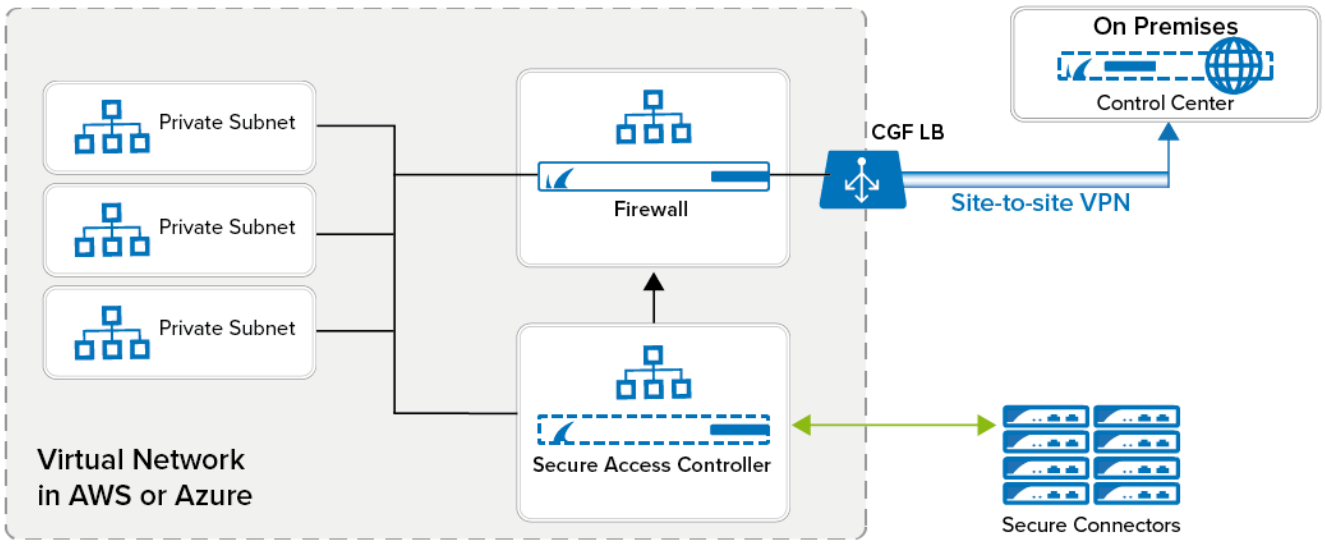
Secure Access Controller in the Public Cloud

https://campus.barracuda.com/doc/95259375/

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 Virtual Access Controller Cloud (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

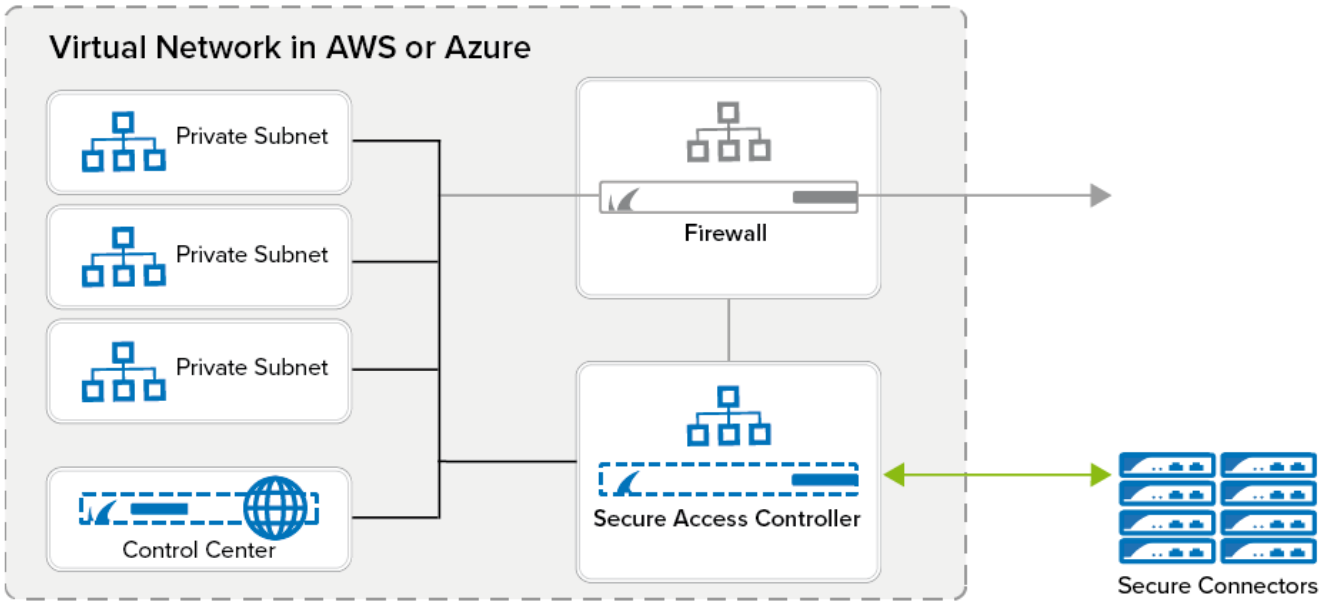
In this scenario, the Secure Connectors connect to the public IP address of the Access Controller. Management traffic from the Secure Connectors is sent either through a dedicated Access Controller to a Control Center VPN tunnel, or through the site-to-site VPN tunnel of an additional CloudGen Firewall that connects your on-premises data center 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 gateway 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. az_sc_integration_cc_onprem.png
2. az_sc_integration_cc_cloud.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.