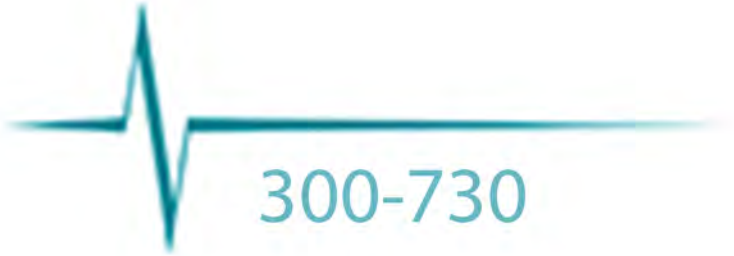
Practice Exam Questions



Implementing Secure Solutions with Virtual Private Networks (SVPN)

EXAMKILLER

Help Pass Your Exam At First Try

Cisco

Exam 300-730

Implementing Secure Solutions with Virtual Private Networks (SVPN)

Version: 5.0

[Total Questions: 146]

Topic break down

Topic	No. of Questions
Topic 1: Site-to-site Virtual Private Networks on Routers and Firewall	10
Topic 2: Remote access VPNs	18
Topic 3: Troubleshooting using ASDM and CLI	12
Topic 4: Secure Communications Architectures	20
Topic 5: Mixed Questions	86

Topic 1, Site-to-site Virtual Private Networks on Routers and Firewall

Question No : 1 - (Topic 1)

Refer to the exhibit.

```
HUB#show ip nhrp
10.0.0.2/32 via 10.0.0.2
   Tunnel0 created 00:02:09, expire 00:00:01
   Type: dynamic, Flags: unique registered used nhop
   NBMA address: 2.2.2.1
10.0.0.3/32 via 10.0.0.3
   Tunnel0 created 00:13:25, 01:46:34
   Type: dynamic, Flags: unique registered used nhop
   NBMA address: 3.3.3.1
```

The DMVPN tunnel is dropping randomly and no tunnel protection is configured. Which spoke configuration mitigates tunnel drops?

A.
```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 20
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 120
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

B.
```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 120
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

C.
```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 20
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

D.
```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 150
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
end
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

Question No : 2 - (Topic 1)

Which two parameters help to map a VPN session to a tunnel group without using the tunnel-group list? (Choose two.)

A. group-alias
B. certificate map
C. optimal gateway selection
D. group-url
E. AnyConnect client version

Answer: A,D

Explanation: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/98580-enable-group-dropdown.html

Question No : 3 - (Topic 1)

Refer to the exhibit.

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.168.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 192.168.0.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #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.: 192.168.0.1, remote crypto endpt.: 192.168.0.2
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
     current outbound spi: 0x3D05D003(1023791107)
     PFS (Y/N): N, DH group: none
```

Which two tunnel types produce the show crypto ipsec sa output seen in the exhibit? (Choose two.)

A. crypto map
B. DMVPN

C. GRE
D. FlexVPN
E. VTI

Answer: B,E

Question No : 4 - (Topic 1)

Refer to the exhibit.

