

# Переход на удаленную работу. Некоторые аспекты



SafeConnect®



SafeInspect  
СИСТЕМА КОНТРОЛЯ



# Удаленная работа до пандемии .....

Сотрудники преимущественно в офисе

Удаленный доступ предоставляется в основном руководству и тем кто в командировках

Для удаленного доступа выдается корпоративный ноутбук, настроенный в соответствии с политиками безопасности

Удаленный доступ = IPSec VPN (сейчас чаще используется в качестве транспорта TLS)

По сути предоставляется туннельный доступ : доступ сетевого устройства к сети предприятия.



# Пандемия .....

Почти **ВСЕХ** сотрудников надо обеспечить удаленным доступом

Служба IT также старается работать из дома..... (по возможности)

Ноутбуков на всех сотрудников нет, как и возможности поддерживать необходимый уровень безопасности таких рабочих мест. Необходимо сделать доступ с домашних устройств

Необходимо с одной стороны дать доступ к компьютерам на рабочих местах и с другой стороны к сервисам внутри компании ...

К инфраструктуре также будет расширен доступ разных организаций, обслуживающих IT инфраструктуру (вендоры, интеграторы, консультанты, работающие по контракту и пр.).



# Старые и новые проблемы

В отдельные промежутки времени, большинство сотрудников подключаются через ВПН

Сложнее делать разграничение доступа к ресурсам, разным группам пользователей (сегментирование??)

Проблемы обеспечения безопасности домашних компьютеров

Домашние компьютеры могут быть устаревшими (старые версии решительно всего дыры в безопасности и прочее.... )

Сложности с утечкой данных на домашних компьютерах....



# Новые проблемы

*Когда все на удаленке и возникают проблемы (остановка работы), перед службой IT или безопасностью встают вопросы:*

Кто сделал эти действия (кто это вообще?)

Зачем он вообще подключался к ресурсам и что то там делал?

Кто и на каком основании дал доступ?

Что вообще он должен был делать, когда ему разрешили доступ?

Что делалось? Что привело к такому результату?



# Проблемы доступа

Использование VPN доступа не снимает проблемы доступа к конкретным ресурсам для выполнения конкретных задач  
VPN в целом решает задачу доступа для авторизованных пользователей

Авторизованный пользователь имеет слабую связь с теми ресурсами, к которым предоставляется доступ. По сути, это доступ к локальной сети или части локальной сети.



# Что нужно?

Организация быстрого доступа к рабочим компьютерам из дома

Разграничение доступа между пользователями (доступ только в свой компьютер)

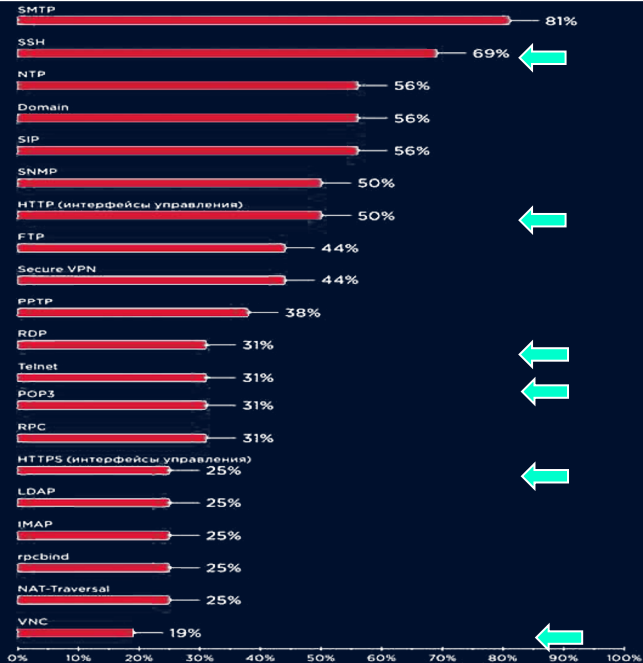
Соблюдение политик безопасности (из vpn можно так же хорошо получать распространение вирусов, как и в самой компании)

