



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.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**

Which two Cisco ASA licensing features are correct with Cisco ASA Software Version 8.3 and later? (Choose two.)

- A. Identical licenses are not required on the primary and secondary Cisco ASA appliance.
- B. Cisco ASA appliances configured as failover pairs disregard the time-based activation keys.
- C. Time-based licenses are stackable in duration but not in capacity.
- D. A time-based license completely overrides the permanent license, ignoring all permanently licensed features until the time-based license is uninstalled.

Correct Answer: AC

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_bulletin_c_25-593781.html

Time-based license stacking: Customers can extend time-based licenses such as Botnet Traffic Filter and SSL VPN Burst by applying multiple licenses. Licensing of high-availability pairs: For several features, the requirement to deploy identical licenses on the standby unit in a high-availability pair has been removed.

Security Plus licenses must still be purchased for both the Active and Standby units.

QUESTION 2

When a Cisco ASA is configured in multiple context mode, within which configuration are the interfaces allocated to the security contexts?

- A. each security context
- B. system configuration
- C. admin context (context with the "admin" role)
- D. context startup configuration file (.cfg file)

Correct Answer: B

<http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/>

[products_configuration_example09186a00808d2b63.shtml](http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a00808d2b63.shtml)

In order to specify the interfaces that you can use in the context, enter the command appropriate for a physical interface or for one or more subinterfaces.

In order to allocate a physical interface, enter this command:

```
hostname(config-ctx)# allocate-interface [mapped_name] [visible | invisible]
```

Context Configurations

The security appliance includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a standalone device. You can store context configurations on the internal Flash



memory or the external Flash memory card, or you can download them from a TFTP, FTP, or HTTP(S) server.

System Configuration

The system administrator adds and manages contexts by configuring each context configuration location, allocated interfaces, and other context operating parameters in the system configuration, which, like a single mode configuration, is the

startup configuration. The system configuration identifies basic settings for the security appliance. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access

network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the admin context. The system configuration does include a specialized failover interface for failover traffic only.

Admin Context Configuration

The admin context is just like any other context, except that when a user logs in to the admin context, then that user has system administrator rights and can access the system and all other contexts. The admin context is not restricted in any

way, and can be used as a regular context. However, because logging into the admin context grants you administrator privileges over all contexts, you might need to restrict access to the admin context to appropriate users. The admin context

must reside on Flash memory, and not remotely.

If your system is already in multiple context mode, or if you convert from single mode, the admin context is created automatically as a file on the internal Flash memory called admin.cfg. This context is named "admin." If you do not want to use

admin.cfg as the admin context, you can change the admin context.

QUESTION 3

On Cisco ASA Software Version 8.4.1 and later, when you configure the Cisco ASA appliance in transparent firewall mode, how is the Cisco ASA management IP address configured?

- A. using the IP address global configuration command
- B. using the IP address GigabitEthernet 0/x interface configuration command
- C. using the IP address BVI x interface configuration command
- D. using the bridge-group global configuration command
- E. using the bridge-group GigabitEthernet 0/x interface configuration command
- F. using the bridge-group BVI x interface configuration command

Correct Answer: C

<http://www.cisco.com/en/US/docs/security/asa/asa84/command/reference/i3.html#wp1898863>



