Vendor: Cisco

Exam Code:642-618

Exam Name: Deploying Cisco ASA Firewall Solutions (FIREWALL v2.0)

Version: Demo

QUESTION 1

On the Cisco ASA Software Version 8.3 and later, which type of NAT configuration can be used to translate the source and destination IP addresses of the packet?

A. auto NAT

B. object NAT

C. one-to-one NAT

D. many-to-one NAT

E. manual NAT

F. identity NAT

Correct Answer: E

http://tunnelsup.com/2011/06/24/nat-for-cisco-asas-version-8-3/

Manual NAT or Twice NAT or Policy NAT or Reverse NAT

The limitation that Auto NAT has is that it cannot take the destination into consideration when conducting it\\'s NAT. This also of course results in it not being able to alter the destination address either. To accomplish either of these tasks you

must use "manual NAT". All of these terms are identical: Manual NAT, Twice NAT, Policy NAT, Reverse NAT. Don\\'t be confused by fancy mumbo jumbo.

http://www.cisco.com/en/US/docs/security/asa/asa83/asdm63/configuration_guide/nat_overview html#wpxref64594

Main Differences Between Network Object NAT and Twice NAT The main differences between these two NAT types are:

-How you define the real address.

Network object NAT--You define NAT as a parameter for a network object; the network object definition itself provides the real address. This method lets you easily add NAT to network objects. The objects can also be used in other parts of

your configuration, for example, for access rules or even in twice NAT rules. -Twice NAT--You identify a network object or network object group for both the real and mapped addresses. In this case, NAT is not a parameter of the network

object; the network object or group is a parameter of the NAT configuration. The ability to use a network object group for the real address means that twice NAT is more scalable.

-How source and destination NAT is implemented.

Network object NAT-- Each rule can apply to either the source or destination of a packet. So two rules might be used, one for the source IP address, and one for the destination IP address. These two rules cannot be tied together to enforce a

specific translation for a source/destination combination.

Twice NAT--A single rule translates both the source and destination. A matching packet only matches the one rule, and

further rules are not checked. Even if you do not configure the optional destination address for twice NAT, a matching

packet still only matches one twice NAT rule. The source and destination are tied together, so you can enforce different translations depending on the source/destination combination. For example, sourceA/destinationA can have a different

translation than sourceA/destinationB.

-Order of NAT Rules.

Network object NAT--Automatically ordered in the NAT table. Twice NAT--Manually ordered in the NAT table (before or after network object NAT rules).

QUESTION 2

A Cisco ASA appliance running software version 8.4.1 has an active botnet traffic filter license with 1 month left on the time-based license. Which option describes the result if a new botnet traffic filter with a 1 year time-based license is activated also?

A. The time-based license for the botnet traffic filter is valid only for another month.

B. The time-based license for the botnet traffic filter is valid for another 12 months.

C. The time-based license for the botnet traffic filter is valid for another 13 months.

D. The new 1 year time-based license for the botnet traffic filter cannot be activated until the current botnet traffic filter license expires in a month.

Correct Answer: C

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.

QUESTION 3

Refer to the exhibit.

Which statement about the Telnet session from 10.0.0.1 to 172.26.1.200 is true?

A. The Telnet session should be successful.

B. The Telnet session should fail because the route lookup to the destination fails.

C. The Telnet session should fail because the inside interface inbound access list will block it.

D. The Telnet session should fail because no matching flow was found.

E. The Telnet session should fail because inside NAT has not been configured.

Correct Answer: C

QUESTION 4

Where in the ACS are the individual downloadable ACL statements configured to achieve the most scalable deployment?

A. Group Setup

B. User Setup

C. Shared Profile Components

D. Network Access Profiles

E. Network Configuration

F. Interface Configuration

Correct Answer: C

The Shared Profile Components section enables you to develop and name reusable, shared sets of authorization components which may be applied to one or more users or groups of users and referenced by name within their profiles. These include network access restrictions (NARs), command authorization sets, and downloadable PIX ACLs.

The Shared Profile Components section of Cisco Secure ACS addresses the scalability of selective authorization. Shared profile components can be configured once and then applied to many users or groups.

Without this ability, flexible and comprehensive authorization could only be accomplished by explicitly configuring the authorization of each user group for each possible command on each possible device. Creating and applying these named shared profile components (access restrictions, command sets, and ACLs) makes it unnecessary to repeatedly enter long lists of devices or commands when defining network access parameters.

