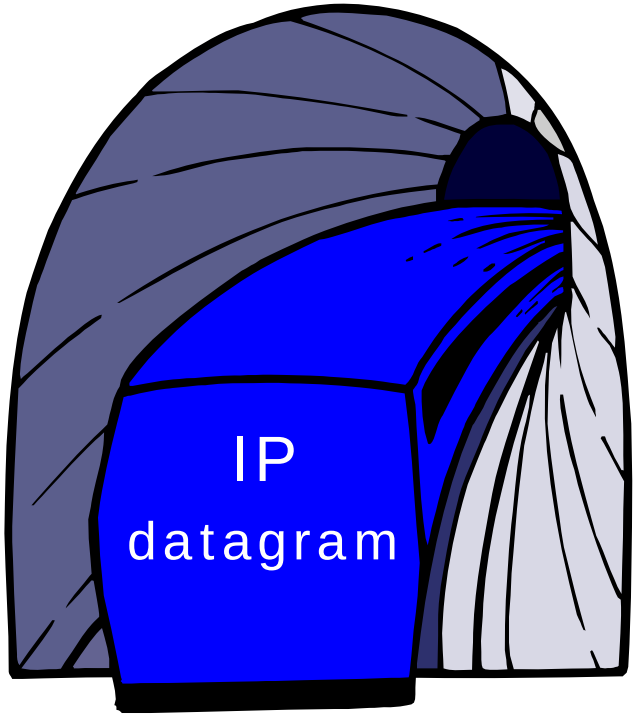
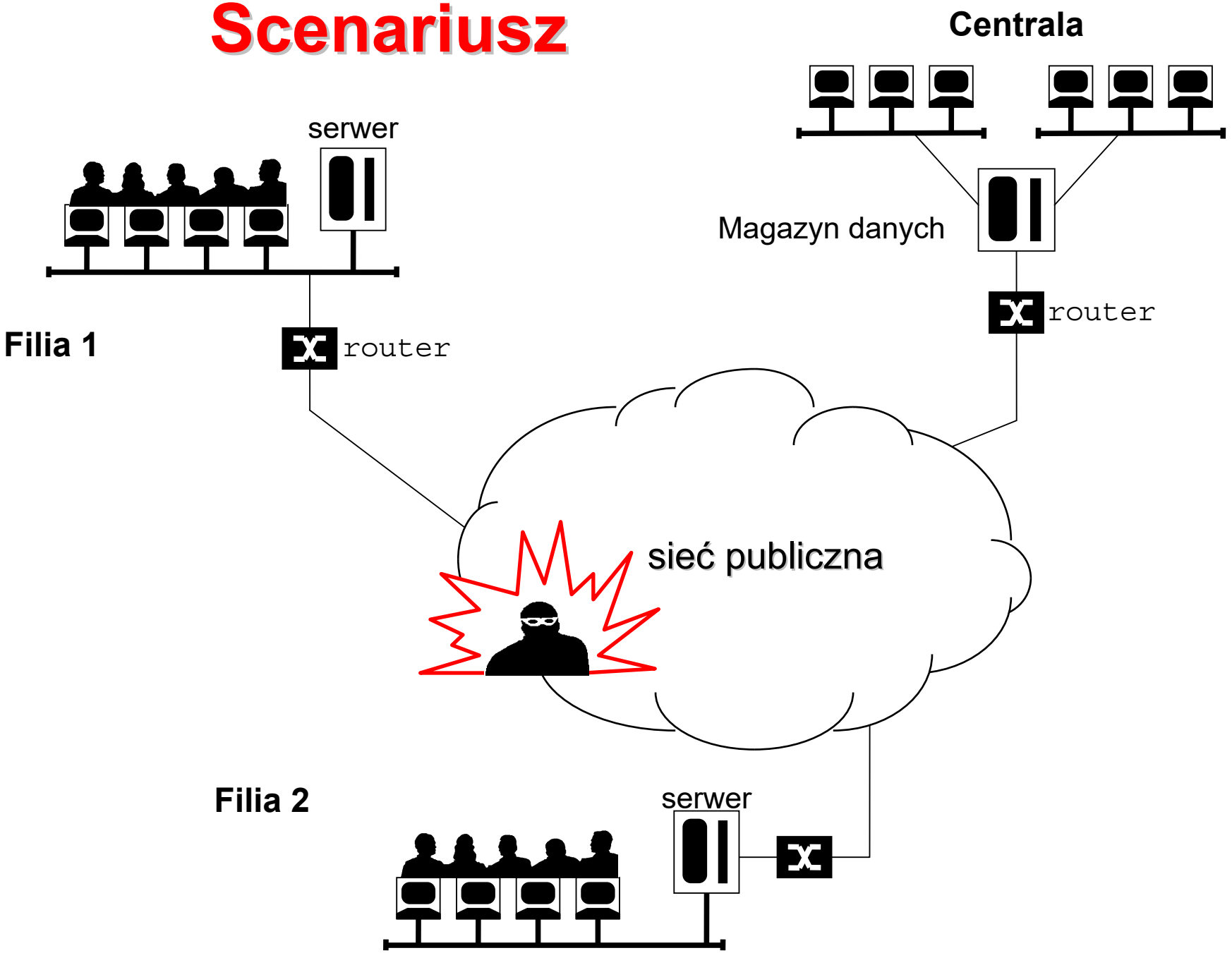
Tunele wirtualne VPN



Zagadnienia

1. Rodzaje tuneli wirtualnych
2. Tunele wirtualne IP (IPsec)
3. Tunele wirtualne SSL/TSL
4. WireGuard
5. Produkty

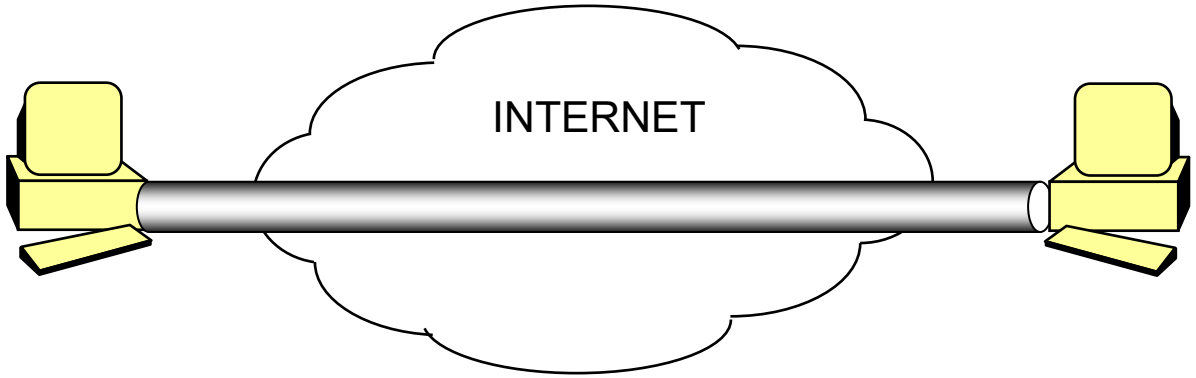
Scenariusz


Centrala
serwer
Magazyn danych
router
Filia 1
router
sieć publiczna
Filia 2
serwer

Tunele wirtualne

Konfiguracje

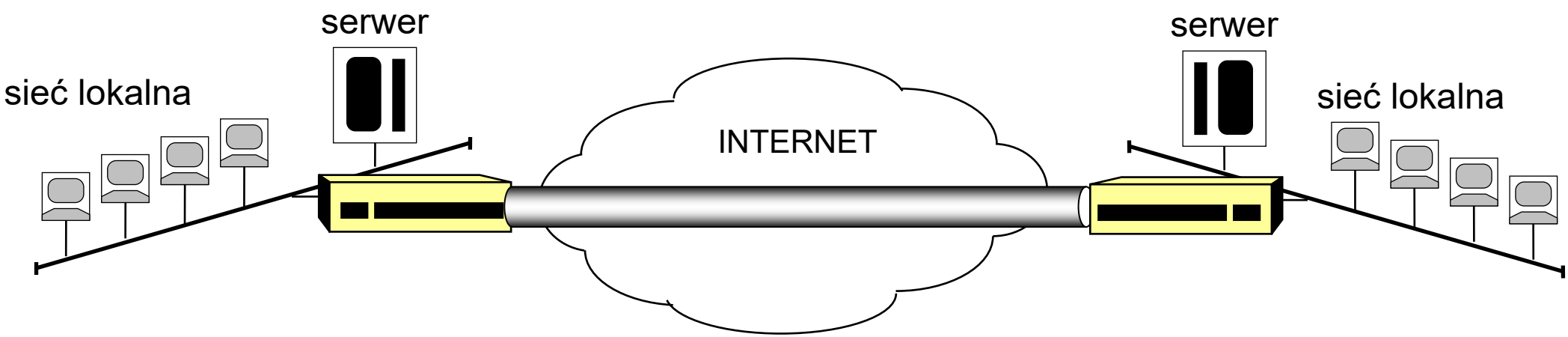
host-to-host



Tunele wirtualne

Konfiguracje

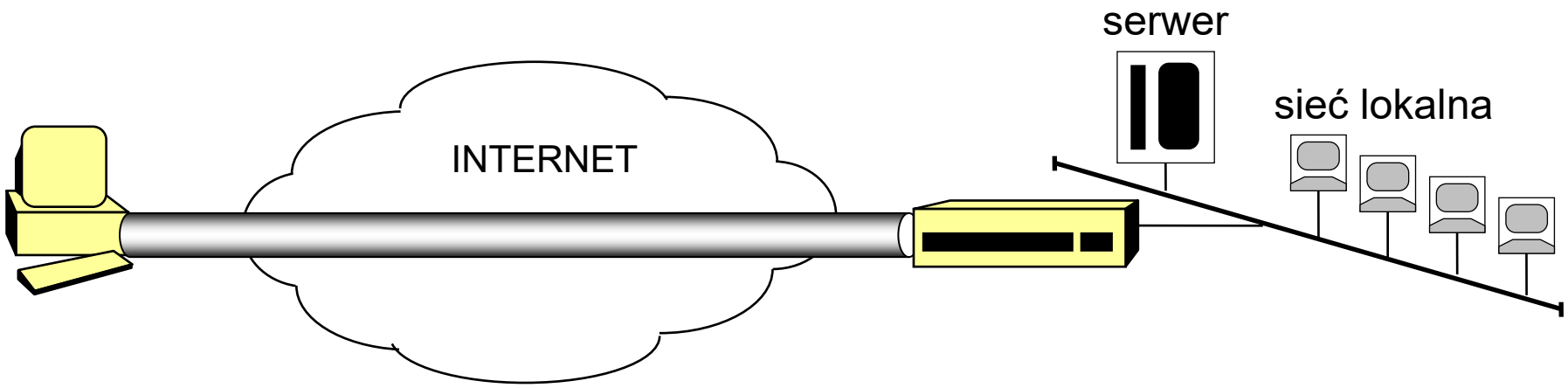
net-to-net



Tunele wirtualne

Konfiguracje

host-to-net



“road warrior”

Tunele wirtualne

VPN chroni przed:

- sniffingiem
- IP spoofingiem
- TCP spoofingiem
- session hijackingiem
- SYN floodingiem
- ...

