ISLEVER

642-618

Deploying Cisco ASA Firewall Solutions (FIREWALL v2.0)

DEMO

https://www.islever.com/642-618.html

https://www.islever.com/cisco.html

For the most up-to-date exam questions and materials, we recommend visiting our website, where you can access the latest content and resources.

Note: The answer is for reference only, you need to understand all question.

QUESTION 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

QUESTION 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

QUESTION 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

QUESTION 4

Refer to the exhibit.

```
ASA-5510# show conn
54764 in use, 54764 most used
TCP outside 172.16.1.118:26093 inside 10.1.1.50:80, idle 0:00:23, bytes 0, flags aB
TCP outside 172.16.5.19:23598 inside 10.1.1.50:80, idle 0:00:13, bytes 0, flags aB
TCP outside 192.168.1.202:32729 inside 10.1.1.50:80, idle 0:00:25, bytes 0, flags aB
TCP outside 192.168.2.20:56481 inside 10.1.1.50:80, idle 0:00:29, bytes 0, flags aB
TCP outside 192.168.3.205:18073 inside 10.1.1.50:80, idle 0:00:02, bytes 0, flags aB
TCP outside 172.16.2.63:51503 inside 10.1.1.50:80, idle 0:00:03, bytes 0, flags aB
TCP outside 172.16.18.60:47733 inside 10.1.1.50:80, idle 0:00:27, bytes 0, flags aB
TCP outside 192.168.1.202:20773 inside 10.1.1.50:80, idle 0:00:02, bytes 0, flags aB
TCP outside 192.168.4.192:23112 inside 10.1.1.50:80, idle 0:00:06, bytes 0, flags aB
TCP outside 172.16.25.60:47733 inside 10.1.1.50:80, idle 0:00:27, bytes 0, flags aB
!<output omitted>

Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
    B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
    D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
    G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
    i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
    k - Skinny media, M - SMTP data, m - SIP media, n - GUP
    O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
    q - SQL*Net data, R - outside acknowledged FIN,
    R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
    s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
    V - VPN orphan, W - WAAS,
    X - inspected by service module
```

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

QUESTION 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

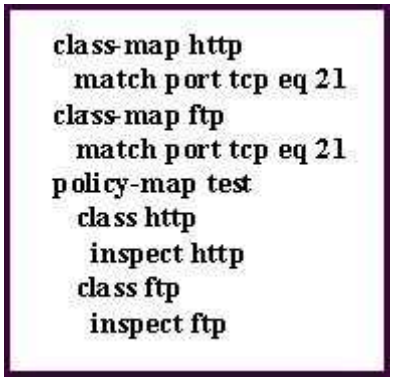
B. DNS inspection and snooping

C. WebACL

D. dynamic botnet database fetches (updates)
E. static blacklist
F. static whitelist

Answer: B

QUESTION 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

QUESTION 7
Refer to the exhibit.