**«Утверждаю»**

заместитель Генерального директора

ТОО «Energy Solutions Center»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Нурпеисов Т.Т.

от «\_\_\_» \_\_\_\_\_\_\_\_\_ 201\_\_г.

**Техническая спецификация**

**на услуги по аренде серверного оборудования**

**для системы ИТ-мониторинга**

1. **Наименование ТРУ: Услуги по аренде серверного оборудования.**
2. **Код ЕНСТРУ:** [**773312.000.000000**](https://enstru.kz/code_new.jsp?&t=%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80&s=common&p=10&n=0&S=773312%2E000&N=%D0%A3%D1%81%D0%BB%D1%83%D0%B3%D0%B8%20%D0%BF%D0%BE%20%D0%B0%D1%80%D0%B5%D0%BD%D0%B4%D0%B5%20%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%BE%D0%B1%D0%BE%D1%80%D1%83%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F&fc=1&fg=0&new=773312.000.000000)**.**
3. **Характеристика услуг:**
   1. В рамках оказания услуг Исполнитель предоставляет Заказчику серверное оборудование, согласно требованием, которое будет размещено на территории Заказчика.
   2. Исполнитель на арендуемом серверном оборудовании должен развернуть систему ИТ-мониторинга и систему безопасности.
4. **Требования к серверному оборудованию Системы:**
   1. Серверное оборудование должно быть сертифицированное и разрешенное к использованию на территории РК оборудование, а также иметь сервисный центр производителя на территории РК.
   2. Детальное требование представлено ниже:

* Количество занимаемых юнитов – не более 4;
* Количество слотов процессоров – не менее 4х;
* Поддержка инструкции AMD64;
* Частота процессора не менее 3400Mhz;
* Количество ядер в процессоре не менее 6/12 (физических, логических);
* Внутренний кэш 1 уровня не менее 64Кбайт;
* Внутренний кэш 2 уровня не менее 256 Кбайт;
* Внутренний кэш 3 уровня не менее 38400 Кбайт;
* Количество слотов памяти не менее 96;
* Тип оперативной памяти – DIMM DDR3 RDIMM или более новее;
* Объем ОЗУ – не менее 512Гбайт;
* Максимальный объем ОЗУ – не менее 3 Тбайт;
* Количество сетевых адаптеров – не менее 4;
* Поддерживаемая скорость сетевого адаптера – не менее 10Гбит/с;
* Количество адаптеров FiberChannel – не менее 4;
* Поддерживаемая скорость FiberChannel – не менее 16Гбит/с;
* Наличие контроллера RAID с поддержкой RAID0/1/10/5/6/50/60 типов массива;
* Тип жестких дисков – SAS;
* Максимальное количество мест для жестких дисков – не менее 8;
* Количество жестких дисков – не менее 2х;
* Объем жесткого диска – не менее 300Гбайт;
* Количество блоков питания – не менее 4;
* Мощность блока питания – не менее 1200Ватт;

1. **Требования к функциональным характеристикам Системы Мониторинга**
   1. Система должна обеспечивать следующие функциональные возможности:

* Мониторинг работоспособности серверов с установленным системным программным обеспечением Windows Server 2003/2008(R2)/2012(R2)/2016;
* Мониторинг работоспособности серверов с установленным системным программным обеспечением на базе ядра Linux;
* Мониторинг работоспособности оборудования через протокол SNMP v1/v2/v3;
* Мониторинг работоспособности оборудования через протокол IPMI;
* Мониторинг работоспособности сервера внутренней корпоративной электронной почты Microsoft Exchange Server 2010 и (или) новее;
* Мониторинг работоспособности управления базами данных под управлением Microsoft SQL Server 2008R2/2012;
* Мониторинг работоспособности серверов виртуализации под управлением гипервизора Microsoft Hyper-V;
* Мониторинг работоспособности файловых сервисов;
* Интеграция системы мониторинга с внутренней корпоративной электронной почтой; создание и настройка канала уведомлений по электронной почте;
* Распределённый мониторинг;
* Сценарии на основе мониторинга;
* Автоматическое обнаружение;
* Централизованный мониторинг журналов;
* Веб-интерфейс для администрирования и настройки;
* Отчётность и тенденции;
* SLA-мониторинг;
* Поддержка высокопроизводительных агентов для всех платформ (Windows, Linux);
* Комплексная реакция на события;
* Поддержка SNMP-ловушек;
* Поддержка мониторинга JMX-приложений;
* Поддержка выполнения запросов в различные базы данных;
* Расширение за счёт выполнения внешних скриптов;
* Гибкая система шаблонов и групп;
* Возможность создавать карты сетей.

