# VPN

Piotr Dobosz

Wyższa Szkoła handlowa, Radom

02.04.2016

WYŻSZA SZKOŁA HANDLOWA W RADOMIU


RADOM ACADEMY OF ECONOMICS

# Spis treści

# Informacje wstępne



- VPN - Virtual Private Network (Wirtualne sieci prywatne)
- określenie to nie jest protokołem połączeniowym samym w sobie
- mianem tym określa się technologie pozwalające na łączenie ze sobą sieci rozproszonych
- w przważającej części rozwiązania te działają w oparciu o architekturę klient-serwer
- niepodważalnym atutem większości technologii wchodzących w skad VPN jest możliwość łączenia sieci poprzez istniejącą już infrastrukturę (np. sieci WAN)

# Działanie VPN



- tworzenie wirtualnej sieci prywatnej rozpoczyna się od zestawienia połączenia, najczęściej punkt-punkt (PPP - Point-to-Point)
- łączone mogą być sieci różnego rodzaju - lokalne, firmowe i korporacyjne (tzw. intranet; oddziały w różnych miejsach świata) czy też po prostu dwa urządzenia w dowolnej lokalizacji
- w zależności od wykorzystywanej technologii połączenia mogą być zestawiane jako równorzędne (prawdziwy punkt-punkt) bądź jako serwer-klient (obecnie dominujące)
- połączenia VPN zwykło określać się mianem tuneli; pakiety przesyłane w ramach takiej sieci są hermetyzowane (kapsułkowane), czyli opatrywane dodatkowym nagłówkiem
- we wszystkich przypadkach połączenia te są szyfrowane celem zapewnienia bezpieczeństwa transmitowanych danych
- połączenia tunelowe wymagają najczęściej dodatkowej autoryzacji (uwierzytelnienia); przeważnie autoryzacja przebiega po loginie i haśle (przestarzałe) po kluczu bądź po integralności oraz pochodzeniu danych (stosuje się jako dodatkową opcję)

# Dedykowana sieć prywatna



- rozwiązanie oparte o fizyczną infrastrukturę i/lub infrastrukturę wydzierżawioną od operatora telekomunikacyjnego (częstsze)
- fizyczna infrastruktura oznacza zestawienie połączenia pomiędzy pożądanymi lokalizacjami przy pomocy kabli miedzianych, światłowodowych bądź medium bezprzewodowego (WLAN, satelita, GSM)
- budowa własnej infrastruktury na potrzeby zestawienia sieci może być opłacalna jedynie w niedużych odległościach punktów końcowych
- w chwili obecnej łącza te buduje się przy użyciu sieci WLAN (zestawy zewnętrzne) ze względu na niskie koszty
- rozwiązanie to jest godne rozpatrzenia pod względem niezależności od innych podmiotów (nie jest jednak stricte rozwiązaniem VPN)

# Dedykowana sieć prywatna



- innym rozwiązaniem jest wynajęcie (dzierżawa) linii od jednego z operatorów telekomunikacyjnych
- koszty będą znacznie niższe niż utrzymywanie własnej linii (zakup, montaż, konserwacja)
- operator może łączyć w ramach dzierżawionej linii punkty w dowolnej lokalizacji(operator międzymiastowy/międzystrefowy)
- obecnie rozwiązanie wykorzystywane tylko w przypadku potrzeby zapewnienia największej jakości połączeń
- działa głównie w oparciu o protokoły X.25 (warstwa 2 i 3 ISO/OSI) lub FrameRelay (warstwa 2 ISO/OSI)

