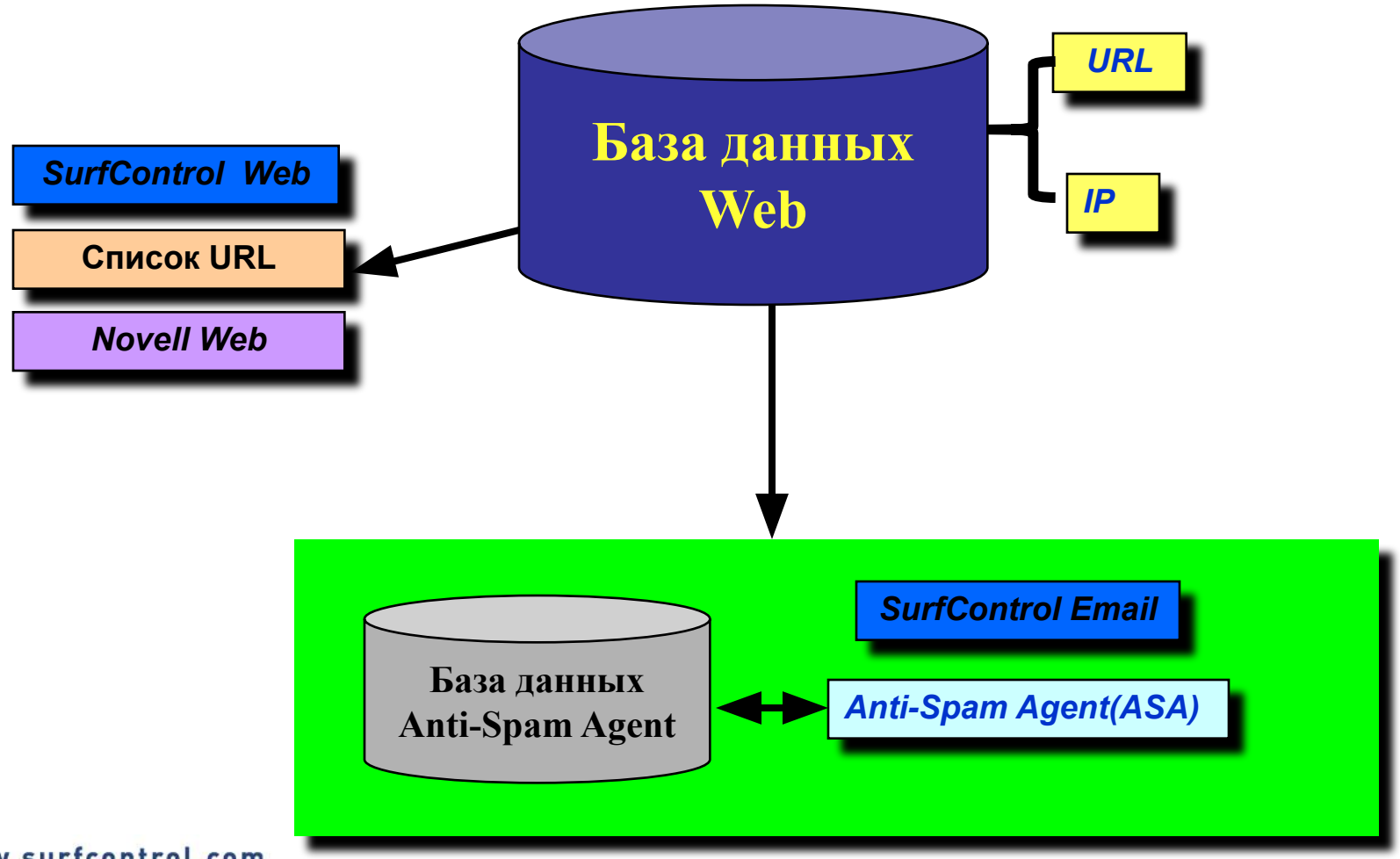
SurfControl®
Enterprise Threat Protection

Техническая информация о продуктах SurfControl

SurfControl®
Enterprise Threat Protection

Базы данных SurfControl



SurfControl®
Enterprise Threat Protection

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**

SurfControl®
Enterprise Threat Protection

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

SurfControl®
Enterprise Threat Protection

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

SurfControl®
Enterprise Threat Protection

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 спамерров

Пользователь может добавлять собственные категории и ключевые слова

SurfControl®
Enterprise Threat Protection

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

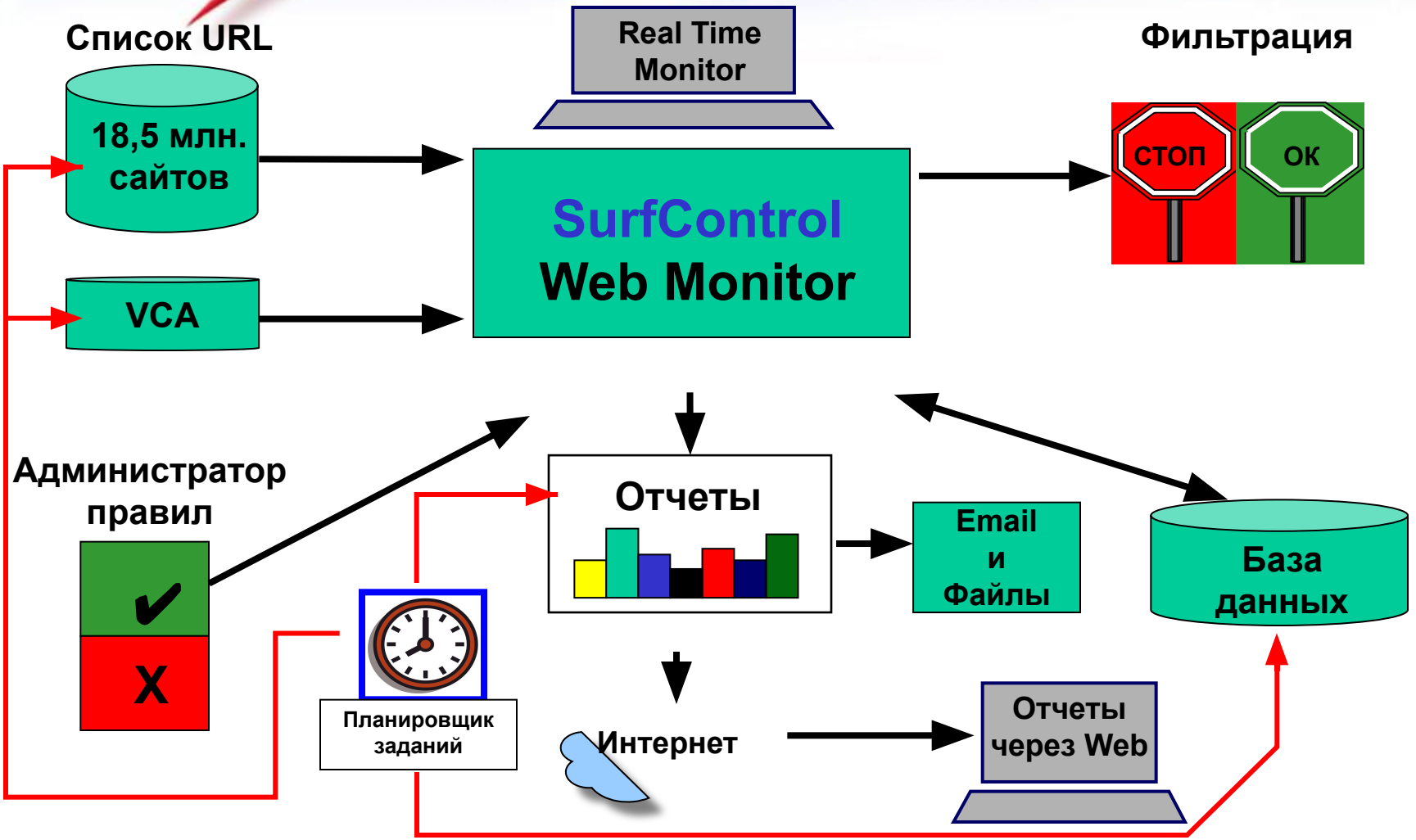
SurfControl® Virtual Learning Agent

SurfControl®
