



Брандмауэр веб-приложений Barracuda Web Application Firewall Vx

Заштите приложения и данные от продвинутых угроз.

Брандмауэр веб-приложений Barracuda Web Application Firewall Vx блокирует угрозы по непрерывно расширяющемуся списку усовершенствованных веб-вторжений и атак, которые нацелены на приложения, размещенные на ваших веб-серверах, а также на чувствительные или конфиденциальные данные, к которым у приложений имеется доступ. Брандмауэр веб-приложений Barracuda Web Application Firewall Vx, действующий между сетью Интернет и веб-серверами, сканирует весь входящий сетевой трафик с целью блокирования атак, а также сканирует исходящий трафик с целью высокоеффективного предотвращения потери данных.

Брандмауэр веб-приложений Barracuda Web Application Firewall Vx облегчает задачу обеспечения безопасности приложений, позволяя вам вместо этого сосредоточиться на вашем бизнесе. Благодаря исчерпывающему набору функций, наличию разнообразных вариантов развертывания и простоте использования брандмауэр позволяет автоматизировать многие задачи обеспечения безопасности приложений.

Постоянная защита от развивающихся угроз

Брандмауэр веб-приложений Barracuda Web Application Firewall Vx обеспечивает непревзойденную защиту от потерь данных, DDoS, а также от атак на приложения по всем известным и неизвестным направлениям (атак нулевого дня). Автоматические обновления обеспечивают защиту от новых угроз по мере их возникновения. По мере возникновения новых типов угроз брандмауэр приобретает новые способности по их блокированию.

Управление идентификацией и доступом

Брандмауэр веб-приложений Barracuda Web Application Firewall Vx обладает мощными возможностями по управлению аутентификацией и контролю доступа, которые обеспечивают безопасность и конфиденциальность путем ограничения доступа, предоставляя доступ к чувствительным приложениям или данным только авторизованным пользователям.

Доступен по цене и прост в использовании

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

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ	360VX	460VX	660VX	760VX	860VX	960VX
БЕЗОПАСНОСТЬ ВЕБ-ПРИЛОЖЕНИЙ						
Защита от 10 серьезнейших угроз безопасности веб-приложений по версии OWASP	✓	✓	✓	✓	✓	✓
Определение местонахождения по IP и репутация IP (включая публичные прокси-сервера и узлы Tor)	✓	✓	✓	✓	✓	✓
Интеллектуальные подписи	✓	✓	✓	✓	✓	✓
Защита от кражи исходящих данных (кредитные карты, номера социального страхования и т.д.)	✓	✓	✓	✓	✓	✓
Адаптивное профилирование	-	-	✓	✓	✓	✓
Эвристика исключений	✓	✓	✓	✓	✓	✓
Двигок автоматического конфигурирования (требуется подписка на продвинутую защиту от ботов – ABP)	✓	✓	✓	✓	✓	✓
Контроль загрузки файлов	✓	✓	✓	✓	✓	✓
Антивирус для защиты при загрузке файлов	-	-	✓	✓	✓	✓
Продвинутая защита от угроз при загрузке файлов (требуется подписка на продвинутую защиту от угроз – ATP)	-	-	✓	✓	✓	✓
Маскирование веб-сайта	✓	✓	✓	✓	✓	✓
Проверки ограничений протоколов	✓	✓	✓	✓	✓	✓
Политики, детально конфигурируемые по URL-адресам / параметрам	✓	✓	✓	✓	✓	✓
Управление скоростью	-	-	✓	✓	✓	✓
Защита на стороне клиента (требуется лицензия на продвинутую защиту от ботов – ABP)	✓	✓	✓	✓	✓	✓
ЗАЩИТА API						
Защита от 10 серьезнейших угроз безопасности API по версии OWASP	-	-	✓	✓	✓	✓
Безопасность API (JSON)	✓	✓	✓	✓	✓	✓
Безопасность API (XML)	✓	✓	✓	✓	✓	✓
Обнаружение API (JSON)	-	✓	✓	✓	✓	✓
Обнаружение API (XML)	✓	✓	✓	✓	✓	✓
ЗАЩИТА ОТ БОТОВ						
Защита от веб-скрипинга	✓	✓	✓	✓	✓	✓
Продвинутая защита от ботов с использованием машинного обучения на основе облачных вычислений (требуется подписка на продвинутую защиту от ботов – ABP)	✓	✓	✓	✓	✓	✓
Разведка активных угроз (требуется лицензия на продвинутую защиту от ботов – ABP)	✓	✓	✓	✓	✓	✓
База данных известных ботов	-	-	✓	✓	✓	✓
Защита от спама ботами (реферальный спам и спам в комментариях)	✓	✓	✓	✓	✓	✓
Защита от спама через формы	-	-	✓	✓	✓	✓
Защита от ввода скомпрометированных идентификационных данных и вброса вредоносного кода в память (требуется подписка на продвинутую защиту от ботов – ABP)	-	-	✓	✓	✓	✓
Защита от брутфорса	✓	✓	✓	✓	✓	✓
Поддержка CAPTCHA	✓	✓	✓	✓	✓	✓
Поддержка reCAPTCHAv2/v3	✓	✓	✓	✓	✓	✓
ЗАЩИТА ОТ DDOS-АТАК						
Защита от объемных DDoS-атак (требуется подписка на продвинутую защиту от DDoS-атак – ADP)	✓	✓	✓	✓	✓	✓
Защита от DDoS-атак на приложения	✓	✓	✓	✓	✓	✓

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ	360VX	460VX	660VX	760VX	860VX	960VX
БЕЗОПАСНАЯ ДОСТАВКА ПРИЛОЖЕНИЙ						
Разгрузка TLS/SSL	✓	✓	✓	✓	✓	✓
Распределение нагрузки	-	✓	✓	✓	✓	✓
Маршрутизация содержания	-	✓	✓	✓	✓	✓
Поддержка сетевых модулей аппаратной защиты (HSM)	-	-	✓	✓	✓	✓
Динамическое шифрование URL-адресов	-	✓	✓	✓	✓	✓
Поддержка HTTP/1.0, HTTP/1.1, HTTP/2.0, WebSocket, FTP/S и IPv6	✓	✓	✓	✓	✓	✓
Поддержка FTP/S	✓	✓	✓	✓	✓	✓
Поддержка IPv6	✓	✓	✓	✓	✓	✓
Контроль запросов и ответов (перевод URL-адресов)	✓	✓	✓	✓	✓	✓
Переводы веб-сайтов	-	✓	✓	✓	✓	✓
Кэширование и сжатие	✓	✓	✓	✓	✓	✓
УПРАВЛЕНИЕ ИДЕНТИФИКАЦИЕЙ И ДОСТУПОМ						
Локальные пользователи / группы (внутренний протокол LDAP)	✓	✓	✓	✓	✓	✓
Сертификаты клиента	✓	✓	✓	✓	✓	✓
LDAP / Active Directory	-	✓	✓	✓	✓	✓
RADIUS	-	✓	✓	✓	✓	✓
SAML	-	-	✓	✓	✓	✓
Поддержка OpenID Connect и JWT	-	-	✓	✓	✓	✓
Kerberos v5	-	✓	✓	✓	✓	✓
Azure AD	-	-	✓	✓	✓	✓
Возможность включения одно- и многодоменного механизма единого входа (SSO)	✓	✓	✓	✓	✓	✓
Интеграция кодов доступа по SMS	-	✓	✓	✓	✓	✓
Интеграция RSA SecurID	-	-	✓	✓	✓	✓
Возможность включения многофакторной аутентификации для служб на основе RADIUS / LDAP	-	✓	✓	✓	✓	✓
Интеграция Duo (SAML)	-	-	✓	✓	✓	✓
Интеграция Okta (OpenID Connect)	-	-	✓	✓	✓	✓
ВИРТУАЛЬНАЯ УСТАНОВКА ПАТЧЕЙ И КОНТУРЫ ОБРАТНОЙ СВЯЗИ						
Менеджер уязвимостей Barracuda	✓	✓	✓	✓	✓	✓
Служба отчетности об уязвимостях Barracuda	✓	✓	✓	✓	✓	✓
Поддержка виртуальной установки патчей для 20+ сканеров уязвимостей	✓	✓	✓	✓	✓	✓
ВЕДЕНИЕ ЖУРНАЛОВ И ОТЧЕТНОСТЬ						
Встроенное ведение журналов (журналы брандмаузеров веб-приложений, журналы доступа, журналы аудита, журналы сетевых брандмаузеров и системные журналы)	✓	✓	✓	✓	✓	✓
Отчетность по запросу и по графику, включающая 30+ готовых отчетов	✓	✓	✓	✓	✓	✓
Экспорт системных журналов	✓	✓	✓	✓	✓	✓
Экспорт AMQP/AMQPS	✓	✓	✓	✓	✓	✓
Центр событий Azure	✓	✓	✓	✓	✓	✓
Облачные службы системных журналов	✓	✓	✓	✓	✓	✓

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ	360VX	460VX	660VX	760VX	860VX	960VX
Поддержка SIEM/SOAR (включает в себя: Splunk, ARCsight, Azure Sentinel, RSA enVision, IBM QRadar, Symantec, Sumologic, Loggly и другое)	✓	✓	✓	✓	✓	✓
ОРГАНИЗАЦИЯ СЕТИ И ВЫСОКАЯ ДОСТУПНОСТЬ						
Поддержка VLAN и NAT	✓	✓	✓	✓	✓	✓
Списки управления доступом (ACL) к сети	✓	✓	✓	✓	✓	✓
Усовершенствованная маршрутизация	-	-	✓	✓	✓	✓
Многопортовое аппаратное обеспечение	-	-	-	-	✓	✓
Высокая доступность в конфигурации с одним доступным сервером («активный-пассивный»)	✓	✓	✓	✓	✓	✓
Высокая доступность в конфигурации с двумя доступными серверами («активный-активный»)	-	-	-	-	✓	✓
ДОПОЛНИТЕЛЬНЫЕ ПОДПИСКИ						
Продвинутая защита от ботов	✓	✓	✓	✓	✓	✓
Активное предотвращение DDoS-атак	✓	✓	✓	✓	✓	✓
Продвинутая защита от угроз	-	-	✓	✓	✓	✓

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ	360VX	460VX	660VX	760VX	860VX	960VX
РАБОЧИЕ ХАРАКТЕРИСТИКИ						
Пропускная способность	25 Мб/с	50 Мб/с	200 Мб/с	500 Мб/с	1 Гб/с	5 Гб/с
Макс. количество серверов обработки бизнес-логики (рекомендованное)	5	10	25	50	150	300
Поддерживаемое количество ядер центрального процессора	2	4	6	8	10	12
Количество транзакций в секунду по HTTP	8000	15000	30000	60000	90000	180000
Количество соединений в секунду по HTTPS	2000	3000	10000	14000	16000	30000
Количество транзакций в секунду по HTTPS	2500	4000	12000	20000	30000	50000
Количество одновременных соединений	90000	150000	500000	700000	950000	1800000

Опции поддержки

- Техническая поддержка в режиме 24/7
- Усиливающие обновления Barracuda
- Стандартная техническая поддержка
- Обновления микропрограммного обеспечения и функционала по мере необходимости
- Автоматическое обновление определений приложений

Функции управления

- Интеграция сканера уязвимостей
- Исключение доверенных хостов
- Rest API
- Пользовательские шаблоны

