M B U M

9/11/2017

Mikrotik Beer User Meeting

Sponsorzy:

Mikrotik Warsaw Training Center

DBG Investment

SYS-COM

Media:

ICT PROFESSIONAL

MIKROTIK ACADEMY

Mikrotik Polish Group

Integracja uwierzytelniania tunelu L2TP/IPsec z Microsoft Active Directory

MBUM

9/11/2017

MIKROTIK BEER USER MEETING

Kilka słów o mnie.

- Damian Mac
- MTCNA, MTCRE, MTCTCE
- 13 lat związany z branżą iT
- Administracja infrastrukturą serwerową
- Monitoring usług sieciowych
- Tunele VPN
- CCTV, KD, SSP

Kilka gram teorii – AD M$

- Active Directory, AD – usługa katalogowa (hierarchiczna baza danych) dla systemów Windows – Windows Server 2016, Windows Server 2012, Windows Server 2008, Windows Server 2003 oraz Windows 2000, będąca implementacją protokołu LDAP. Upubliczniona w 1999 r pod nazwą NT Directory Service przed premierą Windows 2000 Server. (źródło: wikipedia)

Kilka gram teorii – VPN

- VPN - VPN (ang. Virtual Private Network, Wirtualna Sieć Prywatna) – tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. **Można opcjonalnie** kompresować lub **szyfrować** przesyłane dane w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa. (źródło: wikipedia)

Kilka gram teorii - RADIUS

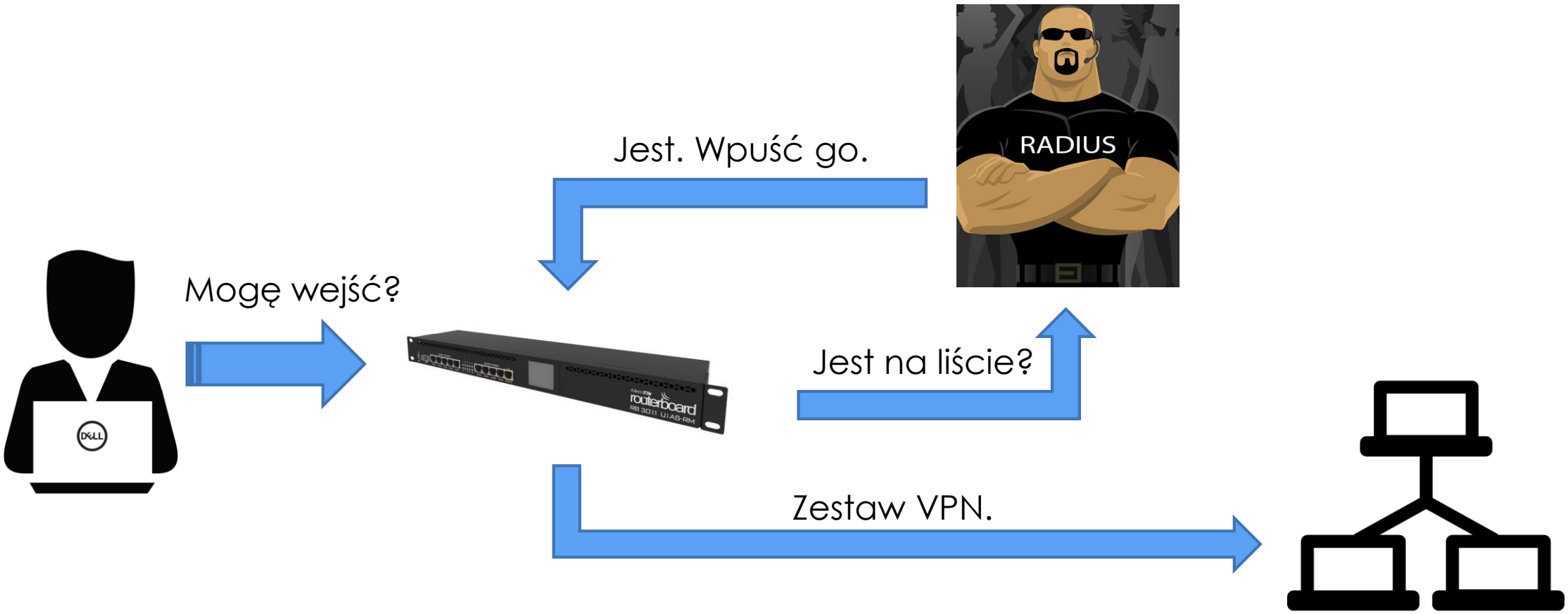
RADIUS - (ang. Remote Authentication Dial In User Service) – usługa zdalnego uwierzytelniania użytkowników, którzy wdzwaniają się do systemu (poprzez usługę „połączenie wdzwaniane"). Obecnie jest najpopularniejszym protokołem uwierzytelniania i autoryzowania użytkowników sieci telefonicznych i tunelowych. Używany jest także w sieciach bezprzewodowych. (źródło: wikipedia)

Kilka gram teorii – RADIUS (działanie)

W odpowiedzi na próbę zalogowania się użytkownika do sieci serwer dostępowy generuje zapytanie o dane użytkownika, w tym jego identyfikator i hasło, (…) identyfikator wraz z zakodowanym hasłem zostają wysłane do serwera RADIUS-a, (…). Po sprawdzeniu danych użytkownika skutkiem ich skonfrontowania z zawartością własnych baz danych serwer RADIUS może odpowiedzieć jednym z następujących komunikatów:

- **ACCEPT** – oznacza sukces uwierzytelniania,
- **REJECT** – użytkownik nie został poprawnie uwierzytelniony, dostęp do zasobów sieci jest zabroniony,
- **CHALLENGE** – prośba o wprowadzenie dodatkowych danych uwierzytelniających.

Kilka gram teorii – RADIUS (działanie)



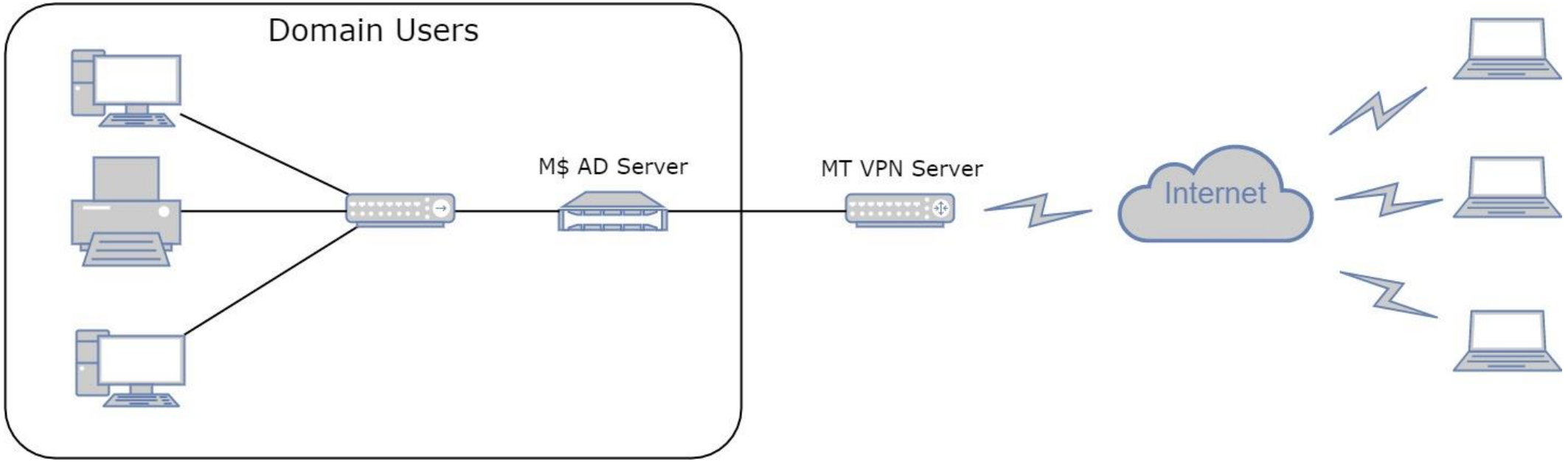
Ale co ma Active Directory do RADIUS?

- Microsoft udostępnia dostęp do bazy userów poprzez NPS
- NPS to nic innego jak rozbudowany server RADIUS
- Akceptuje zapytania od MT i sprawdza w bazie AD.

Korzyści płynące z takiego rozwiązania

- Bezpieczny zdalny dostęp dla użytkowników mobilnych
- Spójna baza danych użytkowników
- Bezpieczna polityka haseł (spójna z domeną)
- Wygodne zarządzanie użytkownikami z „jednego miejsca”
- Stosowanie zasad grupy do użytkowników zdalnych

Schemat sieci



DEMO

START CZĘŚCI PRAKTYCZNEJ

Adresacja sieci