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
```

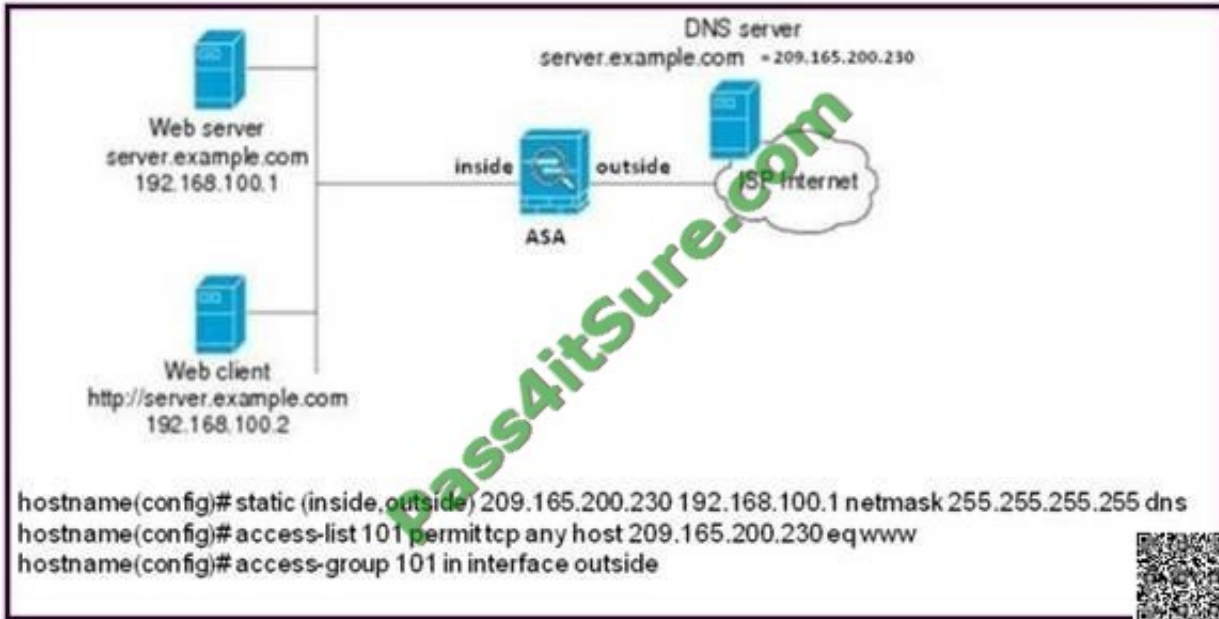
The following example sets the management address and standby address of bridge group 1:

```
hostname(config)# interface bvi 1
hostname(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```



QUESTION 4

Refer to the exhibit.



Which two options will result from the Cisco ASA configuration? (Choose two.)

- A. The outside hosts can use the 192.168.100.1 IP address to reach the web server on the inside network.
- B. The global IP address of the web server is 209.165.200.230.
- C. The inside web client will use the 209.165.200.230 IP address to reach the web server and the Cisco ASA will translate the 209.165.200.230 IP address to the 192.168.100.1 IP address.
- D. The Cisco ASA will translate the DNS A-Record reply from the DNS server to any inside client for the web server (web server IP = 192.168.100.1).
- E. The web server will be reachable only from the inside.
- F. The web server will be reachable only from the outside.

Correct Answer: BD

http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/inspect_basic.html#wp1350877

When DNS inspection is enabled, DNS rewrite provides full support for NAT of DNS messages originating from any interface.

If a client on an inside network requests DNS resolution of an inside address from a DNS server on an outside interface, the DNS A-record is translated correctly.

If the DNS inspection engine is disabled, the A-record is not translated.

As long as DNS inspection remains enabled, you can configure DNS rewrite using the alias, static, or nat commands.

DNS Rewrite performs two functions:

-Translating a public address (the routable or "mapped" address) in a DNS reply to a private address (the "real" address) when the DNS client is on a private interface.

-Translating a private address to a public address when the DNS client is on the public interface.



QUESTION 5

In the default global policy, which traffic is matched for inspections by default?

- A. match any
- B. match default-inspection-traffic
- C. match access-list
- D. match port
- E. match class-default

Correct Answer: B

<http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/inspect.html#wp13836> Default Inspection Policy

By default, the configuration includes a policy that matches all default application inspection traffic and applies inspection to the traffic on all interfaces (a global policy). Default application inspection traffic includes traffic to the default ports for each protocol. You can only apply one global policy, so if you want to alter the global policy, for example, to apply inspection to non- standard ports, or to add inspections that are not enabled by default, you need to either edit the default policy or disable it and apply a new one.

[642-618 PDF Dumps](#)

[642-618 Study Guide](#)

[642-618 Exam Questions](#)



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:



 <p>One Year Free Update 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>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy 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 © pass4itsure, All Rights Reserved.