IPsec

- w IPv4 brak jakichkolwiek mechanizmów bezpieczeństwa
- w 1995 r. IETF przedstawił pierwszą wersję specyfikacji protokołów IPsec (RFC 1825):
  - Encapsulating Security Payload (ESP) – protokół nr 50
  - Authentication Header (AH) – protokół nr 51
- ... których zadaniem jest transparentne dla aplikacji (warstwa sieciowa) wykorzystanie narzędzi kryptograficznych w celu osiągnięcia
  - poufności → ESP
  - integralności → AH
- wkrótce rozszerzono funkcje ESP o ochronę integralności

IPsec

Dlaczego oddzielne składniki AH i ESP:

- AH wystarcza w wielu zastosowaniach, np. DNS
- AH prostszy i łatwiejszy w implementacji, np. IoT (?)
- ograniczenia natury polityczno-prawnej, związane ze stosowaniem kryptografii:

  AH wykorzystując wyłącznie kryptograficzne funkcje skrótu, z reguły traktowane bardziej liberalnie, miał zapewniać ograniczone bezpieczeństwo tam, gdzie szyfrowanie danych było niemożliwe z powodu lokalnych zakazów lub braku możliwości wyeksportowania w pełni funkcjonalnych urządzeń.

IPsec

IPsec (RFC 2401 1998 r., RFC 4301 2005 r.):

AH (Authentication Header, RFC 2402)

- realizuje kontrolę integralności datagramu IP

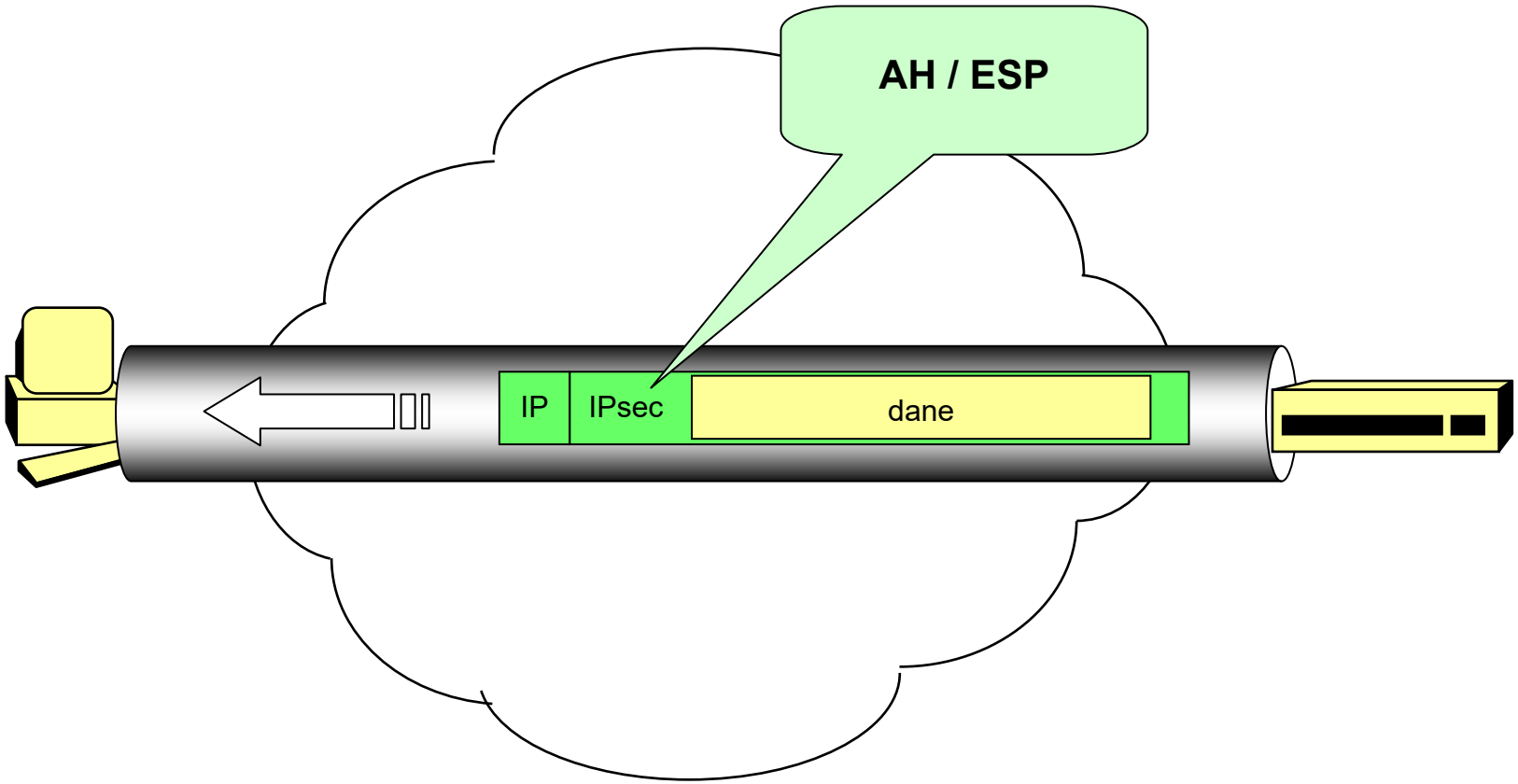
ESP (Encapsulating Security Payload, RFC 2406)

- zapewnia integralność i poufność treści datagramu IP

- IPsec jest zintegrowaną częścią specyfikacji protokołu IPv6
- zatem w protokole IPv6 możliwe jest korzystanie z nagłówków AH i ESP jak z dowolnych innych opcji

