Barracuda **Web Application Firewall**

Protección de aplicaciones y datos en Microsoft Azure

- ☑ **Security**
- ☐ Storage
- ☐ Application Delivery

Barracuda Web Application Firewall **bloquea ataques de DDoS de capa de aplicación y otros vectores de ataque dirigidos a aplicaciones en línea alojadas en Microsoft Azure. Simultáneamente, esto proporciona una protección superior contra la pérdida de datos.**

También ofrece potentes funcionalidades de autenticación y control de accesos para restringir el acceso a aplicaciones y datos sensibles.

La ventaja de Barracuda

- Barracuda Central Operations Center realiza un seguimiento de las amenazas emergentes
- 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
- Diseñado para facilitar a las empresas el cumplimiento de normas como PCI DSS e HIPAA
- Escaneo basado en cloud con Barracuda Vulnerability Manager
- Corrección 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 la identidad para aplicaciones web
- Prevención frente a pérdidas de datos incorporada
- Certificado por ICSA

Protección constante frente a amenazas en evolución

Barracuda Web Application Firewall brinda una protección superior contra las pérdidas de datos, DDoS y todos los vectores de ataque de capa de aplicaciones conocidos. Las actualizaciones automáticas permiten defenderse contra las nuevas amenazas a medida que van apareciendo. A medida que vayan surgiendo nuevos tipos de amenazas, adquirirá nuevas capacidades para bloquearlos.

Administración de identidades y accesos

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 datos sensibles a los usuarios autorizados.

Asequible y fácil de usar

Las plantillas de seguridad predefinidas y la interfaz de usuario 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.

NSS LABS RECOMMENDED

ICSA labs CERTIFIED WEB APPLICATION FIREWALL

Microsoft Azure Certified

Technical Specs

Seguridad de aplicaciones web
- Protección contra las amenazas de OWASP Top 10
- Protección contra ataques comunes
  - Inyección SQL
  - Secuencias de comandos entre sitios
  - 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
- 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 protocolo
- Control de carga de archivos

Protocolos web compatibles
- HTTP/S 0.9/1.0/1.1/2.0
- WebSocket
- FTP/S
- XML

Protección frente a DDoS
- Integración con Barracuda NextGen Firewall para el bloqueo de IPs maliciosas
- Base de datos de reputación de IP de barracuda
- Identificación mediante huellas digitales heurística
- Desafíos mediante CAPTCHA
- Protección frente a clientes lentos
- Layer 3 y Layer 7 Geo IP
- Proxy anónimo
- Nodos de salida ToR
- Lista negra de Barracuda

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

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

Opciones de soporte

Barracuda Energize Updates
- Soporte técnico estándar
- Actualizaciones de firmware y de capacidades según las necesidades
- Actualizaciones de definiciones de aplicaciones automáticas

Características de administración
- Administración basada en funciones personalizable
- Integración con los escáneres de vulnerabilidad
- Excepción de host fiable
- Perfil adaptable para el aprendizaje
- Perfiles de excepciones para ajuste
- 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 programados

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

BARRACUDA WEB APPLICATION FIREWALL	MICROSOFT AZURE - NOMBRE DE INSTANCIA DE COMPUTACIÓN			
	PEQUEÑA (A1)	MEDIANA (A2)	GRANDE (A3)	EXTRA GRANDE (A4)
CAPACIDAD	**Level 1**	**Level 5**	**Level 10**	**Level 15**
Virtual Cores	1	2	4	8
Rendimiento	100 Mbps	200 Mbps	400 Mbps	750 Mbps
Conexiones HTTP por segundo	5.000	7.000	10.000	14.000
Conexiones HTTPS por segundo	5.000	7.000	10.000	14.000
CARACTERÍSTICAS				
Control de respuesta	•	•	•	•
Protección de a Amenazas Persistentes (APT) [3]		•	•	•
Protección contra robo de datos salientes	•	•	•	•
Control de carga de archivos	•	•	•	•
SSL Offloading	•	•	•	•
Integración con los escáneres de vulnerabilidad	•	•	•	•
Protección contra ataques DDos[4]	•	•	•	•
Firewall de red	•	•	•	•
Protección contra legrado de Web	•	•	•	•
Clustering	configuración de sincronización		configuración de sincronización	
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	•	•	•	•
Cifrado de URLs	•	•	•	•
Antivirus para carga de archivos		•	•	•
Firewall XML	•	•	•	•
Seguridad usando JSON	•	•	•	•
Premium Support [2]	Opcional	Opcional	Opcional	Opcional

[1] La agrupación en clústeres permite la sincronización de la configuración entre diversas instancias. Azure Load Balancer se puede utilizar para distribuir el tráfico a varios nodos.
[2] Premium Support garantiza que la red de una organización se ejecute a pleno rendimiento, ya que ofrece el máximo nivel de soporte técnico ininterrumpido para entornos críticos. Para obtener más información, visite https://www.barracuda.com/support/premium.
[3] Requiere una subscripción activa de Advanced Threat Protection. Disponible sólo en modelos BYOL.
[4] Protección volumétrica contra ataques DDoS requiere suscripción.

Especificaciones sujetas a cambio sin previo aviso.