**Q1**
When the interface ACL and global ACL are configured. Not all access list entries are required.
Drag the correct three access list entries (from the left) and drop them (on the right) in order that is used when the interface ACL and global ACL are configured. Not all access list entries are required.
Select and Place:

- Implicit deny ip any any global access list rule entry
- Implicit deny ip any any interface access list rule
- Implicit permit ip any any interface access list rule entry
- Implicit permit ip any any global access list rule entry
- Interface access list entries
- Global access list entries
- Implicit permit ip any any from higher security level interface to lower security level interface

Correct Answer:
Question 2
Which two ways is the Cisco ASA CWS subscription licensed?
In which two ways is the Cisco ASA CWS subscription licensed? (Choose two.)
A. term only
B. term and seat
C. term and application
D. term and session
E. free with purchase of WSE 5-year term subscription license
Correct Answer: AB
Explanation/Reference:

Question 3
Which Cisco ASA NGFW license must the administrator have to detect and monitor the unauthorized command and
control network traffic?
A security administrator suspects that an internal system has been infected by malware and communicates with an external server.
Which Cisco ASA NGFW license must the administrator have to detect and monitor the unauthorized command and
control network traffic?
A. AVC
B. WSE
C. CWS
D. Botnet traffic
Correct Answer: D
Explanation/Reference:

Question 4
Which license is required on the Cisco ASA NGFW for an administrator to manage it securely from a remote laptop?
Which license is required on the Cisco ASA NGFW for an administrator to manage it securely from a remote laptop?
A. AnyConnect Endpoint Assessment
B. AnyConnect Premium
C. AnyConnect for Mobile
D. AnyConnect for Cisco VPN phone

Question 5
Which three input parameters of an end-user system are important for the administrator to identify?
When deploying clientless SSL VPN advanced application access, the administrator needs to collect information about the end-user system. Which three input parameters of an end-user system are important for the administrator to identify? (Choose three.)
A. types of applications and application protocols that are supported
B. types of encryption that are supported on the end-user system
C. the local privilege level of the remote user
D. types of wireless security that are applied to the end-user tunnel interface
E. types of operating systems that are supported on the end-user system
F. type of antivirus software that is supported on the end-user system
Correct Answer: ACE
Explanation/Reference:

Question 6
Which three statements concerning smart tunnel applications are true?
Your IT department needs to run a custom-built TCP application within the clientless SSL VPN tunnel. The network administrator suggests running the smart tunnel application. Which three statements concerning smart tunnel applications are true? (Choose three.)
A. They support active FTP and other RTSP-based applications.
B. They do not require administrator privileges on the remote system.
C. They require the enabling of port forwarding.
D. They are supported on Windows and MAC OS X platforms.
E. They support native client applications over SSL VPN.
F. They require the modification of the Host file on the end-user PC.
Correct Answer: BDE
Explanation/Reference:

Question 7
Which three options are characteristics of Web Type ACLs?
Which three options are characteristics of Web Type ACLs? (Choose three.)
A. They are assigned per-connection profile.
B. They are assigned per-user or per-group policy.
C. They can be defined in the Cisco AnyConnect Profile Editor.
D. They support URL pattern matching.
E. They support implicit deny all at the end of the ACL.
F. They support standard and extended WebType ACLs.
Correct Answer: BDE
Explanation/Reference:

Question 8
Which three are characteristics of DTLS?
Datagram Transport Layer Security (DTLS) was introduced to solve performance issues. Which three are characteristics of DTLS? (Choose three.)
A. It uses TLS to negotiate and establish DTLS connections.
B. It uses DTLS to transmit datagrams.
C. It is disabled by default.
D. It uses TLS for data packet retransmission.
E. It replaces underlying transport layer with UDP 443.
F. It uses TLS to provide low-latency video application tunneling.
Correct Answer: ABE
Explanation/Reference:

**Question 9**
Which three bookmark types are supported?
You are configuring bookmarks for the clientless SSL VPN portal without the use of plug-ins. Which three bookmark types are supported? (Choose three.)
A. RDP
B. HTTP
C. FTP
D. CIFS
E. SSH
F. Telnet

Correct Answer: BCD
Explanation/Reference:

**Question 10**
When the user “contractor” Cisco AnyConnect tunnel is established, what type of Cisco ASA user restrictions are applied to the tunnel?
Refer to the exhibit.

When the user “contractor” Cisco AnyConnect tunnel is established, what type of Cisco ASA user restrictions are applied to the tunnel?
A. full restrictions (no Cisco ASDM, no CLI, no console access)
B. full restrictions (no read, no write, no execute permissions)
C. full restrictions (CLI show commands and Cisco ASDM monitoring permissions only)
D. full access with no restrictions

Correct Answer: D
Explanation/Reference:

**Question 11**
Where should the engineer navigate to, in order to find all the postlogin session parameters?
Refer to the exhibit.
A NOC engineer needs to tune some postlogin parameters on an SSL VPN tunnel. From the information shown, where should the engineer navigate to, in order to find all the postlogin session parameters?

A. “engineering” Group Policy  
B. “contractor” Connection Profile  
C. DefaultWEBVPNGroup Group Policy  
D. DefaultRAGroup Group Policy  
E. “engineer1” AAA/Local Users

Correct Answer: A
Explanation/Reference:

Question 12
Which three action ranges are in the NG IPS profile?
Which three action ranges are in the NG IPS profile? (Choose three.)
A. block only  
B. block and monitor  
C. block and do not monitor  
D. allow only  
E. allow and monitor  
F. allow and do not monitor

Correct Answer: BEF
Explanation/Reference:

Question 13
Which command enables the stateful failover option?
Refer to the exhibit.

Which command enables the stateful failover option?
A. failover link MYFAILOVER GigabitEthernet0/2  
B. failover lan interface MYFAILOVER GigabitEthernet0/2  
C. failover interface ip MYFAILOVER 172.16.5.1 255.255.255.0 standby 172.16.5.10  
D. preempt  
E. failover group 1

Question 14
When the Cisco ASA appliance is processing packets, which action is performed first?
A. Check if the packet is permitted or denied by the inbound interface ACL.
B. Check if the packet is permitted or denied by the outbound interface ACL.
C. Check if the packet is permitted or denied by the global ACL.
D. Check if the packet matches an existing connection in the connection table.
E. Check if the packet matches an inspection policy.
F. Check if the packet matches a NAT rule.

Correct Answer: D

Question 15
Which two options show the required Cisco ASA command(s) to allow this scenario?
An inside client on the 10.0.0.0/8 network connects to an outside server on the 172.16.0.0/16 network using TCP and the server port of 2001. The inside client negotiates a client port in the range between UDP ports 5000 to 5500. The outside server then can start sending UDP data to the inside client on the negotiated port within the specified UDP port range. Which two options show the required Cisco ASA command(s) to allow this scenario? (Choose two.)
A. access-list INSIDE line 1 permit tcp 10.0.0.0 255.0.0.0 172.16.0.0 255.255.0.0 eq 2001 access-group INSIDE in interface inside
B. access-list INSIDE line 1 permit tcp 10.0.0.0 255.0.0.0 172.16.0.0 255.255.0.0 eq 2001 access-list INSIDE line 2 permit udp 10.0.0.0 255.0.0.0 172.16.0.0 255.255.0.0 eq established access-group INSIDE in interface inside
C. access-list OUTSIDE line 1 permit tcp 172.16.0.0 255.255.0.0 10.0.0.0 255.0.0.0 eq 2001 10.0.0.0 255.0.0.0 access-list OUTSIDE line 2 permit udp 172.16.0.0 255.255.0.0 10.0.0.0 255.0.0.0 eq 5000-5500 access-group OUTSIDE in interface outside
D. access-list OUTSIDE line 1 permit tcp 172.16.0.0 255.255.0.0 10.0.0.0 255.0.0.0 eq 2001 10.0.0.0 255.0.0.0 access-list OUTSIDE line 2 permit udp 172.16.0.0 255.255.0.0 10.0.0.0 255.0.0.0 eq established access-group OUTSIDE in interface outside
E. established tcp 2001 permit udp 5000-5500
F. established tcp 2001 permit from udp 5000-5500
G. established tcp 2001 permit to udp 5000-5500

Correct Answer: AG

Question 16
Which two statements correctly describe the NAT table or NAT operations?
On Cisco ASA Software Version 8.3 and later, which two statements correctly describe the NAT table or NAT operations? (Choose two.)
A. The NAT table has four sections.
B. Manual NAT configurations are found in the first (top) and/or the last (bottom) section(s) of the NAT table.
C. Auto NAT also is referred to as Object NAT.
D. Auto NAT configurations are found only in the first (top) section of the NAT table.
E. The order of the NAT entries in the NAT table is not relevant to how the packets are matched against the NAT table.
F. Twice NAT is required for hosts on the inside to be accessible from the outside.

