Құжат «Самұрық-Қазына» ӘАҚ» АҚ электронды порталымен құрылған
Документ сформирован порталом электронных закупок АО «ФНБ «Самрук-Казына»

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 496825
способом Открытый тендер на понижение

Лот № (2936-10 Т, 1759310)

Заказчик: Товарищество с ограниченной ответственностью "Экибастузская ГРЭС-1 имени Булата Нуржанова"
Организатор: Товарищество с ограниченной ответственностью "Экибастузская ГРЭС-1 имени Булата Нуржанова"

1. Краткое описание ТРУ

Наименование	Значение
Номер строки	2936-10 Т
Наименование и краткая характеристика	Программное обеспечение, оригинал программного обеспечения (кроме услуг по разработке программных обеспечении по заказу)
Дополнительная характеристика	Описание: "Программное обеспечение; Сетевой шлюз, обеспечивающий защиту сетевого периметра. IDECO UTM; Программное обеспечение; Сетевой шлюз, обеспечивающий защиту сетевого периметра. IDECO UTM"
Количество	1.000
Единица измерения	Штука
Место поставки	КАЗАХСТАН, Павлодарская область, Экибастуз Г.А., г.Экибастуз, Павлодарская область, г. Экибастуз, Промышленная зона ГРЭС1, строение 2
Условия поставки	DDP
Срок поставки	С даты подписания договора по 12.2020
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 100%, Окончательный платеж - 0%

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

Характеристики товара:
Предназначен для доукомплектования и применения программного шлюза безопасности Ideco UTM, предназначенного для обеспечения задачи безопасного межсетевого взаимодействия, учета и контроля использования ресурсов глобальной сети Интернет для 500 пользователей.
Программный комплекс должен базироваться на ядре Linux.
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 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.
Для доступа в 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 sqlite. Пароли пользователей и административных учетных 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 отчета, какие ресурсы Интернет посещал пользователь или вся группа. Подсчет статистической информации должен вестись в реальном времени, с автоматическим предупреждением и отключение пользователя при превышении установленных лимитов. Статистика посещения ресурсов Интернет должна вестись в Мб.
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 удаленного 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 учетных записей администратора для администрирования через WEB интерфейс.

Осы құжат «Электрондық құжат және электрондық цифрлық қолтаңба туралы» Қазақстан Республикасының 2003 жылғы 7 қаңтардағы N 370-II Заңы 7 бабының 1 тармағына сәйкес қағаз тасығыштағы құжатпен бірдей

Данный документ согласно пункту 1 статьи 7 ЗРК от 7 января 2003 года N370-II «Об электронном документе и электронной цифровой подписи» равнозначен документу на бумажном носителе

Программный комплекс должен функционировать как маршрутизатор, поддерживающий неограниченное число интерфейсов (как локальных, так и внешних). Поддерживать виртуальные 802.1q VLAN интерфейсы, PPTP, PPPoE и OpenVPN интерфейсы. Возможность указать маршруты по источнику.
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.
В системе должна быть 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). Должна иметься возможность фильтрации скачиваемых файлов по расширению и MIME-типам. Также, в соответствии с категориями сайтов должна формироваться веб-отчетность 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.
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.
Система должна обеспечивать возможность доступа сотрудников к внутренней локально-вычислительной сети посредством удаленного подключения по защищенному каналу через сеть Интернет. Должна быть реализована возможность объединить все удаленные подразделения в общую сеть на единой платформе по шифрованным протоколам VPN IKEv2/IPSec, PPTP, L2TP/IPSec, SSTP и OpenVPN 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.
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 трех месяцев;
- службу контроля приложений с возможностью ограничения трафика приложений (не менее чем 100 приложений с помощью DPI, включая торрент-клиенты, Skype, TeamViewer, TikTok, WhatsApp, DNSoverHTTPS, Mining (криптовалюты Bitcoin, Monero, ZCash, Ethereum));
- обратный прокси-сервер для 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;
- 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, защищенного 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;
- полнофункциональный DNS-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.
Цена поставки товара должна быть указана с учетом затрат на осуществление технической поддержки в течение одного года после передачи прав пользования заказчику, уплату налогов и других видов сборов.

3. Присутствует указание характеристик, определяющих принадлежность приобретаемого ТРУ отдельному потенциальному поставщику либо производителю

осуществляются закупки ТРУ для доукомплектования, модернизации, дооснащения, а также для дальнейшего технического сопровождения, сервисного обслуживания и ремонта

Подписал	ТУРЛУБЕКОВА АЛУА БЕКТАСОВНА
Дата подписания	28.10.2020

Осы құжат «Электрондық құжат және электрондық цифрлық қолтаңба туралы» Қазақстан Республикасының 2003 жылғы 7 қаңтардағы N 370-II Заңы 7 бабының 1 тармағына сәйкес қағаз тасығыштағы құжатпен бірдей

Данный документ согласно пункту 1 статьи 7 ЗРК от 7 января 2003 года N370-II «Об электронном документе и электронной цифровой подписи» равнозначен документу на бумажном носителе