mwtc | MikroTik Warsaw Training Center

Wygodna i łatwa w implementacji koncentracja VPN

Na przykładzie firmy outsourcingowej

MBUM #7 Kraków 2023

MikroTik Warsaw Training Center

Michał Filipek

Network Architect
Zabbix Trainer
MikroTik Trainer

/in/michalfilipek

michal@mwtc.pl

Certyfikowane Szkolenia
MikroTik

Sieci IP
Konsultacje,
Projektowanie i
Wdrożenia

Systemy Monitoringu
Szkolenia

ZABBIX

MikroTik TRAINING CENTER

Dla kogo ?

- firma świadcząca obsługę informatyczną IT
- ponad 40 klientów abonamentowych
- każdy klient posiada router, wewnętrzną sieć LAN, serwer Windows, Access Point
- potrzebny bezpieczny dostęp do sieci każdego z klientów w celach serwisowych
- potrzebny dostęp dla pracowników wdzwanianych
- nie każdy klient posiada stały/publiczny adres IP

Wymagania

01 **Koncentrator VPN**

Routery z oddziałów
Pracownicy IT

02 **Serwer Radius**

Uwierzytelnienie VPN
Uwierzytelnienie pracowników IT

03 **Mapowanie adresacji**

Rozwiązanie problemów pokrywającej się adresacji lokalnej klientów

04 **Firewall**

Izolacja klientów
Nadawanie uprawnień na podstawie przynależności do grup/profili

05 **Optymalnie kosztowo**

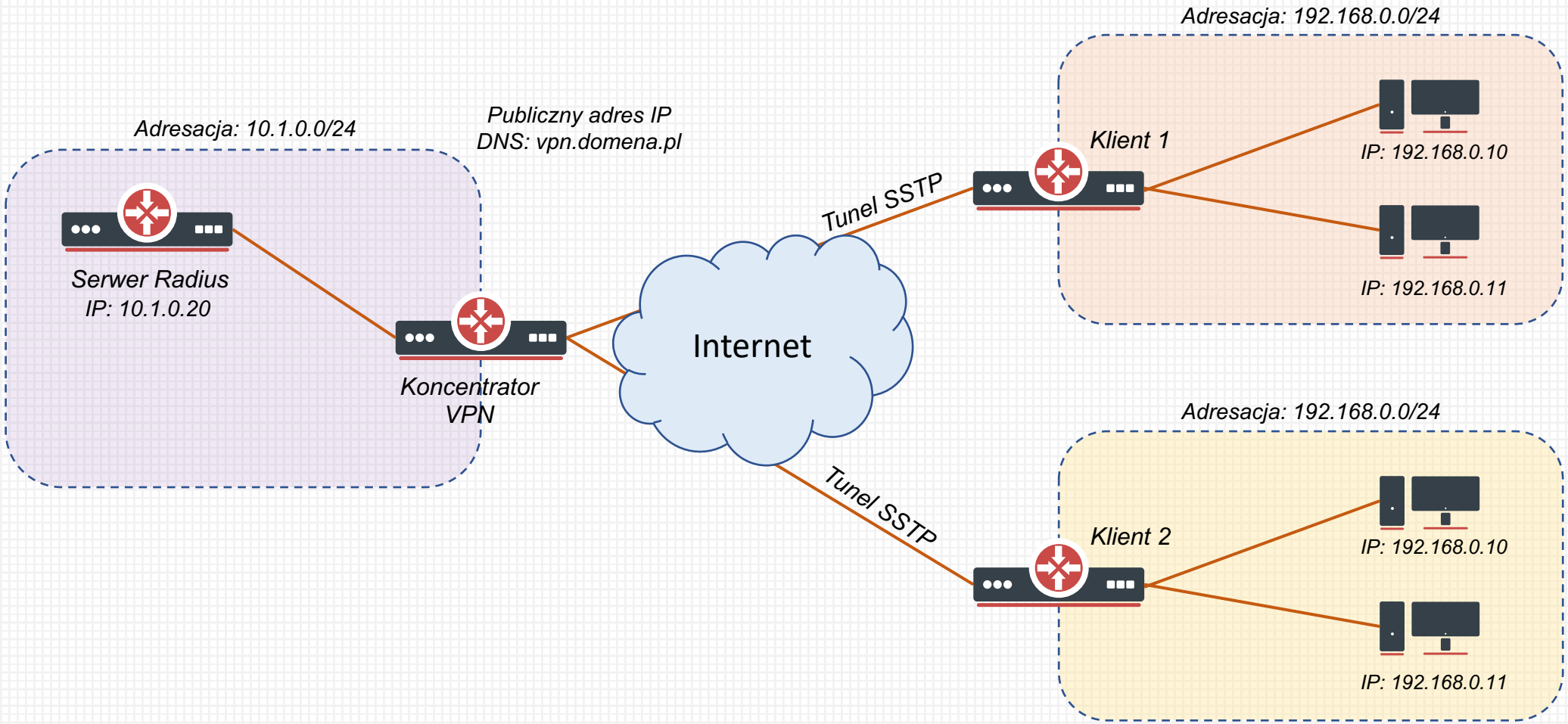
Szybka instalacja
Brak dodatkowych opłat licencyjnych

Koncentrator VPN

Wymagania:

- posiada stały publiczny adres IP
- technologia VPN SSTP (mało wydajny ale łatwy w konfiguracji)
- klienci VPN łączą się podając nazwę DNS vpn.domena.pl zamiast adresu IP
- urządzenie jest klientem serwera RADIUS

Koncentrator VPN



Schemat

Mapowanie adresacji

- Realizowane jest bezpośrednio na routerach klienckich
- Konieczne ze względu na pokrywającą się adresację klientów np. 192.168.0.0/24
- Osobna reguła **netmap** dla łańcucha **src-nat**
- Osobna reguła **netmap** dla łańcucha **dst-nat**

Serwer Radius (user-manager)

RouterOS 7 (w pełni funkcjonalna implementacja Radius):

- uwierzytelnia konta VPN routerów klienckich
- uwierzytelnia dostęp wdzwaniany dla pracowników IT (VPN)
- uwierzytelnia konta dostępu do urządzeń sieciowych
- centralny punkt nadawania/odbierania dostępu
- poza uwierzytelnieniem użytkownika przesyła dodatkowe atrybuty (np grupa)

Firewall

Koncentrator VPN

- izolacja komunikacji pomiędzy klientami
- zapewnienie ruchu z sieci wewnętrznej 10.1.0.0/24 do sieci klientów
- reguły dla użytkowników z dostępem wdzwanianym
- połączenia VPN posiadają dedykowane profile na potrzeby firewall

mwtc

Dziękujemy za uwagę

https://mwtc.pl
email: info@mwtc.pl
facebook.com/mwtcPL

ZABBIX

MikroTik TRAINING CENTER