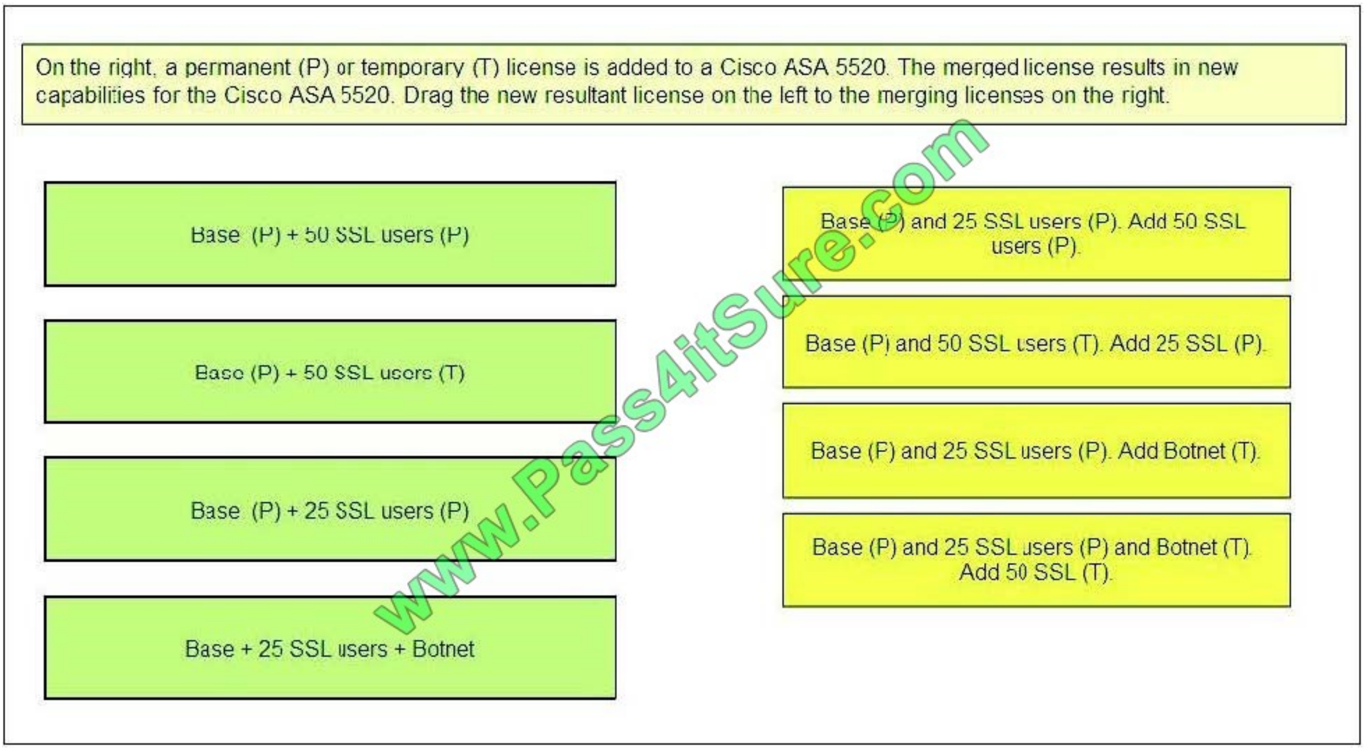
642-648 Q&As

Deploying Cisco ASA VPN Solutions (VPN v2.0)

QUESTION 1

On the right, a permanent (P) or temporary (T) license is added to a Cisco ASA 5520. The merged license result in new capabilities for the Cisco ASA 5520. Drag the new resultant license on the left to the merging licenses on the right.

Select and Place:



On the right, a permanent (P) or temporary (T) license is added to a Cisco ASA 5520. The merged license results in new capabilities for the Cisco ASA 5520. Drag the new resultant license on the left to the merging licenses on the right.

