
S-Series Deployment

<https://campus.barracuda.com/doc/46208891/>

Deploying a Barracuda NextGen S-Series network requires at least one SC Access Cluster, a Next Gen Control Center, and the deployment of the individual SC devices.

SC Access Cluster and NextGen Control Center Deployment

Each SC connecting to your network must be assigned to an SC Access Cluster, comprised of one SAC and a border firewall as well as a NextGen Control Center managing all SACs, F-Series Firewalls, and the SCs. The SC Access Clusters forward management traffic directly to the Control Center and send the rest via the border firewall to its destination. The border firewall routes incoming SC VPN tunnels to the SAC. It also scans and filters user traffic according to your company policies for outgoing traffic from the SC networks.

For more information, see [Secure Access Concentrator and Control Center Deployment](#).

SC Deployment via Configuration File

The configuration for the SC is created centrally on the Control Center using SC templates to reduce the configuration overhead. The SC configuration file is then exported and copied to the SC via USB OTG or web interface. The SC then automatically connects to the SAC in the SC Access Cluster assigned to it via the **sca.conf**. This allows the SC to connect in VPN operational mode and authenticate by the certificates included in the configuration file.

For more information, see [SC Deployment via SC Configuration File](#).

SC Deployment via VPN Deployment Mode

If you do not have physical access to the device, configure the SC in the Control Center. Directly on the SC, configure the WAN connection and VPN so the SC can connect to the SAC in VPN deployment mode. No certificates are required because the SAC uses a passphrase to authenticate. Once connected, the Control Center immediately pushes the operational configuration to the SC and switches the VPN to operational mode.

For more information, see [SC Deployment via VPN Deployment Mode](#).

© Barracuda Networks Inc., 2020 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.