642-648Q&As

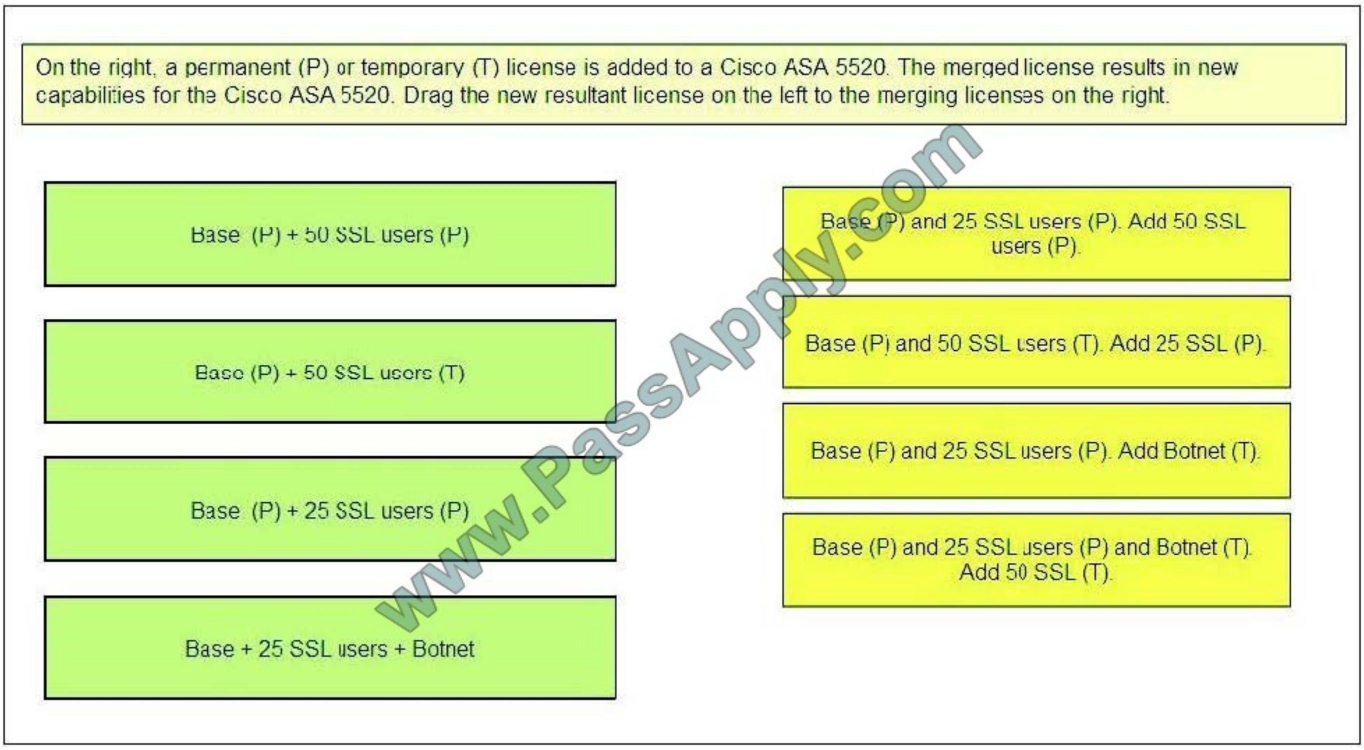
Deploying Cisco ASA VPN Solutions (VPN v2.0)

Pass Cisco 642-648 Exam with 100% Guarantee

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.

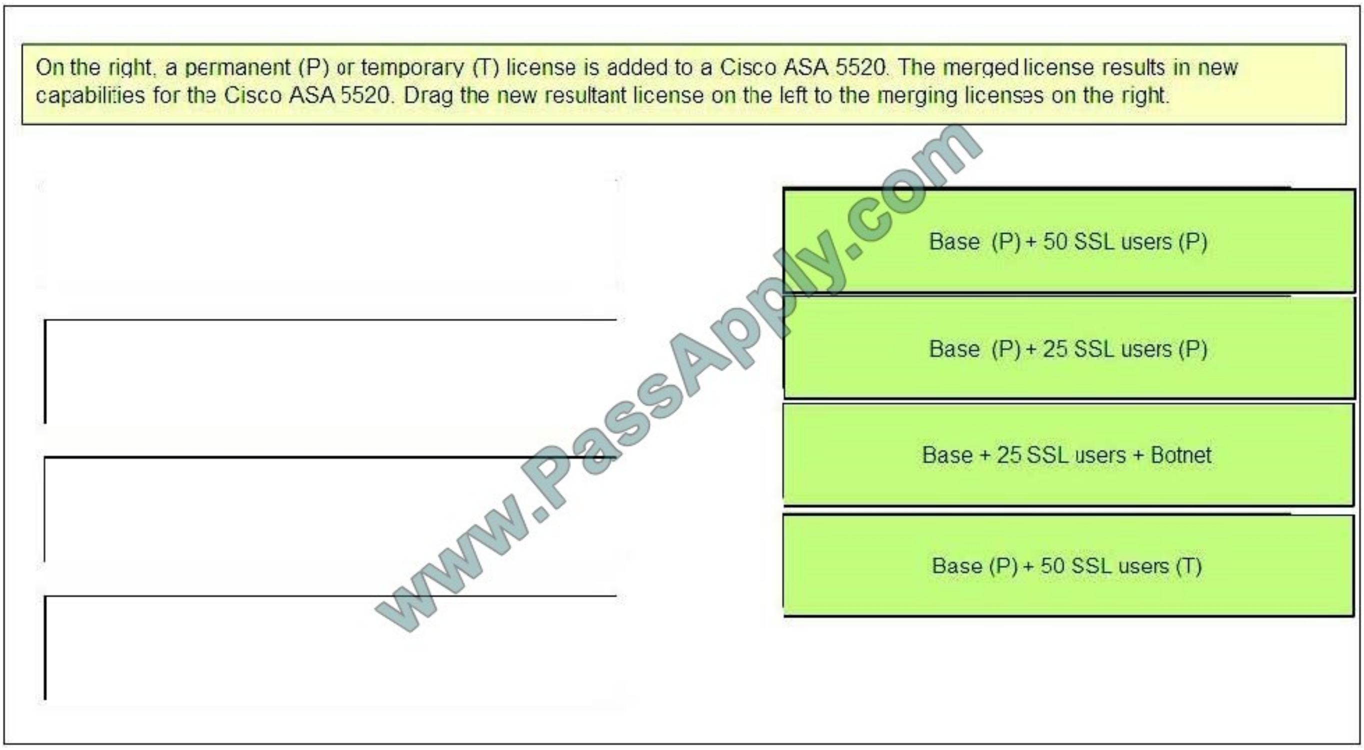
Select and Place:



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

Correct Answer:

