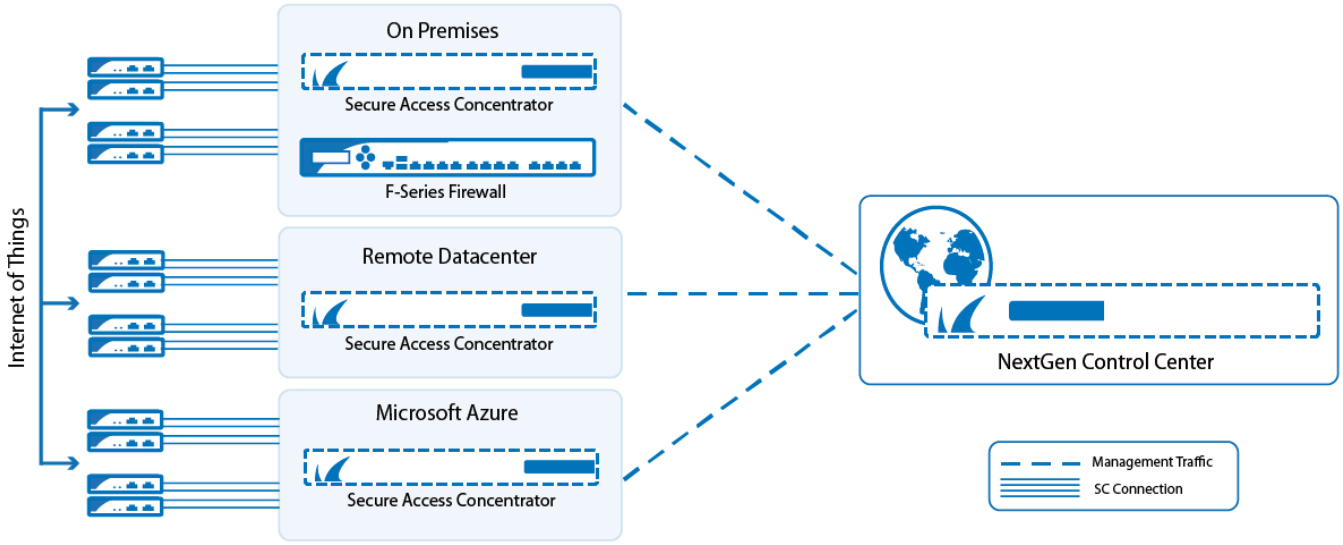
NextGen FSC-Series

https://campus.barracuda.com/doc/48203296/

The Barracuda NextGen FSC-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 (FSC) appliances connect via TINA VPN to their regional Secure Access Concentrator (FSAC). The FSAC 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 FSAC or forwarded to the border firewall. The configuration and lifecycle management for all FSCs and their FSACs 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.



FSC Series Secure Access Concentrator and Integration with the NextGen Control Center

FSC Series Devices on the NextGen Control Center

The NextGen Control Center is a central management appliance for FSC Series and F-Series devices. The Control Center provides a central template-driven configuration management interface, FSC firmware update management, and status information for all FSC Series devices. F-Series and FSC Series devices can be managed on one Control Center, even when together in the same cluster. But unlike the F-Series Firewalls, the FSC 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 FSC 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 FSC networks are also defined via the Control Center, with each FSC network permanently linked to an FSAC. When an FSC is deployed, a subnet of the FSC network is automatically selected and permanently assigned to the FSC.

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

NextGen FSC Series Secure Access Concentrator (FSAC)

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

- **Barracuda NextGen Firewall FSAC 400** – 2 CPU cores, up to 500 FSC connections
- **Barracuda NextGen Firewall FSAC 610** – 4 CPU cores, up to 1200 FSC connections
- **Barracuda NextGen Firewall FSAC 820** – 8 CPU cores, up to 2500 FSC connections

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

NextGen FSC Series Secure Connector (FSC)

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.

FSC WAN Connections

The FSC supports the following WAN connection types:

- DHCP client
- Static IP
- Wi-Fi client

For more information, see FSC WAN Connections.

Networking

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

For more information, see FSC Networking.

FSC Firewall

The FSC 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 FSC:

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

For more information, see FSC Firewall.

VPN Service

The FSC device connects to the FSAC 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 FSC Firewall only allows the user to send LAN traffic through the VPN or to WAN. It is not possible to use an Internet breakout for the devices in the LAN or Wi-Fi.

For more information, see FSC VPN.

Figures

1. s_series_architecture_1.png