

**Cisco 642-647**

**Deploying Cisco ASA VPN Solutions (VPN v1.0)**

**Version: 4.4**

**QUESTION NO: 1**

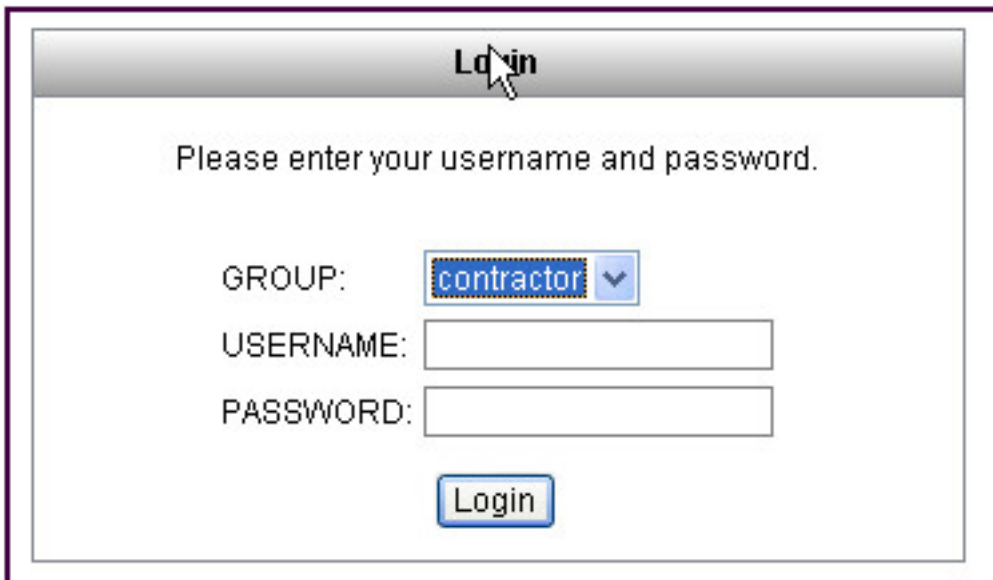
An XYZ Corporation systems engineer, while making a sales call on the ABC Corporation headquarters, tried to access the XYZ sales demonstration folder to transfer a demonstration via FTP from an ABC conference room behind the firewall. The engineer could not reach XYZ through the remote-access VPN tunnel. From home the previous day, however, the engineer connected to the XYZ sales demonstration folder and transferred the demonstration via IPsec over DSL.

To get the connection to work and transfer the demonstration, what can you suggest?

- A. Change the MTU size on the IPsec client to account for the change from DSL to cable transmission.
- B. Enable the local LAN access option on the IPsec client.
- C. Enable the IPsec over TCP option on the IPsec client.
- D. Enable the clientless SSL VPN option on the PC

**Answer: A**

**Explanation:**

**QUESTION NO: 2**

The image shows a web browser window titled "Login". The main content area contains the text "Please enter your username and password." Below this text are three input fields: "GROUP:" with a dropdown menu currently showing "contractor", "USERNAME:", and "PASSWORD:". At the bottom of the form is a "Login" button.

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

- A. Define a special identity certificate with multiple groups that 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 would appear on the login page.

**C.** Under Connection Profiles, define a NOC profile that encompasses the required individual profiles that would appear on the login page.

**D.** Under Connection Profiles, enable group selection from the login page.

**Answer: D**

**Explanation:**

### QUESTION NO: 3

**Instruction**

This item contains a simulation task. Refer to the scenario and topology before starting. Open the Topology window and click the required device to open the GUI window on a virtual terminal. Check your configuration from the client system in the topology. Only after you complete all the required configurations successfully can you access the contractor PC to test the VPN access. To perform the test, enter the <https://192.168.4.2/contractor> URL in the browser, click GO, and log in as contractor1. Then, from the SSL VPN port, choose **Network Access** then **Start AnyConnect**. Use scrolls to view all parts of the Cisco ASDM screens.


