Управление доступом пользователей к корпоративным ресурсам с FortiAuthenticator

Андрей Гиль

системный инженер

cis_se@fortinet.com (инженерная команда)

О чем пойдет речь…

- Обзор возможностей FortiAuthenticator
- Модели и лицензирование
- Отказоустойчивость системы
- Что такое FSSO. Методы FSSO
- Двухфакторная аутентификация
- Возможности FortiAuthenicator по управлению сертификатами
- 802.1x на примере доступа в сеть WiFi
- SAML
- Демонстрация

FortiAuthenticator

Обзор возможностей

Сегодня сеть не имеет границ

Установление личности - краеугольный камень политики безопасности

Управление идентификацией и доступом:

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

Неправильное использование учетных данных и привилегий может стать причиной взлома

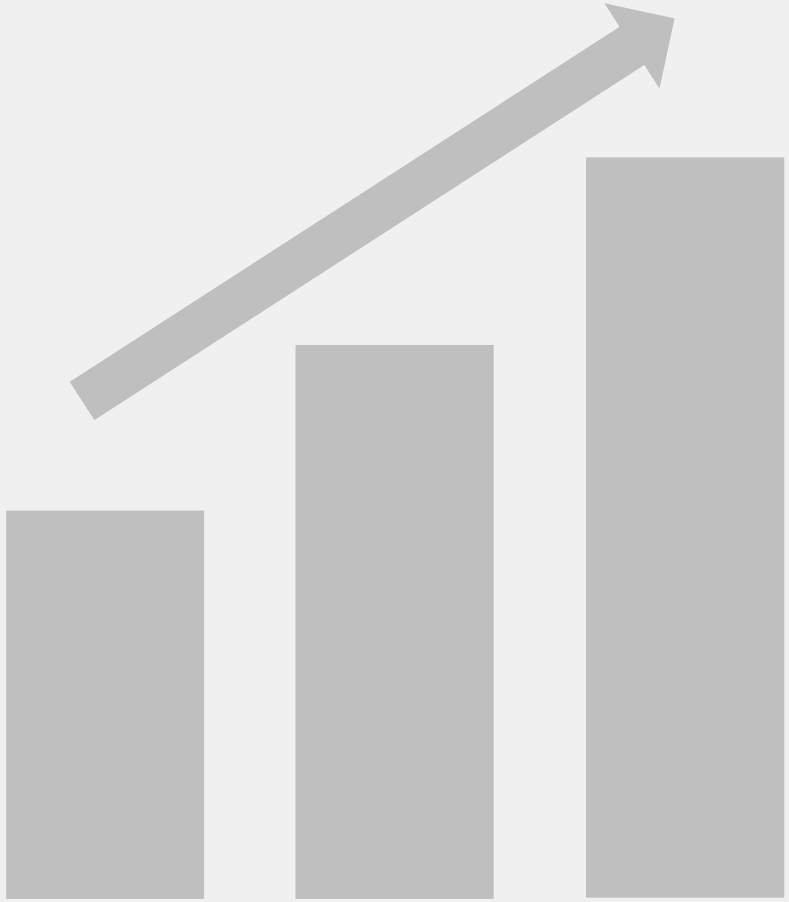
Слабая аутентификация и неправильное управление доступом делают сеть уязвимой

Насколько безопасна аутентификация по паролю?

Неправильное управление приводит к нарушениям…

81%

нарушений в результате использования украденных учетных данных



Источник: Verizon 2020 Data Breach Investigation Report

Fortinet Security Fabric

Прозрачность

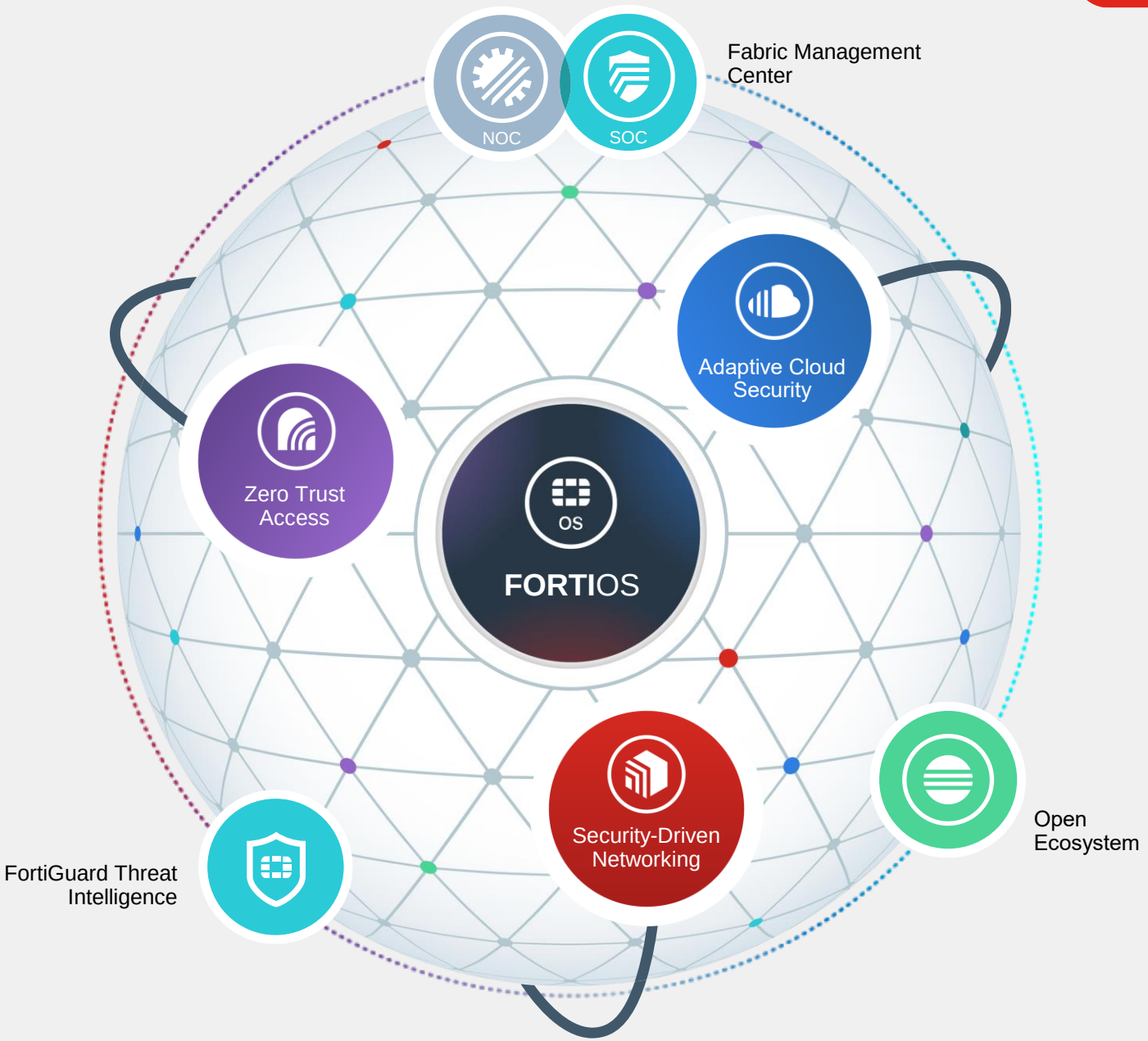
Полная видимость атакуемой поверхности для лучшего управления рисками ИБ

Комплексность

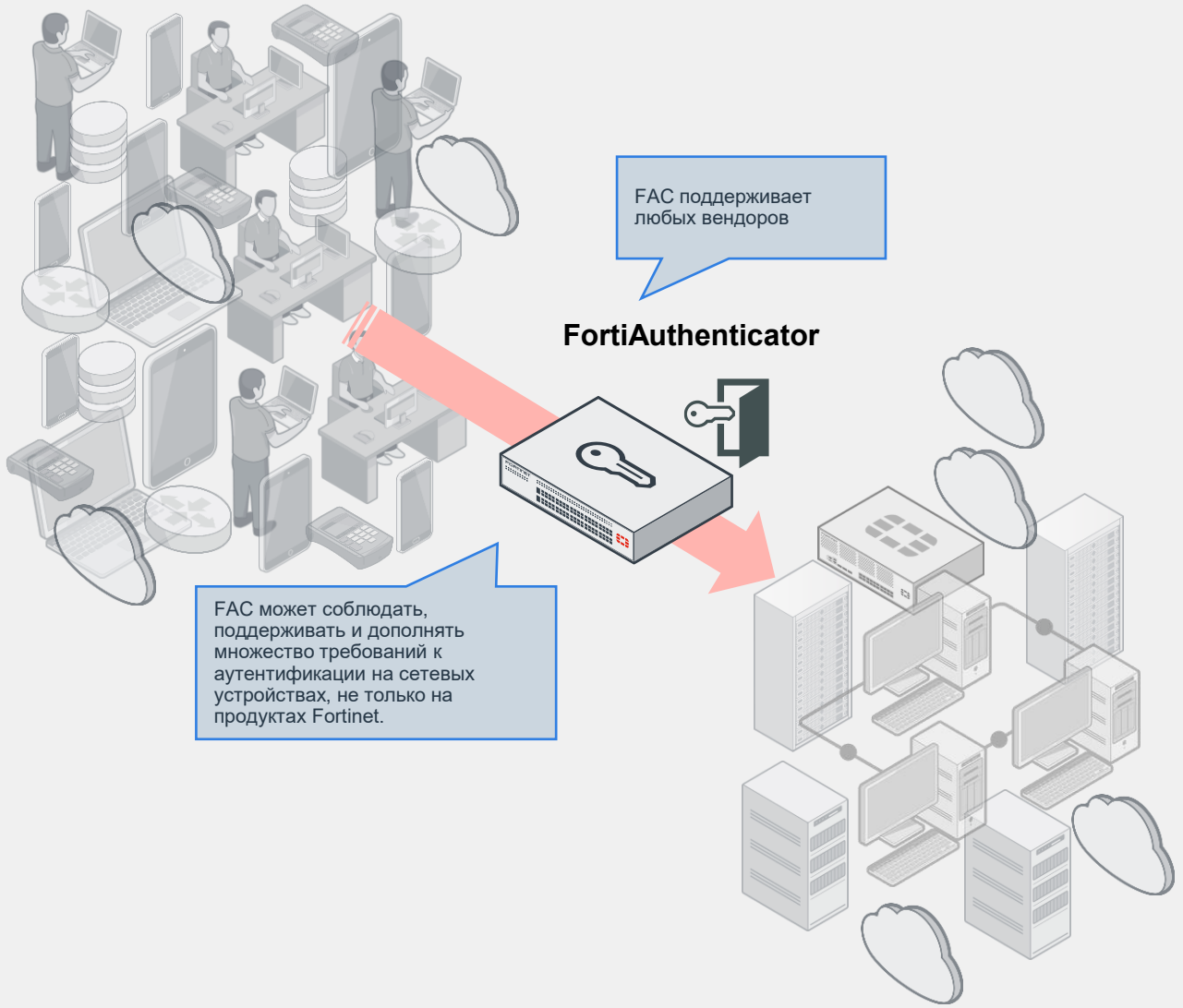
Снижение стоимости эксплуатации за счет объединения всех компонентов в рамках единой платформы

Автоматизация

Самостоятельная инфраструктура под управлением искусственного интеллекта

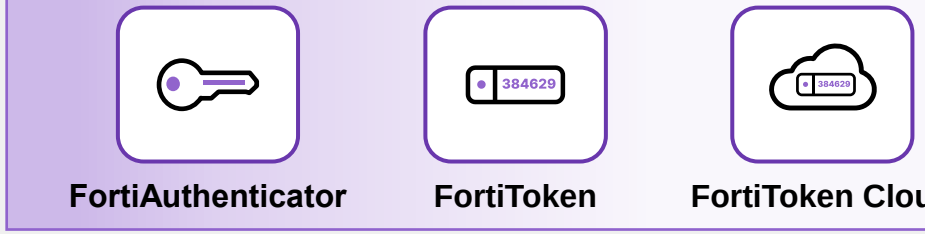


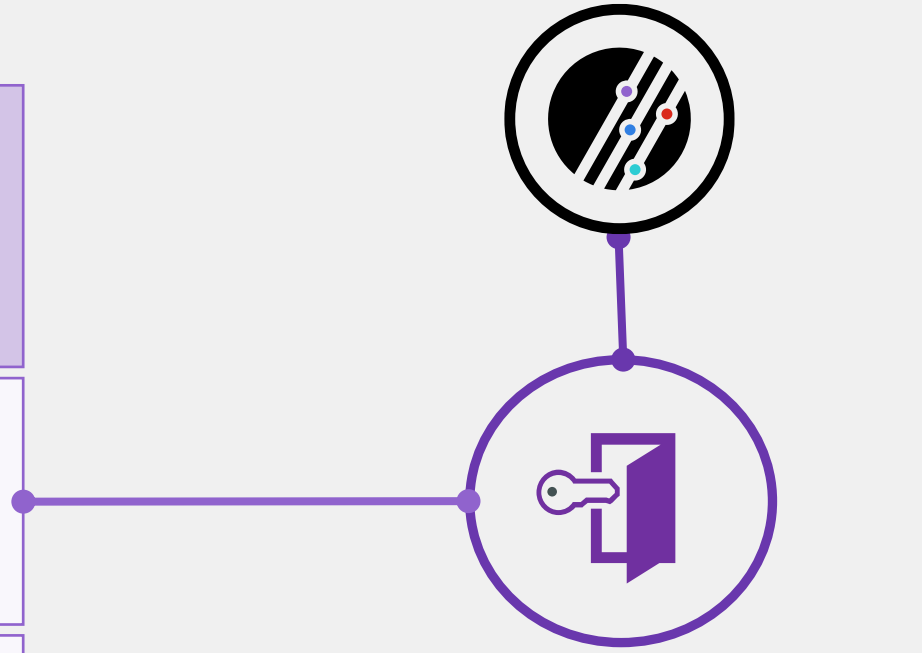
FortiAuthenticator



Fortinet Identity и Access Management (IAM)

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





Identity Access and Management

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

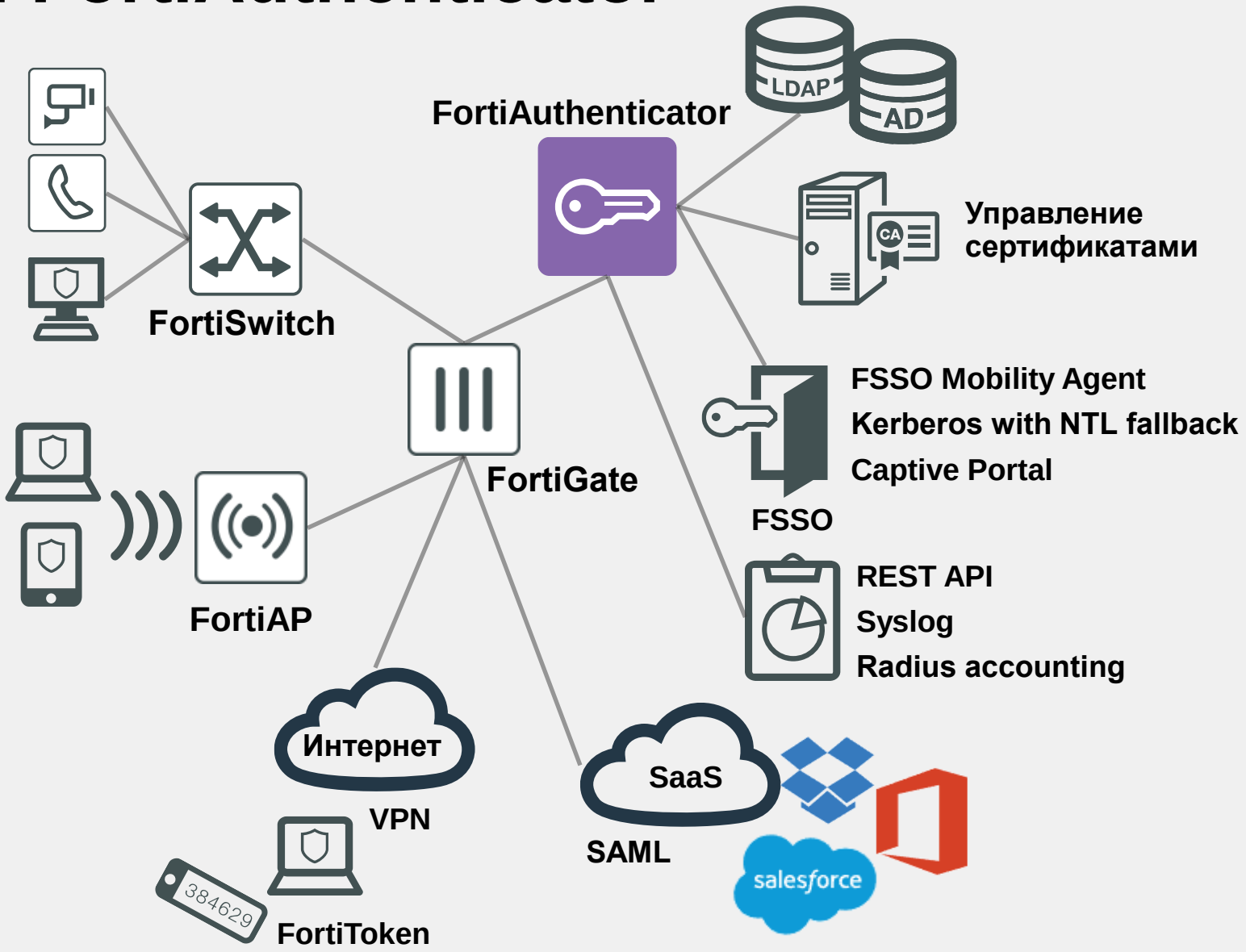
Обзор возможностей FortiAuthenticator

Идентификация и аутентификация
- RADIUS, LDAP, TACACS+, SAML
- AD, Kerberos, FSSO агент
- Captive портал
- REST API

Двухфакторная аутентификация
- FortiToken, физический/программный
- SMS/email

Управление сертификатами
- X.509 Certificate подпись/отзыв
- Удаленные устройства/автоматическая аутентификация

Поддержка IEEE 802.1X
- Аутентификация при доступе к проводными и беспроводным сетям



Fortinet IAM

Упрощение контроля доступа и предоставляемых прав для каждого пользователя

Функционал

Authentication и authorization

Централизованное управление, различные методы аутентификации: проводная, беспроводная, VPN, веб-аутентификация (SAML, oAuth)

Adaptive, strong authentication

Атрибуты доступа пользователя (местоположение, время, сеть) и многофакторная аутентификация

Удобство использования

Вход без пароля, система единого входа, портал самообслуживания

Гибкая, отказоустойчивая и масштабируемая платформа

Поддержка современных технологических тенденций и вариантов развертывания

Преимущества

Включает эффективную политику безопасности и средства управления

Контроль доступа на основе ролей, снижение рисков и упрощение оценки рисков

Повышенная безопасность

Проверка личности, доступ с минимальными привилегиями

Простота использования, снижение затрат на ИТ-поддержку

Снижение усталости пользователей от входа в систему, повышение производительности, оптимизация эксплуатационных расходов на ИТ

Защита инвестиций

Appliance, VM, cloud (private, public), до 1 млн пользователей, обширные партнеры по экосистеме; Высокая доступность и балансировка нагрузки

FortiAuthenticator

Модельный ряд и лицензирование

Варианты исполнения FortiAuthenticator

FortiAuthenticator 300F

Mid Enterprise/Service Provider Deployments

- Support up to 1,500 users
- HDD - 2 X 1TB
- 4 x 10/100/1000 RJ45 ports
- 2 x SFP
- Rack Mountable, 1U
- Optional Dual AC PSU

FortiAuthenticator 800F

Large Enterprise/Service Provider Deployments

- Support up to 8,000/18,000 users
- HDD - 2 X 2TB
- 4 x 10/100/1000 RJ45 ports
- 2 x SFP
- Rack Mountable, 1U
- Dual AC PSU

FortiAuthenticator VM

All Sized Deployments from SME to Service Provider Deployments

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

*** Все Non Hardware поддерживают полностью наращиваемое пользовательское лицензирование**

User Count	Appliance		Virtual Machine
	300F	800F	
100	✓	✓	✓
Stackable	1,500 base	8,000 base	100 base
3,500	MAX		
18,000		MAX	
20,000			
40,000			
1,000,000 Plus			MAX
Upgrade			
100	✓	✓	✓
1,000	✓	✓	✓
10,000		✓	✓

Лицензирование FortiAuthenticator 1/2

- Лицензируется по числу пользователей (User license)
- Для сценария FSSO only также необходимы User license
- HW модель базово 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 FortiAuthenticator 2/2

- Для HA одинаково лицензированы должны быть оба устройства
- 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 два устройства кластера)
- Windows Domain Two Factor Authentication Agent не лицензируется

FortiAuthenticator

Высокая доступность (HA)

