



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.pass4itsure.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.

VPN Client | Create New VPN Connection Entry

Connection Entry: Management

Description: ABC_Corp

Host: 192.168.4.2

Authentication | Transport | Backup Servers | Dial-In

☒ Group Authentication ☐ Mutual Group Authentication

Name: Management

Password: XXXXXXXX

Confirm Password: XXXXXXXX

☐ Certificate Authentication

Name: [Dropdown]

☐ Send CA Certificate Chain

Erase User Password Save Cancel

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.

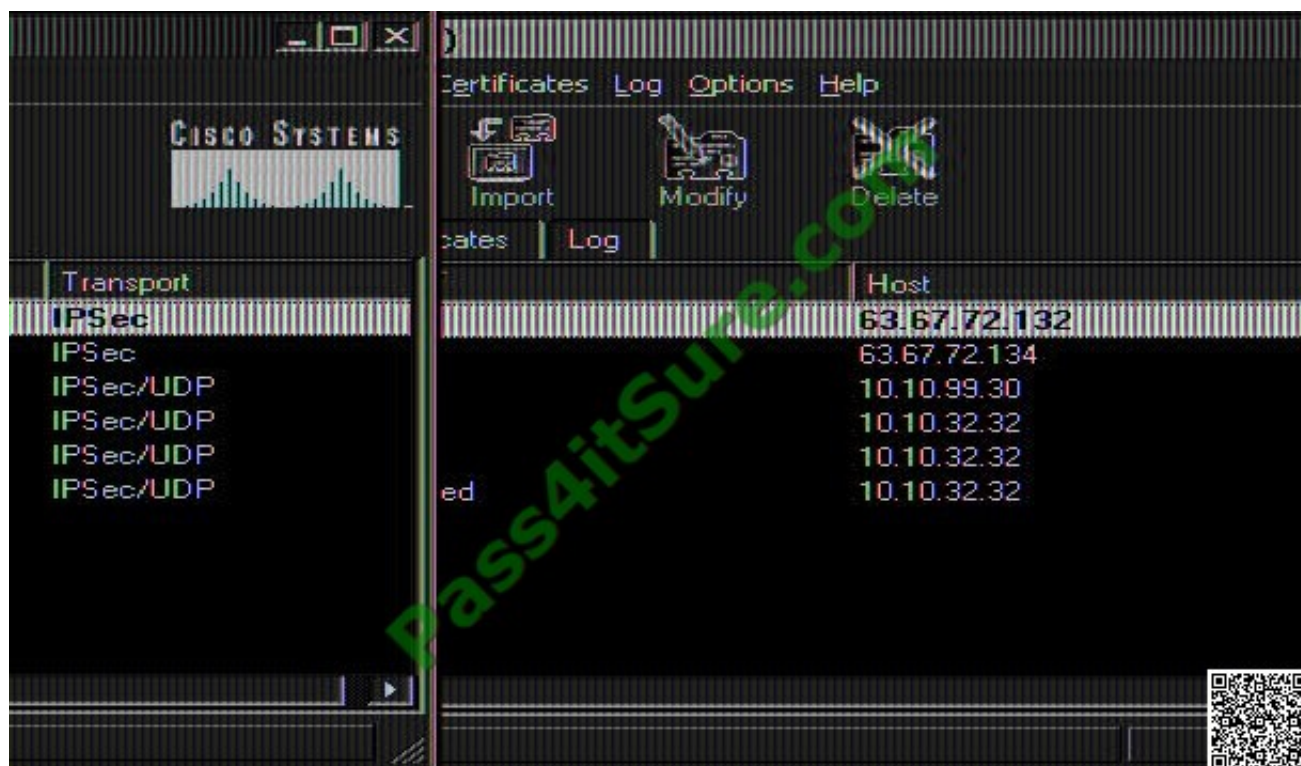
Correct Answer: D

[http://www.cisco.com/en/US/docs/security/vpn_client/cisco_vpn_client/vpn_client46/win/user/guide/vc4.](http://www.cisco.com/en/US/docs/security/vpn_client/cisco_vpn_client/vpn_client46/win/user/guide/vc4.html#wp1074766)

