Barracuda **Web Application Firewall**

Protege las aplicaciones y los datos contra amenazas avanzadas

- ☑ **Security**
- ☐ Data Protection
- ☑ **Application Delivery**

Barracuda Web Application Firewall **bloquea una lista en constante expansión de intrusiones y ataques sofisticados basados en la Web** cuyo objetivo son las aplicaciones alojadas en los servidores web y los datos sensibles a los que tienen acceso.

La ventaja de Barracuda

- Máxima seguridad que utiliza una arquitectura completa de proxy inverso
- Protección contra malware para aplicaciones web colaborativas
- Emplea la inteligencia de reputación de IP para combatir los ataques DDoS
- No se utilizan licencias basadas en usuarios o en módulos
- Diseñado para facilitar a las empresas el cumplimiento de normas como PCI DSS e HIPAA
- Escaneo basado en cloud, Barracuda Vulnerability Manager
- Resolución automática de vulnerabilidades

Puntos destacados del producto

- Protección completa contra ataques entrantes, incluidos los de OWASP Top 10
- El almacenamiento en caché incorporado, la compresión y la agrupación de TCP garantizan la seguridad sin repercutir sobre el rendimiento
- Control de acceso de usuarios basado en su identidad para aplicaciones web
- Prevención frente a pérdidas de datos incorporada
- Certificado por ICSA

Protección constante contra amenazas en evolución

Barracuda Web Application Firewall brinda una protección superior contra las pérdidas de datos, DDoS y todas las modalidades de ataque de capa de aplicación conocidas. Las actualizaciones automáticas permiten defenderse contra las nuevas amenazas a medida que van apareciendo. Cuando surjan nuevos tipos de amenazas, el firewall adquirirá nuevas capacidades para bloquearlas.

Administración de identidad y acceso

Barracuda Web Application Firewall ofrece sólidas prestaciones de autenticación y control de acceso que garantizan la seguridad y la privacidad restringiendo el acceso a aplicaciones o a datos confidenciales a los usuarios autorizados.

Asequible y fácil de usar

Las plantillas de seguridad predefinidas y la interfaz web intuitiva brindan seguridad inmediata sin necesidad de ajustes engorrosos ni de conocimientos sobre la aplicación. La integración con los escáneres de vulnerabilidad de seguridad y las herramientas SIEM automatiza el proceso de evaluación, supervisión y mitigación.

Con Barracuda Web Application Firewall en funcionamiento, demostramos a nuestros clientes y a nuestros socios que nos tomamos en serio la seguridad de sus datos. Permite que nuestro personal se preocupe menos acerca de la seguridad back-end y se concentre más en ofrecer servicios de calidad a nuestros socios y a nuestros clientes.

Michael Fainshtein
Director General de Tecnología
CredoRax.

Especificaciones técnicas

Seguridad de aplicaciones web
- Protección contra las amenazas de OWASP Top 10
- Protección contra ataques comunes
  - Inyección SQL
  - Cross-site scripting
  - Manipulación de cookies o de formularios
- Validación de metadatos de campos de formulario
- Seguridad adaptable
- Encubrimiento de sitios web
- Cifrado de URL
- Control de respuesta
- Inspección de contenido malicioso en JSON
- Cortafuegos XML
- Protección contra legrado de Web
- Protección contra robo de datos salientes
  - Números de tarjetas de crédito
  - Correspondencia de patrones personalizados (regex)
- Políticas granulares para elementos HTML
- Controles de límite de protocolo
- Control de carga de archivos
- Geolocalización de IP
  - Proxy anónimo
- Bloqueo tor

Protección frete a ataques de denegación de servicio (DDoS)
- Pisibilidad de integración con la Barracuda NextGen Firewall pra bloquear IP malignas
- Base de datos de reputación de Barracuda
- Análisis heurístico de huellas
- Desafíos CAPTCHA
- Protección por ralentización de acceso cliente
- Nodos de acceso Tor
- Lista negra de Barracuda
- Protección volumétrica contra ataques DDoS[3]

Autentificación básica
- LDAP/RADIUS
- Certificados de clientes
- SMS Passcode
- Inicio de sesión único
- Soporte Multi-Dominio

Autentificación avanzada
- Kerberos v5
- SAML
- Azure AD
- RSA SecurID

Registro, supervisión y generación de informes
- Registro del sistema
- Registro del firewall web
- Registro de acceso
- Registro de auditoría

Integraciones SIEM
- ArcSight
- RSA enVision
- Splunk
- Symantec
- Microsoft Azure Event Hub
- Personalizadas

</> Protocolos web compatibles
- HTTP/S 0.9/1.0/1.1/2.0
- WebSocket
- FTP/S
- XML
- IPv4/IPv6

Prestación de aplicaciones y aceleración
- Alta disponibilidad
- Descarga de SSL
- Equilibrio de carga
- Direccionamiento de contenido

Redes
- VLAN, NAT
- ACL de red
- Ruteado avanzado

Opciones de soporte

Instant Replacement Service
- Envío de una unidad de reemplazo al siguiente día laborable
- Soporte técnico 24 x 7
- Renovación de hardware cada cuatro años

Opciones de hardware
- Ethernet derivado opcional

Características de administración
- Administración basada en funciones personalizable
- Integración con los escáneres de vulnerabilidad
- Excepción de host fiable
- REST API
- Borradores personalizados
- Informes interactivos y programados

COMPARACIÓN DE MODELOS	360	460	660	860	960
CAPACIDAD					
Servidores back-end compatibles	1-5	5-10	10-25	25-150	150-300
Rendimiento	25 Mbps	50 Mbps	200 Mbps	1 Gbps	5 Gbps
HARDWARE					
Factor de forma	1U Mini	1U Mini	1U Tamaño	2U Tamaño	2U Tamaño
Medidas (cm)	42,7 x 35,6 x 4,3	42,7 x 35,6 x 4,3	42,7x 57,4 x 4,3	44,2 x 64,8 x 8,9	44,2 x 64,8 x 8,9
Peso (kg)	5,4	5,4	11,8	20,9	23,6
Puertos de ruta de acceso a datos	2 x 10/100	2 x GbE	2 x GbE	8 x GbE[1]	8 x GbE[1] ; 2 x 10GbE[1]
Puerto de administración	1 x 10/100	1 x 10/100	1 x 10/100/1000	1 x 10/100/1000	1 x 10/100/1000
Corriente de entrada de CA en 230V (A)	0,6	0,7	0,9	2,1	2,8
Memoria ECC			•	•	•
CARACTERÍSTICAS					
Control de respuesta	•	•	•	•	•
Advanced Threat Protection[2]			•	•	•
Protección contra robo de datos salientes	•	•	•	•	•
Control de carga de archivos	•	•	•	•	•
SSL Offloading	•	•	•	•	•
Autenticación y autorización	•	•	•	•	•
Integración con los escáneres de vulnerabilidad	•	•	•	•	•
Protección contra ataques DDoS[3]	•	•	•	•	•
Protección contra legrado de Web	•	•	•	•	•
Firewall de red	•	•	•	•	•
Alta disponibilidad	Activo/pasivo	Activo/pasivo	Activo/activo	Activo/activo	Activo/activo
Seguridad usando JSON	•	•	•	•	•
Almacenamiento en caché y compresión		•	•	•	•
Autentificación Autorización y Contabilidad basica (AAA)		•	•	•	•
Autentificación Autorización y Contabilidad avanzada (AAA)			•	•	•
Equilibrio de carga		•	•	•	•
Direccionamiento de contenido		•	•	•	•
Perfil adaptable			•	•	•
Antivirus para carga de archivos			•	•	•
Cifrado de URL			•	•	•
Firewall XML			•	•	•

[1] Opciones disponibles de NIC de fibra y Ethernet con bypass por hardware.
[2] Requiere una suscripción activa a la Advanced Threat Protection.
[3] Protección volumétrica contra ataques DDoS requiere suscripción.

Especificaciones sujetas a cambio sin previo aviso.