Overview

https://campus.barracuda.com/doc/48203024/

The Barracuda NextGen Firewall family are purpose-built hardware and virtual appliances designed to protect and connect your network infrastructure. On top of industry-leading centralized management, the highly resilient VPN technology combined with intelligent traffic management capabilities allows customers to increase efficiency and increase overall network availability.

Barracuda NextGen Firewall F-Series

The F-Series firewall is an enterprise-grade, next-generation firewall that was purpose-built for efficient deployment and operation within dispersed, highly dynamic, and security-critical network environments. In addition to next-generation firewall protection, it provides industry-leading operations efficiency and added business value by safeguarding network traffic against line outages and link quality degradation.

User identity and application awareness are used to select the best network path, traffic priority, and available bandwidth for business-critical traffic. The F-Series Firewall can transparently move traffic to alternative lines to keep traffic flowing.

Barracuda NextGen Control Center

All policies and client and device settings for all F-Series Firewalls and FSC-Series Secure Connectors are centrally managed and tracked by the NextGen Control Center. This allows the NextGen F and FSC-Series to meet enterprise requirements of massive scalability, efficient configuration, and life cycle and license management across dispersed networks, while at the same time offering performance guarantees for business-critical applications.

Barracuda NextGen Firewall FSC-Series

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.

Platform Flexibility

The Barracuda NextGen family offers hardware and virtual models in various sizes, from branch offices up to headquarters and datacenters. The NextGen Control Center Vx and Firewall F-Series Vx can run on a wide range of hypervisors, effortlessly integrating with your existing network and server infrastructure. The NextGen F-Series is designed for deployment across the entire enterprise, including the Microsoft Azure, Amazon AWS, and Google Cloud Platform public clouds.

First Steps with the Barracuda NextGen Firewall F-Series and Control Center

Follow the deployment and getting started guides to get up and running:

- Deployment – Deployment for hardware, virtual, and public cloud NextGen Firewall F-Series and Control Center.
- Getting Started – Follow this guide to integrate your NextGen F-Series Firewall and Control Center into your existing network.