ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 347352
способом Открытый тендер на понижение

Лот № (85 Т, 1170277) Маршрутизатор

Заказчик **Товарищество с ограниченной ответственностью "KLPE" (КейЭлПиИ)**
Организатор **Товарищество с ограниченной ответственностью "KLPE" (КейЭлПиИ)**

1. Краткое описание ТРУ

Наименование	Значение
Номер строки	85 Т
Наименование и краткая характеристика	Маршрутизатор, среднего класса
Дополнительная характеристика	Описание: Программно-аппаратный комплекс по информационной безопасности
Количество	1.000
Единица измерения	Штука
Место поставки	КАЗАХСТАН, г.Нур-Султан, район "Есиль", ул. Е-10, 17/10, БЦ "Зеленый квартал", 4 этаж
Условия поставки	DDP
Срок поставки	С даты подписания договора в течение 60 календарных дней
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

2. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики

Маршрутизатор (Программно- аппаратный комплекс по информационной безопасности)

1. Требования к потенциальному поставщику.

Потенциальный поставщик в конкурсной заявке должен предоставить детальную техническую спецификацию на предлагаемое оборудование с указанием производителя, парт номеров, моделей и т.д. для сопоставления с требованиями технической спецификации.
Потенциальный поставщик при поставке товара должен оказать следующие сопутствующие услуги:
1. Осуществить монтаж маршрутизатора в серверном помещении заказчика;
2. Осуществить подключение маршрутизатора в соответствии с сетевой архитектурой Заказчика;
3. Осуществить настройку правил маршрутизации и политик безопасности по согласованию с Заказчиком;
4. Провести инструктаж уполномоченных сотрудников заказчика по работе с Маршрутизатором.
Для оказания сопутствующих услуг по монтажу, настройке и осуществлению технической консультации специалистов Заказчика потенциальный Поставщик должен иметь в своем штате не менее одного технического специалиста, сертифицированного производителем предлагаемого оборудования. Копию сертификата приложить в составе конкурсной заявки.
Потенциальный поставщик должен являться официальным авторизованным партнером компании-производителя программного обеспечения, лицензии и подписок для получения всех возможных обновлений программного обеспечения, сигнатур и угроз, предлагаемых к поставке Маршрутизатора, что должно подтверждаться приложением авторизационного письма от компании-производителя. Копию письма приложить в составе тендерной заявки.

2. Технические требования к Маршрутизатору.

2.1. Общие требования.

2.1.1. Маршрутизатор должен быть выполнен в виде единого устройства высотой не более 1 Rack unit, устанавливаемого в стандартную монтажную стойку 19” с использованием комплектного крепежа;
2.1.2. Маршрутизатор должен иметь специализированную аппаратную платформу, позволяющую беспрепятственно управлять устройством даже в случае его полной загрузки. Должны быть обеспечены выделенные вычислительные ресурсы для обработки контролируемого трафика и отдельно для решения задач управления;
2.1.3. Управление каждым отдельным устройством должно осуществляться по протоколам HTTPS и SSH без необходимости установки какого-либо дополнительного ПО управления на рабочую станцию администратора;
2.1.4. Интерфейс управления Маршрутизатора (веб и CLI) должен быть унифицирован с подсистемой централизованного управления, логирования, отчетности, обновления ПО.

2.2. Требования к производительности Маршрутизатора.

2.2.1. Декларируемая производителем пропускная способность каждого устройства в режиме межсетевого экранирования с обеспечением идентификации приложений и пользователей – не менее 1970 Мбит/сек.;
2.2.2. Декларируемая производителем пропускная способность каждого устройства в режиме межсетевого экранирования с обеспечением идентификации приложений и пользователей с включенным функционалом проверки трафика на наличие угроз (всех сигнатур уязвимостей IPS, вредоносного ПО и Anti-spyware) – не менее 770 Мбит/сек;
2.2.3. Максимальное количество поддерживаемых сессий уровня приложений – не менее 191000.

2.3. Требования к поддерживаемым протоколам и режимам функционирования Маршрутизатора.

2.3.1. Поддержка статической маршрутизации и протоколов динамической маршрутизации BGP, OSPF, RIP v2;
2.3.2. Поддержка работы сетевых интерфейсов в режимах прослушивания «зеркалированного» трафика со SPAN-портов подключаемого коммутационного оборудования, в прозрачном режиме без изменения MAC и IP-адресов, в режиме коммутации трафика (Layer 2), в режиме маршрутизации трафика (Layer 3);
2.3.3. Поддержка одновременной работы разных сетевых интерфейсов в любых перечисленных режимах в любой комбинации без ограничений;
2.3.4. Поддержка IPv6, включая идентификацию приложений и пользователей;
2.3.5. Поддержка multicast – PIM-SM, PIM-SSM, IGMP v1, v2, v3;
2.3.6. Поддержка маршрутизации между VLAN, организованными на Маршрутизаторе;
2.3.7. Поддержка функционала трансляции адресов NAT, сервера DHCP и DHCP relay;
2.3.8. Поддержка тегирования фреймов по 802.1Q (не менее 4094 VLAN);
2.3.9. Размер таблицы ARP-записей – не менее 3000 записей;
2.3.10. Поддержка агрегирования интерфейсов по 802.3ad (поддержка LACP);
2.3.11. Поддержка передачи больших пакетов (Jumbo frames);
2.3.12. Поддержка виртуальных маршрутизаторов – не менее 5 шт.;
2.3.13. Поддержка зон безопасности – не менее 40 шт..

2.4. Требования к интерфейсам Маршрутизатора.

2.4.1. 10/100/1000 Мбит Ethernet с разъемом RJ-45 – не менее 4 портов;
2.4.2. Gigabit Ethernet с разъемом SFP – не менее 4 портов;
2.4.3. Gigabit Ethernet/ Then Gigabit Ethernet с разъемом SFP/SFP+ – не менее 4 портов
2.4.4. Выделенный интерфейс 1 Gigabit Ethernet для объединения в отказоустойчивый кластер – не менее 2 портов;
2.4.5. Выделенный (out-of-band) порт управления Маршрутизатором 10/100/1000 Мбит Ethernet с разъемом RJ-45 – не менее 1 порта;
2.4.6. Консольный порт управления с разъемом RJ-45 – не менее одного.
2.4.7. Консольный порт управления с разъемом micro-USB – не менее одного.
2.4.8. Порт USB – не менее одного.

2.5. Требования к выполняемым функциям Маршрутизатора.

2.5.1. Работа на уровнях с Layer-2 по Layer-7 модели OSI;
2.5.2. Межсетевое экранирование с контролем состояния сессий;
2.5.3. Распознавание и блокировка сетевых приложений на седьмом уровне модели OSI по трафику, проходящему через Маршрутизатор, в том числе индивидуально для всех приложений, использующих общий порт, в том числе 80 и 443, и использующих динамические TCP/UDP-порты;
2.5.4. Распознавание в инспектируемом трафике на Layer-7 модели OSI по сигнатурам, хранимым на МЭ, следующих категорий приложений:
2.5.5. Корпоративные приложения:
2.5.5.1. Сервисы аутентификации, включая Microsoft Active Directory, Netlogon, LDAP, RADIUS, TACACS;
2.5.5.2. СУБД, включая Microsoft SQL, Oracle, DB2, Postgres, Sybase;
2.5.5.3. Файловые сервисы, включая Microsoft SMB;
2.5.5.4. ERP, CRM, включая SAP, 1C;
2.5.5.5. Системы электронного документооборота и обмена сообщениями, в том числе EMC Documentum, Microsoft SharePoint, Exchange, Lync, Office 365, Google Docs, Lotus;
2.5.5.6. Протоколы обмена электронной почтой: SMTP, POP3, IMAP;
2.5.5.7. Протоколы VoIP и аудио-видео-конференций, включая SIP, H.323, H.245, H.225, Webex;
2.5.5.8. Сервисы обновления программного обеспечения, включая Microsoft Update, антивирусное ПО (Kaspersky, Symantec, TrendMicro, McAfee, ESET), Adobe, Java, Apple;
2.5.5.9. Сервисы резервного копирования;
2.5.5.10. Сервисы виртуализации и терминального доступа, включая VMware, Citrix, Microsoft RDP;
2.5.5.11. Прочие протоколы и технологии, применяемые для создания распределенных приложений, включая CORBA, SOAP;
2.5.5.12. Протоколы удаленного доступа, включая Telnet, SSH, VNC, Radmin;
2.5.5.13. Сетевые протоколы, включая протоколы динамической маршрутизации и SSL, IPsec VPN;

2.5.6. Приложения сети Интернет:
• Электронная почта, включая Gmail, Yandex.Mail, Mail.ru, Hotmail;
• Социальные сети, включая Facebook, Google+, LinkedIn, ВКонтакте, Одноклассники, «Мой Мир»;
• Средства мгновенного обмена сообщениями, включая ICQ, Jabber, IRC, MSN, аналогичные сервисы в составе перечисленных социальных сетей;
• Средства аудио-видео-конференций, включая Skype;
• Средства файлового обмена по HTTP(S) и peer-to-peer, включая Dropbox, BitTorrent, eMule, Google Drive, Yandex Disk, Gnutella, Boxnet, SkyDrive, WebDav;
• Потоковое аудио-видео (вне зависимости от веб-сайта), включая YouTube, Vimeo, аудио и видео по HTTP;
• Средства публикации рабочего стола и предоставления удаленного доступа, включая Team-Viewer, LogMeIn;
• Внешние прокси-серверы и анонимайзеры, включая Tor, Ultrasurf, FreeGate, SOCKS, PHP Proxy;
• Средства построения частных VPN и туннелирования поверх других приложений, включая FreeNet, Open-VPN, VTun, RDP-to-TCP, TCP-over-DNS;
2.5.7. Предоставление встроенных в МЭ средств создания собственных сигнатур приложений по регулярным выражениям с использованием декодеров HTTP(S), FTP, SMB, SMTP, RPC и др., а также по маске для содержимого TCP/UDP-пакетов;
2.5.8. Распознавание сетевых приложений по зашифрованному SSL (поддержка ключей RSA до 2048 бит) и SSHv2 трафику, проходящему через Маршрутизатор (дешифрация SSL, SSHv2), - как для входящих, так и для исходящих подключений, прозрачно для пользователей в домене, с возможностью контроля отдельных функций приложений, включая отправку сообщений в социальных сетях, файловый обмен, потоковое аудио, видео;
2.5.9. Инспекция туннелей:
2.5.10. Generic Routing Encapsulation (GRE) (RFC 2784);
2.5.11. Nonencrypted IPSec traffic [NULL Encryption Algorithm for IPSec (RFC 2410);
2.5.12. Transport mode AH IPSec;
2.5.13. General Packet Radio Service (GPRS) Tunneling Protocol for User Data (GTPU)).
2.5.14. Последовательное распознавание различных приложений, используемых в рамках одной сессии;
2.5.15. Распознавание пользователей, использующих сетевые приложения, за счет интеграции с корпоративными сервисами аутентификации пользователей, такими как Microsoft Active Directory, Microsoft Exchange, Novell eDirectory, LDAP, Citrix; возможность интеграции с другими сервисами аутентификации (например, контроллерами беспроводных сетей) через открытый XML API; возможность использования принудительной авторизации пользователей, используя WEB страницу – “Captive portal”; поддержка Kerberos, Tacacs+, SAML v.2, поддержка L3-роуминга пользователей с помощью WMI и NetBios опросов;
2.5.16. Инспекция передаваемого через Маршрутизатор содержимого трафика в реальном режиме времени в потоке по сигнатурам и поведению, защита от уязвимостей, сетевых атак и вредоносного ПО, распознавания типов файлов по их сигнатурам, определение вирусов, передаваемых по веб, через электронную почту, FTP, SMB, шпионского ПО, сетевых червей, блокировка передачи определенного содержимого с использованием регулярных выражений, в том числе для приложений, использующих шифрование SSL и SSHv2;
2.5.17. Создание правил для проходящего через Маршрутизатор трафика в единой политике безопасности, используя в качестве квалификаторов следующие параметры каждого соединения:
2.5.18. IP-адрес отправителя,
2.5.19. IP-адрес получателя,
2.5.20. используемые сервисы уровня L4: порты для протоколов TCP и UDP,
2.5.21. имена пользователей или групп пользователей из Active Directory,
2.5.22. приложения 7 уровня модели OSI,
2.5.23. URL категории.
2.5.24. Создание правил в единой политике безопасности, используя в качестве квалификаторов данные об IP-адресах отправителя, получателя, используемых сервисов (TCP/UDP-портов), имена пользователей, групп пользователей и используемых пользователем или группой пользователей приложений или определенных категорий приложений. В создаваемых политиках должна иметься возможность реализации следующих действий:
• Разрешения или запрета;
• Разрешения конкретному приложению или категории приложений использовать только стандартные или строго определенные TCP/UDP-порты. При этом эти порты не должны быть использованы другими приложениями без политики, разрешающей такие взаимодействия в явном виде;
• Разрешения, но при этом сканирования на вирусы и другие угрозы;
• Разрешения или запрета, основанного на расписании, пользователе или группе пользователей;
• Расшифровать и проверить. Если не удалось расшифровать (в случае нестандартного крипто-алгоритма, устаревшего сертификата и др.) – запретить;
• Не расшифровывать определенные категории URL и отдельные доверенные веб-сайты;
• Применить маркировку DSCP и ограничение по трафику, используя политики QoS на основе приложений, IP-адресов, пользователей и групп пользователей;
• Аппаратная реализация QoS для трафика real-time, идентифицируемого на уровне приложений;
• Применить перенаправление трафика на основе политик (Policy Based Forwarding);
• Разрешить отдельные функции приложения;
• Любая комбинация из вышеприведенных действий;
2.5.25. Антивирусная защита, защита от шпионского ПО, защита от уязвимостей и сетевых атак (система обнаружения и предотвращения вторжений), URL-фильтрация с использованием динамической репутационной базы, поддерживающая

категоризацию для разных разделов одного и того же веб-сайта, включая поддержку категорий для веб-сайтов на русском языке, блокировка передачи файлов по типам, определенных сигнатурами;
2.5.26. Анализ подозрительных DNS-запросов и локализация зараженных станций с помощью технологии DNS sinkhole (подмена ответа DNS-сервера);
2.5.27. Защита от техник уклонения (evasions), пример MPTCP
2.5.28. Предоставить сервис сканирования неизвестных потенциально вредоносных файлов в песочнице с операционными системами Microsoft Windows, Linux методом эмуляции запуска и просмотра документов.
2.5.29. Песочница должна проверять подозрительные исполняемые файлы (в том числе EXE, DLL, SCR, BAT, и др.), ELF файлы, документы форматов PDF, MS Office 2003, 2007 и выше, Java и Flash, Android APK, Mach-O, DMG и PKG, архивы RAR, ZIP, 7Zip.
2.5.30. Маршрутизатор должен отправлять на проверку в песочницу подозрительные файлы, передаваемые в приложениях HTTP, HTTP, SMTP, POP3, IMAP, SMB, FTP, а также их реализации через SSL, если они существуют.
2.5.31. Песочница должна генерировать и присылать в Маршрутизатор отчет о проверке файла.
2.5.32. Песочница должна генерировать сигнатуры для блокирования zero-day для использования на всех Маршрутизаторах компании в перечисленных приложениях в течение 5 минут после получения файла на проверку.
2.5.33. Маршрутизатор должен получать из песочницы сигнатуры файлов и иметь движок блокировки по новым сигнатурам, которые получены от облачной или локальной песочницы.
2.5.34. Облачная песочница поставщика должна иметь возможность обмена сигнатурами между всеми заказчиками поставщика.
2.5.35. Маршрутизатор должен получать из песочницы индикаторы компрометации: IP, URL, DNS, которые использует вредоносный код и блокировать соединения по списку вредоносных индикаторов.
2.5.36. Песочница должна проверять ссылки http:// и https:// в электронной почте по протоколам STMP/POP3.
2.5.37. Песочница должна проверять файлы в приложениях зашифрованных SSL, минимум в HTTPS протоколе.
2.5.38. Песочница должна обеспечивать анализ поведения подозрительных файлов и ссылок в частном или внешнем облаке («песочнице»), обнаружение нового вредоносного ПО и автоматическую генерацию антивирусной сигнатуры в течение 5 мин. и обновление репутационной базы URL в течение 30 мин., устанавливаемые на все устройства Заказчика, имеющие соответствующие подписки;
2.5.39. Возможность интеграции с подсистемой обнаружения угроз «нулевого» дня, реализованной на базе выделенного аппаратного устройства того же производителя, размещаемого на центральном объекте Заказчика (частное облако) и позволяющего автоматическую генерацию антивирусной сигнатуры локально на выделенном аппаратном устройстве на площадке ЦОД Заказчика в течение 5 мин.;
2.5.40. Выделенная локальная песочница должна иметь API для приема файлов на проверку как от Маршрутизаторов, так и сторонних сервисов.
2.5.41. Песочница должна создавать отчеты по выполненным проверкам и иметь возможность просмотра этих отчетов в формате PDF.
2.5.42. Облачная песочница должна использовать технологию Bare metal analysis без использования эмуляции операционной системы.
2.5.43. Маршрутизатор должен иметь возможность разные типы файлов отправлять в разные песочницы, например, exe файлы в облачную песочницу, а DOC файлы в локальную песочницу.
2.5.44. Облачная песочница должна принимать PE файлы на проверку, даже в отсутствии подписки.
2.5.45. Развитые функции визуализации: визуализация в простом и удобно читаемом формате активности сетевых приложений, обнаруженных и блокированных сетевых угроз, использующих приложения пользователей. Возможность фильтрации информации, используя различные фильтры (по приложениям, по угрозам, по пользователям, IP-адресам, TCP/UDP-портам, зонам безопасности, типам угроз и др.);
2.5.46. Обязательно наличие вентильных перепрограммируемых матриц FPGA для обработки трафика антивирусом и IPS.
2.5.47. Автоматическая корреляция логов различного типа (межсетевое экранирование, защита от угроз, контроль передачи файлов, URL-фильтрация), сгенерированных в рамках одной сессии;
2.5.48. Возможность автоматической корреляции событий информационной безопасности на МЭ посредством обновляемых корреляционных объектов, которые задействуют информацию, полученную от антивирусной защиты, защиты от шпионского ПО, защиты от уязвимостей и сетевых атак, защиты от угроз и вирусов 0-ого дня на уровне сети и рабочих станциях с возможностью принудительной аутенфикацию пользователя при помощи двухфакторной аутенфикации (МФА), для которого сработал корреляционный объект;
2.5.49. Защита от кражи логинов и паролей пользователей за счет интеграции с AD, мониторингом пересылки учетных записей в недоверенную зону безопасности, принудительную аутенфикацию пользователя при помощи двухфакторной аутенфикации (МФА);
2.5.50. Создание отчетов. Маршрутизатор должен иметь функции по автоматической генерации отчетов и отчетов по расписанию по различным тематикам (обнаруженные угрозы, объемы переданной информации с разбиением по пользователям, приложениям и пр.), функции по ручной настройке создаваемых отчетов. Должна иметься возможность просмотра отчетов как непосредственно через графический веб-интерфейс управления (GUI) Маршрутизатором, так и возможность экспортирования отчетов в форматы PDF и CSV;
2.5.51. Интеграция с подсистемой централизованного управления, логирования, отчетности, обновления ПО Маршрутизаторов того же производителя;
2.5.52. Наличие функционала отправки расшифрованного SSL трафика на внешние устройства;
2.5.53. Наличие функционала забора трафика с внешних устройств и шифрование в SSL туннель для передачи через Интернет;
2.5.54. Прошивка баз сигнатур приложений и сигнатур IPS и сигнатур антивируса в чипы аппаратной акселерации FPGA для инспекции трафика;

2.5.55. Буферизация логов локально на встроенном жестком диске в случае кратковременной недоступности подсистемы централизованного логирования;
2.5.56. Наличие отдельного отчета по приложениям типа SaaS;
2.5.57. Наличие функционала IPSec VPN, SSL VPN и без клиентского VPN функционала (clientless VPN SSL);
2.5.58. Наличие функционала гранулированного контроля удаленных пользователей к корпоративной рабочей среде с возможностью проверки на наличие определенного программного обеспечения на рабочей станции пользователя, а также доступ через мобильные устройства.
2.5.59. Интеграция со сторонними SIEM/SIM-системами по протоколу Syslog с обеспечением гибкой настройки формата логов;
2.5.60. Ролевое управление доступом локальных администраторов:
2.5.61. Возможность ограничить область просмотра и управления на уровне устройства в целом, а также отдельных виртуальных систем (контекстов);
2.5.62. Возможность предоставить доступ в режиме правки или только для чтения, либо запретить доступ к любому разделу веб-интерфейса МЭ;
2.5.63. Возможность предоставить доступ в режиме правки или только для чтения, либо запретить доступ к CLI МЭ.

2.6. Требования к комплектации Маршрутизатора.

2.6.1. Маршрутизатор должен комплектоваться всеми необходимыми кабелями для включения в сеть электропитания.
2.6.2. В комплект должны входить все необходимые лицензии и подписки для получения всех возможных обновлений программного обеспечения, сигнатур приложений и угроз, репутационной базы URL и использования сервиса обнаружения угроз «нулевого» дня в течении 3 лет.
2.6.3. На Маршрутизатор должна быть предоставлена техническая поддержка от производителя на 3 года.

3. Дополнительные требования при поставке товара
Поставщик при поставке товара должен предоставить гарантию на предлагаемый к поставке Маршрутизатора сроком не менее 36 месяцев, что должно подтверждаться официальным письмом от производителя Комплекса (копию письма приложить при поставке товара).
В целях исключения возможности поставки контрафактного оборудования поставщик должен предоставить письмо от производителя товара, подтверждающее, что поставляемое поставщиком оборудование и программное обеспечение является новым, неиспользованным ранее, не восстановленным, не является контрафактным и поддерживается официально по сервисной линии производителя (копию письма приложить при поставке товара).

Подписал	Скендирова Меруерт Белгибаевна
Дата подписания	25.10.2019