Bezpieczna komunikacja w sieci

Protokoły bezpiecznej komunikacji

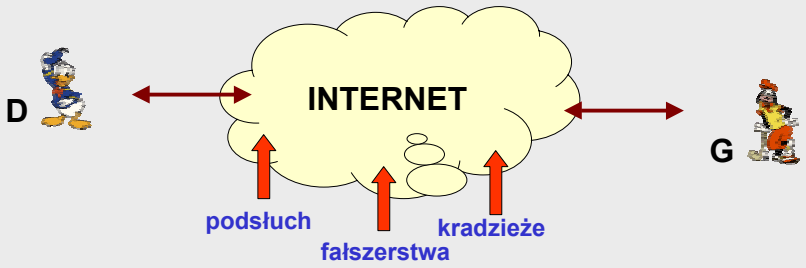
Wprowadzenie

- **Protokoły bezpiecznej komunikacji a model OSI**
  - Warstwa sieciowa - IPSec
  - Warstwa aplikacji - SSH, SSL, S/MIME, PGP
- **Wykorzystanie protokołów bezpiecznej komunikacji**
  - Handel elektroniczny (przeglądarki internetowe) - SSL
  - Zdalny dostęp do poufnych danych (przeglądarki - SSL)
  - Zdalny dostęp do zasobów komputera - SSH
  - Bezpieczna poczta - S/MIME, PGP/MIME
  - Wirtualne sieci prywatne (VPN) - IPSec (L2TP)

Protokoły

➡ **Sformułowanie problemu**

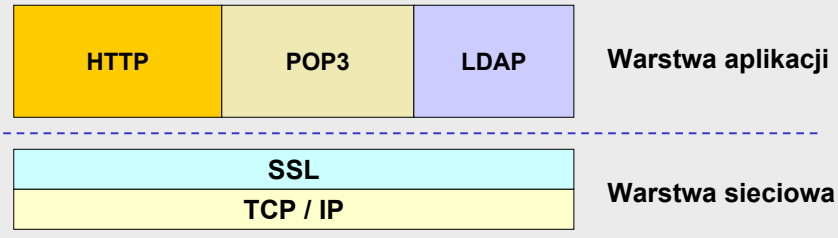
Zapewnić bezpieczeństwo sesji pomiędzy dwoma aplikacjami działającymi na dowolnych dwóch komputerach sieci
(komunikujących się za pomocą protokołu TCP/IP**)**



D i G nie są sobie uwierzytelnione przez jednostkę nadrzędną (jak np. centrum autoryzacji w systemie Kerberos)

Protokół SSL

SSL a warstwowy model OSI



➡ **Warstwy ochrony**

- **Uwierzytelnianie serwera i opcjonalnie klienta (RSA, DH, DSA)**
- **Ochrona poufności danych - szyfrowanie (DES, AES, IDEA...)**
- **Ochrona autentyczności i integralności danych - MAC**

➡ **Typowe zastosowanie - przeglądarki (HTTPS)**

- **Ograniczenia eksportowe na silną kryptografię (512b RSA itp.)**

SSL - ustanowienie sesji

0

HTTP

Wybranie linku do strony chronionej przez serwer WWW protokołem HTTPS

HTTPS

1

Nawiązanie połączenia

Klient	Serwer
Wiadomość CLIENT_HELLO Wersja SSL, liczba losowa (24B), czas, lista **proponowanych** algorytmów szyfrowania symetrycznego i metod wymiany klucza sesji, ID (nowa sesja-0)	
	Analiza i odesłanie SERVER_HELLO Wersja SSL, liczba losowa (24B) i czas, **wybrana** metoda wymiany klucza sesji, **wybrany** algorytm szyfrowania symetrycznego i wyznaczania skrótu, ID przyznany sesji

Bezpieczeństwo systemów informatycznych

SSL - ustanowienie sesji

2

Uwierzytelnienie

Klient	Serwer
	Wysłanie certyfikatu Krok jest opcjonalny i jest pomijany w przypadku uzgodnienia do wymiany klucza prostego wariantu metody Diffie-Hellmana. Jeżeli certyfikat jest wysyłany to ma on format określony przez X.509
Weryfikacja certyfikatu Weryfikacji podlegają: data ważności, CA, dane certyfikatu. Jeżeli CA nie znajduje się na liście zaufanych ośrodków - kontynuacja sesji zależy od użytkownika. Niepomyślna weryfikacja to zerwanie sesji. Pomyślna - serwer jest uwierzytelniony	
	Opcjonalne żądanie certyfikatu klienta Zwykle pomijane (serwer nie ma wtedy klucza publicznego klienta)
Wysłanie certyfikatu	
	Weryfikacja certyfikatu klienta

Krzysztof Ślot © 2002

SSL - ustanowienie sesji

3 **Ustanowienie klucza sesji**

Klient	Serwer
Generacja i wysłanie sekretu wstępnego Tzw. sekret wstępny (pre-master secret) to liczba losowa, o długości zwykle 48B. Sekret jest szyfrowany kluczem publicznym - klucz jest w posiadaniu klienta (w wyniku wymiany certyfikatu) lub jest dosyłany na osobną prośbę klienta (gdy ograniczenie eksportowe długości klucza do 512b)	**Deszyfracja sekretu wstępnego** Odszyfrowanie przy użyciu klucza prywatnego

Utworzenie kluczy szyfrowania i uwierzytelniania (MAC)

Klucze są tworzone na bazie wymienionego sekretu wstępnego i wymienionych w pierwszej fazie połączenia liczb losowych (serwera - LS i klienta - LK) w następujący sposób: tworzony jest tzw. sekret główny (master secret) MS = HASH(sekret wstępny, LS, LK). MS ma 48 bajtów i jest używany do generacji kluczy w drodze uzgodnionej procedury (algorytmy wyznaczania liczby losowej inicjalizowanej MS)

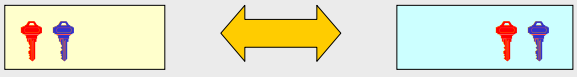
Bezpieczeństwo systemów informatycznych

SSL - ustanowienie sesji

4 **Zakończenie procedury ustanawiania sesji**

Wymiana komunikatu zakończenia fazy ustanawiania połączenia

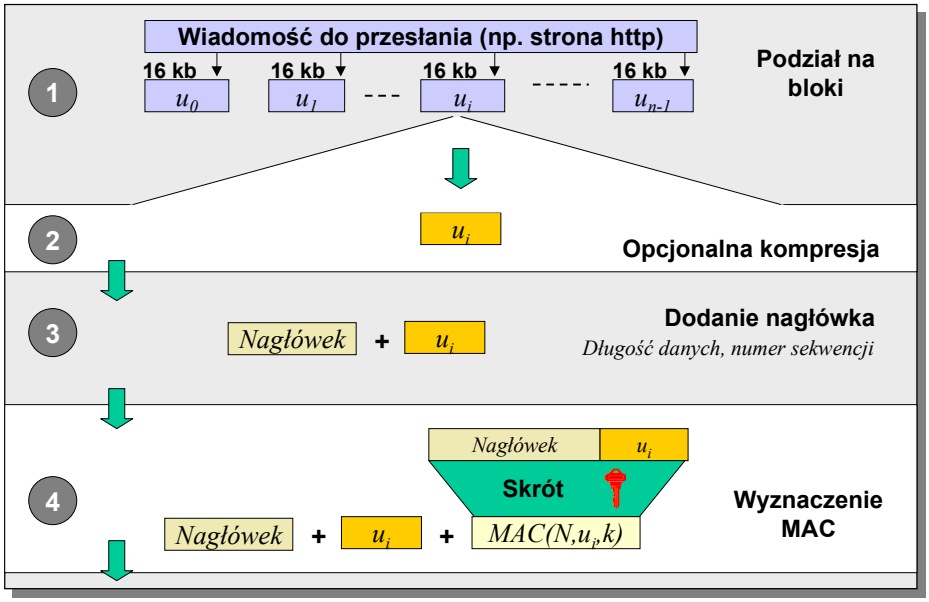
Komunikat jest pierwszą wiadomością zaszyfrowaną według protokołu transmisji, wykorzystującego uzgodnione parametry kryptograficzne - szyfr symetryczny i przyjętą metodę uwierzytelniania



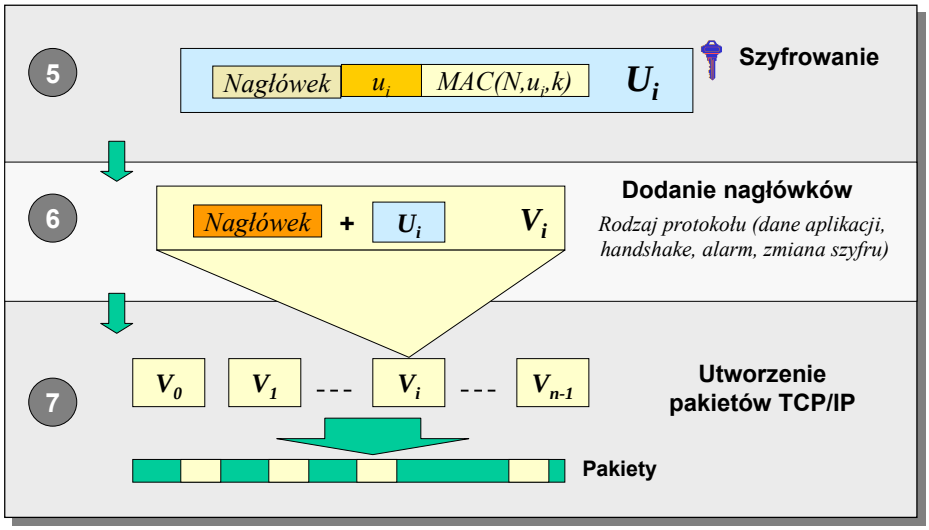
Parametry sesji są zapamiętane na serwerze i używane przy każdym kolejnym połączeniu - procedura ustanawiania sesji nie jest powtarzana

Krzysztof Ślot © 2002

Transmisja danych w SSL



Protokół transmisji danych w SSL

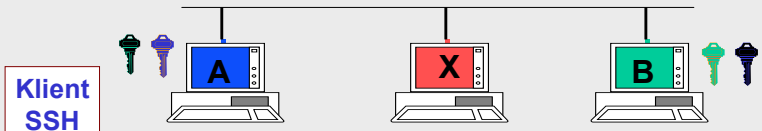


Protokół SSH

- Wprowadzony dla zapewnienia bezpiecznej realizacji operacji zdalnych systemu UNIX - rsh, rcp, rlogin.
- Połączenie odbywa się przez gniazdo TCP/IP (port 22)
- Wbudowana kompresja przesyłanych danych (LZ78 - ZIP)

Czynności konfiguracyjne

Generacja par kluczy RSA na komputerach chronionych protokołem



Klient SSH

Klucz tajny A - KT_A

Klucz jawny B - KJ_B

Klucz tajny B - KT_B

Klucz jawny A - KJ_A

Serwer SSH

Protokół SSH

Połączenie

- Uzgodnienie wersji protokołu (v.2)
- Uwierzytelnienie serwera przez klienta (liczba losowa szyfrowana kluczem publicznym
- Utworzenie klucza sesji (serwer)
- Sesja szyfrowana (szeroki wachlarz dostępnych metod)

Tunelowanie połączeń

- SSH pozwala na przekierowanie komunikacji odbywającej się między dowolnymi aplikacjami dwóch komputerów do utworzonego, bezpiecznego kanału (‘tunelu’). Pakiety adresowane do aplikacji na dowolny port są kierowane na port 22 i odpowiednio oznaczane, a następnie, w komputerze odbiorcy są dostarczane do odpowiedniej aplikacji przez mechanizmy SSH.

