|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Краевое государственное бюджетное учреждение здравоохранения | | |  | Руководителю | |  |  |  |  |
| Краевая клиническая больница | | |  |  |  |  |  |  |  |
| ул. П. Железняка, 3, г. Красноярск, 660022 | | |  |  |  |  |  |  |  |
| Телефон: 8 (391) 220-16-13 | | |  |  |  |  |  |  |  |
| Факс: 8 (391) 220-16-23 | | |  |  |  |  |  |  |  |
| Е-mail: kkb@ medqorod. ru | | |  |  |  |  |  |  |  |
| Http://www.medgorod.ru | | |  |  |  |  |  |  |  |
| ОКПО 01913234 | | |  |  |  |  |  |  |  |
| ИНН/КПП 2465030876/246501001 | | |  |  |  |  |  |  |  |
| 06.06. 2 022 г. №.931-2022 | | |  |  |  |  |  |  |  |
| На №\_\_\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| О коммерческом предложении | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| **Уважаемые господа!** | | | | | | |  |  |  |
| Прошу Вас предоставить коммерческое предложение на право поставки следующего товара или эквивалента: | | | | | | | | | |
| **№ п/п** | **Наименование** | **Характеристики** | **Ед. изм.** | **Кол-во, шт** | **Цена, рублей** | **Страна происхождения** | **Остаточный срок годности** | **ОКПД2\КТРУ** | **Код вида МИ** |
| 1 | Межсетевой экран с системой обнаружения вторжений | Согласно техническому заданию, приложение № 1 к запросу | усл. ед. | 1 |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| Срок поставки: в течение 5-14 календарных дней с момента подписания контракта/получения заявки на поставку.. | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |
| Цена должна быть указана с учетом доставки до КГБУЗ «Краевая клиническая больница» г.Красноярск, ул. Партизана Железняка, 3. | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |
| Информацию необходимо направить по факсу +7 (391) 220-16-23, электронной почте zakupki@medgorod.ru или по адресу г. Красноярск, ул. Партизана Железняка 3-К, отдел обеспечения государственных закупок, тел. 226-99-92, 226-99-91. | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |
| Предложения принимаются в срок до 15.06.2022 17:00:00 по местному времени. | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |
| Руководитель контрактной службы\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Алешечкина Е.А./ | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

Приложение № 1

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

оказание услуги на право использования программного комплекса «Межсетевой экран с системой обнаружения вторжений Ideco UTM» для обеспечения задачи безопасного межсетевого взаимодействия, учета и контроля использования ресурсов глобальной сети Интернет на условиях простой (неисключительной) лицензии для 2000 пользователей.

Программное обеспечение «Ideco UTM» включено в Единый реестр российских программ для

электронных вычислительных машин и баз данных (Запись в реестре №329 от 08.04.2016, ссылка:

https://reestr.digital.gov.ru/reestr/301678/ ) и может применяться как в государственных организациях, так и в коммерческих компаниях любой формы собственности.

Наименование, количественные, качественные и технические характеристики

закупаемой продукции

| **№**  **п/п** | **Наименование** | **Технические характеристики** | **Ед. изм.** | **Кол-во** |
| --- | --- | --- | --- | --- |
| 1. | Право использования программного комплекса «Межсетевой экран с системой обнаружения вторжений Ideco UTM» для обеспечения задачи безопасного межсетевого взаимодействия, учета и контроля использования ресурсов глобальной сети Интернет на условиях простой (неисключительной) лицензии для 2000 пользователей | Программный комплекс соответствует следующим требованиям по безопасности информации: «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» ИТ.СОВ.С4.ПЗ (ФСТЭК России, 2012), «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020).  Программный комплекс базируется на ядре Linux (версия ядра не ниже 5.11).  В системе должен присутствовать модуль постоянного слежения за системой, предотвращающий возможность нарушения работы служб при выходе параметров их работы за определенные установленные рамки.  При загрузке, системой проверяются все параметры оборудования, состояние файловой системы и баз данных, а также контрольная сумма всех неизменяемых файлов.  Используется система автоматического обновления, которая позволяет своевременно переходить на новые версии ПО. Все загружаемые файлы проверяются электронной цифровой подписью, для обеспечения гарантии целостности и подлинности загружаемых данных.  Для доступа в Интернет для каждого пользователя предусмотрена аутентификация по логину и паролю через VPN PPTP, IKEv2/IPSec, L2TP/IPSec, SSTP, идентификация по IP адресу, MAC адресу, аутентификация через WEB. При аутентификации через VPN обеспечена защита от прослушивания трафика и подстановки IP-адреса. Предусмотрена возможность синхронизации пользователей через ActiveDirectory и LDAP сервер с поддержкой кириллических символов в название подразделений и в именах пользователей, их прозрачная (SingleSign-On) аутентификация по протоколу Kerberos, NTLM и по логам безопасности контроллера домена. В том числе возможность интеграции с несколькими независимыми доменами ActiveDirectory.  Вся информация о пользователях хранится в базе данных sqlite. Пароли пользователей и административных учетных записей не хранится в открытом виде. Система должна хранить детализированную статистику каждого пользователя и каждой группы. В любой момент времени предусмотрена возможность посмотреть в форме отчета, какие ресурсы Интернет посещал пользователь или вся группа. Подсчет статистической информации ведется в реальном времени, с автоматическим предупреждением и отключением пользователя при превышении установленных лимитов. Статистика посещения ресурсов Интернет ведется в Мб.  В программной компоненте предусмотрена система автоматического резервного копирования базы данных, конфигурационных файлов и, опционально, каталогов, указанных пользователем на FTP-сервер или общие папки Windows.  Система включает в себя возможность создания отказоустойчивого кластера в режиме Active/Passive.  В систему встроена возможность управления с локальной консоли с полным доступом к файловой системе и системным командам (в том числе удаленный доступ из доверенного контура по протоколу SSH), через WEB интерфейс. Система поддерживает возможность использования нескольких учетных записей администратора для администрирования через WEB интерфейс.  Программный комплекс функционирует как маршрутизатор, поддерживающий неограниченное число интерфейсов (как локальных, так и внешних). Поддерживать виртуальные 802.1q VLAN интерфейсы, PPTP, PPPoE интерфейсы. Возможность указать маршруты по источнику, назначению.  Система обеспечивает поддержку нескольких каналов провайдеров и нескольких внешних сетей. Возможность полного разделения пользователей для выхода в Интернет через разных провайдеров. Автоматическую проверку связи с провайдером и переключение на альтернативного провайдера, в случае необходимости. Подключение к провайдеру по протоколам PPTP VPN, PPPoE и L2TP. Возможность балансировки трафика между каналами.  В системе предусмотрена возможность включения функции контент-фильтра, позволяющего управлять доступом к сайтам определенных категорий (не менее 144 категорий сайтов, и не менее 500 млн. url в базе данных) (значение параметра не требует конкретизации). Имеется возможность фильтрации скачиваемых файлов по расширению и MIME-типам. Также, в соответствии с категориями сайтов формируется веб-отчетность по трафику пользователей. Контент-фильтр фильтрует как HTTP, так и HTTPS-трафик, как с его расшифровкой, так и без расшифровки (с помощью анализа SNI и данных сертификата). База данных контент-фильтра обновляется автоматически не менее одного раза в 24 часа (значение параметра не требует конкретизации).  Программный комплекс обеспечивает защиту компьютеров от атак из Интернет с использованием технологии NAT и межсетевого экрана с контролем состояние соединений. Предусмотрена возможность блокирования ip-адресов и протоколов по заданным условиям. Защита от сканеров сети, защита от DoS-атак и блокирование чрезмерной активности. Фильтрация нежелательной почты (спама). Возможность ограничения трафика по типу, протоколам и портам. Защита от подстановки IP адреса, при авторизации через VPN и PPPoE каждому пользователю назначается личный IP-адрес. Ограничение скорости Интернет-трафика для отдельных пользователей, компьютеров или протоколов. DNAT portmapper. Возможность прозрачной переадресации адресов и портов на другой адрес.  Система обеспечивает возможность доступа сотрудников к внутренней локально-вычислительной сети посредством удаленного подключения по защищенному каналу через сеть Интернет. Реализована возможность объединить все удаленные подразделения в общую сеть на единой платформе по шифрованным протоколам VPN PPTP, L2TP/IPSec, IKEv2/IPSec, SSTP, с возможностью создать закрытые корпоративные серверы для ограниченного круга сотрудников.  Система обеспечивает возможность ограничения полосы пропускания до Интернет-ресурсов (шейпера трафика) для пользователей и групп.  Система обеспечивает возможность интеграции с SIEM-системами по протоколу syslog, системами мониторинга по SNMP, DLP-системами по протоколу ICAP.  Программный комплекс включает в свой состав следующие интегрированные Интернет службы:  - службу предотвращения вторжений, анализирующую трафик на всех интерфейсах сервера, блокирующую опасный трафик и атаки на сервер, сохраняющий информацию о блокированном трафике и предупреждения в логах на срок не менее трех месяцев (значение параметра не требует конкретизации)  - службу контроля приложений с возможностью ограничения трафика приложений: не менее чем 200 приложений с помощью DPI, включая торрент-клиенты, Skype, TeamViewer, TikTok, WhatsApp, DNSoverHTTPS, Mining (криптовалютыBitcoin, Monero, ZCash, Ethereum) (значение параметра не требует конкретизации).  - обратный прокси-сервер для публикации веб-ресурсов с возможностью публикации и защиты HTTP и HTTPS-сайтов  - сконфигурированный и настроенный почтовый сервер с фильтрацией спама. Почтовый ящик создается автоматически при добавлении пользователя. Осуществляется поддержка нескольких почтовых доменов, доверенных сетей и доменов. Предусмотрена поддержка протокола IMAP, защищенного протокола STARTTLS и общих почтовых папок. Предусмотрена блокировка попыток подбора паролей ко всем сервисам почты. Реализован полнофункциональный веб-интерфейс для работы с личной почтой, позволяющий работать с почтой из любой точки мира по шифрованному каналу через обычный браузер. Реализованы возможности, переадресации, групповой рассылки, фильтрации по адресам и содержимому, установка размера почтового ящика и размера письма, дублирования всей почты на один адрес, для контроля и архивирования корреспонденции, загрузки почту с других серверов по протоколам, настраиваемый автоответчик  - полнофункциональныйDNS-сервер с возможностью поддержки DNS-зон и кеширования DNS-запросов из локальной сети. С возможностью перехвата запросов на внешние DNS-сервера и принудительного разрешения доменных имен через встроенный сервер.  - DHCP-сервер для автоматического распределения IP адресов в локальной сети, обеспечивающий возможность: фиксированной привязки IP к MAC адресу компьютера. выдачи DNS и WINS для dhcp клиентов, выдачи маршрутов для DHCP клиентов, указания разных диапазонов на разных интерфейсах и VLAN.  **Подписка на 12 месяцев включает в себя:**  - Право на получение обновлений программы для ЭВМ (возможность получать новые версии продукта, обновление сигнатур)  - Право на получение технической поддержки программы для ЭВМ  - Право использования модуля предотвращения вторжений (возможность использовать модуль и получать его обновления)  - Право использования модуля по контролю приложений (возможность использовать модуль и получать его обновления)  - Право использования модуля по фильтрации контента (возможность использовать модуль и получать его обновления).  Право использования программы для ЭВМ осуществляется в следующих пределах и способами:  - воспроизведение программы для ЭВМ в соответствии с его назначением, ограниченное правом инсталляции, копирования, запуска и хранения в памяти ЭВМ  - осуществление настройки программы для ЭВМ в соответствии с его назначением, не представляющих собой изменение программы для ЭВМ  **В комплект поставки входят:**   * Оптический носитель информации (CD‑ROM) с размещёнными на нём программным обеспечением межсетевого экрана * Защитный пластиковый футляр для хранения оптического носителя информации * Вкладыш в защитный пластиковый футляр для хранения оптического носителя информации * Документированными материалами в составе: руководство администратора защиты, регламент обновления программного обеспечения МЭ * Формуляр в печатном виде * Копия сертификата соответствия. | Усл. ед. | 1 |

Сроки оказания услуг: 12 месяцев с момента заключения контракта