# 642-522

## Securing Networks with PIX and ASA Exam(SNPA)

DEMO

**QUESTION NO: 1**

In the Cisco ASA 5500 series, what is the flash keyword aliased to?

A. Disk0
B. Disk1
C. Flash0
D. Flash1
E. both Disk0 and Disk1

**Answer: A**

**Explanation:**
See the following URL syntax:

disk0:/ [ path / ] filename
For the ASA 5500 series adaptive security appliance, this URL indicates the internal Flash memory. You can also use flash instead of disk0 ; they are aliased.
Reference:
http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_chapter09186a0080450b90.html

**QUESTION NO: 2**

Which of these statements regarding Active/Active failover configurations is correct

A. Configure failover interface parameters in the "admin" context.
B. Use the failover active command to enable Active/Active failover on the Cisco ASA Security Appliance.
C. Allocate interfaces to a failover group using the failover group sub-command mode.
D. Configure two failover groups: group 1 and group 2.

**Answer: A,D**

**Explanation:**
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 , and 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.

As in Active/Standby failover, one unit in an Active/Active failover pair is designated the primary unit, and the other unit the secondary unit. Unlike Active/Standby failover, this designation does not indicate which unit becomes active when both units start simultaneously. Instead, the primary/secondary designation determines which unit provides the running configuration to the pair and on which unit each failover group appears in the active state when both start simultaneously.

Each failover group in the configuration is given a primary or secondary unit preference. This preference determines on which unit in the failover pair the contexts in the failover group appear in the active state when both units start simultaneously. You can have both failover groups be in the active state on a single unit in the pair, with the other unit containing the failover groups in the standby state. However, a more typical configuration is to assign each failover group a different role preference to make each one active on a different unit, balancing the traffic across the devices.

**QUESTION NO: 3**

Which statements about the security appliance's multicasting capabilities are true? (Choose two)

A. The security appliance supports Stub Multicast Routing.
B. When the PIX security appliance is configured for Stub Multicast Routing, it is necessary to construct GRE tunnels to allow multicast traffic to bypass the PIX security appliance.
C. The PIX supports PIM and DVRMP and MOSPF.
D. The PIX security appliance can be configured to act as an IGMP proxy agent.

**Answer: A,D**

**Explanation:**

The security appliance supports both stub multicast routing and PIM multicast routing. However, you cannot configure both concurrently on a single security appliance.

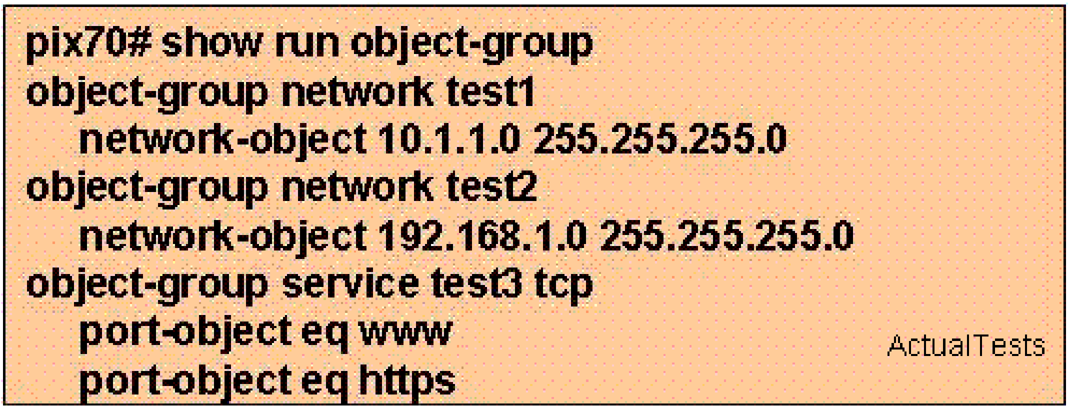
Stub multicast routing provides dynamic host registration and facilitates multicast routing. When configured for stub multicast routing, the security appliance acts as an IGMP proxy agent. Instead of fully participating in multicast routing, the security appliance forwards IGMP messages to an upstream multicast router, which sets up delivery of the multicast data. When configured for stub multicast routing, the security appliance cannot be configured for PIM.

The security appliance supports both PIM-SM and bi-directional PIM. PIM-SM is a multicast routing protocol that uses the underlying unicast routing information base or a separate multicast-

capable routing information base. It builds unidirectional shared trees rooted at a single Rendezvous Point per multicast group and optionally creates shortest-path trees per multicast source.
Reference: Cisco Security Appliance Command Line Configuration Guide 7.0, p. 8-17

**QUESTION NO: 4**

Refer to the show run output in the exhibit. Which access-list configuration using the object-groups shown will only permit HTTP and HTTPS traffic from any host on 10.1.1.0/24 to any host on 192.168.1.0/24?



```
pix70# show run object-group
object-group network test1
   network-object 10.1.1.0 255.255.255.0
object-group network test2
   network-object 192.168.1.0 255.255.255.0
object-group service test3 tcp
   port-object eq www
   port-object eq https
```

A. access-list aclin extended permit ip object-group test1 object-group test2
B. access-list aclin extended permit tcp object-group test2 object-group test1 object-group test3
C. access-list aclin extended permit tcp object-group test1 object-group test2 object-group test3
D. access-list aclin extended permit tcp object-group test1 object-group test3 object-group test2

**Answer: C**

**Explanation:**
To use object groups in an access list, replace the normal protocol ( protocol ), network ( source_addressmask , etc.), service ( operator port ), or ICMP type ( icmp_type ) parameter with object-group grp_id parameter.
For example, to use object groups for all available parameters in the access-list { tcp | udp } command, enter the following command:
hostname(config)# access-list access_list_name [ line line_number ] [ extended ] { deny | permit } { tcp | udp } object-group nw_grp_id [ object-group svc_grp_id ] object-group nw_grp_id [ object-group svc_grp_id ] [ log [[ level ] [ interval secs ] | disable | default ]] [ inactive | time-range time_range_name ]

Fundamentally, the same access rules apply whether of not object groups are used. First, the source network or networks is looked at, then the destination network, and finally the protocols used. Therefore, choice B is correct.
Reference:
http://www cisco com/en/US/products/ps6120/products configuration guide chapter09186a00804