Enterprise Threat Protection

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

SurfControl
Enterprise Threat Protection

SurfControl Web Filter



SurfControl®
Enterprise Threat Protection

Технология

PASS – BY

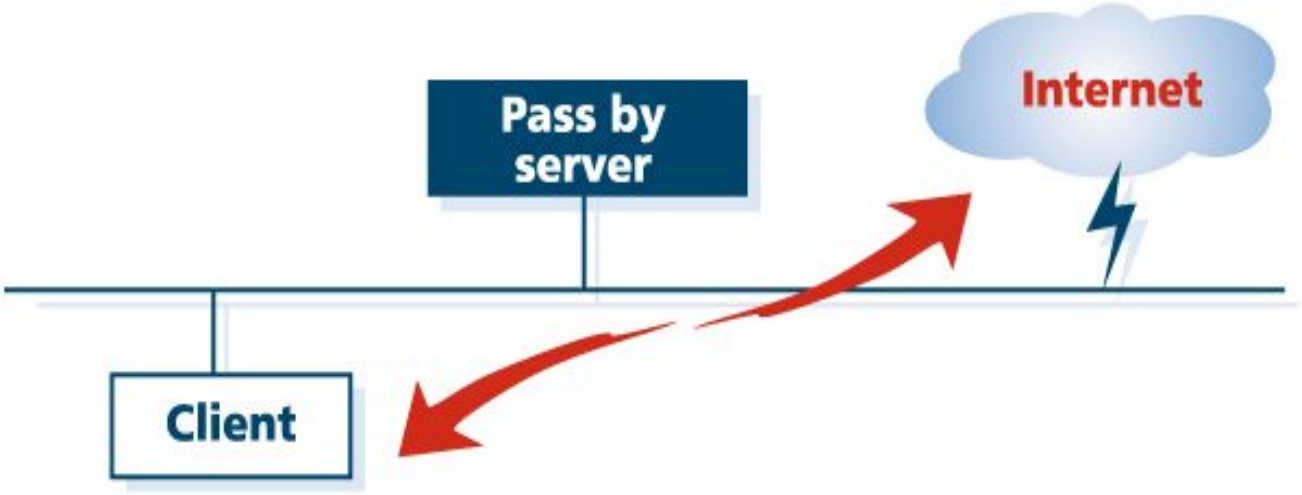
MS Windows 2000/2003

• PASS - THRU

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

SurfControl®
Enterprise Threat Protection

Версия для Windows (Технология Pass-By)

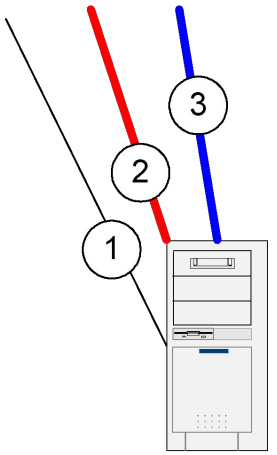


- Использует технологию сниффера
- Не влияет на производительность сети
- Может следить за всеми протоколами, не только за HTTP
- Должен видеть весь трафик в сети

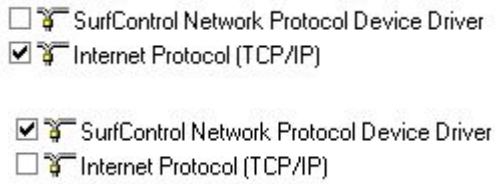
SurfControl
Enterprise Threat Protection

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.



