

*Техническая
информация о
продуктах
SurfControl*

Enterprise Threat Shield

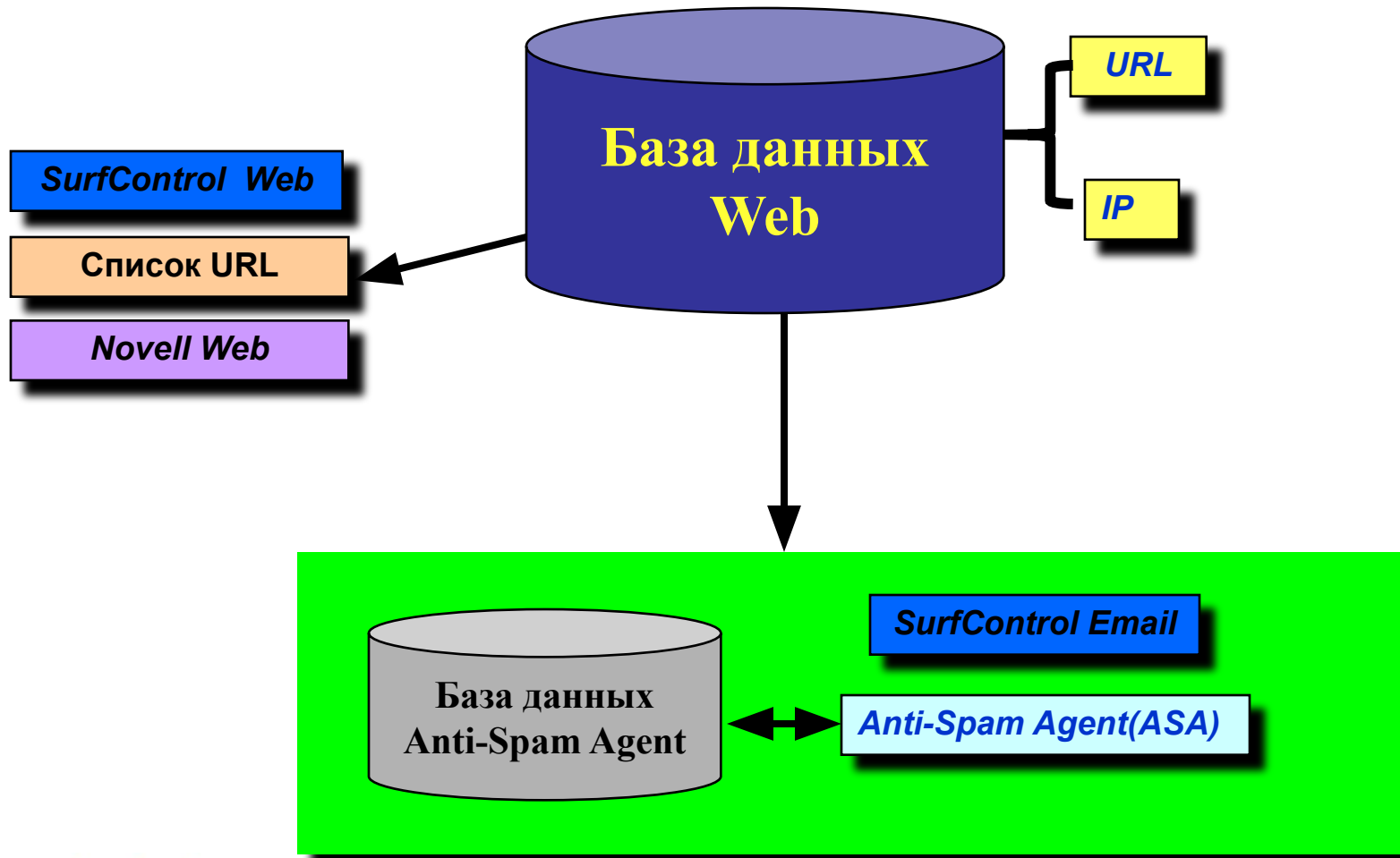
RiskFilter

Adaptive Threat Intelligence

E-mail Filter

Web Filter

Базы данных SurfControl



Исследование Интернет



- **Команда исследователей (60+)**

- *Великобритания*
- *Скоттс Валли*
- *Массачуссетс*
- *Австралия*
- *Австрия*
- *Голландия*
- *Россия*
- *Реселлеры / Партнеры*

- **21 язык**
- **Поиск новых сайтов с использованием автоматических средств**
- **Ручной анализ содержимого страниц**

Список категорий URL

- Все возможные угрозы:
 - Вирусы и вредоносные программы
 - Опасные приложения
 - Конфиденциальность
 - Угроза производительности труда
- 54 категории
- Более 18,5 млн. сайтов, содержащих более 3.3 млрд. страниц
- Сайты на более, чем 70 языках

Статистика

Web

Цифры

Количество сайтов	18,5 млн.
Количество веб-страниц	3.3 млрд.
Скорость наполнения базы данных	65,000 в неделю
Количество категорий	54
Языков в базе данных	70

Email

Цифры

Количество записей Anti-Spam Agent	~400,000
Словари ключевых слов	16 словарей на 11 языках

16 словарей на 11 языках

Эротические материалы
Алкоголь/Табак/Наркотики
Искусство и развлечения
Компьютеры и Интернет
Конфиденциальность
Финансы
Азартные игры
Дискриминация
Поиск работы
Медицина и здоровье
Спам
Интернет-магазины
Спорт
Путешествия
Нарушение законов, оружие
Опечатки спамеров




