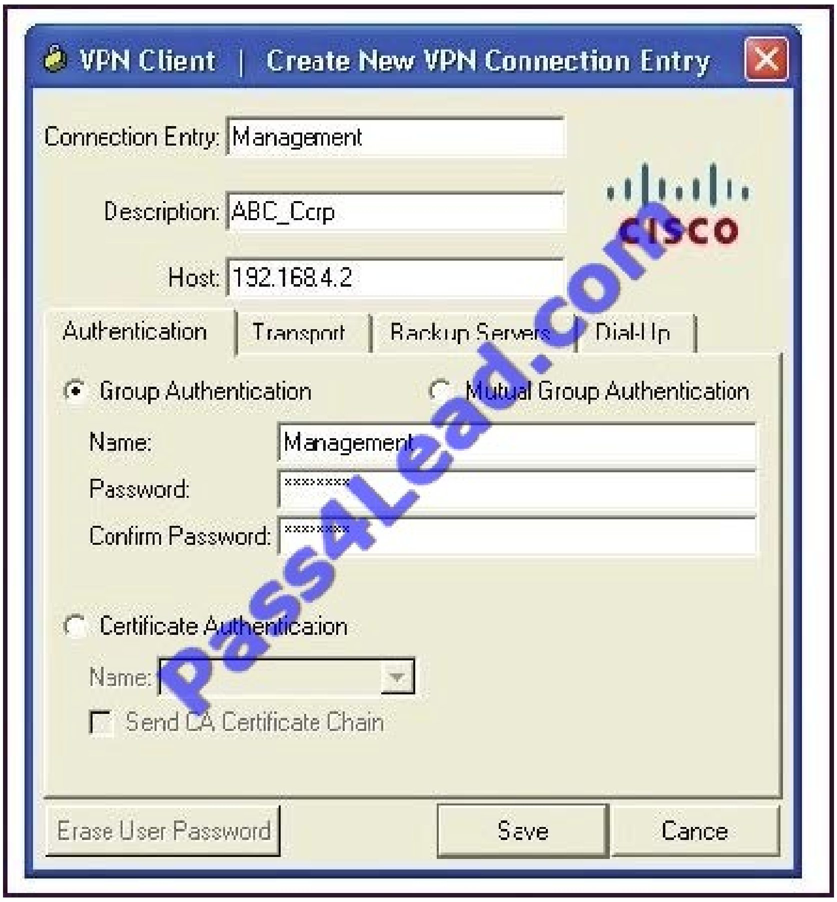
# 642-648$^{\text{Q\&As}}$

Deploying Cisco ASA VPN Solutions (VPN v2.0)

**QUESTION 1**

Refer to the exhibit.



VPN Client | Create New VPN Connection Entry

Connection Entry: Management

Description: ABC_Corp

Host: 192.168.4.2

● Group Authentication ○ Mutual Group Authentication

Name: Management

Password: ********

Confirm Password: ********

○ Certificate Authentication

Name:

□ Send CA Certificate Chain

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.

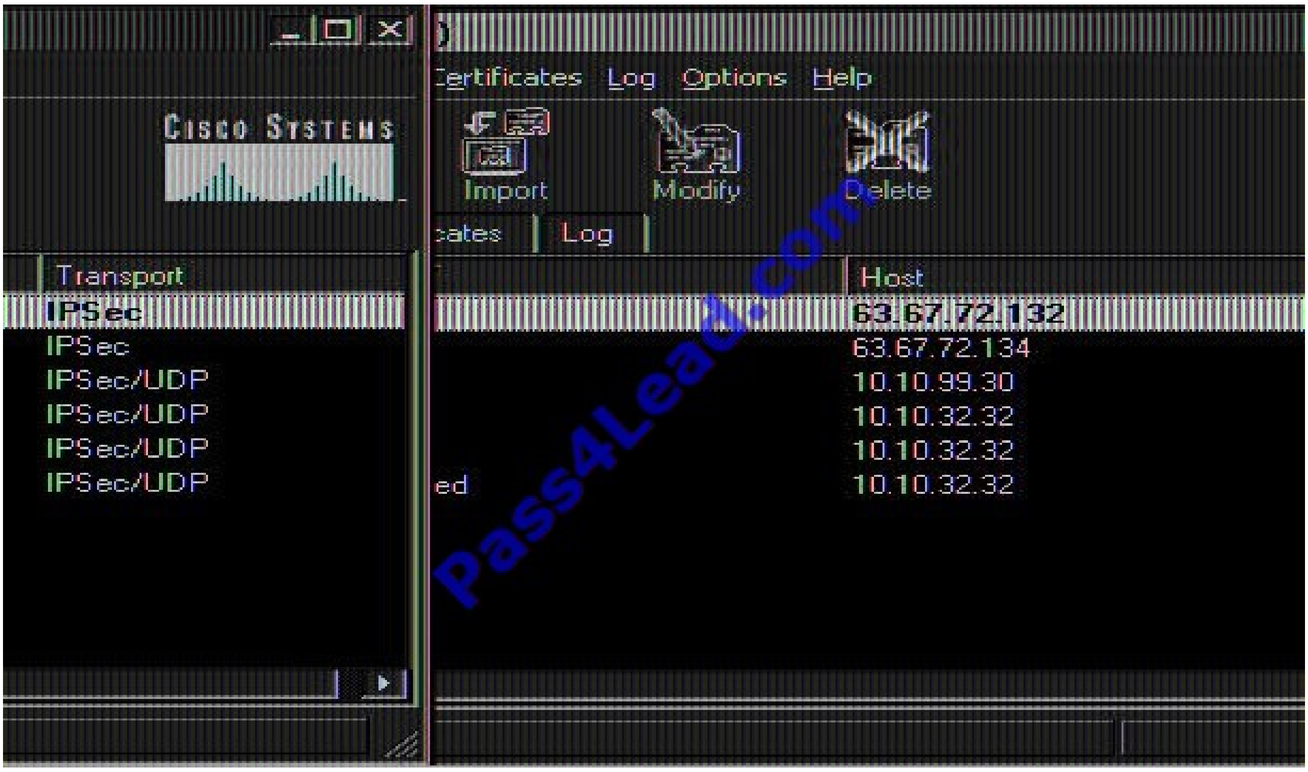
Correct Answer: D

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

html#wp1074766

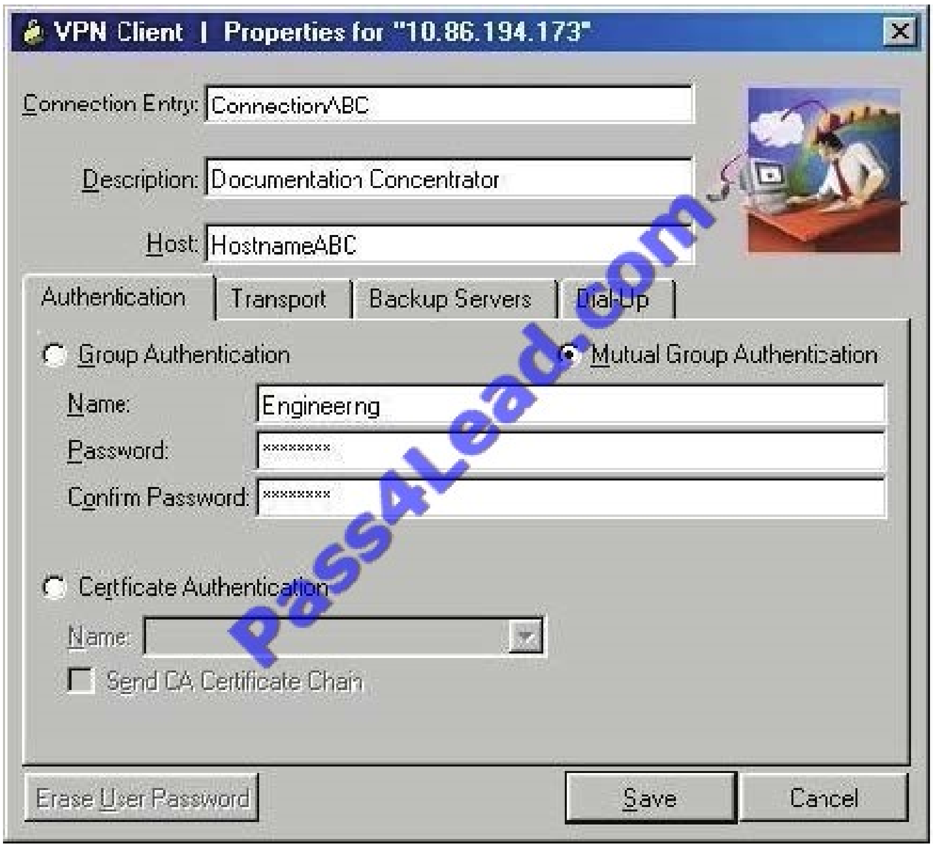
Step 1 Start the VPN Client by choosing Start > Programs > Cisco Systems VPN Client > VPN Client.