Base (P) + 50 SSL users (P)

Base (P) + 50 SSL users (T)

Base (P) + 25 SSL users (P)

Base + 25 SSL users + Botnet

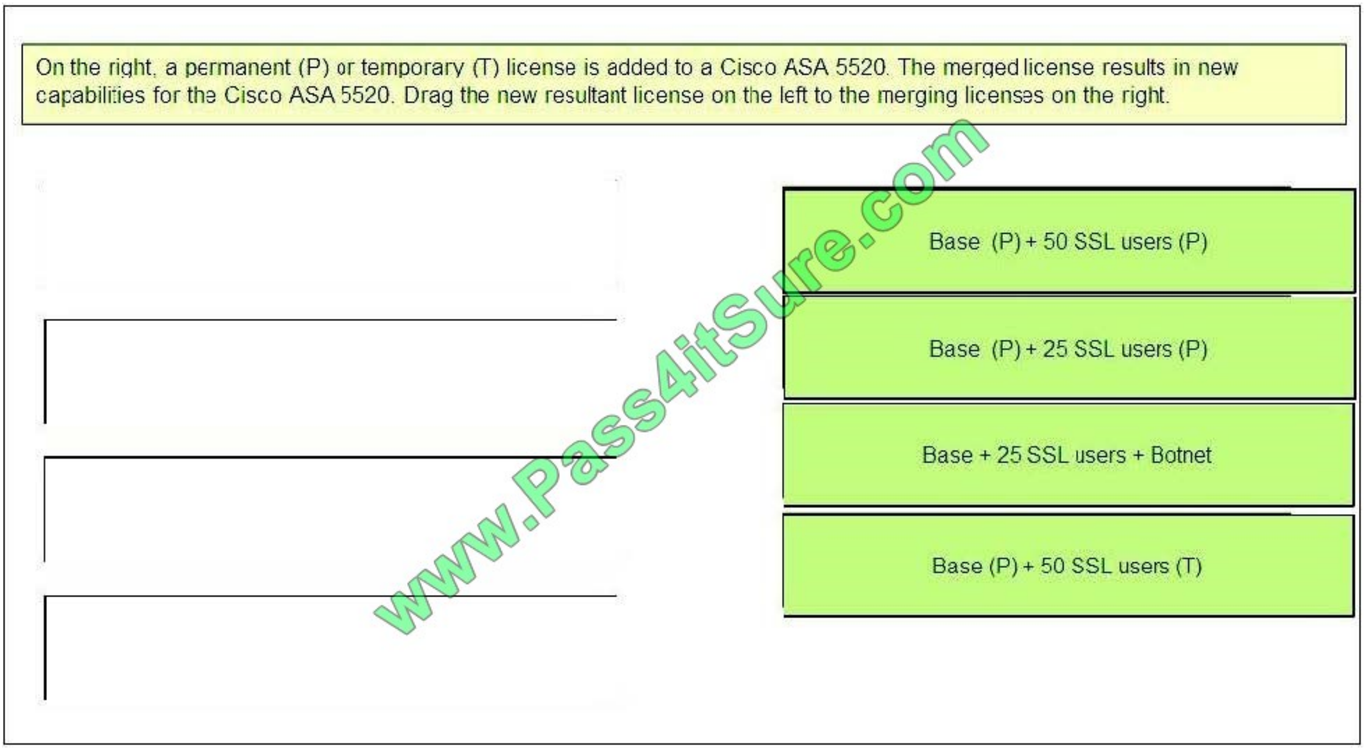
Base (P) and 25 SSL users (P). Add 50 SSL users (P).

Base (P) and 50 SSL users (T). Add 25 SSL (P).

Base (F) and 25 SSL users (P). Add Botnet (T).

Base (P) and 25 SSL users (P) and Botnet (T). Add 50 SSL (T).

Correct Answer:



On the right, a permanent (P) or temporary (T) license is added to a Cisco ASA 5520. The merged license results in new capabilities for the Cisco ASA 5520. Drag the new resultant license on the left to the merging licenses on the right.

Base (P) + 50 SSL users (P)

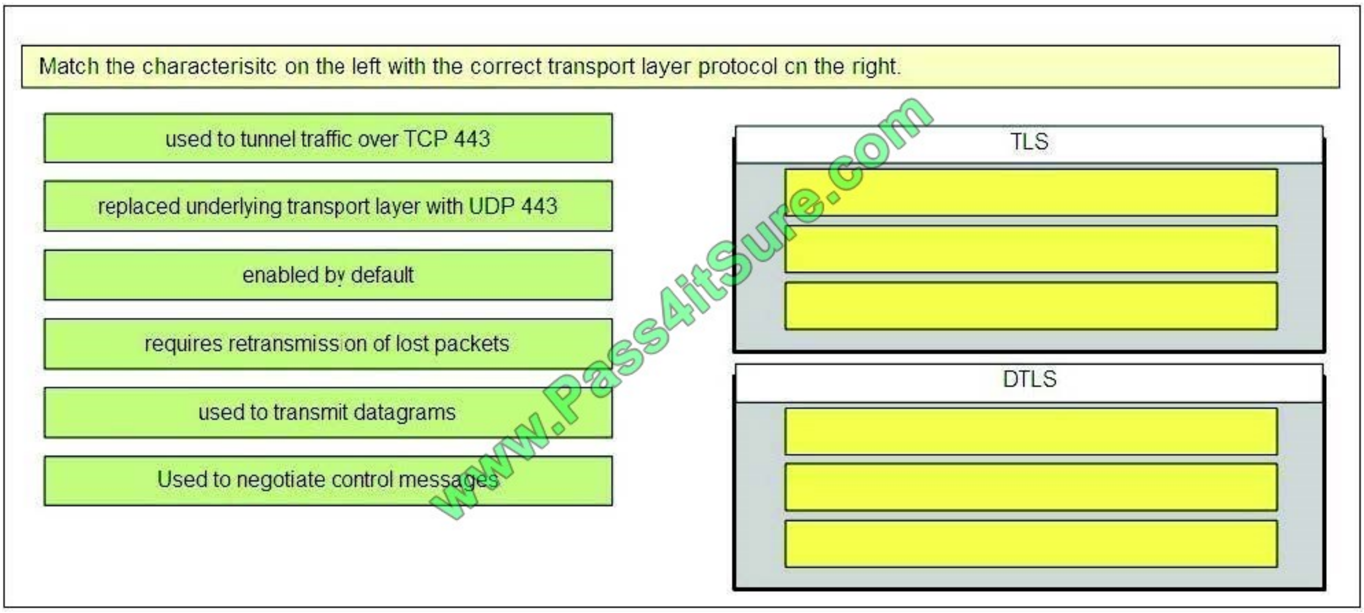
Base (P) + 25 SSL users (P)

Base + 25 SSL users + Botnet

Base (P) + 50 SSL users (T)

QUESTION 2

Select and Place:



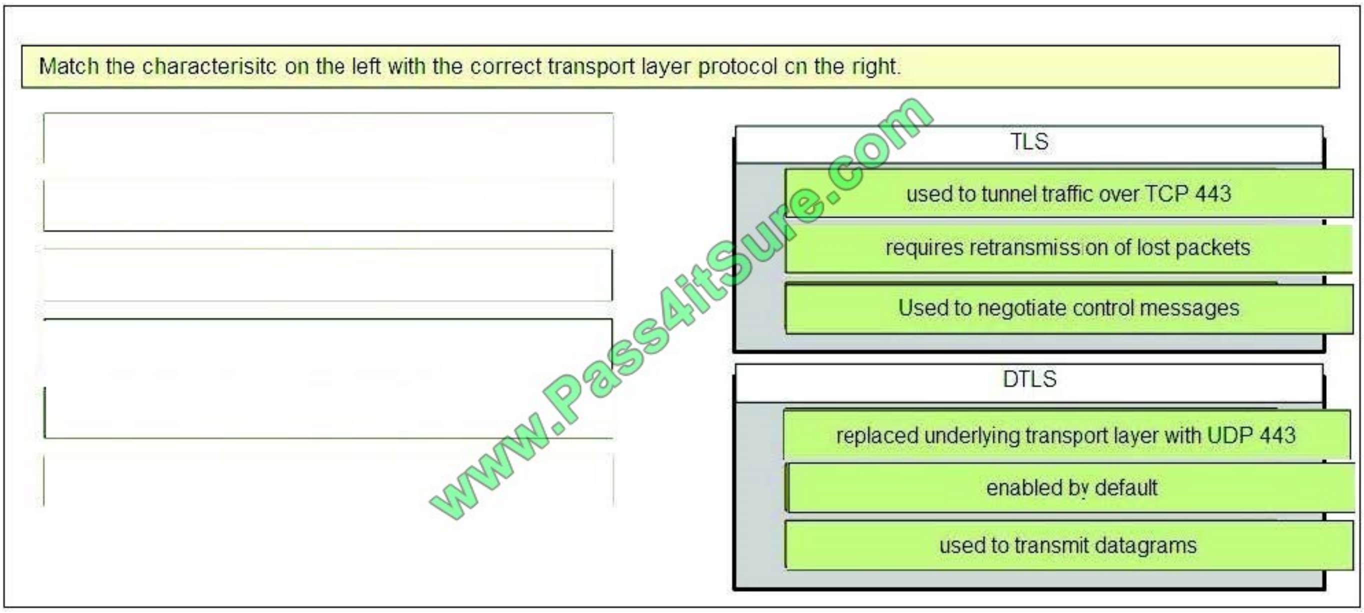
Match the characterisitc on the left with the correct transport layer protocol cn the right.

- used to tunnel traffic over TCP 443
- replaced underlying transport layer with UDP 443
- enabled by default
- requires retransmission of lost packets
- used to transmit datagrams
- Used to negotiate control messages

TLS

DTLS

Correct Answer:



Match the characterisitc on the left with the correct transport layer protocol cn the right.

TLS

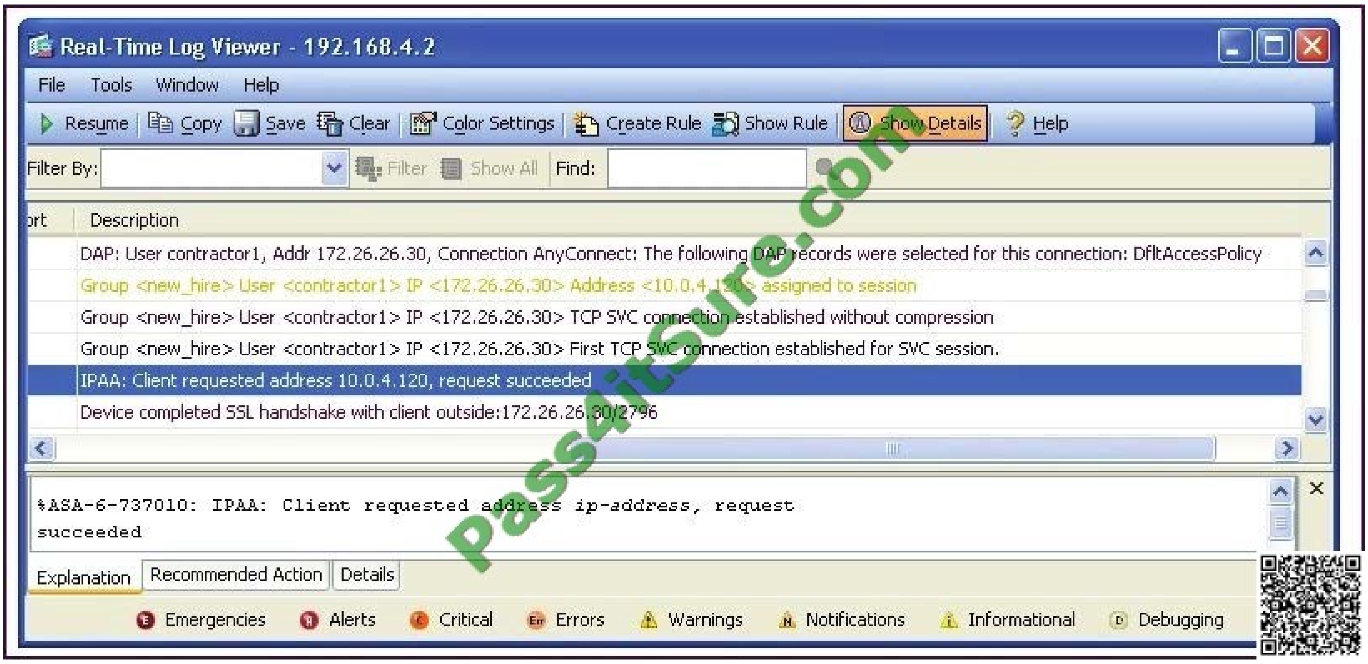
- used to tunnel traffic over TCP 443
- requires retransmiss on of lost packets
- Used to negotiate control messages

DTLS

- replaced underlying transport layer with UDP 443
- enabled by default
- used to transmit datagrams

QUESTION 3

Refer to the exhibit.



Real-Time Log Viewer - 192.168.4.2
File Tools Window Help
Resume Copy Save Clear Color Settings Create Rule Show Rule Show Details Help
Filter By: Filter Show All Find:
ort Description

```
DAP: User contractor1, Addr 172.26.26.30, Connection AnyConnect: The following DAP records were selected for this connection: DfltAccessPolicy
Group <new_hire> User <contractor1> IP <172.26.26.30> Address <10.0.4.120> assigned to session
Group <new_hire> User <contractor1> IP <172.26.26.30> TCP SVC connection established without compression
Group <new_hire> User <contractor1> IP <172.26.26.30> First TCP SVC connection established for SVC session.
IPAA: Client requested address 10.0.4.120, request succeeded
Device completed SSL handshake with client outside:172.26.26.30/2796
```

```
%ASA-6-737010: IPAA: Client requested ip-address, request
succeeded
```

Explanation Recommended Action Details
Emergencies Alerts Critical Errors Warnings Notifications Informational Debugging

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

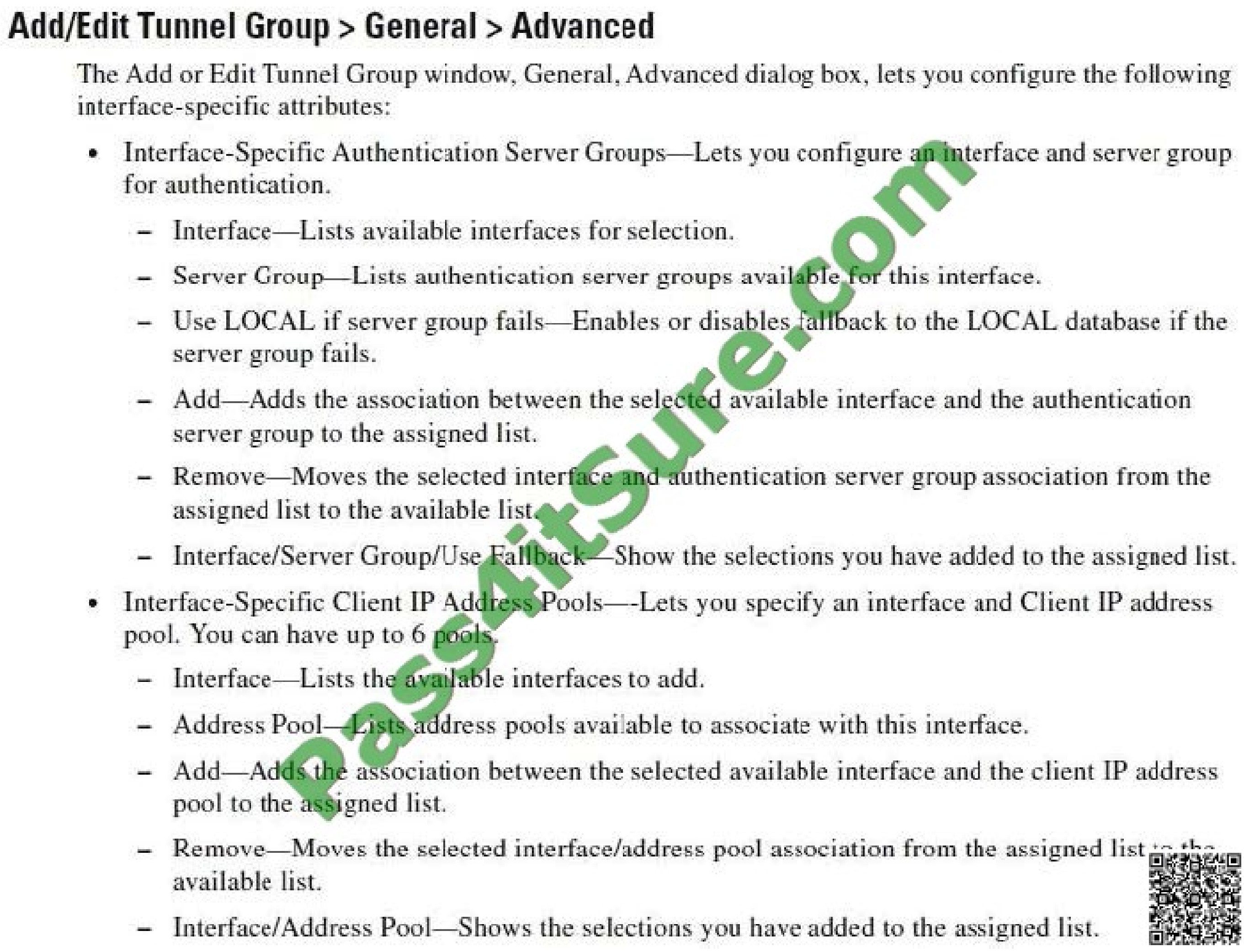
B. Group Policies

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 4

When deploying remote-access IPsec VPN tunnels, what is the key benefit of digital certificates?

A. resiliency

B. simplification

C. scalability

D. centralization

Correct Answer: C

QUESTION 5

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 6

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

Correct Answer: B

QUESTION 7

Which statement is true about configuring the Cisco ASA for Active/Standby failover?

