Cisco 642-617

Deploying Cisco ASA Firewall Solutions (FIREWALL v1.0)

Version: 4.8

QUESTION NO: 1

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

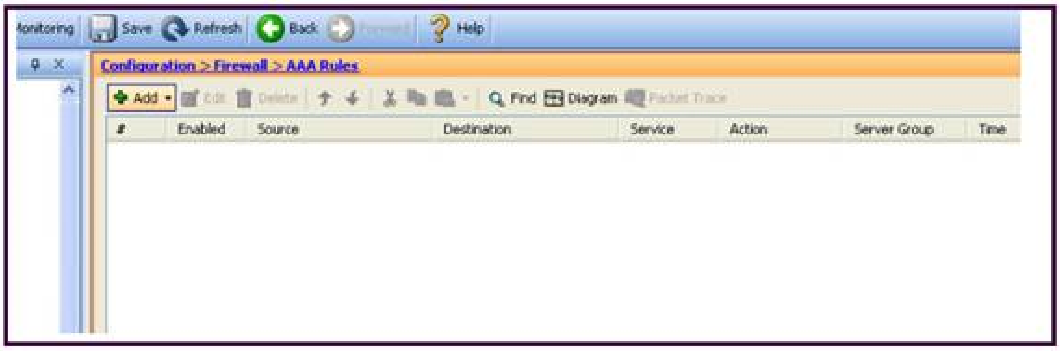
QUESTION NO: 2

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

QUESTION NO: 3



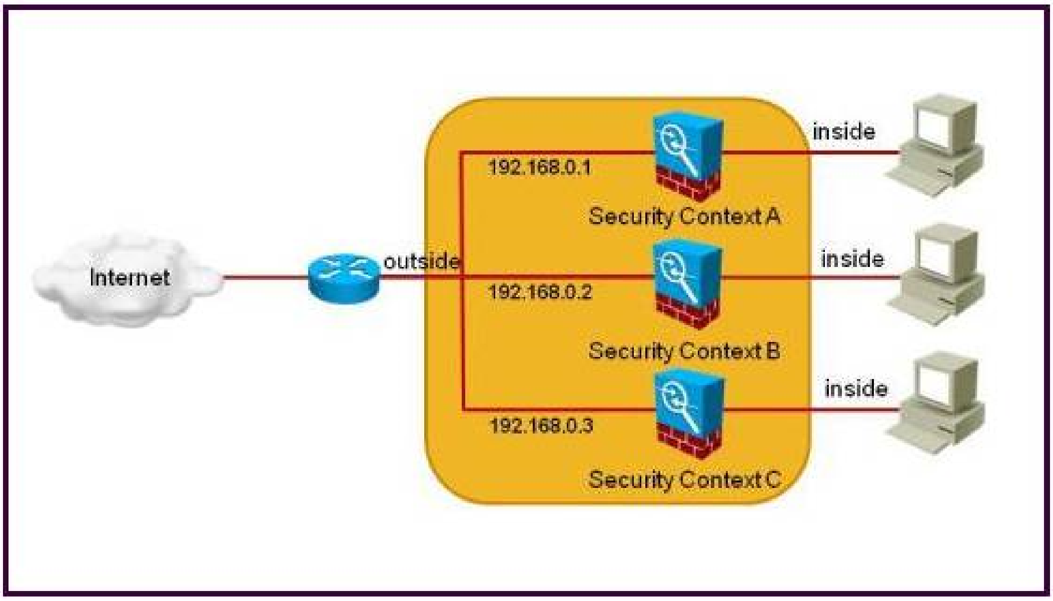
Referto the exhibit. Which Cisco ASA feature can be configured using this Cisco ASDM screen?

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

QUESTION NO: 4



Refer to the exhibit. The Cisco ASA is dropping all the traffic that is sourced from the internet and is destined to any security context inside interface. Which configuration should be verified on the Cisco ASA to solve this problem?

A. The Cisco ASA has NAT control disabled on each security context.
B. The Cisco ASA is using inside dynamic NAT on each security context.
C. The Cisco ASA is using a unique MAC address on each security context outside interface.
D. The Cisco ASA is using a unique dynamic routing protocol process on each security context.
E. The Cisco ASA packet classifier is configured to use the outside physical interface to assign the packets to each security context.

Answer: C

QUESTION NO: 5

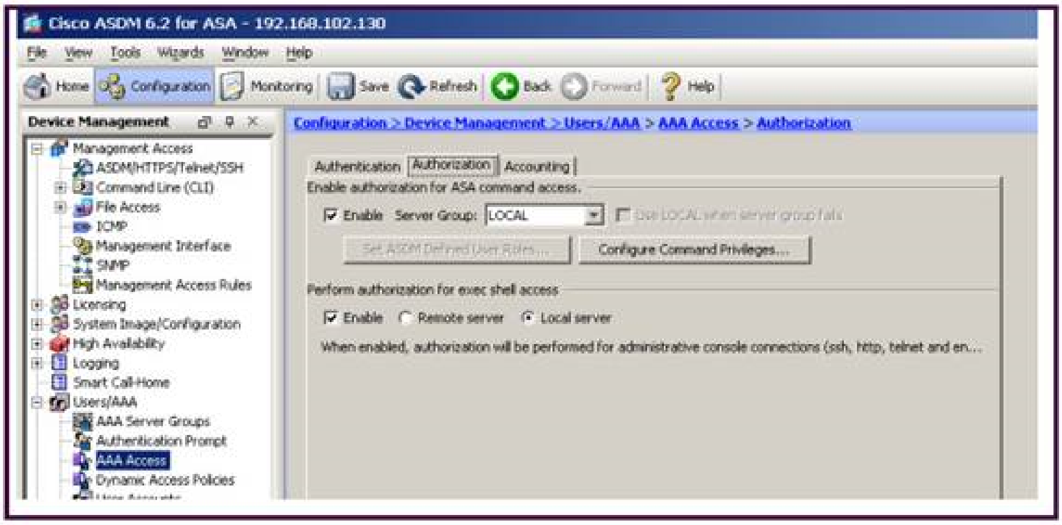
Which four types of ACL object group are supported on the Cisco ASA (release 8.2)? (Choose four.)

A. protocol
B. network
C. port

D. service
E. icmp-type
F. host

Answer: A,B,D,E

QUESTION NO: 6



Enable authorization for ASA command access.

☑ Enable Server Group: LOCAL ☐ Use LOCAL when server group fails

Perform authorization for exec shell access

☑ Enable ○ Remote server ● Local server

When enabled, authorization will be performed for administrative console connections (ssh, http, telnet and en...

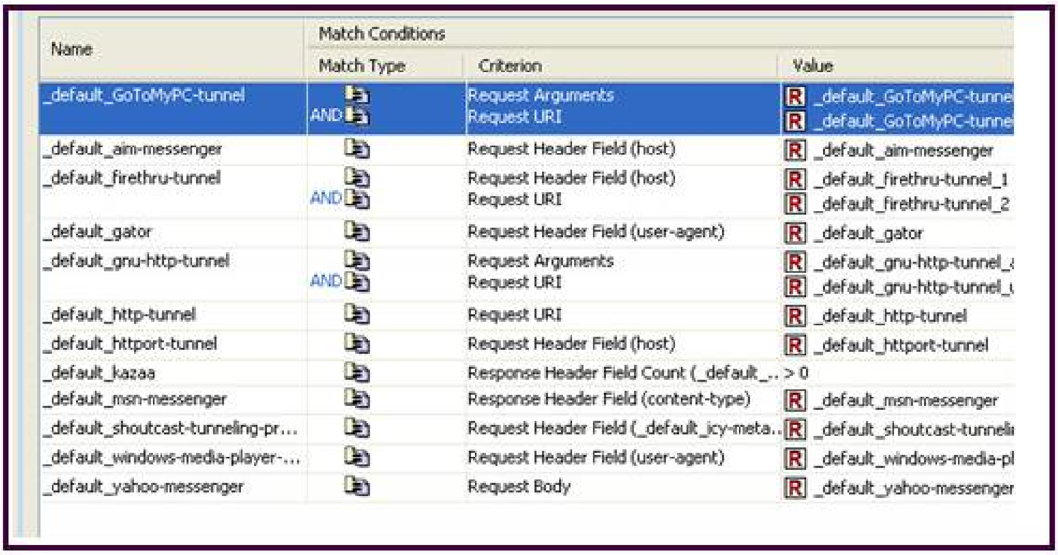
Refer to the exhibit. Which two CLI commands will result? (Choose two.)

A. aaa authorization network LOCAL
B. aaa authorization network default authentication-server LOCAL
C. aaa authorization command LOCAL
D. aaa authorization exec LOCAL
E. aaa authorization exec authentication-server LOCAL
F. aaa authorization exec authentication-server

Answer: C,D

QUESTION NO: 7

Refer to the exhibit.



