300-730$^{\text{Q\&As}}$

Implementing Secure Solutions with Virtual Private Networks (SVPN)

Pass Cisco 300-730 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/300-730.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

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

Correct Answer: D

the keyword here (Which feature can update the client to meet an enterprise security policy)

QUESTION 2

A network administrator is troubleshooting a FlexVPN tunnel. The hub router is unable to ping the spoke router\\'s tunnel interface IP address of 192.168.1.2, even though the tunnel is showing up. The output of the debug ip packet CLI command on the hub router shows the following entry.

IP: tableid=0123456789 s=192.168.1.1 (local), d=192.168.1.2 (loopback2), routed via FIB.

What must be configured to fix this issue?

A. A matching IKEv2 pre-shared key on the hub and spoke routers in the crypto keyring configuration.

B. An outbound ACL on the dynamic VTI of the hub router that allows ICMP traffic to 192.168.1.2.

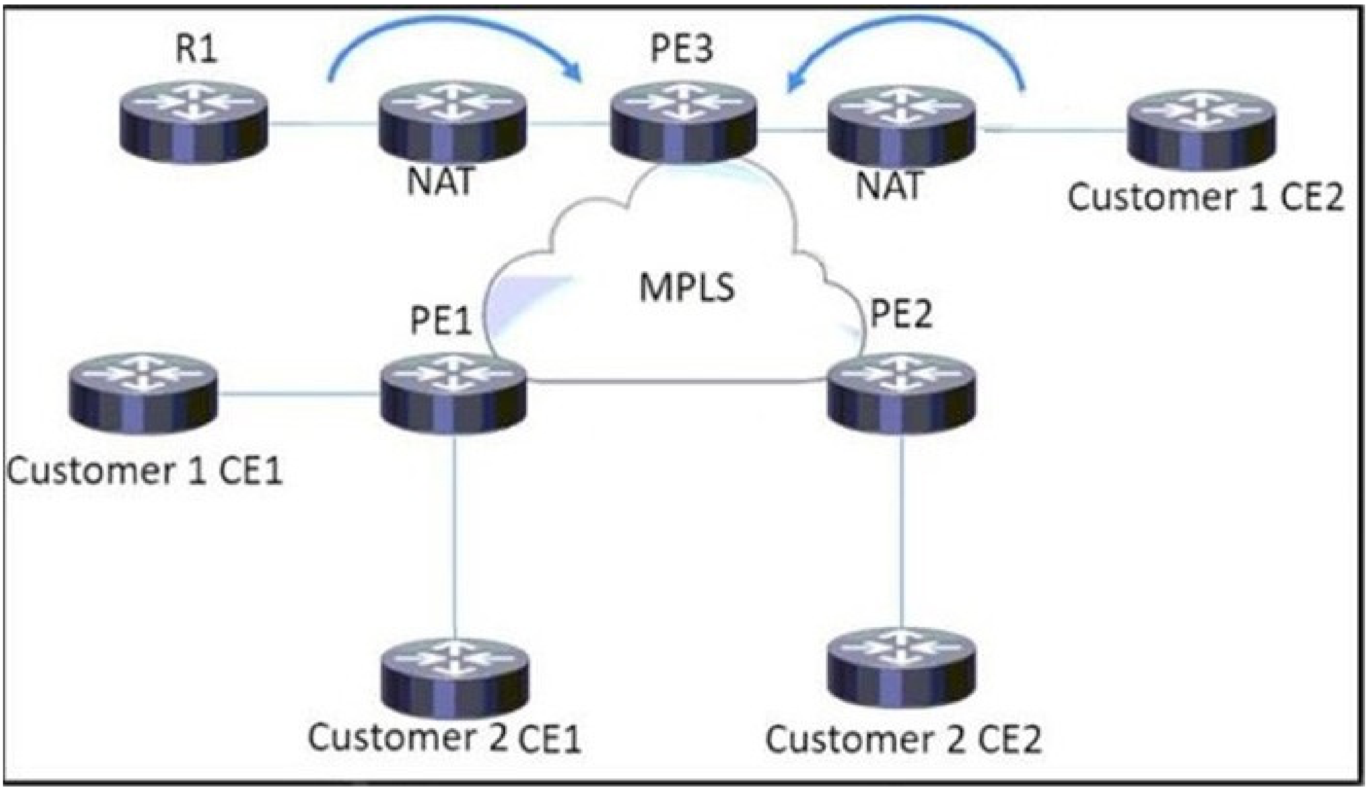
C. An IKEv2 authorization policy must be configured on the spoke router to advertise the interface route.

D. A route map must be configured on hub router to set the next hop for 192.168.1.2 to the dynamic VTI.

Correct Answer: C

QUESTION 3

Refer to the exhibit.



Which component must be configured on routers for a GETVPN deployment work properly?

A. PE3: Key Server ?Customer 2 CEs: Group Members

B. Customer 1 CE1: Key Server ?R1 and Customer 1 CE2: Group Members

C. R1: Key Server ?Customer 1 CEs: Group Members

D. PE3: Key Server ?all CEs: Group Members

Correct Answer: A

QUESTION 4

An administrator is setting up AnyConnect for the first time for a few users. Currently, the router does not have access to a RADIUS server. Which AnyConnect protocol must be used to allow users to authenticate?

A. EAP-GTC

B. EAP-MSCHAPv2

C. EAP-MD5

D. EAP-AnyConnect

Correct Answer: D

QUESTION 5

Which clientless SSLVPN supported feature works when the http-only-cookie command is enabled?

A. Citrix load balancer

B. port reflector

C. Java rewriter

D. script browser

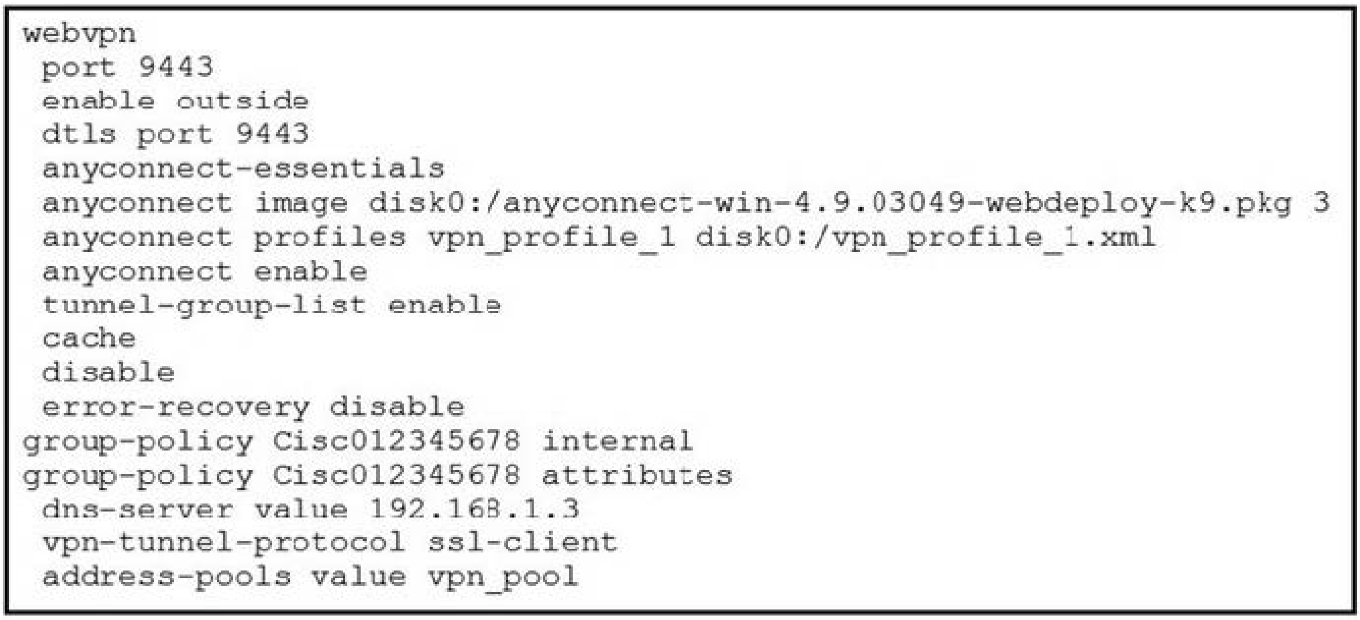
E. Java plug-ins

Correct Answer: D

The following Clientless SSL VPN features will not work when the http-only-cookie command is enabled: ?Java plug-ins ?Java rewriter ?Port forwarding ?File browser ?Sharepoint features that require desktop applications (for example, MS Office applications) ?AnyConnect Web launch ?Citrix Receiver, XenDesktop, and Xenon ?Other non-browser-based and browser plugin-based applications

QUESTION 6

Refer to the exhibit.



```
webvpn
 port 9443
 enable outside
 dtls port 9443
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.9.03049-webdeploy-k9.pkg 3
 anyconnect profiles vpn_profile_1 disk0:/vpn_profile_1.xml
 anyconnect enable
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
group-policy Cisc012345678 internal
group-policy Cisc012345678 attributes
 dns-server value 192.168.1.3
 vpn-tunnel-protocol ssl-client
 address-pools value vpn_pool
```

Which type of Cisco VPN is shown for group Cisc012345678?

A. Cisco AnyConnect Client VPN

B. DMVPN

C. Clientless SSLVPN

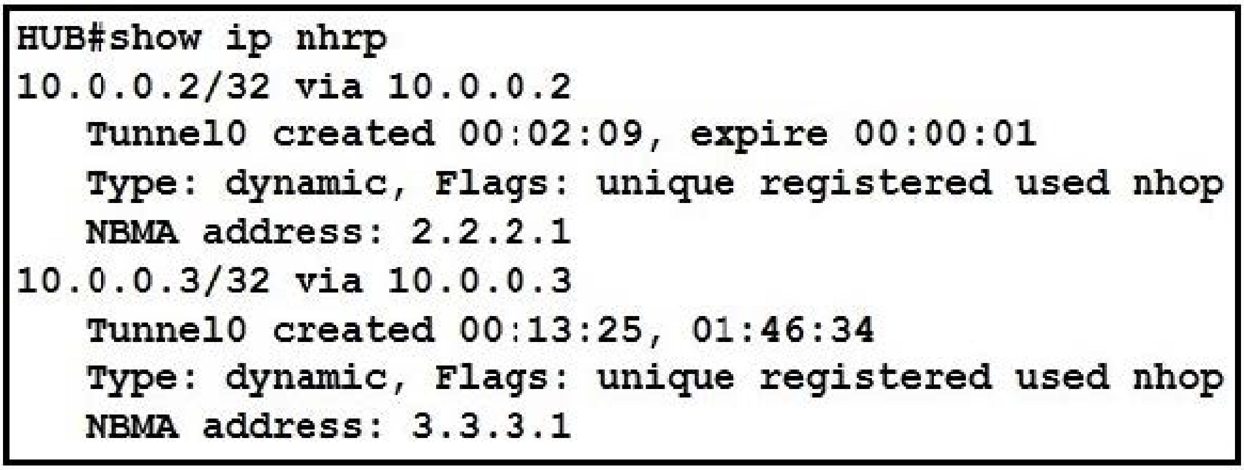
D. GETVPN

Correct Answer: A

It is stated client-vpn as the vpn-tunnel-protocol.

