642-618 Q&As

Deploying Cisco ASA Firewall Solutions (FIREWALL v2.0)

QUESTION 1

In which two directions are the Cisco ASA modular policy framework inspection policies applied? (Choose two.)

A. in the ingress direction only when applied globally

B. in the ingress direction only when applied on an interface

C. in the egress direction only when applied globally

D. in the egress direction only when applied on an interface

E. bi-directionally when applied globally

F. bi-directionally when applied on an interface

Correct Answer: AF

http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/mpf_service_policy.ht ml#wp1162717

Feature Directionality

Actions are applied to traffic bidirectionally or unidirectionally depending on the feature. For features that are applied bidirectionally, all traffic that enters or exits the interface to which you apply the policy map is affected if the traffic matches

the class map for both directions. When you use a global policy, all features are unidirectional; features that are normally bidirectional when applied to a single interface only apply to the ingress of each interface when applied globally.

Because the policy is applied to all interfaces, the policy will be applied in both directions so bidirectionality in this case is redundant.

QUESTION 2

Which addresses are considered "ambiguous addresses" and are put on the greylist by the Cisco ASA botnet traffic filter feature?

A. addresses that are unknown

B. addresses that are on the greylist identified by the dynamic database

C. addresses that are blacklisted by the dynamic database but also are identified by the static whitelist

D. addresses that are associated with multiple domain names, but not all of these domain names are on the blacklist

Correct Answer: D

http://www.cisco.com/en/US/docs/security/asa/asa83/asdm63/configuration_guide/protect_botne t.html

Botnet Traffic Filter Address Categories

Addresses monitored by the Botnet Traffic Filter include:

-Known malware addresses--These addresses are on the blacklist identified by the dynamic database and the static blacklist.

-Known allowed addresses--These addresses are on the whitelist. The whitelist is useful when an address is blacklisted by the dynamic database and also identified by the static whitelist.

-Ambiguous addresses--These addresses are associated with multiple domain names, but not all of these domain names are on the blacklist. These addresses are on the greylist.

-Unlisted addresses--These addresses are unknown, and not included on any list.

QUESTION 3

Which statement about static or default route on the Cisco ASA appliance is true?

A. The admin distance is 1 by default.

B. From the show route output, the [120/3] indicates an admin distance of 3.

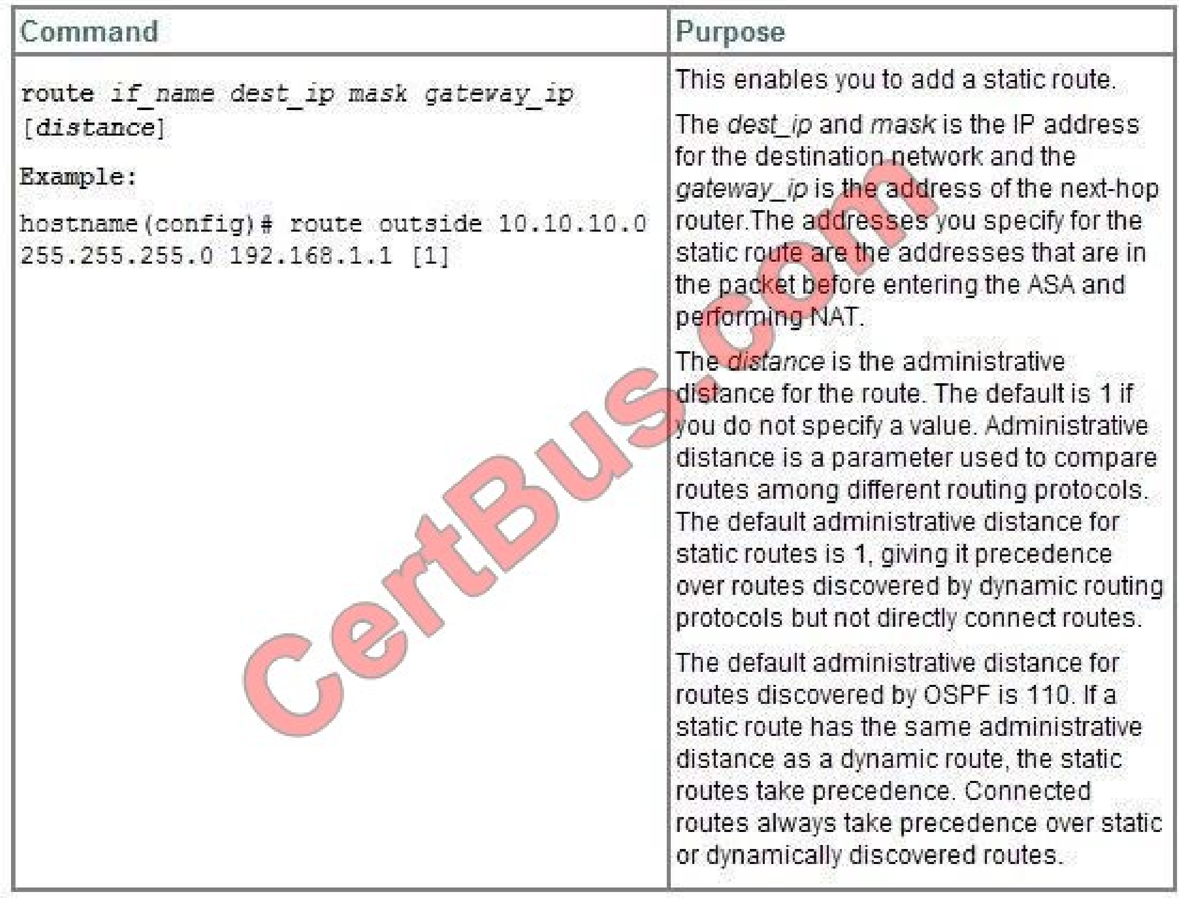
C. A default route is specified using the 0.0.0.0 255.255.255.255 address/mask combination.

