)
What are three technologies that can be used to trace the source of an attack in a network environment with multiple exit/entry points? (Choose three.)

A. ICMP Unreachable messages
B. Sinkholes
C. A honey pot
D. Remotely-triggered destination-based black holing
E. Traffic scrubbing

Answer: ADE

NEW QUESTION 106
- (Exam Topic 1)
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 109
- (Exam Topic 1)
Which are two of the valid IPv6 extension headers? (Choose two.)

A. Options
B. Authentication Header

C. Mobility
D. Protocol
E. Next Header
F. Hop Limit

Answer: BC

NEW QUESTION 111
- (Exam Topic 1)
You are considering using RSPAN to capture traffic between several switches. Which two configuration aspects do you need to consider? (Choose two.)

A. All switches need to be running the same IOS version.
B. All distribution switches need to support RSPAN.
C. Not all switches need to support RSPAN for it to work.
D. The RSPAN VLAN need to be blocked on all trunk interfaces leading to the destination RSPAN switch.
E. The RSPAN VLAN need to be allow on all trunk interfaces leading to the destination RSPAN switch.

Answer: BE

NEW QUESTION 112
- (Exam Topic 1)
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 117
- (Exam Topic 1)
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 121
- (Exam Topic 1)
Refer to the exhibit.

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

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 123
- (Exam Topic 1)
Which two statements about the SeND protocol are true? (Choose two.)

A. It counters neighbor discovery threats.
B. It must be enabled before you can configure IPv6 addresses.
C. It supports numerous custom neighbor discovery messages.
D. It logs IPv6-related threats to an external log server.
E. It supports an autoconfiguration mechanism.
F. It uses IPsec as a baseline mechanism.

Answer: AE

NEW QUESTION 126
- (Exam Topic 1)
Which feature does Cisco VSG use to redirect traffic in a Cisco Nexus 1000v Series Switch?

A. VEM
B. VPC
C. VDC
D. vPath

Answer: D

NEW QUESTION 130
- (Exam Topic 1)
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 132
- (Exam Topic 1)
When applying MD5 route authentication on routers running RIP or EIGRP, which two important key chain considerations should be accounted for? (Choose two.)

A. Key 0 of all key chains must match for all routers in the autonomous system.
B. The lifetimes of the keys in the chain should overlap.
C. Routers should be configured for NTP to synchronize their clocks.
D. No more than three keys should be configured in any single chain.
E. Link compression techniques should be disabled on links transporting any MD5 hash.

Answer: BC

NEW QUESTION 136
- (Exam Topic 1)
Which effect of the crypto pki authenticate command is true?

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

Answer: B

NEW QUESTION 137
- (Exam Topic 1)
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 139
- (Exam Topic 1)
Which three transports have been defined for SNMPv3? (Choose three.)

A. DTLS
B. SSH
C. TLS
D. SSL
E. IPcec secured tunnel
F. GET

Answer: ABC

NEW QUESTION 143

- (Exam Topic 1)
Which three messages are part of the SSL protocol? (Choose three.)

A. Message Authentication
B. CipherSpec
C. Record
D. Alert
E. Change CipherSpec
F. Handshake

Answer: DEF

NEW QUESTION 148
- (Exam Topic 1)
What are the three scanning engines that the Cisco IronPort dynamic vectoring and streaming engine can use to protect against malware? (Choose three.)

A. McAfee
B. TrendMicro
C. Sophos
D. Webroot
E. F-Secure
F. Symantec

Answer: ACD

NEW QUESTION 150
- (Exam Topic 1)
Refer to the exhibit.

```
R1(config)#parameter-map type inspect param-map
R1(config-profile)#sessions maximum 10000
R1(config-profile)#ipv6 routing-header-enforcement loose
R1(config-profile)#
R1(config-profile)#class-map type inspect match-any class
R1(config-cmap)#match protocol tcp
R1(config-cmap)#match protocol udp
R1(config-cmap)#match protocol icmp
R1(config-cmap)#match protocol ftp
R1(config-cmap)#
R1(config-cmap)#policy-map type inspect policy
R1(config-pmap)#class type inspect class
R1(config-pmap-c)#inspect param-map
R1(config-pmap-c)#
R1(config-pmap-c)#zone security z1
R1(config-sec-zone)#zone security z2
R1(config-sec-zone)#
R1(config-sec-zone)#zone-pair security zp source z1 destination z2
R1(config-sec-zone-pair)#service-policy type inspect policy
```

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 153
- (Exam Topic 1)
Which two event can cause a failover event on an active/standby setup? (Choose two)

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

Answer: AE

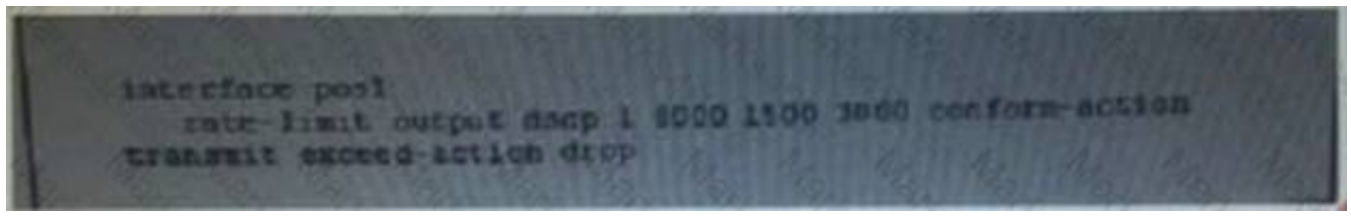
NEW QUESTION 155
- (Exam Topic 1)

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 159
- (Exam Topic 2)
Refer to the exhibit



Which type of packet can trigger the rate hmrter m the given configurator

A. Only DSCP 8000 packets
B. Only DSCP 1 packets
C. Only DSCP 1500 packets
D. DSCP 1, 1500, 3000, and 8000 packets
E. Only DSCP 3000 packets

Answer: A

NEW QUESTION 162
- (Exam Topic 2)
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 163
- (Exam Topic 2)
Which two design options are best to reduce security concerns when adopting loT into an organization? (Choose tow.)

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

Answer: CD

NEW QUESTION 165
- (Exam Topic 2)
AMP for Endpoint is supported on which of these platforms?

A. Windows, MAC, ANDROID
B. Windows, MAC, LINUX (SuSE, UBUNTU), ANDROID
C. Window
D. ANDROID, LINUX (SuSE, REDHAT)
E. Windows, ANDROID, LINUX (REDHA, CentOS), MAC

Answer: D

NEW QUESTION 170
- (Exam Topic 2)
Which command is used to enable 802.1x authentication on an interface?

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

Answer: A

NEW QUESTION 171
- (Exam Topic 2)
Which two options are open-source SDN controllers? (choose two)

A. Opendaylight
B. Big Cloud Fabric
C. Application Policy Infrastructure Controller
D. OpenContrail
E. Virtual Application Networks SDN Controller

Answer: AD

NEW QUESTION 172
- (Exam Topic 2)
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 177
- (Exam Topic 2)
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 179
- (Exam Topic 2)
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 183
- (Exam Topic 2)
Which two combinations of node are allowed in a Cisco ISE distributed deployment? (Choose two)

A. ISE cluster with eight nodes
B. Pair of passive ISE nodes for automatic failover
C. One or more policy service ISE nodes for session failover standalone
D. Primary and secondary administration ISE nodes for high availability
E. Active and standby ISE notes for high availibilty

Answer: BD

NEW QUESTION 185
- (Exam Topic 2)
Which IPS deployment mode is most reliant on the Automatic Application Bypass feature?

A. Passive
B. Strict
C. transparent
D. switched
E. tap
F. inline

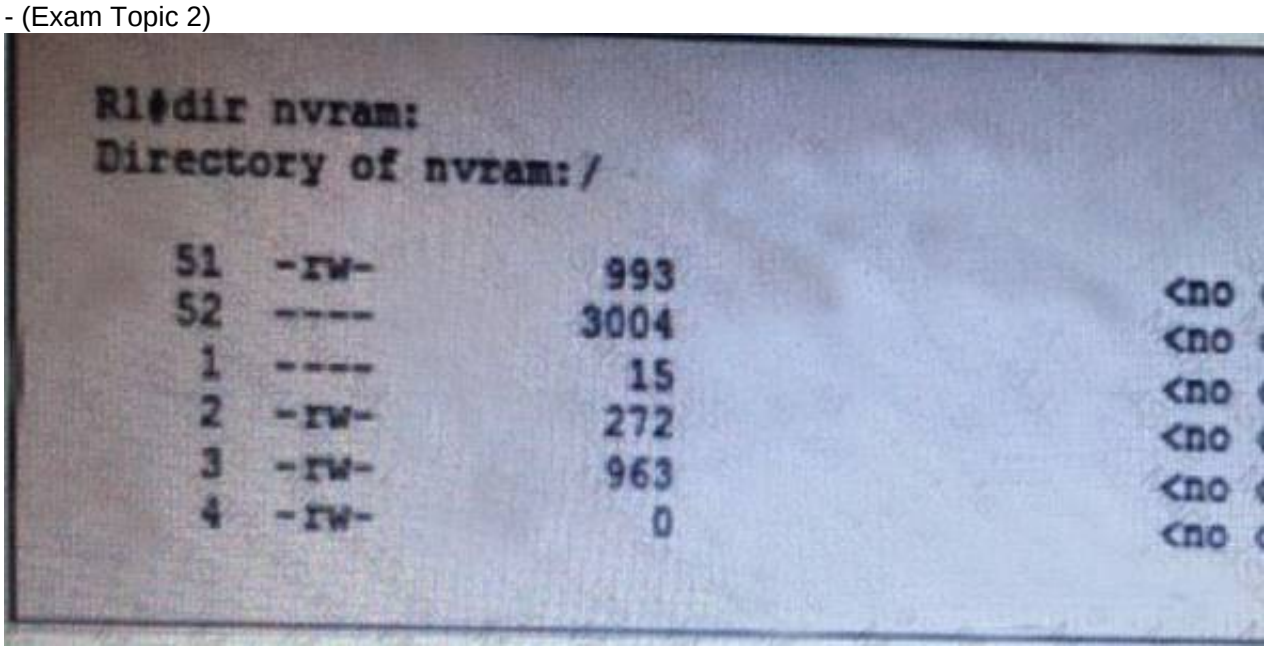
Answer: F

NEW QUESTION 188
- (Exam Topic 2)
Your customer wants to implement Cisco Firepower IPS and 1 secure policy.
However, a monitoring period of 2 weeks is applied against real traffic without causing an outage before going in to fu of the default policies as a base and set the policy action to ensure.
Which two policies to achieve these requirements are true?

