642-618 Q&As

Deploying Cisco ASA Firewall Solutions (FIREWALL v2.0)

Pass Cisco 642-618 Exam with 100% Guarantee

QUESTION 1

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.

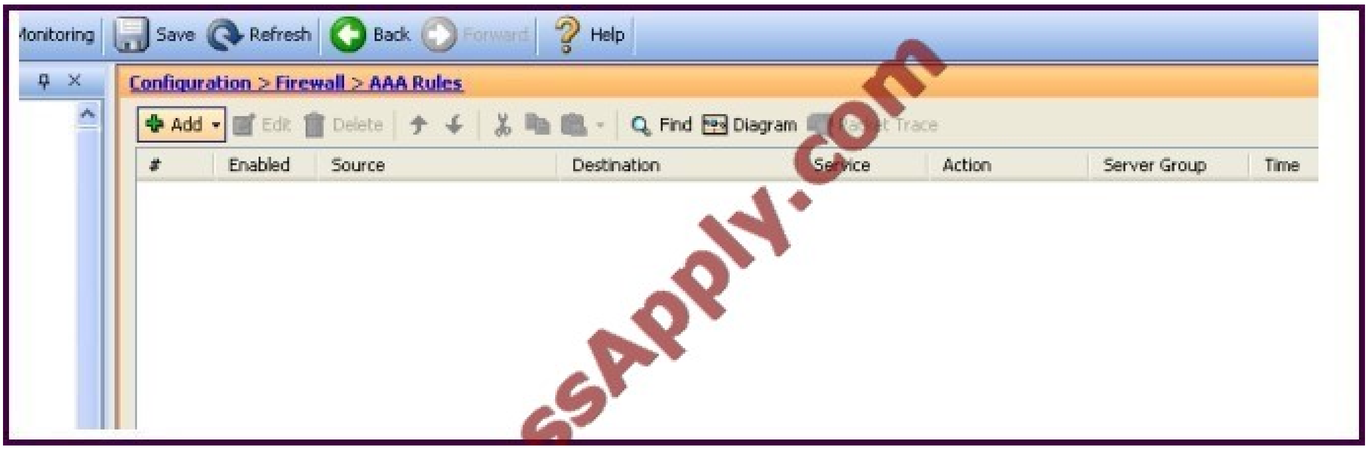
-IPv6 traffic from a higher security interface to a lower security interface. Note These defaults might not be true if you have configured a global access rule. For transparent mode, the following types of traffic are allowed through by default:

-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

QUESTION 2

Refer to the exhibit.



Which Cisco ASA feature can be configured using this Cisco ASDM screen?

A. Cisco ASA command authorization using TACACS+

B. AAA accounting to track serial, ssh, and telnet connections to the Cisco ASA

C. Exec Shell access authorization using AAA

D. cut-thru proxy

E. AAA authentication policy for Cisco ASDM access

Correct Answer: D

http://www.cisco.com/en/US/docs/security/asa/asa72/asdm52/user/guide/aaarules.html

And from http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/access_idfw.html#wp1 324095
Configuring Cut-through Proxy Authentication

In an enterprise, some users log onto the network by using other authentication mechanisms, such as authenticating with a web portal (cut-through proxy) or by using a VPN. For example, users with a Machintosh and Linux client might log in a web portal (cut-through proxy) or by using a VPN. Therefore, you must configure the Identity Firewall to allow these types of authentication in connection with identity-based access policies. The ASA designates users logging in through a web portal (cut-through proxy) as belonging to the Active Directory domain with which they authenticated. The ASA designates users logging in through a VPN as belonging to the LOCAL domain unless the VPN is authenticated by LDAP with Active Directory, then the Identity Firewall can associate the users with their Active Directory domain. The ASA reports users logging in through VPN authentication or a web portal (cut-through proxy) to the AD Agent, which distributes the user information to all registered ASA devices.

