Vendor: Cisco

Exam Code: 210-260

Exam Name: Implementing Cisco IOS Network Security (IINS v3.0) Exam

Version: 19.021

Important Notice

Product

Our Product Manager keeps an eye for Exam updates by Vendors. Free update is available within One year after your purchase.

You can login member center and download the latest product anytime. (Product downloaded from member center is always the latest.)

PS: Ensure you can pass the exam, please check the latest product in 2-3 days before the exam again.

Feedback

We devote to promote the product quality and the grade of service to ensure customers interest.

If you have any questions about our product, please provide Exam Number, Version, Page Number, Question Number, and your Login Account to us, please contact us at support@passleader.com and our technical experts will provide support in 24 hours.

Copyright

Order ID: **********

PayPal Name: **********

PayPal ID: **********

QUESTION 1
Which statement about communication over failover interfaces is true?

A. All information that is sent over the failover interface is sent as clear text, but the stateful failover link is encrypted by default.
B. All information that is sent over the failover and stateful failover interfaces is encrypted by default
C. All information that is sent over the failover and stateful failover interfaces is sent as clear text by default
D. Usernames, password and preshared keys are encrypted by default when they are sent over the failover and stateful failover interfaces, but other information is sent as clear text

Answer: C

QUESTION 2
Which three ESP fields can be encrypted during transmission? (Choose three)

A. Security Parameter Index
B. Sequence Number
C. MAC Address
D. Padding
E. Pad Length
F. Next Header

Answer: DEF

QUESTION 3
According to Cisco best practices, which three protocols should the default ACL allow an access port to enable wired BYOD devices to supply valid credentials and connect to the network? (Choose three)

A. BOOTP
B. TFTP
C. DNS
D. MAB
E. HTTP
F. 802.1x

Answer: ABC

QUESTION 4
Refer to the exhibit. If a supplicant supplies incorrect credentials for all authentication methods configured on the switch, how will the switch respond?

```
authentication event fail action next-method
authentication event no-response action authorize vlan 101
authentication order mab dotlx webauth
authentication priority dotlx mab
authentication port-control auto
dotlx pae authenticator
```

A. The switch will cycle through the configured authentication methods indefinitely
B. The supplicant will fail to advance beyond the webauth method.
C. The authentication attempt will time out and the switch will place the port into the unathorized state
D. The authentication attempt will time out and the switch will place the port into VLAN 101

Answer: B

QUESTION 5
Which SOURCEFIRE logging action should you choose to record the most detail about a connection.

A. Enable logging at the beginning of the session
B. Enable logging at the end of the session
C. Enable alerts via SNMP to log events off-box
D. Enable eStreamer to log events off-box

Answer: B

QUESTION 6
What type of algorithm uses the same key to encryp and decrypt data?

A. a symmetric algorithm
B. an asymetric algorithm
C. a Public Key infrastructure algorithm
D. an IP Security algorithm

Answer: A

QUESTION 7
If a packet matches more than one class map in an individual feature type's policy map, how does the ASA handle the packet?

A. The ASA will apply the actions from only the most specific matching class map it finds for the feature type
B. The ASA will apply the actions from all matching class maps it finds for the feature type
C. The ASA will apply the actions from only the last matching class map it finds for the feature type.
D. The ASA will apply the actions from only the first matching class map it finds for the feature type.

Answer: D

QUESTION 8
You have implemented a Sourcefire IPS and configured it to block certain addresses utilizing Security Intelligence IP address Reputation. A user calls and is not able to access a certain IP address. What action can you take to allow the user access to the IP address?

A. Create a custom blacklist to allow traffic
B. Create a whitelist and add the appropriate IP address to allow traffic.

C. Create a user based access control rule to allo the traffic.
D. Create a network based access control rule to allow the traffic.
E. Create a rule to bypass inspection to allow the traffic

Answer: B

QUESTION 9
Which EAP method uses protected Access Credentials?

A. EAP-TLS
B. EAP-PEAP
C. EAP-FAST
D. EAP-GTC

Answer: C

QUESTION 10
In which two situations should you use out-of-band management? (Choose two)

A. when a network device fails to forward packets
B. when management applications need concurrent access to the device
C. when you require ROMMON access
D. when you require administrator's access from multiple locations
E. when the control plane fails to respond

Answer: AC
Explanation:
OOB management is used for devices at the headquarters and is accomplished by connecting dedicated management ports or spare Ethernet ports on devices directly to the dedicated OOB management network hosting the management and monitoring applications and services. The OOB management network can be either implemented as a collection of dedicated hardware or based on VLAN isolation.
Source:
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg/chap9.html

QUESTION 11
What features can protect the data plane? (Choose three.)

A. policing
B. ACLs
C. IPS
D. antispoofing
E. QoS
F. DHCP-snooping

Answer: BDF
Explanation:
Data Plane Security
Data plane security can be implemented using the following features:

Access control lists
Access control lists (ACLs) perform packet filtering to control which packets move through the network and where.
Antispoofing
ACLs can be used as an antispoofing mechanism that discards traffic that has an invalid source address.
Layer 2 security features
Cisco Catalyst switches have integrated features to help secure the Layer 2 infrastructure.
ACLs
ACLs are used to secure the data plane in a variety of ways, including the following:
Block unwanted traffic or users
ACLs can filter incoming or outgoing packets on an interface, controlling access based on source addresses, destination addresses, or user authentication.
Reduce the chance of DoS attacks
ACLs can be used to specify whether traffic from hosts, networks, or users can access the network. The TCP intercept feature can also be configured to prevent servers from being flooded with requests for a connection.
Mitigate spoofing attacks
ACLs enable security practitioners to implement recommended practices to mitigate spoofing attacks.
Provide bandwidth control
ACLs on a slow link can prevent excess traffic.
Classify traffic to protect other planes
ACLs can be applied on vty lines (management plane).
ACLs can control routing updates being sent, received, or redistributed (control plane).
Antispoofing
Implementing the IETF best current practice 38 (BCP38) and RFC 2827 ingress traffic filtering renders the use of invalid source IP addresses ineffective, forcing attacks to be initiated from valid, reachable IP addresses which could be traced to the originator of an attack.
Features such as Unicast Reverse Path Forwarding (uRPF) can be used to complement the antispoofing strategy.
Layer 2 Data Plane Protection
The following are Layer 2 security tools integrated into the Cisco Catalyst switches:
Port security
Prevents MAC address spoofing and MAC address flooding attacks DHCP snooping
Prevents client attacks on the Dynamic Host Configuration Protocol (DHCP) server and switch
Dynamic ARP inspection (DAI)
Adds security to ARP by using the DHCP snooping table to minimize the impact of ARP poisoning and spoofing attacks
IP source guard
Prevents IP spoofing addresses by using the DHCP snooping table

QUESTION 12
How many crypto map sets can you apply to a router interface?

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

Answer: D

QUESTION 13

What is the transition order of STP states on a Layer 2 switch interface?

A. listening, learning, blocking, forwarding, disabled
B. listening, blocking, learning, forwarding, disabled
C. blocking, listening, learning, forwarding, disabled
D. forwarding, listening, learning, blocking, disabled

Answer: C
Explanation:
The ports on a switch with enabled Spanning Tree Protocol (STP) are in one of the following five port states.
Blocking
Listening
Learning
Forwarding
Disabled
A switch does not enter any of these port states immediately except the blocking state. When the Spanning Tree Protocol (STP) is enabled, every switch in the network starts in the blocking state and later changes to the listening and learning states.
Blocking State
The Switch Ports will go into a blocking state at the time of election process, when a switch receives a BPDU on a port that indicates a better path to the Root Switch (Root Bridge), and if a port is not a Root Port or a Designated Port.
A port in the blocking state does not participate in frame forwarding and also discards frames received from the attached network segment. During blocking state, the port is only listening to and processing BPDUs on its interfaces. After 20 seconds, the switch port changes from the blocking state to the listening state.
Listening State
After blocking state, a Root Port or a Designated Port will move to a listening state. All other ports will remain in a blocked state. During the listening state the port discards frames received from the attached network segment and it also discards frames switched from another port for forwarding. At this state, the port receives BPDUs from the network segment and directs them to the switch system module for processing. After 15 seconds, the switch port moves from the listening state to the learning state.
Learning State
A port changes to learning state after listening state. During the learning state, the port is listening for and processing BPDUs . In the listening state, the port begins to process user frames and start updating the MAC address table. But the user frames are not forwarded to the destination. After 15 seconds, the switch port moves from the learning state to the forwarding state.
Forwarding State
A port in the forwarding state forwards frames across the attached network segment. In a forwarding state, the port will process BPDUs , update its MAC Address table with frames that it receives, and forward user traffic through the port. Forwarding State is the normal state. Data and configuration messages are passed through the port, when it is in forwarding state.
Disabled State
A port in the disabled state does not participate in frame forwarding or the operation of STP because a port in the disabled state is considered non-operational.

QUESTION 14
Which sensor mode can deny attackers inline?

A. IPS
B. fail-close
C. IDS

D. fail-open

Answer: A

QUESTION 15
Which options are filtering options used to display SDEE message types?

A. stop
B. none
C. error
D. all

Answer: CD

QUESTION 16
When a company puts a security policy in place, what is the effect on the company's business?

A. Minimizing risk
B. Minimizing total cost of ownership
C. Minimizing liability
D. Maximizing compliance

Answer: A

QUESTION 17
Which wildcard mask is associated with a subnet mask of /27?

A. 0.0.0.31
B. 0.0.0.27
C. 0.0.0.224
D. 0.0.0.255

Answer: A

QUESTION 18
Which statements about reflexive access lists are true?

A. Reflexive access lists create a permanent ACE
B. Reflexive access lists approximate session filtering using the established keyword
C. Reflexive access lists can be attached to standard named IP ACLs
D. Reflexive access lists support UDP sessions
E. Reflexive access lists can be attached to extended named IP ACLs
F. Reflexive access lists support TCP sessions

Answer: DEF

QUESTION 19
Which actions can a promiscuous IPS take to mitigate an attack?

A. modifying packets
B. requesting connection blocking
C. denying packets
D. resetting the TCP connection
E. requesting host blocking
F. denying frames

Answer: BDE
Explanation:
Promiscuous Mode Event Actions
The following event actions can be deployed in Promiscuous mode. These actions are in affect for a user- configurable default time of 30 minutes. Because the IPS sensor must send the request to another device or craft a packet, latency is associated with these actions and could allow some attacks to be successful.
Blocking through usage of the Attack Response Controller (ARC) has the potential benefit of being able to perform to the network edge or at multiple places within the network.
Request block host: This event action will send an ARC request to block the host for a specified time frame, preventing any further communication. This is a severe action that is most appropriate when there is minimal chance of a false alarm or spoofing.
Request block connection: This action will send an ARC response to block the specific connection. This action is appropriate when there is potential for false alarms or spoofing.
Reset TCP connection: This action is TCP specific, and in instances where the attack requires several TCP packets, this can be a successful action. However, in some cases where the attack only needs one packet it may not work as well. Additionally, TCP resets are not very effective with protocols such as SMTP that consistently try to establish new connections, nor are they effective if the reset cannot reach the destination host in time.
Event actions can be specified on a per signature basis, or as an event action override (based on risk rating values ?event action override only). In the case of event action override, specific event actions are performed when specific risk rating value conditions are met. Event action overrides offer consistent and simplified management. IPS version 6.0 contains a default event action override with a deny-packet-inline action for events with a risk rating between 90 and 100. For this action to occur, the device must be deployed in Inline mode.
Protection from unintended automated action responses
Automated event actions can have unintended consequences when not carefully deployed. The most severe consequence can be a self denial of service (DoS) of a host or network. The majority of these unintended consequences can be avoided through the use of Event Action Filters, Never Block Addresses, Network spoofing protections, and device tuning. The following provides an overview of methods used to prevent unintended consequences from occurring.
Using Event Action Filters and Never Block
By using these capabilities, administrators may prevent a miscreant from spoofing critical IP addresses, causing a self inflicted DoS condition on these critical IP addresses. Note that Never Block capabilities only apply to ARC actions. Actions that are performed inline will still be performed as well as rate limiting if they are configured.
Minimize spoofing
Administrators can minimize spoofed packets that enter the network through the use of Unicast Reverse Path Forwarding. Administrators can minimize spoofing within their network through the use of IP Source Guard. The white paper titled Understanding Unicast Reverse Path Forwarding provides details on configuration of this feature. More information on IP Source Guard is available in the document titled Configuring DHCP Features and IP Source Guard.
Careful Use of Event Actions
By judicious use of event actions that block unwanted traffic, such as using the high signature fidelity rating, and not using automated actions on signatures that are easily spoofed, administrators can reduce the probability of an unintended result. For an event to have a high risk rating, it must have a high signature fidelity rating unless the risk rating is artificially increased

through the use of Target Value Rating or Watch List Rating, which are IP specific increases.
Tuning
By tuning the signature set to minimize false positive events, administrators can reduce the chance of an event action that has an unintended consequence.
High Base Risk Rating Events
In most cases, events with a high base risk rating or a high signature fidelity rating are strong candidates for automated event actions. Care should be taken with protocols that are easily spoofed in order to prevent self DoS conditions.

QUESTION 20
Which Cisco Security Manager application collects information about device status and uses it to generate notifications and alerts?

A. FlexConfig
B. Device Manager
C. Report Manager
D. Health and Performance Monitor

Answer: D
Explanation:
"Report Manager - Collects, displays and exports network usage and security information for ASA and IPS devices, and for remote-access IPsec and SSL VPNs. These reports aggregate security data such as top sources, destinations, attackers, victims, as well as security information such as top bandwidth, duration, and throughput users. Data is also aggregated for hourly, daily, and monthly periods." and
"Health and Performance Monitor (HPM) ?Monitors and displays key health, performance and VPN data for ASA and IPS devices in your network. This information includes critical and non-critical issues, such as memory usage, interface status, dropped packets, tunnel status, and so on. You also can categorize devices for normal or priority monitoring, and set different alert rules for the priority devices."

QUESTION 21
Which command is needed to enable SSH support on a Cisco Router?

A. crypto key lock rsa
B. crypto key generate rsa
C. crypto key zeroize rsa
D. crypto key unlock rsa

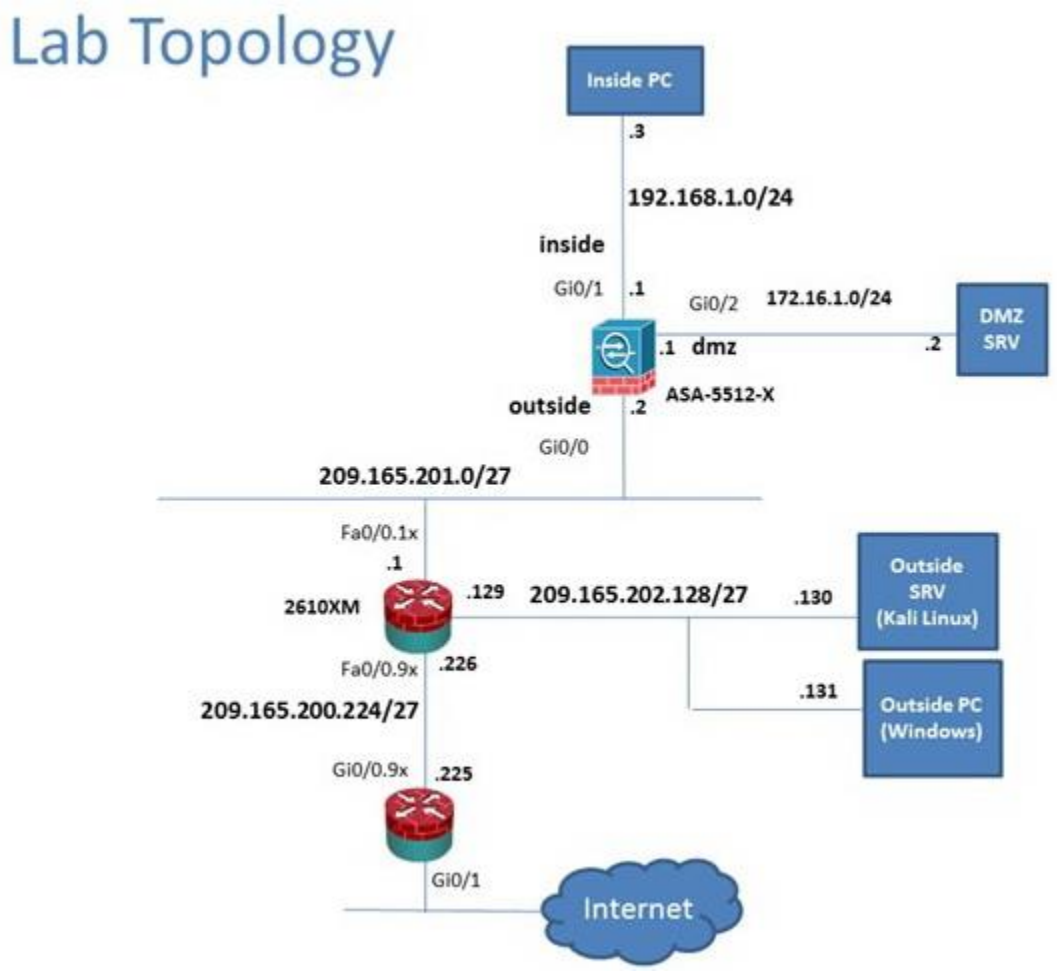
Answer: B

QUESTION 22
In which three ways does the TACACS protocol differ from RADIUS? (Choose three)

A. TACACS uses TCP to communicate with the NAS
B. TACACS can encrypt the entire packet that is sent to the NAS
C. TACACS authenticates and authorizes simultaneously, causing fewer packets to be transmitted
D. TACACS uses UDP to communicate with the NAS
E. TACACS encrypts only the password field in an authentication packet
F. TACACS support per-command authorization

Answer: ABF

QUESTION 23
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.
To access ASDM, click the ASA icon in the topology diagram.
Note: Not all ASDM functionalities are enabled in this simulation.
To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.

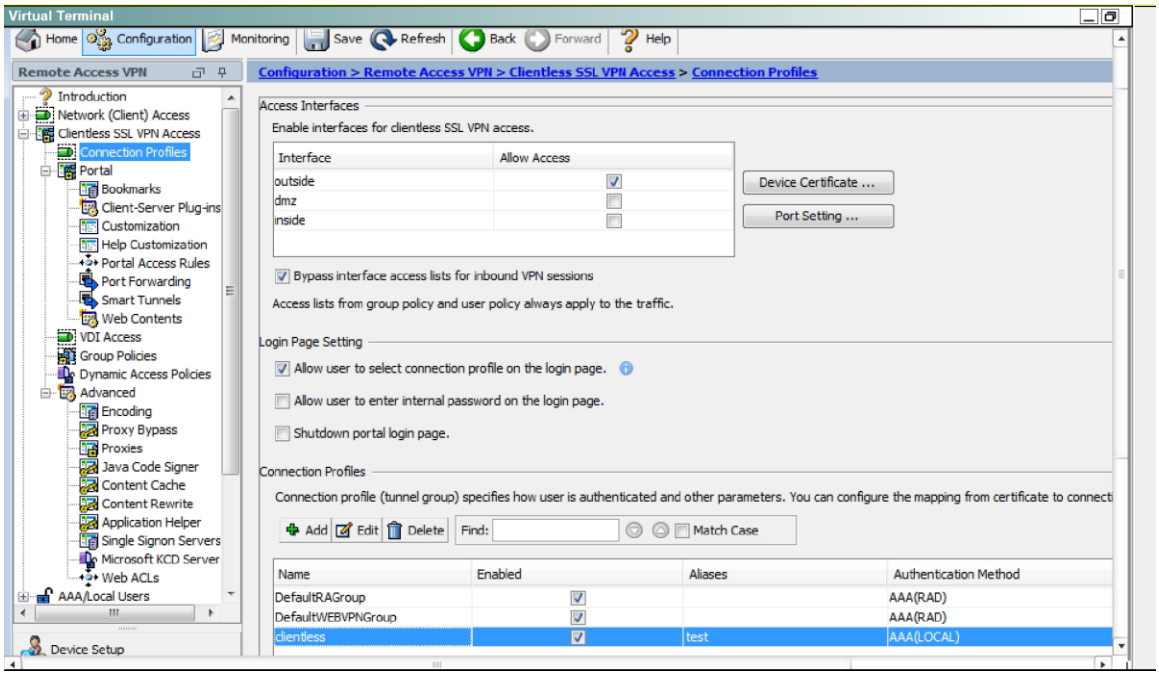


Which user authentication method is used when users login to the Clientless SSL VPN portal using https://209165.201.2/test?

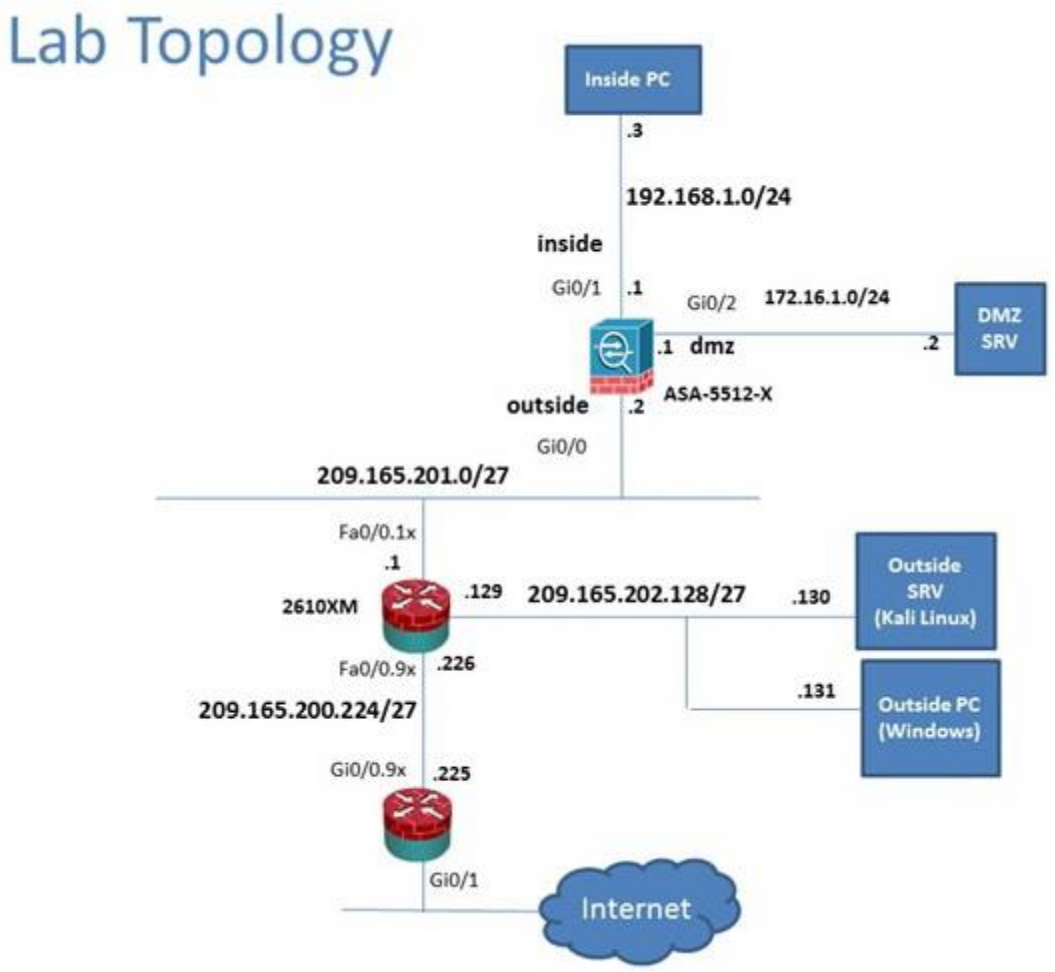
A. Both Certificate and AAA with LOCAL database
B. AAA with RADIUS server
C. Both Certificate and AAA with RADIUS server
D. AAA with LOCAL database
E. Certificate

Answer: D

Explanation:
This can be seen from the Connection Profiles Tab of the Remote Access VPN configuration, where the alias of test is being used.



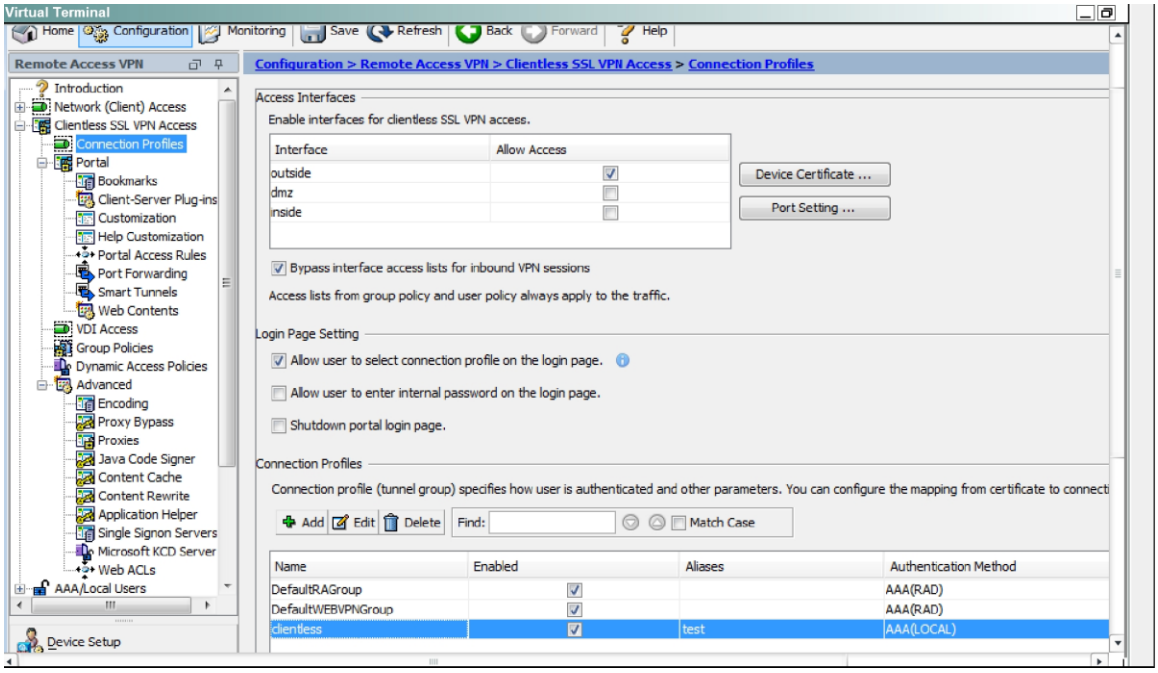
QUESTION 24
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.
To access ASDM, click the ASA icon in the topology diagram.
Note: Not all ASDM functionalities are enabled in this simulation.
To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.



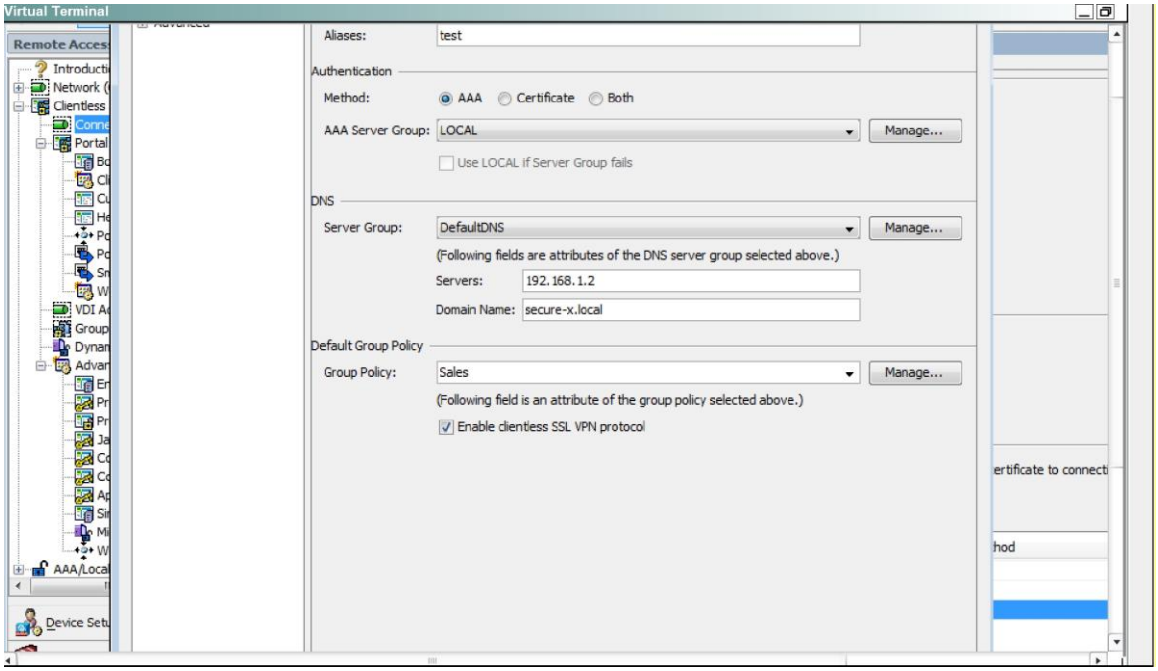
When users login to the Clientless SSL VPN using https://209.165.201.2/test, which group policy will be applied?

A. test
B. Sales
C. DefaultRAGroup
D. DefaultWEBVPNGroup
E. clientless
F. DFTGrpPolicy

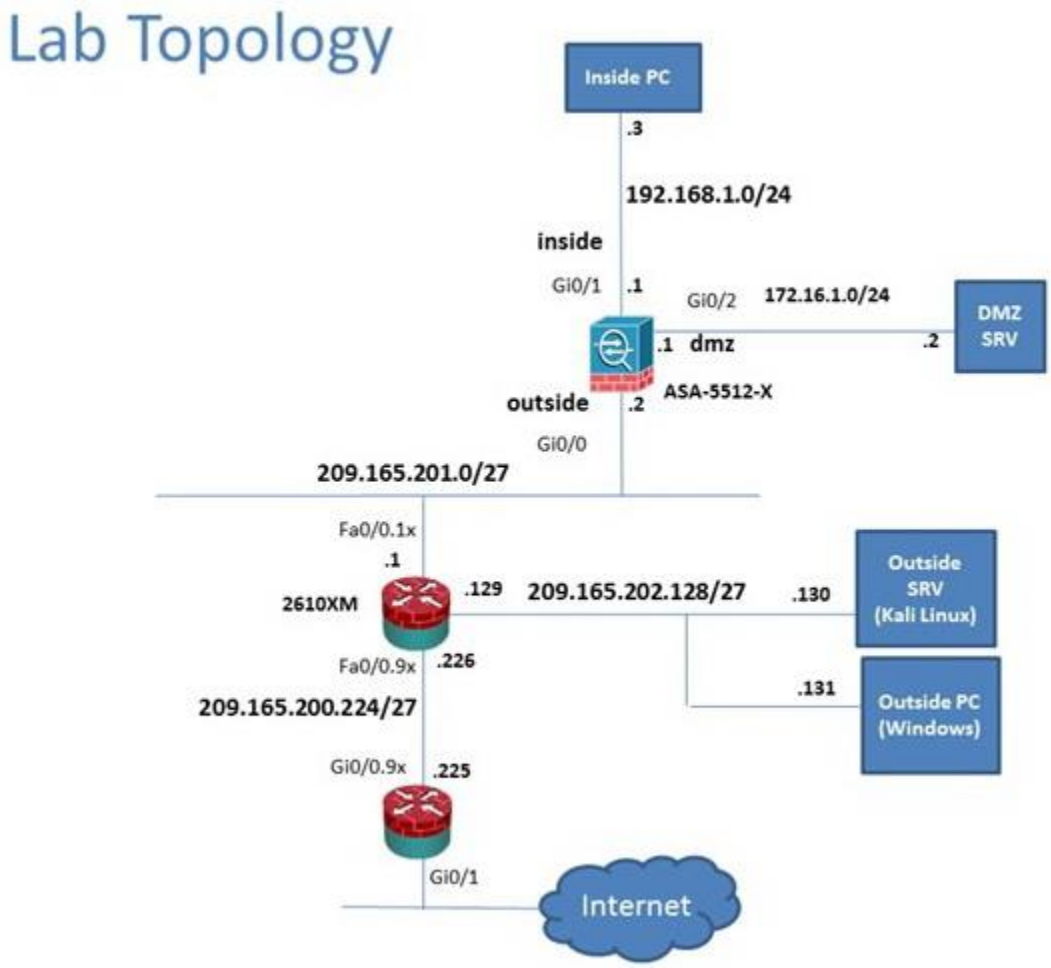
Answer: B
Explanation:
First navigate to the Connection Profiles tab as shown below, highlight the one with the test alias:



Then hit the “edit” button and you can clearly see the Sales Group Policy being applied.



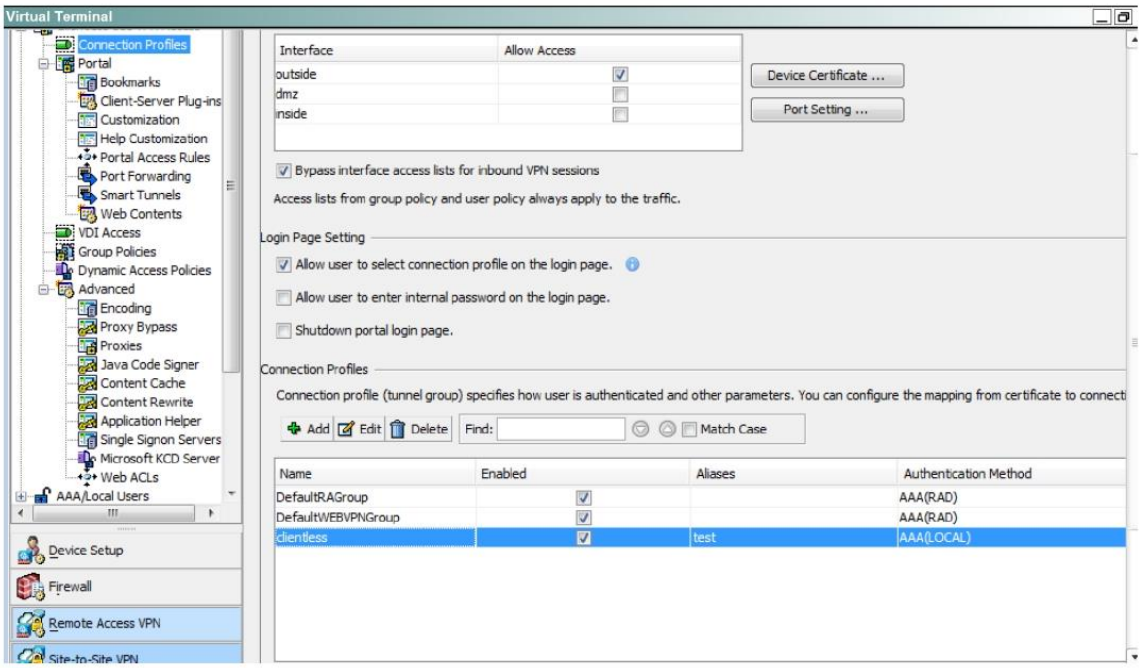
QUESTION 25
Scenario
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.
To access ASDM, click the ASA icon in the topology diagram.
Note: Not all ASDM functionalities are enabled in this simulation.
To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.



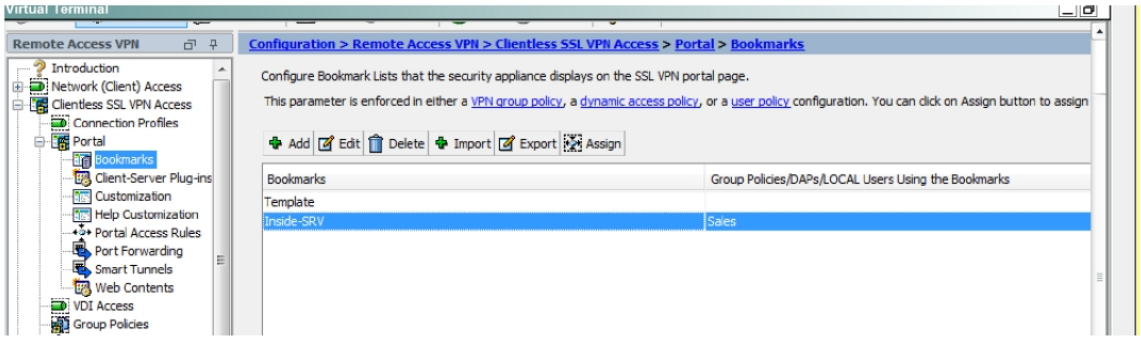
Which two statements regarding the ASA VPN configurations are correct? (Choose two)

A. The Inside-SRV bookmark has not been applied to the Sales group policy
B. The ASA has a certificate issued by an external Certificate Authority associated to the ASDM_Trustpoint1
C. The Inside-SRV bookmark references the https://10.x.x.x URL
D. Any Connect, IPSec IKEv1 and IPSec IKEv2 VPN access is enabled on the outside interface
E. Only Clientless SSL VPN VPN access is allowed with the Sales group Policy
F. The DefaultWEBVPNGroup Connection Profile is using the AAA with Radius server method

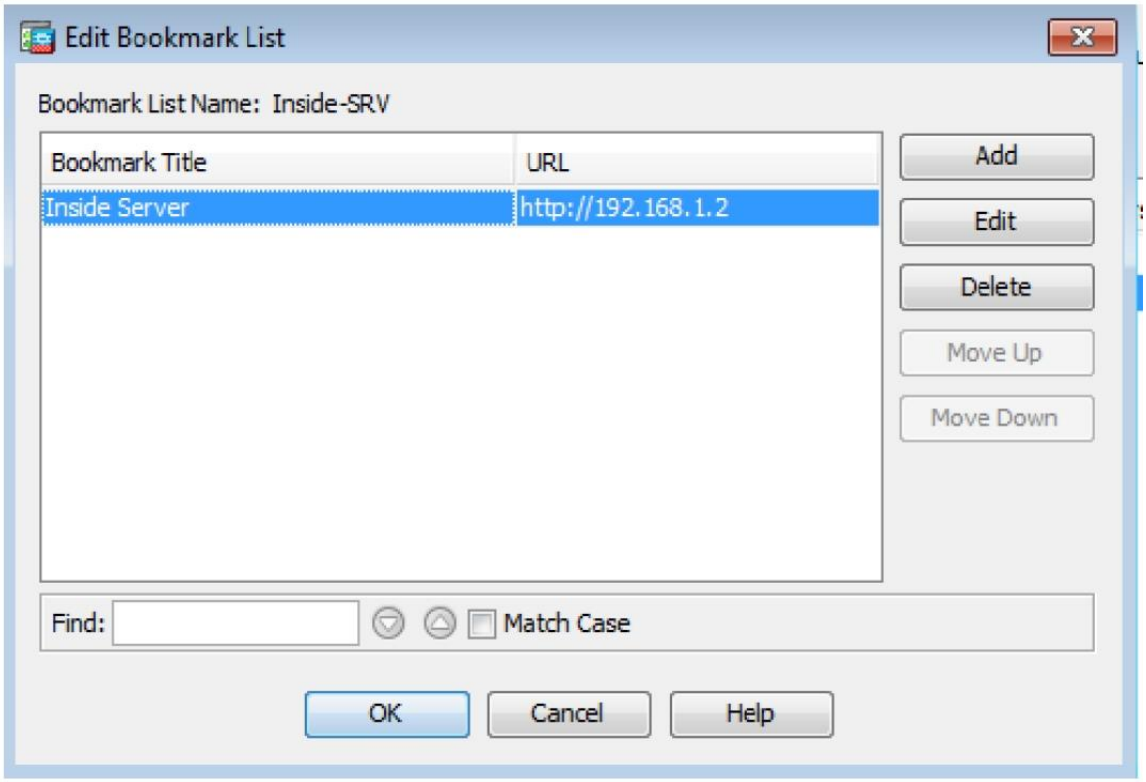
Answer: EF
Explanation:
For F:



Not C, Navigate to the Bookmarks tab:

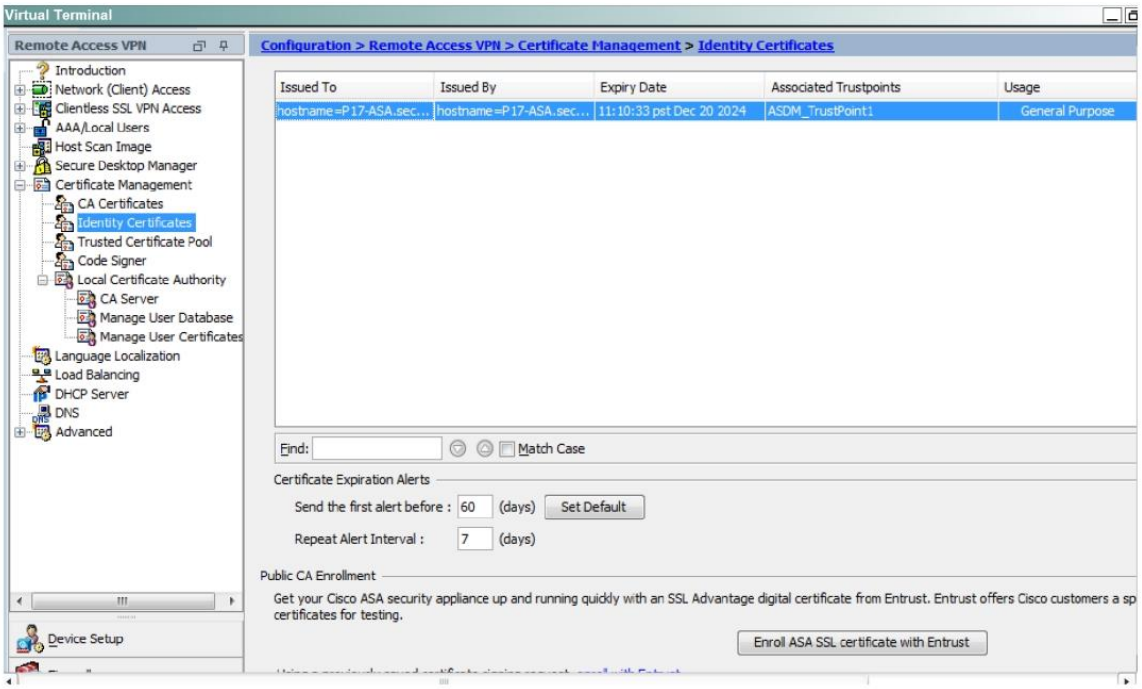


Then hit “edit” and you will see this:

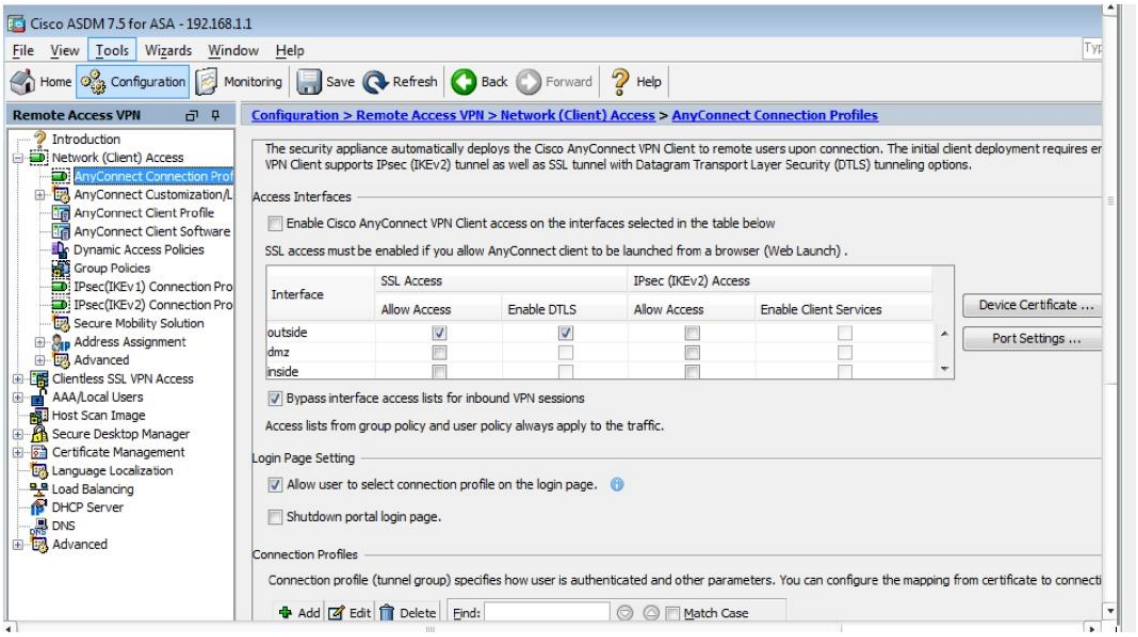


It's http://192.168.1.2 not the https://10.x.x.x

Not B, as this ASDM_TrustPoint1 is listed under the Identity Certificates, not the CA certificates:



Not D:



QUESTION 26

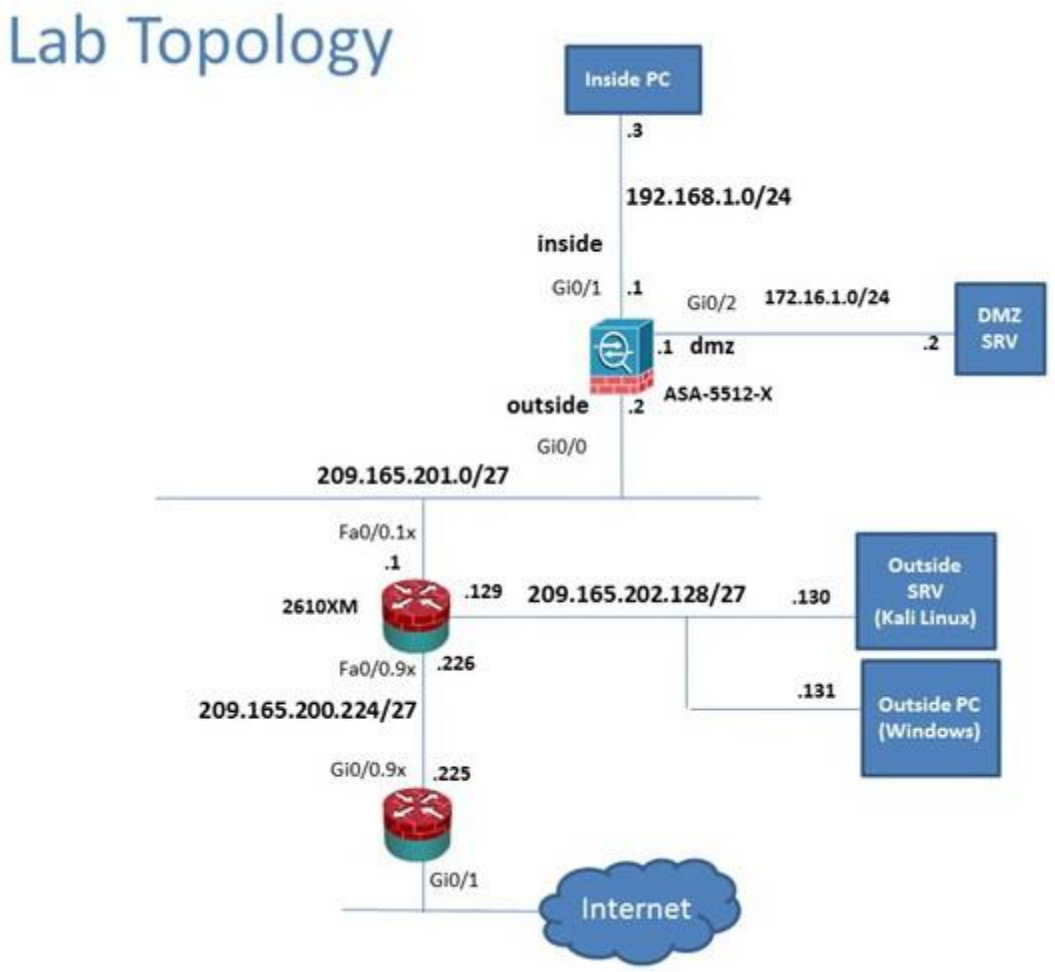
Scenario

In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

To access ASDM, click the ASA icon in the topology diagram.

Note: Not all ASDM functionalities are enabled in this simulation.

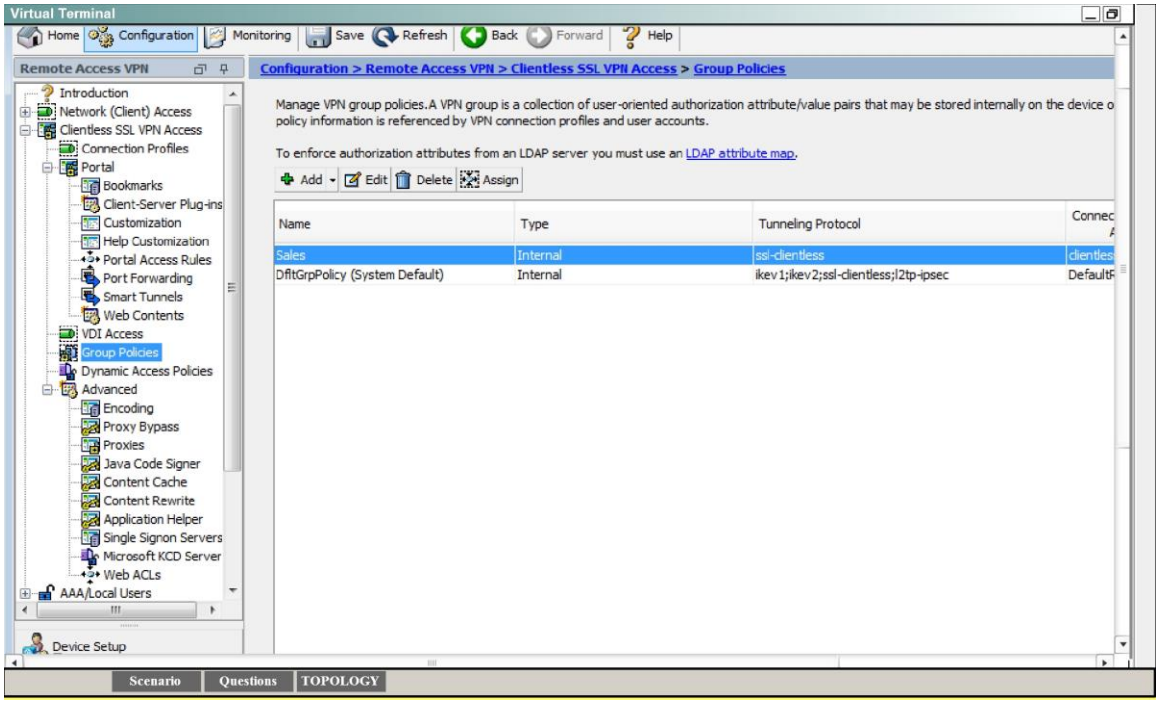
To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.



Which four tunneling protocols are enabled in the DfltGrpPolicy group policy? (choose four)

A. IPsec IKEv1
B. IPsec IKEv2
C. L2TP/IPsec
D. Clientless SSL VPN
E. SSL VPN Client
F. PPTP

Answer: ABCD
Explanation:
By clicking one the Configuration-> Remote Access -> Clientless CCL VPN Access-> Group Policies tab you can view the DfltGrpPolicy protocols as shown below:



QUESTION 27
Scenario
Given the new additional connectivity requirements and the topology diagram, use ASDM to accomplish the required ASA configurations to meet the requirements.
New additional connectivity requirements:

```
- Currently, the ASA configurations only allow on the Inside and DMZ
networks to access any hosts on the Outside. Your task is to use ASDM
to configure the ASA to also allow any host only on the Outside to HTTP
to the DMZ server. The hosts on the Outside will need to use the
209.165.201.30 public IP address when HTTPing to the DMZ server.
- Currently, hosts on the ASA higher security level interfaces are not
able to ping any hosts on the lower security level interfaces. Your
task in this simulation is to use ASDM to enable the ASA to dynamically
allow the echo-reply responses back through the ASA.
```

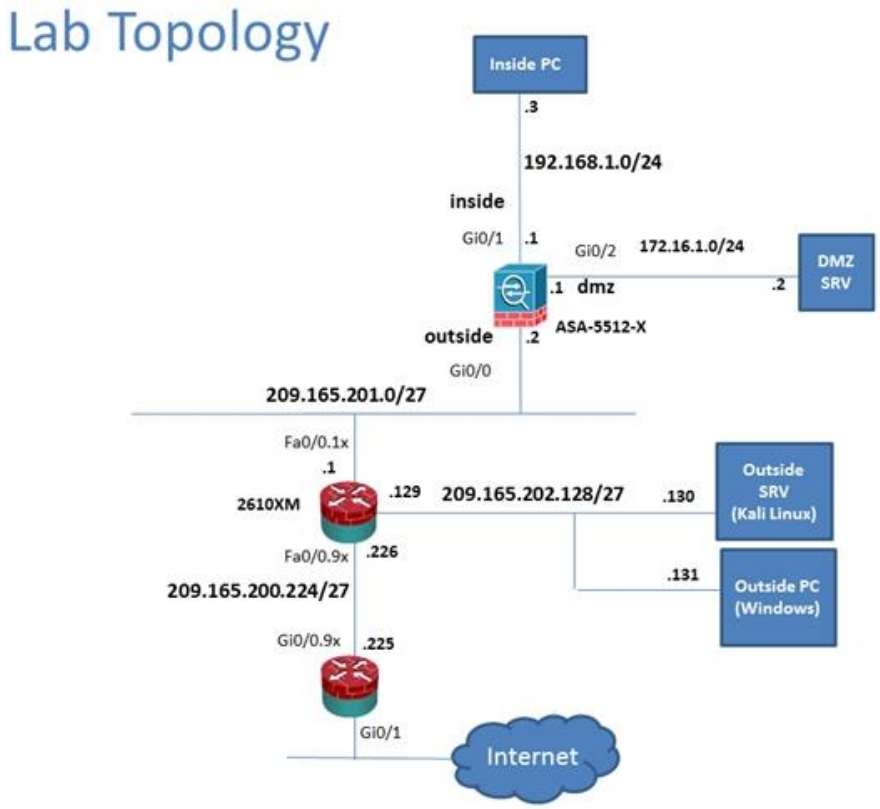
Once the correct ASA configurations have been configured:

```
- You can test the connectivity tohttp://209.165.201,30 from the
Outside PC browser.
- You can test the pings to the Outside (www.cisco.com) by opening the
inside PC command prompt window.
- In this simulation, only testing pings to www.cisco.com will work.
```

To access ASDM, click the ASA icon in the topology diagram.
To access the Firefox Browser on the Outside PC, click the Outside PC icon in the topology diagram.
To access the Command prompt on the Inside PC, click the Inside PC icon in the topology diagram.

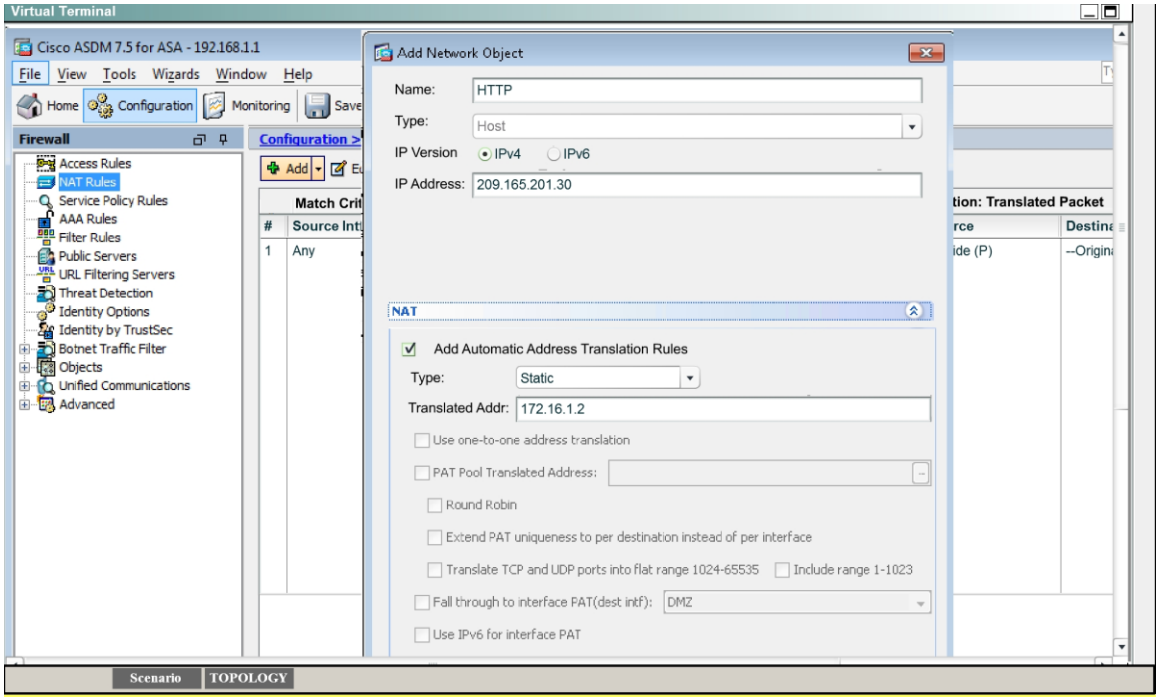
Note:

After you make the configuration changes in ASDM, remember to click Apply to apply the configuration changes.
Not all ASDM screens are enabled in this simulation, if some screen is not enabled, try to use different methods to configure the ASA to meet the requirements.
In this simulation, some of the ASDM screens may not look and function exactly like the real ASDM.

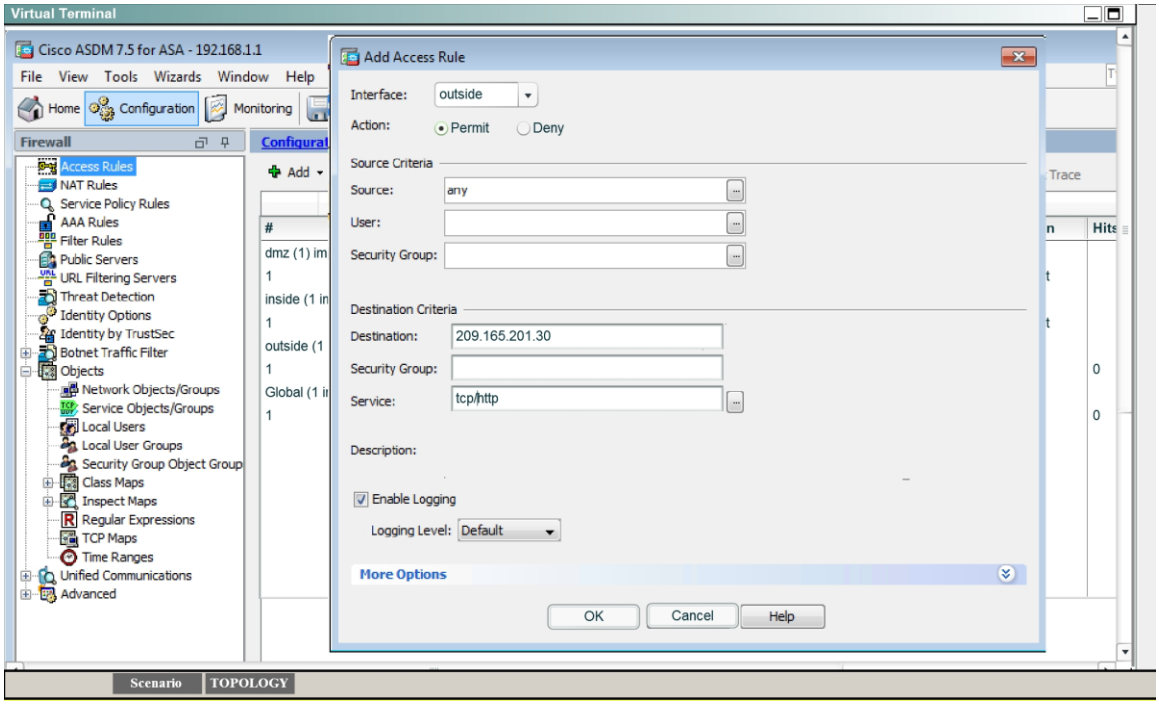


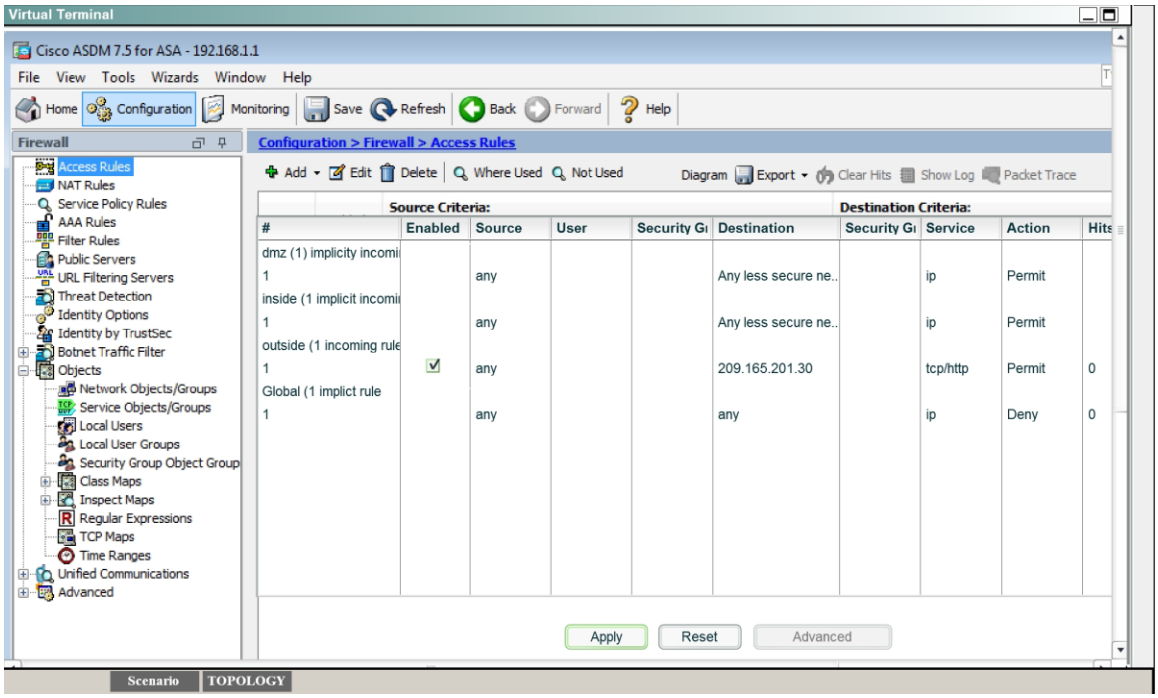
Answer:
Step 1: Firewall, Configuration, NAT Rules, Name=WebSvr, IP version IPv4, IP address=172.16.1.2 Static NAT=209.165.201.30
Step 2: Firewall, Config, Access Rules, Interface=Outside, Action=Permit, Source=any, Destination=209.165.201.30, Service=tcp/http
Step 3: Firewall, Config, Service policy Rules, Click Global Policy and edit, Rule Action tab, Click ICMP and apply
Step 4: Ping www.cisco.com from Inside PC
Step 5: Type http://209.165.201.30 in web browser in the Outside PC

Explanation:
First, for the HTTP access we need to create a NAT object. Here I called it HTTP but it can be given any name.

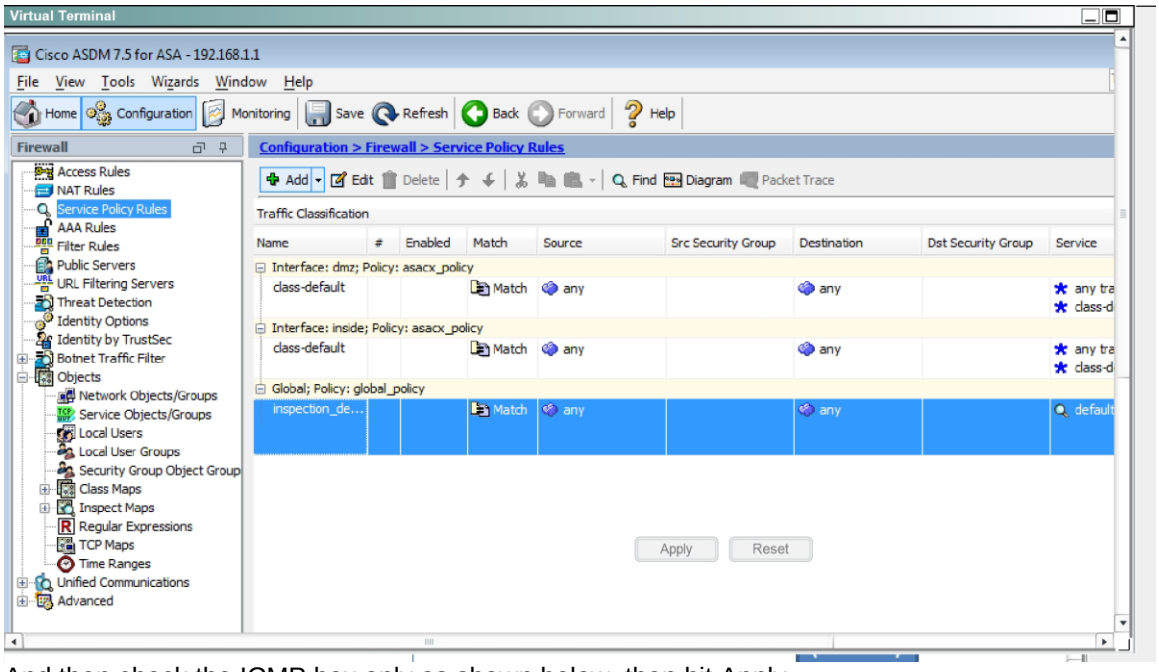


Then, create the firewall rules to allow the HTTP access:

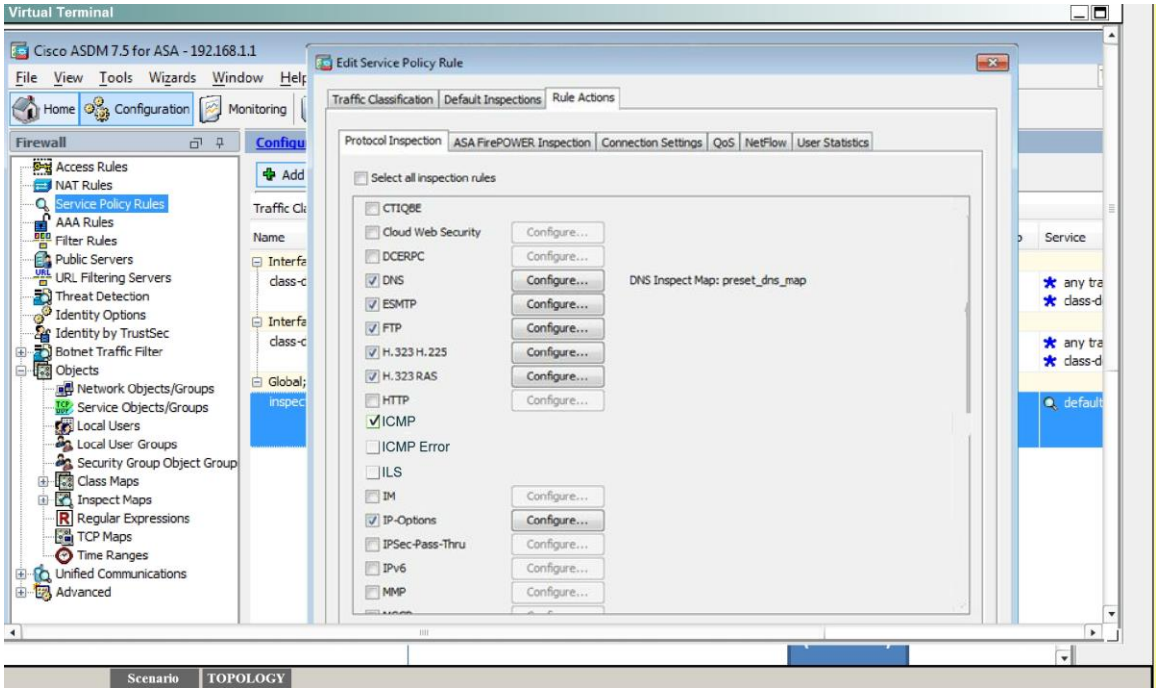




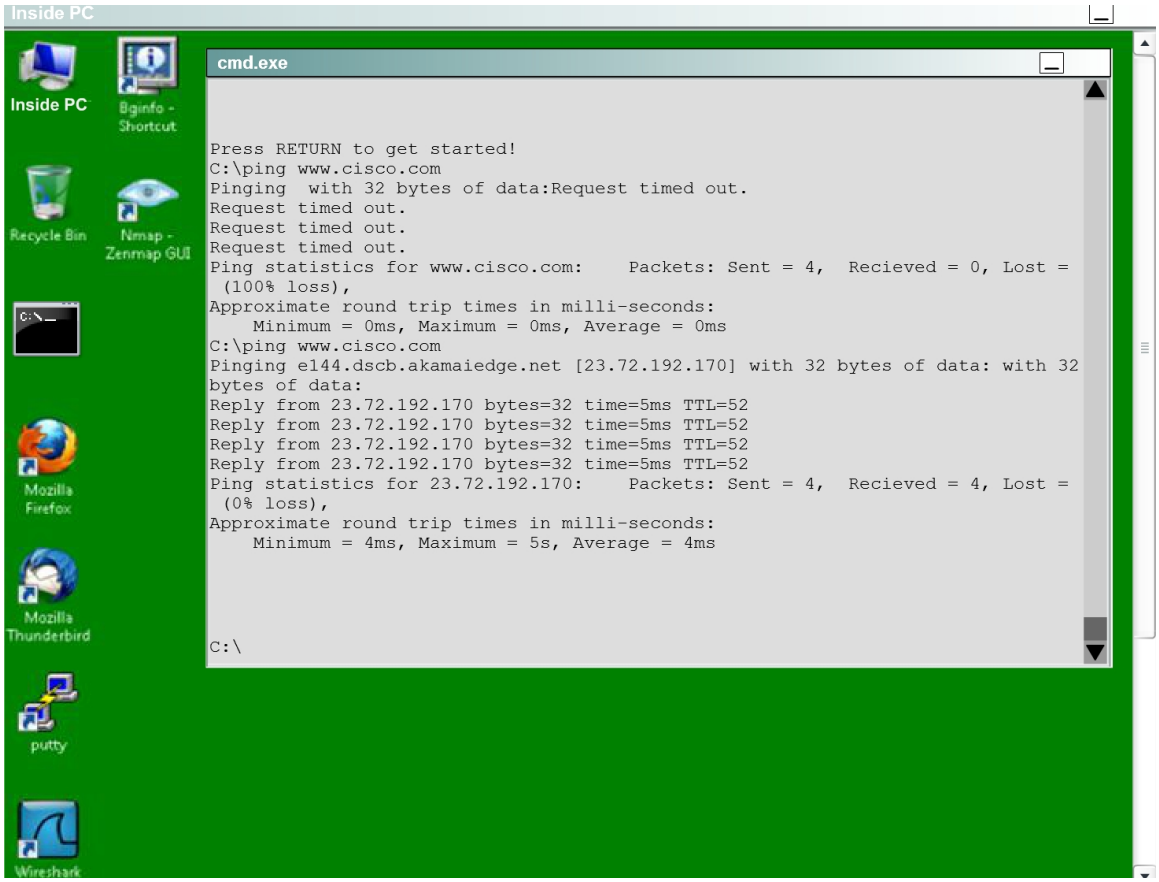
You can verify using the outside PC to HTTP into 209.165.201.30.
For step two, to be able to ping hosts on the outside, we edit the last service policy shown below:



And then check the ICMP box only as shown below, then hit Apply.



After that is done, we can ping www.cisco.com again to verify:



QUESTION 28
What is the purpose of the Integrity component of the CIA triad?

A. to ensure that only authorized parties can modify data
B. to determine whether data is relevant
C. to create a process for accessing data
D. to ensure that only authorized parties can view data

Answer: A

QUESTION 29
Which two statements about Telnet access to the ASA are true? (Choose two).

A. You may VPN to the lowest security interface to telnet to an inside interface.
B. You must configure an AAA server to enable Telnet.
C. You can access all interfaces on an ASA using Telnet.
D. You must use the command virtual telnet to enable Telnet.
E. Best practice is to disable Telnet and use SSH.

Answer: AE

QUESTION 30
Which protocol provides security to Secure Copy?

A. IPsec
B. SSH
C. HTTPS
D. ESP

Answer: B

QUESTION 31
A clientless SSL VPN user who is connecting on a Windows Vista computer is missing the menu option for Remote Desktop Protocol on the portal web page.
Which action should you take to begin troubleshooting?

A. Ensure that the RDP2 plug-in is installed on the VPN gateway
B. Reboot the VPN gateway
C. Instruct the user to reconnect to the VPN gateway
D. Ensure that the RDP plug-in is installed on the VPN gateway

Answer: A
Explanation:
+ RDP plug-in: This is the original plug-in created that contains both the Java and ActiveX Client.
+ **RDP2** plug-in: Due to changes within the RDP protocol, the Proper Java RDP Client was updated in order to support Microsoft Windows 2003 Terminal Servers and **Windows Vista** Terminal Servers.
Source: http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generationfirewalls/113600-technote-product-00.html

QUESTION 32
Which security zone is automatically defined by the system?

A. The source zone
B. The self zone
C. The destination zone
D. The inside zone

Answer: B

QUESTION 33
What are purposes of the Internet Key Exchange in an IPsec VPN? (Choose two.)

A. The Internet Key Exchange protocol establishes security associations
B. The Internet Key Exchange protocol provides data confidentiality
C. The Internet Key Exchange protocol provides replay detection
D. The Internet Key Exchange protocol is responsible for mutual authentication Answer:

Answer: AD

QUESTION 34
Which address block is reserved for locally assigned unique local addresses?

A. 2002::/16
B. FD00::/8
C. 2001::/32
D. FB00::/8

Answer: B

QUESTION 35
What is a possible reason for the error message?

Router(config)#aaa server?%
Unrecognized command

A. The command syntax requires a space after the word "server"
B. The command is invalid on the target device
C. The router is already running the latest operating system
D. The router is a new device on which the aaa new-model command must be applied before continuing

Answer: D

QUESTION 36
Which statements about smart tunnels on a Cisco firewall are true? (Choose two.)

A. Smart tunnels can be used by clients that do not have administrator privileges

B. Smart tunnels support all operating systems
C. Smart tunnels offer better performance than port forwarding
D. Smart tunnels require the client to have the application installed locally

Answer: AC
Explanation:
Smart Tunnel is an advanced feature of Clientless SSL VPN that provides seamless and highly secure remote access for native client-server applications.
Clientless SSL VPN with Smart Tunnel is the preferred solution for allowing access from non-corporate assets as it **does not require the administrative** rights.
Port forwarding is the legacy technology for supporting TCP based applications over a Clientless SSL VPN connection. **Unlike port forwarding, Smart Tunnel simplifies the user experience** by not requiring the user connection of the local application to the local port.
Source: http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/tunnel.pdf

QUESTION 37
Which option describes information that must be considered when you apply an access list to a physical interface?

A. Protocol used for filtering
B. Direction of the access class
C. Direction of the access group
D. Direction of the access list

Answer: C

QUESTION 38
Which source port does IKE use when NAT has been detected between two VPN gateways?

A. TCP 4500
B. TCP 500
C. UDP 4500
D. UDP 500

Answer: C

QUESTION 39
Which of the following are features of IPsec transport mode? (Choose three.)

A. IPsec transport mode is used between end stations
B. IPsec transport mode is used between gateways
C. IPsec transport mode supports multicast
D. IPsec transport mode supports unicast
E. IPsec transport mode encrypts only the payload
F. IPsec transport mode encrypts the entire packet

Answer: ADE
Explanation:
IPSec Transport Mode

IPSec Transport mode is used for end-to-end communications, for example, for communication between a client and a server or between a workstation and a gateway (if the gateway is being treated as a host). A good example would be an encrypted Telnet or Remote Desktop session from a workstation to a server.
Transport mode provides the protection of our data, also known as IP Payload, and consists of TCP/UDP header + Data, through an AH or ESP header. The payload is encapsulated by the IPSec headers and trailers. The original IP headers remain intact, except that the IP protocol field is changed to ESP (50) or AH (51), and the original protocol value is saved in the IPsec trailer to be restored when the packet is decrypted.
IPSec transport mode is usually used when another tunneling protocol (like GRE) is used to first encapsulate the IP data packet, then IPSec is used to protect the GRE tunnel packets. IPSec protects the GRE tunnel traffic in transport mode.

QUESTION 40
Which command causes a Layer 2 switch interface to operate as a Layer 3 interface?

A. no switchport nonnegotiate
B. switchport
C. no switchport mode dynamic auto
D. no switchport

Answer: D

QUESTION 41
Which command verifies phase 1 of an IPsec VPN on a Cisco router?

A. show crypto map
B. show crypto ipsec sa
C. show crypto isakmp sa
D. show crypto engine connection active

Answer: C
Explanation:
show crypto ipsec sa verifies Phase 2 of the tunnel.

QUESTION 42
What is the purpose of a honeypot IPS?

A. To create customized policies
B. To detect unknown attacks
C. To normalize streams
D. To collect information about attacks

Answer: D

QUESTION 43
Which type of firewall can act on the behalf of the end device?

A. Stateful packet
B. Application

C. Packet
D. Proxy

Answer: D

QUESTION 44
Refer to the exhibit. While troubleshooting site-to-site VPN, you issued the show crypto isakmp as command. What does the given output show?

```
dst          src          state      conn-id     slot
10.10.10.2   10.1.1.5     QM_IDLE    1           0
```

A. IPSec Phase 1 is established between 10.10.10.2 and 10.1.1.5
B. IPSec Phase 2 is established between 10.10.10.2 and 10.1.1.5
C. IPSec Phase 1 is down due to a QM_IDLE state
D. IPSEc Phase 2 is down due to a QM_IDLE state

Answer: A

QUESTION 45
What type of attack was the Stuxnet virus?

A. cyber warfare
B. hactivism
C. botnet
D. social engineering

Answer: A

QUESTION 46
Which type of secure connectivity does an extranet provide?

A. remote branch offices to your company network
B. your company network to the Internet
C. new networks to your company network
D. other company networks to your company network

Answer: D

QUESTION 47
After reloading a router, you issue the dir command to verify the installation and observe that the image file appears to be missing. For what reason could the image file fail to appear in the dir output?

A. The secure boot-image command is configured
B. The secure boot-comfit command is configured
C. The confreg 0x24 command is configured.

D. The reload command was issued from ROMMON.

Answer: A

QUESTION 48
What is a reason for an organization to deploy a personal firewall?

A. To protect endpoints such as desktops from malicious activity
B. To protect one virtual network segment from another
C. To determine whether a host meets minimum security posture requirements
D. To create a separate, non-persistent virtual environment that can be destroyed after a session
E. To protect the network from DoS and syn-flood attacks

Answer: A

QUESTION 49
Which FirePOWER preprocessor engine is used to prevent SYN attacks?

A. Rate-Based Prevention
B. Portscan Detection
C. IP Defragmentation
D. Inline Normalization

Answer: A

QUESTION 50
What VPN feature allows traffic to exit the security appliance through the same interface it entered?

A. Hairpinning
B. NAT
C. NAT traversal
D. split tunneling

Answer: A

QUESTION 51
When an IPS detects an attack, which action can the IPS take to prevent the attack from spreading?

A. Perform a Layer 6 reset
B. Deploy an antimalware system
C. Enable bypass mode
D. Deny the connection inline

Answer: D

QUESTION 52

Which statement about Cisco ACS authentication and authorization is true?

A. ACS servers can be clustered to provide scalability
B. ACS can query multiple Active Directory domains
C. ACS uses TACACS to proxy other authentication servers
D. ACS can use only one authorization profile to allo or deny requests

Answer: A

QUESTION 53
What is the only permitted operation for processing multicast traffic on zone-based firewalls?

A. Stateful inspection of multicast traffic is supported only for the self zone
B. Stateful inspection for multicast traffic is supported only between the self-zone and the internal zone
C. Only control plane policing can protect the control plane against multicast traffic.
D. Stateful inspection of multicast traffic is supported only for the internal zone.

Answer: C

QUESTION 54
What is one requirement for locking a wired or wireless device from ISE?

A. The ISE agent must be installed on the device
B. The device must be connnected to the network when the lock command is executed
C. The user must approve the locking action
D. The organization must implement an acceptable use policy allowing device locking

Answer: A

QUESTION 55
Refer to the exhibit. What type of firewall would use the given cofiguration line?

```
UDP outside  209.165.201.225:53 inside  10.0.0.10:52464, idle 0:00:01, bytes 266, flags -
```

A. a stateful firewall
B. a personal firewall
C. a proxy firewall
D. an application firewall
E. a stateless firewall

Answer: A

QUESTION 56
What are two default Cisco IOS privilege levels? (Choose two)

A. 0

B. 5
C. 1
D. 7
E. 10
F. 15

Answer: CF

QUESTION 57
What is the effect of the given command sequence?

```
crypto map mymap 20 match address 201
access-list 201 permit ip 10.10.10.0 255.255.255.0 10.100.100.0 255.255.255.0
```

A. It defines IPSec policy for traffic sourced from 10.10.10.0/24 with a desstination of 10.100.100.0/24
B. It defines IPSec policy for traffic sourced from 10.100.100.0/24 with a destination of 10.10.10.0/24
C. it defines IKE policy for traffic sourced from 10.10.10.0/24 with a destination of 10.100.100.0/24
D. It defines IKE policy for traffic sourced from 10.100.100.0/24 with a destination of 10.10.10.0/24

Answer: A

QUESTION 58
Which tool can an attacker use to attempt a DDos attack?

A. botnet
B. Trojan horse
C. virus
D. adware

Answer: A

QUESTION 59
how does the Cisco ASA use Active Directory to authorize VPN users?

A. It queries the Active Directory server for a specfic attribute for the specific user
B. It sends the username and password to retire an ACCEPT or Reject message from the Active Directory server
C. It downloads and stores the Active Directory databas to query for future authorization
D. It redirects requests to the Active Directory server defined for the VPN group

Answer: A

QUESTION 60
Which statement about application blocking is true?

A. It blocks access to files with specific extensions
B. It blocks access to specific network addresses

C. It blocks access to specific programs
D. It blocks access to specific network services.

Answer: C

QUESTION 61
For what reason would you configure multiple security contexts on the ASA firewall?

A. To enable the use of VFRs on routers that are adjacently connected
B. To provide redundancy and high availability within the organization
C. To enable the use of multicast routing and QoS through the firewall
D. To seperate different departments and business units

Answer: D

QUESTION 62
What VPN feature allows Internet traffic and local LAN/WAN traffic to use the same network connection.

A. split tunneling
B. hairpinning
C. tunnel mode
D. transparent mode

Answer: A

QUESTION 63
When is the best time to perform an anti-virus signature update?

A. When the local scanner has detected a new virus
B. When a new virus is discovered in the wild
C. Every time a new update is available
D. When the system detects a browser hook

Answer: C

QUESTION 64
What is the effect of the send-lifetime local 23:59:00 31 December 31 2013 infinite command?

A. It configures the device to begin transmitting the authentication key to other devices at 00:00:00 local time on January 1, 2014 and continue using the key indefinitely.
B. It configures the device to begin transmitting the authentication key to other devices at 23:59:00 local time on December 31, 2013 and continue using the key indefinitely.
C. It configures the device to begin accepting the authentication key from other devices immediately and stop accepting the key at 23:59:00 local time on December 31, 2013.
D. It configures the device to generate a new authentication key and transmit it to other devices at 23:59 00 local time on December 31, 2013.
E. It configures the device to begin accepting the authentication key from other devices at 23:59:00 local time on December 31, 2013 and continue accepting the key indefinitely.

F. It configures the device to begin accepting the authentication key from other devices at 00:00:00 local time on January 1, 2014 and continue accepting the key indefinitely.

Answer: B

QUESTION 65
Which Statement about personal firewalls is true?

A. They are resilient against kernal attacks
B. They can protect email messages and private documents in a similar way to a VPN
C. They can protect the network against attacks
D. They can protect a system by denying probing requests

Answer: D

QUESTION 66
Refer to the exhibit. While troubleshooting site-to-site VPN, you issued the show crypto ipsec sa command. What does the given output show?

```
current_peer: 10.1.1.5
   PERMIT, flags={origin_is_acl,}
  #pkts encaps: 1205, #pkts encrypt: 1205, #pkts digest 1205
  #pkts decaps: 1168, #pkts decrypt: 1168, #pkts verify 1168
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0,
  #pkts decompress failed: 0, #send errors 0, #recv errors 0
   local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.1.1.5
```

A. ISAKMP security associations are established between 10.1.1.5 and 10.1.1.1
B. IPSec Phase 2 is established between 10.1.1.1 and 10.1.1.5
C. IKE version 2 security associations are established between 10.1.1.1 and 10.1.1.5
D. IPSec Phase 2 is down due to a mismatch between encrypted and decrypted packets

Answer: B

QUESTION 67
Which statement about a PVLAN isolated port configured on a switch is true?

A. The isolated port can communicate only with the promiscous port
B. The isolated port can communicate with other isolated ports and the promiscuous port
C. The isolated port can communicate only with community ports
D. The isolated port can communicate only with other isolated ports

Answer: A

QUESTION 68
Within an 802.1X enabled network with the Auth Fail feature configured, when does a switch port get placed into a restricted VLAN?

A. When user failed to authenticate after certain number of attempts
B. When 802.1X is not globally enabled on the Cisco catalyst switch
C. When AAA new-model is enabled
D. If a connected client does not support 802.1X
E. After a connected client exceeds a specific idle time

Answer: A

QUESTION 69
What type of security support is provided by the Open Web Application Security Project?

A. Education about common Web site vulnerabilities
B. A wb site security framework
C. A security discussion forum for Web site developers
D. Scoring of common vulnerabilities and exposures

Answer: A

QUESTION 70
Refer to the exhibit. Which statement about the device time is true?

```
R1> show clock detail
.22:22:35.123 UTC Tue Feb 26 2013
Time source is NTP
```

A. The time is authoritative because the clock is in sync
B. The time is authoritative, but the NTP process has lost contact with its servers
C. The clock is out of sync
D. NTP is configured incorrectly
E. The time is not authoritative

Answer: B

QUESTION 71
In what type of attack does an attacker virtually change a devices burned in address in an attempt to circumvent access lists and mask the device's true identity?

A. gratuitous ARP
B. ARP poisoning
C. IP Spoofing
D. MAC Spoofing

Answer: D

QUESTION 72
How does a zone-based firewall implementation handle traffic between Interfaces in the same

Zone?

A. traffic between interfaces in the same zone is blocked unless yoc configure the same-security permit command
B. Traffic between interfaces in the same zone is always blocked
C. Traffic between two interfaces in the same zone is allowed by default
D. Traffic between interfaces in the same zone is blocked unless you apply a service policy to the zone pair

Answer: C

QUESTION 73
An attacker installs a rogue switch that sends superior BPDUs on your network.
What is a possible result of this activity?

A. The switch could offer fake DHCP addresses.
B. The switch could become the root bridge.
C. The switch could be allowed to join the VTP domain
D. The switch could become a transparent bridge.

Answer: B

QUESTION 74
Which two next generation encrytption algorithms does Cisco recommend? (Choose two)

A. AES
B. 3DES
C. DES
D. MD5
E. DH-1024
F. SHA-384

Answer: AF

QUESTION 75
In which three cases does the ASA firewall permit inbound HTTP GET requests during normal operations? (Choose three).

A. when a matching TCP connection is found
B. when the firewall requires strict HTTP inspection
C. when the firewall receives a FIN packet
D. when matching ACL entries are configured
E. when the firewall requires HTTP inspection
F. when matching NAT entries are configured

Answer: ADF
Explanation:
See the following links:
https://supportforums.cisco.com/discussion/11809846/asa-5505-using-nat-allowing-incoming-traffic-https

https://supportforums.cisco.com/discussion/12473551/asa-what-allowing-return-http-traffic
Also, there is a modified version of this question where answers D and F are replaced with "When the firewall receives a SYN packet" and "When the firewall receives a SYN-ACK packet". The a SYN-ACK packet coming back from the web server establishes the TCP connection and allows requests to come through, so this is a correct answer.

QUESTION 76
Which two features are commonly used CoPP and CPPr to protect the control plane? (Choose two.)

A. QoS
B. traffic classification
C. access lists
D. policy maps
E. class maps
F. Cisco Express Forwarding

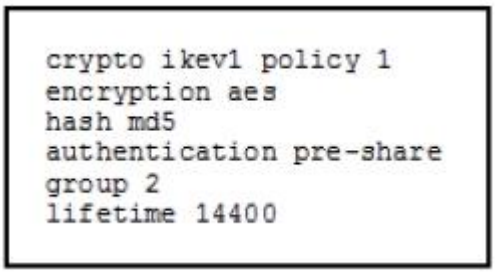
Answer: AB

QUESTION 77
What is an advantage of implementing a Trusted Platform Module for disk encryption?

A. It provides hardware authentication
B. It allows the hard disk to be transferred to another device without requiring re-encryption.dis
C. it supports a more complex encryption algorithm than other disk-encryption technologies.
D. it can protect against single poins of failure.

Answer: A

QUESTION 78
Refer to the exhibit. What is the effect of the given command sequence?



A. It configures IKE Phase 1
B. It configures a site-to-site VPN Tunnel
C. It configures a crypto policy with a key size of 14400
D. It configures IPSec Phase 2

Answer: A

QUESTION 79

A specific URL has been identified as containing malware. What action can you take to block users from accidentaly visiting the URL and becoming infected with malware?

A. Enable URL filtering on the perimeter firewall and add the URLs you want to allow to the routers local URL list
B. Enable URL filtering on the perimeter router and add the URLs you want to allow to the firewalls local URL list
C. Create a blacklist that contains the URL you want to block and activate the blacklist on the perimeter router.
D. Enable URL filtering on the perimeter router and add the URLs you want to block to the routers local URL list
E. Create a whitelist that contains the URls you want to allow and activate the whitelist on the perimeter router.

Answer: D

QUESTION 80
If you change the native VLAN on the port to an unused VLAN, what happens if an attacker attempts a double tagging attack?

A. The trunk port would go into an error-disable state.
B. A VLAN hopping attack would be successful
C. A VLAN hopping attack would be prevented
D. the attacked VLAN will be pruned

Answer: C

QUESTION 81
What is an advantage of placing an IPS on the inside of a network?

A. It can provide higher throughput.
B. It receives traffic that has already been filtered.
C. It receives every inbound packet.
D. It can provide greater security.

Answer: B

QUESTION 82
Which three statements about Cisco host-based IPS soluations are true? (Choose three.)

A. It can view encrypted files.
B. It can have more restrictive policies than network-based IPS.
C. It can generate alerts based on behavior at the desktop level.
D. It can be deployed at the perimeter.
E. It uses signature-based policies.
F. It works with deployed firewalls.

Answer: ABC
Explanation:
If the network traffic stream is encrypted, **HIPS has access to the traffic in unencrypted form**.

HIPS can combine the best features of antivirus, behavioral analysis, signature filters, network firewalls, and application firewalls in one package.
Host-based IPS operates by detecting attacks that occur on a host on which it is installed. HIPS works by intercepting operating system and application calls, securing the operating system and application configurations, validating incoming service requests, and analyzing local log files for after-the-fact suspicious activity.
Source: http://www.ciscopress.com/articles/article.asp?p=1336425&seqNum=3

QUESTION 83
Which syslog severity level is level number 7?

A. Warning
B. Informational
C. Notification
D. Debugging

Answer: D
Explanation:
The list of severity Levels:
0 Emergency: system is unusable
1 Alert: action must be taken immediately
2 Critical: critical conditions
3 Error: error conditions
4 Warning: warning conditions
5 Notice: normal but significant condition
6 Informational: informational messages
7 Debug: debug-level messages

QUESTION 84
Which type of mirroring does SPAN technology perform?

A. Remote mirroring over Layer 2
B. Remote mirroring over Layer 3
C. Local mirroring over Layer 2
D. Local mirroring over Layer 3

Answer: C

QUESTION 85
Which tasks is the session management path responsible for? (Choose three.)

A. Verifying IP checksums
B. Performing route lookup
C. Performing session lookup
D. Allocating NAT translations
E. Checking TCP sequence numbers
F. Checking packets against the access list

Answer: BDF
Explanation:
http://blog.ipexpert.com/a-closer-look-at-stateful-inspection-on-the-cisco-asa/

QUESTION 86
Which network device does NTP authenticate?

A. Only the time source
B. Only the client device
C. The firewall and the client device
D. The client device and the time source

Answer: A

QUESTION 87
What hash type does Cisco use to validate the integrity of downloaded images?

A. Sha1
B. Sha2
C. Md5
D. Md1

Answer: C

QUESTION 88
Which option is the most effective placement of an IPS device within the infrastructure?

A. Inline, behind the internet router and firewall
B. Inline, before the internet router and firewall
C. Promiscuously, after the Internet router and before the firewall
D. Promiscuously, before the Internet router and the firewall

Answer: A

QUESTION 89
If a router configuration includes the line aaa authentication login default group tacacs+ enable, which events will occur when the TACACS+ server returns an error? (Choose two.)

A. The user will be prompted to authenticate using the enable password
B. Authentication attempts to the router will be denied
C. Authentication will use the router`s local database
D. Authentication attempts will be sent to the TACACS+ server

Answer: AD
Explanation:
Two things I need to say. One, local database has nothing to do with enable secret/password as it is literally created using username/password command combinations. Second there is no fallback safety failover with aaa if you specify exact methods. Those exact methods are the only methods used, nothing else.
On the previous post I pasted an output for the authentication process with TACACS+ and enable. At a point there was a timeout message which resulted in switching to the second authentication method, ENABLE.

"Use the **timeout** *integer* argument to specify the period of time (in seconds) the router will wait for a response from the daemon **before it times out and declares an error**."
As a reference I used
http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scftplus.html
What concerns me is „If an ERROR response is received, the network access server will typically try to use an alternative method for authenticating the user." It doesn't specifically say „The router retries to connect with the TACACS+".

QUESTION 90
Which alert protocol is used with Cisco IPS Manager Express to support up to 10 sensors?

A. SDEE
B. Syslog
C. SNMP
D. CSM

Answer: A

QUESTION 91
Which type of address translation should be used when a Cisco ASA is in transparent mode?

A. Static NAT
B. Dynamic NAT
C. Overload
D. Dynamic PAT

Answer: A

QUESTION 92
Which components does HMAC use to determine the authenticity and integrity of a message? (Choose two.)

A. The password
B. The hash
C. The key
D. The transform set

Answer: BC

QUESTION 93
What is the default timeout interval during which a router waits for responses from a TACACS server before declaring a timeout failure?

A. 5 seconds
B. 10 seconds
C. 15 seconds
D. 20 seconds

Answer: A

Explanation:
Router(config)#tacacs-server timeout ?
<1-1000> Wait time (default 5 seconds)

QUESTION 94
Which RADIUS server authentication protocols are supported on Cisco ASA firewalls? (Choose three.)

A. EAP
B. ASCII
C. PAP
D. PEAP
E. MS-CHAPv1
F. MS-CHAPv2

Answer: CEF
Explanation:
The ASA supports the following authentication methods with RADIUS servers:
PAP - For all connection types.
CHAP and MS-CHAPv1 - For L2TP-over-IPsec connections.
MS-CHAPv2 - For L2TP-over-IPsec connections, and for regular IPsec remote access connections when the password management feature is enabled. You can also use MS-CHAPv2 with clientless connections.
Authentication Proxy modes - For RADIUS-to Active-Directory, RADIUS-to-RSA/SDI, RADIUS-to-Token server
http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/aaa_radius.html#77318

QUESTION 95
Which command initializes a lawful intercept view?

A. username cisco1 view lawful-intercept password cisco
B. parser view cisco li-view
C. li-view cisco user cisco1 password cisco
D. parser view li-view inclusive

Answer: C
Explanation:
Before you initialize a lawful intercept view, ensure that the privilege level is set to 15 via the privilege command.
SUMMARY STEPS
1. enable view
2. configure terminal
3. li-view li-password user username password password
4. username lawful-intercept [name] [privilege privilege-level| view view-name] password password
5. parser view view-name
6. secret 5 encrypted-password
7. name new-name

QUESTION 96

Which security measures can protect the control plane of a Cisco router? (Choose two.)

A. CCPr
B. Parser views
C. Access control lists
D. Port security
E. CoPP

Answer: AE
Explanation:
Table 10-3 Three Ways to Secure the Control Plane
Using CoPP or CPPr, you can specify which types of management traffic are acceptable at which levels.
For example, you could decide and configure the router to believe that SSH is acceptable at 100 packets per second, syslog is acceptable at 200 packets per second, and so on. Traffic that exceeds the thresholds can be safely dropped if it is not from one of your specific management stations.
You can specify all those details in the policy.
You learn more about control plane security in Chapter 13, "Securing Routing Protocols and the Control Plane."
Selective Packet Discard (SPD) provides the ability to
Although not necessarily a security feature,
prioritize certain types of packets (for example, routing protocol packets and Layer 2 keepalive messages, route processor [RP]). SPD provides priority of critical control plane traffic which are received by the
over traffic that is less important or, worse yet, is being sent maliciously to starve the CPU of resources required for the RP.

QUESTION 97
Which statement about extended access lists is true?

A. Extended access lists perform filtering that is based on source and destination and are most effective when applied to the destination
B. Extended access lists perform filtering that is based on source and destination and are most effective when applied to the source
C. Extended access lists perform filtering that is based on destination and are most effective when applied to the source
D. Extended access lists perform filtering that is based on source and are most effective when applied to the destination

Answer: B
Explanation:
Standard ACL
1) Able Restrict, deny & filter packets by Host Ip or subnet only.
2) Best Practice is put Std. ACL restriction near from Source Host/Subnet (Interface-In-bound).
3) No Protocol based restriction. (Only HOST IP).
Extended ACL
1) More flexible then Standard ACL.
2) You can filter packets by Host/Subnet as well as Protocol/TCPPort/UDPPort.
3) Best Practice is put restriction near form Destination Host/Subnet. (Interface-Outbound)

QUESTION 98

Which protocols use encryption to protect the confidentiality of data transmitted between two parties? (Choose two.)

A. FTP
B. SSH
C. Telnet
D. AAA
E. HTTPS
F. HTTP

Answer: BE

QUESTION 99
What are the primary attack methods of VLAN hopping? (Choose two.)

A. VoIP hopping
B. Switch spoofing
C. CAM-table overflow
D. Double tagging

Answer: BD

QUESTION 100
How can the administrator enable permanent client installation in a Cisco AnyConnect VPN firewall configuration?

A. Issue the command anyconnect keep-installer under the group policy or username webvpn mode
B. Issue the command anyconnect keep-installer installed in the global configuration
C. Issue the command anyconnect keep-installer installed under the group policy or username webvpn mode
D. Issue the command anyconnect keep-installer installer under the group policy or username webvpn mode

Answer: C

QUESTION 101
What type of security support is provided by the Open Web Application Security Project?

A. Education about common Web site vulnerabilities.
B. A Web site security framework.
C. A security discussion forum for Web site developers.
D. Scoring of common vulnerabilities and exposures.

Answer: A

QUESTION 102
What is the FirePOWER impact flag used for?

A. A value that indicates the potential severity of an attack.

B. A value that the administrator assigns to each signature.
C. A value that sets the priority of a signature.
D. A value that measures the application awareness.

Answer: A

QUESTION 103
Which two services define cloud networks? (Choose two.)

A. Infrastructure as a Service
B. Platform as a Service
C. Compute as a Service
D. Security as a Service
E. Tenancy as a Service

Answer: AB

QUESTION 104
In a security context, which action can you take to address compliance?

A. Implement rules to prevent a vulnerability
B. Correct or counteract a vulnerability
C. Reduce the severity of a vulnerability
D. Follow directions from the security appliance manufacturer to remediate a vulnerability

Answer: A

QUESTION 105
How many times was a read-only string used to attempt a write operation?

```
R1#show snmp
Chassis: FTX123456789
0 SNMP packets input
   6 Bad SNMP version errors
   3 Unknown community name
   9 Illegal operation for community name supplied
   4 Encoding errors
   2 Number of requested variables
   0 Number of altered variables
   98 Get-request PDUs
   12 Get-next PDUs
   2 Set-request PDUs
   0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
   0 Too big errors (Maximum packet size 1500)
   0 No such name errors
   0 Bad values errors
   0 General errors
   31 Response PDUs
   1 Trap PDUs
```

A. 6
B. 9
C. 4
D. 3
E. 2

Answer: B

QUESTION 106
What can the SMTP preprocessor in a FirePOWER normalize?

A. It can extract and decode email attachments in client to server traffic
B. It can look up the email sender
C. it compares known threats to the email sender
D. It can forward the SMTP traffic to an email filter server
E. It uses the Traffic Anomaly Detector

Answer: A

QUESTION 107
You want to allow all of your companies users to access the Internet without allowing other Web servers to collect the IP addresses of individual users.
What two solutions can you use? (Choose two).

A. Configure a proxy server to hide users local IP addresses

B. Assign unique IP addresses to all users.
C. Assign the same IP addresses to all users
D. Install a Web content filter to hide users local IP addresses
E. Configure a firewall to use Port Address Translation.

Answer: AE

QUESTION 108
Which two authentication types does OSPF support? (Choose two)

A. plaintext
B. MD5
C. HMAC
D. AES 256
E. SHA-1
F. DES

Answer: AB

QUESTION 109
Refer to the exhibit. The Admin user is unable to enter configuration mode on a device with the given configuration. What change can you make to the configuration to correct the problem?

```
Username HelpDesk privilege 9 password 0 helpdesk
Username Monitor privilege 8 password 0 watcher
Username Admin password checkme
Username Admin privilege 6 autocommand show running
Privilege exec level 6 configure terminal
```

A. Remove the Auto command keyword and arguments from the Username Admin privilege line
B. Change the Privilege exec level value to 15
C. Remove the two Username Admin lines
D. Remove the Privilege exec line.

Answer: A
Explanation:
The router just executes "show running" and disconnects if set to auto.

QUESTION 110
What command can you use to verify the binding table status?

A. Show ip dhcp snooping binding
B. Show ip dhcp snooping database
C. show ip dhcp snooping statistics
D. show ip dhcp pool
E. show ip dhcp source binding
F. show ip dhcp snooping

Answer: B
Explanation:
"show ip dhcp snooping binding" shows the contents of the binding table, but the summary or overall status is shown by "show ip dhcp snooping database".

QUESTION 111
If a switch receives a superior BPDU and goes directly into a blocked state, what mecanism must be in use?

A. Etherchannel guard
B. root guard
C. loop guard
D. BPDU guard

Answer: D
Explanation:
The key here is the word 'switch'. The entire switch goes into a blocked state, meaning that it can't participate in STP, it is blocked. Root guard basically puts the port in a listening state rather than forwarding, still allowing the device to participate in STP.

QUESTION 112
What type of packet creates and performs network operations on a network device?

A. data plane packets
B. management plane packets
C. services plane packets
D. control plane packets

Answer: D

QUESTION 113
Which two functions can SIEM provide? (Choose Two)

A. Correlation between logs and events from multiple systems.
B. event aggregation that allows for reduced log storage requirements.
C. proactive malware analysis to block malicious traffic.
D. dual-factor authentication.
E. centralized firewall management.

Answer: AB
Explanation:
Security Information Event Management SIEM
+ Log collection of event records from sources throughout the organization provides important forensic tools and helps to address compliance reporting requirements.
+ Normalization maps log messages from different systems into a common data model, enabling the organization to connect and analyze related events, even if they are initially logged in different source formats.
+ Correlation links logs and events from disparate systems or applications, speeding detection of and reaction to security threats.
+ Aggregation reduces the volume of event data by consolidating duplicate event records.

+ Reporting presents the correlated, aggregated event data in real-time monitoring and long-term summaries.
Source: http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-smart-businessarchitecture/sbaSIEM_deployG.pdf

QUESTION 114
What three actions are limitations when running IPS in promiscuous mode? (Choose three.)

A. deny attacker
B. deny packet
C. modify packet
D. request block connection
E. request block host
F. reset TCP connection

Answer: ABC

QUESTION 115
Which command will configure a Cisco ASA firewall to authenticate users when they enter the enable syntax using the local database with no fallback method?

A. aaa authentication enable console LOCAL SERVER_GROUP
B. aaa authentication enable console SERVER_GROUP LOCAL
C. aaa authentication enable console local
D. aaa authentication enable console LOCAL

Answer: D

QUESTION 116
Which accounting notices are used to send a failed authentication attempt record to a AAA server? (Choose two.)

A. start-stop
B. stop-record
C. stop-only
D. stop

Answer: AC

QUESTION 117
If the native VLAN on a trunk is different on each end of the link, what is a potential consequence?

A. The interface on both switches may shut down
B. STP loops may occur
C. The switch with the higher native VLAN may shut down
D. The interface with the lower native VLAN may shut down

Answer: B

QUESTION 118
Which type of IPS can identify worms that are propagating in a network?

A. Policy-based IPS
B. Anomaly-based IPS
C. Reputation-based IPS
D. Signature-based IPS

Answer: B

QUESTION 119
By which kind of threat is the victim tricked into entering username and password information at a disguised website?

A. Spoofing
B. Malware
C. Spam
D. Phishing

Answer: D

QUESTION 120
Which Cisco product can help mitigate web-based attacks within a network?

A. Adaptive Security Appliance
B. Web Security Appliance
C. Email Security Appliance
D. Identity Services Engine

Answer: B

QUESTION 121
Which statement correctly describes the function of a private VLAN?

A. A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains
B. A private VLAN partitions the Layer 3 broadcast domain of a VLAN into subdomains
C. A private VLAN enables the creation of multiple VLANs using one broadcast domain
D. A private VLAN combines the Layer 2 broadcast domains of many VLANs into one major broadcast domain

Answer: A

QUESTION 122
Which Cisco feature can help mitigate spoofing attacks by verifying symmetry of the traffic path?

A. Unidirectional Link Detection
B. Unicast Reverse Path Forwarding

C. TrustSec
D. IP Source Guard

Answer: B

QUESTION 123
What is the most common Cisco Discovery Protocol version 1 attack?

A. Denial of Service
B. MAC-address spoofing
C. CAM-table overflow
D. VLAN hopping

Answer: A

QUESTION 124
What is the Cisco preferred countermeasure to mitigate CAM overflows?

A. Port security
B. Dynamic port security
C. IP source guard
D. Root guard

Answer: B

QUESTION 125
When a switch has multiple links connected to a downstream switch, what is the first step that STP takes to prevent loops?

A. STP elects the root bridge
B. STP selects the root port
C. STP selects the designated port
D. STP blocks one of the ports

Answer: A

QUESTION 126
Which countermeasures can mitigate ARP spoofing attacks? (Choose two.)

A. Port security
B. DHCP snooping
C. IP source guard
D. Dynamic ARP inspection

Answer: BD

QUESTION 127
Which of the following statements about access lists are true? (Choose three.)

A. Extended access lists should be placed as near as possible to the destination
B. Extended access lists should be placed as near as possible to the source
C. Standard access lists should be placed as near as possible to the destination
D. Standard access lists should be placed as near as possible to the source
E. Standard access lists filter on the source address
F. Standard access lists filter on the destination address

Answer: BCE

QUESTION 128
In which stage of an attack does the attacker discover devices on a target network?

A. Reconnaissance
B. Covering tracks
C. Gaining access
D. Maintaining access

Answer: A

QUESTION 129
Which type of security control is defense in depth?

A. Threat mitigation
B. Risk analysis
C. Botnet mitigation
D. Overt and covert channels

Answer: A

QUESTION 130
On which Cisco Configuration Professional screen do you enable AAA?

A. AAA Summary
B. AAA Servers and Groups
C. Authentication Policies
D. Authorization Policies

Answer: A

QUESTION 131
What configure mode you used for the command ip ospf authentication-key c1$c0?

A. global
B. priviliged
C. in-line
D. interface

Answer: D
Explanation:
ip ospf authentication-key is used under interface configuration mode, so it's in interface level, under global configuration mode. If it asks about interface level then choose that.
interface Serial0
ip address 192.16.64.1 255.255.255.0
ip ospf authentication-key c1$c0

QUESTION 132
What are two users of SIEM software? (Choose two)

A. performing automatic network audits
B. configuring firewall and IDS devices
C. alerting administrators to security events in real time
D. scanning emails for suspicious attachments
E. collecting and archiving syslog data

Answer: CE
Explanation:
The other choices are not functions of SIEM software.

QUESTION 133
If a packet matches more than one class map in an individual feature type's policy map, how does the ASA handle the packet?

A. the ASA will apply the actions from only the last matching class maps it finds for the feature type.
B. the ASA will apply the actions from all matching class maps it finds for the feature type.
C. the ASA will apply the actions from only the most specific matching class map it finds for the feature type.
D. the ASA will apply the actions from only the first matching class maps it finds for the feature type

Answer: D
Explanation:
If it matches a class map for a given feature type, it will NOT attempt to match to any subsequent class maps.

QUESTION 134
What statement provides the best definition of malware?

A. Malware is tools and applications that remove unwanted programs.
B. Malware is a software used by nation states to commit cyber-crimes.
C. Malware is unwanted software that is harmful or destructive
D. Malware is a collection of worms, viruses and Trojan horses that is distributed as a single.....

Answer: C

QUESTION 135
Your security team has discovered a malicious program that has been harvesting the CEO's email messages and the company's user database for the last 6 months.
What are two possible types of attacks your team discovered?

A. social activism
B. advanced persistent threat
C. drive-by spyware
D. targeted malware

Answer: B
Explanation:
If required 2 answers in the real exam, please choose BD.

QUESTION 136
Which FirePOWER preprocessor engine is used to prevent SYN attacks?

A. Anomaly.
B. Rate-Based Prevention
C. Portscan Detection
D. Inline Normalization

Answer: B

QUESTION 137
What is the only permitted operation for processing multicast traffic on zone-based firewalls?

A. Stateful inspection of multicast traffic is supported only for the self-zone.
B. Stateful inspection of multicast traffic is supported only between the self-zone and the internal zone.
C. Only control plane policing can protect the control plane against multicast traffic.
D. Stateful inspection of multicast traffic is supported only for the internal zone

Answer: C
Explanation:
Stateful inspection of multicast traffic is NOT supported by Cisco Zone based firewalls OR Cisco Classic firewall.

QUESTION 138
Which of encryption technology has the broadcast platform support to protect operating systems?

A. Middleware
B. Hardware
C. software
D. file-level

Answer: C

QUESTION 139
Which feature of the Cisco Email Security Appliance can mitigate the impact of snowshoe spam and sophisticated phishing attack?

A. holistic understanding of threats

B. graymail management and filtering
C. signature-based IPS
D. contextual analysis

Answer: D

QUESTION 140
Which Sourfire secure action should you choose if you want to block only malicious traffic from a particular end-user?

A. Trust
B. Block
C. Allow without inspection
D. Monitor
E. Allow with inspection

Answer: E
Explanation:
Allow with Inspection allows all traffic except for malicious traffic from a particular end-user. The other options are too restrictive, too permissive, or don't exist.

QUESTION 141
Which two next-generation encryption algorithms does Cisco recommends? (Choose two)

A. SHA-384
B. MD5
C. DH-1024
D. DES
E. AES
F. 3DES

Answer: AE
Explanation:
From Cisco documentation:
A. SHA-384 - YES
B. MD5 - NO
C. DH-1024 - NO
D. DES - NO
E. AES - YES (CBC, or GCM modes)
F. 3DES - Legacy

QUESTION 142
When an administrator initiates a device wipe command from the ISE, what is the immediate effect?

A. It requests the administrator to choose between erasing all device data or only managed corporate data.
B. It requests the administrator to enter the device PIN or password before proceeding with the operation
C. It immediately erases all data on the device.

D. It notifies the device user and proceeds with the erase operation

Answer: A

QUESTION 143
How does a device on a network using ISE receive its digital certificate during the new-device registration process?

A. ISE acts as a SCEP proxy to enable the device to receive a certificate from a central CA server
B. The device request a new certificate directly from a central CA
C. ISE issues a pre-defined certificate from a local database
D. ISE issues a certificate from its internal CA server.

Answer: A
Explanation:
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide.pdf

QUESTION 144
How can you detect a false negative on an IPS?

A. View the alert on the IPS
B. Use a third-party to audit the next-generation firewall rules
C. Review the IPS console
D. Review the IPS log
E. Use a third-party system to perform penetration testing

Answer: E
Explanation:
Only penetration testing can confirm this. All the other options lead to inconclusive results and may still result in false negatives.

QUESTION 145
Which two statement about stateless firewalls is true? (Choose two)

A. the Cisco ASA is implicitly stateless because it blocks all traffic by default.
B. They compare the 5-tuple of each incoming packets against configurable rules.
C. They cannot track connections..
D. They are designed to work most efficiently with stateless protocols such as HTTP or HTTPS..
E. Cisco IOS cannot implement them because the platform is Stateful by nature

Answer: BC
Explanation:
5-tuple is: source/destination IP, ports, and protocols. Stateless firewalls cannot track connections.

QUESTION 146
Which three ESP fields can be encrypted during transmission? (Choose three)

A. Next Header
B. MAC Address
C. Padding
D. Pad Length
E. Sequence Number
F. Security Parameter Index

Answer: ACD
Explanation:
The last encrypted part is the Payload Data. The unencrypted parts are the Security Parameter Index and the Sequence Number.

QUESTION 147
Which type of PVLAN port allows host in the same VLAN to communicate directly with the other?

A. promiscuous for hosts in the PVLAN
B. span for hosts in the PVLAN
C. Community for hosts in the PVLAN
D. isolated for hosts in the PVLAN

Answer: C
Explanation:
Hosts in the same PVLAN Community can communicate with one another.

QUESTION 148
Refer to the exhibit while troubleshooting site-to-site VPN, you issued the show crypto isakamp sa command. What does the given output shows?

```
dst          src          state          conn-id     slot
10.10.10.2   10.1.1.5     MM_NO_STATE    1           0
```

A. IKE Phase 1 main mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2
B. IKE Phase 1 main mode has successfully negotiate between 10.1.1.5 and10.10.10.2
C. IKE Phase 1 aggressive mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2
D. IKE Phase 1 aggressive mode was create on 10.1.1.5, but it failed to negotiate with 10.10.10.2

Answer: A
Explanation:
The MM_NO_STATE state indicates that the phase 1 policy does not match on both sides, therefore main mode failed to negotiate. Aggressive mode is indicated by AG instead of MM.

QUESTION 149
Refer to the exhibit while troubleshooting site-to-site VPN, you issued the show crypto isakamp sa command. What does the given output shows?

```
dst          src         state       conn-id     slot
10.10.10.2   10.1.1.5    QM_IDLE     1           0
```

A. IPSec Phase 2 established between 10.10.10.2 and 10.1.1.5
B. IPSec Phase 1 established between 10.10.10.2 and 10.1.1.5
C. IPSec Phase 2 is down due to a QM_IDLE state.
D. IPSec Phase 1 is down due to a QM_IDLE state.

Answer: B
Explanation:
An IDLE state is good and means that the connection and key exchange have taken place successfully. QM indicates that the device is ready for phase 2 (quick mode) and subsequent data transfer.

QUESTION 150
Refer to the exhibit. You have configured R1 and R2 as shown, but the routers are unable to establish a site-to-site VPN tunnel. What action can you take to correct the problem?

```
R1
Interface GigabitEthernet 0/0
Ip address 10.20.20.4 255.255.255.0

crypto isakmp policy 1
authentication pre-share
lifetime 84600
crypto isakmp key test67890 address 10.20.20.4


R2
Interface GigabitEthernet 0/0
Ip address 10.20.20.4 255.255.255.0

crypto isakmp policy 10
authentication pre-share
lifetime 84600
crypto isakmp key test12345 address 10.30.30.5
```

A. Edit the crypto keys on R1 and R2 to match.
B. Edit the crypto isakmp key command on each router with the address value of its own interface
C. Edit the ISAKMP policy sequence numbers on R1 and R2 to match.
D. set a valid value for the crypto key lifetime on each router.

Answer: A
Explanation:
The crypto keys don't match here. I've inferred and assumed that the destination address at the end of the "Crypto isakmp key test12345 address 10.30.30.5" line is the IP address of R1. By extension, this would produce an MM_NO_STATE state if you ran the "show crypto isakmp sa" command, as it would never connect to begin phase 1.

QUESTION 151
Refer to the exhibit. Which statement about the given configuration is true?

```
tacacs server tacacs1
   address ipv4 1.1.1.1
   timeout 20
   single-connection

tacacs server tacacs2
   address ipv4 2.2.2.2
   timeout 20
   single-connection

tacacs server tacacs3
   address ipv4 3.3.3.3
   timeout 20
   single-connection
```

A. The timeout command causes the device to move to the next server after 20 seconds of TACACS inactivity.
B. The single-connection command causes the device to process one TACACS request and then move to the next server.
C. The single-connection command causes the device to establish one connection for all TACACS transactions.
D. The router communicates with the NAS on the default port, TCP 1645

Answer: C
Explanation:
In order for TACACS+ servers to fail over, they must be configured in a TACACS server group, which these are not, which eliminates A and B. D is incorrect.

QUESTION 152
Refer to the exhibit. What is the effect of the given command?

```
crypto ipsec transform-set myset esp-md5-hmac esp-aes-256
```

A. It configure the network to use a different transform set between peers.
B. It merges authentication and encryption methods to protect traffic that matches an ACL.
C. It configures encryption for MD5 HMAC.
D. It configures authentications as AES 256.

Answer: B
Explanation:
Because a transform set defines a method to encrypt traffic: esp-aes-256 and a method to authenticate: esp-md5-hmac

QUESTION 153
Refer to the exhibit. What are two effects of the given command? (Choose two.)

```
crypto ipsec transform-set myset esp-md5-hmac esp-aes-256
```

A. It configures authentication to use AES 256.
B. It configures authentication to use MD5 HMAC.
C. It configures authorization use AES 256.
D. It configures encryption to use MD5 HMAC.
E. It configures encryption to use AES 256.

Answer: BE

QUESTION 154
What is a valid implicit permit rule for traffic that is traversing the ASA firewall?

A. Unicast IPv6 traffic from a higher security interface to a lower security interface is permitted in transparent mode only
B. Only BPDUs from a higher security interface to a lower security interface are permitted in routed mode.
C. ARPs in both directions are permitted in transparent mode only
D. Unicast IPv4 traffic from a higher security interface to a lower security interface is permitted in routed mode only
E. Only BPDUs from a higher security interface to a lower security interface are permitted in transparent mode.

Answer: C
Explanation:
IPv4 and IPv6 traffic is permitted in both routed and transparent mode from higher to lower security interfaces.

QUESTION 155
You have been tasked with blocking user access to website that violate company policy, but the site use dynamic IP Addresses. What is the best practice URL filtering to solve the problem?

A. Enable URL filtering and create a blacklist to block the websites that violate company policy.
B. Enable URL filtering and create a whitelist to allow only the websites the company policy allow users to access.
C. Enable URL filtering and use URL categorization to allow only the websites the company policy allow users to access
D. Enable URL filtering and create a whitelist to block the websites that violate company policy.
E. Enable URL filtering and use URL categorization to block the websites that violate company policy.

Answer: E
Explanation:
Categorization will catch a large number of related websites, regardless of the address or IP.

QUESTION 156
What is the potential drawback to leaving VLAN 1 as the native VLAN?

A. Gratuitous ARPs might be able to conduct a man-in-the-middle attack.
B. The CAM might be overloaded, effectively turning the switch into hub.
C. VLAN 1 might be vulnerable to IP address spoofing
D. It may be susceptible to a VLAN hopping attack

Answer: D

QUESTION 157
Refer to the exhibit. Which line in this configuration prevents the HelpDesk user from modifying the interface configuration?

```
Username Engineer privilege 9 password 0 configure
Username Monitor privilege 8 password 0 watcher
Username HelpDesk privilege 6 password help
Privilege exec level 6 show running
Privilege exec level 7 show start-up
Privilege exec level 9 configure terminal
Privilege exec level 10 interface
```

A. Privilege exec level 9 show configure terminal
B. Privilege exec level 7show start-up
C. Privilege exec level 10 interface
D. Username HelpDesk privilege 6 password help

Answer: A

QUESTION 158
Which IPS mode provides the maximum number of actions?

A. Inline
B. bypass
C. span
D. failover
E. promiscuous

Answer: A
Explanation:
Because IPS inline gets the live traffic as it's passing through the network and can take direct action on the traffic if it detects any malicious activity. The actions are drop, block, TCP reset, shun, alert, log, modify.

QUESTION 159
In which three cases does the ASA firewall permit inbound HTTP GET requests during normal operations? (Choose three)

A. When matching ACL entries are configured
B. when matching NAT entries are configured

C. When the firewall requires strict HTTP inspection
D. When the firewall requires HTTP inspection
E. When the firewall receives a SYN-ACK packet
F. When the firewall receives a SYN packet

Answer: ABE

QUESTION 160
Which technology can be used to rate data fidelity and to provide an authenticated hash for data?

A. Network blocking
B. signature updates
C. file analysis
D. file reputation

Answer: D

QUESTION 161
What configuration allows AnyConnect to authenticate automatically establish a VPN session when a user logs in to the computer?

A. proxy
B. Trusted Network Detection
C. transparent mode
D. always-on

Answer: D

QUESTION 162
Which statement about the communication between interfaces on the same security level is true?

A. All Traffic is allowed by default between interfaces on the same security level.
B. Interface on the same security level require additional configuration to permit inter-interface communication.
C. Configuring interface on the same security level can cause asymmetric routing.
D. You can configure only one interface on an individual security level.

Answer: B
Explanation:
The following command allows traffic of the same security level:
hostname(config)# same-security-traffic permit inter-interface

QUESTION 163
You have implemented Sourcefire IPS and configure it to block certain addresses utilizing security intelligence IP Addresses Reputation. A user calls and is not able to access a certain IP address. What action can you take to allow the user access to the IP address?

A. create a user based access control rule to allow the traffic.
B. create a custom blacklist to allow the traffic.

C. create a whitelist and add the appropriate IP address to allow the traffic.
D. create a rule to bypass inspection to allow the traffic.

Answer: C
Explanation:
Custom whitelists override blacklists and mitigate false positives.

QUESTION 164
If a switch port goes directly into a blocked state only when a superior BPDU is received, what mechanism must be in use?

A. STP BPDU guard
B. loop guard
C. STP Root guard
D. EtherChannel guard

Answer: C
Explanation:
Root guard allows the device to participate in STP as long as the device does not try to become the root. If root guard blocks the port, subsequent recovery is automatic. Recovery occurs as soon as the offending device ceases to send superior BPDUs.
Source: http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html

QUESTION 165
Which feature filters CoPP packets?

A. Policy maps
B. route maps
C. access control lists
D. class maps

Answer: C

QUESTION 166
In which type of attack does an attacker send email message that ask the recipient to click a link such as https://www.cisco.net.cc/securelogs?

A. pharming
B. phishing
C. solicitation
D. secure transaction

Answer: B

QUESTION 167
If the router ospf 200 command, what does the value 200 stands for?

A. Administrative distance value

B. process ID
C. area ID.
D. ABR ID

Answer: B
Explanation:
Recall that the area is defined in the following command:
hostname(config-router)# network 10.0.0.0 255.0.0.0 area 0

QUESTION 168
Your security team has discovered a malicious program that has been harvesting the CEO's email messages and the company's user database for the last 6 months.
What type of attack did your team discover? (Choose two.)

A. social activism
B. drive-by spyware
C. targeted malware
D. advance persistent threat
E. polymorphic Virus

Answer: CD

QUESTION 169
What is the best way to confirm that AAA authentication is working properly?

A. use the test aaa command
B. use the Cisco-recommended configuration for AAA authentication
C. Log into and out of the router, and then check the NAS authentication log
D. Ping the NAS to confirm connectivity

Answer: A
Explanation:
The other choices do not verify functionality.
There is a test aaa command in IOS, just tried it in my lab:
R1#test aaa group radius admin cisco123 new-code
User successfully authenticated
USER ATTRIBUTES

QUESTION 170
What is the benefit of web application firewall?

A. It accelerate web traffic
B. It blocks know vulnerabilities without patching applications
C. It supports all networking protocols.
D. It simplifies troubleshooting

Answer: B

QUESTION 171

What improvement does EAP-FASTv2 provide over EAP-FAST?

A. It support more secure encryption protocols.
B. It allows multiple credentials to be passed in a single EAP exchange
C. It addresses security vulnerabilities found in the original protocol.
D. It allows faster authentication by using fewer packets.

Answer: B
Explanation:
EAP Chaining with EAP-FASTv2: As an enhancement to EAP-FAST, a differentiation was made to have a User PAC and a Machine PAC. After a successful machine-authentication, ISE will issue a Machine-PAC to the client. Then, when processing a user-authentication, ISE will request the Machine-PAC to prove that the machine was successfully authenticated, too. This is the first time in 802.1X history that multiple credentials have been able to be authenticated within a single EAP transaction, and it is known as “EAP Chaining.”

QUESTION 172
Which statement about IOS privilege levels is true?

A. Each privilege level is independent of all other privilege levels.
B. Each privilege level supports the commands at its own level and all levels above it.
C. Each privilege level supports the commands at its own level and all levels below it.
D. Privilege-level commands are set explicitly for each user.

Answer: C

QUESTION 173
What mechanism does asymmetric cryptography use to secure data?

A. an RSA nonce
B. a public/private key pair.
C. an MD5 hash.
D. shared secret keys.

Answer: B

QUESTION 174
Which statement about application blocking is true?

A. Block access to specific program.
B. Block access to specific network addresses.
C. Block access to specific network services
D. Block access to files with specific extensions.

Answer: A

QUESTION 175
What are the three layers of a hierarchical network design? (Choose three.)

A. core
B. access
C. server
D. user
E. internet
F. distribution

Answer: ABF

QUESTION 176
In which type of attack does the attacker attempt to overload the CAM table on a switch so that the switch acts as a hub?

A. gratuitous ARP
B. MAC flooding
C. MAC spoofing
D. DoS

Answer: B
Explanation:
Switch goes into fail-open mode, becomes a hub.

QUESTION 177
Refer to the exhibit. With which NTP server has the router synchronized?

```
209.114.111.1 configured, ipv4, sane, valid, stratum 2
ref ID 132.163.4.103  , time D7AD124D.9D6FC576 (03:17:33.614 UTC Sun Aug 31 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 46.34 msec, root disp 23.52, reach 1, sync dist 268.59
delay 63.27 msec, offset 7.9817 msec, dispersion 187.56, jitter 2.07 msec
precision 2**23, version 4

204.2.134.164 configured, ipv4, sane, valid, stratum 2
ref ID 241.199.164.101, time D7AD1419.9EB5272B (03:25:13.619 UTC Sun Aug 31 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 256
root delay 30.83 msec, root disp 4.88, reach 1, sync dist 223.80
delay 28.69 msec, offset 6.4331 msec, dispersion 187.55, jitter 1.39 msec
precision 2**20, version 4

192.168.10.7 configured, ipv4, our_master, sane, valid, stratum 3
ref ID 108.61.73.243  , time D7AD0D8F.AE79A23A (02:57:19.681 UTC Sun Aug 31 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 86.45 msec, root disp 87.82, reach 377, sync dist 134.25
delay 0.89 msec, offset 19.5087 msec, dispersion 1.69, jitter 0.84 msec
precision 2**32, version 4
```

A. 192.168.10.7
B. 108.61.73.243
C. 209.114.111.1
D. 204.2.134.164
E. 132.163.4.103

F. 241.199.164.101

Answer: A
Explanation:
Because you have to refer to our_master , which is only showing on 192.168.10.07. on the rest of them you nothing showing.
"our_master" term lists selected synchronization server at the beginning of the line.

QUESTION 178
What are two ways to protect eavesdropping when you perform device-management task? (Choose two)

A. use SNMPv2
B. use SSH connection
C. use SNMPv3
D. use in-band management
E. use out-band management

Answer: BC
Explanation:
These management plane protocols are encrypted.

QUESTION 179
Which firewall configuration must you perform to allow traffic to flow in both directions between two zones?

A. You can configure a single zone pair that allows bidirectional traffic flows from for any zone except the self-zone
B. You must configure two zone pairs, one for each direction
C. You can configure a single zone pair that allows bidirectional traffic flows for any zone
D. You can configure a single zone pair that allows bidirectional traffic flows only if the source zone is the less secure zone.

Answer: B
Explanation:
A single zone pair is NOT bidirectional, so you must have two pairs to cover both directions.

QUESTION 180
Which three ways does the RADIUS protocol differ from TACACS?? (Choose three)

A. RADIUS authenticates and authorizes simultaneously. Causing fewer packets to be transmitted
B. RADIUS encrypts only the password field in an authentication packets
C. RADIUS can encrypt the entire packet that is sent to the NAS
D. RADIUS uses UDP to communicate with the NAS
E. RADIUS uses TCP to communicate with the NAS
F. RADIUS support per-command authentication

Answer: ABD
Explanation:
TACACS+ encypts the entire body of the packet and supports per-command-authentication for

greater granularity.

QUESTION 181
A data breach has occurred and your company database has been copied. Which security principle has been violated?

A. Confidentiality
B. Access
C. Control
D. Availability

Answer: A

QUESTION 182
If a switch receives a superior BPDU and goes directly into a blocked state, what mechanism must be in use?

A. BPDU guard
B. Root guard
C. EherCahannel guard
D. Loop guard

Answer: B

QUESTION 183
What is the primary purposed of a defined rule in an IPS?

A. to detect internal attacks
B. to define a set of actions that occur when a specific user logs in to the system
C. to configure an event action that is pre-defined by the system administrator
D. to configure an event action that takes place when a signature is triggered.

Answer: D

QUESTION 184
How does PEAP protect EAP exchange?

A. it encrypts the exchange using the client certificate.
B. it validates the server-supplied certificate and then encrypts the exchange using the client certificate
C. it encrypts the exchange using the server certificate
D. it validates the client-supplied certificate and then encrypts the exchange using the server certificate.

Answer: C
Explanation:
The client certificate is not used for encryption with PEAP.

QUESTION 185
How can firepower block malicious email attachments?

A. It forwards email requests to an external signature engine
B. It sends the traffic through a file policy
C. It scans inbound email messages for known bad URLs
D. It sends an alert to the administrator to verify suspicious email messages

Answer: B

QUESTION 186
A proxy firewall protects against which type of attacks?

A. DDoS
B. port scanning
C. worm traffic
D. cross-site scripting attacks

Answer: D

QUESTION 187
Which three statements are characteristics of DHCP Spoofing? (Choose three.)

A. Arp Poisoning
B. Modify Traffic in transit
C. Used to perform man-in-the-middle attack
D. Physically modify the network gateway
E. Protect the identity of the attacker by masking the DHCP address
F. Can access most network devices

Answer: ABC
Explanation:
DHCP spoofing occurs when an attacker attempts to respond to DHCP requests and trying to list themselves (spoofs) as the default gateway or DNS server, hence, initiating a man in the middle attack. With that, it is possible that they can intercept traffic from users before forwarding to the real gateway or perform DoS by flooding the real DHCP server with request to choke ip address resources.
https://learningnetwork.cisco.com/thread/67229
https://learningnetwork.cisco.com/docs/DOC-24355

ARP (Address Resolution Protocol) Poisoning (MITM) Attack: Scenario 2 and 3 explain how DHCP spoofing uses ARP poisoning to accomplish a MITM attack.
https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_603839.html

QUESTION 188
In which two situations should you use in-band management? (Choose two)

A. when a network device fails to forward packets
B. when management applications need concurrent access to the device

C. when you require ROMMON access
D. when you require administrator's access from multiple locations
E. when the control plane fails to respond

Answer: BD

QUESTION 189
Which three statements describe DHCP spoofing attacks? (Choose three.)

A. They can modify traffic in transit.
B. They are used to perform man-in-the-middle attacks.
C. They use ARP poisoning.
D. They can access most network devices.
E. They protect the identity of the attacker by masking the DHCP address.
F. They are can physically modify the network gateway.

Answer: ABC
Explanation:
DHCP spoofing occurs when an attacker attempts to respond to DHCP requests and trying to list themselves (spoofs) as the default gateway or DNS server, hence, initiating a man in the middle attack. With that, it is possible that they can intercept traffic from users before forwarding to the real gateway or perform DoS by flooding the real DHCP server with request to choke ip address resources.
https://learningnetwork.cisco.com/thread/67229
https://learningnetwork.cisco.com/docs/DOC-24355

QUESTION 190
What security feature allows a private IP address to access the Internet by translating it to a public address?

A. NAT
B. hairpinning
C. Trusted Network Detection
D. Certification Authority

Answer: A

QUESTION 191
Which Sourcefire event action should you choose if you want to block only malicious traffic from a particular end user?

A. Allow with inspection
B. Allow without inspection
C. Block
D. Trust
E. Monitor

Answer: A

QUESTION 192
Which two NAT types allows only objects or groups to reference an IP address? (choose two)

A. dynamic NAT
B. dynamic PAT
C. static NAT
D. identity NAT

Answer: AC
Explanation:
Adding Network Objects for Mapped Addresses
For dynamic NAT, you must use an object or group for the mapped addresses. Other NAT types have the option of using inline addresses, or you can create an object or group according to this section.
* Dynamic NAT:
+ You cannot use an inline address; you must configure a network object or group.
+ The object or group cannot contain a subnet; the object must define a range; the group can include hosts and ranges.
+ If a mapped network object contains both ranges and host IP addresses, then the ranges are used for dynamic NAT, and then the host IP addresses are used as a PAT fallback.
* Dynamic PAT (Hide):
+ Instead of using an object, you can optionally configure an inline host address or specify the interface address.
+ If you use an object, the object or group cannot contain a subnet; the object must define a host, or for a PAT pool, a range; the group (for a PAT pool) can include hosts and ranges.
* Static NAT or Static NAT with port translation:
+ Instead of using an object, you can configure an inline address or specify the interface address (for static NAT-with-port-translation).
+ If you use an object, the object or group can contain a host, range, or subnet.
* Identity NAT
+ Instead of using an object, you can configure an inline address.
+ If you use an object, the object must match the real addresses you want to translate.
http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/nat_objects.html#61711

QUESTION 193
Which feature allows a dynamic PAT pool to select the next address in the PAT pool instead of the next port of an existing address?

A. next IP
B. round robin
C. dynamic rotation
D. NAT address rotation

Answer: B

QUESTION 194
Which line in the following OSPF configuration will not be required for MD5 authentication to work?

```
interface GigabitEthernet0/1
ip address 192.168.10.1 255.255.255.0
ip ospf authentication message-digest
```

```
ip ospf message-digest-key 1 md5 CCNA
!
router ospf 65000
router-id 192.168.10.1
area 20 authentication message-digest
network 10.1.1.0 0.0.0.255 area 10
network 192.168.10.0 0.0.0.255 area 0
!
```

A. ip ospf authentication message-digest
B. network 192.168.10.0 0.0.0.255 area 0
C. area 20 authentication message-digest
D. ip ospf message-digest-key 1 md5 CCNA

Answer: C

QUESTION 195
Which of the following pairs of statements is true in terms of configuring MD authentication?

A. Interface statements (OSPF, EIGRP) must be configured; use of key chain in OSPF
B. Router process (OSPF, EIGRP) must be configured; key chain in EIGRP
C. Router process (only for OSPF) must be configured; key chain in EIGRP
D. Router process (only for OSPF) must be configured; key chain in OSPF

Answer: C

QUESTION 196
Which component of CIA triad relate to safe data which is in transit.

A. Confidentiality
B. Integrity
C. Availability
D. Scalability

Answer: B
Explanation:
Integrity: Integrity for data means that changes made to data are done only by authorized individuals/systems.
Corruption of data is a failure to maintain data integrity.

QUESTION 197
Which command help user1 to use enable,disable,exit&etc commands?

A. catalyst1(config)#username user1 privilege 0 secret us1pass
B. catalyst1(config)#username user1 privilege 1 secret us1pass
C. catalyst1(config)#username user1 privilege 2 secret us1pass
D. catalyst1(config)#username user1 privilege 5 secret us1pass

Answer: A
Explanation:

To understand this example, it is necessary to understand privilege levels.
By default, there are three command levels on the router:
+ privilege level 0 -- Includes the disable, enable, exit, help, and logout commands.
+ privilege level 1 -- Normal level on Telnet; includes all user-level commands at the router> prompt.
+ privilege level 15 -- Includes all enable-level commands at the router# prompt.
http://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/23383-showrun.html

QUESTION 198
Command ip ospf authentication key 1 is implemented in which level.

A. Interface
B. process
C. global
D. enable

Answer: A
Explanation:
Use the ip ospf authentication-key interface command to specify this password. If you enable MD5 authentication with the message-digest keyword, you must configure a password with the ip ospf message- digest-key interface command.
interface GigabitEthernet0/1
ip address 192.168.10.1 255.255.255.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 CCNA
Cisco Official Certification Guide, Implement Routing Update Authentication on OSPF, p.348 The OSPFv2 Cryptographic Authentication feature allows you to configure a key chain on the OSPF interface to authenticate OSPFv2 packets by using HMAC-SHA algorithms. You can use an existing key chain that is being used by another protocol, or you can create a key chain specifically for OSPFv2.
If OSPFv2 is configured to use a key chain, all MD5 keys that were previously configured using the ip ospf message-digest-key command are ignored.
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet0/0/0
Device (config-if)# ip ospf authentication key-chain sample1
Device (config-if)# end
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-3s/iro-xe-3s-book/iro-ospfv2-crypto-authen-xe.html
In both cases OSPF and OSPFv1 the ip ospf authentication is inserted at interface level

QUESTION 199
Which are two valid TCP connection states (pick 2) is the gist of the question.

A. SYN-RCVD
B. Closed
C. SYN-WAIT
D. RCVD
E. SENT

Answer: AB

Explanation:
TCP Finite State Machine (FSM) States, Events and Transitions + CLOSED: This is the default state that each connection starts in before the process of establishing it begins.
The state is called "fictional" in the standard.
+ LISTEN
+ SYN-SENT
+ SYN-RECEIVED: The device has both received a SYN (connection request) from its partner and sent its own SYN. It is now waiting for an ACK to its SYN to finish connection setup.
+ ESTABLISHED
+ CLOSE-WAIT
+ LAST-ACK
+ FIN-WAIT-1
+ FIN-WAIT-2
+ CLOSING
+ TIME-WAIT
http://tcpipguide.com/free/t_TCPOperationalOverviewandtheTCPFiniteStateMachineF-2.htm

QUESTION 200
Which of the following commands result in a secure bootset? (Choose all that apply.)

A. secure boot-set
B. secure boot-config
C. secure boot-files
D. secure boot-image

Answer: BD

QUESTION 201
What is example of social engineering

A. Gaining access to a building through an unlocked door.
B. something about inserting a random flash drive.
C. gaining access to server room by posing as IT
D. watching you enter your user and password on a network computer (something to that effect)

Answer: C

QUESTION 202
Which port should (or would) be open if VPN NAT-T was enabled?

A. port 4500 outside interface
B. port 4500 in all interfaces where ipsec uses
C. port 500
D. port 500 outside interface

Answer: B
Explanation:
NAT traversal: The encapsulation of IKE and ESP in UDP port 4500 enables these protocols to pass through a device or firewall performing NAT.
https://en.wikipedia.org/wiki/Internet_Key_Exchange
https://supportforums.cisco.com/document/64281/how-does-nat-t-work-ipsec

QUESTION 203
Diffie-Hellman key exchange question

A. IKE
B. IPSEC
C. SPAN
D. STP

Answer: A
Explanation:
https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

QUESTION 204
Security well known terms Choose 2

A. Trojan
B. Phishing
C. Something LC
D. Ransomware

Answer: BD
Explanation:
The following are the most common types of malicious software:
+ Computer viruses
+ Worms
+ Mailers and mass-mailer worms
+ Logic bombs
+ Trojan horses
+ Back doors
+ Exploits
+ Downloaders
+ Spammers
+ Key loggers
+ Rootkits
+ Ransomware

QUESTION 205
What's the technology that you can use to prevent non malicious program to run in the computer that is disconnected from the network?

A. Firewall
B. Software Antivirus
C. Network IPS
D. Host IPS.

Answer: D

QUESTION 206
Which command do you enter to configure your firewall to conceal internal addresses?

A. no ip inspect audit-trail
B. no ip inspect
C. no ip directed-broadcast
D. no ip source-route
E. no proxy-arp
F. no ip logging facility

Answer: E
Explanation:
The Cisco IOS software uses proxy ARP (as defined in RFC 1027) to help hosts with no knowledge of routing determine the media addresses of hosts on other networks or subnets. For example, if the router receives an ARP request for a host that is not on the same interface as the ARP request sender, and if the router has all of its routes to that host through other interfaces, then it generates a proxy ARP reply packet giving its own local data-link address. The host that sent the ARP request then sends its packets to the router, which forwards them to the intended host. Proxy ARP is enabled by default.
Router(config-if)# ip proxy-arp - Enables proxy ARP on the interface.
http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfipadr.html#wp1001233

QUESTION 207
Which statement about college campus is true?

A. College campus has geographical position.
B. College campus Hasn`t got internet access.
C. College campus Has multiple subdomains.

Answer: A

QUESTION 208
Which firepower preprocessor block traffic based on IP?

A. Signature-Based
B. Policy-Based
C. Anomaly-Based
D. Reputation-Based

Answer: D
Explanation:
Access control rules within access control policies exert granular control over network traffic logging and handling. Reputation-based conditions in access control rules allow you to manage which traffic can traverse your network, by contextualizing your network traffic and limiting it where appropriate. Access control rules govern the following types of reputation-based control:
+ Application conditions allow you to perform application control, which controls application traffic based on not only individual applications, but also applications' basic characteristics: type, risk, business relevance, categories, and tags.
+ URL conditions allow you to perform URL filtering, which controls web traffic based on individual websites, as well as websites' system-assigned category and reputation.
The ASA FirePOWER module can perform other types of reputation-based control, but you do not configure these using access control rules. For more information, see:

+ Blacklisting Using Security Intelligence IP Address Reputation explains how to limit traffic based on the reputation of a connection's origin or destination as a first line of defense.
+ Tuning Intrusion Prevention Performance explains how to detect, track, store, analyze, and block the transmission of malware and other types of prohibited files.
http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/AC-Rules-App-URL-Reputation.html

QUESTION 209
Which two NAT types allow only objects or groups to reference an IP address? (Choose two)

A. dynamic NAT
B. dynamic PAT
C. static NAT
D. identity NAT

Answer: AC
Explanation:
Adding Network Objects for Mapped Addresses
For dynamic NAT, you must use an object or group for the mapped addresses. Other NAT types have the option of using inline addresses, or you can create an object or group according to this section.
* Dynamic NAT:
+ You cannot use an inline address; you must configure a network object or group.
+ The object or group cannot contain a subnet; the object must define a range; the group can include hosts and ranges.
+ If a mapped network object contains both ranges and host IP addresses, then the ranges are used for dynamic NAT, and then the host IP addresses are used as a PAT fallback.
* Dynamic PAT (Hide):
+ Instead of using an object, you can optionally configure an inline host address or specify the interface address.
+ If you use an object, the object or group cannot contain a subnet; the object must define a host, or for a PAT pool, a range; the group (for a PAT pool) can include hosts and ranges.
* Static NAT or Static NAT with port translation:
+ Instead of using an object, you can configure an inline address or specify the interface address (for static NAT-with-port-translation).
+ If you use an object, the object or group can contain a host, range, or subnet.
* Identity NAT
+ Instead of using an object, you can configure an inline address.
+ If you use an object, the object must match the real addresses you want to translate.
http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/nat_objects.html#61711

QUESTION 210
What port option in a PVLAN that can communicate with every other ports...

A. Promiscuous..
B. Community ports
C. Ethernet ports
D. Isolate ports

Answer: A
Explanation:

+ Promiscuous -- A promiscuous port belongs to the primary VLAN. The promiscuous port can communicate with all interfaces, including the community and isolated host ports, that belong to those secondary VLANs associated to the promiscuous port and associated with the primary VLAN.
+ Isolated -- An isolated port is a host port that belongs to an isolated secondary VLAN. This port has complete isolation from other ports within the same private VLAN domain, except that it can communicate with associated promiscuous ports
+ Community -- A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with associated promiscuous ports
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.html

QUESTION 211
Which command enable ospf authentication **on an interface**?

A. ip ospf authentication message-digest
B. network 192.168.10.0 0.0.0.255 area 0
C. area 20 authentication message-digest
D. ip ospf message-digest-key 1 md5 CCNA

Answer: A
Explanation:
This question might be incomplete. Both ip ospf authentication message-digest and area 20 authentication message-digest command enable OSPF authentication through MD5.
Use the ip ospf authentication-key interface command to specify this password. If you enable MD5 authentication with the message-digest keyword, you must configure a password with the ip ospf message- digest-key interface command.
interface GigabitEthernet0/1
ip address 192.168.10.1 255.255.255.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 CCNA
Cisco Official Certification Guide, Implement Routing Update Authentication on OSPF, p.348 To enable authentication for an OSPF area, use the area authentication command in router configuration mode.
To remove an authentication specification of an area or a specified area from the configuration, use the no form of this command.
area area-id authentication [message-digest]
no area area-id authentication [message-digest]
http://www.cisco.com/c/en/us/td/docs/ios/12_2/iproute/command/reference/fiprrp_r/1rfospf.html
https://supportforums.cisco.com/document/22961/ospf-authentication

QUESTION 212
Which NAT option is executed first during in case of multiple nat translations?

A. dynamic nat with shortest prefix
B. dynamic nat with longest prefix
C. static nat with shortest prefix
D. static nat with longest prefix

Answer: D

QUESTION 213
Which security term refers to a person, property, or data of value to a company?

A. Risk
B. Asset
C. Threat prevention
D. Mitigation technique

Answer: B

QUESTION 214
Which option is a weakness in an information system that an attacker might leverage to gain unauthorized access to the system or its data?

A. hack
B. mitigation
C. risk
D. vulnerability
E. exploit

Answer: D
Explanation:
A flaw or weakness in a system's design or implementation that could be exploited.

QUESTION 215
What show command can see vpn tunnel establish with traffic passing through?

A. show crypto ipsec sa
B. show crypto session
C. show crypto isakmp sa
D. show crypto ipsec transform-set

Answer: A
Explanation:
#show crypto ipsec sa - This command shows IPsec SAs built between peers In the output you see
#pkts encaps: 345, #pkts encrypt: 345, #pkts digest 0
#pkts decaps: 366, #pkts decrypt: 366, #pkts verify 0
which means packets are encrypted and decrypted by the IPsec peer.
http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html#ipsec_sa

QUESTION 216
Which will auto-nat process first (the focus is on auto-nat)?

A. dynamic Nat shortest prefix
B. dynamic nat longest prefix
C. static nat shortest prefix
D. static nat longest prefix

Answer: D

QUESTION 217
Where OAKLEY and SKEME come to play?

A. IKE
B. ISAKMP
C. DES

Answer: A
Explanation:
The Oakley Key Determination Protocol is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the DiffieHellman key exchange algorithm.
The protocol was proposed by Hilarie K. Orman in 1998, and formed the basis for the more widely used Internet key exchange protocol
https://en.wikipedia.org/wiki/Oakley_protocol
IKE (Internet Key Exchange)
A key management protocol standard that is used in conjunction with the IPSec standard. IPSec is an IP security feature that provides robust authentication and encryption of IP packets. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside of the Internet Security Association and Key Management Protocol (ISAKMP) framework.
ISAKMP, Oakley, and Skeme are security protocols implemented by IKE
https://www.symantec.com/security_response/glossary/define.jsp?letter=i&word=ike-internet-key-exchange

QUESTION 218
What does the key length represent

A. Hash block size
B. Cipher block size
C. Number of permutations

Answer: C
Explanation:
In cryptography, an algorithm's key space refers to the set of all possible permutations of a keys. If a key were eight bits (one byte) long, the keyspace would consist of 28 or 256 possible keys. Advanced Encryption Standard (AES) can use a symmetric key of 256 bits, resulting in a key space containing 2256 (or 1.1579 × 1077) possible keys.
https://en.wikipedia.org/wiki/Key_space_(cryptography)

QUESTION 219
Which type of attack is directed against the network directly?

A. Denial of Service
B. phishing
C. trojan horse

Answer: A

Explanation:
Denial of service refers to willful attempts to disrupt legitimate users from getting access to the resources they intend to. Although no complete solution exists, administrators can do specific things to protect the network from a DoS attack and to lessen its effects and prevent a would-be attacker from using a system as a source of an attack directed at other systems. These mitigation techniques include filtering based on bogus source IP addresses trying to come into the networks and vice versa. Unicast reverse path verification is one way to assist with this, as are access lists. Unicast reverse path verification looks at the source IP address as it comes into an interface, and then looks at the routing table. If the source address seen would not be reachable out of the same interface it is coming in on, the packet is considered bad, potentially spoofed, and is dropped.

QUESTION 220
With which technology do apply integrity, confidentially and authenticate the source

A. IPSec
B. IKE
C. Certificate authority
D. Data encryption standards

Answer: A
Explanation:
IPsec is a collection of protocols and algorithms used to protect IP packets at Layer 3 (hence the name of IP Security [IPsec]). IPsec provides the core benefits of confidentiality through encryption, data integrity through hashing and HMAC, and authentication using digital signatures or using a pre-shared key (PSK) that is just for the authentication, similar to a password.

QUESTION 221
With which type of Layer 2 attack can you intercept traffic that is destined for one host?

A. MAC spoofing
B. CAM overflow

Answer: A

QUESTION 222
Which command can you enter to verify the statistics of cisco IOS resilent configuration on cisco router?

A. Show binary file
B. Show secure boot-set
C. Secure boot-config
D. Secure boot-image

Answer: D

QUESTION 223
What are the challenges faced when deploying host based IPS?

A. Must support multi operating systems

B. Does not have full network picture

Answer: AB
Explanation:
Advantages of HIPS: The success or failure of an attack can be readily determined. A network IPS sends an alarm upon the presence of intrusive activity but cannot always ascertain the success or failure of such an attack. HIPS does not have to worry about fragmentation attacks or variable Time to Live (TTL) attacks because the host stack takes care of these issues. If the network traffic stream is encrypted, HIPS has access to the traffic in unencrypted form.
Limitations of HIPS: There are two major drawbacks to HIPS:
+ HIPS does not provide a complete network picture : Because HIPS examines information only at the local host level, HIPS has difficulty constructing an accurate network picture or coordinating the events happening across the entire network.
+ HIPS has a requirement to support multiple operating systems: HIPS needs to run on every system in the network. This requires verifying support for all the different operating systems used in your network.
http://www.ciscopress.com/articles/article.asp?p=1336425&seqNum=3

QUESTION 224
What encryption technology has broadest platform support

A. hardware
B. middleware
C. Software
D. File level

Answer: C

QUESTION 225
With which preprocesor do you detect incomplete TCP handshakes

A. rate based prevention
B. port scan detection

Answer: A
Explanation:
Rate-based attack prevention identifies abnormal traffic patterns and attempts to minimize the impact of that traffic on legitimate requests. Rate-based attacks usually have one of the following characteristics:
+ any traffic containing excessive incomplete connections to hosts on the network, indicating a SYN flood attack
+ any traffic containing excessive complete connections to hosts on the network, indicating a TCP/IP connection flood attack
+ excessive rule matches in traffic going to a particular destination IP address or addresses or coming from a particular source IP address or addresses.
+ excessive matches for a particular rule across all traffic.
http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-Threat-Detection.html

QUESTION 226
Which type of PVLAN port allows a host in the same VLAN to communicate only with promiscuous hosts?

A. Community host in the PVLAN
B. Isolated host in the PVLAN
C. Promiscuous host in the PVLAN
D. Span for host in the PVLAN

Answer: B
Explanation:
The types of private VLAN ports are as follows:
+ Promiscuous - The promiscuous port can communicate with all interfaces, including the community and isolated host ports, that belong to those secondary VLANs associated to the promiscuous port and associated with the primary VLAN
+ Isolated - This port has complete isolation from other ports within the same private VLAN domain, except that it can communicate with associated promiscuous ports.
+ Community -- A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with associated promiscuous ports.
These interfaces are isolated from all other interfaces in other communities and from all isolated ports within the private VLAN domain.
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.html#42874

QUESTION 227
Which type of encryption technology has the broadcast platform support?

A. Middleware
B. Hardware
C. Software
D. File-level

Answer: C

QUESTION 228
The first layer of defense which provides real-time preventive solutions against malicious traffic is provided by?

A. Banyan Filters
B. Explicit Filters
C. Outbreak Filters

Answer: C

QUESTION 229
SSL certificates are issued by Certificate Authority(CA) are?

A. Trusted root
B. Not trusted

Answer: A

QUESTION 230
SYN flood attack is a form of?

A. Reconnaissance attack
B. Denial of Service attack
C. Man in the middle attack
D. Spoofing attack

Answer: B
Explanation:
A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.
https://en.wikipedia.org/wiki/SYN_flood

QUESTION 231
The command debug crypto isakmp results in ?

A. Troubleshooting ISAKMP (Phase 1) negotiation problems

Answer: A
Explanation:
#debug crypto isakmp
This output shows an example of the debug crypto isakmp command.
processing SA payload. message ID = 0
Checking ISAKMP transform against priority 1 policy
encryption 3DES
hash SHA
default group 2
auth pre-share
life type in seconds
life duration (basic) of 240
atts are acceptable. Next payload is 0
processing KE payload. message ID = 0
processing NONCE payload. message ID = 0
processing ID payload. message ID = 0
SKEYID state generated
processing HASH payload. message ID = 0
SA has been authenticated
processing SA payload. message ID = 800032287
Contains the IPsec Phase1 information.
You can view the HAGLE (Hash, Authentication, DH Group, Lifetime, Encryption) process in the output

QUESTION 232
Which prevent the company data from modification even when the data is in transit?

A. Confidentiality
B. Integrity
C. Vailability
D. Scalability

Answer: B
Explanation:
Integrity: Integrity for data means that changes made to data are done only by authorized individuals/systems.
Corruption of data is a failure to maintain data integrity.

QUESTION 233
The stealing of confidential information of a company comes under the scope of

A. Reconnaissance
B. Spoofing attack
C. Social Engineering
D. Denial of Service

Answer: C
Explanation:
Social engineering
This is a tough one because it leverages our weakest (very likely) vulnerability in a secure system (data, applications, devices, networks): the user. If the attacker can get the user to reveal information, it is much easier for the attacker than using some other method of reconnaissance. This could be done through e-mail or misdirection of web pages, which results in the user clicking something that leads to the attacker gaining information. Social engineering can also be done in person or over the phone.

QUESTION 234
The Oakley cryptography protocol is compatible with following for managing security?

A. IPSec
B. ISAKMP
C. Port security

Answer: B
Explanation:
IKE (Internet Key Exchange)
A key management protocol standard that is used in conjunction with the IPSec standard. IPSec is an IP security feature that provides robust authentication and encryption of IP packets. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside of the Internet Security Association and Key Management Protocol (ISAKMP) framework.
ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.
https://www.symantec.com/security_response/glossary/define.jsp?letter=i&word=ike-internet-key-exchange

QUESTION 235
Which two features of Cisco Web Reputation tracking can mitigate web-based threats? (Choose Two)

A. outbreak filter
B. buffer overflow filter
C. bayesian overflow filter

D. web reputation filter
E. exploit filtering

Answer: AE

QUESTION 236
I had the "nested" question (wording has been different). Two answers ware related to hierarchy:

A. there are only two levels of hierarchy possible
B. the higher level hierarchy becomes the parent for lower one parent
C. inspect something is only possible with in a hierachy...
D. some command question....

Answer: C

QUESTION 237
Which statement about command authorization and security contexts is true?

A. If command authorization is configured, it must be enabled on all contexts
B. The changeto command invokes a new context session with the credentials of the currently logged-in user
C. AAA settings are applied on a per-context basis
D. The enable_15 user and admins with changeto permissions have different command authorization levels per context

Answer: B
Explanation:
The capture packet function works on an individual context basis. The ACE traces only the packets that belong to the context where you execute the capture command. You can use the context ID, which is passed with the packet, to isolate packets that belong to a specific context. To trace the packets for a single specific context, use the changeto command and enter the capture command for the new context.
To move from one context on the ACE to another context, use the changeto command Only users authorized in the admin context or configured with the changeto feature can use the changeto command to navigate between the various contexts. Context administrators without the changeto feature, who have access to multiple contexts, must explicitly log in to the other contexts to which they have access.
http://www.cisco.com/c/en/us/td/docs/interfaces_modules/services_modules/ace/vA5_1_0/command/ reference/ACE_cr/execmds.html

QUESTION 238
Unicast Reverse Path Forwarding definition:

A. See the explanation

Answer: A
Explanation:
Unicast Reverse Path Forwarding
Unicast Reverse Path Forwarding (uRPF) can mitigate spoofed IP packets. When this feature is enabled on an interface, as packets enter that interface the router spends an extra moment considering the source address of the packet. It then considers its own routing table, and if the

routing table does not agree that the interface that just received this packet is also the best egress interface to use for forwarding to the source address of the packet, it then denies the packet.

QUESTION 239
The NAT traversal definition:

A. See the explanation

Answer: A
Explanation:
NAT-T (NAT Traversal)
If both peers support NAT-T, and if they detect that they are connecting to each other through a Network Address Translation (NAT) device (translation is happening), they may negotiate that they want to put a fake UDP port 4500 header on each IPsec packet (before the ESP header) to survive a NAT device that otherwise may have a problem tracking an ESP session (Layer 4 protocol 50).
https://supportforums.cisco.com/document/64281/how-does-nat-t-work-ipsec

QUESTION 240
Man-in-the-middle attack definition:

A. See the explanation

Answer: A
Explanation:
Man-in-the-middle attacks: Someone or something is between the two devices who believe they are communicating directly with each other. The "man in the middle" may be eavesdropping or actively changing the data that is being sent between the two parties. You can prevent this by implementing Layer 2 dynamic ARP inspection (DAI) and Spanning Tree Protocol (STP) guards to protect spanning tree. You can implement it at Layer 3 by using routing protocol authentication. Authentication of peers in a VPN is also a method of preventing this type of attack.

QUESTION 241
Which privileged level is ... by default? for user exec mode

A. 0
B. 1
C. 2
D. 5
E. 15

Answer: B
Explanation:
User EXEC mode commands are privilege level 1
Privileged EXEC mode and configuration mode commands are privilege level 15.
http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/fsecur_r/srfpass.html

QUESTION 242
When is "Deny all" policy an exception in Zone Based Firewall

A. traffic traverses 2 interfaces in same zone
B. traffic sources from router via self zone
C. traffic terminates on router via self zone
D. traffic traverses 2 interfaces in different zones
E. traffic terminates on router via self zone

Answer: A
Explanation:
+ There is a default zone, called the self zone, which is a logical zone. For any packets directed to the router directly (the destination IP represents the packet is for the router), the router automatically considers that traffic to be entering the self zone. In addition, any traffic initiated by the router is considered as leaving the self zone.
By default, any traffic to or from the self zone is allowed, but you can change this policy.
+ For the rest of the administrator-created zones, no traffic is allowed between interfaces in different zones.
+ For interfaces that are members of the same zone, all traffic is permitted by default.

QUESTION 243
Cisco Resilient Configuration Feature:

A. Required additional space to store IOS image file
B. Remote storage required to save IOS image
C. Can be disabled ...remote session
D. Automatically detects image or config.version missmatch

Answer: D
Explanation:
The following factors were considered in the design of Cisco IOS Resilient Configuration:
+ The configuration file in the primary bootset is a copy of the running configuration that was in the router when the feature was first enabled.
+ The feature secures the smallest working set of files to preserve persistent storage space. No extra space is required to secure the primary Cisco IOS image file.
+ The feature automatically detects image or configuration version mismatch .
+ Only local storage is used for securing files, eliminating scalability maintenance challenges from storing multiple images and configurations on TFTP servers.
+ The feature can be disabled only through a console session
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/15-mt/sec-usr-cfg-15-mt-book/sec-resil-config.html

QUESTION 244
What are the two characteristics of IPS?

A. Can drop traffic
B. Does not add delay to traffic
C. It is cabled directly inline
D. Can`t drop packets on its own

Answer: AC
Explanation:
+ Position in the network flow: Directly inline with the flow of network traffic and every packet goes through the sensor on its way through the network.
+ Mode: Inline mode

+ The IPS can drop the packet on its own because it is inline. The IPS can also request assistance from another device to block future packets just as the IDS does.

QUESTION 245
What can cause the state table of a stateful firewall to update? (choose two)

A. when connection is created
B. connection timer expired within state table
C. when packet is evaluated against the inbound access list and is ...
D. outbound packets forwarded to inbound interface
E. when rate limiting is applied

Answer: AB
Explanation:
Stateful inspection monitors incoming and outgoing packets over time, as well as the state of the connection, and stores the data in dynamic state tables. This cumulative data is evaluated, so that filtering decisions would not only be based on administrator-defined rules, but also on context that has been built by previous connections as well as previous packets belonging to the same connection.
Entries are created only for TCP connections or UDP streams that satisfy a defined security policy.
In order to prevent the state table from filling up, sessions will time out if no traffic has passed for a certain period. These stale connections are removed from the state table.
https://en.wikipedia.org/wiki/Stateful_firewall

QUESTION 246
What IPSec mode is used to encrypt traffic between client and server vpn endpoints?

A. tunnel
B. Trunk
C. Aggregated
D. Quick
E. Transport

Answer: E
Explanation:
+ IPSec Transport mode is used for end-to-end communications, for example, for communication between a client and a server or between a workstation and a gateway (if the gateway is being treated as a host). A good example would be an encrypted Telnet or Remote Desktop session from a workstation to a server.
+ IPsec supports two encryption modes: Transport mode and Tunnel mode. Transport mode encrypts only the data portion (payload) of each packet and leaves the packet header untouched. Transport mode is applicable to either gateway or host implementations, and provides protection for upper layer protocols as well as selected IP header fields.
http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html
http://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/2-0/ip_security/provisioning/guide/ IPsecPG1.html
Generic Routing Encapsulation (GRE) is often deployed with IPsec for several reasons, including the following:
+ IPsec Direct Encapsulation supports unicast IP only. If network layer protocols other than IP are to be supported, an IP encapsulation method must be chosen so that those protocols can be transported in IP packets.

+ IPmc is not supported with IPsec Direct Encapsulation. IPsec was created to be a security protocol between two and only two devices, so a service such as multicast is problematic. An IPsec peer encrypts a packet so that only one other IPsec peer can successfully perform the de-encryption. IPmc is not compatible with this mode of operation.
https://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008074f26a.pdf

QUESTION 247
Which command is used to verify VPN connection is operational (or something like that) ?

A. crypto ipsec sa

Answer: A
Explanation:
#show crypto ipsec sa - This command shows IPsec SAs built between peers In the output you see
#pkts encaps: 345, #pkts encrypt: 345, #pkts digest 0
#pkts decaps: 366, #pkts decrypt: 366, #pkts verify 0
which means packets are encrypted and decrypted by the IPsec peer.
http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html#ipsec_sa

QUESTION 248
What is the command to authenticate an NTP time source? (something in those lines)

A. #ntp authentication-key 1 md5 141411050D 7
B. #ntp authenticate
C. #ntp trusted-key 1
D. #ntp trusted-key 1

Answer: B
Explanation:
The command "*ntp authenticate*" authenticates the time source.
The command "*ntp authentication-key*" is the authentication key for trusted time sources.
See the following from a live router:
R1(config)# ntp ?

access-group	Control NTP access
allow	Allow processing of packets
authenticate	Authenticate time sources
authentication-key	Authentication key for trusted time sources

QUESTION 249
How can you allow bidirational traffic? (something in those lines)

A. static NAT
B. dynamic NAT
C. dynamic PAT
D. multi-NAT

Answer: A
Explanation:

Bidirectional initiation--Static NAT allows connections to be initiated bidirectionally, meaning both to the host and from the host.
http://www.cisco.com/c/en/us/td/docs/security/asa/asa83/configuration/guide/config/nat_overview.html

QUESTION 250
Which option is the default value for the Diffie–Hellman group when configuring a site-to-site VPN on an ASA device?

A. Group 1
B. Group 2
C. Group 7
D. Group 5

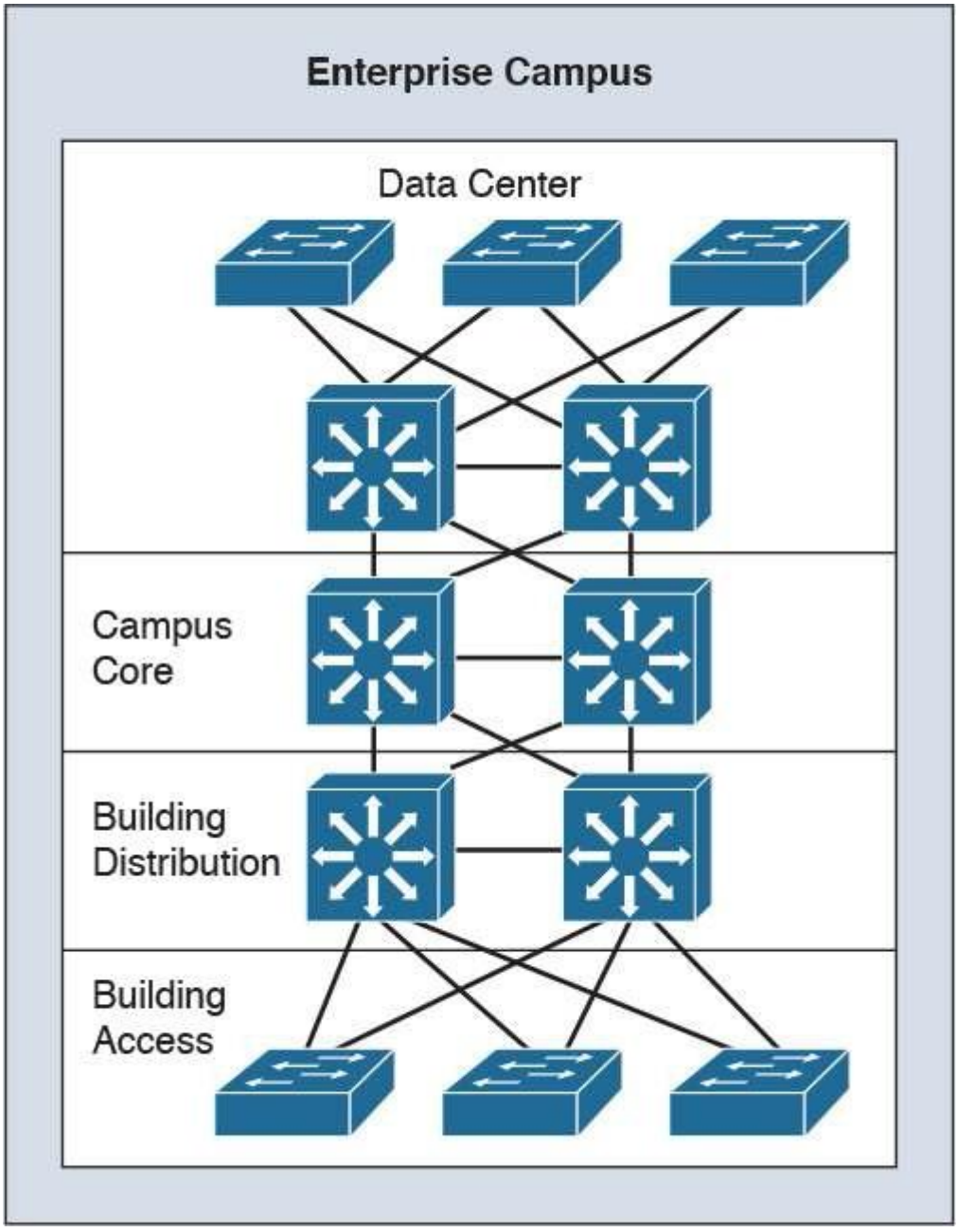
Answer: B

QUESTION 251
What two devices are components of the BYOD architecture framework? (Choose two)

A. Identity Service Engine
B. Cisco 3845 Router
C. Wireless Access Points
D. Nexus 7010 Switch
E. Prime Infrastructure

Answer: AE

QUESTION 252
Where does the Datacenter operate?



A. Distribution
B. Access
C. Core

Answer: A

QUESTION 253
Which option is the cloud based security service from Cisco that provides URL filtering web browsing content security, and roaming user protection?

A. Cloud web security

B. Cloud web Protection
C. Cloud web Service
D. Cloud advanced malware protection

Answer: A

QUESTION 254
Which product can be used to provide application layer protection for TCP port 25 traffic?

A. ESA
B. CWS
C. WSA
D. ASA

Answer: A

QUESTION 255
What is the actual IOS privilege level of User Exec mode?

A. 1
B. 0
C. 5
D. 15

Answer: A
Explanation:
By default, the Cisco IOS software command-line interface (CLI) has two levels of access to commands: **user EXEC mode (level 1)** and privileged EXEC mode (level 15). However, you can configure additional levels of access to commands, called privilege levels, to meet the needs of your users while protecting the system from unauthorized access. Up to 16 privilege levels can be configured, from level 0, which is the most restricted level, to level 15, which is the least restricted level.
http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfpass.html

QUESTION 256
What two actions would the zone base firewall when looking at the traffic?

A. drop
B. inspect
C. forward

Answer: AB

QUESTION 257
What you called a person who hacks the system with script but instead of writing own script, the person uses existing script?

A. script kiddy
B. white hat hacker

C. phreaker
D. hacktivist

Answer: A

QUESTION 258
Regarding PVLAN diagram question:

```
Switch was in VLAN 300
Isolated Host 1 on VLAN 301
Host 2 and Host 4 on VLAN 303 or something (Community PVLAN)
```

Server is connected to Switch.
All host connects to switch.

A. Host 2 (Host is part of community PVLAN).
B. Other devices on VLAN XXX (VLAN were isolated host is connected, in my case it was Host 1).
C. Server
D. Host 4 (Host is part of community PVLAN)

Answer: C
Explanation:
Host 3 is not part of anyh PVLAN. It is also connected to switch.
So, Host 3 was not an option otherwise it could also be an answer.

QUESTION 259
Nat (inside,outside) dynamic interface

A. static PAT
B. static NAT
C. dynamic PAT
D. dynamic NAT

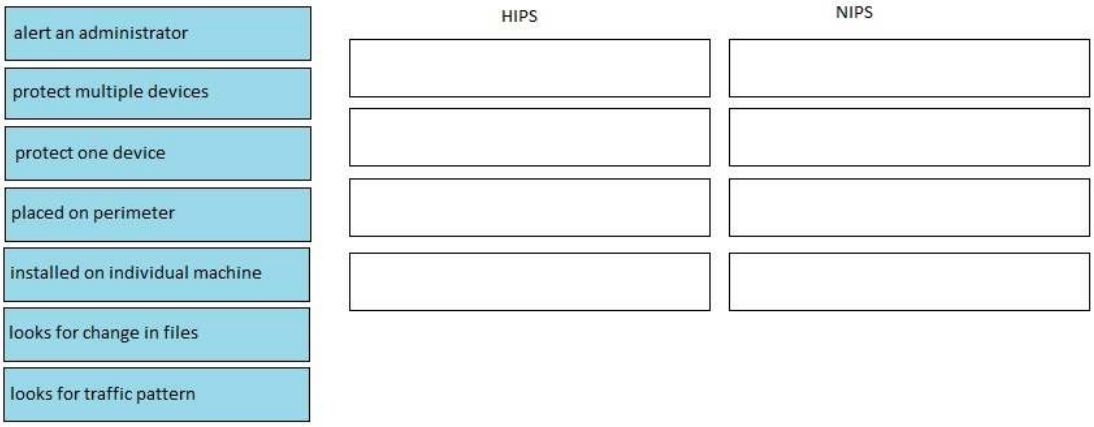
Answer: C
Explanation:
Configuring Dynamic NAT
nat (inside,outside) dynamic my-range-obj
Configuring Dynamic PAT (Hide)
nat (inside,outside) dynamic interface
http://www.cisco.com/c/en/us/td/docs/security/asa/asa83/configuration/guide/config/nat_objects.html

QUESTION 260
Which two characteristics of an application layer firewall are true? (Choose two)

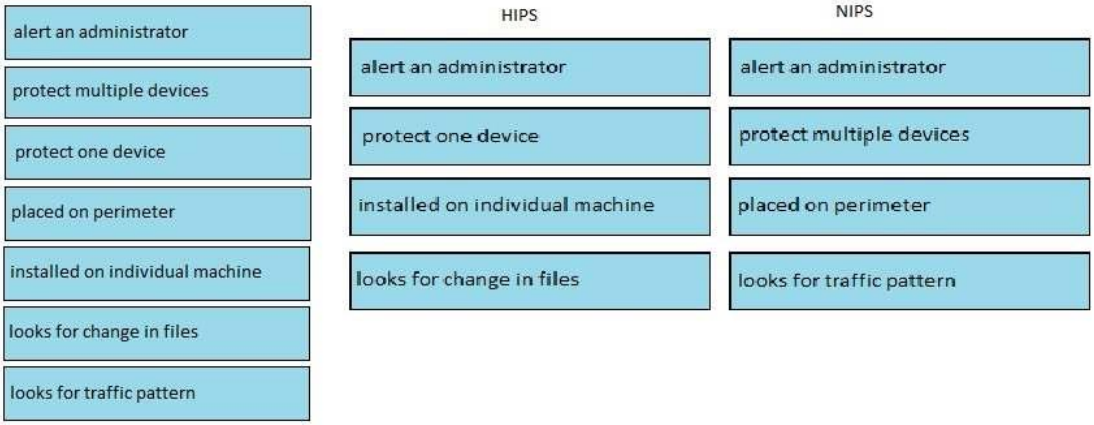
A. provides reverse proxy services
B. is immune to URL manupulation
C. provides protection for multiple applications
D. provide statefull firewall security
E. has low processor usage

Answer: AC

QUESTION 261
HIPS and NIPS
You need to place these 7 options into HIPS and NIPS. Each section has 4 choices which means one out of these 7 options goes into both.



Answer:



QUESTION 262
Which label is given to a person who uses existing computer scripts to hack into computers lacking the expertise to write their own?

A. white hat hacker
B. hacktivist
C. phreaker
D. script kiddy

Answer: D

QUESTION 263
When Cisco IOS zone-based policy firewall is configured, which three actions can be applied to a traffic class? (Choose three.)

A. pass
B. police
C. inspect
D. drop
E. queue
F. shape

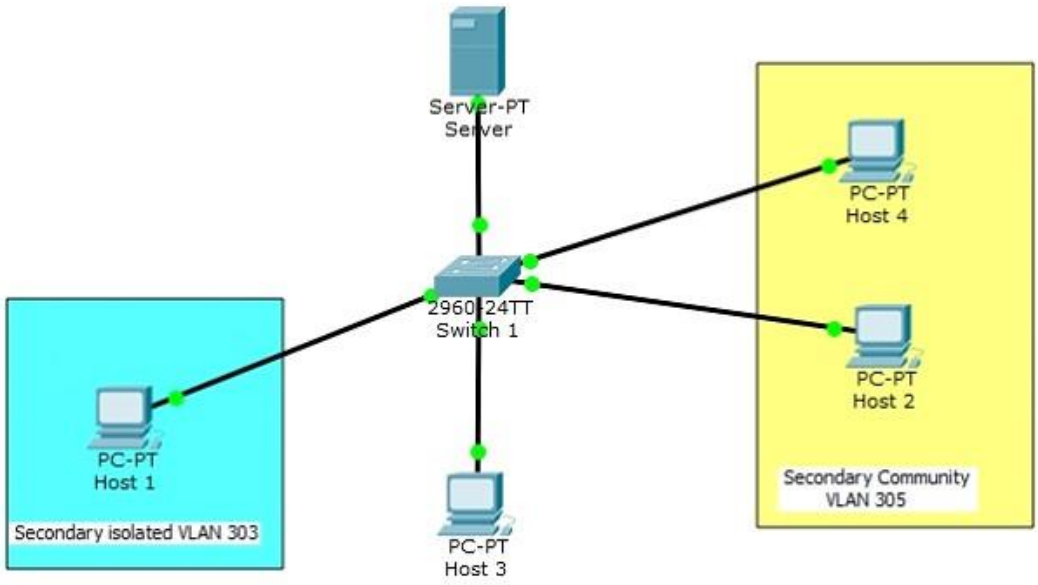
Answer: ACD

QUESTION 264
Which four tasks are required when you configure Cisco IOS IPS using the Cisco Configuration Professional IPS wizard? (Choose four.)

A. Select the interface(s) to apply the IPS rule.
B. Select the traffic flow direction that should be applied by the IPS rule.
C. Add or remove IPS alerts actions based on the risk rating.
D. Specify the signature file and the Cisco public key.
E. Select the IPS bypass mode (fail-open or fail-close).
F. Specify the configuration location and select the category of signatures to be applied to the selected interface(s).

Answer: ABDF

QUESTION 265
Refer to the exhibit. All ports on switch 1 have a primary VLAN of 300. Which devices can host 1 reach?



A. Host 2
B. Server
C. Host 4
D. Other devices within VLAN 303

Answer: B

QUESTION 266
What is the effect of the ASA command crypto isakmp nat-traversal?

A. It opens port 4500 only on the outside interface.
B. It opens port 500 only on the inside interface.
C. It opens port 500 only on the outside interface.
D. It opens port 4500 on all interfaces that are IPSec enabled.

Answer: D

QUESTION 267
What is true about the Cisco IOS Resilient Configuration feature?

A. The feature can be disabled through a remote session
B. There is additional space required to secure the primary Cisco IOS Image file
C. The feature automatically detects image and configuration version mismatch
D. Remote storage is used for securing files

Answer: C

QUESTION 268
Which two characteristics apply to an Intrusion Prevention System (IPS) ? Choose two

A. Does not add delay to the original traffic.
B. Cabled directly inline with the flow of the network traffic.
C. Can drop traffic based on a set of rules.
D. Runs in promoscous mode.
E. Cannot drop the packet on its own

Answer: BC
Explanation:
+ Position in the network flow: Directly inline with the flow of network traffic and every packet goes through the sensor on its way through the network.
+ Mode: Inline mode
+ The IPS can drop the packet on its own because it is inline. The IPS can also request assistance from
another device to block future packets just as the IDS does.

QUESTION 269
What information does the key length provide in an encryption algorithm?

A. the packet size
B. the number of permutations
C. the hash block size
D. the cipher block size

Answer: B

QUESTION 270
Which type of layer 2 attack enables the attacker to intercept traffic that is intended for one specific recipient?

A. BPDU attack
B. DHCP Starvation
C. CAM table overflow
D. MAC address spoofing

Answer: D

QUESTION 271
What feature defines a campus area network?

A. It has a single geographic location.
B. It has limited or restricted Internet access.
C. It has a limited number of segments.
D. it lacks external connectivity.

Answer: A

QUESTION 272
A Cisco ASA appliance has three interfaces configured. The first interface is the inside interface with a security level of 100. The second interface is the DMZ interface with a security level of 50. The third interface is the outside interface with a security level of 0.
By default, without any access list configured, which five types of traffic are permitted? (Choose five.)

A. outbound traffic initiated from the inside to the DMZ
B. outbound traffic initiated from the DMZ to the outside
C. outbound traffic initiated from the inside to the outside
D. inbound traffic initiated from the outside to the DMZ
E. inbound traffic initiated from the outside to the inside
F. inbound traffic initiated from the DMZ to the inside
G. HTTP return traffic originating from the inside network and returning via the outside interface
H. HTTP return traffic originating from the inside network and returning via the DMZ interface
I. HTTP return traffic originating from the DMZ network and returning via the inside interface
J. HTTP return traffic originating from the outside network and returning via the inside interface

Answer: ABCGH
Explanation:
http://www.cisco.com/en/US/docs/security/asa/asa70/configuration/guide/intparam.html

QUESTION 273
Which type of Cisco ASA access list entry can be configured to match multiple entries in a single statement?

A. nested object-class
B. class-map
C. extended wildcard matching
D. object groups

Answer: D

QUESTION 274
What are two well-known security terms? (Choose Two)

A. Phishing.
B. BPDU guard
C. LACP
D. ransomeware
E. hair-pinning

Answer: AD

QUESTION 275
How to verify that TACACS+ connectivity to a device?

A. You successfully log in to the device by using the local credentials.
B. You connect to the device using SSH and receive the login prompt.
C. You successfully log in to the device by using ACS credentials.
D. You connect via console port and receive the login prompt.

Answer: B

QUESTION 276
Which two actions can a zone-based firewall take when looking at traffic? (Choose two)

A. Filter
B. Forward
C. Drop
D. Broadcast
E. Inspect

Answer: CE

QUESTION 277
What technology can you use to provide data confidentiality, data integrity and data origin authentication on your network?

A. Certificate Authority
B. IKE
C. IPSec
D. Data Encryption Standards

Answer: C

QUESTION 278
In which type of attack does an attacker send email messages that ask the recipient to click a link such as https://www.cisco.net.cc/securelogon?

A. phishing
B. pharming
C. solicitation
D. secure transaction

Answer: A

QUESTION 279
When is the default deny all policy an exception in zone-based firewalls?

A. When traffic traverses two interfaces in in the same zone
B. When traffic terminates on the router via the self zone
C. When traffic sources from the router via the self zone
D. When traffic traverses two interfaces in different zones

Answer: A

QUESTION 280
In which configuration mode do you configure the ip ospf authentication-key 1 command?

A. Interface
B. routing process
C. global
D. privileged

Answer: A

QUESTION 281
Which statement about zone-based firewall configuration is true?

A. Traffic is implicitly denied by default between interfaces the same zone
B. Traffic that is desired to or sourced from the self-zone is denied by default
C. The zone must be configured before a can be assigned
D. You can assign an interface to more than one interface

Answer: C

QUESTION 282
Refer to the above. Which translation technique does this configuration result in?

```
# nat (inside,outside) dynamic interface
```

A. Static NAT
B. Dynamic NAT
C. Dynamic PAT
D. Twice NAT

Answer: C

QUESTION 283
Which term best describes the concept of preventing the modification of data in transit and in storage?

A. Confidentiality
B. Integrity
C. Availability
D. fidelity

Answer: B
Explanation:
Integrity for data means that changes made to data are done only by authorized individuals/systems.
Corruption of data is a failure to maintain data integrity. Source: Cisco Official Certification Guide, Confidentiality, Integrity, and Availability, p.6

QUESTION 284
Which option is a characteristic of the RADIUS protocol?

A. uses TCP
B. offers multiprotocol support
C. combines authentication and authorization in one process
D. supports bi-directional challenge

Answer: C
Explanation:
http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml
Authentication and Authorization
RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization.
TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a NAS authenticates on a Kerberos server, it requests authorization information from a TACACS+ server without having to re-authenticate. The NAS informs the TACACS+ server that it has successfully authenticated on a Kerberos server, and the server then provides authorization information.
During a session, if additional authorization checking is needed, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command.

This provides greater control over the commands that can be executed on the access server while decoupling from the authentication mechanism.

QUESTION 285
What do you use when you have a network object or group and want to use an IP address?

A. Static NAT
B. Dynamic NAT
C. identity NAT
D. Static PAT

Answer: B

QUESTION 286
What are two challenges faced when deploying host-level IPS? (Choose Two)

A. The deployment must support multiple operating systems.
B. It does not provide protection for offsite computers.
C. It is unable to provide a complete network picture of an attack.
D. It is unable to determine the outcome of every attack that it detects.
E. It is unable to detect fragmentation attacks.

Answer: AC
Explanation:
Advantages of HIPS: The success or failure of an attack can be readily determined. A network IPS sends an alarm upon the presence of intrusive activity but cannot always ascertain the success or failure of such an attack. HIPS does not have to worry about fragmentation attacks or variable Time to Live (TTL) attacks because the host stack takes care of these issues. If the network traffic stream is encrypted, HIPS has access to the traffic in unencrypted form.
Limitations of HIPS: There are two major drawbacks to HIPS:
+ HIPS does not provide a complete network picture: Because HIPS examines information only at the local host level, HIPS has difficulty constructing an accurate network picture or coordinating the events happening across the entire network. + HIPS has a requirement to support multiple operating systems: HIPS needs to run on every system in the network. This requires verifying support for all the different operating systems used in your network.
Source: http://www.ciscopress.com/articles/article.asp?p=1336425&seqNum=3

QUESTION 287
When AAA login authentication is configured on Cisco routers, which two authentication methods should be used as the final method to ensure that the administrator can still log in to the router in case the external AAA server fails? (Choose two.)

A. group RADIUS
B. group TACACS+
C. local
D. krb5
E. enable
F. if-authenticated

Answer: CE
Explanation:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scftplus.html

QUESTION 288
With Cisco IOS zone-based policy firewall, by default, which three types of traffic are permitted by the router when some of the router interfaces are assigned to a zone? (Choose three.)

A. traffic flowing between a zone member interface and any interface that is not a zone member
B. traffic flowing to and from the router interfaces (the self zone)
C. traffic flowing among the interfaces that are members of the same zone
D. traffic flowing among the interfaces that are not assigned to any zone
E. traffic flowing between a zone member interface and another interface that belongs in a different zone
F. traffic flowing to the zone member interface that is returned traffic

Answer: BCD
Explanation:
http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml
Rules For Applying Zone-Based Policy Firewall
Router network interfaces' membership in zones is subject to several rules that govern interface behavior, as is the traffic moving between zone member interfaces:
A zone must be configured before interfaces can be assigned to the zone. An interface can be assigned to only one security zone. All traffic to and from a given interface is implicitly blocked when the interface is assigned to a zone, except traffic to and from other interfaces in the same zone, and traffic to any interface on the router.
Traffic is implicitly allowed to flow by default among interfaces that are members of the same zone. In order to permit traffic to and from a zone member interface, a policy allowing or inspecting traffic must be configured between that zone and any other zone. The self zone is the only exception to the default deny all policy. All traffic to any router interface is allowed until traffic is explicitly denied. Traffic cannot flow between a zone member interface and any interface that is not a zone member. Pass, inspect, and drop actions can only be applied between two zones.
Interfaces that have not been assigned to a zone function as classical router ports and might still use classical stateful inspection/CBAC configuration. If it is required that an interface on the box not be part of the zoning/firewall policy. It might still be necessary to put that interface in a zone and configure a pass all policy (sort of a dummy policy) between that zone and any other zone to which traffic flow is desired. From the preceding it follows that, if traffic is to flow among all the interfaces in a router, all the interfaces must be part of the zoning model (each interface must be a member of one zone or another).
The only exception to the preceding deny by default approach is the traffic to and from the router, which will be permitted by default. An explicit policy can be configured to restrict such traffic.

QUESTION 289
Which statement is a benefit of using Cisco IOS IPS?

A. It uses the underlying routing infrastructure to provide an additional layer of security.
B. It works in passive mode so as not to impact traffic flow.
C. It supports the complete signature database as a Cisco IPS sensor appliance.
D. The signature database is tied closely with the Cisco IOS image.

Answer: A

QUESTION 290
Which command do you enter to enable authentication for OSPF on an interface?

A. router(config-if)#ip ospf message-digest-key 1 md5 CISCOPASS
B. router(config-router)#area 0 authentication message-digest
C. router(config-router)#ip ospf authentication-key CISCOPASS
D. router(config-if)#ip ospf authentication message-digest

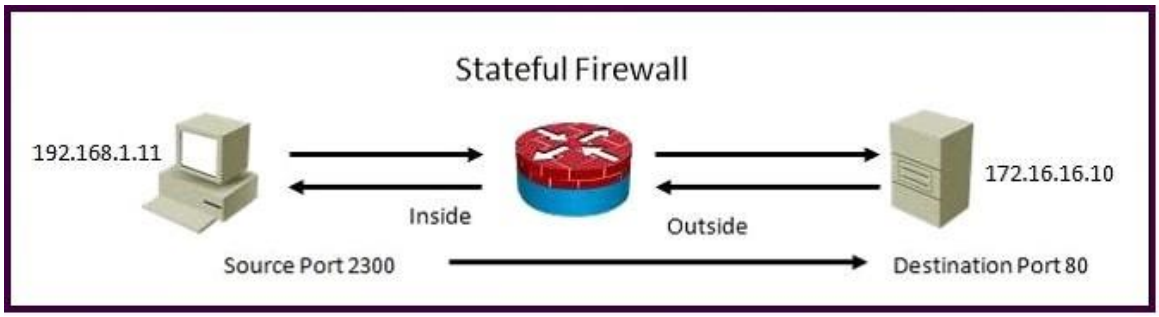
Answer: D

QUESTION 291
Which two options are advantages of an application layer firewall? (Choose two.)

A. provides high-performance filtering
B. makes DoS attacks difficult
C. supports a large number of applications
D. authenticates devices
E. authenticates individuals

Answer: BE
Explanation:
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_white_paper0900aecd8058ec85.html
Adding Intrusion Prevention
Gartner's definition of a next-generation firewall is one that combines firewall filtering and intrusion prevention systems (IPSs). Like firewalls, IPSs filter packets in real time. But instead of filtering based on user profiles and application policies, they scan for known malicious patterns in incoming code, called signatures. These signatures indicate the presence of malware, such as worms, Trojan horses, and spyware.
Malware can overwhelm server and network resources and cause denial of service (DoS) to internal employees, external Web users, or both. By filtering for known malicious signatures, IPSs add an extra layer of security to firewall capabilities; once the malware is detected by the IPS, the system will block it from the network. Firewalls provide the first line of defense in any organization's network security infrastructure. They do so by matching corporate policies about users' network access rights to the connection information surrounding each access attempt. If the variables don't match, the firewall blocks the access connection. If the variables do match, the firewall allows the acceptable traffic to flow through the network.
In this way, the firewall forms the basic building block of an organization's network security architecture. It pays to use one with superior performance to maximize network uptime for business-critical operations. The reason is that the rapid addition of voice, video, and collaborative traffic to corporate networks is driving the need for firewall engines that operate at very high speeds and that also support application-level inspection. While standard Layer 2 and Layer 3 firewalls prevent unauthorized access to internal and external networks, firewalls enhanced with application-level inspection examine, identify, and verify application types at Layer 7 to make sure unwanted or misbehaving application traffic doesn't join the network. With these capabilities, the firewall can enforce endpoint user registration and authentication and provide administrative control over the use of multimedia applications.

QUESTION 292
Refer to the exhibit. Using a stateful packet firewall and given an inside ACL entry of permit ip 192.16.1.0 0.0.0.255 any, what would be the resulting dynamically configured ACL for the return traffic on the outside ACL?



A. permit tcp host 172.16.16.10 eq 80 host 192.168.1.11 eq 2300
B. permit ip 172.16.16.10 eq 80 192.168.1.0 0.0.0.255 eq 2300
C. permit tcp any eq 80 host 192.168.1.11 eq 2300
D. permit ip host 172.16.16.10 eq 80 host 192.168.1.0 0.0.0.255 eq 2300

Answer: A

QUESTION 293
Which command is used to verify that a VPN connection is established between two endpoints and that the connection is passing?

A. Firewall#sh crypto ipsec sa
B. Firewall#sh crypto isakmp sa
C. Firewall#debug crypto isakmp
D. Firewall#sh crypto session

Answer: A

QUESTION 294
Which TACACS+ server-authentication protocols are supported on Cisco ASA firewalls? (Choose three.)

A. EAP
B. ASCII
C. PAP
D. PEAP
E. MS-CHAPv1
F. MS-CHAPv2

Answer: BCE

QUESTION 295
Which two protocols enable Cisco Configuration Professional to pull IPS alerts from a Cisco ISR router? (Choose two.)

A. syslog
B. SDEE
C. FTP

D. TFTP
E. SSH
F. HTTPS

Answer: BF
Explanation:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd805c4ea8.html

QUESTION 296
Refer to the below. Which statement about this debug output is true?

```
Router# debug tacacs

14:00:09: TAC+: Opening TCP/IP connection to 192.168.60.15 using source
10.116.0.79
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 192.168.60.15
(AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 192.168.60.15
14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 192.168.60.15
(AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 192.168.60.15
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 192.168.60.15
(AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 192.168.60.15
14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15
```

A. The requesting authentication request came from username GETUSER.
B. The TACACS+ authentication request came from a valid user.
C. The TACACS+ authentication request passed, but for some reason the user's connection was closed immediately.
D. The initiating connection request was being spoofed by a different source address.

Answer: B

QUESTION 297
Which IOS command is used to define the authentication key for NTP?

A. Switch(config)#ntp authentication-key 1 md5 C1sc0
B. Switch(config)#ntp trusted-key 1
C. Switch(config)#ntp source 192.168.0.1
D. Switch(config)#ntp authenticate

Answer: A

QUESTION 298
Which aaa accounting command is used to enable logging of the start and stop records for user terminal sessions on the router?

A. aaa accounting network start-stop tacacs+
B. aaa accounting system start-stop tacacs+
C. aaa accounting exec start-stop tacacs+
D. aaa accounting connection start-stop tacacs+
E. aaa accounting commands 15 start-stop tacacs+

Answer: C
Explanation:
http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html
aaa accounting
To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the aaa accounting command in global configuration mode or template configuration mode. To disable AAA accounting, use the no form of this command. aaa accounting {auth-proxy | system | network | exec | connection | commands level | dot1x} {default | list-name
| guarantee-first} [vrf vrf-name] {start-stop | stop-only | none} [broadcast] {radius | group group-name}
no aaa accounting {auth-proxy | system | network | exec | connection | commands level | dot1x} {default | listname
| guarantee-first} [vrf vrf-name] {start-stop | stop-only | none} [broadcast] {radius | group group-name} exec
Runs accounting for the EXEC shell session.
start-stop
Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.

QUESTION 299
What can cause the the state table of a stateful firewall to update? (choose two)

A. when a connection is created
B. When a connection's timer has expired within state table
C. when packet is evaluated against the outbound access list and is denied
D. when outbound packets forwarded to outbound interface
E. when rate-limiting is applied

Answer: AB

QUESTION 300
On Cisco ISR routers, for what purpose is the realm-cisco.pub public encryption key used?

A. used for SSH server/client authentication and encryption
B. used to verify the digital signature of the IPS signature file

C. used to generate a persistent self-signed identity certificate for the ISR so administrators can authenticate the ISR when accessing it using Cisco Configuration Professional
D. used to enable asymmetric encryption on IPsec and SSL VPNs
E. used during the DH exchanges on IPsec VPNs

Answer: B
Explanation:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd805c4ea8.html

QUESTION 301
Which type of PVLAN port allows communication from all port types?

A. isolated
B. community
C. in-line
D. promiscuous

Answer: D

QUESTION 302
Which three options are common examples of AAA implementation on Cisco routers? (Choose three.)

A. authenticating remote users who are accessing the corporate LAN through IPsec VPN connections
B. authenticating administrator access to the router console port, auxiliary port, and vty ports
C. implementing PKI to authenticate and authorize IPsec VPN peers using digital certificates
D. tracking Cisco NetFlow accounting statistics
E. securing the router by locking down all unused services
F. performing router commands authorization using TACACS+

Answer: ABF
Explanation:
http://www.cisco.com/en/US/products/ps6638/products_data_sheet09186a00804fe332.htm l
Need for AAA Services
Security for user access to the network and the ability to dynamically define a user's profile to gain access to network resources has a legacy dating back to asynchronous dial access. AAA network security services provide the primary framework through which a network administrator can set up access control on network points of entry or network access servers, which is usually the function of a router or access server.
Authentication identifies a user; authorization determines what that user can do; and accounting monitors the network usage time for billing purposes. AAA information is typically stored in an external database or remote server such as RADIUS or TACACS+.
The information can also be stored locally on the access server or router. Remote security servers, such as RADIUS and TACACS+, assign users specific privileges by associating attribute-value (AV) pairs, which define the access rights with the appropriate user. All authorization methods must be defined through AAA.

QUESTION 303
Which type of encryption technology has the broadest platform support to protect operating

systems?

A. software
B. hardware
C. middleware
D. file-level

Answer: A

QUESTION 304
Refer to the exhibit. Which statement about this output is true?

```
Oct 13 19:46:06.170: AAA/MEMORY: create_user (0x4C5E1F60) user='tecteam'
ruser='NULL' ds0=0 port='tty515' rem_addr='10.0.2.13' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0', vrf= (id=0)
Oct 13 19:46:06.170: AAA/AUTHEN/START (2600878790): port='tty515' list=''
action=LOGIN service=ENABLE
Oct 13 19:46:06.170: AAA/AUTHEN/START (2600878790): console enable - default to
enable password (if any)
Oct 13 19:46:06.170: AAA/AUTHEN/START (2600878790): Method=ENABLE
Oct 13 19:46:06.170: AAA/AUTHEN (2600878790): status = GETPASS
Oct 13 19:46:07.266: AAA/AUTHEN/CONT (2600878790): continue_login
(user='(undef)')
Oct 13 19:46:07.266: AAA/AUTHEN (2600878790): status = GETPASS
Oct 13 19:46:07.266: AAA/AUTHEN/CONT (2600878790): Method=ENABLE
Oct 13 19:46:07.266: AAA/AUTHEN(2600878790): password incorrect
Oct 13 19:46:07.266: AAA/AUTHEN (2600878790): status = FAIL
Oct 13 19:46:07.266: AAA/MEMORY: free_user (0x4C5E1F60) user='NULL'
ruser='NULL' port='tty515' rem_addr='10.0.2.13' authen_type=ASCII service=ENABLE
priv=15 vrf= (id=0)
```

A. The user logged into the router with the incorrect username and password.
B. The login failed because there was no default enable password.
C. The login failed because the password entered was incorrect.
D. The user logged in and was given privilege level 15.

Answer: C
Explanation:
http://www.cisco.com/en/US/docs/ios/12_2/debug/command/reference/dbfaaa.html

QUESTION 305
You are the security administrator for a large enterprise network with many remote locations. You have been given the assignment to deploy a Cisco IPS solution.
Where in the network would be the best place to deploy Cisco IOS IPS?

A. Inside the firewall of the corporate headquarters Internet connection
B. At the entry point into the data center

C. Outside the firewall of the corporate headquarters Internet connection
D. At remote branch offices

Answer: D
Explanation:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/product_data_sheet0900aecd803137cf.html

QUESTION 306
Which two characteristics of the TACACS+ protocol are true? (Choose two.)

A. uses UDP ports 1645 or 1812
B. separates AAA functions
C. encrypts the body of every packet
D. offers extensive accounting capabilities
E. is an open RFC standard protocol

Answer: BC
Explanation:
http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml

QUESTION 307
What is a benefit of a web application firewall?

A. It blocks known vulnerabilities without patching applications.
B. It simplifies troubleshooting.
C. It accelerates web traffic.
D. It supports all networking protocols.

Answer: A

QUESTION 308
Which filter uses in Web reputation to prevent from Web Based Attacks? (Choose two)

A. outbreak filter
B. buffer overflow filter
C. bayesian overflow filter
D. web reputation
E. exploit filtering

Answer: AE

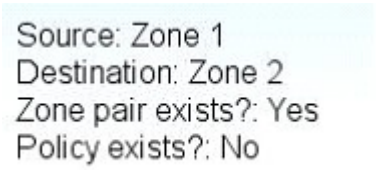
QUESTION 309
Which option is the default value for the DiffieHellman group when configuring a site-to- site VPN on an ASA device?

A. Group 1
B. Group 2
C. Group 5

D. Group 7

Answer: B

QUESTION 310
Which option is the resulting action in a zone-based policy firewall configuration with these conditions?



A. no impact to zoning or policy
B. no policy lookup (pass)
C. drop
D. apply default policy

Answer: C
Explanation:
http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/sec-zone- pol-fw.html

QUESTION 311
Referring to CIA (confidentiality,Integrity and Availability), where would a hash-only make more sense?

A. Data at Rest
B. Data on File
C. ...
D. ...

Answer: A
Explanation:
Confidentiality
Confidentiality ensures that data is only viewable by authorized users. In other words, the goal of confidentiality is to prevent the unauthorized disclosure of information. Loss of confidentiality indicates that unauthorized users have been able to access information.
If there is a risk of sensitive data falling into the wrong hands, it should be encrypted to make it unreadable. This includes encrypting data at rest and data in motion. **Data at rest is any data stored as a file on a hard drive, mobile device, or even a USB flash drive**. Data in motion is any data traveling over a network. AES is the most common symmetric encryption protocol used to encrypt data at rest. **SSH, IPsec, SSL, and TLS are some common encryption protocols used to encrypt data in motion**.
Additionally, data should be protected with access controls to enforce confidentiality.

QUESTION 312
Phishing method on the phone.

A. vishing
B. mishing
C. phishing
D. ...

Answer: A

QUESTION 313
At which Layer Data Center Operate?

A. Data Center
B. ...
C. ...
D. ...

Answer: A

QUESTION 314
How can you stop reconnaissance attack with cdp.

A. disable CDP on edge ports (computers)
B. ...
C. ...
D. ...

Answer: A

QUESTION 315
For Protecting FMC what/which is used.

A. AMP
B. ...
C. ...
D. ...

Answer: A

QUESTION 316
Which IPS deployment is not most secure but best for network throughput?

A. Promiscuous
B. ...
C. ...
D. ...

Answer: A

QUESTION 317

Which feature allow from dynamic NAT pool to choose next IP address and not a port on a used IP address?

A. next IP
B. round robin
C. Dynamic rotation
D. Dynamic PAT rotation

Answer: B

QUESTION 318
Zone based firewall

A. enable zones first / zones must be made before applying interfaces.
B. enable zones first
C. ...
D. ...

Answer: A

QUESTION 319
Which ports need to be active for AAA server to integrate with Microsoft AD?

A. 445 & 389
B. 445 & 8080
C. 443 & 389
D. 443 & 8080

Answer: A

QUESTION 320
What does the command crypto isakmp nat-traversal do?

A. Enables udp port 4500 on all IPsec enabled interfaces
B. Rebooting the ASA the global command

Answer: A

QUESTION 321
Why ipsec tunnel is not working?

A. because the ASA can't receive packets from remote endpoint
B. ...
C. ...
D. ...

Answer: A

QUESTION 322
What data is transferred during DH for making public and private key?

A. Random prime Integer
B. Encrypted data transfer
C. Diffie-Hellman

Answer: A

QUESTION 323
Dos attack difficult to discover

A. Low-rate dos attack
B. Syn-flood attack
C. Peer-to-peer attacks
D. Trojan

Answer: A

QUESTION 324
Protocols supported in contest aware VRF over VRF lite (Choose 2)

A. EIGRP
B. Multicast
C. OSPF
D. Unicast

Answer: AB

QUESTION 325
question about show crypto isakmp sa ?

A. Remote peer was not able to encrypt the packet
B. ...
C. ...
D. ...

Answer: A

QUESTION 326
What are the quantifiable things you would verify before introducing new technology in your company

A. risk
B. exploit
C. vulnerability
D. virus

Answer: A

QUESTION 327
Which type of social-engineering attacks uses normal telephone service as the attack vector?

A. vishing
B. phising
C. smishing
D. war dialing

Answer: A

QUESTION 328
What causes a client to be placed in a guest or restricted (cant remember) VLAN on an 802.1x enabled network?

A. client entered wrong credentials multiple times.
B. client entered wrong credentials First time.

Answer: A

QUESTION 329
Self zone (2 option)?

A. can be source or deatination zone.
B. can be use statful filtering during multicast.
C. all interfaces wil be used for self zone
D. ...

Answer: AC
Explanation:
DHCP spoofing occurs when an attacker attempts to respond to DHCP requests and trying to list themselves (spoofs) as the default gateway or DNS server, hence, initiating a man in the middle attack. With that, it is possible that they can intercept traffic from users before forwarding to the real gateway or perform DoS by flooding the real DHCP server with request to choke ip address resources.
https://learningnetwork.cisco.com/thread/67229
https://learningnetwork.cisco.com/docs/DOC-24355

QUESTION 330
Which IDS/IPS is used for monitoring system?

A. HIPS
B. WIPS
C. Visibility Tool

Answer: A

QUESTION 331

Which IPS detection method can you use to detect attacks that based on the attackers IP addresses?

A. Policy-based
B. Anomaly-based
C. Reputation-based
D. Signature-based

Answer: A

QUESTION 332
Which type of attack can exploit design flaws in the implementation of an application without going noticed?

A. Volume-based DDoS attacks.
B. application DDoS flood attacks.
C. DHCP starvation attacks
D. low-rate DoS attacks

Answer: D

QUESTION 333
Which IOS command do you enter to test authentication against a AAA server?

A. dialer aaa suffix <suffix> password <password>
B. ppp authentication chap pap test
C. aaa authentication enable default test group tacacs+
D. test aaa-server authentication dialergroup username <user> password.

Answer: D

QUESTION 334
How can you proect CDP from reconnaissance attacks?

A. Enable dot1x on all ports that are connected to other switches.
B. Disable CDP on ports connected to endpoints.
C. Disbale CDP on trunk ports.
D. Enable dynamic ARP inspection on all untrusted ports.

Answer: B

QUESTION 335
How does PEAP protect the EAP exchange?

A. It encrypts the exchange using the server certificate.
B. It encrypts the exchange using the client certificate.
C. It validates the server-supplied certificate, and then encrypts the exchange using the client certificate.
D. It validates the client-supplied certificate, and then encrypts the exchange using the server

certificate.

Answer: A

QUESTION 336
Referencing the CIA model, in which scenario is a hash-only function most appropriate?

A. securing wireless transmissions.
B. securing data in files.
C. securing real-time traffic
D. securing data at rest

Answer: D

QUESTION 337
If you change the native VLAN on the trunk port to an unused VLAN, what happens if an attacker attempts a double-tagging attack?

A. The trunk port would go into an error-disabled state.
B. A VLAN hopping attack would be successful.
C. A VLAN hopping attack would be prevented.
D. The attacked VLAN will be pruned.

Answer: C

QUESTION 338
Which option is a key security component of an MDM deployment?

A. using MS-CHAPv2 as the primary EAP method.
B. using self-signed certificates to validate the server.
C. using network-specific installer packages
D. using an application tunnel by default.

Answer: B

QUESTION 339
Which Firepower Management Center feature detects and blocks exploits and hack attempts?

A. intrusion prevention
B. advanced malware protection
C. content blocker
D. file control

Answer: A

QUESTION 340
Which IDS/IPS solution can monitor system processes and resources?

A. IDS
B. HIPS
C. PROXY
D. IPS

Answer: B

QUESTION 341
What IPSec mode is used to encrypt traffic between a server and VPN endpoint?

A. tunnel
B. Trunk
C. Aggregated
D. Quick
E. Transport

Answer: E

QUESTION 342
Refer to the exhibit. What type of firewall would use the given configuration line?

```
UDP outside  209.165.201.225:53 inside  10.0.0.10:52464, idle 0:00:01, bytes 266, flags -
```

A. a stateful firewall
B. a personal firewall
C. a proxy firewall
D. an application firewall
E. a stateless firewall

Answer: A

QUESTION 343
What are two ways to prevent eavesdropping when you perform device-management tasks? (Choose two.)

A. Use an SSH connection.
B. Use SNMPv3.
C. Use out-of-band management.
D. Use SNMPv2.
E. Use in-band management.

Answer: AB

QUESTION 344
Which ports need to be active for AAA server and a Microsoft server to permit Active Directory authentication?

A. 445 and 389
B. 888 and 3389
C. 636 and 4445
D. 363 and 983

Answer: A

QUESTION 345
Which description of the nonsecret numbers that are used to start a Diffie-Hellman exchange is true?

A. They are large pseudorandom numbers.
B. They are very small numbers chosen from a table of known values
C. They are numeric values extracted from hashed system hostnames.
D. They are preconfigured prime integers

Answer: D

QUESTION 346
Which quantifiable item should you consider when your organization adopts new technologies?

A. threats
B. vulnerability
C. risk
D. exploits

Answer: C

QUESTION 347
What is the primary purpose of a defined rule in an IPS?

A. to configure an event action that takes place when a signature is triggered
B. to define a set of actions that occur when a specific user logs in to the system
C. to configure an event action that is pre-defined by the system administrator
D. to detect internal attacks

Answer: A

QUESTION 348
Which IPS mode is less secure than other options but allows optimal network throughput?

A. promiscuous mode
B. inline mode
C. inline-bypass mode
D. transparent mode.

Answer: A

QUESTION 349
Which three statements about host-based IPS are true? (Choose three.)

A. It can view encrypted files.
B. It can have more restrictive policies than network-based IPS.
C. It can generate alerts based on behavior at the desktop level.
D. It can be deployed at the perimeter.
E. It uses signature-based policies.
F. It works with deployed firewalls.

Answer: ABC
Explanation:
If the network traffic stream is encrypted, **HIPS has access to the traffic in unencrypted form**. HIPS can combine the best features of antivirus, behavioral analysis, signature filters, network firewalls, and application firewalls in one package.
Host-based IPS operates by detecting attacks that occur on a host on which it is installed. HIPS works by intercepting operating system and application calls, securing the operating system and application configurations, validating incoming service requests, and analyzing local log files for after-the-fact suspicious activity.
Source: http://www.ciscopress.com/articles/article.asp?p=1336425&seqNum=3

QUESTION 350
Which two statements about the self zone on a Cisco zone-based policy firewall are true? (Choose Two)

A. Multiple interfaces can be assigned to the self zone.
B. Traffic entering the self zone must match a rule.
C. Zone pairs that include the self zone apply to traffic transiting the device.
D. It can be either the source zone or the destination zone.
E. It supports stateful inspection for multicast traffic.

Answer: AD

QUESTION 351
Which type of PVLAN port allows hosts in the same VLAN to communicate directly with each other?

A. community for hosts in the PVLAN
B. promiscuous for hosts in the PVLAN
C. isolated for hosts in the PVLAN
D. span for hosts in the PVLAN

Answer: A

QUESTION 352
What configuration allows AnyConnect to automatically establish a VPN session when a user logs in to the computer?

A. always-on
B. proxy

C. transparent mode
D. Trusted Network Detection

Answer: A

QUESTION 353
What are two uses of SIEM software? (Choose two.)

A. collecting and archiving syslog data
B. alerting administrators to security events in real time
C. performing automatic network audits
D. configuring firewall and IDS devices
E. scanning email for suspicious attachments

Answer: AB

QUESTION 354
Which two devices are components of the BYOD architectural framework?

A. Prime Infrastructure
B. Nexus 7010 Switch
C. Cisco 3945 Router
D. Wireless Access Points
E. Identity Services Engine

Answer: AE

QUESTION 355
Refer to the exhibit. The Admin user is unable to enter configuration mode on a device with the given configuration. What change can you make to the configuration to correct the problem?

```
Username HelpDesk privilege 9 password 0 helpdesk
Username Monitor privilege 8 password 0 watcher
Username Admin password checkme
Username Admin privilege 6 autocommand show running
Privilege exec level 6 configure terminal
```

A. Remove the autocommand keyword and arguments from the username admin privilege line.
B. Change the Privilege exec level value to 15.
C. Remove the two Username Admin lines.
D. Remove the Privilege exec line.

Answer: A

QUESTION 356
Refer to the exhibit. While troubleshooting site-to-site VPN, you issued the show crypto isakmp sa command.

What does the given output show?

```
dst          src         state          conn-id     slot
10.10.10.2   10.1.1.5    MM_NO_STATE    1           0
```

A. IKE Phase 1 main mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2.
B. IKE Phase 1 main mode has successfully negotiated between 10.1.1.5 and 10.10.10.2.
C. IKE Phase 1 aggressive mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2.
D. IKE Phase 1 aggressive mode has successfully negotiated between 10.1.1.5 and 10.10.10.2.

Answer: A

QUESTION 357
Which two features do CoPP and CPPr use to protect the control plane? (Choose two.)

A. QoS
B. traffic classification
C. access lists
D. policy maps
E. class maps
F. Cisco Express Forwarding

Answer: AB

QUESTION 358
What type of algorithm uses the same key to encrypt and decrypt data?

A. a symmetric algorithm
B. an asymmetric algorithm
C. a Public Key Infrastructure algorithm
D. an IP security algorithm

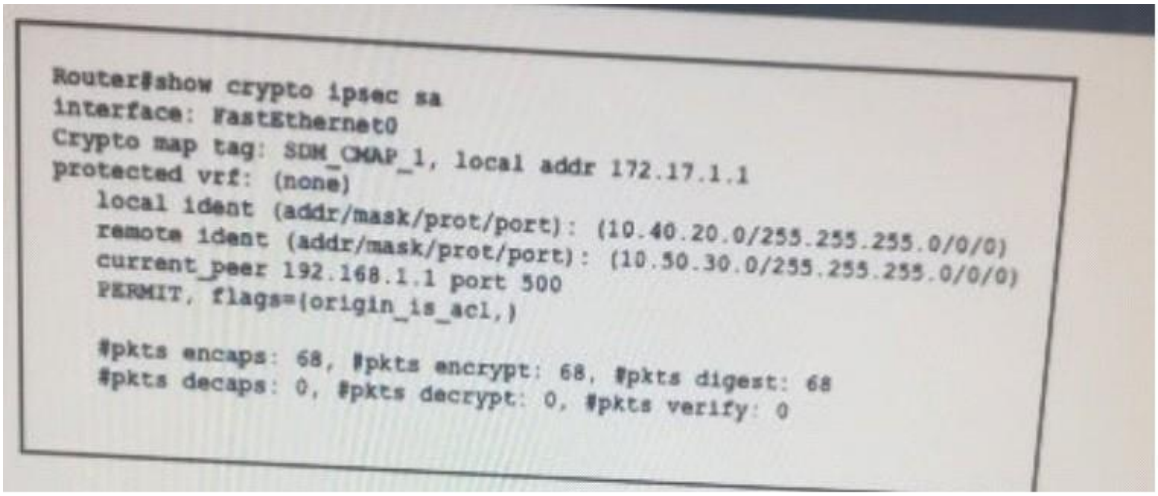
Answer: A

QUESTION 359
Which two features are supported in a VRF-aware software infrastructure before VRF-lite? (Choose two)

A. priority queuing
B. EIGRP
C. multicast
D. WCCP
E. fair queuing

Answer: BC

QUESTION 360
Refer to the exhibit. For which reason is the tunnel unable to pass traffic?



A. UDP port 500 is blocked.
B. The IP address of the remote peer is incorrect.
C. The tunnel is failing to receive traffic from the remote peer.
D. The local peer is unable to encrypt the traffic.

Answer: C

QUESTION 361
Which of the Diffie-Hellman group are support by cisco VPN Product? (Choose all that apply)

A. Group1
B. Group2
C. Group3
D. Group5
E. Group7
F. Group8
G. Group9

Answer: ABDE

QUESTION 362
What type of Diffie-Hellman group would you expect to be utiliazed on a wireless device ?

A. Group4
B. Group7
C. Group5
D. Group3

Answer: B

QUESTION 363
Which of the following are IKE modes? (Choose all and apply)

A. Main Mode
B. Fast Mode
C. Aggressive Mode
D. Quick Mode
E. Diffie-Hellman Mode

Answer: ACD
Explanation:
Main mode and aggressive mode are in IKE phase 1 negotiation and quick mode is in IKE phase 2.

QUESTION 364
Which two statements describe DHCP spoofing attacks? (Choose Two.)

A. They can modify the flow of traffic in transit.
B. They can access most network devices.
C. They can physically modify the network gateway.
D. They are used to perform man-in-the-middle attacks.
E. They protect the identity of the attacker by masking the DHCP address.
F. They use ARP poisoning.

Answer: AD
Explanation:
DHCP spoofing occurs when an attacker attempts to respond to DHCP requests and trying to list themselves (spoofs) as the default gateway or DNS server, hence, initiating a man in the middle attack.
With that, it is possible that they can intercept traffic from users before forwarding to the real gateway or perform DoS by flooding the real DHCP server with request to choke ip address resources.
https://learningnetwork.cisco.com/thread/67229 https://learningnetwork.cisco.com/docs/DOC-24355

QUESTION 365
What's the highest security level can be applied to an ASA interface?

A. 0
B. 50
C. 100
D. 200

Answer: C

QUESTION 366
How will the traffic be affected if policy from the self zone is removed ?

A. all traffic will be inspected.

B. traffic will not be inspected.
C. traffic will be passed with logging action.

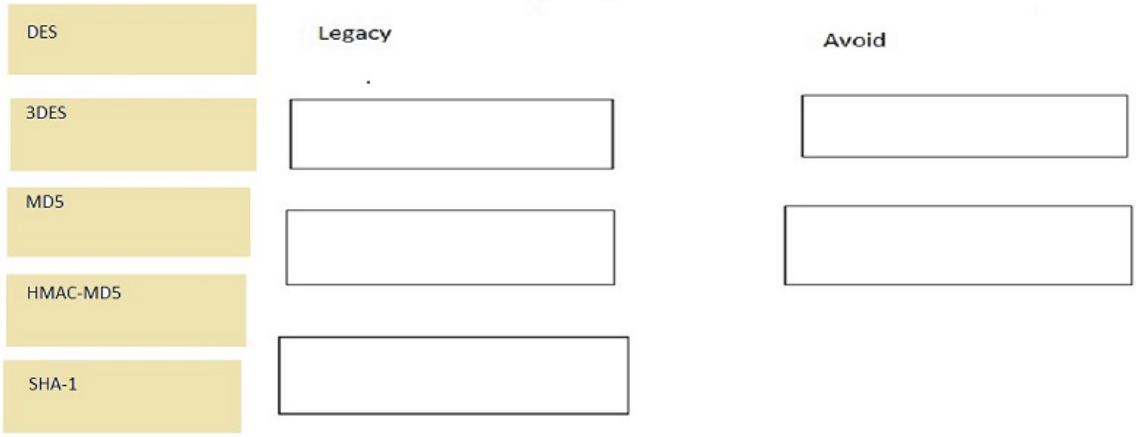
Answer: B

QUESTION 367
How will SDM be accessed?

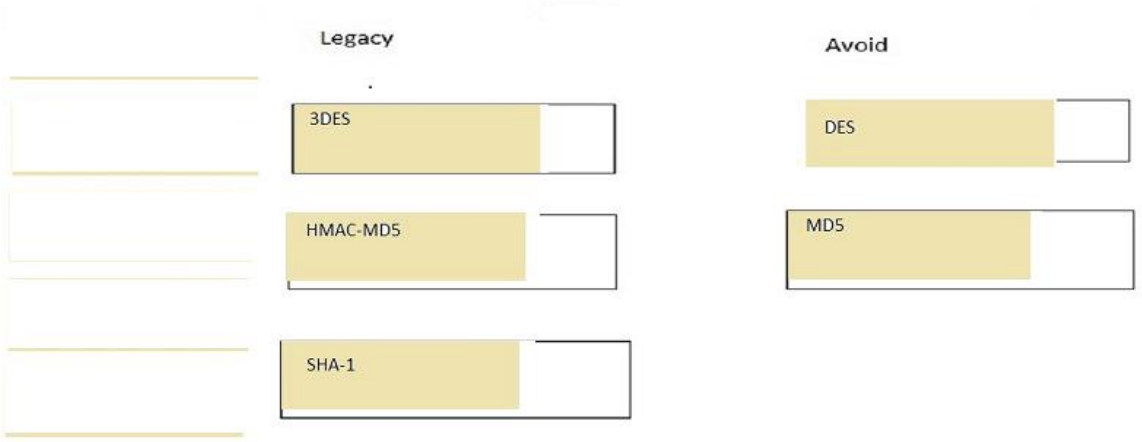
A. from pc
B. from mobile
C. from router flash
D. from some cisco web portla

Answer: A

QUESTION 368
Drag and Drop with hashing and encryption technologies obsoletes and legacy DES/3DES/MD5/HMAC-MD5/SHA1



Answer:



QUESTION 369
What is the effect of the ip scp server enable command?

A. It allows the router to initiate requests to an SCP server
B. It references an access list that allows specific SCP servers
C. It adds SCP to the list of allowed copy functions
D. It allows the router to become an SCP server

Answer: D

QUESTION 370
Which two SNMPv3 services support its capabilities as a secure network management protocol? (Choose two)

A. accounting
B. authentication
C. the shared secret key
D. access control
E. authorization

Answer: BD

QUESTION 371
Which component of a BYOD architecture provides AAA services for endpoint access?

A. access point
B. Integrated Services Router
C. Identify Services Engine
D. ASA

Answer: C

QUESTION 372

Which two statements about routed firewall mode are true? (Choose two)

A. this mode conceals the presence of the firewall
B. By default, this mode permits most traffic to pass through the firewall
C. the firewall acts as a routed hop in the network
D. the firewall requires a unique IP address for each interface
E. this mode allows the firewall to be added to an existing network with minimal additional configuration

Answer: CD

QUESTION 373
How can you mitigate attacks in which the attacker attaches more than one VLAN tag to a packet?

A. Disable EtherChannel
B. Enable transparent VTP on the switch
C. Explicitly identify each VLAN allowed across the trunk
D. Assign an access VLAN to every active port on the switch

Answer: C

QUESTION 374
You are configuring a NAT rule on a Cisco ASA. Which description of a mapped interface is true?

A. It is mandatory for identify NAT only
B. It is optional in routed mode
C. It is mandatory for all firewall modes
D. It is optional in transparent mode

Answer: B

QUESTION 375
Which technology can you implement to centrally mitigate potential threats when users on your network download files that might be malicious?

A. Implement URL filtering on the perimeter firewall
B. Verify that are company IPS blocks all known malicious websites
C. Enable file reputation services to inspect all files that traverse the company network and block files with low reputation scores
D. Verify that antivirus software is installed and up to date for all users on your network

Answer: C

QUESTION 376
When using the Adaptive Security Device Manager (ASDM), which two options are available to add a new add a new root certificate? (Choose two)

A. use LDAP

B. use SCEP
C. install from a file
D. install from SFTP server
E. use HTTPS

Answer: BC

QUESTION 377
Which description of the use of a private key is true?

A. the sender signs a message using their private key
B. the sender signs a message using the receiver's private key
C. the sender encrypts a message using the receiver's private key
D. the receiver decrypts a message using the sender's private key

Answer: A

QUESTION 378
What is the most common implementation of PAT in a standard networked environment?

A. configuring multiple internal hosts to communicate outside of the network using the outside interface IP address
B. configuring multiple internal hosts to communicate outside of the network by using the inside interface IP address
C. configuring multiple external hosts to join the self-zone and to communicate with one another
D. configuring an any any rule to enable external hosts to communicate inside the network

Answer: A

QUESTION 379
Which standard is a hybrid protocol that uses Oakley and Skeme key exchanges in an ISAKMP framework?

A. IPSec
B. SHA
C. DES
D. IKE

Answer: D
Explanation:
The Oakley Key Determination Protocol is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the Diffie琀ellman key exchange algorithm.
The protocol was proposed by Hilarie K. Orman in 1998, and formed the basis for the more widely used Internet key exchange protocol
Source:
https://en.wikipedia.org/wiki/Oakley_protocol
IKE (Internet Key Exchange)
A key management protocol standard that is used in conjunction with the IPSec standard. IPSec is an IP security feature that provides robust authentication and encryption of IP packets. IPSec

can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside of the Internet Security Association and Key Management Protocol (ISAKMP) framework.
ISAKMP, Oakley, and Skeme are security protocols implemented by IKE Source: https://www.symantec.com/security_response/glossary/define.jsp?letter=i&word=ike-internet-key-exchange

QUESTION 380
Which two primary security concerns can you mitigate with a BYOD solution? (Choose two)

A. Schedule for patching the device
B. compliance with applicable policies
C. device lagging and inventory
D. Connections to public Wi-Fi networks
E. Securing access to a trusted corporate network.

Answer: BE

QUESTION 381
Which command should be used to enable AAA authentication to determine if a user can access the privilege command level?

A. aaa authentication enable level
B. aaa authentication enable default local
C. aaa authentication enable method default
D. aaa authentication enable local

Answer: B
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/fsecur_r/srfathen.html

QUESTION 382
Which type of firewall can serve as the intermediary between a client and a server?

A. Application firewall
B. stateless firewall
C. Personal firewall
D. Proxy firewall

Answer: D
Explanation:
http://searchsecurity.techtarget.com/definition/proxy-firewall

QUESTION 383
What is the highest security level that can be configured for an interface on an ASA?

A. 0

B. 50
C. 100
D. 200

Answer: C
Explanation:
Security level 100: This is the highest security level on our ASA and by default this is assigned to the "inside" interface. Normally we use this for our "LAN". Since this is the highest security level, by default it can reach all the other interfaces.
https://networklessons.com/cisco/asa-firewall/cisco-asa-security-levels/

QUESTION 384
Which two characteristics of a PVLAN are true?

A. isolated ports cannot communicate with other ports on the same VLAN.
B. They require VTP to be enabled in server mode.
C. Promiscuous ports can communicate with PVLAN ports
D. PVLAN ports can be configured as EtherChannel ports.
E. Community ports have to be a part of the trunk.

Answer: AC
Explanation:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/pvlans.pdf

QUESTION 385
By default, how does a zone-based firewall handle traffic to and from the self zone?

A. It permits all traffic without inspection.
B. It inspects all traffic to determine how it is handled.
C. it permits all traffic after inspection
D. it drops all traffic.

Answer: C

QUESTION 386
Which two options are the primary deployment models for mobile device management? (Choose two)

A. Single-site
B. hybrid cloud-based
C. on-permises
D. Cloud based
E. Multisite

Answer: CD
Explanation:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_MDM_Int.pdf

QUESTION 387
How does a zone paid handle traffic if the policy definition of the zone pair is missing?

A. It permits all traffic without logging.
B. it drops all traffic
C. it permits and logs all traffic
D. it inspects all traffic

Answer: B

QUESTION 388
Which two characteristics of symmetric encryption are true? (Choose two)

A. It uses digital certificates.
B. It uses a public key and a private key to encrypt and decrypt traffic.
C. it requires more resources than asymmetric encryption
D. it is faster than asymmetric encryption
E. It uses the same key to encrypt and decrypt the traffic.

Answer: DE
Explanation:
http://searchsecurity.techtarget.com/definition/secret-key-algorithm

QUESTION 389
How can you protect CDP from reconnaissance attacks?

A. Enable dot1x on all ports that are connected to other switches.
B. Disable CP on ports connected to endpoints.
C. Enable dynamic ARP inspection on all untrusted ports.
D. Disable CDP on trunk ports.

Answer: B

QUESTION 390
Which Auto NAT policies are processed first ?

A. Dynamic with longest prefix
B. Dynamic with shortest prefix
C. Static with longest prefix
D. Static with shortest prefix

Answer: C
Explanation:
All packets processed by the ASA are evaluated against the NAT table. This evaluation starts at the top (Section 1) and works down until a NAT rule is matched. Once a NAT rule is matched, that NAT rule is applied to the connection and no more NAT policies are checked against the packet. + Section 1 - Manual NAT policies: These are processed in the order in which they appear in the configuration.
+ Section 2 - Auto NAT policies: These are processed based on the NAT type (static or dynamic)

and the prefix (subnet mask) length in the object.
+ Section 3 - After-auto manual NAT policies: These are processed in the order in which they appear in the configuration.
Source:
http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/116388-technote-nat-00.html

QUESTION 391
What are characteristics of the Radius Protocol? choose Two

A. Uses TCP port 49
B. Uses UDP Port 49
C. Uses TCP 1812/1813
D. Uses UDP 1812/1813
E. Comines authentication and authorization

Answer: DE

QUESTION 392
Which command is to make sure that AAA Authentication is configured and to make sure that user can access the exec level to configure?

A. AAA authentication enable default local
B. AAA authentication enable local
C. AAA authentication enable tacacs+ default

Answer: A

QUESTION 393
Which primary security attributes can be achieved by BYOD Architecture?

A. Trusted enterprise network
B. public wireless network
C. checking compliance with policy
D. pushing patches

Answer: AC

QUESTION 394
A user reports difficulties accessing certain external web pages, When examining traffic to and from the external domain in full packet captures, you notice many SYNs that have the same sequence number, source, and destination IP address, but have different payloads. Which problem is a possible explanation of this situation?

A. insufficient network resources
B. failure of full packet capture solution
C. misconfiguration of web filter
D. TCP injection

Answer: D

QUESTION 395
What is the primary purpose of the Integrated Services Routers (ISR) in the BYOD solution?

A. Provide connectivity in the home office environment back to the corporate campus
B. Provide WAN and Internet access for users on the corporate campus
C. Enforce firewall-type filtering in the data center
D. Provide connectivity for the mobile phone environment back to the corporate campus

Answer: A

QUESTION 396
Which is not a function of mobile device management (MDM)?

A. Enforce strong passwords on BYOD devices
B. Deploy software updates to BYOD devices
C. Remotely wipe data from BYOD devices
D. Enforce data encryption requirements on BYOD devices

Answer: B

QUESTION 397
The purpose of the certificate authority (CA) is to ensure what?

A. BYOD endpoints are posture checked
B. BYOD endpoints belong to the organization
C. BYOD endpoints have no malware installed
D. BYOD users exist in the corporate LDAP directory

Answer: B

QUESTION 398
The purpose of the RSA SecureID server/application is to provide what?

A. Authentication, authorization, accounting (AAA) functions
B. One-time password (OTP) capabilities
C. 802.1X enforcement
D. VPN access

Answer: B

QUESTION 399
What does ASA Transparent mode support?

A. it supports OSPF
B. it supports the use dynamic NAT
C. IP for each interface

D. requires a management IP address.

Answer: B

QUESTION 400
What will happen with traffic if zone-pair created, but policy did not applied?

A. All traffic will be droped.
B. All traffic will be passed with logging.
C. All traffic will be passed without logging.
D. All traffic will be inspected.

Answer: A

QUESTION 401
Which cisco IOS device support firewall, antispyware, anti-phishing, protection, etc.

A. Cisco IOS router
B. Cisco 4100 IOS IPS appliance
C. Cicso 5500 series ASA
D. Cisco 5500x next generation ASA

Answer: D

QUESTION 402
What configs are under crypto map? (Choose two)

A. set peer
B. set host
C. set transform-set
D. inerface

Answer: AC

QUESTION 403
Which two options are Private-VLAN secondary VLAN types?

A. Isolated
B. Secured
C. Community
D. Common
E. Segregated

Answer: AC

QUESTION 404
Which type of VLANs can communicate to PVLANs? (something like this) (choose 2)

A. promiscuous
B. isolated
C. community
D. backup
E. secondary

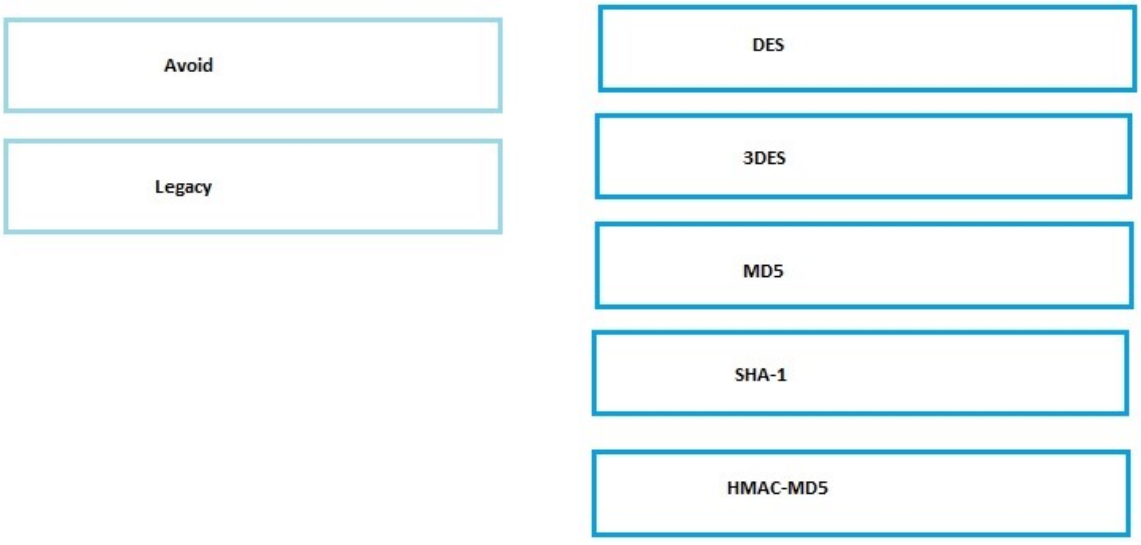
Answer: AB

QUESTION 405
What protocol provides CIA ?

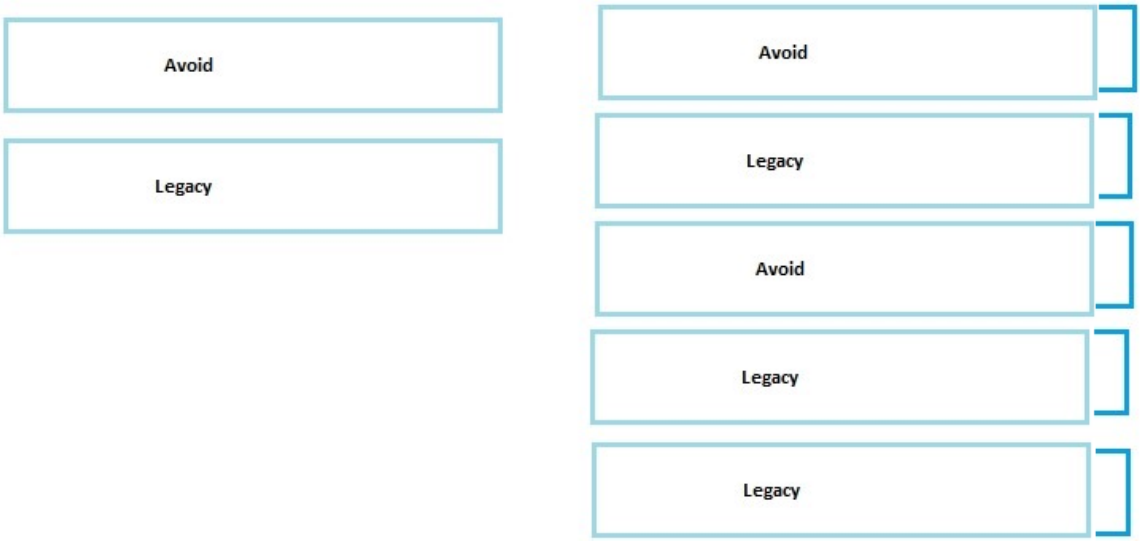
A. HA
B. ESP
C. IKEV1
D. IKEV2

Answer: B
Explanation:
Encapsulating Security Payload or ESP refers to the protocol which offers confidentiality on top of integrity and authentication to the IPSec data.

QUESTION 406
Drag and Drop Question
Drag the recommendations on the left to the Cryptographic Algorithms on the right. Options will be used more than once.

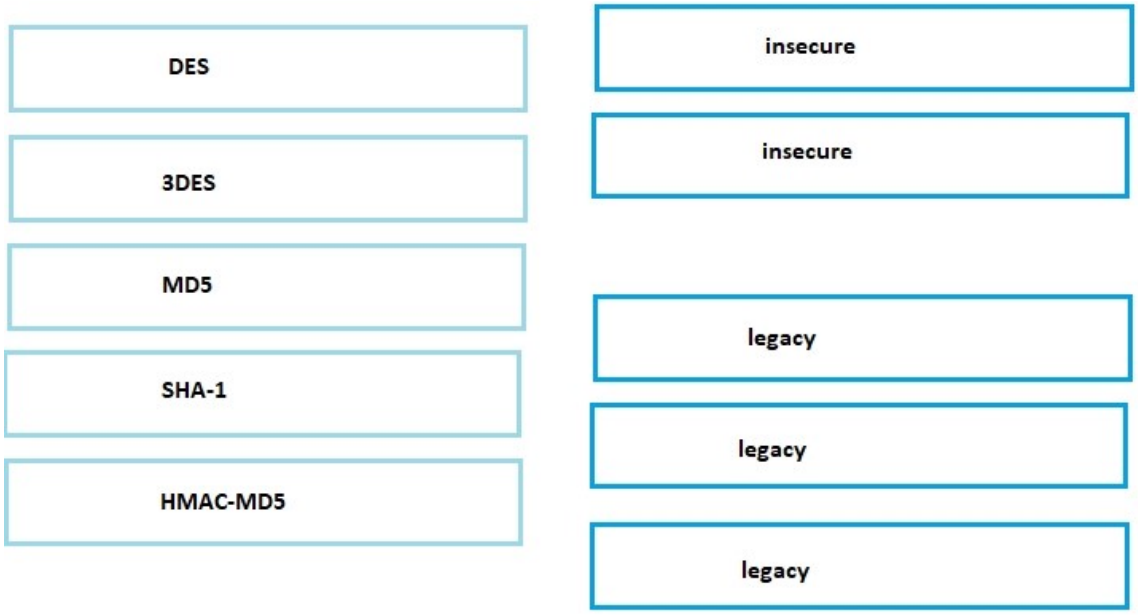


Answer:

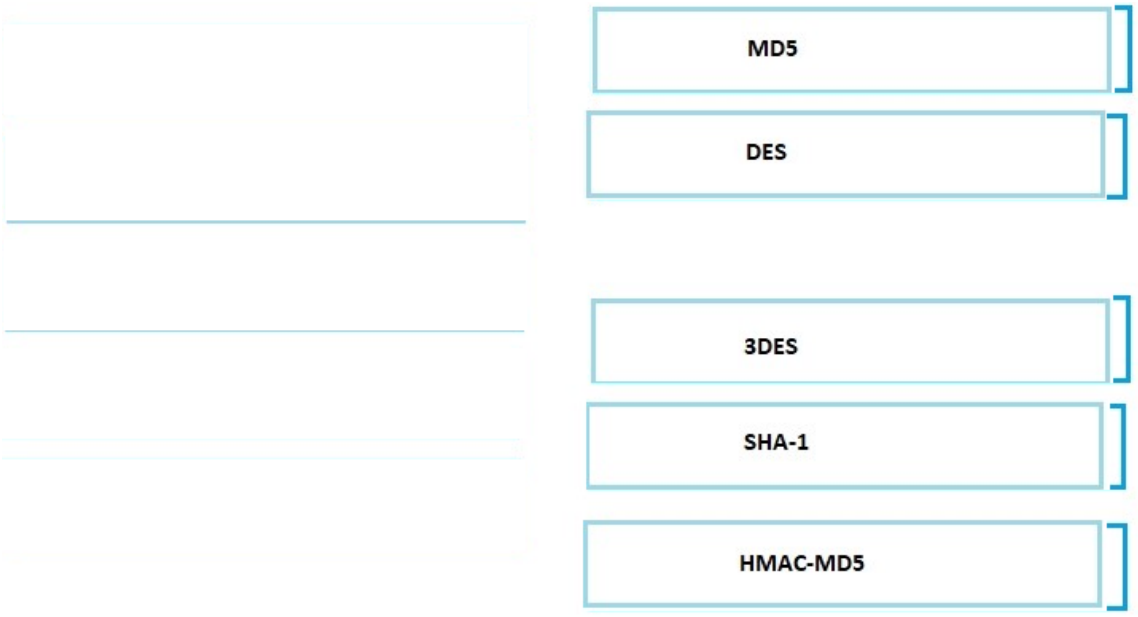


Explanation:
https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html

QUESTION 407
Drag and Drop Question
Drag the hash or algorithm from the left column to its appropriate category on the right.



Answer:



Explanation:
https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html

QUESTION 408
Which two default settings for port security are true? (Choose two.)

A. Maximum number of MAC addresses is 1.
B. Maximum number of MAC addresses is 2.
C. Violation is Restrict.
D. Violation is Protect.
E. Violation is Shutdown.

Answer: AE

QUESTION 409
Which networks topology describes multiple LANs in a geographically limited area?

A. CAN
B. MAN
C. SOHO
D. PAN

Answer: A
Explanation:
Campus Network (CAN) A network of multiple interconnected local area networks (LAN) in a limited geographical area.
https://www.techopedia.com/definition/25931/campus-area-network-can

QUESTION 410
Which IPSec mode is used to encrypt traffic directly between a client and a server VPN endpoint?

A. transport mode
B. tunnel mode
C. quick mode
D. aggressive mode

Answer: A

QUESTION 411
Which two characteristics of RADIUS are true? (Choose two.)

A. It encrypts only the password between user and server.
B. It uses UDP ports 1812/1813.
C. It uses TCP port 49.
D. It uses TCP ports 1812/1813.
E. It uses UDP port 49.

Answer: AB

QUESTION 412
Which protocol offers data integrity, encryption, authentication, and antireplay functions for IPsec VPN?

A. AH protocol
B. ESP protocol
C. IKEv2 protocol
D. IKEv1 protocol

Answer: B
Explanation:
IP Security Protocol--Encapsulating Security Payload (ESP) Encapsulating Security Payload (ESP) is a security protocol used to provide confidentiality (encryption), data origin authentication, integrity, optional antireplay service, and limited traffic flow confidentiality by defeating traffic flow analysis.
http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=3

QUESTION 413
Which two types of VLANs using PVLANs are valid? (Choose two.)

A. secondary
B. community
C. isolated
D. promiscuous
E. backup

Answer: BC

QUESTION 414
Which two types of firewalls work at Layer 4 and above? (Choose two.)

A. application-level firewall
B. static packet filter
C. stateful inspection
D. Network Address Translation
E. circuit-level gateway

Answer: AC

QUESTION 415
Which two commands are used to implement Cisco IOS Resilient Configuration? (Choose two.)

A. secure boot-image
B. copy running-config startup-config
C. secure boot-config
D. copy flash:/ios.bin tftp
E. copy running-config tftp

Answer: AC
Explanation:
The Cisco IOS Resilient Configuration feature enables a router to secure and maintain a working copy of the running image and configuration so that those files can withstand malicious attempts to erase the contents of persistent storage (NVRAM and flash).
In 12.3(8)T this feature was introduced.
The following commands were introduced or modified: secure boot-config, secure boot- image, showsecure bootset.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/15-mt/sec-usr-cfg-15-mt-book/sec-resil-config.html

QUESTION 416
Which mechanism does the FireAMP Connector use to avoid conflicts with other security applications such as antivirus products?

A. exclusions
B. virtualization
C. containers
D. sandboxing

Answer: A
Explanation:
To prevent conflicts between the FireAMP Connector and antivirus or other security software, you must create exclusions so that the Connector doesn't scan your antivirus directory and your antivirus doesn't scan the Connector directory. This can create problems if antivirus signatures contain strings that the Connector sees as malicious or cause issues with quarantined files. The first step is to create an exclusion by navigating to Management > Exclusions in the FireAMP console.
https://www.cisco.com/c/dam/en/us/td/docs/security/sourcefire/fireamp/fireamp-cloud/FireAMPDeploymentStrategy.pdf

QUESTION 417
Which two SNMP3 services support its capabilities as a secure network management protocol?

A. access control
B. authentication
C. the shared secret key
D. authorization
E. accounting

Answer: AB

QUESTION 418
Which component offers a variety of security solutions, including firewall, IPS, VPN, antispyware, antivirus, and antiphishing features?

A. Cisco ASA 5500-X Series Next Gen Security appliance.
B. Cisco IOS router
C. Cisco 4200 series IPS appliance
D. Cisco ASA 5500 series security appliance

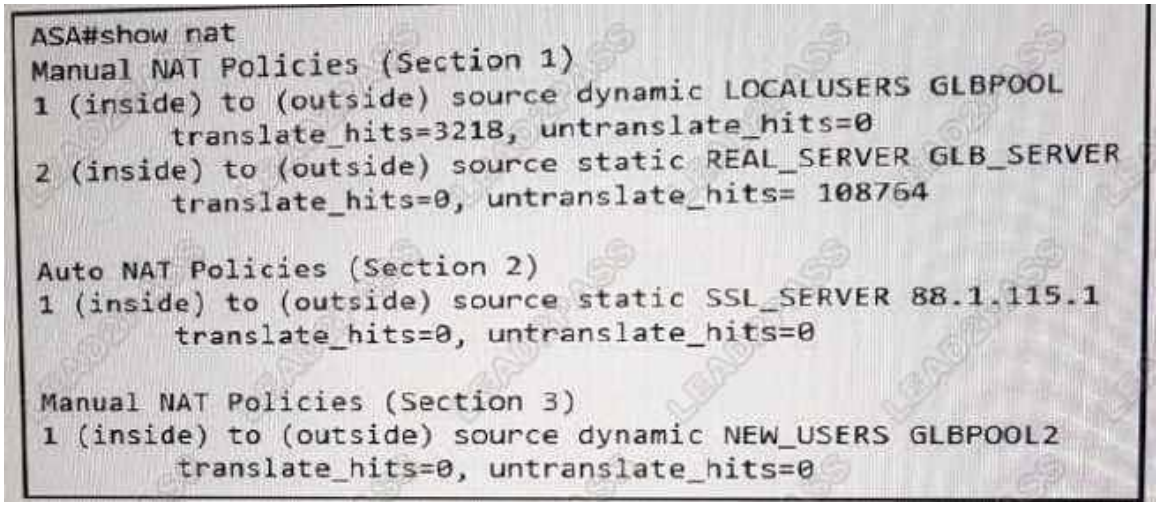
Answer: A

QUESTION 419
On an ASA, the policy that indicates that traffic should not be translated is often referred to as which of the following?

A. NAT zero
B. NAT allow
C. NAT null
D. NAT forward

Answer: A

QUESTION 420
Refer to the exhibit. A network security administrator checks the ASA firewall NAT policy table with the show nat command. Which statement is false?



A. There are only reverse transalation matches for the REAL_SERVER object.
B. First policy in the Section 1 is as dynamic nat entry defined in the object configuration.
C. NAT policy in Section 2 is a static entry defined in the obkect configuration
D. Transalation in Section 3 used when a connection does not match any entries in first two sections.

Answer: B

QUESTION 421
Which two attack types can be prevented with the implementation of a Cisco IPS solution? (Choose two)

A. ARP spoofing
B. DDoS
C. VLAN hopping
D. man-in-the-middle
E. worms

Answer: DE

QUESTION 422
Which EAp method authentic a client against Active Directory without the use client-side 80.1x certificates?

A. EAP-MSCHAPV2
B. EAP-GTC
C. EAP-TLS
D. EAP-PEAP

Answer: A

QUESTION 423
Which two attack types can be prevented with the implementation of a Cisco IPS solution?(Choose two.)

A. VLAN hooping
B. DDos
C. Worms
D. ARP spoofing
E. man-in-the -middle

Answer: CE

QUESTION 424
Which STP feature can prevent an attacker from becoming the root bridge by immediately shutting down the interface when it receives a BPDU?

A. BPDU filtering

B. root guard
C. BPDU guard
D. portFast

Answer: C

QUESTION 425
Which two ESA services are available for incoming and outgoing mails? (Choose two.)

A. DLP
B. reputation filter
C. content filter
D. anti-Dos
E. antispam

Answer: CE

QUESTION 426
Which IKE phase 1 parameter can you use to require the site-to-site VPN to us a pre-shared key?

A. group
B. hash
C. authentication
D. encryption

Answer: C

QUESTION 427
Which command do you enter to verify the status and settings of an IKE Phase 1 tunnel?

A. show crypto Ipsec as output
B. show crypto isakmp policy
C. show crypto isakmp sa
D. show crypto ipsec transform-sat

Answer: C

QUESTION 428
Which statement represents a difference between an access list on an ASA versus an acess list on a router?

A. The ASA does not support extended access lists
B. The ASA does not support number access lists
C. The ASA does not ever use a wildcard mask
D. The ASA does not support standard access lists

Answer: C

QUESTION 429
What are two limitations of the self-zone policies on a zone-based firewall? (Choose two)

A. They restnct SNMP traffic
B. They are unable to implement application inspection
C. They are unable to block HTTPS traffic
D. They are unable to support HTTPS traffic
E. They are unable to perform rate limiting.

Answer: BE

QUESTION 430
Which two descriptions of TACACS+ are true? (Choose two.)

A. It uses TCP as its transport protocol.
B. It combines authentication and authorization.
C. Only the password is encrypted.
D. The TACACS+ header is unencrypted
E. It uses UDP as its transport protocol.

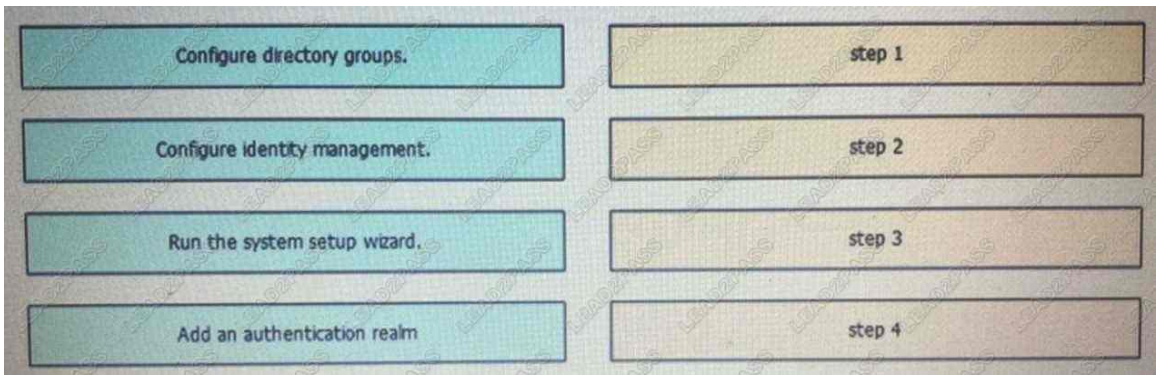
Answer: AB

QUESTION 431
Which two actions does an IPS perform? (Choose two.)

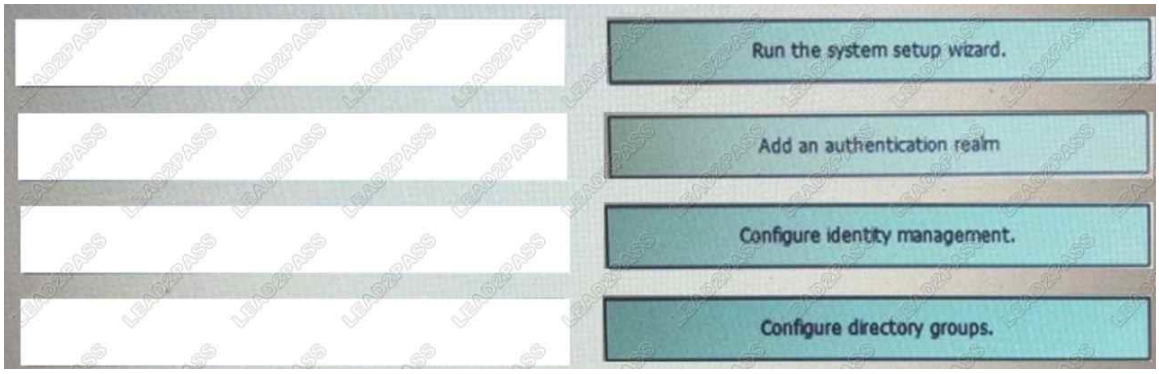
A. it spans the traffic
B. it reconfigures a device to block the traffic
C. it reflects the traffic back to the sender
D. it encrypts the traffic
E. it terminates the user session or connection of the attacker

Answer: AE

QUESTION 432
Drag and Drop Question
Drag and drop the steps to configure a WSA from the left into the correct order on the right.



Answer:



QUESTION 433
In which form of fraud does an attacker try to team information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels'?

A. Hacking
B. Phishing
C. Identity Spoofing
D. Smarting

Answer: B

QUESTION 434
What is a limitation of network-based IPS?

A. It is most effective at the individual host level.
B. It must be individually configured to support every operating system on the network.
C. It is unable to monitor attacks across the entire network.
D. Large installations require numerous sensors to fully protect the network

Answer: D

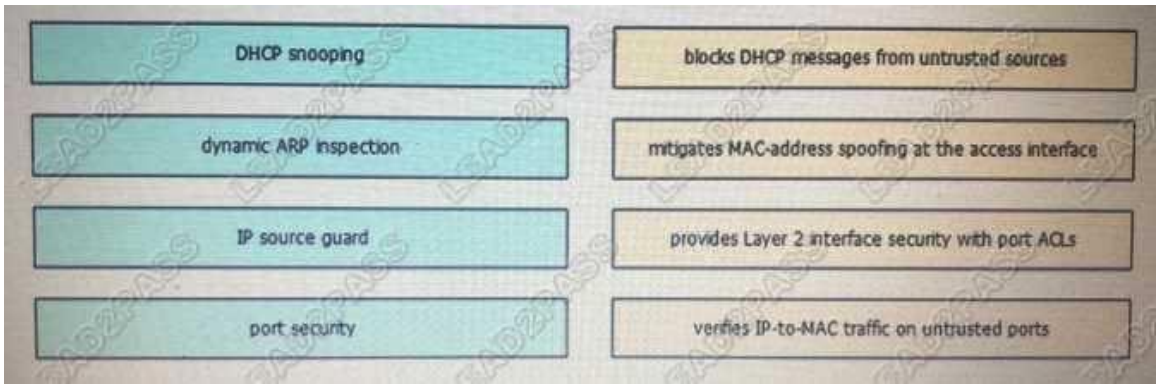
QUESTION 435
Which feature can help a router or switch maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch?

A. Control Plane Policing
B. Service Policy
C. Cisco Express Forwarding
D. Policy Map

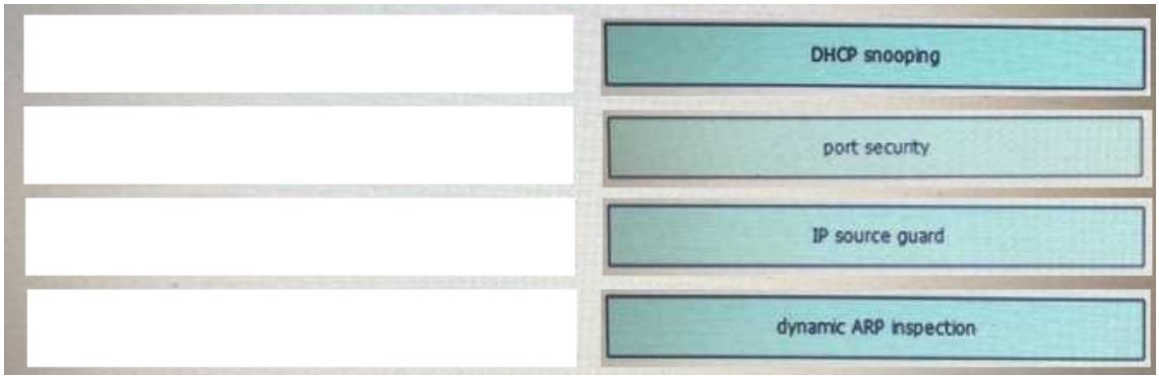
Answer: A

QUESTION 436
Drag and Drop Question

Drag and drop each feature that can protect against DHCP attacks from the left onto the correct description on the right.



Answer:



QUESTION 437
Which command successfully creates an administrative user with a password of "Cisco" on a Cisco router?

A. usemame Operator privilege 7 password Cisco
B. username Operator privilege 1 password cisco
C. user name Operator privilege 15 password cisco
D. usemame Operator password cisco privilege 15

Answer: C

QUESTION 438
Which technology can best protect data at rest on a user system?

A. network IPS
B. router ACL
C. full-disk encryption
D. IPsec tunnel

Answer: C

QUESTION 439
What are two reasons to recommend SNMPv3 over SNMPv2? (Choose two.)

A. SNMPv3 is secure because you can configure authentication and privacy
B. SNMPv3 is a Cisco proprietary protocol
C. SNMPv2 is secure because you can configure authentication and privacy
D. SNMPv2 is insecure because it sends information in clear text
E. SNMPv3 is insecure because it sends information in clear text

Answer: AD

QUESTION 440
Which two options are primary deployment model for mobile device management (Choose two)

A. Cloud-based
B. Hybrid-cloud based
C. Multisite
D. On-Perimeter
E. Single site

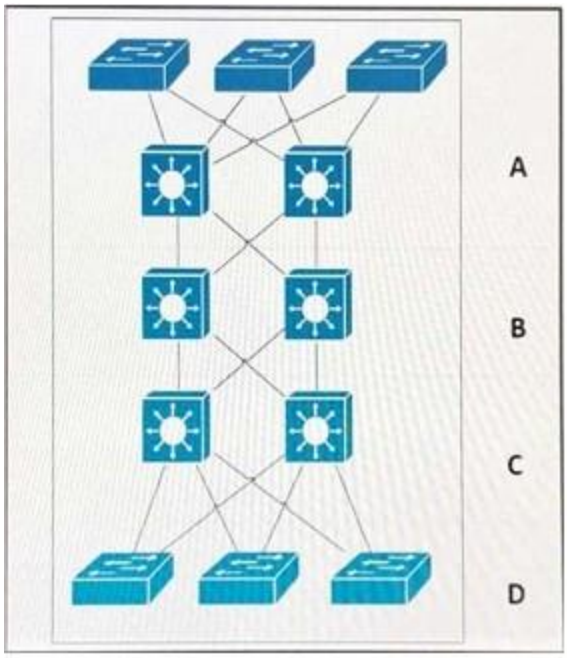
Answer: AD

QUESTION 441
Which two are valid types of VLANs using PVLANs? (Choose two.)

A. Backup VLAN
B. Secondary VLAN
C. Promiscuous VLAN
D. Community VLAN
E. Isolated VLAN

Answer: DE

QUESTION 442
Refer to the exhibit. Which area represents the data center?



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

Answer: A

QUESTION 443
Which security principle has been violated if data is altered in an unauthorized manner?

A. accountability
B. availability
C. confidentiality
D. integrity

Answer: D

QUESTION 444
Which two actions can a zone-based firewall apply to a packet as it transits a zone pair? (Choose two.)

A. drop
B. inspect
C. queue
D. quarantine
E. block

Answer: AB

QUESTION 445
Which information can you display by executing the show crypto ipsec sa command?

A. proxy information for the connection between two peers
B. IPsec SAs established between two peers
C. recent changes to the IP address of a peer router
D. ISAKMP SAs that are established between two peers

Answer: C

QUESTION 446
Which command can you enter to configure OSPF to use hashing to authenticate routing updates?

A. ip ospf authentication message-digest
B. ip ospf priority 1
C. neighbor 192.168.0.112 cost md5
D. ip ospf authentication-key

Answer: C

QUESTION 447
How is management traffic isolated on a Cisco ASR 1002?

A. Traffic is isolated based upon how you configure routing on the device
B. There is no management traffic isolation on a Cisco ASR 1002
C. The management interface is configured in a special VRF that provides traffic isolation from the default routing table
D. Traffic isolation is done on the VLAN level

Answer: D

QUESTION 448
Which statement about traffic inspection using the Cisco Modular Policy Framework on the ASA is true?

A. HTTP inspection is supported with Cloud Web Security inspection
B. QoS policing and QoS pnonty queuing can be configured for the same traffic
C. ASA with FirePOWER supports HTTP inspection
D. Traffic can be sent to multiple modules for inspection

Answer: A

QUESTION 449
Which feature can help a router or switch maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch?

A. Control Plane Policing

B. Policy Map
C. Service Policy
D. Cisco Express Forwarding

Answer: A

QUESTION 450
Refer to the exhibit. What is the effect of the given configuration?

```
Router1config)#interface fastEthernet 0/0
Router1(config-if)#ip ospf message-digest-key 1 md5 CISCOPASS
Router1(config-if)#ip ospf authentication message-digest

Router2(config)#interface fastEthernet 0/0
Router2(config-if)#ip ospf message-digest-key 1 md5 CISCOPASS
Router2(config-if)#ip ospf authentication message-digest
```

A. The two routers receive normal updates from one another
B. It enables authentication
C. It prevents keycham authentication
D. The two devices are able to pass the message digest to one another.

Answer: D

QUESTION 451
What are two challenges of using a network-based IPS? (Choose two)

A. It must support multiple operating systems
B. It is unable to determine whether a detected attack was successful.
C. As the network expands, it requires you to add more sensors
D. It requires additional storage and processor capacity on syslog servers.
E. It is unable to detect attacks across the entire network

Answer: CE

QUESTION 452
How can you prevent NAT rules from sending traffic to incorrect interfaces?

A. Configure twice NAT instead of object NAT
B. Add the no-proxy-arp command to the nat line
C. Assign the output interface in the NAT statement
D. Use packet-tracer rules to reroute misrouted NAT entries

Answer: D

QUESTION 453

How does the 802.1x supplicant communicate with the authentication server?

A. The supplicant creates EAP packets and sends them to the authenticator. which translates them into RADIUS and forwards them to the authentication server
B. The supplicant creates EAP packets and sends them to the authenticator. which encapsulates them into RADIUS and forwards them to the authentication server
C. The supplicant creates RADIUS packets and sends them to the authenticator, which translates them into EAP and forwards them to the authentication server
D. The supplicant creates RADIUS packets and sends them to the authenticator. which encapsulates them into EAP and forwards them to the authentication server

Answer: B

QUESTION 454
Which two advantages does the on-premise model for MDM deployment have over the cloud-based model? (Choose two)

A. The on-premise moctel provides more control of the MDM solution than the cloud-based model
B. The on-premise model is more scalable than the cloud-based model
C. The on-premtse model is generally less expensive than the cloud-based model
D. The on-premise model is easier and faster to deploy than the cloud-based model
E. The on-premise model generally has less latency than the cloud-based model

Answer: AE

QUESTION 455
What are two advanced features of the Cisco AMP solution for endpoints? (Choose two)

A. reflection
B. foresight
C. sandboxing
D. contemplation
E. reputation

Answer: CE

QUESTION 456
Which action does standard antivirus software perform as part of the file-analysis process?

A. execute the file in a simulated environment to examine its behavior
B. flag the unexamined file as a potential threat
C. examine the execution instructions in the file
D. create a backup copy of the file

Answer: A

QUESTION 457
What does the policy map do in CoPP?

A. defines the action to be performed
B. defines packet selection parameters
C. defines the packet filter
D. defines service parameters

Answer: A

QUESTION 458
Where does ip dhcp snooping trust command use?

A. Where the dhcp server is connected
B. At the aggregation point
C. At access layer

Answer: A

QUESTION 459
Which statement about NAT table evaluation in the ASA in true?

A. Auto-NAT executed first
B. After Auto-NAT executed first
C. Auto-NAT executed after the Manual NAT

Answer: A

QUESTION 460
Which two parameters can you view in the Cisco ASDM Protocol Statistics window? (Choose two)

A. the number of active tunnels
B. the number of rejected connection attempts
C. the number of tunnels that have been established since the Cisco ASA was rebooted
D. the number of closed tunnels
E. the user attempting the connection

Answer: AE

QUESTION 461
When would you configure the ip dhcp snooping trust command on a switch'?

A. when the switch is working in an edge capacity
B. when the switch is connected to a client system
C. when the switch is serving as an aggregator
D. when the switch is connected to a DHCP server

Answer: C

QUESTION 462

Which command can you enter to verify the status of Cisco IOS Resilient Configuration on a Cisco router?

A. show binary file
B. secure boot-config
C. secure boot-image
D. show secure bootset

Answer: D

QUESTION 463
Which command do you enter to verify the Pnase 1 status of a VPN connection?

A. debug crypto isakm
B. sh crypto session
C. sh crypto isakmp sa
D. sh crypto ipsec sa

Answer: D

QUESTION 464
What are two default behaviour of the traffic on a zone-based firewall? (Choose two.)

A. The CBAC rules that are configure on router interface apply to zone interfaces.
B. Communication is blocked between interfaces that are members of the same zone.
C. Traffic within self zone uses an implicit deny all
D. All traffic between zones is implicitly blocked.
E. Communication is allowed beteen interfaces that are members of the same zone.

Answer: DE

QUESTION 465
A user on your network inadvertently activates a botnet program that was received as an email attachment Which type of mechanism does Cisco Firepower use to detect and block only the botnet attack?

A. network-based access control rule
B. botnet traffic filter
C. reputation-based
D. user-based access control rule

Answer: B

QUESTION 466
Which statement about NAT table evaluation in the ASA is true?

A. Manual NAT policies are applied first
B. The ASA uses the most specific match
C. Auto NAT policies are applied first

D. After-auto NAT polices are applied first

Answer: B