Barracuda **Web Application Firewall Vx**

Protege las aplicaciones y los datos contra amenazas avanzadas

- ☑ **Security**
- ☐ Storage
- ☐ 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
- Protección frente a ataques DoS a la aplicación

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.

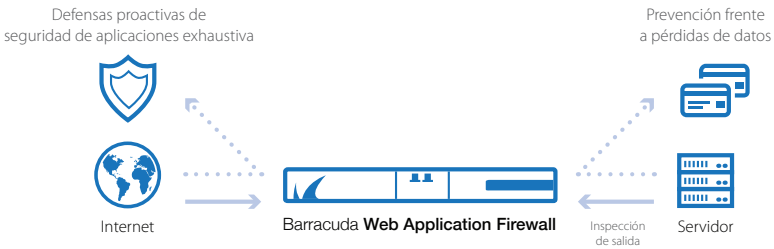
Administración de identidad y acceso

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.

Proteja los servidores, las aplicaciones y los datos contra ataques basados en Web.



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
Chief Technology Officer
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
- Control de respuesta
- Cortafuegos XML
- Inspección de contenido malicioso en JSON
- 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 protocolos
- Control de carga de archivos

Soporte de Hypervisores

- VMware ESX/ESXi
- VMware Server/Fusion/Workstation/Player
- Citrix Xenserver
- Oracle VirtualBox
- Microsoft Hyper-V

</> Protocolos web compatibles

- HTTP/S 0.9/1.0/1.1/2.0
- WebSocket
- FTP/S
- XML

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

Autentificación básica

- LDAP/RADIUS
- Certificados de clientes
- SMS Passcode
- Single Sign-On
- Soporte Multi-Dominio

Autentificación avanzada

- Kerberos v5
- SAML
- Azure AD
- RSA SecurID

Integraciones SIEM

- HPE ArcSight
- RSA enVision
- Splunk
- Symantec
- Microsoft Azure Event Hub
- Personalizadas

Opciones de soporte

Barracuda Energize Updates

- Soporte técnico estándar
- Actualizaciones de firmware y de capacidades según las necesidades
- Actualizaciones de definiciones de aplicaciones automática

Características de administración

- Administración basada en funciones personalizable
- Integración con los escáneres de vulnerabilidad
- Excepción de host fiable
- REST API
- Borradores personalizados

Registro, supervisión y generación de informes

- Registro del sistema
- Registro del firewall web
- Registro de acceso
- Registro de auditoría
- Registro del firewall de red
- Informes exhaustivos a demanda y programadoss

Administración centralizada

- Supervise y configure diversos productos Barracuda desde una sola interfaz
  - Compruebe el estado y ejecute informes
  - Asigne funciones con permisos variados
  - Disponible en cualquier lugar

COMPARACIÓN DE MODELOS	360VX	460VX	660VX	760VX	860VX	960VX
CAPACIDAD						
Servidores back-end compatibles	1-5	5-10	10-25	25-50	50-150	150-300
Número de núcleos compatibles	2	4	6	8	10	12
Rendimiento	25Mbps	50Mbps	200Mbps	500Mbps	1Gbps	5Gbps
CARACTERÍSTICAS						
SSL Offloading	●	●	●	●	●	●
Control de respuesta	●	●	●	●	●	●
Protección contra robo de datos salientes	●	●	●	●	●	●
Control de carga de archivos	●	●	●	●	●	●
Antivirus para carga de archivos			●	●	●	●
Advanced Threat Protection[1]			●	●	●	●
Autenticación y autorización	●	●	●	●	●	●
Autentificación Autorización y Contabilidad basica (AAA)		●	●	●	●	●
Autentificación Autorización y Contabilidad avanzada (AAA)			●	●	●	●
Protección contra ataques DDoS[2]	●	●	●	●	●	●
Protección contra legrado de Web	●	●	●	●	●	●
Firewall de red	●	●	●	●	●	●
Alta disponibilidad	Activo/pasivo	Activo/pasivo	Activo/activo	Activo/activo	Activo/activo	Activo/activo
Firewall XML			●	●	●	●
Cifrado de URL		●	●	●	●	●
Perfil adaptable		●	●	●	●	●
Integración con los escáneres de vulnerabilidad	●	●	●	●	●	●
Equilibrio de carga		●	●	●	●	●
Almacenamiento en caché y compresión		●	●	●	●	●
Direccionamiento de contenido		●	●	●	●	●
Direccionamiento avanzado			●	●	●	●

[1] Requiere una suscripción activa a la Advanced Threat Protection.
[2] Protección volumétrica contra ataques DDoS requiere suscripción.

Specifications subject to change without notice.