642-618 Q&As

Deploying Cisco ASA Firewall Solutions (FIREWALL v2.0)

Pass Cisco 642-618 Exam with 100% Guarantee

QUESTION 1

Which three actions can be applied to a traffic class within a type inspect policy map? (Choose three.)

A. drop

B. priority

C. log

D. pass

E. inspect

F. reset

Correct Answer: ACF

http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/mpc.html hostname(config-pmap-c)# {[drop [send-protocol-error] | drop-connection [send-protocol-error]| mask | reset] [log] | rate-limit message_rate}

The drop keyword drops all packets that match.

The send-protocol-error keyword sends a protocol error message. The drop-connection keyword drops the packet and closes the connection. The mask keyword masks out the matching portion of the packet. The reset keyword drops the

packet, closes the connection, and sends a TCP reset to the server and/or client.

The log keyword, which you can use alone or with one of the other keywords, sends a system log message.

The rate-limit message_rate argument limits the rate of messages.

QUESTION 2

Which statement about the Cisco ASA botnet traffic filter is true?

A. The four threat levels are low, moderate, high, and very high.

B. By default, the dynamic-filter drop blacklist interface outside command drops traffic with a threat level of high or very high.

C. Static blacklist entries always have a very high threat level.

D. A static or dynamic blacklist entry always takes precedence over the static whitelist entry.

Correct Answer: C

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

Information About the Static Database You can manually enter domain names or IP addresses (host or subnet) that you want to tag as bad names in a blacklist. Static blacklist entries are always designated with a Very High threat level. You can also enter names or IP addresses in a whitelist, so that names or addresses that appear on both the dynamic blacklist and the whitelist are identified only as whitelist addresses in syslog messages and reports. Note that you see syslog messages for whitelisted addresses even if the address is not also in the dynamic blacklist.

QUESTION 3

On the Cisco ASA Software Version 8.4.1, which three parameters can be configured using the set connection command within a policy map? (Choose three.)

A. per-client TCP and/or UDP idle timeout

B. per-client TCP and/or UDP maximum session time

C. TCP sequence number randomization

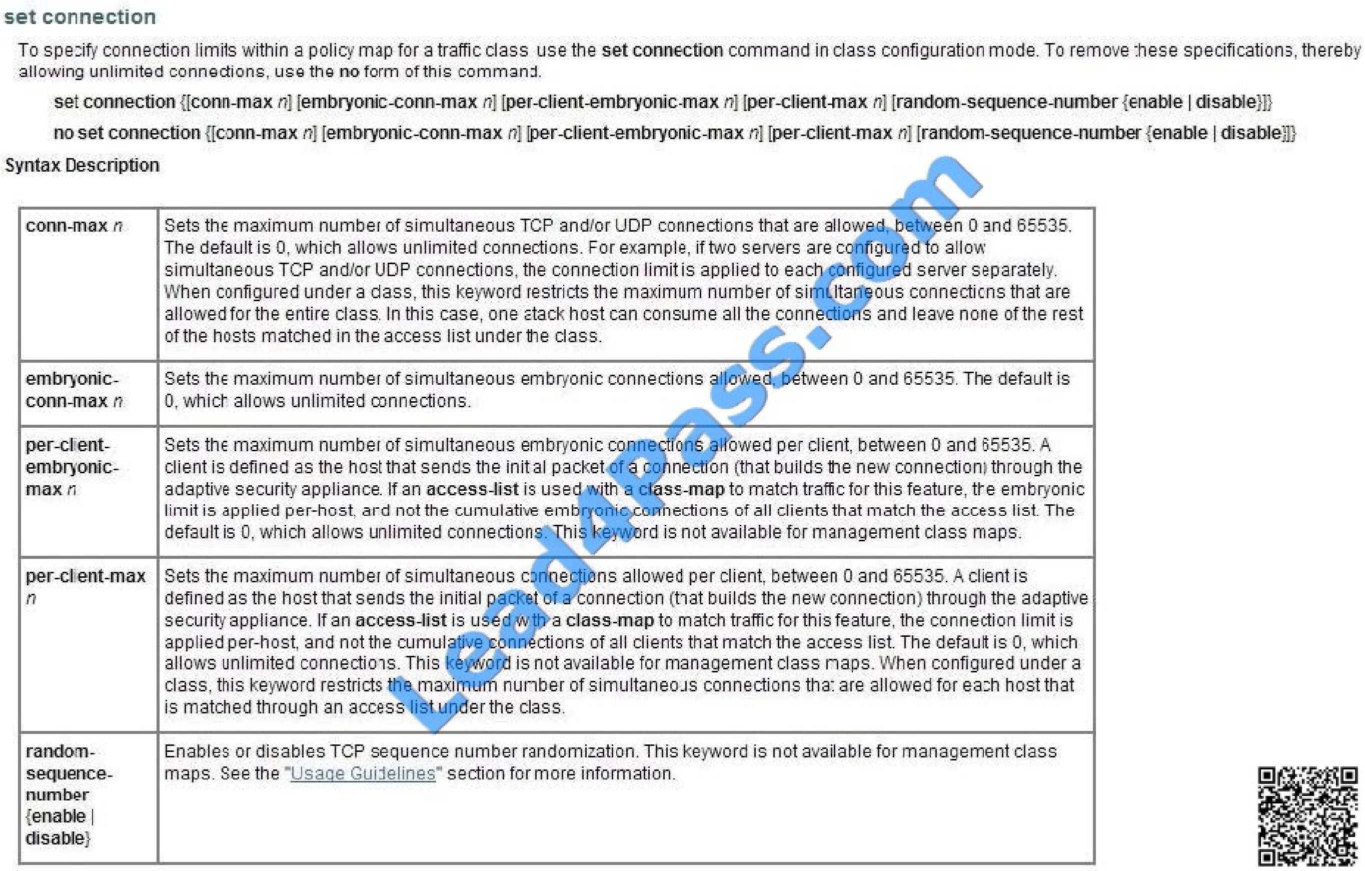
D. maximum number of simultaneous embryonic connections

