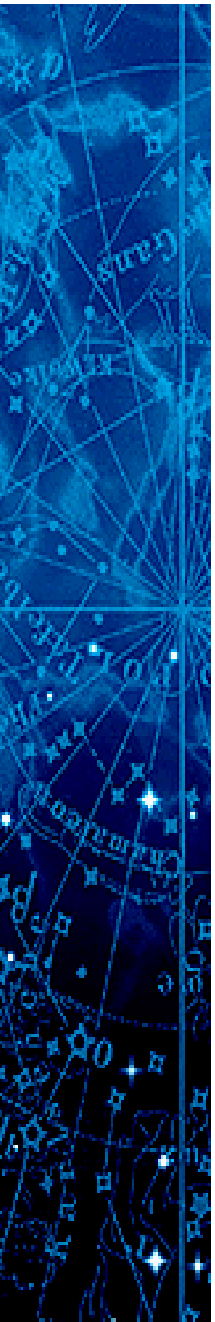


Content Security - moda czy konieczność?

"CC" - Otwarte Systemy Komputerowe
Rakowiecka 36, 02-532 Warszawa
Grzegorz.Blinowski@cc.com.pl
tel. +48 22 646-6873 fax. +48 22 606-3780

Instytut Informatyki
Politechnika Warszawska
Nowowiejska 15/19 00-665 Warszawa
gjb@ii.pw.edu.pl
tel. +48 22 660-7995

Plan wykładu

- Co to jest “Content Security”?
- Aspekt Techniczny i Biznesowy
- Przykłady rozwiązań - przegląd dostępnych produktów

Co to jest Content Security?

- Jeżeli system firewall porównamy z kontrolą paszportową to oprogramowanie Content Security spełnia rolę kontroli celnej
- Firewall - analizuje i ocenia poprawność oraz zgodność z regułami wchodzącego i wychodzącego ruchu sieciowego
- Oprogramowanie CS - bada **zawartość** przesyłanej informacji

Content Security - aspekt Techniczny

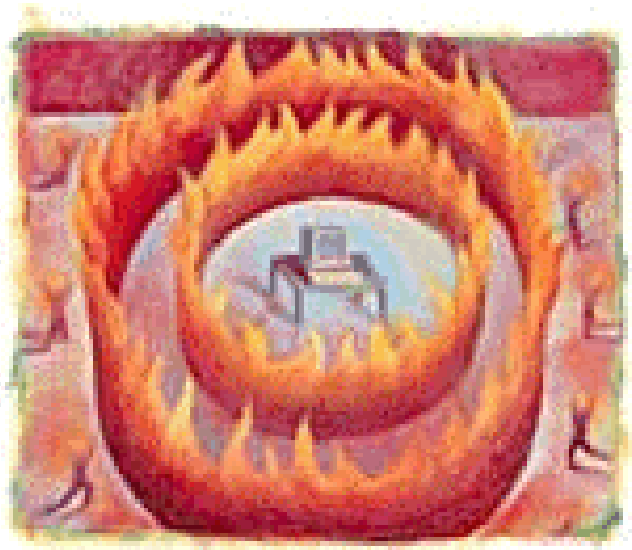
- Ryzyko związane z:
  - zainfekowaniem sieci firmowej wirusami
  - wprowadzeniem tzw. “koni trojańskich”
  - atakami DoS przeprowadzonymi przy pomocy kodu Java/JavaScript/ActiveX zawartego w przesyłkach e-mail/stronach WWW
  - Spamem, atakami DoS
  - przeciążaniem sieci (np. syndromy “kartek świątecznych” i MP3)

Content Security - aspekt biznesowy

- “Integralność biznesowa” (vs. “integralność systemów”):
  - wyciek informacji poufnych
  - ochrona przed odpowiedzialnością prawną (np. kwestia rozpowszechniania pornografii!)
  - ochrona przed spam-em i pokrewnymi nadużyciami
  - kwestie związane z wydajnością pracy

Firewall - "ściana ognia"

- Firewall = sprzęt + oprogramowanie + polityka bezpieczeństwa
- Kontrola dostępu
- Pełen audyt - logowanie
  - autoryzacja
  - szyfrowanie
  - cache
  - zarządzanie adresami

