



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.passapply.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.

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

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

- 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

QUESTION 2

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



PassApply.com

QUESTION 3

SIMULATION A. Please check the explanation

Correct Answer: A



Scenario

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

TOPOLOGY



Explanation: 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

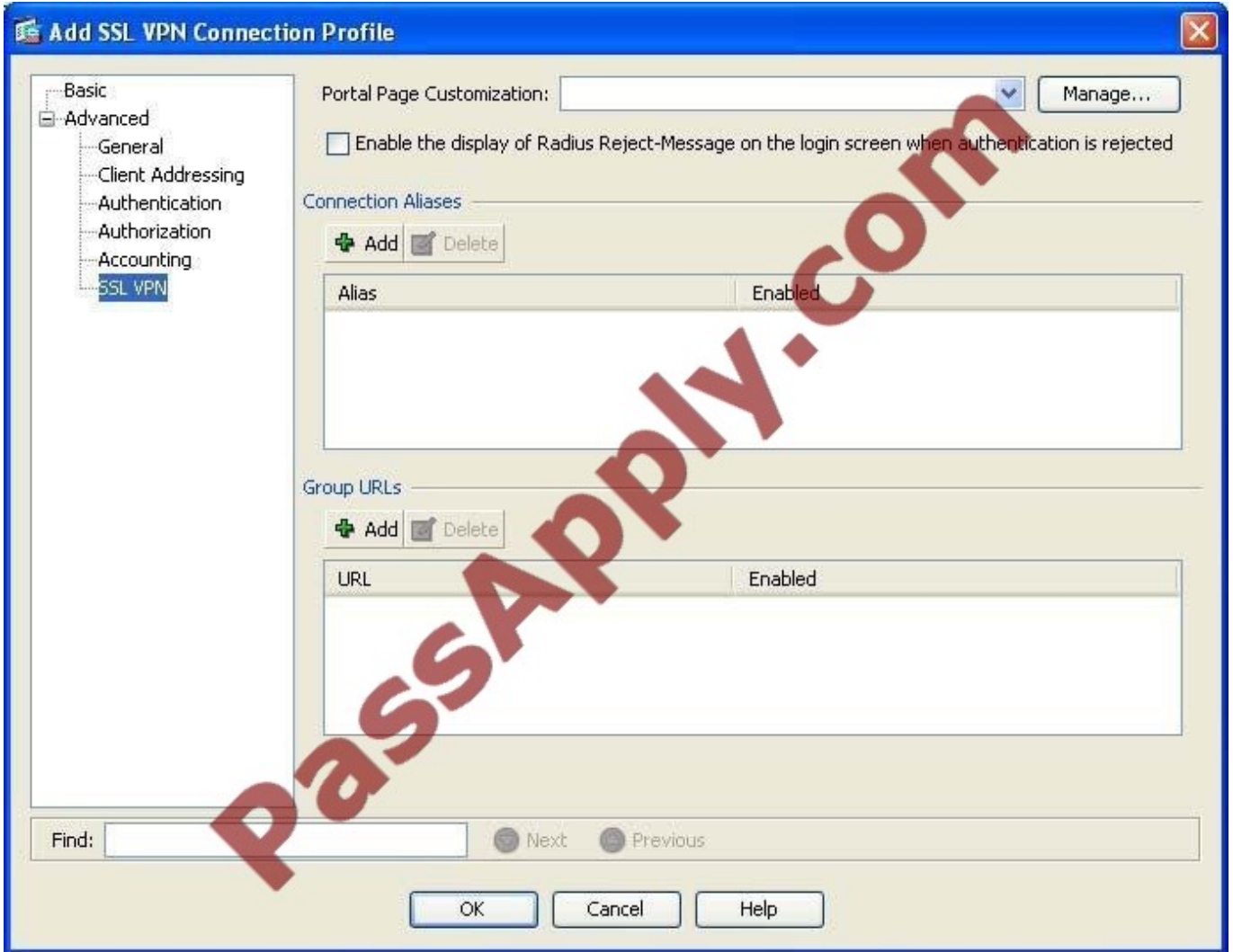
Subnet Mask: 255.255.255.0

OK Cancel Help

Navigate to:

[Configuration > Remote Access VPN > Network \(Client\) Access > AnyConnect Connection Profiles](#)

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...

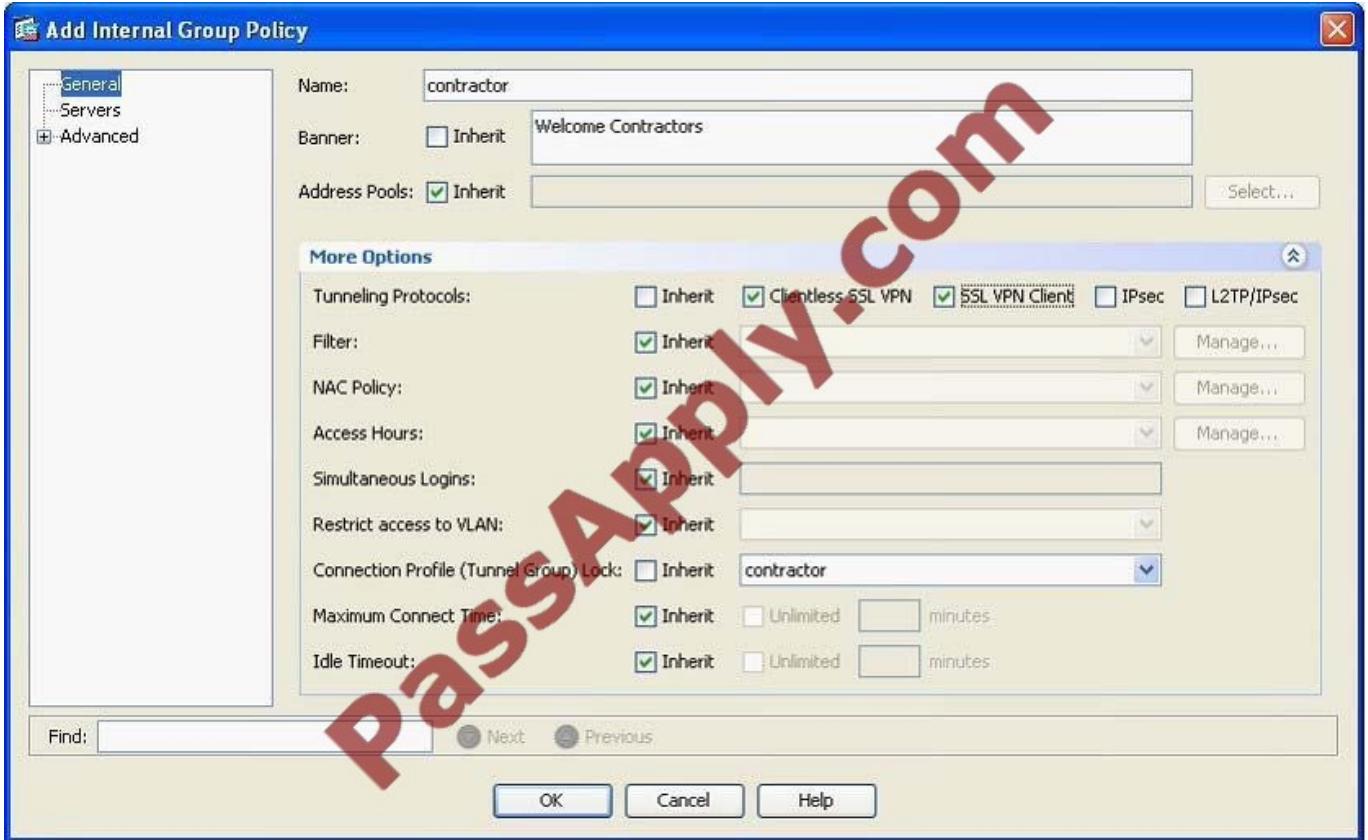
(Following field is an attribute of the group policy selected above.)

Enable SSL VPN Client protocol

Find: Next Previous

OK Cancel Help

[Configuration](#) > [Remote Access VPN](#) > [Network \(Client\) Access](#) > [Group Policies](#)



Navigate back to:

[Configuration > Remote Access VPN > Network \(Client\) Access > AnyConnect Connection Profiles](#)

And update Default Group Policy



Edit SSL VPN Connection Profile: contractor

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: contractor Manage...

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

Enable SSL VPN Client protocol

Find: Next Previous

OK Cancel Help

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.

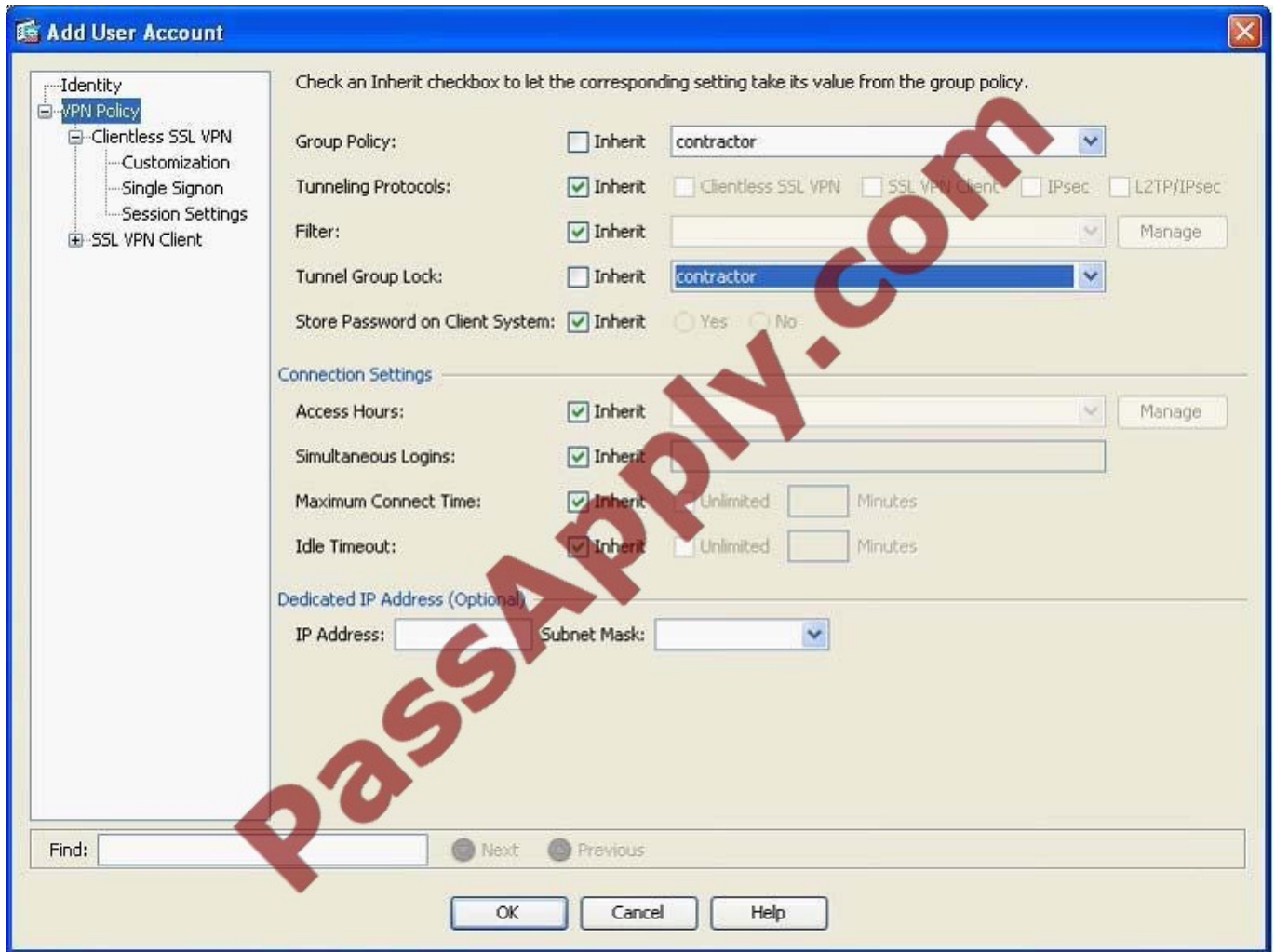
Full access(ASDM, SSH, Telnet and Console)
Privilege level is used with command authorization.
Privilege Level: 2

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:



The screenshot shows the Cisco ASA configuration interface. The breadcrumb navigation is Configuration > Remote Access VPN > AAA/Local Users > Local Users. The main content area displays instructions for creating local users and a table with the following data:

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

Buttons for Add, Edit, and Delete are visible on the right side of the table. The interface also includes a left-hand navigation pane and a top toolbar with various icons.

QUESTION 4

Refer to the 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 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?

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

Correct Answer: B

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

QUESTION 5

Match the characteristic on the left with the correct IKE Mode on the right.

Select and Place:

Match the characteristic on the left with the correct IKE Mode on the right.

<div style="border: 1px solid black; background-color: #e0ffe0; padding: 5px; margin-bottom: 5px;">IPsec Session Keys</div> <div style="border: 1px solid black; background-color: #e0ffe0; padding: 5px; margin-bottom: 5px;">Supports dynamically addressed peers using PSK</div> <div style="border: 1px solid black; background-color: #e0ffe0; padding: 5px; margin-bottom: 5px;">D-H Group 2-Default</div> <div style="border: 1px solid black; background-color: #e0ffe0; padding: 5px; margin-bottom: 5px;">IPsec SA</div> <div style="border: 1px solid black; background-color: #e0ffe0; padding: 5px; margin-bottom: 5px;">D-H Group 1-Default</div> <div style="border: 1px solid black; background-color: #e0ffe0; padding: 5px;">Protects Peer Identity</div>	<div style="border: 1px solid black; background-color: #ffffe0; padding: 5px; margin-bottom: 5px;">IKE Main Mode</div> <div style="border: 1px solid black; background-color: #ffffe0; height: 20px; margin-bottom: 5px;"></div> <div style="border: 1px solid black; background-color: #ffffe0; height: 20px; margin-bottom: 5px;"></div> <div style="border: 1px solid black; background-color: #ffffe0; padding: 5px; margin-bottom: 5px;">IKE Aggressive Mode</div> <div style="border: 1px solid black; background-color: #ffffe0; height: 20px; margin-bottom: 5px;"></div> <div style="border: 1px solid black; background-color: #ffffe0; height: 20px; margin-bottom: 5px;"></div> <div style="border: 1px solid black; background-color: #ffffe0; padding: 5px; margin-bottom: 5px;">IKE Quick Mode</div> <div style="border: 1px solid black; background-color: #ffffe0; height: 20px; margin-bottom: 5px;"></div> <div style="border: 1px solid black; background-color: #ffffe0; height: 20px;"></div>
---	---

Correct Answer:



Match the characteristic on the left with the correct IKE Mode on the right.

	IKE Main Mode
	Protects Peer Identity
	D-H Group 1-Default
	IKE Aggressive Mode
	Supports dynamically addressed peers using PSK
	D-H Group 2-Default
	IKE Quick Mode
	IPsec Session Keys
	IPsec SA

[Latest 642-648 Dumps](#)

[642-648 PDF Dumps](#)

[642-648 Study Guide](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

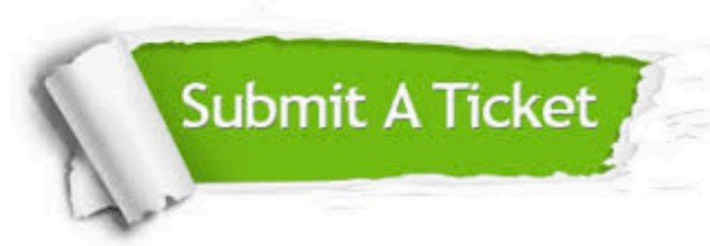
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [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.passapply.com/allproducts>

Need Help

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



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © passapply, All Rights Reserved.