

Jak zrealizować system Content Security dla kilku(nastu) tysięcy użytkowników? - rozwiązania firmy Clearswift

CC Otwarte Systemy Komputerowe Sp z o.o.

<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

Co to jest CC?

- **CC Otwarte Systemy Komputerowe** działa od 1995 r. (sp. z o.o. od 2001)
- Oferujemy:
 - Rozwiązania z dziedziny bezpieczeństwa sieci komputerowych
 - Produkcja własnego, wyspecjalizowanego oprogramowania
- Afiliacje:
 - CLEARSWIFT Content Technologies „Premium Partner”
 - iPlanet „Enterprise Partner” ("Netscape Solution Expert")
 - SUN Microsystem Partner
 - inne: Vasco, Network Privacy, StoneSoft

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 **Content Security** - bada **zawartość** przesyłanej informacji

Zagrożenia

Poczta elektroniczna:

- Nadużycia - korzystanie niezgodnie z przeznaczeniem
- Wyciek poufnych informacji
- Odpowiedzialność prawna
- Spam
- Zniszczenie i uszkodzenie danych - n.p. wirusy

Zagrożenie integralności:

Sieci Biznesu



WWW:

- Pornografia, inne "nieproduktywne"
- Zniszczenie i uszkodzenie danych (Virus, Java, ActiveX)



Content Security - Wybrane zagrożenia na przykładzie Poczty Elektronicznej



CLEARSWIFT™
CORPORATION



CC
Otwarte Systemy
Komputerowe Sp. z o.o.

Złe publicity

**Gigant telekomunikacji wyrzucony za
z pracy 30...**

**porn
ich w**

**Ministerstwo Obrony
zawie...**

**Cywilna pracownica londyńskiej policji
odszkodowania
£40,000 molestowal
kolegę z pracy, Lipiec 2001**

www.theregister.co.uk,

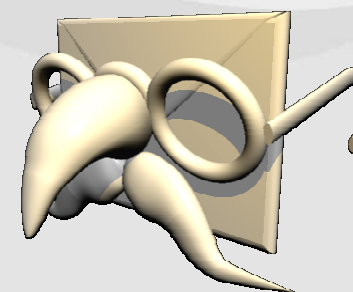
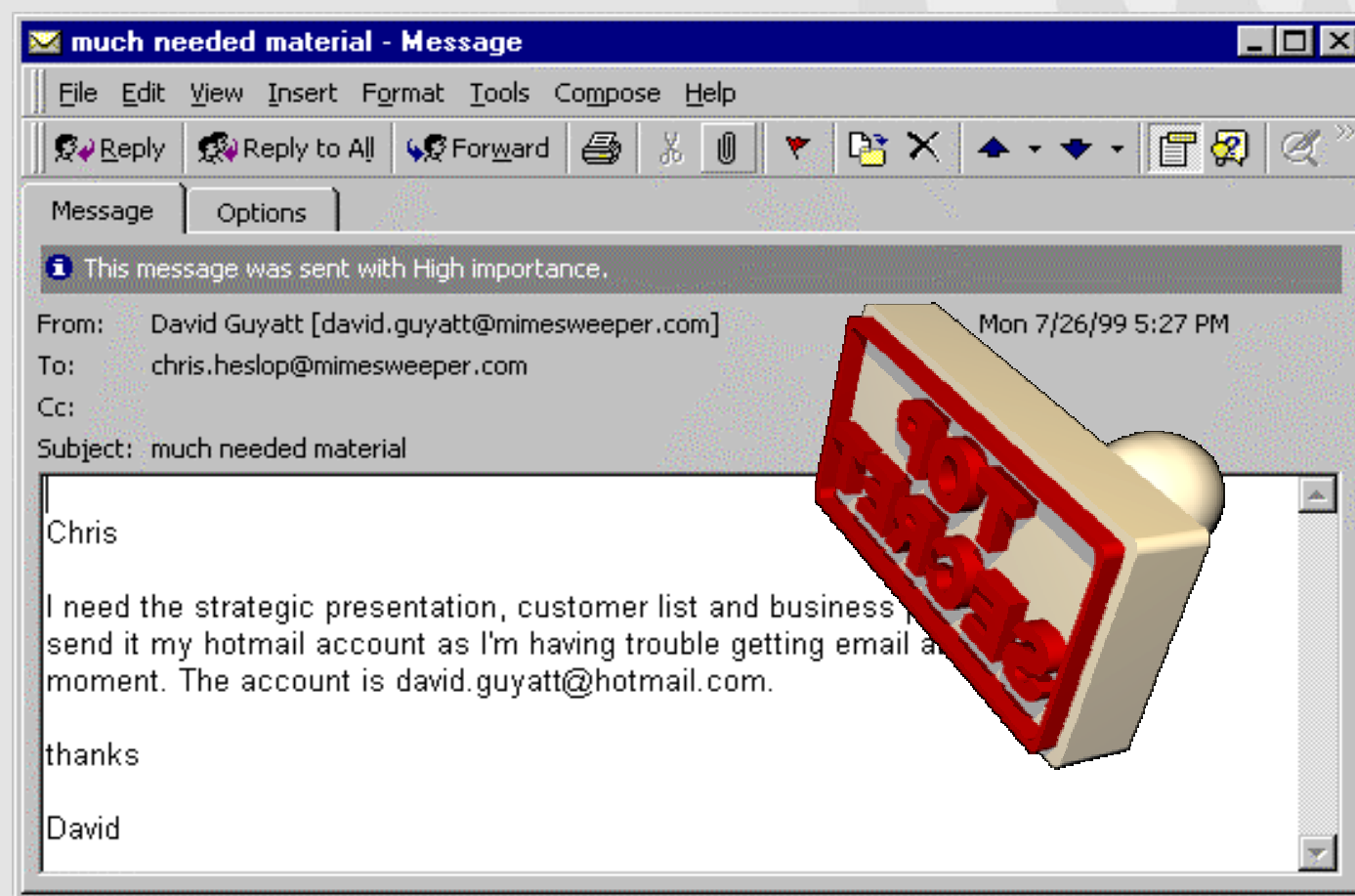
www.theregister.co.uk,

tytułu e-mailowego przez koleżankę z pracy, Sierp. 2000

Odpowiedzialność prawna

- Rozpowszechnianie kradzionego oprogramowania
- Inne naruszenia praw autorskich
- Złamanie umów o poufności
- Molestowanie na tle seksualnym, rasowym ,...
- Rozpowszechnianie treści obscenicznych
- Łamanie ustawowych wymagań dot. ochrony danych (np. osobowych)
- Rozpowszechnianie wirusów

"Spoofing"

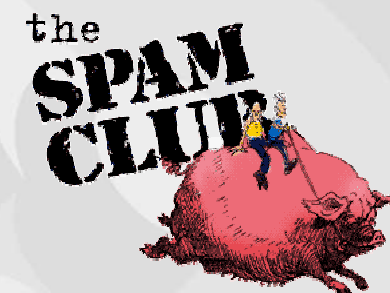


SPAM



*Newsweek
Polska
1.09.2002*

- Możemy być źródłem lub przekaźnikiem spamu nie wiedząc o tym
- Konsekwencje - złe publicity, poważne obniżenie wydajności pracy serwerów pocztowych i firewalli



SPAM - termin oryginalnie pochodzący z "Latającego Cyrku" Monty Pythona oznacza mielonkę

W odniesieniu do poczty elektr. oznacza zalew nie chcianych maili o charakterze reklamowym

<http://www.mimesweeper.pl/>

Jak się bronić?

Content Security

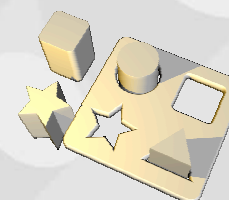
- Analiza meta-informacji
 - adresy URL
 - nagłówki protokołu http, SMTP
 - nagłówki wiadomości SMTP
 - **Zaleta: szybkie**
- Analiza informacji
 - Faktyczna analiza danych e-mail/WWW
 - **Zaleta: Dokładne**

Weryfikacja URL-i

1) Użytkownik wpisuje/klika na link, np.
<http://www.samochody.pl/>



2) System CS bada kwalifikację adresu w swojej bazie danych kategorii linków



3) Użytkownik otrzymuje żadaną stronę lub informację, że zakazano dostępu

Baza danych linków jest stale aktualizowana poprzez Internet (na zasadzie subskrypcji), odpowiednie mechanizmy kompresji zapewniają, że sklasyfikować można b. wiele (miliony) adresów.

Weryfikacja URL-i - problemy

- Nie ma żadnej ochrony przed treścią (wirusami, kodem wykonywalnym, itp.)
- Jesteśmy zawsze "o pół kroku do tyłu" w stosunku do twórców nowych serwisów
- Klasyfikacja może być niedokładna

198.179.242.131:

www.goga.pl
laski.goga.pl
sex.goga.pl
xxx.goga.pl

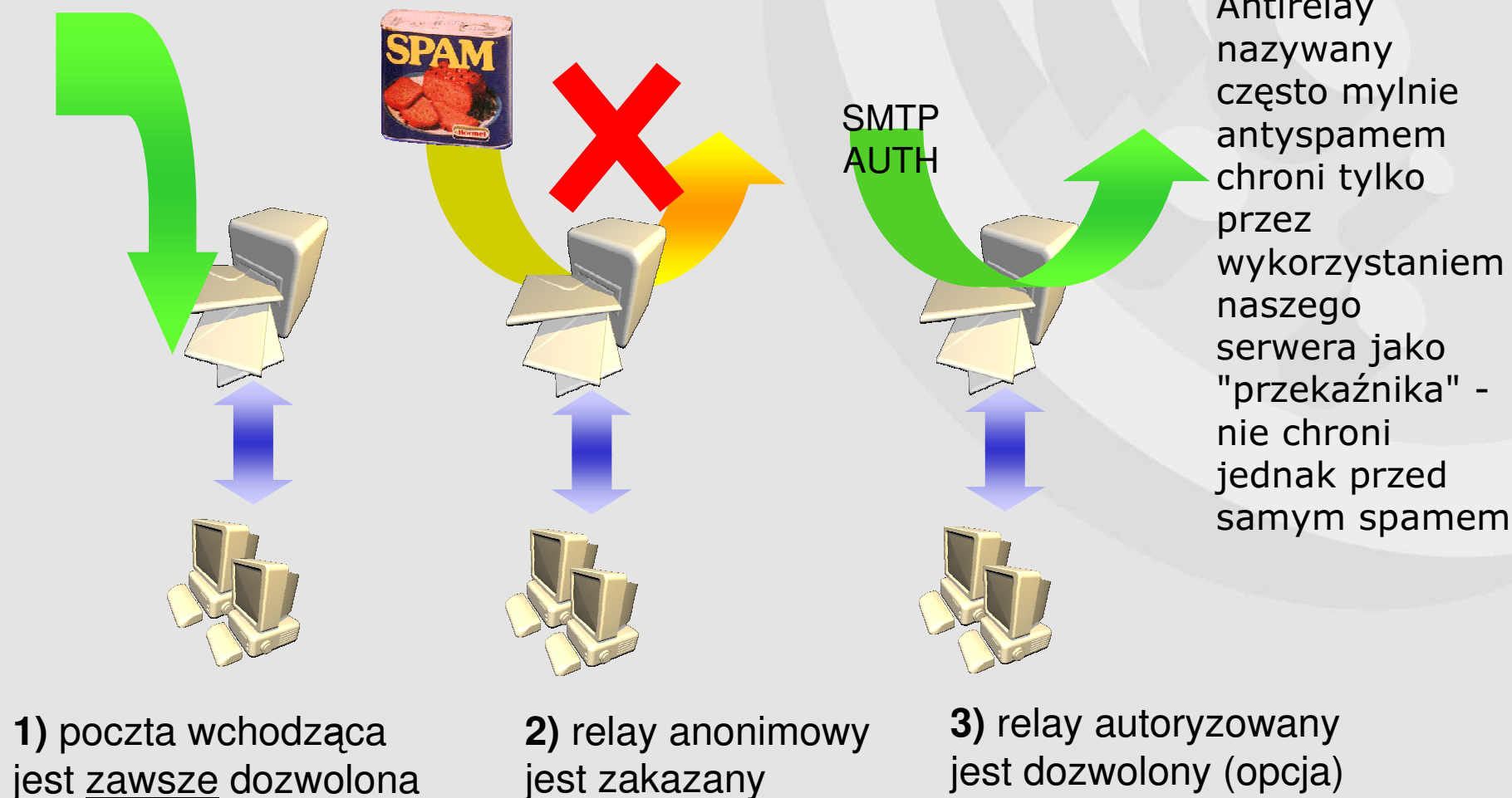
...

biznes.goga.pl



Znaczna liczba wirt. serwerów o kategorii "sex" spowoduje sklasyfikowanie całego serwera, tj. jego adresu IP jako "sex" i odcięcie dostępu do innych tematycznych serwisów WWW

Kontrola nagłówków SMTP - "Antirelay"



Zestawienie

- Analiza meta-informacji
 - **Zalety:** szybkie
 - **Wady:**
 - mało precyzyjne
 - zawsze o "krok do tyłu"
- Analiza informacji
 - **Zalety:**
 - dokładne
 - wszechstronne (słowa kluczowe, wirusy, typy danych)
 - **Wady:** powolne

MIMEsweeper

Co to jest MIMESweeper?

- Największy dostawca oprogramowania "Content Security"
- Obecny w: Wlk. Brytania (centrala), Francja, Niemcy, USA, Australia, Japonia
- 12,000+ klientów na całym świecie
 - 40 z 64 największych banków
 - Wszystkie z 10 największych firm prawniczych
 - 70% firm z FTSE 200
 - 40% firm z grupy Global 500
- 40% udziału w runku "E-mail/Web Content Security"
[IDC, 2000]

Co to jest MIMEsweeper?

1995

- Pierwsza wersja



MIMEsweeper v1

1997

- \$5 mln przychodów
- podwojenie przychodów co rok
- wersja 3



2000

- wersja 4
- > 6,000 klientów
- Przejęcie przez Baltimore za \$1 mld.



2002

- >12,000 klientów
- Połączenie z ClearSwift



Co to jest **MIMESweeper?**

- **MAILsweeper for SMTP**
- **MAILsweeper for Microsoft Exchange 5.x/2000**
- **MAILsweeper for Lotus Domino R5**
- **WEBsweeper**
- **IMAGEmanagement (PORNsweeper)**

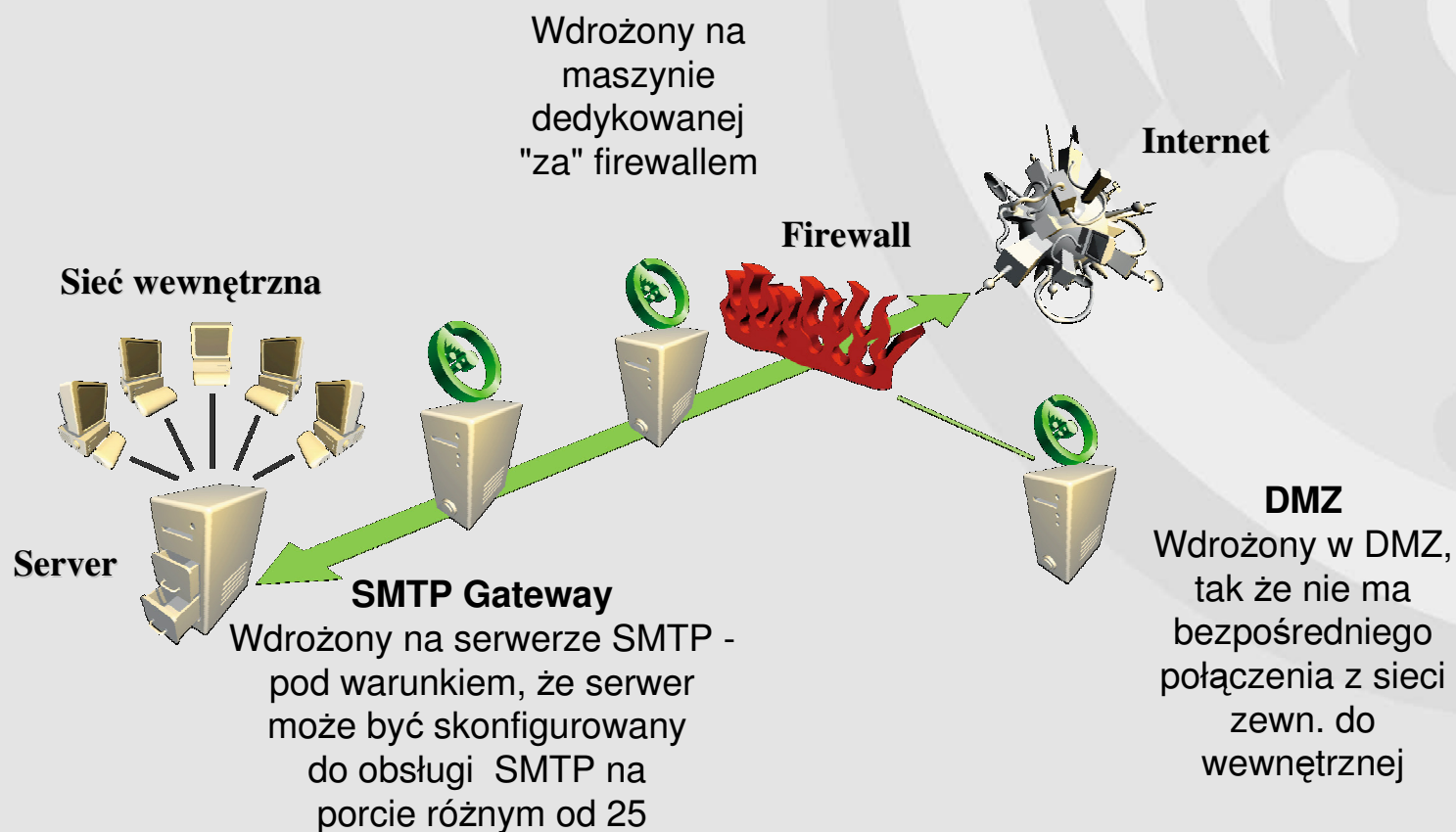
MAILsweeper

- Cechy:

- Zarządzanie polityką bezpieczeństwa
- Intuicyjne GUI
- Czyszczenie i regeneracja wiadomości
- analiza leksykalna (słowa klucz. i frazy)
- Anty-Spam
- Architektura wielowątkowa
- Architektura skalowalna i odporna na błędy
- Wszechstronne logowanie i audyt
- Wsparcie dla wiadomości szyfrowanych (osobny moduł)
- Wsparcie dla analizy obrazów (osobny moduł)



MAILsweeper



MIMEsweeper - GUI

MSW - [Console Root\MAILsweeper Policy on Gateway1\MAILsweeper for SMTP\Policies\Scenarios]

Console Window Help

Action View

Console Root

- MAILsweeper Policy on Gateway1
 - Licences
 - MAILsweeper for SMTP
 - Address Lists
 - Policies
 - Classifications
 - Scenarios**
 - Incoming
 - Outgoing
 - from Sales
 - from Development
 - from Administration
 - from Marketing
 - from Finance
 - Internal
 - Relay
 - Message Areas
 - Alerters
 - SMTP Relay
 - Manager

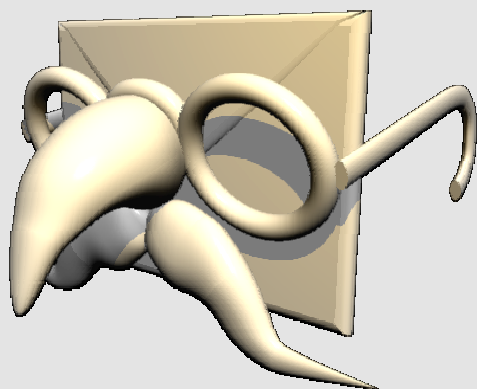
Name	Origin	State
Incoming		
Outgoing		
Internal		
Relay		
Anti-virus (Sophos)	Scenarios	Active
arc	Scenarios	Active
Delay Large E-mail	Scenarios	Active
Spoof E-mail	Scenarios	Active

MAILsweeper - scenariusze

- Spam Manager
- Spoof Notifier
- Text Analyzer
- Size Manager
- Virus Manager
- File Blocker
- Data Type Manager
- Pattern Matcher
- Attachment Manager
- Legal Disclaimer
- Commercial Disclaimer
- Archiver
- HTML Manager
- Signature Detect
- Executable

Scenariusze MAILsweepera

- Spam Manager
- **Spoof Notifier**
- Inteligentne wykrywanie "spoofingu" adresów e-mail
- Wykrywanie hakerskich technik adresowania n.p. %hack
- Ostrzega o próbach spoofingu



Scenariusze MAILsweepera

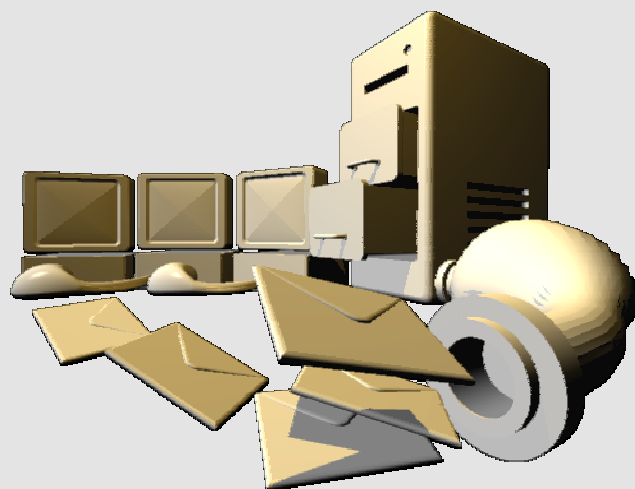
- Spam Manager
- Spoof Notifier
- **Text Analyzer**



- Wykrywanie słów i fraz
- Analiza kontekstowa:
 - (word 1 NEAR word 2)
 - (word 1 NOT with word 2)
- Reguły "wagowe"
- Zastosowania:
 - kwestie poufności
 - wulgaryzmy, itp.

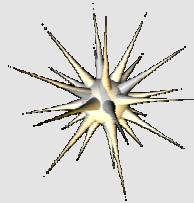
Scenariusze MAILsweepera

- Spam Manager
- Spoof Notifier
- Text Analyzer
- **Size Manager**



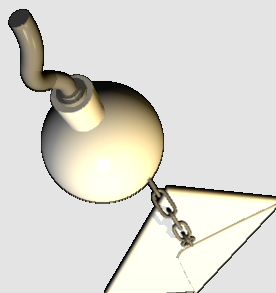
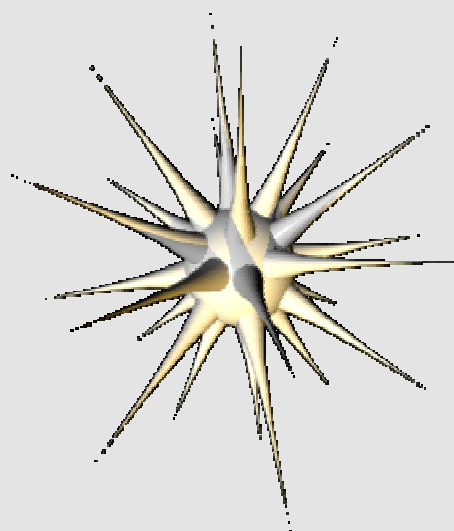
- Usuwanie wiadomości zbyt dużych
- Np. wideo "Star Wars": 25MB
- Blokowanie lub "parkowanie" (opóźnianie) do dostarczenia w godzinach "poza biurowych"
- Unikamy obciążenia sieci w godzinach biurowych

Scenariusze MAILsweepera

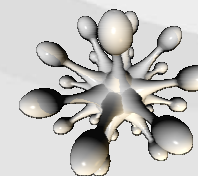


- Spam Manager
- Spoof Notifier
- Text Analyzer
- Size Manager

- **Virus Manager**

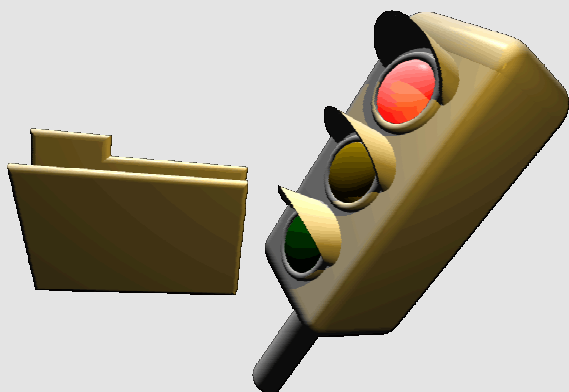


- Szeroki wybór skanerów antywirusowych firm trzecich
- Wykrywanie wirusów i "koni trojańskich"
- Reakcja na wykrycie wirusa:
 - Kwarantanna
 - Czyszczenie i rekompozycja
 - Usuwanie i informowanie



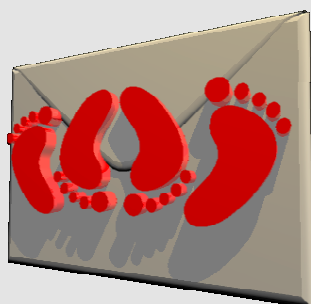
Scenariusze MAILsweepera

- Spam Manager
 - Spoof Notifier
 - Text Analyzer
 - Size Manager
 - Virus Manager
 - **File Blocker**
- Rozpoznawanie typów plików n.p. *.vbs
 - Blokowanie i parkowanie konkretnych typów plików np. filmów "Budweiser"



Scenariusze MAILsweepera

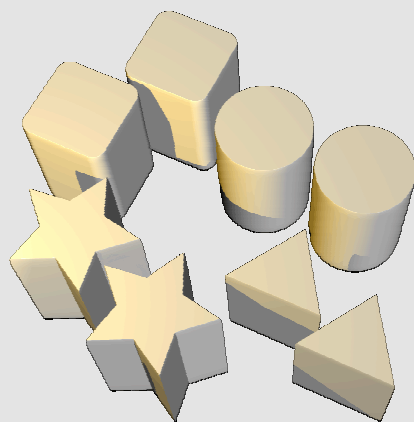
- Spam Manager
- Spoof Notifier
- Text Analyzer
- Size Manager
- Virus Manager
- File Blocker
- **Data Type Manager**



- Rozpoznawanie typu plików
- Rozpoznawanie po strukturze pliku NIE rozszerzeniu
- Format Manager rozpoznaje:
 - Formaty skompresowane
 - Dokumenty
 - Pliki wykonywalne
 - Wideo
 - Obrazki
- Ochrona przed rozpowszechnianiem materiałów obraźliwych lub szkodliwych dla image-u firmy

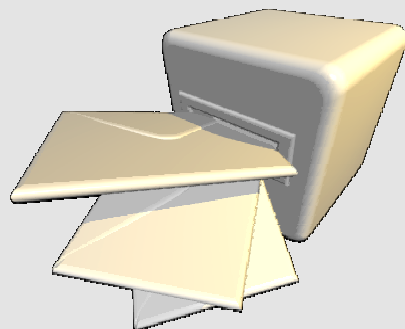
Scenariusze MAILsweepera

- Spam Manager
- Spoof Notifier
- Text Analyzer
- Size Manager
- Virus Manager
- File Blocker
- Data Type Manager
- **Pattern Matcher**
- Rozpoznawanie nowych typów plików:
 - np.: MP4, CAD
- Rozpoznawanie po strukturze pliku NIE rozszerzeniu
- Unikamy rozpowszechniania informacji potencjalnie groźnych dla image-u firmy



Scenariusze MAILsweepera

- Spam Manager
- Spoof Notifier
- Text Analyzer
- Size Manager
- Virus Manager
- File Blocker
- Data Type Manager
- Pattern Matcher
- **Attachment Manager**
- Kontrola liczby przesyłanych załączników
- Ochrona przed degradacją wydajności



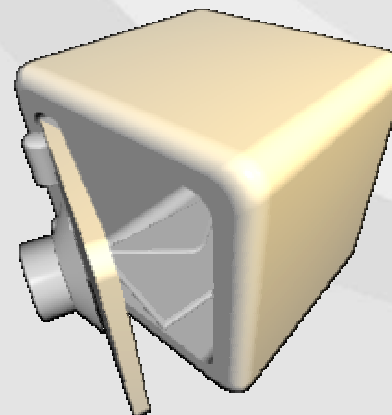
Scenariusze MAILsweepera

- Spam Manager
 - Spoof Notifier
 - Text Analyzer
 - Size Manager
 - Virus Manager
 - File Blocker
 - Data Type Manager
 - Pattern Matcher
 - Attachment Manager
 - **Legal Disclaimer**
 - **Commercial Disclaimer**
- Polityka firmowa może wymagać załączania standardowej stopki dot. Np. odpowiedzialności prawnej, itp.



Scenariusze MAILsweepera

- Spam Manager
- Spoof Notifier
- Text Analyzer
- Size Manager
- Virus Manager
- File Blocker
- Data Type Manager
- Pattern Matcher
- Attachment Manager
- Legal Disclaimer
- Commercial Disclaimer
- **Archiver**
 - Archiwizacja wszystkich przechodzących przez serwer przesyłek
 - Archiwa poczty elektronicznej z możliwością przeszukania



Scenariusze MAILsweepera

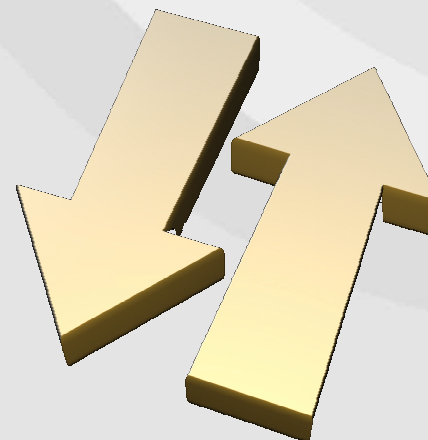
- Spam Manager
 - Spoof Notifier
 - Text Analyzer
 - Size Manager
 - Virus Manager
 - File Blocker
 - Data Type Manager
 - Pattern Matcher
 - Attachment Manager
 - Legal Disclaimer
 - Commercial Disclaimer
 - Archiver
 - **HTML Manager**
- Wykrywanie "ukrytego" kodu HTML i JavaScript
 - Wykrywanie konstrukcji "mailto"
 - Ochrona przed koniami trojańskimi, których celem jest "wyssanie" informacji z zainfekowanej maszyny



Scenariusze MAILsweepera

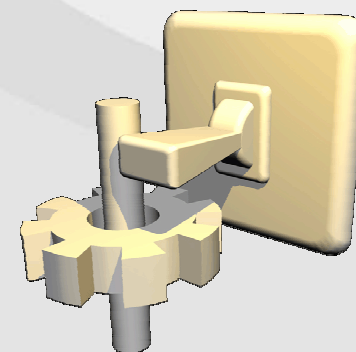
- Spam Manager
- Spoof Notifier
- Text Analyzer
- Size Manager
- Virus Manager
- File Blocker
- Data Type Manager
- Pattern Matcher
- Attachment Manager
- Legal Disclaimer
- Commercial Disclaimer
- Archiver
- HTML Manager
- **Signature Detect**

- Wykrywanie enkrypcji, podpisów cyfrowych, itp.
- Zapobieganie autoryzowanej wymianie poufnych informacji

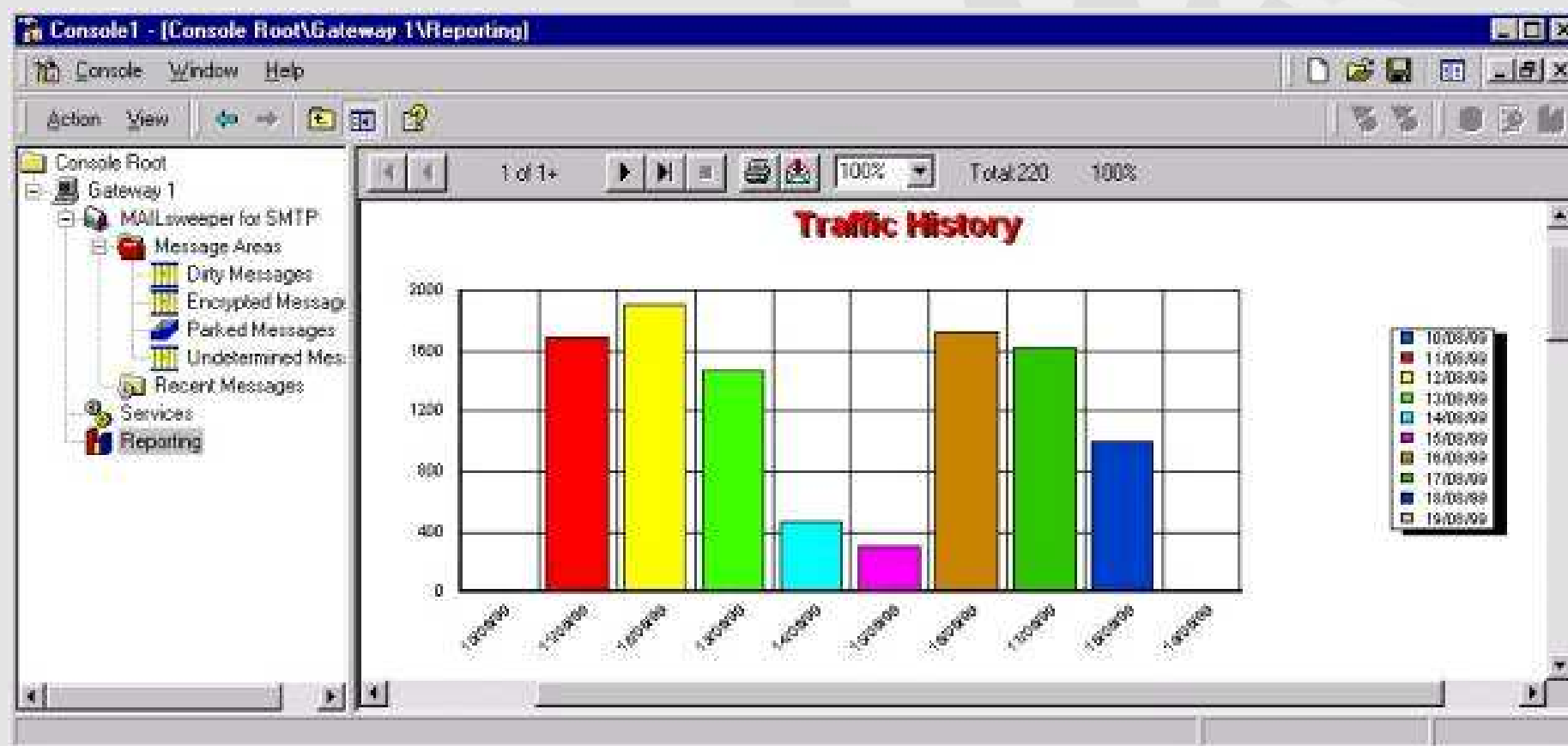


Scenariusze MAILsweepera

- Spam Manager
- Spoof Notifier
- Text Analyzer
- Size Manager
- Virus Manager
- File Blocker
- Data Type Manager
- Pattern Matcher
- Attachment Manager
- Legal Disclaimer
- Commercial Disclaimer
- Archiver
- HTML Manager
- Signature Detect
- **Executable**
- Zewnętrzne programy mogą być uruchamiane przez serwer MAILsweeper w celu przeprowadzenia dodatkowych testów
- Zastosowania:
 - SCRIPTS.EXE - rozpoznawanie skryptów w załącznikach
 - zewnętrzne skanery kodu



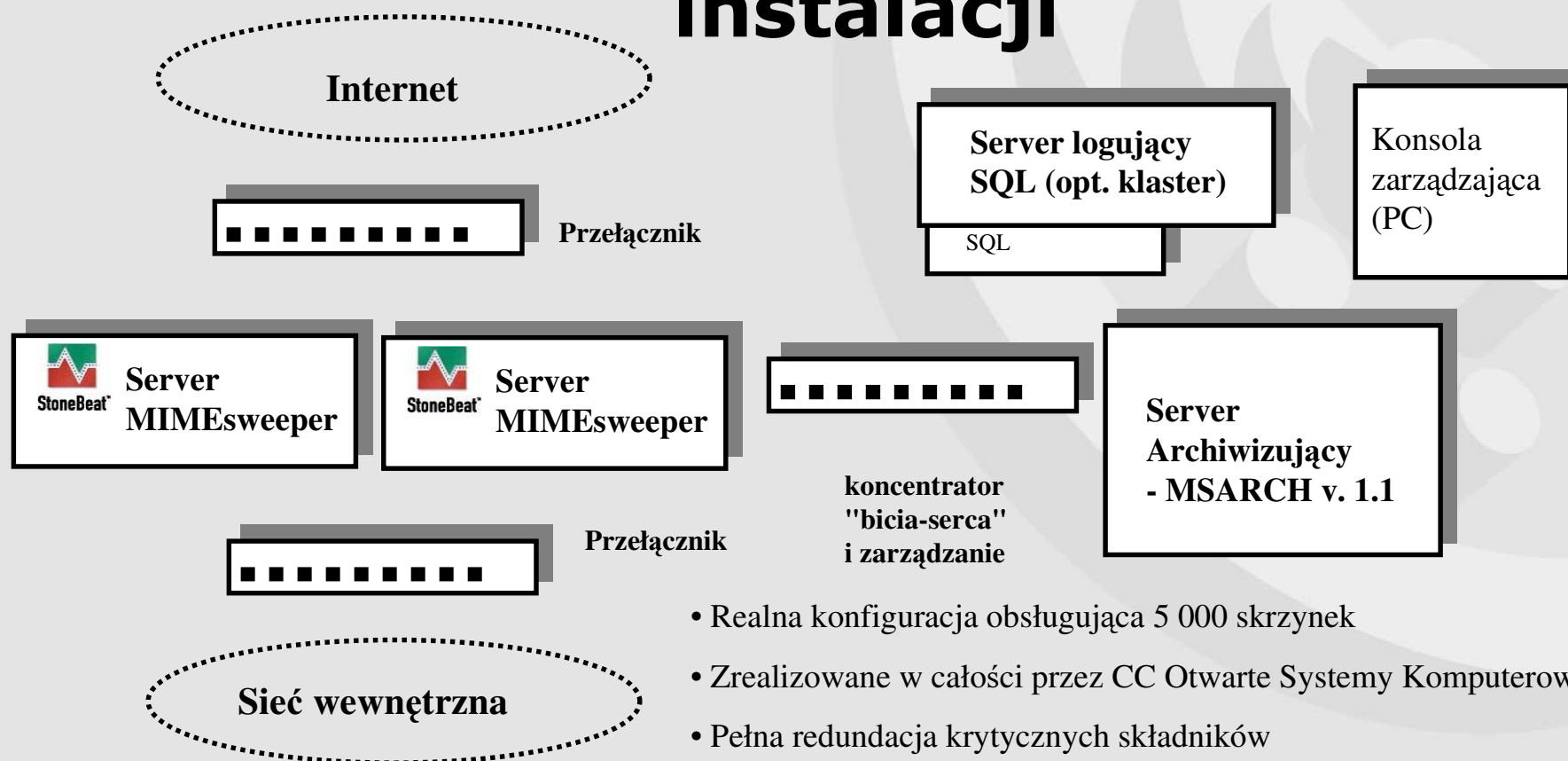
MAILsweeper - raporty



MAILsweeper - własne raporty

- Logowanie do bazy SQL pozwala na budowanie własnych raportów poprzez:
 - aplikację Crystal Reports
 - dowolny interfejs z dostępem do bazy SQL (np. skrypty ASP, PHP, ...)
- Przykładowe raporty (statystyki):
 - typy i podtypy załączników,
 - wirusy i ich źródła (nadawcy wg. domeny),
 - wystąpienia słów kluczowych w przesyłkach i załącznikach

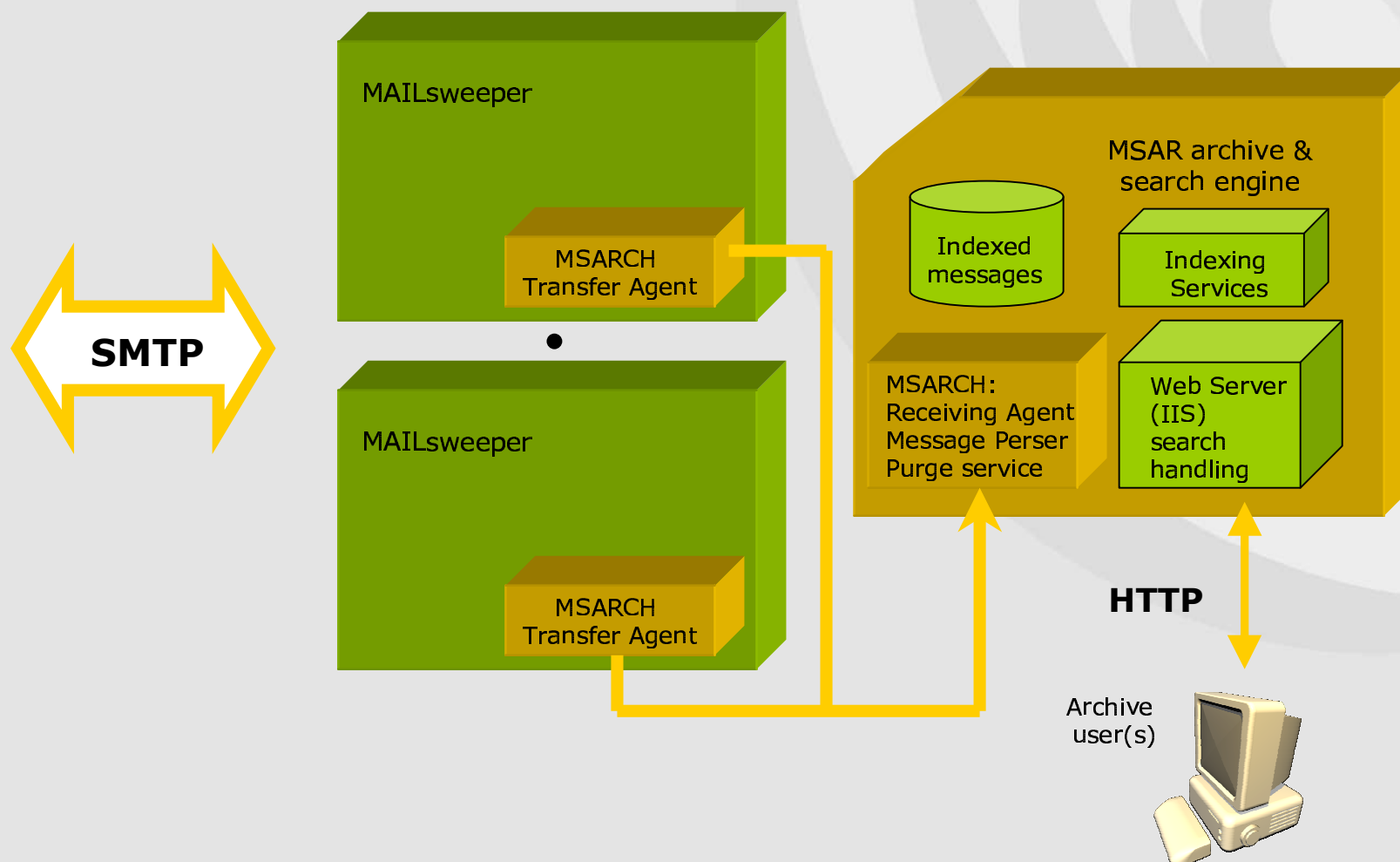
Przykładowa konfiguracja dużej instalacji



- Realna konfiguracja obsługująca 5 000 skrzynek
- Zrealizowane w całości przez CC Otwarte Systemy Komputerowe
- Pełna redundacja krytycznych składników
- Równoważenie obciążenia
- Software: MAILsweeper 4.2, StoneBeat Security Cluster, Microsoft Advanced Server 2000, Microsoft SQL Server, własne oprogramowanie MSARCH v. 1.4

MSARCH v. 1.4

archiwizacja przesyłek e-mail



IMAGEmanagement (d. PORNsweeper)



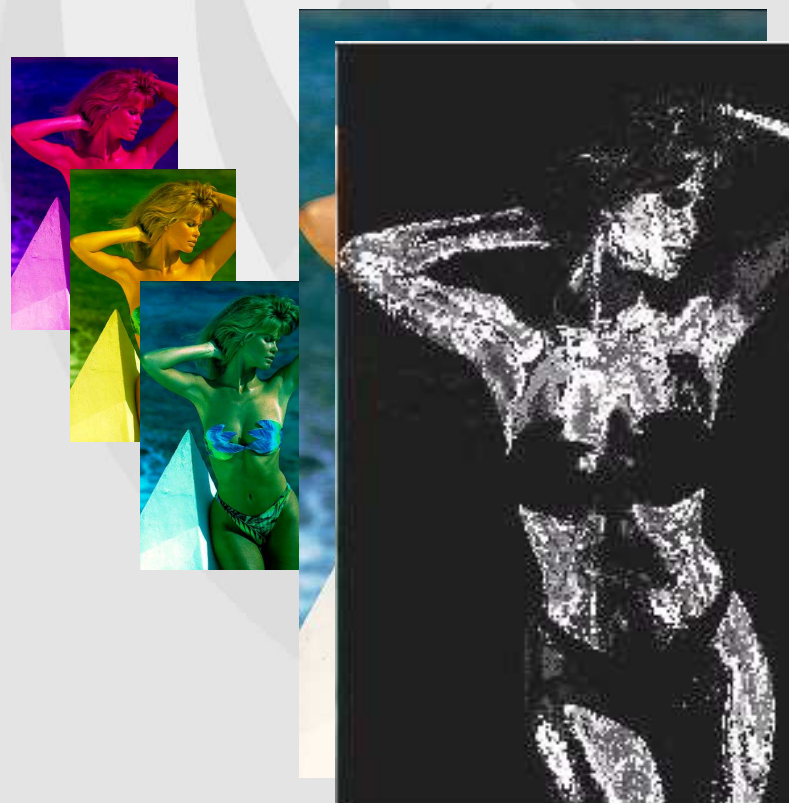
- "Sex" - najczęściej wyszukiwany termin w Internecie
wg: www.wordtracker.com
- 70% transmisji danych związanych z seksem ma miejsce w godzinach pracy
wg: www.sextracker.com
- Do 30 milionów odwiedzających strony pornograficzne dziennie
wg: www.cnet.com
- Rozpowszechnianie materiałów "obscenicznych" jest nielegalne w większości krajów świata.
- Przemysł pornograficzny w internecie generuje 1 miliard USD rocznie - tendencja jest rosnąca.
wg: Forrester Research

PORNSweeper

Fazy 1 i 2:

(**PORNSweeper**)

- Wykrycie obrazka jako typu danych
- Konwersja na 24 bitową mapę bitową
- Analiza tekstury w celu wykrycia obszarów nagiego ciała



The “likely” skin mask

PORNSweeper

Faza 3 (**PORNsweeper**)

- Wydzielenie obszarów ciała
- Obliczenie:
 - relatywnej całkowitej powierzchni nagiego ciała
 - liczby obszarów nagiego ciała (skin blobs)
 - relatywnej powierzchni obszarów w stosunku do całkowitej powierzchni ciała



The “likely” skin mask

PORNSweeper

Faza 4 (**PORNsweeper**)

- "Rozpoznanie" twarzy (Digitech Projects)
 - Lokalizacja twarzy
 - Lokalizacja oczu
 - Lokalizacja owalu twarzy
 - Obliczenie relatywnej wielkości twarzy w stosunku do reszty ciała

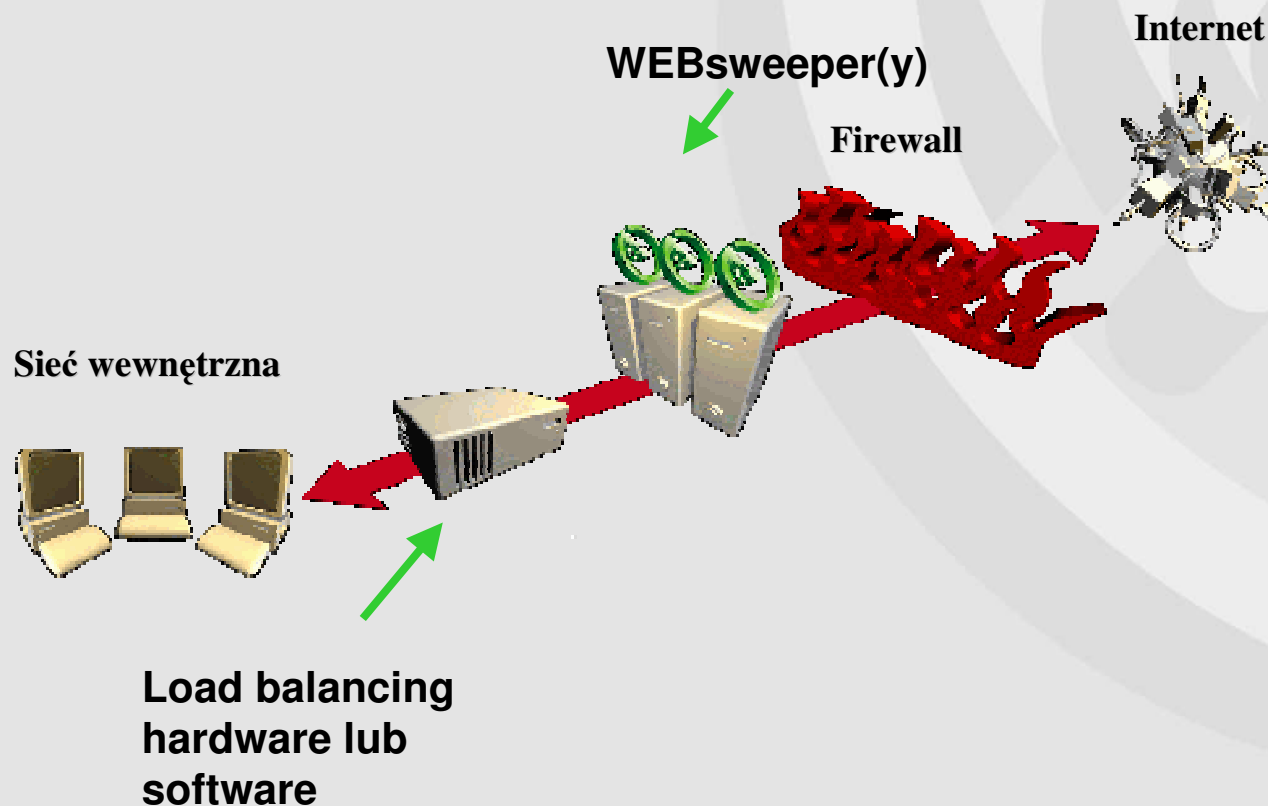


WEBSweeper

- Zarządzanie polityką bezp.
- Intuicyjne GUI
- Autentykacja użytkowników (NT domain, LDAP, text)
- Dwu kierunkowy cache
- Czyszczenie i regeneracja danych
- Analiza leksykalna (słowa klucz. i frazy)
- Architektura wielowątkowa
- Architektura skalowalna i odporna na błędy
- Wszechstronne logowanie i audyt
- Blokowanie adresów (sieciowa baza danych kilku mln. URL-i pogrupowanych w kilkudziesięciu kategoriach)



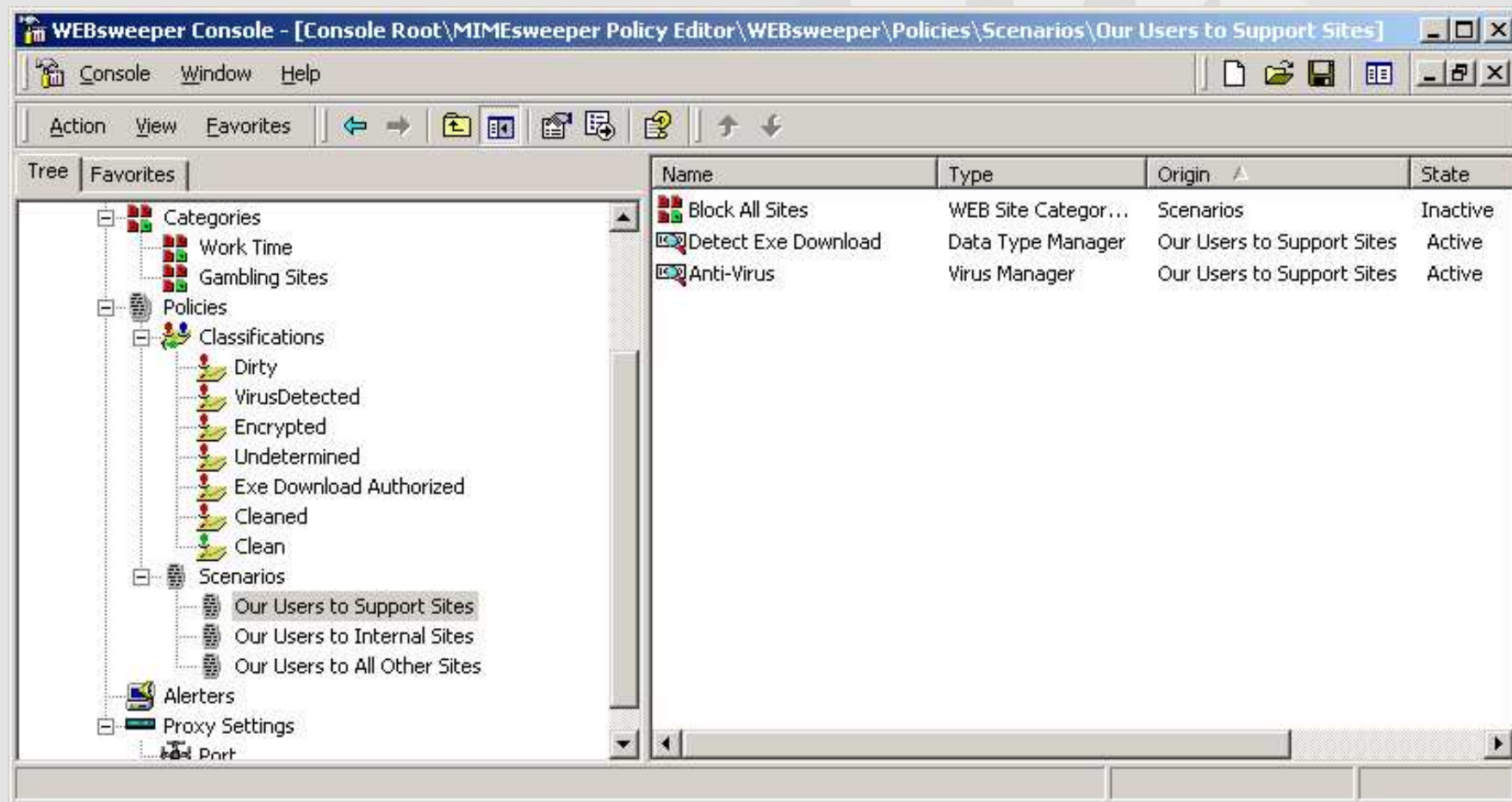
WEBSweeper - wdrożenie



Więcej niż 700 użytkowników - load balancing:

<http://www.mimesweeper.pl/>

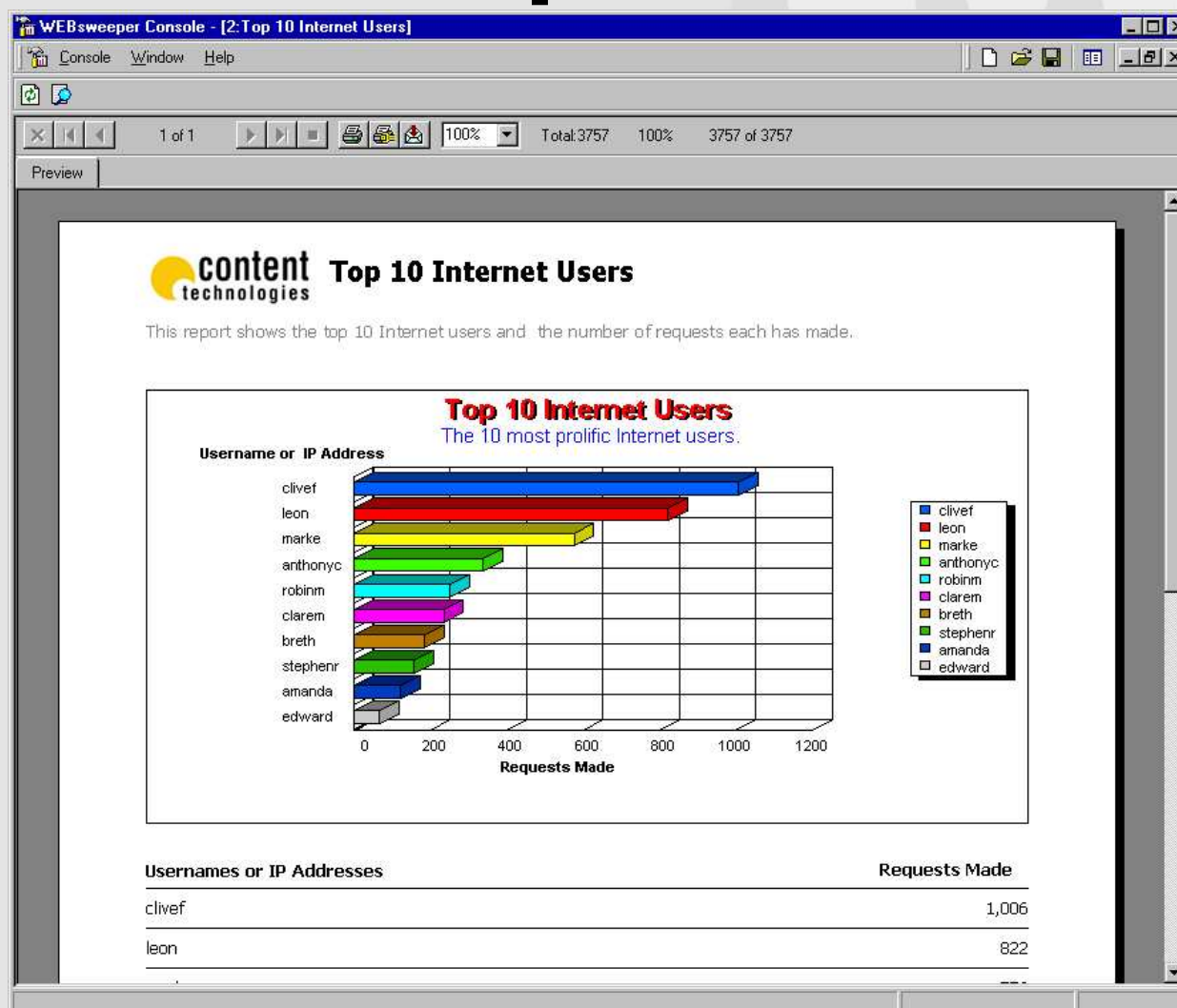
WEBSweeper - GUI



WEBsweeper - scenariusze

- Authenticode Manager
- Website Categoriser
- Cookies Manager
- Portable Code Manager
- File Blocker
- Data Type Manager
- Classifier
- Executables
- HTML Manager
- Pattern Matcher
- Text Analyser
- Virus Manager

WEBSweeper - raportowanie



Podsumowanie

- MAILsweeper i WEBsweeper - kompleksowa ochrona danych przesyłanych siecią

Pytania?