Управление доступом и централизованной аутентификацией пользователей

на основе решения FortiAuthenticator

Юрий Захаров
Системный инженер

cis_se@fortinet.com

11 августа 2020

О чем пойдет речь…

- ✓ Обзор функциональных возможностей FortiAuthenticator
- ✓ Лицензирование и отказоустойчивость системы
- ✓ Методы FSSO
- ✓ SSO Mobility Agent (SSOMA)
- ✓ Сценарии двухфакторной аутентификации на базе sms, email или мобильного токена
- ✓ Пример настройки SSL-VPN с двухфакторной аутентификацией на основе FortiToken Mobile с применением Push Notification

FortiAuthenticator

Обзор функциональных возможностей

Сегодня сеть не имеет границ

Установление личности - краеугольный камень эффективной политики безопасности

Управление идентификацией и доступом:
Дисциплина безопасности, которая позволяет нужным людям получать доступ к нужным ресурсам в нужное время и по правильным причинам.

FORTINET

Неправильное использование учетных данных и привилегий может стать причиной взлома

Слабая аутентификация и неправильное управление доступом делают сеть уязвимой

Fortinet Security Fabric

Комплексная

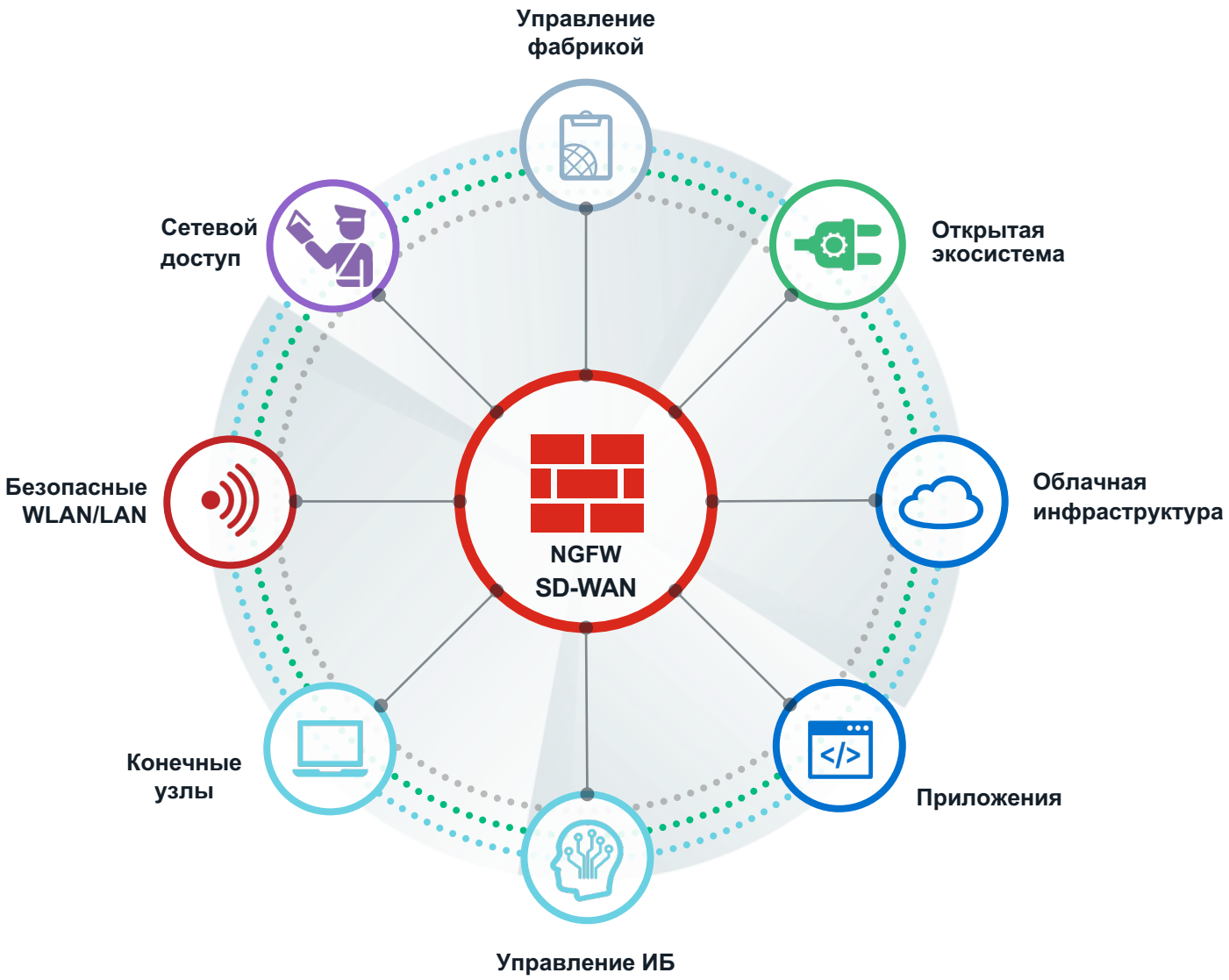
Обеспечение полной видимости поверхности цифровой атаки для лучшего управления рисками ИБ

Интегрированная

Уменьшение сложности сопровождения множества разнородных продуктов

Автоматизированная

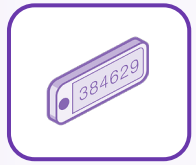
Увеличение скорости управления и отклика



Безопасный доступ для пользователей

Решение Fortinet по аутентификации и управлению доступом простое и изначально интегрировано с Security Fabric

FortiAuthenticator



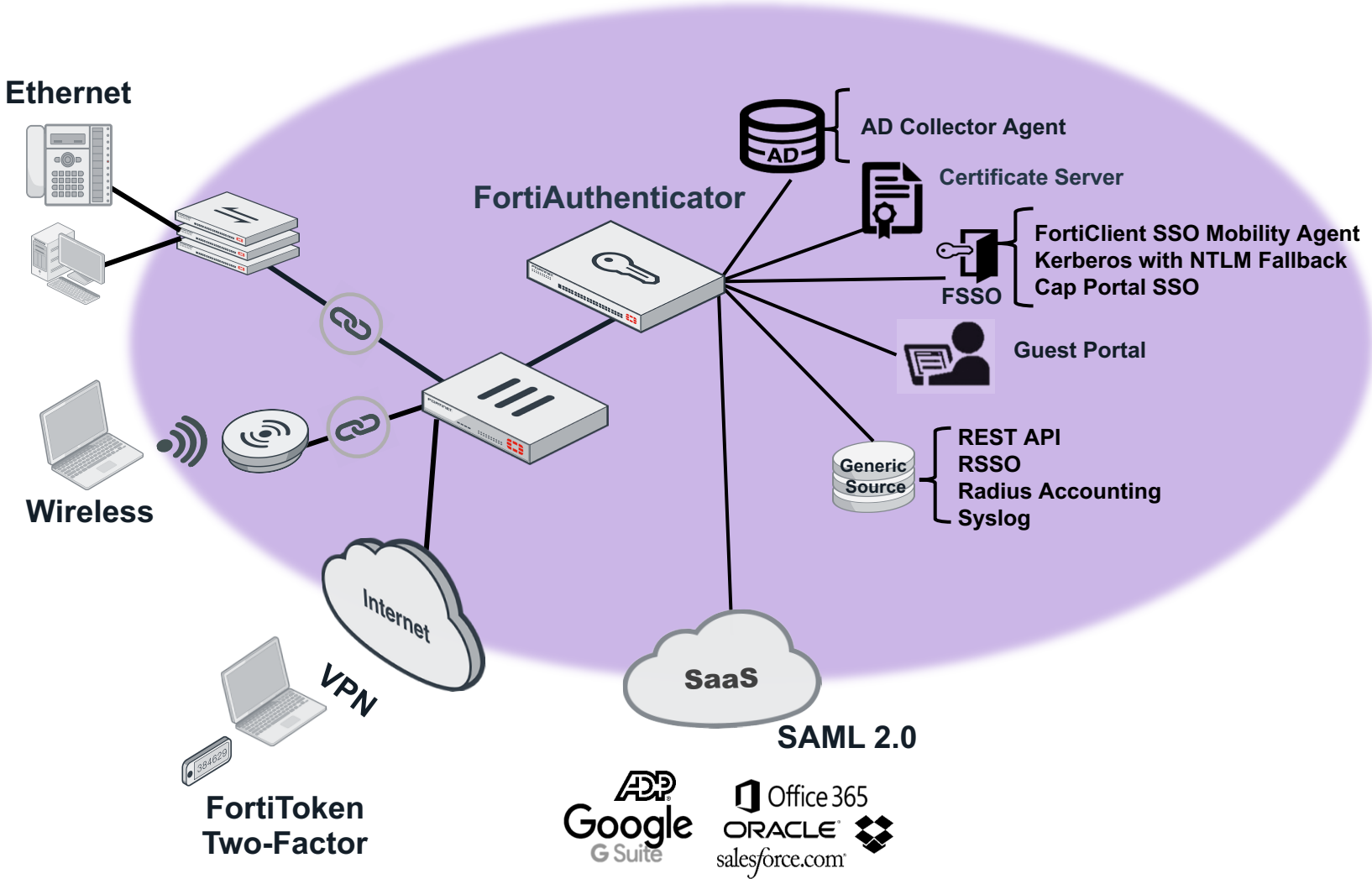
FortiTokens

- Контроль прав доступа для каждого пользователя
- Многофакторная аутентификация
- Удобство в повседневной работе (SSO)

Identity Access & Management

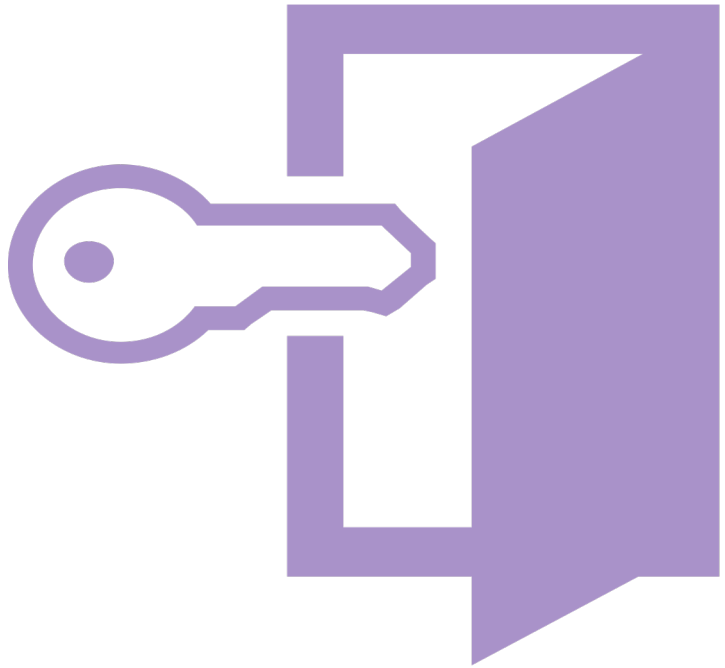
Управление идентификацией и доступом от Fortinet

- **Аутентификация и авторизация**
  – Доступ на основе ролей
- **Fortinet Single Sign On**
- **Single Sign On via SAML**
- **Двух факторная аутентификация**
- **Управление сертификатами**
- **Управления гостевым доступом**



Дополнительные преимущества

- Интеграция с Fortinet Security Fabric
- Удобство в повседневной работе благодаря технологии Fortinet Single Sign-On без ущерба безопасности
- Поддержка 2FA
- Различные варианты исполнения: HW, VM, Cloud (Token)
- Удобный инструмент управления гостевым доступом



FortiAuthenticator

Лицензирование и модельный ряд

Модельный ряд FortiAuthenticator

FortiAuthenticator 200E

Небольшие организации

- Support up to 500 users
- HDD – 1 x 1TB
- 4 x 10/100/1000 RJ45 ports
- Rack Mountable, 1U
- Single AC PSU

FortiAuthenticator 400E

Средние организации

- Support up to 2,000 users
- HDD – 2 x 1TB
- 4 x 10/100/1000 RJ45 ports
- Rack Mountable, 1U
- Single AC PSU

FortiAuthenticator 1000D

Крупные организации

- Support up to 10,000 users
- 2 X 2TB SAS storage.
- 4 x 10/100/1000 RJ45 ports
- 2 x SFP
- Rack Mountable, 2U
- Dual AC PSU

FortiAuthenticator 2000E

FortiAuthenticator 2000E

Крупные организации / провайдер услуг

- Supports up to 20,000 Users
- 2 X 2TB SAS storage.
- 4 x 10/100/1000 RJ45 ports
- 2 x GE SFP

FortiAuthenticator 3000E

FortiAuthenticator 3000E

Провайдер услуг

- Supports up to 40,000 Users
- 2 X 2TB SAS storage
- 4 x 10/100/1000 RJ45 ports
- 2 x GE SFP

FortiAuthenticator VM

Компании любого масштаба

- From 100 to 1M+ users
- Unlimited CPU
- Unlimited RAM

***Поддержка стекирования лицензий для FAC-VM**

FORTINET

Лицензирование FAC (1)

- Лицензируется по числу пользователей (User license)
- Для сценария FSSO only также необходимы User license
- HW модель предварительно пролицензирована
- VM модель: базовая VM-Base + дополнительные наборы по 100, 1К, 10К and 100К пользователей (лицензии для VM стекируются)
- Каждый набор User upgrade licenses открывает дополнительные квоты на функции FAC: Total Users (Local + Remote), FortiTokens, RADIUS Clients (NAS Devices), User Groups, CA Certificates, User Certificates и др.)

Дополнительная информация по квотам на функции для HW моделей и для VM в datasheet и (более подробно) в Release Notes в разделах *Maximum values for hardware appliances* и *Maximum values for VM*

Лицензирование FAC (2)

- Для HA одинаково лицензированы должны быть обе ноды
- SMS лицензируются отдельно (SMS-LIC-100), в том случае если они от Fortinet
- SMS интеграция со сторонним SMS Gateway не требует лицензии
- Single Sign-On Mobility Agent (SSOMA) лицензируется (FCC-FACXX-LIC)
- Лицензии на токены FortiToken Mobile переиспользуются в кластере (требуется 1 лицензия на две ноды)
- Windows Domain Two Factor Authentication Agent не лицензируется

FortiAuthenticator

Сценарии высокой доступности (HA)

Высокая доступность FortiAuthenticator

- Сценарий HA:
  - Active/Passive – L2
  - Active/Active – L3 Geo-Location HA

- HA Роли:
  - Cluster Members (A/P)
  - Standalone Master (A/A)
  - Load Balancing Slaves (A/A)

Высокая доступность FortiAuthenticator

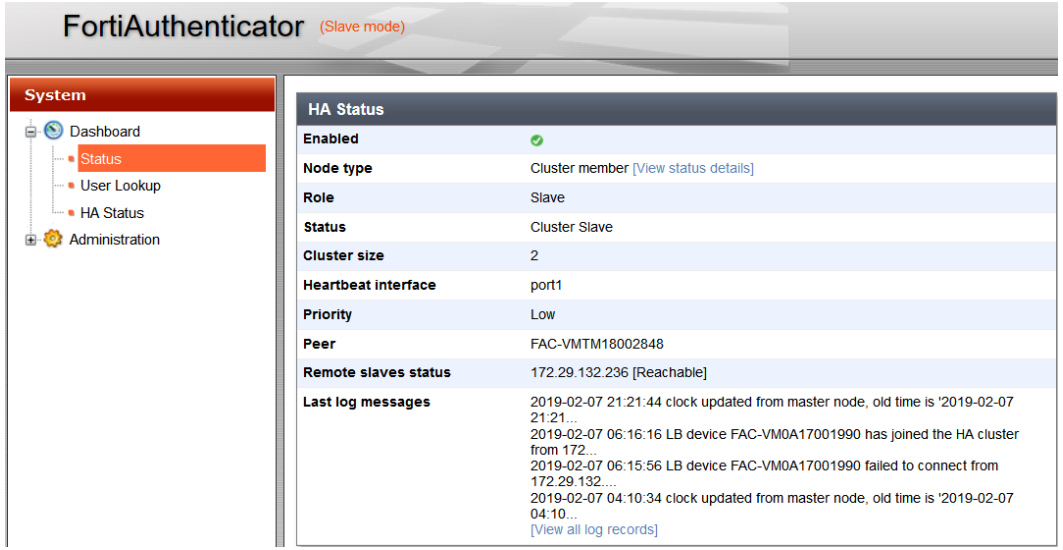
- Требования к HA:
  - Active/Passive (L2)
    - Платформы – одинаковые
    - ПО – одной версии
    - Лицензии
      - User Licenses - одинаковые
      - Token License – одна на кластер
  - Active/Active (L3)
    - Платформы – могут отличаться
    - ПО – одной версии
    - Лицензии
      - User Licenses – Могут отличаться (зависит от сценарии внедрения)
      - Token License – одна на кластер

Сценарии HA

Cluster Member (Active-Passive)

HA Cluster Member (Active-Passive)

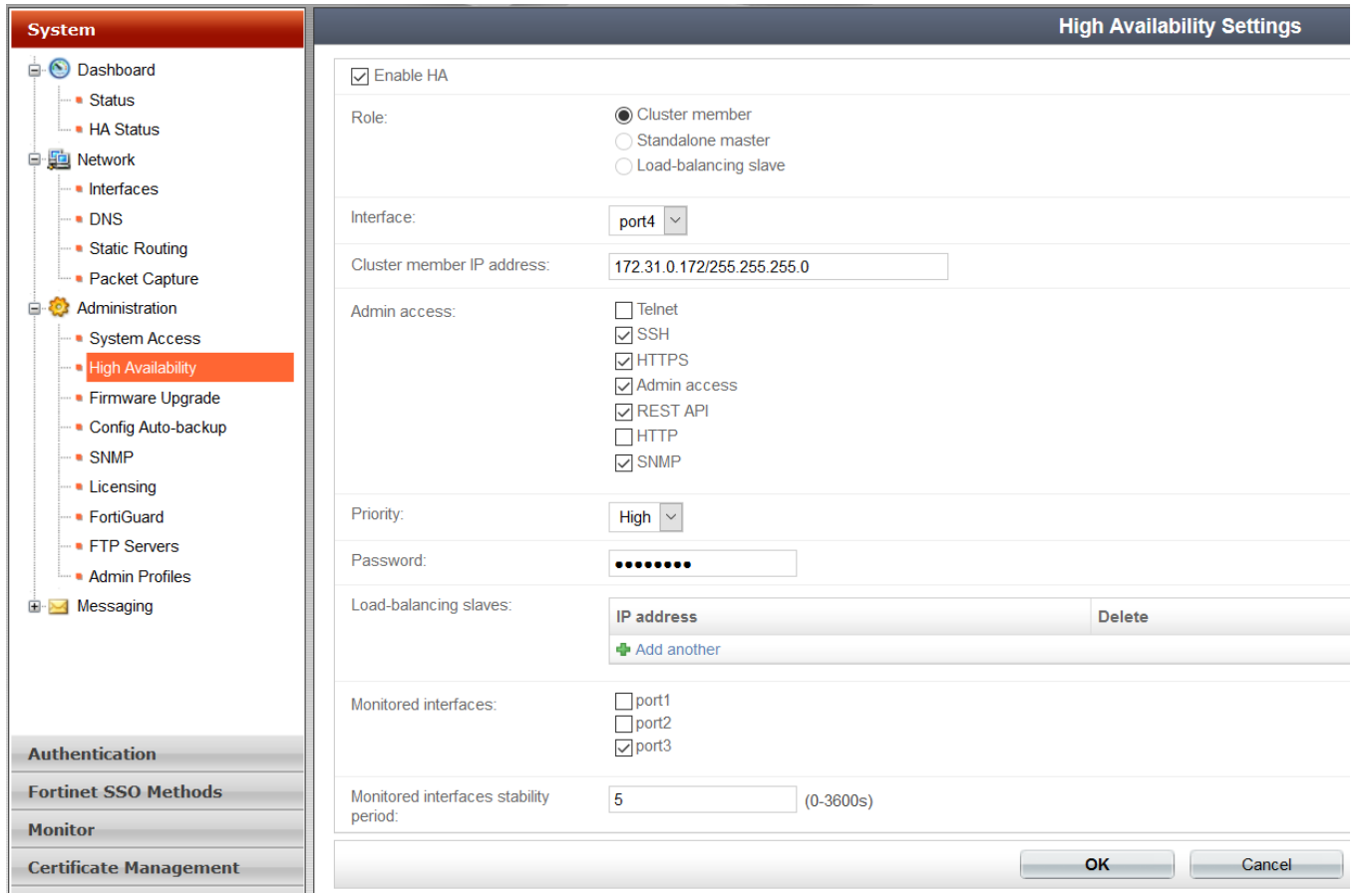
- Roles – Cluster Member
  - Active unit – «живой»
  - Passive unit – «в горячем резерве»



- Взаимодействие участников кластера
  - Passive unit следит за Active через HA интерфейс (L2)
  - Heartbeat traffic (HA Interface)
    - Sent to 169.254.0.63, UDP port 720 (src/dst) to dst broadcast MAC (ff:ff:ff:ff:ff:ff)
    - IP 169.254.0.1/26 (high-priority) and 169.254.0.2 (low-priority)
    - UDP Server 169.254.0.63
    - Every second
  - Синхронизация конфигурации (HA Interface)
    - IPSec AES encrypted
    - Every 2 seconds
  - PostgreSQL (HA interface)
    - Slave to master
    - Message based protocol – dst TCP/5432

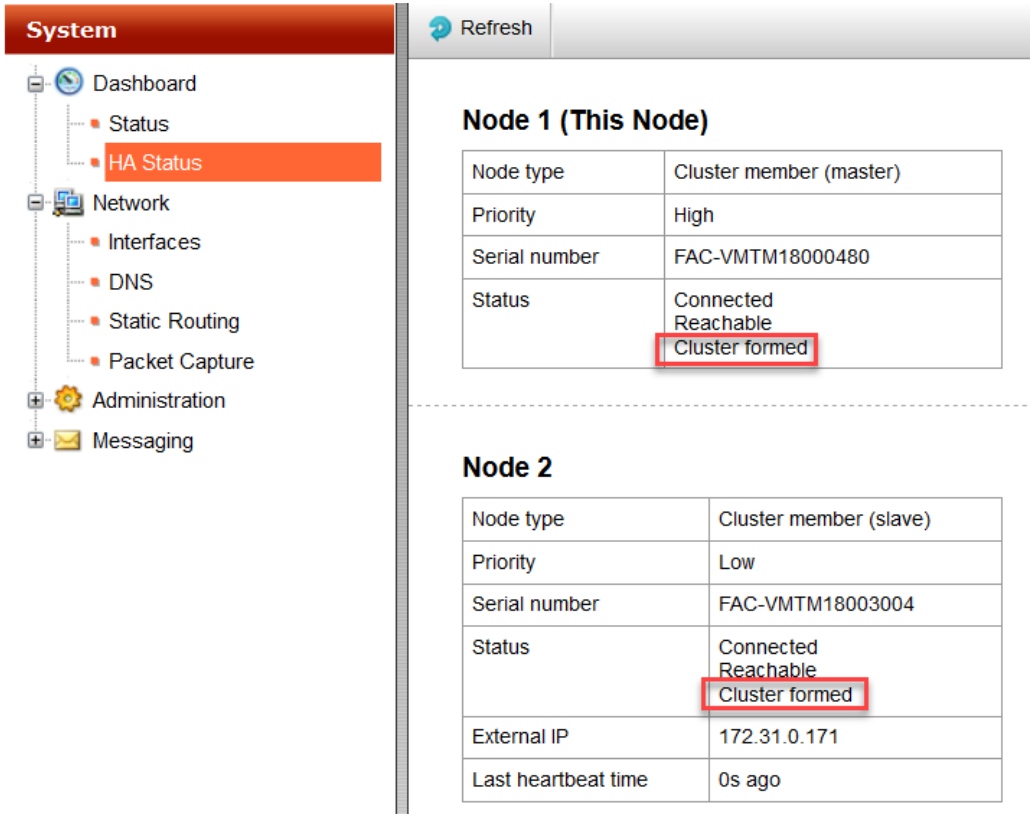
HA Cluster Member (Active-Passive)

- Настройка Master Unit HA (High Priority)
  - Passive Unit использует другой Cluster Member IP адрес в той же подсети



HA Cluster Member (Active-Passive)

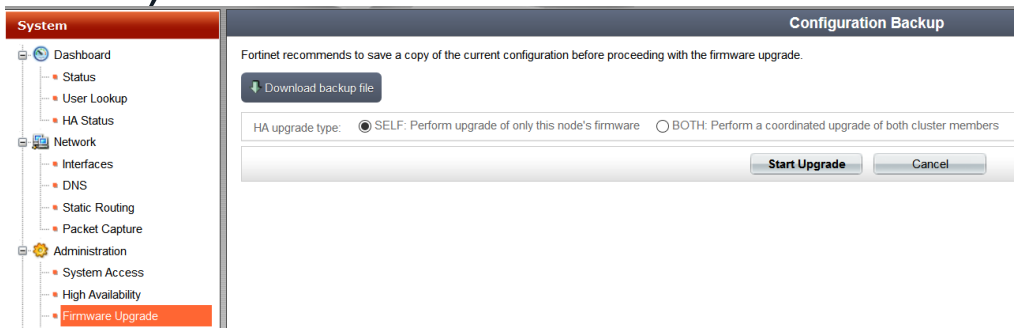
- После того, как Passive unit лицензирован и настроен в кластере с использованием выбранного порта, статус HA мастера должен быть следующим:



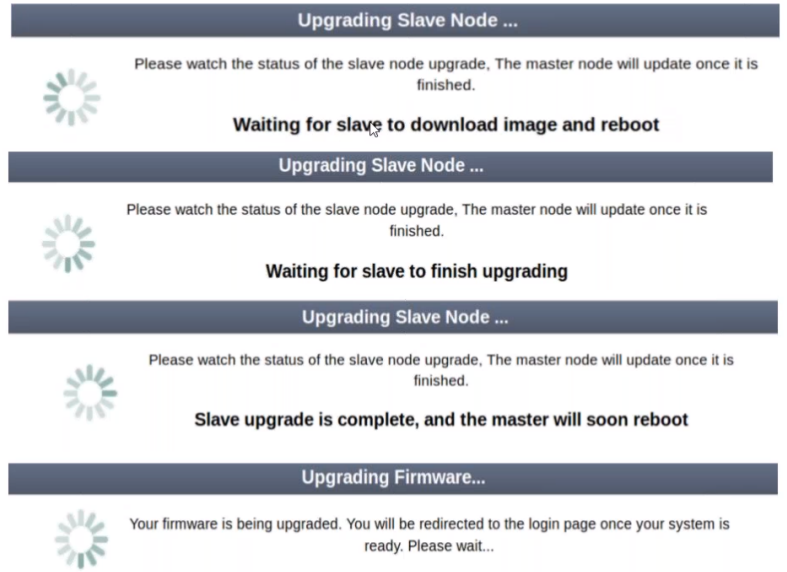
- При создании кластера статус '**Cluster Formed**' должен отображаться для обоих нод

HA Cluster Member (Active-Passive)

- Автоматическое обновление ПО (появился в FAC 5.5)
  - Доступно только на Active Unit
  - Обновление только этого юнита или всего кластера



  - Процедура обновления
    - Образ ПО загружен на Active ноду
    - Active нода загружает образ ПО на Passive ноду
    - Начинаем обновление Passive ноды
    - Ждем пока passive нода вернется и будет статус up and sync
    - Начинаем обновление Active ноды -> reboot
    - Passive нода становится Active
    - Первоначальная Active нода возвращается и получает статус up и in sync
    - Первоначальная Active нода становится Active снова



Сценарии HA

Load-balanced slave (Active-Active)

HA Cluster Member (Active-Active)

- Роли
  - Master
    - Cluster Members – возможно сконфигурировать redundant master, создав A/P cluster
    - Standalone Master
  - Load balanced slave – до10 удаленных L3-связанных slaves
- Трафик аутентификации может быть разбалансирован средствами:
  - NAS client load distribution
  - Round Robin DNS
  - Внешний балансировщик
- Взаимодействие между Master и LB-slaves
  - Cluster Member взаимодействует с LB-slaves через HA port UDP/721
  - Standalone Master не требует HA port
  - Heartbeat traffic
    - OpenVPN – UDP/1194
    - Каждые 20 сек
  - Синхронизация конфигурации
    - OpenVPN – UDP/1194

HA Cluster Member (Active-Active)

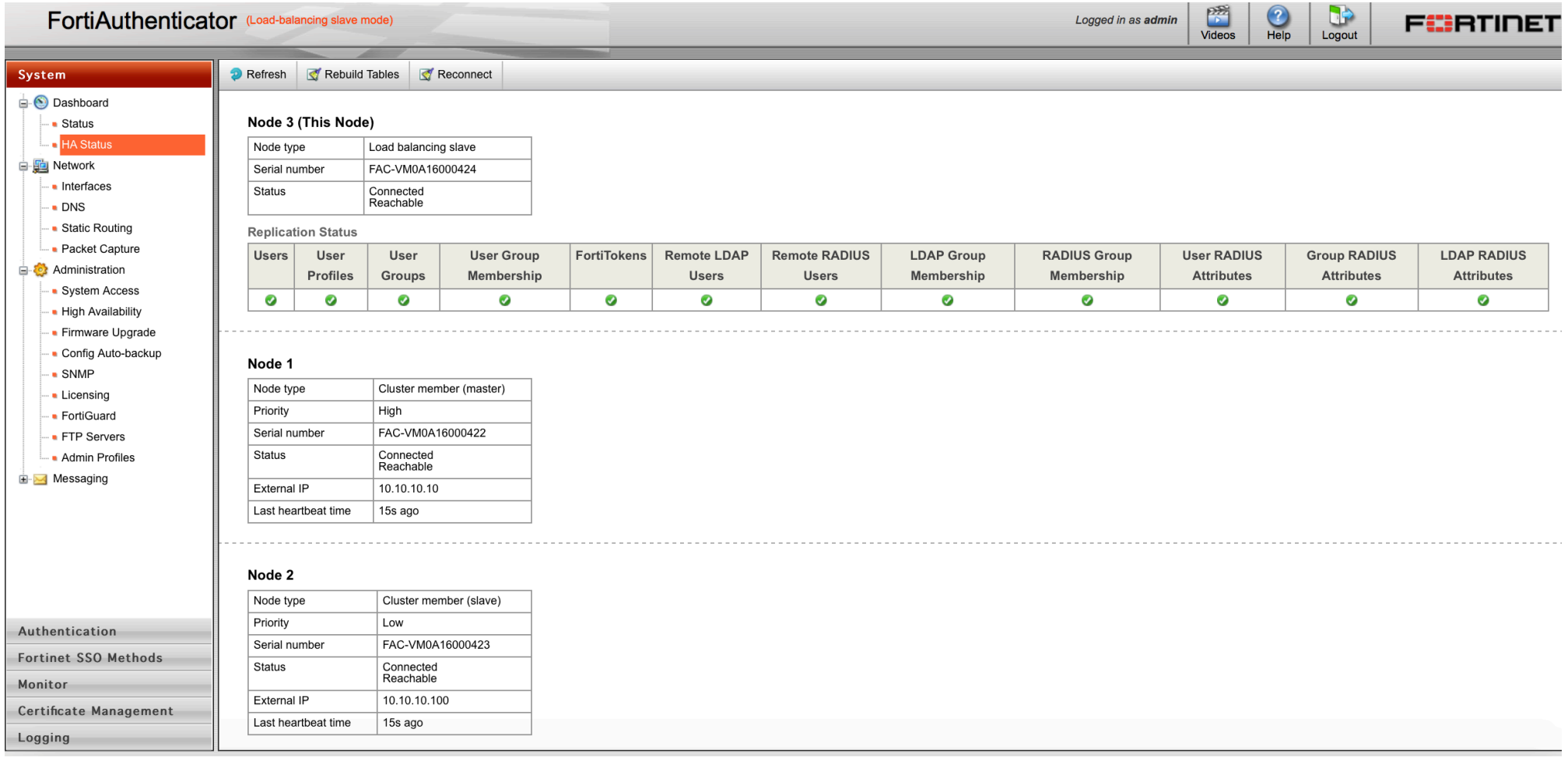
- Изначально был разработал для репликации токенов
- Синхронизируются только следующие элементы :
  - Token & Seeds
  - Local User DB
  - Remote User DB
  - Group mappings
  - Token/User mappings
  - RADIUS Attributes

Users	User Profiles	User Groups	User Group Membership	FortiTokens	Remote LDAP Users	Remote RADIUS Users	LDAP Group Membership	RADIUS Group Membership	User RADIUS Attributes	Group RADIUS Attributes	LDAP RADIUS Attributes
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

- Объекты, такие как Remote Directory Servers должны быть настроены вручную на нодах Geo-HA Active
- HA интерфейсы должны взаимодействовать без NAT
- Поддерживается до 10 Load-Balancing Slaves

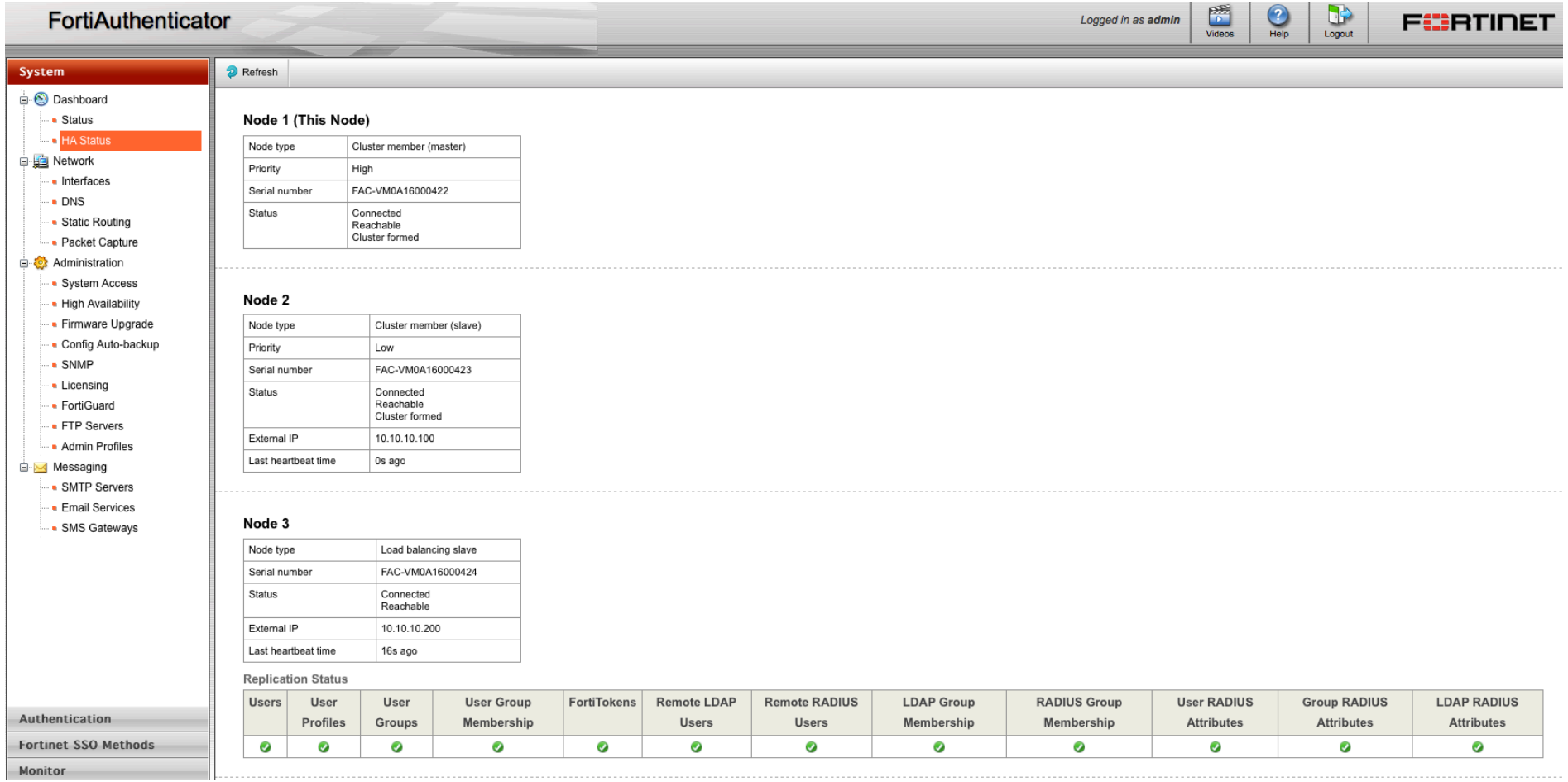
HA Cluster Member (Active-Active)

- LB Slave



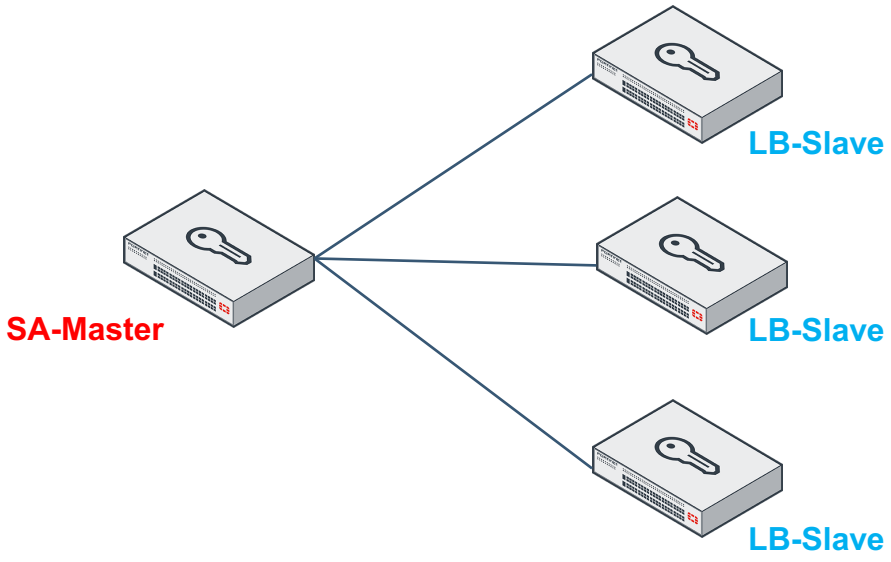
HA Cluster Member (Active-Active)