A. All versions of Cisco ASA software need to have the same licensing on both devices.

B. Both devices perform load sharing until a failure occurs.

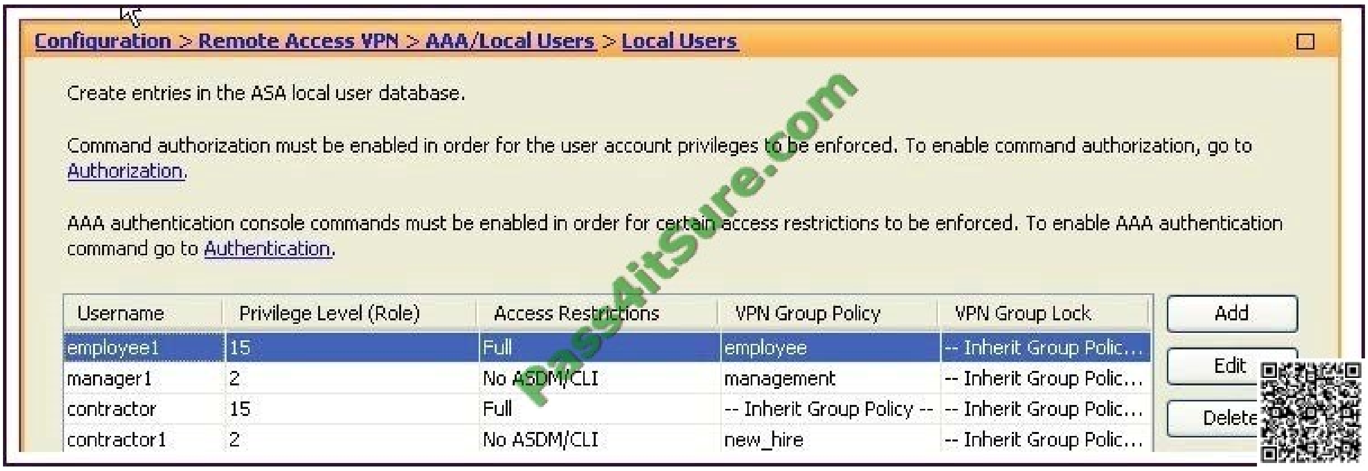
C. All VPN-related configurations and files are automatically replicated.

D. VPN images, profiles, and plug-ins must be manually provisioned to both devices.

Correct Answer: D

QUESTION 8

Refer to the exhibit.



Configuration > Remote Access VPN > AAA/Local Users > Local Users

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to Authorization.

AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to Authentication.

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock
employee1	15	Full	employee	-- Inherit Group Polic...
manager1	2	No ASDM/CLI	management	-- Inherit Group Polic...
contractor	15	Full	-- Inherit Group Policy --	-- Inherit Group Polic...
contractor1	2	No ASDM/CLI	new_hire	-- Inherit Group Polic...

The user "contractor" inherits which VPN group policy?

A. employee

B. management

C. DefaultWEBVPNGroup

D. DfltGrpPolicy

E. new_hire

Correct Answer: D

QUESTION 9

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.

Correct Answer: A

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:?reate 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. ?reate 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:?mart tunnel offers better performance than plug-ins. ?nlike port forwarding, smart tunnel simplifies the user experience by not requiring the user connection of the local application to the local port. ?nlike 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:?he 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. ?mart tunnel auto sign-on supports only Microsoft Internet Explorer on Windows. ?he browser must be enabled with Java, Microsoft ActiveX, or both. ?mart 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.

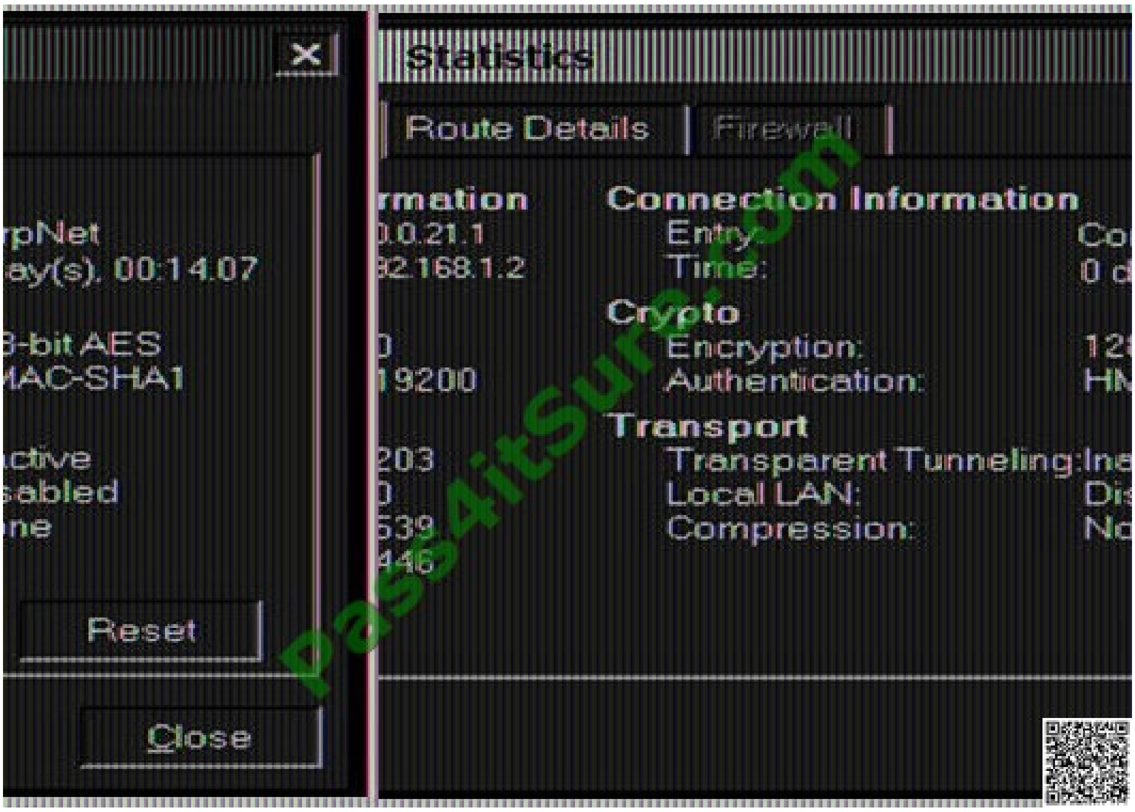
In an HTTP-based remote access scenario, sometimes a subnet does not provide user access to the VPN gateway. In this case, a proxy placed in front of the ASA to route traffic between the web and the end user\\'s location provides web access. However, only VPN users can configure proxies placed in front 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. ?hen 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.

? stateful failover does not retain smart tunnel connections. Users must reconnect following a failover.

QUESTION 10

Refer to the exhibit.



```
rpNet                     rmation       Connection Information
ay(s). 00:14.07           0.0.21.1         Entry:                        Co
                          92.168.1.2       Time:                         0 d
                                          Crypto
8-bit AES                 0                Encryption:                   12
MAC-SHA1                  19200            Authentication:               HM
                                          Transport
ctive                     203              Transparent Tunneling:Ina
sabled                    0                Local LAN:                    Dis
ne                        539              Compression:                  No
                          446
```

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.

Correct Answer: B

QUESTION 11

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.

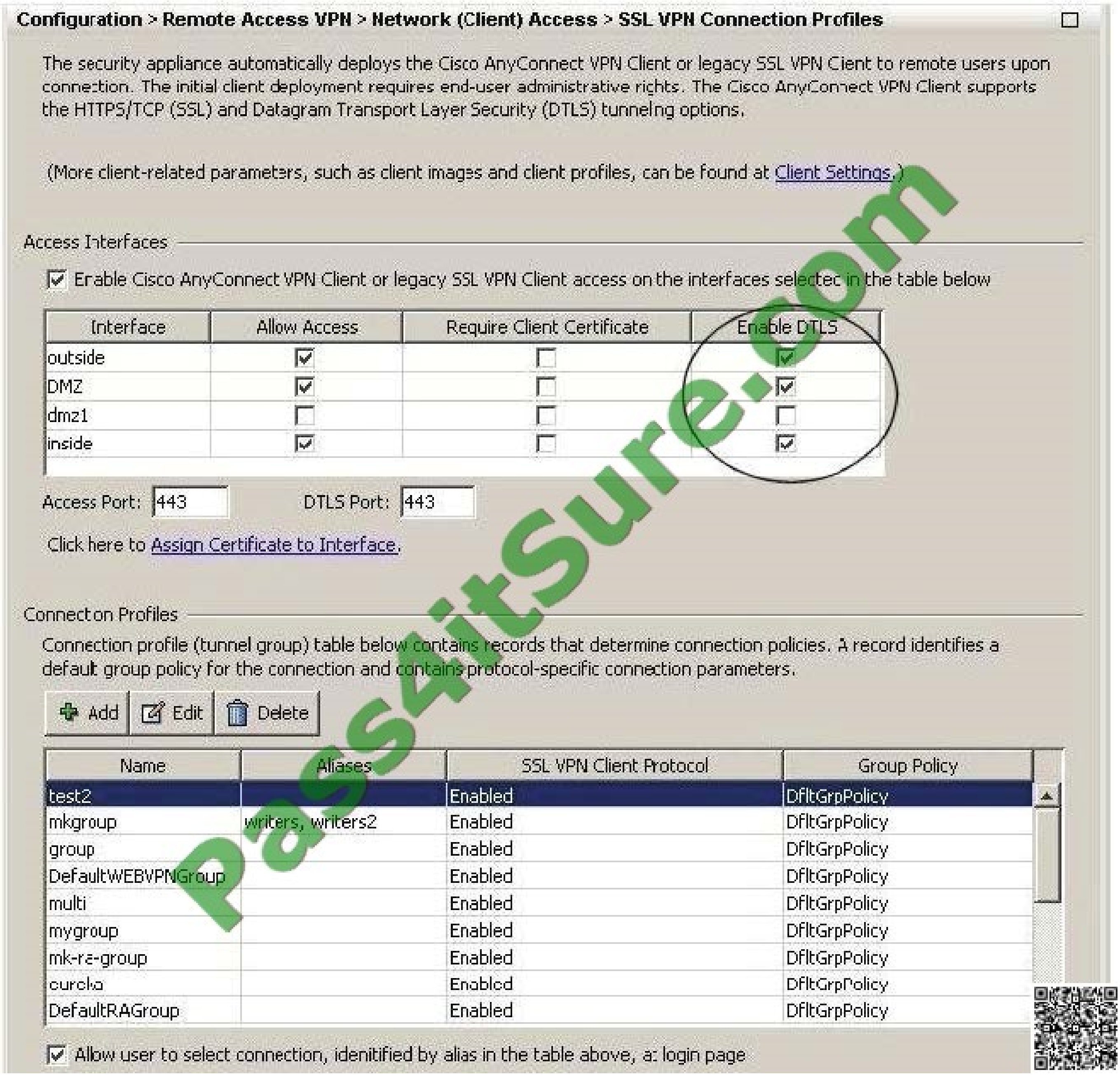
E. It replaces underlying transport layer with UDP 443.

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



Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the HTTPS/TCP (SSL) and Datagram Transport Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at Client Settings.)

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below

Interface	Allow Access	Require Client Certificate	Enable DTLS
outside	☑	□	☑
DMZ	☑	□	☑
dmz1	□	□	□
inside	☑	□	☑

Access Port: 443 DTLS Port: 443

Click here to Assign Certificate to Interface.

Connection Profiles

Connection profile (tunnel group) table below contains records that determine connection policies. A record identifies a default group policy for the connection and contains protocol-specific connection parameters.

Name	Aliases	SSL VPN Client Protocol	Group Policy
test2		Enabled	DfltGrpPolicy
mkgroup	writers, writers2	Enabled	DfltGrpPolicy
group		Enabled	DfltGrpPolicy
DefaultWEBVPNGroup		Enabled	DfltGrpPolicy
multi		Enabled	DfltGrpPolicy
mygroup		Enabled	DfltGrpPolicy
mk-ra-group		Enabled	DfltGrpPolicy
eureka		Enabled	DfltGrpPolicy
DefaultRAGroup		Enabled	DfltGrpPolicy

☑ Allow user to select connection, idenitified by alias in the table above, at login page

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 12

While configuring a new clientless SSL VPN group in Cisco ASDM, the administrator chooses to accept a number of the default parameter values. The administrator decides to view the actual value for the parameter, rather than just checking the inherit box.

Under which default group can the administrator verify the default value for the group parameter?

A. DefaultRAGroup

B. DefaultWEBVPNGroup

C. DfltGrpPolicy

D. DefaultSVCGroup

Correct Answer: C

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

Try our product !

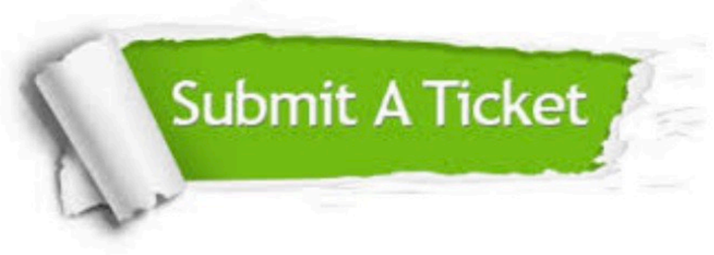
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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:



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.
All trademarks are the property of their respective owners.