**VCE & PDF**

**Pass4itSure.com**

# 642-618<sup>Q&As</sup>

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.pass4itsure.com/642-618.html**

## 100% Passing Guarantee
## 100% Money Back Assurance

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

**Instant Download** After Purchase

**100% Money Back** Guarantee

**365 Days** Free Update

**800,000+** Satisfied Customers

**QUESTION 1**

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 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**

By default, not all services in the default inspection class are inspected. Which Cisco ASA CLI command do you use to determine which inspect actions are applied to the default inspection class?

A. show policy-map global_policy

B. show policy-map inspection_default

C. show class-map inspection_default

D. show class-map default-inspection-traffic

E. show service-policy global

Correct Answer: E

http://www.cisco.com/en/US/docs/security/asa/asa81/command/ref/s7.html#wp1254424

**show service-policy**

To display the service policy statistics, use the **show service-policy** command in privileged EXEC mode.

show service-policy [global | interface *intf*] [csc | inspect | ips | police | priority | shape]

show service-policy [global | interface *intf*] [set connection [details]]

show service-policy [global | interface *intf*] [flow *protocol* {host *src_host* | *src_ip src_mask*} [eq *src_port*] {host *dest_host* | *dest_ip dest_mask*} [eq *dest_

**Syntax Description**

| csc | (Optional) Limits the output to policies that include the **csc** command. |
|---|---|
| *dest_ip dest_mask* | The destination IP address and netmask of the traffic flow. |
| details | (Optional) Displays per-client connection information, if a per-client connection limit is enabled. |
| eq *dest_port* | (Optional) The equals operator, requiring the destination port to match the port number that follows. |
| eq *src_port* | (Optional) The equals operator, requiring the source port to match the port number that follows. |
| flow *protocol* | (Optional) Specifies a traffic flow for which you want to see the policies that the security appliance would apply to the flow. The arg flow keyword specify the flow in ip-5-tuple format. Valid values for the *protocol* argument are listed in the "Usage Guidelines" secti |
| global | (Optional) Limits output to the global policy, which applies to all interfaces. |
| host *dest_host* | The host destination IP address of the traffic flow. |
| host *src_host* | The host source IP address of the traffic flow. |
| *icmp_control_message* | (Optional) Specifies an ICMP control message of the traffic flow. Valid values for the *icmp_control_message* argument are listed i below. |
| *icmp_number* | (Optional) Specifies the ICMP protocol number of the traffic flow. |
| inspect | (Optional) Limits the output to policies that include an **inspect** command. |
| interface *intf* | (Optional) Displays policies applied to the interface specified by the *intf* argument, where *intf* is the interface name given by the na |
| ips | Limits output to policies that include the **ips** command. |
| police | Limits output to policies that include the **police** command. |

**QUESTION 4**

Which Cisco ASA configuration is used to configure the TCP intercept feature?

A. a TCP map

B. an access list

C. the established command

D. the set connection command with the embryonic-conn-max option

E. a type inspect policy map

Correct Answer: D

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/conns_connlimits.html #wp1080734

**QUESTION 5**

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

Correct Answer: C

http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/access_rules.html#wp 1083496

Implicit Permits

For routed mode, the following types of traffic are allowed through by default:

-IPv4 traffic from a higher security interface to a lower security interface.

-IPv6 traffic from a higher security interface to a lower security interface. Note These defaults might not be true if you have configured a global access rule. For transparent mode, the following types of traffic are allowed through by default:

-IPv4 traffic from a higher security interface to a lower security interface. -IPv6 traffic from a higher security interface to a lower security interface.

-ARPs in both directions

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.pass4itsure.com/allproducts

## Need Help

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





Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © pass4itsure, All Rights Reserved.