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

«29» сентябр 2025 г.
№ 218

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

«Приобретение лицензий на систему защиты веб-трафика (Forcepoint Web Security) и продление техподдержки для нужд банка»

Ташкент 2025 год

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Продление лицензии Forcepoint Web Security и масштабирование до 700 пользователей для нужд банка

1. ОБЩИЕ СВЕДЕНИЯ

1.1 Наименование.

Продление лицензии Forcepoint Web Security и масштабирование до 700 пользователей для нужд банка

Условное обозначение системы: Система защиты веб-трафика (Forcepoint Web Security).

1.2. Цель закупки.

Цель закупки: обеспечить централизованную защиту веб-доступа, фильтрацию контента и TLS/SSL-инспекцию, контроль категорий и политик доступа, отчётность и расследования инцидентов, интеграцию с AD/IWA (NTLMv2/Kerberos), а также расширение лицензии с 400 до 700 пользователей с ко-термином.

1.3. Назначение системы защиты веб-трафика.

— Веб-фильтрация и категоризация доступа (HTTP/HTTPS).

— TLS/SSL-инспекция с политикой исключений (SSL bypass).

— Превентивная/проактивная защита от веб-угроз (встроенный AV-движок и анализаторы).

— Интеграция с Active Directory (IWA NTLMv2/Kerberos), Multi-Realm.

— **Отчётность**, делегирование видимости, **теневая копия «чистого» трафика** для расследований.

— **DLP** по **ICAP** и/или встроенный модуль (при необходимости).

2. ОБЛАСТЬ ПРИМЕНЕНИЯ.

Решение применяется в информационной инфраструктуре **АКБ «Банк Развития Бизнеса»** (головной офис и филиалы).

1. ТРЕБОВАНИЯ К РЕШЕНИЮ

1.1. Предусматривается увеличение текущего количества пользователей с **400** до **700.**

1.2. Система должна содержать отдельный менеджмент-сервер на Windows-платформе, который должен является единой консолью управления для разных систем защиты помимо защиты доступа к сети Интернет, дополнительно консоль может быть использована для защита почтового трафика и для контроля утечек конфиденциальной информации.

1.3. Система должна работать с БД Microsoft SQL, использующийся для хранения логов трафика и конфигураций системы, а также для корреляции сырых логов с Log Server (на платформе с ОС Windows).

1.4. Система должна обеспечивать поддержку развертывания основных серверных компонентов как на платформе ОС Windows, так и на ОС Unix/Linux.

1.5. Лицензия должна разрешать разворачивать любое количество виртуальных устройств без дополнительной оплаты.

1.6. Решение должно поддерживать одновременную возможность развертывания как в прозрачном режиме, так и в режиме явного «proxy».

1.7. Система должна поддерживать работу по протоколу WCCP V.2 с любым сетевым устройством производителя Cisco Systems.

1.8. Система должна поддерживать прозрачный режим прокси с помощью Policy Based Routing (PBR) с NGFW.

1.9. Система должна поддерживать PAC и WPAD в режиме явного прокси-сервера с автоматической настройкой браузера.

1.10. Система должна поддерживать интеграцию с Active Directory и бесшовную технологию аутентификации - Integrated Windows Authentication (NTLMV2 и Kerberos).

1.11. Система должна поддерживать аутентификацию Multi-Realm для работы с несколькими недоверенными доменами на разных удаленных сайтах домена, используя разные методы связки: AD, RADIUS, LDAP, NTLM и другие.

1.12. Система должна создавать профили аутентификации на основе адресов рабочих станций или портов прокси-сервера.

1.13. Система должна обеспечивать бесшовную идентификацию для всех устройств/пользователей в сети.

1.14. Система должна использовать Captive Portal, как резервный подтип аутентификации пользователей через специальную веб страницу.

1.15. Система должна обеспечивать кеширование часто запрашиваемых объектов.

1.16. Система должна поддерживать превентивные и проактивные методы фильтрации контента и защиты от malware.

1.17. Антивирусный движок системы должен быть встроен в саму систему без необходимости развертывания отдельных устройств и решений.

1.18. Система должна обеспечивать динамическую классификацию web-страниц, элементов сайтов в режиме реального времени.

1.19. Система должна использовать специализированные анализаторы (в дополнение к антивирусной инспекции).

1.20. Система должна обнаруживать и блокировать нестандартное шифрование.

1.21. Система должна обнаруживать криминальное шифрование (шпиона) в исходящем трафике.

1.22. Система должна обеспечивать защиту от связок эксплойтов и других особо опасных веб-угроз.

1.23. Система должна обнаруживать кражу паролей в исходящем трафике.

1.24. Система должна поддерживать фильтрацию более 150 протоколов IM, P2P, Streaming Media, протоколов удаленного доступа, возможности обхода прокси-сервера и других приложений.

1.25. Система должна содержать встроенный функционал автоматической классификации сайтов по содержимому страниц, распознающая не менее 100 тематических категорий (без использования облачных вычислений).

1.26. Система должна поддерживать защиту от обхода прокси-сервера.

1.27. Система должна сохранять теневую копию трафика в чистом виде для расследования.

1.28. Система должна сканировать весь траффик в обоих направлениях и определять бот-сети и кражу данных в исходящем траффике.

1.29. Система должна обеспечивать режим безопасного поиска основных поисковых систем: Google, Bing, Yahoo, Yandex.

1.30. Система должна поддерживать возможность включать и выключать инспекцию в трафике activex, javascript, vbscript.

1.31. Система должна обеспечивать анализ приложений web 2.0/ajax.

1.32. Система должна поддерживать терминацию HTTPS трафика для инспекции трафика и BYPASS инспекции SSL.

1.33. Система должна содержать механизм, который поддерживает детальное управление политиками по пользователю, группе, ip адресам или времени.

1.34. Система должна поддерживать временную квоту для определенных категорий сайтов.

1.35. Система должна содержать оптимизатор трафика, который определяет загрузку канала и в случае превышения определенного порога блокирует доступ к указанным категориям сайтов.

1.36. При необходимости, система должна иметь возможность поддерживать работу с своей программно-аппаратной системой эмуляции кода «песочницей».

1.37. Система должна предоставлять интегрированную графическую отчётность, готовые шаблоны более 60 типов, с возможностью агрегации отчетов в случае установки нескольких прокси-серверов.

1.38. Система должна строить интерактивные отчеты с поддержкой «углубления» (Drilling Down).

1.39. Система должна ограничивать (делегировать) видимость данных отчетности по подразделениям.

1.40. Система должна поддерживать централизованную настройку политик с применением ко всем устройствам в кластере.

1.41. Система должна обеспечивать расследование инцидентов безопасности с теневой копией трафика.

1.42. Система должна обеспечивать делегирование прав на настройку политик фильтрации по подразделениям.

1.43. Система должна поддерживать интеграцию по ICAP с любой DLP.

1.44. Система должна иметь возможность включения встроенного DLP-модуля с OCR функцией без использования ICAP связки.

1.45. Система должна осуществлять OCR поддержку без дополнительных лицензий.

1.46. Система при опциональном использовании встроенного модуля DLP, должна иметь полноценный функционал DLP на веб канале со следующими классификаторами для определения конфиденциальной информации: цифровые слепки (технология Preciseid), машинное обучение, свойства файла, регулярные выражения, словари и ключевые фразы.

1.47. Система должна обеспечивать интеграцию фильтра веб-категоризации с маршрутизаторами Cisco на уровне стандартной функциональности Cisco IOS.

1.48. Система должна иметь возможность установки системы в Standalone режим с подключением к mirror-порту коммутатора через технологию SPAN (поддержка TCP-reset).

2. ТРЕБОВАНИЯ К ИСПОЛНИТЕЛЮ.

1. Исполнитель должен предоставить копию авторизационного письма от Производителя Продукта с подтверждением наличия у Участника права на продажу с последующим внедрением предлагаемого ПО для конечного Заказчика на территории Республики Узбекистан. Авторизационное письмо должно содержать номер текущей закупки, а также быть датированным не ранее даты публикации/выхода закупки на официальном портале. В случае предоставления авторизационного письма на иностранном языке, участник должен предоставить заверенный перевод на русский язык.

2. Исполнитель должен предоставить официальное письмо-гарантию на своем бланке об обязательстве выполнить поставку Системы во владение и её технической поддержки от одного производителя сроком на 1 (одного) года с даты активации Продукта у Заказчика.

3. ТРЕБОВАНИЯ ПО ПРАВИЛАМ СДАЧИ И ПРИЕМКИ

Ссылка на скачивание программного продукта последней стабильной версии, лицензия и инструкция по установке отправляется Исполнителем на электронную почту Заказчика.

4. ТРЕБОВАНИЯ К ОБЪЕМУ И/ИЛИ СРОКУ ПРЕДОСТАВЛЕНИЯ ГАРАНТИЙ

Количество пользователей 700 шт, срок техническое поддержки 1 год.

5. Дополнительные (иные) требования

Исполнитель должен защитить Покупателя от материальной ответственности по искам третьих лиц в отношении нарушения патентных и лицензионных прав, а также прав на применение торговой марки или промышленных разработок, связанных с использованием товаров, любой их части в стране Заказчика.

6. Требования к количеству, комплектации, месту и сроку (периодичности) поставки

Сроки поставки лицензий — до 15 рабочих дней. Место поставки — г. Ташкент, ул. Навои 18А, 100011 или электронная почта f.turgunbayev@brb.uz.

согласные: B.Shamsiyev, Z.Orifxo‘jayev

https://hujjat.brb.uz/?pin=iQ11bV91&id=3a455ebf-a6d4-4b79-8a96-93b213ea3c9d