A. Set IPs policy to trust
B. Set IPs policy to Monitor
C. Base the IPS policy on the default Advanced Security over Connection
D. Base the IPS policy on the default Balanced Security and Connection
E. Base the IPS policy on the default Connectivity over Security
F. Base the IPS policy on the default Security over Connectivity
G. Set IPS Policy to No Drop

Answer: BD

NEW QUESTION 189
- (Exam Topic 2)



Refer to the exhibit. Which statement about router R1 is true?

A. Its NVRAM contains public and private crypto keys
B. RMON is configured
C. Its private-config is corrupt
D. Its startup configuration is missing
E. It running configuration is missing

Answer: A

Explanation:
https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/50282-ios-caios. html

NEW QUESTION 193
- (Exam Topic 2)
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 198
- (Exam Topic 2)
Which three flow protocols can tie SealthWatch System use lo monitor potential security threats? (Choose two)

A. OpenFlow
B. Ntop
C. IPFIX
D. NetFlow
E. sFlow
F. Jflow

Answer: CDE

NEW QUESTION 203
- (Exam Topic 2)
Which command sequence can you enter to enable IP multicast for WCCPv2?

A. Router(config)#ip wccp web-cache group-address 224.1.1.100 Router(config)# interface FastEthernet0/0Router(config-if)#ip wccp web-cache redirect out
B. Router(config)#ip wccp web-cache group-list Router(config)# interface FastEthernet0/0 Router(config)# ip wccp web-cache group-listen
C. Router(config)#ip wccp web-cache service-list Router(config)# interface FastEthernet0/0 Router(config)# ip wccp web-cache group-listen
D. Router(config)#ip wccp web-cache group-address 224.1.1.100 Router(config)# interface FastEthernet0/0Router(config)# ip wccp web-cache redirect in
E. Router(config)#ip wccp web-cache group-address 224.1.1.100 Router(config)# interface FastEthernet0/0Router(config)# ip wccp web-cache group-listen

Answer: E

NEW QUESTION 204
- (Exam Topic 2)
Which command is required for bonnet filter on Cisco ASA to function properly?

A. dynamic-filter inspect tcp /80
B. dynamic-filter whitelist
C. inspect botnet
D. inspect dns dynamic-filter-snoop

Answer: D

NEW QUESTION 207
- (Exam Topic 2)
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 212
- (Exam Topic 2)
Which three EAP protocols are supported in WPA and WPA2? (Choose three)

A. EAP-PSK
B. EAP-EKE
C. EAP-FAST
D. EAP-AKA
E. EAP-SIM
F. EAP-EEE

Answer: CDE

NEW QUESTION 215
- (Exam Topic 2)
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 217
- (Exam Topic 2)
Which statement about the restrictions of redirection on Cisco Cloud Web Security tunnels on ISR4000 Series Router is true?

A. The cws-tunnel out command can be configured up to a maximum of three WAN interfaces
B. User authentication (through NTLM) is supported
C. Access lists based on object groups are supported in white listing and redirect list configuration
D. IPv6 is not supported
E. Multiple access list are supported for white listing

Answer: C

NEW QUESTION 219
- (Exam Topic 2)
When you use the Firepower Management Center to deploy an access control policy to a managed device, which process is restarted?

A. kupdate
B. snort
C. crond
D. reportd
E. mysqld

Answer: B

NEW QUESTION 223
- (Exam Topic 2)
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 225
- (Exam Topic 2)
Which Cisco ISE profiler service probe can collect information about Cisco Discovery Protocol?

A. DHCP SPAN
B. RADIUS
C. SNMP Query
D. NetFlow
E. HTTP
F. DHCP

Answer: C

NEW QUESTION 227
- (Exam Topic 2)
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 232
- (Exam Topic 2)
Which two statements about the TTL value in an IPv4 header are true? (Choose two)

A. It is a 4-bit value.
B. It can be used for traceroute operations.
C. When it reaches 0, the router sends an ICMP Type 11 message to the originator.
D. Its maximum value is 128.
E. It is a 16-bit value.

Answer: BC

NEW QUESTION 237
- (Exam Topic 2)
Which IPS deployment mode can blacklist traffic?

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

Answer: C

NEW QUESTION 240
- (Exam Topic 2)
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 242
- (Exam Topic 2)
What are two types of attacks against wireless networks that be prevented by a WLC? (Choose two)

A. DHCP rouge server attacks
B. Layer 3 flooding attacks
C. Inverse ARP attacks on specific ports
D. IP spoofing attacks
E. ARP sniffing attacks on specific ports

Answer: AD

NEW QUESTION 246
- (Exam Topic 2)
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 -I 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 249
- (Exam Topic 2)
Refer to the exhibit.

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

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

A. User five can execute the show run command.
B. User five can view usernames and passwords.
C. User superuser can change usernames and passwords.
D. User superuser can view the configuration.
E. User superuser can view usernames and passpords.
F. User cisco can view usernames and passwords.

Answer: AD

NEW QUESTION 250
- (Exam Topic 2)
A new computer is not getting its IPv6 address assigned by the router. While running WireShark to try to troubleshoot the problem, you find a lot of date that is not helpful to nail down the problem. What two filters
would you apply to WireShark to filter the data that you are looking for?(Choose two)

A. icmpv6.type == 135
B. icmpv6type == 136
C. icmpv6.type == 136
D. icmpv5type == 135
E. icmpv6type == 135

Answer: AC

NEW QUESTION 254
- (Exam Topic 2)
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

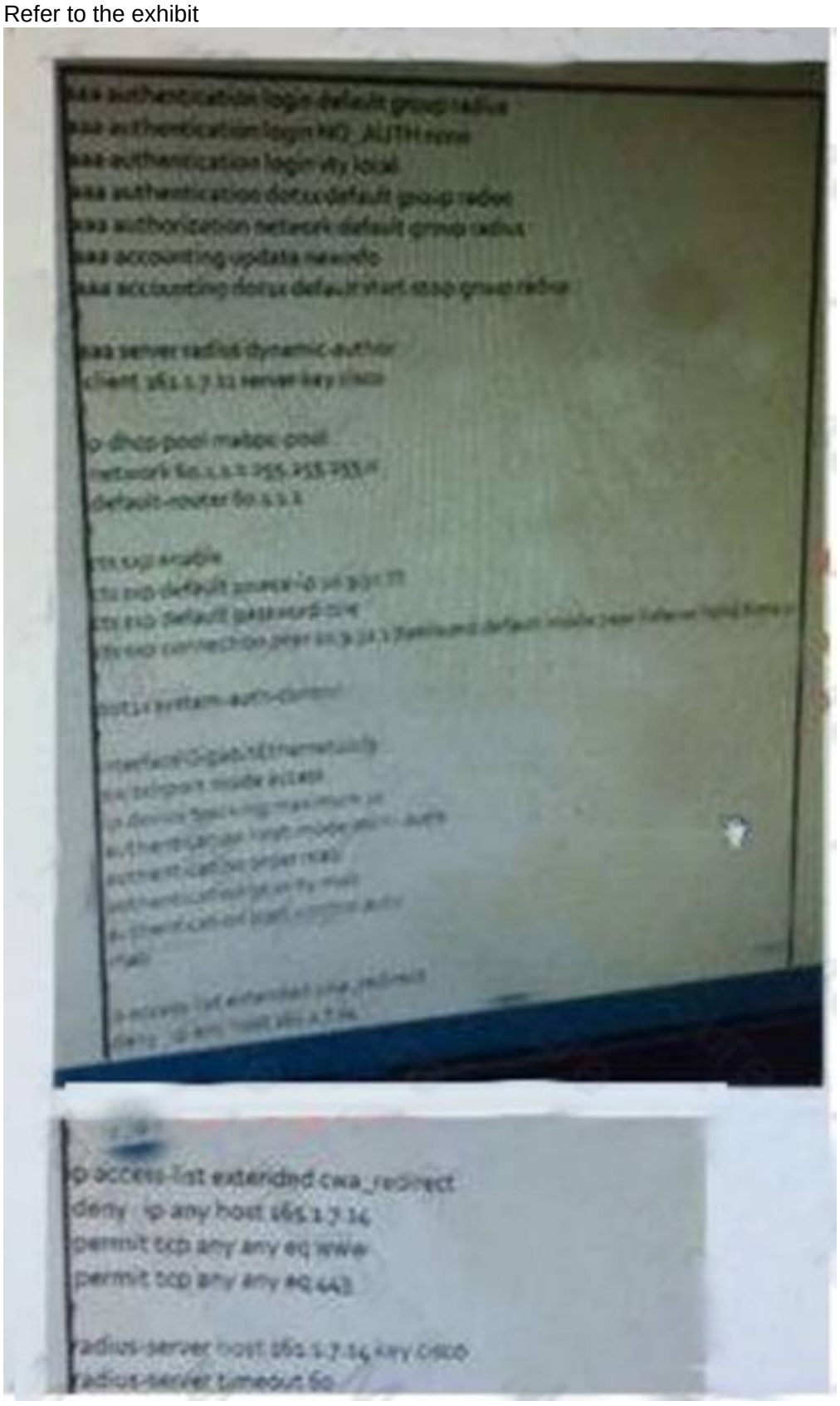
Answer: F

NEW QUESTION 258
- (Exam Topic 2)
On a Cisco Wireless LAN Controller (WLC), which web policy enables failed Layer 2 authentication to fall back to WebAuth authentication with a user name and password?

A. On MACFilter Failure
B. Passthrough
C. Splash Page Web Redirect
D. Conditional Web Redirect
E. Authentication

Answer: A

NEW QUESTION 260
- (Exam Topic 2)
Refer to the exhibit



Refer to the exhibit Customer has opened a case with Cisco TAC reporting issue that client connect to the network using guest account. Looking at the

configuration of the switch, w possible issue?

A. MAB should be disabled on the authentication port
B. Dynamic authorization configuration has incorrect RADIUS server
C. issue with the DHCP pool configuration
D. Dot1x is disabled on the authentication port
E. AAA network authorization incorrectly configured
F. CTS is incorrectly configured
G. Issue with redirect ACL "cwa_edirecrt"

Answer: G

NEW QUESTION 264
- (Exam Topic 2)
Which two characteristics of DTLS are true? (Choose two)

A. It is used mostly by applications that use application layer object-protocols
B. It includes a congestion control mechanism
C. It completes key negotiation and bulk data transfer over a single channel.
D. It supports long data transfers and connectionless data transfers.
E. It cannot be used if NAT exists along the path.
F. It concludes a retransmission method because it uses an unreliable datagram transport.

Answer: BF

NEW QUESTION 268
- (Exam Topic 2)
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 272
- (Exam Topic 2)
Which of the following is AMP Endpoint offline engine for windows?

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

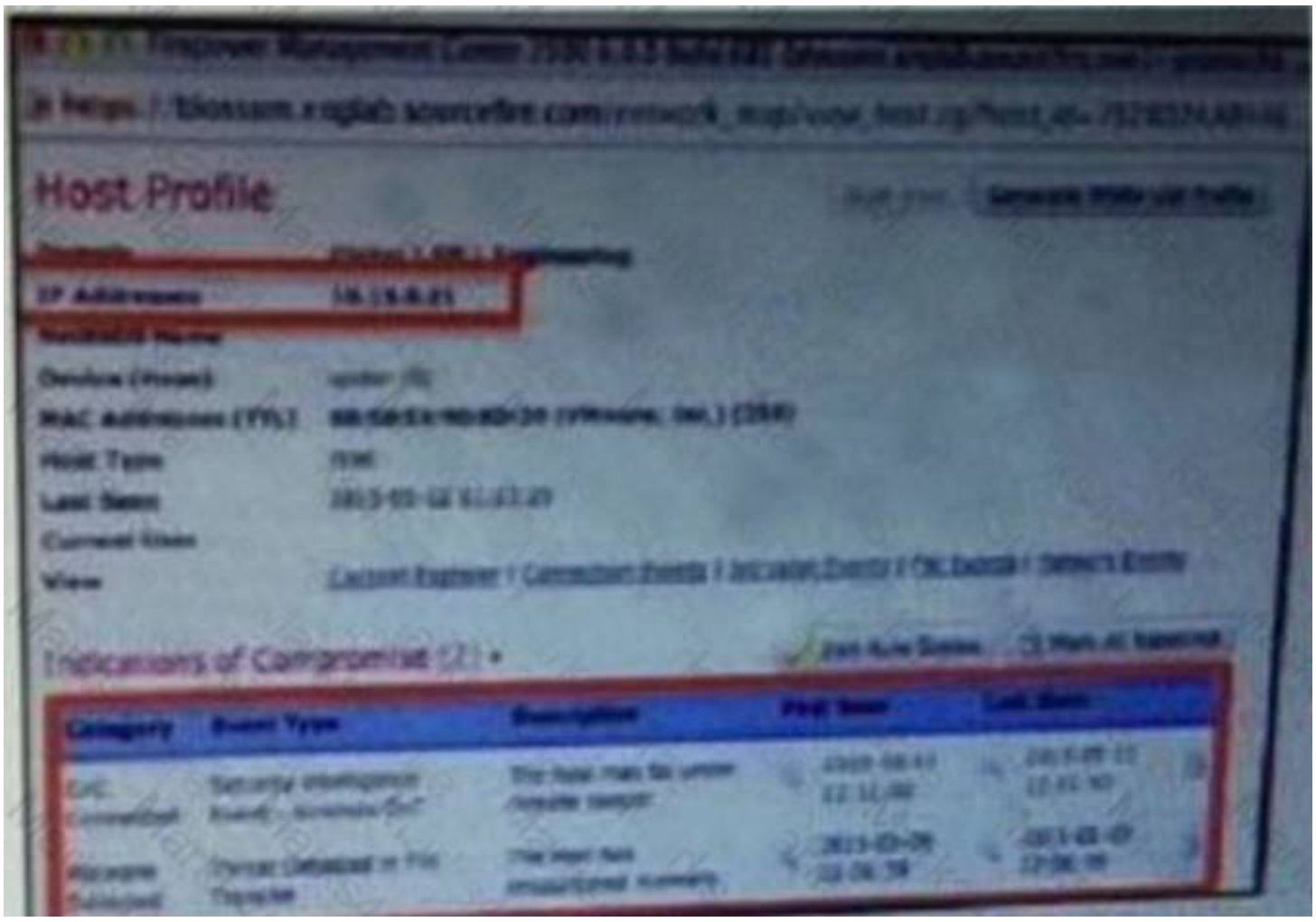
Answer: D

NEW QUESTION 276
- (Exam Topic 2)
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 279
- (Exam Topic 2)



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 281
- (Exam Topic 2)
In which two ways does OpenDNS ensure security? (Choose two)

A. OpenDNS servers run a proprietary version of djbdns, which is a s maximum security
B. OpenDNS servers can analyze the hash of incoming URL stings to
C. It supports certificate authenticate for DNS connections
D. OpenDNS servers can integrate with the Cisco Network Registrar DNS traffic
E. It encrypts all DNS connections with SSL
F. The 24-hour network operations center guarantees that critical
G. hardware vendors are applied within 12 hours of release
H. It limits caching to efficiently purge spoofed and malicious address
I. It encrypts all DNS connections with DNSCrypt

Answer: BH

NEW QUESTION 286
- (Exam Topic 2)
Which of these command sequences will send an email to holly@invalid.com using SMTP?

A. HELO invalid.comMAIL TO:<holly@invalid.com> MESSAGEEND
B. MAIL FROM:<david@invalid.com> RCPT TO:<holly@invalid.com> DATA
C. HELO invalid.comMAIL FROM:<david@invalid.com> RCPT TO:<holly@invalid.com> BODY
D. MAIL FROM:<david@invalid.com>RCPT TO:<holly@invalid.com> MESSAGE

Answer: B

NEW QUESTION 289
- (Exam Topic 2)
In which two ways does the Open DNS infrastructure ensure reliability? (Choose two)

A. It ensures redundancy by using at least two telecom carters at each site
B. it limits caching to reduce the Incidence of state and dead links
C. ft uses a self-healing network to protect against individual failures
D. Its networks are geographical^ integrated to reduce the potential impact of local issues.
E. Regional sites load-balance among one another to prevent bottlenecks
F. ft uses multicast routing to ensure that requests are routes to the nearest data center
G. ft uses a specialized form of multicast addressing called Geo cast ensure the most efficient when a local site goes down

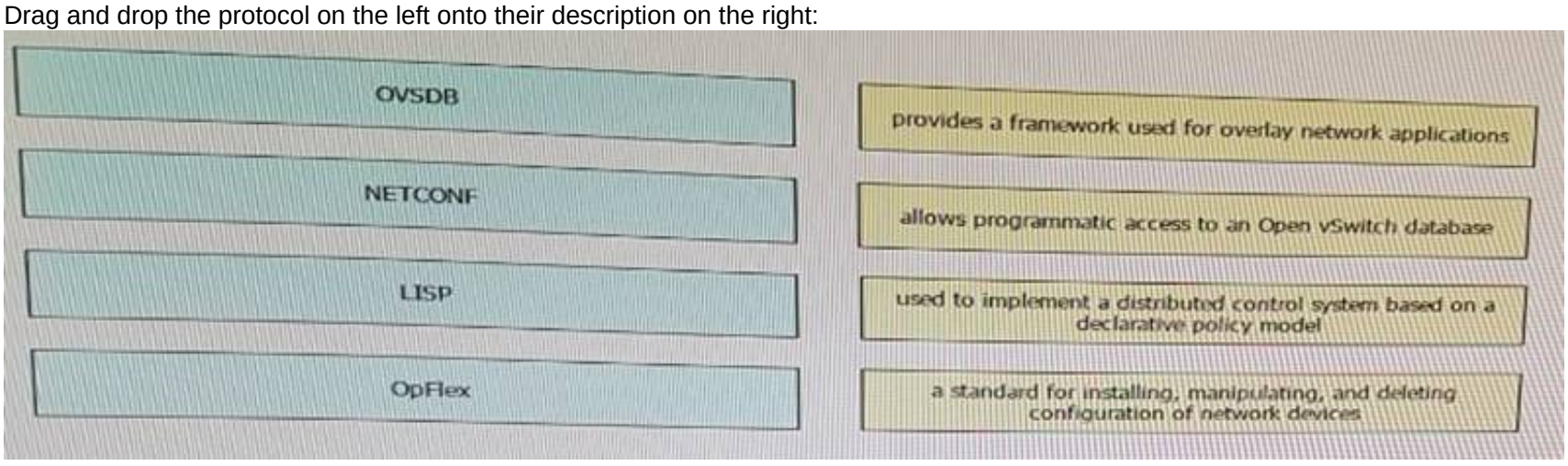
Answer: AG

NEW QUESTION 292
- (Exam Topic 2)
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 295
- (Exam Topic 2)
Drag and drop the protocol on the left onto their description on the right:



A. Mastered
B. Not Mastered

Answer: A

Explanation:
A-2 B-4 C-1 D-3

NEW QUESTION 298
- (Exam Topic 2)
In which type of multicast does the Cisco ASA forward IGMP messages to the upstream router?

