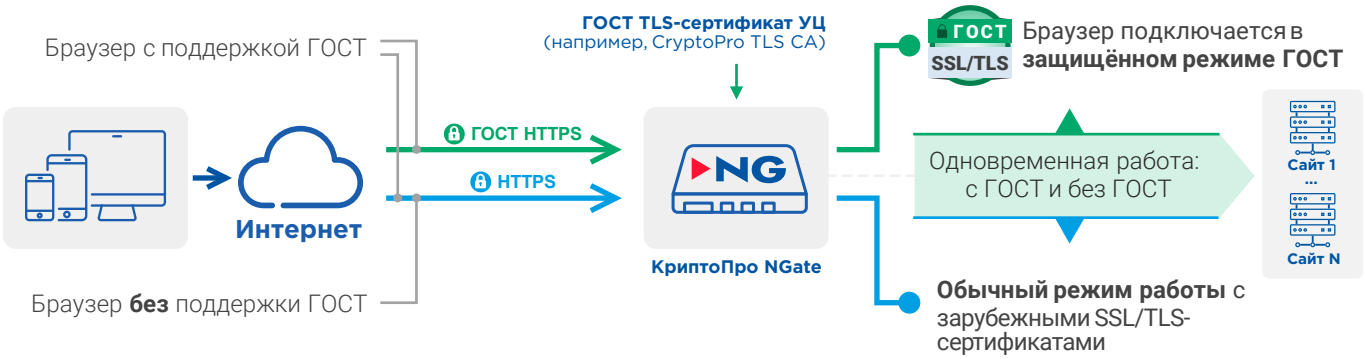
КРИПТОПРО NGate TLS-VPN

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

1. **WEB TLS**
   TLS-сервер доступа к веб-сайтам
2. **WEB Portal TLS**
   Сервер портального доступа
3. **Point-to-Site TLS VPN**
   VPN-сервер удаленного доступа
4. **Site-to-Site IPsec VPN**
   VPN-сервер доступа между площадками

1 WEB TLS

TLS-сервер доступа к веб-сайтам



Режим TLS-сервера используется для безопасного подключения к веб-сайтам и снятия нагрузки по обработке TLS-соединений с веб-серверов. В данном режиме NGate может использоваться для обеспечения доступа к госпорталам, сайтам организаций и ДБО и др., предоставляющих доступ пользователей через веб-браузер.

NGate обеспечивает одновременную поддержку TLS с ГОСТ и зарубежными криптоалгоритмами. Это позволяет реализовать плавный перевод защиты доступа к веб-сайтам на ГОСТ.

2 WEB Portal TLS

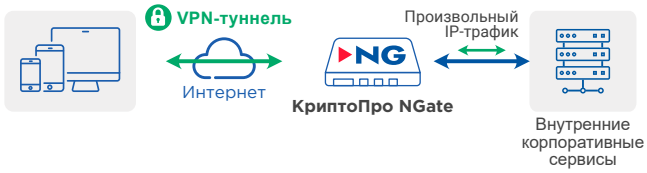
Сервер портального доступа

Режим сервера портального доступа используется для организации персонального доступа пользователей к опубликованным на портале **NGate** веб–ресурсам в соответствии с корпоративными политиками ИБ.

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

3 Point-to-Site TLS VPN

VPN-сервер удаленного доступа

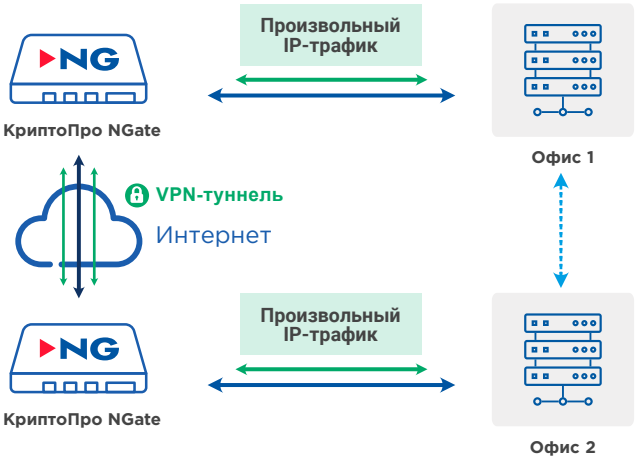


Режим VPN-сервера удаленного доступа используется для подключения к произвольным ресурсам с помощью VPN–клиента, поддерживающего все популярные платформы. При этом разграничение доступа возможно на уровне подсетей, в том числе виртуальных (VLAN).

4 Site-to-Site IPsec VPN

VPN-сервер доступа между площадками

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



БЕЗОПАСНЫЙ ДОСТУП

Многофакторная аутентификация (по сертификату, LDAP / AD, Radius) 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 – 13

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

iOS

Android

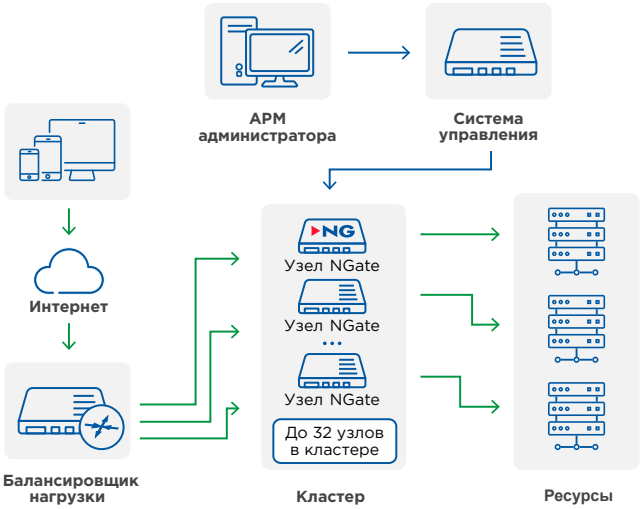
Аврора

Поддержка процессорных архитектур **x86**, **ARM** (в т.ч. Байкал) и **E2K** (Эльбрус).

Компоненты NGate сертифицированы ФСБ России по классам КС1, КС2 и КС3. Это позволяет использовать **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 **NGate** держит до 45 000 соединений с обработкой информационных потоков до 20 Гбит/с в режиме TLS-сервера. Кластер может содержать до 32 узлов.



КриптоПро NGate использует в своем составе сертифицированное ФСБ России СКЗИ **КриптоПро CSP** с российскими криптографическими алгоритмами:
ГОСТ 28147-89,
ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012,
ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012.