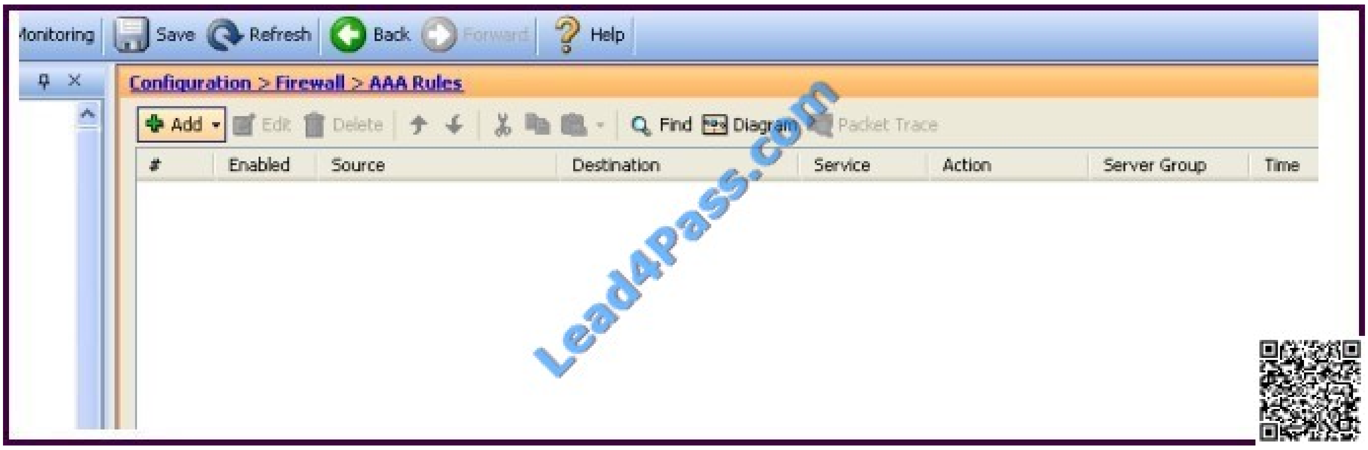
642-618 Q&As

Deploying Cisco ASA Firewall Solutions (FIREWALL v2.0)

Pass Cisco 642-618 Exam with 100% Guarantee

QUESTION 1

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 2

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

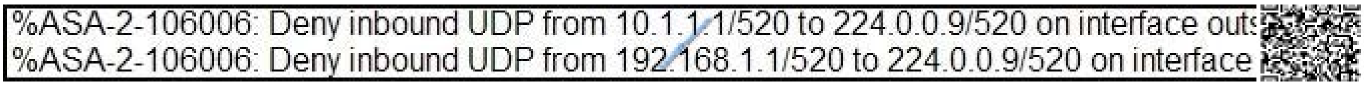
5 minute drop rate, 0 pkts/sec

Redundancy Information:

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

QUESTION 3

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 4

On the Cisco ASA Software Version 8.4.1, which three parameters can be configured using the set connection command within a policy map? (Choose three.)

