**Assignment 4: (Team and Individual Assignment)** Install and configure Proxy Server and Authentication Server using Squid and FreeRADIUS3. *(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 Monitoring and Auditing Sever from assignment 3
* Windows 10 workstation from assignment 2

**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, research and troubleshooting.**

**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 –Update YourInitials\_ISEC2700\_Glossary document.**

**\*\* 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 Glossary and submit it you’re your personal drop box.

*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 make sure to include at least **one example** where possible, and add your research to your Glossary document:

1. Proxy Server. What is this and what are the advantages and disadvantages is using a Proxy?
2. Reverse Proxy Server. What is this and what are the advantages and disadvantages is using a Reverse Proxy?
3. Transparent Proxy. What is this and what are the advantages and disadvantages is using a Transparent Proxy?
4. Proxy Port, what is the default port? Would you change this port and if so why otherwise, why not?
5. Google Safe Browsing. What is it and what resources are required to configure it? Would you recommend using Google Safe Browsing and why or why not?
6. How does radius authentication work?

**Team Portion of Assignment**

**Task 2 - Install and configure a Squid Proxy Server**

We will be adding Squid Proxy to your PFSense Security Server so first we must

* Add the “**squid**” Package to our PFSense (do Not install the Light version).
* Confirm package is installed.
* Do any updates if required.

Now we will configure our **Squid Proxy Server** service on our pfSense server.

* Under Local Cache
* Set your Hard Disk Cache Size to 200
* Do not adjust your squid Memory Cache settings but **Record** the maximum object size value you can have based on your installed RAM and add it to your documentation.
* Enable Cache Dynamic Content
* Don’t forget to save your settings

Now we will complete the rest of our configurations

* Under General Squid Settings
  + Enable Squid Proxy
  + Disable Keep Settings/Data
  + Confirm your Proxy Interface is set to LAN
  + Allow Users on Interface
  + Enable Resolve DNS IPv4 First
  + Don’t forget to **save** your settings
* Do not adjust the port settings **Record** the default Proxy and SSL Proxy ports in your documentation.
* For proper reconfiguration reboot your PFSense server from your pfSense web interface to restart all services. **Record** where to find your reboot command from your pfSense web portal and add it to your documentation.
* Log back into your PFSense Web interface
* View under Status/Services to confirm your Squid Proxy server is started
* *Make sure to record your settings and configurations made to your Server Journal.*

Now that we have setup our Proxy Server lets do some testing.

* First we will need to manually direct our browser through our Proxy Server
  + Edit your windows workstation Proxy Settings for your new Proxy server
  + Set your Preference to Manual proxy setup
  + Remember which interface and port you configured for your Squid

Now that we have configured our Squid Proxy and setup our browser traffic to direct it through our proxy let’s setup some ACLs

* If required log back into your PFSense
* Find your Squid Proxy ACLs
* Using your Blacklist block the domains
  + nscc.ca
  + reddit.com
* Save your ACLs

Let’s test our new settings

* Open your Edge browser and go to reddit Halifax ([www.reddit.com/r/halifax/](http://www.reddit.com/r/halifax/) )
* Now let’s visit nscc.ca
* Oops, we made a mistake and didn’t mean to block nscc.ca as they are our hosting organization
* Remove nscc.ca from the Blacklist ACL and add them to the Whitelist
* In your Edge browser, try visiting nscc.ca again

Now let’s make one more change for security reasons

* In your general settings for your Squid Proxy, modify your Proxy Port to use **1377**
* Now let’s do one last test. In your Edge Browser go to apple.com
* OK, we see we were successful in finding the site. Let’s update our ACL blacklist by adding the domain **apple.com**
* Test your new listing by putting apple.com in your edge browser again

**Task 3 - Configure Virus Scanner on your PFSense Security Server**

* Let’s view the status of our services in PFSence as we did previously. Notice there is already an antivirus installed by default with Squid Proxy but it is not running.
* **Record** the name of the antivirus and add it to your documentation.

Let’s setup Squid to work with our Antivirus.

* In our **Squid Proxy Server** dashboard select your Antivirus
* Enable AV

Notice we have the option to redirect our users to a URL if a virus is detected. This seems like it would be a great idea to make users aware of any potential issues and what steps they should take to protect their workstations.

* Create a small HTML webpage on your **Ubuntu Server** that:
  + Identifies Company Inc as the organization
  + Includes the company logo in the form of a graphic
  + Notifies users that a Virus has been detected on this page
  + Contains contact information about the Network Administrator
  + Contains an email link to the Network Administrator (NetAdmin@CompanyInc.ca)
  + Includes a coloured background
  + Is properly formatted (looks professional not all aligned to one side)
  + Save your file and logo graphic to your /var/www/html directory Hint: Don’t forget to set your permissions
* Set your Redirect URL to your webpage you created. You MUST use an <http://format>
* Set your Antivirus Database to update every 24 hours
* Set your Regional ClamAV Database Update Mirror to Canada
* Force an update immediately for your antivirus (hint: you may need to save your settings before you can update)
* Check your Real Time “freshclam logs” to confirm your database is up to date.
* **Include** a copy of your Web Page (with correct content and formatting) converted to text in your Professional Documentation.
* **Stop.** We have made some significant changes so this might be a good time to take a snapshot of our pfSense server and Windows workstation.

