Overview

https://campus.barracuda.com/doc/93201218/

CloudGen Access brings Zero Trust/BeyondCorp Security to your endpoint. In short, with CloudGen Access, you can implement secure access to enterprise resources, whether they are on-premises or in the cloud, with a quick and easy configuration process.

CloudGen Access has three main components: an agent (CloudGen Access App), a proxy (CloudGen Access Proxy), and an administration console (CloudGen Access Enterprise Console). It is very simple to start using CloudGen Access: just register a proxy and invite your employees to install the CloudGen Access App. Check our Getting Started article for more details.

About Zero Trust

The days of the VPN are gone. It is no longer feasible to establish a secure network perimeter with a hybrid setup with cloud resources and the myriad of devices that need to access company resources from anywhere. One single breach on a VPN setup can be catastrophic depending on the network setup and configuration.

Zero Trust builds upon the assertion that the network is assumed to be hostile. As a result, network locality is not sufficient for establishing trust, and every flow must be authenticated and authorized in a dynamic fashion. This creates an effective separation between the *control plane* – the supporting system that implements the flow authentication and authorization according to the defined policies – and the *data plane*.

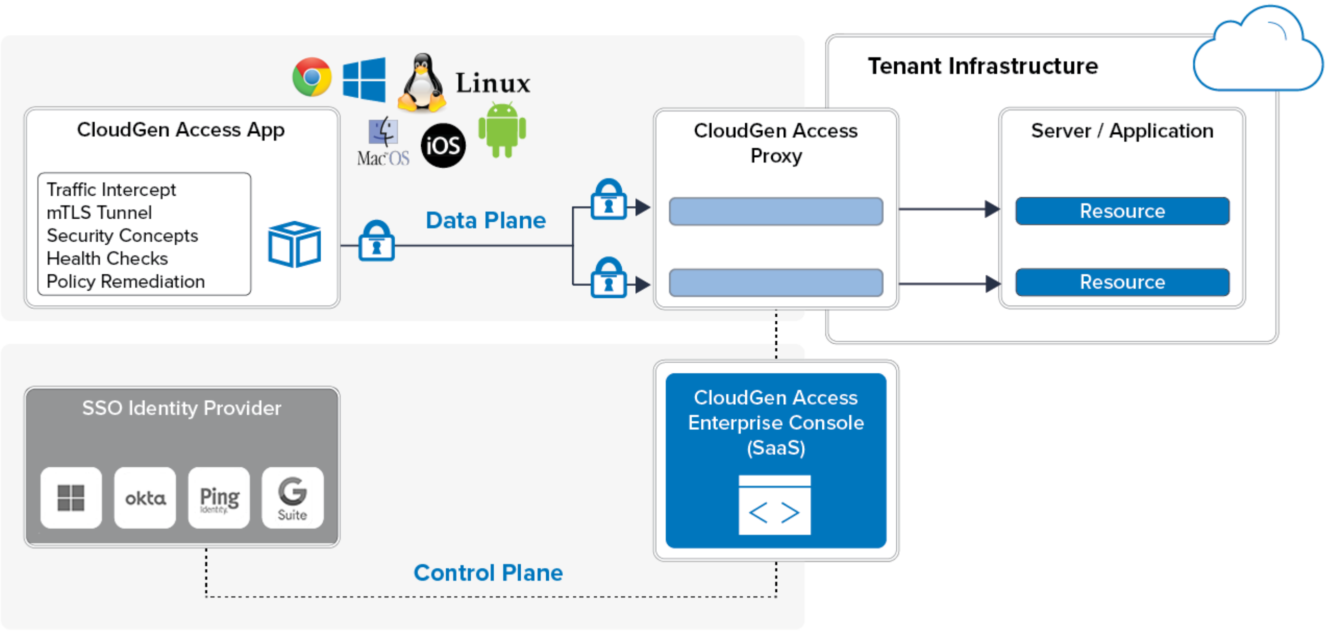
To learn more about Zero Trust, see Zero Trust Networks: Building Secure Systems in Untrusted Networks and the BeyondCorp paper by Google.

> Inbound connections to the CloudGen Access proxy must not be SSL/TLS intercepted; i.e., connections to the proxy should be exempted from any SSL interception firewall.

Architecture Overview

As mentioned, the CloudGen Access architecture relies on three main components: an agent (CloudGen Access App), a proxy (CloudGen Access Proxy), and an administration console (CloudGen Access Enterprise Console). The CloudGen Access agent operates at the network layer. When a device starts a connection to a protected resource, the CloudGen Access agent intercepts it and opens an mTLS connection with the CloudGen Access Proxy, also sending the device and user attributes to the CloudGen Access Enterprise console, which then evaluates the policy, checks the attributes, and allows or denies the connection to the resource. Admins can configure policies on the CloudGen Access Enterprise Console UI.

We also provide an API for the CloudGen Access Enterprise Console functionality, as well as a thin wrapper around it as a command line utility - CloudGen Access CLI.



Use Cases

With CloudGen Access, you can do the following:

- Immediately replace your VPN(s)
- Implement multi-cloud access
- Enable and disable access, on a per-user or per-device level
- Implement policies to protect resources according to criticality level
- Get visibility on traffic flows to resources for auditing purposes

Next Steps

To start using CloudGen Access, see Getting Started.

Figures