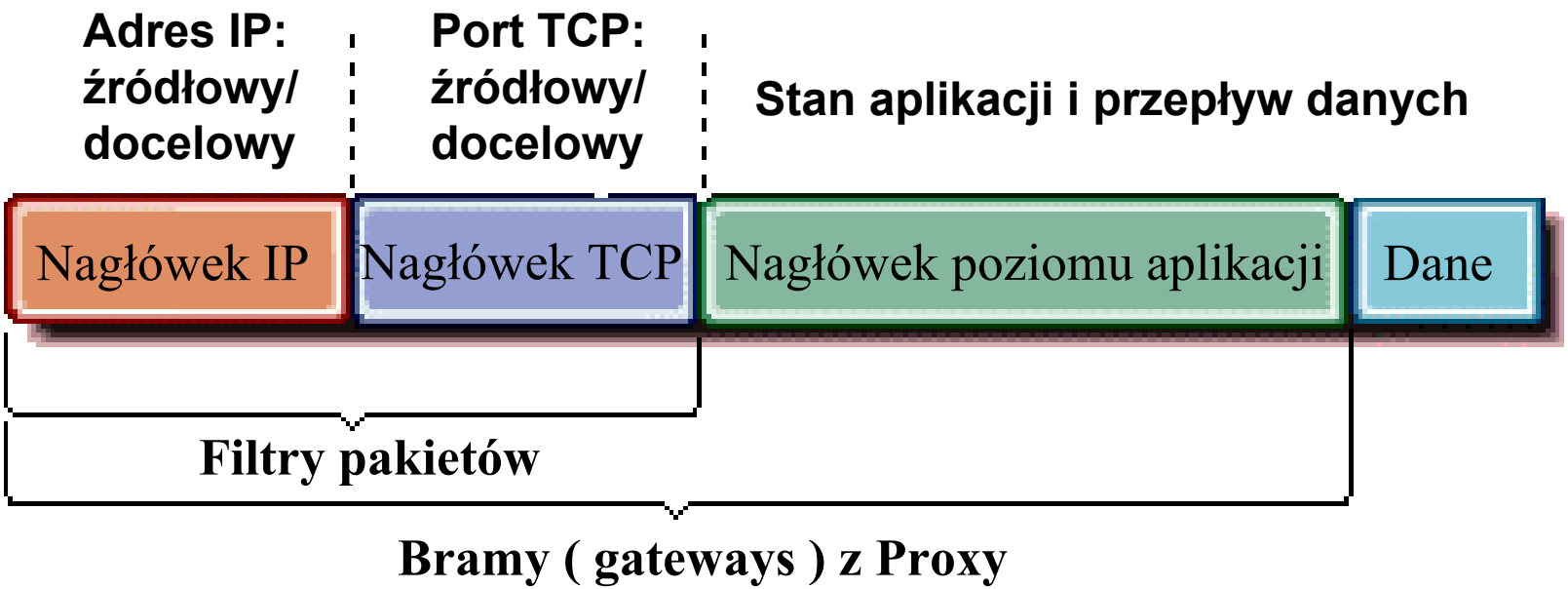


Rodzaje systemów Firewall

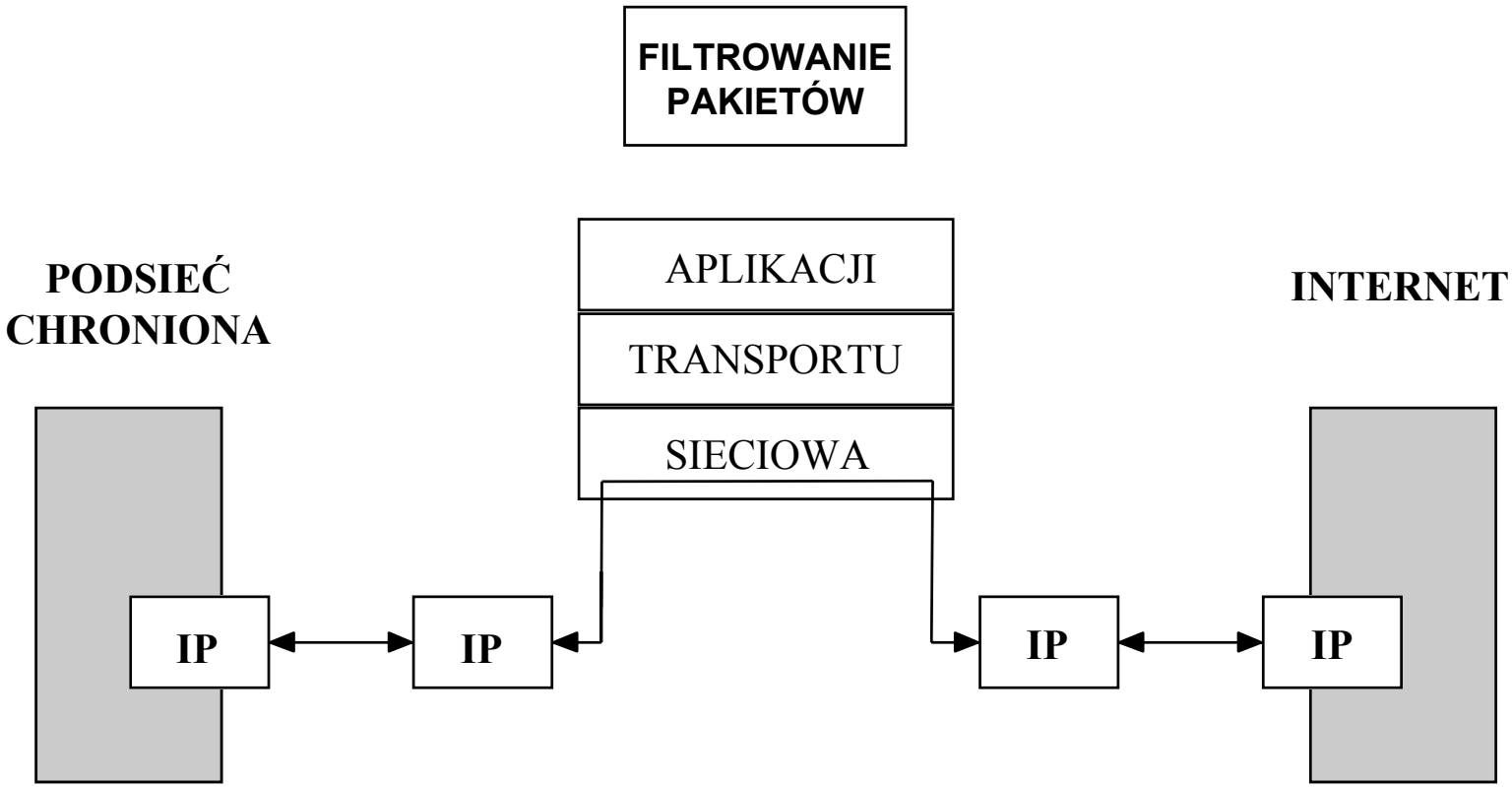
- Model OSI - w którym miejscu jakie informacje ?

- Filtrowanie pakietów (packet filtering)
