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 Services (QoS) features.

**The Barracuda Advantage**
- Secure and reliable connectivity between on-premises and Amazon Web Services deployments
- Granular Application Control
- Full User Awareness
- Central management of all functionality for both, on-premises and Amazon Web Services deployments
- Unrivaled Quality of Service capabilities

**Product Spotlight**
- Powerful next-generation network firewall
- Advanced Threat Detection
- Built-in web security and IDS/IPS
- Client-to-Site VPN via browser (SSL VPN), mobile apps and desktop VPN clients
- Full application visibility and granular control
- Intelligent traffic regulation including application-based provider selection
- Tightly integrated Quality of Service (QoS) and link balancing
- Centralized management of all functionality
- Template-based and role-based configuration

**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.

**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.

**Central Management**
The Barracuda NextGen Firewall F-Series benefits of 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 Amazon Web Services and the Barracuda NextGen Firewall F-Series deployment itself.

---

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
- Intrusion Detection and Prevention System (IDS/IPS)
- Application control and granular application enforcement
- Interception and decryption of SSL/TLS encrypted applications
- Antivirus and web filtering in single pass mode
- SafeSearch enforcement
- Google Accounts Enforcement
- Denial of Service protection (DoS/DDoS)
- Spoofing and flooding protection
- ARP spoofing and caching protection
- DNS reputation filtering
- TCP stream reassembly
- Transparent proxying (TCP)
- NAT (SNAT, DNAT), PAT
- Dynamic rules / timer triggers
- Single object-oriented rule set for routing, bridging, and routed bridging
- Virtual machine test environment
- Firewall
- Application Control
- IPS
- VPN (Site-to-Site and Client-to-Site)
- SSL Interception
- WLAN Optimization
- Network Access Control for VPN client-to-site connections
- Malware Protection
- Advanced Threat Detection
- Premium Remote Access
- Premium Support

**User Identity Awareness**
- Terminal Server Agent
- Domain Controller Agent
- Authentication – supports x.509, NTLM, RADIUS, RSA SecurID, LDAP/LDAP, Active Directory, TACACS+, SMS Passcode (VPN), local authentication database

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

**Traffic Optimization**
- Link monitoring, aggregation, and failover
- Dynamic routing
- Application-based provider selection
- Traffic shaping and QoS
- On-the-fly flow prioritization
- Stream and packet compression
- Byte-level data deduplication
- WAN optimization (SMBv2)

**VPN**
- Drag & drop VPN tunnel configuration
- Secure site-to-site, client-to-site VPN
- Supports AES-128/256, 3DES, DES, null ciphers
- Private CA or external PKI
- IPsec / SSL VPN
- VPN certified (basic interoperability)
- Application-aware traffic routing
- PPTP / L2TP (IPSec)
- Network Access Control
- iOS and Android mobile device VPN support

**Advanced Threat Detection**
- Dynamic, on-demand analysis of malware programs (sandboxing)
- Dynamic analysis of documents with embedded exploits (PDF, Office, etc.)
- Detailed forensics for both, malware binaries and web threats (exploits)
- Support for multiple operating systems (Windows, Android, etc.)
- Botnet and Spyware Protection
- Flexible malware analysis in the cloud

**Infrastructure Services**
- SIP, HTTP, SSH, FTP proxies
- SNMP and IPFIX support
- DNS Cache
- SMTP gateway and SPAM filter

**Protocol Support**
- IPv4, IPv6, ARP
- BGP/OSPF/RIP
- VoIP (H.323, SIP, SCCP [skinny])
- RPC protocols (ONC-RPC, DCE-RPC)

**Central Management Options**
- Barracuda NextGen Control Center
  - Central administration of unlimited F-Series Firewalls
  - Support for multi-tenancy
  - Multi-administrator support & RCS

**Support Options**
- Barracuda Energize Updates
  - Standard technical support
  - Firmware updates
  - IPS signature updates

**Security Options**
- Application control definition updates
- Web filter updates
- Advanced Threat Detection
- Malware Protection

**BARRACUDA NEXTGEN FIREWALL F-SERIES**

<table>
<thead>
<tr>
<th>AWS COMPUTE INSTANCE NAME</th>
<th>BRING-YOUR-OWN-LICENSE</th>
<th>PAY-AS-YOU-GO LICENSE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CAPABILITIES</strong></td>
<td><strong>T2.SMALL</strong></td>
<td><strong>C3.MEDIUM</strong></td>
</tr>
<tr>
<td>Virtual Cores</td>
<td>Level 2</td>
<td>Level 4</td>
</tr>
<tr>
<td>Max Number of Interfaces</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td><strong>FEATURES</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN (Site-to-Site and Client-to-Site)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL Interception</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Access Control for VPN client-to-site connections</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware Protection</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>Advanced Threat Detection</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>Premium Remote Access</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>Premium Support</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1 Including FTP, mail and Web protocols
2 Requires Malware Protection subscription
3 Basic Remote Access is included in Energize Updates
4 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

Specifications subject to change without notice.