

Managing outbound traffic from your application

Downloaded from Epic Games Confluence

Date: 2025-07-12 04:08:08

Original URL: <https://confluence-epicgames.atlassian.net/wiki/spaces/CDE/pages/81068464>

Document Level Classification

[200](#)

- [Introduction](#)
- [Outbound traffic to the internet](#)
- [Outbound traffic to Amazon S3 or DynamoDB](#)
- [Outbound traffic to AWS Service Endpoints](#)
- [Outbound connections to other applications in your Substrate cluster](#)
- [Outbound traffic to Infrastructure and Developer Applications](#)
- [Outbound traffic to applications in other Substrate clusters](#)
- [Outbound traffic to OldProd](#)

Introduction

For applications that are making outbound network requests, the network path and authorization depends on the destination. Review the common types of outbound traffic below.

The [security group](#) attached to the underlying *Nodes* for your *Pod* allow all outbound traffic on all ports using any protocol - there is no additional

authorization required on the *source side* for an application to connect to external resources.

Outbound traffic to the internet

Applications running in a Substrate cluster will typically be placed in *NAT* subnets. This provides a network path through [NAT](#) and [Internet](#) gateways for applications to connect to external (internet) resources. No additional configurations are needed for your application to connect to the internet. However, traffic traversing the NAT gateway is subject to the [rules and characteristics of NAT gateways](#).

Outbound traffic to Amazon S3 or DynamoDB

Requests to Amazon S3 or DynamoDB APIs will resolve and route to [Gateway Endpoints](#) deployed to the Amazon VPC (traffic does not route via the internet). No additional configurations are needed for your application to connect to Amazon S3 or DynamoDB.

Outbound traffic to AWS Service Endpoints

Requests to AWS Service Endpoints that are not Amazon S3 or DynamoDB will resolve to the [public regional endpoints](#) and route via the internet. When using AWS SDKs, it is recommended to use the `in-region` [configuration defaults](#).

Outbound connections to other applications in your Substrate cluster

Requests to other applications in the same Substrate cluster may either stay internal to the cluster or route via the internet depending on configurations options. See [Managing traffic between applications in your Substrate cluster](#) for more details.

Outbound traffic to Infrastructure and Developer Applications

Substrate clusters are, by default, configured to connect to GitHub Enterprise, Artifactory, HashiCorp Vault, and other applications that are used to manage deployments to your Substrate cluster.

Outbound traffic to applications in other Substrate clusters

Requests to applications in other Substrate clusters, by default, is not routed unless both the source and destination account VPC's are on the [Service Network](#). If your account is not connected to the Service Network then a request must be made to provision the account for a Service Network attachment by reaching out to [#cloud-network-ext](#).on slack. If the source and destination account VPC's do have a Service Network attachment, you will need to request the service owner of the other application to [allow traffic from your Substrate cluster](#).

Outbound traffic to OldProd

HTTP/S Connections from your Substrate cluster to service endpoints in OldProd is supported and routed using the [Service Network](#). If your account is not connected to the Service Network then a request must be made to provision the account for a Service Network attachment by reaching out to [#cloud-network-ext](#).on slack

Page Information:

Page ID: 81068464

Space: Cloud Developer Platform

Downloaded: 2025-07-12 04:08:08