



# 642-648<sup>Q&As</sup>

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**

Which three Host Scan checks on a remote endpoint can you configure Cisco Secure Desktop to perform? (Choose three.)

- A. registry checks
- B. user rights checks
- C. group policy objects checks
- D. file checks
- E. virus software checks F. process checks

Correct Answer: ADF

<http://www.cisco.com/en/US/docs/security/csd/csd341/configuration/guide/CSDhscan.html> You can specify a set of registry entries, filenames, and process names, which form a part of Basic Host Scan. Host Scan, which includes Basic Host Scan and Endpoint Assessment, or Advanced Endpoint Assessment; occurs after the prelogin assessment but before the assignment of a DAP. Following the Basic Host Scan, the security appliance uses the login credentials, the host scan results, prelogin policy, and other criteria you configure to assign a DAP. See the sections that name the types of Basic Host Scan entries you would like to configure: Adding a File Check Adding a Registry Key Check Adding a Process Check

---

**QUESTION 2**

Refer to following Exhibit and answer the following question below:



**Instructions**

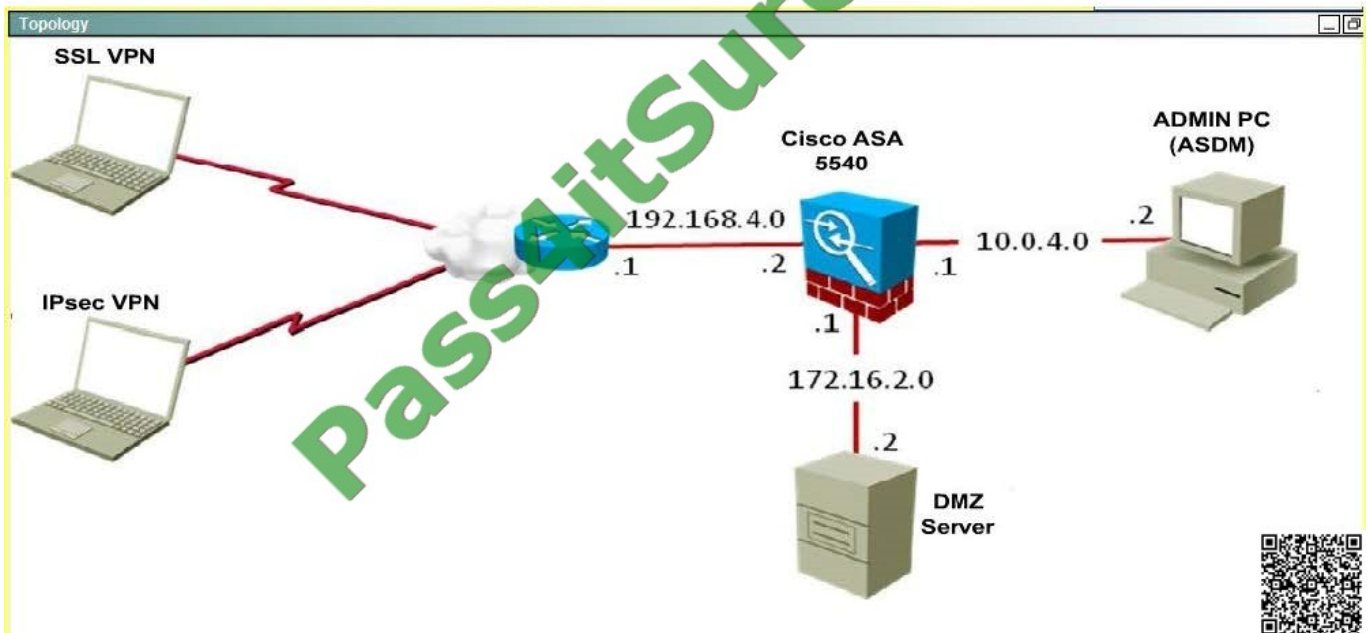
Click the grey buttons at the bottom of this frame to view the different windows.

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.





