Exam Questions 642-618

Deploying Cisco ASA Firewall Solutions (FIREWALL v2.0)
1. 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
   Answer: E

2. By default, which traffic can pass through a Cisco ASA that is operating in transparent mode without explicitly allowing it using an ACL?
   A. ARP
   B. BPDU
   C. CDP
   D. OSPF multicasts
   E. DHCP
   Answer: A

3. When enabling a Cisco ASA to send syslog messages to a syslog server, which syslog level will produce the most messages?
   A. notifications
   B. informational
   C. alerts
   D. emergencies
   E. errors
   F. debugging
   Answer: F

4. Refer to the exhibit. What can be determined about the connection status?
   A. The output is showing normal activity to the inside 10.1.1.50 web server.
   B. Many HTTP connections to the 10.1.1.50 web server have successfully completed the three-way TCP handshake.
   C. Many embryonic connections are made from random sources to the 10.1.1.50 web server.
   D. The 10.1.1.50 host is triggering SYN flood attacks against random hosts on the outside.
   E. The 10.1.1.50 web server is terminating all the incoming HTTP connections.
   Answer: C

5. What mechanism is used on the Cisco ASA to map IP addresses to domain names that are contained in the botnet traffic filter dynamic database or local blacklist?
   A. HTTP inspection
   B. DNS inspection and snooping
C. WebACL
D. dynamic botnet database fetches (updates)
E. static blacklist
F. static whitelist
Answer: B

6. Refer to the exhibit.
Which statement about the policy map named test is true?
A. Only HTTP inspection will be applied to the TCP port 21 traffic.
B. Only FTP inspection will be applied to the TCP port 21 traffic.
C. both HTTP and FTP inspections will be applied to the TCP port 21 traffic.
D. No inspection will be applied to the TCP port 21 traffic, because the http class map configuration conflicts with the ftp class map.
E. All FTP traffic will be denied, because the FTP traffic will fail the HTTP inspection.
Answer: B

7. Refer to the exhibit.
Which Cisco ASA feature can be configured using this Cisco ASDM screen?
A. Cisco ASA command authorization using TACACS+
B. AAA accounting to track serial, ssh, and telnet connections to the Cisco ASA
C. Exec Shell access authorization using AAA
D. cut-thru proxy
E. AAA authentication policy for Cisco ASDM access
Answer: D

8. 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 primary
F. failover lan unit primary
Answer: A

9. In which type of environment is the Cisco ASA MPF set connection advanced-options tcp-statebypass option the most useful?
A. SIP proxy
B. WCCP
C. BGP peering through the Cisco ASA
D. asymmetric traffic flow
E. transparent firewall
10. Refer to the exhibit.

Which statement about the MPF configuration is true?

A. Any non-RFC complaint FTP traffic will go through additional deep FTP packet inspections.
B. FTP traffic must conform to the FTP RFC, and the FTP connection will be dropped if the PUT command is used.
C. Deep FTP packet inspections will be performed on all TCP inbound and outbound traffic on the outside interface.
D. The ftp-pm policy-map type should be type inspect.
E. Due to a configuration error, all FTP connections through the outside interface will not be permitted.

Answer: B

11. Refer to the exhibit.

What is a reasonable conclusion?

A. The maximum number of TCP connections that the 10.1.1.99 host can establish will be 146608.
B. All the connections from the 10.1.1.99 have completed the TCP three-way handshake.
C. The 10.1.1.99 hosts are generating a vast number of outgoing connections, probably due to a virus.
D. The 10.1.1.99 host on the inside is under a SYN flood attack.
E. The 10.1.1.99 host operations on the inside look normal.

Answer: C

12. By default, how does the Cisco ASA authenticate itself to the Cisco ASDM users?

A. The administrator validates the Cisco ASA by examining the factory built-in identity certificate thumbprint of the Cisco ASA.
B. The Cisco ASA automatically creates and uses a persistent self-signed X.509 certificate to authenticate itself to the administrator.
C. The Cisco ASA automatically creates a self-signed X.509 certificate on each reboot to authenticate itself to the administrator.
D. The Cisco ASA and the administrator use a mutual password to authenticate each other.
E. The Cisco ASA authenticates itself to the administrator using a one-time password.

Answer: C

13. When will a Cisco ASA that is operating in transparent firewall mode perform a routing table lookup instead of a MAC address table lookup to determine the outgoing interface of a packet?

A. if multiple context mode is configured
B. if the destination MAC address is unknown
C. if the destination is more than a hop away from the Cisco ASA
D. if NAT is configured
E. if dynamic ARP inspection is configured

Answer: D
14. Which flag shown in the output of the show conn command is used to indicate that an initial SYN packet is from the outside (lower security-level interface)?

A. B
B. D
C. b
D. A
E. a
F. i
G. I
H. O

Answer: A

15. Which statement about the default ACL logging behavior of the Cisco ASA is true?

A. The Cisco ASA generates system message 106023 for each denied packet when a deny ACE is configured.
B. The Cisco ASA generates system message 106023 for each packet that matched an ACE.
C. The Cisco ASA generates system message 106100 only for the first packet that matched an ACE.
D. The Cisco ASA generates system message 106100 for each packet that matched an ACE.
E. No ACL logging is enabled by default.

Answer: A

16. Which Cisco ASA feature enables the ASA to do these two things? 1) Act as a proxy for the server and generate a SYN-ACK response to the client SYN request. 2) When the Cisco ASA receives an ACK back from the client, the Cisco ASA authenticates the client and allows the connection to the server.

A. TCP normalizer
B. TCP state bypass
C. TCP intercept
D. basic threat detection
E. advanced threat detection
F. botnet traffic filter

Answer: C

17. Which option is not supported when the Cisco ASA is operating in transparent mode and also is using multiple security contexts?

A. NAT
B. shared interface
C. security context resource management
D. Layer 7 inspections
E. failover

Answer: B

18. Refer to the exhibit.
What does the * next to the CTX security context indicate?

A. The CTX context is the active context on the Cisco ASA.
B. The CTX context is the standby context on the Cisco ASA.
C. The CTX context contains the system configurations.
D. The CTX context has the admin role.

Answer: D

19. Which Cisco ASA feature is implemented by the `ip verify reverse-path interface interface_name` command?

A. uRPF
B. TCP intercept
C. botnet traffic filter
D. scanning threat detection
E. IPS (IP audit)

Answer: A

20. In one custom dynamic application, the inside client connects to an outside server using TCP port 4444 and negotiates return client traffic in the port range of 5000 to 5500. The server then starts streaming UDP data to the client on the negotiated port in the specified range. Which Cisco ASA feature or command supports this custom dynamic application?

A. TCP normalizer
B. TCP intercept
C. ip verify command
D. established command
E. tcp-map and tcp-options commands
F. set connection advanced-options command

Answer: D
Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

642-618 Practice Exam Features:

* 642-618 Questions and Answers Updated Frequently
* 642-618 Practice Questions Verified by Expert Senior Certified Staff
* 642-618 Most Realistic Questions that Guarantee you a Pass on Your First Try
* 642-618 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 642-618 Practice Test Here