IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

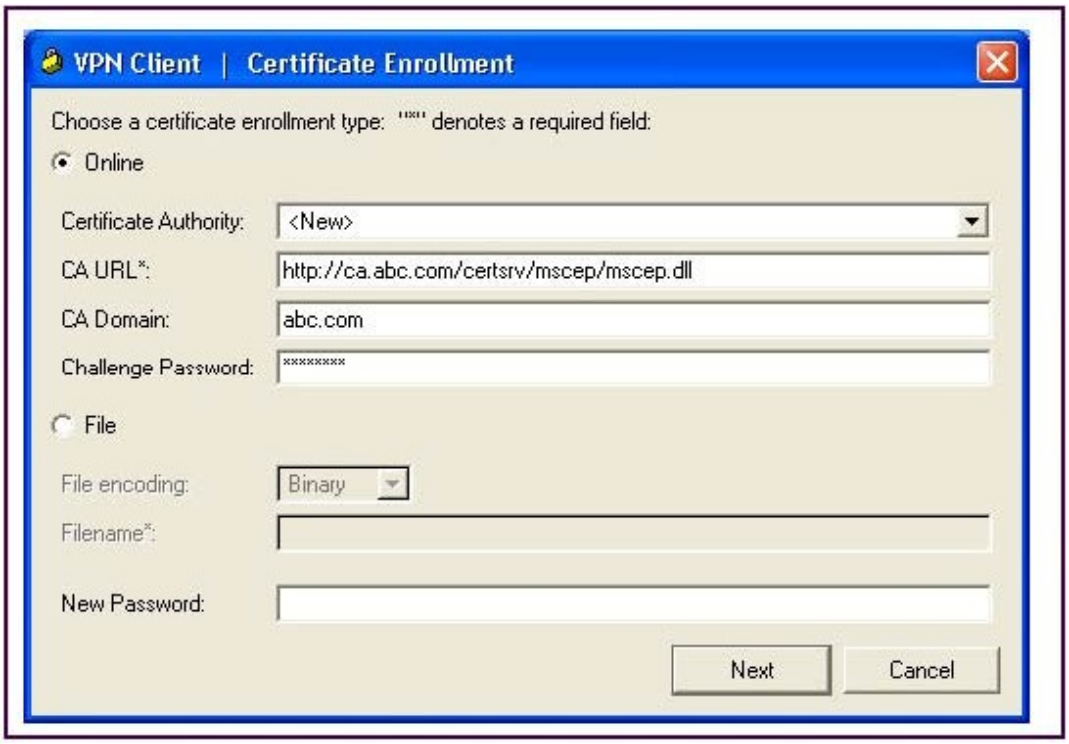
Exam : **642-648**

Title : Deploying Cisco ASA VPN Solutions (VPN v2.0)

Version : DEMO

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/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.

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 certificate that is within its valid time range has been revoked by its issuing CA. CRL configuration is a part of the configuration 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 is unavailable to provide updated CRL data. The security appliance can retrieve CRLs from CAs using HTTP, SCEP, or LDAP. CRLs retrieved for each trustpoint 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 to retrieve a newer version of the CRL the next time a certificate authentication requires checking the stale CRL.

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

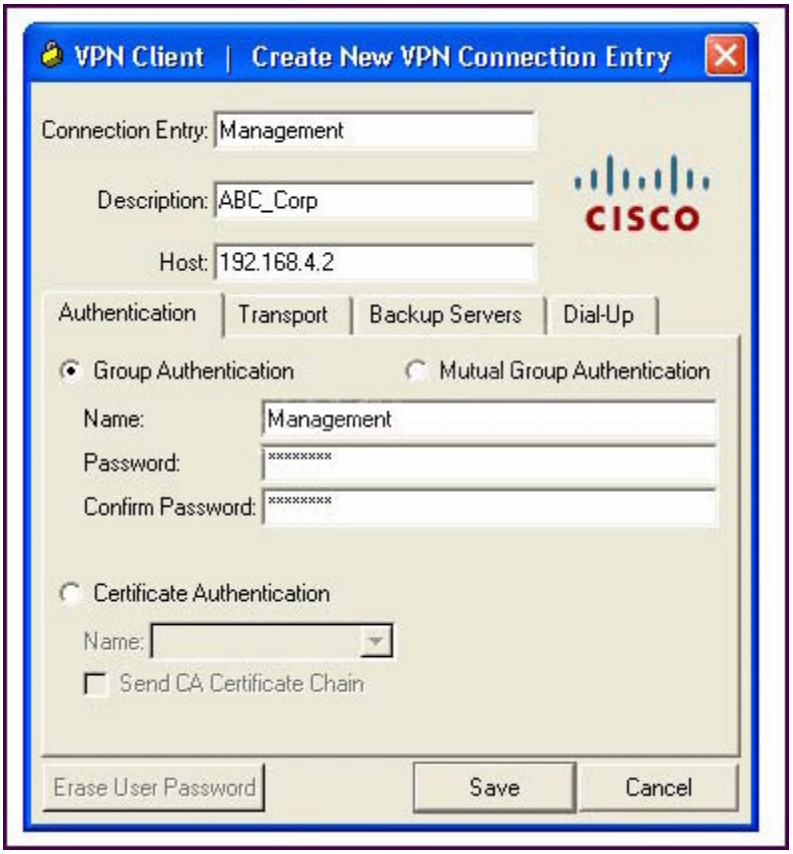
configuration should you use?
A. Configure the Cisco ASA appliance for split tunneling.
B. Configure network access exceptions in the SSL VPN customization editor.
C. Configure the Cisco ASA appliance to disable content rewriting.
D. Configure the Cisco ASA appliance to enable URL Entry bypass.
E. Configure 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 that includes advanced elements such as JavaScript, VBScript, Java, and multi-byte characters to proxy HTTP traffic which may have different semantics and access control rules depending on whether the user is using an application within or independently of an SSL VPN device.
By default, the security appliance rewrites, or transforms, all clientless traffic. You might not want some applications and web resources (for example, public websites) to go through the security appliance. The security appliance therefore lets you create rewrite rules that let users browse certain sites and applications without 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 searches rewrite rules by order number, starting with the lowest, and applies the first rule that matches.

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.

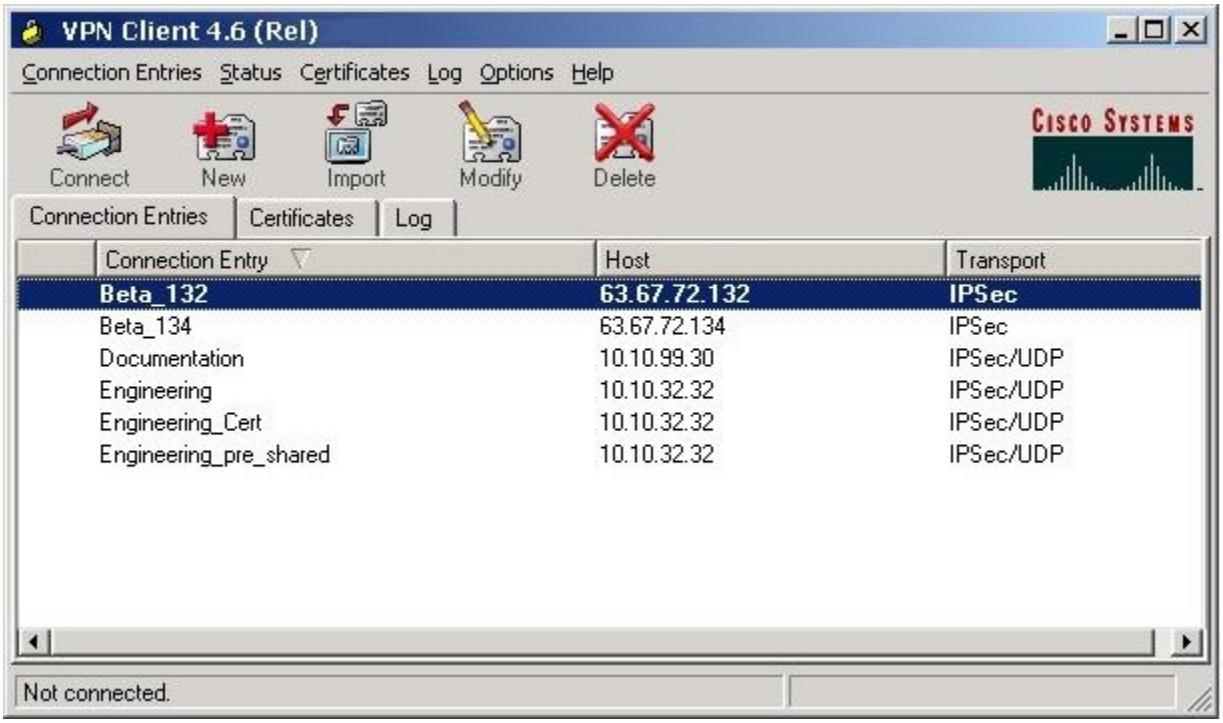
Answer: D
Explanation:
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html
Certificates have a date and time that they become valid and that they expire. When the security appliance enrolls with a CA and gets a certificate, the security appliance checks that the current time is within the valid range for the certificate. If it is outside that range, enrollment fails. Same would apply to communication between ASA and PC

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 41). If you are not already there, open the Options menu in simple mode and choose Advanced Mode or press Ctrl-M.

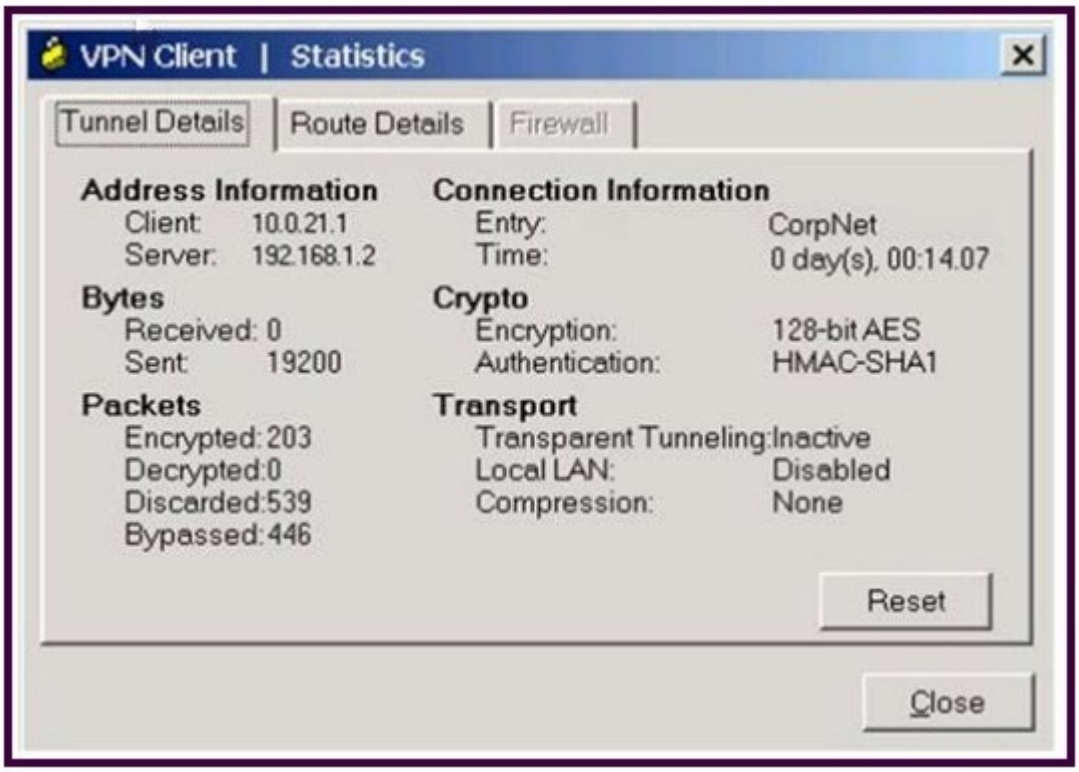


Step 3 Select New from the toolbar or the Connection Entries menu. The VPN Client displays a form

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.

6.Refer to the exhibit.

