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.passapply.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

When troubleshooting redundant interface operations on the Cisco ASA, which configuration should be verified?

A. The name if configuration on the member physical interfaces are identical.

B. The MAC address configuration on the member physical interfaces are identical.

C. The active interface is sending periodic hellos to the standby interface.

D. The IP address configuration on the logical redundant interface is correct.

E. The duplex and speed configuration on the logical redundant interface are correct.

Correct Answer: D

Concept A logical redundant interface is a pair of an active and a standby physical interface. When the active interface fails, the standby interface becomes active. From firewall perspective this event is completely transparent and can be viewed as a single logical interface. We can use redundant interfaces to increase the security appliance reliability. This feature is separate from device-level failover, but you can configure redundant interfaces as well as failover if desired. We can configure upto 8 redundant interfaces.

Redundant interface are number from 1 to 8 and have the name redundant X. When adding physical interfaces to the redundant pair, please make sure there is no configuration on it and interface is also in no shutdown state. This is just a precaution, the firewall will remove these settings when adding the physical interface to a new group. The logical redundant interface will take the MAC address of the first interface added to the group.

This MAC address is not changed with the member interface failures, but changes when you swap the order of the physical interfaces to the pair.

Once we have configured a redundant interface, we can assign it a name and a security level, followed by an IP address. The procedure is the same as with any interface in the system.

Configuration --> interface GigabitEthernet0/0 no nameif no security-level no ip address ! interface GigabitEthernet0/1 no nameif no security-level no ip address interface Redundant1 member-interface GigabitEthernet0/0 member-interface GigabitEthernet0/1 nameif outside security-level 0 ip address 1.1.1.1 255.255.255.0

Verify You can use the following command to verify---> ciscoasa(config)# show interface redundant 1 Interface Redundant1 "outside", is up, line protocol is up Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps) MAC address 5475.d0d4.9594, MTU 1500 IP address 1.1.1.1, subnet mask 255.255.255.0 27 packets input, 12330 bytes, 0 no buffer Received 27 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 27 overrun, 0 ignored, 0 abort 10 L2 decode drops 1 packets output, 64 bytes, 0 underruns 0 output errors, 0 collisions, 0 interface resets 0 late collisions, 0 deferred 0 input reset drops, 0 output reset drops input queue (curr/max packets): hardware (5/25) software (0/0) output queue (curr/max packets): hardware (0/1) software (0/0)

Traffic Statistics for "outside": 17 packets input, 7478 bytes 1 packets output, 28 bytes 17 packets dropped 1 minute input rate 0 pkts/sec, 92 bytes/sec 1 minute output rate 0 pkts/sec, 0 bytes/sec 1 minute drop rate, 0 pkts/sec

5 minute input rate 0 pkts/sec, 0 bytes/sec

5 minute output rate 0 pkts/sec, 0 bytes/sec

5 minute drop rate, 0 pkts/sec

Redundancy Information:

Member GigabitEthernet0/0(Active), GigabitEthernet0/1 Last switchover at 23:13:03 UTC Dec 15 2011

QUESTION 2

Which option can cause the interactive setup script not to work on a Cisco ASA 5520 appliance running software version 8.4.1?

A. The clock has not been set on the Cisco ASA appliance using the clock set command.

B. The HTTP server has not been enabled using the http server enable command.

C. The domain name has not been configured using the domain-name command.

D. The inside interface IP address has not been configured using the ip address command.

E. The management 0/0 interface has not been configured as management-only and assigned a name using the nameif command.

Correct Answer: E

http://www.checkthenetwork.com/networksecurityCiscoASA1.asp shows need for nameif and http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/intparam.html shows manaagement only The ASA 5510 and higher adaptive security appliance also includes the following type: -management The management interface is a Fast Ethernet interface designed for management traffic only, and is specified as management0/0. You can, however, use it for through traffic if desired (see the management-only command). In

transparent firewall mode, you can use the management interface in addition to the two interfaces allowed for through traffic. You can also add subinterfaces to the management interface to provide management in each security context for multiple context mode.

Append the subinterface ID to the physical interface ID separated by a period (.). In multiple context mode, enter the mapped name if one was assigned using the allocate- interface command.

For example, enter the following command:

hostname(config)# interface gigabitethernet0/1.1

Step 2 To name the interface, enter the following command: hostname(config-if)# nameif name

The name is a text string up to 48 characters, and is not case-sensitive. You can change the name by reentering this command with a new value. Do not enter the no form, because that command causes all commands that refer to that name

to be deleted.

Step 3 To set the security level, enter the following command:

hostname(config-if)# security-level number Where number is an integer between 0 (lowest) and 100 (highest).

Step 4 (Optional) To set an interface to management-only mode, enter the following command:

hostname(config-if)# management-only The ASA 5510 and higher adaptive security appliance includes a dedicated management interface called Management 0/0, which is meant to support traffic to the security appliance. However, you can

configure any interface to be a management- only interface using the management-only command. Also, for Management 0/0, you can disable management-only mode so the interface can pass through traffic just like any other interface.

QUESTION 3

Which two statements about Cisco ASA failover troubleshooting are true? (Choose two.)

A. With active/active failover, failover link troubleshooting should be done in the system execution space.

B. With active/active failover, ASR groups must be enabled.

C. With active/active failover, user data passing interfaces troubleshooting should be done within the context execution space.

D. The failed interface threshold is set to 1. Using the show monitor-interface command, if one of the monitored interfaces on both the primary and secondary Cisco ASA appliances is in the unknown state, a failover should occur.

E. Syslog level 1 messages will be generated on the standby unit only if the logging standby command is used.

Correct Answer: AC

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.

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.

QUESTION 4

Refer to the exhibit.

```
      Context Name      Class      Interfaces              URL
       admin            default    GigabitEthernet0/0,     disk0:/admin.cfg
                                   GigabitEthernet0/1
      *CTX              default    GigabitEthernet0/0,     disk0:/CTX.cfg
                                   GigabitEthernet0/2

Total active Security Contexts: 2
```

What does the * next to the CTX security context indicate?

A. The CTX context is the active context on the Cisco ASA.

B. The CTX context is the standby context on the Cisco ASA.

C. The CTX context contains the system configurations.

D. The CTX context has the admin role.

Correct Answer: D

http://www.cisco.com/en/US/docs/security/asa/asa70/configuration/guide/mngcntxt.html#wp110 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.

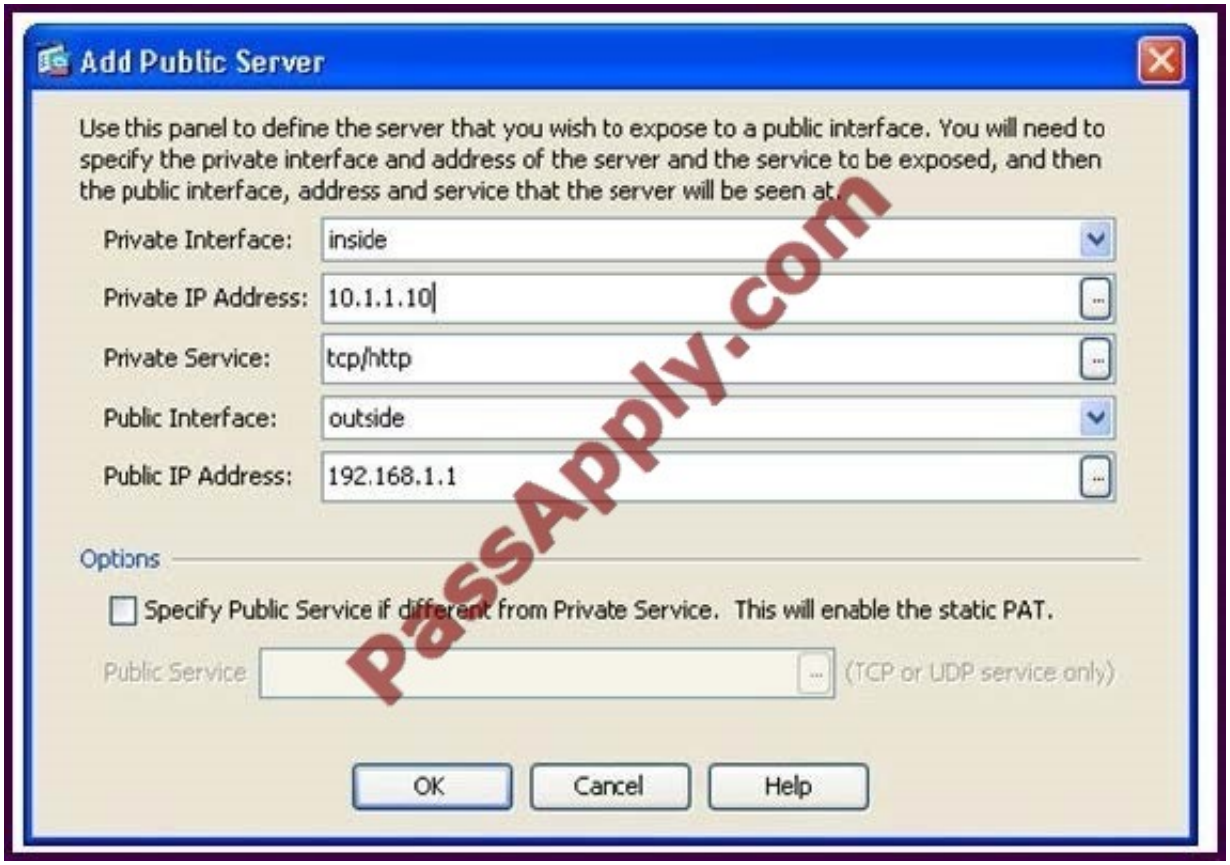
Admin Context Configuration The admin context is just like any other context, except that when a user logs in to the admin context, then that user has system administrator rights and can access the system and all other contexts. The admin context is not restricted in any way, and can be used as a regular 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 5

Refer to the exhibit.



On Cisco ASA Software Version 8.3 and later, which two sets of CLI configuration commands result from this Cisco ASDM configuration? (Choose two.)

A. nat (inside) 1 10.1.1.10 global (outside) 1 192.168.1.1

B. nat (outside) 1 192.168.1.1 global (inside 1 10.1.1.10

C. static(inside,outside) 192.168.1.1 10.1.1.10 netmask 255.255.255.255 tcp 0 0 udp 0

D. static(inside,outside) tcp 192.168.1.1 80 10.1.1.10 80

E. object network 192.168.1.1 nat (inside,outside) static 10.1.1.10

F. object network 10.1.1.10 nat (inside,outside) static 192.168.1.1

G. access-list outside_access_in line 1 extended permit tcp any object 10.1.1.10 eq http access-group outside_access_in in interface outside

H. access-list outside_access_in line 1 extended permit tcp any object 192.168.1.1 eq http access-group outside_access_in in interface outside

Correct Answer: FG