



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.geekcert.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 Cisco ASA Software Version 8.4.1 and later, when you configure the Cisco ASA appliance in transparent firewall mode, which configuration is mandatory?

- A. NAT
- B. static routes
- C. ARP inspections
- D. EtherType access-list
- E. bridge group(s)
- F. dynamic MAC address learning

Correct Answer: E



Command History

Release	Modification
7.0(1)	For routed mode, this command was changed from a global configuration command to an interface configuration mode command.
8.4(1)	For transparent mode, bridge groups were introduced. You now set the IP address for the BVI, and not globally.

Usage Guidelines

In single context routed firewall mode, each interface address must be on a unique subnet. In multiple context mode if this interface is on a shared interface, then each IP address must be unique but on the same subnet. If the interface is unique, this IP address can be used by other contexts if desired.

A transparent firewall does not participate in IP routing. The only IP configuration required for the ASA is to set the BVI address. This address is required because the ASA uses this address as the source address for traffic originating on the ASA, such as system messages or communications with AAA servers. You can also use this address for remote management access. This address must be on the same subnet as the upstream and downstream routers. For multiple context mode, set the management IP address within each context. For models that include a Management interface, you can also set an IP address for this interface for management purposes.

The standby IP address must be on the same subnet as the main IP address.

Examples

The following example sets the IP addresses and standby addresses of two interfaces:

```
hostname(config)# interface gigabitethernet0/2
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/3
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0 standby 10.1.2.2
hostname(config-if)# no shutdown
```



QUESTION 2

Refer to the exhibit.



Name	Match Conditions		
	Match Type	Criterion	Value
_default_GoToMyPC-tunnel	AND	Request Arguments Request URI	R _default_GoToMyPC-tunnel R _default_GoToMyPC-tunnel
_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_httpport-tunnel		Request Header Field (host)	R _default_httpport-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-mess

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.

Correct Answer: BC

QUESTION 3

Which statement about SNMP support on the Cisco ASA appliance is true?

- A. The Cisco ASA appliance supports only SNMPv1 or SNMPv2c.
- B. The Cisco ASA appliance supports read-only and read-write access.
- C. The Cisco ASA appliance supports three built-in SNMPv3 groups in Cisco ASDM: Authentication and Encryption, Authentication Only, and No Authentication, No Encryption.
- D. The Cisco ASA appliance can send SNMP traps to the network management station only using SNMPv2.

Correct Answer: C

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/monitor_snmp.html#w.p1042029

SNMP Version 3 Overview

SNMP Version 3 provides security enhancements that are not available in SNMP Version 1 or SNMP Version 2c. SNMP



Versions 1 and 2c transmit data between the SNMP server and SNMP agent in clear text. SNMP Version 3 adds authentication and privacy options to secure protocol operations. In addition, this version controls access to the SNMP agent and MIB objects through the User-based Security Model (USM) and Viewbased Access Control Model (VACM). The

ASA 5500 series ASAs also support the creation of SNMP groups and users, as well as hosts, which is required to enable transport authentication and encryption for secure SNMP communications.

Security Models

For configuration purposes, the authentication and privacy options are grouped together into security models.

Security models apply to users and groups, and are divided into the following three types:

- NoAuthPriv--No Authentication and No Privacy, which means that no security is applied to messages.
- AuthNoPriv--Authentication but No Privacy, which means that messages are authenticated.
- AuthPriv--Authentication and Privacy, which means that messages are authenticated and encrypted.

QUESTION 4

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 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

Correct Answer: B

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

[Latest 642-618 Dumps](#)

[642-618 PDF Dumps](#)

[642-618 VCE Dumps](#)



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.geekcert.com/allproducts>

Need Help

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



 One Year Free Update <p>Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 Money Back Guarantee <p>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 Security & Privacy <p>We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

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