Приложение 1

к извещению об осуществлении закупки

**Описание объекта закупки**

**(техническое задание)**

**1.** **Предмет муниципального контракта**: оказание услуг по передаче неисключительных прав на использование программного обеспечения прокси-сервера.

**2.** **Требования к предоставляемым услугам:**

2.1. Место оказания услуг: по месту нахождения Исполнителя. Адрес для предоставления сертификата лицензии на право использования программного обеспечения: 628260, Ханты-Мансийский автономный округ-Югра, г.Югорск, ул. 40 лет Победы, 11, каб.203.

2.2. Целью оказания услуг является приобретение неисключительных прав на использование программного обеспечения прокси-сервера, предназначенного для обеспечения задачи безопасного межсетевого взаимодействия, учёта и контроля использования ресурсов глобальной сети Интернет для 250 пользователей со сроком подписки на 12 месяцев.

2.3. Лицензия на неисключительные права на использование программного обеспечения прокси-сервера действует бессрочно с даты покупки.

2.4. Исполнитель предоставляет Заказчику сертификат лицензии на право использования программного обеспечения прокси-сервера.

2.5. Приобретаемое программное обеспечение прокси-сервера должно быть включено в Единый реестр российских программ для электронных вычислительных машин и баз данных, иметь сертификат Федеральной службы по техническому и экспортному контролю (ФСТЭК).

**3. Перечень предоставляемых услуг (код ОКПД2 63.11.13.000):**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование услуг | Характеристика предоставляемых услуг | Кол-во |
| 1 | Оказание услуг по передаче неисключительных прав на использование программного обеспечения прокси-сервера | Право на использование программного обеспечения для организации защищённого доступа в сеть Интернет в корпоративной сети на 250 пользователей. | 1 штука |

**4. Требования к программному обеспечению (ПО):**

4.1. В программном обеспечении прокси-сервера должен присутствовать модуль постоянного слежения за системой, предотвращающий возможность нарушения работы служб при выходе параметров их работы за определённые установленные рамки.

При загрузке, системой должны быть проверены все параметры оборудования, состояние файловой системы и баз данных, а также контрольная сумма всех неизменяемых файлов.

Должна использоваться система автоматического обновления, которая позволяет своевременно переходить на новые версии ПО. Все загружаемые файлы должны проверяются электронной цифровой подписью, для обеспечения гарантии целостность и подлинность загружаемых данных.

4.2. Для доступа в сеть Интернет для каждого пользователя должна быть предусмотрена авторизация по логину и паролю через VPN PPTP, IKEv2/IPSec, L2TP/IPSec, SSTP, PPPoE, IP адресу, MAC адресу, через специально разработанную и включенную в комплект поставки программу доступа, через WEB. При авторизации через VPN и PPPoE должна быть обеспечена защита от прослушивания трафика и подстановки IP-адреса. Должна быть предусмотрена возможность синхронизации пользователей через Active Directory и LDAP сервер, их прозрачная (Single Sign-On) авторизация по протоколу Kerberos, NTLM и по логам безопасности контроллера домена. В том числе возможность интеграции с несколькими независимыми доменами Active Directory.

Вся информация о пользователях должна храниться в базе данных. Пароли пользователей и административных учётных записей не должны храниться в открытом виде. Система должна хранить детализированную статистику каждого пользователя и каждой группы. В любой момент времени должна быть предусмотрена возможность посмотреть в форме отчёта, какие ресурсы Интернет посещал пользователь или вся группа. Подсчёт статистической информации должен вестись в реальном времени, с автоматическим предупреждением и отключение пользователя при превышении установленных лимитов. Статистика посещения ресурсов Интернет должна вестись в мегабайтах.

4.3. В программной компоненте должна быть предусмотрена система автоматического резервного копирования базы данных, конфигурационных файлов и, опционально, каталогов, указанных пользователем на FTP-сервер или общие папки Windows.

В систему должна быть встроена возможность управления с локальной консоли с полным доступом к файловой системе и системным командам (в том числе удаленный доступ по протоколу SSH), возможность подключения и удалённого управления из Интернет по VPN (IKEv2/IPSec, L2TP/IPSec, SSTP, PPTP), по протоколу SSH (в т.ч. с правами суперпользователя root), через WEB интерфейс. Система должна поддерживать возможность использования нескольких учётных записей администратора для администрирования через WEB интерфейс.

4.4. Программный комплекс должен функционировать 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 (в том числе использовать пользователей или сети в качестве источника).

Система должна обеспечивать 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.

4.5. В системе должна быть предусмотрена возможность включения функции контент-фильтра, позволяющего управлять доступом к сайтам определённых категорий (не менее 144 категорий сайтов, и не менее 500 млн url в базе данных). Должна иметься возможность фильтрации скачиваемых файлов по расширению и MIME-типам. Также, в соответствии с категориями сайтов должна формироваться веб-отчётность по трафику пользователей. Контент-фильтр должен фильтровать 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 должна обновляться автоматически не реже одного раза в 24 часа.

Системой должна осуществляться антивирусная проверка веб-трафика (HTTP и HTTPS), а также проверка на вирусы почтовых сообщений. Антивирусные базы сигнатур должны обновляться автоматически, без участия администратора.

4.6. Программный комплекс должен обеспечивать защиту компьютеров от атак из Интернет с использованием технологии NAT и межсетевого экрана с контролем состояние соединений. Должна быть предусмотрена возможность блокирование 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.

4.7. Система должна обеспечивать возможность доступа сотрудников к внутренней локально-вычислительной сети посредством удалённого подключения по защищённому каналу через сеть Интернет. Должна быть реализована возможность объединить все удалённые подразделения в общую сеть на единой платформе по шифрованным протоколам VPN IKEv2/IPSec, PPTP, L2TP/IPSec, SSTP с возможностью создать закрытые корпоративные серверы для ограниченного круга сотрудников.

Система должна обеспечивать возможность ограничения полосы пропускания до Интернет-ресурсов (шейпера трафика) для пользователей и групп.

4.8. Система должна обеспечивать возможность интеграции с SIEM-системами по протоколу syslog, системами мониторинга по SNMP, DLP-системами по протоколу ICAP.

Программный комплекс должен включать 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 трёх месяцев;

- службу контроля приложений с возможностью ограничения трафика приложений (не менее чем 150 приложений с помощью DPI, включая торрент-клиенты, Skype, TeamViewer, TikTok, WhatsApp, DNSoverHTTPS, Mining (криптовалюты Bitcoin, Monero, ZCash, Ethereum));

- обратный прокси-сервер для публикации веб-ресурсов с возможностью публикации и защиты HTTP и HTTPS-сайтов;

- межсетевой экран уровня веб-приложений с возможностью блокировки SQLi, XSS и других атак на опубликованные веб-сайты;

- полнофункциональный DNS-сервер с возможностью поддержки forward 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.

- NTP-сервер точного времени, для синхронизации времени с серверов устройствами локальной сети.

- сконфигурированный и настроенный почтовый сервер с фильтрацией спама. Почтовый ящик должен создаваться автоматически при добавлении пользователя. Должна осуществляться поддержка нескольких почтовых доменов, доверенных сетей и доменов. Должна быть предусмотрена поддержка протокола IMAP, защищённого протокола STARTTLS и общих почтовых папок. Должна быть предусмотрена блокировка попыток подбора паролей ко всем сервисам почты. Должен быть реализован полнофункциональный веб-интерфейс для работы с личной почтой, позволяющий работать с почтой из любой точки мира по шифрованному каналу через обычный браузер. Должны быть 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;

4.9. Подписка на 12 месяцев также должна включать в себя:

- право на получение обновлений ПО (возможность получать новые версии продукта, обновление сигнатур);

- право на получение технической поддержки ПО;

- 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).

4.10. Право использования ПО осуществляется в следующих пределах и способами:

- воспроизведение ПО в соответствии с его назначением, ограниченное правом инсталляции, копирования, запуска и хранения в памяти сервера;

- осуществление настройки программного обеспечения в соответствии с его назначением, не представляющих собой изменение программного обеспечения;

- запрещено предоставлять право использования программного обеспечения третьим лицам, в частности, путём предоставления доступа и/или передачи электронного ключа;

- осуществление использования программного обеспечения на территории России и стран СНГ.

Согласовано:

Начальник отдела

информационных технологий: П.Н. Ефремов

Контрактная служба: О.В. Дергилев