Exam Report: A.11 Security Pro Certification Practice Exam

Date: 1/28/2020 9:37:30 pm
Time Spent: 01:23:11 of 02:00:00

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 57%

Passing Score: 95%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

To answer this question, complete the lab using information below.
You have completed this lab and may go on to the next question.

Launch Lab

You did not complete the lab correctly.

Close Lab Report

Your Performance
Your Score: 0 of 4 (0%)
Elapsed Time: 17 minutes 2 seconds

Pass Status: Not Passed
Required Score: 100%

Task Summary
✗On Support, configure Windows Update Hide Details
⛔Install updates on Wednesday
⛔Install updates at 2:00 am
⛔Allow other users to install updates
⛔Include recommended updates
✗On Support, configure driver updates to install if they are not found on the computer
✗On ITAdmin, Enable automatic updates Hide Details
⛔Install updates automatically
⛔Include recommended updates for other Microsoft products
✗On ITAdmin, configure driver updates to download apps and icons for new devices

Explanation
In this lab, you perform the following tasks:

- Configure Windows Update on Support (which is running Windows 7) as follows:
  - Download and install updates automatically each **Wednesday** at **2:00 am**.
  - Include recommended updates.
  - Allow any user on the computer to install updates.
  - Configure driver updates to install drivers if they are not found on the computer.
- Configure Windows Update on ITAdmin as follows:
  - Configure Windows Update to install updates automatically.
  - Configure Windows Update to install updates for other Microsoft products when Windows is updated.
  - Configure driver updates to download apps and icons for new devices.

Complete this lab as follows:

1. On Support, modify Windows Update settings as follows:
   a. Select **Start**.
   b. Select **Control Panel**.
   c. Select **System and Security**.
   d. Select **Windows Update**.
   e. On the left, select **Change settings**.
   f. Configure the update ***day*** and ***time***.
   g. Select **Give me recommended updates the same way I receive important updates** to include recommended updates.
   h. Select **Allow all users to install updates on this computer** to allow any user to install updates.
   i. Click **OK**.

[q_Dom6_secPro6.exm AUTOUP]

Question 2: Correct

To answer this question, complete the lab using information below.
You have completed this lab and may go on to the next question.

Launch Lab

You completed the lab correctly.

Close Lab Report

Your Performance

Your Score: 4 of 4 (100%) Pass Status: Pass
Elapsed Time: 9 minutes 38 seconds Required Score: 100%

Task Summary

✓Create the VLAN Hide Details
✚Use 2 as the VLAN number (ID)
✚Use IPCameras as the name
✚Include ports 18, 19, 20, and 21
✓Connect the IP cameras to the VLAN and mount the IP cameras to the wall Hide Details
✚Make the connections in the lobby
✚Make the connections in the networking closet
✓Connect the laptop to the VLAN
✓Launch the IP camera monitoring software and confirm that the IP cameras are online

Explanation

In this lab, you perform the following:

- Access the switch management console from ITAdmin using the following credentials:
  - Address: **http://192.168.0.2**
  - Username: **ITSwitchAdmin**
  - Password: **Admin$0nly** (0 is zero)
- Create a VLAN on the switch as follows:
  - Number (ID): **2**
  - Name: **IPCameras**
  - Ports: **18**, **19**, **20**, **21**
- In the networking closet and lobby, perform the following:
  - Connect a Cat5e cable to the RJ-45 ports on the IP camera

and the IP camera wall plate.
- Mount the IP camera on the wall plate.

- In the networking closet, connect the DHCP server to the VLAN using a **Cat5e cable** from switch port 21 to patch panel port 21 in the rack.
- In the IT administration office, connect a **Cat5e cable** to the laptop's network port and the open port on the wall plate.
- On ITAdmin-Lap, verify the VLAN configuration and IP camera installation as follows:
  1. Select **Start** > **All Apps** > **IP Cameras**.
  2. Verify that the program detects the IP cameras on the VLAN 2 network.

Complete this lab as follows:

1. Configure a VLAN as follows:
   a. From the taskbar, open **Internet Explorer**.
   b. Maximize Internet Explorer.
   c. In the URL field, enter **192.168.0.2** and press **Enter**.
   d. In the Username field, enter **ITSwitchAdmin**.

[q_Dom5_secPro6.exm SWITCH_VLAN]

Question 3: Correct

To answer this question, complete the lab using information below.
You have completed this lab and may go on to the next question.

Launch Lab

You completed the lab correctly.

Close Lab Report

Your Performance

Your Score: 5 of 5 (100%) Pass Status: Pass
Elapsed Time: 3 minutes 49 seconds Required Score: 100%

Task Summary

✔Enable the TPM
✔Activate the TPM
✔Turn On BitLocker for the System (C:) drive
✔Save the recovery key on CorpServer
✔Perform a BitLocker system check

Explanation

In this lab, you configure BitLocker drive encryption as follows:

- Turn on TPM in the BIOS.
- Activate TPM in the BIOS.
- Turn on BitLocker for the Local Drive (C:) drive.
- Save the recovery key to **\\CorpServer\BU-Office1**.
- Run the BitLocker system check.
- Encrypt the entire **Local Drive (C:)** drive.

Complete this lab as follows:

1. Right-click **Start** and select **Control Panel**.
2. Select **System and Security**.
3. Select **BitLocker Drive Encryption**.
4. Select **Turn on BitLocker** next to C:.
5. Notice, at the bottom of the window, that Windows indicates that a

5. Notice, at the bottom of the window, that Windows indicates that a TPM was not found.
6. Click **Cancel**.
7. Click **Start**.
8. Click **Power**.
9. Click **Restart** to restart Office1 and activate TPM.
10. When the TestOut logo appears, press **Delete** to enter the BIOS.
11. Turn on and activate TPM as follows:
    a. In the left pane, expand **Security**.
    b. Select **TPM Security**.
    c. In the right pane, select **TPM Security** to turn TPM security on.
    d. Click **Apply**.
    e. Click **Activate**.
    f. Click **Apply**.
    g. Click **Exit**.
12. Turn on BitLocker as follows:
    a. After Office1 finishes rebooting, right-click **Start** and select **Control Panel**.
    b. Select **System and Security**.
    c. Select **BitLocker Drive Encryption**.
    d. Next to C:, select **Turn on BitLocker**. Now Windows is able to begin the Drive Encryption setup.
13. Save the recovery key to \\CorpServer\BU-Office1 as follows:
    a. Select **Save to a file** to back up your recovery key to a file.
    b. Browse the network to **\\CorpServer\BU-Office1** and click Save.

[q_Dom8_secPro6.exm BITLOCKER]

Question 4: Incorrect

To answer this question, complete the lab using information below.
You have completed this lab and may go on to the next question.

Launch Lab

You did not complete the lab correctly.

Close Lab Report

Your Performance

Your Score: 0 of 5 (0%) Pass Status: Not Passed
Elapsed Time: 1 minute 47 seconds Required Score: 100%

Task Summary

❌Set the **Application Identity** service to Automatic
❌Set the **Remote Registry** service to Disabled
❌Set the **Routing and Remote Access** service to Disabled
❌Set the **SSDP Discovery** service to Disabled
❌Set the **UPnP Device Host** service to Disabled

Explanation

In this lab, you configure the Workstation GPO with the following settings:

Service	Setting
Application Identity	Automatic
Remote Registry	Disabled
Routing and Remote Access	Disabled
SSDP Discovery	Disabled
UPnP Device Host	Disabled

Complete this lab as follows:

1. From Server Manager, select **Tools** > **Group Policy Management**.
2. Expand **Forest: CorpNet.com** > **Domains** > **CorpNet.com** > **Group Policy Objects**.
3. Right-click **WorkstationGPO** and select **Edit**.

[q_Dom6_secPro6.exm GPO_SERVICES]

Question 5: Incorrect

To answer this question, complete the lab using information below.
You have completed this lab and may go on to the next question.

Launch Lab

You did not complete the lab correctly.

Close Lab Report

Your Score: 0 of 6 (0%)

Elapsed Time: 1 minute 22 seconds

✗ Create the wireless profile for the PoliceVan network
✗ Use WPA2-Personal authentication
✗ Use AES encryption
✗ Use 4WatchingU for the security key
✗ Start the connection automatically if the network is detected
✗ Delete the out-of-date TrendNet-BGN wireless profile

Explanation

In this lab, your task is to do the following:

- Manually create a wireless network profile on the laptop as follows:
  - Network name (SSID): **PoliceVan** (The SSID name is case sensitive.)
  - Security type: **WPA2-Personal**
  - Encryption type: **AES**
  - Security Key/Passphrase: **4WatchingU** (The security key is case sensitive.)
  - Start the connection automatically.
  - Connect even if the network is not broadcasting.
  - Start this connection automatically.
  - Connect even if the network is not broadcasting.
- Delete the out-of-date **TrendNet-BGN** wireless profile.

Complete this lab as follows:

1. Manually create the wireless network profile on the laptop as follows:
   a. Right-click the **networking** icon in the notification area and select **Open Network and Sharing Center**.
   b. Select **Set up a new connection or network**.
   c. Select **Manually connect to a wireless network**; then click **Next**.
   d. Enter the ***network name***.

[q_Dom4_secPro6.exm WIRELESS4]

Question 6: Correct

To answer this question, complete the lab using information below.
You have completed this lab and may go on to the next question.

Launch Lab

You completed the lab correctly.

Close Lab Report

Your Performance

Your Score: 7 of 7 (100%) Pass Status: Pass
Elapsed Time: 7 minutes 56 seconds Required Score: 100%

Task Summary

✓Configure the Maggie Brown email account for SSL
✓Configure the Emily Smith email account for SSL
✓Turn off AutoFill on Safari Hide Details
➕Set Use Contact Info to OFF
➕Set Names and Passwords to OFF
✓Set BlockCookies to Allow from Websites I Visited
✓Turn on Fraud Warning
✓Turn off JavaScript
✓Turn on Block Pop-ups

Explanation

In this lab, you perform the following:

- Configure each email account to use SSL for incoming mail.
- Secure the Internet browser as follows:
  - Turn off AutoFill
  - Accept cookies only from visited sites
  - Turn on Fraud Warning
  - Turn off JavaScript
  - Turn on Block Pop-ups

Complete this lab as follows:

1. Configure email for SSL as follows:
   a. Select **Settings**.
   b. Select **Mail, Contacts, Calendars**.
   c. Select an ***email account***.
   d. Select **Account**.
   e. Select **Advanced**.
   f. Under Incoming Settings, set Use SSL to **ON**.
   g. Select **Account**.
   h. Click **Done**.
   i. At the top, select **Mail, Contacts**.
   j. Repeat steps 1c–1i for each email account.
2. Secure the Internet browser as follows:
   a. From the left menu, select **Safari**.

[q_Dom7_secPro6.exm IPAD_EMAIL]

Question 7: Incorrect

To answer this question, complete the lab using information below.
You have completed this lab and may go on to the next question.

Launch Lab

You did not complete the lab correctly.

Close Lab Report

Your Performance

Your Score: 0 of 5 (0%) Pass Status: Not Passed
Elapsed Time: 1 minute 22 seconds Required Score: 100%

Task Summary

❌Create the Administrators (built-in) local group
❌Select Delete all member users
❌Select Delete all member groups
❌Add BUILTIN\Administrator to the group
❌Add %DOMAINNAME%\Domain Admins to the group

Explanation

In this lab, you edit the Default Domain policy and configure the Local Users and Groups policy settings as follows:

- Create a policy to update the built-in Administrator local group.
- Delete all member users.
- Delete all member groups.
- Add BUILTIN\Administrator to the group.
- Add %DOMAINNAME%\Domain Admins to the group.

