Fixing Netscan Abuse Reports on a Windows Server: Blocking Teredo and Private Networks

How-to Guides · https://www.hyyat.com/en/knowledgebase/fix-netscan-abuse-windows-server/

This guide covers two Windows Firewall settings that stop a server from sending traffic that looks like network scanning:

- Blocking Teredo ports so packets are not sent to the internet.
- Blocking traffic to private networks.

A common reason to do this is an abuse report saying your server is making a large number of network scans. Port and network scanning is not allowed under the Hyyat Host terms of service.

The logs in such a report often look like this:

```
> time             protocol  src_ip          src_port    dest_ip                 dest_port
> ---------------------------------------------------------------------------------------
> [DATE and time]  UDP       [Your Server IP] 59300  =>  [some destination IP 1]  3544
> [DATE and time]  UDP       [Your Server IP] 59300  =>  [some destination IP 2]  3544
> [DATE and time]  UDP       [Your Server IP] 59300  =>  [some destination IP 3]  3544
> [DATE and time]  TCP       [Your Server IP] 59762  =>  10.0.0.138 [a private IP] 10983
```

The source port, 59300, is normal and should not be blocked; other services use it too. There are two problems in this log:

- Port 3544 is the port Teredo listens on at the destination, so your server is sending requests to other servers on their port 3544.
- Private IP addresses appear in the list. These should be blocked too.

> **Note:** Teredo is an IPv6 transition technology. It gives IPv6 addresses and automatic host-to-host tunnels for IPv6 traffic when hosts sit behind one or more IPv4 NAT devices.

Before you start

You only need to be able to log in with an account that has administrator rights.

Step 0: open the Windows Firewall settings

Open **Windows Defender Firewall with Advanced Security** in one of two ways:

- Press **Windows + R**, type `wf.msc` and press **Enter**.
- Open the Start menu, type “Windows Defender Firewall with Advanced Security” and choose the result.

In steps 1 and 2 you add new outbound rules. In the firewall window, click **Outbound Rules** on the left, then **New Rule…** in the Actions pane on the right (or right-click **Outbound Rules** and choose **New Rule…**).

Step 1: block the destination port (Teredo port 3544)

This stops connections to outside servers on port 3544, the port they use for Teredo.

> **Note:** If another program is doing the scanning, use the destination port you see in your own log instead. You can also disable the program or service causing the traffic (such as Teredo) rather than blocking its port, especially if you need that port open for something else.

Open the firewall as in step 0, then:

1. In the **New Outbound Rule** wizard, choose **Port** and click **Next**.
2. The log shows the traffic was UDP, so choose **UDP**. Under the remote ports question, choose **Specific remote ports**, enter `3544` and click **Next**.
3. Make sure **Block the connection** is selected and click **Next**.
4. Leave **When does this rule apply?** at the defaults and click **Next**.
5. Give the rule a name (required) and a description (optional), then click **Finish**.

All connections to remote hosts on port 3544 are now dropped by your firewall before they reach the network.

Step 2: block traffic to private networks

Now add rules that block outbound traffic to these private networks:

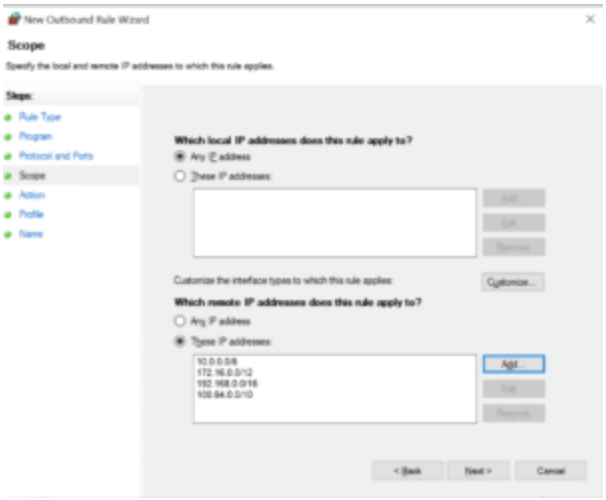
- `10.0.0.0/8`
- `172.16.0.0/12`
- `192.168.0.0/16`
- `100.64.0.0/10`

These are not public addresses; they are reserved for internal networks, such as the address you use to configure a home router (often starting with 192) or an office printer (often 192 or 172). A badly configured application may try to reach them.

An example of doing this by accident: you build or use an app made for a company's internal network that connects to a local server on a private address. If you copy that app to your server to publish it, it keeps trying to reach a private address that does not exist on the server's network.

Open the firewall as in step 0, then:

1. In the **New Outbound Rule** wizard, choose **Custom** and click **Next**.
2. Leave the program on **All programs** and click **Next**. Leave the protocol and port settings at the defaults and click **Next**.
3. Under **Which remote IP addresses does this rule apply to?**, choose **These IP addresses**.
4. Click **Add…** to enter the range you want to block.
5. In **IP address or subnet**, enter the first range, `10.0.0.0/8`, and click **OK**.
6. Repeat step 5 for `172.16.0.0/12`, `192.168.0.0/16` and `100.64.0.0/10`.



7. Click **Next**.
8. Make sure **Block the connection** is selected and click **Next**.
9. Leave **When does this rule apply?** at the defaults and click **Next**.
10. Give the rule a name and an optional description, then click **Finish**.

The rule takes effect right away. Outbound traffic to these ranges is dropped by Windows Firewall before it reaches the network, so it will no longer trigger abuse reports.

Step 3: IPv6 without Teredo (optional)

Teredo is useful for IPv6, and we have just blocked it. If you need IPv6, you can still use it: Hyyat Host servers come with native IPv6. In fact, Teredo should be disabled when native IPv6 is available.

Step 4: find the cause (optional)

If your log shows different source or destination ports, these tips help you find which program uses them. You can then block it as above or fix it in the application.

Tip 1: find the process from the source port (for example 59244). Open PowerShell as administrator (Start menu, type *powershell*, right-click it and choose *Run as administrator*) and run:

```
Get-Process -Id (Get-NetUDPEndpoint -LocalPort 59244).OwningProcess
```

Replace 59244 with your port. For TCP ports, replace `Get-NetUDPEndpoint` with `Get-NetTCPConnection`.

Tip 2: find the process from the destination port. Open CMD and run:

```
netstat -ano | findStr "XXXX"
```

Replace XXXX with the port number and keep the quotes. The last column is the process ID; you can look it up in Process Explorer.

Once you know the process, you can also keep watching it with Process Explorer.

Summary

You have hardened Windows Firewall to stop your server from sending traffic that looks like network abuse. We used Teredo as the example, but the same method works for any application, for instance a test build that sends stray packets because of a bug. If the abuse reports continue, watch the program responsible with Process Explorer and `netstat` as shown in step 4.

Related service: Cloud VPS servers from Hyyat Host, with support that answers tickets within 24 hours at most.

Related guides

- How to Install Windows Server on Your Cloud Server
- The difference between cloud servers and dedicated servers
- How to Order a Cloud Server from Hyyat Host, Step by Step

All usage guides →

Need this service from Hyyat Host?Our team handles it for you, with support replying to tickets within 24 hours at most.
windows hosting