



Barracuda Web Application Firewall

Schützen Sie Anwendungen und Daten vor Advanced Threats.

Barracuda Web Application Firewall blockiert eine stetige wachsende Anzahl hochentwickelter webbasierter Eindringversuche und Angriffe, deren Ziel die auf Webservern gehosteten Anwendungen sowie die sensiblen und vertraulichen Daten, auf die diese Zugriff haben, sind. Barracuda Web Application Firewall befindet sich zwischen dem Internet und Webservern. Die Lösung scannt sowohl den gesamten eingehenden Web-Traffic, um Angriffe abzuwehren, als auch den ausgehenden Traffic, um einen hochwirksamen Schutz vor Datenverlust zu bieten.

Barracuda Web Application Firewall vereinfacht die Anwendungssicherheit, damit Sie sich auf Ihr Unternehmen konzentrieren können. Dank ihrer umfassenden Funktionen, ihrer vielseitigen Bereitstellungsoptionen sowie ihrer Benutzerfreundlichkeit können zahlreiche Anwendungssicherheitsaufgaben automatisiert werden – unabhängig davon, ob sich Ihre Web-Infrastruktur vor Ort, in einer virtualisierten Umgebung oder in der Cloud befindet.

Ständiger Schutz vor sich weiterentwickelnden Bedrohungen

Barracuda Web Application Firewall bietet höchsten Schutz vor Datenverlust, DDoS-Angriffen sowie allen bekannten und unbekanntem (Zero-Day-) Angriffsvektoren. Automatische Updates ermöglichen die Abwehr neuer Bedrohungen, sobald diese auftreten. Mit dem Aufkommen neuer Bedrohungsarten, werden neue Funktionen integriert, um diese Bedrohungen zu blockieren.

Vereinfachen Sie Identitäts- und Zugriffsverwaltung

Barracuda Web Application Firewall verfügt über sichere Funktionen für die Authentifizierung und Zugriffskontrolle, die für Sicherheit und Datenschutz sorgen, indem der Zugriff auf sensible Anwendungen oder Daten auf befugte Benutzer beschränkt wird.

Vereinfachung von Web-App-Security

Vorgefertigte Sicherheitsvorlagen und eine intuitive Web-Oberfläche bieten sofortige Sicherheit ohne zeitaufwendiges Abstimmen oder Erlernen von Anwendungen. Durch die Integration von Schwachstellen-Scannern und SIEM-Tools werden Bewertungs-, Monitoring- und Abwehrprozesse automatisiert.

Shared Services	Cloud-Erkennung und Cloud-Services (Threat Intelligence, Scan-Dienste für Anwendungen)				
Benutzerfreundlichkeit	Berichte und Analysen	Virtuelles Patching	Bootstrapping und Rehydrierung	Auto-Scaling	
Zugriffskontrolle	Authentifizierung		Autorisierung		
Sicherheit	OWASP Top 10 und andere	Schutz für APIs	Advanced-Bot-Protection	DDoS-Prävention	Advanced Threat Protection
App-Bereitstellung	Load Balancing	Caching und Komprimierung	Content-Routing	Traffic-Verschlüsselung	

API-gestützt und DevSecOps-fähig

Technische Details

MERKMALE	360	460	660	86X-SERIES	96X-SERIES	106X-SERIES
WEB-APPLICATION-SECURITY						
OWASP Top 10 – Web Application Security Schutz vor Risiken	✓	✓	✓	✓	✓	✓
Geo-IP und IP-Reputation (einschließlich öffentlicher Proxies und Tor-Nodes)	✓	✓	✓	✓	✓	✓
Intelligente Signaturen	✓	✓	✓	✓	✓	✓
Schutz vor Diebstahl ausgehender Daten (Kreditkarten, SSN, usw.)	✓	✓	✓	✓	✓	✓
Adaptive Profiling	-	-	✓	✓	✓	✓
Ausnahmenheuristik	✓	✓	✓	✓	✓	✓
Datei-Upload-Kontrolle	✓	✓	✓	✓	✓	✓
File Upload Security (Anti-Virus und Advanced Threat Protection) (für ATP ist eine Subscription erforderlich)	-	-	✓	✓	✓	✓
Website-Cloaking	✓	✓	✓	✓	✓	✓
Protokollprüfungen für HTTP- und HTTPS-Traffic	✓	✓	✓	✓	✓	✓
Granular nach URL-/Parameter-Richtlinien	✓	✓	✓	✓	✓	✓
Mengenregelung	-	-	✓	✓	✓	✓
API-SCHUTZ						
Schutz vor API-Sicherheitsrisiken der OWASP Top 10	Teilweise	Teilweise	✓	✓	✓	✓
API-Security (JSON)	✓	✓	✓	✓	✓	✓
API-Security (XML)	-	-	✓	✓	✓	✓
API-Discovery (JSON)	✓	✓	✓	✓	✓	✓
API-Discovery (XML)	-	-	✓	✓	✓	✓