E. maximum number of simultaneous TCP and/or UDP connections

F. fragments reassembly options

Correct Answer: CDE

http://www.cisco.com/en/US/docs/security/asa/asa82/command/reference/s1.html#wp1424045



set connection

To specify connection limits within a policy map for a traffic class use the **set connection** command in class configuration mode. To remove these specifications, thereby allowing unlimited connections, use the **no** form of this command.

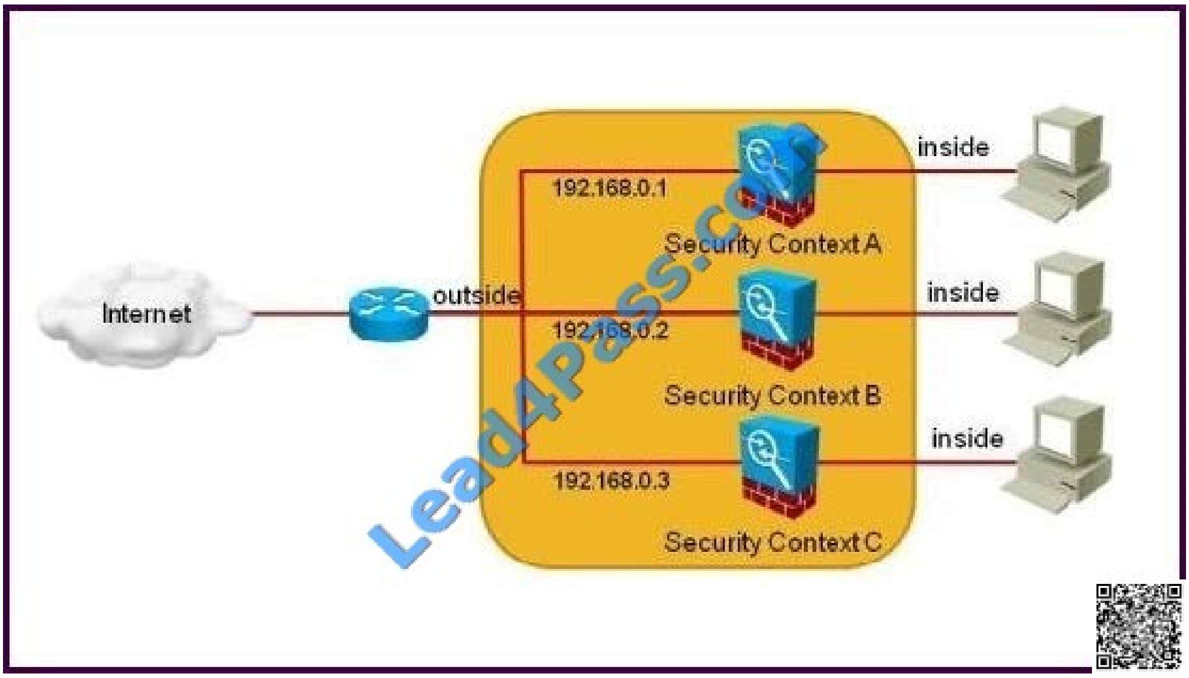
```
set connection {[conn-max n] [embryonic-conn-max n] [per-client-embryonic-max n] [per-client-max n] [random-sequence-number {enable | disable}]}
no set connection {[conn-max n] [embryonic-conn-max n] [per-client-embryonic-max n] [per-client-max n] [random-sequence-number {enable | disable]}
```

Syntax Description

conn-max *n*	Sets the maximum number of simultaneous TCP and/or UDP connections that are allowed, between 0 and 65535. The default is 0, which allows unlimited connections. For example, if two servers are configured to allow simultaneous TCP and/or UDP connections, the connection limit is applied to each configured server separately. When configured under a class, this keyword restricts the maximum number of simultaneous connections that are allowed for the entire class. In this case, one attack host can consume all the connections and leave none of the rest of the hosts matched in the access list under the class.
embryonic-conn-max *n*	Sets the maximum number of simultaneous embryonic connections allowed, between 0 and 65535. The default is 0, which allows unlimited connections.
per-client-embryonic-max *n*	Sets the maximum number of simultaneous embryonic connections allowed per client, between 0 and 65535. A client is defined as the host that sends the initial packet of a connection (that builds the new connection) through the adaptive security appliance. If an **access-list** is used with a **class-map** to match traffic for this feature, the embryonic limit is applied per-host, and not the cumulative embryonic connections of all clients that match the access list. The default is 0, which allows unlimited connections. This keyword is not available for management class maps.
per-client-max *n*	Sets the maximum number of simultaneous connections allowed per client, between 0 and 65535. A client is defined as the host that sends the initial packet of a connection (that builds the new connection) through the adaptive security appliance. If an **access-list** is used with a **class-map** to match traffic for this feature, the connection limit is applied per-host, and not the cumulative connections of all clients that match the access list. The default is 0, which allows unlimited connections. This keyword is not available for management class maps. When configured under a class, this keyword restricts the maximum number of simultaneous connections that are allowed for each host that is matched through an access list under the class.
random-sequence-number {**enable** | **disable**}	Enables or disables TCP sequence number randomization. This keyword is not available for management class maps. See the "Usage Guidelines" section for more information.

QUESTION 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.

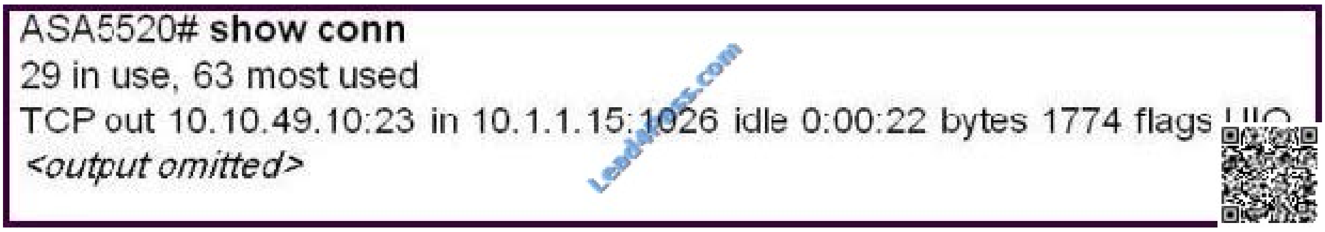
E. The Cisco ASA packet classifier is configured to use the outside physical interface to assign the packets to each security context.

Correct Answer: C

http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/mode_contexts.html# wp1134937

QUESTION 5

Which flag not 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)?



```
ASA5520# show conn
29 in use, 63 most used
TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22 bytes 1774 flags UIO
<output omitted>
```

A. B

B. D

C. b

D. A

E. a

F. i

G. I

H. O

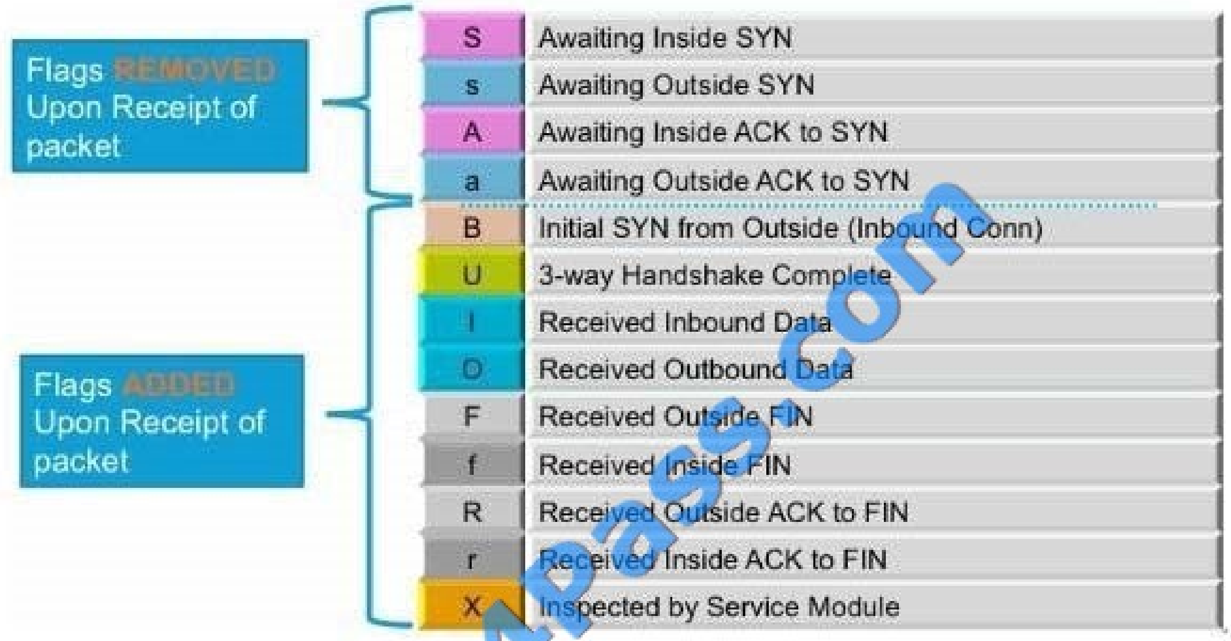
Correct Answer: A

http://www.cisco.com/en/US/products/ps6120/products_tech_note09186a0080bcad00.shtml

Originally answer from dump was A meaning B or initial SYN from outside but B is not shown in the output.

The question used to read ".. 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)?

TCP Connection Flag Values

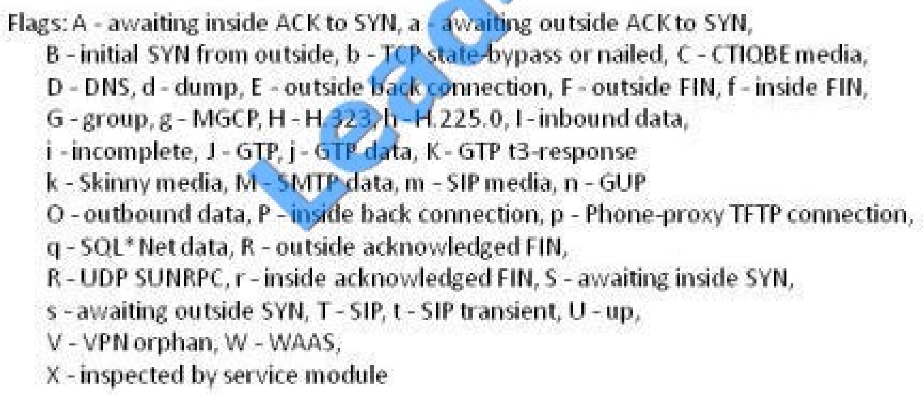


Flags REMOVED Upon Receipt of packet

S	Awaiting Inside SYN
s	Awaiting Outside SYN
A	Awaiting Inside ACK to SYN
a	Awaiting Outside ACK to SYN

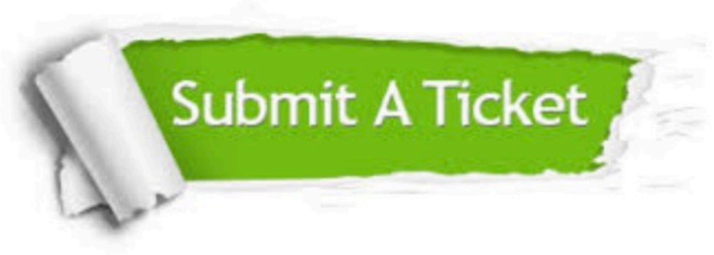
Flags ADDED Upon Receipt of packet

B	Initial SYN from Outside (Inbound Conn)
U	3-way Handshake Complete
I	Received Inbound Data
O	Received Outbound Data
F	Received Outside FIN
f	Received Inside FIN
R	Received Outside ACK to FIN
r	Received Inside ACK to FIN
X	Inspected by Service Module



```
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
```

Latest 642-618 Dumps   642-618 Exam Questions   642-618 Braindumps


Submit A Ticket

100%