VPN-и, поддържани от MikroTik - сравнение

MikroTik Net Camp 2017

Трявна

Петър Димитров

За мен:

- Име: Петър Димитров
- Опит в областта на компютърните мрежи: от 2002 г.
- Опит с MikroTik: от 2005 г.
- MikroTik Trainer: от 2013 г.
- Предлагани MikroTik обучения:

MTCNA, MTCWE, MTCRE, MTCTCE, MTCUME, MTCIPv6E, MTCINE

Virtual Private Networks

- Тунелите са начин за разширяване на вашата частна мрежа чрез осигуряване на отдалечен достъп до локални ресурси.
- Най-често за преносна среда се използва Интернет.
- Обикновено от съображение за сигурност се използва криптиране.

Кой е правилния VPN?

- Целта на тази презентация е да разгледа различните аспекти на поддържаните в RouterOS VPN-и, за да помогне при избора на подходящ VPN за различни цели.
- Ще разгледаме реални тестове за производителност на различни тунели при различни устройства и ще сравним резултатите.

Видове VPN-и

VPN-ите могат да се класифицират по различни начини:

- От гледна точка на приложението:
  - За отдалечен достъп на потребители (road warrior, remote access VPN, client-based VPN).
  - За свързване на отдалечени мрежи (site-to-site VPN, network-based VPN).

Видове VPN-и

- От гледна точка на осигуряваните мрежови услуги:
  - VPN-и, осигуряващи Layer 2 свързаност.
  - VPN-и, осигуряващи Layer 3 свързаност.
- Също може да се разглеждат различни видове VPN-и на база транспорт, протоколи, автентикация, криптиране, наличие на тунелен интерфейс и други.

Поддържани VPN-и

- Към момента в RouterOS има поддръжка на:
  - Клиент-сървър базираните PPTP, L2TP, SSTP, OVPN
  - Тунели EoIP, IPIP, GRE
  - IPsec
  - PPPoE, чието приложение най-често е предоставяне на услуга от ISP, използва Ethernet за транспорт и не е предмет на тази презентация.

PPTP

- Използва TCP порт 1723 и GRE, осигурява тунелен интерфейс.
- Автентикация с потребител и парола, може да осигури MPPE128 криптиране.
- Пренася PPP фреймове, осигурява Layer 3 свързаност, с BCP може да осигури Layer 2 свързаност.
- По-често се използва за отдалечен достъп на потребители, отколкото за свързване на отдалечени мрежи.
- Лесен за конфигуриране, ниско ниво на сигурност. Нужда от NAT helper-и.

L2TP

- Използва UDP порт 1701, осигурява тунелен интерфейс.
- Автентикация с потребител и парола, може да осигури MPPE128 криптиране.
- Пренася PPP фреймове, осигурява Layer 3 свързаност, с BCP може да осигури Layer 2 свързаност.
- Често се използва в комбинация с IPsec за отдалечен достъп на потребители, по-рядко за свързване на отдалечени мрежи.
- Без IPsec има ниско ниво на сигурност, но комбинацията с IPsec е стандартна и имплементирана в повечето клиенти.

SSTP

- Използва TCP порт 443, осигурява тунелен интерфейс.
- Автентикация с потребител и парола + сертификат, осигурява AES256 криптиране.
- Пренася PPP фреймове, осигурява Layer 3 свързаност, с BCP може да осигури Layer 2 свързаност.
- Често се използва за свързване на отдалечени мрежи между MikroTik рутери, понякога за отдалечен достъп на Windows потребители.
- Много лесно минава през защитни стени (firewall), осигурява високо ниво на сигурност.

OVPN

- Използва към момента TCP (в бъдеще ще има поддръжка и на UDP), порта е конфигурируем (по подразбиране 1194), осигурява тунелен интерфейс.
- Автентикация с потребител и парола + сертификат, осигурява различни видове криптиране (включително AES256).
- Режим ethernet (TAP) осигурява Layer 2 свързаност, режим ip (TUN) осигурява Layer 3 свързаност.
- Използва се както за отдалечен достъп на потребители, така и за свързване на отдалечени мрежи.
- Труден за конфигуриране, осигурява високо ниво на сигурност.

