|  |  |
| --- | --- |
| **Описание** | **Спецификация** |
| Количество одновременно поддерживаемых VPN туннелей | Неограниченное количество. |
| Производительность | Не менее 200 Мб/с для Сервера защиты (определяется договором на поставку);  Не менее 7 Мб/с для Устройства защиты клиента. |
| Количество сетевых интерфейсов | Не менее 2 для Сервера защиты (определяется договором на поставку);  2 для Устройства защиты клиента. |
| Алгоритмы шифрования | СТБ 34.101.31-2011 (п. 6.3, 6.4, 6.5);  ГОСТ 28147-89 (п.3, 4). |
| Алгоритмы контроля целостности (имитозащита) | СТБ 34.101.31-2011 (п. 6.6);  СТБ 34.101.47-2017 (п. 6.1);  ГОСТ 28147-89 (п. 5). |
| Генерация ключевой пары | СТБ 34.101.45-2013 с использованием физического датчика случайных чисел. |
| Алгоритмы электронной цифровой подписи | СТБ 34.101.45-2013. |
| Алгоритмы вычисления хэш сумм | СТБ 34.101.31-2011 (п. 6.9). |
| Взаимная аутентификация устройств и выработка общего ключа | СТБ 34.101.66-2014 (п.7.5). |
| Генерация случайных чисел | Аппаратный физический датчик. |
| Генерация псевдослучайных чисел | СТБ 34.101.47-2017 (п. 6.2, 6.3). |
| Формат сертификатов открытых ключей | СТБ 34.101.19-2012. |
| Поддерживаемые системы сертификатов открытого ключа | ГосСУОК, УЦ БУТБ, УЦ «АСБ Беларусбанк», УЦ «ИВЦ Минфина». |
| Формат запроса на выпуск сертификата открытого ключа | СТБ 34.101.17-2012. |
| Поддержка списка отозванных сертификатов | СТБ 34.101.19-2012. |
| Стандарты IKE/IPsec | RFC 4301-4308. |
| Защита трафика | Протоколы IPsec:  – IPsec Encapsulating Security Payload (ESP) – инкапсуляция пакетов данных;  – IPsec Authentication Header (AH) – защищенный заголовок. |
| Управление ключами | Протокол IKEv2. |
| Смена ключей шифровани | Автоматически:  – при достижении объема переданного трафика;  – при истечении установленного времени. |
| Работа через NAT | Протокол NAT Traversal IPsec. |
| Обеспечение надежности защищенных соединений | Протокол Dead Peer Detection (DPD). |
| Управление | – локально;  – удаленно по протоколу SSH. |
| Событийное протоколирование | Средствами SYSLOG. |
| Защита от несанкционированного доступа | Датчик вскрытия корпуса. |
| Самотестирование | При запуске устройства и по запросу администратора:  – контроль работоспособности аппаратных компонентов устройства;  – контроль целостности встроенного ПО;  – контроль работоспособности криптографических алгоритмов. |
| Электропитание | Сервер защиты:  – от сети электропитания общего пользования 220-230 В / 49-51 Гц.  Устройства защиты клиента:  – от защищаемой сети по протоколу PoE (IEEE 802.3at);  – от сети электропитания общего пользования 220-230 В / 49-51 Гц с использованием micro-USB AC-DC адаптера;  – от USB 3.0-порта защищаемого оборудования. |
| Потребляемая мощность | До 50 Вт для Сервера защиты.  До 5 Вт для Устройства защиты клиента. |
| Фильтрация трафика | Средствами iptables. |
| Предоставление статистики | SNMP |
| Поддержка защиты данных второго уровня сетевой модели (L2) | При помощи проткола L2TPv3 pseudowire. |
| Маршрутизация | Статическая маршрутизация.  Динамическая маршрутизация:  – Routing Information Protocol (RIP);  – Open Shortest Path First (OSPF);  – Border Gateway Protocol (BGP). |
| Механизмы обеспечения отказоустойчивости | Virtual Router Redundancy Protocol (VRRP);  Common Address Redundancy Protocol (CARP);  Reverse Route Injection (RRI). |