Complete this lab as follows:

1. From Server Manager, select **Tools** > **Group Policy Management**.
2. Expand **Forest: CorpNet.com** > **Domains** > **CorpNet.com**.
3. Right-click **Default Domain Policy** and select **Edit**.
4. Under Computer Configuration, expand **Preferences** > **Control Panel Settings**.
5. Right-click **Local Users and Groups** and select **New** > **Local Group**.
6. In the Group name field, select **Administrators (built-in)** from the drop-down list.
7. Select **Delete all member users** to remove all member users.
8. Select **Delete all member groups** to remove all member groups.
9. Click **Add**.
10. In the Name field, enter **BUILTIN\Administrator**; then click **OK**.
11. Click **Add**.
12. In the Name field, enter **%DOMAINNAME%\Domain Admins**; then click **OK**.
13. Click **OK** to save the policy.

[q_Dom1_secPro6.exm GPO_RLOCAL]

Question 8: Correct

To answer this question, complete the lab using information below.
You have completed this lab and may go on to the next question.

Launch Lab

You completed the lab correctly.

Close Lab Report

Your Performance

Your Score: 9 of 9 (100%)

Your Score: 9 of 9 (100%)
Elapsed Time: 8 minutes 43 seconds

Task Summary
✓Enable Audit Policies Hide Details
+Audit: Force audit policy subcategory settings (Windows Vista or later) to ov
policy category settings:--Enabled
+Audit: Shut down system immediately if unable to log security audits--Enabl
✓Enable Event Log Policy Hide Details
+Retention method for security log: Enabled--do not overwrite events (clear l
✓Enable Account Logon Audit Policy Hide Details
+Audit Credential Validation: Success and Failure
✓Enable Account Management Audit Policies Hide Details
+Audit User Account Management: Success and Failure
+Audit Security Group Management: Success and Failure
+Audit Other Account Management Events: Success and Failure
+Audit Computer Account Management: Success
✓Enable Detailed Tracking Audit Policy Hide Details
+Audit Process Creation: Success
✓Enable Logon-Logoff Audit Policies Hide Details
+Audit Logon: Success and Failure
+Audit Logoff: Success
✓Enable Policy Change Audit Policies Hide Details
+Audit Authentication Policy Change: Success
+Audit Audit Policy Change: Success and Failure
✓Enable Privelege Use Audit Policy Hide Details
+Audit Sensitive Privilege Use: Success and Failure
✓Enable System Audit Policies Hide Details
+Audit System Integrity: Success and Failure
+Audit Security System Extension: Success and Failure
+Audit Security State Change: Success and Failure
+Audit IPsec Driver: Success and Failure

Explanation
In this lab, you configure the following audit policy settings in WorkstationGPO

Local Policies
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings
Audit: Shut down system immediately if unable to log security audits

Event Log	Setting
Retention method for security log	Enabled: Do not overwrite events (clear log

Advanced Audit Policy Configuration	Setting

Explanation

Use Group Policy Management to edit the WorkstationGPO to configure the Advanced Audit Policies.
To find the necessary policies, browse to the following areas:

- **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security**

Options
• Computer Configuration\Policies\Windows Settings\Security Settings\Event Log
• Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration

Note: Remember to not use the old Audit Policies located in **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policies**.

Following are steps that an expert might take to perform the tasks in this lab.

Edit Audit Policies

1. Click **Start/Administrative Tools/Group Policy Management**.
2. Browse to the policy. Right-click the policy and select **Edit...**.
3. In the Group Policy Management Editor, browse to the location of the policy settings.
4. On the right, right-click the policy you want to edit and select **Properties** (or double-click).
5. Select **Define this policy setting**. Select the type of auditing or additional settings as required.
6. Click **OK**.
7. Repeat steps 3 through 6 for additional policy settings.

[q_Dom9_secPro6.exm GPO_AUDIT]

Question 9: Incorrect

To answer this question, complete the lab using information below.
You have completed this lab and may go on to the next question. Launch Lab

You did not complete the lab correctly. Close Lab Report

Your Performance
Your Score: 0 of 5 (0%) Pass Status: Not Passed
Elapsed Time: 53 seconds Required Score: 100%

Task Summary
✗ Create an access profile to restrict management access Hide Details
- Create the MgtAccess profile
- Create the deny rule

✗ Add a profile rule Hide Details
- Create the allow rule

✗ Set the active access profile
✗ Save changes to the startup configuration
✗ Upgrade the firmware

Explanation
In this lab, you perform the following:

- Create an Access Profile called **MgtAccess** and configure it with with the following settings:

Setting	Value
Access Profile Name	**MgtAccess**
Rule Priority	**1**
Management Method	**All**
Action	**Deny**
Applies to Interface	**All**
Applies to Source IP address	**All**

- Add a Profile Rule to the **MgtAccess** profile with the following settings:

Setting	Value
Rule Priority	**2**

Management Method	**HTTP**
Action	**Permit**
Applies to interface	**All**
Applies to Source IP address	**User defined** IP Version: **Version 4** IP Address: **192.168.0.10** Network Mask: **255.255.255.0**

- Set the **MgtAccess** profile as the active access profile.
- Save the changes to the switch's startup configuration file.
- Update the firmware image to the latest version by downloading the firmware files found in **C:\Sx300_Firmware\Sx300_FW-1.2.7.76.ros**.

Complete this lab as follows:

[q_Dom5_secPro6.exm SWITCH_HARD2]

Question 10: Correct

To answer this question, complete the lab using information below.
You have completed this lab and may go on to the next question.

Launch Lab

You completed the lab correctly.

Close Lab Report

Your Performance

Your Score: 2 of 2 (100%) Pass Status: Pass
Elapsed Time: 4 minutes 28 seconds Required Score: 100%

Task Summary

✓Create a backup schedule Hide Details
Items to back up: System State
Backup schedule: Once a day at 1:00 a.m.
Backup location: \\CorpFiles12\Backup
✓Perform an immediate backup of the server Hide Details
Items to back up: System State and Local Disk (C:)
Backup location: \\CorpFiles12\Backup

Explanation

In this lab, your task is to use Windows Server Backup to complete the following tasks:

- Create a regular backup schedule for the CorpDC4 server using the following settings:
  - Backup type: **Custom**
  - Items to back up: **System State**
  - Backup frequency: **Once a day**
  - Backup time: **1:00 am**

[q_Dom8_secPro6.exm WSB_BACKUP1]

Question 11: Correct

To answer this question, complete the lab using information below.
You have completed this lab and may go on to the next question.

Launch Lab

You completed the lab correctly.

Close Lab Report

Your Performance

Your Score: 4 of 4 (100%) Pass Status: Pass
Elapsed Time: 3 minutes 47 seconds Required Score: 100%

Task Summary
✓Install the smart card key readers Hide Details
+Install the card reader outside the building's front door
+Install the card reader outside the Networking Closet door
✓Install the IP security cameras Hide Details
+Install the IP security camera inside the networking closet
+Install the IP security camera outside the networking closet
✓Install the Restricted Access sign on the networking closet door
✓Install the visitor log on the lobby desk

Explanation
In this lab, your task is to perform the following:

- Install the smart card key readers
- Install the IP security cameras
- Install the Restricted Access sign on the networking closet door
- Install the visitor log on the Lobby desk

Complete this lab as follows:

1. Install the key card readers as follows:
   a. Expand the **Door Lock** category on the shelf.
   b. Drag a key card reader from the shelf to a highlighted wall just outside the building's front door.
   c. Drag a key card reader from the shelf to the highlighted wall just outside the networking closet.
2. Install the security cameras as follows:
   a. Expand the **CCTV Cameras** category on the shelf.

[q_Dom3_secPro6.exm PHYS_SEC]

Question 12: Correct

To answer this question, complete the lab using information below.
You have completed this lab and may go on to the next question.

Launch Lab

You completed the lab correctly.

Close Lab Report

Your Performance
Your Score: 4 of 4 (100%)
Elapsed Time: 8 minutes 39 seconds R c

Task Summary
✓Create the Juan Suarez account Hide Details
+Create the Juan Suarez account in the Marketing\MarketingManagers OU
+Set the first name, last name, and full name properties
+Use jsuarez@CorpNet.com for the logon name
+Specify a password of 1234abcd$
+Require a password change at next logon
+Enable the account
✓Create the Susan Smith account Hide Details
+Create the Susan Smith account in the Sales\PermSales OU
+Set the first name, last name, and full name properties
+Use ssmith@CorpNet.com for the logon name
+Set the password to 1234abcd$
+Require a password change at next logon

Enable the account
Create the Borey Chan account Hide Details
Create the Borey Chan account in the Sales\TempSales OU
Set the first name, last name, and full name properties
Use bchan@CorpNet for the logon name
Set the password to 1234abcd$
Require a password change at next logon
Enable the account
Limit the logon hours of Borey Chan to allow logon only from 8 am to 5 pm, M
Friday.
Expire the Borey Chan account on December 31st
Create the Mark Burnes account Hide Details
Create the Mark Burnes account in the Sales\SalesManagers
Set the first name, last name, and full name properties
Use mburnes@CorpNet for the logon name
Set the password to 1234abcd$
Require a password change at next logon
Enable the account
Explanation
In this lab, you use Active Directory Users and Computers to create the following

User	Job Role	User Name	OU
Juan Suarez	Marketing manager	jsuarez	Marketing\Ma
Susan Smith	permanent sales employee	ssmith	Sales\PermSa
Borey Chan	temporary sales employee	bchan	Sales\TempSa

[q_Dom1_secPro6.exm AD_USER1]

Question 13: Incorrect

To answer this question, complete the lab using information below.
You have completed this lab and may go on to the next question.

Launch Lab

You did not complete the lab correctly.

Close Lab Report

Your Performance
Your Score: 0 of 5 (0%)
Elapsed Time: 3 minutes
Pass Status: Not Passed
Required Score: 100%

Task Summary
Configure Internet Explorer GPO Settings Hide Details
Security Zones: Do not allow users to add/delete sites - Enabled
Security Zones: Do not allow users to change policies - Enabled
Turn on ActiveX Filtering - Enabled
Configure Internet Explorer>Internet Control Panel GPO Settings Hide Details
Prevent Ignoring Certificate Errors - Enabled
Configure Internet Explorer>Internet Control Panel>Security Page>Internet Zone GPO Settings Hide Details

Java permissions - Enabled
Java permissions - Set to Java Disabled
Turn on Protected Mode - Enabled
Turn on Protected Mode - Set to Enable
Configure Internet Explorer>Internet Control Panel>Security Page>Restricted Sites Zone GPO Settings Hide Details
Allow File Downloads - Enabled
Allow File Downloads - Set to Disable
Java permissions - Enabled
Java permissions - Set to Java Disabled
Turn on Protected Mode - Enabled
Turn on Protected Mode - Set to Enable
Configure Internet Explorer>Security Features GPO Settings Hide Details
Object Caching Protection > Internet Explorer Processes - Enabled
Protection From Zone Elevation > Internet Explorer Processes - Enabled
Restrict ActiveX Install > Internet Explorer Processes - Enabled
Restrict File Download > Internet Explorer Processes - Enabled

Explanation

In this lab, your task is to configure the following Internet Explorer policy settings in the WorkstationGPO:

Policy	Setting
Security Zones: Do not allow users to add/delete sites	Enabled
Security Zones: Do not allow users to change policies	Enabled
Turn on ActiveX Filtering	Enabled
Internet Control Panel > Prevent Ignoring Certificate Errors	Enabled
Internet Control Panel > Security Page > Internet Zone > Java permissions	Enabled: Disable Java
Internet Control Panel > Security Page > Internet Zone > Turn on Protected Mode	Enabled: Enable

[q_Dom7_secPro6.exm GPO_IE]

Question 14: Correct

To answer this question, complete the lab using information below.
You have completed this lab and may go on to the next question.

Launch Lab

You completed the lab correctly.

Close Lab Report

Your Performance

Your Score: 2 of 2 (100%) Pass Status: Pass
Elapsed Time: 1 minute 47 seconds Required Score: 100%

Task Summary

Add and IPSec VPN Connection Hide Details
Description: CorpNetVPN

Description: CorpNetVPN
Server Address: 198.28.56.34
User Account: mbrown
Secret: 1a!2b@3c#4d$
Turn On VPN and connect

Explanation

In this lab, you perform the following:

- Add an IPSec VPN Connection using the following values:

Parameter	Value
Description	CorpNetVPN
Server	198.28.56.34
Account	mbrown
Secret	1a!2b@3c#4d$

- Turn on the VPN.
- Verify that a connection is established. The password for mbrown is **L3tM31nN0w** (0 = zero).

Complete this lab as follows:

1. Select **Settings**.
2. Select **Wi-Fi**.
3. Verify that you are connected to the **Home-Wireless** network.
4. From the left menu, select **General**.
5. Select **VPN**.
6. Select **Add VPN Configuration**.
7. Select **IPSec**.
8. In the Description field, enter the ***description***.
9. In the Server field, enter ***server IP address***.
10. In the Account field, enter ***account admin username***.
11. In the Secret field, enter the ***pass phrase***.
12. Click **Save**.
13. Under VPN Configuration, set Not Connected to **ON**.
14. Enter **L3tM31nN0w** (0 = zero) as the password.
15. Click **OK**.

[q_Dom2_secPro6.exm IPAD_VPN]

Question 15: Incorrect

To answer this question, complete the lab using information below.
You have completed this lab and may go on to the next question.

Launch Lab

You did not complete the lab correctly.

Close Lab Report

Your Performance

Your Score: 1 of 2 (50%) Pass Status: Not Passed
Elapsed Time: 3 minutes 33 seconds Required Score: 100%

Task Summary
✔VPN Wizard Configuration Show Details
➕Connection Name: CorpNetVPN
➕Preshared Key: 1a!2b@3c#4d$
➕Local IP Address: 198.28.56.34
✖Configure IPSec users Hide Details
➕Username: mbrown
➕Password: L3tM31nN0w
➖Username: jgolden
➖Password: L3tM31nT00
➕Username: sbarnes
➕Password: Adm1nsR0ck
Explanation
In this lab, your task is to perform the following:

- Configure Remote Access VPN using the following settings:

Parameter	Value
VPN Type	Remote Access
Connection Name	CorpNetVPN
Pre-shared Key	1a!2b@3c#4d$
Local Gateway Type	IP Address
Local WAN's IP Address	198.28.56.34

- Verify that the VPN Policy was created.
- Verify that the IKE Policy was created.
- Configure the following Standard IPSec users:

User	Password
mbrown	L3tM31nN0w
jgolden	L3tM31nT00
sbarnes	Adm1nsR0ck

Complete this lab as follows:

1. From the top menu, select **VPN**.
2. Under About VPN Wizard, select the **VPN type**.
3. Enter the ***connection name***

[q_Dom4_secPro6.exm NSA_VPN]