A. clustering
B. PIM multicast routing
C. stub multicast routing
D. multicast group concept

Answer: C

NEW QUESTION 302
- (Exam Topic 2)
Which description of configuring the port security feature true?

A. With regards to setting the maximum number of MACs formaximum number of allowed AMCs for the access and voice
B. With regards to setting the maximum number of MACs for f maximum number of allowed ACs for the access VLAN only'
C. It is not possible to set the maximum number MACs on the ; configured on the same switch port
D. With regards to setting the maximum number of post secure number of allowed MACs for the voice VLAN only as a phone

Answer: A

NEW QUESTION 303
- (Exam Topic 2)
Which three statements about VXLAN are true? (Choose three.)

A. It can converge topology without STP.
B. It enables up to 24 million VXLAN segments to coexist in the same administrative domain.
C. It uses encrypted TCP/IP packets to transport data over the physical network.
D. The VTEP encapsulates and de-encapsulates VXLAN traffic by adding or removing several fields, including a 16-bit VXLAN header.
E. It uses a 24-bit VXLAN network identifier to provide layer 2 isolation between LAN segments.
F. It can migrate a virtual machine from one Layer 2 domain to another over a Layer 3 network.

Answer: ADE

NEW QUESTION 308
- (Exam Topic 2)
Which difference between DomainKeys and DKIM in Cisco ESA deployment is true?

A. Only Domain Keys support incoming-mail authentication
B. AsyncOS supports mail signing for DKIM only
C. Bounce and delay messages can use DKIM only
D. AsyncOS suppoets mail signing and incoming –mail authentication for DomainKeys only
E. If DomainKeys and DKIM are associated to mail flow AsynOS uses only DKIM to sign outgoing
F. Messages
G. Only DKIM supports incoming-mail verifications

Answer: D

NEW QUESTION 309
- (Exam Topic 2)
Which tunnel type does the Cisco unified Wireless Solution use to map a provisioned guest WLAN to an anchor WLC?

A. PEAP
B. IPsec
C. TLS
D. GRE
E. EAPoL
F. EoIP

Answer: F

NEW QUESTION 310
- (Exam Topic 2)
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 315
- (Exam Topic 2)
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 320
- (Exam Topic 2)
How does Scavenger-class Qos mitigate Dos and worm attacks?

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

Answer: D

NEW QUESTION 321
- (Exam Topic 2)
How is the Cisco IronPort email data loss prevention licensed?

A. It is a per-site license
B. It comes free with Iron Port Email server
C. It is a per-enterprise license
D. It is a per-server license
E. It is a per-user license

Answer: E

NEW QUESTION 324
- (Exam Topic 2)
Which three ESMTP extensions are supported by the Cisco ASA?Choose three

A. NOOP
B. PIPELINING
C. SAML

D. 8BITMIME
E. STARTTLS
F. ATRN

Answer: ACE

NEW QUESTION 326
- (Exam Topic 2)
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 329
- (Exam Topic 2)
Which two statements about the Cognitive Threat Analytics feature of Cisco AMP for Web Security are true? (Choose two.)

A. It can locate and identify indicators of prior malicious activity on the network and preserve information for forensic analysis.
B. It can identify potential data exfiltration.
C. It uses a custom virtual appliance to perform reputation-based evaluation and blocking of incoming files.
D. It can perform file analysis by sandboxing known malware and comparing unknown files to a local repository of threats.
E. It can identify anomalous traffic passing through the Web gateway by comparing it to an established baseline of expected activity.
F. It can identify anomalous traffic within the network by comparing it to an established baseline of expected activity.

Answer: BF

NEW QUESTION 334
- (Exam Topic 2)
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

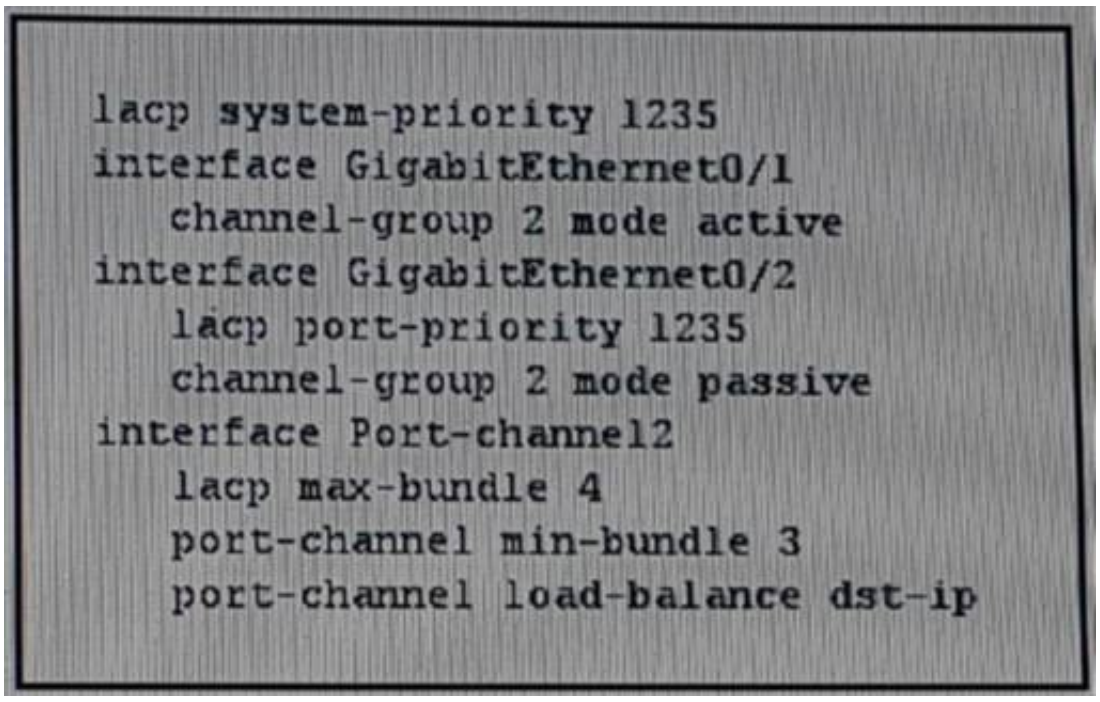
NEW QUESTION 337
- (Exam Topic 2)
Refer to the exhibit:
1d00h: IPSec (validate transform proposal): proxy identities not supported 1d00h: ISAKMP: IPSec policy invalid proposal
1d00h: ISAKMP (0:2): SA not acceptable

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 342
- (Exam Topic 2)
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 347
- (Exam Topic 2)
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.

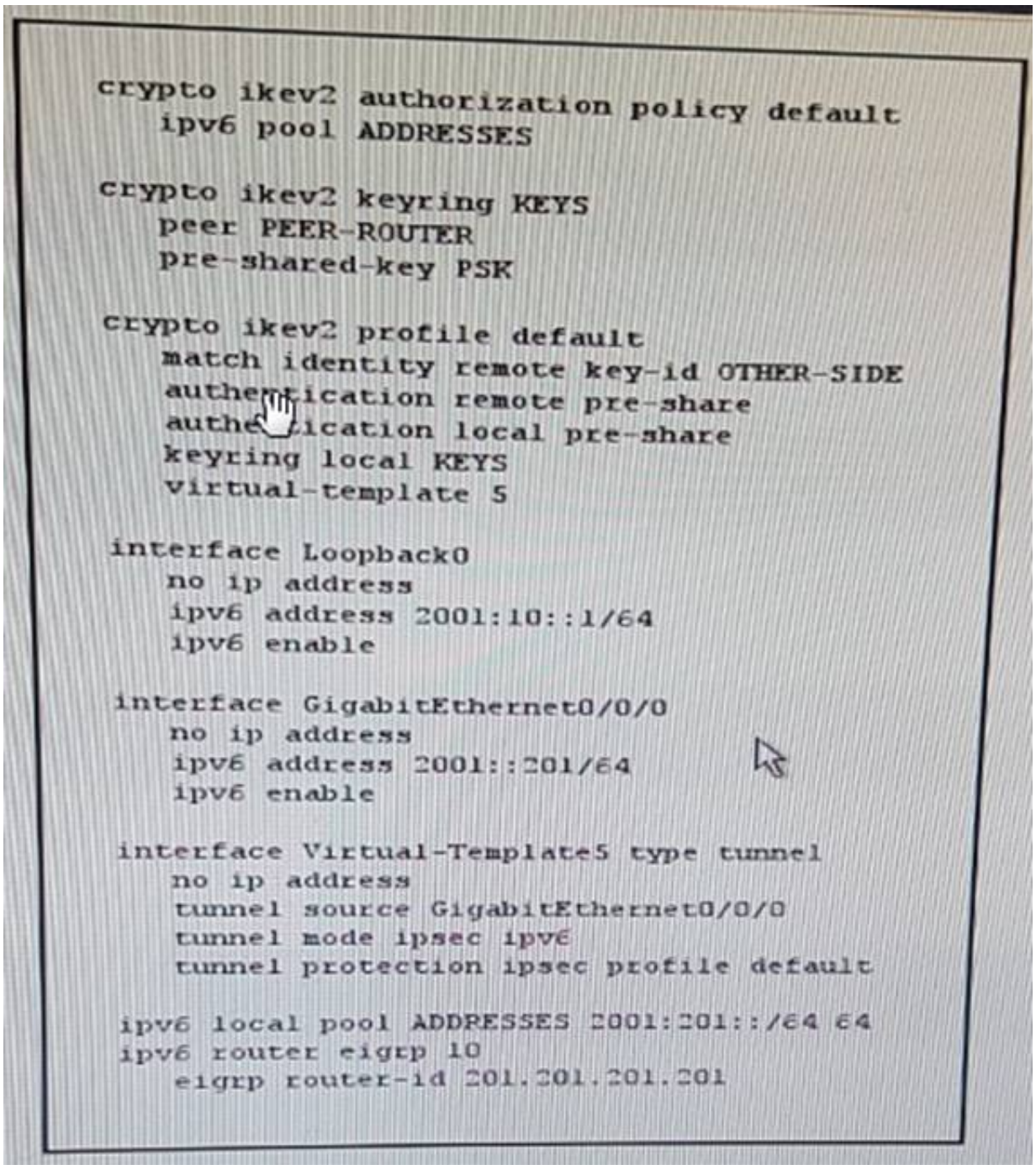
Answer: AE

NEW QUESTION 349
- (Exam Topic 2)
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 350
- (Exam Topic 2)
Refer to the exhibit.