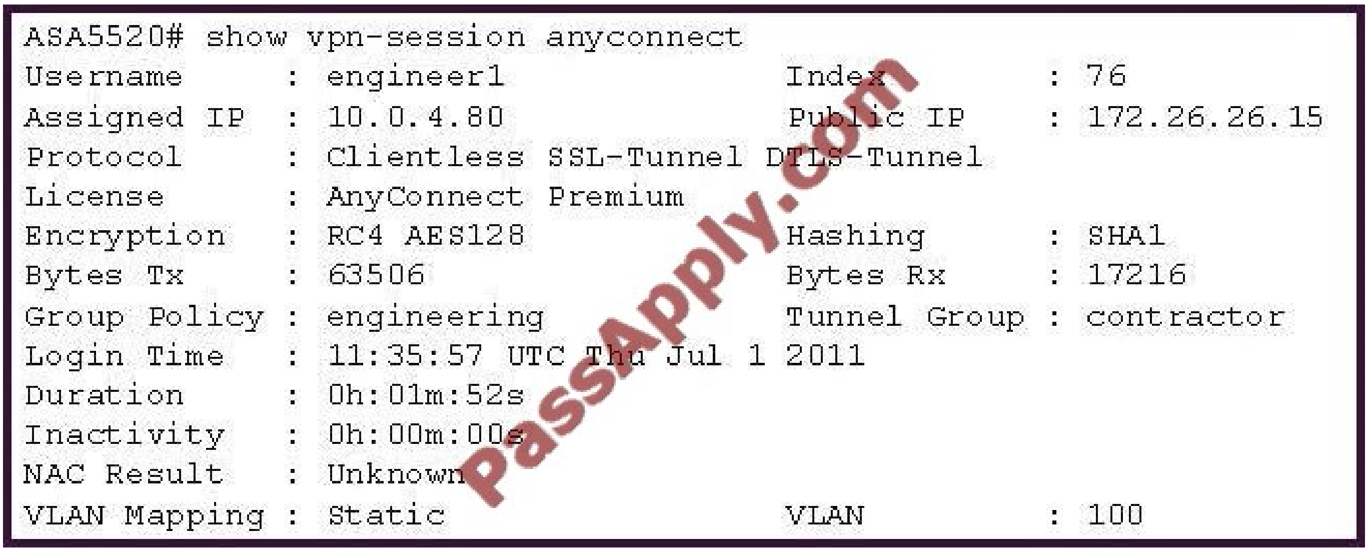


On the right, a permanent (P) or temporary (T) license is added to a Cisco ASA 5520. The merged license results in new capabilities for the Cisco ASA 5520. Drag the new resultant license on the left to the merging licenses on the right.

