

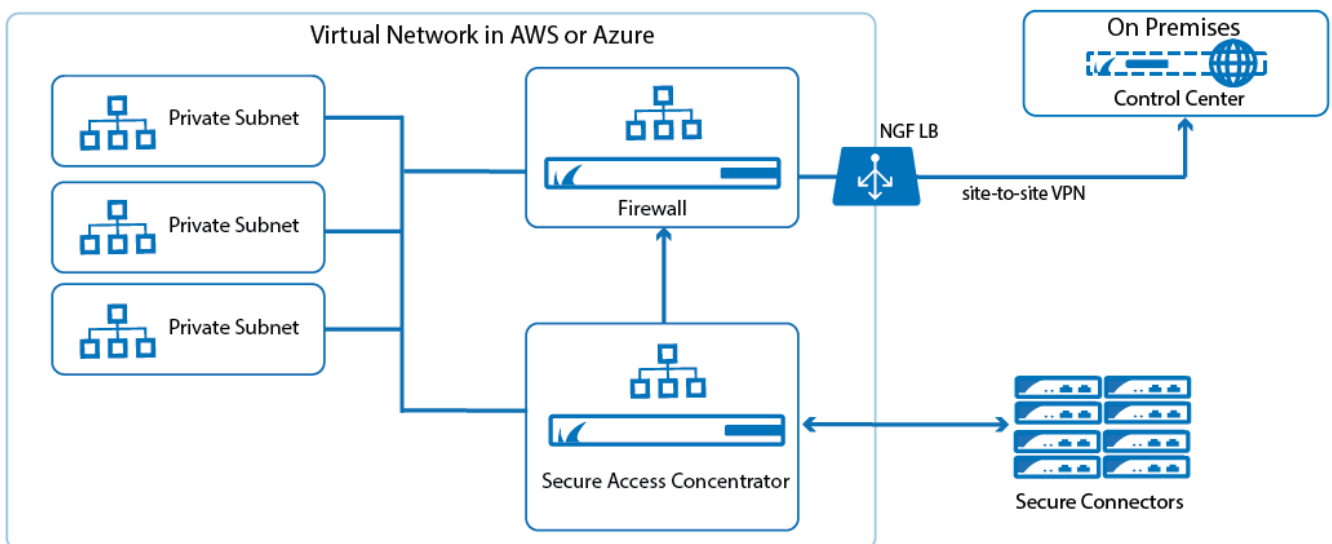
## Secure Access Concentrator in the Public Cloud

<https://campus.barracuda.com/doc/53248299/>

The Secure Access Concentrator 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 FSAC 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 Concentrator is used in combination with an F-Series Firewall. You have two options for setting up the Secure Access Concentrator. The deployment steps are the same as the steps required for an on-premises Access Concentrator.

### Access Concentrator and F-Series Firewall in the Public Cloud, Control Center on-premises

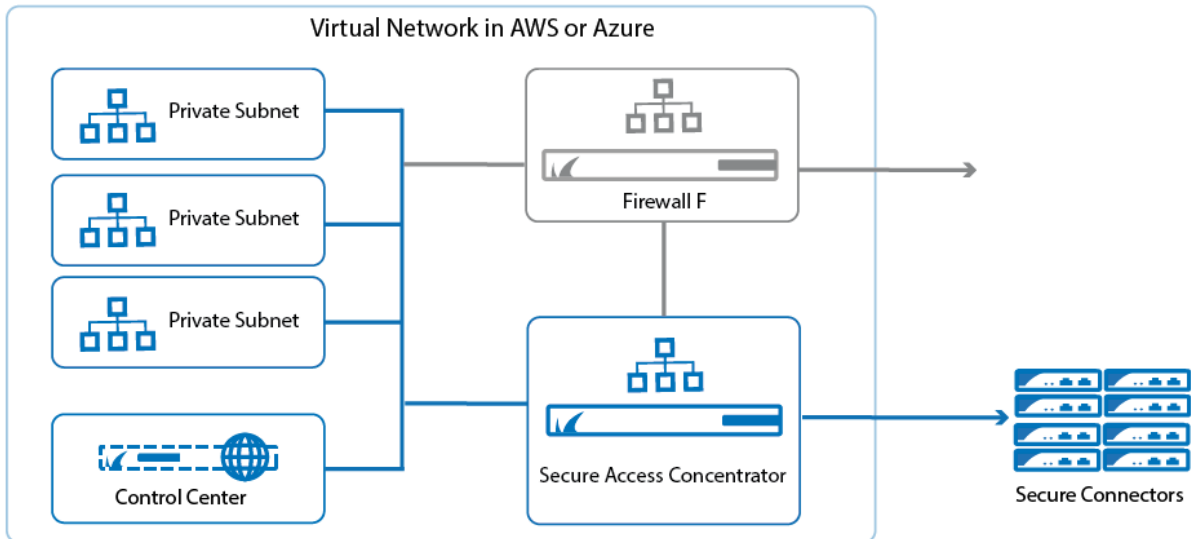
In this scenario, the Secure Connectors connect to the public IP address of the Access Concentrator. Management traffic from the Secure Connectors is sent either through a dedicated Access Concentrator to Control Center VPN Tunnel, or through the site-to-site VPN tunnel of an additional F-Series Firewall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



### Access Concentrator, F-Series Firewall, and Control Center in Azure or AWS

The client connects to the public IP address of the Access Concentrator. Traffic to the backend is routed either through the optional F-Series Firewall, or directly to the backend subnets. Management traffic from the Secure Connectors is forwarded by the Access Concentrator directly to the Control

Center in the cloud. The Access Concentrator 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 Concentrator is configured to work in tandem with an additional F-Series Firewall acting as the border firewall.



## Figures

1. Azure\_SAC\_Integration\_CC\_onprem.png
2. SAC\_Integration\_CC\_Cloud.png

© Barracuda Networks Inc., 2019 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.