Cisco 642-618

Deploying Cisco ASA Firewall Solutions (FIREWALL) V2.0

Version: 6.0

QUESTION NO: 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

Explanation:

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/conns_tcpnorm.html

QUESTION NO: 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

Explanation:

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/fwmode.html

QUESTION NO: 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

Explanation:

QUESTION NO: 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

Explanation:

QUESTION NO: 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

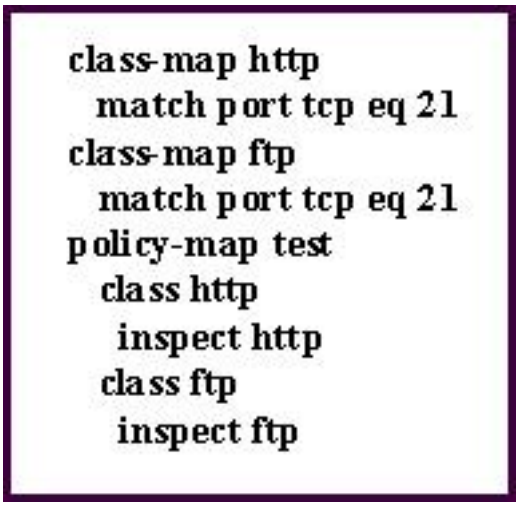
Answer: B

Explanation:

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/conns_botnet.html

QUESTION NO: 6

Refer to the exhibit.



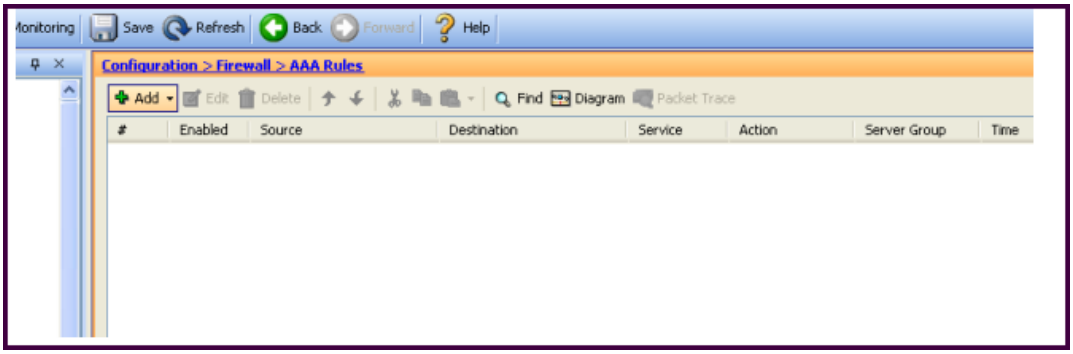
Which statement about the policy map named test is true?

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
Explanation:

QUESTION NO: 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
Explanation:
http://www.cisco.com/en/US/docs/security/asa/asa72/asdm52/user/guide/aaarules.html

And from

http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/access_idfw.html#wp1324095

Configuring Cut-through Proxy Authentication
In an enterprise, some users log onto the network by using other authentication mechanisms, such asauthenticating with a web portal (cut-through proxy) or by using a VPN. For example, users with a Machintoshand Linux client might log in a web portal (cut-through proxy) or byusing a VPN. Therefore, you must configurethe Identity Firewall to allow these types of authentication in connection with identity-based access policies.
The ASA designates users logging in through a web portal (cut-through proxy) as belonging to the

ActiveDirectory domain with which they authenticated. The ASA designates users logging in through a VPN asbelonging to the LOCAL domain unless the VPN is authenticated by LDAP with Active Directory, then theIdentity Firewall can associate the users with their Active Directory domain. The ASA reports users logging inthrough VPN authentication or a web portal (cut-through proxy) to the AD Agent, which distributes the userinformation to all registered ASA devices.
Users can log in by using HTTP/HTTPS, FTP, Telnet, or SSH. When users log in with these authenticationmethods, the following guidelines apply:
•For HTTP/HTTPS traffic, an authentication window appears for unauthenticated users.
•For Telnet and FTP traffic, users must log in through the cut-through proxy and again to Telnet and FTPserver.
•A user can specify an Active Directory domain while providing login credentials (in the format domain\username). The ASA automatically selects the associated AAA server group for the specified domain.
•If a user specifies an Active Directory domain while providing login credentials (in the format domain\username), the ASA parses the domain and uses it to select an authentication server from the AAA serversconfigured for the Identity Firewall. Only the username is passed to the AAA server.
•If the backslash (\) delimiter is not found in the log in credentials, the ASA does not parse a domain andauthentication is conducted with the AAA server that corresponds to default domain configured for the IdentityFirewall.
•If a default domain or a server group is not configured for that default domain, the ASA rejects theauthentication.
•If the domain is not specified, the ASA selects the AAA server group for the default domain that is configuredfor the Identity Firewall.

QUESTION NO: 8

Refer to the exhibit.

```
failover
failover lan unit primary
failover lan interface MYFAILOVER GigabitEthernet0/2
failover interface ip MYFAILOVER 172.16.5.1 255.255.255.0 standby 172.16.5.10
failover link  MYFAILOVER  GigabitEthernet0/2
failover key cisco123
failover group 1
primary
preempt
failover group 2
secondary
preempt
```

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

Explanation:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a00807dac5f.shtml

QUESTION NO: 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

Answer: D

Explanation:

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/conns_tcpstatebypass.html

QUESTION NO: 10

Refer to the exhibit.

```
class-map type inspect ftp match-all ftp-cmd
 match request-command put
policy-map type inspect ftp ftp-insp
 class ftp-cmd
 reset
access-list ftp-acl extended permit tcp any any eq ftp
class-map ftp-cm
 match access-list ftp-acl
policy-map ftp-pm
 class ftp-cm
  inspect ftp strict ftp-insp
service-policy ftp-pm interface outside
```

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
Explanation:

QUESTION NO: 11

Refer to the exhibit.