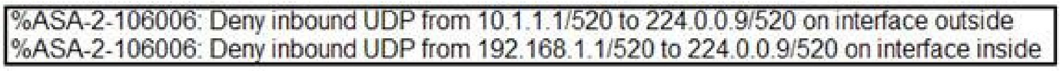
Name	Match Conditions		
	Match Type	Criterion	Value
_default_GoToMyPC-tunnel	 AND	Request Arguments Request URI	R _default_GoToMyPC-tunne R _default_GoToMyPC-tunne
_default_aim-messenger		Request Header Field (host)	R _default_aim-messenger
_default_firethru-tunnel	 AND	Request Header Field (host) Request URI	R _default_firethru-tunnel_1 R _default_firethru-tunnel_2
_default_gator		Request Header Field (user-agent)	R _default_gator
_default_gnu-http-tunnel	 AND	Request Arguments Request URI	R _default_gnu-http-tunnel_ R _default_gnu-http-tunnel_
_default_http-tunnel		Request URI	R _default_http-tunnel
_default_httport-tunnel		Request Header Field (host)	R _default_httport-tunnel
_default_kazaa		Response Header Field Count (_default_...	> 0
_default_msn-messenger		Response Header Field (content-type)	R _default_msn-messenger
_default_shoutcast-tunneling-pr...		Request Header Field (_default_icy-meta...	R _default_shoutcast-tunneli
_default_windows-media-player-...		Request Header Field (user-agent)	R _default_windows-media-pl
_default_yahoo-messenger		Request Body	R _default_yahoo-messenger

Which two statements about the class maps are true? (Choose two.)

A. These class maps are referenced within the global policy by default for HTTP inspection.
B. These class maps are all type inspect http class maps.
C. These class maps classify traffic using regular expressions.
D. These class maps are Layer 3/4 class maps.
E. These class maps are used within the inspection_default class map for matching the default inspection traffic.

Answer: B,E

QUESTION NO: 8



```
%ASA-2-106006: Deny inbound UDP from 10.1.1.1/520 to 224.0.0.9/520 on interface outside
%ASA-2-106006: Deny inbound UDP from 192.168.1.1/520 to 224.0.0.9/520 on interface inside
```

Refer to the exhibit. A Cisco ASA in transparent firewall mode generates the log messages seen in the exhibit. What should be configured on the Cisco ASA to allow the denied traffic?

A. extended ACL on the outside and inside interface to permit the multicast traffic
B. EtherType ACL on the outside and inside interface to permit the multicast traffic
C. stateful packet inspection
D. static ARP mapping
E. static MAC address mapping

Answer: A

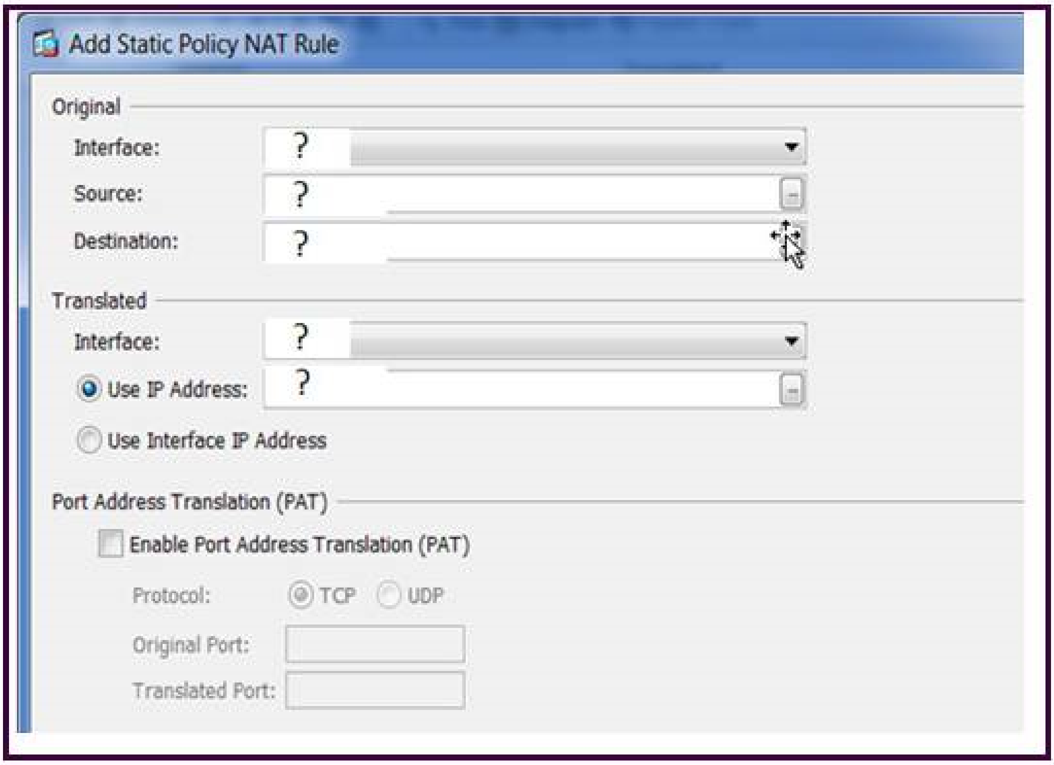
QUESTION NO: 9

The Cisco ASA must support dynamic routing and terminating VPN traffic. Which three Cisco ASA options will not support these requirements? (Choose three.)

A. transparent mode
B. multiple context mode
C. active/standby failover mode
D. active/active failover mode
E. routed mode
F. no NAT-control

Answer: A,B,D

QUESTION NO: 10



Refer to the exhibits. Which five options should be entered into the five fields in the Cisco ASDM Add Static Policy NAT Rule screen? (Choose five.)

access-list **POLICY_NAT_ACL** extended **permit ip host 172.16.0.10 10.0.1.0 255.255.255.0**
static (dmz,outside) 192.168.2.10 access-list **POLICY_NAT_ACL**

A. dmz = Original Interface
B. outside = Original Interface
C. 172.16.0.10 = Original Source

D. 192.168.2.10 = Original Source
E. 10.0.1.0/24 = Original Destination
F. 192.168.2.10 = Original Destination
G. dmz = Translated Interface
H. outside = Translated Interface
I. 192.168.2.10 = Translated Use IP Address
J. 172.16.0.10 = Translated Use IP Address

Answer: A,C,E,H,I

QUESTION NO: 11

By default, which access rule is applied inbound to the inside interface?

A. All IP traffic is denied.
B. All IP traffic is permitted.
C. All IP traffic sourced from any source to any less secure network destinations is permitted.
D. All IP traffic sourced from any source to any more secure network destinations is permitted

Answer: C

QUESTION NO: 12

In which type of environment is the Cisco ASA MPF set connection advanced-options tcp-state-bypass 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

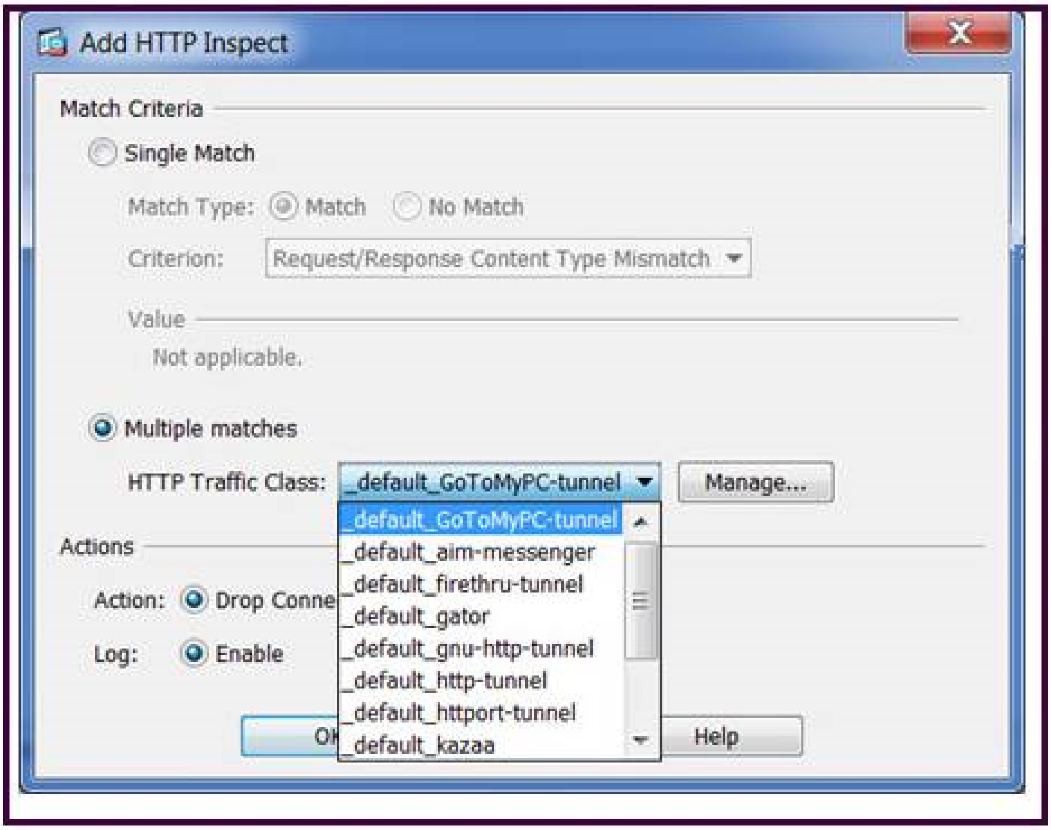
QUESTION NO: 13

Which Cisco ASA platform should be selected if the requirements are to support 35,000 connections per second, 600,000 maximum connections, and traffic shaping?

A. 5540
B. 5550
C. 5580-20
D. 5580-40

Answer: B

QUESTION NO: 14



Add HTTP Inspect

Match Criteria

○ Single Match

Match Type: ● Match ○ No Match

Criterion: Request/Response Content Type Mismatch

Value

Not applicable.

● Multiple matches

HTTP Traffic Class: _default_GoToMyPC-tunnel

Actions

Action: ● Drop Conne

Log: ● Enable

Refer to the exhibit. What is the resulting CLI command?

A. match request uri regex _default_GoToMyPC-tunnel
drop-connection log
B. match regex _default_GoToMyPC-tunnel
drop-connection log
C. class _default_GoToMyPC-tunnel
drop-connection log
D. match class-map _default_GoToMyPC-tunnel
drop-connection log

Answer: C

QUESTION NO: 15

A customer is ordering a number of Cisco ASAs for their network. For the remote or home office, they are purchasing the Cisco ASA 5505. When ordering the licenses for their Cisco ASAs, which two licenses must they order that are "platform specific" to the Cisco ASA 5505? (Choose two.)

A. AnyConnect Essentials license
B. per-user Premium SSL VPN license
C. VPN shared license
D. internal user licenses
E. Security Plus license

Answer: D,E

QUESTION NO: 16

With Cisco ASA active/standby failover, what is needed to enable subsecond failover?

A. Use redundant interfaces.
B. Enable the stateful failover interface between the primary and secondary Cisco ASA.
C. Decrease the default unitfailover polltime to 300 msec and the unitfailover holdtime to 900 msec
D. Decrease the default number of monitored interfaces to 1.

Answer: C

QUESTION NO: 17

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 NO: 18

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

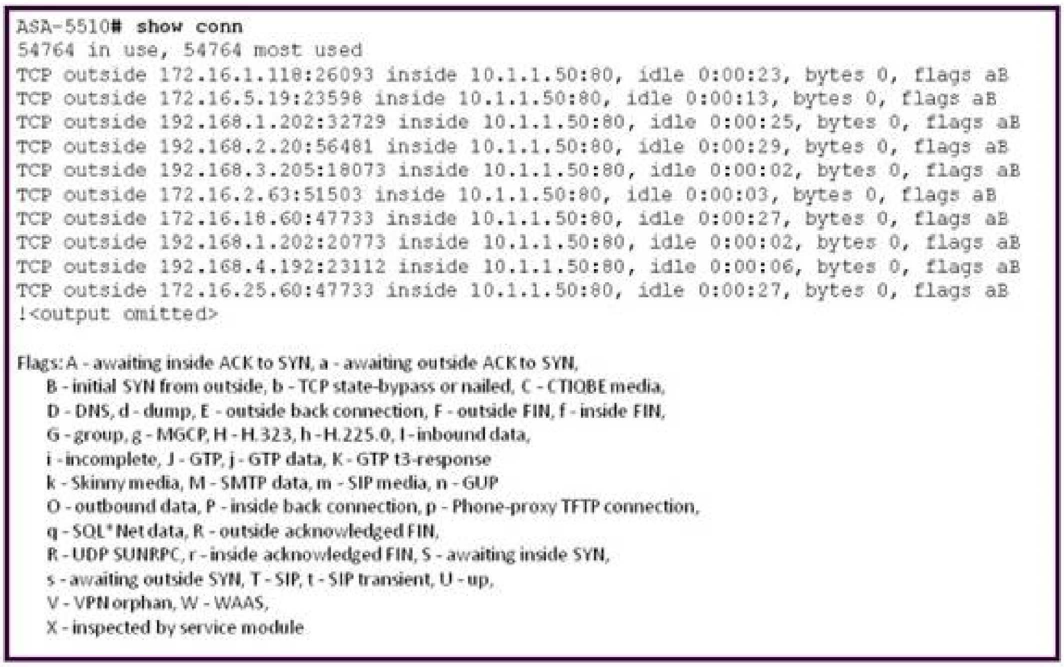
QUESTION NO: 19

A Cisco ASA requires an additional feature license to enable which feature?

A. transparent firewall
B. cut-thru proxy
C. threat detection
D. botnet traffic filtering
E. TCP normalizer

Answer: D

QUESTION NO: 20



```
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
```

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