Sieci Komputerowe

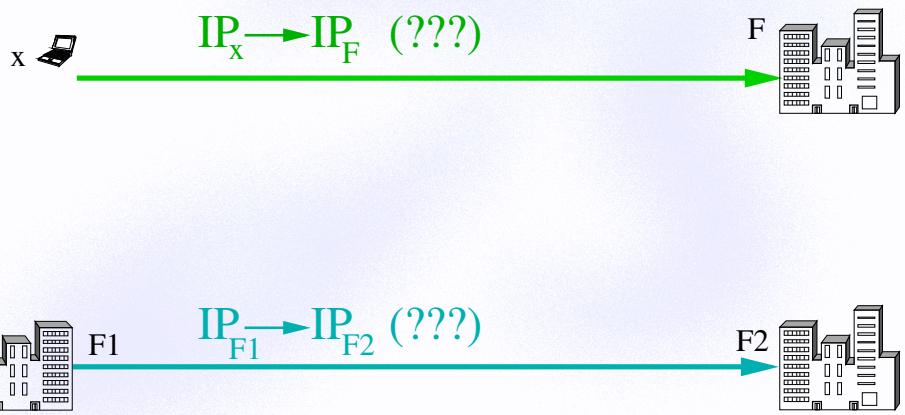
Wirtualne sieci prywatne

mgr inż. Jerzy Sobczyk

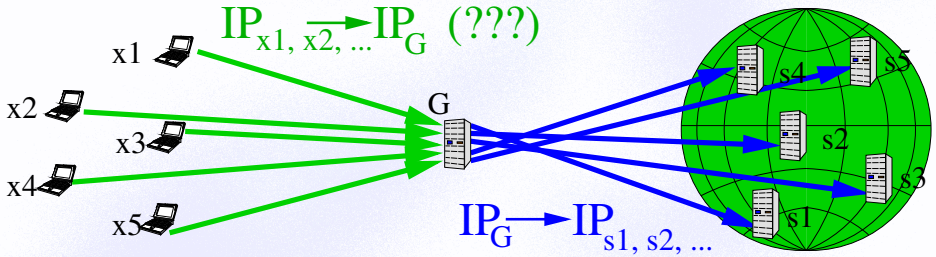
Plan wykładu

- Po co VPN?.
- Jak zabezpieczyć dane?.
- Elementy kryptografii.
- Rodzaje połączeń
- Proste metody.
- Protokół PPTP.
- Protokół L2TP.
- Protokół IPSec.
- Inne protokoły.