**Note:** In this simulation, not all Cisco ASDM screens are fully functional.

**Scenario**

You are the firewall administrator for a small company. The company currently supports SSL VPN for "employees" only. Your job is to add support for a new group of Cisco AnyConnect SSL VPN users, "contractors", on the Cisco ASA using Cisco ASDM. For this exercise, the SSL VPN wizard has been deactivated. You will be asked to add a new connection profile, a new Group Policy, and a new user account. Use this information to complete the configurations:

- New Connection Profile
  - Name: contractor
  - AAA server group: LOCAL
  - Default Group Policy: contractor
  - 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
  - Only permitted these two tunneling protocols: 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**



The topology diagram shows a laptop labeled "Contractor" PC connected to a cloud, which is in turn connected to a Cisco ASA firewall. A red line indicates the connection between the laptop and the cloud, and another red line connects the cloud to the firewall. The firewall is labeled with the number 1.

Which four parameters must be defined in an ISAKMP policy when 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

**Answer: A,B,C,E**

**Explanation:**

**QUESTION NO: 4**

An administrator has preconfigured the Cisco ASA 5505 user settings with a username and a password. When the telecommuter first turns on the Cisco ASA 5505 and attempts to establish a VPN tunnel, the user is prompted for a username and password. Which two Cisco ASA 5505 Group Policy features require this extra level of authentication? (Choose two.)

- A. New Unit Authentication
- B. Extended Group Authentication
- C. Secure Unit Authentication
- D. Role-Based Access Control Authentication
- E. Compartmented Mode Authentication
- F. Individual User Authentication

**Answer: C,F**

**Explanation:**

**QUESTION NO: 5**

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

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

- 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.

**Answer: B,E**

**Explanation:**

**QUESTION NO: 6**

Which Cisco ASA SSL VPN feature provides support for PCI compliance by allowing for the validation of two sets of username and password credentials on the SSL VPN login page?

- A. Single Sign-On
- B. Certificate to Profile Mapping
- C. Double Authentication
- D. RSA OTP

**Answer: D**

**Explanation:**

#### QUESTION NO: 7

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

**Answer: E,F**

**Explanation:**

#### QUESTION NO: 8

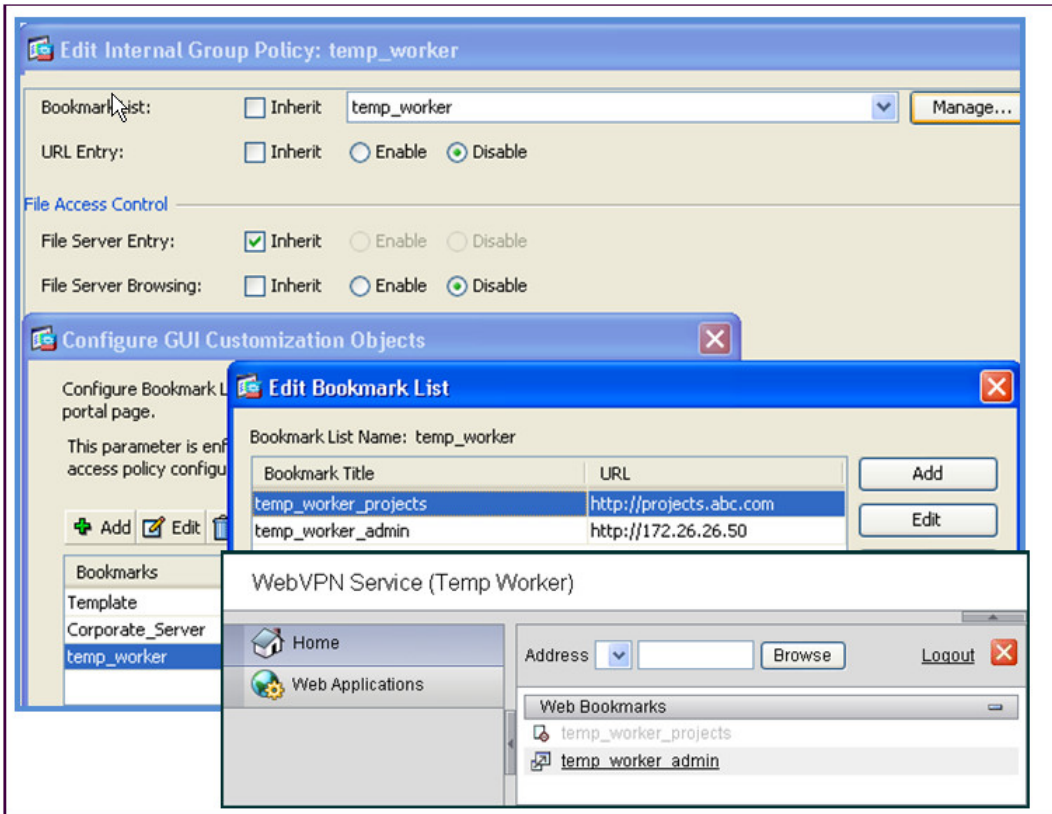
Your corporate finance department purchased a new non-web-based TCP application tool to run on one of its servers. The finance employees need remote access to the software during non-business hours. The employees do not have "admin" privileges to their PCs. How would you configure the SSL VPN tunnel 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.

**Answer: A**

**Explanation:**

#### QUESTION NO: 9



Refer to the exhibit. A new network engineer configured the ABC adaptive security appliance with two bookmarks for a new temporary employee. 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 (greyed-out) bookmark. It was determined that the URL and IP addressing information in the GUI screens is correct.

What is wrong with the configuration?

- 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

**Answer: C**

**Explanation:**

**QUESTION NO: 10**

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

Name	Type	Tunneling Protocol	AAA Server Group
new_hire	Internal	webvpn	-- N/A --
contractor	Internal	webvpn,svc	-- N/A --
employee	Internal	webvpn,svc	-- N/A --
management	Internal	IPsec,svc	-- N/A --
engineering	Internal	IPsec,svc	-- N/A --
DfltGrpPolicy (System Default)	Internal	IPsec,webvpn,svc	-- 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: ●●●●

Login

Refer to the exhibit. 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. Along with 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?

- 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.

**Answer: D**

**Explanation:**

## QUESTION NO: 11

Which two statements about the Cisco ASA load balancing feature are correct? (Choose two.)

- A. The Cisco ASA load balances both site-to-site and remote-access VPN tunnels.
- B. The Cisco ASA load balances remote-access VPN tunnels only.
- C. The Cisco ASA load balances IPsec VPN tunnels only.
- D. The Cisco ASA load balances IPsec VPN and Cisco AnyConnect SSL VPN tunnels only.

E. The Cisco ASA load balances IPsec VPN, clientless, and Cisco AnyConnect SSL VPN tunnels

**Answer: B,E**

**Explanation:**

Load balancing is effective only on remote sessions initiated with the following clients:

- Cisco AnyConnect VPN Client (Release 2.0 and later)
- Cisco VPN Client (Release 3.0 and later)
- Cisco ASA 5505 Security Appliance (when acting as an Easy VPN client)
- Cisco VPN 3002 Hardware Client (Release 3.5 or later)
- Cisco PIX 501/506E when acting as an Easy VPN client
- IOS EZVPN Client devices supporting IKE-redirect (IOS 831/871)
- Clientless SSL VPN (not a client)

Load balancing works with IPsec clients and SSL VPN client and clientless sessions. All other VPN connection types (L2TP, PPTP, L2TP/IPsec), including LAN-to-LAN, can connect to an adaptive security appliance on which load balancing is enabled, but they cannot participate in load balancing.

Reference:

<http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/vpnsysop.html#wp10488>  
34

### QUESTION NO: 12 DRAG DROP

On the right, a permanent (P) or temporary (T) license is added to a Cisco ASA 5520. The merged license results in new capabilities for the Cisco ASA 5520. Drag the new resultant license on the left to the merging licenses on the right.

<div style="background-color: #c6e0b4; padding: 5px; margin-bottom: 5px; border: 1px solid black;">Base (P) + 50 SSL users (P)</div> <div style="background-color: #c6e0b4; padding: 5px; margin-bottom: 5px; border: 1px solid black;">Base (P) + 50 SSL users (T)</div> <div style="background-color: #c6e0b4; padding: 5px; margin-bottom: 5px; border: 1px solid black;">Base (P) + 25 SSL users (P)</div> <div style="background-color: #c6e0b4; padding: 5px; border: 1px solid black;">Base + 25 SSL users + Botnet</div>	<div style="background-color: #ffffcc; padding: 5px; margin-bottom: 5px; border: 1px solid black;">Base (P) and 25 SSL users (P). Add 50 SSL users (P).</div> <div style="background-color: #ffffcc; padding: 5px; margin-bottom: 5px; border: 1px solid black;">Base (P) and 50 SSL users (T). Add 25 SSL (P).</div> <div style="background-color: #ffffcc; padding: 5px; margin-bottom: 5px; border: 1px solid black;">Base (P) and 25 SSL users (P). Add Botnet (T).</div> <div style="background-color: #ffffcc; padding: 5px; border: 1px solid black;">Base (P) and 25 SSL users (P) and Botnet (T). Add 50 SSL (T).</div>
--	--

**Answer:**



On the right, a permanent (P) or temporary (T) license is added to a Cisco ASA 5520. The merged license results in new capabilities for the Cisco ASA 5520. Drag the new resultant license on the left to the merging licenses on the right.

Base (P) + 50 SSL users (P)	Base (P) + 50 SSL users (P)
Base (P) + 50 SSL users (T)	Base (P) + 25 SSL users (P)
Base (P) + 25 SSL users (P)	Base + 25 SSL users + Botnet
Base + 25 SSL users + Botnet	Base (P) + 50 SSL users (T)

**Explanation:**

- Base (P) + 50 SSL users (P)
- Base (P) + 25 SSL users (P)
- Base + 25 SSL Users + Botnet
- Base (P) + 50 SSL Users (T)

**QUESTION NO: 13 DRAG DROP**

What is the selection hierarchy to which attributes are applied to a clientless SSL VPN user? Drag an attribute policy on the left to the correct priority level within the attribute hierarchy on the right.

Group Policy attributes attached to the user profile	highest priority
User Policy attributes	
DAP attributes	
Default Group Policy attributes	
Group Policy attributes attached to the connection profile	lowest priority

**Answer:**

What is the selection hierarchy to which attributes are applied to a clientless SSL VPN user? Drag an attribute policy on the left to the correct priority level within the attribute hierarchy on the right.

Group Policy attributes attached to the user profile	DAP attributes
User Policy attributes	User Policy attributes
DAP attributes	Group Policy attributes attached to the user profile
Default Group Policy attributes	Group Policy attributes attached to the connection profile
Group Policy attributes attached to the connection profile	Default Group Policy attributes

**Explanation:** DAP attributes

User Policy Attributes

Group Policy Attributes attached to the user profile

Group Policy Attributes attached to the connection profile

Default Group Policy Attributes

#### QUESTION NO: 14

A Cisco AnyConnect user profile can be pushed to the PC of a remote user from a Cisco ASA. Which three user profile parameters are configurable? (Choose three.)

- A. Backup Server list
- B. DTLS Override
- C. Auto Reconnect
- D. Simultaneous Tunnels
- E. Connection Profile Lock
- F. Auto Update

**Answer:** A,C,F

**Explanation:**

#### QUESTION NO: 15