**Пользователь может
добавлять собственные
категории и ключевые слова**

SurfControl - Максимальная защита


SurfControl®
Web Filter

-  Microsoft
-  Cisco CE
-  Juniper


SurfControl®
Web Filter

-  Check Point
-  BlueCoat
-  Novell BM


SurfControl®
E-mail Filter

-  SMTP
-  MS Exchange
-  Riskfilter


SurfControl®
Virtual Control Agent


SurfControl®
Mobile Filter


SurfControl®
Enterprise Threat Shield


SurfControl®
Anti-Virus Agent

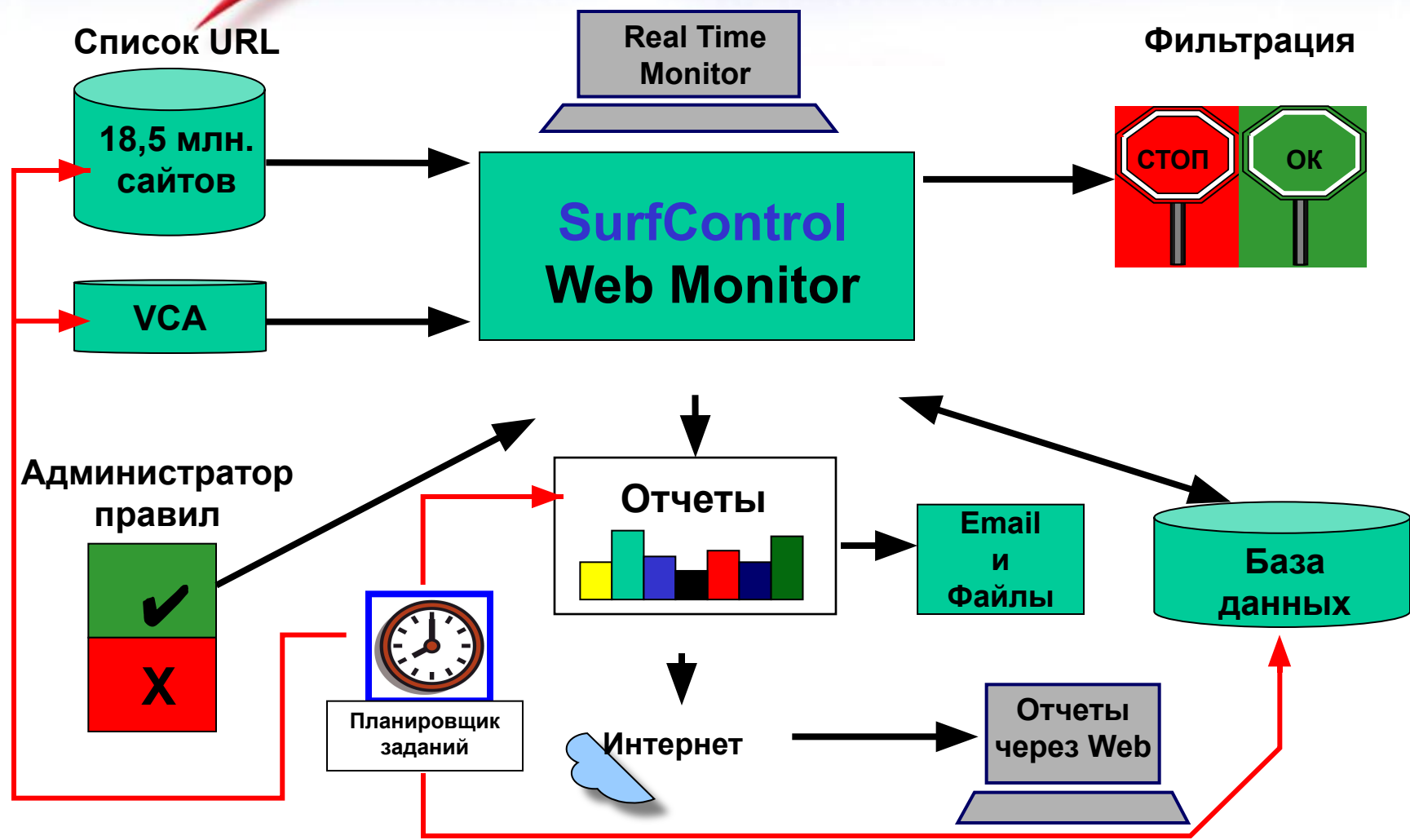

SurfControl®
Virtual Image Agent


SurfControl®
Anti-Spam Agent


SurfControl®
Virtual Learning Agent

SurfControl Web Filter 2000/2003, MS Proxy, MS ISA Обзор

SurfControl Web Filter



Технология



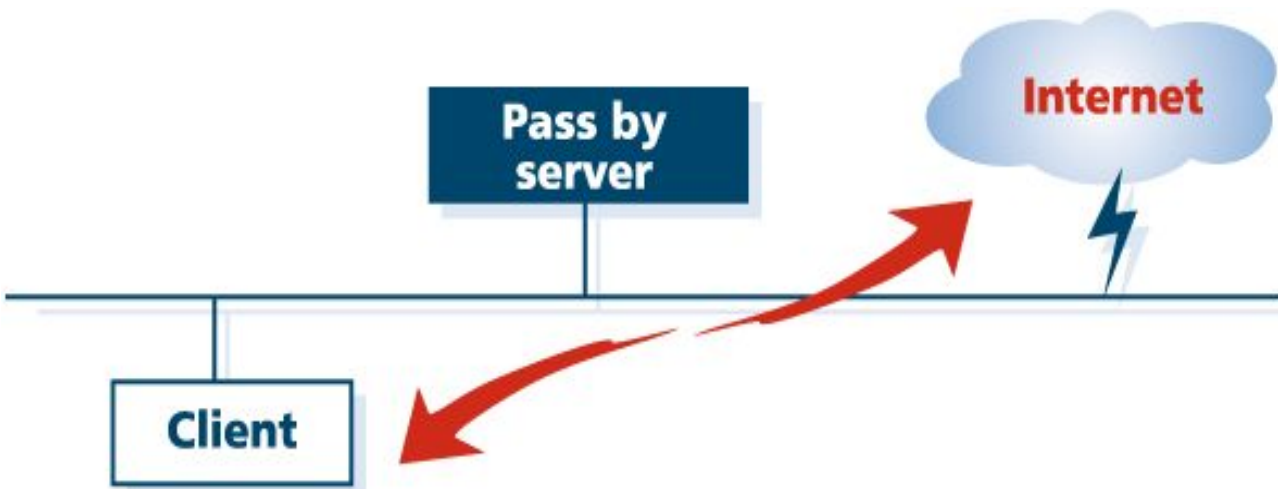
PASS – BY

MS Windows 2000/2003

• PASS - THRU

- MS ISA Server 2000
- MS Proxy Server
- Bluecoat Proxy SG
- Check Point FireWall-1
- Novell BorderManager
- Cisco CE

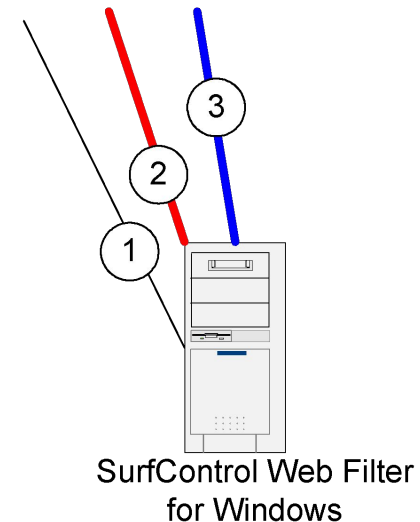
Версия для Windows (Технология Pass-By)



- Использует технологию sniffера
- Не влияет на производительность сети
- Может следить за всеми протоколами, не только за HTTP
- Должен видеть весь трафик в сети

Требования к оборудованию

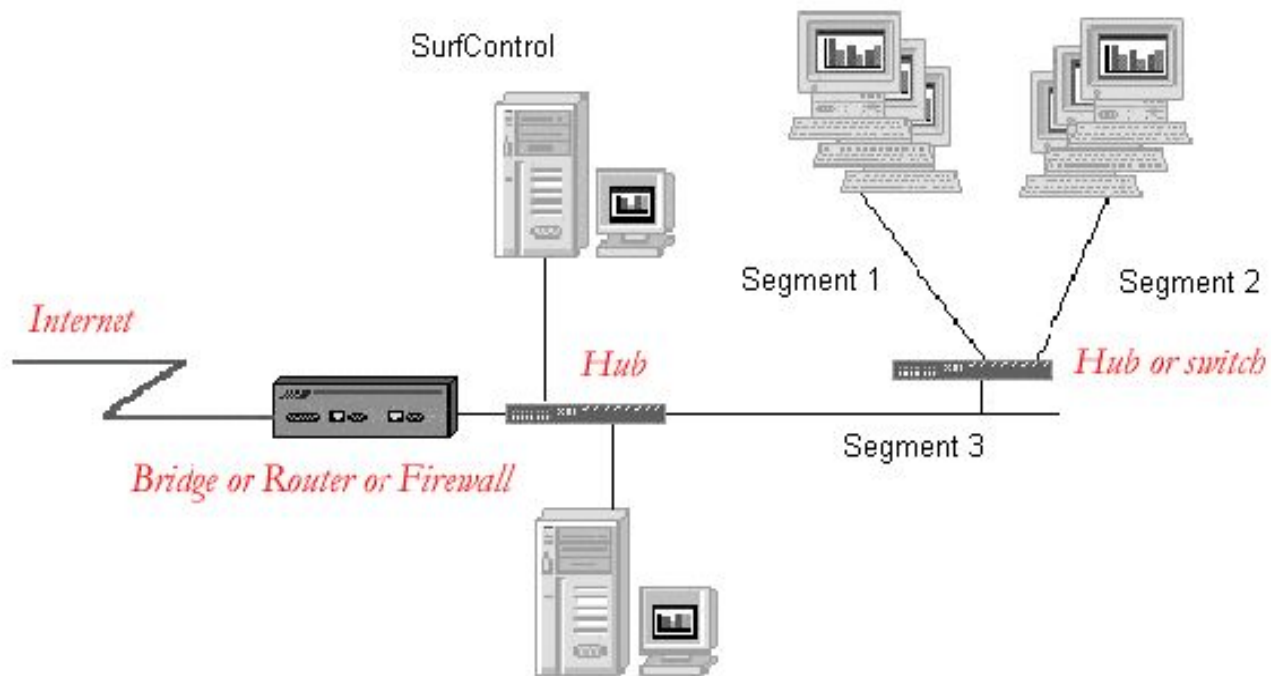
- Две сетевые карты
- №1 используется для прослушивания сети
- №2/3 используются для обычного трафика TCP, взаимодействия с базой данных, запросов DNS и др.



- SurfControl Network Protocol Device Driver
- Internet Protocol (TCP/IP)
- SurfControl Network Protocol Device Driver
- Internet Protocol (TCP/IP)

SurfControl Web Filter

- Пример конфигурации сети:



SurfControl Web Filter

Хаб рассылает пакет данных от клиента к серверу Surfcontrol и в Интернет

Surfcontrol анализирует пакет данных



SurfControl

Fin

Сайт должен быть заблокирован,
клиенту отправляется команда FIN

Fin

Сообщение от
www.playboy.com:
Доступ
заблокирован
surfCONTROL

Fin

Закреть
соединение
(FIN)

www.surfcontrol.com



Компьютер клиента:
192.168.0.1

Запрос в Интернет:
www.playboy.com



Hub

Fin

Сообщение от 192.168.0.1

Сбросить соединение (FIN/RST)

Fin

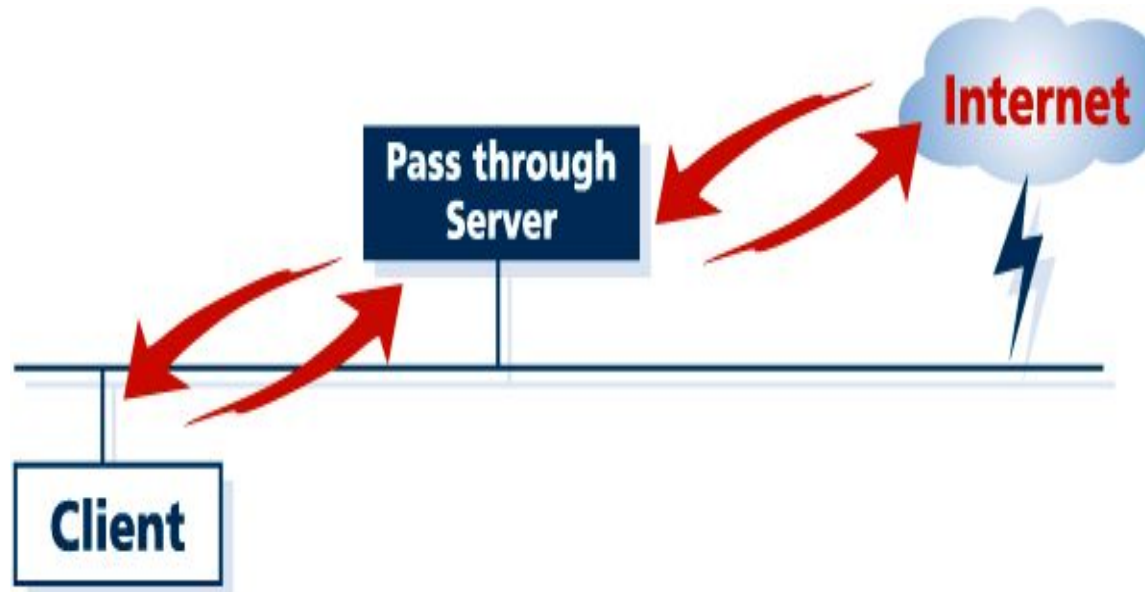


Router



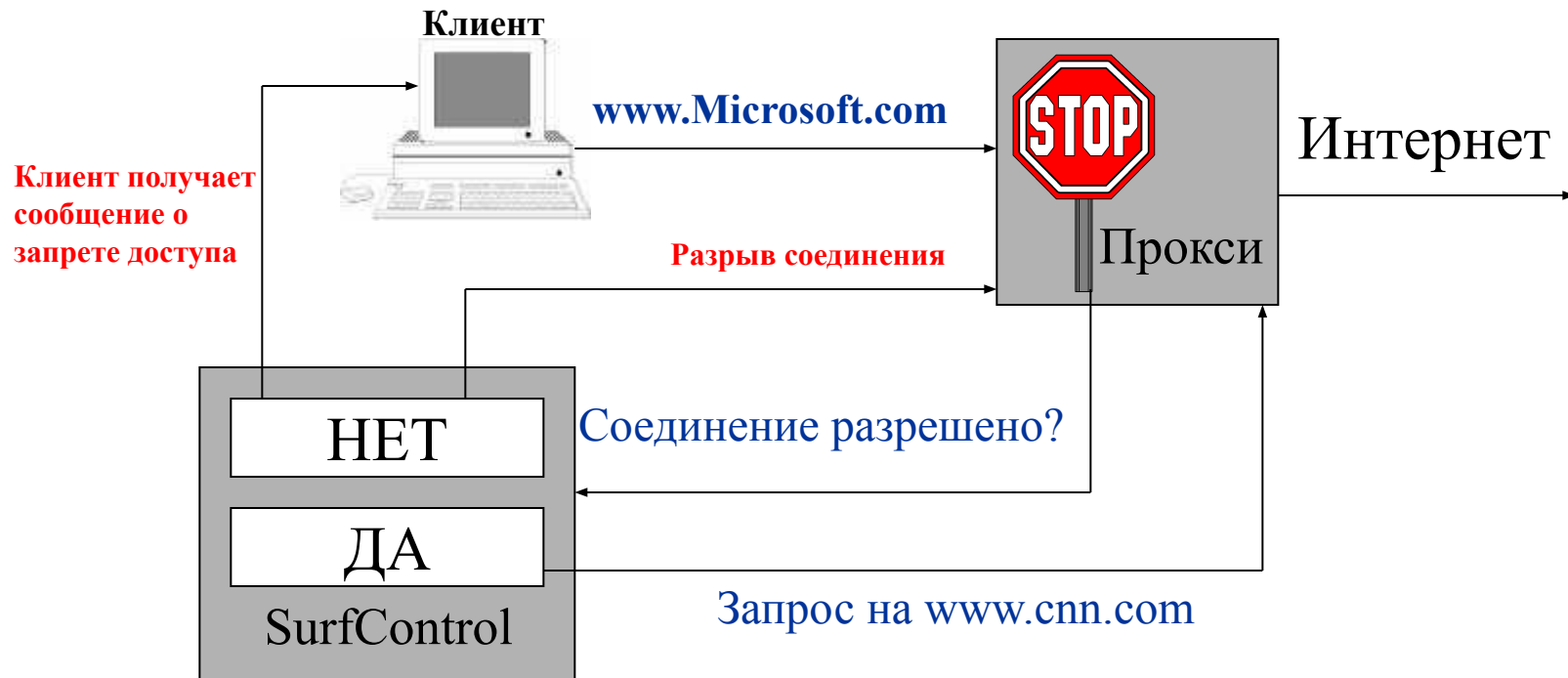
Веб-сервер Playboy.com

SurfControl Web для шлюзов (Технология pass-through)



- Использует технологию pass-through
- Подключается к прокси-серверу в качестве плагина

SurfControl Web Filter ДЛЯ ШЛЮЗОВ



Определение имен пользователей

- **Pass-Through**
 - Активное определение имен, используя авторизацию прокси-сервера
- **Pass-By**
 - Запрос по NetBIOS
 - Невысокая скорость работы, проблемы в сетях с маршрутизаторами
 - Enterprise User Monitor
 - Решает указанную проблему

Системные требования

	SurfControl Web Filter Win2000/Win2003	SurfControl Web Filter MS Proxy	SurfControl Web Filter MS ISA
Процессор	Pentium IV	Pentium IV	Pentium IV
Оперативная память	1 GB	1 GB	1 GB
Свободное место на жестком диске	1 GB	1 GB	1 GB
Сетевая карта	Поддержка режима «Promiscuous mode»		
Приложения		MS Proxy	MS ISA Server
Операционная система	Win2000 Server SP1 Win2000 AS SP1 Win2003	Win2000 Server SP1 Win2000 AS SP1	Win2000 Server SP1 Win2000 AS SP1 Win2003

Дополнительные средства SurfControl Web Filter

SurfControl Monitor

- Показывает информацию по:

Пользователю



Сайту



SuperScout Monitor - [SurfControl Scout]

File View Configure Window Help

Users

Display users which contain:

User Name	Workstation Name	IP Address	First Seen	Last Seen	Hits
jsbsv\anniew	ANNIEWYNLNT	192.132.210.207	10/4/2000 8:22:11	10/16/2000 10:51:31	339
ANNIEWYNLNT	ANNIEWYNLNT	192.132.210.207	10/3/2000 9:23:03	10/11/2000 15:02:48	163

Sites

Display sites which contain:

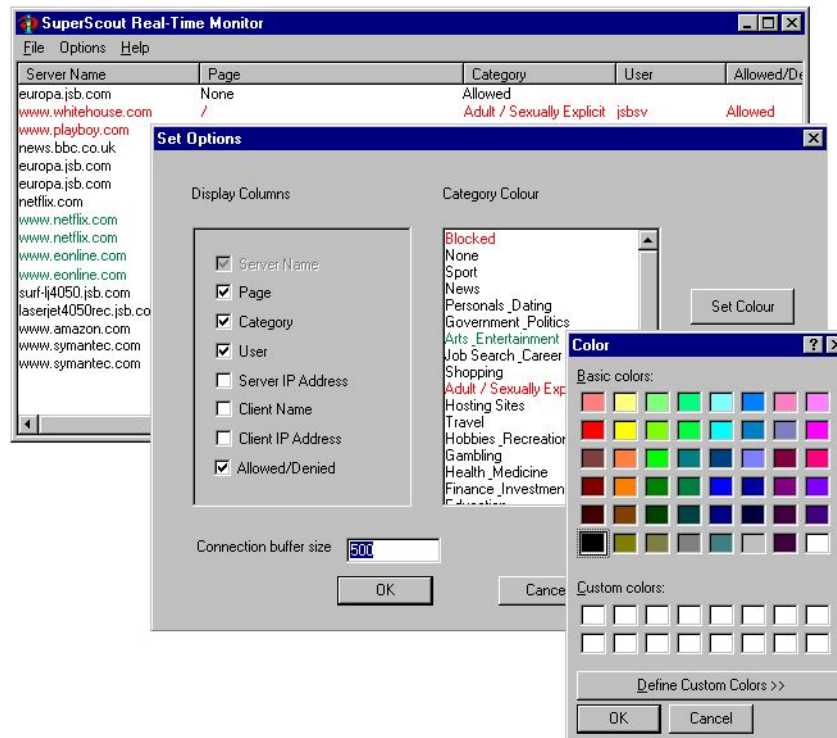
Host Name	IP Address	First Seen	Last Seen	Hits	Category
www.doitsports.com	209.249.105.34	10/16/2000 10:47...	10/16/2000 10:47:04	1	Sport
www.bsim.org	216.228.2.96	10/16/2000 10:43...	10/16/2000 10:46:35	28	Sport
www.yahoo.com	204.71.200.67	10/3/2000 9:23:17	10/16/2000 10:42:27	11	Search Engines
www.coolrunning.com	207.244.125.122	10/16/2000 10:39...	10/16/2000 10:39:43	2	Sport
mm3.bizar.com	216.205.139.49	10/16/2000 10:32...	10/16/2000 10:32:34	1	Adult / Sexually Explicit
www.softwarewithbrains.com	208.56.129.210	10/16/2000 10:32...	10/16/2000 10:32:17	1	
www.playboy.com	206.251.29.10	10/16/2000 10:29...	10/16/2000 10:29:50	1	Adult / Sexually Explicit
www.etrade.com	167.216.184.33	10/16/2000 10:28...	10/16/2000 10:29:24	2	Finance & Investment
listings.ebay.com	216.32.120.142	10/16/2000 10:22...	10/16/2000 10:27:37	6	Shopping
www.ebay.com	216.32.120.133	10/16/2000 10:21...	10/16/2000 10:22:50	2	Shopping
www.surfcontrol.com	208.1.69.111	10/3/2000 10:26:23	10/16/2000 9:56:18	72	Computing & Internet
www.eonline.com	216.136.194.201	10/3/2000 9:43:15	10/16/2000 9:46:24	56	Arts & Entertainment
www.vivonic.com	192.102.211.80	10/16/2000 9:33:19	10/16/2000 9:38:26	0	

For Help, press F1

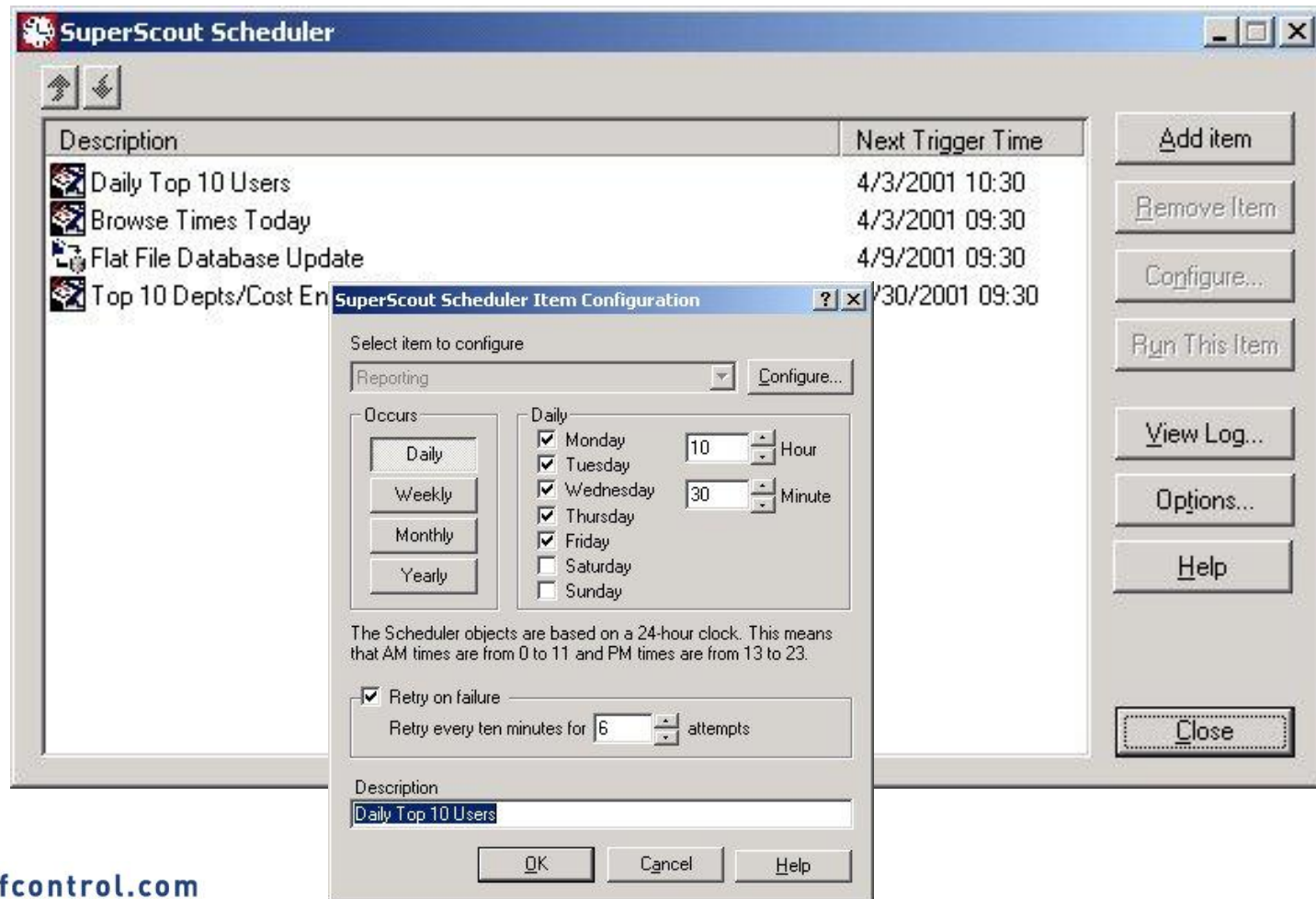
65 Records

Real-Time Monitor

- Цветовое выделение для наглядности

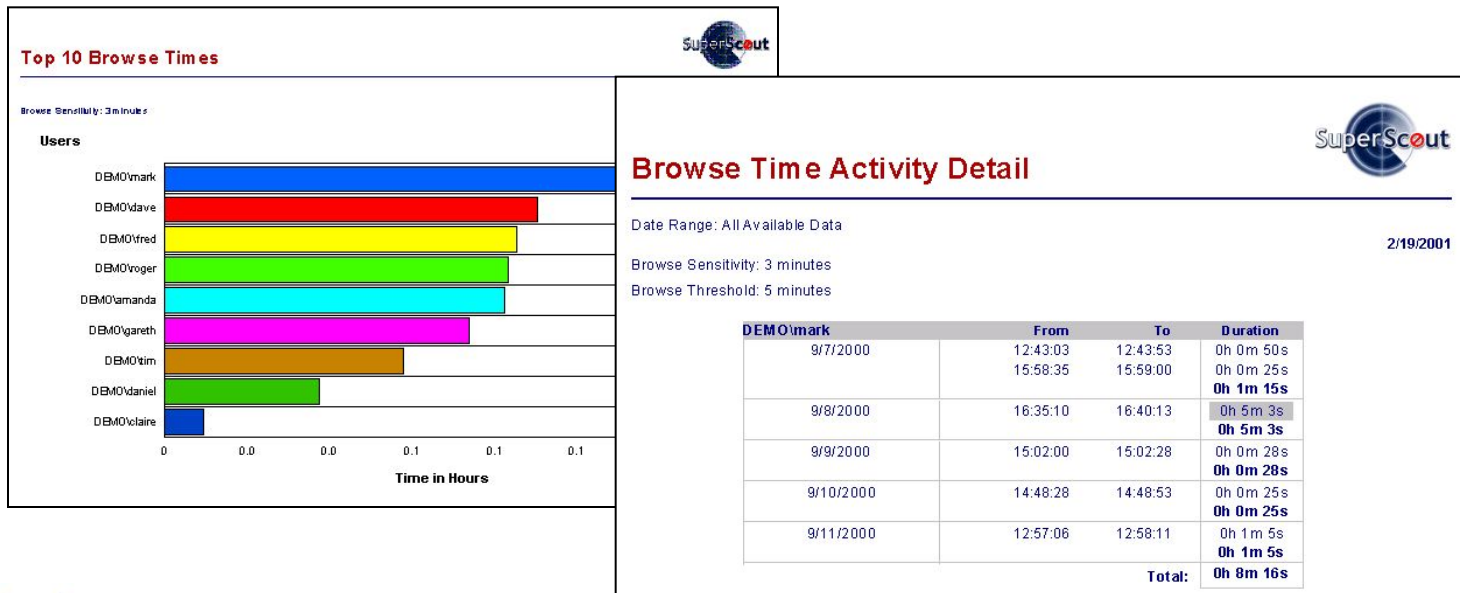


Гибкий планировщик заданий



Создание отчетов

- Доступ по HTTP/HTTPS
- Формат файлов: PDF, Word и т.д.



SurfControl Web Filter Virtual Control Agent

Virtual Control Agent



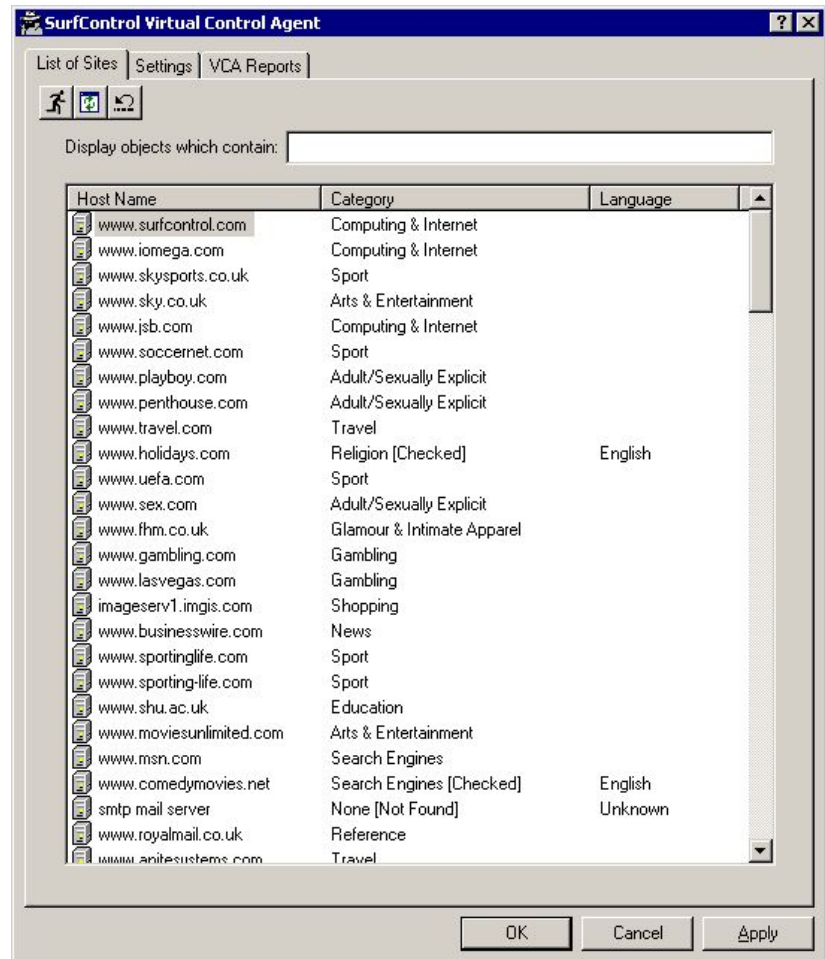
Использует нейронные сети



Автоматически категоризует новые сайты



Распределяет сайты по категориям SurfControl



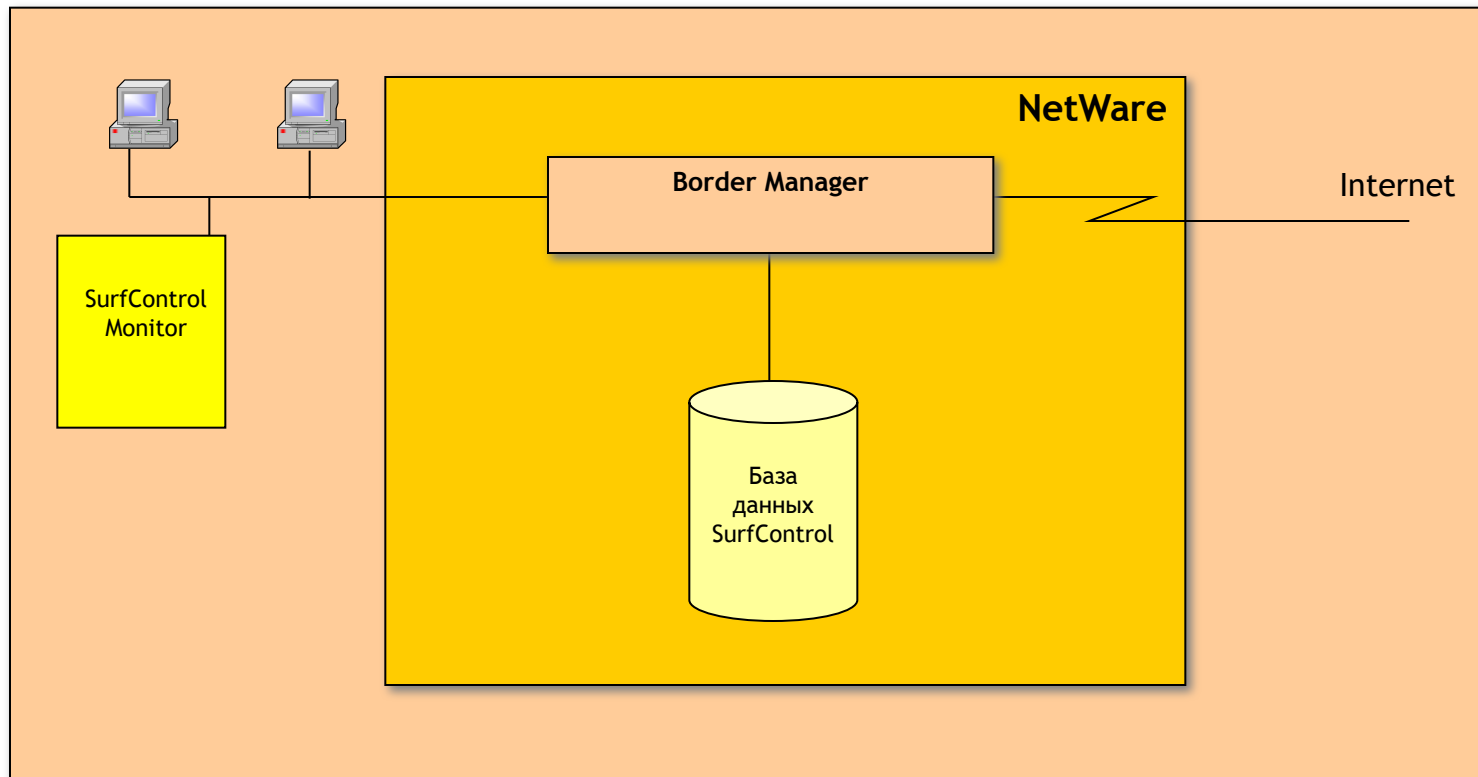
SurfControl Web Filter Border Manager Обзор



SurfControl Web Filter для Border Manager 3.7 или выше

- База данных SurfControl
 - Интегрируется с Novell Border Manager
 - Устанавливается на NetWare
- Опциональный модуль Monitor & Reporter
 - Более 50 различных отчетов
 - Устанавливается на Windows 2000/2003

Архитектура сети



SurfControl FireWall-1 Обзор



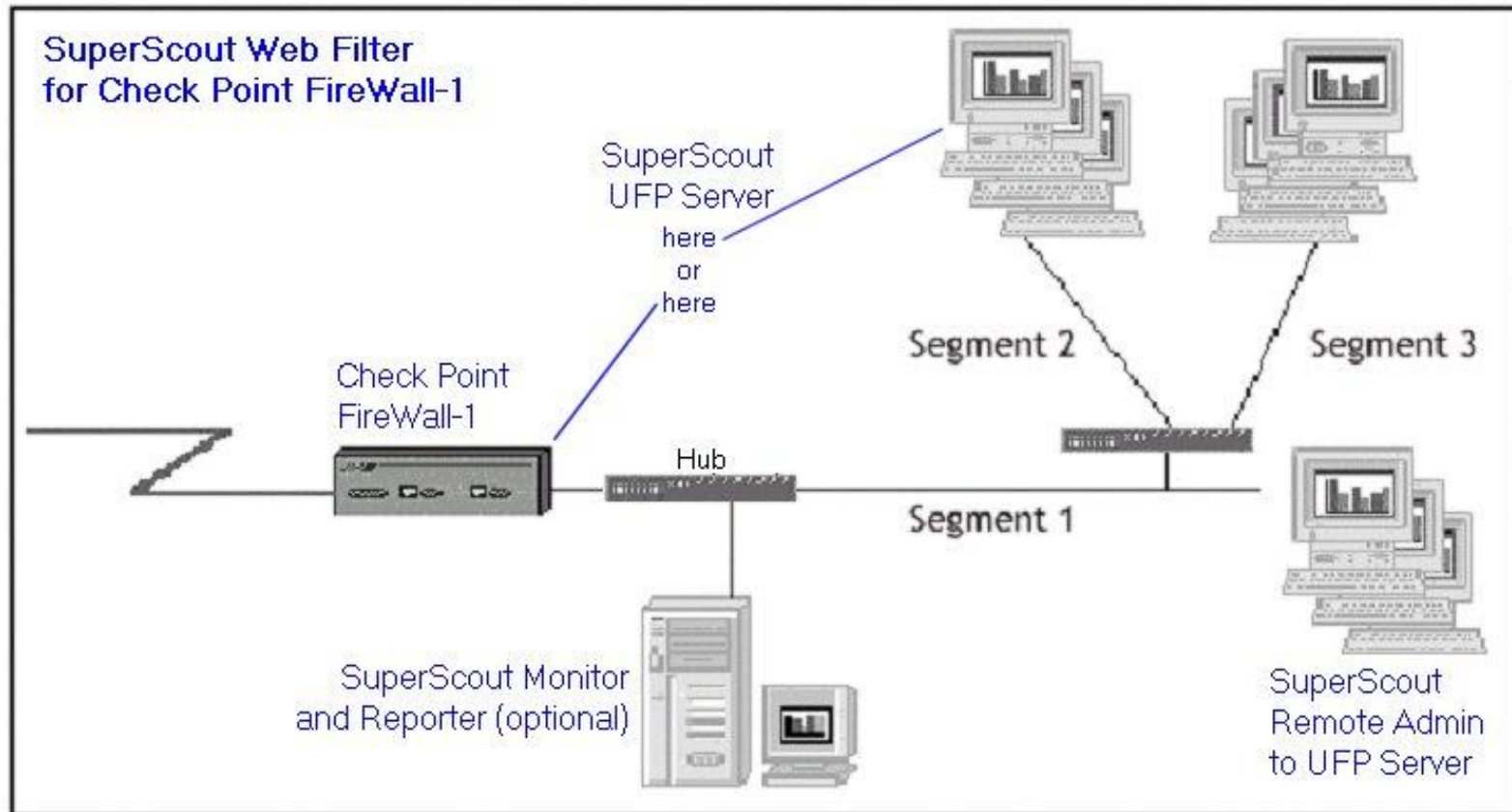
Linux
Windows

Windows

КОМПОНЕНТЫ

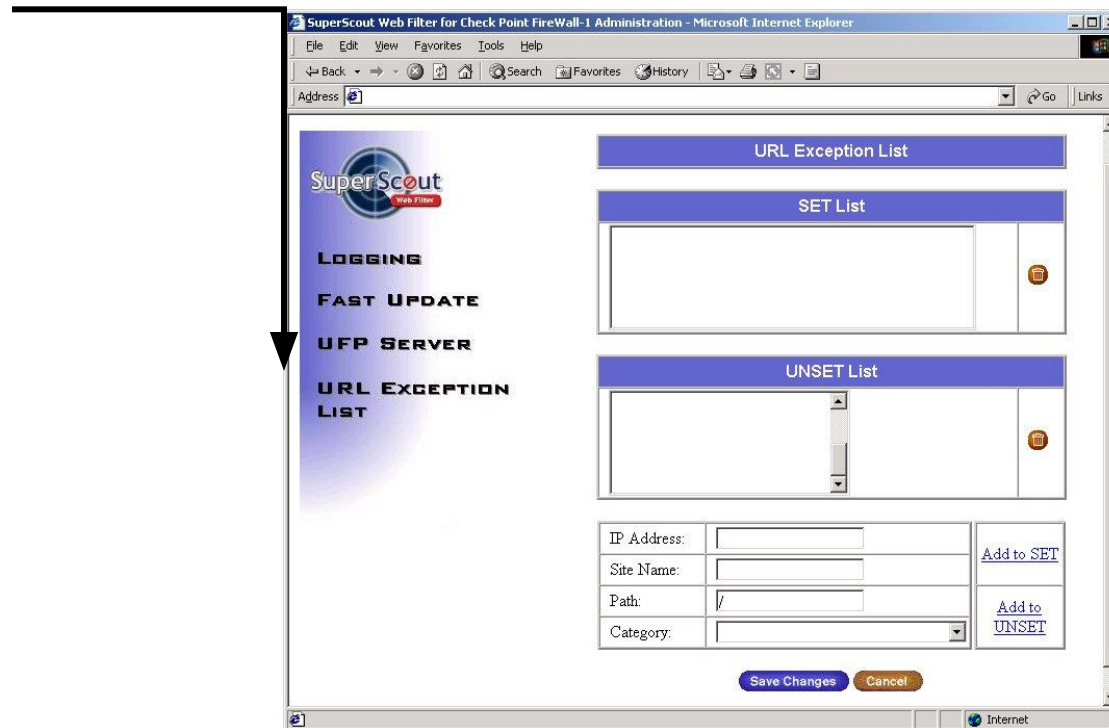
- SurfControl UFP Server
 - Протокол UFP
 - Блокировка на основе URL
- SurfControl Monitor and Reporter (опционально)
 - Мониторинг
 - По пользователям и по сайтам
 - Real-Time Monitor
 - Отчеты
 - Более 50 отчетов

