642-648 Q&As

Deploying Cisco ASA VPN Solutions (VPN v2.0)

Pass Cisco 642-648 Exam with 100% Guarantee

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

https://www.certbus.com/642-648.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Refer to the exhibit.

A NOC engineer is in the process of entering information into the Create New VPN Connection Entry fields. Which statement correctly describes how to do this?

A. In the Connection Entry field, enter the name of the connection profile as it is specified on the Cisco ASA appliance.

B. In the Host field, enter the IP address of the remote client device.

C. In the Authentication tab, click the Group Authentication or Mutual Group Authentication radio button to enable symmetrical pre-shared key authentication.

D. In the Name field, enter the name of the connection profile as it is specified on the Cisco ASA appliance.

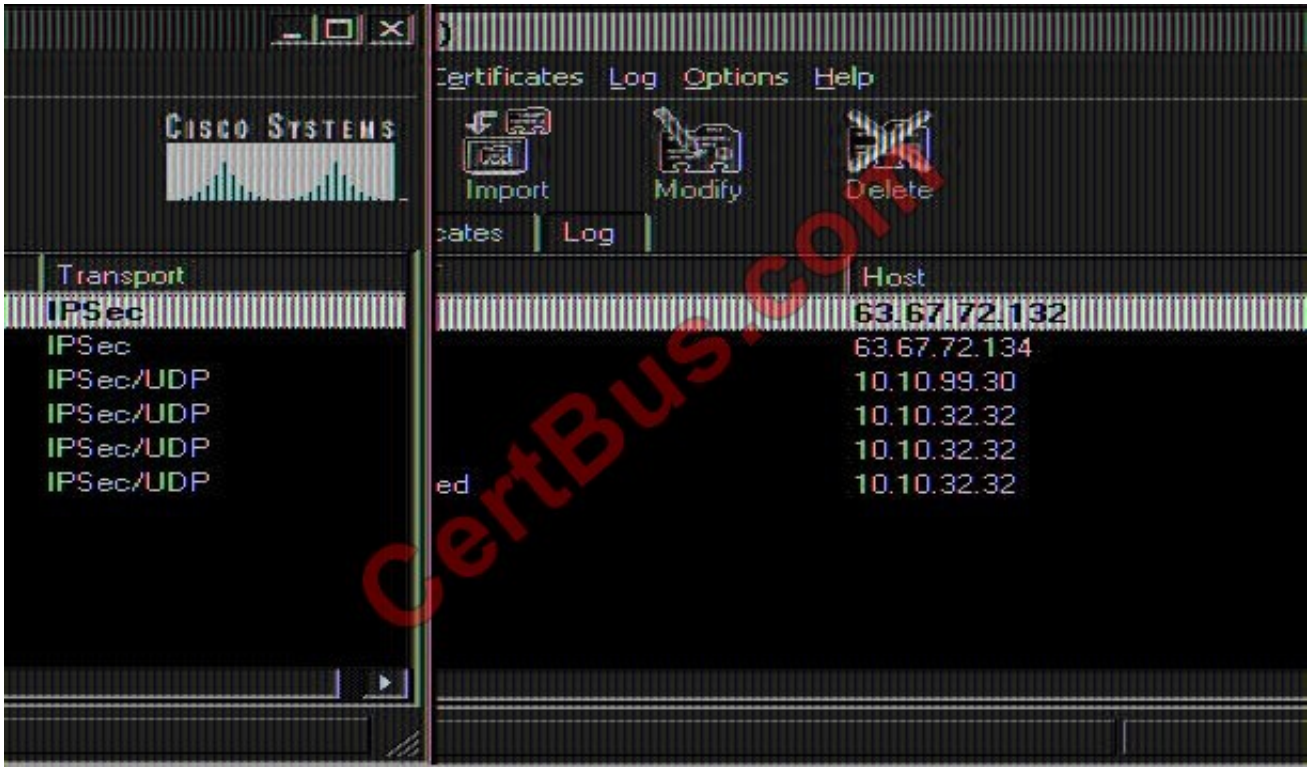
Correct Answer: D

http://www.cisco.com/en/US/docs/security/vpn_client/cisco_vpn_client/vpn_client46/win/user/guide/vc4.

html#wp1074766

Step 1 Start the VPN Client by choosing Start > Programs > Cisco Systems VPN Client > VPN Client.

Step 2 The VPN Client application starts and displays the advanced mode main window (Figure 4-1). If you are not already there, open the Options menu in simple mode and choose Advanced Mode or press Ctrl-M.



Step 3 Select New from the toolbar or the Connection Entries menu. The VPN Client displays a form

Step 4 Enter a unique name for this new connection. You can use any name to identify this connection; for example, Engineering. This name can contain spaces, and it is not case-sensitive. Step 5 Enter a description of this connection. This

field is optional, but it helps further identify this connection.

For example, Connection to Engineering remote server. Step 6 Enter the hostname or IP address of the remote VPN device you want to access.

Group Authentication

Your network administrator usually configures group authentication for you. If this is not the case, use the following procedure:

Step 1 Click the Group Authentication radio button.

Step 2 In the Name field, enter the name of the IPSec group to which you belong. This entry is case-sensitive.

Step 3 In the Password field, enter the password (which is also case-sensitive) for your IPSec group. The field displays only asterisks.

Step 4 Verify your password by entering it again in the Confirm Password field.

QUESTION 2

Cisco Secure Desktop seeks to minimize the risks that are posed by the use of remote devices in establishing a Cisco clientless SSL VPN or Cisco AnyConnect VPN Client session. Which two statements concerning the Cisco Secure Desktop Host Scan feature are correct? (Choose two.)

A. It is performed before a user establishes a connection to the Cisco ASA.

B. It is performed after a user establishes a connection to the Cisco ASA but before logging in.

C. It is performed after a user logs in but before a group profile is applied.

D. It is supported on endpoints that run a Windows operating system only.

E. It is supported on endpoints that run Windows and MAC operating systems only.

F. It is supported on endpoints that run Windows, MAC, and Linux operating systems.

Correct Answer: BF

DAP and Anti-Virus, Anti-Spyware, and Personal Firewall Programs The security appliance uses a DAP policy when the user attributes matches the configured AAA and endpoint attributes. The Pre login Assessment and Host Scan modules

of Cisco Secure Desktop return information to the security appliance about the configured endpoint attributes, and the DAP subsystem uses that information to select a DAP record that matches the values of those attributes. Most, but not all,

anti-virus, anti-spyware, and personal firewall programs support active scan, which means that the programs are memory-resident, and therefore always running. Host Scan checks to see if an endpoint has a program installed, and if it is

memory resident as follows:

?If the installed program does not support active scan, Host Scan reports the presence of the software. The DAP system selects DAP records that specify the program. ?If the installed program does support active scan, and active scan is

enabled for the program, Host Scan reports the presence of the software. Again the security appliance selects DAP records that specify the program.

?If the installed program does support active scan and active scan is disabled for the program, Host Scan ignores the presence of the software. The security appliance does not select DAP records that specify the program. Further, the output

of the debug trace command, which includes a lot of information about DAP, does not indicate the program presence, even though it is installed.

The following sequence outlines a typical remote access connection establishment.

1.

A remote client attempts a VPN connection.

2.

The security appliance performs posture assessment, using configured NAC and Cisco Secure Desktop Host Scan values.

Operating system support

?Microsoft Windows 2000, Windows XP, or Windows Vista ?Macintosh OS X 10.4.6

?Linux (Redhat RHEL 3.0 +, FEDORA 5, or FEDORA 6)

3.

The security appliance authenticates the user via AAA. The AAA server also returns authorization attributes for the user.

4.

The security appliance applies AAA authorization attributes to the session, and establishes the VPN tunnel.

5.

The security appliance selects DAP records based on the user AAA authorization information and the session posture assessment information. 6. The security appliance aggregates DAP attributes from the selected DAP records, and they

become the DAP policy.

7. The security appliance applies the DAP policy to the session.

QUESTION 3

In which three ways can a Cisco ASA security appliance obtain a certificate revocation list? (Choose three.)

A. FTP

B. SCEP

C. TFTP

D. HTTP

E. LDAP

F. SCP

Correct Answer: BDE

CRLs

CRLs provide the ASA with one way of determining whether a certificate that is within its valid time range has been revoked by the issuing CA. CRL configuration is part of configuration of a trustpoint.

You can configure the ASA to make CRL checks mandatory when authenticating a certificate by using the revocation-check crl command. You can also make the CRL check optional by using the revocation-check crl none command, which

allows the certificate authentication to succeed when the CA is unavailable to provide updated CRL data.

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

When the ASA has cached a CRL for longer than the amount of time it is configured to cache CRLs, the ASA considers the CRL too old to be reliable, or "stale." The ASA tries to retrieve a newer version of the CRL the next time that a

certificate authentication requires a check of the stale CRL.

The ASA caches CRLs for an amount of time determined by the following two factors:

?he number of minutes specified with the cache-time command. The default value is 60 minutes. ?he NextUpdate field in the CRLs retrieved, which may be absent from CRLs. You control whether the ASA requires and uses the NextUpdate

field with the enforcenextupdate command. The ASA uses these two factors in the following ways:

?f the NextUpdate field is not required, the ASA marks CRLs as stale after the length of time defined by the cache-time command.?f the NextUpdate field is required, the ASA 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 ASA marks CRLs as stale in 70 minutes.

QUESTION 4

Which statement regarding hashing is correct?

A. MD5 produces a 64-bit message digest.

B. SHA-1 produces a 160-bit message digest.

C. MD5 takes more CPU cycles to compute than SHA-1.

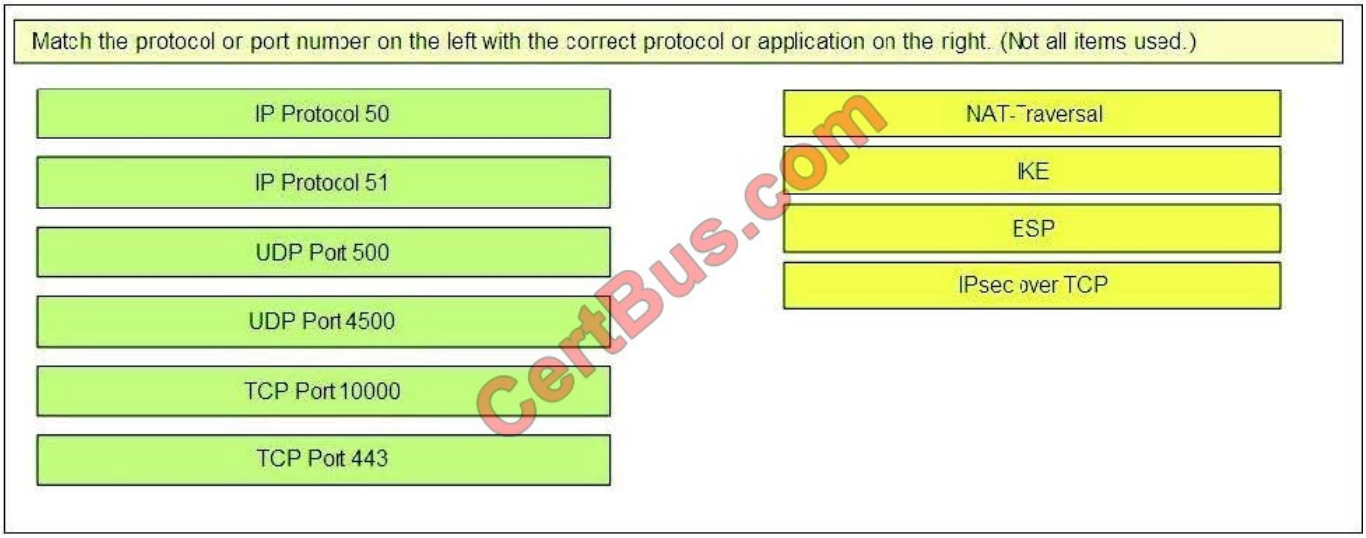
D. Changing 1 bit of the input to SHA-1 can change up to 5 bits in the output.

Correct Answer: B

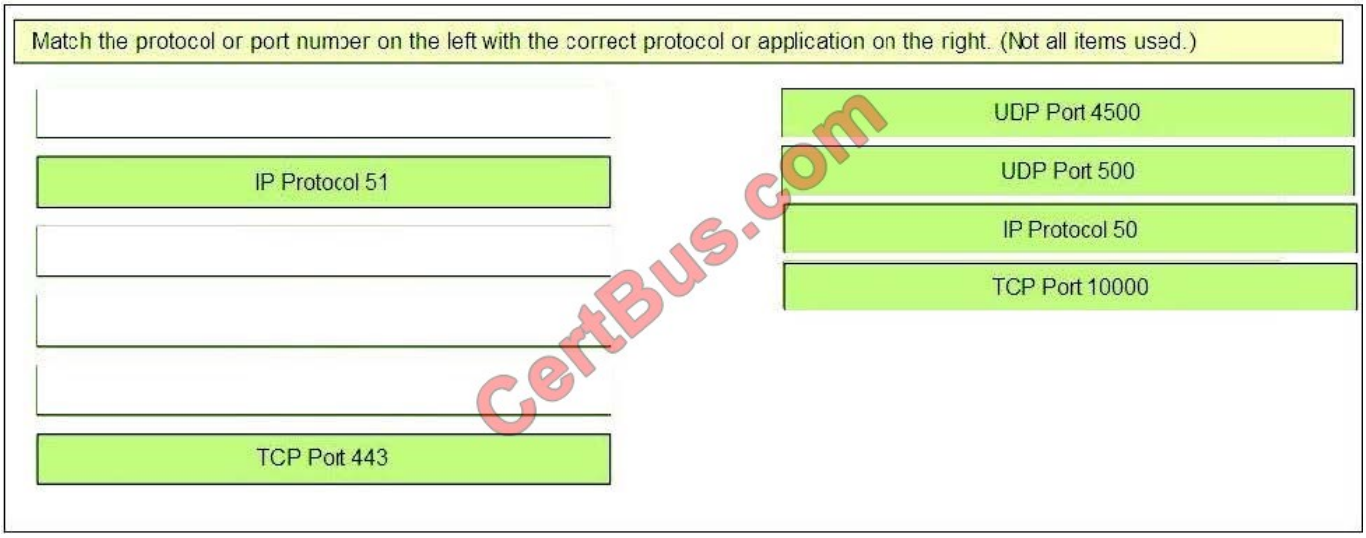
QUESTION 5

Match the protocol or port number on the left with the correct protocol or application on the right. (Not all items used.)

Select and Place:



Correct Answer:



QUESTION 6

An IT manager and a Security manager are discussing the deployment options for clientless SSL VPN. They are trying to decide which groups are best suited for this new deployment option. Which two groups are the best candidates for the clientless SSL VPN rollout? (Choose two.)

A. an IT administrator who needs to manage servers from a corporate laptop

B. employees who need occasional access to check their email accounts

C. a vendor who needs access to confidential corporate presentations via Secure FTP

D. customers who need interactive access to the corporate invoice server

Correct Answer: BC

QUESTION 7

When configuring dead peer detection for remote-access VPN, what does the confidence level parameter represent?

A. It specifies the number of seconds the adaptive security appliance should allow a peer to idle before beginning keepalive monitoring.

B. It specifies the number of seconds to wait between IKE keepalive retries.

C. The higher the number, the more reliable the link is.

D. It is determined dynamically based on reliability, uptime, and load.

Correct Answer: A

```
Chicago(config)# crypto map outside_map 10 set connection-type originate-only
```

ISAKMP Keepalives

The ISAKMP keepalives feature is a way to determine whether the remote VPN peer is still reachable or there are any lingering SAs (SAs that do not get cleared properly). By default, Cisco ASA starts sending Dead Peer Detection (DPD) packets after it stops receiving encrypted traffic over the tunnel from the peer. If it does not hear from its peer for 10 seconds (confidence interval), it sends out a DPD R_U_THERE packet. It keeps sending the R_U_THERE packets every 2 seconds (the retry interval). If it does not receive R_U_THERE_ACK for four consecutive DPDs polling periods, the security appliance deletes the corresponding ISAKMP and IPSec SAs.

QUESTION 8

Which three statements concerning keystroke logger detection are correct? (Choose three.)

A. It requires administrative privileges in order to run.

B. It runs on Windows and MAC OS X systems.

C. It detects loggers that run as a process or kernel module.

D. It detects both hardware- and software-based keystroke loggers.

E. It allows the administrator to define "safe" keystroke logger applications.

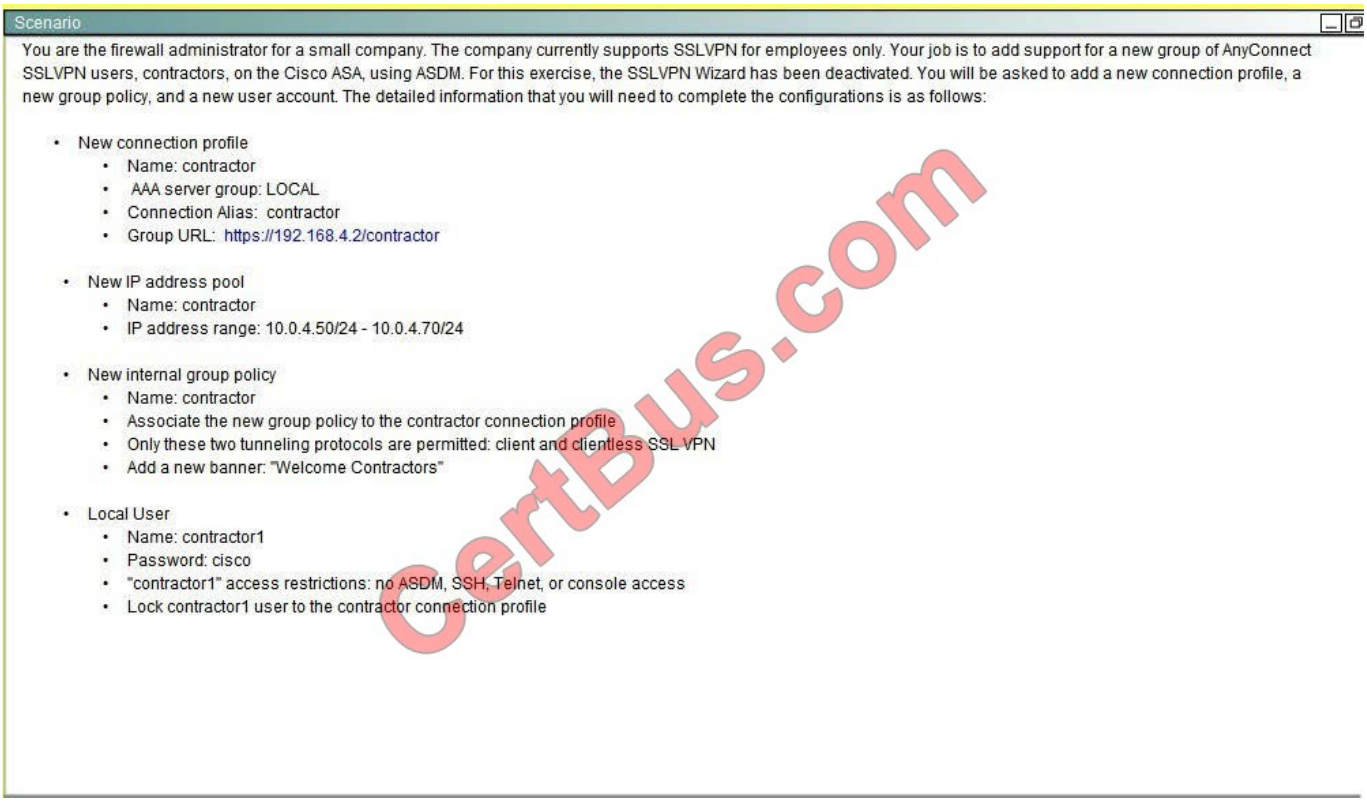
Correct Answer: ACE

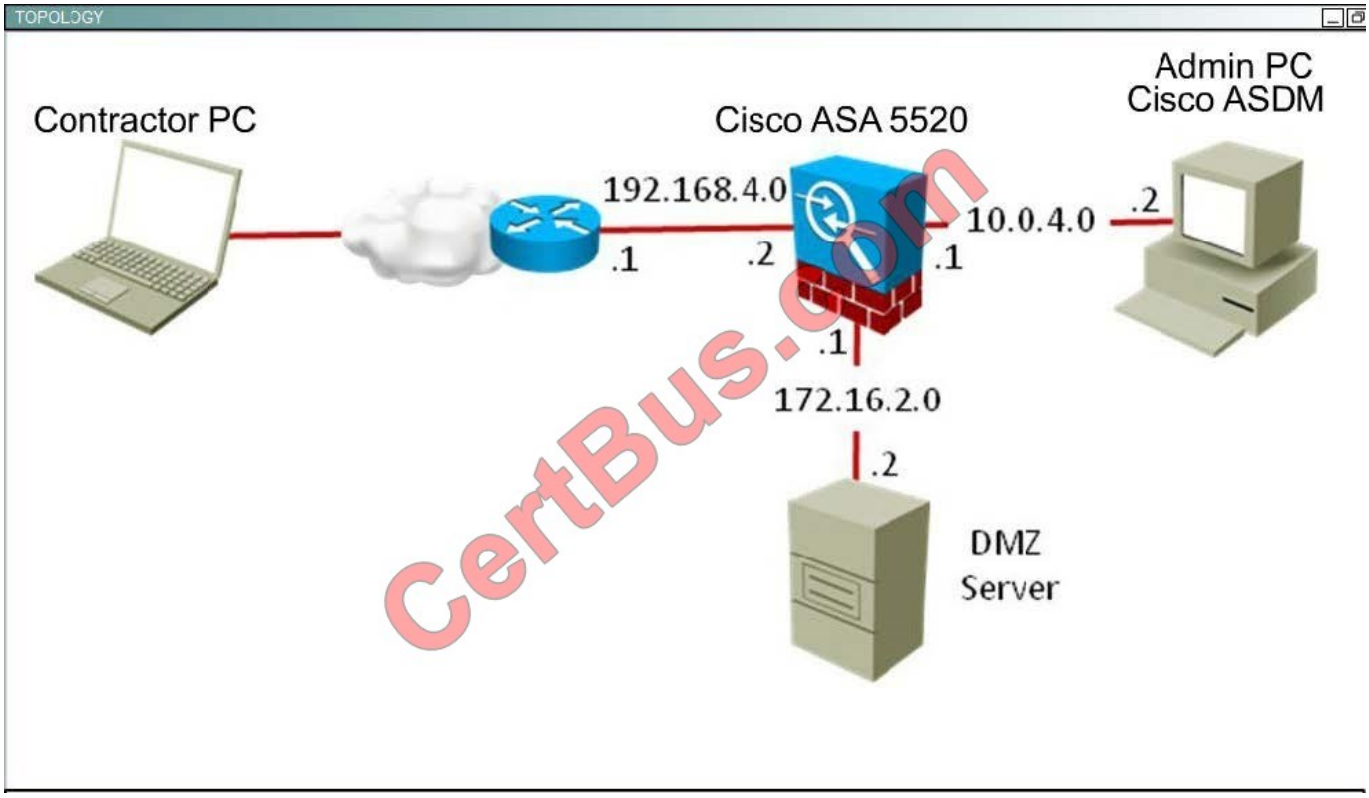
http://www.cisco.com/en/US/docs/security/csd/csd321/configuration/guide/CSDJfaq.html and
http://www.cisco.com/en/US/docs/security/csd/csd_32/configuration/guide/CSDJtuto.html

QUESTION 9

SIMULATION A. Please check the explanation

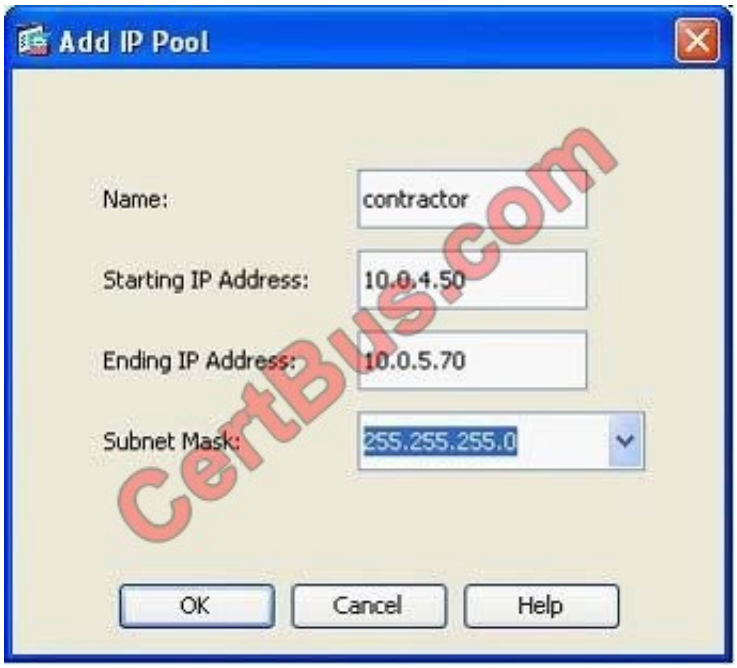
Correct Answer: A





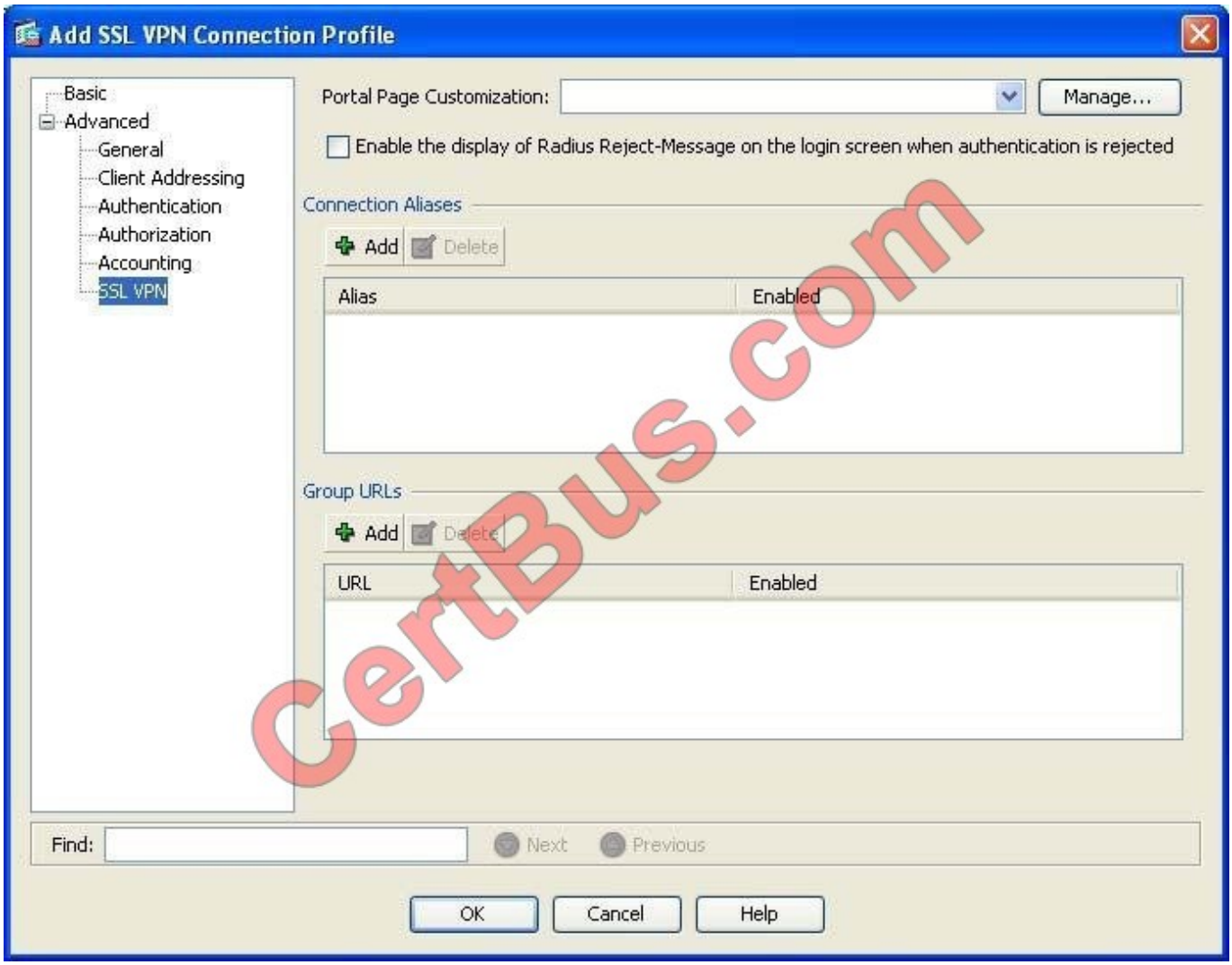
Explanation: Navigate to:

Address Pools:

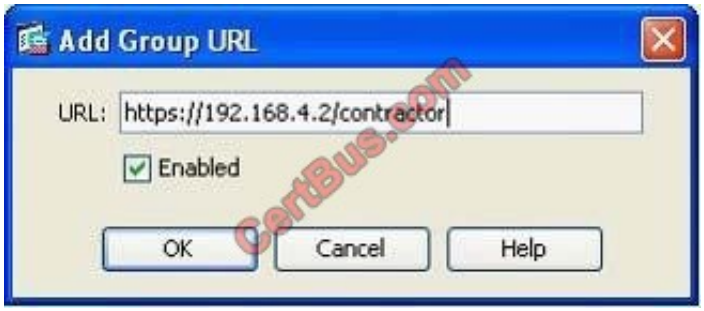


Navigate to:

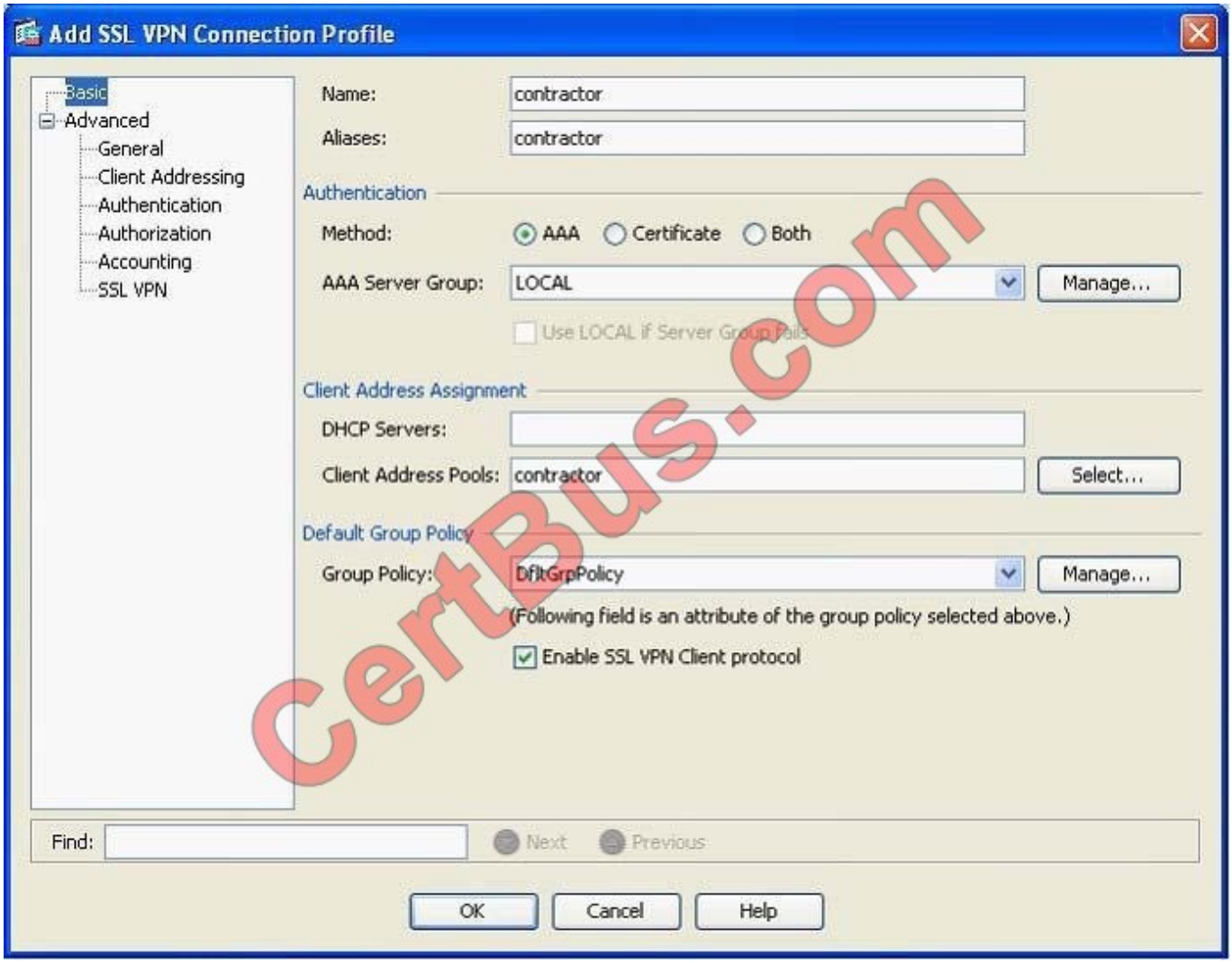
Connection Profiles ADD



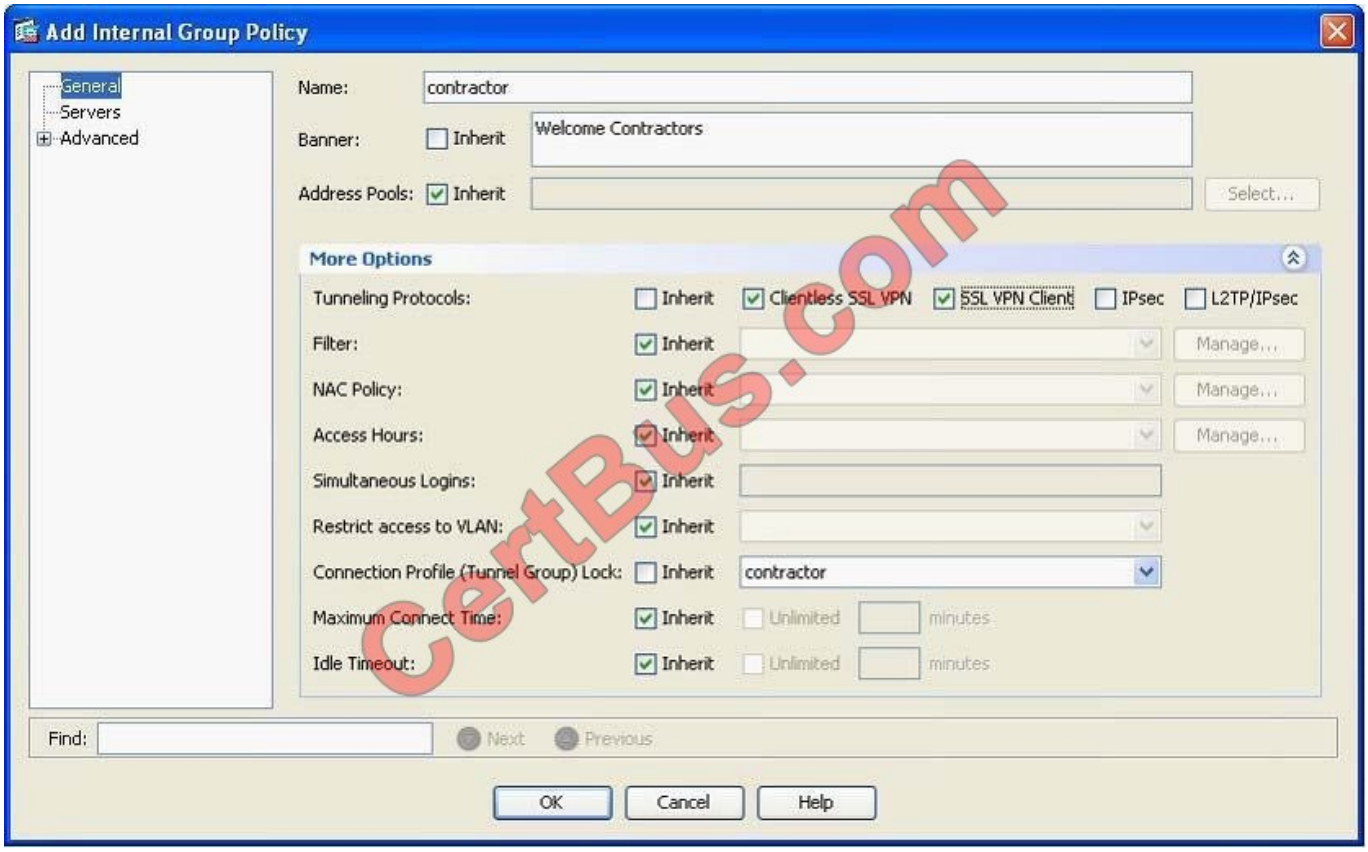
Advanced SSLVPN:



Basic: Navigate to:

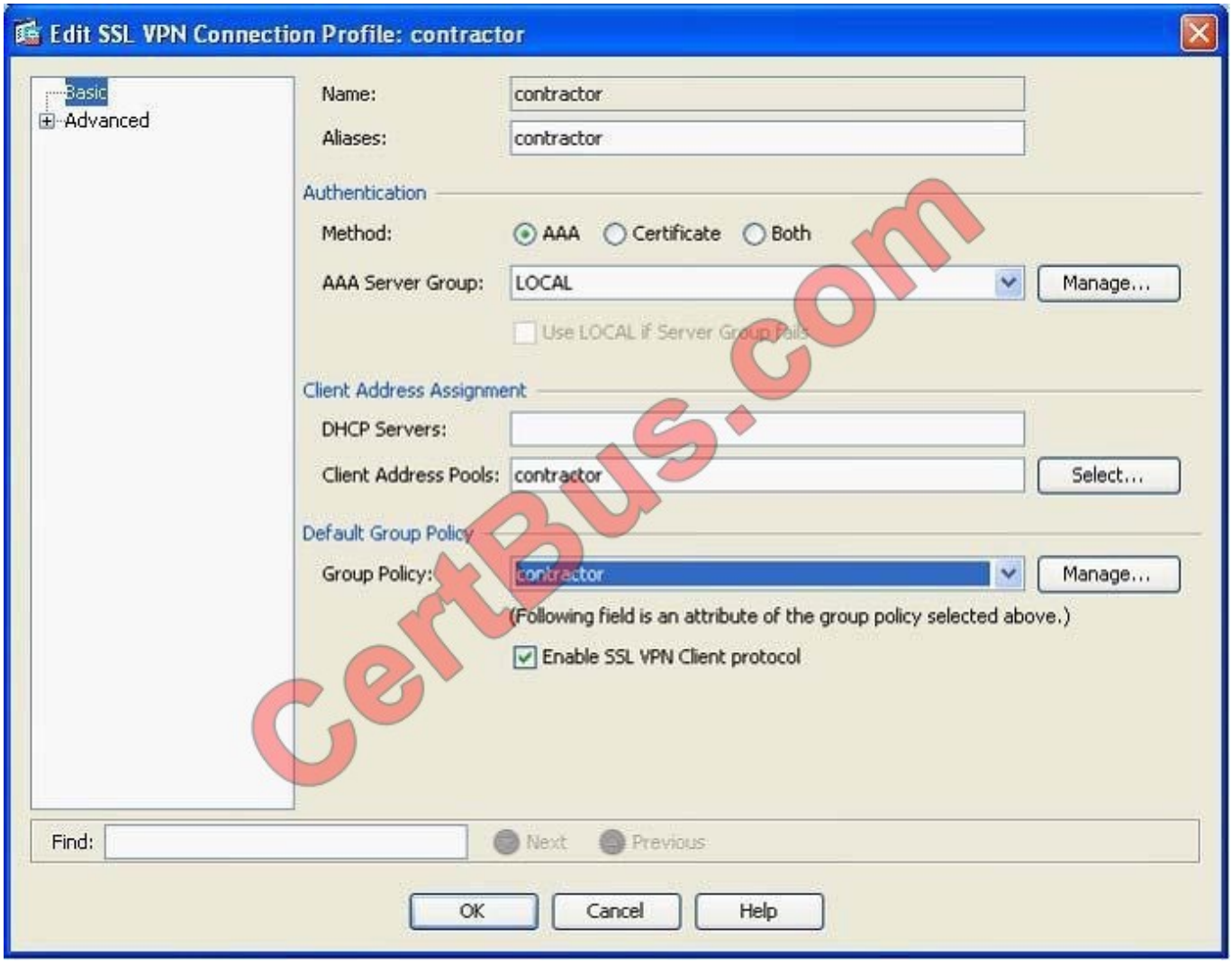

Add SSL VPN Connection Profile
Basic
Advanced
General
Client Addressing
Authentication
Authorization
Accounting
SSL VPN
Name:
contractor
Aliases:
contractor
Authentication
Method:
AAA
Certificate
Both
AAA Server Group:
LOCAL
Manage...
Use LOCAL if Server Group Fails
Client Address Assignment
DHCP Servers:
Client Address Pools:
contractor
Select...
Default Group Policy
Group Policy:
DfltGrpPolicy
Manage...
(Following field is an attribute of the group policy selected above.)
Enable SSL VPN Client protocol
Find:
Next
Previous
OK
Cancel
Help


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



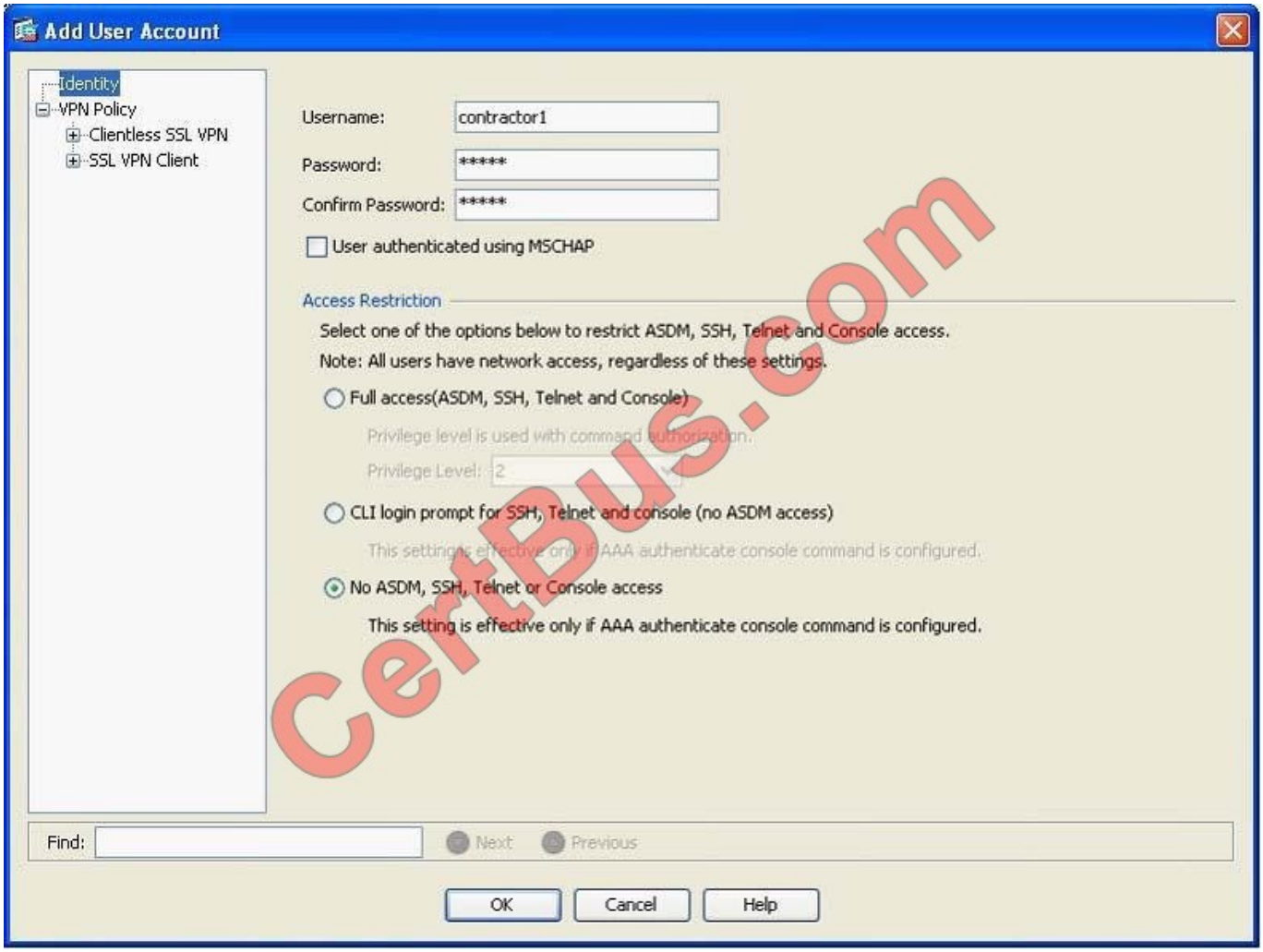
Navigate back to:

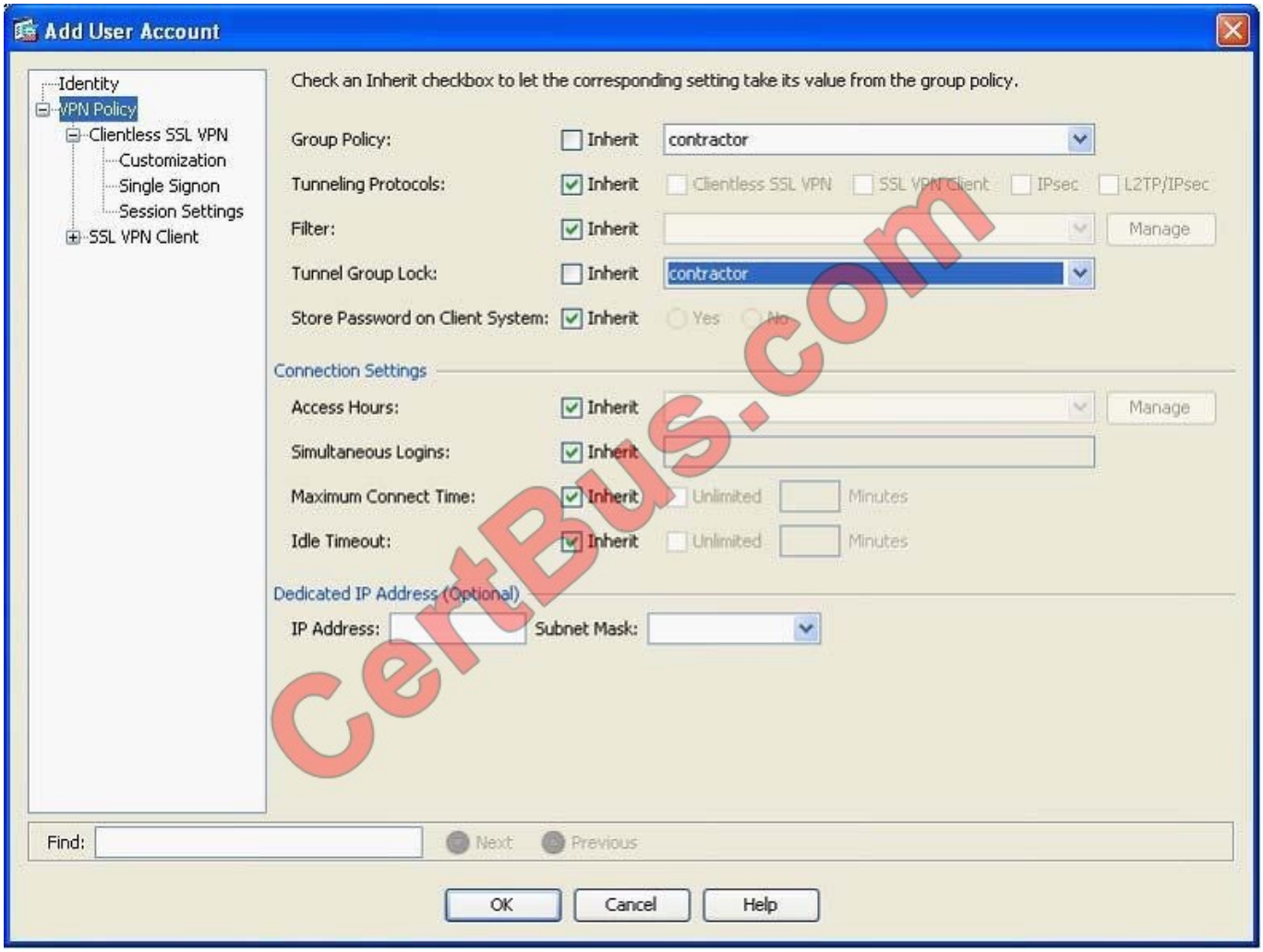
And update Default Group Policy



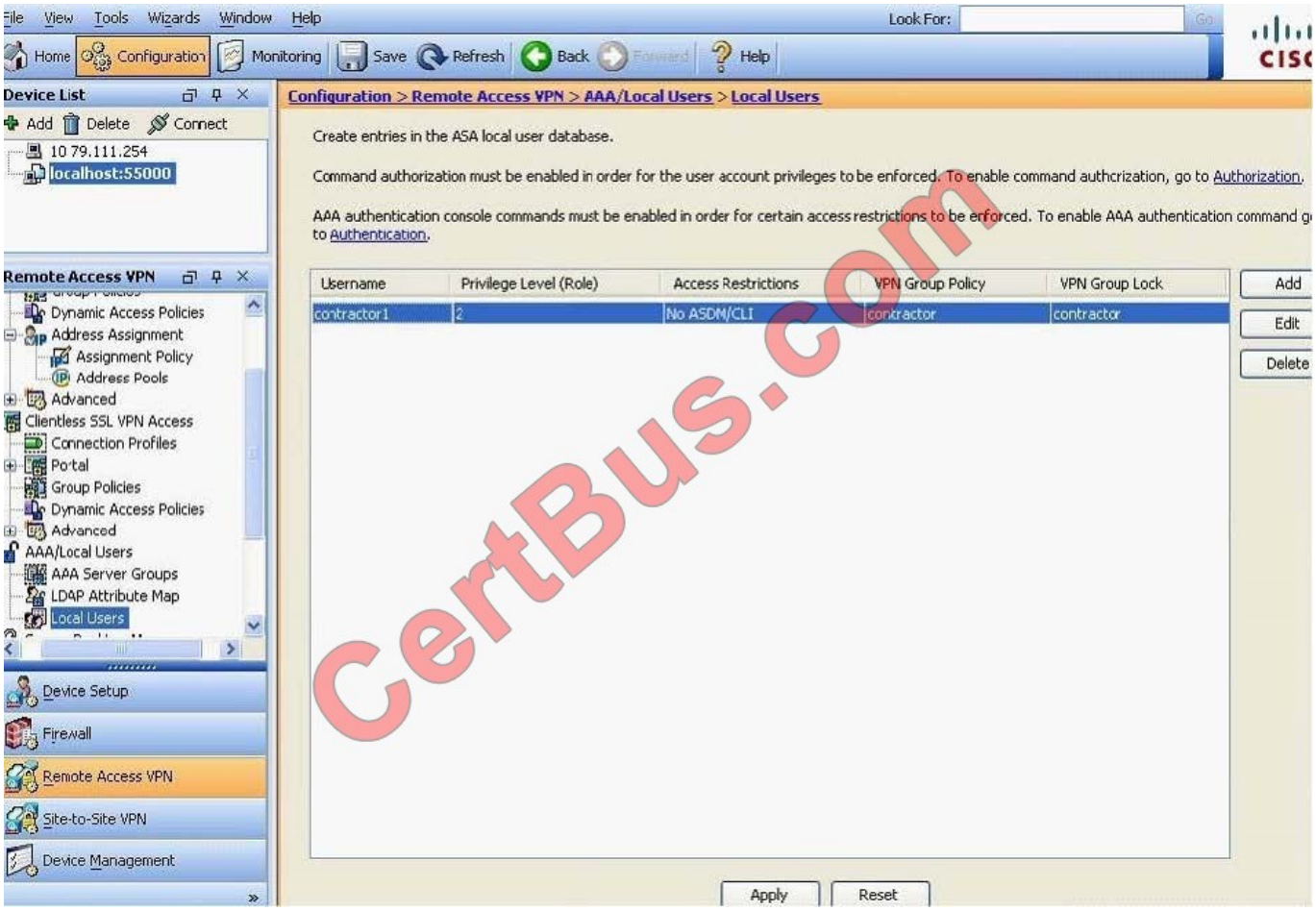
Navigate to: Then

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.
Find:
Next
Previous
OK
Cancel
Help



And we have:



QUESTION 10

Cisco AnyConnect profiles can be used to set which three options? (Choose three.)

A. Define a list of VPN gateways that are presented to users upon login.

B. Define a quarantine VLAN for remote devices that fail a host scan.

C. Define a guest VLAN to all "noncompany" Cisco IOS WebVPN users.

D. Define a list of backup servers if primary gateways are unavailable.

E. Activate the SSL VPN tunnel as part of the Windows login sequence.

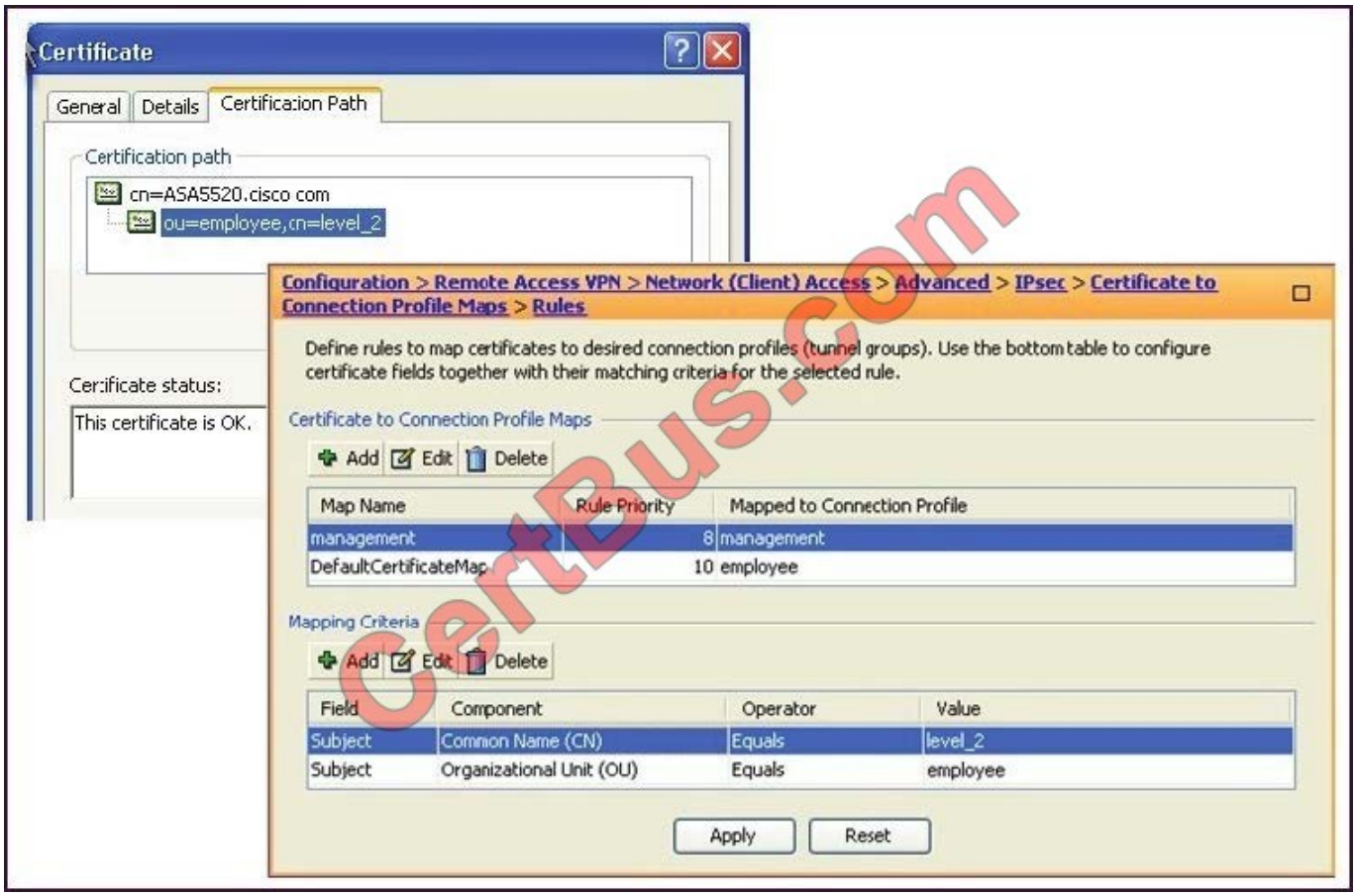
F. Configure the Cisco Secure Desktop vault.

Correct Answer: ADE

http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect20/administrative/guide/ad minapa.pdf

QUESTION 11

Refer to the exhibit.



The ABC Corporation is changing remote-user authentication from pre-shared keys to certificate-based authentication. For most employee authentication, its group membership (the employees) governs corporate access. Certain management personnel need access to more confidential servers. Access is based on the group and name, such as finance and level_2. When it is time to pilot the new authentication policy, a finance manager is able to access the department-assigned servers but cannot access the restricted servers.

As the network engineer, where would you look for the problem?

A. Check the validity of the identity and root certificate on the PC of the finance manager.

B. Change the Management Certificate to Connection Profile Maps > Rule Priority to a number that is greater than 10.

C. Check if the Management Certificate to Connection Profile Maps > Rules is configured correctly.

D. Check if the Certificate to Connection Profile Maps > Policy is set correctly.

Correct Answer: D

Cisco ASDM User Guide Version 6.1

QUESTION 12

You are the network security administrator. You receive a call from a user stating that he cannot log onto the network. In the process of troubleshooting, you determine that this user is accessing the network via certificate-based Cisco AnyConnect SSL VPN.

What is a troubleshooting step that you should perform to determine the cause of the access problem?

A. Revoke and reissue the certificate, and have the user try again.

B. Verify that a connection can be made without using certificates.

C. Ask the user to use IPsec, and test the connection attempts.

D. Check the WebACLs on the Cisco ASA.

Correct Answer: B

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.certbus.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: