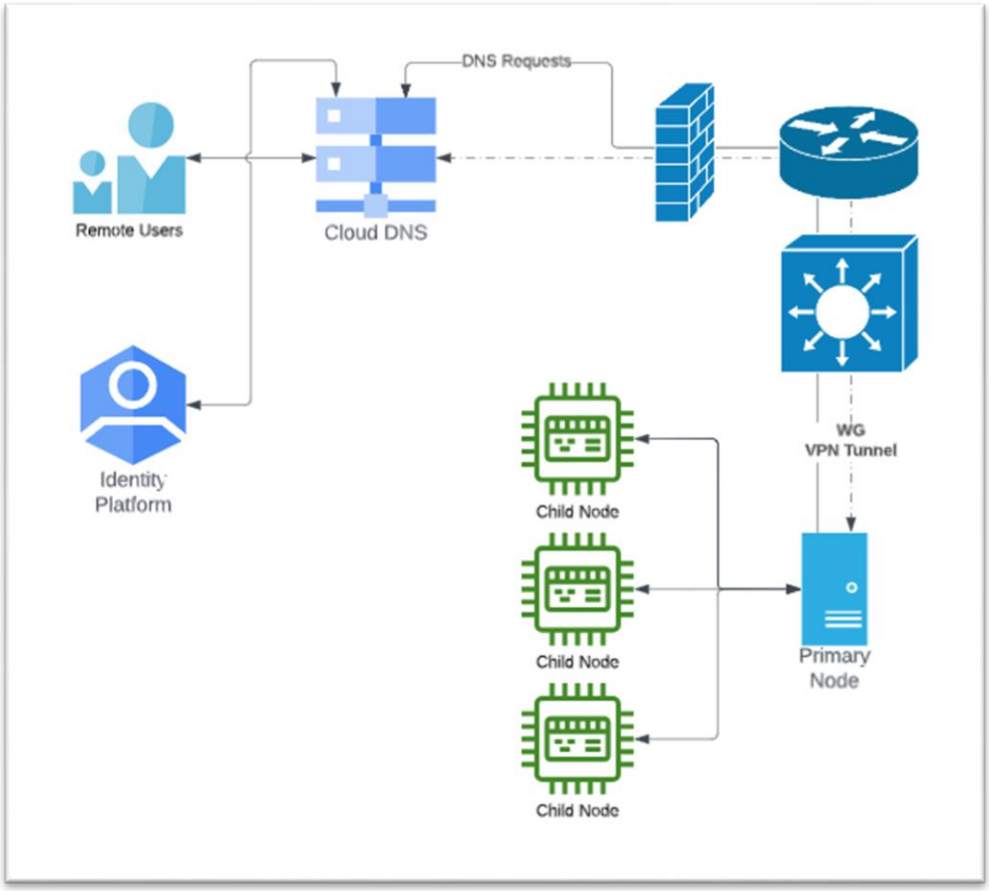
Halo Connected Architecture

Sentinel Link

Summary

Sentinel Link is a WireGuard (WG) based Virtual Private Network (VPN) solution that creates an overlay network allowing for secure communication. This is facilitated by a local service running on the node that creates the tunnel connection to our Domain Name System (DNS) provider. Once connected to the DNS provider, services can be accessed by authorized users from the internet through this tunnel. Exposed services require authentication through an Identity Provider (IdP/IDP). Once authenticated the user is presented with only the services, they have authorized access to.



HIGH LEVEL

The Halo Appliance is a standard Linux host running on any x86 processor. This appliance has been hardened to prevent unauthorized access. Additionally, all installed services utilize containerization, when possible, to further reduce the risk of a malicious actor gaining access to any critical system, service, or secret.

Key Features

- DNS Monitoring
- Hybrid Access
- Zero Trust
- Cloud Access Security Broker (CASB)

DNS Monitoring

The Primary node and all child nodes are configured to only use our Enterprise DNS server. This DNS server applies Access Control Rules and logging to all DNS resolutions. DNS resolutions go through the local network infrastructure allowing local admins to monitor this network traffic.

Hybrid Access

All services can be accessed locally through the Primary node without data leaving the local network. Access to these services is accomplished either by directly connecting by using either the assigned IP address or a configured local DNS record.

The Sentinel Link tunnel allows remote access by connecting the primary node to a publicly accessible URL. To access any service associated URL the user is presented with an authentication challenge. The identity used to authenticate is maintained either by Halo Connected Architecture or the customer. This allows Sentinel Link to use many different Identity providers without placing onerous requirements on the customer.

Zero Trust

Industrial Control Systems (ICS) must be properly secured and monitored. For this reason, Sentinel Link requires authentication before any external access is allowed. These authentications are tied to an Identity provider such as Microsoft, Google, Github, Okta, and others. This allows each customer to scope remote access and monitor these authentications using their preexisting processes.

Cloud Access Security Broker (CASB)

Together, these distinctive features effectively create a Cloud Access Security Broker (CASB). This allows granular access to authorized services deployed in a hybrid manner; the user chooses how and where they want to run services.

Remote Support

When remote support is required the remote support technician will authenticate through the Halo identity provider. Once authenticated all administrative changes either happen using an internal process or directly on the device using SSH. This allows for session monitoring and recording; no actions will be taken that are not monitored ensuring all changes are auditable.