RealTest.300-209.137Questions

VCEplus.com

Number: 300-209
Passing Score: 800
Time Limit: 120 min
File Version: 6.3

Implementing Cisco Secure Mobility Solutions

- Excellent Questions, I pass with 90% with these questions. Guys just read this only.
- Added Explanations and Exhibits most of the questions.
- Modified few questions, fixed few spelling mistakes and typos.
- Nicely written Questions with many corrections inside.

Exam A

QUESTION 1
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A company has decided to migrate an existing IKEv1 VPN tunnel to IKEv2. 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
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
Section: (none)
Explanation

Explanation/Reference:
Hello - here is a reference an explanation that can be included with this test.

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-flex- spoke.html#GUID-4A10927D-4C6A-4202-B01C-DA7E462F5D8A

Configuring the Virtual Tunnel Interface on FlexVPN Spoke

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 7
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 to directly communicating with each other
D. It makes sure that each VPN spoke directly communicates with the hub

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
answer is verified

QUESTION 8
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
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
Section: (none)

Explanation

Explanation/Reference:

QUESTION 12
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Refer to the exhibit.

```
crypto pki certificate map CERTMAP
subject-name co cn=cisco.com
crypto ikev2 profile IKEPROFILE
authentication local pre-share
authentication remote rsa-sig
keyring local KEYRING1
match identity remote address 209.165.200.225 255.255.255.255
match identity remote address 209.165.202.155 255.255.255.255
match certificate CERTMAP
pki trustpoint TRUSTPOINT1
```

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
Section: (none)
Explanation

Explanation/Reference:
answer is accurated

QUESTION 16
Which three settings are required for crypto map configuration? (Choose three.)

A. match address
B. set peer
C. set transform-set
D. set security-association lifetime
E. set security-association level per-host
F. set pfs

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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
Section: (none)
Explanation

Explanation/Reference:
The reference:
http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect20/administrati ve/guide/admin/admin5.html

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 20
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
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 l2l
D. migrate remote-access ssl

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Below is a reference for this question:
http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation- firewalls/113597-ptn-113597.html

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 {l2l | remote-access {ikev2 | ssl} | overwrite} Things of note:

Keyword definitions:

l2l - This converts current IKEv1 l2l 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 26
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
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 1234 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
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
encryption aes 254
B. crypto isakmp policy 10
encryption aes 192
C. crypto isakmp policy 10
encryption aes 256
D. crypto isakmp policy 10
encryption aes 196
E. crypto isakmp policy 10
encryption aes 199
F. crypto isakmp policy 10
encryption aes 64

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
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
Section: (none)
Explanation

Explanation/Reference:
answer is modified

QUESTION 41
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

Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
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
Section: (none)
Explanation

Explanation/Reference:
http://www.cisco.com/c/en/us/support/docs/security/ssl-vpn-client/70664-IOSthinclient.html 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, SSH, 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 50
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Which protocol supports high availability in a Cisco IOS SSL VPN environment?

A. HSRP
B. VRRP
C. GLBP
D. IRDP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which hash algorithm is required to protect classified information?

A. MD5
B. SHA-1

C. SHA-256
D. SHA-384

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which algorithm is replaced by elliptic curve cryptography in Cisco NGE?

A. 3DES
B. AES
C. DES
D. RSA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
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: A
Section: (none)
Explanation

Explanation/Reference:
answer is updated

QUESTION 59
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-network-list splitlist

E. crypto anyconnect vpn-tunnel-policy tunnelspecified crypto anyconnect split-tunnel-network-list ipv4 1 209.165.201.0 255.255.255.224 crypto anyconnect split-tunnel-network-list ipv4 2 209.165.202.128 255.255.255.224

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
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
Section: (none)

Explanation

Explanation/Reference:

QUESTION 67
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
Section: (none)
Explanation

Explanation/Reference:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/T- Z/cmdref4/v.html#pgfId-1842564

QUESTION 68
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69

Instructions

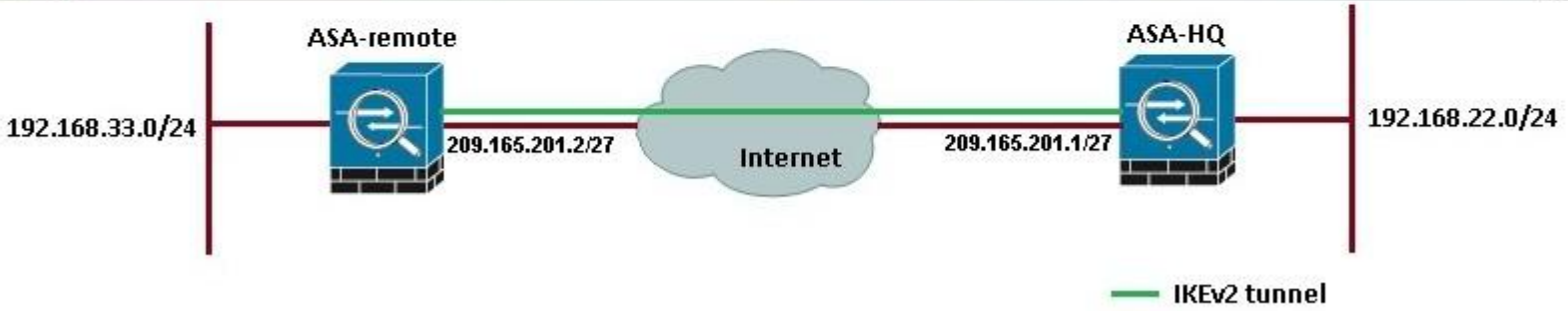
Click the grey buttons at the bottom of this frame to view the different windows.

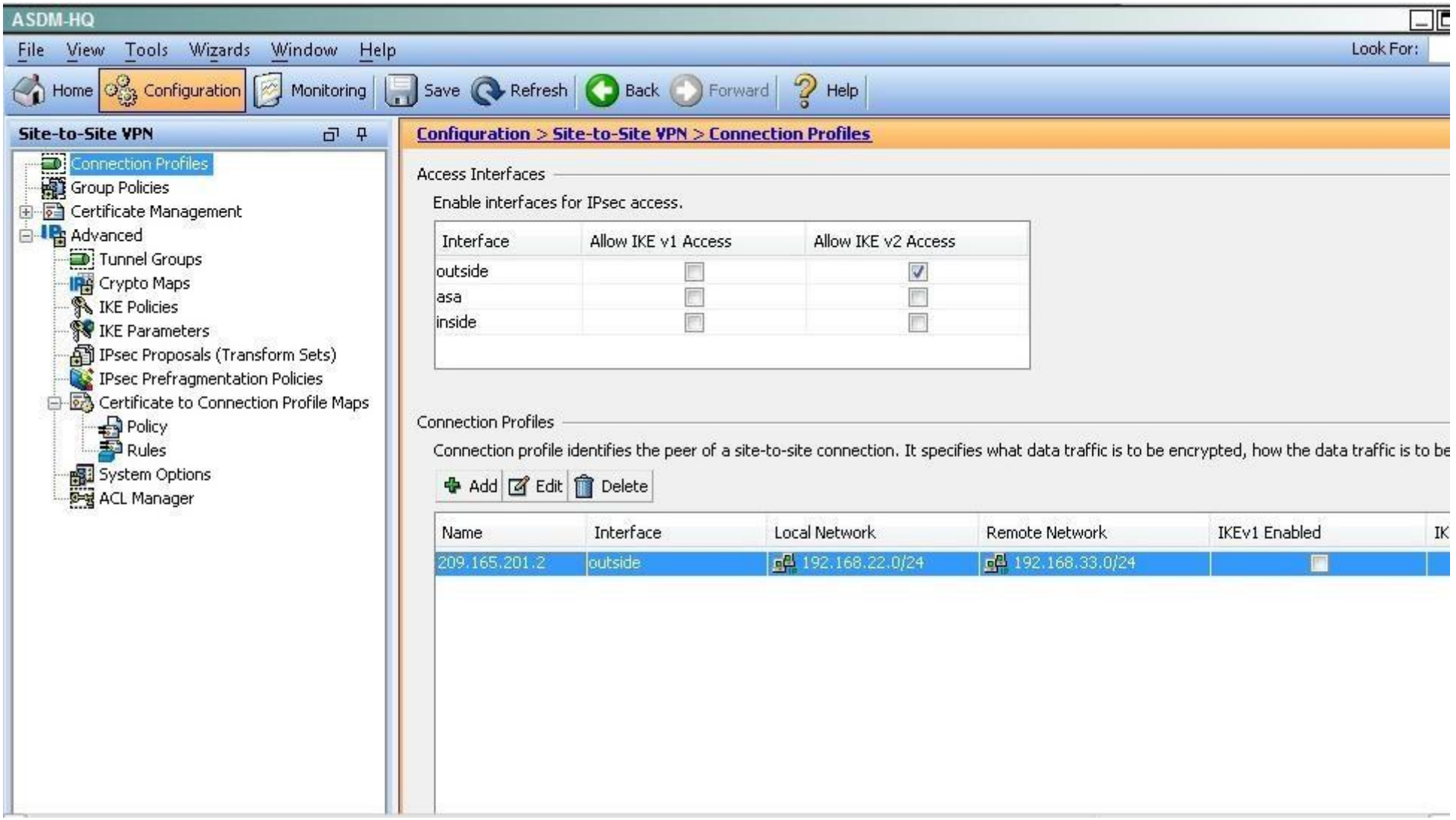
Windows can be minimized and repositioned. You can also reposition a window by dragging it by the title bar.

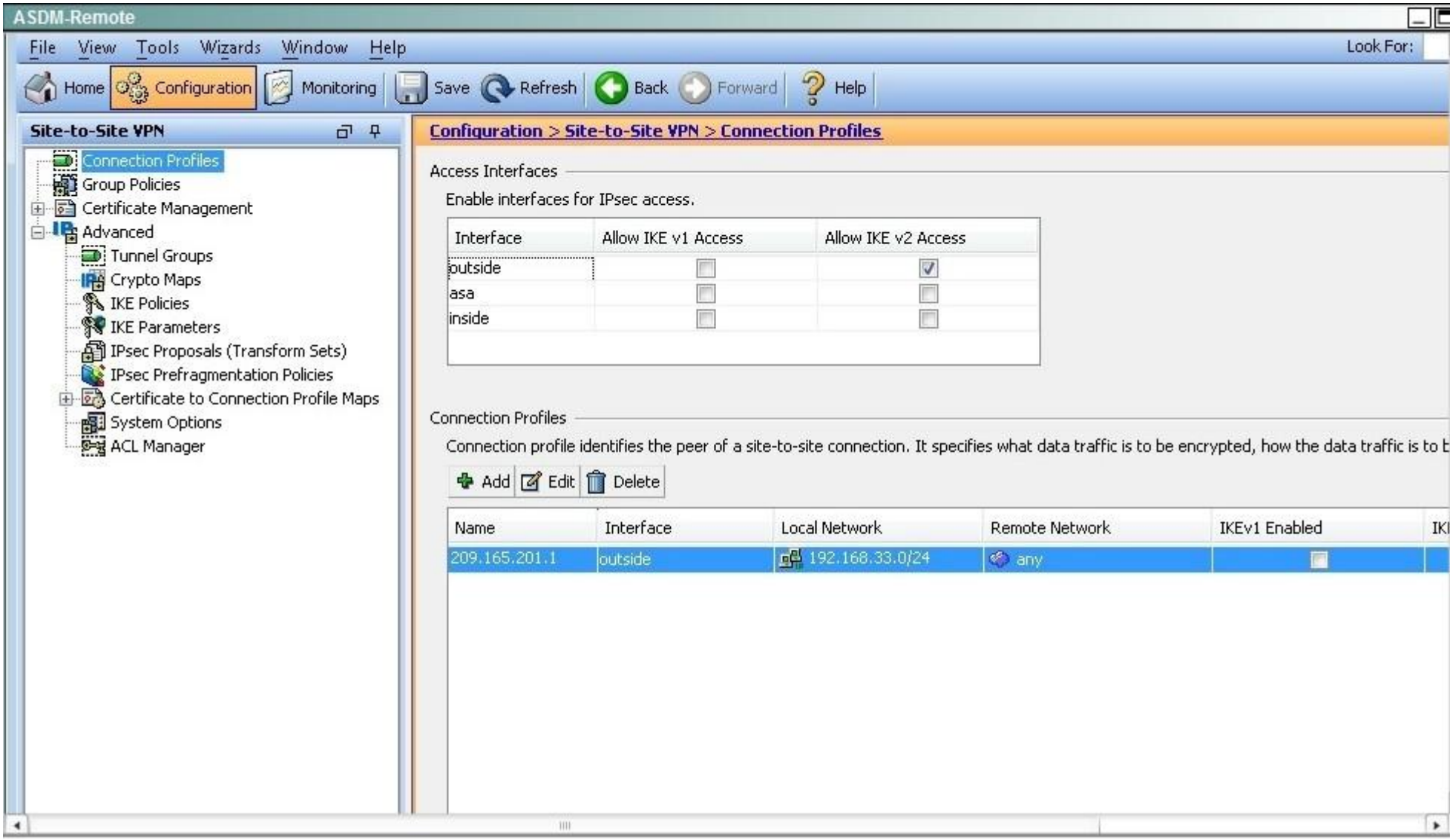
Scenario

A network administrator has been tasked with implementing an IKEv2 tunnel from a remote site to a headquarter 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.

Topology




ASDM-HQ
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Site-to-Site VPN
Connection Profiles
Group Policies
Certificate Management
Advanced
Tunnel Groups
Crypto Maps
IKE Policies
IKE Parameters
IPsec Proposals (Transform Sets)
IPsec Prefragmentation Policies
Certificate to Connection Profile Maps
Policy
Rules
System Options
ACL Manager
Configuration > Site-to-Site VPN > Connection Profiles
Access Interfaces
Enable interfaces for IPsec access.
Interface
Allow IKE v1 Access
Allow IKE v2 Access
outside
asa
inside
Connection Profiles
Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be
Add Edit Delete
Name
Interface
Local Network
Remote Network
IKEv1 Enabled
IK
209.165.201.2
outside
192.168.22.0/24
192.168.33.0/24



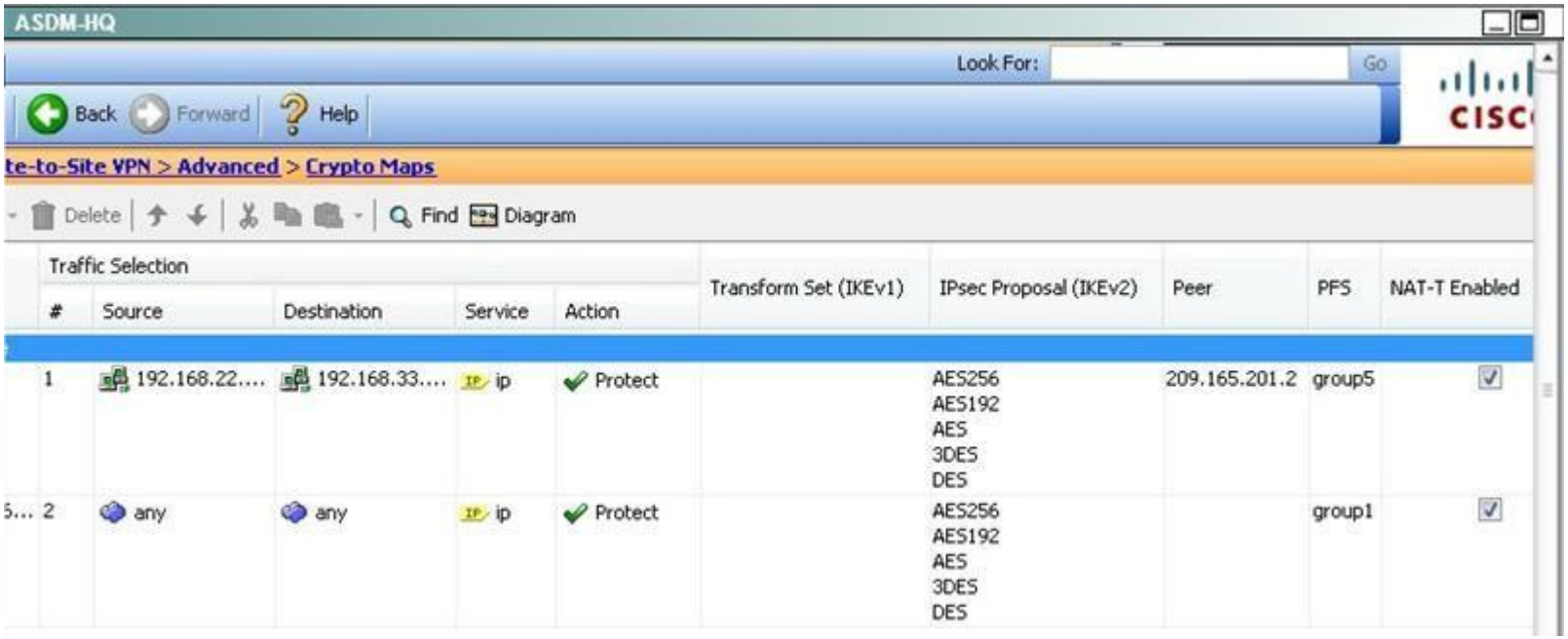
When a tunnel is initiated by the headquarter ASA, which one of the following Diffie-Hellman groups is selected by the headquarter ASA during CREATE_CHILD_SA exchange?

A. 1

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Traffic initiated by the HQ ASA is assigned to the static outside crypto map, which shown below to use DH group 5.



QUESTION 70

Instructions

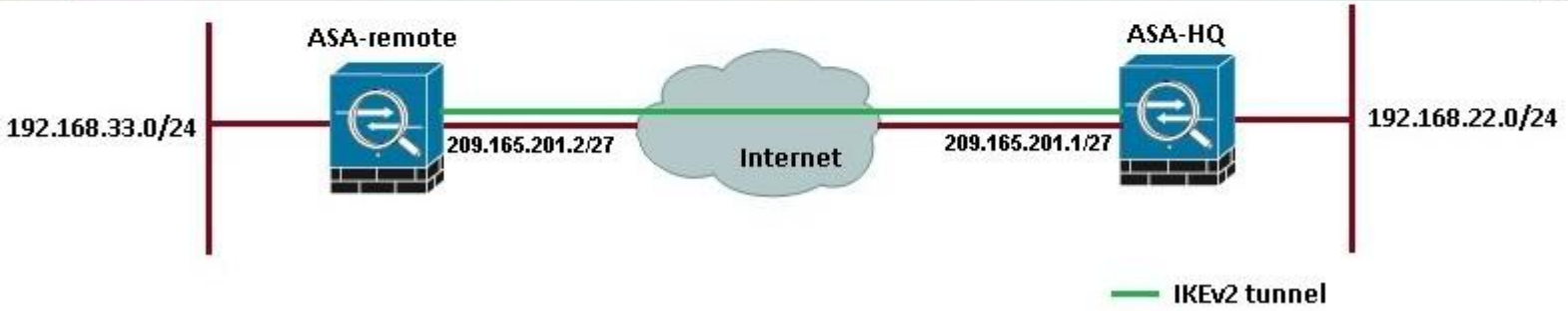
Click the grey buttons at the bottom of this frame to view the different windows.

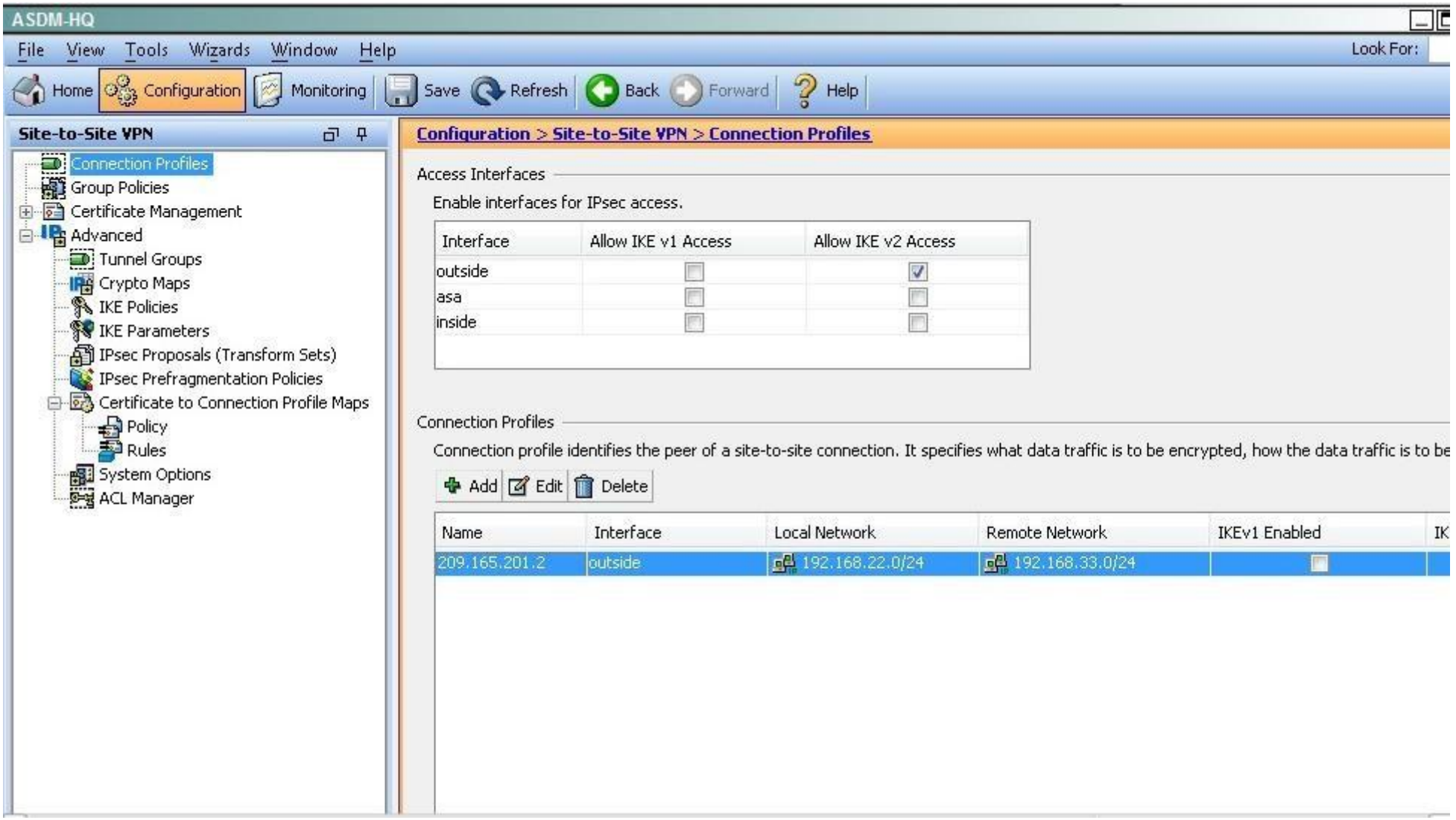
Windows can be minimized and repositioned. You can also reposition a window by dragging it by the title bar.