```
ASA-4-751015 Local:0.0.0.0:0 Remote:0.0.0.0:0 Username:Unknown SA request
rejected by CAC. Reason: IN-NEGOTIATION SA LIMIT REACHED
```

A customer cannot establish an IKEv2 site-to-site VPN tunnel between two Cisco ASA devices. Based on the syslog message, which action brings up the VPN tunnel?

A. Reduce the maximum SA limit on the local Cisco ASA.
B. Increase the maximum in-negotiation SA limit on the local Cisco ASA.
C. Remove the maximum SA limit on the remote Cisco ASA.
D. Correct the crypto access list on both Cisco ASA devices.

Answer: B

Question No : 5 - (Topic 1)

Which two changes must be made in order to migrate from DMVPN Phase 2 to Phase 3 when EIGRP is configured? (Choose two.)

A. Add NHRP shortcuts on the hub.
B. Add NHRP redirects on the spoke.
C. Disable EIGRP next-hop-self on the hub.
D. Enable EIGRP next-hop-self on the hub.
E. Add NHRP redirects on the hub.

Answer: D,E

Explanation: DMVPN disables the EIRGP next-hop-self with "no ip next-hop-self eigrp

xxx" in DMVPN phase 2, and to go from Phase 2 to 3 you need use the NHRP protocol, and again enable EIRGP next-hop-self with "ip next-hop-self eigrp 134" under the tunnel interface https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-dmvpn.html#GUID-BF561439-BCC0-4AAF-80D9-1F7876CB7B81

Question No : 6 - (Topic 1)

Which method dynamically installs the network routes for remote tunnel endpoints?

A. policy-based routing
B. CEF
C. reverse route injection
D. route filtering

Answer: C

