**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

на поставку программно-аппаратного комплекса с программным обеспечением

Приобретение VipNet Coordinator HW10 4.x в количестве 1 единицы;

**1. Объект закупки и его количество**

Таблица №1

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Наименование | Ед. изм. | Объем |
| 1 | Поставка программно-аппаратного комплекса VipNet Coordinator HW10 4.x | шт | 1 |

1. **Технические требования к программно-аппаратному комплексу (далее – ПАК) криптографической защиты информации (далее – Криптошлюз) ViPNet Coordinator HW10 C, аппаратная платформа HW10 F1.**

2.1 Функциональные требования

Криптошлюз должен обеспечивать:

* возможность построения VPN-сети, позволяющей организовать одно или множество сетевых соединений (логическую сеть) поверх каналов связи сетей передачи данных, использующих протоколы семейства TCP/IP;
* криптографическую защиту данных (шифрование, аутентификацию, защиту от повторов и изменений), передаваемых по каналам VPN;
* регистрацию информации о текущих IP-адресах и способах подключения к каналам связи узлов VPN-сети и ее распространение;
* установление каналов VPN между клиентами в защищенных сетях и удаленными клиентами VPN через межсетевые экраны и устройства с NAT;
* возможность подключения клиентов VPN по протоколу TCP при недоступности UDP;
* возможность организации в одном устройстве защищенного соединения как на сетевом, так и канальном уровне модели OSI;
* динамическую маршрутизацию средствами протокола OSPF;
* контроль и фильтрацию информационных потоков данных в соответствии с заданными правилами;
* трансляцию сетевых адресов (SNAT/DNAT);
* обработку прикладных протоколов FTP, DNS, H.323, SCCP, SIP для всех видов трафика (защищенного, открытого и туннелируемого);
* проксирование и фильтрацию HTTP-трафика по командам и мобильному коду;
* статическую маршрутизацию;
* предоставление DHCP-, DNS-, NTP-сервисов защищаемым сетевым объектам;
* возможность построения виртуальных локальных сетей (поддержка стандарта VLAN IEEE 802.1Q);
* возможность использования технологии агрегирования – объединения нескольких физических каналов передачи данных в сетях Ethernet в один логический;
* реализацию политики качества обслуживания (QoS) приоритетной обработки средствами сервиса дифференцированного обслуживания (DiffServ);
* экспорт журнала регистрации IP-пакетов по сети в формате CEF;
* балансировку нагрузки на вычислительную сеть и резервирование каналов доступа во внешнюю сеть средствами функции MultiWAN, включающую в себя проверку состояния шлюзов и политики маршрутизации;
* возможность антивирусной защиты HTTP-трафика при взаимодействии по протоколу ICAP с внешним средством антивирусной защиты;
* возможность изменения значения MTU для сетевых интерфейсов;
* взаимодействие с источником бесперебойного питания (UPS) для корректного завершения своей работы в случае получения сигнала об истощении батареи;
* удаленное (защищенное) управление и мониторинг с помощью веб-интерфейса и SSH;
* сигнализацию о событиях по протоколам SNMP, syslog;
* удаленное обновление собственного программного обеспечения;
* возможность кластеризации с целью обеспечения горячего резервирования.

2.2 Требования к аппаратной части

Криптошлюз должен удовлетворять следующим требованиям:

* форм-фактор: мини-компьютер;
* наличие не менее 1 (одного) сетевого интерфейса Ethernet RJ45 1 Гбит/с;
* наличие не менее 2 (двух) сетевых интерфейсов Ethernet RJ45 2,5 Гбит/с.

2.3 Требования к производительности

Криптошлюз должен обеспечивать следующие показатели производительности:

* пропускная способность L3 VPN – до 35 Мбит/с;
* пропускная способность межсетевого экранирования – до 200 Мбит/с.

2.4 Требования к сертификации

Криптошлюз должен соответствовать:

* требованиям ФСБ России к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС3;
* требованиям документов «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016).

Для поставки необходимо **наличие у Исполнителя действующей лицензии** на разработку, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

Основанием требования наличия лицензий является: п. 1, ч.1, ст. 12 Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», Постановление Правительства РФ от 16.04.2012 N 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».