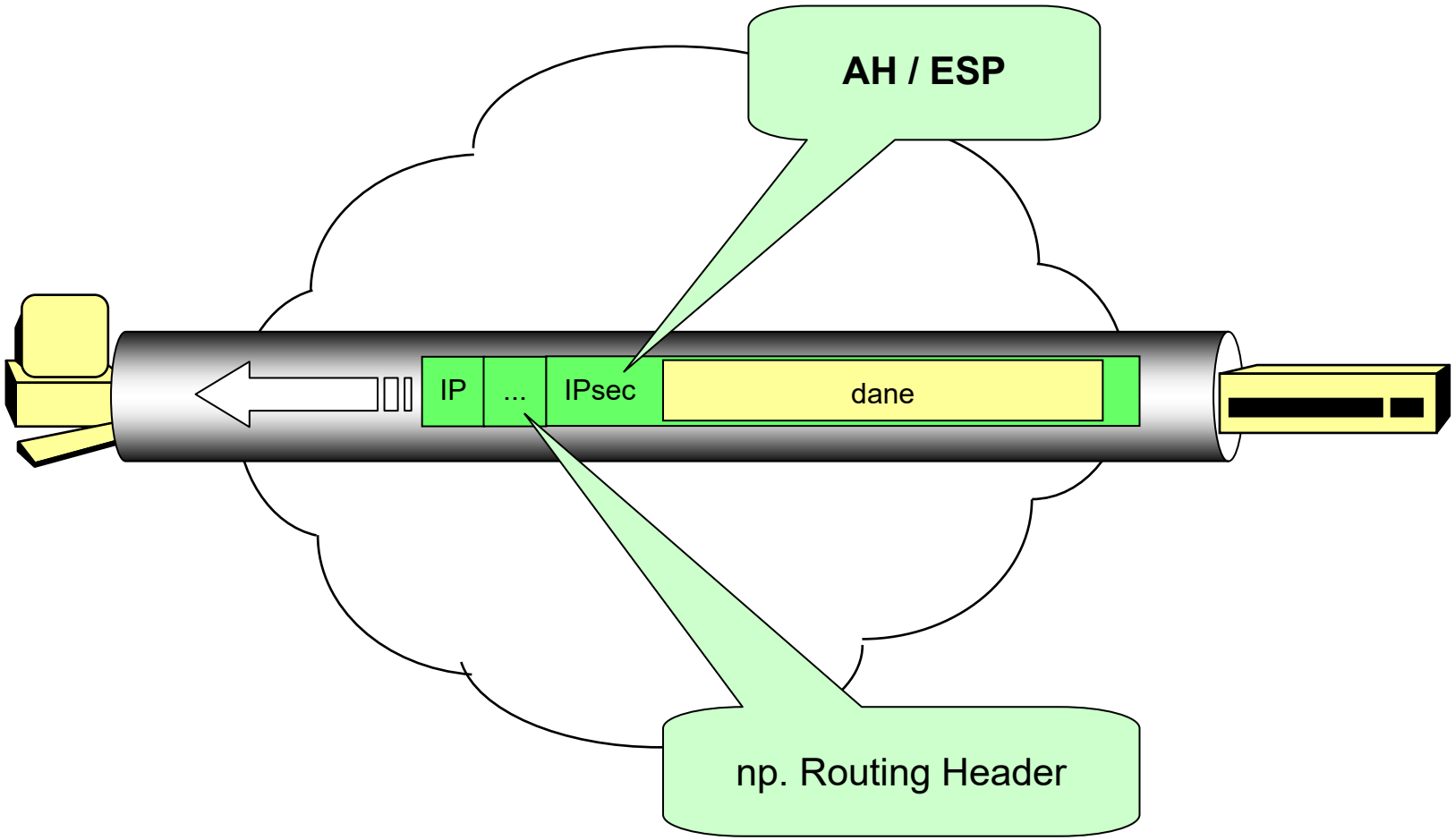
IPsec

- nagłówek IPsec musi być umieszczony bezpośrednio przed zabezpieczanymi danymi



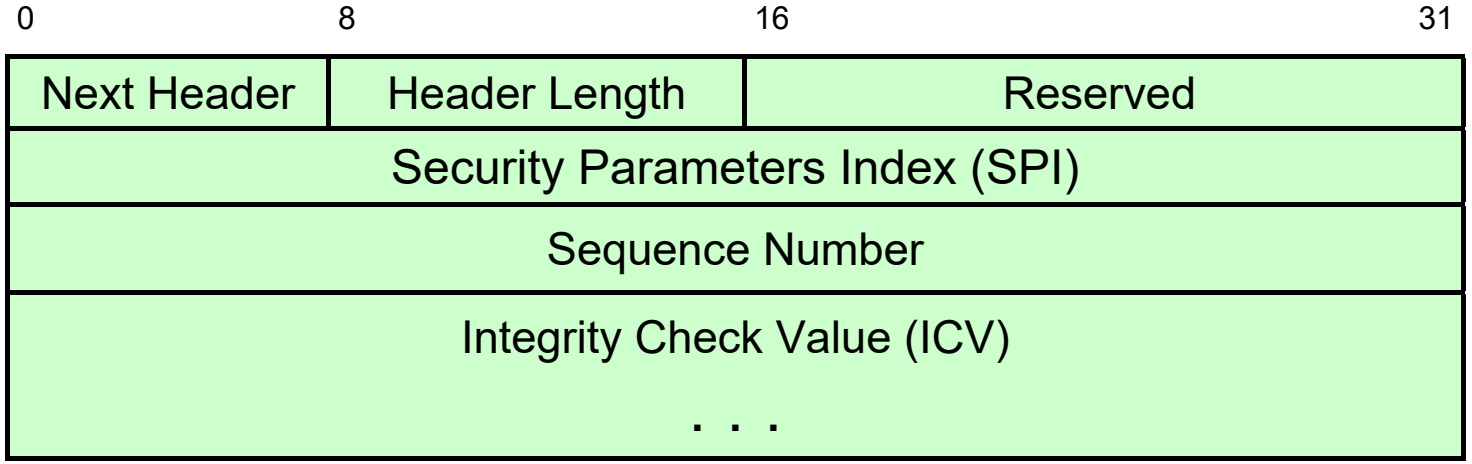
IPsec

- nagłówek IPsec musi być umieszczony bezpośrednio przed zabezpieczanymi danymi



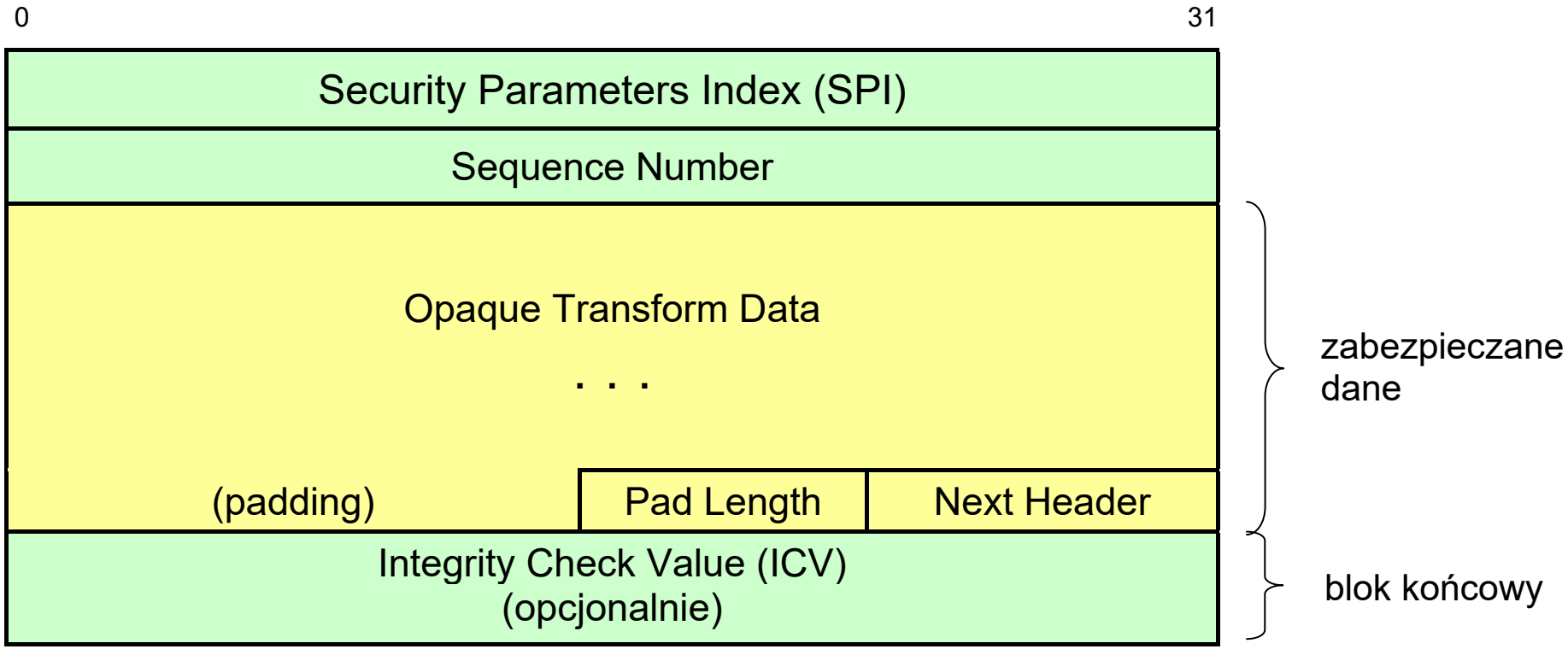
AH (Authentication Header)

- ICV = szyfrowany skrót treści datagramu oraz stałych pól nagłówka IP (lub nagłówka podstawowego IPv6)
- funkcje skrótu MD5, SHA-1, SHA-2, RIPEMD-160 lub inne (negocjowane)



ESP (Encapsulating Security Payload)

- szyfry blokowe w trybie CBC, np. DES, 3DES, Blowfish, CAST-128
- aktualnie również AES, w tym *Authenticated encryption mode*, np. AES-GCM



IPsec

Możliwe jest połączenie mechanizmów AH i ESP

1. najpierw szyfrowane są dane za pomocą ESP, a następnie cały datagram jest zabezpieczony przez AH

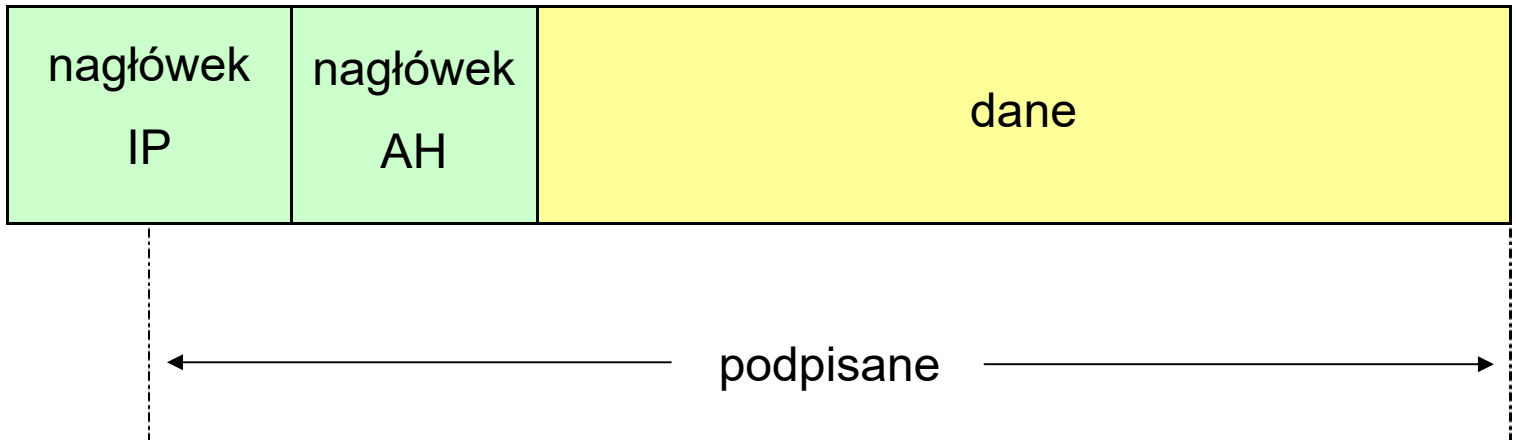
2. najpierw wyznacza się nagłówek AH i umieszcza się go w datagramie, a następnie szyfruje całość przez ESP

Tryby pracy

Tryb transportowy/bezpośredni (*transport mode*)

– do datagramu IP dodany jest nagłówek AH / ESP i dane datagramu (IP SDU, czyli ramka TCP, UDP, ICMP, ...) zostają zabezpieczone (podpisane / zaszyfrowane) bezpośrednio za nim

AH:

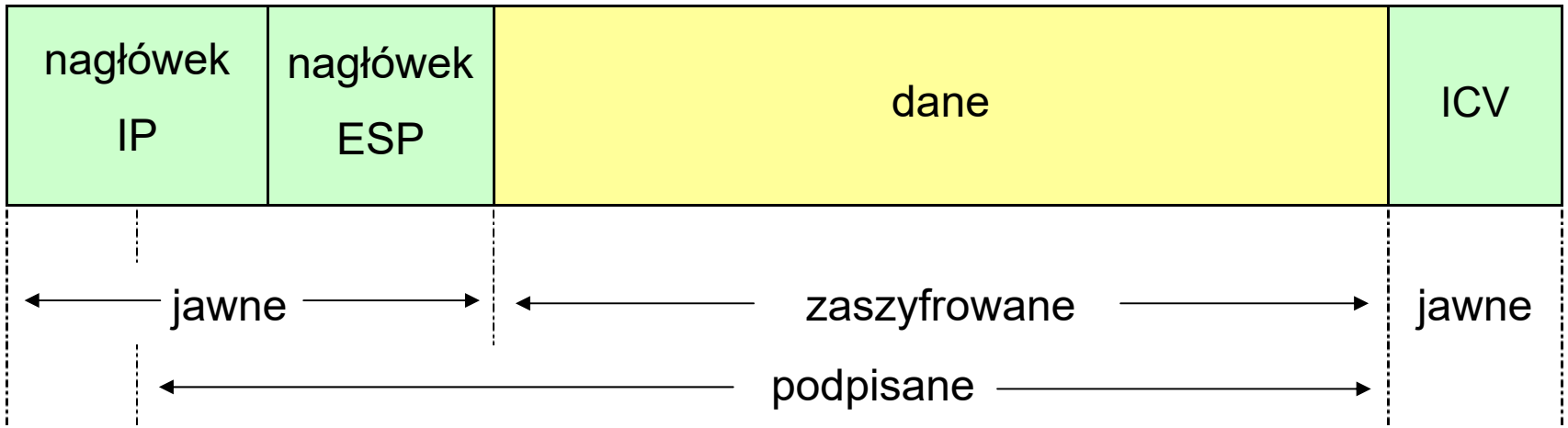


Tryby pracy

Tryb transportowy/bezpośredni (*transport mode*)

– do datagramu IP dodany jest nagłówek AH / ESP i dane datagramu (IP SDU, czyli ramka TCP, UDP, ICMP, ...) zostają zabezpieczone (podpisane / zaszyfrowane) bezpośrednio za nim

ESP:

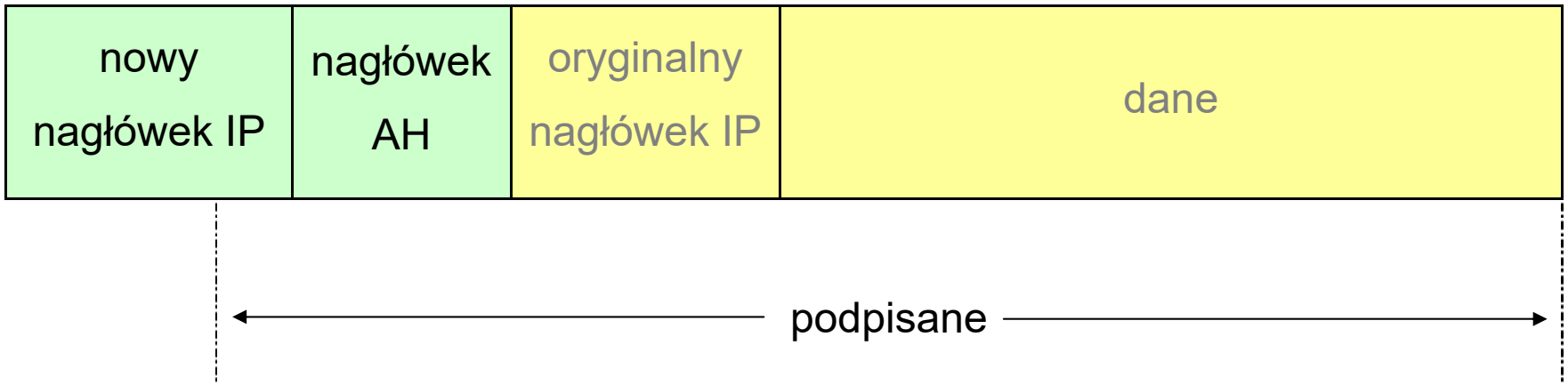


Tryby pracy

Tryb tunelowy (*tunnel mode*)

– oryginalny datagram IP (IP PDU) zostanie zabezpieczony w całości, a następnie umieszczony wraz z nagłówkiem protokołu IPsec w nowym datagramie IP jako jego dane (SDU)

AH:

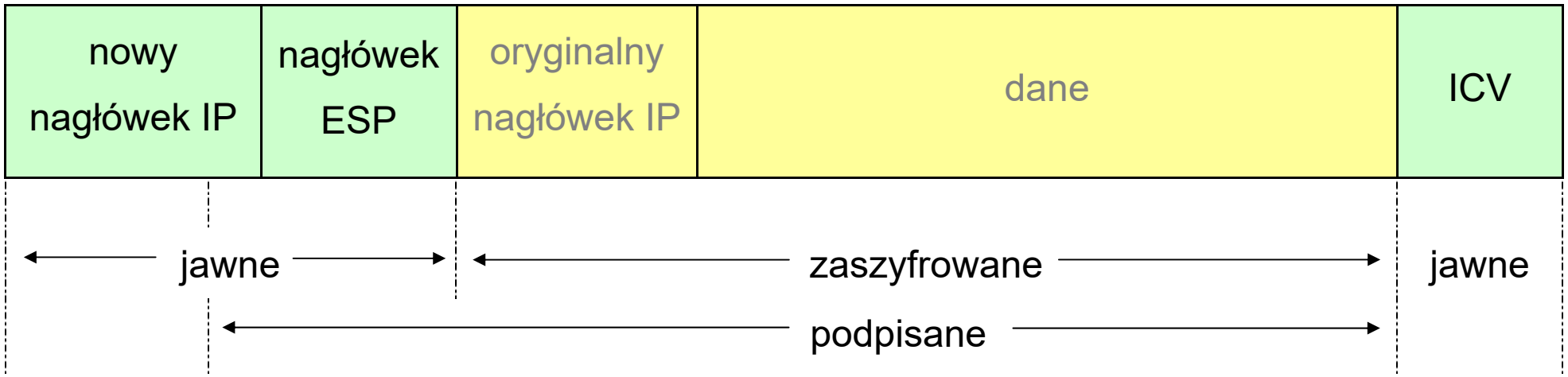


Tryby pracy

Tryb tunelowy (*tunnel mode*)

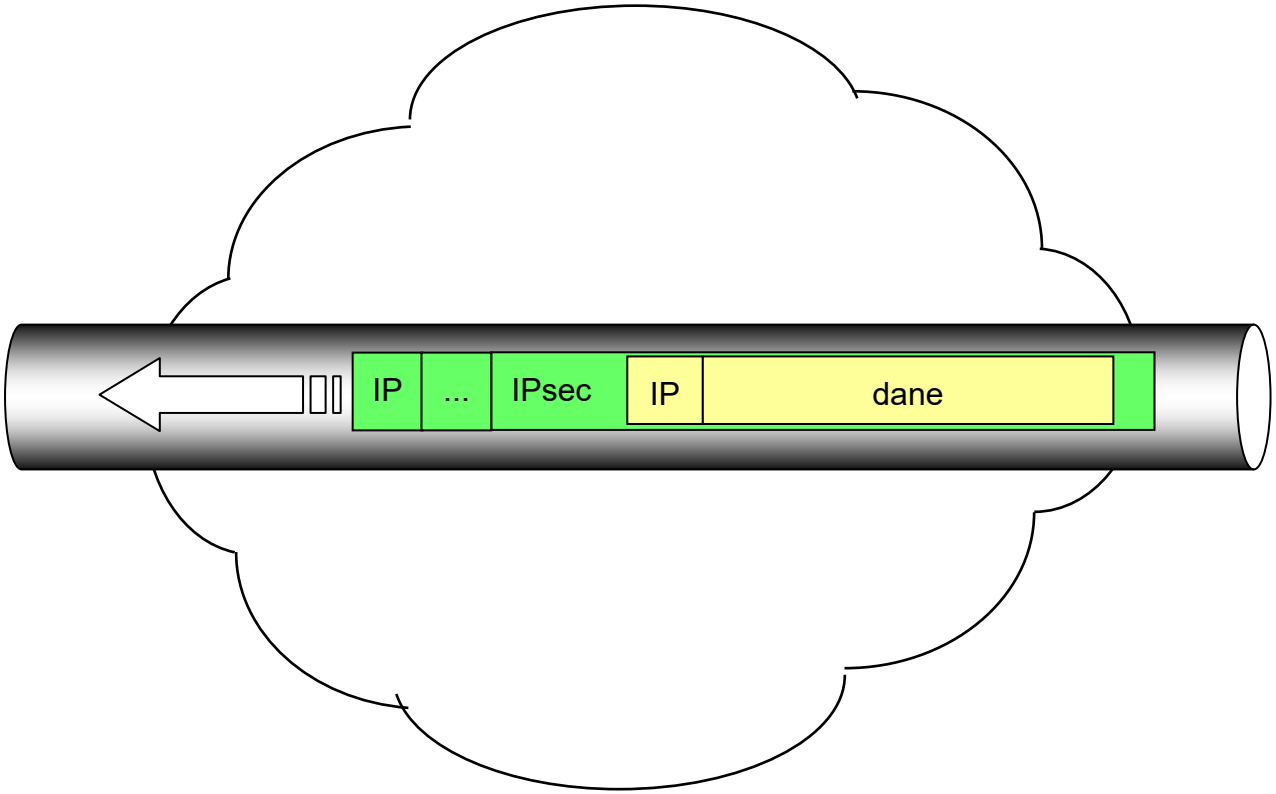
– oryginalny datagram IP (IP PDU) zostanie zabezpieczony w całości, a następnie umieszczony wraz z nagłówkiem protokołu IPsec w nowym datagramie IP jako jego dane (SDU)

ESP:



Tryby pracy

Tryb tunelowy (*tunnel mode*)



- który tryb jest dogodniejszy dla konfiguracji host-to-host, net-to-net, host-to-net?

IPsec

Protokół

- **połączeniowy**

czy

- **bezpołączeniowy**

IPsec

Asocjacja bezpieczeństwa (*Security Association*)

- zbiór parametrów charakteryzujących bezpieczną komunikację między nadawcą a odbiorcą (kontekst), utrzymywany przez nadawcę i unikalnie identyfikowany przez SPI (*Security Parameters Index*)
- asocjacja bezpieczeństwa (blok parametrów asocjacji) nie jest przesyłana siecią – przesyłany jest tylko SPI
- asocjacja bezpieczeństwa jest jednokierunkowa – w łączności obukierunkowej wymagane są dwie asocjacje – daje to dużą elastyczność ruch w każdym kierunku może być szyfrowany innym kluczem i może mieć inny okres ważności
- kanały SA mogą się wzajemnie w sobie zawierać i nie muszą się zaczynać w tych samych miejscach (na tych samych stacjach)

IPsec

Blok parametrów asocjacji:

rodzaj metody użytej do podpisu AH
klucze wykorzystane w tej metodzie
rodzaj metody użytej do szyfrowania datagramu w ESP
klucze wykorzystane w tej metodzie
dane inicjujące algorytmy szyfrujące
rodzaj metody użytej do podpisu w ESP
klucze wykorzystane w tej metodzie
czas ważności kluczy
czas ważności asocjacji
adresy IP mogące współdzielić asocjację
opcjonalna etykieta poziomu bezpieczeństwa (tajne, ściśle tajne itd.)

IPsec

Schemat działania

Działania wykonywane przy wysyłaniu pakietu:

1. Sprawdzenie czy i w jaki sposób wychodzący pakiet ma być zabezpieczony:
   - sprawdzenie polityki bezpieczeństwa w SPD (*Security Policy Database*)
   - jeśli polityka bezpieczeństwa każe odrzucić pakiet to pakiet jest odrzucany
   - jeśli pakiet nie musi być zabezpieczany to jest wysyłany
2. Ustalenie, które SA powinno być zastosowane do pakietu:
   - odszukanie istniejącego SA w bazie SAD (*SA Database*) lub
   - nawiązanie odpowiedniego SA jeśli nie jest jeszcze nawiązane
3. Wykonanie zabezpieczeń wykorzystując algorytmy i parametry zawarte w SA:
   - wynikiem jest stworzenie nagłówka AH lub ESP
   - dodatkowo może zostać również utworzony nowy nagłówek IP (w trybie tunelowym)
4. Wysłanie powstałego pakietu IP

IPsec

Schemat działania

Działania wykonywane przy odbieraniu pakietu

1. Sprawdzenie nagłówka IPsec:
   - odszukanie odpowiedniego SA w SAD na podstawie SPI zawartego w nagłówku
   - i postępowanie zgodnie z informacjami zawartymi w SA
   - jeśli SA wskazywany przez SPI nie istnieje, to pakiet jest odrzucany
2. Sprawdzenie czy i jak pakiet powinien był być zabezpieczony:
   - sprawdzenie polityki bezpieczeństwa w SPD
   - jeśli polityka bezpieczeństwa każe odrzucić pakiet to pakiet jest odrzucany
   - jeśli zabezpieczenia pakietu nie odpowiadają polityce bezpieczeństwa to pakiet jest odrzucany
   - jeśli pakiet był zabezpieczony prawidłowo to przekazywany jest wyżej

IPsec

Skąd biorą się

- parametry SA

w tym

- **klucze**

IPsec

Zarządzanie SA i kluczami

Zarządzanie SA i dystrybucja kluczy nie są uwzględnione w specyfikacji IPsec !

Możliwe sposoby dystrybucji kluczy:

- dystrybucja ręczna – administrator (małej sieci lokalnej) wyznacza wszystkie klucze
- automatyczne – początkowo myślano o DNS jako repozytorium kluczy (DNSsec)
- ostatecznie wprowadzono nowe protokoły i specyfikacje serwerów kluczy: np. SKIP (Simple Key Management for IP), Photuris, SKEME (Secure Key Exchange MEchanism), IKE (Internet Key Exchange)

IPsec

Zarządzanie SA i kluczami

Protokoły zarządzania SA

(1) wzajemne uwierzytelnianie podmiotów nawiązujących SA,
poprzez np. wspólne hasło (*shared secret*), certyfikaty X.509, klucze PGP, ...

oraz

(2) uzgadnianie kluczy sesji i in. parametrów na potrzeby obu kanałów SA

IPsec

Zarządzanie SA i kluczami

Uwierzytelnianie

- w najprostszym przypadku każda para węzłów musi mieć ustalone wspólne hasło
- wykorzystane do obliczania kluczy metodą Diffiego-Hellmana
- pracochłonne w przypadku dużych sieci
- spotykane rozszerzenie XAUTH umożliwia wykorzystanie protokołu RADIUS
- a często możliwe jest zastosowanie kluczy publicznych podpisanych przez nadrzędny urząd certyfikujący CA (np. certyfikatów X.509)

IPsec

VPN chroni przed:

- sniffingiem
- IP spoofingiem
- TCP spoofingiem
- session hijackingiem
- SYN floodingiem
- ...

} IPsec AH + SA

IPsec

Protokół IKE (*Internet Key Exchange*)

- IKE – RFC 2409 – obejmuje 2 składniki:
  - Internet Security Association and Key Management Protocol (ISAKMP) – RFC 2408
    – protokół negocjacji parametrów IPsec
    – uwierzytelnia strony i zestawia kanał ISAKMP SA (UDP port 500), który wykorzystuje do negocjacji (renegocjacji) IPsec SA
  - Oakley Key Determination Protocol – RFC 2412 – kryptograficzny protokół wymiany kluczy za pomocą algorytmu Diffiego-Hellmana
- ISAKMP stanowi trzon całości i niekiedy nazwy tej używa się zamiennie z IKE
- IKEv2 – RFC 4306 (2005 r.), m.in. ECDH with authentication

IPsec

Protokół IKE

PKI (*Public Key Infrastructure*)

- IKE pozwala wykorzystać możliwości PKI
- po nawiązaniu komunikacji, ale przed uzgodnieniem ISAKMP SA węzeł może zweryfikować autentyczność certyfikatu drugiej strony
- w skrajnym przypadku węzeł nie musi wiedzieć nic o innych węzłach, z którymi będzie się łączył, lub które będą się łączyć z nim
- wymaga to jedynie lokalnego dostępu (zainstalowania w tym węźle) klucza publicznego urzędu CA

IPsec

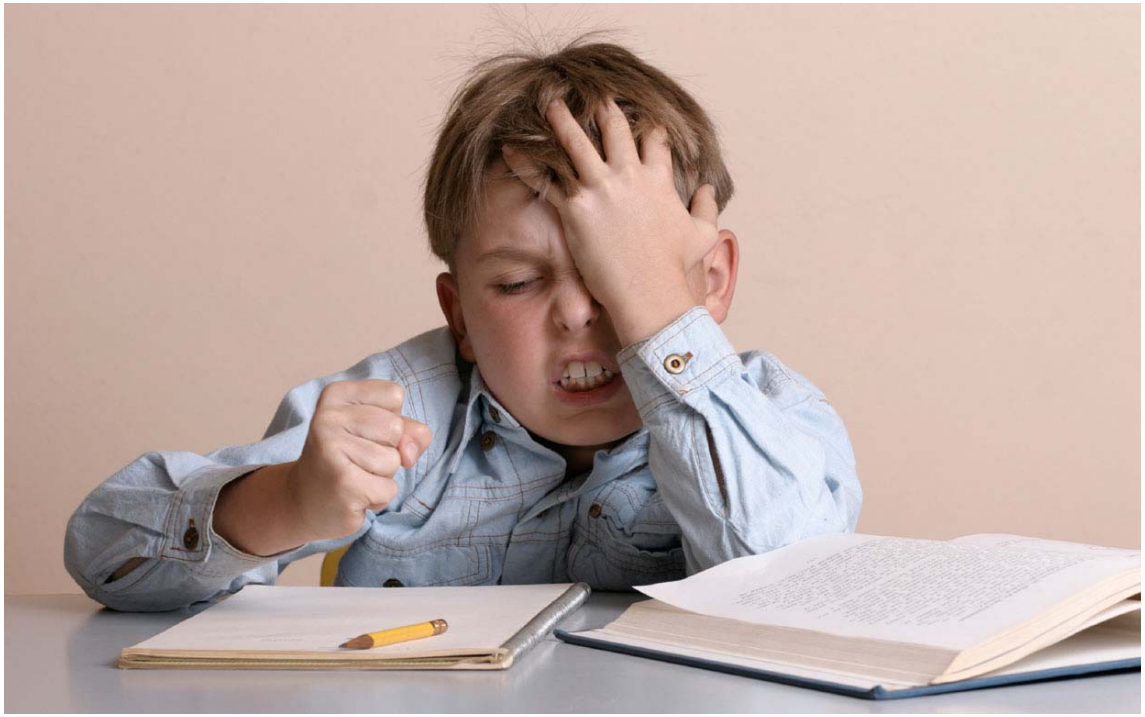
Protokół IKE

Klucze

- IKE umożliwia też automatyczną renegocjację kluczy kryptograficznych co określony interwał (nawet często)
- w razie złamania bieżącego klucza, dane zaszyfrowane poprzednimi i następnymi kluczami nie są zagrożone
- ogranicza to ataki, w których zapisywane są wszystkie przechwycone dane w nadziei, że kiedyś uda mu się uzyskać klucz potrzebny do ich rozszyfrowania
- w przypadku renegocjacji klucza poprzedni klucz jest usuwany z pamięci i włamywacz nie znajdzie go w systemie nawet w przypadku opanowania węzła

HOMEWORK
=
Half Of My Energy Wasted On Random Knowledge

→ Perfect Forward Secrecy



IPsec

Protokół IKE

Rozszerzenia

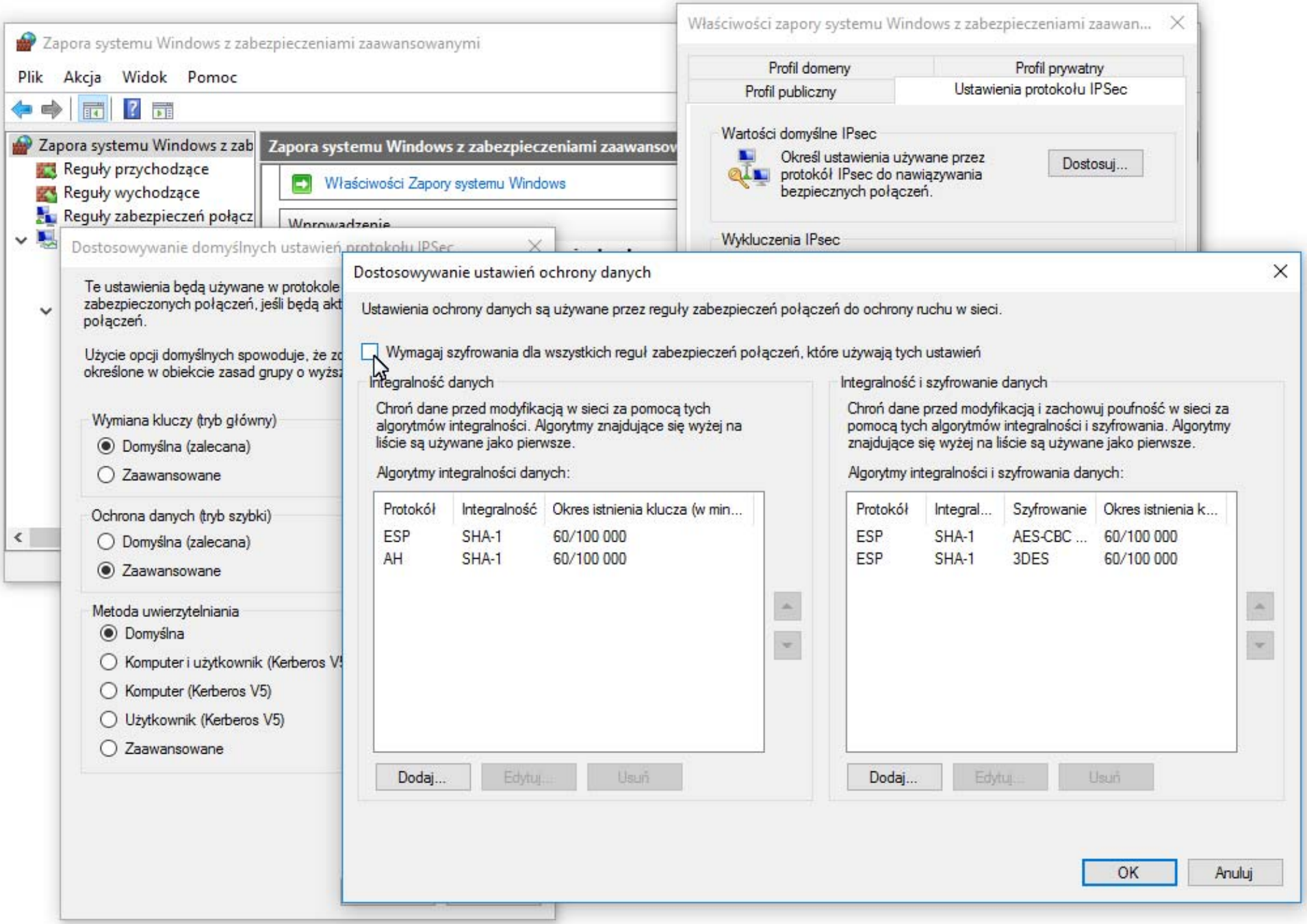
- negocjowane parametry SA można przystosować całkowicie do własnych potrzeb:
  - własny zestaw szyfrów
  - własne mechanizmy uwierzytelnienia
- do uwierzytelniania można wykorzystać EAP (IKEv2)

IPsec w Windows

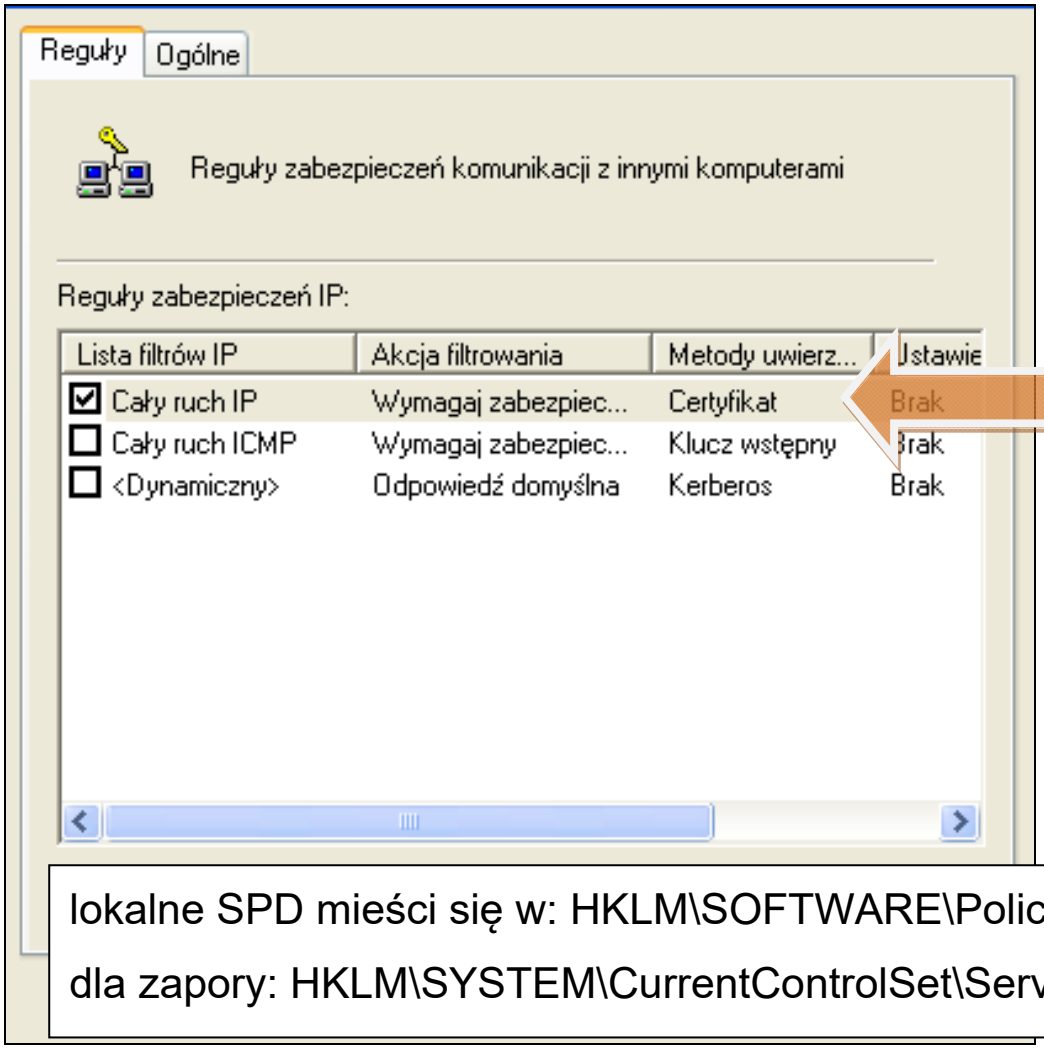
Składniki implementacji

1. sterownik IPsec w jądrze systemu operacyjnego
2. implementacja IKE/ISAKMP (na podstawie porozumienia z Cisco)
   - negocjuje ISAKMP SA i IPsec SA
3. AuthIP (rozszerzenie IKE o obsługę AD i NAP)
4. IPsec Policy Agent
   - pobiera politykę IPsec z lokalnego SPD, z AD lub z lokalnego cache polityk AD
   - przekazuje wymagania polityki do IKE (uwierzytelnianie) i do sterownika (reguły zabezpieczeń w postaci filtrów IP)

IPsec w Windows



IPsec w Windows



Uwierzytelnianie

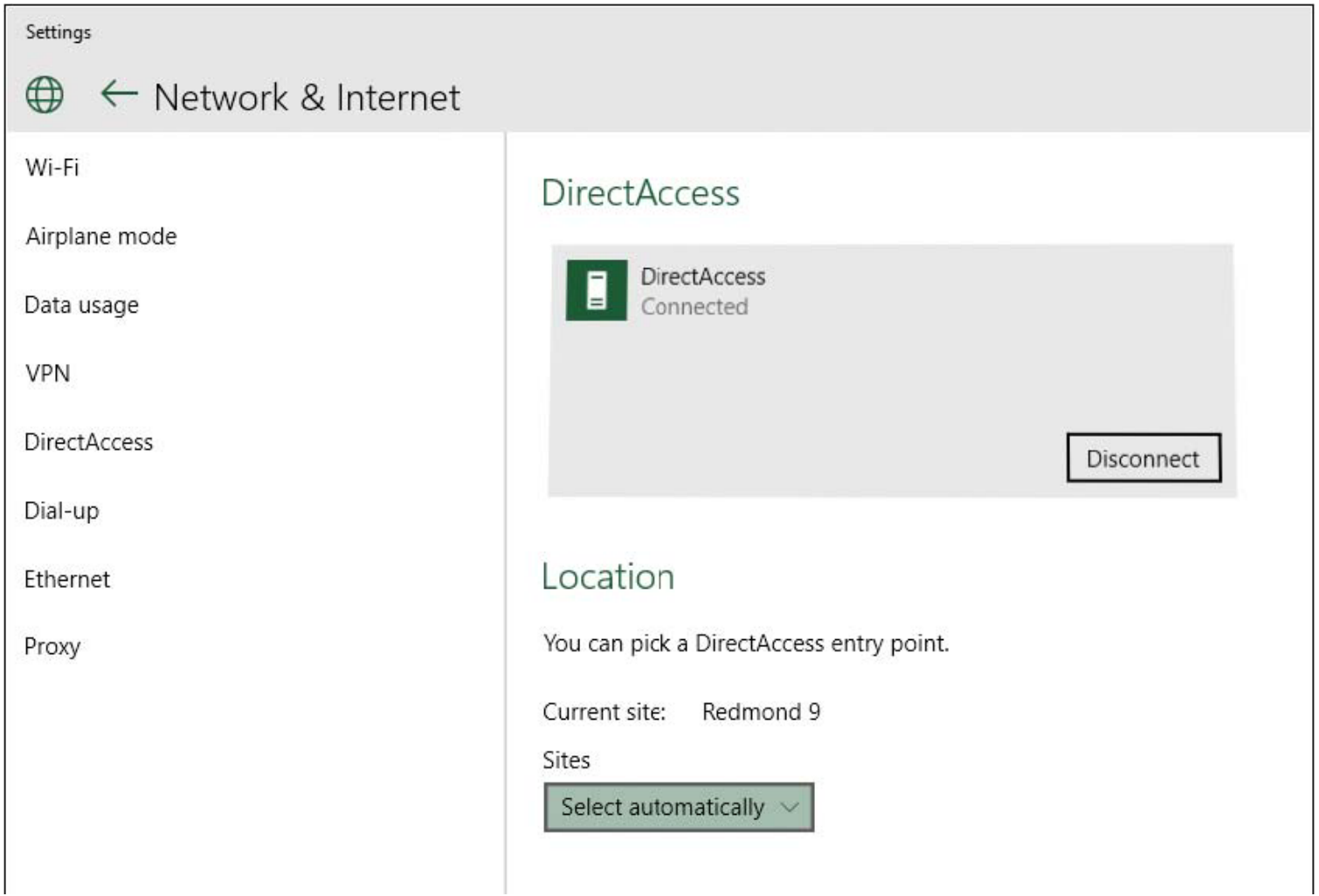
- preshared key składowany jawnie (!) w SPD
- certyfikat X.509 – wymagane wskazanie CA i posiadanie certyfikatu root CA; zamiast IKE tu angażowany jest Win CAPI (Cryptographic API)
- Kerberos

lokalne SPD mieści się w: HKLM\SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Local\
dla zapory: HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\

IPsec w Windows

DirectAccess

- zautomatyzowany korporacyjny VPN



IPsec

Ograniczenia IPsec

- praktycznie od początku był IPsec krytykowany za niekonsekwencje projektowe i nadmierne skomplikowanie
  - np. ochrona integralności zapewniana jest w równym stopniu przez ESP i AH – usunięcie tego ostatniego ze specyfikacji postulowano już kilkukrotnie
- niektóre błędy zostały usunięte w wersji z 1998 r. (część potencjalnych furtek do ataków DoS) – w sporej mierze na podstawie sugestii autorów implementacji
- wskazywane usterki nie mają raczej charakteru otwartych dziur, grożących złamaniem bezpieczeństwa sieci, ale są za to dość liczne i ułatwiają powstawanie potencjalnych słabości w samych implementacjach

IPsec

Ograniczenia IPsec

- jednak IPsec jest wykorzystywany powszechnie i praktycznie nie ma alternatywy

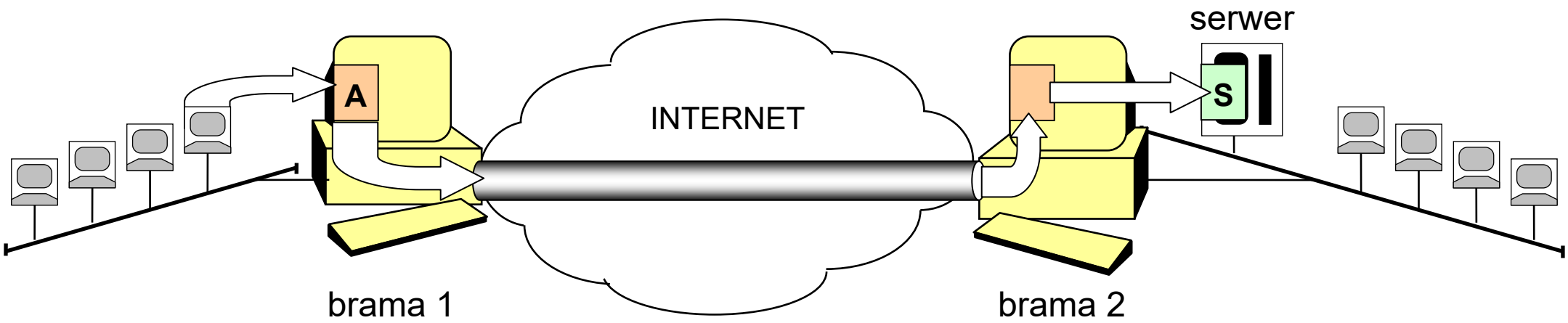
  [Niels Fergusson, Bruce Schneier; analiza IPsec 1999]:

  „Nawet pomimo dość poważnych zarzutów jakie wysunęliśmy wobec IPsec, jest on prawdopodobnie najlepszym protokołem bezpieczeństwa z obecnie dostępnych. W przeszłości przeprowadziliśmy podobne analizy innych protokołów o analogicznym przeznaczeniu. Żaden ze zbadanych protokołów nie spełnił swojego celu, ale IPsec zbliżył się do niego najbardziej. (...) *Mamy ambiwalentne odczucia wobec IPsec. Z jednej strony IPsec jest znacznie lepszy niż jakikolwiek protokół bezpieczeństwa IP stworzony w ostatnich latach. Z drugiej strony nie wydaje nam się, by zaowocował on kiedykolwiek stworzeniem w pełni bezpiecznego systemu."*

Inne techniki realizacji tuneli VPN

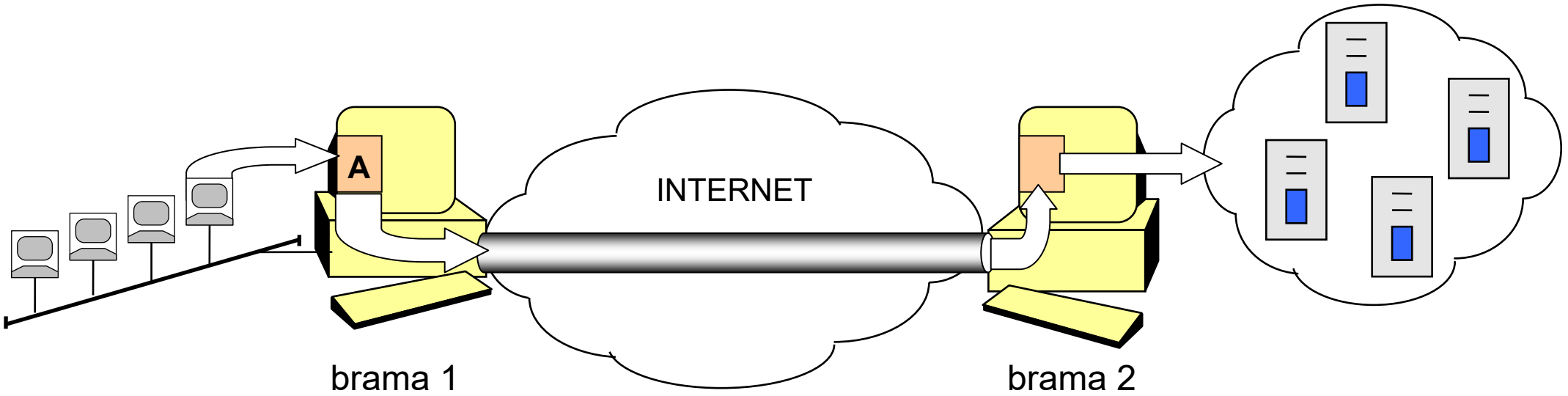
Propagowanie połączeń aplikacyjnych (*port forwarding*)

- tunele wirtualne na poziomie warstwy aplikacji (oferuje je np. SSH)
- połączenia na port **A bramy 1** są tunelowane do **bramy 2** i dalej propagowane na port **S serwera** w sieci lokalnej za **bramą 2**



Propagowanie połączeń aplikacyjnych

- SSH oferuje też funkcję pełnego proxy aplikacyjnego SOCKS (SOCKet Secure)



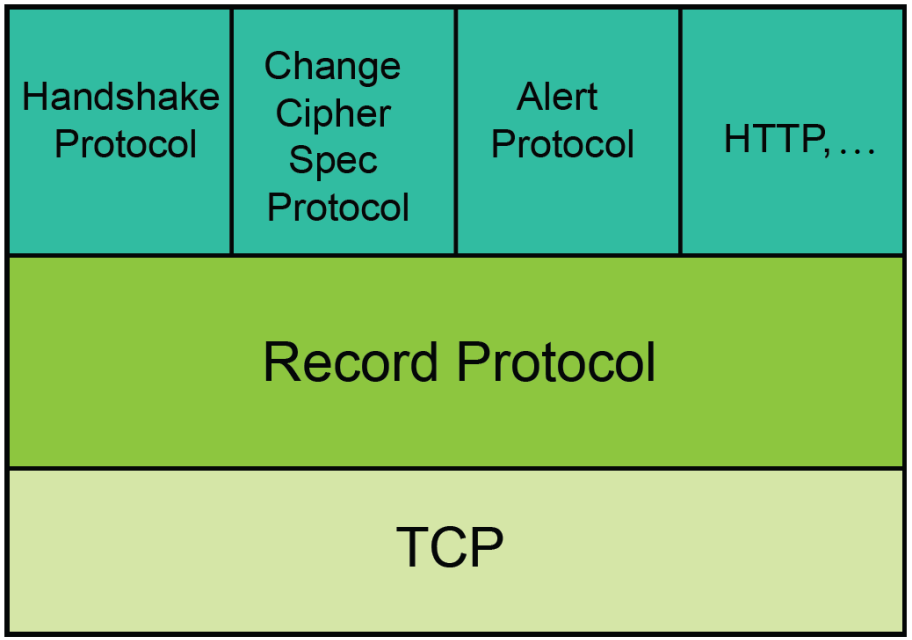
Tunele SSL/TLS

- SSL (*Secure Socket Layer*) to połączeniowy protokół sesji oferujący tunel kryptograficzny host-to-host
- uwierzytelnianie, ochrona poufności, integralności i autentyczności z wykorzystaniem certyfikatów X.509
- HTTPS – port 443, SMTP – 465, IMAPs – 993, POPs – 995
- następca: TLS (*Transport Layer Security*) – standard IETF
  TLS 1.0 RFC 2246, TLS 1.1 RFC 4346, TLS 1.2 RFC 5246 (2008 r.),
  TLS 1.3 RFC 8446 (2018 r.)
- inne usługi, dowolny ruch (stunnel, OpenVPN net-to-net, host-to-net)
- wersja na UDP – DTLS (*Datagram TLS*) 1.0 RFC 4347, 1.2 RFC 6347 (2012 r.)
- biblioteki OpenSSL, NSS, GnuTLS, ...

Tunele SSL/TLS

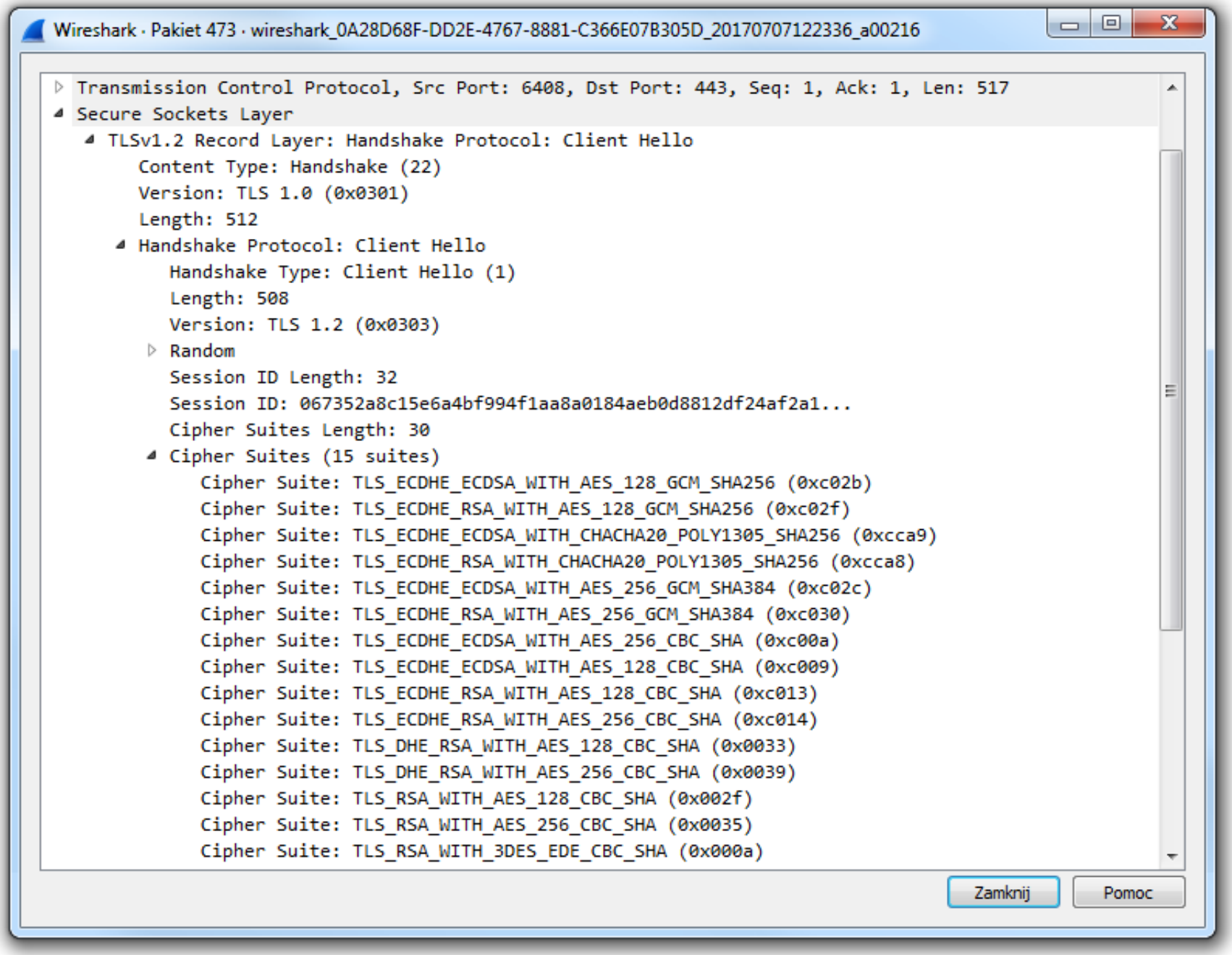
Protokoły składowe:

- Handshake Protocol – uzgadnianie sesji
- Change Cipher – wybór i zmiana metody szyfrowania
- Alert Protocol – sygnalizacja zdarzeń i błędów
- Record Protocol – tunelowanie PDU aplikacyjnych:
  - szyfrowanie symetryczne
  - integralność
  - kompresja



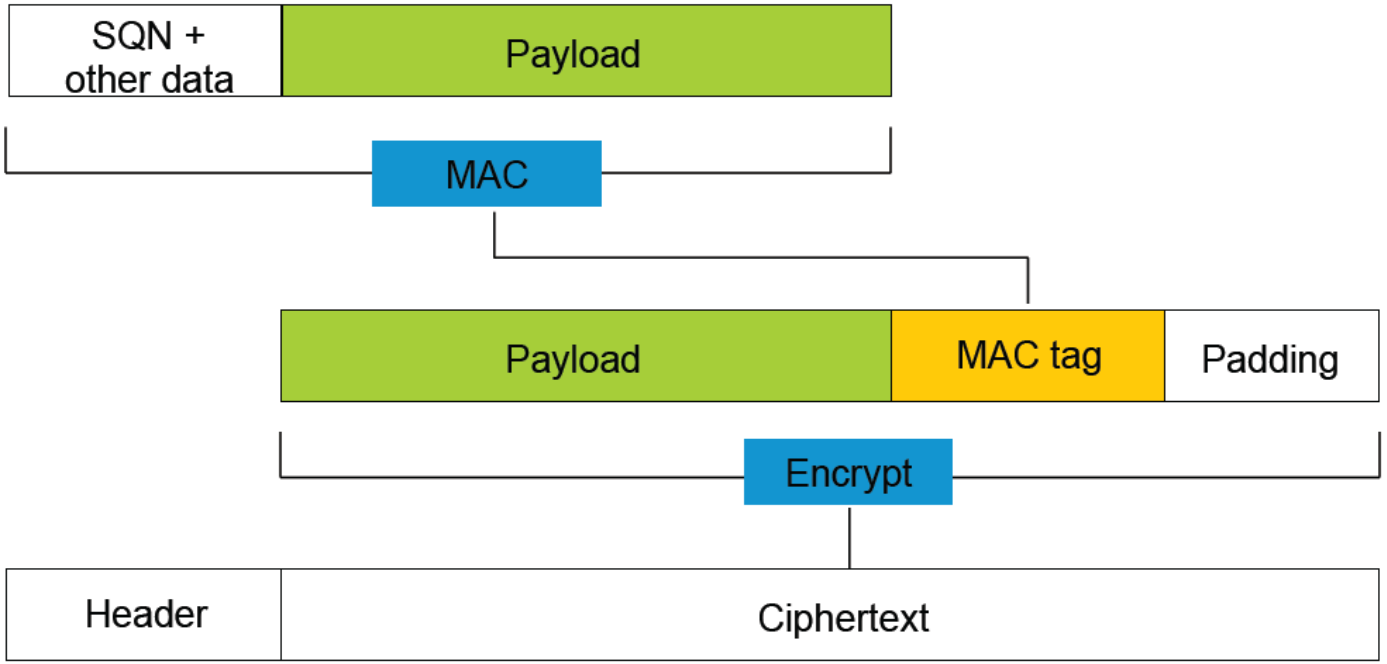
Tunele SSL/TLS

Handshake Protocol



Tunele SSL/TLS

Record Protocol



Tunele SSL/TLS

Record Protocol

- do wersji TLS 1.1 (2006 r.) problematyczny dobór IV szyfrowania CBC skutkował możliwością przeprowadzenia teoretycznego ataku
  - IV dla nowego komunikatu (rekordu) jest ostatnim blokiem kryptogramu poprzedniego rekordu
  - tymczasowy workaround stanowiło szyfrowanie wstępnie pustego rekordu
  - OpenSSL podjął tę taktykę już w 2002 r., ale wycofał się z niej, bowiem ... MS Windows nie radził sobie z obsługą rekordów zerowej długości
- uskutecznionego praktycznie w 2011 r. (*predictable IV attack* → BEAST attack tool)
- problemy z implementacjami rozszerzeń (Heartbeat → Heartbleed)

Tunele SSL/TLS

Feralna seria podatności 2010-2015

- Renegotiation Attack, Truncation Attack, Triple Handshake Attack, Lucky Thirteen
- BEAST (Browser Exploit Against SSL/TLS), Poodle, GoldenDoodle, ...
- CRIME (Compression Ratio Infoleak Made Easy)
- BREACH (Browser Reconnaissance and Exfiltration ..., http://breachattack.com)
- FREAK (Factoring Attack on RSA-EXPORT Keys, https://FREAKattack.com/)
- Heartbleed (CVE-2014-0160, http://heartbleed.com)
- Alternative Chains Certificate Forgery (CVE-2015-1793)
- ... ➔ https://en.wikipedia.org/wiki/Transport_Layer_Security#Attacks_against_TLS.2FSSL

https://www.howsmyssl.com

https://www.ssllabs.com/ssltest

Tunele SSL/TLS

TLS 1.3

Key exchange/agreement and authentication

Algorithm	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
RSA	Yes	Yes	Yes	Yes	Yes	No
DH-RSA	No	Yes	Yes	Yes	Yes	No
DHE-RSA (forward secrecy)	No	Yes	Yes	Yes	Yes	Yes
ECDH-RSA	No	No	Yes	Yes	Yes	No
ECDHE-RSA (forward secrecy)	No	No	Yes	Yes	Yes	Yes
DH-DSS	No	Yes	Yes	Yes	Yes	No
DHE-DSS (forward secrecy)	No	Yes	Yes	Yes	Yes	No
ECDH-ECDSA	No	No	Yes	Yes	Yes	No
ECDHE-ECDSA (forward secrecy)	No	No	Yes	Yes	Yes	Yes
PSK	No	No	Yes	Yes	Yes	
PSK-RSA	No	No	Yes	Yes	Yes	

Nowe trendy

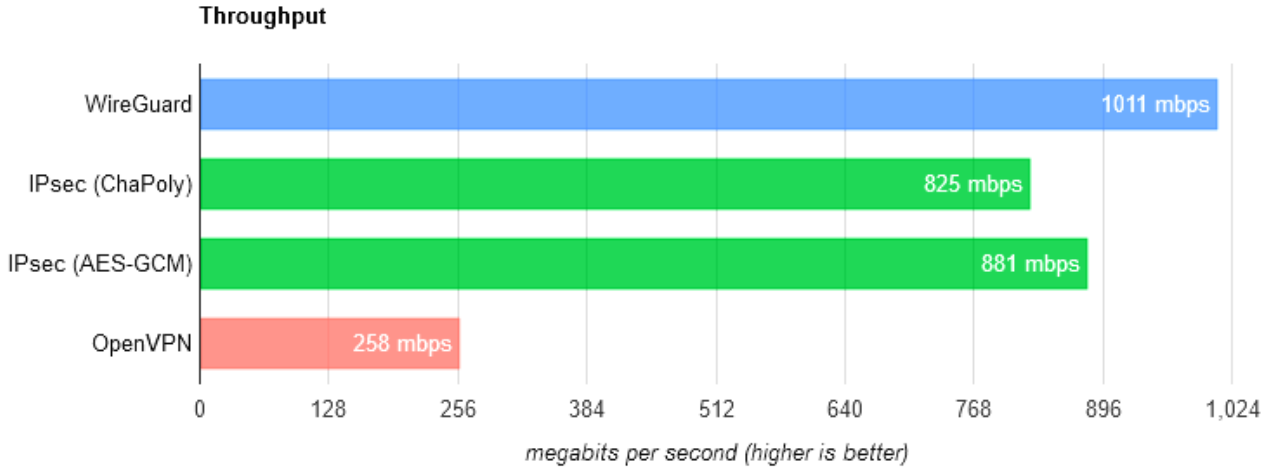
- WireGuard
- BeyondCorp
- IKE-less IPsec w SDN
- autorskie protokoły wykorzystywane w SDN i SD-WAN (np. Cisco OMP)

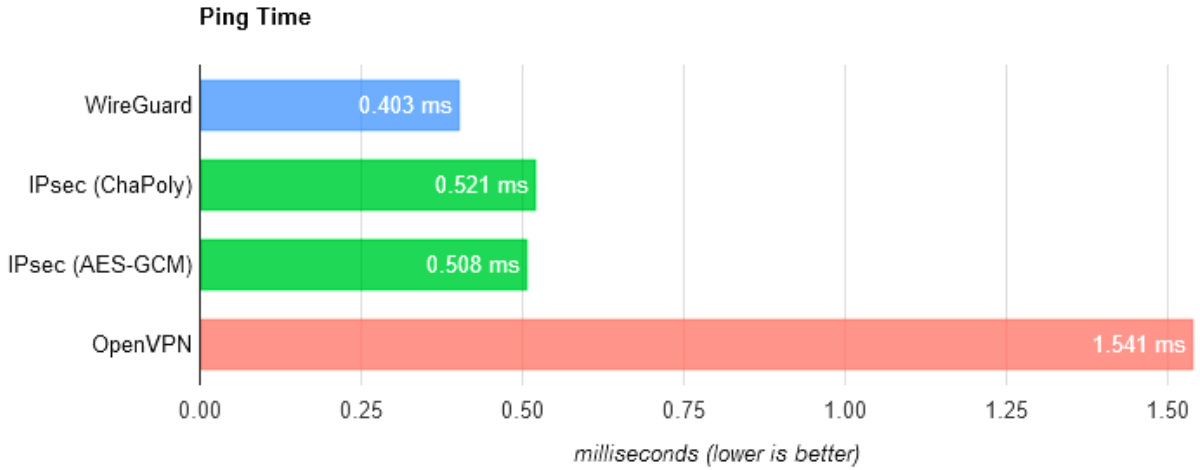
WireGuard ➔ https://www.wireguard.com/protocol/

- open-source (GPLv2)
- Noise framework (www.noiseprotocol.org), “zero trust networking”
- Linux (od jądra 5.6), Android, Windows, macOS, iOS
- UDP na IPv4/IPv6
- ChaCha20, Poly1305 authenticator, BLAKE2 hash (RFC7693)
- HMAC-based Extract-and-Expand Key Derivation Function (HKDF, RFC5869)
- tunele w topologii P2P, star (client-server), mesh

➔ https://tailscale.com/blog/how-tailscale-works/

WireGuard®


Throughput
WireGuard
IPsec (ChaPoly)
IPsec (AES-GCM)
OpenVPN
1011 mbps
825 mbps
881 mbps
258 mbps
0
128
256
384
512
640
768
896
1,024
megabits per second (higher is better)


Ping Time
WireGuard
IPsec (ChaPoly)
IPsec (AES-GCM)
OpenVPN
0.403 ms
0.521 ms
0.508 ms
1.541 ms
0.00
0.25
0.50
0.75
1.00
1.25
1.50
milliseconds (lower is better)

Przykładowe produkty

VPN – produkty

Cisco 7500

1. centralna (programowa na poziomie IOS,
   wykonywana przez RSP = *Route Switch Processor*)

2. na poszczególnych portach modułu VIP-40 = *Versatile Interface Processor*
   (każdy moduł oddzielnie)
   - przy 100% obciążeniu procesora samym tylko szyfrowaniem, producent szacuje przepustowość 3÷10 Mb/s – ad. 1) i 2)
   - realnie przepustowość może być zdecydowanie niższa od 3 Mb/s;

3. dedykowany moduł *Encryption Service Adapter* (z równoważeniem obciążenia)
   - wyjęcie lub manipulacja układem blokuje adapter kasując klucze;
   - ponowne uruchomienie wymaga podania hasła operatora

VPN – produkty

Bramki VPN

- CheckPoint Connetra
- SonicWall Aventail
- Juniper Secure Access
- Cisco ASA
- . . .

Juniper Secure Access 2500