**Task 4 – Install and configure a radius server**

First we will need to add the freeradius3 package to our pfSense

* Add freeradius3 package
* Confirm your package has been installed by viewing your installed packages

Now we will setup and configure our freeradius3

* Open your FreeRADIUS service and configure your Interfaces with the following settings:

Add a New **Interface**

* Interface IP = \*
  + This will allow it to bind to all interfaces
* Leave default port
  + **record** default port and add to your documentation
* Interface Type = Authentication
* IP Version = IPv4
* Description = “Authentication – ‘FirstInitialLastInitial’”
* Don’t forget to save your settings
* Repeat steps to create Accounting Interface
* Set default port to the next port (1813)
* Description = Accounting – “YourInitials”
* Don’t forget to save your settings
* **Question 1.** What is the difference between and Authentication interface and an Accounting interface? Why do we have both?
* Now we will Add and configure our **NAS/Client** for our freeRADIUS server
* Add a new Client IP Address
* Client IP = pfSense WAN in CIDR
* Client IP version = IPv4
* Client shortname = RadiusNAS
* Shared secret = Passw0rd123
* Don’t forget to save your settings

Now we will configure our authentication settings for pfSense

* From your Dashboard select System/user manager/authentication server/
* Add a new server with the following settings:
* Descriptive name = FreeRADIUS Auth Server
* Type = radius
* Protocol = MS-CHAPv2
* Hostname or IP = pfSense LAN
* Add shared secret from above
* Notice the Radius NAS IP Attribute = our WAN (if WAN not selected please select)
* Reboot your system from your pfSense Dashboard to confirm your new packages and settings.

Now we will setup a couple of new users we can use to test our radius with.

* Services/freeRADIUS/Users
* Add a new user:
  + Username = ABrown
  + Password = Passw0rd
* Save
* Add a second user:
  + Username = EOrca
  + Password = Passw0rd
* Save

Now let’s test our new users have the ability to authenticate by running a test.

* Diagnostics /Authentication
* Authentication server = FreeRADIUS Auth Server
* Username = ABrown
* Password = Passw0rd
* Now repeat for EOrca
  + BUT use Password = Passw0rd2
  + Repeat one more time with the correct password.
* Hint: If your authentications fails when it should pass, I recommend checking and resaving your NAS/Client and Authentication Server settings. Then restart your pfSense again.

We have now confirmed our users are created and Radius authentication is working locally.

Now we will setup a modified VPN to use as our Radius connection

* **Disable** (Do not delete) your previous OpenVPN Server
* OpenVPN/Wizards/OpenVPN Remote Access Server Setup/Server Type = RADIUS
* Radius Server = FreeRADIUS Auth Server
* Keep your VPN CA and VPN Cert from your previous configuration
* General OpenVPN Server Information
  + Accept all defaults except:
    - Description: **Radius ISEC\_VPN**
* Since we have made some changes to our VPN we will need to download your new VPN client to your windows workstation
* To remove any confusion between the two OpenVPN clients, uninstall your old client and clean out (**delete**) all OpenVPN directories (2 locations) left behind after uninstalling.
* **Stop.** Record the location of your two OpenVPN directories left behind after your uninstall and ABroadd them to your documentation.
* Download and install a new copy of the client export as we will now be connecting via freeRADIUS3.
* Now test your new RADIUS configuration by connecting your Windows Client via OpenVPN using the ABrown and then EOrca.
* **Record** the IP assigned to each user once they authenticated through Radius.
* Confirm internet access by going to Google.ca
* If either user is not able to successfully connect please troubleshoot the issue.
* To confirm our only users that have authentication via RADIUS are ABrown and EOrca, try to authenticate to your OpenVPN as CBruce.
* We are now going to setup some new security for our Radius. This would be a good time to take a new **snapshot** of your pfSense server.

OK, so we have confirmed radius authentication is working with our OpenVPN client. Now we will set a specific IP and security for each connection through the client.

* If required log back into your Ubuntu Server and pfSense dashboard.
* Service/FreeRADIUS users/users
* Modify the following information for ABrown
  + IPv4 Address = 192.168.99.50
  + Subnet mask = as required
  + Account **expiration** = Nov 1, 2025
  + Available login time = Tuesday and Thursday between 8:30 and 3:30 ONLY
* Modify the following information for EOrca
  + IPv4 Address = 192.168.99.51
  + Subnet mask = as required
  + Account expiration = Dec 31, 2025
  + Available login times = Weekdays 8:30 – 5:30 pm
* Reconnect each user via OpenVPN and check they are receiving the correct IPs as assigned
* **Stop**. Copy the log for ABrown after login that shows the correct IP assignments at connection.
* Notice the Warning in the log. Remove the warning and add extra security to your connection by modifying the openVPNConfig file as identified in the error.
* **Stop**. Record the steps used to modify the config file.
* Log in as EOrca and to confirm the error is gone.
* **Stop**. Copy the log for EOrca that shows the correct IP assignments and does NOT show the warning.