MERKMALE	360	460	660	86X-SERIES	96X-SERIES	106X-SERIES
BOT-PROTECTION						
Schutz vor Web-Scraping einschließlich Datenbank bekannter Bots	✓	✓	✓	✓	✓	✓
Erweiterter Bot-Schutz mit cloud-basiertem maschinellem Lernen (ABP-Subscription erforderlich)	✓	✓	✓	✓	✓	✓
Bot-Spam-Schutz (Referrer- und Kommentar-Spam)	✓	✓	✓	✓	✓	✓
Formular-Spam-Schutz	-	-	✓	✓	✓	✓
Credential-Stuffing und -Spraying Schutz (ABP-Subscription erforderlich)	-	-	✓	✓	✓	✓
Brute-Force-Attack-Schutz	✓	✓	✓	✓	✓	✓
CAPTCHA-Support (intern, reCAPTCHA v2 und v3)	✓	✓	✓	✓	✓	✓
DDOS-SCHUTZ						
Volumetrischer DDoS-Schutz (ADP-Subscription erforderlich)	✓	✓	✓	✓	✓	✓
Application-DDoS-Protection	✓	✓	✓	✓	✓	✓
SICHERE ANWENDUNGSBEREITSTELLUNG						
TLS/SSL-Offloading	✓	✓	✓	✓	✓	✓
Load-Balancing und Content-Routing	-	✓	✓	✓	✓	✓
Netzwerk-HSM-Support	-	-	✓	✓	✓	✓
Dynamische URL-Verschlüsselung	-	-	✓	✓	✓	✓
HTTP/1.0, HTTP/1.1, HTTP/2.0, WebSocket (Passthrough), FTP/S und IPv6	✓	✓	✓	✓	✓	✓
Anfrage- und Antwortsteuerung (URL-Übersetzung)	✓	✓	✓	✓	✓	✓
Website-Übersetzungen	-	✓	✓	✓	✓	✓
Caching und Komprimierung	✓	✓	✓	✓	✓	✓
IDENTITÄTS- UND ZUGRIFFSKONTROLLE						
Lokale Benutzer/Gruppe (internes LDAP), Client-Zertifikate	✓	✓	✓	✓	✓	✓
Support: LDAP/Active Directory, RADIUS, OpenID Connect, Kerberos v5, SMS-Passcodes, Okta	-	✓	✓	✓	✓	✓
Integrationen: SAML, Azure AD, Duo Support, RSA SecurID	-	-	✓	✓	✓	✓
Azure AD	-	-	✓	✓	✓	✓
Single- und Multi-Domain-SSO aktivieren	✓	✓	✓	✓	✓	✓
MFA mit RADIUS/LDAP-basierten Services aktivieren	✓	✓	✓	✓	✓	✓
VIRTUELLES PATCHING UND FEEDBACK-LOOPS						
Barracuda Vulnerability Remediation Service	✓	✓	✓	✓	✓	✓
Support von virtuellem Patching für mehr als 20 Schwachstellen-Scanner	✓	✓	✓	✓	✓	✓

MERKMALE	360	460	660	86X-SERIES	96X-SERIES	106X-SERIES
PROTOKOLLIERUNG UND BERICHTE						
Onboard-Protokollierung (Web-Firewall-Protokolle, Zugriffsprotokolle, Audit- Protokolle, Netzwerk Firewall- Protokolle und System-Protokolle)	✓	✓	✓	✓	✓	✓
On-Demand- sowie vorausgeplantes Reporting mit mehr als 30 OOTB-Reports	✓	✓	✓	✓	✓	✓
Syslog-Export	✓	✓	✓	✓	✓	✓
SIEM/SOAR-Unterstützung (umfasst: Splunk, ARCSight, Azure Log Analytics, RSA enVision, IBM Qradar, Symantec, Sumologic, Loggly, Azure Event Hub und mehr)	✓	✓	✓	✓	✓	✓
NETWORKING UND HOCHVERFÜGBARKEIT						
VLAN- und NAT-Support	✓	✓	✓	✓	✓	✓
Network-ACL	✓	✓	✓	✓	✓	✓
Erweitertes Routing	-	-	✓	✓	✓	✓
Multi-Port-Hardware	-	-	-	✓	✓	✓
Link-Bonding	-	-	-	✓	✓	✓
Active/Passive Hochverfügbarkeit	✓	✓	✓	✓	✓	✓
Active/Active Hochverfügbarkeit	-	-	✓	✓	✓	✓
ADD-ON-SUBSCRIPTIONS						
Advanced-Bot-Protection	✓	✓	✓	✓	✓	✓
Aktive DDoS-Prävention	✓	✓	✓	✓	✓	✓
Advanced Threat Protection	-	-	✓	✓	✓	✓

MERKMALE	360	460	660	860	861	862
MODELLVERGLEICH						
Durchsatz	25 Mbit/s	50 Mbit/s	200 Mbit/s	1 Gbit/s	1 Gbit/s	1 Gbit/s
Max. Backend-Server (empfohlen)	5	10	25	150	150	150
HTTP-Transaktionen pro Sekunde	8000	15000	30000	90000	90000	90000
HTTP-Verbindungen pro Sekunde	2000	3000	10000	16000	16000	16000
HTTPS-Transaktionen pro Sekunde	2500	4000	12000	30000	30000	30000
Gleichzeitige Verbindungen	90000	150000	500000	950000	950000	950000
HARDWARE-SPEZIFIKATIONEN						
Formfaktor	1U-Mini	1U-Mini	1 U	1 U	1 U	1 U
„Abmessungen (in Zoll) B x T x H“	17,2 x 1,7 x 1,4	17,2 x 1,7 x 1,4	17,2 x 1,7 x 22,6	17,2 x 22,4 x 1,73	17,2 x 22,4 x 1,73	17,2 x 22,4 x 1,73
Gewicht (lbs)	12	12	26	26,45	26,45	26,45
ECC-Arbeitsspeicher	-	-	-	Ja	Ja	Ja
Management-Port	10 100 1000	10 100 1000	10 100 1000	10 100 1000	10 100 1000	10 100 1000
Ethernet-Anschlüsse	2 x 10/100 RJ45 mit Bypass	-	-	-	-	-
Gigabit-Ethernet-Ports	-	2 x 1 G RJ45 mit Bypass	2 x 1 G RJ45 mit Bypass	8 x 1 G RJ45	8 x 1 G RJ45 mit Bypass	8 x 1 G SFP (MM) mit Bypass
10 Gigabit-Ethernet-Ports	-	-	-	-	-	-
Stromversorgung	1	1	1	2	2	2
AC-Eingangstrom (Ampere)	1,2	1,4	1,8	4,2	4,2	4,2
Wärmeabgabe (BTU/Std.)	490	575	740	967,78	967,78	1001,91
Betriebs-temperatur	5 °C – 35 °C (41 °F – 95 °F)	5 °C – 35 °C (41 °F – 95 °F)	5 °C – 35 °C (41 °F – 95 °F)	„0 ~ 40 °C (32 ~ 104 °F)“	„0 ~ 40 °C (32 ~ 104 °F)“	„0 ~ 40 °C (32 ~ 104 °F)“
Relative Luftfeuchtigkeit beim Betrieb	8 % ~ 90 % (nicht-kondensierend)	8 % ~ 90 % (nicht-kondensierend)	8 % ~ 90 % (nicht-kondensierend)	„10 ~ 85 % relative Luftfeuchtigkeit“	„10 ~ 85 % relative Luftfeuchtigkeit“	„10 ~ 85 % relative Luftfeuchtigkeit“
Sicherheits- und EMC-Zertifizierungen	Auf Anfrage verfügbar	Auf Anfrage verfügbar	„EN 60950 FCC, CE“	„EN 60950 FCC, CE“	„EN 60950 FCC, CE“	„EN 60950 FCC, CE“

MERKMALE	960	961	964	1060	1061	1062
Durchsatz	5 Gbit/s	5 Gbit/s	5 Gbit/s	10 Gbit/s	10 Gbit/s	10 Gbit/s
Max. Backend-Server (empfohlen)	300	300	300	600	600	600
HTTP-Transaktionen pro Sekunde	180000	180000	180000	190000	190000	190000
HTTP-Verbindungen pro Sekunde	30000	30000	30000	70000	70000	70000
HTTPS-Transaktionen pro Sekunde	50000	50000	50000	70000	70000	70000
Gleichzeitige Verbindungen	1800000	1800000	1800000	2800000	2800000	2800000
HARDWARE-SPEZIFIKATIONEN						
Formfaktor	1 U	1 U	1 U	2 U	2 U	2 U
„Abmessungen (in Zoll) B x T x H“	17,2 x 22,4 x 1,73	17,2 x 22,4 x 1,73	17,2 x 22,4 x 1,73	17,4 x 3,5 x 25,5	17,4 x 3,5 x 25,5	17,4 x 3,5 x 25,5
Gewicht (lbs)	26,45	26,45	26,45	52	52	52
ECC-Arbeitsspeicher	Ja	Ja	Ja	Ja	Ja	Ja
Management-Port	10 100 1000	10 100 1000	10 100 1000	10 100 1000	10 100 1000	10 100 1000
Ethernet-Anschlüsse	-	-	-	-	-	-
Gigabit-Ethernet-Ports	8 x 1 G RJ45	8 x 1 G RJ45 mit Bypass	8 x 1 G SFP (MM) mit Bypass	16 x 1 G RJ45	8 x 1 G RJ45 mit Bypass	8 x 1 G Glasfaser mit Bypass
10 Gigabit-Ethernet-Ports	2 x 10 G RJ45	2 x 10 G RJ45 mit Bypass	2 x 10 G SFP+ (MM) mit Bypass	4 x 10 G RJ45	4 x 10 G RJ45 mit Bypass	4 x 10 G Glasfaser mit Bypass
Stromversorgung	2	2	2	2	2	2
Leistungsaufnahme AC (Ampere)	4,2	4,2	4,2	5,4	5,4	5,4
Wärmeleistung (BTU/h)	1003,8	1003,8	1044,38	2200	2200	2200
Betriebstemperatur	„0 ~ 40 °C (32 ~ 104 °F)“	„0 ~ 40 °C (32 ~ 104 °F)“	„0 ~ 40 °C (32 ~ 104 °F)“	5 °C – 35 °C (41 °F – 95 °F)	5 °C – 35 °C (41 °F – 95 °F)	5 °C – 35 °C (41 °F – 95 °F)
Relative Luftfeuchtigkeit beim Betrieb	„10 ~ 85 % relative Luftfeuchtigkeit“	„10 ~ 85 % relative Luftfeuchtigkeit“	„10 ~ 85 % relative Luftfeuchtigkeit“	8 % ~ 90 % (nicht kondensierend)	8 % ~ 90 % (nicht kondensierend)	8 % ~ 90 % (nicht kondensierend)
Sicherheits- und EMC-Zertifizierungen	„EN 60950 FCC, CE“	„EN 60950 FCC, CE“	„EN 60950 FCC, CE“	„EN 60950 FCC, CE“	„EN 60950 FCC, CE“	„EN 60950 FCC, CE“

Support-Optionen

Sofortiger Ersatzservice

- Versand eines Ersatzgeräts am nächsten Arbeitstag
- Technischer Support rund um die Uhr
- Hardware-Upgrade alle vier Jahre

Barracuda Energize Updates

- Technischer Standardsupport
- Firmware-Updates und Nachrüstungen nach Bedarf
- Automatische Aktualisierung von Anwendungsdefinitionen

Verwaltungsfunktionen

- Individuelle, rollenbasierte Administration
- Schwachstellen-Scanner-Integration
- Trusted-Host-Ausnahme
- Rest-API
- Benutzerdefinierte Vorlagen
- Interaktive und vorausgeplante Berichte

