«Капитал Банкы» ААК ,
Кыргыз Республикасы, 720017,
Бишкек ш., Москва көч, 161
тел.: +996 (312) 31 30 30,
факс: +996 (312) 90 54 84

ОАО «Капитал Банк», 720017,
Кыргызская Республика,
г. Бишкек, ул. Московская, 161
тел.: +996 (312) 31 30 30,
факс: +996 (312) 90 54 84

OJSC «Capital Bank»,
161, Moskovskaya str., Bishkek
720017, Kyrgyz Republic
tel.: +996 (312) 31 30 30,
fax: +996 (312) 90 54 84

office@capitalbank.kg

www.capitalbank.kg

Приглашение к участию в тендере

Всем организациям, независимо от форм собственности,

зарегистрированным на территории

Кыргызской Республики

Источник финансирования: собственные средства

1. ОАО «Капитал Банк» и Тендерная комиссия ОАО «Капитал Банк» объявляет конкурс на закупку оборудования Cheek Point для внедрения двухфакторной аутентификации и обеспечения сетевой инфраструктуры.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ И СПЕЦИФИКАЦИЯ

Check Point Quantum 6400 Security Gateway (NGFW)

CPAP-SG6400-SNBT	6400 Base Appliance with SandBlast subscription package for 1 year Железка NGFW 6400 с оперативкой 8 ГБ.
CPAC-RAM8GB-6400-INSTALL	Memory Upgrade Kit from 8GB to 16GB for 6400 series appliances +1 оперативка 1х8 ГБ для увеличения. Чтобы у железки было в итоге 16 ГБ.
CPAC-Rails-6000/7000/MLS200	Slide Rails for 6000/7000/MLS200 series Направляющие
CPSM-NGSM5-L	Next Generation Security Management Software for 5 gateways (SmartEvent & Compliance 1 year) Менеджмент (управление) софтовая
CPES-SS-STANDARD-L	Enterprise SW Subscription and Standard Support Тех. поддержка на 1 год
CPES-SS-STANDARD-ADD-L	Enterprise Software Subscription and Standard Support additional product Тех. поддержка на 1 год
CPSB-MOB-50-L	Mobile Access Blade for 50 concurrent connections VPN 50 шт.

Web Application Firewall (WAF)

CP-CGAS-100-1Y-YN	AppSec 100M requests 1Y subscription
CPES-SS-STANDARD-L	Enterprise SW Subscription and Standard Suppor

Комплект поставки должен включать в себя следующие компоненты:

Наименование	К-во шт.
Программный комплекс для управления межсетевыми экранами	1
Межсетевой экран	1

1. Требования к программному комплексу для управления межсетевыми экранами.

1.1. Решение должно обеспечивать функционал централизованного управления безопасностью.

1.1.1. Все приложения безопасности Брандмауэра следующего поколения должны быть управляемыми с центральной консоли GUI.

1.1.2. Централизованное управление безопасностью должно управлять 5 шлюзами.

1.1.3. Приложение для управления безопасностью должно поддерживать учетные записи администраторов на основе ролей. Например, только роли для управления политикой брандмауэра или только роль для просмотра журнала.

1.1.4. Решение должно обеспечивать возможность обеспечения высокой доступности системы управления, используя резервный сервер управления, который автоматически синхронизируется с активным сервером.

1.1.5. Решение должно включать возможность централизованного распространения и применения новых версий шлюзового программного обеспечения.

1.1.6. Решение должно включать инструмент для централизованного управления лицензиями всех шлюзов, контролируемых станцией управления.

1.2. Решение должно обеспечивать механизм обновлении во всех приложениях включая IPS, Управление приложениями, URL-фильтрацию, Anti-Bot и Anti-Virus.

1.3. Решение должно обеспечивать функционал Централизованного Протоколирования & Мониторинга.

1.3.1. Система централизованного протоколирования событий должна быть частью системы управления.

1.3.2. Решение должно протоколировать все правила.

1.3.3. У средства просмотра журналов событий должна быть возможность индексированного поиска.

1.3.4. Решение должно иметь возможность протоколирования событий во всех интегрированных приложениях безопасности на шлюзе (включая виртуальные шлюзы), включая Firewall, IPSEC VPN, IPS, Идентификация пользователей, Мобильный доступ, DLP, Управление приложениями, URL-фильтрацию, Anti-Bot, Anti-Virus, Sandboxing.

1.3.5. У системы протоколирования должен быть безопасный канал для передачи данных для предотвращения подслушивания, канал передачи должен быть зашифрован и проходить проверку подлинности.

1.3.6. Журналы событий должны безопасно передаваться между шлюзом и управлением или

выделенным сервером журналов и консолью просмотра журналов в компьютере администратора.

1.3.7. Решение должно включать опцию динамического блокирования активного соединения в графическом интерфейсе системы протоколирования событий без необходимости внесения изменений в базу правил.

1.3.8. Решение должно включать настраиваемую установку пороговых значений параметров для выполнения действий при достижении определенных пороговых значений на шлюзе. Действия должны включать: запись события, оповещение, отправка SNMP trap, отправка электронного письма и выполнение определенного пользователем предупреждения.

1.3.9. Решение должно включать предварительно настроенные графики для мониторинга трафика во времени и системных счетчиков: главные правила безопасности, основные пользователи P2P, VPN туннели, сетевой трафик и другая полезная информация. Решение должно обеспечивать возможность создания новых графиков с различными типами диаграмм.

1.3.10. Решение должно поддерживать сегментирование политики безопасности по слоям с возможностью делегирования полномочий разным администорам с точностью до блоков правил в общей политике.

1.3.11. Решение должно обеспечивать хранение ревизий политик для файрволов следующего поколения с возможностью возврата изменений к предыдущим версиям ревизий.

1.4. Решение должно обеспечивать функционал Централизованной Корреляции событий и Отчетов.

1.4.1. Решение должно иметь возможность корреляции событий из всех приложений, включая Firewall, IPSEC VPN, IPS, Идентификация пользователей, Мобильный доступ, DLP, Управление приложениями, URL-фильтрация, Anti-Bot, Anti-Virus, Sandboxing.

1.4.2. Решение должно включать инструмент для корреляции событий из всех функций шлюза и сторонних устройств.

1.4.3. Приложение корреляции событий должно обеспечивать графическое представление событий на основе времени.

1.4.4. Решение должно включать возможность поиска внутри списка событий, углубления в детали для изучения и расследования инцидентов.

1.4.5. Решение должно включать предопределенные ежечасные, ежедневные, еженедельные и ежемесячные отчеты, в том числе, как минимум, Основные события, Основные источники, Основные пункты назначения, Основные сервисы, Основные источники и их основные события, Основные пункты назначения и их основные события, и Основные сервисы и их основные события.

1.4.6. Решение должно поддерживать автоматическое распространение отчетов по электронной почте, загрузку на FTP/Веб-сервер и скрипт рассылки внешних пользовательских отчетов.

1.1.1. Решение должно обеспечивать функционал управления рисками и соответствия требованиям (GRC) – лучших практик безопасности.

1.1.2. Решение должно обеспечивать оценку соблюдения основных регуляторных требований в режиме реального времени (поддержка стандартов ISO 27001/27002, PCI-DSS,HiPPA,SOX и т.д.).

1.1.3. Решение должно предоставлять рекомендации по реализации лучших практик безопасности.

1.1.4. Решение должно переводить регуляторные требования в инструкции для выполнения лучших практик безопасности.

1.1.5. Решение должно постоянно контролировать конфигурацию шлюза при помощи лучших практик безопасности.

1.1.6. Решение должно генерировать автоматические отчеты по оценке для определения рейтинга соответствия регуляторным требованиям.

1.1.7. Решение должно полностью интегрироваться в Архитектуру программного обеспечения и Инфраструктуру управления.

1.1.8. Решение должно обеспечивать мгновенное уведомление об изменениях политики, влияющих на соответствие регуляторным требованиям.

1.5. Технические требования, поддержка и подписка. Система централизованного управления безопасностью должна быть выполнена в виде программного комплекса со следующими характеристиками:

1.5.1. Система централизованного управления безопасностью должна быть выполнена в виде программного обеспечения, устанавливаемого на сервера, входящие в список аппаратной совместимости производителя, а так же виртуальные машины, функционирующие в средах виртуализации VMWare, Microsoft, KVM.

1.5.2. Поддержка и подписка сроком на 1 года от производителя, 9x5

2. Требования к межсетевому экрану.

2.1. Шлюз безопасности должен использовать контроль состояния соединений на основе детализированного анализа связи и состояния приложения для отслеживания и управления сетевым потоком.

2.2. Решение должно поддерживать DHCP, сервер и relay.

2.3. Решение должно поддерживать HTTP & HTTPS proxy.

2.4. Решение должно поддерживать функционал reverse proxy.

2.5. Решение должно поддерживать работу в режиме Mail Transfer Agent.

2.6. Решение должно включать в себя возможность работы в режиме Transparent/Bridge.

2.6.1. Решение должно поддерживать работу на 2 уровне модели OSI (режим bridge).

2.6.2. Решение должно поддерживать Firewall, IPS, URL-фильтрацию, DLP, Antibot, Antivirus, Управление приложениями, инспекцию HTTPS, Identity Awareness и Sandboxing в режиме bridge.

2.6.3. Решение должно поддерживать кластеризацию Active/Standby в режиме bridge.

2.7. Решение должно поддерживать высокую доступность шлюза и распределение нагрузки с синхронизацией состояний сетевых соединений. В режиме высокой доступности или режиме распределения нагрузки должно поддерживаться до 31 узла кластера.

2.8. Решение должно поддерживать виртуализацию шлюза безопасности для консолидации нескольких виртуальных шлюзов на одном физическом устройстве.

2.8.1. Решение должно иметь возможность расширения до 10 виртуальных систем при применении дополнительной лицензии.

2.8.2. Сетевые возможности: решение должно поддерживать виртуальные коммутаторы и виртуальные маршрутизаторы для конфигурирования сетевых коммуникаций между виртуальными системами (виртуальными шлюзами).

2.8.3. Эффективное обеспечение безопасности: каждый виртуальный шлюз должен иметь возможность запуска своего собственного набора сервисов безопасности. Например, один виртуальный шлюз работает как Firewall, второй – как Firewall и IPS, третий – Firewall, IPS, Application Control, URL Filtering, и так далее.

2.8.4. Решение должно иметь специальные модули безопасности, позволяющие защищать IoT устройства (при наличии дополнительной лицензии)

2.8.5. Выделение ресурсов: решение должно обеспечивать управление вычислительными мощностями, гарантируя, что каждая виртуальная система получит то количество процессорной мощности и оперативной памяти, которая необходима для выполнения ее задач.

2.9. Решение должно обеспечивать поддержку IPv6.

2.10. Решение должно поддерживать политику, основанную на QoS.

2.10.1. Решение должно позволять гарантировать или ограничивать пропускную способность и управлять задержкой для определенного IP источника, IP пункта назначения или сервиса.

2.10.2. Решение должно иметь возможность произвольного применения правил QoS для VPN трафика.

2.11. Решение должно обеспечивать функционал IPS (системы предотвращения вторжений).

2.11.1. Система IPS должна основываться на следующих механизмах обнаружения: использование сигнатур, отслеживание аномалий протоколов, управление приложениями и обнаружение на основе поведения.

2.12. Решение должно обеспечивать функционал Идентификации пользователей.

2.12.1. Должно быть способно к сбору идентификаторов пользователей посредством запроса Microsoft Active Directory на основе событий безопасности.

2.12.2. Должно иметь метод аутентификации идентификатора пользователя на основе браузера для недоменных пользователей или компьютеров.

2.12.3. Должно иметь специального агента, который может быть установлен по политике на компьютерах пользователей, и который может собирать и передавать идентификаторы на шлюз безопасности.

2.13. Решение должно обеспечивать функционал Управления приложениями и URL-фильтрации.

2.13.1. База данных управления приложениями должна содержать свыше 10000 известных приложений.

2.13.2. Решение должно обеспечивать детальный контроль безопасности минимум для 250000 Web 2.0 виджетов.

2.13.3. Решение должно обеспечивать URL категоризацию, включающую более 200 миллионов URL.

2.13.4. Решение должно обеспечивать защиту от целевого фишинга (новых фишинговых сайтов без репутации).

2.14. Решение должно обеспечивать функционал Anti-Bot и Anti-Virus.

2.14.1. Приложение Anti-bot должно быть способно обнаружить и остановить подозрительное анормальное сетевое поведение.

2.14.2. Приложение Anti-Bot должно использовать многоуровневый механизм обнаружения, который включает репутацию IP, URL и DNS адресов и обнаружение ботов по шаблонам протоколов связи, а так же иметь механизмы, применяющие интеллектуальную аналитику для автоматической защиты от атак в протоколе DNS, включая механизмы защиты от DGA.

2.14.3. Приложение Anti-virus должно предотвращать доступ к вредоносным веб-сайтам и останавливать входящие вредоносные файлы.

2.14.4. Приложение Anti-virus должно быть способно проверять шифрованный SSL трафик.

2.15. Решение должно поддерживать инспекцию многоканального SMBv3.

2.16. Решение должно обеспечивать функционал инспекции SSL (входящего / исходящего трафика).

2.17. Решение должно обеспечивать функционал «песочницы» Sandboxing (инспекция – в облаке или на выделенном локальном устройстве).

2.17.1. Функционал «песочницы» должен обеспечивать защиту от атак нулевого дня.

2.17.2. Топология внедрения песочницы:

- Поддержка режима сетевой песочницы (network based);
- Поддержка режима инлайн (bridge mode);
- Поддержка режима почтового агента (mail transfer agent).
- Поддержка режима зеркального порта (TAP/SPAN порт).

2.17.3. Решение не должно содержать раздельную инфраструктуру для защиты почты и веба.

2.17.4. Решение должно эмулировать исполняемые файлы, архивы, документы, включая Java и flash.

2.17.5. Движок эмуляции должен поддерживать различные операционные системы, например, XP и Windows 7, в том числе специально настроенные образы (customized images).

2.17.6. Движок эмуляции должен инспектировать, эмулировать, предотвращать и передавать события в инфраструктуру защиты от зловредного ПО.

2.17.7. Решение должно обеспечивать эмуляцию файлов как небольшого размера, так и размером свыше 10Мбайт.

2.17.8. Решение должно детектировать атаки на стадии выполнения экслойта (exploitation) – т.е. до того как запускается шелл-код (shell code) и осуществляется загрузка/исполнение самого кода зловредного ПО.

2.17.9. Решение должно детектировать ROP (return oriented programming) и другие техники эксплойтов (а том числе эскалацию привилегий – privilege exploitation) посредством мониторинга выполнения последовательности инструкций центрального процессора.

2.17.10. Решение должно обеспечивать сканирование ссылок внутри почтовых сообщений для защиты от атак нулевого дня (0-day attacks), а также от неизвестного зловредного ПО.

2.17.11. Решение должно содержать средства борьбы с методиками детектирования исполнения в песочнице.

2.17.12. Решение должно обеспечивать возможность управления им с централизованного менеджмента.

2.17.13. Решение должно генерировать детальный отчет по результатам анализа каждого зараженного файла.

2.17.14. Решение должно поддерживать мгновенную доставку безопасной копии потенциально опасного документа.

2.17.15. Решение должно поддерживать следующие технологии очистки документа от потенциальных угроз:

- Конвертация в PDF с сохранением исходного форматирования, нейтрализацией ссылок, возможностью выделения и копирования текста;
- Конвертация с сохранением исходного формата и удалением активного контента: скрипты, макросы, активные ссылки, вложенные объекты, нестандартные и стандартные поля.

2.17.16. Решение должно поддерживать Веб-портал самообслуживания для запроса исходных файлов пользователями после проверки их в «песочнице».

1.17.17. Решение должно обеспечивать гибкие настройки по поддержке оригинального формата файлов и указания тех видов контента, который должен быть удален.

1.18. Решение должно обеспечивать функционал Anti-Spam и безопасности электронной почты.

1.19. Решение должно обеспечивать сканирование ссылок внутри почтовых сообщений для защиты от атак нулевого дня, решение должно поддерживать возможность блокировки ссылок с отложенной атакой.

1.20. Решение должно обеспечивать функционал IPSEC VPN.

1.20.17. Должна быть поддержка внутреннего CA (Certificate Authority), а также внешних сторонних CA.

1.20.18. Решение должно поддерживать 3DES и AES-256 шифрование для IKE фазы I и II IKEv2, а также "Suite-B-GCM-128" и "Suite-B-GCM-256" для фазы II.

1.20.19. Решение должно поддерживать как минимум следующие группы Diffie-Hellman: Группа 1 (768 бит), Группа 2 (1024 бит), Группа 5 (1536 бит), Группа 14 (2048 бит), Группа 19 и Группа 20

1.20.20. Решение должно поддерживать обеспечение целостности данных средствами md5, sha1 SHA-256, SHA-384 и AES-XCBC

1.20.21. Решение должно включать в себя поддержку для VPN типа site-to-site в следующих топологиях:

1.20.21.1. Полносвязная сеть (все-со-всеми),

1.20.21.2. Звездообразная сеть (удаленные офисы к центральному сайту)

1.20.21.3. Веерная сеть (удаленный сайт через центральный сайт на другой удаленный сайт)

1.20.22. Иметь возможность приобретения лицензии на функционал DLP. Функционал DLP должен обеспечивать контроль за утечкой конфиденциальной информации по протоколам SMTP, FTP, HTTP, HTTPS, TLS и веб-почте, должна поддерживаться возможность расшифровки SSL-трафика. Должна поддерживаться возможность определения конфиденциальных документов по преднастроенным шаблонам или по метке документов водяными знаками. Система должна поддерживать более 500 типов данных

1.21. Удаленный мобильный доступ

1.21.17. Решение должно обеспечивать функционал Удаленного мобильного доступа минимум для 50 одновременных соединений пользователей.

1.21.18. Решение должно поддерживать управляемые и неуправляемые устройства доступа, такие как BYOD (принеси собственное устройство)

1.21.19. Решение должно обеспечивать Мобильный VPN-Клиент: VPN-приложение, обеспечивающее безопасный доступ к корпоративным ресурсам через SSL или IPsec туннель.

1.21.20. Решение должно обеспечивать SSL VPN-Портал: механизм для безопасного подключения к корпоративным ресурсам через портал из веб-браузера.

1.21.21. Решение должно обеспечивать функционал безклиентного VPN: плагин, который обеспечивает удаленный доступ с предоставлением полной возможности сетевого соединения для IP-приложений. Решение должно обеспечивать функционал SSL VPN 3-уровня по запросу для подключения к корпоративным ресурсам. Решение должно поддерживать любое IP-приложение, включая ICMP, TCP и UDP, не требуя сложной конфигурации для поддержки каждого приложения. Он должен работать на удаленных компьютерах, не требуя прав администратора.

1.21.22. Решение должно обеспечивать технологию виртуального рабочего стола, которая позволяет защищать данные во время сеансов пользователей и позволяет чистить кэш после окончания сеансов. Технология виртуального рабочего стола должна защищать все данные конкретной сессии на стороне клиента, а также:

- Создавать безопасную виртуальную среду, изолированную от хоста,
- Шифровать и удалять кэш, файлы и т.д. браузера и приложений, когда сеанс окончен.

1.21.23. Решение должно поддерживать интеграцию с решениями двухфакторной аутентификации.

1.21.24. Решение должно реализовать функционал интегрированной системы предотвращение вторжений от вредоносного кода, передаваемого в веб-приложениях. Решение должно быть способно блокировать червей, различные атаки, такие как переполнение буфера, SQL и инъекции команд, межсайтовый скриптинг, настраиваемый модуль блокирования HTTP червей, защиту от обход каталога (directory traversal), защиту от отклонения заголовков (header rejection),защиту от вредоносного HTTP-кода.

1.21.25. В целом, решение должно обеспечивать следующие функции:

- Безопасный SSL VPN доступ
- Ассоциирование мобильных устройств с конечными пользователями
- Обеспечение соответствия конечных точек соединения корпоративной политике

1.22. Аппаратные и рабочие требования к шлюзу.

1.22.17. Продуктивные сетевые интерфейсы (минимальные требования):

10x1 Гбит/с медных Ethernet

1.22.18. Пропускная способность Firewall: минимум 12 Гбит/с.

1.22.19. Пропускная способность IPS: минимум 6.5 Гбит/с.

1.22.20. Пропускная способность NGFW (с активированным функционалом Firewall, Application Control и IPS): минимум 5.5 Гбит/с.

1.22.21. Пропускная способность Threat Prevention (с активированным функционалом Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot и облачный Sandbox): минимум 2.5 Гбит/с.

1.22.22. Одновременные соединения: минимум 4 миллионов.

1.22.23. Новые соединения: минимум 90 000 в секунду.

1.22.24. Локальное дисковое пространство: не менее 1x240 Гб SDD.

1.22.25. ОЗУ: не менее 16 Гб.

1.22.26. Металлические рельсы, для монтажа в серверную стойку, совместимая с данным оборудованием.

1.23. Поддержка и подписка.

Поддержка и подписка сроком на 1 год от производителя, 9x5; гарантийная замена оборудования; должны быть включены все необходимые подписки на сервисы б

Функциональные требования

1. Система защиты веб приложений должна состоять из двух подсистем:

- Подсистемы контроля и анализа трафика web-приложений (далее – WAF)
- Подсистемы управления WAF, представляющей из себя облачный сервис поставляемый производителем WAF.

2. Подсистема управления WAF должна обеспечивать управление всеми функциями WAF через web-браузер, по защищенному соединению протоколом TLS версии не ниже 1.2

3. Подсистема управления WAF должна обеспечивать сбор журнальных сообщений от WAF.

4. Подсистема управления WAF должна обеспечивать возможность настройки гранулярной политики безопасности web-приложения, с учетом портов взаимодействия и специфических URI.

5. Подсистема управления WAF должна поддерживать поиск и фильтрацию по журнальным сообщениям от WAF с заданным временным промежутком.

6. Подсистема управления WAF должна поддерживать агрегацию журнальных сообщений WAF в единый дашборд по следующим категориям:

- ТОП атакуемых web-приложений;
- ТОП источников вредоносного трафика;
- Распределение зафиксированных атак по уровням их критичности;
- Статистику запросов к web-приложениям и распределения атак по ним.

7. Подсистема управления WAF должна поддерживать автоматическую фильтрацию событий по критическим событиям в системе.

8. Подсистема управления WAF должна поддерживать профили для WAF, с возможностью задания следующих параметров:

- Токен-аутентификации для компонентов подсистемы WAF;
- Способ обновления компонентов WAF – автоматическое, по расписанию, в ручном режиме;
- Максимальное количество компонентов WAF, обслуживаемых данным профилем;

9. Подсистема управления WAF должна поддерживать возможность выгрузки политики защиты для подсистемы WAF в формате JSON.

10. Подсистема управления WAF должна поддерживать возможность настройки зон безопасности, базируясь на профилях подсистемы WAF.

11. Подсистема управления WAF должна поддерживать возможность гранулярной настройки пересылаемых в облако событий от подсистемы WAF.

12. Подсистема управления WAF должна поддерживать регистрацию событий аудита, включая события входа, изменения конфигураций, применения политик и других изменений в системе управления WAF.

13. Подсистема управления WAF должна обеспечивать возможность внесения множественных изменений в конфигурацию WAF без автоматического применения конфигурации к развернутым системам WAF. Внесенные изменения в конфигурацию должны применяться только по команде администратора.

14. Подсистема управления WAF должна поддерживать ролевую модель доступа.

15. WAF должен поддерживать возможность развертывания в следующих сценариях:

- В качестве виртуальной машины на гипервизоре ESXi с обеспечением механизма Reverse-proxy;
- В качестве нано-агента, интегрируемого с балансировщиком нагрузки NGINX;
- В качестве контейнера с интеграций в ingress controller кластера kubernetes.

16. WAF должен обеспечивать постоянное автоматическое изучение характера и шаблонов трафика при нормальной работе web-приложения.

17. WAF должен обеспечивать возможность фильтрации трафика на основе зон безопасности, без использования IP-адресов.

18. WAF должен обеспечивать непрерывное автоматическое изучение шаблона нормальной работы web-приложения на основе нескольких алгоритмов машинного обучения (Machine learning) и составления из них профиля обучения.

19. WAF должен предусматривать возможность внесения исключений в политики безопасности, после формирования профиля обучения.

20. WAF должен поддерживать автоматическое профилирование поведения отдельных пользователей, с целью уменьшения ложных срабатываний при применении механизмов защиты.

21. WAF должен поддерживать возможность формирования политик защиты от атак на основе графического интерфейса и критериев в виде защищаемого web-приложения.

22. WAF должен обеспечивать защиту от автоматических программ (ботов), а также поддерживать возможность внесения исключений для разрешения специфических ботов.

23. WAF должен обеспечивать проверку HTTP методов с автоматическим блокированием неразрешенных.

24. WAF должен поддерживать функцию сжатия контента на базе GZIP.

25. WAF должен обеспечивать проверку запросов к web-приложению на предмет обнаружения и предотвращения атак грубой силы (brute force) в формах аутентификации web-приложения.

26. WAF должен обеспечивать защиту от подмены контента на защищаемом web-приложении(defacing).

27. WAF должен обеспечивать автоматическое обновление своих компонентов, по средством связи с облачными серверами производителя.

28. WAF должен обеспечивать фильтрацию запросов, базируясь на белых/черных списках IP-адресов.

29. WAF должен поддерживать возможность создавать комплексные исключения в политике безопасности на основе комбинаций одного или нескольких критериев:

- URI;
- IP источника;
- Имен параметров web-трафика;
- Значений параметров web-трафика.

30. WAF должен обеспечивать защиту взаимодействий с программными интерфейсами приложений API (Application programming interfaces).

31. WAF должен поддерживать возможность проверки запросов к API по шаблону в формате OpenApi 3.

32. WAF должен обеспечивать минимум 100 миллионов транзакций в год.

33. Лицензия или подписка на программное обеспечение WAF должна позволять приобретения дополнительного количества транзакций в течение используемого периода.

34. Техническая поддержка должна оказываться производителем программного обеспечения со сроком на 1 год, 9x5; в том числе регулярные обновления версии программного обеспечения в течение всего используемого периода лицензии или подписки.

2. Всем заинтересованным правомочным юридическим и физическим лицам необходимо выслать выражение заинтересованности на электронную почту: t.isaeva@capitalbank.kg

Вместе, с выражением заинтересованности необходимо выслать документы, подтверждающие Вашу правомочность: Для Юридических лиц, копии документов, определяющих организационно-правовую форму юридического лица, место регистрации и основной вид деятельности: - Свидетельство о гос. регистрации/перерегистрации. Для Индивидуальных предпринимателей: предоставить копию Свидетельства о регистрации в качестве индивидуального предпринимателя или копию действующего патента (при этом вид деятельности должен совпадать с предметом и территорией закупки и охватывать минимум период до полной поставки товара и передачи по акту, сведения о наличии опыта представления аналогичных по характеру и объему услуг/товара в течение последних трех лет (заверенные или прошитые экземпляры договоров надлежащим образом), по годам, рекомендательные письма, сведения об основных позициях оборудования/техники, необходимых для выполнения услуг/поставки товара. Заполненная техническая характеристика с точным указанием наименования, спецификаций товара подписанная и заверенная печатью участника. В случае не предоставления заявка будет отклонена. Конкурсная заявка должна быть подписана руководителем организации. В случае, если конкурсная заявка не подписана руководителем организации, то к конкурсной заявке прикрепляется доверенность на другое лицо, дающее право подписи от имени Участника.

Заполненный конкурсный документ необходимо отправить по электронной почте: t.isaeva@capitalbank.kg либо по адресу: 720017, Кыргызская Республика, г. Бишкек. ул. Московская, 161. ОАО «Капитал Банк», начальнику АХО Исаевой Т., тел: +996 312 90-54-88, +996 312 90-54-70, сот тел: +996 706 97-75-53 не позднее 14:00 часов «20» марта 2024 г.

3. Закупки будут проводиться методом неограниченного участия.

Исп.: Начальник АХО Исаева Т.
тел: +996 312 90-54-88