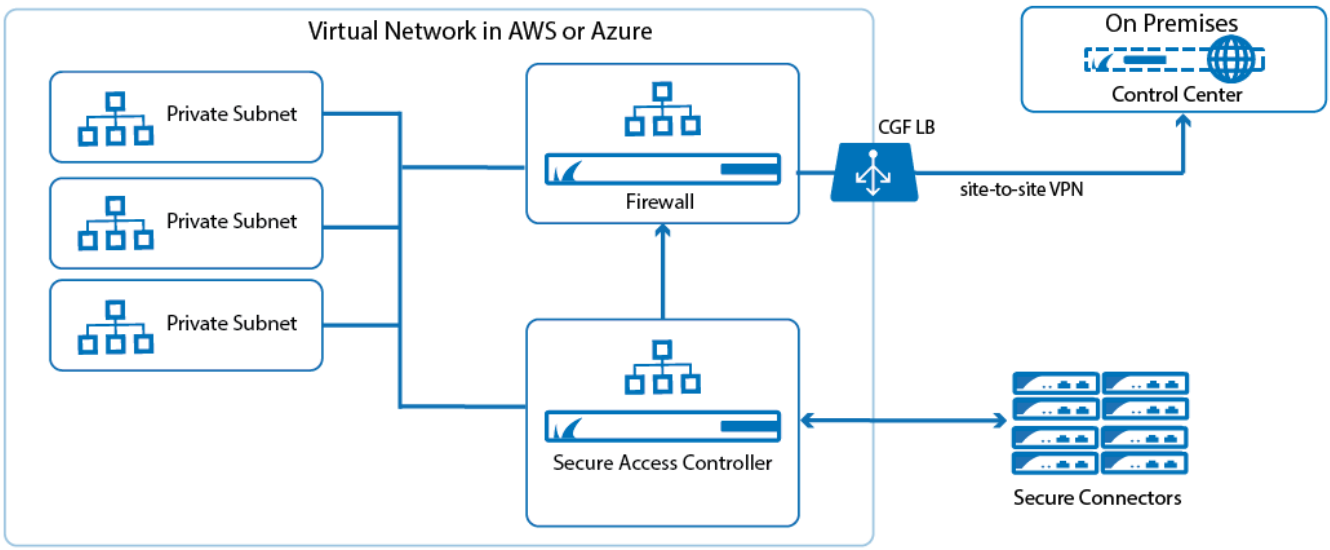
Secure Access Controller in the Public Cloud

https://campus.barracuda.com/doc/73718937/

The Secure Access Controller can be deployed in Azure and AWS if your Secure Connectors are geographically dispersed and/or your backend systems are hosted in Azure and/or AWS. The VACC connects your Secure Connectors with your cloud resources and allows you to monitor the traffic between the Secure Connector and the private subnets. If VPN connectivity is required, the Access Controller is used in combination with a CloudGen Firewall. You have two options for setting up the Secure Access Controller. The deployment steps are the same as the steps required for an on-premises Access Controller.

Access Controller and CloudGen Firewall in the Public Cloud, Control Center On-Premises

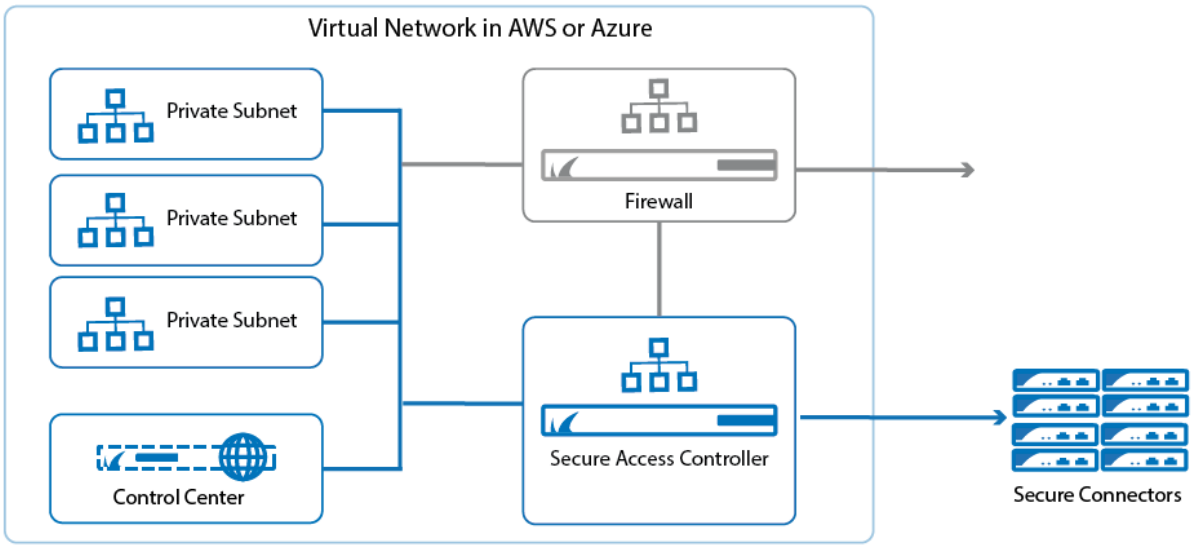
In this scenario, the Secure Connectors connect to the public IP address of the Access Controller. Management traffic from the Secure Connectors is sent either through a dedicated Access Controller to Control Center VPN Tunnel, or through the site-to-site VPN tunnel of an additional CloudGen Firewall is present that connects your on-premises datacenter to the cloud.



Access Controller, CloudGen Firewall, and Control Center in Azure or AWS

The client connects to the public IP address of the Access Controller. Traffic to the backend is routed either through the optional CloudGen Firewall, or directly to the backend subnets. Management traffic from the Secure Connectors is forwarded by the Access Controller directly to the Control Center in the

cloud. The Access Controller can act as the outgoing gateways for the backend services, or if site-to-site, or client-to-site VPN connectivity is required, the Access Controller is configured to work in tandem with an additional CloudGen Firewall acting as the border firewall.



Figures

1. Azure_SAC_Integration_CC_onprem.png
2. SAC_Integration_CC_Cloud.png