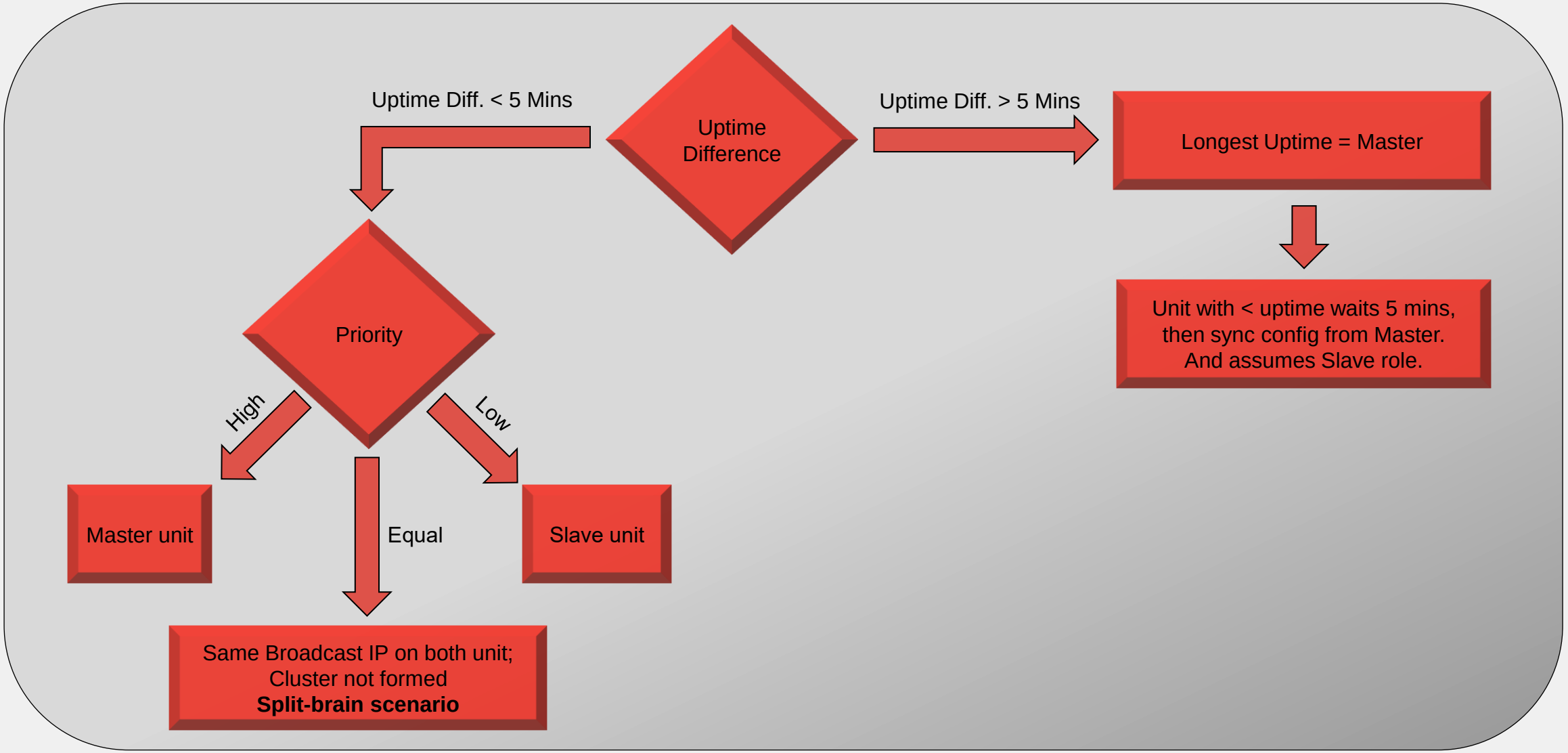
Сценарии высокой доступности

Active/Passive (Redundant)	Active/Active (Load balancing)
Одно устройство primary, остальные standby	Primary кластер может резервироваться на другие
Standby отслеживает состояние primary через HA интерфейс	
Необходимо взаимодействие на Layer 2 между устройствами	Необходимо взаимодействие на Layer 3
Failover занимает некоторое время, синхронизируется все	**Синхронизация только для: token, local user database, group mappings, token/user mapping**

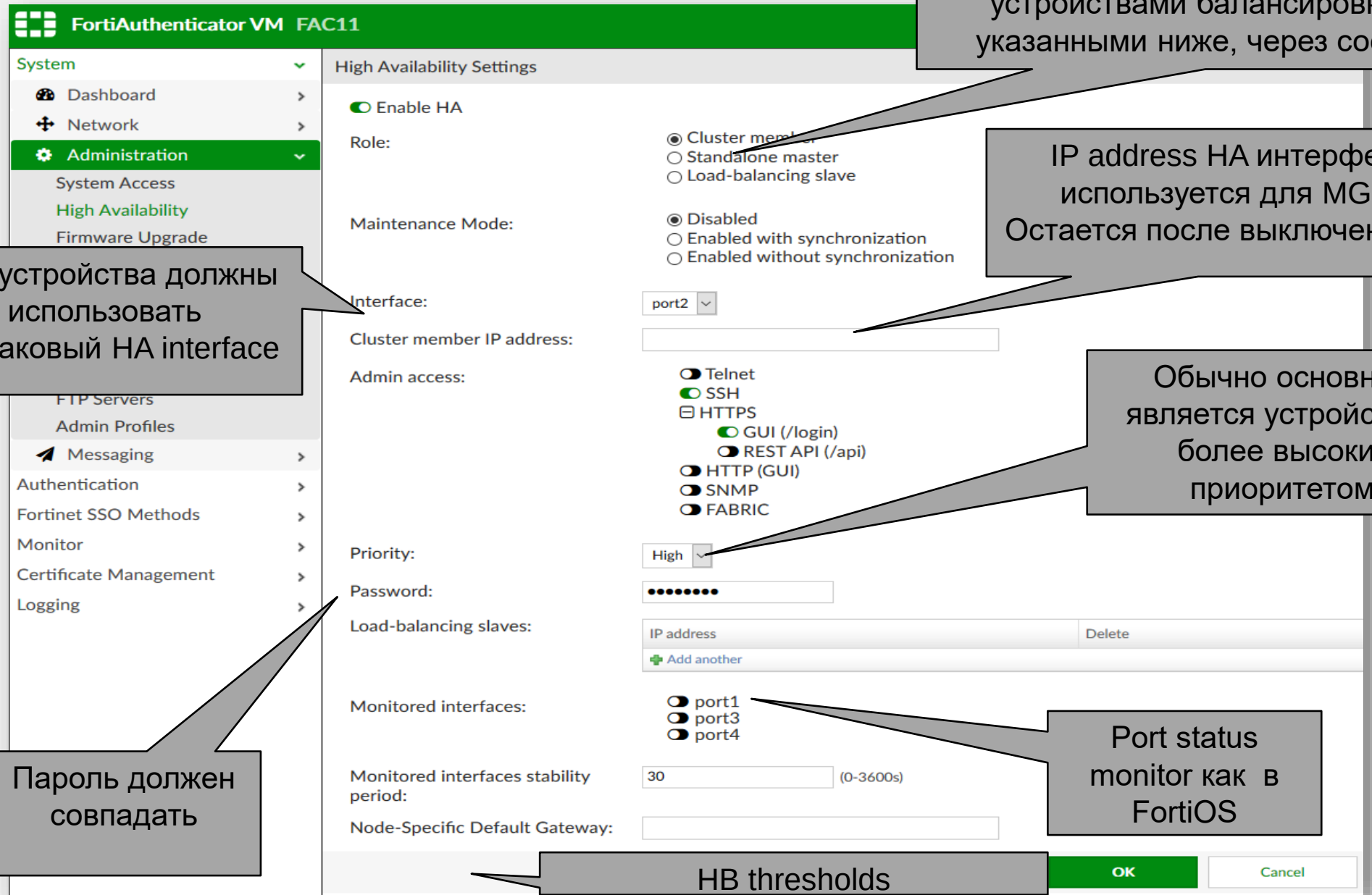
Требования к высокой доступности (HA)

Active/Passive (Redundant)	Active/Active (Load balancing)
Платформы должны быть одинаковые	Платформы могут отличаться
ПО должно быть одной версии	ПО должно быть одной версии
Лицензия User License должны быть одинаковые	Лицензия User License могут отличаться
Лицензии Token License – одна на кластер	**Лицензии Token License – одна на кластер**

Master/Slave определение



High Availability (A/P) configuration



Standalone Master поддерживает A-P или обменивается данными с 10 подчиненными устройствами балансировки нагрузки, указанными ниже, через соединение L3

IP address HA интерфейса используется для MGMT. Остается после выключения HA!

Оба устройства должны использовать одинаковый HA interface

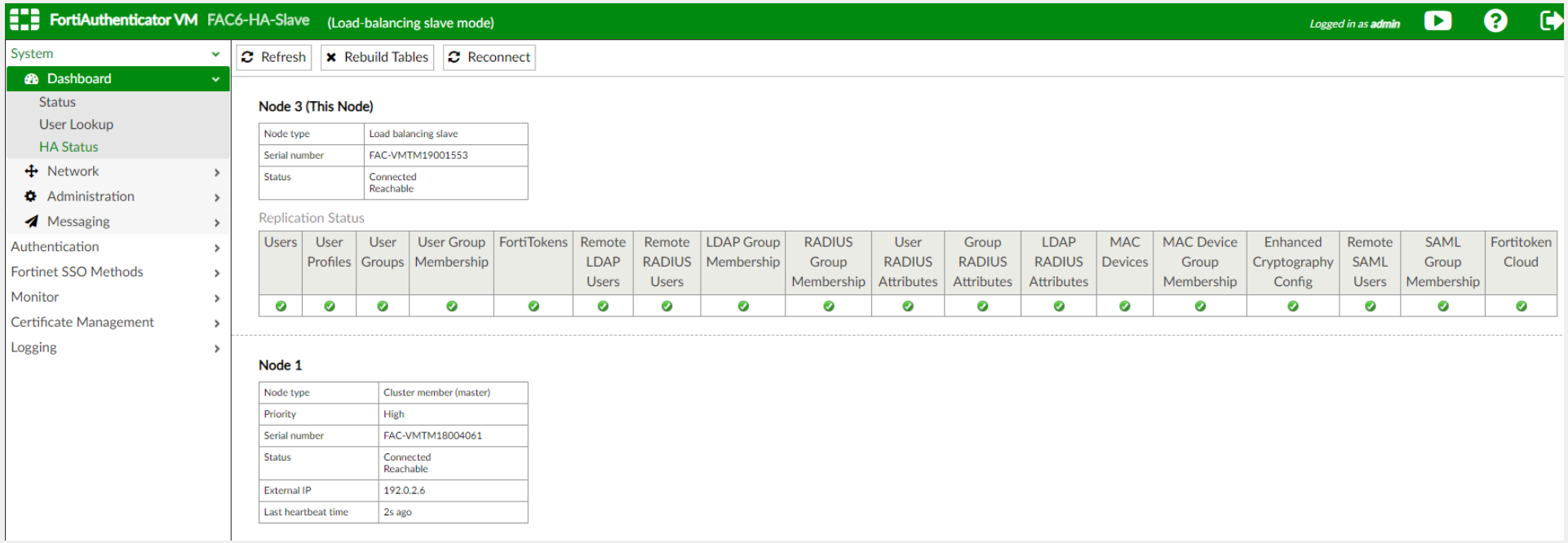
Обычно основным является устройство с более высоким приоритетом.

Пароль должен совпадать

Port status monitor как в FortiOS

HB thresholds

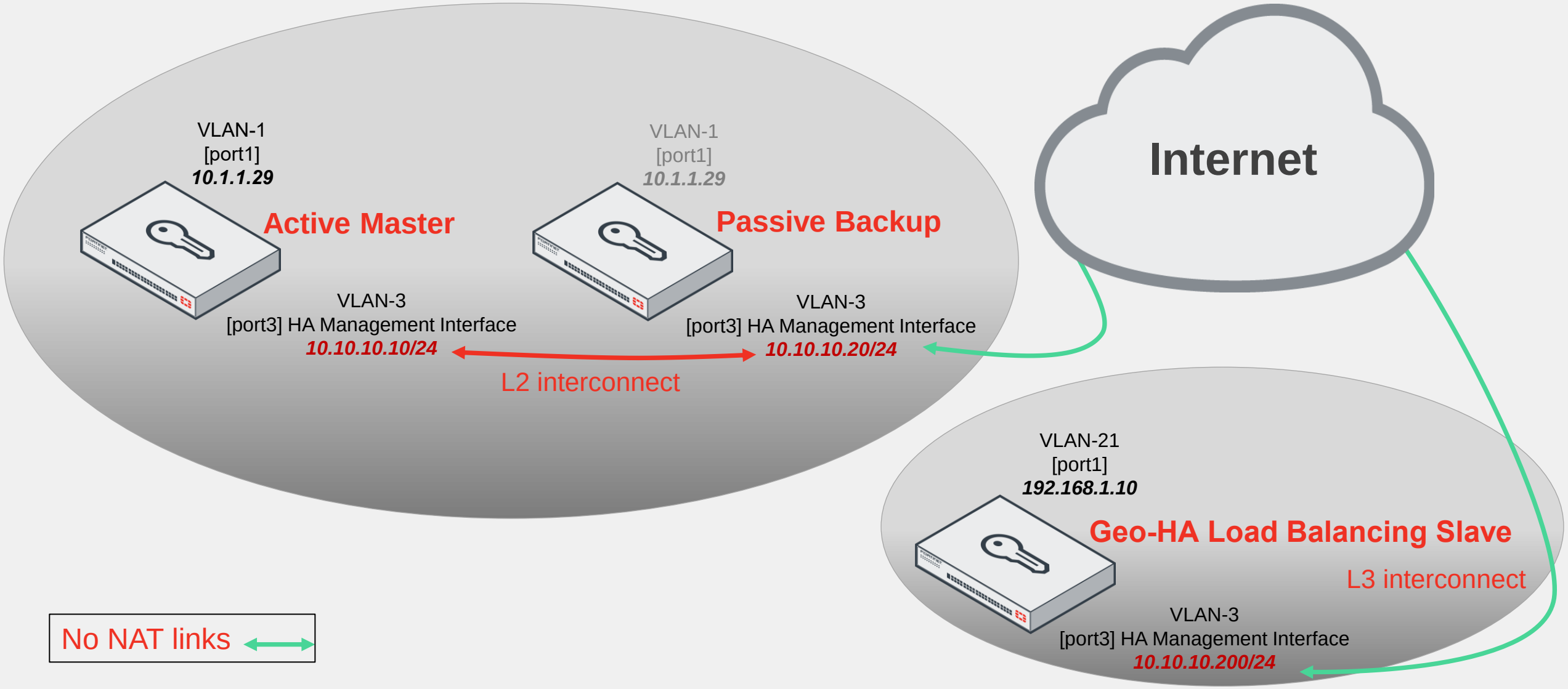
HA проверка состояния



Посмотреть статус в GUI:

→ GUI / System / Dashboard / HA Status для просмотра sync status синхронизируемых данных

Active/Pasive плюс Geo-HA в удаленных филиалах

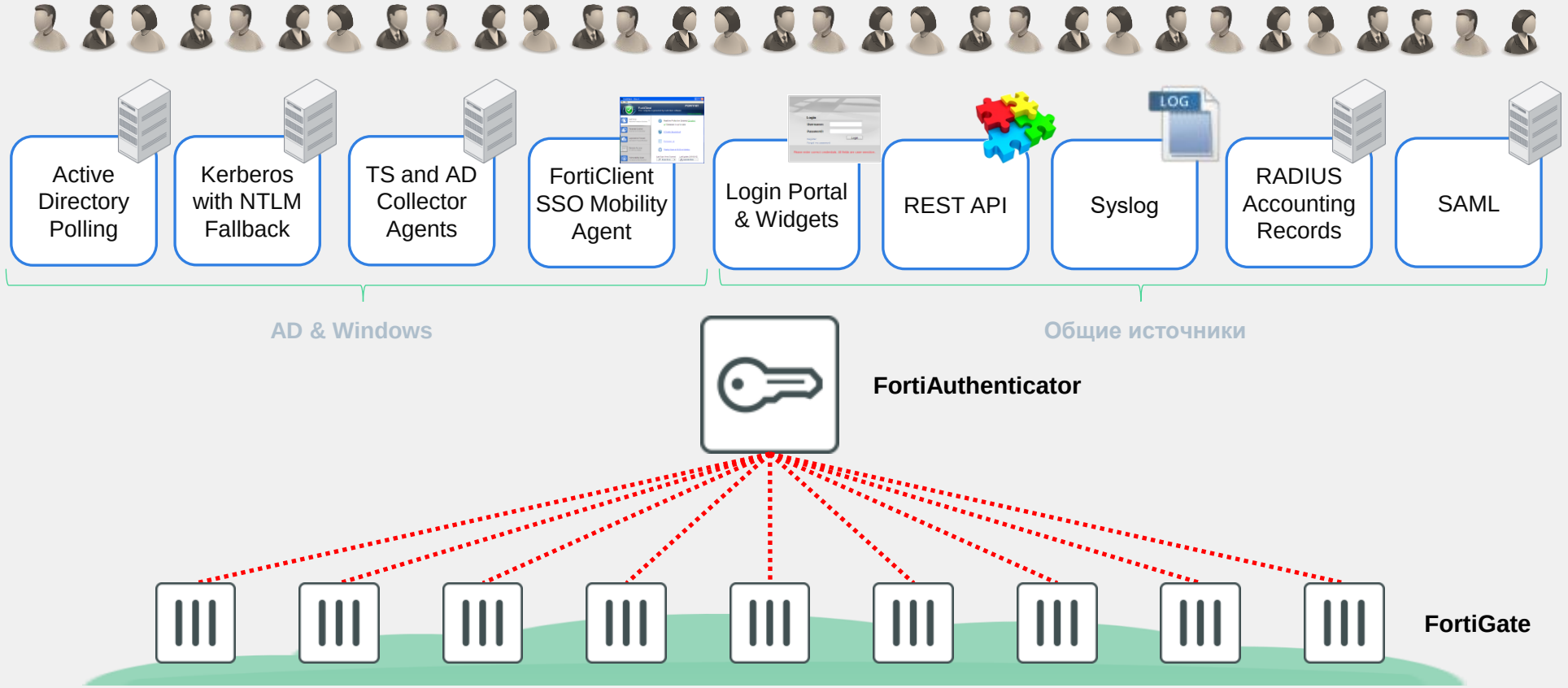


FortiAuthenticator

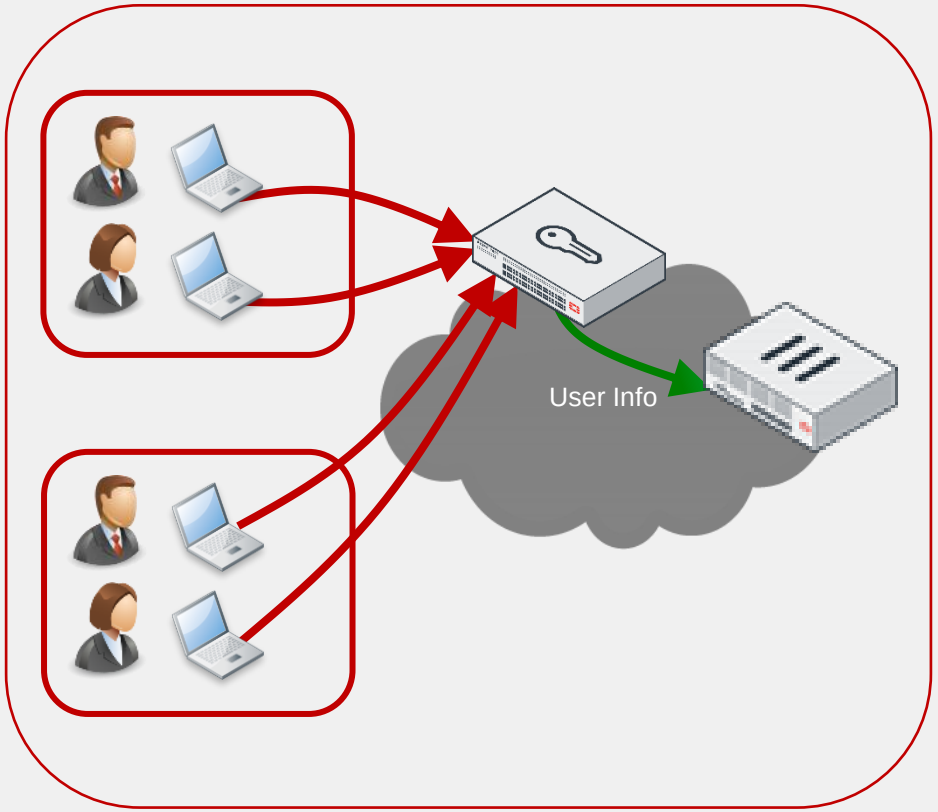
FSSO

Fortinet Single Sign-On – (FSSO)

Источники идентификации пользователя, используемые в качестве первичных данных для пассивной аутентификации.



FortiAuthenticator FSSO – SSO Mobility Agent

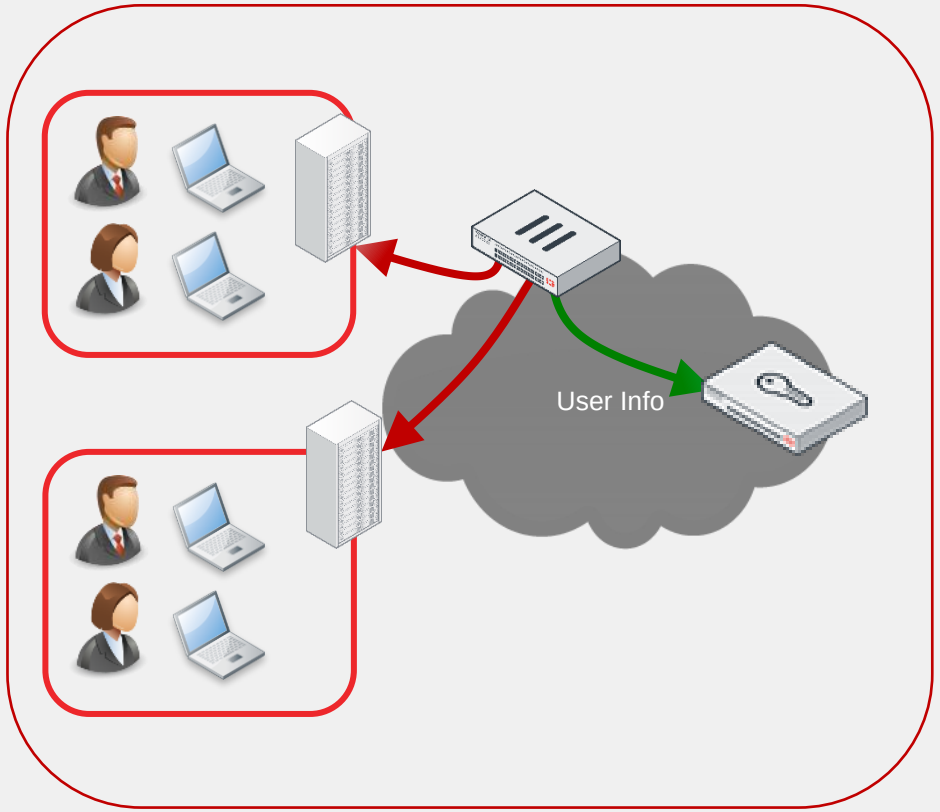


Лучшая масштабируемость и обнаружение выхода из системы

SSO Mobility Agent

- FortiClient User Identification
  - Обнаруживает login/logout/IP изменения
  - Отправляет hello packets регулярно для обнаружения выключения, гибернации и тд
  - Standalone (background service installer возможен)
- Самый масштабируемый FSSO ID Method
- Поддерживает multiple forests, domains и cross domain группы

FortiAuthenticator FSSO – Active Directory Polling



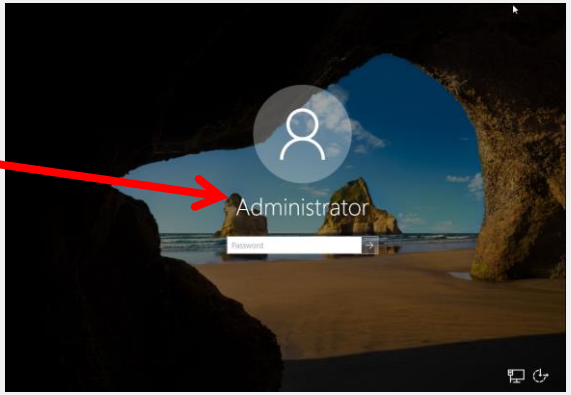
Active Directory Polling

- WinSec (Windows Security Event Logs)
  - 5 second polling
  - Event IDs - 672, 680, 4776 and 4768
  - Дополнительные IDs – 528, 540, 4624 (MacOS)
- WMI (инструментарий управления **Windows**)
  - 5 second polling
  - Требует открытие портов на Windows FW tcp ports 135&445
- NetApi

FortiAuthenticator FSSO – DCAgent

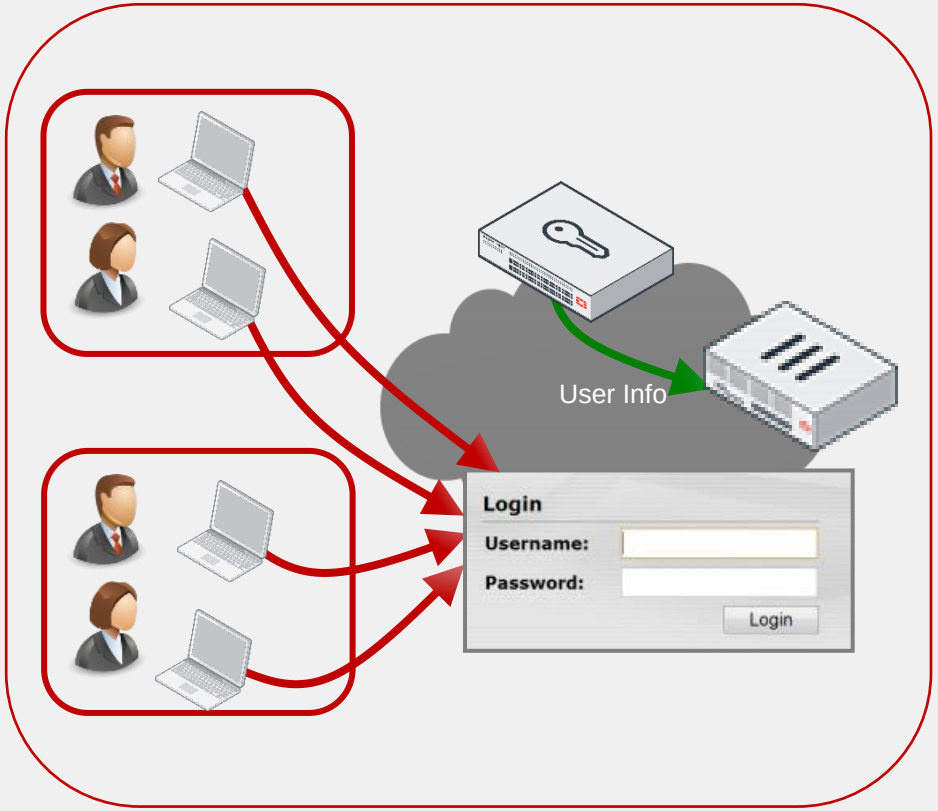
- Самый старый метод - наименее требовательный и надежный

- DCAgent - это DLL, работающая в контексте службы LSAAS.
  - пакет дополнительной аутентификации
  - срабатывает всякий раз, когда пользователь входит в систему с использованием «интерактивного входа»



  - Работает синхронно (lsass ожидает завершения)
    - разбирает имя пользователя, рабочую станцию, домен
    - Resolve имена рабочих станций
    - отправляет пакет уведомления о входе udp / 8002 на все * настроенные * FSSO CA

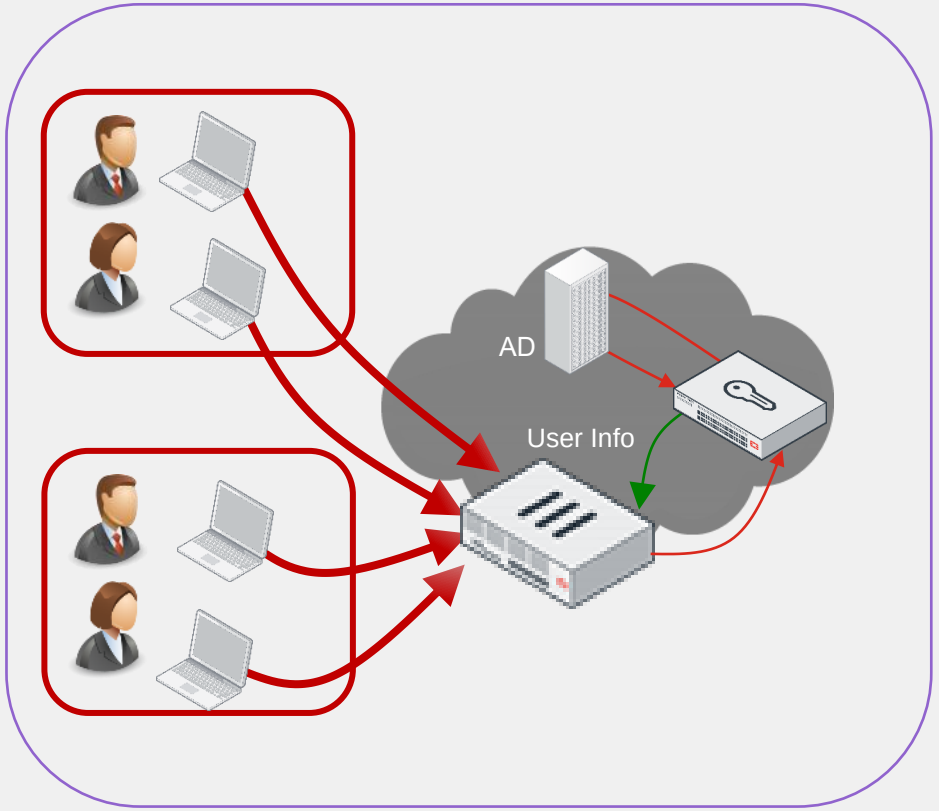
FortiAuthenticator FSSO – Портал и Widget



Портал Authentication и Widgets

- Captive login портал для ручной аутентификации
  - Отлавливает системы, не поддерживаемые другими методами
  - Виджеты могут быть встроены в домашнюю страницу интрасети организации.
  - Пользовательский «токен» хранится в cookie для идентификации пользователя при последующем доступе (действителен до 30 дней)

FortiAuthenticator FSSO – Kerberos SSO



- Перенаправить неаутентифицированных пользователей с FortiGate на FortiAuthenticator
- FortiAuthenticator запрашивает сервисный ticket
- Браузер получает ticket от Ticket Granting Service и пересылает его в FortiAuthenticator
- FortiAuthenticator расшифровывает и использует ticket для проверки личности пользователя

FortiAuthenticator

Двухфакторная аутентификация (2FA)

FortiToken двухфакторная аутентификация (2FA)

FortiToken

Identity and Access Management

Различные варианты токенов, простые в использовании и развертывании

- FortiToken Mobile app упрощает вход до одного клика
- Hardware tokens подходит для всех случаев использования
- Простота внедрения и развертывания
- Perpetual licensing, отсутствие текущих сборов за локально управляемые FortiTokens.

Варианты исполнения FortiToken

FortiToken Mobile

Multi platform OATH OTP application with push notification of login attempts and one tap approval

FortiToken 300

Driverless USB Device
FIPS-140 compliant
Economical PKI authentication

FortiToken 220

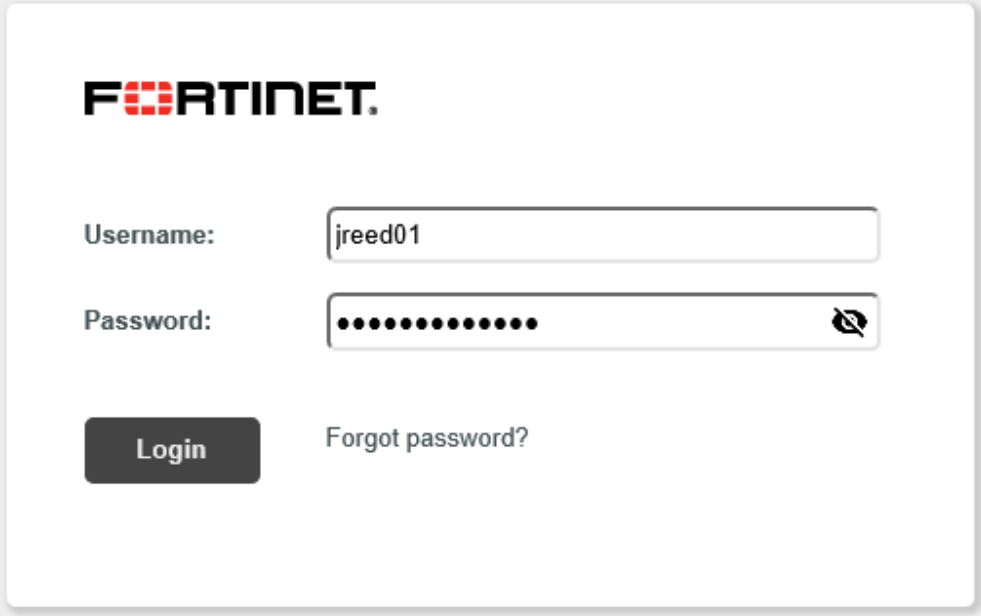
The FortiToken 220 OTP token is a mini credit card form factor token. There is also a companion tool for Android devices on Google Play that allows users to reprogram the token seed*.

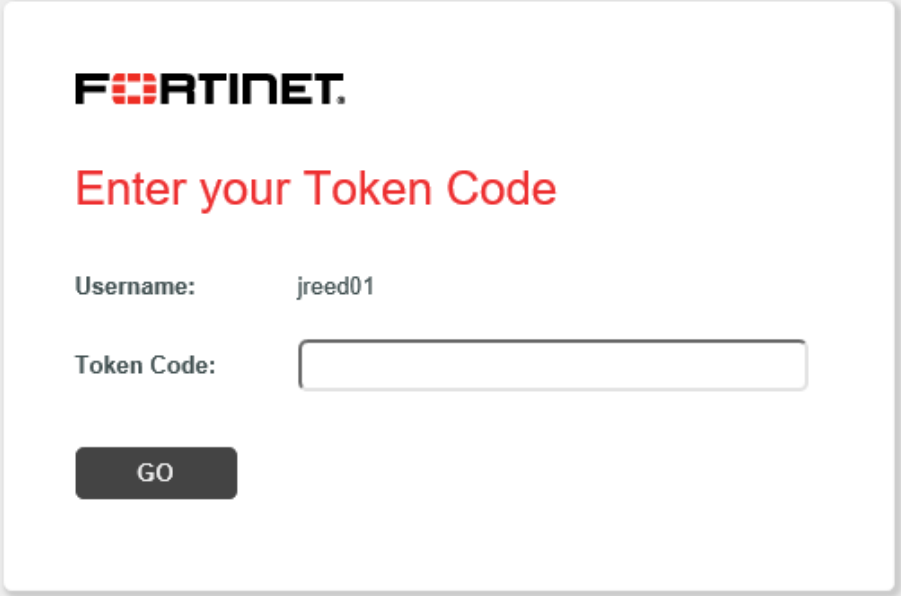
FortiToken 200/200CD

Durable, large display, OATH OTP token with FortiGuard activation or optional encrypted activation file.

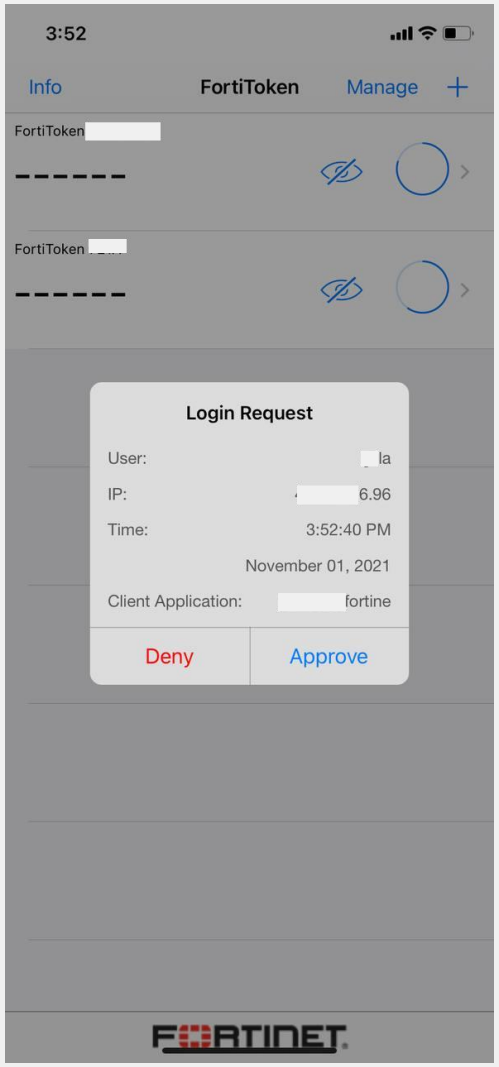
FortiAuthenticator Captive Portal

Служба портала позволяет вам предоставлять удаленным пользователям доступ к определенным частям вашей сети с использованием делегированной аутентификации.



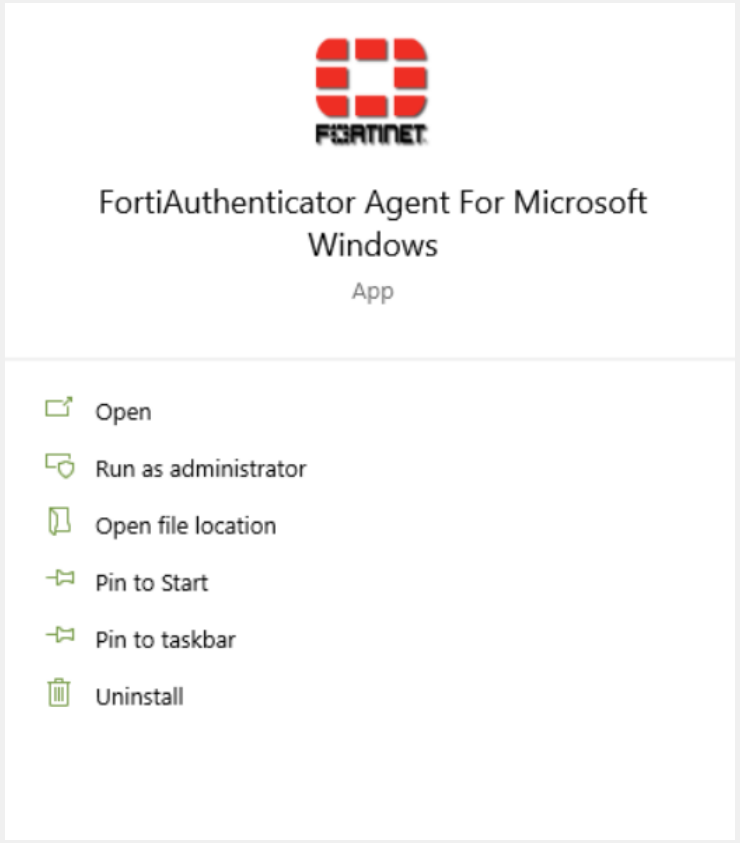


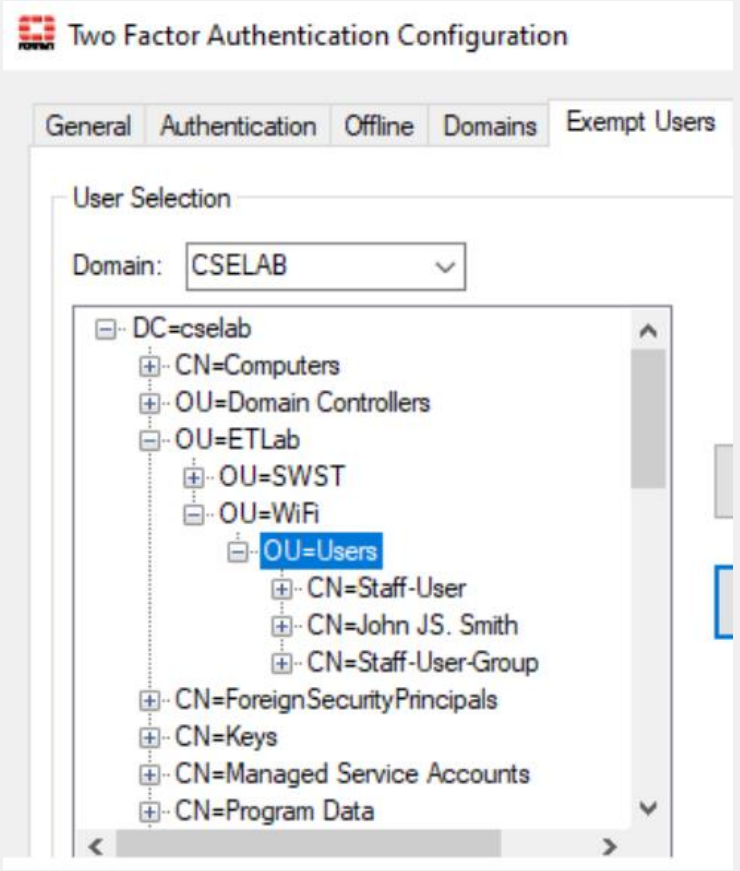
PUSH-уведомления

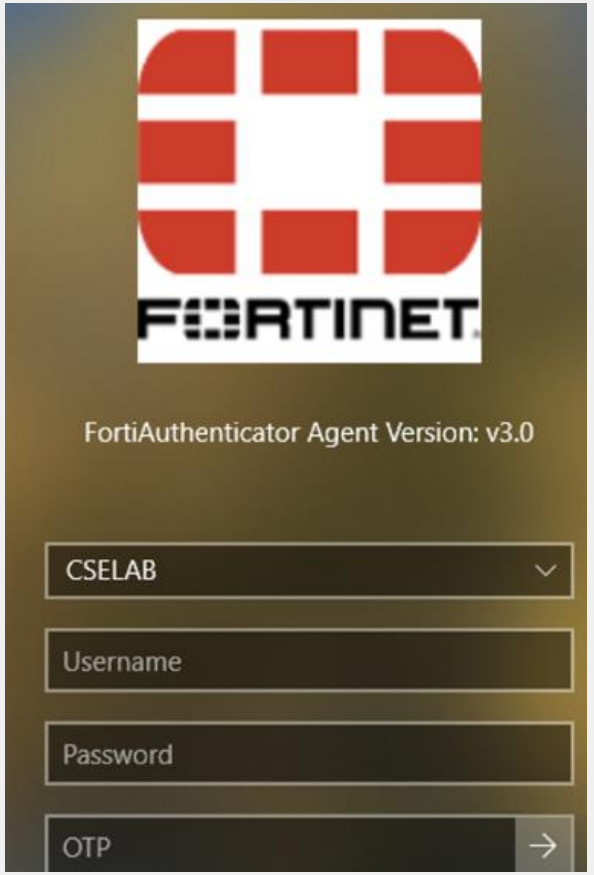


- PUSH-уведомления используются для отправки предупреждений на устройство конечного пользователя каждый раз, когда делается запрос на вход. Предупреждение содержит информацию о попытке входа в систему, например, местоположение, из которого была совершена попытка.
- Используя PUSH, когда требуется аутентификация, пользователям FortiToken Mobile не нужно открывать код в FortiToken и вводить его в свой браузер.
- Вместо этого отправляется запрос FortiToken Mobile, и пользователь просто нажимает на него, чтобы утвердить или отклонить запрос.
- В случае утверждения новый OTP автоматически создается и отправляется FortiToken Mobile для прозрачной аутентификации конечного пользователя в фоновом режиме.
- В случае отказа FortiToken Mobile автоматически отправляет уведомление системному администратору.

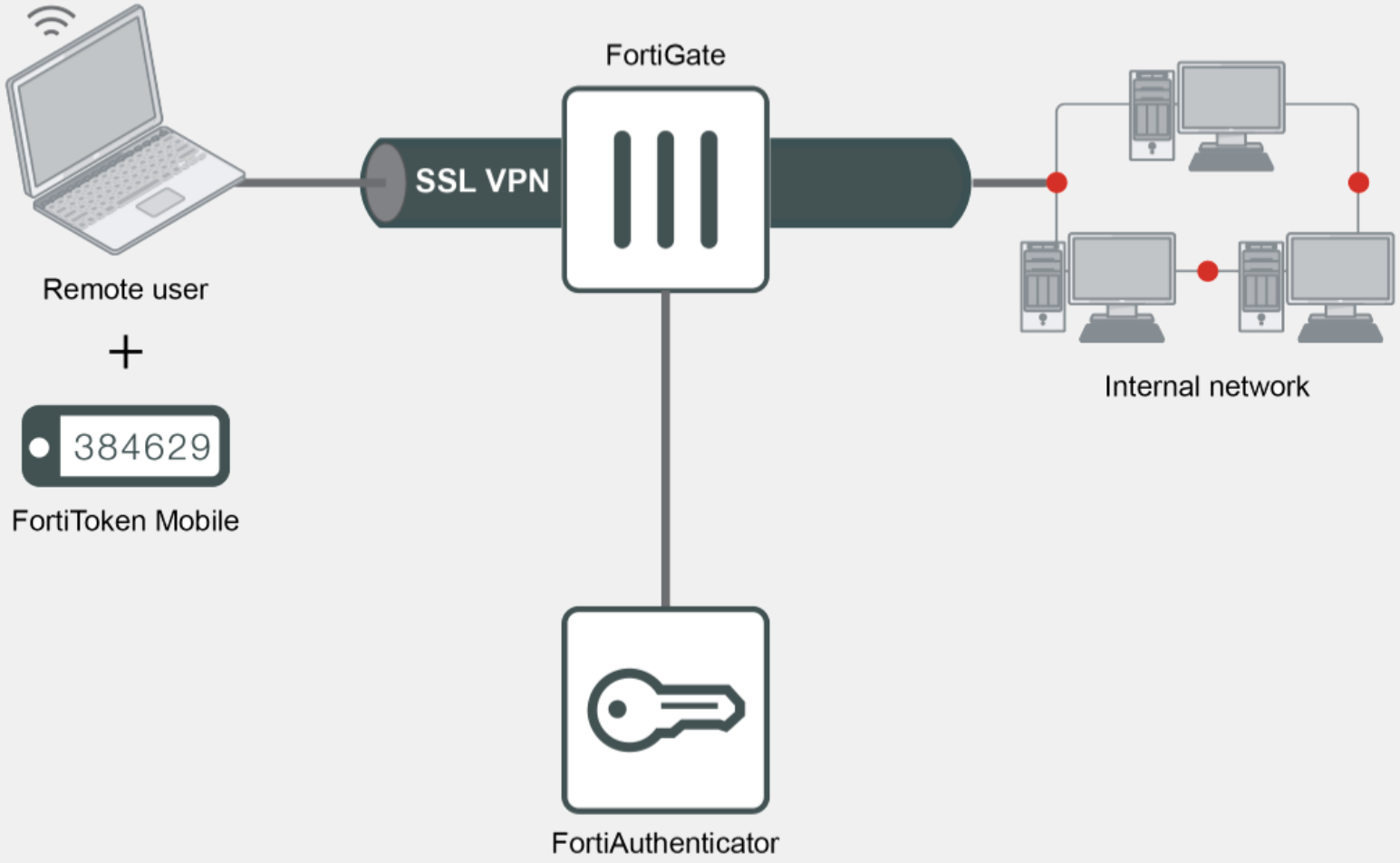
FortiAuthenticator Agent для Microsoft Windows



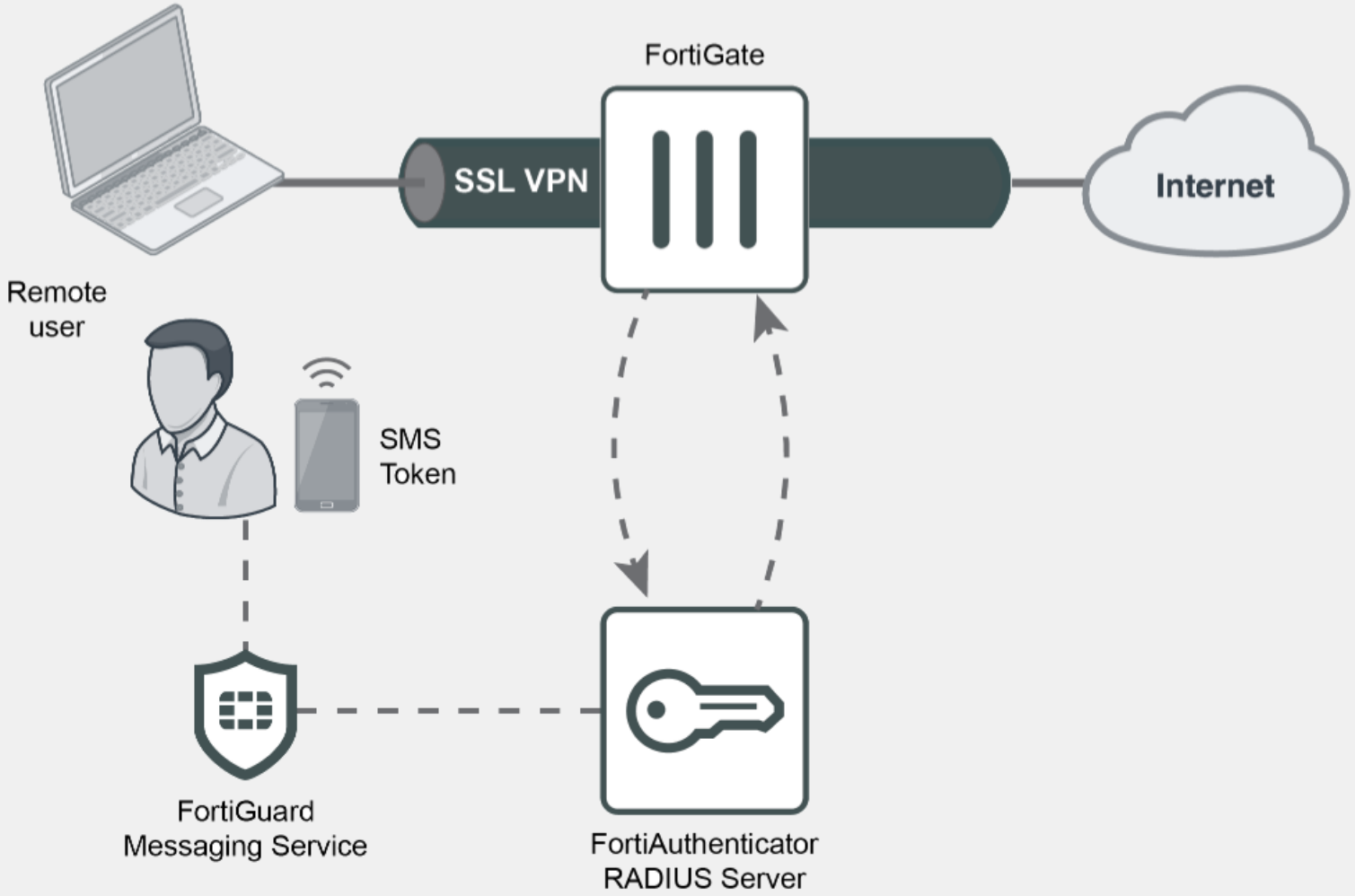




Пример. SSL VPN + 2FA (FortiToken)



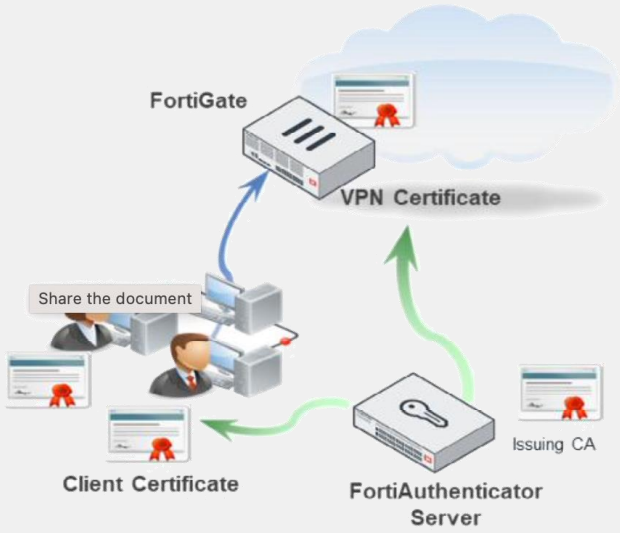
Пример. SSL VPN + 2FA (SMS)



FortiAuthenticator

Управление сертификатами

FortiAuthenticator – Центр Сертификации



FortiAuthenticator может действовать как самозаверяющий или локальный центр сертификации для создания, подписания и отзыва сертификатов X.509, таких как сертификаты сервера для HTTPS и SSH и клиентские сертификаты для HTTPS, SSL и IPsec VPN.

Эти сертификаты могут использоваться для проверки подлинности VPN, проверки подлинности 802.1X, проверки подлинности Windows, проверки подлинности на основе токенов и других задач.

FortiAuthenticator – Центр Сертификации

FortiAuthenticator может действовать как SCEP сервер для:

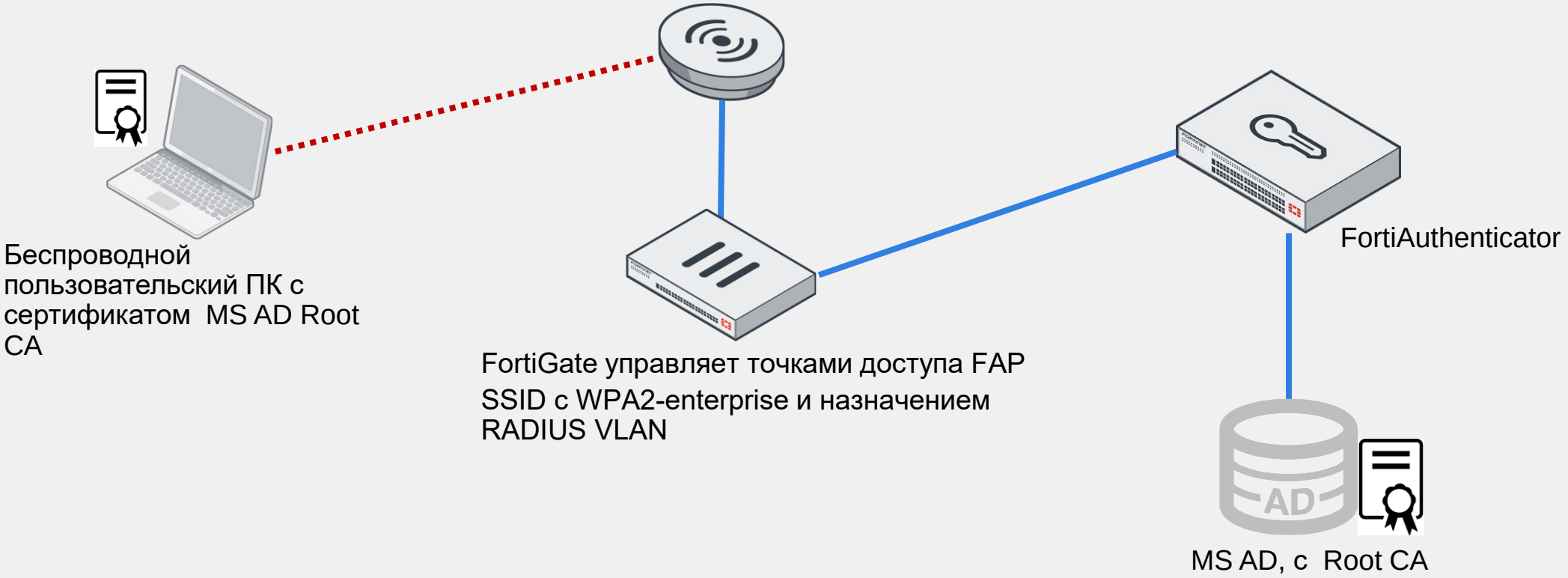
- Подписания пользовательских CSRs
- Распространения CRLs
- Распространения CA сертификатов

FortiAuthenticator может вставлять OCSP (Online Certificate Status Protocol) URLs для проверки статуса сертификата

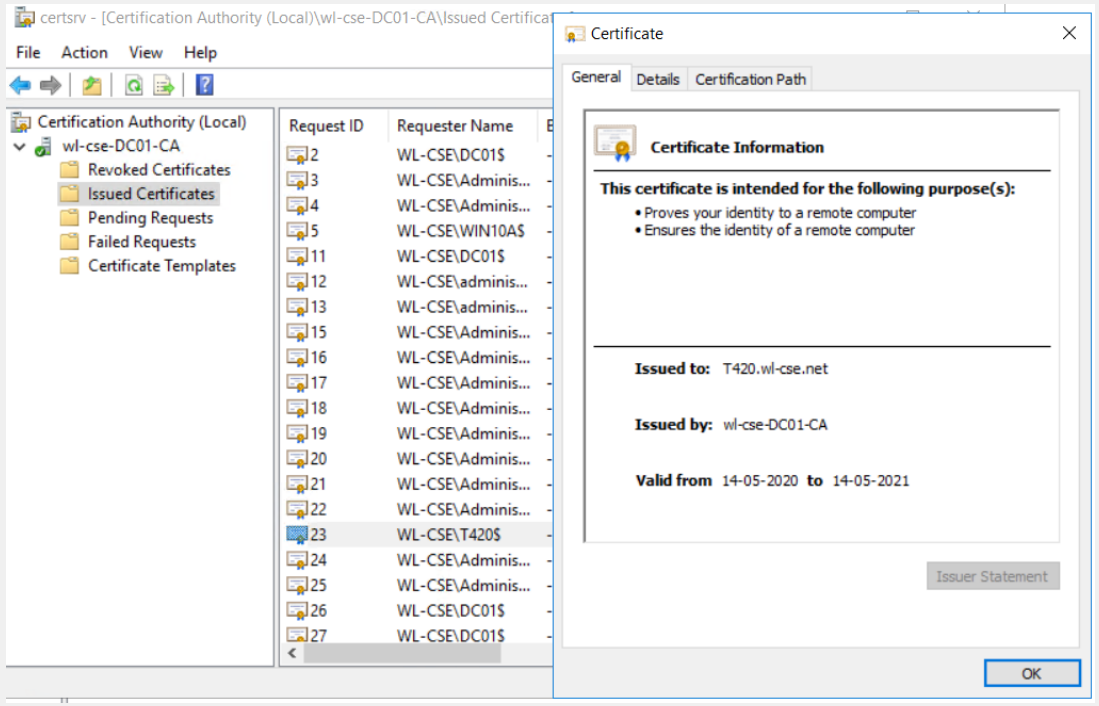
FortiAuthenticator

ПРИМЕР – 802.1x Аутентификация

ПРИМЕР 802.1x – топология



ПРИМЕР 802.1x – Сертификат клиента



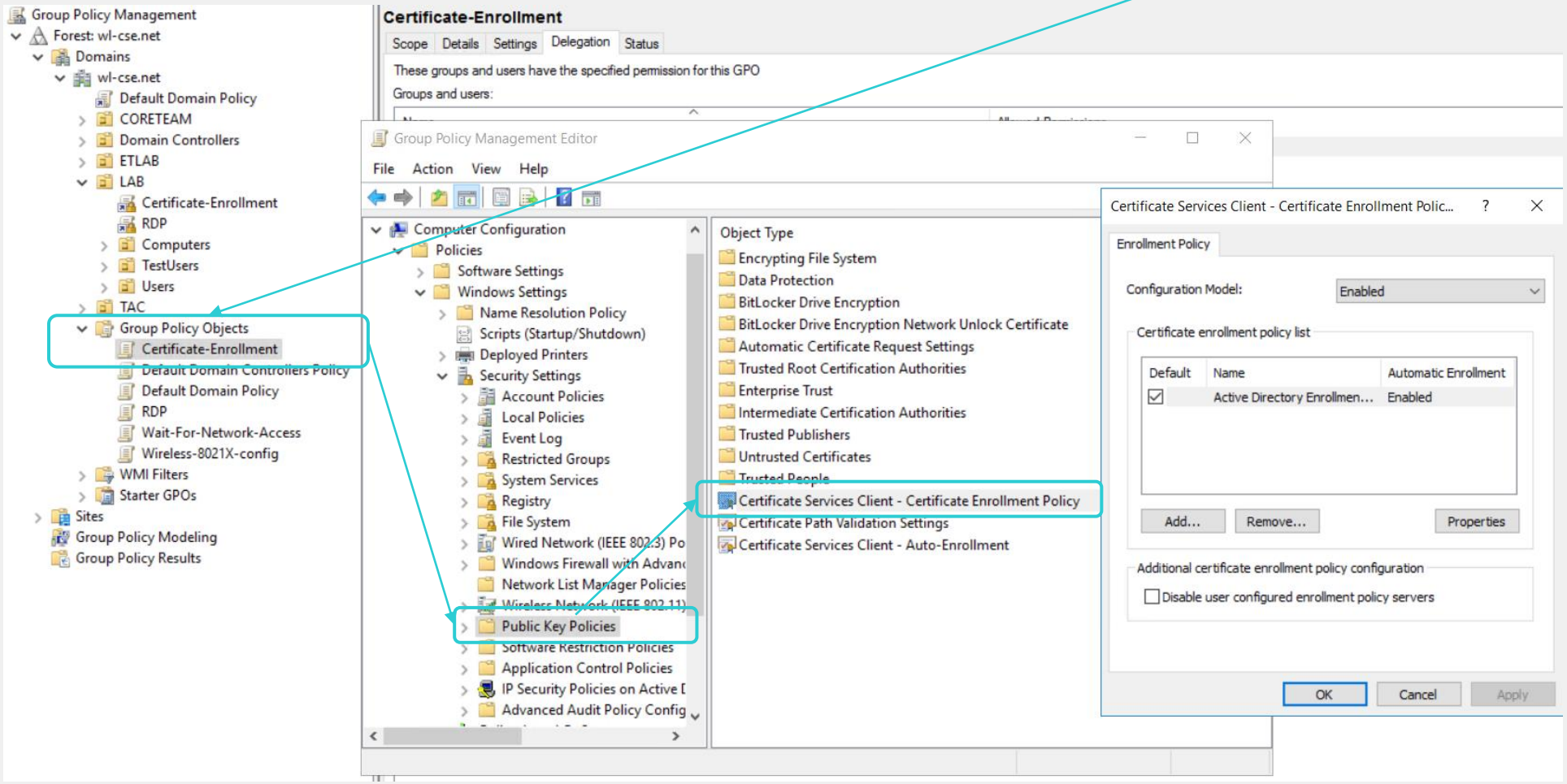
Устанавливаем сертификат клиента на ПК

С помощью MS AD сервера в качестве Root CA, используя групповые политики устанавливаем клиентские сертификаты на доменные ПК

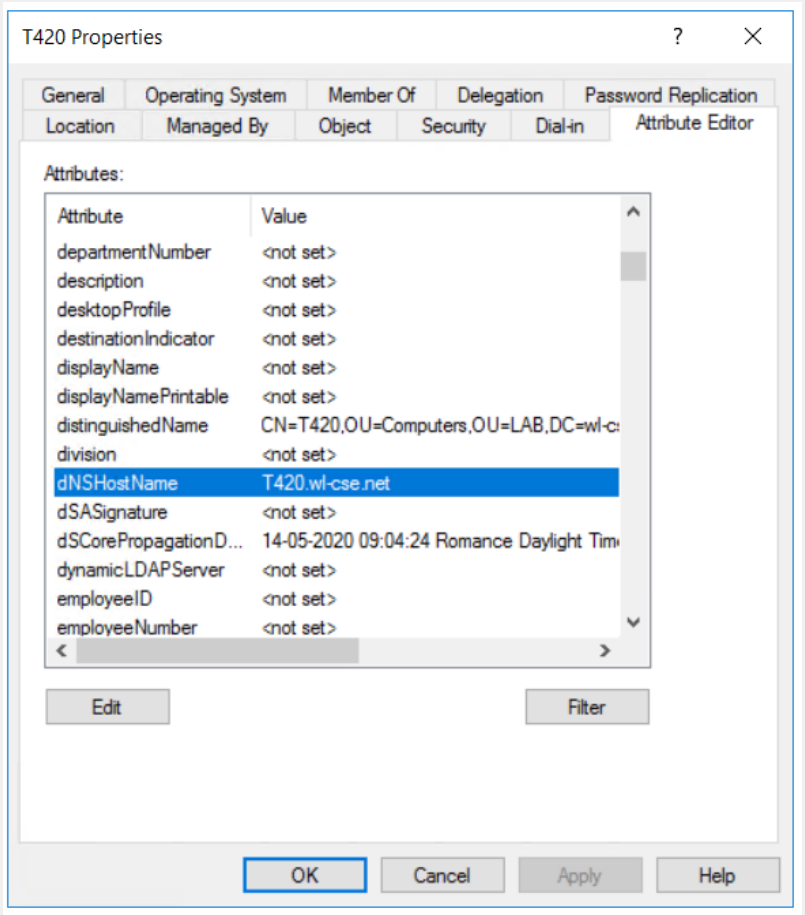
Этот сертификат в дальнейшем используем для валидации RADIUS запроса.