Конфигурация сети



SurfControl UFP Server

- Удаленное администрирование через браузер



SurfControl UFP Server

- Обновление базы данных по расписанию

SuperScout Web Filter for Check Point FireWall-1 Administration - Microsoft Internet Explorer

Address <http://qasolaris.svqa.jsb.com:9999/>

SuperScout
Web Filter

LOGGING

FAST UPDATE

UFP SERVER

URL EXCEPTION LIST

Fast Update →

<input checked="" type="checkbox"/>	Enable URL Category List Updates
Primary Server:	<input type="text"/>
On Port:	<input type="text" value="80"/>
Path:	<input type="text"/>
Fallback Server:	<input type="text"/>
On Port:	<input type="text" value="80"/>
Path:	<input type="text"/>

Local Settings

Working Directory:

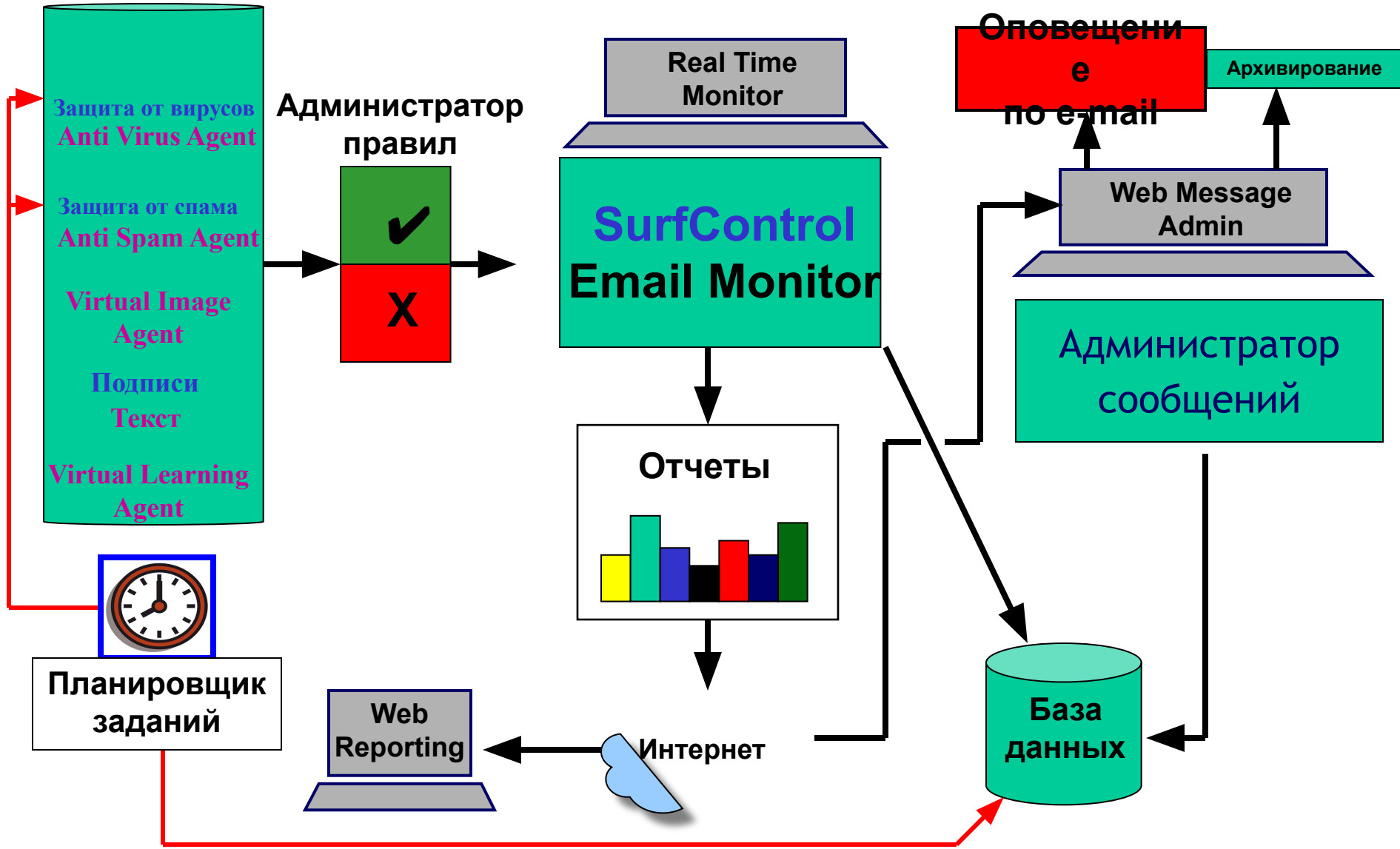
Save Changes **Cancel**

Done Internet

SurfControl E-mail Filter Обзор

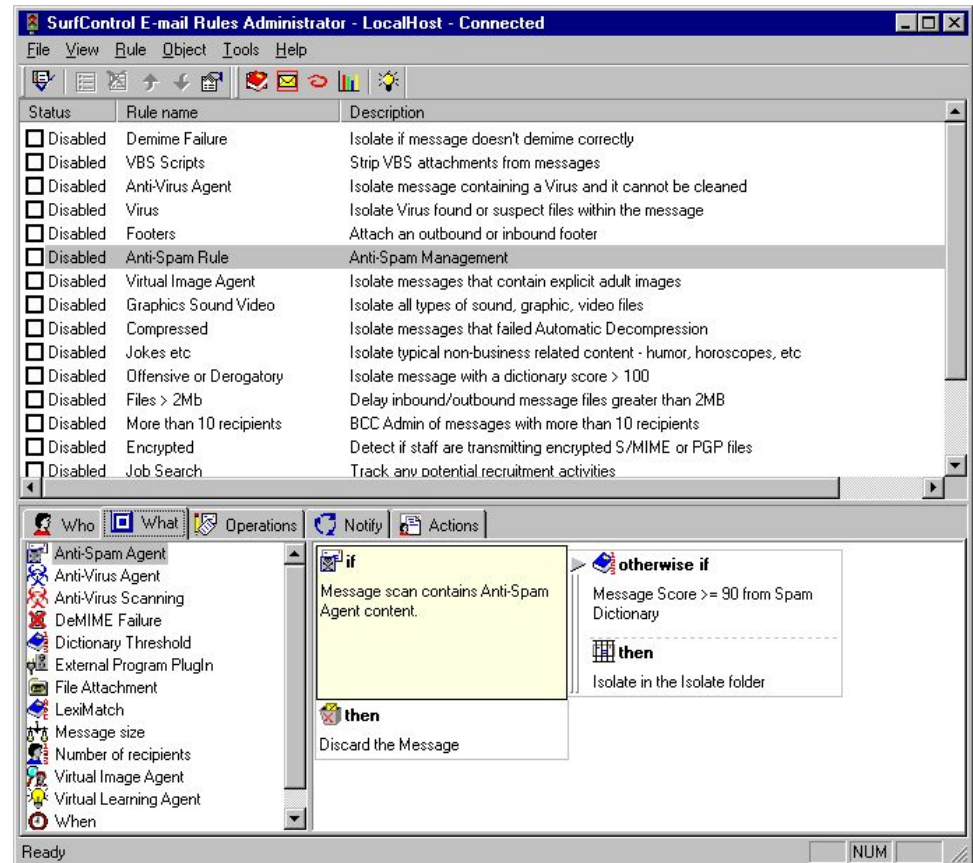


SurfControl Email Filter



Администратор правил E-Mail Filter

 Простота использования





The screenshot shows the SurfControl E-mail Rules Administrator interface. The main window displays a list of rules with columns for Status, Rule name, and Description. The 'Anti-Spam Rule' is highlighted. Below the list, there are tabs for 'Who', 'What', 'Operations', 'Notify', and 'Actions'. The 'What' tab is active, showing a rule configuration for 'Anti-Spam Agent'. The rule logic is defined as: 'if Message scan contains Anti-Spam Agent content. otherwise if Message Score >= 90 from Spam Dictionary. then Discard the Message. then Isolate in the Isolate folder'.

