



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.

Неправильное использование учетных данных и привилегий может стать причиной взлома



Слабая аутентификация и неправильное управление доступом делают сеть уязвимой

Fortinet Security Fabric

Комплексная

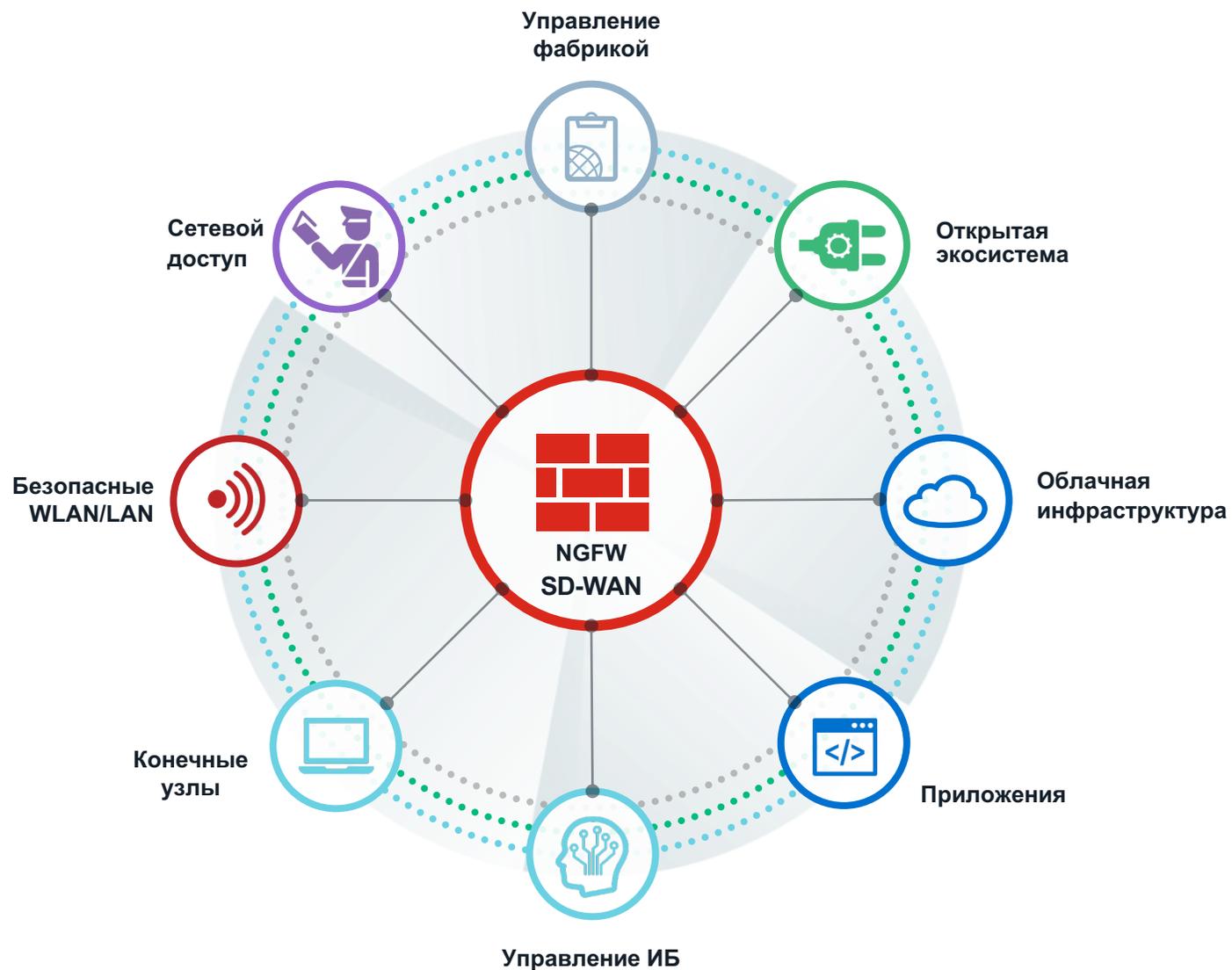
Обеспечение полной видимости поверхности цифровой атаки для лучшего управления рисками ИБ

Интегрированная

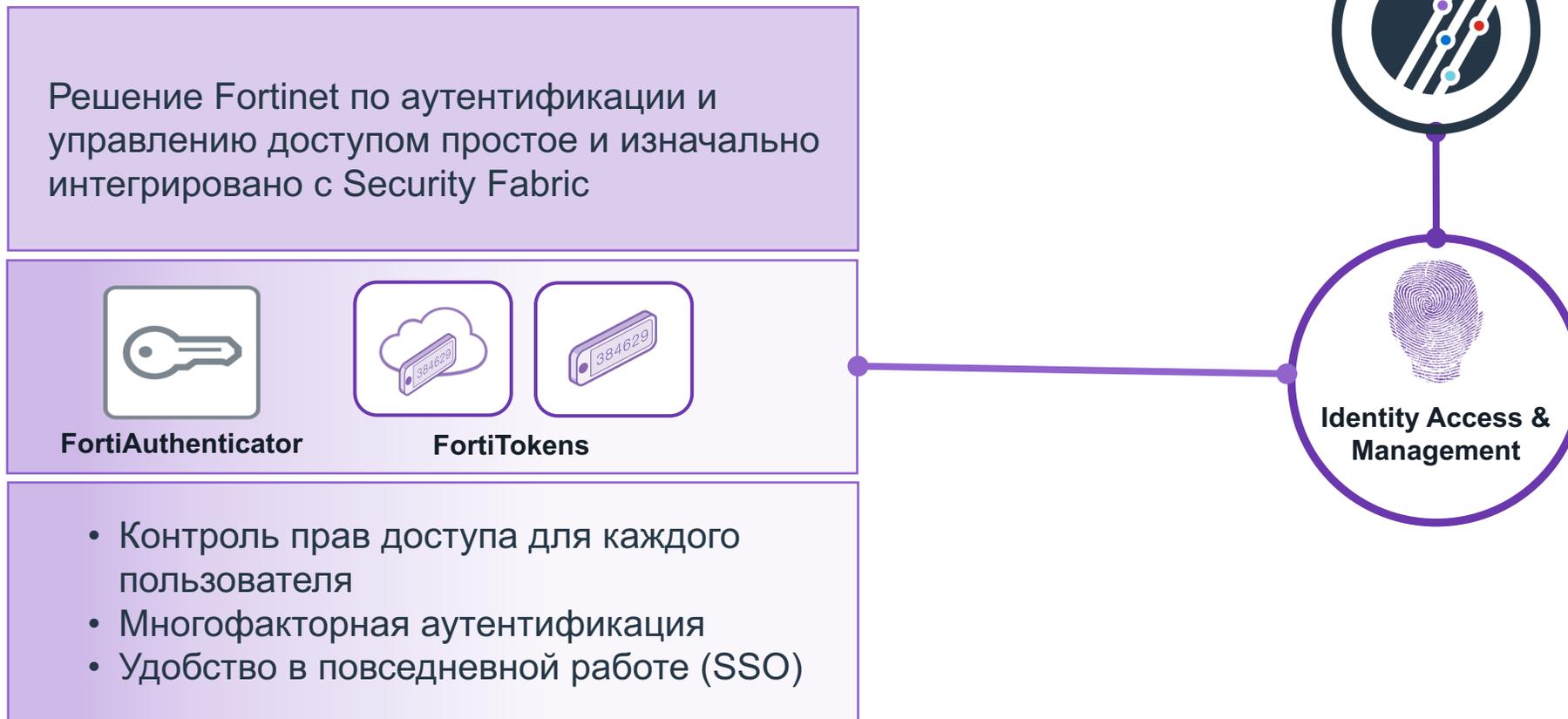
Уменьшение сложности сопровождения множества разнородных продуктов

