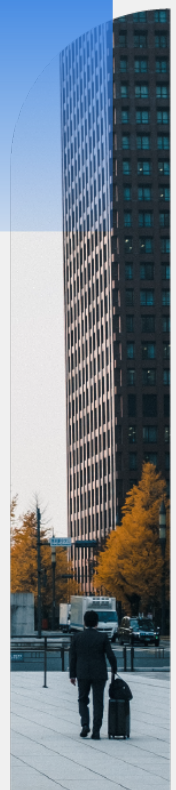


Zero Trust Network Access (ZTNA)

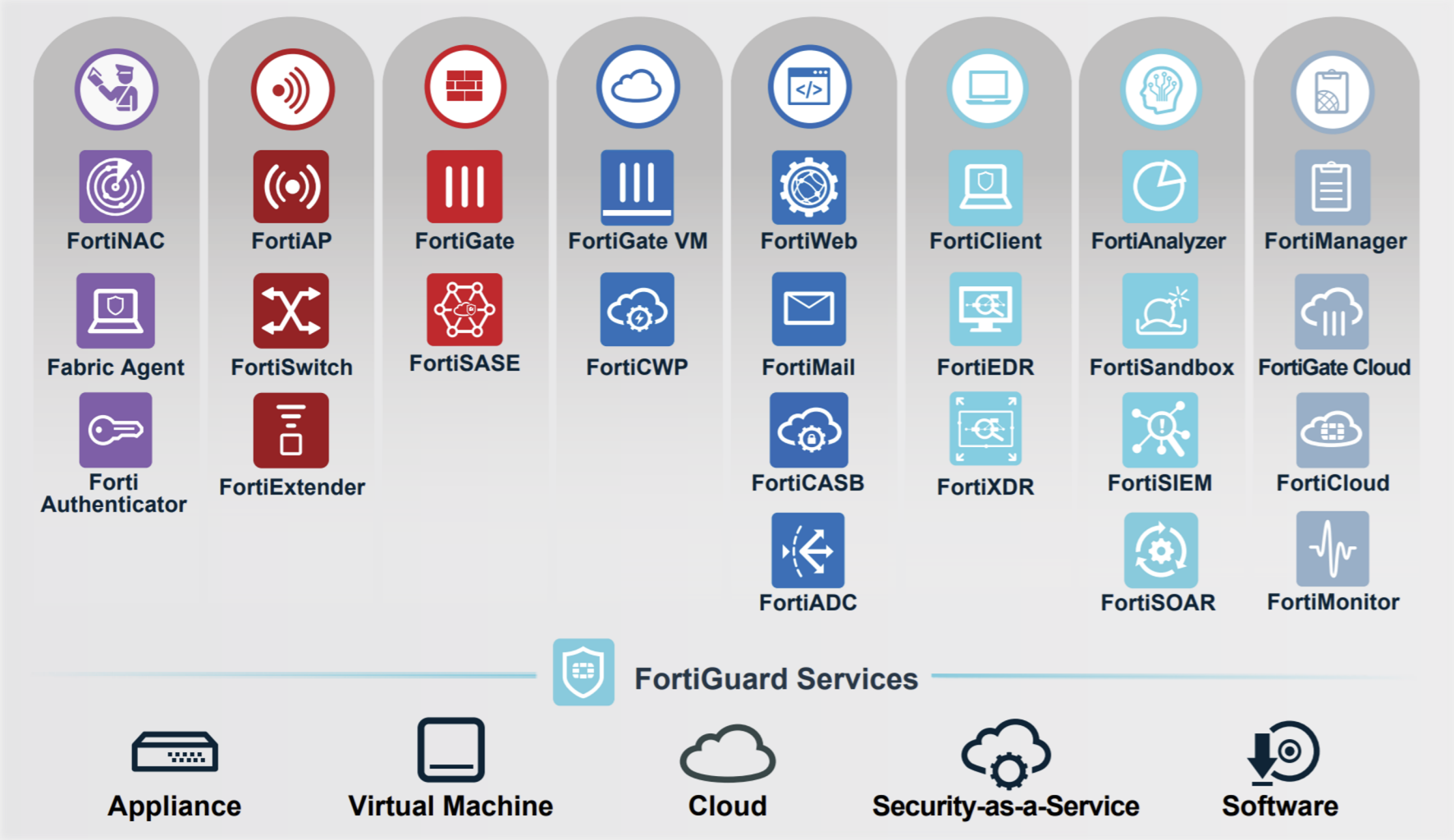
Эволюция удаленного доступа к сервисам

Юрий Захаров, SE

07.04.2021

Портфель решений

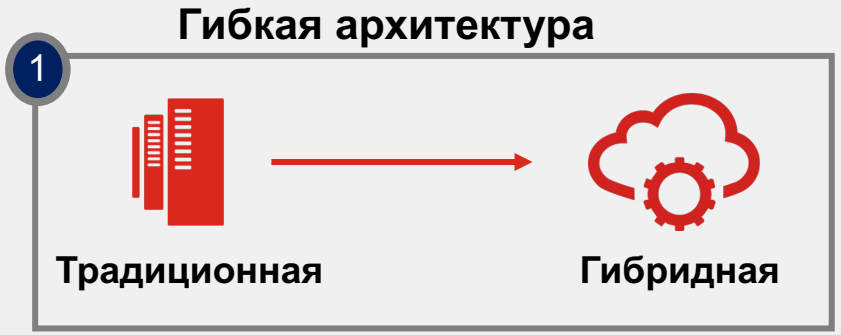
Далеко не полный список решений – только ключевые по направлениям

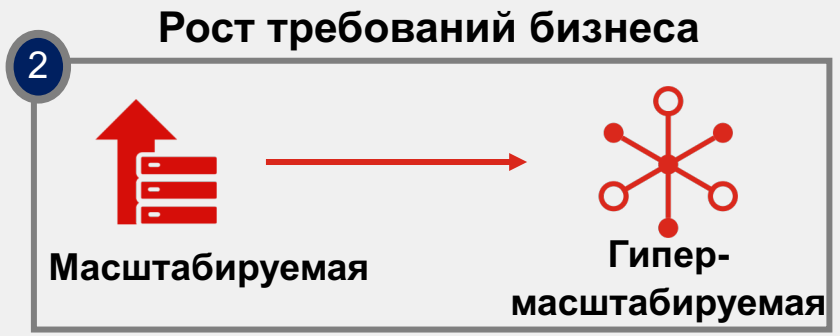



ZERO-
TRUST
Network Access

Динамично-изменяющая сетевая безопасность

Требуется постоянное развитие для соответствия современных запросам и требованиям[1]





1. Gartner: Top 10 Trends Impacting Infrastructure and Operations for 2020 Published 14 April 2020 - ID G00464437

Fortinet Security Fabric

Комплексная

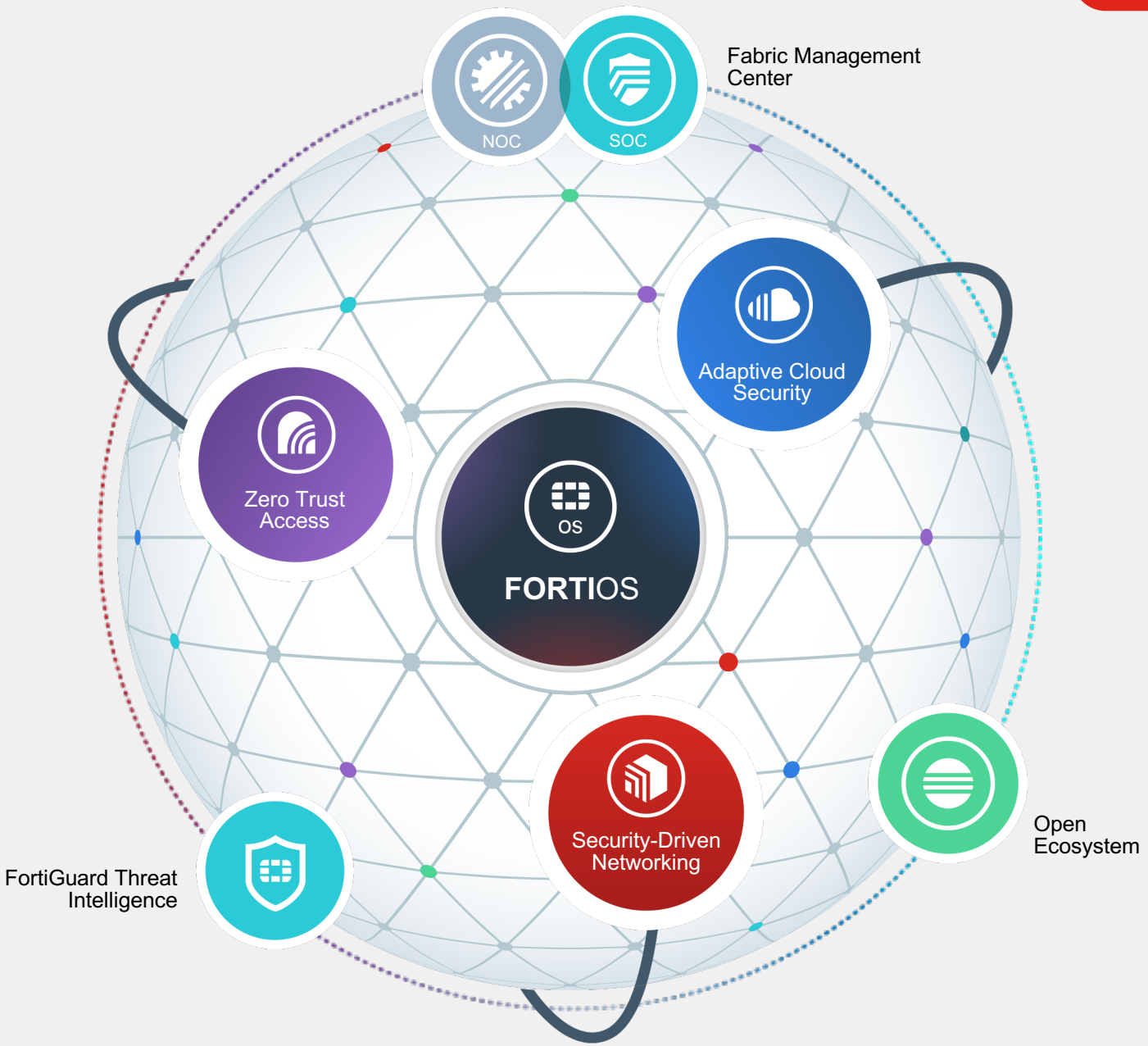
Обеспечение полной видимости поверхности цифровой атаки для лучшего управления рисками ИБ

Интегрированная

Уменьшение сложности сопровождения множества разнородных продуктов

Автоматизированная

Увеличение скорости управления и отклика



Ускоряющаяся конвергенция сети и безопасности

01 **Уменьшить площадь поверхности атаки**

Полная осведомленность, сегментация и защита от угроз с помощью Security Fabric и Enhanced FortiGuard Services

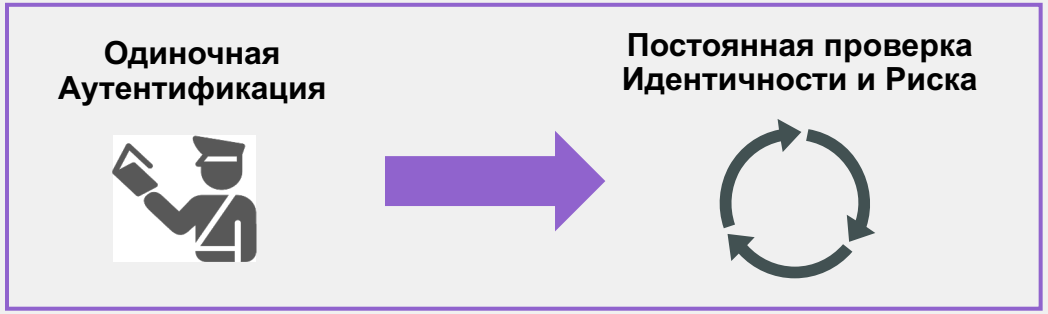
02 **Консолидировать и ускорить**

Сетевые функции и функции безопасности (например IPS, Web Filtering) на любом масштабе (Hyperscale) с использованием SPU

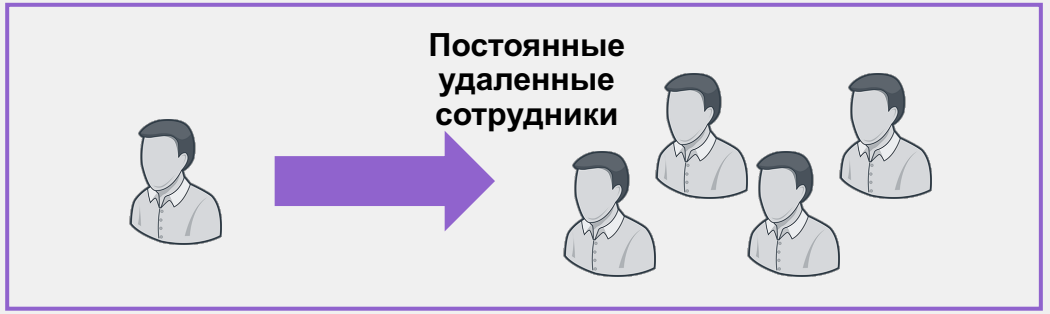
03 **Автоматизировать управление и реагирование на инциденты**

