ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 533295
способом Запрос ценовых предложений на понижение

Лот № (437-1 У, 1883096) Услуги по обеспечению информационной безопасности

Заказчик: Акционерное общество "Алматинские электрические станции"
Организатор: Акционерное общество "Алматинские электрические станции"

1. Краткое описание ТРУ

Наименование	Значение
Номер строки	437-1 У
Наименование и краткая характеристика	Услуги по обеспечению информационной безопасности, Услуги по обеспечению информационной безопасности
Дополнительная характеристика	Техническая поддержка и продление подписки системы сетевой безопасности SOPHOS XG Firewall
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, г.Алматы, Медеуский район, Головной офис, пр. Достык, 7
Условия поставки	-
Срок поставки	С даты подписания договора по 12.2021
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

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

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ
на закуп услуги "Услуги по обеспечению информационной безопасности (Техническая поддержка системы информационной безопасности) для АО «АлЭС»

1. Основание для выполнения услуги: Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности
2. Обеспечение финансированием: Статья затрат Услуги вневедомственной охраны
3. Цель выполнения услуги: Обеспечение информационной безопасности локальной вычислительной сети АО «АлЭС» (продление подписки системы сетевой безопасности SOPHOS XG Firewall - SF SW/Virtual FullGuard Plus with Enhanced Support - UP TO 8 CORES & 16GB RAM - 12 MOS - RENEWAL).
4. Краткая характеристика услуги:
Услуга предоставляется при продлении подписки системы сетевой безопасности Firewall - SF SW/Virtual FullGuard Plus with Enhanced Support - UP TO 8 CORES & 16GB RAM - 12 MOS - RENEWAL с полным сопровождением и настройкой данной системы. Исполнитель обязан осуществлять услугу до полного завершения настройки которые требует Заказчик.
Услуга будет предоставляется в Головном офисе АО «АлЭС» который находится по адресу г. Алматы, пр. Достык 7, также данная услуга может предоставляться на производственных департаментах АО «АлЭС» при необходимости.
Система сетевой безопасности Sophos XG Firewall базируется на решениях сетевого шлюза следующего поколения. Система обеспечивает контроль приложений и защиту от угроз, в том числе: визуализация приложений, глобальный сбор информации об угрозах на основе репутации, автоматически сообщает об угрозах, проверяет зашифрованный трафик, предотвращает вторжения, производит антивирусную защиту и фильтрацию содержимого. Sophos XG Firewall имеет возможность подключения к глобальной службе сбора сведений об угрозах информационной безопасности. Подсистема работает круглосуточно в режиме реального времени, для защиты от кибер угроз по всем направлениям, включая файлы, Интернет, сообщения и сеть. Sophos XG Firewall использует службу репутаций сетевых соединений для выявления доменов, IP-адресов и портов, которые совершают атаки и вследствие чего блокируются. Sophos XG Firewall использует службу веб-репутаций для выявления зараженных или использующихся злоумышленниками URL-адресов, сайты с нежелательным содержимым. Система сетевой безопасности Sophos XG Firewall имеет возможность расширения и полную совместимость для интеграции в режим работы “синхронизированной безопасности” (Synchronised Security).
Система сетевой безопасности Sophos XG Firewall реализована на виртуальной платформе (Поддержка систем виртуализации (VMware, Hyper-V, KVM, Citrix XenApp, Microsoft Azure)).
Виртуальная платформа обладает следующим техническим параметрам:
1. Поддержка 8 ядер vCPU Xeon и 16 ГБ оперативной памяти;
2. Пропускная Способность Межсетевого Экрана: 37 Гбит пакетами 1500 байт
3. Пропускная способность IPS: 893 Мбит (Imix traffic)

4. Пропускная способность VPN: 1200 Мбит (Imix traffic)
5. Пропускная способность антивируса (прокси): 1440 Мбит (Imix traffic)
6. Одновременных соединений: 20 000 000
7. Новых соединений/сек: 200 000
Максимальное количество лицензированных пользователей: без ограничений
Наименования и описание продляемых подсистем в рамках подписки SF SW/Virtual FullGuard Plus with Enhanced Support - UP TO 8 CORES & 16GB RAM - 12 MOS - RENEWAL:
1. Наименование подсистемы: Base Firewall (Межсетевой экран)
Описание подсистемы:
Система базовой защиты обеспечивает базовый функционал маршрутизации трафика в реальном времени, как входящего, так и исходящего. Построение VPN туннелей. Аутентификацию пользователей. Управление беспроводными сетями.
Система базовой защиты должна включать в себя следующий функционал:
Обеспечивать маршрутизацию пакетов, в том числе:
- Статическая маршрутизация, Multicast routing, Policy routing
- Динамическая маршрутизация (OSPF, BGP, RIP, PIM-SM)
Базовый функционал шейпинга пакетов (QoS) и квотирование трафика.
Функционал управления точками доступа, настройки защищенных беспроводных сетей, подключения и управления точками доступа, создание пользовательского портала для аутентификации пользователей в беспроводной сети.
Функционал аутентификации пользователей, используя как свою локальную базу пользователей, так и следующие сервера аутентификации: LDAP Server, Active Directory, RADIUS Server, TACACS+ Server, eDirectory также, должна включать в себя пользовательский портал с возможностью создания одноразового пароля для гостевого доступа и систему и функционал Clientless users для жесткой привязки имени пользователя к определенному IP адресу
Функционал создания VPN туннелей, включающий в себя:
- Возможность создания Site-to-site IPSec туннеля
- Возможность создания Site-to-Site SSL VPN туннеля
- Пользовательский SSL VPN
- Пользовательский L2TP VPN
- Пользовательский PPTP
- HTML5 VPN
Состав подсистемы:
Управление
● Специально разработанный, оптимизированный пользовательский интерфейс
● Простая навигация - любая функция в 3-х кликах
● Пользовательский интерфейс поддерживается в любом современном браузере и не требует Java
Само документированная система со ссылками на конкретные пункты документации
● Расширенный набор графических инструментов поиска неисправностей (например Packet Capture)
● Интерфейс командной строки (CLI) доступный из графического интерфейса
● Интерфейс командной строки (CLI) доступный по SSH v2 протоколу с аутентификацией по сертификатам
● Ролевое администрирование
● Автоматическое уведомление об обновлениях прошивки с легким автоматизированным процессом обновления и функцией отката
● Повторное использование системных объектов для сетей, сервисов, хостов, периодов времени, пользователей и их групп, клиентов и серверов
● Пользовательский портал
● Отслеживание изменений в конфигурации
● Гибкий контроль доступа с помощью разделения на зоны
● Опции оповещения по электронной почте или по протоколу SNMP
● Поддержка протоколов SNMP и Netflow
● Резервное копирование и восстановление конфигураций: локальное, по FTP или электронной почте; по запросу, ежедневное, еженедельное или ежемесячное
● Кластеризация с синхронизацией между нодами всей информации (конфигурация, журналы, состояния TCP стека, IPSec и тд)
● Кластеризация работает на L2 уровне - ноды кластера имеют единые IP адреса и общий виртуальный MAC адрес
● API для интеграции сторонних устройств
● Встроенные в Интерфейс ссылки на практические руководства в формате видео
● Опция предоставления удаленного доступа для технической поддержки
● Многоязычный интерфейс с поддержкой русского языка
Межсетевой экран, Сеть и Маршрутизация
● Унифицированная модель политик для управления ими из единого экрана
● Инструменты тестирования политик, установленных для правил межсетевого экрана и веб-фильтрации, с помощью симуляции
● Глубокий анализ пакетов межсетевым экраном с сохранением состояния сессий
● FastPath оптимизация передачи пакетов
● Возможность создания сетевых политик основанных на пользователе, группе, виде трафика
● Политики доступа по времени для каждого пользователя/группы
● Применение политик между Зонами, Сетями и Сервисами

● Поддержка политик фильтрации по зонам и изоляции зон
● Предустановленные параметры для зон LAN, WAN, DMZ, LOCAL, VPN и WiFi
● Пользовательские зоны для LAN или DMZ
● Группировка политик, ручная и автоматическая
● Настраиваемые политики NAT с IP маскарадингом
● Защита от Flood атак: Защита от DoS атак, а также блокирование сканирования портов
● Блокирование пользователей по странам с использованием гео-IP
● Маршрутизация: Статическая, Динамическая (BGP, OSPF) и Multicast (PIM-SM)
● Поддержка вышестоящего прокси
● IGMP Snooping маршрутизация широковещательного трафика
● Сетевой мост с поддержкой STP и ARP переадресации
● Балансировка WAN-соединения: несколько подключений к Интернету, автоматическая проверка доступности, автоматическое переключение, автоматическая и взвешенная балансировка
● Наличие аппаратных моделец со встроенным WiFi
● Агрегирование каналов 802.3ad
● Настройка DNS и DHCP
● Динамический DNS
● IGMP Snooping маршрутизация широковещательного трафика
● Сетевой мост с поддержкой STP и ARP переадресации
● Поддержка IPv6 туннелирования с поддержки, включая 6in4, туннель 6to4, 4in6 и быстрого развертывания IPv6 (6rd) через IPSec
● Поддержка подстановочных знаков для имени хоста или объектов домена
● Поддержка VLAN DHCP и тегов
● Поддержка нескольких мостов
Шейпинг трафика и квоты
● Шейпинг трафика, применяемый к конкретному сетевому трафику или к пользователю (QoS)
● Квота загрузки/выгрузки по трафику для пользователя
● Оптимизация в режиме реального времени протокола VoIP
Защита и управление беспроводной WiFi сети
● Простое и быстрое развертывание беспроводного интернет-соединения. Точки доступа автоматически появляются в центре управления межсетевого экрана.
● Центральный монитор и управлять всеми точками доступа и беспроводными клиентами через встроенный контроллер
● Возможность организовать мост между точкой доступа и LAN, VLAN, или настроить отдельную зону с параметром изоляции клиентов
● Поддержка нескольких SSID на точку доступа, в том числе и скрытые SSID
● Поддержка систем безопасности и шифрования, включая WPA2 Personal и WPA2-Enterprise
● Поддержка проверки подлинности IEEE 802.1 x (RADIUS)
● Поддержка стандарту 802.11r (роуминг)
● Поддержка hotspot портала для аутентификации пользователей используя ваучеры, пароль дня, или условия использования
● Гостевой беспроводной доступ в Интернет с простым полным разделением от корпоративного трафика
● Доступ к беспроводной сети с ограничениями по времени
● Наличие точек доступа с поддержкой MESH режима: работа беспроводным ретранслятором и мостом
● Автоматический выбор беспроводного канала
● Поддержка https для портала
● Аутентификация пользователей
● Прозрачная аутентификация пользователя (NTLM/ Kerberos)
● Проверка пользователя через: AD, eDirectory, RADIUS, LDAP и Tacacs+
● Агенты передачи данных об авторизации пользователя в AD на межсетевой экран
● Агенты авторизации пользователя для Windows и Mac OS x, Linux 32/64
● Сертификаты аутентификации для iOS и Android
● Единый вход: AD, eDirectory
● Службы авторизации для IPSec и L2TP, и PPTP и SSL
Пользовательский портал
● Возможность загрузки клиента авторизации пользователя
● Возможность скачать клиент удаленного доступа SSL (Windows) или файлы конфигурации (прочие ОС)
● Информация Hotspot портала
● Изменение имени пользователя и пароля
● Просмотр статистики доступа в интернет
● Доступ к карантину сообщений электронной почты
Базовый VPN
● Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key
● L2TP и PPTP
● Удаленный доступ: SSL, IPsec, поддержка VPN клиентов для iPhone/iPad/ Cisco/Andriod
● Поддержка IKEv2
● SSL-клиент для ОС Windows, отдельно не лицензируемый

IPSec клиент
● Проверка подлинности: Pre-Shared Key (PSK), PKI (X.509), Smartcards, Token и XAUTH
● Шифрование: AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (up to 2048 Bit), DH groups 1/2/5/14, MD5 and SHA-256/384/512
● Интеллектуальное сплит-туннелирование для оптимальной маршрутизации трафика
● Поддержка NAT-traversal
● Мониторинг состояния подключения
2. Наименование подсистемы: Network Protection (Защита сети)
Состав подсистемы:
Система предотвращения вторжений (IPS)
● Встроенный высокопроизводительный IPS движок с глубокой инспекцией пакетов для обеспечения максимальной производительности и защиты
● Добавление собственных IPS правил
Защита от внутренних бот-сетей и обмен телеметрией с конечной точкой
● Защита от расширенных угроз (обнаружение и блокирование попыток связаться с командно-контрольными серверами (C&C), используя многоуровневую проверку: DNS, Proxy и Firewall)
● Мониторинг статуса конечной точки, с возможностью автоматически реагировать на инциденты безопасности, изолируя зараженные системы.
● Формирование ТОП-рейтинга пользователей в группе риска, неизвестных приложений, сложных угроз и аномалий поведения трафика
● Автоматическая идентификация, классификация и контроль всех неизвестных приложений в сети
● Запрашивать информацию о приложениях от конечной точки для идентификации сигнатуры
● Глубокий анализ трафика пользователей, угроз, приложений, использования интернета, и прочей активности в сети.
● Возможность ограничения доступа к сетевым ресурсам или полностью изолировать зараженную систему, пока она не будет очищена
● Обмен телеметрией и состоянием между конечной точкой и межсетевым экраном, для координации ответных мер.
Поддержка работы с Удаленными Ethernet-устройствами с L2VPN для филиалов
● Централизованное управление всеми устройствами
● Без предварительной настройки: автоматическое подключение через облачный сервис при первом запуске
● Безопасный зашифрованный туннель с использованием цифровых сертификатов X.509 и шифрования AES256
● Построение L2VPN между площадками для объединения LAN сегментов в единую L2 сеть
● Управление IP-адресами с центральной системы через настройки DHCP и DNS на ней
● Автоматическая де-авторизация устройств при отсутствии активности
● Сжатие трафика в туннеле
● Наличие вариантов устройств с поддержкой VLAN на портах
Без Клиентский VPN
● Поддержка HTML5 VPN (доступ к SSH, Telnet, RDP, VNC,.. из браузера)
3. Наименование подсистемы: Web Protection (Защита пользователей)
Состав подсистемы:
Веб-фильтрация (прокси)
● Прозрачный прокси для защиты от вредоносных программ и веб-фильтрации
● Защита от продвинутых атак - ATP (например блокирование общения вредоносов с C&C серверами по HTTP(S) протоколу)
● База данных URL с миллионами сайтов
● Возможность установить квоты по времени на каждого пользователя/группу
● Возможность установить политику доступа по времени для каждого пользователя/группы
● Сканирование на вредоносные программы: возможность блокировать все формы вирусов, web malware, трояны и шпионские программы на http/s, FTP и веб-почте
● Улучшенная защита от web malware с использованием JavaScript эмуляции
● Онлайн-защита в режиме реального времени для поиска новейших угроз
● Второй независимый антивирусный движок для двойного сканирования
● Поведенческий анализ потенциально опасных файлов в облачной песочнице
● Режимы сканирования в реальном времени или пакетный режим
● Anti-pharmin защита (защита от подмены IP адреса в DNS записях хостов)
● Сканирование HTTP и HTTPS по пользователям или на основе сетевых политик с настраиваемыми правилами и исключениями
● Сканирование HTTPS с подменой сертификата. Возможность выгрузить свой промежуточный сертификат, выпущенный доверенным центром сертификации
● Сканирование HTTPS без подмены сертификата (без расшифровки) с использованием SNI в сертификате
● Определение протокола SSL туннелирования и принудительное использование шифрования
● Отслеживание конкретных слов на веб странице (фильтрация по контенту / словам)
● Проверка сертификата сайта
● Блокировка Google QUIC протокола
● Поддержка перенаправления HTTP2 на HTTP
● Быстрое кэширование веб-контента
● Кеширование обновлений ПО, в частности антивирусного

● Фильтрация по типу файла: по MIME-типу, расширению и активному контенту (например, Activex, applets, cookies и т. д.)
● Форсирование использования YouTube для школ с безопасным контентом
● Принудительное включение SafeSearch
Защита и управление приложениями
● Контроль приложений по сигнатурам и на уровне Layer 7 шаблонов (DPI)
● Наличие сигнатур более чем для 3000 приложений
● Контроль приложений на основе: категории, характеристик (например, пропускной способности и потребления производительности), технологии (например, P2P) и уровеню риска
● Наличие репутации у приложений для выявления ПО, которое имеет наибольший коэффициент риска. Наличие индикатора с суммирующим риском по всей сети
● Идентификации, классификации и контроль ранее неизвестных приложений на сети
● Политики контроля приложений по пользователям или сетевых политик
● Выявление и отдельных отчёт в реальном времени обо всех облачных приложениях
● Фильтрация по приложения, ранее неизвестных МЭ. Получение информации от агентов на рабочих местах.
Шейпинг трафика L7 приложений и веб-приложений
● Шейпинг пользовательского трафика (QoS) для URL категорий или L7 приложений
4. Наименование подсистемы: Email Protection (Защита электронной почты)
Состав подсистемы:
Защита и контроль электронной почты
● Сканирование электронной почты с поддержкой SMTP, POP3 и IMAP
● Защиты от спама, основанная на запатентованной технологии Recurrent-Pattern-Detection
● Возможность блокировки спама и вредоносных программ по протоколу SMTP
● Второй антивирусный движок для обнаружения вредоносных программ, для двойного сканирования
● Поведенческий анализ потенциально опасных файлов в облачной песочнице
● Защита в режиме реального времени для поиска новейших угроз
● Автоматическая подпись и обновление вирусных баз
● File-Type обнаружения/блокирования/сканирование вложений
● Принять, отклонить или отбросить сообщения большого размера
● Возможность обнаружения фишинговых веб-адресов в электронной почте
● Использовать предварительно определенные правила сканирования контента или возможность создавать свои собственные правила, основанные на различных критериях
● Поддержка TLS шифрования для SMTP, POP3 и IMAP
● Проверка получателя
● Автоматически добавлять подпись ко всем исходящим сообщениям
● Greylisting
● Рилей исходящей почты
Управление Карантином
● Уведомления о письмах в карантине
● Письма с вирусами и спам-карантин с поиском и фильтрацией по дате, отправителю, получателю, теме, и причине, с возможностью высвободить или удалить сообщение
● Пользовательский портал для просмотра и высвобождения писем из карантина
Шифрование и DLP
● Шифрование исходящих писем в шифрованный PDF контейнер
● Получатель PDF контейнера может сам назначать пароль
● Добавление вложений при ответах на полученный PDF контейнер
● Абсолютная прозрачность без дополнительного ПО или клиента
● DLP с автоматическим сканированием электронных сообщений и вложений для определения конфиденциальных данных
● Подготовленные списки конфиденциальных данных, сопровождаемые вендором, для соответствия стандартам PII, PCI, HIPAA
5. Наименование подсистемы: Web Application Firewall
Состав подсистемы:
● Обратный прокси-сервер, URL hardening engine с deep-linking и directory traversal prevention, Form hardening engine, Защита от SQL-инъекций, Защита от Cross-site scripting, Два антивирусных двигателя, HTTPS (SSL) encryption offloading, Cookie signing с digital signatures, Path-based routing, Поддержка Outlook anywhere, Reverse authentication (offloading) для form-based и basic authentication для доступа к серверу
● Абстракция виртуального сервера и физического сервера
● Интегрированная подсистема балансировки нагрузки для нескольких серверов
● Гранулированные исключения отдельных проверок
● Сопоставление запросов от конкретной сети отправителя или заданного целевого URL-адреса
● Поддержка логических операторов и/или
● Совместимость с различными конфигурациями и нестандартными внедрениями
● Возможность настраивать производительность WAF
● Предельный размер сканирования
● Разрешить/блокировать диапазоны IP-адресов
Поддержка Wildcard сертификатов

● Автоматически добавлять префикс/суффикс для аутентификации
6. Наименование подсистемы: Logging and Reporting (Ведение журналов и составление отчетов)
Состав подсистемы:
● Встроенные отчёты с настраиваемыми опциями (включающие: отдельные логи, наличие отчётов и виджетов в зависимости от активированного функционала):
● Основной экран (отчёты по трафику, состоянию безопасности и риск-анализ пользователей),
● Отчеты по приложениям (риск-анализ приложений, заблокированные приложения, веб-трафик, поисковые запросы, веб-серверы, FTP),
● Отчеты о сети и об угрозах (IPS, ATP, WiFi, Телеметрии с конечными точками),
● Отчеты по VPN
● Отчеты о защите и использовании электронной почты
● Отчёты соответствия индустриальным стандартам (HIPAA, GLBA, SOX, FISMA, PCI-DSS, NERC CIP v3, и CIPA)
● Текущий мониторинг активности: состояние системы, активные пользователи, IPsec соединения, удаленные пользователи, текущие соединения, беспроводные клиенты, карантин и DoS-атаки
● Анонимизация отчетов
● Планировщик отправки отчетов нескольким получателям, варианты отчетов с гибкой периодичностью
● Стандартный и гранулированные варианты логов
● Экспорт отчетов в HTML, PDF, в Excel (в формате xls)
● Отчет по аудиту безопасности
● Отчет по контент-фильтрации по ключевым словам
● Закладки отчётов для быстрого доступа
● Просмотр журналов с настройкой по категориям
7. Требования к гарантийному обслуживанию:
24x7 Расширенная техническая поддержка по телефону и электронной почте с удаленной консультацией (до 4 часов)
Открытая документация
Открытая база знаний
Бесплатные обновления и патчи безопасности
Бесплатные обновления программного обеспечения
5. Количественные данные: Количество лицензии пользователей: без ограничений
6. Сроки исполнения услуги: с МПД по 31.12.2021 года.

3. Нормативно-технические документы

№ п/п	Наименование
1	Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности

Подписал Алпысбаев Дархан Сейдуллаевич
Дата подписания 25.01.2021