Автоматизированная

Увеличение скорости управления и отклика

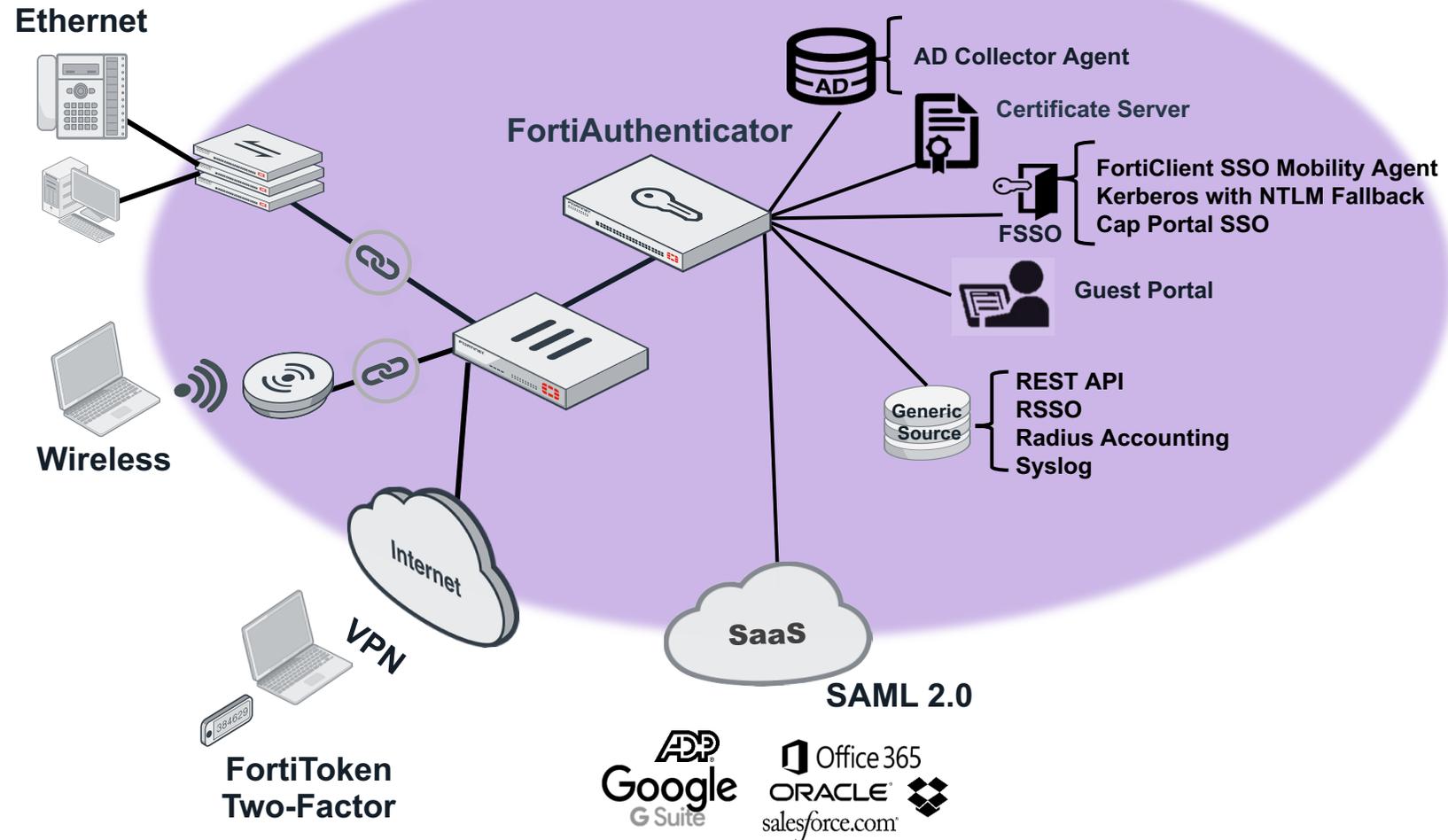


Безопасный доступ для пользователей



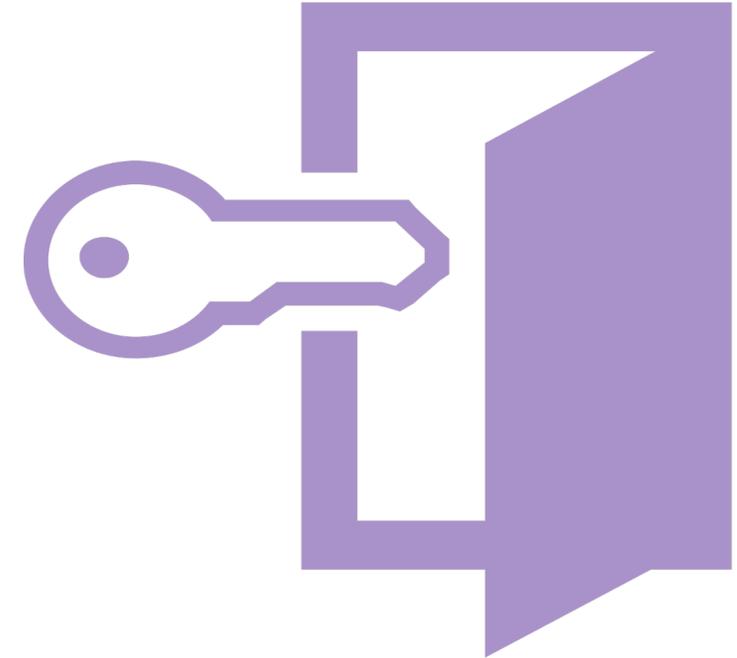
Управление идентификацией и доступом от Fortinet

- 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**

Лицензирование FAS (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 FAS: 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 FACS (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

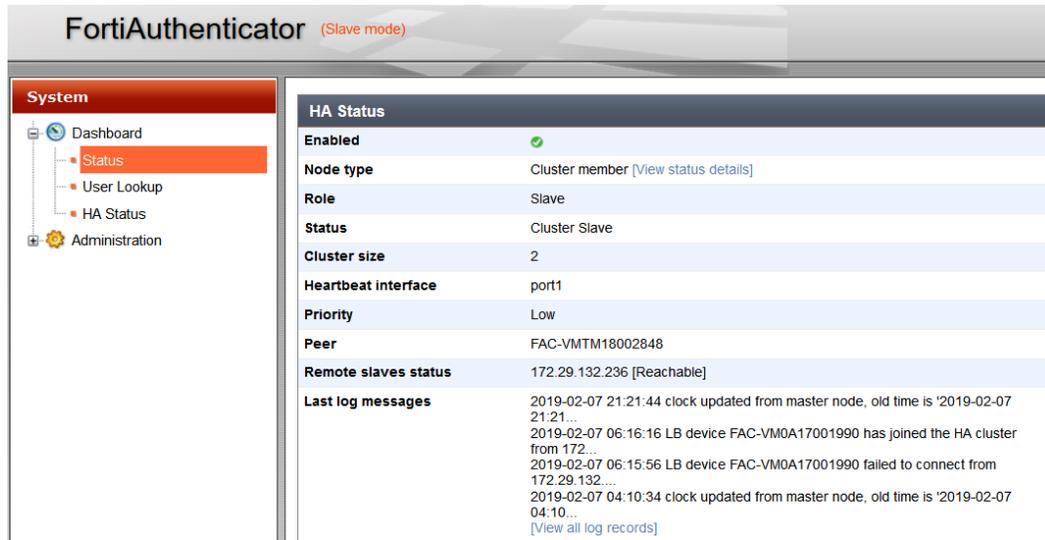
- Требования к HA:
 - Active/Passive (L2)
 - Платформы – одинаковые
 - ПО – одной версии
 - Лицензии
 - User Licenses - одинаковые
 - Token License – одна на кластер
 - Active/Active (L3)
 - Платформы – могут отличаться
 - ПО – одной версии
 - Лицензии
 - User Licenses – Могут отличаться (зависит от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



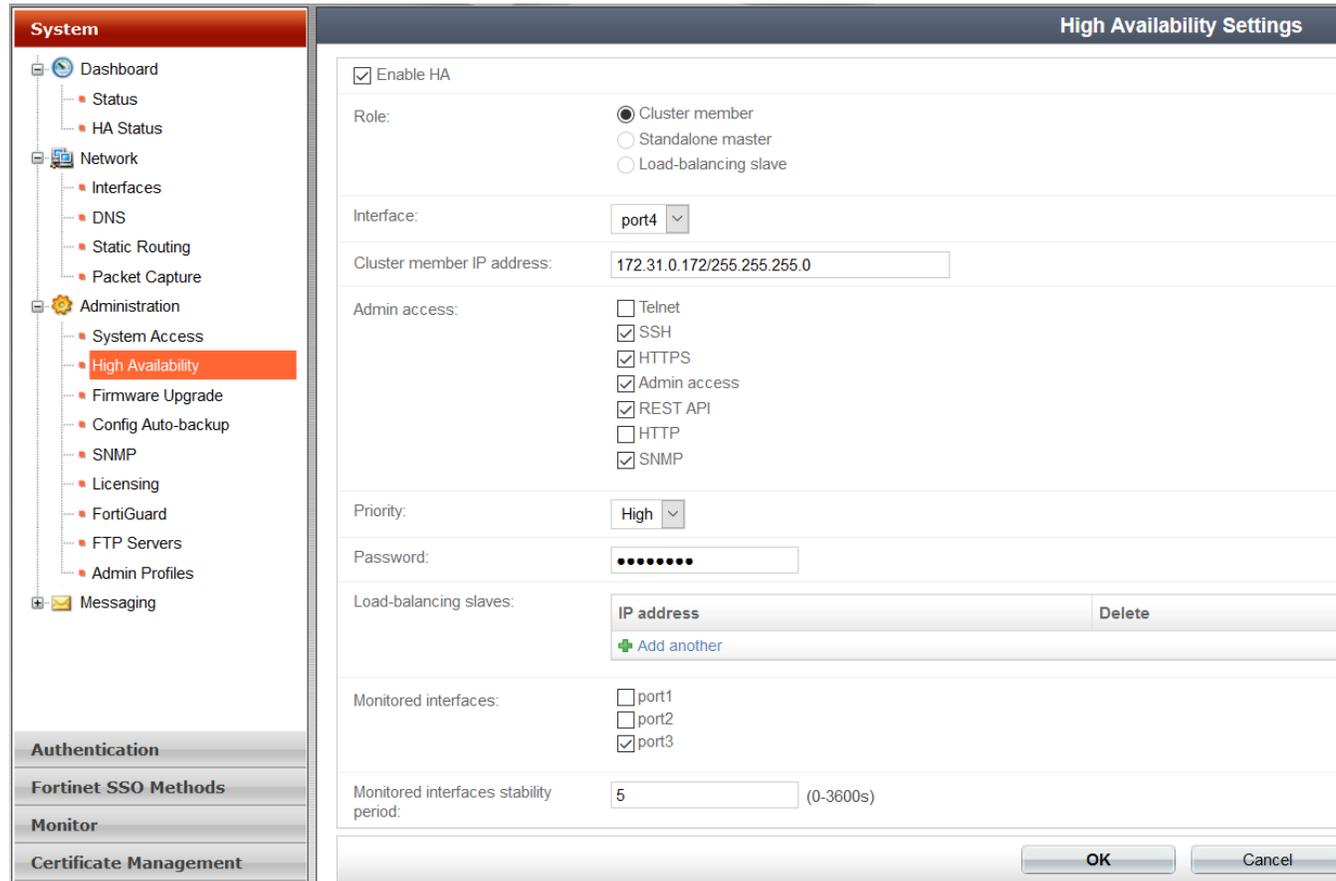
The screenshot shows the FortiAuthenticator web interface in 'Slave mode'. The left sidebar contains navigation options: Dashboard, Status (highlighted), User Lookup, HA Status, and Administration. The main content area displays the 'HA Status' page with the following details:

HA Status	
Enabled	✔
Node type	Cluster member [View status details]
Role	Slave
Status	Cluster Slave
Cluster size	2
Heartbeat interface	port1
Priority	Low
Peer	FAC-VMTM18002848
Remote slaves status	172.29.132.236 [Reachable]
Last log messages	2019-02-07 21:21:44 clock updated from master node, old time is '2019-02-07 21:21:...' 2019-02-07 06:16:16 LB device FAC-VM0A17001990 has joined the HA cluster from 172... 2019-02-07 06:15:56 LB device FAC-VM0A17001990 failed to connect from 172.29.132... 2019-02-07 04:10:34 clock updated from master node, old time is '2019-02-07 04:10:...' [View all log records]

- 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



The screenshot shows the Fortinet web interface for configuring High Availability (HA) settings. The left sidebar contains a navigation menu with categories: System, Authentication, Fortinet SSO Methods, Monitor, and Certificate Management. The 'System' menu is expanded, and 'High Availability' is selected. The main content area is titled 'High Availability Settings' and contains the following configuration options:

- Enable HA
- Role: Cluster member, Standalone master, Load-balancing slave
- Interface: port4
- Cluster member IP address: 172.31.0.172/255.255.255.0
- Admin access: Telnet, SSH, HTTPS, Admin access, REST API, HTTP, SNMP
- Priority: High
- Password: [masked]
- Load-balancing slaves: IP address [input field] Delete, Add another
- Monitored interfaces: port1, port2, port3
- Monitored interfaces stability period: 5 (0-3600s)

Buttons for 'OK' and 'Cancel' are located at the bottom right of the configuration area.

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:

The screenshot shows the Fortinet management interface. On the left is a navigation menu with categories: System, Network, Administration, and Messaging. Under 'System', 'HA Status' is selected. The main content area has a 'Refresh' button and displays two tables for cluster nodes.

Node 1 (This Node)

Node type	Cluster member (master)
Priority	High
Serial number	FAC-VMTM18000480
Status	Connected Reachable Cluster formed

Node 2

Node type	Cluster member (slave)
Priority	Low
Serial number	FAC-VMTM18003004
Status	Connected Reachable Cluster formed
External IP	172.31.0.171
Last heartbeat time	0s ago

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

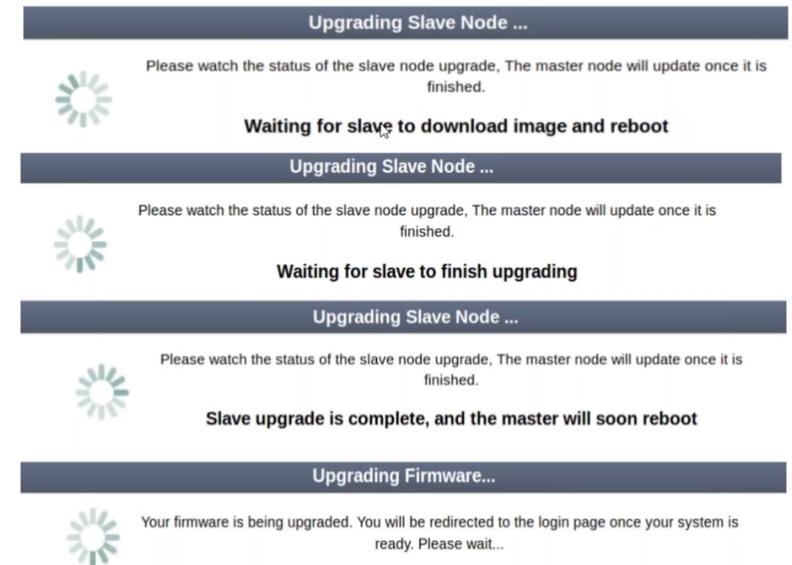
HA Cluster Member (Active-Passive)

- 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 – до 10 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 разработан 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

FortiAuthenticator (Load-balancing slave mode) Logged in as admin    FORTINET

System Refresh Rebuild Tables Reconnect

- Dashboard
 - Status
 - HA Status**
- Network
 - Interfaces
 - DNS
 - Static Routing
 - Packet Capture
- Administration
 - System Access
 - High Availability
 - Firmware Upgrade
 - Config Auto-backup
 - SNMP
 - Licensing
 - FortiGuard
 - FTP Servers
 - Admin Profiles
- Messaging

Authentication
Fortinet SSO Methods
Monitor
Certificate Management
Logging

Node 3 (This Node)

Node type	Load balancing slave
Serial number	FAC-VM0A16000424
Status	Connected Reachable

Replication Status

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
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Node 1

Node type	Cluster member (master)
Priority	High
Serial number	FAC-VM0A16000422
Status	Connected Reachable
External IP	10.10.10.10
Last heartbeat time	15s ago

Node 2

Node type	Cluster member (slave)
Priority	Low
Serial number	FAC-VM0A16000423
Status	Connected Reachable
External IP	10.10.10.100
Last heartbeat time	15s ago

HA Cluster Member (Active-Active)

- Вид со стороны Master

FortiAuthenticator Logged in as admin    FORTINET

System

- Dashboard
 - Status
 - HA Status
- Network
 - Interfaces
 - DNS
 - Static Routing
 - Packet Capture
- Administration
 - System Access
 - High Availability
 - Firmware Upgrade
 - Config Auto-backup
 - SNMP
 - Licensing
 - FortiGuard
 - FTP Servers
 - Admin Profiles
- Messaging
 - SMTP Servers
 - Email Services
 - SMS Gateways

Authentication

Fortinet SSO Methods

Monitor

Refresh

Node 1 (This Node)

Node type	Cluster member (master)
Priority	High
Serial number	FAC-VM0A16000422
Status	Connected Reachable Cluster formed

Node 2

Node type	Cluster member (slave)
Priority	Low
Serial number	FAC-VM0A16000423
Status	Connected Reachable Cluster formed
External IP	10.10.10.100
Last heartbeat time	0s ago

Node 3

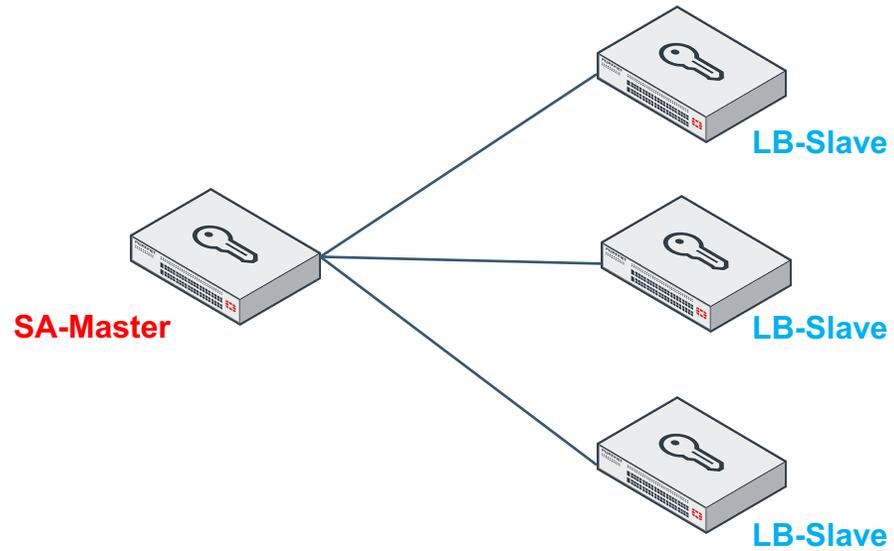
Node type	Load balancing slave
Serial number	FAC-VM0A16000424
Status	Connected Reachable
External IP	10.10.10.200
Last heartbeat time	16s ago

Replication Status

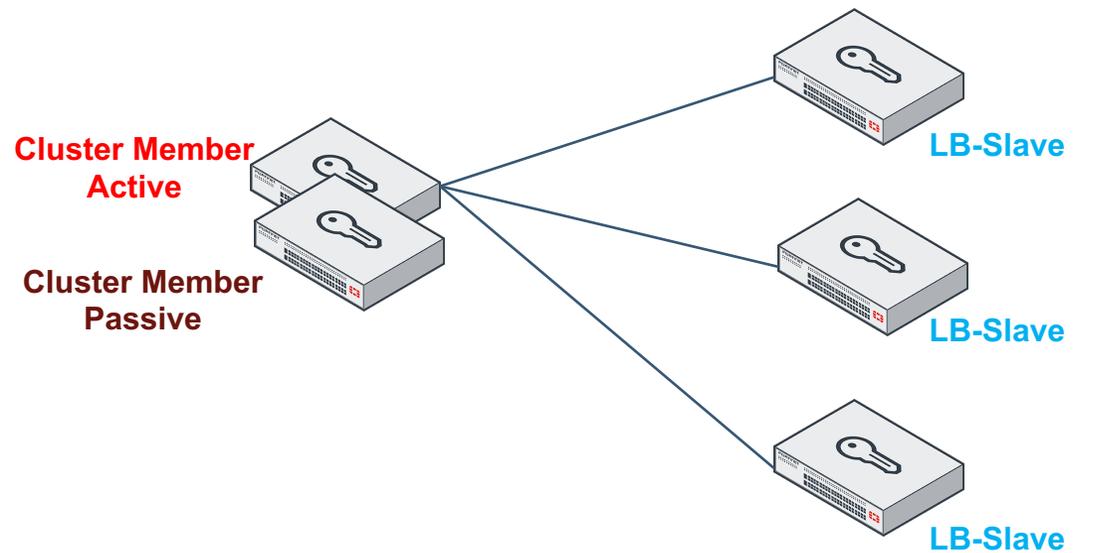
Users	User Profiles	User Groups	User Group Membership	FortiTokens	Remote LDAP Users	Remote RADIUS Users	LDAP Group Membership	RADIUS Group Membership	User RADIUS Attributes	Group RADIUS Attributes	LDAP RADIUS Attributes
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