Защита гибридных IT с помощью расширенных функций Fabric Automation и Unified Console

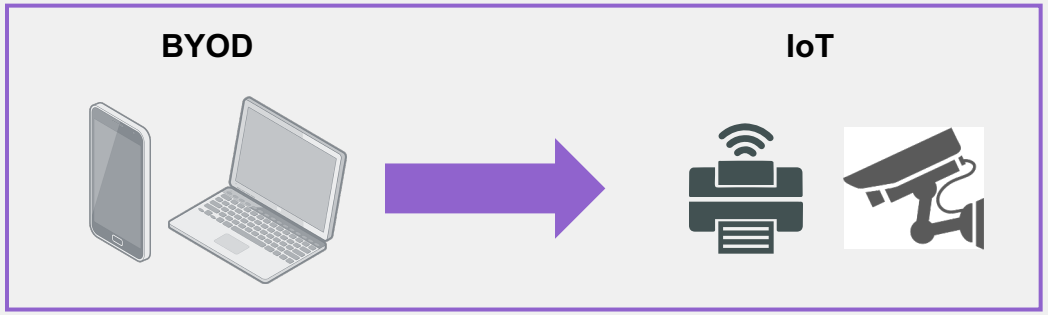
Тренды в развитии сетевого доступа



К 2024г, 70% приложений будет использовать MFA (по сравнению с 10% на сегодняшний момент[1]



С 4% до 30% возрастет доля сотрудников работающих постоянно удаленно к концу 2021[2]



К 2025г, в мире будет **12 МЛРД** установленных устройств IoT[3]

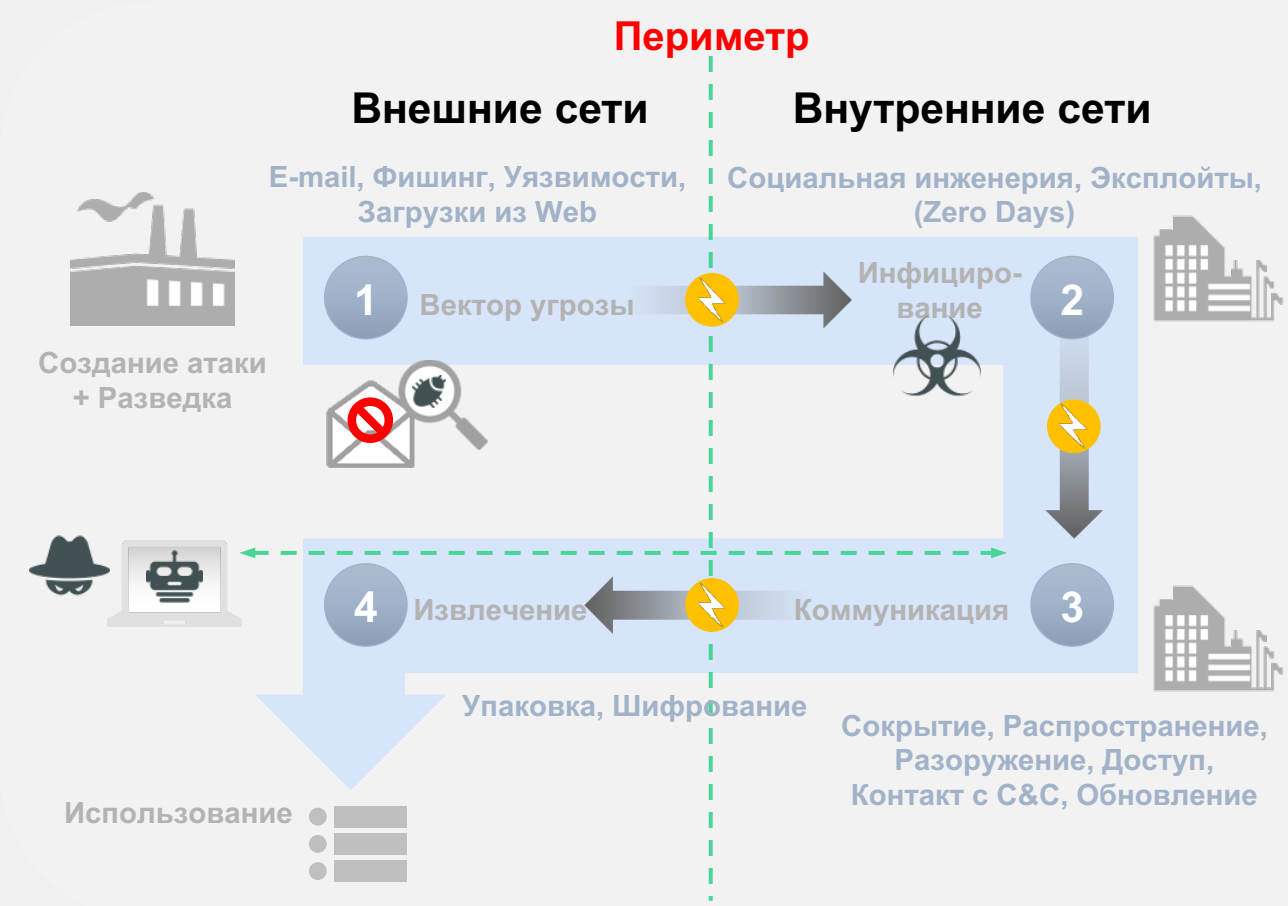
К 2025, в мире будет **3.7 МЛРД** установленных IoT устройств в промышленности, сфере обслуживания и на транспорте[3]

1 Gartner Magic Quadrant for Access Management, 12 August 2019
2 Global Workplace Analytics
3 Gartner. IoT Forecast

Традиционная модель безопасности

Реальность - Злоумышленники умеют развивать атаки внутри доверенной сети

- Традиционная модель защиты сети сфокусирована на защите Периметра
- Внутренние сети:
  - Плоская структура безопасности
  - Доверенная зона с малым количеством проверок и мер сдерживания
  - Слабый мониторинг безопасности, медленная реакция на инциденты ИБ
- Много способов проникнуть в сеть
- Оказавшись внутри сети, Злоумышленник становится частью доверенной зоны безопасности и имеет широкие возможности для горизонтального развития сетевой атаки



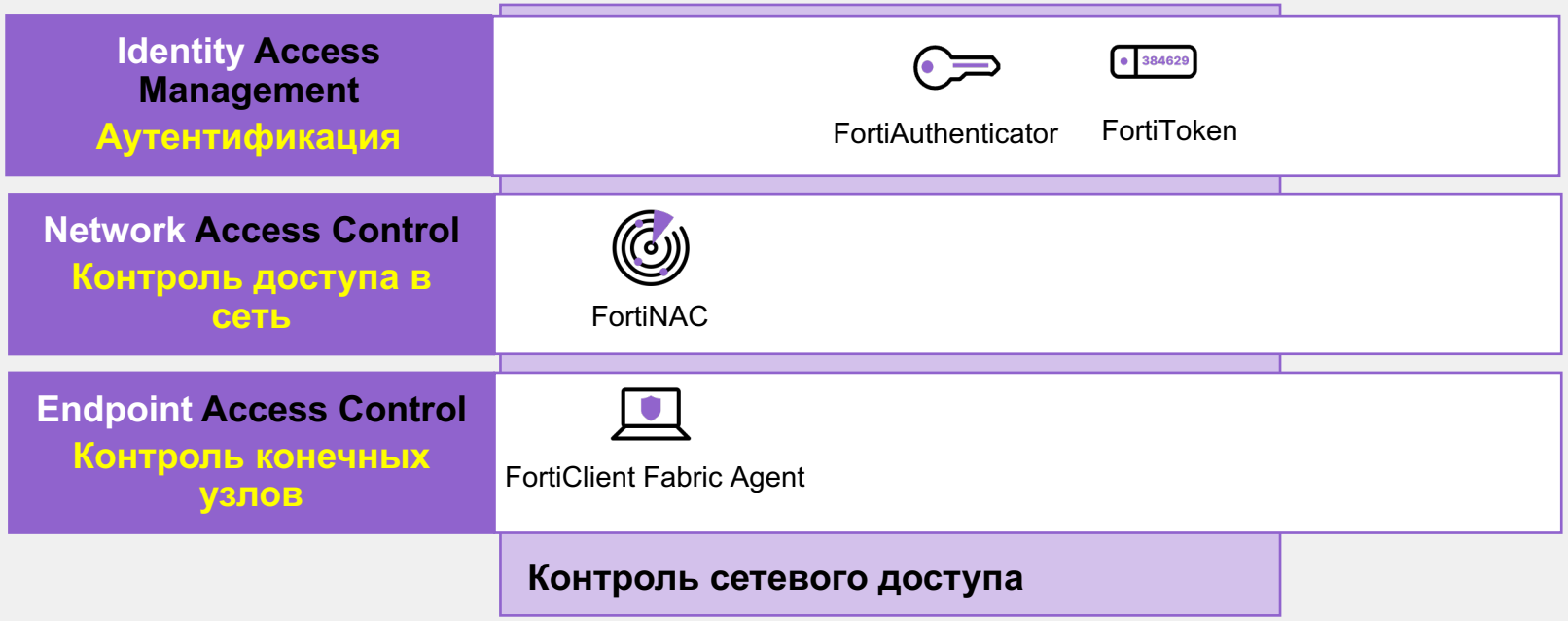
Zero-Trust Network Access

Знание и Контроль за Всеми и Всем внутри и вовне Сети

Обеспечение целостной политики безопасности в Сети, Облаке и вне Сети

Zero Trust Access (2020)

Компоненты решения



Контроль сетевого доступа

Контроль, КТО подключен к сети

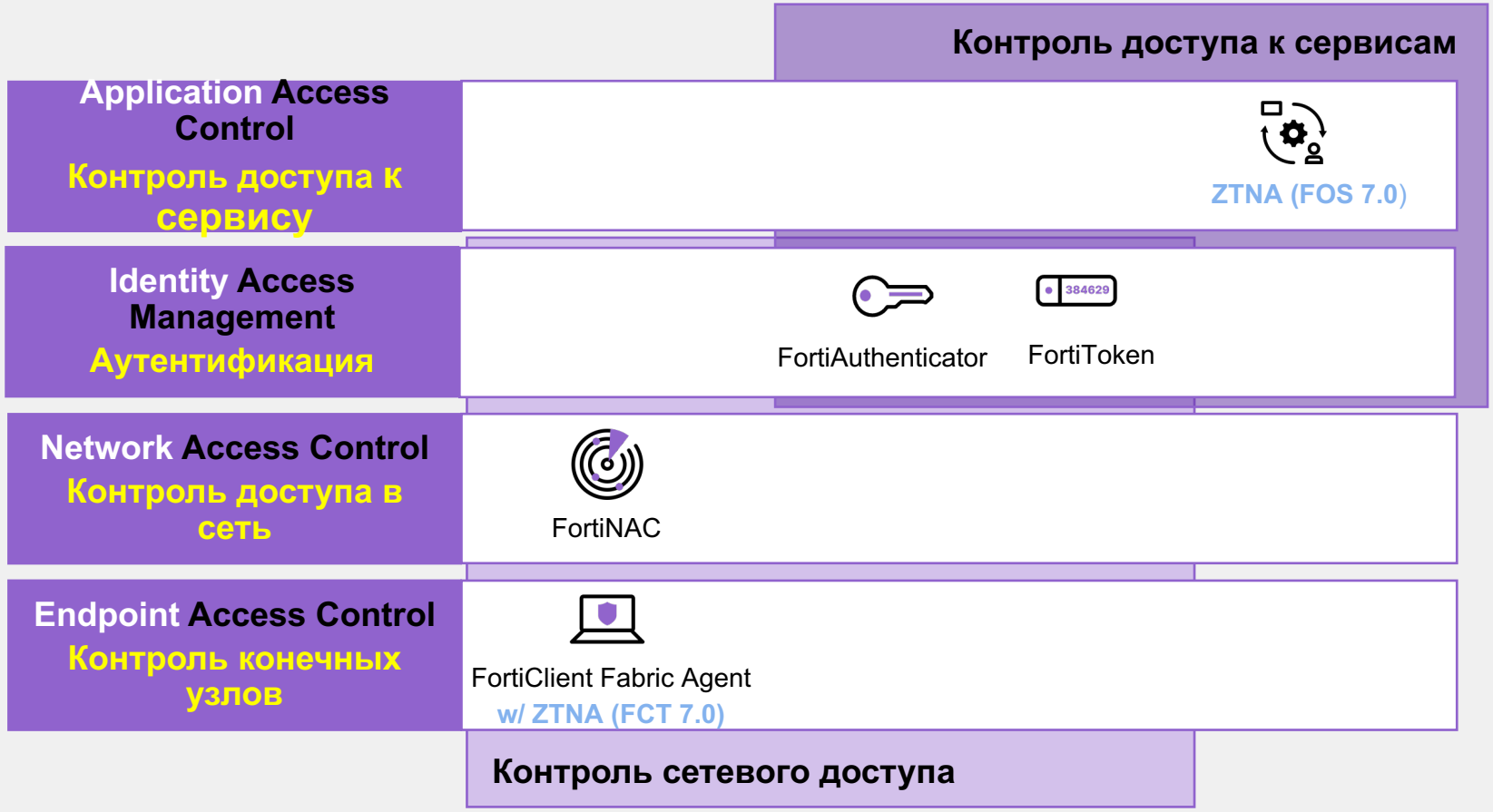
Контроль, ЧТО подключено к сети

Контроль устройств внутри и вовне сети

- Автоматическое установление VPN вне сети (off net)

