“Content Security” - rodzina produktów MIMEsweeper

"CC" - Otwarte Systemy Komputerowe

http://www.cc.com.pl/

Rakowiecka 36, 02-532 Warszawa

Grzegorz.Blinowski@cc.com.pl

tel. +48 22 646-6873 fax. +48 22 606-3780

Baltimore | MIMEsweeper™

Open Compu

Plan wystapienia

- Co to jest Content Security?
- CS a systemy firewall
- Przeglad komercyjnych systemów CS
- Rodzina produktów **MIMEsweeper** firmy Baltimore

Co to jest “Content Security”?

- Jezeli system firewall porównamy z kontrola paszportowa to oprogramowanie Content Security spelnia role kontroli celnej
- **Firewall -** analizuje i ocenia poprawnosc oraz zgodnosc z regulami wchodzacego i wychodzacego ruchu sieciowego
- Oprogramowanie **Content Security -** bada **zawartosc** przesylanej informacji

Cele stosowania Content Security - aspekt techniczny

- Ryzyko zwiazane z:
  - zainfekowaniem sieci firmowej wirusami
  - wprowadzeniem tzw. “koni trojanskich”
  - atakami DoS przeprowadzonymi przy pomocy kodu Java/JavaScript/ActiveX zawartego w przesylkach e-mail/stronach WWW
  - spamem, atakami DoS
  - przeciazaniem sieci (np. syndromy “kartek swiatecznych” i MP3)

Cele stosowania Content Security - aspekt biznesowy

- “Integralnosc biznesowa” (vs. “integralnosc systemów”):
  - wyciek informacji poufnych
  - ochrona przed odpowiedzialnoscia prawna (np. kwestia rozpowszechniania pornografii!)
  - ochrona przed spam-em i pokrewnymi naduzyciami
  - kwestie zwiazane z wydajnoscia pracy

Firewall - "sciana ognia"

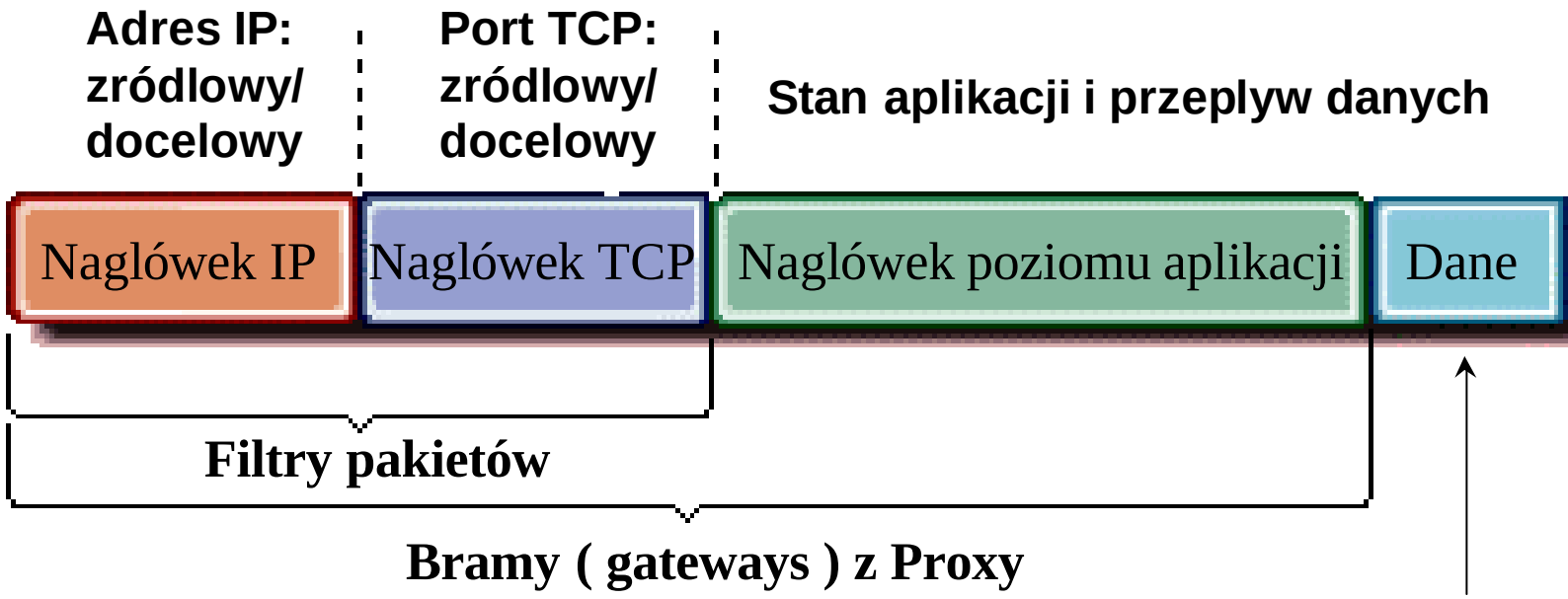
- Firewall = sprzet + oprogramowanie + polityka bezpieczenstwa
- Kontrola dostepu
- Pelen audyt - logowanie
- autoryzacja
- szyfrowanie
- cache
- zarzadzanie adresami

Rodzaje systemów Firewall

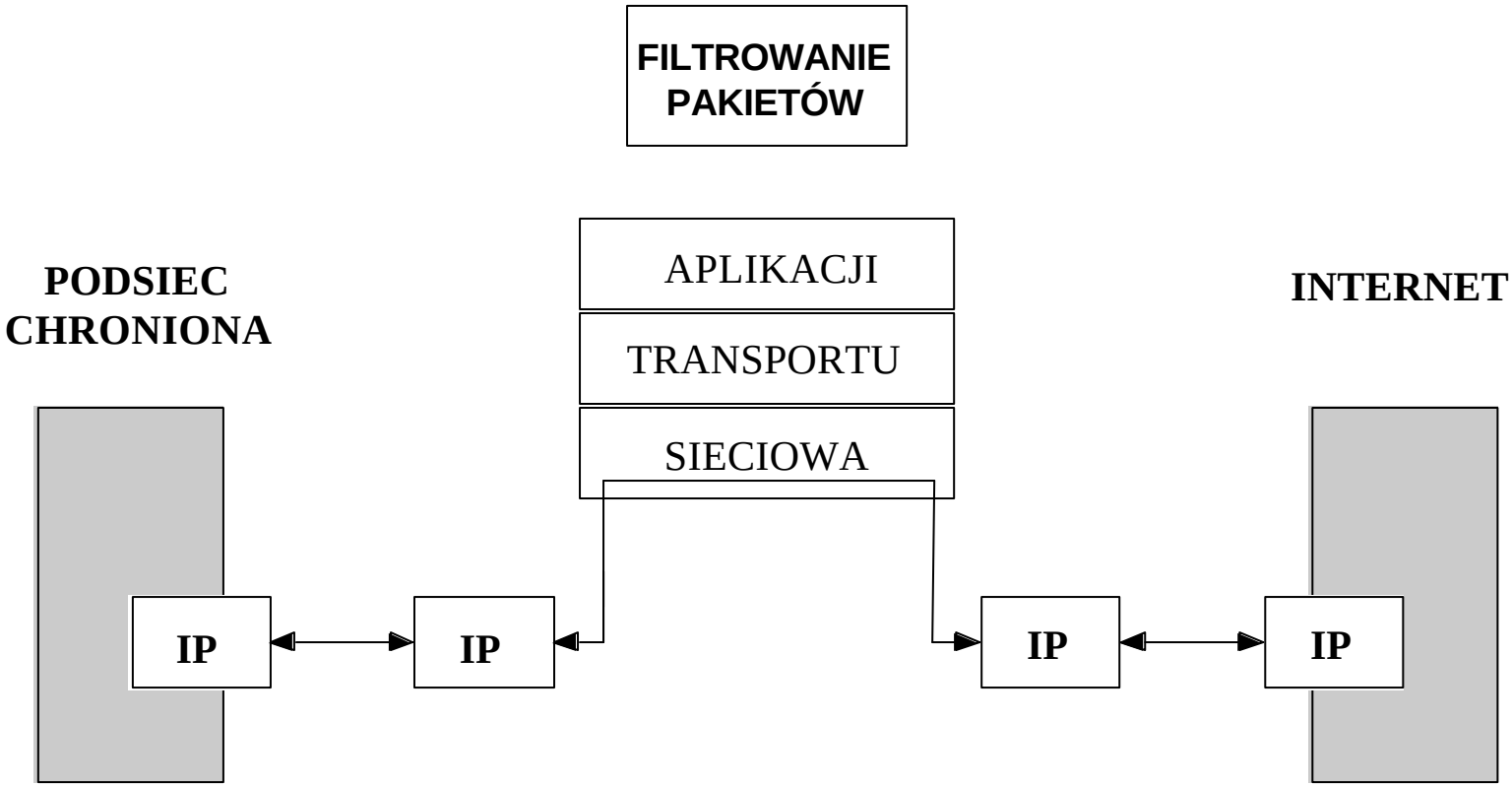
- Model OSI - w którym miejscu jakie informacje ?

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

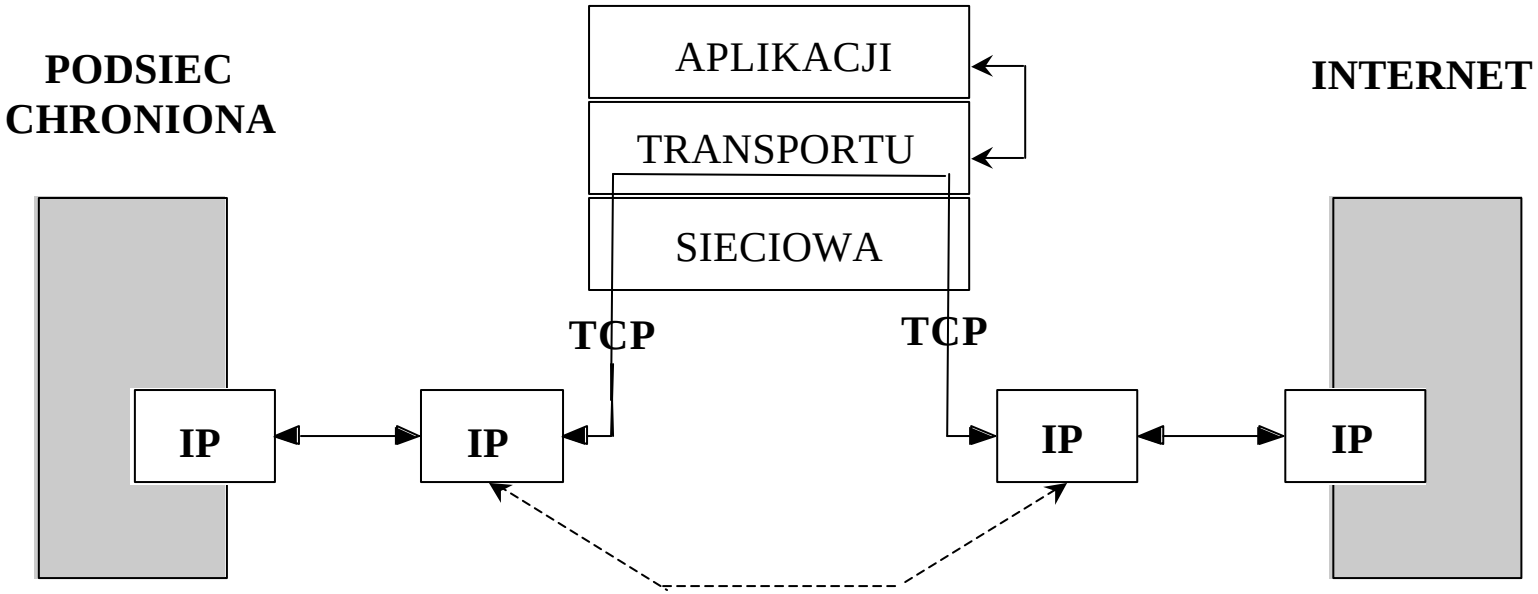
Model OSI - w którym miejscu jakie informacje



