

# Barracuda NextGen Firewall F

Protección de sus activos digitales en Amazon Web Services



El crecimiento en capacidades y servicios de computación en la nube ha llevado a más datos a lugares donde las medidas tradicionales de seguridad de TI no pueden llegar - los centros de datos que no son propiedad de su grupo de TI. Más allá de su poderoso firewall de red, IPS y tecnologías VPN, el Barracuda NextGen Firewall F-Series integra un conjunto completo de tecnologías de **Firewall de Última Generación, que incluye funciones integrales de control de aplicaciones, disponibilidad y calidad de servicios (QoS).**

- ✓ Seguridad
  - Protección de datos
  - Aplicación de entrega

## La ventaja de Barracuda

- Un verdadero firewall de generación de nube: implementado cómo lo necesita, aprovecha todas las características incorporadas de AWS y los modelos de licencia aseguran el comercio sin contratiempos
- Simplicidad de operación, conexión en el local y seguridad en la nube en una sola interfaz
- Conectividad segura y confiable entre las instalaciones y las implementaciones de Amazon Web Services
- Administración central de todas las funcionalidades para ambos, en las instalaciones y las implementaciones de Amazon Web Services
- Capacidades inigualables de calidad de servicio

## Producto destacado

- Conocimiento completo de usuario / grupo
- Visibilidad completa de la aplicación y control de acceso granular
- Protección avanzada contra amenazas (incluido sandboxing)
- Seguridad web incorporada e IDS / IPS
- Capacidades SD-WAN completas incluidas
- Selección del proveedor basado en la aplicación
- Soporte completo para AWS Direct Connect
- Verdadera flexibilidad de licencia con Bring-Your-Own-License o Pay-as-You-Go (por hora o por volumen)



## Control de aplicación granular

Barracuda NextGen Firewall F-Series le da a los administradores control granular sobre las aplicaciones, lo que les permite definir reglas para reenviar el tráfico de datos utilizando los mejores canales de transmisión según el tipo de aplicación, usuario, contenido, hora del día y ubicación geográfica. Barracuda NextGen Firewall F-Series permite a las organizaciones priorizar tráfico al imitar o restringir el acceso a actividades no relacionadas con el negocio, aplicaciones y tráfico de red, incluso cuando esté cifrado.



## Administración Central

Barracuda NextGen Firewall F-Series se beneficia del mismo líder en la industria de las implementaciones locales o en sitio. Administre fácilmente las conexiones seguras VPN, desde, hacia y dentro de Amazon Web Services y la implementación misma de Barracuda NextGen Firewall F-Series.



## Seguridad y Conectividad integrada de Nueva Generación

La detección de intrusiones de la serie F de Barracuda NextGen Firewall y el Sistema de Prevención (IDS / IPS) mejora fuertemente la seguridad de la red al proporcionar en tiempo real una completa protección de red contra una amplia gama de amenazas, vulnerabilidades, exploits y exposición en sistemas operativos, aplicaciones y bases de datos previniendo de ataques a la red tales como inyecciones de SQL y ejecuciones de código arbitrario.

La Serie F incorpora capacidades de VPN sitio a sitio avanzado y de cliente a sitio, utilizando SSL y Protocolos IPsec para asegurar que los usuarios remotos puedan fácilmente y seguramente acceder a los recursos de red sin configuración y administración complejas del cliente.



El tablero de Barracuda CloudGen Firewall proporciona información en tiempo real y resúmenes de lo que está sucediendo en la red de una organización.



Estamos utilizando Barracuda NextGen Firewalls, aprovisionados a través de AWS Marketplace, para proteger eficazmente nuestra aplicación contra los ataques basados en la web y los ataques de la capa de aplicación. La solución Barracuda se conecta perfectamente con nuestro entorno AWS y está haciendo su trabajo de minimizar el área de superficie de ataque y ayuda a nuestros clientes a mantenerse protegidos en los datos del titular de la tarjeta del miembro del club.

Max Longin  
Founding Partner  
Club Automation

## Especificaciones técnicas

### Firewall

- Inspección y reenvío de paquetes con indicador de estado
- Conocimiento completo de la identidad del usuario
- IDS/IPS
- Control de aplicaciones y aplicación granular
- Intercepción y descifrado de aplicaciones encriptadas SSL / TLS
- Antivirus y filtrado web en modo de paso único
- Seguridad del correo electrónico
- Aplicación SafeSearch
- Aplicación de cuentas de Google
- Protección de negación de servicio (DoS / DDoS)
- Protección de spoofing e inundación (flooding)
- ARP Protección de suplantación y destrucción
- Filtrado de reputación DNS
- NAT (SNAT, DNAT), PAT
- Reglas dinámicas / activadores del temporizador
- Conjunto de reglas orientadas a objetos individuales para enrutamiento, puenteo y puente enrutado
- Entorno de prueba de regla virtual

### Protocolos soportados

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

### Detección y Prevención de Intrusos

- Protección contra exploits, amenazas y vulnerabilidades
- Anomalía de paquetes y protección contra la fragmentación
- Técnicas avanzadas contra la evasión y la ofuscación
- Actualizaciones automáticas de firmas

### Protección avanzada contra amenazas (ATP)

- Análisis dinámico a pedido de programas de malware (sandboxing)
- Análisis dinámico de documentos con exploits incrustados (PDF, Office, etc.)
- Análisis forense detallado
- Protección de botnet y spyware
- TypoSquatting y protección de enlaces para correo electrónico

### Opciones de administración central a través de Barracuda Firewall Control Center

- Administración para un número ilimitado de firewalls
- Soporte para multi-cliente
- Soporte multigestor y RCS
- Licencia Enterprise / MSP amigable
- Gestión basada en plantillas y repositorios
- API REST

### Servicios de infraestructura

- Servidor DHCP, relay
- Proxies SIP, HTTP, SSH, FTP
- Compatible con SNMP e IPFIX
- Caché de DNS

### Inteligencia de tráfico y SD-WAN

- Uso simultáneo de múltiples enlaces ascendentes (transportes) por túnel VPN
- Criptografía certificada FIPS 140-2
- ACreación de túnel VPN automático entre ubicaciones remotas basadas en el tipo de aplicación
- Detección dinámica de ancho de banda
- Selección de transporte basado en el rendimiento
- Equilibrio de sesión adaptable en múltiples enlaces ascendentes
- Replicación del tráfico (corrección de errores hacia adelante)
- Selección del proveedor basado en la aplicación
- Enrutamiento de tráfico con reconocimiento de aplicaciones (VPN)
- Traffic shaping y QoS
- Deduplicación de datos incorporada

### VPN

- Arrastrar y soltar la configuración del túnel VPN
- Control de acceso a la red
- Soporte de VPN para dispositivos móviles con iOS y Android
- Autenticación de múltiples factores para SSL VPN y CudaLaunch

### Barracuda Energize Updates

- Soporte técnico estándar
- Actualizaciones de firmware
- Actualizaciones de firmas IPS
- Actualizaciones de definición de control de aplicaciones
- Actualizaciones de filtro web

BARRACUDA NEXTGEN FIREWALL F-SERIES	BRING-YOUR-OWN-LICENSE				PAY-AS-YOU-GO LICENSE	
	Level 2	Level 4	Level 6	Level 8	HOURLY-BASED	VOLUME-BASED
<b>CAPABILITIES</b>					not restricted	not restricted
Virtual Cores	1	2	4	8	1 - 16	1 - 16
Max Number of Interfaces	2	2	4	4	4	4
<b>FEATURES</b>						
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	●	●	●	●	●	●
Energize Updates	●	●	●	●	●	●
Malware Protection <sup>1</sup>	Optional	Optional	Optional	Optional	-	-
Advanced Threat Protection <sup>1</sup>	Optional	Optional	Optional	Optional	-	-
Advanced Remote Access	Optional	Optional	Optional	Optional	●	●
Premium Support <sup>3</sup>	Optional	Optional	Optional	Optional	-	-

<sup>1</sup> Including FTP, mail and Web protocols

<sup>2</sup> 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>.

## Opciones de seguridad

- **La protección avanzada contra amenazas** impide incumplimientos de red, identifica malware de día cero exploits, ataques dirigidos, amenazas persistentes avanzadas y otro malware avanzado.

- **Malware Protection** proporciona protección contra malware, virus, spyware y otros programas no deseados dentro del tráfico SMTP / S, HTTP / S y FTP

- **Advanced Remote Access** proporciona una VPN SSL personalizable y fácil de usar basada en portal, así como sofisticado control de acceso a la red (NAC) y soporte CudaLaunch.

Specifications subject to change without notice.