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

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

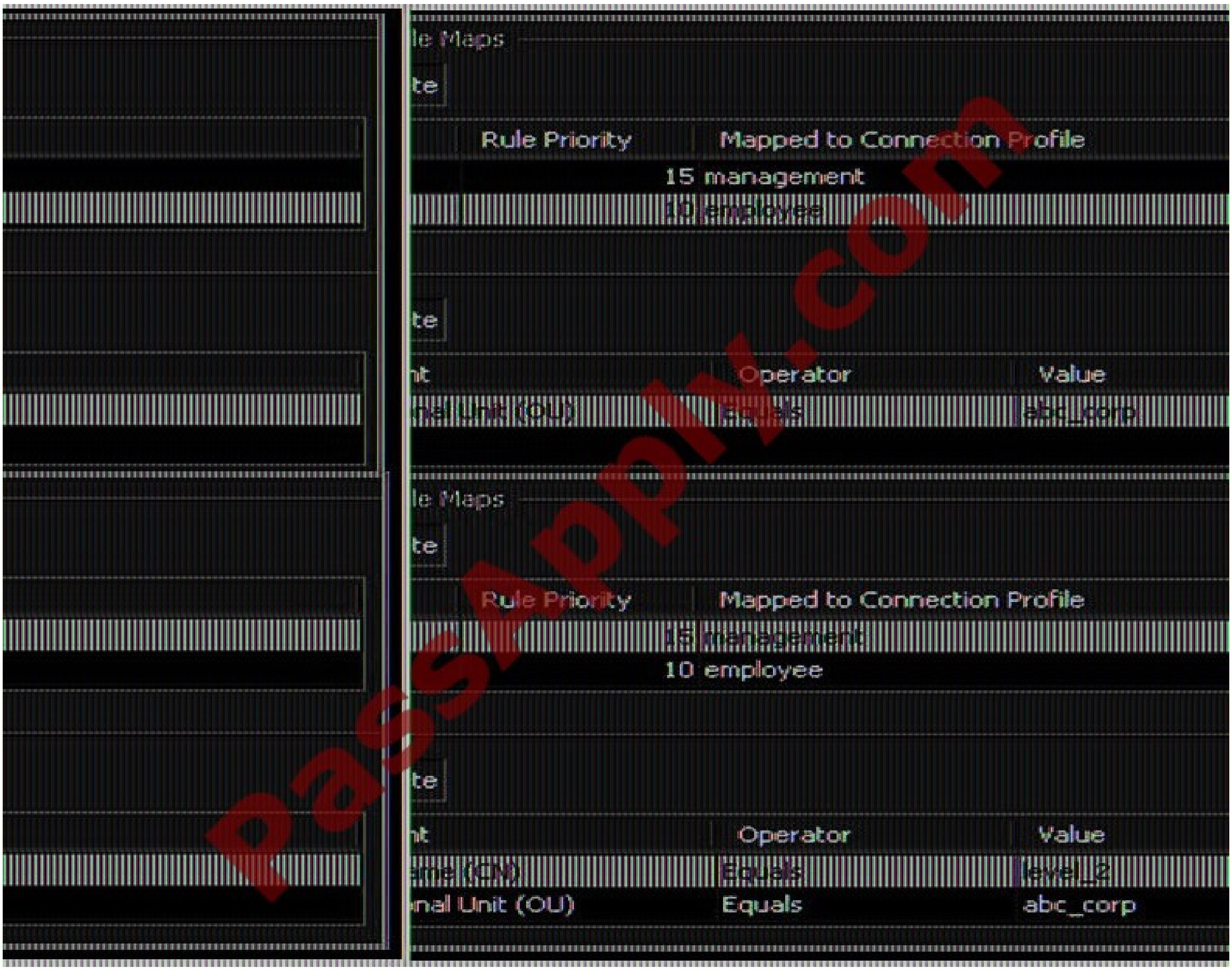
D. DfltGrpPolicy Group Policy

Correct Answer: B

http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/ac05hostscanposture.html#wp1039696

QUESTION 3

Refer to the exhibit.



le Maps

te

Rule Priority	Mapped to Connection Profile
15	management
10	employee

te

nt	Operator	Value
nal Unit (OU)	Equals	abc_corp

le Maps

te

Rule Priority	Mapped to Connection Profile
15	management
10	employee

te

nt	Operator	Value
ame (CN)	Equals	level_2
nal Unit (OU)	Equals	abc_corp

You have configured two SSL VPN Certificate to Connection Profile Maps for all employee and management users. The Connection Profiles for the management users are not being applied when the "management" users connect.

Based on the configuration that is shown, what is the most likely cause of this issue?

A. The rule priority of the employee mapping is not low enough, and it needs to be lowered to 1.

B. The priority of the employee mapping is too low, and it needs to be increased, but not higher than the rule priority of the management mapping.

C. The priority of the management mapping is too high, and it needs to be lower than the rule priority of the employee mapping.

D. The matching criteria for the management mapping is too specific, and the CN matching parameter should be removed.

Correct Answer: C

ASDM user guide p[age 35 52 Use the Add/Edit Certificate Matching Rule dialog box to assign the name of a list (map) to a connection profile. Fields ?Map--Choose one of the following: - Existing--Select the name of the map to include the rule. New--Enter a new map name for a rule. ?Rule Priority--Type a decimal to specify the sequence with which the security appliance evaluates the map when it receives a connection request. For the first rule defined, the default priority is 10. The security appliance evaluates each connection against the map with the lowest priority number first. ?Mapped to Connection Profile--Select the connection profile, formerly called a "tunnel group," to map to this rule. If you do not assign a rule criterion to the map, as described in the next section, the security appliance ignores the map entry.

QUESTION 4

When deploying clientless SSL VPN advanced application access, the administrator needs to collect information about the end-user system. Which three input parameters of an end-user system are important for the administrator to identify? (Choose three.)

A. types of applications and application protocols that are supported

B. types of encryption that are supported on the end-user system

C. the local privilege level of the remote user

D. types of wireless security that are applied to the end-user tunnel interface

E. types of operating systems that are supported on the end-user system

F. type of antivirus software that is supported on the end-user system

Correct Answer: ACE

When enabling port forwarding, the SSL VPN gateway will modify the hosts file on the PC of the remote user. Some software configurations and software security applications will detect this modification and prompt the remote user to select "Yes" to permit. To permit the modification, the remote user must have local administrative privileges. To securely access resources on a private network behind an SSL VPN gateway, the remote user of an SSL VPN service must have the following: ?;Thin Clien"; support used for TCP port-forwarding applications requires administrative privileges on the computer of the remote user. ?;Tunnel mod"; for Cisco SSL VPN requires administrative privileges for initial installation of the full tunnel client. ?The remote user must have local administrative privileges to use thin client or full tunnel client features. Operating system support ?Microsoft Windows 2000, Windows XP, or Windows Vista ?Macintosh OS X 10.4.6 ?Linux (Redhat RHEL 3.0 +, FEDORA 5, or FEDORA 6) SSL VPN-supported browser--The following browsers have been verified for SSL VPN. Other browsers might not fully support SSL VPN features.

QUESTION 5

In Cisco ASDM v6.4, what are four ways to implement single sign-on (SSO)? (Choose four.)

A. Use SSO for smart tunnels.

B. Use Kerberos SSO.

C. Use the HTTP Form protocol.

D. Use a dedicated SSO server.

E. Use SSO for application plug-ins.

F. Use auto sign-on for servers that do not require authentication credentials.

Correct Answer: ACDE

The security appliance can use the HTTP Form protocol for single sign-on (SSO) authentication of WebVPN users only. Single sign-on support lets WebVPN users enter a username and password only once to access multiple protected services and Web servers. The WebVPN server running on the security appliance acts as a proxy for the user to the authenticating server. When a user logs in, the WebVPN server sends an SSO authentication request, including username and password, to the authenticating server using HTTPS. If the server approves the authentication request, it returns an SSO authentication cookie to the WebVPN server. The security appliance keeps this cookie on behalf of the user and uses it to authenticate the user to secure websites within the domain protected by the SSO server. In addition to the HTTP Form protocol, WebVPN administrators can choose to configure SSO with the HTTP Basic and NTLM authentication protocols (the auto-signon command), or with Computer Associates eTrust SiteMinder SSO server (formerly Netegrity SiteMinder) as well. For an in-depth discussion of configuring SSO with either HTTP Forms, auto-signon or SiteMinder, The Auto Signon window or tab lets you configure or edit auto signon for users of Clientless SSL VPN. Auto signon is a simplified single signon method that you can use if you do not already have an SSO method deployed on your internal network. With auto signon configured for particular internal servers, the security appliance passes the login credentials that the user of Clientless SSL VPN entered to log in to the security appliance (username and password) to those particular internal servers. You configure the security appliance to respond to a specific authentication method for a particular range of servers. The authentication methods you can configure the security appliance to respond to consists of authentication using Basic (HTTP), NTLM, FTP and CIFS, or all of these methods. Auto signon is a straight-forward method for configuring SSO for particular internal servers. This section describes the procedure for setting up SSO with auto signon. If you already have SSO deployed using Computer Associates\\' SiteMinder SSO server, or if you have Security Assertion Markup Language (SAML) Browser Post Profile SSO, To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

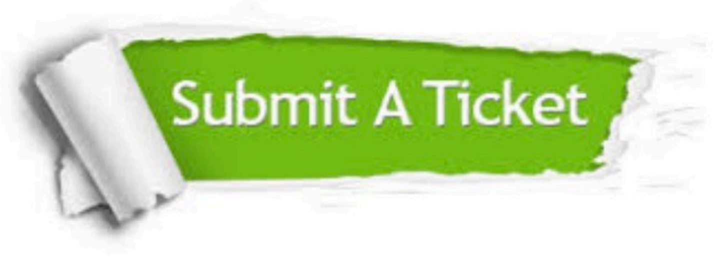
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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.passapply.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.