

Безопасность сети в условиях удаленного доступа

Дмитрий Хомутов

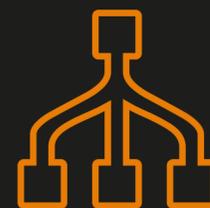
Директор по развитию



Находимся в Екатеринбурге. Работаем с 2005 года. Помогаем клиентам защититься от современных угроз безопасности, средствами удобного и «умного» межсетевого экрана нового поколения **Ideco UTM**.



Более 4 000 компаний
используют Ideco UTM



Более 40 000 человек
используют
VPN-подключения

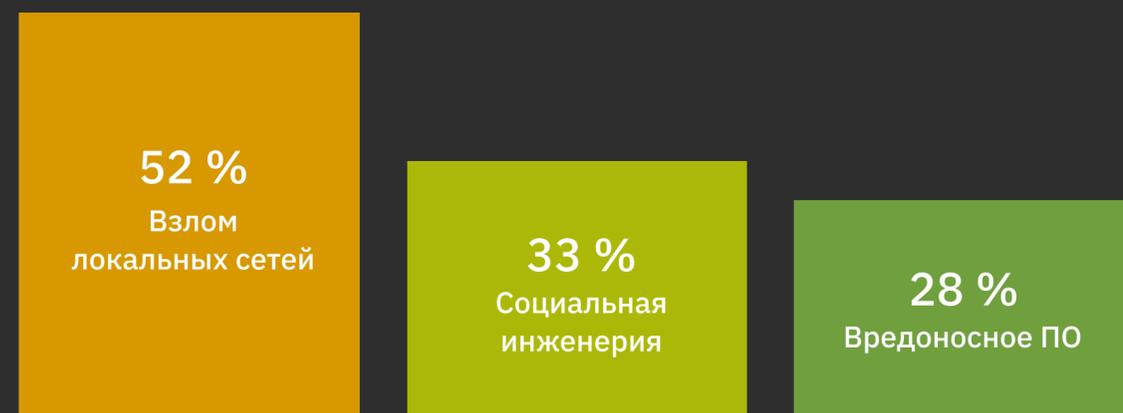


Год сами
работаем удаленно

По данным **Cybersecurity Ventures**:

68% крупных компаний считают, что риски в области кибербезопасности возрастают в связи с удаленным доступом сотрудников.

Кибер - атаки в 2020



Global Cybercrime Damage Costs:

- **\$6 Trillion USD a Year.** *
- **\$500 Billion a Month.**
- **\$115.4 Billion a Week.**
- **\$16.4 Billion a Day.**
- **\$684.9 Million an Hour.**
- **\$11.4 Million a Minute.**
- **\$190,000 a Second.**



