SMB Protocol Explained: File Sharing, Ports, Security Risks, and Protection Measures

TechRounder PDF Edition

Live article:
https://www.techrounder.com/insights/smb-protocol-explained-file-sharing-ports-security-risks-and-protection-measures/

By Vipin PG | Published April 21, 2025 | Updated January 4, 2026 | Format: Analysis | 3 min read

In brief

The Server Message Block (SMB) protocol plays a major role in how computers communicate over a network. Whether you're accessing shared files, network printers, or remote servers, SMB is the invisible backbone making it all work smoothly.

The Server Message Block (SMB) protocol plays a major role in how computers communicate over a network. Whether you're accessing shared files, network printers, or remote servers, SMB is the invisible backbone making it all work smoothly.

In this article, we'll check what SMB is, how it works, the ports it uses, potential risks, major attack incidents like WannaCry, and-most importantly-how you can protect your network from SMB-based threats.

What is the SMB Protocol?

SMB (Server Message Block) is a communication protocol that enables applications and systems on a network to share files, printers, and other resources. It facilitates client-server communication and supports inter-process communication between devices in the same network.

This means with SMB, your system can:

- Access files on a remote server
- Print documents using a shared printer
- Read and write to remote files as if they are local

How Does SMB Work?

SMB uses a request-response model where a client sends a request and the server responds with the appropriate action. For example:

- A client requests a file
- The server verifies access and sends the file back

Earlier versions of SMB operated over NetBIOS (on port 139), but since Windows 2000, SMB has been working over TCP/IP using port 445, which is now the standard.

SMB Versions and Dialects

SMB has evolved significantly over the years. Here are the key versions and implementations:

SMB Version: SMB 1.0 | Year Introduced: 1984 | Key Features: Original version, used opportunistic locking

SMB Version: CIFS | Year Introduced: 1996 | Key Features: Microsoft's extension of SMB, added larger file support

SMB Version: SMB 2.0 | Year Introduced: 2006 | Key Features: Reduced command count for better performance

SMB Version: SMB 2.1 | Year Introduced: 2010 | Key Features: Improved energy efficiency and performance

SMB Version: SMB 3.0 | Year Introduced: 2012 | Key Features: Introduced encryption and failover features

SMB Version: SMB 3.02 | Year Introduced: 2014 | Key Features: Disabled SMB 1.0 support

SMB Version: SMB 3.1.1 | Year Introduced: 2015 | Key Features: Improved security with preauthentication and encryption

Other notable SMB implementations:

- Samba : Open-source SMB for Linux/Unix systems
- MoSMB : Enterprise-grade SMB for Unix-like systems
- NQ : Cross-platform SMB for embedded devices
- Tuxera SMB : Proprietary SMB used in high-performance systems
- Likewise : Identity-aware SMB with multi-protocol support

SMB Ports: 139 vs. 445

SMB uses two main ports depending on the version and configuration:

- Port 139 : Used by older versions over NetBIOS (SMB 1.0)
- Port 445 : Used by newer versions directly over TCP/IP (SMB 2 and above)

> Quote: Port 445 is the standard today but has become a major target for attackers.

Security Risks of SMB

Despite its usefulness, SMB has a history of being vulnerable to cyberattacks, especially when exposed to the internet. Here’s why:

Common Threats:

- Unauthorized Access : Weak permissions allow intruders to view sensitive files
- SMB Scanning : Tools like Nmap and Metasploit can find devices using SMB
- Ransomware : SMB vulnerabilities have been used in major global attacks like WannaCry

WannaCry and EternalBlue: A Major SMB Exploit

In 2017, the WannaCry ransomware outbreak exploited a vulnerability in SMBv1 using the EternalBlue exploit. It affected thousands of systems across businesses, banks, and hospitals globally.

How It Worked:

- Scanned networks for open port 445
- Exploited the SMBv1 vulnerability
- Spread automatically across machines without user interaction

Microsoft later released emergency security patches even for older systems like Windows XP and Server 2003 to mitigate the attack.

How to Protect Your SMB Ports (139 & 445)

Here are key strategies to secure SMB-enabled systems:

Block Unused SMB Ports

- Block port 445 on devices not using SMB

- Use a firewall rule like: ‘Source: Any Destination: Any Destination Port: 445 Action: Deny‘

Use Firewalls and Endpoint Security

- Implement firewall policies to block external SMB traffic
- Use endpoint protection tools with IP blacklists and attack pattern detection

Use VPNs and VLANs

- VPNs encrypt network traffic, protecting SMB sessions
- VLANs isolate internal SMB traffic from external access

Patch Your Systems Regularly

- Ensure Windows updates are applied
- Disable SMBv1 completely on all modern systems

Monitor Network Activity

- Use SIEM (Security Information and Event Management) systems
- Deploy Intrusion Detection/Prevention Systems (IDS/IPS)

EventLog Analyzer: SMB Threat Detection in Action

Tools like ManageEngine EventLog Analyzer can help:

- Monitor denied connections on port 445
- Analyze source/destination IPs
- Correlate SMB logs with other network activities
- Create real-time alerts for SMB anomalies

This kind of monitoring is essential for early threat detection and quick response to suspicious SMB traffic.

Conclusion

While SMB is essential for modern network communication, it also brings security challenges if not managed carefully. Open ports like 445 are easy targets for attackers, but with the right mix of firewall rules, monitoring, patching, and network design, you can secure your systems effectively.

Stay alert, update regularly, and never expose SMB to the internet unless absolutely necessary. Security is not just about keeping things working-it’s about keeping them safe too.