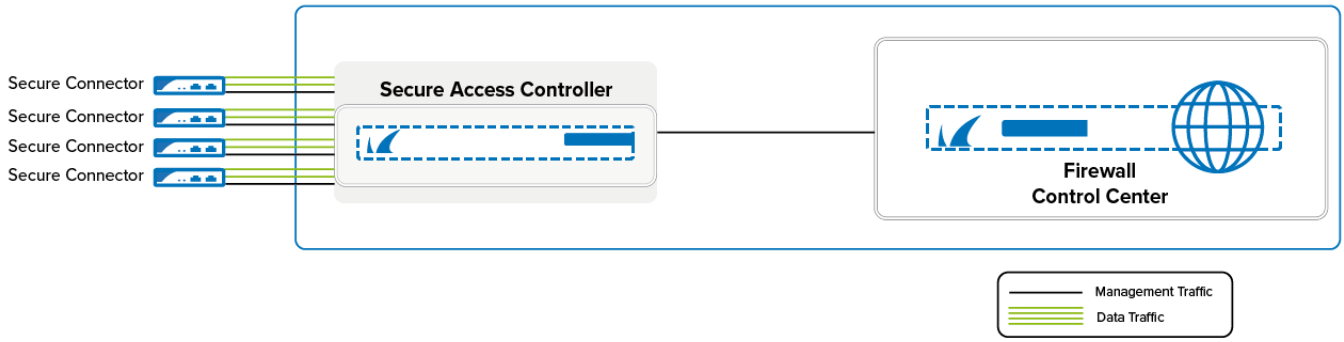
Secure Connector Deployment

https://campus.barracuda.com/doc/98210753/

Deploying a Barracuda Secure Connector (SC) network requires a Secure Access Controller, a Firewall Control Center, and the deployment of the individual Secure Connector devices. The Firewall Control Center manages the Access Controller and all Secure Connector devices. Each Secure Connector connects to an Access Controller, which is the VPN endpoint for the Secure Connectors and forwards management traffic to the Control Center. For more information, see Infrastructure Set-Up.



Secure Connector Deployment

Secure Connectors are configured and managed by the Firewall Control Center using the Secure Connector Editor. You can either create the configuration as a template and then assign it to the Secure Connector device, or directly configure the Secure Connector. With the data network selected in the SC configuration (either directly or in the template) the Access Controller settings (e.g., entry point, port, AC public key) and the management network settings are automatically configured.

For more information, see Secure Connector Setup and Configuration and Configure a Secure Connector via Templates.

Secure Connector Deployment via Configuration File

The configuration for the Secure Connectors is created and managed on the Control Center, optionally using templates to reduce the configuration overhead. The configuration file is then exported and copied to the Secure Connector via USB OTG or web interface. The Secure Connector then automatically connects to the Access Controller assigned to it. This allows the Secure Connector to connect in VPN operational mode and authenticate by the certificates included in the configuration file.

For more information, see Secure Connector Deployment via Configuration File.

Secure Connector Zero Touch Deployment

If the Firewall Control Center is configured to connect to the cloud-based Zero Touch Deployment (ZTD) service, Secure Connectors can be deployed using ZTD. The Secure Connector receives an IP address via DHCP, downloads the basic configuration from the ZTD service and receives the full configuration from the Control Center. The Secure Connector is associated with the Barracuda Cloud Control account.

For more information, see Zero Touch Deployment.

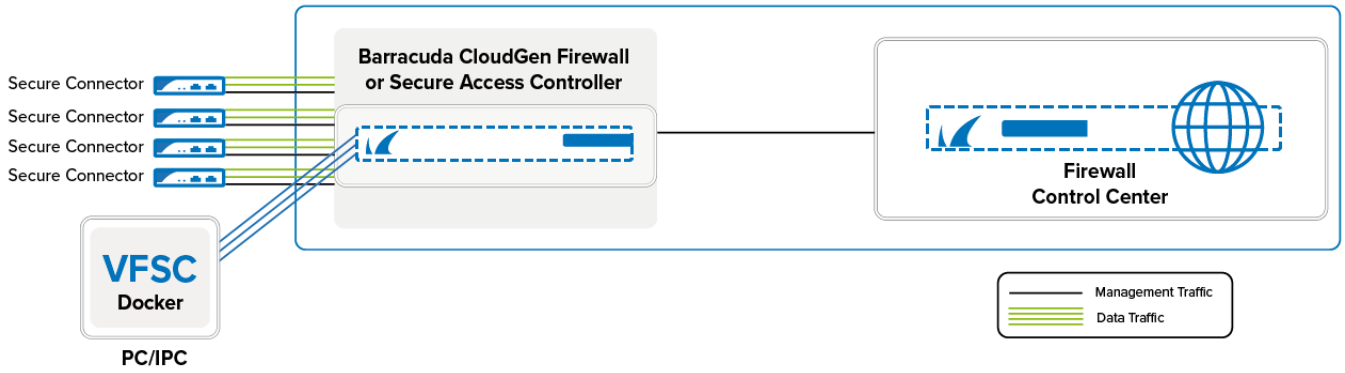
Secure Access Controller in the Public Cloud

The Access Controller can be deployed in the public cloud. This gives the devices behind the Secure Connectors direct access to your backend services that are running in the cloud. The Control Center can also be in the cloud or be located on-premises.

For more information, see Secure Access Controller in the Public Cloud.

Virtual Firewall Secure Connector (VFSC)

Barracuda Secure Connector is also available as a virtual appliance for Docker. The VFSC can be operated in a Docker container on a standard PC or IPC and thus offers a secure connection to your central systems. The Virtual Firewall Secure Connector can be deployed in the same way as the SC series via template-based configuration in the Firewall Control Center.



For more information, see Secure Connector Setup and Configuration and Configure a Secure Connector via Templates.

Figures

1. sc_data_management.png
2. vfsc_data_management.png