ALL FIGURES ARE
PREDICTED BY 2021

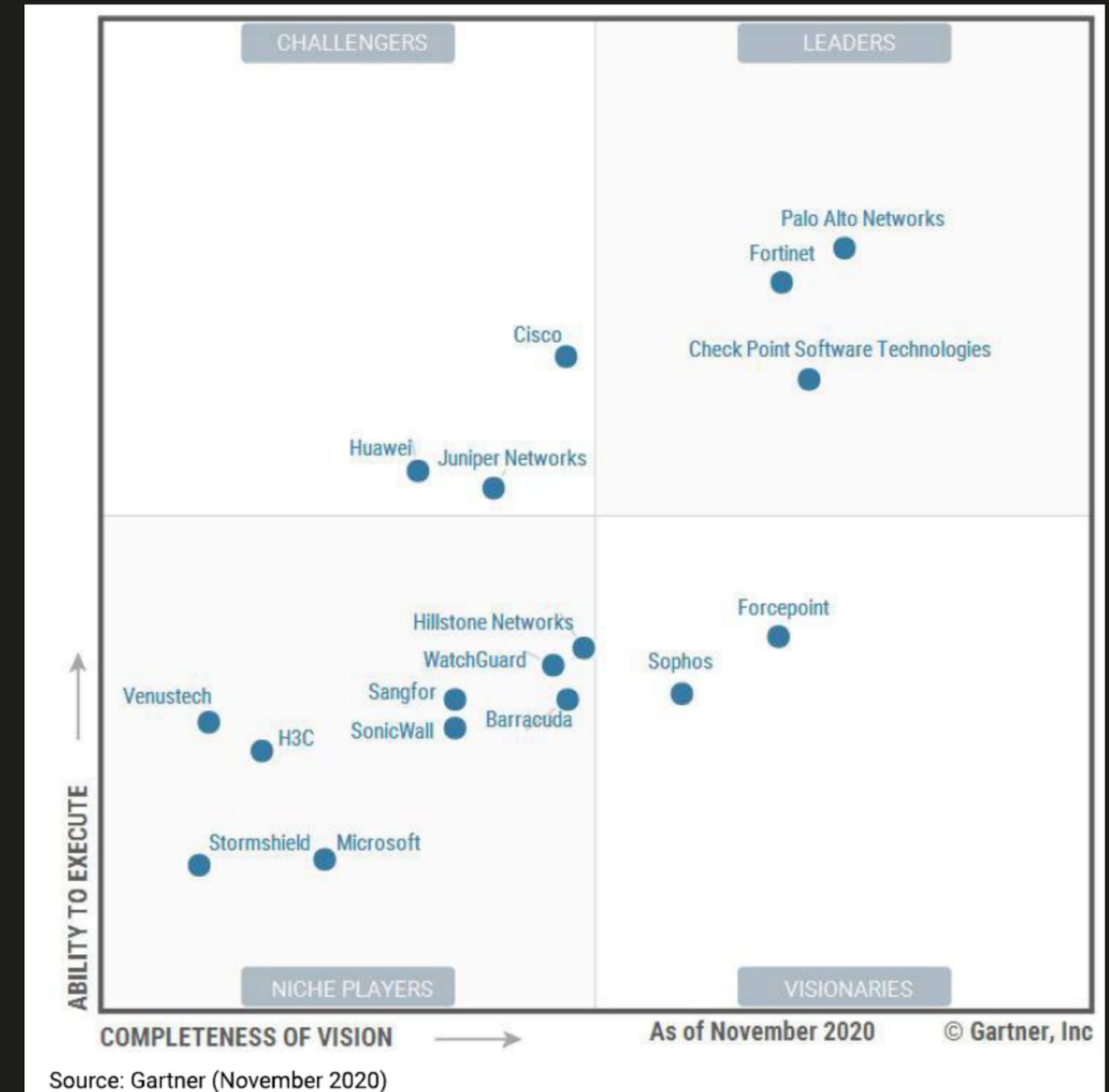
 **CYBERSECURITY
VENTURES**

* SOURCE: CYBERSECURITY VENTURES

Интересный факт: С 6 января 2021 года взломано более 60 000 серверов MS Exchange Server. Патчи безопасности появились 3 марта и развернуты только на 10% серверов.

Текущие решения: UTM/NGFW

- Требуют высокой квалификации специалистов для настройки и поддержки.
- В 95% случаев представляют собой программно-аппаратные комплексы (которые устаревают за 3-4 года).





Решаем проблемы безопасности за вас



Защита сразу «из коробки»