Protokół SSH

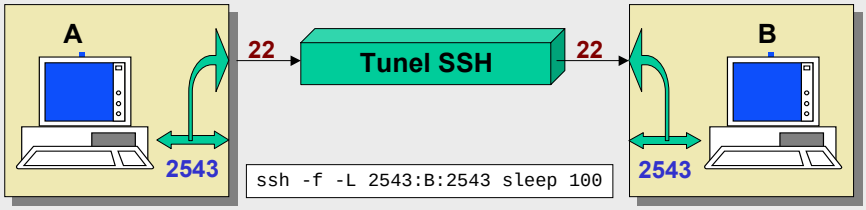
Przekierowanie lokalnego portu TCP

Założenia:

- Serwis X, nieszyfrowany oferowany przez B na porcie p (2543)
- Istnieje tunel SSH między komputerami (B jest serwerem SSH)

Cel

Wykorzystać kanał szyfrowany dla serwisu X




```
ssh -f [user@remote host] -L [local port]:[remote host]:[remote port] [some command]
```


Bezpieczeństwo systemów informatycznych

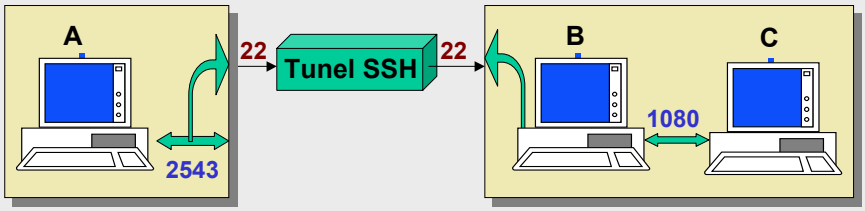
Protokół SSH

Przekierowanie portu zdalnego

Założenia:

- Serwis X, nieszyfrowany oferowany przez C na porcie p (1080)
- C jest połączony z B
- Istnieje tunel SSH między komputerami A i B

Cel Wykorzystać kanał szyfrowany dla komunikacji A - C




```
ssh -f -R 2543:B:1080 C sleep 100
```

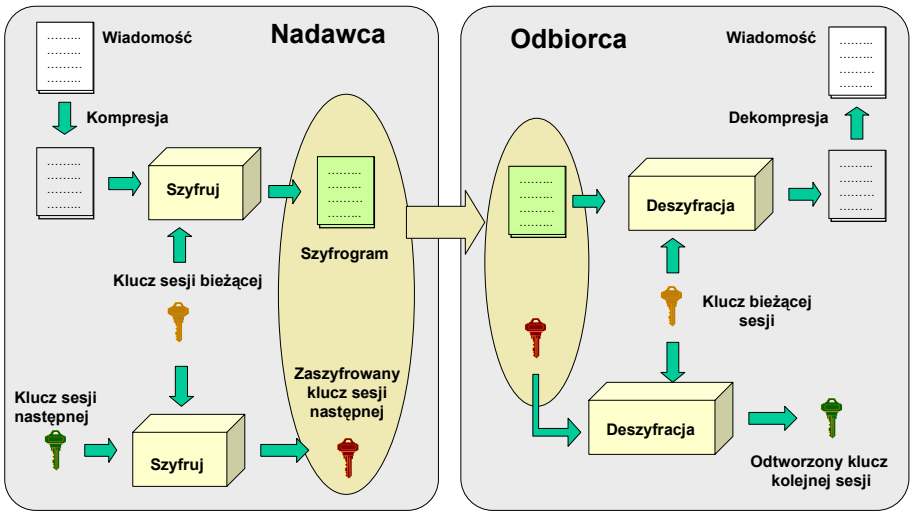
Krzysztof Ślot © 2002

PGP (1991)

- **Uwierzytelnianie**
  - **Algorytm DSA**
  - **Uwierzytelnianie może dotyczyć każdej wiadomości**
- **Poufność**
  - **Wiadomości są szyfrowane, przy czym klucz szyfrowania jest dla każdej wiadomości inny**

    Klucz dla kolejnej wiadomości jest dołączany do wiadomości bieżącej. Kluczem jest 128 bitowa liczba losowa. Liczba ta jest generowana przy wykorzystaniu informacji o ruchu myszki i uderzeniach klawiszy mających miejsce w czasie trwania sesji (losowość). Klucz jest szyfrowany kluczem publicznym odbiorcy wiadomości.
- **Kompresja**
  - **Zwiększenie odporności na ataki kryptograficzne**

Komunikacja w PGP



Klucz prywatny PGP szyfrowany skrótem ‘passphrase’ - frazy

PGP a poczta elektroniczna

- PGP może być użyte do szyfrowania poczty ...

```
From: Hans Kloss <hkloss@abwehra.org>
  To: Czapajew Gieroj<cg@pik.su>
  Mime-Version: 1.0
  Content-Type: multipart/encrypted; boundary=nic;
    protocol="application/pgp-encrypted"

  -- nic
  Content-Type: application/pgp-encrypted
  Version: 1
  -- nic
  Content-Type: application/octet-stream
  -----BEGIN PGP MESSAGE-----
  Version: 2.6.2

  HUYGTf(*jlwonemfysiru*uenrbxhBYlE37(B&Bc0&DBHD89nfszfwtm.fosneu-fnebV
  oencjisurgt9OJBFYVywyc56Vhjlflgojhmoom957s7&(T^59n.gJOInf8^%d0eamqVW3
  c-d=)dmgj:firngig-*Bld.KGNUXVydo*hfirl87sgbuebvyVtcdkurbvauduygsv=
  -----END PGP MESSAGE-----
  -- nic --
```

- ... i podpisywania

```
Content-Type: multipart/signed; boundary=granica; micalg=pgp-md5;
  protocol="application/pgp-signature"
```

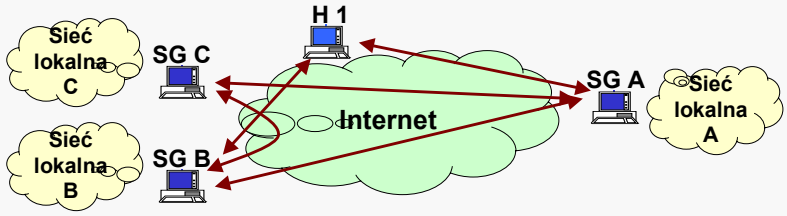

VPN

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

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)

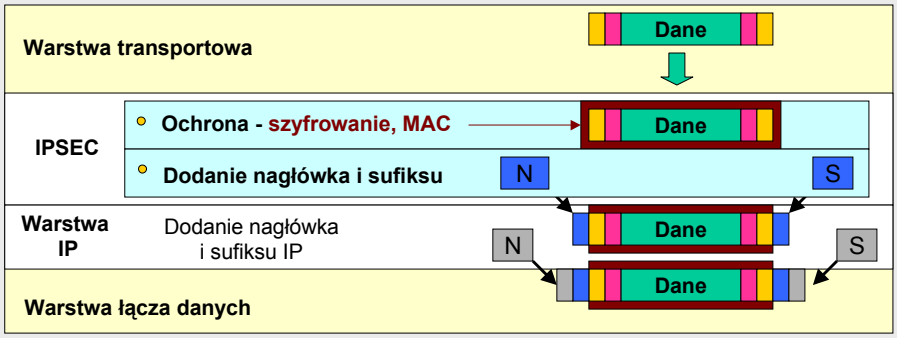
IPSEC

- **IPSEC to zbiór procedur i protokołów dla realizacji ochrony poufności, integralności i autentyczności danych**
- **Protokoły składowe IPSEC**
  - Komunikacja: Authentication Header, Encapsulating Security Payload
  - Wymiana kluczy IKE (internet key exchange)
- **Metoda ochrony to 'opakowanie' przesyłanych danych w ochronne 'kapsułki' ('kapsułkowanie' protokołów)**
- **Procedura komunikacji**
  - Inicjalizacja połączenia
  - Wymiana kluczy i utworzenie SA (security association)

    SA to informacje o danym połączeniu: protokół (AH, EP lub oba), metody ochrony, klucze, sesji, ważność kluczy i SA oraz ID sesji (SPI)
  - Odczyt SPI pakietu - pobranie z SA przyjętych zasad postępowania (np. uwierzytelnić metodą xxx i odszyfrować metodą yyy)

IPSEC

- **Tryby pracy IPSEC**
  - Transportowy - chroniona zawartość pakietów wyższych warstw
  - Tunelowy - chroniony cały pakiet (nowy nagłówek IP)
- **Tryb transportowy**



- Zawartość pakietu jest chroniona (uwierzytelniona i/lub zaszyfrowana)
- W trybie transportowym nagłówek IP i nagłówek IPSEC są niezależne

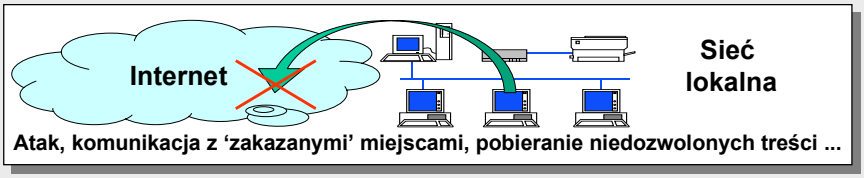
Ochrona dostępu do komputerów sieci

Zapory

Wprowadzenie

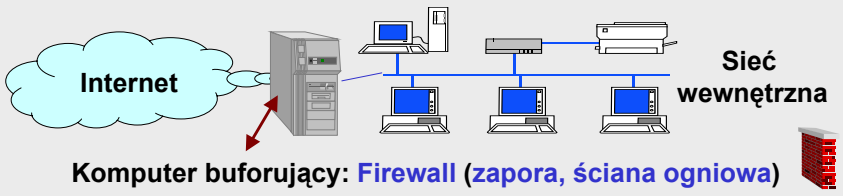
- Zadanie - zabezpieczyć komputery sieci lokalnej przed atakami (nieuprawnionym dostępem) z zewnątrz

- Uniemożliwić niedozwoloną działalność użytkownikom lokalnym



Wprowadzenie

- Metoda - buforowanie sieci przez specjalizowaną jednostkę



Komputer buforujący: Firewall (zapora, ściana ogniowa)

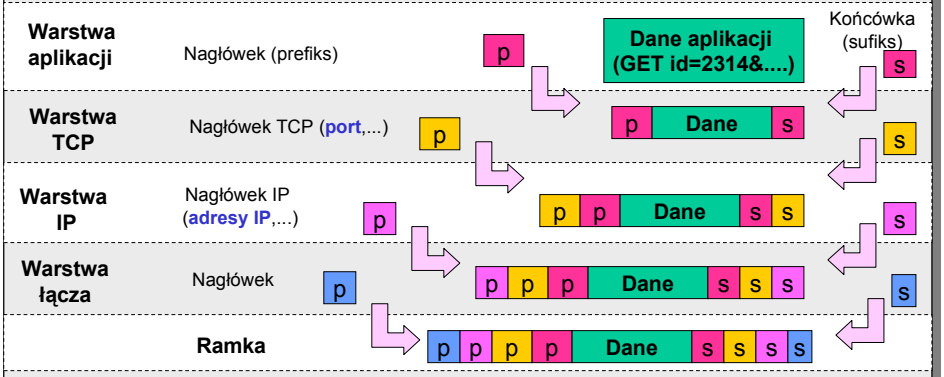
- Funkcja zapory

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

Zapory - filtracja pakietów

Mechanizm tworzenia pakietów TCP/IP

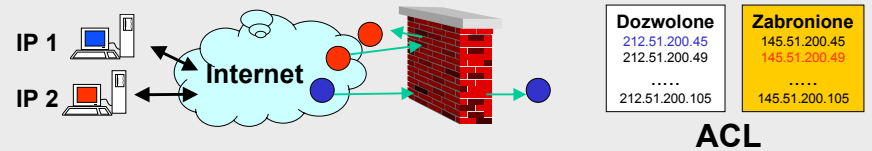


Ramka przesyłana w sieci zawiera adresy źródła i odbiorcy, port i dane aplikacji

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

Kryteria filtracji pakietów

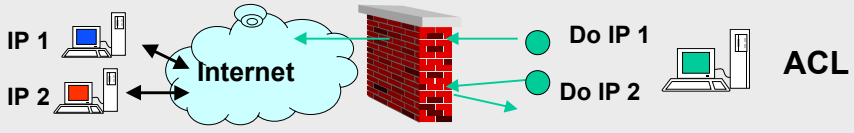
Adresy IP - określenie dozwolonych/zakazanych stron komunikacji



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

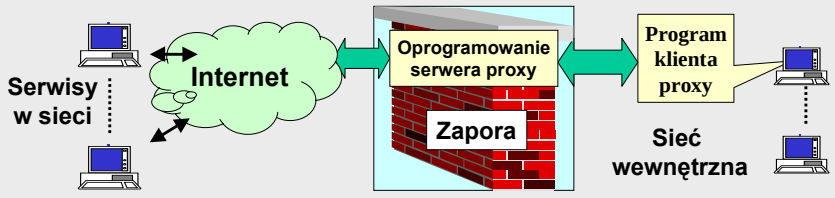
Kryteria filtracji pakietów

- **Numery portów** - wskazywanie dozwolonych usług i aplikacji
  ACL : 212.51.200.45:23-zabronione ⇨ Filtracja poziomu warstwy TCP

- **Typ protokołu** (niekoniecznie związany z numerem portu)
- **Zawartość informacyjna pakietów** - analiza treści
  - 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 analizowane elementy pakietów
  - adresy źródła i przeznaczenia (HTTP - URL, FTP - nazwa katalogu)
  - słowa kluczowe protokołu (rozkazy, np. PUT w FTP)
  - konkretne słowa i zwroty
  - składniki aplikacji (np. obiekty stron HTML - ActiveX..., applety)

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

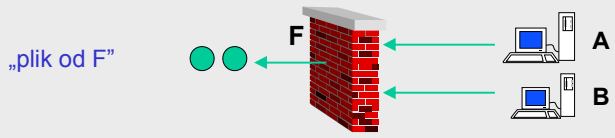


- Właściwości serwerów PROXY
  ☺ Implementacja polityki bezpieczeństwa na najbardziej zaawansowanym poziomie

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

Zapory - NAT, PAT

Dotyczy filtracji poziomu warstw IP i TCP (a nie w. aplikacji)

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**

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

Bezpieczeństwo systemów informatycznych

Metody filtracji pakietów

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

  Analizowane relacje między pakietami

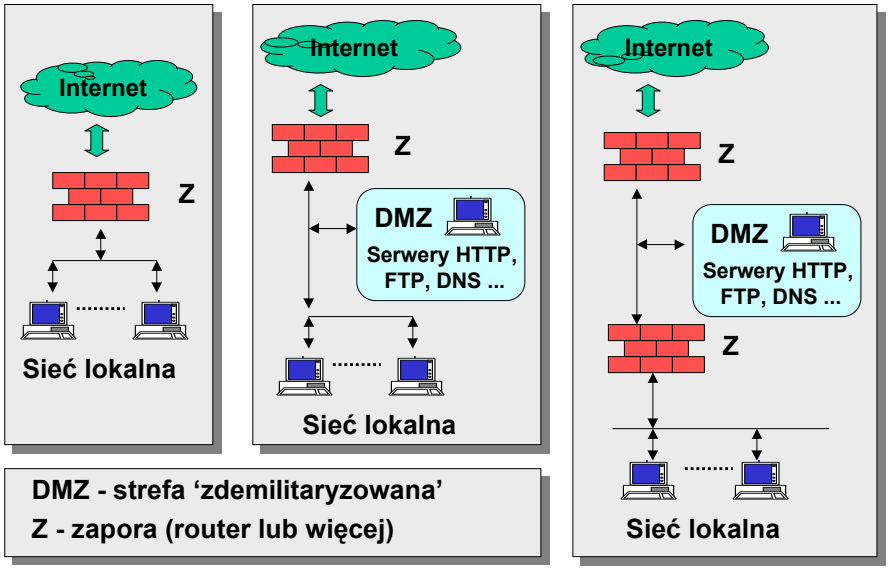
  Cel — **Monitorowanie stanu lub kontekstu połączenia pozwalające na detekcję aktywności charakterystycznej dla potencjalnego ataku**

- **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 (blokowanie, skanowanie, IPSpoofing ...)

Krzysztof Ślot © 2002

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