**Техническая спецификация**

**для приобретения и внедрения оборудования межсетевого экранирования (NGFW).**

1. **Требования к техническим решениям претендентов**
* Предложенное решение должно максимально соответствовать требованиям и рекомендациям, описанным в данном документе.
* Предложение должно содержать в себе документальное подтверждение соответствия Технического задания (ТЗ).
* Одним из критериев оценки претендентов будет являться наибольшее совпадение предлагаемых характеристик с требованиями данного ТЗ.
1. **Общие требования к поставляемому оборудованию**
* По требованию Заказчика Поставщик должен предоставить вместе с товаром все необходимые сертификаты качества и/или соответствия, если в соответствии с законодательством Республики Казахстан оборудование, поставляемое по договору, подлежит обязательной сертификации.
* Техническая документация и все необходимые руководства пользователя должны быть составлены на русском и/или английском языке.
* Поставщик за свой счет проводит обучение персонала (не менее 2 работников) Заказчика на специализированных курсах по настройке и администрированию поставляемого оборудования.
* Поставщик должен обладать достаточными компетенциями по вводу в эксплуатацию и поддержки поставляемого комплекса, а также иметь в штате не менее-2-х сертифицированных инженеров, имеющих сертификаты производителя на инсталляцию и эксплуатацию поставляемого оборудования.
* Поставщик должен провести инсталляцию и настройку оборудования в соответствии с требованиями Заказчика на его площадке.
* Все предлагаемые товары должны быть новыми, не использованными, в заводской упаковке и не иметь физических повреждений на момент передачи Заказчику.
* Все предлагаемые товары должны функционировать при следующих условиях:
* Параметры электропитания (220V ± 20V, 50Hz ± 1Hz).
* Резервирование электропитания по схеме N+1.
* Температура окружающей среды: от +10C° до +32C°.
* Относительная влажность от 10% до 80%.
* Запыленность до 0.4 г/м3.
1. **Обязательные требования к гарантийному обслуживанию**
* Гарантийный срок на оборудование и его компонентов должен быть не менее 12 месяцев со дня отгрузки на склад Заказчика.
* Гарантийная поддержка оборудования производится на площадке Заказчика ДО АО Банк ВТБ (Казахстан) ул. Тимирязева 26, г. Алматы. В случае невозможности исполнения гарантийных обязательств по указанному адресу, исполнение работ по диагностике и ремонту оборудования осуществляется в авторизованном сервисном центре.
* Проведение диагностики и ремонта на месте эксплуатации осуществляется по рабочим и выходным дням.
* Гарантийное обслуживание оборудования должно осуществляться авторизованным сервисным центром/партнером на территории Республики Казахстан. Обслуживание осуществляется бесплатно в течение всего гарантийного срока. Сервисный центр/партнер должен обеспечить ремонт/замену вышедшего из строя оборудование в течении 10 календарных дней на весь гарантийный срок.
* Консультации инженеров «горячей линии» производителя и/или сервисного партнера по вопросам восстановления работоспособности или диагностики, эксплуатации оборудования и программного обеспечения в режиме 24х7.
1. **Состав оборудования и требования к комплексу средств межсетевого экранирования и обнаружения вторжений уровня сети**
	1. Общие требования
2. Количество – 2 единицы.
3. В качестве средства межсетевого экранирования и обнаружения вторжений уровня сети должен использоваться отказоустойчивый кластер/кластеры. В случае выхода из строя одного из комплексов, входящих в кластер, переключение на второй (резервный) комплекс должно происходить автоматически без вмешательства администратора.
4. Функция разграничения сетевого доступа должна поддерживать работу правил межсетевого экранирования на канальном, сетевом, транспортном и прикладном уровнях в режиме реального времени и поддерживать следующие возможности:
* Межсетевое экранирование
* Обнаружение (IDS) и предотвращение вторжений (IPS), IPSec и SSL VPN
* Защита от вредоносных программ (Антивирус)
* Антиспам
* Web-фильтрация
* Контроль приложений
* WAN-оптимизация
* Балансировка нагрузки
* Маршрутизация/коммутация
* Сканер уязвимостей
1. Возможность организации в рамках одного устройства совместно прозрачных (L2/Transparent) и маршрутизируемых (L3/Routed) виртуальных контекстов.
2. Устройство должно поддерживать функционал отказоустойчивого кластера в режимах Active/Active, Active/Passive, Clustering.
3. Балансировка запросов по нескольким WAN-каналам с учетом состояния каналов и их характеристик таких как «latency», «jitter» (SD-WAN).
4. Система должна иметь функциональность управления полосой пропускания трафика (traffic shaping).
5. Поддержка аутентификации и применение политик и профилей безопасности для пользователей и администраторов по протоколу LDAP, Tacacs+, RADIUS.
6. Поддержка Telnet, SSH, SNMP, Web-интерфейса для управления, локальная консоль для составления отчетов в режиме реального времени.
7. Поддержка протоколов (BFD, VPRP) повышения готовности.
8. Поддержка клиента IPsec VPN для основных операционных систем (Windows, MacOS, Linux, Android, IOS).
9. Решение должно поддерживать виртуализацию шлюза безопасности для консолидации нескольких виртуальных шлюзов на одном физическом устройстве.
10. Решение должно иметь возможность расширения минимум до 6 виртуальных систем при применении дополнительной лицензии. МСЭ должнен поддерживать виртуальные коммутаторы и виртуальные маршрутизаторы для конфигурирования сетевых коммуникаций между виртуальными системами (виртуальными шлюзами). Каждый виртуальный шлюз должен иметь возможность запуска своего собственного набора сервисов безопасности. Например, один виртуальный шлюз работает как Firewall, второй – как Firewall и IPS, третий – Firewall, IPS, Application Control, URL Filtering, и так далее.
11. Сервисы обновления сигнатур и подписок (Application Control, IPS, AV, Botnet IP/Domain, Web Filtering) со сроком действия не менее 12 месяцев с момента внедрения оборудования в эксплуатацию.

4.2 Требования к аппаратной части и поддержки сервисов

|  |  |
| --- | --- |
| Пропускная способность в режиме Firewall, Гб/с | ≥ 45 |
| Пропускная способность в режиме Threat Prevention, Гб/с | ≥ 9.5 |
| Пропускная способность в режиме NGFW, Гб/с | ≥ 25 |
| Пропускная способность в режиме IPS, Гб/с | ≥ 25 |
| Пропускная способность VPN, Гб/с | ≥ 11 |
| Количество одновременно поддерживаемых сессий, млн  | ≥ 8 |
| Количество новых сессии в одну секунду в режиме NGFW, тыс | ≥ 300 |
| Наличие SSD диска | + |
| Наличие портов 10/100/1000Base-T RJ-45, шт. | ≥ 8 |
| Наличие портов 1000Base-F SFP, шт. | ≥ 4 |
| Наличие портов 10GBase-F SFP+, шт. | ≥ 4 |
| Наличие портов 40GBase-F QSFP+, шт. | ≥ 2 |
| Наличие портов для создания отказоустойчивого кластера, шт. | ≥ 2 |
| Наличие USB портов | + |
| Наличие консольного порта | + |
| Анализ файлов на уровне процессора, ОС и статический анализ файлов | + |
| Обезвреживание и восстановление файлов с помощью Threat Extraction | + |
| Пассивная и активная агрегация каналов 802.3ad | + |
| Режим высокой доступности 2-го уровня (прозрачный) и 3-го уровня (маршрутизация) | + |
| Обход отказа сессии при изменении маршрутизации, отказе устройства и канал | + |
| Поддержка кластеризации XL или VRRP | + |
| Одноадресная и многоадресная маршрутизация OSPFv2 и v3, BGP, RIP | + |
| Создание виртуальных МСЭ | + |
| Поддержка ikev2 | + |
| Наличие собственного движка IPS и лаборатории сигнатур | + |
| Форм фактор  | Rack Mounting 19” |
| Наличие резервного блока питания | + |
| Тип исполнения | Аппаратный |