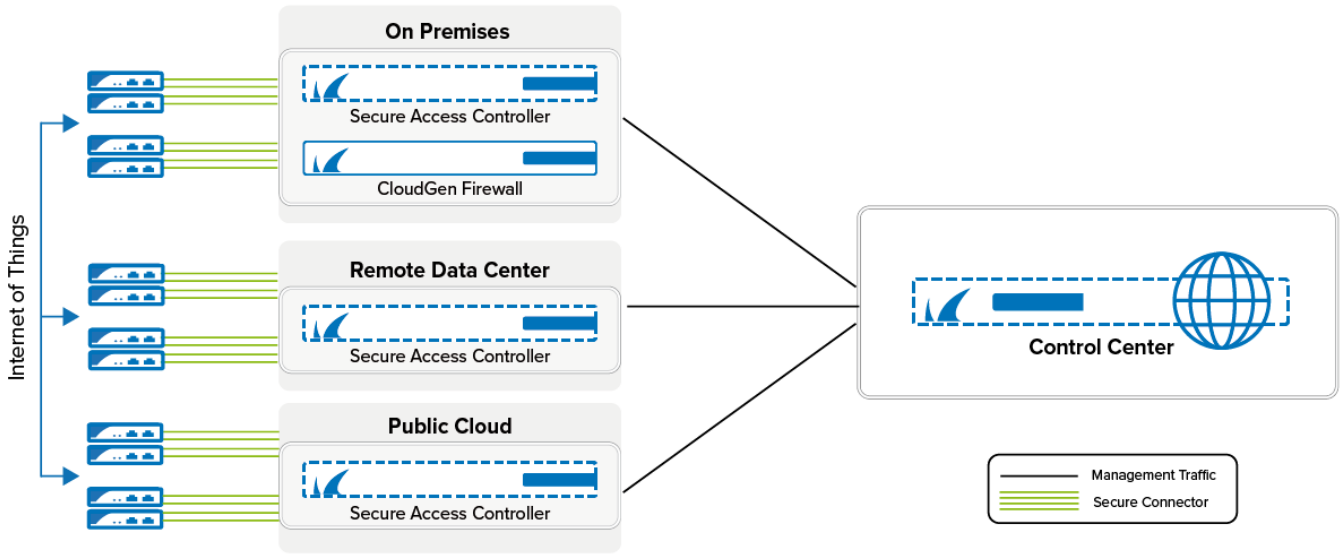
Barracuda Secure Connector

https://campus.barracuda.com/doc/91128292/

The Barracuda Secure Connector (SC) 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 data center. In such a scenario, a large number of small Secure Connector appliances connect via TINA VPN to their regional Secure Access Controller (SAC). The Secure Access Controller acts as the VPN endpoint for the Secure Connectors and forwards the management traffic to the Control Center.

The Secure Access Controller acts as complete security instance for IPS, AV, and ATP scanning. Corporate policies such as Application Control, URL Filtering, Virus Scanning, or ATP are handled either directly on the Secure Access Controller or forwarded to the border firewall. The configuration and life-cycle management for all Secure Connectors and their Secure 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 Connector Integration with the Control Center

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

The Firewall Control Center, a central management appliance for Secure Connector and CloudGen

Firewall devices, provides a central template-driven configuration management interface, firmware update management, and status information for all managed devices. Secure Connector 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 SC appliances. Changes made to the templates are immediately pushed to the Secure Connector. Device-specific settings are 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.

Hardware Specifications

Hardware specifications and power options depend on the appliance. The following Secure Connector models are available:

- SC1 – Via external power supply (5V); via USB/USB OTG
- SC2 – Via external power supply (12V); via PoE

For more information, see Hardware Models.

Access Controller and Secure Connector Deployment

The Secure Access Controller is deployed via virtual CloudGen Firewall images available for on-premises deployments or in the public cloud. The Secure Access Controller handles incoming Secure Connector VPN tunnels. Management traffic is automatically forwarded to the Control Center, and user traffic is processed directly. If the Access Controller is deployed remotely, a VPN tunnel is created between the Access Controller and the Control Center that is also used for the Secure Connector management traffic. If necessary, Access Controllers can be deployed in a high availability cluster.

For more information, see Secure Connector Deployment.

Licensing

To deploy the Secure Connector and Access Controller, you must have an Access Controller license.

You must also assign a Secure Connector Energize Updates 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 Access Controller Licensing.

Secure Connector Web Interface

You can also manage a Secure Connector through the Secure Connector web interface. The Secure Connector web interface provides an overview of all configuration settings. Information is arranged in tabs that allow you to perform firmware updates and to monitor all activities of your Secure Connector. To access the web interface, open a browser, enter the management IP address of the appliance, and log in with your Secure Connector username and password.

For more information, see Secure Connector Web Interface.

Secure Connector Networks

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 an 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 is assigned automatically to the Secure Connector by the Control Center.

Mapped networks must be the same size as the network assigned to the Secure Connector. The management 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.

The Secure Connector supports the following WAN connection types:

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

For more information, see Secure Connector Networking.

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 a passphrase. The Secure Connector Firewall only allows the user to send LAN traffic through the VPN or to the 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.

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.

Figures