5. Connectivity requirements (for local IT)

The IXrouter uses outgoing ports to establish a secure connection to our IXON Cloud. This means there is no need to open any incoming ports in your firewall.

5.1 Overview

Below is an overview of the outgoing ports and protocols that the IXrouter utilizes.

Direction	Port	Transport	Application
Outbound	443	TCP	HTTPS, MQTT (TLS) OpenVPN(1)
Outbound	1194(2)	UDP	OpenVPN
Outbound	8443(3)	TCP	HTTPS
Outbound	53(4)	TCP & UDP	DNS
Outbound	(no port)(5)	ICMP (Echo request)	-

(1) The very first package may be considered unencrypted as the OpenVPN handshake takes place prior to the TLS handshake. For this reason an exception may be required on firewall rules that block non-SSL traffic over SSL-ports.

(2) Only used when VPN connection type is set to UDP.

(3) Only used when stealth mode is activated for connectivity via a censored internet connection (i.e. when located in China).

(4) DNS requests are often handled by local DNS servers. In those cases the listed DNS port can be ignored.

(5) Only used when failover is configured.

5.2 Servers and DNS requests

The IXrouter connects to different IXON servers: REST API, MQTT, and OpenVPN servers, which include the following domains: .ixon.cloud; .ixon.net; .ayayot.com (phonetic IIoT).
Doing a DNS lookup (nslookup) at the following domain name always returns an up-to-date IP list of all current IXON servers: whitelist.ixon.cloud