Легкая интеграция



Понятные настройки



Техподдержка on-line



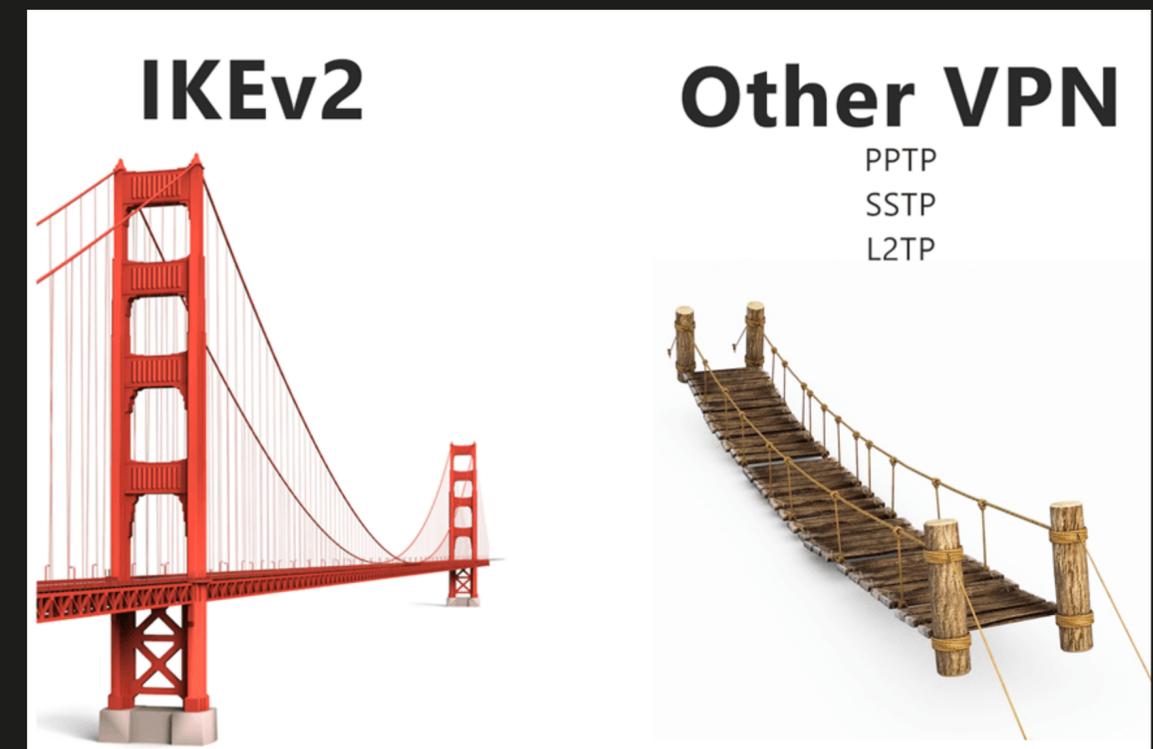
Легкая миграция



Быстрое развертывание

Протокол должен обеспечивать:

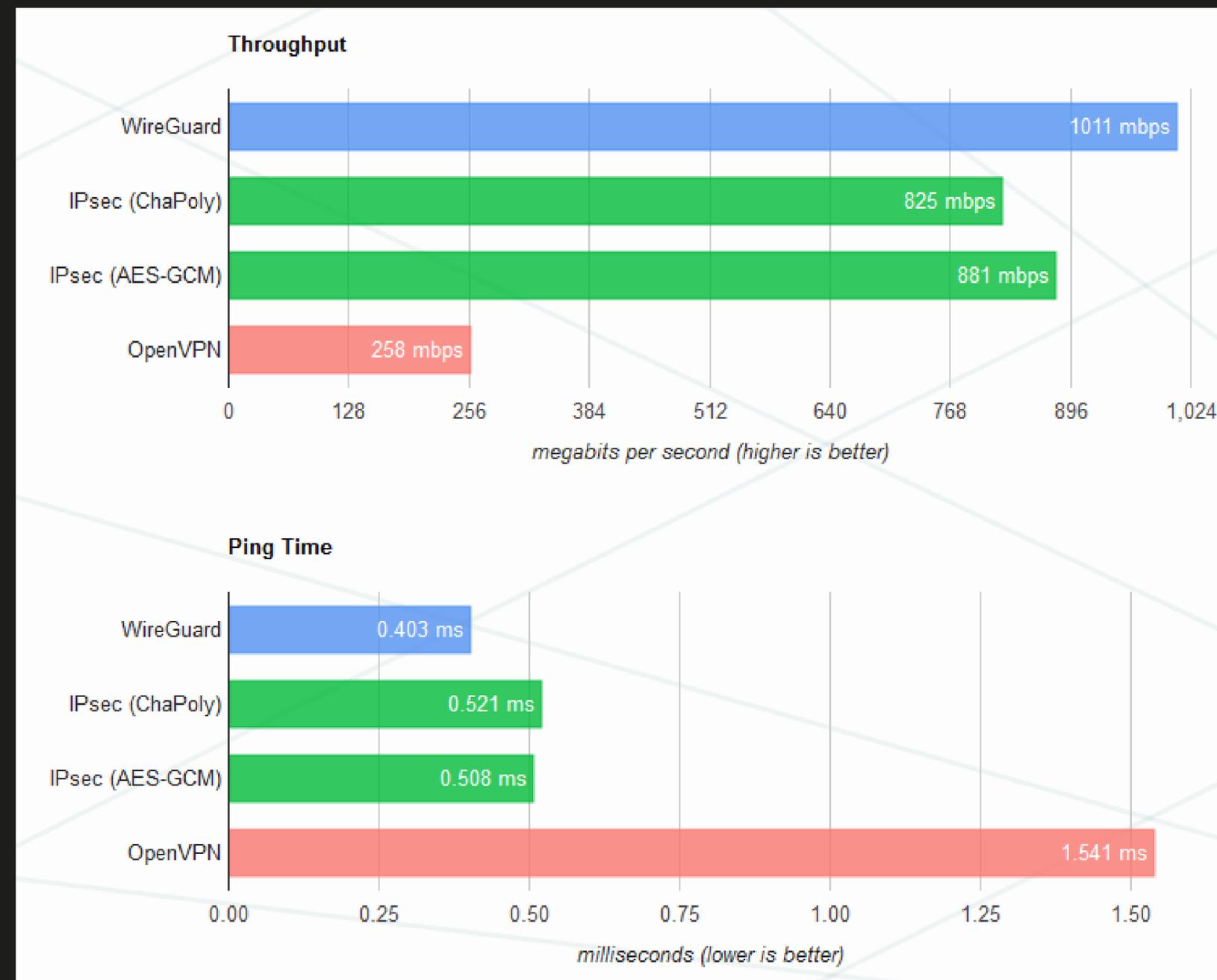
- стабильное соединение
- подключение через любого провайдера
- стабильную и высокую скорость
- поддержку популярных ОС



Как выбрать VPN-протокол

IKEV2/IPSec

- + быстрый
- + поддержка современных ОС
- + стабильное соединение
- + мощная криптография
- для Android нужно дополнительное ПО
- не поддерживаются устаревшие ОС

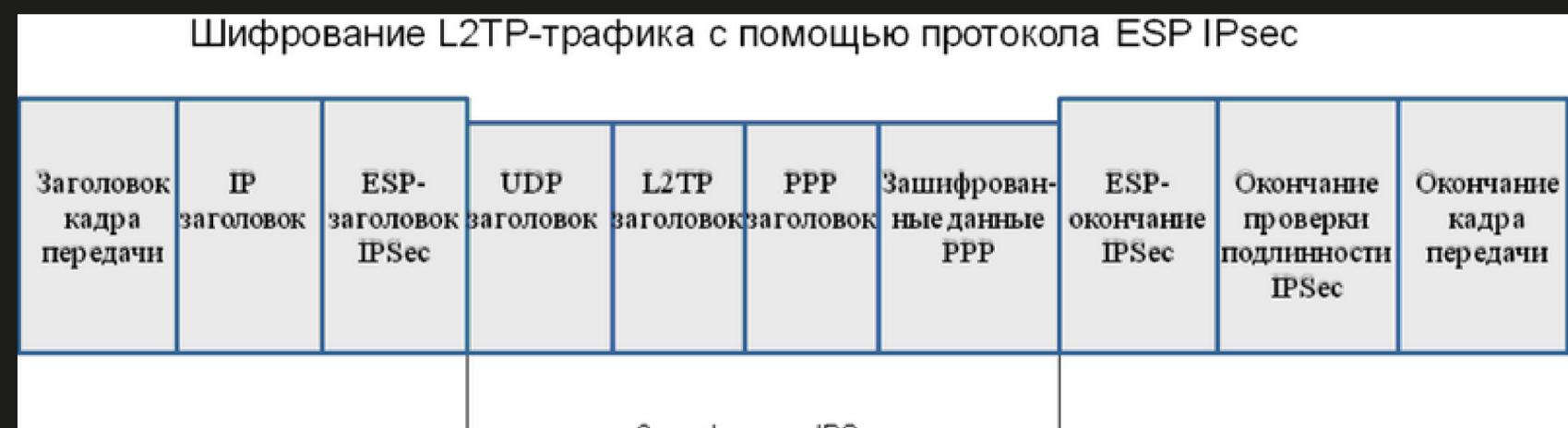


Как выбрать VPN-протокол

L2TP/IPSec

+ поддерживается старыми и новыми ОС

- двойная инкапсуляция трафика
- проблемы с прохождением через некоторых провайдеров
- нельзя подключать несколько устройств из-за NAT



Как выбрать VPN-протокол

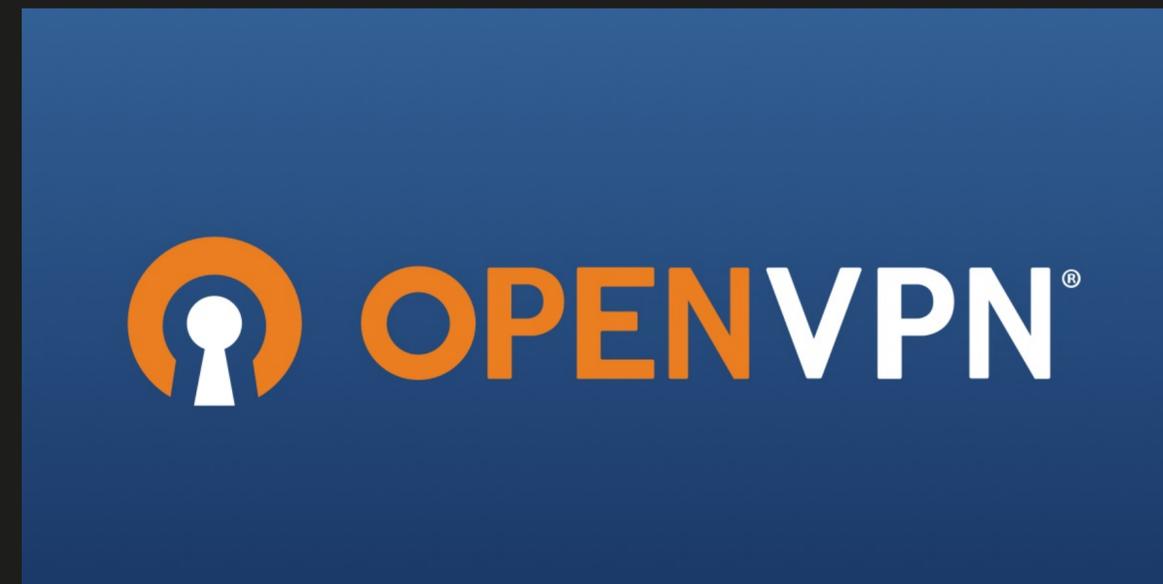
SSTP

- + стабильный (TCP)
- + отлично проходит через провайдеров
- поддерживает только Windows
- большие задержки (инкапсуляция UDP через TCP)
- двойная инкапсуляция (PPP)

8 бит Версия (текущая 1.0)	7 бит Зарезервированы	1 бит Флаг C	4 бита Зарезервированы	12 бит Длина пакета	Данные (PPP)
----------------------------------	--------------------------	-----------------	---------------------------	------------------------	--------------

Open VPN

- + стабильный (TCP/UDP)
- + есть клиенты под все ОС и многие устройства
- + бесплатный
- + открытый исходный код
- требует установки клиентского ПО
- требуется настройка
- медленный из-за реализации в userspace



Маршрутизация в VPN

Настройте маршрутизацию только нужного трафика у пользователей, если у вас ограниченный интернет-канал (чтобы они выходили в интернет не через центральный офис).

Авторизация IKEv2/IPSec

Домен
gw-dev.ideco.ru

Маршруты
10.0.0.0/8

Маршруты
172.16.0.0/12

Будут переданы для VPN-подключения в ОС Windows

[Добавить маршрут](#)

[PowerShell - скрипт для настройки подключений](#)

Ethernet: свойства

Сеть Доступ

Подключение через:
Realtek Gaming GbE Family Controller

Отмеченные компоненты используются этим подключением:

- Планировщик пакетов QoS
- IP версии 4 (TCP/IPv4)
- Протокол мультиплексора сетевого адаптера (Майкрософт)
- Драйвер протокола LLDP (Майкрософт)
- IP версии 6 (TCP/IPv6)
- Отвечающее устройство обнаружения топологии канального уровня
- Ответчик обнаружения топологии канального уровня

Установить... Удалить Свойства

Описание
Протокол TCP/IP. Стандартный протокол глобальных сетей, обеспечивающий связь между различными взаимодействующими сетями.

OK Отмена

Свойства: IP версии 4 (TCP/IPv4)

Общие Альтернативная конфигурация

Параметры IP можно назначать автоматически, если сеть поддерживает эту возможность. В противном случае узнайте параметры IP у сетевого администратора.

Получить IP-адрес автоматически

Использовать следующий IP-адрес:

IP-адрес:

Маска подсети:

Основной шлюз:

Получить адрес DNS-сервера автоматически

Использовать следующие адреса DNS-серверов:

Предпочитаемый DNS-сервер:

Альтернативный DNS-сервер:

Подтвердить параметры при выходе [Дополнительно...](#)

OK Отмена

Дополнительные параметры TCP/IP

Параметры IP DNS WINS

Этот флажок используется только при одновременном подключении к локальной сети и к сети удаленного доступа. Если флажок установлен, данные, которые не удается передать через локальную сеть, направляются в сеть удаленного доступа.

Использовать основной шлюз в удаленной сети

Отключить добавление маршрута, основанное на классе

Автоматическое назначение метрики

Метрика интерфейса:

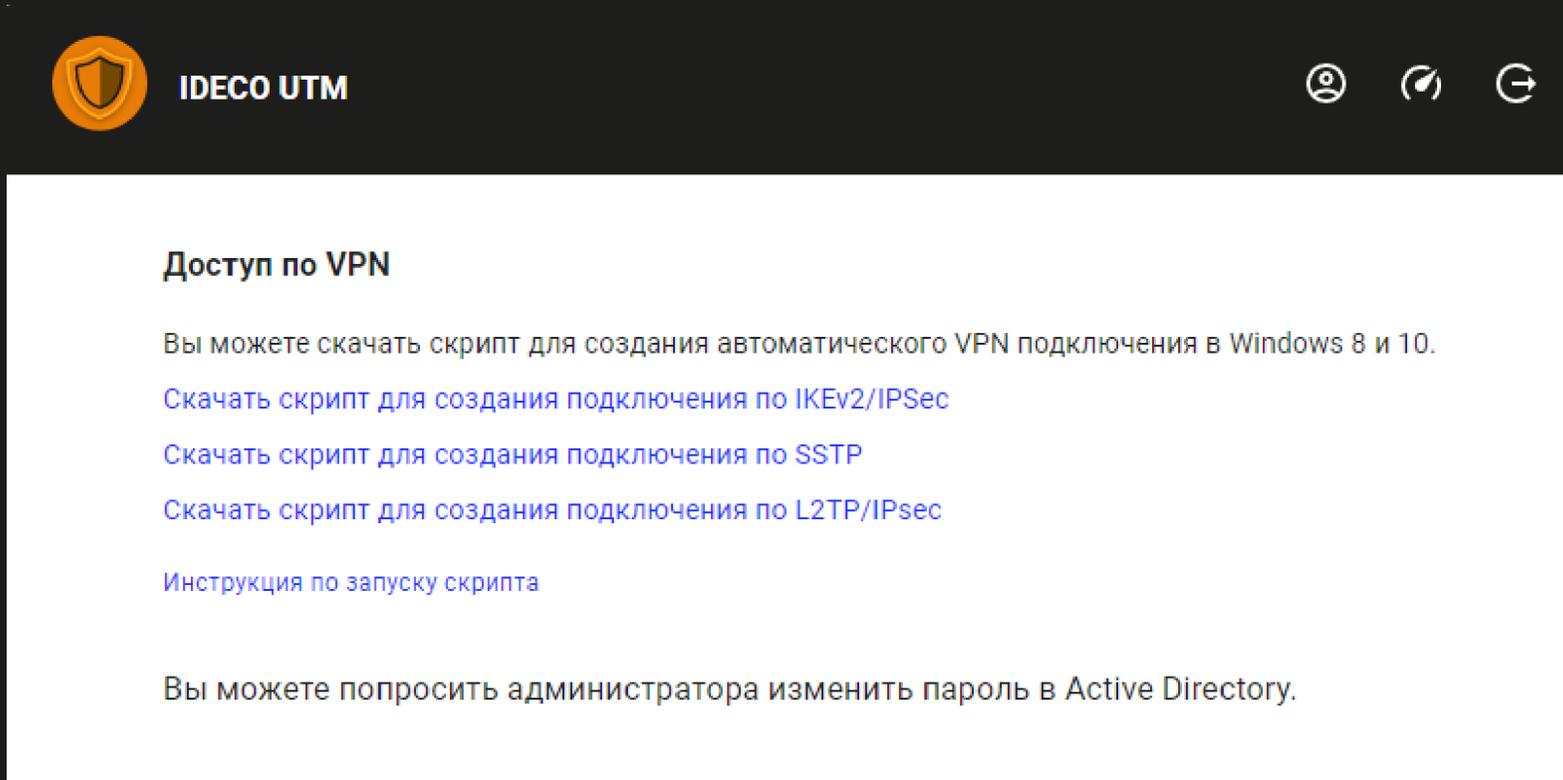
OK Отмена

Авторизация удаленных пользователей

- Используйте единую систему управления учетными данными
- Настройте защиту сервера от брутфорс-атак
- Защититесь от атак по GeoIP и IP Reputation



- Без установки стороннего ПО
- Без передачи ключей или реквизитов доступа
- Без сложных инструкций для пользователей



The screenshot shows a web interface for IDECO UTM. At the top left is the IDECO UTM logo, which consists of a shield icon and the text 'IDECO UTM'. To the right of the logo are three small icons: a user profile, a refresh symbol, and a back arrow. Below the header is a white content area with the following text:

Доступ по VPN

Вы можете скачать скрипт для создания автоматического VPN подключения в Windows 8 и 10.

[Скачать скрипт для создания подключения по IKEv2/IPSec](#)

[Скачать скрипт для создания подключения по SSTP](#)

[Скачать скрипт для создания подключения по L2TP/IPsec](#)

[Инструкция по запуску скрипта](#)

Вы можете попросить администратора изменить пароль в Active Directory.

Защита VPN и публикация ресурсов



DPI

Фильтрация на 7 уровне
модели OSI

15 млн

доменов и IP-адресов C&C
в нашем BlockList

500 млн

URL в обновляемой базе данных



Контентная фильтрация



Блокировка анонимайзеров



Предотвращение вторжений



Контроль приложений (DPI)



Публикация ресурсов



Антивирусная проверка

«Шай-тек» (shy-tech) «скромные технологии» что это такое?

IDECO UTM
9.7 сборка 7

- Пользователи
- Учётные записи
- Авторизация
- Active Directory
- Обнаружение устройств
- Мониторинг
- Правила трафика
- Сервисы
 - Сетевые интерфейсы
 - Балансировка и резервирование
 - Маршрутизация
 - Прокси
 - Обратный прокси
 - DNS
 - DHCP-сервер
 - NTP-сервер
 - IPsec
 - Сертификаты
- Отчёты
- Управление сервером
- Почтовый релей

Авторизация

Работает

Основное **VPN-авторизация** Фиксированные IP-адреса VPN

Сеть для VPN-подключений
10.125.0.0/24

Авторизация PPTP

Авторизация PPPoE

Авторизация IKEv2/IPSec

Домен
domain.com

Маршруты
10.0.0.0/8 X

Маршруты
172.16.0.0/12 X

Будут переданы для VPN-подключения в ОС Windows

Добавить маршрут

[PowerShell - скрипт для настройки подключений](#)

Авторизация SSTP

Домен
domain.com

Порт
4443

[PowerShell - скрипт для настройки подключений](#)

Авторизация L2TP/IPSec

PSK
.....

[PowerShell - скрипт для настройки подключений](#)

Сохранить



Преимущества Ideco UTM



Программное решение



Бесплатное тестирование



Техническая поддержка



Быстрое развитие продукта



**Обратная связь без
посредников**



Гибкая ценовая политика



СПАСИБО ЗА ВНИМАНИЕ

d.homutov@ideco.ru

ideco.ru