**Техническая спецификация**

**по закупу программного обеспечения для нужд**

**АО "Кедентранссервис" по лоту №1**

1. **Общие требования:**
	1. Потенциальный поставщик обязан поставить лицензию на программное обеспечение (далее - Товар) согласно настоящей Технической спецификации;
	2. Потенциальный поставщик обязан обеспечить установку и настройку товара сертифицированными специалистами имеющих опыт работы с активным сетевым оборудованием, с серверным оборудованием (администрирование, настройка, ремонт и т.д.) и программным обеспечением Microsoft, VMware, Oracle Enterprise Linux, RedHat Enterprise Linux, в частности Oracle MySQL Developer, MCSA Security Windows Server, PMI, VMware vSphere ICM, HP VMware vSphere 5, HP ProLiant ML.DL.SL Servers, HP Network Infrastructure, Official certified Installation and Support Storage System Course swich. Products, Official certified Technical Support Server System Course, HP-UX: Администрирование систем и сетей, диагностика систем и сетей, Управление разделами в HP-UX: nPars, vPars и виртуальные машины Integrity (сертификаты приложить в заявке, в случае представления сертификатов на иностранном языке, приложить нотариально заверенный перевод на русском языке);
	3. Потенциальный поставщик обязан подтвердить право на поставку лицензионного программного обеспечения письмом производителя (авторизационное письмо приложить в заявке, в случае представления авторизационного письма на иностранном языке, приложить нотариально заверенный перевод на русском языке);
	4. Потенциальный поставщик должен в составе технической спецификации представить письмо обязательство за подписью первого руководителя о том, что поставляемый потенциальным поставщиком товар будет быть новым, неиспользованным;
	5. Товар должен сопровождаться подпиской на техническую поддержку на период до одного года. Потенциальный поставщик в составе Технической спецификации должен представить гарантийное письмо за подписью первого руководителя с указанием срока технической поддержки и о том, что подписка на техническую поддержку будет предоставляться в соответствии со следующими возможностями:
	6. Контакт со службой технической поддержки посредством телефона, электронной почты и интерактивного чата;
	7. Техническая поддержка должна быть доступна в течение 24 часов – на русском языке в рабочие часы в будни, в ночное время и выходные дни возможно на английском языке;
	8. Обозначение критичности проблемы при создании заявки в службе технической поддержки;
	9. Подписка на техническую поддержку в период своего действия должна гарантировать бесплатные обновления продукта, в том числе бесплатный переход на новую версию продукта.

(приложить гарантийное письмо в составе заявки)

* 1. Срок поставки и инсталляции до 31 декабря 2017 года с момента подписания договора;
	2. Поставка осуществляется путем получения электронных лицензии на программные обеспечения по электронному адресу заказчика lic@kdts.kz и установке на серверах Общества;
	3. Согласование этапов проведения работ;
	4. Консультация представителя Заказчика, базовым навыкам администрирования Товара.

|  |  |
| --- | --- |
| **№ п.п** | **Технические требования к программному обеспечению Kerio Control – 1 штука** |
| **Состав программного обеспечения** |
| 1. | Лицензия на ПО Kerio Control – на 300 активных сессий.  |
| **Программное обеспечение должно обеспечивать следующие основные функции и возможности**  |
| 2. | * 1. ПО должно иметь возможность Межсетевого экрана (файервол) и маршрутизатора:
* Корпоративный межсетевой экран, получивший сертификат ICSA Labs и ФСТЭК\*.
* Deep packet inspection — глубокая проверка пакетов.
* Система обнаружения и предотвращения атак (IPS).
* Контроль приложений.
* Проверка пакетов с отслеживанием состояния.
* DHCP сервер.
* Сервер пересылки DNS.
* Публикация локальных сервисов в Интернет (dNAT).
* Фильтрация по MAC.
* Фильтрация c помощью GeoIP.
* Переадресация запросов на обнаружение сервисов (Service Discovery forwarding).
* Антиспуфинг.
* Гостевая сеть с порталом авторизации.
* Поддержка 802.1Q VLAN.
* Мастер настройки правил трафика.
* Временные условия.
* Ограничения количества подключений.
* Динамические DNS.
* Настраиваемые таблицы маршрутизации.
* Обратный прокси-сервер.
* Одновременная поддержка протоколов IPv4 и IPv6.
* Поддержка трансляции префикса сети для протокола IPv6.
* Объявления маршрутизаторов IPv6.
* Несколько IP-адресов на одном сетевом интерфейсе.
	1. ПО должно иметь возможность организации VPN:
* VPN-клиент для Windows, Mac и Linux.
* Поддержка раздельного туннелирования.
* Одновременное установление нескольких туннелей сеть-к- сети, клиент-к-сети.
* IPsec клиент-сервер и сервер-сервер.
* L2TP/IPsec для мобильных устройств.
* Возможность создания постоянного подключения.
* Шифрование SSL.
* Резервные подключения для VPN туннелей.
* Поддержка NAT.
* Проверка подлинности пользователя при помощи локального каталога.
* Поддержка автоматической и настраиваемой маршрутизации.
	1. ПО должно иметь возможность формирования отчетов и ведения мониторинга:
* Отчеты через Kerio Control Statistics.
* Автоматические отправляемые отчеты по электронной почте.
* Приложение для Android, Apple Watch и iOS (уведомления и мониторинг)
* Подробные отчеты об использовании: веб-сайтов, протоколов, пропускной способности.
* Классификация трафика по категориям (мультимедиа, обмен сообщениями, передача больших файлов...).
* Наиболее часто посещаемые веб-сайты и наиболее активные пользователи по веб-категориям.
* Отчеты можно фильтровать по отдельным пользователям, группам и всей сети.
* Почасовой трафик по пользователям.
* Поиск по ключевым словам через Google.
* Отчеты по фильтрации контента Kerio Control Web Filter.
* Оповещения по электронной почте.
* Ведение внешнего системного журнала.
* Мониторинг SNMP.
* Монитор работоспособности системы.
* Диаграммы трафика.
* Панель администратора.
* Мониторинг активности хостов в реальном времени.
	1. ПО должно иметь возможность управления балансировкой нагрузки и пропускной способностью:
* Балансировка нагрузки между несколькими интернет-каналами.
* Маршрутизация на основе политик.
* Автоматическое переключение активного интернет канала.
* Гарантия скорости передачи данных для трафика с высокой важностью (качество обслуживания QoS).
* Ограничение скорости передачи данных для трафика низкой важности..
* Квотирование объёма передаваемых данных пользователями.
* Регулируемые квоты ограничения для полосы пропускания и ограничения для скорости передачи данных.
* Правила на основе интервала времени, типа трафика, пользователей, служб, значений DSCP.
	1. ПО должно иметь возможность администрирования:
* Веб-консоль для централизованного мониторинга и управления множеством установок Kerio Control.
* Удаленное администрирование веб-интерфейса.
* Настраиваемая панель администрирования.
* Автонастройка или самонастройка конфигурационных параметров.
* Распространение параметров между программными комплектами.
* Экспорт/импорт конфигурации.
* Резервное копирование конфигурации на MyKerio или на FTP-сервер.
* Шаблон для настройки пользователя.
* Регулируемый уровень административных прав.
* Автоматическое обновление версии программного обеспечения.
* Удобные средства отладки.
* Локализация на множество языков, в том числе на русский язык.
	1. ПО должно иметь возможность обеспечения контент-фильтра:
* Ограничение по интервалу времени.
* Блокировщик P2P.
* Категории URL с "белыми списками" (Kerio Control веб-фильтр).
* Правила контента на основе интервалов времени, пользователей, приложений, веб-категорий, URL групп, типов файлов и др..
* Настраиваемая страница отказа в доступе.
* Административные оповещения.
* Настраиваемые URL.
* HTTPS фильтрация.
* Поддержка регулярных выражений в правилах URL.
* Запрещенные слова.
* Безопасный поиск (SafeSearch) для поисковых систем.
* Политика FTP.
* Прокси-сервер c кэшем.
* Фильтрация с помощью антивируса.
* Настраиваемая страница отказа в доступе.
	1. ПО должно иметь возможность аутентификации пользователей:
* Apple/Open Directory.
* 2-факторная проверка пользователя для удаленного доступа.
* Аутентификация терминальных пользователей на прокси-сервере.
* Локальная база данных пользователей.
* Проверка подлинности Kerberos/NTLM.
* RADIUS-сервер.
* Защита от подбора пароля.
	1. ПО должно иметь возможность предотвращения атак:
* Анализ поведения на основе Snort.
* База данных правил Emerging Threats.
* «Черный» список IP-адресов.
* Несколько уровней безопасности.
* Обработчик исключений ложных срабатываний.
	1. ПО должно иметь возможность контроля приложении:
* База данных приложений (Skype, Facebook, BitTorrent, и до.)
* Категории приложений
* Отчеты приложений в режиме реального времени
* Правила содержимого для приложений на основании пользователя, хоста или промежутка времени (разрешение или запрет).
* Правила пропускной способности для приложений (ограничение или резервация).
	1. ПО должно иметь возможность контроля приложении:
 |
| **ПО должно соответствовать следующим системным требованиям** |
| 3. | * 1. Системные требования:
* Процессор: 500 MHz
* Оперативная память: 2 GB RAM
* Жесткий диск: 8 GB HDD
* Сетевой интерфейс: 2 Ethernet (10/100/1000 Mbit).
	1. Системные требования для установки в виртуальной среде:
* Для Vmware:
* Поддерживаемые продукты:
* VMware Workstation/Player 11.0 or 12.0
* VMware Fusion 7.0 or 8.0
* VMware ESXi / vSphere Hypervisor 5.5 or 6.0
* Процессор: 2 GHz
* Оперативная память: 2 GB RAM назначенная виртуальной машине
* Жесткий диск: 8 GB выделенный для HDD
* Сетевой интерфейс: 2 назначенных виртуальных сетевых адаптера
* Для HyperV
* Windows Server 2016
* Windows Server 2012 R2
* Windows Server 2012
* Windows Server 2008 R2
* Процессор: 2 GHz
* Оперативная память: 2 GB RAM назначенная виртуальной машине
* Жесткий диск: 8 GB выделенный для HDD
* Сетевой интерфейс: 2 назначенных виртуальных сетевых адаптера
	1. Системные требования для VPN:
* Операционные системы Windows:
* Windows 10 (all editions)
* Windows 8.1 (all editions except RT)
* Windows 8 (all editions except RT)
* Windows 7 (all editions)
* Windows XP (all editions)
* Windows Vista (all editions)
* Windows Server 2012 R2 (all editions except Core)
* Windows Server 2012 (all editions except Core)
* Windows Server 2008 R2 (all editions except Core)
* Windows Server 2008 (all editions except Core)
* Windows Server 2003 R2 (all editions)
* Windows Server 2003 (all editions)
* Операционные системы macOS:
* OS X 10.8 Mountain Lion
* OS X 10.9 Mavericks
* OS X 10.10 Yosemite
* OS X 10.11 El Capitan
* macOS 10.12 Sierra
* Операционные системы Linux:
* Debian 8
* Ubuntu 15.10 or 16.04
 |