ПРИМЕР 802.1x – MS AD GPO

Используем Group Policy Managment для установки машинных (computer) сертификатов. Создаем новую GPO, с автоматическим применением. И применяем GPO к OU нашей LAB, где расположен тестовый компьютер.



ПРИМЕР 802.1x – MS AD настройка

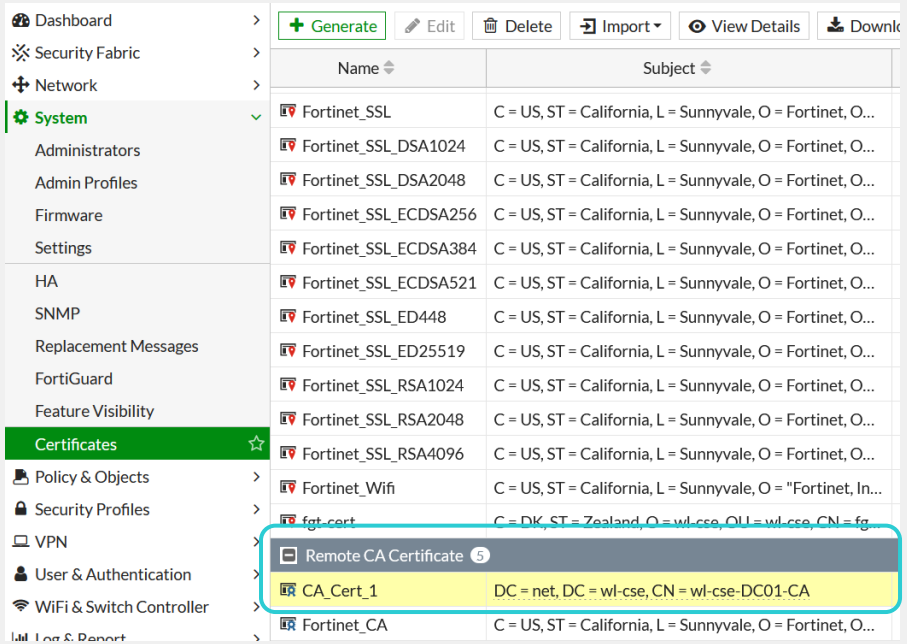


Аккаунт компьютера в AD должен использовать аттрибут dNSHostName со значением имени компьютера.

Используем это аттрибут позже в FortiAuthenticator для создания правил синхронизации Remote Sync Rule.

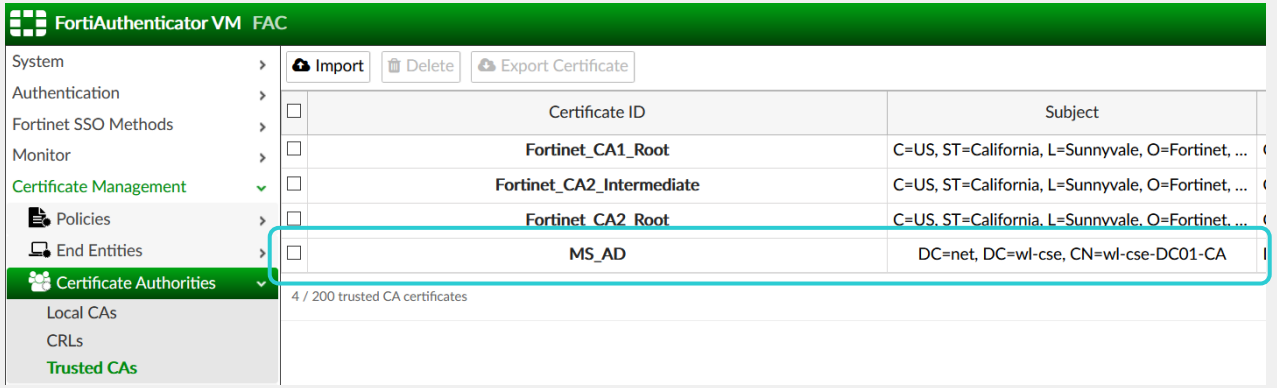
ПРИМЕР 802.1x – Root CA импорт FGT и FAC

System – Certificates – Remote CA Certificate

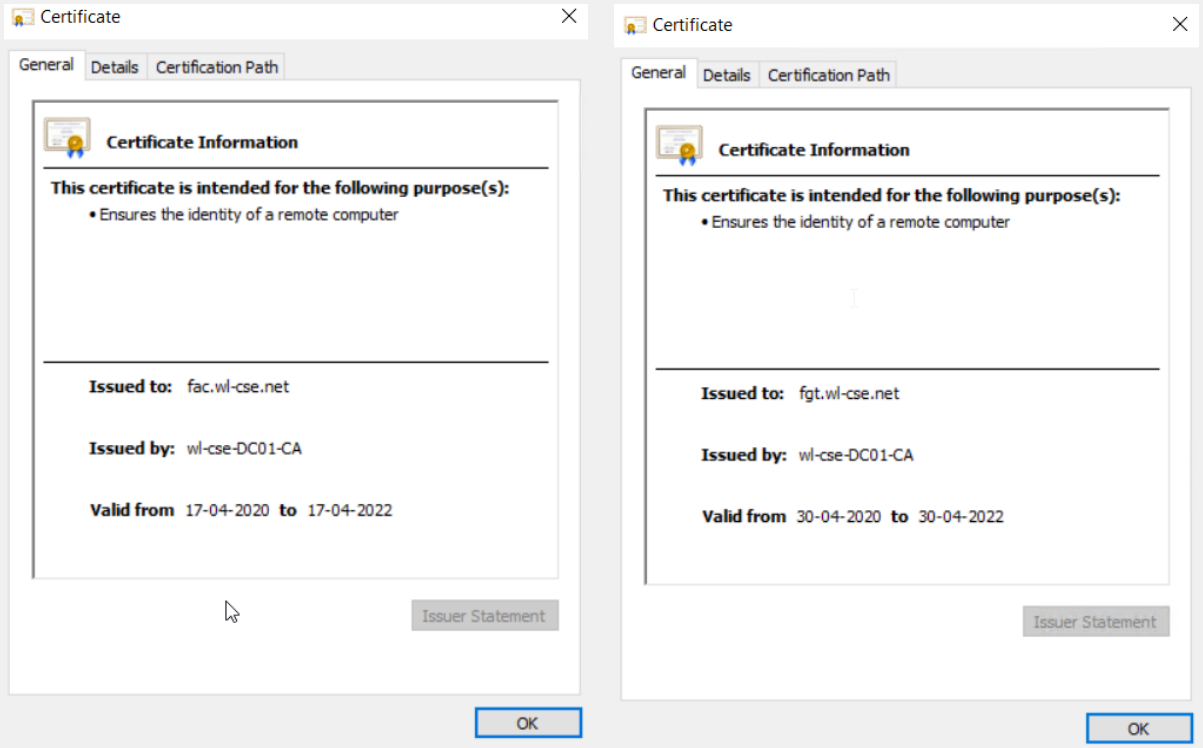


MS AD Root CA добавляем как доверенный CA на FortiGate и FortiAuthenticator.

Certificate Management – Certificate Authorities – Trusted CAs



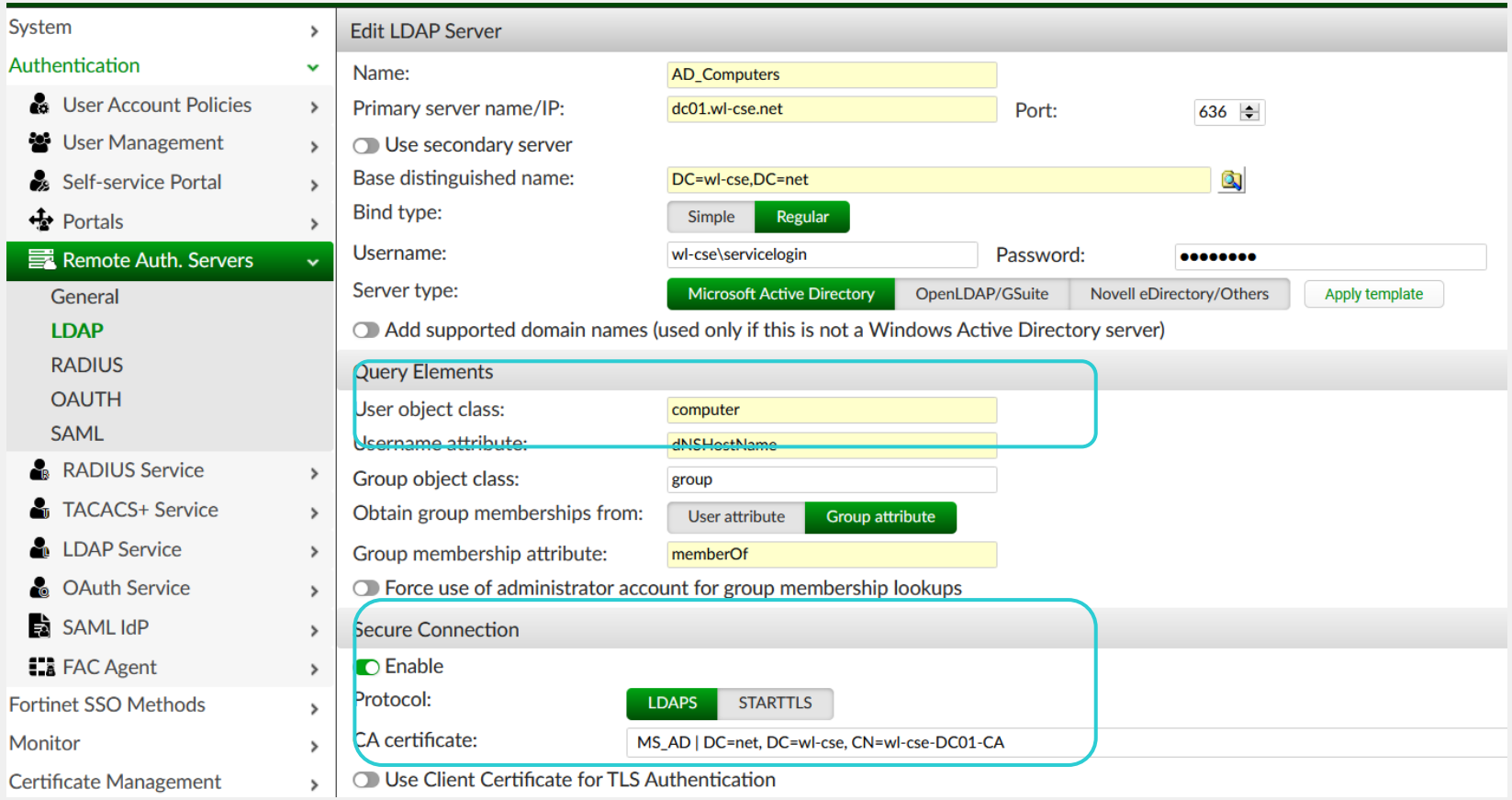
ПРИМЕР 802.1x – выпуск сертификатов



Выпускаем сертификаты используя AD CA для FortiGate и FortiAuthenticator.

ПРИМЕР 802.1x – Remote Auth, LDAP

Authentication – Remote Auth Servers – LDAP



Создаем запись LDAP для remote lookup компьютеров, с аттрибоутом Username имеющим значение dNSHostName

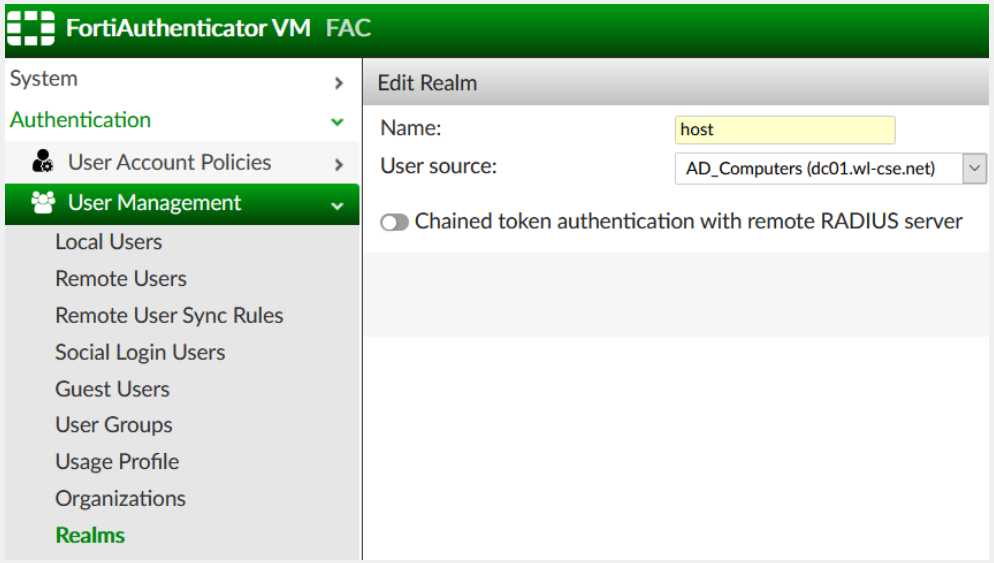
ПРИМЕР 802.1x – Realms

Когда клиент аутентифицируется RADIUS запрос отправляется в формате: host/FQDN

```
 13 0.100318    192.168.200.1    192.168.200.9    RADIUS    372 Access-Request id=90
 14 0.115017    192.168.200.9    192.168.200.1    RADIUS    258 Access-Accept id=90

Attribute Value Pairs
  AVP: t=User-Name(1) l=22 val=host/T420.wl-cse.net
```

Authentication – User Management – Realms

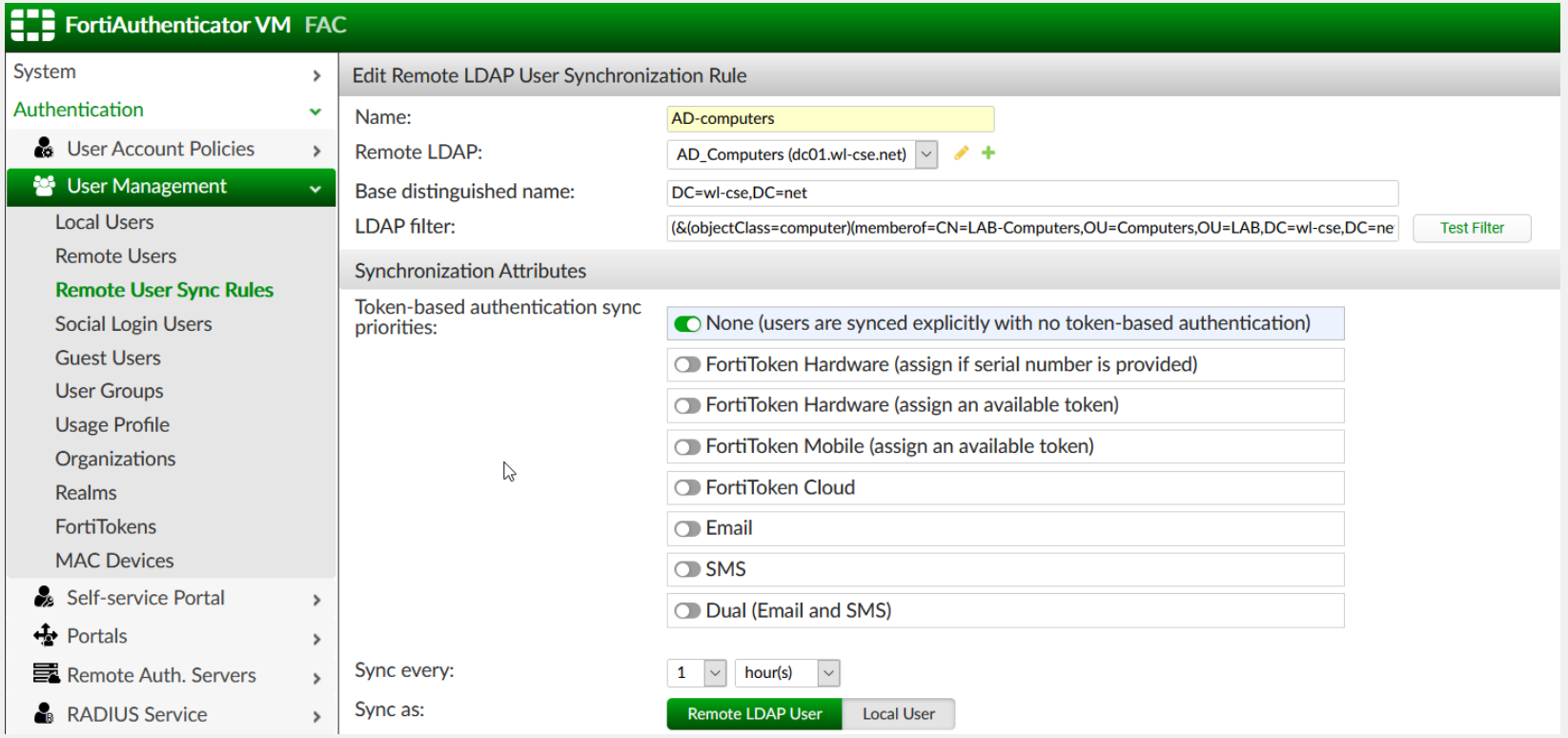


Создаем realm для ”**host**”
Он будет использоваться позднее в RADIUS Policy

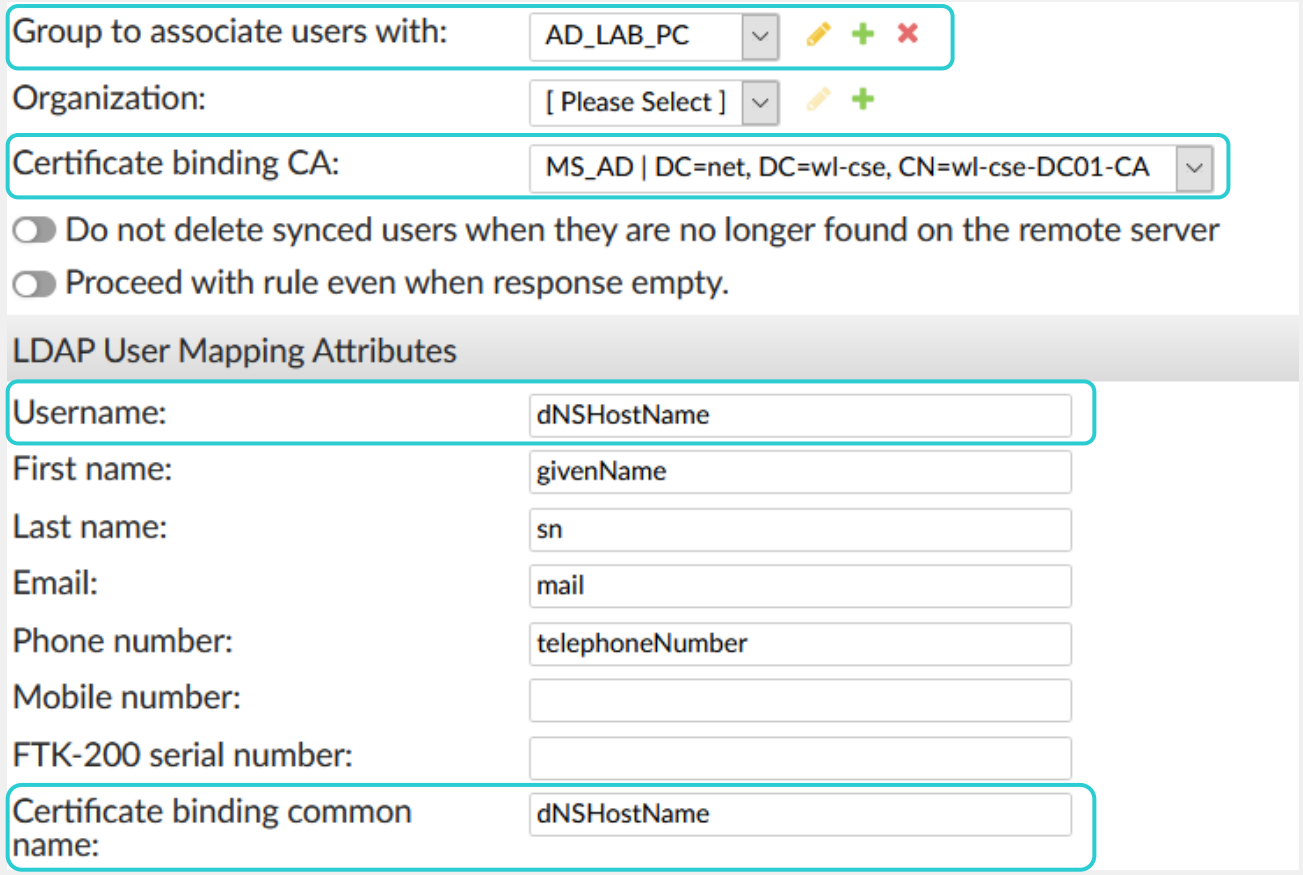
ПРИМЕР 802.1x – Remote LDAP sync rule

Выбираем LDAP filter для соответствия определенным группам AD.

