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.lead4pass.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

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,

QUESTION 2

An IT manager and a Security manager are discussing the deployment options for clientless SSL VPN. They are trying to decide which groups are best suited for this new deployment option. Which two groups are the best candidates for the clientless SSL VPN rollout? (Choose two.)

A. an IT administrator who needs to manage servers from a corporate laptop

B. employees who need occasional access to check their email accounts

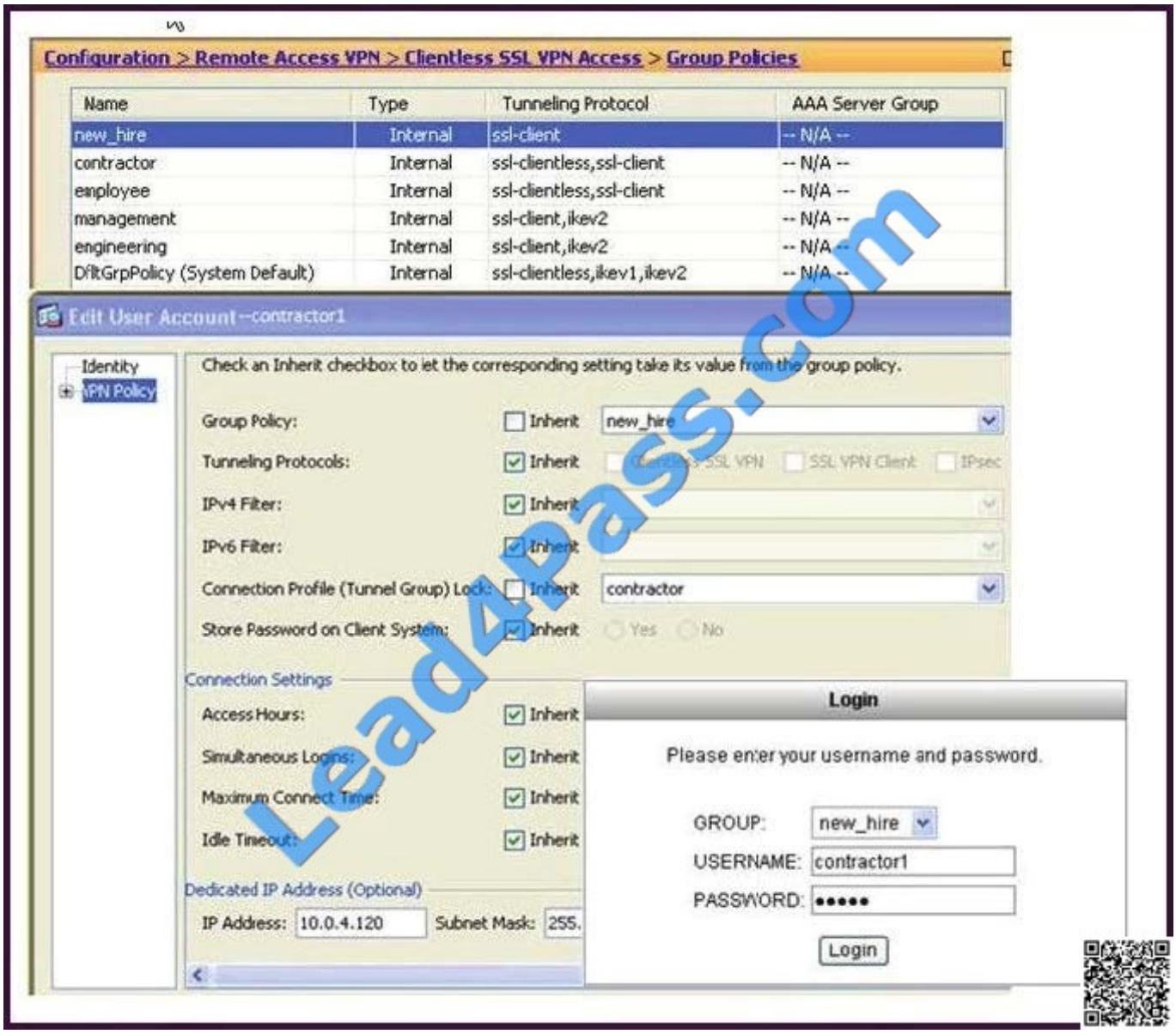
C. a vendor who needs access to confidential corporate presentations via Secure FTP

D. customers who need interactive access to the corporate invoice server

Correct Answer: BC

QUESTION 3

Refer to the exhibit.



When an SSL VPN user, contractor1, enters https://192.168.4.2 (the outside address of the Cisco ASA appliance) into the browser, an SSL VPN Login screen appears.

In addition to the information that is contained in the Cisco ASDM configuration screens, what can an administrator determine about the state of the connection after the user clicks the Login button?

A. The user login will succeed, and an IP address of 10.0.4.120 will be assigned.

B. The user will be presented with a clientless VPN portal page.

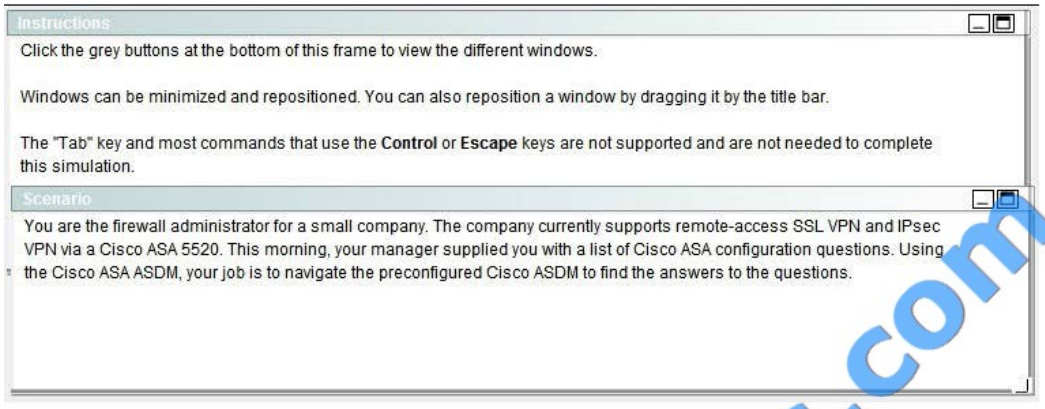
C. The user login will succeed, but the user will be connected to the "contractor" tunnel group.

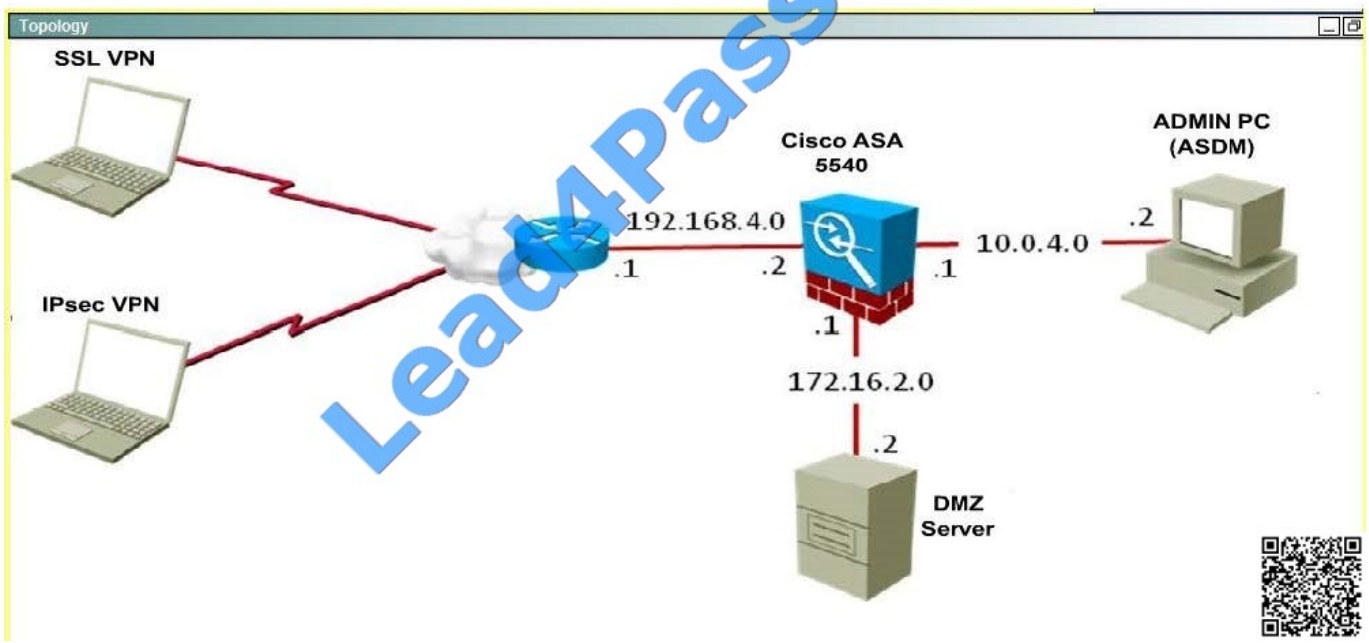
D. The login will fail.

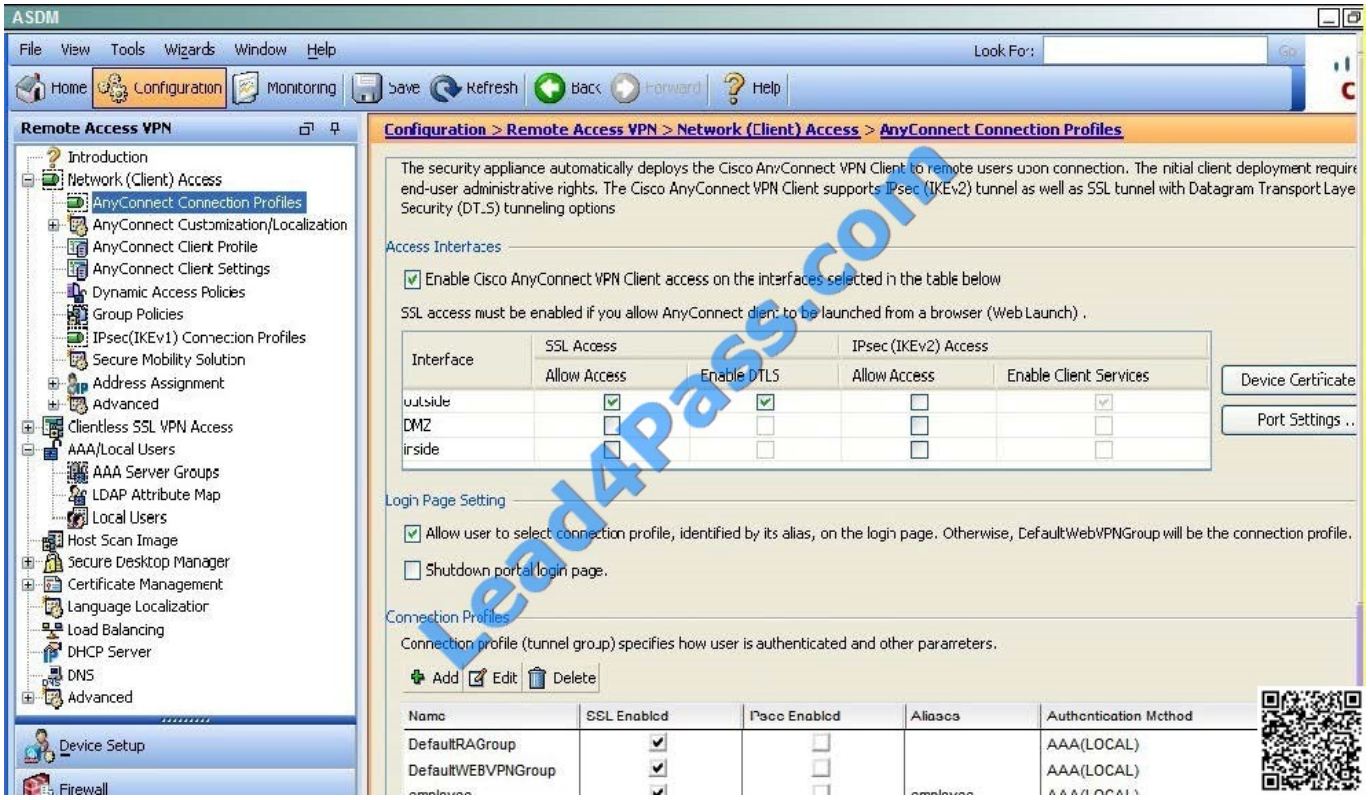
Correct Answer: D

QUESTION 4

Refer to following Exhibit and answer the following question below:







Upon logging in, user, emploeyee1, gets two sets of privileges. Choose the two options that show the privileges that are held by employee1.(Choose two)

A. Cisco ASDM, SSH, Telnet, and console access

B. CLI login prompt for SSH, Telnet, and console only

C. No Cisco ASDM, SSH, or console access

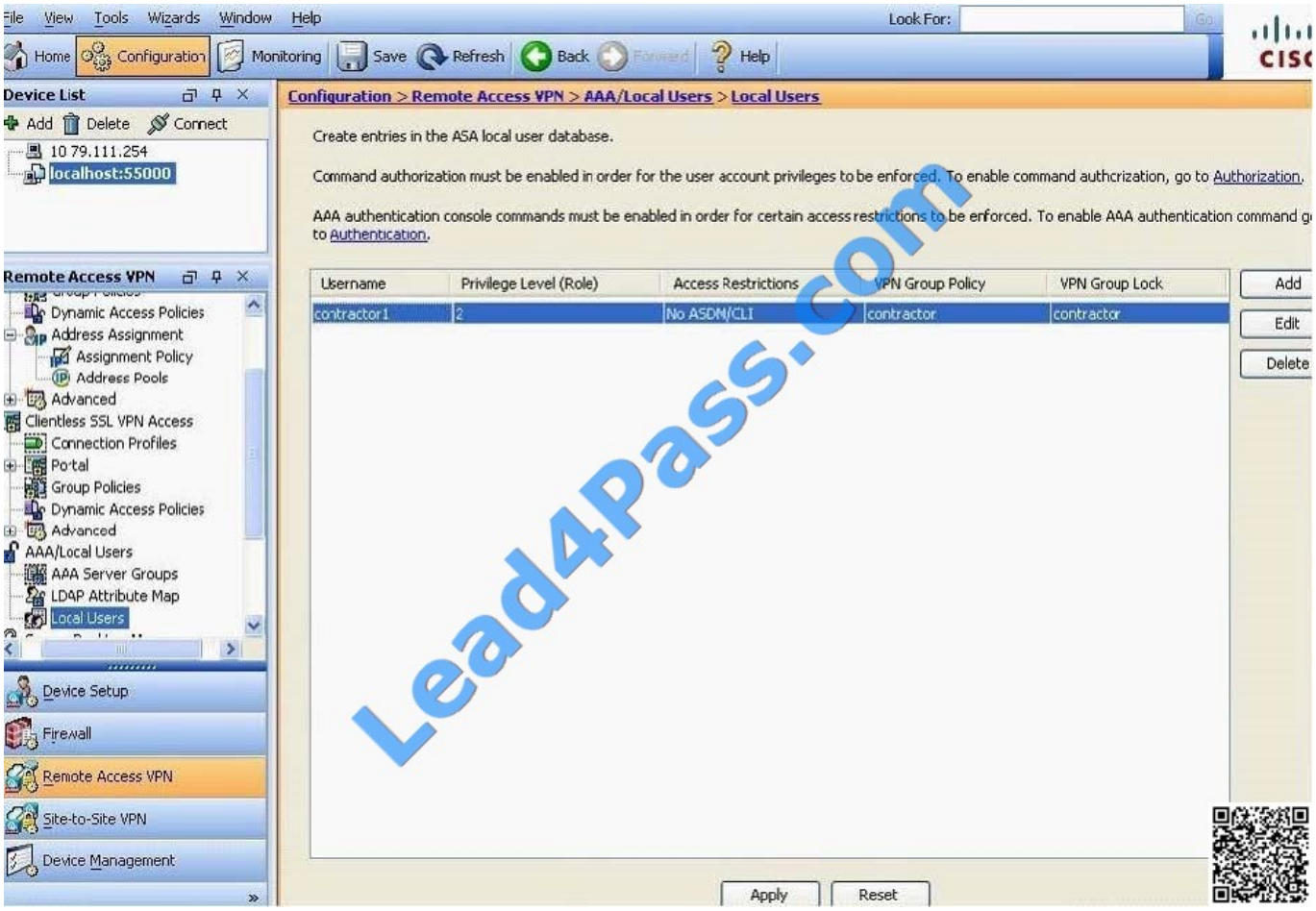
D. Level 15

E. Level 2

F. Level 3

Correct Answer: DE

Command authorization If you turn on command authorization using the local database, then the security appliance refers to the user privilege level to determine what commands are available. Otherwise, the privilege level is not generally used. By default, all commands are either privilege level 0 or level 15. ASDM allows you to enable three predefined privilege levels, with commands assigned to level 15 (Admin), level 5 (Read Only), and level 3 (Monitor Only). If you use the predefined levels, then assign users to one of these three privilege levels. This should show assigned levels for us:; on my demo version I could get the advanced tab to appear on aaa authorization to setup other commands but this shows how I setup contractor1



QUESTION 5

Refer to the exhibit.

```
access-list temp_acl webtype permit tcp host 10.0.4.4 eq 3389 log default
webvpn
 memory-size percent 25
 enable outside
 svc enable
 tunnel-group-list enable
 rewrite order 10 disable resource-mask *://cisco.com/* name cisco-com-bypass
 smart-tunnel list Smart_tunnel_applications Microsoft-RDP-Client MSTSC.EXE platform
windows
group-policy temp_worker internal
group-policy temp_worker attributes
 banner value Welcome Temp Workers!
 vpn-tunnel-protocol svc webvpn
  webvpn
   url-list value temp_worker
   filter value temp_acl
   customization value temp_worker
   smart-tunnel auto-start Smart_tunnel_applications
   file-entry disable
   file-browsing disable
   url-entry disable
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol IPSec svc webvpn
 webvpn
   url-list value Corporate_Server
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
```


The ABC Corporation has a Cisco ASA in its test bed. A new network administrator is instructed to add a smart tunnel application to the existing configuration. The configuration will enable a "temp_worker" who is using Microsoft native RDP to have RDP access to server 10.0.4.4 only.

Which statement is correct concerning the smart-tunnel configuration?

A. The WebType access list is misconfigured.

B. The smart tunnel list parameter is misconfigured.

C. The smart tunnel group policy parameters are misconfigured.

D. The smart tunnel configuration is configured correctly.

Correct Answer: D

642-648 Practice Test 642-648 Exam Questions 642-648 Braindumps