



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 FortiAuthenticator 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



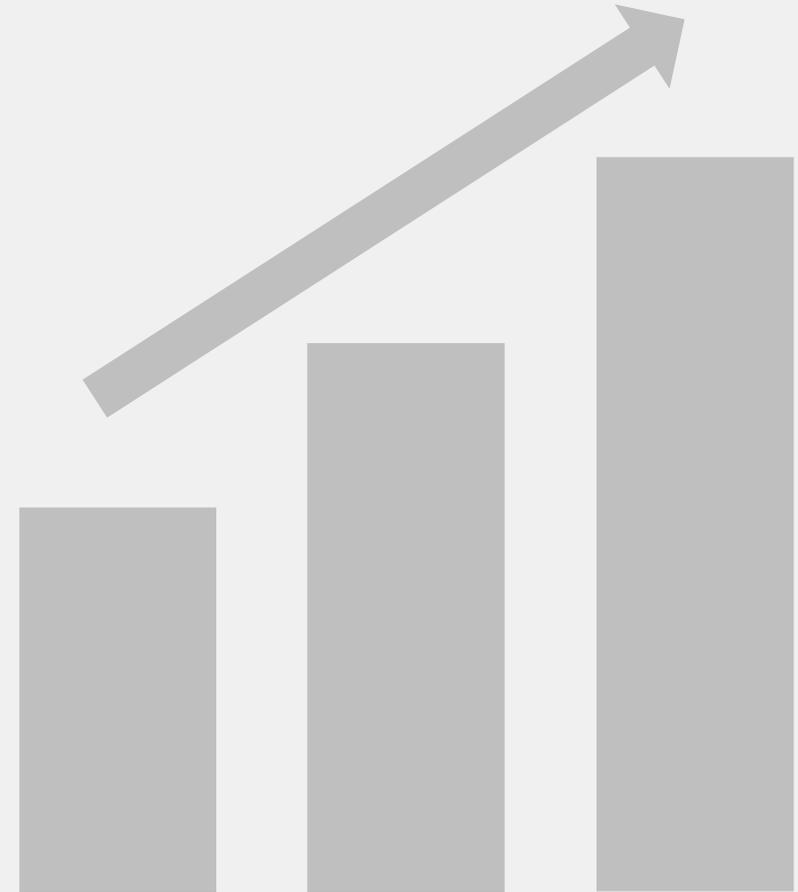
Слабая аутентификация и неправильное управление доступом делают сеть уязвимой

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

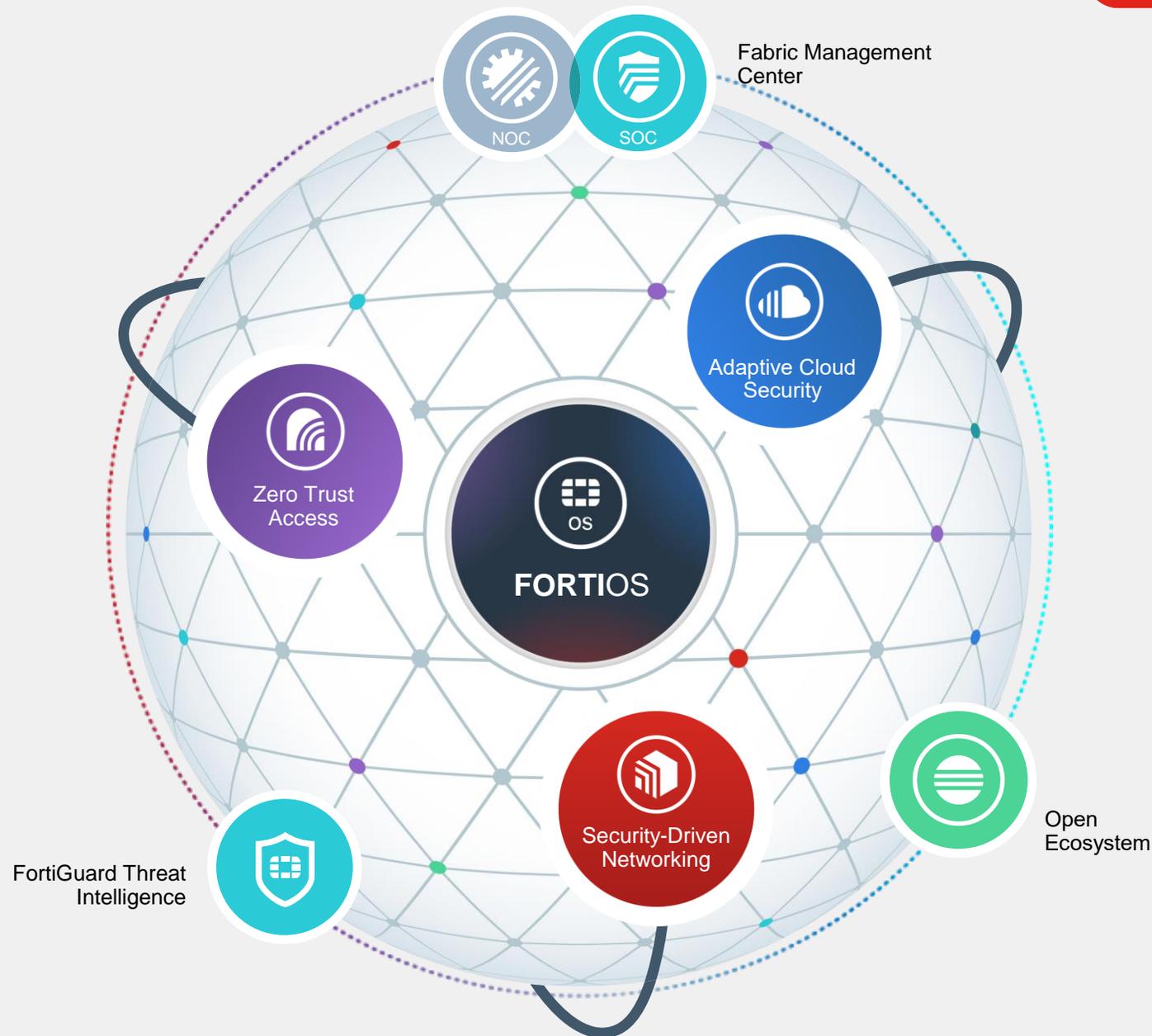
Полная видимость атакуемой поверхности для лучшего управления рисками ИБ

Комплексность

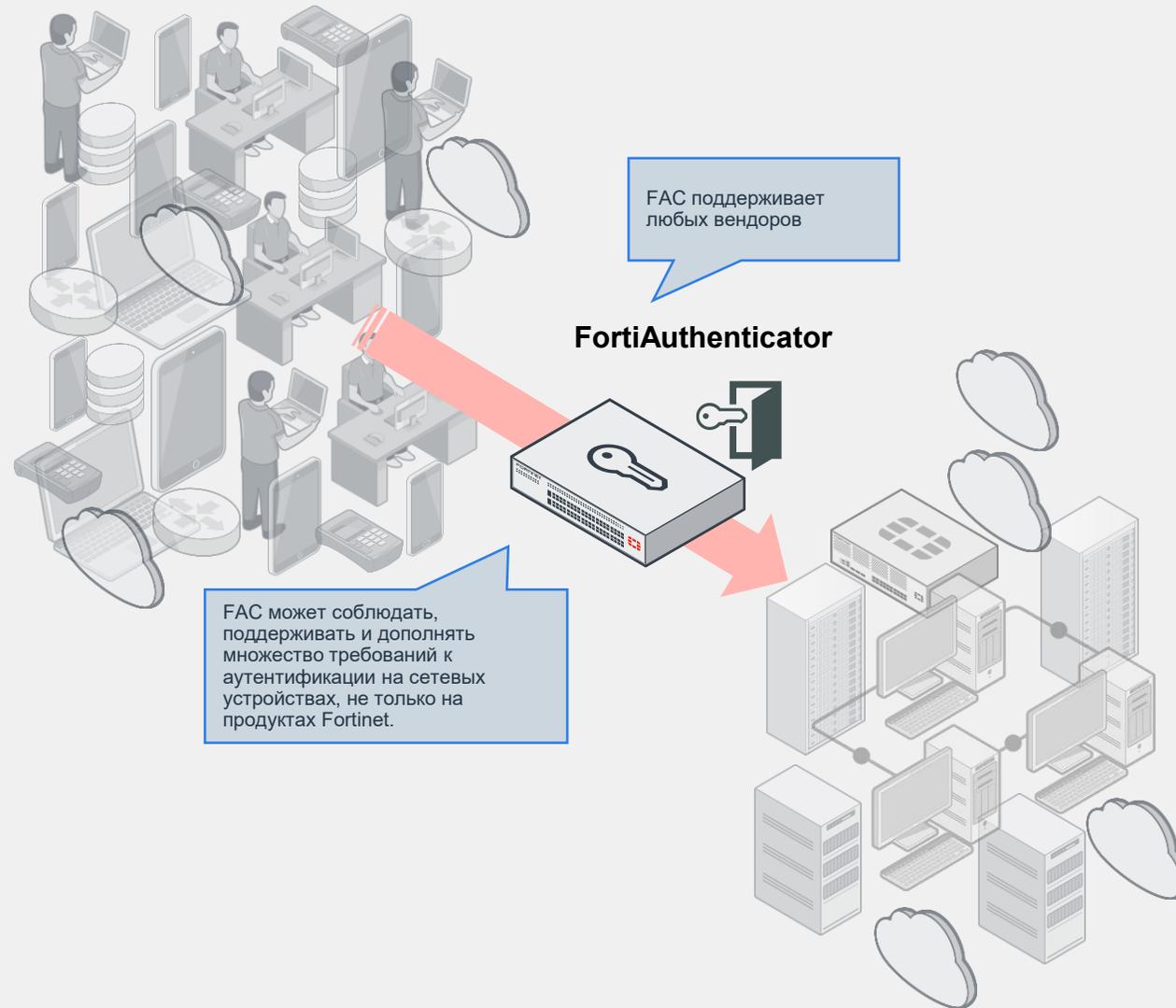
Снижение стоимости эксплуатации за счет объединения всех компонентов в рамках единой платформы

Автоматизация

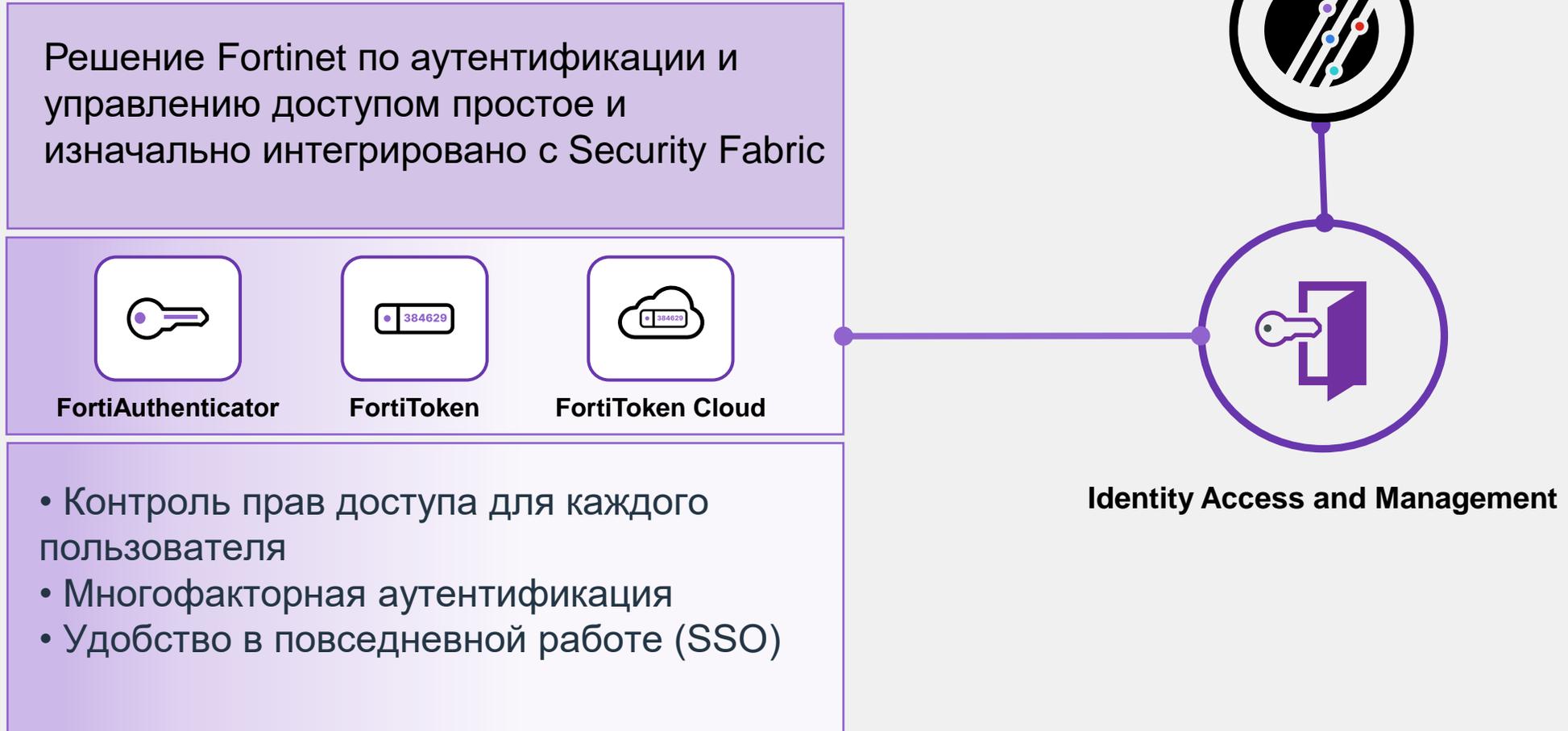
Самостоятельная инфраструктура под управлением искусственного интеллекта



FortiAuthenticator



Fortinet Identity и Access Management (IAM)



