

Firewall Rules

Firewall Rules

Overview

This document will help you understand the mandatory and optional rules that you need to configure on your firewall for a successful Nile Access Service deployment.

Nile NSB Subnet	Port 443, 53, 123	Required so that the Nile Gateways can talk to the Nile Cloud
Nile Sensor IP Subnet	Port 443, 53, 123	Required so that Nile Sensor to talk to cloud
Your Employee, Guest, IoT IP Subnets, etc	Port 443, 53, 67 and 1812	All your clients/endpoint subnets to talk to Internet, DNS server, DHCP server and RADIUS server
Nile Cloud URL	ne-u1.nile-global.cloud	Nile Cloud URL
IP Address	44.238.235.251 52.12.186.175 100.20.40.199 52.13.104.212	Nile Cloud IP Addresses
DHCP	Port 67 IP Address – Your DHCP server IP address	Allow Inbound and Outbound For communication
RADIUS	Port 1812 or another IP Address – Your RADIUS server IP	between your clients (Employees, Guest, IoT Subnets) and your DHCP/RADIUS server, make sure you allow all

		the client subnets to reach both the server
DNS	UDP 53 8.8.8.8 8.8.4.4	Nile Devices use Google DNS by default. If you have your own DNS server, please allow that and let the Nile Team know so that we can set it up while activating the Nile service
Various sites	Google, Zoom, Amazon, Facebook, Office, Dropbox, Youtube, Salesforce, Webex	Nile pings various services for collecting application metrics

Optional

- As part of our zero-trust security model, Nile devices by default doesn't allow east-west traffic between users which means the traffic between one client to another client on the same or different subnet is not allowed. It forwards all the traffic to the upstream firewall/router. If you want to allow east-west traffic which means communication between 2 clients on the same subnet or different subnets, you will have to set up those rules on your firewall/router which is upstream of the Nile gateways.