QUESTION 7

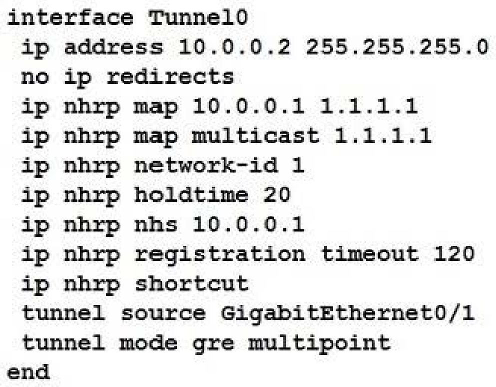
Refer to the exhibit.



```
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
```

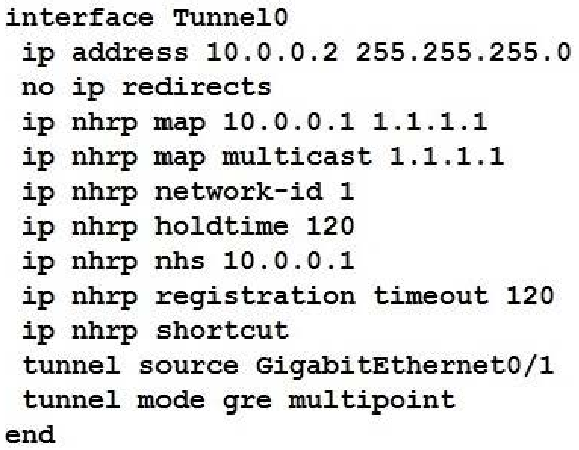
The DMVPN tunnel is dropping randomly and no tunnel protection is configured. Which spoke configuration mitigates tunnel drops?

A.



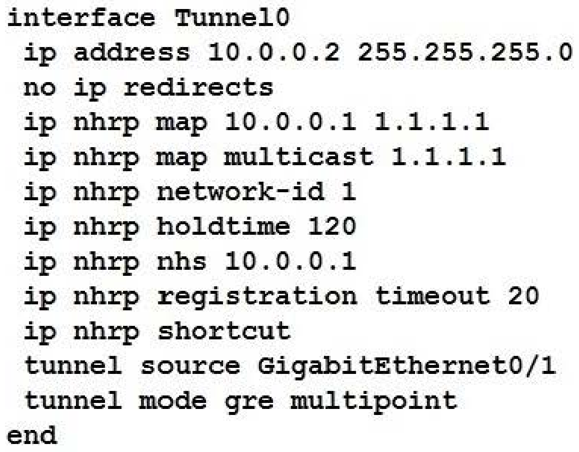
```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 20
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 120
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre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

B.



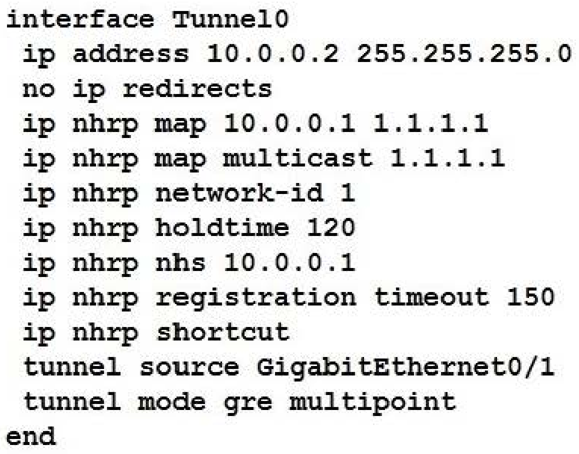
```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip nhrp map 10.0.0.1 1.1.1.1
 ip nhrp map multicast 1.1.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 120
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1
 tunnel mode gre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

Correct Answer: C

QUESTION 8

An engineer has configured Cisco AnyConnect VPN using IKEv2 on a Cisco IOS router. The user cannot connect in the Cisco AnyConnect client, but receives an alert message "Use a browser to gain access." Which action does the engineer take to resolve this issue?

A. Reset user login credentials.

B. Correct the URL address.

C. Connect using HTTPS.

D. Disable the HTTP server.

Correct Answer: D

QUESTION 9

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

Correct Answer: AE

"NOTE You will not see an option of RDP, VNC, SSH, and/or Telnet unless the appropriate client/server plug-in has been installed first. " Leaves only HTTP and CIFS as your options.

QUESTION 10

A router is being configured for IKEv2 AnyConnect using AnyConnect-EAP. How would the administrator separate profiles for administrators and employees so that authorization differs when they connect?

A. Define group aliases on the headend and have the user pick the appropriate alias when they connect

B. Define group-urls on the headend and create two XML profiles to match the administrator and user group urls

C. Create a certificate map and match on the appropriate certificate fields

D. Define key-ids on the headend and create two XML profiles to match the administrator and user key-ids.

Correct Answer: D

QUESTION 11

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.

Correct Answer: C

On ASDM, under connection profile -> access interfaces -> IPSEC (IKEv2) Access : you can check or uncheck the boxes for "allow access" and "enable client access"

QUESTION 12

An engineer must investigate a connectivity issue and decides to use the packet capture feature on Cisco FTD. The goal is to see the real packet going through the Cisco FTD device and see Snort detection actions as a part of the output. After the capture-traffic command is issued, only the packets are displayed. Which action resolves this issue?

A. Specify the trace using the -T option after the capture-traffic command

B. Perform the trace within the Cisco FMC GUI instead of the Cisco FMC CLI

C. Use the verbose option as a part of the capture-traffic command

D. Use the capture command and specify the trace option to get the required information

Correct Answer: A

The correct answer is A. Specify the trace using the -T option after the capture-traffic command. According to the document Use Firepower Threat Defense Captures and Packet Tracer, the capture-traffic command allows you to capture packets on the Snort engine domain of the FTD device. However, by default, it only shows the packet headers and does not include the Snort detection actions. To see the Snort detection actions, you need to use the -T option, which enables tracing. For example: capture-traffic -T This will show the packet headers along with the Snort verdicts, such as allow, block, or replace. You can also use other options to filter or save the capture output1.

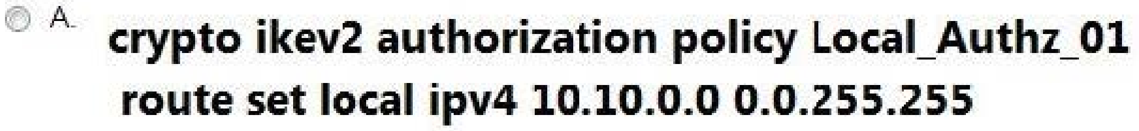
B. Performing the trace within the Cisco FMC GUI instead of the Cisco FMC CLI is not a valid option, because the FMC GUI does not support packet capture or tracing on the FTD device. You can only use the FMC GUI to view and export captures that are taken on the FTD CLI1.

C. Using the verbose option as a part of the capture-traffic command is not a valid option, because there is no verbose option for this command. The verbose option is only available for the capture command, which is used to capture packets on the LINA engine domain of the FTD device1.

D. Using the capture command and specifying the trace option to get the required information is not a valid option, because the capture command does not have a trace option. The capture command allows you to capture packets on the LINA engine domain of the FTD device, but it does not show the Snort detection actions. The trace option is only available for the packet-tracer command, which is used to simulate a packet going through the FTD device and show its processing steps1.

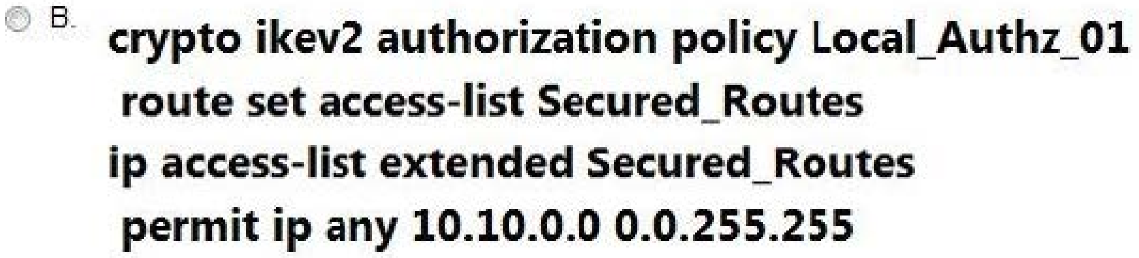
QUESTION 13

An engineer would like Cisco AnyConnect users to be able to reach servers within the 10.10.0.0/16 subnet while all other traffic is sent out to the Internet. Which IPsec configuration accomplishes this task?



