https://cloudblue.com

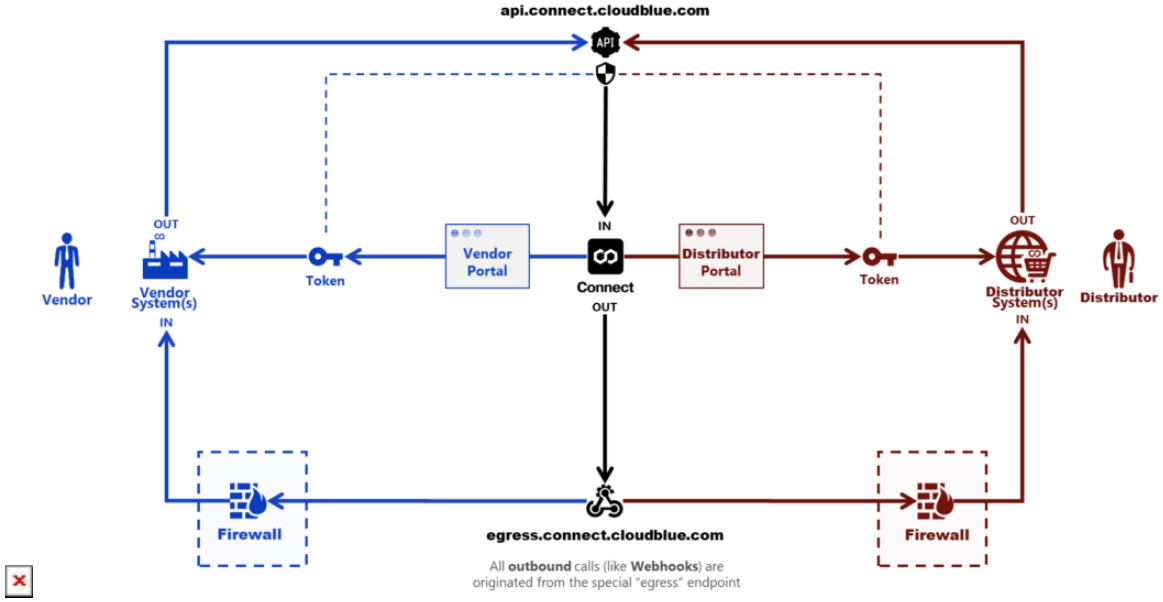
Firewall Configuration

Auto-generated at October 16, 2025

In certain scenarios, like webhooks, CloudBlue Connect initiates HTTP(s) connectivity to the endpoints, specified by Vendors and Providers.

We generally **do not recommend setting up additional firewall rules** for such inbound connections as they can significantly complicate operations and upgrade procedures to our partners.

However, all outbound connections in Connect are initiated from the special endpoint (**egress.connect.cloudblue.com**), so it is possible for our partners to set up inbound firewall rules as schematically illustrated in the following diagram:



Thus, in case of the firewall configuration being a mandatory requirement for the inbound network connectivity of our partners, you can use that special domain **egress.connect.cloudblue.com** to dynamically retrieve IP address(es) for the inbound firewall rules from **A records** of that domain.

A records of the domain could be retrieved, for example, using the ‘dig‘ shell command:

```
$ dig egress.connect.cloudblue.com
```

We strongly recommend you to configure your firewall rules using dynamic DNS retrieval instead of the static IP address since they **may change without notice**. We do NOT guarantee IP addresses of Connect will remain static and won’t change without notice.

In case your firewall does not support domain names to create rules, the list of IPs at the moment of writing this article are:

```
104.43.244.65
```

Important: The above mentioned shared IP addresses are subject to **change without notice.** We will not accept responsibility for any operational issues you may incur as a result of the static configuration of the firewall rules in your systems.