«ПОДТВЕРЖДАЮ»
АКБ «Банк развития бизнеса»
Заместитель председателя правления:
Б.Бобожонов

«18» сентябр 2025 г.
№ 206

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на систему защиты веб сервисов АКБ «Банк Развития Бизнеса»

Ташкент 2025г.

1. Наименование проекта

Повышение защищенности веб сервисов в АКБ «Банк Развития Бизнеса».

2. Информация об участниках проекта

Заказчик: АКБ «Банк развития Бизнеса»

Исполнитель: - будет определен по результатам отбора

3. Назначение и цель проекта

Проект направлен на повышение уровня информационной безопасности и устойчивости интернет-ресурсов компании к внешним угрозам за счёт внедрения современных средств защиты. В рамках проекта планируется развертывание системы защиты веб-приложений (WAF) для обеспечения многоуровневой защиты от атак на уровне приложений (Layer 7), а также развертывания системы для защиты от распределённых атак типа «отказ в обслуживании» (DDoS).

Цель проекта обеспечить непрерывную и безопасную работу веб-ресурсов и онлайн-сервисов компании путём:

- предотвращения и блокировки атак на уровне приложений (SQL-инъекции, XSS, RCE, OWASP Top-10 и др.);
- защиты от volumetric, protocol и application-level DDoS-атак;
- минимизации времени простоя и финансовых потерь, связанных с кибератаками;
- обеспечения соответствия требованиям регуляторов и внутренним политикам безопасности.

4. Техническая часть отбора наилучшего предложения

Качество поставляемой продукции должно соответствовать требованиям, указанным в техническом задании (далее ТЗ).

Количество и объем предоставляемого товара и объем оказываемой услуги согласно ТЗ.

4.1. Плановые сроки поставки товаров и проведения интеграционных работ

Срок поставки товаров: не позднее 100 календарных дней с момента подписания договора.

Сроки проведения интеграционных работ: не более 20 рабочих дней

4.2. Место поставки и проведения работ

Местом поставки и проведения работ является офис Заказчика, расположенный по адресу: г. Ташкент, улица Навои 18А.

4.3. Технические требования к поставляемой продукции

Система защиты веб приложений (WAF)	**Архитектура и форм-фактор:** Виртуальная машина, развернутая на серверах Банка; Поддержка гипервизоров: VMware ESXi, KVM, Hyper-V. Поддержка развертывания в публичных облаках: AWS, Google Cloud, IBM Cloud, Microsoft Azure, Oracle Cloud Реализация всего функционала должна выполняться в рамках одной VM Возможность выделения виртуальной машине X 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. **Требования к производительности:** Пропускная способность L4 уровня – не менее 40 Gbit/s; Пропускная способность L7 уровня – не менее 40 Gbit/s; Количество TCP подключений в секунду – не менее 1 700 000; Максимальное количество одновременных TCP-сессий – не менее 31 000 000 Количество запросов L7 уровня в секунду– не менее 1 500 000 Объем сжатого трафика: Производительность сжатия траффика – не менее 6.8 Gbit/s Производительность SSL-шифрования трафика – не менее 30 Gbit/s Производительность SSL TPS (2k keys) – не менее 19 000 TPS. Поддержка TLS 1.3. **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.	**2 шт.**

	• 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. • Наличие успешных внедрений балансировщика, WAF производителя решения на территории страны. • Проведение обучения сертифицированным тренером на русском языке. • Не менее 5-ти сертификатов уровня «администратор» предлагаемой системы. • Не менее 3-х сертификатов уровня «профильный специалист» предлагаемой системы. • Наличие официального центра поддержки центре партнера или дистрибьютора с часовой разницей не более 4-х часов. • Поддержка в режиме 24x7 на протяжении 1 года • Возможность оперативной замены вышедшего из строя оборудования за 24 часа (Next Business day RMA) • Оказание поддержки на английском, русском или украинском языках. • Наличие авторизационного письма от производителя решения. **Требования к управлению 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. **Отказоустойчивость и масштабирование:** • Должна обеспечиваться схема Active/Passive. • Максимальное количество устройств в схеме Active/Passive – 8. • Должна обеспечиваться схема Active/Active. • Максимальное количество устройств в схеме Active/Active – 8. • Должна обеспечиваться схема синхронизации configuration only	

