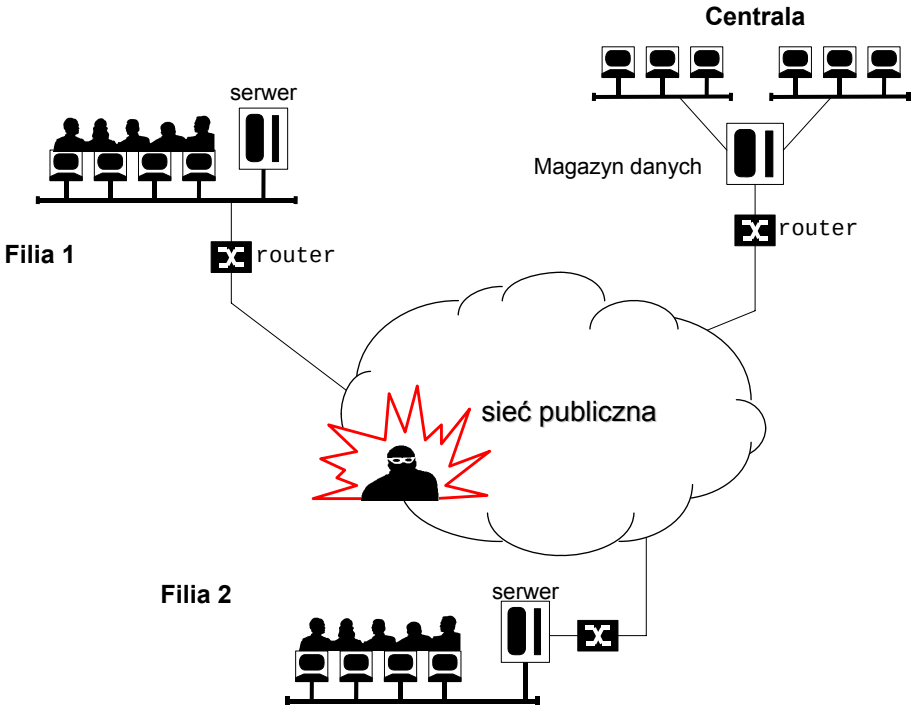
8. Tunele wirtualne VPN

Tunel wirtualny (*Virtual Private Network*, VPN) jest to kanał komunikacyjny chroniony przez niepowołanym dostępem (odczytem i modyfikacją) poprzez zastosowanie kryptografii. Tunel wirtualny VPN umożliwia chronioną transmisję w obszarze publicznej sieci rozległej, np. w celu realizacji bezpiecznego połączenia pomiędzy różnymi jednostkami, najczęściej geograficznie odległymi (rysunek 1). W sieci publicznej należy się liczyć z potencjalnymi naruszeniami poufności, integralności i autentyczności transmitowanych danych. Poznane we wcześniejszych modułach mechanizmy kryptograficzne umożliwiają skuteczną ochronę wszystkich tych własności informacji.

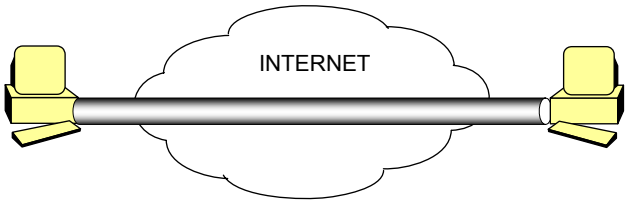


Rysunek 1. Schemat sieci publicznej analizowany jako scenariusz zagrożeń

Konfiguracje sieci VPN

Konfiguracja host-to-host

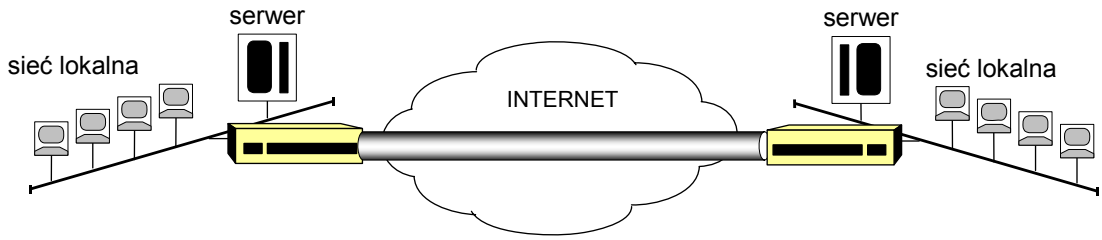
W konfiguracji tej końcami tunelu są pojedyncze stanowiska, wyposażone w odpowiednie oprogramowanie lub sprzęt (karty sieciowe) umożliwiające szyfrowanie i deszyfrowanie transmisji pomiędzy nimi.



Rysunek 2. Konfiguracja host-to-host

Konfiguracja net-to-net

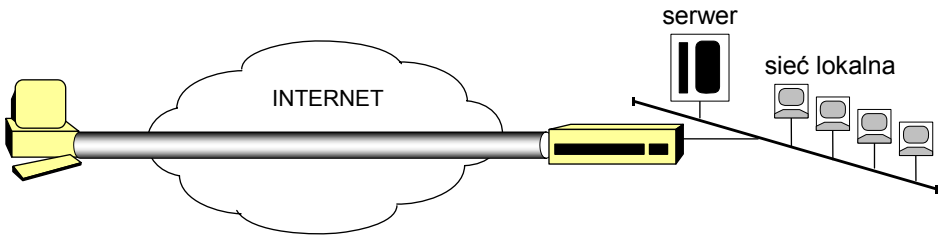
W konfiguracji tej końcami tunelu są pojedyncze węzły międzysieciowe (np. dedykowane urządzenia szyfrujące, routery brzegowe z modułami kryptograficznymi). Mogą one szyfrować całą transmisję wychodzącą ze swoich sieci lokalnych lub wybrany ruch sieciowy. Transmisja odbywająca się wewnątrz poszczególnych sieci nie jest szyfrowana.



Rysunek 3. Konfiguracja net-to-net

Konfiguracja host-to-net

W konfiguracji tej jednym z końców tunelu jest pojedyncze stanowisko, które uzyskuje dostęp do zasobów pewnej sieci lokalnej (np. korporacyjnej). Cała komunikacja lub wybrany ruch (wybrane usługi) poddawane są szyfrowaniu. Jest to model typowy dla środowisk pracy zdalnej.



Rysunek 4. Konfiguracja host-to-net

Protokół IPsec

Jak wiemy w protokole IPv4 brak praktycznie jakichkolwiek mechanizmów bezpieczeństwa. W związku z rosnącymi wymagani 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

Zadaniem protokołu IPsec operującego w warstwie sieciowej jest transparentne dla aplikacji wykorzystanie narzędzi kryptograficznych w celu osiągnięcia

- integralności – poprzez funkcje protokołu AH
- poufności – poprzez funkcje protokołu ESP

Jednak wkrótce rozszerzono funkcje ESP o ochronę również integralności. W efekcie funkcje ochrony integralności zostały powielone w obu składowych protokołu IPsec. Dlaczego zatem utrzymano oddzielne składniki AH i ESP? Z jednej strony przemawiają za tym trudności merytoryczne, zrozumiałe w tak złożonym projekcie jak ESP. Ponadto przemawiały pierwotnie za tym ograniczenia natury polityczno-prawnej, związane ze stosowaniem kryptografii – AH wykorzystując wyłącznie kryptograficzne funkcje skrótu, z reguły był traktowany bardziej liberalnie. Ostatecznie jednak należy przyznać, iż funkcjonalność AH wystarcza w wielu zastosowaniach, np. w przypadku ochrony usługi DNS, gdzie informacje udostępniane przez tę usługę są z reguły publiczne i nie ma potrzeby ich szyfrowania, ważne jest natomiast by nie zostały one po drodze sfałszowane.

Ostateczna wersja IPsec (RFC 2401, 1998 r.) obejmuje zatem specyfikacje dwu protokołów:

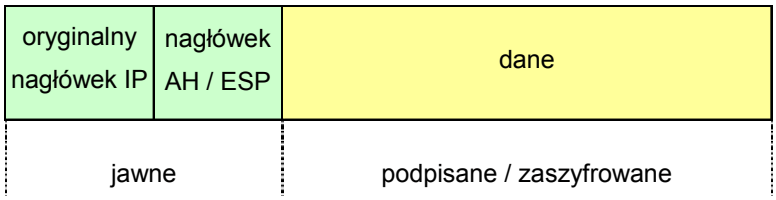
http://www.ipsec.pl/

- **AH** (Authentication Header, RFC 2402)
  - który realizuje kontrolę integralności i autentyczności datagramu IP oraz umożliwia uwierzytelnianie
- **ESP** (Encapsulating Security Payload, RFC 2406)
  - który zapewnia integralność i poufność treści datagramu

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

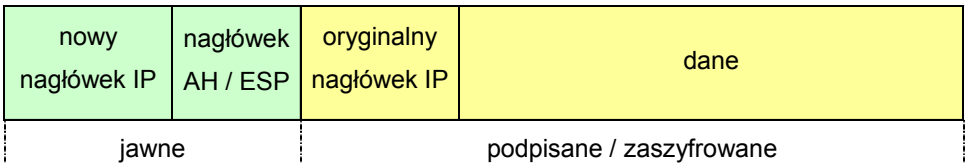
Tryby pracy protokołów IPsec

Tryb transportowy (*transport mode*), inaczej nazywany bezpośrednim, charakteryzuje się tym, że do datagramu dodany jest nagłówek AH / ESP i dane datagramu (ramka TCP, UDP, ICMP, ...) zostają zabezpieczone (podpisane / zaszyfrowane) bezpośrednio za nim.



Rysunek 5. Postać chronionego datagramu w trybie transportowym

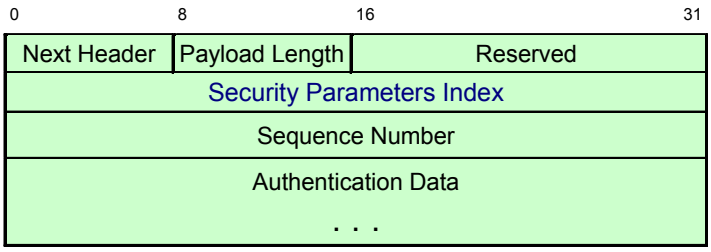
W trybie tunelowym (*tunnel mode*) natomiast oryginalny datagram IP zostanie zabezpieczony (podpisany / zaszyfrowany) w całości z nagłówkiem w ramkę protokołu AH / ESP, a następnie umieszczony w niezabezpieczonym datagramie IP jako jego dane.



Rysunek 6. Postać chronionego datagramu w trybie tunelowym

Protokół AH (Authentication Header)

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



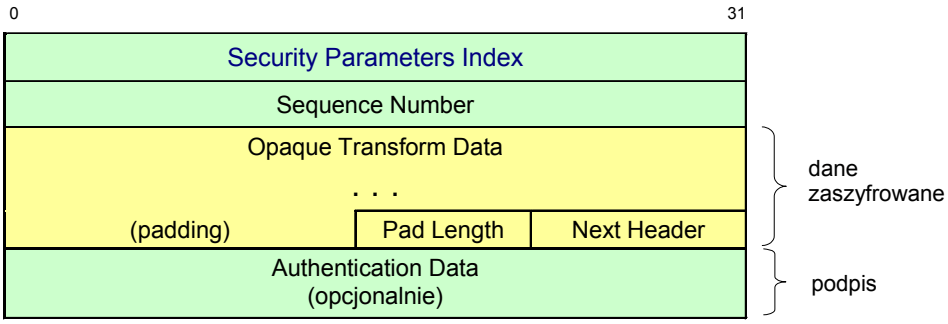
Rysunek 7. Schemat budowy datagramu protokołu AH

Protokół ESP (Encapsulating Security Payload)

Protokół ESP Umożliwia podpisywanie datagramu (stosuje te same algorytmy co w AH – uwzględnia w podpisie statyczne pola nagłówka podstawowego IP) oraz zaszyfrowanie

datagramu – wykorzystuje szyfry blokowe w trybie CBC, np. DES, 3DES (z 3-ma kluczami), Blowfish, CAST-128 czy Rijndael/AES, aktualnie również 3-IDEA (z 3-ma kluczami)

Nagłówek ESP jest umieszczany bezpośrednio przed zaszyfrowanymi danymi. Format i długość zaszyfrowanych danych zależy od wybranej metody kryptograficznej.



Rysunek 8. Schemat budowy datagramu protokołu ESP

Możliwe jest połączenie mechanizmów AH i ESP. Przykładowo, najpierw szyfrowane są dane za pomocą ESP, a następnie cały datagram jest zabezpieczony przez AH. Alternatywnie, najpierw wyznacza się nagłówek AH i umieszcza się go datagramie, a następnie szyfruje w całości przez ESP (tuneluje).

Asocjacja bezpieczeństwa (*Security Association*)

Asocjacja bezpieczeństwa SA jest to zbiór parametrów charakteryzujących bezpieczną komunikację między nadawcą a odbiorcą (kontekst), utrzymywany przez nadawcę i unikalnie identyfikowany przez SPI (*Security Parameters Index*). Blok parametrów asocjacji obejmuje następujące dane:

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.)

Asocjacja bezpieczeństwa (a dokładniej blok parametrów asocjacji) nie jest przesyłana siecią – przesyłany jest tylko numer 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).

Poniżej przedstawiony zostanie schemat działania stacji protokołu IPsec. Działania wykonywane przy wysyłaniu pakietu są następujące:

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
3. 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)
4. Wysłanie powstałego pakietu IP

Natomiast działania wykonywane przy odbieraniu pakietu są następujące:

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

Zarządzanie kluczami

Zarządzanie i dystrybucja kluczy nie są uwzględnione w specyfikacji samego standardu IPsec. Możliwe jest jednak wykorzystanie kluczy dwojakiego typu:

- klucze przypisane do użytkownika
- klucze przypisane do stacji sieciowej

Możliwe są też bardzo różnorodne sposoby dystrybucji:

- dystrybucja ręczna – administrator (małej sieci lokalnej) wyznacza wszystkie klucze
- wykorzystanie istniejących systemów dystrybucji (np. systemu 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)

Protokoły zarządzania kluczami mają na celu wzajemne uwierzytelnianie podmiotów nawiązujących asocjacje IPsec oraz uzgadnianie kluczy sesji na potrzeby poszczególnych kanałów SA. Obie te funkcje realizowane są na podstawie skonfigurowanych na stałe danych uwierzytelniających. Może to być np. hasło wspólne dla pary stacji (*shared secret*), certyfikaty X.509, klucze PGP. Niektóre implementacje (SKIP, Photuris) umożliwiają wyłącznie uwierzytelnienie na podstawie haseł, a popularny protokół IKE obsługuje natomiast wszystkie wyżej wymienione metody i umożliwia jeszcze prywatne rozszerzenia.

Protokół IKE (*Internet Key Exchange*)

Protokół 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. Protokół ISAKMP korzysta z UDP (port 500).

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.

Uwierzytelnianie może być realizowane na ogół na dwa sposoby. W najprostszym przypadku każda para węzłów musi mieć ustalone wspólne hasło, które służy do obliczania kluczy metodą Diffiego-Hellmana. Oznacza to konieczność konfigurowania haseł na wszystkich węzłach, co jest istotnym ograniczeniem tej metody i może okazać się zbyt pracochłonne w przypadku dużych sieci. Alternatywną metodą jest zastosowanie kluczy publicznych podpisanych przez nadrzędny urząd certyfikujący CA (np. certyfikatów X.509), które jest wolne od ograniczeń ręcznej definicji haseł.

protokół ISAKMP jest łatwo rozszerzalny. Pewne parametry (*Domain of Interpretation*, DOI) można przystosować całkowicie do potrzeb własnej instytucji:

- własny zestaw szyfrów
- własne mechanizmy uwierzytelnienia

PKI (*Public Key Infrastructure*)

Protokół 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. Znacznie ułatwia to realizację złożonych topologii.

Co istotne, IKE umożliwia też automatyczną renegocjację kluczy kryptograficznych co określony interwał (nawet często). W takim przypadku, 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. Implementacja obligowana jest by w przypadku renegocjacji klucza poprzedni klucz był usuwany z pamięci. Wówczas włamywacz nie znajdzie go w systemie nawet w przypadku opanowania systemu operacyjnego węzła.

Ograniczenia

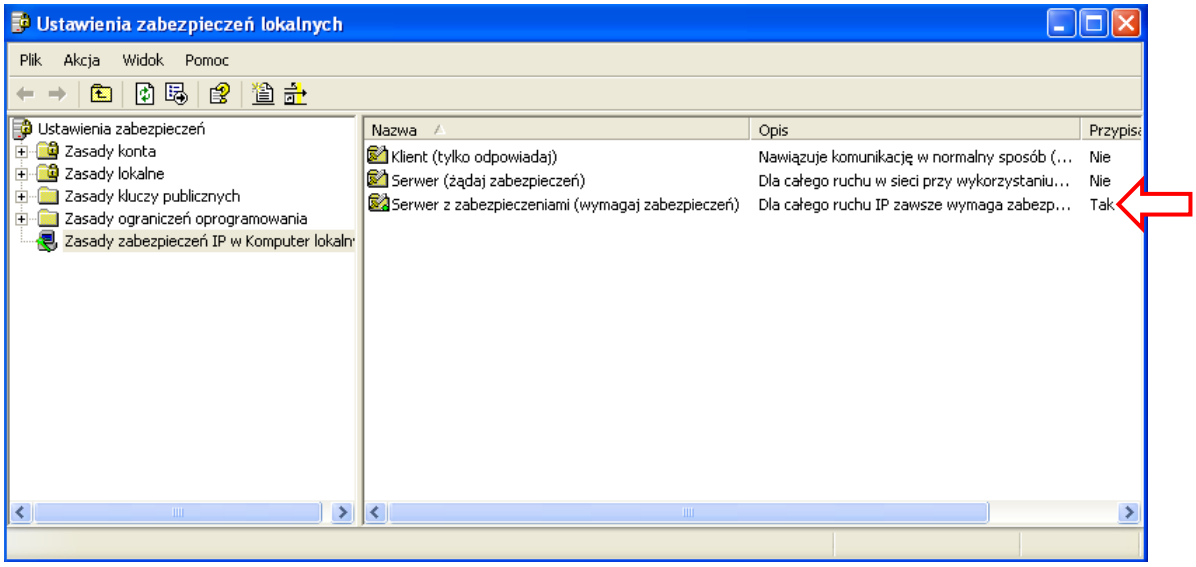
Protokół IPsec dobrze nadaje się do realizacji tuneli wirtualnych VPN. Jednak nie jest idealnym rozwiązaniem problemu bezpiecznej komunikacji. Praktycznie od początku był IPsec krytykowany za niekonsekwencje projektowe i nadmierne skomplikowanie. Wytykano, iż np. ochrona integralności zapewniana jest niemal w równym stopniu przez ESP, jak i AH. Niektóre odkryte błędy zostały usunięte w wersji z 1998 r. (np. część potencjalnych furtek do ataków DoS). Gwoli ścisłości należy zaznaczyć, iż zdiagnozowane 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.

Mimo tego jednak, IPsec jest wykorzystywany powszechnie i praktycznie nie ma dla niego alternatywy. Jako reprezentatywną opinię można przytoczyć tu podsumowanie analizy IPsec dokonanej w 1999 r. przez znanych kryptologów Nielsa Fergussona i Bruce'a Schneiera:

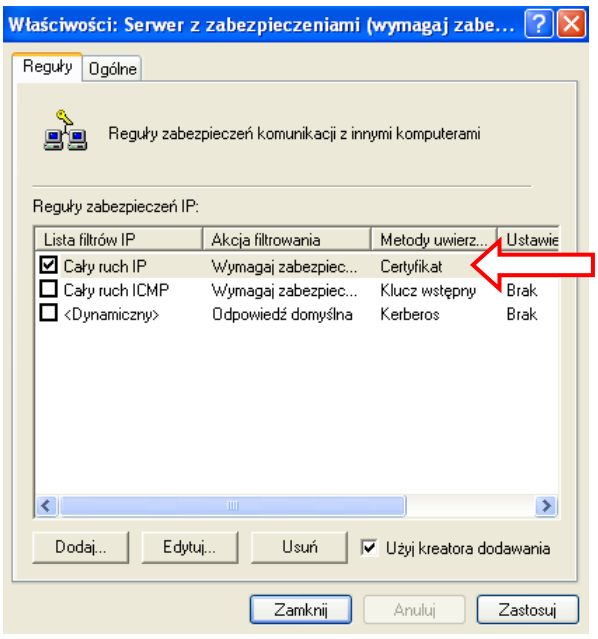
> *,,Nawet pomimo dość poważnych zarzutów jakie wysunęliśmy wobec IPSec, jest on prawdopodobnie najlepszym protokołem bezpieczeństwa z obecnie dostępnych. W przeszłości przeprowadziliśmy podobne analizy innych protokołów o analogicznym przeznaczeniu* (*w tym PPTP*)*. Żaden ze zbadanych protokołów nie 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."*

IPsec w Windows

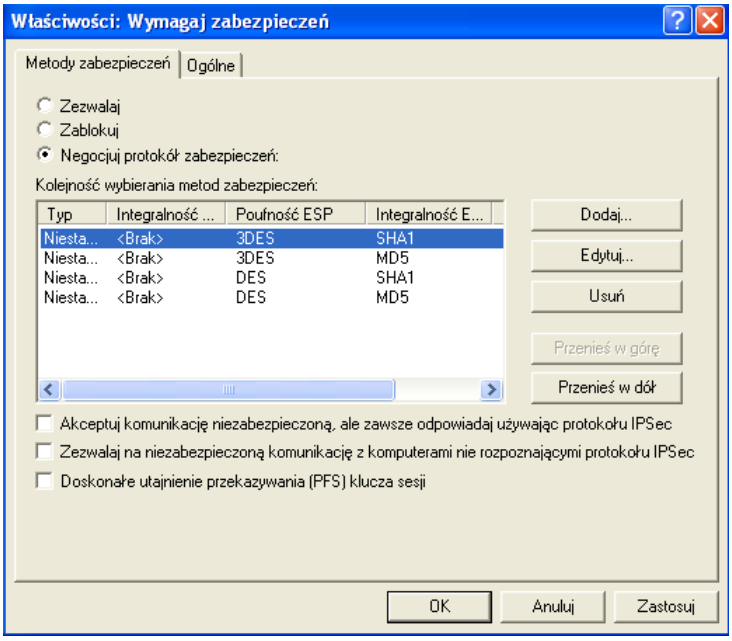
W Windows 2000 i XP wbudowano obsługę IPsec (ESP) zintegrowaną z usługą Active Directory. Sam IPsec tuneluje tylko ruch IP.



Rysunek 9. Uaktywnienie obsługi protokołu IPsec w Windows



Rysunek 10. Przykład definicji tunelowania ruchu IP



Rysunek 11. Szczegóły definicji tunelowania ruchu (zmienne parametry SA)

Bezpieczeństwo w IPv6

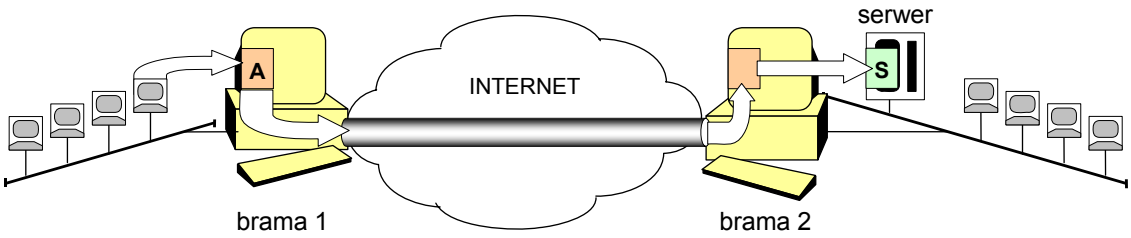
Uzupełniając wiadomości o protokole IPsec, należy dodać, iż jest on zintegrowaną częścią specyfikacji protokołu IP w wersji 6. Zatem w protokole IPv6 możliwe jest korzystanie z nagłówków AH i ESP jak z dowolnych innych opcji protokołu.

Propagowanie połączeń aplikacyjnych (*port forwarding*)

Aczkolwiek najbardziej uniwersalny tunel wirtualny osiągnąć można na poziomie warstwy sieciowej, to jednak mechanizmy kryptograficznej ochrony komunikacji można zaprząc do pracy w innych warstwach.

Szyfrowane propagowanie połączeń jest metodą realizacji tuneli wirtualnych na poziomie warstwy aplikacji. Oferuje je np. protokół SSH. Działanie mechanizmu propagowanie połączeń można przedstawić następująco (rysunek 12).

- połączenia na port **A bramy 1** są tunelowane do **bramy 2**
- i dalej propagowane na port **S serwera** w sieci lokalnej za **bramą 2**
- tunel między **bramą 1** a **bramą 2** jest szyfrowany
- komunikacja poza tunelem (w obu sieciach lokalnych – czyli od klienta do **bramy 1** oraz od **bramy 2** do serwera nie jest szyfrowana



Rysunek 12. Schemat działania propagacji połączeń

Tunele SSL

Tunele wirtualne można realizować na poziomie warstwy sesji. Znanym powszechnie przykładem jest SSL (*Secure Socket Layer*) – połączeniowy protokół oferujący dwupunktowy tunel kryptograficzny z wykorzystaniem certyfikatów, zaprojektowany z myślą o ochronie sesji takich protokołów jak HTTP, POP/IMAP, SMTP. SSL oferuje ochronę poufności, integralności i autentyczności danych. I tak przykładowo HTTPS – protokół HTTP tunelowany poprzez SSL – jest powszechnie wykorzystywaną w sieci internetowej usługą (port 443). Odpowiednio istnieją wersje tunelowane innych usług (POPS, IMAPS). W praktyce SSL potrafi tunelować dowolny ruch (stunnel, OpenVPN).

Aktualna wersja SSL nosi numer 3.0. Równolegle z tą wersją występuje jego następca – protokół TLS (*Transport Layer Security*). TLS v.1.0 jest standardem IETF – RFC 2246.

Pytania problemowe

1. Który tryb pracy protokołów IPsec – transportowy czy tunelowy – jest dogodniejszy dla konfiguracji: host-to-host, net-to-net, host-to-net?

2. Wyjaśnij dlaczego najbardziej uniwersalny tunel wirtualny osiągnąć można na poziomie warstwy sieciowej.