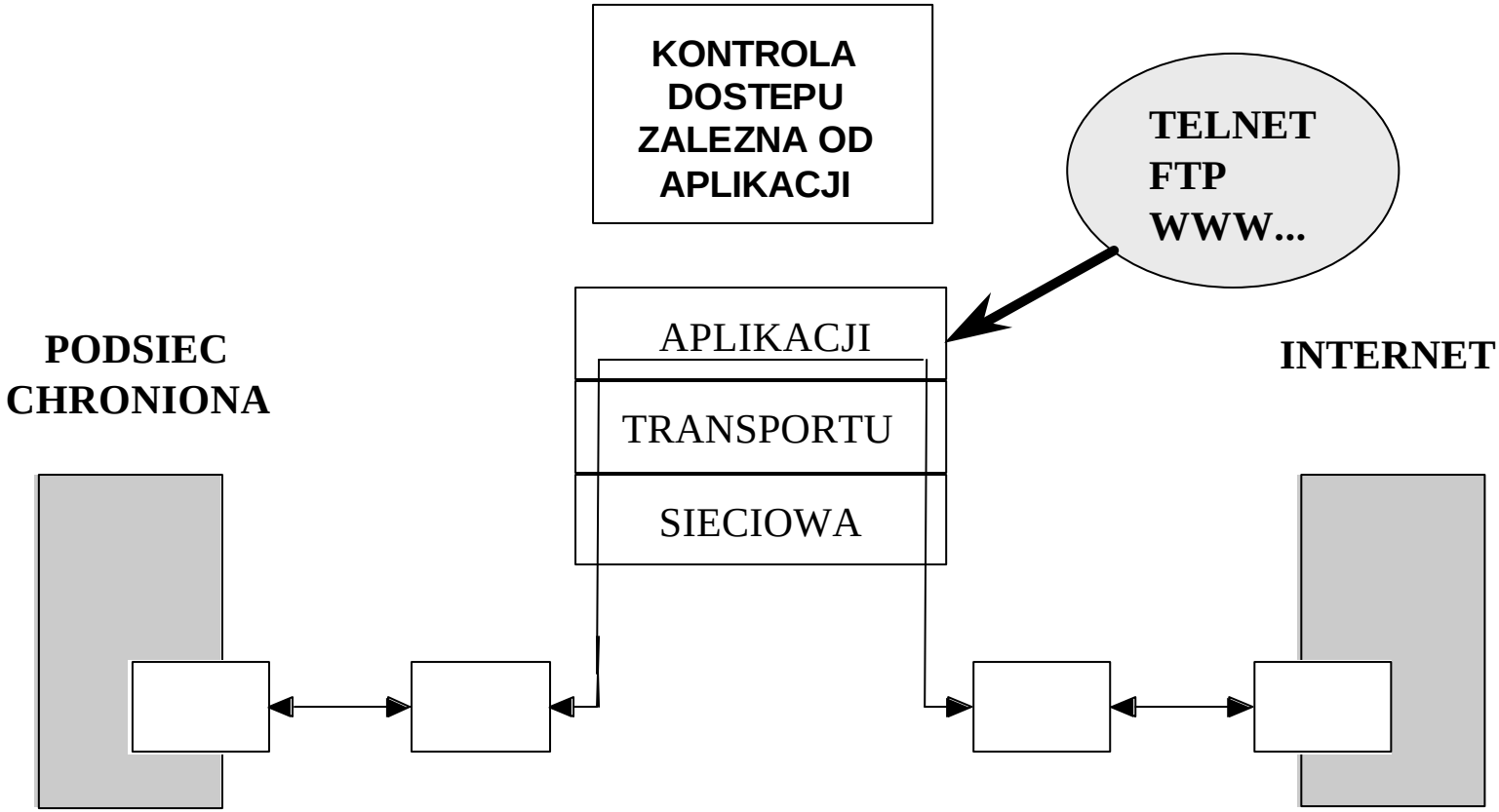
Filtrowanie pakietów (packet filtering)



Analiza stanu polaczen (circuit level firewall)



Proxy (application level firewall, application gateway)



Bezpieczenstwo na poziomie zawartosci mozna realizowac tylko w systemach typu “proxy”!

Filtrowanie adresów na poziomie aplikacji

- Filtrowanie adresów URL poprzez porównanie z baza adresów “zakazanych”
- **CheckPoint Firewall-1** (OPSEC), **Axent Raptor** WebNot/NewsNOT (SurfControl), CISCO PIX poprzez prod. firm trzecich (n.p. WebSense)
- Nastepuje porównanie zadanego adresu z wbudowana (sieciowa) baza danych oraz jego akceptacja lub odrzucenie
- **Nie** nastepuje faktyczna analiza zawartosci strony
- **Zalety -** szybkosc, **wady -** powierzchownosc

Filtrowanie adresów na poziomie aplikacji - SurfControl

- Podstawa rodziny aplikacji jest tzw. “engine” klasyfikujacy 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, sound clips*

Baltimore | MIMEsweeper™
policy-based content security

- MAILsweeper for SMTP
- MAILsweeper for Microsoft Exchange
- MAILsweeper for Lotus Domino R5
- WEBsweeper
- PORNsweeper

content technologies

BALTIMORE

Baltimore | MIMEsweeper™
policy-based content security

- MIMEsweeper - 10 mln. licencji, 10 tys. klientów
- MIMEsweeper rozwijany byl przez ContentTechnologies od 1995 r.
- Pazdziernik 2000 - Przejecie **Content Technologies** przez **Baltimore**

MIMEsweeper

MIMEsweeper

- Rodzina produktów stanowiaca uzupelnienie dla firewall-i oraz serwerów e-mail
- Oprogramowanie autonomiczne tj. nie wspólpracujace bezposrednio z firewallem:
  - **MAILsweeper -** poczta elektroniczna (takze wersje dla Lotus Domino i Exchange)
  - **WEBsweeper -** filtr zawartosci WWW
  - **PORNsweeper**, **SECRETsweeper -** dodatkowe moduly MAILsweepera

MAILsweeper

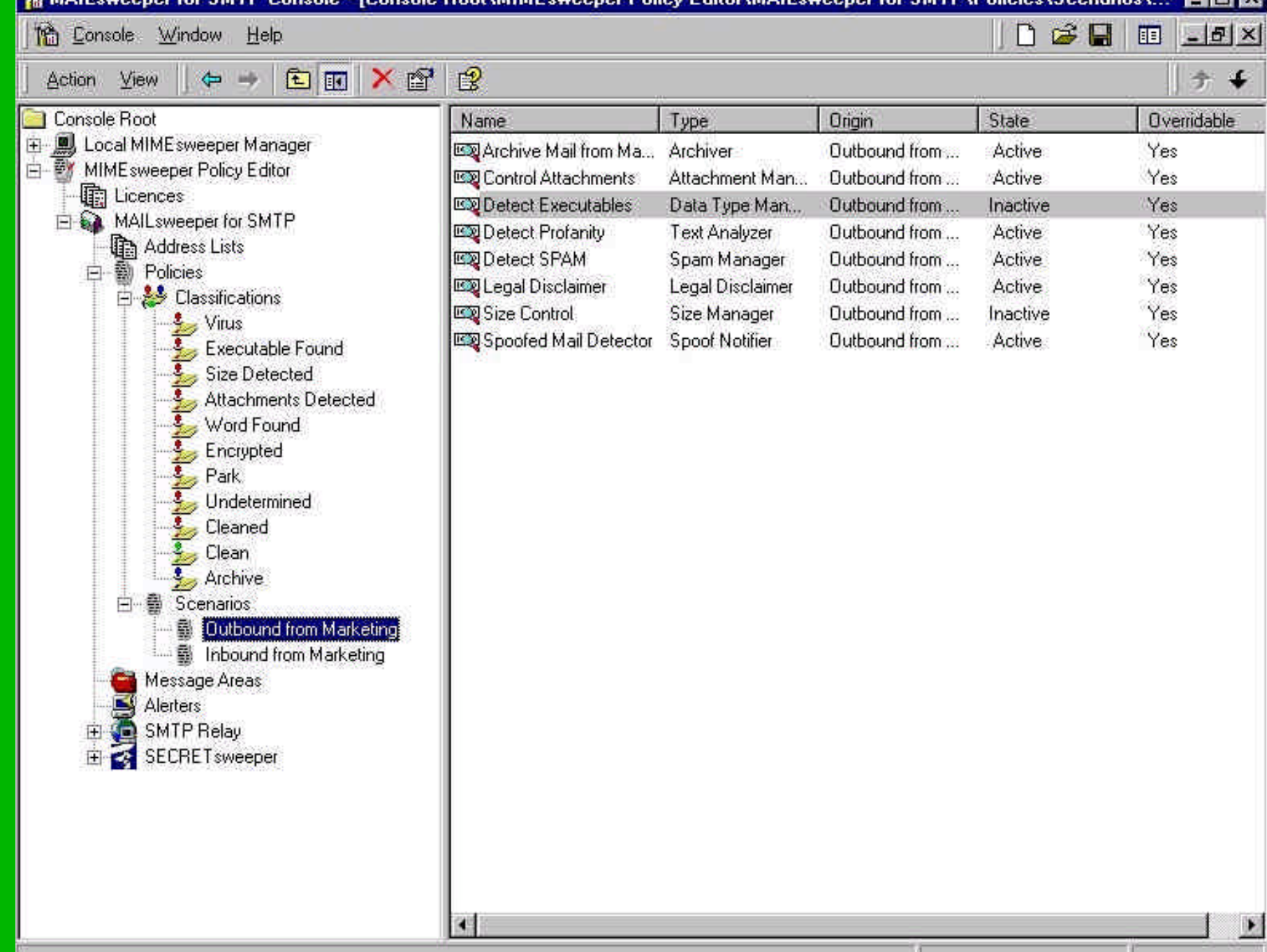
- Pracuje jako dwukierunkowe proxy SMTP
- Tzw. “scenariusze” okreslaja reguly filtracji i akcje dla poszczególnych uzytkowników i ich grup
- Klasyfikacja wiadomosci - skanowanie wirusowe, analiza kontekstowa tresci, reguly zwiazane z naglówkiem SMTP, analiza typów zalaczników
- Rózne reakcje i metody kwarantanny
- Dodatkowe funkcje, m.in. doklejanie standardowej stopki

MAILsweeper

- Ochrona przez niechcianymi przesylkami (spam-em):
  - blokowanie i usuwanie przesylek na podstawie analizy pól naglówka przesylki
- Usuwanie zalaczonych plików o niedozwolonych typach:
  - rozpoznawanie typów zalaczników
  - blokowanie (usuwanie) okreslonych typów zalaczników
  - usuwanie wszystkich zalaczników (attachment stripping)

MAILsweeper

- Reakcja na inne naduzycia, takie jak: przekroczenie dozwolonego rozmiaru przesylki, wystapienie słów kluczowych, itd.:
  - Wykrywanie słów kluczowych i fraz w tresci przesylki
  - Róznicowanie regul filtracji w zaleznosci od nadawcy i odbiorcy
  - "kwarantanna" dla podejrzanych przesylek
  - archiwizacja przesylek
  - funkcje alertu, raportowania i audytu


Console Window Help
Action View
Console Root
Local MIMEsweeper Manager
MIMEsweeper Policy Editor
Licences
MAILsweeper for SMTP
Address Lists
Policies
Classifications
Virus
Executable Found
Size Detected
Attachments Detected
Word Found
Encrypted
Park
Undetermined
Cleaned
Clean
Archive
Scenarios
Outbound from Marketing
Inbound from Marketing
Message Areas
Alerters
SMTP Relay
SECRETsweeper
Name
Type
Origin
State
Overridable
Archive Mail from Ma... Archiver Outbound from ... Active Yes
Control Attachments Attachment Man... Outbound from ... Active Yes
Detect Executables Data Type Man... Outbound from ... Inactive Yes
Detect Profanity Text Analyzer Outbound from ... Active Yes
Detect SPAM Spam Manager Outbound from ... Active Yes
Legal Disclaimer Legal Disclaimer Outbound from ... Active Yes
Size Control Size Manager Outbound from ... Inactive Yes
Spoofed Mail Detector Spoof Notifier Outbound from ... Active Yes

MIMEsweeper

- Współpracuje z nastepujacymi 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 nastepujace 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

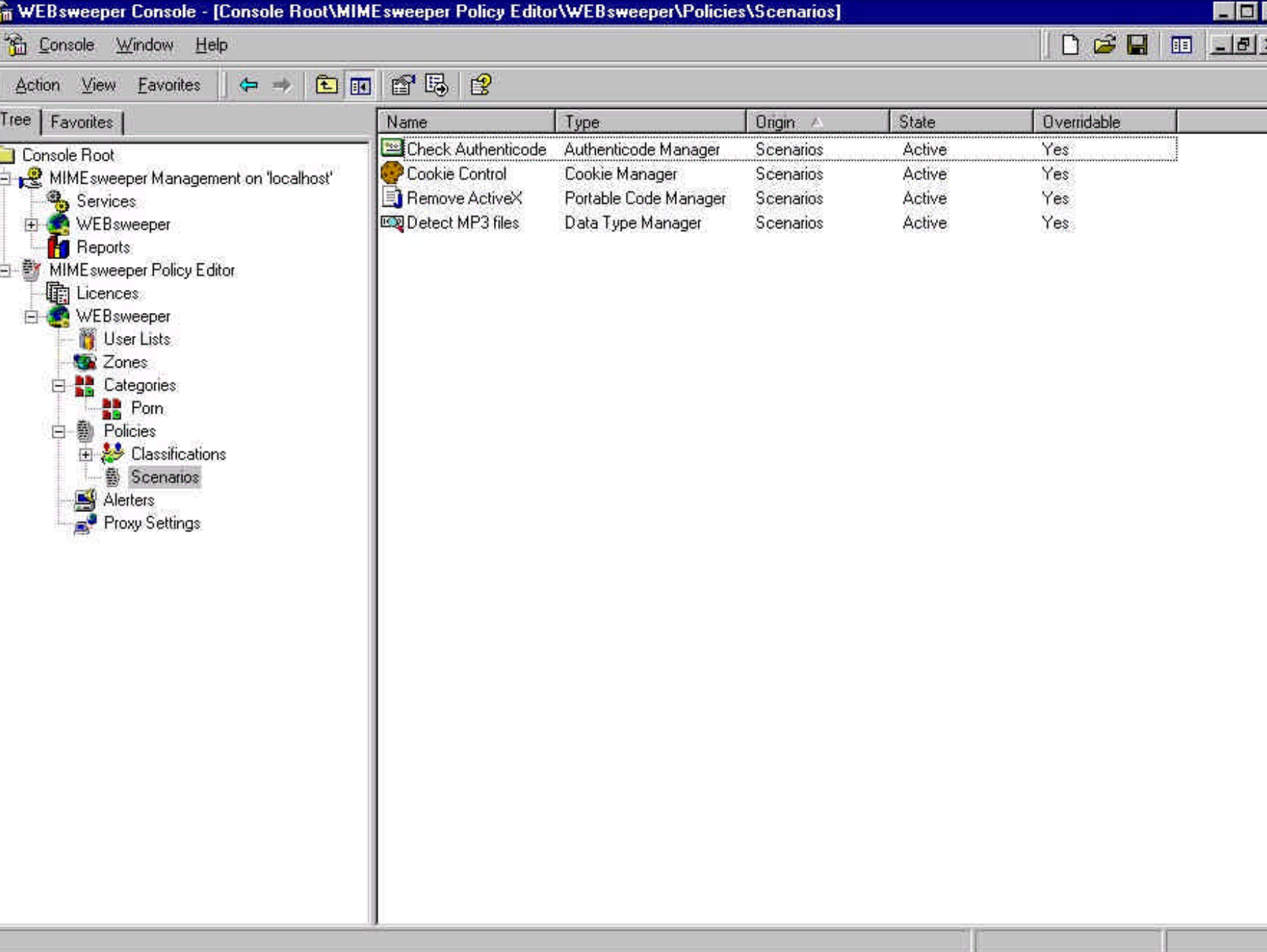
WEBsweeper

- Identyfikacja i usuwanie wirusów z sesji WWW (http) oraz FTP:
  - Wspólpracuje z szerokim wachlarzem popularnych skanerów anty-wirusowych
  - Usuwa wirusy z plików
  - Integruje sie z oprogramowaniem firm trzecich blokujacym adresy URL
  - Skanuje tresc na podstawie słów kluczowych.
  - Wykrywa i blokuje applety Java, komponenty ActiveX oraz ukryte formularze
  - Usuwa nielegalne typy danych, np.: audio, video, cookies, itd.

MIMEsweeper

WEBsweeper

- Obsluga protokolów http 1.1 i https
- Rozbudowane logowanie i raportowanie
- Zróznicowanie polityki bezpieczenstwa wg: uzytkowników i grup, czasu
- Uwierzytelnianie uzytkowników
- Wybiórcze traktowanie ActiveX, Java, JavaScript, itd.
- Analiza kontekstowa zawartosci (w jez angielskim)
- Cache WWW
- Mechanizm "browser comforting" - utrzymywanie sesji z przegladarka uzytkownika i informowanie go o procesie skanowania.
- Praca w klastrach (równowazenie obciazenia do 32 maszyn)


WEBsweeper Console - [Console Root\MIMEsweeper Policy Editor\WEBsweeper\Policies\Scenarios]
Console
Window
Help
Action
View
Favorites
Tree
Favorites
Console Root
MIMEsweeper Management on 'localhost'
Services
WEBsweeper
Reports
MIMEsweeper Policy Editor
Licences
WEBsweeper
User Lists
Zones
Categories
Porn
Policies
Classifications
Scenarios
Alerters
Proxy Settings
Name
Type
Origin
State
Overridable
Check Authenticode
Authenticode Manager
Scenarios
Active
Yes
Cookie Control
Cookie Manager
Scenarios
Active
Yes
Remove ActiveX
Portable Code Manager
Scenarios
Active
Yes
Detect MP3 files
Data Type Manager
Scenarios
Active
Yes

MIMEsweeper

PORNsweeper

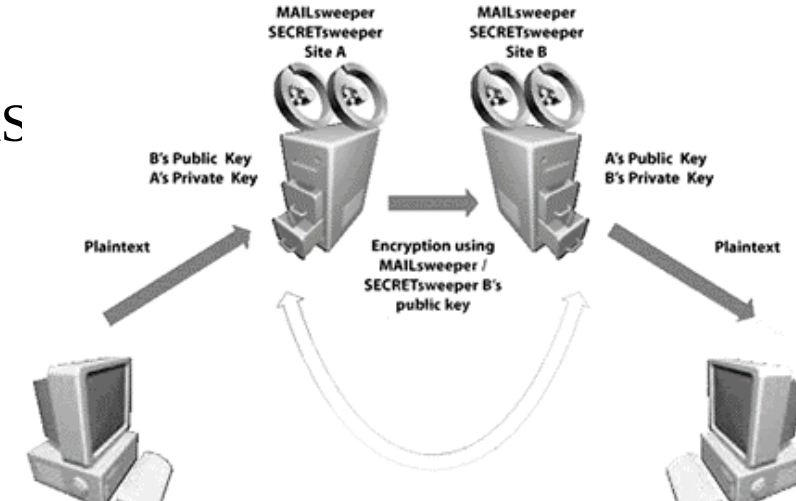
- **PORNsweeper** - modul **MAILsweeper-a** sluzacy do wykrywania i usuwania tresci pornograficznych z przesylek e-mail.
- Akcje podejmowane w przypadku wykrycia próby przeslania tresci pornograficznych - usuniecie, alarm, notyfikacja, itd.
- Definiowanie parametrów akceptowanej i nieakceptowanej grafiki - rozmiary plików, wielkosc obrazka, typ pliku, itd.
- Definiowanie "poziomu pewnosci" algorytmu rozpoznawania obrazów
- Róznicowanie regul w zaleznosci od: typów przesylanych plików, odbiorcy, na poziomie grup oraz indywidualnych osób

Inne moduly

- MAILsweeper for Domino
- MAILsweeper for Exchange
- Czesto stosowana jest kombinacja MAILsweeper for Domino/Exchange + MAILsweeper for SMTP:
  - pierwszy pakiet zapewnia bezpieczenstwo wewnetrzne
  - drugi bezpieczenstwo przy wymianie danych ze swiatem zewnetrznym

Inne moduly

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



Baltimore | MIMEsweeper™
policy-based content security

Pytania?