	• Максимальное количество устройств в схеме синхронизации configuration only – 32. • 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. **Требования к функционалу сетевого взаимодействия:** Взаимодействие на L2 уровне: • Поддержка 802.1q VLAN, VLAN Groups. • Поддержка STP. • Поддержка LACP. • Поддержка LLDP. • Поддержка VXLAN, NVGRE. • Поддержка L2TP, PPTP, PPP. 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. • Поддержка VRF. • Поддержка работы с VRRP. 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.	

	• Поддержка VRF. • Статическая маршрутизация. • Должна обеспечиваться изолированная таблица маршрутизации для интерфейса управления. **Требования к системным функциям решения:** **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. **Управление SSL-сертификатами:** • Должна обеспечиваться возможность добавления/удаления сертификатов для SSL-траффика. • Должна обеспечиваться возможность мониторинга состояния сертификатов SSL-траффика. **Ролевая модель разграничения прав пользователей системы:** • Должна поддерживаться интеграция с LDAP, RADIUS, TACACS+, 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; **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. **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). **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 **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. **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. • Механизм обработки SSL должен выполняться на аппаратном уровне средствами предлагаемого решения (для аппаратных решений). • Должен обеспечиваться механизм шифрования/дешифрования SSL аппаратными средствами сервера, где работает виртуальное решения (опциональная функция, требует приобретения доп лицензии) • 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. **Требования к системе балансировки нагрузки веб приложений:** 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. 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. 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. **Привязка сеансов к объекту балансировки:** Должны обеспечиваться следующие режимы балансировки нагрузки: • 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. **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. **Фильтрация трафика на основе репутационной базы IP адресов:** 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. 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. 1.1.1. Должны обеспечиваться механизмы "track session IDs", "prevent cookie injection, cookie tampering" и обеспечиваться защита от "session hijacking attacks". Общие требования - Должна обеспечиваться защита от следующих типов атак на приложения: - OWASP Top 10 2021 - OS Command Injection - SQL Injection - Session Hijacking - Site Reconnaissance - Site Scraping - Cross Site Scripting - Cross Site Request Forgery - Zero Day Web Worm - Должна обеспечиваться возможность интеграции со сканерами уязвимостей такими, как WhiteHat, IBM, Cenzic, HP, Qualys. - Должны обеспечиваться механизмы "digitally sign cookies", "encrypt cookies", and "rewrite URLs". - Обеспечиваться безопасность и целостность XML-контента в соответствии с их схемами (а также SOAP, WSDL, JSON, AJAX). - Правила безопасности для WebSocket - Система должна поддерживать отправку webhook событий; - Поддержка HTTP/2, 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. - Опциональная защита мобильных приложений при помощи интеграции с SDK WAF (требуется доп лицензия).	

	• Возможность проверки данных пользователя (логин и пароль) в базе скомпрометированных данных (требуется доп лицензия). • 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. **Защита API:** • Наличие встроенного мастера защиты 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. **Защита от ботов:** • 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; **Лицензии:** Система WAF должна поставляться в виде виртуальной машины, в количестве 2 шт. Лицензия на функционал WAF должна быть бессрочной. Решение должно поддерживать не менее 8vCPU. Система должна иметь лицензию на обновления сигнатур угроз сроком на 12 месяцев Система должна иметь лицензию для получения информации о вредоносных IP адресах сроком на 12 месяцев **Гарантия и сервисная поддержка** Система WAF должна обеспечиваться гарантией от производителя и сервисной поддержкой сроком не менее 12 месяцев уровня Premium. Условия сервисной поддержки должны включать в себя возможность регистрации сервисных случаев в режиме 24x7x365, обновление версий установленного программного обеспечения.	

Anti DDOS	🕐 Система должна поставляться в виде программно-аппаратного комплекса. 🕐 Система подавления должна защищать от всего спектра DDoS-атак с минимальным количеством ложных срабатываний, обеспечивая пропуск почти 100% легитимного трафика. 🕐 Основной режим обнаружения и подавления — автоматический, без вмешательства человека. 🕐 Система должна автоматически создавать фильтры L3–L7 в режиме реального времени для угроз нулевого дня на основе анализа трафика атаки. 🕐 Требования к производительности: o Общий объем входящего трафика (Гбит/с) должен быть не менее 10 Гбит/с o Лицензируемая полоса очищенного трафика должна быть не менее 5 Гбит/с и 14 MPPS. o Одновременное подавление должно иметь не менее 48 различных атак выделенных направлений. 🕐 Максимальная задержка должна быть не более 10 мкс Требования к интерфейсам: o Количество интерфейсов со скоростью не менее чем 1GE (медь)- не менее 8 портов. o Количество интерфейсов со скоростью не менее чем 10GE (SFP+)- не менее 4 портов. 🕐 Наличие резервного блока питания с возможностью горячей замены 🕐 Выделенный порт управления (OOBM), мин. 1 🕐 Режим Работа – L2 прозрачный 🕐 Режим работы – L3 маршрутизируемый 🕐 Время реакции на подавление для статической контрмеры, должно быть не более 1 сек. 🕐 Время реакции на подавление для динамической (динамические фильтры) контрмеры, должно быть не более 15 сек. 🕐 Обнаружение и защита от всех типов атак должны осуществляться автоматически. 🕐 Система должна поддерживать режим как с однонаправленным, так и с двунаправленным трафиком (OOP и встроенный). 🕐 Система должна поддерживать фильтрацию аномальных пакетов. 🕐 Система должна поддерживать сочетание обоих режимов, однонаправленного и двунаправленного трафика (OOP и встроенный). 🕐 Система должна иметь полную поддержку стека протоколов IPv4 и IPv6 для подавление атак. 🕐 Защита от многовекторных DDoS-атак, нацеленных на разные уровни модели OSI (3-7) одновременно. 🕐 Защита от атак TCP-флуда, включая: o SYN,	**2 шт.**

	○ SYN-ASK, ○ PUSH, ○ FIN, ○ RST, ○ флуд ASK, генерируемый потоком Mirai, ○ флуд фрагментов TCP, 🕐 флуд, генерируемый недействительными пакетами TCP. 🕐 Система должна обеспечивать защиту от флуда TCP-соединений. 🕐 Система должна обеспечивать защиту от флуда ICMP (эхо-запрос, недоступность, подавление источника). 🕐 Система должна обеспечивать защиту от флуда внутри туннеля GRE. 🕐 Система должна обеспечивать защиту фрагментированного IGMP-флуда. 🕐 Система должна обеспечивать защиту от флуда HTTP-соединений, включая механизм C/R на основе перенаправления 302 и скрипта JAVA 🕐 Система должна обеспечивать защиту от атак методом подбора приложений: ○ HTTP/S ○ SIP ○ DNS 🕐 Система должна обеспечивать защиту от флуда SIP. 🕐 Система должна обеспечивать защиту от Burst-атаки. 🕐 Система должна обеспечивать защиту против неизвестных атак (нулевого дня), автоматическая генерация расшифровок (фильтров) атак в режиме реального времени. 🕐 Система должна предоставлять возможность создания L3-L7 фильтров атак в ручном режиме. 🕐 Система должна предоставлять защиту от атак SSL/TLS (включая повторное согласование, рукопожатие, флуд). 🕐 Система должна предоставлять защиту от атак HTTPS без расшифровки трафика (включая флуд HTTPS-соединения, флуд страниц и т.е. флуд внутри TLS/SSL-соединения) на основе технологии отпечатков пальцев, которая может идентифицировать (различать) более 10,000 разновидностей. 🕐 Система должна обеспечивать защиту от атак HTTPS при работе в режиме OOP (включая флуд соединений HTTPS, флуд страниц и, т. е. флуд внутри соединения TLS/SSL), с расшифровкой и без нее. 🕐 Система должна обеспечивать автоматическую возможность выборочной полной расшифровки SSL только подозрительных сеансов, находящихся под атакой.	

	• Система должна обеспечивать возможность полной расшифровки SSL в направлении защищенного сервера.
	• Система должна поддерживать защиту HTTPS без ключей SSL.
	• Система должна обеспечивать защиту от флуда UDP, включая:
	  ○ флуд случайных портов,
	  ○ флуд случайных источников,
	  ○ флуд, исходящий от Mirai
	• Система должна обеспечивать защиту от атак усиления.
	• Защита DNS, включая:
	  ○ поддельный адрес источника
	  ○ Атака случайных поддоменов
	  ○ Атака с отражением усиления
	  ○ Атаки по словарю и атаки методом подбора
	• Система должна обеспечивать позитивную модель защиты DNS, основанную на автоматическом составлении белого списка доменов и поддоменов с возможностью ручного редактирования.
	• Система должна предоставлять администратору возможность создавать политики безопасности и изменять их в режиме реального времени.
	• Система должна поддерживать ограничение скорости трафика от определенного источника к получателю или их комбинацию на уровне протокола, приложения, сегмента сети, физического порта, группы.
	• Система должна поддерживать ограничение соединения от определенного источника к получателю или их комбинацию на уровне протокола, приложения, сегмента сети, физического порта, группы.
	• Система должна поддерживать ограничение PPS трафика от определенного источника к получателю или их комбинацию на уровне протокола, приложения, сегмента сети, физического порта, группы.
	• Система должна поддерживать ограничение PPS трафика в сеансе от определенного источника к получателю или их комбинацию на уровне протокола, приложения, сегмента сети, физического порта, группы.
	• Защита от известных уязвимостей в режиме реального времени (регулярные и экстренные обновления сигнатур).
	• Система должна поддерживать списки разрешений и блокировок (черные/белые).
	• Система должна поддерживать функцию блокировки и ограничения скорости ро GEO (возможно с дополнительной лицензией).
	• Система должна поддерживать определяемый пользователем список блокировки, который	

	должен обновляться автоматически из внешней системы с запланированным периодом. - Система должна поддерживать список наиболее активных злоумышленников/хостов, которые участвовали во вредоносных действиях за последние 24 часа. Этот список должен регулярно обновляться автоматически (возможно с дополнительной лицензией). Эти хосты должны блокироваться автоматически без ручного вмешательства. - Система должна поддерживать возможность фильтрации пакетов на основе информации L3–L7 (включая регулярные выражения). - Система должна поддерживать защиту от «вертикального» и горизонтального сканирования, L3–L4. - Система должна обеспечивать защиту протокола QUIC. - Система должна иметь модуль IPS (система предотвращения вторжений). - IPS должна поддерживать автоматическое и ручное обновление подписей. - IPS должна предоставлять возможность определять собственные подписи. - Система должна поддерживать политики защиты на основе тега VLAN и префикса IP. - Система должна поддерживать захват пакетов. - Система должна автоматически создавать профили трафика (базовый уровень) и применять изученный порог. - Система должна обеспечивать базовый уровень с несколькими базовыми параметрами IP (PPS, BPS, размер пакета, протокол, флаги TCP, контрольная сумма IP и т. д.) для создания правил автоматической фильтрации пакетов. - В случае утечки трафика атаки группа экспертов по безопасности должна быть доступна для исправления конфигурации системы в заданном SLA. - Система должна иметь программируемую плоскость управления защитой. - Система должна поддерживать подход «плати по мере роста». - Система должна предоставлять возможность загрузки стороннего фида, формата STIX/TAXII или в виде текстового файла. - Управление, отчетность и аналитика должны быть следующими: - Управление, отчетность и аналитика должны быть реализованы как виртуальное устройство. - Следующие системы виртуализации должны поддерживаться — VMware (6.7, 7.0) и KVM - Поддерживаемые интерфейсы: HTTPS, SSH, REST API	

	• Поддерживаемые протоколы отчетности: SNMP v.1/2/3, SNMP Trap, SYSLOG, SMTP (email) • Доступ к интерфейсу Системы управления должен осуществляться через веб-браузер. • RBAC с внешней аутентификацией LDAP, TACACS+. • Глобальная панель управления для устройства/политики/выбранных политик. • Расширенные возможности криминалистики — возможность создания расширенных отчетов с логическими выражениями. • Отчеты должны иметь возможность включать выборку PCAP из атаки. • Формирование запланированных отчетов в разных форматах, как минимум CSV, PDF. • Система должна выполнять следующие функции с точки зрения управления устройствами для предотвращения DDoS-атак: • Управление устройствами; • Отображение информации об устройстве, такой как: использование ЦП; • Отображение информации о версии установленного программного обеспечения устройства; • Резервное копирование файлов конфигурации устройства. **Требования к системе управления, аналитике и отчетности:** • Все модули системы аналитики должны предоставлять возможность получать информацию за любой временной интервал, выбирая между быстрым диапазоном, абсолютным или относительным. • Система аналитики должна поддерживать следующие основные модули: • Модуль мониторинга для отслеживания безопасности во всей сети, которую защищают ваши устройства. Панели мониторинга суммируют существующую сетевую инфраструктуру в виде графиков, диаграмм и таблиц. Должна давать возможность выполнять глубокий анализ, где это необходимо, углубляясь в детали событий. • В панели мониторинга должна отображаться следующая информация: o Использование лицензии пропускной способности o Общий входящий трафик — скорость в бит/с общего полученного трафика и общего сброшенного трафика o Статистика входящего трафика — скорость входящего трафика в бит/с, пакетах/секунду и соединениях/секунду o Входящая пропускная способность по политике — отображает кольцевую	

	диаграмму, показывающую пропускную способность для каждой из политик защиты ○ Состав трафика — отображает кольцевую диаграмму, показывающую долю различных протоколов во всем трафике ○ Пропускная способность трафика — полученный, сброшенный и исключенный трафик с течением времени (BPS или PPS; входящий или исходящий) 🕐 В панели атак должна отображаться следующая информация: ○ Основные исходные и конечные IP-адреса, ○ Основные исходные и конечные порты, ○ Основные протоколы ○ Распределение размера пакетов ○ Флаги TCP 🕐 В панели аналитики должна отображаться следующая информация: ○ Основные исходные и конечные IP-адреса, ○ Основные приложения, ○ Основные протоколы 🕐 В панели мониторинга политики безопасности должна отображаться следующая информация: ○ входящий трафик ○ Скорость атак последнего периода (в битах/сек и пакетах/сек) ○ Основные источники атак ○ Основные направления атак ○ Пропускная способность трафика политики (BPS или PPS — и входящий или исходящий). 🕐 В панели отчётов должна отображаться следующая информация: ○ Создание и генерация отчета и его просмотр на лету ○ Создание и генерация сложных настраиваемых отчетов 🕐 Должна предоставляться возможность создания шаблонов отчетов. 🕐 Модуль экспертизы для анализа и обнаружения источника атак безопасности, методов и тенденций атак или других проблемных инцидентов 🕐 Модуль оповещения для настройки правил для запуска, генерации и отправки оповещений. **Требования лицензированию** **Система централизованного управления и аналитики** 🕐 Должна обеспечивать ведение отчётности и аналитики по безопасности в режиме реального времени и ретроспективном режиме. 🕐 Лицензия должна предоставляться по модели подписки сроком не менее 1 года, с технической поддержкой. 🕐 Должна включать возможность установки сервера управления в виде виртуальной машины. 🕐 Должна обеспечивать управление не менее чем 2	

	инстансами. - Должна поддерживаться возможность расширения количества управляемых устройств за счёт приобретения дополнительных лицензий. **Базовая лицензия** должна включать: - Поведенческую защиту от Flood-атак , Burst-атак, Botnet-атак, DNS флуд атак. - Базовая лицензия должна поставляться в виде бессрочной лицензии. **Подписка на расширенную защиту** должна включать: - регулярные обновления безопасности, - доступ к актуальной информации об активных источниках атак, - возможность добавления пользовательских фидов, - функции геолокационного ограничения и фильтрации. - Продвинутый поведенческий анализ для распознавания и блокировки атак в зашифрованном трафике. - TLS инспекцию и защиту DNS - Данная лицензия должна быть с сроком действия не менее 12 месяцев.	

5. Требования к уровню технической поддержки со стороны Исполнителя

В поставку должна быть включена техническая поддержка L1 на систему WAF от поставщика сроком на 12 месяцев.

Формат предоставления технической поддержки L1

Удалённая техническая поддержка, включая:

- Прием, регистрацию и первичную обработку инцидентов.
- Оценку критичности инцидента и эскалацию при необходимости.
- Сбор диагностических файлов и дальнейшая передача в техническую поддержку вендора.
- Контроль выполнения работ, информирование Заказчика о статусе запроса.
- Поддержку в установке обновлений и патчей.
- Организацию онлайн-консультаций с инженерами вендора при необходимости.

Дополнительные требования:

Наличие инженера со знанием **узбекского и английского языков** для взаимодействия с пользователями и ведения коммуникации по техническим вопросам со специалистами вендора.

6. Требования к Исполнителю

6.1. Квалификационные требования

Исполнитель должен отвечать следующим квалификационным требованиям:

- Исполнитель должен иметь не менее 1-го (одного) сертифицированного производителем инженера предлагаемого оборудования.
- Исполнитель должен иметь необходимые статусы авторизации и предоставить авторизационные письма (MAF) от всех производителей оборудования, программного обеспечения и материалов для выполнения в полном объеме требуемых работ согласно данного ТЗ.

6.2. Прочие требования к Исполнителю

7. Требования к интеграционным работам и обучению

Обучение и внедрение

- В предложение должно быть включено онлайн обучения от Производителя по администрированию систем Anti-DDOS и WAF для не менее 2 сотрудников.
- Онлайн обучение должно быть на английском языке и должен быть предоставлен сертификат о прохождении от Производителя.
- Минимальное количество сотрудников Заказчика, подлежащих обучению – 2 сотрудника.
- Должен быть обеспечен доступ к платформе обучения производителя системы Anti-DDOS для одного пользователя сроком не менее 12 месяцев.
- В предложение должно быть включено услуга базовой удалённой инсталляция системы Anti-DDOS сроком до 4 рабочих дней.
- Услуга внедрения системы WAF должна быть предоставлена в количестве 270 рабочих часов. Должен быть предусмотрен тариф на оказание услуг по внедрению в случае выполнения работ сверх установленного рабочего времени в количестве 81 часов.

Требования к документации проекта

В рамках выполнения работ Заказчику должны быть предоставлены Исполнителем нижеперечисленные документы:

- Техническая документация от производителя оборудования;
- Исполнительная документация проекта со включением отчета по тестированию
- Акт приемки в промышленную эксплуатацию.

согласные: B.Shamsiyev, Z.Orifxo‘jayev