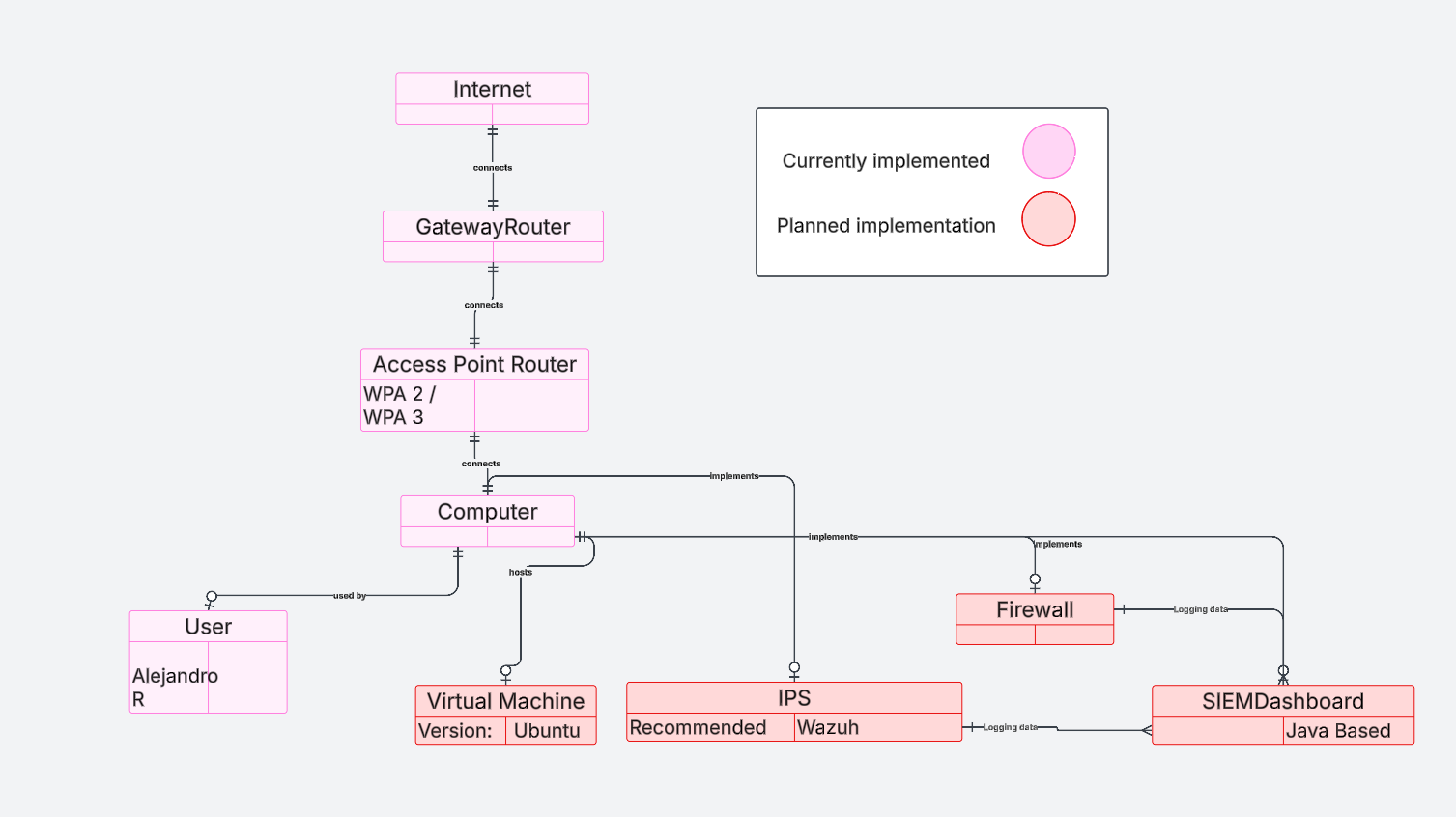
**Threat Modeling**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat** | **Likelihood** | **Impact** | **Prevention / Mitigation** | **Current Standard** |
| Data Loss | Low | High | Cloud backup or physical backup | Microsoft one drive uploaded backup. |
| Weak Passwords or compromised passwords | Medium | Medium | Implement a password manager and 2FA | No active password manager, but 2FA is active for most websites |
| Phishing attacks | High | Medium | Awareness training and filtering out spam emails | Awareness of potential phishing attacks and Gmail filters out spam |
| Malware Infection | Medium | High | Antivirus software installed and up to date. | Microsoft Defender Antivirus is on and up to date. Last checked 3/28/2025 |

The table above is the threat modeling. The modeling takes more of a focus on external threats over internal threats since there is only one authorized user and one device of focus. Some of these threats mitigations can be sources of an idea of further improvement for the home office setup. The data loss line on the table is an example, currently the only backup that is available if the computer hard drive is only cloud source. However, it is a plan for the future to ensure that I have a backup hard drive for the desktop computer in case the hard driver ever suddenly expires without warning. The priority of getting a spare storage device is low. The potential weak passwords are only mitigated by the fact that there is a two factor authentication present. There is room for improvement as a password manager such as KeePassXC can be installed and utilized to generate randomized and strong passwords. This software saves on the computer is not in an online database, but if there is an issue with data loss. This becomes another problem. Of course, passwords can also be saved into a physical book just in case this is a significant issue. Phishing attacks are going to be something that is constant, but Gmail has some filters present. It does not stop all, but it eliminates the majority of phishing emails. The only improvement is to review how to detect a phishing email. The final thing on the threat modeling table is malware infection. Currently, Microsoft defender is the only antivirus this computer utilizes. It previously had Norton, but was installed when it began to request a yearly subscription. The reason that antimalware like Norton is not installed is due to previous experience of maxing out CPU on an old computer and lack of trust in antimalware.

**Entity Relationship**

****

The diagram above is a visualization of all that is planned for this SOHO network project. For reiteration, the goal of this project is to enhance security on a desktop computer without interfering with the bandwidth of other users in the home. In order to maximize security for the desktop computer, there are implementations such as a virtual machine, IPS, a firewall and a SIEM dashboard for logging requirements. The purpose of the virtual machine is that it simulates another computer within a computer. This is useful in case there is ever malware infection. If there is malware present, then with a virtual machine it is not difficult to roll back to a secure snapshot of the virtual machine. The purpose for the IPS is to prevent any unauthorized access from successfully getting onto the desktop. The purpose of modifying the firewall is to limit the attack surface of attackers onto the desktop. The SIEM dashboard’s purpose is to gather logging data from the IPS and firewall logs from the computer. The currently implementations such as the access point utilizes WPA2 and WPA3 security for wireless security. One router only focuses on routing from the modem to the access point router. The last aspect is the internet which hosts many different servers and websites. This SOHO network is not focused on any one particular business organization at this time.