Firewall Best Practices

Nasuni Corporation — Boston, MA

Introduction

This document is intended to guide you in configuring your network to install and configure the Nasuni Filer.

Ports

Port number	Associated protocols	Used for	Inbound (to Nasuni Filer)	Outbound (from Nasuni Filer)
8443	HTTPS	Access Nasuni Filer administrative interface.	Optional (but not recommended), open to Nasuni Filer for external management access direct or via NAT.	N/A
443	HTTPS	Nasuni Management Console Administrative Access; Web Access; Desktop and Mobile Access; Nasuni Desktop Client (Windows, Linux, and OSX clients); and Mobile Access (iOS and Android clients).	Optional, but required if using Web Access, or Desktop and Mobile Access and external access is desired without VPN. Optional, open to Nasuni Management Console for external management access direct or via NAT. Optionally, open to `av-updates.api.nasuni.com` for AntiVirus updates.	At a minimum, open to `*.nasuni.com`, `*.amazonaws.com`, and `*.windows.net` ***Note**:* Firewalls or any other security devices or software that process, inspect, or log port 443 traffic from the Nasuni Filer can affect performance when the Nasuni Filer is communicating with the cloud. If you must use IP addresses (not recommended), see Appendix D, "Port 443 Outbound Details," on page 73 of the *Best Practices Guide*.
123	NTP (Network Time Protocol)	Connecting to Network Time Protocol (NTP) servers.	N/A	Optional, if connecting to external Network Time Protocol (NTP) servers.
161	SNMP (Simple Network Management Protocol)	Connecting to Simple Network Management Protocol (SNMP) services.	N/A	Optional, if using external Simple Network Management Protocol (SNMP) trap addresses.
25	SMTP (Simple Mail Transfer Protocol)	Simple Mail Transfer Protocol (SMTP) processing for outgoing email	N/A	Optional, if using external servers for email for Nasuni Filer messages.

Discussion

The Nasuni Filer must be able to talk to both Nasuni (to send alerts and metrics, download new versions, and so forth) and to the cloud (to reach cloud storage with Amazon S3 or Azure).

Because of the load-balancing nature of our systems, it is best not to perform this using IP. Instead, we suggest that you open HTTPS traffic (port 443) to *nasuni.com and *amazonaws.com. If you plan to deploy the Nasuni Management Console (NMC), also include *windows.net for HTTPS traffic.

While our IP list for *nasuni.com is limited to just a few machines, the distributed nature of Amazon S3 means that there are many IP addresses in multiple large blocks (see https://forums.aws.amazon.com/thread.jspa?messageID=82757), to the point that Amazon doesn't recommend or offer IP address recommendations.

***Tip**:* Certain firewall manufacturers offer Nasuni application types for their whitelists or allow lists, and these should be enabled.

Required Port

The Nasuni Filer has 1 port that is required to be open on your network (outbound only):

443 – HTTPS: This port is used when transferring data from the Nasuni Filer to the cloud storage provider. At a minimum, open to *.nasuni.com, *.amazonaws.com, and *.windows.net.

***Note**:* Firewalls that process and log port 443 traffic from the Nasuni Filer can affect performance when the Nasuni Filer is communicating with the cloud.

***Note**:* Web security can affect performance when the Nasuni Filer is communicating with the cloud.

Optional Ports

The Nasuni Filer has several ports that are optional to be open on your network:

123 – NTP (Network Time Protocol): You can configure the Nasuni Filer to use your local NTP server. However, if you use the default settings, you must open port 123 on your network to use the default NTP servers. These servers are from pool.ntp.org.

25 – SMTP: You can configure the Nasuni Filer to use your local SMTP server. However, if you use the default settings, you must open port 25 on your network. This is so the Nasuni Filer can send you alerts via SMTP if you configure it to do so.

161 – SNMP: You can configure the Nasuni Filer to use SNMP. However, if you use the default settings, you must open port 161 on your network.

8443 – Optional, for external management access direct or via NAT.

Ports for internal network firewalls

In addition to the preceding, for environments with internal network firewalls and segmentation, the following inbound port configurations between users and the Nasuni Filer might be necessary for the respective protocol to function:

Port number	Associated protocols	Used for	Inbound (to Nasuni Filer)
222	SSH	Support	Close this port. If Nasuni Customer Support requests you to open this port, open this port temporarily to all clients/ranges.
443	TCP	Web Access, Mobile Access (iOS and Android devices), Desktop Sync, AntiVirus updates.	If these features are in use, Nasuni recommends opening this port to all clients/ranges. Note that these features must be enabled on the Nasuni Filer.
8443	TCP	To administer the Nasuni Filer and Nasuni Management Console.	Open to clients that need to use the Nasuni administration interface.
88, 139, and 445	TCP	SMB/CIFS and Active Directory	Open to clients that need to use SMB/CIFS.
111, 662, 875, 892, 2049, and 32803	TCP and UDP	NFS	Open to clients that need to use NFS.
3260	TCP	iSCSI	Open to clients that need to use iSCSI.
161	UDP	SNMP	Open to clients that need to use SNMP.
88	UDP	Kerberos	Open to clients that need to use Kerberos.
53	TCP and UDP	DNS	Open to clients that need to use DNS.

Connecting Nasuni Filers to the Internet at large

Nasuni recommends the following:

- Close all ports that are not actively needed.
- Restrict access to only the client machines that are needed.
- Use only HTTPS protocol. For example, do not use SMB.

Contacting Technical Support

Telephone: 1-888-6NASUNI (888-662-7864)
Email: support@nasuni.com
Technical Support is available 24/7/365 for full production clients.