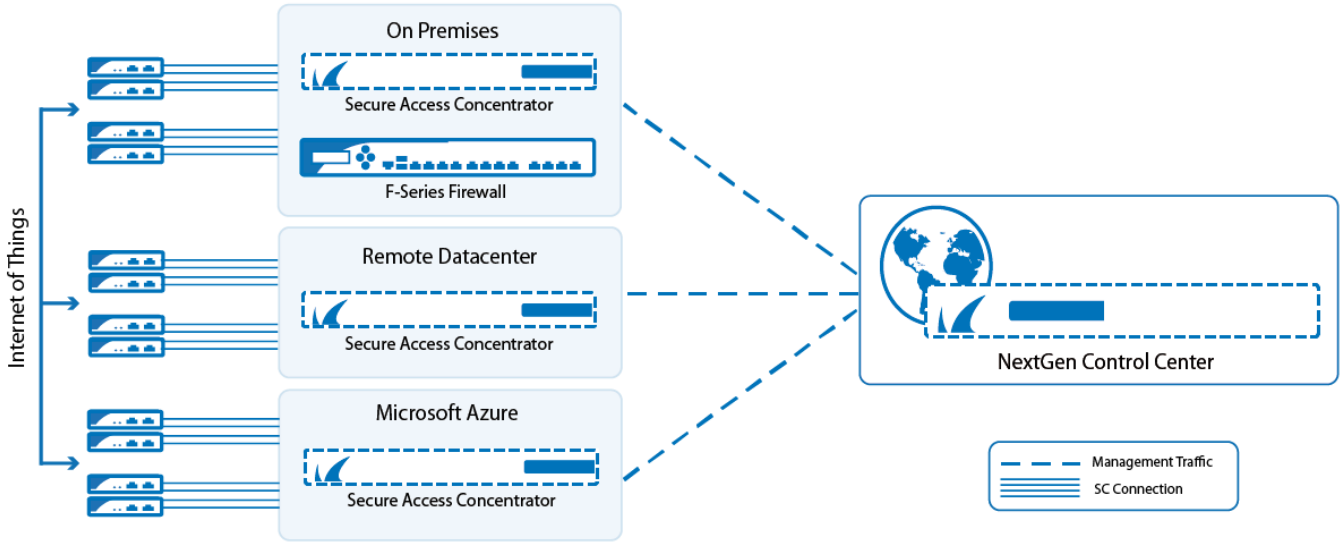
NextGen S-Series

https://campus.barracuda.com/doc/46209430/

The Barracuda NextGen S-Series offers large-scale remote access capabilities. It enables the ever-growing number of IoT devices and micro-networks to securely connect to the central or distributed corporate datacenter. In such a scenario, a large number of small Secure Connector (SC) appliances connect via TINA VPN to their regional Secure Access Concentrator (SAC). The SAC forwards the management traffic to the NextGen Control Center. Corporate policies such as Application Control, URL Filtering, and Virus Scanning are handled either directly on the SAC or forwarded to the border firewall. The configuration and lifecycle management for all SCs and their SACs are handled by one central NextGen Control Center. The Control Center can manage multiple Secure Access Concentrators, allowing you to scale up the network at will.



S-Series Secure Access Concentrator and Integration with the NextGen Control Center

S-Series Devices on the NextGen Control Center

The NextGen Control Center is a central management appliance for S-Series and F-Series devices. The Control Center provides a central template-driven configuration management interface, SC firmware update management, and status information for all S-Series devices. F-Series and S-Series devices can be managed on one Control Center, even when together in the same cluster. But unlike the F-Series Firewalls, the S-Series Secure Connector configuration is not configured in a tree structure; instead, configuration is handled through a single interface: the Secure Connector Editor. The Secure Connector Editor allows you to create configuration templates and link them to individual appliances. Changes to the templates are immediately pushed out to the SC devices. The administrator decides which configuration options are device-specific. These settings are then

configured directly on the device. Although it is possible to change the configuration of an individual device via the Web Interface, the Control Center configuration overrides the changes made after the Web Interface configuration lock is released. The SC networks are also defined via the Control Center, with each SC network permanently linked to an SAC. When an SC is deployed, a subnet of the SC network is automatically selected and permanently assigned to the SC.

For more information, see Secure Access Concentrator and Control Center Deployment and How to Create and Apply SC Templates.

NextGen S-Series Secure Access Concentrator (SAC)

The SAC is available as a virtual image for on-premise deployments or as an image in Microsoft Azure public cloud. It handles incoming SC VPN tunnels. Management traffic is automatically forwarded to the NextGen Control Center, and user traffic is processed either directly on the SAC, or forwarded to the internal, border firewall. If necessary, SACs can be deployed in a high availability cluster. Independent of the SAC license, you must also assign a SC Energize Update pool license. The number of instances in the SC pool license determines the number of SC configurations allowed per SAC. The size of the SC pool license may not exceed the maximum number of SC VPN connections for a SC model. The following SAC models are available:

- **NextGen SAC 400** – 2 CPU cores, up to 500 SC connections
- **NextGen SAC 610** – 4 CPU cores, up to 1200 SC connections
- **NextGen SAC 820** – 8 CPU cores, up to 2500 SC connections

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

NextGen S-Series Secure Connector (SC)

The Secure Connector is a small hardware appliance optimized to efficiently connect remote devices and micro-networks to the corporate datacenter via TINA VPN tunnel. The configuration is centrally managed by the NextGen Control Center, but can be overridden by the Web Interface on the device.

SC WAN Connections

The SC supports the following WAN connection types:

- DHCP client
- Static IP
- Wi-Fi client

For more information, see SC WAN Connections.

Networking

The SC VIP network is automatically assigned to the SC by the Control Center. The Wi-Fi access point on the SC uses a separate network from the SC network, accessing the other zones via source NAT firewall rules.

For more information, see SC Networking.

SC Firewall

The SC appliances use a different Firewall service from the F-Series Firewalls. The Firewall allows you to create rules defining access, source, and destination NAT based on four network zones defined for the SC:

- LAN
- Wi-Fi
- WAN (including Wi-Fi client)
- VPN

For more information, see SC Firewall.

VPN Service

The SC device connects to the SAC and the Control Center via one site-to-site tunnel on port TCP or UDP 692. In Operational mode, the VPN tunnel is authenticated via certificates, in Deployment mode via passphrase. The SC Firewall only allows the user to send LAN traffic through the VPN to LAN/WAN. It is not possible to use an Internet breakout for the devices in the LAN or Wi-Fi.

For more information, see SC VPN.

Figures