Users can log in by using HTTP/HTTPS, FTP, Telnet, or SSH. When users log in with these authentication methods, the following guidelines apply:

-For HTTP/HTTPS traffic, an authentication window appears for unauthenticated users. -For Telnet and FTP traffic, users must log in through the cut-through proxy and again to Telnet and FTP server.

-A user can specify an Active Directory domain while providing login credentials (in the format domain \username). The ASA automatically selects the associated AAA server group for the specified domain.

-If a user specifies an Active Directory domain while providing login credentials (in the format domain \username), the ASA parses the domain and uses it to select an authentication server from the AAA servers configured for the Identity

Firewall. Only the username is passed to the AAA server.

-If the backslash (\) delimiter is not found in the log in credentials, the ASA does not parse a domain and authentication is conducted with the AAA server that corresponds to default domain configured for the Identity Firewall.

-If a default domain or a server group is not configured for that default domain, the ASA rejects the authentication.

-If the domain is not specified, the ASA selects the AAA server group for the default domain that is configured for the Identity Firewall.

QUESTION 3

In which type of environment is the Cisco ASA MPF set connection advanced-options tcp- statebypass option the most useful?

A. SIP proxy

B. WCCP

C. BGP peering through the Cisco ASA

D. asymmetric traffic flow

E. transparent firewall

Correct Answer: D

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

QUESTION 4

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 5

Which statement about the Cisco ASA 5505 configuration is true?

A. The IP address is configured under the physical interface (ethernet 0/0 to ethernet 0/7).

B. With the default factory configuration, the management interface (management 0/0) is configured with the 192.168.1.1/24 IP address.

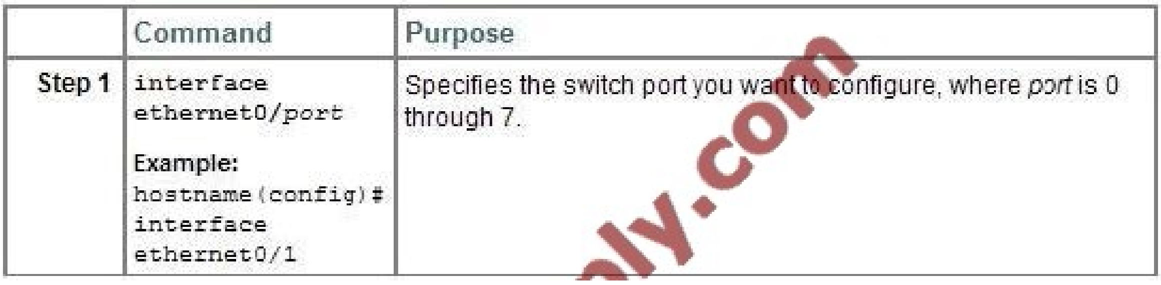
C. With the default factory configuration, Cisco ASDM access is not enabled.

D. The switchport access vlan command can be used to assign the VLAN to each physical interface (ethernet 0/0 to ethernet 0/7).

E. With the default factory configuration, both the inside and outside interface will use DHCP to acquire its IP address.

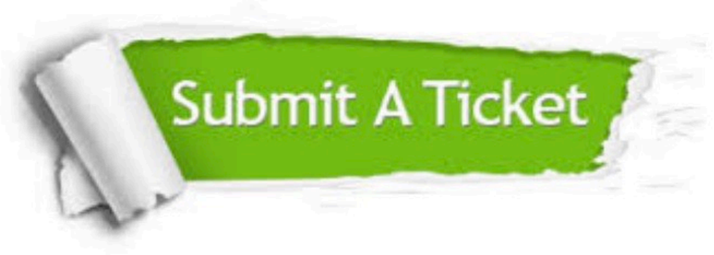
Correct Answer: D

http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/interface_start_5505.ht ml



	Command	Purpose

Step 1	`interface ethernet0/port`
	Example:
	`hostname(config)# interface ethernet0/1`
		Specifies the switch port you want to configure, where *port* is 0 through 7.


Submit A Ticket