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

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

On Cisco ASA Software Version 8.4 and later, which two options show the maximum number of active and standby ports that an EtherChannel can have? (Choose two.)

A. 2 active ports

B. 4 active ports

C. 6 active ports

D. 8 active ports

E. 2 standby ports

F. 4 standby ports

G. 6 standby ports

H. 8 standby ports

Correct Answer: DH

http://www.cisco.com/en/US/docs/security/asa/asa84/asdm64/configuration_guide/interface_star t.pdf

Channel Group Interfaces

Each channel group can have eight active interfaces. Note that you can assign up to 16 interfaces to a channel group. While only eight interfaces can be active, the remaining interfaces can act as standby links in case of interface failure.

All interfaces in the channel group must be the same type and speed. The first interface added to the channel group determines the correct type and speed.

The EtherChannel aggregates the traffic across all the available active interfaces in the channel. The port is selected using a proprietary hash algorithm, based on source or destination MAC addresses, IP addresses, TCP and UDP port

numbers and vlan numbers

QUESTION 3

On Cisco ASA Software Version 8.3 and later, which two statements correctly describe the NAT table or NAT operations? (Choose two.)

A. The NAT table has four sections.

B. Manual NAT configurations are found in the first (top) and/or the last (bottom) section(s) of the NAT table.

C. Auto NAT also is referred to as Object NAT.

D. Auto NAT configurations are found only in the first (top) section of the NAT table.

E. The order of the NAT entries in the NAT table is not relevant to how the packets are matched against the NAT table.

F. Twice NAT is required for hosts on the inside to be accessible from the outside.

Correct Answer: BC

http://www.cisco.com/en/US/docs/security/asa/asa83/upgrading/migrating.html

Table 3 *New NAT Commands*

New Commands	Configuration Mode	Syntax
Network Object NAT (Typically used for regular NAT configurations.)		

nat dynamic	Object network	object network *name*
		   nat [(real_ifo,mapped_ifo)] dynamic
		    {[mapped_inline_host_ip] [interface] |
		    [mapped_obj] [pat-pool mapped_obj [round-robin]] [interface]} [dns]

nat static	Object network	object network *name*
		   nat [(real_ifo,mapped_ifo)] static
		    {mapped_inline_ip | mapped_obj | interface}
		    [dns | service {tcp | udp} real_port mapped_port]
		    [no-proxy-arp] [route-lookup]

Twice NAT (Typically used for policy NAT configurations.)		

nat source dynamic	Global	nat [(real_ifo,mapped_ifo)] [line | {after-object [line]}]
		   source dynamic {real_obj | any}
		   {[mapped_obj] [pat-pool mapped_obj [round-robin]] [interface]}
		   [destination static {mapped_obj | interface} {real_obj | any}]
		   [service {mapped_dest_svo_obj real_dest_svo_obj] [dns] [unidirectional]
		   [inactive] [description deso]

nat source static	Global	nat [(real_ifo,mapped_ifo)] [line | {after-object [line]}]
		   source static {real_obj | any} {mapped_obj | interface | any}}
		   [destination static {mapped_obj | interface} {real_obj | any}}
		   [service {real_sro_mapped_dest_svo_obj | any}
		   mapped_sro_real_dest_svo_obj] [dns] [unidirectional | [no-proxy-arp]
		   [route-lookup]] [inactive] [description deso]

QUESTION 4

Refer to the exhibit.

%ASA-2-106006: Deny inbound UDP from 10.1.1.1/520 to 224.0.0.9/520 on interface outs
%ASA-2-106006: Deny inbound UDP from 192.168.1.1/520 to 224.0.0.9/520 on interface

A Cisco ASA in transparent firewall mode generates the log messages seen in the exhibit. What should be configured on the Cisco ASA to allow the denied traffic?

A. extended ACL on the outside and inside interface to permit the multicast traffic

B. EtherType ACL on the outside and inside interface to permit the multicast traffic

C. stateful packet inspection

D. static ARP mapping

E. static MAC address mapping

Correct Answer: A

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/mpf.html#wp1101685

Allowing Broadcast and Multicast Traffic through the Transparent Firewall In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access list, including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay). Transparent firewall mode can allow any IP traffic through. This feature is especially useful in multiple context mode, which does not allow dynamic routing, for example.

QUESTION 5

For which purpose is the Cisco ASA CLI command aaa authentication match used?

A. Enable authentication for SSH and Telnet connections to the Cisco ASA appliance.

B. Enable authentication for console connections to the Cisco ASA appliance.

C. Enable authentication for connections through the Cisco ASA appliance.

D. Enable authentication for IPsec VPN connections to the Cisco ASA appliance.

E. Enable authentication for SSL VPN connections to the Cisco ASA appliance.

F. Enable authentication for Cisco ASDM connections to the Cisco ASA appliance.

Correct Answer: C

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

Or

http://www.cisco.com/en/US/products/ps6120/products_tech_note09186a0080ba6110.shtml

To enable network access authentication, perform the following steps:

Step 1 Using the aaa-server command, identify your AAA servers. If you have already identified your AAA servers, continue to the next step.

Step 2 Using the access-list command, create an access list that identifies the source addresses and destination addresses of traffic you want to authenticate. The permit ACEs mark matching traffic for authentication, while deny entries

exclude matching traffic from authentication. Be sure to include the destination ports for either HTTP, HTTPS, Telnet, or FTP in the access list because the user must authenticate with one of these services before other services are allowed

through the ASA.

Step 3 To configure authentication, enter the following command:

hostname(config)# aaa authentication match acl_name interface_name server_group

Where acl_name is the name of the access list you created; interface_name is the name of the interface as specified with the nameif command, and server_group is the AAA server group you created.

The following commands authenticate Telnet traffic from the outside interface to a particular server (209.165.201.5):

hostname(config)# aaa-server AuthInbound protocol tacacs+ hostname(config-aaa-server-group)# exit

hostname(config)# aaa-server AuthInbound (inside) host 10.1.1.1 hostname(config-aaa-server-host)# key TACPlusUauthKey hostname(config-aaa-server-host)#exit

hostname(config)# access-list TELNET_AUTH extended permit tcp any host 209.165.201.5 eq telnet

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: