Below is your **sentence-by-sentence study note breakdown** of *“Using Software Firewalls Notes.docx”*, structured professionally for **clean pasting into Microsoft Word**. The formatting uses **tight bulleting**, consistent spacing, and numbered topic headings for clarity and alignment with **CompTIA A+ 220-1102** objectives.

**Using Software Firewalls – Study Notes (CompTIA A+ 220-1102)**

**1. Introduction**

* This session covers how to configure **Windows Firewall** and **Mac Firewall**.
* Both systems offer different interfaces and control levels, but similar principles apply.

**2. Configuring Windows Firewall (Windows Defender Firewall with Advanced Security)**

**2.1 Accessing the Advanced Firewall Console:**

* Open the **Start menu** (Windows key).
* Navigate to **Windows Administrative Tools**.
* Select **Windows Defender Firewall with Advanced Security**.

**2.2 Overview of the Firewall Interface:**

* This interface allows configuration of:
  + **Inbound rules**
  + **Outbound rules**
  + **Monitoring settings**
* Once configured, firewall policies can be **exported** for backup or replication.

**2.3 Profile Overview:**

* Three profiles exist:
  + **Domain profile**: Example shows it is turned off.
  + **Private profile**: Firewall is ON.
  + **Public profile**: Firewall is ON.
* Private and public profiles block **unsolicited inbound traffic**, but allow **outbound connections** unless explicitly denied.

**2.4 Rule Example – SSH (Secure Shell):**

* SSH rule is enabled across all profiles.
* Allows traffic from any program, any local address to any remote address over **TCP port 22**.

**2.5 Rule Example – App Installer:**

* Rule allows **any local address to any remote**, using **any protocol and port**.
* Considered an **“any-any” rule**, which is very permissive and potentially risky.

**2.6 Creating a New Allow Rule – Example: Web Server**

* Click **New Rule**.
* Choose rule type: **Program**, **Port**, **Predefined**, or **Custom**.
* For a web server, select **Port**.
* Choose **TCP** (used for web servers).
* Specify ports: **80** (HTTP) and **443** (HTTPS).
* Choose to **Allow the connection**.
* Choose applicable profiles: typically **Domain**, **Private**, and **Public**.
* Name the rule (e.g., “Jason’s Web Server”).
* Rule allows traffic over TCP from any source to any destination on ports 80 and 443.

**2.7 Creating a Block Rule – Example: Telnet**

* Telnet is considered insecure.
* Create a new rule to block **TCP port 23**.
* Apply the rule to all three profiles.
* Name it (e.g., “Blocking Telnet”).
* This prevents unencrypted Telnet access into the system.

**3. Monitoring in Windows Firewall**

**3.1 Accessing Monitoring Features:**

* View current **active profile**.
* Access **log files** to check:
  + Dropped packets
  + Successful connections
* Logs are configurable to show more detail.

**3.2 Viewing Active Rules:**

* Active rules for the current profile can be reviewed.
* Rules applied to **“All” or “Public”** are visible.
* Rules for **“Private” or “Domain”** are hidden unless that profile is active.

**4. Configuring Mac Firewall (macOS GUI Firewall)**

**4.1 Accessing Firewall Settings:**

* Go to the **Apple menu > System Preferences**.
* Select **Security & Privacy**.
* Click on the **Firewall tab**.

**4.2 Unlocking Firewall Controls:**

* Click the **lock icon** in the lower left corner.
* Enter the **admin username and password** to make changes.

**4.3 Configuration Options:**

* Toggle firewall **ON or OFF**.
* Options include:
  + **Block all incoming connections**
  + View apps that are **allowed through the firewall**
  + Automatically allow **Apple built-in software**
  + Automatically allow **downloaded signed software**

**4.4 Examples of Allowed Applications:**

* **Skype** and **Google Drive** may be allowed for incoming connections.

**4.5 Stealth Mode:**

* **Stealth mode** prevents the Mac from responding to ping requests.
* Helps avoid detection during **ping sweeps or network reconnaissance**.

**4.6 Adding an Application to the Firewall:**

* Click the **plus sign (+)** to add a program.
* Locate the desired application (e.g., Chess) and click **Add**.
* It will **default to allowing** incoming connections.
* To remove it, select the app and click the **minus sign (–)**.

**4.7 Limitations Compared to Windows:**

* macOS GUI firewall offers **limited control** compared to Windows.
* To get **advanced control**, use command-line tools:
  + **PF (Packet Filter)**
  + **IPFW (Internet Protocol Firewall)**

**5. Key Takeaways for the Exam**

* **Windows Firewall with Advanced Security** supports detailed rule sets and profiles.
* **Rules can be created, exported, and managed** for both inbound and outbound traffic.
* **TCP and UDP protocols**, **specific ports**, and **application-based filtering** can be configured.
* **macOS Firewall** offers a **basic GUI interface**, useful for typical users.
* For greater control on macOS, use **terminal-based tools like PF or IPFW**.
* **Stealth mode** is a useful option for security-conscious users on macOS.
* Understanding **firewall rule behavior**, **profiles**, and **port functions** is essential for **CompTIA A+ 220-1102 Objective 2.6 and 4.2**.

Would you like a professionally aligned **quiz** based on this breakdown to test retention and exam readiness?