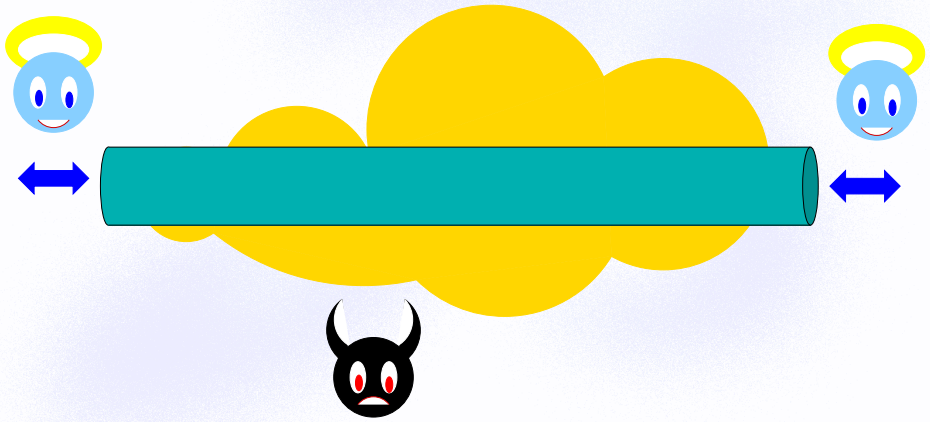
VPN - ochrona danych



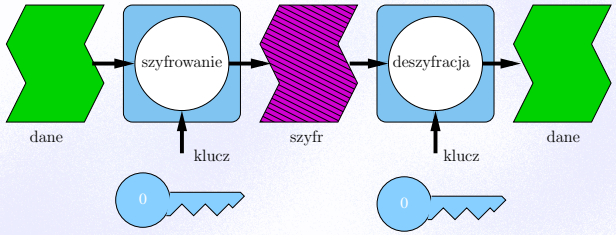
VPN - ukrycie tożsamości



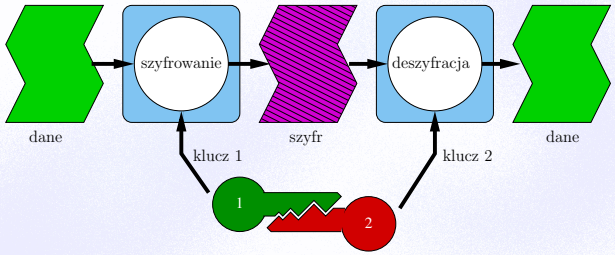
VPN - tunel



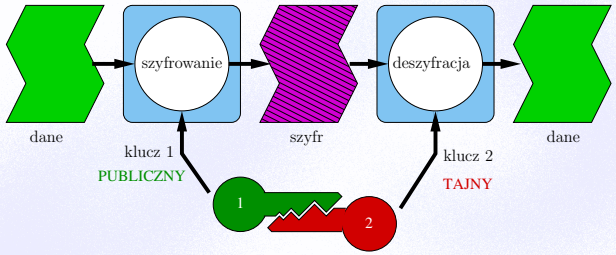
Szyfr symetryczny



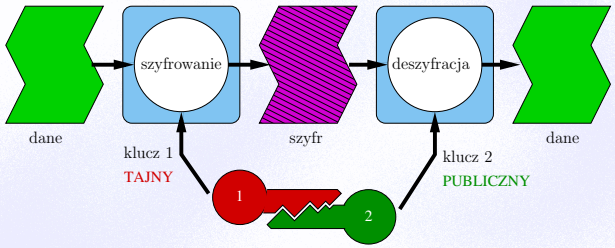
Szyfr asymetryczny



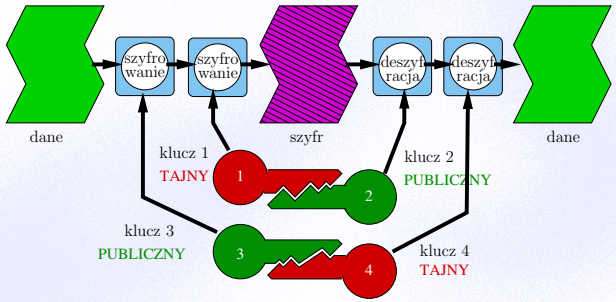
Tajność



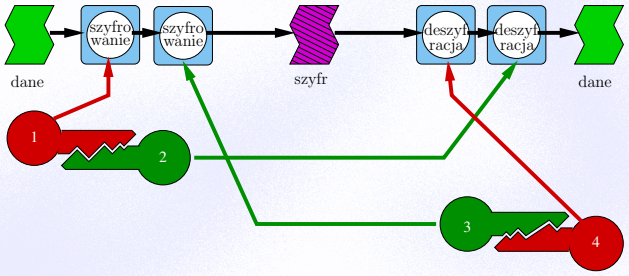
Autentyczność



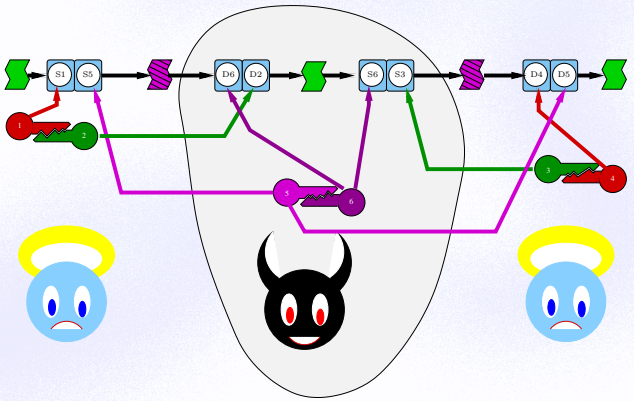
Tajność i autentyczność



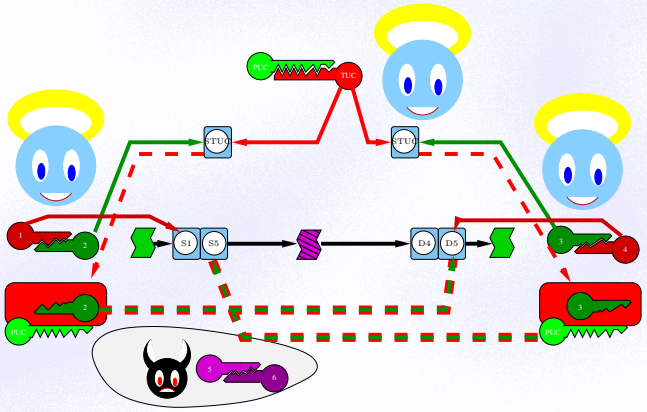
Wymiana kluczy



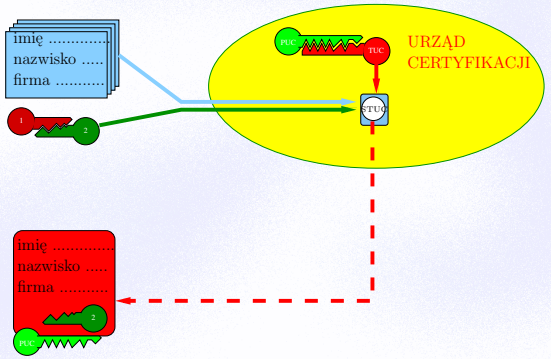
Atak „man in the middle”



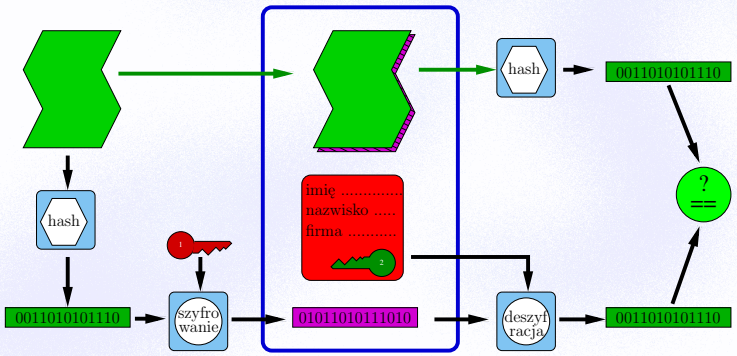
