Дата: «16» марта 2026г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

На анализ рынка с целью выбора системы Web Application Firewall (WAF) на базе F5 BIG-IP

Наименование:

«Внедрение системы Web Application Firewall (WAF) на базе F5 BIG-IP»

Заказчик: АО «Национальный Межбанковский Процессинговый Центр» (НМПЦ)

Контактное лицо: Тоиров А. (Главный специалист отдела по закупкам, +998781132407 / 7733, tender@nmpc.uz)

Согласовано:

Заместитель председателя правления
по ИТ и технологической инфраструктуре _____Самигуллин Д.Р.

Директор департамента
информационной безопасности _____Гафуров А.А.

Директор департамента ИТ-Инфраструктуры _____ Холматов Н.О.

Начальник отдела архитектурных решений _____ Володикова Е.О.

Разработал:

Специалист отдела контроля зашищённости
информационных ресурсов и систем _____ Абдуллаев Д.М.

Техническое задание на проведение анализа рынка

Наименование проекта: Внедрение системы Web Application Firewall (WAF) на базе решения F5 BIG-IP

1. Оглавление

2. Общие сведения

2.1. Наименование системы

Система защиты веб-приложений Web Application Firewall (WAF) на базе F5 BIG-IP

2.2. Основания для проведения работ

1. Необходимость обеспечения защиты веб-ресурсов и API мобильного приложения «Super APP» от современных кибератак и угроз информационной безопасности.
2. Необходимость внедрения системы Web Application Firewall (WAF) для защиты веб-приложений, веб-сервисов и API, используемых мобильным приложением «Super APP».
3. Необходимость обеспечения защиты инфраструктуры мобильного приложения от атак на веб-приложения, включая атаки, описанные в стандарте OWASP Top 10.
4. Обеспечение непрерывной и безопасной работы мобильного приложения «Super APP», а также предотвращение несанкционированного доступа и эксплуатации уязвимостей веб-приложений.

2.3. Назначение системы

Система Web Application Firewall (WAF) на базе F5 BIG-IP предназначена для обеспечения защиты API мобильного приложения «Super APP» АО НМПЦ от современных кибератак и угроз информационной безопасности.

2.4. Цели проведения работ

- Повышение уровня защищенности информационных ресурсов и сервисов мобильного приложения.
- Исполнение регуляторных требований в области обеспечения информационной безопасности.

3. Требования к системе

3.1. Общие требования к Системе

- Система Web Application Firewall (WAF) должна функционировать в виде виртуаль ного комплекса с размещением на вычислительных ресурсах Заказчика. Использование облачных решений не рассматривается.
- Установка, настройка и ввод системы в эксплуатацию осуществляются силами и за счет Поставщика. В рамках гарантийного периода Поставщик обязан обеспечить устранение неисправностей программного обеспечения, обновление системы и восстановление работоспособности. В постгарантийный период сопровождение, обновление и техническая поддержка системы должны осуществляться в соответствии с условиями технической поддержки, указанными в коммерческом предложении Поставщика.

- – информацию о наличии сервисных центров и/или авторизованных партнеров на территории Республики Узбекистан для обеспечения гарантийного и послегарантийного обслуживания (список и адреса сервисных центров, авторизованных партнеров).
- Все компоненты и модули решения должны быть от одного производителя, и иметь соответствующею гарантию с описанием что входит в гарантию.
- Предполагаемое решение будет внедрятся в 2х ЦОД в разных локациях. Решение (включая (модули администрирования/управления/

3.2 Требования к производителю

- Производитель решения должен не менее 10 лет присутствовать на рынке Application Delivery Controllers (ADC).
- Производитель должен иметь собственный облачный центр очистки DDoS L3-L7 для веб приложений.
- Наличие аппаратных и виртуальных решений с одинаковыми функциональными возможностями;
- Наличие ознакомительной лицензии с доступом ко всем функциональным модулям системы.
- Наличие специальной лицензии для тестовой среды.
- Поддержка одинаковых настроек шифрования SSL/TLS шифрования на физических и виртуальных устройствах производителя решения.
- Проведение обучения сертифицированным тренером на русском языке.
- Не менее 10-ти сертификатов уровня «администратор» предлагаемой системы.
- Не менее 5-х сертификатов уровня «профильный специалист» предлагаемой системы.
- Наличие официального центра поддержки в центре партнера или дистрибьютора с часовой разницей не более 4-х часов.
- Поддержка в режиме 24х7 на протяжении 3 года
- Оказание поддержки на английском или русском языках.
- Наличие авторизационного письма от производителя решения.

3.3 Требования к виртуальной машине

3.3.1 Требования к ресурсам виртуальной машины

- Поддержка гипервизоров: VMware ESXi, KVM, Microsoft Hyper-V.
- Реализация всего функционала должна выполняться в рамках одной VM.
- Лицензия не должна ограничивать пропускную способность решения.
- Виртуальная машина должна иметь минимум 8 vCPU с возможностью расширения.
- Возможность расширения виртуальной машины до 24 vCPU
- Возможность переактивации лицензии на другой виртуальной машине, как на локальном гипервизоре, так и в публичном облаке.
- Виртуальная машина должна поддерживать SR-IOV.

3.4 Управление решением

- Управление решением должно выполняться как с GUI-консоли, так и с CLI-консоли.

- Подсистема управления должна быть изолирована от подсистемы обработки трафика
- Наличие REST API интерфейса для управления решением.
- Менеджмент интерфейс должен поддерживать IPv4 и IPv6
- Предлагаемое решение должно иметь функцию для создания отчетов о моментальных снимках устройства, которые затем должны быть загружены в онлайн-инструмент, предоставленный OEM-производителем, и получить обратную связь о работоспособности устройства и необходимых исправлениях и лучших практиках.

3.5 Отказоустойчивость и масштабирование

- Должна обеспечиваться схема Failover (Active/Passive).
- Максимальное количество устройств в схеме Failover – 32.
- Должна обеспечиваться схема Load Sharing (Active/Active).
- Максимальное количество устройств в схеме Load Sharing – 8.
- Должна обеспечиваться возможность объединения как физических, так и виртуальных устройств в отказоустойчивую схему.
- Должна обеспечиваться возможность объединения различных моделей устройств в единую отказоустойчивую схему.
- Должна обеспечиваться поддержка возможности передачи обработки SSL-трафика на устройства с аппаратным ускорителем в рамках отказоустойчивой схемы.
- Должно обеспечиваться сохранение состояния сессий в момент переключения между устройствами в отказоустойчивой схеме.
- Должна обеспечиваться синхронизация SSL соединений, терминированных системой, чтобы в момент HA Failover не происходил обрыв соединений.
- Должна обеспечиваться синхронизация привязки сеансов к объекту балансировки.
- Должен обеспечиваться механизм Graceful Shutdown для обрабатываемых сессий в отказоустойчивой схеме работы.
- Должна обеспечиваться как ручная, так и автоматическая синхронизация конфигурации между устройствами.

3.6 Требования к функционалу сетевого взаимодействия

3.6.1 Взаимодействие на L2 уровне

- Поддержка 802.1q VLAN, VLAN Groups.
- Поддержка STP.
- Поддержка LACP.
- Поддержка LLDP.
- Поддержка VXLAN, NVGRE.
- Поддержка L2TP, PPTP, PPP.

3.6.2 Взаимодействие на L3 уровне

- Поддержка IPv4 и IPv6, IPX/SPX.
- Поддержка NAT, PAT, SNAT.
- Поддержка lan-to-lan IPSEC, GRE-туннелирования.
- Поддержка QoS.
- Поддержка WCCP.
- Поддержка функции фильтрации пакетов.

3.6.3 Маршрутизация

- Должна обеспечиваться возможность дополнения решения следующими алгоритмами динамической маршрутизации без замены оборудования(необходима покупка доп лицензии):
  - Поддержка BGP.
  - Поддержка OSPF.
  - Поддержка IS-IS.
  - Поддержка RIP.
- Статическая маршрутизация.
- Должна обеспечиваться изолированная таблица маршрутизации для интерфейса управления.