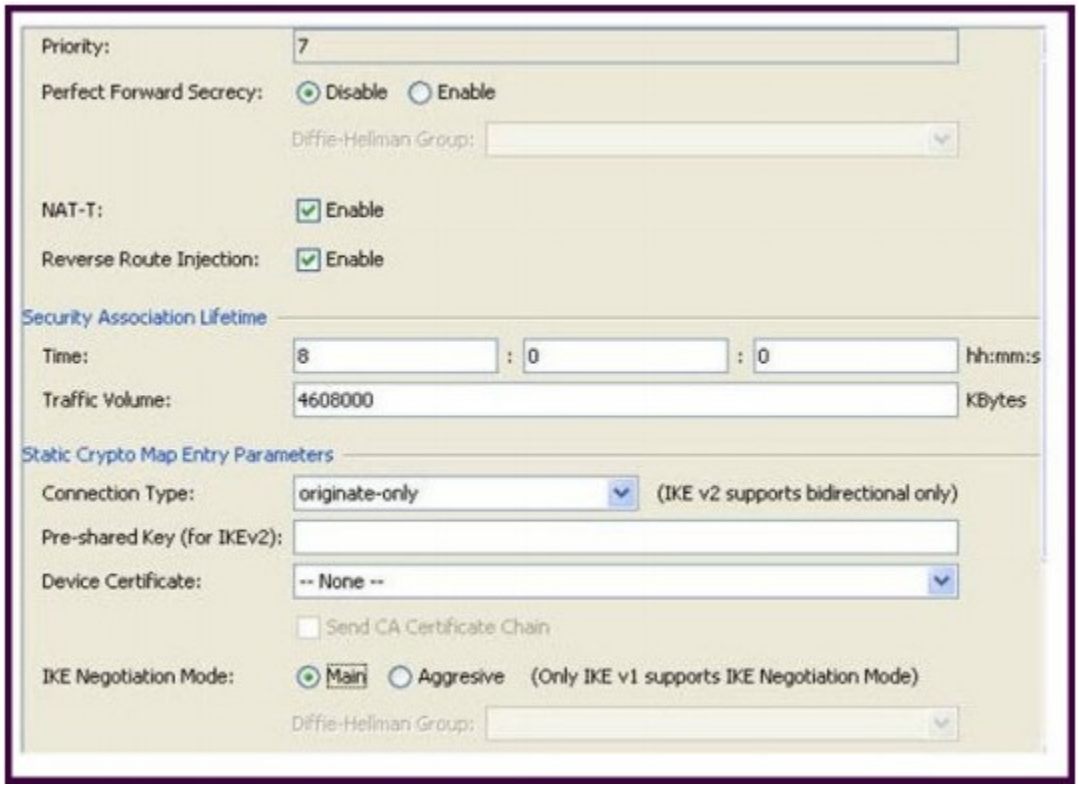


A new NOC engineer is troubleshooting a VPN connection.
Which statement about the fields within the Cisco VPN Client Statistics screen is correct?
A. The ISP-assigned IP address of 10.0.21.1 is assigned to the VPN adapter of the PC.
B. The IP address of the security appliance to which the Cisco VPN Client 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

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 an environment 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 existing firewall rules. IPSec over TCP encapsulates both the IKE and IPSec protocols within a TCP packet, and it enables secure tunneling through both Network Address Translation (NAT) and Port Address Translation (PAT) devices and firewalls

8.Refer to the exhibit.



While configuring a site-to-site VPN tunnel, a new NOC engineer encounters the Reverse Route Injection parameter.
Assuming that static routes are redistributed by the Cisco ASA to the IGP, what effect does enabling Reverse Route Injection on the local Cisco ASA have on a configuration?
A. The local Cisco ASA advertises its default routes to the distant end of the site-to-site VPN tunnel.
B. The local Cisco ASA advertises routes from the dynamic routing protocol that is running on the local Cisco ASA to the distant end of the site-to-site VPN tunnel.
C. The local Cisco ASA advertises routes that are at the distant end of the site-to-site VPN tunnel.

D. The local Cisco ASA advertises routes that are on its side of the site-to-site VPN tunnel to the distant end of the site-to-site VPN tunnel.
Answer: C

9.Refer to the exhibit.

```
ASA5520# show vpn-session anyconnect
Username     : engineer1              Index        : 76
Assigned IP  : 10.0.4.80              Public IP    : 172.26.26.15
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 63506                  Bytes Rx     : 17216
Group Policy : engineering            Tunnel Group : contractor
Login Time   : 11:35:57 UTC Thu Jul 1 2011
Duration     : 0h:01m:52s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : Static                 VLAN         : 100
```

A NOC engineer needs to tune some prelogin parameters on an SSL VPN tunnel.
From the information that is shown, where should the engineer navigate to find the prelogin session attributes?
A. "engineering" Group Policy
B. "contractor" Connection Profile
C. "engineer1" AAA/Local Users
D. DfltGrpPolicy Group Policy
Answer: B

10.Refer to the exhibit.

```
ASA5520# show vpn-session anyconnect
Username     : engineer1              Index        : 76
Assigned IP  : 10.0.4.80              Public IP    : 172.26.26.15
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 63506                  Bytes Rx     : 17216
Group Policy : engineering            Tunnel Group : contractor
Login Time   : 11:35:57 UTC Thu Jul 1 2011
Duration     : 0h:01m:52s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : Static                 VLAN         : 100
```

A NOC engineer needs to tune some postlogin parameters on an SSL VPN tunnel.
From the information shown, where should the engineer navigate to, in order to find all the postlogin session parameters?
A. "engineering" Group Policy
B. "contractor" Connection Profile
C. DefaultWEBVPNGroup Group Policy
D. DefaultRAGroup Group Policy

E. "engineer1" AAA/Local Users

Answer: A

Explanation:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htwebvpn.html#wp1054618

The policy group is a container that defines the presentation of the portal and the permissions for resources that are configured for a group of remote users. Entering the policy group command places the router in webvpn group policy configuration mode. After it is configured, the group policy is attached to the SSL VPN context configuration by configuring the default-group-policy command.

The following tasks are accomplished in this configuration:

11.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 WebVPN login page.

As the Cisco ASA administrator, how would you accomplish this task?

A. Define a special identity certificate with multiple groups, which 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 will appear on the login page.

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

D. Under Connection Profiles, enable "Allow user to select connection profile."

Answer: D

Explanation:

Cisco ASDM User Guide Version 6.1 Add or Edit SSL VPN Connections > Advanced > SSL VPN This dialog box lets you configure attributes that affect what the remote user sees upon login. Fields • Login Page Customization—Configures the look and feel of the user login page by specifying which preconfigured customization attributes to apply. The default is DfltCustomization.

• Manage—Opens the Configure GUI Customization Objects window. • Connection Aliases—Lists in a

table the existing connection aliases and their status and lets you add or delete items in that table. A connection alias appears on the user login page if the connection is configured to allow users to select a particular connection (tunnel group) at login. – Add—Opens the Add Connection Alias window, on which you can add and enable a connection alias. – Delete—Removes the selected row from the connection alias table. There is no confirmation or undo. • Group URLs—Lists in a table the existing group URLs and their status and lets you add or delete items in that table. A group URL appears on the user login page if the connection is configured to allow users to select a particular group at login. – Add—Opens the Add Group URL window, on which you can add and enable a group URL. – Delete—Removes the selected row from the connection alias table. There is no confirmation or undo.

12.Refer to the exhibit.

```
access-list temp_acl webtype permit url http://10.0.4.10
webvpn
 enable outside
 svc enable
 tunnel-group-list enable
group-policy temp_worker internal
group-policy temp_worker attributes
 banner value Welcome Temp Workers!
 vpn-tunnel-protocol webvpn
 vlan 100
 webvpn
  url-list value Corporate_Server
  url-entry disable
group-policy Default attributes
 vpn-tunnel-protocol IPSec svc webvpn
 webvpn
  url-list value Corporate_Server
  filter value temp_acl
username temp1 password cisco
```

```
username temp1 attributes
 vpn-group-policy temp_worker
 vpn-tunnel-protocol webvpn
 group-lock value temp_worker
 service-type remote-access
 webvpn
  file-browsing disable
  file-entry enable
  url-entry disable
 hidden-shares none
  url-list value Corporate_Server
  customization value temp_worker
tunnel-group temp_worker type remote-access
tunnel-group temp_worker general-attributes
 default-group-policy temp_worker
tunnel-group temp_worker webvpn-attributes
 customization temp_worker
 group-alias temp_worker enable
 group-url https://192.168.4.2/temp_worker enable
```

A junior network engineer configured the corporate Cisco ASA appliance to accommodate a new temporary worker. For security reasons, the IT department wants to restrict the internal network access of the new temporary worker to the corporate server, with an IP address of 10.0.4.10. After the junior network engineer finished the configuration, an IT security specialist tested the account of the temporary worker. The tester was able to access the URLs of additional secure servers from the WebVPN user account of the temporary worker.

What did the junior network engineer configure incorrectly?

A. The ACL was configured incorrectly.

B. The ACL was applied incorrectly or was not applied.

C. Network browsing was not restricted on the temporary worker group policy.

D. Network browsing was not restricted on the temporary worker user policy.

Answer: B

13.Your corporate finance department purchased a new non-web-based TCP application tool to run on one of its servers. Certain finance employees need remote access to the software during nonbusiness hours. These employees do not have "admin" privileges to their PCs.

What is the correct way to 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:
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/webvpn.html A smart tunnel is a connection between a TCP-based application and a private site, using a clientless (browser based) SSL VPN session with the security appliance as the pathway, and the security appliance as a proxy server. You can identify applications to which you want to grant smart tunnel access, and specify the local path to each application. For applications running on Microsoft Windows, you can also require a match of the SHA-1 hash of the checksum as a condition for granting smart tunnel access. Lotus SameTime and Microsoft Outlook Express are examples of applications to which you might want to grant smart tunnel access. Configuring smart tunnels requires one of the following procedures, depending on whether the application is a client or is a web-enabled application:
Create one or more smart tunnel lists of the client applications, then assign the list to the group policies or local user policies for whom you want to provide smart tunnel access.
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. You can also list web-enabled applications for which to automate the submission of login credentials in smart tunnel connections over clientless SSL VPN sessions. Why Smart Tunnels? Smart tunnel access lets a client TCP-based application use a browser-based VPN connection to connect to a service. It offers the following advantages to users, compared to plug-ins and the legacy technology, port forwarding:
Smart tunnel offers better performance than plug-ins.
Unlike port forwarding, smart tunnel simplifies the user experience by not requiring the user connection of the local application to the local port.
Unlike port forwarding, smart tunnel does not require users to have administrator privileges. The advantage of a plug-in is that it does not require the client application to be installed on the remote computer. Smart Tunnel Requirements, Restrictions, and Limitations The following sections categorize the smart tunnel requirements and limitations. General Requirements and Limitations Smart tunnel has the following general requirements and limitations:
The remote host originating the smart tunnel must be running a 32-bit version of Microsoft Windows Vista, Windows XP, or Windows 2000; or Mac OS 10.4 or 10.5.
Smart tunnel auto sign-on supports only Microsoft Internet Explorer on Windows.
The browser must be enabled with Java, Microsoft ActiveX, or both.
Smart tunnel supports only proxies placed between computers running Microsoft Windows and the security appliance. Smart tunnel uses the Internet Explorer configuration (that is, the one intended for system-wide use in Windows). If the remote computer requires a proxy server to reach the security appliance, the URL of the terminating end of the connection must be in the list of URLs excluded from proxy services. If the proxy configuration specifies that traffic destined for the ASA goes through a proxy, all smart tunnel traffic goes through the proxy.
In an HTTP-based remote access scenario, sometimes a subnet does not provide user access to the VPN gateway. In this case, a proxy placed in front of the ASA to route traffic between the web and the end

user's location provides web access. However, only VPN users can configure proxies placed in front of the ASA.
When doing so, they must make sure these proxies support the CONNECT method. For proxies that require authentication, smart tunnel supports only the basic digest authentication type.
When smart tunnel starts, the security appliance by default passes all browser traffic through the VPN session if the browser process is the same. The security appliance also does this if a tunnel-all policy applies. If the user starts another instance of the browser process, it passes all traffic through the VPN session. If the browser process is the same and the security appliance does not provide access to a URL, the user cannot open it. As a workaround, assign a tunnel policy that is not tunnel-all.
A stateful failover does not retain smart tunnel connections. Users must reconnect following a failover.

14.Which statement about plug-ins is false?
A. Plug-ins do not require any installation on the remote system.
B. Plug-ins require administrator privileges on the remote system.
C. Plug-ins support interactive terminal access.
D. Plug-ins are not supported on the Windows Mobile platform.
Answer: B
Explanation:
http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deployhtml#wp1162435
Plug-ins
The security appliance supports Java plug-ins for clientless SSL VPN connections. Plug-ins are Java programs that operate in a browser. These plug-ins include SSH/Telnet, RDP, VNC, and Citrix. Per the GNU General Public License (GPL), Cisco redistributes plug-ins without making any changes to them. Per the GPL, Cisco cannot directly enhance these plug-ins. To use plug-ins you must install Java Runtime Environment (JRE) 1.4.2.x or greater. You must also use a compatible browser specified here:
http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpncompatibility.html

15.A temporary worker must use clientless SSL VPN with an SSH plug-in, in order to access the console of an internal corporate server, the projects.xyz.com server. For security reasons, the network security auditor insists that the temporary user is restricted to the one internal corporate server, 10.0.4.18. You are the network engineer who is responsible for the network access of the temporary user.
What should you do to restrict SSH access to the one projects.xyz.com server?
A. Configure access-list temp_user_acl extended permit TCP any host 10.0.4.18 eq 22.
B. Configure access-list temp_user_acl standard permit host 10.0.4.18 eq 22.
C. Configure access-list temp_acl webtype permit url ssh://10.0.4.18.
D. Configure a plug-in SSH bookmark for host 10.0.4.18, and disable network browsing on the clientless SSL VPN portal of the temporary worker.
Answer: C
Explanation: Web ACLs
The Web ACLs table displays the filters configured on the security appliance applicable to Clientless SSL VPN traffic. The table shows the name of each access control list (ACL), and below and indented to the right of the ACL name, the access control entries (ACEs) assigned to the ACL. Each ACL permits or denies access permits or denies access to specific networks, subnets, hosts, and web servers. Each ACE