- Вид со стороны Master

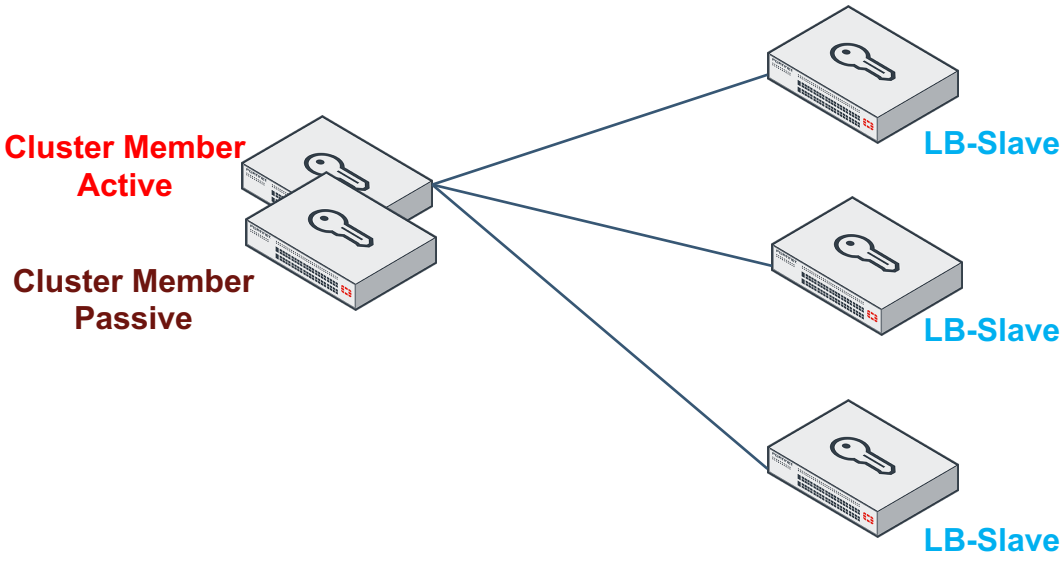


HA Design Solutions

- *Standalone Master*



- *Redundant Master*

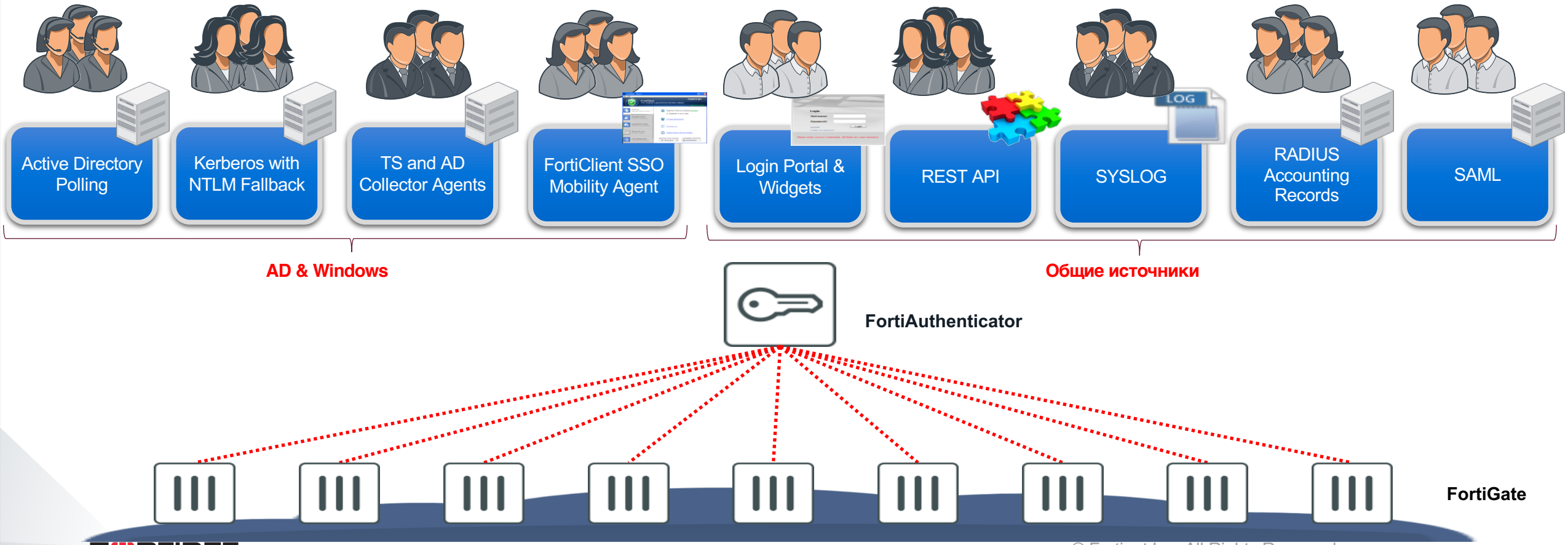


FortiAuthenticator

Сценарии Fortinet Single Sign-On (FSSO)

Fortinet Single Sign-On (FSSO)

- Источники информации о пользователях



FSSO методы

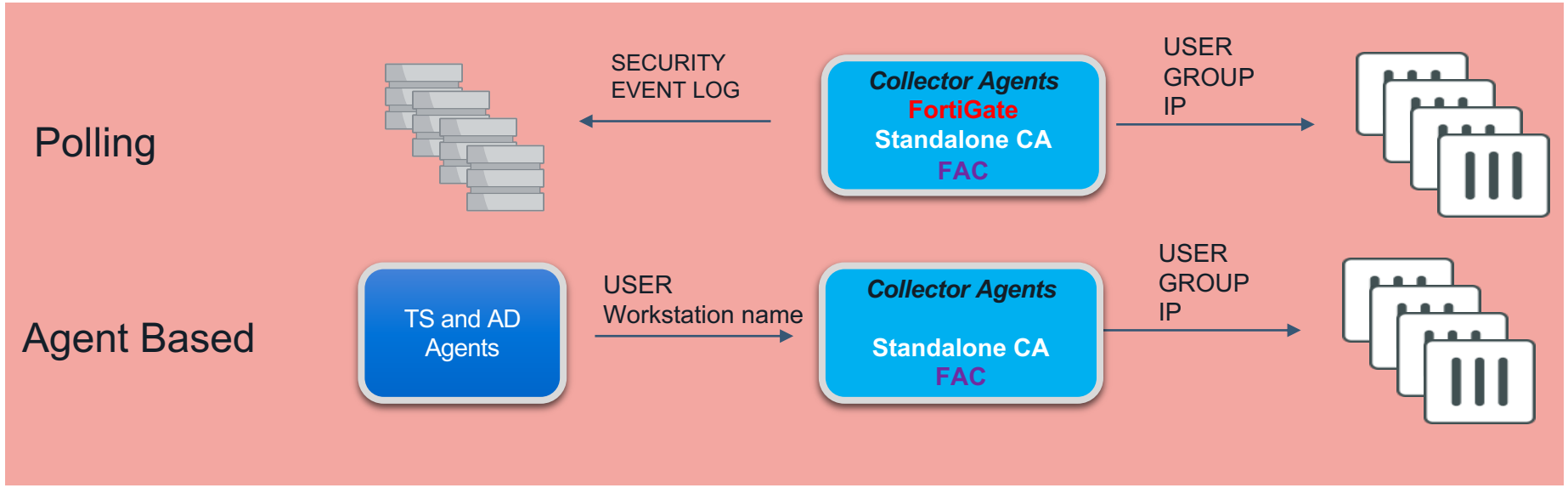
AD и Windows

Fortinet Single Sign-On (FSSO)

Получить идентификационные данные - AD и Windows

Collector Agents

- FortiGate (least features)
- Standalone CA (Win App)
- FAC



- Monitoring AD Security Event Log for logon only messages **(no logout)**

Наиболее точное и масштабируемое FSSO решение

Mobility Agent

- Sends identity (IP & DOMAIN\Username) to FAC on login
- Updates identity on IP stack change (wireless roaming, connect after hibernation, unclean shutdown, hibernation, cable pulled)
- Sends **logout** event on clean logout
- Sends heartbeats to keep user authenticated

FORTINET

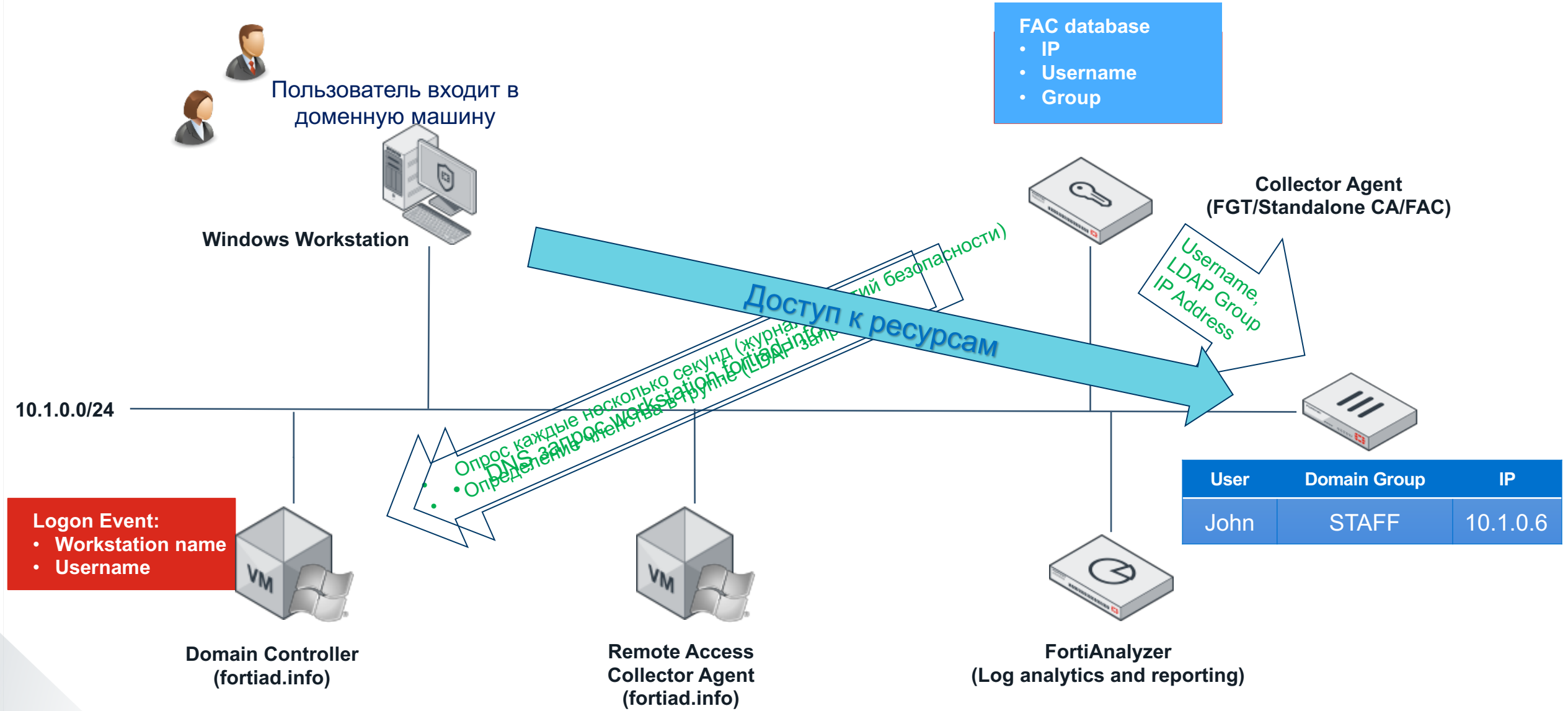
FSSO методы

AD и Windows - Polling

FSSO – Collector Agent Polling Method

- **Получить идентификационные данные - AD и Windows**
  - Polling методы
    - NetAPI
      - *NetSessionEnum* Microsoft API
      - Временной интервал – каждые 9 сек
      - Наиболее быстрый метод, но может пропустить какие-то события, если сервер перегружен
    - WinSec (Windows Security Event Logs)
      - Event IDs - 672, 680, 4776 and 4768
      - Дополнительные IDs – 528, 540, 4624 (MacOS)
      - Каждые 5 сек
    - WMI (инструментарий управления **Windows**)
      - For polling WinSec (Standalone CA only)
      - For detecting workstation logoffs
      - Требует открытие портов на Windows FW tcp ports 135&445
    - Рейтинг эффективности
      1. WinSec + Workstation WMI
      2. WinSec
      3. NetAPI

Режим Collector Agent Polling

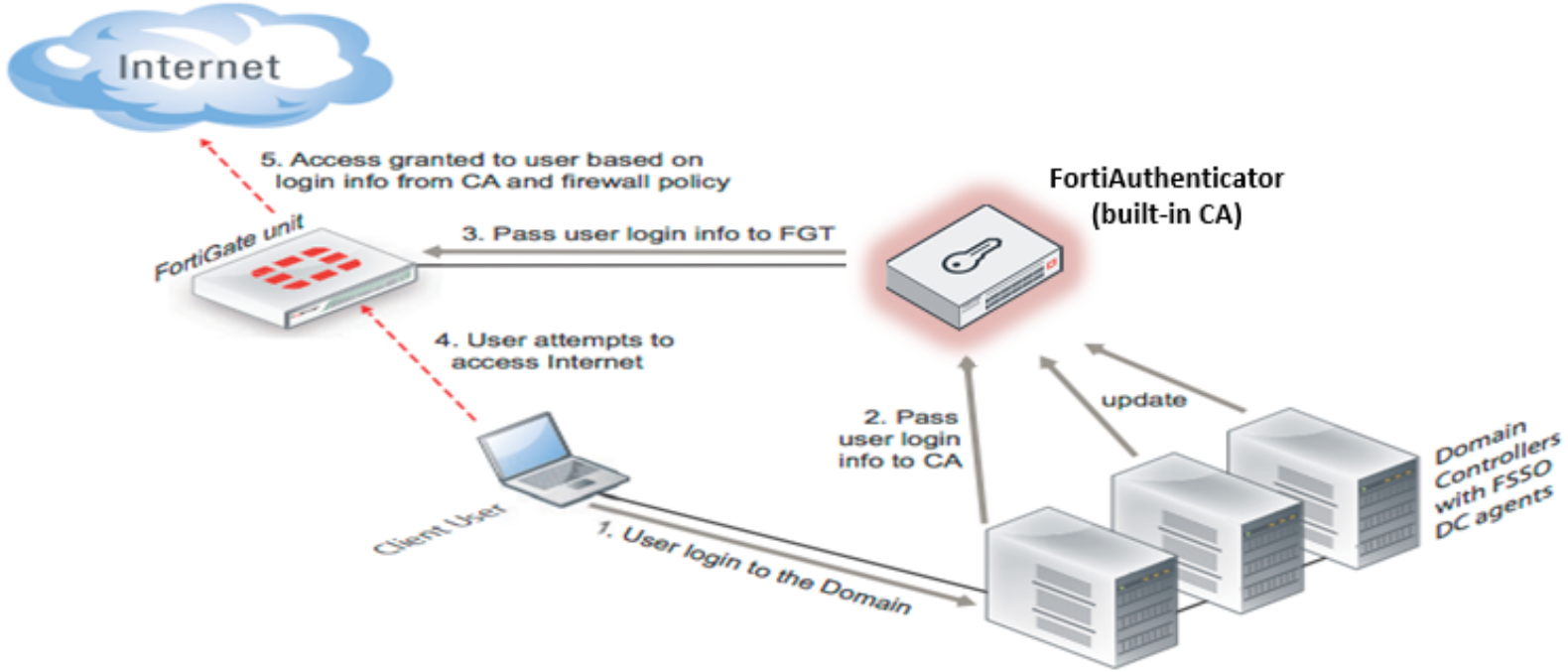


FSSO методы

AD и Windows – на базе агента

FSSO – AD Agent метод

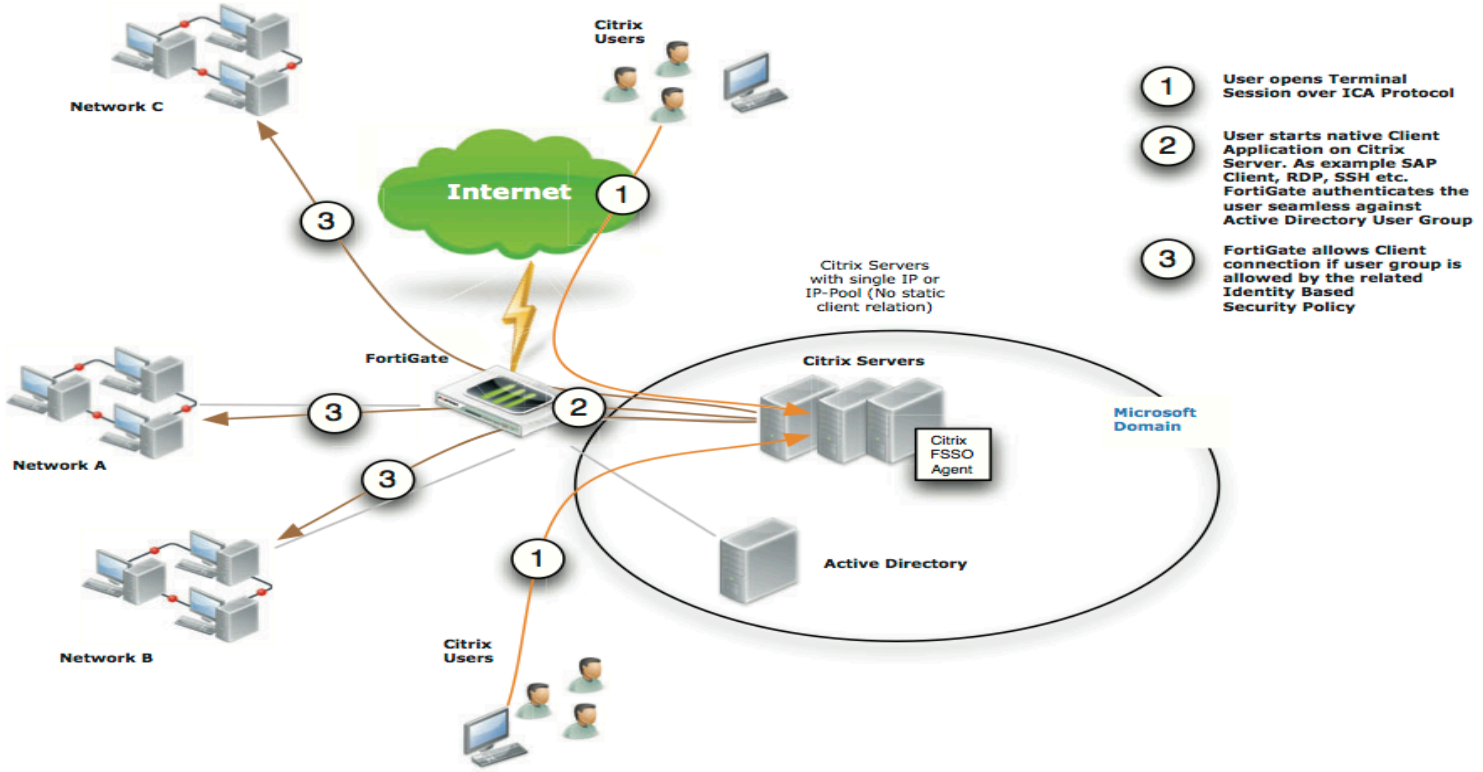
- Active Directory Agent



- Обычная реализация FSSO
- DC Agent должен быть установлен на всех Domains Controllers
- DC Agent представляет собой dll файл под именем `dcagent.dll`
- Он отслеживает logon события и передает их на Collector Agent или FortiAuthenticator
- Это достаточно надежный метод FSSO
- После установки агентов на DC требуется перезагрузка

