Preventing SMB traffic from lateral connections and entering or leaving the network

Archived: 2026-04-05 16:45:17 UTC

▶ Applies To

Summary

Server Message Block (SMB) is a network file sharing and data fabric protocol. SMB is used by billions of devices in a diverse set of operating systems, including Windows, MacOS, iOS, Linux, and Android. Clients use SMB to access data on servers. This allows sharing of files, centralized data management, and lowered storage capacity needs for mobile devices. Servers also use SMB as part of the Software-defined Data Center for workloads such as clustering and replication.

Because SMB is a remote file system, it requires protection from attacks in which a Windows computer might be tricked into contacting a malicious server that's running inside a trusted network or to a remote server outside the network perimeter. Firewall best practices and configurations can enhance security and prevent malicious traffic from leaving the computer or its network.

Effect of changes

Blocking connectivity to SMB might prevent various applications or services from functioning. For a list of Windows and Windows Server applications and services that may stop functioning in this situation, see Service overview and network port requirements for Windows

More information

Perimeter firewall approaches

Perimeter hardware and appliance firewalls that are positioned at the edge of the network should block unsolicited communication (from the internet) and outgoing traffic (to the internet) to the following ports.

Application protocol	Protocol	Port
SMB	TCP	445
NetBIOS Name Resolution	UDP	137

NetBIOS Datagram Service	UDP	138
NetBIOS Session Service	TCP	139

It is unlikely that any SMB communication originating from the internet or destined for the internet is legitimate. The primary case might be for a cloud-based server or service such as Azure Files. You should create IP address-based restrictions in your perimeter firewall to allow only those specific endpoints. Organizations can allow port 445 access to specific Azure Datacenter and O365 IP ranges to enable hybrid scenarios in which on-premises clients (behind an enterprise firewall) use the SMB port to talk to Azure file storage. You should also allow only SMB 3.*x* traffic and require SMB AES-128 encryption. See the "References" section for more information.

Note The use of NetBIOS for SMB transport ended in Windows Vista, Windows Server 2008, and in all later Microsoft operating systems when Microsoft introduced SMB 2.02. However, you may have software and devices other than Windows in your environment. You should disable and remove SMB1 if you have not already done so because it still uses NetBIOS. Later versions of Windows Server and Windows no longer install SMB1 by default and will automatically remove it if allowed.

Windows Defender firewall approaches

All supported versions of Windows and Windows Server include the Windows Defender Firewall (previously named the Windows Firewall). This firewall provides additional protection for devices, especially when devices move outside a network or when they run within one.

The Windows Defender Firewall has distinct profiles for certain types of networks: Domain, Private, and Guest/Public. The Guest/Public network typically gets much more restrictive settings by default than the more trustworthy Domain or Private networks. You may find yourself having different SMB restrictions for these networks based on your threat assessment versus operational needs.

Inbound connections to a computer

For Windows clients and servers that do not host SMB shares, you can block all inbound SMB traffic by using the Windows Defender Firewall to prevent remote connections from malicious or compromised devices. In the Windows Defender Firewall, this includes the following inbound rules.

Name	**Profile**	**Enabled**
File and Printer Sharing (SMB-In)	All	No
Netlogon Service (NP-In)	All	No

Remote Event Log Management (NP-In)	All	No
Remote Service Management (NP-In)	All	No

You should also create a new blocking rule to override any other inbound firewall rules. Use the following suggested settings for any Windows clients or servers that do not host SMB Shares:

- **Name**: Block all inbound SMB 445
- **Description**: Blocks all inbound SMB TCP 445 traffic. Not to be applied to domain controllers or computers that host SMB shares.
- **Action**: Block the connection
- **Programs**: All
- **Remote Computers**: Any
- **Protocol Type**: TCP
- **Local Port**: 445
- **Remote Port**: Any
- **Profiles**: All
- **Scope (Local IP Address)**: Any
- **Scope (Remote IP Address)**: Any
- **Edge Traversal**: Block edge traversal

You must not globally block inbound SMB traffic to domain controllers or file servers. However, you can restrict access to them from trusted IP ranges and devices to lower their attack surface. They should also be restricted to Domain or Private firewall profiles and not allow Guest/Public traffic.

Note The Windows Firewall has blocked all inbound SMB communications by default since Windows XP SP2 and Windows Server 2003 SP1. Windows devices will allow inbound SMB communication only if an administrator creates an SMB share or alters the firewall default settings. You should not trust the default out-of-box experience to still be in-place on devices, regardless. Always verify and actively manage the settings and their desired state by using Group Policy or other management tools.

For more information, see Designing a Windows Defender Firewall with Advanced Security Strategy and Windows Defender Firewall with Advanced Security Deployment Guide

Outbound connections from a computer

Windows clients and servers require outbound SMB connections in order to apply group policy from domain controllers and for users and applications to access data on file servers, so care must be taken when creating firewall rules to prevent malicious lateral or internet connections. By default, there are no outbound blocks on a Windows client or server connecting to SMB shares, so you will have to create new blocking rules.

You should also create a new blocking rule to override any other inbound firewall rules. Use the following suggested settings for any Windows clients or servers that do not host SMB Shares.

Guest/Public (untrusted) networks

- **Name**: Block outbound Guest/Public SMB 445
- **Description**: Blocks all outbound SMB TCP 445 traffic when on an untrusted network
- **Action**: Block the connection
- **Programs**: All
- **Remote Computers**: Any
- **Protocol Type**: TCP
- **Local Port**: Any
- **Remote Port**: 445
- **Profiles**: Guest/Public
- **Scope (Local IP Address)**: Any
- **Scope (Remote IP Address)**: Any
- **Edge Traversal**: Block edge traversal

Note Small office and home office users, or mobile users who work in corporate trusted networks and then connect to their home networks, should use caution before they block the public outbound network. Doing this may prevent access to their local NAS devices or certain printers.

Private/Domain (trusted) networks

- **Name**: Allow outbound Domain/Private SMB 445
- **Description**: Allows outbound SMB TCP 445 traffic to only DCs and file servers when on a trusted network
- **Action**: Allow the connection if it is secure
- **Customize Allow if Secure Settings**: *pick one of the options, set Override block rules = ON*
- **Programs**: All

- **Protocol Type**: TCP
- **Local Port**: Any
- **Remote Port**: 445
- **Profiles**: Private/Domain
- **Scope (Local IP Address)**: Any
- **Scope (Remote IP Address)**: *<list of domain controller and file server IP addresses>*
- **Edge Traversal**: Block edge traversal

Note You can also use the Remote Computers instead of Scope remote IP addresses, if the secured connection uses authentication that carries the computer's identity. Review the Defender Firewall documentation for more information about "Allow the connection if is secure" and the Remote Computer options.

- **Name**: Block outbound Domain/Private SMB 445
- **Description**: Blocks outbound SMB TCP 445 traffic. Override by using the "Allow outbound Domain/Private SMB 445" rule
- **Action**: Block the connection
- **Programs**: All
- **Remote Computers**: N/A
- **Protocol Type**: TCP
- **Local Port**: Any
- **Remote Port**: 445
- **Profiles**: Private/Domain
- **Scope (Local IP Address)**: Any
- **Scope (Remote IP Address)**: N/A
- **Edge Traversal**: Block edge traversal

You must not globally block outbound SMB traffic from computers to domain controllers or file servers. However, you can restrict access to them from trusted IP ranges and devices to lower their attack surface.

For more information, see Designing a Windows Defender Firewall with Advanced Security Strategy and Windows Defender Firewall with Advanced Security Deployment Guide

Security connection rules

You must use a security connection rule to implement the outbound firewall rule exceptions for the "Allow the connection if it is secure" and "Allow the connection to use null encapsulation" settings. If you do not set this rule on all Windows-based and Windows Server-based computers, authentication will fail, and SMB will be blocked outbound.

For example, the following settings are required:

- **Rule type**: Isolation
- **Requirements**: Request authentication for inbound and outbound connections
- **Authentication method**: Computer and user (Kerberos V5)
- **Profile**: Domain, Private, Public
- **Name**: Isolation ESP Authentication for SMB overrides

For more information about security connection rules, see the following articles:

- Designing a Windows Defender Firewall with Advanced Security Strategy
- Checklist: Configuring Rules for an Isolated Server Zone

Windows Workstation and Server Service

For consumer or highly isolated, managed computers that do not require SMB at all, you can disable the Server or Workstation services. You can do this manually by using the “Services” snap-in (Services.msc) and the PowerShell **Set-Service** cmdlet, or by using Group Policy Preferences. When you stop and disable these services, SMB can no longer make outbound connections or receive inbound connections.

You must not disable the Server service on domain controllers or file servers or no clients will be able to apply group policy or connect to their data anymore. You must not disable the Workstation service on computers that are members of an Active Directory domain or they will no longer apply group policy.

References

Designing a Windows Defender Firewall with Advanced Security Strategy Windows Defender Firewall with Advanced Security Deployment Guide Azure remote apps Azure datacenter IP addresses Microsoft O365 IP addresses

Need more help?

Want more options?

Explore subscription benefits, browse training courses, learn how to secure your device, and more.