Shared profile components also enable Cisco Secure ACS to authorize a command on behalf of another device or devices. Their scalability extends to the following capabilities: A way to determine the list of commands a user could issue against one or more devices in the network.

A way to determine the list of devices on which a particular user may execute a particular command and http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_chapter09186a0 080205a4a.html

---

QUESTION 5

When enabling a Cisco ASA to send syslog messages to a syslog server, which syslog level will produce the most messages?

A. notifications

B. informational

C. alerts

D. emergencies

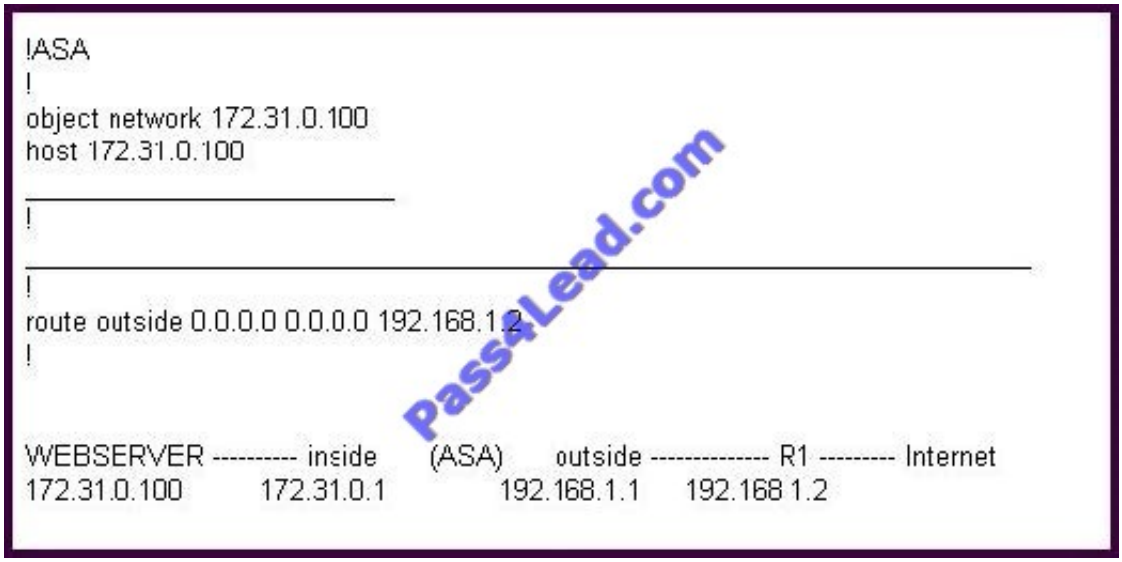
E. errors

F. debugging

Correct Answer: F

QUESTION 6

Refer to the partial Cisco ASA configuration and the network topology shown in the exhibit.



Which two Cisco ASA configuration commands are required so that any hosts on the Internet can HTTP to the WEBSERVER using the 192.168.1.100 IP address? (Choose two.)

A. nat (inside,outside) static 192.168.1.100

B. nat (inside,outside) static 172.31.0.100

C. nat (inside,outside) static interface

D. access-list outside_access_in extended permit tcp any object 172.31.0.100 eq http

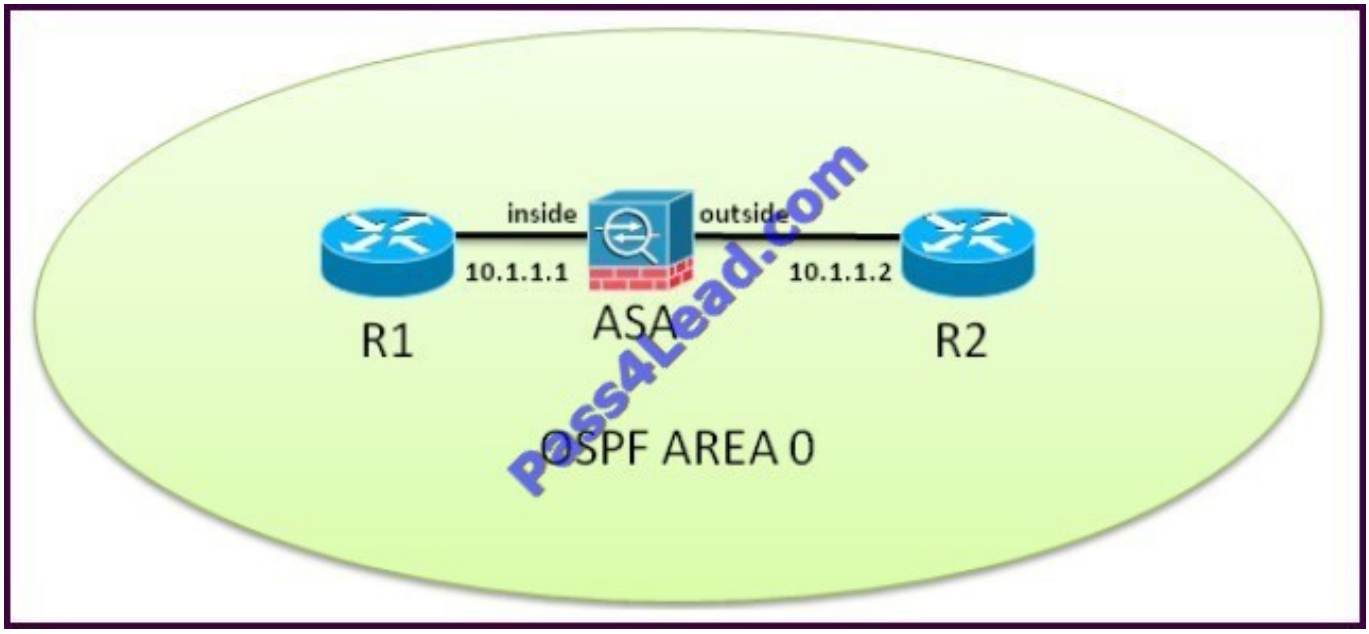
E. access-list outside_access_in extended permit tcp any object 192.168.1.100 eq http

F. access-list outside_access_in extended permit tcp any object 192.168.1.1 eq http

Correct Answer: AD

QUESTION 7

Refer to the exhibit.



The Cisco ASA is operating in transparent mode. What is required on the Cisco ASA so that R1 and R2 can form OSPF neighbor adjacency?

A. Map the R1 and R2 MAC address in the Cisco ASA MAC address table using the mac- address-table static if_name MAC_address command.

B. Configure OSPF stateful packet inspection using MPF.

C. Apply an EtherType ACL to the inside and outside interfaces to permit OSPF multicast traffic.

D. Apply an extended ACL to the inside and outside interfaces to permit OSPF multicast traffic.

E. Enable Advanced Application Inspection using MPF.

Correct Answer: D

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 8

When active/active failover is implemented on the Cisco ASA, how many failover groups are supported on the Cisco ASA?

A. 1

B. 2

C. 1 failover group per configured security context

D. 2 failover groups per configured security context

Correct Answer: B

http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00808340 58.shtml#act1

Active/Active Failover Overview Active/Active failover is only available to security appliances in multiple context mode. In an Active/Active failover configuration, both security appliances can pass network traffic. In Active/Active failover, you divide the security contexts on the security appliance into failover groups. A failover group is simply a logical group of one or more security contexts. You can create a maximum of two failover groups on the security appliance. The admin context is always a member of failover group 1. Any unassigned security contexts are also members of failover group 1 by default. The failover group forms the base unit for failover in Active/Active failover. Interface failure monitoring, failover, and active/standby status are all attributes of a failover group rather than the unit. When an active failover group fails, it changes to the standby state while the standby failover group becomes active. The interfaces in the failover group that becomes active assume the MAC and IP addresses of the interfaces in the failover group that failed. The interfaces in the failover group that is now in the standby state take over the standby MAC and IP addresses.

Note: A failover group failing on a unit does not mean that the unit has failed. The unit may still have another failover group passing traffic on it.

QUESTION 9

Which three configurations are needed to enable SNMPv3 support on the Cisco ASA? (Choose three.)

A. SNMPv3 Local EngineID

B. SNMPv3 Remote EngineID

C. SNMP Users

D. SNMP Groups

E. SNMP Community Strings

F. SNMP Hosts

Correct Answer: CDF

http://www.cisco.com/en/US/docs/security/asa/asa82/snmp/snmpv3_1.html The adaptive security appliance requires that you configure the SNMP server group, the SNMP server user associated with the group, and the SNMP server host, which specifies the user for receiving SNMP traps.

