

Cyber Security (CSE 4003)

Digital Assignment 2

Name: John Klinges

Reg. No: 15BCE1335

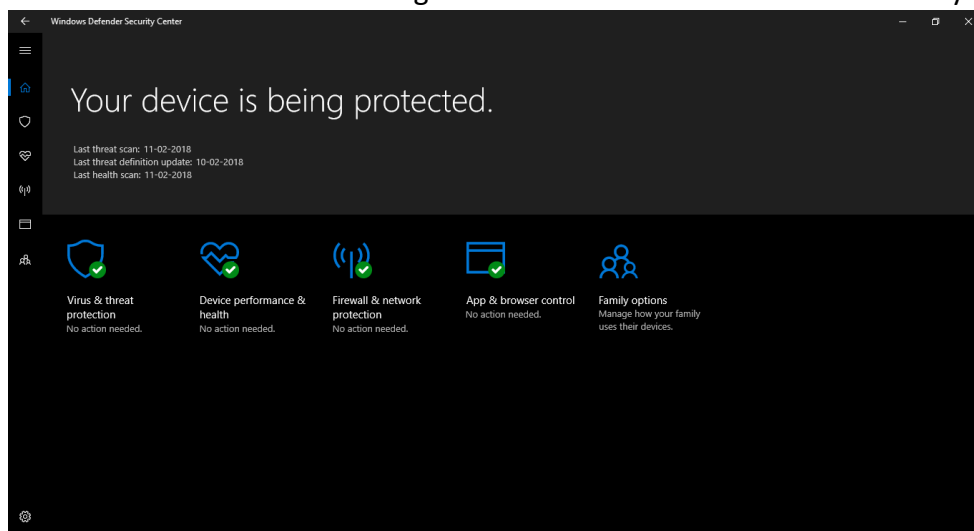
Faculty: Dr. Subbulakshmi T

Question: Process the windows firewall / security settings to have maximum security for your computer.

Solution:

All of the mentioned settings are with respect to Windows 10 Home – v1709 (OS Build 16299.15)

1. Basic Windows Defender settings available in Windows Defender Security Center.

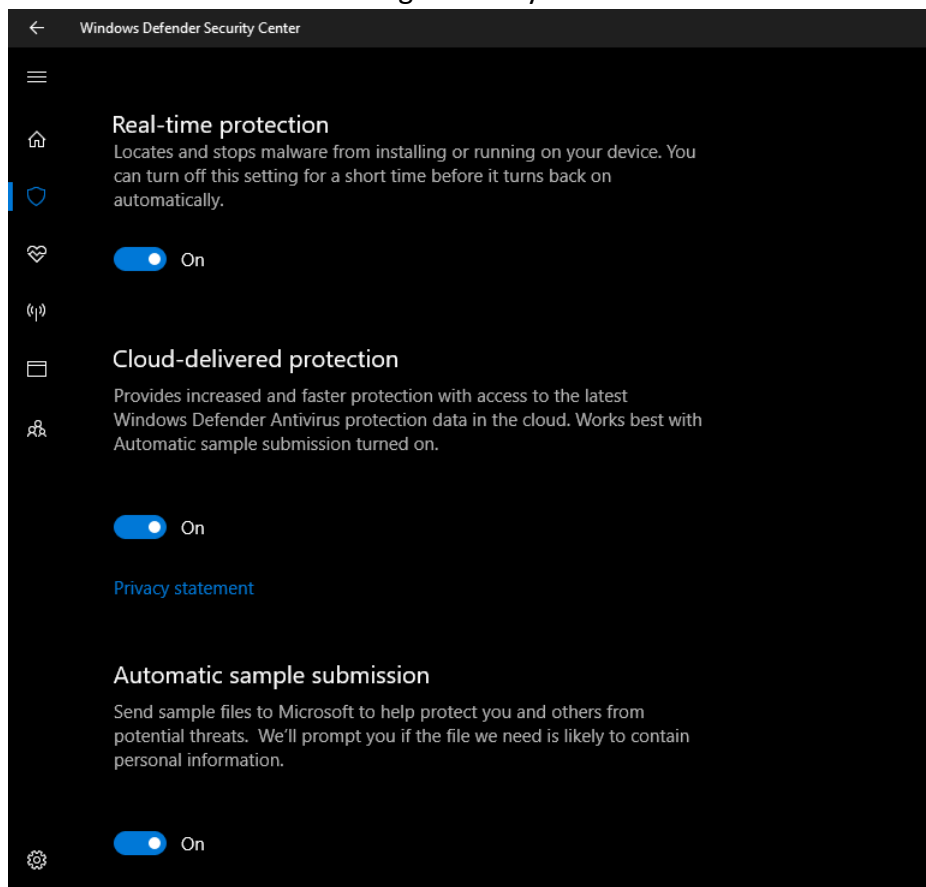


a. Virus & Threat Protection

This includes the automated virus and threat protection settings available from Windows Defender itself. It scans the computer for malicious softwares and viruses. It includes:

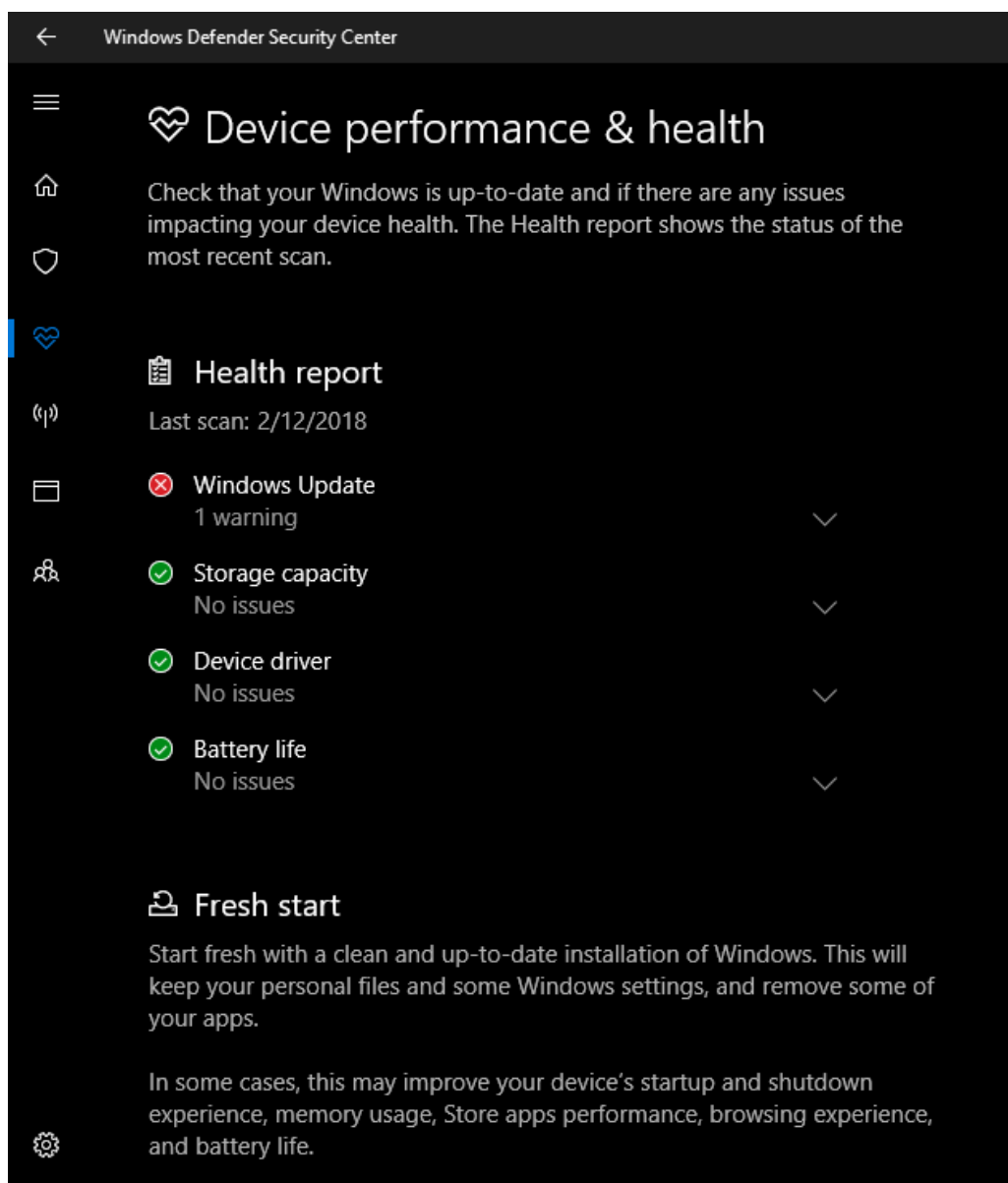
- Real Time Protection
 - This setting is controlled by an automatic triggering service.
 - We can disable this setting for some time before it turns back on automatically.
 - It locates and stops malware from installing or running on your device.
 - Its best to keep it turned on for protection.

- Cloud Delivered Protection
 - It provides protection with the help of Windows defender antivirus protection data in the cloud.
 - It uses our automatic sample submissions of defender log files for personalised maximum protection.
- Automatic Sample Submission
 - Send sample files to Microsoft cloud for protection against potential threats.
 - The reports of the defender are sent regularly to the Microsoft.
- Controlled folder access
 - Protects our files and folders from unauthorized changes by unfriendly applications.
 - These are 3rd party applications installed from sources other than windows store.
- Other Settings
 - Excluded files and folders
 - For manual exclusions
 - Notification Settings
 - To change the way of alerts and notifications.



b. Device Performance and Health

- Checks that the Windows is up-to-date and if there are any issues impacting your device health. The Health report shows the status of the most recent scans.
- This also includes the feature of fresh start which provides user the control the clean the system as in removal of apps and system settings and will provide a fresh system to work with.
- The Health report contains
 - Windows Update
 - Storage Capacity
 - Device Driver
 - Battery Life



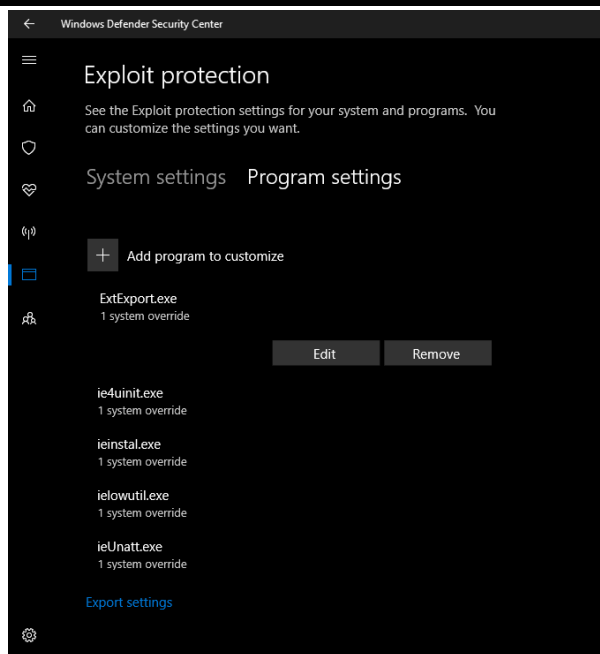
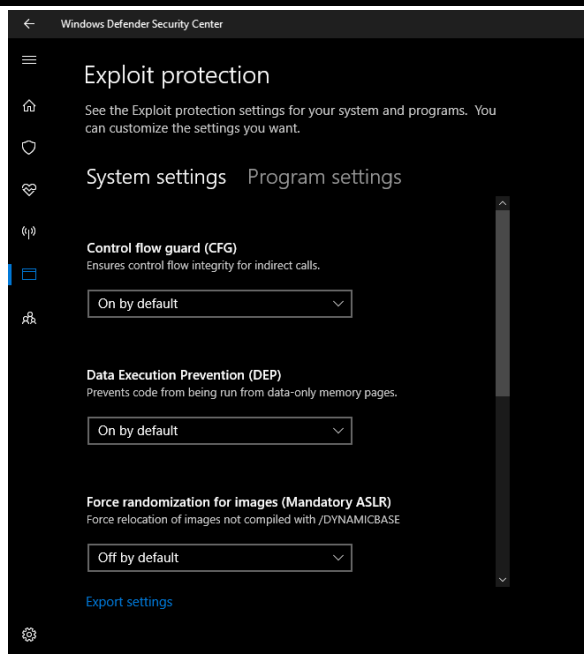
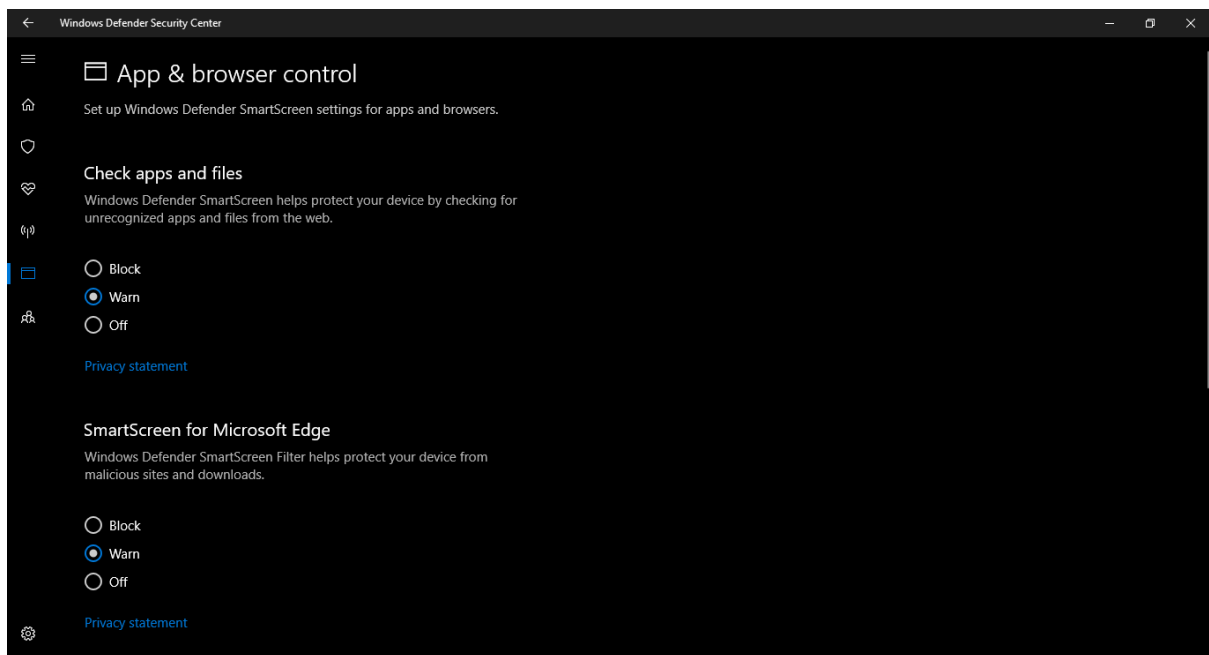
#Note- I have turned off the windows update as it is large in size otherwise its recommended to keep windows up to date.

c. App and browser control

This sets up a Windows defender Smart screen that check unrecognised apps and files from web or malicious sites and downloads, etc.

This includes:

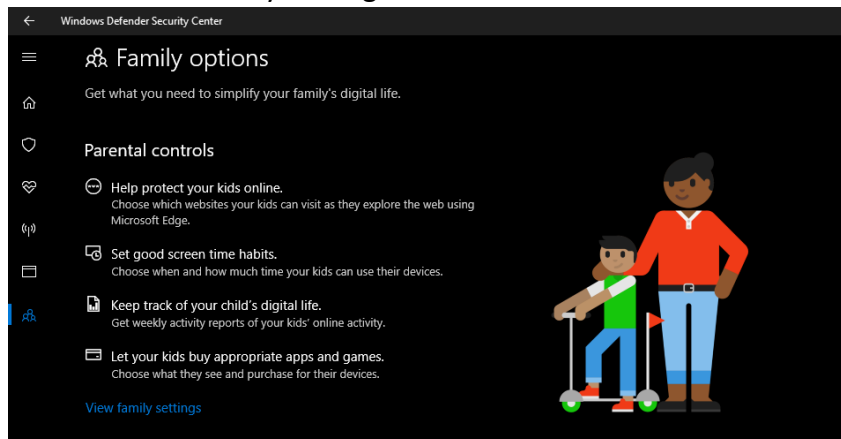
- Check Apps and files
- Smart screen for Microsoft Edge
- Smart screen for Windows Store Apps
- Exploit protection
 - Windows 10 build in feature
 - Automated Protection against attacks
 - System settings (Most are turned ON by default)
 - Control Flow Guard (CFG)
 - Ensures Control flow integrity for indirect calls.
 - Data Execution Prevention (DEP)
 - Prevents code from being run from data-only memory pages.
 - Force randomization for images (Mandatory ASLR)
 - Force relocation of images not compiled with /DYNAMICBASE
 - Such as the relative path not included in production build.
 - ASLR – Address Space Layout Randomization (Memory protection process)
 - Randomize Memory Allocation (Bottom-up ASLR)
 - Randomize locations for virtual memory allocations
 - Done by Virtual Box/ VMWare while creating a virtual environment hard drive.
 - Validate Exception chains (SEHOP)
 - Ensures the integrity of exception chain during dispatch.
 - SEHOP – Structured Exception Handling Overwrite Protection
 - Validate Heap integrity
 - Terminates a process when heap corruption is detected.
 - Heap corruption occurs when a program damages the allocator's view of the heap. The outcome can be relatively benign and cause a memory leak or it may be fatal and cause a memory fault, usually within the allocator itself.
 - Program Settings
 - Gives override access to limited services or apps



d. Family Options (Requires Microsoft login)

Mostly consists of Parental Controls. Includes controls like:

- Manage Apps
- Activity Reporting
- Block Specific sites
- Screen time settings
- Web browser settings
- Purchase and Spending settings
- X-Box Privacy Settings

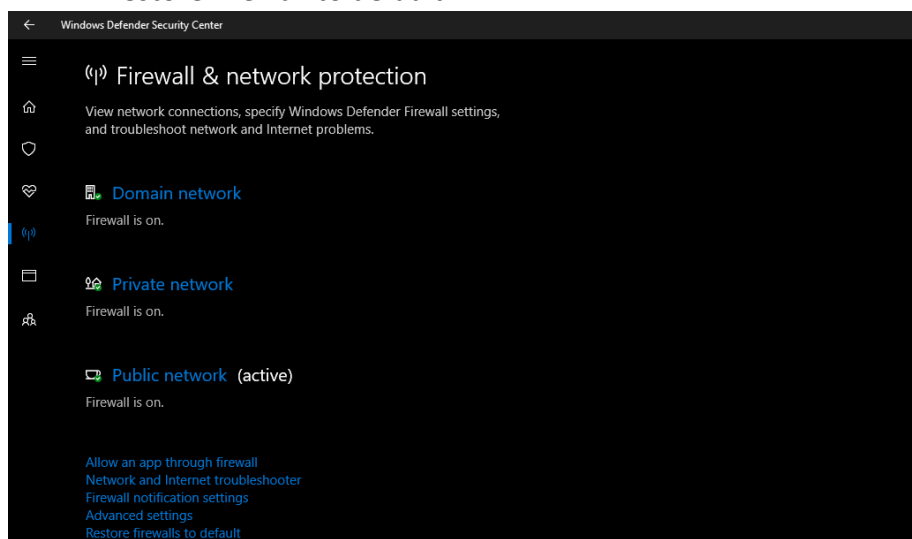


e. Firewall & Network protection

Controls network connections and handles Windows Defender firewall settings. We can change the firewall settings in general for Domain, Private or Public networks.

Other than these general settings we have some additional settings like

- Allow an App through Firewall
- Network and Internet Trouble shooter
- Firewall notification settings
- Advanced Settings
- Restore firewall to default



2. Firewall Settings

a. Allow an App through Firewall

Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Change settings

Allowed apps and features:		
Name	Private	Public
<input checked="" type="checkbox"/> AllJoyn Router	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> App Installer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Captive Portal Flow	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Cast to Device functionality	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Connect	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Core Networking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Cortana	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Delivery Optimization	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> DiagTrack	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> DIAL protocol server	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Distributed Transaction Coordinator	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Dolby Atmos for Headphones	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Details...

Remove

Allow another app...

We can add, change or remove allowed apps and ports through firewall. Only known apps should be allowed through private network and only trusted apps should be allowed through public network for maximum protection.

b. Firewall Troubleshoot

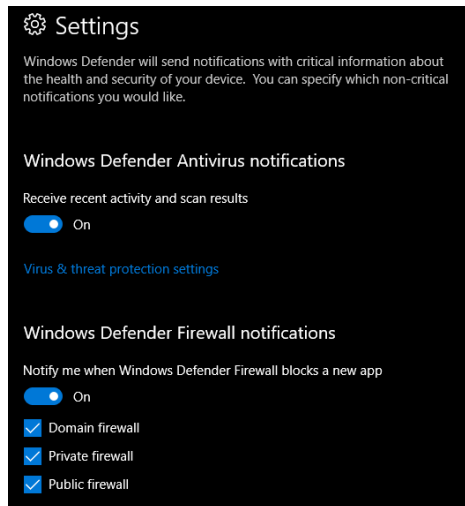
If something isn't working as it's supposed to, then troubleshoot.



Other than the visible settings, we have

- Bluescreen
- Bluetooth
- Hardware and devices
- Home group
- Incoming Connections
- Keyboard
- Network Adapter
- Power
- Etc...

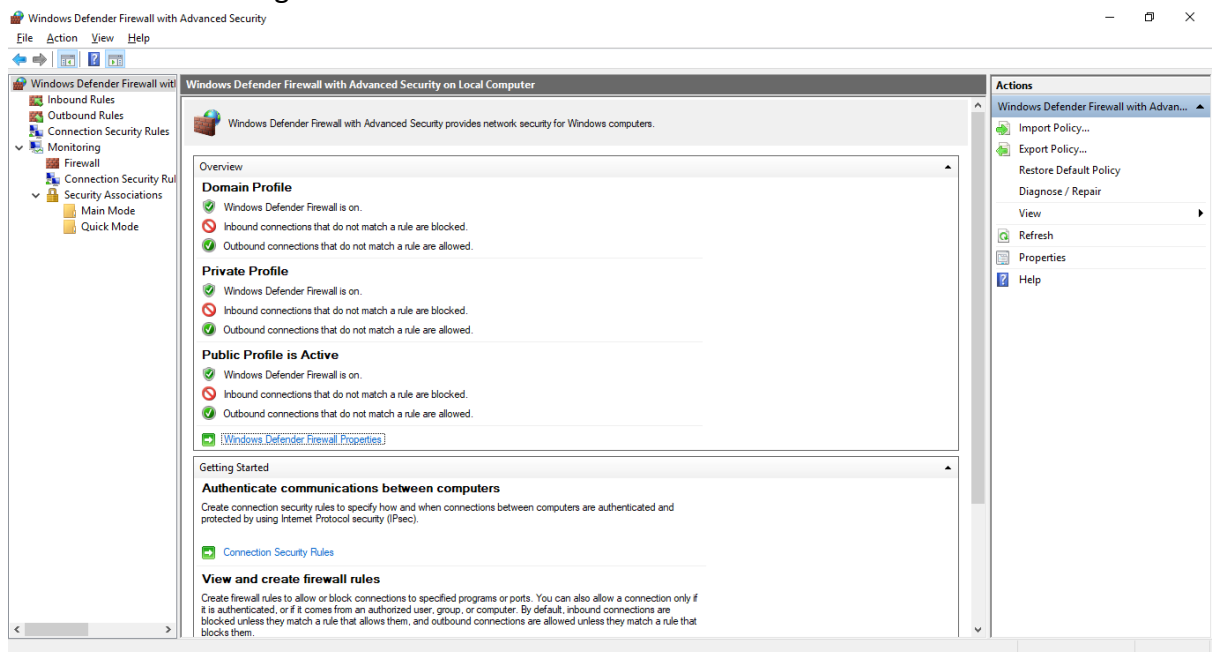
c. Firewall notification



d. Advanced Firewall Settings

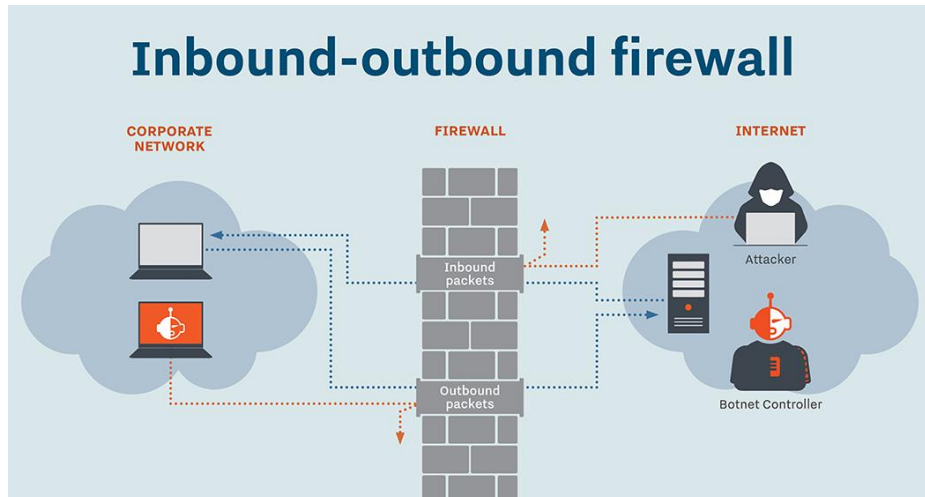
The advanced setting gives us control over the following aspects of firewall

- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring – Gives us control and access over above mentioned settings for the active network.



3. Inbound and Outbound Firewall

An inbound firewall protects the network against incoming traffic from the internet or other network segments, namely disallowed connections, malware and denial-of-service attacks. An outbound firewall protects against outgoing traffic originating inside an enterprise network.



It's actually rare to see an outbound firewall used because of the complexities that it introduces into the network. Oftentimes, outbound firewalls interrupt application traffic, disrupt business workflows and get users upset unless close attention has been paid to configuring the firewall in just such a way to enable everything to work.

The screenshot shows the 'New Inbound Rule Wizard' window. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Rule Type' with the instruction 'Select the type of firewall rule to create.' On the left, a 'Steps' pane lists: Rule Type (selected), Program, Protocol and Ports, Scope, Action, Profile, and Name. The main area asks 'What type of rule would you like to create?' and offers four options:

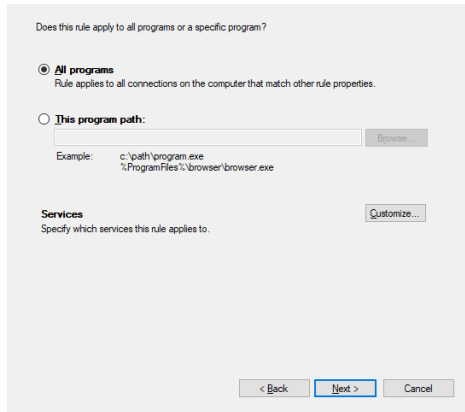
- ☐ **Program**: Rule that controls connections for a program.
- ☐ **Port**: Rule that controls connections for a TCP or UDP port.
- ☐ **Predefined:** A dropdown menu shows 'AllJoyn Router'. Description: Rule that controls connections for a Windows experience.
- ☒ **Custom**: Custom rule.

 At the bottom right are buttons for '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

We can create our own rules to allow or block specific program, port, IP address or specific packets type (TCP, UDP, etc.)

For maximum protection, we can just disable any type of connection with our system over any type of network. To do so, we will create a new rule in both inbound and outbound firewall.

1.



Does this rule apply to all programs or a specific program?

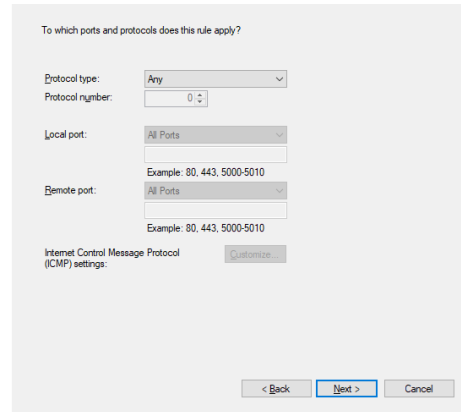
☒ **All programs**
Rule applies to all connections on the computer that match other rule properties.

☐ **This program path:**
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Services
Specify which services this rule applies to.

< Back Next > Cancel

2.



To which ports and protocols does this rule apply?

Protocol type: Any

Protocol number: 0

Local port: All Ports

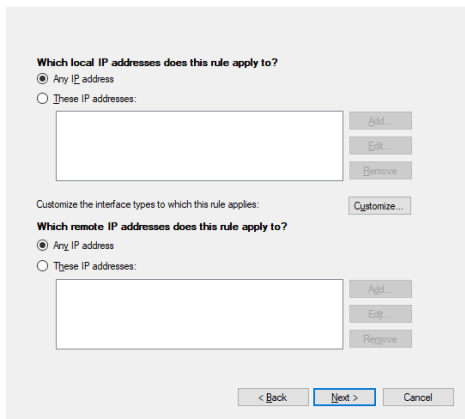
Remote port: All Ports

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings: Customize...

< Back Next > Cancel

3.



Which local IP addresses does this rule apply to?

☒ Any IP address

☐ These IP addresses:

Customize the interface types to which this rule applies: Customize...

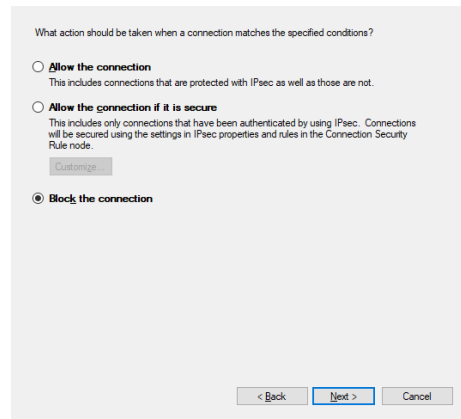
Which remote IP addresses does this rule apply to?

☒ Any IP address

☐ These IP addresses:

< Back Next > Cancel

4.



What action should be taken when a connection matches the specified conditions?

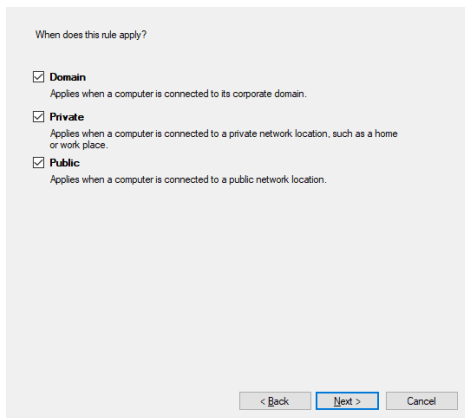
☐ Allow the connection
This includes connections that are protected with IPsec as well as those are not.

☐ Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

☒ Block the connection

< Back Next > Cancel

5.



When does this rule apply?

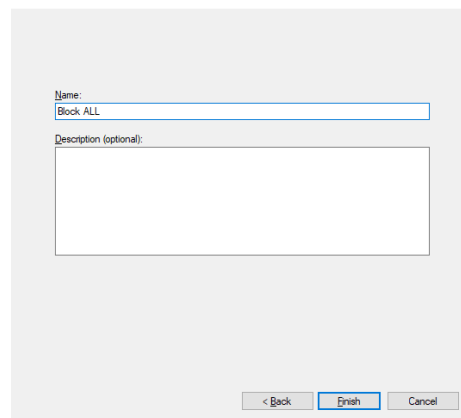
☒ **Domain**
Applies when a computer is connected to its corporate domain.

☒ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☒ **Public**
Applies when a computer is connected to a public network location.

< Back Next > Cancel

6.



Name: Block ALL

Description (optional):

< Back Finish Cancel

4. Connection Security Rules

This consists of advanced security rules creation and manipulations like:

- Isolation
 - Restrict connection based on authentication criteria such as domain membership or health status.
 - Authentication can be requested or required.
 - Authentication can be default as in IPsec settings or Kerberos V5 (Computer-User or Computer only) or Custom authentication.
- Authentication Exemption
 - Do not authenticate connection from specific computer.
 - Requires the IP address of that computer in the remote computers list.
- Server-to-Server authentication
 - Authenticate connection between specified computers.
 - Requires IP address of both end-points. (can be set to any)
 - Authentication can be default as in IPsec settings or Kerberos V5 (Computer-User or Computer only) or Custom authentication.
 - Computer certificate authentication can also be used as in digital signature servers.
- Tunnel
 - Authenticate connection between two computers
 - Requires tunnel type as an additional setting
 - Tunnel type can be Client-to-Gateway, vice-versa or custom
- Custom Rule

These connection rules are to manage group policies. We need to be a part of the group to manage and test these rules. We are required to create a Group Policy object to manage these settings.

Apart from these settings, we can manipulate the security of our system, using self-written bash scripts which can be executed at start up of the OS or the kernel.