642-618 Q&As

Deploying Cisco ASA Firewall Solutions (FIREWALL v2.0)

Pass Cisco 642-618 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4lead.com/642-618.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Which Cisco ASDM 6.4.1 pane is used to enable the Cisco ASA appliance to perform TCP checksum verifications?

A. Configuration > Firewall > Service Policy Rules

B. Configuration > Firewall > Advanced > IP Audit > IP Audit Policy

C. Configuration > Firewall > Advanced > IP Audit > IP Audit Signatures

D. Configuration > Firewall > Advanced > TCP options

E. Configuration > Firewall > Objects > TCP Maps

F. Configuration > Firewall > Objects > Inspect Maps

Correct Answer: E

http://www.cisco.com/en/US/docs/security/asa/asa72/asdm52/release/notes/rn524.html shows:

Firewall Features	
TCP Normalization Enhancements	You can now configure TCP normalization actions for certain packet types. Previously, the default actions for these kinds of packets was to drop the packet. Now you can set the TCP normalizer to allow the packets. • TCP invalid ACK check (the **invalid-ack** command) • TCP packet sequence past window check (the **seq-past-window** command) • TCP SYN-ACK with data check (the **synack-data** command) You can also set the TCP out-of-order packet buffer timeout (the **queue** command **timeout** keyword). Previously, the timeout was 4 seconds. You can now set the timeout to another value. The default action for packets that exceed MSS has changed from drop to allow (the **exceed-mss** command). The following non-configurable actions have changed from drop to clear for these packet types: • Bad option length in TCP • TCP Window scale on non-SYN • Bad TCP window scale value • Bad TCP SACK ALLOW option In ASDM, see the Configuration > Global Objects > TCP Maps pane. *Also available in Version 8.0(4).*

http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/user/guide/protect.html

shows

a.

In the TCP Map Name field, enter a name.

b.

In the Queue Limit field, enter the maximum number of out-of-order packets, between 0 and 250.

c.

In the Reserved Bits area, click Clear and allow, Allow only, or Drop. Allow only allows packets with the reserved bits in the TCP header. Clear and allow clears the reserved bits in the TCP header and allows the packet. Drop drops the packet with the reserved bits in the TCP header.

d.

Check any of the following options:

-Clear Urgent Flag--Allows or clears the URG pointer through the security appliance. -Drop Connection on Window Variation--Drops a connection that has changed its window size unexpectedly.

-Drop Packets that Exceed Maximum Segment Size--Allows or drops packets that exceed MSS set by peer.

-Check if transmitted data is the same as original--Enables and disables the retransmit data checks.

-Drop SYN Packets With Data--Allows or drops SYN packets with data. -Enable TTL Evasion Protection--Enables or disables the TTL evasion protection offered by the security appliance.

-Verify TCP Checksum--Enables and disables checksum verification. e. To set TCP options, check any of the following options:

-Clear Selective Ack--Lists whether the selective-ack TCP option is allowed or cleared.

-Clear TCP Timestamp--Lists whether the TCP timestamp option is allowed or cleared. -Clear Window Scale--Lists whether the window scale timestamp option is allowed or cleared.

-Range--Lists the valid TCP options ranges, which should fall within 6-7 and 9-255. The lower bound should be less than or equal to the upper bound.

f. Click OK.

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 which type of encrypted traffic can a Cisco ASA appliance running software version 8.4.1 perform application inspection and control?

A. IPsec

B. SSL

C. IPsec or SSL

D. Cisco Unified Communications

E. Secure FTP

Correct Answer: D

http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns165/ns391/guide__c07- 494658.html

QUESTION 4

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

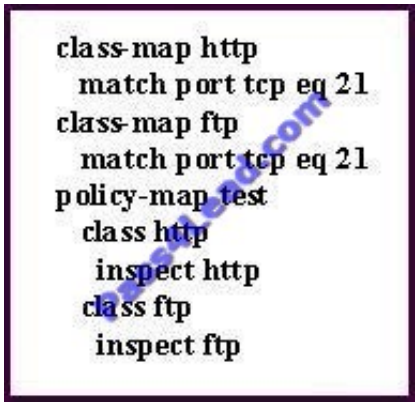
E. Security Plus license

Correct Answer: DE

Cisco ASA Model	ASA 5505 / Security Plus
	
Maximum Firewall Throughput[1]	150 Mbps
Maximum Firewall Throughput (Multi-Protocol)	-
Maximum Concurrent Threat Mitigation Throughput (Firewall + IPS Services)	75 Mbps with AIP SSC-5
Maximum Firewall Connections	10,000 /25,000
Maximum Firewall Connections/Second	4,000
Packets per second (64 byte)	85,000
Maximum 3DES/AES VPN Throughput[2]	100 Mbps
Maximum Site-to-Site and IPsec IKEv1 Client VPN User Sessions	10/25
Maximum AnyConnect or Clientless VPN User Sessions	25
Bundled SSL VPN User Sessions	2
Security Contexts (Included, Maximum)	Not available
VLANs	3 (trunking disabled) /20

QUESTION 5

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.

Correct Answer: B

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.pass4lead.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: