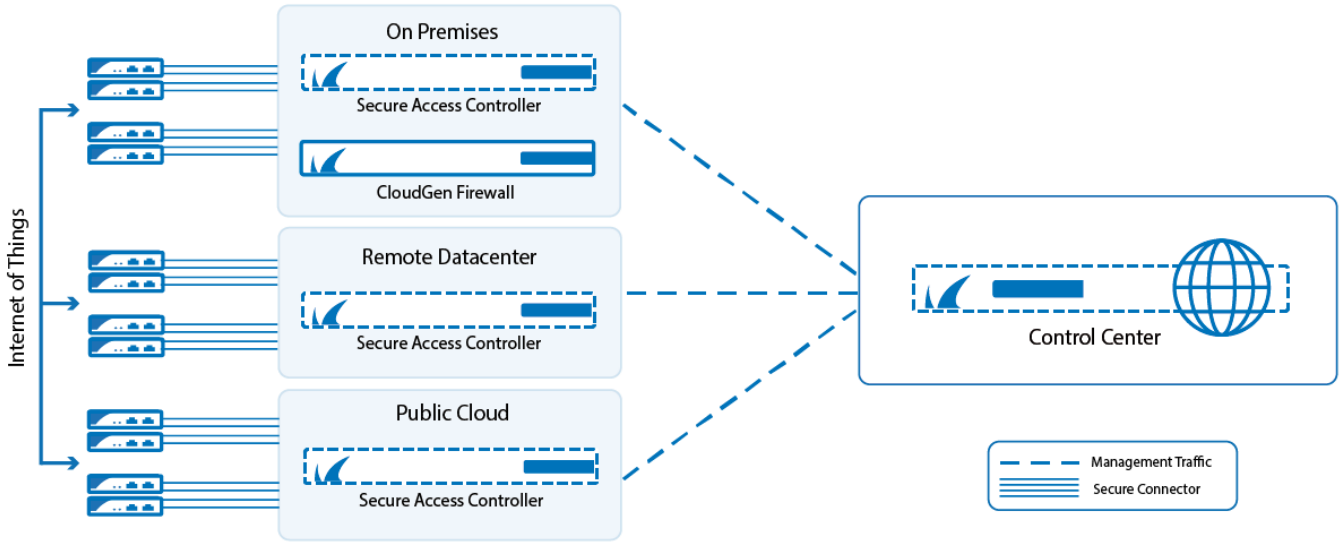
Barracuda Secure Connector

https://campus.barracuda.com/doc/79462649/

The Barracuda Secure Connector offers large-scale remote access capabilities. It enables the ever-growing number of IoT devices and micro-networks to securely connect to the central or distributed corporate datacenter. In such a scenario, a large number of small Secure Connector appliances connect via TINA VPN to their regional Secure Access Controller. The Access Controller acts as the VPN endpoint for the Secure Connectors and forwards the management traffic to the Control Center. Corporate policies such as Application Control, URL Filtering, Virus Scanning, or ATP are handled either directly on the Access Controller or forwarded to the border firewall. The configuration and lifecycle management for all Secure Connectors and their Access Controllers are handled by one Control Center. The Control Center can manage multiple Secure Access Controllers, allowing you to scale up the network at will.



Secure Access Controller and Integration with the Control Center

Secure Connector Devices on the Control Center

The Control Center is a central management appliance for Secure Connector and CloudGen devices. The Control Center provides a central template-driven configuration management interface, firmware update management, and status information for all managed devices. CloudGen Firewalls and Secure Connector devices are managed on one Control Center. But unlike the firewalls, the Secure Connector configuration is not configured in a tree structure; instead, configuration is handled through a single interface: the Secure Connector Editor. The Secure Connector Editor allows you to create configuration templates and link them to individual appliances. Changes to the templates are immediately pushed out to the Secure Connector. The administrator decides which configuration options are device-specific. These settings are then configured directly on the device. Although it is

possible to change the configuration of an individual device via the web interface, the Control Center configuration overrides the changes made when the web interface configuration lock is released.

The data and management networks for the Secure Connectors are also defined via the Control Center. Data networks (the networks behind a Secure Connector) are used for traffic to and from the devices behind the Secure Connector and can be routed to and from the client's infrastructure via the Access Controller. The management network is the the network used for management traffic between the Secure Connectors and the Control Center. Over the management network all configuration, management, and container traffic is sent. The management network ensures unique VIPs per Secure Connector on Control Center-level, the data networks only have to be unique per Access Controller. This enables the usage of similar or overlapping data networks on different Access Controllers.

For more information, see Secure Access Controller and Control Center Deployment and How to Create and Apply Secure Connector Templates.

Secure Access Controller

The Access Controller is deployed via virtual CloudGen Firewall images available for on-premise deployments or in the public cloud. It handles incoming Secure Connector VPN tunnels. Management traffic is automatically forwarded to the Control Center, and user traffic is processed either directly. If the Access Controller is deployed remotely in a VPN tunnel is created between the Access Controller and the Control Center that is also used for the Secure Connector managment traffic. If necessary, Access Controller can be deployed in a high availability cluster. In addition to the Access Controller license, you must also assign a Secure Connector Energize Update pool license. The number of instances in the pool license determines the number of Secure Connectors allowed to connect. The size of the Secure Connector pool license may not exceed the maximum number of VPN connections for the Access Controller model. The following models are available:

- **Barracuda CloudGen Firewall VACC 400** – 2 CPU cores, up to 500 VPN connections
- **Barracuda CloudGen Firewall VACC 610** – 4 CPU cores, up to 1200 VPN connections
- **Barracuda CloudGen Firewall VACC 820** – 8 CPU cores, up to 2500 VPN connections

For more information, see Secure Access Controller and Control Center Deployment.

Secure Connector

The Secure Connector is a small hardware appliance optimized to efficiently connect remote devices and micro-networks to the corporate datacenter via TINA VPN tunnel. The configuration is centrally managed by the Control Center, but can be overridden via the web Interface on the device. When a Secure Connector is deployed, a management and a data network is automatically selected and permanently assigned to the device.

For more information, see Secure Access Controller and Control Center Deployment and How to Create and Apply Secure Connector Templates.

Secure Connector WAN Connections

The Secure Connector supports the following WAN connection types:

- DHCP client
- Static IP
- Wi-Fi client
- WWAN Modem

For more information, see Secure Connector WAN Connections.

Networking

The Secure Connector network can be configured in several ways:

- **Manual** – The network must be entered manually. Devices behind the Secure Connector require a static IP address.
- **Manual Mapped** – The network is entered manually. Devices behind the Secure Connector require a static IP address. The static network is mapped to a automatically assigned subnet out of the Secure Connector data network.
- **DHCP Server** – The network is entered manually. Devices behind the Secure Connector receive an IP address from the DHCP server on the Secure Connector.
- **DHCP Server Mapped** – The network is entered manually. Devices behind the Secure Connector receive an IP address from the DHCP server on the Secure Connector. The network is mapped to an automatically assigned subnet out of the Secure Connector data network.
- **Automatic** – The network assigned to the Secure Connector is assigned automatically by the Control Center.

Mapped networks must be the same size as the network assigned to the Secure Connector. The managment network offers access The Wi-Fi access point can use a separate network from the Secure Connector network, accessing the other zones via source NAT firewall rules.

For more information, see Secure Connector Networking.

Secure Connector Firewall

The Secure Connector appliances use a different Firewall service from the CloudGen Firewalls. The Firewall allows you to create rules defining access, source, and destination NAT based on four network zones defined for the Secure Connector:

- LAN

- Wi-Fi
- WAN (including Wi-Fi client)
- VPN

For more information, see Secure Connector Firewall.

VPN Service

The Secure Connector device connects to the Access Controller and the Control Center via one site-to-site tunnel on port TCP or UDP 692. The VPN tunnel is authenticated via certificates or passphrase. The Secure Connector Firewall only allows the user to send LAN traffic through the VPN or to WAN. It is not possible to use an Internet breakout for the devices in the LAN or Wi-Fi.

For more information, see Secure Connector VPN.

Figures

1. s_series_architecture_1.png