Which three additional configuration elements must you apply to complete a functional FlexVPN deployment? (Choose three)

A. crypto ikev2 keyring default peer PEER-ROUTERaddress 2001::101/64interface virtual-template5 type tunnel ip nhrp network-id 10ip nhrp shortcut loopback0
B. interface loopback0 tunnel mode ipsec ipv6tunnel protection ipsec profile default
C. interface Tunnel0bfd interval 50 min_rx 50 multiplier 3 no bfd echo
D. crypto ikev2 keyring KEYS peer PEER-ROUTERaddress 2001::101/64 crypto ikev2 profile defaultaaa authorization group pak list ccie default
E. interface virtual-template5 type tunnel ipv6 unnumbered loopback0ipv6 eigrp 10 ipv6 enableinterface loopback0 ipv6 eigrp 10
F. aaa authorization network ccie local

Answer: CDE

NEW QUESTION 352
- (Exam Topic 2)
Which two description of the HomeNet and ExternalNet variable sets that are used within Cisco Firepower access control and IPS policies are true? (Choose two)

A. They are used to exclude or include protected network subnets form security intelligence and blacklist filtering
B. They are used to decrease the number of false positives by defining the protected network
C. They are used to fine tune the performance of the appliance by optimizing how signatures are matched to packets based on the source and destination addresses in a packet
D. They are used for reporting reasons to give context on the direction of a connection or maliciousattack as it appears in the event viewer reports
E. They are a legacy sport feature that has no effect since Firepower 6.x.

Answer: AD

NEW QUESTION 357
- (Exam Topic 2)
In which two situations is web authentication appropriate? (Choose two)

A. When secure connections to the network are unnecessary.
B. When a fallback authentication method is necessary
C. When 802.1x authentication is required.
D. When devices outside the control of the orgacization`s IT department are permitted to connect to the network.
E. When WEP encryption must be deployed on a large scale.

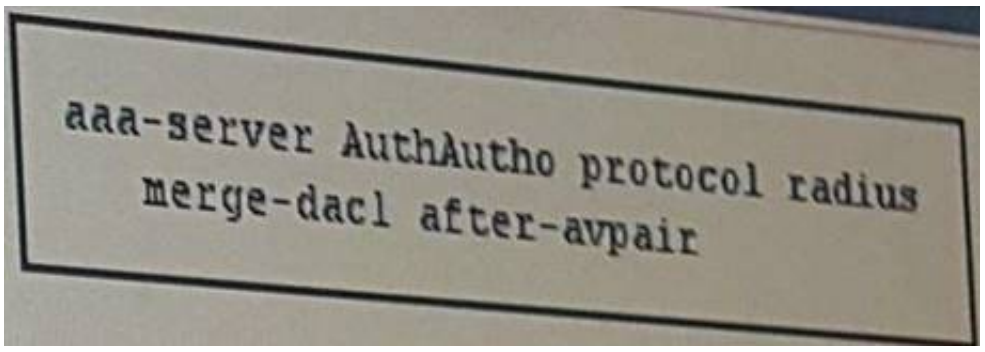
Answer: BD

NEW QUESTION 360
- (Exam Topic 2)
Which two limitations of ISE inline posture are true?

A. The Cisco Discovery Protocol is not supported
B. QoS is not supported in a virtual environment
C. The Simple Network Management Protocol agent is not supported
D. Flexible NetFlow is not supported
E. Multicast is not supported

Answer: AC

NEW QUESTION 364
- (Exam Topic 2)
Refer to the exhibit.



Which effect of this configuration is true?

A. The downloadable ACL and AV pair ACL are merged after three connection attempts are made to the RADIUS server.
B. The downloadable ACL and AV pair ACL are merged immediately when the RADIUS server is activated.
C. For all users, entries in a downloadable ACL are given priority over entries in an AC pair ACL.
D. The downloadable ACL and AV pair ACL entries are merged together,one ACE at a time.
E. A downloadable ACL is applied after an AV pair ACL.

Answer: E

NEW QUESTION 366
- (Exam Topic 2)
Which three VSA attributes are present in a RADIUS WLAN Access-Accept packet? (Choose three)

A. Tunnel-Private-Group-ID
B. Tunnel-Type
C. SSID
D. EAP-Message
E. LEAP Session-Key
F. Authorization-Algorithm-Type

Answer: CEF

NEW QUESTION 367
- (Exam Topic 2)
What are three pieces of data you should review in response to a supported SSL MITM attack? (Choose three.)

A. the MAC address of the SSL server
B. the MAC address of the attacker
C. the IP address of the SSL server
D. the X.509 certificate of the attacker
E. the X.509 certificate of the SSL server
F. the DNS name of the SSL server

Answer: CEF

NEW QUESTION 372
- (Exam Topic 2)
Which option does a wired MAB appear in ISE RADIUS live logs?

A. (Radius: Service-Type equals Framed) and (Radius: NAS-Port-Type equals Ethernet)
B. (Radius: Service-Type equals Call–Check) and (Radius: NAS-Port-Type equals Ethernet)
C. (Radius: Service-Type equals Call–Check) and (Radius: NAS-Port-Type equals PPPoEoVLAN)
D. (Radius: Service-Type equals Call–Check) and (Radius: NAS-Port-Type equals PPPoEoVLAN)

Answer: C

NEW QUESTION 376
- (Exam Topic 3)
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 380
- (Exam Topic 3)
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 383
- (Exam Topic 3)
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 385
- (Exam Topic 3)
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.

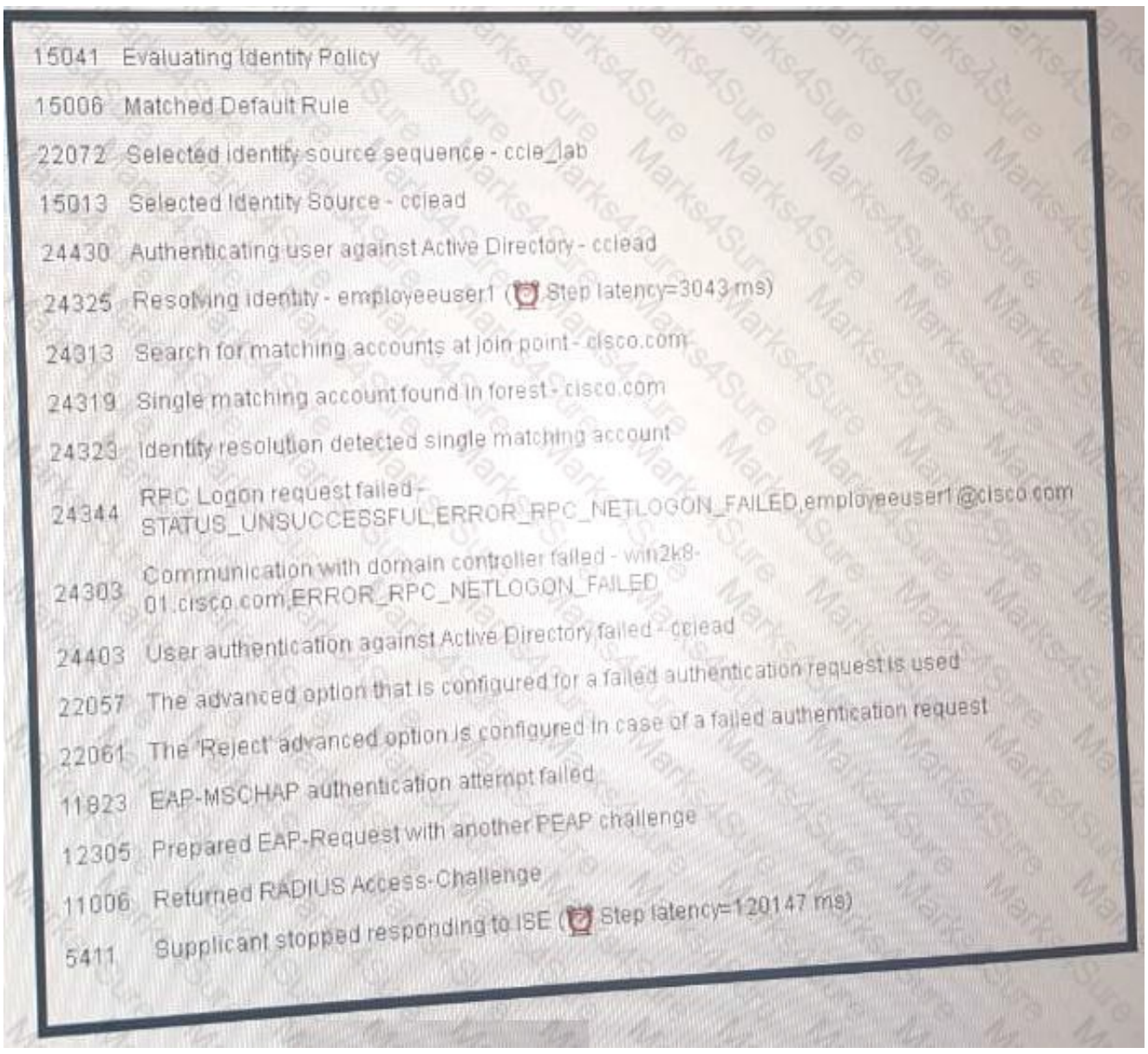
Answer: A

NEW QUESTION 390
- (Exam Topic 3)
Which two protocols are used by the management plane in a Cisco IOS device? (Choose two)

A. DHCP
B. FTP
C. NTP
D. CHAP
E. IKEv2
F. NETFLOW
G. PAP
H. TLS
I. 3DES

Answer: BF

NEW QUESTION 391
- (Exam Topic 3)
Refer to the exhibit. Refer to the Exhibit.

