Below is a **comprehensive, sentence-by-sentence breakdown** of the document titled **“223. Microsoft Defender Firewall Notes”**, structured into professional **study notes format for Word**, with no excessive spacing and all critical points retained. These notes are aligned with **CompTIA A+ 220-1102 Objective 2.5**.

**Microsoft Defender Firewall – Study Notes**

**(CompTIA A+ 220-1102 – Objective 2.5)**

**1. Introduction to Microsoft Defender Firewall**

* Microsoft Defender Firewall is a **built-in host-based (personal/software) firewall**.
* Included by default in **Windows 10** and **Windows 11**—no third-party software required.
* Host-based firewalls protect **individual devices**, while **network-based firewalls** protect traffic at the network perimeter.
* Best practice: **Use both types together** for layered security.

**2. Accessing the Firewall**

* To access:
  + Click **Start/Windows key**
  + Type **"Firewall"**
  + Select **Firewall & network protection** under system settings

**3. Network Profiles**

Microsoft Defender Firewall allows configuration per **network type**:

| **Network Type** | **Description** |
| --- | --- |
| **Domain Network** | Enterprise-managed networks, like corporate LANs. |
| **Private Network** | Trusted networks like home Wi-Fi. |
| **Public Network** | Untrusted networks like cafés or airports. |

* You can **enable or disable** the firewall on each network individually.
* Requires **UAC (User Account Control)** approval to toggle settings.

**4. Activating and Deactivating the Firewall**

* Turning firewall **off** triggers a warning in Windows Security:
  + "Your device may be unsafe."
* To re-enable:
  + Navigate back to the network type
  + Toggle firewall **back to On**
  + Confirm via UAC

**5. Blocking Incoming Connections**

* Each network profile allows the **optional blocking of all incoming connections**, including those from allowed apps.
* Use this in **Public networks** to enhance security.
* If running a **server**, blocking incoming connections may interfere with service delivery.
* To unblock, simply uncheck the block option.

**6. Allowing Apps Through the Firewall**

**6.1 Process to Allow Apps**

* Navigate to **Firewall & network protection**
* Select **Allow an app through the firewall**
* You'll see a list of apps with checkboxes for:
  + **Private network access**
  + **Public network access**

**6.2 Modifying App Permissions**

* Click **Change Settings**
* Approve with **UAC**
* You can then:
  + Enable/disable public/private access per app
  + Add new apps using **“Allow another app”**

**6.3 Adding Custom Apps**

* Use **Browse** to locate the app (e.g., C:\Program Files\OneDrive\OneDrive.exe)
* Choose desired network types (Private/Public)
* Click **Add** → App is now whitelisted

**7. Port Control Limitations and Advanced Security**

* **Basic Defender Firewall GUI does not allow port-specific rules**.
* Port configuration requires using:
  + **Windows Defender Firewall with Advanced Security**

**7.1 Accessing Advanced Security**

* Open **Firewall & network protection**
* Click **Advanced Settings**
* Approve via **UAC**
* Opens the **Advanced Firewall Console**, allowing configuration of:
  + Inbound Rules
  + Outbound Rules
  + Connection Security Rules
  + Monitoring

**8. Creating Inbound Rules (Allowing Traffic)**

**Example: Allow SSH on TCP Port 22**

1. Go to **Inbound Rules** → **New Rule**
2. Choose **Port**
3. Select **TCP**
4. Specify **Port 22**
5. Choose **Allow the connection**
6. Select applicable profiles: **Domain, Private, Public**
7. Name rule: **SSH TCP**
8. Click **Finish**

* Rule now appears with:
  + **Green check mark**
  + **All profiles enabled**
  + **Allow action**
  + **Protocol: TCP**
  + **Port: 22**
  + Applies to all programs and addresses unless further scoped

**9. Rule Scope Configuration**

* You can edit each rule’s **Properties** to define:
  + **Local/remote IP addresses**
  + **Users or computers**
  + **Application packages**
* Allows **fine-grained control** for securing services or restricting access

**10. Creating Inbound Rules (Blocking Traffic)**

**Example: Block FTP on TCP Port 21**

1. Go to **Inbound Rules** → **New Rule**
2. Choose **Port**
3. Select **TCP**
4. Specify **Port 21**
5. Choose **Block the connection**
6. Select all profiles
7. Name rule: **Block FTP**
8. Click **Finish**

* Rule now appears with:
  + **Red circle (block symbol)**
  + **All profiles enabled**
  + **Block action**
  + **Port: 21**
  + Applies broadly unless narrowed with scope

**Summary of Key Functional Areas**

| **Function** | **Description** |
| --- | --- |
| **Firewall Profiles** | Configure protection separately for Domain, Private, and Public networks. |
| **App Whitelisting** | Allow or deny apps through the firewall for selected networks. |
| **Incoming Connection Control** | Block all incoming traffic on public/untrusted networks. |
| **Advanced Security** | Used for creating **port-specific rules** and defining **custom rule scopes**. |
| **Inbound & Outbound Rules** | Control which programs and ports can send/receive traffic. |
| **UAC Elevation** | Required for changing settings or applying new rules. |

**Real-World Examples**

* **Home Office Setup**:
  + Allow apps like Zoom and Outlook through private networks only.
* **Public Network Protection**:
  + Block all incoming connections when using hotel Wi-Fi.
* **IT Technician Configuring FTP Restrictions**:
  + Block TCP Port 21 to prevent FTP traffic on internal servers.
* **Secure Developer Server**:
  + Create inbound rule allowing SSH (Port 22) only on private networks.

**Exam Inclusion Notification**

✔ **Included in the CompTIA A+ 220-1102 Exam**

* Mapped to **Objective 2.5**: *"Given a scenario, manage and configure basic security settings in Microsoft Windows OS."*
* Topics covered:
  + Enabling/disabling firewalls
  + Managing app access
  + Configuring ports via advanced settings
  + Differentiating between network profiles
  + Blocking/allowing traffic at both app and port levels

Microsoft Defender Firewall configuration is a **high-yield scenario** on the A+ 1102 exam.