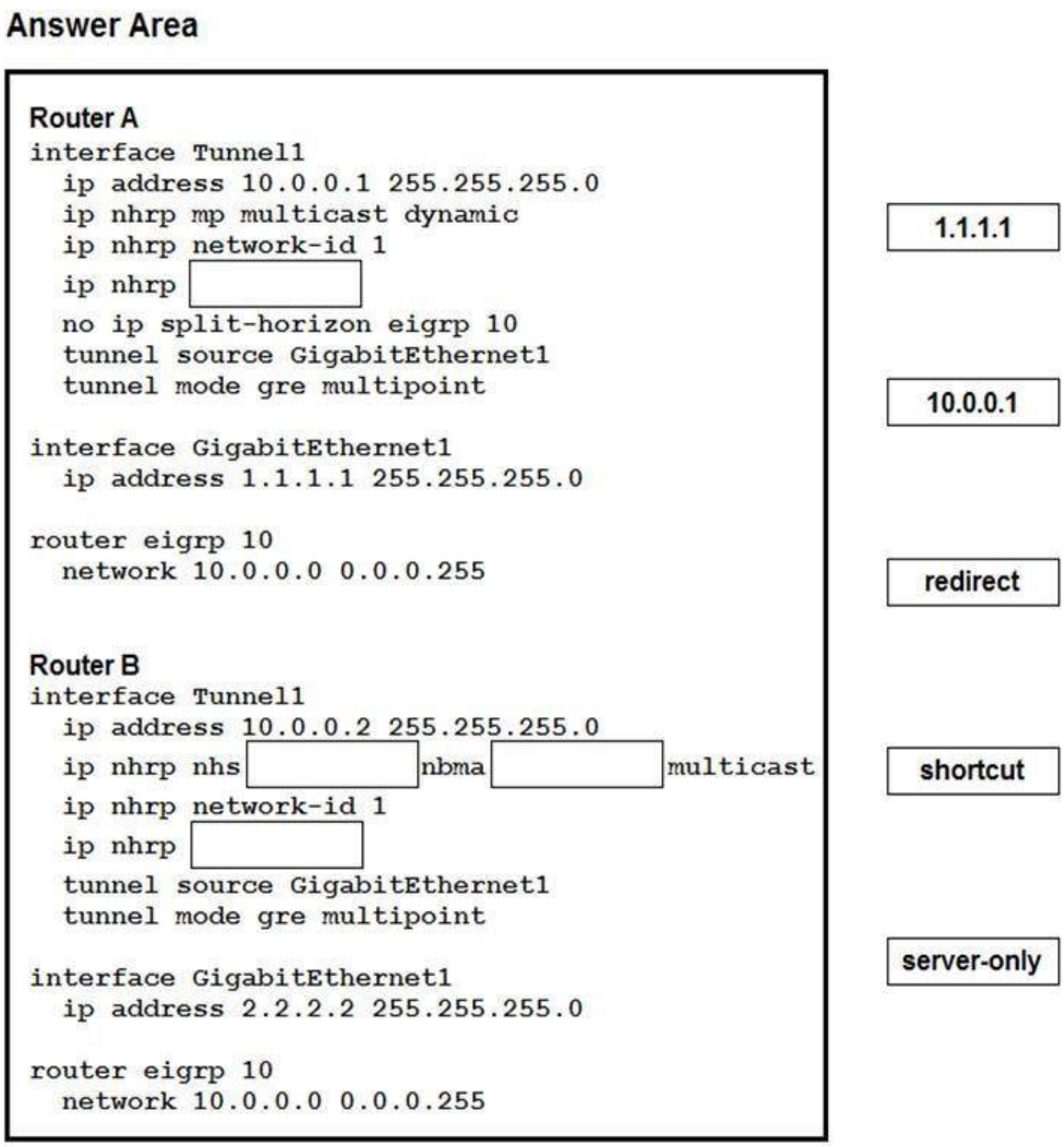
Cisco

Exam Questions 300-730

Implementing Secure Solutions with Virtual Private Networks (SVPN)

NEW QUESTION 1
DRAG DROP
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.
Select and Place:



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-16/sec-conn-dmvpn-xe-16-book/sec-conn-dmvpn-summ-maps.html

NEW QUESTION 2
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

NEW QUESTION 3
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: CE

NEW QUESTION 4
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

NEW QUESTION 5
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:
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

NEW QUESTION 6
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

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

NEW QUESTION 7
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

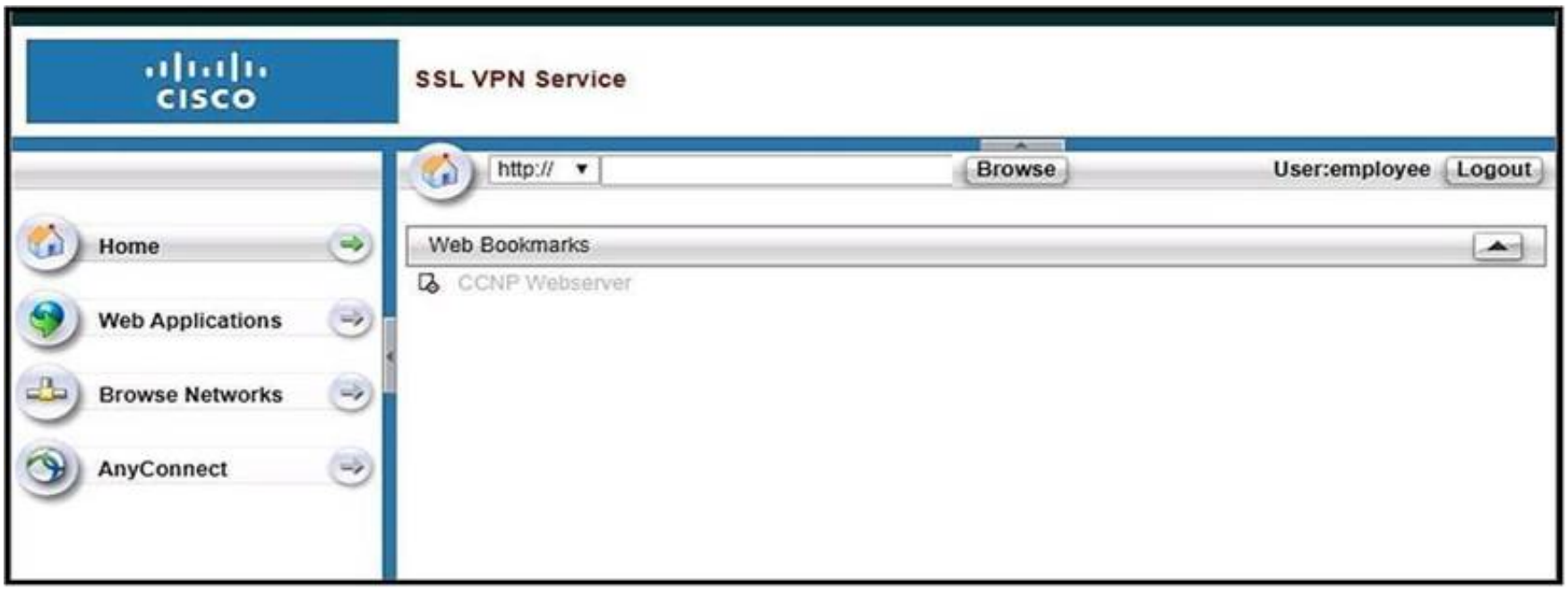
Answer: D

NEW QUESTION 8
Which two features provide headend resiliency for Cisco AnyConnect clients? (Choose two.)

A. AnyConnect Auto Reconnect
B. AnyConnect Network Access Manager
C. AnyConnect Backup Servers
D. ASA failover
E. AnyConnect Always On

Answer: CD

NEW QUESTION 9
Refer to the exhibit.



Based on the exhibit, why are users unable to access CCNP Webserver bookmark?

A. The URL is being blocked by a WebACL.
B. The ASA cannot resolve the URL.
C. The bookmark has been disabled.
D. The user cannot access the URL.

Answer: C

NEW QUESTION 10
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

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

NEW QUESTION 10
In a FlexVPN deployment, the spokes successfully connect to the hub, but spoke-to-spoke tunnels do not form. Which troubleshooting step solves the issue?

A. Verify the spoke configuration to check if the NHRP redirect is enabled.
B. Verify that the spoke receives redirect messages and sends resolution requests.
C. Verify the hub configuration to check if the NHRP shortcut is enabled.
D. Verify that the tunnel interface is contained within a VRF.

Answer: B

Explanation:
Reference: 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-summ-maps.pdf

NEW QUESTION 13
An engineer is troubleshooting a new DMVPN setup on a Cisco IOS router. After the show crypto isakmp sa command is issued, a response is returned of "MM_NO_STATE." Why does this failure occur?

A. The ISAKMP policy priority values are invalid.
B. ESP traffic is being dropped.
C. The Phase 1 policy does not match on both devices.
D. Tunnel protection is not applied to the DMVPN tunnel.

Answer: B

NEW QUESTION 14
Refer to the exhibit.

```
*Nov 26 00:52:20.002: IKEv2:(SESSION ID = 1,SA ID = 1):Received Packet [From 10.10.10.1:500/To 10.10.10.2:500/VRF i0:f0]
Initiator SPI : D5684E1462991856 - Responder SPI : 2162145C95256F6A Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
*Nov 26 00:52:20.002: IKEv2-PAK:(SESSION ID = 1,SA ID = 1):Next payload: ENCR, version: 2.0 Exchange type: IKE_AUTH, flags: RESPONDER MSG-RESPONSE Message id: 1, length: 236
Payload contents:
 VID Next payload: IDr, reserved: 0x0, length: 20
 IDr Next payload: AUTH, reserved: 0x0, length: 12
   Id type: IPv4 address, Reserved: 0x0 0x0
 AUTH Next payload: SA, reserved: 0x0, length: 28
   Auth method PSK, reserved: 0x0, reserved: 0x0
 SA Next payload: TSi, reserved: 0x0, length: 40
  last proposal: 0x0, reserved: 0x0, length: 35
  Proposal: 1, Protocol id: ESP, SPI size: 4, #trans: 3 last transform: 0x3, reserved: 0x0: length: 8
   type: 1, reserved: 0x0, id: 3DES
   last transform: 0x3, reserved: 0x0: length: 8
   type: 3, reserved: 0x0, id: SHA96
   last transform: 0x0, reserved: 0x0: length: 8
   type: 5, reserved: 0x0, id: Don't use ESN
TSi Next payload: TSr, reserved: 0x0, length: 24
   Num of TSs: 1, reserved 0x0, reserved 0x0
   TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
   start port: 0, end port: 65535
   start addr: 30.30.30.0, end addr: 30.30.30.255
TSr Next payload: NOTIFY, reserved: 0x0, length: 24
   Num of TSs: 1, reserved 0x0, reserved 0x0
   TS type: TS_IPV4_ADDR_RANGE, proto id: 0, length: 16
   start port: 0, end port: 65535
   start addr: 20.20.20.0, end addr: 20.20.20.255
NOTIFY(SET_WINDOW_SIZE) Next payload: NOTIFY, reserved: 0x0, length: 12
   Security protocol id: Unknown - 0, spi size: 0, type: SET_WINDOW_SIZE
NOTIFY(ESP_TFC_NO_SUPPORT) Next payload: NOTIFY, reserved: 0x0, length: 8
   Security protocol id: Unknown - 0, spi size: 0, type: ESP_TFC_NO_SUPPORT
NOTIFY(NON_FIRST_FRAGS) Next payload: NONE, reserved: 0x0, length: 8
   Security protocol id: Unknown - 0, spi size: 0, type: NON_FIRST_FRAGS

*Nov 26 00:52:20.003: IKEv2:(SESSION ID = 1,SA ID = 1):Process auth response notify
*Nov 26 00:52:20.003: IKEv2:(SESSION ID = 1,SA ID = 1):Searching policy based on peer's identity '10.10.10.1' of type 'IPv4 address'
*Nov 26 00:52:20.004: IKEv2-ERROR:(SESSION ID = 1,SA ID = 1):: Failed to locate an item in the database
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Verification of peer's authentication data FAILED
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Auth exchange failed
*Nov 26 00:52:20.004: IKEv2-ERROR:(SESSION ID = 1,SA ID = 1):: Auth exchange failed
Router#
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Abort exchange
*Nov 26 00:52:20.004: IKEv2:(SESSION ID = 1,SA ID = 1):Deleting SA
```

The IKEv2 site-to-site VPN tunnel between two routers is down. Based on the debug output, which type of mismatch is the problem?

A. preshared key
B. peer identity
C. transform set
D. ikev2 proposal

Answer: B

NEW QUESTION 16
Refer to the exhibit.

```
HUB configuration:

crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn hub.cisco.com
 authentication local rsa-sig
 authentication remote pre-shared-key cisco
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1

---

SPOKE 1 configuration:

crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke.cisco.com
 authentication local rsa-sig
 authentication remote pre-shared-key cisco
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1

---

SPOKE 2 configuration:

crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke2.cisco.com
 authentication local pre-shared-key flexvpn
 authentication remote rsa-sig
 pki trustpoint CA
aaa authorization group cert list default default
virtual-template 1
```

What is a result of this configuration?

A. Spoke 1 fails the authentication because the authentication methods are incorrect.
B. Spoke 2 passes the authentication to the hub and successfully proceeds to phase 2.
C. Spoke 2 fails the authentication because the remote authentication method is incorrect.
D. Spoke 1 passes the authentication to the hub and successfully proceeds to phase 2.

Answer: A

NEW QUESTION 17
Refer to the exhibit.
An SSL client is connecting to an ASA headend. The session fails with the message “Connection attempt has timed out. Please verify Internet connectivity.”
Based on how the packet is processed, which phase is causing the failure?

A. phase 9: rpf-check
B. phase 5: NAT
C. phase 4: ACCESS-LIST
D. phase 3: UN-NAT

Answer: D

NEW QUESTION 21
Which technology works with IPsec stateful failover?

A. GLBR
B. HSRP
C. GRE
D. VRRP

Answer: B

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/ios/12_2/12_2y/12_2yx11/feature/guide/ft_vpnha.html#wp1122512

NEW QUESTION 25
Which VPN solution uses TBAR?

A. GETVPN
B. VTI
C. DMVPN
D. Cisco AnyConnect

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xe-3s/sec-get-vpn-xe-3s-book/sec-get-vpn.html

NEW QUESTION 29
Which VPN does VPN load balancing on the ASA support?

A. VTI
B. IPsec site-to-site tunnels
C. L2TP over IPsec
D. Cisco AnyConnect

Answer: D

NEW QUESTION 33
Which technology is used to send multicast traffic over a site-to-site VPN?

A. GRE over IPsec on IOS router
B. GRE over IPsec on FTD
C. IPsec tunnel on FTD
D. GRE tunnel on ASA

Answer: B

NEW QUESTION 38
Refer to the exhibit.

```
ip access-list extended CCNP
 permit 192.168.0.10
 permit 192.168.0.11

webvpn gateway SSL_Gateway
 ip address 172.16.0.25 port 443
 ssl trustpoint AnyConnect_Cert
 inservice

webvpn context SSL_Context
 gateway SSL_Gateway

 ssl authenticate verify all
 inservice

policy group SSL_Policy
   functions svc-enabled
   svc address-pool "ACPool" netmask 255.255.255.0
   svc dns-server primary 192.168.0.100
   svc default-domain cisco.com
default-group-policy SSL_Policy
```

Cisco AnyConnect must be set up on a router to allow users to access internal servers 192.168.0.10 and 192.168.0.11. All other traffic should go out of the client's local NIC. Which command accomplishes this configuration?

A. svc split include 192.168.0.0 255.255.255.0
B. svc split exclude 192.168.0.0 255.255.255.0
C. svc split include acl CCNP
D. svc split exclude acl CCNP

Answer: C

NEW QUESTION 43
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

300-730 Practice Exam Features:

* 300-730 Questions and Answers Updated Frequently

* 300-730 Practice Questions Verified by Expert Senior Certified Staff

* 300-730 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 300-730 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year