КриптоПро NGate – уникальный шлюз и VPN

Новый взгляд на удалённый доступ в компании

Рыночные тренды

КРИПТОПРО

Тенденции	Возможный ответ
Централизация всех видов доступа в крупных организациях	Необходимо высокомасштабируемое решение для всех пользователей с обеспечением различных видов аутентификации
Увеличение количества используемых мобильных устройств	Расширение списка поддерживаемых ОС, с которых может быть обеспечен безопасный доступ к ресурсам организаций
Необходимость непрерывного доступа с любых устройств и во всех возможных условиях	Обеспечение непрерывной работы сервисов
Увеличение числа высокотехнологичных атак с использованием различного вредоносного ПО	Система анализа безопасности подключаемых устройств
Постоянный рост числа сотрудников и партнёров, которым необходим удалённый доступ	Применение политик безопасности и разграничения доступа пользователей к ресурсам

Удалённый доступ — это проблема?

КРИПТОПРО

- Большое количество разных ОС и мобильных устройств
- Разнотипное подключение:
  - приложение – приложение
  - сетевой доступ
  - доступ браузером
- Неуправляемое устройство может быть захвачено
- Текущая технология аутентификации пользователя по сертификату сейчас явно недостаточна. Поскольку проверяется по сути правильность выдачи сертификата нужным УЦ. Администратор может определить только, кто подключен по факту на основе сертификата или пароля
- Предоставление нужного уровня доступа к ресурсам компании требует более гранулированной проверки пользователя
- Внутри туннелей трудно определить откуда идет соединение, когда одновременно подключено много пользователей
- Потенциальные проблемы и дыры в безопасности – слишком простые реализации с базовым функционалом по созданию туннеля
- Невозможность применять гранулированную политику безопасности к подключаемым клиентам или приложениям

Что хочет клиент?

КРИПТОПРО

- Надёжное и простое в управлении решение
- Мультиплатформенность клиентского решения, в особенности поддержка сертифицированных ОС
- Как можно более простое клиентское решение, не требующее управления со стороны клиента, но гибко управляемое из центра администратором
- Возможность для пользователя подключаться как через VPN-клиент, так и без применения клиента.
- Кластеризация и масштабирование
- Производительность
- Политика безопасности на основе данных пользователя, типа доступа и других признаков
- Сертификация по классу, позволяющему не задумываться, при применении в системах ГИС, КИИ, Персональных данных и других
- ТСО решения

Самое важное при выборе решения

КРИПТОПРО

- Тип доступа: портальный доступ, туннельный доступ, подключение конкретного приложения или SSL offload как частное решение по ГОСТ, или все сразу ?
- Необходимо обеспечивать защищенный режим доступа удаленного клиента без возможности для него подключения к каким либо другим ресурсам, кроме выделенных?
- Универсальное решение позволяющее осуществлять доступ не только со стационарного ПК, но и с мобильного устройства
- Разграничение доступа для отдельных пользователей, групп пользователей или другим признакам
- Производительность, кластеризация
- Защищенность реализации (а на чем основано решение, действительно обеспечивает безопасность?)
- Стоимость владения

Частные критерии портального решения

КРИПТОПРО

- Все решения могут обеспечивать прозрачную работу с защищаемыми ресурсами обеспечивая как строгую аутентификацию так и просто аутентификацию сервера?
- Какие поддерживает операционные системы?
- Аутентификация - сертификат - проверка правильности выпуска нужным УЦ или что то большее?
- Позволяет ли опубликовать любые ресурсы?
- Поддержка одновременно ГОСТ и не ГОСТ для плавного перехода во всех режимах?

Безопасность решения

КРИПТОПРО

- А на чем основано решение? (Heart bleed?)
- Требует ли клиент запуститься под правами администратора?
- Решены ли вопросы запрета маршрутизации разных сетей и адресов внутрь туннеля?
- Решена ли безопасность решения в целом ?
- Можно ли разграничивать доступ пользователей к приложениям?
- Решение просто ставится на обычную операционную систему или это специально подготовленный ПАК с решением вопросов безопасности?
- Проводились ли тесты безопасности?

Применимость решения к нуждам компании

КРИПТОПРО

- Что умеет шлюз - просто сделать туннель или веб доступ или что-то ещё?
- Поддержка энтерпрайз технологий (VLAN, маршрутизация)?
- Поддержка облачных инфраструктур (можно ли, например, поделить шлюз на много независимых сегментов?)
- Поддержка веб технологий (динамические, статические заголовки);
- Поддержка требуемых платформ (например, начальник не расстаётся с МАКбуком или Айпадом?)
- Можно ли строить отказоустойчивые решения в рамках ЦОДов или другой инфраструктуры компании ?

Представляем новое средство обеспечения удаленного доступа

КРИПТОПРО

КриптоПро NGate

Универсальный шлюз доступа NGate

КРИПТОПРО

Безопасность:

- Двухфакторная аутентификация
- Интеграция с любыми каталогами (AD, LDAP, Oracle и др.)
- Поддержка всех необходимых критптоалгоритмов (ГОСТ, другие)
- Концепция ***least privileges*** – только то, что разрешено

Универсальность:

- Соединения с помощью динамического клиента, статического клиента
- Соединения веб-браузером через портал
- Обеспечение подключений приложения к приложению

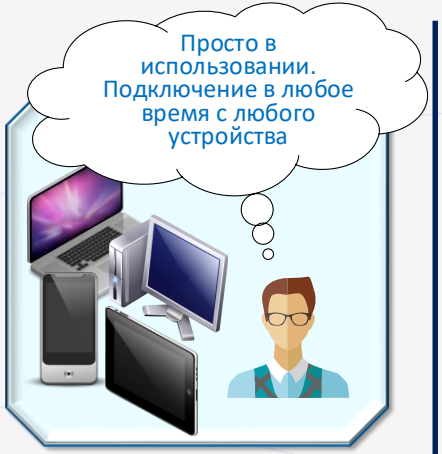
Производительность:

- Высокая скорость доступа к шлюзу (одна из самых высоких в своём классе)
- Высокая нагрузочная способность (как по скорости, так и по соединениям)
- Кластеризация и масштабируемость (много устройств в кластере)

Удобство:

- Не нужно думать о клиентской ОС (клиенты Windows, Linux, Mac и другие)
- Не нужно иметь несколько разных шлюзов под разные задачи – всё в одном!

Простое в использовании решение



Пользователь:

- Поддержка разных платформ
- Нет настроек на стороне клиента – все настройки автоматически импортируются из центра
- Двухфакторная аутентификация
- Разные политики безопасности для разных видов доступа
- Высокая скорость соединения
- Работа из движущегося транспорта без разрыва соединений

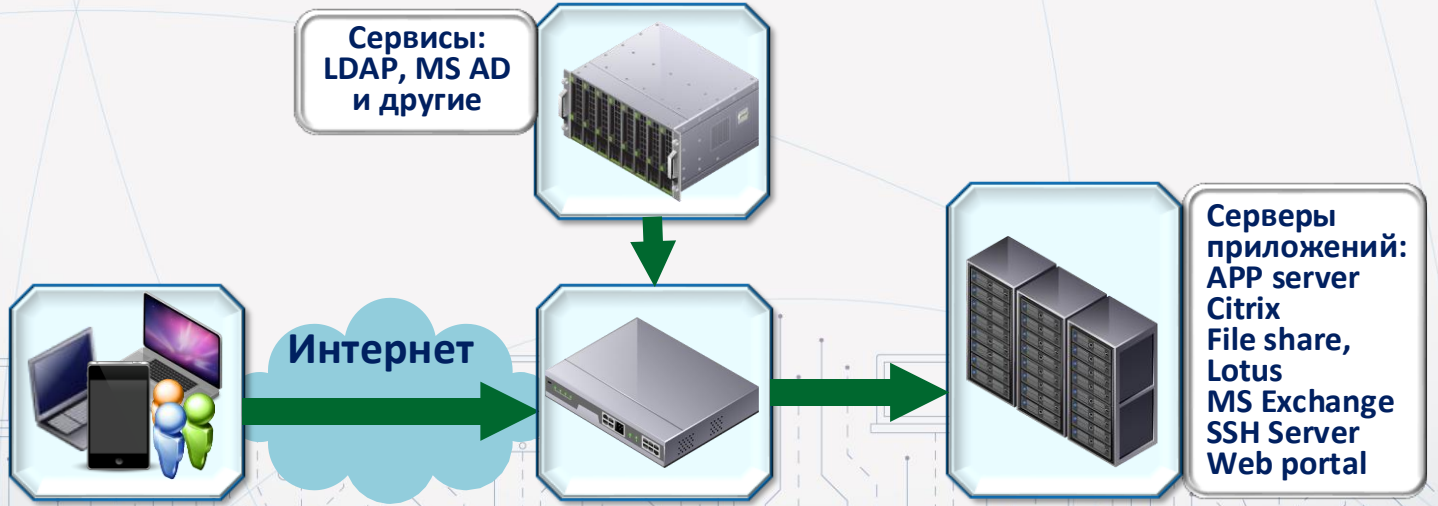
Администратор:

- Единое устройство для всех видов доступа!
- Высокая производительность
- Большое количество виртуальных безопасных порталов
- Масштабируемость: просто добавьте устройство!
- Возможность подключения через портал, статически клиентом (приложение – приложение), динамическим клиентом VPN без сложных настроек
- Интеграция с системами SIEM
- Интеграция с системами мониторинга по SNMP

Типичное применение шлюза доступа

КРИПТОПРО

- Обеспечение универсального, защищенного доступа пользователей к ресурсам информационных систем с использованием VPN (ГОСТ)
- Создание защищенных порталов доступа к различным ресурсам
- Обеспечение вынесения криптофункций высоконагруженных информационных систем в отдельный шлюз с обеспечением режима SSL Offload
- Обычно шлюз устанавливается в DMZ компании. К шлюзу открывается доступ только по HTTP и HTTPS
- Соединения проводятся исключительно через SSL туннель со строгой аутентификацией



Порталы доступа

КРИПТОПРО

Виртуальные безопасные порталы:

Создайте столько порталов сколько нужно для подключения разных групп пользователей или для динамического доступа к ресурсам с использованием VPN клиента

Разграничение доступа между группами пользователей надёжно обеспечивается не только правилами доступа и матрицей доступа, но и сертификатом, который может быть уникальным для каждого портала! Таким образом, не имея ключа к порталу, подключиться невозможно!

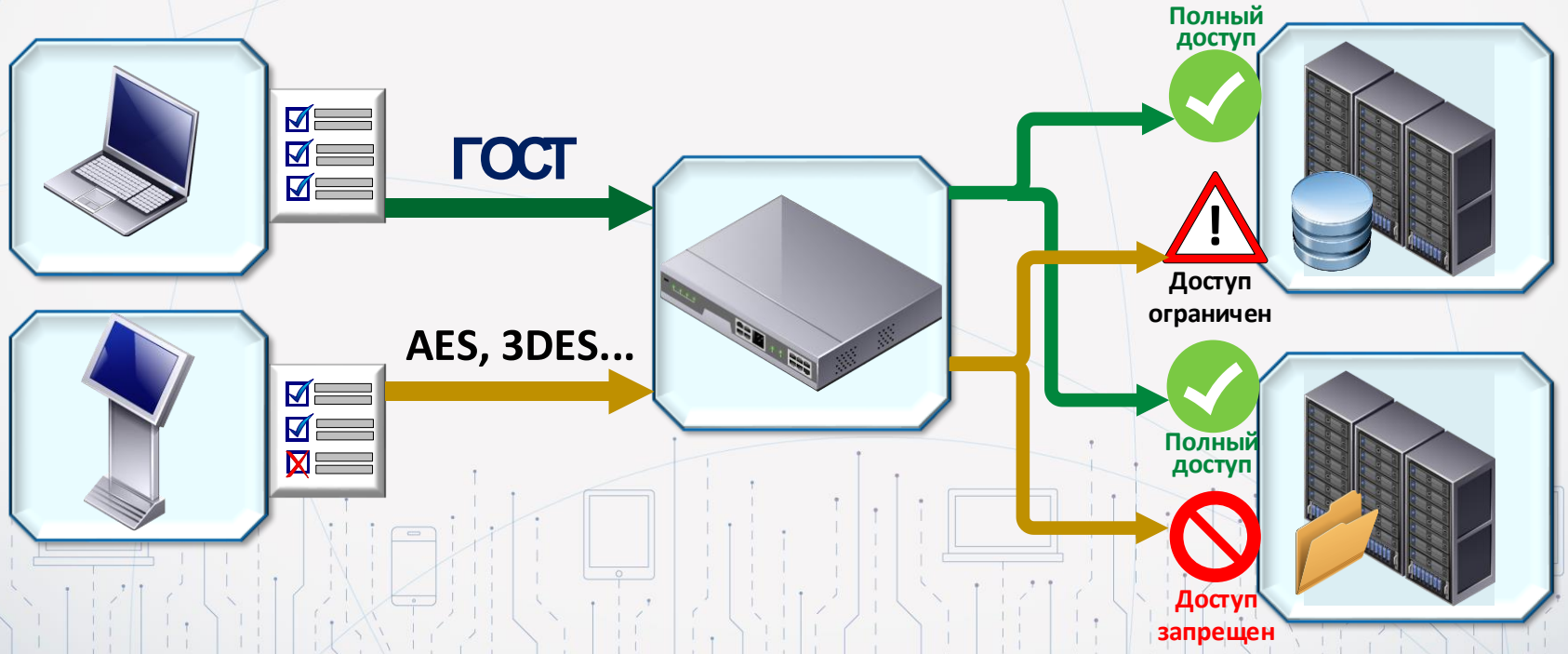
Кластеризация

- Не меняйте устройство шлюза, если растёт ваш бизнес – просто добавьте ещё!
- Управляйте кластером NGate, как единым устройством!

Обеспечение перехода на ГОСТ (импортозамещение)

КРИПТОПРО

- Возможность обеспечения плавного перехода к использованию Российских криптоалгоритмов
- Для разных типов подключения можно обеспечить разные типы доступа



Сертификация

КРИПТОПРО

Ведутся работы по сертификации различных исполнений как шлюза доступа по разным классам, так и клиента в разных операционных системах!

Сертификация ФСТЭК – прорабатывается сертификация по требованиям к Межсетевым экранам.

Шлюз NGate – возьми всё лучшее!

КРИПТОПРО

Производительность!

Высокая производительность как самого шлюза – в 2-3 раза выше основных аналогов, высокая скорость работы клиентского доступа, забудьте о лагах. До 45000 подключений на одно устройство!!!!

Безопасность!

- Обеспечение безопасности на каждом шаге, от аутентификации до доступа к ресурсам.
- Гибкие и строгие политики безопасности

Шлюз NGate

Простота!

Простой, интуитивно понятный VPN клиент, или просто веб доступ, в зависимости от ваших потребностей, все политики получаются из центра незаметно для пользователя.
Просто работайте с вашими приложениями!

Универсальность!

Нет необходимости выбора между удобством и применяемой технологией или операционной системой – все технологии доступа в одном устройстве. Подключайтесь с удобного вам ноутбука (Linux, Windows, MAC …)

Масштабируемость!

Простая кластеризация, добавьте в кластер любые устройства и увеличьте мощность работы вашего шлюза. Создайте столько порталов доступа сколько вам нужно

Соответствие требованиям!

Сертификация устройств по самым жестким стандартам и критериям, используйте решение в любых системах с любыми требованиями по сертификации

Чем отличается от других решений удалённого доступа с поддержкой ГОСТ?

КРИПТОПРО

- Целостное универсальное решение – всё в одном. Не нужно отдельно ставить Портал с SSL доступом и отдельно VPN
- Работа в разных режимах, в том числе разные виды туннелей и web-браузер (в том числе поддерживается Sputnik)
- Масштабируемость до любых размеров!!!
- Нечувствительно к NAT (не надо это настраивать, как в других классических решениях)
- Работа на разных платформах (Linux, Mac, Windows, IOS, Android, Sailfish)
- Использует общие всегда открытые порты – нет проблем с МЭ
- Не зависит от типа сети
- Просто в установке и распространении. Интуитивно понятно для пользователя
- Высокая производительность

9 причин выбрать именно NGate

КРИПТОПРО

1. Высокий уровень безопасности: решение вопросов безопасности как на клиентском месте, так и на шлюзе по умолчанию
2. Наличие простой и эффективной системы централизованного управления
3. Снижение расходов на управление политиками безопасности и на инфраструктуру удаленного доступа
4. Сертифицированность – не надо думать как выполнить стандарты и требования регуляторов
5. Высокая отказоустойчивость (ДО 32 устройств в кластере)
6. Одна из самых высокоскоростных платформ – реальная производительность до 10 – 15 ГБ/с на устройство и почти линейное повышение производительности в кластере
7. Полноценная защита в виртуальной среде
8. Простое освоение пользователями системы как портального доступа, так и клиентского доступа
9. Один из самых низких TCO среди подобных систем

Спасибо за внимание!