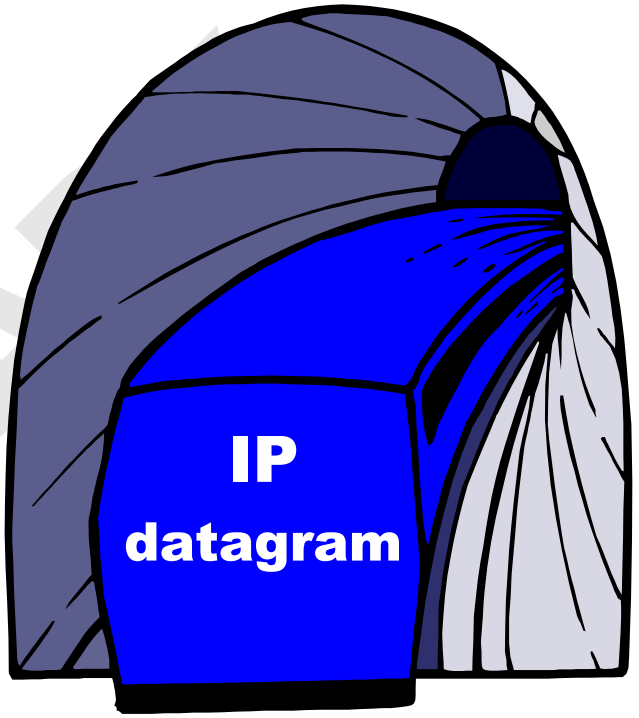
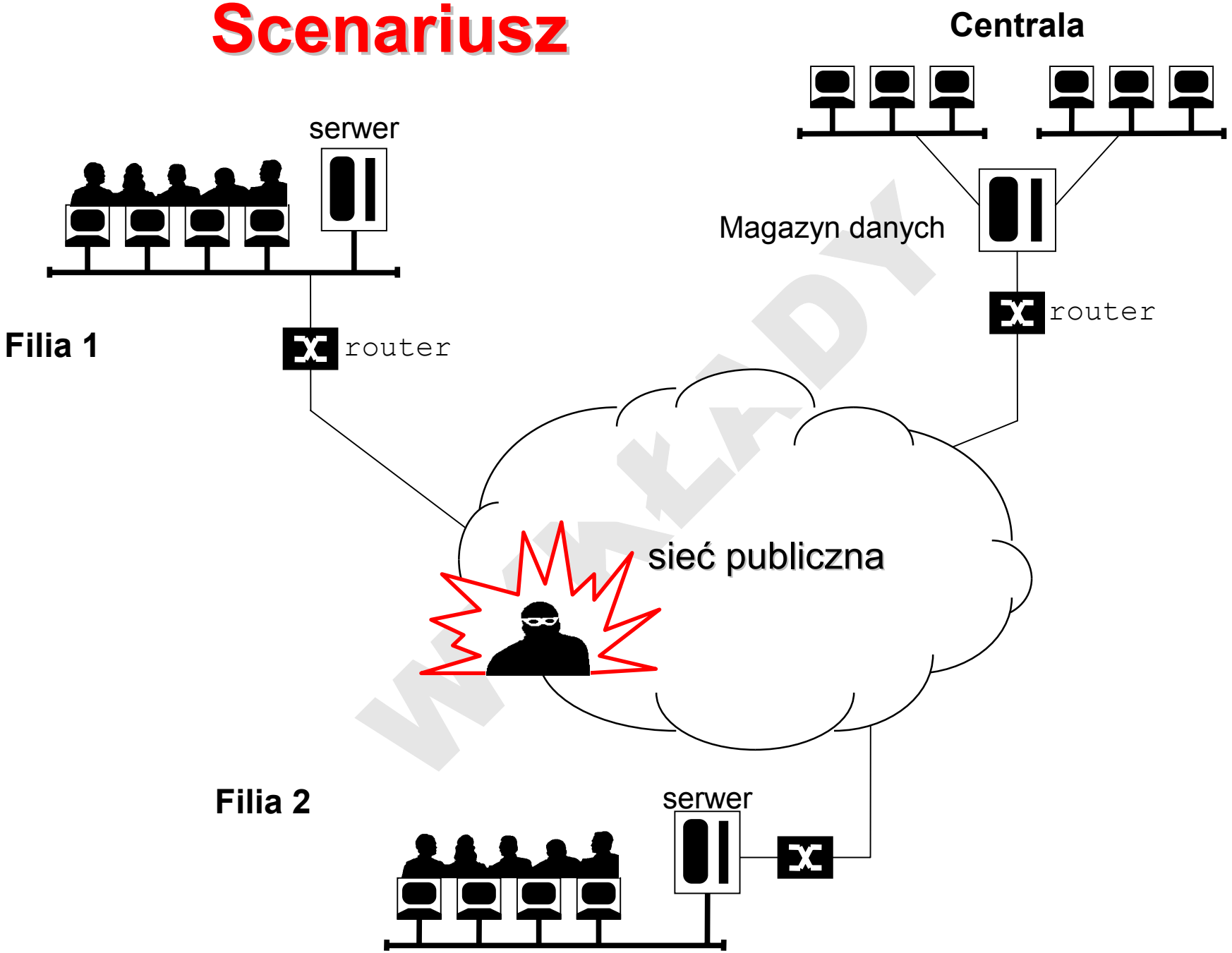
Tunele wirtualne VPN



Zagadnienia

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

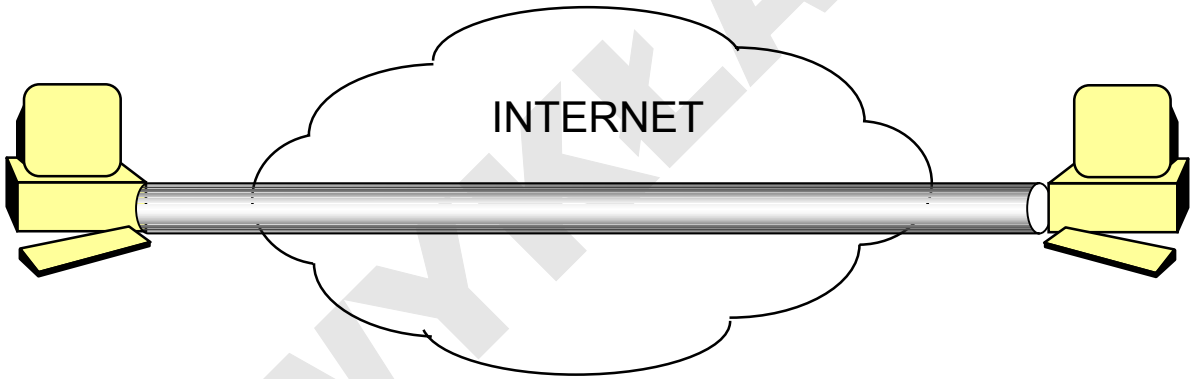
Scenariusz



Tunele wirtualne

Konfiguracje

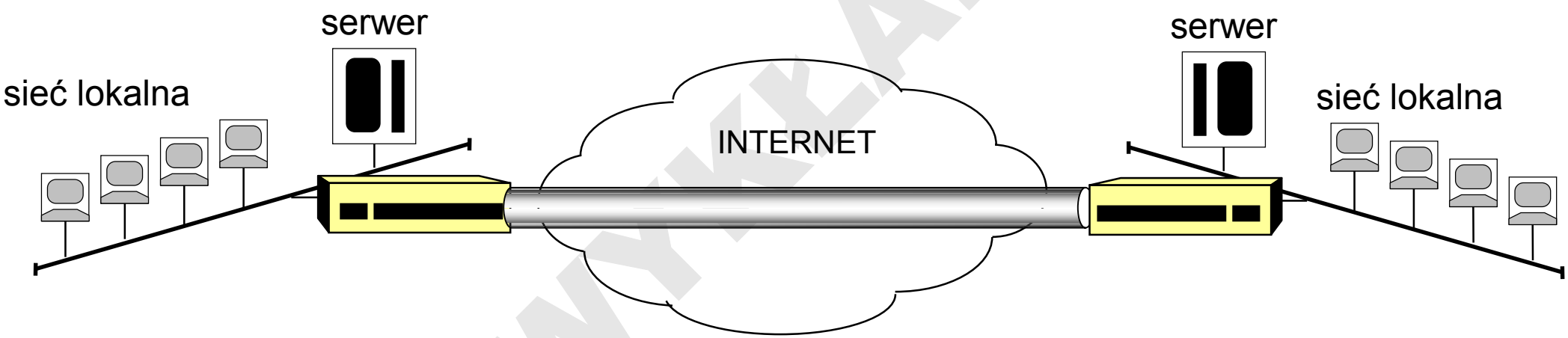
host-to-host



Tunele wirtualne

Konfiguracje

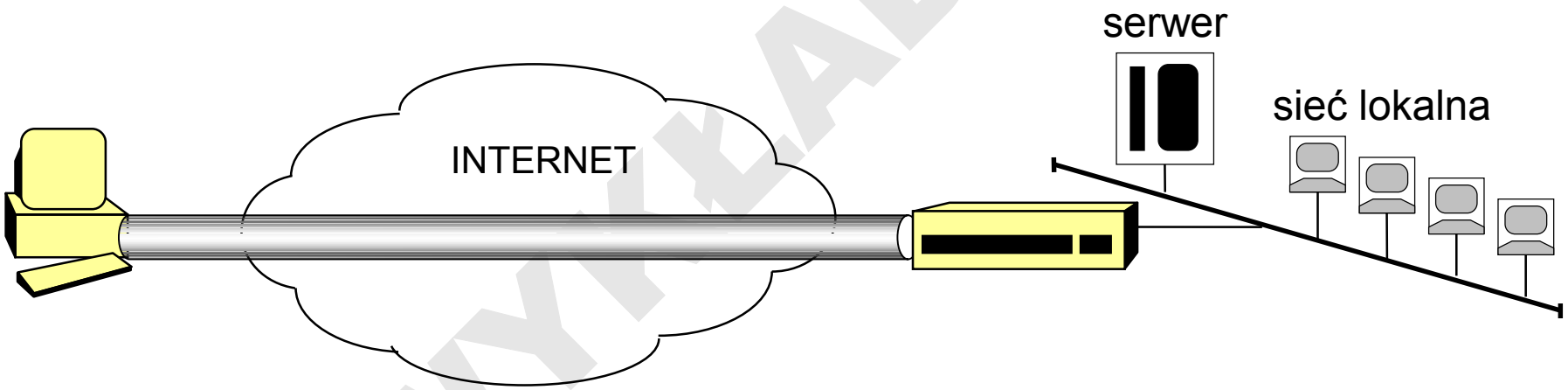
net-to-net



Tunele wirtualne

Konfiguracje

host-to-net



IPsec

- w IPv4 brak jakichkolwiek mechanizmów bezpieczeństwa
- w 1995 r. przedstawiono (IETF) pierwszą wersję specyfikacji protokołu sieciowego IPsec (RFC 1825), zawierającego dwie składowe
  - Authentication Header (AH) – protokół nr 51
  - Encapsulating Security Payload (ESP) – protokół nr 50
- ... którego zadaniem jest transparentne dla aplikacji (warstwa sieciowa) wykorzystanie narzędzi kryptograficznych w celu osiągnięcia
  - integralności – poprzez AH
  - poufności – poprzez ESP
- wkrótce rozszerzono funkcje ESP o ochronę integralności

IPsec

Dlaczego oddzielne składniki AH i ESP:

- trudności merytoryczne – złożony protokół
- 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.

- funkcjonalność AH wystarcza w wielu zastosowaniach, np. DNS

IPsec

IPsec (RFC 2401, 1998 r.):

- **AH** (Authentication Header, RFC 2402)
  - realizuje kontrolę integralności i autentyczności datagramu IP oraz umożliwia uwierzytelnianie

- **ESP** (Encapsulating Security Payload, RFC 2406)
  - zapewnia integralność i poufność treści datagramu

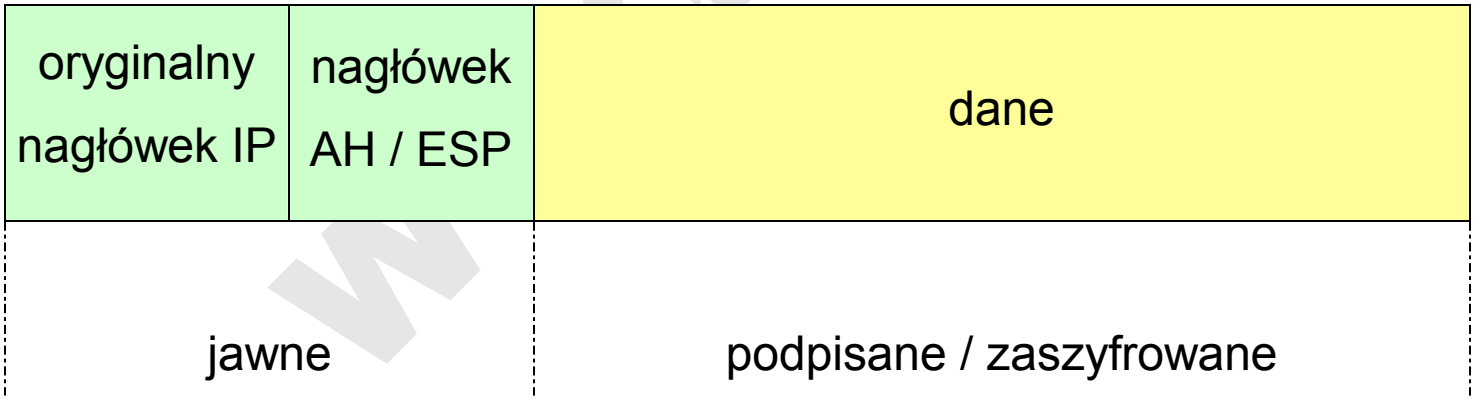
Uwierzytelnianie stron jest realizowane do pewnego stopnia przez sam protokół IPsec i może być rozszerzane przez dodatkowe mechanizmy.

http://www.ipsec.pl/

Tryby pracy

Tryb transportowy/bezpośredni (*transport mode*)

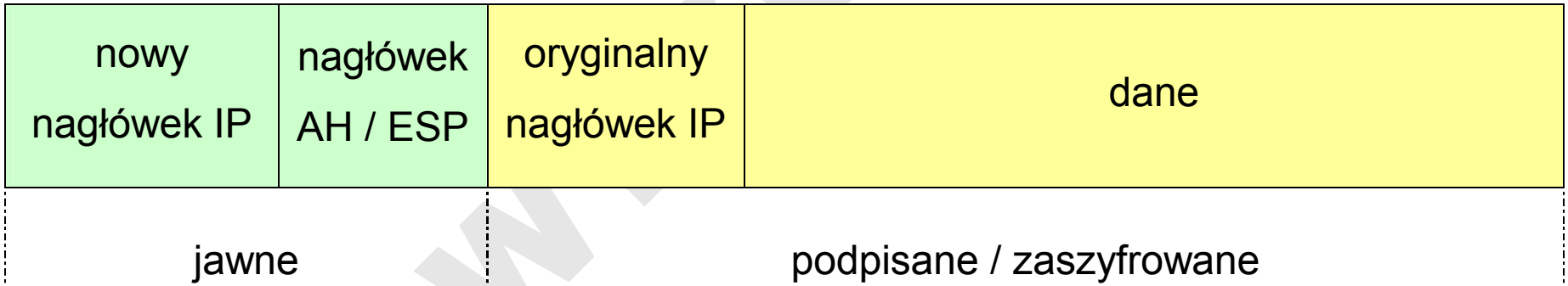
– do datagramu dodany jest nagłówek AH / ESP i dane datagramu (ramka TCP, UDP, ICMP, ...) zostają zabezpieczone (podpisane / zaszyfrowane) bezpośrednio za nim



Tryby pracy

Tryb tunelowy (*tunnel mode*)

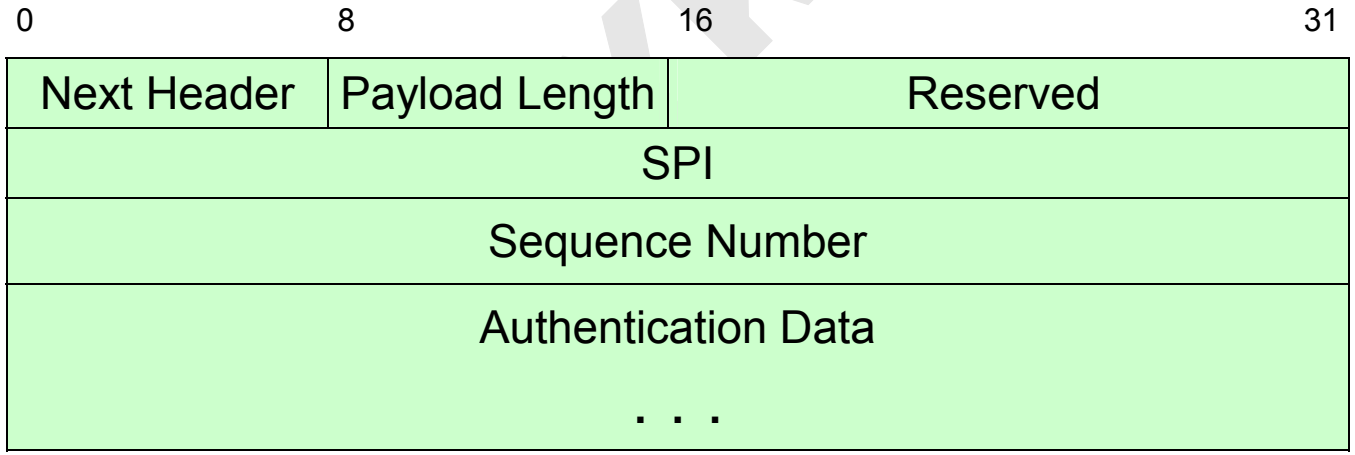
– oryginalny datagram IP zostanie zabezpieczony (podpisany / zaszyfrowany) w całości z nagłówkiem w PDU protokołu IPsec (ramkę AH / ESP), a następnie umieszczony w niezabezpieczonym datagramie IP jako jego dane



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

AH (Authentication Header)

- AH przenosi wartość jednokierunkowej funkcji skrótu treści datagramu oraz stałych pól nagłówka (zarówno w trybie transportowym jak i tunelowym!)
- wykorzystywane funkcje HMAC: MD5, SHA-1, RIPEMD-160 lub inne (negocjowane)
- fragmentacja datagramu jest dokonywana wcześniej (podpisywany jest każdy fragment oddzielnie)
- niezaprzeczalność osiągana jest poprzez silne algorytmy kryptograficzne, np. RSA



ESP (Encapsulating Security Payload)

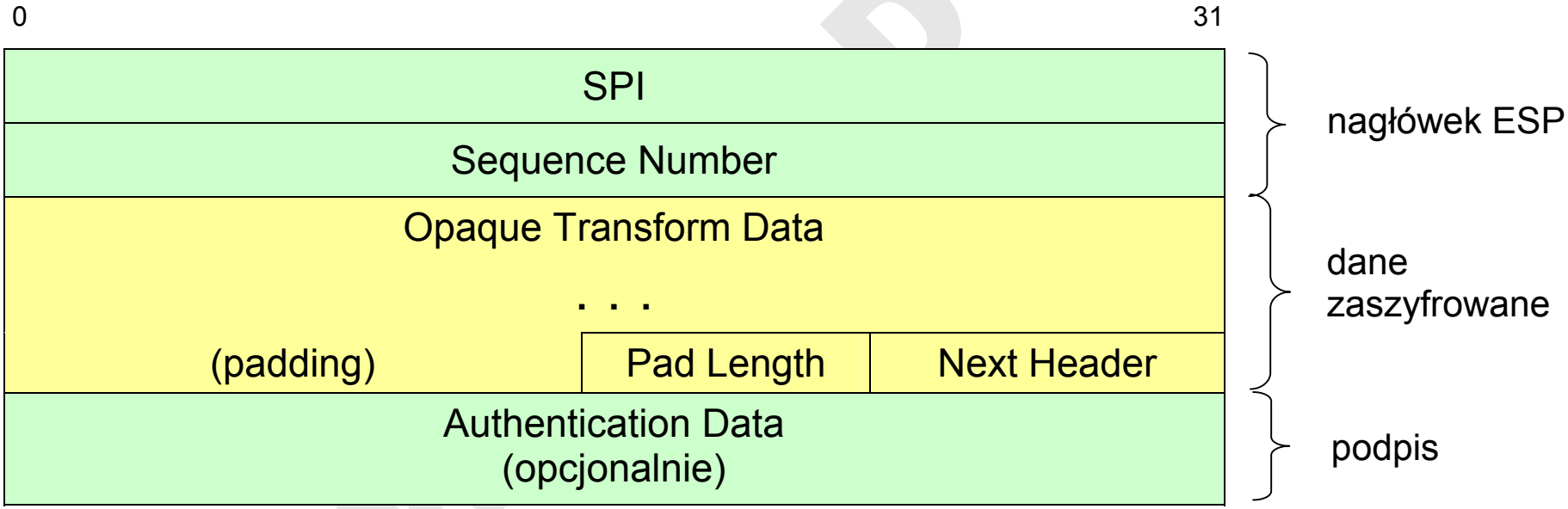
Umożliwia:

- podpisywanie datagramu (te same algorytmy co w AH – w trybie transportowym uwzględnia w podpisie statyczne pola nagłówka podstawowego IP)
- zaszyfrowanie datagramu – szyfry blokowe w trybie CBC, np. DES, 3DES (3-keys), Blowfish, CAST-128 czy Rijndael/AES, aktualnie również 3-IDEA (3-keys)

Nagłówek ESP musi być umieszczony bezpośrednio przed zaszyfrowanymi danymi.

ESP (Encapsulating Security Payload)

- format i długość zaszyfrowanych danych zależy od metody szyfracji podanej w SPI



- odebranie datagramu wymaga odczytania SPI, odszyfrowania i odtworzenia oryginalnej treści wraz z nagłówkami

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 datagramie, a następnie szyfruje w całości przez ESP (tuneluje)

IPsec

Asocjacja bezpieczeństwa (*Security Association*)

- jest to 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 uzyskania AH (algorytm)
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 weryfikacji tożsamości w ESP
klucze wykorzystane w tej metodzie
czas ważności kluczy (zalecane)
czas ważności asocjacji
adresy IP mogące współdzielić asocjację
etykieta poziomu bezpieczeństwa (formalna: 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 SA w bazie SAD (*SA Database*) lub
   - nawiązanie odpowiedniego SA jeśli nie jest jeszcze nawiązane
4. Wykonanie zabezpieczeń wykorzystując algorytmy, parametry i klucze zawarte w SA:
   - wynikiem jest stworzenie nagłówka AH lub ESP,
   - dodatkowo może zostać również utworzony nowy nagłówek IP (w trybie tunelowym).
5. 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

Zarządzanie kluczami

Zarządzanie i dystrybucja kluczy nie są uwzględnione w specyfikacji IPsec !

Typy kluczy:

- przypisane do użytkownika (Kerberos)
- przypisane do stacji sieciowej (nie zabezpiecza sieci przed atakami od wewnątrz)

IPsec

Zarządzanie kluczami

Możliwe sposoby dystrybucji:

- dystrybucja ręczna – administrator (małej sieci lokalnej) wyznacza wszystkie klucze
- wykorzystanie istniejących systemów dystrybucji (np. Kerberos)
- automatyczne – początkowo myślano o DNS jako repozytorium kluczy
- ostatecznie wprowadzono nowe protokoły i specyfikacje serwerów kluczy (niezależne od IPsec): np. SKIP (Sun), Photuris, IKE (*Internet Key Exchange*)
- integracja serwerów kluczy z usługami katalogowymi (DNSsec, LDAP)

IPsec

Zarządzanie kluczami

Protokoły zarządzania kluczami

- ich zadanie – wzajemne uwierzytelnianie podmiotów nawiązujących asocjacje IPsec
- oraz uzgadnianie kluczy sesji na potrzeby poszczególnych kanałów SA
- obie funkcje realizowane są na podstawie skonfigurowanych na stałe danych uwierzytelniających, np. hasło wspólne dla pary stacji (*shared secret*), certyfikaty X.509, klucze PGP
- niektóre implementacje (SKIP, Photuris) umożliwiają wyłącznie uwierzytelnienie na podstawie haseł
- protokół IKE obsługuje natomiast wszystkie wyżej wymienione metody i umożliwia jeszcze prywatne rozszerzenia

IPsec

Protokół IKE (*Internet Key Exchange*)

- IKE obejmuje 2 składniki:
  - ISAKMP (*Internet Security Association and Key Management Protocol*) – faktyczny protokół negocjacji parametrów IPSec
  - Oakley – kryptograficzny protokół wymiany kluczy za pomocą algorytmu Diffiego-Hellmana
- ISAKMP (RFC 2408) stanowi trzon całości i z tego powodu nazwy tej używa się niekiedy zamiennie z IKE
- ISAKMP korzysta z UDP (port 500)

IPsec

Protokół IKE

Wymiana kluczy

- następuje dwuetapowo
- najpierw ustalana jest tożsamość komunikujących się węzłów i tworzony jest bezpieczny kanał (tzw. ISAKMP SA), utrzymywany przez cały czas trwania sesji i służący następnie do właściwej negocjacji parametrów asocjacji
- negocjacja obejmuje m.in. listę obsługiwanych algorytmów szyfrujących, co ułatwia obsługę środowisk heterogenicznych

IPsec

Protokół IKE

Uwierzytelnianie

- w najprostszym przypadku każda para węzłów musi mieć ustalone wspólne hasło
- które służy do obliczania kluczy metodą Diffiego-Hellmana
- konieczność konfigurowania haseł na wszystkich węzłach jest istotnym ograniczeniem – wymaga wiedzy o strukturze (topologii) połączeń *a priori*
- pracochłonne w przypadku dużych sieci
- zastosowanie kluczy publicznych podpisanych przez nadrzędny urząd certyfikujący CA (np. certyfikatów X.509) jest wolne od takich ograniczeń

IPsec

PKI (*Public Key Infrastructure*)

- IKE pozwala wykorzystać możliwości PKI
- po nawiązaniu komunikacji, ale przed uzgodnieniem ISAKMP SA węzeł może zweryfikować autentyczność certyfikatu drugiej strony dzięki podpisowi CA
- 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 – będzie to jeden i ten sam klucz na wszystkich węzłach
- ułatwia to realizację złożonych topologii

IPsec

PKI

- IKE umożliwia też automatyczną renegocjację kluczy kryptograficznych co określony interwał (nawet często)
- w razie złamania bieżącego klucza, dane zaszyfrowane poprzednimi kluczami nie są narażone
- cecha ta, określana jako *Perfect Forward Security*, chroni przed sytuacją gdy atakujący zapisuje wszystkie przechwycone w przeszłości dane w nadziei, że kiedyś uda mu się zdobyć klucz do ich rozszyfrowania
- w przypadku renegocjacji klucza (właściwie dobieranych – silna losowość) poprzedni klucz jest usuwany z pamięci i włamywacz nie znajdzie go w systemie nawet w przypadku opanowania węzła

IPsec

DOI (*Domain of Interpretation*)

- protokół ISAKMP jest łatwo rozszerzalny
- pewne parametry (DOI) można przystosować całkowicie do potrzeb własnej instytucji:
  - własny zestaw szyfrów
  - własne mechanizmy uwierzytelnienia

IPsec

Ograniczenia

- praktycznie od początku był IPsec krytykowany za niekonsekwencje projektowe i nadmierne skomplikowanie
  - np. ochrona integralności zapewniana jest niemal 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

Implementacje

- w przypadku systemów kryptograficznych jakość implementacji ma bardzo duże znaczenie
- trudno ocenić jakość dostępnych obecnie implementacji – brak wyników audytów – nie wiadomo nawet czy takie audyty są prowadzone
- certyfikaty przyznawane przez instytucje takie jak ICSA (http://www.icsa.net/html/communities/ipsec/) są raczej stwierdzeniem zgodności ze specyfikacją niż faktycznej poprawności implementacji

IPsec

Ograniczenia

- jednak IPsec jest wykorzystywany powszechnie i praktycznie nie ma alternatywy

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

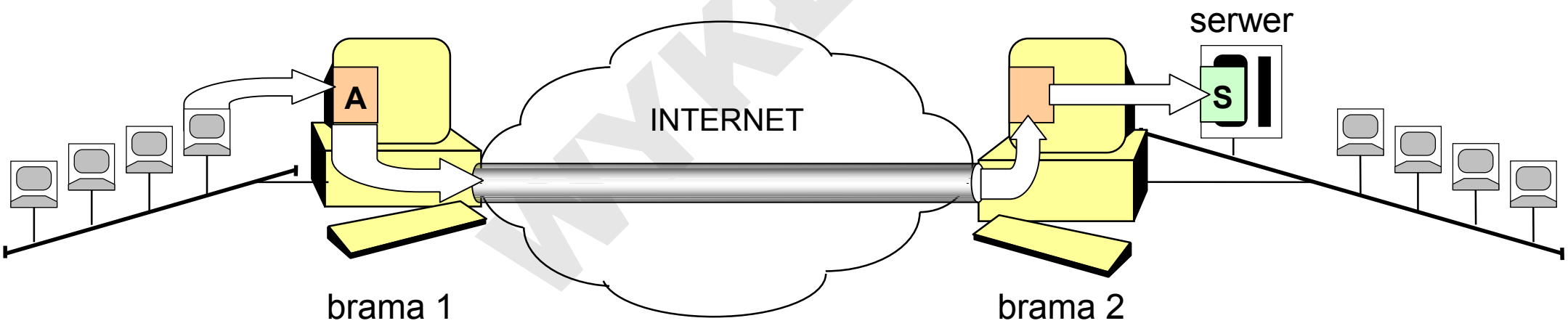
  „Nawet pomimo dość poważnych zarzutów jakie wysunęliśmy wobec IPSec, jest on prawdopodobnie najlepszym protokołem bezpieczeństwa z obecnie dostępnych. W przeszłości przeprowadziliśmy podobne analizy innych protokołów o analogicznym przeznaczeniu (w tym PPTP). Żaden ze zbadanych protokołów nie spełnił swojego celu, ale IPSec zbliżył się do niego najbliżej. (...) Mamy ambiwalentne odczucia wobec IPSec. Z jednej strony IPSec jest znacznie lepszy niż jakikolwiek protokół bezpieczeństwa IP stworzony w ostatnich latach: Microsoft PPTP, L2TP itp. Z drugiej strony nie wydaje nam się, by zaowocował on kiedykolwiek stworzeniem w pełni bezpiecznego systemu.”

Bezpieczeństwo w IPv6

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

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**



Tunele SSL

- SSL (*Secure Socket Layer*) to połączeniowy protokół transportowy
- oferujący dwupunktowy tunel kryptograficzny z wykorzystaniem certyfikatów
- zaprojektowany z myślą o ochronie sesji HTTP, POP/IMAP, SMTP
- oferuje ochronę poufności, integralności i autentyczności danych
- aktualnie SSL v.3.0
- oraz jego następca TLS (*Transport Layer Security*) – początkowo opracowany przez Netscape Comm. Corp., TLS v.1.0 jest standardem IETF – RFC 2246
- HTTPS – port 443

Tunele PPTP

Protokół PPTP (*Point-to-Point Tunneling Protocol*)

- Microsoft, 3Com, US Robotics,...
- OSI Layer 2 – rozszerzony PPP – kopertuje protokoły IP, IPX, NetBEUI,...
- szyfrowanie MPPE (ang. *Microsoft Point-to-Point Encryption*) oparte na RSA
- element usługi *Remote Access Services* w Windows NT (host-to-host)
- oraz usługi *Routing and Remote Access Service* (host-to-net, net-to-net)
- wspiera takie mechanizmy jak NAT

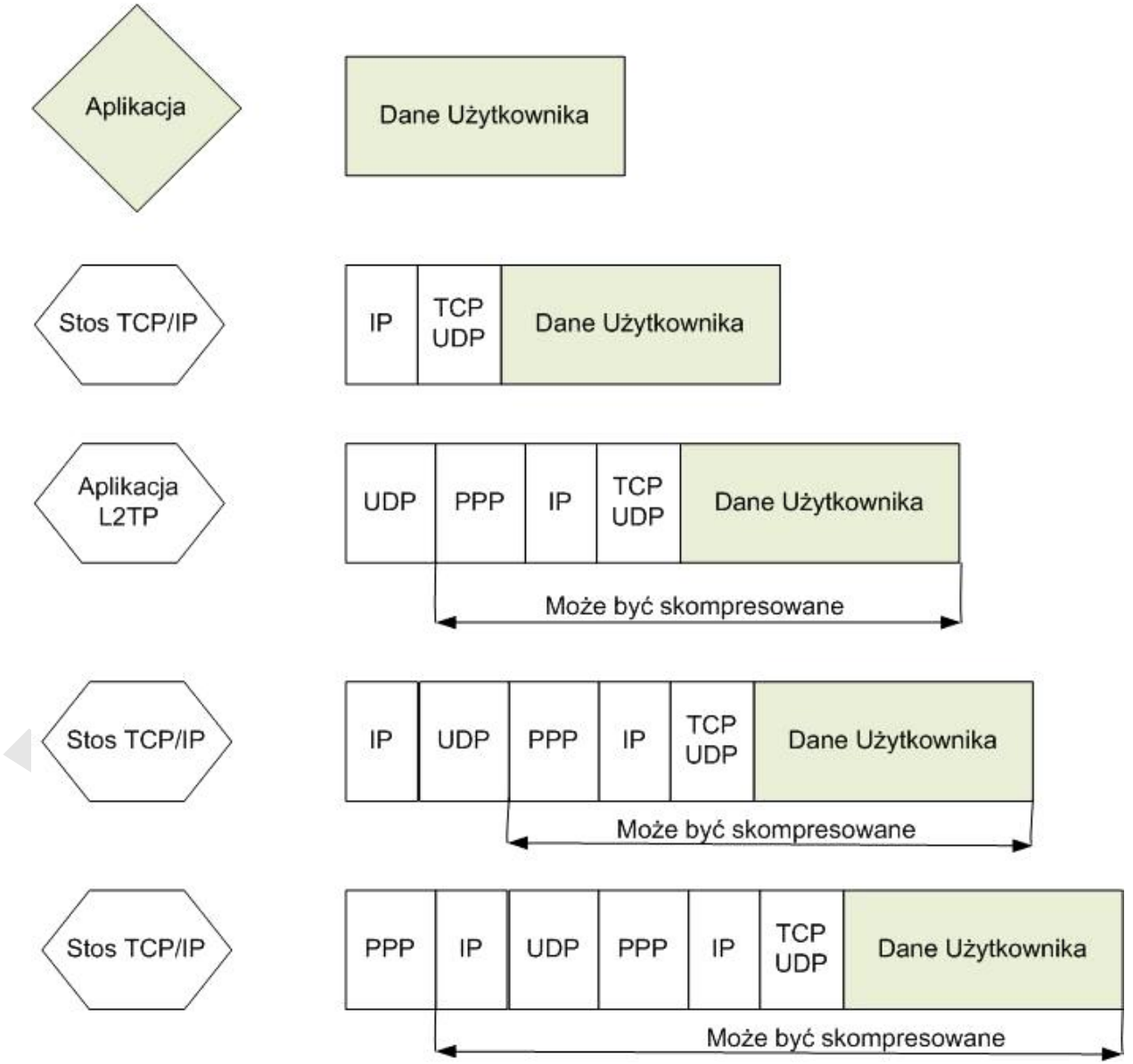
Tunele L2TP

Protokół L2TP (*Layer 2 Tunneling Protocol*)

- połączenie protokołów PPP i L2F (ang. *Layer Two Forwarding*, Cisco)
- PPP tunelowany w warstwie sieciowej / transportowej
- Windows NT/2000/XP
- typowe zastosowanie: host-to-net
- brak wsparcia dla NAT
- wymaga dostępu do centrum certyfikacji (systemu PKI)

Tunele L2TP

Kopertowanie



IPsec w Windows

- w Windows 2000 i XP wbudowano obsługę IPsec (ESP)
- ... zintegrowaną z Active Directory
- sam IPsec tuneluje tylko ruch IP
- stos L2TP/IPsec tuneluje także IPX

VPN – produkty

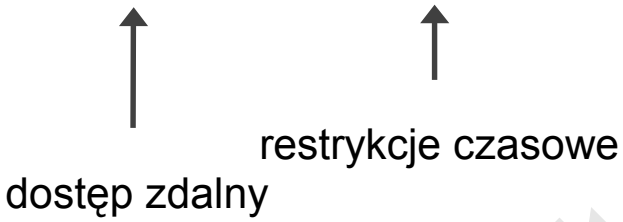
PIX = Private Internet eXchange (Cisco)

- PIX-PL (Private Link) od 1998 pod nazwą PIX Ravlin IPsec Card
  - IPsec (RFC-2401, RFC-2410), IKE, X.509 v.3, DSS
  - zarządzanie certyfikatami kluczy X.509 v.3
  - klucze do 168b
- konfiguracja (model PIX 535):
  - 10 x 10/100BASE-T lub 9 x 1000BASE-X, 95 Mb/s przy szyfracji DES,
  - 2000 tuneli VPN (IP)
  - redundancja *fail-over* + dodatkowe interfejsy sieciowe
- wersje zależne od przepustowości i liczby jednoczesnych połączeń TCP/UDP (do 100 tys.)

VPN – produkty

SecureLAN / SecureWAN (Cylink/Cisco)

- AAA = Authentication Authorization Accounting



- protokół TACACS +
- szyfracja
- centralne zarządzanie kluczami i hasłami kont Unixowych
- Sun Solaris

VPN – produkty

Cisco 7500

szyfracja programowa DES 56b, DSS (na poziomie IOS) w routerze:

1. centralna (wykonywana przez RSP = *Route Switch Processor*)
2. na poszczególnych portach modułu VIP-40 = *Versatile Interface Processor* (każdy moduł oddzielnie, bez równoważenia obciążenia)
   - 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 sprzętowej szyfracji *Encryption Service Adapter* (dla całego routera wystarczy 1 moduł – obsługuje do 299 połączeń)
   - wyjęcie lub manipulacja układem blokuje adapter kasując klucze;
   - ponowne uruchomienie wymaga podania hasła operatora

Border Guard (Network Security Systems / SkyLine)

1) **Packet Control Facility** – kontrola pakietów IP
   - kontrola poprawności ramek (błędów)
   - filtracja na podstawie adresów i usług
   - kontrola dostępu do portów (IP spoofing)
   - szyfracja danych kierowanych na wybrane adresy
2) **Bridge Control Facility** – podobnie, lecz na poziomie mostu (Ethernet)
3) **Data Privacy Facility**
   - kompresja (metodą ADLC opracowaną przez IBM)
   - wybór algorytmu szyfracji (NSC1, DES, 3DES, IDEA)
   - podpis elektroniczny MD5
   - transaction reply prevention – zapobiega powtórnemu wykonaniu tej samej transakcji (finanse – bankomaty)
   - szyfrowania całych pakietów (encapsulation)

- jako zwykły router obsługuje RIP, EGP, IPX, XNS, AppleTalk, Vines, X.25, Frame Relay
- interfejsy LAN: Ethernet AUI, RJ45
- interfejsy WAN: V.35, V.11/X.25, RS-232, RS-449, sychr. CSU/DSU, ISDN