EoIP

- Използва TCP и GRE, осигурява тунелен интерфейс.
- Самостоятелно не осигурява автентикация и криптиране.
- Пренася Ethernet фреймове, което го прави много удобен за осигуряване Layer 2 свързаност.
- Лесен за конфигуриране, стабилен и безпроблемен. Може да се използва само между устройства с RouterOS.

IPIP

- Използва IP протокол 4 (ip-encap), осигурява тунелен интерфейс.
- Самостоятелно не осигурява автентикация и криптиране.
- Пренася IP пакети, осигурява само Layer 3 свързаност.
- Използва се между рутери (не само MikroTik).

GRE

- Използва IP протокол 47 (gre), осигурява тунелен интерфейс.
- Самостоятелно не осигурява автентикация и криптиране.
- Осигурява Layer 3 свързаност.
- Използва се между рутери (не само MikroTik).

IPsec

- Набор от протоколи, осигуряващи защита при пренос на IP пакети (Layer 3 свързаност).
- IKE използва UDP порт 500 или друг.
- NAT-T използва UDP порт 4500.
- Използва IP протокол 50 (ipsec-esp) и/или IP протокол 51 (ipsec-ah).
- Може да осигури различни видове автентикация и/или криптиране.
- Не осигурява тунелен интерфейс.

IPsec

- Транспортен режим осигурява защита на комуникация между два хоста, често се използва за криптиране на други тунели (L2TP, IPIP, EOIP, GRE).
- Тунелен режим осигурява защита на комуникация между мрежи (в частност хостове, различни от осигуряващите тунела), използва се за свързване на отдалечени мрежи.
- Труден за конфигуриране, осигурява високо ниво на сигурност.
- Единствения VPN, който използва хардуерното ускорение за AES криптиране на устройствата, които имат такова.

Препоръки за отдалечен достъп на потребители

Вариант 1: Използвайте L2TP/IPsec.

- Лесен за конфигуриране, високо ниво на сигурност, стандартно поддържан от клентските устройства.
- Понякога проблеми със стабилността, проблем при повече от един потребител от един публичен адрес.

Препоръки за отдалечен достъп на потребители

Вариант 2: Използвайте OpenVPN.

- Труден за конфигуриране от страна на клиента, високо ниво на сигурност и стабилност.
- Изисква допълнителен клиент.

Препоръки за отдалечен достъп на потребители

Вариант 3: Използвайте IKEv2 (IPsec).

- Сравнително лесен за конфигуриране от страна на клиента, високо ниво на сигурност.
- Малко клентски устройства го поддържат, по-сложна конфигурация на сървъра.

Препоръки за свързване на отдалечени мрежи

Вариант 1: Използвайте IPsec, това е възприето като стандарт.

- Високо ниво на сигурност, поддръжка от всякакви устройства (не само MikroTik). Ако е необходим тунелен интерфейс, използвайте IPIP или GRE тунели криптирани с IPsec.
- Можете да се възползвате от устройства с хардуерно ускорение за AES (като 750Gr3, 1100, CCR).

Препоръки за свързване на отдалечени мрежи

Вариант 2: Между две устройства с RouterOS при малък трафик използвайте SSTP.

- Високо ниво на сигурност, лесно минава през защитни стени (firewall), лесно се конфигурира.

Тестове за производителност

- Ще разгледаме резултати при bandwidth test и при прехвърляне на 1GB файл през:
  - PPTP
  - SSTP
  - IPsec
- Тестовете ще направим с директна връзка с MTU 1500 байта:
  - между два RB952Ui-5ac2nD
  - между два CCR1036-8G-2S+

Тестове за производителност

Тунел	RB952Ui-5ac2nD		CCR1036-8G-2S+	
	btest	1GB файл	btest	1GB файл
PPTP/MPPE128	77 Mbps	00:01:47	141 Mbps	00:00:59
SSTP/AES256	29 Mbps	00:15:58	86 Mbps	N/A
IPsec/AES128	34 Mbps	00:05:37	338 Mbps	00:00:30
IPsec/AES256	28 Mbps	00:06:35	320 Mbps	00:00:33

Искате ли сега да направим някакви тестове ?

Благодаря за вниманието!