- Analiza stanu połączeń (circuit level firewall)
- Proxy (application level firewall)

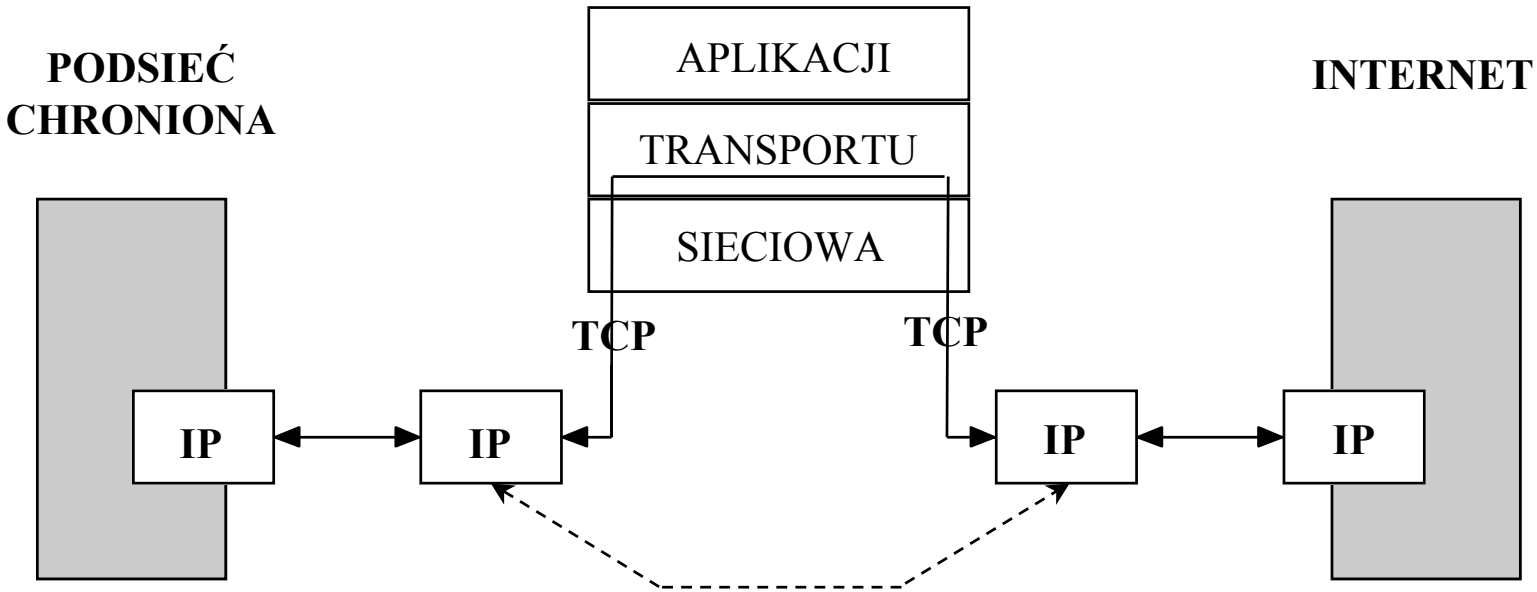
Model OSI - w którym miejscu jakie informacje ?



