Простой и безопасный доступ к корпоративной сети из любой точки

Kaspersky ZTNA

kaspersky активируй будущее

25%

сотрудников в России сегодня полностью или частично работают из дома[1]

70,5%

работников используют собственную технику в своей работе[2]

до 25%

всех корпоративных утечек в 2025 году происходило с персональных устройств[3]

на 30%

увеличилось число кибератак, совершаемых через личные устройства сотрудников в России за первое полугодие 2025 года по сравнению с тем же периодом 2024 года[3]

Работа из дома и с личных устройств как новая норма

Распределенные модели занятости стали неотъемлемой частью операционной деятельности любой организации. Удаленный и гибридный форматы работы обусловили необходимость предоставления сотрудникам доступа к корпоративным системам из-за пределов защищённого офисного контура. Дополнительным фактором выступает политика BYOD (Bring Your Own Device), предполагающая использование личных устройств в рабочих целях. Такие тенденции, обеспечивая гибкость и повышая производительность, одновременно трансформируют ландшафт угроз информационной безопасности, увеличивая поверхность атаки.

Традиционная модель безопасности строилась на разделении доверенной внутренней и недоверенной внешней сети. Однако при подключении через публичные сети, из неконтролируемых точек и с личных устройств с негарантированным уровнем защиты концепция периметровой защиты утрачивает свою эффективность.

Использование классических VPN-подключений в данном контексте несет значительные риски:

- Увеличение поверхности атаки
- Уязвимость личных устройств
- Возможность «горизонтального перемещения» для атакующего
- Избыточный доступ к корпоративным ресурсам
- Сложность контроля и аудита
- Неудобство администрирования для IT-служб

1 Источник: Аналитический центр ВЦИОМ
2 Источник: РБК, исследование iRU
3 Источник: CISO Club, исследование Бастион

Kaspersky ZTNA

Zero Trust Network Access (ZTNA) —

это модель безопасности, предоставляющая доступ к корпоративным ресурсам на основе принципа «никому не доверяй, всегда проверяй».

Она обеспечивает безопасный, адаптивный и сегментированный доступ к приложениям и ресурсам.

Kaspersky ZTNA – решение для подключения сотрудников к корпоративным сервисам и приложениям, которое предоставляет доступ на основе строгой и непрерывной проверки каждого запроса.

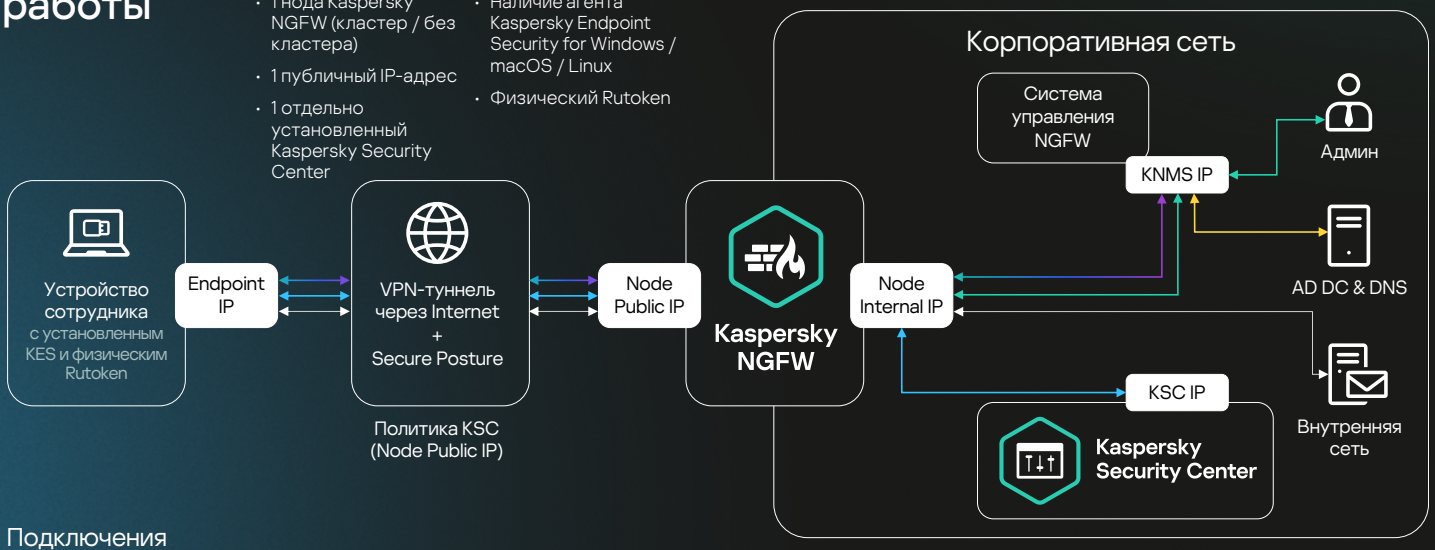
- Организация безопасного подключения сотрудников к корпоративной сети
- Предоставление доступа только к конкретному приложению или ресурсу
- Снижение рисков компрометации данных за счет непрерывной проверки пользователя и его устройства
- Ограничение возможности атак и снижение поверхности атаки
- Упрощение и повышение безопасности подключения подрядчиков и временных сотрудников
- Сокращение расходов на построение безопасной инфраструктуры
- Упрощение управления доступами для администраторов
- Соответствие регуляторным требованиям

Критерий	Классический VPN	ZTNA
Модель доступа	После подключения пользователь получает доступ к сегменту сети	Доступ предоставляется только к конкретному приложению или сервису
Уровень доверия	После аутентификации внутри периметра пользователю доверяют больше	По умолчанию нет доверия ни к чему, каждый запрос проверяется
Контроль действий	После подключения контроль действий пользователя внутри сети менее детализирован	Действия внутри системы постоянно анализируются и могут быть ограничены в реальном времени

Схема работы

Условия работы решения

- 1 нода Kaspersky NGFW (кластер / без кластера)
- 1 публичный IP-адрес
- 1 отдельно установленный Kaspersky Security Center
- Наличие агента Kaspersky Endpoint Security for Windows / macOS / Linux
- Физический Rutoken



Подключения

- RA VPN Connection
- KSC Connection
- ZTNA Connection
- Management Connection
- DC Connection

Основные компоненты решения

Технологическую основу решения составляют несколько ключевых продуктов «Лаборатории Касперского».

Наличие этих продуктов — обязательное условие для работы Kaspersky ZTNA.

Kaspersky Endpoint Security

Клиент

Kaspersky Endpoint Security (KES) проверяет устройство на соответствие политикам безопасности (Secure Posture) и предоставляет удаленный доступ в корпоративную сеть.

- Выполняет роль клиента при построении VPN-туннелей от устройства до корпоративной сети
- Проверяет устройство пользователя на вирусное ПО и соответствие политикам безопасности перед каждым подключением
- Является удобным интерфейсом для подключения

Kaspersky NGFW

Сервер

Kaspersky NGFW получает идентифицированный, контролируемый трафик и маршрутизирует его в сеть в соответствии с правилами безопасности.

- Выполняет роль сервера для подключения
- Идентифицирует подключаемых пользователей
- Подключает пользователя только к разрешенным приложениям и сервисам согласно групповым политикам

Описание лицензий

Решение Kaspersky ZTNA представлено в двух вариантах: Connect и Secure

Connect

Для простого удаленного подключения

Базовый защищенный удаленный доступ без проверок подключаемых устройств на соответствие политикам безопасности

Представляет собой технологию Remote Access VPN

Secure

Для более безопасного удаленного подключения

Защищенный удаленный доступ с проверкой устройств на наличие вредоносного ПО и соответствие политикам безопасности перед подключением к корпоративным сервисам и приложениям

Представляет собой технологию Zero Trust Network Access

Уровни и возможности Kaspersky ZTNA

Возможности		Connect	Secure
Подключение, управление и мониторинг	Организация удаленного подключения	●	●
	Раздельное туннелирование	●	●
	Многофакторная аутентификация (MFA) с сертификатом на Rutoken	●	●
	Ручная настройка нескольких серверов для подключения KES с приоритетами	●	●
	Автоматическое переподключение при сбое соединения и постоянное соединение (keep alive)	●	●
	Настройка политик сетевого доступа	●	●
	Интеграция с Active Directory / ALD Pro для настройки политик доступа по пользователям/группам	●	●
	Централизованная синхронизация настроек подключения[1]	●	●
	Автоматический выбор серверной ноды на основе качества подключения[2]		●
	Автоматическов определение нахождения в локальной сети (on-net / off-net)[2]		●
	Reverse Proxy ZTNA — доступ к ресурсам без установки туннеля		●
Проверка состояния безопасности	Настройка критериев Secure Posture для проверки устройства клиента перед подключением		●
	Формирование политик доступа NGFW на основе результатов Secure Posture		●
	Continuous check — постоянная проверка на соответствие Secure Posture		●
Безагентный доступ к приложениям[2]	Clientless ZTNA — веб-портал для доступа без клиента		●

1 При наличии развернутого Kaspersky Security Center
2 В будущих релизах

Условия функционирования

Необходимо наличие решения Kaspersky NGFW в качестве серверной части

Примечание

- Аппаратная платформа от Kaspersky NGFW может быть любой: от KX-100 до KX-3500
- Лицензия Kaspersky NGFW может быть любой: Standard или Advanced
- Уровень технической поддержки Kaspersky NGFW также может быть любым: Premium или Premium Plus

Kaspersky NGFW

Подробнее

Необходимо наличие физического средства аутентификации — Rutoken

Необходимо наличие агента Kaspersky Endpoint Security

Примечание

- Агент Kaspersky Endpoint Security может быть любой для одной из трёх ОС: Windows, macOS, Linux
- Агент Kaspersky Endpoint Security может быть в составе любого решения, например Kaspersky Endpoint Security для бизнеса / Kaspersky EDR / Kaspersky Symphony XDR и других
- Использование бесплатного агента Kaspersky Endpoint Security возможно только при лицензии Connect

Примеры решений с агентом KES

Kaspersky Endpoint Security для бизнеса
Расширенный

Подробнее

Kaspersky Endpoint Detection and Response
Expert

Подробнее

Kaspersky EDR для бизнеса
Оптимальный

Подробнее

Kaspersky Symphony Security

Подробнее

Необходимо наличие лицензии Kaspersky ZTNA

Лицензирование

1

Лицензирование Kaspersky ZTNA осуществляется по модели подписки на

1 год | 2 года | 3 года

с возможностью пролонгации на более выгодных условиях

2

Количество лицензий считается по количеству уникальных устройств, удаленно подключаемых к корпоративной сети в период действия подписки

Количество устройств может быть любым

3

Возможно комбинирование Connect и Secure лицензий в одной инфраструктуре

Пример спецификации

Компании необходимо организовать удаленный доступ к своим сервисам и приложениям для 500 сотрудников

Продукт	SKU Name	Кол-во	Объект подсчета
Аппаратная платформа Kaspersky NGFW	NGFW KX-3500	2	Устройство
Лицензия Kaspersky NGFW	Kaspersky NGFW KX-3500 Advanced	2	Устройство
Гарантия Kaspersky NGFW	Kaspersky Maintenance Service Agreement NGFW for KX-3500	2	Устройство
Лицензия Kaspersky ZTNA	Kaspersky ZTNA Secure	500	Устройство (endpoint)
У заказчика уже куплены 1000 Kaspersky Endpoint Security			
Kaspersky Endpoint Security для бизнеса	Kaspersky Endpoint Security for Business — Advanced	1000	Устройство (endpoint)

Почему Kaspersky ZTNA

Собственная архитектура и лидерские технологии

Упрощение эксплуатации решения за счет использования одного агента: антивирус + VPN

Снижение архитектурной сложности у заказчика, экономия бюджетов без компромисса по безопасности

Полностью российский продукт, соответствующий стратегии движения к импортонезависимости

Меньшие затраты на поддержку благодаря экосистемному подходу

Соответствие требованиям регулятора

Kaspersky ZTNA

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее