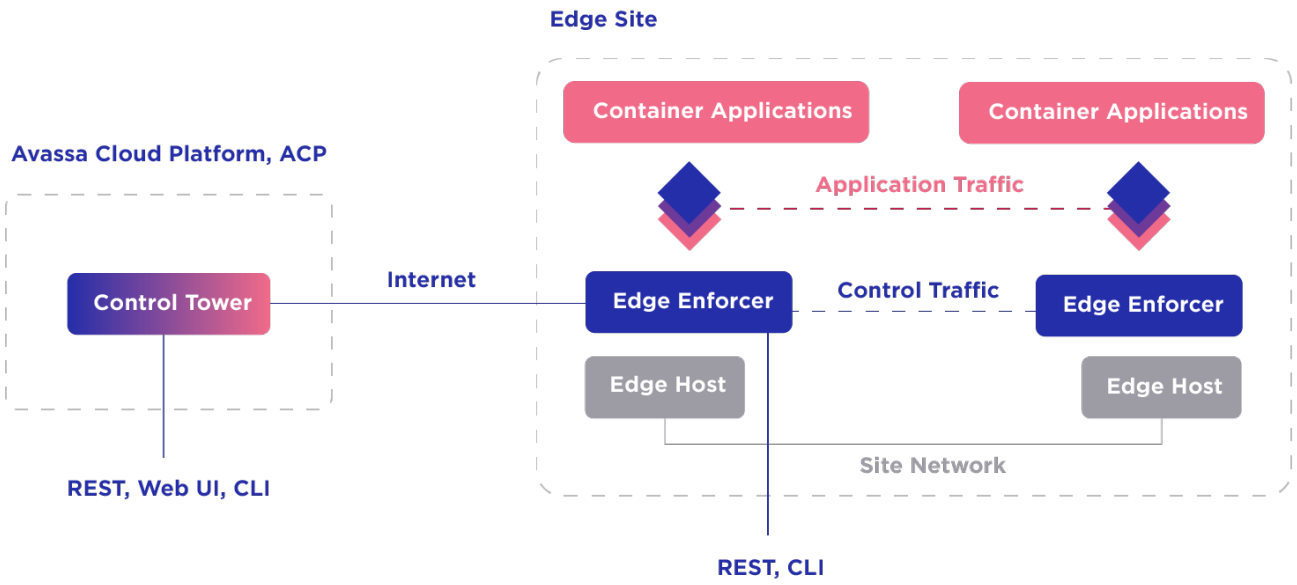
Avassa
Security Overview

This document aims to give an overview of the security aspects of the Avassa Edge Platform.

Avassa Overview

The main components of Avassa are:



- Avassa Cloud Platform (ACP); is a SaaS solution where customers register and can create Control Tower instances.

- Control Tower: the central orchestrator for all edge sites. It runs in the cloud by default; customers can have several instances within ACP. It can also be installed on-premise.

- Edge Enforcer: a container installed on each edge host, Edge Enforcers can optionally form an edge site cluster. It manages the customer container workloads on the sites and is orchestrated by the Control Tower.

- The edge sites and the central components provide a secure REST API. A **Web UI** (only Control Tower) and a **Command Line Interface** are provided that uses the **REST API** towards Avassa.

From security aspects, the following observations are essential with the above as background:

1. ACP and Control Tower needs to be secured in the cloud.
2. The Control Tower communicates over the internet to the edge sites.
3. The Edge Enforcer needs to provide local security on the edge sites. Edge sites might not have perimeter security like cloud solutions do.
4. The Edge site needs to provide IP connectivity between Edge hosts. This network cannot be assumed to be secured.
5. Application networks need to be isolated
6. Avassa has built-in support for multi-tenancy. Users are created as belonging to a tenant. All tenants need to be totally isolated.

Authentication, Access Control, and Auditing

Users can be managed locally in Control Tower or externally using OAuth2. MFA can be enabled for user logins, either by users themselves or enforced by administrators. Centrally managed access policies control which data and operations are allowed for a user. By default, the system blocks calls not matched by any policy. While users and policies are managed centrally, they are synchronized to each local edge site. This means that AAA functions are securely performed even when the edge site loses connection to the Control Tower.

All calls to the APIs are audit-logged. The site audit log is kept both locally at the site and propagated to the central Control Tower.

Network security

The communication between the Edge Enforcer and the Control Tower is always encrypted over TLS. All traffic is initiated from the site (well-known HTTPS port); no ports need to be opened from the outside. Edge hosts need to identify themselves to be accepted by the Control Tower, using a shared secret, normally the host id. Client certificates can also be required for an extra level of security.

The network at the edge site is provided outside the control of Avassa.
We can not assume that it is safe, therefore, all application traffic is encrypted using WireGuard. Application traffic is automatically isolated and micro-segmented using VXLAN. The Avassa system automatically configures a firewall around the applications which by default locks down as much as possible.
A minimum set of ports and protocols are whitelisted.

For example; a container application is not by default reachable on the site. Explicit ingress networks can be configured to allow access to an application.

Avassa control traffic between hosts in an edge site is always encrypted using TLS and mutually authenticated using client certificates.

Edge security

Each edge site/host is sealed with unique keys. Without that key the site is locked down, secret data is encrypted and can not be accessed. If a host reboots it will come up in a sealed state; at this point, it needs to reach back to the Control Tower or a peer host on the site and identify itself to get access to decryption keys.

If an administrator considers a site to be jeopardized, he can block the site; at this point, the site will drop its crypto keys and will not be able to access any sensitive information.

After blocking a site, the Control Tower automatically rotates keys across all edge sites.

Sensitive data is encrypted using unique keys per site and per tenant. This means that if one site is compromised, all other sites are still secure.

Tenants are given different access to edge sites, ranging from which sites they can “see” down to fine-grained resource limits.

Data security for applications

Edge applications usually need to manage sensitive data per edge site. Avassa supports a central secrets manager. You can define secrets with associated fine-grained distribution policies. For example: require a secret to “follow” which sites a specific application is provisioned to. In this way, you can ensure that secrets only live on sites where they are needed. They are, of course, distributed and stored encrypted. And maybe even more critical, secrets are automatically cleaned up when an application is decommissioned from a site. Secrets can also only be distributed to sites to which a tenant has access.

Communication between nodes at an edge site is secured using mutual TLS. A compromised node can be isolated and will not gain access to the secret data.

The secrets manager can also generate and renew custom application certificates.

ACP Security

Authentication to ACP is handled through Auth0. Currently, each organization has a single administrator that can create and delete Control Tower instances (environments).

Further, the Control Towers in ACP are protected by load balancers, only allowing control traffic from the edge sites, no direct external access is allowed.

Each Control Tower runs on a dedicated VPC with no traffic allowed between Control Tower instances.

READ MORE

Infrastructure networking:
https://docs.avassa.io/fundamentals/infrastructure- networking

Application networking:
https://docs.avassa.io/fundamentals/application-networking

Secrets manager:
https://docs.avassa.io/fundamentals/strongbox

Edge host requirements:
https://docs.avassa.io/how-to/sizing

To learn more about the Avassa platform can help your business, visit our website avassa.io or get in touch.