Zero Trust Access (2021)

Компоненты решения



Контроль доступа к сервисам
- Кто имеет доступ к сервисам

Контроль сетевого доступа

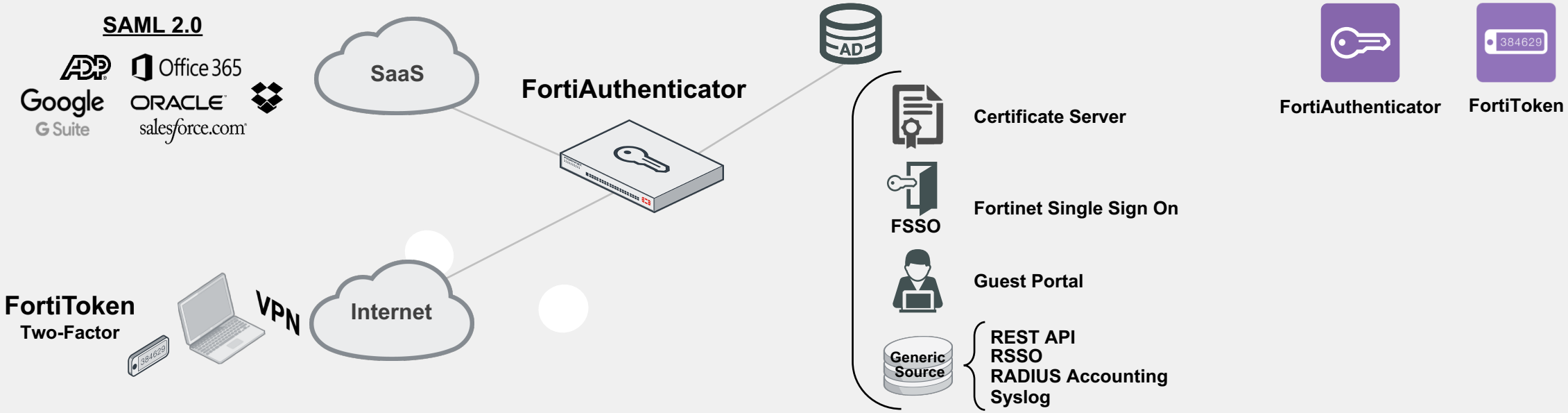
Контроль, КТО подключен к сети

Контроль, ЧТО подключено к сети

Контроль устройств внутри и вовне сети
- Защищенный ZTNA вне сети (off net)

Zero Trust Network Access - Идентификация пользователей

Необходимо знать, **КТО** подключен к сети

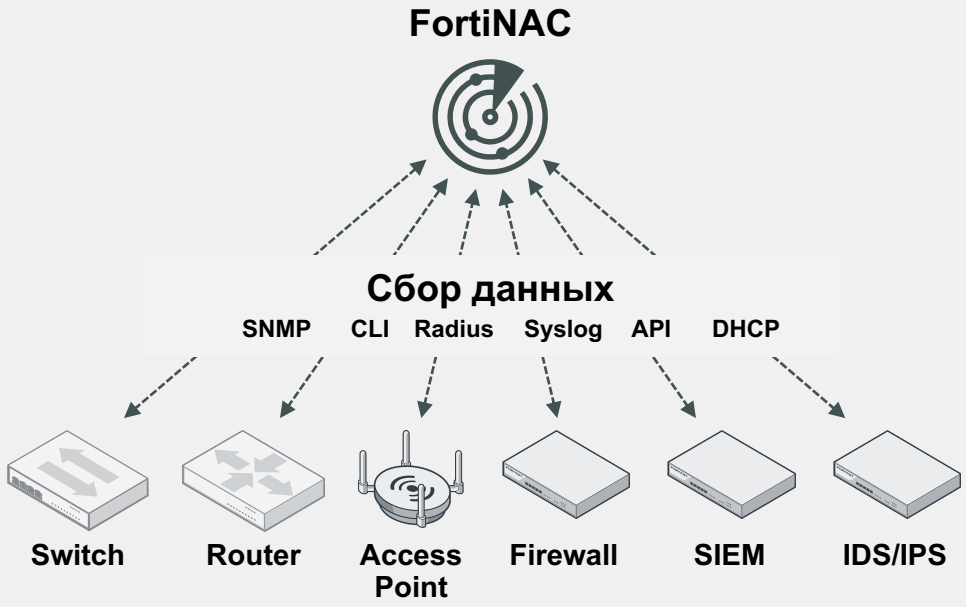


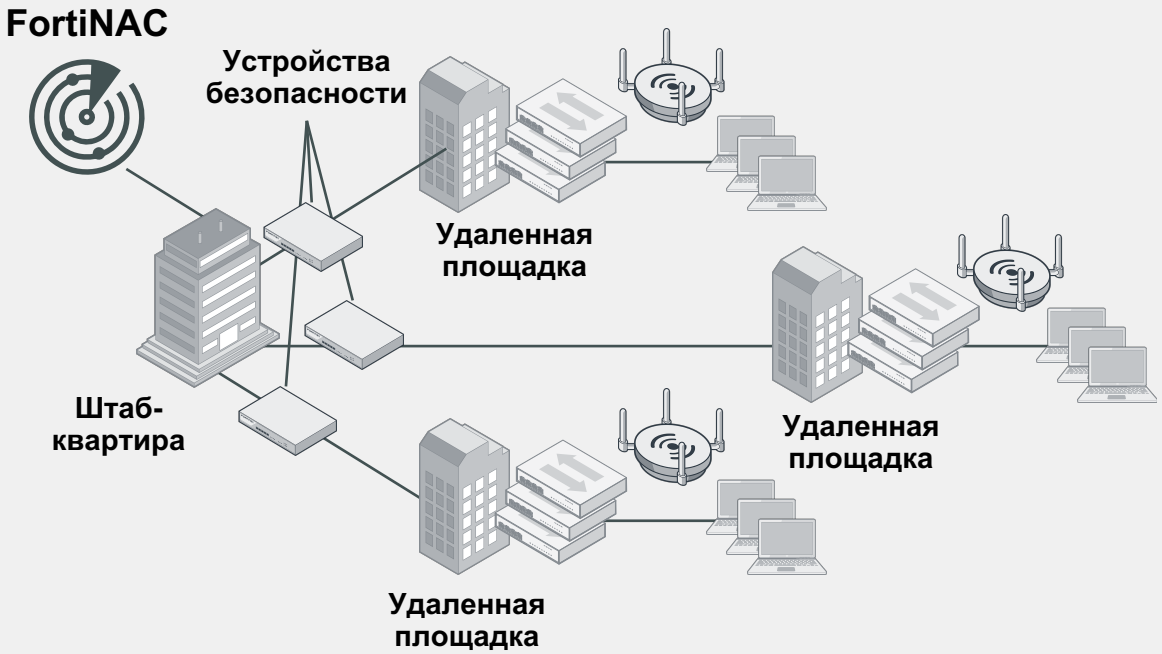
Аутентификация	Ролевой Доступ	Single Sign On
Установить личность / идентичность с помощью логина / пароля, сертификата, и / или ввода дополнительного фактора	Обеспечить информацией от источника аутентификации для использований привилегий	Упростить процесс для пользователя, обеспечив безопасность

Zero Trust Network Access— Контроль подключений устройств

Необходимо знать, **ЧТО** подключено в сеть

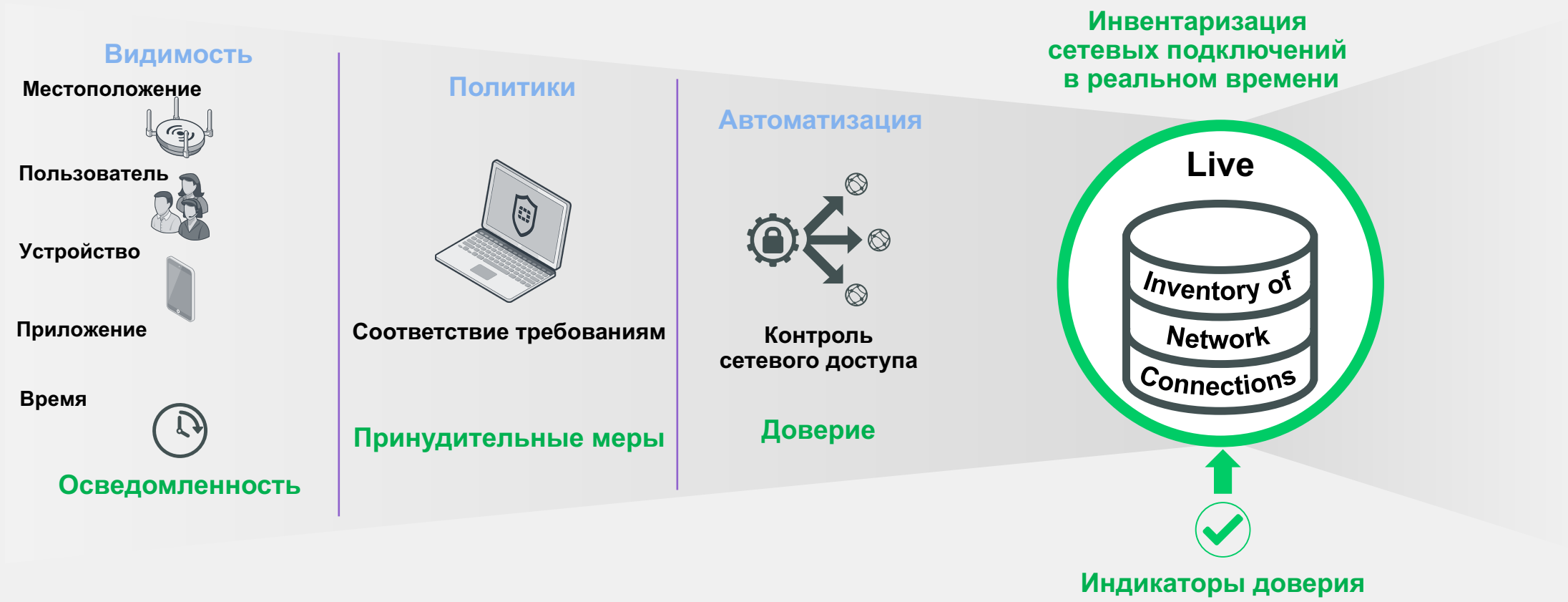
FortiNAC





Видимость	Динамический контроль	Непрерывное реагирование
Идентификация устройств, профилирование, поиск уязвимостей	Динамическая микро-сегментация Поддержка сегментации по намерениям	Автоматическое реагирование и оркестрация сети Расширение Security Fabric

Управление рисками до подключения в сеть

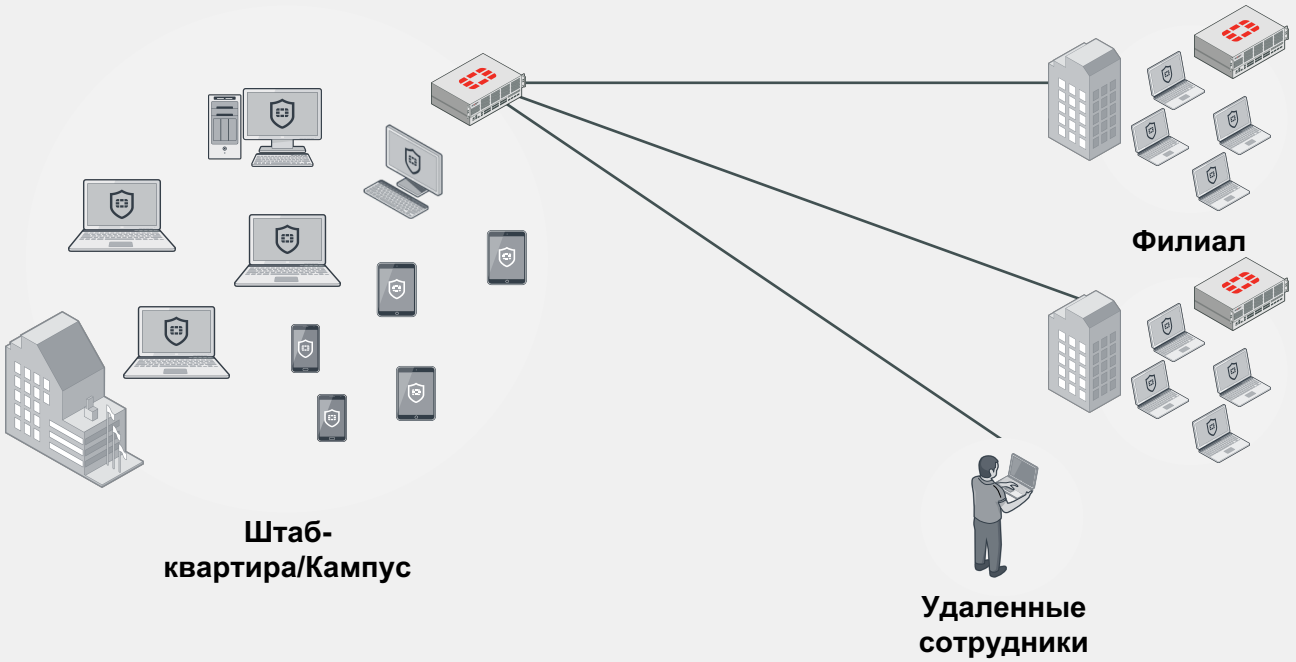


Управление рисками после подключения в сеть

Zero-Trust Network Access - Защита Устройств

Защита устройств внутри и вовне сети организации

FortiClient
Fabric Agent



Видимость конечных узлов	Контроль Цифровой Гигиены	Безопасный Удаленный Доступ
Сбор телеметрии Статус защиты Установленные приложения	Поиск Уязвимостей Веб Фильтрация Установка Исправлений / Патчей Динамическая Группировка	Динамический Контроль Доступа Организация VPN Single Sign On (SSO)

Ценность модели безопасности Zero-Trust Network Access

ВЫЗОВЫ	ПРЕИМУЩЕСТВА
Слабые и украденные пароли	Усиление безопасности с помощью двухфакторной аутентификации (2FA)
Слабый контроль за устройствами в сети	Возможность контролировать, какие устройства и пользователи подключены в сеть
Растущая плоскость атаки на IoT	Микросегментация с использованием политик доступа по принципу наименьших привилегий
Видимость и контроль за сотрудниками на удаленном доступе	Сбор телеметрии с устройств вне сети и принудительное применение и исполнение политик безопасности

Тренды области VPN

Gartner Market Guide for VPN, ноябрь 2020

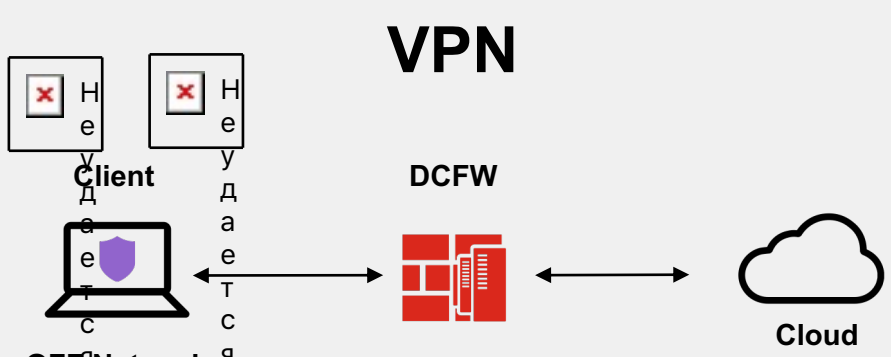
Ключевые моменты

Всплеск удаленной работы заставил срочно пересмотреть требования к удаленному доступу.

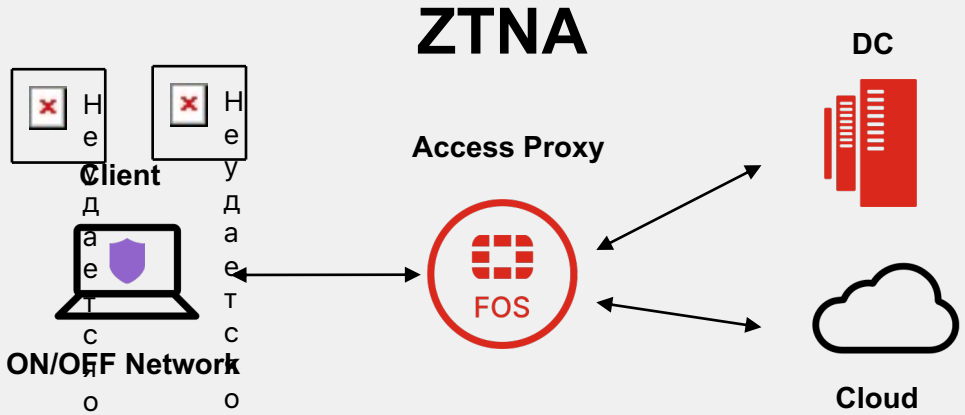
Технология IPsec VPN - это зрелый стандарт для безопасных зашифрованных сетевых подключений. Он остается выбором по умолчанию для потребностей конечного пользователя в доступе

Традиционный VPN постепенно заменяется новыми вариантами облачной безопасности, такими как ZTNA и CASB.

Переход от традиционных VPN к ZTNA

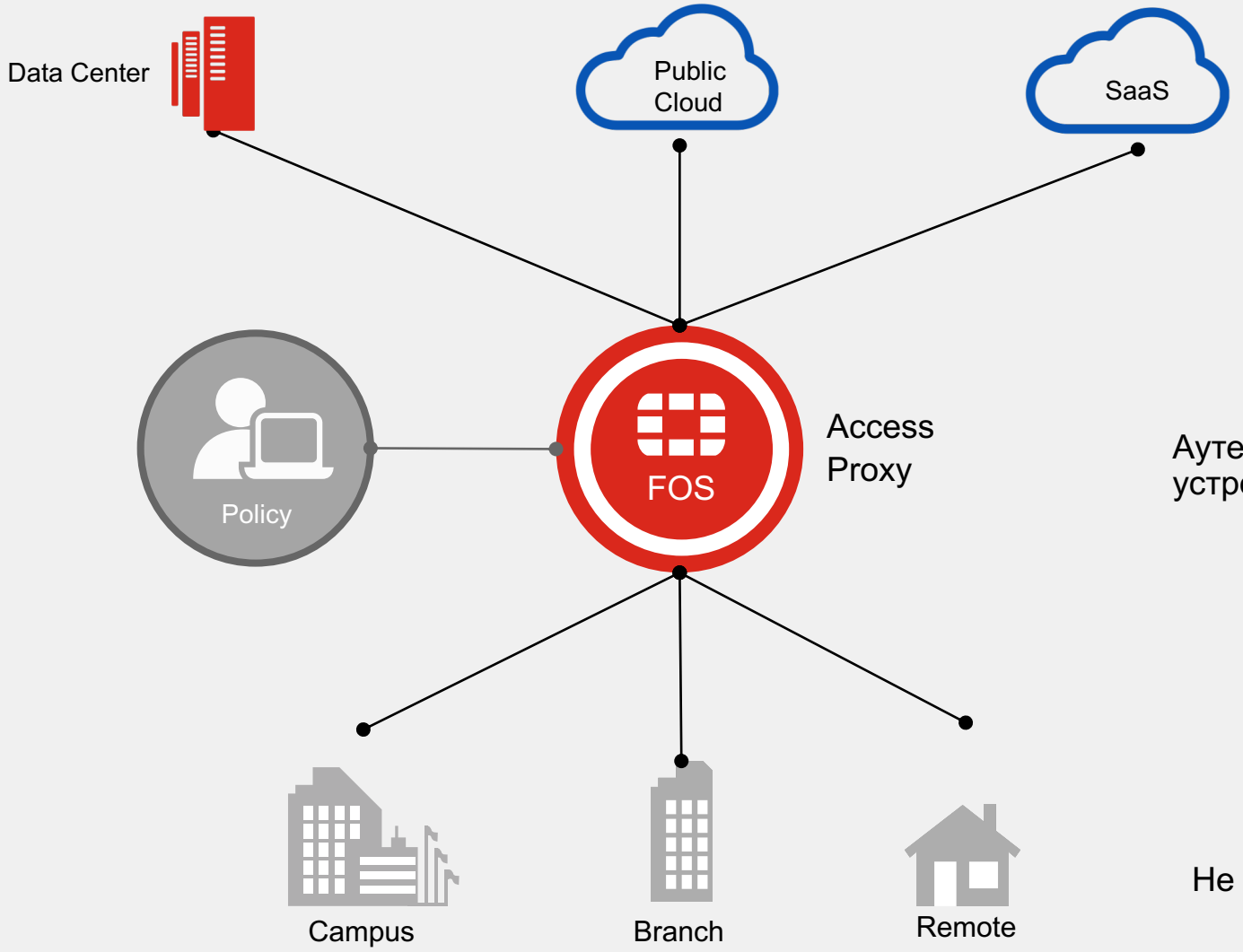


- Основная задача – получить **доступ внутрь сети** через установление VPN туннеля к МСЭ ЦОД
- **Все сервисы** доступны через данное подключение
- После установления VPN (прохождения аутентификации, в т.ч. 2FA) пользователь получает **полный доступ** к приложению **без дополнительного контроля**



- Предоставляет **доступ только к определенному сервису** для пользователя внутри или снаружи сети
- FOS (***Access Proxy***) прозрачен для пользователей и доступен в составе DC Firewall, SASE или Cloud
- Управляет **доступом к сервисам по ролям** и отслеживает поведение после подключения

ZTNA: гибкая архитектура

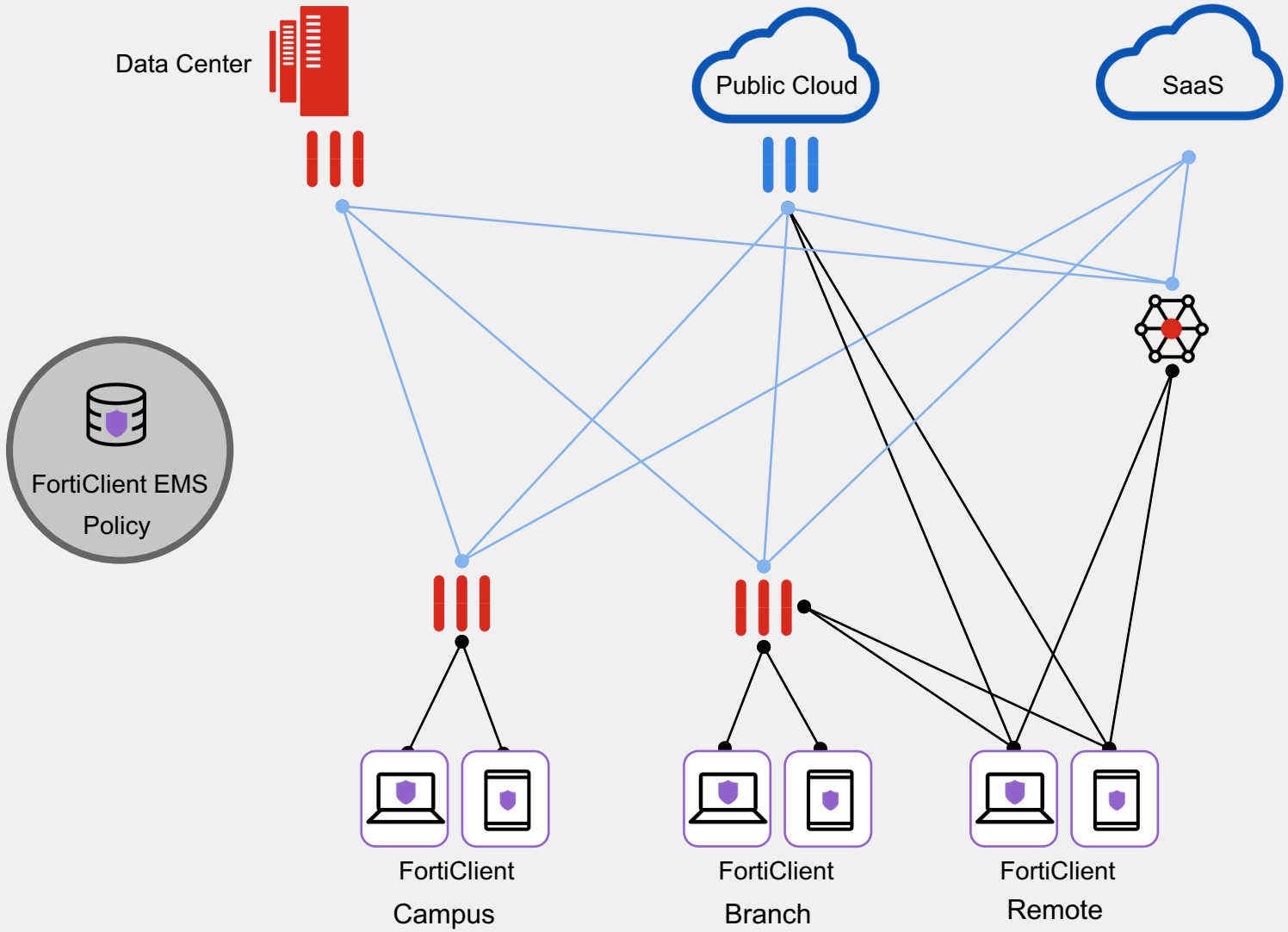


Не зависит от расположения сервиса

Аутентификация и проверка состояния устройства

Не зависит от локации пользователя

ZTNA: автоматические защищенные подключения



Использование существующей инфраструктуры

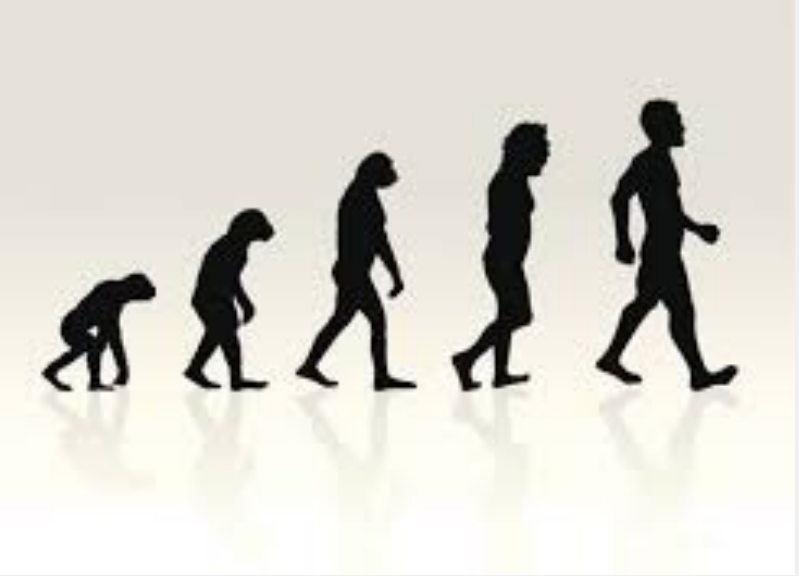
Непрерывная переоценка и контроль (Enforcement)

Автоматические защищенные ZTNA туннели (HTTPS/SSH)

Zero Trust Network Access

Эволюция VPN доступа и доступа к сервисам

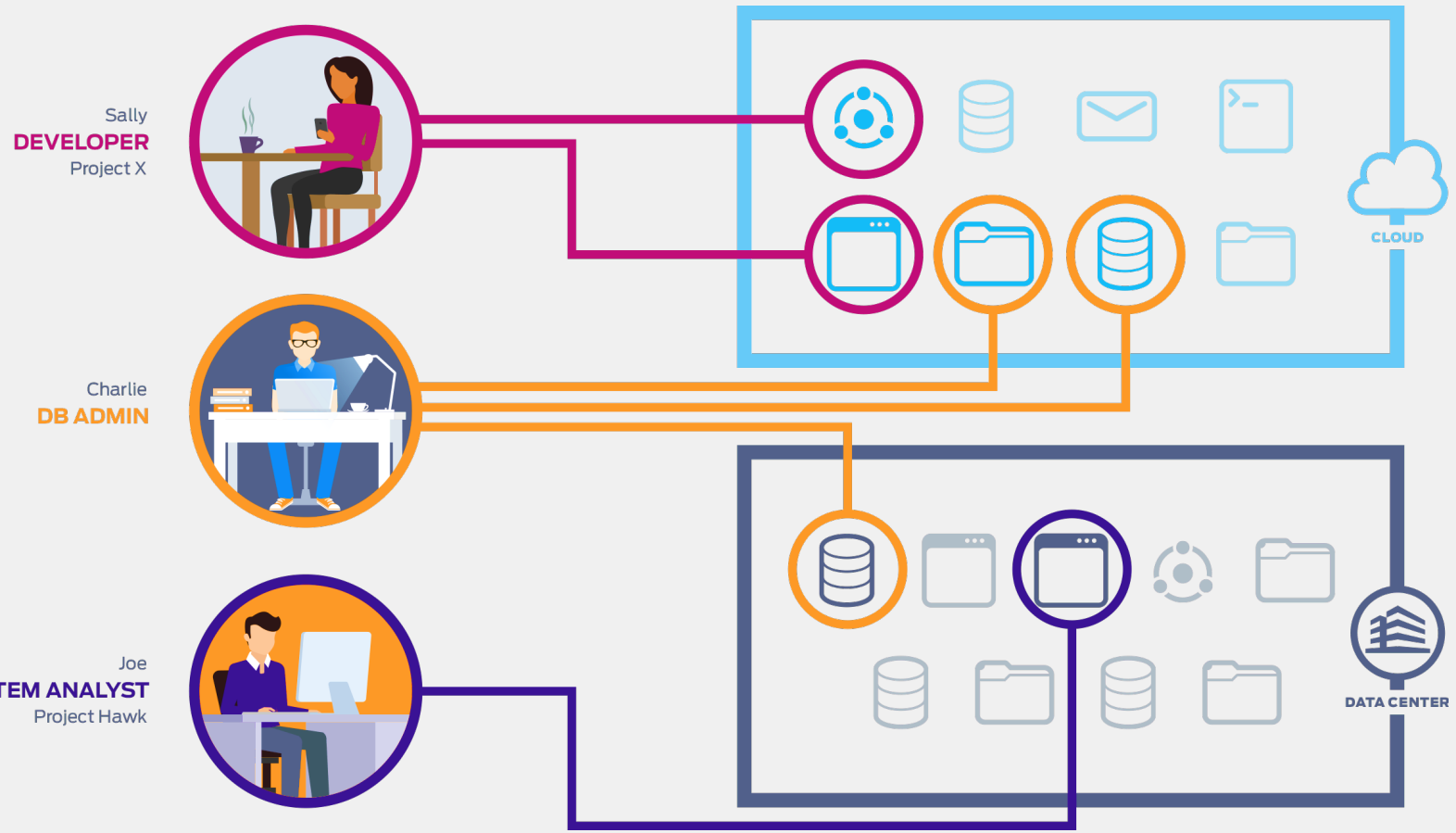
- Более детальный контроль
  - По приложениям, по сессионная аутентификация
  - Больше нет широкого доступа к сети через VPN
- Удобство для пользователей
  - Автоматически инициирует безопасный туннель, когда пользователь обращается к приложениям
  - Централизованно настраивается через EMS
- Общая политика, не зависящая от местоположения
  - Местоположение **пользователя** не имеет значения (on-net, off-net)
  - Местоположение **приложения** не имеет значения



ZTNA: удобство для пользователей

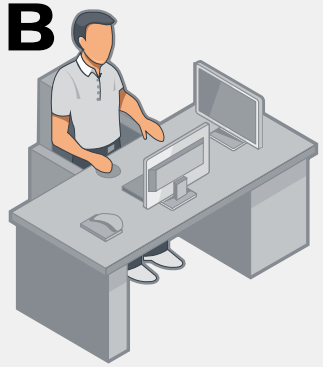
Не зависит от местоположения пользователя

- Пользователи в офисе или вне его
- Автоматические безопасные туннели к приложениям
- Приложения, расположенные где угодно
- Поддержка SSO
- Поддержка 2FA

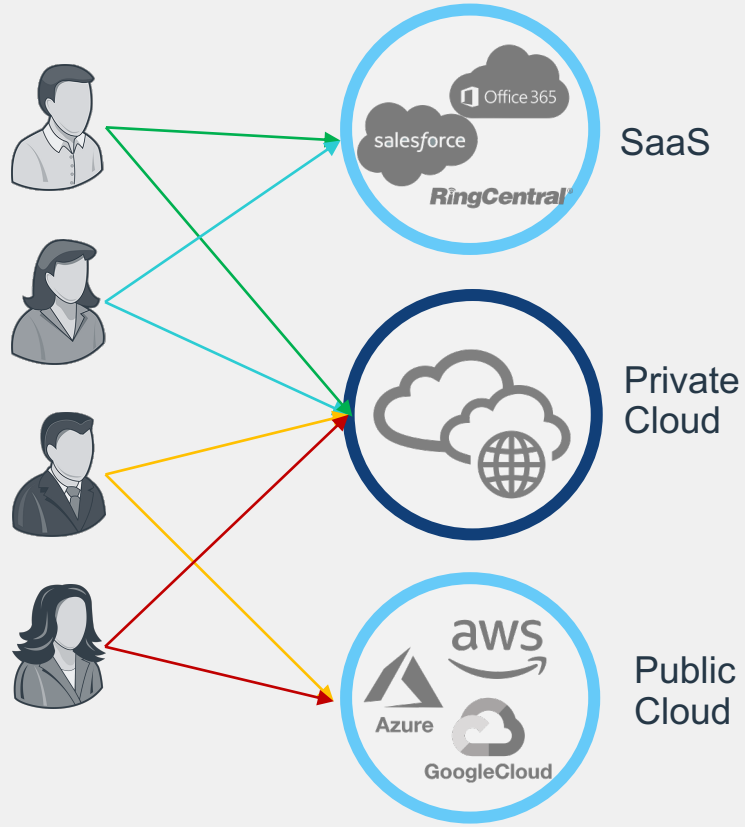


ZTNA: удобство для администраторов

Не зависит от местоположения приложения / сервиса



- Детальный контроль
  - Посессионная аутентификация
  - Поддержка MFA
  - Включена оценка рисков от устройств
- Централизованно управляемый
  - Внутри сети или за ее пределами
  - Поддержка групп пользователей позволяет выполнять массовую настройку политик
- Приложения, расположенные где угодно
- Доступ пользователей разрешен только к необходимым приложениям и данным



ZTNA от Fortinet

Состав решения

Основные элементы

FortiGate

- FortiGate строит безопасный туннель, поддерживает таблицу доступа пользователей /групп / приложений (FortiOS 7.0)

FortiClient / FortiClient EMS

- FortiClient как агент ZTNA для безопасного подключения к FortiGate (FortiClient 7.0, обязателен EMS)

FortiAuthenticator

- FortiAuthenticator обеспечивает многофакторную аутентификацию и поддержку SAML для единого входа в облачных приложениях.

FortiManager

- FortiManager обеспечивает централизованное управления в распределенных сетях, для большого количества FortiGate.

Преимущества ZTNA от Fortinet

В сравнение с решениями других производителей

- Обеспечение управления приложениями как для локальных, так и для удаленных пользователей
  - Большинство решений ZTNA - это варианты только для SASE с большими финансовыми затратами на покрытие сети распределенной компании.
  - Предоставляет защиту на базе FortiGate, где бы вы ни находились
- Упрощенное управление и отчетность
  - Интегрирован в платформу Security Fabric.
  - Консолидированное решение для конечных точек - агент фабрики, безопасные туннели
- Повышенная безопасность
  - Передовые технологии инспекции трафика средствами FortiGate
- Лицензии не требуются
  - Просто включите функцию в FortiOS и FortiClient!

Лицензирование FortiClient 7.0

FORTICLIENT EDITION	ZTNA	EPP / APT	SASE SIA	CHROMEBOOK
Zero Trust Security	Windows, Mac, Linux	Windows, Mac, Linux	Windows, Mac, Linux	Chromebook
Zero Trust Agent with MFA	✓	✓	✓	
Central Management via EMS	✓	✓	✓	✓
Central Logging & Reporting	✓	✓	✓	✓
Dynamic Security Fabric Connector	✓	✓	✓	
Vulnerability Agent & Remediation	✓	✓	✓	
SSL VPN with MFA	✓	✓	✓	
IPSEC VPN with MFA	✓	✓	✓	
FortiGuard Web Filtering	✓	✓	✓	✓
USB Device Control	✓	✓	✓	
Next Generation Endpoint Security				
AI powered NGAV		✓	✓	
FortiClient Cloud Sandbox[1]		✓	✓	
Automated Endpoint Quarantine		✓	✓	
Application Firewall[1]		✓	✓	
Application Inventory		✓	✓	
Ransomware Protection[2]		✓	✓	
Cloud Based Endpoint Security				
SSL Inspection			✓	
Inline AV & Anti-Malware			✓	
Intrusion Prevention (IPS)			✓	
FortiGuard Web Filtering			✓	
DNS Security			✓	
Data Leak Prevention			✓	
Additional Services				
Cloud Hosted EMS		Add-on		
24×7 Support		Included		
FortiCare BPS		Included first year		

1. FortiClient (Linux) does not support this feature.
2. Only FortiClient (Windows) supports this feature.

ZTNA от Fortinet

Подведем итоги

- ZTNA от Fortinet построено на базе NGFW FortiGate – лидера в классе
- ZTNA от Fortinet предоставляет гибкие возможности по выбору архитектуры: on-prem ПАК, ВМ или SASE сервис
- ZTNA от Fortinet обеспечивает инлайн инспекцию трафика на 7 уровне и защиту от ВПО и утечки данных
- ZTNA от Fortinet отслеживает состояние сессий и поведение пользователей
- FortiClient обеспечивает автоматическое установление защищенных туннелей до публикуемого сервиса и в дополнение защищает рабочую станцию средствами межсетевого экранирования, веб фильтрации, поиск уязвимостей, отправляется телеметрия
- FortiClient обеспечивает динамический контроль доступа на основе анализа состояния рабочей станции (endpoint posture и zero trust tags)
- Решение от одного вендора, включая средства аутентификации (RBAC), 2FA (FortiToken), централизованное управление (FortiManager)
- В дополнение к ZTNA Fortinet предлагает решения по контролю сетевого доступа, идентификации и профилированию устройств (FortiNAC)

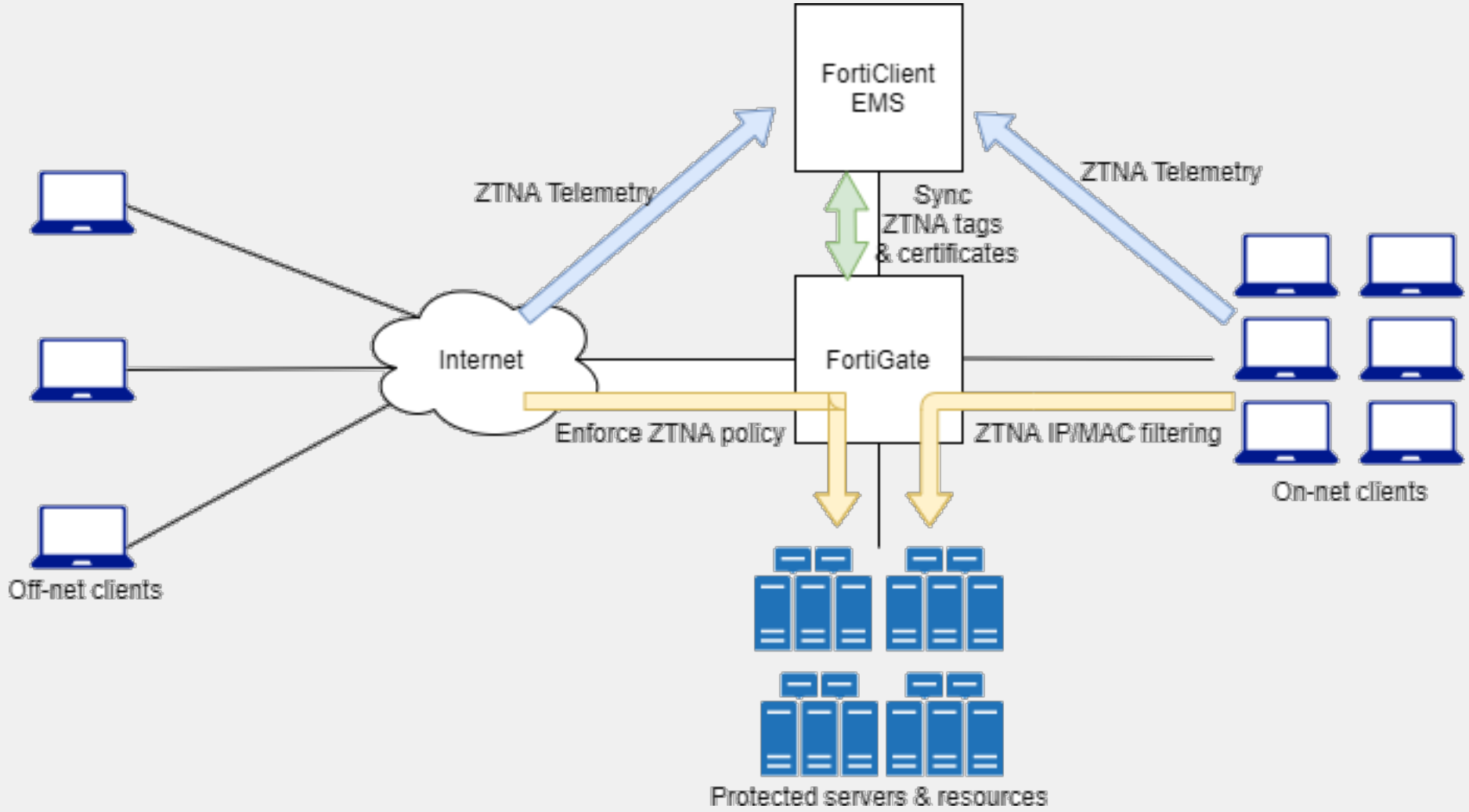
Zero Trust Network Access

Принцип работы и сценарии в FortiOS 7.0

Zero Trust Network Access в FortiOS 7.0

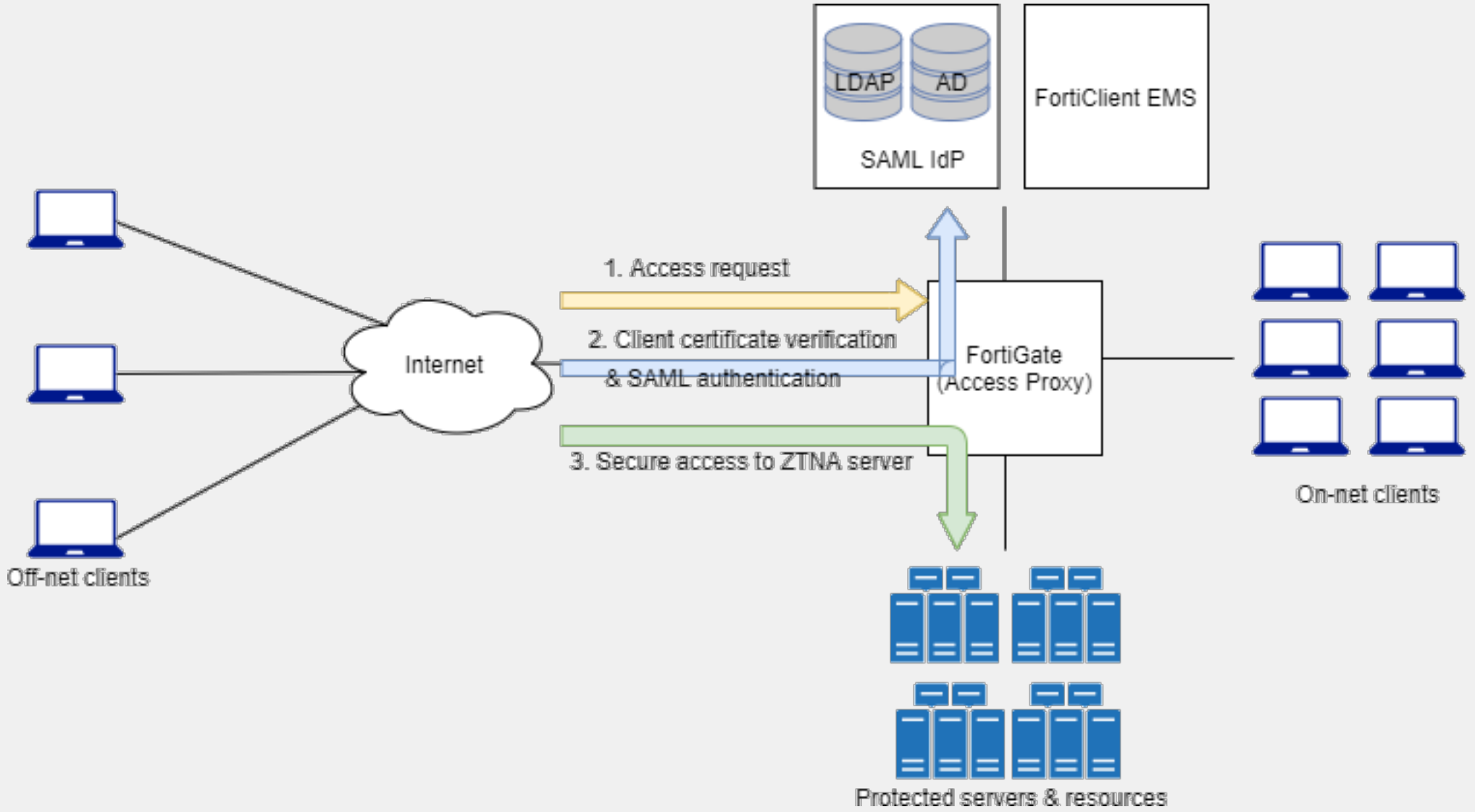
Два режима ZTNA

- Full ZTNA
- IP/MAC filtering



Zero Trust Network Access в FortiOS 7.0

Access proxy



Zero Trust Network Access в FortiOS 7.0

Основные компоненты настройки ZTNA

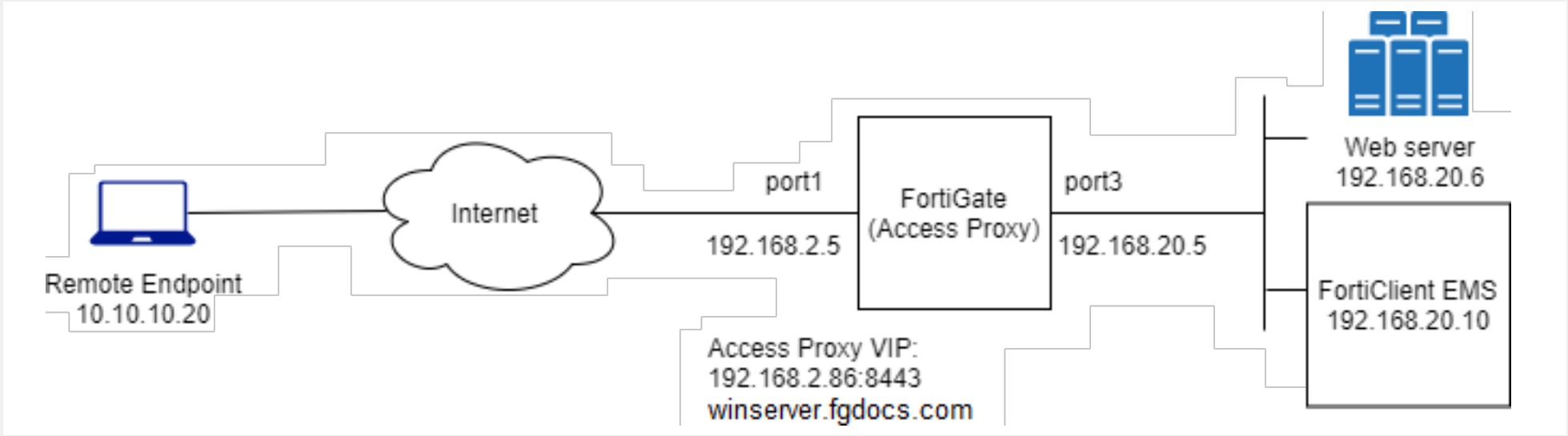
1. FortiClient EMS fabric connector и ZTNA tags

Требуется FortiOS 7.0, EMS 7.0

2. ZTNA server
3. ZTNA rule
4. Firewall policy

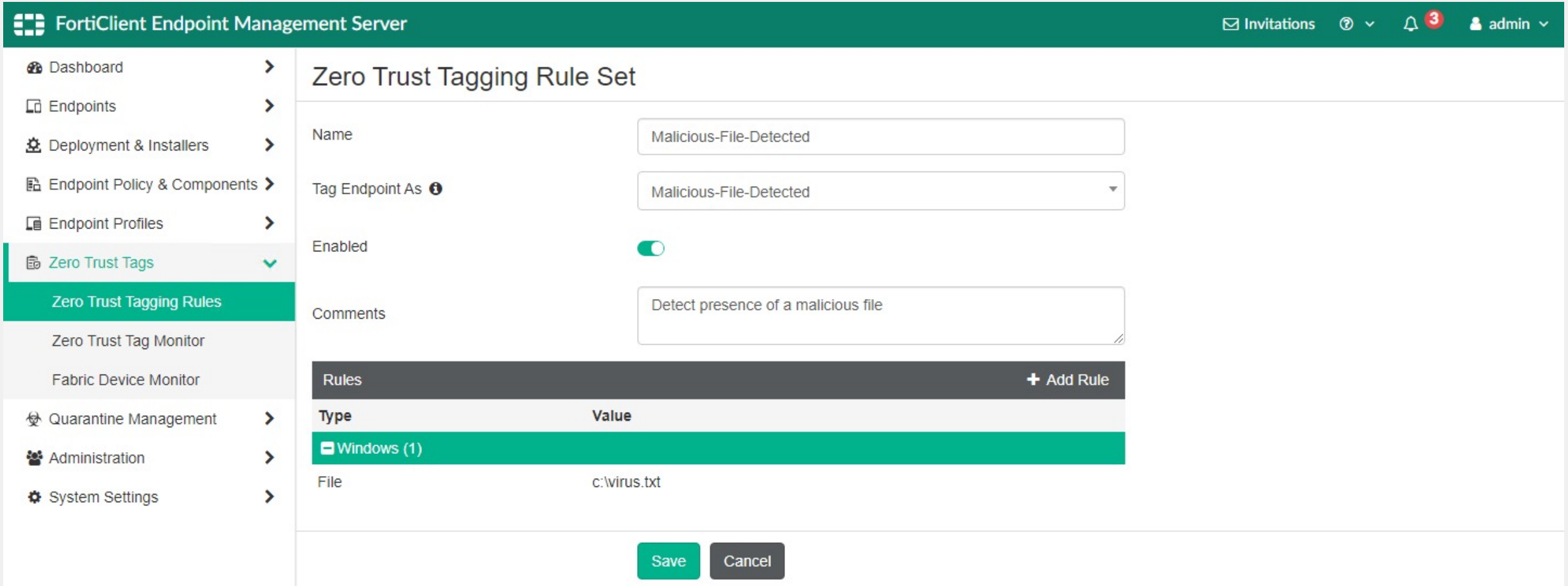
Zero Trust Network Access в FortiOS 7.0

ZTNA HTTPS access proxy



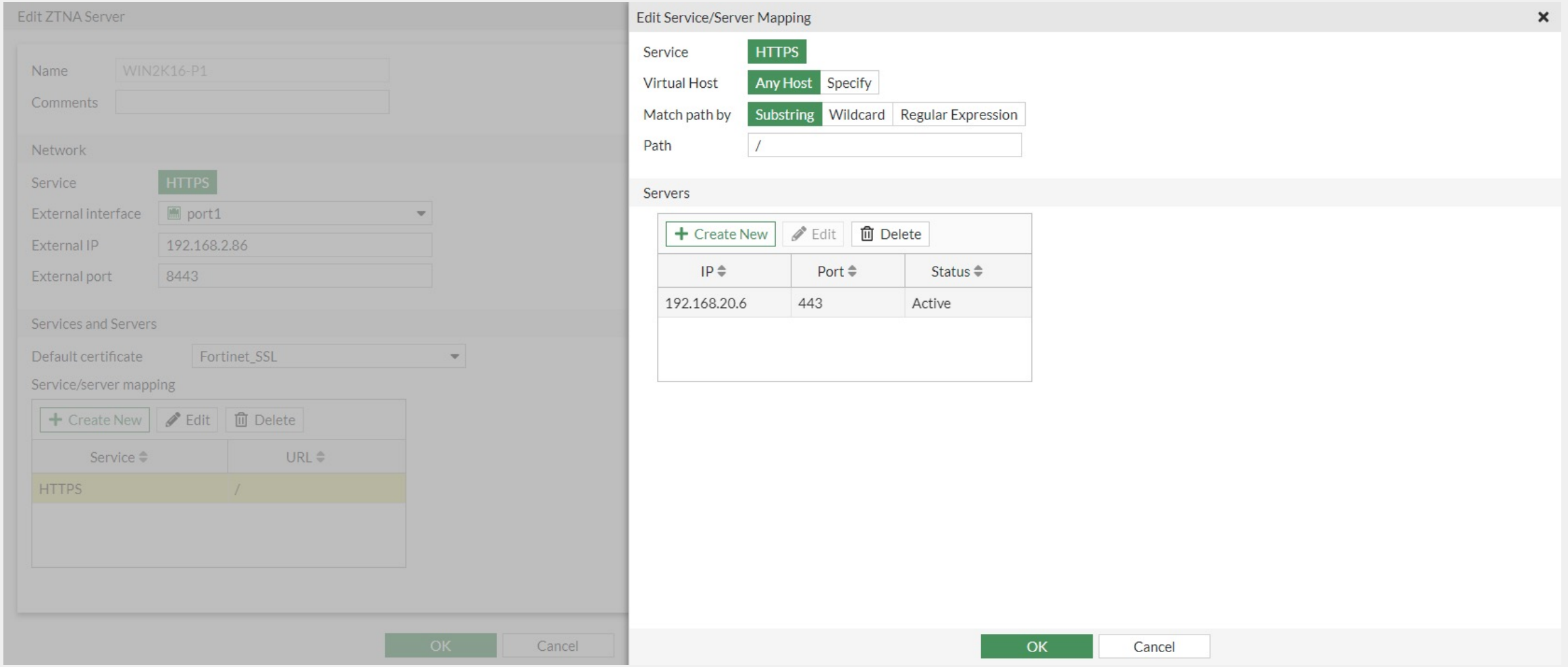
Zero Trust Network Access в FortiOS 7.0

Zero Trust tagging rule



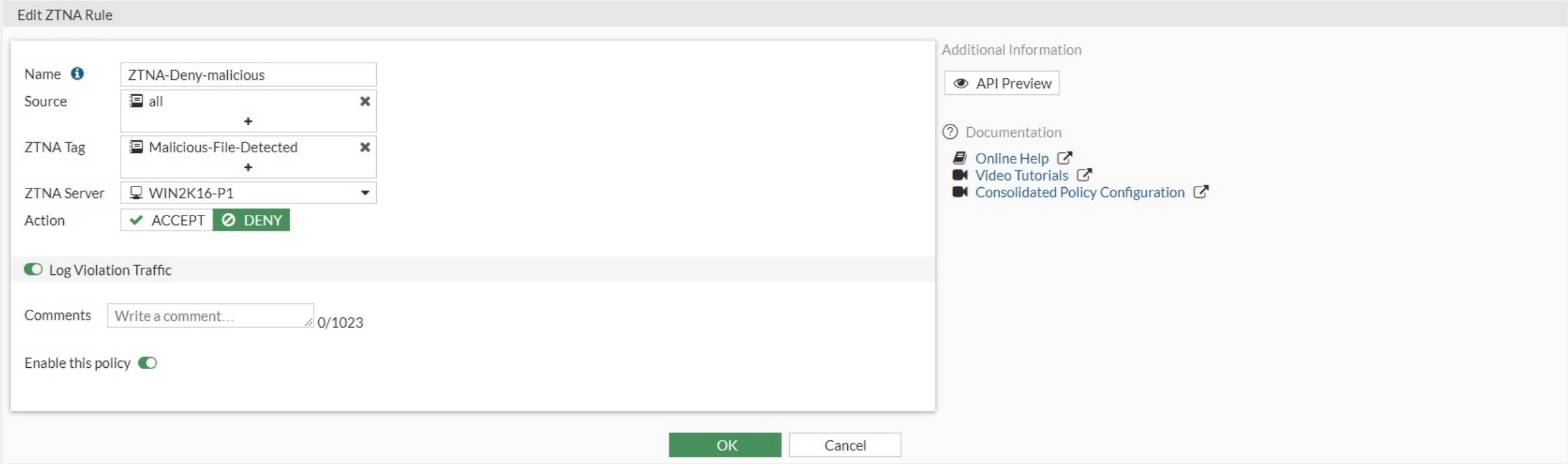
Zero Trust Network Access в FortiOS 7.0

HTTPS access proxy VIP



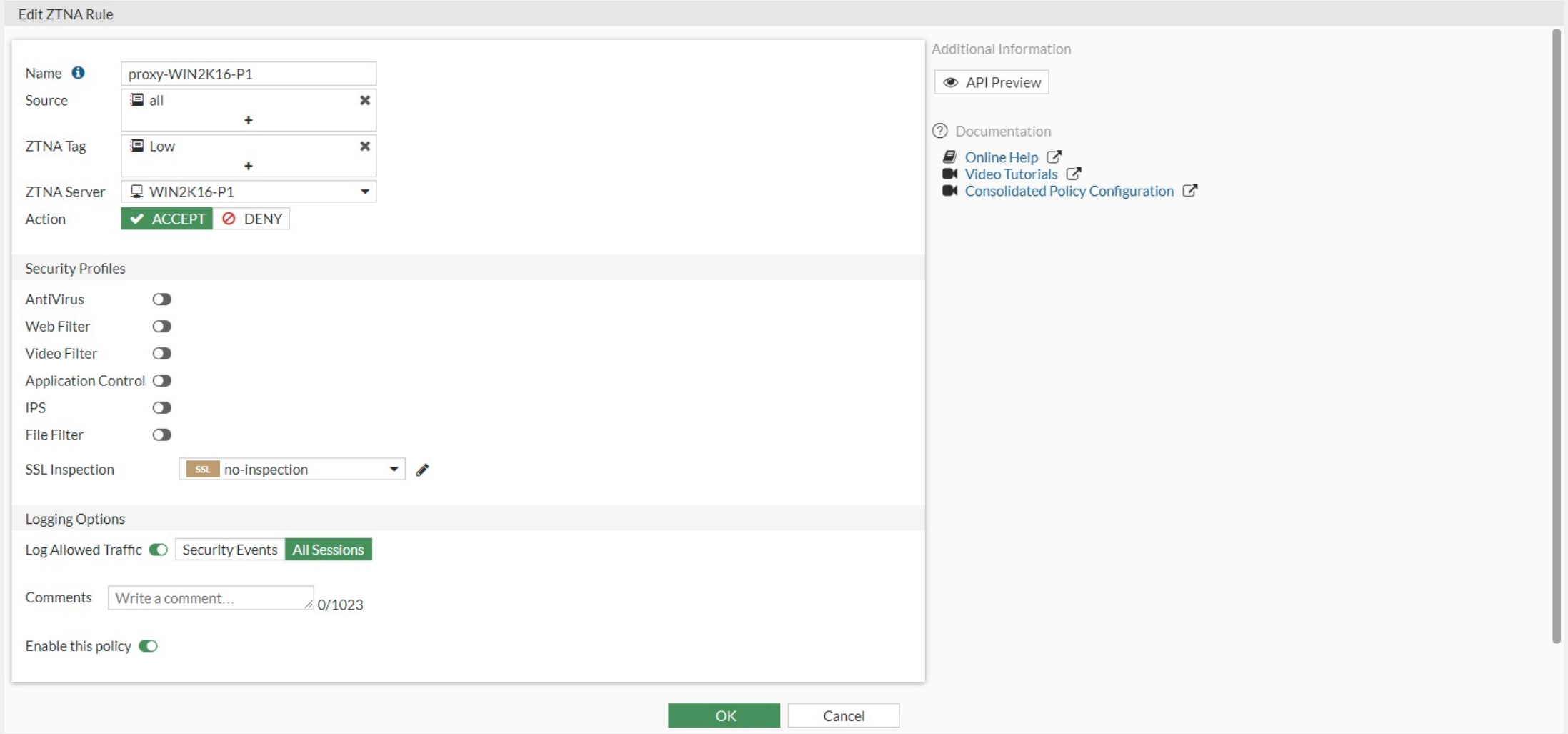
Zero Trust Network Access в FortiOS 7.0

ZTNA rules



Zero Trust Network Access в FortiOS 7.0

ZTNA HTTPS access proxy



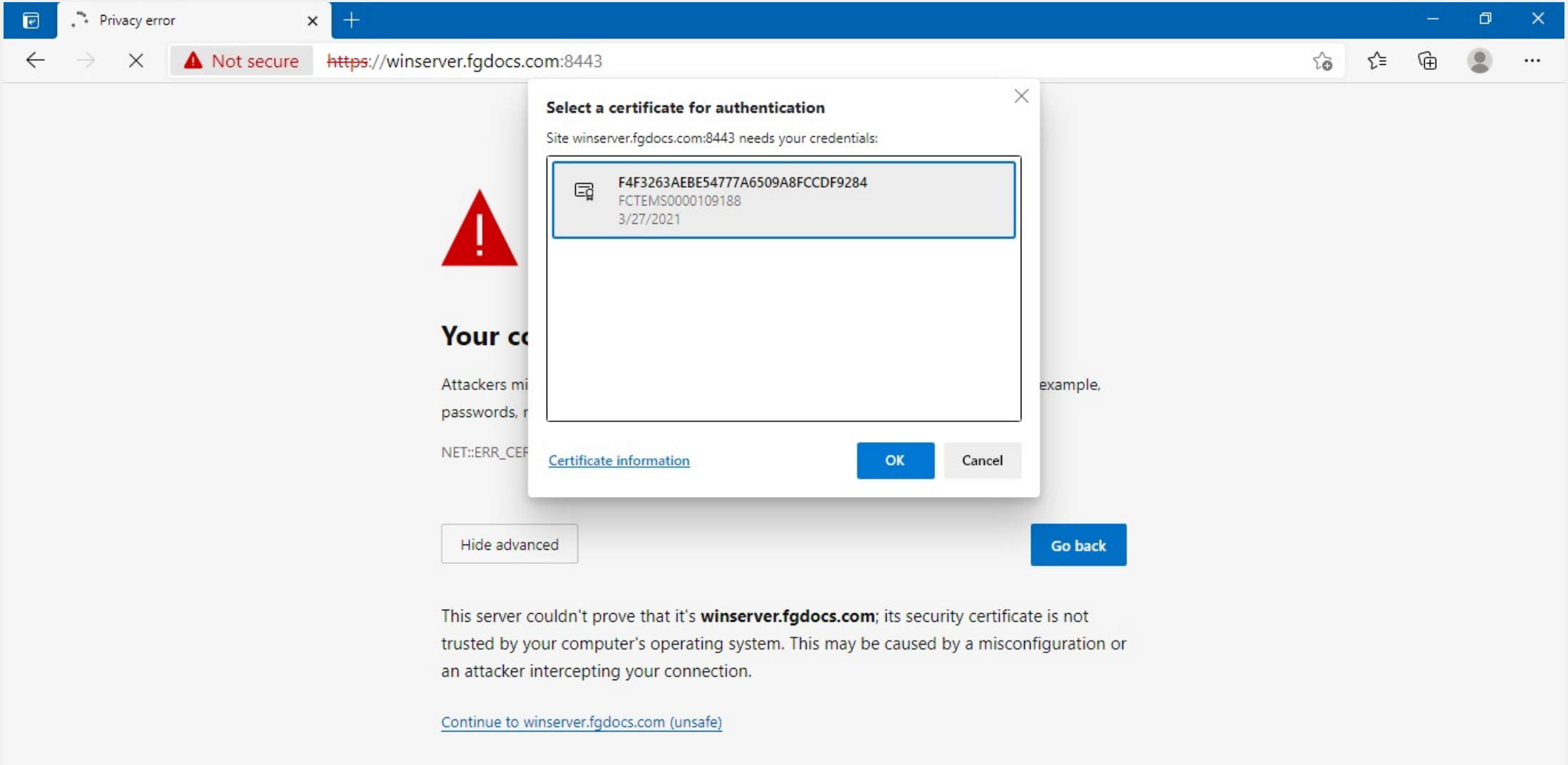
Zero Trust Network Access в FortiOS 7.0

Настройка Firewall policy (full ZTNA)

```
config firewall policy
    edit 24
        set name "ZTNA-P1"
        set srcintf "port1"
        set dstintf "any"
        set srcaddr "all"
        set dstaddr "WIN2K16-P1"
        set action accept
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set logtraffic all
        set nat enable
    next
end
```

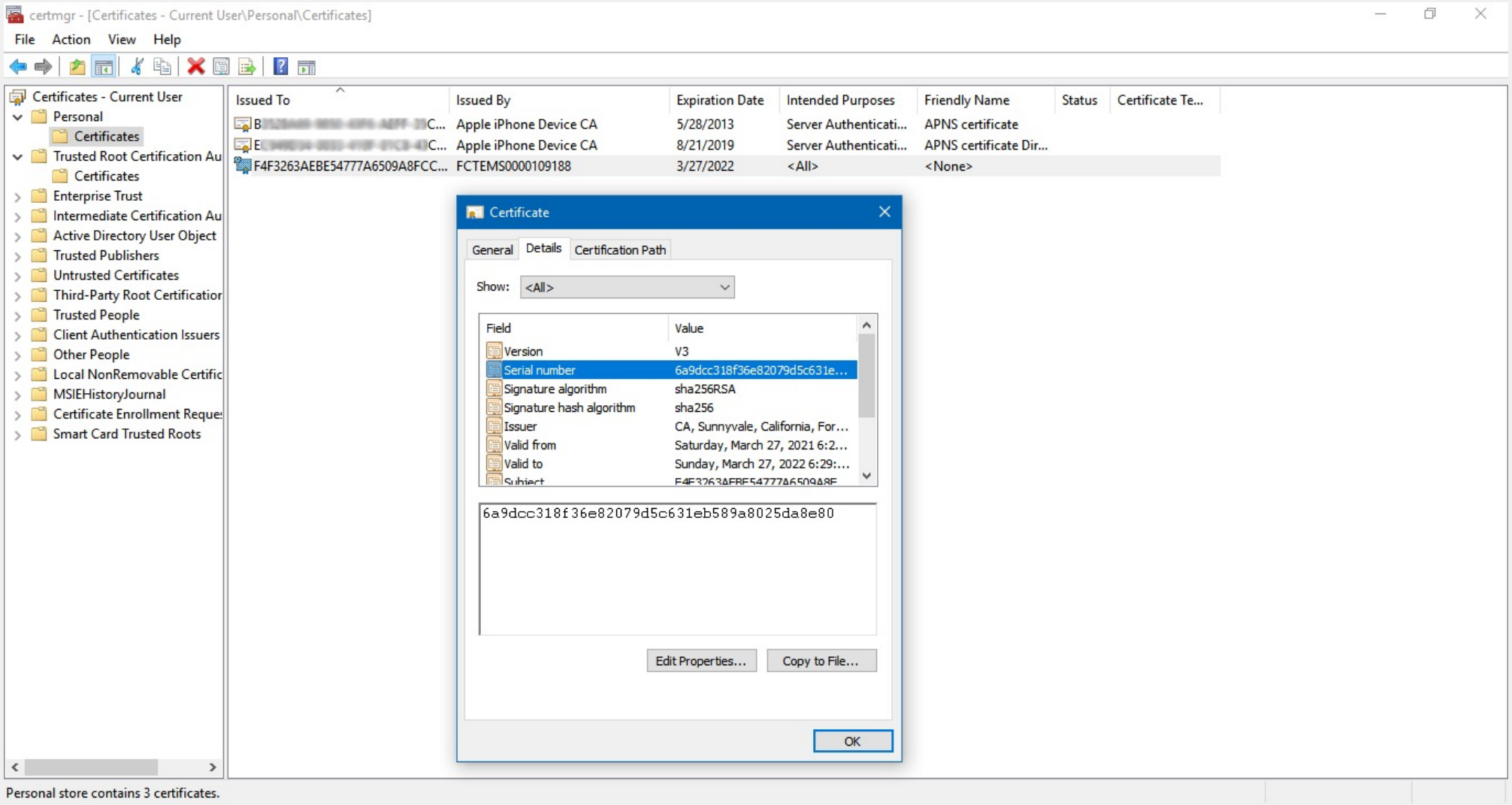
Zero Trust Network Access в FortiOS 7.0

ZTNA HTTPS access proxy: проверка доступа



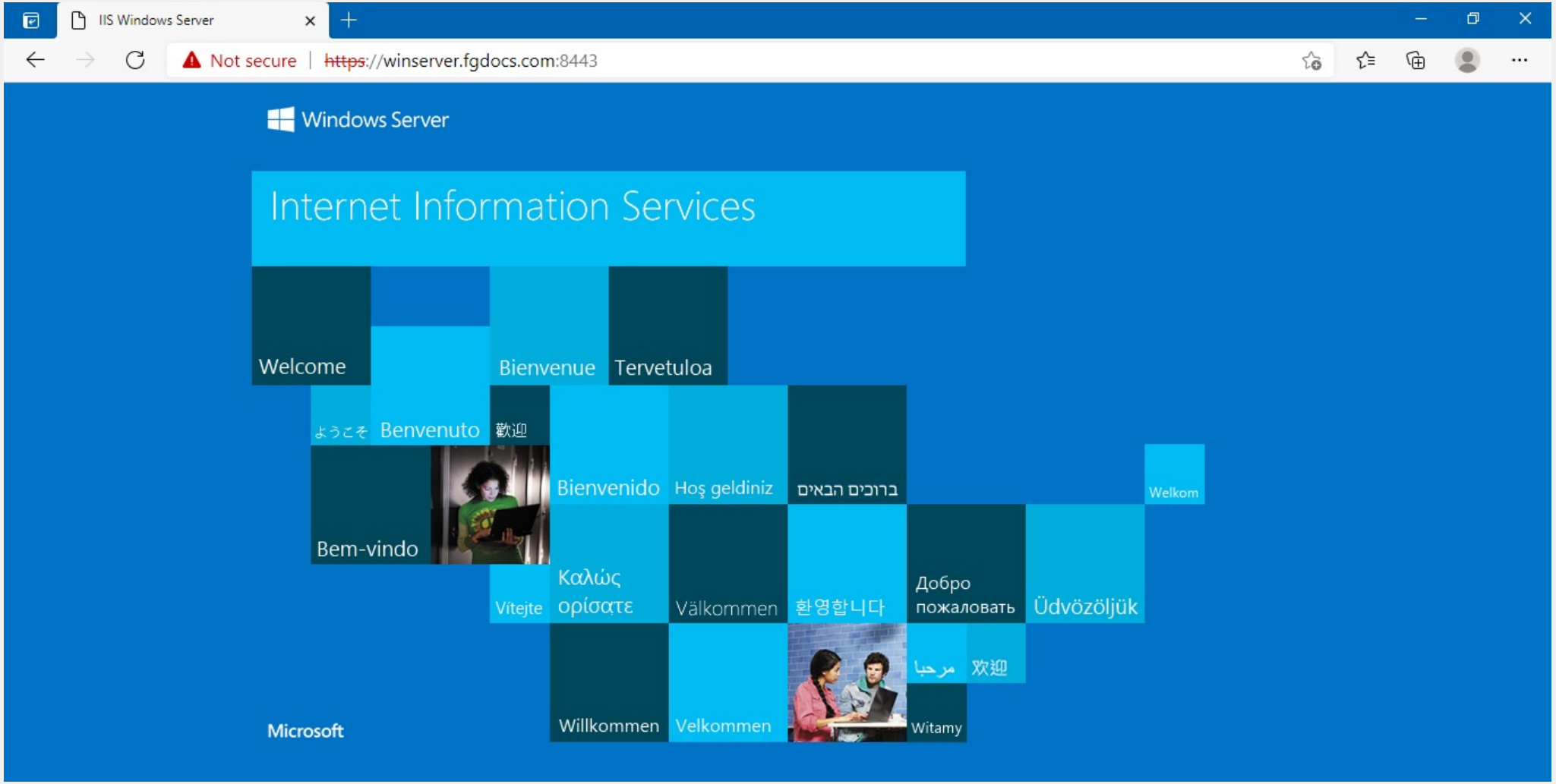
Zero Trust Network Access в FortiOS 7.0

ZTNA HTTPS access proxy



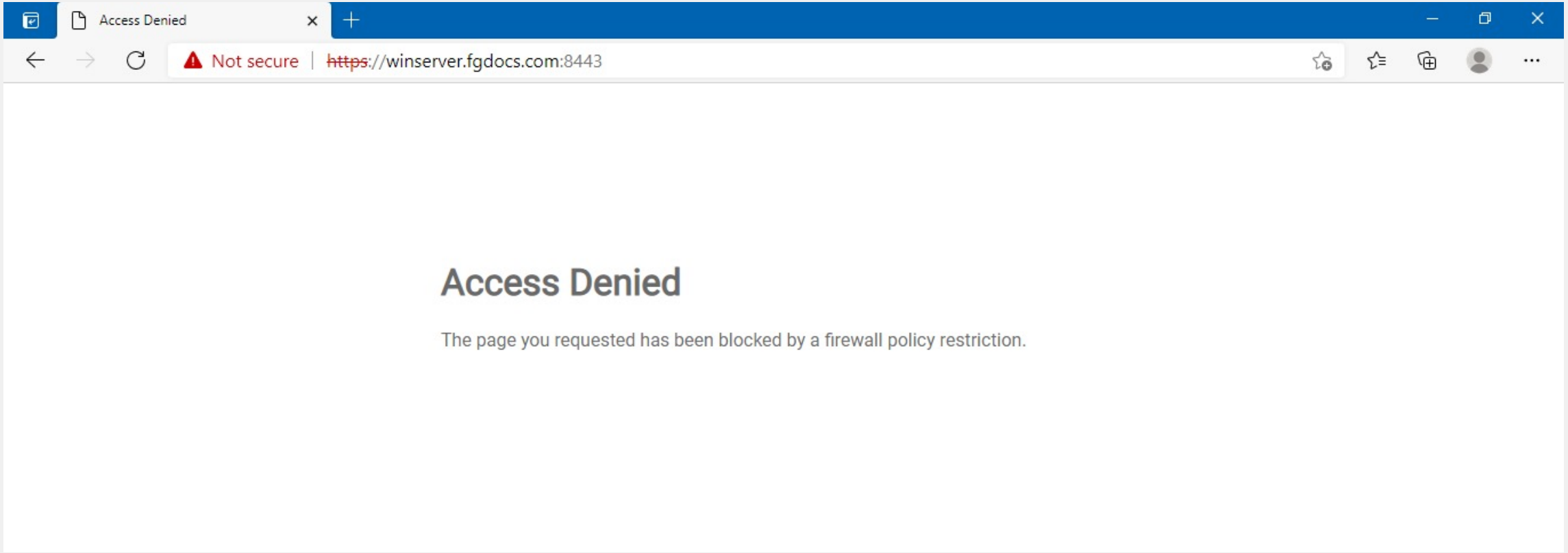
Zero Trust Network Access в FortiOS 7.0

ZTNA HTTPS access proxy



Zero Trust Network Access в FortiOS 7.0

ZTNA HTTPS access proxy




FORTINET