specifies one rule that serves the function of the ACL. You can configure ACLs to apply to Clientless SSL VPN traffic. The following rules apply: • If you do not configure any filters, all connections are permitted. • The security appliance supports only an inbound ACL on an interface. • At the end of each ACL, an implicit, unwritten rule denies all traffic that is not explicitly permitted. You can use the following wildcard characters to define more than one wildcard in the Webtype access list entry: • Enter an asterisk "°"¡± t match no characters or any number of characters. • Enter a question mark "° "¡± to natch any one characte exactly. • Enter square brackets "ſ"¡± to cr eate a r ange operato t hat nat ches any one chara cte in a r ange The following examples show how to use wildcards in Webtype access lists. • The following example matches URLs such as http://www.cisco.com/ and http://wwz.caco.com/: access-list test webtype permit url http://ww?.c*co*/

16.Authorization of a clientless SSL VPN defines the actions that a user may perform within a clientless SSL VPN session. Which statement is correct concerning the SSL VPN authorization process?
A. Remote clients can be authorized by applying a dynamic access policy, which is configured on an external AAA server.
B. Remote clients can be authorized externally by applying group parameters from an external database.
C. Remote client authorization is supported by RADIUS and TACACS+ protocols.
D. To configure external authorization, you must configure the Cisco ASA for cut-through proxy.
Answer: B

17.After adding a remote-access IPsec tunnel via the VPN wizard, an administrator needs to tune the IPsec policy parameters.
Where is the correct place to tune the IPsec policy parameters in Cisco ASDM?
A. IPsec user profile
B. Crypto Map
C. Group Policy
D. IPsec Policy
E. IKE Policy
Answer: B
Explanation:

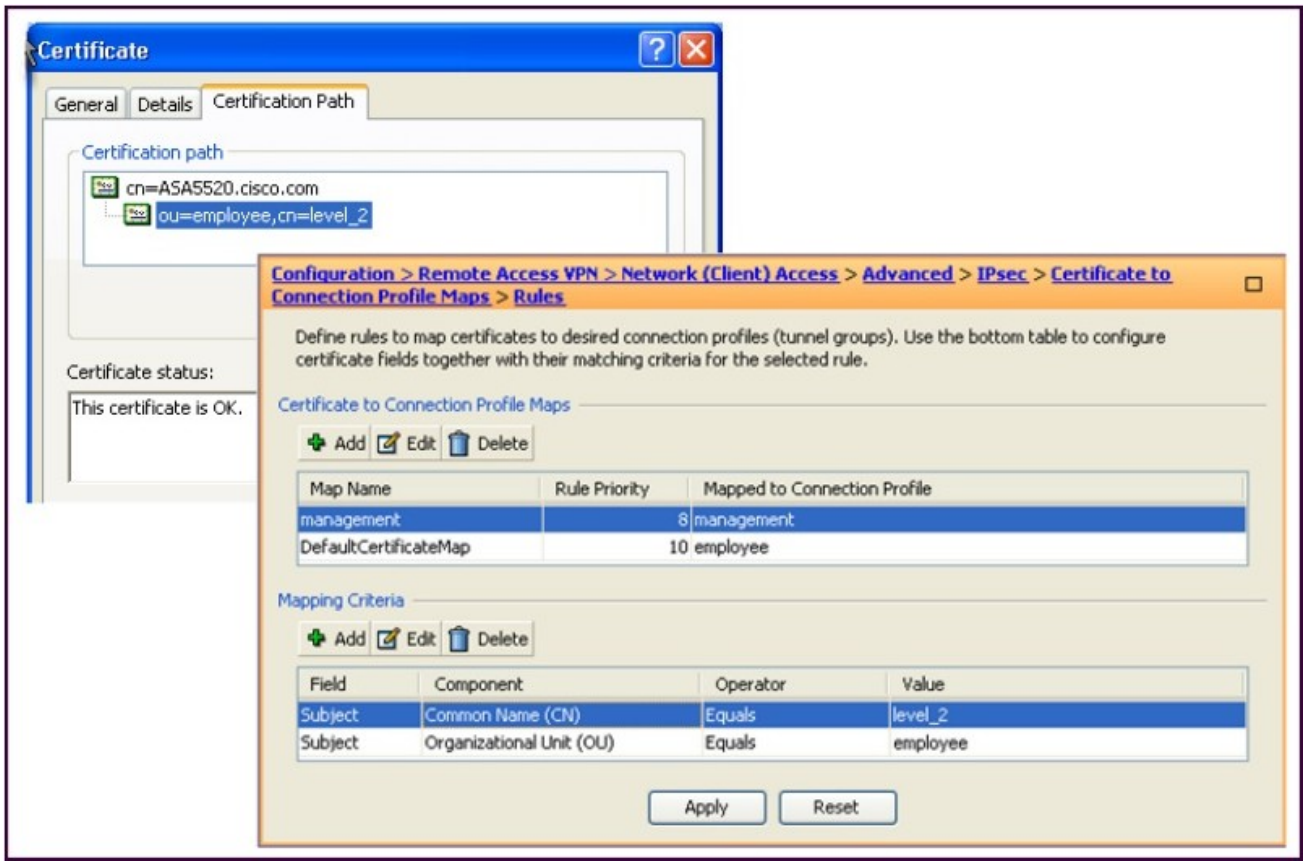
18.Refer to the exhibit.

