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:

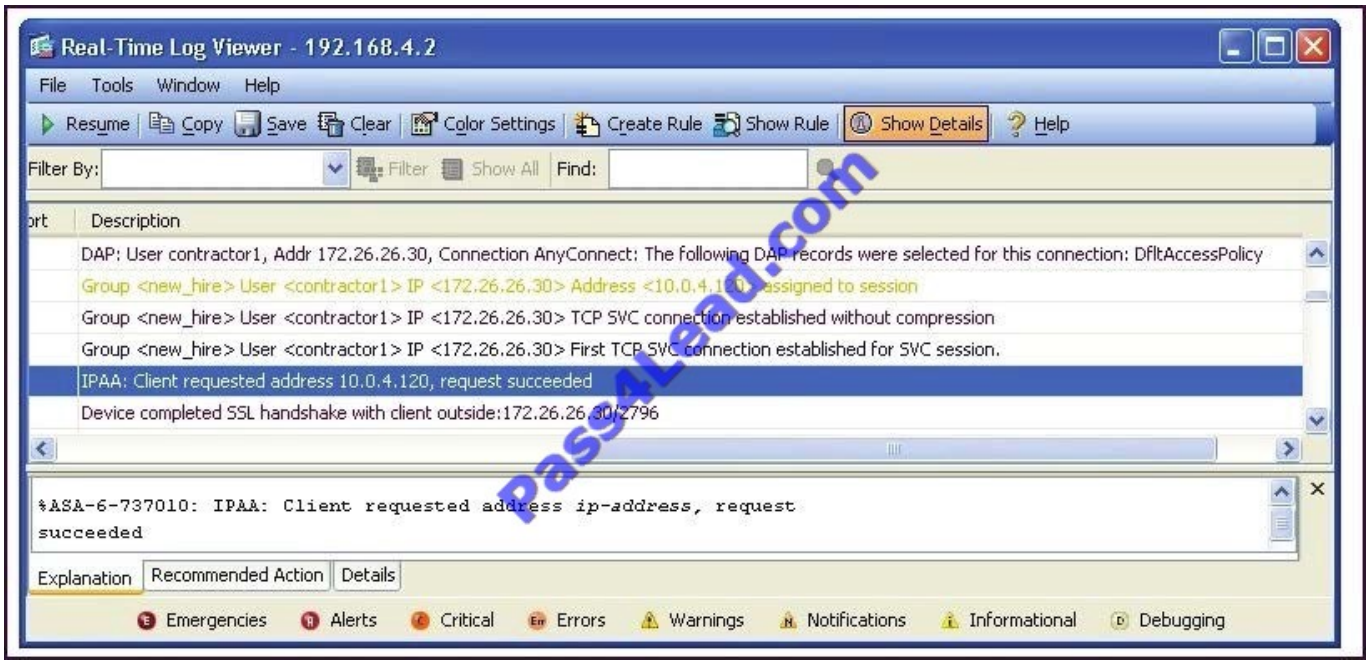
https://www.pass4lead.com/642-648.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Refer to the exhibit.



After being with the company for more than six months, Sue is no longer considered a new hire employee. In converting her from a new hire to a full-time employee, her SSL VPN address will change from the "Client requested address 10.0.4.120" to a random address from the employee address pool.

To "disable" the 10.0.4.120 IP address, the network administrator should navigate to which Cisco ASDM pane?

A. Connection Profile

B. Group Policies

C. Local Users

D. Address Pools

Correct Answer: C

Users are assigned IP addresses based on the address pool associated with their group. Change group of Sue to use employee address pool

Add/Edit Tunnel Group > General > Advanced

The Add or Edit Tunnel Group window, General, Advanced dialog box, lets you configure the following interface-specific attributes:

- Interface-Specific Authentication Server Groups—Lets you configure an interface and server group for authentication.
  - Interface—Lists available interfaces for selection.
  - Server Group—Lists authentication server groups available for this interface.
  - Use LOCAL if server group fails—Enables or disables fallback to the LOCAL database if the server group fails.
  - Add—Adds the association between the selected available interface and the authentication server group to the assigned list.
  - Remove—Moves the selected interface and authentication server group association from the assigned list to the available list.
  - Interface/Server Group/Use Fallback—Show the selections you have added to the assigned list.
- Interface-Specific Client IP Address Pools—-Lets you specify an interface and Client IP address pool. You can have up to 6 pools.
  - Interface—Lists the available interfaces to add.
  - Address Pool—Lists address pools available to associate with this interface.
  - Add—Adds the association between the selected available interface and the client IP address pool to the assigned list.
  - Remove—Moves the selected interface/address pool association from the assigned list to the available list.
  - Interface/Address Pool—Shows the selections you have added to the assigned list.

QUESTION 2

Refer to the exhibit.

```
http://server/homepage/CSCO_WEBVPN_USERNAME.html
ssh://sshserver/?csco_sso=1
```

Which two statements are correct regarding these two Cisco ASA clientless SSL VPN bookmarks? (Choose two.)

A. CSCO_WEBVPN_USERNAME is a user attribute.

B. CSCO_WEBVPN_USERNAME is a Cisco predefined variable that is used for macro substitution.

C. The CSCO_WEBVPN_USERNAME variable is enabled by using the Post SSO plug-in.

D. CSCO_SSO is a Cisco predefined variable that is used for macro substitution.

E. The CSCO_SSO=1 parameter enables SSO for the SSH plug-in.

F. The CSCO_SSO variable is enabled by using the Post SSO plug-in.

Correct Answer: BE

http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html

Introduction to URL Variable Substitution:

Your configuration will most likely require personalized resources that contain the username and password, for example, in URL lists or in group URLs. URL variable substitution lets the remote user enter username and password credentials

once, when initiating the session, then login automatically to internal resources such as

Citrix, OWA, Sharepoint, and the internal portal.

Clientless SSL VPN supports the following macro substitutions:

CSCO_WEBVPN_USERNAME--User login name

CSCO_WEBVPN_PASSWORD--Obtained from user login password
CSCO_WEBVPN_INTERNAL_PASSWORD--Obtained from the Internal password field. You can use this field as Domain for Single Signon operations.

CSCO_WEBVPN_CONNECTION_PROFILE--User login group drop-down (tunnel group alias)

CSCO_WEBVPN_MACRO1--Set via Radius or LDAP vendor specific attribute CSCO_WEBVPN_MACRO2--Set via Radius or LDAP vendor specific attribute Each time the security appliance recognizes one of these strings in an end-user

request, it replaces the string with the user-specific value before passing the request to a remote server.

For example, a URL list that contains the link:

http://someserver/homepage/CSCO_WEBVPN_USERNAME.

Html is translated by the security appliance to the following links for SSL VPN USER1 and USER2:

http://someserver/homepage/USER1.html

http://someserver/homepage/USER2.html

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

Datagram Transport Layer Security (DTLS) was introduced to solve performance issues. Choose three characteristics of DTLS. (Choose three.)

A. It uses TLS to negotiate and establish DTLS connections.

B. It uses DTLS to transmit datagrams.

C. It is disabled by default.

D. It uses TLS for data packet retransmission.

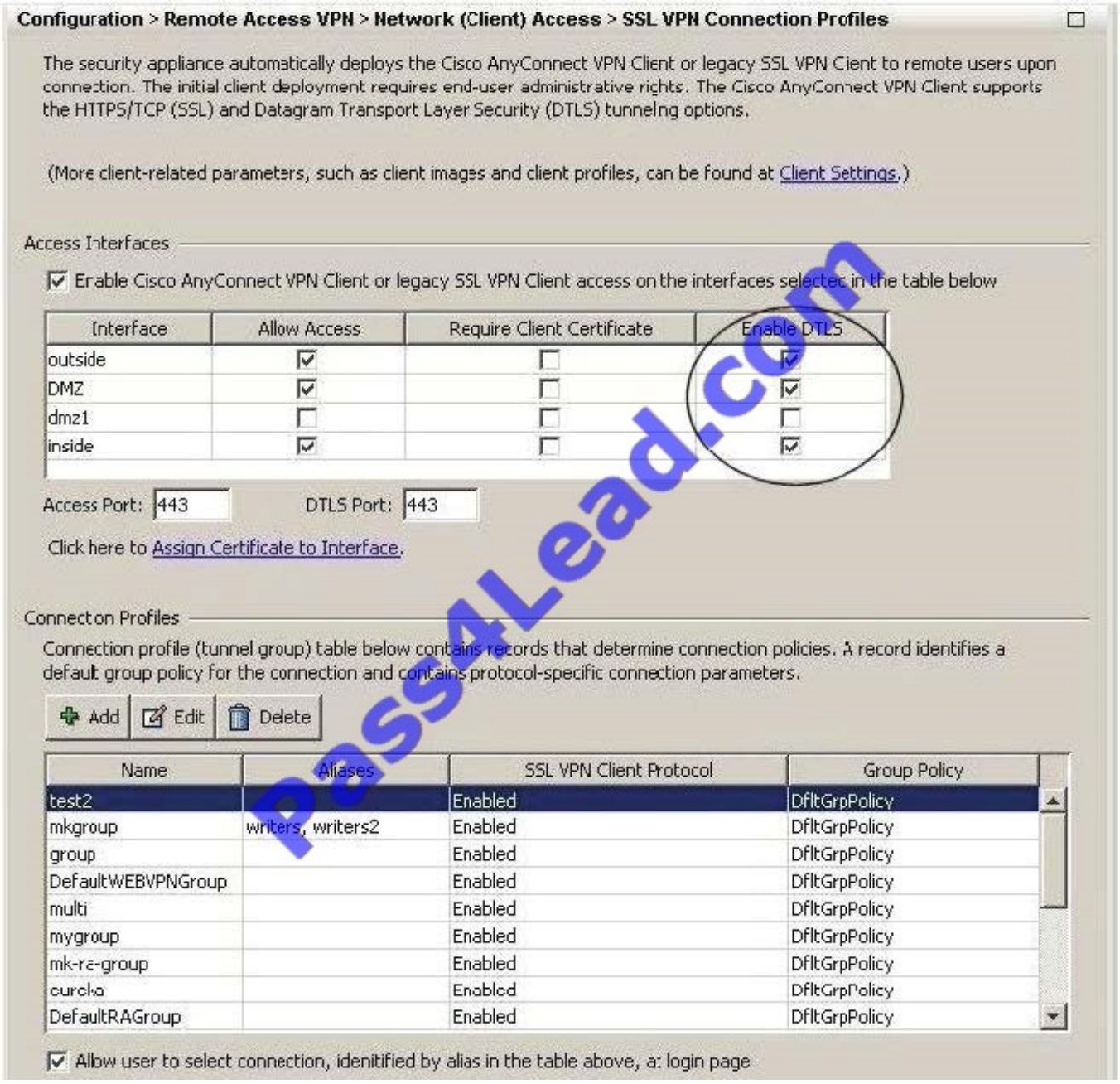
E. It replaces underlying transport layer with UDP 443.

F. It uses TLS to provide low-latency video application tunneling.

Correct Answer: ABE

http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect23/administration/23admin2.html#wp1029596

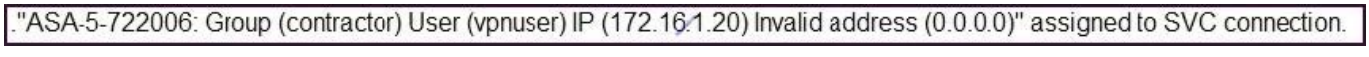
Enabling Datagram Transport Layer Security (DTLS) with AnyConnect (SSL) Connections Datagram Transport Layer Security avoids latency and bandwidth problems associated with some SSL-only connections, including AnyConnect connections, and improves the performance of real-time applications that are sensitive to packet delays. DTLS is a standards-based SSL protocol that provides a low-latency data path using UDP. For detailed information about DTLS, see RFC 4347 (http://www.ietf.org/rfc/rfc4347.txt). Datagram Transport Layer Security (DTLS) allows the AnyConnect client establishing an SSL VPN connection to use two simultaneous tunnels--an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays. If you do not enable DTLS, AnyConnect/SSL VPN connections connect with an SSL VPN tunnel only. You cannot enable DTLS globally with ASDM. The following section describes how to enable DTLS for any specific interface. To enable DTLS for a specific interface, select Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN Connection profiles. The SSL VPN Connection Profiles dialog box opens (Figure 2-3).Figure 2-3 Enable DTLS Check Box



Enabling Datagram Transport Layer Security (DTLS) allows the AnyConnect VPN Client establishing an SSL VPN connection to use two simultaneous tunnels--an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of realtime applications that are sensitive to packet delays. If you do not enable DTLS, AnyConnect client users establishing SSL VPN connections connect with an SSL VPN tunnel only. Fields ?Interface--Displays a list of interfaces on the security appliance. ?DTLS Enabled--Check to enable DTLS connections with the AnyConnect client on the interfaces. ?UDP Port (default 443)--(Optional) Specify a separate UDP port for DTLS connections.

QUESTION 5

Refer to the exhibit.



While troubleshooting on a remote-access VPN application, a new NOC engineer received the message that is shown. What is the most likely cause of the problem?

A. The IP address that is assigned to the PC of the VPN user is not within the range of addresses that are assigned to the SVC connection.

B. The IP address that is assigned to the PC of the VPN user is in use. The remote user needs to select a different host address within the range.

C. The IP address that is assigned to the PC of the VPN user is in the wrong subnet. The remote user needs to select a different host number within the correct subnet.

D. The IP address pool for contractors was not applied to their connection profile.

Correct Answer: D

%ASA-5-722006: Group group User user-name IP IP_address Invalid address IP_address assigned to SVC connection. An invalid address was assigned to the user. Recommended Action Verify and correct the address assignment, if possible.

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: