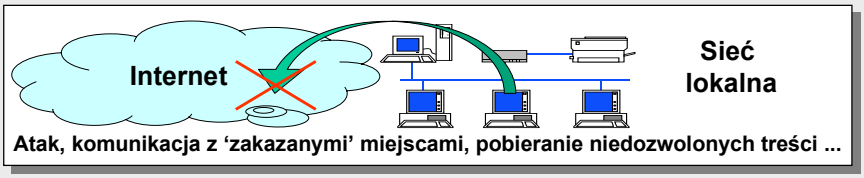
Ochrona dostępu do komputerów sieci

Zapory i wirtualne sieci prywatne (VPN)

Wprowadzenie

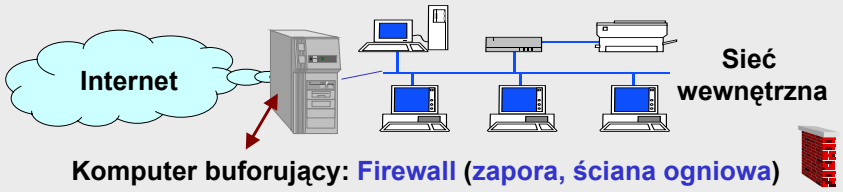
- Zadanie - zabezpieczyć komputery sieci lokalnej przed atakami (nieuprawnionym dostępem) z zewnątrz

- Uniemożliwić niedozwoloną działalność użytkownikom lokalnym



Wprowadzenie

Metoda - buforowanie sieci przez specjalizowaną jednostkę



Komputer buforujący: Firewall (zapora, ściana ogniowa)

Funkcja zapory

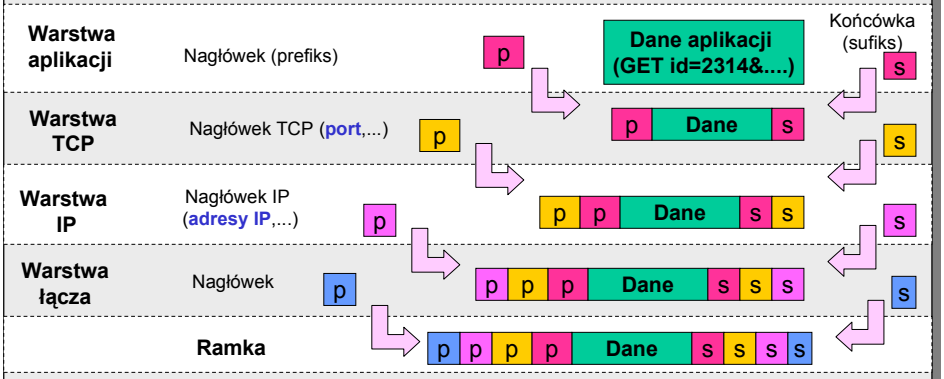
Ograniczenie dostępu do sieci dla jednostek i/lub danych, realizowane zgodnie z przyjętą polityką bezpieczeństwa

Sposób realizacji funkcji

- **Filtracja ruchu - odrzucanie pakietów naruszających określone warunki**
- **Ukrywanie struktury sieci wewnętrznej**
- **Ograniczenie komunikacji do komputerów znających wymagany sekret**

Pakiety

Mechanizm tworzenia pakietów TCP/IP

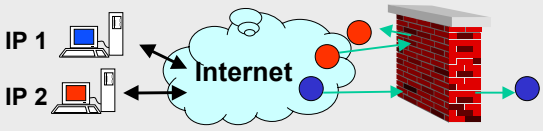


Ramka przesyłana w sieci zawiera adresy źródła i odbiorcy, port i dane aplikacji

Analiza pakietu pozwala wdrożyć zasady polityki bezpieczeństwa - kto z kim, jakie aplikacje i jakie treści

Kryteria filtracji pakietów

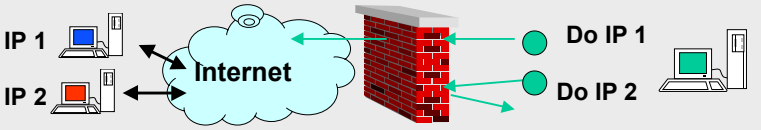
➡ **Adresy IP** - określenie dozwolonych/zakazanych stron komunikacji



Dozwolone	Zabronione
212.51.200.45	145.51.200.45
212.51.200.49	145.51.200.49
.....	.....
212.51.200.105	145.51.200.105

ACL
Access control list

Adres **nadawcy** porównywany z danymi ACL



Adres **odbiorcy** porównywany z danymi ACL

Spotykana nazwa podejścia - **filtracja poziomu warstwy IP**

Bezpieczeństwo systemów informatycznych

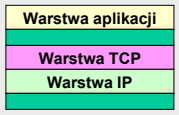
Kryteria filtracji pakietów

➡ **Numery portów** - wskazywanie dozwolonych usług i aplikacji

ACL

Dozwolone IN	Zabronione IN
212.51.200.45:22	212.51.200.45:23
212.51.200.49	145.51.200.22
.....	.....
212.51.200.105:80	145.51.200.105

Filtracja poziomu warstwy TCP ➡



➡ **Typ protokołu**

Jest niekoniecznie związany z numerem portu - aplikacja lub usługa może działać na jednym porcie według jednego protokołu, na jednym porcie według wielu protokołów lub na różnych portach według jednego protokołu

Krzysztof Ślot © 2002

Kryteria filtracji pakietów

- **Zawartość informacyjna pakietów - analiza treści wymienianych między aplikacjami**

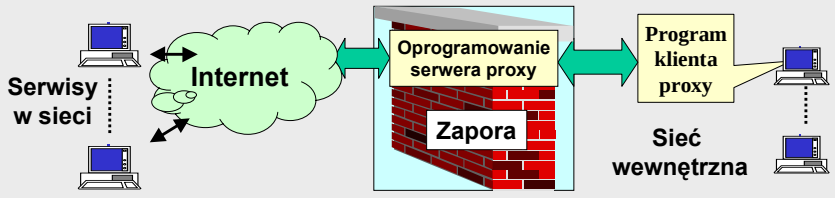
  Programy specjalizowane w analizie danych warstwy aplikacji pod kątem realizacji polityki bezpieczeństwa - serwery PROXY

  - **Serwer PROXY jest wyspecjalizowany w obsłudze jednego, konkretnego protokołu, np. FTP, HTTP ...**

- **Typowe zasady bezpieczeństwa określane dla protokołów**
  - **filtracja adresów źródła i przeznaczenia (HTTP - URL, FTP - nazwa hosta, katalogu)**
  - **eliminacja słów kluczowych protokołu (rozkazów aplikacji - PUT w FTP,** if (connected) erase_disk()**)**
  - **eliminacja konkretnych treści (słów i zwrotów)**
  - **eliminacja składników aplikacji (np. obiektów stron HTML - ActiveX...)**

Filtracja - serwery PROXY

- **Komunikacja z serwerem PROXY następuje za pośrednictwem odpowiedniego oprogramowania na komputerze klienta**
- **Serwer PROXY komunikuje się z zewnętrznymi serwerami usług w imieniu klientów sieci wewnętrznej**



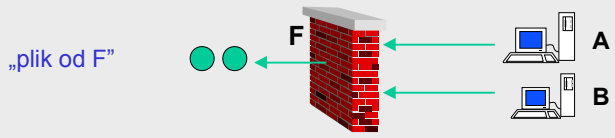
- **Właściwości serwerów PROXY**

  ☺ **Implementacja polityki bezpieczeństwa na najbardziej zaawansowanym poziomie**

Filtracja - serwery PROXY

Właściwości serwerów PROXY

☺ **Utajnienie struktury sieci wewnętrznej**



Strony nie wymieniają pakietów bezpośrednio - nie istnieje bezpośrednie połączenie między komputerami sieci wewnętrznej i sieci zewnętrznej

☹ **Operacje filtracji są kosztowne obliczeniowo**

Serwery PROXY - filtracja poziomu warstwy aplikacji

Metody filtracji pakietów

Stosowane procedury filtracji (dowolna warstwa)

- **Filtracja statyczna**

  Reguły filtracji pakietów są sztywno ustalone w postaci list, pakiety są analizowane niezależnie

  ☺ **Szybkość analizy pakietów, prostota zasad (realizacje sprzętowe)**

  ☹ **Istnienie stałego połączenia między maszynami, mała elastyczność**

- **Filtracja dynamiczna**

  Zasady filtracji mogą być zmieniane w trakcie pracy, zgodnie z rozwojem sytuacji, pakiety są analizowane niezależnie

  Na przykład, pakiety FTP będą przepuszczane dopiero gdy komputer z sieci chronionej chce nawiązać sesję, po zakończeniu sesji następuje zamknięcie kanału

Metody filtracji pakietów

➡ **Inspekcja stanu komunikacji** (stateful inspection)

Analizowane relacje między pakietami

Cel — **Monitorowanie stanu lub kontekstu połączenia pozwalające na detekcję aktywności charakterystycznej dla potencjalnego ataku**

➡ **Metoda postępowania**

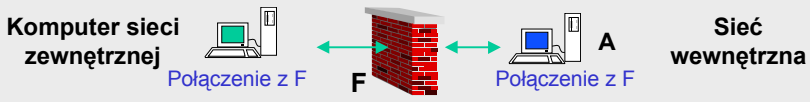
- **Rejestracja historii połączeń - tablica połączeń**
- **Przeglądanie tablicy i analiza pakietów dochodzących i wychodzących w celu określenia odpowiadających sobie par oraz ewolucji połączenia**

Technika konieczna dla zapewnienia ochrony przed pewnymi rodzajami ataków (SYNFlood, IPSpoofing, LAND, teardrop)

Zapory - NAT, PAT

➡ **NAT - network address translation**

Cel - ukrywanie adresów IP komputerów sieci wewnętrznej



- **Metoda realizacji: zapora przekształca pakiety, zamieniając adresy IP nadawcy i odbiorcy - nie istnieje bezpośrednia łączność stron komunikacji**
- **NAT pozwala używać adresy zarezerwowane - np. z puli** 10.x.x.x

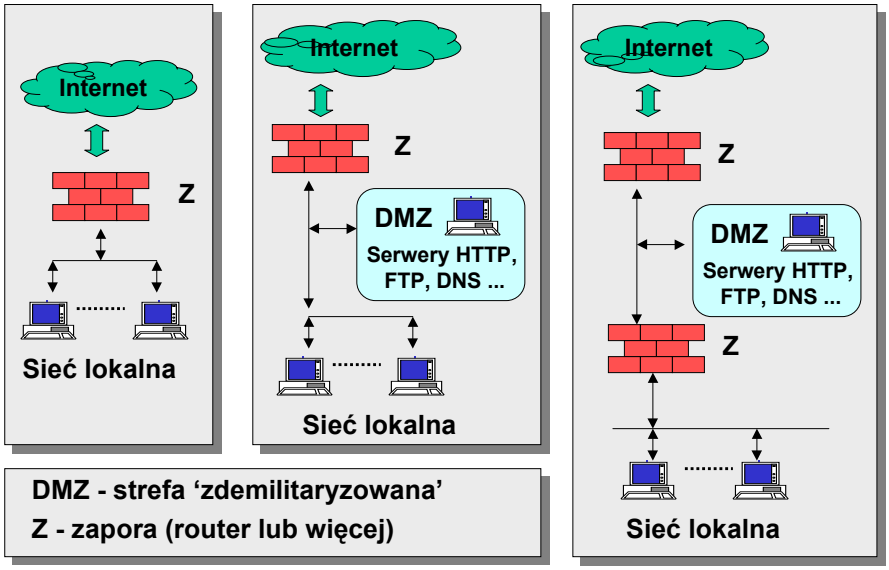
➡ **PAT - port-address address translation**

Cel - ukrycie numeru portu docelowego

- **Metoda realizacji: zapora przepisuje pakiet, odpowiednio zmieniając port**

Przykład - ukrycie portu komunikacji z bazą danych z poziomu appletu w stronie www (niedozwolone polityką ochrony zapory F)

Zapory - architektury



Zapory - architektury

- **Architektura DMZ**
  - Chroni klientów sieci przed atakami przypuszczanymi na serwery usług publicznych
  - Zapora - sieć lokalna - DMZ: 'Dual Homed Gateway' - zapora pośredniczy w ruchu do dwóch sieci wewnętrznych - maszyn użytkowników i serwerów usług publicznych
- **Architektura z podwójną zaporą**
  - Uniezależnienie ochrony komputerów sieci lokalnej i serwerów usług publicznych
  - Najbezpieczniejsza
- **Zapory osobiste (personal firewalls)**
  - Programy do instalacji na komputerach sieci lokalnej - ostatnia linia obrony, pozwalająca na indywidualne zaostrzenie zabezpieczeń

Zapory - bezpieczne połączenia

- Trzecia technika ochrony - tzw. Circuit-level (CL) firewall
  - Implementacja zasady uwierzytelniania z wykorzystaniem tajnych, współdzielonych kluczy
  - Uwierzytelnianie stron komunikacji dokonywane jest tylko w fazie ustanawiania połączenia - dalsza komunikacja nie jest analizowana
  - Działanie sprowadza się do ustanowienia wirtualnego obwodu - bezpiecznego połączenia klient-serwer (nazwa metody)
  - W połączeniu zawsze pośredniczy zapora - dla każdej sesji klient-serwer istnieją dwa połączenia: klient-zapora i zapora-serwer.
  - Sposób implementacji zapór typu CL - SOCKS
  - Zapory typu CL wymagają zmian w aplikacjach użytkowych

Zapory - podsumowanie

- Określenie i wdrożenie polityki bezpieczeństwa w jednym miejscu
- Określenie typu zapory i mechanizmów ochrony

  Fizyczna postać zapory - software, router monitorujący (screening router), dedykowany komputer. Wybór architektury systemu.
  Wybrane metoda ochrony - odpowiednia filtracja pakietów, utworzenie kanałów komunikacji, kombinacja obydwu podejść.
- Implementacja reguł bezpieczeństwa w posiadanych zasobach

Założenie Obsługa serwisu pocztowego (SMTP) za wyjątkiem hosta zly.com

Wdrożone zasady

Statyczna filtracja pakietów poziomów IP i TCP	Odrzucaj pakiety od IP = zly.com Zezwalaj używanie protokołu SMTP Zezwalaj na korzystanie z portu 25 TCP

- Zapory nie chronią przed: atakami od wewnątrz, innymi drogami - modemy itp, wirusami ...

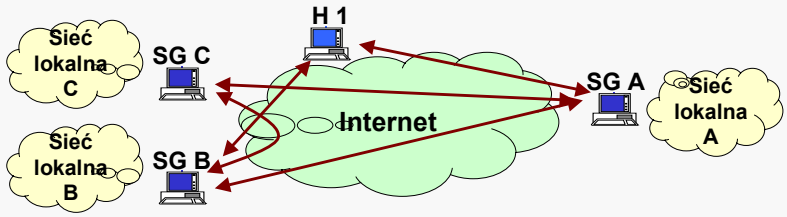
VPN

Wirtualne Sieci Prywatne
Virtual Private Networks

- Wykorzystanie istniejącego połączenia (Internetu) do realizacji sieci połączeń o ograniczonej liczbie użytkowników
  - Brak kosztów instalacji sieci
- Metoda - tworzenie połączeń tunelowanych
- Wprowadzenie mechanizmów bezpieczeństwa
  - Uwierzytelnianie
  - Ochrona poufności, integralności i autentyczności danych
- Z punktu widzenia realizacji polityki bezpieczeństwa VPN to rozwinięcie koncepcji zapór typu CL

VPN

- Elementy VPN
  - Specjalizowane bramy bezpieczeństwa (security gateway - SG) - chroniące dostępu do sieci prywatnej (= zapory)
  - Komputery (H), wyposażone w odpowiednie oprogramowanie
- Możliwe typy połączeń: H - H, H - SG, SG - SG



- Podstawowy (obecnie) protokół komunikacji VPN

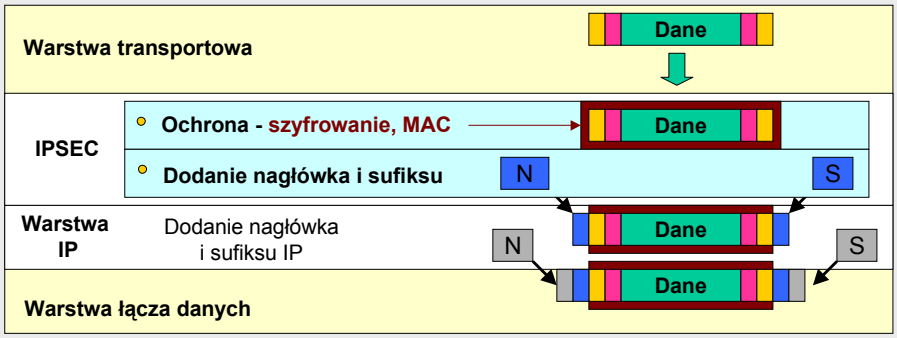
IPSec - (IP security protocol)

IPSEC

- IPSEC to zbiór procedur i protokołów niezbędnych dla ustanowienia bezpiecznej komunikacji oraz zbiór narzędzi dla realizacji ochrony poufności, integralności i autentyczności danych
  - Negocjowane protokoły bezpieczeństwa
  - Negocjowane algorytmy ochrony i wymiany poufnych informacji
- Metoda ochrony to 'opakowanie' przesyłanych danych w ochronne 'kapsułki' ('kapsułkowanie' protokołów)
- IPSEC ma dwa tryby pracy
  - Tryb transportowy
    Ochronie podlega zawartość pakietów wyższych warstw
  - Tryb tunelowy
    Chroniony jest cały pakiet - tworzony jest nowy nagłówek IP

IPSEC

- Tryb transportowy



  - Zawartość pakietu jest chroniona (uwierzytelniona i/lub zaszyfrowana)
  - Nagłówek IP i nagłówek IPSEC są niezależne
- Identyfikator protokołu IPSEC to liczba 50 w polu protokół IPv4 lub w polu NEXT_HEADER IPv6

Protokół IPSEC

Polityka bezpieczeństwa

- Określenie sieci lokalnych i indywidualnych komputerów tworzących sieć VPN
- Instalacja i konfiguracja systemu

Podstawowa różnica w stosunku do formułowania zasad bezpieczeństwa dla zapór (za wyjątkiem zapór CL) tkwi w istocie komunikacji VPN - zawsze odbywa się ona między uwierzytelnionymi i z góry określonymi stronami

Protokoły składowe IPSEC

- Komunikacja
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- Wymiana kluczy
  - IKE (internet key exchange)

Bezpieczeństwo systemów informatycznych

Protokół IPSEC

Protokoły zapewnienia bezpieczeństwa ruchu IPSEC

- Authentication Header (AH) ➡ □
- Encapsulating Security Payload (ESP) ➡ □

□ □ Uwierzytelnienie źródła danych
□ □ Kontrola integralności danych
□ □ Odrzucanie powtórnie przesyłanych pakietów
□ □ Kontrola dostępu (do części zasobów)
□ Częściowe ukrycie ruchu w sieci
□ Ochrona poufności danych (szyfrowanie)

ESP i AH mogą być używane niezależnie lub jednocześnie

Szyfrowanie danych w IPSec

DES i 3DES

Krzysztof Ślot © 2002

IPSEC

Gospodarowanie kluczami

- Każdy z węzłów VPN musi posiadać unikalny klucz i znać klucze (publiczne lub współdzielone) innych węzłów
- Ustalenie kluczy sesyjnych następuje według protokołu IKE lub jego odmian

Protokoły nawiązania połączenia i wymiany kluczy

EAP (Enhanced Authentication Protocol) - implementacja WIndows

- EAP-MD5 = CHAP
- EAP-TLS (bazujący na SSL) - korzysta z certyfikatów i kryptografii klucza publicznego. Podstawowe cechy:

  - obustronna weryfikacja certyfikatów
  - generacja i wymiana klucza sesyjnego przy użyciu kluczy publicznych stron

Bezpieczeństwo systemów informatycznych

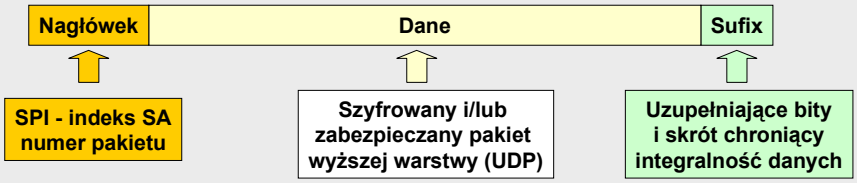
IPSEC

Procedura komunikacji

- Inicjalizacja połączenia
- Wymiana kluczy i utworzenie SA (security association)

SA zawiera zbiór informacji dotyczących konkretnego połączenia: protokół (AH, EP lub oba), uzgodniona metoda szyfrowania, uzgodniona metoda uwierzytelniania, utworzone klucze, czas ważności kluczy i czas ważności SA oraz identyfikator połączenia (SPI - security parameter index)

Pakiet IPSEC



Krzysztof Ślot © 2002

IPSEC

Procedura komunikacji

- **Uaktualnienie bazy danych Security Policy Database (SPD) informacjami o nowym SA**
- **Sesja**

  Pakiety (na podstawie analizy nagłówka) są przetwarzane na jeden z trzech sposobów, zależnie od zasad określonych w SPD:
  - **Skorzystanie z narzędzi IPSec**
  - **Odrzucenie pakietu**
  - **Ominięcie ingerencji IPSec**

Skorzystanie z narzędzi IPSec

Dla pakietu, na podstawie SPI, określane są zapisane w SA zasady postępowania z pakietem - np. uwierzytelnić metodą xxx i odszyfrować metodą yyy

VPN w dostępie zdalnym

Protokoły komunikacji dostępu zdalnego

- PPP (point-to-point protocol)
- PPTP (point-to-point tunneling protocol)
- L2F - (layer-2 forwarding)
- L2TP - (layer-2 tunneling protocol)

PPP

Protokół transportowy dla pakietów warstwy 2 między użytkownikiem a NAS (network access server), przy użyciu modemu, ISDN itp. Połączenie PPP to połączenie użytkownik-NAS (identyczne z L2).

VPN w dostępie zdalnym

L2TP - połączenie PPTP i L2F

- **L2TP rozszerza PPP w taki sposób, że połączenie PPP kończy się w koncentratorze, skąd dalej pakiety są komutowane do NAS. Oznacza to brak konieczności fizycznego (L2) połączenia między użytkownikiem a NAS. Podstawowa korzyść i pierwotnie, powód wprowadzenia - oszczędności. Pakiety są 'tunelowane' przez sieć od koncentratora do komputera docelowego.**
- **Tunel w podstawowej wersji L2TP nie daje żadnej ochrony danych (nie ma technik szyfrowania)**
- **Rozszerzenie L2TP - adaptacja IPSec jako protokołu transportowego**