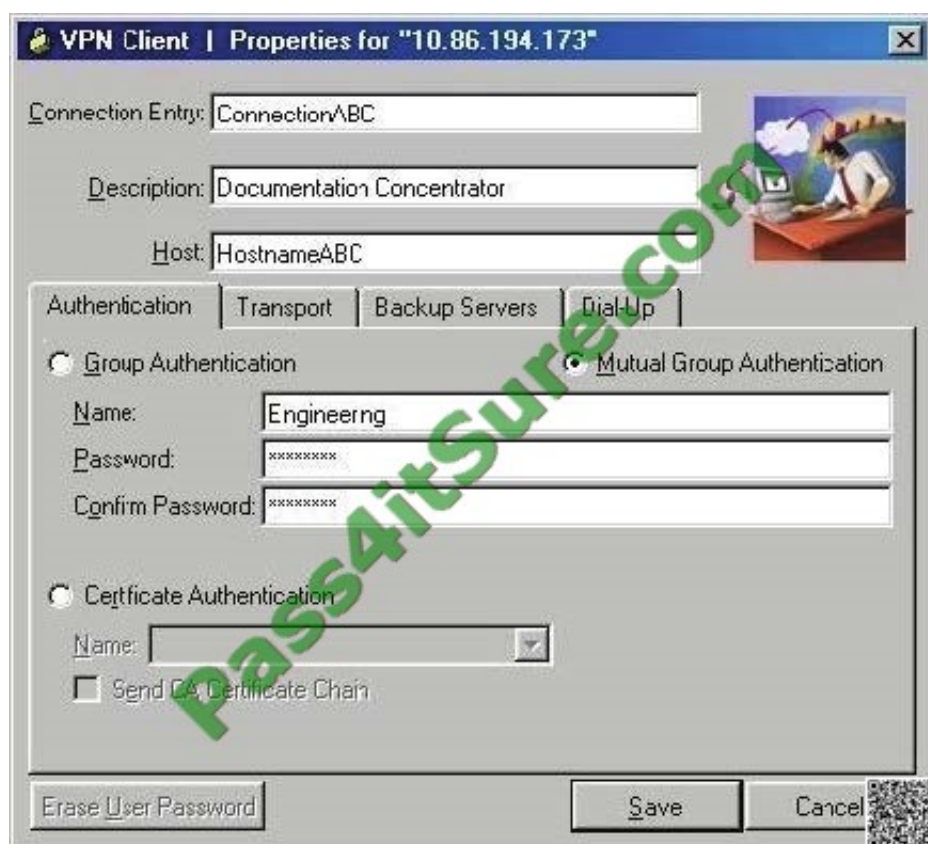
[html#wp1074766](http://www.cisco.com/en/US/docs/security/vpn_client/cisco_vpn_client/vpn_client46/win/user/guide/vc4.html#wp1074766)

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

Refer to following Exhibit and answer the following question below:



Instructions

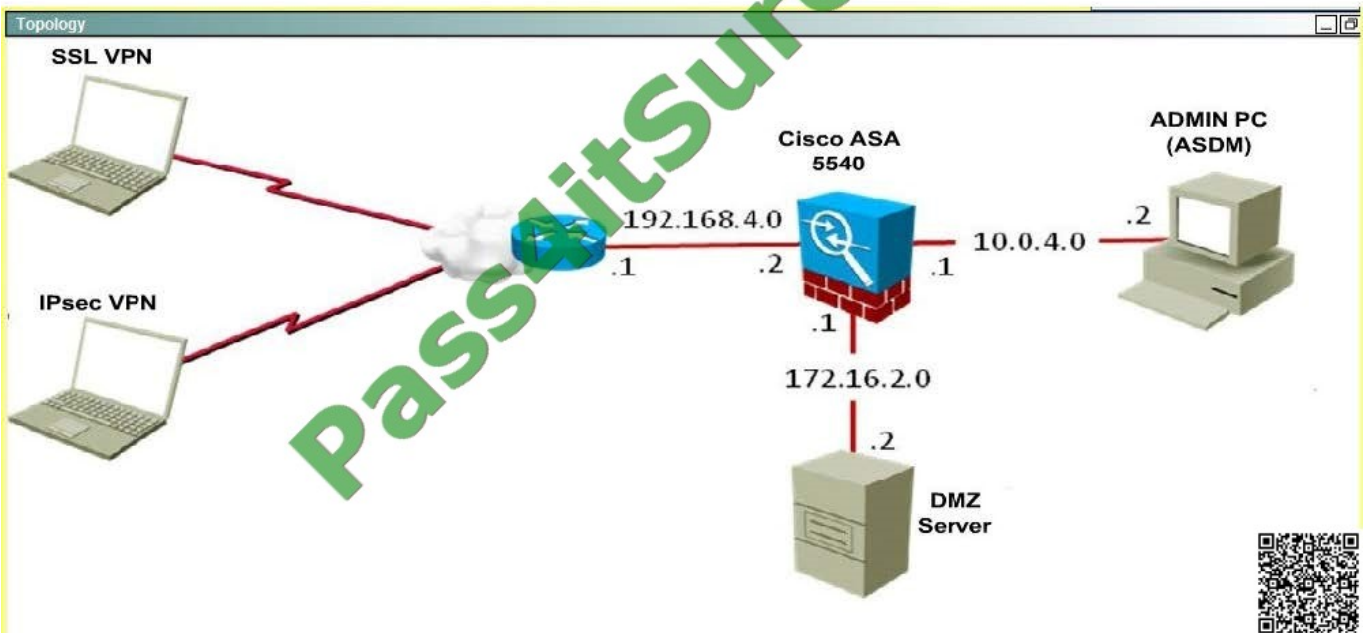
Click the grey buttons at the bottom of this frame to view the different windows.

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

The "Tab" key and most commands that use the **Control** or **Escape** keys are not supported and are not needed to complete this simulation.

Scenario

You are the firewall administrator for a small company. The company currently supports remote-access SSL VPN and IPsec VPN via a 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 the answers to the questions.





ASDM

File View Tools Wizards Window Help

Look For: Go

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer 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 (Web Launch).

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
DMZ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Device Certificate

Port Settings ..

Login Page Setting

☒ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.

☐ Shutdown portal login page.

Connection Profiles

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

☒ Add ☒ Edit ☐ Delete

Name	SSL Enabled	IPsec Enabled	Alias	Authentication Method
DefaultRAGroup	<input checked="" type="checkbox"/>	<input type="checkbox"/>		AAA(LOCAL)
DefaultWEBVPNGroup	<input checked="" type="checkbox"/>	<input type="checkbox"/>		AAA(LOCAL)
employee	<input checked="" type="checkbox"/>	<input type="checkbox"/>	employee	AAA(LOCAL)

QR Code

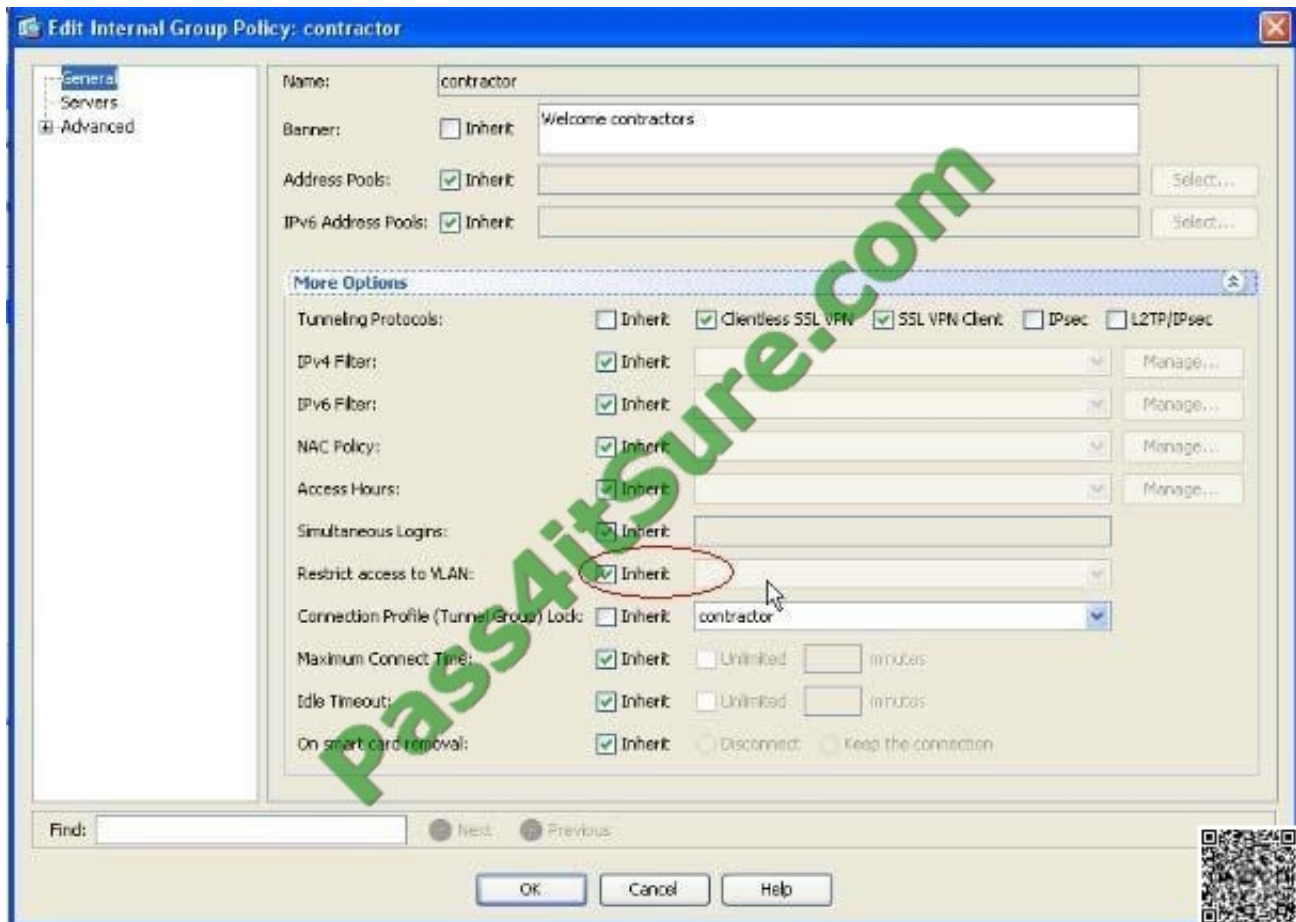
Which group policy restricts the VPN user access to VLAN 100?

- A. Employee
- B. Contractor
- C. Management
- D. Engineering

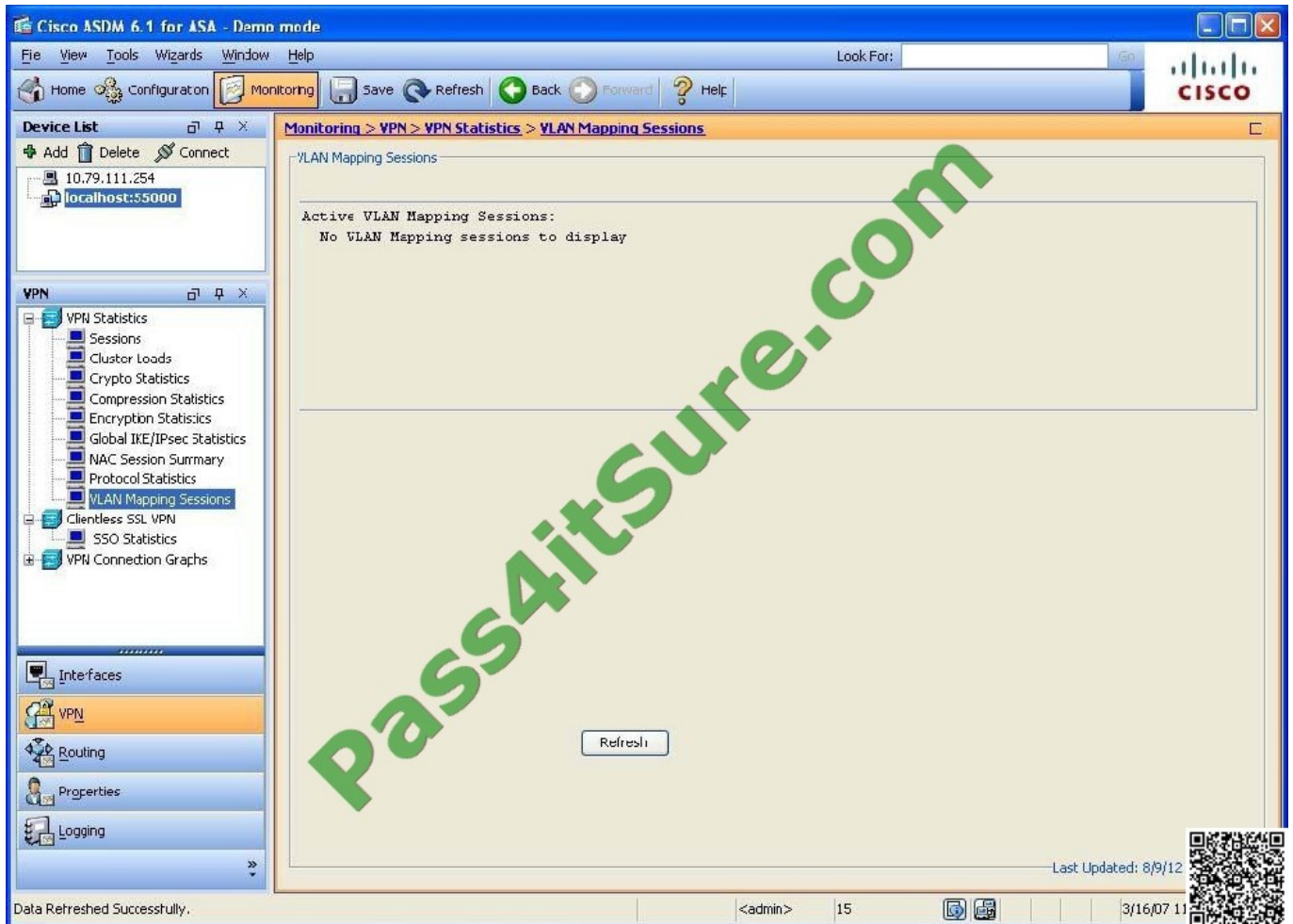
Correct Answer: B

Explanation:

configuration > network client access > any connect connection profiles > connection profiles > edit



For each profile > general > more options > restricted VLAN Monitoring > VPN > VPN statistics Sessions, vlan mapping sessions



QUESTION 3

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

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



CAURL	CertificateEnrolment	<p>Identifies the SCEP CA server.</p> <p>Permitted values: Fully qualified domain name or IP Address of CA server.</p> <p>In the following example, the CAURL field identifies <code>http://ca01.cisco.com</code> as the name of the SCEP CA server.</p> <p>Attributes of CAURL:</p> <p>PromptForChallengePW: Used for manual get certificate requests. After the user clicks Get Certificate, they will be prompted for their username and one time password.</p> <p>Permitted values: true, false</p> <p>The <code>PromptForChallengePW</code> attribute in the example below is configured "true."</p> <p>Thumbprint: The CA's certificate thumbprint. Use SHA1 or MD5 hashes. The <code>Thumbprint</code> attribute in the example below is 8475B631202E3414D4BB223A464E6AAB8CA123AB.</p> <p>Note Obtain the CA URL and thumbprint, from your CA server administrator. The CA server administrator should retrieve the thumbprint directly from the server and not from a "fingerprint" or "thumbprint" attribute from a certificate it issued.</p>
-------	----------------------	--

QUESTION 4

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



	<ul style="list-style-type: none">• Network Access Manager• Telemetry• Highly secure remote-access connectivity• Single license per device model• Full Tunneling access to enterprise applications
op capabilities connect Secure g Full Tunneling	<ul style="list-style-type: none">• Includes clientless SSL VPN, Cisco Secure Desktop (including Host Scan), and support for Cisco AnyConnect Mobility. Provides Essentials capabilities, including access to enterprise applications
rs, and is available as	<ul style="list-style-type: none">• License is based on number of simultaneous use a single device or shared license
Cisco IronPort Web	<ul style="list-style-type: none">• Cisco AnyConnect Secure Mobility also requires a Security Appliance license
	ses
to Essentials or	<ul style="list-style-type: none">• Enables Mobile OS platform compatibility• One license required per ASA platform, in addition Premium license
ties (such as auto-	<ul style="list-style-type: none">• Enables advanced endpoint assessment capability remediation)
ses (not available with	<ul style="list-style-type: none">• Required per device, in addition to Premium license AnyConnect Essentials)
ndent of where the	<ul style="list-style-type: none">• Enforce security policy in every transaction, independent of where user is located
g license and optional AnyConnect Premium	<ul style="list-style-type: none">• For use with Cisco IronPort Web Security Appliance AnyConnect Premium license, or standalone license

An engineer, while working at a home office, wants to launch the Cisco AnyConnect Client to the corporate offices while simultaneously printing network designs on the home network.

Without allowing access to the Internet, what are the two best ways for the administrator to configure this application? (Choose two.)

- A. Select the Tunnel All Networks policy.
- B. Select the Tunnel Network List Below policy.
- C. Select the Exclude Network List Below policy.
- D. Configure an exempted network list.
- E. Configure a standard access list and apply it to the network list.



F. Configure an extended access list and apply it to the network list.

Correct Answer: CE

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

QUESTION 5

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

[642-648 Practice Test](#)

[642-648 Exam Questions](#)

[642-648 Braindumps](#)



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.pass4itsure.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 One Year Free Update <p>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>	 Money Back Guarantee <p>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 Security & Privacy <p>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 © pass4itsure, All Rights Reserved.