Cisco 642-648 Exam Questions & Answers

Number: 642-648
Passing Score: 800
Time Limit: 120 min
File Version: 22.3

Cisco 642-648 Exam Questions & Answers

Exam Name: Deploying Cisco ASA VPN Solutions (VPN v2.0)

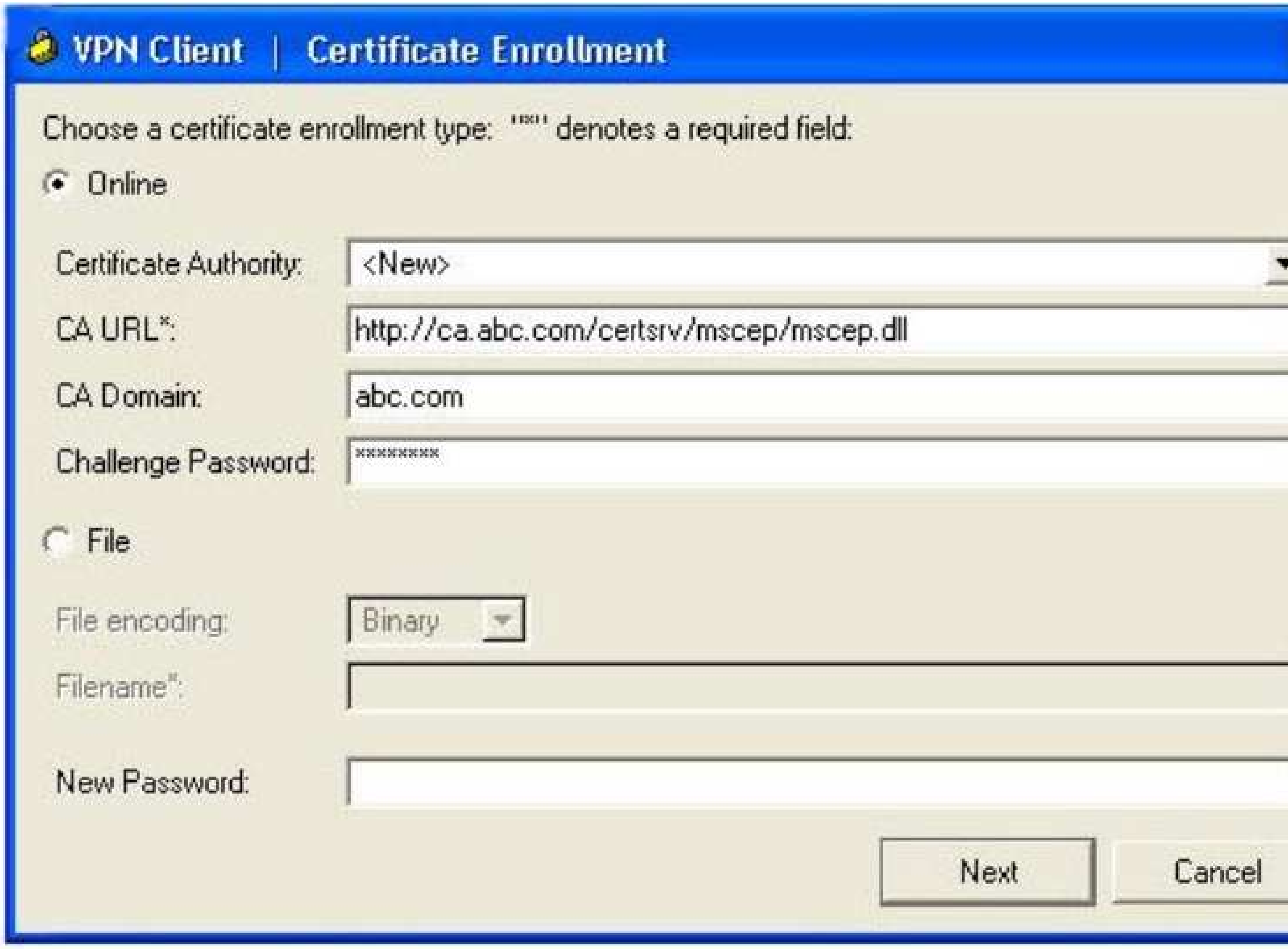
Sections

Exam A

QUESTION 1
Refer to the exhibit.

You are configuring a laptop with the Cisco VPN Client, which uses digital certificates for authentication. Which protocol does the Cisco VPN Client use to retrieve the digital certificate from the CA server?

Exhibit:



Choose a certificate enrollment type: "*" denotes a required field:

● Online

Certificate Authority: <New>

CA URL*: http://ca.abc.com/certsrv/mscep/mscep.dll

CA Domain: abc.com

Challenge Password: *********

○ File

File encoding: Binary

Filename*:

New Password:

A. FTP
B. LDAP
C. HTTPS
D. SCEP
E. OSCP

Correct Answer: D
Section: Certifcates
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html

About CRLs

Certificate Revocation Lists provide the security appliance with one means of determining whether a certificate that is within its valid time range has been revoked by its issuing CA. CRL configuration is a part of the configuration of a trustpoint.

You can configure the security appliance to make CRL checks mandatory when authenticating a certificate (revocation-check crl command). You can also make the CRL check optional by adding the none argument (revocation-check crl none command), which allows the certificate authentication to succeed when the CA is unavailable to provide updated CRL data.

The security appliance can retrieve CRLs from CAs using HTTP, SCEP, or LDAP. CRLs retrieved for each trustpoint are cached for a length of time configurable for each trustpoint.

When the security appliance has cached a CRL for more than the length of time it is configured to cache CRLs, the security appliance considers the CRL too old to be reliable, or "stale". The security appliance attempts to retrieve a newer version of the CRL the next time a certificate authentication requires checking the stale CRL.

QUESTION 2
When using clientless SSL VPN, you might not want some applications or web resources to go through the Cisco ASA appliance. For these application and web resources, as a Cisco ASA administrator, which configuration should you use?

A. Configure the Cisco ASA appliance for split tunneling.
B. Configure network access exceptions in the SSL VPN customization editor.
C. Configure the Cisco ASA appliance to disable content rewriting.
D. Configure the Cisco ASA appliance to enable URL Entry bypass.
E. Configure smart tunnel to bypass the Cisco ASA appliance proxy function.

Correct Answer: C
Section: SSLVPN clientless
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/user/guide/vpn_web.html

Content Rewrite

The Content Rewrite pane lists all applications for which content rewrite is enabled or disabled.

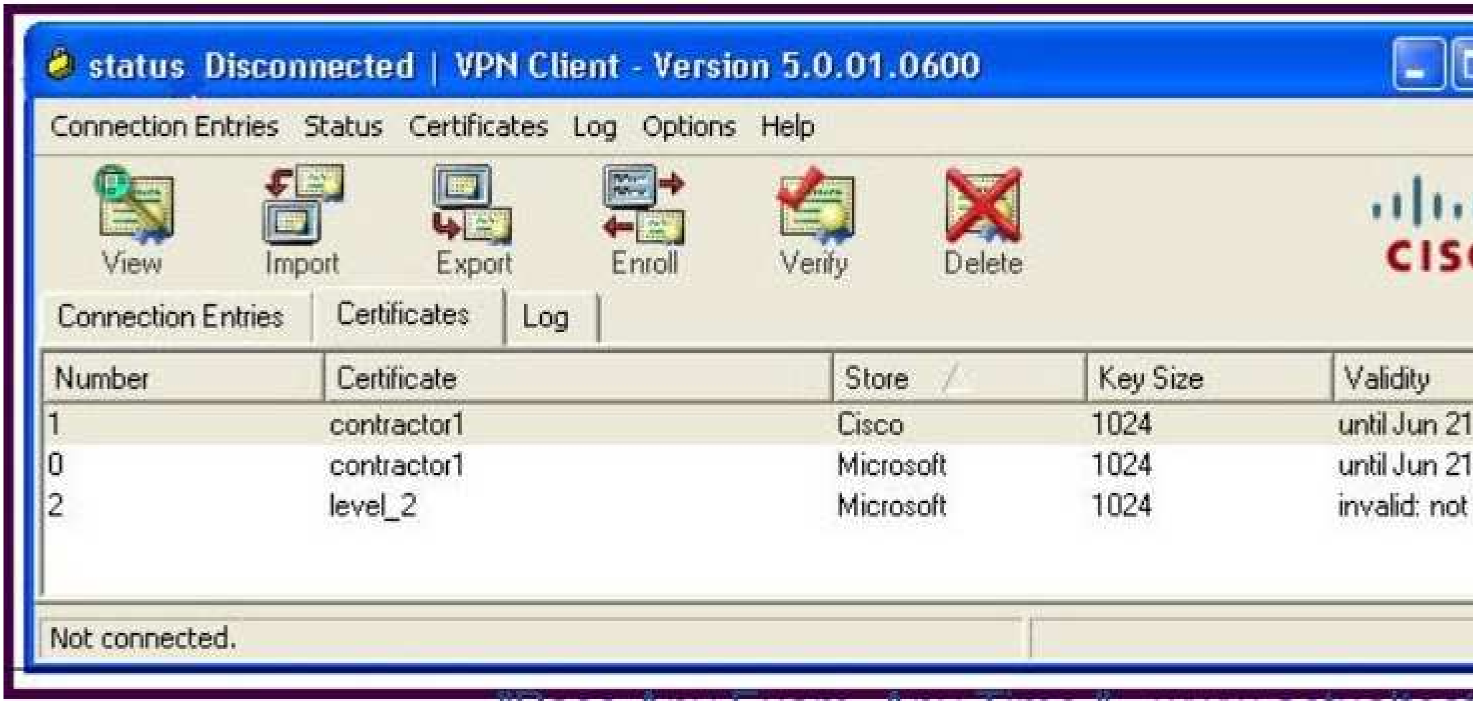
Clientless SSL VPN processes application traffic through a content transformation/rewriting engine that includes advanced elements such as JavaScript, VBScript, Java, and multi-byte characters to proxy HTTP traffic which may have different semantics and access control rules depending on whether the user is using an application within or independently of an SSL VPN device.

By default, the security appliance rewrites, or transforms, all clientless traffic. You might not want some applications and web resources (for example, public websites) to go through the security appliance. The security appliance therefore lets you create rewrite rules that let users browse certain sites and applications without going through the security appliance. This is similar to split-tunneling in an IPSec VPN connection.

You can create multiple rewrite rules. The rule number is important because the security appliance searches rewrite rules by order number, starting with the lowest, and applies the first rule that matches.

QUESTION 3
The "level_2" digital certificate was installed on a laptop.What can cause an "invaliD. not active" status message?

Exhibit:



Number	Certificate	Store	Key Size	Validity
1	contractor1	Cisco	1024	until Jun 21
0	contractor1	Microsoft	1024	until Jun 21
2	level_2	Microsoft	1024	invalid: not

Not connected.

A. On first use, a CA server-supplied passphrase is entered to validate the certificate.

B. A "newly installed" digital certificate does not become active until it is validated by the peer device upon its first usage.

C. The user has not clicked the Verify button within the Cisco VPN Client.

D. The CA server and laptop PC clocks are out of sync.

Correct Answer: D
Section: Troubleshoot
Explanation

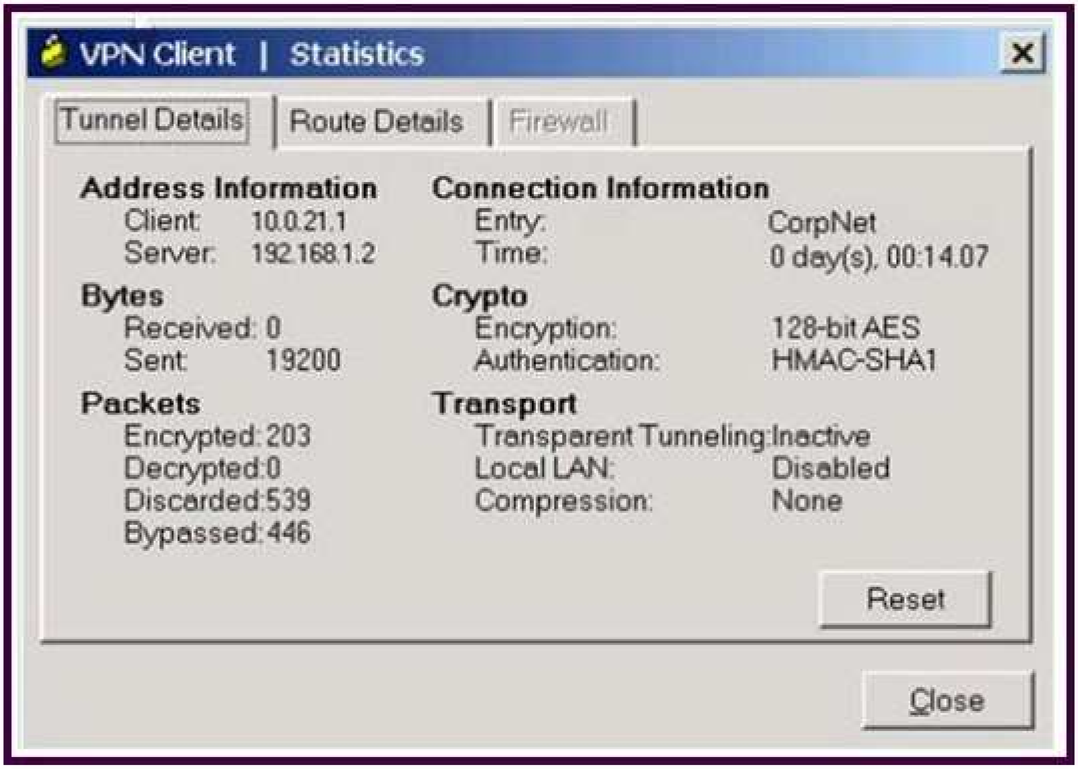
Explanation/Reference:
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html

Certificates have a date and time that they become valid and that they expire. When the security appliance enrolls with a CA and gets a certificate, the security appliance checks that the current time is within the valid range for the certificate. If it is outside that range, enrollment fails.

Same would apply to communciation between ASA and PC

QUESTION 4
A new NOC engineer is troubleshooting a VPN connection. Which statement about the fields within the Cisco VPN Client Statistics screen is correct?

Exhibit:



```
Address Information            Connection Information
   Client:   10.0.21.1            Entry:                      CorpNet
   Server:   192.168.1.2          Time:                       0 day(s), 00:14.07
Bytes                          Crypto
   Received: 0                    Encryption:                 128-bit AES
   Sent:     19200                Authentication:             HMAC-SHA1
Packets                        Transport
   Encrypted: 203                 Transparent Tunneling:Inactive
   Decrypted:0                    Local LAN:                  Disabled
   Discarded:539                  Compression:                None
   Bypassed: 446
```

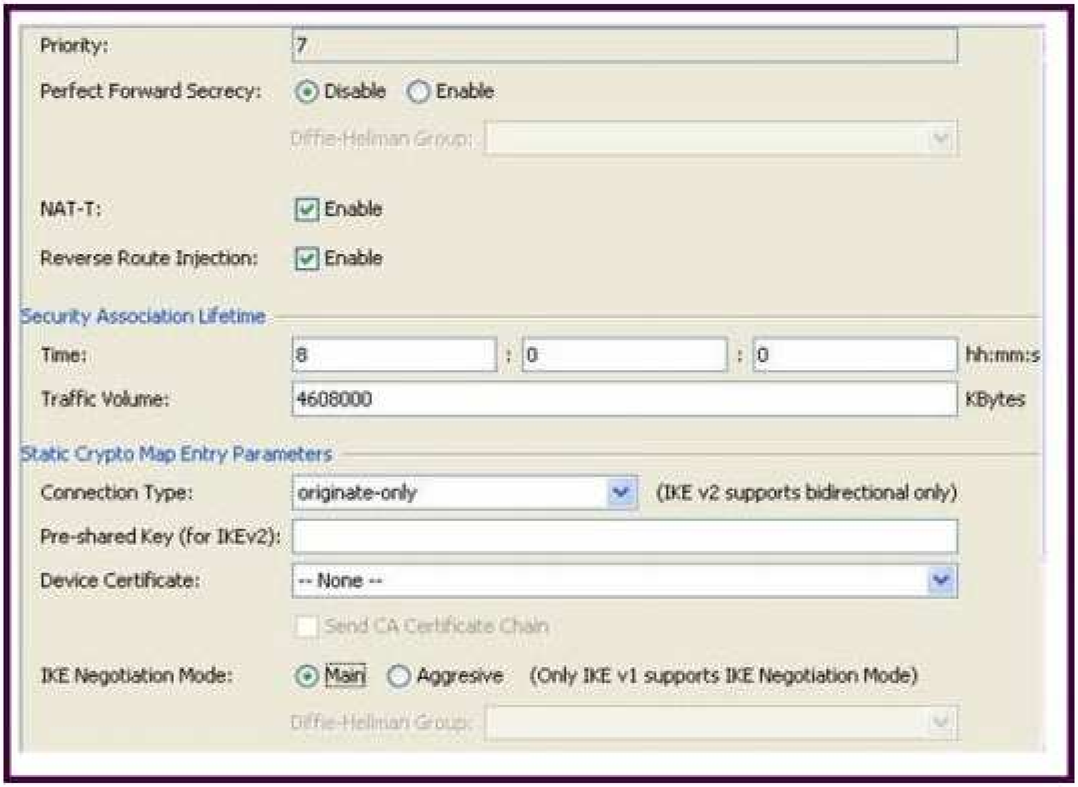
A. The ISP-assigned IP address of 10.0.21.1 is assigned to the VPN adapter of the PC.
B. The IP address of the security appliance to which the Cisco VPN Client is connected is 192.168.1.2.
C. CorpNet is the name of the Cisco ASA group policy whose tunnel parameters the connection is using.
D. The ability of the client to send packets transparently and unencrypted through the tunnel for test purposes is turned off.
E. With split tunneling enabled, the Cisco VPN Client registers no decrypted packets.

Correct Answer: B
Section: Troubleshoot
Explanation

Explanation/Reference:

QUESTION 5
While configuring a site-to-site VPN tunnel, a new NOC engineer encounters the Reverse Route Injection parameter. Assuming that static routes are redistributed by the Cisco ASA to the IGP, what effect does enabling Reverse Route Injection on the local Cisco ASA have on a configuration?

Exhibit:



Priority: 7

Perfect Forward Secrecy: ● Disable ○ Enable

Diffie-Hellman Group:

NAT-T: ☑ Enable

Reverse Route Injection: ☑ Enable

Security Association Lifetime

Time: 8 : 0 : 0 hh:mm:s

Traffic Volume: 4608000 KBytes

Static Crypto Map Entry Parameters

Connection Type: originate-only (IKE v2 supports bidirectional only)

Pre-shared Key (for IKEv2):

Device Certificate: -- None --

□ Send CA Certificate Chain

IKE Negotiation Mode: ● Main ○ Aggresive (Only IKE v1 supports IKE Negotiation Mode)

Diffie-Hellman Group:

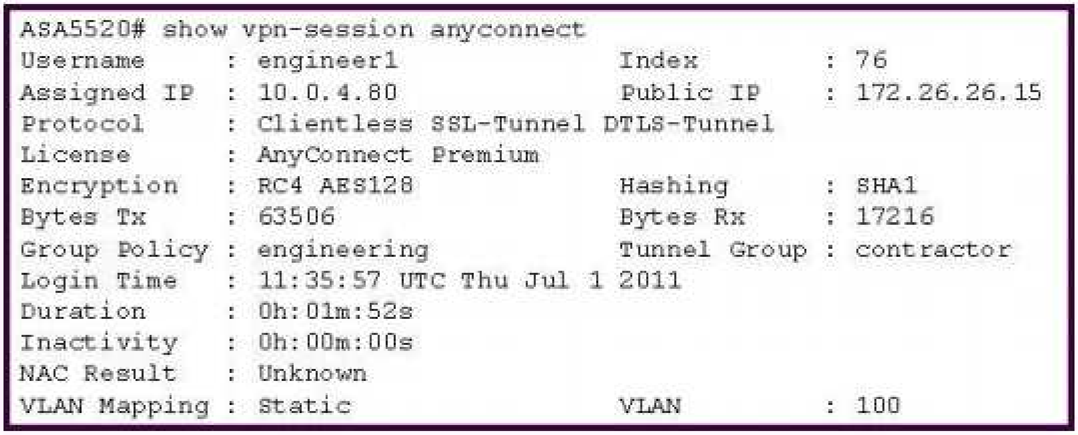
A. The local Cisco ASA advertises its default routes to the distant end of the site-to-site VPN tunnel.
B. The local Cisco ASA advertises routes from the dynamic routing protocol that is running on the local Cisco ASA to the distant end of the site-to-site VPN tunnel.
C. The local Cisco ASA advertises routes that are at the distant end of the site-to-site VPN tunnel.
D. The local Cisco ASA advertises routes that are on its side of the site-to-site VPN tunnel to the distant end of the site-to-site VPN tunnel.

Correct Answer: C
Section: IPsec
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809d07de.shtml

QUESTION 6
A NOC engineer needs to tune some prelogin parameters on an SSL VPN tunnel.
From the information that is shown, where should the engineer navigate to find the prelogin session attributes?

Exhibit:



```
ASA5520# show vpn-session anyconnect
Username     : engineer1              Index        : 76
Assigned IP  : 10.0.4.80              Public IP    : 172.26.26.15
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 63506                  Bytes Rx     : 17216
Group Policy : engineering            Tunnel Group : contractor
Login Time   : 11:35:57 UTC Thu Jul 1 2011
Duration     : 0h:01m:52s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : Static                 VLAN         : 100
```

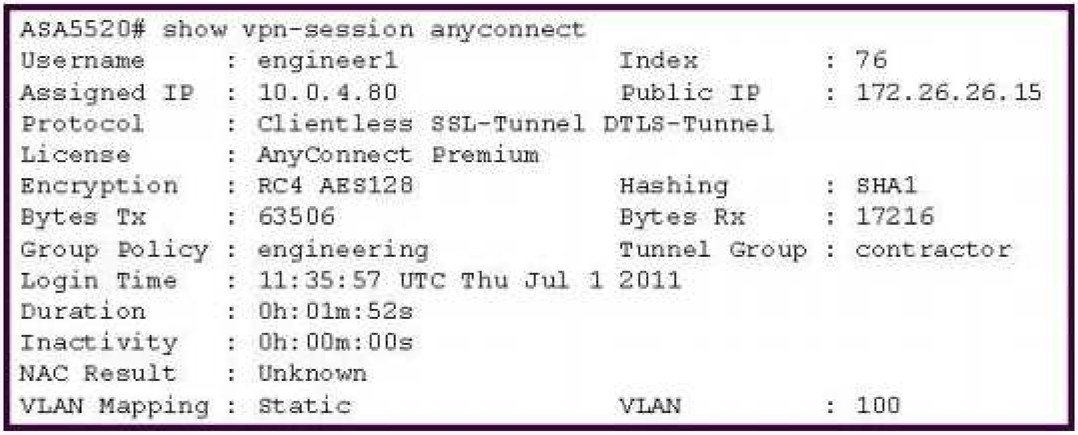
A. "engineering" Group Policy
B. "contractor" Connection Profile
C. "engineer1" AAA/Local Users
D. DfltGrpPolicy Group Policy

Correct Answer: B
Section: Troubleshoot
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/ac05hostscanposture.html#wp1039696

QUESTION 7
A NOC engineer needs to tune some postlogin parameters on an SSL VPN tunnel.
From the information shown, where should the engineer navigate to, in order to find all the postlogin session parameters?

Exhibit:



```
ASA5520# show vpn-session anyconnect
Username     : engineer1              Index        : 76
Assigned IP  : 10.0.4.80              Public IP    : 172.26.26.15
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 63506                  Bytes Rx     : 17216
Group Policy : engineering            Tunnel Group : contractor
Login Time   : 11:35:57 UTC Thu Jul 1 2011
Duration     : 0h:01m:52s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : Static                 VLAN         : 100
```

A. "engineering" Group Policy
B. "contractor" Connection Profile
C. DefaultWEBVPNGroup Group Policy
D. DefaultRAGroup Group Policy
E. "engineer1" AAA/Local Users

Correct Answer: A
Section: Troubleshoot
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htwebvpn.html#wp1054618

The policy group is a container that defines the presentation of the portal and the permissions for resources that are configured for a group of remote users. Entering the policy group command places the router in webvpn group policy configuration mode. After it is configured, the group policy is attached to the SSL VPN context configuration by configuring the default-group-policy command. The following tasks are accomplished in this configuration:

•The presentation of the SSL VPN portal page is configured.

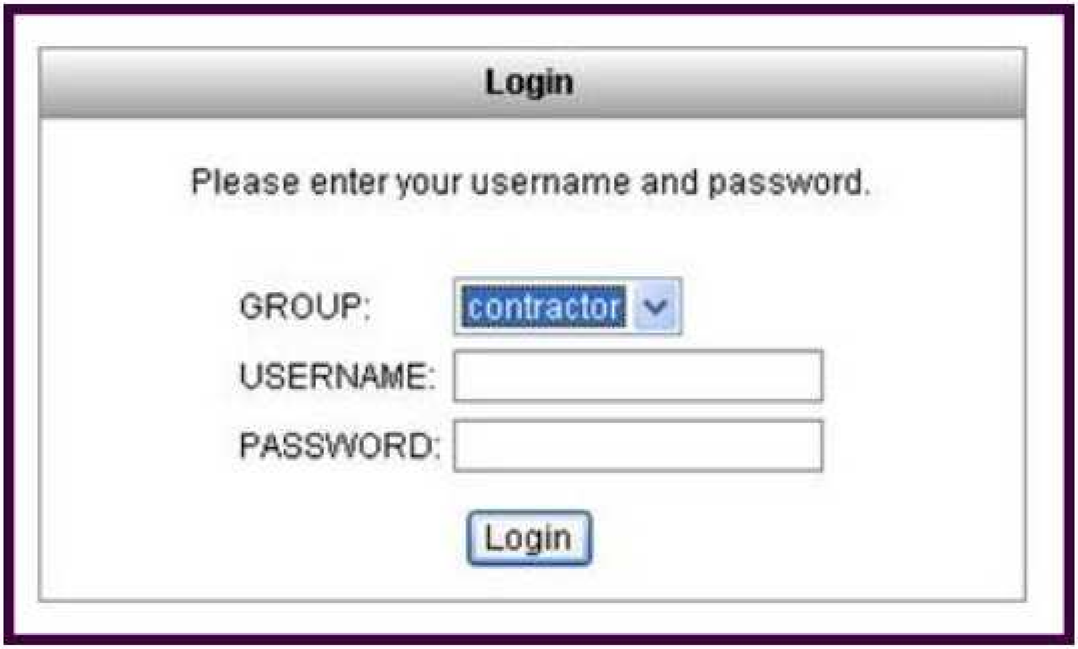
•A NetBIOS server list is referenced.

•A port-forwarding list is referenced.

•The idle and session timers are configured.
•A URL list is referenced.

QUESTION 8
For the ABC Corporation, members of the NOC need the ability to select tunnel groups from a drop-down menu on the Cisco WebVPN login page.
As the Cisco ASA administrator, how would you accomplish this task?

Exhibit:



Login

Please enter your username and password.

GROUP: contractor

USERNAME:

PASSWORD:

A. Define a special identity certificate with multiple groups, which are defined in the certificate OU field, that will grant the certificate holder access to the named groups on the login page.
B. Under Group Policies, define a default group that encompasses the required individual groups that will appear on the login page.
C. Under Connection Profiles, define a NOC profile that encompasses the required individual profiles that will appear on the login page.
D. Under Connection Profiles, enable "Allow user to select connection profile."

Correct Answer: D
Section: Troubleshoot
Explanation

Explanation/Reference:
Cisco ASDM User Guide Version 6.1

Add or Edit SSL VPN Connections > Advanced > SSL VPN

This dialog box lets you configure attributes that affect what the remote user sees upon login. **Fields** • Login Page Customization—Configures the look and feel of the user login page by specifying which preconfigured customization attributes to apply. The default is DfltCustomization. • Manage—Opens the Configure GUI Customization Objects window. • Connection Aliases—Lists in a table the existing connection aliases and their status and lets you add or delete items in that table. A connection alias appears on the user login page if the connection is configured to allow users to select a particular connection (tunnel group) at login. **–** Add—Opens the Add Connection Alias window, on which you can add and enable a connection alias. **–** Delete—Removes the selected row from the connection alias table. There is no confirmation or undo. • Group URLs—Lists in a table the existing group URLs and their status and lets you add or delete items in that table. A group URL appears on the user login page if the connection is configured to allow users to select a particular group at login. **–** Add—Opens the Add Group URL window, on which you can add and enable a group URL. **–** Delete—Removes the selected row from the connection alias table. There is no confirmation or undo.

QUESTION 9
Your corporate finance department purchased a new non-web-based TCP application tool to run on one of its servers. Certain finance employees need remote access to the software during nonbusiness hours. These employees do not have "admin" privileges to their PCs.
What is the correct way to configure the SSL VPN tunnel to allow this application to run?

A. Configure a smart tunnel for the application.
B. Configure a "finance tool" VNC bookmark on the employee clientless SSL VPN portal.
C. Configure the plug-in that best fits the application.
D. Configure the Cisco ASA appliance to download the Cisco AnyConnect SSL VPN Client to the finance employee each time an SSL VPN tunnel is established.

Correct Answer: A
Section: Troubleshoot
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/webvpn.html

A smart tunnel is a connection between a TCP-based application and a private site, using a clientless (browser-based) SSL VPN session with the security appliance as the pathway, and the security appliance as a proxy server. You can identify applications to which you want to grant smart tunnel access, and specify the local path to each application. For applications running on Microsoft Windows, you can also require a match of the SHA-1 hash of the checksum as a condition for granting smart tunnel access.

Lotus SameTime and Microsoft Outlook Express are examples of applications to which you might want to grant smart tunnel access.

Configuring smart tunnels requires one of the following procedures, depending on whether the application is a client or is a web-enabled application:

•Create one or more smart tunnel lists of the client applications, then assign the list to the group policies or local user policies for whom you want to provide smart tunnel access.

•Create one or more bookmark list entries that specify the URLs of the web-enabled applications eligible for smart tunnel access, then assign the list to the DAPs, group policies, or local user policies for whom you want to provide smart tunnel access.

You can also list web-enabled applications for which to automate the submission of login credentials in smart tunnel connections over clientless SSL VPN sessions.

Why Smart Tunnels?

Smart tunnel access lets a client TCP-based application use a browser-based VPN connection to connect to a service. It offers the following advantages to users, compared to plug-ins and the legacy technology, port forwarding:

•Smart tunnel offers better performance than plug-ins.

•Unlike port forwarding, smart tunnel simplifies the user experience by not requiring the user connection of the local application to the local port.

•Unlike port forwarding, smart tunnel does not require users to have administrator privileges.

The advantage of a plug-in is that it does not require the client application to be installed on the remote computer.

Smart Tunnel Requirements, Restrictions, and Limitations

The following sections categorize the smart tunnel requirements and limitations.

General Requirements and Limitations

Smart tunnel has the following general requirements and limitations:

•The remote host originating the smart tunnel must be running a 32-bit version of Microsoft Windows Vista, Windows XP, or Windows 2000; or Mac OS 10.4 or 10.5.

•Smart tunnel auto sign-on supports only Microsoft Internet Explorer on Windows.

•The browser must be enabled with Java, Microsoft ActiveX, or both.

•Smart tunnel supports only proxies placed between computers running Microsoft Windows and the security appliance. Smart tunnel uses the Internet Explorer configuration (that is, the one intended for system-wide use in Windows). If the remote computer requires a proxy server to reach the security appliance, the URL of the terminating end of the connection must be in the list of URLs excluded from proxy services. If the proxy configuration specifies that traffic destined for the ASA goes through a proxy, all smart tunnel traffic goes through the proxy.

In an HTTP-based remote access scenario, sometimes a subnet does not provide user access to the VPN gateway. In this case, a proxy placed in front of the ASA to route traffic between the web and the end user's location provides web access. However, only VPN users can configure proxies placed in front of the ASA. When doing so, they must make sure these proxies support the CONNECT method. For proxies that require authentication, smart tunnel supports only the basic digest authentication type.

•When smart tunnel starts, the security appliance by default passes all browser traffic through the VPN session if the browser process is the same. The security appliance also does this if a tunnel-all policy applies. If the user starts another instance of the browser process, it passes all traffic through the VPN session. If the browser process is the same and the security appliance does not provide access to a URL, the user cannot open it. As a workaround, assign a tunnel policy that is not tunnel-all.

•A stateful failover does not retain smart tunnel connections. Users must reconnect following a failover.

QUESTION 10
Which statement about plug-ins is false?

A. Plug-ins do not require any installation on the remote system.
B. Plug-ins require administrator privileges on the remote system.
C. Plug-ins support interactive terminal access.
D. Plug-ins are not supported on the Windows Mobile platform.

Correct Answer: B
Section: SSLVPN clientless
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html#wp1162435

Plug-ins

The security appliance supports Java plug-ins for clientless SSL VPN connections. Plug-ins are Java programs that operate in a browser. These plug-ins include SSH/Telnet, RDP, VNC, and Citrix.

Per the GNU General Public License (GPL), Cisco redistributes plug-ins without making any changes to them. Per the GPL, Cisco cannot directly enhance these plug-ins.

To use plug-ins you must install Java Runtime Environment (JRE) 1.4.2.x or greater. You must also use a compatible browser specified here: http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html

QUESTION 11
Authorization of a clientless SSL VPN defines the actions that a user may perform within a clientless SSL VPN session. Which statement is correct concerning the SSL VPN authorization process?

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

Correct Answer: B
Section: SSLVPN clientless
Explanation

Explanation/Reference:
CISCO SSL VPN guide

The **aaa authentication** command is entered to specify an authentication list or server group under a SSL VPN context configuration. If this command is not configured and AAA is configured globally on the router, global authentication will be applied to the context configuration.
The database that is configured for remote-user authentication on the SSL VPN gateway can be a local

database, or the database can be accessed through any RADIUS or TACACS+ AAA server.
We recommend that you use a separate AAA server, such as a Cisco Access Control Server (ACS). A separate AAA server provides a more robust security solution. It allows you to configure unique passwords for each remote user and accounting and logging for remote-user sessions.

QUESTION 12
After adding a remote-access IPsec tunnel via the VPN wizard, an administrator needs to tune the IPsec policy parameters. Where is the correct place to tune the IPsec policy parameters in Cisco ASDM?

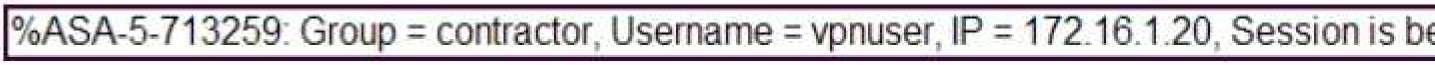
A. IPsec user profile
B. Crypto Map
C. Group Policy
D. IPsec Policy
E. IKE Policy

Correct Answer: B
Section: IPsec
Explanation

Explanation/Reference:

QUESTION 13
While troubleshooting a remote-access application, a new NOC engineer received the logging message that is shown in the exhibit.
Which configuration is most likely to be mismatched?

Exhibit:



```
%ASA-5-713259: Group = contractor, Username = vpnuser, IP = 172.16.1.20, Session is be
```

A. IKE configuration
B. extended authentication configuration
C. IPsec configuration
D. digital certificate configuration

Correct Answer: C
Section: IPsec
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a00800949c5.shtml

and

```
%ASA-5-713259: Group = groupname, Username = username, IP = peerIP,
Session is being torn down. Reason: reason
```

Explanation The termination reason for the ISAKMP session appears, which occurs when the session is torn down through session management.

•groupname—The tunnel group of the session being terminated

•username—The username of the session being terminated

•peerIP—The peer address of the session being terminated

•reason—The RADIUS termination reason of the session being terminated. Reasons include the following:

- Port Preempted (simultaneous logins)

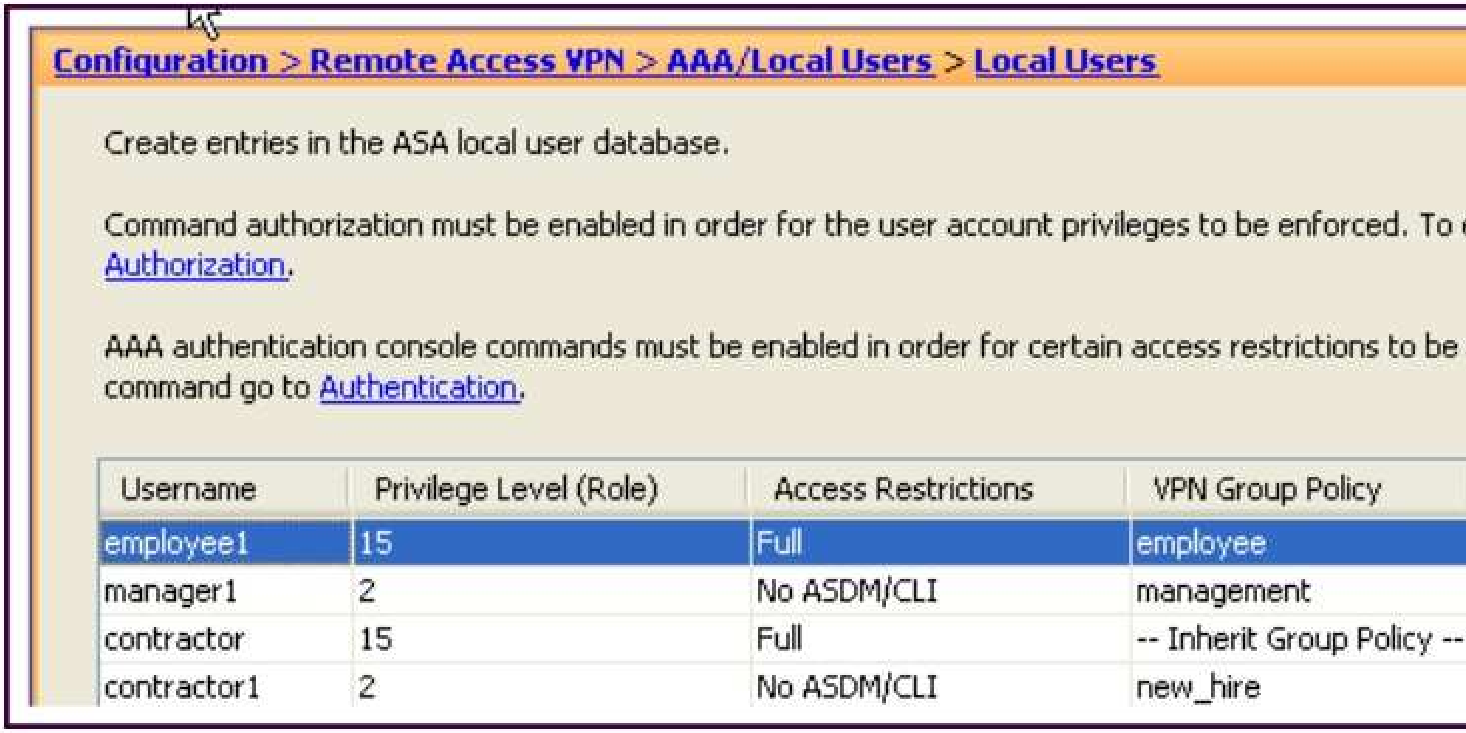
- Idle Timeout

- Max Time Exceeded

- Administrator Reset

QUESTION 14
The user "contractor" inherits which VPN group policy?

Exhibit:



Configuration > Remote Access VPN > AAA/Local Users > Local Users

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To
Authorization.

AAA authentication console commands must be enabled in order for certain access restrictions to be
command go to Authentication.

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy
employee1	15	Full	employee
manager1	2	No ASDM/CLI	management
contractor	15	Full	-- Inherit Group Policy --
contractor1	2	No ASDM/CLI	new_hire

A. employee
B. management
C. DefaultWEBVPNGroup
D. DfltGrpPolicy
E. new_hire

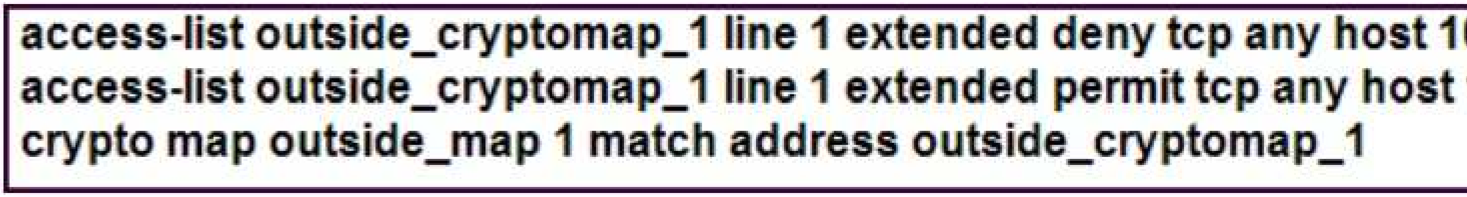
Correct Answer: D
Section: SSLVPN clientless
Explanation

Explanation/Reference:

QUESTION 15

In the CLI snippet that is shown, what is the function of the deny option in the access list?

Exhibit:



```
access-list outside_cryptomap_1 line 1 extended deny tcp any host 1
access-list outside_cryptomap_1 line 1 extended permit tcp any host
crypto map outside_map 1 match address outside_cryptomap_1
```

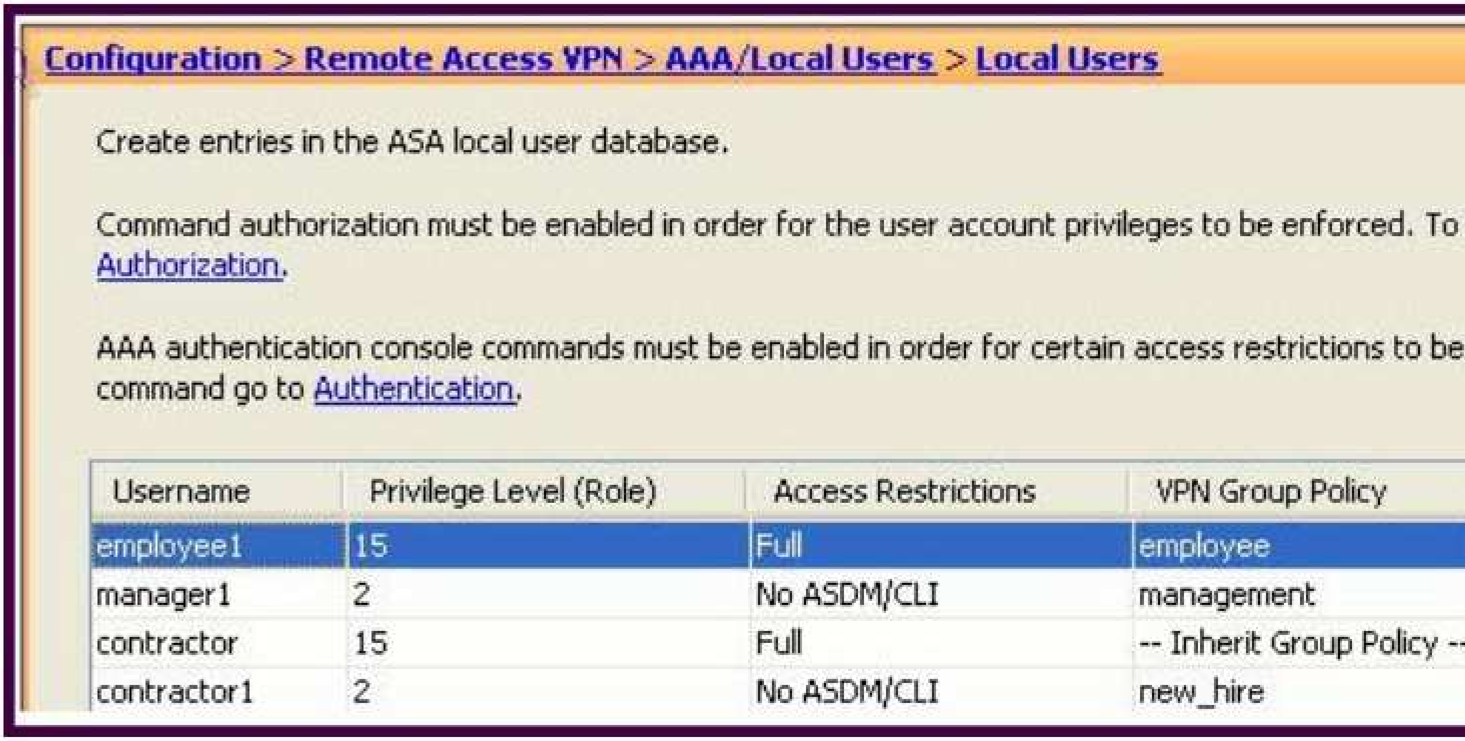
A. When set in conjunction with outbound connection-type bidirectional, its function is to prevent the specified traffic from being protected by the crypto map entry.
B. When set in conjunction with connection-type originate-only, its function is to instruct the Cisco ASA to deny specific inbound traffic if it is not encrypted.
C. When set in conjunction with outbound connection-type answer-only, its function is to instruct the Cisco ASA to deny specific outbound traffic if it is not encrypted.
D. When set in conjunction with connection-type originate-only, its function is to cause all IP traffic that matches the specified conditions to be protected by the crypto map.

Correct Answer: A
Section: IPsec
Explanation

Explanation/Reference:

QUESTION 16
When the user "contractor" Cisco AnyConnect tunnel is established, what type of Cisco ASA user restrictions are applied to the tunnel?

Exhibit:



Configuration > Remote Access VPN > AAA/Local Users > Local Users

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To Authorization.

AAA authentication console commands must be enabled in order for certain access restrictions to be command go to Authentication.

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy
employee1	15	Full	employee
manager1	2	No ASDM/CLI	management
contractor	15	Full	-- Inherit Group Policy --
contractor1	2	No ASDM/CLI	new_hire

A. full restrictions (no Cisco ASDM, no CLI, no console access)
B. full restrictions (no read, no write, no execute permissions)
C. full restrictions (CLI show commands and Cisco ASDM monitoring permissions only)
D. full access with no restrictions

Correct Answer: D
Section: SSLVPN clientless
Explanation

Explanation/Reference:

QUESTION 17
When initiating a new SSL or TLS session, the client receives the server SSL certificate and validates it. After validating the server certificate, what does the client use the certificate for?

A. The client and server use the server public key to encrypt the SSL session data.
B. The server creates a separate session key and sends it to the client. The client decrypts the session key by using the server public key.
C. The client and server switch to a DH key exchange to establish a session key.
D. The client generates a random session key, encrypts it with the server public key, and then sends it to the server.

Correct Answer: D
Section: Certifcates
Explanation

Explanation/Reference:

QUESTION 18
When attempting to tunnel FTP traffic through a stateful firewall that might be performing NAT or PAT, which type of VPN tunneling should you use to allow the VPN traffic through the stateful firewall?

A. clientless SSL VPN
B. IPsec over TCP
C. smart tunnel
D. SSL VPN plug-ins

Correct Answer: B
Section: IPsec
Explanation

Explanation/Reference:
IP Security (IPSec) over Transmission Control Protocol (TCP) enables a VPN Client to operate in an environment in which standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange (IKE, User Datagram Protocol (UDP) 500) cannot function, or can function only with modification to existing firewall rules. IPSec over TCP encapsulates both the IKE and IPSec protocols within a TCP packet, and it enables secure tunneling through both Network Address Translation (NAT) and Port Address Translation (PAT) devices and firewalls

QUESTION 19
What is a valid reason for configuring a list of backup servers on the Cisco AnyConnect VPN Client profile?

A. to access a backup authentication server
B. to access a backup DHCP server
C. to access a backup VPN server
D. to access a backup CA server

Correct Answer: C
Section: SSLVPN client
Explanation

Explanation/Reference:

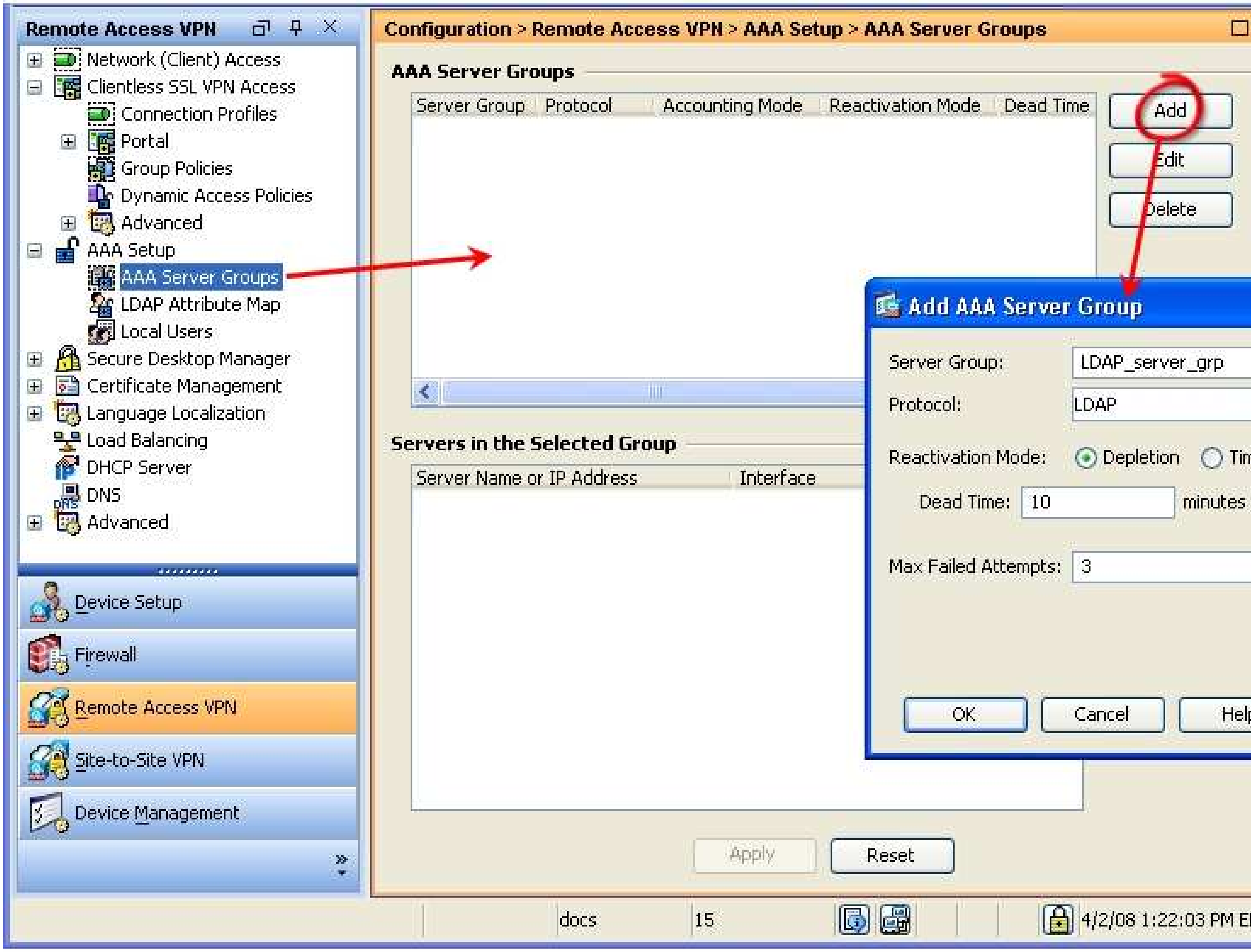
QUESTION 20
Which statement about CRL configuration is correct?

A. CRL checking is enabled by default.
B. The Cisco ASA relies on HTTPS access to procure the CRL list.
C. The Cisco ASA relies on LDAP access to procure the CRL list.
D. The Cisco Secure ACS can be configured as the CRL server.

Correct Answer: C
Section: Certifcates
Explanation

Explanation/Reference:
ASA SSLVPN deployment guide:

The security appliance supports various authentication methods: RSA one-time passwords, Radius, Kerberos, LDAP, NT Domain, TACACS, Local/Internal, digital certificates, and a combination of both authentication and certificates.



Configuration > Remote Access VPN > AAA Setup > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time

Servers in the Selected Group

Server Name or IP Address	Interface

Add AAA Server Group

Server Group: LDAP_server_grp

Protocol: LDAP

Reactivation Mode: ● Depletion ○ Tim

Dead Time: 10 minutes

Max Failed Attempts: 3

OK Cancel Help

QUESTION 21
When preconfiguring a Cisco AnyConnect profile for the user group, which file is output by the Cisco AnyConnect profile editor?

A. user.ini
B. user.html
C. user.pcf
D. user.xml

Correct Answer: D
Section: SSLVPN clientless
Explanation

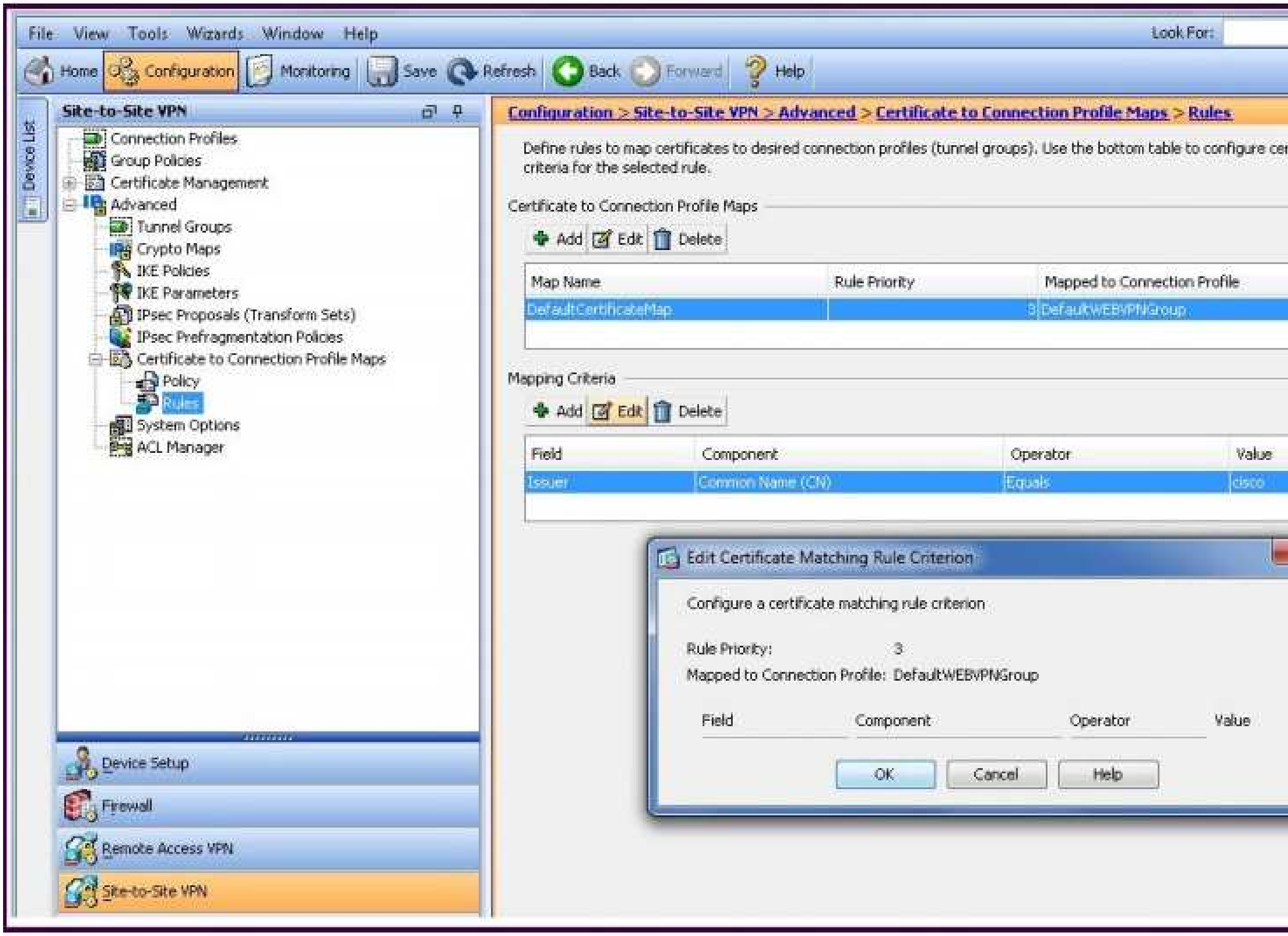
Explanation/Reference:
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/ac02asaconfig.html

QUESTION 22
In the Edit Certificate Matching Rule Criterion window, you want to change the Mapped to

Connection Profile. However, you cannot perform that action from this window.

Where should you navigate to and what should you do, in order to perform this change?

Exhibit:



Configuration > Site-to-Site VPN > Advanced > Certificate to Connection Profile Maps > Rules

Define rules to map certificates to desired connection profiles (tunnel groups). Use the bottom table to configure cer
criteria for the selected rule.

Certificate to Connection Profile Maps

Map Name	Rule Priority	Mapped to Connection Profile
DefaultCertificateMap	3	DefaultWEBVPNGroup

Mapping Criteria

Field	Component	Operator	Value
Issuer	Common Name (CN)	Equals	cisco

Edit Certificate Matching Rule Criterion

Configure a certificate matching rule criterion

Rule Priority: 3

Mapped to Connection Profile: DefaultWEBVPNGroup

Field Component Operator Value

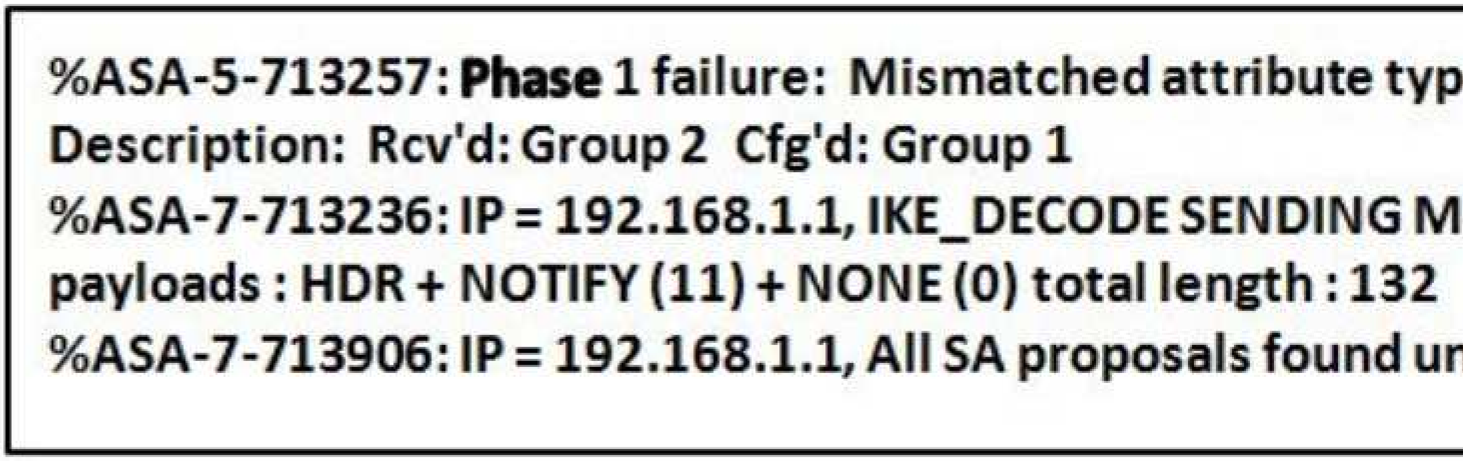
A. Edit the entry in the Certificate Management window.
B. Edit the entry in the Connection Profiles window.
C. Edit the entry in the Certificate to Connection Profile Maps window.
D. Edit the entry in IKE Policies window.
E. Delete this entry in the Mapping Criteria window, and add a new entry in the same location.

Correct Answer: C
Section: Certifcates
Explanation

Explanation/Reference:

QUESTION 23
What is the likely cause of the failure?

Exhibit:



```
%ASA-5-713257: Phase 1 failure:  Mismatched attribute typ
Description:  Rcv'd: Group 2  Cfg'd: Group 1
%ASA-7-713236: IP = 192.168.1.1, IKE_DECODE SENDING M
payloads : HDR + NOTIFY (11) + NONE (0) total length : 132
%ASA-7-713906: IP = 192.168.1.1, All SA proposals found ur
```

A. A msgid of 0 signifies a zero payload, indicating that the peer did not send any IKE proposals.
B. The remote peer did not respond to the 11 notifications that were sent by the originating IPsec endpoint.
C. There are mismatched IKE policies.
D. There are mismatched tunnel groups.

Correct Answer: C
Section: IPsec
Explanation

Explanation/Reference:
```
%ASA-5-713257: Phase var1 failure: Mismatched attribute types for
class var2: Rcv'd: var3 Cfg'd: var4
```

Explanation An adaptive security appliance has acted as the responder in a LAN-to-LAN connection. It indicates that the adaptive security appliance crypto configuration does not match the configuration of the initiator. The message specifies during which phase the mismatch occurred, and which attributes both the responder and the initiator had that were different.

•var1—The phase during which the mismatch occurred

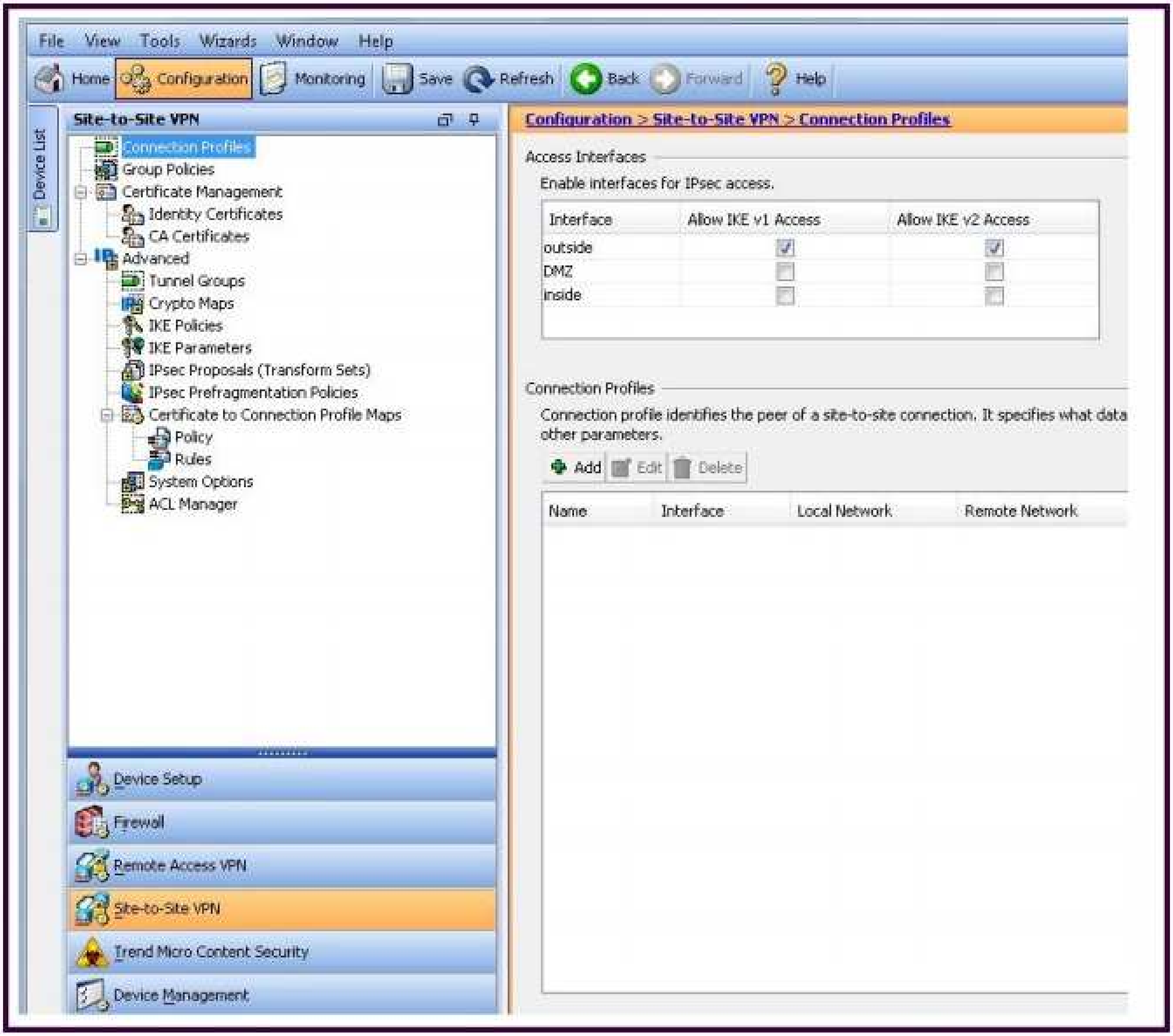
•var2—The class to which the attributes that do not match belong

•var3—The attribute received from the initiator

•var4—The attribute configured

QUESTION 24
You are the network security administrator. You have received calls from site-to-site IPsec VPN users saying that they cannot connect into the network. In troubleshooting this problem, you discover that some sites can connect, but other sites cannot. It is not always the same sites experiencing problems. You suspect that the permitted number of simultaneous logins has been reached and needs to be increased.
In which configuration window or tab should you accomplish this task?

Exhibit:



Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	☑	☑
DMZ	☐	☐
inside	☐	☐

Connection Profiles

Connection profile identifies the peer of a site-to-site connection. It specifies what data other parameters.

Name	Interface	Local Network	Remote Network

A. in the IKE Policies window
B. in the IKE Parameters window
C. in the System Options window
D. in the Device Management tab

Correct Answer: C
Section: IPsec
Explanation

Explanation/Reference:
ASDM User guide Page 35-81

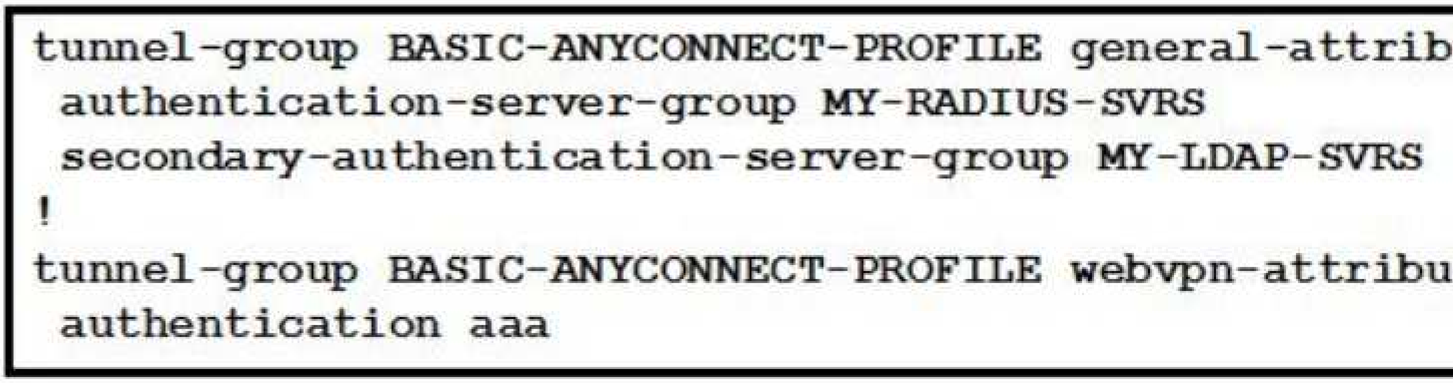
Limit the maximum number of active IPSec VPN sessions

—Enables or disables limiting the maximum number of active IPSec VPN sessions. The range depends on the hardware platform and the software license.
– Maximum Active IPSec VPN Sessions—Specifies the maximum number of active IPSec VPN sessions

allowed. This field is active only when you select the preceding check box to limit the maximum number of active IPSec VPN sessions.

QUESTION 25
Given the example that is shown, what can you determine?

Exhibit:



```
tunnel-group BASIC-ANYCONNECT-PROFILE general-attrib
 authentication-server-group MY-RADIUS-SVRS
 secondary-authentication-server-group MY-LDAP-SVRS
!
tunnel-group BASIC-ANYCONNECT-PROFILE webvpn-attribu
 authentication aaa
```

A. Users are required to perform RADIUS or LDAP authentication when connecting with the Cisco AnyConnect client.
B. Users are required to perform AAA authentication when connecting via WebVPN.
C. Users are required to perform double AAA authentication.
D. The user access identity is prefilled at login, requiring users to enter only their password.

Correct Answer: C
Section: SSLVPN clientless
Explanation

Explanation/Reference:

Exam B

QUESTION 1
When deploying clientless SSL VPNs, what should you do to support external unmanaged VPN clients?

A. Deploy a private PKI service.
B. Issue self-signed identity certificates for the external clients that you wish to provide with access to your enterprise.
C. Configure policies specifically for the clients that have a group userID and password.
D. Implement a global PKI service.

Correct Answer: D
Section: Certifcates
Explanation

Explanation/Reference:

QUESTION 2
Which option limits a clientless SSL VPN user to specific resources upon successful login?

A. modify the Cisco ASA Modular Policy Framework access control
B. user-defined bookmarks
C. RADIUS authorization
D. disable portal features

Correct Answer: B
Section: SSLVPN clientless
Explanation

Explanation/Reference:
Effective with Cisco IOS Release 12.4(15)T, users can bookmark URLs while connected through an SSL VPN tunnel. Users can access the bookmarked URLs by clicking the URLs.
User-level bookmarking is turned by default. There is no way to turn it off. To set the storage location, administrators can use the **user-profile location** command. If the **user-profile location** command is not configured, the location flash:/webvpn/{context name}/ is used.

QUESTION 3
You have just configured new clientless SSL VPN access parameters. However, when users connect, they are not getting the expected access that was configured. What is one possible reason this is occurring?

A. The correct Tunnel Group Lock is not properly set.
B. The corresponding Cisco ASA interface is not enabled for SSL VPN access.
C. The Connection Alias is not enabled.
D. Portal features are disabled.

Correct Answer: A
Section: SSLVPN clientless
Explanation

Explanation/Reference:

QUESTION 4

When a VPN client that is using redundant peering and has obtained an IP address from the primary VPN gateway loses connection to that gateway, how is traffic rerouted?

A. The secondary VPN gateway automatically routes the traffic back to the client using the same IP address.
B. Redundant Internet routing protocols reroute the traffic to and from the client and the gateway.
C. Traffic flow stops, and the client must reestablish connection. Once connection is established, the same IP address is issued to the client and similarly routed.
D. The secondary VPN gateway issues the client a new IP address and routes traffic accordingly.

Correct Answer: D
Section: SSLVPN client
Explanation

Explanation/Reference:

QUESTION 5
Which statement is true regarding Cisco ASA stateful failover?

A. It is recommended to share the failover link with the inside interface for security purposes.
B. The failover link is encrypted by default to protect eavesdropping.
C. VPN users must reauthenticate, even though the connection remains established.
D. Clientless features, such as smart tunnels and plug-ins, are not supported.

Correct Answer: D
Section: IPsec
Explanation

Explanation/Reference:

QUESTION 6
Which statement is true about configuring the Cisco ASA for Active/Standby failover?

A. All versions of Cisco ASA software need to have the same licensing on both devices.
B. Both devices perform load sharing until a failure occurs.
C. All VPN-related configurations and files are automatically replicated.
D. VPN images, profiles, and plug-ins must be manually provisioned to both devices.

Correct Answer: D
Section: IPsec
Explanation

Explanation/Reference:
CCNP Security VPN 642-648 Official Cert Guide Page 242

QUESTION 7
When configuring the Cisco ASA for VPN clustering, which IP address or addresses does the end-user device connect to?

A. It connects to individual device addresses of the cluster as provided in the connection profile.
B. It connects to the virtual address.
C. The virtual cluster manager sends the IP address of the least loaded device. The client then connects directly to that device.

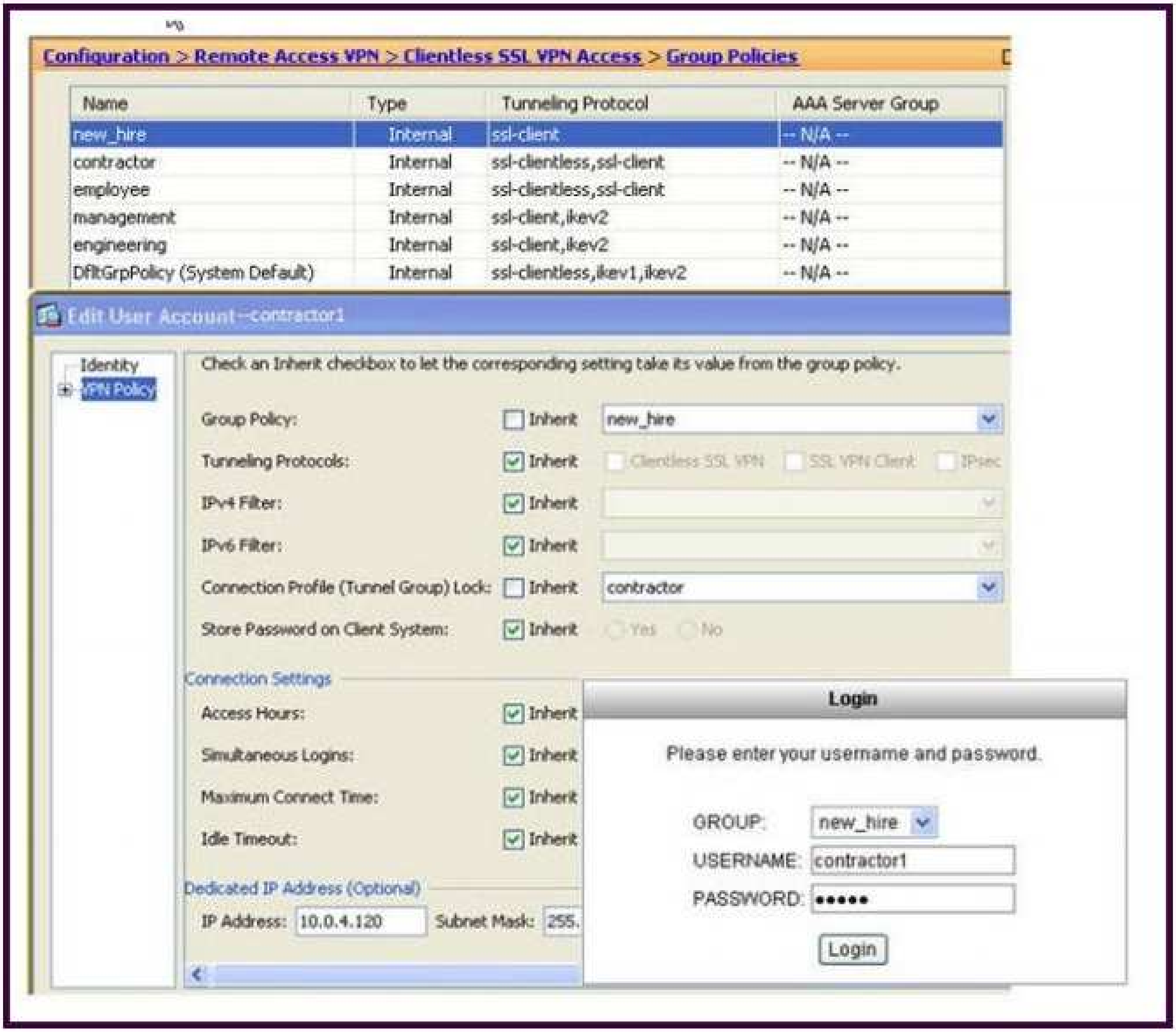
D. The connection IP address is dependent upon whether the initiator is using SSL or IPsec.

Correct Answer: B
Section: IPsec
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00805fda25.shtml

QUESTION 8
When an SSL VPN user, contractor1, enters https://192.168.4.2 (the outside address of the Cisco ASA appliance) into the browser, an SSL VPN Login screen appears.
In addition to the information that is contained in the Cisco ASDM configuration screens, what can an administrator determine about the state of the connection after the user clicks the Login button?

Exhibit:



Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies

Name	Type	Tunneling Protocol	AAA Server Group
new_hire	Internal	ssl-client	-- N/A --
contractor	Internal	ssl-clientless,ssl-client	-- N/A --
employee	Internal	ssl-clientless,ssl-client	-- N/A --
management	Internal	ssl-client,ikev2	-- N/A --
engineering	Internal	ssl-client,ikev2	-- N/A --
DfltGrpPolicy (System Default)	Internal	ssl-clientless,ikev1,ikev2	-- N/A --

Edit User Account--contractor1

Identity
VPN Policy

Check an Inherit checkbox to let the corresponding setting take its value from the group policy.

Group Policy: ☐ Inherit new_hire
Tunneling Protocols: ☑ Inherit ☐ Clientless SSL VPN ☐ SSL VPN Client ☐ IPsec
IPv4 Filter: ☑ Inherit
IPv6 Filter: ☑ Inherit
Connection Profile (Tunnel Group) Lock: ☐ Inherit contractor
Store Password on Client System: ☑ Inherit ○ Yes ○ No

Connection Settings
Access Hours: ☑ Inherit
Simultaneous Logins: ☑ Inherit
Maximum Connect Time: ☑ Inherit
Idle Timeout: ☑ Inherit

Dedicated IP Address (Optional)
IP Address: 10.0.4.120 Subnet Mask: 255.

Login

Please enter your username and password.

GROUP: new_hire
USERNAME: contractor1
PASSWORD: •••••

A. The user login will succeed, and an IP address of 10.0.4.120 will be assigned.
B. The user will be presented with a clientless VPN portal page.

C. The user login will succeed, but the user will be connected to the "contractor" tunnel group.

D. The login will fail.

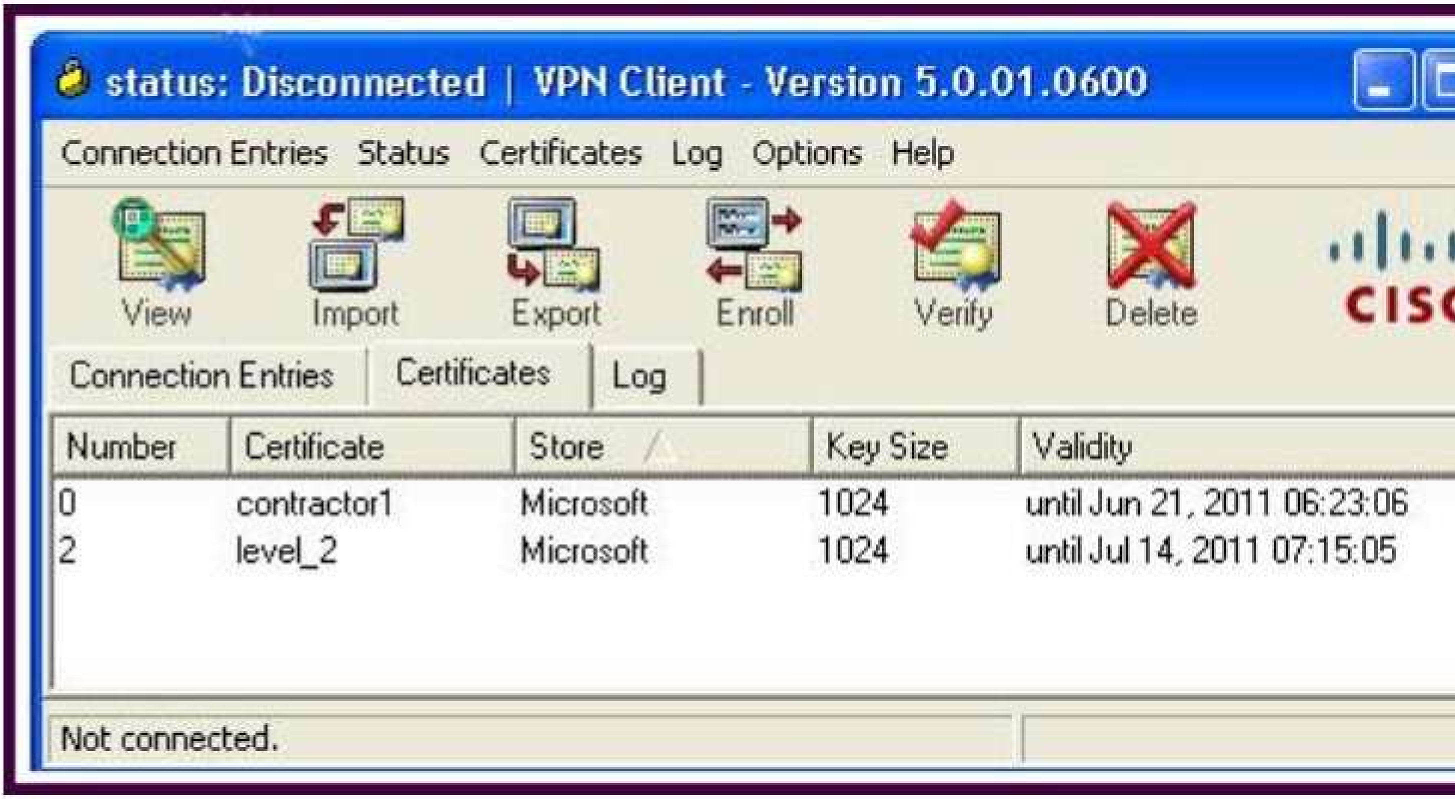
Correct Answer: D
Section: SSLVPN clientless
Explanation

Explanation/Reference:

QUESTION 9

As the administrator of a Cisco ASA security appliance for remote-access IPsec VPNs, you are assisting a user who has a digital certificate that is configured for the Cisco VPN Client.
Based on the exhibit, what do you do to find the MD5 thumbprint of the "level_2" certificate?

Exhibit:



Number	Certificate	Store	Key Size	Validity
0	contractor1	Microsoft	1024	until Jun 21, 2011 06:23:06
2	level_2	Microsoft	1024	until Jul 14, 2011 07:15:05

Not connected.

A. Choose the certificate, then click Status > Certificates from the menu bar.

B. Choose the certificate, then click the View button.

C. Choose the certificate, then click Options > Properties from the menu bar.

D. Choose the certificate, then click the Verify button.

Correct Answer: B
Section: Certifcates
Explanation

Explanation/Reference:

QUESTION 10

A Unified Communications Certificate is used on the Cisco ASA appliance to support which option?

A. certificate + double AAA authentication
B. certificate + AAA authentication
C. certificate maps
D. Cisco ASA VPN clustering load balancing

Correct Answer: D
Section: IPsec
Explanation

Explanation/Reference:

Server Certificate Types

Cisco uses these self-signed (own) certificate types in Cisco Unified Communications Manager servers:
HTTPS certificate (tomcat_cert)—This self-signed root certificate is generated during the Cisco Unified Communications Manager installation for the HTTPS server.
Cisco Unified Communications Manager node certificate—This self-signed root certificate automatically installs when you install Cisco Unified Communications Manager 5.1 for the Cisco Unified Communications Manager server. Cisco Unified Communications Manager certificates provide server identification, which includes the Cisco Unified Communications Manager server name and the Global Unique Identifier (GUID).
CAPF certificate—The system copies this root certificate to all servers in the cluster after you complete the Cisco CTL client configuration.
IPsec certificate (ipsec_cert)—This self-signed root certificate is generated during Cisco Unified Communications Manager installation for IPsec connections with MGCP and H.323 gateways.
SRST-enabled gateway certificate—When you configure a secure SRST reference in Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager retrieves the SRST-enabled gateway certificate from the gateway and stores it in the Cisco Unified Communications Manager database. After you reset the devices, the certificate is added to the phone configuration file. Because the certificate is stored in the database, this certificate is not integrated into the certificate management tool.

https://supportforums.cisco.com/docs/DOC-5964

For more information on VPN Load Balancing/Clustering High Availability services of the ASA appliances please consult the configuraiton guide at http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/vpnsysop.html#wp1048834. Please check cisco.com for new versions of the document.
For more information on configuring Certificates on the the ASA appliances please consult the configuraiton guide at
http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/cert_cfg.html .Please check cisco.com for new versions of the document.

QUESTION 11
In clientless SSL VPN, administrators can control user access to the internal network or resources of a company. What is this control based on?

A. interface ACLs
B. WebType ACLs
C. per-user or per-group ACLs
D. MPF-configured service policies

Correct Answer: B
Section: SSLVPN clientless
Explanation

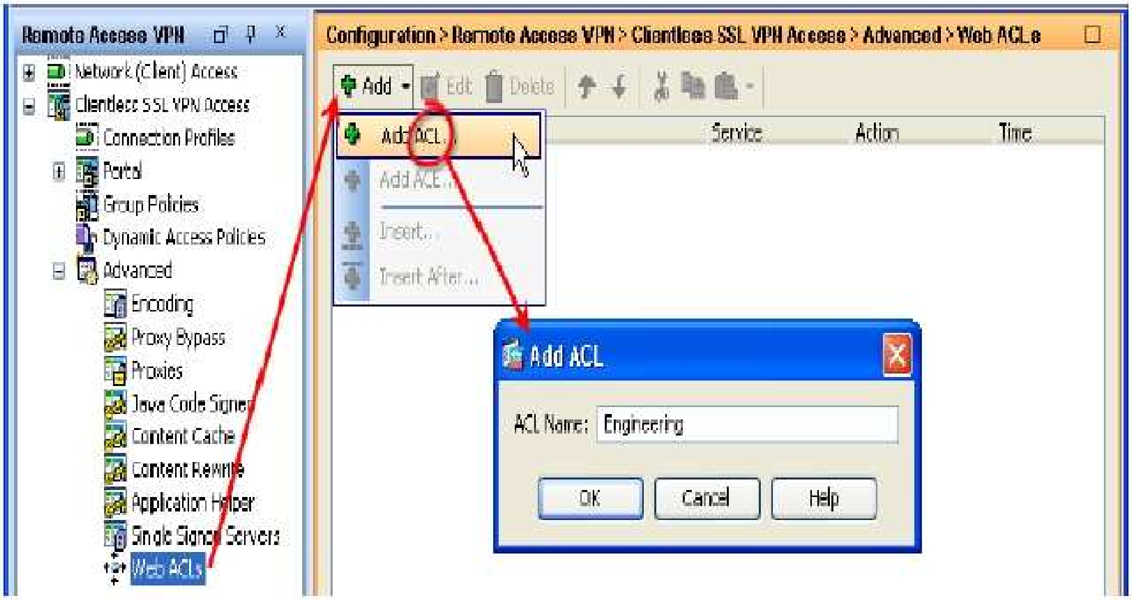
Explanation/Reference:

Creating WebType ACLs

Web Access control lists (ACLs) filter internet traffic for clientless users. The ACLs table displays the filters configured on the security appliance and the access control entries (ACEs) for each ACL. Each ACL permits or denies access to specific networks, subnets, hosts, and web servers; the ACE specifies one rule for the ACL. To create an ACL, follow these steps:

Step 1 Navigate to Clientless SSL VPN Access > Advanced > Web ACLs.

Step 2 Click **Add** and enter *Engineering* as the ACL name.

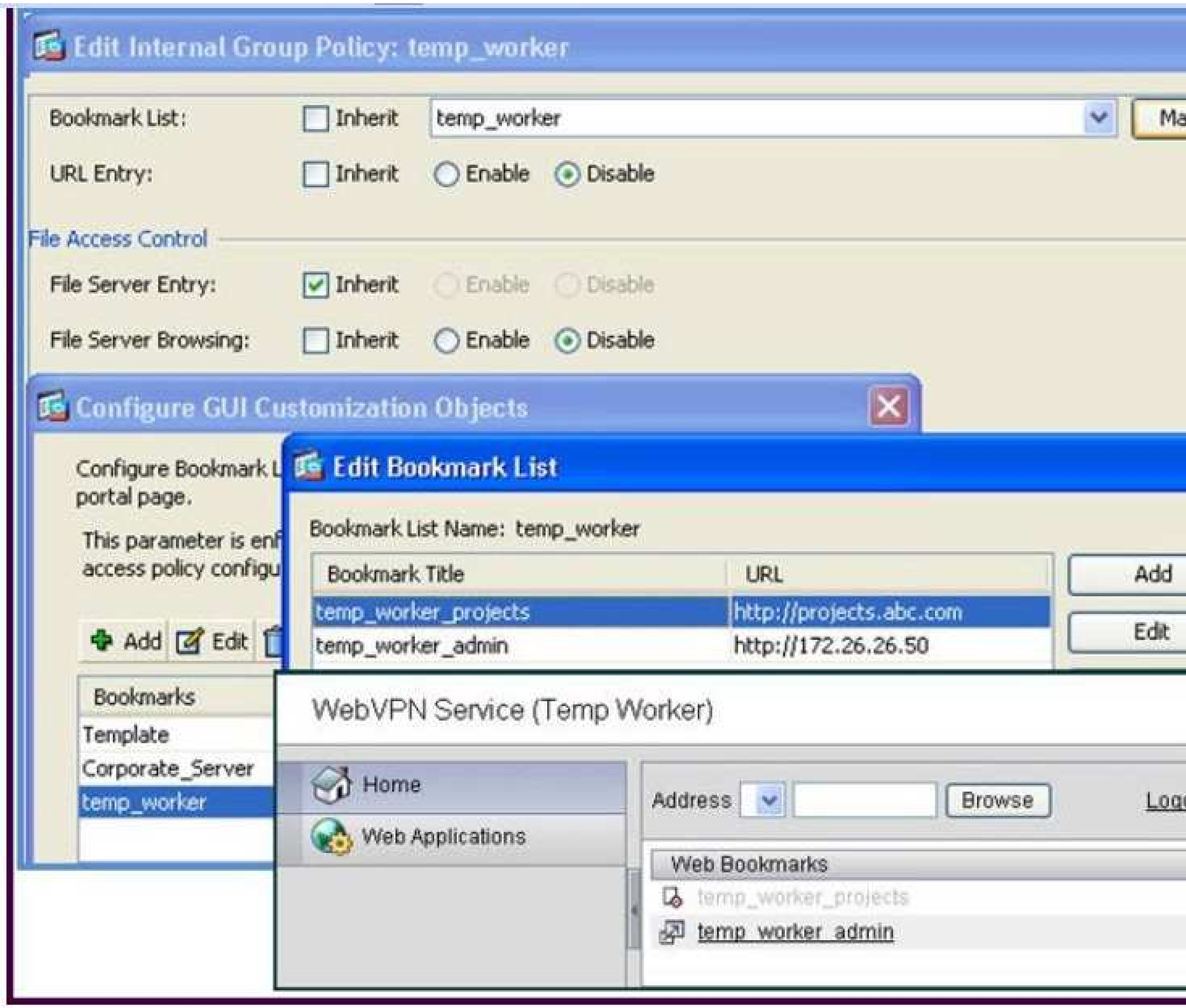


ACL Name: Engineering

Step 3 Click **Add** and select **Add ACE** .

QUESTION 12
A new network engineer configured the ABC adaptive security appliance with two bookmarks for a new temporary worker. The temporary worker can connect to the administrator server via the temp_worker_admin bookmark but cannot connect to the project server via the temp_worker_projects bookmark (which is grayed out). It was determined that the URL and IP addressing information in the GUI screens is correct.
What is wrong with the configuration?

Exhibit:



Edit Internal Group Policy: temp_worker

Bookmark List: □ Inherit temp_worker

URL Entry: □ Inherit ○ Enable ● Disable

File Access Control

File Server Entry: ☑ Inherit ○ Enable ○ Disable

File Server Browsing: □ Inherit ○ Enable ● Disable

Configure GUI Customization Objects

Configure Bookmark L portal page.

This parameter is enf access policy configu

Bookmarks
Template
Corporate_Server
temp_worker

Edit Bookmark List

Bookmark List Name: temp_worker

Bookmark Title	URL
temp_worker_projects	http://projects.abc.com
temp_worker_admin	http://172.26.26.50

WebVPN Service (Temp Worker)

Web Bookmarks

temp_worker_projects

temp_worker_admin

A. URL Entry should be enabled.

B. The File Server Entry Inherit parameter should be overwritten and set for enabled.

C. The DNS server information is incorrect.

D. File Server Browsing should be enabled.

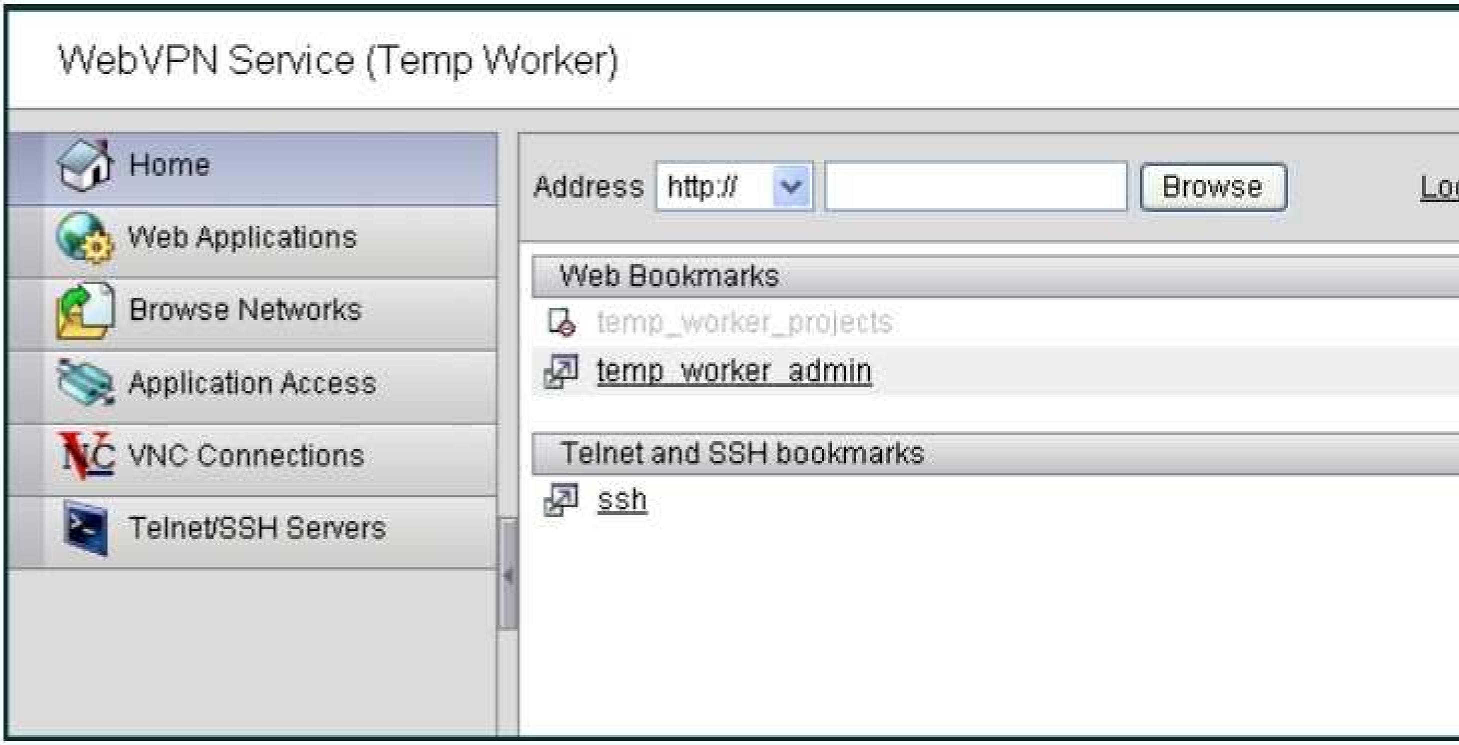
Correct Answer: C
Section: SSLVPN clientless
Explanation

Explanation/Reference:

QUESTION 13
Today was the first day on a new project for an offsite temporary worker at the XYZ Corporation. The worker was told to launch the SSL VPN session and then use the smart tunnel application to

start a remote desktop application on the project server, projects_server.xyz.com. The worker looked at the portal screen that was provided, but she did not know how to access the smart tunnel application.
As the help desk person, what should you instruct the temporary worker to do?

Exhibit:



A. Click the Web Applications button.
B. Click the Applications Access button.
C. Click the Browse Networks button.
D. On the Home page, click the Address drop-down menu, choose RDP://, and fill in the destination host name, which is projects_server.abc.com.

Correct Answer: B
Section: SSLVPN client
Explanation

Explanation/Reference:

QUESTION 14
After adding a remote-access IPsec tunnel via the VPN wizard, an administrator needs to tune the IKE policy parameters. Where is the correct place to tune IKE policy parameters?

A. Cisco IPsec VPN SW Client > Client Profile
B. IPsec User Profile
C. Group Policy
D. IKE Policy
E. Crypto Map

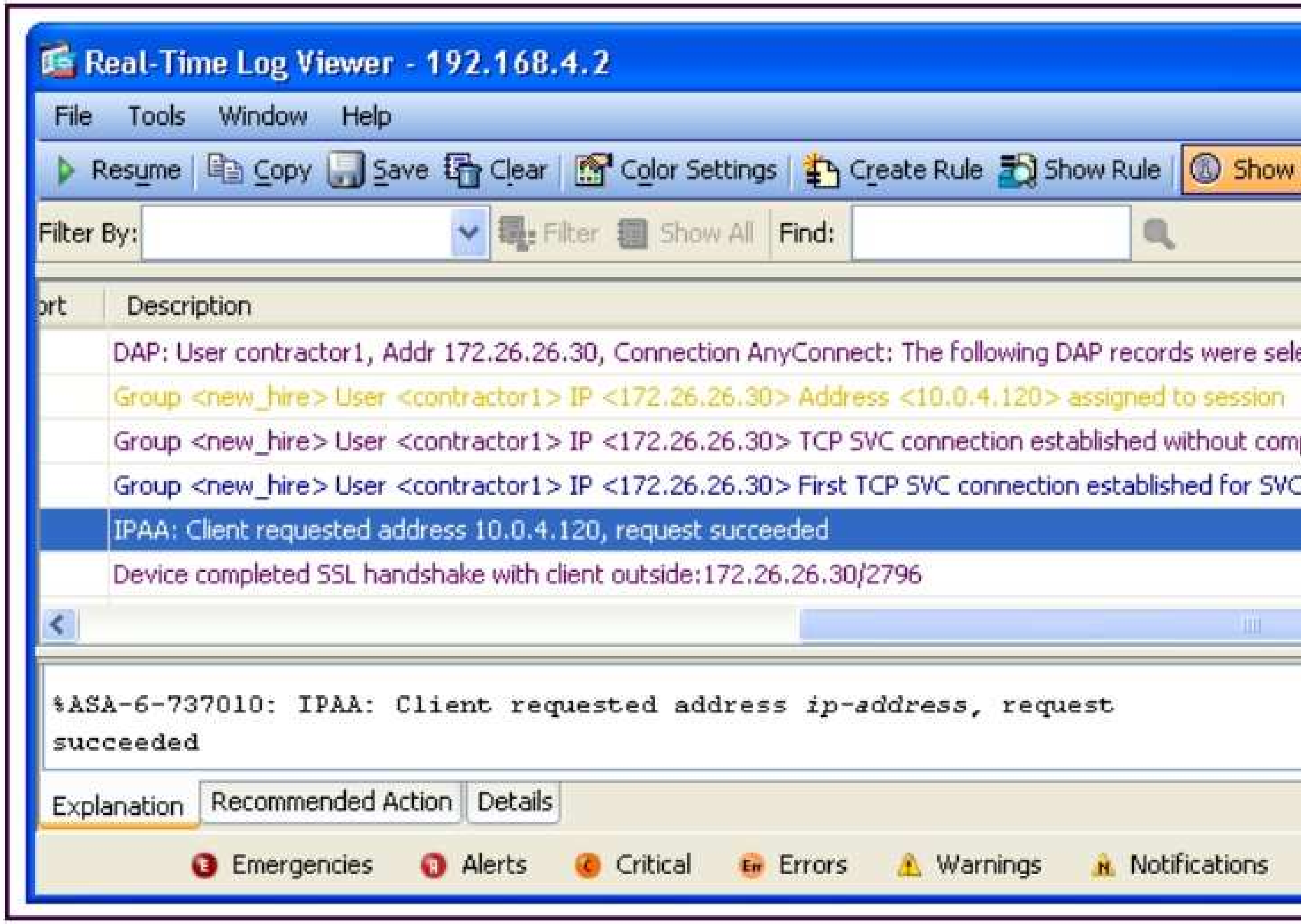
Correct Answer: D

Section: IPsec
Explanation

Explanation/Reference:

QUESTION 15
After being with the company for more than six months, Sue is no longer considered a new hire employee. In converting her from a new hire to a full-time employee, her SSL VPN address will change from the "Client requested address 10.0.4.120" to a random address from the employee address pool.
To "disable" the 10.0.4.120 IP address, the network administrator should navigate to which Cisco ASDM pane?

Exhibit:



```
DAP: User contractor1, Addr 172.26.26.30, Connection AnyConnect: The following DAP records were sele
Group <new_hire> User <contractor1> IP <172.26.26.30> Address <10.0.4.120> assigned to session
Group <new_hire> User <contractor1> IP <172.26.26.30> TCP SVC connection established without com
Group <new_hire> User <contractor1> IP <172.26.26.30> First TCP SVC connection established for SVC
IPAA: Client requested address 10.0.4.120, request succeeded
Device completed SSL handshake with client outside:172.26.26.30/2796
```

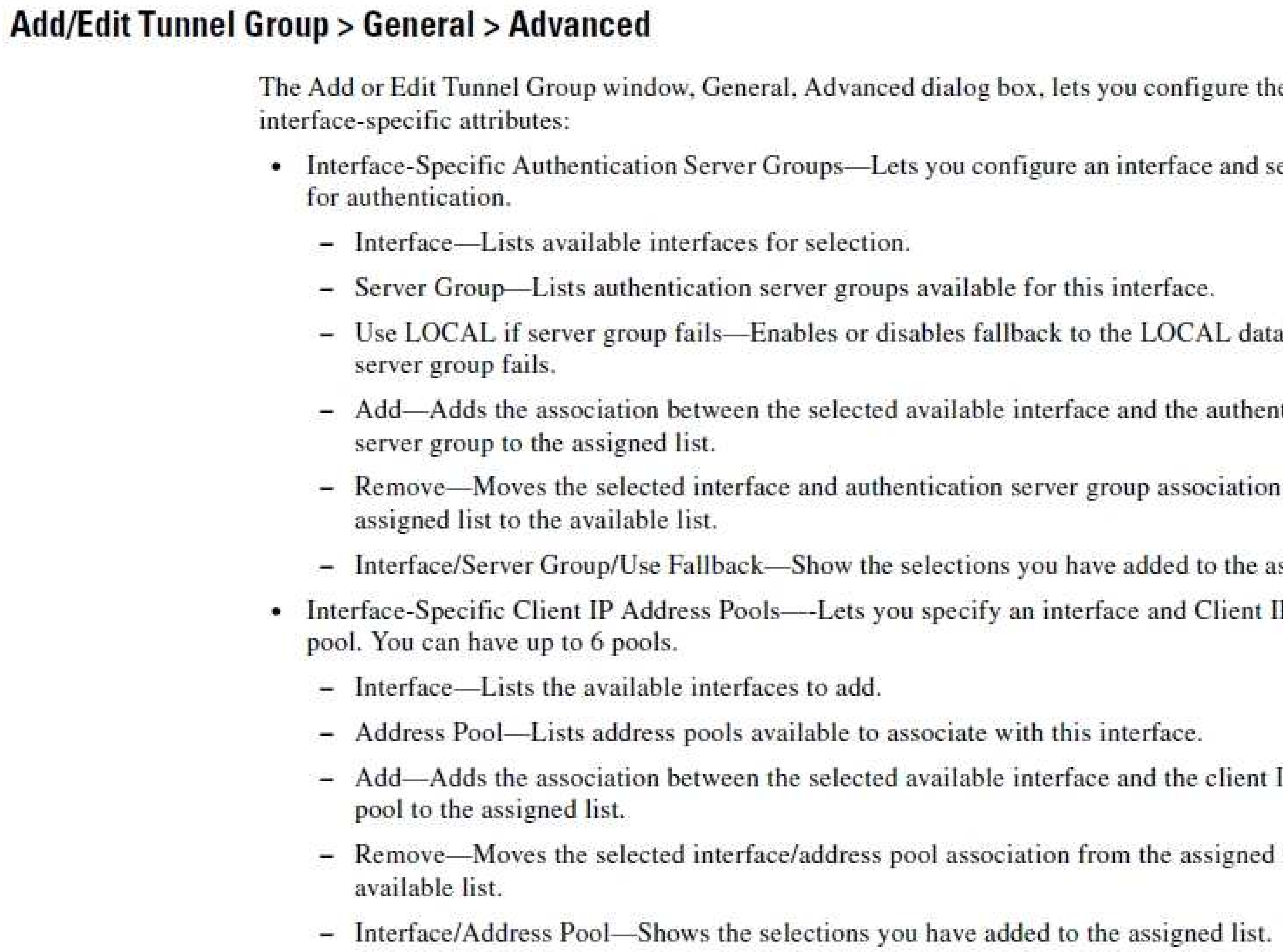
```
%ASA-6-737010: IPAA: Client requested address ip-address, request
succeeded
```

A. Connection Profile
B. Group Policies
C. Local Users
D. Address Pools

Correct Answer: C
Section: SSLVPN client

Explanation

Explanation/Reference:
Users are assigned IP addresses based on the adress pool asscoiated with their group. Change group of Sue to use empoyee address pool



Add/Edit Tunnel Group > General > Advanced

The Add or Edit Tunnel Group window, General, Advanced dialog box, lets you configure the interface-specific attributes:

- Interface-Specific Authentication Server Groups—Lets you configure an interface and se for authentication.
  - Interface—Lists available interfaces for selection.
  - Server Group—Lists authentication server groups available for this interface.
  - Use LOCAL if server group fails—Enables or disables fallback to the LOCAL data server group fails.
  - Add—Adds the association between the selected available interface and the authent server group to the assigned list.
  - Remove—Moves the selected interface and authentication server group association assigned list to the available list.
  - Interface/Server Group/Use Fallback—Show the selections you have added to the as
- Interface-Specific Client IP Address Pools—-Lets you specify an interface and Client I pool. You can have up to 6 pools.
  - Interface—Lists the available interfaces to add.
  - Address Pool—Lists address pools available to associate with this interface.
  - Add—Adds the association between the selected available interface and the client I pool to the assigned list.
  - Remove—Moves the selected interface/address pool association from the assigned available list.
  - Interface/Address Pool—Shows the selections you have added to the assigned list.

QUESTION 16
While configuring a new clientless SSL VPN group in Cisco ASDM, the administrator chooses to accept a number of the default parameter values. The administrator decides to view the actual value for the parameter, rather than just checking the inherit box.
Under which default group can the administrator verify the default value for the group parameter?

A. DefaultRAGroup
B. DefaultWEBVPNGroup
C. DfltGrpPolicy
D. DefaultSVCGroup

Correct Answer: C
Section: SSLVPN clientless
Explanation

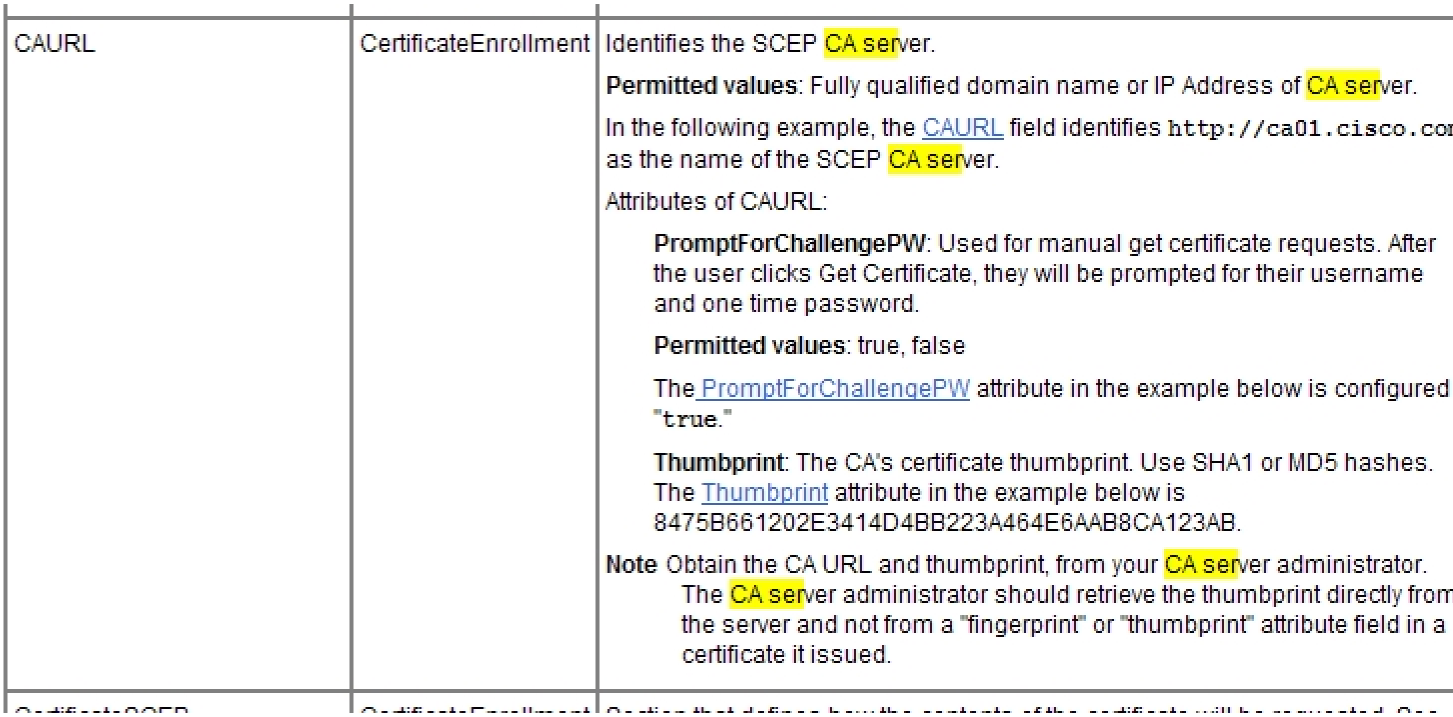
Explanation/Reference:

QUESTION 17
With SCEP enabled in a Cisco AnyConnect Connection Profile, what additional configuration step must you do when using Cisco ASA 8.4 software?

A. Configure local authentication prior to the enrollment process.
B. Configure the client to poll the CA for a response to the certificate request.
C. Configure the location of the CA server.
D. Configure the profile to inherit the SCEP forwarding URL.

Correct Answer: C
Section: Certifcates
Explanation

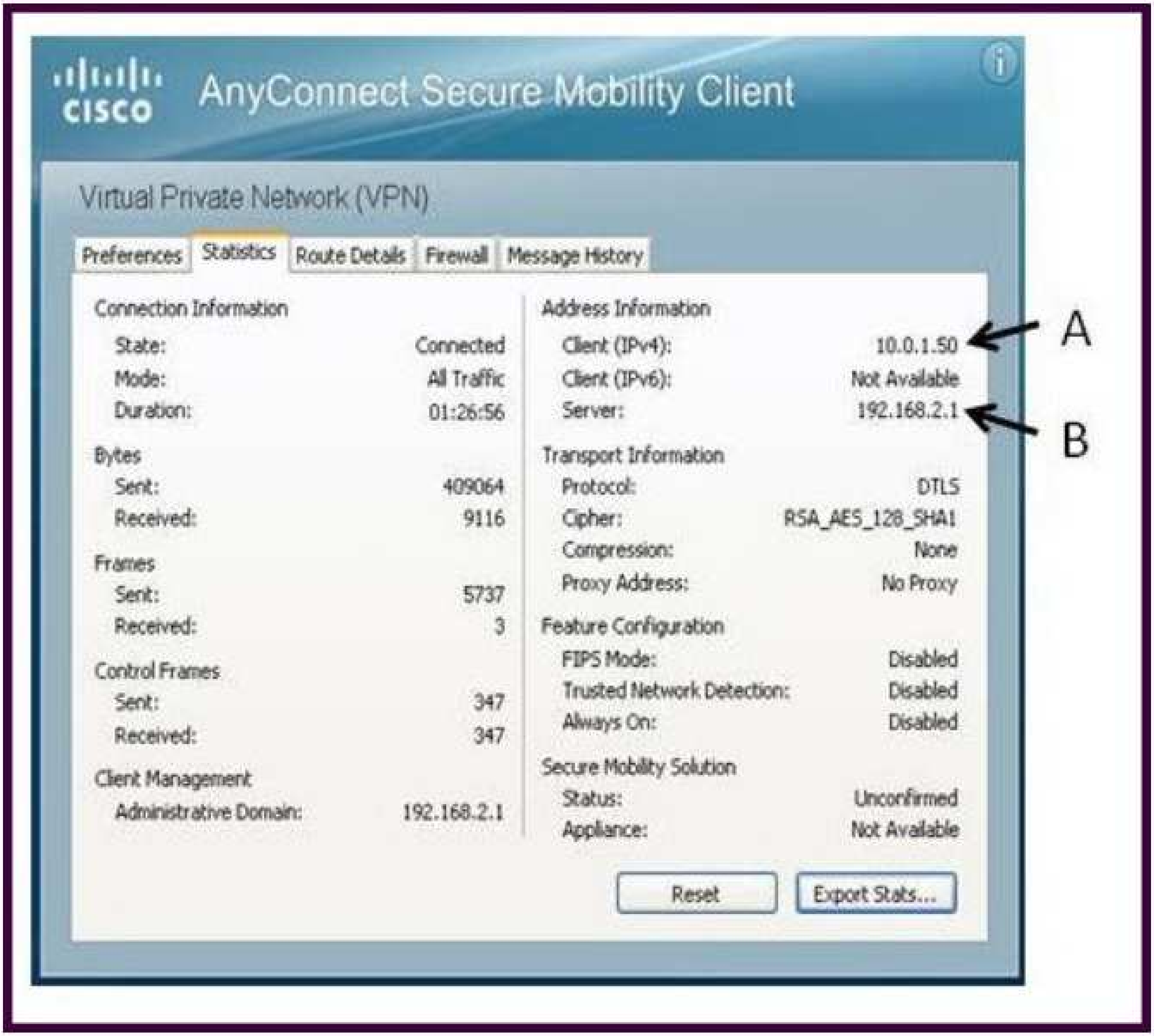
Explanation/Reference:
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect24/administration/guide/ac03features.html#wp1072891



CAURL	CertificateEnrollment	Identifies the SCEP CA server. **Permitted values**: Fully qualified domain name or IP Address of CA server. In the following example, the CAURL field identifies `http://ca01.cisco.co` as the name of the SCEP CA server. Attributes of CAURL: **PromptForChallengePW**: Used for manual get certificate requests. After the user clicks Get Certificate, they will be prompted for their username and one time password. **Permitted values**: true, false The PromptForChallengePW attribute in the example below is configured "`true`." **Thumbprint**: The CA's certificate thumbprint. Use SHA1 or MD5 hashes. The Thumbprint attribute in the example below is 8475B661202E3414D4BB223A464E6AAB8CA123AB. **Note** Obtain the CA URL and thumbprint, from your CA server administrator. The CA server administrator should retrieve the thumbprint directly fro the server and not from a "fingerprint" or "thumbprint" attribute field in a certificate it issued.
CertificateSCEP	CertificateEnrollment	Section that defines how the contents of the certificate will be requested. See

QUESTION 18
After a remote user established a Cisco AnyConnect session from a wireless card through the Cisco ASA appliance of a partner to a remote server, the user opened the Cisco AnyConnect VPN Client Statistics Details screen.
What are the two sources of the IP addresses that are marked A and B? (Choose two.)

Exhibit:



AnyConnect Secure Mobility Client

Virtual Private Network (VPN)

Connection Information
State: Connected
Mode: All Traffic
Duration: 01:26:56

Bytes
Sent: 409064
Received: 9116

Frames
Sent: 5737
Received: 3

Control Frames
Sent: 347
Received: 347

Client Management
Administrative Domain: 192.168.2.1

Address Information
Client (IPv4): 10.0.1.50
Client (IPv6): Not Available
Server: 192.168.2.1

Transport Information
Protocol: DTLS
Cipher: RSA_AES_128_SHA1
Compression: None
Proxy Address: No Proxy

Feature Configuration
FIPS Mode: Disabled
Trusted Network Detection: Disabled
Always On: Disabled

Secure Mobility Solution
Status: Unconfirmed
Appliance: Not Available

A. IP address that is assigned to the wireless Ethernet adapter of the remote user
B. IP address that is assigned to the remote user from the Cisco ASA address pool
C. IP address of the Cisco ASA physical interface of the partner
D. IP address of the Cisco ASA virtual HTTP server of the partner
E. IP address of the default gateway router of the remote user
F. IP address of the default gateway router of the partner

Correct Answer: BC
Section: SSLVPN client
Explanation

Explanation/Reference:

QUESTION 19

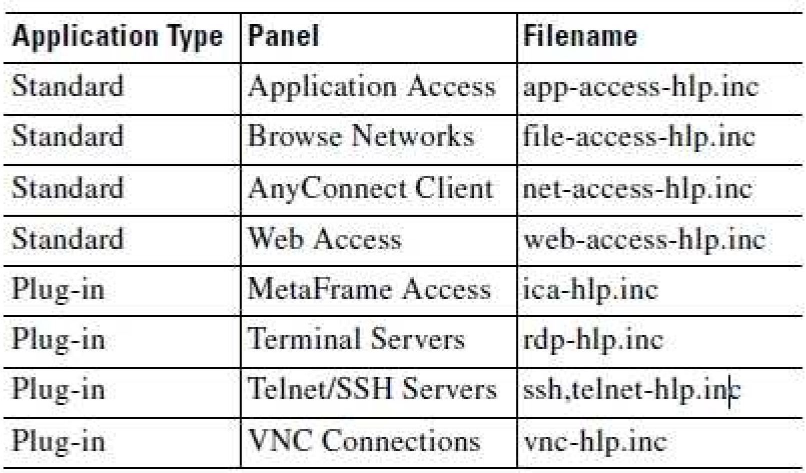
In Cisco ASA Software Release 8.4.1, which three plug-ins are Cisco ASA-supported plug-ins? (Choose three.)

A. SSH
B. TN3270
C. SCP
D. RDP
E. ICA
F. ARAP

Correct Answer: ADE
Section: SSLVPN client
Explanation

Explanation/Reference:

Clientless Applications



Application Type	Panel	Filename
Standard	Application Access	app-access-hlp.inc
Standard	Browse Networks	file-access-hlp.inc
Standard	AnyConnect Client	net-access-hlp.inc
Standard	Web Access	web-access-hlp.inc
Plug-in	MetaFrame Access	ica-hlp.inc
Plug-in	Terminal Servers	rdp-hlp.inc
Plug-in	Telnet/SSH Servers	ssh,telnet-hlp.inc
Plug-in	VNC Connections	vnc-hlp.inc

QUESTION 20
ABC Corporation has hired a temporary worker to help out with a new project. The network administrator gives you the task of restricting the internal clientless SSL VPN network access of the temporary worker to one server with the IP address of 172.26.26.50 via HTTP.
Which two actions should you take to complete the assignment? (Choose two.)

A. Configure access-list temp_acl webtype permit url http://172.26.26.50.
B. Configure access-list temp_acl_stand_ACL standard permit host 172.26.26.50.
C. Configure access-list temp_acl_extended extended permit http any host 172.26.26.50.
D. Apply the access list to the temporary worker Group Policy.
E. Apply the access list to the temporary worker Connection Profile.
F. Apply the access list to the outside interface in the inbound direction.

Correct Answer: AD
Section: SSLVPN clientless
Explanation

Explanation/Reference:

Web ACLs

The Web ACLs table displays the filters configured on the security appliance applicable to Clientless SSL VPN traffic. The table shows the name of each access control list (ACL), and below and indented to the right of the

ACL name, the access control entries (ACEs) assigned to the ACL. Each ACL permits or denies access permits or denies access to specific networks, subnets, hosts, and web servers. Each ACE specifies one rule that serves the function of the ACL. You can configure ACLs to apply to Clientless SSL VPN traffic. The following rules apply: • If you do not configure any filters, all connections are permitted. • The security appliance supports only an inbound ACL on an interface. • At the end of each ACL, an implicit, unwritten rule denies all traffic that is not explicitly permitted. You can use the following wildcard characters to define more than one wildcard in the Webtype access list entry: • Enter an asterisk "*" to match no characters or any number of characters. • Enter a question mark "?" to match any one character exactly. • Enter square brackets "[]" to create a range operator that matches any one character in a range. The following examples show how to use wildcards in Webtype access lists. • The following example matches URLs such as http://www.cisco.com/ and http://wwz.caco.com/: access-list test webtype permit url http://ww?.c*co*/

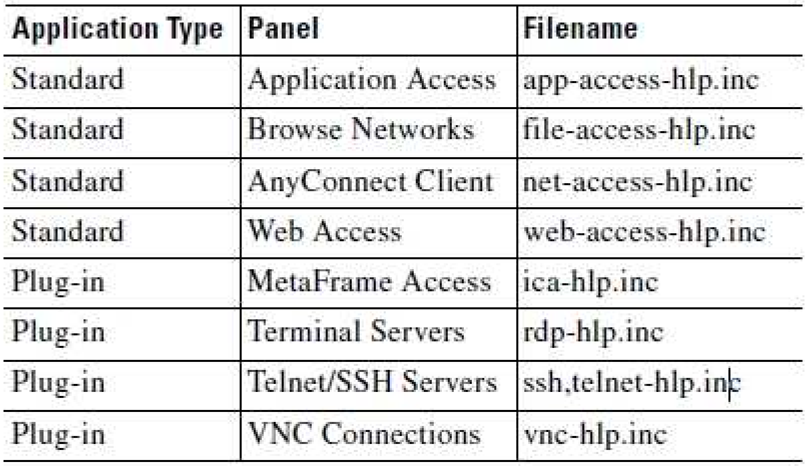
QUESTION 21
Your corporation has contractors that need remote access to server desktops, in order to diagnose issues and load software during nonbusiness hours. Which three clientless SSL VPN configurations allow these contractors to access the desktops of remote servers? (Choose three.)

A. XWindows bookmark by using the XWindows plug-in
B. RDP bookmark by using the RDP plug-in
C. SCP bookmark by using SCP plug-in
D. VNC bookmark by using the VNC plug-in
E. SSH bookmark by using the SSH plug-in
F. Citrix plug-in by using the Citrix plug-in

Correct Answer: BDF
Section: SSLVPN clientless
Explanation

Explanation/Reference:

Clientless Applications



Application Type	Panel	Filename
Standard	Application Access	app-access-hlp.inc
Standard	Browse Networks	file-access-hlp.inc
Standard	AnyConnect Client	net-access-hlp.inc
Standard	Web Access	web-access-hlp.inc
Plug-in	MetaFrame Access	ica-hlp.inc
Plug-in	Terminal Servers	rdp-hlp.inc
Plug-in	Telnet/SSH Servers	ssh,telnet-hlp.inc
Plug-in	VNC Connections	vnc-hlp.inc

QUESTION 22
Which three statements about clientless SSL VPN are true? (Choose three.)

A. Users are not tied to a particular PC or workstation.
B. Users have full application access to internal corporate resources.
C. Minimal IT support is required.
D. Cisco AnyConnect SSL VPN software is automatically downloaded to the remote user at the start of the clientless session.

E. For security reasons, browser cookies are disabled for clientless SSL VPN sessions.
F. Clientless SSL VPN requires an SSL-enabled web browser.

Correct Answer: ACF
Section: SSLVPN clientless
Explanation

Explanation/Reference:

QUESTION 23
When establishing a Cisco AnyConnect SSL VPN tunnel, a system administrator wants to restrict remote home office users to either print to their local printer or send the remaining traffic down the Cisco AnyConnect SSL VPN tunnel (with restricted Internet access).
Choose both a tunnel policy option and an ACL type to accomplish this design goal. (Choose two.)

A. tunnel all networks
B. tunnel network list below
C. exclude network list from the tunnel
D. standard ACL
E. web ACL
F. extended ACL

Correct Answer: CD
Section: SSLVPN client
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080702992.shtml

Exam C

QUESTION 1
Upon receiving a digital certificate, what are three steps that a Cisco ASA performs to authenticate the digital certificate? (Choose three.)

A. The identity certificate validity period is verified against the system clock of the Cisco ASA.
B. The identity certificate thumbprint is validated using the private key of the stored CA.
C. The identity certificate signature is validated by using the stored root certificate.
D. The signature is validated by using the stored identity certificate.
E. If enabled, the Cisco ASA locates the CRL and validates the identity certificate.

Correct Answer: ACE
Section: Certifcates
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html#wp1052825

Certificate Revocation Lists provide the security appliance with one means of determining whether a certificate that is within its valid time range has been revoked by its issuing CA. CRL configuration is a part of the configuration of a trustpoint.

You can configure the security appliance to make CRL checks mandatory when authenticating a certificate (revocation-check crl command). You can also make the CRL check optional by adding the none argument (revocation-check crl none command), which allows the certificate authentication to succeed when the CA is unavailable to provide updated CRL data.

The security appliance can retrieve CRLs from CAs using HTTP, SCEP, or LDAP. CRLs retrieved for each trustpoint are cached for a length of time configurable for each trustpoint.

When the security appliance has cached a CRL for more than the length of time it is configured to cache CRLs, the security appliance considers the CRL too old to be reliable, or "stale". The security appliance attempts to retrieve a newer version of the CRL the next time a certificate authentication requires checking the stale CRL.

The security appliance caches CRLs for a length of time determined by the following two factors:

•The number of minutes specified with the cache-time command. The default value is 60 minutes.

•The NextUpdate field in the CRLs retrieved, which may be absent from CRLs. You control whether the security appliance requires and uses the NextUpdate field with the enforcenextupdate command.

The security appliance uses these two factors as follows:

•If the NextUpdate field is not required, the security appliance marks CRLs as stale after the length of time defined by the cache-time command.

•If the NextUpdate field is required, the security appliance marks CRLs as stale at the sooner of the two times specified by the cache-time command and the NextUpdate field. For example, if the cache-time command is set to 100 minutes and the NextUpdate field specifies that the next update is 70 minutes away, the security appliance marks CRLs as stale in 70 minutes.

QUESTION 2
Datagram Transport Layer Security (DTLS) was introduced to solve performance issues. Choose three characteristics of DTLS. (Choose three.)

A. It uses TLS to negotiate and establish DTLS connections.
B. It uses DTLS to transmit datagrams.

C. It is disabled by default.
D. It uses TLS for data packet retransmission.
E. It replaces underlying transport layer with UDP 443.
F. It uses TLS to provide low-latency video application tunneling.

Correct Answer: ABE
Section: SSLVPN client
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect23/administration/23admin2.html#wp1029596

Enabling Datagram Transport Layer Security (DTLS) with AnyConnect (SSL) Connections

Datagram Transport Layer Security avoids latency and bandwidth problems associated with some SSL-only connections, including AnyConnect connections, and improves the performance of real-time applications that are sensitive to packet delays. DTLS is a standards-based SSL protocol that provides a low-latency data path using UDP. For detailed information about DTLS, see RFC 4347 (http://www.ietf.org/rfc/rfc4347.txt).

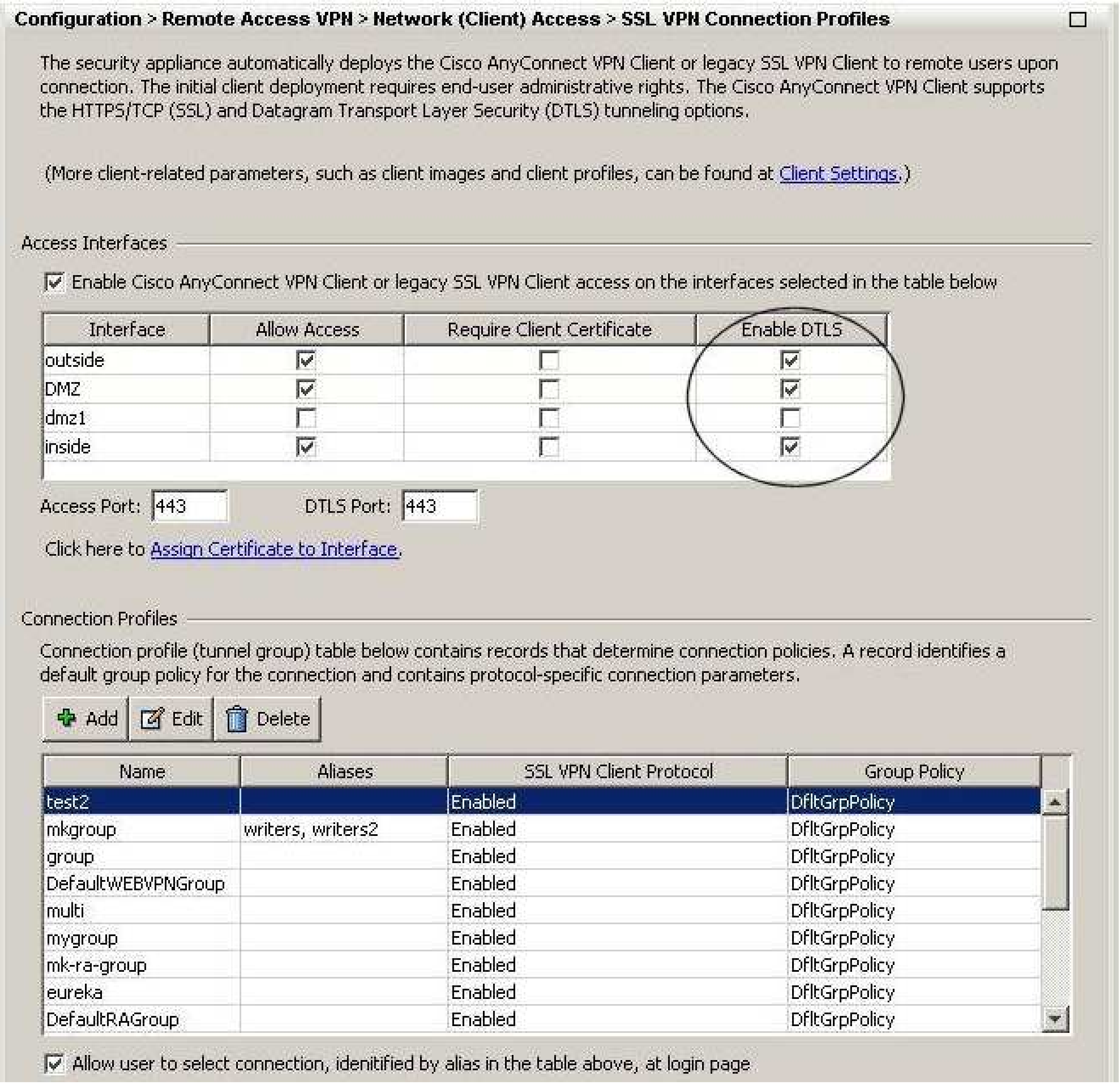
Datagram Transport Layer Security (DTLS) allows the AnyConnect client establishing an SSL VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

If you do not enable DTLS, AnyConnect/SSL VPN connections connect with an SSL VPN tunnel only.

You cannot enable DTLS globally with ASDM. The following section describes how to enable DTLS for any specific interface.

To enable DTLS for a specific interface, select Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN Connection profiles. The SSL VPN Connection Profiles dialog box opens (Figure 2-3).

Figure 2-3 Enable DTLS Check Box



Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the HTTPS/TCP (SSL) and Datagram Transport Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at Client Settings.)

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below

Interface	Allow Access	Require Client Certificate	Enable DTLS
outside	☑	□	☑
DMZ	☑	□	☑
dmz1	□	□	□
inside	☑	□	☑

Access Port: 443 DTLS Port: 443

Click here to Assign Certificate to Interface.

Connection Profiles

Connection profile (tunnel group) table below contains records that determine connection policies. A record identifies a default group policy for the connection and contains protocol-specific connection parameters.

Name	Aliases	SSL VPN Client Protocol	Group Policy
test2		Enabled	DfltGrpPolicy
mkgroup	writers, writers2	Enabled	DfltGrpPolicy
group		Enabled	DfltGrpPolicy
DefaultWEBVPNGroup		Enabled	DfltGrpPolicy
multi		Enabled	DfltGrpPolicy
mygroup		Enabled	DfltGrpPolicy
mk-ra-group		Enabled	DfltGrpPolicy
eureka		Enabled	DfltGrpPolicy
DefaultRAGroup		Enabled	DfltGrpPolicy

☑ Allow user to select connection, idenitified by alias in the table above, at login page

Enabling Datagram Transport Layer Security (DTLS) allows the AnyConnect VPN Client establishing an SSL VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays. If you do not enable DTLS, AnyConnect client users establishing SSL VPN connections connect with an SSL VPN tunnel only. **Fields** • Interface—Displays a list of interfaces on the security appliance. • DTLS Enabled—Check to enable DTLS connections with the AnyConnect client on the interfaces. • UDP Port (default 443)—(Optional) Specify a separate UDP port for DTLS connections.

QUESTION 3
Which three options are characteristics of WebType ACLs? (Choose three.)

A. They are assigned per-connection profile.
B. They are assigned per-user or per-group policy.
C. They can be defined in the Cisco AnyConnect Profile Editor.
D. They support URL pattern matching.
E. They support implicit deny all at the end of the ACL.
F. They support standard and extended WebType ACLs.

Correct Answer: BDE
Section: SSLVPN clientless
Explanation

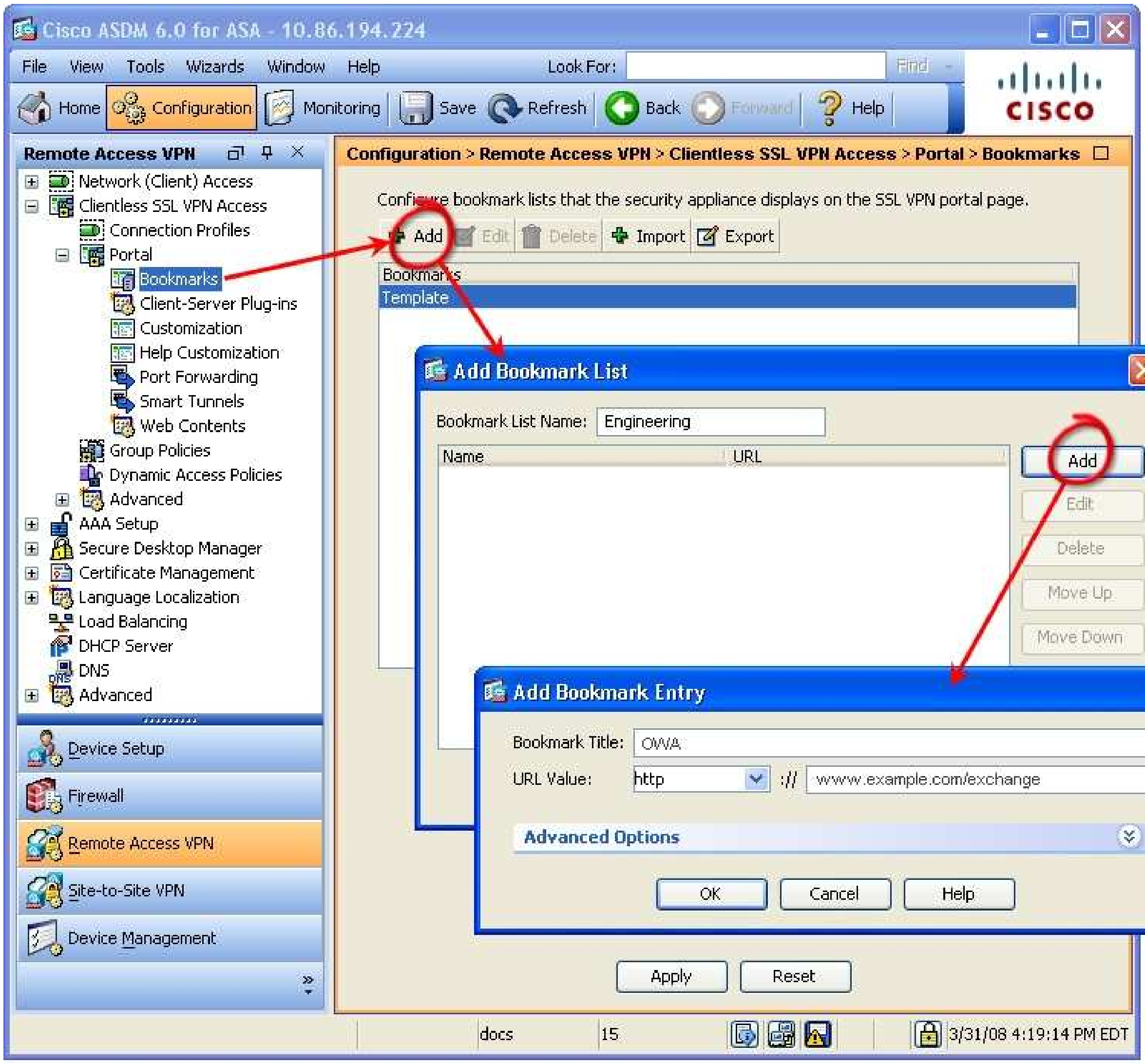
Explanation/Reference:
You can configure ACLs (Access Control Lists) to apply to user sessions. These are filters that permit or deny user access to specific networks, subnets, hosts, and web servers. • If you do not define any filters, all connections are permitted. • The security appliance supports only an inbound ACL on an interface. • At the end of each ACL, there is an implicit, unwritten rule that denies all traffic that is not permitted. If traffic is not explicitly permitted by an access control entry (ACE), the security appliance denies it. ACEs are referred to as rules in this topic. This pane lets you add and edit ACLs to be used for Clientless SSL VPN sessions, and the ACL entries each ACL contains. It also displays summary information about ACLs and ACEs, and lets you enable or disable them, and change their priority order.

QUESTION 4
For clientless SSL VPN users, bookmarks can be assigned to their portal. What are three methods for assigning bookmarks? (Choose three.)

A. connection profiles
B. group policies
C. XML profiles
D. LDAP or RADIUS attributes
E. the portal customization tool
F. user policies

Correct Answer: BDF
Section: SSLVPN clientless
Explanation

Explanation/Reference:
Create one or more bookmark list entries that specify the URLs of the web-enabled applications eligible for smart tunnel access, then assign the list to the DAPs, group policies, or local user policies for whom you want to provide smart tunnel access. e.g.



Cisco ASDM 6.0 for ASA - 10.86.194.224

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

Configure bookmark lists that the security appliance displays on the SSL VPN portal page.

Add Bookmark List

Bookmark List Name: Engineering

Add Bookmark Entry

Bookmark Title: OWA

URL Value: http :// www.example.com/exchange

docs 15 3/31/08 4:19:14 PM EDT

Dynamic access policies (DAP)

VPN gateways operate in dynamic environments. Multiple variables can affect each VPN connection, for example, intranet configurations that frequently change, the various roles each user may inhabit within an organization, and logins from remote access sites with different configurations and levels of security. The task of authorizing users is much more complicated in a VPN environment than it is in a network with a static configuration.

Dynamic Access Policies (DAP) on the security appliance let you configure authorization that addresses these many variables. You create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session. These attributes address issues of multiple group membership and endpoint security. That is, the security appliance grants access to a particular user for a particular session based on the policies you define. It generates a DAP at the time the user connects by selecting and/or aggregating attributes from one or more DAP records. It selects these DAP records based on the endpoint security information of the remote device and the AAA authorization information for the authenticated user. It then applies the DAP record to the user tunnel or session.

QUESTION 5

Your IT department needs to run a custom-built TCP application within the clientless SSL VPN tunnel. The network administrator suggests running the smart tunnel application. Which three statements concerning smart tunnel applications are true? (Choose three.)

A. They support active FTP and other RTSP-based applications.
B. They do not require administrator privileges on the remote system.
C. They require the enabling of port forwarding.
D. They are supported on Windows and MAC OS X platforms.
E. They support native client applications over SSL VPN.
F. They require the modification of the Host file on the end-user PC.

Correct Answer: BDE
Section: SSLVPN clientless
Explanation

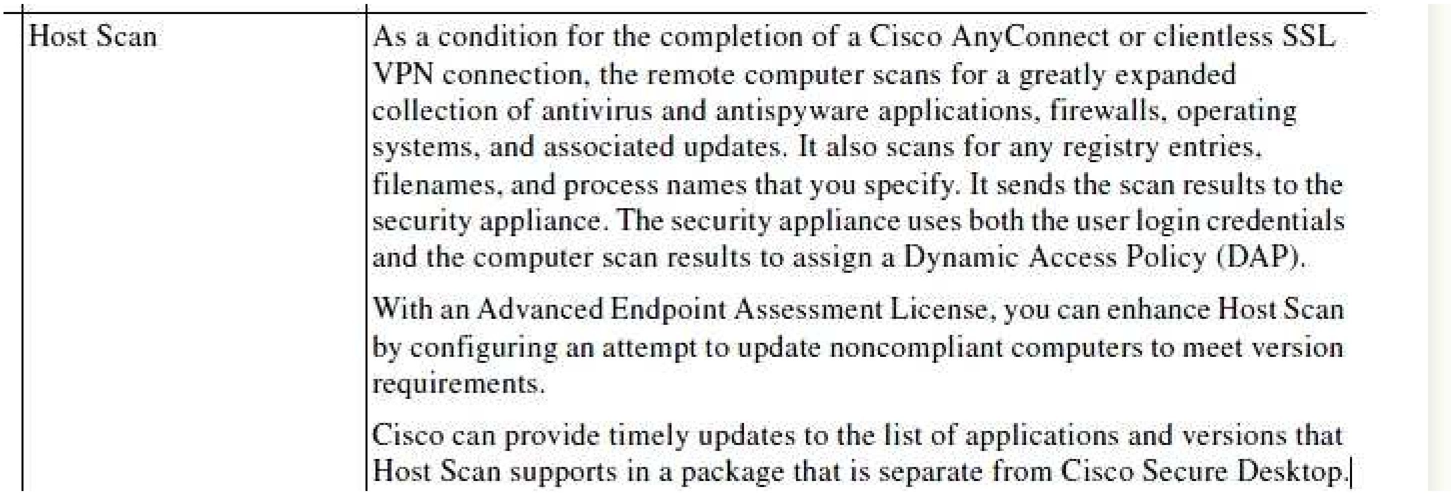
Explanation/Reference:
Smart Tunnel—Connects a Winsock 2, TCP-based application installed on the end station to a server on the intranet, using a clientless (browser-based) SSL VPN session with the security appliance as the pathway, and the security appliance as a proxy server.
– Smart Tunnel List—Select the list name from the drop-down menu if you want to provide smart tunnel access. Assigning a smart tunnel list to a group policy or username enables smart tunnel access for all users whose sessions are associated with the group policy or username, but restricts smart tunnel access to the applications specified in the list. To view, add, modify, or delete a smart tunnel list, click the adjacent **Manage** button.
– Auto Start (Smart Tunnel List)—Check to start smart tunnel access automatically upon user login. Uncheck to enable smart tunnel access upon user login, but require the user to start it manually, using the Application Access > Start Smart Tunnels button on the Clientless SSL VPN Portal Page.
– Auto Sign-on Server List—Select the list name from the drop-down menu if you want to reissue the user credentials when the user establishes a smart tunnel connection to a server. Each smart tunnel auto sign-on list entry identifies a server with which to automate the submission of user credentials. To view, add, modify, or delete a smart tunnel auto sign-on list, click the adjacent **Manage** button.
– Domain Name (Optional)—Specify the Windows domain to add it to the username during auto sign-on, if the universal naming convention (domain\username) is required for authentication. For example, enter CISCO to specify CISCO\jsmith when authenticating for the username jsmith. You must also check the “Use Windows domain name with user name” option when configuring associated entries in the auto sign-on server list.

QUESTION 6
Which four statements about the Advanced Endpoint Assessment are correct? (Choose four.)

A. It examines the remote computer for personal firewall applications.
B. It examines the remote computer for antivirus applications.
C. It examines the remote computer for antispyware applications.
D. It examines the remote computer for malware applications.
E. It does not perform any remediation, but it provides input that can be evaluated by DAP records.
F. It performs active remediation by applying rules, activating modules, and providing updates where applicable.

Correct Answer: ABCF
Section: SSLVPN client
Explanation

Explanation/Reference:



Host Scan	As a condition for the completion of a Cisco AnyConnect or clientless SSL VPN connection, the remote computer scans for a greatly expanded collection of antivirus and antispyware applications, firewalls, operating systems, and associated updates. It also scans for any registry entries, filenames, and process names that you specify. It sends the scan results to the security appliance. The security appliance uses both the user login credentials and the computer scan results to assign a Dynamic Access Policy (DAP). With an Advanced Endpoint Assessment License, you can enhance Host Scan by configuring an attempt to update noncompliant computers to meet version requirements. Cisco can provide timely updates to the list of applications and versions that Host Scan supports in a package that is separate from Cisco Secure Desktop.

QUESTION 7
The software-based Cisco IPsec VPN Client solution uses bidirectional authentication, in which the client authenticates the Cisco ASA, and the Cisco ASA authenticates the user. Which three methods are software-based Cisco IPsec VPN Client to Cisco ASA authentication methods? (Choose three.)

A. Unified Client Certificate authentication
B. Secure Unit authentication
C. Hybrid authentication
D. Certificate authentication
E. Group authentication

Correct Answer: CDE
Section: IPsec
Explanation

Explanation/Reference:
ASDM user guide Page 35-69

Authentication Mode—Specifies the authentication mode: none, xauth, or hybrid.

hybrid—Specifies the use of Hybrid mode, which lets you use digital certificates for security appliance authentication and a different, legacy method—such as RADIUS, TACACS+ or SecurID—for remote VPN user authentication. This mode breaks phase 1 of the Internet Key Exchange (IKE) into the following steps, together called hybrid authentication:

xauth—Specifies the use of IKE Extended Authentication mode, which provides the capability of authenticating a user within IKE using TACACS+ or RADIUS.

QUESTION 8
Which two options are correct regarding IKE and IPv6 VPN support on the Cisco ASA using version 8.4? (Choose two.)

A. The Cisco ASA supports full IKEv2 IPv6 for site-to-site VPNs only.
B. The Cisco ASA supports full IKEv2 IPv6 for remote-access VPNs.
C. The Cisco ASA supports IKEv1 and IKEv2 configuration on the same crypto map.
D. The Cisco ASA supports negotiation of authentication type using IKEv2 with IPv6.
E. The Cisco ASA supports all types of VPN configurations when using IPv6

Correct Answer: AC
Section: IPsec
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_bulletin_c25-593781.html

• IPv6 IPsec Site-to-Site VPN: Customers can now create encrypted IPsec VPN connections over IPv6 networks

http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/vpn_site2site.html#wp1061313

For IKEv2, you can configure multiple encryption and authentication types, and multiple integrity algorithms for a single policy. The ASA orders the settings from the most secure to the least secure and negotiates with the peer using that order. This allows you to potentially send a single proposal to convey all the allowed transforms instead of the need to send each allowed combination as with IKEv1.

QUESTION 9
In Cisco ASDM v6.4, what are four ways to implement single sign-on (SSO)? (Choose four.)

A. Use SSO for smart tunnels.
B. Use Kerberos SSO.
C. Use the HTTP Form protocol.
D. Use a dedicated SSO server.
E. Use SSO for application plug-ins.
F. Use auto sign-on for servers that do not require authentication credentials.

Correct Answer: ACDE
Section: SSLVPN client
Explanation

Explanation/Reference:
The security appliance can use the HTTP Form protocol for single sign-on (SSO) authentication of WebVPN users only. Single sign-on support lets WebVPN users enter a username and password only once to access multiple protected services and Web servers. The WebVPN server running on the security appliance acts as a proxy for the user to the authenticating server. When a user logs in, the WebVPN server sends an SSO authentication request, including username and password, to the authenticating server using HTTPS. If the server approves the authentication request, it returns an SSO authentication cookie to the WebVPN server. The security appliance keeps this cookie on behalf of the user and uses it to authenticate the user to secure websites within the domain protected by the SSO server. In addition to the HTTP Form protocol, WebVPN administrators can choose to configure SSO with the HTTP Basic and NTLM authentication protocols (the **auto-signon** command), or with Computer Associates eTrust SiteMinder SSO server (formerly Netegrity SiteMinder) as well. For an in-depth discussion of configuring SSO with either HTTP Forms, **auto-signon** or SiteMinder,

The Auto Signon window or tab lets you configure or edit auto signon for users of Clientless SSL VPN. Auto signon is a simplified single signon method that you can use if you do not already have an SSO method deployed on your internal network. With auto signon configured for particular internal servers, the security appliance passes the login credentials that the user of Clientless SSL VPN entered to log in to the security appliance (username and password) to those particular internal servers. You configure the security appliance to respond to a specific authentication method for a particular range of servers. The authentication methods you can configure the security appliance to respond to consists of authentication using Basic (HTTP), NTLM, FTP and CIFS, or all of these methods. Auto signon is a straight-forward method for configuring SSO for particular internal servers. This section describes the procedure for setting up SSO with auto signon. If you already have SSO deployed using Computer Associates' SiteMinder SSO server, or if you have Security Assertion Markup Language (SAML) Browser Post Profile SSO,

QUESTION 10
Which two types of digital certificate enrollment processes are available for the Cisco ASA security appliance? (Choose two.)

A. LDAP
B. FTP
C. TFTP
D. HTTP
E. SCEP
F. Manual

Correct Answer: EF
Section: Certifcates
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080b25dc1.shtml

and

http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00808b3cff.shtml

QUESTION 11
Which four parameters must be defined in an ISAKMP policy when you are creating an IPsec site-to-site VPN using the Cisco ASDM? (Choose four.)

A. encryption algorithm
B. hash algorithm
C. authentication method
D. IP address of remote IPsec peer
E. D-H group
F. perfect forward secrecy

Correct Answer: ABCE
Section: IPsec
Explanation

Explanation/Reference:
ASDM User guide Page 34-5

Should this not be IKE policy?
.

Fields

Priority #—Type a number to set a priority for the IKE policy. The range is 1 to 65,543, with 1 the highest priority.

Encryption—Select an encryption method. This is a symmetric encryption method that protects data transmitted between two IPsec peers.The choices follow:

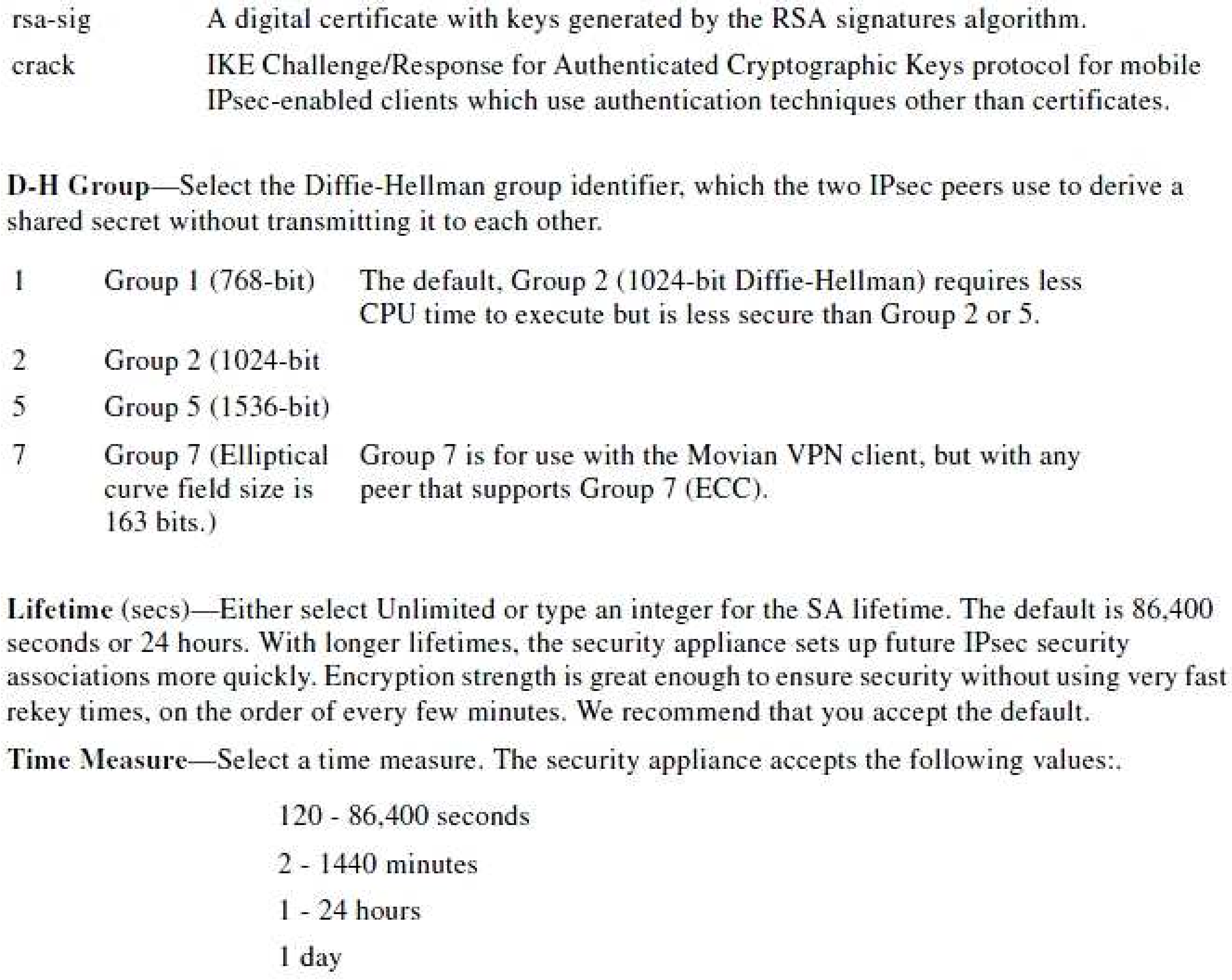
des	56-bit DES-CBC. Less secure but faster than the alternatives. The default.
3des	168-bit Triple DES.
aes	128-bit AES.
aes-192	192-bit AES.
aes-256	256-bit AES.

Hash—Select the hash algorithm that ensures data integrity. It ensures that a packet comes from whom you think it comes from, and that it has not been modified in transit.

sha	SHA-1	The default is SHA-1. MD5 has a smaller digest and is considered to be slightly faster than SHA-1. A successful (but extremely difficult) attack against MD5 has occurred; however, the HMAC variant IKE uses prevents this attack.
md5	MD5	

Authentication—Select the authentication method the security appliance uses to establish the identity of each IPsec peer. Pre-shared keys do not scale well with a growing network but are easier to set up in a small network. The choices follow:

pre-share	Pre-shared keys.



rsa-sig	A digital certificate with keys generated by the RSA signatures algorithm.
crack	IKE Challenge/Response for Authenticated Cryptographic Keys protocol for mobile IPsec-enabled clients which use authentication techniques other than certificates.

D-H Group—Select the Diffie-Hellman group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other.

1	Group 1 (768-bit)	The default, Group 2 (1024-bit Diffie-Hellman) requires less CPU time to execute but is less secure than Group 2 or 5.
2	Group 2 (1024-bit	
5	Group 5 (1536-bit)	
7	Group 7 (Elliptical curve field size is 163 bits.)	Group 7 is for use with the Movian VPN client, but with any peer that supports Group 7 (ECC).

Lifetime (secs)—Either select Unlimited or type an integer for the SA lifetime. The default is 86,400 seconds or 24 hours. With longer lifetimes, the security appliance sets up future IPsec security associations more quickly. Encryption strength is great enough to ensure security without using very fast rekey times, on the order of every few minutes. We recommend that you accept the default.

Time Measure—Select a time measure. The security appliance accepts the following values:.

120 - 86,400 seconds

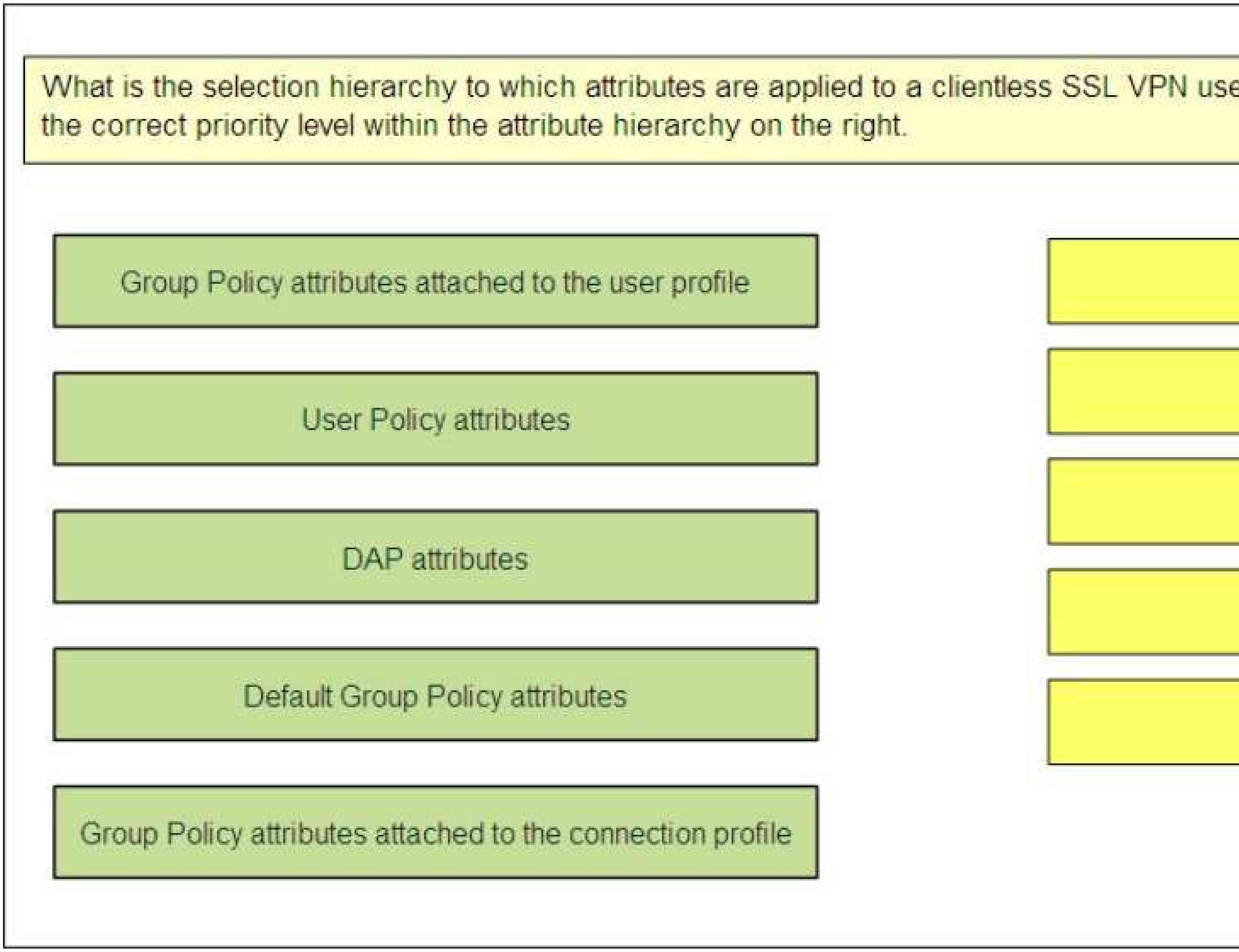
2 - 1440 minutes

1 - 24 hours

1 day

QUESTION 12

Select and Place:



What is the selection hierarchy to which attributes are applied to a clientless SSL VPN use
the correct priority level within the attribute hierarchy on the right.

Group Policy attributes attached to the user profile

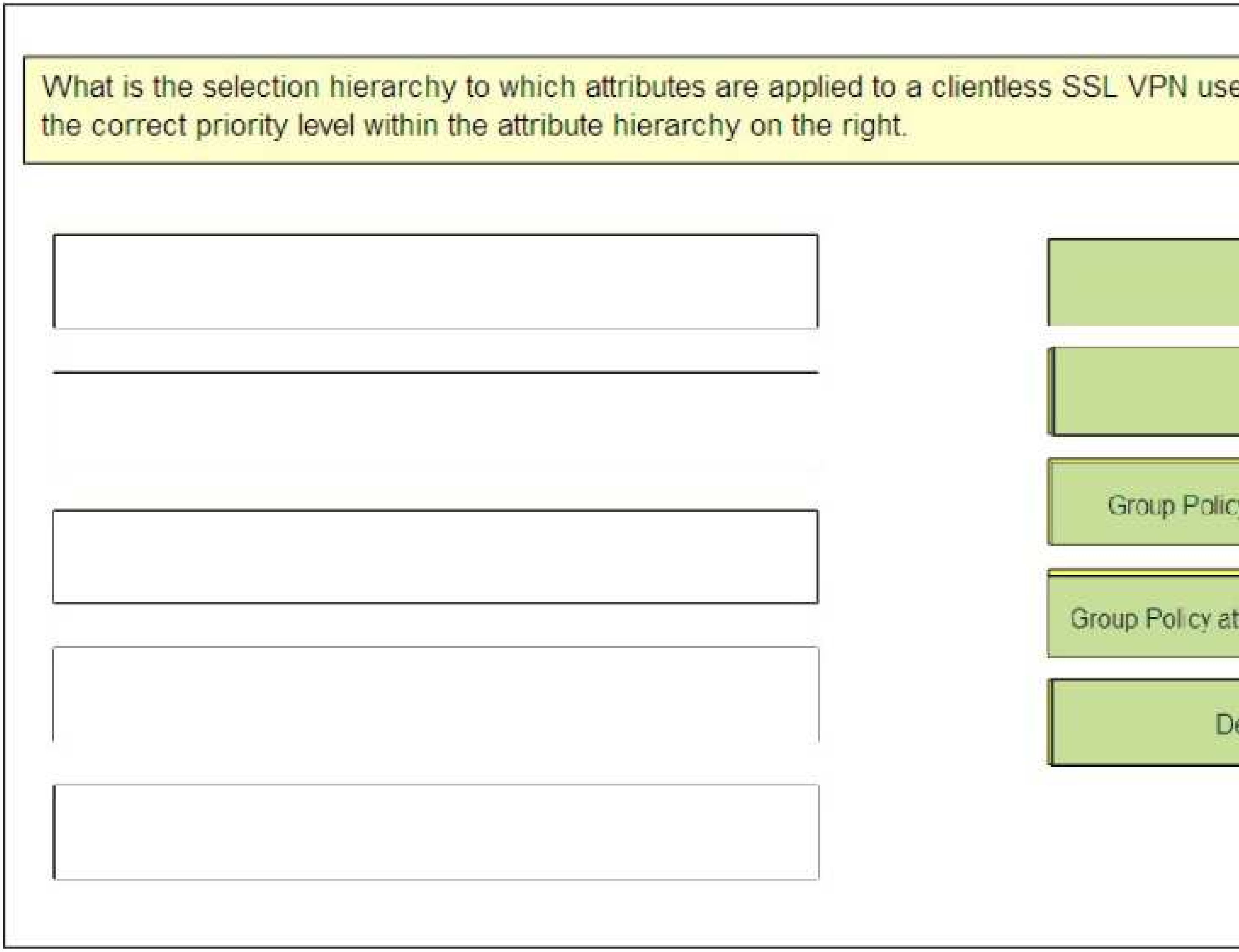
User Policy attributes

DAP attributes

Default Group Policy attributes

Group Policy attributes attached to the connection profile

Correct Answer:



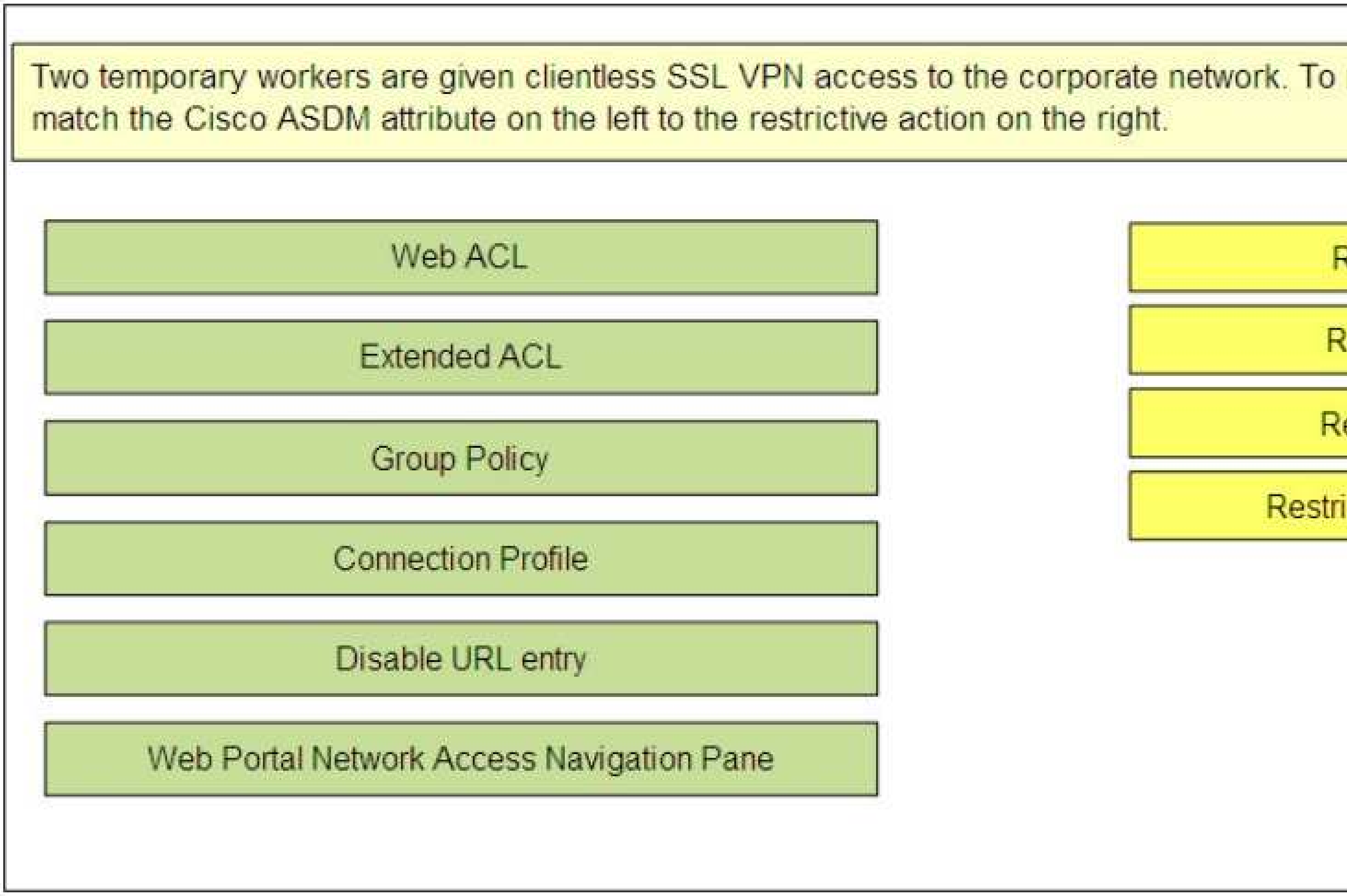
What is the selection hierarchy to which attributes are applied to a clientless SSL VPN use
the correct priority level within the attribute hierarchy on the right.

Section: D & D
Explanation

Explanation/Reference:

QUESTION 13

Select and Place:



Two temporary workers are given clientless SSL VPN access to the corporate network. To
match the Cisco ASDM attribute on the left to the restrictive action on the right.

Web ACL

Extended ACL

Group Policy

Connection Profile

Disable URL entry

Web Portal Network Access Navigation Pane

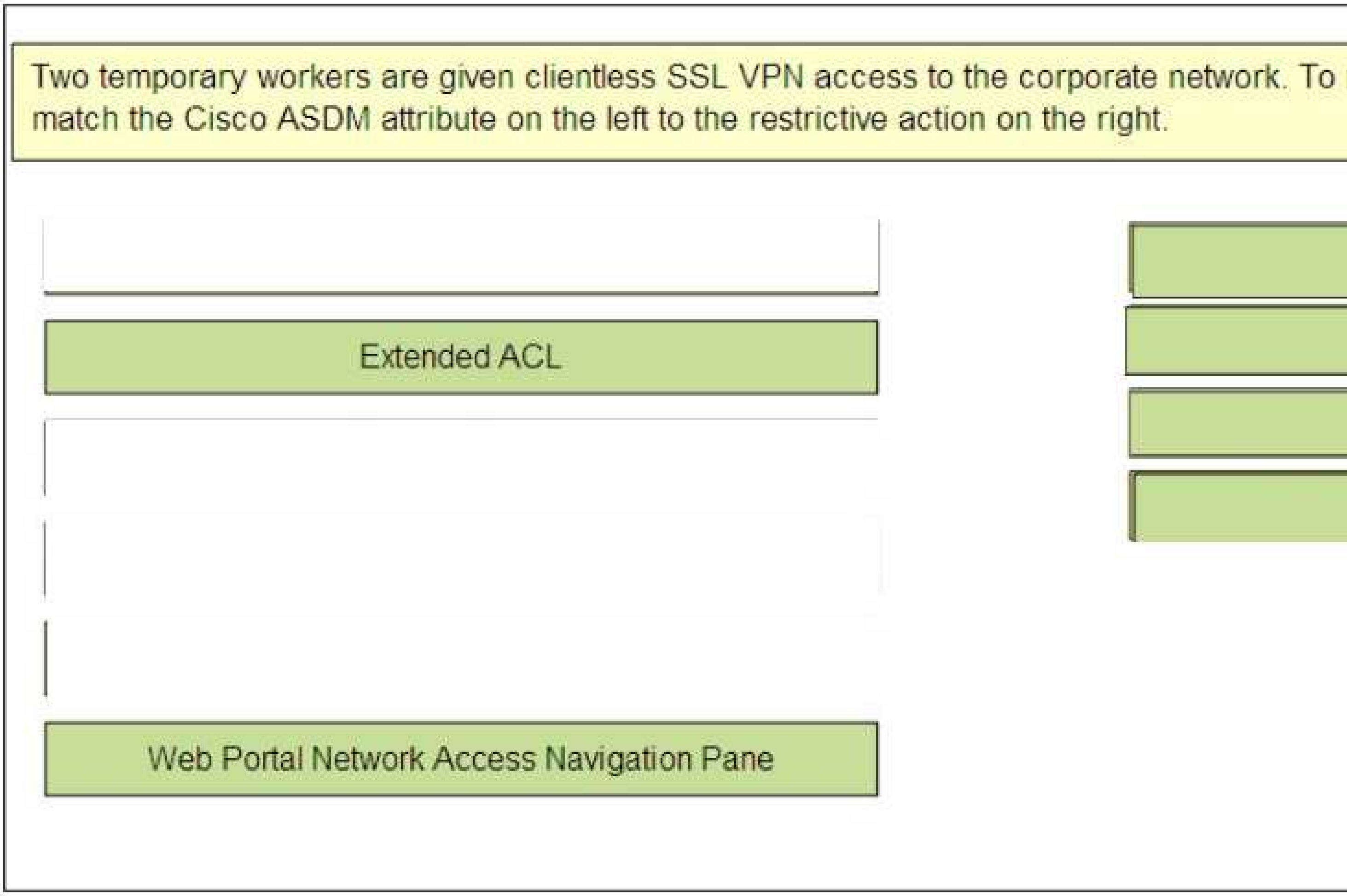
R

R

Re

Restri

Correct Answer:



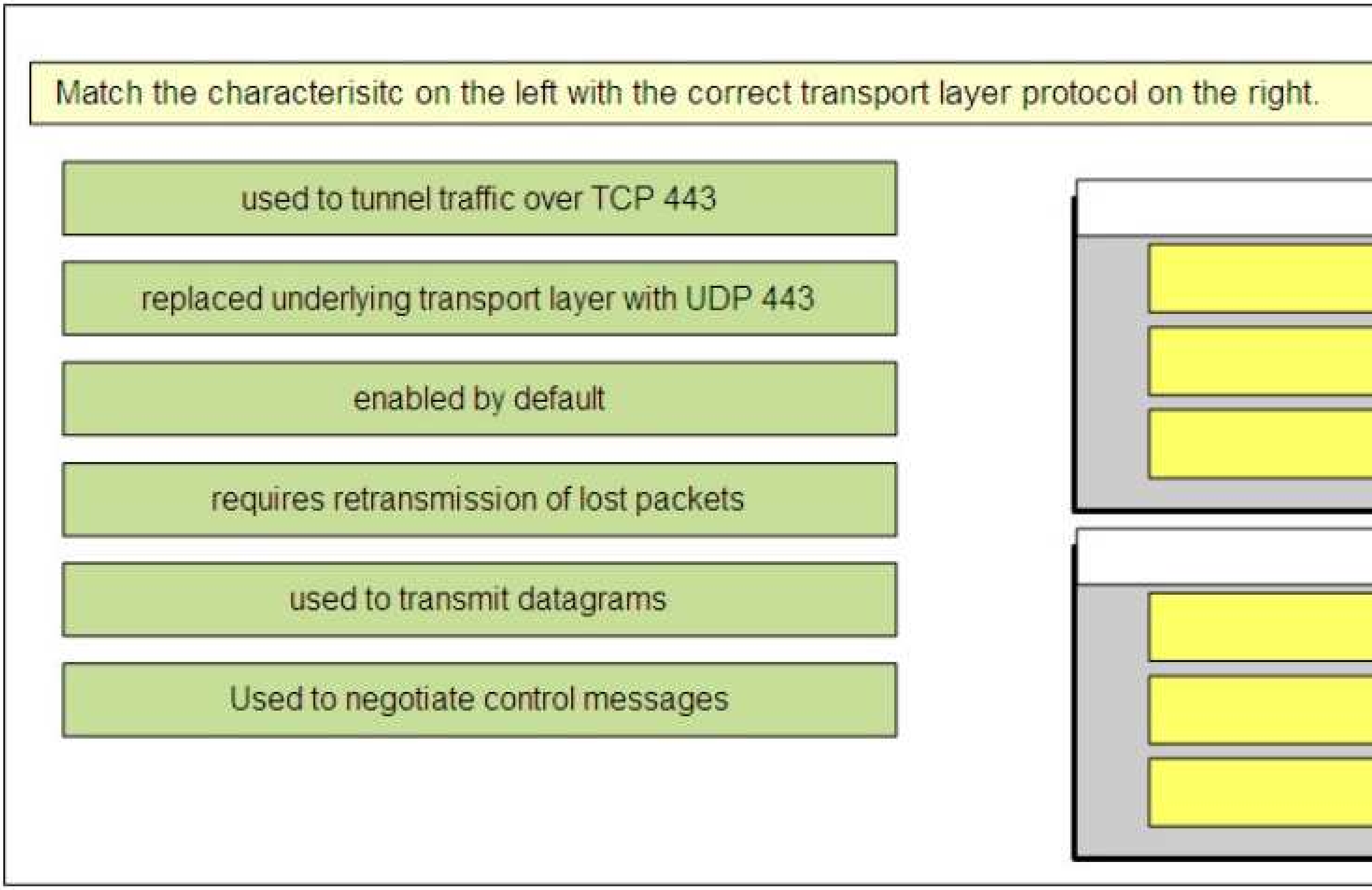
Two temporary workers are given clientless SSL VPN access to the corporate network. To
match the Cisco ASDM attribute on the left to the restrictive action on the right.

Section: D & D
Explanation

Explanation/Reference:

QUESTION 14

Select and Place:



Match the characterisitc on the left with the correct transport layer protocol on the right.

used to tunnel traffic over TCP 443

replaced underlying transport layer with UDP 443

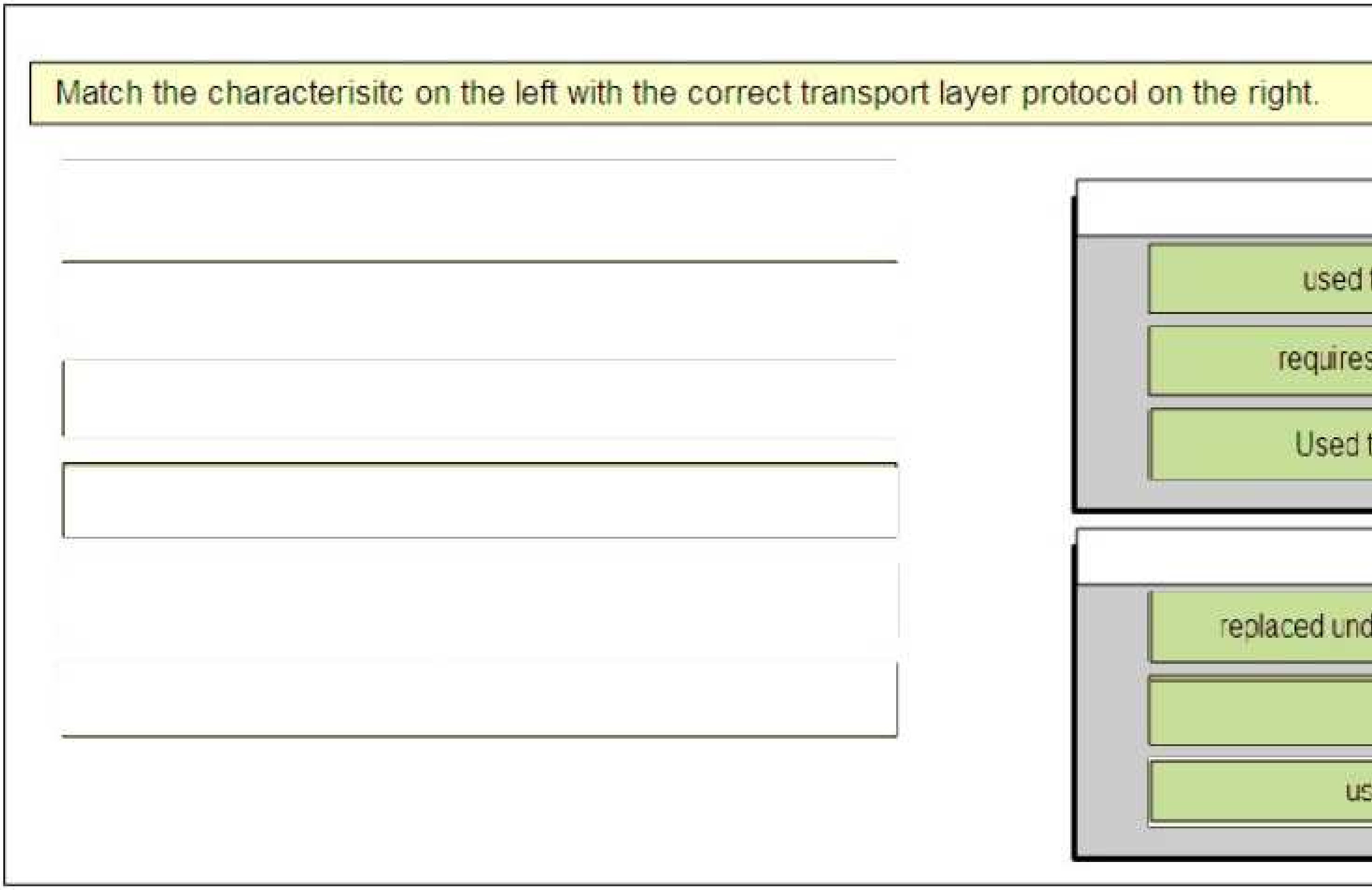
enabled by default

requires retransmission of lost packets

used to transmit datagrams

Used to negotiate control messages

Correct Answer:



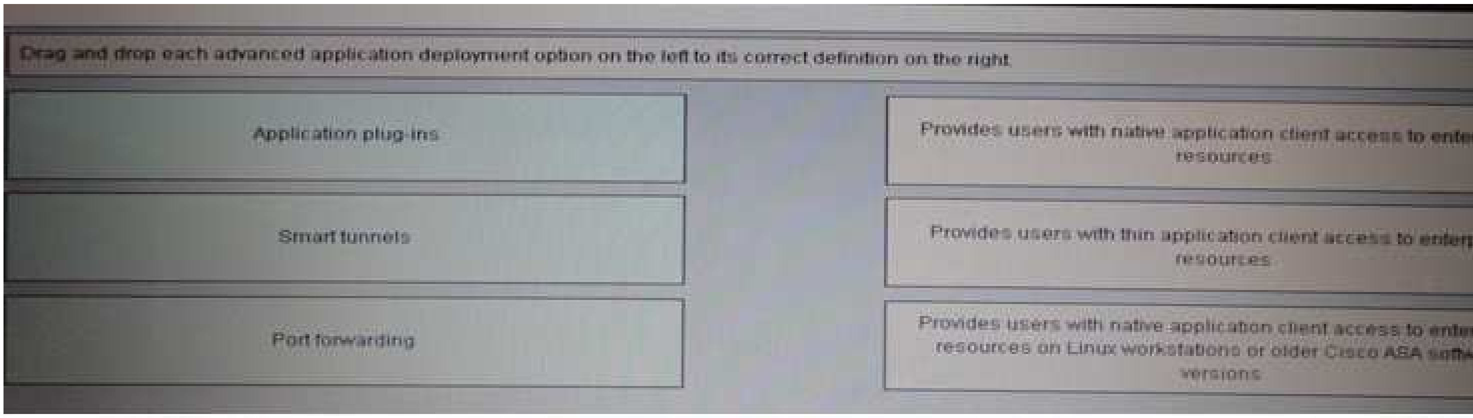
Match the characterisitc on the left with the correct transport layer protocol on the right.

Section: D & D
Explanation

Explanation/Reference:

QUESTION 15

Select and Place:



Drag and drop each advanced application deployment option on the left to its correct definition on the right.

Application plug-ins

Smart tunnels

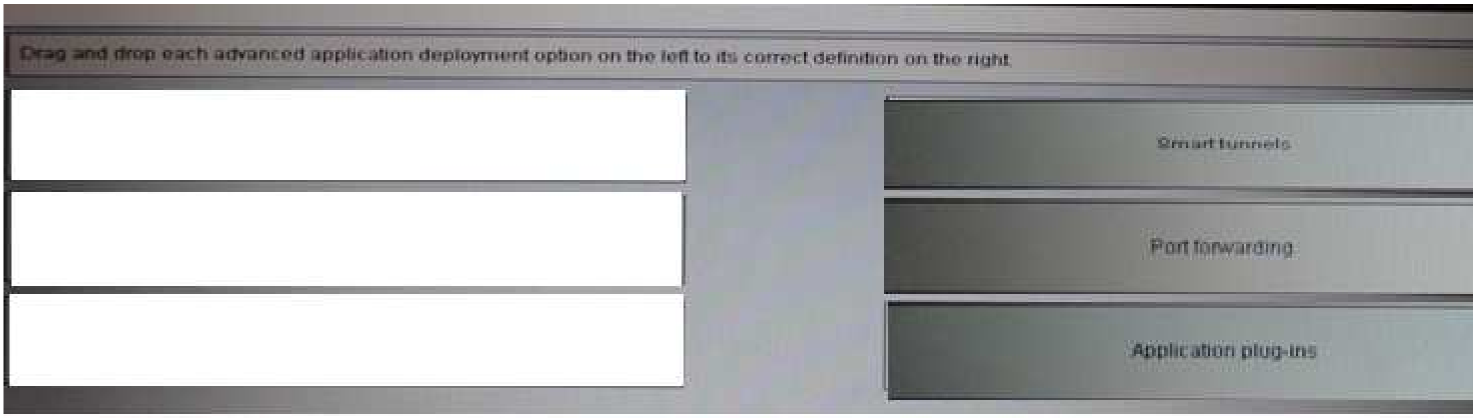
Port forwarding

Provides users with native application client access to ente resources

Provides users with thin application client access to enterp resources

Provides users with native application client access to ente resources on Linux workstations or older Cisco ASA softw versions

Correct Answer:



Drag and drop each advanced application deployment option on the left to its correct definition on the right.

Section: D & D
Explanation

Explanation/Reference:

Explanation:

Application plugin *Provide users with thin native application client access to enterprise resources on Linux workstations or older Cisco ASA software versions

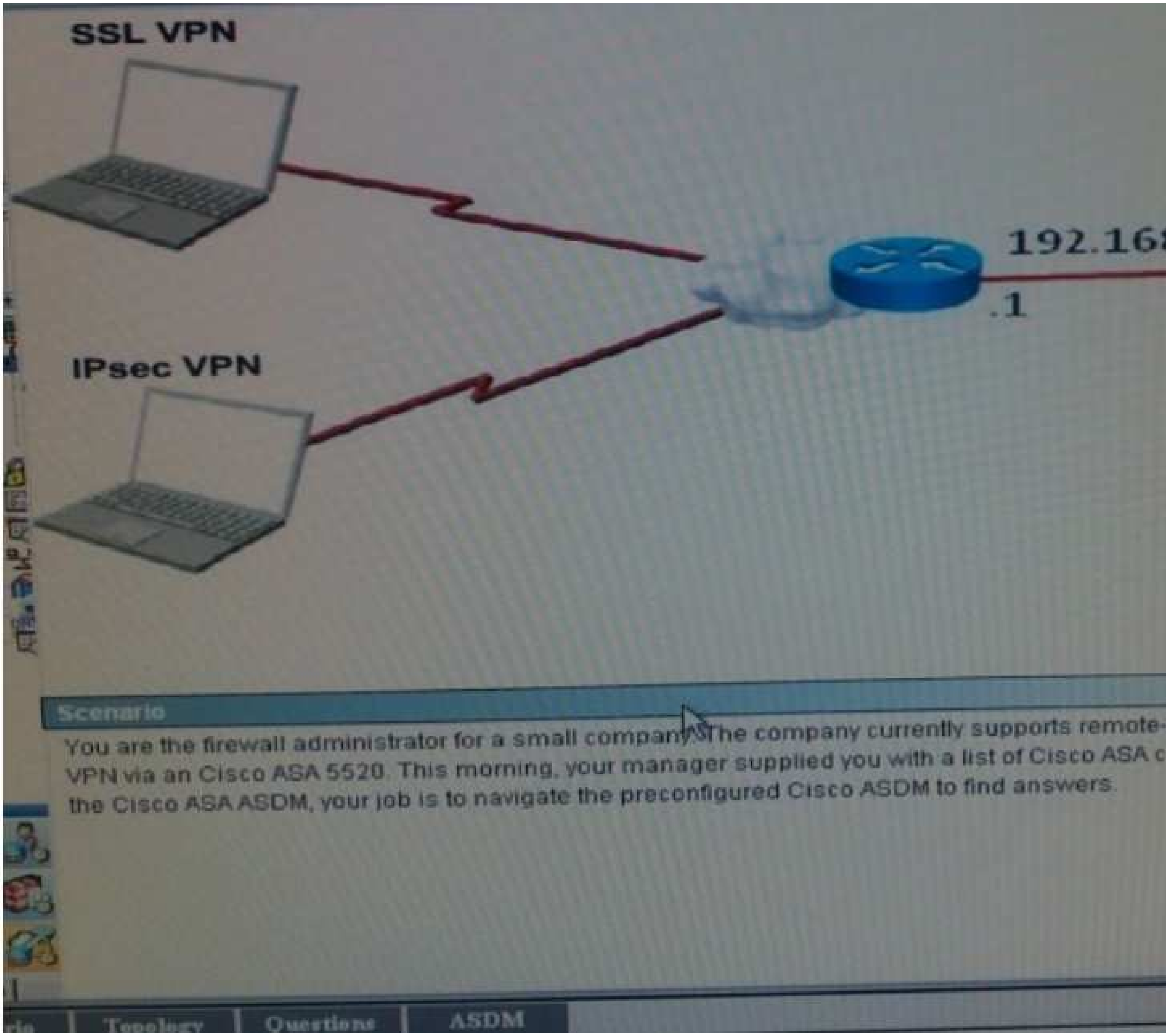
Smart tunnel *Provide users with native application client access to enterprise resources

Port Forwarding *Provides user with thin application client access to enterprise resources

QUESTION 16
After providing the correct VPN login credentials, user, contractor1, is enabled to use which VPN access type?

Case Study Title (Case Study):
After providing the correct VPN login credentials, user, contractor1, is enabled to use which VPN access type?

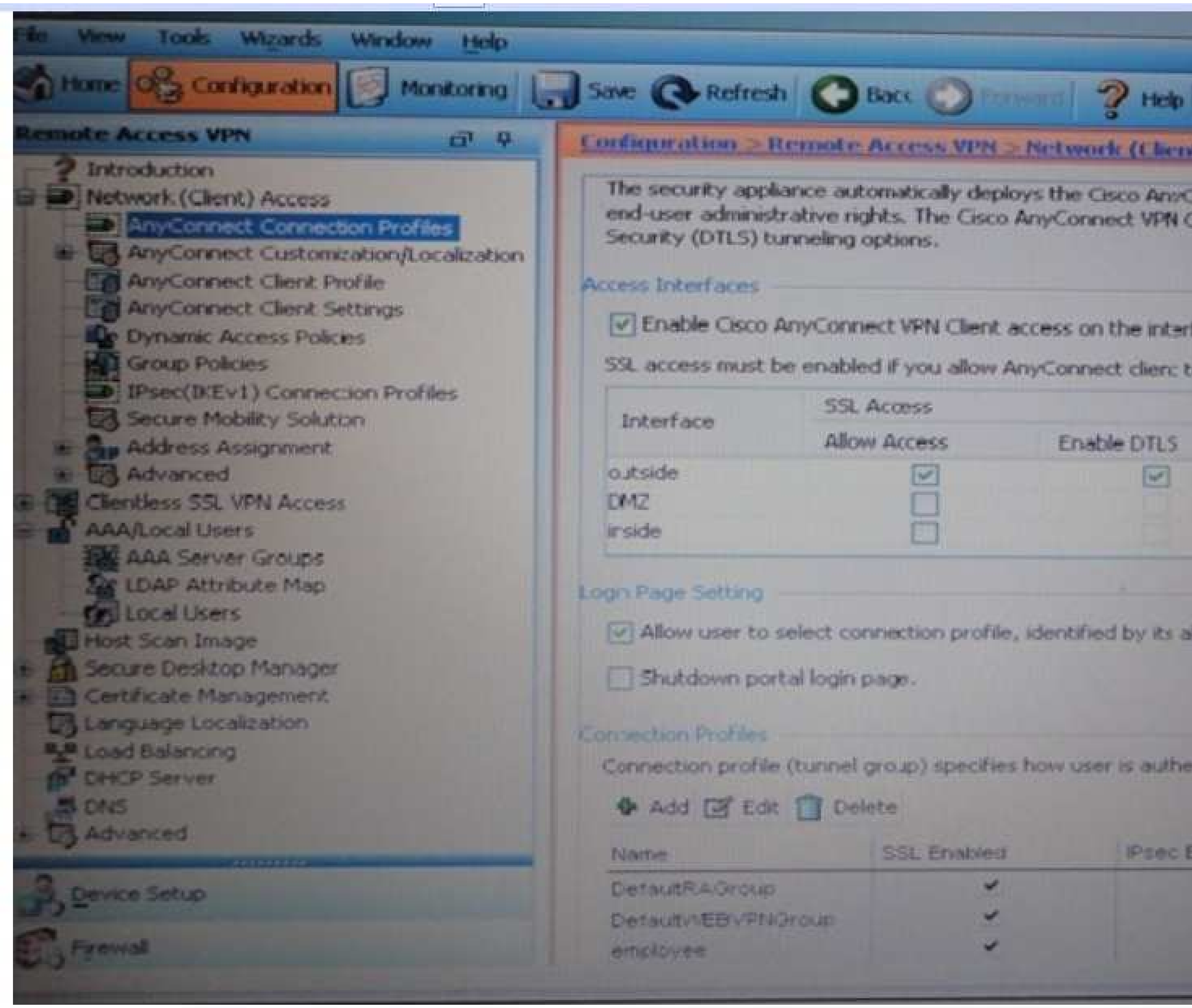
1 (exhibit):



Scenario

You are the firewall administrator for a small company. The company currently supports remote-
VPN via an Cisco ASA 5520. This morning, your manager supplied you with a list of Cisco ASA c
the Cisco ASA ASDM, your job is to navigate the preconfigured Cisco ASDM to find answers.

2 (exhibit):



Configuration > Remote Access VPN > Network (Clien

The security appliance automatically deploys the Cisco AnyC end-user administrative rights. The Cisco AnyConnect VPN C Security (DTLS) tunneling options.

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the inter

SSL access must be enabled if you allow AnyConnect clien t

Interface	SSL Access	
	Allow Access	Enable DTLS
outside	☑	☑
DMZ	□	
inside	□	

Login Page Setting

☑ Allow user to select connection profile, identified by its a

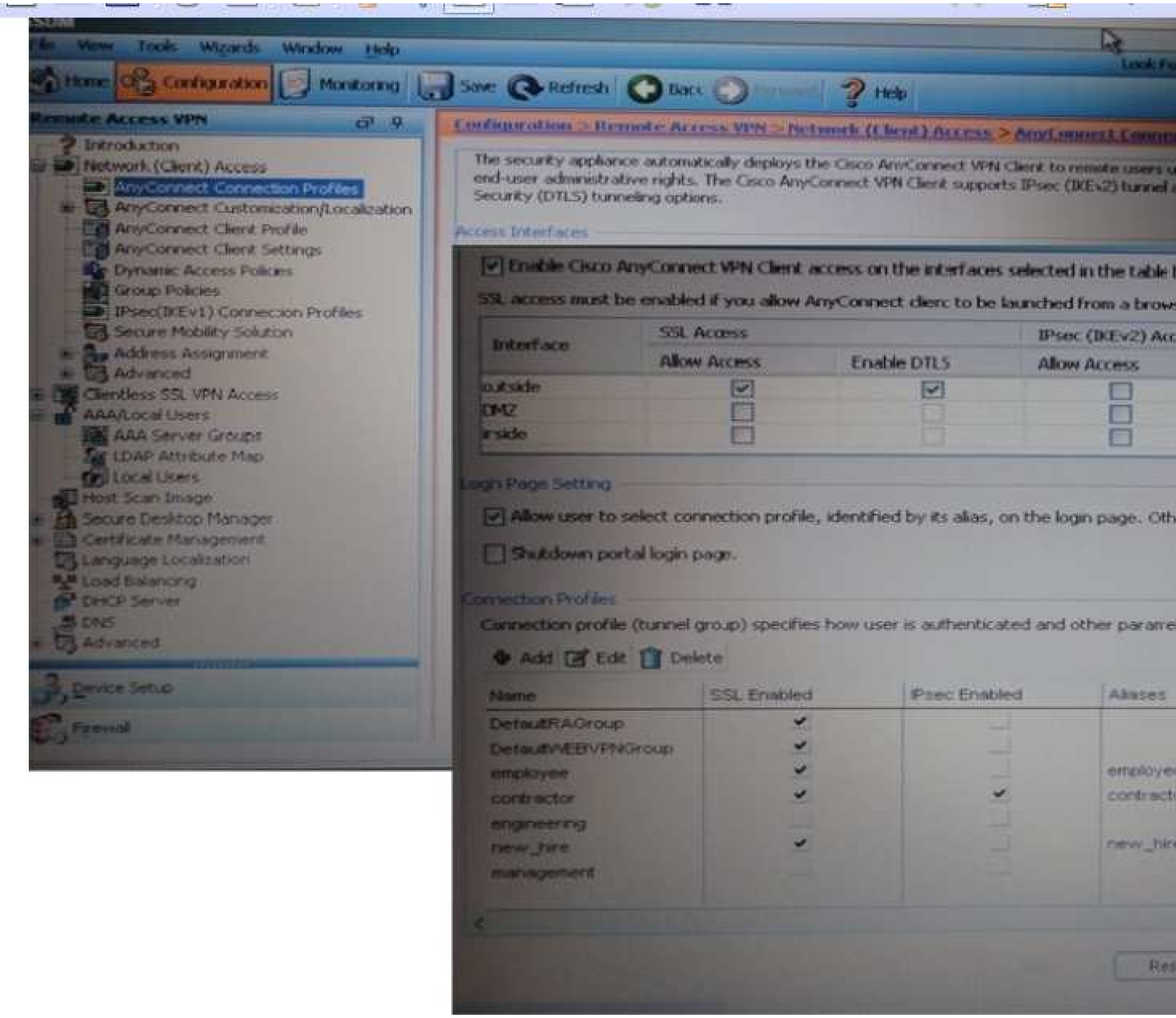
□ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authe

Name	SSL Enabled	IPsec E
DefaultRAGroup	✓	
DefaultWEBVPNGroup	✓	
employee	✓	

3 (exhibit):



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Conne

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users u end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel a Security (DTLS) tunneling options.

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table b

SSL access must be enabled if you allow AnyConnect clenc to be launched from a brow

Interface	SSL Access		IPsec (IKEv2) Acc
	Allow Access	Enable DTLS	Allow Access
outside	☑	☑	□
DMZ	□	□	□
inside	□	□	□

Login Page Setting

☑ Allow user to select connection profile, identified by its alias, on the login page. Oth

□ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parame

Add Edit Delete

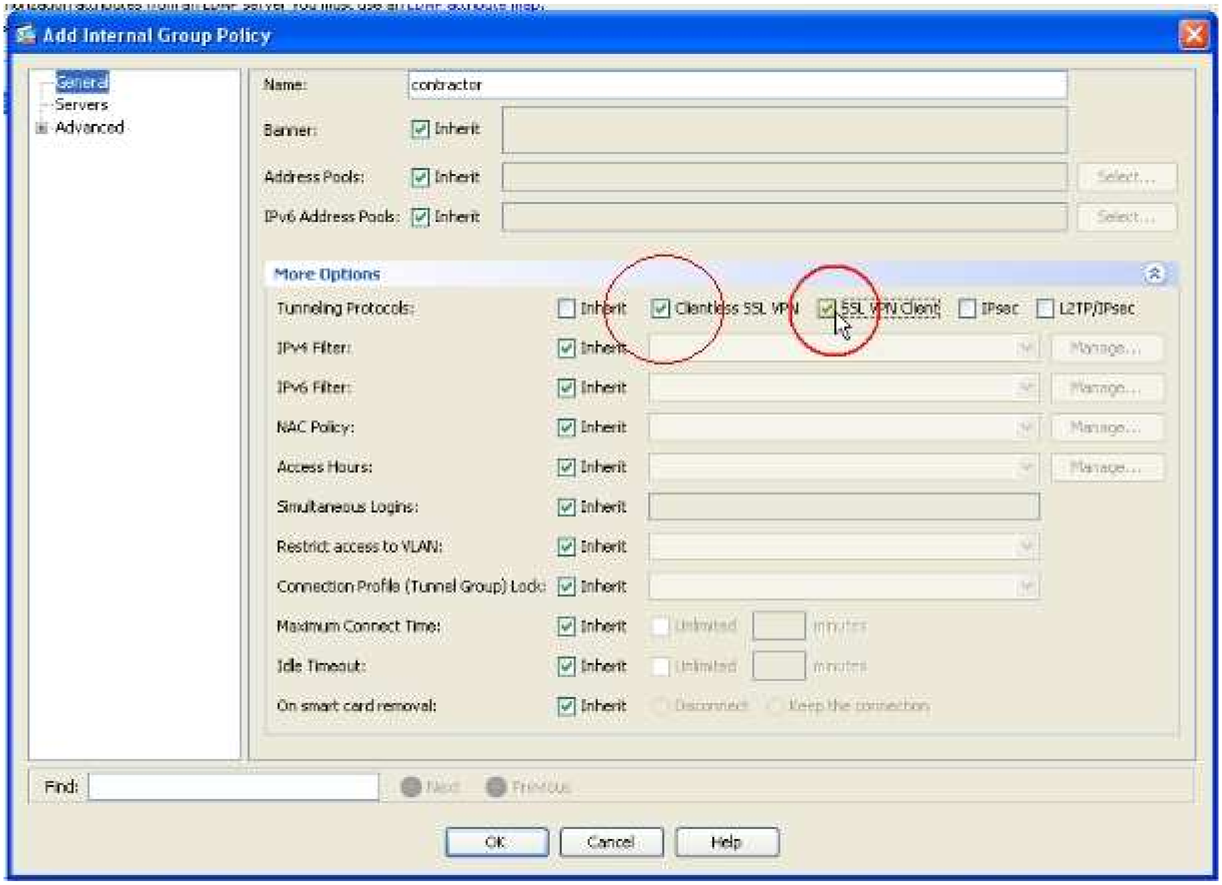
Name	SSL Enabled	IPsec Enabled	Aliases
DefaultRAGroup	✓		
DefaultWEBVPNGroup	✓		
employee	✓		employe
contractor	✓	✓	contract
engineering			
new_hire	✓		new_hir
management			

Res

A. Cisco Any Connect VPN
B. Clientless VPN
C. Cisco Any Connect VPN and clientless VPN
D. Cisco Any Connect VPN, clientless VPN, and IPsec VPN

Correct Answer: C
Section: SIMLET
Explanation

Explanation/Reference:
Explanation: configuration > network client access > any connect connection profiles >connection profiles > edit for each profile > general > more options > tunneling protocol > see the check marks



Add Internal Group Policy

Name: contractor

Banner: ☑ Inherit

Address Pools: ☑ Inherit

IPv6 Address Pools: ☑ Inherit

More Options

Tunneling Protocols: □ Inherit ☑ Clientless SSL VPN ☑ SSL VPN Client □ IPsec □ L2TP/IPsec

IPv4 Filter: ☑ Inherit

IPv6 Filter: ☑ Inherit

NAC Policy: ☑ Inherit

Access Hours: ☑ Inherit

Simultaneous Logins: ☑ Inherit

Restrict access to VLAN: ☑ Inherit

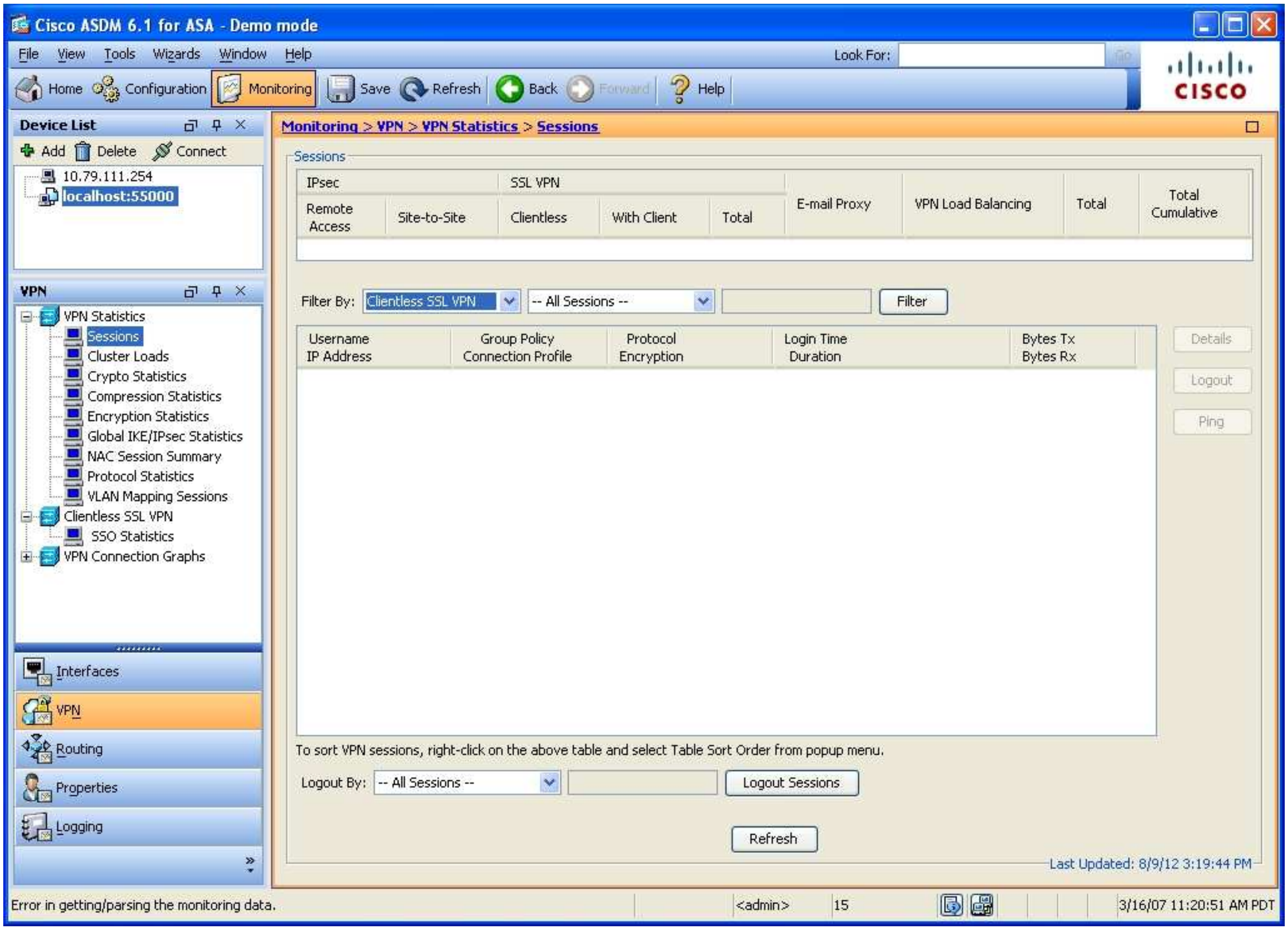
Connection Profile (Tunnel Group) Lock: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ Unlimited minutes

On smart card removal: ☑ Inherit ○ Disconnect ○ Keep the connection

Monitoring > VPN > VPN statistics > sessions filter by >>> choose contractor1



Monitoring > VPN > VPN Statistics > Sessions

Sessions

IPsec		SSL VPN			E-mail Proxy	VPN Load Balancing	Total	Total Cumulative
Remote Access	Site-to-Site	Clientless	With Client	Total				

Filter By: Clientless SSL VPN | -- All Sessions --

Username IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessions --

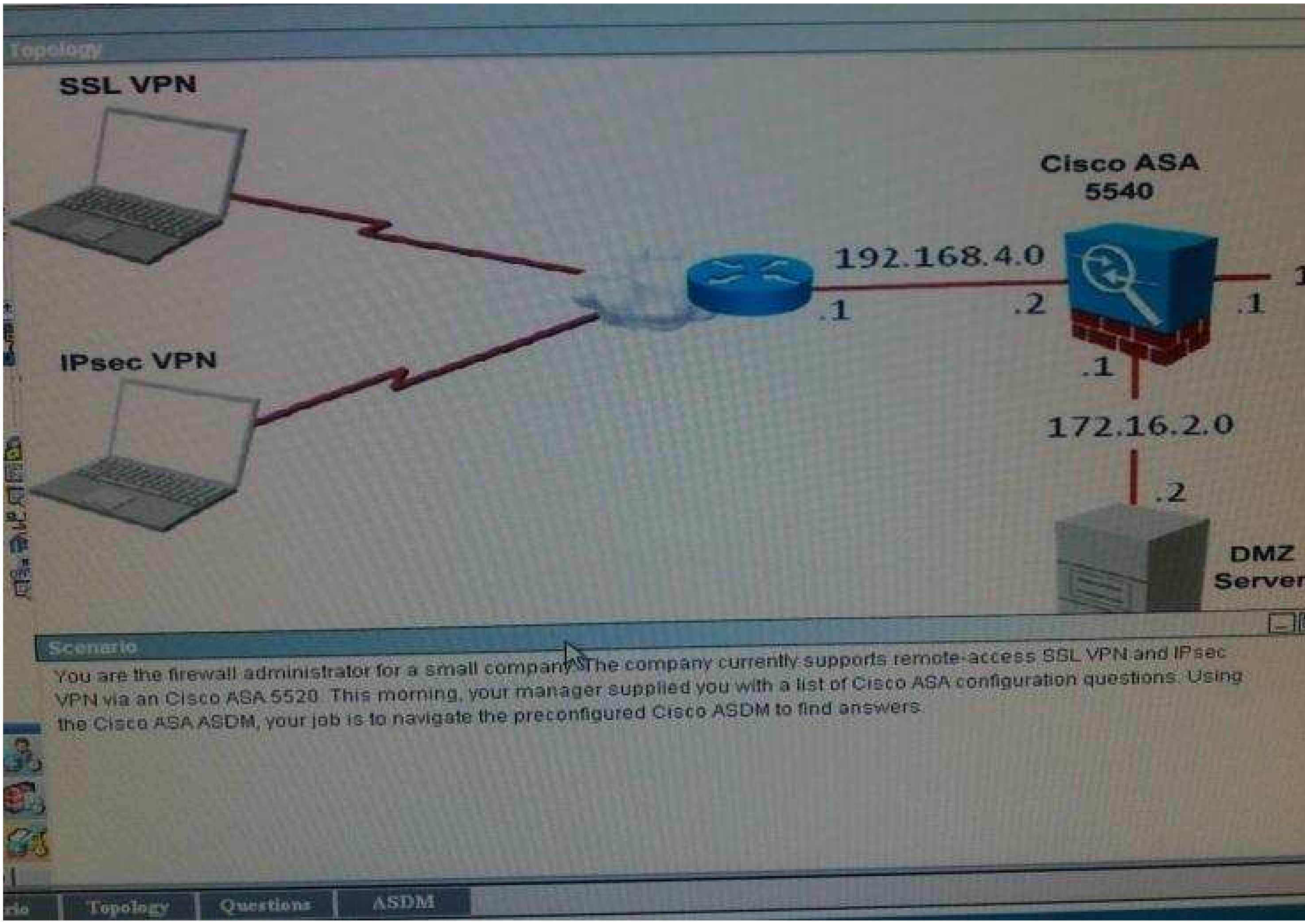
Last Updated: 8/9/12 3:19:44 PM

Error in getting/parsing the monitoring data. <admin> 15 3/16/07 11:20:51 AM PDT

QUESTION 17
Upon logging in, user, employee1, has two privileges: (Choose two)

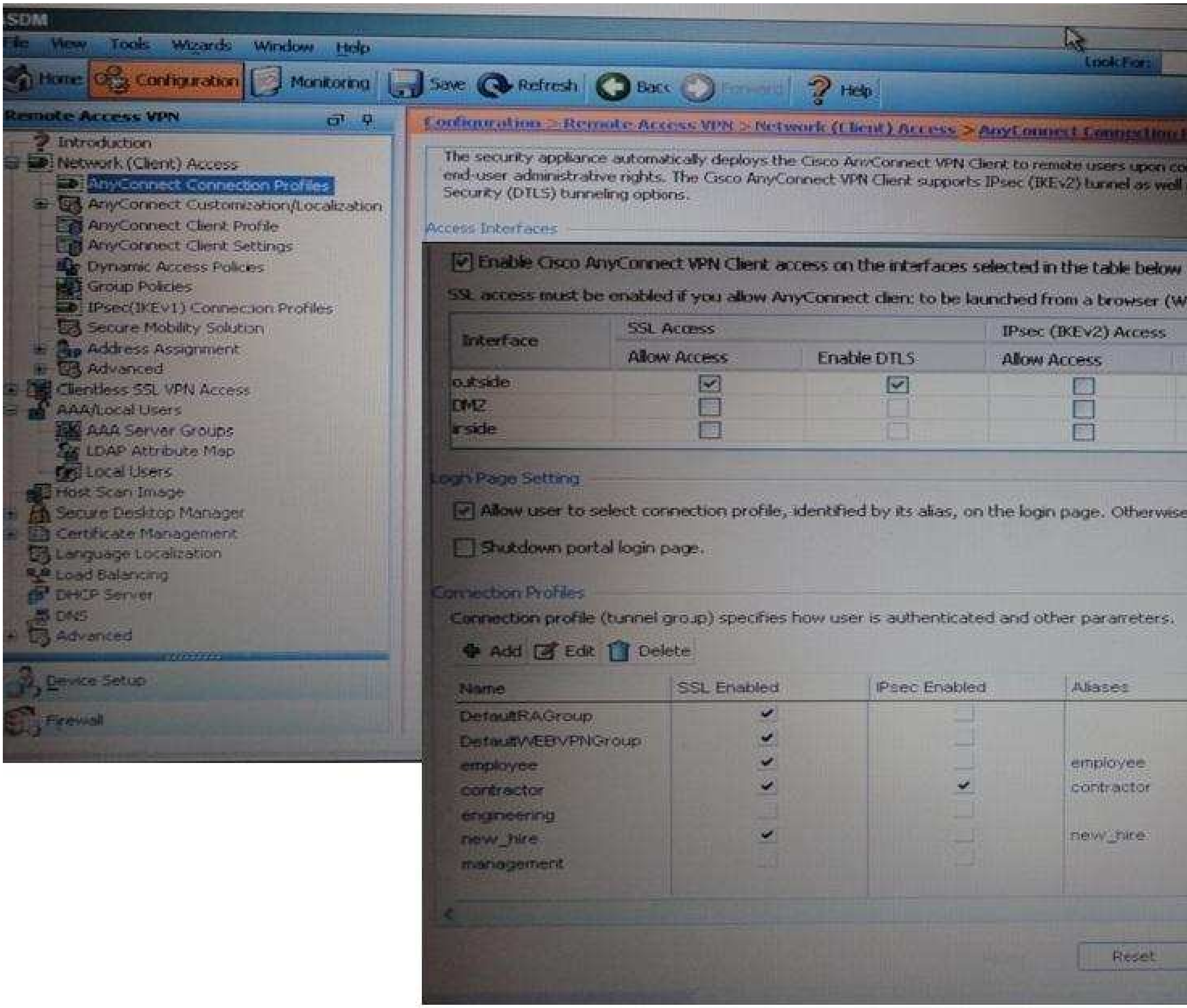
Case Study Title (Case Study):
Upon logging in, user, emploeyee1, has two privileges: (Choose two)

31-C (exhibit):



You are the firewall administrator for a small company. The company currently supports remote-access SSL VPN and IPsec VPN via an Cisco ASA 5520. This morning, your manager supplied you with a list of Cisco ASA configuration questions. Using the Cisco ASA ASDM, your job is to navigate the preconfigured Cisco ASDM to find answers.

31-D (exhibit):



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon co end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well Security (DTLS) tunneling options.

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (W

Interface	SSL Access		IPsec (IKEv2) Access
	Allow Access	Enable DTLS	Allow Access
outside	☑	☑	□
DMZ	□	□	□
inside	□	□	□

Login Page Setting

☑ Allow user to select connection profile, identified by its alias, on the login page. Otherwise

□ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters.

Name	SSL Enabled	IPsec Enabled	Aliases
DefaultRAGroup	✓	□	
DefaultWEBVPNGroup	✓	□	
employee	✓	□	employee
contractor	✓	✓	contractor
engineering	□	□	
new_hire	✓	□	new_hire
management	□	□	

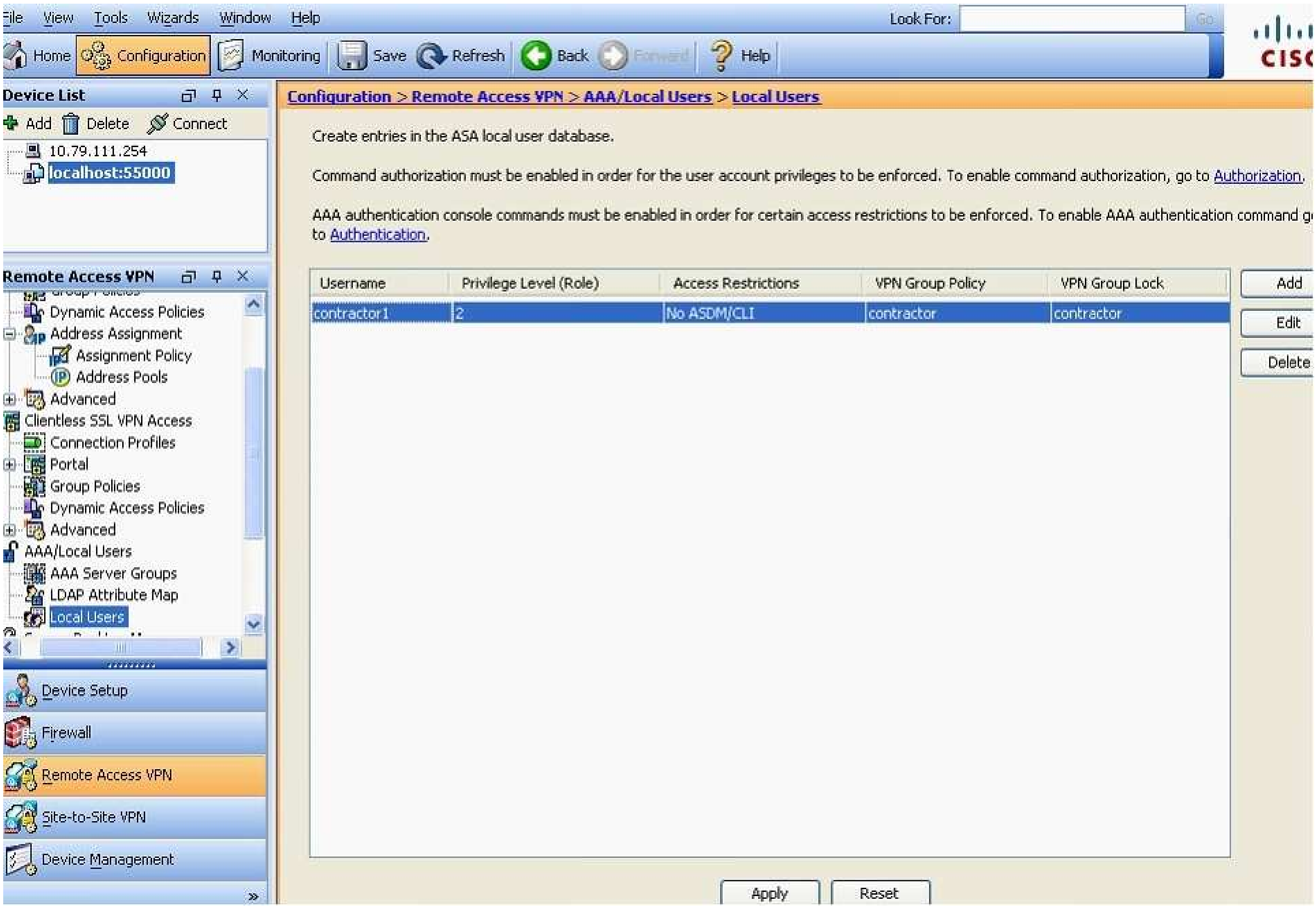
A. Cisco ASDM, SSH, Telnet, and console access
B. CLI login prompt for SSH, Telnet, and console only
C. No Cisco ASDM, SSH, or console access
D. Level 15
E. Level 2
F. Level 3

Correct Answer: DE
Section: SIMLET
Explanation

Explanation/Reference:
Command authorization
If you turn on command authorization using the local database, then the security appliance refers to the user privilege level to determine what commands are available. Otherwise, the privilege level is not generally used.

By default, all commands are either privilege level 0 or level 15. ASDM allows you to enable three predefined privilege levels, with commands assigned to level 15 (Admin), level 5 (Read Only), and level 3 (Monitor Only). If you use the predefined levels, then assign users to one of these three privilege levels.

This should show assigned levels for us:; on my demo version I could get the advanced tab to appear on aaa suthorization to setup other commands but this shows how I setup contractor1



Configuration > Remote Access VPN > AAA/Local Users > Local Users

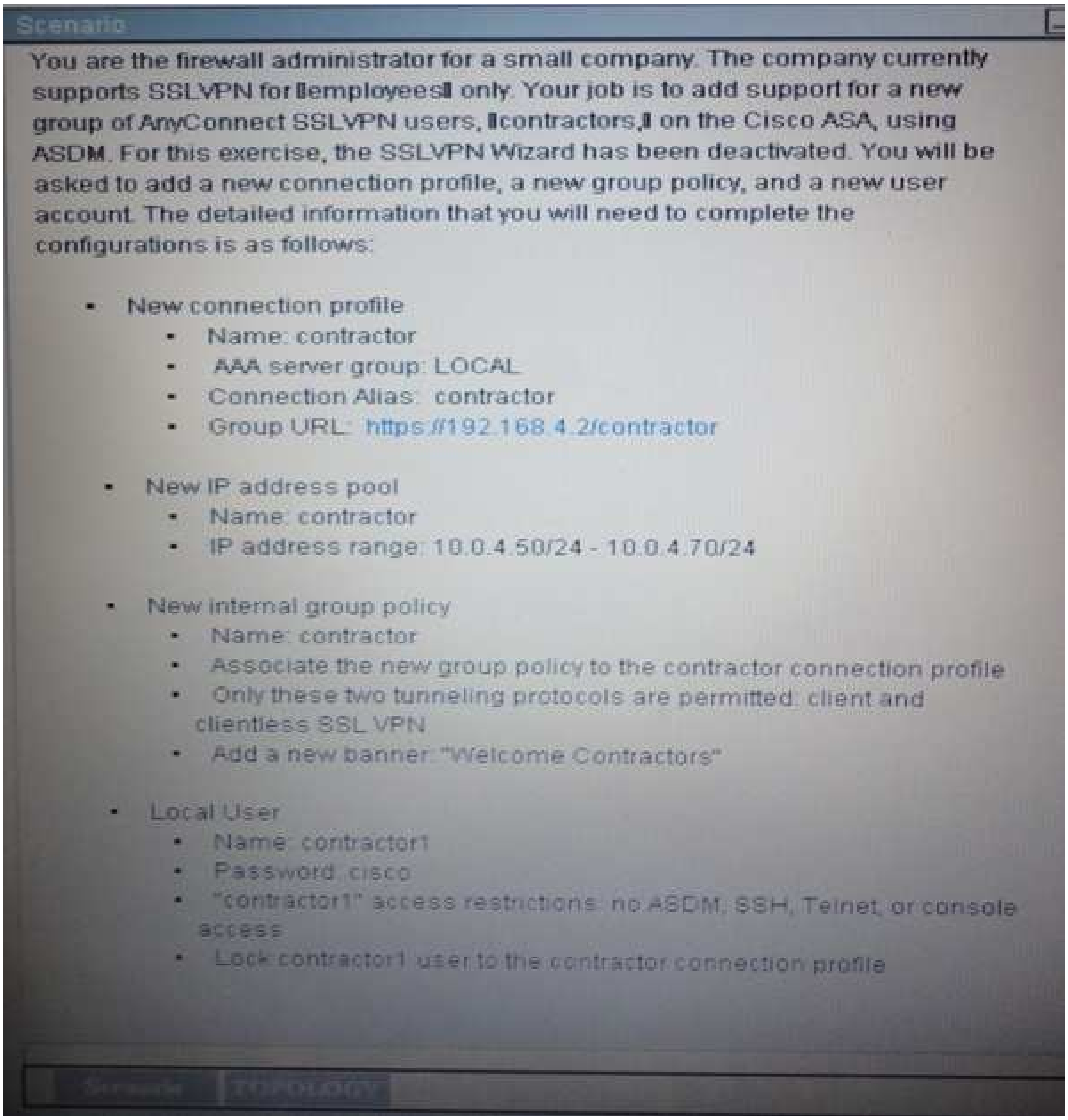
Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to Authorization.

AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command g to Authentication.

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock
contractor1	2	No ASDM/CLI	contractor	contractor

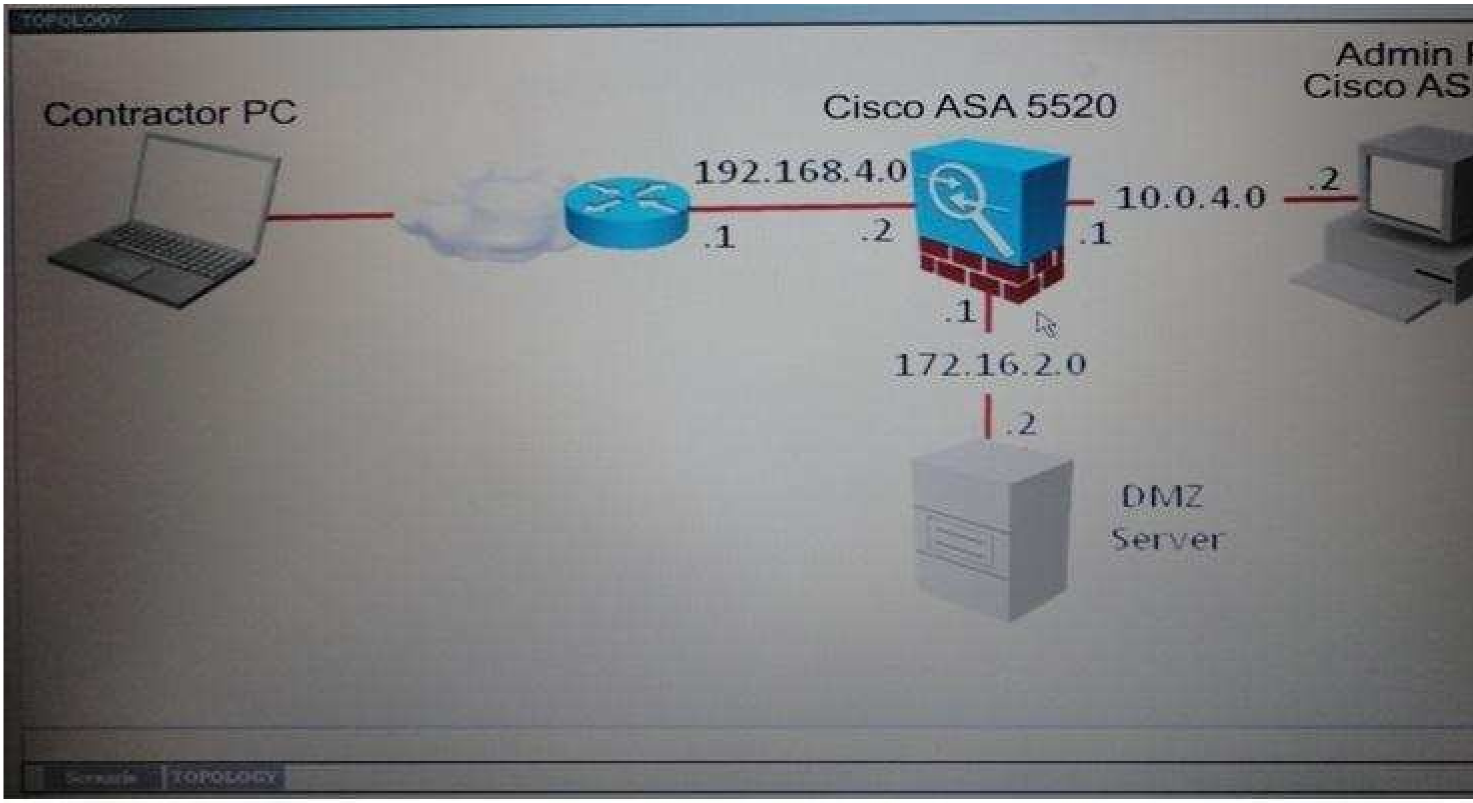
QUESTION 18



You are the firewall administrator for a small company. The company currently supports SSLVPN for ▮employees▮ only. Your job is to add support for a new group of AnyConnect SSLVPN users, ▮contractors,▮ on the Cisco ASA, using ASDM. For this exercise, the SSLVPN Wizard has been deactivated. You will be asked to add a new connection profile, a new group policy, and a new user account. The detailed information that you will need to complete the configurations is as follows:

- New connection profile
  - Name: contractor
  - AAA server group: LOCAL
  - Connection Alias: contractor
  - Group URL: https://192.168.4.2/contractor
- New IP address pool
  - Name: contractor
  - IP address range: 10.0.4.50/24 - 10.0.4.70/24
- New internal group policy
  - Name: contractor
  - Associate the new group policy to the contractor connection profile
  - Only these two tunneling protocols are permitted: client and clientless SSL VPN
  - Add a new banner: "Welcome Contractors"
- Local User
  - Name: contractor1
  - Password: cisco
  - "contractor1" access restrictions: no ASDM, SSH, Telnet, or console access
  - Lock contractor1 user to the contractor connection profile

Exhibit:

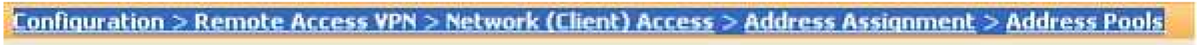


A.

Correct Answer: A
Section: Lab
Explanation

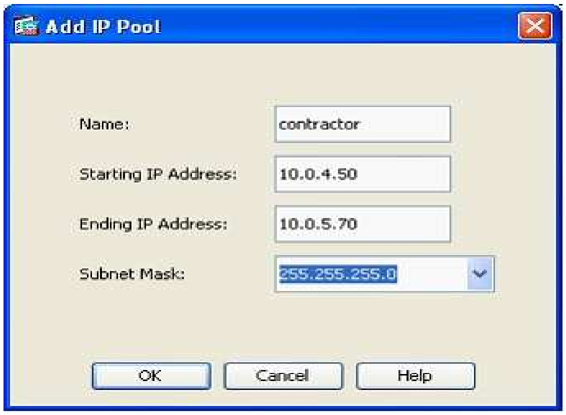
Explanation/Reference:
My revised answer:

Navigate to:



Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools

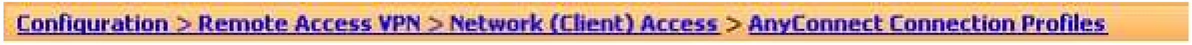
Address Pools :



Add IP Pool

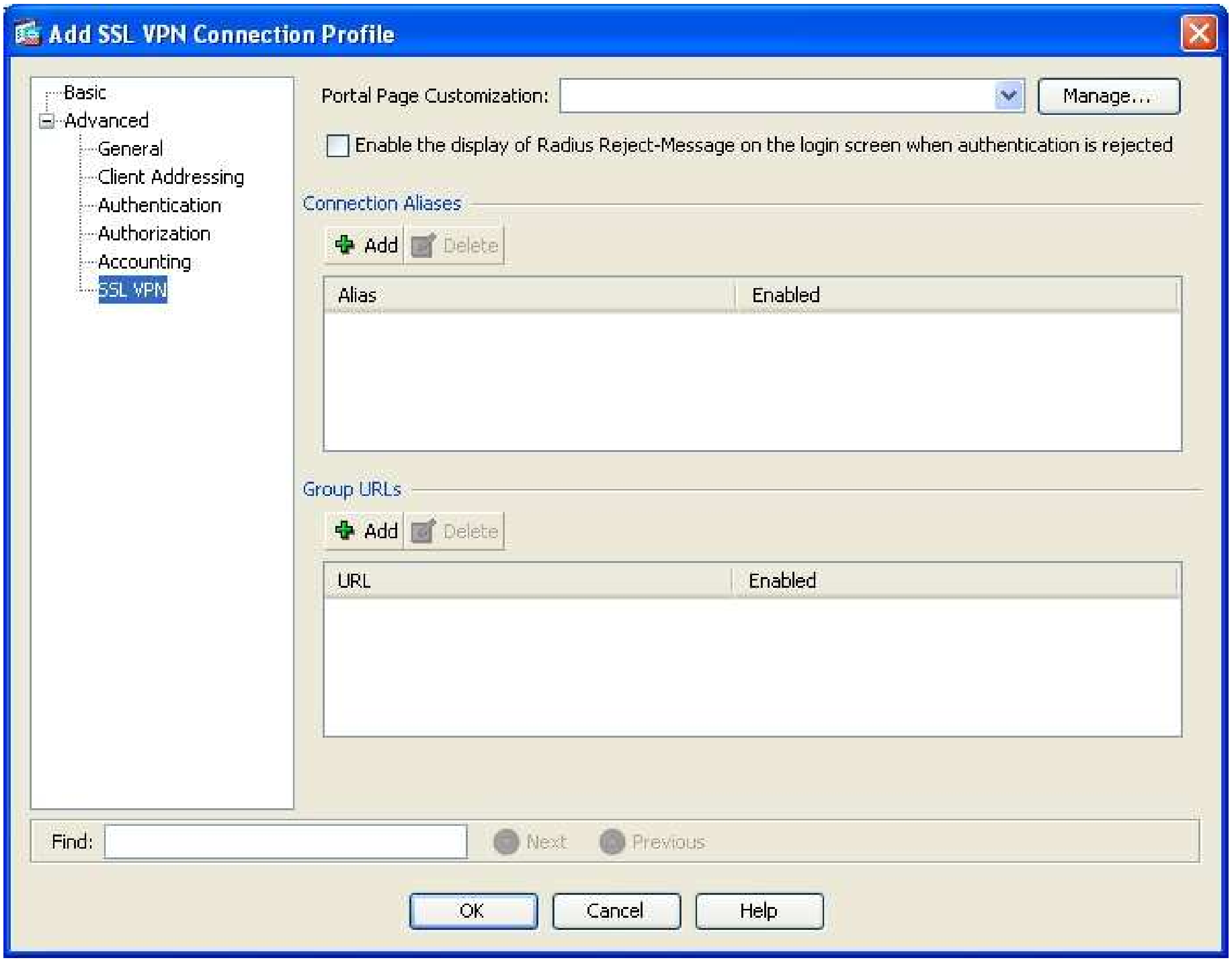
Name:	contractor
Starting IP Address:	10.0.4.50
Ending IP Address:	10.0.5.70
Subnet Mask:	255.255.255.0

Navigate to :

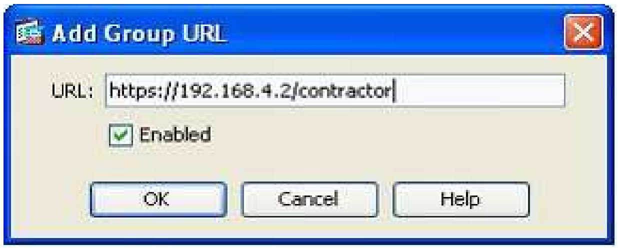


Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

Connection Profiles ADD



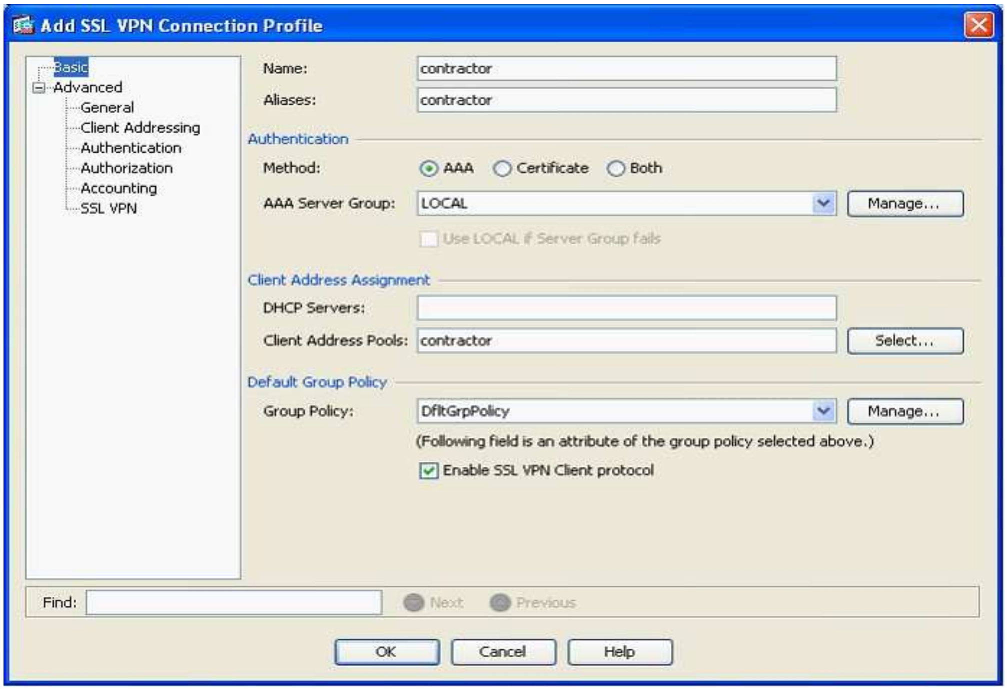
Advanced SSLVPN:



URL: https://192.168.4.2/contractor

☑ Enabled

Basic:



Add SSL VPN Connection Profile

Name: contractor

Aliases: contractor

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

Client Address Pools: contractor

Default Group Policy

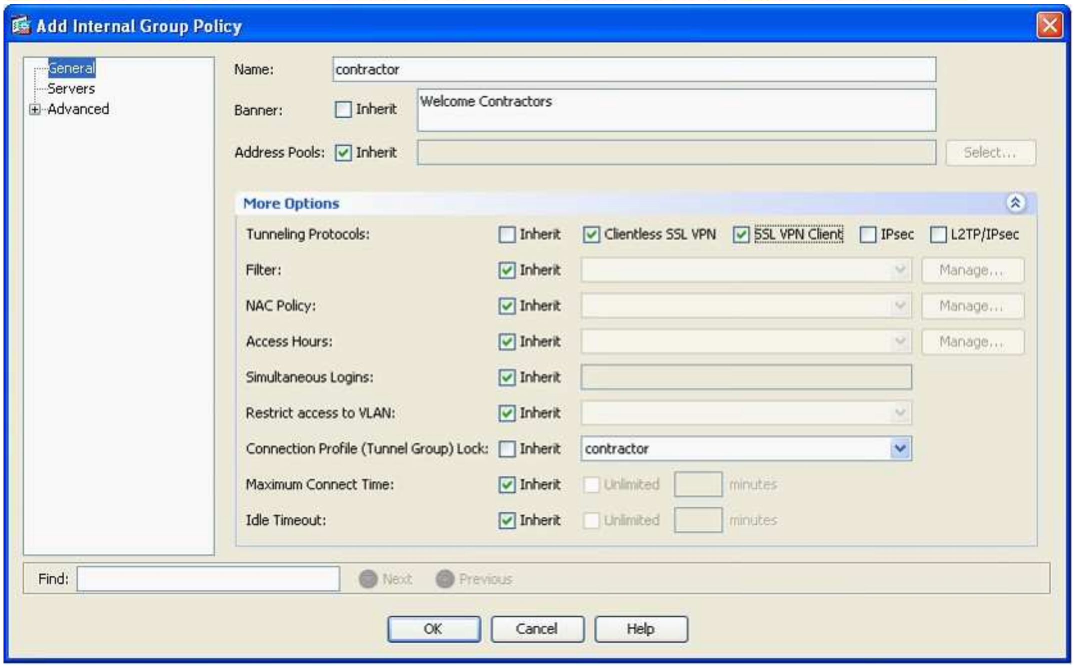
Group Policy: DfltGrpPolicy

(Following field is an attribute of the group policy selected above.)

☑ Enable SSL VPN Client protocol

Navigate to:

Configuration > Remote Access VPN > Network (Client) Access > Group Policies



Add Internal Group Policy

Name: contractor

Banner: □ Inherit Welcome Contractors

Address Pools: ☑ Inherit

More Options

Tunneling Protocols: □ Inherit ☑ Clientless SSL VPN ☑ SSL VPN Client □ IPsec □ L2TP/IPsec

Filter: ☑ Inherit

NAC Policy: ☑ Inherit

Access Hours: ☑ Inherit

Simultaneous Logins: ☑ Inherit

Restrict access to VLAN: ☑ Inherit

Connection Profile (Tunnel Group) Lock: □ Inherit contractor

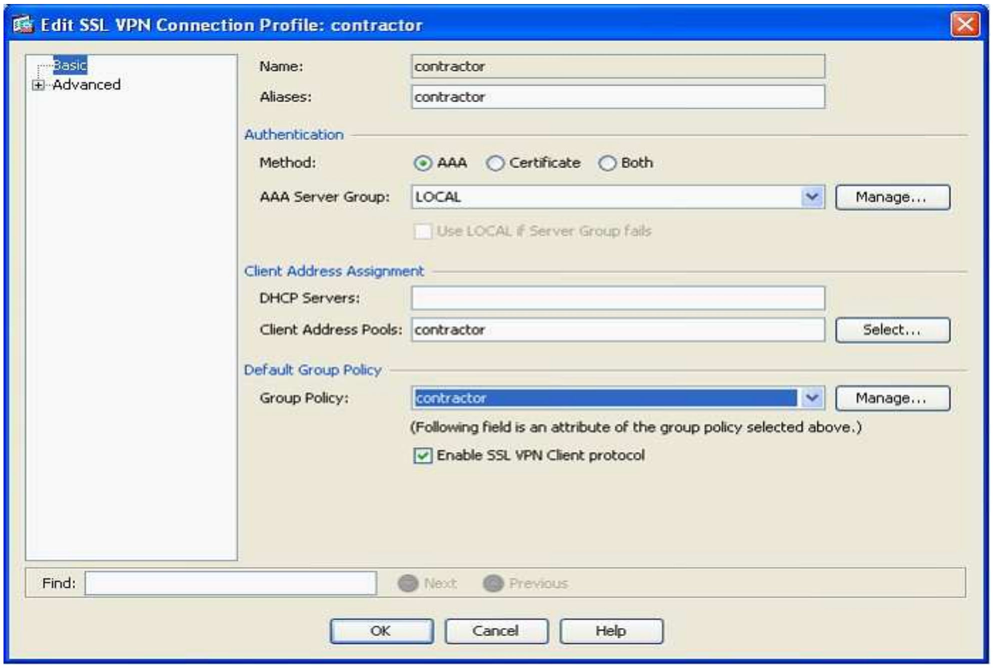
Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ Unlimited minutes

Navigate **back** to:

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

And **update** Default Group Policy



Edit SSL VPN Connection Profile: contractor

Basic
Advanced

Name: contractor
Aliases: contractor

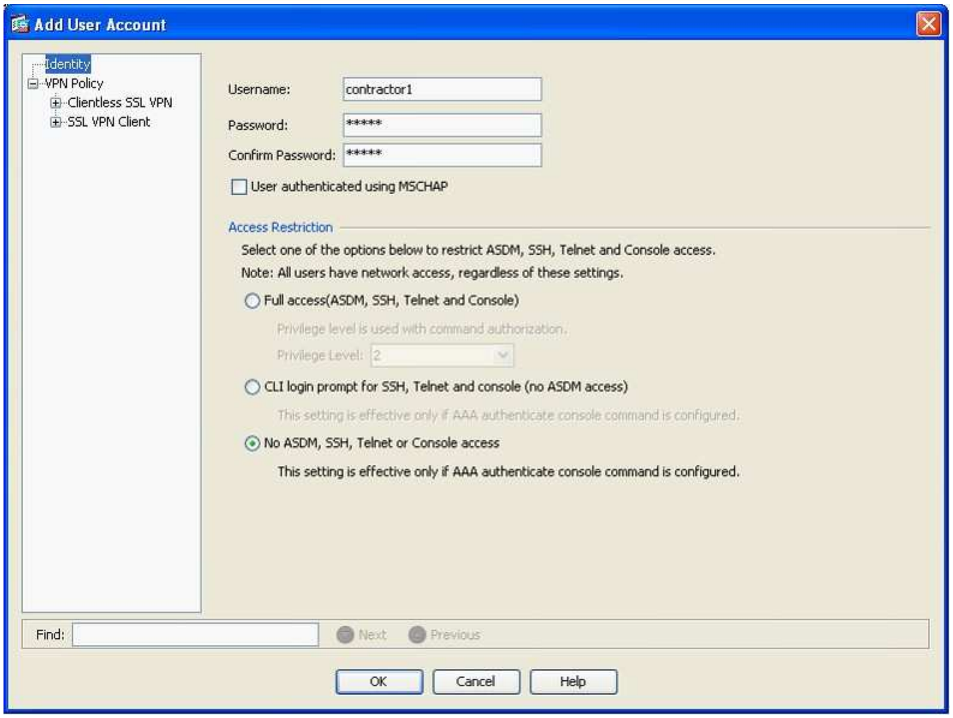
Authentication
Method: ● AAA ○ Certificate ○ Both
AAA Server Group: LOCAL
□ Use LOCAL if Server Group fails

Client Address Assignment
DHCP Servers:
Client Address Pools: contractor

Default Group Policy
Group Policy: contractor
(Following field is an attribute of the group policy selected above.)
☑ Enable SSL VPN Client protocol

Navigate to :

Configuration > Remote Access VPN > AAA/Local Users > Local Users



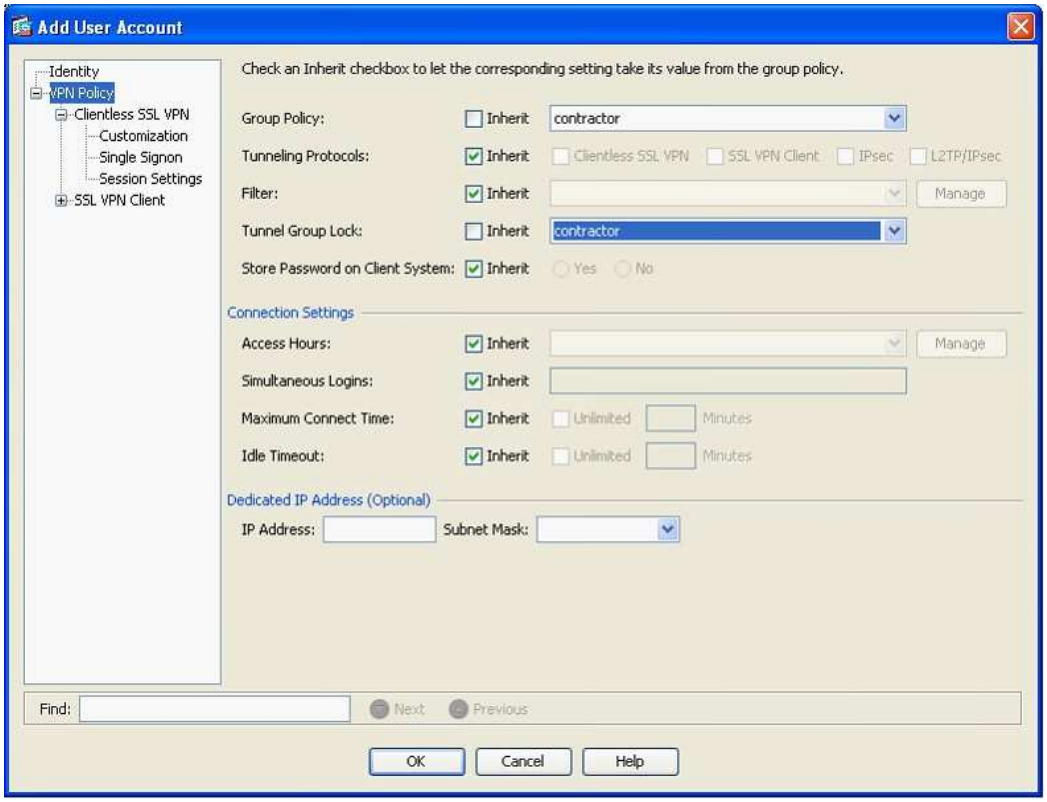
Add User Account

Identity
VPN Policy
Clientless SSL VPN
SSL VPN Client

Username: contractor1
Password: *****
Confirm Password: *****
□ User authenticated using MSCHAP

Access Restriction
Select one of the options below to restrict ASDM, SSH, Telnet and Console access.
Note: All users have network access, regardless of these settings.
○ Full access(ASDM, SSH, Telnet and Console)
Privilege level is used with command authorization.
Privilege Level: 2
○ CLI login prompt for SSH, Telnet and console (no ASDM access)
This setting is effective only if AAA authenticate console command is configured.
● No ASDM, SSH, Telnet or Console access
This setting is effective only if AAA authenticate console command is configured.

Then



Add User Account

- Identity
- VPN Policy
  - Clientless SSL VPN
    - Customization
    - Single Signon
    - Session Settings
  - SSL VPN Client

Check an Inherit checkbox to let the corresponding setting take its value from the group policy.

Group Policy: □ Inherit contractor

Tunneling Protocols: ☑ Inherit □ Clientless SSL VPN □ SSL VPN Client □ IPsec □ L2TP/IPsec

Filter: ☑ Inherit Manage

Tunnel Group Lock: □ Inherit contractor

Store Password on Client System: ☑ Inherit ○ Yes ○ No

Connection Settings

Access Hours: ☑ Inherit Manage

Simultaneous Logins: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited Minutes

Idle Timeout: ☑ Inherit □ Unlimited Minutes

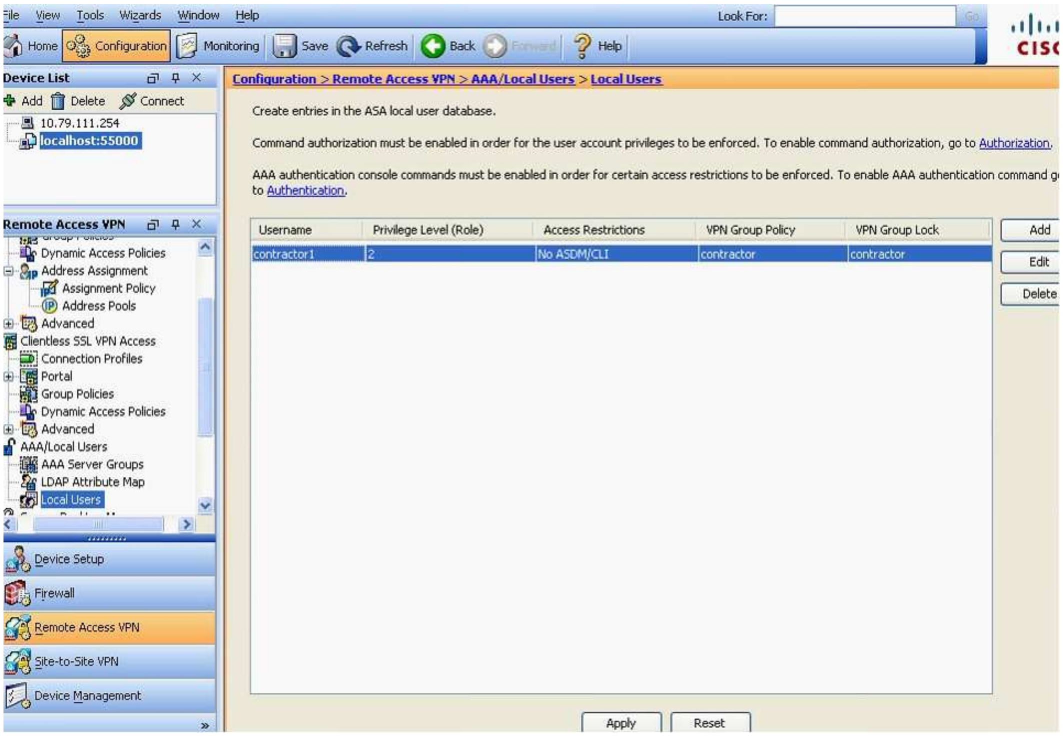
Dedicated IP Address (Optional)

IP Address: Subnet Mask:

Find: Next Previous

OK Cancel Help

And we have:



Configuration > Remote Access VPN > AAA/Local Users > Local Users

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to Authorization.

AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command g to Authentication.

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock
contractor1	2	No ASDM/CLI	contractor	contractor

Add Edit Delete

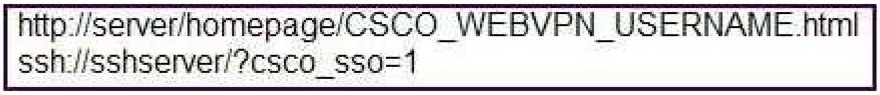
Apply Reset

OLD Answer: Here is the solution step by step below:

```
ip local pool contractor 10.1.4.50-10.1.4.70 mask 255.255.255.0
group-policy contractor internal
group-policy contractor attributes
vpn-tunnel-protocol ssl-clientless ssl-client
banner value Welcome Contractors
exit
tunnel-group contractor type remote-access
tunnel-group contractor general-attributes
default-group-policy contractors
address-pool contractor
tunnel-group contractors webvpn-attributes
group-alias contractor enable
group-url https://192.168.4.2/Contractor enable
username contractor1 password cisco privilege 2
username contractor1 attributes
service-type remote-access
vpn-group-policy contractors
exit
```

Exam D

QUESTION 1
Refer to the exhibit. Which two statements are correct regarding these two Cisco ASA clientless SSL VPN bookmarks? (Choose two.)



```
http://server/homepage/CSCO_WEBVPN_USERNAME.html
ssh://sshserver/?csco_sso=1
```

A. CSCO_WEBVPN_USERNAME is a user attribute.
B. CSCO_WEBVPN_USERNAME is a Cisco predefined variable that is used for macro substitution.
C. The CSCO_WEBVPN_USERNAME variable is enabled by using the Post SSO plug-in.
D. CSCO_SSO is a Cisco predefined variable that is used for macro substitution.
E. The CSCO_SSO=1 parameter enables SSO for the SSH plug-in.
F. The CSCO_SSO variable is enabled by using the Post SSO plug-in.

Correct Answer: BE
Section: SSLVPN clientless
Explanation

Explanation/Reference:
http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html

Introduction to URL Variable Substitution:

Your configuration will most likely require personalized resources that contain the username and password, for example, in URL lists or in group URLs. URL variable substitution lets the remote user enter username and password credentials once, when initiating the session, then login automatically to internal resources such as Citrix, OWA, Sharepoint, and the internal portal.
Clientless SSL VPN supports the following macro substitutions:

CSCO_WEBVPN_USERNAME—User login name

CSCO_WEBVPN_PASSWORD—Obtained from user login password

CSCO_WEBVPN_INTERNAL_PASSWORD—Obtained from the Internal password field. You can use this field as Domain for Single Signon operations.

CSCO_WEBVPN_CONNECTION_PROFILE—User login group drop-down (tunnel group alias)

CSCO_WEBVPN_MACRO1—Set via Radius or LDAP vendor specific attribute

CSCO_WEBVPN_MACRO2—Set via Radius or LDAP vendor specific attribute

Each time the security appliance recognizes one of these strings in an end-user request, it replaces the string with the user-specific value before passing the request to a remote server.

For example, a URL list that contains the link: http://someserver/homepage/
CSCO_WEBVPN_USERNAME.html

is translated by the security appliance to the following links for SSL VPN USER1 and USER2:

http://someserver/homepage/USER1.html
http://someserver/homepage/USER2.html

QUESTION 2
A network architect designed a redundant site-to-site IPsec VPN. In this site-to-site IPsec VPN solution are two

standalone Cisco ASA appliances that are deployed at the headquarters office site. A site-to-site VPN tunnel is established between the remote office and online peer (192.168.4.1).
To enable the remote office devices to be advertised correctly at headquarters, select the three

Cisco ASA parameters and the ends in which they should be applied. R=remote end; H=headquarters end. (Choose three)

A. R-Configure Originate-Only
B. H-Configure Originate-Only
C. R-Configure Answer-Only
D. H-Configure Answer-Only
E. R-Enable RRI
F. H-Enable RRI

Correct Answer: AF
Section: IPsec
Explanation

Explanation/Reference:
http://secret-epedemiology-statistic.org.ua/1587052091/ch15lev1sec4.html

Connection Type
The Cisco ASA in the site-to-site tunnel can respond and initiate a VPN connection. This bidirectional default behavior can be changed to answer-only or originate-only mode. For example, if you want to limit the security Cisco ASA to just initiate IKE tunnels, you can set the connection type to originate-only. This way, if the remote VPN peer tries to initiate the connection, the local Cisco ASA will not honor the request. Similarly, if you want the security Cisco ASA to accept IKE tunnels only from the peer, then you can set the connection type to answer-only. The command syntax to set the connection type is

```
crypto map map-name seq-num set connection-type {answer-only | bidirectional |
```