



Barracuda Web Application Firewall

Leistungstarker Schutz auf Applikations-Ebene für Websites und Webserver.

Die Barracuda Web Application Firewall schützt Websites und Webanwendungen vor Angreifern, die Protokoll- oder Anwendungsschwächen nutzen, um Datendiebstahl, Denial-of-Service oder die Verunstaltung von Unternehmens-Websites anzuzetteln. Im Gegensatz zu traditionellen Firewalls oder Intrusion Detection-Systemen, die HTTP-, HTTPS- oder FTP-Datenverkehr für Webanwendungen einfach weitergeben, übernimmt die Barracuda Web Application Firewall für diesen Verkehr eine Proxyfunktion und überprüft ihn auf Angriffe, um Webserver vor dem direkten Zugriff durch Hacker zu schützen.

Umfassender Schutz für Websites

Die Barracuda Web Application Firewall bietet preisgekrönten Schutz vor allen bekannten Bedrohungen für Webanwendungen, inklusive SQL-Injections, Cross-Site-Scripting, Session Tempering und Buffer Overflows. Als vollwertiger Proxy blockiert oder stoppt die Barracuda Web Application Firewall Angriffe und schützt gleichzeitig sensible ausgehende Daten, wie z. B. Kreditkartendaten und Sozialversicherungsnummern.

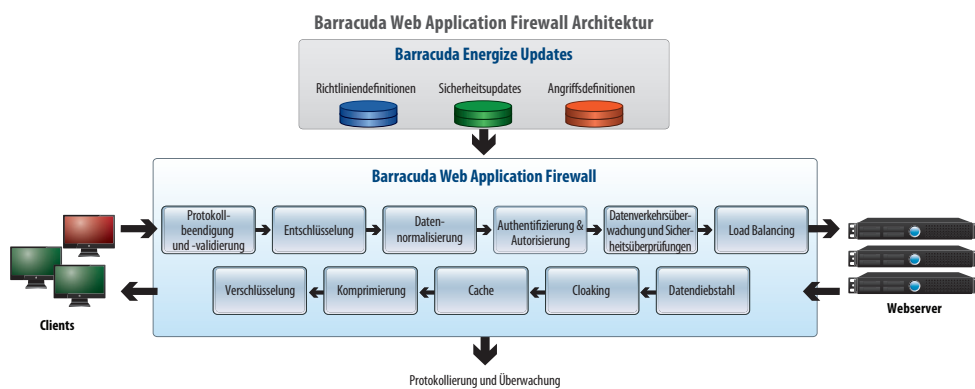
Des Weiteren entschärft die Barracuda Web Application Firewall beeinträchtigte Zugriffskontrollen auf Applikationen, indem die Manipulation von Cookies und die Beschädigung des Zugriffskontrollsystems einer Anwendung verhindert werden. Im Gegensatz zu Intrusion Detection-Systemen, die lediglich nach Mustern analysieren, beendet die Barracuda Web Application Firewall HTTP-Datenverkehr im Namen des Webserver, um Zeichensätze zu entschlüsseln, Padded Spacing zu entfernen und gängige Techniken zur Codetarnung zu normalisieren. Für zusätzlichen Schutz bietet die Barracuda Web Application Firewall vollständige PKI-Integration zur Verwendung mit Clientanwendungen, um die Identität von Clients zu überprüfen, die auf die Webanwendungen zugreifen.

Fortschrittliches Traffic Management und Acceleration

Um den Administrationsaufwand zu minimieren, der beim Schutz von Websites vor Anwendungsschwachstellen entsteht, empfängt die Barracuda Web Application Firewall automatisch Energize Updates mit den neuesten Richtlinien-, Sicherheits- und Angriffsdefinitionen. Neben den umfassenden Sicherheitsvorteilen gibt es zudem Funktionen für die Anwendungsbereitstellung, wie z. B. SSL-Offloading, SSL-Acceleration und Load Balancing. Mit diesen Funktionen können Sie die Leistung, Skalierbarkeit und den Verwaltungsaufwand für die heutigen äußerst anspruchsvollen Datacenter-Infrastrukturen optimieren.



Die Barracuda Web Application Firewall überwacht und zeichnet gängige Applikations-Angriffe, Leistungsstatistiken und Bandbreitennutzung auf.



- MODELL**
- 360
 - 460
 - 660
 - 860
 - 960



BARRACUDA WEB APPLICATION FIREWALL

MODELL
360
460
660
860
960



Typisches Szenario



Internet

Firewall

Barracuda Web Application Firewall

Webserver

TECHNISCHE DETAILS

Hauptmerkmale

UNTERSTÜTZTE WEB-PROTOKOLLE

- HTTP/S 0.9/1.0/1.1
- FTP/S
- XML
- IPv6 Ready

WEB APPLICATION SECURITY

- OWASP-Top-Ten-Schutz
- Schutz vor gängigen Angriffen
 - SQL-Injektion
 - OS-Command Injection
 - Cross-Site-Skripting
 - Manipulation von Cookies oder Formularen
- Formularfeld-Metadatenvalidierung
- Anpassbare Sicherheit
- Website-Cloaking
- Response Control
 - Sperren von Clients
 - Zurücksetzen der Verbindung
 - Umleiten
 - Benutzerdefinierte Antwort
- Schutz vor Diebstahl von ausgehenden Daten
 - Kreditkartennummern
 - Sozialversicherungsnummern

WEB APPLICATION SECURITY (FORTS.)

- Benutzerdefiniertes Pattern-Matching (regex)
- Granulare Richtlinien für HTML-Elemente
- Überprüfung von Protokollgrenzen
- Überprüfen von hochgeladenen Dateien
- Schutz vor Brute-Force-Angriffen
- Session Tracking

AUTHENTIFIZIERUNG UND AUTORISIERUNG

- LDAP-/RADIUS-/lokale Benutzerdatenbank
- Clientzertifikate
- Single Sign-On
- RSA SecurID²
- CA SiteMinder²

PROTOKOLLIERUNG, ÜBERWACHUNG UND REPORTING

- Systemprotokoll
- Web Firewall-Protokoll
- Zugriffsprotokoll
- Überwachungsprotokoll

SIEM-INTEGRATION

- ArcSight

RSA ENVISION

- Splunk
- Symantec

ANWENDUNGSBEREITSTELLUNG UND -BESCHLEUNIGUNG

- Hochverfügbarkeit
- SSL-Offloading
- Load Balancing
- Content Routing

XML FIREWALL

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

Systemmerkmale

- Grafische Benutzeroberfläche
- Rollenbasierte Administration
- Sichere Remote-Administration
- Optionale Ethernet-Umgehung
- Ausnahmeregelung für vertrauenswürdige Hosts
- Integrierter Schwachstellenscanner

Hardwaremerkmale

ANSCHLUSSMÖGLICHKEITEN

- WAN/LAN/MGMT ports
- Serieller Anschluss (DB-9) für Konsolen

HARDWARESICHERHEITSMODUL

- FIPS 140-2 HSM-Modell verfügbar

STROMVERSORGUNG

- AC-Eingangsspannung - 110-240 VAC
- Frequenz - 50/60 Hz

Virtual Appliance-Modelle

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

Supportoptionen

- Energize Updates-Abonnement
- Instant Replacement-Service

MODELLVERGLEICH	MODELL 360	MODELL 460	MODELL 660	MODELL 860	MODELL 960
KAPAZITÄT*					
Unterstützung von Back-End-Servern	1-5	5-10	10-25	25-150	150-300
Durchsatz	25 Mbps	50 Mbps	100 Mbps	600 Mbps	1 Gbps
HARDWARE					
Rackmount-Gehäuse	1U Mini	1U Mini	1U Fullsize	2U Fullsize	2U Fullsize
Abmessungen (Zoll)	16,8 x 1,7 x 14	16,8 x 1,7 x 14	16,8 x 1,7 x 22,6	17,4 x 3,5 x 25,5	17,4 x 3,5 x 25,5
Abmessungen (cm)	42,7 x 4,3 x 35,6	42,7 x 4,3 x 35,6	42,7 x 4,3 x 57,4	44,2 x 8,9 x 64,8	44,2 x 8,9 x 64,8
Gewicht (lbs/kg)	12 / 5,4	12 / 5,4	26 / 11,8	46 / 20,9	52 / 23,6
Netzwerkanschlüsse					
Kupfer-NIC (Standard)	2 x 10/100	2 x Gigabit	2 x Gigabit	2 x Gigabit	2 x Gigabit
Glasfaser-NIC (Optional) ¹				2 x Gigabit	2 x Gigabit
Verwaltungsanschluss	1 x 10/100	1 x 10/100	1 x Gigabit	1 x Gigabit	1 x Gigabit
AC-Eingangsstrom (A)	1,2	1,4	1,8	4,1	5,4
ECC-Arbeitsspeicher			✓	✓	✓
MERKMALE					
HTTP-/HTTPS-/FTP-Protokollvalidierung	✓	✓	✓	✓	✓
Schutz vor gängigen Angriffen	✓	✓	✓	✓	✓
Formularfeld-Metadatenvalidierung	✓	✓	✓	✓	✓
Website-Cloaking	✓	✓	✓	✓	✓
Antwortsteuerung	✓	✓	✓	✓	✓
Schutz vor Diebstahl von ausgehenden Daten	✓	✓	✓	✓	✓
Granulare Richtlinien für HTML-Elemente	✓	✓	✓	✓	✓
Überprüfen von hochgeladenen Dateien	✓	✓	✓	✓	✓
Protokollierung, Überwachung und Reporting	✓	✓	✓	✓	✓
Hohe Verfügbarkeit	✓	✓	✓	✓	✓
SSL-Offloading	✓	✓	✓	✓	✓
Authentifizierung und Autorisierung	✓	✓	✓	✓	✓
Integrierter Schwachstellenscanner	✓	✓	✓	✓	✓
Zentrale Verwaltung	✓	✓	✓	✓	✓
Caching und Komprimierung		✓	✓	✓	✓
LDAP-/RADIUS-Integration		✓	✓	✓	✓
Load Balancing		✓	✓	✓	✓
Inhalts-Routing		✓	✓	✓	✓
Anpassbares Profiling			✓	✓	✓
AV für hochgeladene Dateien			✓	✓	✓
XML Firewall			✓	✓	✓

DE 15.3

Diese Angaben können sich ohne Ankündigung ändern.

* Die Kapazität hängt von der Umgebung und ausgewählten Optionen ab.

¹ Glasfaser-NIC-Option ersetzt die standardmäßigen 2x-Kupfer-Gigabit-Ports durch 2x-Glasfaser-Gigabit-Ports.

² Verfügbar für die Modelle 660 und höher.

¹ Virtual Appliances sind auch für VMware ESX/ESXi-, VMware Server-, Citrix XenServer-, Microsoft Hyper-V- und Oracle VirtualBox-Umgebungen verfügbar.

Rufen Sie an, um weitere Informationen zu erhalten.