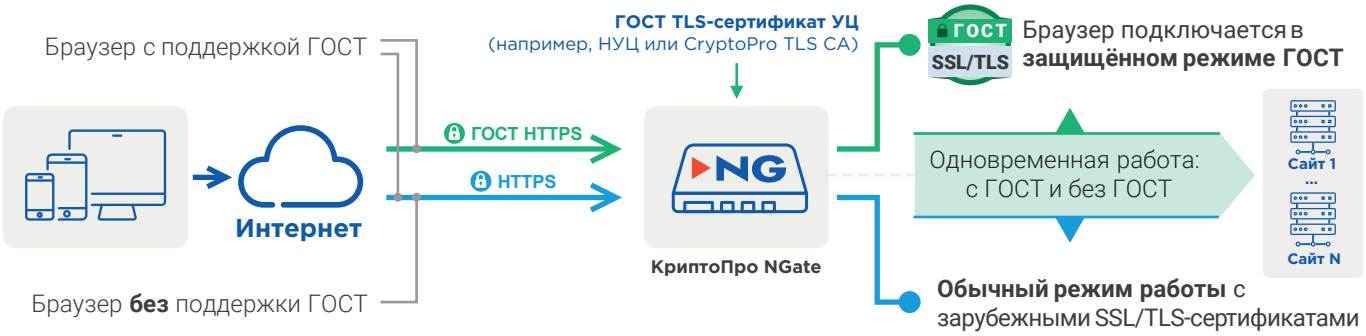
КриптоПро NGate

КриптоПро NGate – это универсальный криптографический шлюз удаленного доступа и VPN, объединяющий в себе четыре сценария применения:

1. **Web TLS**
   TLS-шлюз доступа к веб-сайтам
2. **Web Portal TLS**
   Шлюз портального доступа
3. **Point-to-Site TLS VPN**
   VPN-шлюз удаленного доступа
4. **Site-to-Site IPsec VPN**
   VPN-шлюз доступа между площадками

1 Web TLS

TLS-шлюз доступа к веб-сайтам



Режим TLS-шлюза используется для безопасного подключения к веб-сайтам и снятия нагрузки по обработке TLS-соединений с веб-серверов. В данном режиме КриптоПро NGate может использоваться для обеспечения доступа к госпорталам, сайтам организаций, ДБО, сервисам телемедицины и другим информационным системам, доступ пользователей к которым производится через веб-браузер.

КриптоПро NGate обеспечивает одновременную поддержку TLS как с отечественными, так и зарубежными криптоалгоритмами. Это позволяет реализовать плавную миграцию механизмов защиты доступа к веб-сайтам на ГОСТ.

2 Web Portal TLS

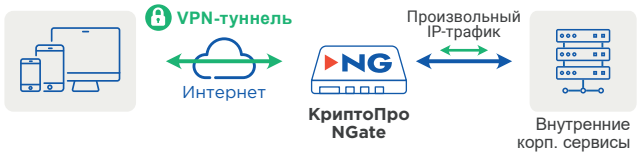
Шлюз портального доступа

Режим шлюза портального доступа используется для организации персонального доступа пользователей к опубликованным посредством **КриптоПро NGate** веб–ресурсам в соответствии с корпоративными политиками ИБ.

+7 (495) 995-48-20 ngate@cryptopro.ru @CryptoProAssistantBot

3 Point-to-Site TLS VPN

VPN-шлюз удаленного доступа

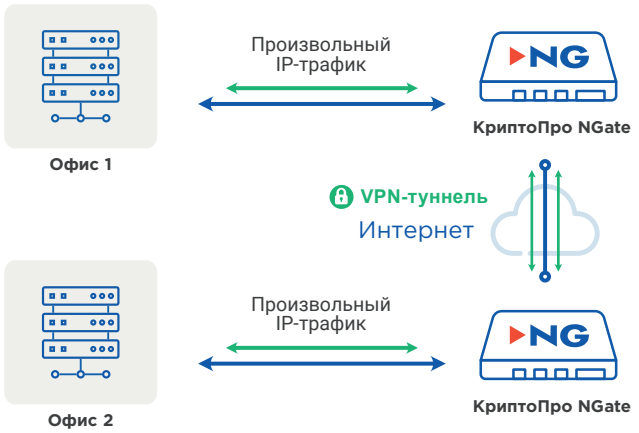


Режим VPN-шлюза удаленного доступа используется для подключения к произвольным ресурсам с помощью VPN–клиента, поддерживающего все популярные платформы и архитектуры. При этом разграничение доступа возможно на уровне подсетей, в том числе виртуальных (VLAN).

4 Site-to-Site IPsec VPN

VPN-шлюз доступа между площадками

Режим VPN-шлюза доступа между площадками используется для объединения нескольких территориально распределённых площадок (в том числе ЦОДов) в единую защищённую логическую сеть.



БЕЗОПАСНЫЙ ДОСТУП

Многофакторная аутентификация (по клиентским сертификатам, LDAP / AD, RADIUS, TOTP/HOTP) и гибкое разграничение прав доступа к ресурсам. Поддержка аппаратных ключевых носителей: Рутокен, eToken, JaCarta, ESMART и др. Поддержка ПАК **КриптоПро HSM** для хранения серверных ключей.

ОБЛАСТЬ ПРИМЕНЕНИЯ

Субъекты КИИ, государственные органы, операторы ПДн, финансовые и иные организации, которым необходимо обеспечить защиту передаваемой информации и удаленного доступа.

ОС и процессорные архитектуры, поддерживаемые VPN-клиентом

Windows 7 / 8 / 8.1 / 10 / 11

MacOS X 10.13 – 15

Linux (Astra, ALT, РЕД ОС, RHEL, CentOS, Debian, Ubuntu, ROSA и др.)

iOS

Android

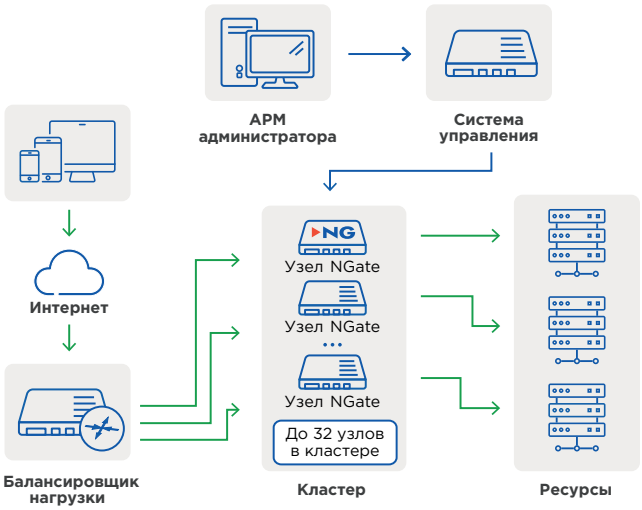
Аврора

Поддержка процессорных архитектур **x86**, **ARM**, **RISK-V** и **E2K** (Эльбрус).

Компоненты КриптоПро NGate сертифицированы ФСБ России по классам КС1, КС2 и КС3. Это позволяет использовать **КриптоПро NGate** в том числе для защиты ПДн (152-ФЗ) при передаче по незащищенным каналам связи, в том числе за пределами Российской Федерации.

НАГРУЗКА

Один узел шлюза **КриптоПро NGate** способен поддерживать до 45 000 соединений с обработкой информационных потоков до 20 Гбит/с в режиме TLS-шлюза. Кластер может содержать до 32 узлов.



КриптоПро NGate использует в своем составе сертифицированное ФСБ России СКЗИ **КриптоПро CSP** с российскими криптографическими алгоритмами:

ГОСТ Р 34.10-2012 (34.10-2018), ГОСТ Р 34.11-2012 (34.11-2018), ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018), ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018)