Обзор возможностей FortiAuthenticator

Идентификация и аутентификация

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

Двухфакторная аутентификация

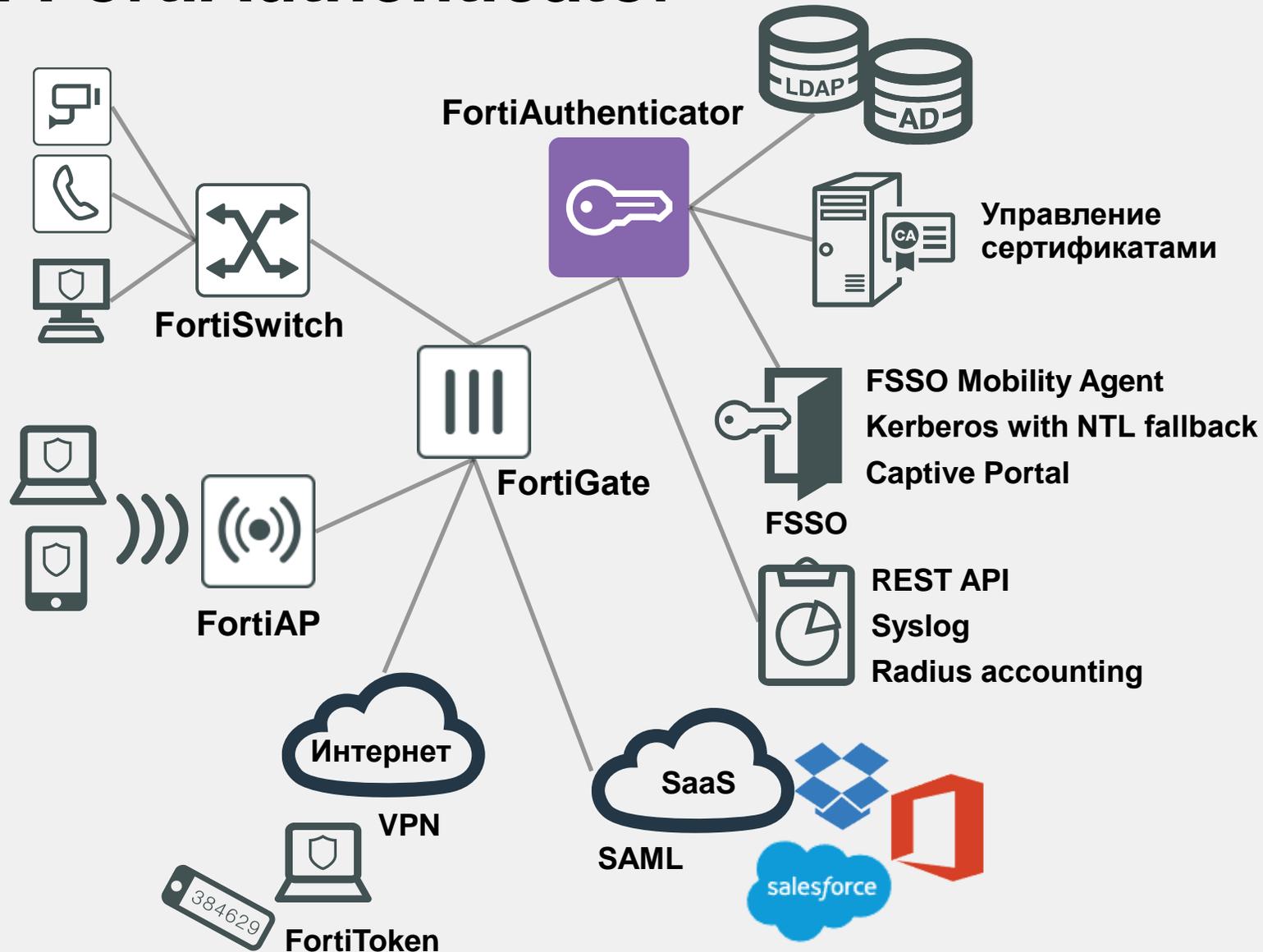
- FortiToken, физический/программный
- SMS/email

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

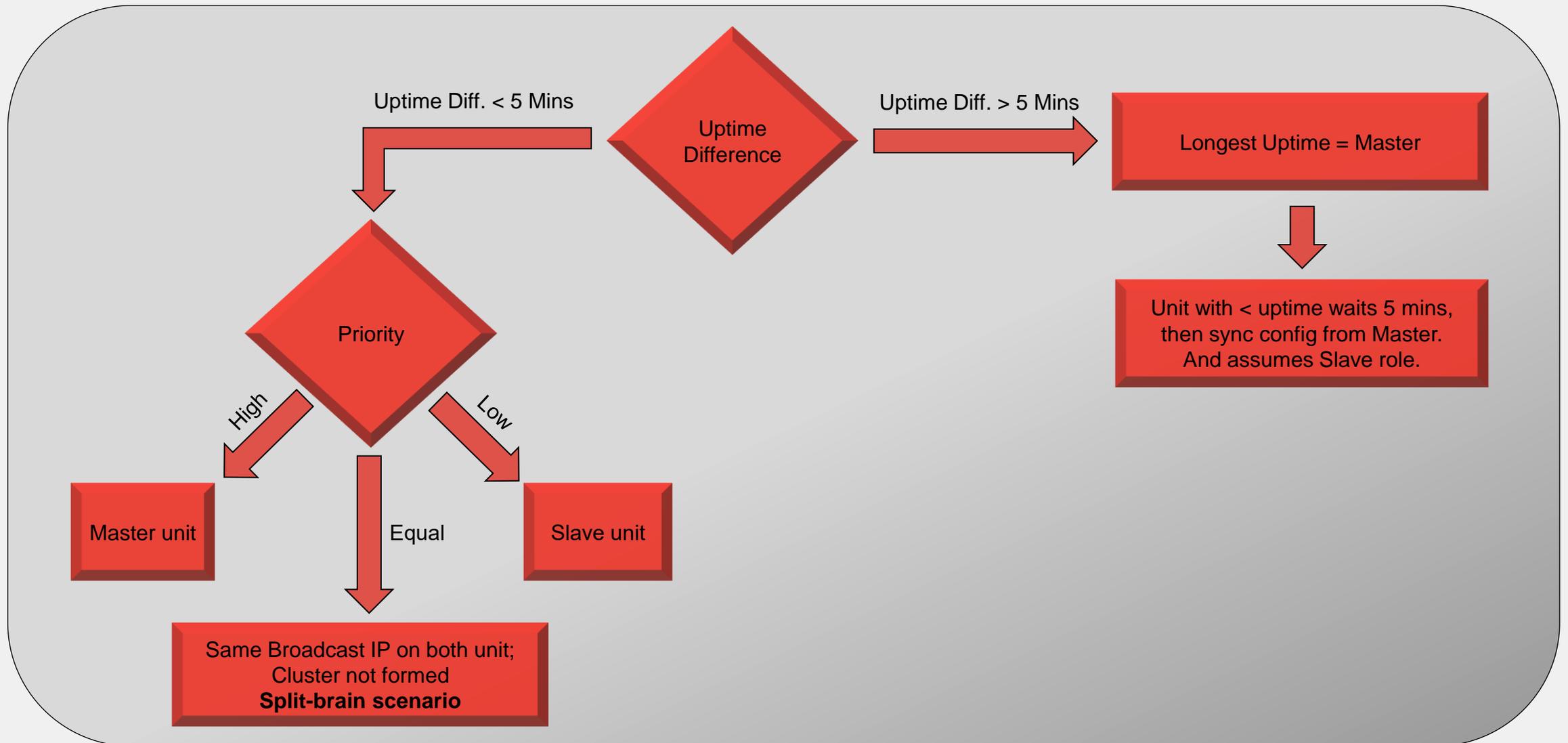


Требования к высокой доступности (HA)

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

The screenshot shows the 'High Availability Settings' configuration page for FortiAuthenticator VM. The left sidebar contains a navigation menu with 'Administration' selected. The main content area includes the following fields and options:

- System:** FortiAuthenticator VM FAC11
- High Availability Settings:**
 - Enable HA
 - Role:**
 - Cluster member
 - Standalone master
 - Load-balancing slave
 - Maintenance Mode:**
 - Disabled
 - Enabled with synchronization
 - Enabled without synchronization
 - Interface:** port2
 - Cluster member IP address:** [Empty text field]
 - Admin access:**
 - Telnet
 - SSH
 - HTTPS
 - GUI (/login)
 - REST API (/api)
 - HTTP (GUI)
 - SNMP
 - FABRIC
 - Priority:** High
 - Password:** [Masked text field]
 - Load-balancing slaves:**

IP address	Delete
[Empty text field]	Delete

[+ Add another](#)
 - Monitored interfaces:**
 - port1
 - port3
 - port4
 - Monitored interfaces stability period:** 30 (0-3600s)
 - Node-Specific Default Gateway:** [Empty text field]

At the bottom, there are 'OK' and 'Cancel' buttons, and a label 'HB thresholds' pointing to the 'Monitored interfaces stability period' field.

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

Оба устройства должны использовать одинаковый HA interface

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

Обычно основным является устройство с более высоким приоритетом.

Пароль должен совпадать

Port status monitor как в FortiOS

HB thresholds



HA проверка состояния

FortiAuthenticator VM FAC6-HA-Slave (Load-balancing slave mode) Logged in as admin

System Dashboard

Refresh Rebuild Tables Reconnect

Node 3 (This Node)

Node type	Load balancing slave
Serial number	FAC-VMTM19001553
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	MAC Devices	MAC Device Group Membership	Enhanced Cryptography Config	Remote SAML Users	SAML Group Membership	Fortitoken Cloud
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Node 1

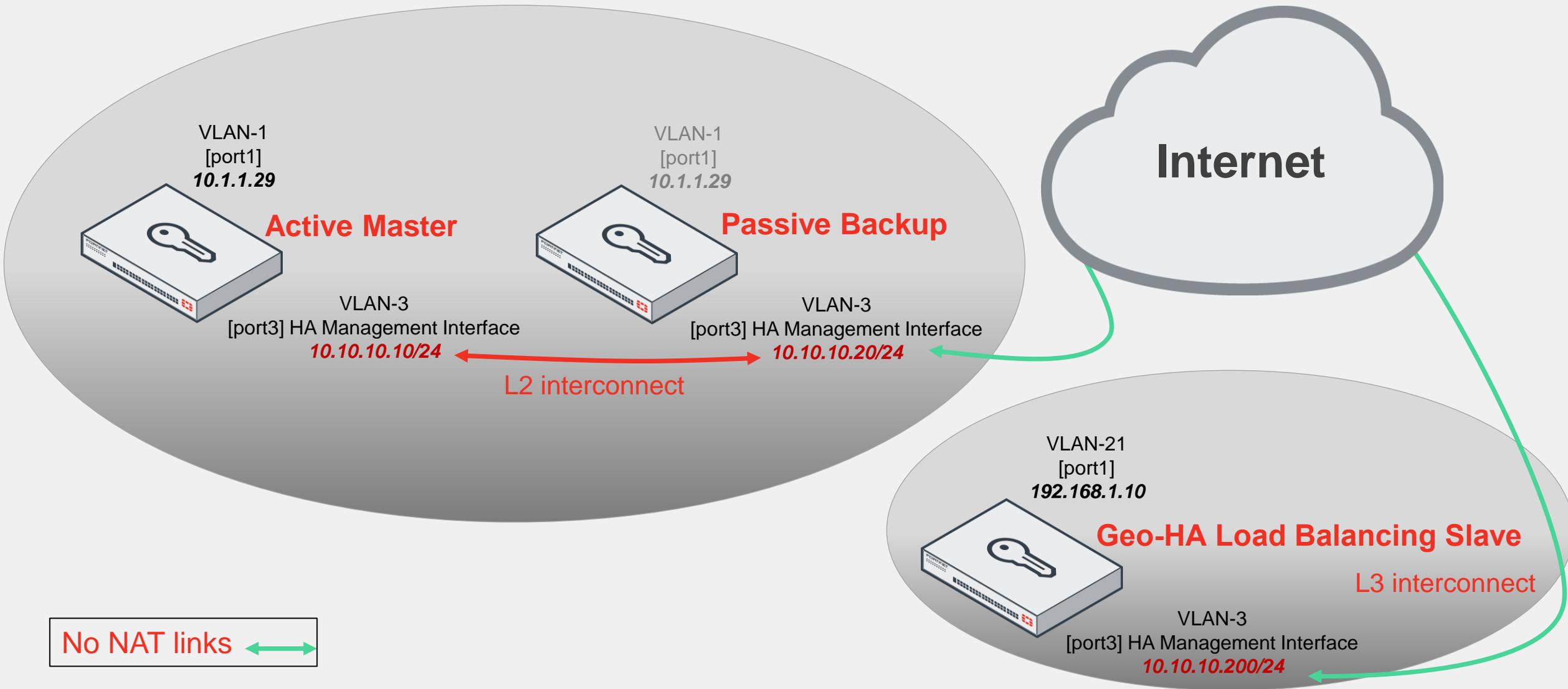
Node type	Cluster member (master)
Priority	High
Serial number	FAC-VMTM18004061
Status	Connected Reachable
External IP	192.0.2.6
Last heartbeat time	2s ago

Посмотреть статус в GUI:

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



Active/Passive plus Geo-HA в удаленных филиалах





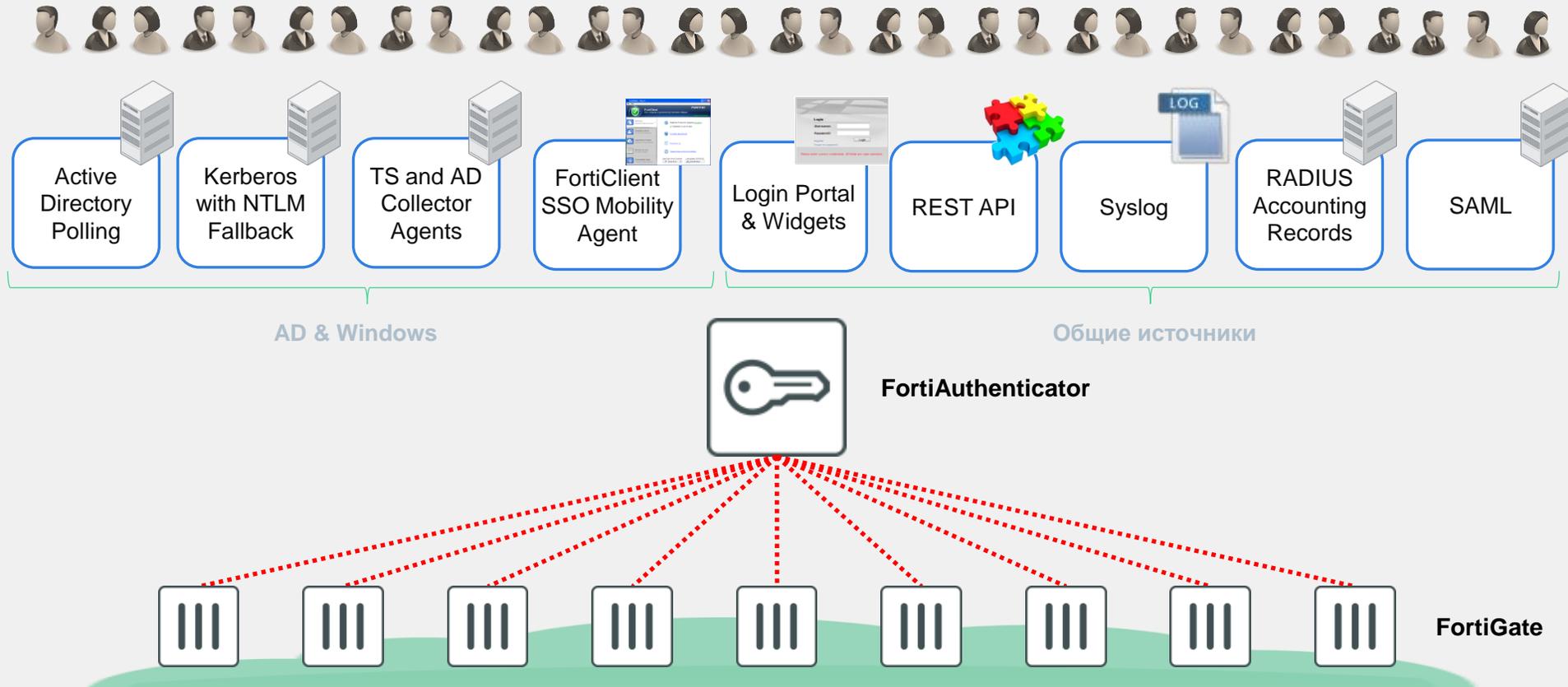
FortiAuthenticator

FSSO



Fortinet Single Sign-On – (FSSO)

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

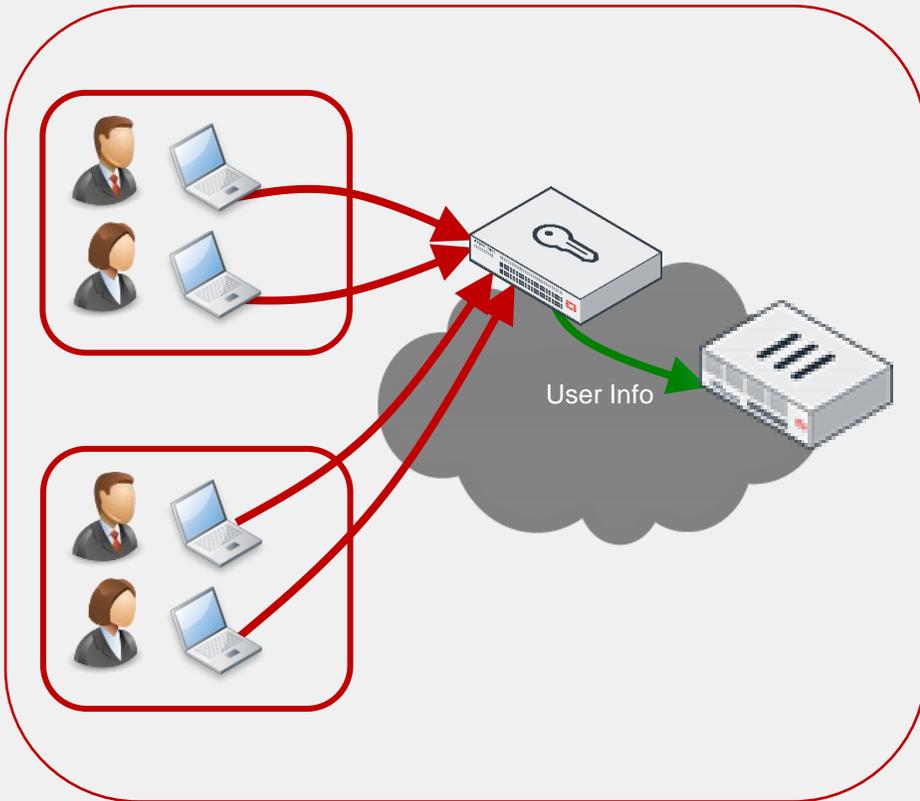


FortiAuthenticator FSSO – SSO Mobility Agent

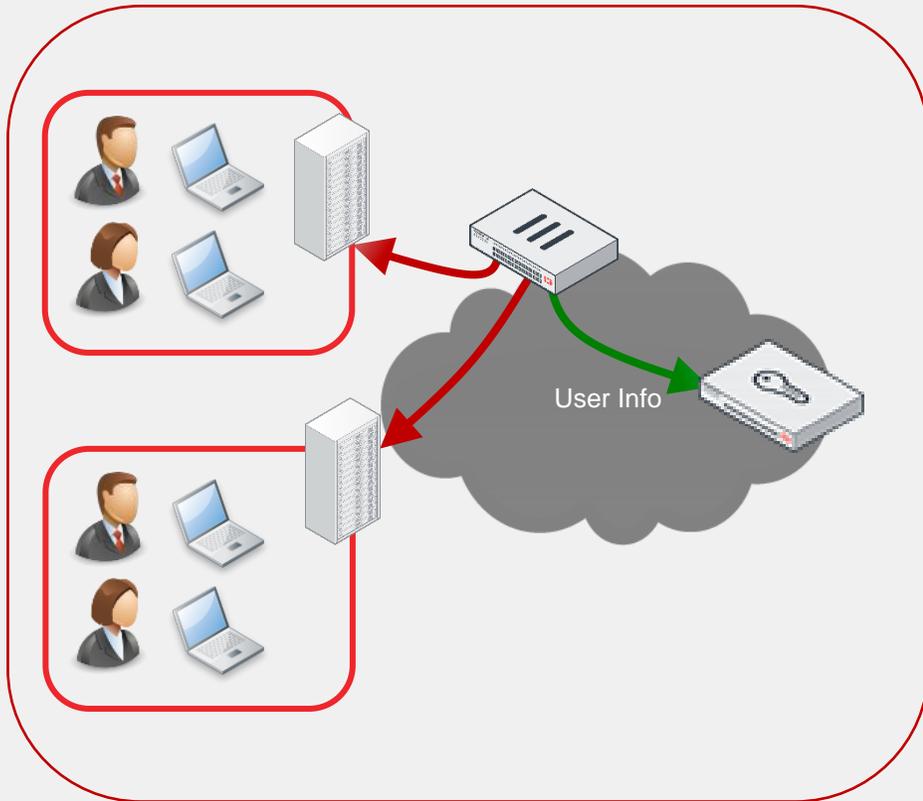
Лучшая масштабируемость и обнаружение выхода из системы

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

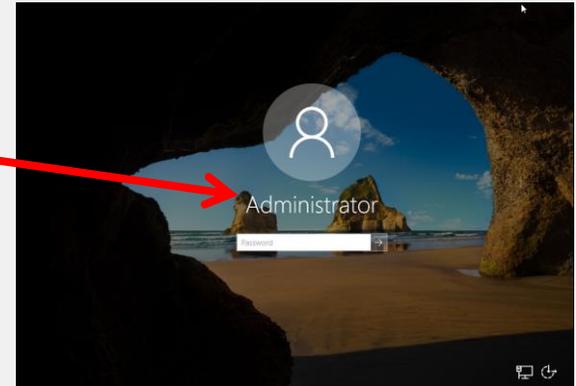


Active Directory Polling

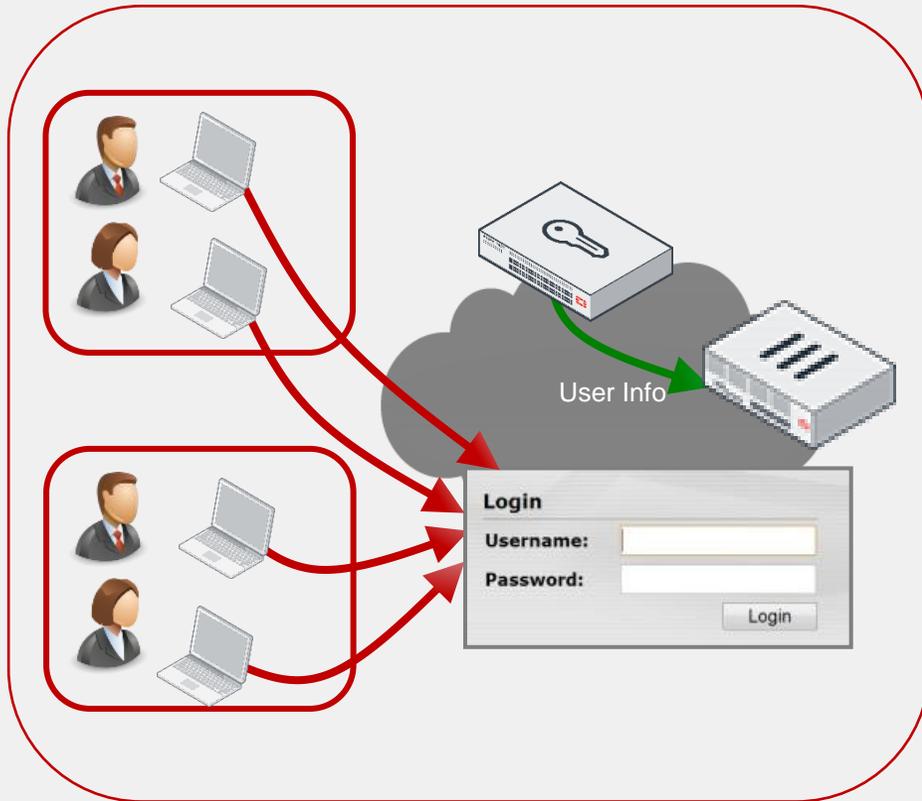
- WinSec (Windows Security Event Logs)
 - 5 second polling
 - Event IDs - 672, 680, 4776 and 4768
 - Дополнительные IDs – 528, 540, 4624 (MacOS)
- WMI (инструментарий управления **Windows**)
 - 5 second polling
 - Требуется открытие портов на Windows FW tcp ports 135&445
- NetApi

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



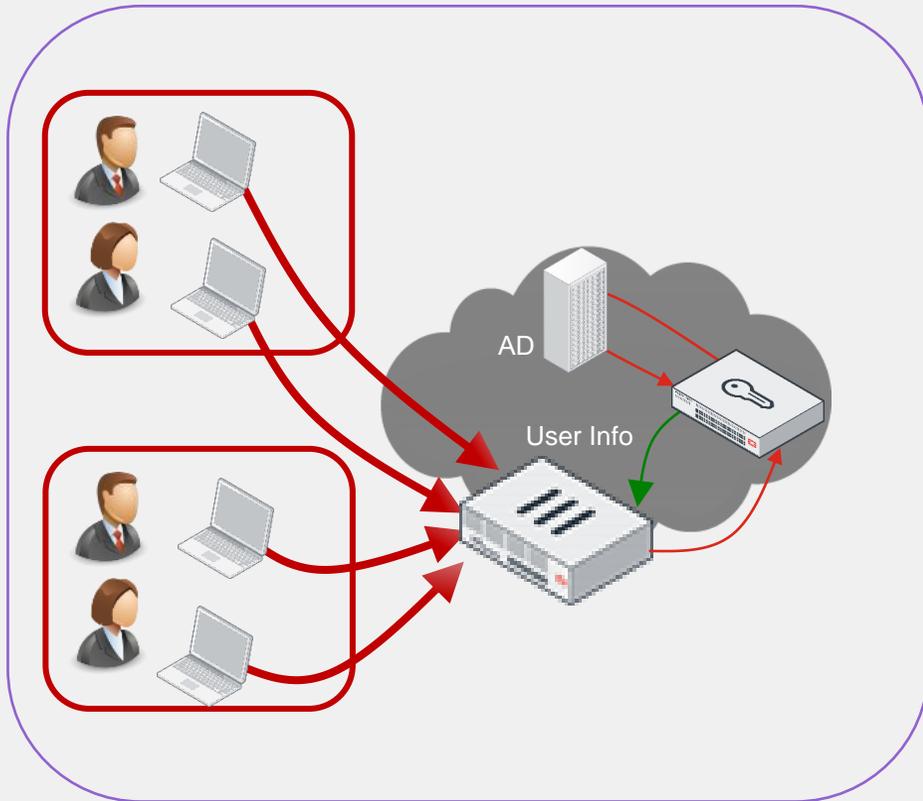
FortiAuthenticator FSSO – Портал и Widget



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

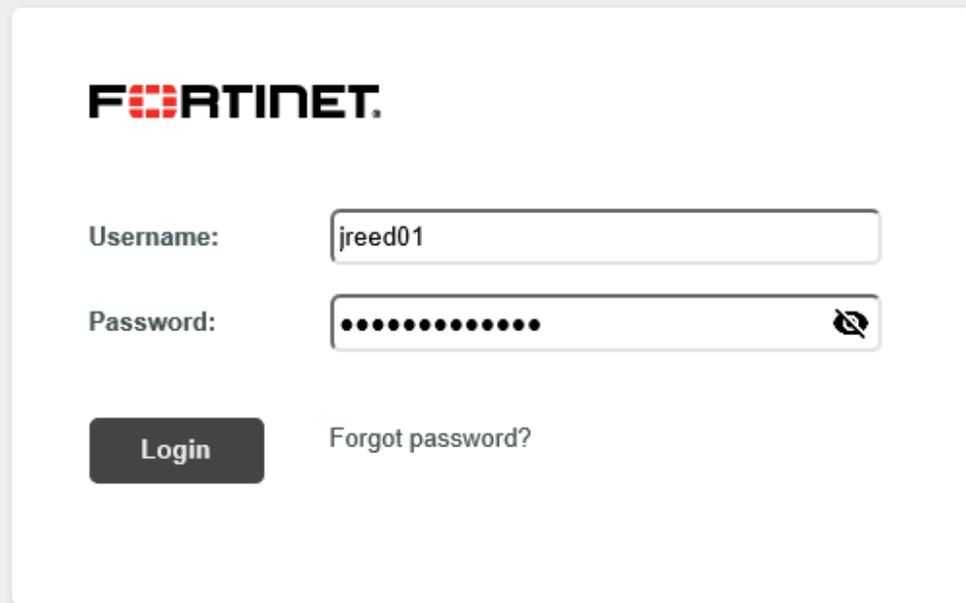


Durable, large display, OATH OTP token with FortiGuard activation or optional encrypted activation file.

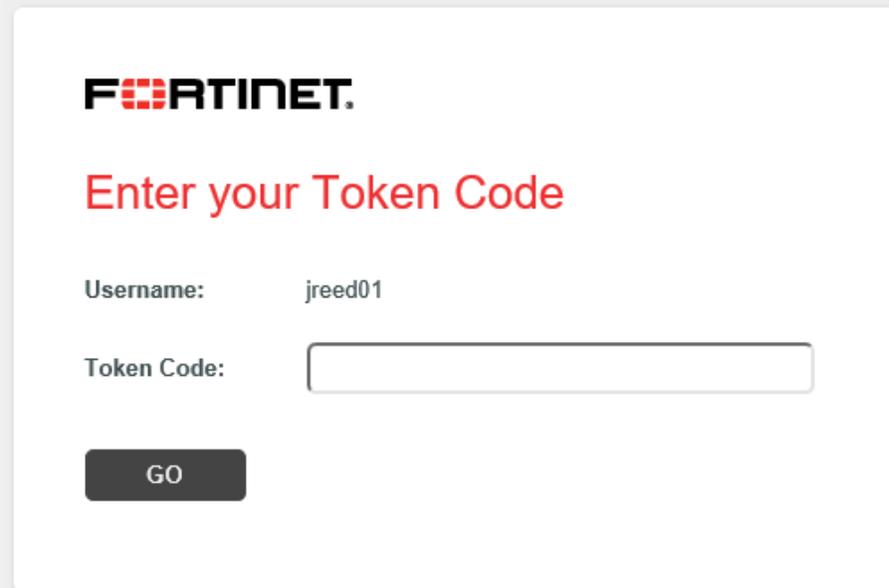


FortiAuthenticator Captive Portal

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



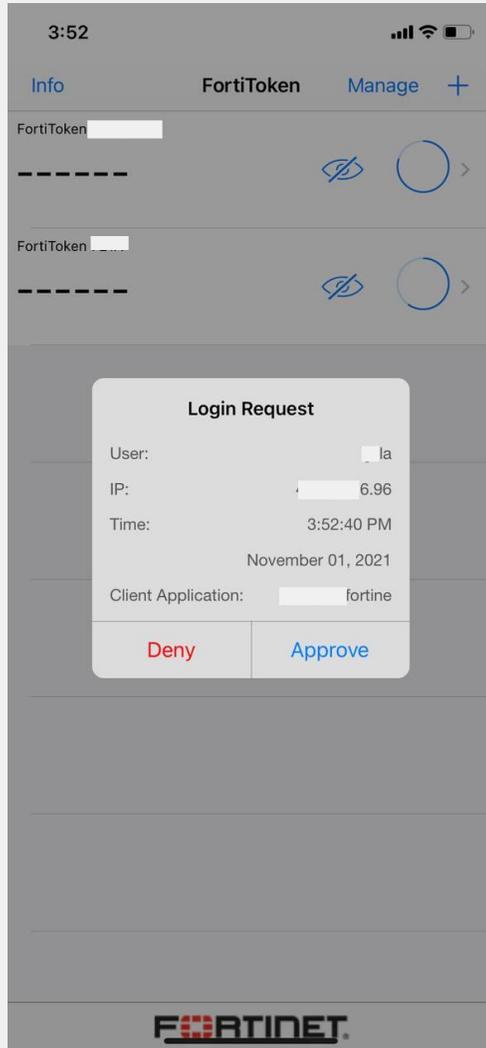
The image shows the first step of the Fortinet Captive Portal login process. It features the Fortinet logo at the top left. Below it, there are two input fields: 'Username:' with the value 'jreed01' and 'Password:' with a masked password of ten dots. To the right of the password field is a small icon of a key. At the bottom left is a dark 'Login' button, and to its right is a link for 'Forgot password?'.



The image shows the second step of the Fortinet Captive Portal login process. It features the Fortinet logo at the top left. Below it, the text 'Enter your Token Code' is displayed in red. There are two input fields: 'Username:' with the value 'jreed01' and 'Token Code:' with an empty field. At the bottom left is a dark 'GO' button.

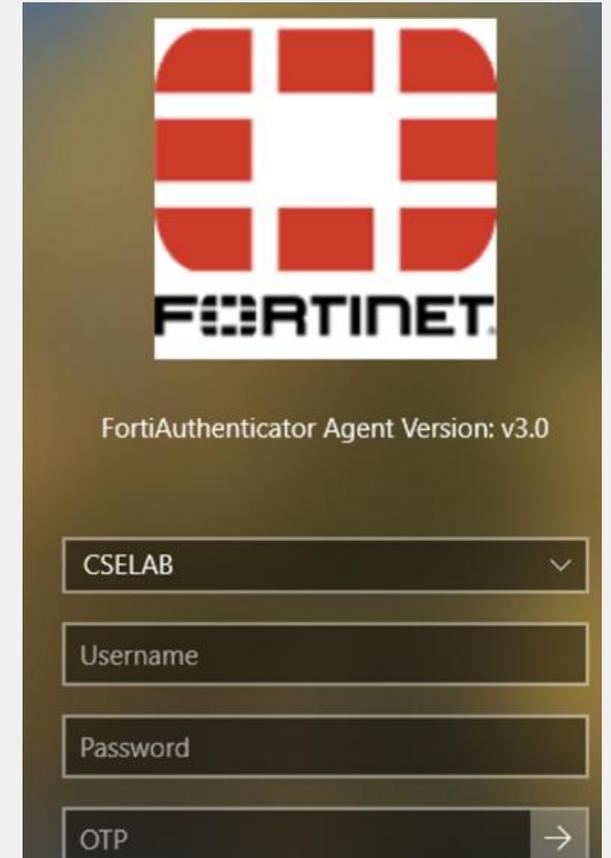
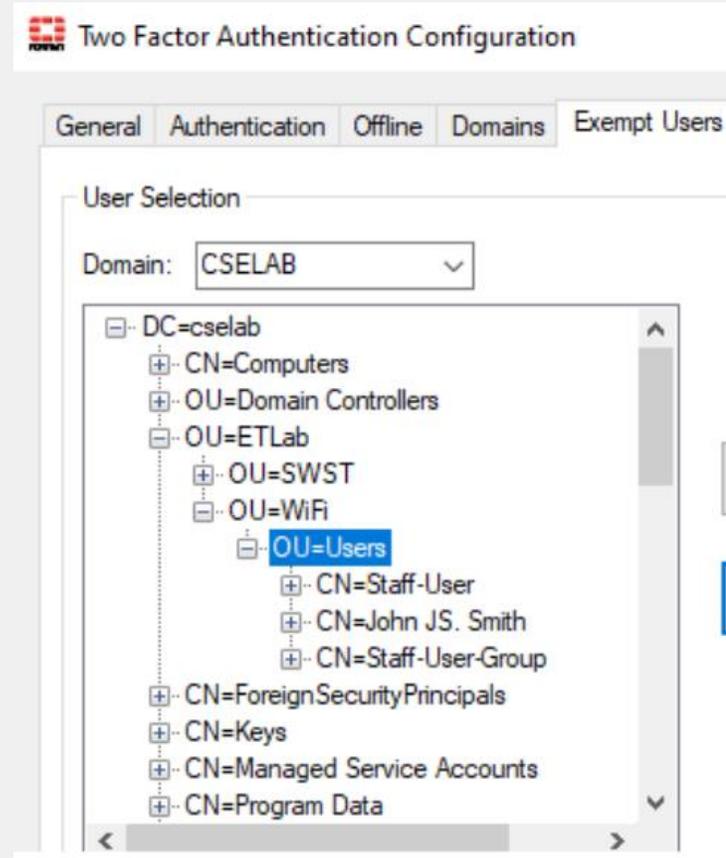
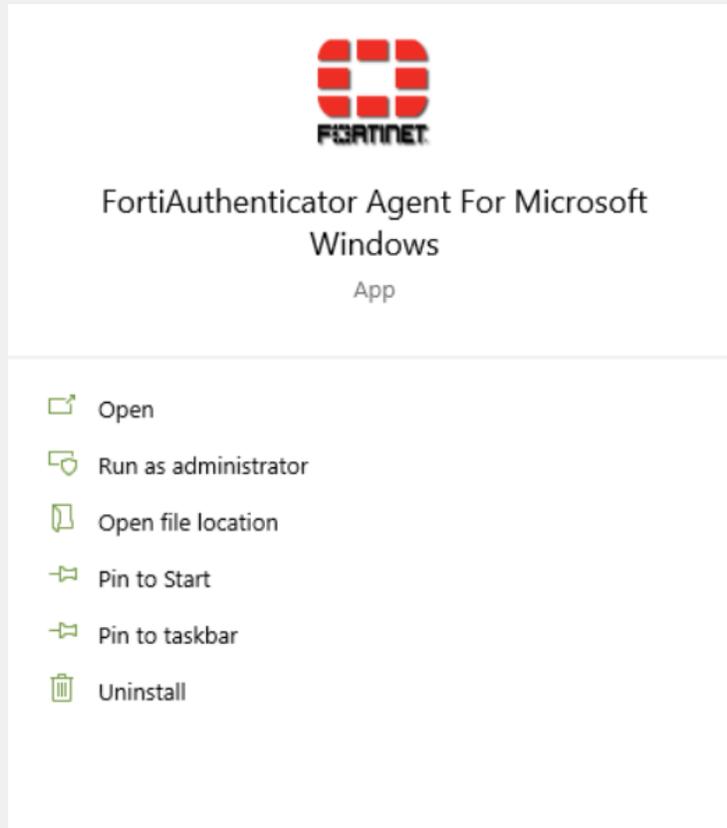


PUSH-уведомления

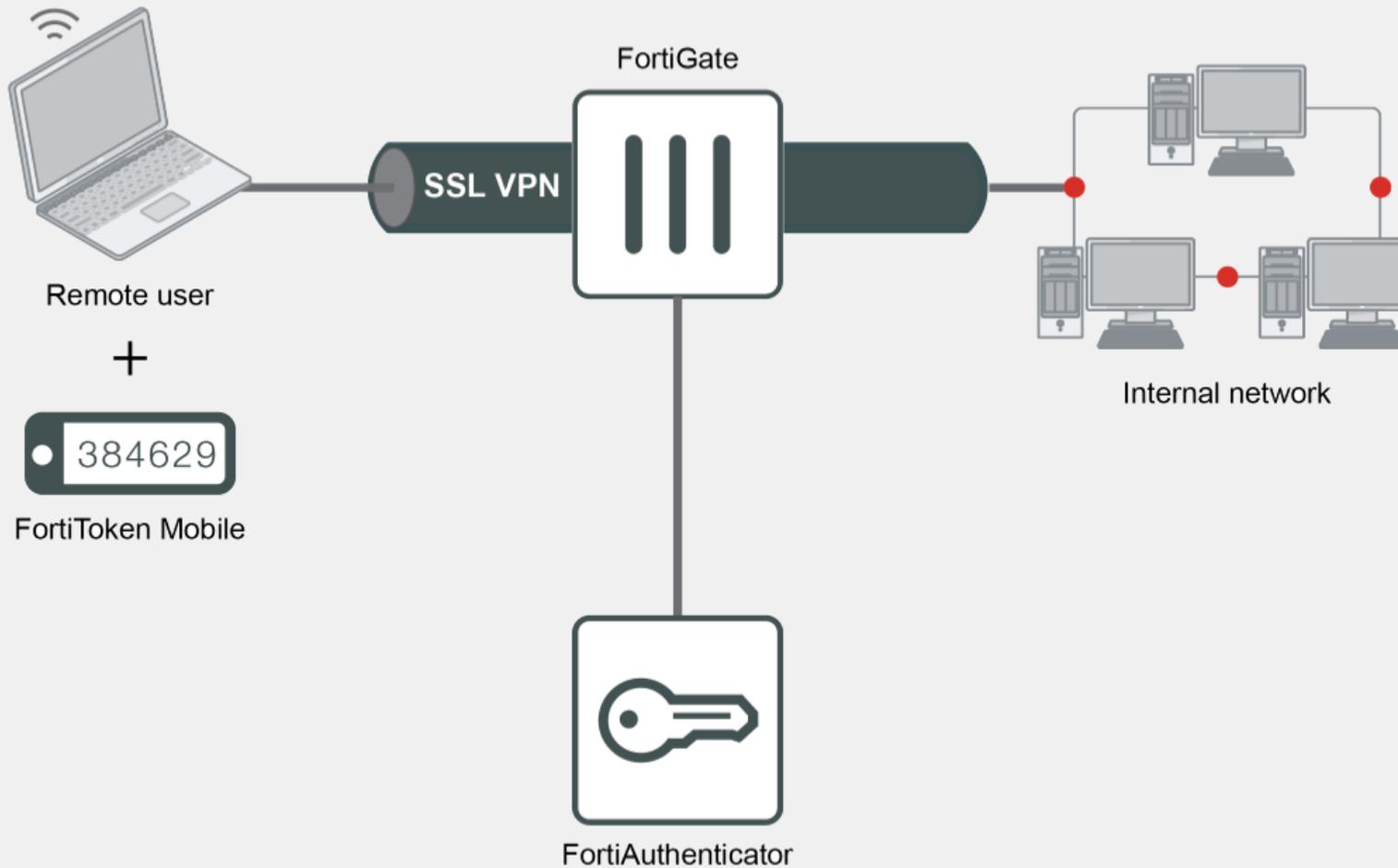


- PUSH-уведомления используются для отправки предупреждений на устройство конечного пользователя каждый раз, когда делается запрос на вход. Предупреждение содержит информацию о попытке входа в систему, например, местоположение, из которого была совершена попытка.
- Используя PUSH, когда требуется аутентификация, 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.

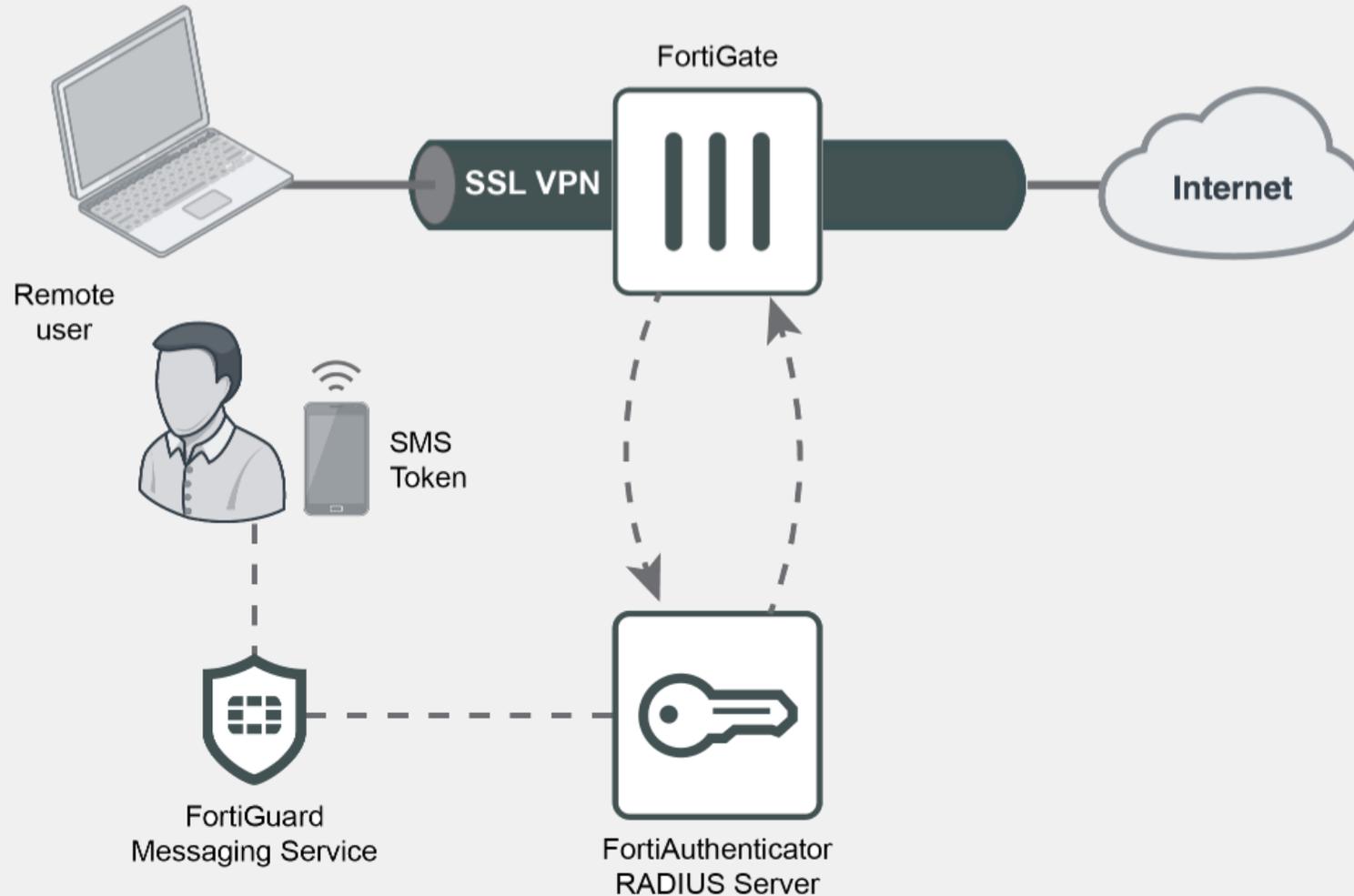
FortiAuthenticator Agent для Microsoft Windows



Пример. SSL VPN + 2FA (FortiToken)



Пример. SSL VPN + 2FA (SMS)





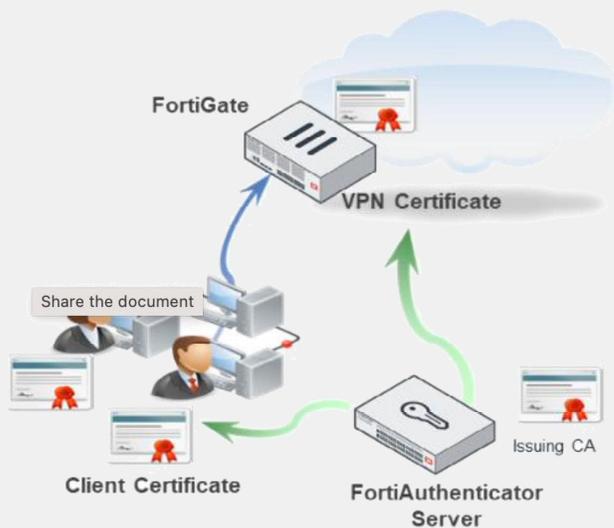
FortiAuthenticator

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



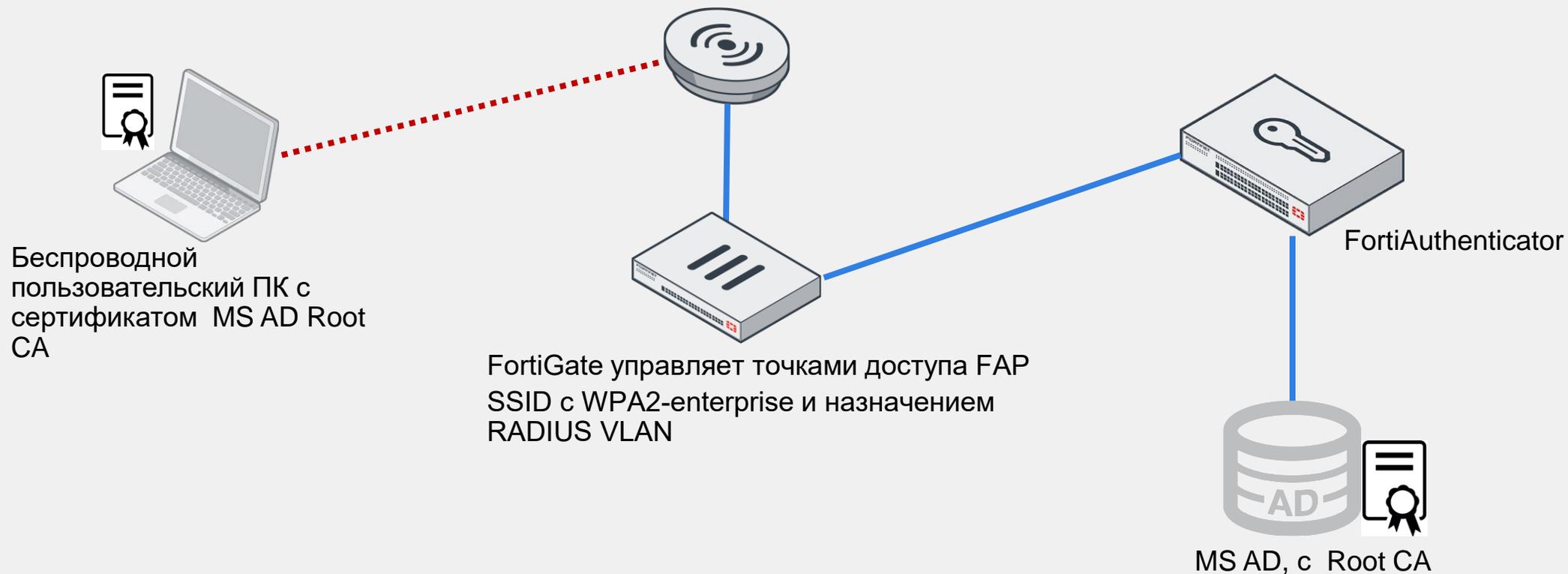


FortiAuthenticator

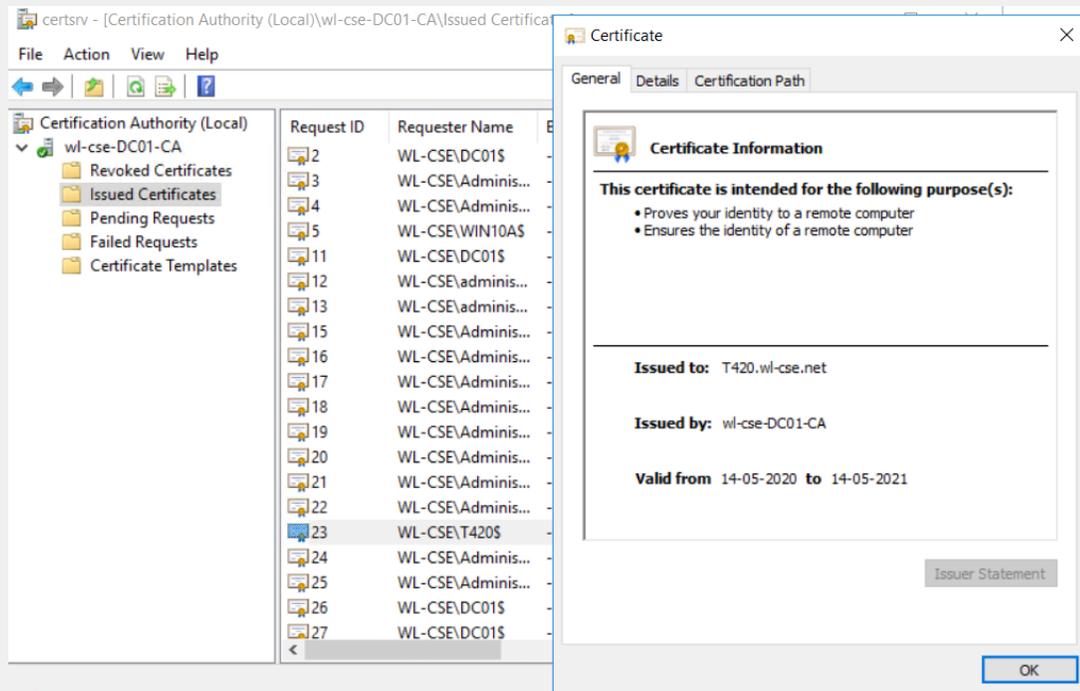
ПРИМЕР – 802.1x Аутентификация



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

The screenshot displays the Group Policy Management console with the following components:

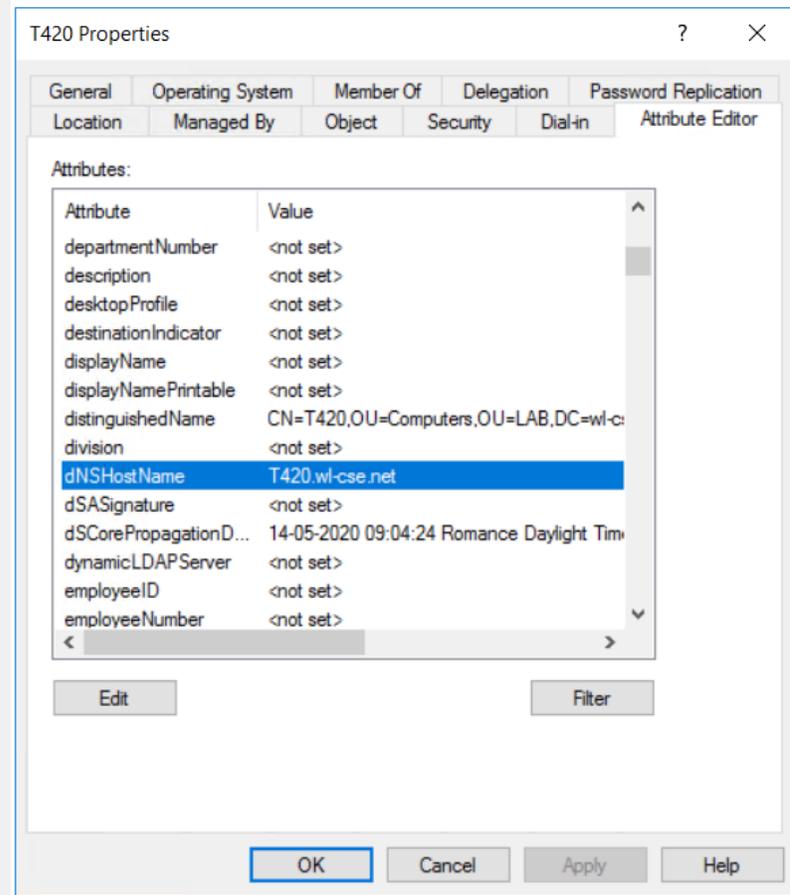
- Left Pane (Group Policy Objects):** Shows a hierarchy for 'Forest: wl-cse.net' > 'Domains' > 'LAB' > 'Group Policy Objects'. The 'Certificate-Enrollment' GPO is selected and highlighted with a red box.
- Right Pane (Certificate-Enrollment):** Shows the 'Certificate-Enrollment' GPO details, including 'Scope', 'Details', 'Settings', 'Delegation', and 'Status' tabs. The 'Settings' tab is active, showing 'These groups and users have the specified permission for this GPO'.
- Group Policy Management Editor:** Shows the configuration path: 'Computer Configuration' > 'Policies' > 'Security Settings' > 'Public Key Policies'. The 'Certificate Services Client - Certificate Enrollment Policy' is selected and highlighted with a red box.
- Object Type List:** Shows a list of object types, including 'Certificate Services Client - Certificate Enrollment Policy', which is highlighted with a red box.
- Configuration Dialog:** A dialog box titled 'Certificate Services Client - Certificate Enrollment Policy' is open. It shows the 'Enrollment Policy' configuration with the 'Configuration Model' set to 'Enabled'. The 'Certificate enrollment policy list' table is visible:

Default	Name	Automatic Enrollment
<input checked="" type="checkbox"/>	Active Directory Enrollmen...	Enabled

Additional configuration options include 'Add...', 'Remove...', 'Properties', and 'Disable user configured enrollment policy servers' (unchecked). The dialog has 'OK', 'Cancel', and 'Apply' buttons at the bottom.