(&(objectClass=computer)(memberof=CN=LAB-Computers,OU=Computers,OU=LAB,DC=wl-cse,DC=net))



ПРИМЕР 802.1x – Remote LDAP sync правила



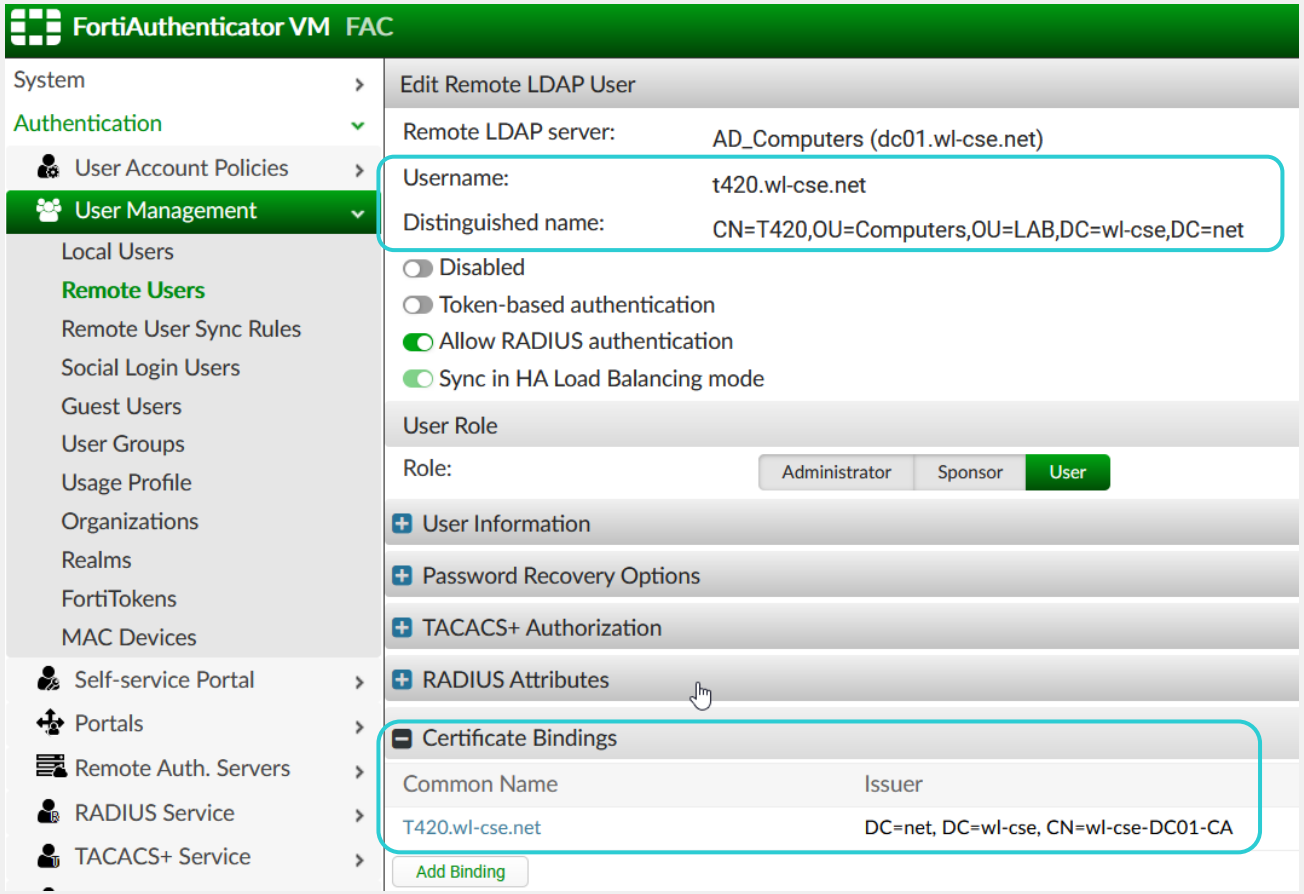
Создаем ассоциацию с группой (используется для RADIUS аттрибутов).

Создаем связь с сертификатом.

ДляLDAP username мы используем dNSHostNAme, и его же для привязки сертификата. Должно совпадать с CN выпущенного сертификата.

ПРИМЕР 802.1x – Проверка запаси компьютера

Authentication – User Management – Remote Users

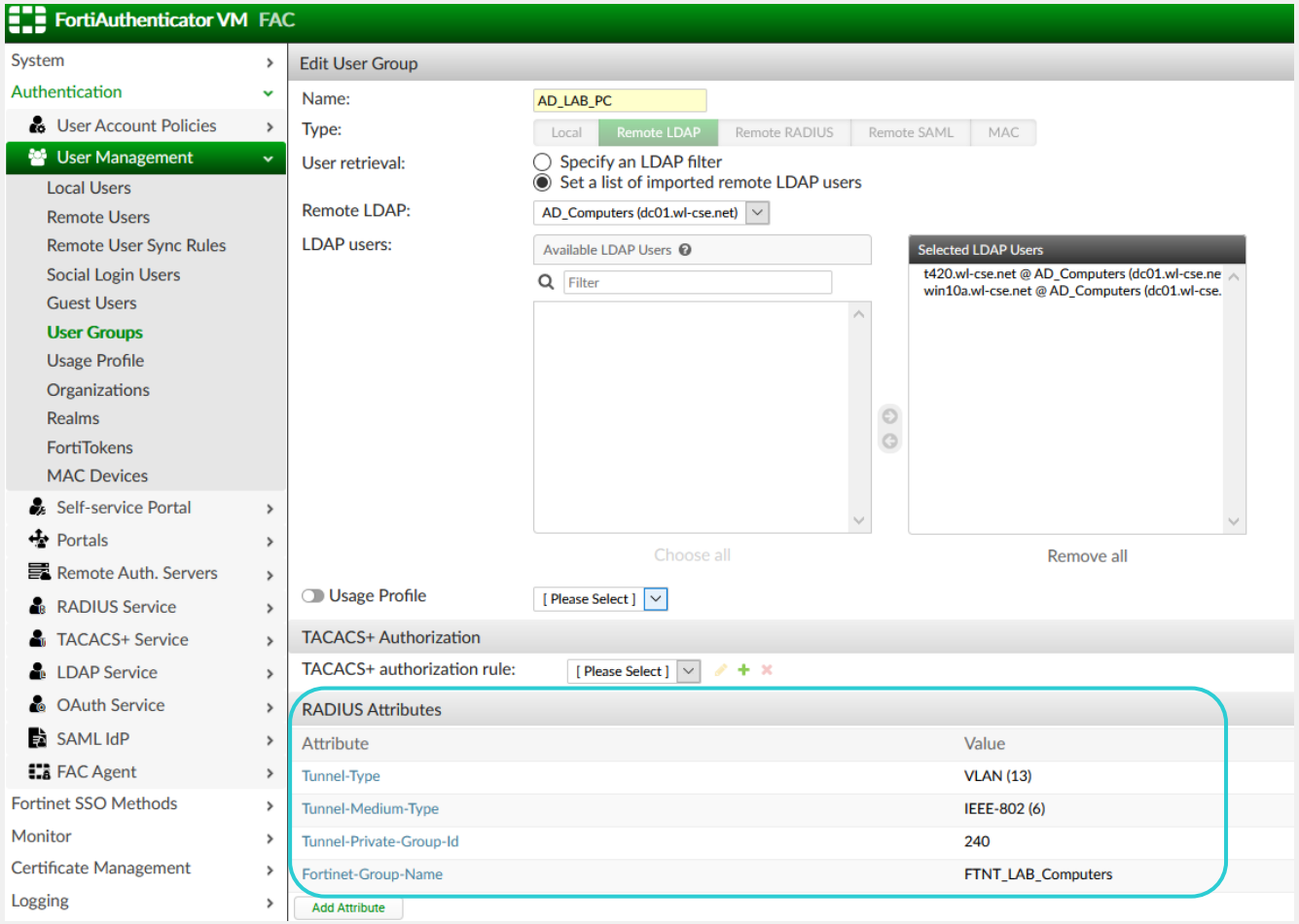


Проверяем ”user” запись для компьютера созданную правилами синхронизации.

Проверяем привязку сертификатов.

ПРИМЕР 802.1x – групповые атрибуты

Authentication – User Management – User Groups



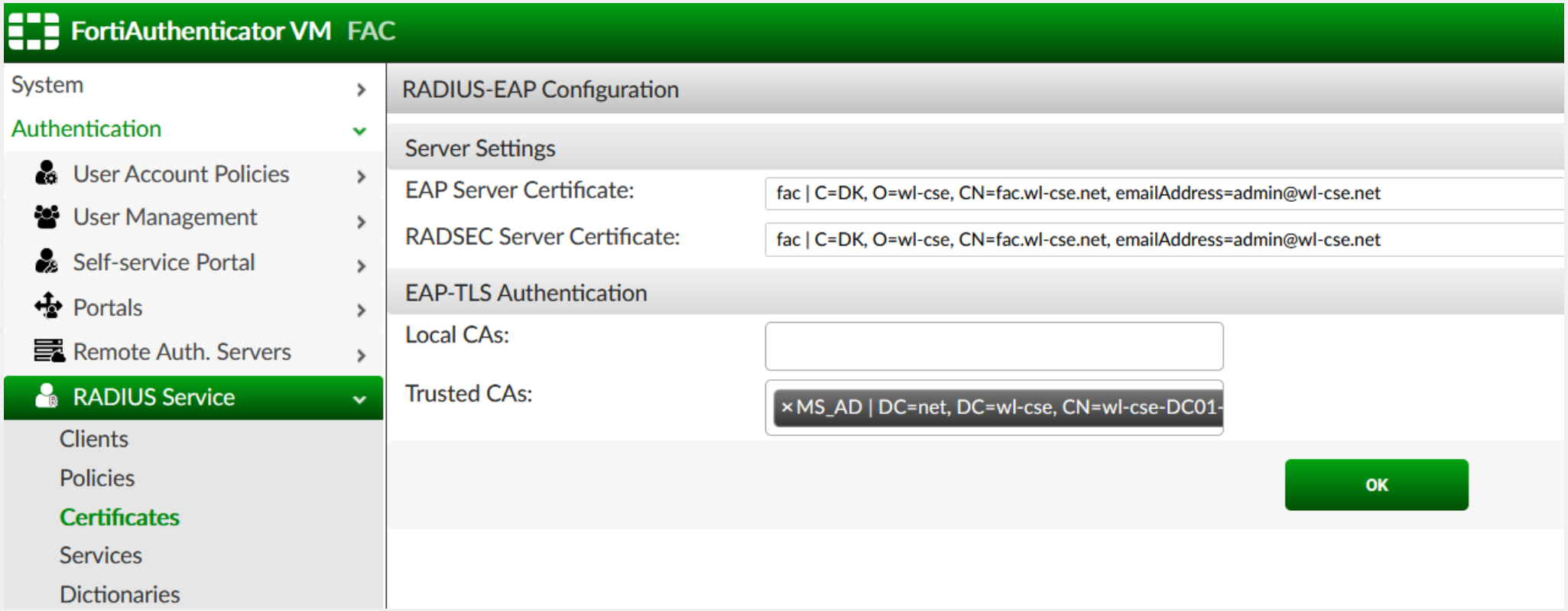
Добавляем необходимые нам RADIUS атрибуты, в нашем примере VLAN id.

Атрибуты будут переданы FAC вместе с RADIUS Accept сообщением

ПРИМЕР 802.1x – RADIUS Service Сертификаты

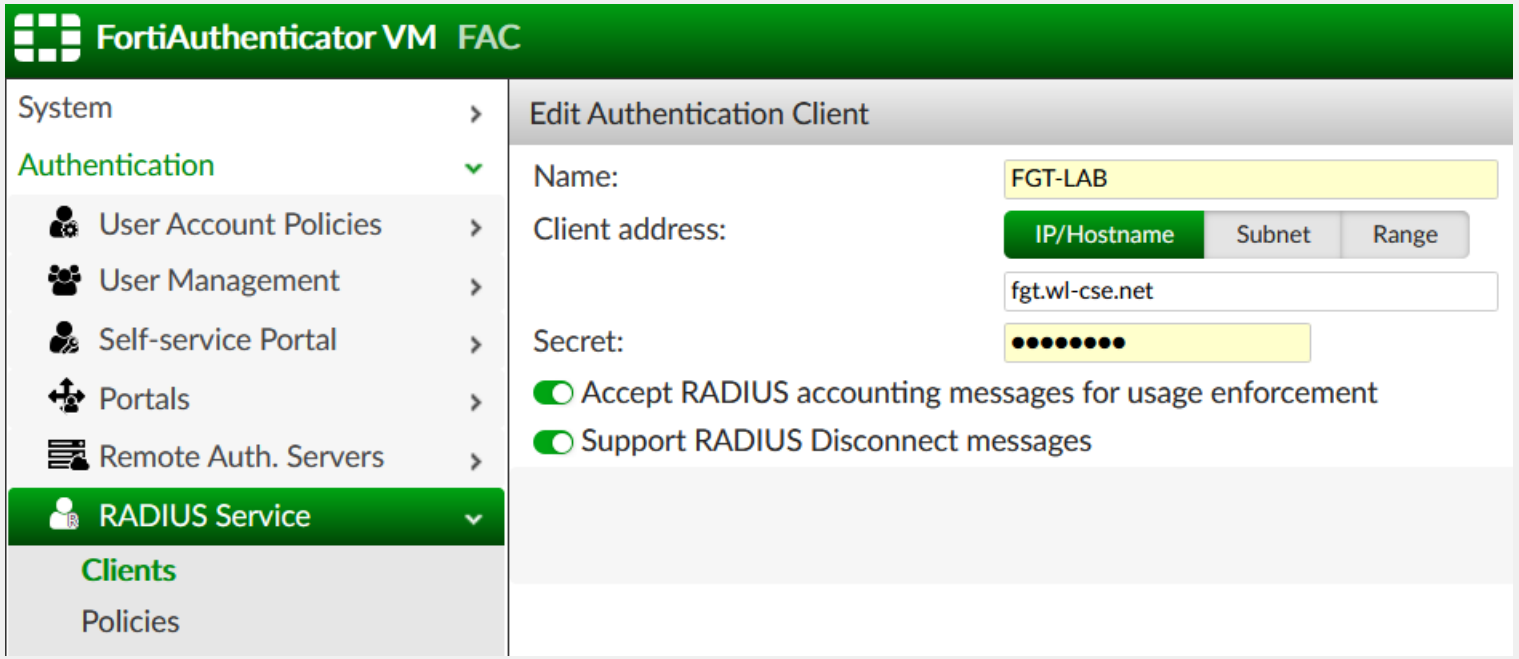
Для RADIUS Service указываем сертификат используемый FAC в EAP, и доверенный CA (наш AD)

Authentication – RADIUS Service – Certificates



ПРИМЕР 802.1x – RADIUS клиенты

Authentication – RADIUS Service – Clients

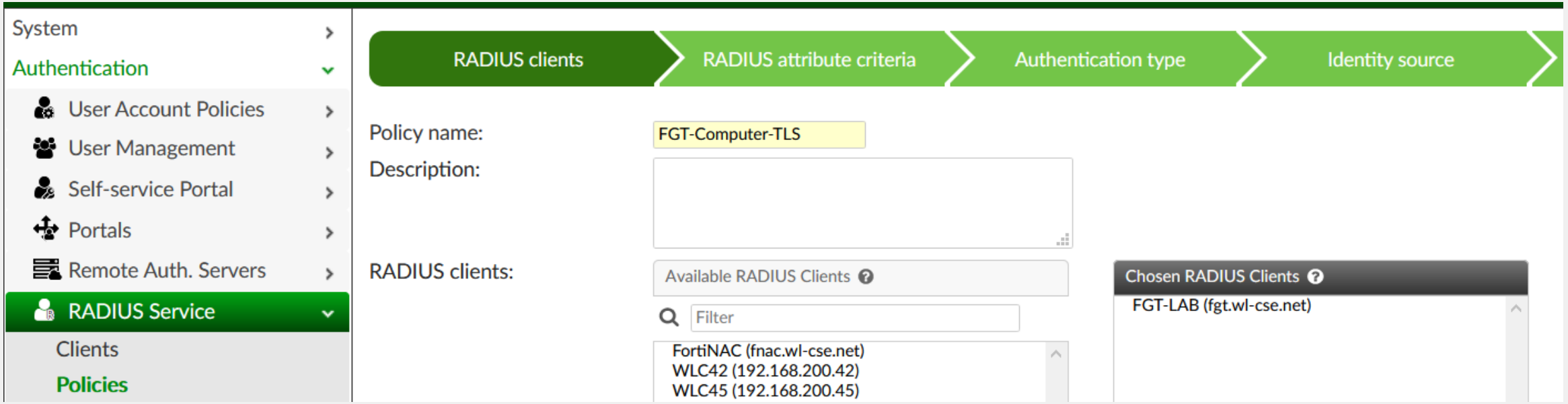


Добавляем FortiGate в качестве RADIUS клиента на FrotiAuthenticator.

ПРИМЕР 802.1x – RADIUS Policy #1

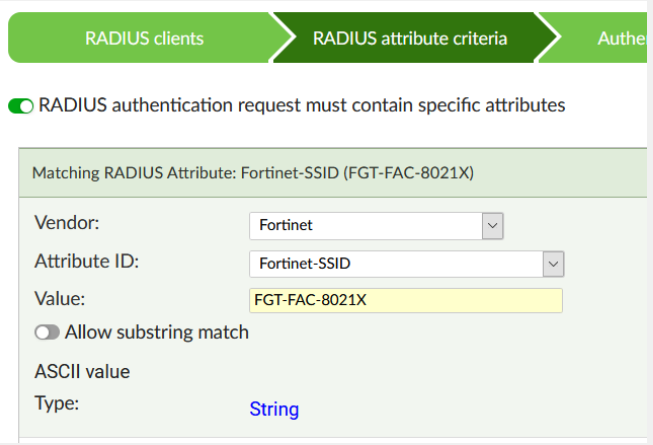
Создаем RADIUS Policy для обработки EAP-TLS (сертификат) клиентов

Authentication – RADIUS Service – Policies

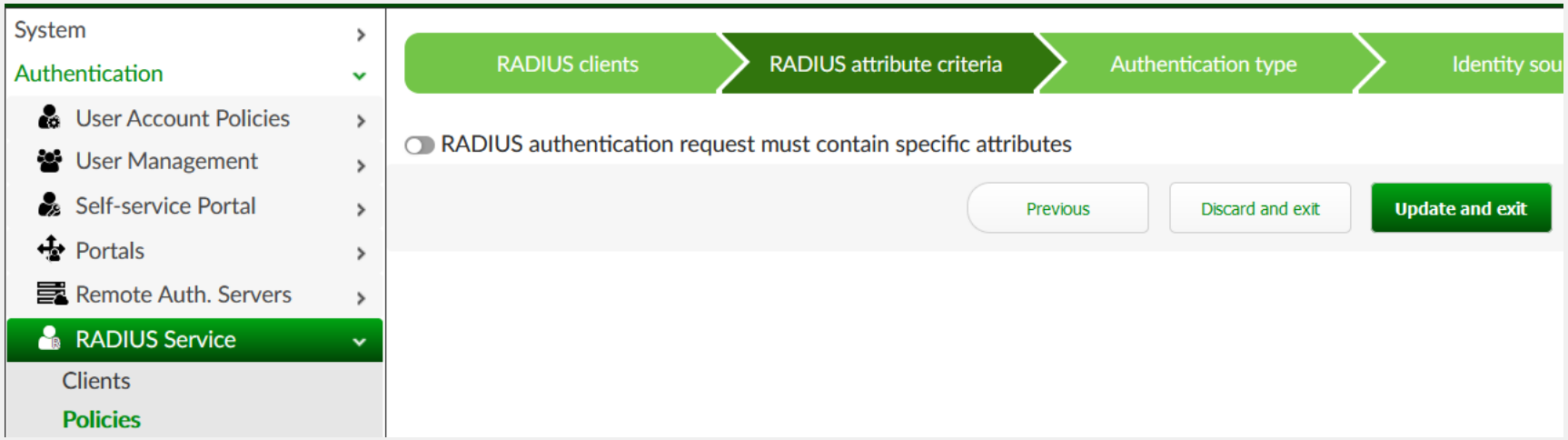


ПРИМЕР 802.1x – RADIUS Policy #2

Создаем RADIUS Policy для обработки EAP-TLS (сертификат) клиентов



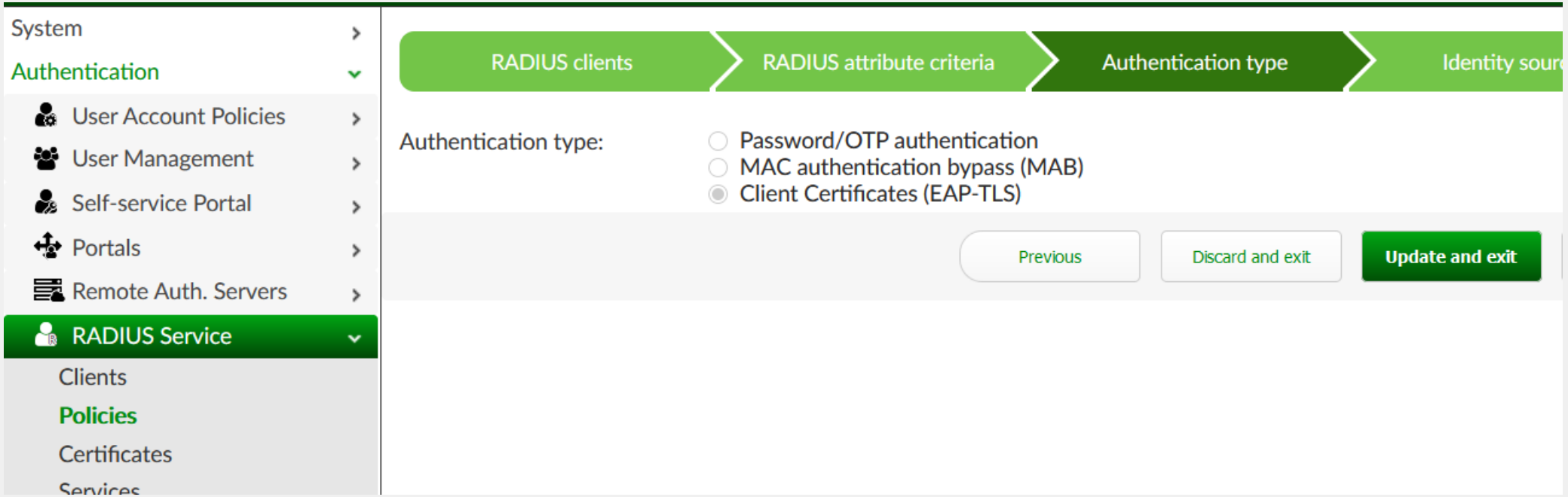
В нашем примере мы не задаем никаких параметров, можно, например указать SSID.



ПРИМЕР 802.1x – RADIUS Policy #3

Создаем RADIUS Policy для обработки EAP-TLS (сертификат) клиентов

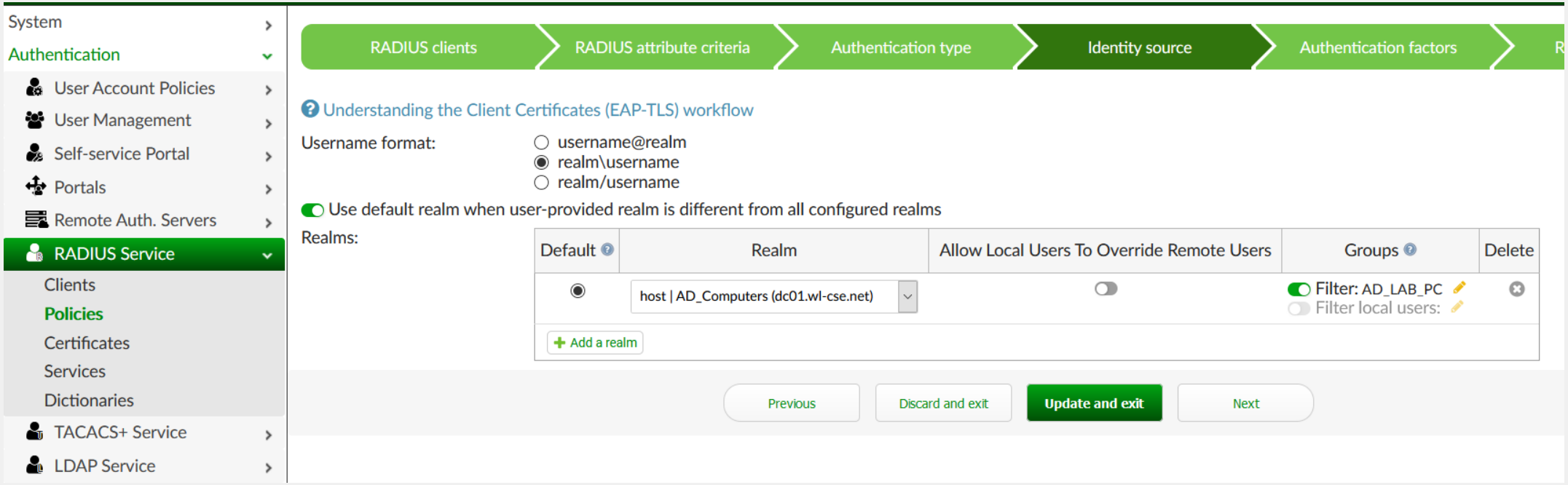
Выбираем клиентский сертификат (EAP-TLS)



ПРИМЕР 802.1x – RADIUS Policy #4

Создаем RADIUS Policy для обработки EAP-TLS (сертификат) клиентов

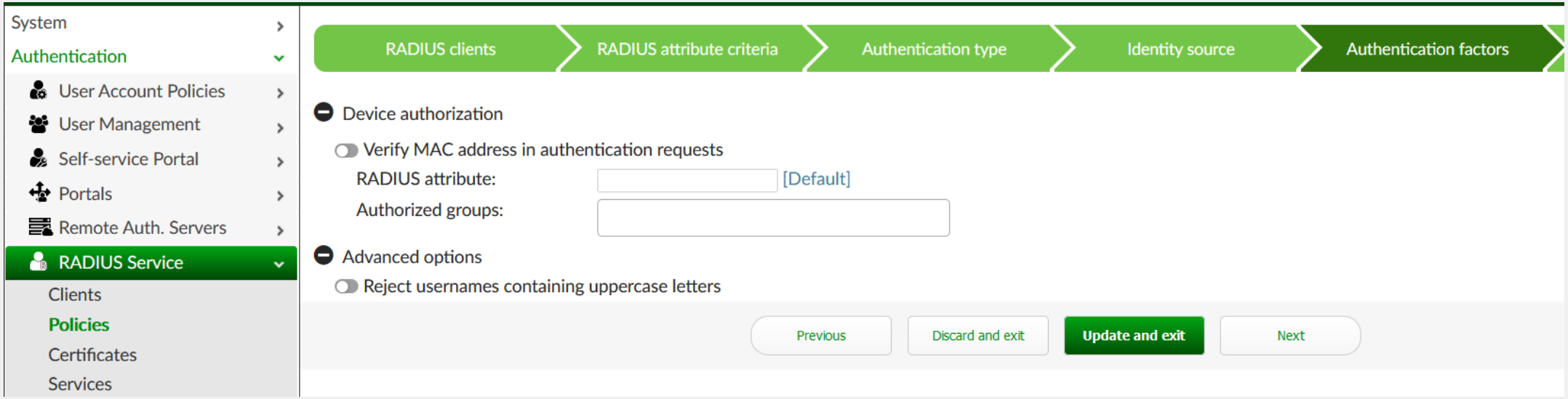
Выбираем username формат, и используем наш realm (host)



ПРИМЕР 802.1x – RADIUS Policy #5

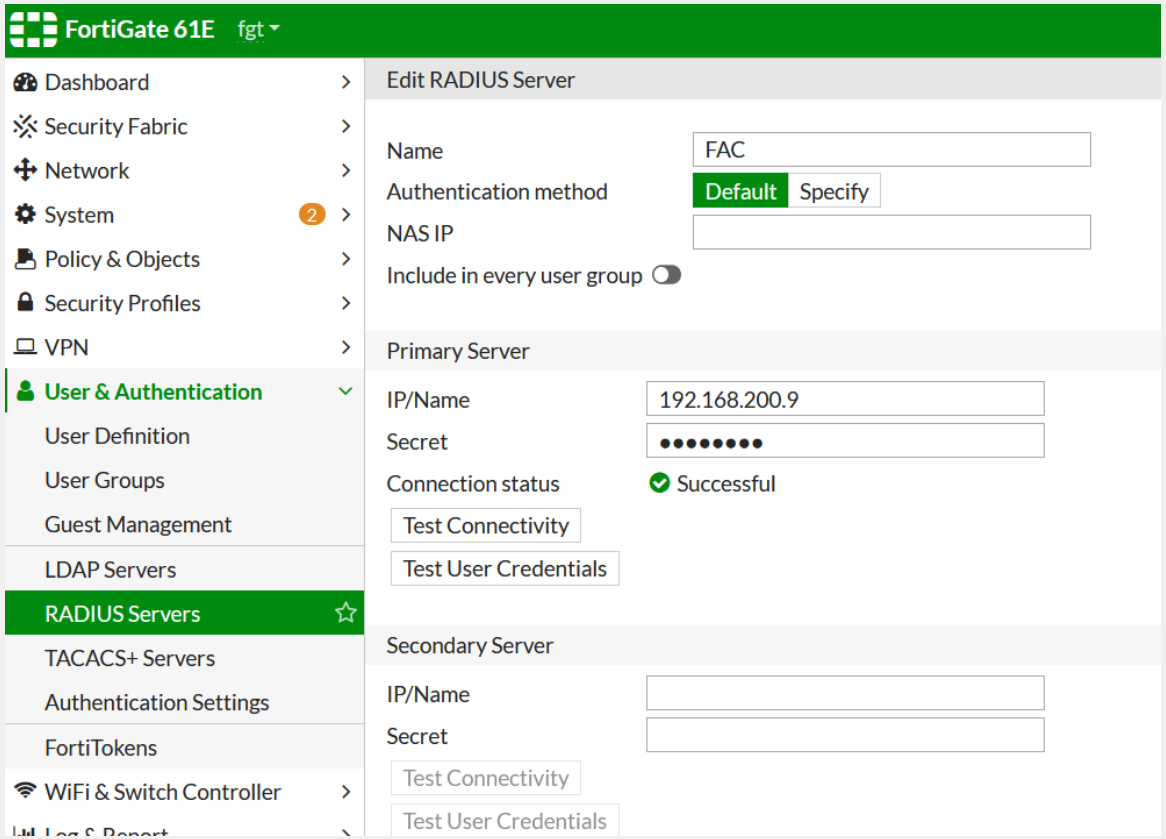
Создаем RADIUS Policy для обработки EAP-TLS (сертификат) клиентов

На данной вкладке оставляем все как есть. Все применяем.



ПРИМЕР 802.1x – FortiGate: RADIUS

User & Authentication – RADIUS Servers

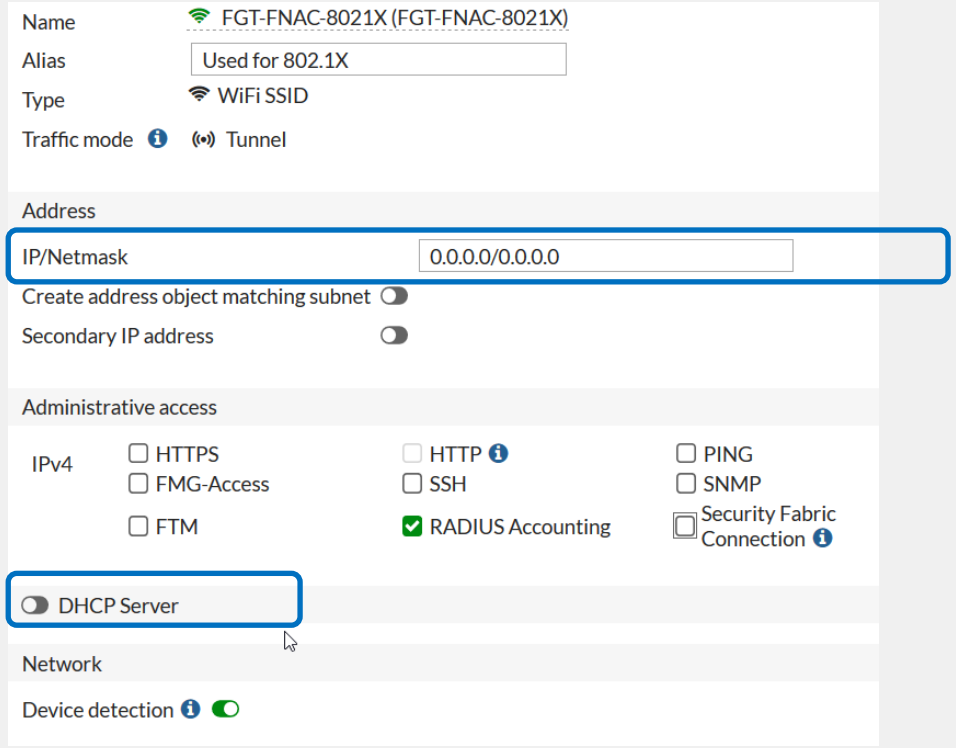


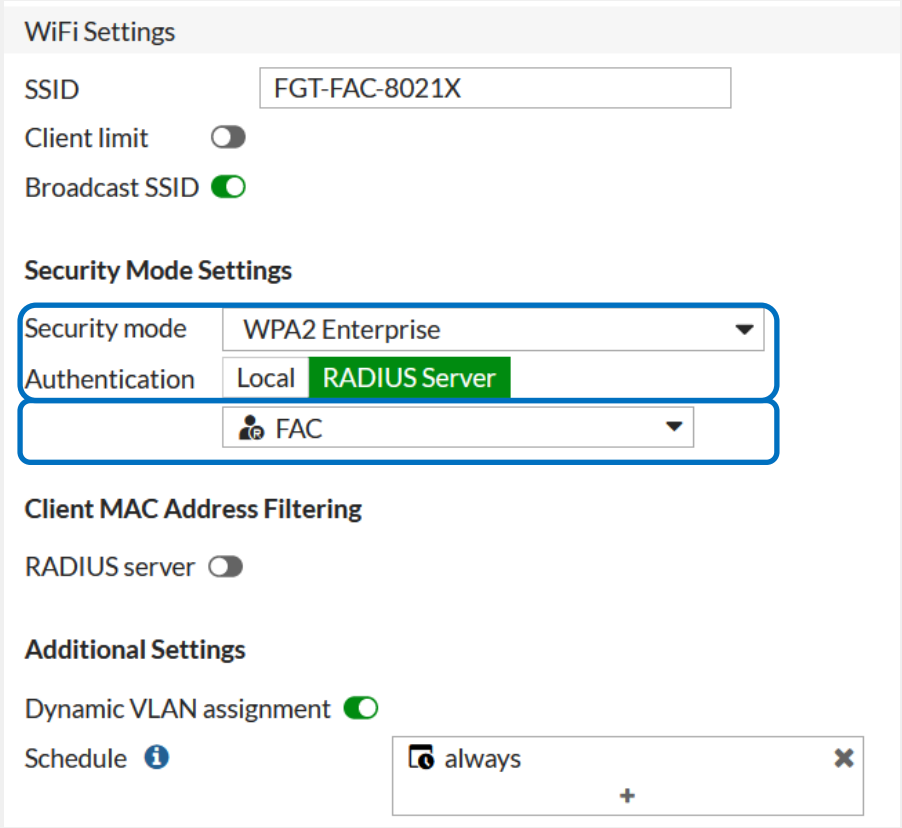
Создаем RADIUS Server аккаунт на FortiGate и привязываем к FortiAuthenticator (в нашем примере 192.168.200.9)

ПРИМЕР 802.1x – FortiGate: SSID

WiFi & Switch Controller – SSIDs

Создаем новый SSID, используем Dynamic VLAN assignment.



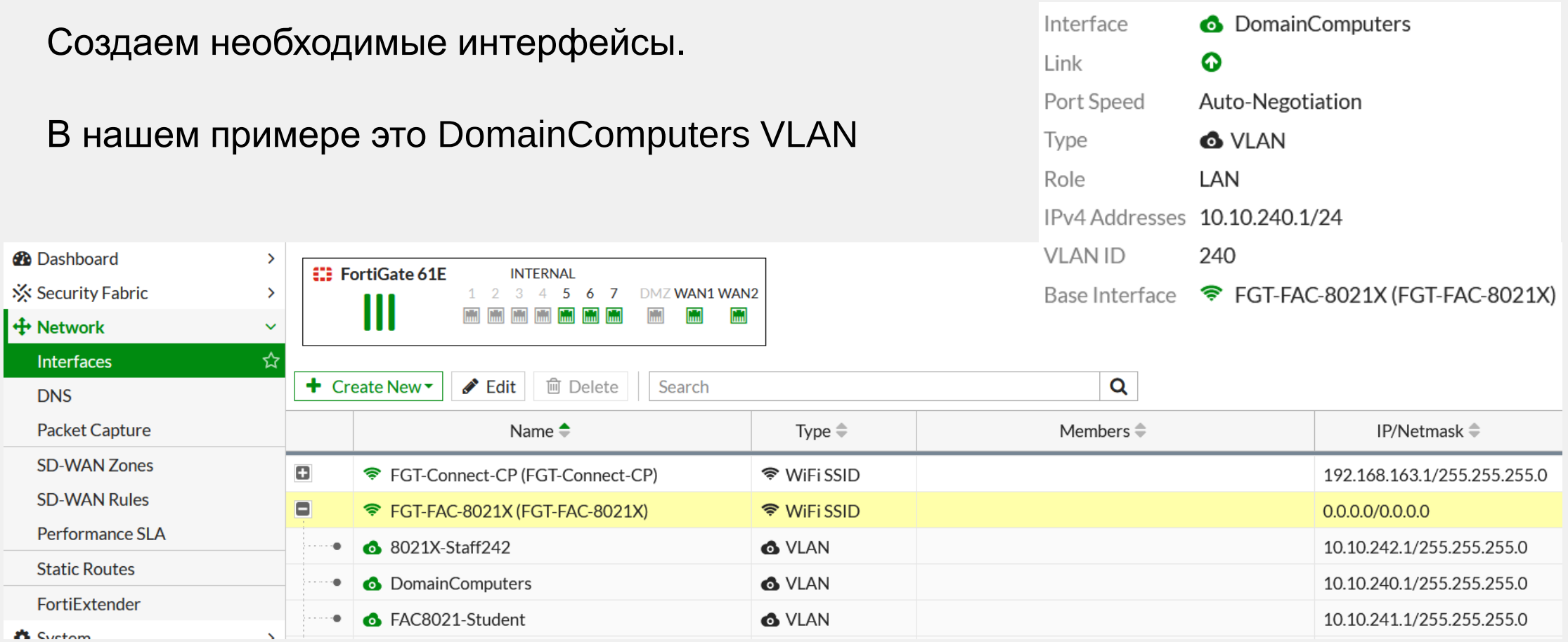


ПРИМЕР 802.1x – FortiGate: Интерфейсы

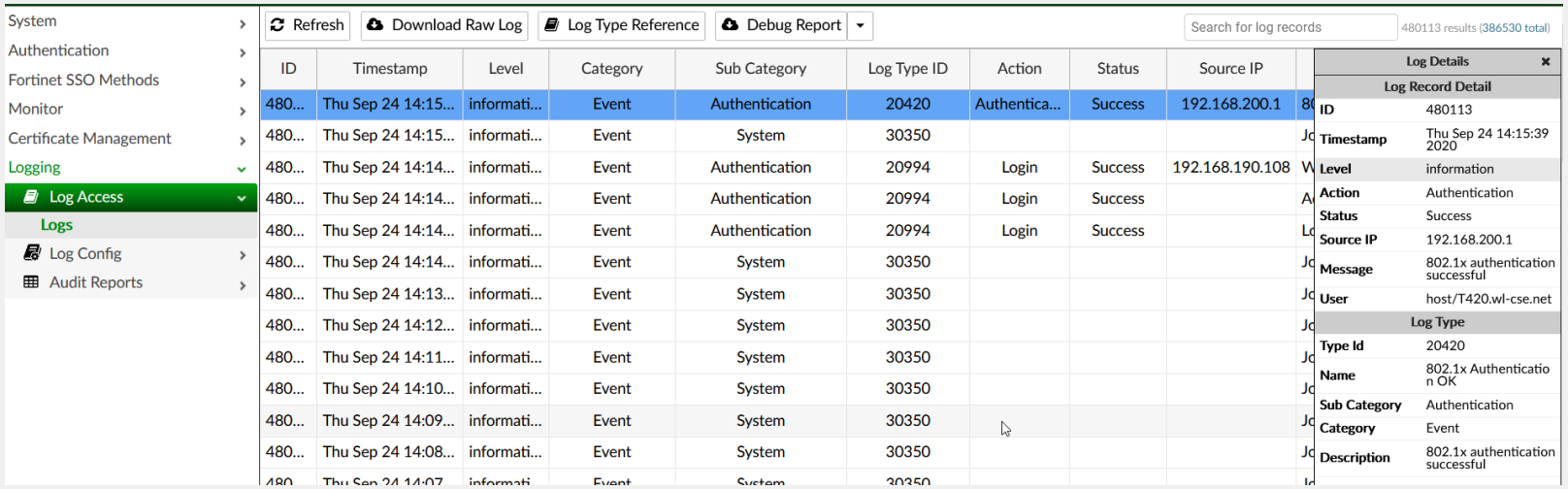
Network – Interfaces

Создаем необходимые интерфейсы.

В нашем примере это DomainComputers VLAN

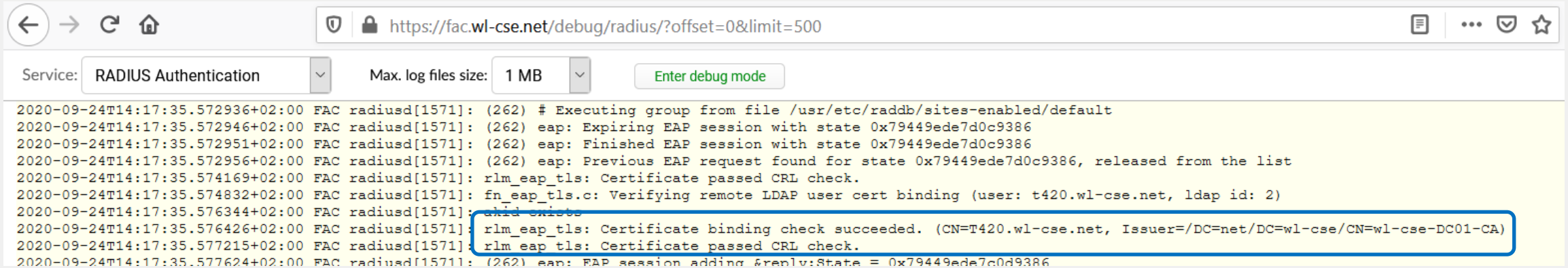


ПРИМЕР 802.1x – FortiAuthenticator: Logs

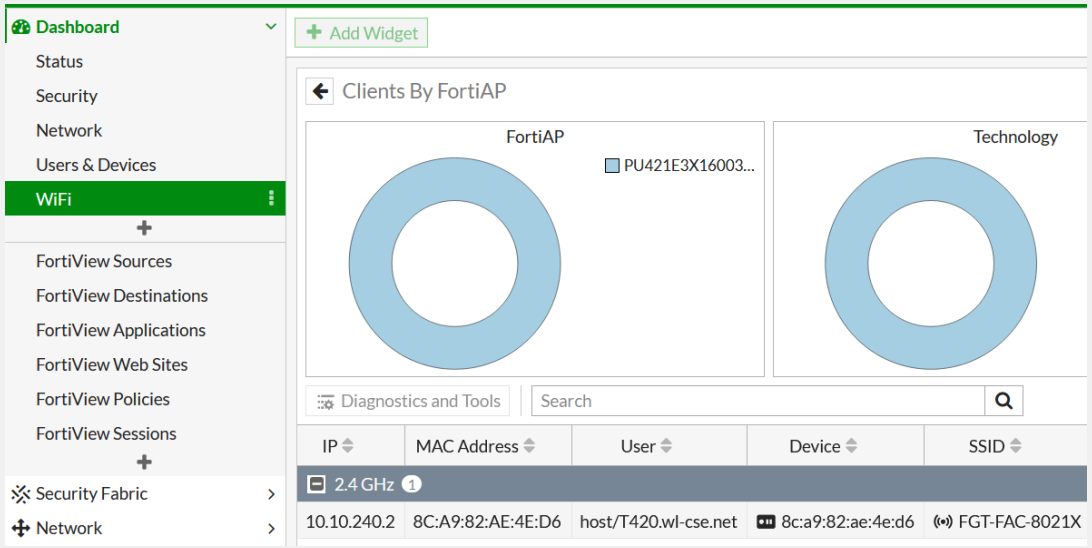


Подключаем нашего клиента и получаем сообщение Authentication Success в логах FortiAuthenticator

А если заглянуть в debug обнаружим что binding/check is passed.



ПРИМЕР 802.1x – проверка RADIUS Accept и VLANid



На Fortigate мы видим что пользователь подключен.

А заглянув в содержимое пакетов обрануживаем RADIUS-Accept сообщение включая назначение VLAN 240

```
    14 0.122548      192.168.200.9        192.168.200.1        RADIUS     304 Access-Accept id=111
    Authenticator: 960d1fd1eb07285343c9710b9886a250
    [This is a response to a request in frame 13]
    [Time from request: 0.016899000 seconds]
  v Attribute Value Pairs
    > AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
    > AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
    > AVP: t=EAP-Message(79) l=6 Last Segment[1]
    > AVP: t=Message-Authenticator(80) l=18 val=c0dc18c09834985ce1a3f6ce03c1c71b
    > AVP: t=User-Name(1) l=22 val=host/T420.wl-cse.net
    > AVP: t=Tunnel-Medium-Type(65) l=6 Tag=0x00 val=IEEE-802(6)
    > AVP: t=Tunnel-Type(64) l=6 Tag=0x00 val=VLAN(13)
    > AVP: t=Tunnel-Private-Group-Id(81) l=5 val=240
```

FortiAuthenticator

Security **A**ssertion **M**ark-up **L**anguage (SAML)

SAML – что это?

Что такое SAML (Security Assertion Mark-up Language) ?

- Открытый стандарт обмена данными аутентификации и авторизации между участниками.
- Основное применение multiply-domain web SSO
- Только browser-based

SAML – компоненты

Principal

- Сущность которая запрашивает доступ к сервису требующему аутентификации и авторизации (пользователь, группа, или устройство)

Identity provider (IdP) (поставщик учетных записей)

- Создание, хранение и управление идентификационной иформации
- Отвечает на запросы SAML от SP

Service Provider (SP) (поставщик сервиса)

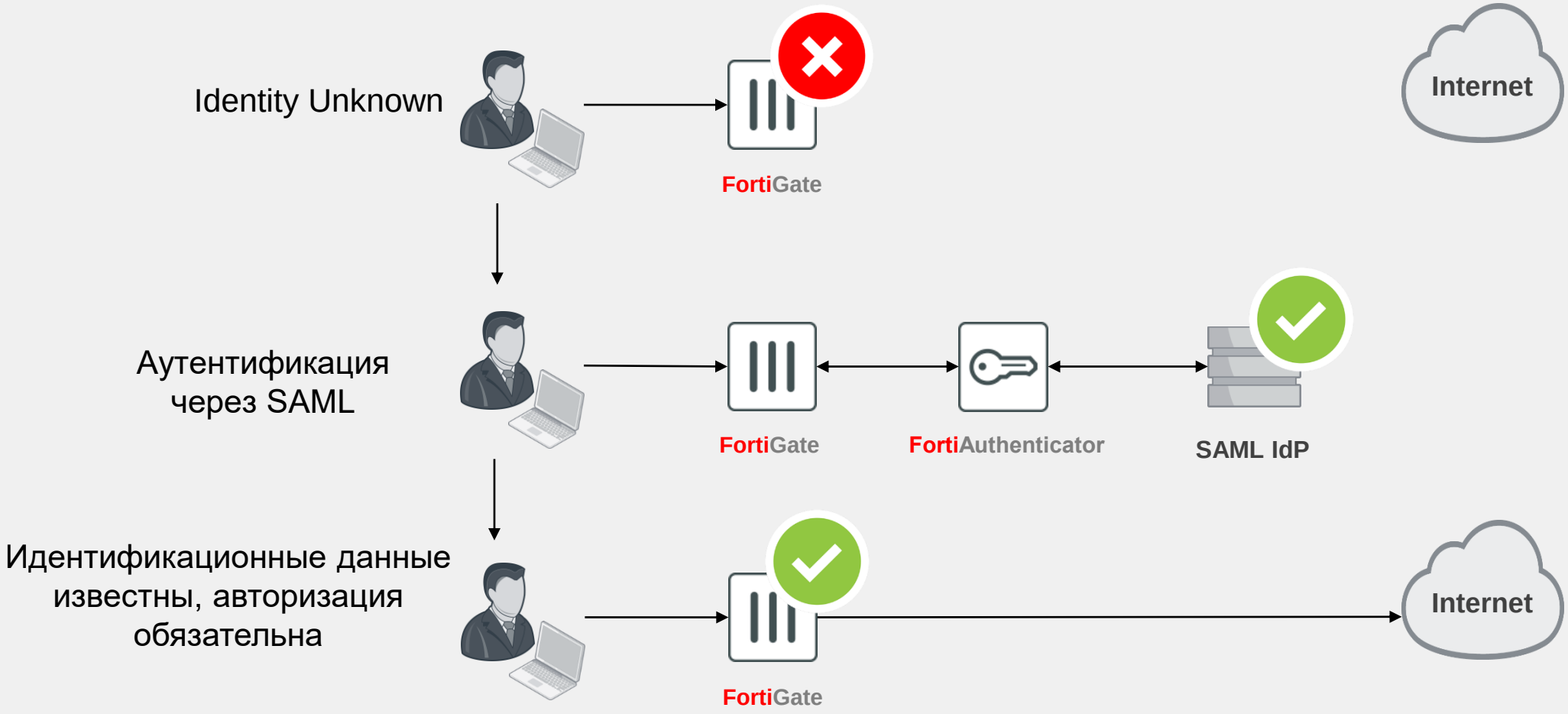
- Предоставляет сервис **Principal**
- **Полагается на IdP для аутентификации и авторазации**

SAML – как это работает?

SAML передает пользовательские данные от IdP к SP через Principal

- SP доверяет IdP
- IdP генерирует SAML assertions с информацией пользователя
- SAML assertion cookies позволяют получать доступ к SP без повторной аутентификации

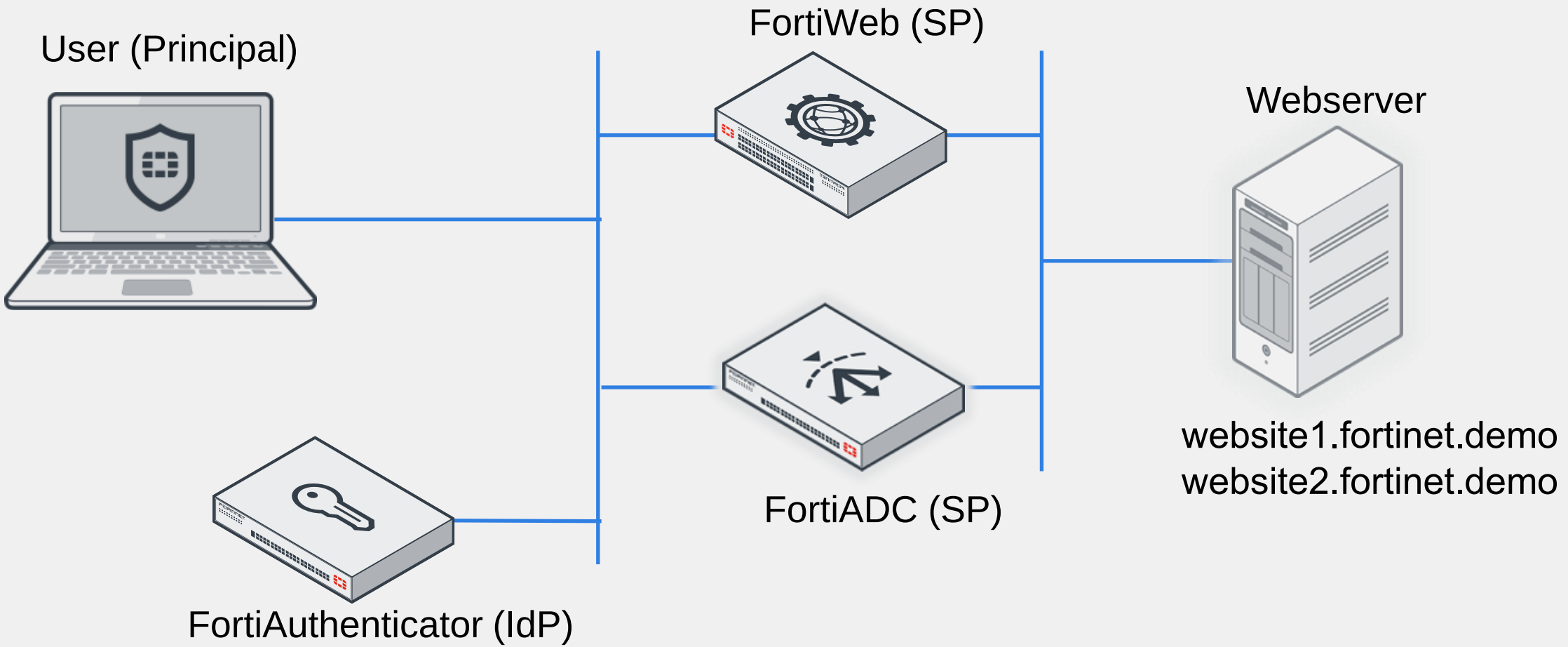
SAML – FSSO упрощенно



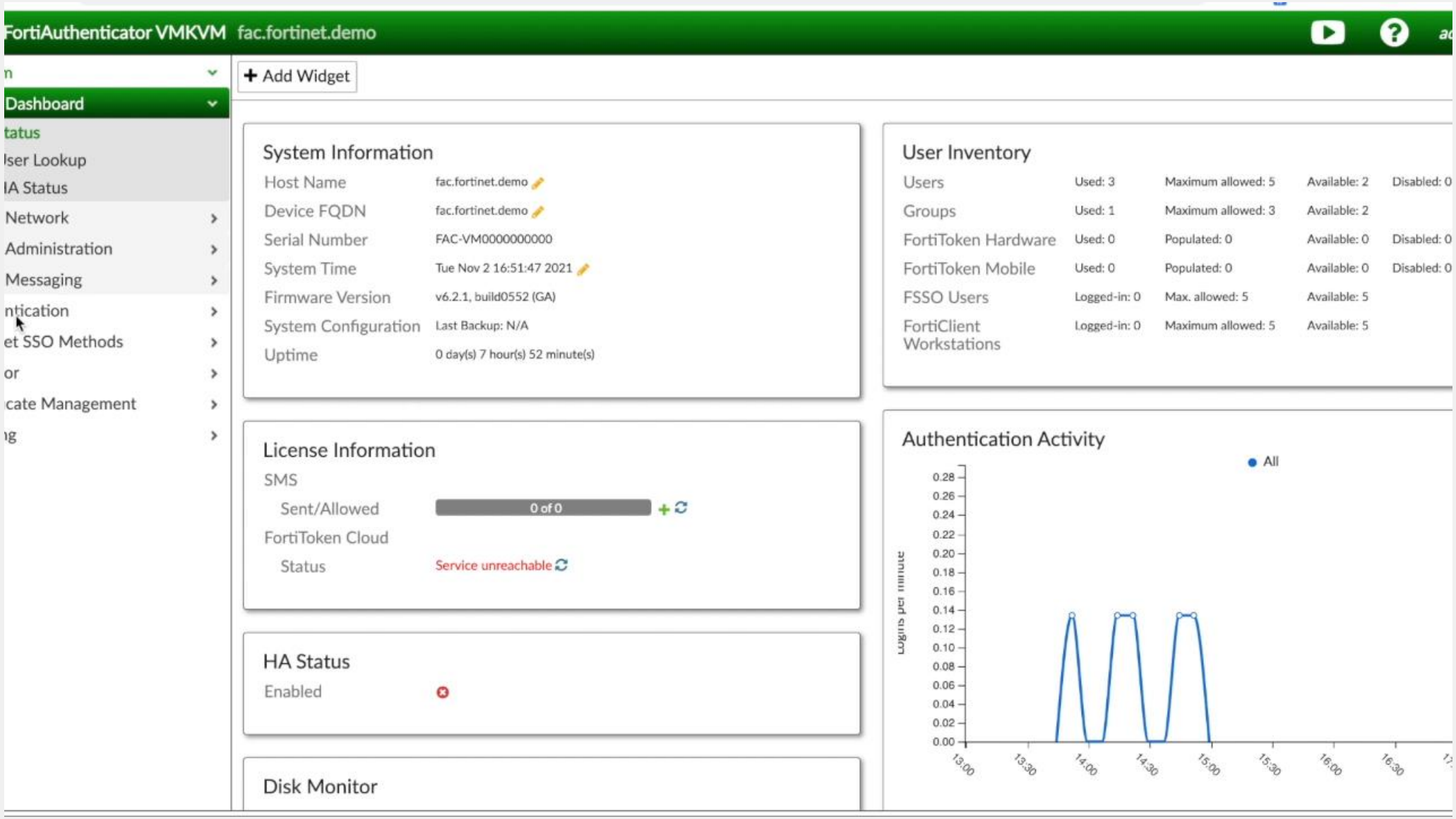
FortiAuthenticator

Демонстрации

Демонстрация работы SAML



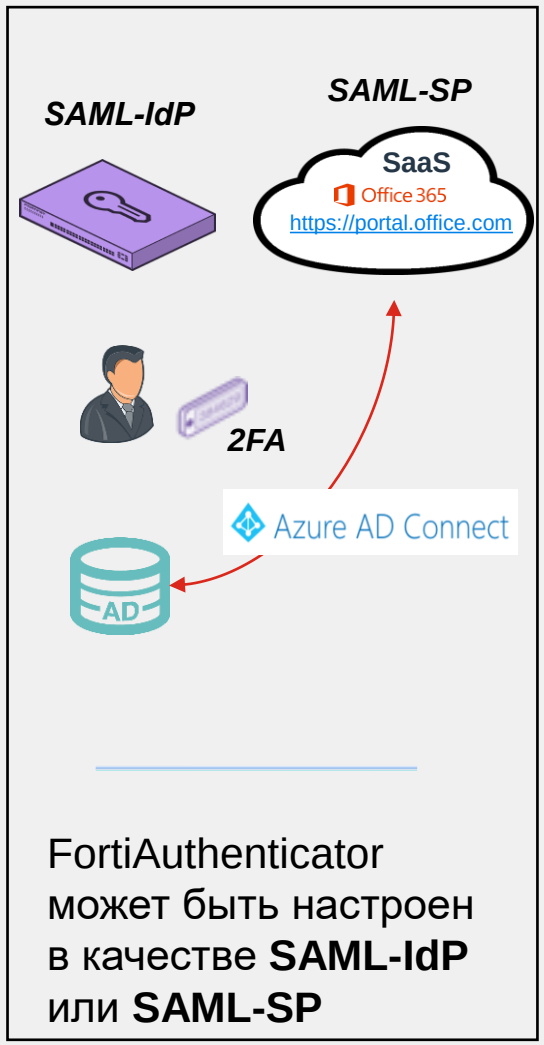
Демонстрация работы SAML



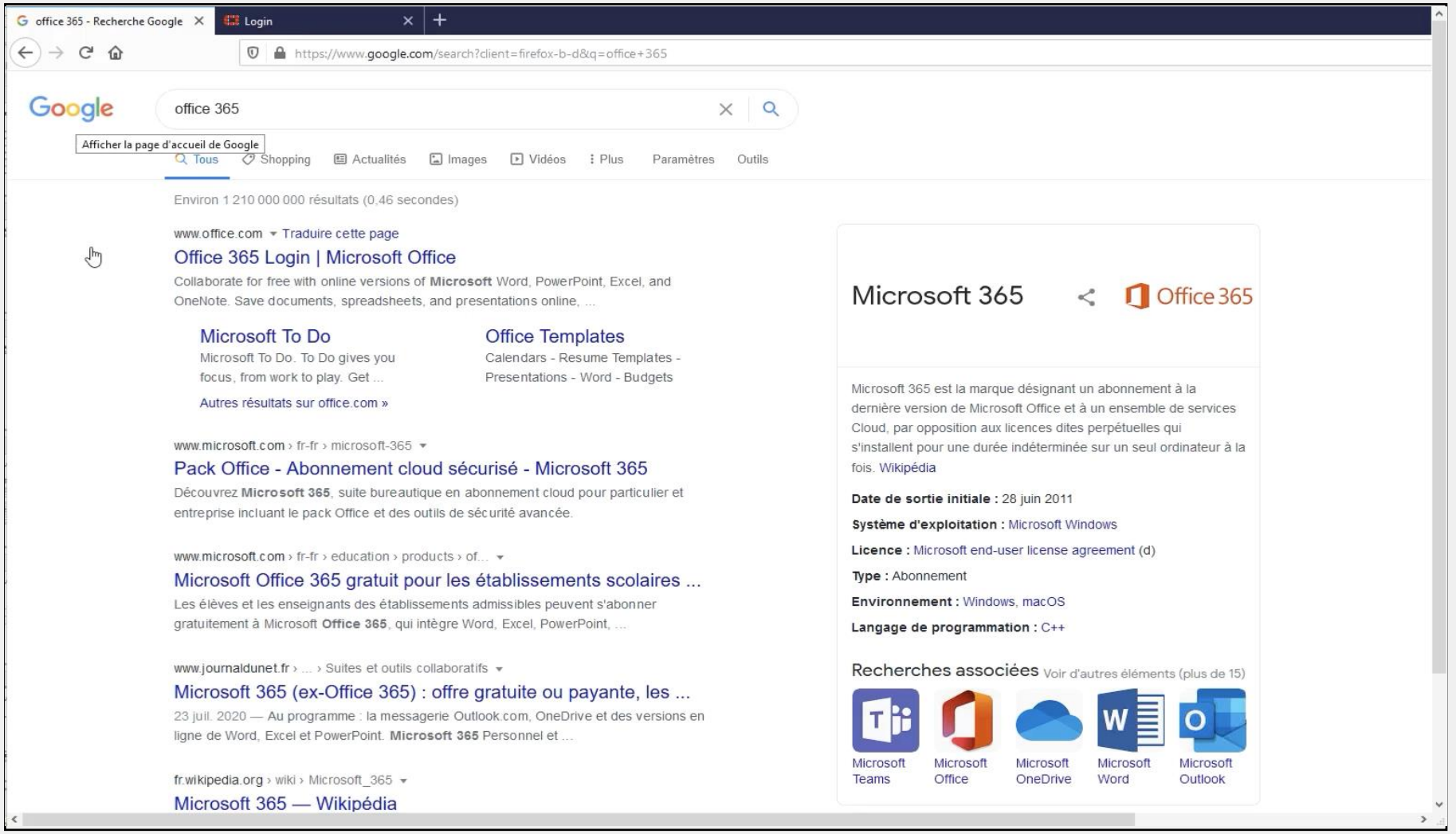
2FA для облачных приложений на примере O365

Демонстрация (видеоролик 2 мин)

Office365 и FortiToken Mobile (с Push нотификациями)



FortiAuthenticator может быть настроен в качестве **SAML-IdP** или **SAML-SP**



cis_se@fortinet.com (инженерная команда)