HA Design Solutions

- *Standalone Master*



- *Redundant Master*



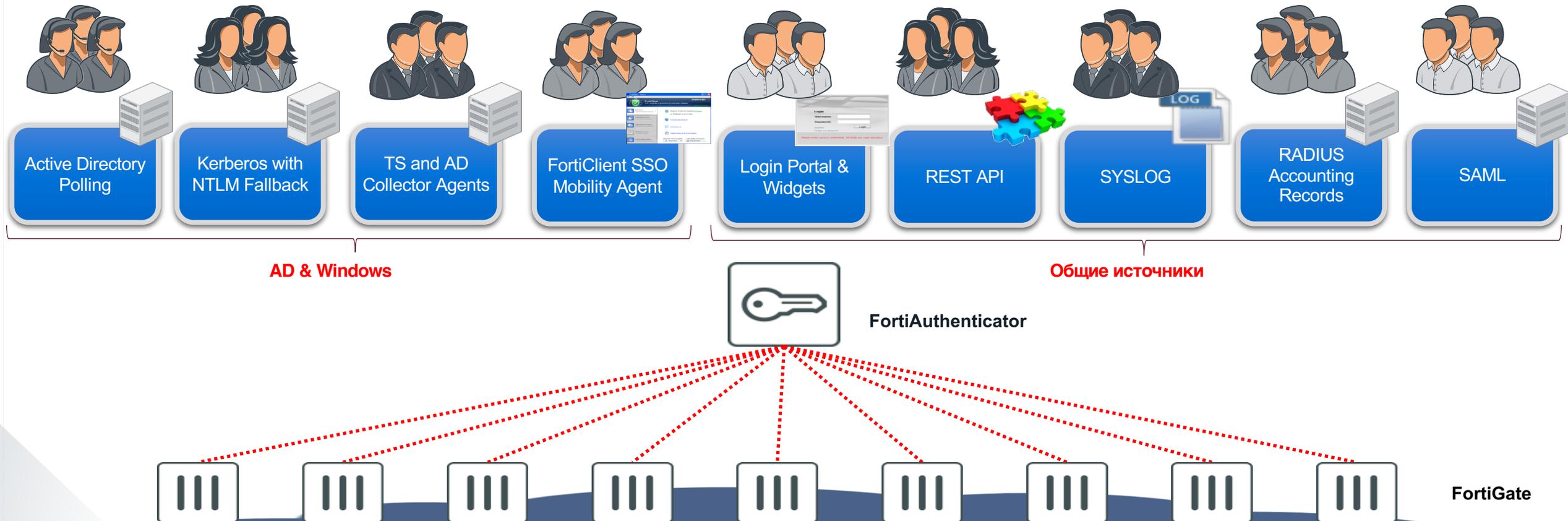


FortiAuthenticator

Сценарии Fortinet Single Sign-On (FSSO)

Fortinet Single Sign-On (FSSO)

- Источники информации о пользователях



FSSO методы

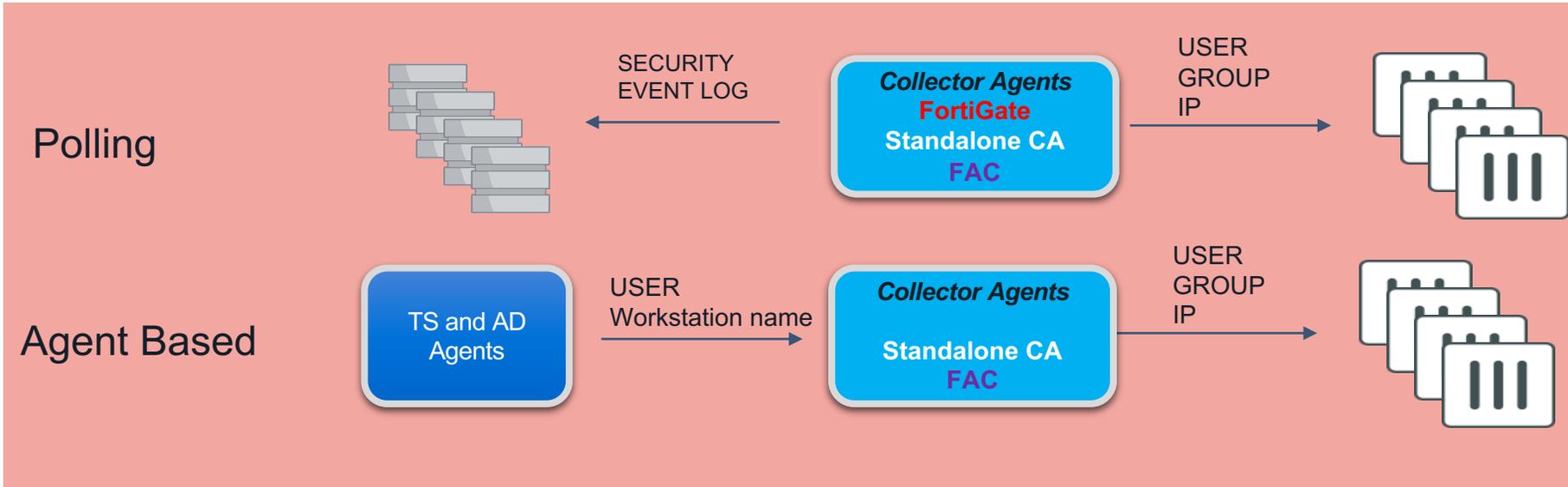
AD и Windows

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**)

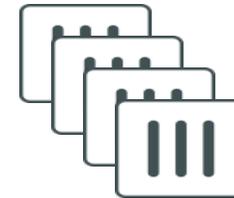
Наиболее точное и масштабируемое FSSO решение



USER IP



USER GROUP IP



Mobility Agent

- Sends identity (IP & DOMAINUsername) 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

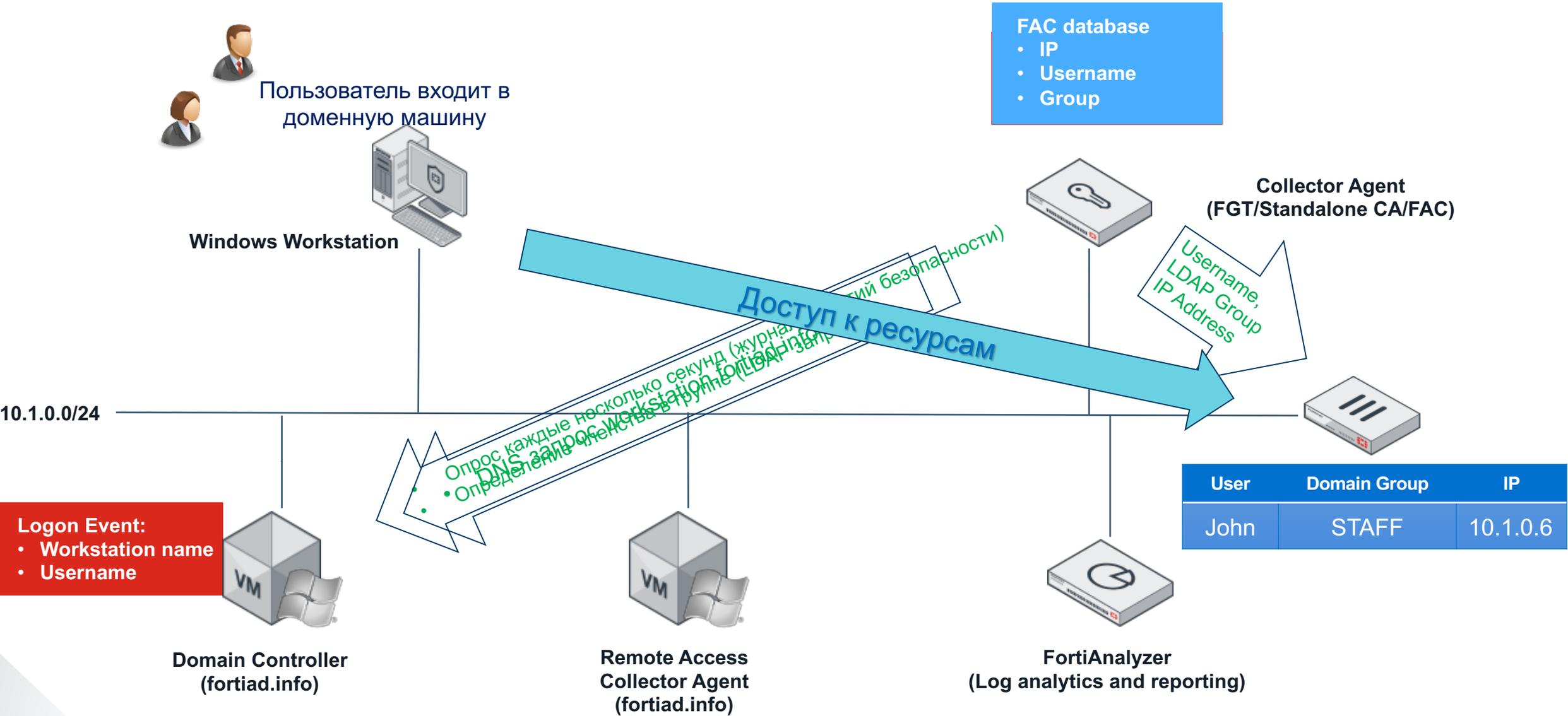
FSSO методы

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
 - Требуется открытие портов на Windows FW tcp ports 135&445
 - Рейтинг эффективности
 1. WinSec + Workstation WMI
 2. WinSec
 3. NetAPI

Режим Collector Agent Polling

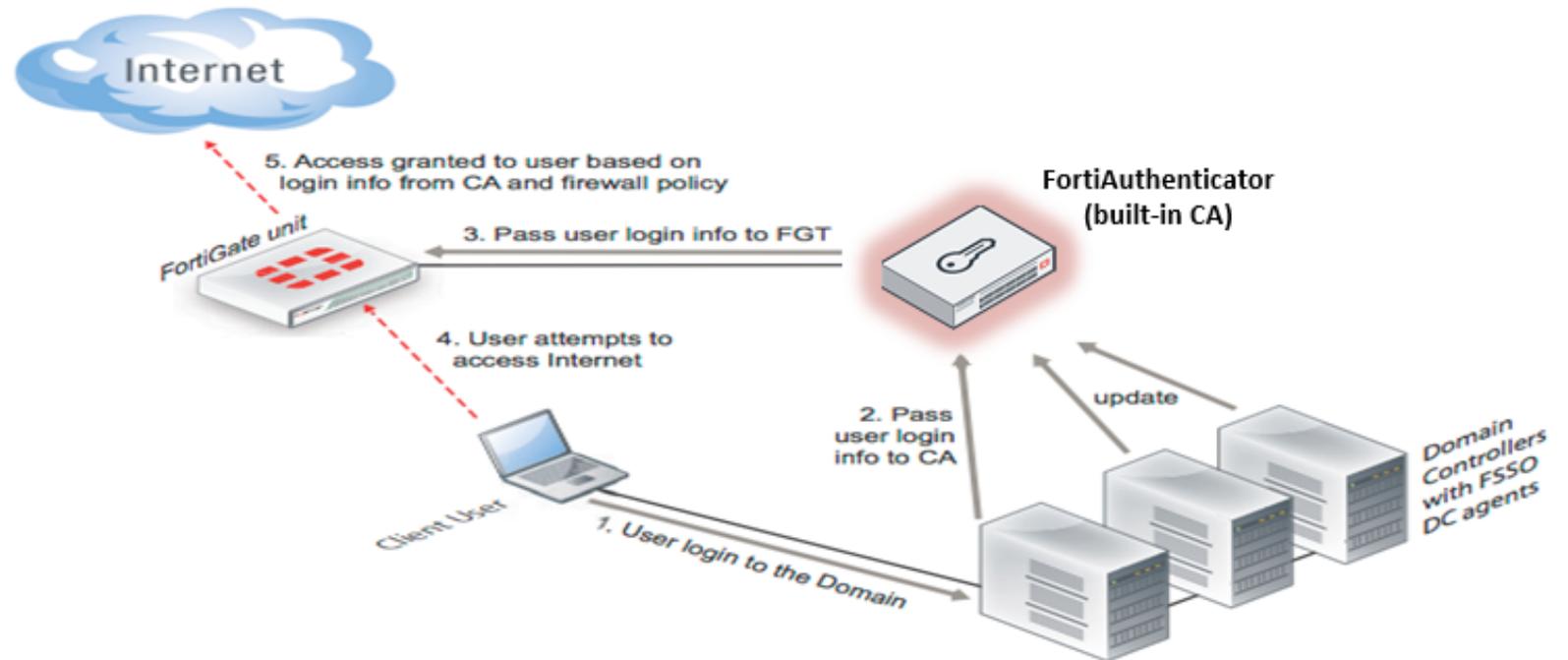


FSSO методы

AD и Windows – на базе агента

FSSO – AD Agent метод

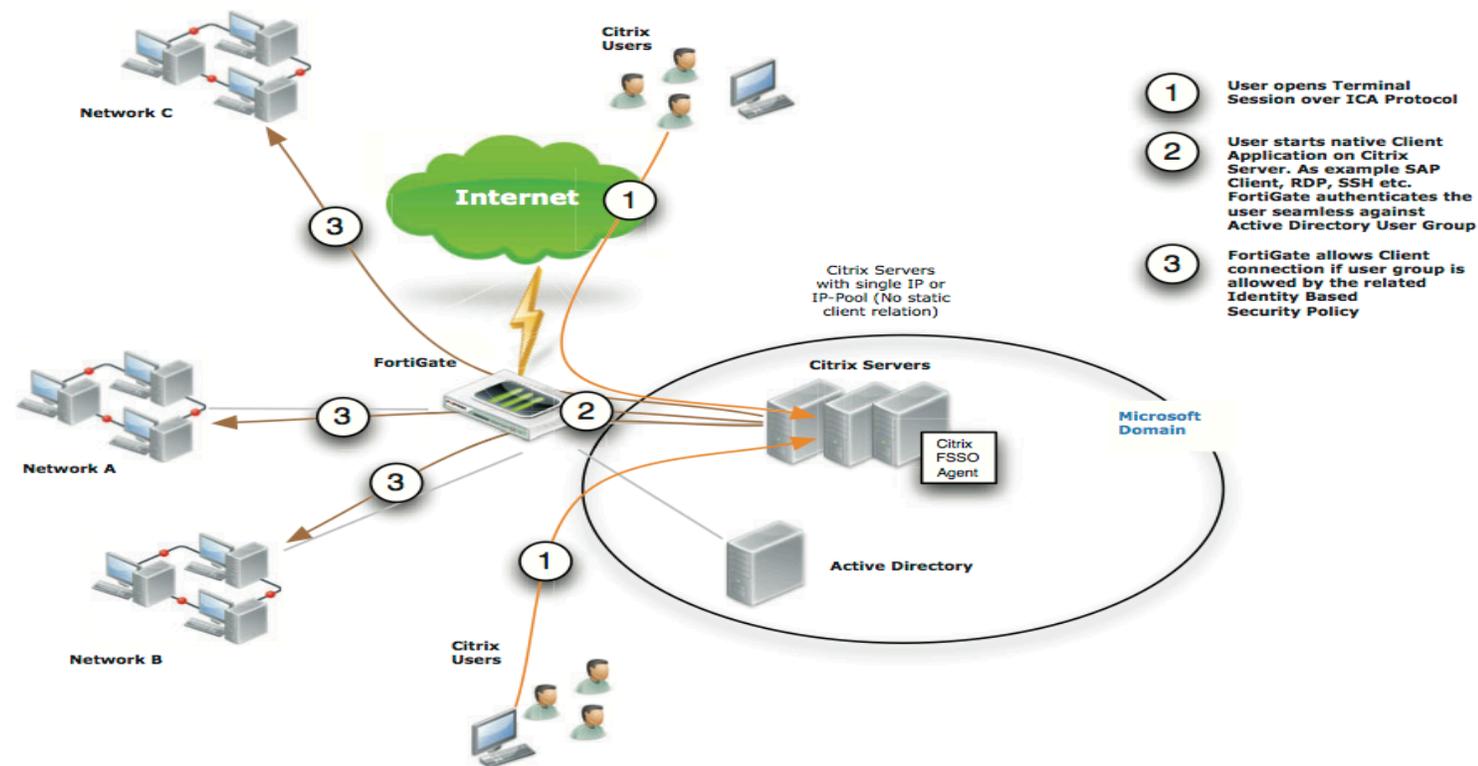
- Active Directory Agent



- » 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

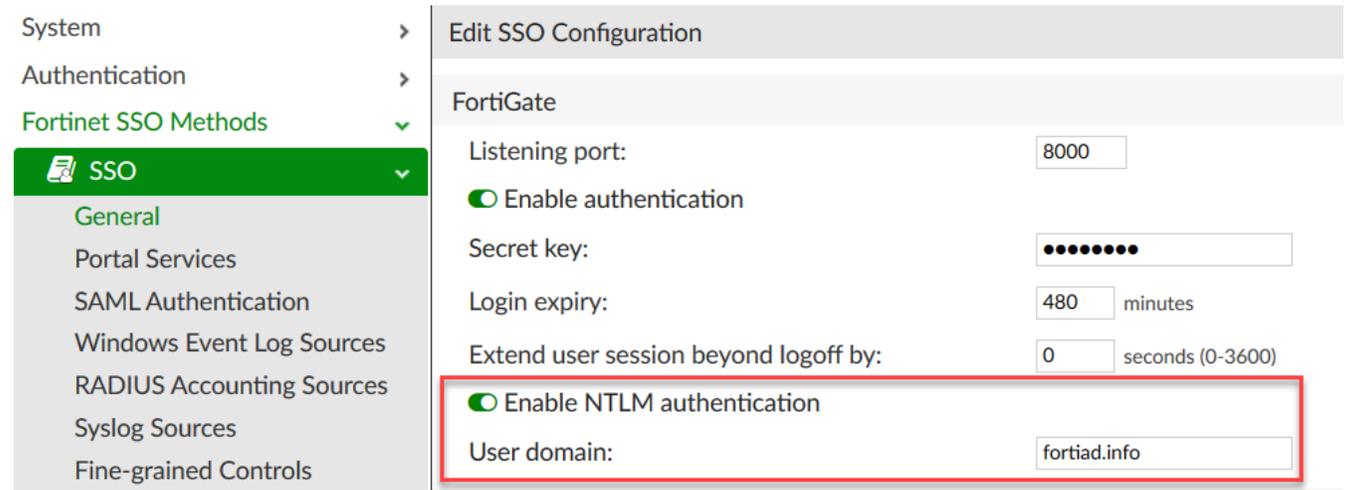


- » Позволяет отслеживать события logon множества пользователей с одного IP адреса
- » Основан на назначении разных source ports диапазонов для каждой сессии пользователя
- » Default pool имеет 200 портов
- » Может отправлять logon информацию на FortiAuthenticator
- » Поддерживает отслеживание logoff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

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



The screenshot shows the FortiGate configuration interface. On the left, a navigation menu is visible with the following items: System, Authentication, Fortinet SSO Methods, SSO (highlighted in green), General, Portal Services, SAML Authentication, Windows Event Log Sources, RADIUS Accounting Sources, Syslog Sources, and Fine-grained Controls. The main configuration area is titled 'Edit SSO Configuration' and shows the 'FortiGate' section. The following settings are visible: Listening port: 8000; Enable authentication: ; Secret key: [masked]; Login expiry: 480 minutes; Extend user session beyond logoff by: 0 seconds (0-3600); Enable NTLM authentication: (highlighted with a red box); User domain: fortiad.info.

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 выявления 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 смене 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

SSOMA Agent Solution



Пользователь входит в доменную машину

- FAC database
 - IP
 - Username
 - Group

Windows Workstation



SSOMA Agent – sends username and IP to FAC



FortiAuthenticator (Identity Access and Management)

Username, LDAP Group, IP Address

Доступ к ресурсам

Query LDAP server for Group membership



FortiAnalyzer

User	Domain Group	IP
Carl	STAFF	10.1.0.6

10.1.0.0/24



Domain Controller (fortiad.info)



Remote Access Collector Agent (fortiad.info)

Сравнение методов

	Решение на основе Collector Agent	Решение на основе SSO Mobility Agent
Точность	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Нет зависимостей• более высокая точность
Внедрение	<ul style="list-style-type: none">• Может быть развернут без FAC• Terminal Services Agent	<ul style="list-style-type: none">• Требуется установка агента на всех конечных точках• Terminal Services Agent
Общее	<ul style="list-style-type: none">• В режиме опроса он генерирует множество сообщений в больших сетях (каждые несколько секунд)• DNS-трафик• Опрос WMI	<ul style="list-style-type: none">• 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



FortiAuthenticator

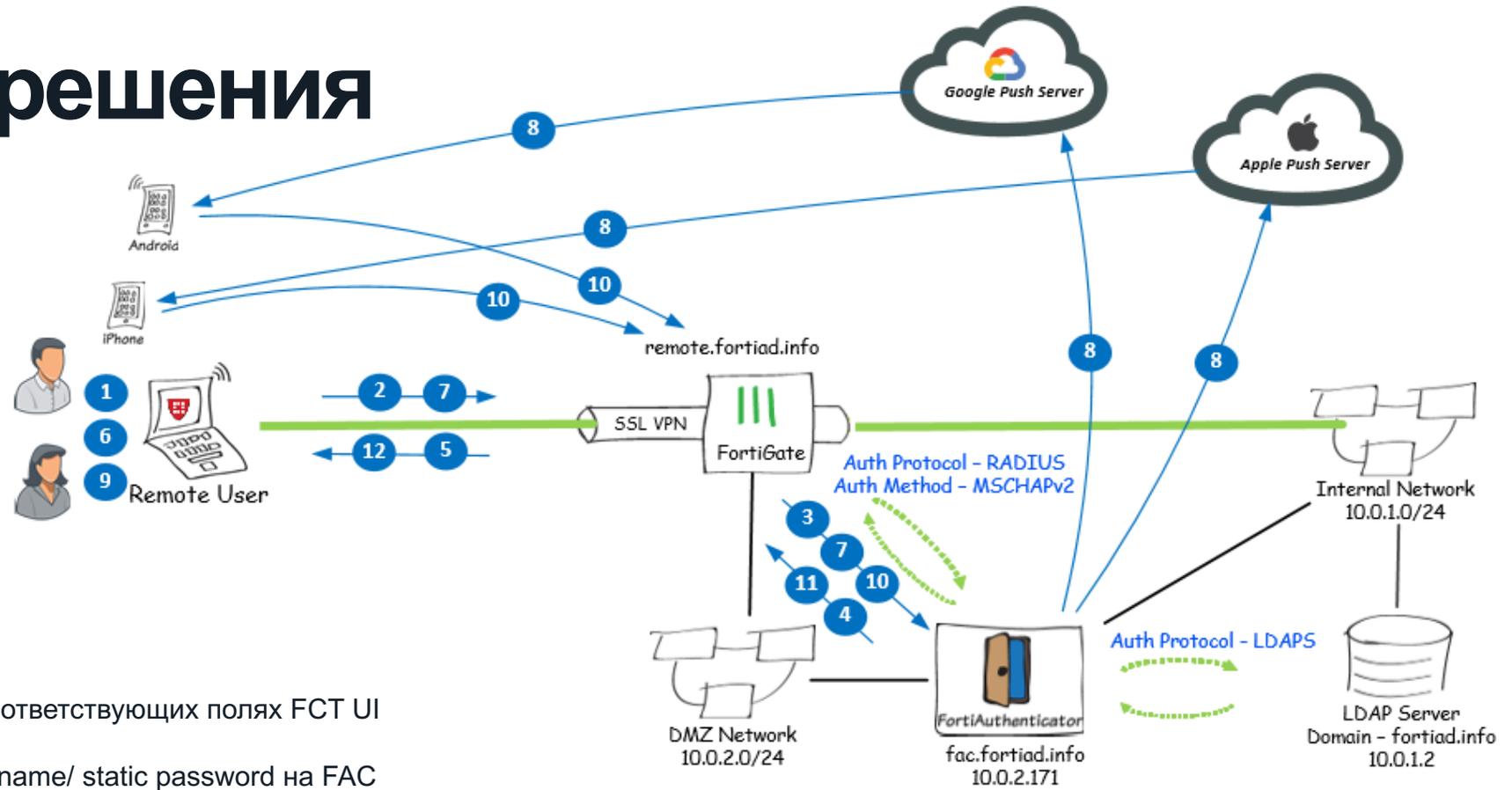
Пример настройки SSL-VPN с двухфакторной аутентификацией на основе FortiToken Mobile с применением Push Notification

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

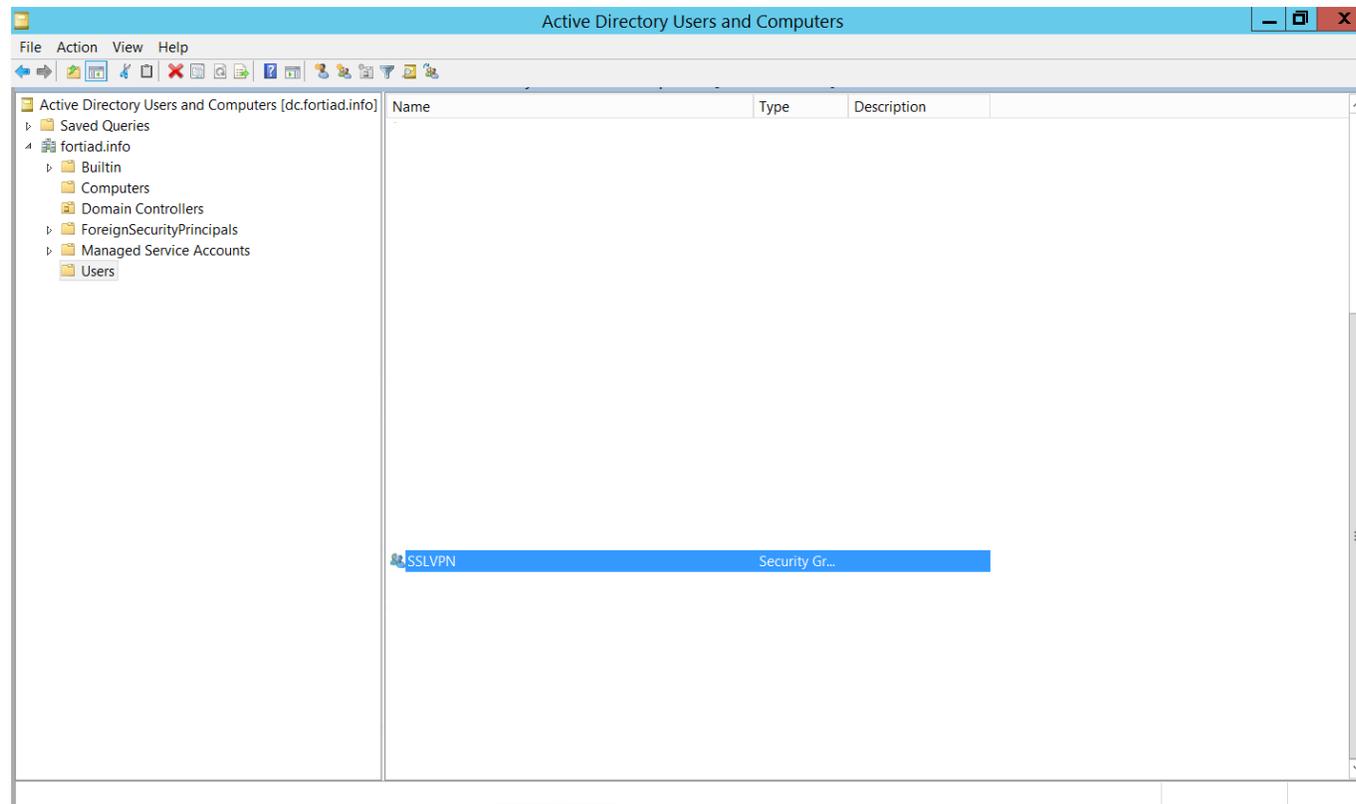
Процесс аутентификации для установки ssl vpn с 2FA, где второй фактор - FortiToken Mobile, настроенный для push-уведомлений, выглядит следующим образом:



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

The screenshot shows the 'Joe Bloggs Properties' dialog box with the following fields and values:

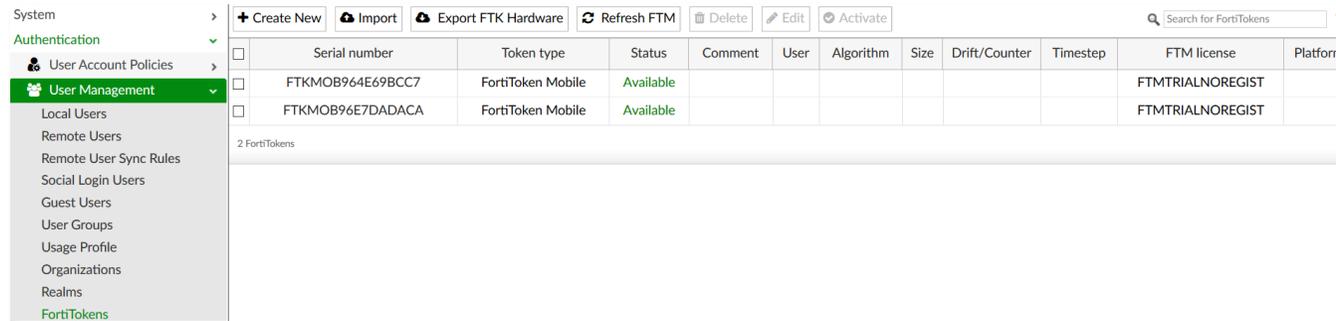
Field	Value
First name	Joe
Last name	Bloggs
Display name	Joe Bloggs
Description	
Office	
Telephone number	
E-mail	sini@fortinet.com
Web page	

The screenshot shows the 'SSLVPN Properties' dialog box, 'Members' tab. The 'Members' list contains one entry:

Name	Active Directory Domain Services Folder
Joe Bloggs	fortiad.info/Users

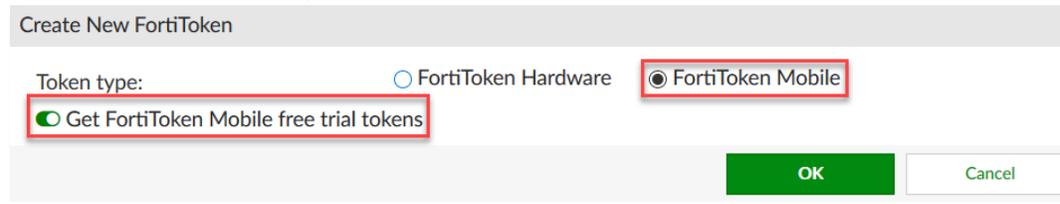
Настройка FortiAuthenticator

- Убедитесь, что FortiToken Mobile free trial tokens доступны в меню **Authentication → User Management → FortiTokens**



Serial number	Token type	Status	Comment	User	Algorithm	Size	Drift/Counter	Timestep	FTM license	Platform
FTKMOB964E69BCC7	FortiToken Mobile	Available							FTMTRIALNOREGIST	
FTKMOB96E7DADACA	FortiToken Mobile	Available							FTMTRIALNOREGIST	

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



Create New FortiToken

Token type: FortiToken Hardware FortiToken Mobile

Get FortiToken Mobile free trial tokens

OK Cancel

- 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.

The screenshot displays the 'Create New Remote LDAP User Synchronization Rule' configuration page. The left sidebar shows the navigation menu with 'User Management' expanded to 'Remote User Sync Rules'. The main configuration area includes the following fields and options:

- Name:** SSLVPN Users
- Remote LDAP:** fortiad.info_ldaps (10.100.88.5)
- Base distinguished name:** dc=fortiad,dc=info
- LDAP filter:** (memberOf=CN=SSLVPN,cn=Users,DC=fortiad,DC=info) [Test Filter]
- Synchronization Attributes:**
 - Token-based authentication sync priorities:**
 - FortiToken Mobile (assign an available token)
 - None (users are synced explicitly with no token-based authentication)
 - FortiToken Hardware (assign if serial number is provided)
 - FortiToken Hardware (assign an available token)
 - Email
 - SMS
- Sync every:** 1 hour(s)
- Sync as:** Remote LDAP User Local User
- User Role:**
 - Administrator
 - Sponsor
 - User

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>

System > Authentication > User Management > Create New User Group

Name: SSLVPN Users

Type: Local Remote LDAP Remote RADIUS Remote SAML MAC

User retrieval: Specify an LDAP filter Set a list of imported remote LDAP users

Remote LDAP: fortiad.info_ldaps (10.100.88.5)

LDAP filter: (memberOf=CN=SSLVPN,cn=Users,DC=fortiad,DC=info) Test Filter

Usage Profile [Please Select]

OK Cancel

Test LDAP Filter

LDAP server: 10.100.88.5:636

Filter: (memberOf=CN=SSLVPN,cn=Users,DC=fortiad,DC=info) Apply Clear

Filter child nodes and show number of children

📁 CN=Users (1)
📁 CN=Joe Bloggs

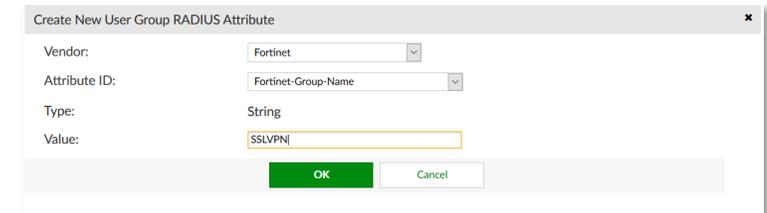
Organization: [Please Select]

Use Filter Cancel

- Выбираем **Test Filter** для просмотра всех пользователей в данной группе AD
- Выберите OK, 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)



Create New User Group RADIUS Attribute

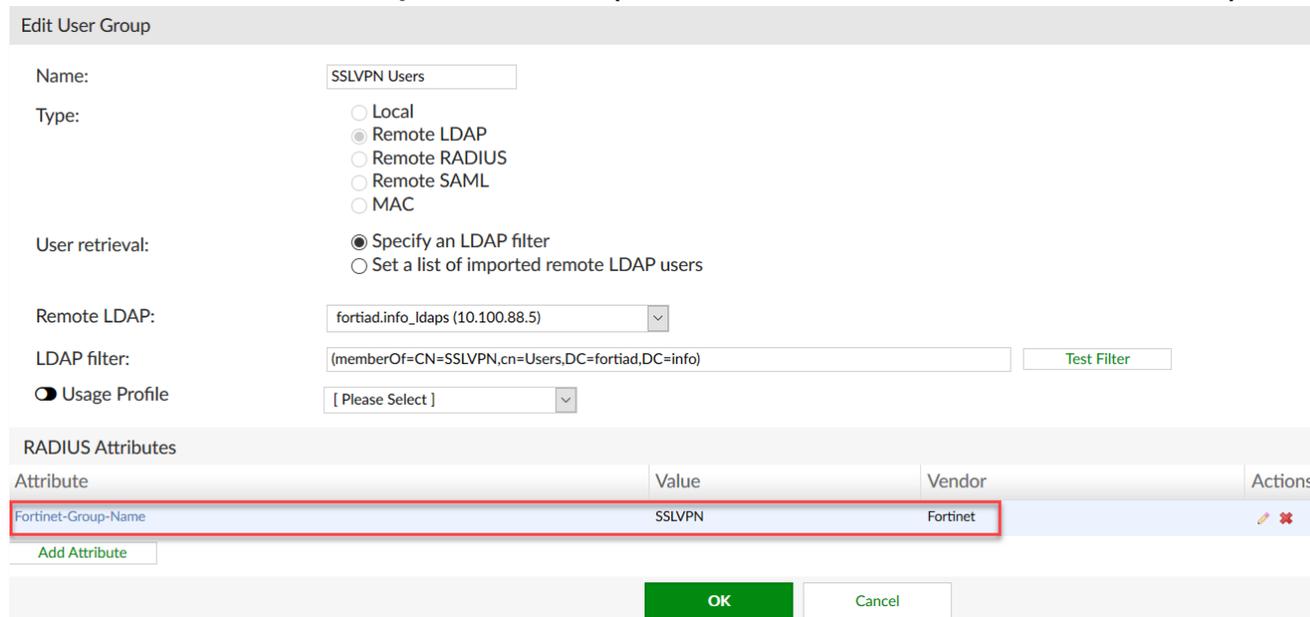
Vendor: Fortinet

Attribute ID: Fortinet-Group-Name

Type: String

Value: SSLVPN

OK Cancel



Edit User Group

Name: SSLVPN Users

Type:
 Local
 Remote LDAP
 Remote RADIUS
 Remote SAML
 MAC

User retrieval:
 Specify an LDAP filter
 Set a list of imported remote LDAP users

Remote LDAP: fortiad.info_ldaps (10.100.88.5)

LDAP filter: (memberOf=CN=SSLVPN,cn=Users,DC=fortiad,DC=info) [Test Filter](#)

Usage Profile: [Please Select]

RADIUS Attributes

Attribute	Value	Vendor	Actions
Fortinet-Group-Name	SSLVPN	Fortinet	Edit Delete

[Add Attribute](#)

OK Cancel

Настройка FortiAuthenticator (5)

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

Create New Realm

Name:

User source:

Chained token authentication with remote RADIUS 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>

Edit RADIUS Client

Name: FG12

Client address: IP/Hostname Subnet Range
10.100.88.136

Secret:

Guest portal: Accept guest portal requests from related Access Points

Accept RADIUS accounting messages for usage enforcement
 Support RADIUS Disconnect messages

Profiles

Default

Add New Profile

Profile name: Default

Description:

Apply this profile based on RADIUS attributes.

EAP types: EAP-GTC EAP-TLS PEAP EAP-TTLS

Device Authentication

MAC Authentication Bypass(MAB)
 AD machine authentication
 MAC device filtering

User Authentication

Authentication method: Enforce two-factor authentication
 Apply two-factor authentication if available (authenticate any user)
 Password-only authentication (exclude users without a password)
 FortiToken-only authentication (exclude users without a FortiToken)

Enable FortiToken Mobile push notifications authentication

Username input format: username@realm
 realm/username
 realm/username

Realms:

Default	Realm	Allow local users to override remote users	Use Windows AD domain authentication	Groups	Delete
<input checked="" type="radio"/>	fortiad.info fortiad.info Idaps (10.100.88.5)	<input type="checkbox"/>	<input type="checkbox"/>	Filter: SSLVPN Users (Edit)	

Add a realm

Save

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

Edit System Access Settings

Administrative Access

- Require strong cryptography.
- Enable pre-authentication warning message.

CLI Access

CLI idle timeout: 0 minutes (0-480 mins)

GUI Access

GUI idle timeout: 480 minutes (1-480 mins)

Maximum HTTP header length: 4 (4-16 KB)

HTTPS Certificate: fac9_portal.fortiad.info | O=FortiAD, CN=fac9.fortiad.info, emailAddress=support@fortiad.info

HTTP Strict Transport Security(HSTS) Expiry 180 (0-730 days)

Certificate authority type: Local CA Trusted CA

CA certificate that issued the server certificate: FAC9_ROOT_CA | O=FortiAD, CN=fac9.fortiad.info, emailAddress=support@fortiad.info

Additional allowed hosts/domain names: 10.100.88.175, 172.31.0.175, portal2.fortiad.info, remote.fortiad.info

Public IP/FQDN for FortiToken Mobile: remote.fortiad.info:5555

OK

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)**

The screenshot shows the 'Edit Network Interface' configuration page. The interface is named 'port2' and is currently up. The IP address is set to 10.100.88.175/255.255.255.0. Under 'Access Rights', the 'Admin access' section has 'SSH' and 'HTTPS' (with sub-options 'GUI (/login)', 'REST API (/api)', and 'Fabric (/api/v1/fabric)') checked. The 'Services' section has 'HTTPS' checked, with several sub-options including 'FortiToken Mobile API (/api/v1/pushauthresp, /api/v1/transfertoken)', which is highlighted with a red box.