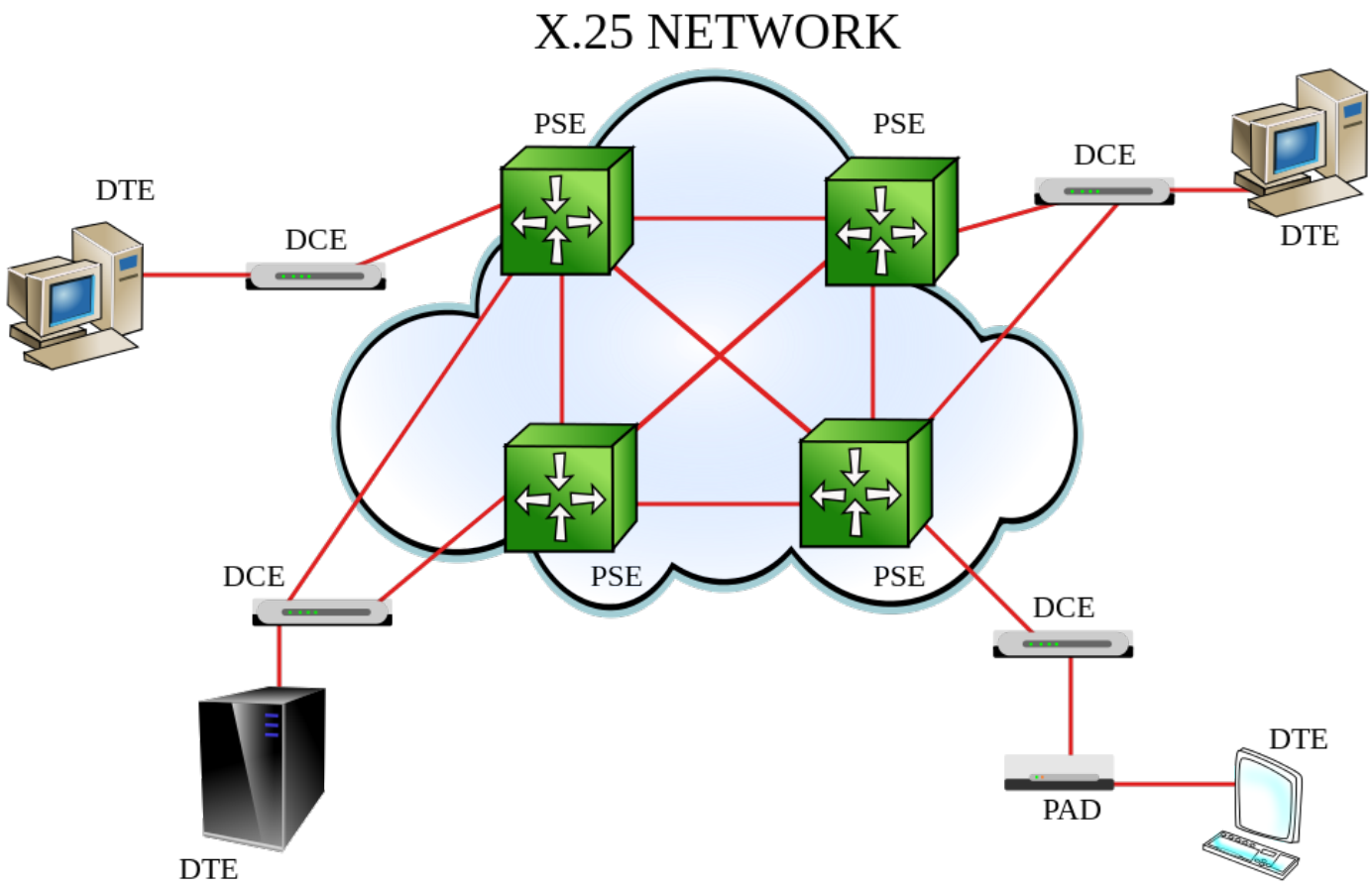
# Działanie sieci dzierżawionej



- połączenia X.25/Frame Relay należą do typu sieci z przełączanymi pakietami (switch packed network)
- przełączanie pakietów polega na przydzielaniu im niezależnych torów transmisyjnych (wirtualnych obwodów/tuneli)
- w celu zestawienia linii dzierżawionej tworzone są tzw. stałe wirtualne obwowdy
- dzieki temu zestawione połączenie trwa nawet w przypadku braku transmisji (zapewnia to największą jakoś połączenia)
- w przypadku sieci prywatnej następuje sprawdzenie przez stronę docelową adresu IP z odebranego pakietu; jeżeli adres zgadza się adresacją sieci docelowej zostaje zestawione połączenie sieciowe; w przeciwnym wypadku pakiet (oraz następne) zostaną odrzucone (zingnorowane)