A. per-client TCP and/or UDP idle timeout

B. per-client TCP and/or UDP maximum session time

C. TCP sequence number randomization

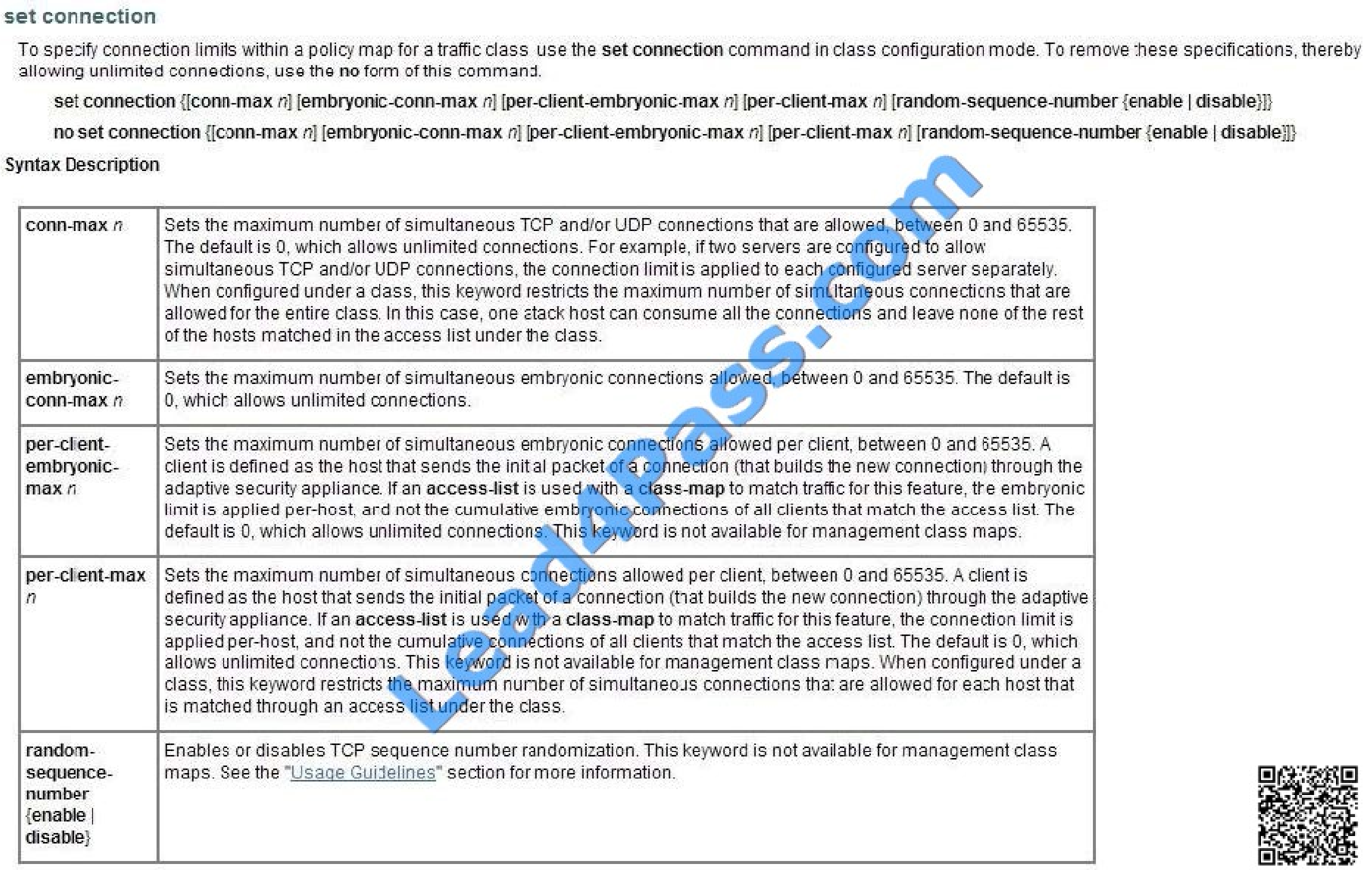
D. maximum number of simultaneous embryonic connections

E. maximum number of simultaneous TCP and/or UDP connections

F. fragments reassembly options

Correct Answer: CDE

http://www.cisco.com/en/US/docs/security/asa/asa82/command/reference/s1.html#wp1424045



set connection

To specify connection limits within a policy map for a traffic class use the **set connection** command in class configuration mode. To remove these specifications, thereby allowing unlimited connections, use the **no** form of this command.

