Техническое задание

на поставку программно-аппаратного комплекса UserGate для защиты сети

1. **Общие требования**
   1. Поставка должна включать в себя программно-аппаратный комплекс (далее – ПАК) UserGate со всеми сопутствующими подписками на сервисы безопасности и технической поддержкой от производителя 24х7 сроком на 36 месяцев согласно следующей спецификации:

|  |  |  |  |
| --- | --- | --- | --- |
| Артикул | Описание продуктов UserGate | | **Кол-во, шт** |
| **Покупка для E3000 без ограничения числа пользователей** | | | |
| 1 | UG-BLC1-E3000-U | Лицензия без ограничения числа пользователей для UserGate E3000 (кластер, 1-я нода) | 1 |
| 2 | UG-BLC2-E3000-U | Лицензия без ограничения числа пользователей для UserGate E3000 (кластер, 2-я нода) | 1 |
| 3 | UG-E3000 | Аппаратная платформа UserGate E3000 | 2 |
| 4 | UG-AT-E3000-U | Модуль Advanced Threat Protection на 1 год для UserGate E3000 без ограничения числа пользовате-лей | 1 |
| 5 | UG-MS-E3000-U | Модуль Mail Security на 1 год для UserGate E3000 без ограничения числа пользователей | 1 |
| 6 | UG-SA-E3000-U | Модуль Stream Antivirus на 1 год для UserGate E3000 без ограничения числа пользователей | 1 |
| Продление на 2 года | | | |
| 1 | UG-SUC2-E3000-U-2Y | Подписка Security Updates на 2 года для UserGate E3000 без ограничения числа пользователей (кла-стер из 2 нод) | 1 |
| 2 | UG-AT-E3000-U-2Y | Продление модуля Advanced Threat Protection на 2 года для UserGate E3000 без ограничения числа пользователей | 1 |
| 3 | UG-MS-E3000-U-2Y | Продление модуля Mail Security на 2 года для UserGate E3000 без ограничения числа пользовате-лей | 1 |
| 4 | UG-SA-E3000-U-2Y | Продление модуля Stream Antivirus на 2 года для UserGate E3000 без ограничения числа пользовате-лей | 1 |
| **Покупка для E1000 без ограничения числа пользователей** | | | |
| 1 | UG-BLC1-E1000-U | Лицензия без ограничения числа пользователей для UserGate E1000 (кластер, 1-я нода) | 1 |
| 2 | UG-BLC2-E1000-U | Лицензия без ограничения числа пользователей для UserGate E1000 (кластер, 2-я нода) | 1 |
| 3 | UG-E1000 | Аппаратная платформа UserGate Е1000 | 2 |
| 4 | UG-NCS410 | Сетевая карта 4\*10 Гб/c для UserGate D200, D500, E1000, E3000 и F8000 | 8 |
| 5 | UG-TSR | Модуль оптический (10Gb, 850nm, 500m., LC, DDM) | 32 |
| 6 | UG-NCS81 | Сетевая карта 8\*1 Гб/c для UserGate D200, D500, E1000, E3000 и F8000 | 2 |
| 7 | UG-AT-E1000-U | Модуль Advanced Threat Protection на 1 год для UserGate E1000 без ограничения числа пользовате-лей | 1 |
| 8 | UG-SA-E1000-U | Модуль Stream Antivirus на 1 год для UserGate E1000 без ограничения числа пользователей | 1 |
| Продление на 2 года | | | |
| 1 | UG-SUC2-E1000-U-2Y | Подписка Security Updates на 2 года для UserGate E1000 без ограничения числа пользователей (кла-стер из 2 нод) | 1 |
| 2 | UG-AT-E1000-U-2Y | Продление модуля Advanced Threat Protection на 2 года для UserGate E1000 без ограничения числа пользователей | 1 |
| 3 | UG-SA-E1000-U-2Y | Продление модуля Stream Antivirus на 2 года для UserGate E1000 без ограничения числа пользовате-лей | 1 |
| UserGate Log Analyzer | | | |
| 1 | UG-LA | Лицензия UserGate Log Analyzer | 1 |
| 2 | UG-LA-E14 | Аппаратная платформа UserGate LogAn Е14 | 2 |
| 3 | UG-LAC2-E3000-U | Сенсор для подключения UserGate Log Analyzer E3000 (кластер, 2 ноды) | 1 |
| 4 | UG-LAC2-E1000-U | Сенсор для подключения UserGate Log Analyzer E1000 (кластер, 2 ноды) | 1 |
| Продление на 2 года | | | |
| 1 | UG-LAC2-SU-E3000-U-2Y | Подписка Security Updates на сенсор для UserGate Log Analyzer E3000 (кластер, 2 ноды) на 2 года | 1 |
| 2 | UG-LAC2-SU-E1000-U-2Y | Подписка Security Updates на сенсор для UserGate Log Analyzer E1000 (кластер, 2 ноды) на 2 года | 1 |

* 1. Поставляемый ПАК должен устанавливаться на площадке Заказчика.
  2. Все поставляемое оборудование должно быть новым, не бывшим в употреблении, в заводской упаковке и полной комплектации в соответствии с моделями, указанными в спецификации выше.
  3. Условия оплаты - по умолчанию 50% предоплата, 50 после подписания актов выполненных работ;
  4. Локальная техническая поддержка – 3 года.
  5. Срок поставки оборудования - 70 рабочих дней с даты подписания договора.
  6. Срок оказания Поставщиком услуг по установке и настройке поставляемого оборудования – 30 рабочих дней с даты поставки оборудования.
  7. Готовность подписать договор - по умолчанию 10 календарных дней с момента объявления победителя.

1. Требуемые функциональные, технические, качественные и эксплуатационные характеристики межсетевых экранов **UserGate.**
   1. **Функциональные требования к межсетевым экранам** 
      1. Лицензирование должно осуществляться для неограниченного количества пользователей.
      2. Межсетевой экран (далее – МСЭ) должен регулярно получать обновления сигнатур модулей безопасности и перечень актуальных угроз с сервера производителя.
      3. МСЭ должен поддерживать объединение в кластер не менее 2 устройств с возможностью создания типов кластеров с холодным резервом (active/passive) и с горячим резервом (active/active).
      4. МСЭ должен иметь функциональность межсетевого экранирования, то есть обеспечивать возможность создания правил фильтрации сетевого трафика на основе IP адресов, портов и приложений.
      5. МСЭ должен иметь функциональность балансировки нагрузки.
      6. МСЭ должен иметь функциональность управления полосой пропускания трафика (traffic shaping).
      7. МСЭ должен обеспечивать инспекцию SSL трафика c возможностями анализа и передачи проинспектированного трафика во внешние системы по протоколу ICAP (Internet Content Adaptation Protocol).
      8. МСЭ должен обеспечивать анализ SSH трафика (SSH inspection).
      9. МСЭ должен обеспечивать динамическую маршрутизацию IPv4, IPv6.
      10. МСЭ должен иметь возможность работы по протоколу WCCP (как в режиме сервера, так и в режиме клиента).
      11. МСЭ должен обеспечивать оптимизацию WAN соединений.
      12. МСЭ должен обеспечивать антивирусную защиту.
      13. МСЭ должен иметь функциональность предотвращения вторжения IPS.
      14. МСЭ должен обеспечивать WEB фильтрацию трафика с возможностью ограничения доступа к определенным категориям сайтов.
      15. В МСЭ должна обеспечиваться WEB фильтрация трафика по не менее 85 категориям.
      16. МСЭ должен позволять принудительное включение режима безопасного поиска в популярных поисковых Системах.
      17. МСЭ должен иметь функциональность контроля приложений.
      18. МСЭ должен иметь функциональность Web-proxy.
      19. МСЭ должен иметь возможность проверки на наличие вирусов внутри HTTP, SMTP, POP3, IMAP, FTP и IM трафика.
      20. МСЭ должен иметь возможность автоматически по расписанию получать обновления антивирусных баз.
      21. МСЭ должен иметь возможность помещать инфицированные сообщения в карантин.
      22. МСЭ должен иметь возможность блокировки передачи файлов в зависимости от размера.
      23. МСЭ должен иметь возможность блокировки передачи файлов в зависимости от типа.
      24. МСЭ должен поддерживать соединения множества WAN сетей.
      25. МСЭ должен поддерживать маршрутизацию на основе политик.
      26. МСЭ должен поддерживать динамическую маршрутизацию на основе протоколов RIP v1 и v2, OSPF, BGP.
      27. МСЭ должен поддерживать использование зон безопасности.
      28. МСЭ должен поддерживать маршрутизацию между зонами.
      29. МСЭ должен поддерживать маршрутизацию между виртуальными сетями.
      30. МСЭ должен поддерживать администрирование на основе ролей.
      31. МСЭ должен поддерживать несколько уровней администраторов и пользователей.
      32. МСЭ должен поддерживать обновление встроенного ПО через протокол TFTP и веб-интерфейс.
      33. МСЭ должен поддерживать возможность возврата к предыдущему состоянию (версии) встроенного ПО.
      34. МСЭ должен поддерживать аутентификацию пользователей посредством внутренней базы данных.
      35. МСЭ должен поддерживать Kerberos аутентификацию пользователей.
      36. МСЭ должен поддерживать аутентификацию пользователей посредством Windows Active Directory при этом аутентификация пользователей операционных систем Windows 7 и выше, включенных в домен, должна выполняться автоматически без дополнительных процедур запроса паролей.
      37. МСЭ должен поддерживать аутентификацию пользователей посредством внешней базы данных RADIUS/LDAP.
      38. МСЭ должен поддерживать аутентификацию пользователей через привязку по IP/MAC-адресу.
      39. МСЭ должен поддерживать аутентификацию на основе групп пользователей.
      40. МСЭ должен поддерживать функции NAT, PAT, «прозрачный» (мост).
      41. МСЭ должен поддерживать функции NAT на основе политик.
      42. МСЭ должен поддерживать функции VLAN Tagging (802.1Q).
      43. МСЭ должен поддерживать настройку профилей безопасности.
      44. МСЭ должен уметь предотвращать не менее 10000 типов сетевых атак.
      45. МСЭ должен иметь возможность настройки списка сигнатур атак.
      46. МСЭ должен поддерживать автоматическое обновление базы атак и сигнатур IPS.
      47. МСЭ должен регулярно получать с сервера производителя «черный» список IP адресов спамеров и открытых релеев.
      48. МСЭ должен поддерживать фильтрацию по «черным/белым» спискам IP-адресов.
      49. МСЭ должен иметь возможность отсылки логов на удаленный Syslog сервер.
      50. МСЭ должен поддерживать сервис извлечения исполняемой составляющей из файлов форматов Microsoft Office и PDF, сохраняя исходный формат файла.
      51. МСЭ должен иметь графические средства для мониторинга сетевого трафика, состояния системы и обнаруженных угрозах.
      52. МСЭ должен иметь возможность отправки уведомлений по электронной почте о вирусах и сетевых атаках.
      53. МСЭ должен поддерживать отправку файлов и URL на анализ в Сloud Sandbox (облачную песочницу) для обнаружения неизвестных угроз класса “0-day”.
      54. МСЭ должен иметь лицензирование в комплекте поставки для анализа в Cloud Sandbox не менее 10 000 объектов (файлов и URL) в день (24 часа).
      55. МСЭ должен поддерживать протокол VRRP.
      56. МСЭ должен поддерживать интеграцию с SIEM.
      57. МСЭ должен иметь возможность установления гарантированной, максимальной или приоритетной пропускной способности.
      58. МСЭ должен поддерживать обнаружение и контроль использования служб мгновенных сообщений.
      59. МСЭ должен поддерживать управление через веб-интерфейс.
      60. МСЭ должен иметь возможность интеграции с Системами централизованного управления и построения отчетов.
      61. МСЭ должен поддерживать протоколы NetFlow, sFlow.
      62. МСЭ должен обеспечивать возможность управления политиками безопасности в консольном режиме из командной строки.
      63. МСЭ должен поддерживать интеграцию с внешними Системами для получения информации телеметрии, включающей информацию о пользователях, используемой модели и версии операционной системы, IP адрес, MAC адрес, информацию об обнаруженных уязвимостях.
      64. МСЭ должен поддерживать интеграцию с внешними Системами для оценки соответствия рабочих станций корпоративной политике безопасности. В случае несоответствия политике безопасности проверяемый хост должен быть помещен в карантин с ограничением сетевого доступа.
   2. Технические требования к программно-аппаратному комплексу **UserGate**
      1. Требуемые минимальные технические характеристики:

* Производительность системы по функциональности межсетевого экранирования (1518/512/64 byte UDP): 32/32/24 Гбит/c;
* Количество правил межсетевого экранирования, доступных для настройки в системе: не менее 10000;
* Количество новых сессий в секунду (TCP): не менее 450000;
* Производительность инспекции IPS: не менее 7,8 Гбит/с;
* Производительность инспекции Application Control: не менее 12 Гбит/с;
* Производительность при одновременной работе инспекций Firewall + Application Control + AV+ IPS: не менее 5 Гбит/с;
* Количество сетевых интерфейсов: 16 х GE RJ45;
* Количество слотов GE SFP: не менее 16;
* Количество USB-портов: не менее 2 шт.;
* Внутренний блок питания постоянного тока с внешним питанием 100–240V AC, 50–60 Hz: не менее 1 шт.
* Возможность установки в стандартную серверную стойку 19” (тип исполнения rack).
* Включенные в поставку трансиверы SFP: не менее 2.

1. **Требования к потенциальному Поставщику**
   1. Потенциальный Поставщик должен предоставить на конкурс авторизационное письмо

от производителя UserGate о том, что имеет право на продажу решения и оказание услуг

локальной технической поддержки на территории Республики Казахстан.

* 1. В рамках поставки потенциальный Поставщик должен произвести все необходимые

работы по установке и настройке поставляемого решения, в соответствии с

международными стандартами информационной безопасности и внутренними

нормативными правилами на территории Заказчика.

* 1. У потенциального Поставщика должно быть в штате не менее 2-х сертифицированных производителем специалистов, с опытом работы не менее 1 года. Квалификация специалиста должна быть подтверждена сертификатами.
  2. Потенциальный Поставщик должен оказывать локальную техническую поддержку 24х7 путем принятия обращений от Заказчика по телефону или по электронной почте (email) в течение 36 месяцев с даты ввода оборудования в промышленную эксплуатацию.