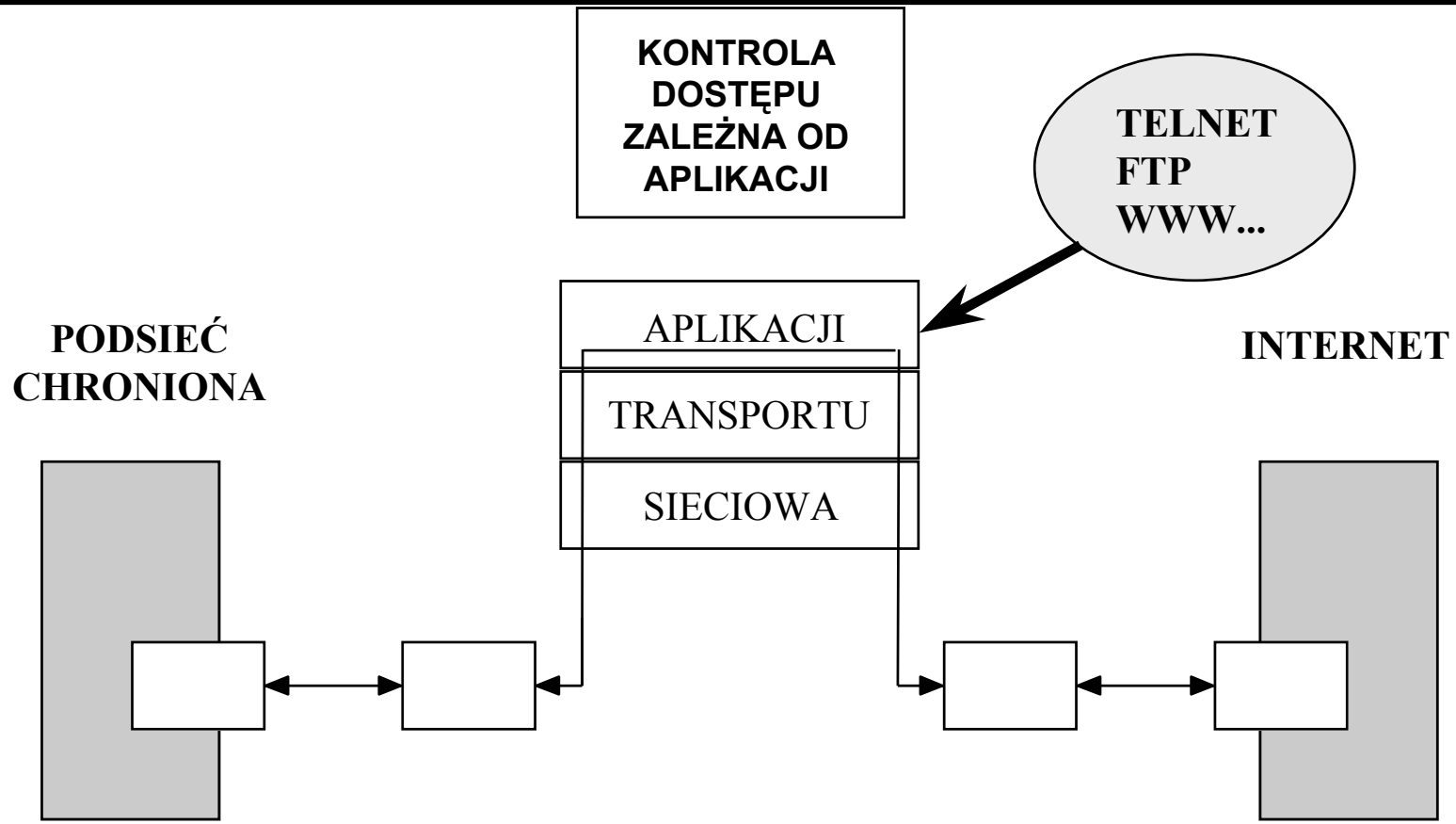
Filtrowanie pakietów (packet filtering)



Analiza stanu połączeń (circuit level firewall)

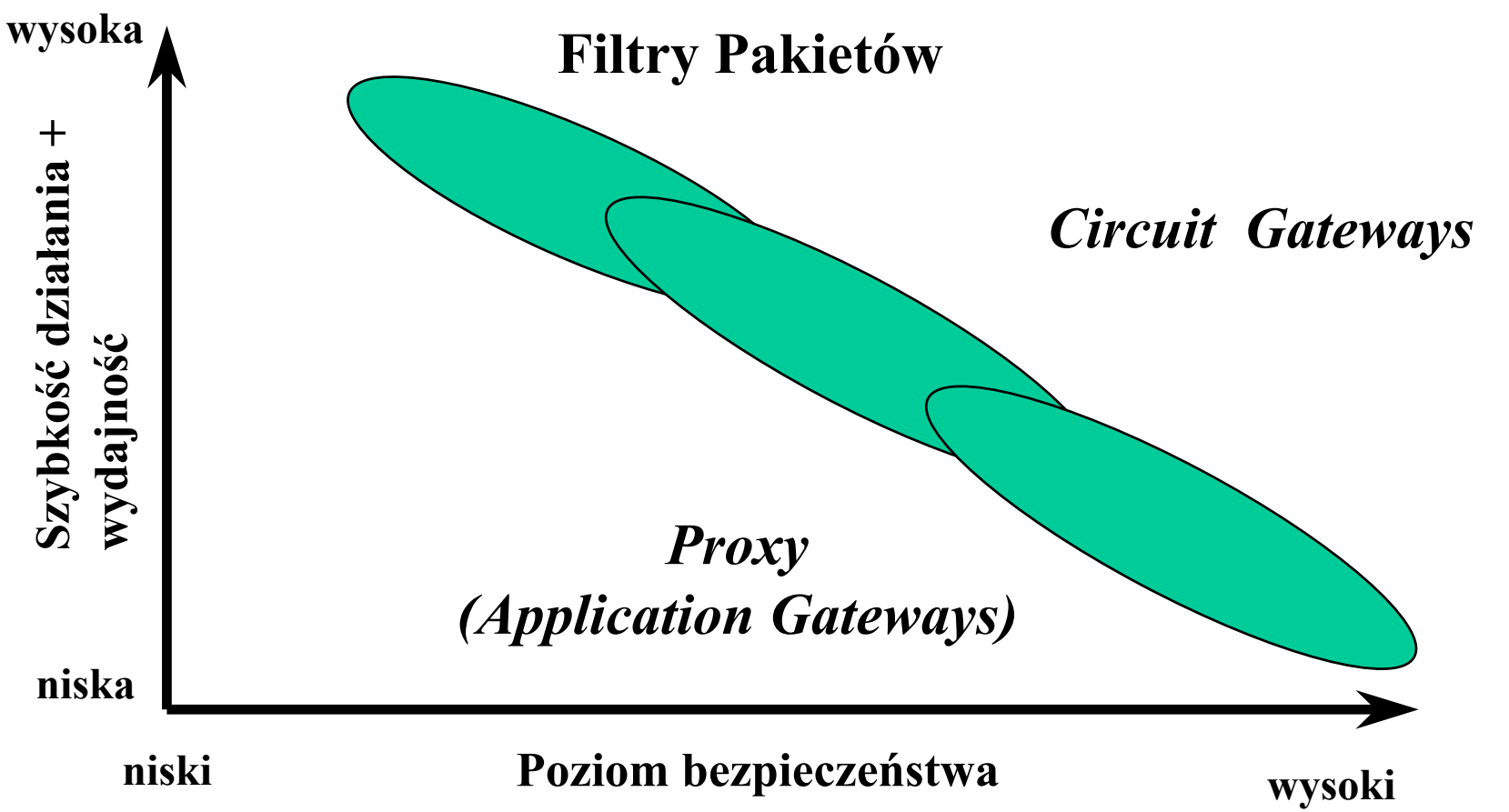


Proxy (application level firewall, application gateway)



Bezpieczeństwo na poziomie zawartości można realizować tylko w systemach typu “proxy”!

Packet Filters & Gateways



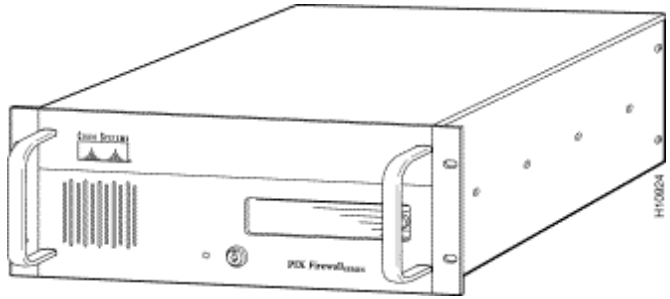
Przegląd rodzin produktów

- Skanery wirusowe, zintegrowane z systemem firewall lub z serwerem poczty
- Skanery treści zintegrowane z systemem firewall lub z serwerem poczty
- Autonomiczne skanery uniwersalne

Przegląd produktów

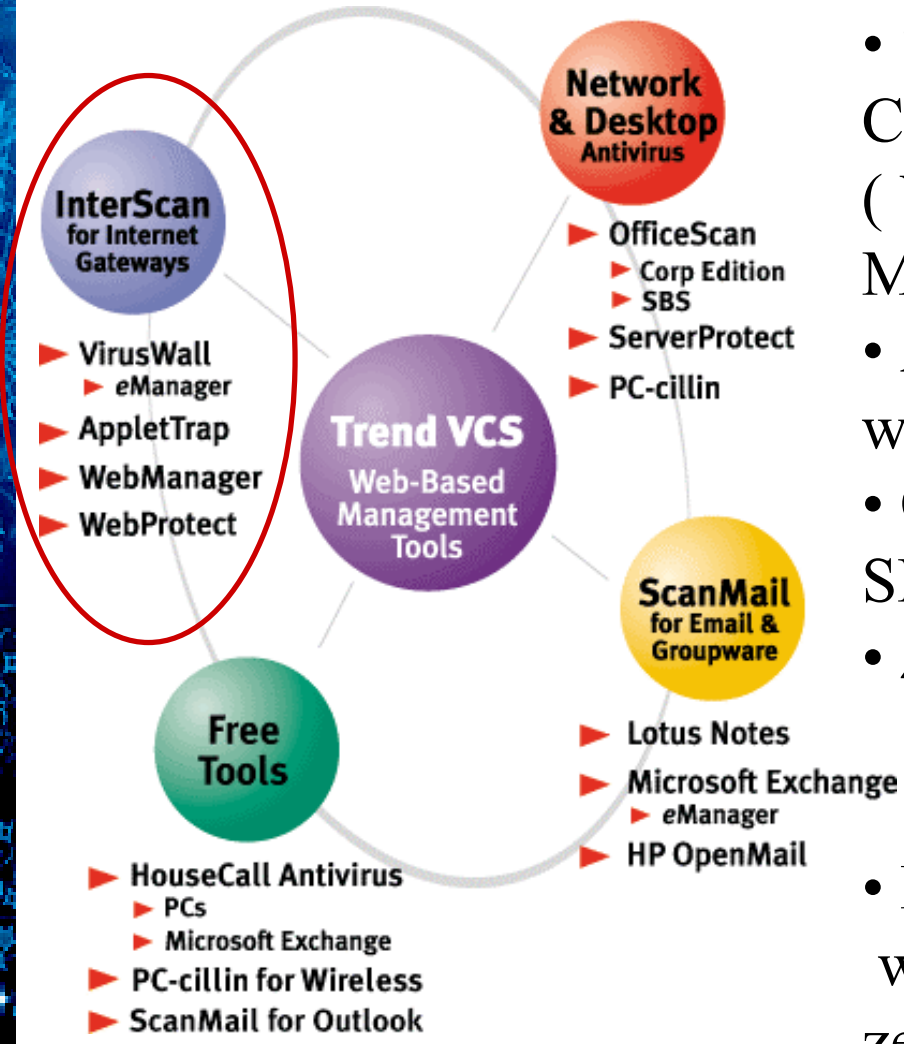
- CISCO PIX i inne rozwiązania sprzętowe
- Ochrona danych na przykładzie systemów firewall CheckPoint Firewall-1 i Axent Raptor 6.5
- Rozwiązania kompleksowe:
  - surfCONTROL - JSB technologies
  - Esafe - Alladin
  - MIMEsweeper - Baltimore (d. Content Technologies)

Rozwiązania “hardwarowe” na przykładzie CISCO PIX



- Firewall sprzętowy posiadający pewne cechy proxy aplikacyjnego
- Filtrowanie adresów (URL) w protokole http (WWW)
- Blokowanie appletów Java
- proxy SMTP (Mail Guard)

Skanowanie antywirusowe na przykładzie TrendMicro InterScan VirusWall



- Skaner wirusowy zgodny z CheckPoint OPSEC (Współpracuje też z Lucent Managed Firewall)
- Automatyczne uaktualnianie wzorców wirusów
- Obsługuje WWW, FTP, SMTP (e-mail)
- Zarządzanie przez konsolę GUI lub przeglądarkę WWW

- Przy współpracy z fw-1 wystarczy dodać InterScan do zestawu std. reguł firewall-a

Filtrowanie adresów na poziomie aplikacji

- Filtrowanie adresów URL poprzez porównanie z bazą adresów “zakazanych”
- CheckPoint Firewall-1 (poprzez rozszerzenia OPSEC), Axent Raptor poprzez WebNot/NewsNOT (SurfControl)
- Następuje porównanie żądanego adresu z wbudowaną (sieciową) bazą danych oraz jego akceptacja lub odrzucenie
- **Nie** następuje faktyczna analiza zawartości strony
- Zalety - szybkość, wady - powierzchowność

Filtrowanie adresów na poziomie aplikacji - JSB SurfControl

- Podstawą rodziny aplikacji jest tzw. engine klasyfikujący URL-e
- Kategorie (39), m.in: "Adult/Sexually Explicit, Advertisements, Arts & Entertainment, Chat, Computing & Internet, Criminal Skill, Drugs, Alcohol & Tobacco, Finance & Investment, Food & Drink, Gambling, Games, Hacking, Hate Speech, Health & Medicine, Hobbies & Recreation, Motor Vehicles, Personals and Dating, Photo Searches, Religion, Shopping, Sports, Weapons, …"
- Arts & Entertainment: Television, movies, music and video programming guides, Comics, jokes, movie, video or sound clips

Alladin ESafe

- Zgodny z firewall-1 / OPSEC (od niedawna także wersja autonomiczna)
- Analiza połączeń http, ftp w czasie rzeczywistym
- przezroczyste proxy SMTP
- Wykrywanie wrogich appletów Java, programów ActiveX, VisualBasic
- Obsługa formatów skompresowanych
- Anty-spam, anty-spoof, anty-mail-bomb poprzez reguły obejmujące adresy domenowe i pola adresowe nagłówka
- Obszary kwarantanny

Alladin ESafe

- Zgodny z surfCONTROL (analiza adresów URL)
- Skanowanie antywirusowe (wykrywa także wirusy polimorficzne oraz wirusy "stealth")
- Ochrona przed makro-wirusami
- Obsługa "cookies"
- Logowanie i alarmy

content technologies

BALTIMORE

MIMEsweeper

MIMEsweeper

- Rodzina produktów stanowiąca uzupełnienie dla firewall-i oraz serwerów e-mail
- Oprogramowanie autonomiczne tj. nie współpracujące bezpośrednio z firewallem, jak i związane z firewall-em lub serwerem pocztowym
  - **MAILsweeper** - poczta elektroniczna (także wersje dla Lotus Domino i Exchange)
  - **PORNsweeper**, **SECRETsweeper**, **Archivist** - dodatkowe moduły MAILsweepera
  - **WEBsweeper** - filtr zawartości WWW

MIMEsweeper

MAILsweeper

- Pracuje jako SMTP proxy (dwukierunkowe)
- Tzw. “scenariusze” określają reguły filtracji i akcje dla poszczególnych użytkowników i ich grup
- Różne reakcje i metody kwarantanny
- Skanowanie wirusowe, analiza kontekstowa treści, reguły związane z nagłówkiem SMTP, analiza typów załączników
- Dodatkowe funkcje, m.in. doklejanie standardowej stopki

MAILsweeper

- Ochrona przez niechcianymi przesyłkami (spam-em):
  - blokowanie i usuwanie przesyłek na podstawie analizy pól nagłówka przesyłki
- Usuwanie załączonych plików o niedozwolonych typach:
  - rozpoznawanie typów załączników
  - blokowanie (usuwanie) określonych typów załączników

MAILsweeper

- Reakcja na inne nadużycia, takie jak: przekroczenie dozwolonego rozmiaru przesyłki, wystąpienie słów kluczowych, itd.:
  - Wykrywanie słów kluczowych i fraz w treści przesyłki
  - Różnicowanie reguł filtracji w zależności od nadawcy i odbiorcy
  - "kwarantanna" dla podejrzanych przesyłek
  - archiwizacja przesyłek
  - funkcje alertu, raportowania i audytu

MIMEsweeper

- Współpracuje z następujacymi skanerami wirusów: Symantec, Dr.Solomon's Anti-Virus Toolkit, McAfee VirusScan, Sophos Anti-Virus, F-Prot, Thunderbyte Anti-Virus, VET Anti-Virus, Leprechaun Cyberbuster, Norman Virus Control
- Rozpoznaje następujące typy dokumentów: CDA (.doc, .xls, .ppt, etc.) PDF, text; i plików: - JPEG, BMP, GIF, TIF, AVI, MPEG, WAV i inne
- Rozpoznaje archiwa: BINHEX, CMP, GZIP, LZH, MIME, TAR, TNEF, UUE (wiele wariantów), ZIP

MIMEsweeper

PORNsweeper

- PORNsweeper - moduł MAILsweeper-a służący do wykrywania i usuwania treści pornograficznych z przesyłek e-mail.
- Akcje podejmowane w przypadku wykrycia próby przesłania treści pornograficznych - usunięcie, alarm, notyfikacja, itd.
- Definiowanie parametrów akceptowanej i nieakceptowanej grafiki - rozmiary plików, wielkość obrazka w pikselach, typ pliku, itd.
- Definiowanie "poziomu pewności" algorytmu rozpoznawania obrazów
- Różnicowanie reguł w zależności od typów przesyłanych plików
- Różnicowanie reguł w zależności od odbiorcy, na poziomie grup użytkowników oraz indywidualnych osób

Archivist i inne moduły

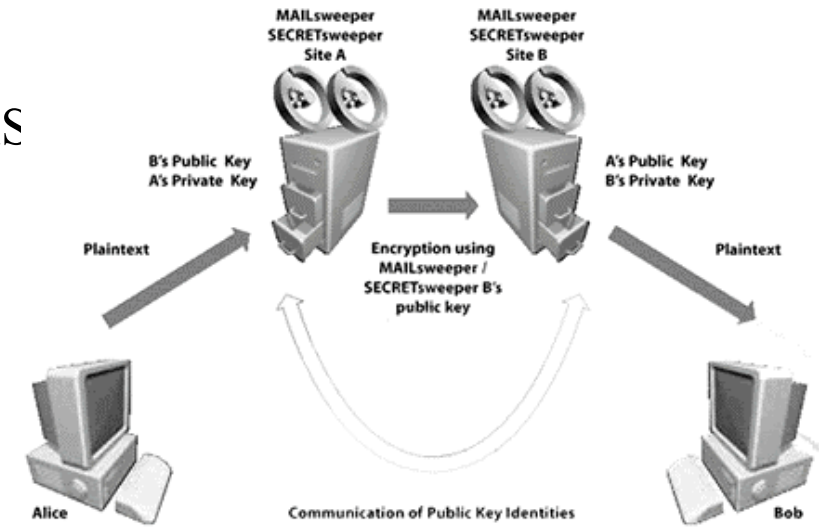
MIMEsweeper

- Zcentralizowana archiwizacja przesyłek e-mail prowadzona z serwera
- Pełna archiwizacja (nagłówek, załączniki)
- Archiwizacja sterowana poprzez zbiór reguł
- Zdalna archiwizacja
- Automatyczne indeksowanie i wyszukiwanie w archiwum
- Interfejs HTML oraz MMC (MS Management Console)
- współpraca z systemami HSM

Archivist i inne moduły

MIMEsweeper

- **SECRETsweeper** - realizuje "VPN" pomiędzy serwerami e-mail:
  - kodowanie S/MIME (DES, 3DES, RC2)
  - obsługa certyfikatów X.509, weryfikacja podpisów
  - "Zestawienie łącza"
- **E-sweeper**
  - zintegrowany pakiet dla ISP/AS
  - obsługa wielu domen/MX-ów
  - billing
  - rozproszona architektura



MIMEsweeper

WEBsweeper

- Identyfikacja i usuwanie wirusów z sesji WWW (http) oraz FTP:
  - Współpracuje z szerokim wachlarzem popularnych skanerów anty-wirusowych
  - Usuwa wirusy z plików
  - Integracja z oprogramowaniem firm trzecich blokującym adresy URL
  - Skanowanie na podstawie słów kluczowych.
  - Wykrywanie i blokowanie appletów Java, komponentów ActiveX oraz ukrytych formularzy
  - Usuwanie nielegalnych typów danych, np.: audio, wideo, cookies, itd.

MIMEsweeper

WEBsweeper

- Mechanizm "browser comforting" polegający na utrzymywaniu sesji z przeglądarką użytkownika oraz informowaniu go o procesie skanowania - istotne w przypadku analizy b. obszernych stron WWW.
- Obsługa protokołu http 1.1, obsługa protokołu https
- Rozbudowane logowanie i raportowanie
- Zróżnicowanie polityki bezpieczeństwa wg: użytkowników i grup, a także wg. czasu
- Uwierzytelnianie użytkowników
- Wybiórcze traktowanie ActiveX, Java, JavaScript, itd. (blokowanie lub usuwanie)
- Analiza kontekstowa zawartości (w jęz angielskim)