3.7 Требования к системным функциям решения

3.7.1 Управление модулями решения

- Должна обеспечиваться возможность добавления/удаления функциональных модулей решения.
- Добавление/удаление функциональных модулей должно происходить без изменения конфигурации аппаратных средств.
- Добавление/удаление функциональных модулей должно происходить без необходимости инсталляции дополнительного программного обеспечения.
- Должно обеспечиваться гарантированное выделение ресурсов под каждый функциональный модуль.
- Должен обеспечиваться контроль использования ресурсов при добавлении/удалении функциональных модулей.
- Должна поддерживаться база данных геолокации без необходимости каких-либо дополнительных лицензий и предоставлять регулярные обновления на веб-сайте производителя.

3.7.2 Управление SSL-сертификатами

- Должна обеспечиваться возможность добавления/удаления сертификатов для SSL-траффика.
- Должна обеспечиваться возможность мониторинга состояния сертификатов SSL-траффика.

3.7.3 Ролевая модель разграничения прав пользователей системы

- Каталог пользователей:
  - Должна поддерживаться интеграция с LDAP.
  - Должна поддерживаться интеграция с RADIUS.
  - Должна поддерживаться интеграция с TACACS+.
  - Должна поддерживаться интеграция с Microsoft AD.
  - Должна поддерживаться интеграция с ClientCert LDAP.
  - Должен обеспечиваться локальный каталог пользователей.
- Должен обеспечиваться механизм распределения ролей пользователей для доступа к решению
- Должен обеспечиваться механизм разделения конфигурации на логическом уровне с предоставлением к ней прав доступа.

- Должно обеспечиваться разделение устройства на несколько административных разделов для доступа разными группами пользователей без ограничения функционала настройки приложений;

3.7.4 Управление системными журналами

- Должна обеспечиваться возможность выгрузки системных журналов в режиме реального времени на стороннее программное обеспечение.
- Должен обеспечиваться функционал управления правилами фильтрации системных журналов.
- Должен обеспечиваться механизм разграничения прав доступа пользователей к системным журналам.
- Должен обеспечиваться функционал управления конфигурацией уровня сообщений системного журнала как с GUI-интерфейса, так и с CLI-интерфейса.
- Должен обеспечиваться функционал управления системными журналами для каждого отдельного модуля решения.
- Должен поддерживать механизм создания нестандартных журналов с помощью встроенного скриптового языка.

3.7.5 Управление резервными копиями конфигурации системы

- Должна обеспечиваться функция создания архива всей конфигурации решения как с GUI-консоли, так и с CLI-консоли.
- Должна поддерживаться возможность создания различных версий архива конфигурации.
- Должна поддерживаться возможность управления архивами конфигурации (создание, удаление, экспорт, импорт).

3.8 Мониторинг системы

- Должна обеспечиваться отчетность по производительности системы с такими параметрами:
  - Объем используемой оперативной памяти.
  - Производительность CPU.
  - Утилизация кеш-памяти.
  - Количество активных сессий, новых сессий.
  - Используемая пропускная способность в бит/с, пакетов/с.
  - Количество HTTP запросов.
  - Количество SSL-транзакций.
- Должна обеспечиваться возможность мониторинга решения сторонним программным обеспечением.
- Должна обеспечиваться поддержка следующих протоколов мониторинга:
- SNMP v1/2/3, SNMP Traps.
- sFlow
- Возможность мониторинга состояния публикуемых/защищаемых приложений при помощи протоколов мониторинга системы

3.9 Обработка трафика

- Возможность независимого применения настроек как на стороне клиента и сервера:
  - IP
  - TCP

- HTTP
- HTTP/2
- LDAP
- WebSocket

- Наличие шаблонов предварительно настроенных конфигурация которых являются best practice для различных сценариев использования решения, например WAN сеть, LAN сеть, мобильная сеть.
- Возможность применения индивидуальный правил обработки трафика на основе критериев этого подраздела но не ограничиваясь ими.

3.10 Обработка SSL-трафика

- Должен обеспечиваться механизм SSL Offload, который позволит перенести процесс шифрования/дешифрования траффика к/от пользователя на предлагаемое решение.
- Возможность применения разных настроек шифрования на стороне клиента и сервера.
- Должна обеспечиваться поддержка возможности передачи обработки SSL-трафика на устройства с аппаратным ускорителем в рамках отказоустойчивой схемы.
- Должна обеспечиваться возможность направления расшифрованного трафика по ICAP на средства его анализа.
- Должны обеспечиваться индивидуальные правила работы с SSL/TLS трафиком и направления на средства анализа на основе FQDN и/или IP адреса.
- Должна обеспечиваться возможность использования сторонних центров сертификатов (Microsoft PKI).
- Подсистема защиты от целевых атак и атак нулевого дня должны быть интегрированы с подсистемой инспекции SSL.

3.11 Требования к системе балансировки нагрузки веб приложений

3.11.1 Режимы балансировки

- Должны обеспечиваться следующие режимы балансировки нагрузки:
- Стандартный режим балансировки нагрузки приложений, позволяющий терминировать сессии пользователей отдельно от сессий серверов.
- Режим пересылки запросов L3 уровня.
- Режим пересылки и акселерации HTTP запросов.
- Режим балансировки пакетных протоколов.

3.11.2 Методы балансировки

- Система должна поддерживать методы балансировки как в рамках пула балансировки приложения, так и всего сервера целиком.
- Должен обеспечиваться механизм балансировки Round Robin.
- Должен обеспечиваться механизм балансировки Round Robin с указанием приоритета, как в рамках пула балансировки приложения, так и всего сервера целиком.
- Должен обеспечиваться механизм балансировки с отслеживанием количества подключений на объект в рамках приложения и в рамках сервера.
- Должен обеспечиваться механизм балансировки с отслеживанием количества подключений и использованием приоритетов в рамках приложения и в рамках сервера.

3.11.3 Мониторинг объектов балансировки

- Должны обеспечиваться следующие методы мониторинга состояния объектов балансировки:
  - FTP.
  - ICMP.
  - ICMP Gateway.
  - HTTP.
  - HTTPS.
  - SOAP.
  - TCP.
  - TCP Echo.
  - UDP.
- Должен обеспечиваться механизм Graceful Shutdown для активных сессий пользователей в момент вывода объекта из процесса балансировки.
- Наличие инструмента отладки пользовательских мониторов, который позволит проверять работу монитора на любом IP:PORT не применяя его на приложении.

3.11.4 Привязка сеансов к объекту балансировки

- Должен обеспечиваться функционал привязки сеансов к объекту с использованием IP адресов источника и получателя.
- Должен обеспечиваться функционал привязки сеансов к объекту с использованием идентификатора хоста.
- Должен обеспечиваться функционал привязки сеансов к объекту с использованием механизма Cookie.

3.11.5 Оптимизация траффика

- Должен обеспечиваться механизм компрессии HTTP-трафика.
- Механизм компрессии HTTP-трафика должен выполняться на программном аппаратном уровне предлагаемого решения с возможностью до установки аппаратного компонента для этой задачи.
- Должен обеспечиваться механизм кеширования часто используемого контента.
- Должен обеспечиваться механизм агрегации запросов различных пользователей в одну сессию к объекту балансировки.

3.11.6 Программируемость

- Все настройки балансировки должны применяться на основе FQDN и/или IP и/или информации из payload
- Должен обеспечиваться механизм создания и управления специализированными правилами и сценариями обработки трафика средствами предлагаемого решения.
- Должен обеспечиваться механизм создания и управления специализированными правилами и сценариями балансировки нагрузки средствами предлагаемого решения.
- Должна обеспечиваться возможность управления предустановленными либо специализированными наборами манипуляции трафиком и его содержимым.

3.12 Фильтрация трафика на основе репутационной базы IP адресов.

3.12.1 Возможность фильтрации запросов на основе репутационной базы IP адресов:

- Должен обеспечиваться механизм управления репутационной базой данных IP адресов.
- Должен обеспечиваться механизм создания как «черных», так и «белых» списков IP адресов.
- Должен обеспечиваться механизм категоризации «черных» списков IP адресов.
- Должен обеспечиваться механизм конфигурирования различных правил обработки трафика для различных категорий «черного» списка IP адресов.

3.12.2 Репутационная база IP адресов:

- Должен обеспечиваться механизм управления репутационной базой данных IP адресов.
- Должен обеспечиваться механизм создания как «черных», так и «белых» списков IP адресов.
- Должен обеспечиваться механизм категоризации «черных» списков IP адресов.
- Должен обеспечиваться механизм конфигурирования различных правил обработки трафика для различных категорий «черного» списка IP адресов.

3.13 Требование к системе защиты веб приложений

3.13.1 Общие требования

- Должна обеспечиваться защита от следующих типов атак на приложения:
  - OWASP Top 10 2025
  - OS Command Injection
  - SQL Injection
  - Session Hijacking
  - Site Reconnaissance
  - Site Scraping
  - Cross Site Scripting
  - Cross Site Request Forgery
- Должна обеспечиваться защита от «Zero Day Web Worm» атак.
- Должна обеспечиваться защита от CSRF атак.
- Должна обеспечиваться защита от SSRF атак.
- Должна обеспечиваться возможность интеграции с сканерами уязвимостей такими, как WhiteHat, IBM, Cenzic, HP, Qualys.
- Должны обеспечиваться механизмы "digitally sign cookies", "encrypt cookies", and "rewrite URLs".
- Должны обеспечиваться механизмы "track session IDs", "prevent cookie injection, cookie tampering" и обеспечиваться защита от "session hijacking attacks".
- Обеспечиваться безопасность и целостность XML-контента в соответствии с их схемами (а так же SOAP, WSDL, JSON, AJAX).
- Правила безопасности для WebSocket
- Система должна поддерживать отправку webhook событий;
- Поддержка HTTP/2
- Поддержка HTTP/3 и QUIC
- Возможность лицензионного расширения функций до определения мошеннических действий вредоносного ПО при работе с приложения на стороне пользователя или действий Man-In-The-Middle.
- Интеграция с антивирусом по протоколу ICAP

- Определение автоматического обхода CAPTCHA
- Определение попыток обхода политики безопасности WAF
- Опциональная возможность блокировки на основе базы зараженных fingerprint клиентов.
- Возможность мониторинга работоспособности приложения под защитой и переключения трафика на другой веб сервер в случае неисправности основного приложения;
- Поддержка и использование предустановленных политик и отчетов в том числе для аудита PCI DSS.
- Поддержка и использование предустановленных политик и отчетов в том числе для аудита OWASP top 10.
- Кастомные сигнатуры SoC производителя на основе текущих атак.
- Возможность онлайн и офлайн обновления сигнатур WAF, Bot, серверных технологий независимо друг от друга.

3.13.2 Защита API

- Наличие встроенного мастера защиты API.
- Защита REST API.
- Возможность автоматизации создания политики защиты API на основе OpenAPI файла, которая включает:
  - Разрешенные API методы
  - Доступные API endpoints
  - Доступные параметры
  - Тип параметра
  - Комбинация метод+API endpoint + параметр
- Наличие предустановленного шаблона для защиты GraphQL API.
- Опциональная возможность расширения функционала защиты API:
  - Проверка на предмет того, что API запросы направлены на разрешенный API endpoint.
  - Проверка валидности JWT токенов в API запросе.
  - Указание ответов по умолчанию для каждого API endpoint.
  - Интеграция с OAuth провайдером для проверки логинов с использованием OAuth 2.0
  - Rate limiting для каждого API endpoint.

3.13.3 Построения политик безопасности приложений

- Возможность защиты нескольких веб приложений на основе SNI и/или FQDN различными политиками защиты индивидуально для каждого приложения.
- Предлагаемое решение WAF должно поддерживать как положительную, так и отрицательную модель безопасности, а также должно обеспечивать регулярное обновление сигнатур CVE.
- Как положительная, так и отрицательная модель безопасности должны постоянно изучать приложение. Режим обучения не должен останавливаться даже после применения политик в блокирующем состоянии.
- Предлагаемое решение WAF должно обеспечивать автоматическое создание правил безопасности на основе поведенческого анализа реального трафика.
- Система обучения должна обучаться как на основании запросов, так и ответов

- Предлагаемое решение WAF должно иметь возможность выбора скорости автоматического создания правил безопасности на основе поведенческого анализа реального трафика.
- Обеспечиваться автоматическое создание правил безопасности на основе отчетов сканеров уязвимостей.
- Обеспечиваться автоматическое создание правил безопасности на основе реального трафика приложения.
- Возможность исключения указанных IP адресов при автоматическом обучении.
- Возможность указать доверенные IP адреса для повышения скорости обучения.
- Обеспечиваться автоматическое создание правил безопасности по предустановленным шаблонам.
- Возможность применения необходимых исключений в политику безопасности по заблокированному или подозрительному запросу.
- Обеспечиваться тонкая настройка существующих правил безопасности в ручном режиме
- Обеспечиваться создание специализированных правил безопасности для специализированных приложений как в автоматическом, так и ручном режиме
- Возможность применения правил блокировки в режиме обучения без блокировки.
- Наличие механизма для сокращения False/Positive сработок.
- Возможность дополнения существующих политик безопасности результатами анализа сканеров уязвимостей;
- Предлагаемое решение должно иметь возможность отслеживать изменения приложений с течением времени и настраивать элементы конфигурации и правила на основе этих данных.
- Предлагаемое решение должно иметь возможность отслеживать неиспользуемые элементы в политике и предлагать удалять их через указанный период времени.
- Предлагаемое решение должно иметь возможность автоматически обнаруживать программное обеспечение/серверную технологию, используемую на серверной стороне, для определения наборов сигнатур, необходимых для построения политики защиты решения.
- Решение должно быть способно идентифицировать подключения Web Socket и обеспечивать безопасность для WebSocket.
- Предлагаемое решение должно строить карту защищаемого ресурса в виде дерева URL с параметрами.
- Решение должно иметь возможность выполнять профилирование JSON. HTTP-запросы в формате JSON должны быть изучены WAF с параметрами.
- Xml-защита, предлагаемая решением, должна быть аналогична защите веб-приложения, предоставляемой возможностью автоматического профилирования/обучения.
- Предлагаемое решение WAF должно иметь возможность проверки коррелированных атак или функции корреляции, которые проверяют несколько атрибутов, таких как соответствие протоколу HTTP, нарушения профиля, сигнатуры, специальные символы и репутация пользователя, чтобы точно предупреждать или блокировать атаки, а также устранять ложные срабатывания.
- Возможность задания «испытательного срока» для новых сигнатур для избежания ложных срабатываний. Система должна сигнализировать, но не блокировать согласно новым сигнатурам

- Возможность изменять или добавлять сигнатуры.
- Возможность изменять или добавлять наборы сигнатур.
- Система должна поддерживать создание собственных типов уязвимостей, правил их определения, их описания и отражения во внутренней и системе мониторинга событий безопасности
- Предлагаемое решение WAF должно иметь функциюю корреляции атак, которая проверяет сразу несколько атрибутов, таких как соответствие протоколу HTTP, нарушения профилей, сигнатуры, специальные символы и репутация пользователя, чтобы точно предупреждать или блокировать атаки, устраняя ложные срабатывания.
- Решение должно иметь возможность построения базовой политики и наследования дочерних политик от нее.
- Наследование должно поддерживать ограничение изменений базовых параметров политики
- Решение должно предоставлять панель мониторинга соответствия OWASP, которая предоставляет интерактивный интерфейс, который измеряет соответствие политики безопасности приложения требованиям OWASP Application Security Top 10, а также предоставляет рекомендации для устранения несоответствия и настройки политик для него.
- Решение должно иметь возможность создавать fingerprint клиента с целью его отслеживания, даже в тех случаях, когда один пользователь пытается использовать несколько сессий;
- Возможность маскирования чувствительных данных:
  - http заголовков
  - параметры в URL
  - параметры в теле запроса
  - значение cookie

3.13.4 Анализ событий политики безопасности приложений

- Экспертная оценка каждого события политики безопасности приложения:
  - Определяться степень угрозы на приложение
  - Предоставляться детальное описание угрозы
  - Предоставляться подробное описание ущерба на защищаемое приложение
  - Перечень предлагаемых рекомендаций для изменения политики для изменения политики безопасности приложения
  - Мониторинг трафика защищаемых ресурсов на выявление аномалий
  - Обеспечивать оповещение о выявленных аномалиях.
  - Возможность определять и сдерживать атаки, направленные на обнаружение уязвимостей веб-сайта и его сканирование.
  - Доступ к событиям на основе ролевого управления.
  - Поддержка отправки логов на удаленные приемники.
  - Предлагаемое решение должно иметь возможность логирования как
  - HTTP-запросов так и HTTP-ответов.
  - Возможность выборочного или гарантированного логирования и отображения как запроса так и ответа.

3.13.5 Защита от brute force атак

- Наличие механизма автоматического определение страниц с формами авторизации
- Защита на основании источника:
  - Уникальный username
  - Идентификатор устройства
  - IP адрес
  - Обхода CAPTCHA
- Защита от распределённой brute force атаки.
- Возможность внесения IP адресов в белый список для исключения brute force защиты.
- Опциональная возможность блокировки попыток входа при помощи базы данных украденных паролей.
- Возможность создания индивидуальной логики блокировки brute force

3.13.6 Бот защита

- Предлагаемое решение WAF должно различать входящий трафик между пользовательским и бот-трафиком, идентифицировать «хороших» и «плохих» и «подозрительных» ботов;
- Наличие пошагового мастера настройки защиты приложения от бот атак
- Наличие базы бот сигнатур
- Возможность задания «испытательного срока» для новых сигнатур для избежания ложных срабатываний. Система должна сигнализировать, но не блокировать согласно новым сигнатурам
- Обеспечиваться категоризационная база BotNet сетей
- Обеспечиваться индивидуальные правила обработки для каждой категории
- Обеспечиваться механизм автоматического определения BotNet на базе встраиваемого Java Script или поведенческого анализа.
- Поддержка CAPTCHA со звуком
- Автоматическое определение ботов на основе их поведения;
- Должна обеспечиваться поддержка следующих методов блокировки траффика:
  - Уведомление
  - Блокировка
  - Механизм защиты от BotNet на базе CAPTCHA TCP Reset
  - Переадресация на с пул серверов
  - Rate limit
  - Страница ловушка для ботов прошедших CAPTCHA;

3.13.7 Защита от DoS/DDoS атак уровня WEB приложения

- Наличие пошагового мастера настройки защиты приложения от Dos атак
- Решение должно обеспечить очистку трафика, направленную на снижение нагрузки на атакуемый ресурс, путем выявления и блокировки паразитного трафика для WEB приложения.
- Решение должно обеспечивать очистку трафика (атаки, основанные на использовании протоколов http и https).
- Должно обеспечить реализацию комплекса механизмов выявления паразитного трафика, при этом обеспечивать использование следующих механизмов фильтрации:

- Фильтрацию на основании задаваемых через программный интерфейс черных и белых списков IP-адресов, формируемых Заказчиком;
- Фильтрацию по географическому признаку (месторасположение источника трафика) как с возможностью исключения определенных регионов, так и с возможностью приема трафика только от определенного списка регионов;
- Иметь возможность мониторинга трафика защищаемых ресурсов на предмет выявления аномалий и иметь систему оповещения о выявленных аномалиях.
- Работа в пассивном режиме с копией трафика в целях мониторинга.
- DoS/DDoS защита приложения на 7-м уровне модели OSI с возможностью анализа и блокирования по следующим критериям:
  - IP адрес источника
  - идентификатор устройства
  - геолокация
  - URL
  - Автоматически созданных сигнатур
- Возможность записи трафика в процессе DDoS атаки
- Возможности блокировки атаки:
  - Ограничение
  - Блокировка
  - Captcha