List of domains and protocols to allow through a firewall.

These are the flows that need to be allowed through firewalls for the product to fully function. We do not recommend allowing by IP address since those may change from time to time and without previous notice, however if you would like to do it by IP address, we strongly encourage you to regularly monitor the IP Addresses used by the specified domains.

Best practices and the strong recommendation to allow the container to fully function is to allow everything in and out of the container locally on the host it is running, and when possible, to allow open communication in and out of the container and host to the network and to the internet. If this is not possible then follow the table below to grant unrestricted access as described.

The following table shows the main service, domains related to it and the protocol and port identified.

Service	Domain	Protocol/Port
Discovery	local network in and out	allow_all
Scanning	local network in and out	allow_all
Google	*.google.com *.googleusercontent.com *.gcr.io *.appspot.com *.cloudfunctions.net *.firebaseapp.com *.googleapis.com *.datastore.googleapis.com *.storage.googleapis.com	HTTPS (TCP 443)
Github	*.github.com *.github.dev *. github.io *.githubassets.com *.githubusercontent.com	HTTPS (TCP 443) Git (TCP 9418)

	*.blob.core.windows.net *.actions.githubusercontent.com	
Docker Hub	*.docker.com *. docker.io *.cloudflare.docker.com cdn.auth0.com	HTTPS (TCP 443)
Remote.it	*.rt3.io *. remote.it *. remot3.it *.prod.yoics.org	443**, 5959-5970
PublicIP	ident.me ifconfig.me/ip ipecho.net/plain api.seeip.org/geoip api.seeip.org/jsonip	HTTPS (TCP 443)
IOT KORE	*.korewireless.com iotcore.omnicore.korewireless.com	MQTT (TCP 1883) MQTTS (TCP 8883)
NTP	129.6.15.28 pool.ntp.org time.nist.gov 194.35.252.5	NTP (UDP 123) Above 1023
DNS	8.8.8.8	DNS (TCP 53) DNS (UDP 53)