Windows Firewall

Devin P. Johnson

Old Dominion University: School of Cybersecurity

CYSE 608: Windows Systems for Cybersecurity

Dr. Malik A. Gladden

April 23, 2026

Introduction

Windows Defender Firewall (WDF) is a host-based security control. It regulates what traffic a Windows system can send and receive. As threats evolve and networks become more distributed, firewall policy must shift from perimeter support to endpoint enforcement. This shift is especially important in remote work and hybrid cloud environments. It is also critical in segmented internal networks. Strong rule design can reduce attack surface, slow lateral movement, and support detection. Weak rule design can increase exposure and undermine security outcomes.

Threat Driven Changes to Firewall Policy

Current threat activity often follows a common sequence. Attackers gain initial access. They then use legitimate administrative services to move laterally. MITRE documents remote services as a major lateral movement technique category. It also identifies RDP as a specific method used to expand access when it is enabled and reachable (MITRE ATT&CK, n.d.-a). This threat pattern changes firewall priorities. The key question is not only "what do we block from the internet?" The key question becomes "which internal systems can communicate with which other systems, and over what protocols?"

Network architecture trends reinforce this. Hybrid and remote access reduce the protective value of perimeter controls. Endpoints must remain protected even when they are off the network. At the same time, segmentation strategies push enforcement down to the host level. NIST explains that firewall policy should specify how traffic is handled for defined address ranges and use cases. NIST also emphasizes configuration discipline, testing, and continuous monitoring as core firewall management practices (Scarfone, 2009). As organizations adopt segmentation, jump hosts, and dedicated management networks, WDF rules often become the mechanism that enforces those boundaries on each endpoint.

Application behavior also matters. Windows hosts run many services that listen on ports only when required. Microsoft notes that the firewall blocks inbound traffic by default. Administrators typically add inbound exception rules to allow legitimate services (Microsoft, 2025). This is beneficial, but it creates a structural risk. Every inbound exception expands attack surface. As attackers increasingly target exposed services, policy design must follow allow by need and apply strict scoping.

Security Effects of Inbound, Outbound, and Scoped Rules

Firewall rule impact depends on direction, protocol, and scope. Some rule types create much higher risk than others.

1. Allow rules expand attack surface.
Allowing inbound traffic for remote management services increases exposure. RDP is a clear

example. MITRE notes that adversaries use RDP for lateral movement when it is available and accessible (MITRE ATT&CK, n.d.). RDP rules significantly increase risk. Safer practice is to restrict inbound management rules to:

- Specific management subnets,
- Domain profile only when appropriate,
- Privileged access workflows with strong authentication controls.

2. Scope restrictions can matter as much as port numbers.
A rule allowing TCP/445 (SMB) from "Any" is not equivalent to a rule allowing SMB only from file servers or authorized management systems. Scope is where firewall rules act as segmentation controls. Narrow scope reduces lateral movement paths by limiting who can initiate administrative protocols.

3. Outbound rules can reduce C2 and exfiltration.
Many environments focus on inbound filtering, but modern malware often relies on outbound connectivity. It may need C2 access, payload retrieval, or data exfiltration. NIST's firewall guidance stresses that policy should cover both inbound and outbound traffic handling (Scarfone, 2009).

4. Logging rules support detection and response.
Firewall logs help reconstruct events during investigations. They also help ensure that segmentation is working. NIST highlights that effective firewall programs require testing and ongoing management. Monitoring and reviewing firewall behavior are part of that requirement (Scarfone, 2009).

Conclusion

Emerging threats and modern network architecture increase the security importance of Windows Defender Firewall. As attackers rely on remote services for lateral movement, firewall policy must reduce unnecessary exposure and enforce segmentation at the endpoint (MITRE ATT&CK, n.d.). Windows Defender Firewall's default inbound block posture is a strong baseline. However, every inbound exception must be justified and tightly scoped (Microsoft, 2025). Strong deployments prioritize least-privilege network access, narrow rule scope, feasible outbound controls, and continuous monitoring to reduce attack surface and improve resilience (Scarfone, 2009).

References

Microsoft. (2025, June 6). *Windows Firewall rules*. Microsoft Learn. https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/rules

MITRE ATT&CK. (n.d.-a). *Remote services (T1021)*. https://attack.mitre.org/techniques/T1021/

MITRE ATT&CK. (n.d.-b). Remote desktop protocol (T1021.001). https://attack.mitre.org/techniques/T1021/001/

Scarfone, K. (2009). *Guidelines on firewalls and firewall policy (NIST SP 800-41 Rev. 1)*. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/41/r1/final