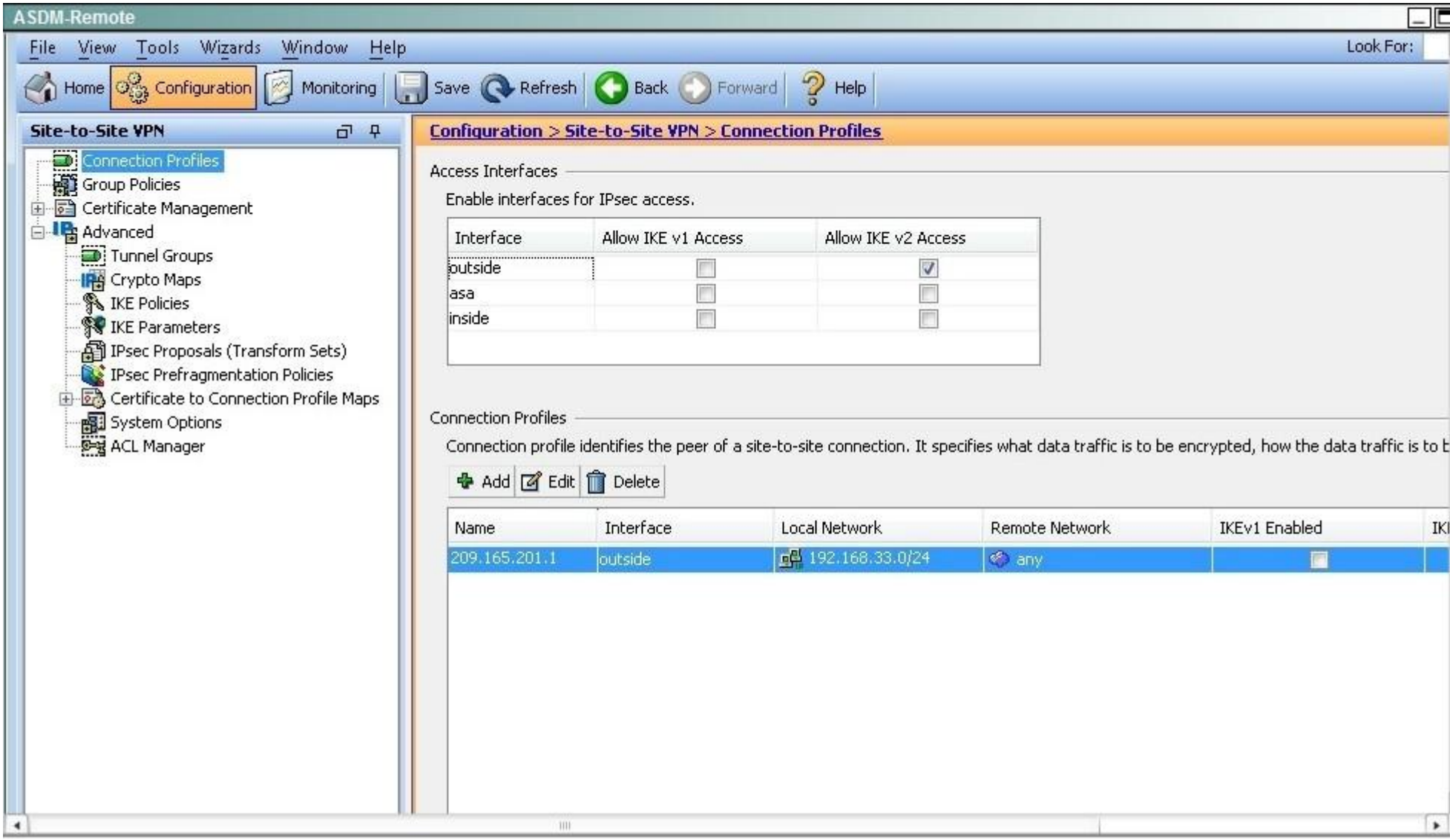
Scenario

A network administrator has been tasked with implementing an IKEv2 tunnel from a remote site to a headquarter 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.

Topology







Based on the provided ASDM configuration for the remote ASA, which one of the following is correct?

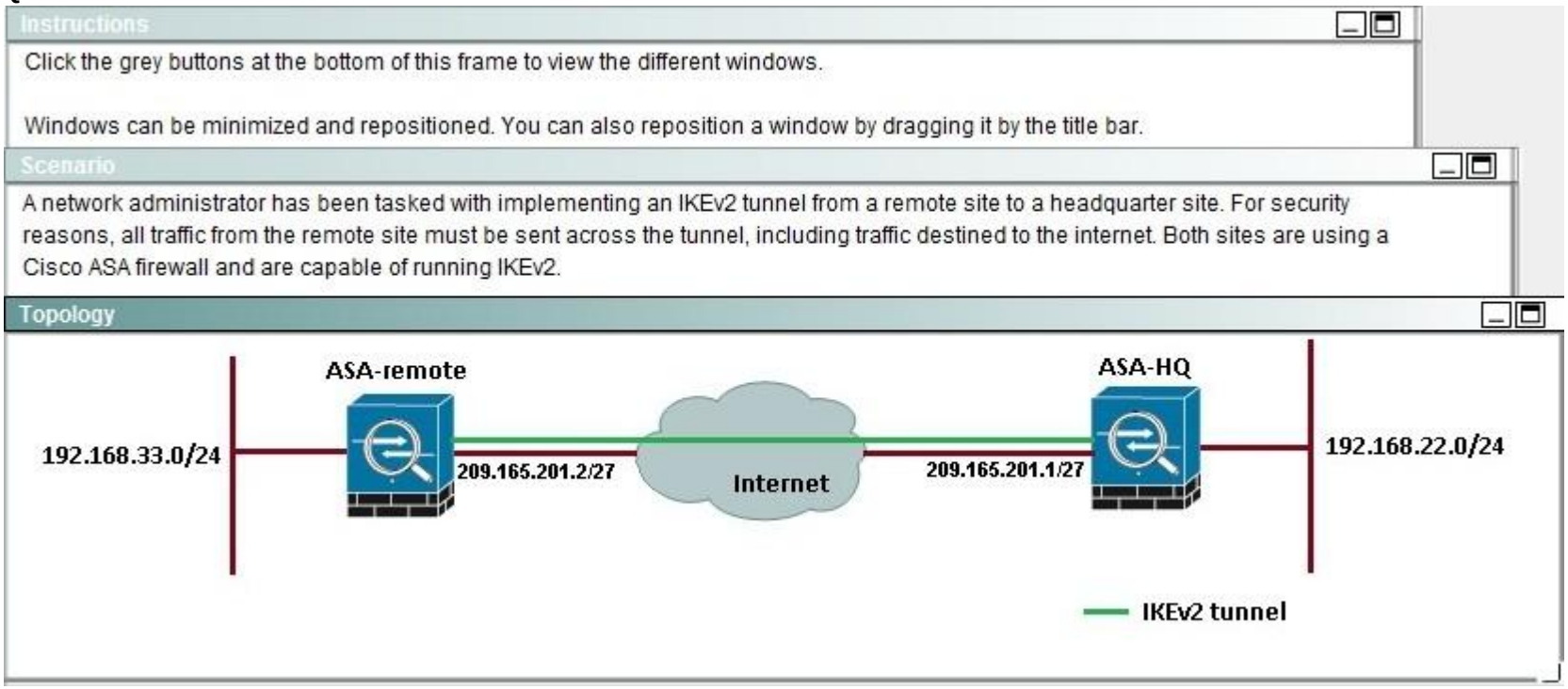
A. An access-list must be configured on the outside interface to permit inbound VPN traffic
B. A route to 192.168.22.0/24 will not be automatically installed in the routing table

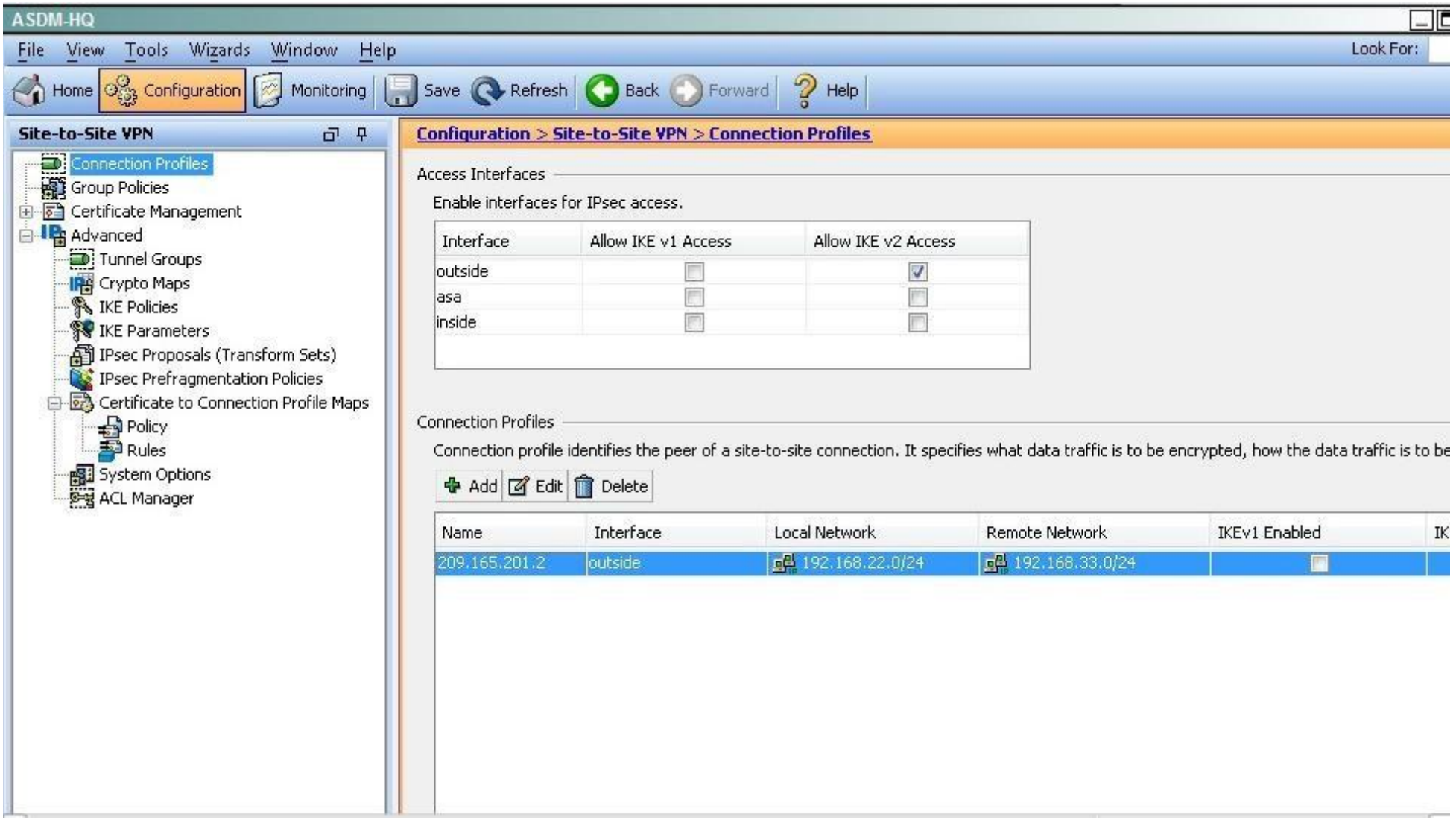
C. The ASA will use a window of 128 packets (64x2) to perform the anti-replay check _
D. The tunnel can also be established on TCP port 10000

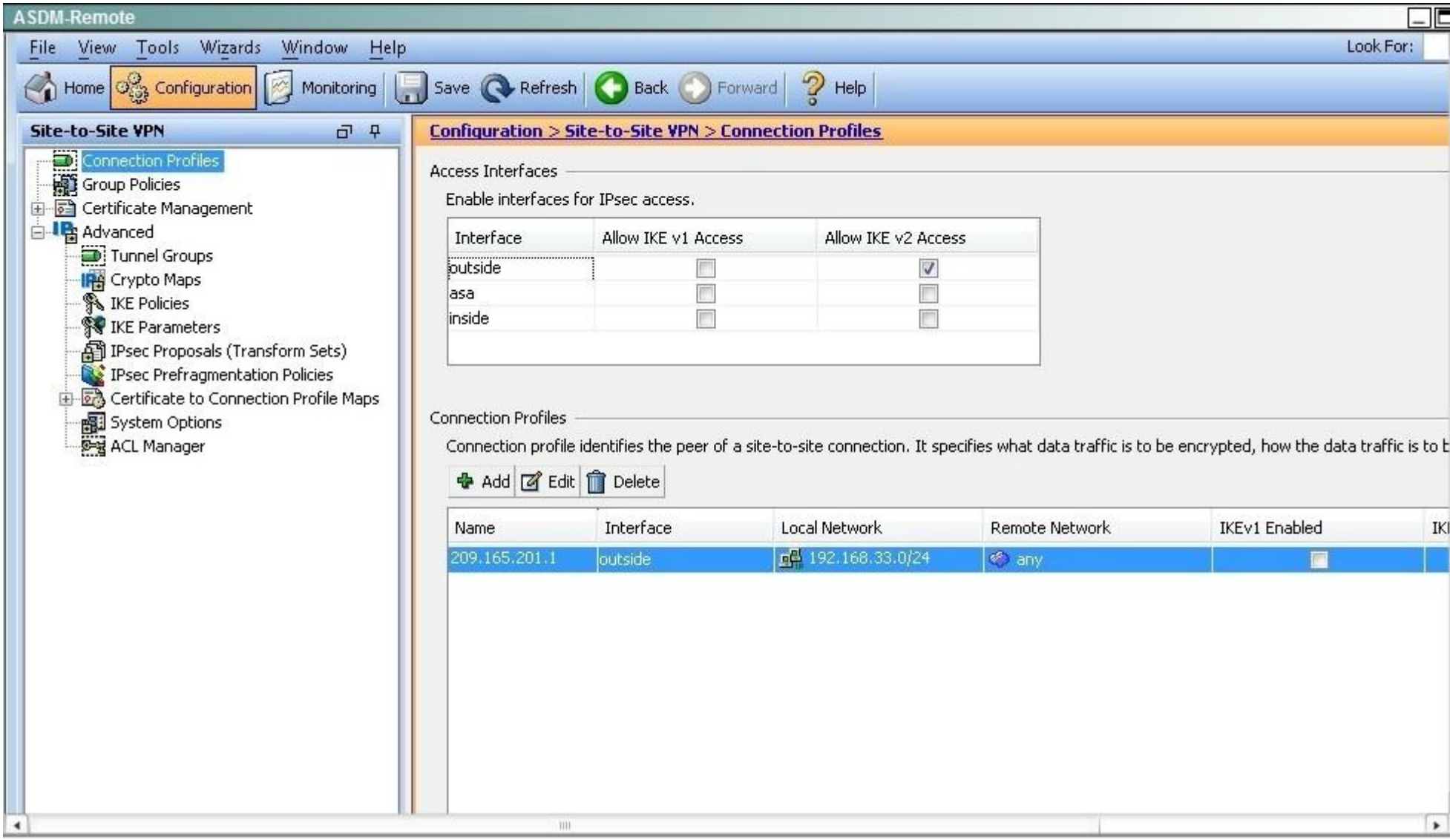
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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 71







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

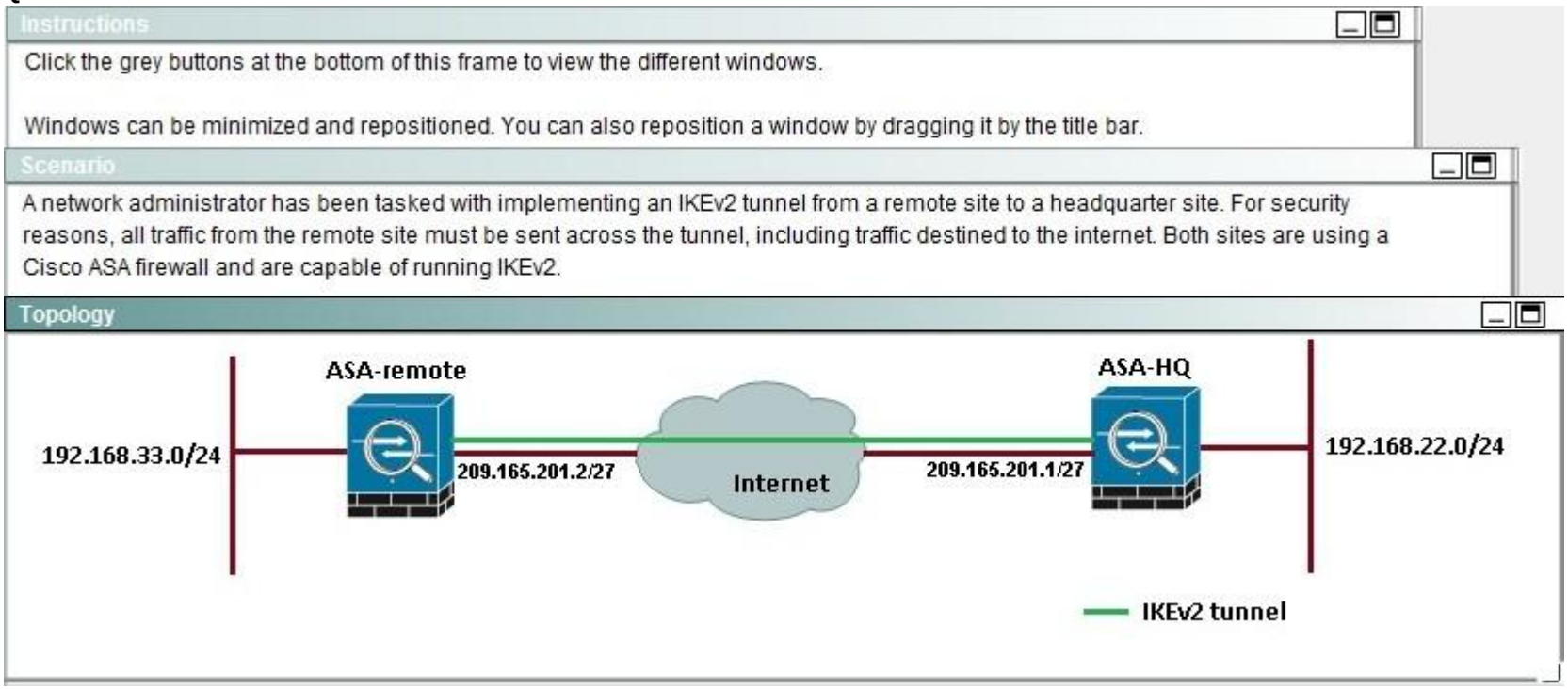
A. DES
B. 3DES

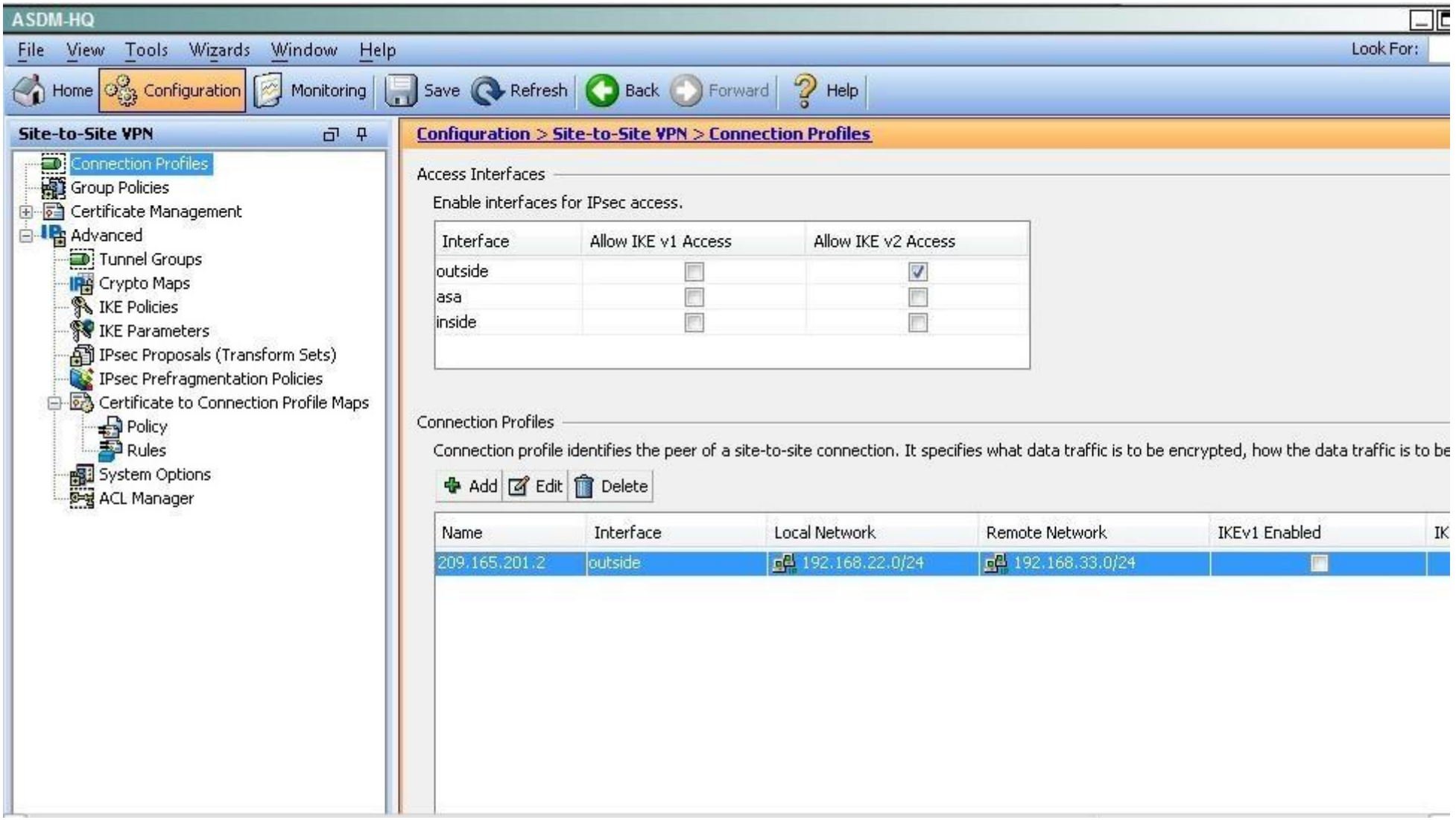
C. AES
D. AES192
E. AES256

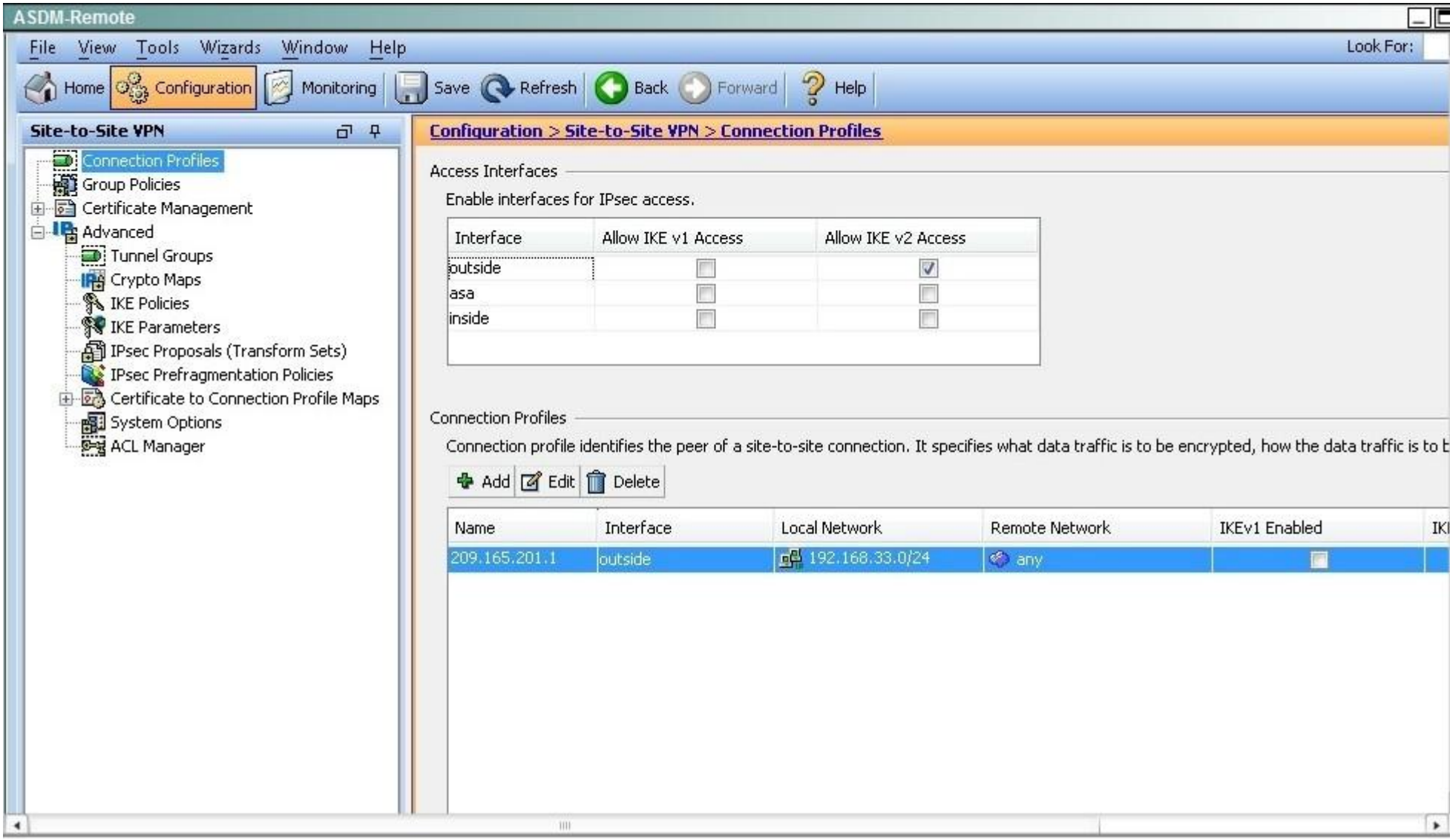
Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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 72




ASDM-HQ
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Site-to-Site VPN
Connection Profiles
Group Policies
Certificate Management
Advanced
Tunnel Groups
Crypto Maps
IKE Policies
IKE Parameters
IPsec Proposals (Transform Sets)
IPsec Prefragmentation Policies
Certificate to Connection Profile Maps
Policy
Rules
System Options
ACL Manager
Configuration > Site-to-Site VPN > Connection Profiles
Access Interfaces
Enable interfaces for IPsec access.
Interface
Allow IKE v1 Access
Allow IKE v2 Access
outside
asa
inside
Connection Profiles
Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be
Add Edit Delete
Name
Interface
Local Network
Remote Network
IKEv1 Enabled
IK
209.165.201.2
outside
192.168.22.0/24
192.168.33.0/24



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?

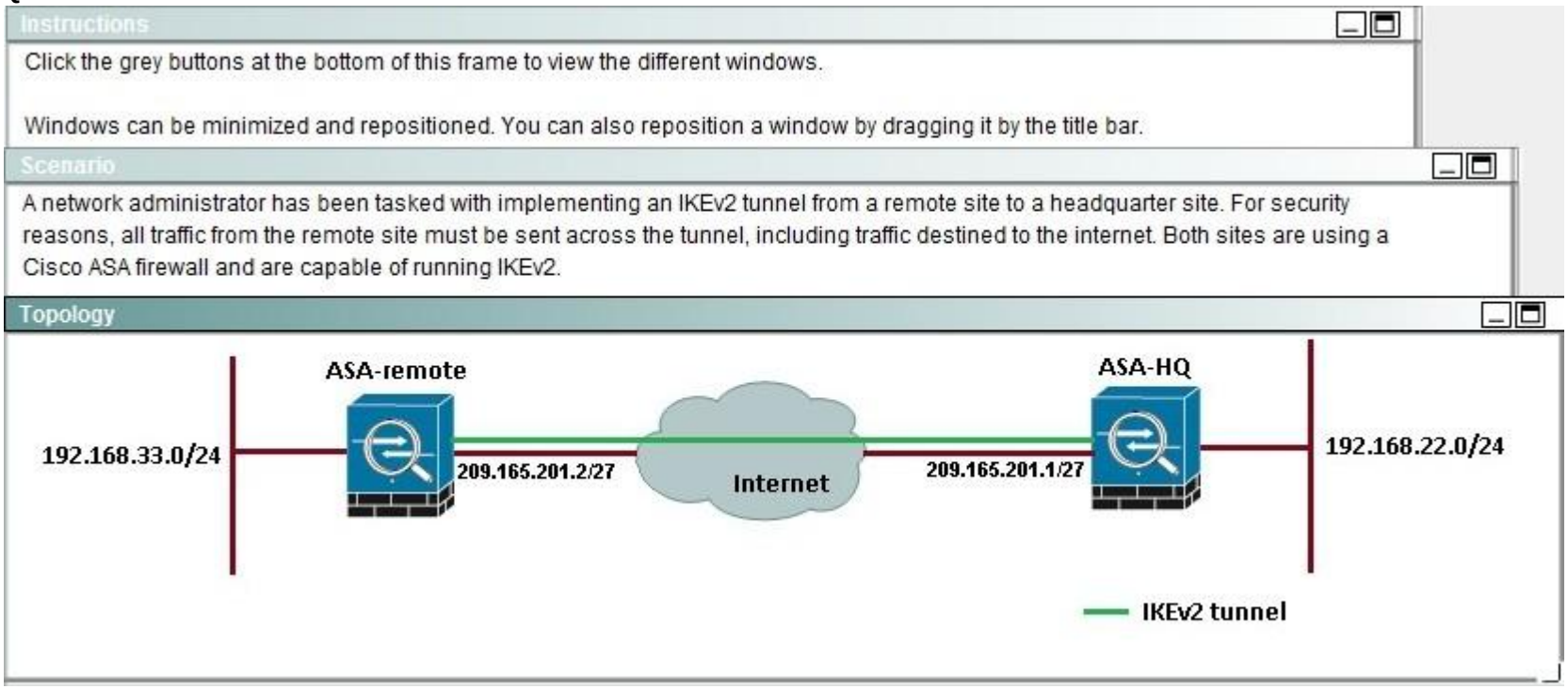
A. Change the Diffie-Hellman group on the headquarter ASA to group5forthe dynamic crypto map

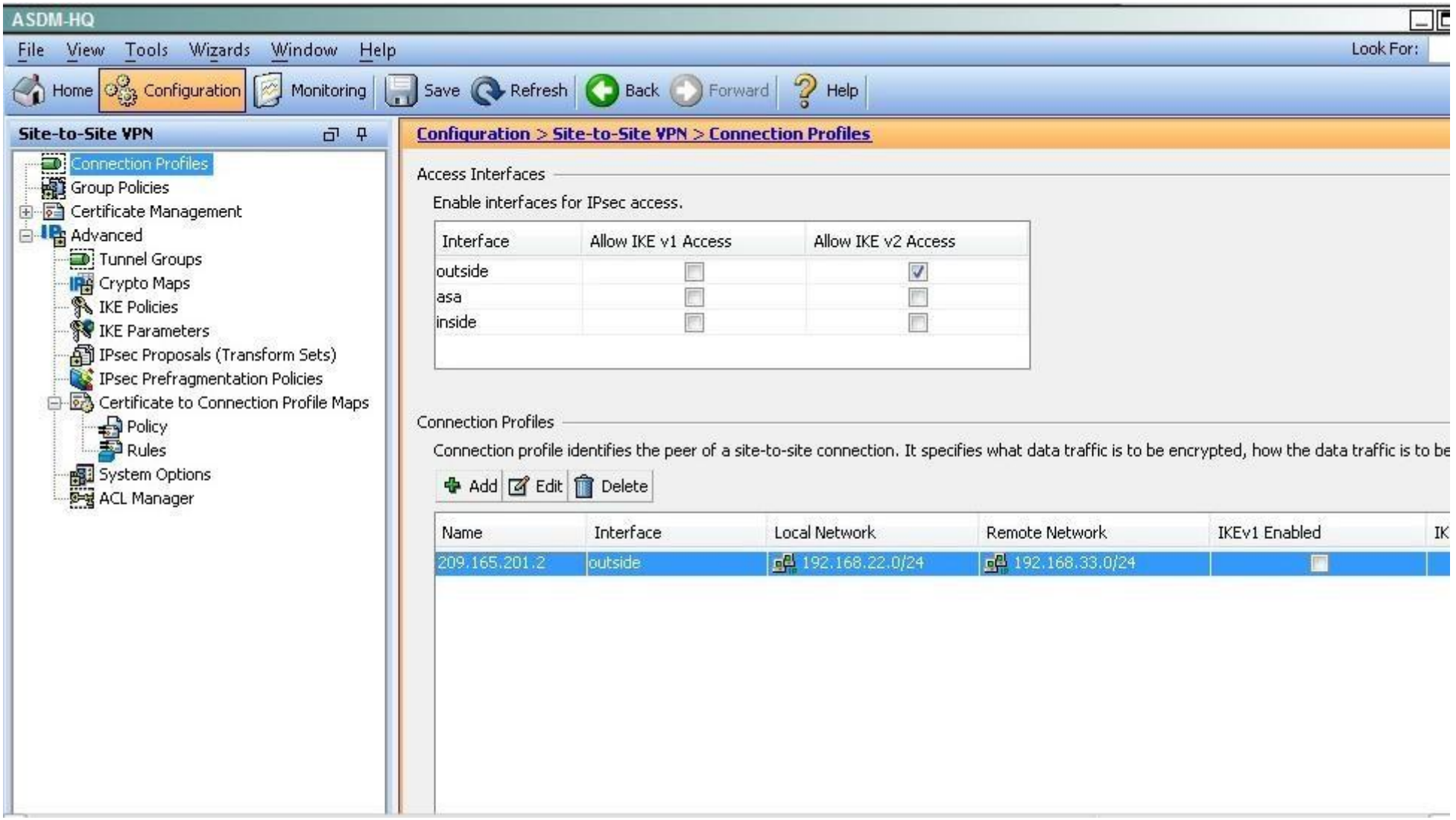
B. Change the remote traffic selector on the remote ASA to 192.168.22.0/24
C. Change to an IKEvI configuration since IKEv2 does not support a full tunnel with static peers
D. Change the local traffic selector on the headquarter ASA to 0.0.0.0/0
E. Change the remote traffic selector on the headquarter ASA to 0.0.0.0/0

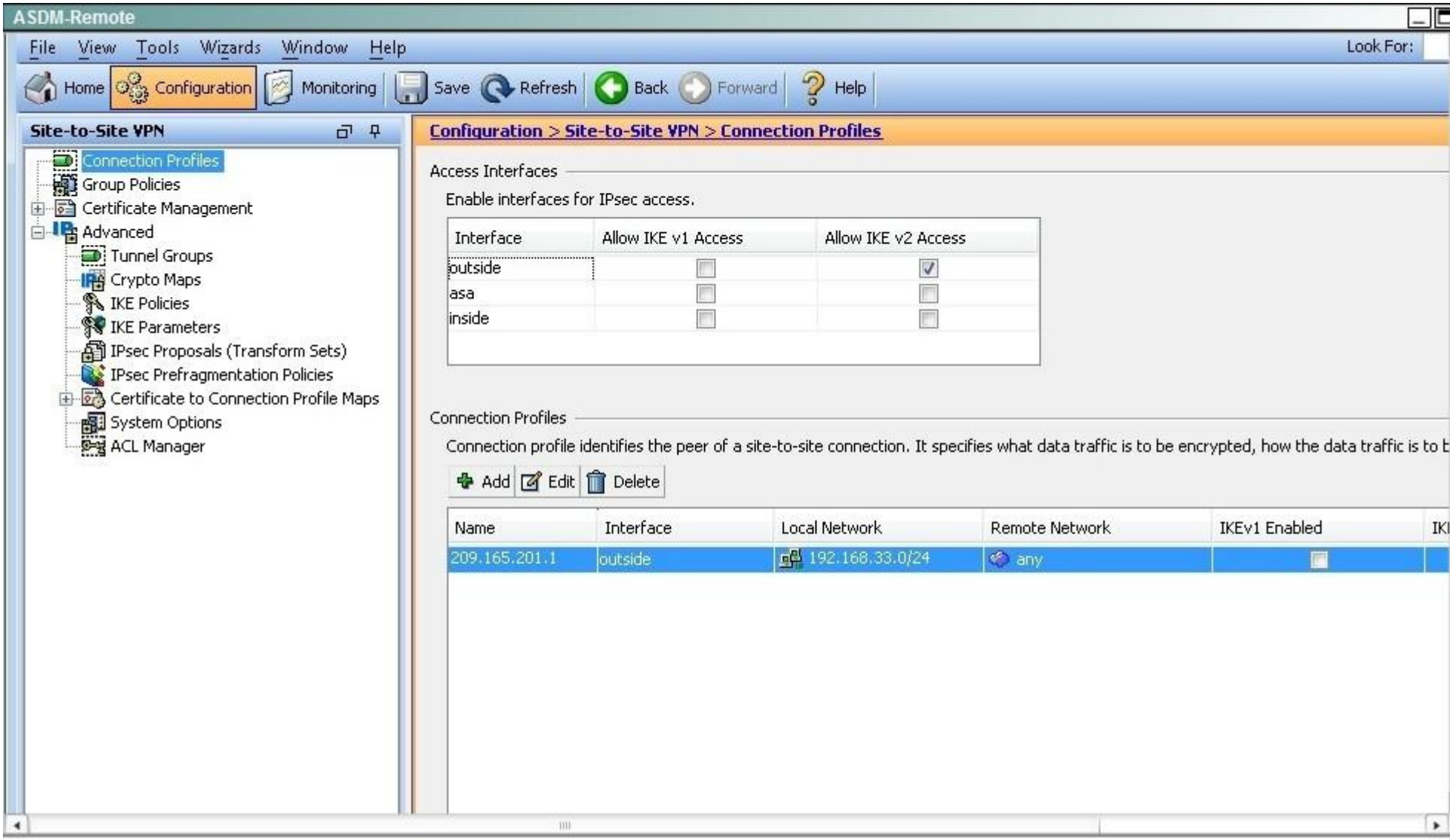
Correct Answer: B
Section: (none)
Explanation

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 73




ASDM-HQ
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Site-to-Site VPN
Connection Profiles
Group Policies
Certificate Management
Advanced
Tunnel Groups
Crypto Maps
IKE Policies
IKE Parameters
IPsec Proposals (Transform Sets)
IPsec Prefragmentation Policies
Certificate to Connection Profile Maps
Policy
Rules
System Options
ACL Manager
Configuration > Site-to-Site VPN > Connection Profiles
Access Interfaces
Enable interfaces for IPsec access.
Interface
Allow IKE v1 Access
Allow IKE v2 Access
outside
asa
inside
Connection Profiles
Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be
Add Edit Delete
Name
Interface
Local Network
Remote Network
IKEv1 Enabled
IK
209.165.201.2
outside
192.168.22.0/24
192.168.33.0/24



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

A. Local selector 192.168.33.0/0-192.168.33.255/65535 Remote selector 192.168.20.0/0- 192.168.20.255/65535
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

C. Local selector 192.168.22.0/0-192.168.22.255/65535 Remote selector 192.168.33.0/0- 192.168.33.255/65535
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
Section: (none)
Explanation

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 74
A custom desktop application needs to access an internal server. An administrator is tasked with configuring the company's SSL VPN gateway to allow remote users to work. Which two technologies would accommodate the company's requirement? (Choose two).

A. AnyConnect client
B. Smart Tunnels
C. Email Proxy
D. Content Rewriter
E. Portal Customizations

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
A rogue static route is installed in the routing table of a Cisco FlexVPN and is causing traffic to be blackholed. 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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Refer to the exhibit.

```
Tunnel-id   Local                 Remote                    fvrf/ivrf            Status
1           209.165.202.130/500   209.165.200.230/500       none/none            READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/7141 sec
      CE id: 1001, Session-id: 1
      Status Description: Negotiation done
      Local spi: C156F9DB2F08AE06       Remote spi: B383BC5A6A805430
      Local id: R002.example.com
      Remote id: R005.example.com
      Local req msg id:  4              Remote req msg id:  3
      Local next msg id: 4              Remote next msg id: 3
      Local req queued:  4              Remote req queued:  3
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      Fragmentation not configured.
      Extended Authentication not configured.
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Assigned host addr: 10.2.2.10
      Initiator of SA : No
      Remote subnets:
      10.2.2.10 255.255.255.255
```

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
Section: (none)
Explanation

Explanation/Reference:
answer is corrected

QUESTION 77
Refer to the exhibit.

```
aaa new-model
aaa authentication network FLEXVPN local

crypto ikev2 authorization policy SPOKES
 pool FlexPOOL
 route set interface
 route accept any distance 255
crypto ikev2 keyring SPOKES
 peer ALLSPOKES
  identity fqdn domain example.com
  pre-shared-key Cisco123
 !
crypto ikev2 profile SPOKES
 match identity remote fqdn domain example.com
 identity local fqdn R002.example.com
 authentication remote pre-share
 authentication local pre-share
 keyring local SPOKES
 aaa authorization group psk list FLEXVPN SPOKES
 virtual-template 10
 set ikev2-profile SPOKES
```

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Refer to the exhibit.

```
interface Tunnel10
 ip address 209.165.200.225 255.255.255.254
 ipv6 address 2001:DB8:100::1/64
 ipv6 enable
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 209.165.201.20
 tunnel protection ipsec profile default
end
```

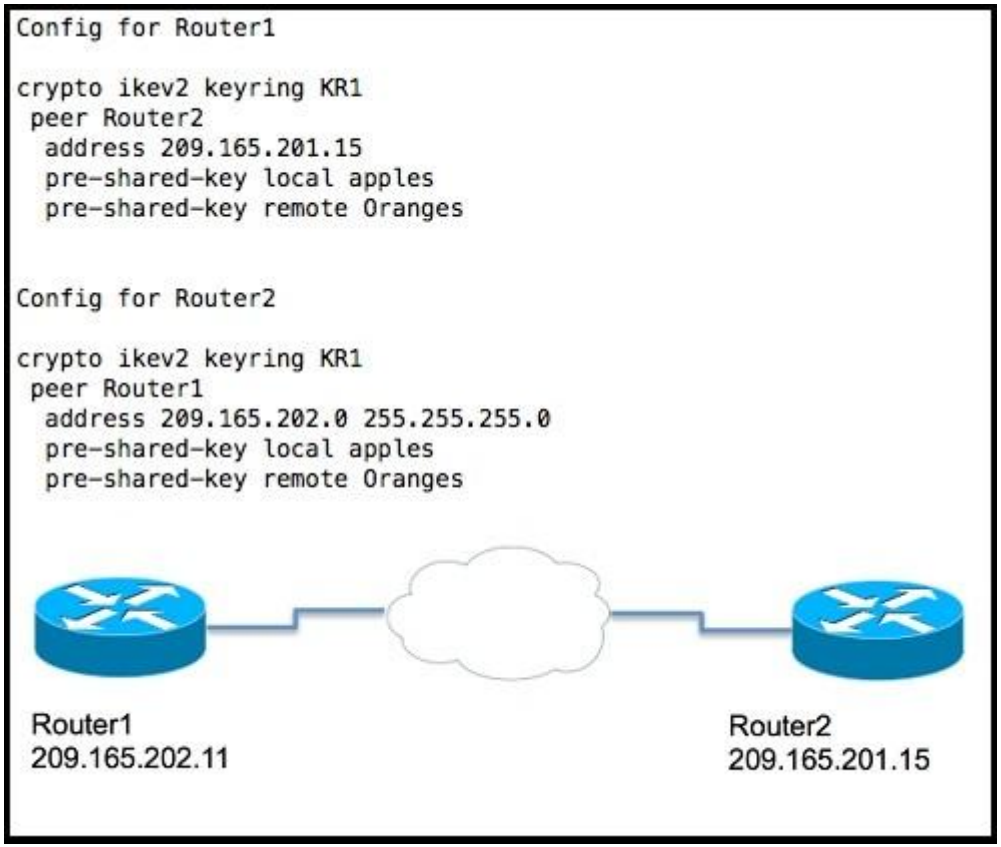
An administrator is adding IPv6 addressing to an already functioning tunnel. The administrator is unable to ping 2001:DB8:100::2 but can ping 209.165.200.226. Which configuration needs to be added or changed?

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: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
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 digest: 34836 #pkts decaps: 26922, #pkts decrypt: 19211, #pkts verify: 19211 #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

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Refer to the exhibit.

```
     <ServerList>
          <HostEntry>
               <HostName>SIMOS ASA</HostName>
               <HostAddress>simos.cisco.com</HostAddress>
               <UserGroup>simos-group</UserGroup>
          <PrimaryProtocol>IPsec</PrimaryProtocol>
          </HostEntry>
     </ServerList>

tunnel-group AC general-attributes
 address-pool VPN-POOL
 default-group-policy GroupPolicy_AC
tunnel-group AC webvpn-attributes
 group-alias simos-group enable
 group-url https://simos.cisco.com/simos-group enable
```

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
Section: (none)
Explanation

Explanation/Reference:
answer is accurated

QUESTION 86
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Refer to the exhibit.

```
Hub config :

crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto ipsec profile DMVPN
 set transform-set myset
!
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 no ip redirects
 ip nhrp authentication DMVPN01
 ip nhrp map multicast dynamic
 ip nhrp network-id 100
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN
!
interface Ethernet0/0
 ip address 209.165.200.234 255.255.255.248


Spoke 2 Config :

crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto ipsec profile DMVPN
 set transform-set myset
!
interface Tunnel0
 ip address 172.16.1.3 255.255.255.0
 no ip redirects
 ip nhrp authentication DMVPN1
 ip nhrp map 172.16.1.1 209.165.200.234
 ip nhrp map multicast 209.165.200.234
 ip nhrp network-id 200
 ip nhrp nhs 172.16.1.1
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN

!
interface Ethernet0/0
 ip address 209.165.202.146  255.255.255.248

Hub debugs :

*Apr 25 19:32:30.867: NHRP: Receive Registration Request via Tunnel0 vrf 0, packet size: 107
*Apr 25 19:32:30.868: NHRP-ATTR: Sending error indication
```

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
Section: (none)
Explanation

Explanation/Reference:
http://www.cisco.com/c/en/us/td/docs/ios/12_4/ip_addr/configuration/guide/hadnhrp.html#wp10 55049

QUESTION 91
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
A spoke has two Internet connections for failover. 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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
In DMVPN phase 2, which two EIGRP features need to be disabled on the hub to allow spoke- to-spoke communication? (Choose two.)

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which cryptographic algorithms are a part of the Cisco NGE suite?

A. HIPPA DES
B. AES-CBC-128
C. RC4-128
D. AES-GCM-256

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
https://www.cisco.com/web/learning/le21/le39/docs/tdw166_prezo.pdf

QUESTION 99
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
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 ikev2 sa

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
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
Section: (none)
Explanation

Explanation/Reference:
answer is valid

QUESTION 102
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
D. Via the svc trusted-network command under the global webvpn sub-configuration mode on the ASA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
The following configuration steps have been completeD. · WebVPN was enabled on the ASA outside interface.
· SSL VPN client software was loaded to the ASA.
· 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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
Refer to the exhibit.

```
router-01(config)#crypto isakmp keepalive 60 5
router-01(config)#crypto isakmp policy 10
router-01(config-isakmp)#encryption 3des
router-01(config-isakmp)#hash md5
router-01(config-isakmp)#authentication rsa-encr
router-01(config-isakmp)#group 2
router-01(config-isakmp)#lifetime 28800
```

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
Refer to the exhibit.

```
crypto isakmp policy 5
   authentication pre-share
   group 2

crypto isakmp key dmvpnkey address 0.0.0.0 0.0.0.0
crypto isakmp nat keepalive 20
```

Which two statements about the given configuration are true? (Choose two.)

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
Refer to the exhibit.

```
crypto ikev2 keyring KR1
 peer ALL
  address ::/0
  pre-shared-key local cisco
  pre-shared-key remote cisco
 !
```

What technology does the given configuration demonstrate?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
In which situation would you enable the Smart with clientless SSL VPN?

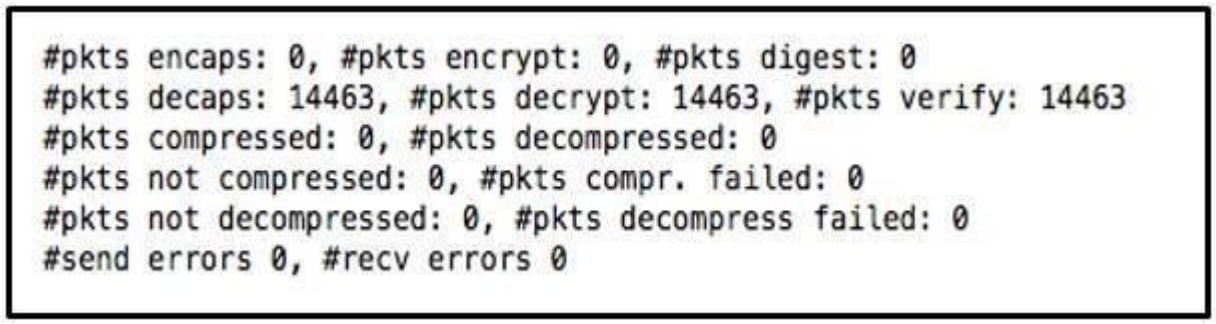
A. when a user is using an outdated version of a web browser
B. when an application is failing in the rewrite process
C. when IPsec should be used over SSL VPN

D. when a user has a nonsupported Java version installed
E. when cookies are disabled

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
Refer to the exhibit.



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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
Which technology is FlexVPN based on?

A. OER
B. VRF
C. IKEv2
D. an RSA nonce

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Which application does the Application Access feature of Clientless VPN support?

A. TFTP
B. VoIP
C. Telnet
D. active FTP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
Which is used by GETVPN, FlexVPN and DMVPN?

A. NHRP
B. MPLS
C. GRE
D. ESP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
Which VPN solution is best for a collection of branch offices connected by MPLS that frequenty make VoIP calls between branches?

A. GETVPN
B. Cisco AnyConnect
C. site-to-site
D. DMVPN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
Refer to the exhibit.

```
crypto ikev2 proposal PROP
 encryption aes-cbc-128
 integrity sha256
 group 20

crypto ikev2 policy IKEV2_POLICY
 match address local 10.1.1.2
 proposal PROP

crypto ikev2 keyring KEYRING
 peer spokes
  address 10.0.0.0 255.0.0.0
  pre-shared-key local cisco123
  pre-shared-key remote cisco123

crypto ikev2 profile PROFILE_IKEV2
 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 ikev2 dpd 30 5 on-demand

crypto ipsec transform-set TRANSFORM_IPSEC esp-gcm
 mode transport


crypto ipsec profile PROFILE_IPSEC
 set transform-set TRANSFORM_IPSEC
 set ikev2-profile PROFILE_IKEV2

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback100
 tunnel path-mtu-discovery
 tunnel protection ipsec profile PROFILE_IPSEC
```

Which VPN solution does this configuration represent?