To configure SNMP Version 3 operations, the required sequence of commands is as follows:

Snmp-server

group

Snmp-server

user

Snmp-server

host

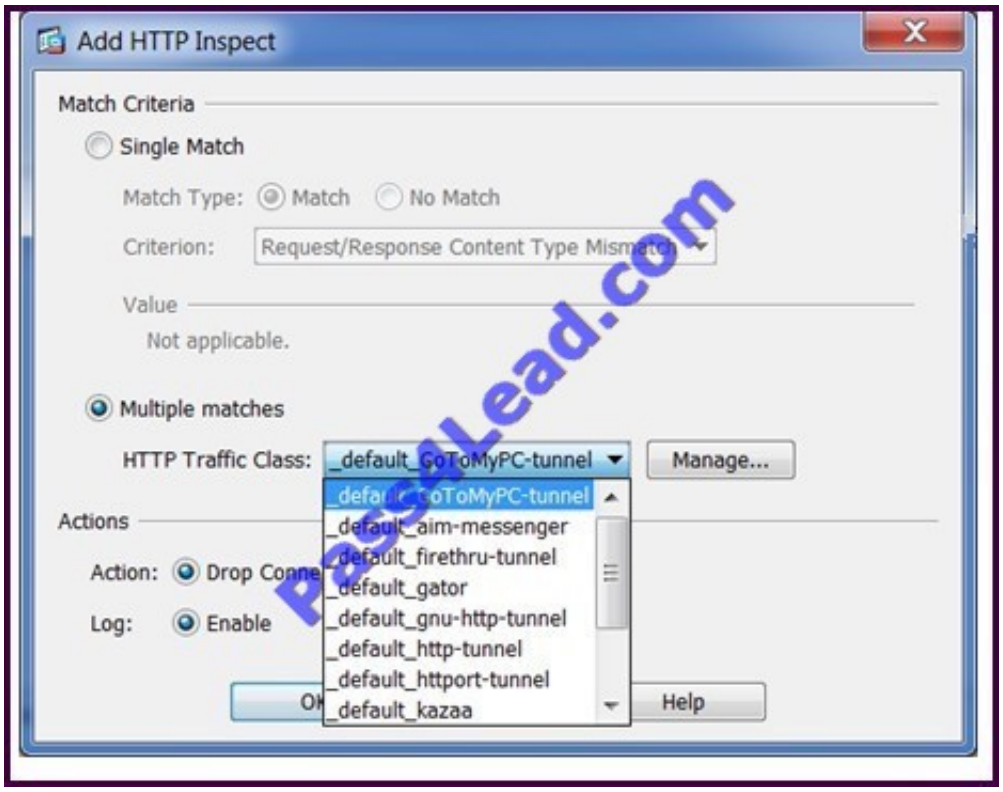
The following shows an example adaptive security appliance configuration:

hostname# snmp-server group authPriv v3 priv hostname# snmp-server group authNoPriv v3 auth hostname# snmp-server group noAuthNoPriv v3 noauth

---

QUESTION 10

Refer to the exhibit.



What is the resulting CLI command?

A. match request uri regex _default_GoToMyPC-tunnel drop-connection log

B. match regex _default_GoToMyPC-tunnel drop-connection log

C. class _default_GoToMyPC-tunnel drop-connection log

D. match class-map _default_GoToMyPC-tunnel drop-connection log

Correct Answer: C

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/inspect_basic.html Step 6 To apply actions to matching traffic, perform the following steps. a. Specify the traffic on which you want to perform actions using one of the following methods:

Specify the DNS class map that you created in Step 3 by entering the following command:

hostname(config-pmap)# class class_map_name

hostname(config-pmap-c)#

Specify traffic directly in the policy map using one of the match commands described in Step 3. If you use a match not command, then any traffic that does not match the criterion in the match not command has the action applied.

b. Specify the action you want to perform on the matching traffic by entering the following command:

hostname(config-pmap-c)# {[drop [send-protocol-error] | drop-connection [send-protocol-error]| mask | reset] [log] | rate-limit message_rate}

Not all options are available for each match or class command. See the CLI help or the Cisco ASA 5500 Series Command Reference for the exact options available.

The drop keyword drops all packets that match.

The send-protocol-error keyword sends a protocol error message. The drop-connection keyword drops the packet and closes the connection. The mask keyword masks out the matching portion of the packet. The reset keyword drops the

packet, closes the connection, and sends a TCP reset to the server and/or client.

