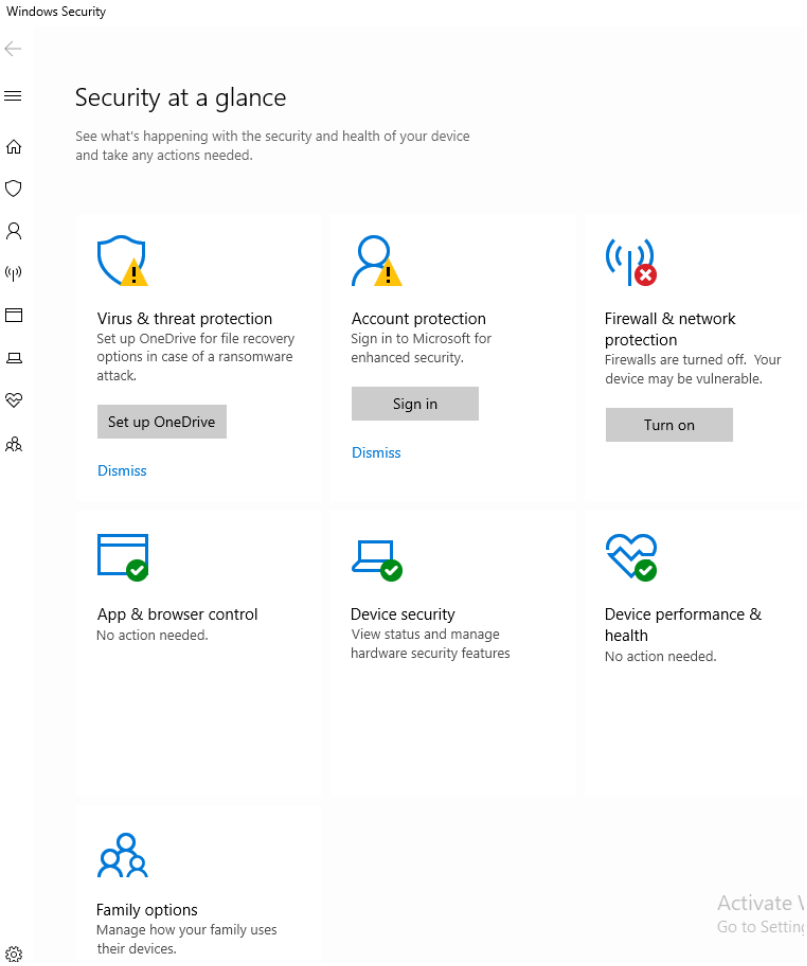
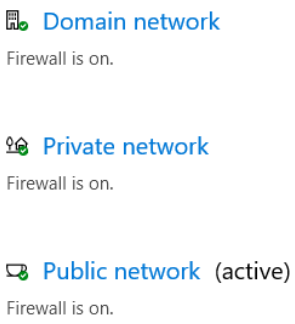
Firewall Configuration Manual for Personal laptops

Description:This manual would be best suited for laptops/Desktops that are meant for personal use, any device being used for commercial purpose must implement the necessary changes required for sattisfying the business needs.

Accessing the defender: In the *Search Bar* , type security. Click on the filtered out option named *Windows Security*. Here you would find multiple options, most probably, the 3rd option would be Firewall and network settings.



The Basics: To turn on the firewall, simply click the turn on button under the Domain network category.



For further configurations, Click on the Advanced Settings option.

Inbound rules (Incoming traffic):

- Starting off by allowing relevant traffic:
  To create an Inbound rule to allow traffic, click on new Rule under Inbound rules section in the right panel. Select on the relevant rule type. Select the relevant interfaces required for configuration. Select if the rule is to allow, block or allow specific connections. Select the network that you want to apply this rule to. Provide relevant name to the Rule and click finish.

Below are some inbound rules to allow connections.

HTTP (Port 80) and HTTPS (Port 443) [Windows Update Service on private and domain network]

Click on New Rule
Select Ports option, Click next
Select TCP and Specific local ports 80,443.
Select Allow Connections.
Uncheck the Public network option.
Feed the name as Windows Update Service.
Click Finish.

More Rules to allow:

- **DNS (Port 53)**
- **DHCP (Port 67 and 68)**
- **Kerberos Authentication (Port 88)**
- **LDAP (Port 389)**
- **SMB (Port 445)**
- **SMTP (Port 25)**
- **Kerberos Change/set Password (Port 464)**
- **TCP 110: POP3 (Post Office Protocol version 3)**
- **TCP 143: IMAP (Internet Message Access Protocol)**
- **TCP 587: SMTP (Submission)**
- **TCP 443: HTTPS (Outlook Web Access)**
- **FTP (File Transfer Protocol): Port 21**
- **SNMP (Simple Network Management Protocol): Port 161**

It is recommended to allow all ports below port number 1024 on private and Domain network.

Now lets block the unnecessary traffic:
Start off by blocking the ports 80 and 443 on public networks

Click on New Rule
Select Ports option, Click next
Select TCP and Specific local ports 80,443.

Select Block Connections.
Uncheck the Private and network option.
Feed the name as Windows Update Service.
Click Finish.

It is recommended to block all incoming traffic except the DNS on a Public network. One can directly select apply to all ports option instead of providing specific port numbers.

One can similarly configure the Outbound rules based on the needs of ports, services, application and more.