1. **Требования к функциональным характеристикам Системы безопасности**
   1. Система безопасности должна использовать контроль состояния соединений на основе детализированного анализа связи и состояния приложения для отслеживания и управления сетевым потоком.
   2. Система должна включать в себя возможность работы в режиме Transparent/Bridge.
   3. Система должна поддерживать работу на 2 уровне модели OSI (режим bridge).
   4. Система должна поддерживать следующий функционал:

* Firewall
* DHCP сервер и DHCP relay
* HTTP & HTTPS proxy
* IPS, URL-фильтрацию, контроль приложений, анти-бот, антивирус, инспекцию HTTPS
* Интеграция с Active Directory
* Возможность настройки контроля приложений и контроля доступа к сетевым ресурсам для пользователей, групп пользователей или компьютеров
* Возможность интеграции с аппаратной «песочницей».
  1. Функционал потокового антивируса с блокировкой вредоносных файлов по хешам без ограничения на количество сигнатур.
  2. Система должна иметь возможность активации функционала DLP (при наличии дополнительной лицензии). Функционал DLP должен обеспечивать контроль за утечкой конфиденциальной информации по протоколам SMTP, FTP, HTTP и веб-почте, должна поддерживаться возможность расшифровки SSL-трафика. Должна поддерживаться возможность определения конфиденциальных документов по преднастроенным шаблонам или пометке документов водяными знаками. Система должна анализировать контент более чем 800 типов файлов.
  3. IPS должна поддерживать следующие механизмы детектирования угроз: использование сигнатур, отслеживание аномалий протоколов, управление приложениями и обнаружение угроз на основе поведения.
  4. Система должна поддерживать кластеризацию Active/Standby в режиме bridge.
  5. Система должна поддерживать высокую доступность шлюза и распределение нагрузки с синхронизацией состояний сетевых соединений (Cluster HA Active\Active). В режиме высокой доступности или режиме распределения нагрузки должна поддерживаться не менее 5 узлов кластера.
  6. Система должна обеспечивать поддержку IPv6.
  7. Система должна поддерживать политику, основанную на QoS.
  8. Система должна позволять гарантировать или ограничивать пропускную способность и управлять задержкой для определенного IP источника, IP пункта назначения или сервиса.
  9. Система должна иметь возможность произвольного применения правил QoS для VPN трафика.
  10. Система должна включать в себя поддержку для VPN типа site-to-site в следующих топологиях:
* Полносвязная сеть (все-со-всеми);
* Звездообразная сеть (удаленные офисы к центральному сайту);
* Веерная сеть (удаленный сайт через центральный сайт на другой удаленный сайт).
  1. Система должна обеспечивать функционал идентификации пользователей.
  2. Система должна быть способна к сбору идентификаторов пользователей посредством запроса Microsoft Active Directory на основе событий безопасности.
  3. Система должна иметь метод аутентификации идентификатора пользователя на основе браузера для недоменных пользователей или компьютеров.
  4. База данных управления приложениями должна содержать свыше 7 700 известных приложений (со ссылкой на сайт производителя).
  5. Система должна обеспечивать детальный контроль безопасности не менее 255,700 Web 2.0 виджетов (со ссылкой на сайт производителя).
  6. Система должна обеспечивать URL категоризацию, включающую более 200 миллионов URL.
  7. Приложение защита от ботнет-атак должно быть способно обнаружить и остановить подозрительное анормальное сетевое поведение.
  8. Приложение защита от ботнет-атак должно использовать многоуровневый механизм обнаружения, который включает репутацию IP, URL и DNS адресов и обнаружение ботов по шаблонам протоколов связи.
  9. Приложение антивирус должно предотвращать доступ к вредоносным веб-сайтам и остановить входящие вредоносные файлы.
  10. Система должна обеспечивать функционал расшифровки и инспекции SSL (входящего / исходящего трафика).
  11. Приложение антивирус должно быть способно проверять шифрованный SSL трафик.
  12. Система должна обеспечивать функционал антиспам и почтового антивируса.
  13. Система должна поддерживать внутренний CA (Certificate Authority), а также внешние сторонние CA.
  14. Управление безопасностью, анализ событий и отчетность.
  15. Система должна обеспечивать функционал централизованного управления безопасностью.
  16. Все приложения безопасности брандмауэра следующего поколения должны быть управляемыми с центральной консоли GUI.
  17. Централизованное управление безопасностью должно управлять не менее 5 шлюзами или «песочницами».
  18. Приложение для управления безопасностью должно поддерживать учетные записи администраторов на основе ролей. Например, только роли для управления политикой межсетевого экрана или только роль для просмотра журнала.
  19. Система должна включать возможность централизованного распространения и применения новых версий шлюзового программного обеспечения.
  20. Решение включая оборудование от производителя также должно поддерживать возможность установки на следующие платформы:
* Открытые сервера, входящие в список аппаратной совместимости производителя;
* Виртуальные машины, функционирующие в средах гипервизоров VMWare vSphere, Microsoft Hyper-V, KVM.
  1. Система должна включать инструмент для централизованного управления лицензиями всех шлюзов или «песочниц» контролируемых станцией управления.
  2. Система должна обеспечивать механизм обновлений во всех приложениях, включая IPS, управление приложениями, URL-фильтрацию, защита от ботнет-атак, антивирус и антиспам.
  3. Система должна обеспечивать функционал централизованного протоколирования и мониторинга.
  4. Система централизованного протоколирования событий должна быть частью системы управления.
  5. Система должна протоколировать все правила.
  6. У средства просмотра журналов событий должна быть возможность индексированного поиска.
  7. Система должна иметь возможность протоколирования событий во всех интегрированных приложениях безопасности на шлюзе (включая виртуальные шлюзы), включая Firewall, IPSEC VPN, IPS, идентификация пользователей, мобильный доступ, управление приложениями, URL-фильтрацию, защита от ботнет-атак, антивирус.
  8. У системы протоколирования должен быть безопасный канал для передачи данных для предотвращения подслушивания, Система должна быть зашифровано и пройти проверку подлинности.
  9. Журналы событий должны безопасно передаваться между шлюзом и управлением или выделенным сервером журналов и консолью просмотра журналов в компьютере администратора.
  10. Система должна включать опцию динамического блокирования активного соединения в графическом интерфейсе системы протоколирования событий без необходимости внесения изменений в базу правил.
  11. Система должна включать настраиваемую установку пороговых значений параметров для выполнения действий при достижении определенных пороговых значений на шлюзе. Действия должны включать: запись события, оповещение, отправка SNMP trap, отправка электронного письма и выполнение определенного пользователем предупреждения.
  12. Система должна включать предварительно настроенные графики для мониторинга эволюции во времени трафика и системных счетчиков: главные правила безопасности, основные пользователи P2P, VPN туннели, сетевой трафик. Система должна обеспечивать возможность создания новых кастомизируемых графиков с различными типами диаграмм.
  13. Система должна обеспечивать функционал централизованной корреляции событий и отчетов.
  14. Система должна иметь возможность корреляции событий из всех приложений, включая Firewall, IPS, идентификация пользователей, мобильный доступ, управление приложениями, URL-фильтрация, защита от ботнет-атак, антивирус, «песочница».
  15. Система должна включать инструмент для корреляции событий из всех функций шлюза и сторонних устройств.
  16. Приложение корреляции событий должно обеспечивать графическое представление событий на основе времени.
  17. Система должна включать возможность поиска внутри списка событий, углубления в детали для изучения и расследования инцидентов.
  18. Система должна включать предопределенные ежечасные, ежедневные, еженедельные и ежемесячные отчеты, в том числе, как минимум, основные события, основные источники, основные пункты назначения, основные сервисы, основные источники и их основные события, основные пункты назначения и их основные события, и основные сервисы, и их основные события.
  19. Система должна поддерживать автоматическое распространение отчетов по электронной почте, загрузку на FTP/Веб-сервер и скрипт рассылки внешних пользовательских отчетов.
  20. Система должна переводить регуляторные требования в выполнимые лучшие практики безопасности.
  21. Система должна генерировать автоматические отчеты по оценке для определения рейтинга соответствия регуляторным требованиям.
  22. Система должна обеспечивать мгновенное уведомление об изменениях политики, влияющих на соответствие регуляторным требованиям.

1. **Порядок оказания услуг:** 
   1. Исполнитель обязуется в течение 5 (пяти) рабочих дней со дня получения подписания договора, оказать услуг по аренде серверного оборудования. Серверное оборудование должно быть новое, принадлежать Исполнителю на праве собственности, не является предметом залога и быть свободно от прав третьих лиц.
   2. При оказании услуги Исполнитель использует собственные материалы и запасные части, стоимость которых включена в стоимость услуги.
   3. Доставка арендуемого оборудования, его погрузка, разгрузка, сборка и монтаж, а также подъем на 2 этаж осуществляется Исполнителем за счет своих средств.
2. **Сроки оказания Услуги:** с момента заключения договора до 31 декабря 2018 года по заявке Заказчика.
3. **Порядок оплаты:** ежемесячно по факту оказания услуг, после подписания соответствующего акта оказанных услуг.
4. **Место оказания услуги:** Республика Казахстан, г.Астана, пр.Кабанбай батыра 15 А, блок Б, серверное помещение.

**Исполнитель:**

Начальник отдела

по управлению данными и информацией Н.Артықалы

**Согласовано:**

Главный экономист

отдела экономики,

финансового и налогового учета А.Джансерикова

Начальник

отдела закупок С.Дуйсенбинов