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.



| Transport | | Host |
|---|---|---|
| IPSec | | 63.67.72.132 |
| IPSec | | 63.67.72.134 |
| IPSec/UDP | | 10.10.99.30 |
| IPSec/UDP | | 10.10.32.32 |
| IPSec/UDP | | 10.10.32.32 |
| IPSec/UDP | ed | 10.10.32.32 |

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


VPN Client | Properties for "10.86.194.173"

Connection Entry: ConnectionABC

Description: Documentation Concentrator

Host: HostnameABC

○ Group Authentication ● Mutual Group Authentication

Name: Engineerng

Password: ********

Confirm Password: ********

○ Certficate Authentication

Name:

□ Send CA Certificate Chain

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**

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

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 3**

For clientless SSL VPN users, bookmarks can be assigned to their portal. What are three methods for assigning bookmarks? (Choose three.)

A. connection profiles

B. group policies

C. XML profiles

D. LDAP or RADIUS attributes

E. the portal customization tool

F. user policies

Correct Answer: BDF

Create one or more bookmark list entries that specify the URLs of the web-enabled applications eligible for smart tunnel access, then assign the list to the DAPs, group policies, or local user policies for whom you want to provide smart tunnel access. e.g.

Dynamic access policies (DAP)

VPN gateways operate in dynamic environments. Multiple variables can affect each VPN connection, for example, intranet configurations that frequently change, the various roles each user may inhabit within an organization, and logins from

remote access sites with different configurations and levels of security. The task of authorizing users is much more complicated in a VPN environment than it is in a network with a static configuration.

Dynamic Access Policies (DAP) on the security appliance let you configure authorization that addresses these many variables. You create a dynamic access policy by setting a collection of access control attributes that you associate with a

specific user tunnel or session. These attributes address issues of multiple group membership and endpoint security. That is, the security appliance grants access to a particular user for a particular session based on the policies you define. It generates a DAP at the time the user connects by selecting and/or aggregating attributes from one or more DAP records. It selects these DAP records based on the endpoint security information of the remote device and the AAA

authorization information for the authenticated user. It then applies the DAP record to the user tunnel or session.

**QUESTION 4**

An on-screen keyboard is a programmable SSL VPN option. Which three options are keyboard- configurable parameters that the administrator can enable or disable? (Choose three.)

A. Show only if Secure Desktop Vault is disabled.

B. Do not show onscreen keyboard.

C. Show only for the login page.

D. Show for all user input fields.

E. Show for all portal pages that require authentication.

F. Show for all plug-in pages.

Correct Answer: BCE

Onscreen keyboard The security appliance includes an onscreen keyboard option for the login page and subsequent authentication requests for internal resources. This provides additional protection against software-based keystroke loggers by requiring a user to use a mouse to click characters in an onscreen keyboard for authentication, rather than entering the characters on a physical keyboard.

**QUESTION 5**

Which three options are characteristics of WebType ACLs? (Choose three.)

A. They are assigned per-connection profile.

B. They are assigned per-user or per-group policy.

C. They can be defined in the Cisco AnyConnect Profile Editor.

D. They support URL pattern matching.

E. They support implicit deny all at the end of the ACL.

F. They support standard and extended WebType ACLs.

Correct Answer: BDE

You can configure ACLs (Access Control Lists) to apply to user sessions. These are filters that permit or deny user access to specific networks, subnets, hosts, and web servers. ?If you do not define any filters, all connections are permitted. ? The security appliance supports only an inbound ACL on an interface. ?At the end of each ACL, there is an implicit, unwritten rule that denies all traffic that is not permitted. If traffic is not explicitly permitted by an access control entry (ACE), the security appliance denies it. ACEs are referred to as rules in this topic. This pane lets you add and edit ACLs to be used for Clientless SSL VPN sessions, and the ACL entries each ACL contains. It also displays summary information about ACLs and ACEs, and lets you enable or disable them, and change their priority order.

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

# Try our product !

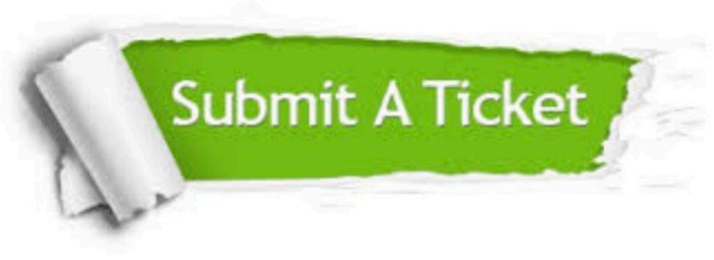
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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.pass4lead.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**

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.

**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.

**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.

Any charges made through this site will appear as Global Simulators Limited.