Working with pfSense and pfBlockerNG

Learning objective: Configure pfBlockerNG in pfSense to block malicious IP addresses and analyze blocked traffic.

Follow the steps provided below and capture screenshots to document the process accurately

**Configure and prepare pfBlockerNG**

1. Open a web browser on a Windows 10/11 machine and enter the IP address of Pfsense LAN in the URL address bar and log in to pfSense using the following credentials:

Username: admin Password: pfsense

1. Go to "System" and select "Package Manager."
2. In the Package Manager, click on "Available Packages."
3. Find and install "pfBlockerNG-devel" package.
4. Once the installation is complete, go to "Firewall" and select "pfBlockerNG."
5. Click on "Next" to finish the setup process.
6. Enable pfBlockerNG by setting it to "Enable" and click on "Save."
7. Go to "Feeds" to select and configure block lists.
8. Review the built-in feeds available for pfSense, such as SANS' Internet Storm, Spamhaus, Talos network analysis, etc.
9. To add additional feeds, click on "Add tag" and choose at least 2 feeds
10. Click on "Enable All" to download existing blocking rules for the selected feeds.
11. Configure the blocking rules choose IP—IPv4:
    * Choose the appropriate Alias from the drop-down list for "Alias Deny"
    * Click on "Save" to apply the configuration.
12. Go to "Update" and click on "Run" to update the feed lists.
13. Navigate to "Firewall," then select "Rules" and "LAN" to view the configured rules.
14. Verify that the rule has been added by hovering the mouse over it to display a list of blocked IP addresses.

|  |  |
| --- | --- |
| Open pfsense |  |
| Go to package |  |
| Install pfblocker |  |
| Packages installed |  |
| Done with installed |  |
| Start configuration |  |
| Click next |  |
| Finish configuration |  |
| Open pfblocker |  |
| Go to feeds |  |
| Enable and add some feeds |  |
| Run update |  |
| Allias deny for feeds |  |
| Results for ip list |  |

**Test**

1. Choose random IP addresses [ at least 4 IPs] from the previously blocked list. For example: IP Address: 1.14.75.32
2. Copy and paste the IP address into a new browser tab and observe that the website does not respond, indicating it has been blocked.

|  |  |
| --- | --- |
| **CHOSE IP AND TESTED** |  |

**Further analysis**

To further analyze the blocked traffic, you can explore the other report options available in pfBlockerNG.

1. Click on "Reports" to access the pfBlockerNG reports.
2. Take screenshots for the following reports :
3. Top sources: This report provides information about the top sources of blocked traffic.
4. Top destinations: This report displays the most blocked destinations.
5. GeoIP: This report shows the geographical distribution of blocked traffic based on IP addresses.
6. DNSBL: This report focuses on DNS-based blocking events.

|  |  |
| --- | --- |
| CLIKC ON REPORT TO SHOW THE REPORT FOR IP |  |

Challenge task

Schedule and Update Settings: configure the update schedule for the block lists and feeds used by pfBlockerNG. This ensures that the lists are regularly updated with the latest threat intelligence.

Note: Here are a few common settings you may come across that you should consider changing, while leaving the other settings as they are or selecting what you find suitable

* Update Frequency: Daily.
* Source Selection: Select the specific threat intelligence sources or block lists
* Update Method: automatic.