Edit Network Interface	
Interface Status	
Interface:	port2
Status:	●
IP Address / Netmask	
IPv4:	10.100.88.175/255.255.255.0
IPv6:	
Access Rights	
Admin access:	<input type="radio"/> Telnet <input checked="" type="radio"/> SSH <input checked="" type="checkbox"/> HTTPS <ul style="list-style-type: none"><input checked="" type="radio"/> GUI (/login)<input checked="" type="radio"/> REST API (/api)<input checked="" type="radio"/> Fabric (/api/v1/fabric) <input type="radio"/> HTTP (GUI) <input type="radio"/> SNMP
Services:	<input checked="" type="checkbox"/> HTTPS <ul style="list-style-type: none"><input checked="" type="radio"/> Self-service Portal (/login)<input checked="" type="radio"/> Guest Portals (/guests)<input checked="" type="radio"/> SAML IdP (/saml-idp)<input checked="" type="radio"/> SAML SP SSO (/saml-sp, /login/saml-auth)<input checked="" type="radio"/> Kerberos SSO (/login/kerb-auth)<input checked="" type="radio"/> SCEP (/cert/scep)<input checked="" type="radio"/> CRL Downloads (/cert/crl)<input checked="" type="radio"/> FortiToken Mobile API (/api/v1/pushauthresp, /api/v1/transfertoken)<input checked="" type="radio"/> OAuth Service API (/api/v1/oauth)

Настройка FortiGate

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

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > Security Profiles > VPN > **User & Device** > User Definition > User Groups > Guest Management > Device Inventory > Custom Devices & Groups > LDAP Servers > **RADIUS Servers** > Authentication Settings > FortiTokens > SAML SSO > WiFi & Switch Controller >

Edit RADIUS Server

Name: FortiAuthenticator

Authentication method: Default Specify

NAS IP:

Include in every user group:

Primary Server

IP/Name: 10.100.88.175

Secret:

Connection status: Successful

Test Connectivity

Test User Credentials

Secondary Server

IP/Name:

Secret:

Test Connectivity

Test User Credentials

OK Cancel

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

Test User Credentials

Username: joe

Password:

Connection status: Successful

User credentials: Successful

Server message:

```
AVP: 1=14 t=Vendor-Specific(26) v=Fortinet(12356)
VSA: 1=8 t=Fortinet-Group-Name(1)
Value: 'SSLVPN'
```

Test Close

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**

New User Group

Name: SSLVPN Users

Type: Firewall

Members: +

Remote Groups

+ Add Edit Delete

Remote Server	Group Name
No matching entries found	

OK Cancel

New User Group

Name: SSLVPN Users

Type: Firewall

Members: +

Remote Groups

+ Add Edit Delete

Remote Server	Group Name
FortiAuthenticator	SSLVPN

OK Cancel

Add Group Match

Remote Server: FortiAuthenticator

Groups: any Specify

SSLVPN

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**

New Authentication/Portal Mapping

Users/Groups: SSLVPN Users

Realm: Default realm Specify

Portal: full-access

Authentication/Portal Mapping ⓘ

+ Create New Edit Delete

Users/Groups	Realm	Portal
SSLVPN Users	/	full-access
All Other Users/Groups	/	web-access

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**

New Virtual IP

VIP type: IPv4

Name: VIP-to-FAC with port forwarding

Comments: Write a comment... 0/255

Color: Change

Network

Interface: any

Type: Static NAT

External IP address/range: 100.100.100.100

Mapped IP address/range: 10.100.88.5

Optional Filters: Off

Port Forwarding: On

Protocol: TCP

External service port: 55555

Map to port: 443

remote.fortiad.info

FAC IP address

Port advertised on FAC

Edit System Access Settings

Administrative Access

Require strong cryptography.

Enable pre-authentication warning message.

CLI Access

CLI idle timeout: 0 minutes (0-480 mins)

GUI Access

GUI idle timeout: 480 minutes (1-480 mins)

Maximum HTTP header length: 4 (4-16 KB)

HTTPS Certificate: fac9_portal.fortiad.info | O=FortiAD, CN=fac9.fortiad.info, emailAddress=support@fortiad.info

HTTP Strict Transport Security(HSTS) Expiry: 180 (0-730 days)

Certificate authority type: Local CA Trusted CA

CA certificate that issued the server certificate: FAC9_ROOT_CA | O=FortiAD, CN=fac9.fortiad.info, emailAddress=support@fortiad.info

Additional allowed hosts/domain names: 10.100.88.175, 172.31.0.175, portal2.fortiad.info, remote.fortiad.info

Public IP/FQDN for FortiToken Mobile: remote.fortiad.info:55555

OK

Настройка FortiGate (6)

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

SSL-VPN tunnel interface (ssl.root) → SERVER 2							
51		SSLVPN_TUNNEL_ADDR1 SSLVPN Users	all	always	ALL	ACCEPT	Enabled

- 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

UNTRUSTED → SERVER 2							
49		all	VIP-to-FAC with	always	ALL	ACCEPT	Disabled

- To allow FortiAuthenticator access to the Internet

SERVER → UNTRUSTED 4							
52		FortiAuthenticator	all	always	ALL	ACCEPT	Enabled

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**

<input type="button" value="+ Create New"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Manual Sync"/>				● LDAP users ○ SAML users		
<input type="checkbox"/>	Name	Remote LDAP	Base Distinguished Name	LDAP filter	Sync every	Last Sync
<input checked="" type="checkbox"/>	SSLVPN Users	fortiad.info_ldaps (10.100.88.5)	dc=fortiad,dc=info	(memberOf=CN=SSLVPN,cn=Users,DC=fortiad,DC=info)	14 days	Tue Jun 18 10:58:42 2019

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

<input type="button" value="Import"/> <input type="button" value="Export Users"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Re-Enable"/>				Search for remote LDAP users <input type="text"/>		● LDAP users
<input type="checkbox"/>	Username	Remote LDAP server	Admin	Status	Token	
<input type="checkbox"/>	joe	fortiad.info_ldaps (10.100.88.5)	+	✓	FortiToken Mobile (FTKMOB96E7DADACA)	

- 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

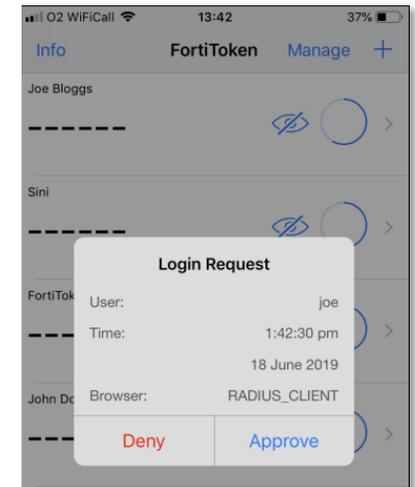
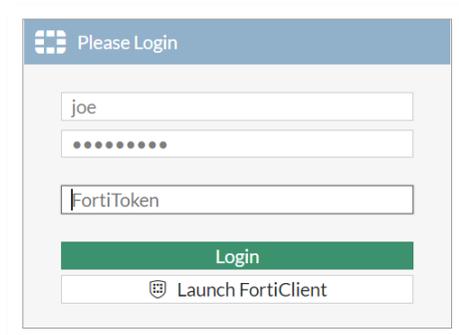
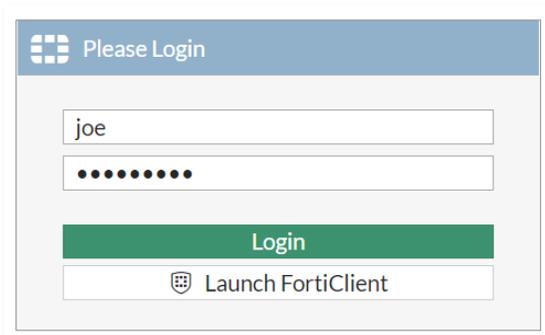
"EEIO4QBQZN634OAAQ"

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 you will need to contact your system administrator to re-enable your activation.

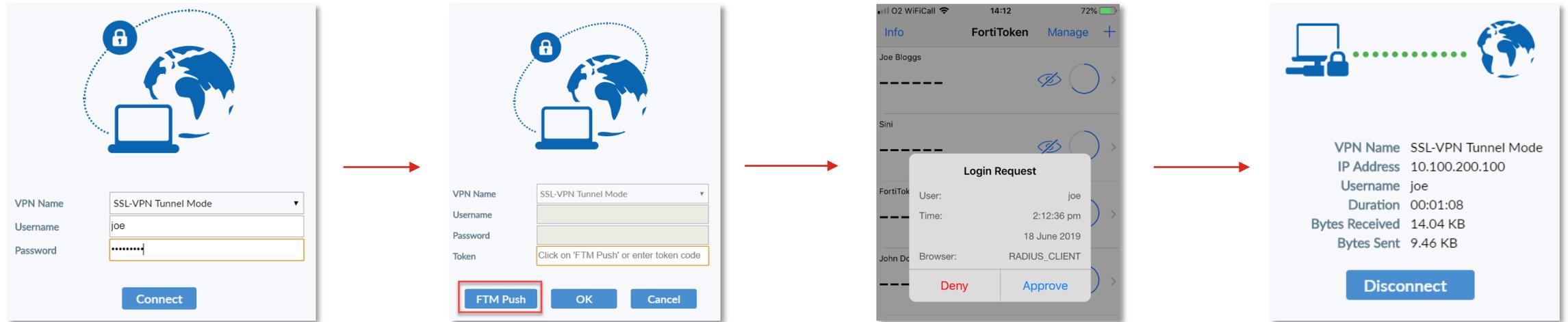
Проверка (3)

- 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
- Пример Web based ssl-vpn



Проверка (4)

- Пример Tunnel (FortiClient) based ssl-vpn



Проверка и диагностика

- FortiAuthenticator Log File entry

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

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

F **ORTINET**®