The screenshot shows the ASDM configuration page for Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles. The page includes a left sidebar with a tree view of configuration options, a main content area with configuration details, and a bottom status bar.

**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"/>            |

**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.

| Name               | SSL Enabled                         | IPsec Enabled            | Aliases   | Authentication Method |
|--------------------|-------------------------------------|--------------------------|-----------|-----------------------|
| DefaultRAGroup     | <input checked="" type="checkbox"/> | <input type="checkbox"/> |           | AAA(LOCAL)            |
| DefaultWEBVPNGroup | <input checked="" type="checkbox"/> | <input type="checkbox"/> |           | AAA(LOCAL)            |
| employee1          | <input checked="" type="checkbox"/> | <input type="checkbox"/> | employee1 | AAA(LOCAL)            |

Device Certificate  
Port Settings ..

Upon logging in, user, employee1, gets two sets of privileges. Choose the two options that show the privileges that are held by employee1.(Choose two)

- 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

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 authorization to setup other commands but this shows how I setup contractor1



The screenshot shows the Cisco ASA configuration interface. The left sidebar displays the configuration tree with 'Local Users' selected under 'Remote Access VPN'. The main pane shows the 'Local Users' configuration page. It includes instructions on creating entries and enabling command authorization. A table lists the configured users.

| 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 on the right. 'Apply' and 'Reset' buttons are at the bottom. A QR code is in the bottom right corner.

### QUESTION 3

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 antispayware 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



|           |  |
|-----------|--|
| Host Scan | <p>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).</p> <p>With an Advanced Endpoint Assessment License, you can enhance Host Scan by configuring an attempt to update noncompliant computers to meet version requirements.</p> <p>Cisco can provide timely updates to the list of applications and versions. Host Scan supports in a package that is separate from Cisco Secure Desktop.</p> |
|-----------|--|



#### QUESTION 4

Which statement is correct concerning the trusted network detection (TND) feature?

- A. The Cisco AnyConnect 3.0 Client supports TND on Windows, Mac, and Linux platforms.
- B. With TND, one result of a Cisco Secure Desktop basic scan on an endpoint is to determine whether a device is a member of a trusted or an untrusted network.
- C. If enabled, and a CSD scan determines that a host is a member of an untrusted network, an administrator can configure the TND feature to prohibit an end user from launching the Cisco AnyConnect VPN Client.
- D. When the user is inside the corporate network, TND can be configured to automatically disconnect a Cisco AnyConnect session.

Correct Answer: D

[http://www.cisco.com/en/US/docs/security/vpn\\_client/anyconnect/anyconnect25/administration/guide/ac03features.html](http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect25/administration/guide/ac03features.html)

Trusted Network Detection Trusted Network Detection (TND) gives you the ability to have AnyConnect automatically disconnect a VPN connection when the user is inside the corporate network (the trusted network) and start the VPN connection when the user is outside the corporate network (the untrusted network). This feature encourages greater security awareness by initiating a VPN connection when the user is outside the trusted network.

If AnyConnect is also running Start Before Logon (SBL), and the user moves into the trusted network, the SBL window displayed on the computer automatically closes. TND does not interfere with the ability of the user to manually establish a VPN connection. It does not disconnect a VPN connection that the user starts manually in the trusted network. TND only disconnects the VPN session if the user first connects in an untrusted network and moves into a trusted network. For example, TND disconnects the VPN session if the user makes a VPN connection at home and then moves into the corporate office. Because the TND feature controls the AnyConnect GUI and automatically initiates connections, the GUI should run at all times. If the user exits the GUI, TND does not automatically start the VPN connection.

You configure TND in the AnyConnect profile. No changes are required to the ASA configuration.



### QUESTION 5

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

[642-648 VCE Dumps](#)

[642-648 Study Guide](#)

[642-648 Exam Questions](#)



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:



|   |   |  |
|---|---|--|
|  <b>One Year Free Update</b> <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> |  <b>Money Back Guarantee</b> <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> |  <b>Security &amp; Privacy</b> <p>We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information &amp; 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.