Correct Answer: BC

Question 17
Which traffic is permitted on the inside interface without any interface ACLs configured?
Refer to the exhibit.

Which traffic is permitted on the inside interface without any interface ACLs configured?
A. any IP traffic input to the inside interface
B. any IP traffic input to the inside interface destined to any lower security level interfaces
C. only HTTP traffic input to the inside interface
D. only HTTP traffic output from the inside interface
E. No input traffic is permitted on the inside interface
F. No output traffic is permitted on the inside interface

Correct Answer: C

Question 18
Which MPF CLI configuration command?
On the Cisco ASA, tcp-map can be applied to a traffic class using which MPF CLI configuration command?
A. inspect
B. sysopt connection
C. tcp-options
D. parameters
E. set connection advanced-options

Correct Answer: E

Question 19
Which Cisco ASA CLI commands configure these static routes in the Cisco ASA routing table?
A. route dmz 10.2.2.0 0.0.0.255 172.16.1.10
route dmz 10.3.3.0 0.0.0.255 172.16.1.11
B. route dmz 10.2.2.0 0.0.0.255 172.16.1.10 1
route dmz 10.3.3.0 0.0.0.255 172.16.1.11 1
C. route dmz 10.2.2.0 0.0.0.255 172.16.1.10
route dmz 10.3.3.0 0.0.0.255 172.16.1.11 2
D. route dmz 10.2.2.0 255.255.255.0 172.16.1.10
route dmz 10.3.3.0 255.255.255.0 172.16.1.11
E. route dmz 10.2.2.0 255.255.255.0 172.16.1.10 1
route dmz 10.3.3.0 255.255.255.0 172.16.1.11 1
F. route dmz 10.2.2.0 255.255.255.0 172.16.1.10
route dmz 10.3.3.0 255.255.255.0 172.16.1.11 2

Correct Answer: F

Question 20
Which four unicast or multicast routing protocols are supported by the Cisco ASA appliance?
Which four unicast or multicast routing protocols are supported by the Cisco ASA appliance? (Choose four.)
A. RIP (v1 and v2)
B. OSPF
C. IS-IS
D. BGP
E. EIGRP
F. Bidirectional PIM
G. MOSPF
H. PIM dense mode
Correct Answer: ABEF
Explanation/Reference:

**Question 21**
Which two Cisco ASA licensing features are correct with Cisco ASA Software Version 8.3 and later?
Which two Cisco ASA licensing features are correct with Cisco ASA Software Version 8.3 and later? (Choose two.)
A. Identical licenses are not required on the primary and secondary Cisco ASA appliance.
B. Cisco ASA appliances configured as failover pairs disregard the time-based activation keys.
C. Time-based licenses are stackable in duration but not in capacity.
D. A time-based license completely overrides the permanent license, ignoring all permanently licensed features until the time-based license is uninstalled.
Correct Answer: AC
Explanation/Reference:

**Question 22**
Which Cisco Fire POWER services license must the administrator have to detect and monitor the unauthorized command-and-control network traffic?
Which Cisco Fire POWER services license must the administrator have to detect and monitor the unauthorized command-and-control network traffic?
A. AVC
B. WSE
C. CWS
D. AMP
Correct Answer: D
Explanation/Reference:

**Question 23**
Which Cisco SFR feature license is needed to allow a high school security administration to implement a policy to allow student access to only highreputation websites?
Which Cisco SFR feature license is needed to allow a high school security administration to implement a policy to allow student access to only highreputation websites?
A. AVC
B. Botnet Traffic Filtering
C. URL
D. NGIPS
E. AMP
Correct Answer: C
Explanation/Reference:

**Question 24**
Which three Fire POWER services features require a subscription license?
Which three Fire POWER services features require a subscription license? (Choose three.)
A. URL filtering
B. AVC
C. high availability

Question 25
Which two settings are configurable as part of a health policy?
Which two settings are configurable as part of a health policy? (Choose two.)
A. time-synchronization status
B. user access
C. intrusion policy preferences
D. database status
E. advanced malware protection

Correct Answer: AE
Explanation/Reference:

Question 26
Files may be submitted to the cloud-based sandbox for dynamic analysis using which two ports?
Files may be submitted to the cloud-based sandbox for dynamic analysis using which two ports? (Choose two.)
A. TCP/443
B. TCP/80
C. TCP/3389
D. TCP/500
E. TCP/32137

Correct Answer: AE
Explanation/Reference:

Question 27
Which threat score rating is the default value that identifies malware?
Which threat score rating is the default value that identifies malware?
A. greater than or equal to 80
B. greater than or equal to 76
C. greater than or equal to 75
D. greater than or equal to 85

Correct Answer: B
Explanation/Reference:

Question 28
Which three options are assignable file dispositions?
Which three options are assignable file dispositions? (Choose three.)
A. malware
B. unassigned
C. custom detection
D. user-defined
E. permit
F. unknown

Correct Answer: ACF
Explanation/Reference:

Question 29
Which statement describes what happens during a file-disposition check for malware?
Which statement describes what happens during a file-disposition check for malware?
A. The managed device extracts the pieces of file from the data stream, calculates a hash on each piece, and forwards each piece to the cloud for checking. If all pieces are clean, the original file is forwarded to the destination.
B. The managed device extracts all pieces of a file before calculating a hash on the complete file. Each piece is forwarded to the destination with the final piece being released if the entire file is deemed clean.
C. The managed device extracts all pieces of a file before calculating a hash on the complete file. If the entire file is deemed clean, it is forwarded to the destination.
D. The managed device extracts the pieces of file from the data stream, calculates a hash on each piece, and forwards each piece to the cloud for checking. All pieces are also forwarded to the destination with the last piece being forwarded if it is deemed clean.

Correct Answer: B
Explanation/Reference:

**Question 30**
Which three actions are supported by file policies?
Which three actions are supported by file policies? (Choose three.)
A. malware cloud lookup
B. Spero dynamic analysis
C. block files
D. detect malware
E. bypass
F. block malware

Correct Answer: ACF
Explanation/Reference:

**Question 31**
Which option best describes the role of an IoC?
Which option best describes the role of an IoC?
A. tags on a host that indicate that an infection event has occurred
B. statically assigned target values on a host
C. a flag that indicates that a host operating system needs patching
D. an impact flag of an infection event

Correct Answer: A
Explanation/Reference:

**Question 32**
A file-type embedded attack is an example of which IoC event category?
A file-type embedded attack is an example of which IoC event category?
A. security intelligence
B. IPS
C. malware
D. firewall

Correct Answer: C
Explanation/Reference:

**Question 33**
Detection of an exploit kit that is installed on a device is an example of which IoC event category?
Detection of an exploit kit that is installed on a device is an example of which IoC event category?
A. security intelligence
B. IPS
C. malware
D. firewall

Correct Answer: B
Explanation/Reference:
Question 34
Which option best describes what happens if a reputation is not available for a URL?
An access policy that uses URL reputation values is defined. Which option best describes what happens if a reputation is not available for a URL?
A. The URL check is not triggered, and the default policy action is applied.
B. The URL check fails, and the traffic is dropped.
C. The URL check is unknown, and the traffic is quarantined.
D. The URL check is not triggered and, by default, the user is prompted to take an action to permit or deny.

Correct Answer: A
Explanation/Reference:

Question 35
Which access policy action should be applied if traffic is to pass without applying any additional inspection?
Which access policy action should be applied if traffic is to pass without applying any additional inspection?
A. trust
B. allow
C. permit
D. monitor

Correct Answer: A
Explanation/Reference:

Question 36
Which port should be allowed to support communications between Sourcefire User Agent and FireSIGHT Management Center?
Which port should be allowed to support communications between Sourcefire User Agent and FireSIGHT Management Center?
A. TCP/3306
B. TCP/3389
C. UDP/3389
D. TCP/443

Correct Answer: A
Explanation/Reference:

Question 37
Which application is required to enable Microsoft Active Directory identity integration for FirePOWER services?
Which application is required to enable Microsoft Active Directory identity integration for FirePOWER services?
A. Sourcefire User Agent
B. Microsoft Active Directory Manager
C. Cisco Directory Agent
D. Microsoft Active Directory Agent

Correct Answer: A
Explanation/Reference:

Question 38
Which three policy types are configured using Fire SIGHT Management Center?
Which three policy types are configured using Fire SIGHT Management Center? (Choose three.)
A. remote access
B. file
C. health
D. network discovery
E. malware
F. access list
G. firewall
Question 39
Which command must be executed on the module to establish connectivity to FireSIGHT Management Center? An SFR module has been installed in the adaptive security appliance. Which command must be executed on the module to establish connectivity to FireSIGHT Management Center?
A. system install manager
B. config manager fmc host
C. config manager add
D. system manager fmc

Correct Answer: B
Explanation/Reference: