

Сервер многофакторной аутентификации ViPNet



Арина Эм

Ведущий менеджер продуктов

Что такое многофакторная аутентификация?

Многофакторная аутентификация (MFA) – метод защиты учётных записей, при котором требуется **два или более** независимых фактора для подтверждения личности

MFA усложняет несанкционированный доступ к аккаунту



Компоненты для работы многофакторной аутентификации

Клиентское устройство с ViPNet Client 5

Сервер многофакторной аутентификации ViPNet

Radius-сервер

Каталог пользователей

Мобильное устройство

Клиентское устройство



компьютер/планшет/телефон,
которому нужен доступ к защищенным ресурсам



На клиентском устройстве должно быть



VIPNet Client 5 и ключи



Связь с узлом сервера МФА (Client Auth Server)



Учетная запись пользователя
в Пользовательском каталоге

Сервер многофакторной аутентификации ViPNet

Сервер МФА

серверное приложение, которое работает как шлюз между ViPNet Client и сторонней системой аутентификации

Watchdog

Для отслеживания состояния сервера аутентификации

Актуальная версия сервера:
2.1

Поддерживаемые ОС

- Astra Linux 1.7, 1.8
- Ubuntu 22.04 LTS, 24.04 LTS
- РЕД ОС 7.3, 8
- Альт СП 10

Обязательные настройки сервера МФА

- ViPNet Client (Имя узла: Client Auth Server)
- Порт сервера (по умолчанию 8070)
- Адрес и порт radius-сервера
- Секретная фраза

Radius - сервер

Radius-сервер – это приложение, работающее с протоколом radius (RFC 2865)

✓ Осуществляет проверку валидности пользовательских учетных записей

🔗 В разных реализациях radius-сервер либо сам подключается к каталогу пользователей, либо опосредованно, через другие сервисы вендора МФА

Настройки параметров подключения к серверу МФА

- IP-адрес и порт сервера МФА
- Секретная фраза (равна секретной фразе в настройках сервера МФА)

Поддерживаемые Radius-серверы



MULTIFACTOR

Multifactor

AVANPOST

Avanpost FAM



Индид
Indeed AM

Контур ID

Контур ID



Аладдин
Аладдин JAS

freeRADIUS



Windows
Server

Каталог пользователей



Доступность варианта каталога пользователей зависит от реализации его поддержки вендором.



Некоторые позволяют подключить несколько каталогов, настроить дополнительные фильтры пользователей, указать особые группы пользователей (например, группа с отключенным вторым фактором), отслеживать срок действия пароля и другие параметры.



Мобильное устройство

Варианты вторых факторов



Push-уведомление



OTP



SMS-код

Схема работы в защищенной сети

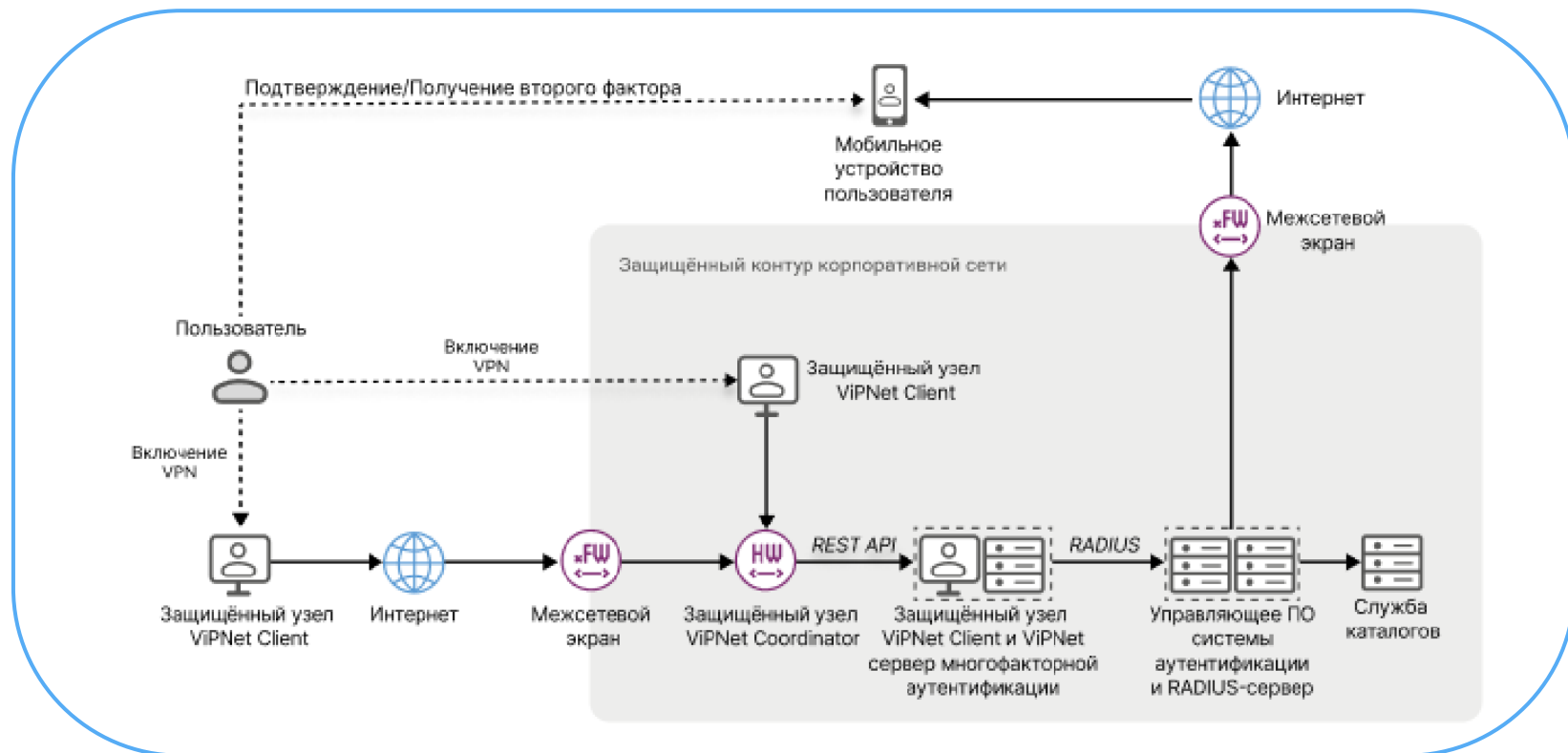
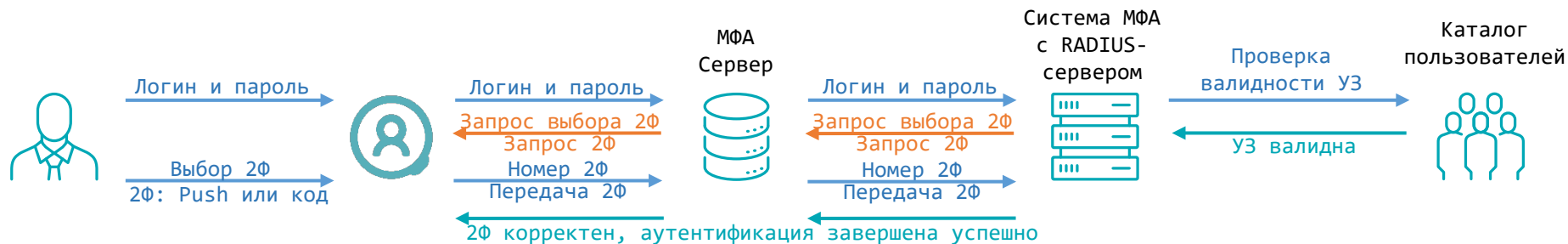


Схема взаимодействия компонентов



Демонстрация

САНКТ
ПЕТЕРБУРГ

инфотекс
ТЕХНОДЕСТ

инфотекс
Академия



AMPIRE

TELEOFIS

КОМФОРТЕЛ
оператор связи бизнес-класса

RVTOKEN
АКТИВ

TS Solution

AXOFT

Подписывайтесь
на наши соцсети