Explanation: Reverse route injection (RRI) is a method that dynamically installs the network routes for remote tunnel endpoints. The RRI feature allows the router to automatically learn the routes for the remote networks and automatically install these routes into the routing table. This eliminates the need for the administrator to manually configure and maintain the routes for the remote networks. This feature is commonly used in VPN environments, where the router at the VPN endpoint needs to learn the routes for the remote networks behind the other VPN endpoint. The other options such as policy-based routing, CEF, and route filtering are not used to dynamically install the network routes for remote tunnel endpoints

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/12-4t/sec-vpn- availability-12-4t-book/sec-rev-rte-inject.html

Question No : 7 - (Topic 1)

On a FlexVPN hub-and-spoke topology where spoke-to-spoke tunnels are not allowed, which command is needed for the hub to be able to terminate FlexVPN tunnels?

A. interface virtual-access
B. ip nhrp redirect
C. interface tunnel
D. interface virtual-template

Answer: D

Explanation:

On a FlexVPN hub-and-spoke topology where spoke-to-spoke tunnels are not allowed, the command that is needed for the hub to be able to terminate FlexVPN tunnels is interface virtual-template. The interface virtual-template command is used to configure a virtual template interface which provides a secure tunnel for FlexVPN connections. The other commands listed - interface virtual-access, ip nhrp redirect, and interface tunnel - are not related to FlexVPN and are not used to terminate FlexVPN tunnels.

Question No : 8 - (Topic 1)

Which statement about GETVPN is true?

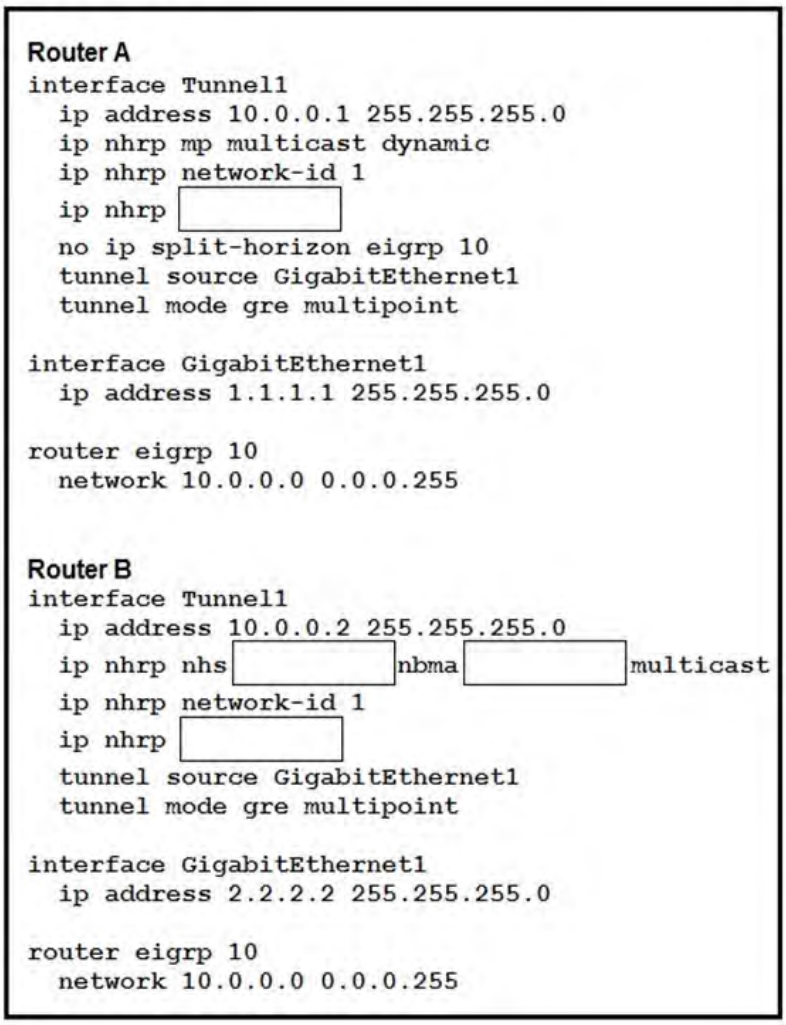
A. The configuration that defines which traffic to encrypt originates from the key server.
B. TEK rekeys can be load-balanced between two key servers operating in COOP.
C. The pseudotime that is used for replay checking is synchronized via NTP.
D. Group members must acknowledge all KEK and TEK rekeys, regardless of configuration.

Answer: A

Question No : 9 DRAG DROP - (Topic 1)

Drag and drop the correct commands from the night onto the blanks within the code on the left to implement a design that allow for dynamic spoke-to-spoke communication. Not all comments are used.

Answer Area



1.1.1.1

10.0.0.1

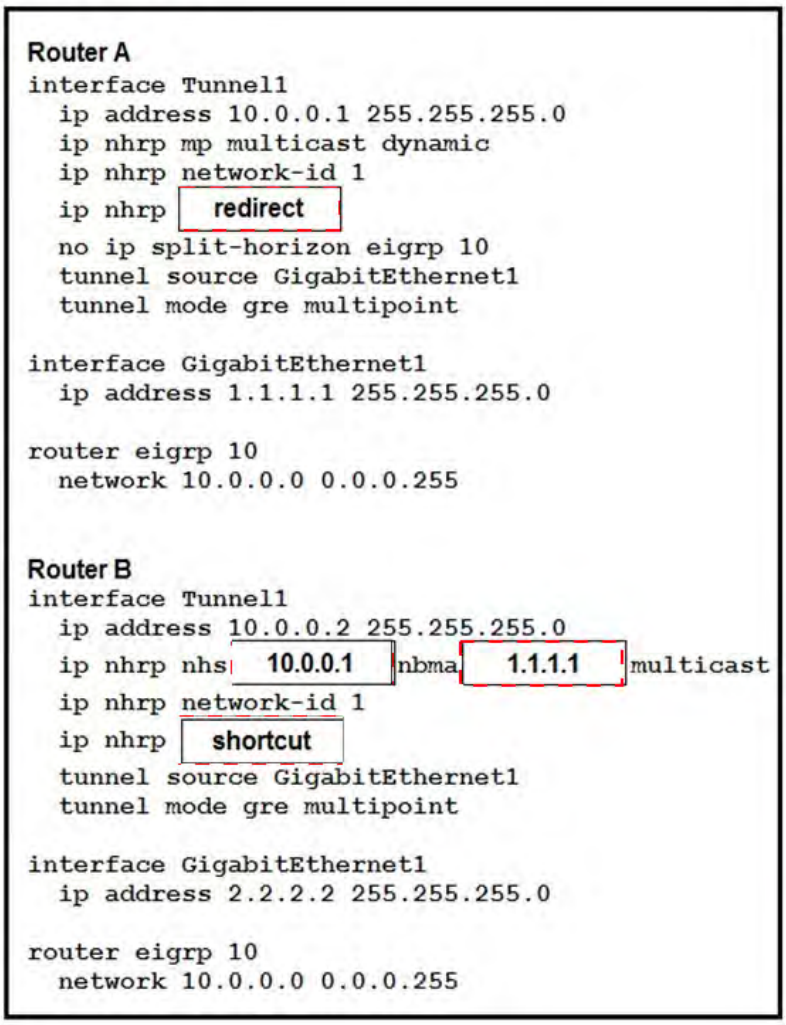
redirect

shortcut

server-only

Answer:

Answer Area



1.1.1.1

10.0.0.1

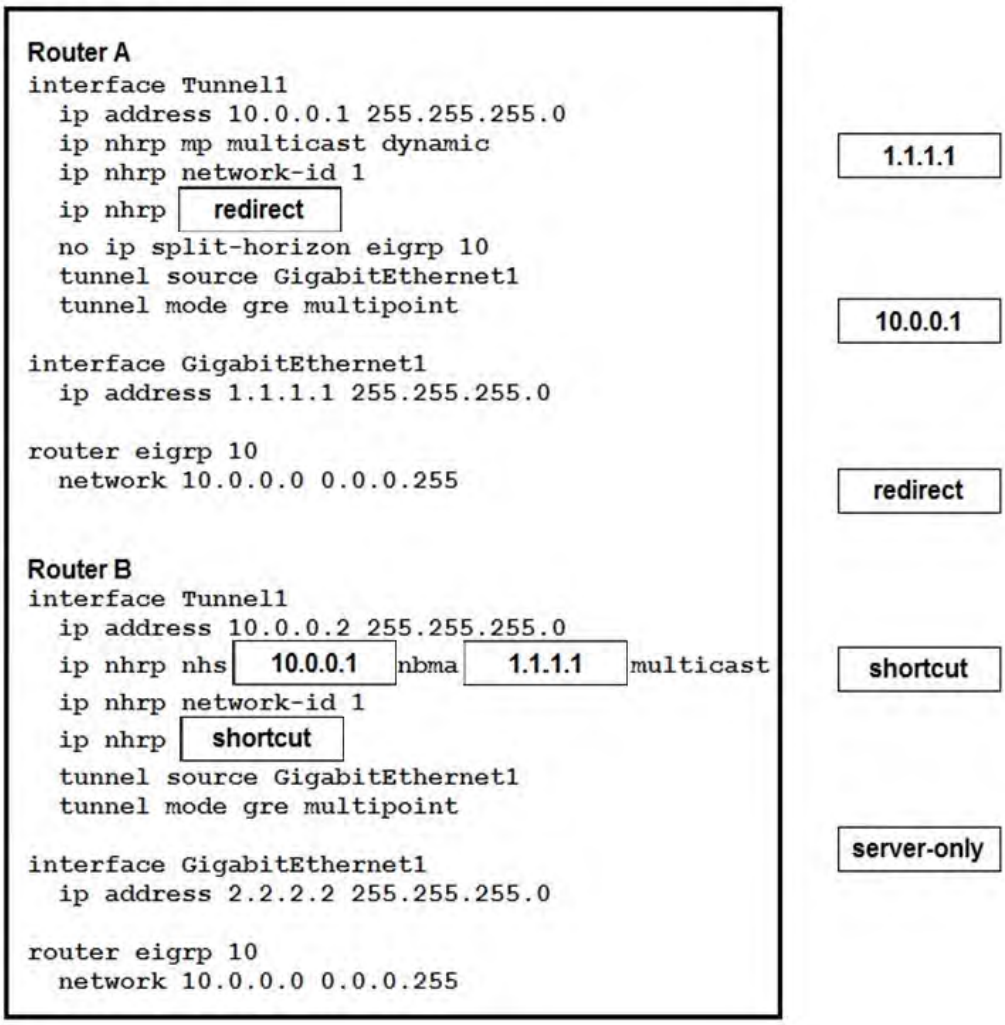
redirect

shortcut

server-only

Explanation:

Answer Area



Question No : 10 - (Topic 1)

A second set of traffic selectors is negotiated between two peers using IKEv2. Which IKEv2 packet will contain details of the exchange?

A. IKEv2 IKE_SA_INIT
B. IKEv2 INFORMATIONAL
C. IKEv2 CREATE_CHILD_SA
D. IKEv2 IKE_AUTH

Answer: C

Explanation: The IKEv2 CREATE_CHILD_SA packet is used to establish a new security association (SA) between two peers. This packet contains the details of the exchange, including the traffic selectors, the cryptographic algorithms and keys to be used, and any other relevant information

Topic 2, Remote access VPNs

Question No : 11 - (Topic 2)

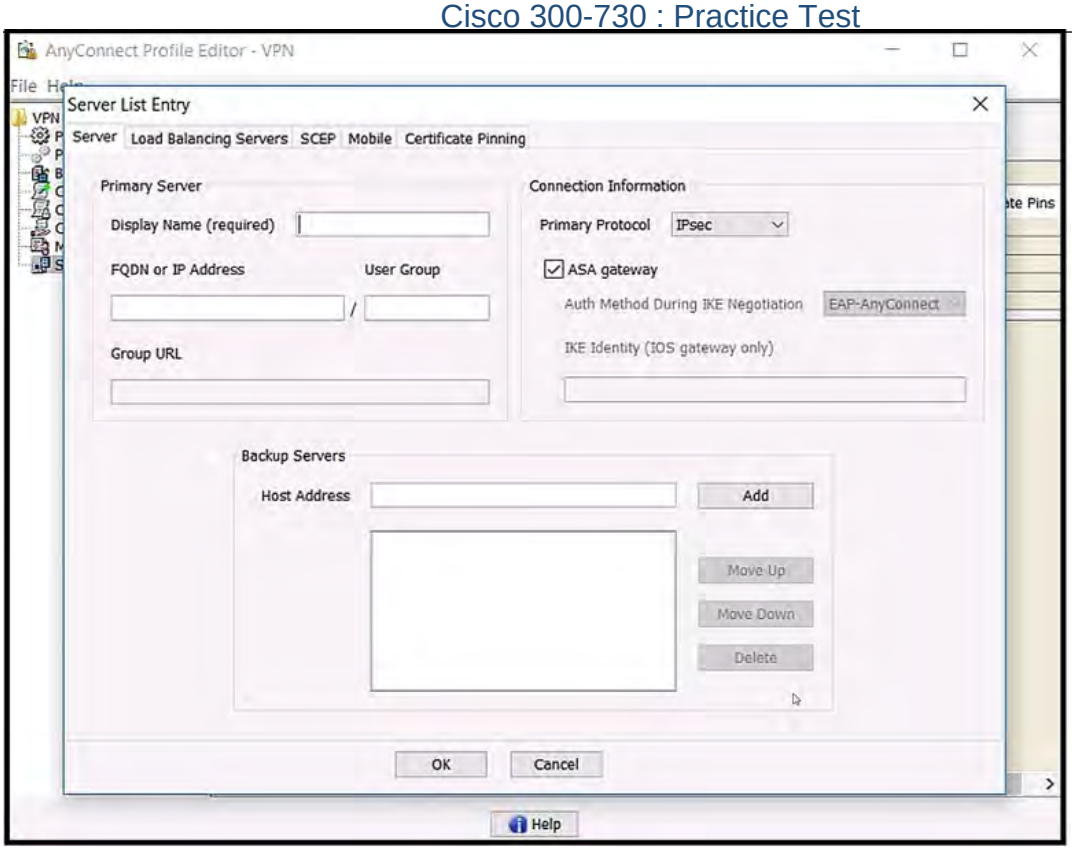
Which command identifies a Cisco AnyConnect profile that was uploaded to the flash of an IOS router?

A. svc import profile SSL_profile flash:simos-profile.xml
B. anyconnect profile SSL_profile flash:simos-profile.xml
C. crypto vpn anyconnect profile SSL_profile flash:simos-profile.xml
D. webvpn import profile SSL_profile flash:simos-profile.xml

Answer: C
Reference: https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200533- AnyConnect-Configure-Basic-SSLVPN-for-I.html

Question No : 12 - (Topic 2)

Refer to the exhibit.



Which value must be configured in the User Group field when the Cisco AnyConnect Profile is created to connect to an ASA headend with IPsec as the primary protocol?

A. address-pool
B. group-alias
C. group-policy
D. tunnel-group

Answer: D

Explanation: The user group is used in conjunction with Host Address to form a group-based URL. If you specify the Primary Protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group). For SSL, the user group is the group-url of the connection profile.
https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/administration/guide/b_AnyConnect_Administrator_Guide_4-0/anyconnect-profile-editor.html#ID-1430-0000026c

Reference:
https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect41/administration/guide/b_AnyConnect_Administrator_Guide_4-1/configure-vpn.html

Question No : 13 - (Topic 2)

Refer to the exhibit.

```
aaa new-model
!
aaa authorization network local-group-author-list local
!
crypto pki trustpoint trustpoint1
 enrollment url http://192.168.3.1:80
 revocation-check crl
!
crypto pki certificate map certmap1 1
 subject-name co cisco
!
crypto ikev2 authorization policy author-policy1
 ipv6 pool v6-pool
 ipv6 dns 2001:DB8:1::11 2001:DB8:1::12
 ipv6 subnet-acl v6-acl
!
crypto ikev2 profile ikev2-profile1
 match certificate certmap1
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint trustpoint1
 aaa authorization group cert list local-group-author-list
author-policy1
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ipv6 address 2001:DB8:1::1/32
!
interface Virtual-Template1 type tunnel
 ipv6 unnumbered Ethernet0/0
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile ipsec-profile1
!
ipv6 local pool v6-pool 2001:DB8:1::10/32 48
!
ipv6 access-list v6-acl
 permit ipv6 host 2001:DB8:1::20 any
 permit ipv6 host 2001:DB8:1::30 any
```

What is configured as a result of this command set?

A. FlexVPN client profile for IPv6
B. FlexVPN server to authorize groups by using an IPv6 external AAA
C. FlexVPN server for an IPv6 dVTI session
D. FlexVPN server to authenticate IPv6 peers by using EAP

Answer: C

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/flexvpn/116528-config-flexvpn-00.html

Question No : 14 - (Topic 2)

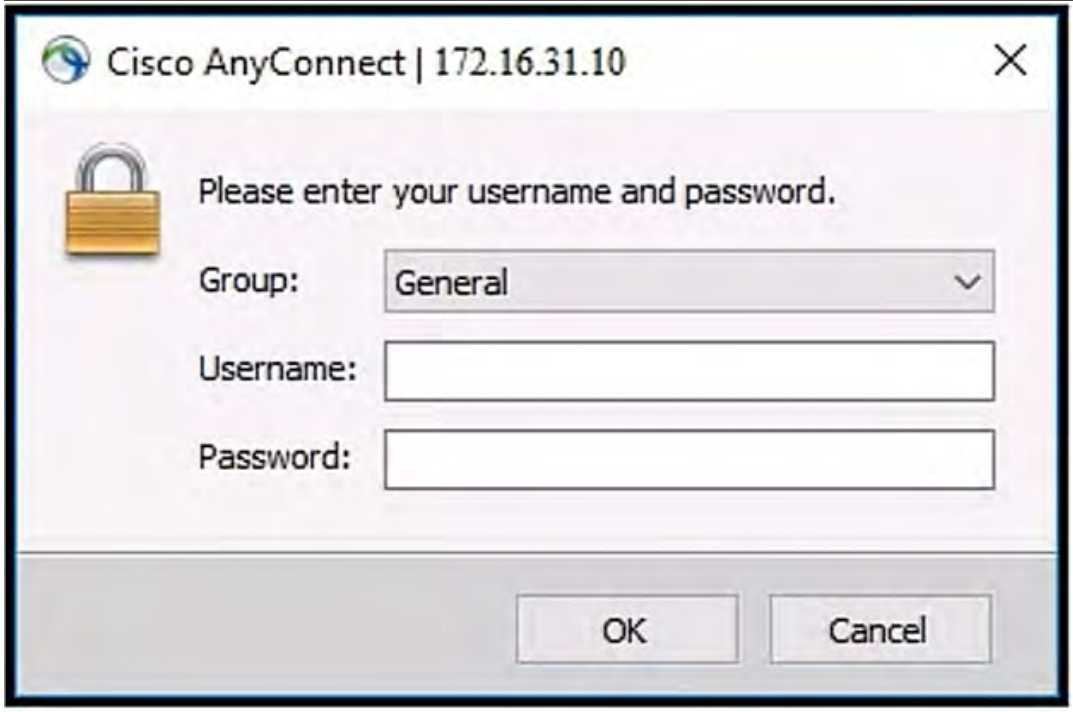
Under which section must a bookmark or URL list be configured on a Cisco ASA to be available for clientless SSLVPN users?

A. tunnel-group (general-attributes)
B. tunnel-group (webvpn-attributes)
C. webvpn (group-policy)
D. webvpn (global configuration)

Answer: C

Question No : 15 - (Topic 2)

Refer to the exhibit.



Which two commands under the tunnel-group webvpn-attributes result in a Cisco AnyConnect user receiving the AnyConnect prompt in the exhibit? (Choose two.)

A. group-url https://172.16.31.10/General enable
B. group-policy General internal
C. authentication aaa
D. authentication certificate
E. group-alias General enable

Answer: C,E

Explanation: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/98580-enable-group-dropdown.html

Question No : 16 - (Topic 2)

Which command automatically initiates a smart tunnel when a user logs in to the WebVPN portal page?

A. auto-upgrade
B. auto-connect
C. auto-start
D. auto-run

Answer: C
Reference:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/vpn/asa_91_vpn_config/ webvpn-configure-policy-group.html

Question No : 17 - (Topic 2)

Which two types of web resources or protocols are enabled by default on the Cisco ASA Clientless SSL VPN portal? (Choose two.)

A. HTTP
B. ICA (Citrix)
C. VNC
D. RDP
E. CIFS

Answer: A,E
Explanation: HTTP (Hypertext Transfer Protocol) is used for transferring web resources, such as web pages and HTML documents, across the internet. CIFS (Common Internet File System) is used for sharing files and printers between computers on a network. ICA (Citrix), VNC (Virtual Network Computing), and RDP (Remote Desktop Protocol) are not enabled by default on the Cisco ASA Clientless SSL VPN portal.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/vpn/asa-94-vpn-config/webvpn-configure-gateway.html

Question No : 18 - (Topic 2)

A Cisco AnyConnect client establishes a SSL VPN connection with an ASA at the corporate office. An engineer must ensure that the client computer meets the enterprise security policy. Which feature can update the client to meet an enterprise security policy?

A. Endpoint Assessment
B. Cisco Secure Desktop
C. Basic Host Scan
D. Advanced Endpoint Assessment

Answer: D

Question No : 19 - (Topic 2)

Cisco AnyConnect Secure Mobility Client has been configured to use IKEv2 for one group of users and SSL for another group. When the administrator configures a new AnyConnect release on the Cisco ASA, the IKEv2 users cannot download it automatically when they connect. What might be the problem?

A. The XML profile is not configured correctly for the affected users.
B. The new client image does not use the same major release as the current one.
C. Client services are not enabled.
D. Client software updates are not supported with IKEv2.

Answer: D

Explanation: Cisco AnyConnect Secure Mobility Client uses IKEv2 for one group of users and SSL for another group. However, IKEv2 does not support client software updates, which means that when the administrator configures a new AnyConnect release on the Cisco ASA, the IKEv2 users cannot download it automatically when they connect.

Question No : 20 - (Topic 2)

Which feature allows the ASA to handle nonstandard applications and web resources so that they display correctly over a clientless SSL VPN connection?

A. single sign-on
B. Smart Tunnel
C. WebType ACL
D. plug-ins