Secure SMB Traffic in Windows Server

Article • 12/23/2021 • 7 minutes to read •

Is this page helpful?

In this article

As a defense in depth measure, you can use segmentation and isolation techniques to secure SMB traffic and reduce threats between devices on your network.

SMB is used for file sharing, printing, and inter-process communication such as named pipes and RPC. It's also used as a network data fabric for technologies such as Storage Spaces Direct, Storage Replica, Hyper-V Live Migration, and Cluster Shared Volumes. Use the following sections to configure SMB traffic segmentation and endpoint isolation to help prevent outbound and lateral network communications.

Block inbound SMB access

Block TCP port 445 inbound from the internet at your corporate hardware firewalls. Blocking inbound SMB traffic protects devices inside your network by preventing access from the internet.

If you want users to access their files inbound at the edge of your network, you can use SMB over QUIC. This uses TCP port 443 by default and provides a TLS 1.3-encrypted security tunnel like a VPN for SMB traffic. The solution requires Windows 11 and Windows Server 2022 Datacenter: Azure Edition file servers running on Azure Stack HCI. For more information, see SMB over QUIC .

Block outbound SMB access

Block TCP port 445 outbound to the internet at your corporate firewall. Blocking outbound SMB traffic prevents devices inside your network from sending data using SMB to the internet.

It is unlikely you need to allow any outbound SMB using TCP port 445 to the internet unless you require it as part of a public cloud offering. The primary scenarios include Azure Files and Office 365.

If you are using Azure Files SMB, use a VPN for outbound VPN traffic. By using a VPN, you restrict the outbound traffic to the required service IP ranges. For more information about Azure Cloud and Office 365 IP address ranges, see:

- Azure IP ranges and service tags: public cloud ,US government cloud , Germany cloud , or China cloud . The JSON files are updated weekly and include versioning both for the full file and each individual service tag. The *AzureCloud* tag provides the IP ranges for the cloud (Public, US government, Germany, or China) and is grouped by region within that cloud. Service tags in the file will increase as Azure services are added.
- Office 365 URLs and IP address ranges.

With Windows 11 and Windows Server 2022 Datacenter: Azure Edition, you can use SMB over QUIC to connect to file servers in Azure. This uses TCP port 443 by default and provides a TLS 1.3-encrypted security tunnel like a VPN for the SMB traffic. For more information, see SMB over QUIC .

Inventory SMB usage and shares

By inventorying your network's SMB traffic, you get an understanding of traffic that is occurring and can determine if it's necessary. Use the following checklist of questions to help identify unnecessary SMB traffic.

For server endpoints:

1. Which server endpoints require inbound SMB access to do their role? Do they need inbound access from all clients, certain networks, or certain nodes?
2. Of the remaining server endpoints, is inbound SMB access necessary?

For client endpoints:

1. Which client endpoints (for example, Windows 10) require inbound SMB access? Do they need inbound access from all clients, certain networks, or certain nodes?
2. Of the remaining client endpoints, is inbound SMB access necessary?
3. Of the remaining client endpoints, do they need to run the SMB server service?

For all endpoints, determine if you allow outbound SMB in the safest and most minimal fashion.

Review server built-in roles and features that require SMB inbound. For example, file servers and domain controllers require SMB inbound to do their role. For more information on built-in roles and feature network port requirements, see Service overview and network port requirements for Windows.

Review servers that need to be accessed from inside the network. For example, domain controllers and file servers likely need to be accessed anywhere in the network. However, application server access may be limited to a set of other application servers on the same subnet. You can use the following tools and features to help you inventory SMB access:

- Use Get-FileShares script to examine shares on servers and clients.
- Enable an audit trail of SMB inbound access using the registry key `Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\File Share`. Since the number of events may be large, consider enabling for a specified amount of time or use Azure Monitor .

Examining SMB logs lets you know which nodes are communicating with endpoints over SMB. You can decide if an endpoint's shares are in use and understand which to exist.

Configure Windows Defender Firewall

Use firewall rules to add extra connection security. Configure rules to block both inbound and outbound communications that include exceptions. An outbound firewall policy that prevents use of SMB connections both outside and inside your managed network while allowing access to the minimum set of servers and no other devices is a lateral defense-in-depth measure.

For information on the SMB firewall rules you need to set for inbound and outbound connections, see the support article Preventing SMB traffic from lateral connections and entering or leaving the network .

The support article includes templates for:

- Inbound rules that are based on any kind of network profile.
- Outbound rules for private/domain (trusted) networks.
- Outbound rules for guest/public (untrusted) networks. This template is important to enforce on mobile devices and home-based telecommuters that are not behind your firewall that is blocking outbound traffic. Enforcing these rules on laptops reduces the odds of phishing attacks that send users to malicious servers to harvest credentials or run attack code.
- Outbound rules that contain an override *allowlist* for domain controllers and file servers called *Allow the connection if secure*.

To use the null encapsulation IPSEC authentication, you must create a Security Connection rule on all computers in your network that are participating in the rules. Otherwise, the firewall exceptions won't work and you'll only be arbitrarily blocking.

> ⊗ **Caution**
>
> You should test the Security Connection rule before broad deployment. An incorrect rule could prevent users from accessing their data.

To create a *Connection Security* rule, use Windows Defender Firewall with Advanced Security control panel or snap-in:

1. In Windows Defender Firewall, select *Connection Security Rules* and choose a **New rule**.
2. In *Rule Type*, select **Isolation** then select **Next**.
3. In *Requirements*, select **Request authentication for inbound and outbound connections** then select **Next**.
4. In *Authentication Method*, select **Computer and User (Kerberos V5)** then select **Next**.
5. In *Profile*, check all profiles (*Domain, Private, Public*) then select **Next**.
6. Enter a name your rule then select **Finish**.

Remember, the Connection Security rule must be created on all clients and servers participating in your inbound and outbound rules or they will be blocked from connecting SMB outbound. These rules may already be in place from other security efforts in your environment and like the firewall inbound/outbound rules, can be deployed via group policy.

When configuring rules based on the templates in the Preventing SMB traffic from lateral connections and entering or leaving the network support article, set the following to customize the *Allow the connection if secure* action:

1. In the *Action* step, select **Allow the connection if it is secure** then select **Customize**.
2. In *Customize Allow if Secure Settings*, select **Allow the connection to use null encapsulation**.

The *Allow the connection if it is secure* option allows override of a global block rule. You can use the easy but least secure *Allow the connection to use null encapsulation* with *override block rules, which relies on Kerberos and domain membership for authentication. Windows Defender Firewall allows for more secure options like IPSEC.

For more information about configuring the firewall, see Windows Defender Firewall with Advanced Security deployment overview.

Disable SMB Server if unused

Windows clients and some of your Windows Servers on your network may not require the SMB Server service to be running. If the SMB Server service isn't required, you can disable the service. Before disabling SMB Server service, be sure no applications and processes on the computer require the service.

You can use Group Policy Preferences to disable the service on a large number of machines when you are ready to implement. For more information about configuring Group Policy Preferences, see Configure a Service Item.

Test and deploy using policy

Begin by testing using small-scale, hand-made deployments on select servers and clients. Use phased group policy rollouts to make these changes. For example, start with the heaviest user of SMB such as your own IT team. If your team's laptops and apps and file share access work well after deploying your inbound and outbound firewall rules, create test group policy within your broad test and QA environments. Based on results, start sampling some departmental machines, then expand out.

Next steps

Watch Jessica Payne's Ignite conference session Demystifying the Windows Firewall

Recommended content

Improve performance of a file server with SMB Direct

Describes the SMB Direct feature in Windows Server 2012 R2, Windows Server 2012, and Windows Server 2016.

Advanced Troubleshooting Server Message Block (SMB)

Introduces the advanced Server Message Block (SMB) troubleshooting methods.

SMB security enhancements

This topic explains the SMB security enhancements in Windows Server.

Reduced performance after SMB Encryption or SMB Signing is enabled - Windows Server

Describes an issue in which networking performance is reduced after you enable SMB Encryption or SMB Signing in Windows Server 2016 and Windows Server 2019. Provides a solution to this issue.

Show more