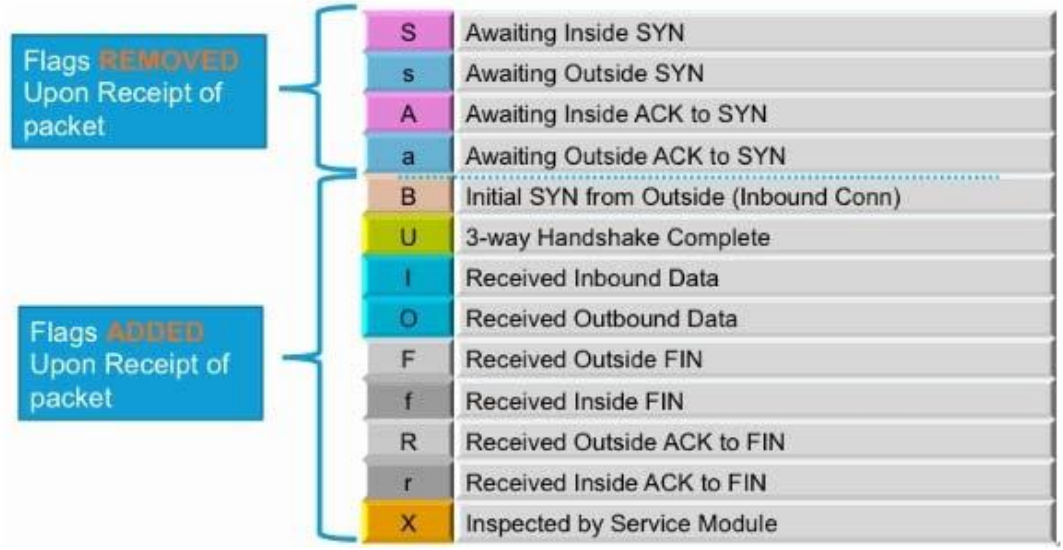
```
ASA# show local-host 10.1.1.99
Interface inside: 250 active, 250 maximum active, 0 denied
local host: <10.1.1.99>,
TCP connection count/limit = 146608/unlimited
TCP embryonic count = 146606
UDP connection count/limit = 0/unlimited
Xlate(s):
Global 209.165.201.21 Local 10.1.1.99
Conn(s):
TCP out 10.101.32.157:135 in 10.1.1.99:34580 idle 0:01:43 Bytes 0 flags saA
TCP out 10.103.108.191:135 in 10.1.1.99:8688 idle 0:01:43 Bytes 0 flags saA
TCP out 10.100.205.160:135 in 10.1.1.99:7774 idle 0:01:43 Bytes 0 flags saA
TCP out 10.101.182.19:135 in 10.1.1.99:39193 idle 0:01:43 Bytes 0 flags saA
TCP out 10.102.218.45:135 in 10.1.1.99:16462 idle 0:01:43 Bytes 0 flags saA
TCP out 10.100.21.120:135 in 10.1.1.99:30322 idle 0:01:43 Bytes 0 flags saA
TCP out 10.101.25.195:135 in 10.1.1.99:41116 idle 0:01:43 Bytes 0 flags saA
TCP out 10.103.17.219:135 in 10.1.1.99:59163 idle 0:01:43 Bytes 0 flags saA
TCP out 10.102.201.141:135 in 10.1.1.99:2978 idle 0:01:43 Bytes 0 flags saA
! <output omitted>
```

What is a reasonable conclusion?

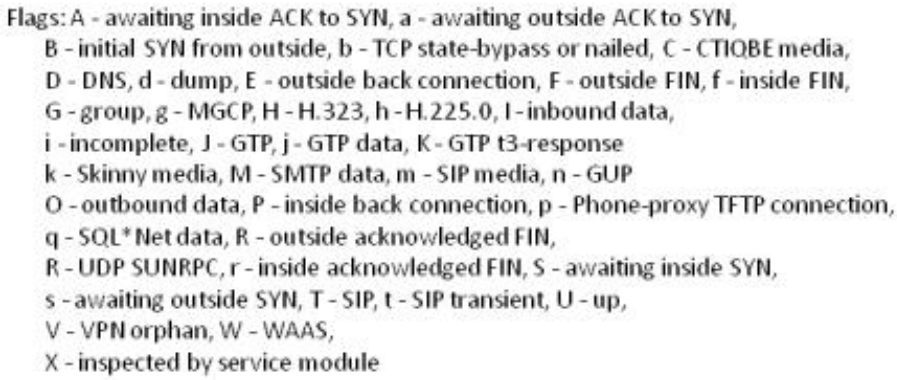
A. The maximum number of TCP connections that the 10.1.1.99 host can establish will be 146608.
B. All the connections from the 10.1.1.99 have completed the TCP three-way handshake.
C. The 10.1.1.99 hosts are generating a vast number of outgoing connections, probably due to a virus.
D. The 10.1.1.99 host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

Answer: C

Explanation:



C:\Documents and Settings\user-nwz\Desktop\1.JPG



C:\Documents and Settings\user-nwz\Desktop\1.JPG

QUESTION NO: 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
Explanation:
http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00808efbd2.shtml

QUESTION NO: 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