

Barracuda Web Application Firewall

Защитите приложения и данные от дополнительных угроз



Barracuda Web Application Firewall **блокирует по непрерывно расширяющемуся списку изощренных вторжений и сетевых атак**, которые нацелены на приложения, размещенные на ваших веб-серверах – и на секретные или конфиденциальные данные, к которым у них имеется доступ.

- ✓ **Безопасность**
- Хранение
- ✓ **Доставка приложений**

Преимущества Barracuda

- Безопасность самого современного уровня, использующая архитектуру полного реверсного проксирования
- Защита от вредоносного кода для веб-приложений совместного использования
- Использует разведку на основе репутации по IP для ликвидации DDoS атак
- Без лицензирования по каждому пользователю или по каждому модулю
- Разработан для облегчения соответствия вашей организации положениям PCI, DSS и HIPAA
- Облачное сканирование с менеджером уязвимостей Barracuda Vulnerability Manager
- Автоматическое исправление уязвимостей

Ключевые характеристики

- Комплексная защита от входящих атак, включая OWASP Top 10
- Встроенное кэширование, сжатие и создание пула TCP обеспечивают безопасность без воздействия на производительность
- Контроль доступа пользователей к веб-приложениям на основе идентификаторов
- Встроенное предотвращение потери данных
- Сертифицировано ICISA



Постоянная защита от развивающихся угроз

Безопасность приложений, обеспечиваемая брандмауэром веб-приложений Barracuda Web Application Firewall, предоставляет высочайшую защиту от потерь данных, DDoS, и всех известных атак на уровне приложений. Автоматические обновления обеспечивают защиту от новых угроз по мере их возникновения. По мере возникновения новых типов угроз появляются новые возможности их блокирования.



Управление идентификацией и доступом

Брандмауэр веб-приложений Barracuda Web Application Firewall обладает мощными возможностями по управлению аутентификацией и контролем доступа, которые обеспечивают безопасность и конфиденциальность путем ограничения доступа к приложениям, требующим защиты или данным авторизованных пользователей.



Доступный по цене и легкий в использовании

Предустановленные шаблоны безопасности, а также интуитивный веб-интерфейс обеспечивают немедленную безопасность без необходимости длительной настройки или изучения приложения. Интеграция со сканерами уязвимостей и инструментами SIEM автоматизирует оценку, мониторинг и процесс ликвидации угроз.

Защитите серверы, приложения и данные от сетевых атак.



Интернет



Barracuda Web Application Firewall



Сервер



Входящая проверка атак 7 уровня



Исходящая проверка для защиты от кражи данных

Установив брандмауэр веб-приложений Barracuda Web Application Firewall мы показываем нашим клиентам и партнерам, что мы серьезно относимся к безопасности их данных. Он позволяет нашим сотрудникам меньше беспокоиться о внутренней безопасности и сосредоточиться на предоставлении качественных услуг нашим партнерам и клиентам.

Майкл Файнштейн
Технический руководитель
CredoRax

Технические характеристики

Технические характеристики

- Безопасность веб-приложений
- Защита в Топ 10 по OWASP
- Защита от обычных атак
 - Внедрение SQL кода
 - Межсайтовый скриптинг
 - Несанкционированное вмешательство в файлы куки или формы
- Проверка метаданных полей форм
- Адаптивная безопасность
- Маскирование веб-сайта
- Шифрование URL
- Контроль за реакцией
- Проверка полезной нагрузки JSON
- Защита от веб-агрегаторов
- Защита от исходящей кражи данных
 - Номера кредитных карт
 - Совпадение пользовательских шаблонов (regex)
- Выборочные политики по элементам HTML
- Проверки ограничений протоколов
- Контроль загрузки файлов
- Топопривязка по IP
 - Анонимный прокси
- Блокирование Tor

Сетевой режим

- VLAN, NAT
- Сетевые ACL
- Усовершенствованная маршрутизация

Поддерживаемые веб-протоколы

- HTTP/5 0.9/1.0/1.1/2.0
- WebSocket
- FTP/S
- XML
- IPv4/IPv6

Аутентификация/санкционирование

- LDAP/RADIUS/база данных местных пользователей
- SAML 2.0
- Сертификаты клиента
- Система единого входа
- Azure AD
- RSA SecurID
- SMS Passcode
- Kerberos v5
- Поддержка нескольких доменов

Защита от DDoS

- Интеграция с брандмауэром Barracuda NextGen для блокирования вредоносных IP
- Репутационная база данных IP Barracuda
- Эвристический анализ отпечатков пальцев
- Задания капчи
- Защита медленных клиентов
- Выходные узлы ToR
- Черный список Barracuda

Интеграция SIEM

- HP ArcSight
- RSA enVision
- Splunk
- Symantec
- Microsoft Azure Event Hub
- Настраиваемое

Доставка приложений и ускорение

- Высокая доступность
- Выгрузка SSL
- Распределение нагрузки
- Маршрутизация содержимого

Брандмауэр XML

- Защита XML DOS
- Применение Schema/WSDL
- Проверки на соответствие WS-I

Ведение журнала, мониторинг и отчетность

- Репутационная база данных IP Barracuda
- Эвристический анализ отпечатков пальцев
- Задания капчи
- Защита медленных клиентов

Опции поддержки

- Служба мгновенной замены**
 - Отгрузка замены блока на следующий рабочий день
 - Круглосуточная техническая поддержка
 - Обновление оборудования каждые четыре года

Параметры оборудования

- Доступность модели FIPS 140-2 HSM
- Опция обхода Ethernet

Функции управления

- Настраиваемое ролевое администрирование
- Интеграция сканера уязвимостей
- Исключение доверенных хостов
- Rest API
- Пользовательские шаблоны
- Интерактивные и запланированные отчеты



СРАВНЕНИЕ МОДЕЛЕЙ	360	460	660	860	960
ЕМКОСТЬ					
Поддержка внутренних серверов	1-5	5-10	10-25	25-150	150-300
Пропускная способность	25 Мб/с	50 Мб/с	200 Мб/с	1 Гб/с	5 Гб/с
ОБОРУДОВАНИЕ					
Форм фактор	1U Mini	1U Mini	1U Fullsize	2U Fullsize	2U Fullsize
Размеры (дюйм)	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
Вес (фунт)	12	12	26	46	52
Порты передачи данных	2 x 10/100	2 x GbE	2 x GbE	8 x GbE ¹	8 x GbE ¹ ; 2 x 10GbE ¹
Порт управления	1 x 10/100	1 x 10/100	1 x 10/100/1000	1 x 10/100/1000	1 x 10/100/1000
Сила входящего переменного тока (ампер)	1,2	1,4	1,8	4,1	5,4
Память ECC					
ХАРАКТЕРИСТИКИ					
Контроль за реакцией	•	•	•	•	•
Расширенная защита от угроз ²			•	•	•
Защита кражи исходящих данных	•	•	•	•	•
Контроль загрузки файлов	•	•	•	•	•
Выгрузка SSL	•	•	•	•	•
Авторизация и аутентификация	•	•	•	•	•
Встроенный сканер уязвимостей	•	•	•	•	•
Защита от DDoS атак	•	•	•	•	•
Защита от веб-агрегаторов	•	•	•	•	•
Сетевой брандмауэр	•	•	•	•	•
Высокая доступность	Активный/пассивный	Активный/пассивный	Активный/активный	Активный/активный	Активный/активный
Безопасность JSON	•	•	•	•	•
Кэширование и сжатие		•	•	•	•
Интеграция LDAP/RADIUS		•	•	•	•
Распределение нагрузки		•	•	•	•
Маршрутизация содержания		•	•	•	•
Адаптивное профилирование			•	•	•
Антивирус для загрузок файлов			•	•	•
Шифрование URL			•	•	•
Брандмауэр XML			•	•	•

¹ Доступны опции оптоволоконного NIC и жесткого обхода Ethernet. Характеристики могут быть изменены без уведомления.

² Требуется активная подписка на Продвинутое обеспечение безопасности от угроз