Łukasz Buczyński

Połączenie oddziałów firmy za pomocą tuneli IPIP+IPSEC oraz routingu dynamicznego OSPF - case study

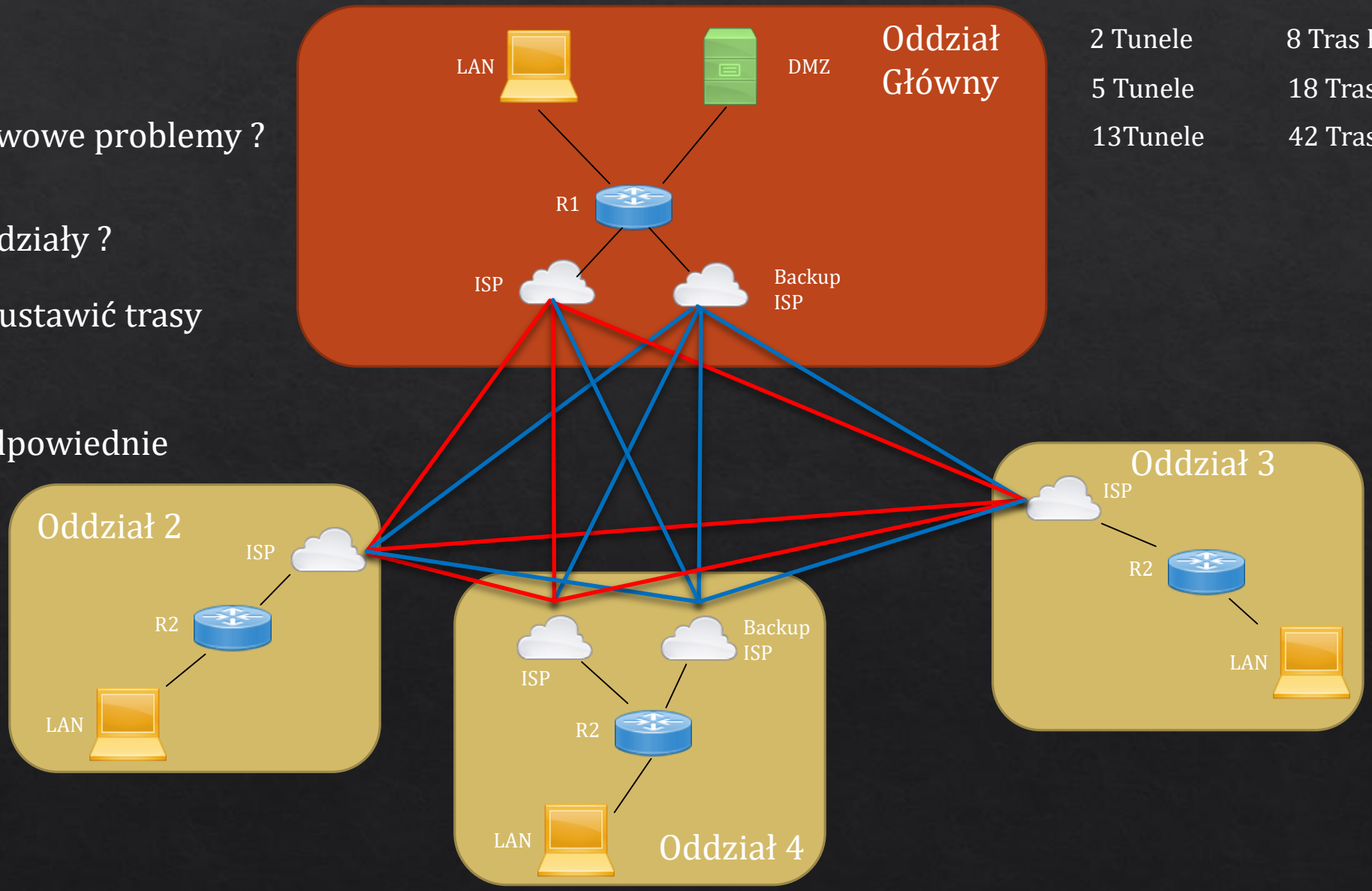
Kim jestem ?

Administrator sieci z wieloletnim doświadczeniem, obecnie zarządza infrastrukturą w dużym przedsiębiorstwie. Specjalizuje się w zagadnieniach: routing, zabezpieczenia brzegu sieci oraz VPN na urządzeniach Mikrotik i Fortinet. Posiada szeroką wiedzę w zakresie konfiguracji IP-PBX. Po godzinach, jeśli tylko zostaje trochę czasu - pasjonat elektroniki.
- MTCNA, MTCRE, MTCWE

Stare Dobre Czasy

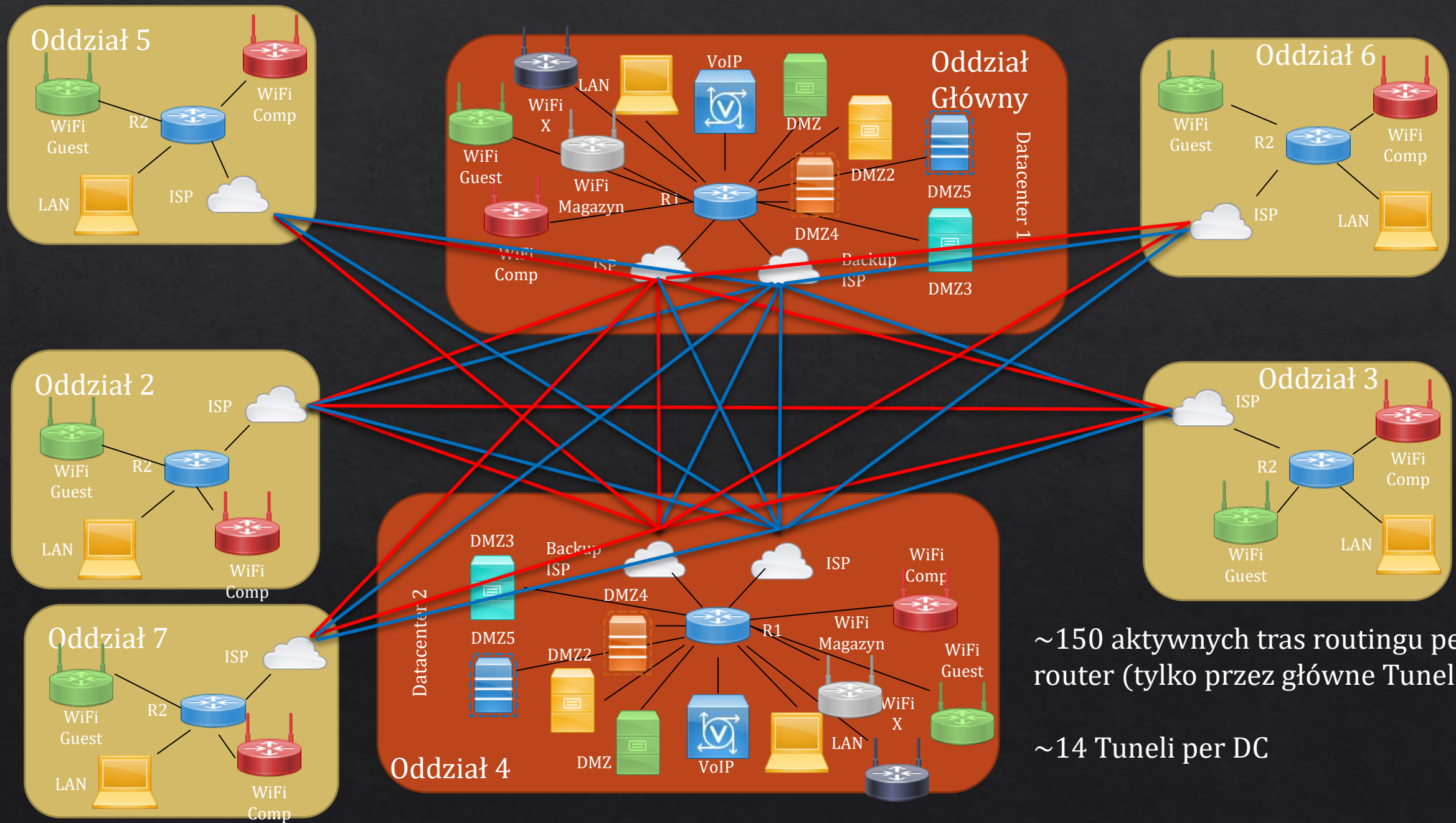
Jakie mamy podstawowe problemy ?

1. Jak połączyć oddziały ?
2. Jak optymalnie ustawić trasy komunikacji?
3. Jak zapewnić odpowiednie reguły dostępu?



2 Tunele	8 Tras Routingu
5 Tunele	18 Tras Routingu
13Tunele	42 Tras Routingu

Co mamy obecnie



~150 aktywnych tras routingu per-router (tylko przez główne Tunele)

~14 Tuneli per DC

1. Jak to połączyć ?

I dlaczego akurat IPIP + IPSec?, a statyczny routing nie wystarczy?

VPN (ang. *Virtual Private Network*, Wirtualna Sieć Prywatna)

Najczęściej spotykane rodzaje VPN według Wikipedii

- Hamachi
- PPTP

PPTP is a secure tunnel for transporting IP traffic using PPP. PPTP encapsulates PPP in virtual lines that run over IP. PPTP incorporates PPP and MPPE (Microsoft Point to Point Encryption) to make encrypted links. The purpose of this protocol is to make well-managed secure connections between routers as well as between routers and PPTP clients (clients are available for and/or included in almost all OSs including Windows).

- L2TP

L2TP is a secure tunnel protocol for transporting IP traffic using PPP. L2TP encapsulates PPP in virtual lines that run over IP, Frame Relay and other protocols (that are not currently supported by MikroTik RouterOS). L2TP incorporates PPP and MPPE (Microsoft Point to Point Encryption) to make encrypted links. The purpose of this protocol is to allow the Layer 2 and PPP endpoints to reside on different devices interconnected by a packet-switched network.

- OpenVPN

OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol[9] that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls. It was written by James Yonan and is published under the GNU General Public License (GPL).

- SSTP

Secure Socket Tunneling Protocol (SSTP) transports a PPP tunnel over a TLS 1.0 channel. The use of TLS over TCP port 443 allows SSTP to pass through virtually all firewalls and proxy servers.

- IPSec

Internet Protocol Security (IPsec) is a set of protocols defined by the Internet Engineering Task Force (IETF) to secure packet exchange over unprotected IP/IPv6 networks such as Internet. IpSec protocol suite can be divided in following groups:

- Authentication Header (AH) RFC 4302
- Encapsulating Security Payload (ESP) RFC 4303
- Internet Key Exchange (IKE) protocols. Dynamically generates and distributes cryptographic keys for AH and ESP.

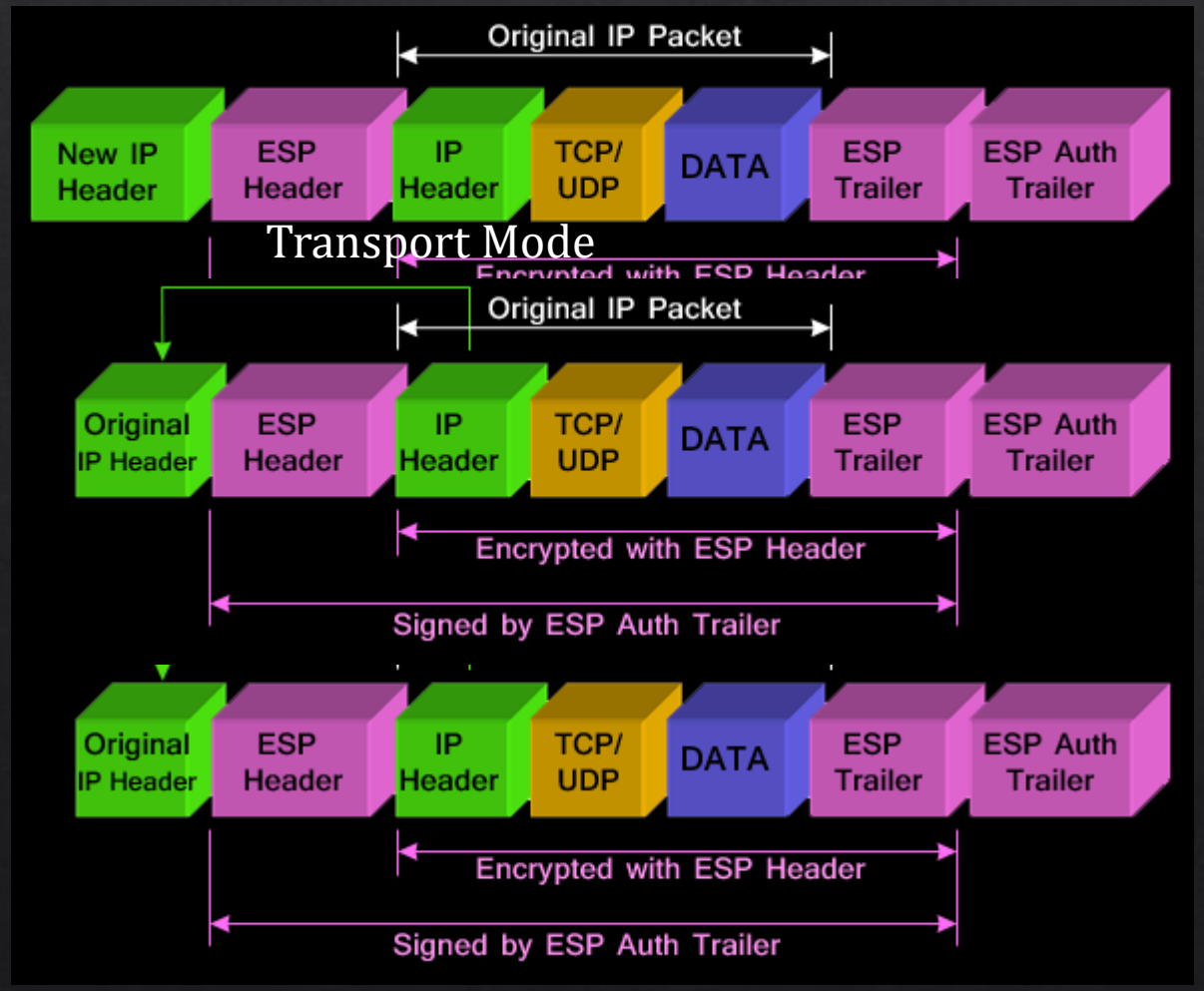
Źródło: Wikipedia https://pl.wikipedia.org/wiki/Virtual_Private_Network https://en.wikipedia.org/wiki/OpenVPN https://wiki.mikrotik.com

1. Jak to połączyć ?

Nie taki IPSec straszny

Authentication Header (AH) Encapsulating Security Payload (ESP) Internet Key Exchange (IKE)

Tunnel Mode



Phase1 – ISAKMP (Internet Security Association and Key Managment Protocol)

- Przeprowadza uwierzytelnianie (może wykorzystać współdzielony klucz, podpisy RSA, certyfikaty X.509 lub kerberos)
- Przeprowadza bezpieczne uzgodnienie kluczy kryptograficznych oraz ich parametrów
- Tworzy kanał ISAKMP SA (Security Association)
- Zarządza utworzonym kanałem oraz w razie potrzeby go renegocjuje

Phase2 - Oakley (OKLEY Key Determination Protocol)

- Wykorzystuje bezpieczny kanał utworzony w Fazie 1
- Negocjuje parametry szyfrowania (proposals)
- Zestawia relację IPSec SA używaną do właściwego szyfrowania danych

Trochę Praktyki

1. Jak to połączyć cd. ?

I dlaczego akurat IPIP + IPSec?

Tunel – zestawienie połączenia między dwoma odległymi hostami tak, by stworzyć wrażenie, że są połączone bezpośrednio.

- IPIP

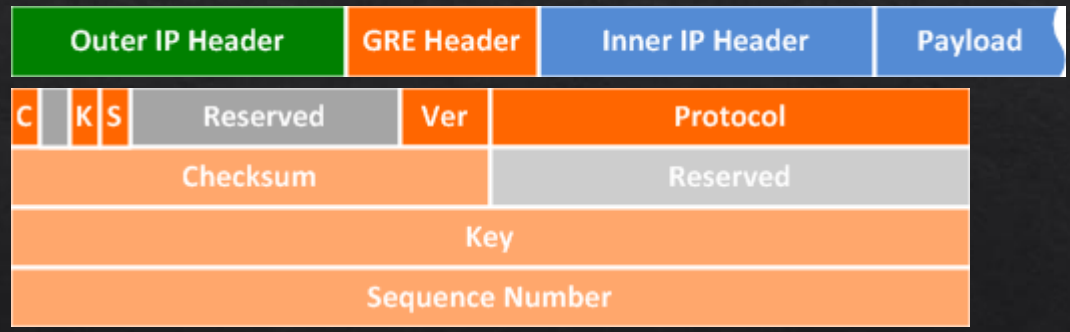
IP-in-IP encapsulation is exactly what it sounds like: one IP packet encapsulated inside anothe

20 byte overhead (normal IP header)

- GRE

GRE goes a step further than IP-in-IP, adding an additional header of its own between the inside and outside IP headers.

20 +4 to 16 bytes, depending on which optional features have been enabled



- EoIP

Ethernet over IP (EoIP) Tunneling is a MikroTik RouterOS protocol that creates an Ethernet tunnel between two routers on top of an IP connection.

42 byte overhead (8byte GRE + 14 byte Ethernet + 20 byte IP)

Źródło: Wikipedia https://pl.wikipedia.org/wiki/Virtual_Private_Network https://pl.wikipedia.org/wiki/Tunel_(informatyka) http://packetlife.net https://wiki.mikrotik.com

Trochę Praktyki
+
Bonus: Ułatwienia Mikrotika

2. Jak optymalnie ustawić trasy komunikacji?

I dlaczego OSPF

Trasowanie (ang. *routing*, ruting, rutowanie) – wyznaczanie trasy i wysłanie nią pakietu danych w sieci komputerowej.

1. Routing Statyczny

ECMP is a routing strategy where next-hop packet forwarding to a single destination can occur over multiple "best paths" which tie for top place in routing metric calculation

2. Routing Dynamiczny

BGP (ang. **Border Gateway Protocol**) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet.

IGMP-proxy Internet Group Management Protocol (IGMP) proxy can be used to implement multicast routing.

Multicast Protocol Independent Multicast - Sparse Mode (PIM-SM or PIM) enables RouterOS to support multicast streaming over network area where routers have PIM set up.

MME (Mesh Made Easy) is a MikroTik routing protocol suited for IP level routing in wireless mesh networks. It is based on ideas from B.A.T.M.A.N. (Better Approach To Mobile Ad-hoc Networking) routing protocol.

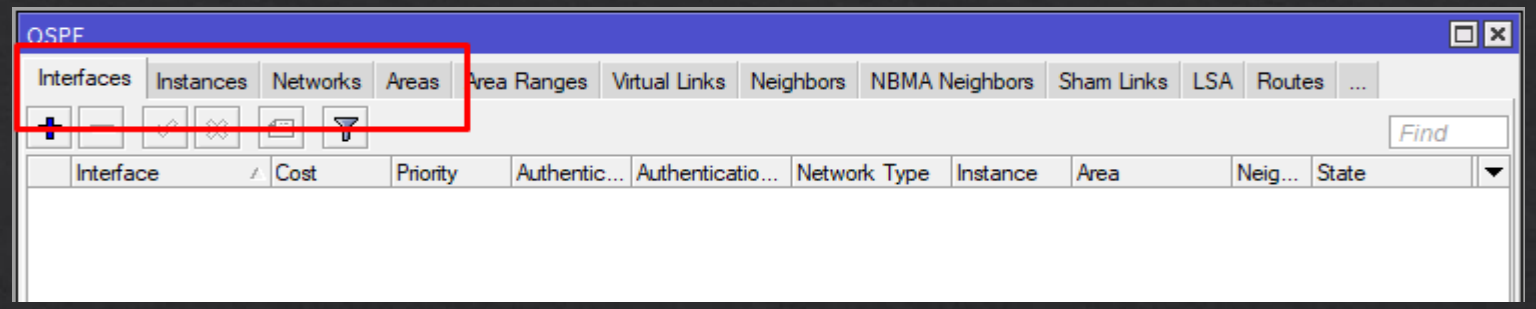
RIP enables routers in an autonomous system to exchange routing information. It always uses the best path (the path with the fewest number of hops (i.e. routers)) available.

OSPF (ang. *Open Shortest Path First*) – s a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS)

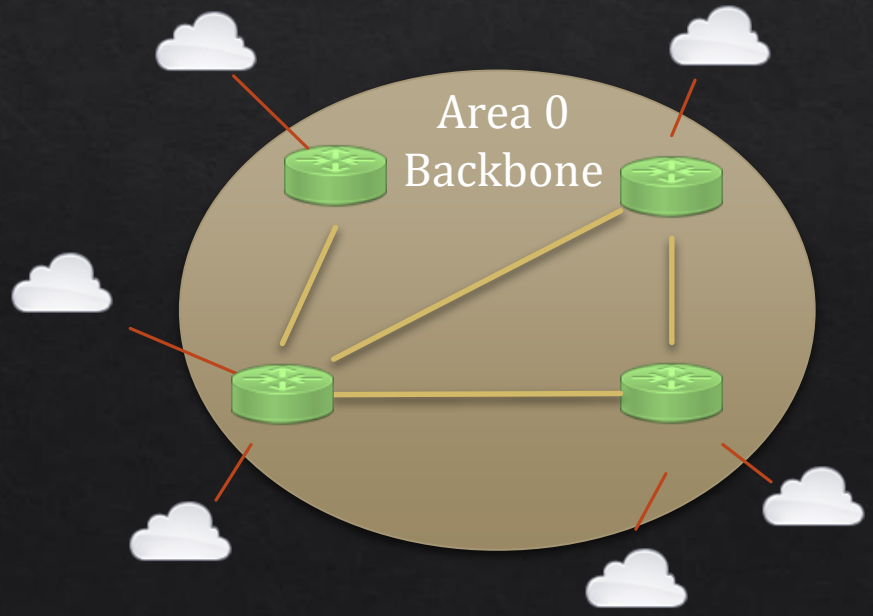
Źródło: Wikipedia https://pl.wikipedia.org/wiki/Open_Shortest_Path_First https://pl.wikipedia.org/wiki/Border_Gateway_Protocol https://wiki.mikrotik.com

2. Jak optymalnie ustawić trasy komunikacji?

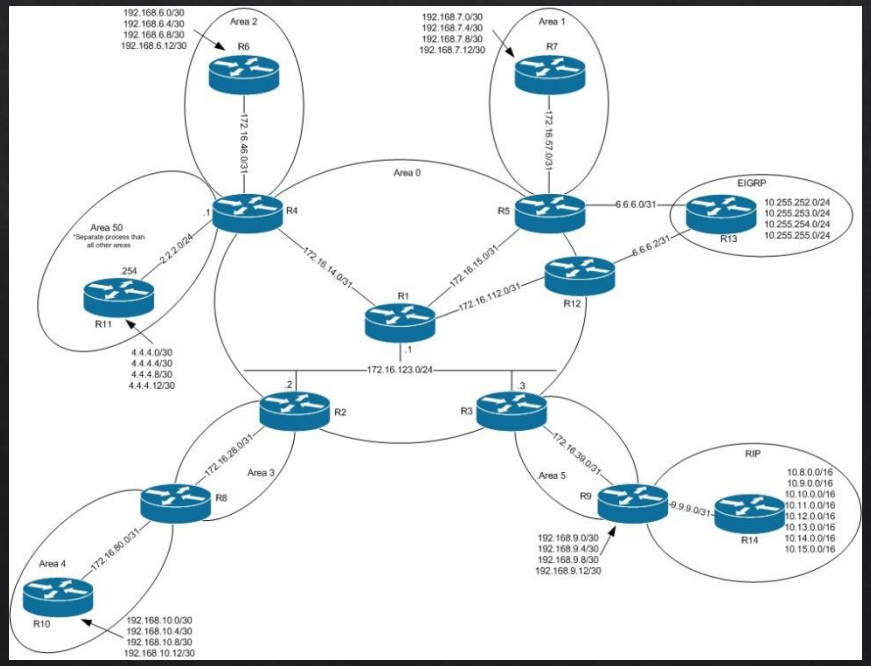
Nie taki OSPF straszny



Jednoobszarowy OSPF



Wieloobszarowy OSPF



https://packetsdropped.wordpress.com/

Trochę Praktyki
+
Kolejne ułatwienie od Mikrotika

Wreszcie Koniec!

Kontakt: buczynsl@gmail.com