

Practical no: 1

Name: Saloni Vishwakarma

Batch-Roll no: C1-13

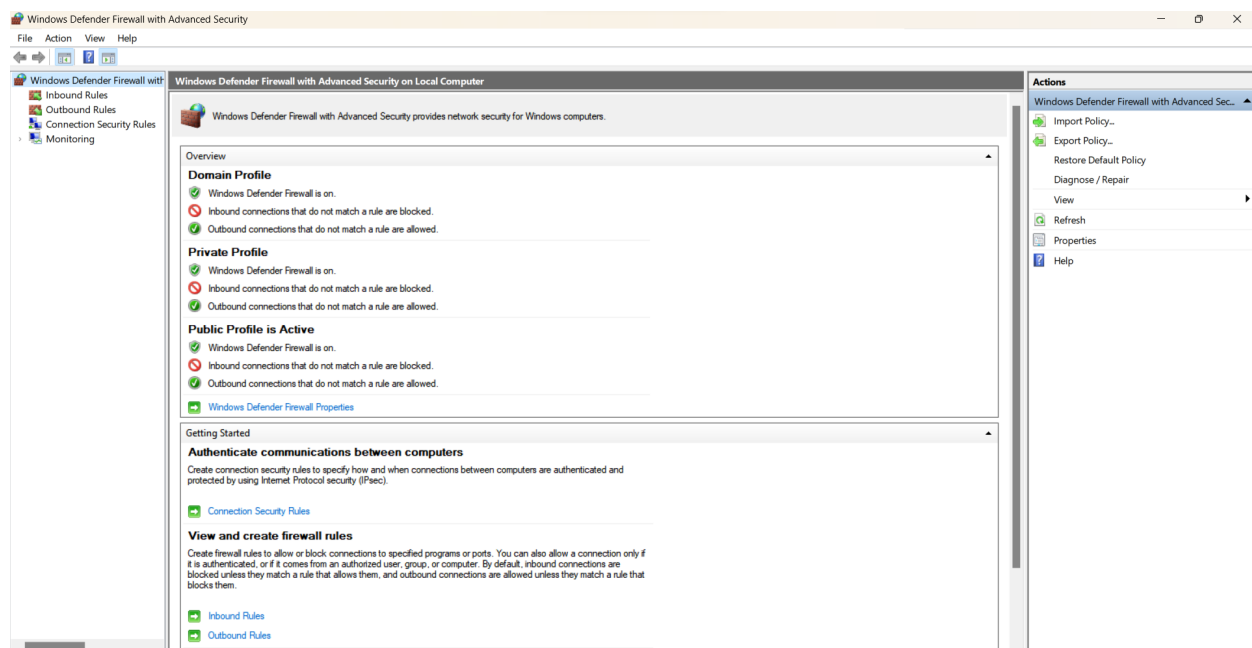
Subject: Computer Security Lab

Date of execution: 2 September 2023

Aim: Introduction to Computer Security Foundations

Task 5: Introduction to Firewalls and Intrusion Detection Systems

- Install a software firewall on a virtual machine.
- Configure firewall rules to allow/block specific network traffic.
- Experiment with intrusion detection system settings and triggers.



Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall with Advanced Security

Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
AnyDesk	Domain	Domain	Yes	Allow	No	C:\Progra...	Any	Any	TCP
AnyDesk	Domain	Domain	Yes	Allow	No	C:\Progra...	Any	Any	UDP
AnyDesk	Public	Public	Yes	Allow	No	C:\Progra...	Any	Any	TCP
AnyDesk	Public	Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
AnyDesk	Private	Private	Yes	Allow	No	C:\Progra...	Any	Any	UDP
AnyDesk	Private	Private	Yes	Allow	No	C:\Progra...	Any	Any	TCP
edipse.exe	Public	Public	Yes	Block	No	C:\users\...	Any	Any	UDP
edipse.exe	Public	Public	Yes	Block	No	C:\users\...	Any	Any	TCP
Firefox	Public	Public	Yes	Block	No	C:\progra...	Any	Any	TCP
Firefox	Public	Public	Yes	Block	No	C:\progra...	Any	Any	UDP
Firefox (C:\Program Files\Mozilla Firefox)	Private	Private	Yes	Allow	No	C:\progra...	Any	Any	TCP
Firefox (C:\Program Files\Mozilla Firefox)	Private	Private	Yes	Allow	No	C:\progra...	Any	Any	UDP
IntelliJ IDEA 2023.1	Private	Private	Yes	Allow	No	C:\progra...	Any	Any	TCP
IntelliJ IDEA 2023.1	Private	Private	Yes	Allow	No	C:\progra...	Any	Any	UDP
Java(TM) Platform SE binary	Private	Private	Yes	Allow	No	C:\progra...	Any	Any	UDP
Java(TM) Platform SE binary	Private	Private	Yes	Allow	No	C:\progra...	Any	Any	TCP
javaw.exe	Private	Private	Yes	Allow	No	C:\users\...	Any	Any	TCP
javaw.exe	Private	Private	Yes	Allow	No	C:\users\...	Any	Any	UDP
Microsoft Lync	Public	Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
Microsoft Lync	Public	Public	Yes	Allow	No	C:\Progra...	Any	Any	TCP
Microsoft Lync Ucmapi	Public	Public	Yes	Allow	No	C:\Progra...	Any	Any	TCP
Microsoft Lync Ucmapi	Public	Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
Microsoft Office Outlook	Public	Public	Yes	Allow	No	C:\Progra...	Any	Any	UDP
NVIDIA SHIELD Streaming NSS TCP Except...	All	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
NVIDIA SHIELD Streaming NSS UDP Except...	All	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
NVIDIA SHIELD Streaming NVStreamer TCP...	All	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
NVIDIA SHIELD Streaming NVStreamer UDP...	All	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
NVIDIA SHIELD Streaming SSAS UDP Except...	All	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
NVIDIA SHIELD Streaming SSAS UDP Except...	All	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
Packet Tracer Executable	Public	Public	Yes	Block	No	C:\progra...	Any	Any	UDP
Packet Tracer Executable	Public	Public	Yes	Block	No	C:\progra...	Any	Any	UDP
Visual Studio Code	Public	Public	Yes	Block	No	C:\users\...	Any	Any	TCP
Visual Studio Code	Public	Public	Yes	Block	No	C:\users\...	Any	Any	UDP
zoom.exe	Public	Public	Yes	Block	No	C:\users\...	Any	Any	TCP
zoom.exe	Public	Public	Yes	Block	No	C:\users\...	Any	Any	UDP

Actions

Inbound Rules

New Rule...

Filter by Profile

Filter by State

Filter by Group

View

Refresh

Export List...

Help

Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall with Advanced Security

Outbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
@(Microsoft.Windows.Search_1.16.0.22000...	@(Microsoft.Windows.Search_1.16.0.22000...	All	Yes	Allow	No	Any	Any	Any	Any
Acer Product Registration	Acer Product Registration	All	Yes	Allow	No	Any	Any	Any	Any
AllJoyn Router (TCP-Out)	AllJoyn Router	Domain	Yes	Allow	No	%System...	Any	Any	TCP
AllJoyn Router (UDP-Out)	AllJoyn Router	Domain	Yes	Allow	No	%System...	Any	Any	UDP
App Installer	App Installer	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local subnet	UDP
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any	UDP
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
Connected Devices Platform - Wi-Fi Direct...	Connected Devices Platform	Public	Yes	Allow	No	%System...	Any	Any	TCP
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domain	Yes	Allow	No	%System...	Any	Any	TCP
Connected Devices Platform (UDP-Out)	Connected Devices Platform	Domain	Yes	Allow	No	%System...	Any	Any	UDP
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP
Core Networking - Dynamic Host Configu...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP

Actions

Outbound Rules

New Rule...

Filter by Profile

Filter by State

Filter by Group

View

Refresh

Export List...

Help

Conclusion: Firewalls and their associated inbound and outbound rules play a critical role in safeguarding networks and systems from various cyber threats. Implementing and managing them effectively is essential for maintaining the security and integrity of an organization's digital assets.