D. The tunneled command option is used to enable route tracking.

E. The interface-name parameter in the route command is an optional parameter if the static route points to the next-hop router IP address.

Correct Answer: A

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/route_static.html#wp1 121521



Command	Purpose

`route if_name dest_ip mask gateway_ip [distance]`
Example:
`hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 [1]`
	This enables you to add a static route.
	The *dest_ip* and *mask* is the IP address for the destination network and the *gateway_ip* is the address of the next-hop router.The addresses you specify for the static route are the addresses that are in the packet before entering the ASA and performing NAT.
	The *distance* is the administrative distance for the route. The default is 1 if you do not specify a value. Administrative distance is a parameter used to compare routes among different routing protocols. The default administrative distance for static routes is 1, giving it precedence over routes discovered by dynamic routing protocols but not directly connect routes.
	The default administrative distance for routes discovered by OSPF is 110. If a static route has the same administrative distance as a dynamic route, the static routes take precedence. Connected routes always take precedence over static or dynamically discovered routes.

QUESTION 4

Which Cisco ASA feature enables the ASA to do these two things?

1) Act as a proxy for the server and generate a SYN-ACK response to the client SYN request.

2) When the Cisco ASA receives an ACK back from the client, the Cisco ASA authenticates the client and allows the connection to the server.

A. TCP normalizer

B. TCP state bypass

C. TCP intercept

D. basic threat detection

E. advanced threat detection

F. botnet traffic filter

Correct Answer: C

http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/conns_connlimits.html #wp1080734

TCP Intercept and Limiting Embryonic Connections Limiting the number of embryonic connections protects you from a DoS attack. The ASA uses the per-client limits and the embryonic connection limit to trigger TCP Intercept, which protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. TCP Intercept uses the SYN cookies algorithm to prevent TCP SYN-flooding attacks. A SYN-flooding attack consists of a series of SYN packets usually originating from spoofed IP addresses. The constant flood of SYN packets keeps the server SYN queue full, which prevents it from servicing connection requests.

When the embryonic connection threshold of a connection is crossed, the ASA acts as a proxy for the server and generates a SYN-ACK response to the client SYN request. When the ASA receives an ACK back from the client, it can then authenticate the client and allow the connection to the server.

QUESTION 5

When the Cisco ASA appliance is processing packets, which action is performed first?

A. Check if the packet is permitted or denied by the inbound interface ACL.

B. Check if the packet is permitted or denied by the outbound interface ACL.

C. Check if the packet is permitted or denied by the global ACL.

D. Check if the packet matches an existing connection in the connection table.

E. Check if the packet matches an inspection policy.

F. Check if the packet matches a NAT rule.

Correct Answer: D

http://www.cisco.com/en/US/products/ps6120/products_tech_note09186a0080ba9d00.shtml

QUESTION 6

Which option is one requirement before a Cisco ASA appliance can be upgraded from Cisco ASA Software Version 8.2 to 8.3?

A. Remove all the pre 8.3 NAT configurations in the startup configuration.

B. Upgrade the memory on the Cisco ASA appliance to meet the memory requirement of Cisco ASA Software Version 8.3.

C. Request new Cisco ASA licenses to meet the 8.3 licensing requirement.

D. Upgrade Cisco ASDM to version 6.2.

E. Migrate interface ACL configurations to include interface and global ACLs.

Correct Answer: B

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_bulletin_c 25-586414.html

QUESTION 7

On Cisco ASA Software Version 8.4.1 and later, when you configure the Cisco ASA appliance in transparent firewall mode, how is the Cisco ASA management IP address configured?

A. using the IP address global configuration command

B. using the IP address GigabitEthernet 0/x interface configuration command

C. using the IP address BVI x interface configuration command

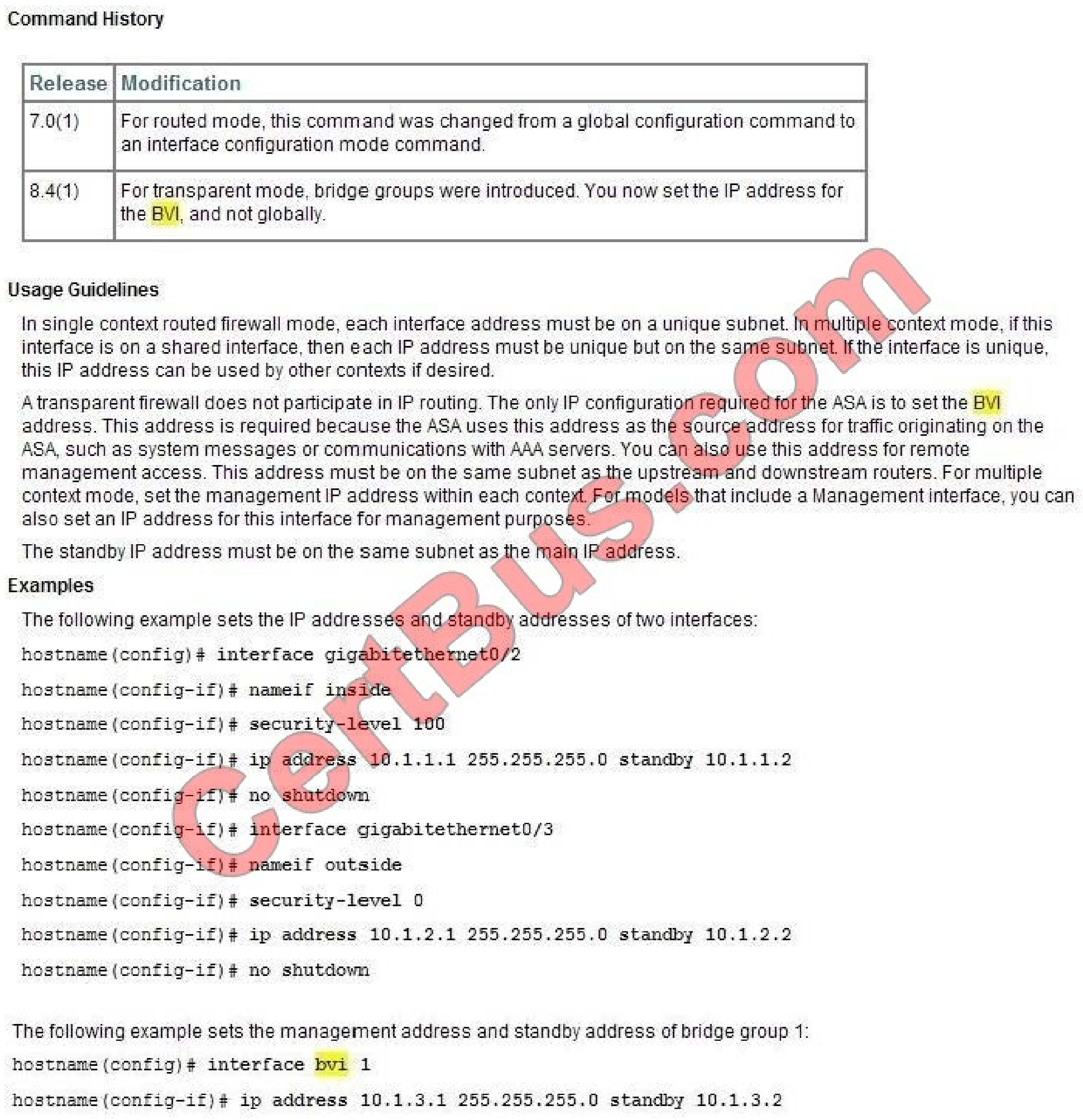
D. using the bridge-group global configuration command

E. using the bridge-group GigabitEthernet 0/x interface configuration command

F. using the bridge-group BVI x interface configuration command

Correct Answer: C

http://www.cisco.com/en/US/docs/security/asa/asa84/command/reference/i3.html#wp1898863



Command History

Release	Modification
7.0(1)	For routed mode, this command was changed from a global configuration command to an interface configuration mode command.
8.4(1)	For transparent mode, bridge groups were introduced. You now set the IP address for the BVI, and not globally.

Usage Guidelines

In single context routed firewall mode, each interface address must be on a unique subnet. In multiple context mode, if this interface is on a shared interface, then each IP address must be unique but on the same subnet. If the interface is unique, this IP address can be used by other contexts if desired.

A transparent firewall does not participate in IP routing. The only IP configuration required for the ASA is to set the BVI address. This address is required because the ASA uses this address as the source address for traffic originating on the ASA, such as system messages or communications with AAA servers. You can also use this address for remote management access. This address must be on the same subnet as the upstream and downstream routers. For multiple context mode, set the management IP address within each context. For models that include a Management interface, you can also set an IP address for this interface for management purposes.

The standby IP address must be on the same subnet as the main IP address.

Examples

The following example sets the IP addresses and standby addresses of two interfaces:

```
hostname(config)# interface gigabitethernet0/2
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/3
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0 standby 10.1.2.2
hostname(config-if)# no shutdown
```

The following example sets the management address and standby address of bridge group 1:

```
hostname(config)# interface bvi 1
hostname(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

QUESTION 8

On Cisco ASA Software Version 8.4 and later, which two options show the maximum number of active and standby ports that an EtherChannel can have? (Choose two.)

A. 2 active ports

B. 4 active ports

C. 6 active ports

D. 8 active ports

E. 2 standby ports

F. 4 standby ports

G. 6 standby ports

H. 8 standby ports

Correct Answer: DH

http://www.cisco.com/en/US/docs/security/asa/asa84/asdm64/configuration_guide/interface_star t.pdf

Channel Group Interfaces

Each channel group can have eight active interfaces. Note that you can assign up to 16 interfaces to a channel group. While only eight interfaces can be active, the remaining interfaces can act as standby links in case of interface failure.

All interfaces in the channel group must be the same type and speed. The first interface added to the channel group determines the correct type and speed.

The EtherChannel aggregates the traffic across all the available active interfaces in the channel. The port is selected using a proprietary hash algorithm, based on source or destination MAC addresses, IP addresses, TCP and UDP port

numbers and vlan numbers

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

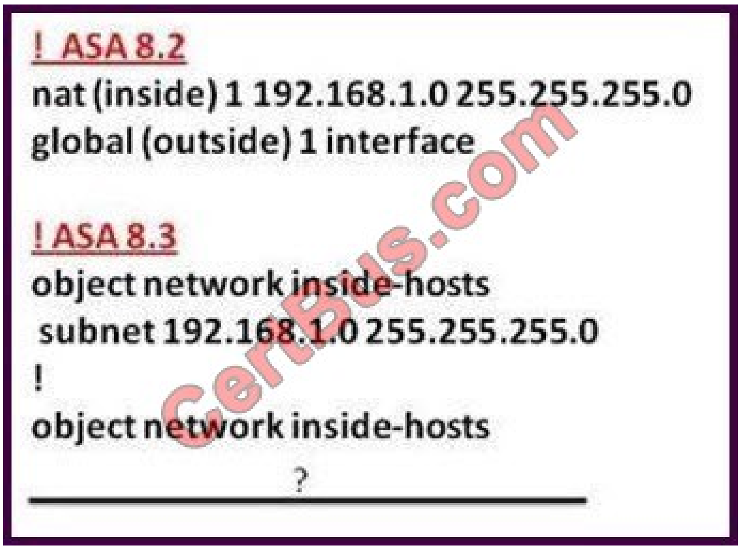
host

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.



