[Updated Constantly]

HERE

CCNA Security v2.0 Chapter 10 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.

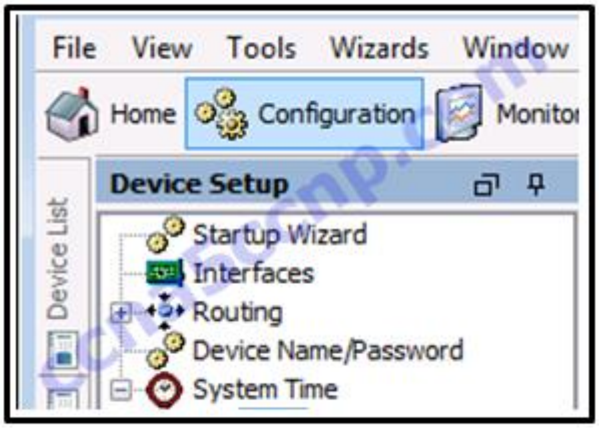
NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. **Which ASDM configuration option is used to configure the ASA enable secret password?**

- **Device Setup***
- Monitoring
- Interfaces
- Device Management

The two main ASDM options used to configure an ASA are Device Setup and Device Management. Within Device Setup are the Startup Wizard, Interfaces, Routing, Device Name/Password, and System Time options.

2. **Refer to the exhibit. Which Device Setup ASDM menu option would be used to configure the ASA for an NTP server?**



- Startup Wizard
- Device Name/Password
- Routing
- Interfaces
- **System Time***

The System Time option is used to manually configure the time zone, date, and time or to configure the system to obtain the date and time from an NTP server.

3. **True or False?**
   The ASA can be configured through ASDM as a DHCP server.

- false
- **true***

Use the Device Management configuration option to select DHCP and configure DHCP inside and outside settings.

4. **Which ASDM interface option would be used to configure an ASA as a DHCP server for local corporate devices?**

- DMZ
- outside
- local
- **inside***

ASDM supports DHCP server and relay settings. From the DHCP Server menu option, select the inside interface and enable the DHCP server option to provide addresses for devices attached through the inside ASA interface. The DMZ commonly contains servers that have statically assigned IP addresses. The outside interface connects to the WAN and would not have devices that would use corporate-provided DHCP.

5. **When ASDM is used to configure an ASA site-to-site VPN, what can be customized to secure traffic?**

- ISAKMP
- IKE
- **IKE and ISAKMP***
- preshared key

When selected traffic is being secured during ASDM site-to-site VPN configuration, both IKE and ISAKMP parameters can be set. The authentication options are a preshared key or the use of a digital certificate.

6. **Which VPN solution allows the use of a web browser to establish a secure, remote-access VPN tunnel to the ASA?**

- **clientless SSL***
- site-to-site using an ACL
- site-to-site using a preshared key
- client-based SSL

When a web browser is used to securely access the corporate network, the browser must use a secure version of HTTP to provide SSL encryption. A VPN client is not required to be installed on the remote host, so a clientless SSL connection is used.

7. **What must be configured on an ASA before it can be accessed by ASDM?**

- **web server access***
- Telnet or SSH
- an Ethernet port other than 0/0
- Ethernet 0/0 IP address

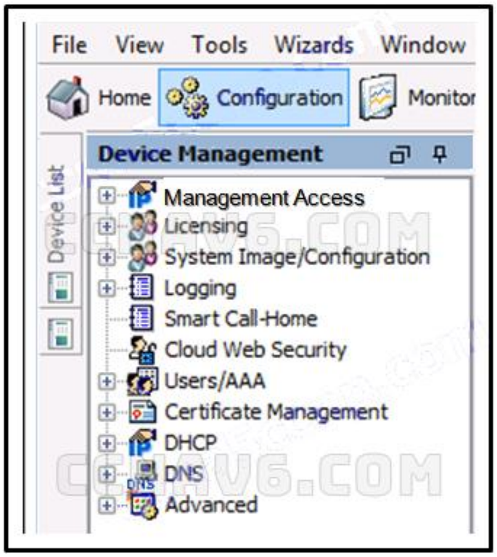
Before an ASA can be accessed using ASDM, the ASA must have access permissions and the ASA web server enabled. Furthermore, a management interface must be configured. On an ASA 5505, a logical VLAN interface and Ethernet port other than 0/0 must be configured. All other ASAs must have a dedicated Layer 3 management interface that is assigned an IP address and appropriate security level.

8. **How is an ASA interface configured as an outside interface when using ASDM?**

- Select a check box from the Interface Type option that shows inside, outside, and DMZ.
- Select outside from the Interface Type drop-down menu.
- **Enter the name “outside” in the Interface Name text box.***
- Drag the interface to the port labeled “outside” in the ASA drawing.

To configure an ASA interface using ASDM, select the desired interface and click Add. In the Interface Name textbox, enter outside. Assign the security level, IP address, and subnet mask. Do not forget to enable the Enable Interface check box.

9. **Refer to the exhibit. Which Device Management menu item would be used to access the ASA command line from within Cisco ASDM?**



- Licensing
- System Image/Configuration
- **Management Access***
- Advanced

To access the command line, expand the Management Access option, expand the Command Line (CLI) section, and select CLI Prompt.

10. **Which remote-access VPN connection allows the user to connect by using a web browser?**

- IPsec (IKEv2) VPN
- site-to-site VPN
- **clientless SSL VPN***
- IPsec (IKEv1) VPN

When a web browser is used to securely access the corporate network, the browser must use a secure version of HTTP to provide SSL encryption. A VPN client is not required to be installed on the remote host, so a clientless SSL connection is used.

11. **Which ASDM configuration option re-encrypts all shared keys and passwords on an ASA?**

- security master
- super encryption
- **master passphrase***
- device protection

The master passphrase is used to reversibly encrypt shared keys and passwords.

12. **Which type of encryption is applied to shared keys and passwords when the master passphrase option is enabled through ASDM for an ASA?**

- 3DES
- public/private key
- **AES***
- 128-bit

The master passphrase is used to reversibly encrypt shared keys and passwords. Once enabled, AES encryption is used for the password encryption.

13. **Which statement describes the function provided to a network administrator who uses the Cisco Adaptive Security Device Manager (ASDM) GUI that runs as a Java Web Start application?**

- **The administrator can connect to and manage a single ASA.***

- The administrator can connect to and manage multiple ASA devices.
- The administrator can connect to and manage multiple ASA devices and Cisco routers.
- The administrator can connect to and manage multiple ASA devices, Cisco routers, and Cisco switches.

Cisco Adaptive Security Device Manager (ASDM) is a Java-based GUI tool that facilitates the management of Cisco ASAs. Cisco ASDM can be used to manage multiple ASAs that run the same ASDM version. ASDM can be run as a Java Web Start application that allows an administrator to configure and monitor that ASA device. Otherwise ASDM can also be downloaded from flash and installed locally on a host as an application; which allows an administrator to use ASDM (local application) to manage multiple ASA devices.

14. **What is one benefit of using ASDM compared to using the CLI to configure the Cisco ASA?**

- It does not require any initial device configuration.
- **It hides the complexity of security commands.***
- ASDM provides increased configuration security.
- It does not require a remote connection to a Cisco device.

Cisco ASDM facilitates configuration of Cisco ASAs because it hides the complexity of the configuration commands. The ASA is required to have a minimum configuration before accessing the ASDM. ASDM is accessed using a web browser connection or local application which provides no more security than being consoled into the device.

15. **Which type of security is required for initial access to the Cisco ASDM by using the local application option?**

- **SSL***
- WPA2 corporate
- biometric
- AES

ASDM is accessed using an SSL local application connection.

16. **Which minimum configuration is required on most ASAs before ASDM can be used?**

- SSH
- **a dedicated Layer 3 management interface***
- a logical VLAN interface and an Ethernet port other than 0/0
- Ethernet 0/0

Before an ASA can be accessed using ASDM, the ASA must have a management interface configured. On an ASA 5505 , a logical VLAN interface and Ethernet port other than 0/0 must be configured. All other ASAs must have a dedicated Layer 3 management interface that is assigned an IP address and appropriate security level.

17. **When the CLI is used to configure an ISR for a site-to-site VPN connection, which two items must be specified to enable a crypto map policy? (Choose two.)**

- the hash
- **the peer***
- encryption
- the ISAKMP policy
- **a valid access list***
- IP addresses on all active interfaces

After the crypto map command in global configuration mode has been issued, the new crypto map will remain disabled until a peer and a valid access list have been configured.

18. **What is the purpose of the ACL in the configuration of an ISR site-to-site VPN connection?**

- to permit only secure protocols
- to log denied traffic
- to identify the peer
- **to define interesting traffic***

An ACL is used in the ISR configuration of a site-to-site VPN connection to define traffic that will be permitted. This traffic is referred to as interesting traffic.

19. **Which remote-access VPN connection allows the user to connect using Cisco AnyConnect?**

- **IPsec (IKEv2) VPN***
- site-to-site VPN
- clientless SSL VPN
- IPsec (IKEv1) VPN

Cisco AnyConnect is used to create an IPsec (IKEv2) VPN connection. A web browser is used for a clientless SSL VPN. A Cisco VPN client uses IPsec (IKEv1).

20. **Which statement describes available user authentication methods when using an ASA 5505 device?**

- **The ASA 5505 can use either a AAA server or a local database.***
- The ASA 5505 only uses a AAA server for authentication.
- The ASA 5505 only uses a local database for authentication.
- The ASA 5505 must use both a AAA server and a local database.

Authentication on an ASA 5505 device can be accomplished by using a AAA server and indicating the location of the server. Alternatively, a local database can be used by entering the appropriate username and password.

21. **Which remote-access VPN connection needs a bookmark list?**

- IPsec (IKEv1) VPN
- IPsec (IKEv2) VPN
- site-to-site VPN
- **clientless SSL VPN***

The clientless SSL VPN uses a web browser for access and uses a set of URLs that are configured to be used with the web portal.

22. **What occurs when a user logs out of the web portal on a clientless SSL VPN connection?**

- The browser cache is cleared.
- Downloaded files are deleted.
- **The user no longer has access to the VPN.***
- The web portal times out.

When a user logs out, he or she loses access to the VPN. The user does receive a message advising to clear the browser cache, delete the downloaded files, and close the browser window for added security. If the user does not log out, the connection will eventually time out.

23. **If an outside host does not have the Cisco AnyConnect client preinstalled, how would the host gain access to the client image?**

- The host initiates a clientless connection to a TFTP server to download the client.
- **The host initiates a clientless VPN connection using a compliant web browser to download the client.***
- The Cisco AnyConnect client is installed by default on most major operating systems.
- The host initiates a clientless connection to an FTP server to download the client.

If an outside host does not have the Cisco AnyConnect client preinstalled, the remote user must initiate a clientless SSL VPN connection via a compliant web browser, and then download and install the AnyConnect client on the remote host.

24. **What is an optional feature that is performed during the Cisco AnyConnect Secure Mobility Client VPN establishment phase?**

- security optimization
- host-based ACL installation

- **posture assessment***
- quality of service security

During the process of establishing a VPN connection, a posture assessment can be performed in order to identify the client operating system, antivirus, antispyware, and firewall software. Once identified, a determination can be made whether remote access is allowed.

25. **Which item describes secure protocol support provided by Cisco AnyConnect?**

- neither SSL nor IPsec
- SSL only
- **both SSL and IPsec***
- IPsec only

Both IPsec and SSL are supported by Cisco AnyConnect.

26. **What is the purpose of configuring an IP address pool to be used for client-based SSL VPN connections?**

- to assign addresses to the interfaces on the ASA
- to identify which users are allowed to download the client image
- **to assign IP addresses to clients when they connect***
- to identify which clients are allowed to connect

The IP address pool is assigned to clients when they connect. The IP address pool configuration is required for successful client-based SSL VPN connectivity. Without an available IP address pool, the connection to the security appliance fails.