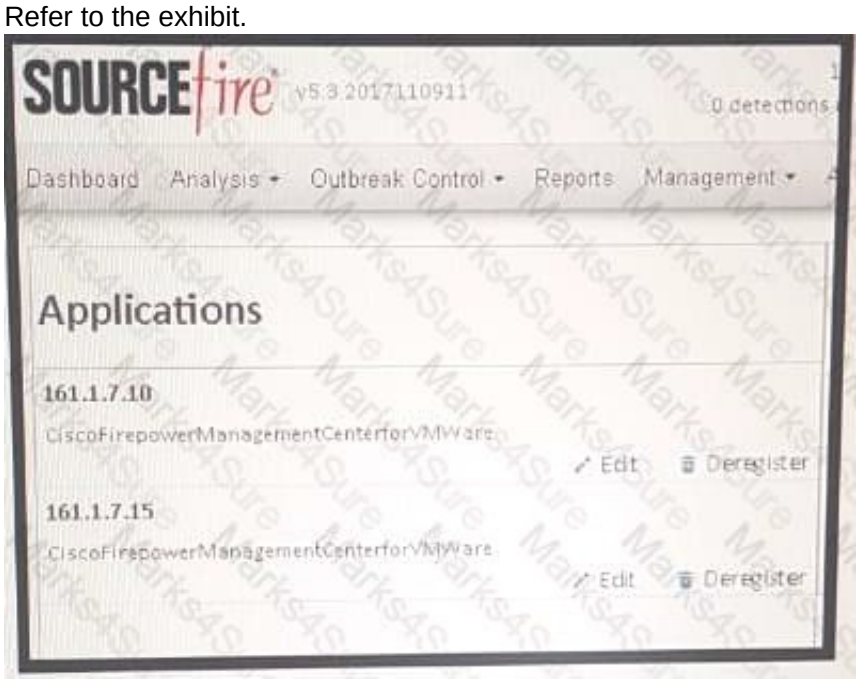


What could be the reason for Dot1x session failure?

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 394
- (Exam Topic 3)
Refer to the exhibit.

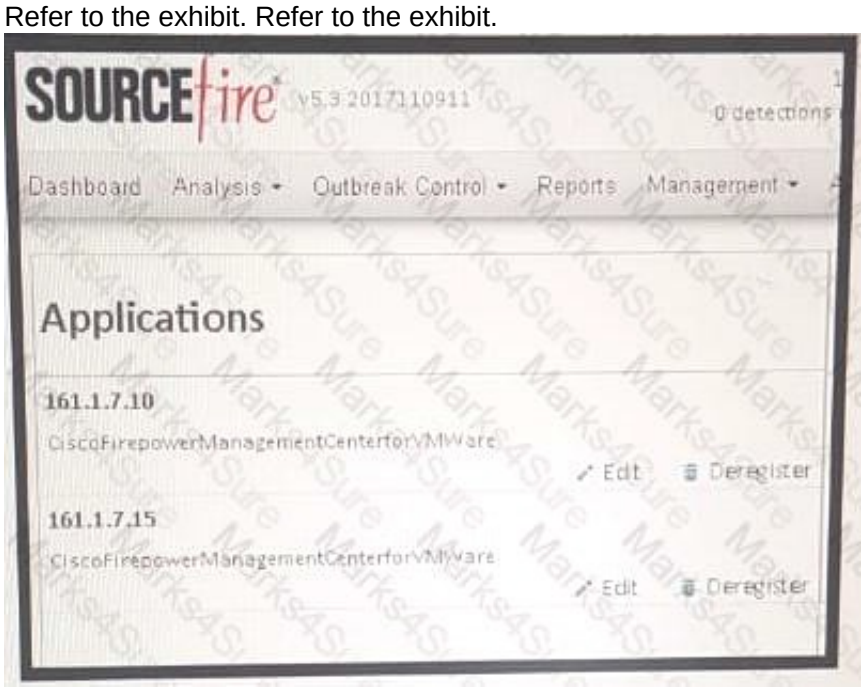


The FMC with address 161 1 7 16 is not seeing AMP Connector scan events that are reported to the AMP cloud from the test-pc Windows machine that belongs to "protect" group. Which cause of the issue is true?

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 399
- (Exam Topic 3)
Refer to the exhibit. Refer to the exhibit.



FMC with address 161.1.7.15 is not seeing AMP connector scan events reported to
AMP cloud from "test-pc" windows machine that belongs to "Protect" group. What could be the issue?

A. Windows machine not reporting scan events to AMP cloud
B. Windows machine not reporting events to FMC
C. Incorrect group is selected for the events export in AMP cloud for FMC
D. AMP cloud not added in FMC
E. FMC not added in AMP cloud
F. Windows machine belongs to incorrect group in AMP cloud policy.
G. Event should be viewed as "Connection" event in FMC

Answer: F

NEW QUESTION 400
- (Exam Topic 3)
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 404
- (Exam Topic 3)
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 408
- (Exam Topic 3)
Which description of TAP mode deployment in IPS is true?

A. Access rules configured in TAP mode does not generate events.
B. TAP mode is available when ports are configured as passive interfaces.
C. TAP mode implementation requires SPAN configuration on a switch.
D. TAP mode is not available when IPS is deployed inline.
E. Access rules configured in TAP mode generates events when triggered and perform definer action on the traffic stream.
F. In TAP mode, traffic flow gets disturbed for analysis.

Answer: E

NEW QUESTION 410
- (Exam Topic 3)
Which statement about VRF-lite implementation in a service provider network is true?

A. It requires multiple links between CE and PE for each VPN connection to enable privacy
B. It uses input interfaces to differentiate routes for different VPNs on the CE device
C. It can only support one VRF instance per CE device
D. It can have multiple VRF instances associated with a single interface on a CE device
E. It supports multiple VPNs at a CE device but their address spaces should not overlap

Answer: B

NEW QUESTION 415
- (Exam Topic 3)
Which description of a hybrid SDN framework is true?

A. The control plane and data plane are pulled from the networking element and put in an 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 an SDN controller.
D. The control plane is pulled from the networking element and put in an SDN controller

Answer: B

NEW QUESTION 420
- (Exam Topic 3)
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 421
- (Exam Topic 3)
As an enterprise, you have decided to use Cisco Umbrella (OpenDNS) services for all public DNS requests. In which two ways can you ensure that all DNS clients (endpoints) use this service for external requests only? (Choose two.)

A. Install the umbrella proxy server on all the supported operating systems and configure it appropriately
B. Use DHCP to push the OpenDNS servers to the endpoints
C. Install the Umbrella server in your data center that will provide these services locally
D. Install the Umbrella client on all the supported operating systems and configure it appropriately
E. Configure the OpenDNS servers as forwarders on your internal DNS servers

Answer: DE

NEW QUESTION 423
- (Exam Topic 3)
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 427
- (Exam Topic 3)
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 429
- (Exam Topic 3)
What is the best description of a docker file?

A. Text document used to build an image
B. Message Daemon files
C. Software used to manage containers
D. Repository for docker images

Answer: A

NEW QUESTION 433
- (Exam Topic 3)
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 435
- (Exam Topic 3)
Which statement about the failover link when ASAs are configured in the failover mode is true?

A. The information sent over the failover link can he sent only as a secured communication
B. The information sent over the failover link cannot be sent in clear text, but it could be secured communication using a failover key
C. It is not recommended to use secure communication over the failover link when ASA terminating the VPN tunnel
D. Only the configuration replication that is sent across the link can be secured using a failover key
E. The information sent over the failover link can be in clear text
F. Failover key is not required for the secure communication over the failover link

Answer: E

NEW QUESTION 436
- (Exam Topic 3)
Which entity is responsible for the Stealthwatch Management Center to interact with ISE?

A. FMC
B. DNA
C. pxGrid
D. ASA
E. Threat grid
F. NGIPs

Answer: CF

NEW QUESTION 440
- (Exam Topic 3)
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 445
- (Exam Topic 3)
Which statement about VRF-Lite implementation in a service provider network is true?

A. It disables the sharing of one CE device among multiple customers.
B. It can have multiple VRF instances associated with a single interface on a CE device.
C. It requires multiple links between CE and PE for each VPN connection to enable privacy.
D. It supports multiple VPNs at a CE device but their address spaces must not overlap.
E. It uses input interfaces to differentiate routes for different VPNs on the CE device.
F. It can support only one VRF instance per CE device.

Answer: E

NEW QUESTION 447
- (Exam Topic 3)
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 452
- (Exam Topic 3)
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 454
- (Exam Topic 3)
Refer to the exhibit.
Missing Exhibit
AMP cloud is configured to report AMP connector scan events from windows machine
belonging to "Audit" group to FMC, but the scanned events are not showing up in FMC. What could be the possible cause?

A. AMP cloud is pointing to incorrect FMC address
B. Possible issues with certificate download form AMP cloud fro FMC integration
C. Incorrect group is selected for the events export in AMP cloud for FMC
D. Event should be viewed as "Malware" event in FMC
E. DNS address is misconfigured on FMC
F. FMC is pointing to incorrect AMP cloud address

Answer: D

NEW QUESTION 458
- (Exam Topic 3)
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 463
- (Exam Topic 3)
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 467
- (Exam Topic 3)
Which of the following correctly describes NVGRE functionality?

A. In NVGRE network the endpoints are not responsible for the NVGRE encapsulation removal
B. It allows to create physical layer-2 topologies on physical layer-3 network
C. It tunnels PPP frames inside an IP packet over a physical network
D. In NVGRE network VSID does not need to be unique
E. It tunnels Ethernet frames inside an IP packet over a virtual network
F. It allows to create physical layer-2 topologies on virtual layer-3 network
G. In NVGRE network VSID is used to identify tenant’s address space

Answer: G

NEW QUESTION 471
- (Exam Topic 3)
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 473
- (Exam Topic 3)
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 476
- (Exam Topic 3)
Which statement correctly describes Botnet attack?

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

Answer: D

NEW QUESTION 481
- (Exam Topic 3)
Which of the following is true regarding failover link when ASAs are configured in the failover mode?

A. It is not recommended to use secure communication over failover link when ASA is terminating the VPN tunnel
B. Only the configuration replication sent across the link can be secured using a failover key
C. The information sent over the failover link can only be in clear text
D. The information sent over the failover link can be send in clear text, or it could be secured communication using a failover key
E. Failover key is not required for the secure communication over the failover link
F. The information sent over the failover link can only be sent as a secured communication

Answer: C

NEW QUESTION 486
- (Exam Topic 3)
An university has hired you as a consultant to advise them on the best method to prevent DHCP starvation attacks in the campus. They have already implemented DHCP snooping and port security to control the situation, but those do not fully contain the issue. Which two actions do you suggest to fix this issue? (Choose two.)

A. Use the ip dhcp snooping limit rate command on trusted and untrusted interfaces and set the rate to suitable values that are relevant to each interface reqpectively.
B. Use the ip dhcp snooping verify mac-address command to ensure that the source MAC address in the DHCP rquest matches the client hardware address (CHADDR) sent to the DHCP server.
C. Use the ip dhcp snooping verify mac-address command to ensure that the source MAC address in the DHCP request matches the client identifier (CLID) field sent to the DHCP server.
D. Use the ip dhcp snooping limit rate command only to ensure that the source MAC address in the DHCP request matches the client identifier (CLID) field sent to the DHCP server.
E. User the ip dhcp snooping limit rate command on trusted and untrusted interfaces set to the same rate value.
F. Use the ip dhcp snooping limit rate command only on untrusted interfaces and set the rate to suitable values that are relevant to the interface.

Answer: BF

NEW QUESTION 489
- (Exam Topic 3)
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 491
- (Exam Topic 3)
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 492
- (Exam Topic 3)
In which two modes can a private AMP cloud be deployed? (Choose two.)

A. internal mode
B. hybrid mode
C. air gap mode
D. cloud-proxy mode
E. cloud-proxy public mode
F. external mode

Answer: CD

NEW QUESTION 496
- (Exam Topic 3)
A client computerat10.10.7.14 is trying to access a Linux server (11.0.1.9)that is running a Tomcat Server 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

A.

Answer: A

NEW QUESTION 499
- (Exam Topic 3)
Which of the following is true regarding ASA clustering requirements?

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 can have different amount of flash memory

Answer: F

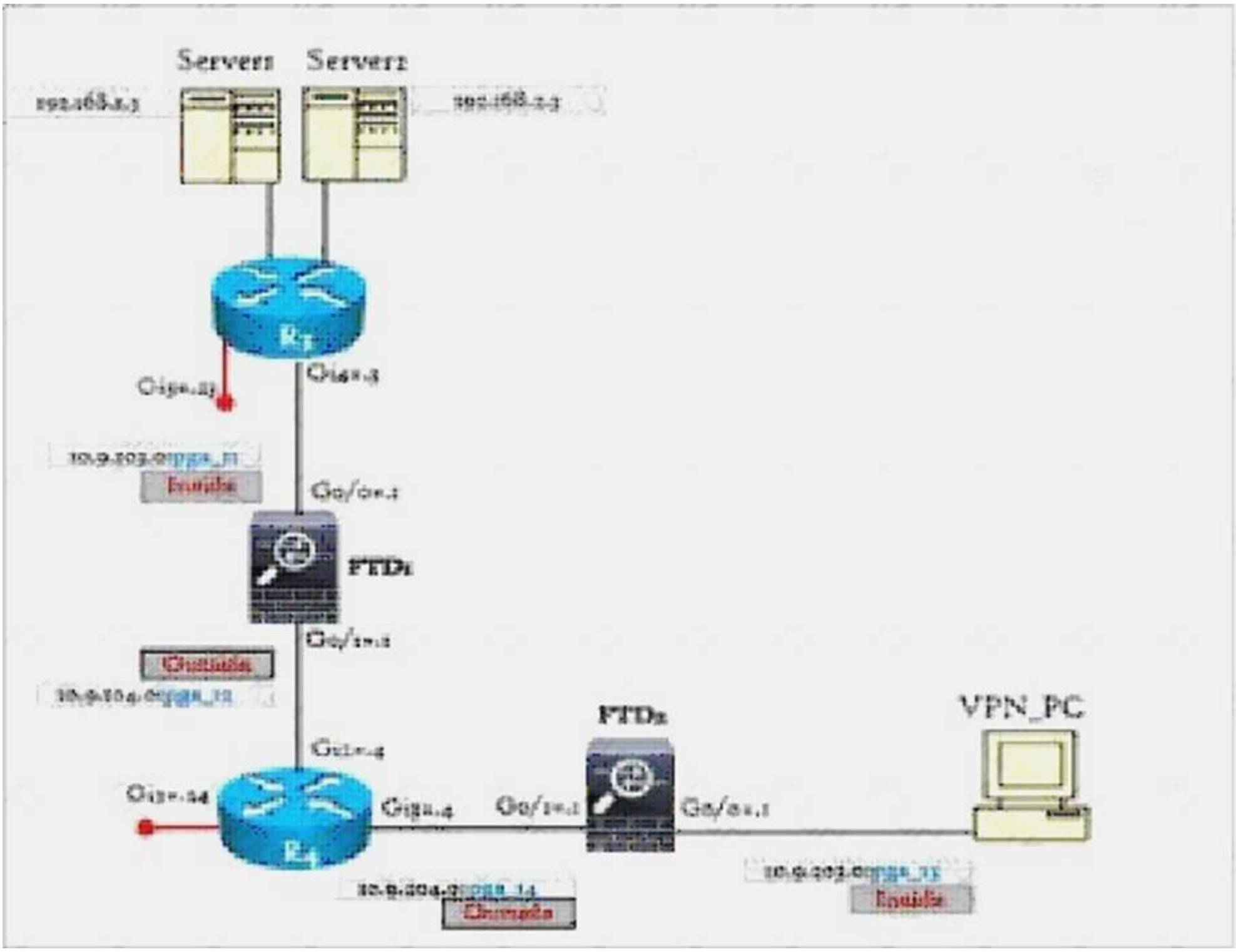
NEW QUESTION 500
- (Exam Topic 3)
Which statement correctly describes 3DES encryption algorithm?

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 505
- (Exam Topic 3)
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 510
- (Exam Topic 3)
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 511

- (Exam Topic 3)
Which description of a Botnet attack is true ?

A. It can be used to participate in DDOS
B. It is from a wireless attack where the attacker installs an access point to create backdoor to a network
C. It is launched by collection of non compromised 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 from of a fragmentation attack to evade an intrusion prevention security device
F. It is a from of a man-in-the-middle attack where the compromised machine is controlled remotely

Answer: A

NEW QUESTION 516
- (Exam Topic 3)
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 517
- (Exam Topic 3)
Which two options can be used to further harden a Cisco Email Security Appliance? (Choose two.)

A. Disable telnet
B. Rename the default administrator password
C. Disable HTTP and FTP services that are not required
D. Enable Cisco Discovery Protocol
E. Turn off TCP small services

Answer: AB

NEW QUESTION 518
- (Exam Topic 3)
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 522
- (Exam Topic 3)
Which statement about SenderBase reputation scoring on an ESA device is true?

A. Application traffic from known bad sites can be throttled or blocked
B. By default, all messages with a score below zero are dropped or throttled
C. MAil with scores in the medium range can be automatically routed for antimalware scanning
D. You can configure a custom score threshold for whitelisting messages
E. A high score indicates that a message is very likely to be spam
F. Sender reputation scores can be assigned to domains, IP addresses, and MAC addresses

Answer: D

NEW QUESTION 525
- (Exam Topic 3)
Which statement about the Sender Base functionality is true?

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

Answer: A

NEW QUESTION 528
- (Exam Topic 3)
If multiple contexts share an ingress interface, which would be the criteria used by ASA for packet classification?

A. Destination IP address
B. ASA ingress interface IP address
C. ASA ingress interface unique MAC address
D. ASA NAT configuration
E. Policy based routing on ASA
F. ASA egress interface IP address
G. Destination MAC address

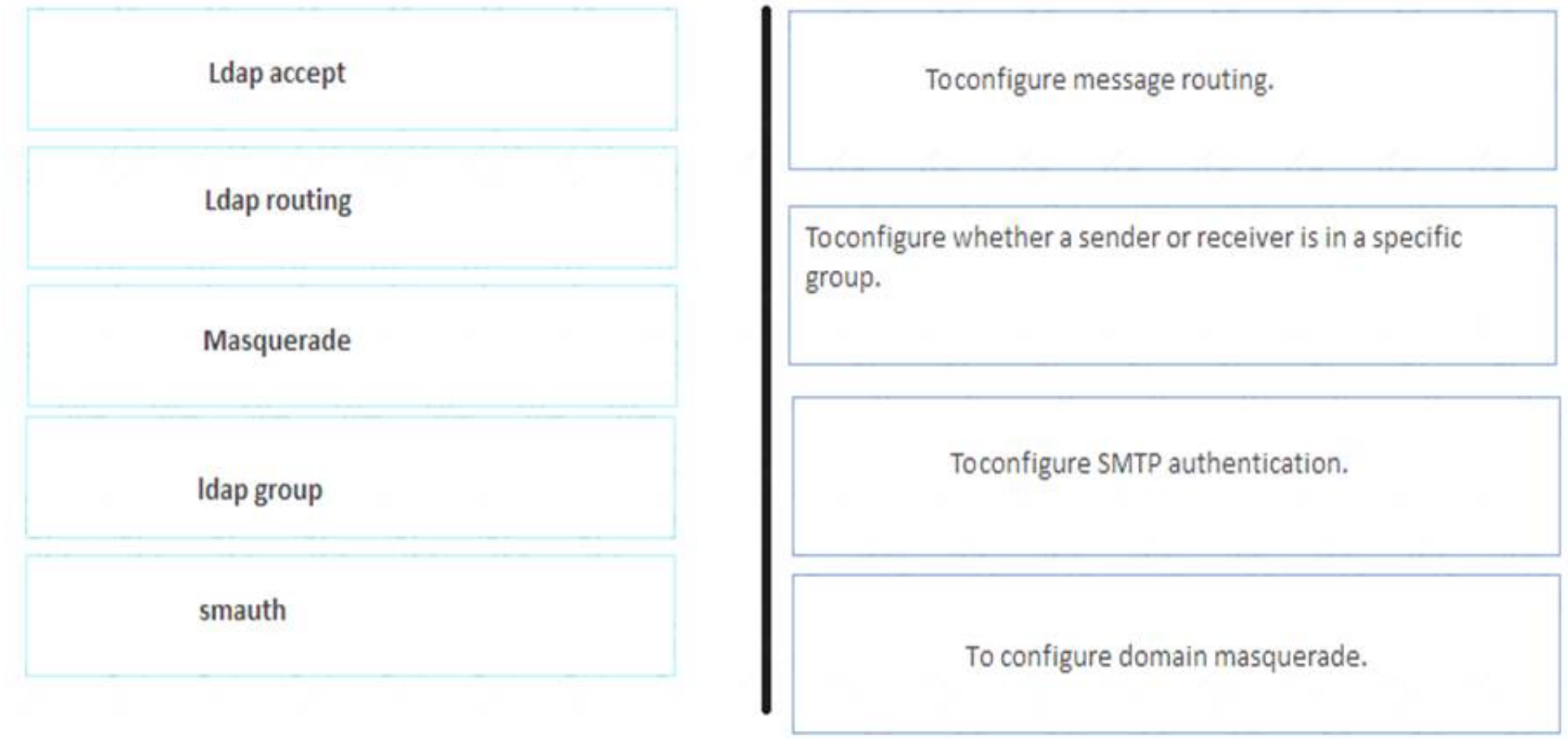
Answer: C

NEW QUESTION 532
- (Exam Topic 3)
Which statement about zone-based policy firewall implementation is true?

A. All the interfaces of the device cannot be the part of a same zone
B. By default, traffic between the interfaces in the same zone is allowed
C. An interface can be member of multiple one zones
D. If default zone is enabled, then traffic from zone interface to non-zone interface is dropped
E. A zone pair cannot have a zone as both source and destination
F. If an interface belong to a zone, then the traffic to and from that interface is always allowed

Answer: B

NEW QUESTION 537
- (Exam Topic 3)
Drag LDAP queries used by ESA to query LDAP server on the left to its functionality on the right.



A. Mastered
B. Not Mastered

Answer: A

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

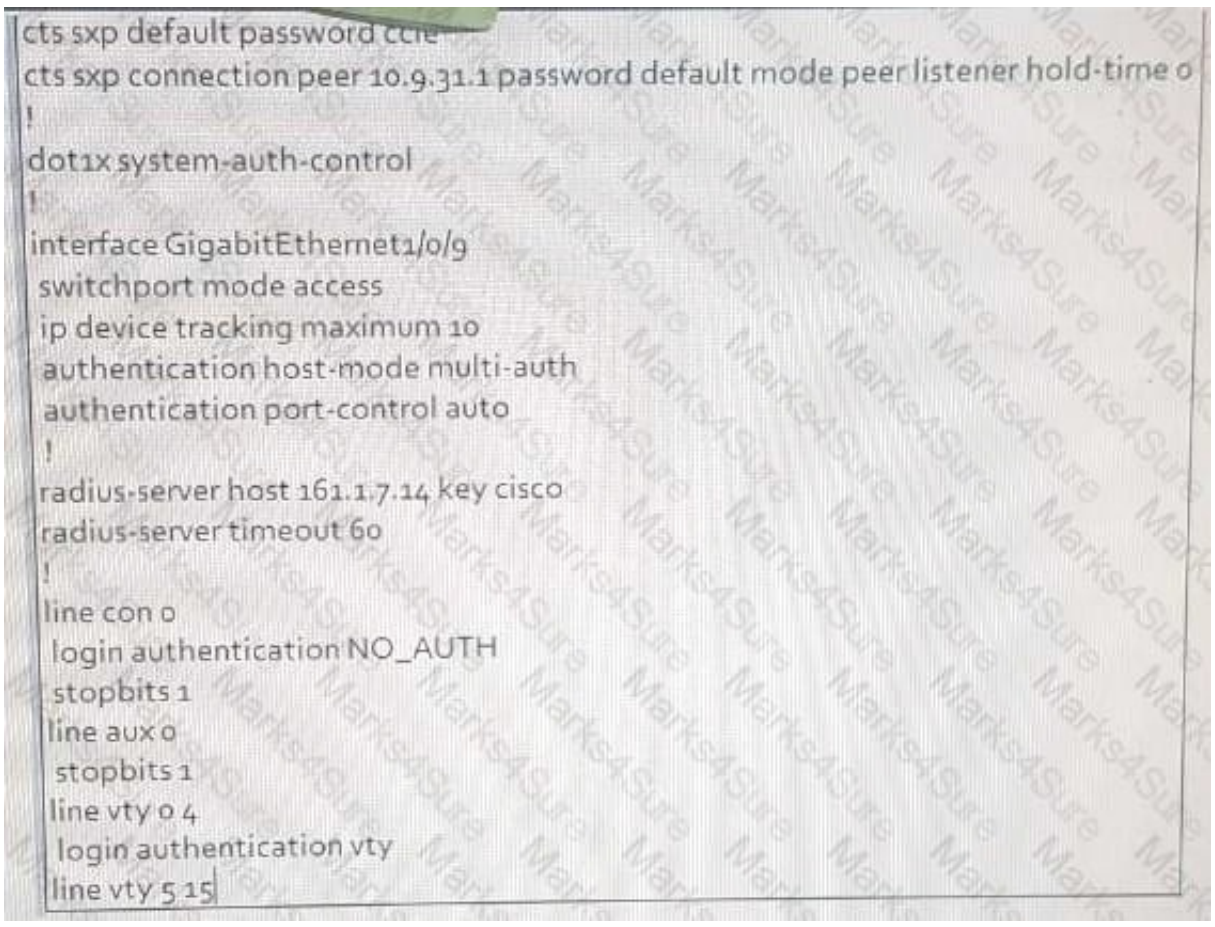
NEW QUESTION 540
- (Exam Topic 3)
Your organization is deploying an ESA for email security for inbound and outbound email. To receive inbound emails from external organizations, you must set up your DNS servers with the appropriate records so that the sending email server can determine which email gateway 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 543
- (Exam Topic 3)
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 548
- (Exam Topic 3)
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 550
- (Exam Topic 3)
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 553
- (Exam Topic 3)
Which statement is true about the traffic substitution and insertion attack?

A. It is a form of pivoting in the network
B. It only works with FTP session
C. It is a form of DoS attack
D. It is an evasion technique
E. It is a form of timing attack
F. It is used for reconnaissance

Answer: D

NEW QUESTION 556
- (Exam Topic 3)
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 557
- (Exam Topic 3)
Which LDAP query is used by ESA to authenticate users logging into an appliance?

A. chain queries
B. spam quarantine end-user authentication
C. group queries
D. acceptance query
E. spam quarantine alias consolidation
F. external authentication
G. SMTP authentication
H. certificate authentication

Answer: F

NEW QUESTION 561
- (Exam Topic 3)
Refer to the exhibit. interface GigabitEthernet0/0 nameif outside
security-level 0
ip address 20.1.2.1 255.255.255.0
!i
nterface GigabitEthernet0/1 nameif inside
security-level 100
ip address 10.1.22.1 255.255.255.0
!i
nterface Management0/0 management-only nameif mgmt
security-level 100
ip address 150.1.7.55 255.255.255.0
!
access-list
ccieacls webtype permit url http://server.cisco.com:80 log default
!c
rypto ca trustpoint ccietrust enrolment self
subject-name CN=ASA2 serial-number
keypair cciekey crl configure
!s
sl trust-point ccietrust outside
!d
ns domain-lookup inside
dns server-group DefaultDNS name-server 150.1.7.100 domain-name cisco.com
!g
roup-policy cciegroup internal group-policy ciegroup attributes banner value CCIE Written!
vpn-tunnel-protocol ssl-clientless webvpn
url-list value servers filter value ccieacls
!t
unnel-group ccietunnel type remote-access tunnel-group ccietunnel general-attributes
default-group-policy cciegroup
!w ebvpn
enable outside
tunnel-group-list enable
!c
rypto ikev2 remote-access trustpoint ccietrust dynamic-access-policy-record DfltAccessPolicy
username ccie password mflDmeWbPK0tCAwZ encrypted username ccie attributes
service-type remote-access
ASA2 is configured for the clientless SSL VPN connection with DNS server at

150.1.7.200 that is reachable only from the Management0/0 interface. The incoming VPN session will be received on outside interface with authentication credentials Username: ccie, Password: ccie. ASA 2 is configured for the self-signed certificate with trustpoint "ccietrust" enabled for the outside interface. It has been reported that resources accessibility is timing out after the VPN connection establishment. What could be the reason?

A. The CA trustpoint "ccietrust" has incorrect keypair
B. The tunnel group is tied up with the incorrect group policy
C. Webvpn needs to be enabled on the management interface
D. Management interface has incorrect security level configured
E. The "ccieacl" should be configured for port 443
F. The domain-lookup should be performed from management interface
G. Incorrect banner value in the group policy

Answer: F

NEW QUESTION 565
- (Exam Topic 3)
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 569
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 400-251 Exam with Our Prep Materials Via below:

https://www.certleader.com/400-251-dumps.html