ПРИМЕР 802.1x – MS AD настройка



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

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

ПРИМЕР 802.1x – Root CA импорт FGT и FAC

System – Certificates – Remote CA Certificate

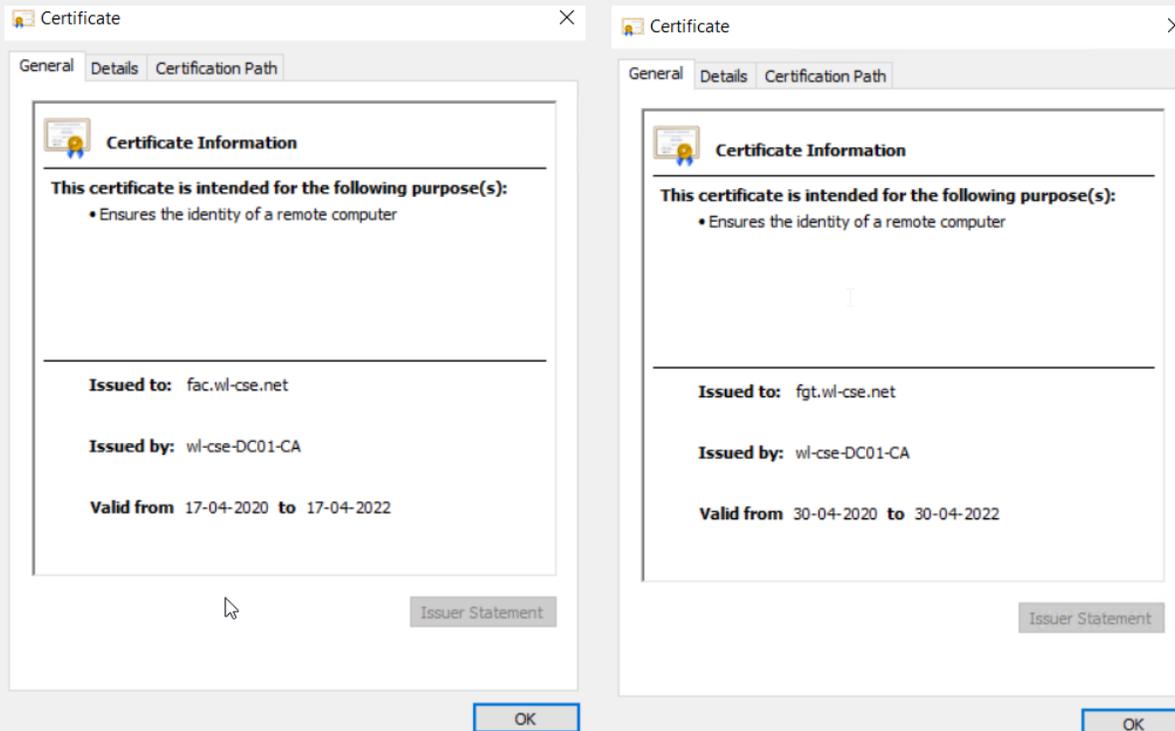
Name	Subject
Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...
Fortinet_SSL_DSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...
Fortinet_SSL_DSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...
Fortinet_SSL_ECDSA256	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...
Fortinet_SSL_ECDSA384	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...
Fortinet_SSL_ECDSA521	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...
Fortinet_SSL_ED448	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...
Fortinet_SSL_ED25519	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...
Fortinet_SSL_RSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...
Fortinet_SSL_RSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...
Fortinet_SSL_RSA4096	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...
Fortinet_Wifi	C = US, ST = California, L = Sunnyvale, O = "Fortinet, In...
fgt-cert	C = DK, ST = Zealand, O = wl-cse, OU = wl-cse, CN = fg...
Remote CA Certificate	
CA_Cert_1	DC = net, DC = wl-cse, CN = wl-cse-DC01-CA
Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...

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

Certificate Management – Certificate Authorities – Trusted CAs

Certificate ID	Subject
Fortinet_CA1_Root	C=US, ST=California, L=Sunnyvale, O=Fortinet, ...
Fortinet_CA2_Intermediate	C=US, ST=California, L=Sunnyvale, O=Fortinet, ...
Fortinet_CA2_Root	C=US, ST=California, L=Sunnyvale, O=Fortinet, ...
MS_AD	DC=net, DC=wl-cse, CN=wl-cse-DC01-CA

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

The screenshot shows the 'Edit LDAP Server' configuration page in the Fortinet management console. The left sidebar contains a navigation menu with 'Remote Auth. Servers' selected. The main content area is divided into several sections:

- General:** Name: AD_Computers; Primary server name/IP: dc01.wl-cse.net; Port: 636; Use secondary server: ; Base distinguished name: DC=wl-cse,DC=net; Bind type: Regular; Username: wl-cse\servicelogin; Password: [masked]; Server type: Microsoft Active Directory; Add supported domain names: .
- Query Elements:** User object class: computer; Username attribute: dNSHostName; Group object class: group; Obtain group memberships from: Group attribute; Group membership attribute: memberOf; Force use of administrator account for group membership lookups: .
- Secure Connection:** Enable: ; Protocol: LDAPS; CA certificate: MS_AD | DC=net, DC=wl-cse, CN=wl-cse-DC01-CA; Use Client Certificate for TLS Authentication: .

Создаем запись LDAP для remote lookup компьютеров, с атрибутом 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

FortiAuthenticator VM FAC

System > Edit Realm

Authentication >

User Account Policies >

User Management >

Local Users

Remote Users

Remote User Sync Rules

Social Login Users

Guest Users

User Groups

Usage Profile

Organizations

Realms

Name: host

User source: AD_Computers (dc01.wl-cse.net)

Chained token authentication with remote RADIUS server

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))`

The screenshot shows the configuration interface for a Remote LDAP User Synchronization Rule in FortiAuthenticator VM FAC. The left sidebar shows the navigation menu with 'User Management' > 'Remote User Sync Rules' selected. The main configuration area includes:

- Name:** AD-computers
- Remote LDAP:** AD_Computers (dc01.wl-cse.net)
- Base distinguished name:** DC=wl-cse,DC=net
- LDAP filter:** (&(objectClass=computer)(memberof=CN=LAB-Computers,OU=Computers,OU=LAB,DC=wl-cse,DC=ne) [Test Filter]
- Synchronization Attributes:**
 - Token-based authentication sync priorities:
 - None (users are synced explicitly with no token-based authentication)
 - FortiToken Hardware (assign if serial number is provided)
 - FortiToken Hardware (assign an available token)
 - FortiToken Mobile (assign an available token)
 - FortiToken Cloud
 - Email
 - SMS
 - Dual (Email and SMS)
- Sync every:** 1 hour(s)
- Sync as:** Remote LDAP User (selected), Local User

ПРИМЕР 802.1x – Remote LDAP sync правила

Group to associate users with:   

Organization:  

Certificate binding CA:

Do not delete synced users when they are no longer found on the remote server

Proceed with rule even when response empty.

LDAP User Mapping Attributes

Username:	<input type="text" value="dNSHostName"/>
First name:	<input type="text" value="givenName"/>
Last name:	<input type="text" value="sn"/>
Email:	<input type="text" value="mail"/>
Phone number:	<input type="text" value="telephoneNumber"/>
Mobile number:	<input type="text"/>
FTK-200 serial number:	<input type="text"/>
Certificate binding common name:	<input type="text" value="dNSHostName"/>

Создаем ассоциацию с группой (используется для RADIUS атрибутов).

Создаем связь с сертификатом.

Для LDAP username мы используем dNSHostName, и его же для привязки сертификата. Должно совпадать с CN выпущенного сертификата.



ПРИМЕР 802.1x – Проверка записи компьютера

Authentication – User Management – Remote Users

The screenshot shows the FortiAuthenticator VM FAC interface. The left sidebar contains a navigation menu with categories like System, Authentication, User Management, Local Users, Remote Users, Social Login Users, Guest Users, User Groups, Usage Profile, Organizations, Realms, FortiTokens, MAC Devices, Self-service Portal, Portals, Remote Auth. Servers, RADIUS Service, and TACACS+ Service. The 'Remote Users' section is expanded, showing configuration options for a Remote LDAP server. The 'Certificate Bindings' section is also expanded, showing a table of bindings.

Common Name	Issuer
T420.wl-cse.net	DC=net, DC=wl-cse, CN=wl-cse-DC01-CA

Проверяем "user" запись для компьютера созданную правилами синхронизации.

Проверяем привязку сертификатов.

ПРИМЕР 802.1x – групповые атрибуты

Authentication – User Management – User Groups

FortiAuthenticator VM FAC

System > Authentication > User Management > User Groups > Edit User Group

Name: AD_LAB_PC

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: AD_Computers (dc01.wl-cse.net)

LDAP users:

Available LDAP Users: [Filter]

Selected LDAP Users:

- t420.wl-cse.net @ AD_Computers (dc01.wl-cse.net)
- win10a.wl-cse.net @ AD_Computers (dc01.wl-cse.net)
- win10a.wl-cse.net @ AD_Computers (dc01.wl-cse.net)

Choose all Remove all

Usage Profile: [Please Select]

TACACS+ Authorization

TACACS+ authorization rule: [Please Select]

RADIUS Attributes

Attribute	Value
Tunnel-Type	VLAN (13)
Tunnel-Medium-Type	IEEE-802 (6)
Tunnel-Private-Group-Id	240
Fortinet-Group-Name	FTNT_LAB_Computers

Add Attribute

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

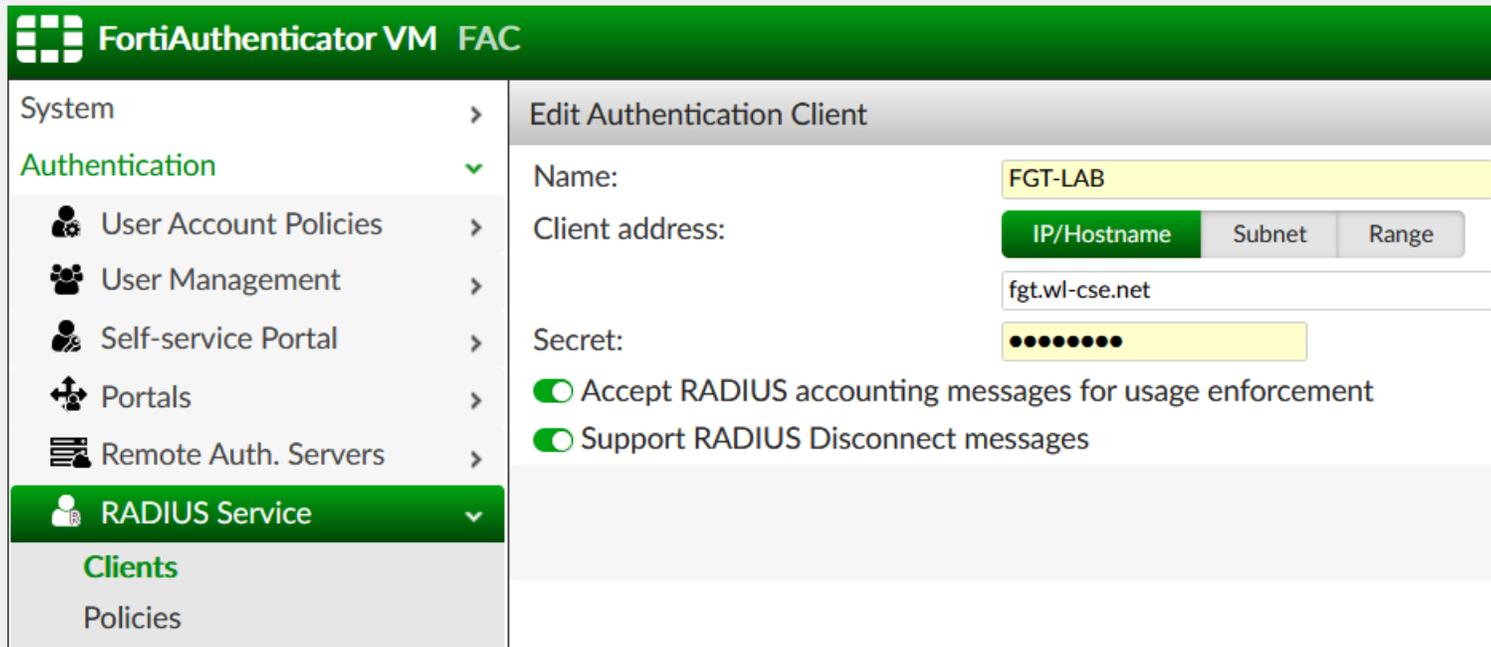
The screenshot shows the configuration page for RADIUS Service Certificates in FortiAuthenticator VM. The left sidebar contains a navigation menu with the following items: System, Authentication, User Account Policies, User Management, Self-service Portal, Portals, Remote Auth. Servers, RADIUS Service (highlighted), Clients, Policies, Certificates (highlighted), Services, and Dictionaries. The main content area is titled 'RADIUS-EAP Configuration' and includes the following sections:

- Server Settings**
 - EAP Server Certificate:
 - RADSEC Server Certificate:
- EAP-TLS Authentication**
 - Local CAs:
 - Trusted CAs:

An 'OK' button is located at the bottom right of the configuration area.

ПРИМЕР 802.1x – RADIUS клиенты

Authentication – RADIUS Service – Clients



The screenshot displays the FortiAuthenticator VM FAC web interface. The left sidebar shows the navigation menu with 'RADIUS Service' expanded to 'Clients'. The main content area is titled 'Edit Authentication Client' and contains the following configuration fields:

- Name:** FGT-LAB
- Client address:** fgt.wl-cse.net (Selected: IP/Hostname)
- Secret:** [Redacted]
- Accept RADIUS accounting messages for usage enforcement
- Support RADIUS Disconnect messages

Добавляем FortiGate в качестве RADIUS клиента на FortiAuthenticator.

ПРИМЕР 802.1x – RADIUS Policy #1

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

Authentication – RADIUS Service – Policies

The screenshot shows the Fortinet FortiNAC configuration interface for creating a RADIUS Policy. The left sidebar contains a navigation menu with the following items: System, Authentication, User Account Policies, User Management, Self-service Portal, Portals, Remote Auth. Servers, RADIUS Service (highlighted), Clients, and Policies. The main content area is titled 'RADIUS Policy' and features a breadcrumb trail: RADIUS clients > RADIUS attribute criteria > Authentication type > Identity source. The configuration form includes: Policy name: FGT-Computer-TLS; Description: (empty text area); RADIUS clients: Available RADIUS Clients (with a filter box) and Chosen RADIUS Clients (containing FGT-LAB (fgt.wl-cse.net)). The available clients list includes FortiNAC (fnac.wl-cse.net), WLC42 (192.168.200.42), and WLC45 (192.168.200.45).



ПРИМЕР 802.1x – RADIUS Policy #2

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

The screenshot shows a configuration page for RADIUS attribute criteria. At the top, there are three tabs: 'RADIUS clients', 'RADIUS attribute criteria', and 'Authen'. The 'RADIUS attribute criteria' tab is active. Below the tabs, there is a toggle switch labeled 'RADIUS authentication request must contain specific attributes' which is turned on. Underneath, a section titled 'Matching RADIUS Attribute: Fortinet-SSID (FGT-FAC-8021X)' contains the following fields: 'Vendor' (dropdown menu with 'Fortinet' selected), 'Attribute ID' (dropdown menu with 'Fortinet-SSID' selected), 'Value' (text input field with 'FGT-FAC-8021X' entered), 'Allow substring match' (radio button, currently unselected), 'ASCII value' (checkbox, currently unchecked), and 'Type' (dropdown menu with 'String' selected).

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

The screenshot shows the Fortinet web interface. On the left is a navigation menu with 'System' and 'Authentication' expanded. Under 'Authentication', 'RADIUS Service' is selected, with sub-items 'Clients' and 'Policies'. The main content area shows a breadcrumb trail: 'RADIUS clients' > 'RADIUS attribute criteria' > 'Authentication type' > 'Identity sou'. Below the breadcrumb, there is a toggle switch for 'RADIUS authentication request must contain specific attributes' which is turned on. At the bottom of the page, there are three buttons: 'Previous', 'Discard and exit', and 'Update and exit'.

ПРИМЕР 802.1x – RADIUS Policy #3

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

Выбираем клиентский сертификат (EAP-TLS)

The screenshot shows the Fortinet FortiGate configuration interface for a RADIUS Policy. On the left is a navigation menu with the following items: System, Authentication, User Account Policies, User Management, Self-service Portal, Portals, Remote Auth. Servers, RADIUS Service (highlighted), Clients, Policies, Certificates, and Services. The main content area shows a breadcrumb trail: RADIUS clients > RADIUS attribute criteria > Authentication type > Identity source. Below the breadcrumb, the 'Authentication type' section has three radio button options: Password/OTP authentication, MAC authentication bypass (MAB), and Client Certificates (EAP-TLS), which is selected. At the bottom of the configuration area are three buttons: Previous, Discard and exit, and Update and exit.

ПРИМЕР 802.1x – RADIUS Policy #4

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

Выбираем username формат, и используем наш realm (host)

System >

Authentication >

- User Account Policies >
- User Management >
- Self-service Portal >
- Portals >
- Remote Auth. Servers >
- RADIUS Service** >

 - Clients
 - Policies**
 - Certificates
 - Services
 - Dictionaries

- TACACS+ Service >
- LDAP Service >

RADIUS clients > RADIUS attribute criteria > Authentication type > Identity source > Authentication factors > R

? Understanding the Client Certificates (EAP-TLS) workflow

Username format:

- username@realm
- realm\username
- realm/username

Use default realm when user-provided realm is different from all configured realms

Realms:

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
<input checked="" type="radio"/>	host AD_Computers (dc01.wl-cse.net)	<input type="checkbox"/>	<input checked="" type="checkbox"/> Filter: AD_LAB_PC <input type="checkbox"/> Filter local users:	

[+ Add a realm](#)

Previous Discard and exit **Update and exit** Next

ПРИМЕР 802.1x – RADIUS Policy #5

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

На данной вкладке оставляем все как есть. Все применяем.

System >

Authentication ✓

- User Account Policies >
- User Management >
- Self-service Portal >
- Portals >
- Remote Auth. Servers >
- RADIUS Service** v
- Clients
- Policies
- Certificates
- Services

RADIUS clients > RADIUS attribute criteria > Authentication type > Identity source > Authentication factors

Device authorization

- Verify MAC address in authentication requests
- RADIUS attribute:
- Authorized groups:

Advanced options

- Reject usernames containing uppercase letters

Previous Discard and exit Update and exit Next



ПРИМЕР 802.1x – FortiGate: RADIUS

User & Authentication – RADIUS Servers

The screenshot shows the FortiGate 61E web interface. The left sidebar is expanded to 'User & Authentication' > 'RADIUS Servers'. The main content area is titled 'Edit RADIUS Server'. The configuration is as follows:

- Name:** FAC
- Authentication method:** Default (selected), Specify
- NAS IP:** (empty field)
- Include in every user group:**
- Primary Server:**
 - IP/Name:** 192.168.200.9
 - Secret:** (masked with dots)
 - Connection status:** Successful
 - Test Connectivity:** (button)
 - Test User Credentials:** (button)
- Secondary Server:**
 - IP/Name:** (empty field)
 - Secret:** (empty field)
 - Test Connectivity:** (button)
 - Test User Credentials:** (button)

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.

Name  FGT-FNAC-8021X (FGT-FNAC-8021X)

Alias

Type  WiFi SSID

Traffic mode   Tunnel

Address

IP/Netmask

Create address object matching subnet

Secondary IP address

Administrative access

IPv4	<input type="checkbox"/> HTTPS	<input type="checkbox"/> HTTP 	<input type="checkbox"/> PING
	<input type="checkbox"/> FMG-Access	<input type="checkbox"/> SSH	<input type="checkbox"/> SNMP
	<input type="checkbox"/> FTM	<input checked="" type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> Security Fabric Connection 

DHCP Server

Network

Device detection 

WiFi Settings

SSID

Client limit

Broadcast SSID

Security Mode Settings

Security mode

Authentication

Client MAC Address Filtering

RADIUS server

Additional Settings

Dynamic VLAN assignment

Schedule 



ПРИМЕР 802.1x – FortiGate: Интерфейсы

Network – Interfaces

Создаем необходимые интерфейсы.

В нашем примере это DomainComputers VLAN

Interface	DomainComputers
Link	↑
Port Speed	Auto-Negotiation
Type	VLAN
Role	LAN
IPv4 Addresses	10.10.240.1/24
VLAN ID	240
Base Interface	FGT-FAC-8021X (FGT-FAC-8021X)

	Name	Type	Members	IP/Netmask
+	FGT-Connect-CP (FGT-Connect-CP)	WiFi SSID		192.168.163.1/255.255.255.0
-	FGT-FAC-8021X (FGT-FAC-8021X)	WiFi SSID		0.0.0.0/0.0.0.0
•	8021X-Staff242	VLAN		10.10.242.1/255.255.255.0
•	DomainComputers	VLAN		10.10.240.1/255.255.255.0
•	FAC8021-Student	VLAN		10.10.241.1/255.255.255.0



ПРИМЕР 802.1x – FortiAuthenticator: Logs

ID	Timestamp	Level	Category	Sub Category	Log Type ID	Action	Status	Source IP
480...	Thu Sep 24 14:15...	informati...	Event	Authentication	20420	Authentica...	Success	192.168.200.1
480...	Thu Sep 24 14:15...	informati...	Event	System	30350			
480...	Thu Sep 24 14:14...	informati...	Event	Authentication	20994	Login	Success	192.168.190.108
480...	Thu Sep 24 14:14...	informati...	Event	Authentication	20994	Login	Success	
480...	Thu Sep 24 14:14...	informati...	Event	System	30350			
480...	Thu Sep 24 14:13...	informati...	Event	System	30350			
480...	Thu Sep 24 14:12...	informati...	Event	System	30350			
480...	Thu Sep 24 14:11...	informati...	Event	System	30350			
480...	Thu Sep 24 14:10...	informati...	Event	System	30350			
480...	Thu Sep 24 14:09...	informati...	Event	System	30350			
480...	Thu Sep 24 14:08...	informati...	Event	System	30350			
480...	Thu Sep 24 14:07...	informati...	Event	System	30350			

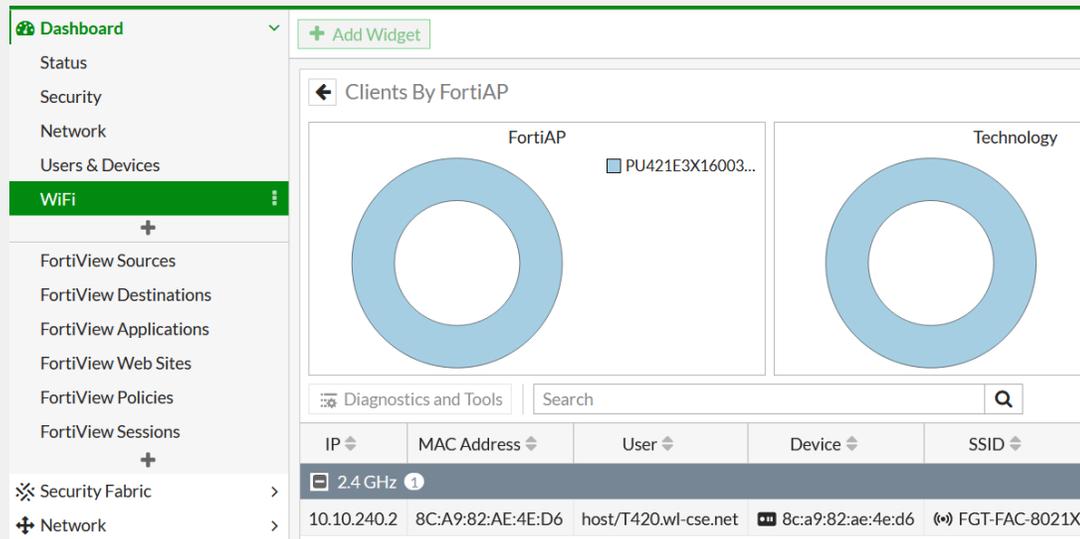
Подключаем нашего клиента и получаем сообщение Authentication Success в логах FortiAuthenticator

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

```
https://fac.wl-cse.net/debug/radius/?offset=0&limit=500
Service: RADIUS Authentication Max. log files size: 1 MB Enter debug mode
2020-09-24T14:17:35.572936+02:00 FAC radiusd[1571]: (262) # Executing group from file /usr/etc/raddb/sites-enabled/default
2020-09-24T14:17:35.572946+02:00 FAC radiusd[1571]: (262) eap: Expiring EAP session with state 0x79449ede7d0c9386
2020-09-24T14:17:35.572951+02:00 FAC radiusd[1571]: (262) eap: Finished EAP session with state 0x79449ede7d0c9386
2020-09-24T14:17:35.572956+02:00 FAC radiusd[1571]: (262) eap: Previous EAP request found for state 0x79449ede7d0c9386, released from the list
2020-09-24T14:17:35.574169+02:00 FAC radiusd[1571]: rlm_eap_tls: Certificate passed CRL check.
2020-09-24T14:17:35.574832+02:00 FAC radiusd[1571]: fn_eap_tls.c: Verifying remote LDAP user cert binding (user: t420.wl-cse.net, ldap id: 2)
2020-09-24T14:17:35.576344+02:00 FAC radiusd[1571]: rlm_eap_tls: Certificate binding check succeeded. (CN=T420.wl-cse.net, Issuer=/DC=net/DC=wl-cse/CN=wl-cse-DC01-CA)
2020-09-24T14:17:35.576426+02:00 FAC radiusd[1571]: rlm_eap_tls: Certificate passed CRL check.
2020-09-24T14:17:35.577215+02:00 FAC radiusd[1571]: (262) eap: EAP session adding &renlv:State = 0x79449ede7c0d9386
```



ПРИМЕР 802.1x – проверка RADIUS Акцепт и VLANid



На Fortigate мы видим что пользователь подключен.

А заглянув в содержимое пакетов обнаруживаем RADIUS-Акцепт 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]
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 Assertion Mark-up Language (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 информации
- Отвечает на запросы SAML от SP

Service Provider (SP) (поставщик сервиса)

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



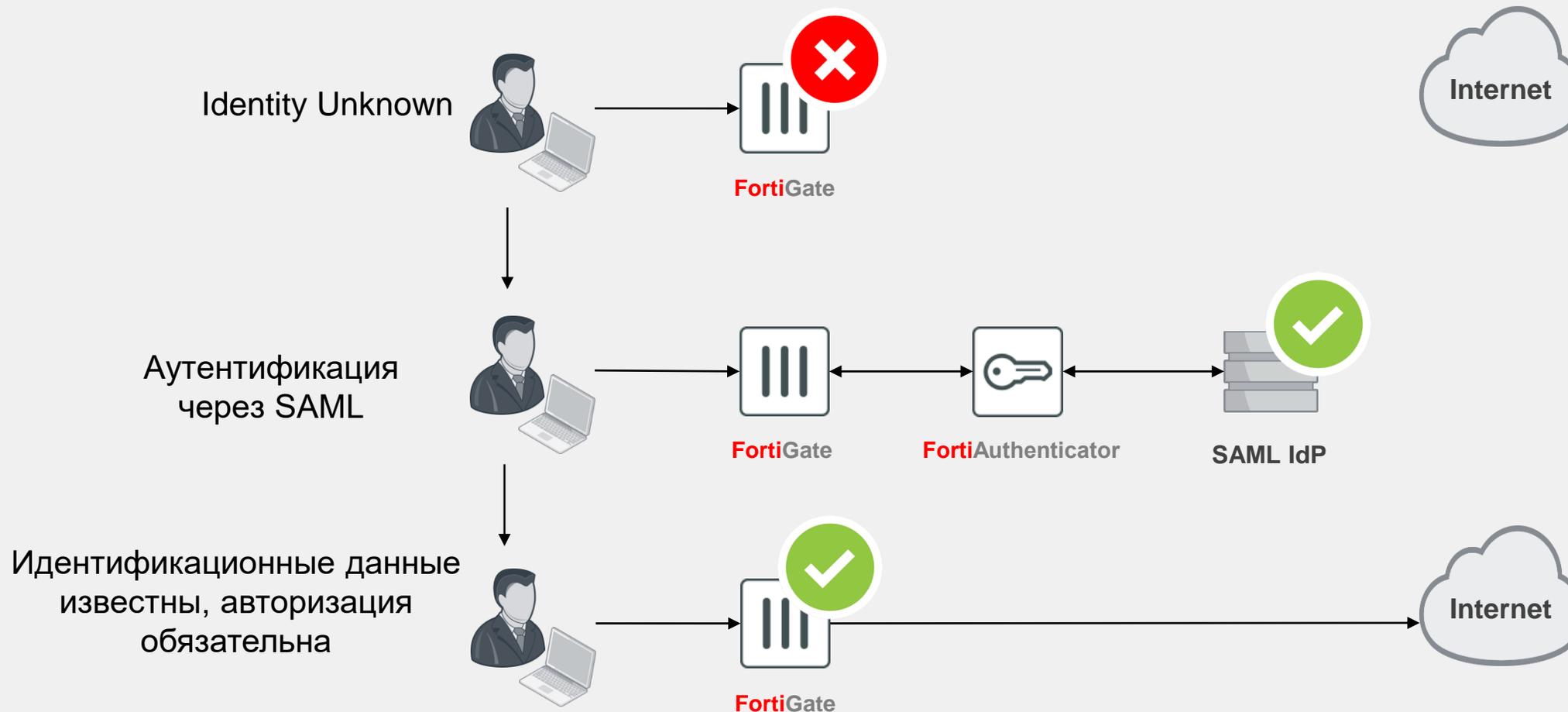
SAML – как это работает?

