Barracuda Secure Connector Deployment

https://campus.barracuda.com/doc/79462666/

Deploying a Barracuda Secure Connector (SC) network requires at least one Secure Connector Access Cluster, a Firewall Control Center, and the deployment of the individual Secure Connector devices.

Secure Connector Access Cluster and Firewall Control Center Deployment

Each Secure Connector connecting to your network must be assigned to an Access Controller and a Firewall Control Center managing the Access Controllers and Secure Connectors. The Access Controller is the VPN endpoint for the Secure Connectors and forwards management traffic to the Control Center. If the Access Controller is not in the same network a dedicated site-to-site VPN tunnel can be created from the Access Controller to the Control Center.

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

Access Controller in the Public Cloud

The Access Controller can be deployed directly in the public cloud. This allows the devices behind the Secure Connectors direct access to your backend services running in the Cloud. The Control Center can also be in the cloud, or be located on-premises. In case the Control Center is not directly reachable, a VPN tunnel from the Access Controller to the Control Center can be configured to transmit managment traffic from the Access Controller and the Secure Connectors to the Control Center.

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

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 service, Secure Connectors can be deployed using Zero Touch Deployment (ZTD). The Secure Connector receives an IP address via DHCP, downloads the basic configuration from the Zero Touch Deployment 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.