```
! ASA 8.2
nat (inside) 1 192.168.1.0 255.255.255.0
global (outside) 1 interface

! ASA 8.3
object network inside-hosts
 subnet 192.168.1.0 255.255.255.0
!
object network inside-hosts
                    ?
_____________________________________
```

Which corresponding Cisco ASA Software Version 8.3 command accomplishes the same Cisco ASA Software Version 8.2 NAT configuration?

A. nat (any,any) dynamic interface

B. nat (any,any) static interface

C. nat (inside,outside) dynamic interface

D. nat (inside,outside) static interface

E. nat (outside,inside) dynamic interface

F. nat (outside,inside) static interface

Correct Answer: C

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

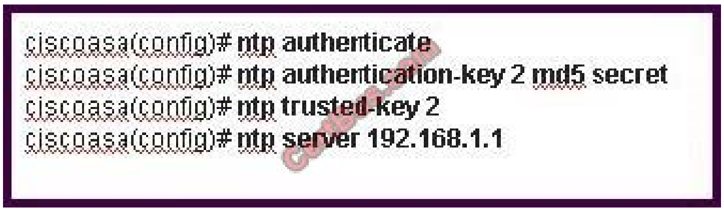
To create a many-to-one NAT where the entire inside network is getting PAT\\'d to a single outside IP do the following.

Old 8.2 command:

nat (inside) 1 10.0.0.0 255.255.255.0 global (outside) 1 interface New 8.3 equivalent command: object network inside-net subnet 10.0.0.0 255.255.255.0 nat (inside,outside) dynamic interface Note: the "interface" command is the 2nd interface in the nat statement, in this case the outside.

QUESTION 11

Refer to the exhibit.



```
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp authentication-key 2 md5 secret
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp server 192.168.1.1
```

Which reason explains why the Cisco ASA appliance cannot establish an authenticated NTP session to the inside 192.168.1.1 NTP server?

A. The ntp server 192.168.1.1 command is incomplete.

B. The ntp source inside command is missing.

C. The ntp access-group peer command and the ACL to permit 192.168.1.1 are missing.

D. The trusted-key number should be 1 not 2.

Correct Answer: A

http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/basic.html#wp106776 hostname(config)# ntp server ip_address [key key_id] [source interface_name][prefer] ntp server 192.168.1.1 2

QUESTION 12

Which option can cause the interactive setup script not to work on a Cisco ASA 5520 appliance running software version 8.4.1?

A. The clock has not been set on the Cisco ASA appliance using the clock set command.

B. The HTTP server has not been enabled using the http server enable command.

C. The domain name has not been configured using the domain-name command.

D. The inside interface IP address has not been configured using the ip address command.

E. The management 0/0 interface has not been configured as management-only and assigned a name using the nameif command.

Correct Answer: E

http://www.checkthenetwork.com/networksecurityCiscoASA1.asp shows need for nameif and http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/intparam.html shows manaagement only The ASA 5510 and higher adaptive security appliance also includes the following type: -management The management interface is a Fast Ethernet interface designed for management traffic only, and is specified as management0/0. You can, however, use it for through traffic if desired (see the management-only command). In

transparent firewall mode, you can use the management interface in addition to the two interfaces allowed for through traffic. You can also add subinterfaces to the management interface to provide management in each security context for multiple context mode.

Append the subinterface ID to the physical interface ID separated by a period (.). In multiple context mode, enter the mapped name if one was assigned using the allocate- interface command.

For example, enter the following command:

```
hostname(config)# interface gigabitethernet0/1.1
```

Step 2 To name the interface, enter the following command: hostname(config-if)# nameif name

The name is a text string up to 48 characters, and is not case-sensitive. You can change the name by reentering this command with a new value. Do not enter the no form, because that command causes all commands that refer to that name

to be deleted.

Step 3 To set the security level, enter the following command:

hostname(config-if)# security-level number Where number is an integer between 0 (lowest) and 100 (highest).

Step 4 (Optional) To set an interface to management-only mode, enter the following command:

hostname(config-if)# management-only The ASA 5510 and higher adaptive security appliance includes a dedicated management interface called Management 0/0, which is meant to support traffic to the security appliance. However, you can

configure any interface to be a management- only interface using the management-only command. Also, for Management 0/0, you can disable management-only mode so the interface can pass through traffic just like any other interface.

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

Try our product !

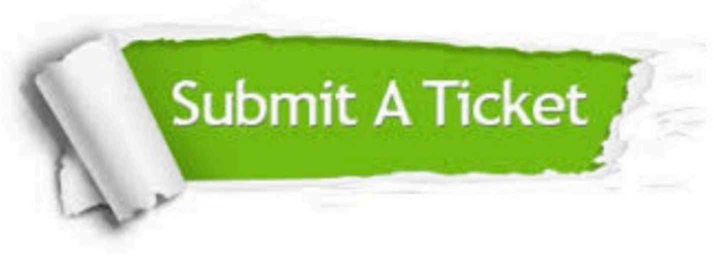
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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.certbus.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.