Cisco 642-648

Deploying Cisco ASA VPN Solutions (VPN v2.0)
Version: 6.0

QUESTION NO: 1

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.

Answer: D
Explanation:
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect25/administration/gui de/ac03features.html

Trusted Network Detection
Trusted Network Detection (TND) gives you the ability to have AnyConnect automatically disconnect a VPNconnection when the user is inside the corporate network (the trusted network) and start the VPN connectionwhen the user is outside the corporate network (the untrusted network). This feature encourages greatersecurity 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 SBLwindow displayed on the computer automatically closes.
TND does not interfere with the ability of the user to manually establish a VPN connection. It does notdisconnect a VPN connection that the user starts manually in the trusted network. TND only disconnects theVPN 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 thecorporate office.

Because the TND feature controls the AnyConnect GUI and automatically initiates connections, the GUI shouldrun 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 NO: 2

Refer to the exhibit.

You are configuring a laptop with the Cisco VPN Client, which uses digital certificates for authentication.

Which protocol does the Cisco VPN Client use to retrieve the digital certificate from the CA server?

A. FTP
B. LDAP
C. HTTPS
D. SCEP
E. OCSP

Answer: D

Explanation:

http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html

About CRLs

Certificate Revocation Lists provide the security appliance with one means of determining whether a certificatethat is within its valid time range has been revoked by its issuing CA. CRL configuration is a part of theconfiguration of a trustpoint.

You can configure the security appliance to make CRL checks mandatory when authenticating a

certificate(revocation-check crl command). You can also make the CRL check optional by adding the none argument(revocation-check crl none command), which allows the certificate authentication to succeed when the CA isunavailable to provide updated CRL data.

The security appliance can retrieve CRLs from CAs using HTTP, SCEP, or LDAP. CRLs retrieved for eachtrustpoint are cached for a length of time configurable for each trustpoint.

When the security appliance has cached a CRL for more than the length of time it is configured to cache CRLs,the security appliance considers the CRL too old to be reliable, or "stale". The security appliance attempts toretrieve a newer version of the CRL the next time a certificate authentication requires checking the stale CRL.

QUESTION NO: 3

When using clientless SSL VPN, you might not want some applications or web resources to go through the Cisco ASA appliance. For these application and web resources, as a Cisco ASA administrator, which configuration should you use?

A. Configure the Cisco ASA appliance for split tunneling.
B. Configure network access exceptions in the SSL VPN customization editor.
C. Configure the Cisco ASA appliance to disable content rewriting.
D. Configure the Cisco ASA appliance to enable URL Entry bypass.
E. Configure smart tunnel to bypass the Cisco ASA appliance proxy function.

Answer: C
Explanation:
http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/user/guide/vpn_web.html

Content Rewrite
The Content Rewrite pane lists all applications for which content rewrite is enabled or disabled. Clientless SSL VPN processes application traffic through a content transformation/rewriting engine thatincludes advanced elements such as JavaScript, VBScript, Java, and multi-byte characters to proxy HTTPtraffic which may have different semantics and access control rules depending on whether the user is using anapplication within or independently of an SSL VPN device.

By default, the security appliance rewrites, or transforms, all clientless traffic. You might not want someapplications and web resources (for example, public websites) to go through the security appliance. Thesecurity appliance therefore lets you create rewrite rules that let users browse certain sites and applicationswithout going through the security appliance. This is similar to split-tunneling in an IPSec VPN connection.

You can create multiple rewrite rules. The rule number is important because the security appliance searchesrewrite rules by order number, starting with the lowest, and applies the first rule that matches.

QUESTION NO: 4

Refer to the exhibit.
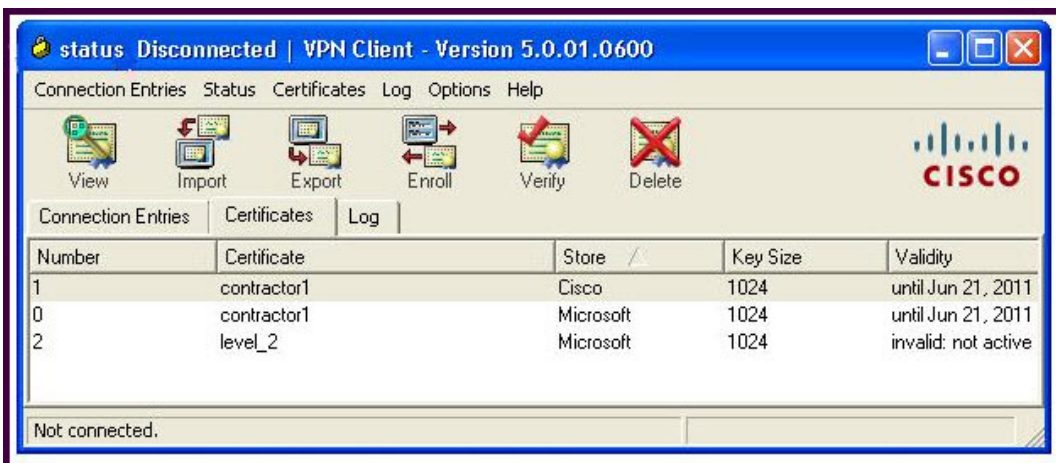
The "level_2" digital certificate was installed on a laptop.

What can cause an "invalid not active" status message?

A. On first use, a CA server-supplied passphrase is entered to validate the certificate.
B. A "newly installed" digital certificate does not become active until it is validated by the peer device upon its first usage.
C. The user has not clicked the Verify button within the Cisco VPN Client.
D. The CA server and laptop PC clocks are out of sync.

Answer: D

Explanation:
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html

Certificates have a date and time that they become valid and that they expire. When the security applianceenrolls with a CA and gets a certificate, the security appliance checks that the current time is within the validrange for the certificate. If it is outside that range, enrollment fails.
Same would apply to communication between ASA and PC

QUESTION NO: 5

Refer to the exhibit.

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.

Answer: D
Explanation:
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 arenot already there, open the Options menu in simple mode and choose Advanced Mode or press Ctrl-M.
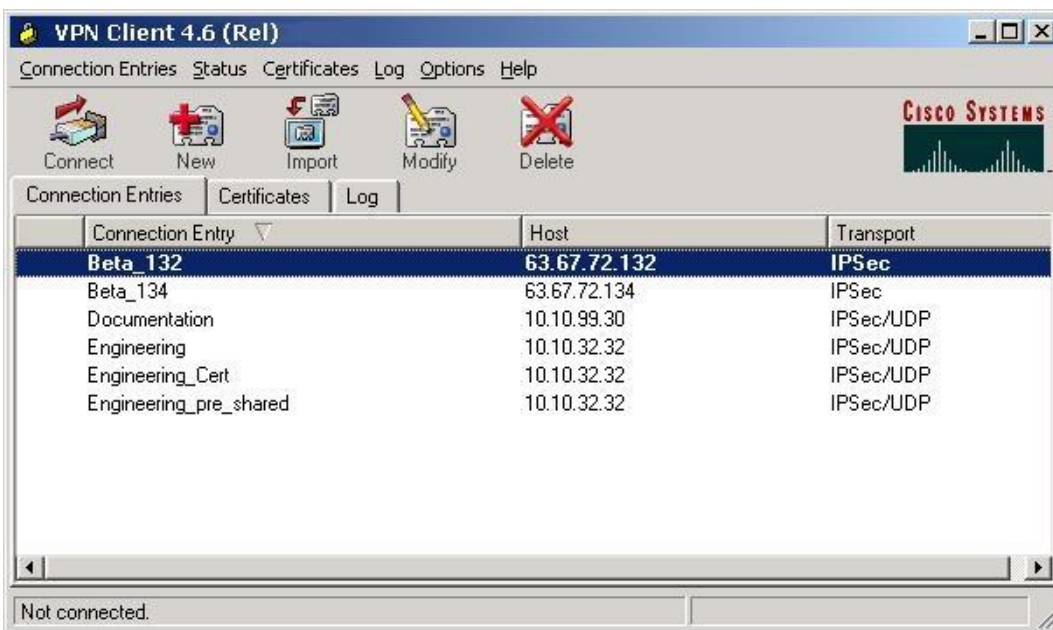
C:\Documents and Settings\user-nwz\Desktop\1.JPG

Step 3 Select New from the toolbar or the Connection Entries menu. The VPN Client displays a form
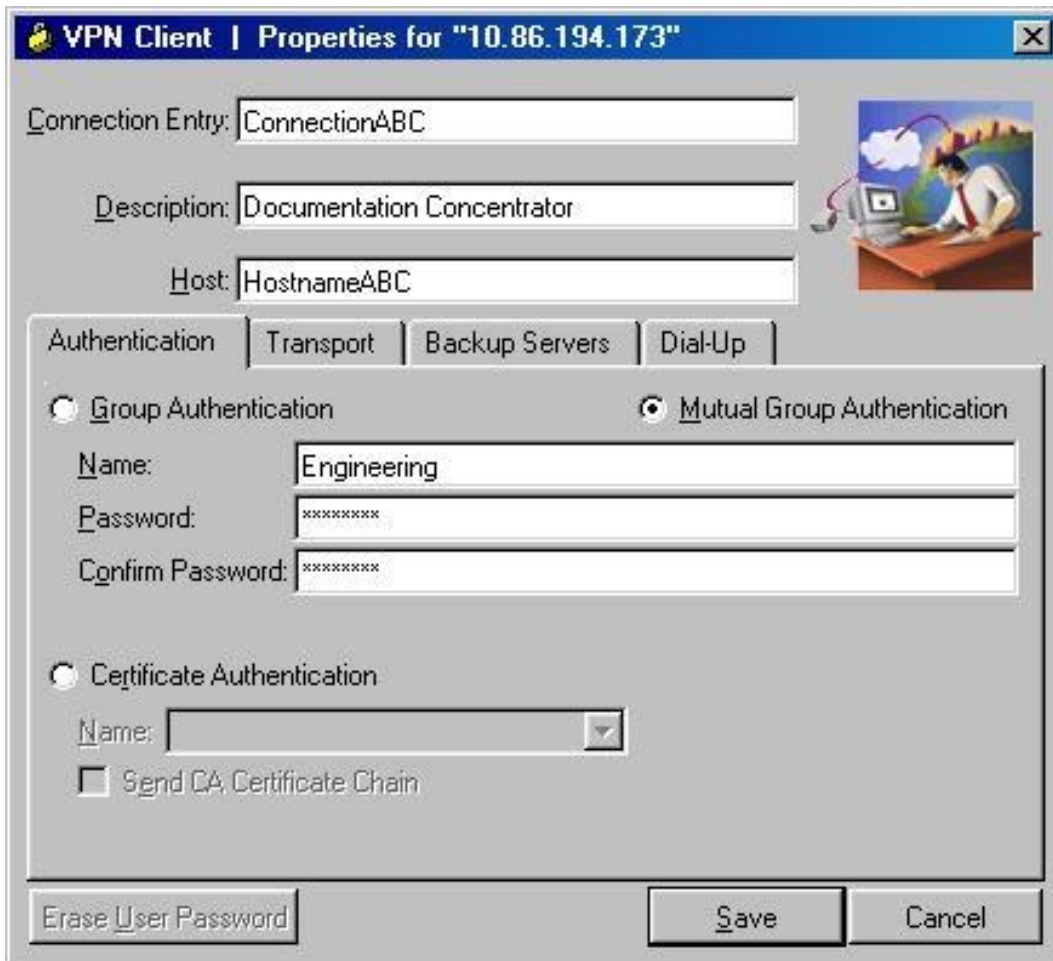
C:\Documents and Settings\user-nwz\Desktop\1.JPG

Step 4 Enter a unique name for this new connection. You can use any name to identify this connection; forexample, 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 thefollowing 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 entryis case-sensitive.

Step 3 In the Password field, enter the password (which is also case-sensitive) for your IPSec group. The fielddisplays only asterisks.

Step 4 Verify your password by entering it again in the Confirm Password field.

QUESTION NO: 6

Refer to the exhibit.
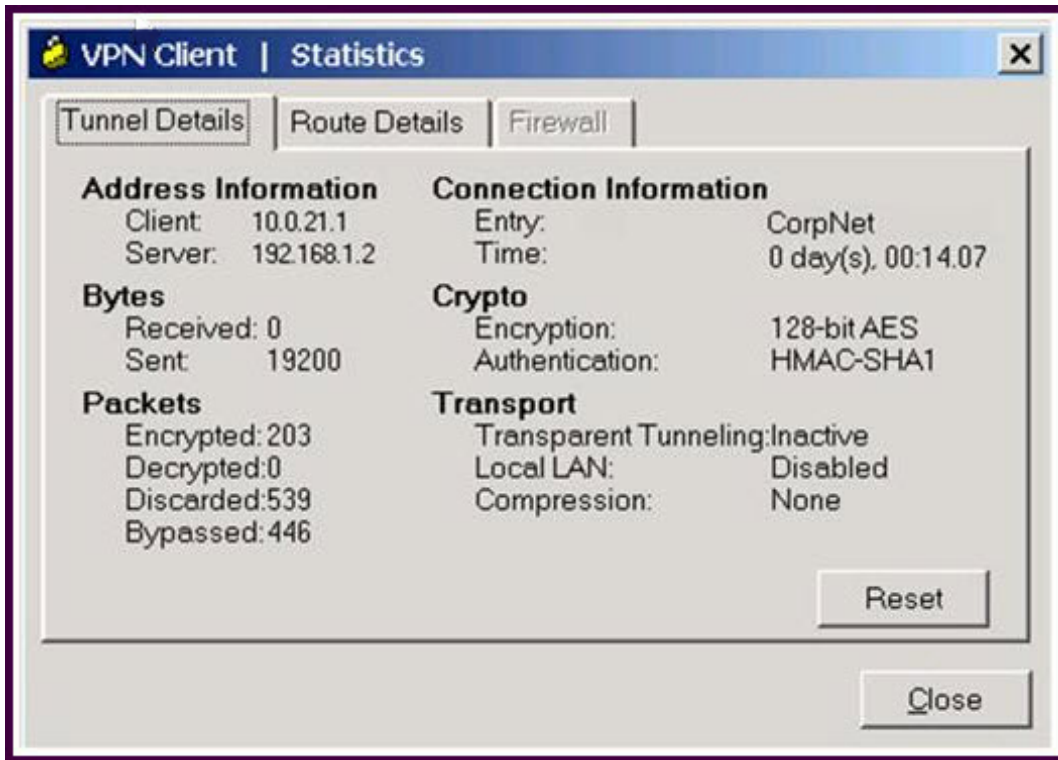
A new NOC engineer is troubleshooting a VPN connection.

Which statement about the fields within the Cisco VPN Client Statistics screen is correct?

A. The ISP-assigned IP address of 10.0.21.1 is assigned to the VPN adapter of the PC.
B. The IP address of the security appliance to which the Cisco VPN Client is connected is 192.168.1.2.
C. CorpNet is the name of the Cisco ASA group policy whose tunnel parameters the connection is using.
D. The ability of the client to send packets transparently and unencrypted through the tunnel for test purposes is turned off.
E. With split tunneling enabled, the Cisco VPN Client registers no decrypted packets.

Answer: B
Explanation:

QUESTION NO: 7

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 did connect 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 should the engineer do?

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: C

Explanation:

IP Security (IPSec) over Transmission Control Protocol (TCP) enables a VPN Client to operate in anenvironment in which standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange(IKE, User Datagram Protocol (UDP) 500) cannot function, or can function only with modification to existingfirewall rules. IPSec over TCP encapsulates both the IKE and IPSec protocols within a TCP packet, and itenables secure tunneling through both Network Address Translation (NAT) and Port Address Translation (PAT)devices and firewalls

QUESTION NO: 8

Refer to the exhibit.