FSSO – TS Agent метод

- Terminal Services Agent

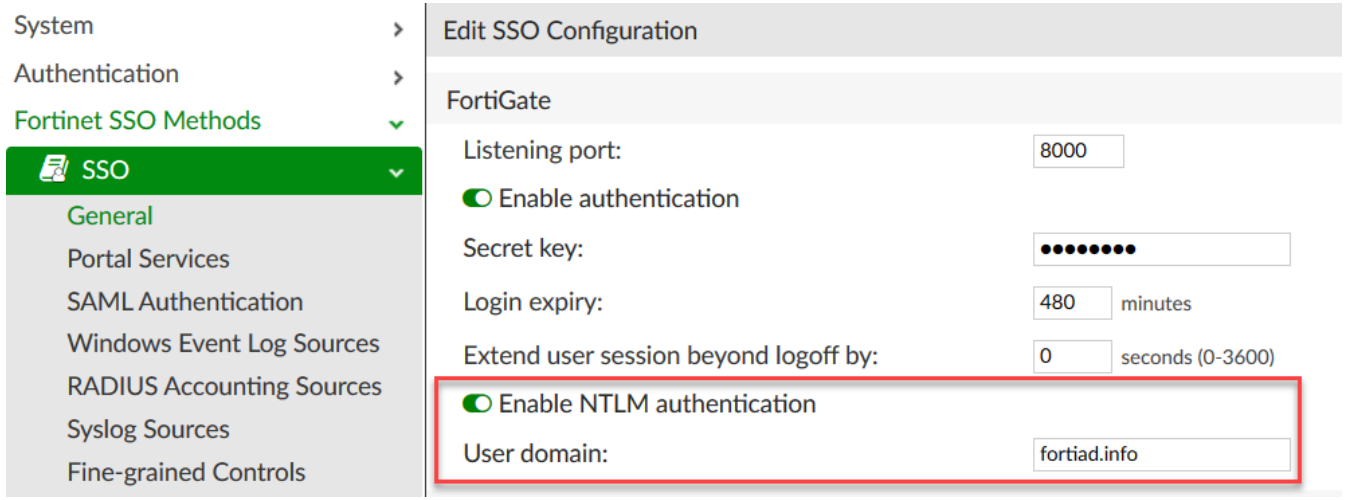


- Позволяет отслеживать события logon множества пользователей с одного IP адреса
- Основан на назначении разных source ports диапазонов для каждой сессии пользователя
- Default pool имеет 200 портов
- Может отправлять logon информацию на FortiAuthenticator
- Поддерживает отслеживание logoff событий

FSSO – NTLM backup

- NTLM будет использован только в случае, если Collector Agent потерял доступ к AD (polling перестал работать)
- NTLM включается per FGT security policy и является глобальной настройкой CA

```
config firewall policy
    edit 5
        set ntlm enable
        set ntlm-enabled-browsers "MSIE" "Mozilla" "Opera"
        set groups <FSSO-GROUP>
    next
end
```



FSSO – Общее сравнение методов

Collector Agent	Polling		Дополнительные методы	Назначение	Доп. инфо
	Метод	Частота			
FortiGate	WinSec	10 sec	CA feed (Windows CA and/or FAC CA)	Demo and Small (up to approx 20 users)	Least accurate, very resource intensive
Windows CA	WinSec WMI WinSec NetAPI	5 seconds 300 sec (configurable) 9 sec	TS Agent AD Agent Radius Accounting Syslog Client NTLM Windows CA Sync	Enterprise Small/medium	Dependency on DNS, lots of messages generated with WMI polling
FortiAuthenticator	WinSec WMI Workstation	5 seconds 300 sec	TS Agent AD Agent Radius Accounting Syslog Server/Client NTLM API Portal SAML Mobility Agent (SSOMA) Windows CA input (syslog) FAC CA Sync (one-way)	Enterprise Small/medium/large	Dependency on DNS, Multiple methods support

FSSO методы

Mobility Agent

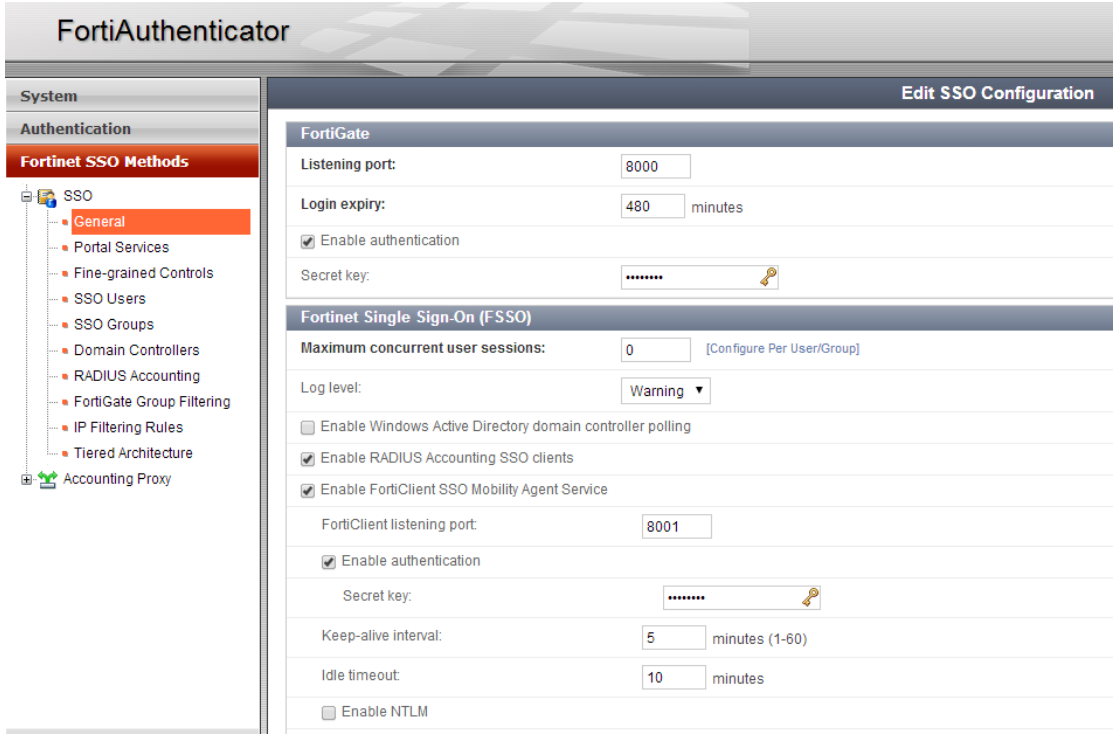
FSSO – SSO Mobility Agent (SSOMA)

- Компоненты
  - **Single Sign-on Mobility Agent (SSOMA)** это ПО, устанавливаемое на Windows машины или MAC для выявление logged in пользователей и передачи этой информации на user FortiAuthenticator (FAC) для ее дальнейшего использования в Identity Based Policies:
    - Пользователь должен быть доменный
    - Отправляет данные identity (IP & DOMAIN\Username) на FAC во время входа пользователя
    - Обновляет данные identity при смете IP адреса (wireless roaming, подключение после гибернации, неправильного shutdown)
    - Отправляет logout event при правильном logout
    - Отправляет heartbeats для отслеживания, что пользователь все еще аутентифицирован. Пропущенные heartbeats запускают процесс де-аутентификации со стороны FAC.
  - **FortiAuthenticator**
    - Передает информацию, полученную от SSOMA клиентов на FortiGate/s
    - Для маппинга пользователей и групп требуется LDAP интеграция с Active Directory Server

FSSO – Method2 (SSO Mobility Agent)

- Настройка SSOMA
  - » SSOMA это компонент FortiClient
  - » Standalone (доступен в виде отдельного инсталлера)
  - » Наиболее масштабируемый метод FSSO
  - » Поддерживает несколько лесов, доменов и междоменных групп

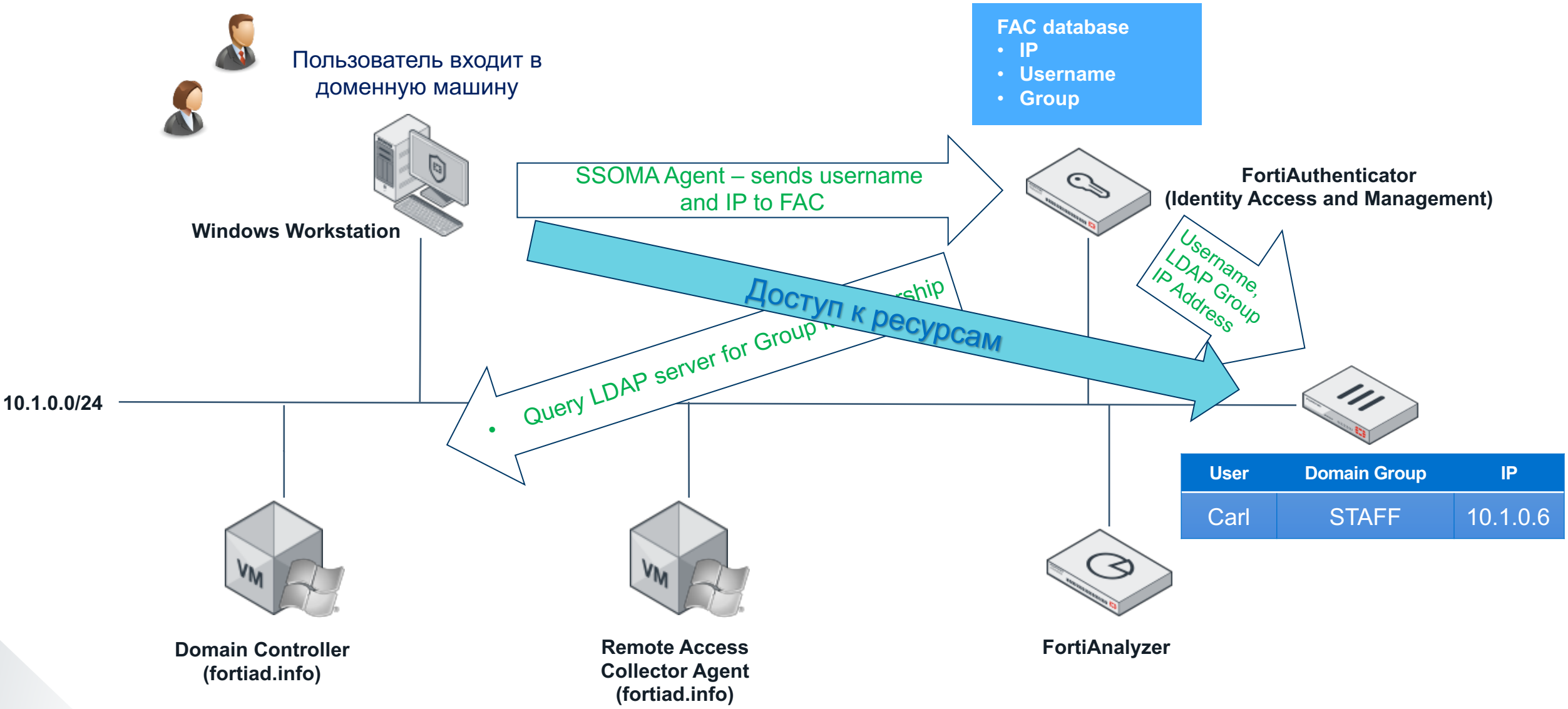
  - » Agent настраивается со стороны FortiAuthenticator
    - Keep-alive interval: Default 5 мин (допускает 1 to 60 мин)
    - Idle timeout: 10 мин (допускается Keepalive value до 10000)



- SSOMA имеет несколько уровней защиты, встроенной в клиент
  - » Взаимодействие с FortiAuthenticator на порт 8001 зашифровано SSL
    - Использует дефолтный сертификат FAC (может быть изменен)
  - » Pre-shared key используется для аутентификации клиента при подключении к FAC
    - Препятствует подключению неавторизованных клиентов к FAC
  - » Учетные данные пользователя проверяются путем валидации CHAP password hash against known AD using NTLM
    - Предотвращают подключение PC к посторонним DC и подмену учетных данных пользователей

FORTINET

SSOMA Agent Solution



Сравнение методов

	Решение на основе Collector Agent	Решение на основе SSO Mobility Agent
Точность	• Зависимость от интервала опроса или предоставленной информации syslog/radius • Зависимость от разрешения DNS (разрешение имени рабочей станции, особенно при переходе из проводной сети в беспроводную • Зависимость от WMI-опроса конечных точек	• Нет зависимостей • более высокая точность
Внедрение	• Может быть развернут без FAC • Terminal Services Agent	• Требуется установка агента на всех конечных точках • Terminal Services Agent
Общее	• В режиме опроса он генерирует множество сообщений в больших сетях (каждые несколько секунд) • DNS-трафик • Опрос WMI	• Меньше сетевого трафика - без DNS-запросов или опроса WMI • Лучшая масштабируемость

FortiAuthenticator

Сценарии двухфакторной аутентификации на базе sms, email или мобильного токена

Двухфакторная аутентификация – варианты реализации сервиса

Группа	Функция	FortiGate	FortiGate + FortiAuthenticator
Масштабируемость	Рекомендуемое количество пользователей	от 1 до 100	от 100 и выше
	Портал самообслуживания для самостоятельного выпуска токенов пользователями	Нет	Да
	Возможность использования токенов в нескольких FortiGate	Нет	Да
	Поддержка аутентификации сторонних веб-приложений	Нет	Да
Двухфакторная аутентификация	SMS/Email	Да: - SMTP-SMS шлюз - сервис FortiSMS	Да: - HTTP-SMS шлюз - SMTP-SMS шлюз - сервис FortiSMS
	FortiToken Mobile	Да лицензия по количеству токенов	Да лицензия по количеству пользователей и токенов
	FortiToken Cloud	Да лицензия по количеству пользователей и времени работы	Нет
	2FA OTP Push	Да	Да
	Аппаратный FortiToken	Да требуется приобретение токенов	Да требуется приобретение токенов
	Интеграция по RADIUS с внешней системой	Да	Да
	Интеграция по SAML с внешней системой	Да только для SSL VPN	Да только для SSL VPN
	Аутентификация доступа по цифровому сертификату	Да	Да

Двух-факторная аутентификация

FortiToken Mobile

- Поддерживается технология Push notification
- Дополнительная защита приложения с помощью PIN кода с поддержкой Touch ID и Face ID
- 6 или 8 символов в качестве OTP, с обновлением каждые 30 или 60 сек
- Поддержка распространения через QR Code

FortiToken Hardware

- Несколько аппаратных вариантов исполнения
- 6 или 8 символов в качестве OTP, с обновлением каждые 30 или 60 сек
- При использовании FortiAuthenticator возможно использовать сторонние токены

Варианты FortiToken

FortiToken Mobile

Приложение для смартфона с поддержкой генератора OTP и технологии PUSH уведомления approval

FortiToken 300

- USB брелок: не требует установки драйверов
- Применяется для PKI аутентификации

FortiToken 220

Исполнение в виде пластиковой карты с экраном

FortiToken 200/200CD

- Исполнение в виде брелка
- Время работы от батарейки: до 3х лет

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiToken_Mobile.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiToken_200.pdf

FORTINET

FortiAuthenticator

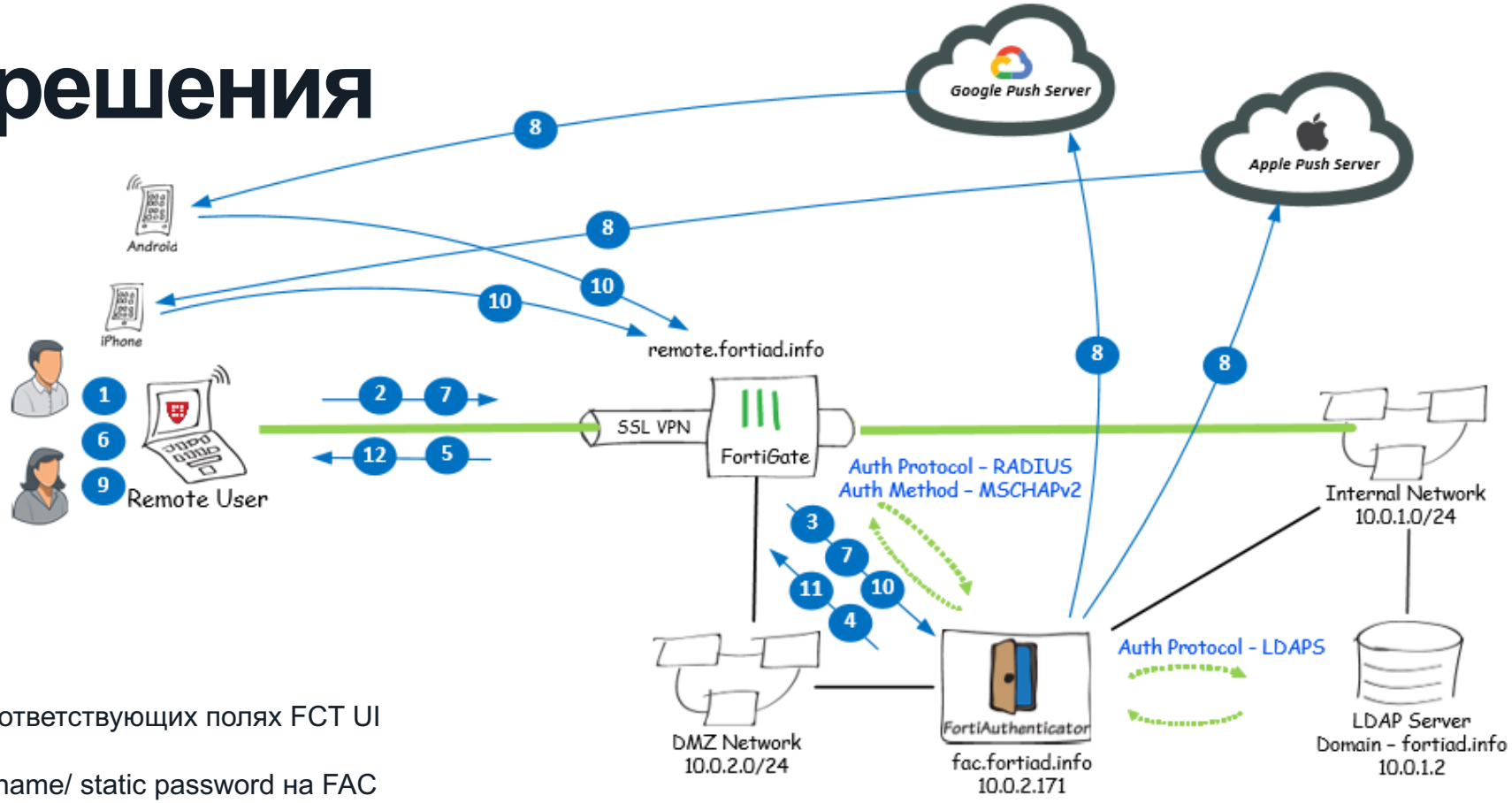
Пример настройки SSL-VPN с двухфакторной аутентификацией на основе FortiToken Mobile с применением Push Notification

Обзор технологии Push Notification

- Двухфакторная аутентификация (2FA) стала стандартом в наши дни. Наиболее распространенное применение этого метода - подключение SSL VPN.
- Вторым фактором (в 2FA) может быть все, что есть у пользователя, и в большинстве случаев мы говорим о токенах, аппаратных или программных.
- В push-уведомлении используется программный токен FortiToken Mobile, одно нажатие кнопки позволяет подтвердить второй фактор.
- В этом разделе презентации описывается полный процесс развертывания push-уведомлений с помощью FortiAuthenticator, FortiGate и FortiToken Mobile.

Схема работы решения

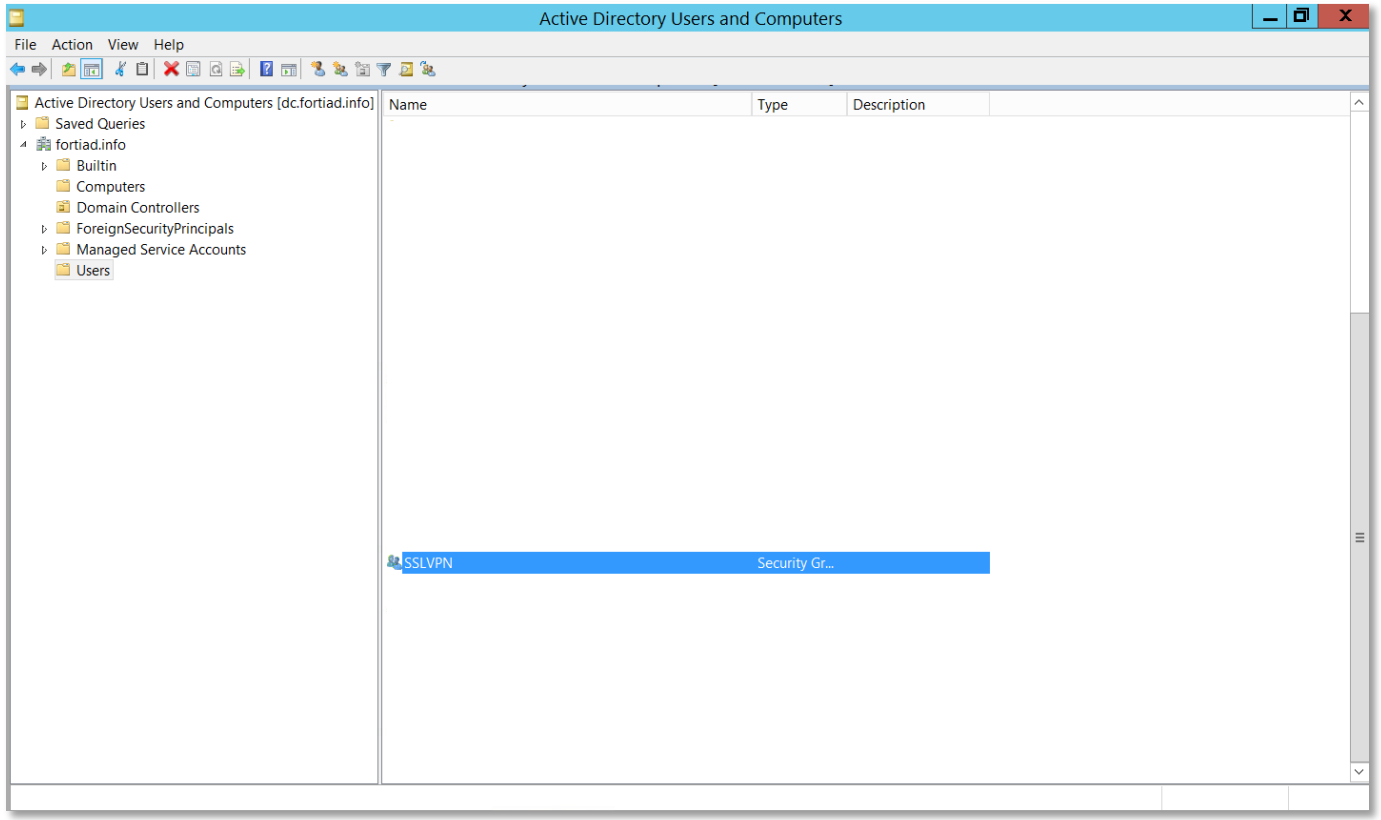
Процесс аутентификации для установки ssl vpn с 2FA, где второй фактор - FortiToken Mobile, настроенный для push-уведомлений, выглядит следующим образом:



1. Пользователь вводит username и password в соответствующих полях FCT UI
2. FCT отправляет VPN auth запрос на FGT
3. FGT отправляет RADIUS Access-Request с username/ static password на FAC
4. FAC проверяет username и static password и отвечает с RADIUS Challenge-Request, с запросом пустого поля пароля для запуска push-уведомления или ручного ввода кода токена.
5. FGT передает Challenge Request на FCT и указывает , что доступен push
6. FCT предлагает конечному пользователю ввести код токена или использовать Push.
7. Если пользователь выбирает Push, FCT отправляет обратно пустое поле пароля в FAC через FGT в последующем запросе доступа.
8. FAC видит пустое значение пароля и отправляет push через сервер Google или Apple Push.
9. Конечный пользователь одобряет (или отклоняет) попытку входа в систему на мобильном устройстве.
10. Если пользователь одобряет, FTM отправляет OTP на IP-адрес и порт, указанные FAC.
11. FAC отправляет запрос доступа обратно в FGT.
12. FGT сигнализирует FCT о том, что доступ предоставлен и VPN подключен.

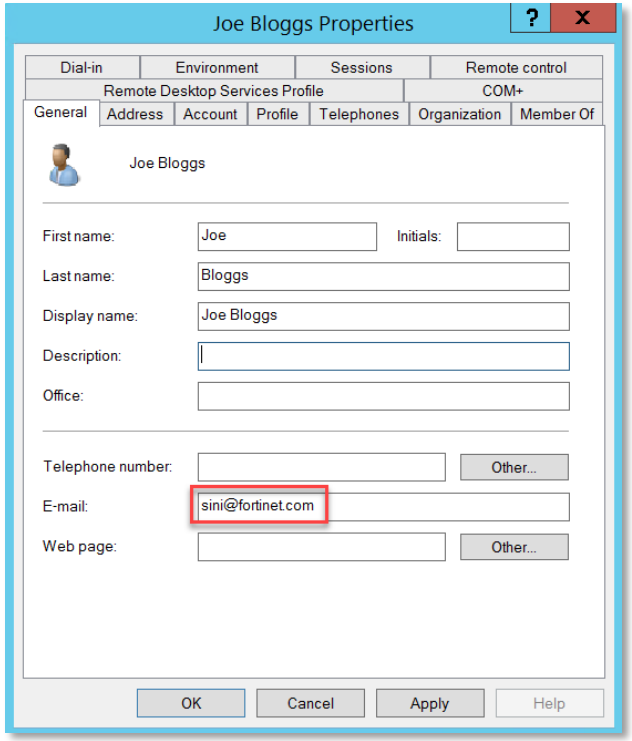
Настройка Active Directory

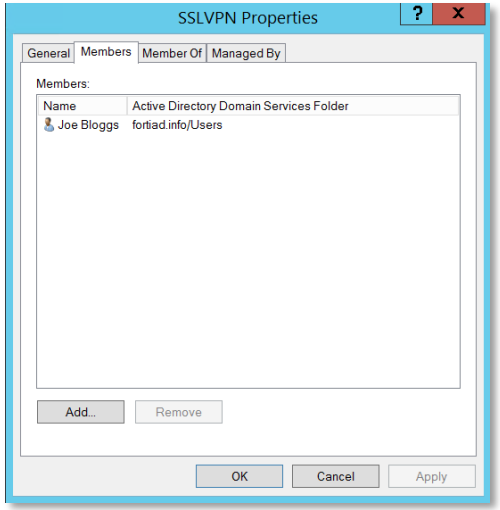
- В этом примере мы использовали простую структуру AD, где группа SSLVPN находилась в основном контейнере Users.



Настройка Active Directory (2)

- Пользователи в группе удаленного доступа должны иметь адреса электронной почты, определенные как часть их профиля.
- Примечание - адрес электронной почты будет использоваться для автоматической доставки кода FTM (FortiToken Mobile).
- Убедитесь, что пользователь является членом группы SSLVPN

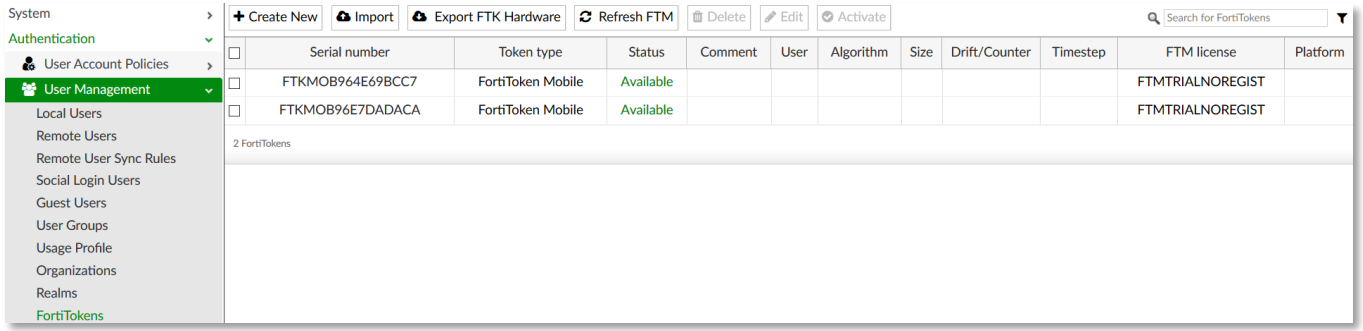




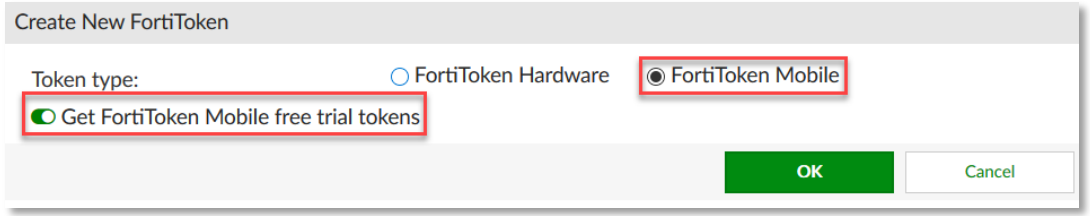
Настройка FortiAuthenticator

- Убедитесь, что FortiToken Mobile free trial tokens доступны в меню

Authentication → User Management → FortiTokens



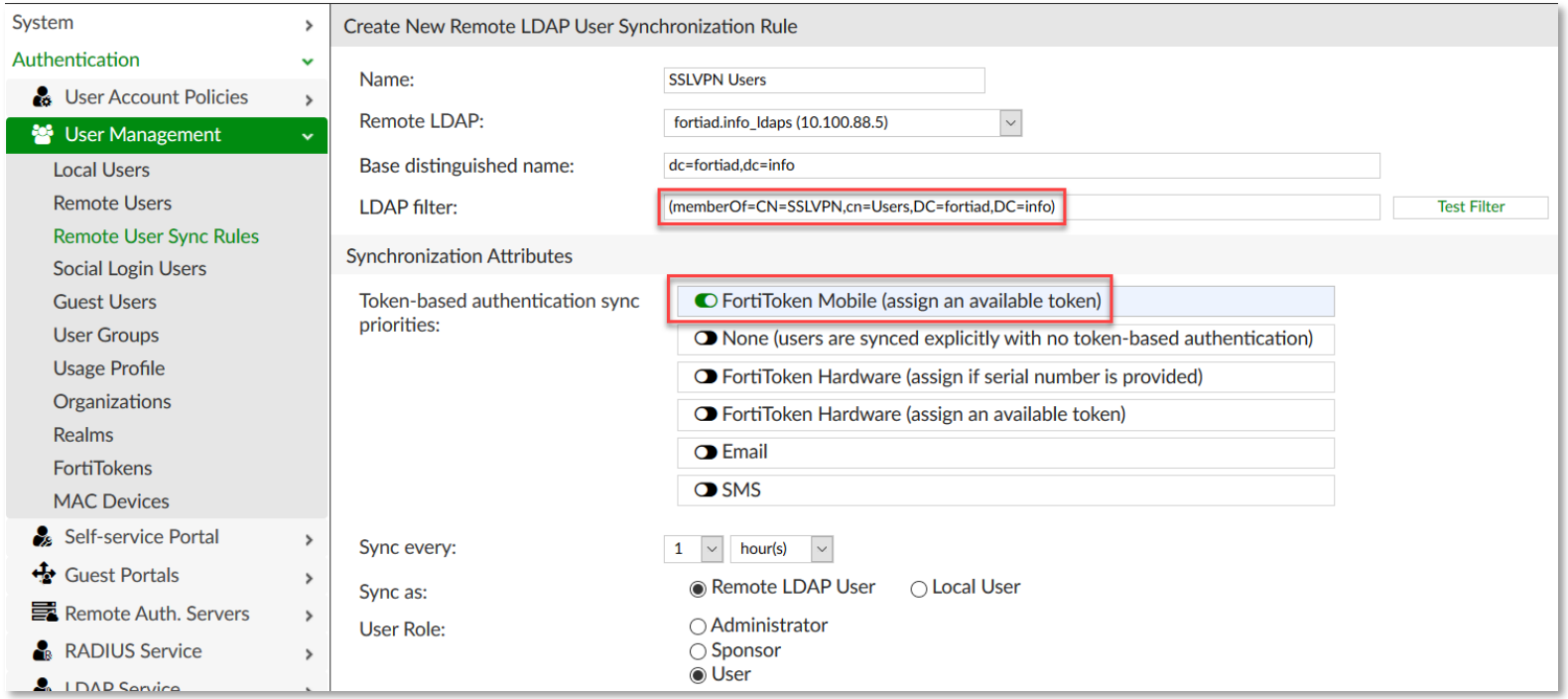
- Если у вас не отображаются бесплатные токены, выберите «Создать новый», выберите параметры, указанные ниже, и нажмите «ОК».



- Ваши бесплатные токены должны появиться в окне FortiTokens.

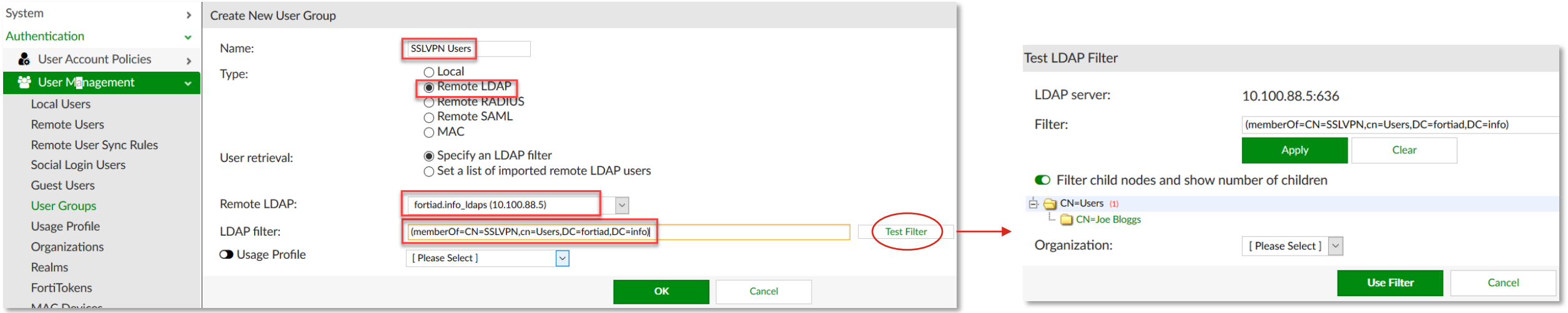
Настройка FortiAuthenticator (2)

- Настраиваем Remote User Sync Rule under ***Authentication → User Management → Remote User Sync Rules***
  - ***LDAP filter*** **=** <LDAP filter>
  - ***Sync Priorities*** **= FortiToken Mobile (assign an available token)**
  - Нажмите ОК внизу страницы, чтобы применить изменения.



Настройка FortiAuthenticator (3)

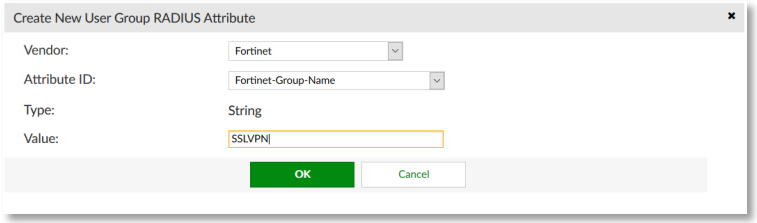
- Создаем новую User Group в ***Authentication → User Management → User Groups***
  - **Name =** <Group Name>
  - **Type = Remote LDAP**
  - **User retrieval = Specify an LDAP filter**
  - **Remote LDAP =** <LDAP Server>
  - **LDAP filter =** <LDAP filter>

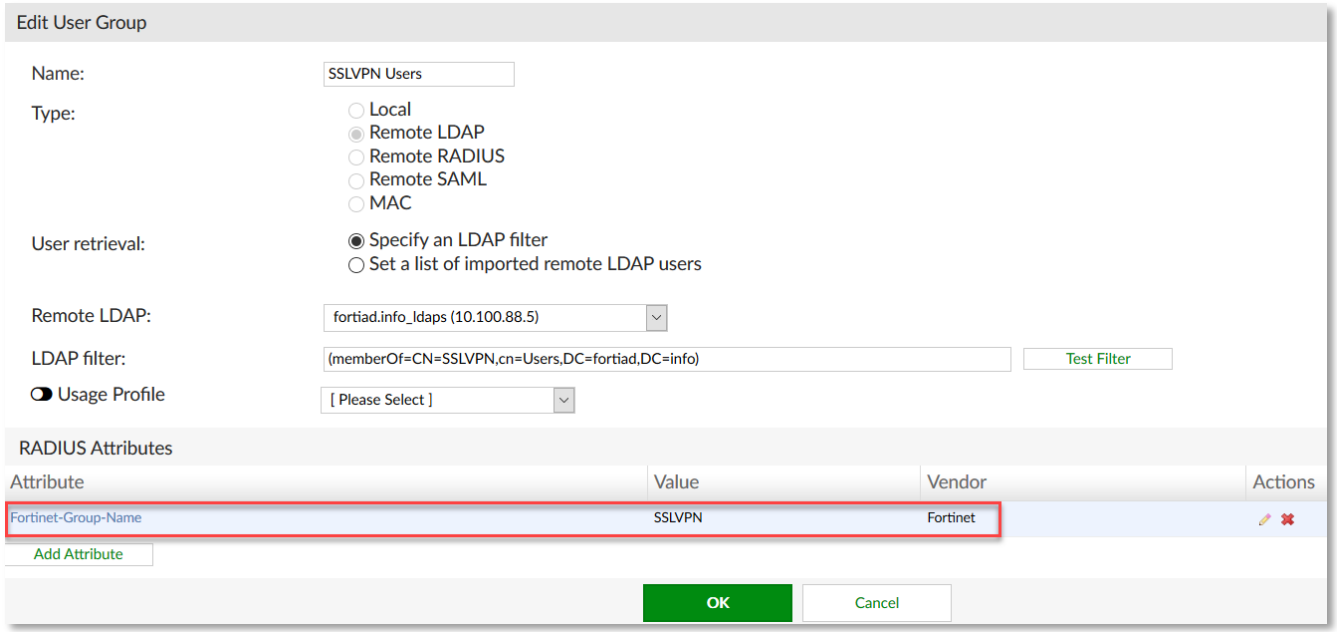


- Выбираем **Test Filter** для просмотра всех пользователей в данной группе AD
- Выберите ОК, чтобы применить конфигурацию.

Настройка FortiAuthenticator (4)

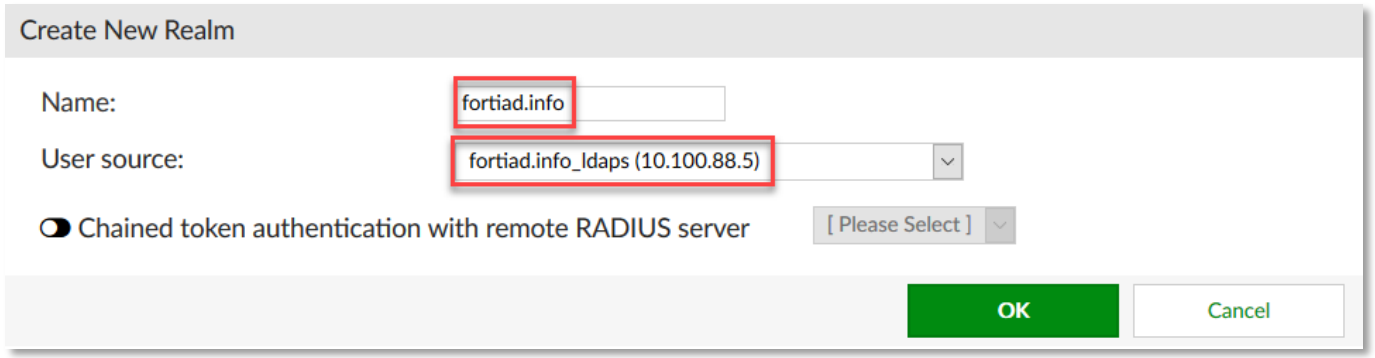
- Создаем Radius Group Name Attribute для вновь определенной группы пользователей
- Edit User Group
  - ***RADIUS Attribute → Add Attribute***
    - ***Vendor*** **=** Fortinet
    - ***Attribute ID*** **=** Fortinet-Group-Name
    - ***Value*** **=** <Group Name> (needs to match on FortiGate)





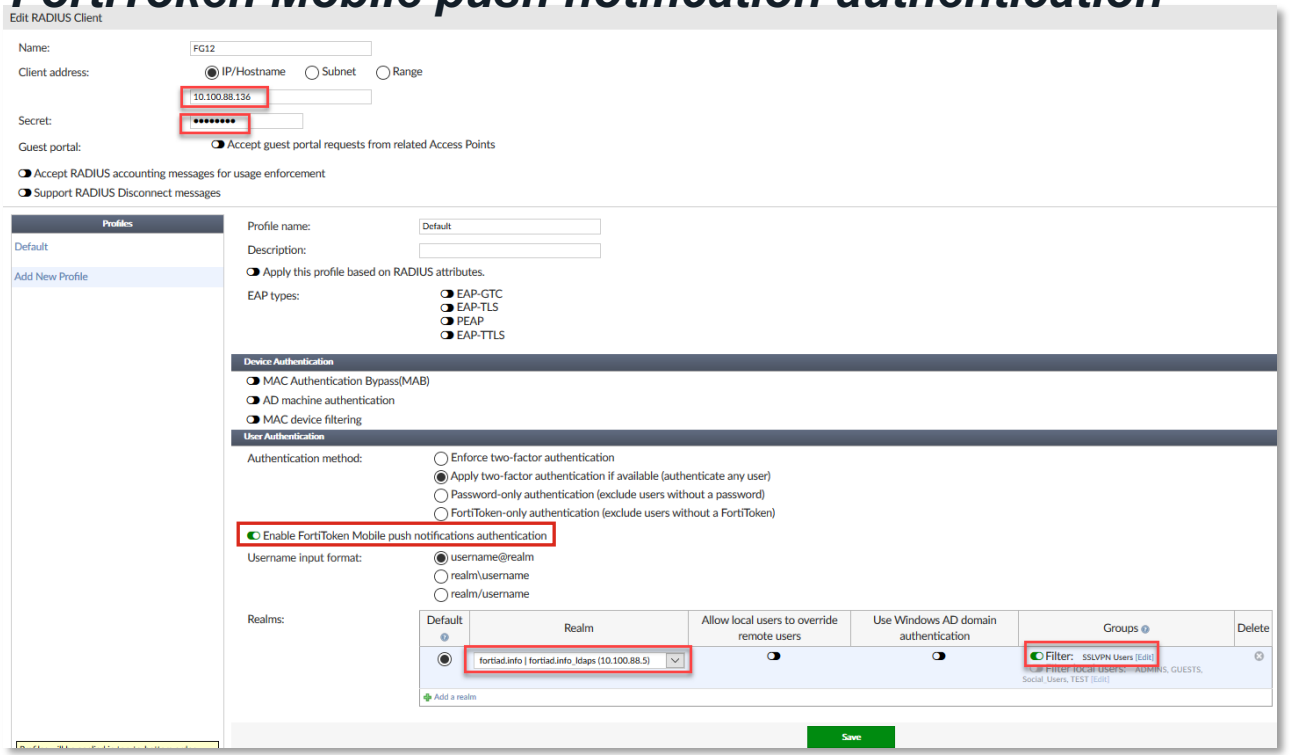
Настройка FortiAuthenticator (5)

- Создаем Authentication Realm for LDAP Server under ***Authentication → User Management → Realms → Create New***
  - ***Name*** = <DNS domain name>
  - ***User Source*** = <LDAP Server>



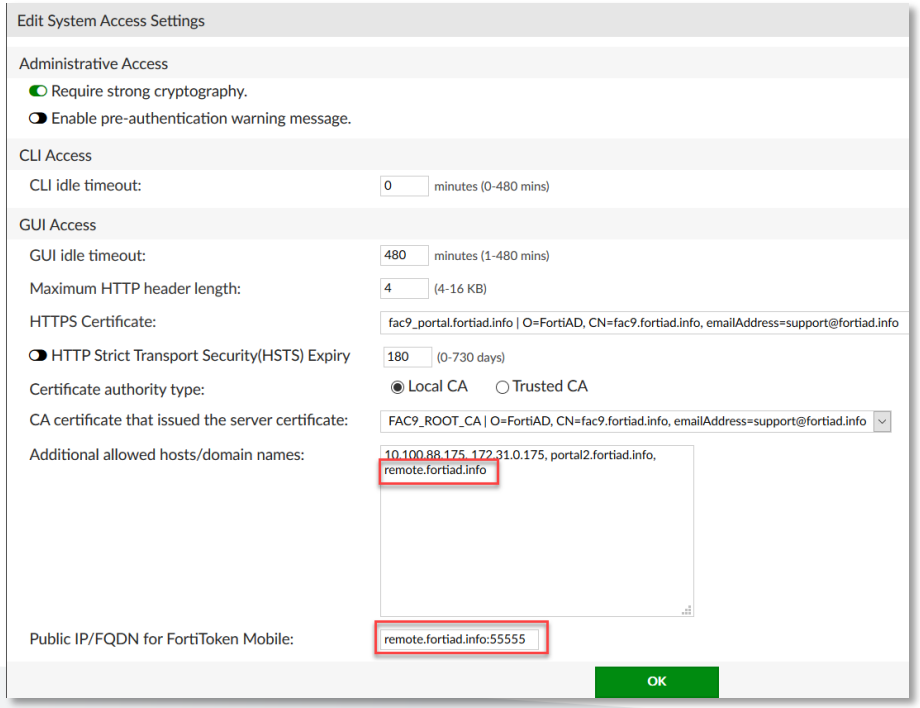
Настройка FortiAuthenticator (6)

- Настройка Radius Client Configuration в меню ***Authentication → Radius Service → Clients***
  - ***Name =*** *<Display Name>*
  - ***Client address = IP/Hostname =*** *<FW IP Address>*
  - ***Secret =*** *<secret> (needs to match on the fw)*
  - ***Profile = Default = User Authentication= Enable FortiToken Mobile push notification authentication***
  - ***Profile = Default = User Authentication=Realms***
    - ***Realm =*** *<Realm Name>*
    - ***Groups = Filter =*** <User Group>



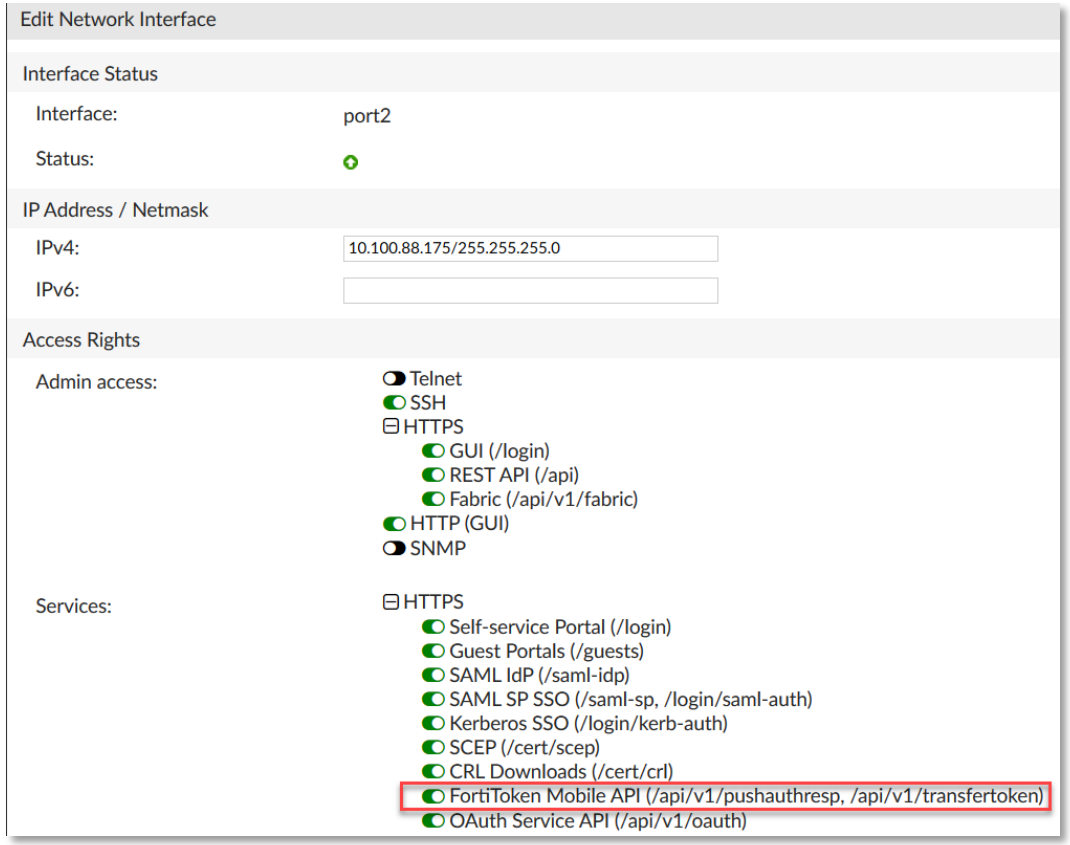
Настройка FortiAuthenticator (7)

- Настройте Alternative IP-адреса для доступа через API, указав public IP-адрес, который будет использоваться для доступа к FAC.
- Этот Virtual IP должен быть настроен на FortiGate
  - This is done under ***System → Administration → System Access***
    - ***Additional allowed hosts/domain names*** = <Firewall VIP>
    - ***Public IP/FQDN for FortiToken Mobile*** = <Firewall VIP:port>
      - in case a single public IP is available, optional port can be advertised externally



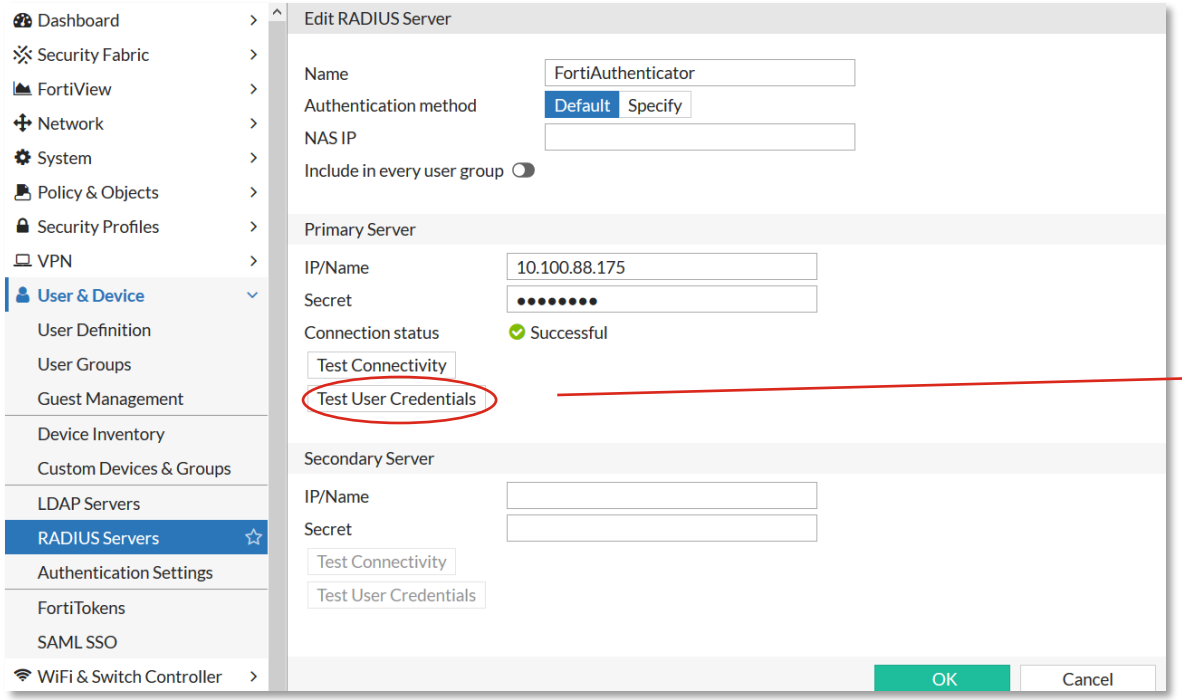
Настройка FortiAuthenticator (8)

- Настройте Interface API access under ***Network → Interfaces*** and Select and **Edit** Interface
  - Go to ***Services → HTTPS*** and enable ***FortiToken Mobile API (/api/v1/pushauthresp, /api/v1/transfertoken)***

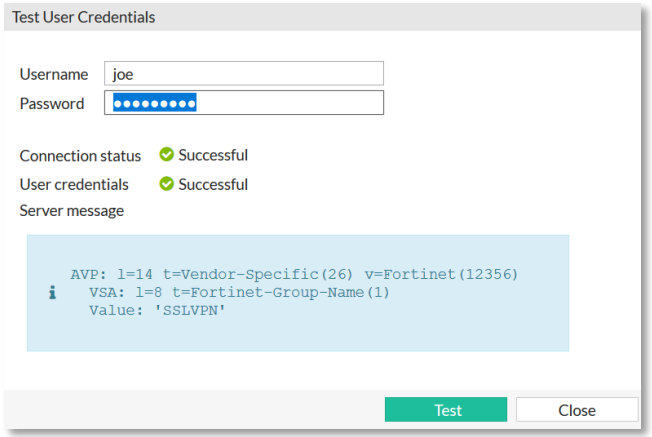


Настройка FortiGate

- Создаем новый Radius Server в меню ***User & Device → RADIUS Servers → Create New***
  - ***Name*** = <Display Name>
  - ***Primary Server***

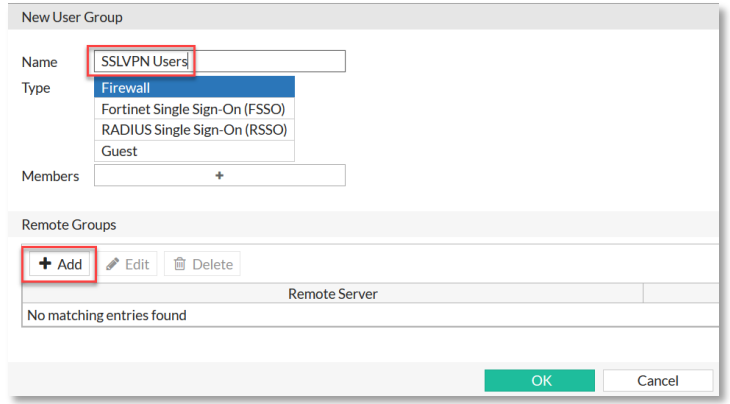


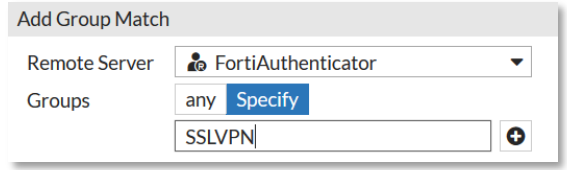
- Select ***Test User Credentials*** to verify authentication settings

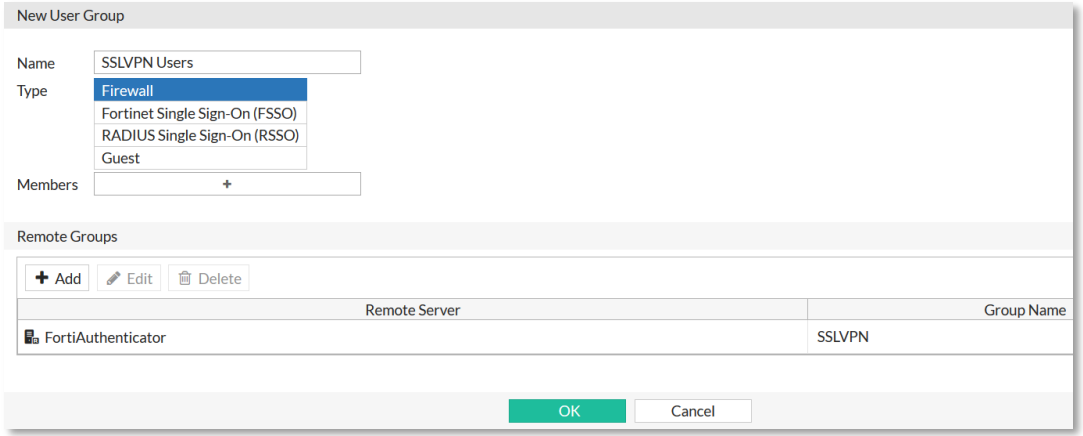


Настройка FortiGate (2)

- Создаем новую User Group under ***User & Device → User Groups → Create New***
  - ***Name =*** <Display Name>
  - ***Remote Groups → Add***
    - ***Remote Server =*** <Radius Server>
    - ***Groups =*** <matching FAC radius group attribute>
    - Select ***OK***
  - Select ***OK***

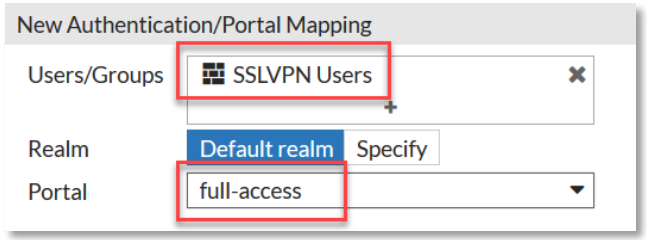






Настройка FortiGate (3)

- Настраиваем SSL-VPN settings under ***VPN → SSL-VPN Settings***
  - ***Listen on Interface(s)*** = <select interface>
  - ***Authentication/Portal Mapping → Create New***
    - ***User/Groups*** = <User Group created>
    - ***Portal*** = full-access
    - Select ***OK***



Настройка FortiGate (4)

- Настраиваем authentication timers через CLI
  - ***Global Remote Authentication Timeout***

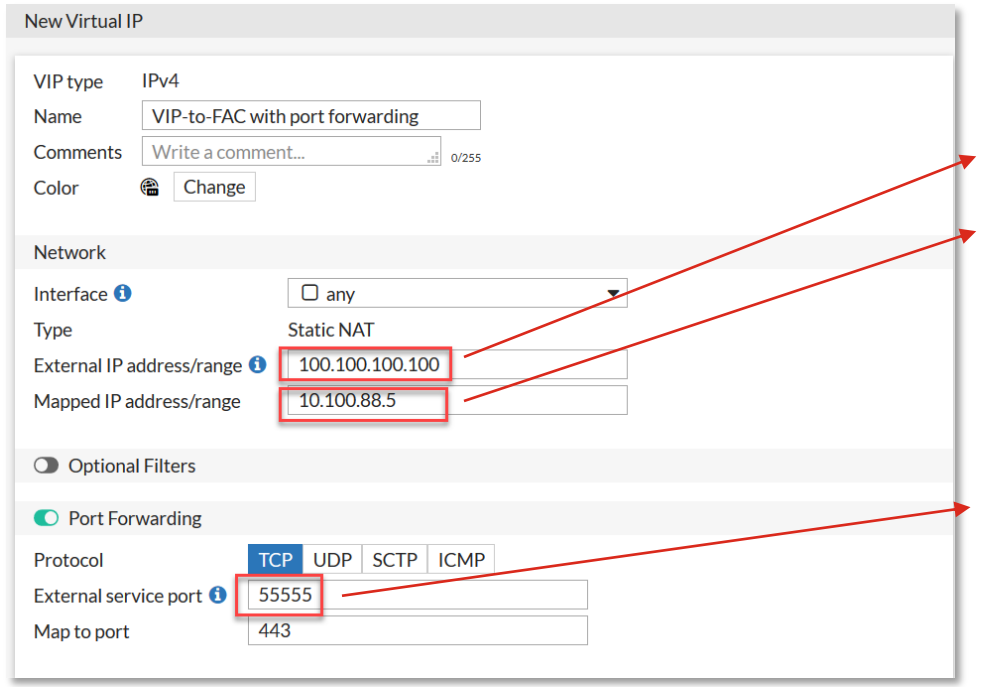
FortiGate # config system global

FortiGate (global) # set remoteauthtimeout 60 (range is 5-300, default is 5 seconds)

FortiGate (global) # end

Настройка FortiGate (5)

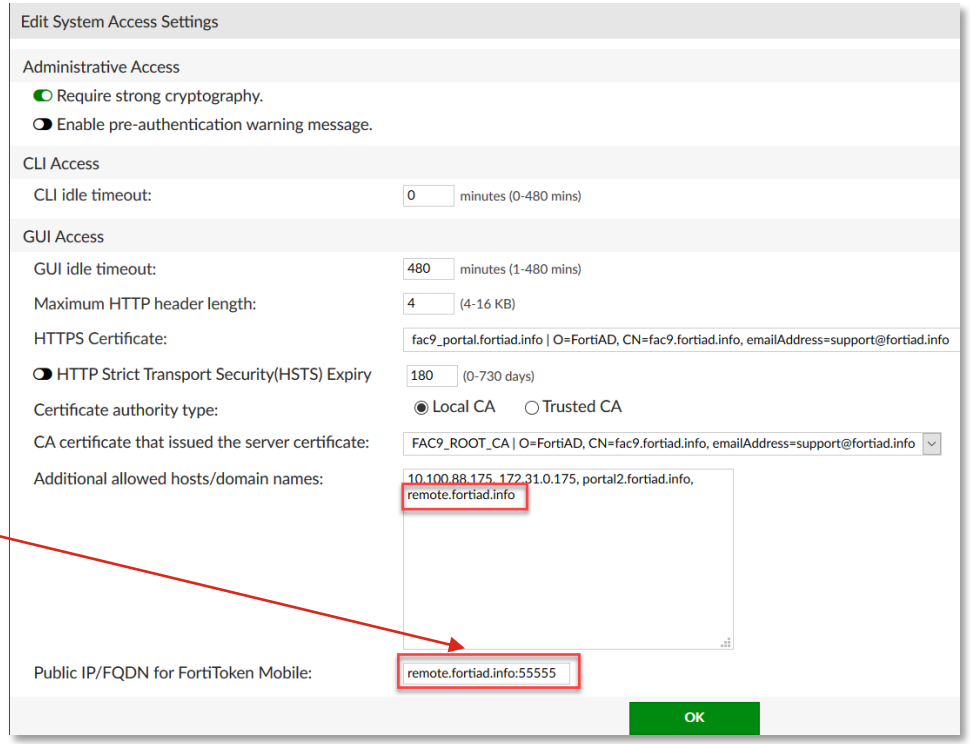
- Настраиваем Virtual IP to be used in FortiGate Security Policy to allow remote communication between mobile phones and FAC (Step 10 on the overview diagram)
  - Create a VIP with port forwarding under ***Policy & Objects → Virtual IPs***



remote.fortiad.info

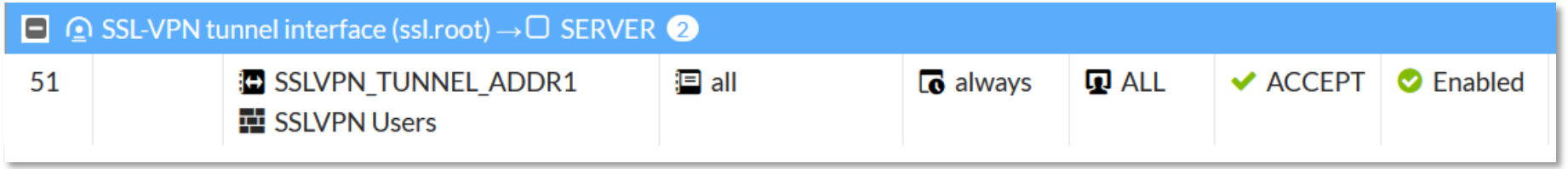
FAC IP address

Port advertised on FAC



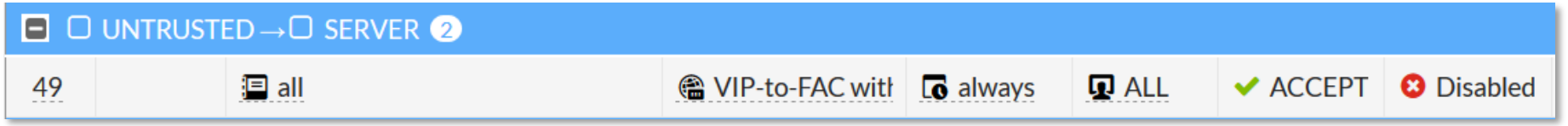
Настройка FortiGate (6)

- Настройте следующие политики безопасности FortiGate
- To allow SSL VPN Users access to local resources

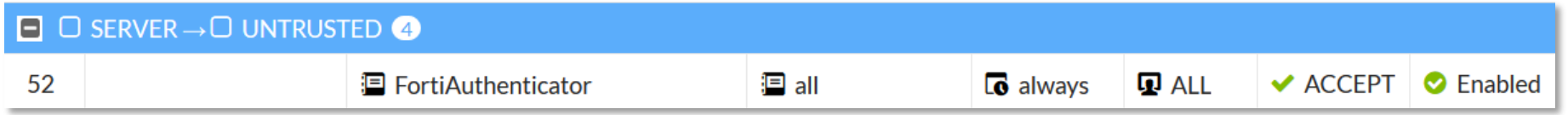


  - Обратите внимание– if you have split-tunnelling enabled within SSL portal, select relevant destination subnet

- To allow mobile phones access to FAC for API push notification



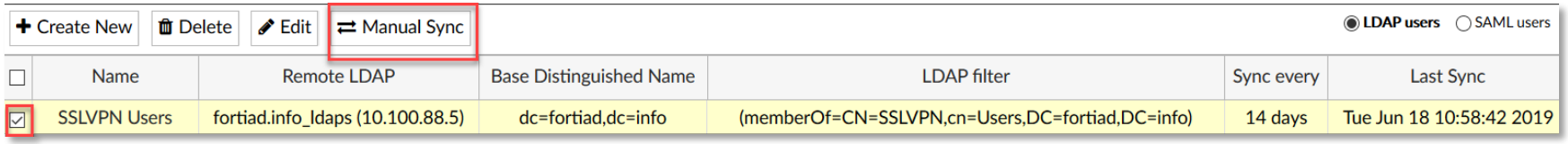
- To allow FortiAuthenticator access to the Internet



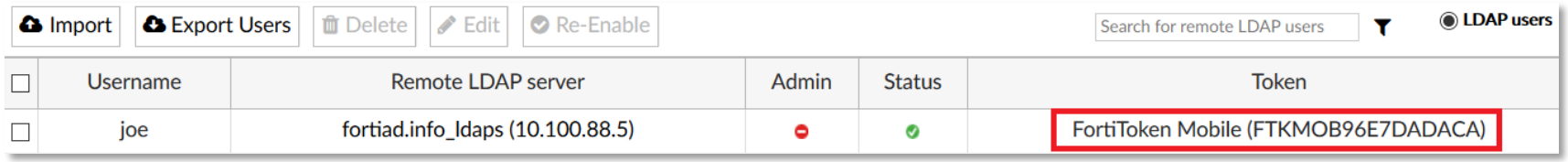
Проверка и траблшутинг

Проверка

- Manually Sync Users in order to receive FortiTokens, by going to FortiAuthenticator ***Authentication → User Management → Remote User Sync Rules***
  - Select ***User Group*** and point to ***Manual Sync***



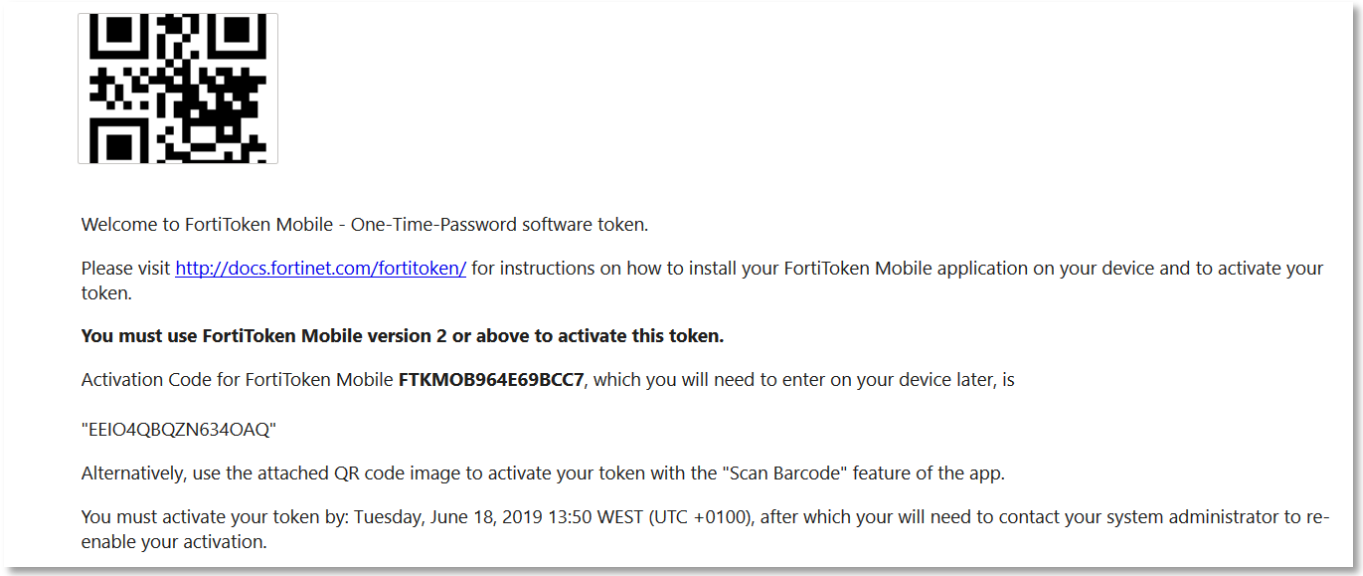
  - Check that the users are imported and assigned FTMs, by going to ***Authentication → User Management → Remote Users***



    - The newly imported users with FTM assigned will appear in the user list

Проверка (2)

- Проверьте свой почтовый ящик на наличие кода активации FTM и добавьте его в приложение FTM, работающее на вашем мобильном устройстве.



Welcome to FortiToken Mobile - One-Time-Password software token.

Please visit http://docs.fortinet.com/fortitoken/ for instructions on how to install your FortiToken Mobile application on your device and to activate your token.

You must use FortiToken Mobile version 2 or above to activate this token.

Activation Code for FortiToken Mobile **FTKMOB964E69BCC7**, which you will need to enter on your device later, is

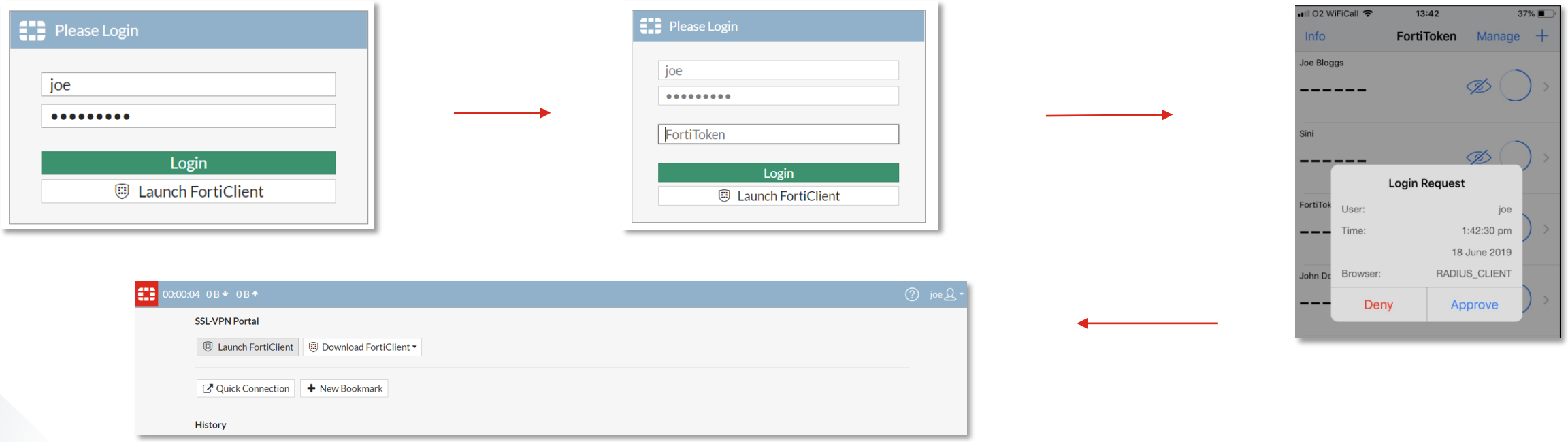
"EEIO4QBQZN634OAQ"

Alternatively, use the attached QR code image to activate your token with the "Scan Barcode" feature of the app.

You must activate your token by: Tuesday, June 18, 2019 13:50 WEST (UTC +0100), after which your will need to contact your system administrator to re-enable your activation.

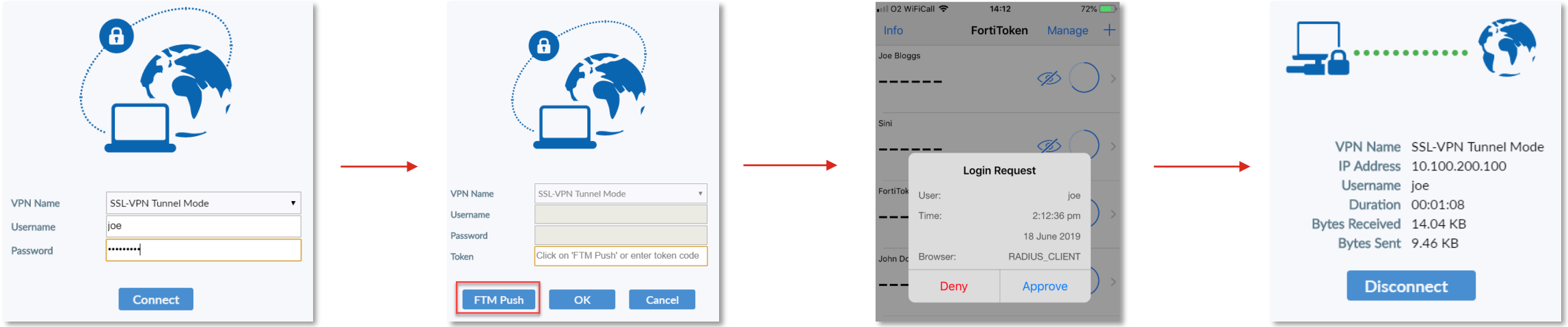
Проверка (3)

- Следующий шаг - инициировать vpn. В зависимости от технологии будут доступны следующие варианты:
  - Для web based ssl-vpn – push notification работает автоматически
  - Для Tunnel based ssl-vpn – пользователь получает возможность включить push-уведомление
- Примепр Web based ssl-vpn



Проверка (4)

- Пример Tunnel (FortiClient) based ssl-vpn



Проверка и диагностика

- FortiAuthenticator Log File entry

Refresh | Download Raw Log | Log Type Reference | Debug Report

Search for log records

ID	Timestamp	Level	Category	Sub category	Type id	Action	Status	Source IP	Short message	User
10155	Tue Jun 18 15:30:45 2019	information	Event	Authentication	20002	Authentication	Success	10.100.88.136	Remote LDAP user authentication with FortiToken successful (chosen FTM push notification)	joe
10154	Tue Jun 18 15:30:42 2019	information	Event	Web Service	50501	Authentication	Pending	localhost	Sending authentication notification to User[joe]	
10153	Tue Jun 18 15:30:37 2019	information	Event	Authentication	20300	Authentication	Pending	10.100.88.136	Remote LDAP user authentication partially done (chosen FTM push notification), expecting FortiToken	joe
10152	Tue Jun 18 15:30:33 2019	information	Event	Authentication	20300	Authentication	Pending	10.100.88.136	Remote LDAP user authentication partially done, expecting FortiToken	joe

- FortiGate Traffic Log Entry – please note that FAC is aprox. 4 seconds ahead of FortiGate system clock.
  - FAC sending push notification to Apple Push Server and then 2 secs after that it receives a notification from iphone

Add Filter | Details

Date/Time		Source	Destination	Result	Policy
2019/06/18 15:30:40		192.168.0.1	192.168.0.175	✔ Accept: session start	49
2019/06/18 15:30:38		10.100.88.175	17.188.165.136 (gateway.push.apple.com)	✔ Accept: session start	52

Проверка и диагностика

- FortiAuthenticator
  - Debug radius аутентификации содержит три последовательных части

```
2019-06-18T15:30:33.795623+01:00 fac9 radiusd[4062]: ===>NAS IP:10.100.88.136
2019-06-18T15:30:33.795625+01:00 fac9 radiusd[4062]: ===>Username:joe
2019-06-18T15:30:33.795627+01:00 fac9 radiusd[4062]: ===>Timestamp:1560868233.795401, age:0ms
2019-06-18T15:30:33.795628+01:00 fac9 radiusd[4062]: Found NAS from preloaded collections for 10.100.88.136: FG12 (10.100.88.136)
2019-06-18T15:30:33.796208+01:00 fac9 radiusd[4062]: Found NAS profile for client, NAS: 10.100.88.136 profile: Default
2019-06-18T15:30:33.796377+01:00 fac9 radiusd[4062]: Setting 'Auth-Type := FACAUTH'
2019-06-18T15:30:33.796382+01:00 fac9 radiusd[4062]: [pap] WARNING! No "known good" password found for the user.  Authentication may fail because of this.
2019-06-18T15:30:33.796383+01:00 fac9 radiusd[4062]: # Executing group from file /usr/etc/raddb/sites-enabled/default
2019-06-18T15:30:33.796565+01:00 fac9 radiusd[4062]: Found NAS from preloaded collections for 10.100.88.136: FG12 (10.100.88.136)
2019-06-18T15:30:33.796812+01:00 fac9 radiusd[4062]: Found NAS profile for client, NAS: 10.100.88.136 profile: Default
2019-06-18T15:30:33.796958+01:00 fac9 radiusd[4062]: Realm: (null) (default realm id: 2) username: joe
2019-06-18T15:30:33.797169+01:00 fac9 radiusd[4062]: Realm not specified, default goes to remote LDAP, id: 1
2019-06-18T15:30:33.797174+01:00 fac9 radiusd[4062]: FAC local user overrides, try searching local user first
2019-06-18T15:30:33.797405+01:00 fac9 radiusd[4062]: ERROR: local user 'joe' not found
2019-06-18T15:30:33.797410+01:00 fac9 radiusd[4062]: Local user not found, try searching remote user
2019-06-18T15:30:33.797756+01:00 fac9 radiusd[4062]: Loaded remote ldap (regular bind) 10.100.88.5:636
2019-06-18T15:30:33.801800+01:00 fac9 radiusd[4062]: Try to bind with DN: CN=Joe Bloggs,CN=Users,DC=fortiad,DC=info
2019-06-18T15:30:33.802534+01:00 fac9 radiusd[4062]: Remote LDAP user password authenticated
2019-06-18T15:30:33.803118+01:00 fac9 radiusd[4062]: Partial auth done, challenge for token code
2019-06-18T15:30:33.803363+01:00 fac9 radiusd[4062]: Sending Access-Challenge.
2019-06-18T15:30:33.803371+01:00 fac9 radiusd[4062]: Updated auth log 'joe': Remote LDAP user authentication partially done, expecting FortiToken
2019-06-18T15:30:33.803373+01:00 fac9 radiusd[4062]: Waking up in 4.9 seconds.
2019-06-18T15:30:37.079454+01:00 fac9 radiusd[4062]: # Executing section authorize from file /usr/etc/raddb/sites-enabled/default
```

Initial user authentication (username and password)

```
2019-06-18T15:30:37.079465+01:00 fac9 radiusd[4062]: ===>NAS IP:10.100.88.136
2019-06-18T15:30:37.079466+01:00 fac9 radiusd[4062]: ===>Username:joe
2019-06-18T15:30:37.079468+01:00 fac9 radiusd[4062]: ===>Timestamp:1560868237.79263, age:0ms
2019-06-18T15:30:37.079470+01:00 fac9 radiusd[4062]: Found NAS from preloaded collections for 10.100.88.136: FG12 (10.100.88.136)
2019-06-18T15:30:37.079876+01:00 fac9 radiusd[4062]: Found NAS profile for client, NAS: 10.100.88.136 profile: Default
2019-06-18T15:30:37.080107+01:00 fac9 radiusd[4062]: Setting 'Auth-Type := FACAUTH'
2019-06-18T15:30:37.080112+01:00 fac9 radiusd[4062]: [pap] WARNING! No "known good" password found for the user.  Authentication may fail because of this.
2019-06-18T15:30:37.080113+01:00 fac9 radiusd[4062]: # Executing group from file /usr/etc/raddb/sites-enabled/default
2019-06-18T15:30:37.080115+01:00 fac9 radiusd[4062]: This is a response to Access-Challenge
2019-06-18T15:30:37.080116+01:00 fac9 radiusd[4062]: Partial auth user found
2019-06-18T15:30:37.080118+01:00 fac9 radiusd[4062]: Check if request contains FTM push trigger
2019-06-18T15:30:37.080119+01:00 fac9 radiusd[4062]: Request contains FTM push trigger
2019-06-18T15:30:37.080121+01:00 fac9 radiusd[4062]: Sending FTM push notification
2019-06-18T15:30:37.080122+01:00 fac9 radiusd[4062]: Initiate push_auth to FTK-Mobile client
2019-06-18T15:30:37.080123+01:00 fac9 radiusd[4062]: Sending request: [0][66][{"username": "joe", "user_agent": "RADIUS_CLIENT", "realm": "e:2"}]
2019-06-18T15:30:37.080555+01:00 fac9 radiusd[4062]: initiate_push_auth done: session_id=dc71e4b153f54a87b969038eea92644c
2019-06-18T15:30:37.080559+01:00 fac9 radiusd[4062]: Successfully found partially authenticated user instance.
2019-06-18T15:30:37.080710+01:00 fac9 radiusd[4062]: Hold request to wait for FTM push notification reply (request will be dropped after 30 sec)
2019-06-18T15:30:37.080718+01:00 fac9 radiusd[4062]: Updated auth log 'joe': Remote LDAP user authentication partially done (chosen FTM push notification), expecting FortiToken
2019-06-18T15:30:37.080719+01:00 fac9 radiusd[4062]: Waking up in 1.7 seconds.
2019-06-18T15:30:38.807505+01:00 fac9 radiusd[4062]: Waking up in 28.2 seconds.
2019-06-18T15:30:42.094527+01:00 fac9 radiusd[4062]: Waking up in 24.9 seconds.
2019-06-18T15:30:45.307701+01:00 fac9 radiusd[4062]: # Executing section authorize from file /usr/etc/raddb/sites-enabled/default
```

FortiAuthenticator is sending push notification to Google/iPhone Push Server and is waiting for a reply

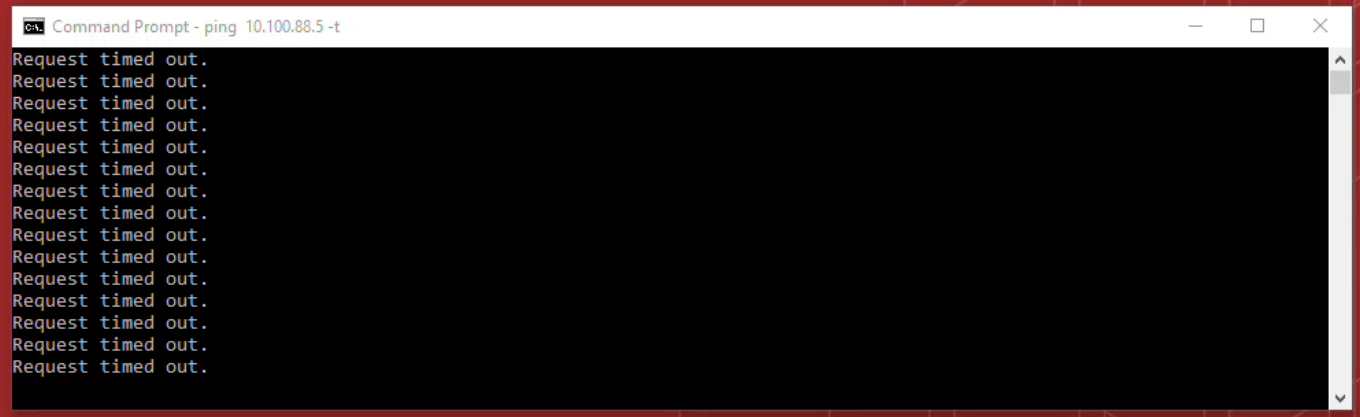
Проверка и диагностика

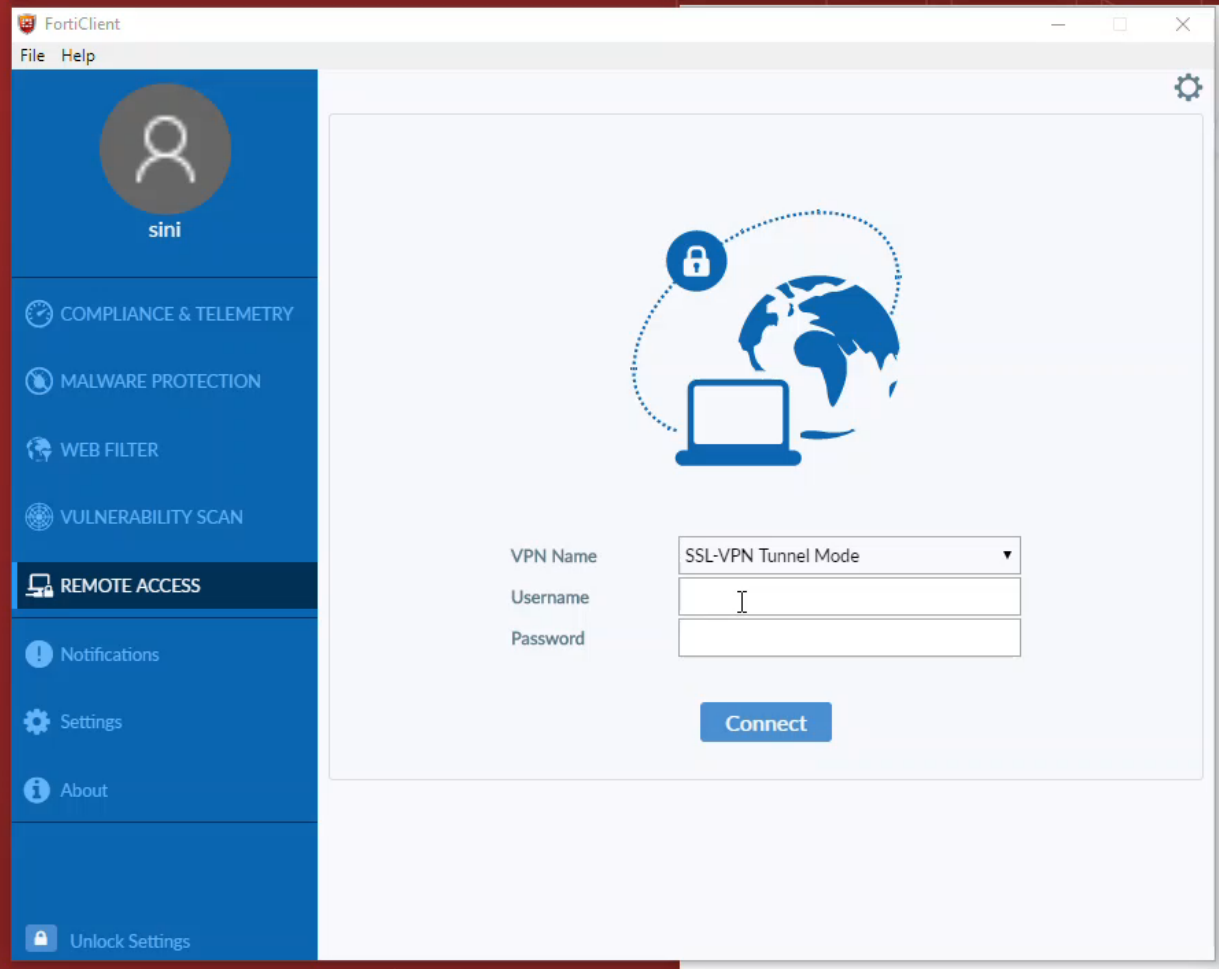
- FortiAuthenticator

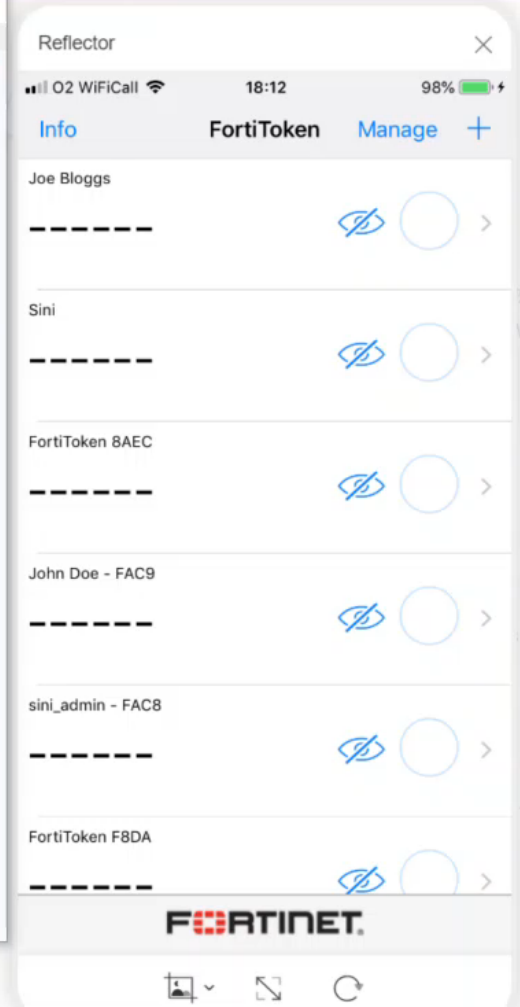
```
2019-06-18T15:30:45.307711+01:00 fac9 radiusd[4062]: ===>NAS IP:127.0.0.1
2019-06-18T15:30:45.307713+01:00 fac9 radiusd[4062]: ===>Username:joe
2019-06-18T15:30:45.307714+01:00 fac9 radiusd[4062]: ===>Timestamp:1560868245.307533, age:0ms
2019-06-18T15:30:45.307716+01:00 fac9 radiusd[4062]: Setting 'Auth-Type := FACAUTH'
2019-06-18T15:30:45.307717+01:00 fac9 radiusd[4062]: [pap] WARNING! No "known good" password found for the user.  Authentication may fail because of this.
2019-06-18T15:30:45.307719+01:00 fac9 radiusd[4062]: # Executing group from file /usr/etc/raddb/sites-enabled/default
2019-06-18T15:30:45.307720+01:00 fac9 radiusd[4062]: This is a response to Access-Challenge
2019-06-18T15:30:45.307722+01:00 fac9 radiusd[4062]: Trying to find FTM push auth user: joe session_id: dc71e4b153f54a87b969038eea92644c
2019-06-18T15:30:45.307723+01:00 fac9 radiusd[4062]: Partial auth user found
2019-06-18T15:30:45.307725+01:00 fac9 radiusd[4062]: Successfully found partially authenticated user instance.
2019-06-18T15:30:45.307829+01:00 fac9 radiusd[4062]: Switch to the original request from 10.100.88.136 id=67 to continue FTM push auth
2019-06-18T15:30:45.308885+01:00 fac9 radiusd[4062]: Update lastgood/drift successful
2019-06-18T15:30:45.308890+01:00 fac9 radiusd[4062]: Authentication OK
2019-06-18T15:30:45.308892+01:00 fac9 radiusd[4062]: Setting 'Post-Auth-Type := FACAUTH'
2019-06-18T15:30:45.309424+01:00 fac9 radiusd[4062]: Add Radius attribute: 809762817, SSLVPN
2019-06-18T15:30:45.309434+01:00 fac9 radiusd[4062]: Updated auth log 'joe': Remote LDAP user authentication with FortiToken successful (chosen FTM push notification)
2019-06-18T15:30:45.309436+01:00 fac9 radiusd[4062]: facauth: sending Access-Accept packet for FTM push auth to 10.100.88.136 port 13233, id=67, code=2, length=34
2019-06-18T15:30:45.309437+01:00 fac9 radiusd[4062]: # Executing section post-auth from file /usr/etc/raddb/sites-enabled/default
2019-06-18T15:30:45.309439+01:00 fac9 radiusd[4062]: Waking up in 4.9 seconds.
2019-06-18T15:30:50.315542+01:00 fac9 radiusd[4062]: Waking up in 16.7 seconds.
2019-06-18T15:31:07.099493+01:00 fac9 radiusd[4062]: Ready to process requests.
```

Final stage upon receiving a push notification from the client

Демонстрация


Command Prompt - ping 10.100.88.5 -t
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.


FortiClient
File Help
sini
COMPLIANCE & TELEMETRY
MALWARE PROTECTION
WEB FILTER
VULNERABILITY SCAN
REMOTE ACCESS
Notifications
Settings
About
Unlock Settings
VPN Name
SSL-VPN Tunnel Mode
Username
Password
Connect


Reflector
O2 WiFiCall
18:12
98%
Info
FortiToken
Manage
Joe Bloggs
Sini
FortiToken 8AEC
John Doe - FAC9
sini_admin - FAC8
FortiToken F8DA
FORTINET


FORTINET