Barracuda **Web Application Firewall**

Schützt Anwendungen und Daten vor komplexen Bedrohungen

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

Die Barracuda Web Application Firewall **blockiert eine kontinuierlich erweiterte Anzahl ausgefeilter internetbasierter Eindringversuche und Angriffe**, deren Ziel auf Ihren Webservern gehostete Anwendungen sind – und die sensiblen oder vertraulichen Daten, auf die diese Zugriff haben.

Der Barracuda-Vorteil

- Modernste Sicherheit durch Nutzung einer vollwertigen Reverse-Proxy-Architektur
- Malware-Schutz für kollaborative Webanwendungen
- Verwendung von IP-Reputationsinformationen zur Abwehr von DDoS-Angriffen
- Keine benutzerbasierte oder modulbasierte Lizenzierung
- Entwickelt, um Unternehmen die Einhaltung von Vorschriften wie PCI DSS und HIPAA zu erleichtern

Produktmerkmale

- Umfassender Schutz vor eingehenden Angriffen einschließlich der OWASP Top 10
- Integrierte Caching-, Komprimierungs- und TCP-Pooling-Funktionen zur Gewährleistung von Sicherheit ohne Leistungsverlust
- Identitätsbasierte Benutzerzugriffsteuerung für Webanwendungen
- Integrierter Schutz vor Datenverlust
- ICSA-zertifiziert

Dauerhafter Schutz vor sich weiterentwickelnden Bedrohungen

Die Barracuda Web Application Firewall bietet überragenden Schutz vor Datenverlust, DDoS-Angriffen und allen bekannten Angriffsmodalitäten auf Anwendungsebene. Automatische Updates bieten Schutz vor den neuesten Bedrohungen, sobald diese aufkommen. Mit dem Aufkommen neuer Bedrohungsarten werden neue Funktionen zur Blockierung dieser Bedrohungen integriert.

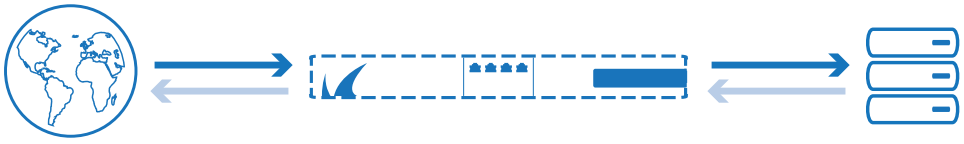
Identitäts- und Zugriffsmanagement

Die Barracuda Web Application Firewall verfügt über sichere Funktionen für die Benutzerauthentifizierung und Zugriffskontrolle, die die Sicherheit und den Datenschutz gewährleisten, indem sie den Zugriff auf sensible Anwendungen oder Daten auf autorisierte Benutzer beschränken.

Kostengünstig und benutzerfreundlich

Vorgefertigte Sicherheitsvorlagen und eine intuitive Web-Benutzeroberfläche bieten sofortige Sicherheit ohne zeitaufwendige Feineinstellungen oder Anwendungserlernprozesse. Durch die Integration von Sicherheitsschwachstellenscannern und SIEM-Tools werden Bewertung, Überwachung und Abwehrprozesse automatisiert.

Schutz für Server, Anwendungen und Daten vor webbasierten Angriffen.



→ Untersuchung eingehender Daten auf Layer-7-Angriffe

← Untersuchung ausgehender Daten zum Schutz vor Datendiebstahl

Durch den Einsatz der Barracuda Web Application Firewall zeigen wir unseren Kunden und Partnern, dass wir die Sicherheit Ihrer Daten ernst nehmen. Unsere Mitarbeiter müssen sich weniger um die Back-End-Sicherheit kümmern und können sich verstärkt auf die Bereitstellung qualitativ hochwertiger Services für unsere Partner und Kunden konzentrieren.

Michael Fainshtein
Chief Technology Officer
CredoRax.

Technische Details

Web Application Security
- OWASP-Top-10-Schutz
- Schutz vor gängigen Angriffen
  - SQL-Injektion
  - Cross-Site-Skripting
  - Manipulation von Cookies/Formularen
- Formularfeld-Metadatenvalidierung
- Anpassbare Sicherheit
- Website-Cloaking
- Response Control
- Schutz vor Diebstahl von ausgehenden Daten
  - Kreditkartennummern
  - Benutzerdefiniertes Pattern-Matching (regex)
- Granulare Richtlinien für HTML-Elemente
- Überprüfen von Protokollgrenzen
- Überprüfen von hochgeladenen Dateien
- Geo IP Location
  - Anonymer Proxy

DDoS Schutz
- Barracuda IP Reputationsdatenbank
- Heuristisches Fingerprinting
- CAPTCHA Aufgaben
- Slow-Client Schutz

Unterstützte Web Protokolle
- HTTP/S 0.9/1.0/1.1
- FTP/S
- XML
- IPv4/IPv6

Authentifizierung & Autorisierung
- LDAP-/RADIUS-/lokale Benutzerdatenbank
- SAML 2.0
- Clientzertifikate
- Single Sign-On
- Azure AD
- RSA SecurID
- CA SiteMinder
- SMS Passcode

Protokollierung, Überwachung & Reporting
- Systemprotokoll
- Web Firewall-Protokoll
- Zugriffsprotokoll
- Überwachungsprotokoll

SIEM-Integration
- ArcSight
- RSA enVision
- Splunk
- Symantec
- Anpassbar

Anwendungsbereitstellung & -beschleunigung
- Hochverfügbarkeit
- SSL-Offloading
- Load Balancing
- Content Routing

XML Firewall
- XML DOS Protection
- Schema-/WSDL-Durchsetzung
- WS-I-Konformitätsüberprüfungen

Netzwerk
- VLAN, NAT
- Network ACLs

Support-Optionen

Instant Replacement Service
- Austauschgeräteversand innerhalb eines Werktags
- Technischer 24-Stunden-Support
- Alle vier Jahre Hardware Refresh

Hardwaremerkmale
- FIPS 140-2 HSM-Modell verfügbar
- Optionaler Ethernet Bypass

Managementmerkmale
- Anpassbare, rollenbasierte Administration
- Integrierter Schwachstellenscanner
- Ausnahmeregelung für vertrauenswürdige Hosts

ICSA labs CERTIFIED

MODELLVERGLEICH	360	460	660	860	960
KAPAZITÄT					
Unterstützte Back-End-Server	1-5	5-10	10-25	25-150	150-300
Durchsatz	25 Mbps	50 Mbps	200 Mbps	1 Gbps	4 Gbps
HARDWARE					
Formfaktor	1U Mini	1U Mini	1U Fullsize	2U Fullsize	2U Fullsize
Abmessungen (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
Gewicht (kg)	5,4	5,4	11,8	20,9	23,6
Netzwerkanschlüsse	2 x 10/100	2 x GbE	2 x GbE	2 x GbE[1]	2 x 10GbE[1]
Management Port	1 x 10/100	1 x 10/100	1 x 10/100	1 x 10/100	1 x 10/100
AC-Eingangsstrom (A)	1,2	1,4	1,8	4,1	5,4
ECC-Arbeitsspeicher			●	●	●
MERKMALE					
Response Control	●	●	●	●	●
Schutz vor Diebstahl von ausgehenden Daten	●	●	●	●	●
Überprüfen von hochgeladenen Dateien	●	●	●	●	●
SSL-Offloading	●	●	●	●	●
Authentifizierung und Autorisierung	●	●	●	●	●
Integrierter Schwachstellenscanner	●	●	●	●	●
Schutz vor DDoS Angriffen	●	●	●	●	●
Netzwerk Firewall	●	●	●	●	●
Hochverfügbarkeit	Aktiv/Passiv	Aktiv/Passiv	Aktiv/Aktiv	Aktiv/Aktiv	Aktiv/Aktiv
Caching und Komprimierung		●	●	●	●
LDAP-/RADIUS-Integration		●	●	●	●
Load Balancing		●	●	●	●
Content Routing		●	●	●	●
Advanced Routing			●	●	●
Anpassbares Profiling			●	●	●
Antivirus für hochgeladene Dateien			●	●	●
XML Firewall			●	●	●

[1] Glasfaser NIC und Ethernet Hard Bypass verfügbar.

Diese Angaben können sich ohne Ankündigung ändern.