%ASA-5-713259: Group = contractor, Username = vpnuser, IP = 172.16.1.20, Session is being torn down. Reason: Phase 2 Mismatch

While troubleshooting a remote-access application, a new NOC engineer received the logging message that is shown in the exhibit.
Which configuration is most likely to be mismatched?
A. IKE configuration
B. extended authentication configuration
C. IPsec configuration
D. digital certificate configuration
Answer: C
Explanation:
http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a00800949c5.shtmlan
d %ASA-5-713259: Group = groupname, Username = username, IP = peerIP, Session is being torn down.

Reason: reason Explanation The termination reason for the ISAKMP session appears, which occurs when the session is torn down through session management.
groupname—The tunnel group of the session being terminated
username—The username of the session being terminated
peerIP—The peer address of the session being terminated
reason—The RADIUS termination reason of the session being terminated. Reasons include the following:
-Port Preempted (simultaneous logins)
-Idle Timeout
-Max Time Exceeded
-Administrator Reset

19.Refer to the exhibit.



The ABC Corporation is changing remote-user authentication from pre-shared keys to certificate-based authentication. For most employee authentication, its group membership (the employees) governs corporate access. Certain management personnel need access to more confidential servers. Access is based on the group and name, such as finance and level_2. When it is time to pilot the new authentication policy, a finance manager is able to access the department-assigned servers but cannot access the restricted servers.
As the network engineer, where would you look for the problem?
A. Check the validity of the identity and root certificate on the PC of the finance manager.
B. Change the Management Certificate to Connection Profile Maps > Rule Priority to a number that is greater than 10.
C. Check if the Management Certificate to Connection Profile Maps > Rules is configured correctly.

D. Check if the Certificate to Connection Profile Maps > Policy is set correctly.

Answer: D

Explanation:

Cisco ASDM User Guide Version 6.1

To configure the evaluation of IPSec or SSL VPN connections against certificate criteria-based rules, use the IPSec Certificate to Connection Maps > Rules or Certificate to SSL VPN Connections Profile Maps panel.

This panel lets you create the certificate-based criteria for each IPSec and SSL VPN connection profile, as follows:

Step 1 Use the table at the top (Certificate to Connection Profile Maps) to do one of the following:

- Create a list name, called a "map," specify the priority of the list, and assign the list to a connection profile.

  ASDM highlights the list after you add it to the table.
- Confirm that a list is assigned to the connection profile for which you want to add certificate-based rules.

  ASDM highlights the list after you add it to the table and displays any associated list entries in the table at the bottom of the pane.

Step 2 Use the table at the bottom (Mapping Criteria) to view, add, change or delete entries to the selected list.

Each entry in the list consists of one certificate-based rule. All of the rules in the mapping criteria list need to match the contents of the certificate for the security appliance to choose the associated map index. To assign a connection if one criterion or another matches, create one list for each matching criterion.

20.Refer to the exhibit.

The user "contractor" inherits which VPN group policy?

A. employee

B. management

C. DefaultWEBVPNGroup

D. DfltGrpPolicy

E. new_hire

Answer: D