Windows Network Connections & Firewall Audit

Project Type: Endpoint Network Security Assessment

Prepared by: Niknaz (Nikki) Sadehvandi

Role: Founder & Cybersecurity Consultant

Organization: NS Cybersecurity

Date: December 2024

Objective

The objective of this assessment was to evaluate the network exposure and firewall security posture of a Windows endpoint. The review focused on identifying insecure inbound or outbound firewall rules, abnormal network connections, and potential indicators of unauthorized access or malicious activity using native Windows security and networking tools.

Tools & Technologies

- Windows Defender Firewall with Advanced Security
- Command Prompt (Administrator)
- netstat -ano
- Process ID (PID) correlation

Technical Steps Performed

1. Inbound Firewall Rule Review

- Reviewed all enabled inbound firewall rules using Windows Defender Firewall with Advanced Security.
- Analyzed allowed applications and services to identify unnecessary or risky inbound access.
- Verified exposure of commonly targeted services and ports.

2. Outbound Firewall Rule Review

- Reviewed outbound firewall rules to assess egress control.
- Identified applications permitted to initiate outbound connections.
- Verified rules were primarily associated with trusted Windows system components.

3. Live Network Connection Analysis

- Executed netstat -ano to enumerate all active TCP and UDP connections.
- Reviewed:
    - Listening ports
    - Established outbound connections
    - External IP addresses and destination ports
- Correlated Process IDs (PIDs) with known Windows services and applications.

Findings

Firewall Configuration Findings

- Inbound firewall rules were limited to expected applications and services.
- No high-risk inbound ports (e.g., RDP 3389, SMB 445, Telnet 23, FTP 21, SSH 22) were exposed.
- Outbound firewall rules were largely system-generated and associated with trusted Microsoft components.
- No unknown or suspicious firewall rules were identified.

Network Traffic Findings

- Active outbound connections were observed only to legitimate services, including Microsoft and cloud content delivery networks.
- No connections to suspicious, foreign, or high-risk IP addresses were detected.
- No unexpected listening services or unauthorized network listeners were identified.

Outcome

- Confirmed a low-risk network and firewall posture for the Windows endpoint.
- Verified the absence of unauthorized inbound exposure or suspicious outbound activity.
- Established a baseline of normal network behavior suitable for ongoing monitoring and SOC triage.
- Produced verifiable evidence supporting endpoint network security and firewall hardening.

This project demonstrates hands-on experience conducting endpoint network audits, firewall configuration reviews, and real-time traffic analysis using SOC-relevant methodologies.

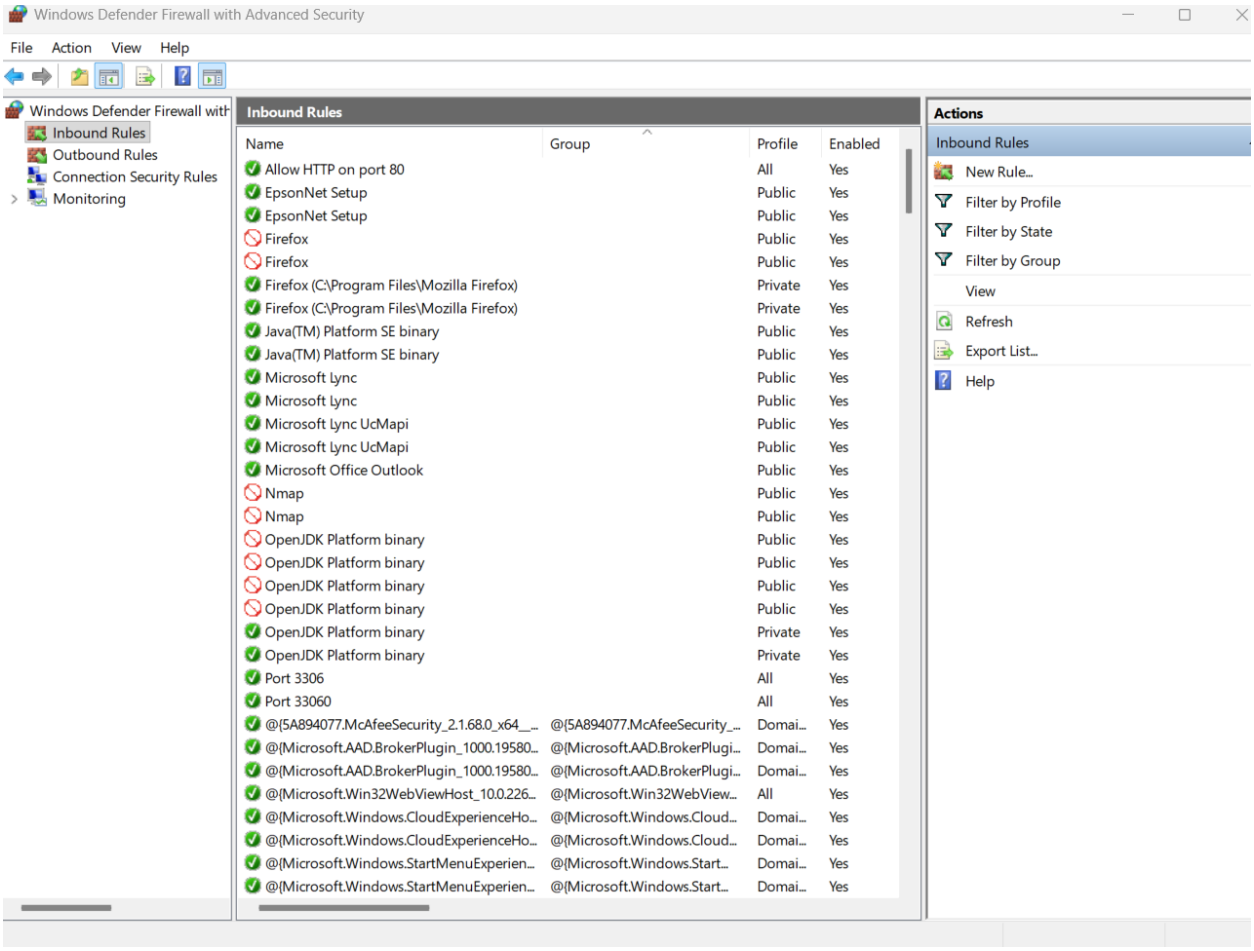
Portfolio Status

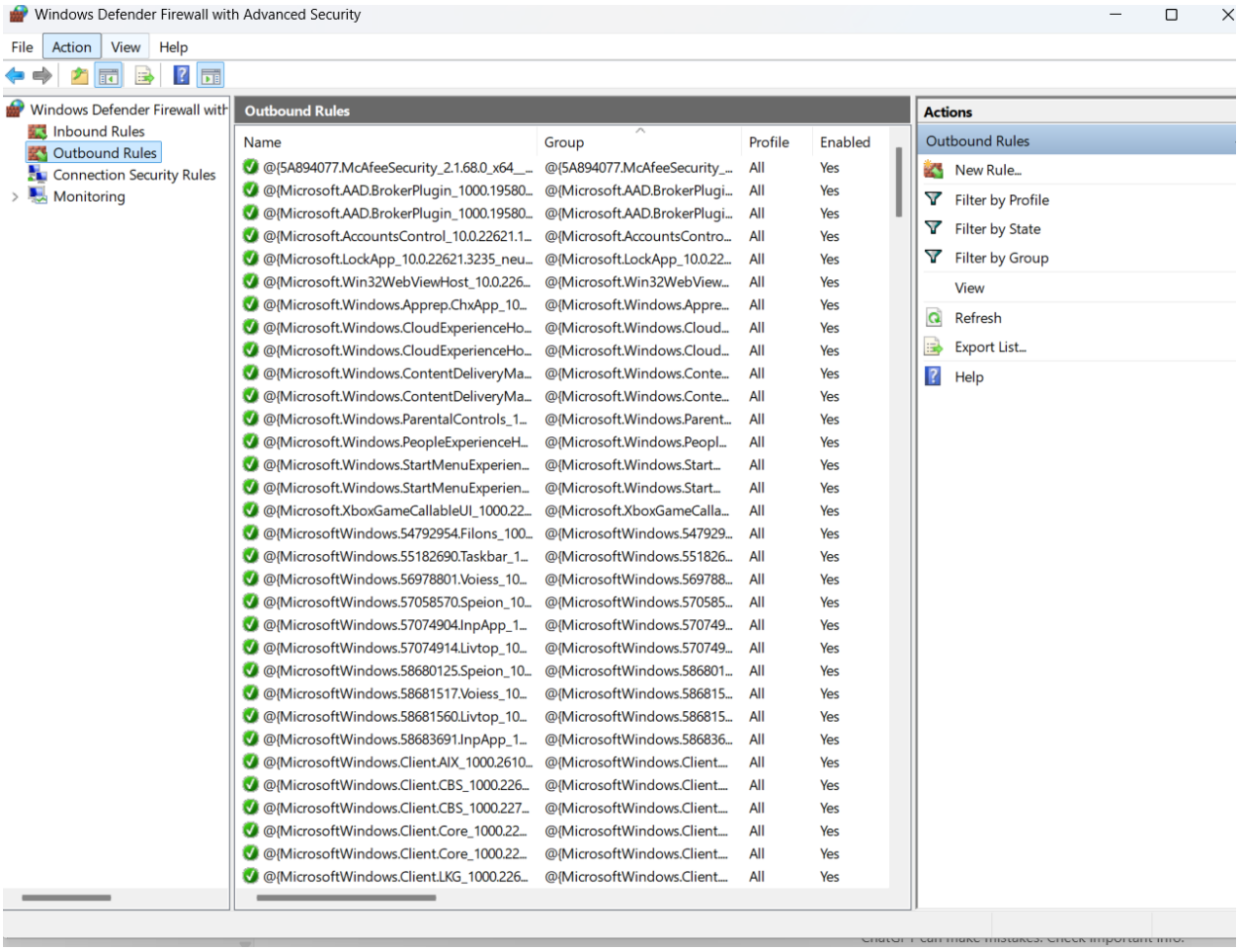
Project Status: Completed

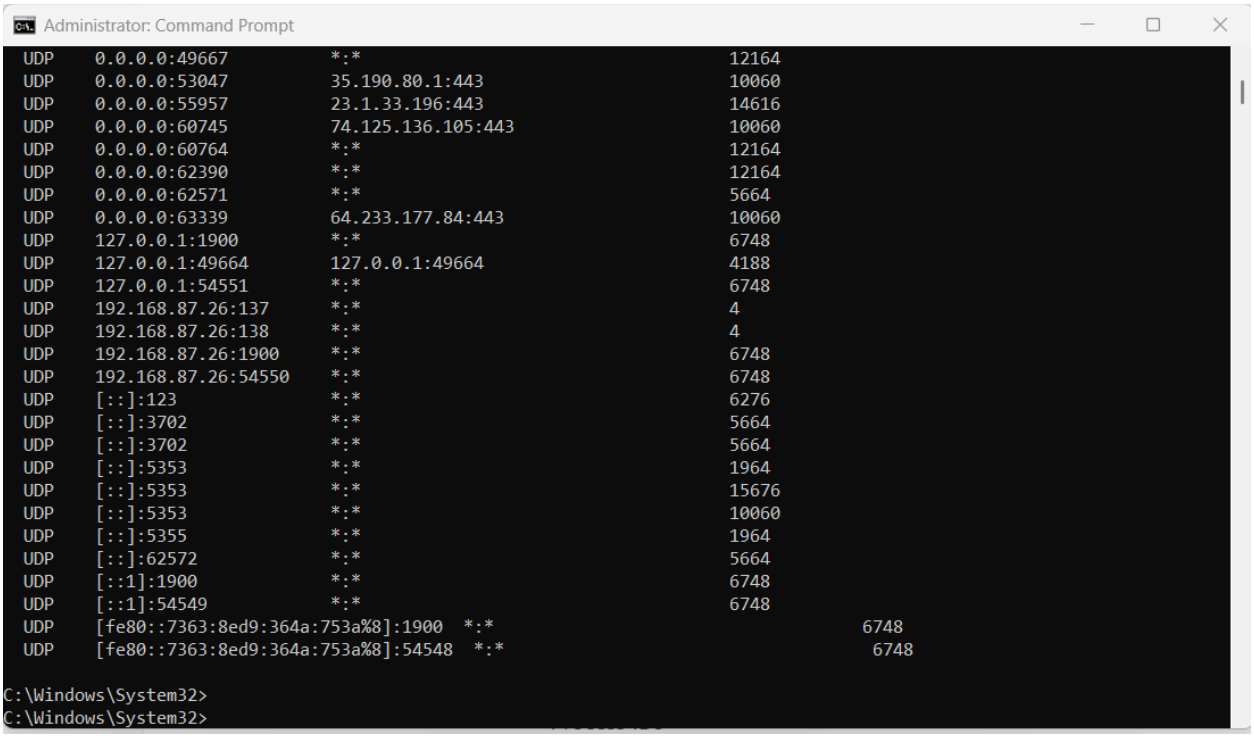
Deliverable:
NETWORK_SECURITY_&_FIREWALL_REVIEW_CONSULTING_PROJECT.pdf

Evidence: Inbound/outbound firewall rule screenshots, netstat -ano output

---


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name Group Profile Enabled
Allow HTTP on port 80 All Yes
EpsonNet Setup Public Yes
EpsonNet Setup Public Yes
Firefox Public Yes
Firefox Public Yes
Firefox (C:\Program Files\Mozilla Firefox) Private Yes
Firefox (C:\Program Files\Mozilla Firefox) Private Yes
Java(TM) Platform SE binary Public Yes
Java(TM) Platform SE binary Public Yes
Microsoft Lync Public Yes
Microsoft Lync Public Yes
Microsoft Lync UcMapi Public Yes
Microsoft Lync UcMapi Public Yes
Microsoft Office Outlook Public Yes
Nmap Public Yes
Nmap Public Yes
OpenJDK Platform binary Public Yes
OpenJDK Platform binary Public Yes
OpenJDK Platform binary Public Yes
OpenJDK Platform binary Public Yes
OpenJDK Platform binary Private Yes
OpenJDK Platform binary Private Yes
Port 3306 All Yes
Port 33060 All Yes
@{5A894077.McAfeeSecurity_2.1.68.0_x64__... @{5A894077.McAfeeSecurity_... Domai... Yes
@{Microsoft.AAD.BrokerPlugin_1000.19580... @{Microsoft.AAD.BrokerPlugi... Domai... Yes
@{Microsoft.AAD.BrokerPlugin_1000.19580... @{Microsoft.AAD.BrokerPlugi... Domai... Yes
@{Microsoft.Win32WebViewHost_10.0.226... @{Microsoft.Win32WebView... All Yes
@{Microsoft.Windows.CloudExperienceHo... @{Microsoft.Windows.Cloud... Domai... Yes
@{Microsoft.Windows.CloudExperienceHo... @{Microsoft.Windows.Cloud... Domai... Yes
@{Microsoft.Windows.StartMenuExperien... @{Microsoft.Windows.Start... Domai... Yes
@{Microsoft.Windows.StartMenuExperien... @{Microsoft.Windows.Start... Domai... Yes
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
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Outbound Rules
Name
Group
Profile
Enabled
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help


Administrator: Command Prompt
UDP 0.0.0.0:49667 *:* 12164
UDP 0.0.0.0:53047 35.190.80.1:443 10060
UDP 0.0.0.0:55957 23.1.33.196:443 14616
UDP 0.0.0.0:60745 74.125.136.105:443 10060
UDP 0.0.0.0:60764 *:* 12164
UDP 0.0.0.0:62390 *:* 12164
UDP 0.0.0.0:62571 *:* 5664
UDP 0.0.0.0:63339 64.233.177.84:443 10060
UDP 127.0.0.1:1900 *:* 6748
UDP 127.0.0.1:49664 127.0.0.1:49664 4188
UDP 127.0.0.1:54551 *:* 6748
UDP 192.168.87.26:137 *:* 4
UDP 192.168.87.26:138 *:* 4
UDP 192.168.87.26:1900 *:* 6748
UDP 192.168.87.26:54550 *:* 6748
UDP [::]:123 *:* 6276
UDP [::]:3702 *:* 5664
UDP [::]:3702 *:* 5664
UDP [::]:5353 *:* 1964
UDP [::]:5353 *:* 15676
UDP [::]:5353 *:* 10060
UDP [::]:5355 *:* 1964
UDP [::]:62572 *:* 5664
UDP [::1]:1900 *:* 6748
UDP [::1]:54549 *:* 6748
UDP [fe80::7363:8ed9:364a:753a%8]:1900 *:* 6748
UDP [fe80::7363:8ed9:364a:753a%8]:54548 *:* 6748
C:\Windows\System32>
C:\Windows\System32>