Понимание кому какой доступ выдали и для чего

Простые действия со стороны удаленного компьютера

# Что включено в периметр организации

- SSH - 69%
- RDP - 31%
- HTTP (управление) - 50% !!!
- Telnet - 31% !!!
- HTTPS (управление) - 25%
- VNC - 19%





# Количество уязвимостей в зависимости от сервисов

Web приложения и службы удаленного доступа лидируют!!!  
При этом многие организации очень быстро выставили, например, свои сервера RDP в интернет для обеспечения удаленного доступа....





# SafeConnect - простой защищенный доступ

Простой и защищённый доступ к приложениям, используемым в компании

Доступ к компьютерам и другим устройствам с использованием разных протоколов

Обеспечение безопасности подключения пользователей по принципу приложение – приложение

Полноценная работа с документами и данными

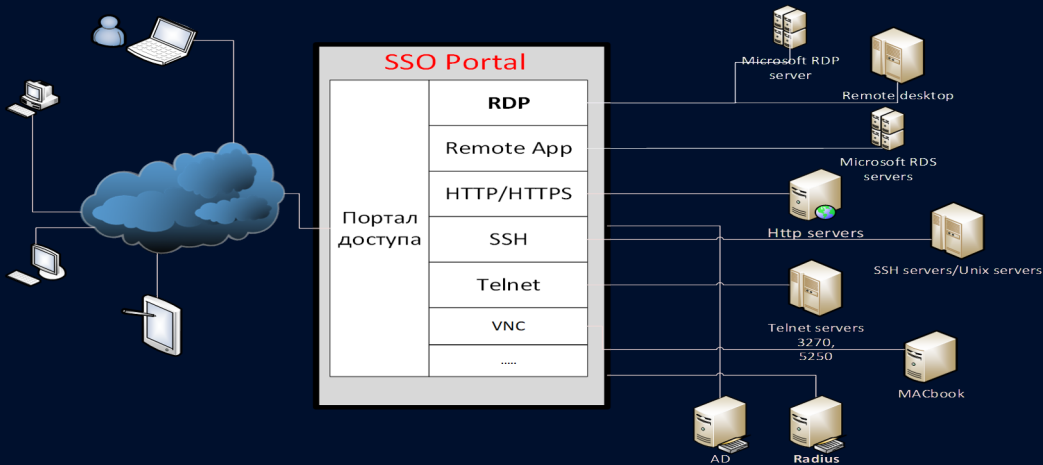
Без клиентского ПО и каких-либо серьезных настроек безопасности

Мультифакторная аутентификация

Реализация SSO



# SafeConnect - простой, защищенный доступ



## Доступ к ресурсам на основе заданий

Снимает много проблем у администратора: для любого подключения всегда можно понять – что за подключение, для чего оно выдано, когда закончится

У пользователя подключения появляются и исчезают автоматически, в зависимости от выданного доступа

В процессе работы, в рамках задания можно запросить новый доступ, или изменить параметры текущего доступа. Все запросы регистрируются

Доступ может быть один для группы пользователей, то есть задание будет одно, а доступы автоматически появятся у всей группы пользователей, которым он был предназначен.

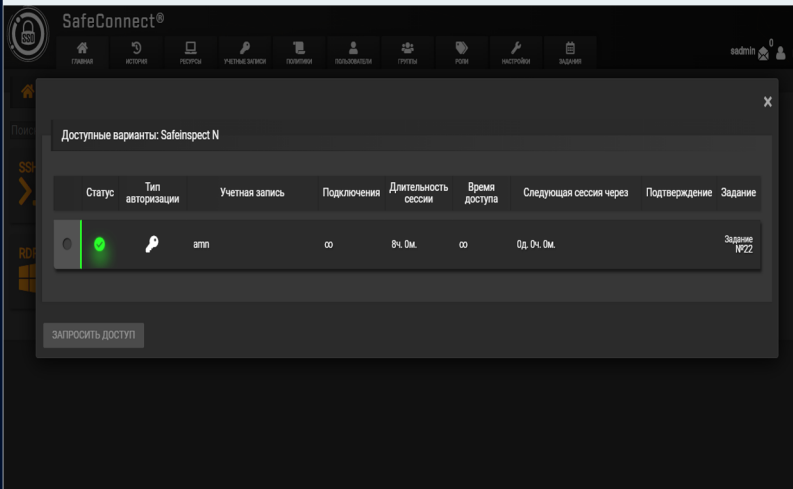
The screenshot shows the SafeConnect web interface. At the top, there is a navigation bar with the SafeConnect logo and three menu items: Главная (Home), История (History), and Задачи (Tasks). The main content area displays a request for access to a resource, titled "Задание №27" (Task #27) and "нгейт через инспект" (ngate through inspect). Below the title, it says "то же самое только через инспект" (the same thing only through inspect) and shows the user "admin" and the time "8/20/2020, 1:35:52 PM". There is a button "Добавить пользователей\*" (Add users\*) and a button "ДОБАВИТЬ ПОЛЬЗОВАТЕЛЕЙ" (ADD USERS). Below this, it shows "Пользователи:" (Users:) with "Mike" and "\_newinforec.ru". There is also a field for "Номер задания во внешней системе" (Task number in external system). A table lists resources with columns: Название ресурса (Resource name), Тип авторизации (Authorization type), Учетные записи (Accounts), Подключения (Connections), Длительность (Duration), Время доступа (Access time), Расписание (Schedule), and Подтверждение (Confirmation). The table has one row: "ngate SSH", "Сопоставление" (Mapping), "Хrtngate", "0", "Вч. Ом.", and "Разрешено" (Allowed). Below the table is a "Комментарий" (Comment) field. At the bottom, there is a button "Запросить сопоставление\*" (Request mapping\*) and a button "ЗАПРОСИТЬ СОПОСТАВЛЕНИЕ" (REQUEST MAPPING).



## Простой интерфейс для пользователя ресурсов

На экране он видит иконки доступа к ресурсам. Они динамически появляются или исчезают в зависимости от решаемых задач. Как только задача будет решена и задача закрыта, ненужные иконки доступа исчезнут с экрана

Когда пользователь нажимает на иконку доступа к ресурсу, он увидит всю информацию по этому соединению. Если непонятно, что делать по этому соединению, можно кликнуть на номер Задания и прочитать его.



# Гибкая система назначения прав пользователей

Возможность гибкого назначения прав пользователей и администраторов

Ролевая модель

Мандатный принцип доступа (уровни безопасности ресурса)

Создание ролей в соответствии с штатной структурой подразделений компании.

The screenshot displays the SafeConnect user management interface. At the top, the 'Роли' (Roles) section is active, with a 'ДОБАВИТЬ' (ADD) button. A modal window titled 'Добавление роли' (Add role) is open, showing a form for creating a new role. The 'Название' (Name) field contains 'Название роли' and has a warning icon. The 'Описание' (Description) field is empty. Below the form, a list of permissions is shown, including 'Просмотр ресурсов', 'Редактирование ресурсов', 'Удаление ресурсов', 'Просмотр учётных записей', 'Редактирование учётных записей', 'Удаление учётных записей', 'Просмотр пользовательских ресурсов', 'Редактирование пользовательских ресурсов', 'Удаление пользовательских ресурсов', 'Просмотр пользователей', 'Редактирование пользователей', 'Удаление пользователей', 'Просмотр ролей', 'Редактирование ролей', 'Удаление ролей', 'Права на подтверждение сессий с УЗ, требующими подтверждения', 'Разрешить использование ресурсов с отметкой FG 152', 'Разрешить использование ресурсов с отметкой GDPR', 'Разрешить доступ на критические ресурсы', and 'Просмотр групп'. The interface also shows a list of existing roles on the left and a log of role creation actions on the right.



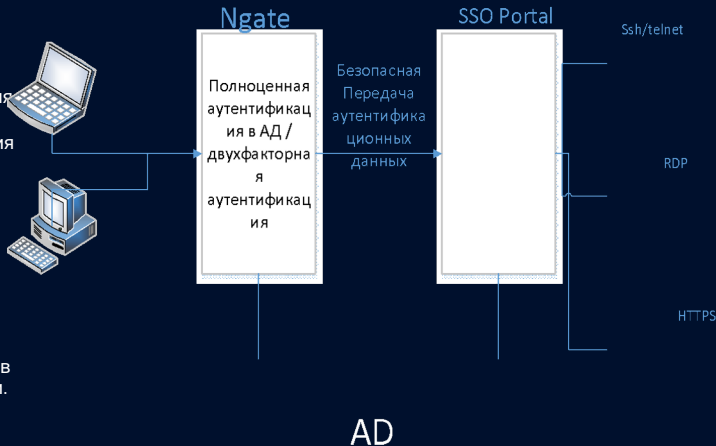


# Интеграция с разными производителями

При необходимости использования сертифицированных средств шифрования возможна интеграция с Cryptopro Ngate

В этом случае, пользователи подключаются по ГОСТ к Ngate.

Далее, путем автоматической авторизации на портале для пользователя предоставляется интерфейс доступа уже в портале в соответствии с его полномочиями.

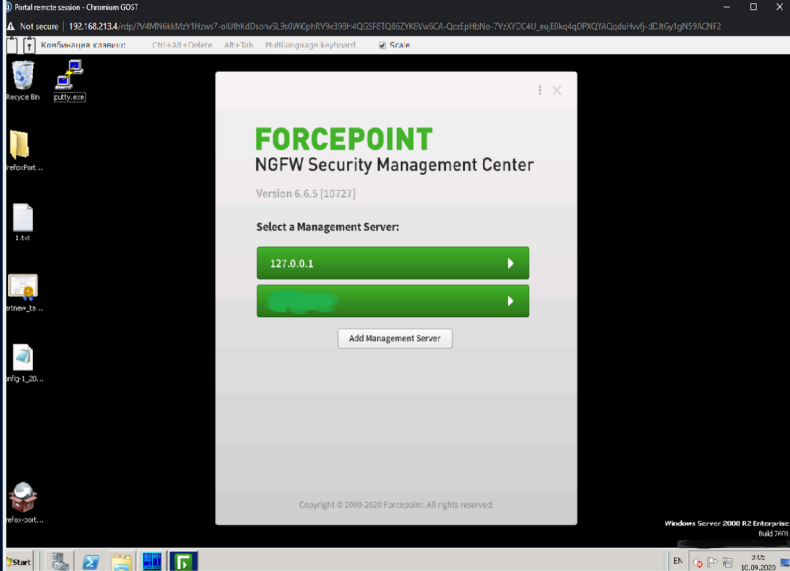


# Подключение к удаленной системе

Подключение к удаленной системе происходит автоматически после выбора варианта доступа

Система позволяет комфортно работать с удаленным рабочим столом с любого устройства

Решены также и вопросы работы буфера обмена прямо через браузер





# Подключение к SafeConnect

Позволяет работать комфортно и с мобильных устройств.

The screenshot shows a mobile device interface with a remote desktop connection. The desktop background is a Linux desktop with various application icons. A web browser window displays the Forcepoint NGFW Security Management Center interface, and a terminal window shows the contents of the /etc directory.

**Forcepoint NGFW Security Management Center**  
Version 6.6.5 [10727]  
Select a Management Server:

File	Size	Modify time	File
./			./
./cache	4096	Aug 29 2019	./cache
./config	4096	Aug 29 2019	./config
./local	4096	Aug 29 2019	./local
./nano	4096	Mar 11 2020	./nano
./ssh	4096	Mar 6 2020	./ssh
./bash_history	15100	Sep 10 11:12	./bash_history
./bashrc	570	Jan 31 2010	./bashrc
./profile	148	Aug 17 2015	./profile
ngate-update-complete-1.0-1-20200327.tar	3101608	Apr 1 01:53	ngate-update-complete-1.0-1-20200327.tar





## Усиление безопасности

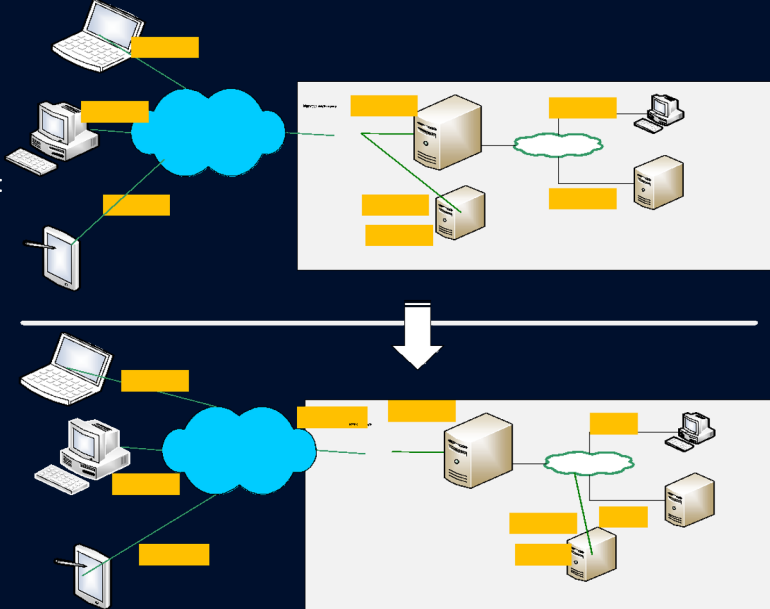
После внедрения SafeConnect:

Все подключения строго по HTTPS со строгой аутентификацией

Возможность использования 2 и даже 3 факторов при аутентификации

Внутри остается привычная инфраструктура

Не нужны дополнительные Jump сервера





# Действенный контроль

Простой доступ пользователей с использованием браузера по протоколу TLS

Все необходимые действия по запросу управлению доступом и др. осуществляется автоматически и полностью протоколируются

Полноценное маскирование названий аккаунтов и данных по аутентификации, они могут быть полностью недоступны для пользователя. Он имеет только доступ к своей учетной записи доступа к portalу

Полноценная поддержка заявленных протоколов (например, для RDP поддерживается сору- past текста и данных, без использования общих дисков!)

Доступ на основе заданий, позволяющий точно понимать когда, кто, какие действия сделал и в соответствии с каким заданием



# Эффективная стоимость владения

**РАЗНЫЕ ВАРИАНТЫ ПРОДУКТА:** может быть установлен как Virtual Appliance (в разных виртуальных средах), а также на «железо» (сервера)

**ВЫСОКАЯ МАСШТАБИРУЕМОСТЬ:** поддерживается горизонтальная кластеризация

**ПРОСТОТА ПРИМЕНЕНИЯ:** Нет необходимости в тренингах пользователей или изменении бизнес-процессов

**БЕЗ АГЕНТОВ:** Нет необходимости в инсталляции дополнительного ПО или агентов на серверах

**ПРОСТАЯ ИНТЕГРАЦИЯ:** Легко интегрируется как в инфраструктуру безопасности (VPN, DLP, PAM), так и в сетевую инфраструктуру (поддержка Vlan).



# СПАСИБО ЗА ВНИМАНИЕ!

ООО «Новые технологии безопасности»  
Москва, ул. Бутырский вал 68/70  
+7 (499) 647 4872

[www.newinfosec.ru](http://www.newinfosec.ru)