set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

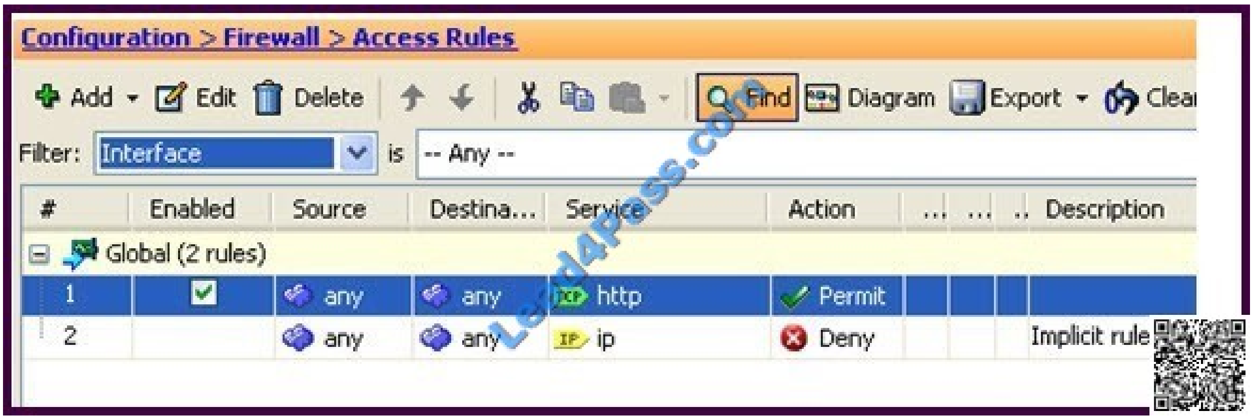
no set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

Syntax Description

conn-max *n*	Sets the maximum number of simultaneous TCP and/or UDP connections that are allowed, between 0 and 65535. The default is 0, which allows unlimited connections. For example, if two servers are configured to allow simultaneous TCP and/or UDP connections, the connection limit is applied to each configured server separately. When configured under a class, this keyword restricts the maximum number of simultaneous connections that are allowed for the entire class. In this case, one attack host can consume all the connections and leave none of the rest of the hosts matched in the access list under the class.
embryonic-conn-max *n*	Sets the maximum number of simultaneous embryonic connections allowed, between 0 and 65535. The default is 0, which allows unlimited connections.
per-client-embryonic-max *n*	Sets the maximum number of simultaneous embryonic connections allowed per client, between 0 and 65535. A client is defined as the host that sends the initial packet of a connection (that builds the new connection) through the adaptive security appliance. If an **access-list** is used with a **class-map** to match traffic for this feature, the embryonic limit is applied per-host, and not the cumulative embryonic connections of all clients that match the access list. The default is 0, which allows unlimited connections. This keyword is not available for management class maps.
per-client-max *n*	Sets the maximum number of simultaneous connections allowed per client, between 0 and 65535. A client is defined as the host that sends the initial packet of a connection (that builds the new connection) through the adaptive security appliance. If an **access-list** is used with a **class-map** to match traffic for this feature, the connection limit is applied per-host, and not the cumulative connections of all clients that match the access list. The default is 0, which allows unlimited connections. This keyword is not available for management class maps. When configured under a class, this keyword restricts the maximum number of simultaneous connections that are allowed for each host that is matched through an access list under the class.
random-sequence-number {**enable** | **disable**}	Enables or disables TCP sequence number randomization. This keyword is not available for management class maps. See the "Usage Guidelines" section for more information.

QUESTION 5

Refer to the exhibit.



Configuration > Firewall > Access Rules

Filter: Interface is -- Any --

#	Enabled	Source	Destina...	Service	Action	...	...	..	Description
Global (2 rules)									
1	☑	any	any	http	✓ Permit				
2		any	any	ip	Deny				Implicit rule

Which traffic is permitted on the inside interface without any interface ACLs configured?

A. any IP traffic input to the inside interface

B. any IP traffic input to the inside interface destined to any lower security level interfaces

C. only HTTP traffic input to the inside interface

D. only HTTP traffic output from the inside interface

E. No input traffic is permitted on the inside interface.

F. No output traffic is permitted on the inside interface.

Correct Answer: C

Latest 642-618 Dumps   642-618 Practice Test   642-618 Braindumps

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

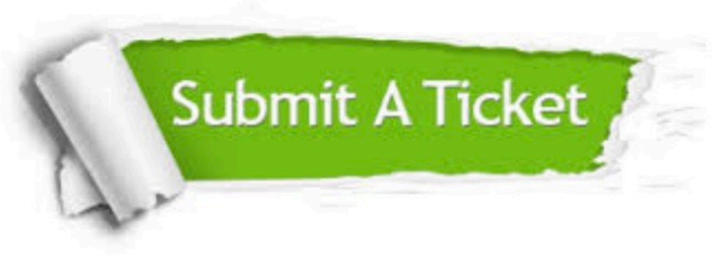
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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.lead4pass.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
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.

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.

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.

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.