ZeroTier

czyli teoretycznie bezproblemowe rozwiązanie VPN?

Wojtek Mańka

mikrotikon.pl
kontakt@mikrotechnology.eu

Na co dzień pracuję jako administrator sieci w ISP mając styczność z rozwiązaniami zarówno klasy operatorskiej jak i urządzeniami dla użytkownika końcowego.

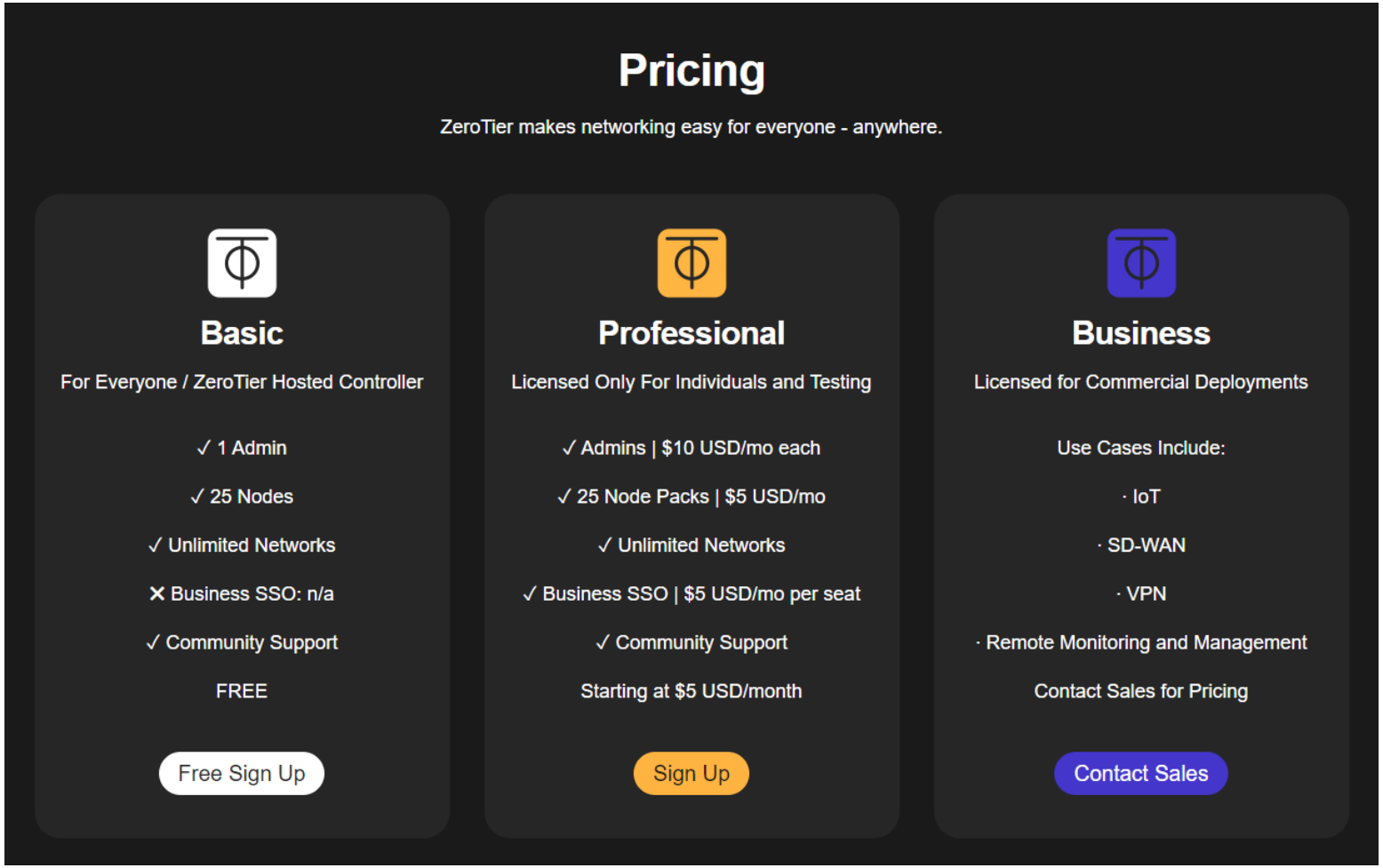
Oprócz „adminowania” zajmuje się również utrzymaniem i konfiguracją sieci u swoich klientów gdzie głównie pracuję na sprzęcie MikroTik.

Posiadam wszystkie certyfikaty MikroTik

Co to jest ZeroTier?

- Jest to usługa sieciowa stworzona przez amerykańską firmę ZeroTier, Inc.
- Usługa ZeroTier pozwala na darmowe tworzenie sieci wirtualnych które docelowo tworzą bezpieczny szyfrowany tunel peer to peer
- Usługa wymaga aplikacji zewnętrznej

Darmowa… ale do czasu



Stan na dzień 23.09.2023r.

Czy ZeroTier jest bezpieczny?

- Domyślnie sieci ZeroTier wymagają autoryzacji każdego urządzenia w panelu zarządzania
- Komunikacja zabezpieczona jest 256-bitowym szyfrem zrealizowanym End-to-End
- Docelowo każde połączenie pomiędzy urządzeniami jest realizowane bezpośrednio peer-to-peer

Wymagania sieciowe dla ZeroTier

- Nie ograniczaj wychodzących pakietów UDP
- Unikaj symetrycznego NAT'a (w tym przypadku zalecany jest „Full-cone NAT" (jeden na jednego) lub „Port-restricted cone NAT" (Stożkowy NAT z ograniczonymi portami)
- Nie używaj wielu NAT
- UDP timeout w NAT powinien być nie krótszy niż 60 sekund
- ZeroTier używa portów UDP: 9993 oraz kilku wysokich losowych portów
- UPnP można znacznie poprawić wydajność (ale wiadomo, zmniejszy bezpieczeństwo)

Jak działa bezpośrednia komunikacja bez publicznego IP?

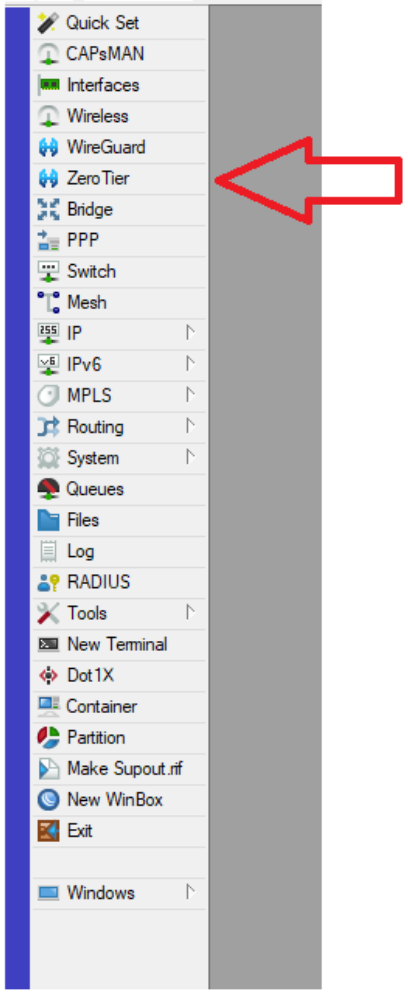
Wykorzystuje tzw. „hole punching”.

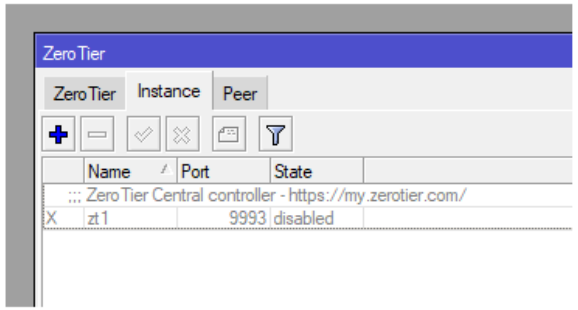
1. Do zestawienia komunikacji pomiędzy dwoma hostami (R1,R2) które mają wyłącznie adresy prywatne potrzebny jest trzeci host (S) (zwykle dostępny w publicznym Internecie).
2. Hosty R1 i R2 wysyłają pakiety do hosta S z których odczytuje on adresy z których pochodzą oraz porty źródłowe.
3. Następnie host S podaje dane R1 hostowi R2 i odwrotnie.
4. Hosty R1 i R2 wykorzystując ten sam numer portu zaczynają komunikację do siebie nawzajem (do publicznych IP), w ten sposób wpisując dane o swoim połączeniu w tablice NAT wszystkich urządzeń po drodze.
5. Finalnie (za sprawą zachowania portu) urządzenia komunikują się ze sobą wzajemnie.

ZeroTier w RouterOS

- Wymaga RouterOS v7 (zaimplementowany w v7.1rc2)
- Jest instalowany jako pakiet dodatkowy (extra-packages)
- Został wydany jedynie dla modeli urządzeń z procesorami architektury ARM i ARM64
- Nie jest objęty licencjonowaniem

Konfiguracja w RouterOS





Po zainstalowaniu pakietu dodatkowego w menu głównym pojawia się zakładka ZeroTier

Po wejściu w nią mamy 3 zakładki:

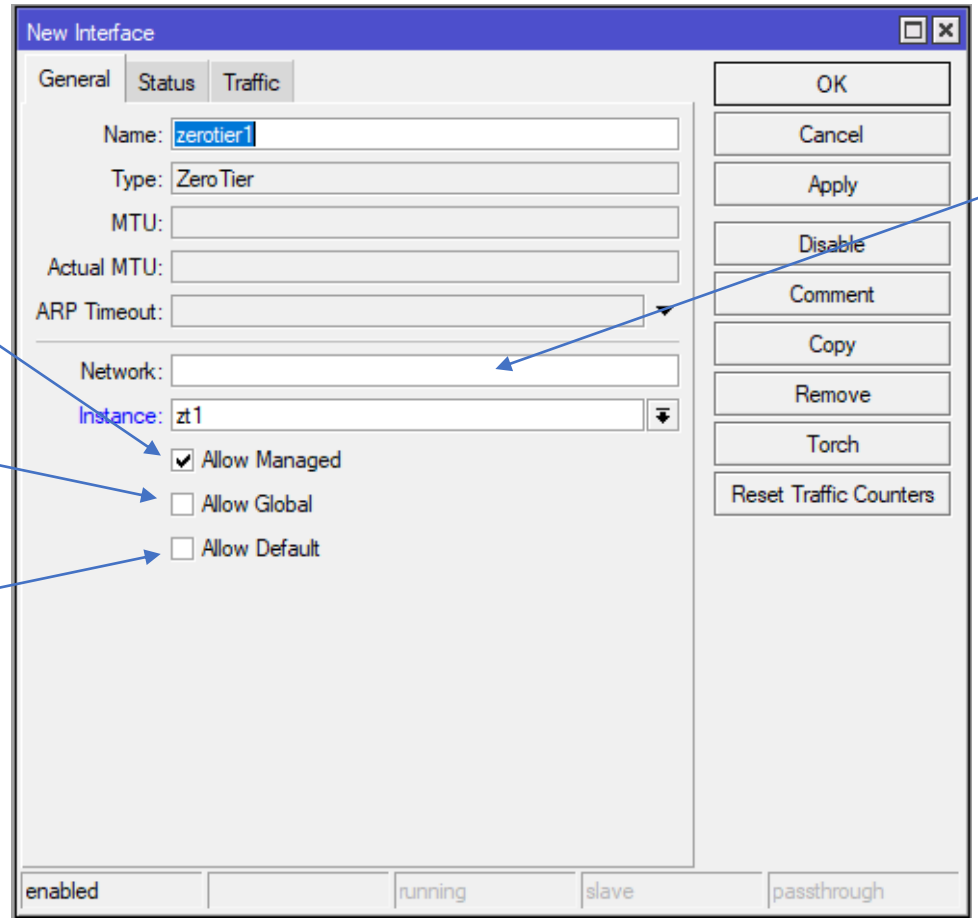
- Instance – instancje ZeroTier (domyślnie dodana jest instancja do pracy jako członek sieci)
- ZeroTier – dodajemy tutaj sieci w których ma działać MikroTik wraz z konfiguracją opcji
- Peer – lista węzłów, które zna nasz węzeł

Dodawanie sieci w RouterOS

Akceptowanie adresów IP i prywatnych tras routingu nadanych przez sieć

Akceptowanie routingów do klas publicznych

Akceptowanie trasy domyślnej (0.0.0.0/0)



Identyfikator sieci ZeroTier (nadany w panelu zarządzania)

Czas na LAB

Dziękuję za uwagę

Zapraszam na mojego bloga

mikrotikon.pl