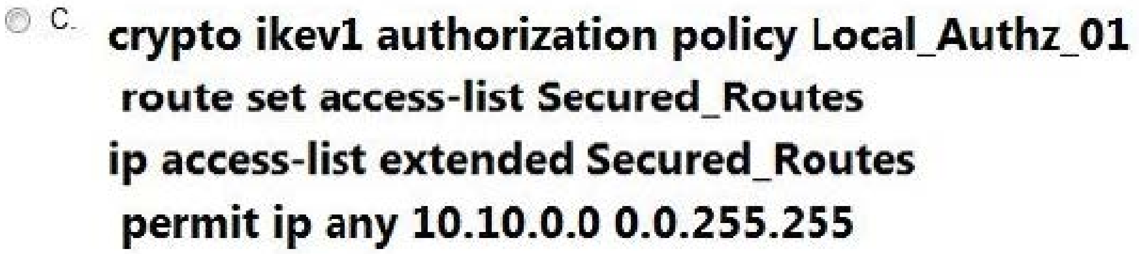
○ A.

```
crypto ikev2 authorization policy Local_Authz_01
 route set local ipv4 10.10.0.0 0.0.255.255
```



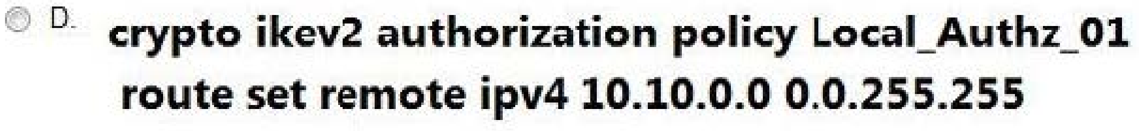
○ B.

```
crypto ikev2 authorization policy Local_Authz_01
 route set access-list Secured_Routes
ip access-list extended Secured_Routes
 permit ip any 10.10.0.0 0.0.255.255
```



○ C.

```
crypto ikev1 authorization policy Local_Authz_01
 route set access-list Secured_Routes
ip access-list extended Secured_Routes
 permit ip any 10.10.0.0 0.0.255.255
```



○ D.

```
crypto ikev2 authorization policy Local_Authz_01
 route set remote ipv4 10.10.0.0 0.0.255.255
```

A. Option A

B. Option B

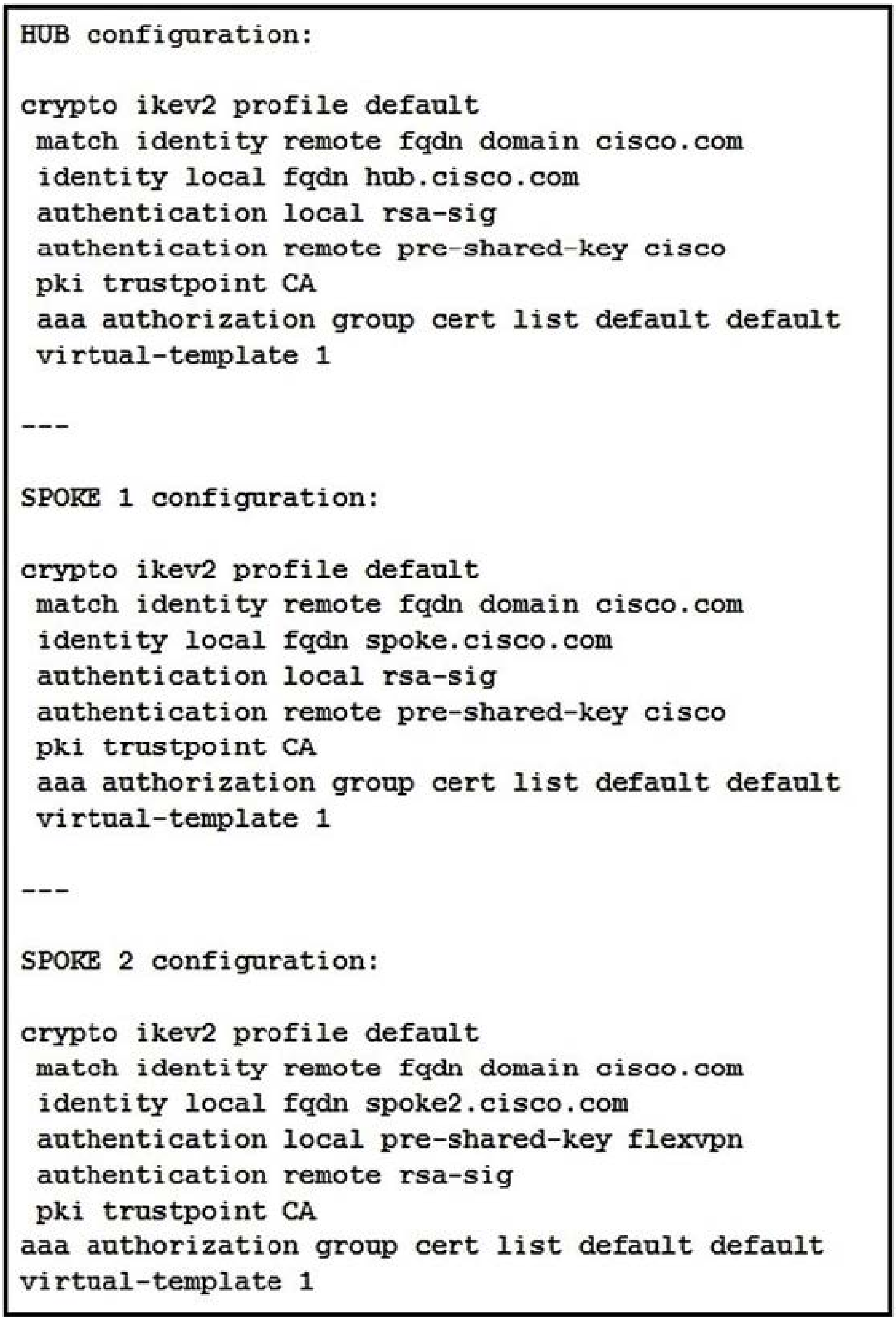
C. Option C

D. Option D

Correct Answer: B

QUESTION 14

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.

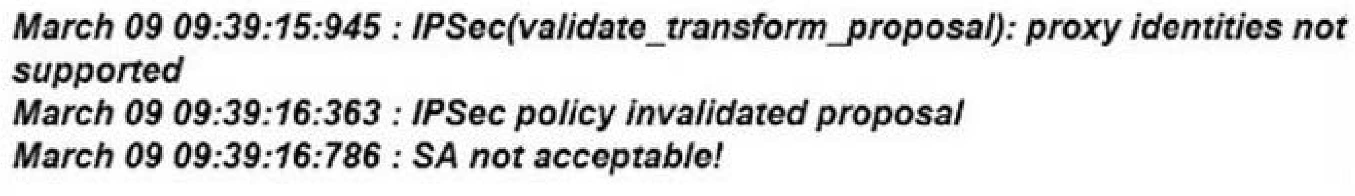
C. Spoke 2 fails the authentication because the remote authentication method is incorrect.

D. Spoke 1 passes the authentication to the hub and successfully proceeds to phase 2.

Correct Answer: A

QUESTION 15

Refer to the exhibit.



```
March 09 09:39:15:945 : IPSec(validate_transform_proposal): proxy identities not
supported
March 09 09:39:16:363 : IPSec policy invalidated proposal
March 09 09:39:16:786 : SA not acceptable!
```

Which action must be taken on the IPsec tunnel configuration to resolve the issue?

A. The access lists on each peer must mirror each other.

B. The transform set on each peer must match.

C. The access lists on each peer must be identical.

D. The transform set on each peer must be compatible.

Correct Answer: A

Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html