Status	Rule name	Description
<input type="checkbox"/> Disabled	Demime Failure	Isolate if message doesn't demime correctly
<input type="checkbox"/> Disabled	VBS Scripts	Strip VBS attachments from messages
<input type="checkbox"/> Disabled	Anti-Virus Agent	Isolate message containing a Virus and it cannot be cleaned
<input type="checkbox"/> Disabled	Virus	Isolate Virus found or suspect files within the message
<input type="checkbox"/> Disabled	Footers	Attach an outbound or inbound footer
<input type="checkbox"/> Disabled	Anti-Spam Rule	Anti-Spam Management
<input type="checkbox"/> Disabled	Virtual Image Agent	Isolate messages that contain explicit adult images
<input type="checkbox"/> Disabled	Graphics Sound Video	Isolate all types of sound, graphic, video files
<input type="checkbox"/> Disabled	Compressed	Isolate messages that failed Automatic Decompression
<input type="checkbox"/> Disabled	Jokes etc	Isolate typical non-business related content - humor, horoscopes, etc
<input type="checkbox"/> Disabled	Offensive or Derogatory	Isolate message with a dictionary score > 100
<input type="checkbox"/> Disabled	Files > 2Mb	Delay inbound/outbound message files greater than 2MB
<input type="checkbox"/> Disabled	More than 10 recipients	BCC Admin of messages with more than 10 recipients
<input type="checkbox"/> Disabled	Encrypted	Detect if staff are transmitting encrypted S/MIME or PGP files
<input type="checkbox"/> Disabled	Job Search	Track any potential recruitment activities

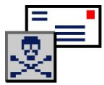
Правила



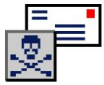
Anti Virus Agent

-  Использует технологию McAfee.
-  Максимальная защита против вирусов в e-mail

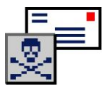
Anti-Spam Agent



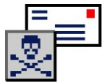
Фильтрация спама на сетевом шлюзе.



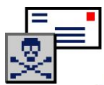
Увеличение скорости работы сети и почтового сервера.



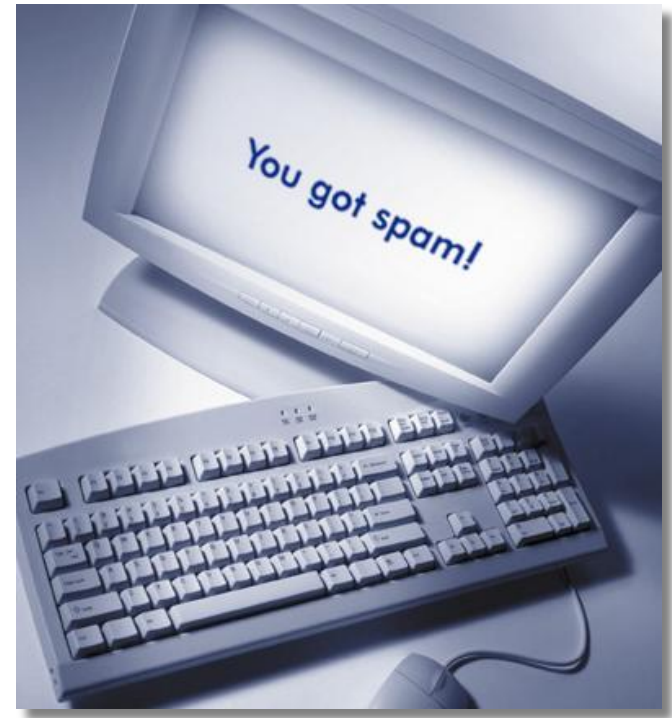
Минимизирует влияние спама на производительность.



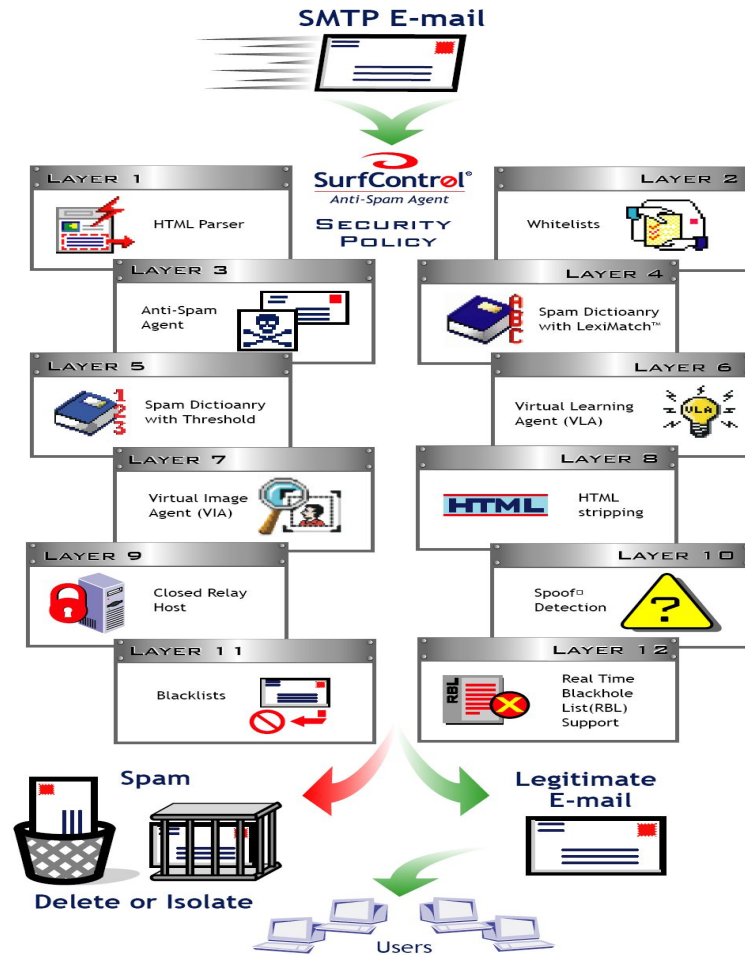
Максимизирует безопасность.



100% точность.



12 уровней защиты от спама



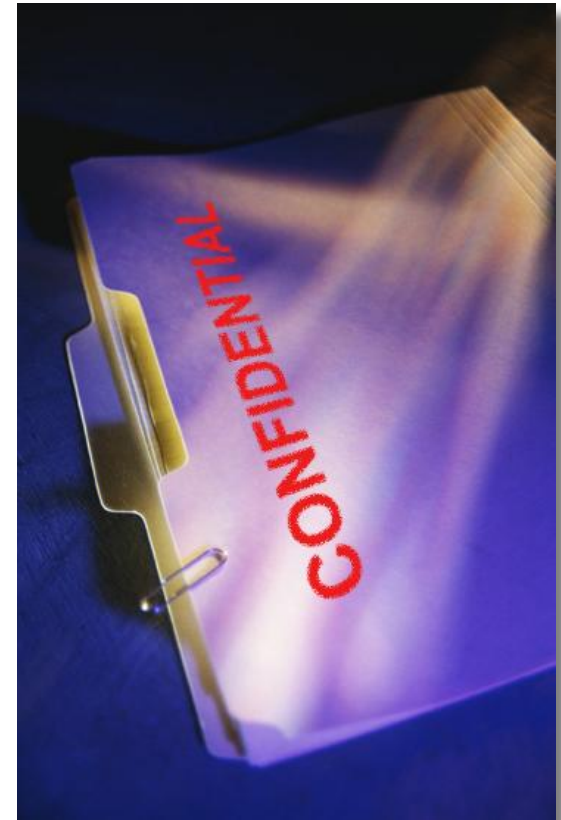
Virtual Learning Agent



Защищает от утечки
конфиденциальной
информации.



Обучается на основе
документов пользователя.



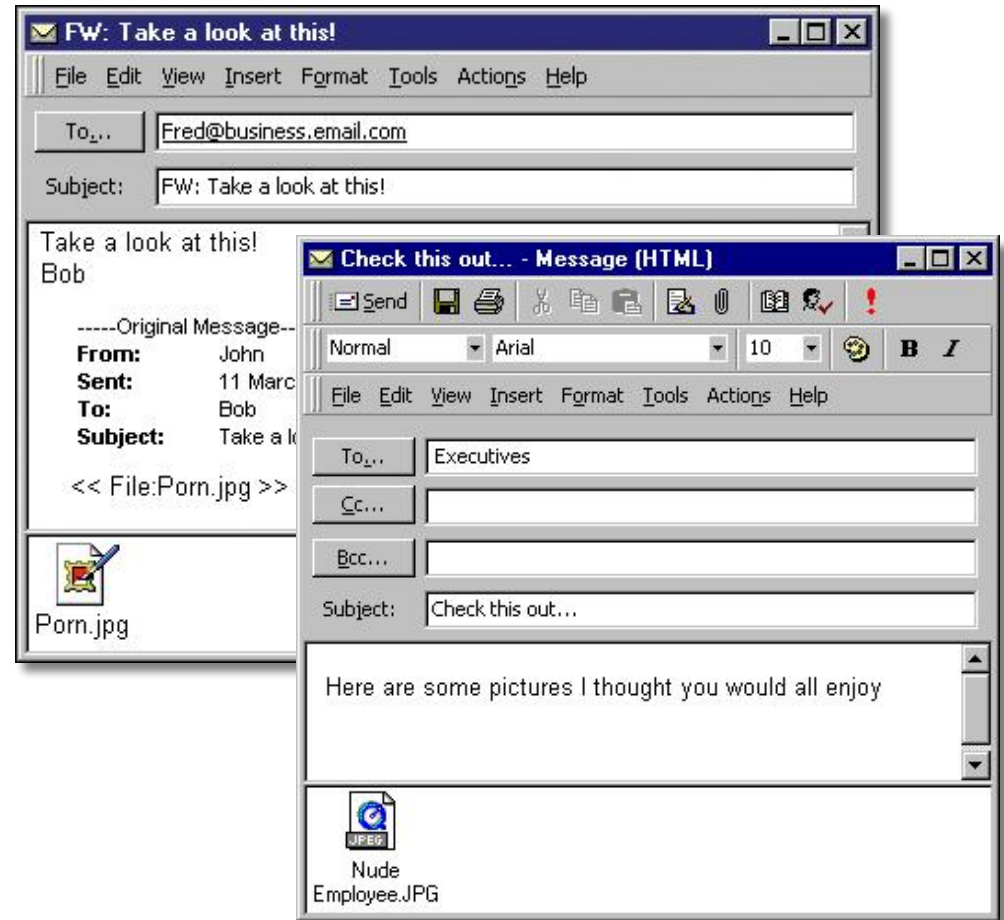
Virtual Image Agent



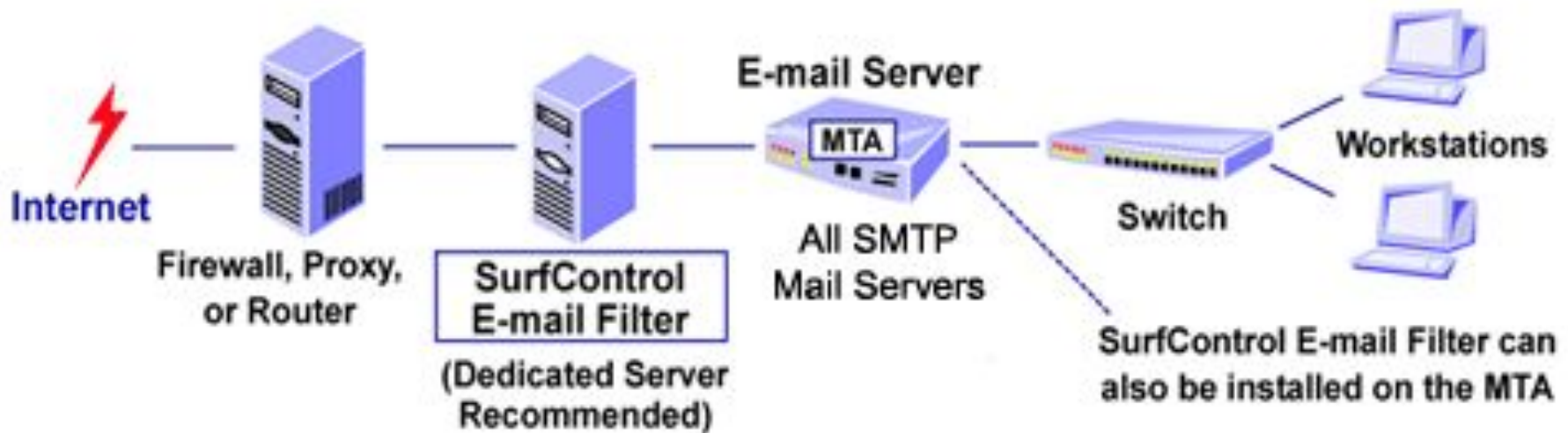
Удаляет эротические фотографии из e-mail



Использует искусственный интеллект



Конфигурация сети



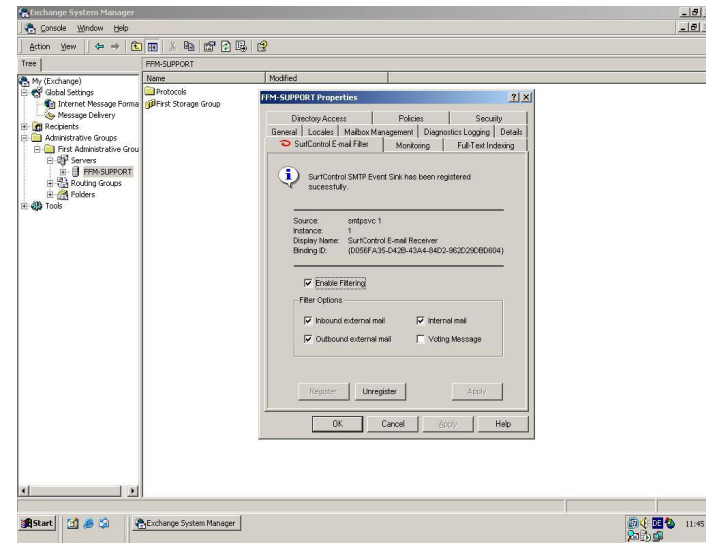
Сканируются входящие и исходящие сообщения по e-mail (SMTP)

SurfControl E-mail Filter для Exchange



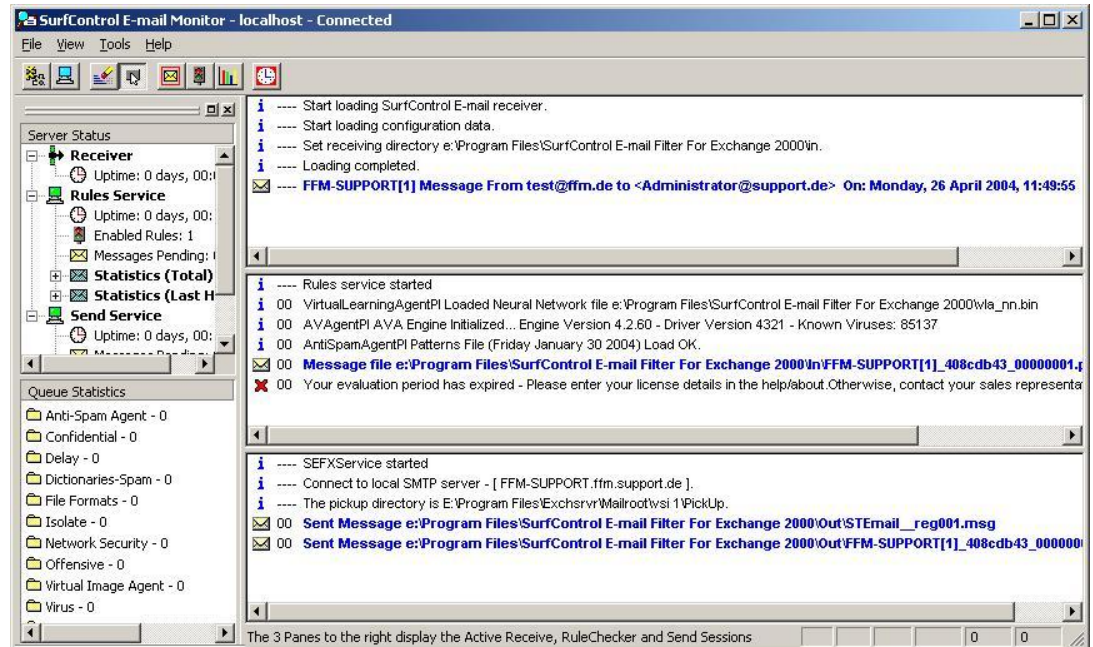
MS Exchange - SEF Plug-In

- Дополняет стандартные фильтры MS Exchange
- Пользователь сам выбирает, какие письма проверяются e-mail фильтром



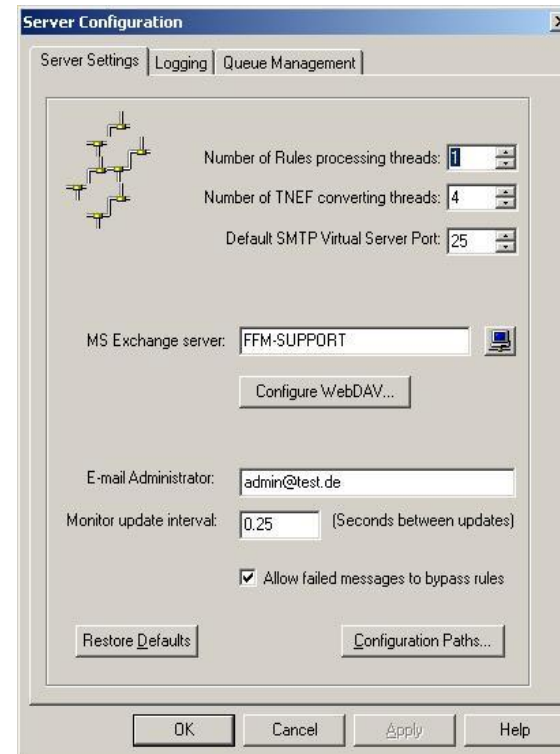
E-mail Filter Monitor

- Возможность слежения за потоком сообщений



Настройка сервера

- Настройка взаимодействия с Exchange
- Использование WebDAV



Системные требования

	SurfControl E-Mail Filter SMTP	SurfControl E-Mail Filter MS Exchange 2000/2003
Процессор	Pentium III 600 MHz	Pentium III 600 MHz
Оперативная память	Минимум 512 МВ	Минимум 512 МВ
Свободное место на диске	1 GB	1 GB
Приложение	Почтовая система	MS Exchange 2000/2003
Операционная система	Win2000 Server SP3 Win2000 AS SP3 Windows 2003	Win2000 Server SP3 Win2000 AS SP2 Windows 2003

*Спасибо за
ВНИМАНИЕ*



Enterprise Threat Shield
RiskFilter
Adaptive Threat Intelligence
E-mail Filter
Web Filter