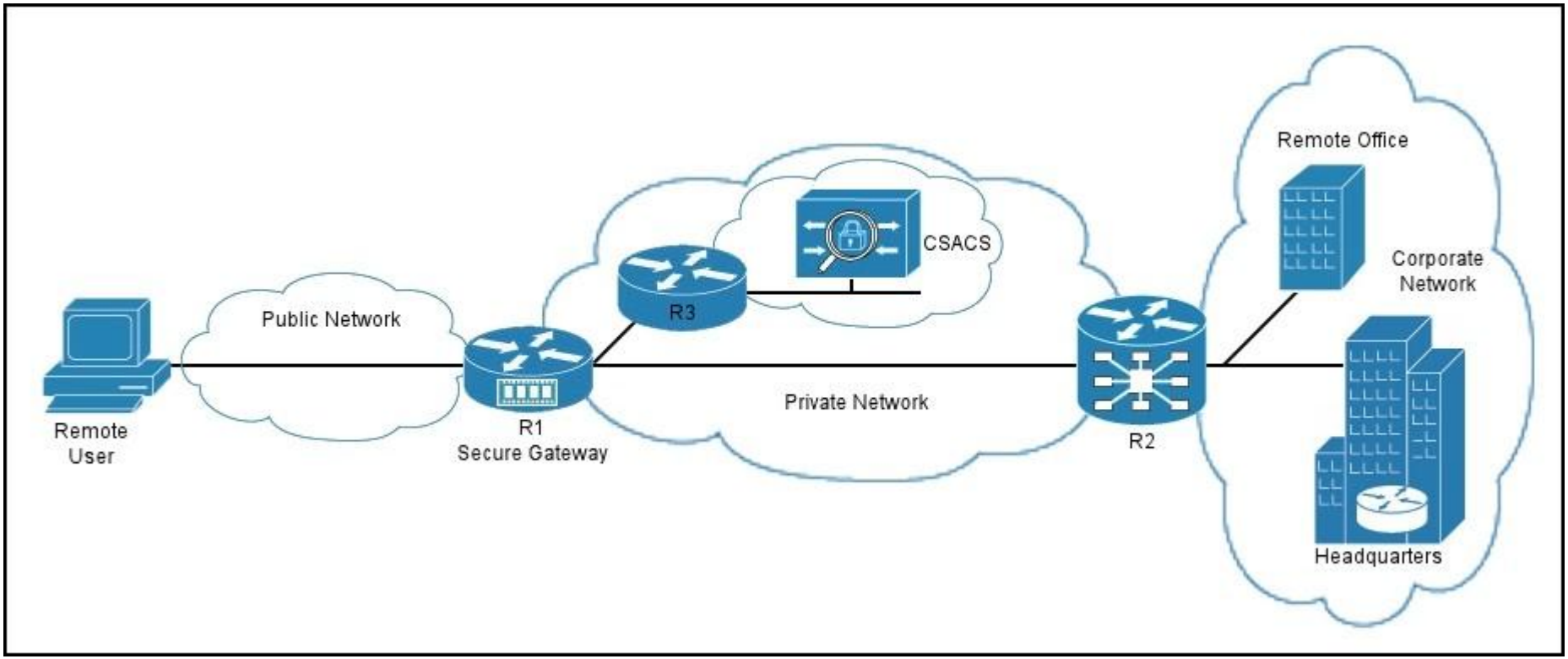
A. DMVPN

B. GETVPN
C. FlexVPN
D. site-to-site

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
answer is verified

QUESTION 124
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
Refer to the exhibit.

```
crypto ipsec transform-set transform esp-des
 mode tunnel
!
crypto map tmap 10 ipsec-isakmp
 set peer 20.1.1.1
 set transform-set transform
 match address 101
 crypto map tmap
!
interface Ethernet0/3
 description OUTSIDE
 ip address 20.1.1.2 255.255.255.252
 crypto map tmap
!
access-list 101 permit udp host 20.1.1.2 eq 1701 host 20.1.1.1 eq 1701
```

Which VPN solution does this configuration represent?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
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
Section: (none)

Explanation

Explanation/Reference:

QUESTION 128
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
Refer to the exhibit.

```
Apr  2 12:03:55.391: ISAKMP (14): beginning Main Mode exchange
Apr  2 12:03:57.199: ISAKMP (14): processing SA payload. message ID = 0
Apr  2 12:03:57.203: ISAKMP (14): Checking ISAKMP transform 1 against priority 1 policy
Apr  2 12:03:57.203: ISAKMP:      encryption DES-CBC
Apr  2 12:03:57.207: ISAKMP:      hash MD5
Apr  2 12:03:57.207: ISAKMP:      default group 1
Apr  2 12:03:57.207: ISAKMP:      auth pre-share
Apr  2 12:03:57.211: ISAKMP (14): atts are acceptable. Next payload is 0
Apr  2 12:03:57.215: Crypto engine 0: generate alg param
```

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
Which two technologies are considered to be Suite B cryptography? (Choose two.)

A. MD5
B. SHA2
C. Elliptical Curve Diffie-Hellman
D. 3DES
E. DES

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
Which protocol does DTLS use for its transport?

A. TCP
B. UDP
C. IMAP
D. DDE

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

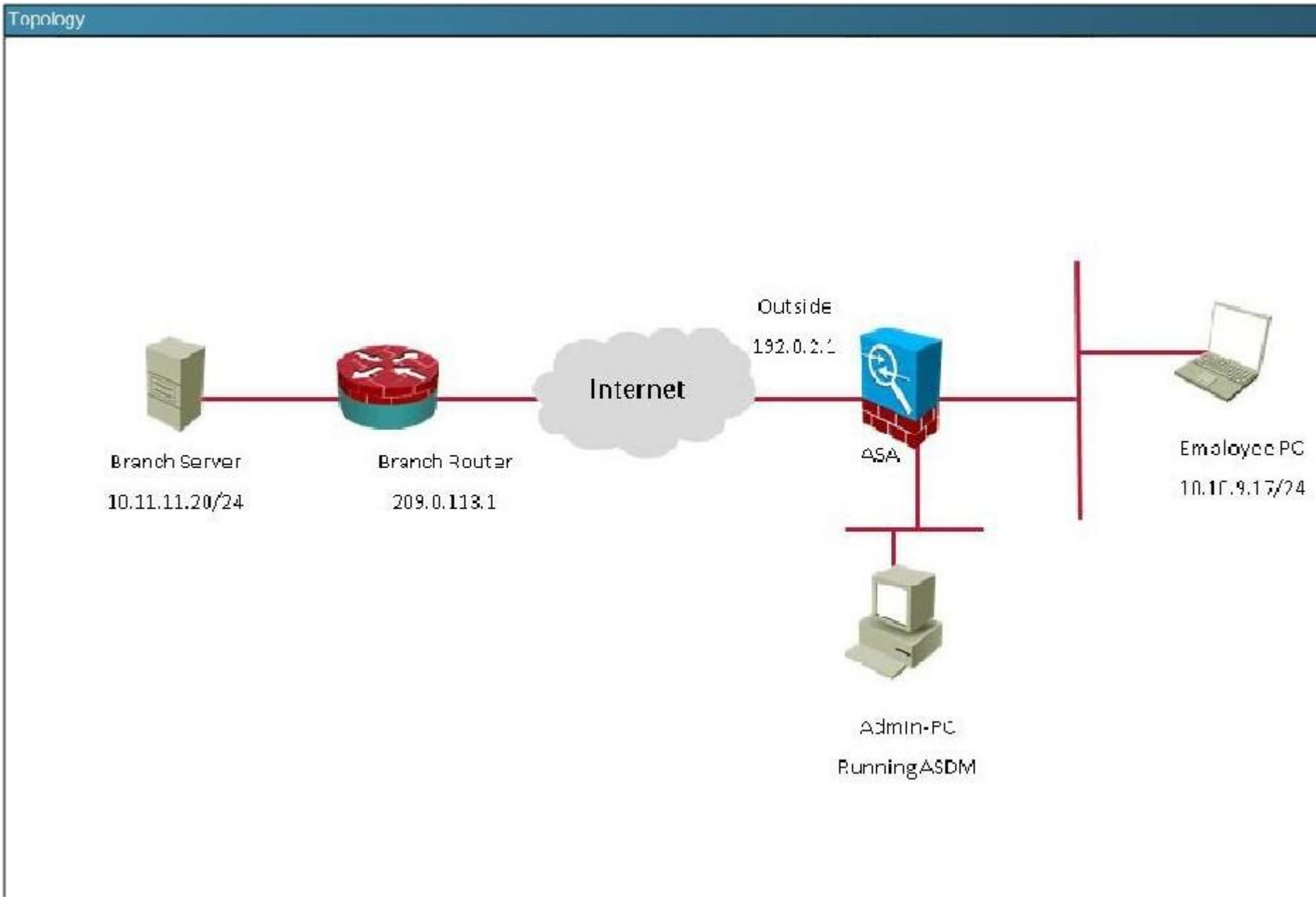
QUESTION 132
Scenario:

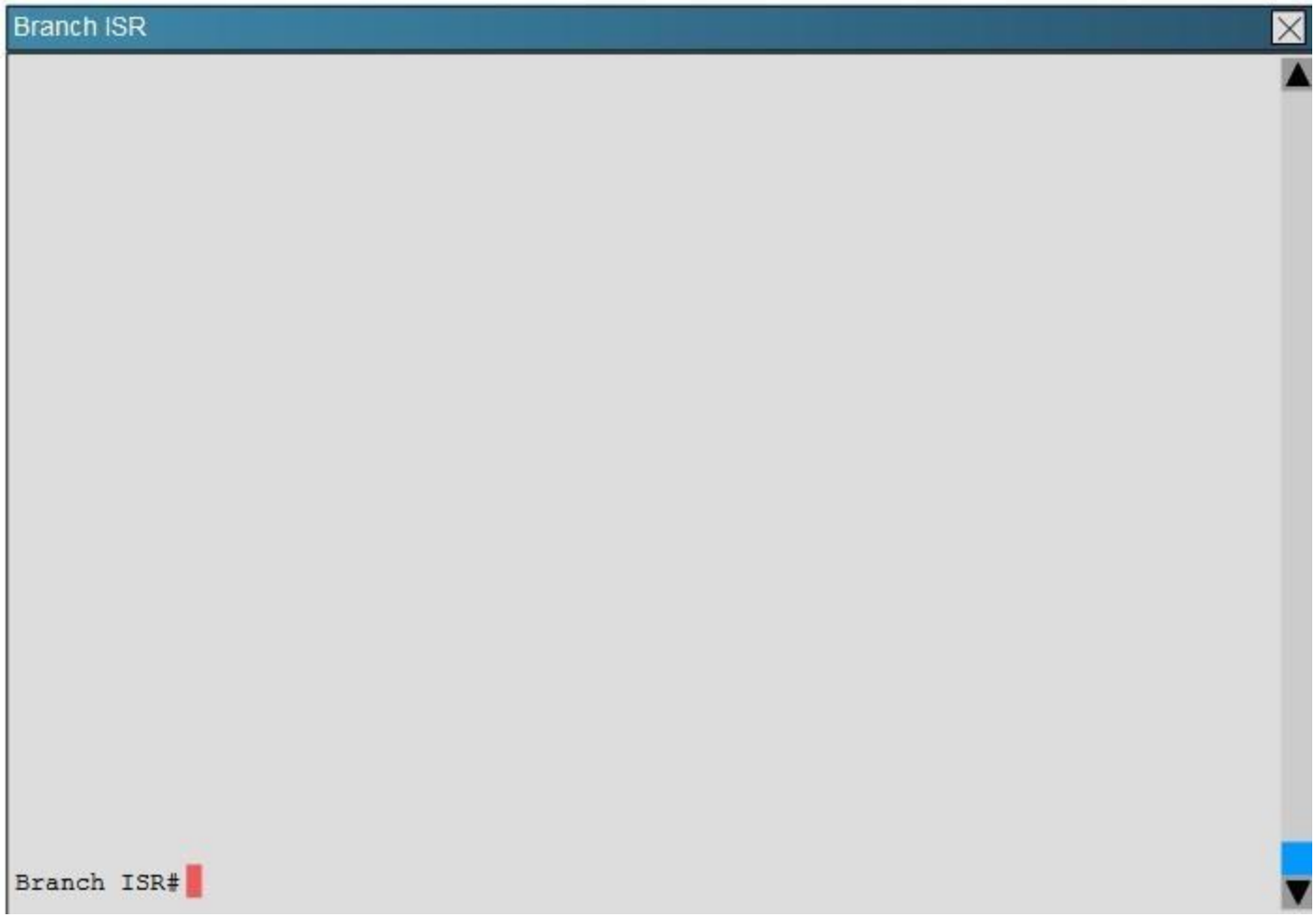
You are the senior network security administrator for your organization. Recently and junior engineer configured a site-to-site IPsec VPN connection between your headquarters Cisco ASA and a remote branch office.

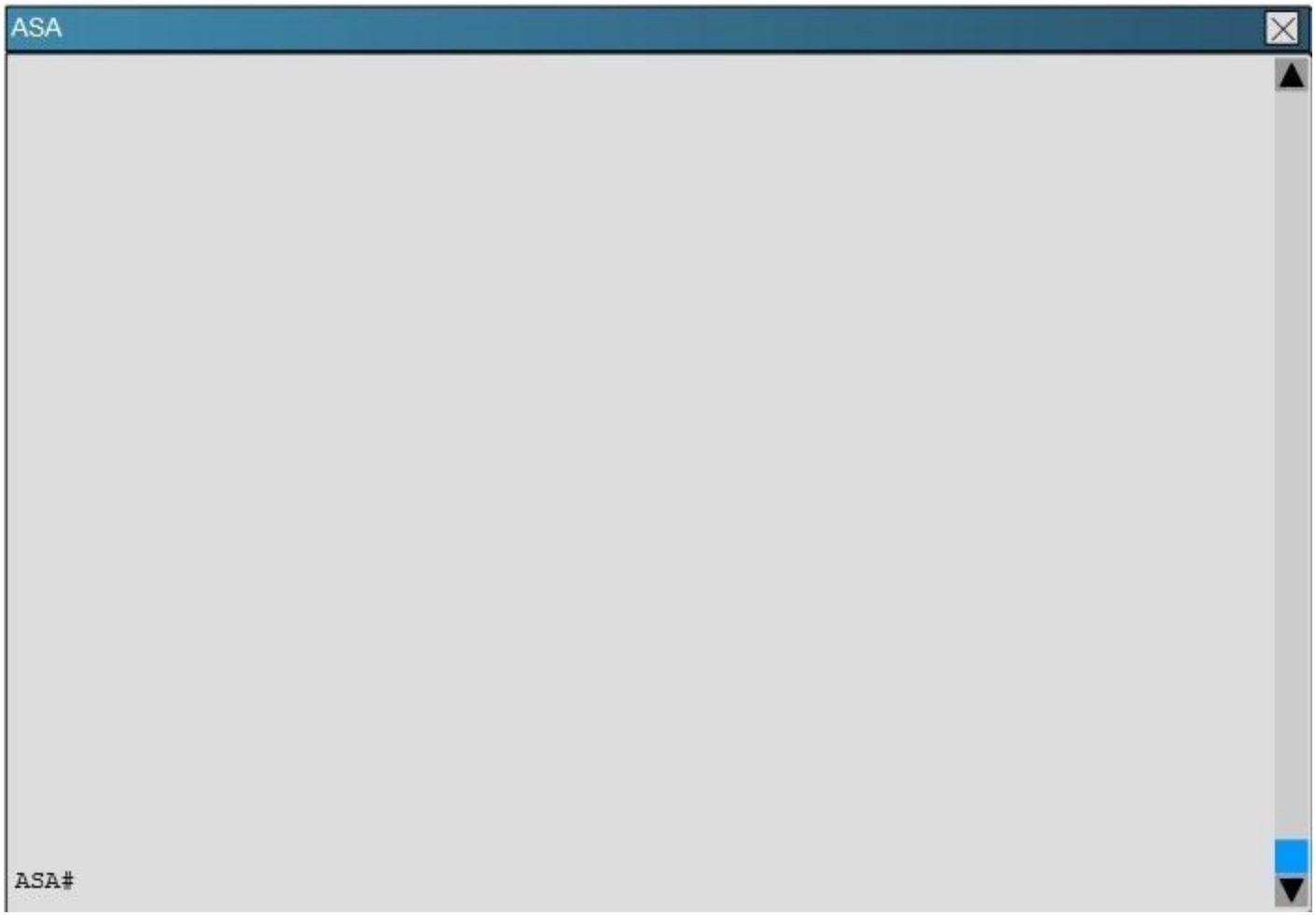
You are now tasked with verifying the IKEvl IPsec installation to ensure it was properly configured according to designated parameters. Using the CLI on both the Cisco ASA and branch ISR. verify the IPsec configuration is properly configured between the two sites.

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

Topology:







What is being used as the authentication method on the branch ISR?

A. Certifcates
B. Pre-shared keys
C. RSA public keys
D. Diffie-Hellman Group 2

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:

The show crypto isakmp key command shows the preshared key of "cisco"

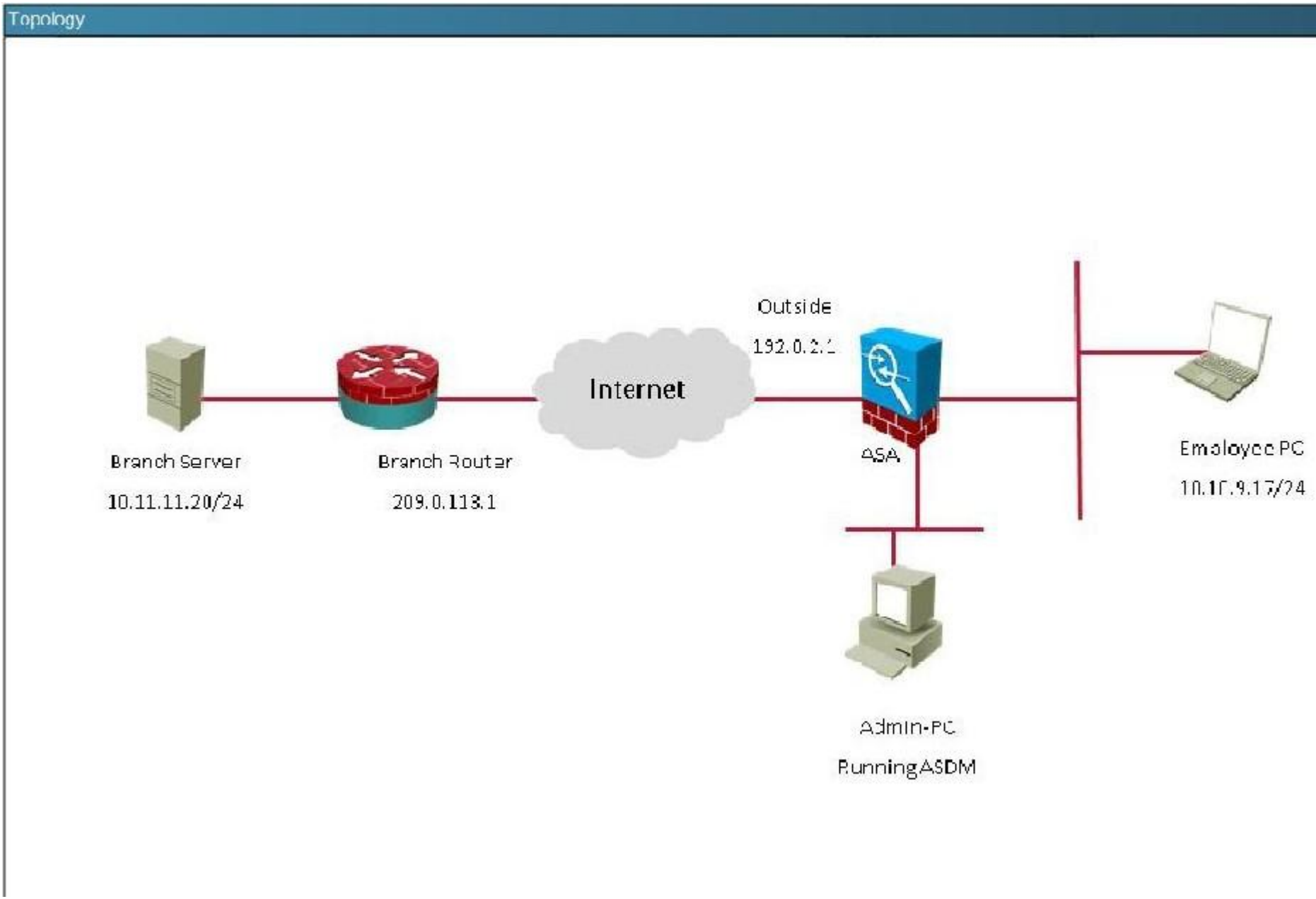
```
Branch ISR#show crypto isakmp key
Keyring      Hostname/Address                                Preshared Key

default      192.0.2.1                                       cisco
Branch ISR#
Branch TSR#
Branch ISR#
```

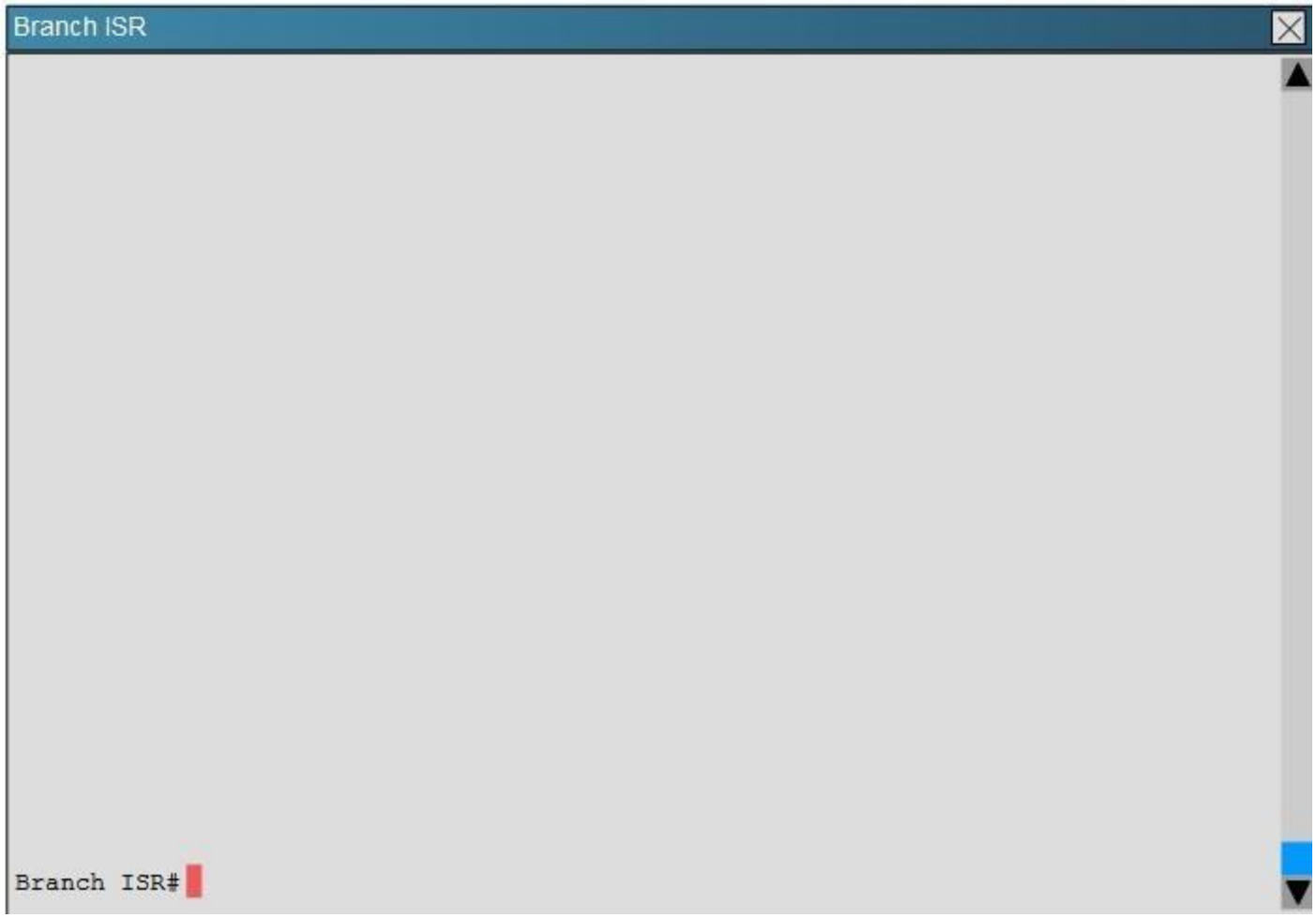
QUESTION 133
Scenario:

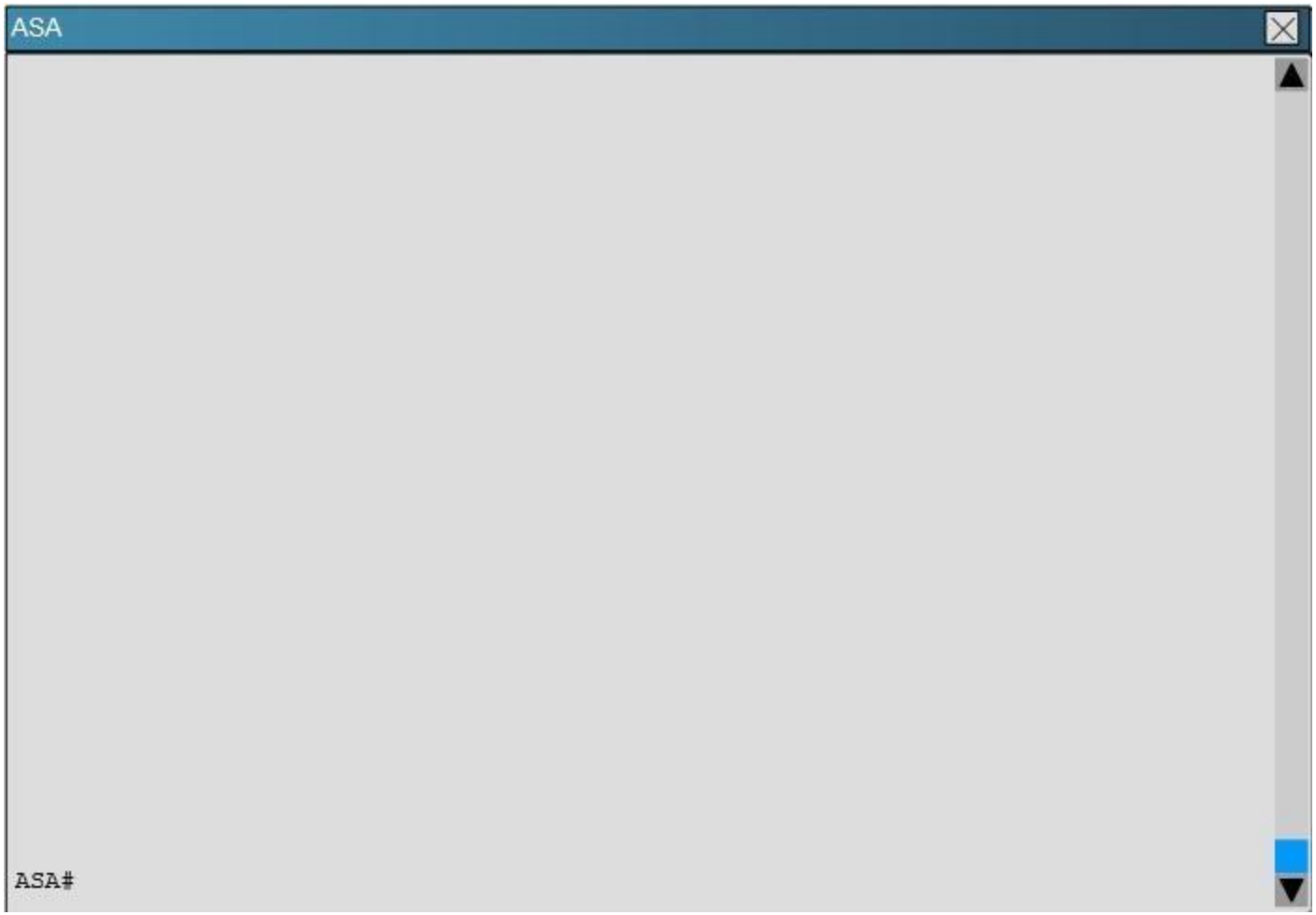
You are the senior network security administrator for your organization. Recently and junior engineer configured a site-to-site IPsec VPN connection between your headquarters Cisco ASA and a remote branch office.

You are now tasked with verifying the IKEvl 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 the 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
Section: (none)

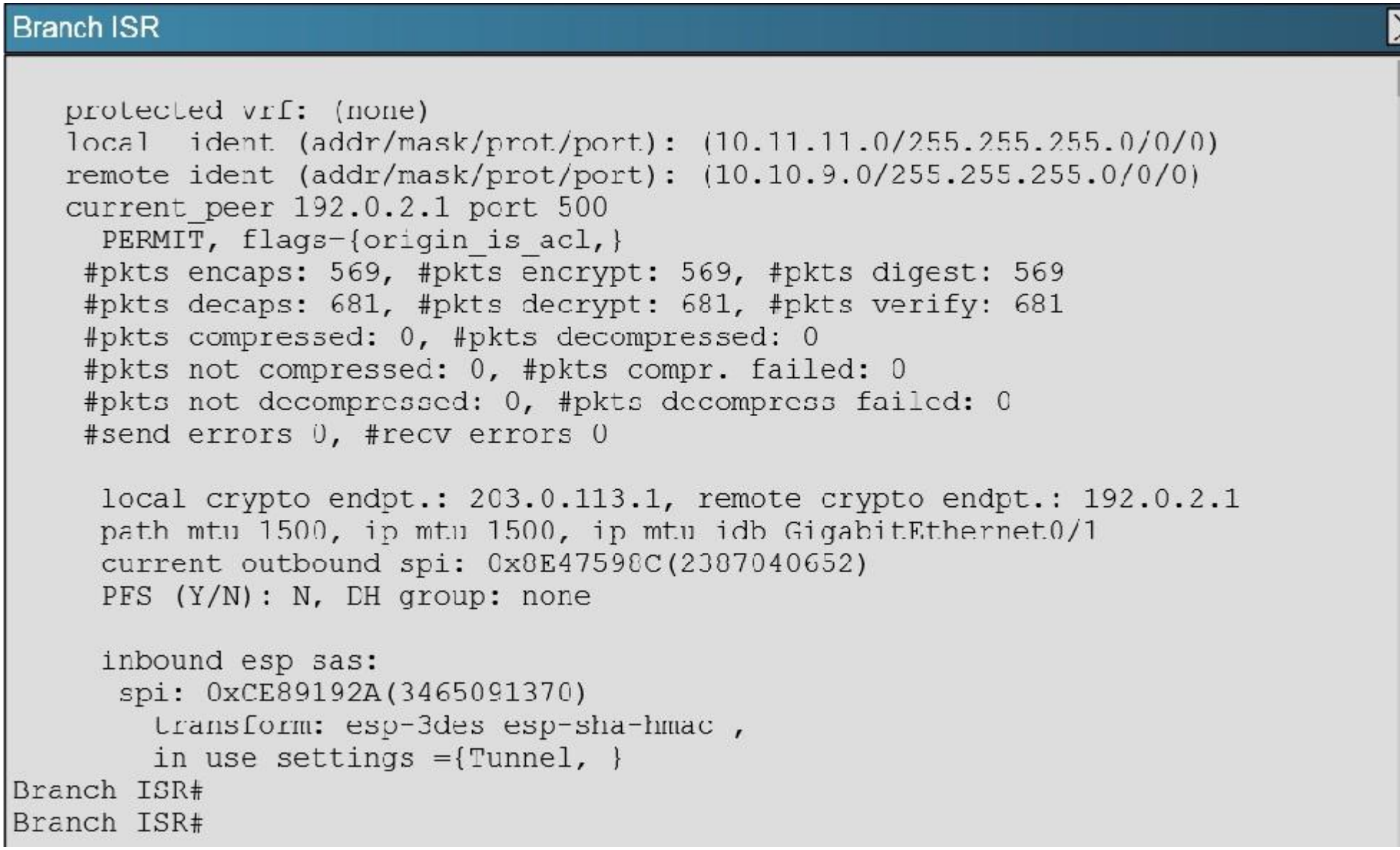
Explanation

Explanation/Reference:
Explanation:

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: VPN-to-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)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xCE89192A(3465091370)
        transform: esp-3des esp-sha-hmac ,
```



QUESTION 134
Scenario:

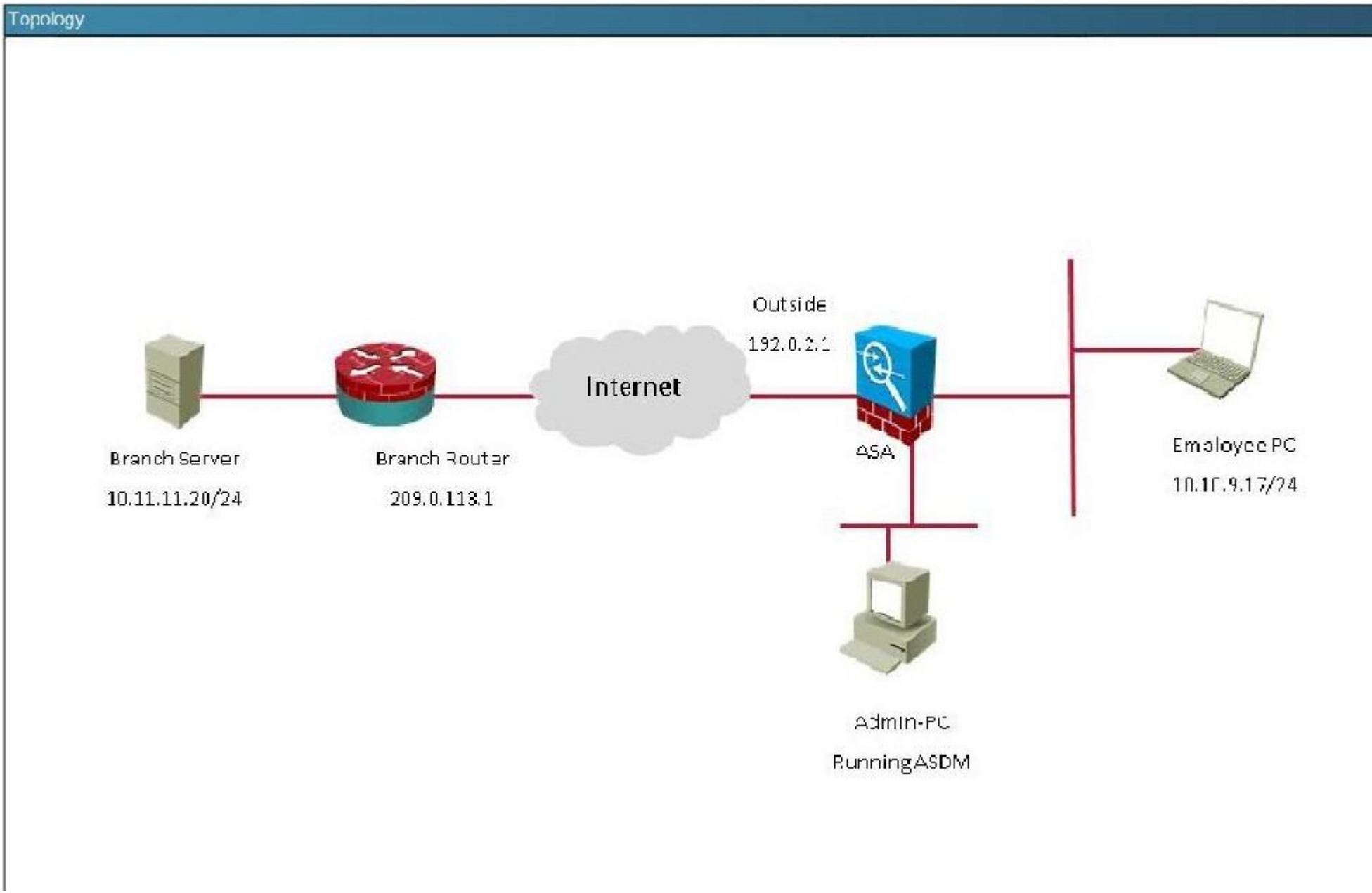
You are the senior network security administrator for your organization. Recently and junior engineer configured a site-to-site IPsec VPN connection between your headquarters Cisco ASA and a remote branch office.

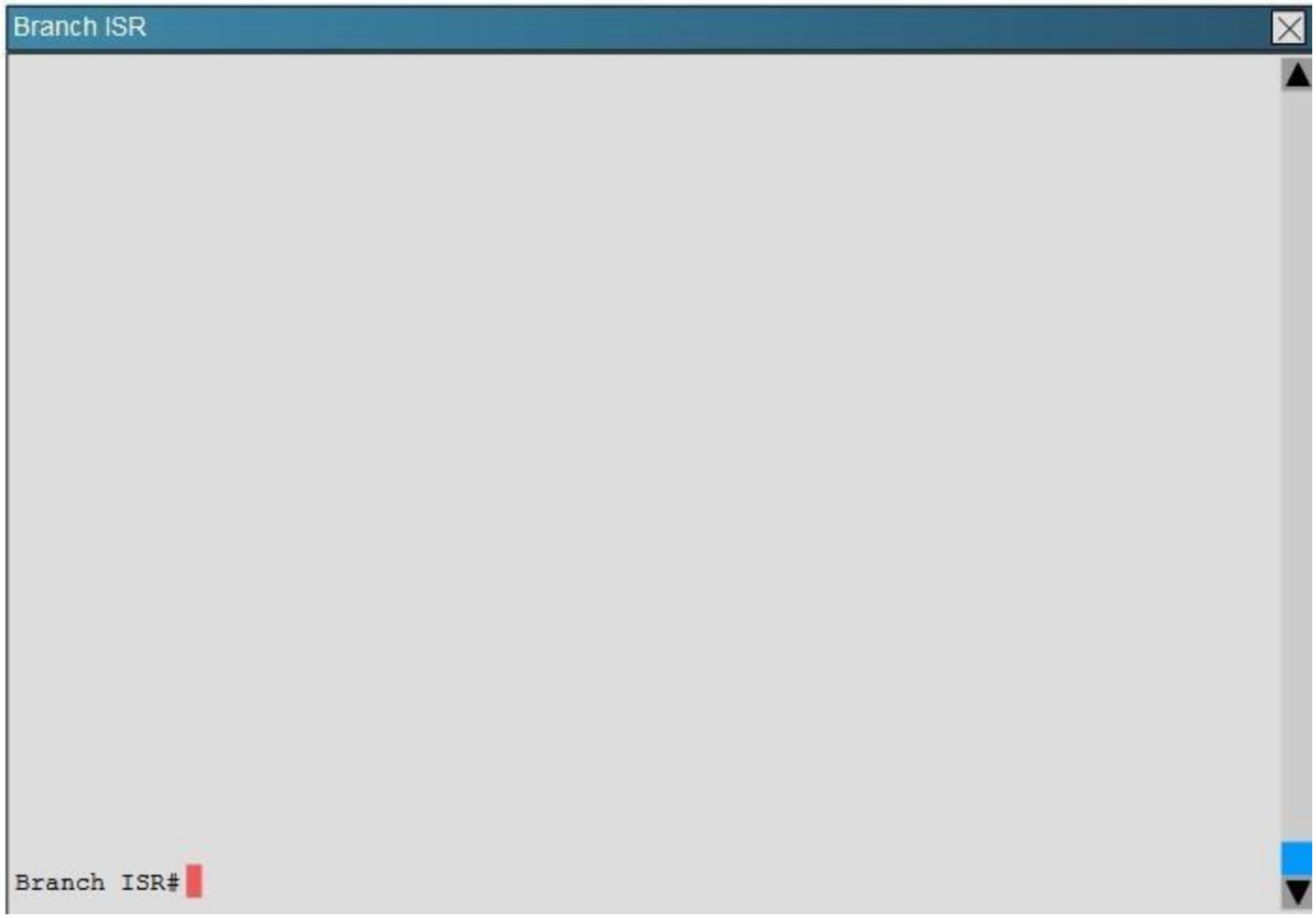
You are now tasked with verifying the IKEvl IPsec installation to ensure it was properly configured according to designated parameters. Using the CLI on both the Cisco ASA and branch ISR. verify the IPsec configuration is properly configured between the two sites.

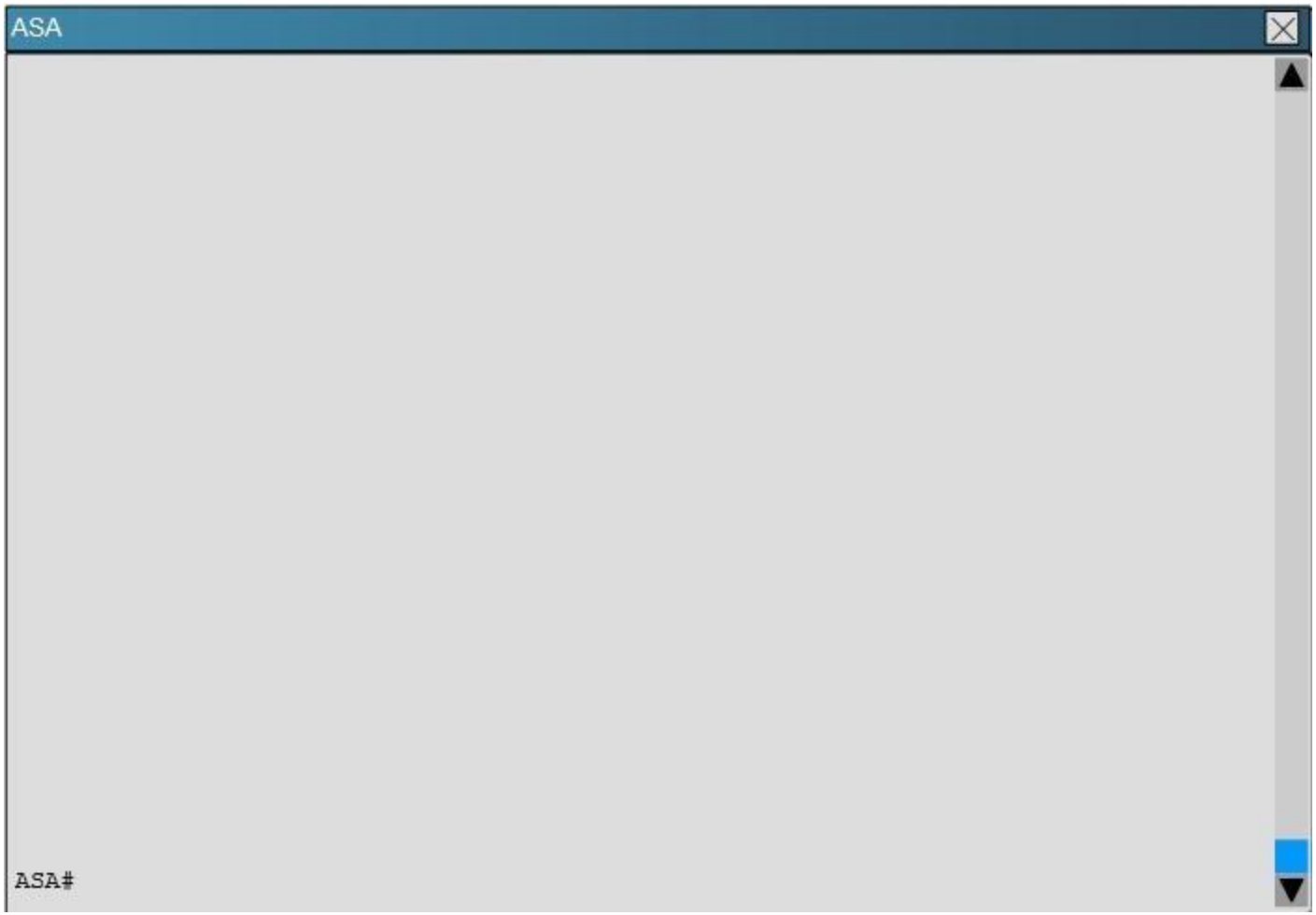
NOTE: the show running-config command cannot be used for the this exercise.

Topology:

Topology







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
Section: (none)

Explanation

Explanation/Reference:
Explanation:

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
```

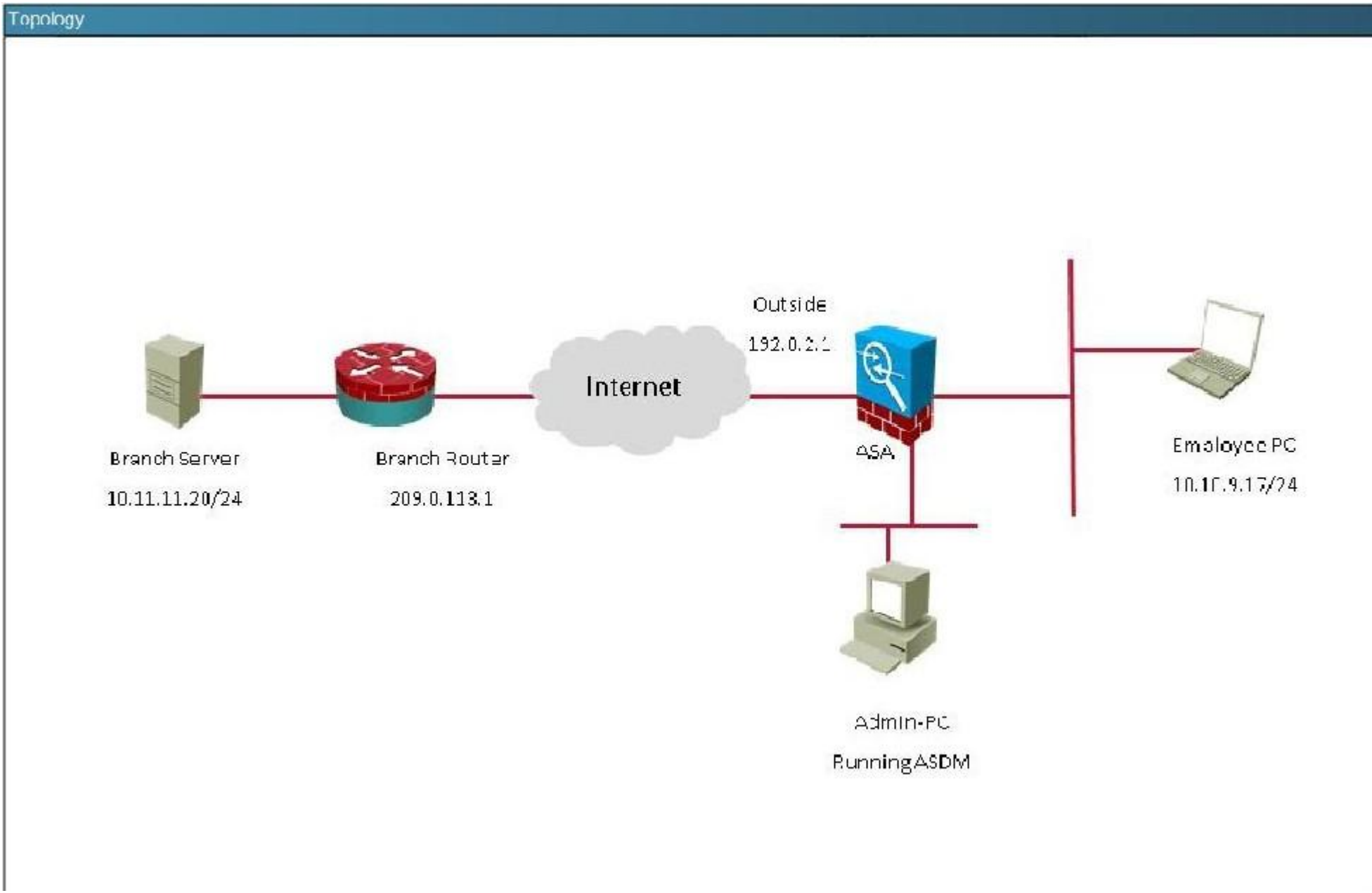
QUESTION 135
Scenario:

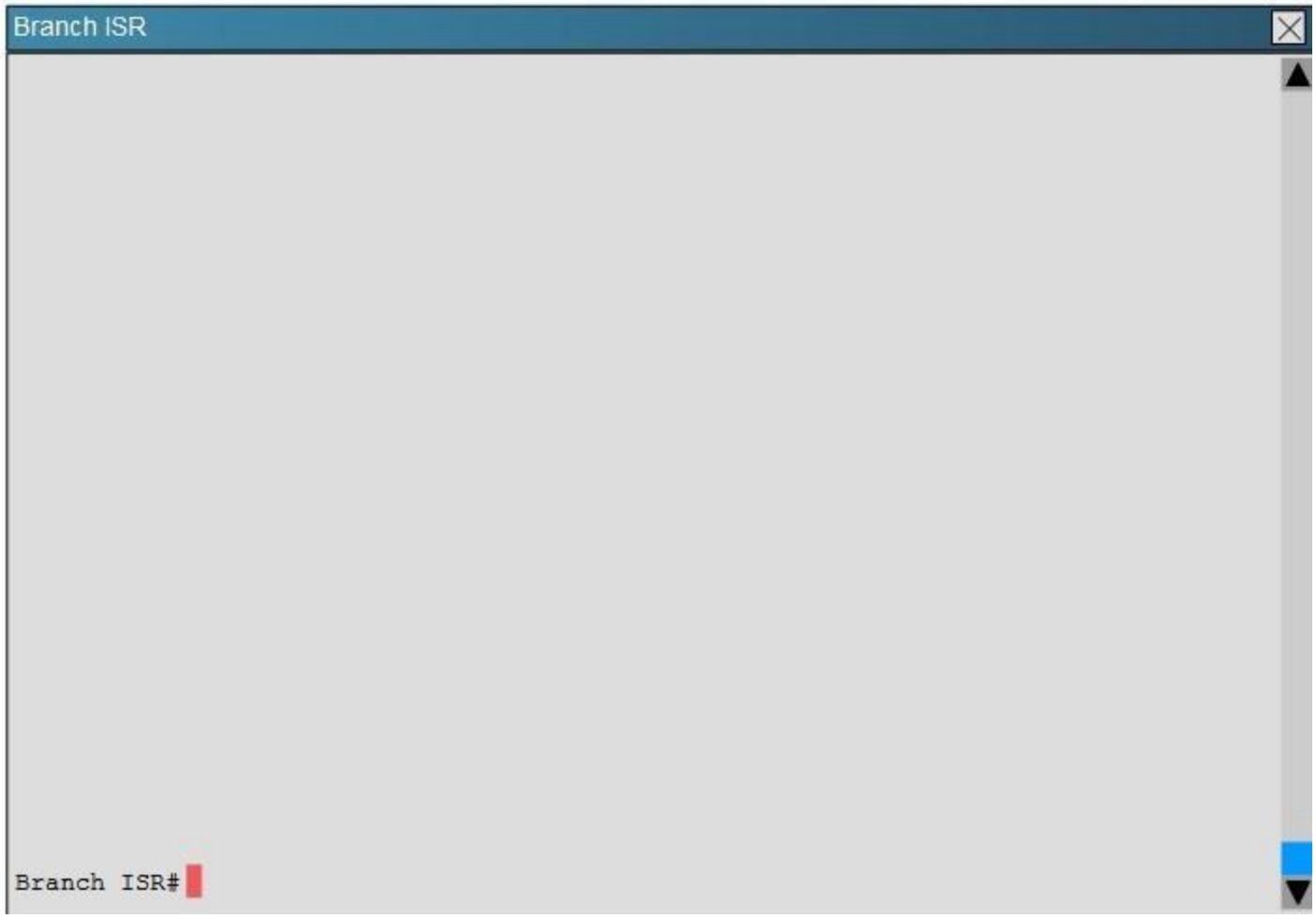
You are the senior network security administrator for your organization. Recently and junior engineer configured a site-to-site IPsec VPN connection between your headquarters Cisco ASA and a remote branch office.
You are now tasked with verifying the IKEvl IPsec installation to ensure it was properly 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.

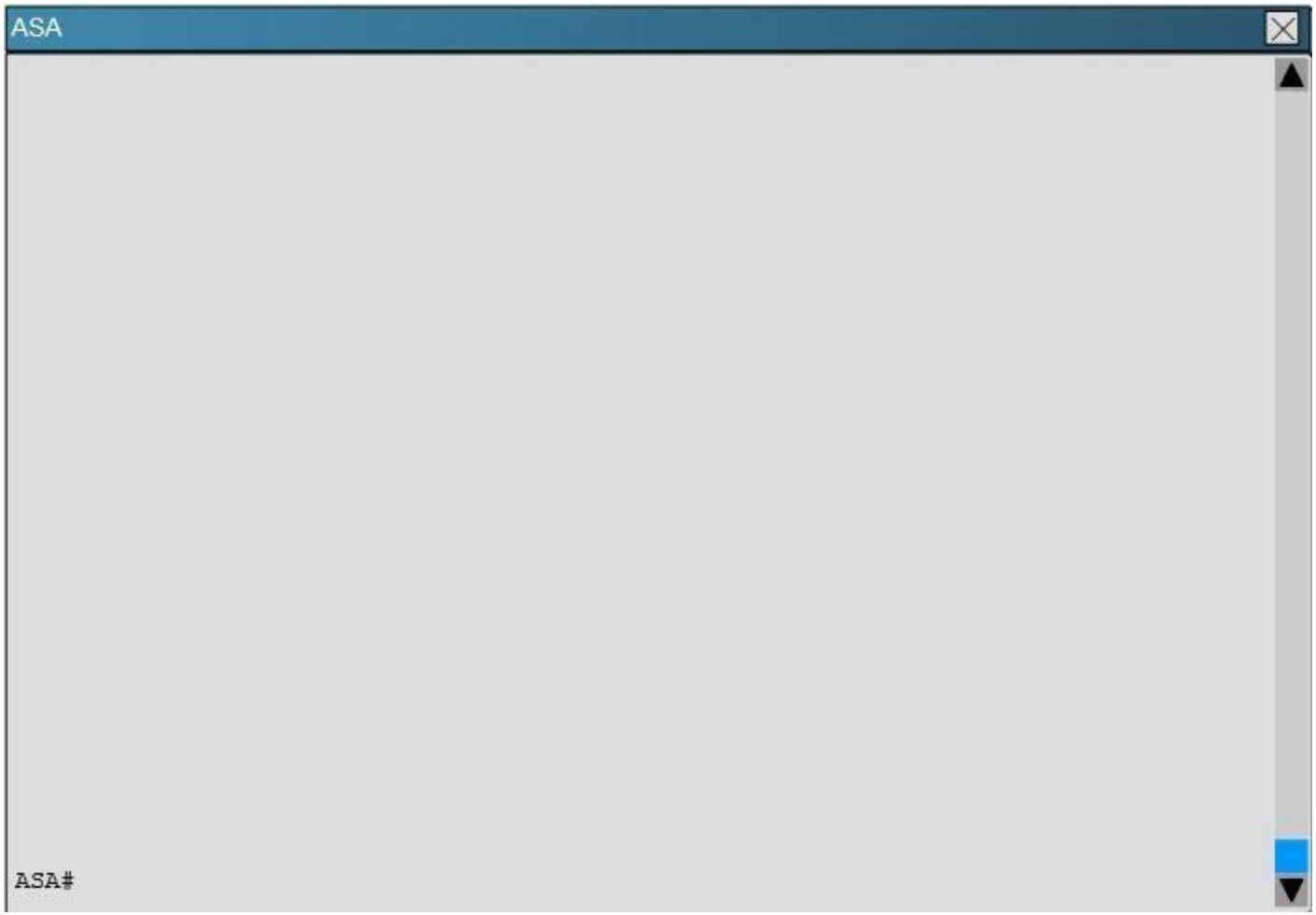
NOTE: the show running-config command cannot be used for the this exercise.

Topology:

Topology







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

A. outside_cryptomap
B. VPN-to-ASA
C. L2L_Tunnel
D. outside_map1

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:

This is seen from the "show crypto ipsec sa" command on the ASA.

ASA

```
ASA#sho 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 decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs 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
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
```

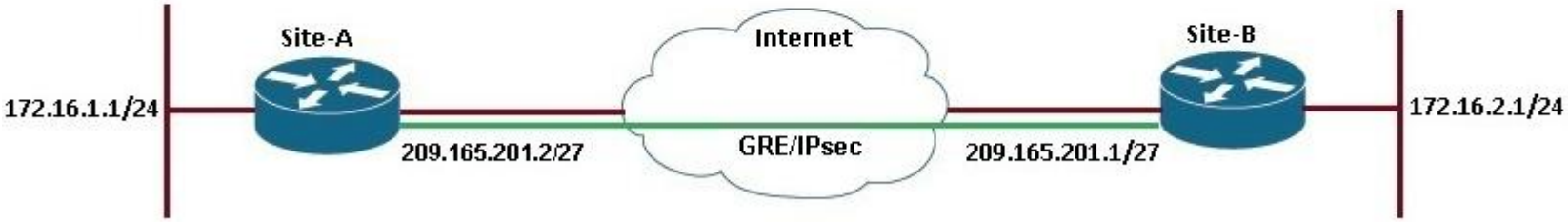
QUESTION 136

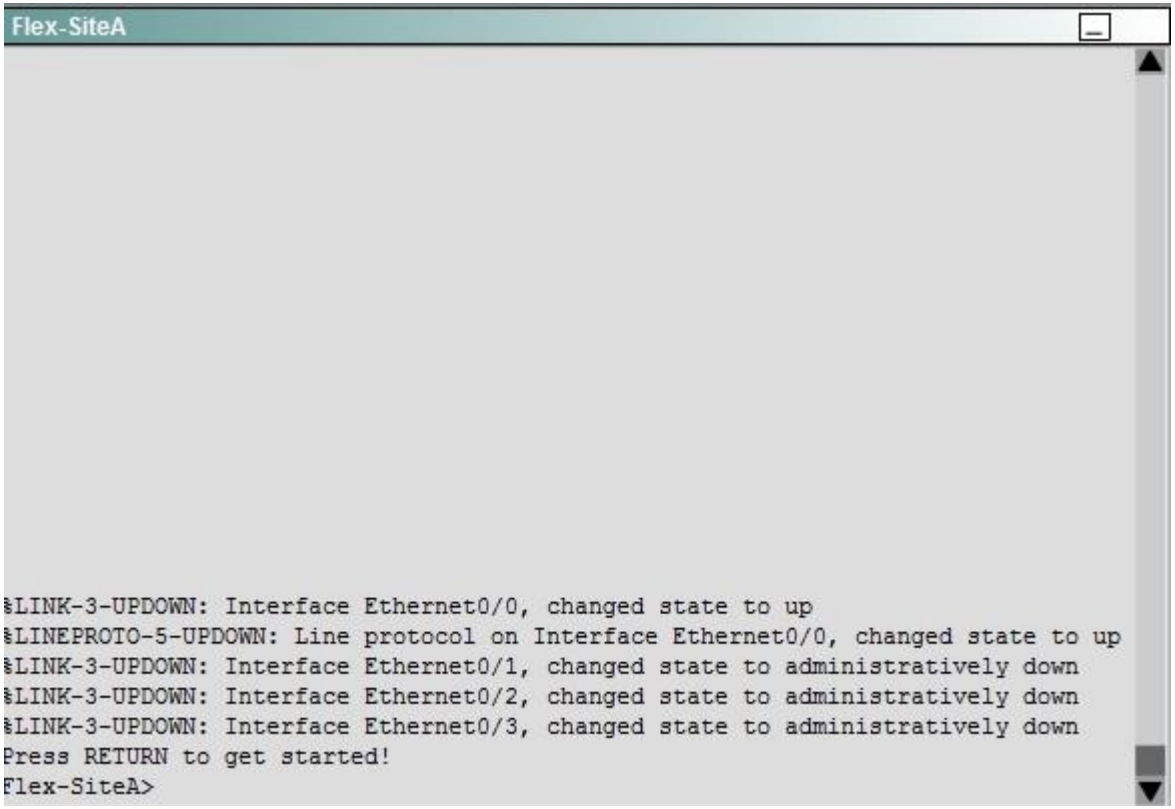
Scenario

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 FlexVPN framework. The router at Site B is preconfigured. You must use the IKEv2 configuration blocks to accomplish this task.

- Configure a point-to-point GRE tunnel on the router and use interface Ethernet0/0 as the tunnel source (Use tunnel 0 for this purpose). Configure 10.1.1.1/24 as the IP address on the tunnel interface. Verify that you are able to ping across the GRE tunnel
- Configure an IKEv2 proposal, and make sure that the tunnel uses the following parameters:
  - Encryption algorithm: **AES 128**
  - Integrity algorithm: **SHA1**
  - Diffie-Hellman group: **5**
- Configure an IKEv2 key ring, with the local pre-shared key **$iteA** and remote pre-shared key **$iteB**.
- 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 IPsec 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.

Topology





Correct Answer: Answer: Here are the steps as below:
Section: (none)
Explanation

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
Keyring local mykeys

Step 3: Create the GRE Tunnel and apply profile
crypto ipsec 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

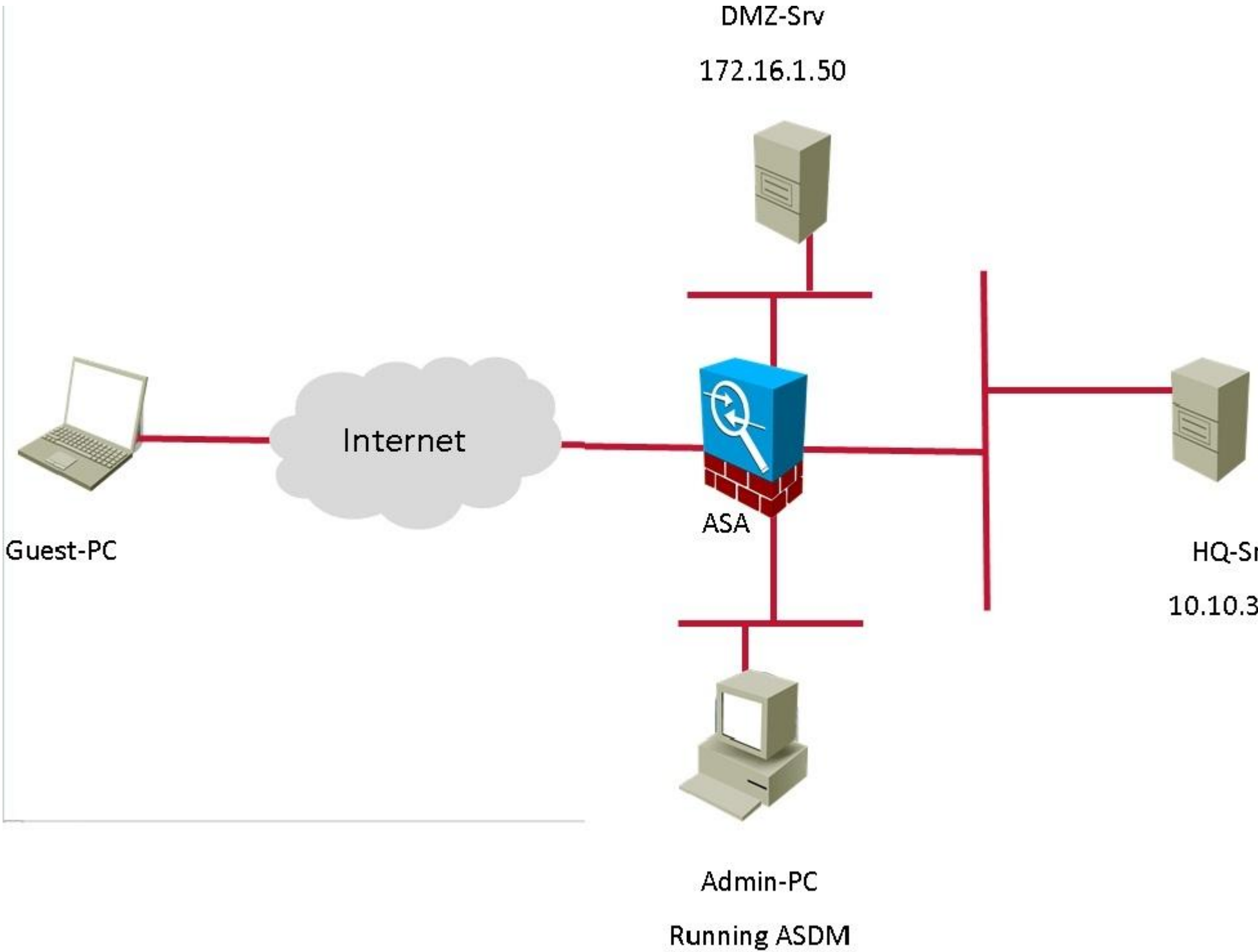
QUESTION 137
You are the network security manager for your organization. Your manager has received a request to allow an external user to access to your HQ and DM2 servers. You are given the following connection parameters for this task.
Using ASDM on the ASA, configure the parameters below and test 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.

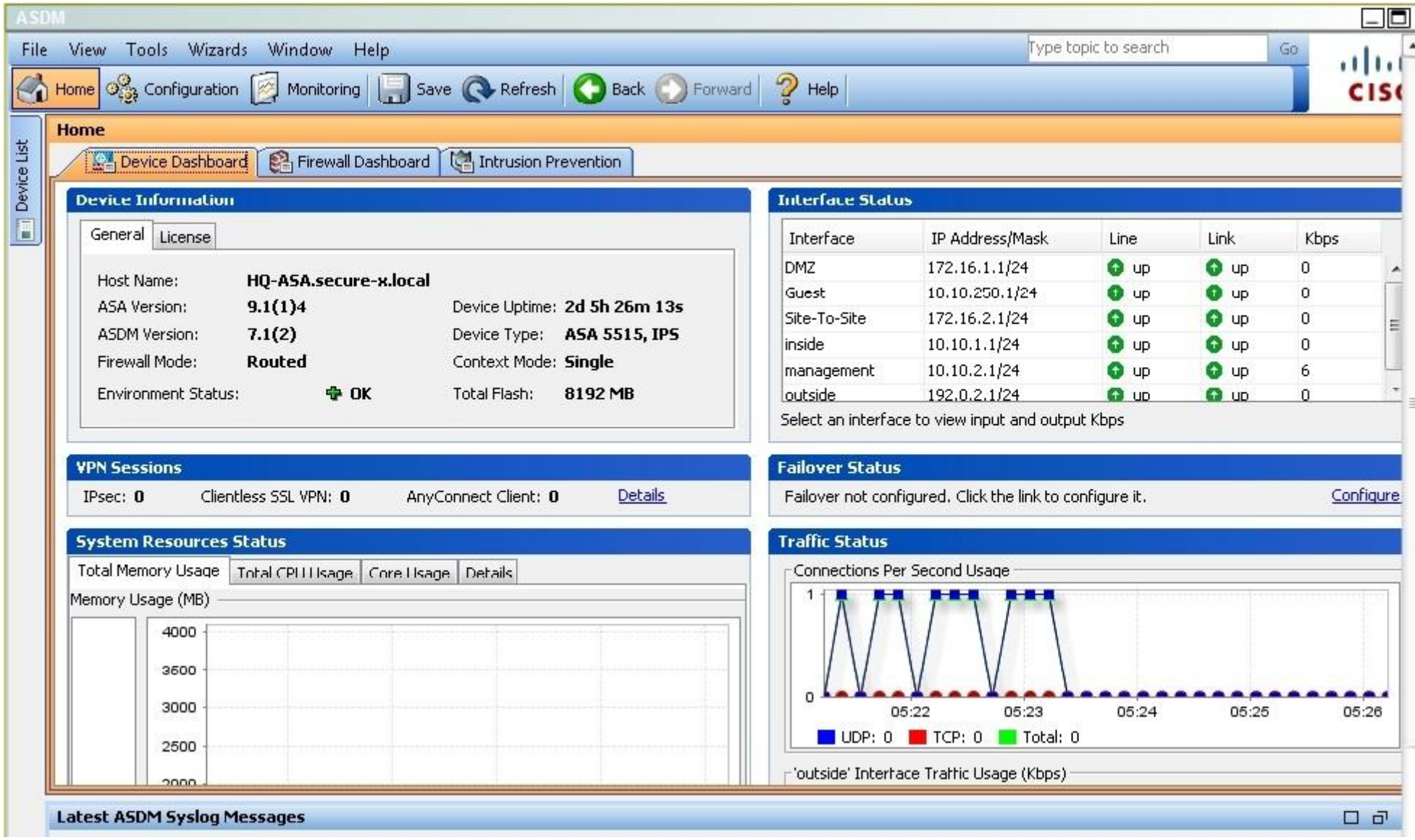
- Enable Clientless SSL VPN on the outside interface
- Using the Guest PC, open an Internet Explorer window and test and verify the basic connection to the SSL VPN portal using address: https://vpn-secure-x.public
- a. You may notice a certificate error in the status bar, this can be ignored for this 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
- e. Assign the configured Bookmarks to:
- i. DfltGrpPolicy
- ii. DfltAccessPolicy

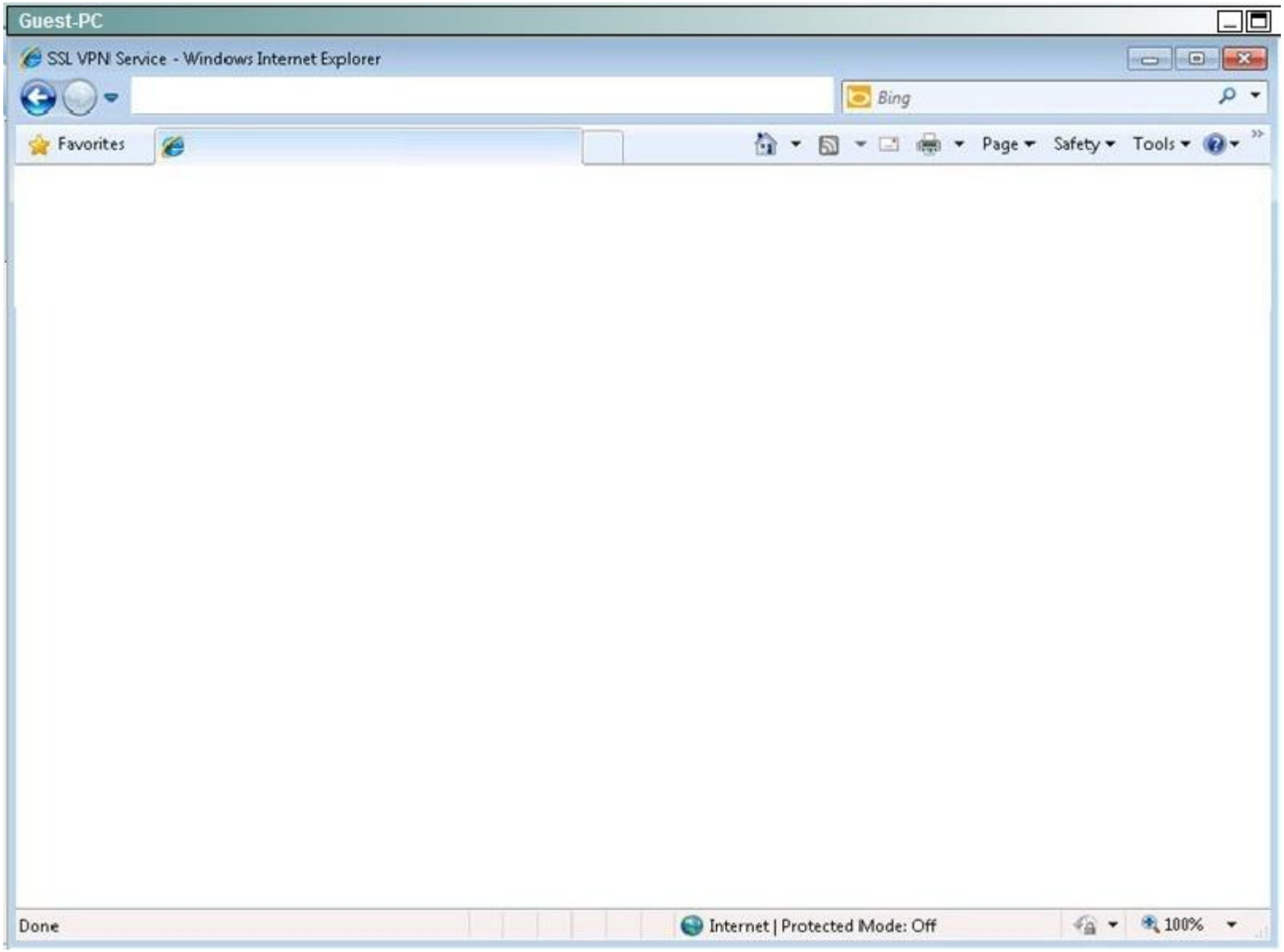
- iii. LOCAL User: vpnuser
- From the Guest PC, reconnect to the SSL VPN Portal
- Test both configured Bookmarks to ensure desired connectivity

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

Topology:


DMZ-Srv
172.16.1.50
Internet
Guest-PC
ASA
HQ-Sr
10.10.3
Admin-PC
Running ASDM



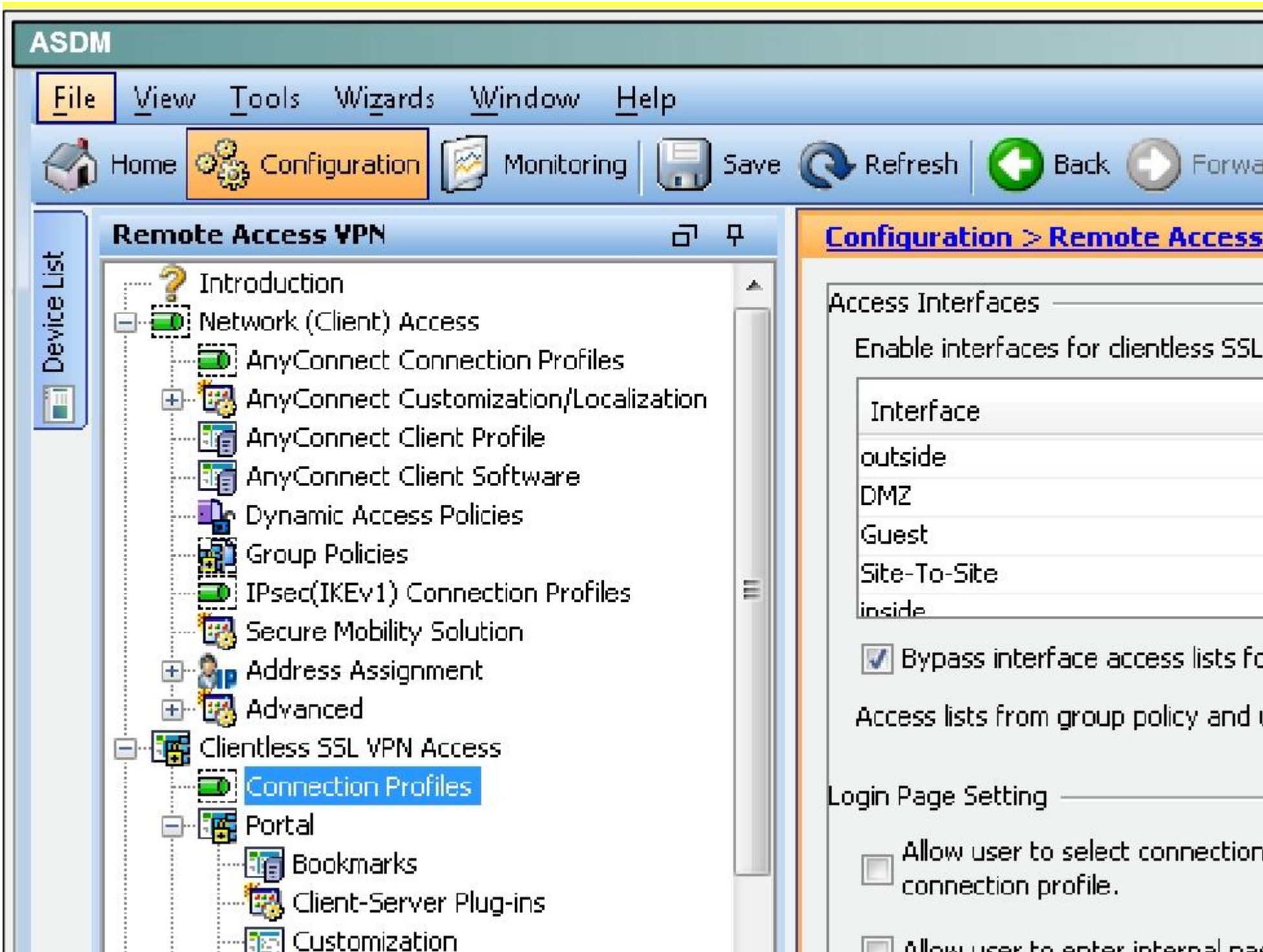


Correct Answer: Answer: Please find the solution in below explanation.
Section: (none)

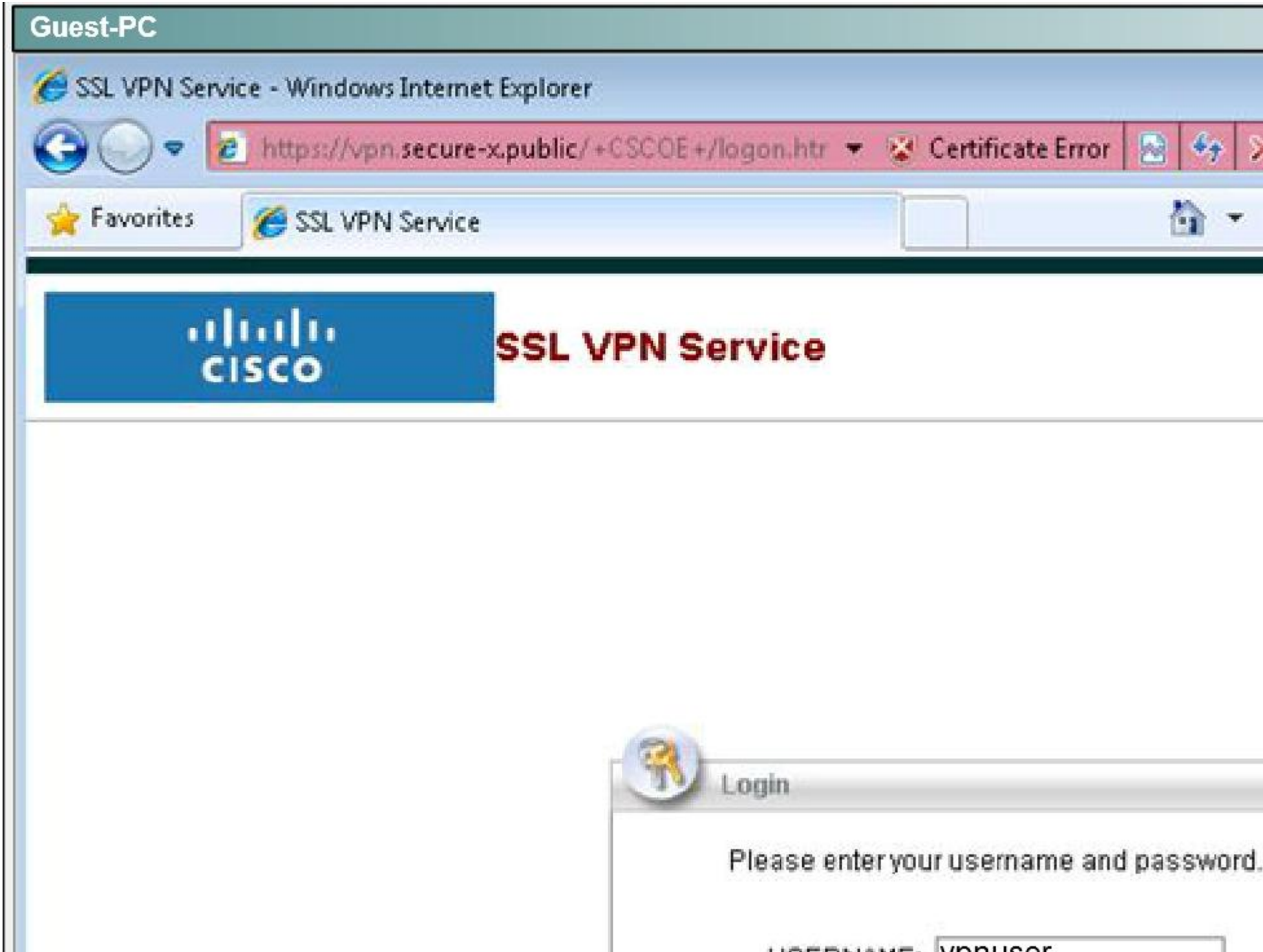
Explanation

Explanation/Reference:
Explanation:

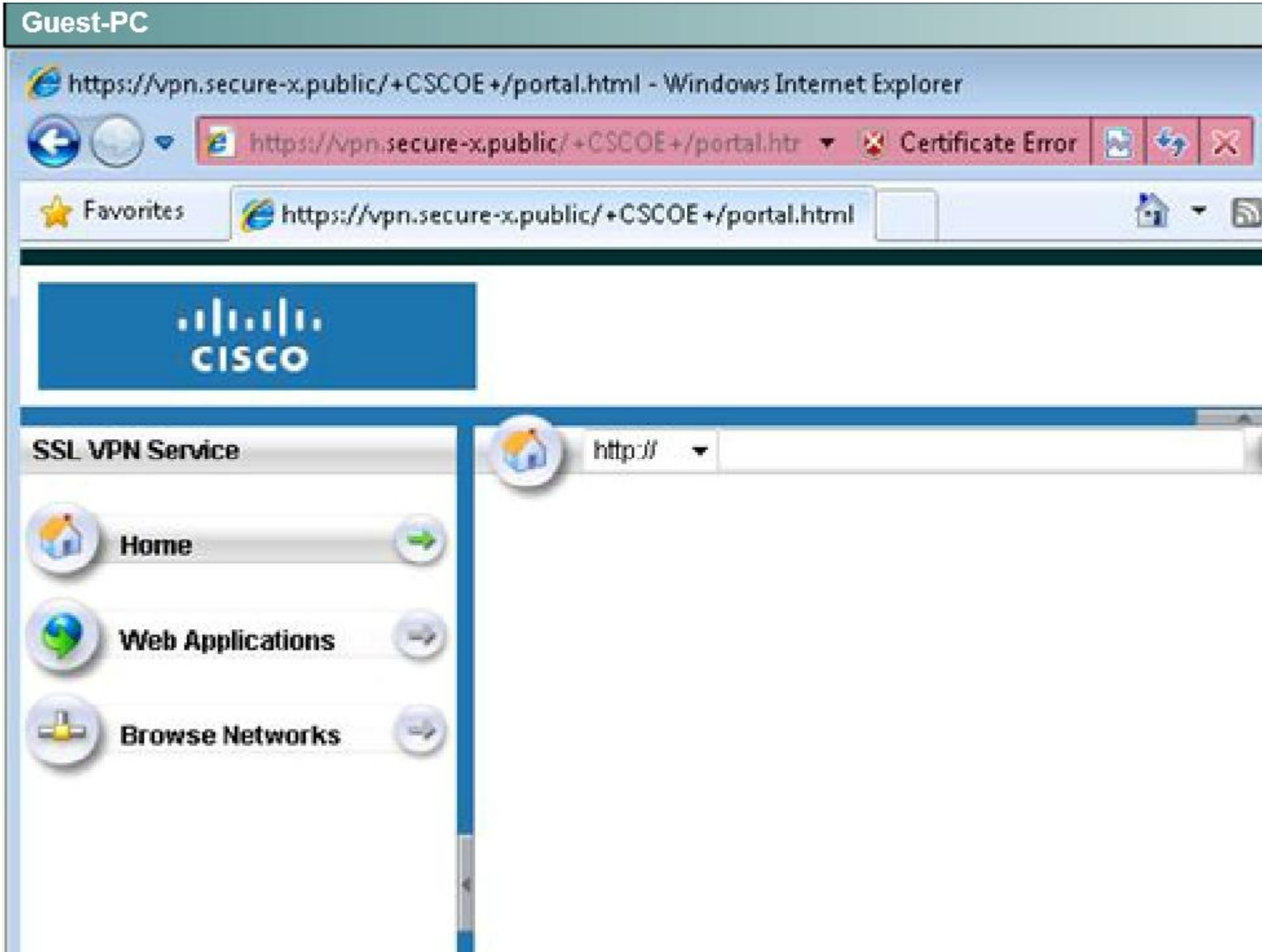
First, enable clientless VPN access on the outside interface by checking the box found below:


ASDM
File
View
Tools
Wizards
Window
Help
Home
Configuration
Monitoring
Save
Refresh
Back
Device List
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Configuration > Remote Access
Access Interfaces
Enable interfaces for clientless SSL
Interface
outside
DMZ
Guest
Site-To-Site
Bypass interface access lists fo
Access lists from group policy and
Login Page Setting
Allow user to select connection
connection profile.

Then, log in to the given URL using the vpnuser/cisco123 credentials:

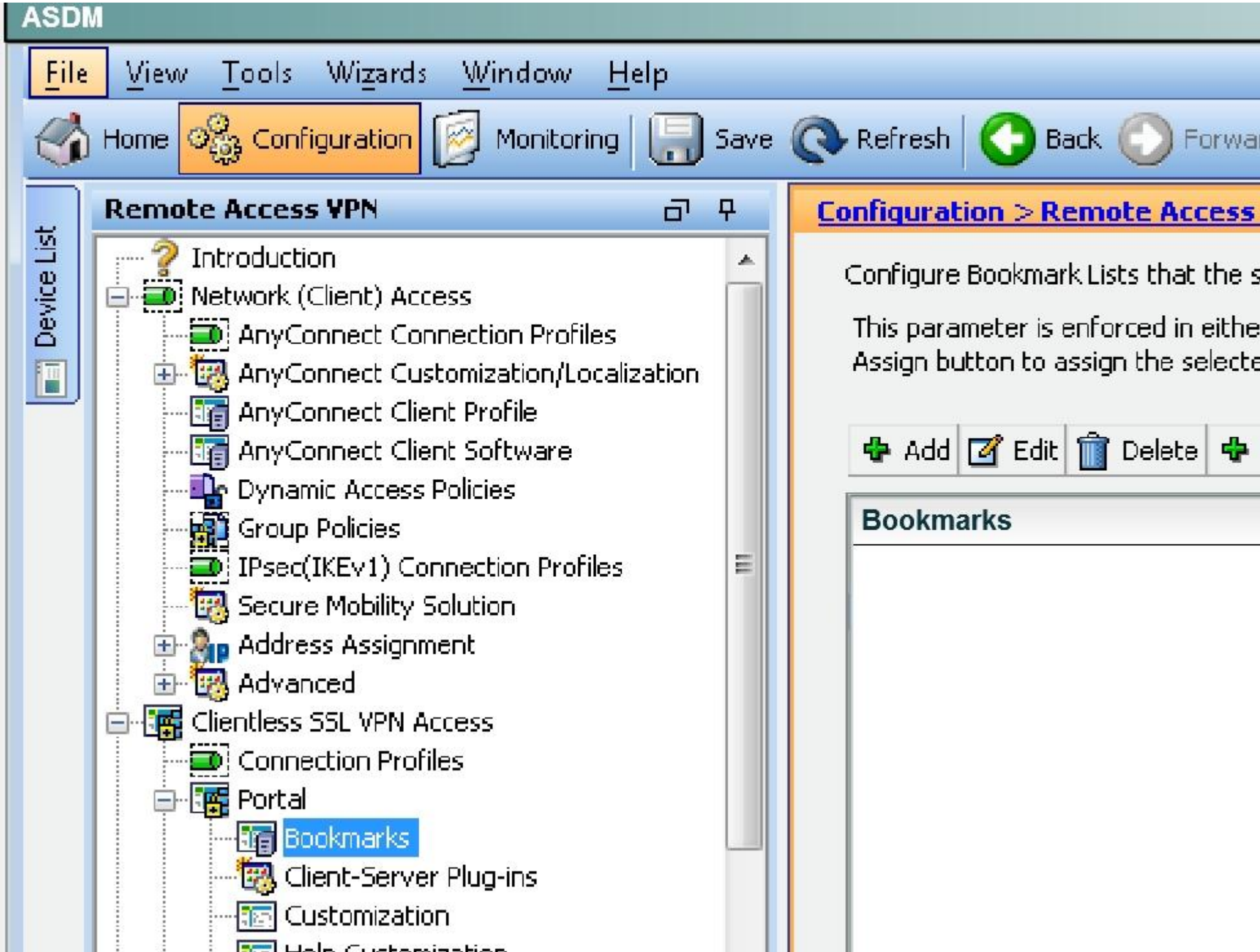

Guest-PC
SSL VPN Service - Windows Internet Explorer
https://vpn.secure-x.public/+CSCOE+/logon.htr
Certificate Error
Favorites
SSL VPN Service
CISCO
SSL VPN Service
Login
Please enter your username and password.

Logging in will take you to this page, which means you have now verified basic connectivity:

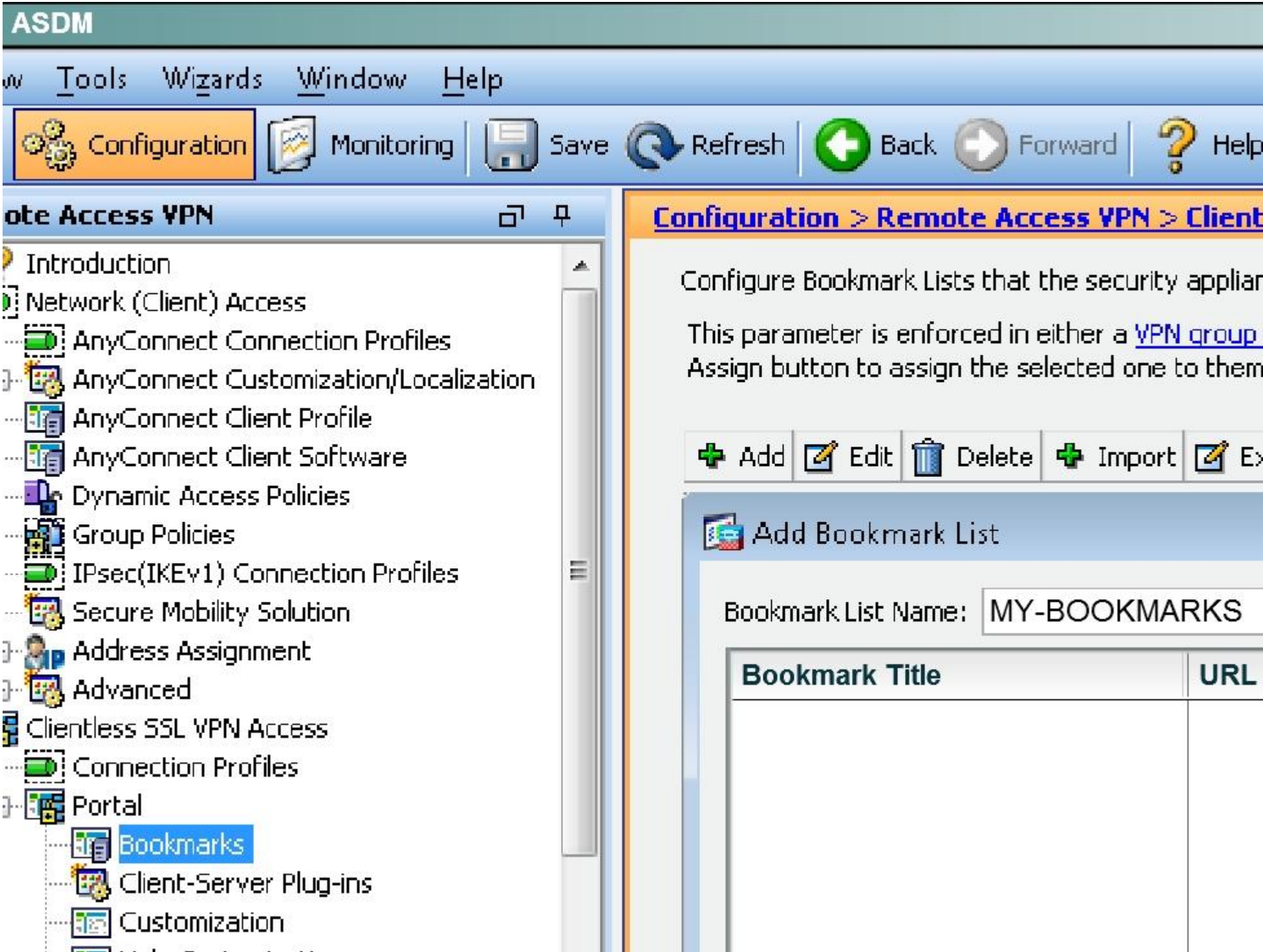

Guest-PC
https://vpn.secure-x.public/+CSCOE+/portal.html - Windows Internet Explorer
https://vpn.secure-x.public/+CSCOE+/portal.htr
Certificate Error
Favorites
https://vpn.secure-x.public/+CSCOE+/portal.html
CISCO
SSL VPN Service
http://
Home
Web Applications
Browse Networks

Now log out by hitting the logout button.

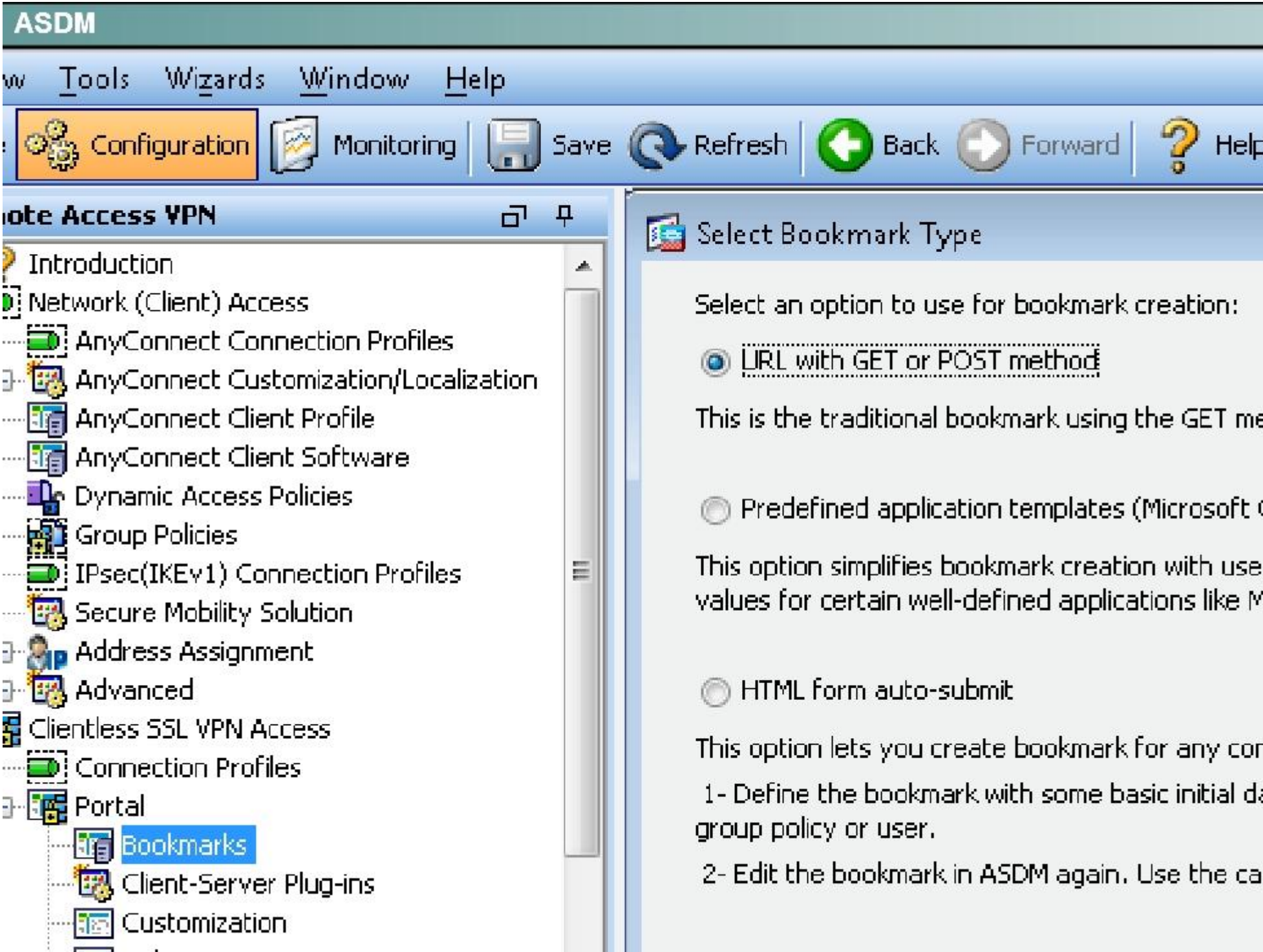
Now, go back to the ASDM and navigate to the Bookmarks portion:


ASDM
File
View
Tools
Wizards
Window
Help
Home
Configuration
Monitoring
Save
Refresh
Back
Device List
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Configuration > Remote Access
Configure Bookmark Lists that the s
This parameter is enforced in eithe
Assign button to assign the selecte
Add
Edit
Delete
Bookmarks

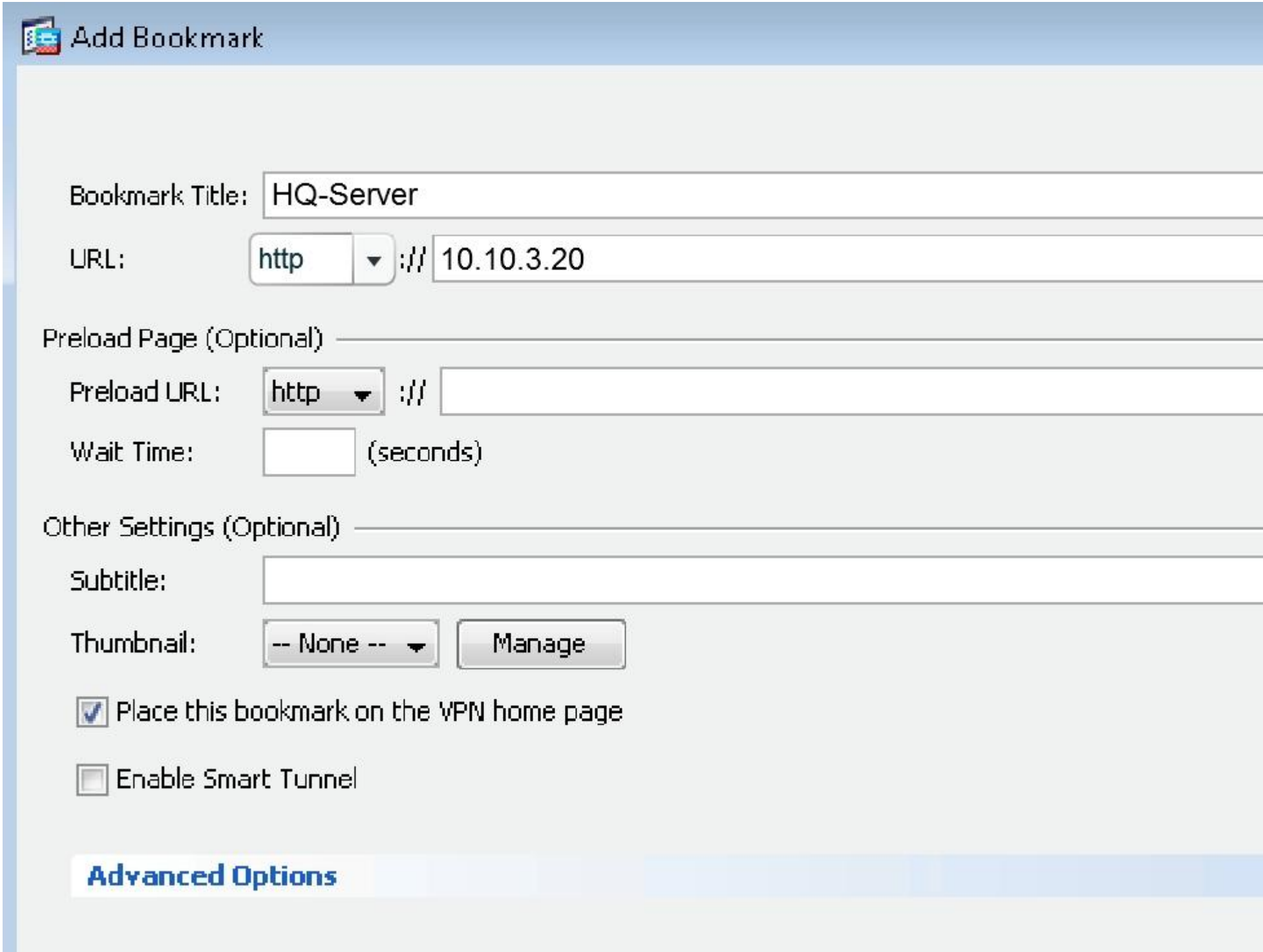
Make the name MY-BOOKMARKS and use the “Add” tab and add the bookmarks per the instructions:

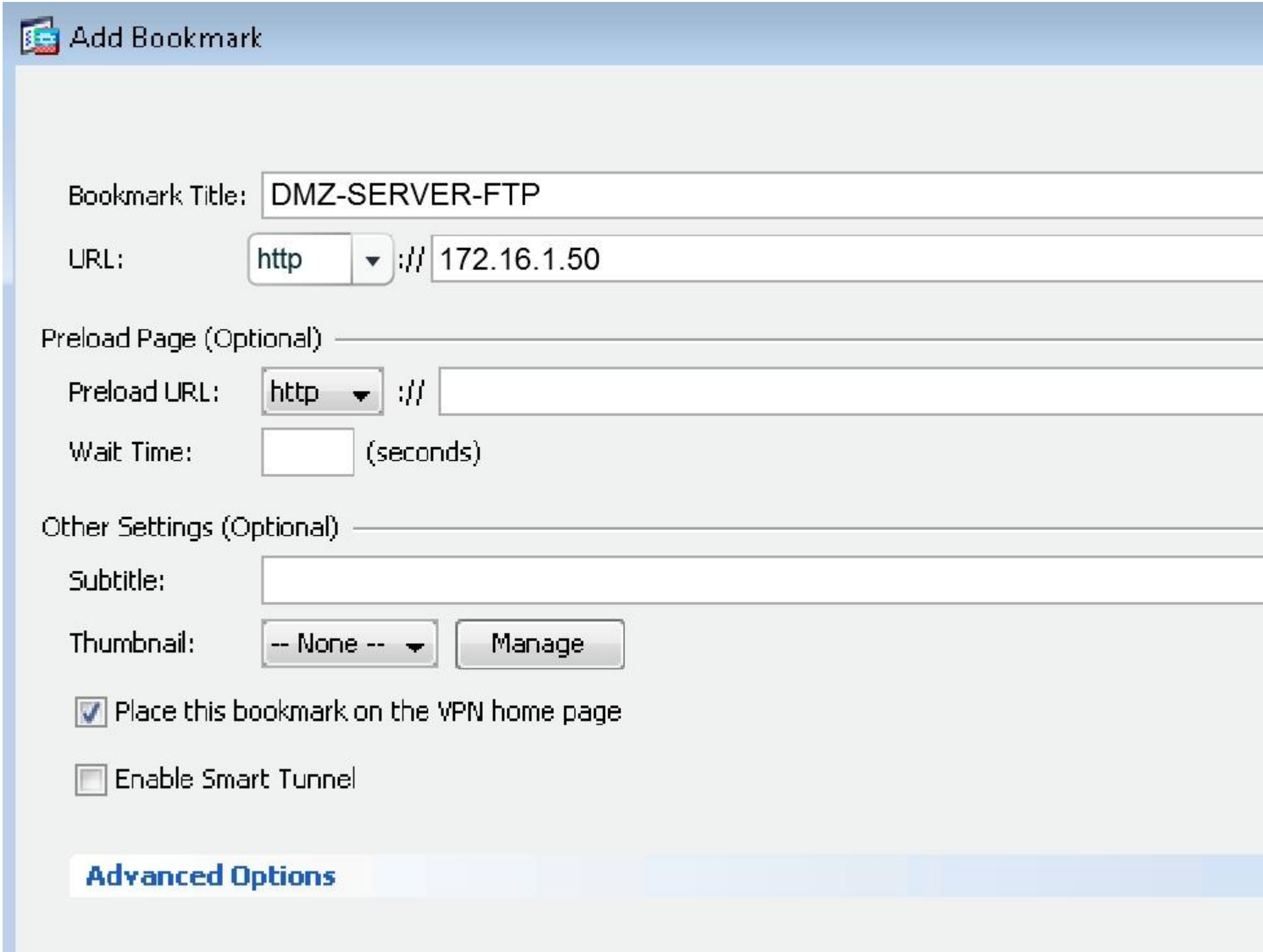

ASDM
Tools
Wizards
Window
Help
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
ote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Configuration > Remote Access VPN > Client
Configure Bookmark Lists that the security appliar
This parameter is enforced in either a VPN group
Assign button to assign the selected one to them
Add
Edit
Delete
Import
Add Bookmark List
Bookmark List Name:
MY-BOOKMARKS
Bookmark Title
URL

Ensure the “URL with GET of POST method” button is selected and hit OK:

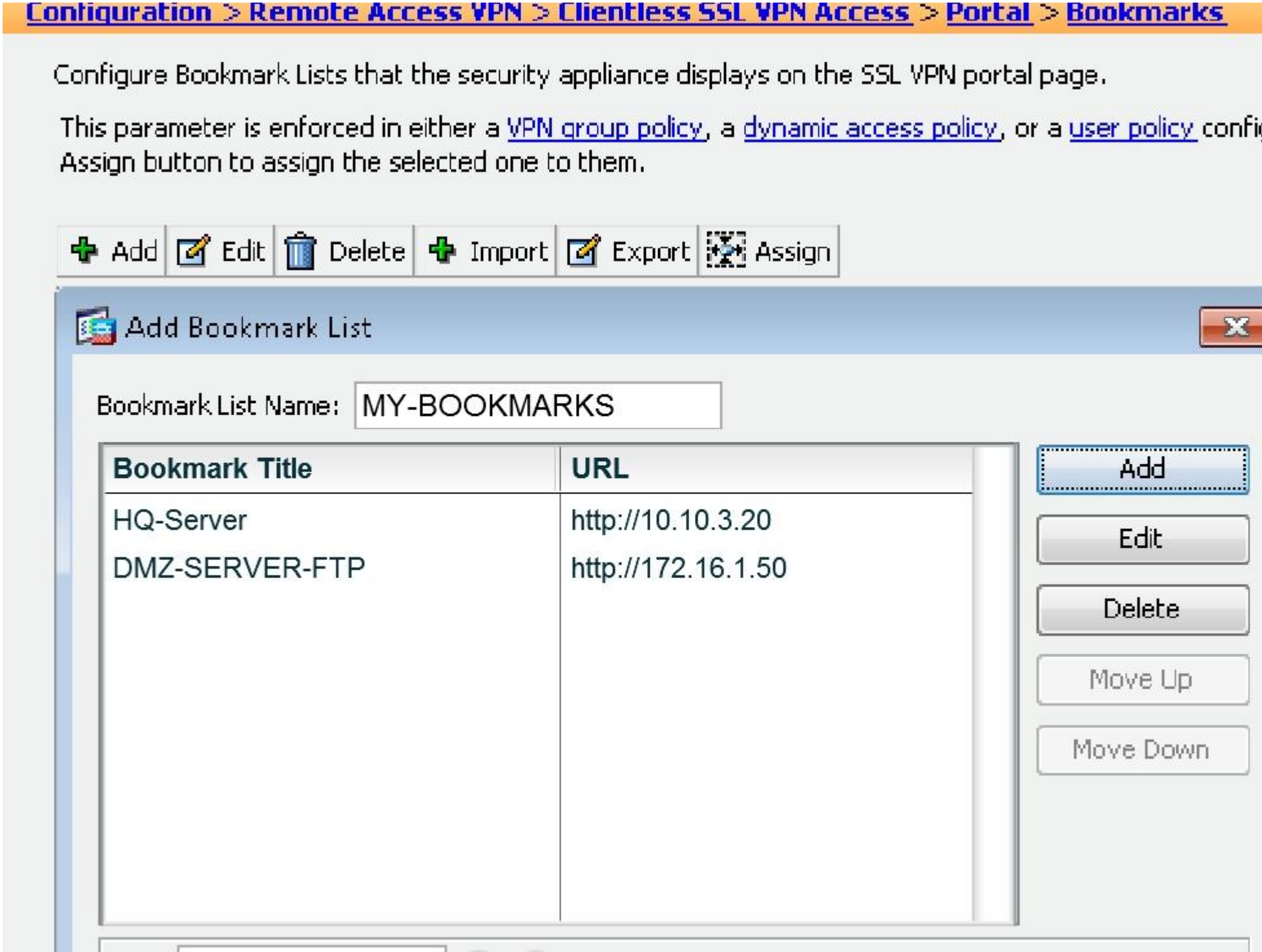

ASDM
Tools
Wizards
Window
Help
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
ote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Select Bookmark Type
Select an option to use for bookmark creation:
URL with GET or POST method
This is the traditional bookmark using the GET me
Predefined application templates (Microsoft
This option simplifies bookmark creation with use
values for certain well-defined applications like M
HTML form auto-submit
This option lets you create bookmark for any con
1- Define the bookmark with some basic initial da
group policy or user.
2- Edit the bookmark in ASDM again. Use the ca

Add the two bookmarks as given in the instructions:

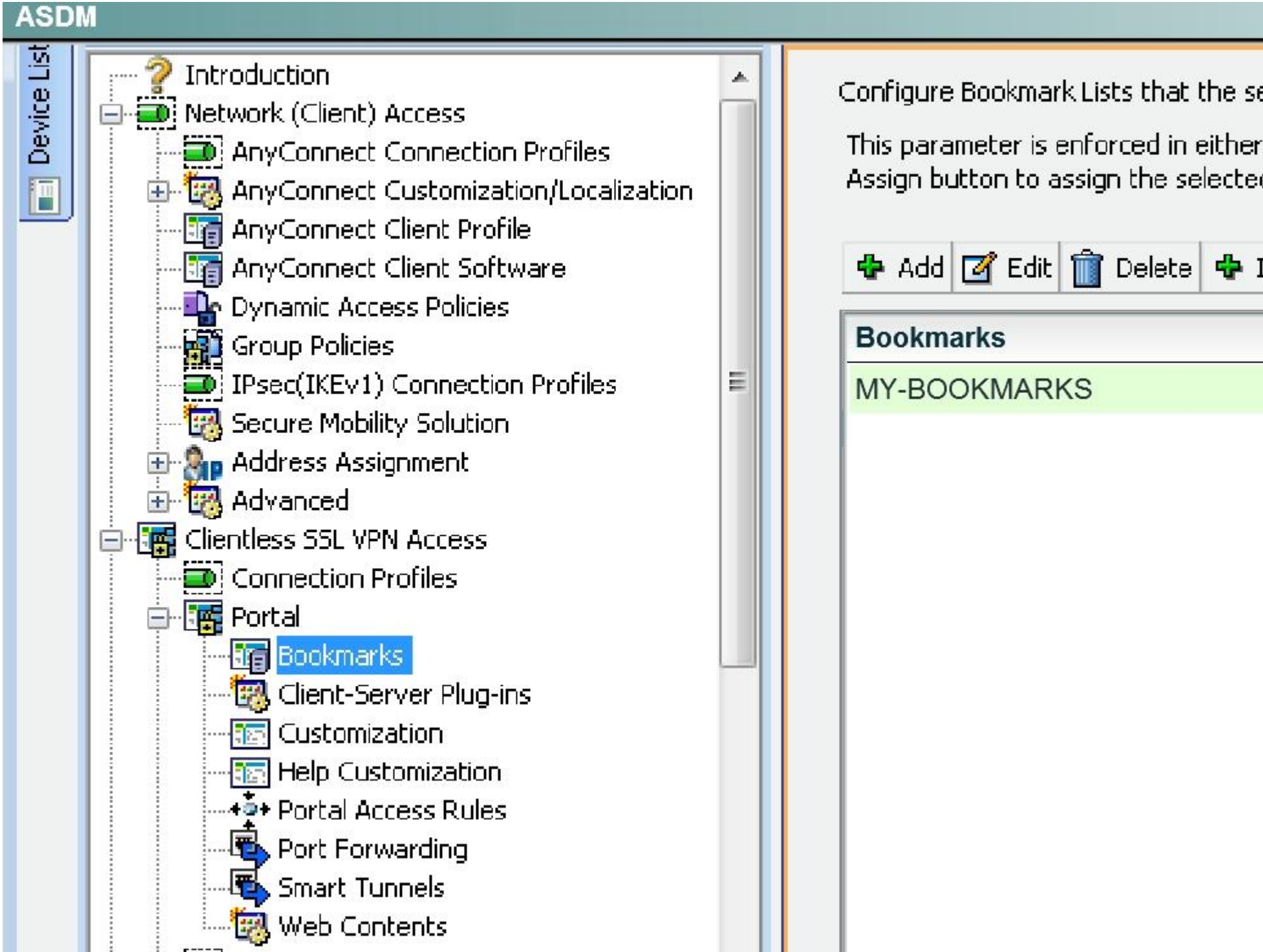

Add Bookmark
Bookmark Title:
HQ-Server
URL:
http
://
10.10.3.20
Preload Page (Optional)
Preload URL:
http
://
Wait Time:
(seconds)
Other Settings (Optional)
Subtitle:
Thumbnail:
-- None --
Manage
Place this bookmark on the VPN home page
Enable Smart Tunnel
Advanced Options


Add Bookmark
Bookmark Title: DMZ-SERVER-FTP
URL: http :// 172.16.1.50
Preload Page (Optional)
Preload URL: http ://
Wait Time: (seconds)
Other Settings (Optional)
Subtitle:
Thumbnail: -- None -- Manage
Place this bookmark on the VPN home page
Enable Smart Tunnel
Advanced Options

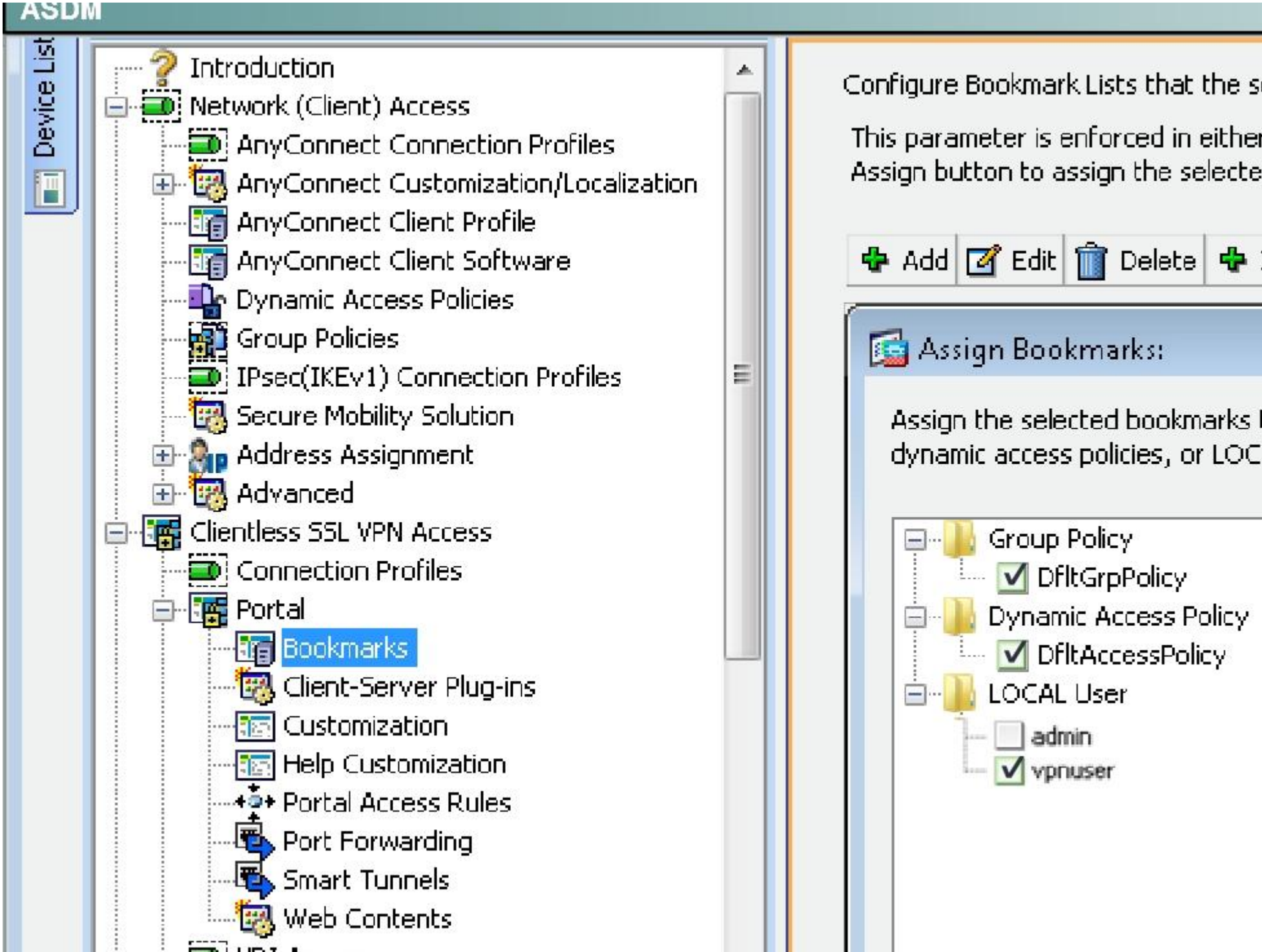
You should now see the two bookmarks listed:


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 confi
Assign button to assign the selected one to them.
Add
Edit
Delete
Import
Export
Assign
Add Bookmark List
Bookmark List Name:
MY-BOOKMARKS
Bookmark Title
URL
HQ-Server
http://10.10.3.20
DMZ-SERVER-FTP
http://172.16.1.50
Add
Edit
Delete
Move Up
Move Down

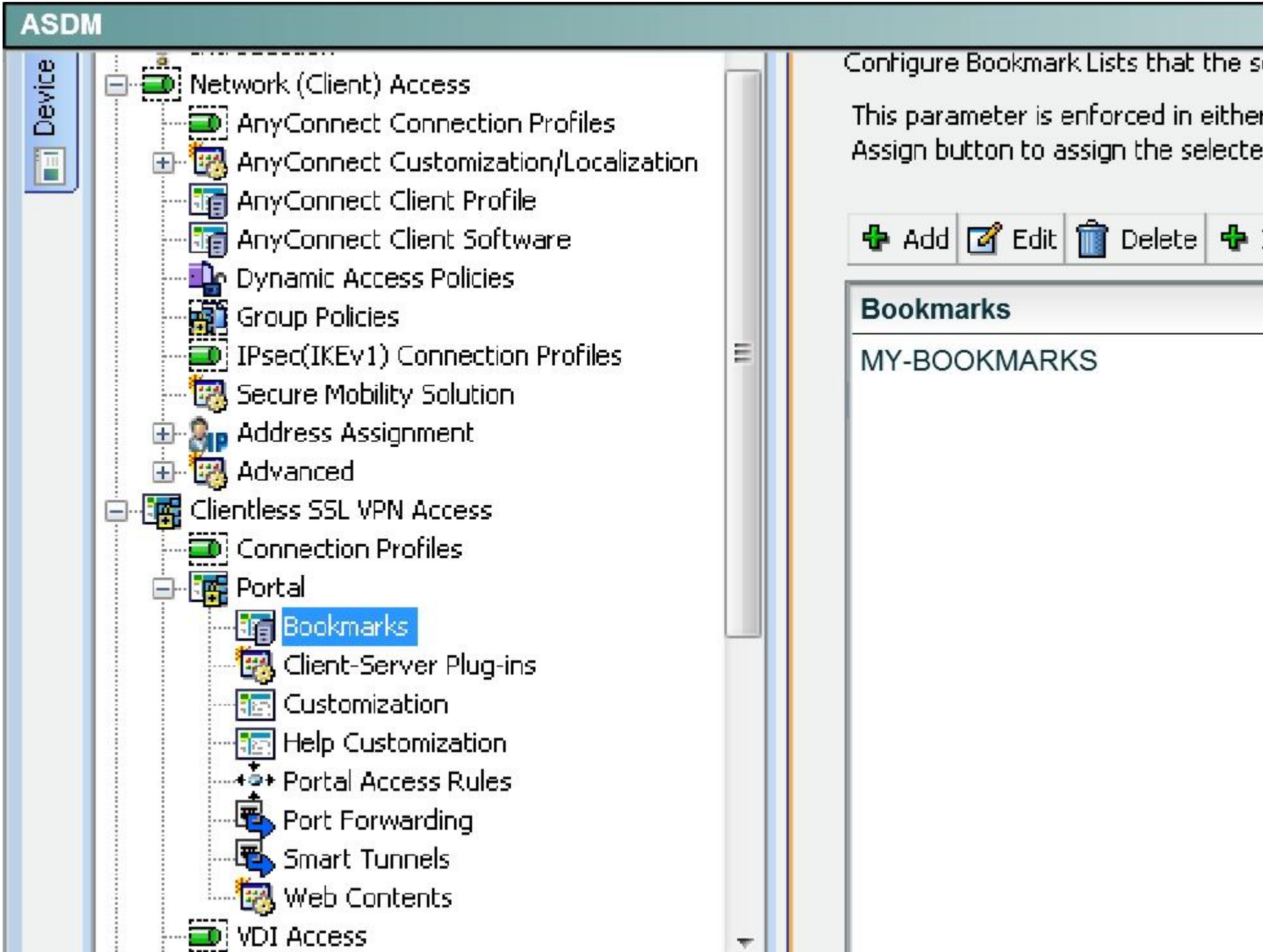
Hit OK and you will see this:


ASDM
Device List
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
Configure Bookmark Lists that the se
This parameter is enforced in either
Assign button to assign the selected
Add
Edit
Delete
Bookmarks
MY-BOOKMARKS

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.


ASDM
Device List
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
Configure Bookmark Lists that the s
This parameter is enforced in either
Assign button to assign the selecte
Add
Edit
Delete
Assign Bookmarks:
Assign the selected bookmarks
dynamic access policies, or LOC
Group Policy
DfltGrpPolicy
Dynamic Access Policy
DfltAccessPolicy
LOCAL User
admin
vpnuser

After hitting OK, you will now see this:


ASDM
Device
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
Connection Profiles
Portal
Bookmarks
Client-Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VDI Access
Configure Bookmark Lists that the s
This parameter is enforced in either
Assign button to assign the selecte
Add
Edit
Delete
Bookmarks
MY-BOOKMARKS

Then, go back to the Guest-PC, log back in and you should be able to test out the two new bookmarks.