[Updated Constantly]

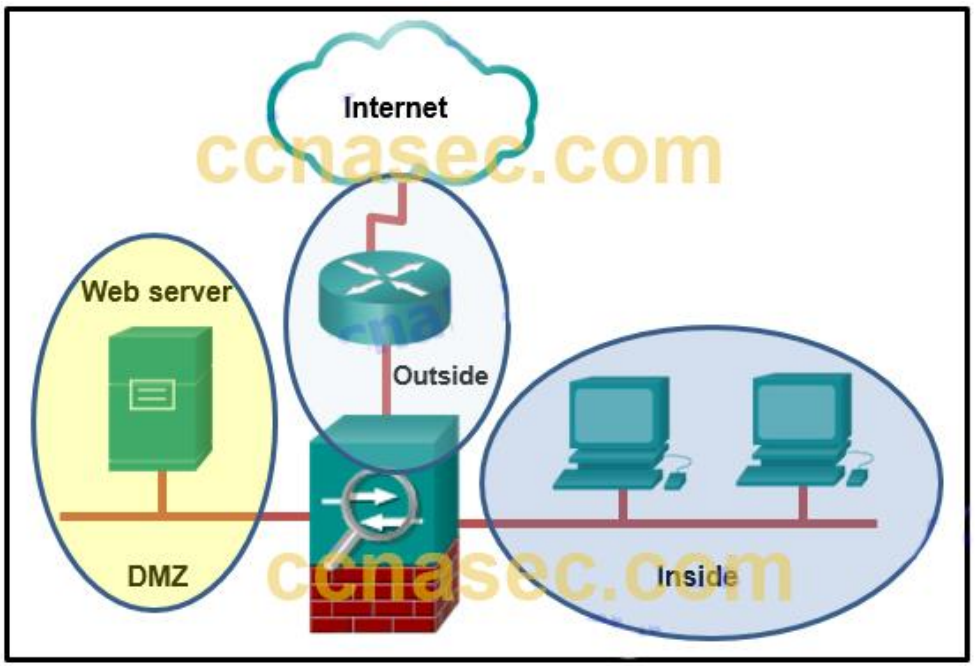
HERE

CCNA Security v2.0 Chapter 9 Exam Answers

How to find: Press “Ctrl + F” in the browser and fill in whatever wording is in the question to find that question/answer.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

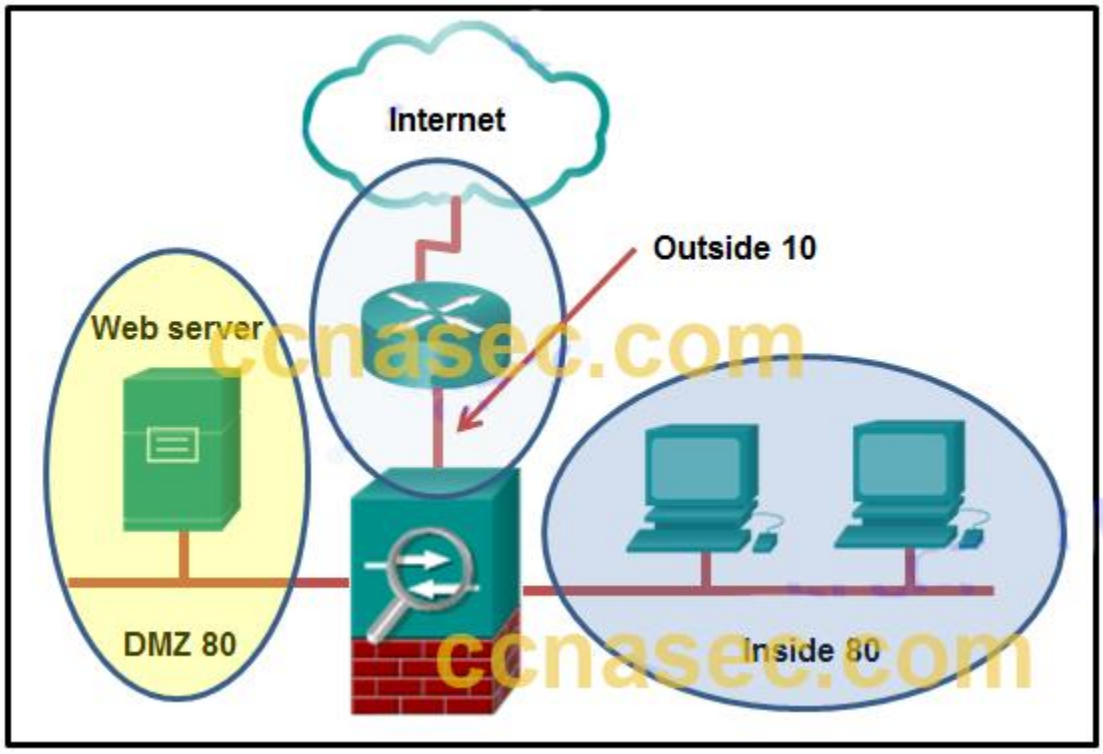
1. **Refer to the exhibit. A network administrator is configuring the security level for the ASA. What is a best practice for assigning the security level on the three interfaces?**



- Outside 40, Inside 100, DMZ 0
- Outside 0, Inside 35, DMZ 90
- Outside 100, Inside 10, DMZ 40
- **Outside 0, Inside 100, DMZ 50***

The Cisco ASA assigns security levels to distinguish among different networks it connects. Security levels define the level of trustworthiness of an interface. The higher the level, the more trusted the interface. The security level numbers range between 0 (untrustworthy) to 100 (very trustworthy). Therefore, the interface connecting to the Internet should be assigned the lowest level. The interface connecting to the internal network should be assigned the highest level. The interface connecting to the DMZ network should be assigned a level between them.

2. **Refer to the exhibit. A network administrator is configuring the security level for the ASA. Which statement describes the default result if the administrator tries to assign the Inside interface with the same security level as the DMZ interface?**



- The ASA allows inbound traffic initiated on the Internet to the DMZ, but not to the Inside interface.
- The ASA console will display an error message.
- **The ASA will not allow traffic in either direction between the Inside interface and the DMZ.***
- The ASA allows traffic from the Inside to the DMZ, but blocks traffic initiated on the DMZ to the Inside interface.

Multiple interfaces in an ASA can be assigned the same security level. To allow connectivity between interfaces with the same security levels, the same-security-traffic permit inter-interface global configuration command is required. Traffic from the higher level network to the lower level network is allowed by default. However, traffic initiated on the lower level network is denied access to the higher level network by default.

3. **What is a difference between ASA IPv4 ACLs and IOS IPv4 ACLs?**
   - ASA ACLs are always named, whereas IOS ACLs are always numbered.
   - Multiple ASA ACLs can be applied on an interface in the ingress direction, whereas only one IOS ACL can be applied.

- **ASA ACLs use the subnet mask in defining a network, whereas IOS ACLs use the wildcard mask.***
- ASA ACLs do not have an implicit deny any at the end, whereas IOS ACLs do.
- ASA ACLs use forward and drop ACEs, whereas IOS ACLs use permit and deny ACEs.

There are many similarities between ASA ACLs and IOS ACLs, including:
In both, there is an implicit deny any
Only one ACL per interface, per protocol, per direction still applies.
Both use deny and permit ACEs.
ACLs can be either named or numbered.
ASA ACLs differ from IOS ACLs in that they use a network mask (e.g., 255.255.255.0) instead of a wildcard mask (e.g. 0.0.0.255). Although most ASA ACLs are named, they can also be numbered.

4. **What is one of the drawbacks to using transparent mode operation on an ASA device?**
   - no support for IP addressing
   - no support for management
   - no support for using an ASA as a Layer 2 switch
   - **no support for QoS***

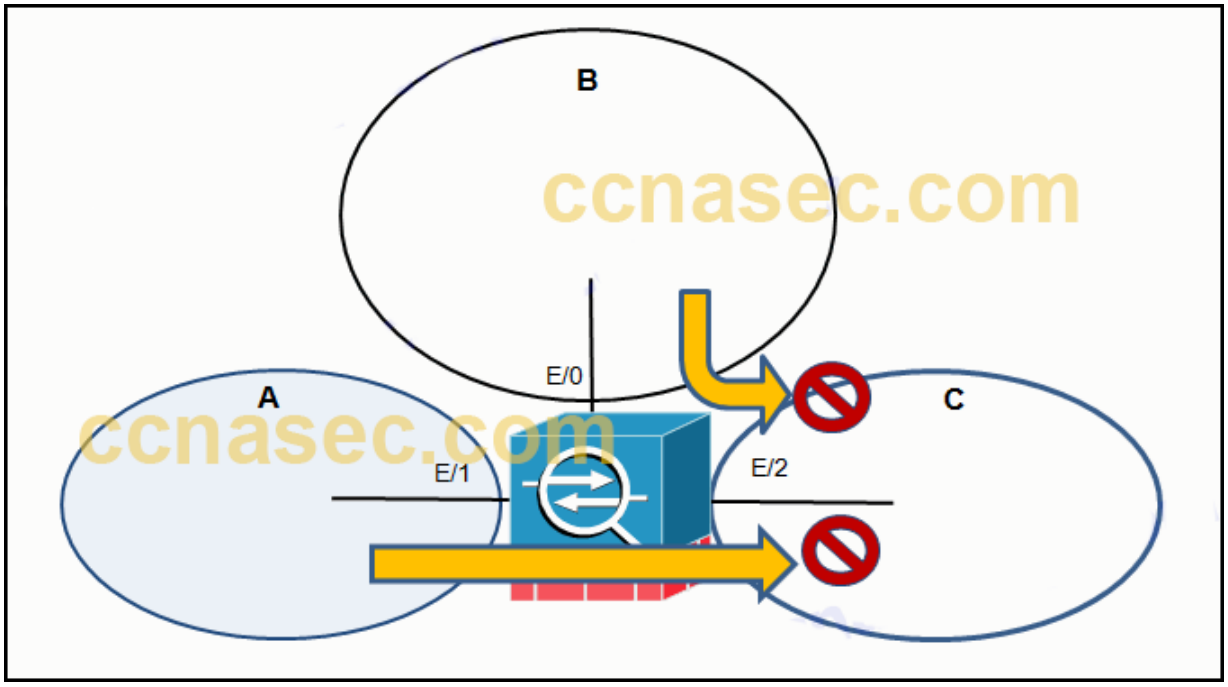
In transparent mode the ASA functions like a Layer 2 device. An ASA device can have an IP address assigned on the local network for management purposes. The drawbacks to using transparent mode include no support for dynamic routing protocols, VPNs, QoS, or DHCP Relay.

5. **What command defines a DHCP pool that uses the maximum number of DHCP client addresses available on an ASA 5505 that is using the Base license?**
   - CCNAS-ASA(config)# dhcpd address 192.168.1.20-192.168.1.50 inside
   - CCNAS-ASA(config)# dhcpd address 192.168.1.10-192.168.1.100 inside
   - **CCNAS-ASA(config)# dhcpd address 192.168.1.25-192.168.1.56 inside***
   - CCNAS-ASA(config)# dhcpd address 192.168.1.30-192.168.1.79 inside

The ASA 5505 Base license is a 10-user license and therefore the maximum number of DHCP clients supported is 32. The only pool that contains 32 addresses is the pool with range 192.168.1.25-192.168.1.56

6. **Refer to the exhibit. An administrator creates three zones (A, B, and C) in an ASA that filters traffic. Traffic originating from Zone A going to Zone C is denied, and traffic originating from Zone B going to Zone C is denied. What is a possible scenario for**

Zones A, B, and C?



- A – DMZ, B – Inside, C – Outside
- A – Inside, B – DMZ, C – Outside
- A – Outside, B – Inside, C – DMZ
- **A – DMZ, B – Outside, C – Inside***

7. **Which two statements are true about ASA standard ACLs? (Choose two.)**
   - They are the most common type of ACL.
   - They are applied to interfaces to control traffic.
   - **They are typically only used for OSPF routes.***
   - They specify both the source and destination MAC address.
   - **They identify only the destination IP address.***

   ASA standard ACLs are used to identify the destination IP addresses, unlike IOS ACLs where a standard ACL identifies the source host/network. They are typically only used for OSPF routes and can be used in a route map for OSPF redistribution. Standard access lists cannot be applied to interfaces to control traffic.

8. **What is a characteristic of ASA security levels?**
   - **An ACL needs to be configured to explicitly permit traffic from an interface with a lower security level to an interface with a higher security level.**
   - Each operational interface must have a name and be assigned a security level from 0 to 200.
   - The lower the security level on an interface, the more trusted the interface.

- Inbound traffic is identified as the traffic moving from an interface with a higher security level to an interface with a lower security level.

The ASA assigns security levels to distinguish between inside and outside networks. The higher the level, the more trusted the interface. The security level numbers range between 0 to 100. When traffic moves from an interface with a higher security level to an interface with a lower security level, it is considered outbound traffic.

9. **What must be configured on a Cisco ASA device to support local authentication?**
   - **AAA***
   - the IP address of the RADIUS or TACACS+ server
   - encrypted passwords
   - SSHv2
   - RSA keys

An ASA can be configured to authenticate by using a local user database or an external server, or both. Local authentication on a Cisco ASA requires the configuration of AAA on the ASA.

10. **Which statement describes a difference between the Cisco ASA IOS CLI feature and the router IOS CLI feature?**
    - ASA uses the ? command whereas a router uses the help command to receive help on a brief description and the syntax of a command.
    - **To use a show command in a general configuration mode, ASA can use the command directly whereas a router will need to enter the do command before issuing the show command.***
    - To complete a partially typed command, ASA uses the Ctrl+Tab key combination whereas a router uses the Tab key.
    - To indicate the CLI EXEC mode, ASA uses the % symbol whereas a router uses the # symbol.

The ASA CLI is a proprietary OS which has a similar look and feel to the Cisco router IOS. Although it shares some common features with the router IOS, it has its unique features. For example, an ASA CLI command can be executed regardless of the current configuration mode prompt. The IOS do command is not required or recognized. Both the ASA CLI and the router CLI use the # symbol to indicate the EXEC mode. Both CLIs use the Tab key to complete a partially typed command. Different from the router IOS, the ASA provides a help command that provides a brief command description and syntax for certain commands.

11. **What are two factory default configurations on an ASA 5505? (Choose two.)**

- VLAN 2 is configured with the name inside.
- The internal web server is disabled.
- DHCP service is enabled for internal hosts to obtain an IP address and a default gateway from the upstream device.
- **PAT is configured to allow internal hosts to access remote networks through an Ethernet interface.***
- **VLAN 1 is assigned a security level of 100.***

The ASA 5505 ships with a default configuration that includes the following:
VLAN 1 – for the inside network with security level 100.
VLAN 2 – for the outside network with security level 0 and it should acquire its IP address and default route from an upstream device.
PAT is configured so that inside host addresses are translated using the outside interface IP address.
HTTP access for ASDM is enabled.
DHCP services are provided to the inside hosts.

12. **Refer to the exhibit. Two types of VLAN interfaces were configured on an ASA 5505 with a Base license. The administrator wants to configure a third VLAN interface with limited functionality. Which action should be taken by the administrator to configure the third interface?**

```
ciscoasa# clock set 8:05:00 3 OCT 2011
ciscoasa# configure terminal
ciscoasa(config)# hostname CCNAS-ASA
CCNAS-ASA(config)# domain-name ccnasecurity.com
CCNAS-ASA(config)# enable password class
CCNAS-ASA(config)# interface vlan 1
CCNAS-ASA(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
CCNAS-ASA(config-if)# security-level 100
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)# interface ethernet0/1
CCNAS-ASA(config-if)# switchport access vlan 1
CCNAS-ASA(config-if)# no shutdown
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)# interface vlan 2
CCNAS-ASA(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
CCNAS-ASA(config-if)# security-level 0
CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)# interface ethernet0/0
CCNAS-ASA(config-if)# switchport access vlan 2
CCNAS-ASA(config-if)# no shutdown
CCNAS-ASA(config-if)# exit
```

- Because the ASA 5505 does not support the configuration of a third interface, the administrator cannot configure the third VLAN.
- **The administrator must enter the no forward interface vlan command before the nameif command on the third interface.**
- The administrator configures the third VLAN interface the same way the other two were configured, because the Base license supports the proposed action.
- The administrator needs to acquire the Security Plus license, because the Base license does not support the proposed action.

An ASA 5505 with a Base license does not allow three fully functioning VLAN interfaces to be created, but a third “limited” VLAN interface can be created if it is first configured with the no forward interface vlan command. When the inside and outside VLAN interfaces are configured, the no forward interface vlan number command must be entered before the nameif command is entered on the third interface. The Security Plus license is required to achieve full functionality.

13. **What is the purpose of the webtype ACLs in an ASA?**

- to inspect outbound traffic headed towards certain web sites
- to restrict traffic that is destined to an ASDM
- to monitor return traffic that is in response to web server requests that are initiated from the inside interface
- **to filter traffic for clientless SSL VPN users***

The webtype ACLs are used in a configuration that supports filtering for clientless SSL VPN users.

14. **Refer to the exhibit. A network administrator has configured NAT on an ASA device. What type of NAT is used?**

```
ciscoasa# clock set 8:05:00 3 OCT 2011
ciscoasa# configure terminal
ciscoasa(config)# hostname CCNAS-ASA
CCNAS-ASA(config)# domain-name ccnasecurity.com
CCNAS-ASA(config)# enable password class
CCNAS-ASA(config)# interface vlan 1
CCNAS-ASA(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
CCNAS-ASA(config-if)# security-level 100
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)# interface ethernet0/1
CCNAS-ASA(config-if)# switchport access vlan 1
CCNAS-ASA(config-if)# no shutdown
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)# interface vlan 2
CCNAS-ASA(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
CCNAS-ASA(config-if)# security-level 0
CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)# interface ethernet0/0
CCNAS-ASA(config-if)# switchport access vlan 2
CCNAS-ASA(config-if)# no shutdown
CCNAS-ASA(config-if)# exit
```

- **inside NAT***
- static NAT
- bidirectional NAT
- outside NAT

NAT can be deployed on an ASA using one of these methods:
inside NAT – when a host from a higher-security interface has traffic destined for a lower-security interface and the ASA translates the internal host address to a global address
outside NAT – when traffic from a lower-security interface destined for a host on the higher-security interface is translated
bidirectional NAT – when both inside NAT and outside NAT are used together
Because the nat command is applied so that the inside interface is mapped to the outside interface, the NAT type is inside. Also, the dynamic keyword in the nat command indicates that it is a dynamic mapping.

15. **Refer to the exhibit. A network administrator is configuring an object group on an ASA device. Which configuration keyword should be used after the object group name**

SERVICE1?

```
CORP-ASA# configure terminal
CORP-ASA(config)# object-group service SERVICE1 keyword
CORP-ASA(config-object-group)# port-object eq www
CORP-ASA(config-object-group)# port-object eq ftp
CORP-ASA(config-object-group)# port-object eq smtp
CORP-ASA(config-object-group)# exit
```

- icmp
- ip
- udp
- **tcp***

Because this is a service object group, the keyword should indicate which protocol is used. The options are tcp, udp, tcp-udp, icmp, and icmpv6. The subsequent commands indicate that the services in the group are WWW, FTP, and SMTP. Because all of these protocols use TCP, the keyword in the service object group should be tcp.

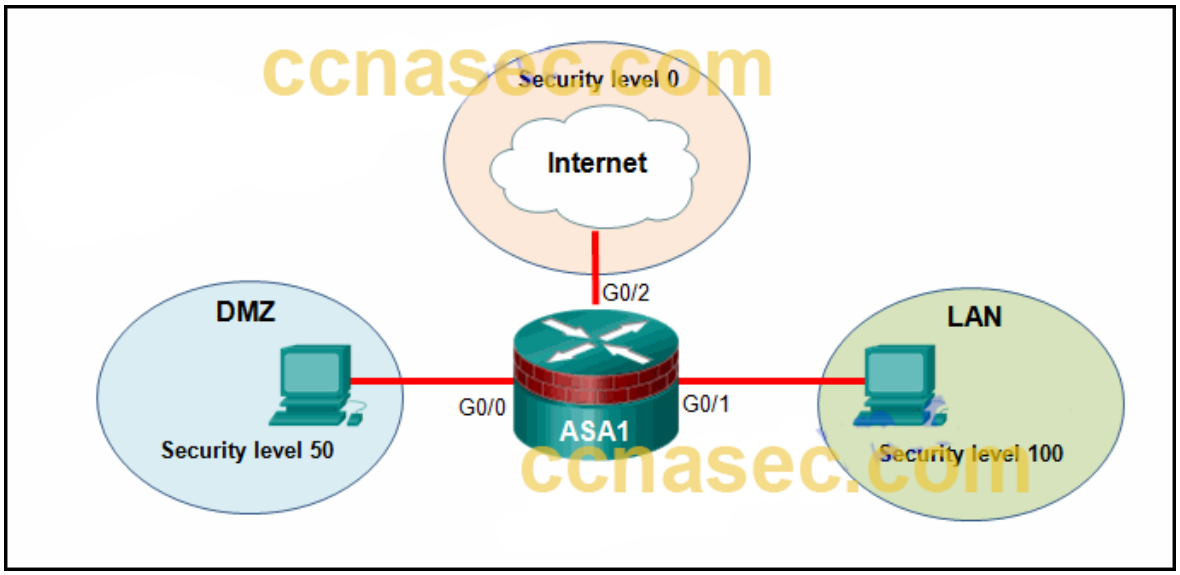
16. **When dynamic NAT on an ASA is being configured, what two parameters must be specified by network objects? (Choose two.)**
    - **a range of private addresses that will be translated***
    - the interface security level
    - **the pool of public global addresses***
    - the inside NAT interface
    - the outside NAT interface

    On an ASA, both the pool of addresses that will be used as inside global address and the range of internal private addresses that should be translated are configured through network objects.

17. **What function is performed by the class maps configuration object in the Cisco modular policy framework?**
    - **identifying interesting traffic***
    - applying a policy to an interface
    - applying a policy to interesting traffic
    - restricting traffic through an interface

    There are three configuration objects in the MPF; class maps, policy maps, and service policy. The class maps configuration object uses match criteria to identify interesting traffic.

18. **Refer to the exhibit. Based on the security levels of the interfaces on ASA1, what traffic will be allowed on the interfaces?**



- Traffic from the Internet and DMZ can access the LAN.
- Traffic from the Internet and LAN can access the DMZ.
- Traffic from the Internet can access both the DMZ and the LAN.
- **Traffic from the LAN and DMZ can access the Internet.***

ASA devices have security levels assigned to each interface that are not part of a configured ACL. These security levels allow traffic from more secure interfaces, such as security level 100, to access less secure interfaces, such as level 0. By default, they allow traffic from more secure interfaces (higher security level) to access less secure interfaces (lower security level). Traffic from the less secure interfaces is blocked from accessing more secure interfaces.

19. **What are three characteristics of the ASA routed mode? (Choose three.)**

- This mode is referred to as a “bump in the wire.”
- In this mode, the ASA is invisible to an attacker.
- **The interfaces of the ASA separate Layer 3 networks and require different IP addresses in different subnets.***
- **It is the traditional firewall deployment mode.***
- This mode does not support VPNs, QoS, or DHCP Relay.
- **NAT can be implemented between connected networks.***

Routed mode is the traditional mode for deploying a firewall where there are two or more interfaces that separate Layer 3 networks. The ASA is considered to be a router hop in the network and can perform NAT between connected networks. Routed mode supports multiple interfaces. Each interface is on a different subnet and requires an IP address on that subnet.

20. **Refer to the exhibit. An administrator has configured an ASA 5505 as indicated but is still unable to ping the inside interface from an inside host. What is the cause of this problem?**

```
CCNAS-ASA(config)# interface vlan 1
CCNAS-ASA(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
CCNAS-ASA(config-if)# security-level 100
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)# no shut
CCNAS-ASA(config-if)# interface e0/1
CCNAS-ASA(config-if)# switchport access vlan 1
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)# interface vlan 2
CCNAS-ASA(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
CCNAS-ASA(config-if)# security-level 0
CCNAS-ASA(config-if)# no shut
CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)# interface e0/0
CCNAS-ASA(config-if)# switchport access vlan 2
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)#
```

- **The no shutdown command should be entered on interface Ethernet 0/1.***
- VLAN 1 should be the outside interface and VLAN 2 should be the inside interface.
- VLAN 1 should be assigned to interface Ethernet 0/0 and VLAN 2 to Ethernet 0/1.
- The security level of the inside interface should be 0 and the outside interface should be 100.
- An IP address should be configured on the Ethernet 0/0 and 0/1 interfaces.

VLAN 1 and VLAN 2 have been configured correctly. Neither e0/0 nor e0/1 have been activated. For an inside host to ping the inside interface would require activating the e0/1 interface.

21. **Refer to the exhibit. According to the command output, which three statements are true about the DHCP options entered on the ASA 5505? (Choose three.)**

```
CCNAS-ASA# show dhcpd state
Context  Configured as DHCP Server
Interface inside, Configured for DHCP SERVER
Interface outside, Configured for DHCP CLIENT
CCNAS-ASA#
```

- The dhcpd address [start-of-pool]-[end-of-pool] inside command was issued to enable the DHCP client.
- The dhcpd auto-config outside command was issued to enable the DHCP server.

- **The dhcpd address [start-of-pool]-[end-of-pool] inside command was issued to enable the DHCP server.***
- **The dhcpd auto-config outside command was issued to enable the DHCP client.***
- The dhcpd enable inside command was issued to enable the DHCP client.
- **The dhcpd enable inside command was issued to enable the DHCP server.***

22. **Refer to the exhibit. What will be displayed in the output of the show running-config object command after the exhibited configuration commands are entered on an ASA 5505?**

```
CCNAS-ASA(config)# object network EXAMPLE-1
CCNAS-ASA(config-network-object)# host 192.168.1.3
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show running-config object
object network EXAMPLE-1
 host 192.168.1.3
CCNAS-ASA(config)#
CCNAS-ASA(config)# object network EXAMPLE-1
CCNAS-ASA(config-network-object)# host 192.168.1.4
CCNAS-ASA(config-network-object)# range 192.168.1.10 192.168.1.20
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
```

- host 192.168.1.4
- host 192.168.1.3, host 192.168.1.4, and range 192.168.1.10 192.168.1.20
- host 192.168.1.4 and range 192.168.1.10 192.168.1.20
- host 192.168.1.3 and host 192.168.1.4
- **range 192.168.1.10 192.168.1.20***
- host 192.168.1.3

The show running-config object command is used to display or verify the IP address/mask pair within the object. There can only be one statement in the network object. Entering a second IP address/mask pair will replace the existing configuration.

23. **Which type of NAT would be used on an ASA where 10.0.1.0/24 inside addresses are to be translated only if traffic from these addresses is destined for the 198.133.219.0/24 network?**

- **policy NAT***
- dynamic NAT
- static NAT
- dynamic PAT

Policy NAT is based on rules that determine when specific source addresses will get translated. Those source addresses are intended for specific destination addresses or for specific ports or for both a destination address and a specific port.

24. **Which statement describes a feature of AAA in an ASA device?**
    - **Accounting can be used alone.***
    - Authorization is enabled by default.
    - If authorization is disabled, all authenticated users will have a very limited access to the commands.
    - Both authorization and accounting require a user to be authenticated first.

AAA services (authentication, authorization, and accounting) are disabled by default. Authentication can be used alone or with authorization and accounting. Authorization always requires a user to be authenticated first. Accounting can be used alone, or with authentication and authorization. Authorization controls the services and commands that are available to each authenticated user. If authorization is not enabled, authentication would provide the same access to services for all authenticated users.

25. **A network administrator is working on the implementation of the Cisco Modular Policy Framework on an ASA device. The administrator issues a clear service-policy command. What is the effect after this command is entered?**
    - All class map configurations are removed.
    - **All service policy statistics data are removed.***
    - All service policies are removed.
    - All policy map configurations are removed.

In an MPF implementation, the clear service-policy command clears the service policy statistics. The clear configure service-policy command in global configuration mode removes all service policies.

26. **What is needed to allow specific traffic that is sourced on the outside network of an ASA firewall to reach an internal network?**
    - **ACL***
    - NAT
    - dynamic routing protocols
    - outside security zone level 0

In order to explicitly permit traffic from an interface with a lower security level to an interface with a higher security level, an ACL must be configured. By default, traffic will only flow from a higher security level to a lower.