We have confirmed our users are authenticating and getting the correct IPs. Now let’s confirm our other settings.

* Attempt to authenticate ABrown during a time outside of their Available Login time. **Record** your results with a screenshot.

**Question 2.** Identify 4 security advantages you have if you are able to assign a specific IP to a user when authentication via Radius.

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.

* Take a snapshot of your pfSense Server in the OFF state
* Take a snapshot of your Windows workstation in the OFF state
* Create a “Gold” copy of your pfSense Server and include a screenshot of your Gold Copy properties with all required information.
* Include all requested **transcripts, scripts and reports** in your documentation.
* Add all supplementary documentation, questions and screenshots to your professional document.
* Add your Glossary Document as **Appendix A in** your documentation.
* **Upload your professional documentation to Brightspace.**

**Marking Rubrics – Individual Portion of Assignment**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Incomplete**  **0** | **Developing**  **1-2** | **Good**  **3-4** | | **Professional**  **5** |
| **Proxy Server** | No attempt made to complete. | 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.** | | Meets **most** requirements. Contains most definitions and information but missing some key required data, information or clarity. **Some sources cites or sources not cited in correct format.** | Meets **all** requirements. Contains all required definitions and information is clear and concise. **Sources cited.** |
| **Reverse Proxy Server** | No attempt made to complete. | 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.** | | Meets **most** requirements. Contains most definitions and information but missing some key required data, information or clarity. **Some sources cites or sources not cited in correct format.** | Meets **all** requirements. Contains all required definitions and information is clear and concise. **Sources cited.** |
| **Transparent Proxy** | No attempt made to complete. | 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.** | | Meets **most** requirements. Contains most definitions and information but missing some key required data, information or clarity. **Some sources cites or sources not cited in correct format.** | Meets **all** requirements. Contains all required definitions and information is clear and concise. **Sources cited.** |
| **Proxy Port** | No attempt made to complete. | 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.** | | Meets **most** requirements. Contains most definitions and information but missing some key required data, information or clarity. **Some sources cites or sources not cited in correct format.** | Meets **all** requirements. Contains all required definitions and information is clear and concise. **Sources cited.** |
| **Google Safe Browsing** | No attempt made to complete. | 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.** | | Meets **most** requirements. Contains most definitions and information but missing some key required data, information or clarity. **Some sources cites or sources not cited in correct format.** | Meets **all** requirements. Contains all required definitions and information is clear and concise. **Sources cited.** |
| **Radius Authentication** | No attempt made to complete. | 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.** | | Meets **most** requirements. Contains most definitions and information but missing some key required data, information or clarity. **Some sources cites or sources not cited in correct format.** | Meets **all** requirements. Contains all required definitions and information is clear and concise. **Sources cited.** |

**Marking Rubrics – Team Portion of Assignment**

|  |  |
| --- | --- |
| **Value** | **Task** |
|  | **Task 1 –** **Install your pfSense Security Server** |
| 2 | Open pfSense web portal\Installed packages to confirm packages installed. |
| 2 | Demo correct Status of Squid |
| 4 | Confirm correct Squid Proxy Server / ACLS and port are correct |
| 10 | Virus redirection page demonstration with correct information. |
| 2 | Antivirus is enabled and configured.   * Open “freshclam logs” |
| 4 | FreeRADIUS Interfaces are correctly configured: |
| 2 | FreeRADIUS NAS/Client is correctly configured |
| 4 | Confirm Authentication Server and configuration: |
| 6 | Radius user and user configuration is correct |
| 10 | Be prepared to demo your OpenVPN connection EOrca |
| 2 | Snapshot of pfSense Server |
| **48** | **Total Marks for comprehensive** |
|  | **Documentation as submitted to Brightspace** |
|  |  |
| 2 | **Record** the default Proxy and SSL Proxy ports |
| 1 | **Record** where to find your reboot command from your pfSense web portal |
| 1 | **Record** the name of the antivirus |
| 3 | **Include** a copy of your Web Page (with correct content and formatting) converted to text in your Professional Documentation. |
| 1 | **record** default port for the FreeRADIUS interface |
| 4 | **Question 1.** What is the difference between and Authentication interface and an Accounting interface? Why do we have both? |
| 1 | Record the location of your two OpenVPN directories |
| 2 | **Record** the IP assigned to each user once they authenticated through Radius (ABrown and EOrca) |
| 2 | Copy the log for ABrown after login that shows the correct IP assignments at connection. |
| 2 | **Stop**. Record the steps used to modify the config file. |
| 2 | Copy the log for EOrca that shows the correct IP assignments and does NOT show the warning. |
| 4 | **Question 2.** Identify 4 security advantages you have if you are able to assign a specific IP to a user when authentication via Radius. |
| 1 | Screenshot of Gold copy properties for pfSense Server including location, creation and modification dates and size. |
| 1 | Document Creation and Professionalism |
| **27** | **Total Marks for D2L Submissions** |
|  |  |
| **75** | **Total Assignment Marks.** |