Wymiana certyfikatów



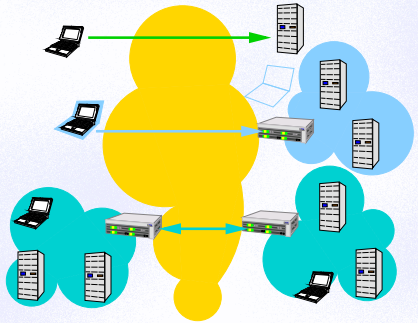
Certyfikat



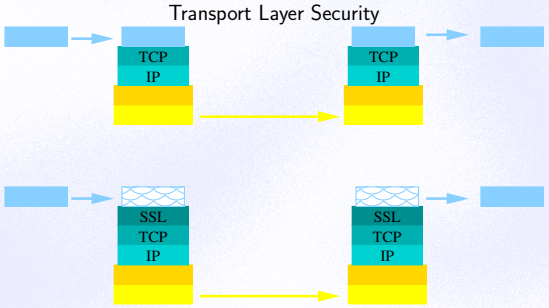
Podpis



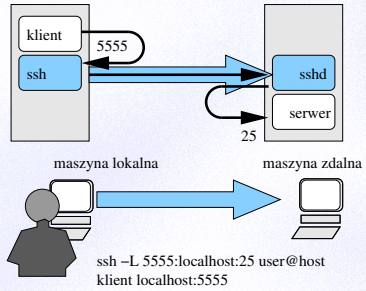
VPN - rodzaje połączeń



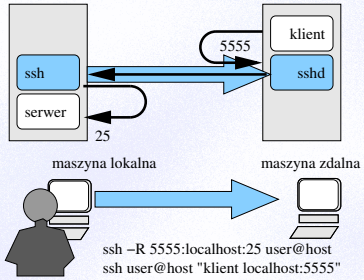
Secure Socket Layer



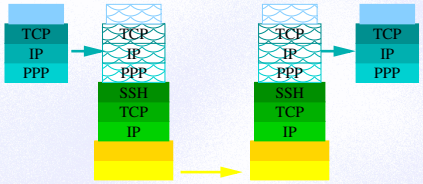
Tunelowanie portów lokalnych w SSH



Tunelowanie portów zdalnych w SSH



TCP over TCP



PPTP

PPTP = Control Connection (port 1723)
+ (PPP + CHAP + RC4)/GRE tunnel

Control Connection Management

Message	Code
Start Ctl. Conn. Request	1
Start Ctl. Conn. Reply	2
Stop Ctl. Conn. Request	3
Stop Ctl. Conn. Reply	4
Echo Request	5
Echo Reply	6

Call Management

Message	Code
Outgoing Call Request	7
Outgoing Call Reply	8
Incoming Call Request	9
Incoming Call Reply	10
Incoming Call Connected	11
Call Claear Request	12
Call Disconnect Notify	13

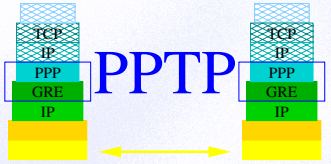
Error Reporting

Message	Code
WAN Error Notify	14

PPP Session Control

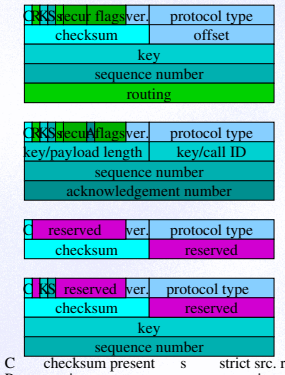
Message	Code
Set link Info	15

Point To Point Tuneling Protocol



http://www.microsoft.com/ntserver/ProductInfo/faqs/PPTPfaq.asp
http://www.schneier.com/pptp-faq.html

Generic Routing Encapsulation



RFC 1701
1994.10

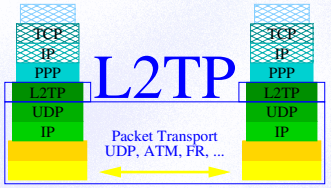
PPTP
1996.06

RFC 2784
2000.03

RFC 2890
2000.10

C	checksum present	s	strict src. route present
R	routing present	recur	recursion control
K	key present	A	acknowledgement present
S	seq. numer present		

Layer 2 Tuneling Protocol - RFC 2661



Layer 2 Tuneling Protocol - RFC 2661

RFC 2661
1999.08

T Type 0=data 1=ctl.
L Length present
S Sequence present (Ns, Nr)
O Offset present
P Priority

Layer 2 Tuneling Protocol

Control Connection Management

Message	Code
Start Ctl. Conn. Request	1
Start Ctl. Conn. Reply	2
Start Ctl. Conn. Connected	3
Stop Ctl. Conn. Notification	4
Hello	6

Call Management

Message	Code
Outgoing Call Request	7
Outgoing Call Reply	8
Outgoing Call Connected	9
Incoming Call Request	10
Incoming Call Reply	11
Incoming Call Connected	12
Call Disconnect Notify	14

Error Reporting

Message	Code
WAN Error Notify	15

PPP Session Control

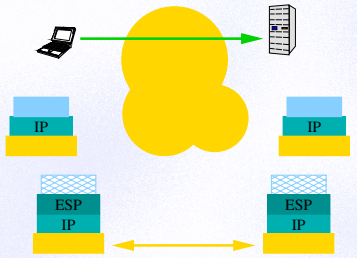
Message	Code
Set link Info	16

IPSec

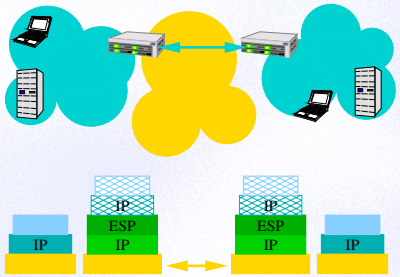
IPSec = AH + ESP + IPcomp + IKE

AH	Authentication Header RFC 1826, **2402**	authentication
ESP	Encapsulating Security Payload RFC 1827, **2406**	authentication + encryption
IPcomp	IP payload compression RFC 2393, **3173**	compression
IKE	Internet Key Exhange RFC **2409**	key negotiation porty 500,4500 UDP
ISAKMP	Internet Security Association and Key Management Protocol RFC **2408**	key management port 500 UDP

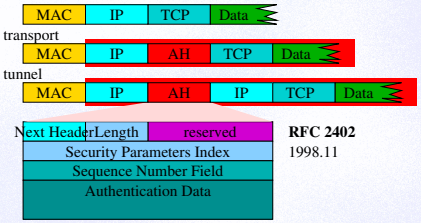
IPSec - transport mode



IPSec - tunnel mode

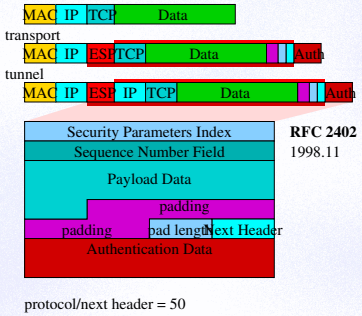


IPSec - Authentication Header - RFC 2402



protocol/next header = 51

IPSec - Encapsulating Security Payload - RFC 2406



protocol/next header = 50

IPSec - uwagi

Niels Ferguson and Bruce Schneier - 1998

http://www.schneier.com/paper-ipsec.html

	Lessons
	Security's worst enemy is complexity.
1	Cryptographic protocols should not be developed by a committee.
2	The documentation of a system should include introductory material, an overview for first-time readers, stated goals, rationale, etc.
3	Authenticate not just the message, but everything that is used to determine the meaning of the message.

	Recommendations
1	Eliminate transport mode.
2	Eliminate the AH protocol.
3	Modify ESP to always provide authentication; only encryption should be optional.
4	Modify the ESP protocol to ensure that it authenticates all data used in the deciphering of the payload.

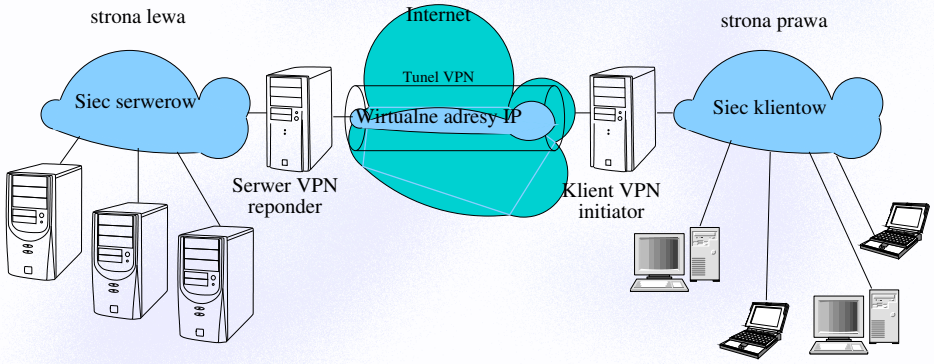
https://www.schneier.com/wp-content/uploads/2016/02/paper-ipsec.pdf

https://www.schneier.com/academic/archives/2003/12/a_cryptographic_eval.html

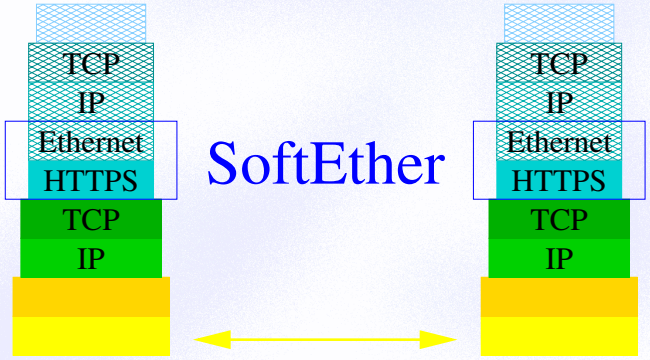
Oprogramowanie

Program	Protokoły	Uwagi
softether	OpenVPN, L2TP, SSTP, EtherIP, SoftEther=Ethernet over HTTPS	Może działac z IPv4 i IPv6
openvpn	OpenVPN = SSL/TLS;	Płatny lub darmowy
strongswan	IKEv2+IPSec	Podobne programy: FreeS/WAN, OpenSwan, LibreSwan
streisand	L2TP, OpenConnect, OpenSSH, OpenVPN, Shadowsocks, Stunnel, Tor bridge, WireGuard;	Skoncentrowany na ochronie prywatności
wireguard	WireGuard=SSL/UDP	
algo	IKEv2, WireGuard;	
pptp-linux, pptpd	PPTP	Protokół PPP ma problemy z bezpieczeństwem - nie polecany.
sstp-client	SSTP	Klient protokołu SSTP firmy Microsoft.

Adresy virtualne



SoftEther



https://www.softether.org/1-features/1._Ultimate_Powerful_VPN_Connectivity

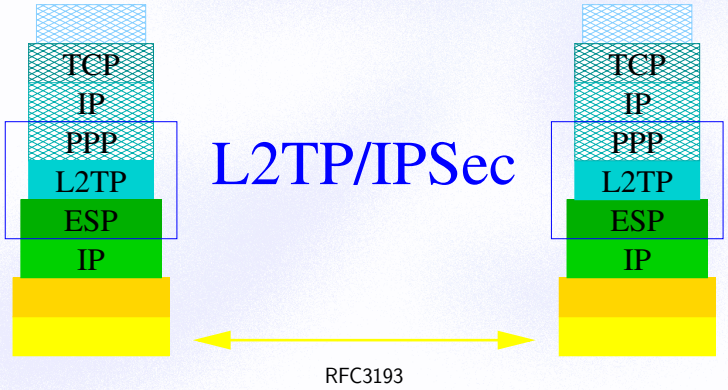
MS-SSTP

Secure Socket Tunneling Protocol

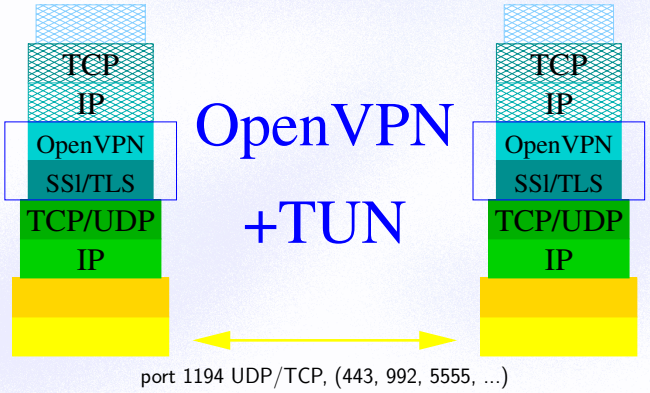
RFC1945, RFC2616 RFC2818

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-sstp/70adc1df-c4fe-4b02-8872-f1d8b9ad806a

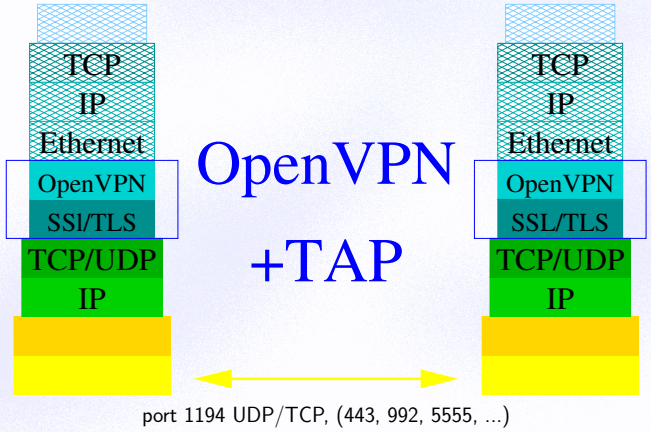
L2TP/IPSec



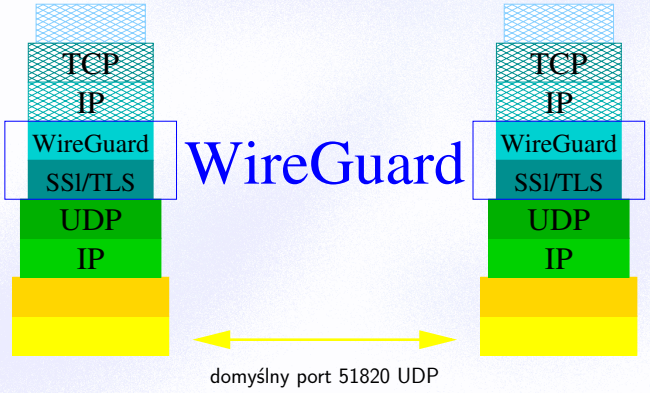
IP / OpenVPN



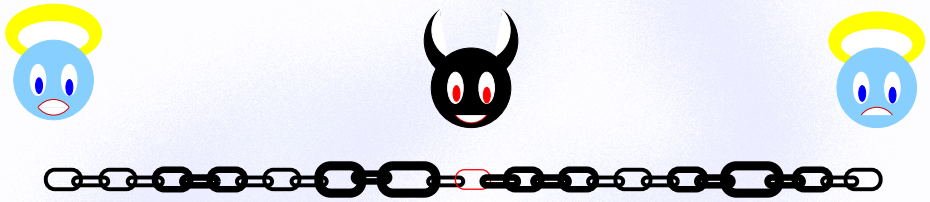
Ethernet / OpenVPN



WireGuard



Najsłabsze ogniwo!



Dziękuję za uwagę

mgr inż. Jerzy Sobczyk