**Assignment 3: (Team and Individual Assignment)** Install and configure Security Server using PfSense . *(This will be marked with a* ***20/70/10*** *split. 20% will be your assignment mark from Individual section, 70% will be your assignment mark for install and hardening, and 10% will be your team rubric.)*

**Required Resources**

* Ubuntu Apache Server created in assignment 1
* pfSense -CE-**2.7.2**-RELEASE-amd64.iso (**I have uploaded a copy to your TEAMs files**)
* Windows 10 Educational Edition 21H2.iso from Azure for Education
* Windows 10 21H2 KMS Key

**Professional Documentation**

All documentation must be done in a **professional style**. It must include:

* Title page
* **Updateable** Table of Contents
* Document introduction
* Section introductions or description, each section must be clearly identified
* Graphics or screenshots MUST include a title with a short description
* Any direct or copied quotes or graphics MUST be properly credited in a footnote
* ALL sources MUST be properly cited (APA format) and placed at the end of your document in a bibliography.
* **NO** embedded, zipped or compressed files. \*\* All scripts must be converted to text before including them in your documentation. \*\*
* **1 Professional Word Document ONLY.**

**Research and documentation sections** -Please complete all research and question responses in your own words. Research sections not completed in your own words may result in a mark of 0 for the section.

**NOTE:** Please do NOT copy and paste responses from internet, **even with a citation**. I expect each section or response to be in your own words. Be prepared to explain your responses and demonstrate your comprehension.

**No marks** will be given for cited or credited information included in document.

***\*\* I recommend completing any research section before completing any required task listed below as you will have a much better understanding of the material and data.***

**Evaluation:** This assignment is markedas per the attached Rubric (marks will be deducted for deviating from Requirements). \*\*You may be asked to demonstrate some of your assignment to show your comprehension of the material.

**Marking and Assignment Notes:**

* ScreenshotsMUST include user or device identifying information.
* Screenshots MUST be added to your document in the order of creation.
* Documentation must meet Professionalism requirements.
* **Automatic mark of 0 - Assignment not submitted or work not original.**

<http://www.nscc.ca/docs/about-nscc/policies-procedures/policy-studentcodeofconduct.pdf>

<https://www.nscc.ca/docs/about-nscc/policies-procedures/policy-academicintegrity.pdf>

***NOTE: This assignment may require some adaption to the current NOS version or Distro (with update), research and troubleshooting.***

**Individual Portion of the Assignment.**

**Task 1– Research and Recommendation Checklist**

**Research Section – Review research requirements on page 1 and complete in your own words.**

**\*\* I recommend completing this section before completing the remainder of the assignment as you will have a much better understanding of the material and data.**

* Update your document called **YourIntials\_ISEC2700\_Glossary** and add the updated document to your personal dropbox in BrightSpace.

*Note: You will update this document throughout the course as you complete the research portion of the assignments.*

* Research and define each of the following, give at least one example and add your research to your Glossary document:

1. Application Detection such as OpenAppID
2. IDS (in reference to security servers)
3. IPS (in reference to security servers)
4. SNORT (Network Intrusion Detection & Prevention System)
5. Virtual Private Network, how do they work and why have them?

**Team Portion of Assignment**

**Team Assignment.** As this is a Team Task please make sure to identify which part(section) of the preparation, configuration/ setup steps or documentation you completed for this assignment. You must identify the authors of each section **and** it must be mirrored in your work journal.

*Ex. Technology Equipment and Disposal Policy by Marie Dutka, edited by Bruce Orca.*

**Task 2 - Install and configure a PfSense Security Server**

Create a Virtual Machine with these settings (**No install or change log required**):

* (Guest Operating System) Kernel = Other / FreeBSD 14 64bit
* 40g drive
* 4g memory
* 1 Processor / 1 Cores
* **Two (2)** NICS (set both to NAT) \*\*Must be created prior to distro install.
  + \*\* Confirm all NICs are set to “connect at power on”
* Virtual Machine follows naming convention
* Modify the Virtual Machine Description to list (you may need to read ahead for some of the information required):
  + Operating System:
  + Creation Date:
  + Hostname: (Set by default during install, record name)
  + Default User Name: Set during install
  + Default User Password: Set during install

Now that we have created our virtual machine lets install and configure our pfSense server.

* Boot to your ISO and Install PfSense -CE-2.7.2-RELEASE
  + \*Partition your hard drive using - **Auto (UFS) BIOS**
  + Accepts all other defaults
* Reboot your server
* Set your LAN IP = 192.168.208.100/24 (static)
  + Do **not** enter an IPv6 , Gateway or HTTP as the webConfigurator protocol
  + Do **not** enable DHCP at this time.
  + Do **not** configure your WAN at this time.
* Leave all other IP Settings and configurations the same
* **STOP**. Record IP settings for both NICs and add the information to your documentation.
* Update your new pfSense server from console
* Since we just completed an update it is a good idea to reboot (normally) our server.

Now we will configure our PfSense using the Web interface. Since we will need a browser to access the web interface we will need to make a couple of modifications to our **Ubuntu Apache Server**.

* Complete an update and upgrade of your Apache server
* Use your command line to install **ubuntu-budgie-desktop**
  + When asked select **GDM3** as your display manager
* User your terminal command line confirm **Firefox** is installed, install if required.
* Since we just installed a new application and a GUI, please update/upgrade your server again
  + Make sure to reboot after the install to complete the modifications and boot into your Budgie Desktop.

Now let’s look at PfSense and start configuring our security server

* Log into your Apache web server as your **default user**
* Open the pfSense configuration page in Firefox using your pfSense Server LAN IP
  + We will be working with Firefox a lot so let’s add it to our “favorites” in your activity list.
  + **Note**, since we have not secured the login page you will receive a couple of warnings and you will need to “Accept the Risk and Continue” the first time we open our pfSense page.
* If required, add the “Permanently store the Security Exception” option as you will access this page again later.
* Login into pfSense web portal but do NOT save the password.
  + Username = admin
  + Password = pfsense
  + \*\* Do **Not** save the username or password on your machine.
* Select the pfsense community icon for the top left corner. Accept the license agreement.
* Review the information on the pfSense Dashboard page.
* Modify the Dashboard so it shows **only**:
  + System Information
  + Interfaces
  + Gateways
  + Installed Packages
  + OpenVPN
  + Services Status
  + S.M.A.R.T. Status
* Modify Dashboard General Setup to include hostname on login banner and set dashboard columns to 3.
* Now rearrange your dashboard by dragging and dropping to ensure you have content in each column, then save your dashboard and **save** your Dashboard layout.

Now that we have setup our pfSence Dashboard the way we like, let’s start configuring our security server.

* Use your System/Setup Wizard page (use the “next” button) to make the following configuration changes:
  + Hostname = pfSenseYour3Initials (ex. pfSensemad) \*\*lowercase
  + Domain = your initials.isec2700.ca (ex. mad.isec2700.ca) \*\*lowercase
  + DNS = Primary 8.8.8.8 / Secondary 8.8.4.4
  + Allow DNS servers to be overridden by DHCP/PPP on WAN
  + Time server host = leave default
  + Time zone = America / Halifax
* Make the following change to **WAN** Interface configuration:
  + Because we are doing this in a virtual network, **uncheck** “Block RFC1918 private networks” and “Block bogon networks”
    - **Stop**. Take a minute to research what these settings mean and add it to your Glossary in your document and be prepared to explain then during demo.
  + Leave all other settings the same
  + Confirm you have the correct LAN IP Addressing and Subnet Mask

We will need a secure password for admin.

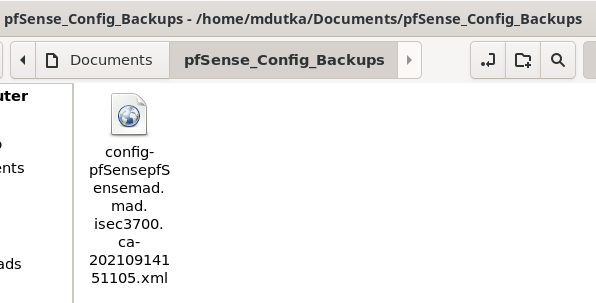
* Set admin password to **PFPassw0rd**
  + Add your pfSense username and password to your pfSense virtual machine VM description on your pfSense Server.
* After your reload you will be prompted to check for any additional updates for your PfSense Security Server, since we just installed and updated the latest version we should **not** need to update do not run “Check for Updates”.
* If required, select finish as we have completed our basic setup by reading the information screen.

Now that we have completed the initial setup for our pfSense server we will capture some data and create our first backup. We will also take the time to capture our base configuration.

* Login to pfSense web interface from Budgie desktop.
* Under Diagnostics/Backup & Restore / Backup & Restore do a configuration backup, accepting all defaults and “Download configuration as XML”
* Create a directory in your Default Users Documents directory (folder) called PfSense \_Config \_Backups
* Move your XML configuration backup you created earlier to your new backup directory

See example below.

*Example*



* **Stop**. Upload a copy of your .xml configuration file to BrightSpace for review as a separate upload.
* This would be a good time to take a snapshot of our pfSense server in the off position.

**Task 3 - Install and configure Snort on your PfSense Security Server**

Now that we have installed and set the base configuration for our pfSense server we will setup some of the security features included with pfSense.

Snort is what is known as an IDS or Intrusion Detection System that can also be used as an Intrusion Prevention System or IPS.

* If required, log into your pfSense server using the Web Portal
* Add **snort 4.1.6\_17** through System/Package Manager/Available Packages
  + Make sure to confirm the install if requested
* Snort should now be listed in your installed packages

Now that we have installed Snort on our security server we will need to setup some Rules

* Lets select our Rule sets through Services/Snort/Global Settings
* Enable Snort VRT
* You must signup for a **free** Registered User Rules Account in order to use the preconfigured VRT rules.
  + Use your NSCC email and Ubuntu server default User password
  + Agree to Snort License
  + Do NOT subscribe to Snort mailing lists.
* Confirm your registration
* Sign in to your subscription and select OinkCode for the left hand menu.

\*\*Make sure to ONLY subscribe to the **FREE** version to get your OinkCode

* Once you have signed up you will receive an Oinkmaster code, use your code to Enable your Snort VRT
* Now that you enabled Snort VRT we will need to enable some of our other rules.
* Enable:
  + GPLv2 Community Rules
  + Emerging Threat (ET) Rules
    - ET Open only
  + OpenAppID Detectors
    - OpenAppID
    - AppID Open Text rules
  + Feodo Tracker Botnet C2 IP rules
* Change your rule update settings to update every 28 days
* Leave all other settings at default
* Now **save** your settings.
* **Question 1.** What does Snort VRT do and why are we enabling it?
* **Question 2.** What is OpenAppID and what is the difference between these two options (OpenAppID and AppID Open Text rules) and why did we enable both?

Now that we have selected our Rules we need to update our Rule Signatures.

* Select Updates from your Services/Snort/ menu bar
* Updates and update all your installed rules Rules
* You should now see all signatures updated.

Once we have installed Snort and added our Rule Sets we need to specify our interfaces to use with snort, since we want to monitor both external and internal traffic we will add both our LAN and WAN interfaces.

* Under Services/Snort/Snort Interfaces
* Add your WAN interface and set your description to **Internet**
  + Accept all other defaults
* Add your LAN interface and set your description to **Internal Network**
  + Accept all other defaults

Now that we have added both our interfaces we want to select which policies and how we will use them for each interface.

* Select the Edit option for your WAN
* Under WAN Categories
  + Use the IPS Policy
  + **Question 3**. What does the IPS Policy do and why are we selecting it?
  + Set IPS Policy Selection to “Security”
  + **Question 4.** What does the IPS Policy Selection do and why did we set our selection to “Security”?
  + For our Select Rulesets (Categories) we will choose **Select All** and **Save** your RuleSets
  + Now **Save** your edits to your interface (bottom of page)

\*\* IPS Policy selections set to Security will supply us with lots of alerts, as we run our security server we might adjust our setting to better suit the data we are trying to capture.

* Edit your LAN Categories to match the configuration of your WAN interface
* **Stop**. Be prepared to demo your WAN and LAN configurations.

Since we have selected OpenAPPID as a Rule option we need to do a little more editing for our LAN

* Select LAN Preprocs
* Expand Application ID Detection
* Enable Both Use OpenAppID to detect various applications and AppID Stats Logging (if required)
* Don’t forget to save your edits.

Since we will be using logging, lets confirm our Log Management settings for both interfaces.

* Select **Log Mgmt** from your Snort menu
* Lets Enable:
  + Auto Log Management
  + Log Directory Size Limit (keep default size)
* Set your appid-alert log retention to 30 days and Max size to 2 MB
* Set your app-stats log retention to 14 days
* **Question 5.** What are the 7 logs are available in your Log Mgmt/Log Size and Retention Limits? What do they capture and how do you access the logs?

Now that we have completed setting up our Snort rules and interfaces we need to turn monitoring on.

* Under Snort Interfaces/Snort Status
* Start your Snort Status for both Interfaces

\*\* **Notice** at this point Blocking is DISABLED because we are using rulesets for detecting only, no blocking has been implemented at this time.

Now let’s see if our PfSense Snort is detecting any Alerts.

* First we will take a minute to generate some traffic, open a second tab in Firefox and go to [www.snort.org](http://www.snort.org)
* Review the website and answer the following question.
* **Question 6.** What is “Talos” and what is it used for and who uses it?
* Now we will use this opportunity to view our alerts
* Move back to your pfSense Dashboard
  + **Hint:** Select the PfSense icon from the top left to take you to your Dashboard.
* Scroll down and confirm you have collected Snort Alerts
* **Confirm** you have successfully collect at least 2 Snort Alerts.

**Question 7.** When we view our PfSense Dashboard we can see several different pieces of information under System Information that help us management our security server. Other then CPU Usage, identify 5 other pieces of information and explain why it is helpful/important to have this data.

Now lets review some traffic data.

* From your PfSense dashboard tabs select Status/Traffic Graph
  + Set your Graph setting to
    - Traffic Graph = LAN
    - Sort by = Bandwidth in
    - Filter = All
    - Display = IP Address

**Question 8.** While watching your Traffic Graph your should see at least 2 or more IPs. Record the 2 IPs from your graph and identify the device they reference. Include a screenshot of your Graph captures and IP capture.

Now that we have successfully setup Snort with some rules and setup logging we will look at some of the other features available in pfSense.

**Task 4 – Install and configure OpenVPN**

We will now setup a VPN connection to our Security Server

* Close your PfSense Web Interface open on your Apache Server
* Create a new Windows 10 22H2 workstation virtual machine.
  + Do a basic install
  + Follow all naming conventions for VM Name, Workstation Name and Default User
  + Set you workstation IP to DHCP for IPv4 and DNS settings
  + Turn off Ipv6
* Log into your new workstation as the Default User
* Now open a new instance of your PfSense Web Interface on your Windows 10 Workstation created above and follow the steps below to setup OpenVPN on your workstation.
* Load PfSense Web Configurator (using LAN IP) on your Workstation **Edge Browser**
* Add your System/Package Manager/Available Packages to install OpenVPN
* Notice OpenVPN is not in our list of available packages because it is already part of pfSense but we need to install the add-on tool “openvpn-client-export” package
* Confirm the package has installed by selecting your Installed Packages

Now lets create our first VPN

* Configure your VPN under VPN \OpenVPN\Wizards
* Leave the type set to Local User Access
* **Stop**. Take a screenshots of your CA settings (see below):
* Create a New Certificate Authority (CA) Certificate
  + Descriptive Name: VPN CA
  + Key Length: 2048 bit
  + Lifespan: 200 days
  + Country Code: CA
  + Province: NS
  + City: Halifax
  + Organization: YourLastName
* **Add new CA**
* Now create a New Server Certificate
  + Descriptive Name: VPN Cert
  + Lifespan: 200
  + Keep all other default information
* **Create the Cert**
* General OpenVPN Server Information
  + Accept all defaults except:
    - Description: ISEC\_VPN
* Cryptographic Settings
  + Accept all defaults
* Tunnel Settings
  + Tunnel Network: 192.168.99.0/24
    - Tunnel network is the IP range which will be used for the systems while in the VPN tunnel
  + Local Network: 192.168.208.0/24
  + Concurrent Connections = 3
  + Accept all other defaults
* Client Settings
  + DNS Server 1: 8.8.8.8
  + Accept all other defaults
* **Next**
* Firewall Rules
  + Traffic from client to server: check box
  + Traffic from clients through VPN: check box
* That was our last configuration so you can select finish to end the wizard
* **Next**
* **Finish**

Now we will complete the rest of our configurations in OpenVPN.

* If required, select Servers, notice our WAN is now listed
* Edit your WAN interface information
  + **Server mode:** Remote Access (User Auth)
    - Note - Remote Access (SSL/TLS and User Auth) creates/requires a certificate for each user.
  + **Stop**. Take a screenshot of your Server Mode setting.
  + Don’t forget to scroll to the bottom of the page to save our new Server Mode settings.

We will now create a user in pfSense who will be allowed to use our VPN

* From your pfSense dashboard System/User Manager/Users and **Add** the following user
  + Username: CBruce
  + Password: Passw0rd
  + Full name: Charlotte Bruce
  + Account expires: Dec 25, 2024
  + Member of: admins group
* **Stop**. Take a screenshot of your new user information for CBruce.
* Don’t forget to scroll to the bottom of the page to save our new Server Mode settings.

Now we will export our VPN Client to our Windows 10 workstation

* From our pfSense dashboard select VPN/OpenVPN/Client Export
* Scroll down until you see your OpenVPN Clients
* Notice all the configuration options available under OpenVPN Clients (Export)
* Select the -*Current Windows Installer* (2.5.x)
* Download your installer to C:\OpenVPN on your Windows workstation
* Wait: Notice that Edge does not allow you to download the file as it may be unsafe.
  + Right click on the … next to the file in the Downloads window and select **Keep**.
  + Now select Show more in the next window and select **Keep anyway**.
* Run the installer
* **Note**: You may receive a Windows Protected your PC warning select more info and run anyway.
* Accept all defaults for your OpenVPN Client install.
* Test your OpenVPN client by selecting your desktop shortcut and connect your VPN
  + Remember to login as your VPN user you set up earlier (CBruce)
* **Stop**. Take a screenshot of your new successful VPN connection include your IP information in your screenshot. Note: You may right click on your VPN in your Taskbar and select Show Status to see all the required information.
* **Do NOT log out of your VNP connection as we will do a little testing first**.

Note that since we setup all out configurations and requirements prior to creating our Client there is no need to add any additional settings, IPs, etc.. in order to connect our VPN. We are only required to authenticate with a valid user.

Now that we have successfully setup OpenVPN and connected let view our System Logs.

* If required Log back into your Apache Server and Open your PfSense Web Interface
* From your PfSense dashboard select Status/System Logs/OpenVPN
* **Stop**. Use a screenshot to capture the IP and Username that successfully authenticated through OpenVPN to your server. Notice the information matches your information captured on your Windows workstation. \*\* Ensure the IP matches the information not just see if it is the same but confirm it is the same.

It is important to keep an up to date record of all changes and modifications made to your server and have a reliable copy available as backup.

* Add lines to the end of your pfSense VM vmx (See Course Resources).
* Take a final snapshot of your pfSense Server in the OFF state
* Create a “Gold” copy of your pfSense Server on your portable drive and take a screenshot of the properties and add it to your documentation.
* Add all supplementary documentation, questions and screenshots to your professional document.
* **Upload your professional documentation to Brightspace.**
* **\*\* You should have two (2) uploads for this assignment.**

**Marking Rubric – Individual Mark**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Incomplete**  **0** | **Developing**  **1** | **Good**  **2** | | **Professional**  **3** |
| **Glossary Term 1.**  **Application Detection such as OpenAppID** | No attempt made to create glossary. | Glossary term missing definitions, sections or definitions are incomplete or unclear. Contains some required information but missing some key required data, information or clarity. **Sources not cited.** | | Glossary term meets **most** requirements. Contains most definitions and information but missing some key required data, information or clarity. Not in Appendix A. **Some sources cites or sources not cited in correct format.** | Glossary term meets **all** requirements. Contains all required definitions and information is clear and concise. **Sources cited.** |
| **Glossary Term 2.**  **IDS (in reference to security servers)** | No attempt made to create glossary. | Glossary term missing definitions, sections or definitions are incomplete or unclear. Contains some required information but missing some key required data, information or clarity. **Sources not cited.** | | Glossary term meets **most** requirements. Contains most definitions and information but missing some key required data, information or clarity. Not in Appendix A. **Some sources cites or sources not cited in correct format.** | Glossary term meets **all** requirements. Contains all required definitions and information is clear and concise. **Sources cited.** |
| **Glossary Term 3.**  **IPS (in reference to security servers)** | No attempt made to create glossary. | Glossary term missing definitions, sections or definitions are incomplete or unclear. Contains some required information but missing some key required data, information or clarity. **Sources not cited.** | | Glossary term meets **most** requirements. Contains most definitions and information but missing some key required data, information or clarity. Not in Appendix A. **Some sources cites or sources not cited in correct format.** | Glossary term meets **all** requirements. Contains all required definitions and information is clear and concise. **Sources cited.** |
| **Glossary Term 4.**  **SNORT (Network Intrusion Detection & Prevention System)** | No attempt made to create glossary. | Glossary term missing definitions, sections or definitions are incomplete or unclear. Contains some required information but missing some key required data, information or clarity. **Sources not cited.** | | Glossary term meets **most** requirements. Contains most definitions and information but missing some key required data, information or clarity. Not in Appendix A. **Some sources cites or sources not cited in correct format.** | Glossary term meets **all** requirements. Contains all required definitions and information is clear and concise. **Sources cited.** |
| **Glossary Term 5.**  **Virtual Private Network, how do they work and why have them?** | No attempt made to create glossary. | Glossary term missing definitions, sections or definitions are incomplete or unclear. Contains some required information but missing some key required data, information or clarity. **Sources not cited.** | | Glossary term meets **most** requirements. Contains most definitions and information but missing some key required data, information or clarity. Not in Appendix A. **Some sources cites or sources not cited in correct format.** | Glossary term meets **all** requirements. Contains all required definitions and information is clear and concise. **Sources cited.** |
| **Document Professionalism** | No attempt made to follow professional document requirements. | Documentation missing sections or meets some professionalism requirements. Contains some required sections and information missing some key required data, settings or configurations. Lacking polish, spelling and grammar issues. | | Documentation meets most professionalism requirements. Contains most required sections and information missing some required data, settings or configurations. All sources are cited. Requires some polish, some spelling or grammar errors. | Documentation meets all professionalism requirements. Contains required sections, information, data, settings and configurations. All sources are cited. Well polished, professional document. |

**Marking Rubric – Team Mark**

|  |  |  |
| --- | --- | --- |
| **Value** | **Marks** | **Task** |
|  |  | **Task 1 –** **Install your pfSense Security Server** |
| 4 |  | Followed naming convention for VM and meets hardware requirements:   * 40g drive * 4g memory * 1 Processor / 1 Cores * **Two (2)** NICS (set both to NAT) * **Virtual Machine Description completed including correct password (after modification)** |
| 2 |  | LAN set to 192.168.208.100/24  WAN IP set by default (192.168.208.128..) |
| 12 |  | Log into pfSense Dashboard to show 3 columns and:   * + System Information   + Interfaces   + Gateways   + Installed Packages   + OpenVPN   + Services Status   + S.M.A.R.T. Status   Check configurations on Dashboard:   * + Hostname and Domain (pfSenseyourintials. yourinitials.isec3700.ca)   + DNS includes (8.8.8.8 and 8.8.4.4)   + Timezone = ADT 2022 |
| 2 |  | Select WAN interface to confirm:  Reserved networks are unchecked. |
| 4 |  | Created backup folder in correct location and backup XMl for pfSense server.  **Documents\ PfSense \_Config \_Backups\.......xml** |
| 3 |  | Snort rules have been correctly enabled and updated.  **Services\Snort\Update Rules** |
| 5 |  | Confirm Snort interfaces and settings:   * + WAN (Internet) (started)   + LAN (Internal Network) (Started)   + WAN & LAN settings:   + IPS Policy | Security | all rule sets selected.   LAN PreProcs:   * + Application ID Detection   + Both OpenAPPID and APPID selected |
| 4 |  | Snort \Log Mgmt   * + Enabled Auto Log MGT and Log Directory Size   + Set your appid-alert log retention to 30 days and Max size to 2 MB   + Set your app-stats log retention to 14 days |
| 10 |  | Be prepared to demo your OpenVPN connection with Charlotte Bruce. |
| 2 |  | Snapshot of Server before SNORT and post assignment |
| **48** |  | **Total Marks for comprehensive** |

|  |  |  |
| --- | --- | --- |
|  |  | **Documentation as submitted to Brightspace** |
| 2 |  | Record your IP LAN and WAN settings and add the information to your documentation. |
| 2 |  | Question 1 |
| 4 |  | Question 2 |
| 2 |  | Question 3 |
| 2 |  | Question 4 |
| 3 |  | Question 5 |
| 4 |  | Question 6 |
| 2 |  | Question 7 |
| 3 |  | Question 8 |
| 2 |  | Screenshot(s) of your CA settings |
| 2 |  | Screenshot of your Server Mode setting. |
| 3 |  | Screenshot of your new user information for CBruce |
| 5 |  | Screenshot of your new successful VPN connection include your IP information in your screenshot. Note: You may right click on your VPN in your Taskbar and select Show Status to see all the required information. |
| 2 |  | Screenshot to capture the IP and Username that successfully authenticated through OpenVPN to your server. Notice the information matches your information captured on your Windows workstation. |
| 2 |  | Gold copy properties including location, creation and modification dates and size. |
| 2 |  | Document Creation and Professionalism |
| **42** |  | **Total Marks for D2L Submissions** |
|  |  |  |
| **90** |  | **Total Assignment Marks.** |