

Barracuda NextGen Firewall F

Protecting Your Digital Assets in Google Cloud



The growth in cloud computing capabilities and services has driven more data into places where traditional IT security measures cannot reach — into data centers not owned by your corporate IT group. Beyond its powerful network firewall, IPS, and VPN technologies, the Barracuda NextGen Firewall F-Series integrates a comprehensive set of **next-generation firewall technologies, including comprehensive application control, availability, and Quality of Service (QoS) features.**

Security

- ☐ Data Protection
- ☐ Application Delivery

The Barracuda Advantage

- Secure and reliable connectivity between on-premises and Google Cloud deployments
- Granular application control
- Full user awareness
- Central management of all functionality for both, on-premises and Google Cloud deployments
- Unrivaled Quality of Service capabilities

Product Spotlight

- Full user/group awareness
- Full application visibility and granular access control
- Advanced Threat Protection (incl. sandboxing)
- Built-in web security and IDS/IPS
- Full SD-WAN capabilities included
- Application-based provider selection



Granular Application Control

The Barracuda NextGen Firewall F-Series gives administrators granular control over applications, allowing them to define rules for forwarding data traffic using the best respective transmission channels based on type of application, user, content, time of day, and geographical location. The Barracuda NextGen Firewall F-Series allows organizations to prioritize traffic by limiting or restricting access to non-business-related applications and network traffic, even when encrypted.



Central Management

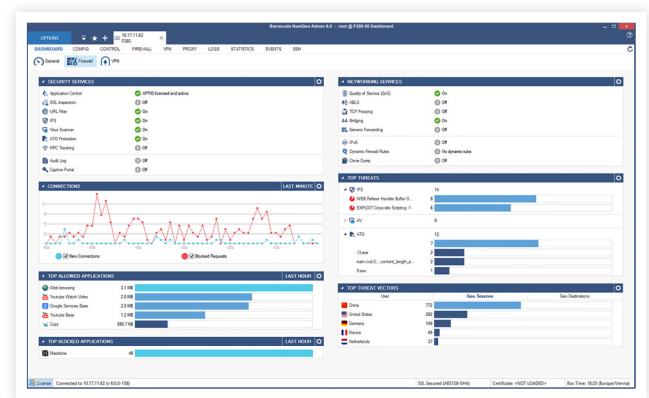
The Barracuda NextGen Firewall F-Series uses the same industry-leading single-pane-of-glass central management as on-premises deployments do. Easily manage the secure VPN connections to, from, and within Google Cloud and the Barracuda NextGen Firewall F-Series deployment itself.



Integrated Next-Generation Security and Connectivity

The Barracuda NextGen Firewall F-Series Intrusion Detection and Prevention System (IDS/IPS) strongly enhances network security by providing complete and comprehensive real-time network protection against a broad range of network threats, vulnerabilities, exploits, and exposures in operating systems, applications, and databases preventing network attacks such as SQL injections and arbitrary code executions.

The F-Series incorporates advanced site-to-site and client-to-site VPN capabilities, using both SSL and IPsec protocols to ensure remote users can easily and securely access network resources without complex client configuration and management.



The Barracuda NextGen Firewall F-Series dashboard provides real-time information and summaries of what is going on in an organization's network.



Technical Specs

Firewall

- Stateful packet inspection and forwarding
- Full user-identity awareness
- IDS/IPS
- Application control and granular application enforcement
- Interception and decryption of SSL/TLS encrypted applications
- Antivirus and web filtering in single pass mode
- Email security
- SafeSearch enforcement
- Google Accounts Enforcement
- Denial of Service protection (DoS/DDoS)
- Spoofing and flooding protection
- ARP spoofing and trashing protection
- DNS reputation filtering
- NAT (SNAT, DNAT), PAT
- Dynamic rules / timer triggers
- Single object-oriented rule set for routing, bridging, and routed bridging
- Virtual rule test environment

Protocol Support

- IPv4, IPv6
- BGP/OSPF/RIP
- VoIP (H.323, SIP, SCCP [skinny])
- RPC protocols (ONC-RPC, DCE-RPC)
- 802.1q VLAN

Intrusion Detection and Prevention

- Protection against exploits, threats and vulnerabilities
- Packet anomaly and fragmentation protection
- Advanced anti-evasion and obfuscation techniques
- Automatic signature updates

Advanced Threat Protection

- Dynamic, on-demand analysis of malware programs (sandboxing)
- Dynamic analysis of documents with embedded exploits (PDF, Office, etc.)
- Detailed forensic analysis
- Botnet and spyware protection
- TypoSquatting and link protection for email

Central Management Options via Barracuda NextGen Control Center

- Unlimited firewalls
- Support for multi-tenancy
- Multi-administrator support & RCS
- Pool license management
- Template & repository-based management
- REST API

Traffic Intelligence & SD-WAN

- Simultaneous use of multiple uplinks (transports) per VPN tunnel
- FIPS 140-2 certified cryptography
- Auto-VPN tunnel creation between remote spoke locations based on application type
- Dynamic bandwidth detection
- Performance-based transport selection
- Application-aware traffic routing
- Adaptive session balancing across multiple uplinks
- Traffic Replication (forward error correction)
- Application-based provider selection
- Application-aware traffic routing (VPN)
- Traffic shaping and QoS
- Built-in data deduplication

VPN

- Drag & drop VPN tunnel configuration
- VPNC certified (basic interoperability)
- Network Access Control
- iOS and Android mobile device VPN support
- Multi-factor authentication for SSL VPN and CudaLaunch

Infrastructure Services

- DHCP server, relay
- SIP, HTTP, SSH, FTP proxies
- SNMP and IPFIX support
- DNS Cache

BARRACUDA NEXTGEN FIREWALL F-SERIES	BRING-YOUR-OWN-LICENSE			
CAPABILITIES	Level 2	Level 4	Level 6	Level 8
Virtual Cores	1	2	4	8
FEATURES				
Firewall	●	●	●	●
Application Control	●	●	●	●
IPS	●	●	●	●
VPN (Site-to-Site and Client-to-Site)	●	●	●	●
SSL Interception	●	●	●	●
WAN Compression	●	●	●	●
Network Access Control for VPN client-to-site connections	●	●	●	●
Malware Protection ¹	Optional	Optional	Optional	Optional
Advanced Threat Protection ¹	Optional	Optional	Optional	Optional
Advanced Remote Access	Optional	Optional	Optional	Optional
Premium Support ²	Optional	Optional	Optional	Optional

¹ Including FTP, mail and Web protocols

² Premium Support ensures that an organization's network is running at its peak performance by providing the highest level of 24x7 technical support for mission-critical environments. For more information please visit <https://www.barracuda.com/support/premium>.

Support Options

Barracuda Energize Updates

- Standard technical support
- Firmware updates
- IPS signature updates
- Application control definition updates
- Web filter updates

Security Options

- Advanced Threat Protection
- Malware Protection
- Advanced Remote Access subscription provides remote access via the CudaLaunch app for Windows, macOS, iOS, and Android devices

Specifications subject to change without notice.