The log keyword, which you can use alone or with one of the other keywords, sends a system log message

The rate-limit message_rate argument limits the rate of messages.

QUESTION 11

With Cisco ASA active/active or active/standby stateful failover, which state information or table is not passed between the active and standby Cisco ASA by default?

A. NAT translation table

B. TCP connection states

C. UDP connection states

D. ARP table

E. HTTP connection table

Correct Answer: E

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/ha_overview.html#wp 1078922

Stateful Failover

When Stateful Failover is enabled, the active unit continually passes per-connection state information to the standby unit. After a failover occurs, the same connection information is available at the new active unit. Supported end-user applications are not required to reconnect to keep the same communication session.

Table 32-2 list the state information that is and is not passed to the standby unit when Stateful Failover is enabled.

Table 32-2 State Information

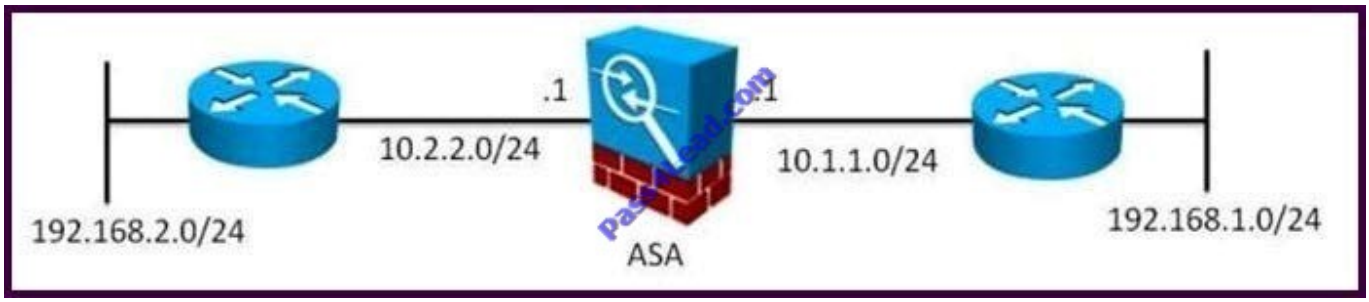
State Information Passed to Standby Unit	State Information Not Passed to Standby Unit
NAT translation table	The HTTP connection table (unless HTTP replication is enabled).
TCP connection states	The user authentication (uauth) table. Inspected protocols are subject to advanced TCP-state tracking, and the TCP state of these connections is not automatically replicated. While these connections are replicated to the standby unit, there is a best-effort attempt to re-establish a TCP state.
UDP connection states	The routing tables. After a failover occurs, some packets may be lost or routed out of the wrong interface (the default route) while the dynamic routing protocols rediscover routes.
The ARP table	State information for Security Service Modules.
The Layer 2 bridge table (when running in transparent firewall mode)	DHCP server address leases.
The HTTP connection states (if HTTP replication is enabled)	Stateful failover for phone proxy. When the active unit goes down, the call fails, media stops flowing, and the phone should unregister from the failed unit and reregister with the active unit. The call must be re-established.
The ISAKMP and IPSec SA table	—
GTP PDP connection database	—
SIP signalling sessions	—

The following WebVPN features are not supported with Stateful Failover:

- Smart Tunnels
- Port Forwarding
- Plugins
- Java Applets
- IPv6 clientless or Anyconnect sessions
- Citrix authentication (Citrix users must reauthenticate after failover)

QUESTION 12

Refer to the exhibit.



Which Cisco ASA configuration has the minimum number of the required configuration commands to enable the Cisco ASA appliance to establish EIGRP neighborship with its two neighboring routers?

A. router eigrp 1 network 10.0.0.0 255.0.0.0

B. router eigrp 1 network 10.0.0.0 255.0.0.0 network 192.168.1.0 255.255.255.0 network 192.168.2.0 255.255.255.0

C. router eigrp 1 network 10.1.1.0 255.255.255.0 network 10.2.2.0 255.255.255.0

D. router eigrp 1

network 10.1.1.0 255.255.255.0

network 10.2.2.0 255.255.255.0

network 192.168.1.0 255.255.255.0

network 192.168.2.0 255.255.255.0

E. router eigrp 1 network 0.0.0.0 255.255.255.255

Correct Answer: A

http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008086eb d2.shtml EIGRP Configuration - the CLI configuration is very similar to the !Cisco IOS router EIGRP configuration.

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

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: