Question 1
Which three configurations are required for both IPsec VTI and crypto map-based VPNs?
Which three configurations are required for both IPsec VTI and crypto map-based VPNs? (Choose three.)
A. transform set
B. ISAKMP policy
C. ACL that defines traffic to encrypt
D. dynamic routing protocol
E. tunnel interface
F. IPsec profile
G. PSK or PKI trustpoint with certificate
Correct Answer: ABG
Explanation/Reference:

Question 2
Which technology should you use?
As network security architect, you must implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity.
Which technology should you use?
A. IPsec DVTI
B. FlexVPN
C. DMVPN
D. IPsec SVTI
E. GET VPN
Correct Answer: E
Explanation/Reference:

Question 3
Which two statements about the Cisco ASA Clientless SSL VPN smart tunnels feature are true?
Which two statements about the Cisco ASA Clientless SSL VPN smart tunnels feature are true? (Choose two.)
A. Smart tunnels are enabled on the secure gateway (Cisco ASA) for specific applications that run on the end client and work irrespective of which transport protocol the application uses.
B. Smart tunnels require Administrative privileges to run on the client machine.
C. A smart tunnel is a DLL that is pushed from the headend to the client machine after SSL VPN portal authentication and that is attached to smarttunneled processes to route traffic through the SSL VPN session with the gateway.
D. Smart tunnels offer better performance than the client-server plugins.
E. Smart tunnels are supported on Windows, Mac, and Linux.
Correct Answer: CD
Explanation/Reference:

Question 4
Which three types of SSO functionality are available on the Cisco ASA without any external SSO servers?
Which three types of SSO functionality are available on the Cisco ASA without any external SSO servers? (Choose three.)
A. SAML
B. HTTP POST
C. HTTP Basic
D. NTLM
E. Kerberos
F. OAuth 2.0
Correct Answer: BCD
Explanation/Reference:

Question 5
Which Cisco ASA SSL VPN feature provides support for PCI compliance by allowing for the validation of two sets of username and password credentials on the SSL VPN login page?
Which Cisco ASA SSL VPN feature provides support for PCI compliance by allowing for the validation of two sets of username and password credentials on the SSL VPN login page?
A. Single Sign-On
B. Certificate to Profile Mapping
C. Double Authentication
D. RSA OTP
Correct Answer: C
Explanation/Reference:

Question 6
Which statement is correct concerning the SSL VPN authorization process?
Authorization of a clientless SSL VPN defines the actions that a user may perform within a clientless SSL VPN session. Which statement is correct concerning the SSL VPN authorization process?

A. Remote clients can be authorized by applying a dynamic access policy, which is configured on an external AAA server.
B. Remote clients can be authorized externally by applying group parameters from an external database.
C. Remote client authorization is supported by RADIUS and TACACS+ protocols.
D. To configure external authorization, you must configure the Cisco ASA for cut-through proxy.

Correct Answer: B
Explanation/Reference:

Question 7
Which Cisco ASA platform should be selected if the requirements are to support 35,000 connections per second, 600,000 maximum connections, and traffic shaping?

A. 5540
B. 5550
C. 5580-20
D. 5580-40

Correct Answer: B
Explanation/Reference:

Question 8
Which three actions can be applied to a traffic class within a type inspect policy map? (Choose three.)

A. drop
B. priority
C. log
D. pass
E. inspect
F. reset

Correct Answer: ACF
Explanation/Reference:

Question 9
Which two Cisco ASA licensing features are correct with Cisco ASA Software Version 8.3 and later? (Choose two.)

A. Identical licenses are not required on the primary and secondary Cisco ASA appliance.
B. Cisco ASA appliances configured as failover pairs disregard the time-based activation keys.
C. Time-based licenses are stackable in duration but not in capacity.
D. A time-based license completely overrides the permanent license, ignoring all permanently licensed features until the time-based license is uninstalled.

Correct Answer: AC
Explanation/Reference:

Question 10
Which two statements about the process to recover the Cisco ASA software image are true?

The Cisco ASA software image has been erased from flash memory. Which two statements about the process to recover the Cisco ASA software image are true? (Choose two.)

A. Access to the ROM monitor mode is required.
B. The Cisco ASA appliance must have connectivity to the TFTP server where the Cisco ASA image is stored through the Management 0/0 interface.
C. The copy tftp flash command is necessary to start the TFTP file transfer.
D. The server command is necessary to set the TFTP server IP address.
E. Cisco ASA password recovery must be enabled

Correct Answer: AD
Explanation/Reference:

Question 11
On which type of encrypted traffic can a Cisco ASA appliance running software version 8.4.1 perform application inspection and control?

A. IPsec
B. SSL
C. IPsec or SSL
D. Cisco Unified Communications
E. Secure FTP

Correct Answer: D
Explanation/Reference:

Question 12
Which Cisco ASA configuration is used to configure the TCP intercept feature?

A. a TCP map
B. an access list
C. the established command
D. the set connection command with the embryonic-conn-max option
E. a type inspect policy map

Correct Answer: D
Explanation/Reference:
Question 13
Which other match command is used with the match flow ip destination-address command within the class map configurations of the Cisco ASA MPF?
A. match tunnel-group
B. match access-list
C. match default-inspection-traffic
D. match port
E. match dscp
Correct Answer: A
Explanation/Reference:

Question 14
How does a Cisco ASA appliance process IP fragments?
By default, how does a Cisco ASA appliance process IP fragments?
A. Each fragment passes through the Cisco ASA appliance without any inspections.
B. Each fragment is blocked by the Cisco ASA appliance.
C. The Cisco ASA appliance verifies each fragment and performs virtual IP re-assembly before the full IP packet is forwarded out.
D. The Cisco ASA appliance forwards the packet out as soon as all of the fragments of the packet have been received.
Correct Answer: C
Explanation/Reference:

Question 15
Which two statements about the running configuration of the Cisco ASA are true?
Which two statements about the running configuration of the Cisco ASA are true? (Choose Two)
A. The auto NAT configuration causes all traffic arriving on the inside interface destined to any outside destinations to be translated with dynamic port address transmission using the outside interface IP address.
B. The Cisco ASA is using the Cisco ASDM image from disk1:/asdm-642.bin
C. The Cisco ASA is setup as the DHCP server for hosts that are on the inside and outside interfaces.
D. SSH and Cisco ASDM access to the Cisco ASA requires AAA authentication using the LOCAL user database.
E. The Cisco ASA is using a persistent self-signed certified so users can authenticate the Cisco ASA when accessing it via ASDM
Correct Answer: AE
Explanation/Reference:

Question 16
How many monitored interface failures will cause failover to occur?
With Cisco ASA active/standby failover, by default, how many monitored interface failures will cause failover to occur?
A. 1
B. 2
C. 3
D. 4
E. 5
Correct Answer: A
Explanation/Reference:

Question 17
Which of these is true regarding tunnel configuration when deploying a Cisco ISR as a DMVPN hub router?
Which of these is true regarding tunnel configuration when deploying a Cisco ISR as a DMVPN hub router?
A. Only one tunnel can be created per tunnel source interface.
B. Only one tunnel can be created and should be associated with a loopback interface for dynamic redundancy
C. The GRE tunnel key is used to encrypt the traffic going through the tunnel through the hub.
D. You can run multiple parallel DMVPNs on the hub router, but each tunnel requires a unique tunnel key.
Correct Answer: D
Explanation/Reference:

Question 18
Which Cisco IOS feature provides secure, on-demand meshed connectivity?
Which Cisco IOS feature provides secure, on-demand meshed connectivity?
A. Easy VPN
B. IPsec VPN
C. mGRE
D. DMVPN
Correct Answer: D
Explanation/Reference:

Question 19
When you are configuring a DMVPN network, which tunnel mode should you use for the hub router configuration?
When you are configuring a DMVPN network, which tunnel mode should you use for the hub router configuration?
A. GRE multipoint
B. classic point-to-point GRE
C. IPsec multipoint
D. nonbroadcast multiaccess
Correct Answer: A
Explanation/Reference:
Question 20
When implementing GET VPN, which of these is a characteristic of GDOI IKE?
A. GDOI IKE sessions are established between all peers in the network
B. GDOI IKE uses UDP port 500
C. Security associations do not need to linger between members once a group member has authenticated to the key server and obtained the group policy
D. Each pair of peers has a private set of IPsec security associations that is only shared between the two peers
Correct Answer: C
Explanation/Reference:

Question 21
Which two ways can the key server distribute the new keys to the group members during the rekey process?
In a GET VPN solution, which two ways can the key server distribute the new keys to the group members during the rekey process? (Choose two.)
A. multicast UDP transmission
B. multicast TCP transmission
C. unicast UDP transmission
D. unicast TCP transmission
Correct Answer: AC
Explanation/Reference:

Question 22
Which is the GET VPN group member GDOI configuration?
Refer to the exhibit. Based on the partial configuration shown, which is the GET VPN group member GDOI configuration?
```
! crypto gdoi group CLASSROOM
   identity number 12345
! crypto map GETVPN_MAP 10 gdoi
   set group CLASSROOM
   ! interface Serial0/0/0
   ip address 192.168.1.2 255.255.255.252
   crypto map GETVPN_MAP
   ! A. key server IP address
   B. local priority
   C. mapping of the IPsec profile to the IPsec SA
   D. mapping of the IPsec transform set to the GDOI group
```
Correct Answer: A
Explanation/Reference:

Question 23
Which Cisco IOS VPN feature simplifies IPsec VPN configuration and design by using on-demand virtual access interfaces that are cloned from a virtual template configuration?
Which Cisco IOS VPN feature simplifies IPsec VPN configuration and design by using on-demand virtual access interfaces that are cloned from a virtual template configuration?
A. GET VPN
B. dynamic VTI
C. static VTI
D. GRE tunnels
E. GRE over IPsec tunnels
F. DMVPN
Correct Answer: B
Explanation/Reference:

Question 24
Which of these are the two types of keys used when implementing GET VPN?
Which of these are the two types of keys used when implementing GET VPN? (Choose two.)
A. key encryption
B. group encryption
C. pre-shared key
D. public key
E. private key
F. traffic encryption key
Correct Answer: AF
Explanation/Reference:

Question 25
SIMULATION
SIMULATION
Scenario
You are the network security administrator for your organization. Your company is growing and a remote branch office is being created. You are tasked with configuring your headquarters Cisco ASA to create a site-to-site IPsec VPN connection to the branch office Cisco ISR. The branch office ISR has already been deployed and configured and you need to complete the IPsec connectivity configurations on the HQ ASA to bring the new office online.
Use the following parameters to complete your configuration using ASDM. For this exercise, not all ASDM screens are active.
. Enable IKEv1 on outside I/F for Site-to-site VPN
. Add a Connection Profile with the following parameters:

Peer IP: 203.0.113.1
Connection name: 203.0.113.1
Local protected network: 10.10.9.0/24
Remote protected network: 10.11.11.0/24
Group Policy Name: use the default policy name supplied
Preshared key: cisco
Disable IKEv2
Encryption Algorithms: use the ASA defaults
Disable pre-configured NAT for testing of the IPsec tunnel
Disable the outside NAT pool rule
Establish the IPsec tunnel by sending ICMP pings from the Employee PC to the Branch Server at IP address 10.11.11.20
Verify tunnel establishment in ASDM VPN Statistics> Sessions window pane.
You have completed this exercise when you have successfully configured, established, and verified site-to-site IPsec connectivity between the ASA and the Branch ISR.

Topology
This is a pretty simple website.

Navigate, explore, experiment!

Original XAMPP Sample Pages

---


dhttp://www.aoowe.com/practice-300-209-3147.html

dhttp://www.aoowe.com/practice-300-209-3147.html

dhttp://www.aoowe.com/
Correct Answer: Review the explanation for detailed answer steps.
Explanation/Reference:
Explanation:
First, click on Configuration -> Site-to-Site VPN to bring up this screen:
Click on “allow IKE v1 Access” for the outside per the instructions as shown below:

Then click apply at the bottom of the page. This will bring up the following pop up message:
Click on Send.
Next, we need to set up the connection profile. From the connection profile tab, click on “Add.”
Then, fill in the information per the instructions as shown below:
Hit OK and you should see this:
To test this, we need to disable NAT. Go to Configuration -> Firewall -> NAT rules and you should see this:
Click on Rule 1 to get the details and you will see this:
We need to uncheck the “Enable rule” button on the bottom. It might also be a good idea to uncheck the “Translate DNS replies that match the rule” but it should not be needed.

Then, go back to the topology:
Click on Employee PC, and you will see a desktop with a command prompt shortcut. Use this to ping the IP address of 10.11.20 and you should see replies:
We can also verify by viewing the VPN Statistics -> Sessions and see the bytes in/out incrementing as shown below:
**Question 26**

Which two networks will be included in the secured VPN tunnel?

**Scenario**

Your organization has just implemented a Cisco AnyConnect SSL VPN solution. Using Cisco ASDM, answer the questions regarding the implementation.

**Note:** Not all screens or option selections are active for this exercise.
Topology

DMZ Network

AnyConnect Client User

Default_Home


http://www.aoowe.com/
Which two networks will be included in the secured VPN tunnel? (Choose two.)

A. 10.10.0.0/16
B. All networks will be securely tunneled
C. Networks with a source of any4
D. 10.10.9.0/24
E. DMZ network

Correct Answer: AE

Explanation/Reference:
Navigate to the Configuration -> Remote Access -> Group Policies tab to observe the following:

Then, click on the DfltGrpPolicy to see the following:
On the left side, select “Split Tunneling” to get to this page:

Here you see that the Network List called “Inside Subnets” is being tunneled (secured). Select Manage to see the list of networks.

Here we see that the 10.10.0.0/16 and DMZ networks are being secured over the tunnel.

Question 27
What two actions will be taken on translated packets when the AnyConnect users connect to the ASA?

Scenario
Your organization has just implemented a Cisco AnyConnect SSL VPN solution. Using Cisco ASDM, answer the questions regarding the implementation.

Note: Not all screens or option selections are active for this exercise.
What is Network (Client) Access?

After a VPN client, such as AnyConnect, is successfully authenticated, remote users can access corporate network and applications as if they were onsite. The data traffic between remote users and the corporate network is encrypted by being encrypted when going through the Internet.

The ASDM Assistant provides a "Walkthrough" help for configuring Network (Client) Access.

Important Concepts:

1. SSL tunnel and EAP tunnel:

They are two different types to encrypt data traffic. An SSL tunnel uses SSL protocol to encrypt data, while an EAP tunnel uses EAP protocol. Cisco AnyConnect VPN client supports both SSL and EAP (EAP-TLS) protocols. Cisco AnyConnect client supports only EAP (EAP-TLS) protocol.

2. User and connection profiles:

To access corporate network resources, remote users must authenticate and identify which Connection Profile (Tunnel Group) to use. This connection profile specifies how the security appliance authenticates users.

You configure user databases in AAA Local Users.

You configure AnyConnect connection profile in AnyConnect Connection Profiles. EAP connection profile is [EAP(TLS)] Connection Profiles.

3. Access Policy:

Access policies control how remote users can access corporate networks. An access policy includes the following:

- Session control: How long a session can remain idle before it is closed.
- Endpoint security: Determines the conditions that remote PCs must satisfy to connect, for example, requiring up-to-date anti-virus software.

You configure access policies in Dynamic Access Policies or Group Policies.

You configure endpoint security policies in Secure Desktop Manager. You also have the option to set up ACB based endpoint security policies.
Manage WPA group policies. A WPA group is a collection of user-oriented authentication attribute/value pairs that may be stored internally on the device or externally on a NAD/SSODAP server. The group policy information is referenced by WPA connection profiles and user accounts.

To enforce authentication attributes from an LDAP server you must use an LDAP attribute map.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Tunneling Protocol</th>
<th>Connection Profiles Assigned To</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroupPolicy1</td>
<td>Internal</td>
<td>L2TP</td>
<td>203.0.113.1</td>
</tr>
<tr>
<td>GroupPolicy2</td>
<td>Internal</td>
<td>L2TP</td>
<td></td>
</tr>
</tbody>
</table>

Default Policy (System Default): Internal

Banner: Inherit
Address Policies: Inherit
IPsec Address Policies: Inherit

More Options

What two actions will be taken on translated packets when the AnyConnect users connect to the ASA? (Choose two.)

A. No action will be taken, they will keep their original assigned addresses
B. The source address will use the outside-nat-pool
C. The source NAT type will be a static translation
D. The source NAT type will be a dynamic translation
E. DNS will be translated on rule matches

Correct Answer: AC

Explanation/Reference:
First, navigate to the Configuration -> NAT Rules tab to see this:

Here we see that NAT rule 2 applies to the AnyConnect clients, click on this rule for more details to see the following:

Here we see that it is a static source NAT entry, but that the Source and Destination addresses remain the original IP address so they are not translated.

Question 28
Which address range will be assigned to the AnyConnect users?

Scenario
Your organization has just implemented a Cisco AnyConnect SSL VPN solution. Using Cisco ASDM, answer the questions regarding the implementation.
Note: Not all screens or option selections are active for this exercise.
300-209 197 Questions Implementing Cisco Secure Mobility Solutions (SIMOS)


http://www.aoowe.com/
Which address range will be assigned to the AnyConnect users?
A. 10.10.15.40-50/24
B. 209.165.201.20-30/24
C. 192.168.1.100-150/24
D. 10.10.15.20-30/24

Correct Answer: D
Explanation/Reference:
First Navigate to the Configuration -> Remote Access VPN tab and then choose the “AnyConnect Connection Profile as shown below:

Then, clicking on the AnyConnect Profile at the bottom will bring you to the edit page shown below:
From here, click the Select button on the “VPN_Address_Pool” and you will see the following pools defined:

Here we see that the VPN_Address_Pool contains the IP address range of 10.10.15.20-10.10.15.30/24.

**Question 29**
Which technology can you implement to reduce latency issues associated with a Cisco AnyConnect VPN?

A. DTLS  
B. SCTP  
C. DCCP  
D. SRTP

Correct Answer: A

**Question 30**
Which option is a required element of Secure Device Provisioning communications?
Which option is a required element of Secure Device Provisioning communications?
A. the introducer
B. the certificate authority
C. the requestor
D. the registration authority

Correct Answer: A
Explanation/Reference:

Question 31
Which option is one component of a Public Key Infrastructure?
A. the Registration Authority
B. Active Directory
C. RADIUS
D. TACACS+

Correct Answer: A
Explanation/Reference:

Question 32
Which three parameters are specified in the isakmp (IKEv1) policy?
A. the hashing algorithm
B. the authentication method
C. the lifetime
D. the session key
E. the transform-set
F. the peer

Correct Answer: ABC
Explanation/Reference:

Question 33
Which option is an example of an asymmetric algorithm?
A. 3DES
B. IDEA
C. AES
D. RSA

Correct Answer: D
Explanation/Reference:

Question 34
Which option is most effective at preventing a remote access VPN user from bypassing the corporate transparent web proxy?
A. using the proxy-server settings of the client computer to specify a PAC file for the client computer to download
B. instructing users to use the corporate proxy server for all web browsing
C. disabling split tunneling
D. permitting local LAN access

Correct Answer: C
Explanation/Reference:

Question 35
Which VPN feature allows remote access clients to print documents to local network printers?
A. Reverse Route Injection
B. split tunneling
C. loopback addressing
D. dynamic virtual tunnels

Correct Answer: B
Explanation/Reference:

Question 36
What must be enabled in the web browser of the client computer to support Clientless SSL VPN?
A. cookies
B. ActiveX
C. Silverlight
D. popups

Correct Answer: A
Explanation/Reference:

Question 37
Which VPN solution does this configuration represent?
Refer to the exhibit.
Which VPN solution does this configuration represent?
A. Cisco AnyConnect (IKEv2)
B. site-to-site
C. DMVPN
D. SSL VPN

Correct Answer: D
Explanation/Reference:

**Question 38**
Which VPN type can be used to provide secure remote access from public internet cafes and airport kiosks?
A. site-to-site
B. business-to-business
C. Clientless SSL
D. DMVPN

Correct Answer: C
Explanation/Reference:

**Question 39**
Which VPN solution does this configuration represent?
Refer to the exhibit.

Which VPN solution does this configuration represent?
A. DMVPN
B. GETVPN
C. FlexVPN
D. site-to-site

Correct Answer: B
Explanation/Reference:

**Question 40**
Which feature do you include in a highly available system to account for potential site failures?
A. geographical separation of redundant devices
B. hot/standby failover pairs
C. Cisco ACE load-balancing with VIP
D. dual power supplies

Correct Answer: A
Explanation/Reference:

**Question 41**
Which action must you take to correct the problem?
You have deployed new Cisco AnyConnect start before logon modules and set the configuration to download modules before logon, but all client connections continue to use the previous version of the module. Which action must you take to correct the problem?
A. Configure start before logon in the client profile.
B. Configure a group policy to prompt the user to download the updated module.
C. Define the modules for download in the client profile.
D. Define the modules for download in the group policy.
**Question 42**
Which group-policy subcommand installs the Diagnostic AnyConnect Report Tool on user computers when a Cisco AnyConnect user logs in?

A. customization value dart  
B. file-browsing enable  
C. smart-tunnel enable dart  
D. anyconnect module value dart

Correct Answer: D

**Explanation/Reference:**

**Question 43**
Which command clears all Cisco AnyConnect VPN sessions?

A. vpn-sessiondb logoff anyconnect  
B. vpn-sessiondb logoff webvpn  
C. vpn-sessiondb logoff l2l  
D. clear crypto isakmp sa

Correct Answer: A

**Explanation/Reference:**

**Question 44**
Which action should you take to begin troubleshooting?

If Web VPN bookmarks are grayed out on the home screen, which action should you take to begin troubleshooting?

A. Determine whether the Cisco ASA can resolve the DNS names.  
B. Determine whether the Cisco ASA has DNS forwarders set up.  
C. Determine whether an ACL is present to permit DNS forwarding.  
D. Replace the DNS name with an IP address.

Correct Answer: A

**Explanation/Reference:**

**Question 45**
What URL do you use to download a packet capture file in a format which can be used by a packet analyzer?

What URL do you use to download a packet capture file in a format which can be used by a packet analyzer?

A. ftp:///capture/  
B. https:///  
C. https:///admin/capture//pcap  
D. https:///pcap

Correct Answer: C

**Explanation/Reference:**

**Question 46**
When you troubleshoot Cisco AnyConnect, which step does Cisco recommend before you open a TAC case?

When you troubleshoot Cisco AnyConnect, which step does Cisco recommend before you open a TAC case?

A. Show applet Lifecycle exceptions.  
B. Disable cookies.  
C. Enable the WebVPN cache.  
D. Collect a DART bundle.

Correct Answer: D

**Explanation/Reference:**

**Question 47**
Which functionality is provided by L2TPv3 over FlexVPN?

Which functionality is provided by L2TPv3 over FlexVPN?

A. the extension of a Layer 2 domain across the FlexVPN  
B. the extension of a Layer 3 domain across the FlexVPN  
C. secure communication between servers on the FlexVPN  
D. a secure backdoor for remote access users through the FlexVPN

Correct Answer: A

**Explanation/Reference:**

**Question 48**
Which two RADIUS attributes are needed for a VRF-aware FlexVPN hub?

Which two RADIUS attributes are needed for a VRF-aware FlexVPN hub? (Choose two.)

A. ip:interface-config=ip unnumbered looback  
B. ip:interface-config=ip vrf forwarding ivrf  
C. ip:interface-config=ip vrf route  
D. ip:interface-config=ip next hop  
E. ip:interface-config=ip neighbor 0.0.0.0

Correct Answer: AB

**Explanation/Reference:**
Question 49
Which option describes the purpose of the command show derived-config interface virtual-access 1?
A. It verifies that the virtual access interface is cloned correctly with per-user attributes.
B. It verifies that the virtual template created the tunnel interface.
C. It verifies that the virtual access interface is of type Ethernet.
D. It verifies that the virtual access interface is used to create the tunnel interface.

Correct Answer: A
Explanation/Reference:

Question 50
Which action is demonstrated by this debug output?
Refer to the exhibit.

Which action is demonstrated by this debug output?
A. NHRP initial registration by a spoke.
B. NHRP registration acknowledgement by the hub.
C. Disabling of the DMVPN tunnel interface.
D. IPsec ISAKMP phase 1 negotiation.

Correct Answer: A
Explanation/Reference:

Question 51
Which three commands are included in the command show dmvpn detail?
(Choose three.)
A. show ip nhrp nhs
B. show crypto session detail
C. show crypto ipsec sa detail
D. show crypto sockets
E. show ip nhrp

Correct Answer: ABC
Explanation/Reference:

Question 52
What is the purpose of the given configuration?
Refer to the exhibit.

What is the purpose of the given configuration?
A. Establishing a GRE tunnel.
B. Enabling IPsec to decrypt fragmented packets.
C. Resolving access issues caused by large packet sizes.
D. Adding the spoke to the routing table.

Correct Answer: C
Explanation/Reference:

Question 53
Which command can you use to view request counters?
You are troubleshooting a DMVPN NHRP registration failure. Which command can you use to view request counters?
A. show ip nhrp nhs detail
B. show ip nhrp tunnel
C. show ip nhrp incomplete
D. show ip nhrp incomplete tunnel_interface_number

Correct Answer: A
Explanation/Reference:

Question 54
Which interface is managed by the VPN Access Interface field in the Cisco ASDM IPsec Site-to-Site VPN Wizard?
Which interface is managed by the VPN Access Interface field in the Cisco ASDM IPsec Site-to-Site VPN Wizard?
A. the local interface named “VPN_access”
B. the local interface configured with crypto enable
C. the local interface from which traffic originates
D. the remote interface with security level 0

Correct Answer: B
Explanation/Reference:

Question 55
Which command can you use to monitor the phase 1 establishment of a FlexVPN tunnel?
Which command can you use to monitor the phase 1 establishment of a FlexVPN tunnel?
A. show crypto ipsec sa
B. show crypto isakmp sa
C. show crypto ikev2 sa
D. show ip nhrp

Correct Answer: C

Explanation/Reference:

**Question 56**
Which technology is represented by this configuration?
Refer to the exhibit.

Which technology is represented by this configuration?
A. AAA for FlexVPN
B. AAA for EzVPN
C. TACACS+ command authorization
D. local command authorization

Correct Answer: A

Explanation/Reference:

**Question 57**
Which statement about the hub in a DMVPN configuration with iBGP is true?
Which statement about the hub in a DMVPN configuration with iBGP is true?
A. It must be a route reflector client.
B. It must redistribute EIGRP from the spokes.
C. It must be in a different AS.
D. It must be a route reflector.

Correct Answer: D

Explanation/Reference:

**Question 58**
Which feature is enabled by the use of NHRP in a DMVPN network?
Which feature is enabled by the use of NHRP in a DMVPN network?
A. host routing with Reverse Route Injection
B. BGP multiaccess
C. host to NBMA resolution
D. EIGRP redistribution

Correct Answer: C

Explanation/Reference:

**Question 59**
Which feature is available in IKEv1 but not IKEv2?
Which feature is available in IKEv1 but not IKEv2?
A. Layer 3 roaming
B. aggressive mode
C. EAP variants
D. sequencing

Correct Answer: B

Explanation/Reference:

**Question 60**
Which option describes what address preservation with IPsec Tunnel Mode allows when GETVPN is used?
Which option describes what address preservation with IPsec Tunnel Mode allows when GETVPN is used?
A. stronger encryption methods
B. Network Address Translation of encrypted traffic
C. traffic management based on original source and destination addresses
D. Tunnel Endpoint Discovery

Correct Answer: C

Explanation/Reference:

**Question 61**
Which crypto map tag is being used on the Cisco ASA?

Scenario:
You are the senior network security administrator for your organization. Recently and junior engineer configured a site-to-site IPsec VPN connection between your headquarters Cisco ASA and a remote branch office.
You are now tasked with verifying the IKEv1 IPsec installation to ensure it was properly configured according to designated parameters. Using the CLI on both the Cisco ASA and branch ISR, verify the IPsec configuration is properly configured between the two sites.

NOTE: the show running-config command cannot be used for this exercise.

Topology:
Which crypto map tag is being used on the Cisco ASA?
Question 62

In what state is the IKE security association in on the Cisco ASA?

Scenario:

You are the senior network security administrator for your organization. Recently and junior engineer configured a site-to-site IPsec VPN connection between your headquarters Cisco ASA and a remote branch office. You are now tasked with verifying the IKEv1 IPsec installation to ensure it was properly configured according to designated parameters. Using the CLI on both the Cisco ASA and branch ISR, verify the IPsec configuration is properly configured between the two sites.

NOTE: The show running-config command cannot be used for this exercise.

Topology:

```
ASA
ASA#sh crypto ipsec sa
interface: outside
  Crypto map tag: outside_map1, seq num: 1, local addr: 192.0.2.1
    access-list outside_cryptomap extended permit ip 10.10.9.0 255.255.255.0
    0.11.11.0 255.255.255.0
    local ident (addr/mask/prot/port): (10.10.9.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (10.11.11.0/255.255.255.0/0/0)
    current_peer: 203.0.113.1
    #pkts encaps: 15, #pkts encrypt: 15, #pkts digest: 15
    #pkts decaps: 16, #pkts decrypt: 16, #pkts verify: 16
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 15, #pkts comp failed: 0, #pkts dcomp failed: 0
    #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
    #FMTUs sent: 0, #FMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
    #TFC rcvd: 0, #TFC sent: 0
    #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
    #send errors: 0, #recv errors: 0
    local crypto endpt.: 192.0.2.1/0, remote crypto endpt.: 203.0.113.1/0
    path mtu 1500, ipsec overhead 58(36), media mtu 1500
    FMTU time remaining (sec): 0, DF policy: copy-df
    ICMP error validation: disabled, TFC packets: disabled
```
In what state is the IKE security association in on the Cisco ASA?
A. There are no security associations in place
B. MM_ACTIVE
C. ACTIVE/ACTIVE
D. QM_IDLE

Correct Answer: B

Explanation/Reference:
This can be seen from the “show crypto isa sa” command:

```
ASA# show crypto isa sa
IKEv1 SAs:
Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 203.0.113.1
  Type : L2L       Role : responder
  Rekey : no       State : MM_ACTIVE

There are no IKEv2 SAs
```

Question 63
Which transform set is being used on the branch ISR?

Scenario:
You are the senior network security administrator for your organization. Recently and junior engineer configured a site-to-site IPsec VPN connection between your headquarters Cisco ASA and a remote branch office.
You are now tasked with verifying the IKEv1 IPsec installation to ensure it was properly configured according to designated parameters. Using the CLI on both the Cisco ASA and branch ISR, verify the IPsec configuration is properly configured between the two sites.

NOTE: the show running-config command cannot be used for this exercise.

Topology:
Which transform set is being used on the branch ISR?
A. Default
B. ESP-3DES ESP-SHA-HMAC
C. ESP-AES-256-MD5-TRANS mode transport
D. TSET

Correct Answer: B

Explanation/Reference:
This can be seen from the "show crypto ipsec sa" command as shown below:

```
Branch ISR

Branch ISR#show crypto ipsec sa
interface: GigabitEthernet0/1
Crypto map tag: VPNeto-ASA, local addr 203.0.113.1

protected vrf: (none)
local ident (addr/mask/prot/port): [10.11.11.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): [10.10.9.0/255.255.255.0/0/0)
current_peer 192.0.2.1 port 500
PERMIT, flags=(origin_is_acl)
#pkts encaps: 569, #pkts encrypt: 569, #pkts digest: 569
#pkts decaps: 681, #pkts decrypt: 681, #pkts verify: 681
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 203.0.113.1, remote crypto endpt.: 192.0.2.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
current outbound spi: 0x8E47598C(2387040652)
FIPS (Y/N): N, FIPS group: none

inbound esp sas:
spi: 0xCE89192A(3465091370)
transform: esp-3des esp-sha-hmac ,
```
Question 64
What is being used as the authentication method on the branch ISR?

Scenario:
You are the senior network security administrator for your organization. Recently and junior engineer configured a site-to-site IPsec VPN connection between your headquarters Cisco ASA and a remote branch office.
You are now tasked with verifying the IKEv1 IPsec installation to ensure it was properly configured according to designated parameters. Using the CLI on both the Cisco ASA and branch ISR, verify the IPsec configuration is properly configured between the two sites.
NOTE: the show running-config command cannot be used for this exercise.

Topology:

![Topology Diagram](image)

Branch ISR

protected vrf: (none)
local ident (addr/mask/prot/port): (10.11.11.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.10.0.0/255.255.255.0/0/0)
current_peer 192.0.2.1 port 500
   PERMIT, flags={origin_is_acl,}
   #pks encaps: 569, #pks encrypt: 569, #pks digest: 569
   #pks decaps: 681, #pks decrypt: 681, #pks verify: 681
   #pks compressed: 0, #pks decompressed: 0
   #pks not compressed: 0, #pks compr. failed: 0
   #send errors 0, #recv errors 0

local crypto endpt.: 203.0.113.1, remote crypto endpt.: 192.0.2.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
current outbound spi: 0x8E47598C(2387040652)
FSS (Y/N): N, DH group: none

inbound esp sas:
   spi: 0xCE89129A(3465053070)
   transform: esp-3des esp-sha-hmac
   in use settings ={Tunnel, }

Branch ISR#
Branch ISR#
What is being used as the authentication method on the branch ISR?
A. Certificates  
B. Pre-shared keys  
C. RSA public keys  
D. Diffie-Hellman Group 2

Correct Answer: B

Explanation/Reference:
The show crypto isakmp key command shows the preshared key of “cisco”.

Question 65
SIMULATION

Scenario:
You are the network security manager for your organization. Your manager has received a request to allow an external user to access to your HQ and DM2 servers.

You are given the following connection parameters for this task.

Using ASDM on the ASA, configure the parameters below and test your configuration by accessing the Guest PC. Not all AS DM screens are active for this exercise.

Also, for this exercise, all changes are automatically applied to the ASA and you will not have to click APPLY to apply the changes manually.

1. Enable Clientless SSL VPN on the outside interface
2. Using the Guest PC, open an Internet Explorer window and test and verify the basic connection to the SSL VPN portal using address: https://vpn-secure-x.public
3. a. You may notice a certificate error in the status bar, this can be ignored for this exercise
   b. Username: vpnuser
   c. Password: cisco123
   d. Logout of the portal once you have verified connectivity

Configure two bookmarks with the following parameters:

a. Bookmark List Name: MY-BOOKMARKS
b. Use the: URL with GET or POST method
c. Bookmark Title: HQ-Server
   i. http://10.10.3.20

d. Bookmark Title: DMZ-Server-FTP
   i. ftp://172.16.1.50

Assign the configured Bookmarks to:
- DfltGrpPolicy
- DfltAccessPolicy
- LOCAL User: vpnuser

From the Guest PC, reconnect to the SSL VPN Portal

Test both configured Bookmarks to ensure desired connectivity

You have completed this exercise when you have configured and successfully tested Clientless SSL VPN connectivity.

Topology:
Correct Answer: Please find the solution in below explanation
Explanation/Reference:

First, enable clientless VPN access on the outside interface by checking the box found below:

Then, login to the given URL using the vpnuser/cisco123 credentials:
Logging in will take you to this page, which means you have now verified basic connectivity:

Now log out by hitting the logout button.
Now, go back to the ASDM and navigate to the Bookmarks portion:
Make the name MY-BOOKMARKS and use the "Add" tab and add the bookmarks per the instructions:

Ensure the "URL with GET or POST method" button is selected and hit OK.
Add the two bookmarks as given in the instructions:

Bookmark Title: HQ-Server
URL: http://10.10.3.20

Preload Page (optional)
Preload URL: http://
Wait Time: (seconds)

Other Settings (optional)
Title:
Thumbnail: None

Place this bookmark on the VPN home page
Enable Smart Tunnel

Advanced Options

You should now see the two bookmarks listed:

**Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks**

Configure Bookmark Lists that the security appliance displays on the SSL VPN portal page.

This parameter is enforced in either a VPN group policy, a dynamic access policy, or a user policy configuration. You can click on Assign button to assign the selected one to them.
Select the MY-BOOKMARKS Bookmarks and click on the "Assign" button. Then, click on the appropriate check boxes as specified in the instructions and hit OK. After hitting OK, you will now see this:
Then, go back to the Guest-PC, log back in and you should be able to test out the two new bookmarks.

Question 66
Which protocol does DTLS use for its transport?
A. TCP
B. UDP
C. IMAP
D. DDE
Correct Answer: B
Explanation/Reference:

Question 67
Which two technologies are considered to be Suite B cryptography?
A. MD5
B. SHA2
C. Elliptical Curve Diffie-Hellman
D. 3DES
E. DES
Correct Answer: BC
Explanation/Reference:

Question 68
Which exchange does this debug output represent?
Refer to the exhibit.

Which exchange does this debug output represent?
A. IKE Phase 1
B. IKE Phase 2
C. symmetric key exchange
D. certificate exchange
Correct Answer: A
Explanation/Reference:

Question 69
Which type of key is the shared secret?
In the Diffie-Hellman protocol, which type of key is the shared secret?
A. a symmetric key
B. an asymmetric key
C. a decryption key
D. an encryption key

Correct Answer: A

Question 70
Which technology must be installed on the client computer to enable users to launch applications from a Clientless SSL VPN?

Which technology must be installed on the client computer to enable users to launch applications from a Clientless SSL VPN?

A. Java
B. QuickTime plug-in
C. Silverlight
D. Flash

Correct Answer: A

Question 71
Which VPN solution does this configuration represent?

Refer to the exhibit.

Which VPN solution does this configuration represent?

A. Cisco AnyConnect
B. IPsec
C. L2TP
D. SSL VPN

Correct Answer: B

Question 72
Which technology can provide high availability for an SSL VPN?

Which technology can provide high availability for an SSL VPN?

A. DMVPN
B. a multiple-tunnel configuration
C. a Cisco ASA pair in active/passive failover configuration
D. certificate to tunnel group maps

Correct Answer: C

Question 73
Which type of communication takes place between the secure gateway R1 and the Cisco Secure ACS?

Refer to the exhibit.

You have implemented an SSL VPN as shown. Which type of communication takes place between the secure gateway R1 and the Cisco Secure ACS?

A. HTTP proxy
B. AAA
C. policy
D. port forwarding
Question 74
Which VPN solution does this configuration represent?
Refer to the exhibit.

```
crypto iskev2 proposal PRoDP
  encryption aes-cbc-128
  integrity sha256
  group 20

crypto iskev2 policy ISKEv2_POLICY
  match address local 10.1.1.2
  proposal PRoDP

crypto iskev2 keyring KEYRING
  peer spokes
  address 10.0.0.0 255.0.0.0
  pre-shared-key local cisco123

crypto iskev2 profile PROFILE_ISKEV2
  match identity remote address 10.0.0.0 255.0.0.0
  authentication remote pre-share
  authentication local pre-share
  keyring local KEYRING
  aaa authorization group psk list default default
  virtual-template 1

crypto iskev2 dpd 10 5 on-demand

crypto ipsec transform-set TRANSFORM_IPSEC esp-gcm
  mode transport

  crypto ipsec profile PROFILE_IPSEC
  set transform-set TRANSFORM_IPSEC
  set iskev2-profile PROFILE_ISKEV2

  interface Virtual-Template type tunnel
  ip unnumbered Loopback100
  tunnel path-mtu-discovery
  tunnel protection ipsec profile PROFILE_IPSEC
```

Which VPN solution does this configuration represent?
A. DMVPN
B. GETVPN
C. FlexVPN
D. site-to-site

Correct Answer: C

Explanation/Reference:

Question 75
Which VPN solution is best for a collection of branch offices connected by MPLS that frequently make VoIP calls between branches?

Which VPN solution is best for a collection of branch offices connected by MPLS that frequently make VoIP calls between branches?
A. GETVPN
B. Cisco AnyConnect
C. site-to-site
D. DMVPN

Correct Answer: A

Explanation/Reference:

Question 76
Which is used by GETVPN, FlexVPN and DMVPN?

Which is used by GETVPN, FlexVPN and DMVPN?
A. NHRP
B. MPLS
C. GRE
D. ESP

Correct Answer: D

Explanation/Reference:

Question 77
Which protocols does the Cisco AnyConnect client use to build multiple connections to the security appliance?

Which protocols does the Cisco AnyConnect client use to build multiple connections to the security appliance?
A. TLS and DTLS
B. IKEv1
C. L2TP over IPsec
D. SSH over TCP

Correct Answer: A

Explanation/Reference:

Question 78
Where do you configure AnyConnect certificate-based authentication in ASDM?

Where do you configure AnyConnect certificate-based authentication in ASDM?
A. group policies
B. AnyConnect Connection Profile
C. AnyConnect Client Profile
D. Advanced Network (Client) Access

Correct Answer: B
Explanation/Reference:

**Question 79**
Which application does the Application Access feature of Clientless VPN support?
A. TFTP
B. VoIP
C. Telnet
D. active FTP

Correct Answer: C
Explanation/Reference:

**Question 80**
Which technology is FlexVPN based on?
A. OER
B. VRF
C. IKEv2
D. an RSA nonce

Correct Answer: C
Explanation/Reference:

**Question 81**
Which type of communication in a FlexVPN implementation uses an NHRP shortcut?
A. spoke to hub
B. spoke to spoke
C. hub to spoke
D. hub to hub

Correct Answer: B
Explanation/Reference:

**Question 82**
Which option describes the purpose of the shared argument in the DMVPN interface command tunnel protection IPsec profile ProfileName shared?
A. shares a single profile between multiple tunnel interfaces
B. allows multiple authentication types to be used on the tunnel interface
C. shares a single profile between a tunnel interface and a crypto map
D. shares a single profile between IKEv1 and IKEv2

Correct Answer: A
Explanation/Reference:

**Question 83**
Which two types of authentication are supported when you use Cisco ASDM to configure site-to-site IKEv2 with IPv6? (Choose two.)
A. preshared key
B. webAuth
C. digital certificates
D. XAUTH
E. EAP

Correct Answer: AC
Explanation/Reference:

**Question 84**
Which statement about the given IKE policy is true?
Refer to the exhibit.

```
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 14463, #pkts decrypt: 14463, #pkts verify: 14463
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

You executed the show crypto ipsec sa command to troubleshoot an IPsec issue. What problem does the given output indicate?
A. IKEv2 failed to establish a phase 2 negotiation.
B. The Crypto ACL is different on the peer device.
C. ISAKMP was unable to find a matching SA.
D. IKEv2 was used in aggressive mode.
Correct Answer: B
Explanation/Reference:

Question 85
In which situation would you enable the Smart Tunnel option with clientless SSL VPN?
A. when a user is using an outdated version of a web browser
B. when an application is failing in the rewrite process
C. when IPsec should be used over SSL VPN
D. when a user has a nonsupported Java version installed
E. when cookies are disabled

Correct Answer: B
Explanation/Reference:

Question 86
Which feature enforces the corporate policy for Internet access to Cisco AnyConnect VPN users?
A. Trusted Network Detection
B. Datagram Transport Layer Security
C. Cisco AnyConnect Customization
D. banner message

Correct Answer: A
Explanation/Reference:

Question 87
Which command enables the router to form EIGRP neighbor adjacencies with peers using a different subnet than the ingress interface?
A. ip unnumbered interface
B. eigrp router-id
C. passive-interface interface name
D. ip split-horizon eigrp as number

Correct Answer: A
Explanation/Reference:

Question 88
What technology does the given configuration demonstrate?
Refer to the exhibit.

A. Keyring used to encrypt IPSec traffic
B. FlexVPN with IPV6
C. FlexVPN with AnyConnect
D. Crypto Policy to enable IKEv2

Correct Answer: B
Explanation/Reference:

Question 89
Which two statements about the given configuration are true?
Refer to the exhibit.

A. Defined PSK can be used by any IPSec peer.
B. Any router defined in group 2 will be allowed to connect.
C. It can be used in a DMVPN deployment
D. It is a LAN-to-LAN VPN ISAKMP policy.
E. It is an AnyConnect ISAKMP policy.
F. PSK will not work as configured

Correct Answer: AC
Explanation/Reference:

Question 90
Which statement about the given IKE policy is true?
Refer to the exhibit.

Which statement about the given IKE policy is true?
A. The tunnel will be valid for 2 days, 88 minutes, and 00 seconds.
B. It will use encrypted nonces for authentication.
C. It has a keepalive of 60 minutes, checking every 5 minutes.
D. It uses a 56-bit encryption algorithm.
Correct Answer: B
Explanation/Reference:

**Question 91**
On which Cisco platform are dynamic virtual template interfaces available?
A. Cisco Adaptive Security Appliance 5585-X
B. Cisco Catalyst 3750X
C. Cisco Integrated Services Router Generation 2
D. Cisco Nexus 7000
Correct Answer: C
Explanation/Reference:

**Question 92**
Which command is used to determine how many GMs have registered in a GETVPN environment?
A. show crypto isakmp sa
B. show crypto gdoi ks members
C. show crypto gdoi gm
D. show crypto ipsec sa
E. show crypto isakmp sa count
Correct Answer: B
Explanation/Reference:

**Question 93**
Which option outlines the steps required to allow users access via the ASA clientless VPN portal?
Remote users want to access internal servers behind an ASA using Microsoft terminal services. Which option outlines the steps required to allow users access via the ASA clientless VPN portal?
A. 1. Configure a static pat rule for TCP port 3389
   2. Configure an inbound access-list to allow traffic from remote users to the servers
   3. Assign this access-list rule to the group policy
B. 1. Configure a bookmark of the type http:// server-IP :3389
   2. Enable Smart tunnel on this bookmark
   3. Assign the bookmark to the desired group policy
C. 1. Configure a Smart Tunnel application list
   2. Add the rdp.exe process to this list
   3. Assign the Smart Tunnel application list to the desired group policy
D. 1. Upload an RDP plugin to the ASA
   2. Configure a bookmark of the type rdp:// server-IP
   3. Assign the bookmark list to the desired group policy
Correct Answer: D
Explanation/Reference:

**Question 94**
What additional step is required if the client software fails to load when connecting to the ASA SSL page?
The following configuration steps have been completed:
1. WebVPN was enabled on the ASA outside interface.
2. SSL VPN client software was loaded to the ASA.
3. A DHCP scope was configured and applied to a WebVPN Tunnel Group.
What additional step is required if the client software fails to load when connecting to the ASA SSL page?
A. The SSL client must be loaded to the client by an ASA administrator
B. The SSL client must be downloaded to the client via FTP
C. The SSL VPN client must be enabled on the ASA after loading
D. The SSL client must be enabled on the client machine before loading
Correct Answer: A
Explanation/Reference:

**Question 95**
Where does the administrator configure this?
An administrator desires that when work laptops are not connected to the corporate network, they should automatically initiate an AnyConnect VPN tunnel back to headquarters. Where does the administrator configure this?
A. Via the svc trusted-network command under the group-policy sub-configuration mode on the ASA
B. Under the “Automatic VPN Policy” section inside the Anyconnect Profile Editor within ASDM
C. Under the TNDPolicy XML section within the Local Preferences file on the client computer
Correct Answer: B
Explanation/Reference:
D. Via the svc trusted-network command under the global webvpn sub-configuration mode on the ASA

Correct Answer: B
Explanation/Reference:

**Question 96**
Which Cisco adaptive security appliance command can be used to view the IPsec PSK of a tunnel group in cleartext?

Which Cisco adaptive security appliance command can be used to view the IPsec PSK of a tunnel group in cleartext?
A. more system:running-config
B. show running-config crypto
C. show running-config tunnel-group
D. show running-config tunnel-group-map
E. clear config tunnel-group
F. show ipsec policy

Correct Answer: A
Explanation/Reference:

**Question 97**
Which command clears all crypto configuration from a Cisco Adaptive Security Appliance?

Which command clears all crypto configuration from a Cisco Adaptive Security Appliance?
A. clear configure crypto
B. clear configure crypto ipsec
C. clear crypto map
D. clear crypto ipv2 sa

Correct Answer: A
Explanation/Reference:

**Question 98**
Which transform set is contained in the IKEv2 default proposal?

Which transform set is contained in the IKEv2 default proposal?
A. aes-cbc-192, sha256, group 14
B. 3des, md5, group 7
C. 3des, sha1, group 1
D. aes-cbc-128, sha, group 5

Correct Answer: D
Explanation/Reference:

**Question 99**
Which cryptographic algorithms are a part of the Cisco NGE suite?

Which cryptographic algorithms are a part of the Cisco NGE suite?
A. HIPP DES
B. AES-CBC-128
C. RC4-128
D. AES-GCM-256

Correct Answer: D
Explanation/Reference:
Reference:

**Question 100**
Which option is a possible solution if you cannot access a URL through clientless SSL VPN with Internet Explorer, while other browsers work fine?

Which option is a possible solution if you cannot access a URL through clientless SSL VPN with Internet Explorer, while other browsers work fine?
A. Verify the trusted zone and cookies settings in your browser.
B. Make sure that you specified the URL correctly.
C. Try the URL from another operating system.
D. Move to the IPsec client.

Correct Answer: A
Explanation/Reference:

**Question 101**
Which three commands can be used for troubleshooting of the AAA subsystem?

A user is trying to connect to a Cisco IOS device using clientless SSL VPN and cannot establish the connection. Which three commands can be used for troubleshooting of the AAA subsystem? (Choose three.)
A. debug aaa authentication
B. debug radius
C. debug vpn authorization error
D. debug ssl openssl errors
E. debug webvpn aaa
F. debug ssl error

Correct Answer: ABD
Explanation/Reference:

**Question 102**
When troubleshooting established clientless SSL VPN issues, which three steps should be taken?

When troubleshooting established clientless SSL VPN issues, which three steps should be taken? (Choose three.)
A. Clear the browser history.
B. Clear the browser and Java cache.
C. Collect the information from the computer event log.
D. Enable and use HTML capture tools.
E. Gather crypto debugs on the adaptive security appliance.
F. Use Wireshark to capture network traffic.

Correct Answer: BEF
Explanation/Reference:

Question 103
What does NHRP stand for?
A. Next Hop Resolution Protocol
B. Next Hop Registration Protocol
C. Next Hub Routing Protocol
D. Next Hop Routing Protocol

Correct Answer: A
Explanation/Reference:

Question 104
Which two EIGRP features need to be disabled on the hub to allow spoke-to-spoke communication?
A. autosummary
B. split horizon
C. metric calculation using bandwidth
D. EIGRP address family
E. next-hop-self
F. default administrative distance

Correct Answer: BE
Explanation/Reference:

Question 105
How can you achieve optimum failover without affecting any other router in the DMVPN cloud?
A. Create another DMVPN cloud by configuring another tunnel interface that is sourced from the second ISP link.
B. Use another router at the spoke site, because two ISP connections on the same router for the same hub is not allowed.
C. Configure SLA tracking, and when the primary interface goes down, manually change the tunnel source of the tunnel interface.
D. Create another tunnel interface with same configuration except the tunnel source, and configure the if-state nhrp and backup interface commands on the primary tunnel interface.

Correct Answer: D
Explanation/Reference:

Question 106
What action does the hub take when it receives a NHRP resolution request from a spoke for a network that exists behind another spoke?
A. The hub sends back a resolution reply to the requesting spoke.
B. The hub updates its own NHRP mapping.
C. The hub forwards the request to the destination spoke.
D. The hub waits for the second spoke to send a request so that it can respond to both spokes.

Correct Answer: C
Explanation/Reference:

Question 107
What could cause this issue?
Refer to the exhibit.
The network administrator is adding a new spoke, but the tunnel is not passing traffic. What could cause this issue?

A. DMVPN is a point-to-point tunnel, so there can be only one spoke.
B. There is no EIGRP configuration, and therefore the second tunnel is not working.
C. The NHRP authentication is failing.
D. The transform set must be in transport mode, which is a requirement for DMVPN.
E. The NHRP network ID is incorrect.

Correct Answer: C

Explanation/Reference:

Question 108
Which option will allow IKEv2 connections on the adaptive security appliance?
Regarding licensing, which option will allow IKEv2 connections on the adaptive security appliance?
A. AnyConnect Essentials can be used for Cisco AnyConnect IKEv2 connections.
B. IKEv2 sessions are not licensed.
C. The Advanced Endpoint Assessment license must be installed to allow Cisco AnyConnect IKEv2 sessions.
D. Cisco AnyConnect Mobile must be installed to allow AnyConnect IKEv2 sessions.

Correct Answer: A

Explanation/Reference:
IKEv1 IPsec sessions are not licensed, and the maximum number of sessions available equal the maximum number available for the ASA platform used. IKEv2 site-to-site VPNs are not licensed either.
IKEv2 IPsec remote-access VPN sessions are available for use only with the AnyConnect client and as such are licensed using the same AnyConnect Essentials or AnyConnect Premium licenses used with SSL VPNs.

Question 109
Which two troubleshooting steps should be taken when Cisco AnyConnect cannot establish an IKEv2 connection, while SSL works fine?
Which two troubleshooting steps should be taken when Cisco AnyConnect cannot establish an IKEv2 connection, while SSL works fine? (Choose two.)
A. Verify that the primary protocol on the client machine is set to IPsec.
B. Verify that AnyConnect is enabled on the correct interface.
C. Verify that the IKEv2 protocol is enabled on the group policy.
D. Verify that ASDM and AnyConnect are not using the same port.
E. Verify that SSL and IKEv2 certificates are not referencing the same trustpoint.

Correct Answer: AC

Explanation/Reference:

Question 110
What is the most likely cause of this problem?
The Cisco AnyConnect client is unable to download an updated user profile from the ASA headend using IKEv2. What is the most likely cause of this problem?
A. User profile updates are not allowed with IKEv2.
B. IKEv2 is not enabled on the group policy.
C. A new profile must be created so that the adaptive security appliance can push it to the client on the next connection attempt.
D. Client Services is not enabled on the adaptive security appliance.

Correct Answer: D
Explanation/Reference:

**Question 111**
What is the most possible cause of this problem?
The Cisco AnyConnect client fails to connect via IKEv2 but works with SSL. The following error message is displayed:
“Login Denied, unauthorized connection mechanism, contact your administrator”

What is the most possible cause of this problem?
A. DAP is terminating the connection because IKEv2 is the protocol that is being used.
B. The client endpoint does not have the correct user profile to initiate an IKEv2 connection.
C. The AAA server that is being used does not authorize IKEv2 as the connection mechanism.
D. The administrator is restricting access to this specific user.
E. The IKEv2 protocol is not enabled in the group policy of the VPN headend.

Correct Answer: E
Explanation/Reference:

**Question 112**
What is the problem?
Refer to the exhibit.

An administrator had the above configuration working with SSL protocol, but as soon as the administrator specified IPsec as the primary protocol, the Cisco AnyConnect client was not able to connect. What is the problem?
A. IPsec will not work in conjunction with a group URL.
B. The Cisco AnyConnect implementation does not allow the two group URLs to be the same. SSL does allow this.
C. If you specify the primary protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group).
D. A new XML profile should be created instead of modifying the existing profile, so that the clients force the update.

Correct Answer: C
Explanation/Reference:

**Question 113**
Which Cisco adaptive security appliance command can be used to view the count of all active VPN sessions?

Which Cisco adaptive security appliance command can be used to view the count of all active VPN sessions?
A. show vpn-sessiondb summary
B. show crypto ikev1 sa
C. show vpn-sessiondb ratio encryption
D. show iskamp sa detail
E. show crypto protocol statistics all

Correct Answer: A
Explanation/Reference:

**Question 114**
What does this output suggest?
After completing a site-to-site VPN setup between two routers, application performance over the tunnel is slow. You issue the show crypto ipsec sa command and see the following output. What does this output suggest?
interface Tunnel100
Crypto map tag: Tunnel100-head-0, local addr 10.10.10.10
protected vrf. (none)
local ident (addr/mask/prot/port): (10.10.10.10/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.20.20.20/255.255.255.255/47/0)
current_peer 209.165.200.230 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 34836, #pkts encrypt: 34836
#pkts decaps: 26922, #pkts decrypt: 19211, #pkts verify: 19211
#pkts compressD. 0, #pkts decompressD. 0
#pkts not compressD. 0, #pkts compr. failsD. 0
#pkts not decompressD. 0, #pkts decompress failsD. 0
#send errors 0, #recv errors 0

A. The VPN has established and is functioning normally.
B. There is an asymmetric routing issue.
C. The remote peer is not receiving encrypted traffic.
D. The remote peer is not able to decrypt traffic.
E. Packet corruption is occurring on the path between the two peers.

Correct Answer: E
Explanation/Reference:

Question 115
Which adaptive security appliance command can be used to see a generic framework of the requirements for configuring a VPN tunnel between an adaptive security appliance and a Cisco IOS router at a remote office?

Which adaptive security appliance command can be used to see a generic framework of the requirements for configuring a VPN tunnel between an adaptive security appliance and a Cisco IOS router at a remote office?
A. vpnsetup site-to-site steps
B. show running-config crypto
C. show vpn-sessiondb l2l
D. vpnsetup ssl-remote-access steps

Correct Answer: A
Explanation/Reference:

Question 116
What does this output suggest?
You are troubleshooting a site-to-site VPN issue where the tunnel is not establishing. After issuing the debug crypto ipsec command on the headend router, you see the following output. What does this output suggest?

1d00h: IPSec (validate_proposal): transform proposal
(port 3, trans 2, hmac_alg 2) not supported
1d00h: ISAKMP (0:2): atts not acceptable. Next payload is 0
1d00h: ISAKMP (0:2) SA not acceptable
A. Phase 1 policy does not match on both sides.
B. The Phase 2 transform set does not match on both sides.
C. ISAKMP is not enabled on the remote peer.
D. The crypto map is not applied on the remote peer.
E. The Phase 1 transform set does not match on both sides.

Correct Answer: B
Explanation/Reference:

Question 117
What does this output suggest?
You are troubleshooting a site-to-site VPN issue where the tunnel is not establishing. After issuing the debug crypto isakmp command on the headend router, you see the following output. What does this output suggest?

1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0
1d00h: ISAKMP (0:1): no offers accepted!
1d00h: ISAKMP (0:1): SA not acceptable!
1d00h: %CRYPTO-6-IKMP MODE FAILURE. Processing of Main Mode failed with peer at 10.10.10.10
A. Phase 1 policy does not match on both sides.
B. The transform set does not match on both sides.
C. ISAKMP is not enabled on the remote peer.
D. There is a mismatch in the ACL that identifies interesting traffic.

Correct Answer: A
Explanation/Reference:

Question 118
Which action will allow the session to establish correctly?
Refer to the exhibit.

The IKEv2 tunnel between Router1 and Router2 is failing during session establishment. Which action will allow the session to establish correctly?
A. The address command on Router2 must be narrowed down to a /32 mask.
B. The local and remote keys on Router2 must be switched.
C. The pre-shared key must be altered to use only lowercase letters.
D. The local and remote keys on Router2 must be the same.

Correct Answer: C
Explanation/Reference:
Question 119
Which configuration needs to be added or changed?
Refer to the exhibit.

An administrator is adding IPv6 addressing to an already functioning tunnel. The administrator is unable to ping 2001:DB8:100::2 but can ping 209.165.200.226.

Which configuration needs to be added or changed?
A. No configuration change is necessary. Everything is working correctly.
B. OSPFv3 needs to be configured on the interface.
C. NHRP needs to be configured to provide NBMA mapping.
D. Tunnel mode needs to be changed to GRE IPv4.
E. Tunnel mode needs to be changed to GRE IPv6.

Correct Answer: D
Explanation/Reference:
We need to encapsulate IPv6 packets in IPv4 packets to deliver them in IPv4 infrastructure. The GRE tunnel must be an IPv4.

Question 120
Which configuration error is causing the failure?
Refer to the exhibit.

An IPsec peer is exchanging routes using IKEv2, but the routes are not installed in the RIB. Which configuration error is causing the failure?
A. IKEv2 routing requires certificate authentication, not pre-shared keys.
B. An invalid administrative distance value was configured.
C. The match identity command must refer to an access list of routes.
D. The IKEv2 authorization policy is not referenced in the IKEv2 profile.

Correct Answer: B
Explanation/Reference:

Question 121
Which authentication method was used by the remote peer to prove its identity?
Refer to the exhibit.
Which authentication method was used by the remote peer to prove its identity?
A. Extensible Authentication Protocol
B. certificate authentication
C. pre-shared key
D. XAUTH

Correct Answer: C
Explanation/Reference:

Question 122
Which command should be used to identify the peer from which that route originated?
A. show crypto ikev2 sa detail
B. show crypto route
C. show crypto ikev2 client flexvpn
D. show ip route eigrp
E. show crypto isakmp sa detail

Correct Answer: A
Explanation/Reference:

Question 123
Which two technologies would accommodate the company’s requirement?
A. AnyConnect client
B. Smart Tunnels
C. Email Proxy
D. Content Rewriter
E. Portal Customizations

Correct Answer: AB
Explanation/Reference:

Question 124
As a network administrator you are tasked with configuring a FlexVPN site-to-site GRE/IPsec tunnel. The two sites use Cisco IOS routers and support the IKEv2 framework. The router at Site B is preconfigured. You must use the IKEv2 configuration options to accomplish this task.

- Configure a point-to-point GRE tunnel on the router and use interface Ethernet0/0 as the tunnel source (Use tunnel0 for this purpose). Configure 10.0.1.1/24 as the IP address on the tunnel interface. Verify that tunnels are functioning properly.
- Configure an IKEv2 proposal, and make sure that the tunnel uses the following parameters:
  - Encryption algorithm: AES 128
  - Hashing algorithm: SHA1
  - Diffie-Hellman group: 5
- Configure an IKEv2 keying, with the local pre-shared key SiteA and remote pre-shared key SiteB
- Configure an IKEv2 profile for pre-shared key authentication (Make sure that you use the FQDN SiteA.cisco.com as the local IKE identity of the router. The peer router is configured to send an identity of SiteB.cisco.com)
- Create an IPv4 profile named default. Reference the IKEv2 profile in the IPsec profile.
- Enable encryption on the GRE tunnel and do not use a crypto map. Verify that the IKEv2 tunnel is up and passing traffic by making sure that you can ping across the tunnel. Use show commands to verify that the tunnel is using the correct encryption and integrity algorithms and that traffic is encrypted/decrypted.
Correct Answer: Here are the steps as below
Explanation/Reference:
Step 1: configure key ring
crypto ikev2 keyring mykeys
peer SiteB.cisco.com
address 209.161.201.1
pre-shared-key local $iteA
pre-shared-key remote $iteB
Step 2: Configure IKEv2 profile
crypto ikev2 profile default
identity local fqdn SiteA.cisco.com
Match identity remote fqdn SiteB.cisco.com
Authentication local pre-share
Authentication remote pre-share
Kecking local mykeys
Step 3: Create the GRE Tunnel and apply profile
crypto ikev2 profile default
set ikev2-profile default
Interface tunnel 0
ip address 10.1.1.1 255.255.255.0
Tunnel source eth 0/0
Tunnel destination 209.165.201.1
tunnel protection ipsec profile default
end

Question 125
Which option shows the correct traffic selectors for the child SA on the remote ASA, when the headquarter ASA initiates the tunnel?
Which option shows the correct traffic selectors for the child SA on the remote ASA, when the headquarter ASA initiates the tunnel?

B. Local selector 192.168.33.0/0-192.168.33.255/65535 Remote selector 192.168.22.0/0-192.168.22.255/65535
D. Local selector 192.168.33.0/0-192.168.33.255/65535 Remote selector 0.0.0.0/0-0.0.0.0/65535
E. Local selector 0.0.0.0/0-0.0.0.0/65535 Remote selector 192.168.22.0/0-192.168.22.255/65535

Correct Answer: B

Explanation/Reference:
The traffic selector is used to determine which traffic should be protected (encrypted over the IPSec tunnel). We want this to be specific, otherwise Internet traffic will also be sent over the tunnel and most likely dropped on the remote side. Here, we just want to protect traffic from 192.168.33.0/24 (THE LOCAL SIDE) to 192.168.22.0/24 (THE REMOTE SIDE).

Question 126
Which of the following can be done to resolve this problem?
After implementing the IKEv2 tunnel, it was observed that remote users on the 192.168.33.0/24 network are unable to access the internet. Which of the following can be done to resolve this problem?

A. Change the Diffie-Hellman group on the headquarter ASA to group5 for the dynamic crypto map
B. Change the remote traffic selector on the remote ASA to 192.168.22.0/24
C. Change to an IKEv1 configuration since IKEv2 does not support a full tunnel with static peers
D. Change the local traffic selector on the headquarter ASA to 0.0.0.0/0
E. Change the remote traffic selector on the headquarter ASA to 0.0.0.0/0
Correct Answer: B

Explanation/Reference:

Explanation:
The traffic selector is used to determine which traffic should be protected (encrypted over the IPSec tunnel). We want this to be specific, otherwise Internet traffic will also be sent over the tunnel and most likely dropped on the remote side. Here, we just want to protect traffic from 192.168.33.0/24 to 192.168.22.0/24.

Question 127
Which encryption algorithm would be used to encrypt traffic?
If the IKEv2 tunnel were to establish successfully, which encryption algorithm would be used to encrypt traffic?

A. DES
B. 3DES
C. AES
D. AES192
E. AES256

Correct Answer: E

Explanation/Reference:
Both ASA’s are configured to support AES 256, so during the IPSec negotiation they will use the strongest algorithm that is supported by each peer.

Question 128
Which one of the following is correct?

A network administrator has been tasked with implementing an IKEv2 connection between a remote site and a headquarters site. For security reasons, all traffic from the remote site must be sent across the tunnel, including traffic destined to the Internet. Both sites are using a Cisco ASA firewall and are capable of running IKEv2.
Based on the provided ASDM configuration for the remote ASA, which one of the following is correct?

A. An access-list must be configured on the outside interface to permit inbound VPN traffic
B. A route to 192.168.22.0/24 will not be automatically installed in the routing table
C. The ASA will use a window of 128 packets (64×2) to perform the anti-replay check
D. The tunnel can also be established on TCP port 10000

Correct Answer: C

Explanation/Reference:
Cisco IP security (IPsec) authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. The decryptor keeps track of which packets it has seen on the basis of these numbers. Currently, the default window size is 64 packets. Generally, this number (window size) is sufficient, but there are times when you may want to expand this window size. The IPsec Anti-Replay Window: Expanding and Disabling feature allows you to expand the window size, allowing the decryptor to keep track of more than 64 packets.

Question 129
When a tunnel is initiated by the headquarter ASA, which one of the following Diffie-Hellman groups is selected by the headquarter ASA during CREATE_CHILD_SA exchange?
When a tunnel is initiated by the headquarter ASA, which one of the following Diffie-Hellman groups is selected by the headquarter ASA during CREATE_CHILD_SA exchange? 

A. 1  
B. 2  
C. 5  
D. 14  
E. 19  

Correct Answer: C  
Explanation/Reference:

Question 130
Which command specifies the path to the Host Scan package in an ASA AnyConnect VPN?
A. csd hostscan path image
B. csd hostscan image path
C. csd hostscan path
D. hostscan image path
Correct Answer: B
Explanation/Reference:

Question 131
Which command will prevent a group policy from inheriting a filter ACL in a clientless SSL VPN?
A. vpn-filter none
B. no vpn-filter
C. filter value none
D. filter value ACLname
Correct Answer: C
Explanation/Reference:

Question 132
What is the default storage location of user-level bookmarks in an IOS clientless SSL VPN?
A. disk0:/webvpn/{context name}/
B. disk1:/webvpn/{context name}/
C. flash:/webvpn/{context name}/
D. nvram:/webvpn/{context name}/
Correct Answer: C
Explanation/Reference:

Question 133
Which two examples of transform sets are contained in the IKEv2 default proposal?
Which two examples of transform sets are contained in the IKEv2 default proposal? (Choose two.)
A. aes-cbc-192, sha256, 14
B. 3des, md5, 5
C. 3des, sha1, 1
D. aes-cbc-128, sha, 5
Correct Answer: BD
Explanation/Reference:

Question 134
Which command configures IKEv2 symmetric identity authentication?
Which command configures IKEv2 symmetric identity authentication?
A. match identity remote address 0.0.0.0
B. authentication local pre-share
C. authentication pre-share
D. authentication remote rsa-sig
Correct Answer: D
Explanation/Reference:

Question 135
Which two cryptographic technologies are recommended for use with FlexVPN?
Which two cryptographic technologies are recommended for use with FlexVPN? (Choose two.)
A. SHA (HMAC variant)
B. Diffie-Hellman
C. DES
D. MD5 (HMAC variant)

Correct Answer: AB
Explanation/Reference:

**Question 136**
Which technology does a multipoint GRE interface require to resolve endpoints?
Which technology does a multipoint GRE interface require to resolve endpoints?
A. ESP
B. dynamic routing
C. NHRP
D. CEF
E. IPSec

Correct Answer: C
Explanation/Reference:

**Question 137**
What is the Cisco recommended TCP maximum segment on a DMVPN tunnel interface when the MTU is set to 1400 bytes?
What is the Cisco recommended TCP maximum segment on a DMVPN tunnel interface when the MTU is set to 1400 bytes?
A. 1160 bytes
B. 1260 bytes
C. 1360 bytes
D. 1240 bytes

Correct Answer: C
Explanation/Reference:

**Question 138**
Which NGE IKE Diffie-Hellman group identifier has the strongest cryptographic properties?
Which NGE IKE Diffie-Hellman group identifier has the strongest cryptographic properties?
A. group 10
B. group 24
C. group 5
D. group 20

Correct Answer: D
Explanation/Reference:

**Question 139**
Which configuration on the ASA will correctly limit the networks reachable to 209.165.201.0/27 and 209.165.202.128/27?
An administrator wishes to limit the networks reachable over the Anyconnect VPN tunnels. Which configuration on the ASA will correctly limit the networks reachable to 209.165.201.0/27 and 209.165.202.128/27?
A. `access-list splitlist standard permit 209.165.201.0 255.255.255.224
access-list splitlist standard permit 209.165.202.128 255.255.255.224`

`group-policy GroupPolicy1 internal
  group-policy GroupPolicy1 attributes
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value splitlist`

B. `access-list splitlist standard permit 209.165.201.0 255.255.255.224
access-list splitlist standard permit 209.165.202.128 255.255.255.224`

`group-policy GroupPolicy1 internal
  group-policy GroupPolicy1 attributes
  split-tunnel-policy tunnelall
  split-tunnel-network-list value splitlist`

C. `group-policy GroupPolicy1 internal
  group-policy GroupPolicy1 attributes
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list ipv4 1 209.165.201.0 255.255.255.224
split-tunnel-network-list ipv4 2 209.165.202.128 255.255.255.224`

D. `access-list splitlist standard permit 209.165.201.0 255.255.255.224
access-list splitlist standard permit 209.165.202.128 255.255.255.224`

`crypto anyconnect vpn-tunnel-policy tunnelspecified
  crypto anyconnect vpn-tunnel-policy tunnelall
  crypto anyconnect split-tunnel-network-list ipv4 1 209.165.201.0 255.255.255.224`

E. `access-list splitlist standard permit 209.165.201.0 255.255.255.224
access-list splitlist standard permit 209.165.202.128 255.255.255.224`

`crypto anyconnect split-tunnel-network-list ipv4 1 209.165.201.0 255.255.255.224`

Correct Answer: A
Explanation/Reference:

**Question 140**
Which encryption and authentication algorithms does Cisco recommend when deploying a Cisco NGE supported VPN solution?
Which encryption and authentication algorithms does Cisco recommend when deploying a Cisco NGE supported VPN solution?
A. AES-GCM and SHA-2
B. 3DES and DH
C. AES-CBC and SHA-1
D. 3DES and SHA-1
Correct Answer: D
Explanation/Reference:

**Question 141**
Which algorithm is replaced by elliptic curve cryptography in Cisco NGE?
A. 3DES
B. AES
C. DES
D. RSA

Correct Answer: D
Explanation/Reference:

**Question 142**
Which Cisco firewall platform supports Cisco NGE?
A. FWSM
B. Cisco ASA 5505
C. Cisco ASA 5580
D. Cisco ASA 5525-X

Correct Answer: D
Explanation/Reference:

**Question 143**
Which cryptographic algorithms are approved to protect Top Secret information?
A. HIPPA DES
B. AES-128
C. RC4-128
D. AES-256

Correct Answer: D
Explanation/Reference:

**Question 144**
Which hash algorithm is required to protect classified information?
A. MD5
B. SHA-1
C. SHA-256
D. SHA-384

Correct Answer: D
Explanation/Reference:

**Question 145**
When you configure IPsec VPN High Availability Enhancements, which technology does Cisco recommend that you enable to make reconvergence faster?
A. EOT
B. IP SLAs
C. periodic IKE keepalives
D. VPN fast detection

Correct Answer: C
Explanation/Reference:

**Question 146**
Which protocol supports high availability in a Cisco IOS SSL VPN environment?
A. HSRP
B. VRRP
C. GLBP
D. IRDP

Correct Answer: A
Explanation/Reference:

**Question 147**
Which command must you configure on the virtual template?
You are configuring a Cisco IOS SSL VPN gateway to operate with DVTI support. Which command must you configure on the virtual template?
A. tunnel protection ipsec
B. ip virtual-reassembly
C. tunnel mode ipsec
D. ip unnumbered

Correct Answer: D
Explanation/Reference:
Question 148
Which protocol is used between the Cisco IOS router and the Windows server?
A Cisco IOS SSL VPN gateway is configured to operate in clientless mode so that users can access file shares on a Microsoft Windows 2003 server. Which protocol is used between the Cisco IOS router and the Windows server?
A. HTTPS
B. NetBIOS
C. CIFS
D. HTTP
Correct Answer: C
Explanation/Reference:

Question 149
What is a possible reason for the failure?
An IOS SSL VPN is configured to forward TCP ports. A remote user cannot access the corporate FTP site with a Web browser. What is a possible reason for the failure?
A. The user’s FTP application is not supported.
B. The user is connecting to an IOS VPN gateway configured in Thin Client Mode.
C. The user is connecting to an IOS VPN gateway configured in Tunnel Mode.
D. The user’s operating system is not supported.
Correct Answer: B
Explanation/Reference:
Reference:
Thin-Client SSL VPN (Port Forwarding)
A remote client must download a small, Java-based applet for secure access of TCP applications that use static port numbers. UDP is not supported. Examples include access to POP3, SMTP, IMAP, SSL, and Telnet. The user needs local administrative privileges because changes are made to files on the local machine. This method of SSL VPN does not work with applications that use dynamic port assignments, for example, several FTP applications.

Question 150
When an IPsec SVTI is configured, which technology processes traffic forwarding for encryption?
When an IPsec SVTI is configured, which technology processes traffic forwarding for encryption?
A. ACL
B. IP routing
C. RRI
D. front door VPN routing and forwarding
Correct Answer: B
Explanation/Reference:

Question 151
Which IKEv2 feature minimizes the configuration of a FlexVPN on Cisco IOS devices?
Which IKEv2 feature minimizes the configuration of a FlexVPN on Cisco IOS devices?
A. IKEv2 Suite-B
B. IKEv2 proposals
C. IKEv2 profiles
D. IKEv2 Smart Defaults
Correct Answer: D
Explanation/Reference:

Question 152
Which technology supports tunnel interfaces while remaining compatible with legacy VPN implementations?
Which technology supports tunnel interfaces while remaining compatible with legacy VPN implementations?
A. FlexVPN
B. DMVPN
C. GET VPN
D. SSL VPN
Correct Answer: A
Explanation/Reference:

Question 153
Which technology can rate-limit the number of tunnels on a DMVPN hub when system utilization is above a specified percentage?
Which technology can rate-limit the number of tunnels on a DMVPN hub when system utilization is above a specified percentage?
A. NHRP Event Publisher
B. interface state control
C. CAC
D. NHRP Authentication
E. ip nhrp connect
Correct Answer: C
Explanation/Reference:

Question 154
Which are two main use cases for Clientless SSL VPN?
Which are two main use cases for Clientless SSL VPN? (Choose two.)
A. In kiosks that are part of a shared environment
B. When the users do not have admin rights to install a new VPN client
C. When full tunneling is needed to support applications that use TCP, UDP, and ICMP
D. To create VPN site-to-site tunnels in combination with remote access
Question 155
What are two benefits of DMVPN Phase 3?
What are two benefits of DMVPN Phase 3? (Choose two.)
A. Administrators can use summarization of routing protocol updates from hub to spokes.
B. It introduces hierarchical DMVPN deployments.
C. It introduces non-hierarchical DMVPN deployments.
D. It supports L2TP over IPSec as one of the VPN protocols.
Correct Answer: AB
Explanation/Reference:

Question 156
Which two features are required when configuring a DMVPN network?
Which two features are required when configuring a DMVPN network? (Choose two.)
A. Dynamic routing protocol
B. GRE tunnel interface
C. Next Hop Resolution Protocol
D. Dynamic crypto map
E. IPsec encryption
Correct Answer: BC
Explanation/Reference:

Question 157
Which two statements are true when designing a SSL VPN solution using Cisco AnyConnect?
Which two statements are true when designing a SSL VPN solution using Cisco AnyConnect? (Choose two.)
A. The VPN server must have a self-signed certificate.
B. A SSL group pre-shared key must be configured on the server.
C. Server side certificate is optional if using AAA for client authentication.
D. The VPN IP address pool can overlap with the rest of the LAN networks.
E. DTLS can be enabled for better performance.
Correct Answer: DE
Explanation/Reference:

Question 158
Which statement is true when implementing a router with a dynamic public IP address in a crypto map based site-to-site VPN?
Which statement is true when implementing a router with a dynamic public IP address in a crypto map based site-to-site VPN?
A. The router must be configured with a dynamic crypto map.
B. Certificates are always used for phase 1 authentication.
C. The tunnel establishment will fail if the router is configured as a responder only.
D. The router and the peer router must have NAT traversal enabled.
Correct Answer: C
Explanation/Reference:

Question 159
Which two qualify as Next Generation Encryption integrity algorithms?
Which two qualify as Next Generation Encryption integrity algorithms? (Choose two.)
A. SHA-512
B. SHA-256
C. SHA-192
D. SHA-380
E. SHA-192
F. SHA-196
Correct Answer: AB
Explanation/Reference:

Question 160
Which two configurations are valid?
A network administrator is configuring AES encryption for the ISAKMP policy on an IOS router. Which two configurations are valid? (Choose two.)
A. crypto isakmp policy 10
eccryption aes 254
B. crypto isakmp policy 10
eccryption aes 192
C. crypto isakmp policy 10
eccryption aes 256
D. crypto isakmp policy 10
eccryption aes 196
E. crypto isakmp policy 10
eccryption aes 199
F. crypto isakmp policy 10
eccryption aes 64
Correct Answer: BC
Explanation/Reference:
Question 161
Which VPN solution satisfies these requirements?
A company needs to provide secure access to its remote workforce. The end users use public kiosk computers and a wide range of devices. They will be accessing only an internal web application. Which VPN solution satisfies these requirements?
A. Clientless SSLVPN
B. AnyConnect Client using SSLVPN
C. AnyConnect Client using IKEv2
D. FlexVPN Client
E. Windows built-in PPTP client

Correct Answer: A
Explanation/Reference:

Question 162
Which technology can a network administrator use to detect and drop the altered data traffic?
A private wan connection is suspected of intermittently corrupting data. Which technology can a network administrator use to detect and drop the altered data traffic?
A. AES-128
B. RSA Certificates
C. SHA2-HMAC
D. 3DES
E. Diffie-Helman Key Generation

Correct Answer: C
Explanation/Reference:

Question 163
Which two VPN solutions meet the application’s network requirement?
An internet-based VPN solution is being considered to replace an existing private WAN connecting remote offices. A multimedia application is used that relies on multicast for communication. Which two VPN solutions meet the application’s network requirement? (Choose two.)
A. FlexVPN
B. DMVPN
C. Group Encrypted Transport VPN
D. Crypto-map based Site-to-Site IPsec VPNs
E. AnyConnect VPN

Correct Answer: AB
Explanation/Reference:

Question 164
What troubleshooting steps would verify the issue without causing additional risks?
A Cisco router may have a fan issue that could increase its temperature and trigger a failure. What troubleshooting steps would verify the issue without causing additional risks?
A. Configure logging using commands “logging on”, “logging buffered 4”, and check for fan failure logs using “show logging”
B. Configure logging using commands “logging on”, “logging buffered 6”, and check for fan failure logs using “show logging”
C. Configure logging using commands “logging on”, “logging discriminator msglog1 console 7”, and check for fan failure logs using “show logging”
D. Configure logging using commands “logging host 10.11.10.11”, “logging trap 2”, and check for fan failure logs at the syslog server 10.11.10.11

Correct Answer: A
Explanation/Reference:

Question 165
Which two features and commands will help troubleshoot the issue?
A user with IP address 10.10.10.10 is unable to access a HTTP website at IP address 209.165.200.225 through a Cisco ASA. Which two features and commands will help troubleshoot the issue? (Choose two.)
A. Capture user traffic using command “capture capin interface inside match ip host 10.10.10.10 any”
B. After verifying that user traffic reaches the firewall using syslogs or captures, use packet tracer command “packet-tracer input inside tcp 10.10.10.10 209.165.200.225 80”
C. Enable logging at level 1 and check the syslogs using commands “logging enable”, “logging buffered 1”, and “show logging | include 10.10.10.10”
D. Check if an access-list on the firewall is blocking the user by using command “show running-config access-list | include 10.10.10.10”
E. Use packet tracer command “packet-tracer input inside udp 0.10.10.10 1234192.168.1.3 161” to see what the firewall is doing with the user’s traffic

Correct Answer: AB
Explanation/Reference:

Question 166
Which Cisco ASDM option configures WebVPN access on a Cisco ASA?
Which Cisco ASDM option configures WebVPN access on a Cisco ASA?
A. Configuration > WebVPN > WebVPN Access
B. Configuration > Remote Access VPN > Clientless SSL VPN Access
C. Configuration > WebVPN > WebVPN Config
D. Configuration > VPN > WebVPN Access

Correct Answer: B
Explanation/Reference:

Question 167
Which Cisco ASDM option configures forwarding syslog messages to email?
Which Cisco ASDM option configures forwarding syslog messages to email?
A. Configuration > Device Management > Logging > E-Mail Setup
B. Configuration > Device Management > E-Mail Setup > Logging Enable
C. Select the syslogs to email, click Edit, and select the Forward Messages option.
D. Select the syslogs to email, click Settings, and specify the Destination Email Address option.

Correct Answer: A
Explanation/Reference:

**Question 168**
Which two filter options would the administrator choose to show only syslog messages relevant to the VPN connection?
A user is unable to establish an AnyConnect VPN connection to an ASA. When using the Real-Time Log viewer within ASDM to troubleshoot the issue, which two filter options would the administrator choose to show only syslog messages relevant to the VPN connection? (Choose two.)
A. Client’s public IP address
B. Client’s operating system
C. Client’s default gateway IP address
D. Client’s username
E. ASA’s public IP address

Correct Answer: AD
Explanation/Reference:

**Question 169**
Which three remote access VPN methods in an ASA appliance provide support for Cisco Secure Desktop?
Which three remote access VPN methods in an ASA appliance provide support for Cisco Secure Desktop? (Choose three.)
A. IKEv1
B. IKEv2
C. SSL client
D. SSL clientless
E. ESP
F. L2TP

Correct Answer: BCD
Explanation/Reference:

**Question 170**
Which command enables IOS SSL VPN Smart Tunnel support for PuTTY?
Which command enables IOS SSL VPN Smart Tunnel support for PuTTY?
A. appl ssh putty.exe win
B. appl ssh putty.exe windows
C. appl ssh putty
D. appl ssh putty.exe

Correct Answer: B
Explanation/Reference:

**Question 171**
Which two statements describe effects of the DoNothing option within the untrusted network policy on a Cisco AnyConnect profile?
Which two statements describe effects of the DoNothing option within the untrusted network policy on a Cisco AnyConnect profile? (Choose two.)
A. The client initiates a VPN connection upon detection of an untrusted network.
B. The client initiates a VPN connection upon detection of a trusted network.
C. The always-on feature is enabled.
D. The always-on feature is disabled.
E. The client does not automatically initiate any VPN connection.

Correct Answer: AD
Explanation/Reference:

**Question 172**
Which statement describes a prerequisite for single-sign-on Netegrity Cookie Support in an IOC SSL VPN?
Which statement describes a prerequisite for single-sign-on Netegrity Cookie Support in an IOC SSL VPN?
A. The Cisco AnyConnect Secure Mobility Client must be installed in flash.
B. A SiteMinder plug-in must be installed on the Cisco SSL VPN gateway.
C. A Cisco plug-in must be installed on a SiteMinder server.
D. The Cisco Secure Desktop software package must be installed in flash.

Correct Answer: C
Explanation/Reference:

**Question 173**
Which command simplifies the task of converting an SSL VPN to an IKEv2 VPN on a Cisco ASA appliance that has an invalid IKEv2 configuration?
Which command simplifies the task of converting an SSL VPN to an IKEv2 VPN on a Cisco ASA appliance that has an invalid IKEv2 configuration?
A. migrate remote-access ssl overwrite
B. migrate remote-access ikev2
C. migrate i2l
D. migrate remote-access ssl

Correct Answer: A
Explanation/Reference:

Below is a reference for this question:
If your IKEv1, or even SSL, configuration already exists, the ASA makes the migration process simple. On the command line, enter the migrate command:
migrate [i2l] {remote-access {ikev2 | ssl} | overwrite}

Things of note:
Keyword definitions:
i2l – This converts current IKEv1 I2L tunnels to IKEv2.
remote access – This converts the remote access configuration. You can convert either the IKEv1 or the SSL tunnel groups to IKEv2.

overwrite – If you have a IKEv2 configuration that you wish to overwrite, then this keyword converts the current IKEv1 configuration and removes the superfluous IKEv2 configuration.

**Question 174**
Which three plugins are available for clientless SSL VPN?
Which three plugins are available for clientless SSL VPN? (Choose three.)
A. CIFS
B. RDP2
C. SSH
D. VNC
E. SQLNET
F. ICMP

Correct Answer: BCD
Explanation/Reference:

**Question 175**
Which file must you configure?
To change the title panel on the logon page of the Cisco IOS WebVPN portal, which file must you configure?
A. Cisco IOS WebVPN customization template
B. Cisco IOS WebVPN customization general
C. web-access-hlp.inc
D. app-access-hlp.inc

Correct Answer: A
Explanation/Reference:

**Question 176**
What are two variables for configuring clientless SSL VPN single sign-on?
What are two variables for configuring clientless SSL VPN single sign-on? (Choose two.)
A. CSCO_WEBVPN_OTP_PASSWORD
B. CSCO_WEBVPN_INTERNAL_PASSWORD
C. CSCO_WEBVPN_USERNAME
D. CSCO_WEBVPN_RADIUS_USER

Correct Answer: BC
Explanation/Reference:

**Question 177**
When Cisco ASA applies VPN permissions, what is the first set of attributes that it applies?
When Cisco ASA applies VPN permissions, what is the first set of attributes that it applies?
A. dynamic access policy attributes
B. group policy attributes
C. connection profile attributes
D. user attributes

Correct Answer: A
Explanation/Reference:

**Question 178**
What are two forms of SSL VPN?
What are two forms of SSL VPN? (Choose two)
A. port forwarding
B. Full Tunnel Mode
C. Cisco IOS WebVPN
D. Cisco AnyConnect

Correct Answer: CD
Explanation/Reference:

**Question 179**
Where do you enable the DTLS protocol setting?
In the Cisco ASDM interface, where do you enable the DTLS protocol setting?
A. Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy
B. Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit
C. Device Management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client
D. Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit

Correct Answer: C
Explanation/Reference:
Reference:
Shows where DTLS can be configured as:
- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy > Advanced > SSL VPN Client
- Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client
- Device Management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client

**Question 180**
What is a possible cause of the connection failure?
Consider this scenario. When users attempt to connect via a Cisco AnyConnect VPN session, the certificate has changed and the connection fails. What is a possible cause of the connection failure?
A. An invalid modulus was used to generate the initial key.
B. The VPN is using an expired certificate.
C. The Cisco ASA appliance was reloaded.
D. The Trusted Root Store is configured incorrectly.

Correct Answer: C
Explanation/Reference:

Question 181
Which feature must be enabled and configured to allow SSH applications to respond on the specified port 8889?
A network is configured to allow clientless access to resources inside the network. Which feature must be enabled and configured to allow SSH applications to respond on the specified port 8889?
A. auto applet download
B. port forwarding
C. web-type ACL
D. HTTP proxy

Correct Answer: B
Explanation/Reference:

Question 182
Which combination of devices can connect?
Refer to the exhibit.
After the configuration is performed, which combination of devices can connect?
A. a device with an identity type of IPv4 address of 209.165.200.225 or 209.165.202.155 or a certificate with subject name of “cisco.com”
B. a device with an identity type of IPv4 address of both 209.165.200.225 and 209.165.202.155 or a certificate with subject name containing “cisco.com”
C. a device with an identity type of IPv4 address of both 209.165.200.225 and 209.165.202.155 and a certificate with subject name containing “cisco.com”
D. a device with an identity type of IPv4 address of 209.165.200.225 or 209.165.202.155 or a certificate with subject name containing “cisco.com”

Correct Answer: D
Explanation/Reference:

Question 183
Which type of interface does a branch router require?
In a spoke-to-spoke DMVPN topology, which type of interface does a branch router require?
A. Virtual tunnel interface
B. Multipoint GRE interface
C. Point-to-point GRE interface
D. Loopback interface

Correct Answer: B
Explanation/Reference:

Question 184
Which two parameters are configured within an IKEv2 proposal on an IOS router?
Which two parameters are configured within an IKEv2 proposal on an IOS router? (Choose two.)
A. authentication
B. encryption
C. integrity
D. lifetime

Correct Answer: BC
Explanation/Reference:
Question 186
Which two IKEv1 policy options must match on each peer when you configure an IPSec site-to-site VPN?
Which two IKEv1 policy options must match on each peer when you configure an IPSec site-to-site VPN? (Choose two.)
A. priority number
B. hash algorithm
C. encryption algorithm
D. session lifetime
E. PRF algorithm
Correct Answer: BC
Explanation/Reference:

Question 187
What are the three primary components of a GET VPN network?
What are the three primary components of a GET VPN network? (Choose three.)
A. Group Domain of Interpretation protocol
B. Simple Network Management Protocol
C. server load balancer
D. accounting server
E. group member
F. key server
Correct Answer: AEF
Explanation/Reference:

Question 188
Which two GDOI encryption keys are used within a GET VPN network?
Which two GDOI encryption keys are used within a GET VPN network? (Choose two.)
A. key encryption key
B. group encryption key
C. user encryption key
D. traffic encryption key
Correct Answer: AD
Explanation/Reference:

Question 189
What is the default topology type for a GET VPN?
What is the default topology type for a GET VPN?
A. point-to-point
B. hub-and-spoke
C. full mesh
D. on-demand spoke-to-spoke
Correct Answer: C
Explanation/Reference:

Question 190
What are three benefits of deploying a GET VPN?
What are three benefits of deploying a GET VPN? (Choose three.)
A. It provides highly scalable point-to-point topologies
B. It allows replication of packets after encryption.
C. It is suited for enterprises running over a DMVPN network.
D. It preserves original source and destination IP address information.
E. It simplifies encryption management through use of group keying.
F. It supports non-IP protocols.
Correct Answer: BDE
Explanation/Reference:

Question 191
What is the role of a NHRP resolution request?
In FlexVPN, what is the role of a NHRP resolution request?
A. It allows these entities to directly communicate without requiring traffic to use an intermediate hop
B. It dynamically assigns VPN users to a group
C. It blocks these entities from directly communicating with each other
D. It makes sure that each VPN spoke directly communicates with the hub
Correct Answer: A
Explanation/Reference:

Question 192
What command can an administrator use to create a virtual template interface that can be configured and applied dynamically to create virtual access interfaces?
In FlexVPN, what command can an administrator use to create a virtual template interface that can be configured and applied dynamically to create virtual access interfaces?
A. interface virtual-template number type template
B. interface virtual-template number type tunnel
C. interface template number type virtual
D. interface tunnel-template number
Correct Answer: B
SUMMARY STEPS
1. enable
2. configure terminal
3. interface virtual-template number type tunnel
4. ip unnumbered tunnel number
5. ip nhrp network-id number
6. ip nhrp shortcut virtual-template-number
7. ip nhrp redirect [timeout seconds]
8. exit

Question 193
Which of the following could be used to configure remote access VPN Host-scan and pre-login policies?

A. ASDM
B. Connection-profile CLI command
C. Host-scan CLI command under the VPN group policy
D. Pre-login-check CLI command

Correct Answer: A

Question 194
Where is split-tunneling defined for remote access clients on an ASA?

A. Group-policy
B. Tunnel-group
C. Crypto-map
D. Web-VPN Portal
E. ISAKMP client

Correct Answer: A

Question 195
Which four activities does the Key Server perform in a GETVPN deployment? (Choose four.)

A. authenticates group members
B. manages security policy
C. creates group keys
D. distributes policy/keys
E. encrypts endpoint traffic
F. receives policy/keys
G. defines group members

Correct Answer: ABCD

Question 196
Which two are valid configuration constructs on a Cisco IOS router? (Choose two.)

A. crypto ikev2 keyring keyring-name
peer peer1
   address 209.165.201.1 255.255.255.255
   pre-shared-key local key1
   pre-shared-key remote key2

B. crypto ikev2 transform-set transform-set-name
   esp-3des esp-md5-hmac
   esp-aes esp-sha-hmac

C. crypto ikev2 map crypto-map-name
   set crypto ikev2 tunnel-group tunnel-group-name
   set crypto ikev2 transform-set transform-set-name

D. crypto ikev2 tunnel-group tunnel-group-name
   match identity remote address 209.165.201.1
   authentication local pre-share
   authentication remote pre-share

E. crypto ikev2 profile profile-name
   match identity remote address 209.165.201.1
   authentication local pre-share
   authentication remote pre-share

Correct Answer: AE

Question 197
Which two are characteristics of GETVPN? (Choose two.)

A. The IP header of the encrypted packet is preserved
B. A key server is elected among all configured Group Members
C. Unique encryption keys are computed for each Group Member
D. The same key encryption and traffic encryption keys are distributed to all Group Members

Correct Answer: AD
Explanation/Reference: