642-618$^{Q\&As}$

Deploying Cisco ASA Firewall Solutions (FIREWALL v2.0)

QUESTION 1

Which two statements about traffic shaping capability on the Cisco ASA appliance are true? (Choose two.)

A. Traffic shaping can be applied to all outgoing traffic on a physical interface or, in the case of the Cisco ASA 5505 appliance, on a VLAN.

B. Traffic shaping can be applied in the input or output direction.

C. Traffic shaping can cause jitter and delay.

D. You can configure traffic shaping and priority queuing on the same interface.

E. With traffic shaping, when traffic exceeds the maximum rate, the security appliance drops the excess traffic.

Correct Answer: AC

http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/qos.html#wp1083655

Information About Traffic Shaping Traffic shaping is used to match device and link speeds, thereby controlling packet loss, variable delay, and link saturation, which can cause jitter and delay.

-Traffic shaping must be applied to all outgoing traffic on a physical interface or in the case of the ASA 5505, on a VLAN. You cannot configure traffic shaping for specific types of traffic. -Traffic shaping is implemented when packets are ready to be transmitted on an interface, so the rate calculation is performed based on the actual size of a packet to be transmitted, including all the possible overhead such as the IPsec header and L2 header. -The shaped traffic includes both through-the-box and from-the-box traffic. -The shape rate calculation is based on the standard token bucket algorithm. The token bucket size is twice the Burst Size value. See the "What is a Token Bucket?" section. -When burst traffic exceeds the specified shape rate, packets are queued and transmitted later. Following are some characteristics regarding the shape queue (for information about hierarchical priority queuing, see the "Information About Priority Queuing" section):

The queue size is calculated based on the shape rate. The queue can hold the equivalent of 200- milliseconds worth of shape rate traffic, assuming a 1500-byte packet. The minimum queue size is 64.

When the queue limit is reached, packets are tail-dropped. Certain critical keep-alive packets such as OSPF Hello packets are never dropped. The time interval is derived by time_interval = burst_size / average_rate. The larger the time interval is, the bustier the shaped traffic might be, and the longer the link might be idle. The effect can be best understood using the following exaggerated example:

Average Rate = 1000000 Burst Size = 1000000 In the above example, the time interval is 1 second, which means, 1 Mbps of traffic can be bursted out within the first 10 milliseconds of the 1-second interval on a 100 Mbps FE link and leave the remaining 990 milliseconds idle without being able to send any packets until the next time interval. So if there is delay sensitive traffic such as voice traffic, the Burst Size should be reduced compared to the average rate so the time interval is reduced.

QUESTION 2

When a Cisco ASA is configured in multiple context mode, within which configuration are the interfaces allocated to the security contexts?

A. each security context

B. system configuration

C. admin context (context with the "admin" role)

D. context startup configuration file (.cfg file)

Correct Answer: B

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/

products_configuration_example09186a00808d2b63.shtml

In order to specify the interfaces that you can use in the context, enter the command appropriate for a physical interface or for one or more subinterfaces.

In order to allocate a physical interface, enter this command:

hostname(config-ctx)# allocate-interface [mapped_name] [visible | invisible]

Context Configurations

The security appliance includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a standalone device. You can store context configurations on the internal Flash

memory or the external Flash memory card, or you can download them from a TFTP, FTP, or HTTP(S) server.

System Configuration

The system administrator adds and manages contexts by configuring each context configuration location, allocated interfaces, and other context operating parameters in the system configuration, which, like a single mode configuration, is the

startup configuration. The system configuration identifies basic settings for the security appliance. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access

network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the admin context. The system configuration does include a specialized failover interface for failover traffic only.

Admin Context Configuration

The admin context is just like any other context, except that when a user logs in to the admin context, then that user has system administrator rights and can access the system and all other contexts. The admin context is not restricted in any

way, and can be used as a regular context. However, because logging into the admin context grants you administrator privileges over all contexts, you might need to restrict access to the admin context to appropriate users. The admin context

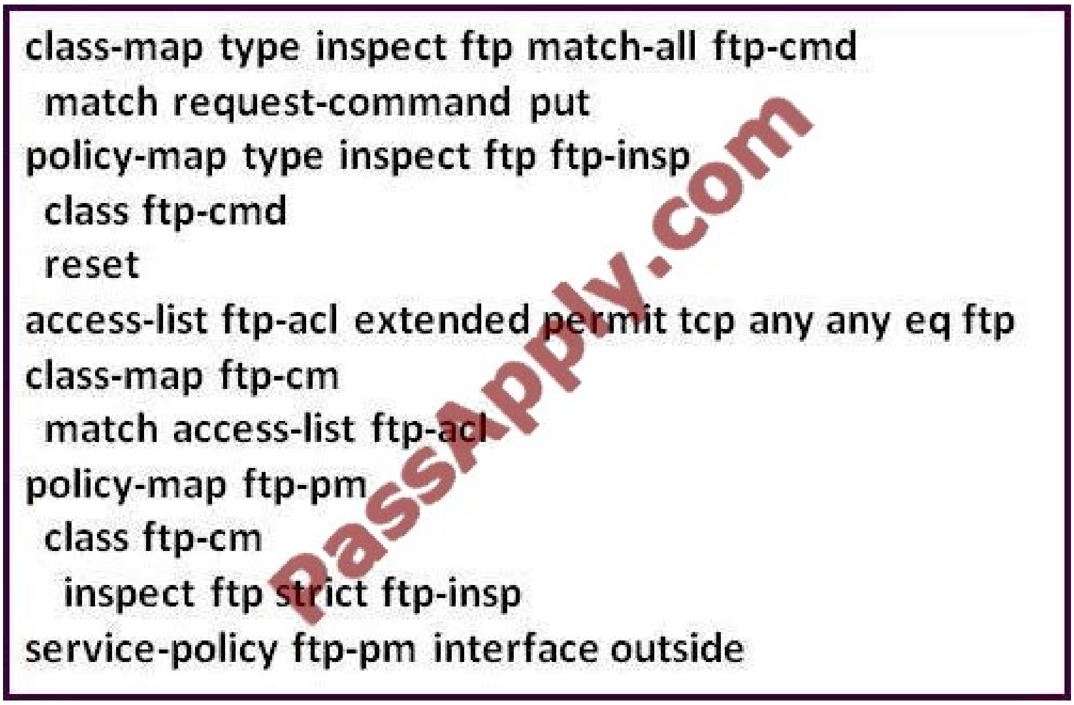
must reside on Flash memory, and not remotely.

If your system is already in multiple context mode, or if you convert from single mode, the admin context is created automatically as a file on the internal Flash memory called admin.cfg. This context is named "admin." If you do not want to use

admin.cfg as the admin context, you can change the admin context.

QUESTION 3

Refer to the exhibit.



```
class-map type inspect ftp match-all ftp-cmd
 match request-command put
policy-map type inspect ftp ftp-insp
 class ftp-cmd
 reset
access-list ftp-acl extended permit tcp any any eq ftp
class-map ftp-cm
 match access-list ftp-acl
policy-map ftp-pm
 class ftp-cm
  inspect ftp strict ftp-insp
service-policy ftp-pm interface outside
```

Which statement about the MPF configuration is true?

A. Any non-RFC complaint FTP traffic will go through additional deep FTP packet inspections.

B. FTP traffic must conform to the FTP RFC, and the FTP connection will be dropped if the PUT command is used.

C. Deep FTP packet inspections will be performed on all TCP inbound and outbound traffic on the outside interface.

D. The ftp-pm policy-map type should be type inspect.

E. Due to a configuration error, all FTP connections through the outside interface will not be permitted.

Correct Answer: B

QUESTION 4

Which three statements are the default security policy on a Cisco ASA appliance? (Choose three.)

A. Traffic that goes from a high security level interface to a lower security level interface is allowed.

B. Outbound TCP and UDP traffic is statefully inspected and returning traffic is allowed to traverse the Cisco ASA appliance.

C. Traffic that goes from a low security level interface to a higher security level interface is allowed.

D. Traffic between interfaces with the same security level is allowed by default.

E. Traffic can enter and exit the same interface by default.

F. When the Cisco ASA appliance is accessed for management purposes, the access must be made to the nearest Cisco ASA interface.

G. Inbound TCP and UDP traffic is statefully inspected and returning traffic is allowed to traverse the Cisco ASA appliance.

Correct Answer: ABF

The security algorithm is responsible for implementing and enforcing your security policies. The algorithm uses a tiered hierarchy that allows you to implement multiple levels of security. To accomplish this, each interface on the appliance is

assigned a security level number from 0 to 100, where 0 is the least secure and 100 is the most secure. The algorithm uses these security levels to enforce its default policies.

Here are the four default security policy rules for traffic as it flows through the appliance:

Traffic flowing from a higher-level security interface to a lower one is permitted by default. Traffic flowing from a lower-level security interface to a higher one is denied by default. Traffic flowing from one interface to another with the same

security level is denied by default. Traffic flowing into and then out of the same interface is denied by default

http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/access_rules.html#wp 1120072 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. 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.

Implicit Deny

Interface-specific access rules do not have an implicit deny at the end, but global rules on inbound traffic do have an implicit deny at the end of the list, so unless you explicitly permit it, traffic cannot pass. For example, if you want to allow all

users to access a network through the adaptive security appliance except for particular addresses, then you need to deny the particular addresses and then permit all others.

When you have no global access rules in your configuration, the implicit deny rule is applied at the end of interface access rules. When you configure both an interface access rule and a global access rule, the implicit deny (any any) is no

longer located at the end of the interface-based access rule. The implicit deny (any any) is enforced at the end of the global access rule. Logically, the entries on the interface-based access rule are processed first, followed by the entries on

the global access rule, and then finally the implicit deny (any any) at the end of the global access rule.

For example, when you have an interface-based access rule and a global access rule in your configuration, the following processing logic applies:

1.

interface access control rules

2.

global access control rules

3.

default global access control rule (deny any any)

When only interface-based access rules are configured, the following processing logic applies:

1.

interface access control rules

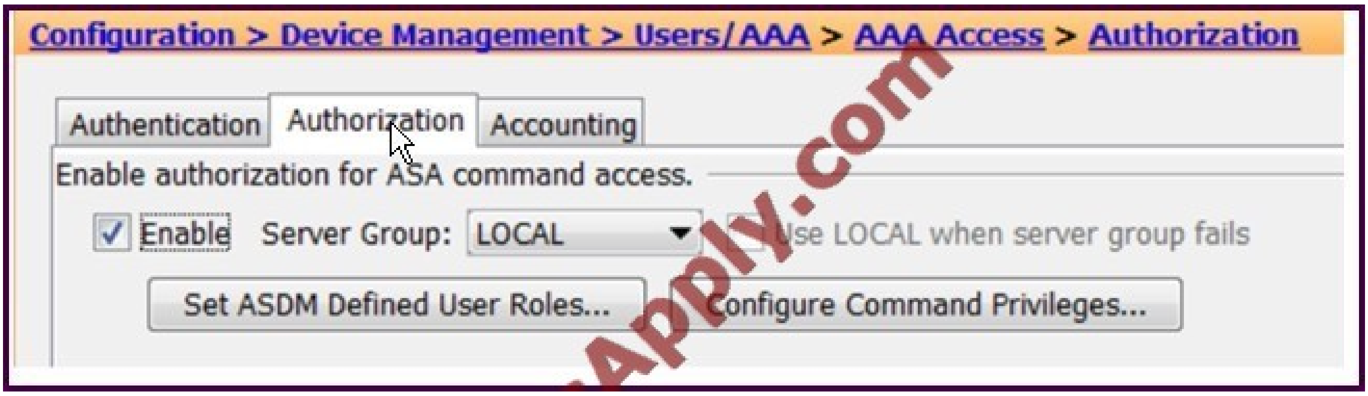
2.

default interface access control rule (deny any any) For EtherType rules, the implicit deny does not affect IPv4 or IPv6 traffic or ARPs; for example, if you allow EtherType 8037 (the EtherType for IPX), the implicit deny at the end of the list does not block any IP traffic that you previously allowed with an access rule (or implicitly allowed from a high security interface to a low security interface). However, if you explicitly deny all traffic with an EtherType rule, then IP and ARP traffic is denied.

Management access to an interface other than the one from which you entered the adaptive security appliance is not supported. For example, if your management host is located on the outside interface, you can only initiate a management connection directly to the outside interface. The only exception to this rule is through a VPN connection, and entering the management- access command. For more information about the management-access command, see the Cisco ASA 5500 Series Command Reference.

QUESTION 5

Refer to the exhibit.



Configuration > Device Management > Users/AAA > AAA Access > Authorization

Authentication
Authorization
Accounting

Enable authorization for ASA command access.

☑ Enable Server Group: LOCAL ☐ Use LOCAL when server group fails

Set ASDM Defined User Roles...
Configure Command Privileges...

Which two functions will the Set ASDM Defined User Roles perform? (Choose two.)

A. enables role based privilege levels to most Cisco ASA commands

B. enables the Cisco ASDM user to assign privilege levels manually to individual commands or groups of commands

C. enables command authorization with a remote TACACS+ server

D. enables three predefined user account privileges (Admin=Priv 15, Read Only=Priv 5, Monitor Only=Priv 3)

Correct Answer: AD

http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/user/guide/devaccss.html -To use predefined user account privileges, click Set ASDM Defined User Roles. The ASDM Defined User Roles Setup dialog box shows the commands and their levels. Click Yes to use the predefined user account privileges: Admin (privilege level 15, with full access to all CLI commands; Read Only (privilege level 5, with read-only access); and Monitor Only (privilege level 3, with access to the Monitoring section only). -To manually configure command levels, click the Configure Command Privileges button. The Command Privileges Setup dialog box appears. You can view all commands by choosing --All Modes-- from the Command Mode drop-down list, or you can choose a configuration mode to view the commands available in that mode. For example, if you choose context, you can view all commands available in context configuration mode. If a command can be entered in user EXEC/privileged EXEC mode as well as configuration mode, and the command performs different actions in each mode, you can set the privilege level for these modes separately. The Variant column displays show, clear, or cmd. You can set the privilege only for the show, clear, or configure form of the command. The configure form of the command is typically the form that causes a configuration change, either as the unmodified command (without the show or clear prefix) or as the no form.

To change the level of a command, double-click it or click Edit. You can set the level between 0 and 15. You can only configure the privilege level of the main command. For example, you can configure the level of all aaa commands, but not the level of the aaa authentication command and the aaa authorization command separately.

To change the level of all shown commands, click Select All and then Edit. Click OK to accept your changes.