Version: 39.1

Question: 1

Which two statements about Network Edge Authentication Technology (NEAT) are true? (Choose two.)

A. It can be configured on both access ports and trunk ports.
B. It allows you to configure redundant links between authenticator and supplicant switches
C. It can be configured on both access ports and EtherChannel ports.
D. It supports port-based authentication on the authenticator switch.
E. It conflicts with auto-configuration
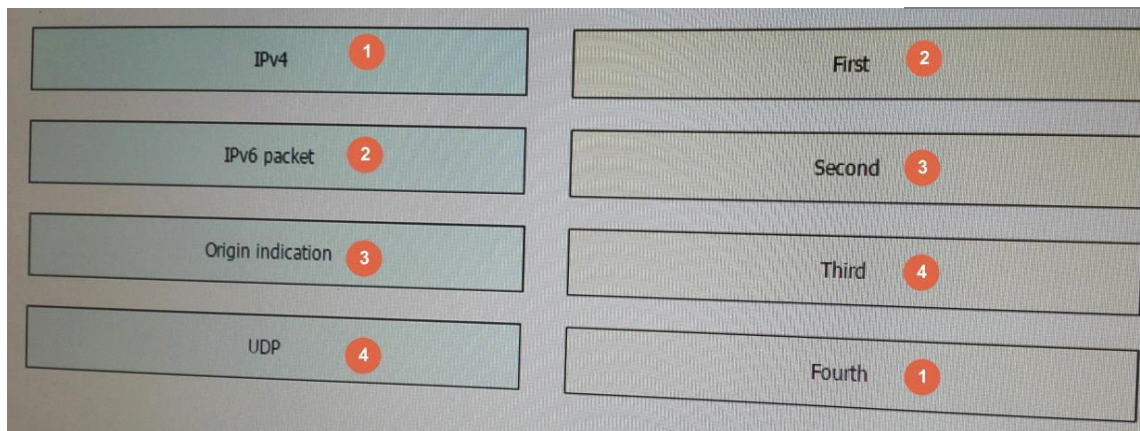F. It requires a standard ACL on the switch port.

Answer: AD

Question: 2

DRAG DROP
Drag and drop the components of a Teredo IPv6 packet from the left to the correct position in the packet on the right
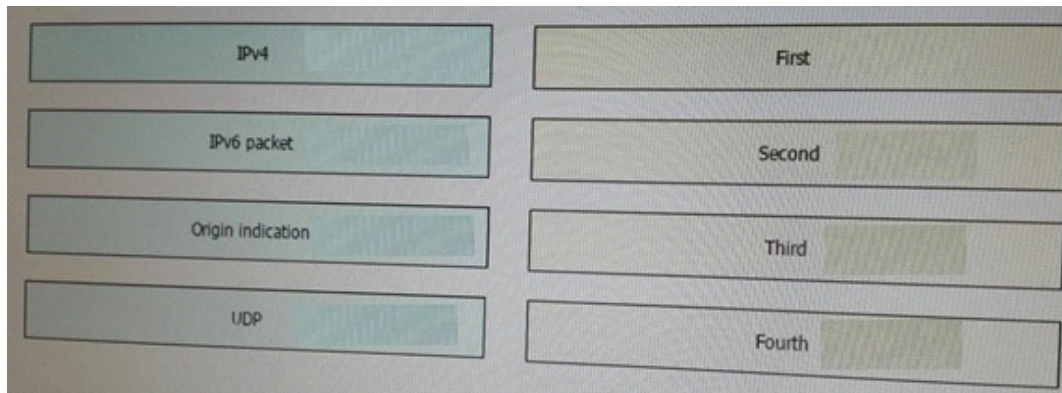
Answer:

Question: 3

Which option describes the purpose of the RADIUS VAP-ID attribute?

A. It sets the minimum bandwidth for the connection.
B. It identifies the VLAN interface to which the client will be associated.
C. It specifies the WLAN ID of the wireless LAN to which the client belongs.
D. It sets the maximum bandwidth for the connection.
E. It specifies the ACL ID to be matches against the client.
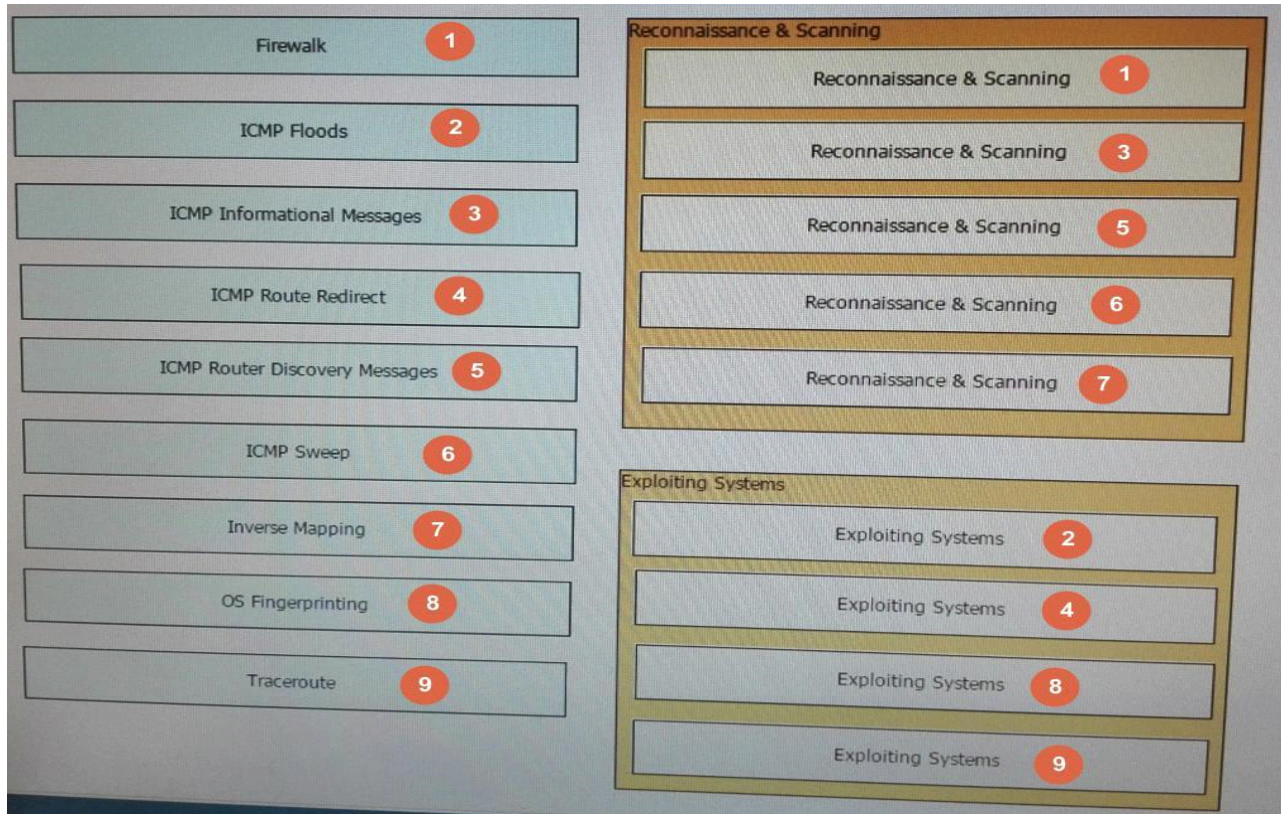F. It specifies the priority of the client.

Answer: C

Question: 4

DRAG DROP
Drag each attack type on the left to the matching attack category on the right.

Firewalk	Reconnaissance & Scanning
	Reconnaissance & Scanning
ICMP Floods	Reconnaissance & Scanning
	Reconnaissance & Scanning
ICMP Informational Messages	Reconnaissance & Scanning
	Reconnaissance & Scanning
ICMP Route Redirect	Reconnaissance & Scanning
ICMP Router Discovery Messages	Reconnaissance & Scanning
ICMP Sweep	
	Exploiting Systems
Inverse Mapping	Exploiting Systems
	Exploiting Systems
OS Fingerprinting	Exploiting Systems
	Exploiting Systems
Traceroute	Exploiting Systems
	Exploiting Systems

Answer:

Firewall **1**	Reconnaissance & Scanning	
	Reconnaissance & Scanning **1**	
ICMP Floods **2**	Reconnaissance & Scanning **3**	
ICMP Informational Messages **3**	Reconnaissance & Scanning **5**	
ICMP Route Redirect **4**	Reconnaissance & Scanning **6**	
ICMP Router Discovery Messages **5**	Reconnaissance & Scanning **7**	
ICMP Sweep **6**	**Exploiting Systems**	
Inverse Mapping **7**	Exploiting Systems **2**	
OS Fingerprinting **8**	Exploiting Systems **4**	
Traceroute **9**	Exploiting Systems **8**	
	Exploiting Systems **9**	

Question: 5

Which of the following Cisco IPS signature engine has relatively high memory usage?

A. The STRING-TCP engine
B. The NORMALIZER engine
C. The STRING-UDP engine
D. The STRING-ICMP engine

Answer: B

Question: 6

ASA v9.2 new feature

A. not possible to point to null0
B. support for policy based routing with route-map
C. backup ASA does ospf neighbor

Answer: A

Question: 7

When you configure ip-port-map http port 8080. What would be the output?

A)

```
R1#sh ip port-map  | i http
Default mapping:  http            tcp port 80           system defined
Default mapping:  http            tcp port 8080         user defined
Default mapping:  https           tcp port 443          system defined
R1#
```

B)

```
R1#sh ip port-map  | i http
Default mapping:  http            tcp port 80           system defined
Default mapping:  http            tcp port 8080         user defined
Default mapping:  http            tcp port 8081         user defined
Default mapping:  https           tcp port 443          system defined
R1#
```

C)

```
R1#sh ip port-map  | i http
Default mapping:  http            tcp port 80           system defined
Default mapping:  http            tcp port 8080         user defined
Default mapping:  http            tcp port 8081         user defined
Default mapping:  http            tcp port 8008         user defined
Default mapping:  https           tcp port 443          system defined
R1#
```

A. Exhibit A
B. Exhibit B
C. Exhibit C

Answer: A

Question: 8

OSPFv3 mechanism of authentication? (choose two)

A. AH
B. ESP
C. MD5
D. SHA
E. IP
F. GRE

Answer: CD

Question: 9

WPA 2 with CCMP encryption? (choose three)

A. AES Counter Mode is a block cipher that encrypts 128-bit blocks of data at a time with a 128-bit encryption key
B. AES Counter Mode is a block cipher that encrypts 256-bit blocks of data at a time with a 256-bit encryption key
C. it encrypt all traffic from the AP to the host

D. The CCMP algorithm produces a message integrity code (MIC) that provides data origin authentication and data integrity for the wireless frame.
E. CCMP is also referred to as CBC-IN-MAC.

Answer: ACD

Question: 10

same security level interface inter-traffic communication.

A. asa support 101 security level and mort than 101 interface (include sub-interface)
B. ASA can assign different interface to the same security level
C. by default, same security level port inter-traffic is not allowed
D. ASA should activate inter-interface communication by default

Answer: ABC

Question: 11

DRAG DROP
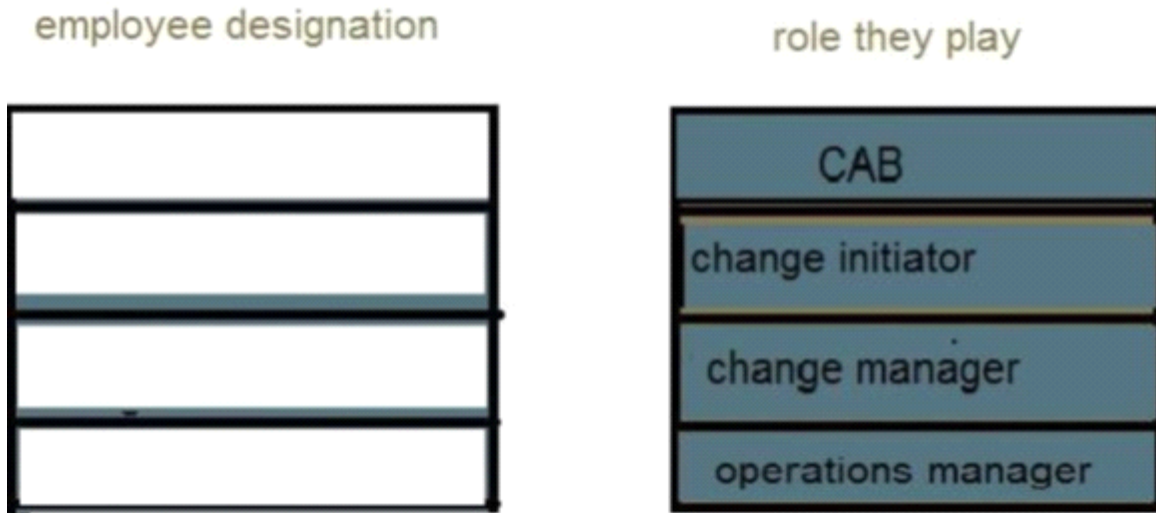Drag the employee designation to right on role they play.

employee designation

role they play

| change initiator |
| operations manager |
| change manager |
| CAB |

| approve change request |
| submit RFC |
| change review & auditing compling change metrics |
| implement change |

Answer:

employee designation

role they play

	CAB
	change initiator
	change manager
	operations manager

There are four major roles involved with the change management process, each with separate and distinct responsibilities. In the order of their involvement in a normal change, the roles are:

• Change initiator: The change initiator is the person who initially perceives the need for the change and develops, plans, and executes the steps necessary to meet the initial requirements for a Request for Change (RFC). like product manager, network architect, network engineer, service manager, security manager or support tier 1,2,3

• Change manager: Larger organizations require a dedicated change manager who is responsible for all changes

• Updating and communicating change procedures

• Leading a team to review and accept completed change requests with a focus on higher-risk changes

• Managing and conducting periodic change review meetings

• Compiling and archiving change requests

• Auditing network changes to ensure that:

– Change was recorded correctly with work matching the RFC

– Change had appropriate risk level

– Configuration items were updated appropriately

– Documentation was updated appropriately

• Change communication and notification

• Managing change postmortems

• Creating and compiling change management metrics

• Change advisory board: The change advisory board (CAB) is a body that exists to support the authorization of changes and to assist change management in the assessment and prioritization of changes. When a CAB is convened, members should be chosen who are capable of ensuring that all changes within the scope of the CAB are adequately assessed from both a business and a technical viewpoint.

The CAB may be asked to consider and recommend the adoption or rejection of changes appropriate for higher-level authorization and then recommendations will be submitted to the appropriate change authority.

Potential members include:

 Customers

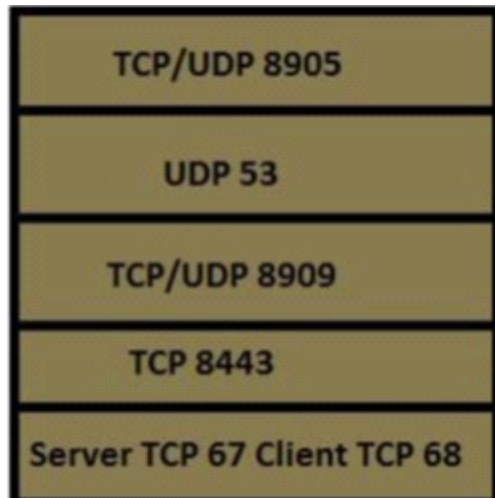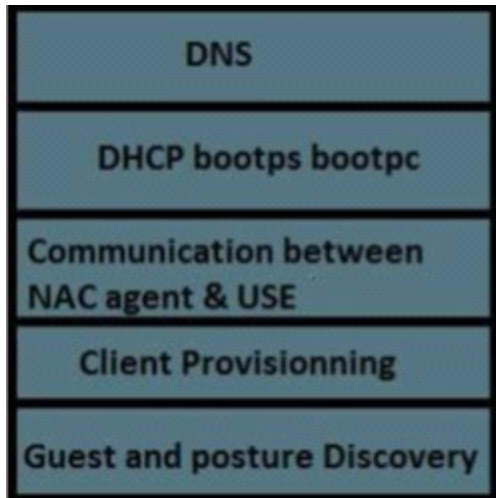 User managers

 User group representatives

Applications developers/maintainers

Specialists/technical consultants

Services and operations staff, such as service desk, test management, continuity management, security, and capacity

Facilities/office services staff (where changes may affect moves/accommodation and vice versa)

Contractors' or third parties' representatives, in outsourcing situations, for example

Other parties as applicable to specific circumstances (such as marketing if public products are affected).
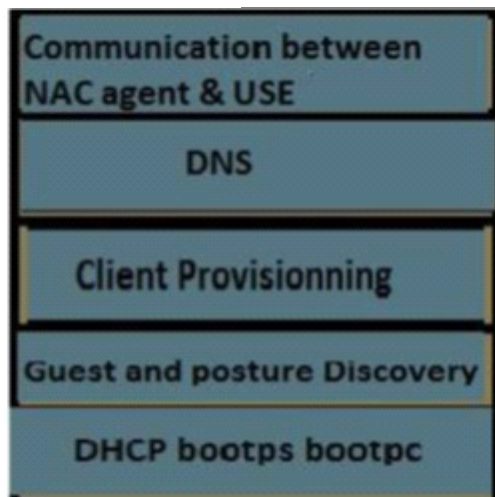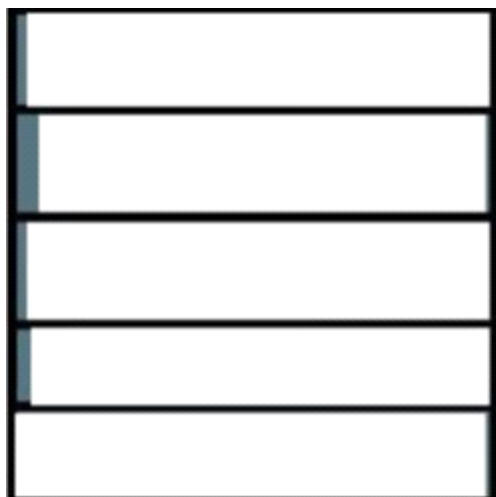
• Change implementation team (operations)

http://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-458050.html

Question: 12

DRAG DROP

Drag from left to right on correct action.

DNS
DHCP bootps bootpc
Communication between NAC agent & USE
Client Provisionning
Guest and posture Discovery

TCP/UDP 8905
UDP 53
TCP/UDP 8909
TCP 8443
Server TCP 67 Client TCP 68

Answer:

Communication between NAC agent & USE
DNS
Client Provisionning
Guest and posture Discovery
DHCP bootps bootpc

Question: 13

Two routers are trying to establish an OSPFv3 adjacency over an Ethernet link, but the adjacency is not forming. Which two options are possible reasons that prevent OSPFv3 to form between these two routers? (Choose two.)

A. mismatch area types
B. mismatch of subnet masks
C. mismatch of network types
D. mismatch of authentication types
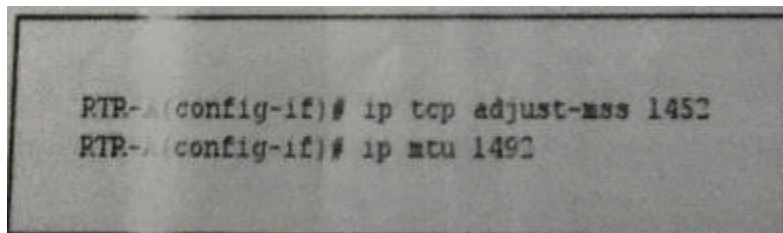E. mismatch of instance IDs

Answer: AE

Question: 14

 The computer at 10.10.10.4 on your network has been infected by a bontnet that directs traffic to a malware site at 168.65.201.120 Assuming that filtering will be performed on a Cisco ASA,What command can you use to block all current and future connections from the infected host?

A. ip access-list extended BLOCK_BOT_OUT deny ip any host 10.10.10.4
B. shun 168.65.201.120 10.10.10.4 6000 80
C. ip access-list extended BLOCK_BOT_OUT deny ip host 10.10.10.4 host 168.65.201.120
D. shun 10.10.10.4 68.65.201.120 6000 80

Answer: B

Question: 15

Refer to the exhibit.


```
RTR- (config-if)# ip tcp adjust-mss 1452
RTR- (config-if)# ip mtu 1492
```
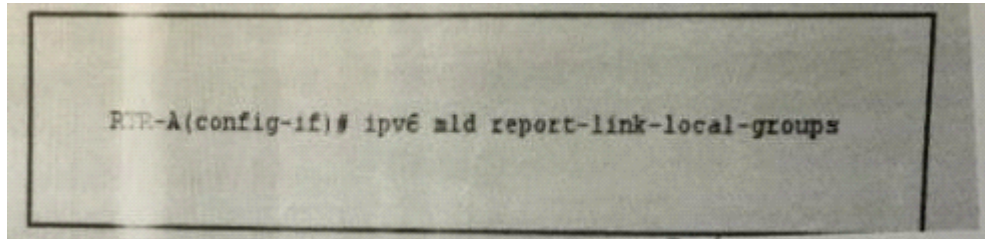
Which effect of this configuration is true?

A. The MSS of TCP SYN packets is set to 1452 bytes and the IP MTU of the interface is set to 1942 bytes
B. The maximum size of TCP SYN+ACK packets passing the transient host is set to 1452 bytes and the IP MTU of the interface is set to 1492 bytes
C. The PMTUD values sets itself to 1452 bytes when the interface MTU is set to 1492 bytes
D. SYN packets carries 1452 bytes in the payload when the Ethernet MTU of the interface is to 1492 bytes
E. The maximum size of TCP SYN+ACK packets passing the router is set to 452 bytes and the IP MTU of the interface is set to 1492 bytes

Answer: A

Question: 16

Refer to the exhibit.


```
RTR-A(config-if)# ipv6 mld report-link-local-groups
```

Which effect of this configuration is true?

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

Answer: C

Question: 17

You have configured an ASA firewall in multiple context mode. If the context are sharing an Interface. What are two of the actions you could take to classify packets to the appropriate Context?(Choose two)

A. Enable DHCP
B. Disable MAC auto-generation and adding unique IP addresses to each interface
C. Enable MAC auto-generation globally
D. Assign a unique MAC address to each interface
E. Apply QoS to each interface

Answer: CD

Question: 18

Refer to the exhibit.

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

What is the effect of the given configuration?

A. It requires the enable password to be authorized by the LOCAL database
B. It allows users to log in with any user name in the LOCAL database
C. It enables management authorization for a user-authenticated RADIUS server
D. Users will be authenticated against the RADIUS servers defined in the adm_net list
E. It allows SSH connections to console login into the ASA

Answer: D

Question: 19

What feature enables extended secure access form non-secure physical locations?

A.NEAT
B.802.1X port-based authentication
C.port security
D.storm-control
E.CBAC

Answer: A

Question: 20

What are the two technologies that support AFT?(Choose two)

A.NAT-6to 4
B.NAT-PT
C.DNAT
D.NAT64
E.NAT-PMP
F.SNAT

Answer: BD

Thank You For Trying 350-018 PDF Demo

To try our 350-018 Premium Files visit link below:

https://examsland.com/latest-exam-questions/350-018/

Start Your 350-018 Preparation

Use Coupon EL25 for extra 25% discount on the purchase of Practice Test Software.