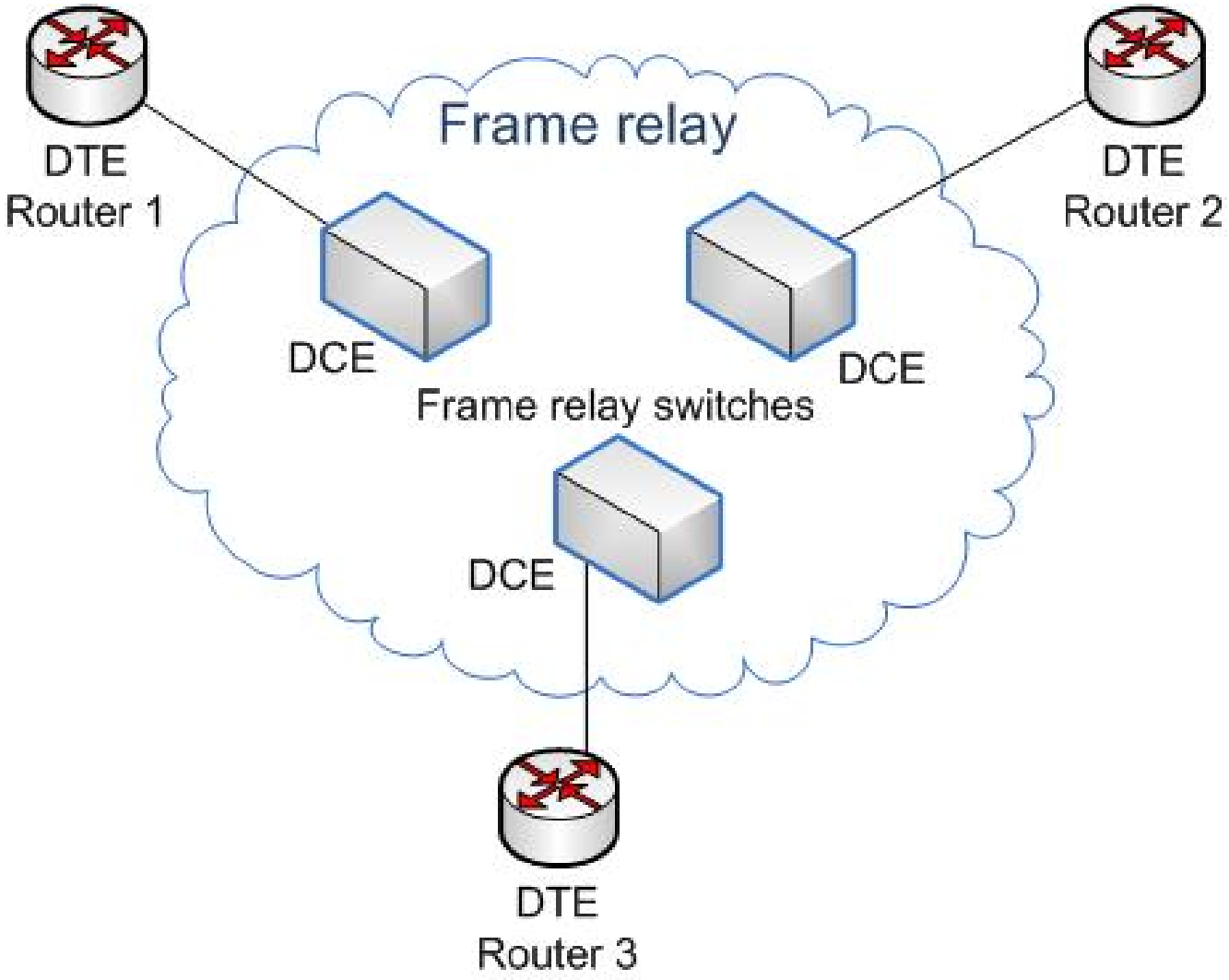
# Budowa sieci X.25





# Budowa sieci Frame Relay





# Sieć VPN w oparciu o publiczną sieć dostępową (Internet)



- wraz ze wzrotem znaczenia sieci IP oraz odejciem od mniej wydajnych technologii zaczęto szukać innych rozwiązań nawiązywania połączeń pomiędzy odległymi sieciami
- nowe rozwiązanie musiało być wolne od wady poprzedniego, tj. ściśle określonych stron połączenia (brak elastyczności i skalowalności)
- rozwiązaniem było zmienić sposób autoryzacji użytkowników/dwóch punktów
- w połowie lat 90 (około 1996 roku) swoją propozycję użycia VPN przedstawia Microsoft - PPTP (Point-to-Point Tunnel Protocol)
- rozwiązanie zyskuje uznanie i staje się standardem sieci VPN
- oczywiście inne firmy/korporacje tworzyły swoje rozwiązania (równolegle) dlatego poznanie prawdziwego twórcy VPN jest niemożliwe
- obecnie firma VirnetX zgłasza pretensje jakoby ona utworzyła podwaliny protokołu PPTP

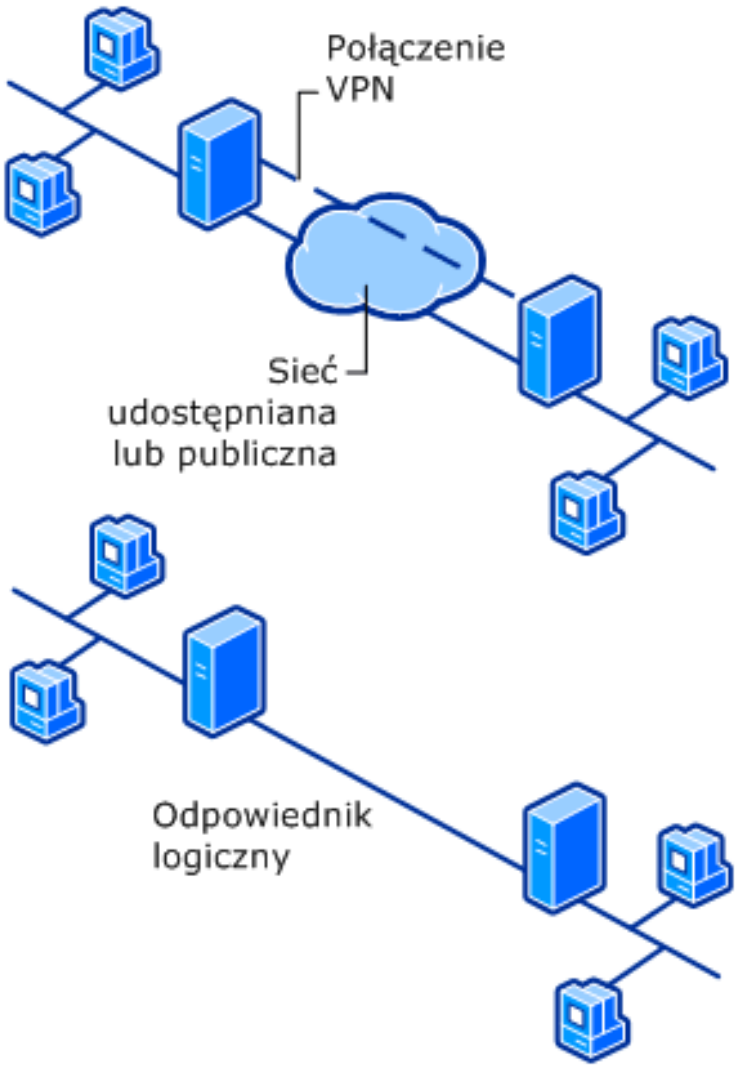
# Nawiązywanie połączenia



- klient inicjuje połączenie z serwerem celem nazwiązania połączenia punkt-punkt
- jeżeli poświadczenia klienta są poprawne następuje inicjalizacja połączenia
- by emulować łącze punkt-punkt przesyłane dane są hermetyzowane (dodatkowy nagłówek)
- nagłówek zawiera tablicę routingu pozwalającą na precyzyjne dotarcie pakietu pomiędzy punktami poprzez sieć rozległą
- dodatkowo dane są szyfrowane i mogą być przeczytane jedynie przez strony posiadające klucze (najczęściej parowane prywatny/publiczny)

# Koncepcja połączeń VPN





# Różnice pomiędzy połączeniem dostępu zdalnego a lokalizacja-lokalizacja



- rozróżnia się dwa wymienione typy połączeń
- określenia dostępu zdalnego używa się w przypadku pojedynczego komputera (np. pracownika firmy) podłączającego się przy pomocy VPN do zasobów sieci firmowej
- w tym wypadku nikt poza nim (w danej lokalizacji) nie będzie miał możliwości korzytsania z zasobów sieci, do której uzyska on podłączenie
- w przypadku połączeń lokalizacja-lokalizacja VPN jest dla użytkowników zupełnie 'przezroczysty' - mogą nie wiedzieć o jego istnieniu
- obsługą połączenia zajmują się routery bądź serwery, na których skonfigurowana jest usługa

# Wstęp



- obecnie istnieje kilka technologii (protokołów) dostępu do VPN
- najbardziej rozpowszechnione są rozwiązania firmy Microsoft - PPTP, L2TP, SSTP
- z rozwiązań otwartoźródłowych na uznanie zasługuje OpenVPN
- wraz z upowszechnianiem się protokołu IPv6 coraz większą rolę mogą odgrywać protokoły dostępu bezpośredniego (w tym zaprojektowany przez Microsoft DirectAccess)
- swoje rozwiązania proponuje także CISCO (np. AnyConnect)

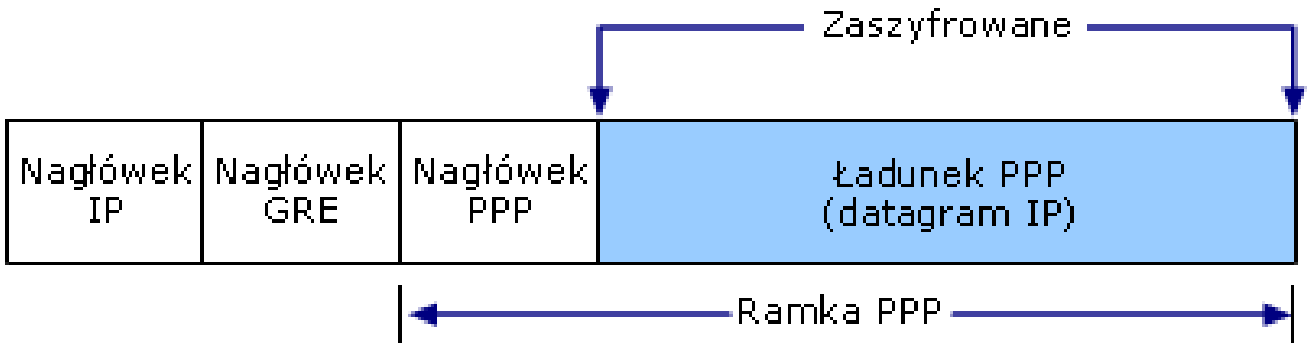
# Protokół PPTP



- najstarsza implementacja protokołu dla VPN
- autoryzacja przebiega identycznie jak w protokole PPP - poprzez nazwę użytkownika oraz hasło
- pierwotnie nie posiadał szyfrowania
- obecnie, po zestawieniu połączenia z wykorzystaniem MS CHAP v2/ EAP-TLS przesyłane dane są szyfrowane kluczem generowanym po każdorazowym zestawieniu połączenia
- protokół dodaje w systemie wirtualny interfejs do obsługi połączeń VPN; traktowany jest jako karta sieciowa (czyli można przez niego np. przepuszać NAT, trasować pakiety itp., aczkolwiek należy to wszystko skonfigurować ręcznie)
- przy połączeniu wykorzystywany jest tunel GRE VPN (Generic Routing Encapsulation) pozwalający na szyfrowanie całego zestawionego tunelu (nie tylko danych); niestety protokół ten jest domyślnie blokowany przez zapory (trzeba tworzyć na niego regułę)

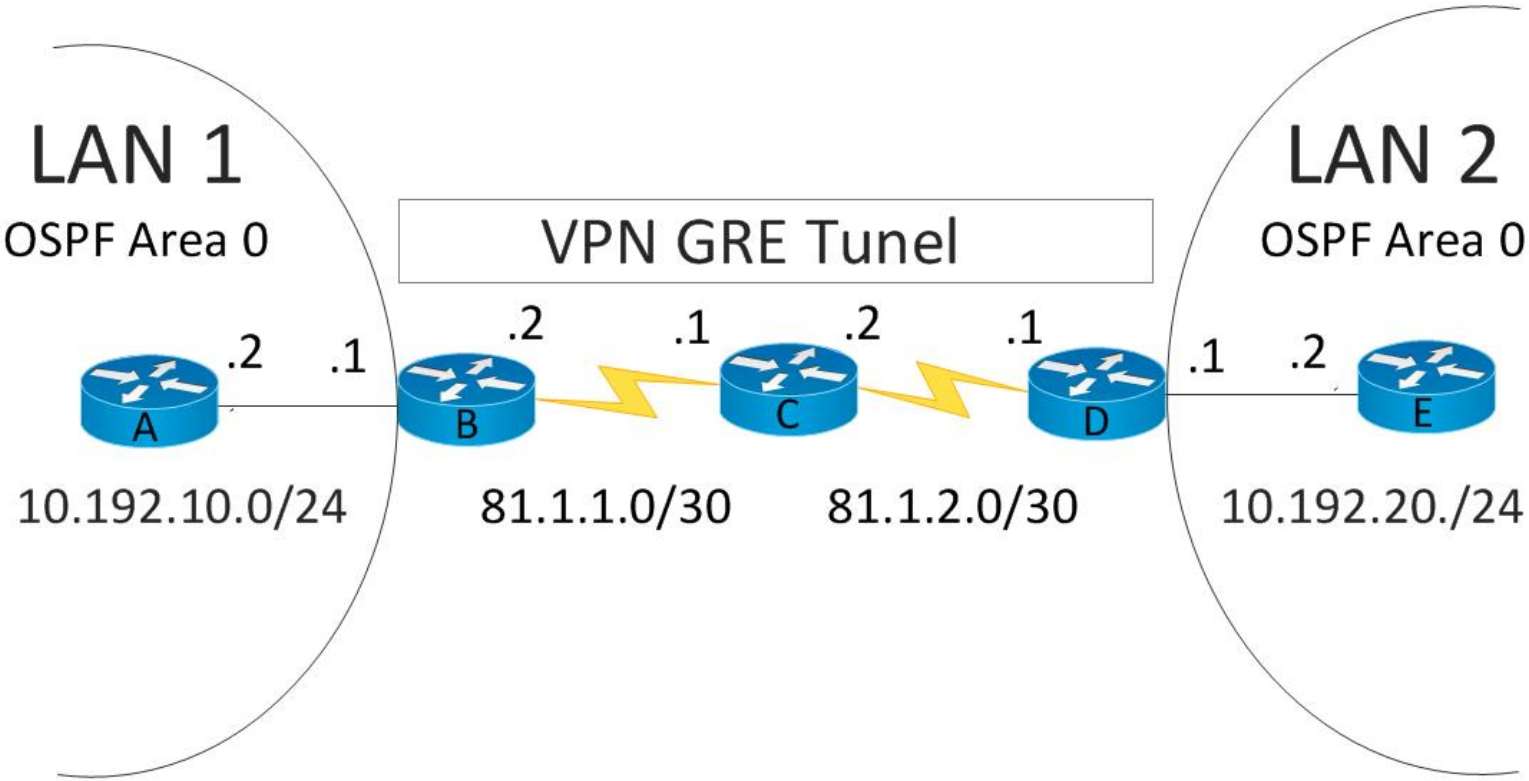
# Nagłówek PPTP





# PPTP - tunel GRE





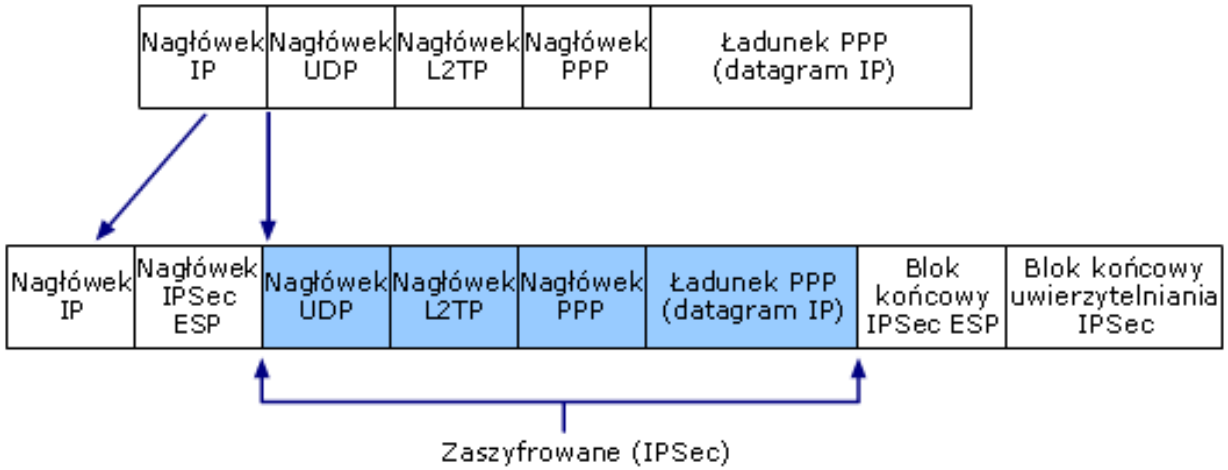
# Protokół L2TP



- podobnie jak PPTP wymaga uwierzytelnienia loginem i hasłem
- w przeciwieństwie jednak do niego nie wykorzystuje protokołu GRE
- zamiast tego wykorzystuje protokół IPSec, który pozwala na lepsze zabezpieczenie danych (prócz samego szyfrowania wykorzystuje sprawdzanie integralności danych)
- niestety szyfrowanie odbywa się przy użyciu kluczy symetrycznych (DES/3DES)

# Nagłówek L2TP





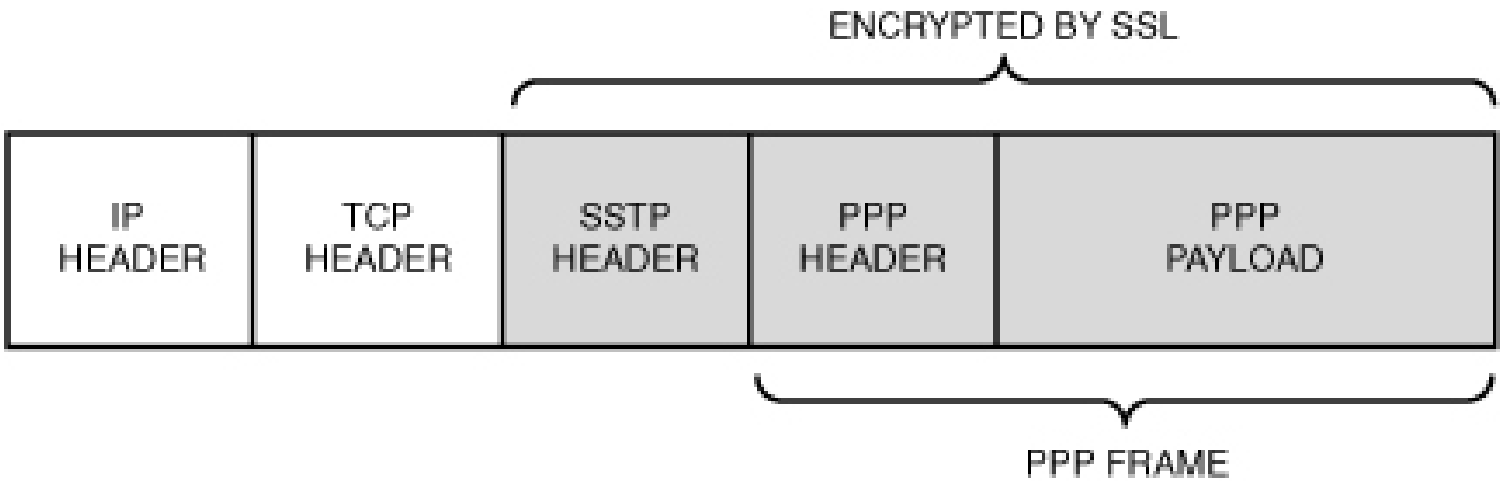
# Protokół SSTP



- 'najnowsze' rozwiązanie VPN dla IPv4 od Microsoft
- również należy do rodziny PPP!
- zaprojektowany z myślą o dostępie do VPN w przypadku, gdy nie mamy możliwości przekierowania określonych portów
- wykorzystuje port 443 i protokół HTTPS do inicjacji połączenia oraz zabezpieczenia danych (tak jak dzieje się np. ze stronami banków)
- dzięki temu rozwiązaniu można uzyskać połączenie zarówno poprzez pośredników sieciowych (PROXY) jak i mocno ograniczony dostęp do sieci Internet (np. poprzez miejskie punkty publicznego dostępu do sieci, na których przeważnie odblokowane są porty 80 i 443)

# Nagłówek SSTP





# Wstęp



- dotychczas przedstawione rozwiązania dotyczyły głównie implementacji dla systemów Microsoft
- chociaż możliwe jest zestawianie połączeń dla innych systemów, to nie są to często rozwiązania satyfakcjonujące
- alternatywą mogą być rozwiązania AnyConnect (CISCO), OpenVPN (otwartoźródłowy VPN), IKEv2 (tunelowanie IPSec dla systemu Linux) czy też popularne Hamachi (oparte na SSL)

# AnyConnect



- standard połączeń zaproponowany przez firmę CISCO
- rozwiązanie złożone jest z kilku modułów, które można włączać/wyłączać (oczywiście niektóre z nich są dodatkowo płatne)
- rozwiązanie autoryzacji nie spoczywa na serwerze z systemem sieciowym, a na specjalnym, dedykowanym urządzeniu ASA (Adaptive Security Appliance) oraz WSA (Web Security Appliance)
- komuniacja dla docelowego użytkownika jest 'przezroczysta' - uwierzytelnienie może następować np. po adresie IP sieci (w przypadku Ipv6 nawet każdego urządzenia) lub poprzez mapowanie nazwy użytkownika
- usługa może być uruchamiana zanim użytkownik zaloguje się do systemu i podtrzymywać połączenie od startu sieci aż do wyłączenia komputera/awarii sieci

# OpenVPN



- rozwiązanie w pełni otwartoźródłowe
- działa na wszystkich systemach operacyjnych (kompilowane na systemy Windows, Linux, OS X, Solaris, Android)
- konfiguracja zarówno serwera jak i klienta może być przenoszona pomiędzy poszczególnymi systemami - jest ona przechowywana w pliku tekstowym
- wraz z OpenVPN można zainstalować centrum certyfikacji (niezbędne w przypadku serwera); pozwala ono na nadawanie kluczy autoryzacyjnych i szyfrujących połączenia
- ruch autoryzowany jest poprzez certyfikat serwera (zmiana certyfikatu uniemożliwia połączenia), a każdy użytkownik musi wykazać się odpowidnim kluczem prywatnym (publiczny przechowywany jest na serwerze)
- powyższe rozwiązanie zapewnia możliwość przezroczystego połączenia klienta z serwerem - brak potrzeby autoryzacji użytkownika (identycznie jak AnyConnect)
- transmisję można dodatkowo szyfrować protokołem TLS

# LogMeIn Hamachi



- rozwiązanie to bazuje na istniejących powszechnie, wcześniej wymienionych protokołach (PPTP/L2TP)
- w przeciwieństwie do samodzielnego zestawiania połączenia (wymagany serwer oraz otwarte wskazane porty) wszystko wykonuje za nas program - klient Hamachi
- do konta użytkownika można utworzyć więcej niż jedną sieć, dzięki czemu można separować poszczególne sieci VPN od siebie (samemu stając się serwerem VPN)
- sieci użytkownika zabezpieczane są loginem i hasłem, mogą też być publiczne (w zależności od potrzeb)
- domyślnie wykorzystywany jest mechanizm szyfrowania danych
- lokalizacje serwerów (m. in. USA, Indie, Serbia, Wileka Brytania) pozwalają na przeglądanie zawartości stron, do których normalnie nie mielibyśmy dostępu (Hamachi przekierowuje ruch sieciowy)
- podstawowa, darmowa wersja, posiada szereg ograniczeń, którego nie ma w wersji płatnej
- eksperci podkreślają, że protokół Hamachi posiada sporo luk i błędów, przez co nie polecają używania tego rozwiązania do zastosowań biznesowych

# DirectAccess



- technologia opracowana przez firmę Microsoft
- wstępnie funkcja została zaprojektowana jedynie dla protokołu IPv6 (obecnie pozwala na łączenie się sieci IPv4 do DirectAccess poprzez np. serwery Toredo)
- w założeniu nie jest to VPN, a jedynie nadzorowane centralnie połączenie pomiędzy serwerem a autoryzowanymi użytkownikami
- elementem autoryzującym jest adres IPv6 + klucze autoryzacyjne (DES/RSA wykorzystywane w IPSec, domyślnie obecnym w IPv6)
- administrator może ustalać, do których części sieci wskazane urządzenia mają dostęp
- możliwe jest nawet wymuszenie tras pakietów oraz użytkowania serwerwów DNS
- rozwiązanie dedykowane jest jedynie dla systemów z rodziny Windows
- najlepiej działa od wersji Windows 8 (klient) i Windows Server 2012 (implementacja bezpośrednio w systemie)

# Pozostali



- przedstawione wyżej rozwiązania to jedynie popularne rozwiązania
- usług i firm oferujących zestawianie sieci jest znacznie więcej
- konkurencją dla sprzetowych rozwiązań CISCO jest np. oferta firmy Juniper, pozwalająca np. na autoryzację poprzez klucze RSA
- Hamachi posiada konkurencję w postaci chociażby tuneli OpenVPN, w ktorych płatność następuje od ilości przetransferowancyh danych (bądź za określoną kwotę limit znika)
- dla protokołów L2TP czy OpenVPN konkurencją może być protokół IKEv2, pozwalający na łączenie bezpośrednie (równorzędność w komunikacji obu stron); niestety ten protokół nie jest wspierany w każdym środowisku

# Podsumowanie



- poznane technologie mają swoje wady i zalety
- na forach można spotkać się z zarówno zwolennikami jak i przeciwnikami danej technologii
- często też producenci ubarwiają funkcjonalność danego podejścia celem zdobycia nowego klienta
- dobrym podsumowaniem będzie zatem przytoczyć wady i zalety poszczególnych rozwiązań

# PPTP



## ZALETY:

- łatwy w konfiguracji pod stronie systemu (wystarczy login i hasło)
- nie potrzebuje dodatkowego oprogramowania (większość systemu ma zaimplementowaną jego obsługę)
- protokół jest szybki (mały narzut nagłówków dodatkowych)
- w roli serwera można ustawowić niemal dowolne urządzenie (nawet router ze średniego przedziału cenowego)

## WADY:

- posiada poważne znane luki w protokole MS CHAPv2, które prawdopodobnie nigdy nie zostaną naprawione
- słabe klucze szyfrujące (bez AES) pozwalają sądzić, że dostęp do tego typu połączeń może być z łatwością łamany
- podejrzewa się, że NSA ma pełen dostęp do każdego tunelu zestawionego w ten sposób
- dodatkowo wymaga ingerencji w otawrciu portów na zaporze sieciowej (zarówno dla portu serwera jak i protokołu GRE - 1723)

# L2TP



## ZALETY:

- konfiguracja przebiega w łatwy sposób
- autoryzcja róœnież nie powinna sprawiać problemów (login/hasło)
- znacznie bezpieczniejszy od PPTP
- działa, podobnie jak poprzednik, niemal na wszystkich platformach i urządzeniach zgodnych z VPN
- szybki poprzez wykorzystanie przy kodowaniu/dekodowaniu wielowątkowości

## WADY:

- może zostać odrzucony przez niektóre zapory sieciowe (dodatkowa konfiguracja)
- niekiedy wspominana jest informacja, że może on być dawno złamany przez agencje rządowe

# SSTP



## ZALETY:

- posiada mocne szyfrowanie (klucz o sile 256 bit i więcej)
- wykorzystuje port 443, przez co nie jest blokowany na zaporze sieciowej/urządzenaich (domyślny port stron HTTPS)
- domyślnie zaimplementowany w systemach z rodziny Windows (Windows Vista SP1 i wyższe) - technologia Microsoft

## WADY:

- działa tylko we wskazanych systemach Windows, chociaż istnieją projekty kliencie np. na system Linux
- bez pełnej dokumentacji kodu brak możliwości rozpoznania pełnego bezpieczeństwa standardu

# OpenVPN



## ZALETY:

- implementacja w pełni otwartoźródłowa - każdy może przejrzeć kod i go usprawnić pod swoje potrzeby
- przy uwierzytelnianiu wykorzystuje szyfrowanie asynchorniczne pozwalające zapomnieć o loginie i haśle
- dodatkowo obsługuje szyfrowanie pakietów pomiędzy serwerem a klientem dodatkowo zwiększając poufność danych
- dzięki swojej otwartości posiada swoje wersje niemal na wszystkie systemy (bądź może posiadać po skompilowaniu)
- konfiguracja stworzona raz może być przenoszona na kolejne jednoski
- działa jako usługa systemowa/demon, przez co połączenie może być nawiązywane automatycznie po podłączeniu do sieci WAN
- prócz powszechnych tuneli pozwala także na mostkowanie sieci (klient otrzymuje dokładnie taki sam adres jak reszta sieci - niczym się nie wyróżnia!)
- klient nie musi NIC konfigurować - niewidzialny dla zapór sieciowych (konfiguracji wymaga serwer)
- działa na dowlnym porcie (w tym np. na 80, 443 i innych, które przeważnie nie mogą być zastrzeżone nawet przy publicznym dostępie sieciowym)

## WADY:

- brak obsługi wielowątkowości po stronie serwera potrafi spowolnić pracę (powyżej 1000 użytkowników na sieć; możliwe obejścia problemu)
- niekiedy ciężki w konfiguracji
- nie jest podstawowym składnikiem systemów operacyjnych

# IKEv2



## ZALETY:

- standard pozwala na przezroczyste połączenie klienta do serwera poprzez wymianę kluczy
- działa w oparciu o IPSec
- bez narzutu PPP, a więc znacznie szybszy od L2TP (również bazującego na IKE)
- bardzo łatwy w konfiguracji po stronie użytkownika
- sam dba o połączenie (wznawia połączenie w przypadku utraty)

## WADY:

- nie wspierany na wielu platformach
- konfiguracja na serwerze potrafi być ciężka
- wykorzystywanie IPSec, potencjalnie złamanego
- ograniczeniem może być szyfrowanie 256 bit

# DirectAccess



## ZALETY:

- standard idealny dla protokołu IPv6
- pozwala na identyfikację po adresie IP, ewentualnie można wykorzystać inne metody autoryzacji
- pozwala na pełne ustawienia uprawnień podłączających się klientów do sieci, ustawienia wymagań systemu (np. posiadanie najnowszych poprawek)
- umożliwia autoryzację maszych łączących się w ramach Active Directory

## WADY:

- działa tylko z systemami Windows (w tym najlepiej z najnowszymi wersjami)
- chociaż pozwala łączyć się użytkownikom sieci IPv4, to same aplikacje MUSZĄ działać w oparciu o IPv6 (inaczej nie zostaną przekierowane)
- serwer autoryzacyjny musi posiadać usługę IIS (autoryzacja przy podłączeniu do sieci przebiega po HTTPS)

# Rozwiązania sprzętowe (CISCO, Juniper



## ZALETY:

- rozwiązania są niezwykle proste do zastosowania - wstępnie zainstalowane i skonfigurowane na dedykowanym sprzęcie
- przeważnie konfiguracja opiera się o przyjazne rozwiązanie strony WWW
- bardziej zaawansowane opcje można aktywować poprzez telnet/SSH
- po stronie klienta sprowadzają się do zainstalowania aplikacji i prostej konfiguracji
- posiadają dobre wsparcie techniczne

## WADY:

- drogie
- wymagają dodatkowej przestrzeni w serwerowni (w szafie)
- dodatkowe urządzenia do obsługi

# Wykorzystane materiały



## Strony WWW:


- https://www.quora.com/Who-invented-virtual-private-networks-VPN
- https://www.ukessays.com/essays/information-technology/history-of-the-virtual-private-network-information-technology-essay.php
- https://www.cactusvpn.com/beginners-guide-to-vpn/vpn-history/
- http://blog.seattlepi.com/microsoft/2010/03/13/should-microsoft-have-patented-its-vpn-in-the-90s/
- https://technet.microsoft.com/pl-pl/library/cc731954(v=ws.10).aspx
- http://www.networkexpert.pl/artykul/35_vpn-gre-tunel-konfiguracja.html
- http://techrepublic123.blogspot.com/2011/10/windows-server-2008-r2-server-to-client.html
- https://www.ukessays.com/essays/information-technology/history-of-the-virtual-private-network-information-technology-essay.php
- https://technet.microsoft.com/pl-pl/library/cc771298(v=ws.10).aspx
- http://www.vsx.pl/struktura-sieci-ipsec-ike-pki-ssl/
- https://www.pluralsight.com/blog/it-ops/cisco-anyconnect-secure-mobility-client
- http://www.cisco.com/c/dam/en/us/td/docs/security/wsa/wsa7-0/user_guide/AnyConnect_Secure_Mobility_SolutionGuide.pdf
- https://openvpn.net/index.php/open-source/overview.html
- https://en.wikipedia.org

# Wykorzystane materiały




- https://community.spiceworks.com/topic/319766-ms-direct-access-alternative
- https://community.spiceworks.com/topic/148726-direct-access-any-real-world-experiences
- http://www.pcworld.com/article/186711/microsoft_directaccess.html
- https://learningnetwork.cisco.com/thread/23247
- http://www.juniper.net/us/en/products-services/network-edge-services/security/junos-vpn-site-secure/
- http://mad-scientist.net/welcome-to-the-lab/juniper-network-connect-vpn/
- http://vpn-services.softwareinsider.com/
- https://www.bestvpn.com/blog/4147/pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/
- https://technet.microsoft.com/pl-pl/library/dd759144(v=ws.11).aspx
- http://www.pcworld.com/article/186711/microsoft_directaccess.html
- https://community.spiceworks.com/topic/319766-ms-direct-access-alternative
- https://community.spiceworks.com/topic/148726-direct-access-any-real-world-experiences
- https://pl.wikipedia.org/wiki/EAP-IKEv2
- http://www.techrepublic.com/blog/10-things/10-things-you-should-know-about-directaccess/
- http://eap-ikev2.sourceforge.net/

# Koniec



Dziękuję za uwagę!