Возможности	КриптоПро NGate 1.0 R2
Общие сведения	
Наличие в реестре отечественного ПО	Да
Сертификаты соответствия	Сертификаты ФСБ России по классам КС1, КС2, КС3 шлюза и VPN-клиента
Модельный ряд	NGate ЦУС 100, NGate ЦУС 200, NGate 300, NGate 600, NGate 1000, NGate 1500, NGate 2000, NGate 3000
Языки интерфейса	Русский и английский, возможно добавление любого языка
Архитектура решения	
Вид поставки	Программно-аппаратный комплекс, виртуальная машина
Архитектура системы	Серверная и клиентская части, центр управления сетью
Совместимость со средами виртуализации	Да
Сетевые интерфейсы младшей модели	Модель NGate 300: 4x10/100/1000BASE-T RJ45
Сетевые интерфейсы старшей модели	Модель NGate 3000: 4x10/100/1000BASE-T RJ45, 4x10GB SFP+
Производительность	
Производительность в режиме HTTPS-прокси младшей модели, Мбит/с	Модель NGate 300: 500
Производительность в режиме HTTPS-прокси старшей модели, Мбит/с	Модель NGate 3000: до 16 000
Количество одновременных аутентифицированных соединений младшей модели, штук	Модель NGate 300: до 500
Количество одновременных аутентифицированных соединений старшей модели, штук	Модель NGate 3000: до 45 000
Аутентификация пользователей	
Аутентификация удалённых пользователей и администратора на основе технологии открытых ключей (X.509 v.3)	Да

Разграничение доступа к защищаемым ресурсам на основе полей сертификата, вплоть до OU (Organization Unit)	Да
Аутентификация пользователей в Active Directory с помощью протокола LDAP с использованием сертификатов, записанных в LDAP (MS AD)	Да
Аутентификация пользователей в Active Directory с помощью протокола LDAP с использованием логина и пароля	Да
Аутентификация пользователей по локальной базе данных	Да
Возможность разрешения, запрещения, ограничения использования веб-приложений клиентом на основе политик	Да
Проверка сертификатов ключей по спискам отозванных сертификатов (CRL)	Да
Поддержка аутентификации по UPN-сертификату	Да
Перечень поддерживаемых идентификаторов	«Рутокен», eToken, JaCarta, ESMART
Режим работы без аутентификации пользователя	Да, в режиме TLS Offload
Работа с криптоключами	
Поддержка зарубежных криптографических алгоритмов	RSA, ECDSA, AES, AES-GCM
Поддержка TLS VPN	Да
Поддержка протокола TLS версий 1.2 и выше	Да
Поддержика Ipsec VPN	Да
Форматы поддерживаемых сертификатов и контейнеров	PEM, DER, PKCS7, PFX
Генерация на TLS-шлюзе закрытого ключа и формирование на его основе открытого ключа с созданием запроса на получение сертификата стороннего удостоверяющего центра (с использованием отечественных криптоалгоритмов)	Да
Генерация на TLS-шлюзе закрытого ключа и формирование на его основе открытого ключа с созданием запроса на получение сертификата стороннего удостоверяющего центра (с использованием зарубежных криптоалгоритмов)	Да
Генерация закрытого ключа и формирование на его основе открытого ключа с созданием запроса на получение сертификата стороннего удостоверяющего центра на TLS-клиенте (с использованием отечественных криптоалгоритмов)	Да
Генерация закрытого ключа и формирование на его основе открытого ключа с созданием запроса на получение сертификата стороннего удостоверяющего центра на TLS-клиенте (с использованием зарубежных криптоалгоритмов)	Да

Соединение		
Поддержка NTP (Network Time Protocol)		Да
Поддержка расширения протокола TLS – Server Name Indication (SNI)		Да
Принудительная аутентификация пользователя через портал		Да
Возможность работы с динамическими VPN-туннелями		Да
Возможность модификации HTTP-заголовков к защищаемым ресурсам по конфигурируемым		Да
Возможность модификации динамически изменяемых HTTP-заголовков к защищаемым ресурсам по конфигурируемым правилам		Да
Очистка сессионной информации при разрыве соединения		Да
Работа с клиентской частью		
Перечень поддерживаемых ОС для собственных TLS-клиентов	Microsoft Windows	7 и выше
	Linux	CentOS 7, Red OS, Fedora, Oracle Linux 7, SUSE Linux Enterprise Server 12, OpenSUSE 13.2, RHEL 7, Ubuntu 14 / 16 / 17 / 18, Linux Mint 13 / 14 / 15 / 16 / 17 / 18, Debian 7 / 8 / 9, Astra Linux Special Edition, Common Edition, ALT Linux 7, «Альт 8 СП», ROSA 2011, РОСА «ХРОМ» / «КОБАЛЬТ» / «НИКЕЛЬ», ThinLinux
	Apple macOS	Mac OS X 10.9 и выше
	Мобильные ОС	Android, iOS, Аврора
Поддерживаемые браузеры		Любой соблюдающий спецификацию TLS
Собственный TLS-клиент		Да
Наличие бесплатного TLS-клиента		Да
Возможность использования защищённых ключевых носителей в клиентском ПО		Да
Поддержка мобильных устройств		Да
Возможность подключения без TLS-клиента		Да
Режимы работы		
Создание защищённого TLS-туннеля для приложений, использующих TCP/IP-протоколы (с использованием TLS-клиента)		Да
Режим прокси (TLS Offload)		Да

Режим публикации приложения на портале	Да
Количество самостоятельных порталов, которые можно создать на шлюзе	Без ограничений
Возможность создания разных самостоятельных порталов на одном и том же порту	Да
Мониторинг и работа с журналами	
Регистрация событий, связанных с настройкой и функционированием TLS-шлюза	Да
Оперативный мониторинг состояния TLS-шлюза и оповещение	Да
Статистика подключений	Да
Возможность экспорта журналов аудита во внешние системы, в том числе в SIEM	Да, через Syslog
Отказоустойчивость и масштабирование	
Возможность «холодного» резервирования аппаратной платформы TLS-шлюза	Да
Возможность полноценной кластеризации в режиме Active-Active с синхронизацией сессий	Да
Возможность масштабирования TLS-шлюза посредством подключения в кластер новых нод шлюзов с синхронизацией сессий	Да, до 32 нод
Возможность автоматического перераспределения нагрузки между элементами высокопроизводительного кластера TLS-шлюзов с использованием внешнего балансировщика трафика	Да
Возможность бесшовного переключения сессии пользователя без разрыва соединения в случае выхода из строя одного или нескольких узлов кластера	Да
Количество узлов в кластере (при использовании синхронизации сессий)	32
Резервное копирование и восстановление настроек	Да
Отсутствие ограничения на количество узлов в кластере (без синхронизации сессий)	Да
Поддержка LACP	Да
Наличие второго блока питания	Да (на старших моделях: NGate 1500, NGate 2000, NGate 3000)
Управление TLS-шлюзом	
Возможность управления несколькими кластерами шлюзов безопасности из одной системы	Да

Поддержка удалённого и локального управления TLS- шлюзом	Да: в случае отдельной инсталляции — локально, в случае распределённой инсталляции — из центра
Возможность удалённого управления TLS-шлюзом с использованием веб-интерфейса	Да
Возможность удалённого обновления программного обеспечения	Да
Управление доступом удалённых пользователей	
Управление доступом пользователей на основе даты и времени	Да
Управление доступом пользователей с двухфакторной аутентификацией через Radius	Да
Автоматическое разграничение доступа пользователей на основе используемых алгоритмов шифрования	Да
Разграничение доступа пользователей к защищаемым подсетям на основе членства в группах доменов	Да
Контроль состояния установленных защищённых соединений с удалёнными пользователями с возможностью принудительного завершения сессии пользователя по команде администратора	Да
Автоматический разрыв активной сессии пользователя по невалидному сертификату на основе полученного CRL	Да
Другие функции	
Внешнее API удаления сессий	Да
Возможность передачи IP-адреса клиента защищаемому ресурсу в начале соединения	Да
Возможность настройки ограничения количества одновременных сессий пользователя на портале	Да
Поддержка туннелирования произвольного TCP-траффика	Да
Auto-reconnect VPN, без необходимости ввода учетных данных	Да
Запрет взаимодействия между пользователями, подключенными к VPN	Да
"Always-On" (предоставляет возможность предотвратить прямой доступа в Интернет, если устройство не подключено к корпоративной сети)	Да
Split-tunneling: возможность отправлять в туннель только трафик до определенных сетей, весь остальной трафик исключить	Да
Split-tunneling: возможность отправлять в туннель весь трафик, за исключением определенных сервисов (исключение на основе IP-адресов)	Да

Возможность формирования различных профилей подключений с предустановленными настройками для VPN-клиентов	Да
Возможность выбора определённого профиля при подключении к VPN	Да
Ограничение количества разрешенных одновременных сессий для одной учетной записи, в рамках одного профиля VPN (в рамках одного шлюза)	Да
Возможность ограничения доступа к ресурсам сети на основе ролевой модели	Да
Возможность смены пароля доменной учетной запсиси при подключении к VPN, в случае истечения срока действия пароля учетной записи	Да
Возможность использования встроенных средств подробного логирования и самодиагностики клиента для решения инцидентов при возникновении проблем с подключением	Да
Возможность географического резервирования VPN (размещение VPN-шлюзов в разных геогрфических точках с балансировкой и резервированием)	Да
Централизованное управление конфигурациями и обновлением VPN-шлюзов	Да
Централизованное управление конфигурациями и обновлением клиентов	Да
Поддержка snmp	Да
Технологические интеграции	
Поддержка функционала оценки состояния устройства пользователя	Да (с применением ПО Сакура/SafeMobile)
Ограничение доступа к сети при несоответствии требованиями политики ИБ	Да (с применением ПО Сакура/SafeMobile)