

PRACTICAL: 10

AIM:

A mid-sized company plans to enhance network security by deploying a robust firewall solution. The IT security team is tasked with studying and testing various firewall software options to determine the most suitable one based on functionality, ease of use, and performance. To evaluate and compare different firewall software solutions for securing network traffic and preventing unauthorized access in a simulated enterprise environment.

THEORY:

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewalls are essential for protecting systems and networks from unauthorized access, malware, and other malicious activities. They can be implemented in both hardware and software and serve as a barrier between trusted internal networks and untrusted external networks, like the internet.

There are several types of firewalls, and the choice of which one to deploy depends on the organization's needs:

- **Packet-Filtering Firewalls:** These are the simplest form of firewalls. They inspect packets of data and determine whether to allow or block them based on IP addresses, port numbers, and protocols. However, they do not track the state of connections, making them less secure.
- **Stateful Inspection Firewalls:** These are more advanced than packet-filtering firewalls, as they track the state of active connections and only allow packets that match an established connection's state. They are more secure and provide more comprehensive monitoring of traffic.
- **Proxy Firewalls:** Proxy firewalls act as intermediaries between the internal network and the external network. They can provide enhanced security by hiding the internal network's details, but they may introduce latency because they must forward requests from the internal network to external destinations and vice versa.
- **Next-Generation Firewalls (NGFW):** NGFWs combine the features of traditional firewalls with additional layers of security, such as intrusion prevention, application awareness, and advanced threat protection. They are capable of detecting more sophisticated attacks, such as zero-day exploits, and they often include VPN support.

Key Functions of Windows Defender Firewall

1. **Traffic Filtering:**
 - Windows Defender Firewall filters traffic based on rules you set. It decides which network traffic can pass through (allow) and which should be blocked (deny).
 - It manages both **inbound traffic** (data coming into your system) and **outbound traffic** (data leaving your system).
2. **Security:**
 - It is primarily designed to prevent unauthorized access to your computer from external sources, such as hackers or malicious software attempting to exploit your computer.

- It blocks connections to untrusted devices or websites and ensures only authorized apps, services, or users can communicate with your computer.
3. **Application Control:**
- The firewall works in conjunction with specific applications on your system. It can block or allow access to individual programs, ensuring that only approved applications can connect to the network.

Components of Windows Defender Firewall

1. **Inbound Rules:**
 - Inbound rules control incoming traffic (from the internet or local network) trying to access services, programs, or resources on your computer.
 - For example, if someone tries to access a web server running on your machine, inbound rules decide whether that traffic should be allowed or blocked.
2. **Outbound Rules:**
 - Outbound rules control traffic leaving your computer. These rules govern which applications or services on your system are allowed to send data to external networks.
 - For example, you can configure outbound rules to block specific apps (such as a torrent client or browser) from accessing the internet.
3. **Connection Security Rules:**
 - These rules are used to establish and maintain secure connections. They manage **IPsec (Internet Protocol Security)**, a set of protocols that encrypt and authenticate data packets.
 - IPsec is used to secure communication between devices by ensuring that only authorized devices can communicate with each other.
4. **Profiles:**
 - Windows Defender Firewall uses **profiles** to manage how the firewall behaves depending on the type of network your computer is connected to. The three types of network profiles are:
 - **Domain Profile:** Applied when your computer is connected to a corporate network that is part of a domain.
 - **Private Profile:** Applied when your computer is connected to a private, trusted network, like a home Wi-Fi network.
 - **Public Profile:** Applied when your computer is connected to a public network, such as a café or airport Wi-Fi. The strictest rules are typically applied in public networks.
5. **Logging:**
 - Windows Defender Firewall can log events to help administrators track traffic and identify potential issues or threats. This can include failed attempts to connect, blocked traffic, or system events.
 - Logs are stored in the **Event Viewer** and can be analyzed to identify patterns of suspicious activity.

How Windows Defender Firewall Works

1. **Filtering Based on Rules:**
 - When a packet of data is sent to or from your system, the firewall evaluates it against the existing rules. These rules specify whether certain types of traffic should be allowed or denied.

- **Rules can be customized** by the user or administrator. For example, you could allow incoming traffic for a web server on port 80 (HTTP) or block outgoing connections for a specific application.
- 2. **Profile-Based Filtering:**
 - Depending on the network your computer is connected to, the firewall switches between different profiles, adjusting security levels based on the environment.
 - **Domain Profile** has more relaxed rules compared to **Public Profile**, as the latter is typically used in public places where more stringent security is required.
- 3. **Default Behavior:**
 - By default, Windows Defender Firewall **blocks all inbound traffic** that is not explicitly allowed by a rule.
 - For outbound traffic, it is typically allowed unless specified otherwise in the firewall rules.
- 4. **Allowing and Blocking Applications:**
 - Applications and services on your computer can request permission from the firewall to access the network. You can choose whether to allow or block specific applications, such as web browsers, email clients, or even background services.
- 5. **Stateful Packet Inspection (SPI):**
 - Windows Defender Firewall performs Stateful Packet Inspection, which means it tracks the state of network connections. It looks at the entire context of the traffic, not just individual packets.
 - For instance, if you initiate a connection to a server, the firewall will "remember" that connection and allow the response from the server to reach you, but it will block any unsolicited responses.

Types of Rules in Windows Defender Firewall

1. **Inbound Rules:**
 - Govern the traffic coming into your system. For example, you can set up inbound rules for allowing access to services such as **HTTP**, **FTP**, or **RDP** (Remote Desktop Protocol).
 - Common scenarios for inbound rules:
 - Allowing a web server (port 80/443) to receive incoming web traffic.
 - Blocking all incoming traffic on an unused port to reduce the attack surface.
2. **Outbound Rules:**
 - Control which applications or processes can send data out of your computer to external networks.
 - Common scenarios for outbound rules:
 - Allowing your browser to access the internet but blocking other apps (like a game) from accessing it.
 - Preventing malware or unauthorized applications from making outbound connections.
3. **Connection Security Rules:**
 - These are used to configure security measures like **IPsec**, which secures traffic between devices on a network.
 - Connection security rules are typically used in corporate or enterprise environments to ensure secure communications.

Creating and Managing Firewall Rules

1. **Create a Rule:**
 - Open **Windows Defender Firewall with Advanced Security** (can be accessed by searching for it in the Start menu).
 - Choose either **Inbound Rules** or **Outbound Rules** on the left sidebar, then select **New Rule**.
 - You can create rules based on:
 - **Program:** Allow or block specific applications.
 - **Port:** Allow/block specific ports.
 - **Predefined:** Choose predefined rules for specific services (e.g., **File and Printer Sharing**).
 - **Custom:** Create highly specific rules based on multiple criteria (program, port, IP address).
2. **Configuring a Rule:**
 - After selecting the rule type, you'll specify what action to take (allow or block).
 - You can also specify the conditions for when the rule should apply (e.g., only on a private network, only for specific IP addresses, etc.).
3. **Managing Rules:**
 - You can enable, disable, or delete rules by selecting them in the list of inbound or outbound rules.
 - You can also prioritize the rules based on their importance.

Best Practices for Windows Defender Firewall

1. **Use Default Settings Where Possible:**
 - For most users, the default firewall settings provide a good level of protection. Don't disable the firewall unless absolutely necessary.
2. **Enable Logging:**
 - Enable logging to help you track unusual network activity and identify potential threats.
3. **Review and Update Firewall Rules Regularly:**
 - Periodically review the rules to ensure they're up to date and that no unnecessary open ports or services exist.
 - Remove any unused or redundant rules to minimize potential vulnerabilities.
4. **Use Profiles Based on Your Network:**
 - Configure the firewall profiles properly based on your network type (home, work, public). Use stricter rules on public networks to reduce exposure to threats.

Some of the top firewall include:

1. **pfSense (Open-source):**
 - Advantages: Highly customizable and flexible, ideal for tech-savvy organizations.
 - Features: Stateful firewall, VPN support, and advanced logging capabilities.
 - Ideal For: Companies with an in-house IT team that can manage and configure it.
2. **FortiGate (Commercial, Next-Generation Firewall):**
 - Advantages: Strong performance, high availability, and advanced security features like IDS/IPS and DDoS protection.
 - Features: NGFW with centralized management, high throughput, and scalability.

- Ideal For: Medium to large enterprises looking for an all-in-one security solution.

3. Check Point Quantum Firewall:

- Advantages: Strong integration with cloud environments, centralized management, and ease of use.
- Features: VPN support, threat prevention, and application control.
- Ideal For: Enterprises needing a combination of strong network security and simplified management.

4. Palo Alto Networks PA-Series:

- Advantages: Highly detailed traffic analysis and real-time protection.
- Features: Advanced threat protection, application visibility, and user identification.
- Ideal For: Organizations with high-performance needs and complex network environments.

5. Cisco ASA:

- Advantages: Proven track record in enterprise environments with strong support and extensive documentation.
- Features: VPN, content filtering, and support for a variety of security protocols.
- Ideal For: Enterprises already using Cisco infrastructure.

ESET's personal firewall, integrated within ESET Internet Security and ESET Smart Security Premium, offers advanced features beyond those of the built-in Windows Defender Firewall. While Windows Defender Firewall provides essential inbound and outbound traffic filtering based on user-defined rules, ESET's firewall enhances this with interactive user prompts for outbound connections, allowing for more granular control over application network access.

Additionally, ESET's firewall includes Intrusion Detection System (IDS) capabilities, which monitor network traffic for suspicious activities and potential threats—a feature not natively available in Windows desktop versions. It's important to note that running two firewalls simultaneously can lead to conflicts; therefore, upon installation, ESET's firewall automatically disables Windows Defender Firewall to prevent such issues.

CODE:

N/A

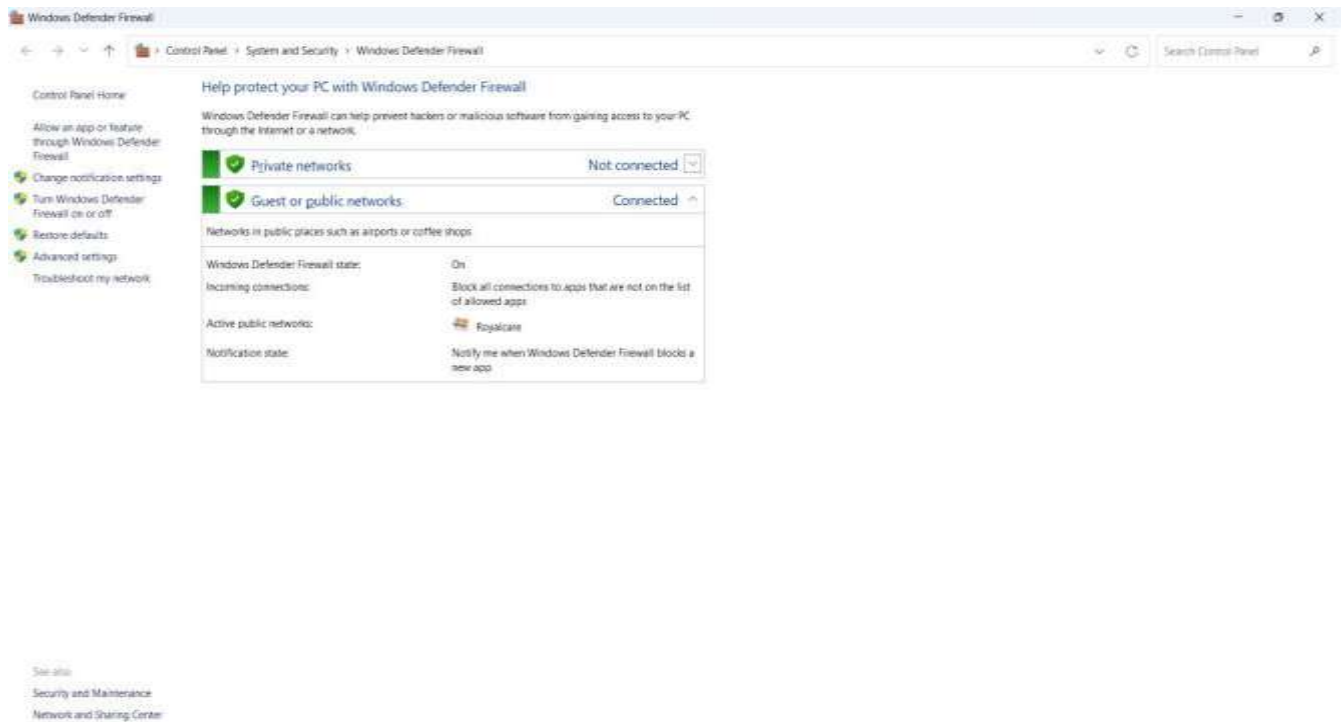
OUTPUT:

Figure 1: Windows Defender Firewall main control panel

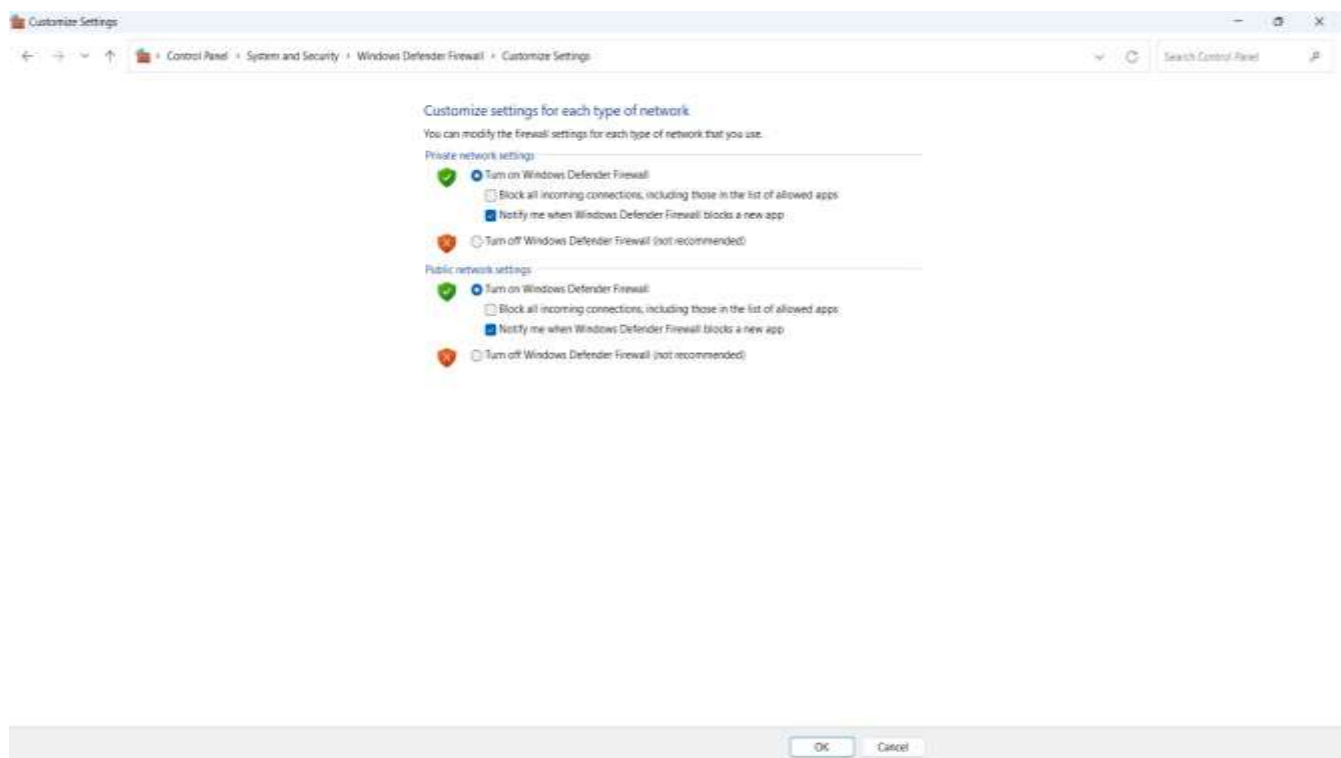


Figure 2: Enable or disable Windows Defender Firewall for different network profiles.

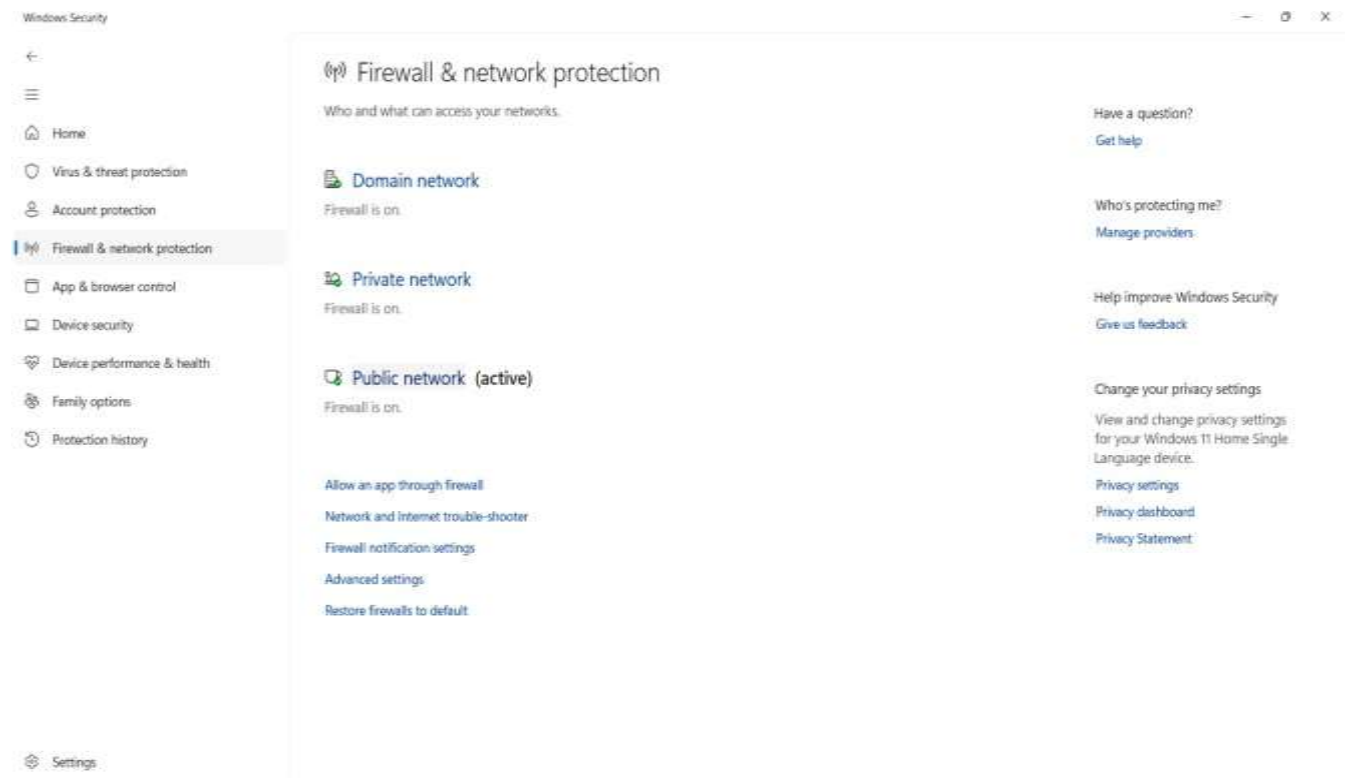


Figure 3: Display of active firewall status

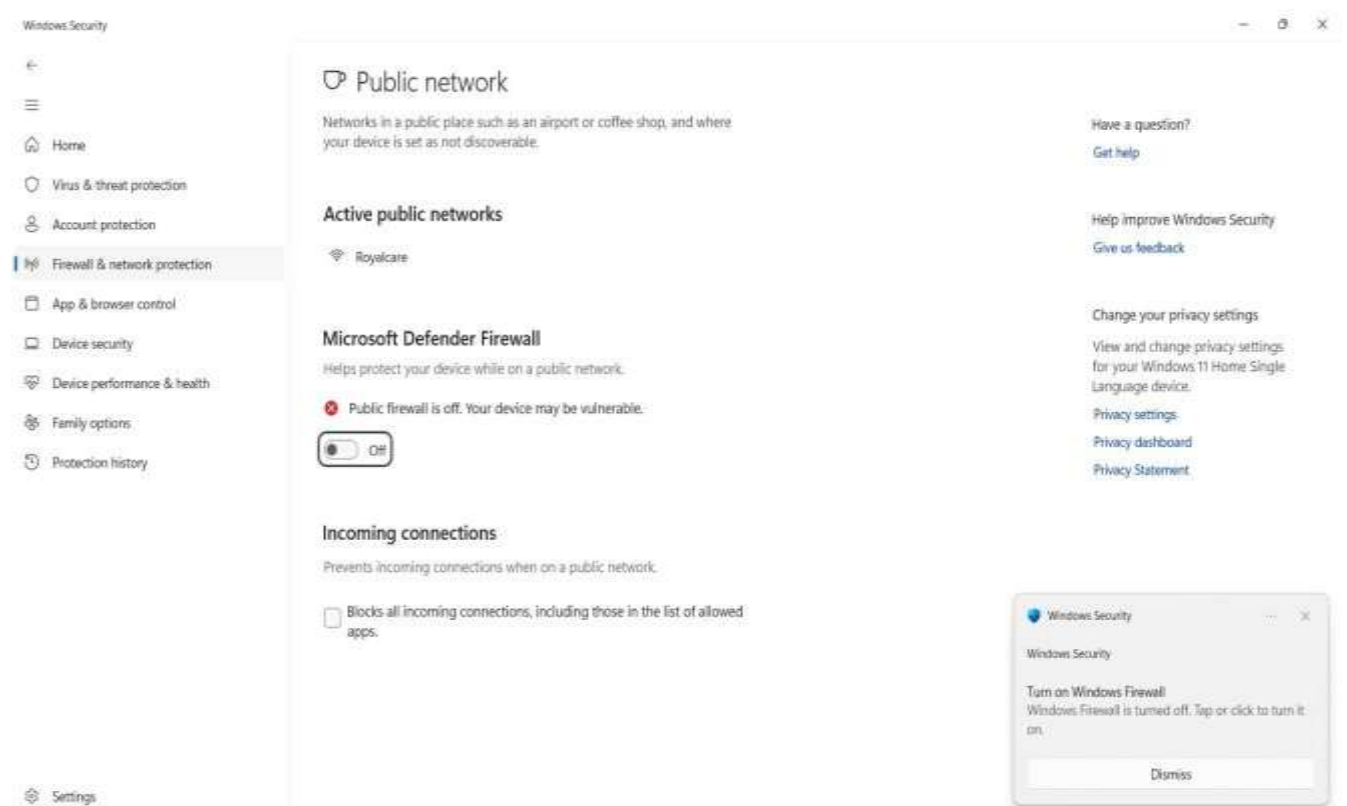


Figure 4: Warning prompt when the firewall is turned off

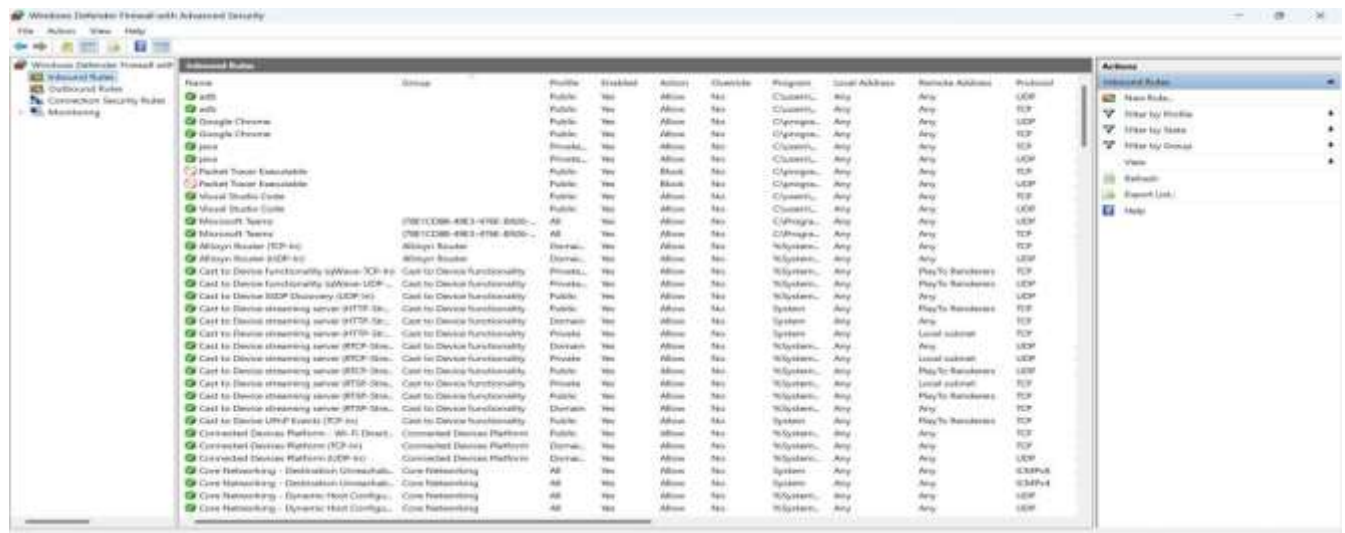


Figure 5: Inbound rule configuration for managing incoming traffic

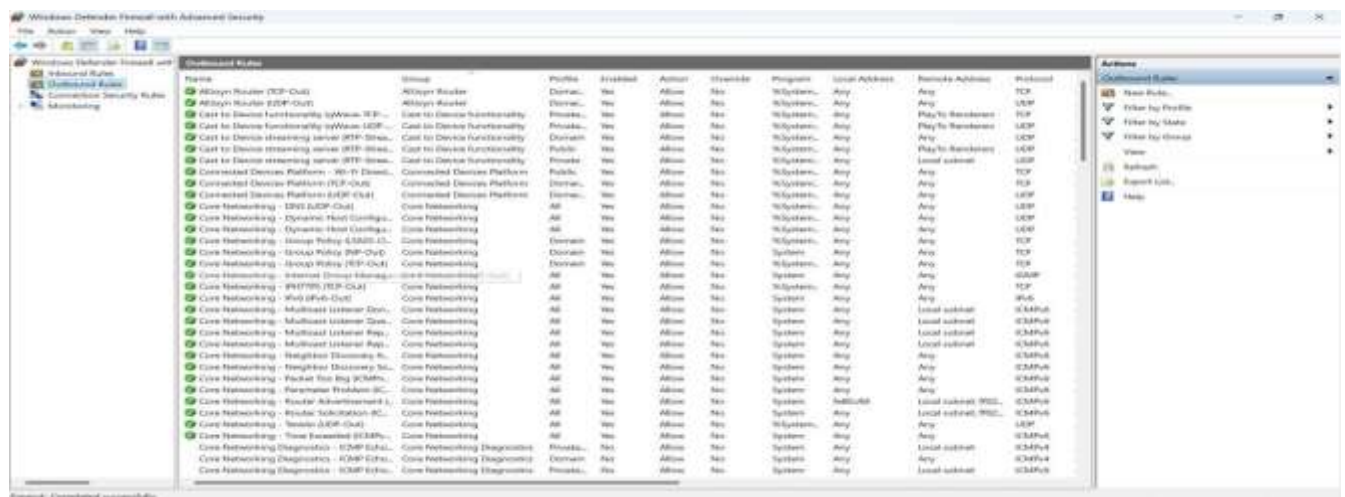


Figure 6: Outbound rule configuration for controlling outgoing traffic

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](#)

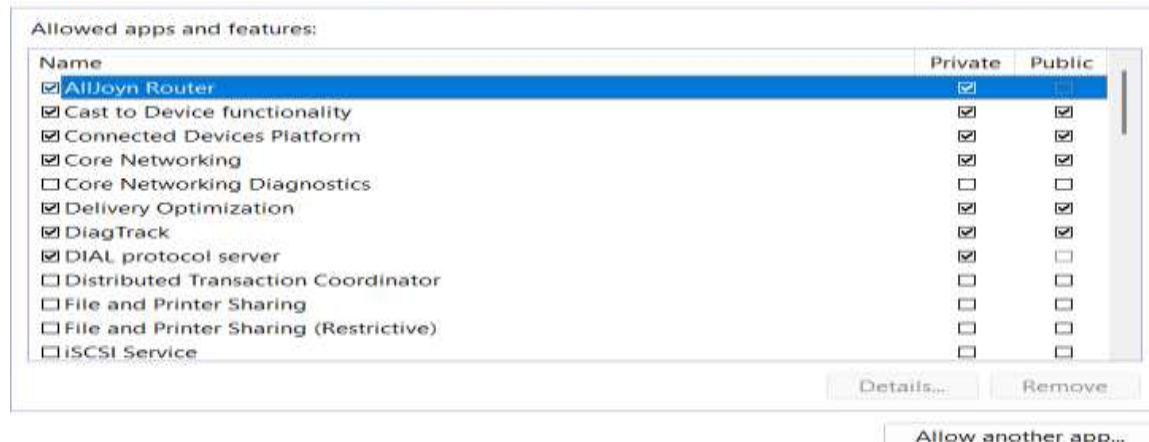


Figure 7: Selecting which applications can communicate through the firewall

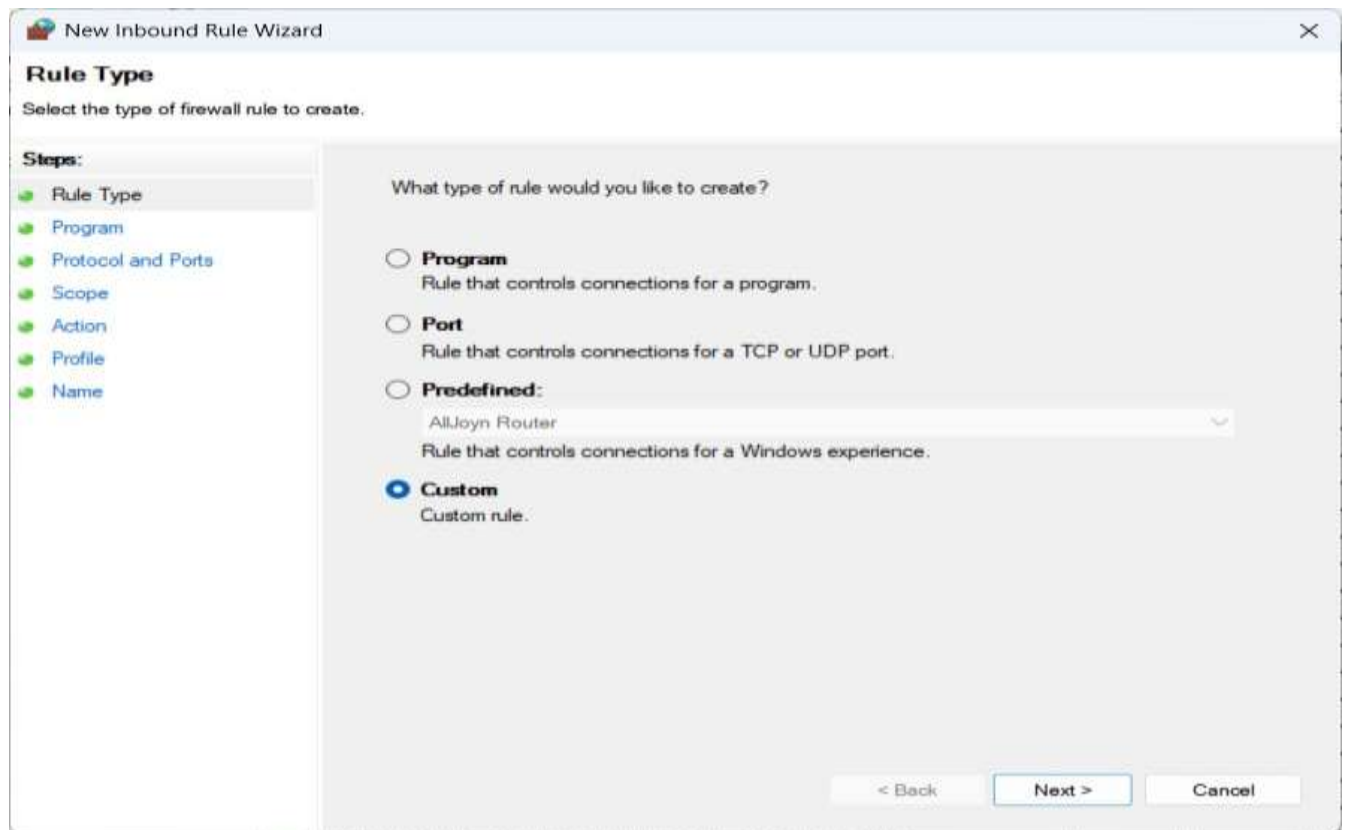


Figure 8: Creating a custom inbound rule with tailored settings

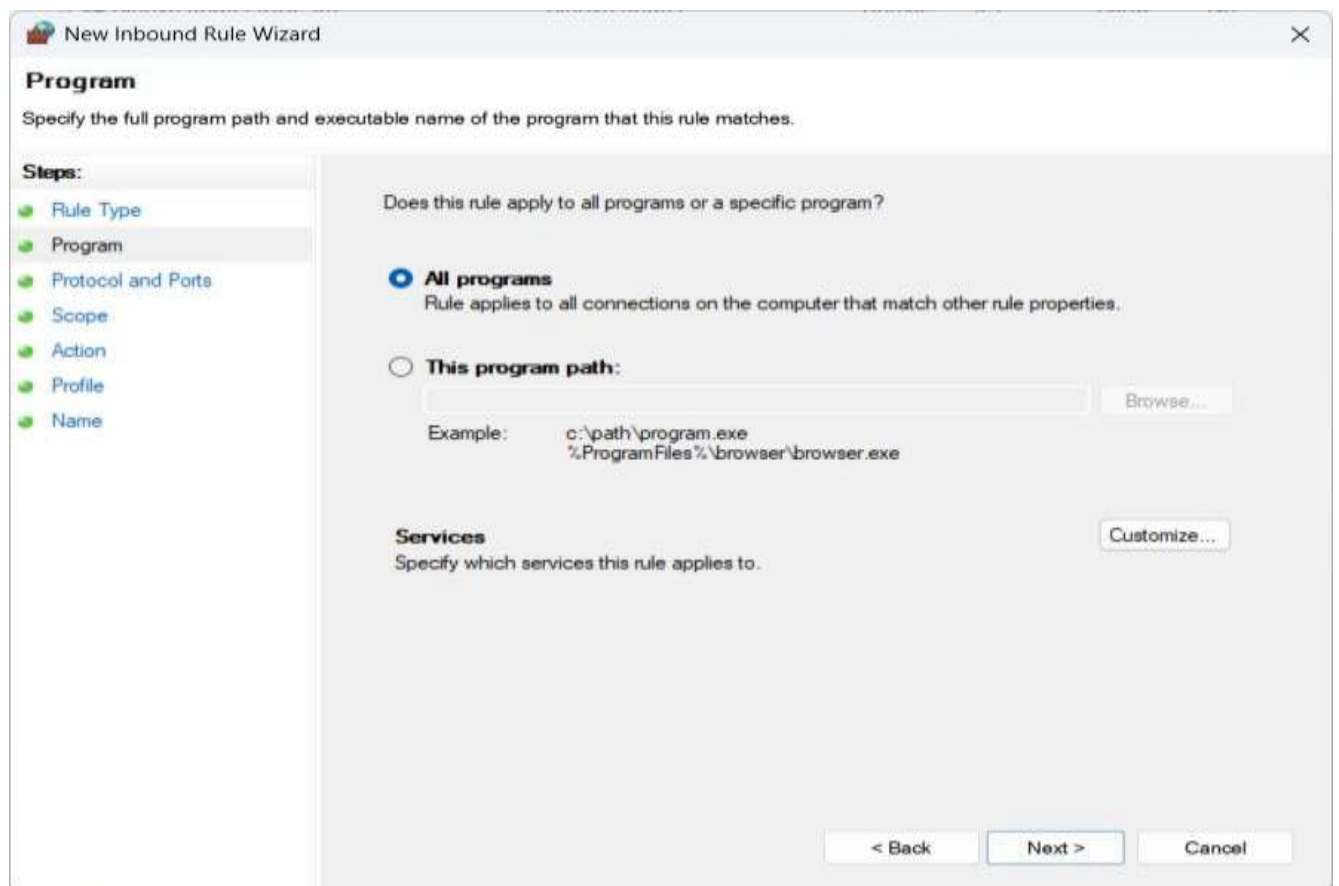
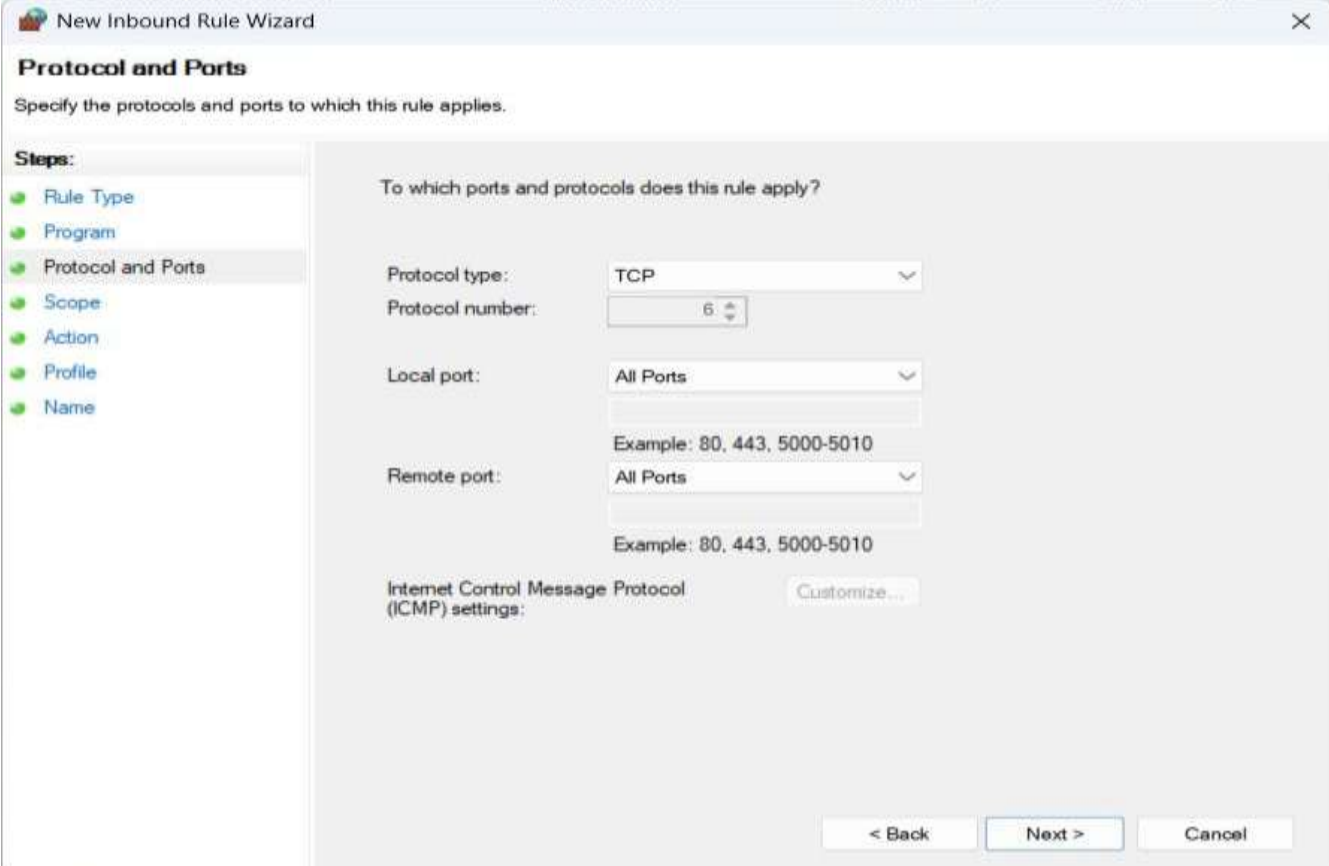


Figure 9: Define rule criteria for specific programs or all programs



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports**
- Scope
- Action
- Profile
- Name

To which ports and protocols does this rule apply?

Protocol type: TCP

Protocol number: 6

Local port: All Ports

Example: 80, 443, 5000-5010

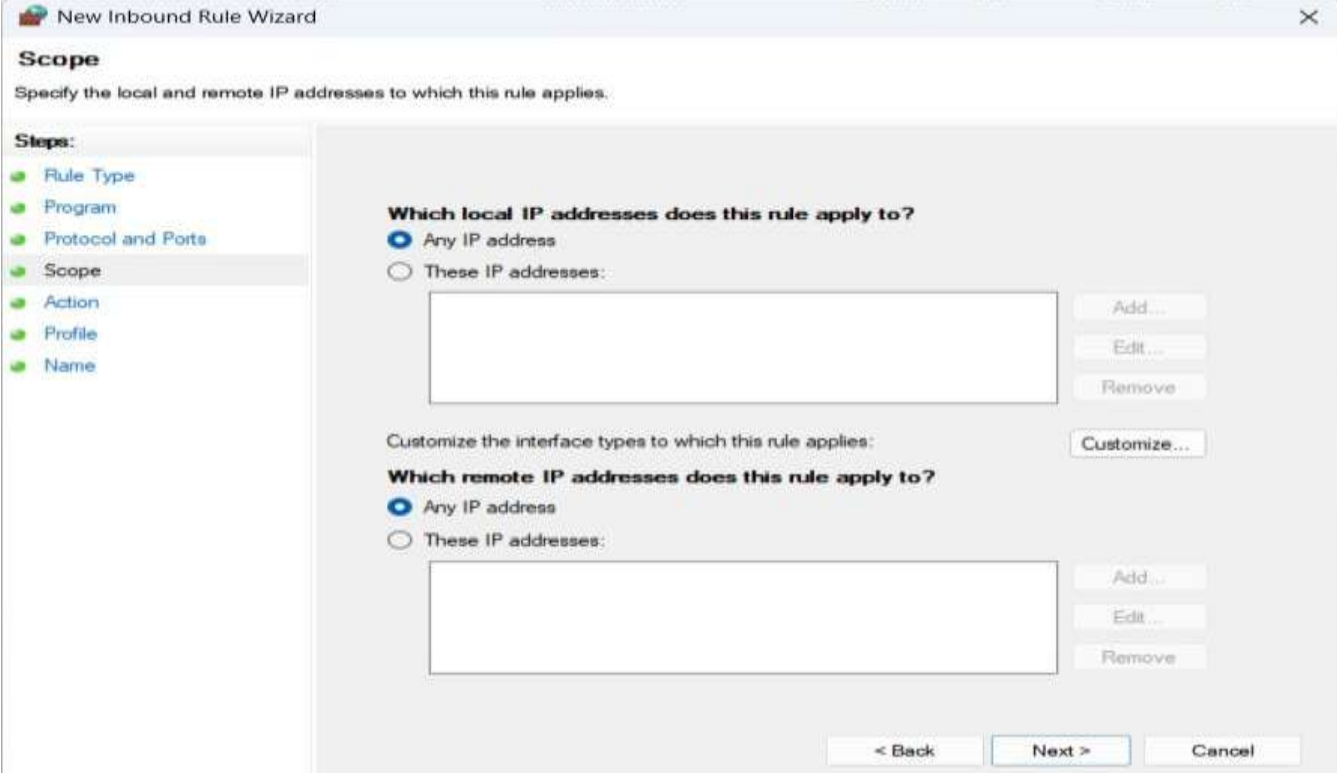
Remote port: All Ports

Example: 80, 443, 5000-5010

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

< Back Next > Cancel

Figure 10: Set protocols and ports for firewall rules



New Inbound Rule Wizard

Scope

Specify the local and remote IP addresses to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope**
- Action
- Profile
- Name

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

Figure 11: Define IP addresses to target specific connections

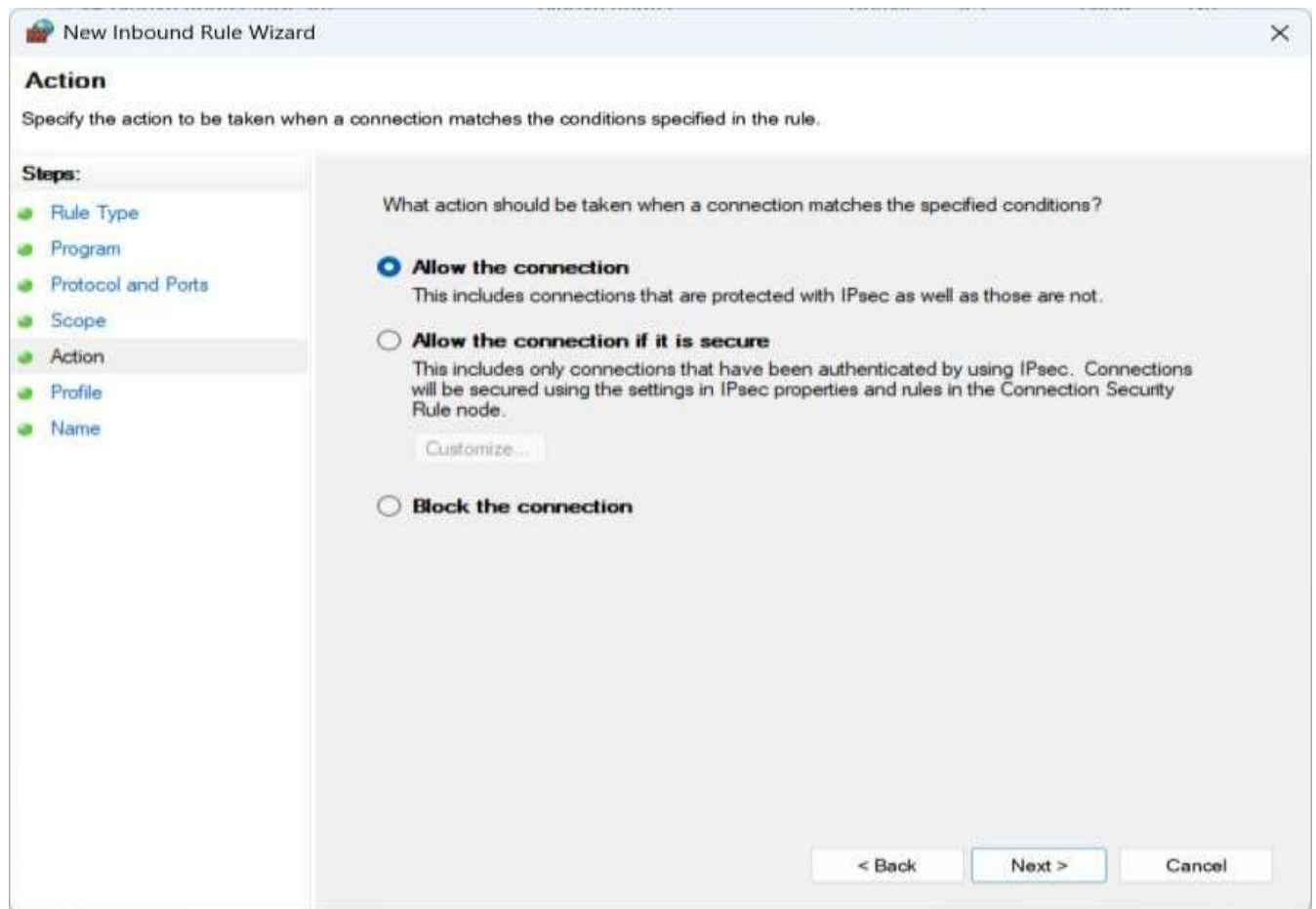


Figure 12: Configure actions — allow or block connections

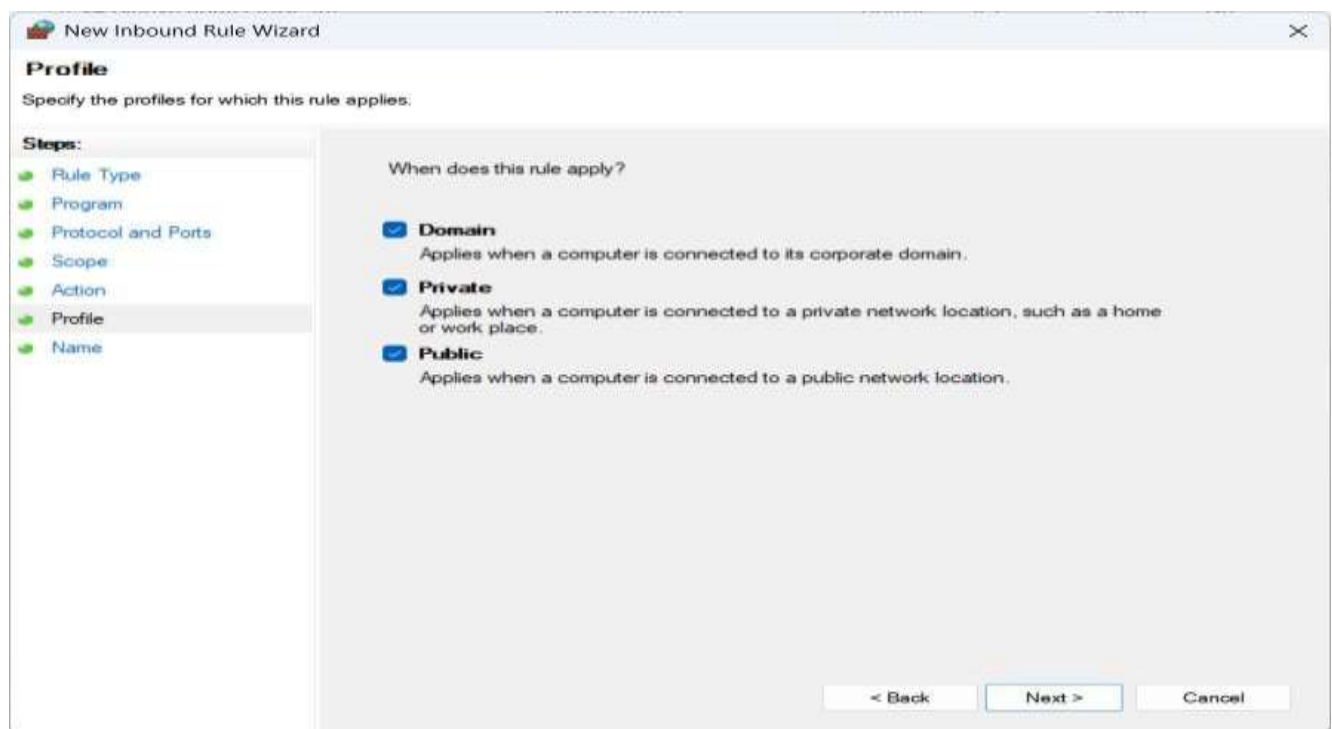


Figure 13: Apply rules to specific network profiles

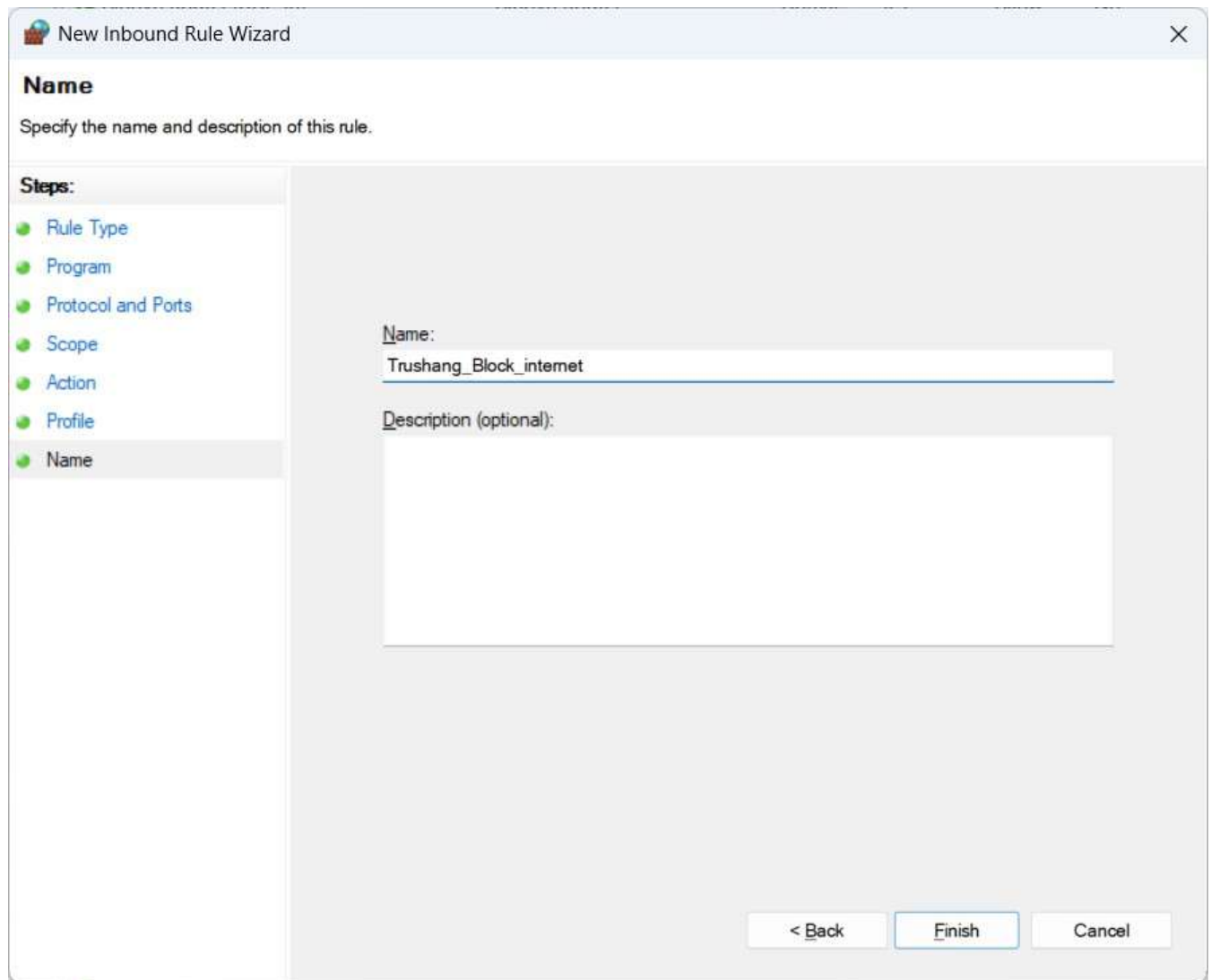


Figure 14: Naming the firewall rule for better management

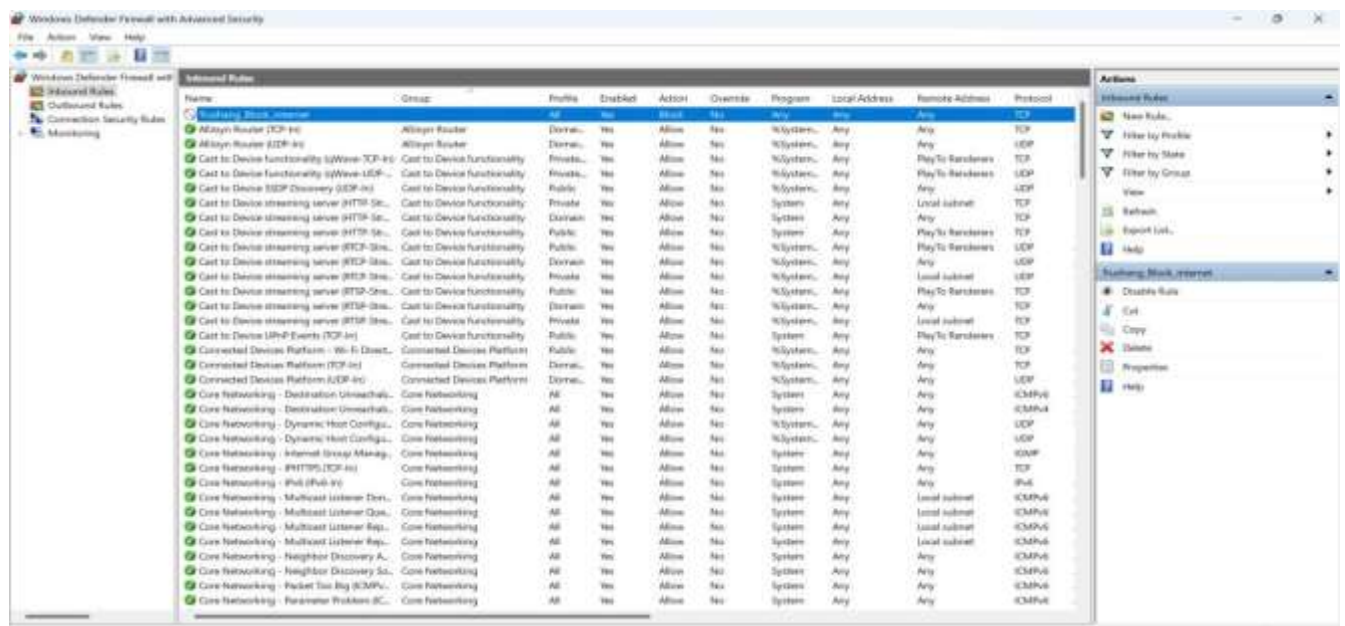


Figure 15: Example of creating an inbound rule to block internet access

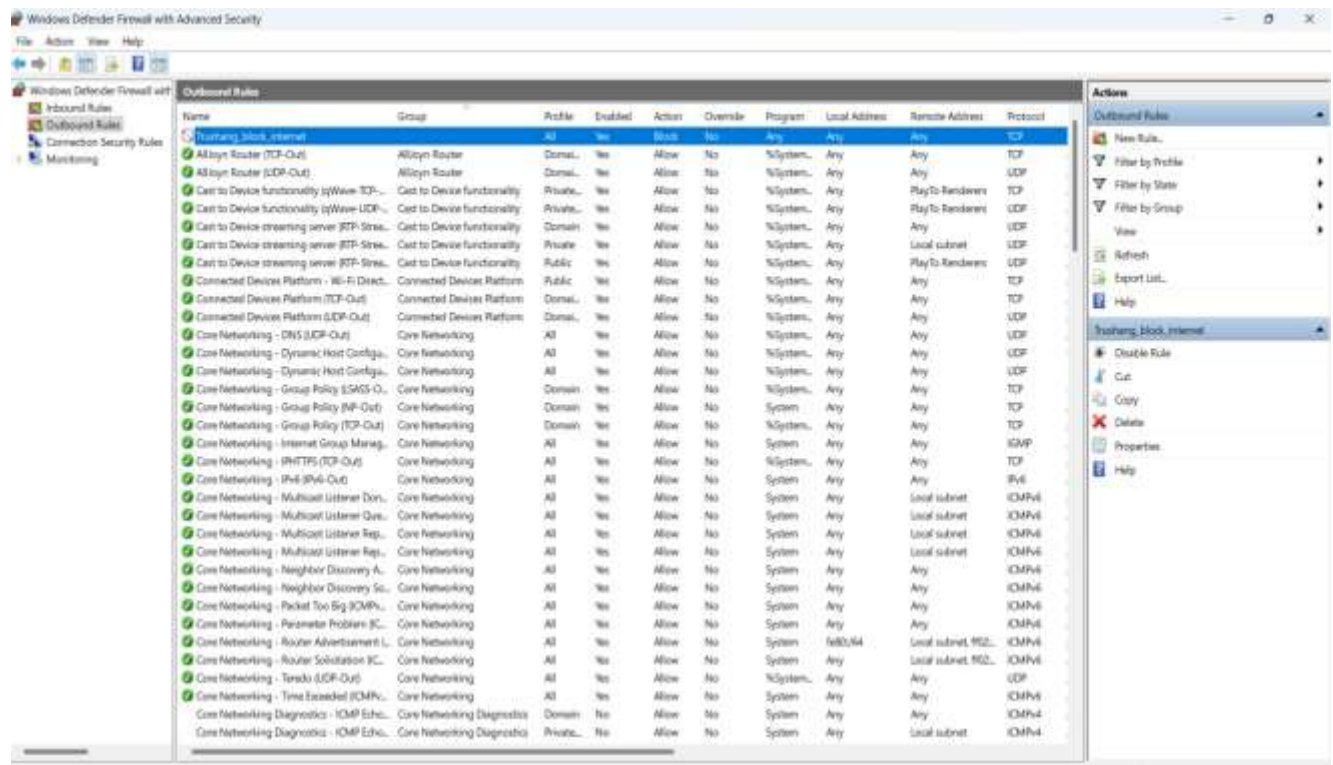


Figure 16: Example of creating an outbound rule to block internet access

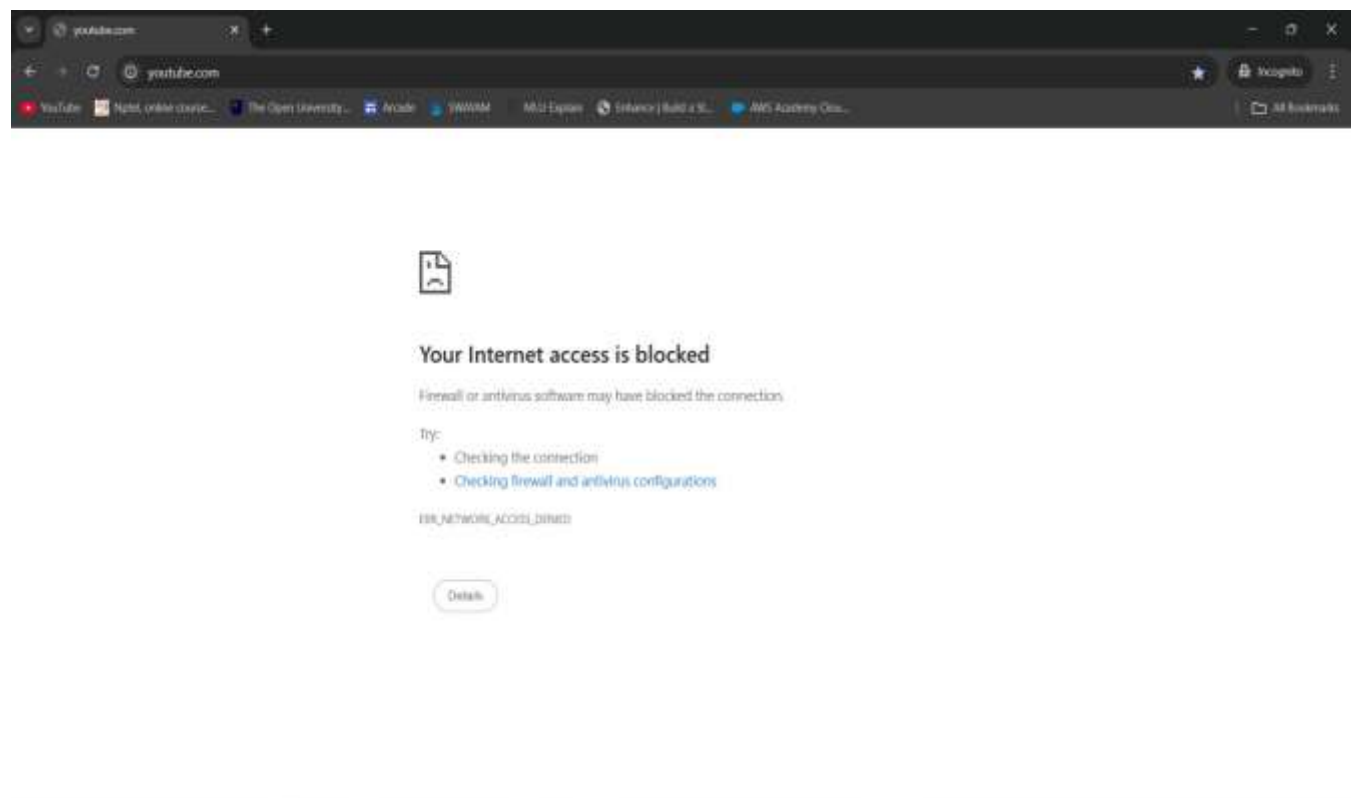


Figure 17: Verification — internet access is successfully blocked

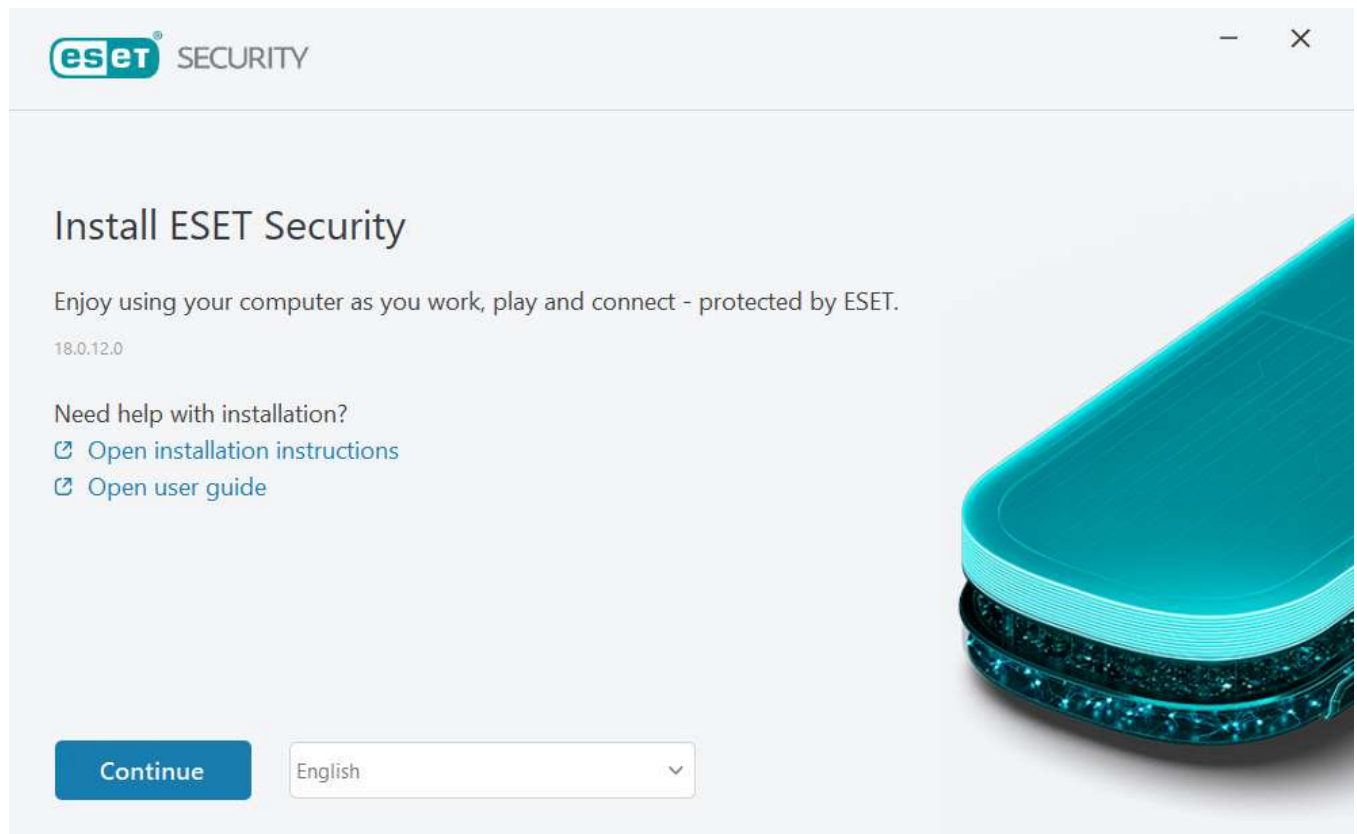


Figure 18: Installing ESET Personal Firewall trial version

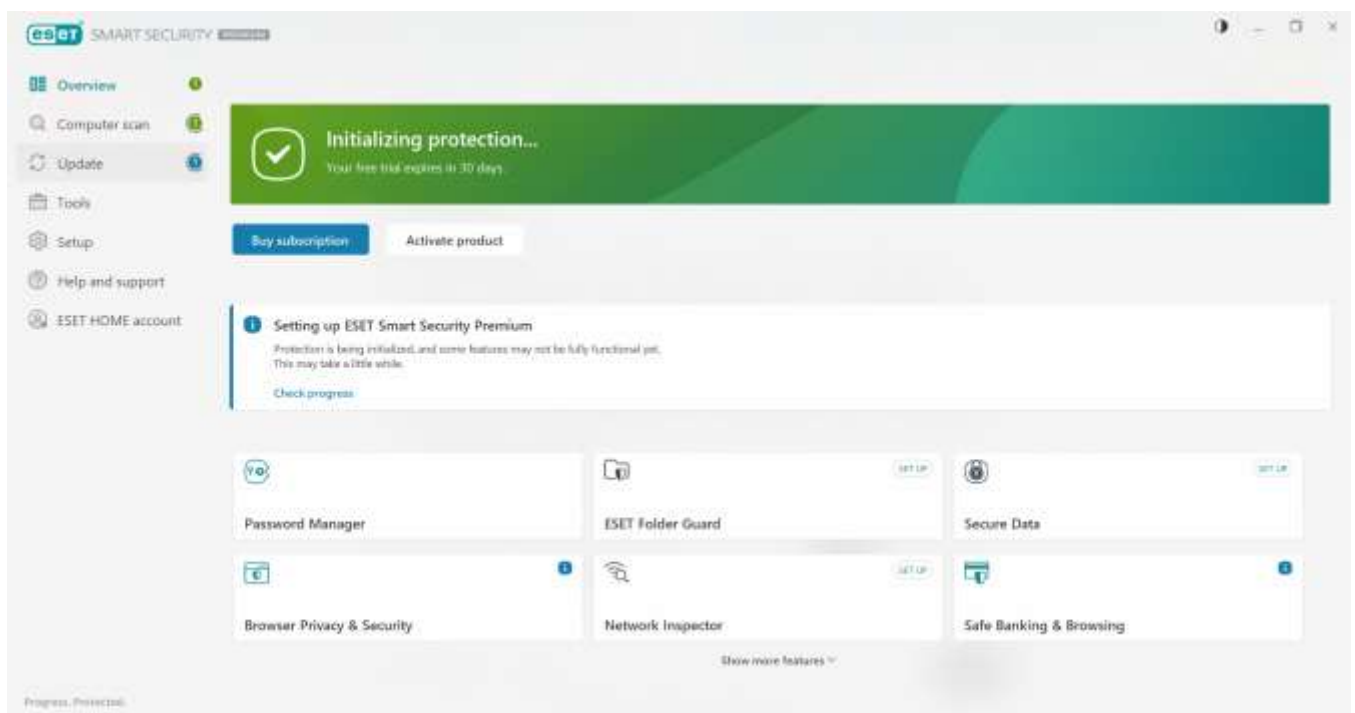


Figure 19: ESET security dashboard overview

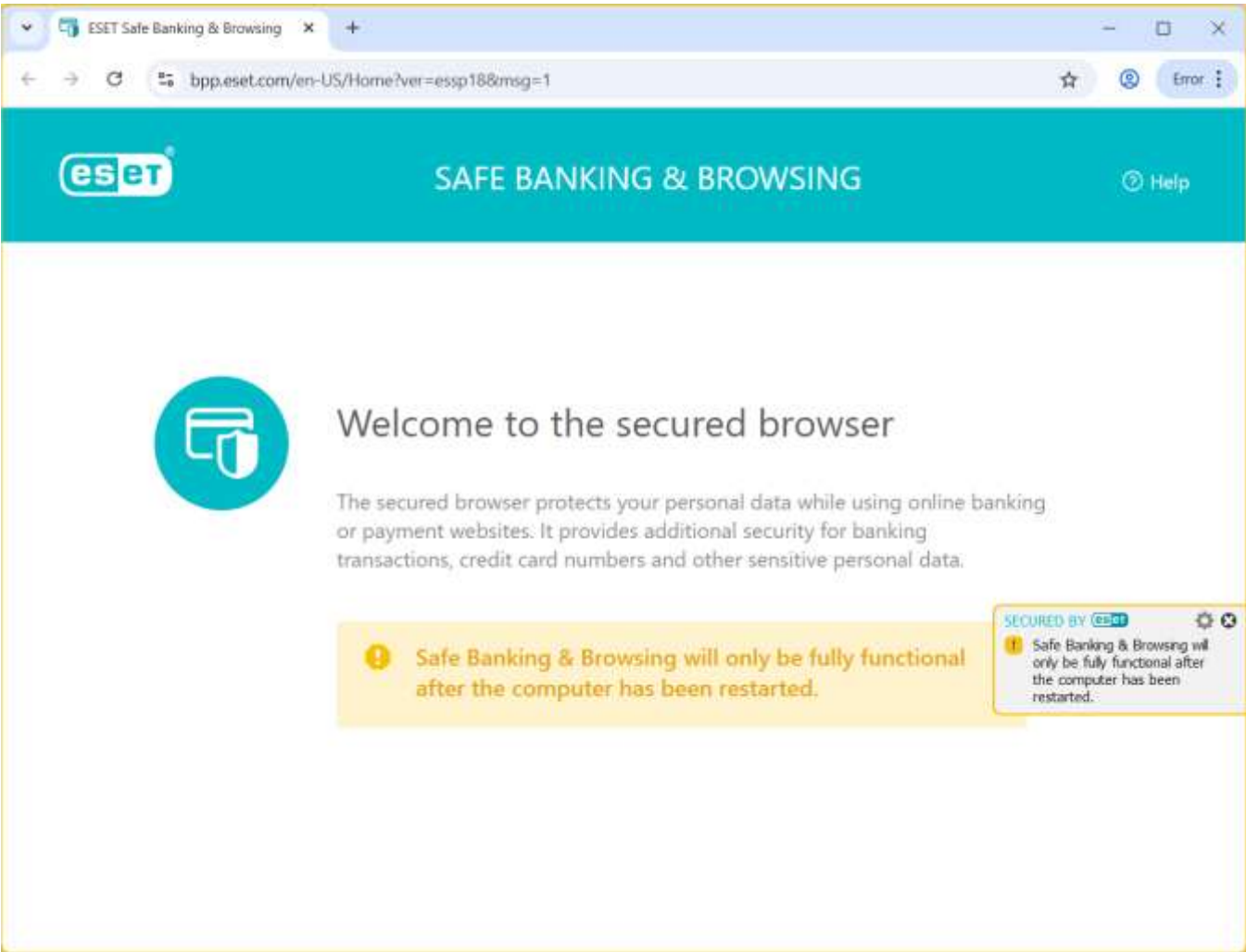


Figure 20: ESET's secure browser for safe banking transactions

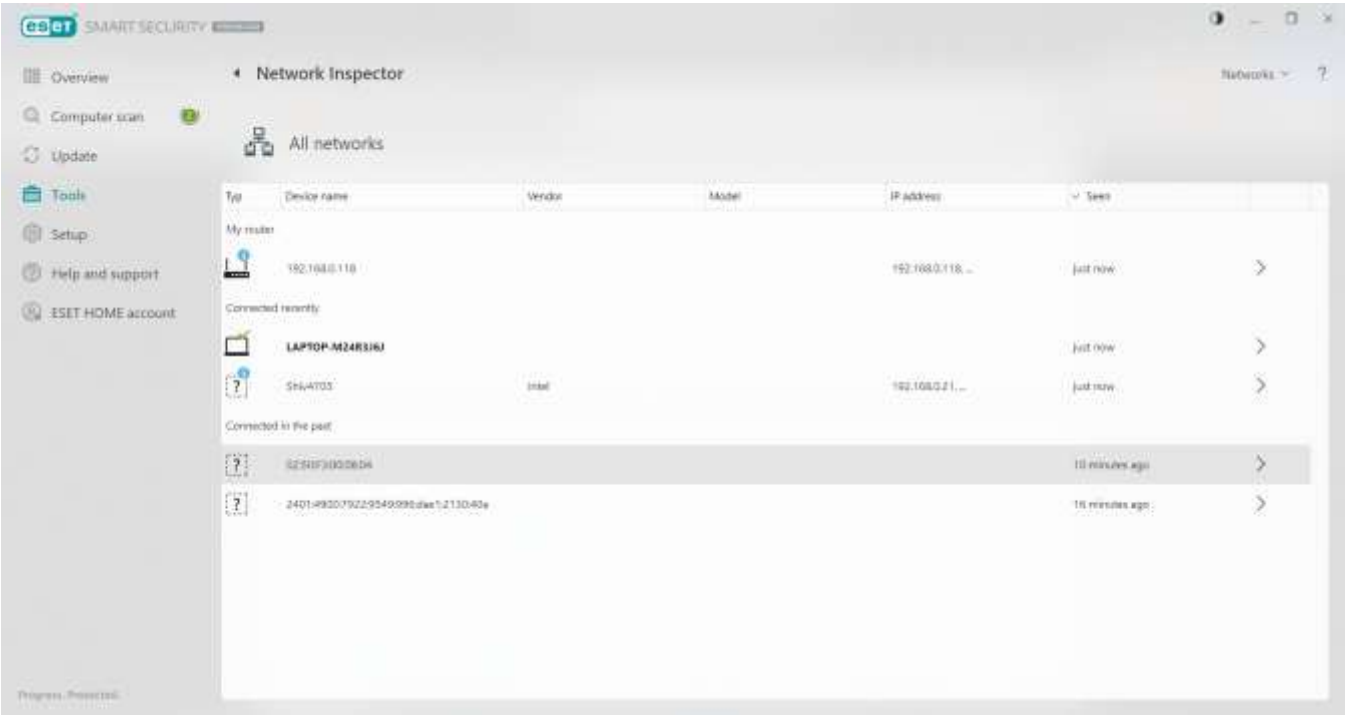


Figure 21: ESET Network Inspector showing connected devices

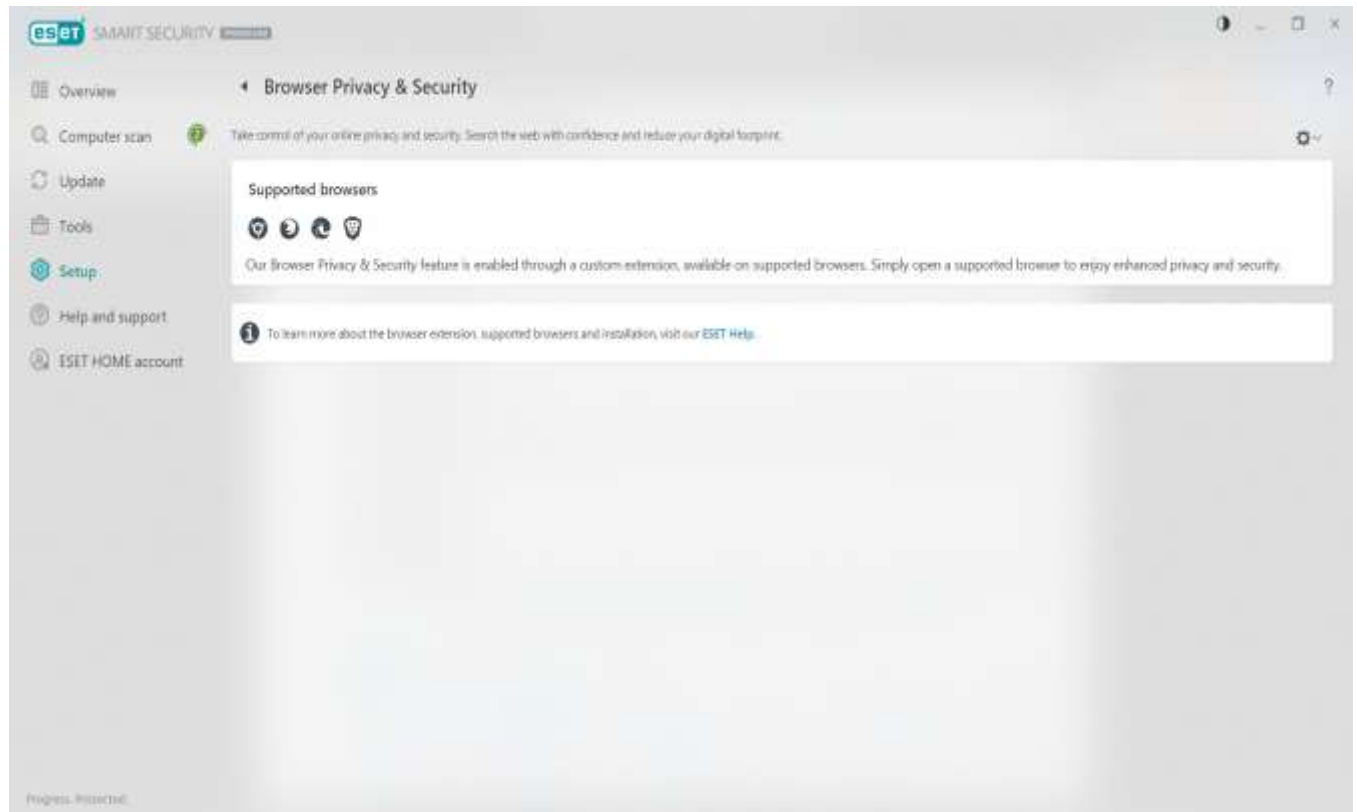


Figure 22: ESET browser security feature in action

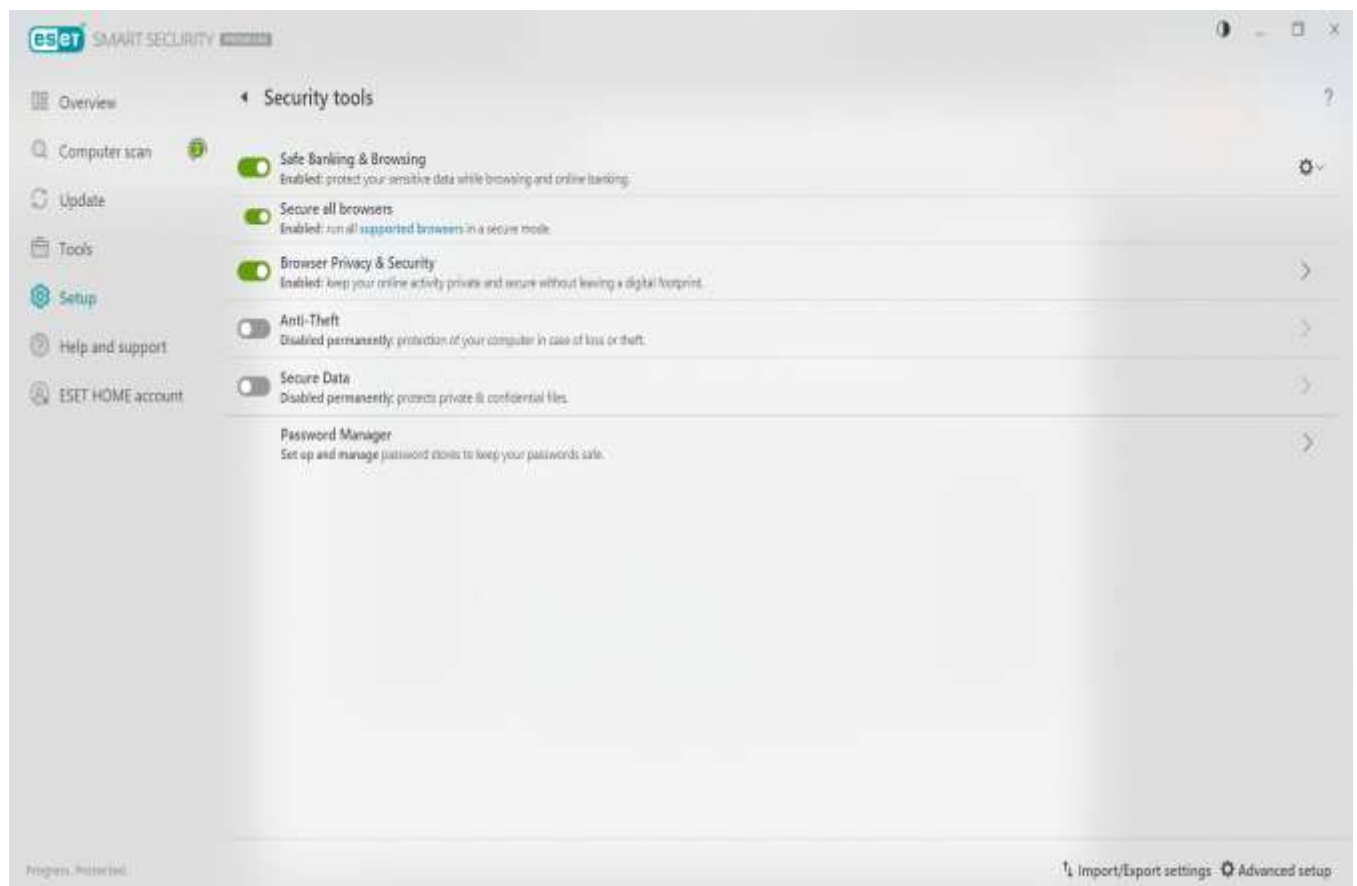


Figure 23: Overview of ESET's security tools

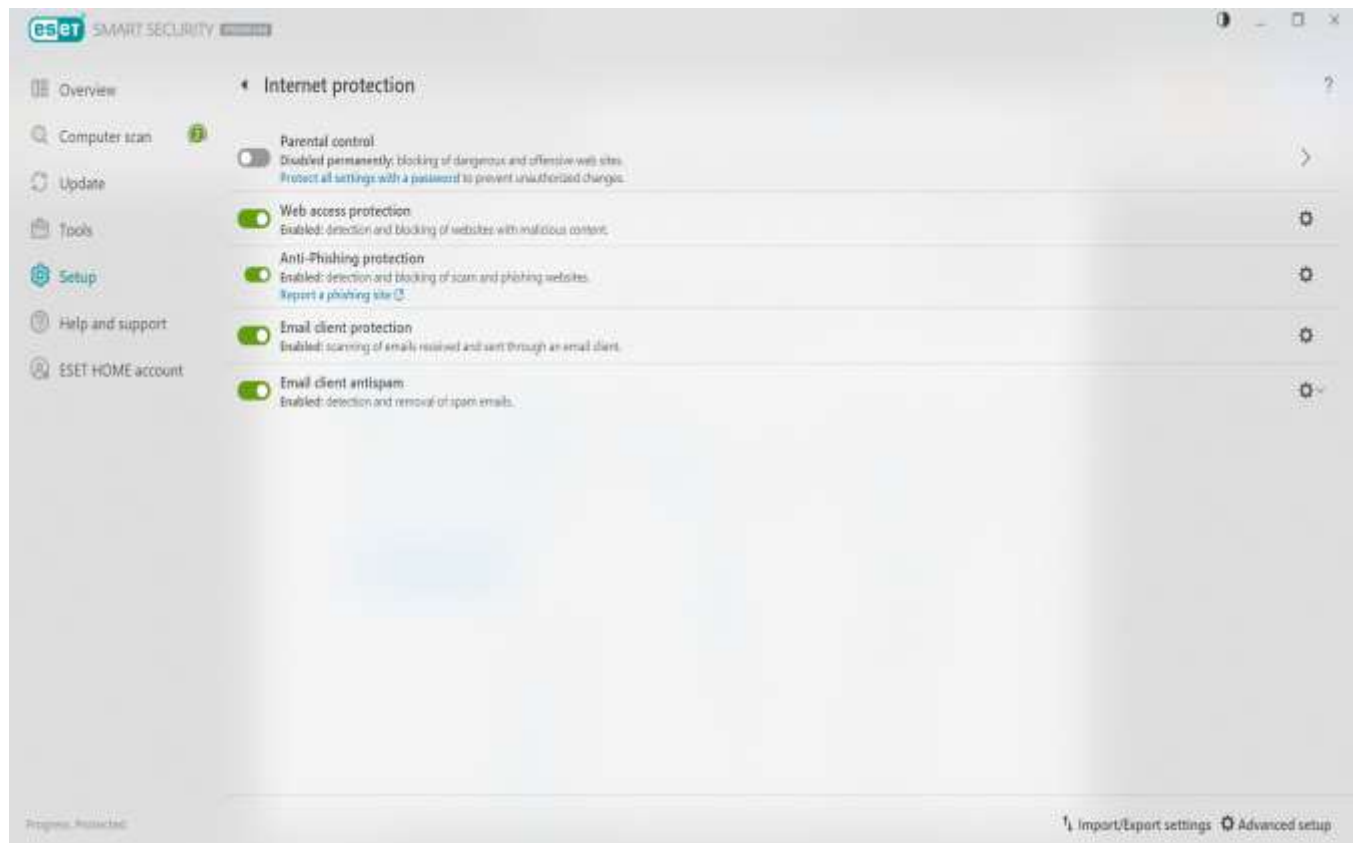


Figure 24: Internet protection settings in ESET

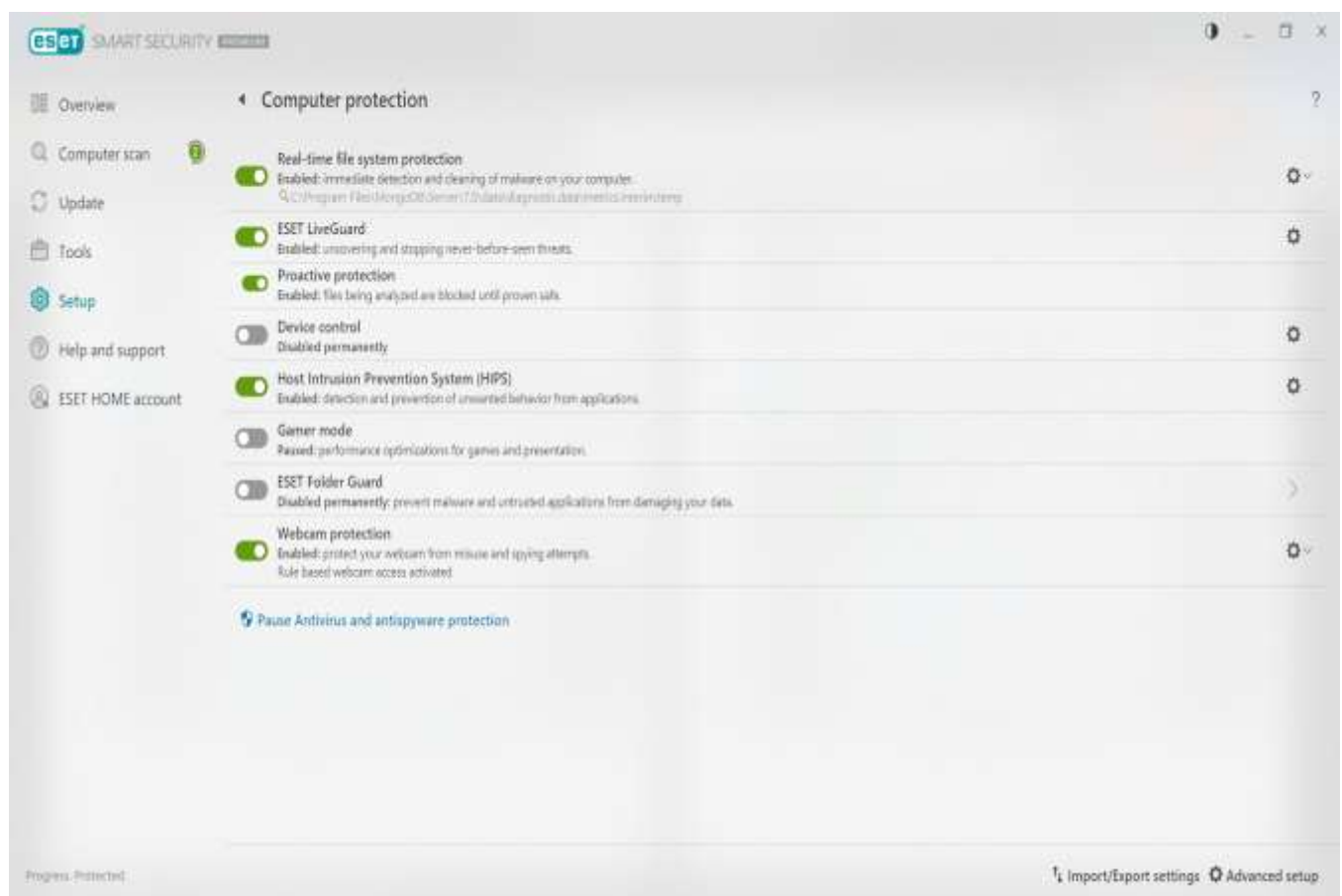


Figure 25: Computer protection settings in ESET

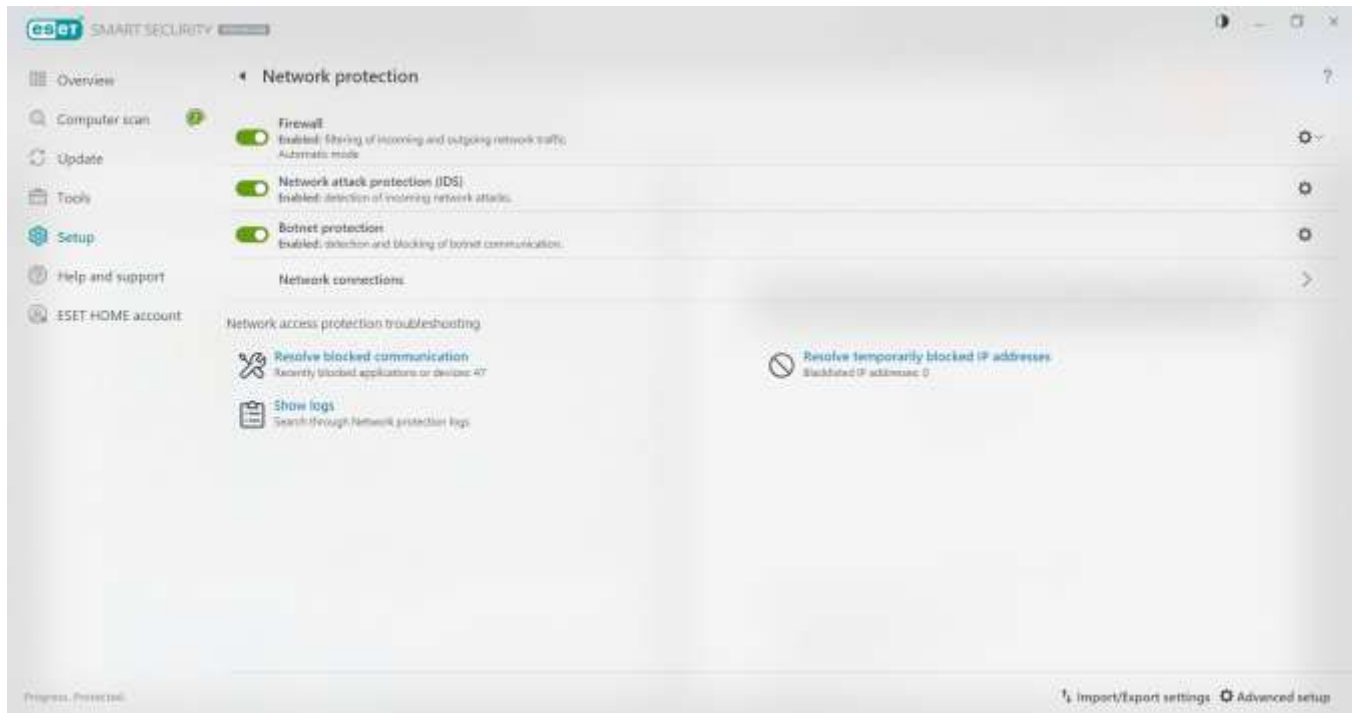


Figure 26: Network protection settings in ESET

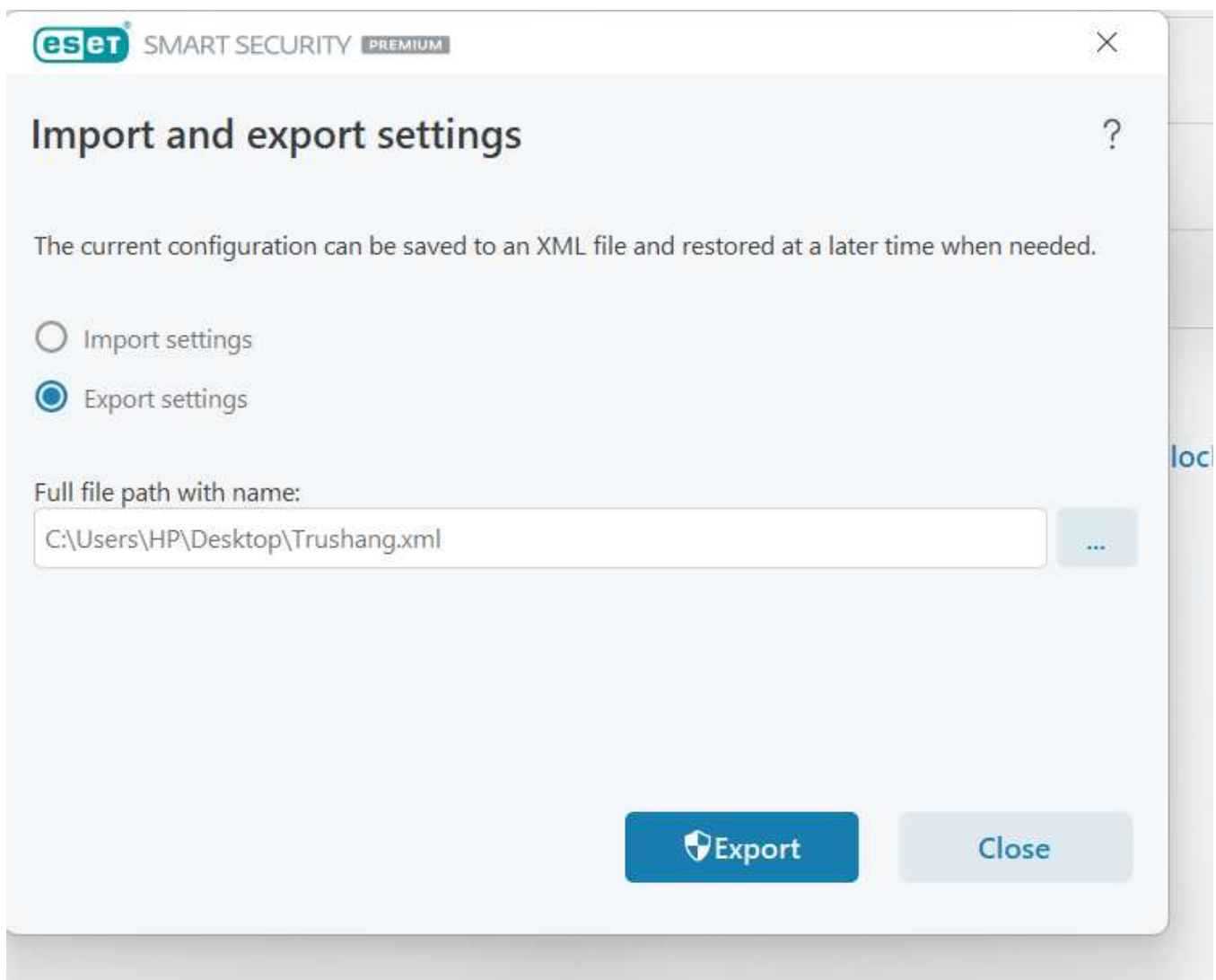


Figure 27: Import/export feature for ESET configuration settings



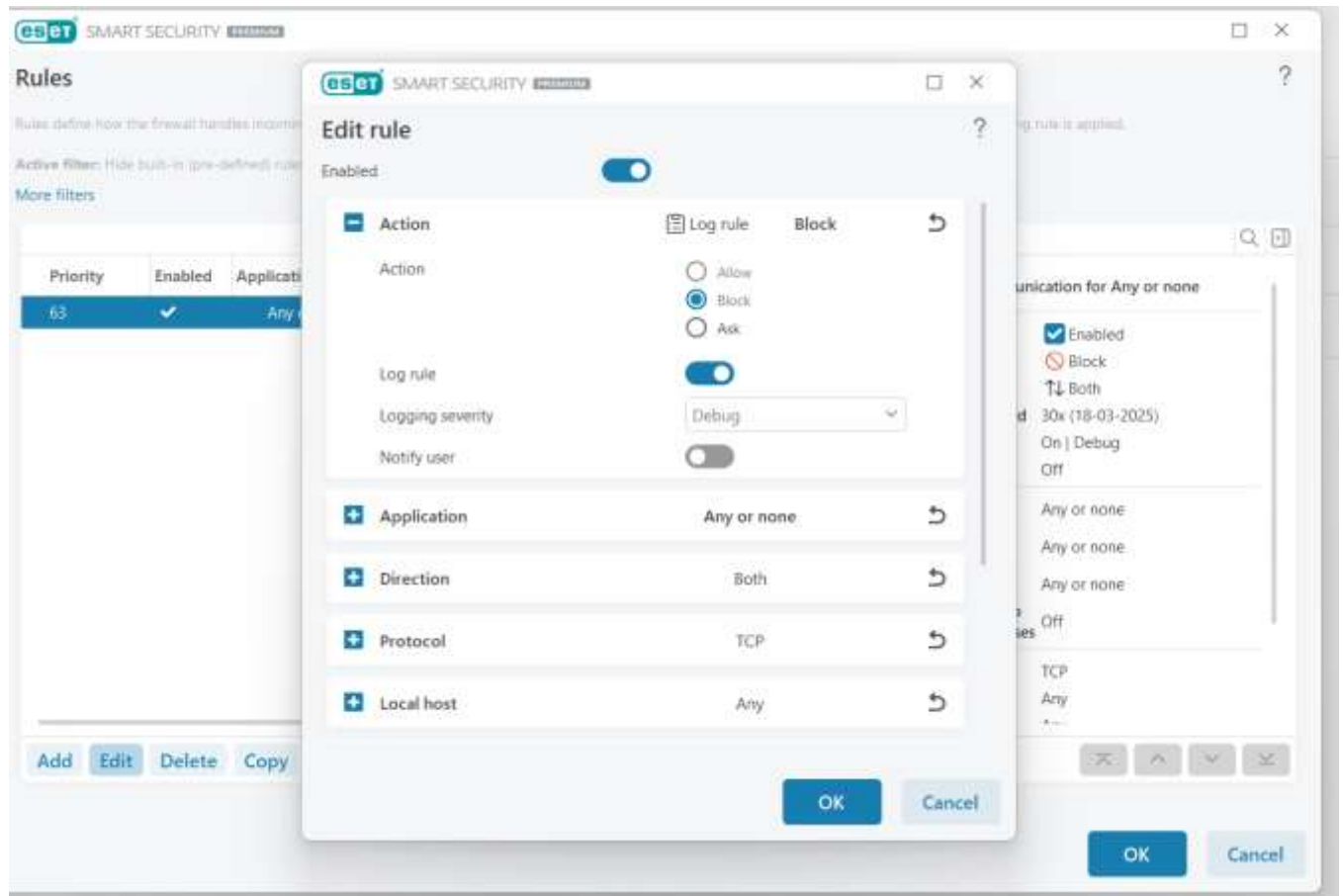


Figure 30: Creating a custom firewall rule in ESET to block internet access

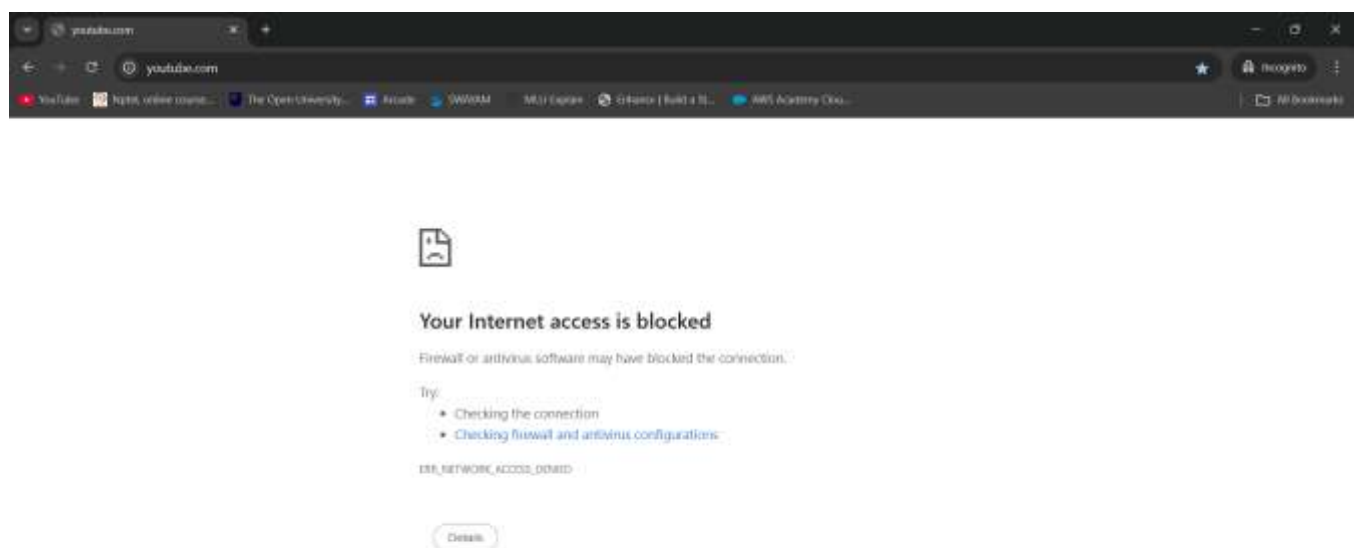


Figure 31: Demonstration of internet access blocked by ESET Firewall

LATEST APPLICATIONS:

- FortiGate Next-Generation Firewall (NGFW)
- Check Point Quantum Firewall
- Cisco Secure Firewall
- pfSense
- ESET

LEARNING OUTCOME:

In this practical, I gained a comprehensive understanding of configuring, managing, and evaluating both Windows Defender Firewall and ESET Personal Firewall. I learned how to create, customize, and apply firewall rules to control network traffic, ensure secure communication, and block unauthorized access. Additionally, I explored advanced security features like intrusion detection, secure browsing, and network monitoring, enhancing my ability to assess and implement firewall solutions in an enterprise environment.

REFERENCES:

1. YouTube : https://www.youtube.com/watch?v=pP7_nFBNR-M
2. ChatGPT: <https://chatgpt.com/>
3. ESET forum : <https://forum.eset.com/topic/25222-eset-firewall-vs-windows-10-firewall/>