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



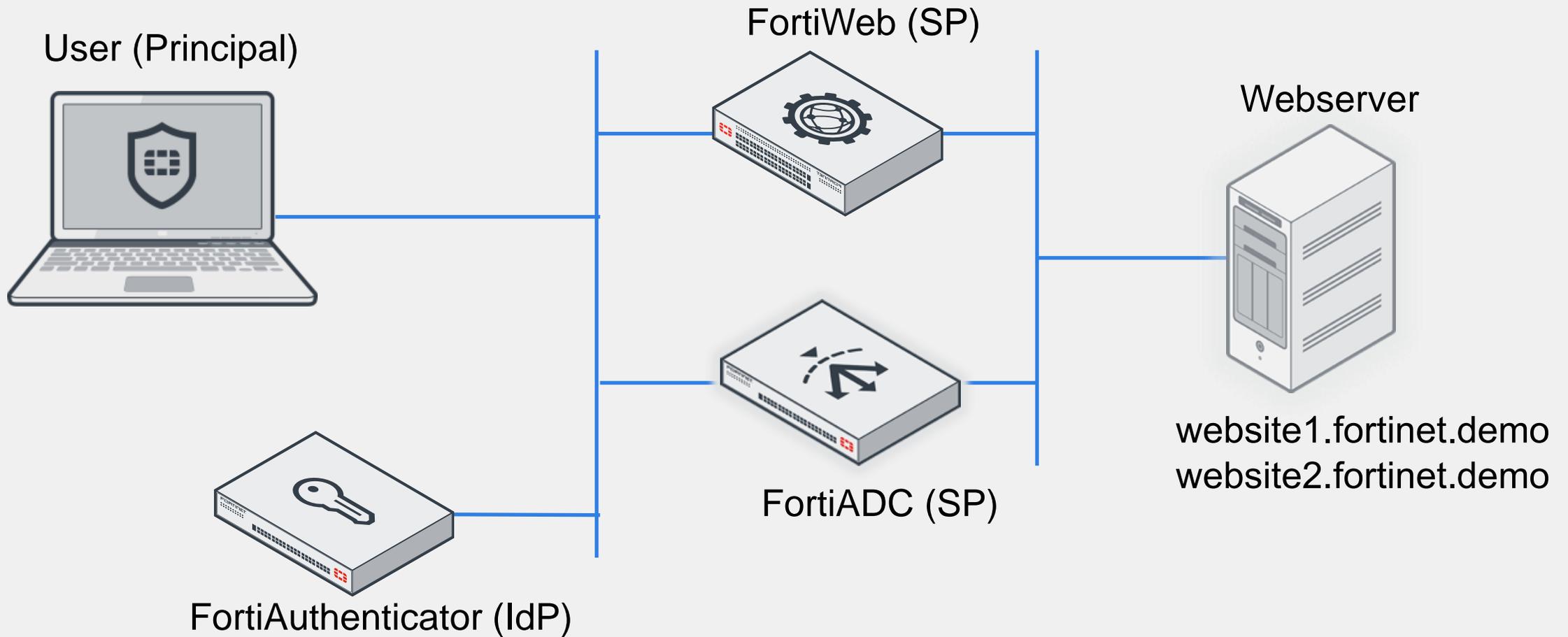


FortiAuthenticator

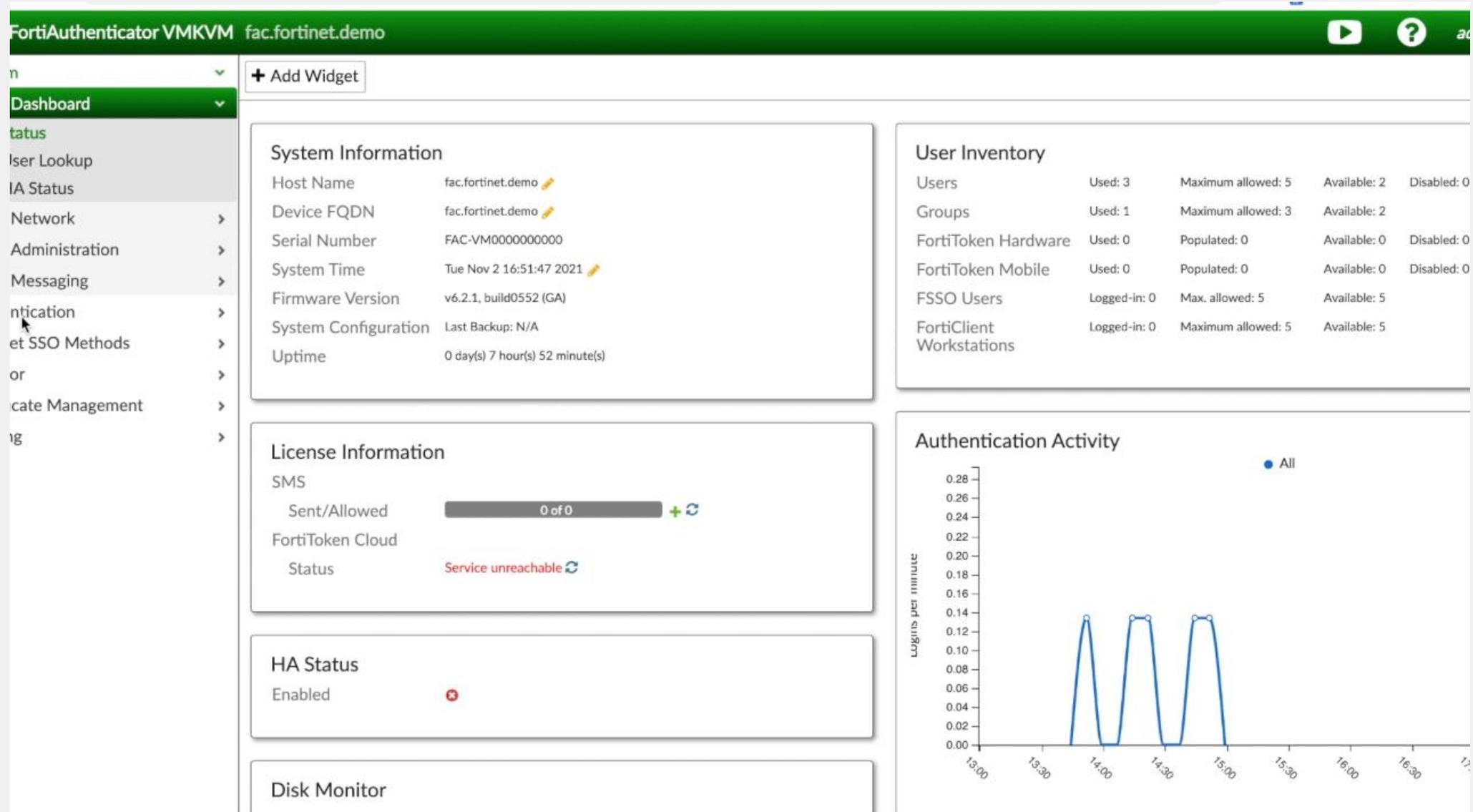
Демонстрации



Демонстрация работы SAML



Демонстрация работы SAML

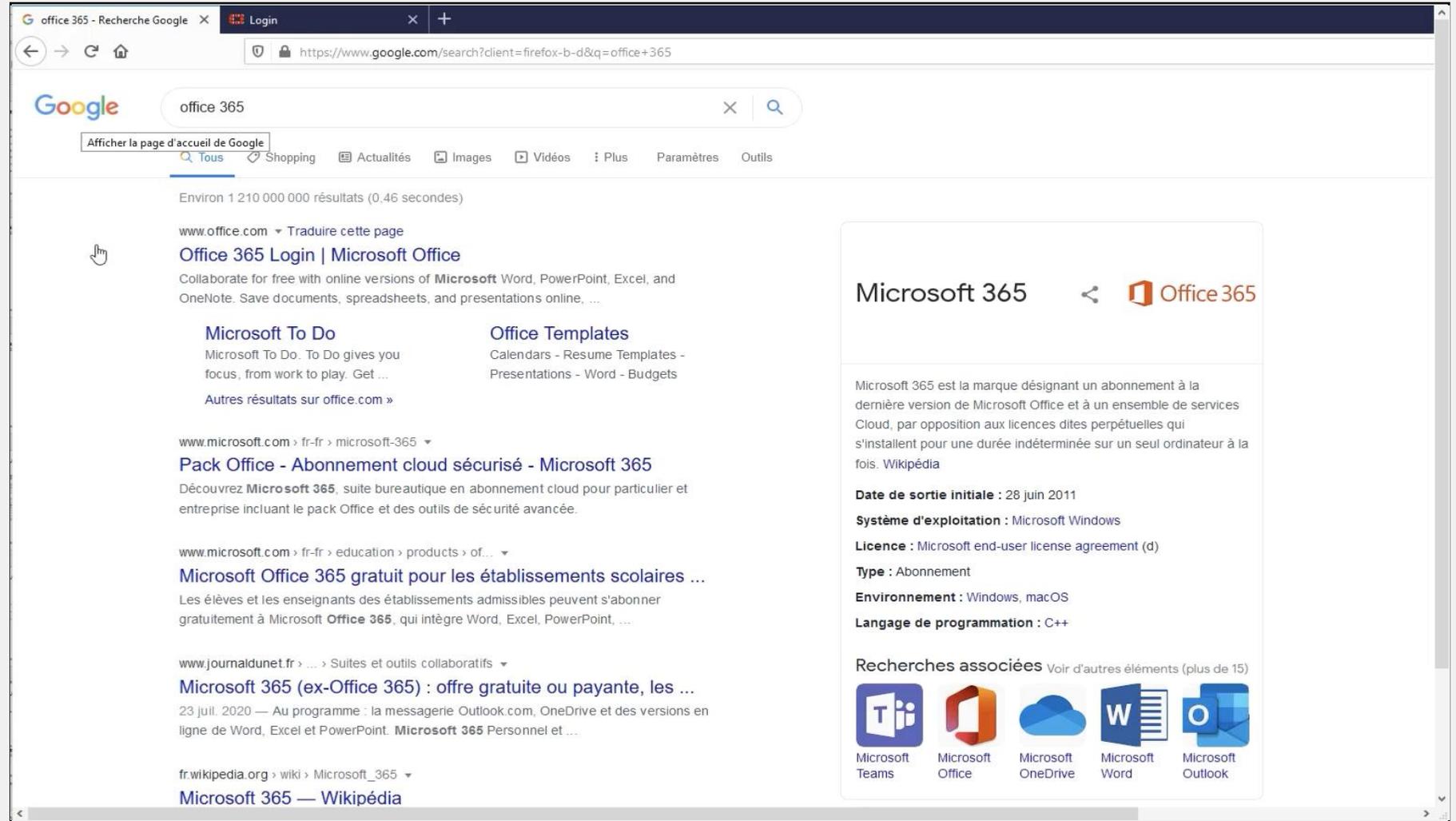
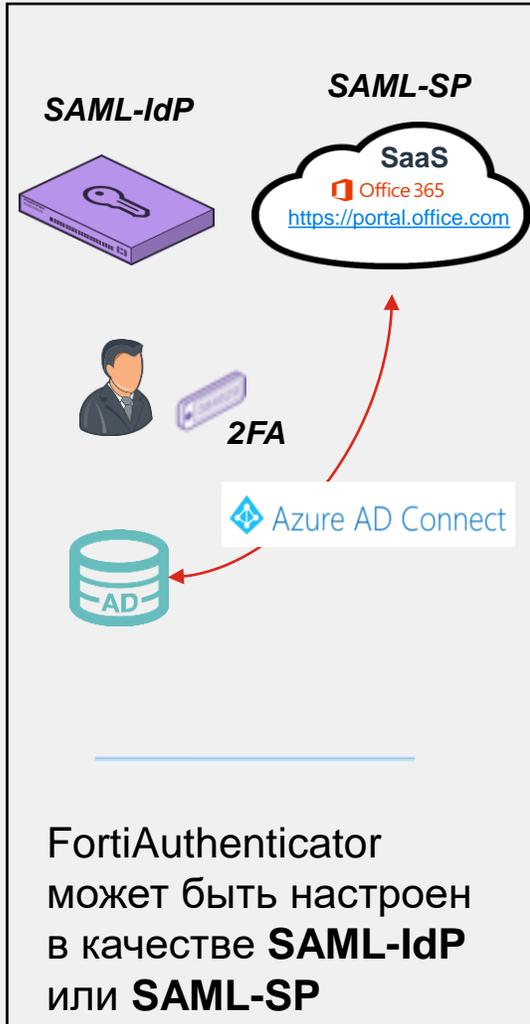


2FA для облачных приложений на примере O365



Демонстрация (видеоролик 2 мин)

Office365 и FortiToken Mobile (с Push нотификациями)





cis_se@fortinet.com (инженерная команда)