IDECO UTM. СРАВНЕНИЕ С MIKROTIK

Mikrotīkls Ltd (торговая марка MikroTik) — латвийский производитель компьютерного сетевого оборудования. MikroTik разрабатывает и продает проводные и беспроводные маршрутизаторы, операционные системы к ним и сопутствующее оборудование.
Подобные (но предназначенные, как правило для SOHO-сегмента) роутеры производят также такие компании, как D-link, TP-link, Asus, Zuxell.

Шлюз безопасности Ideco UTM представляет из себя современное UTM-решение, предназначенное для защиты сетевого периметра. Помимо функций маршрутизации и межсетевого экранирования, он обладает также модулями глубокого анализа трафика: системой предотвращения вторжений, контролем приложений (DPI), контент-фильтром, межсетевым экраном веб-приложений, фильтрации почтового трафика, антивирусной проверки трафика – предназначенными для защиты от современных угроз безопасности.

Интерфейс управления сервером

Функциональность	Ideco UTM	RouterOS
Консольный интерфейс	настройка сервисов, диагностика и восстановление, полный доступ по SSH	Полный доступ по SSH
Веб-интерфейс	+ значительно более простой	+ позволяет осуществлять очень тонкую настройку

Безопасность

Функциональность	Ideco UTM	RouterOS
Система предотвращения вторжений (IPS)	+ блокирование активности троянских и вирусных программ, атак, вредоносного трафика и многое др.	— отсутствие модуля может привести к массовым атакам на устройства
Межсетевой экран	+	+

Защита веб-приложений (Web Application Firewall)	+	—
Защита от подбора паролей (brute force)	+ для всех служб с аутентификацией по паролю	—
Антивирусная проверка веб и почтового трафика	антивирус Касперского, ClamAV	—
Проверка почтового трафика на спам	антиспам Касперского, greylisting, DNSBL, почтовые фильтры	—
Авторизация пользователей	+ разрешен только авторизованный трафик	—

Сетевая функциональность

Функциональность	Ideco UTM	RouterOS
Интеграция с Active Directory	Импорт пользователей (в том числе из нескольких доменов). Авторизация по Kerberos/NTLM и логам безопасности домена.	—
VPN IPsec	+	+
VPN OpenVPN	+	+
Резервирование каналов	+	+
Ограничение полосы пропускания	+	+
Публикация ресурсов	Обратный прокси (HTTP/HTTPS), публикация Outlook Web Access, DNAT, почтовый релей	DNAT
Кэширование веб-трафика и DNS-запросов	+	—

Контентная фильтрация

Функциональность	Ideco UTM	RouterOS
Количество категорий в контент-фильтре	144	—
Количество URL в БД контентного-фильтра	более 500 млн.	возможности по фильтрации сильно ограничены
Фильтрация HTTPS	+ с подменой и без подмены сертификата	—
Блокировка файлов по MIME-типам и расширениям	+ предустановленные группы ресурсов (исполняемые, аудио, видео и др.)	—

Дополнительные службы

Функциональность	Ideco UTM	RouterOS
DNS-сервер	+	+
DHCP	+ интегрирован с модулем пользователей	+
Почтовый сервер	+ настроен и интегрирован с др. службами	—

Разное

	Ideco UTM	Бесплатный дистрибутив
Обновление	Автоматическое обновление системы, компонентов и баз данных, автоматическая миграция настроек со старых версий.	Обновление необходимо осуществлять вручную.
Техническая поддержка	Техническая поддержка пользователей, помощь в настройках и исправление ошибок осуществляется	Осуществляется самостоятельно

	компанией «Айдеко» (в т.ч. с подключением к серверам клиентов).	
Документация	Вся документация регулярно обновляется и представлена на русском языке.	Документация на английском языке.

ПРЕИМУЩЕСТВА IDECO UTM НАД МАРШРУТИЗАТОРАМИ И МЕЖСЕТЕВЫМИ ЭКРАНАМИ

Наличие роутера с развитой функциональностью по маршрутизации трафика, не исключает необходимости в решении по фильтрации трафика и продвинутой защиты сетевого периметра (просто межсетевого экрана и NAT уже недостаточно).
Ideco UTM может использоваться совместно с любым роутером, образуя мощный эшелон защиты от вредоносного трафика.

Используя шлюз безопасности Ideco UTM вы получаете:

- Актуальные базы сигнатур **системы предотвращения вторжений**, включая правила блокирования командных центров ботнетов (C&C), анонимайзеров, вирусной активности, GeoIP, IP Reputation и множество других.
- Мощную базу **системы контентной фильтрации** – 144 категории трафика, включая более чем 500 млн. URL, оптимизированные для российского интернет-сегмента. Блокирование фишинговых, зараженных и распространяющих вирусы сайтов существенно повышает защиту конечных устройств от интернет-угроз.
- **Отчетность** по использованию интернет-ресурсов пользователями.
- **Контроль приложений** – с возможность запретить BiTorrent, Skype, TOR, TeamView и трафик других приложений на 7-ом уровне модели OSI.
- **Модули антивирусной проверки -** для веб и почтового трафика.
- **Проверка почтового трафика –** на спам, мошеннические и фишинговые письма.
- **Обязательная авторизация устройств –** для применения правил фильтрации, хранения статистики и расследования инцидентов безопасности.
- **Техническую поддержку** и документацию к продукту на русском языке.
- **Быстрые обновления** – новую функциональность, устранение ошибок и потенциальных уязвимостей. 5-6 мажорных релизов Ideco UTM в год.

Уязвимости маршрутизаторов Mikrotik часто приводят к массированным заражениям:
https://xakep.ru/2018/09/05/mikrotik-still-under-attack/
https://xakep.ru/2018/08/03/mikrotik-under-attack/
https://ideco.ru/company/blog/vpnfilter