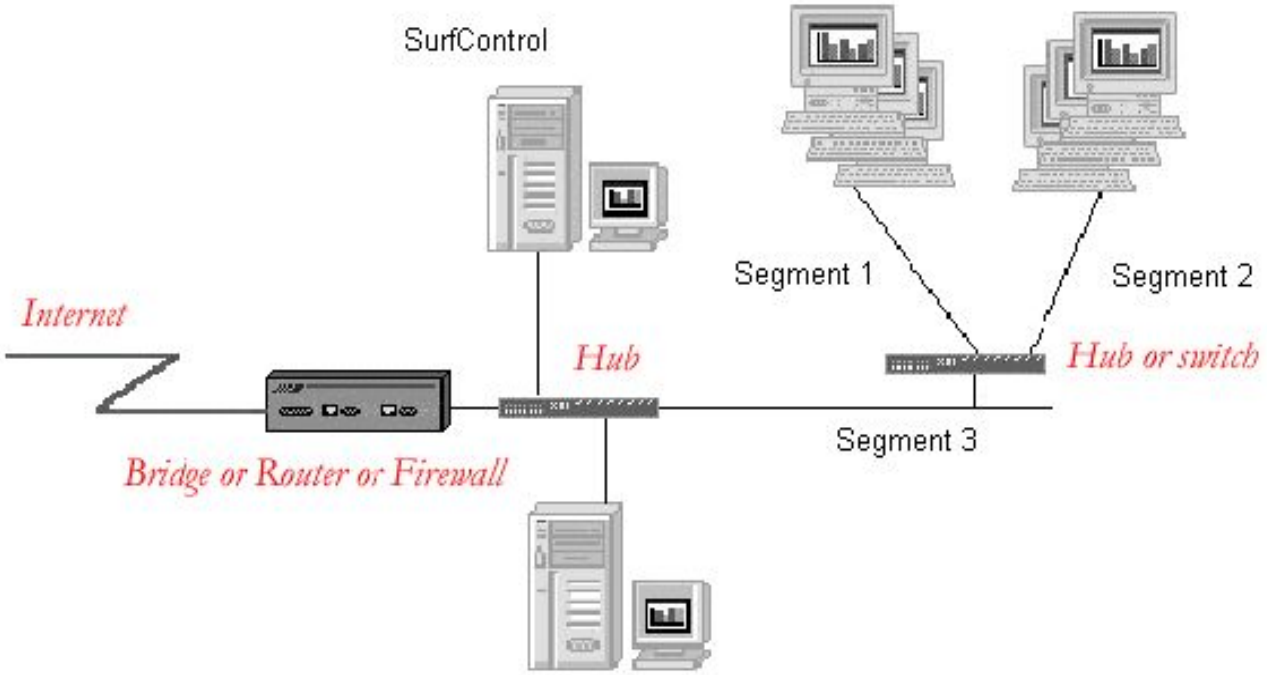
SurfControl Web Filter
for Windows



SurfControl®
Enterprise Threat Protection

SurfControl Web Filter

- **Пример конфигурации сети:**



SurfControl
Enterprise Threat Protection

SurfControl Web Filter

Surfcontrol анализирует пакет данных

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

SurfControl

Fin

Сайт должен быть заблокирован, клиенту отправляется команда FIN

Fin

Сообщение от www.playboy.com: Доступ заблокирован surfCONTROL

Закрыть соединение (FIN)

Fin

Компьютер клиента: 192.168.0.1

Запрос в Интернет: www.playboy.com

Hub

Fin

Router

Fin

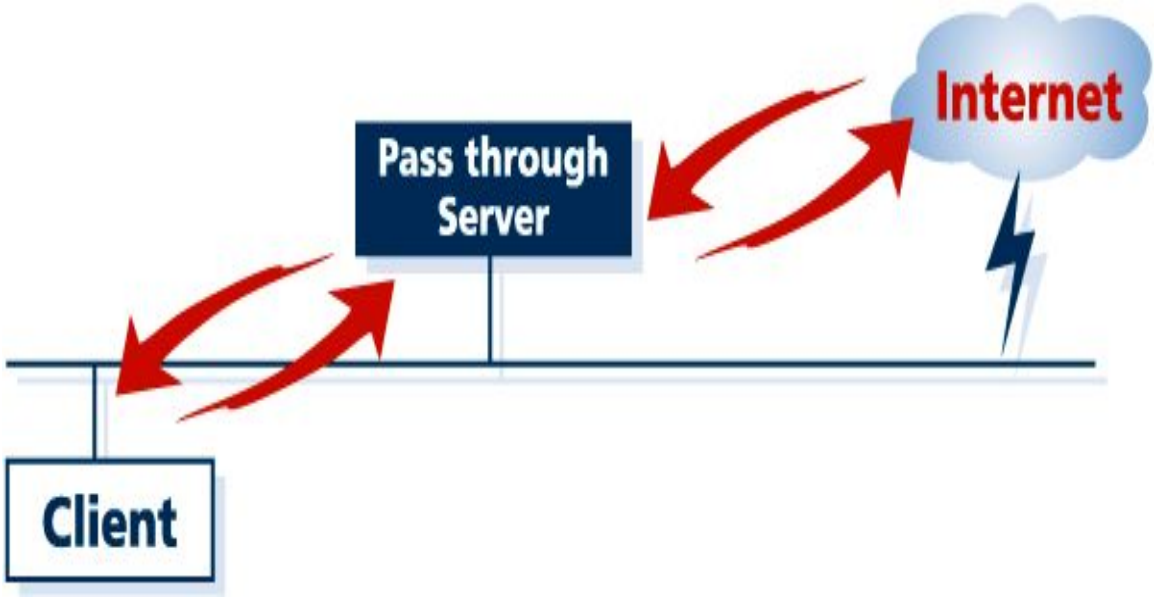
Сообщение от 192.168.0.1

Сбросить соединение (FIN/RST)

Веб-сервер Playboy.com

SurfControl®
Enterprise Threat Protection

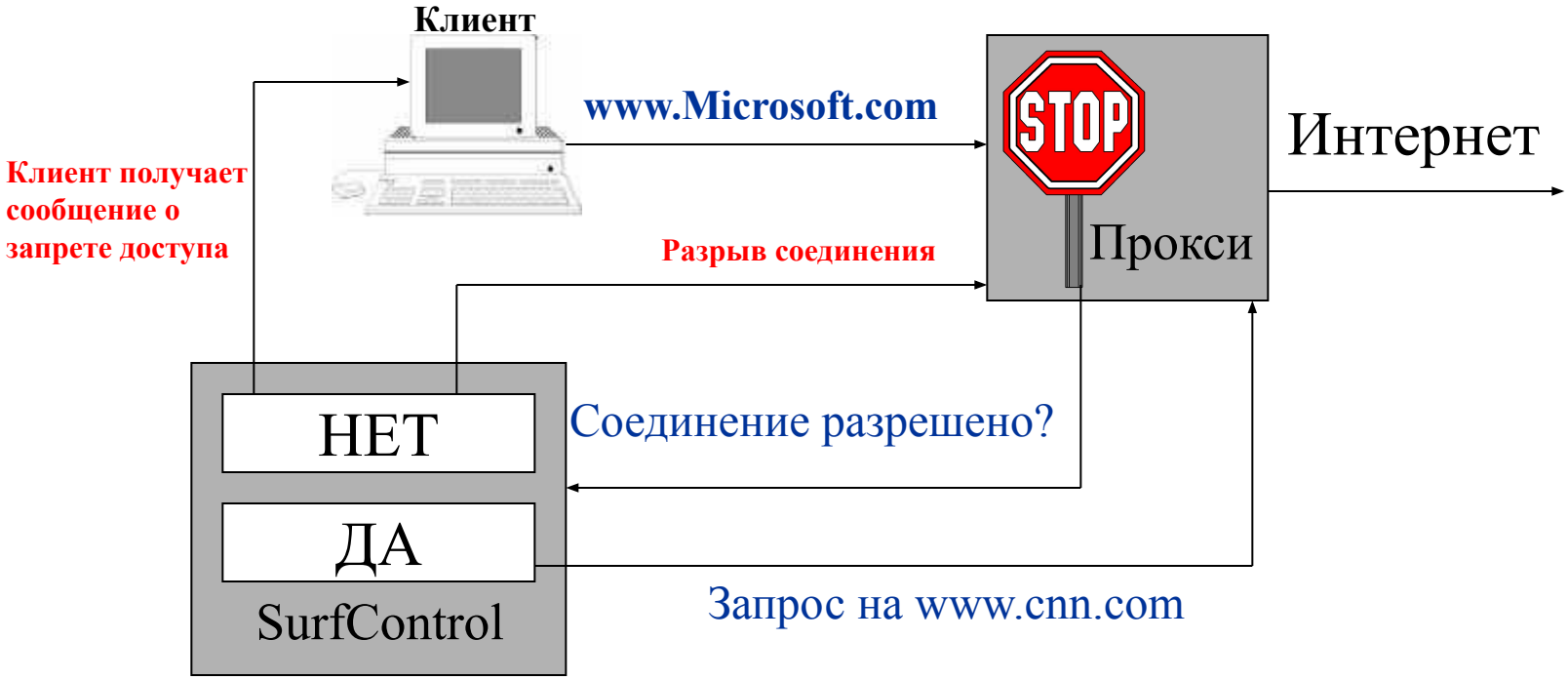
SurfControl Web для шлюзов (Технология pass-through)



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

SurfControl®
Enterprise Threat Protection

SurfControl Web Filter для шлюзов



SurfControl®
Enterprise Threat Protection

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

SurfControl®
Enterprise Threat Protection

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

SurfControl®
Enterprise Threat Protection

Дополнительные средства SurfControl Web Filter

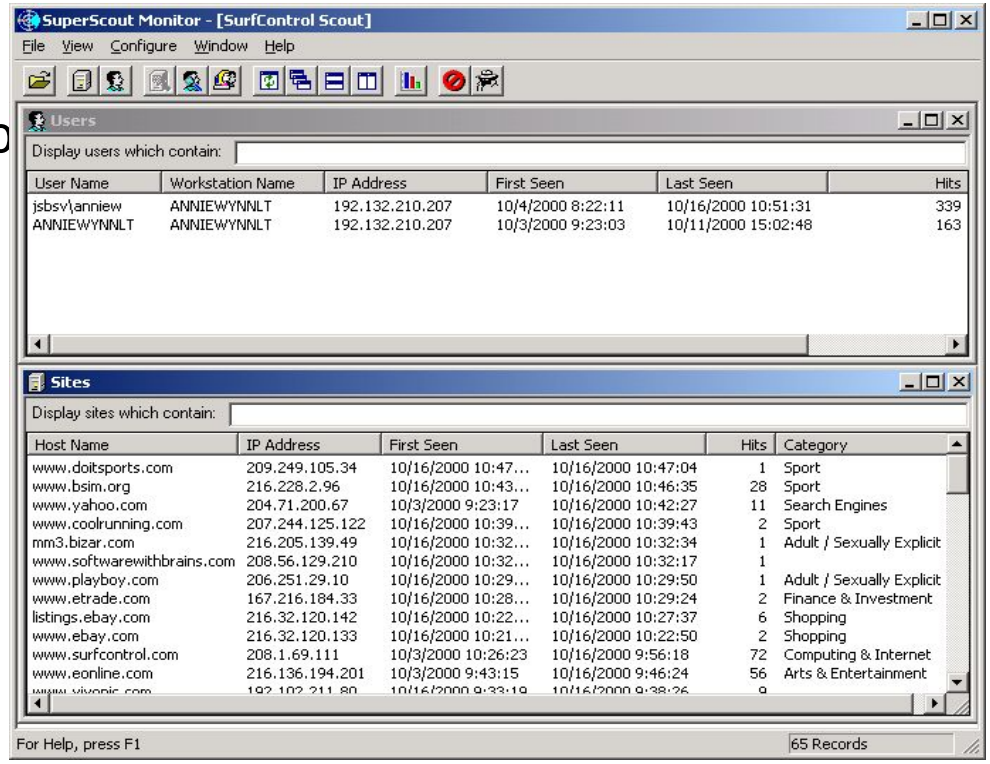
SurfControl®
Enterprise Threat Protection

SurfControl Monitor

- Показывает информацию по:

Пользователю

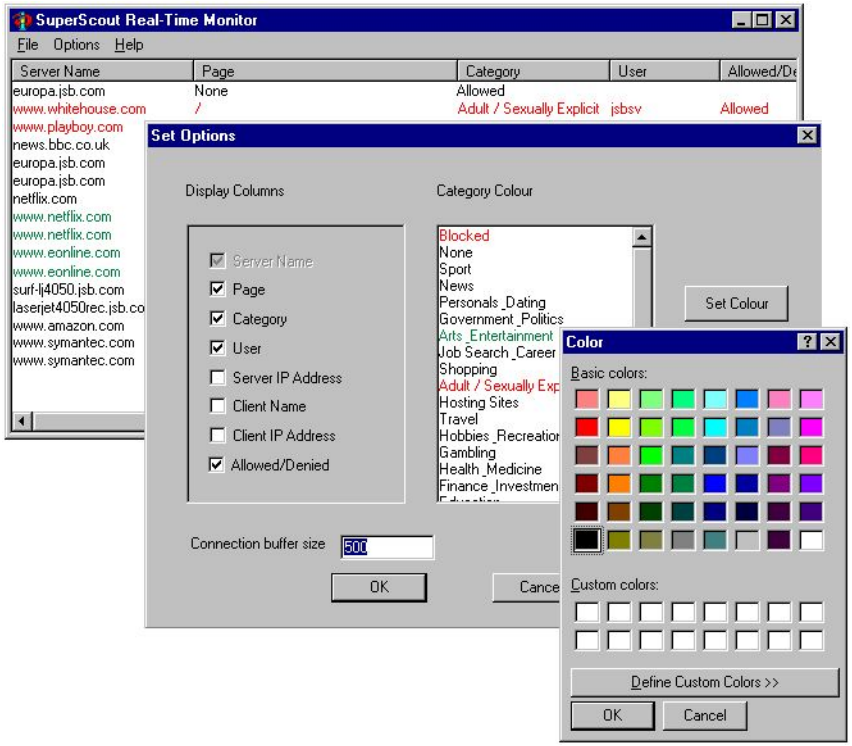
Сайту



SurfControl®
Enterprise Threat Protection

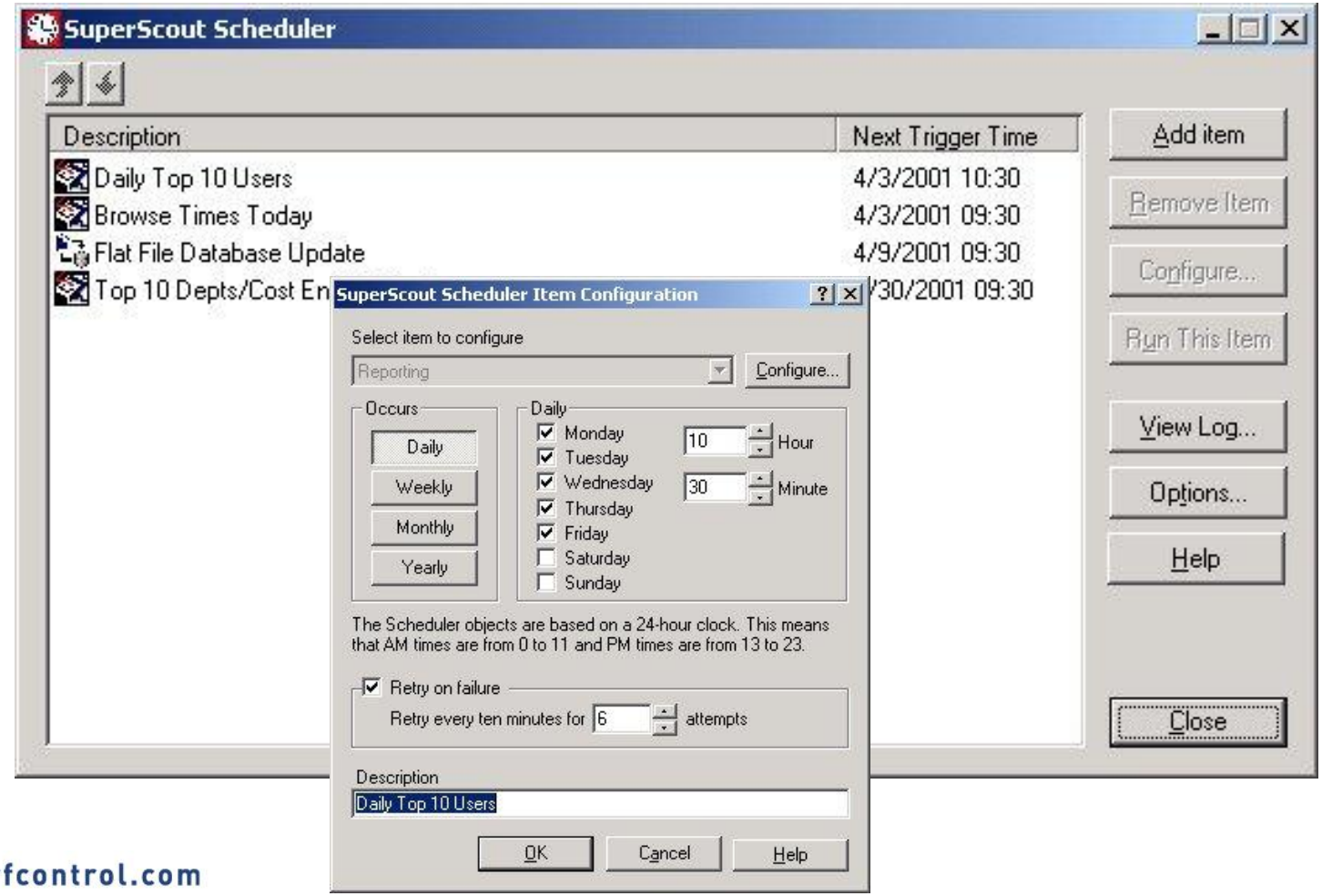
Real-Time Monitor

- Цветовое выделение для наглядности



SurfControl®
Enterprise Threat Protection

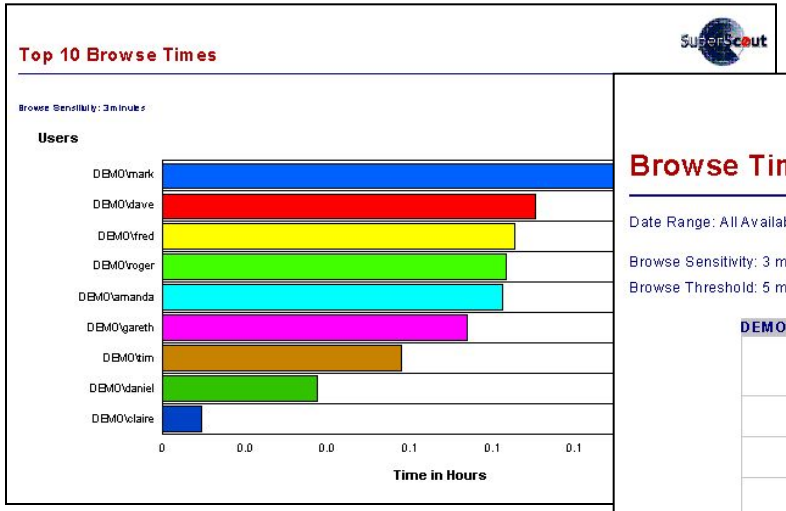
Гибкий планировщик заданий

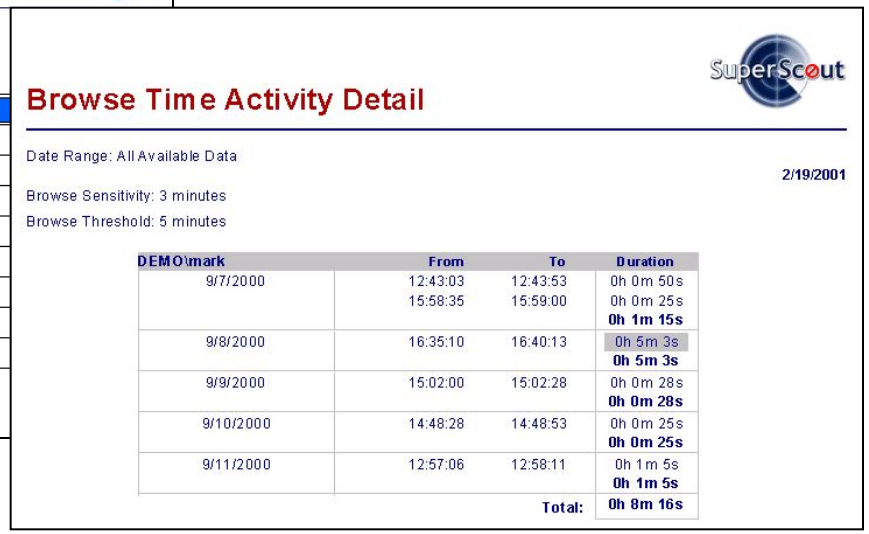


SurfControl®
Enterprise Threat Protection

Создание отчетов

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





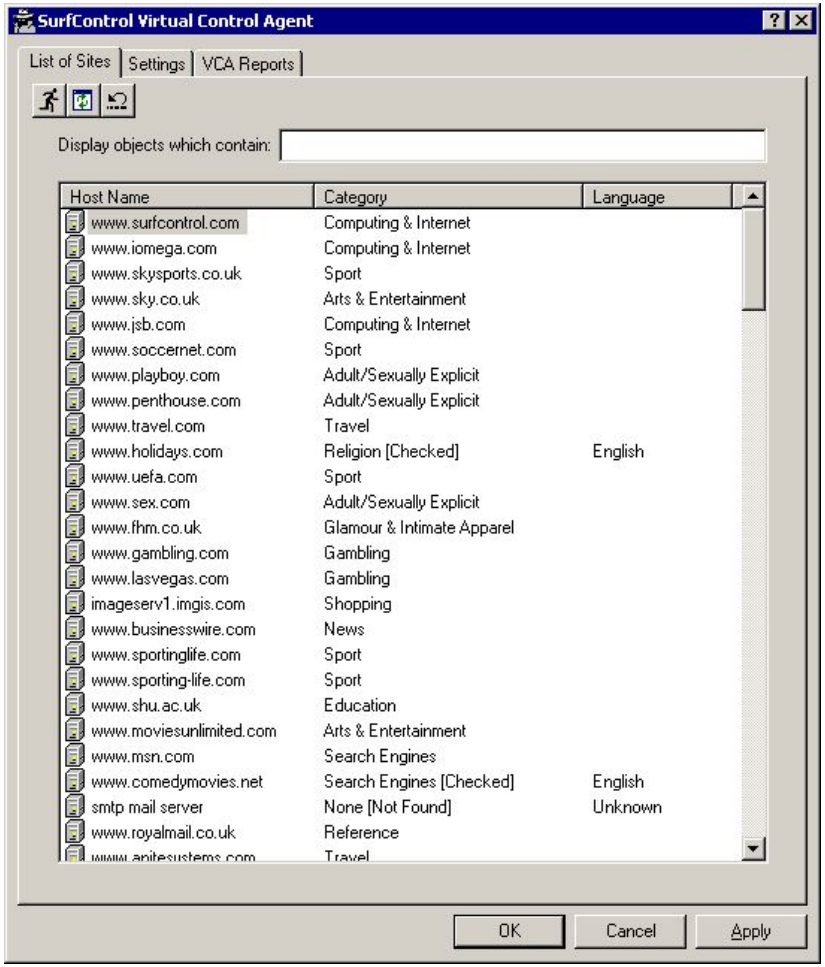
SurfControl®
Enterprise Threat Protection

SurfControl Web Filter
Virtual Control Agent

SurfControl®
Enterprise Threat Protection

Virtual Control Agent

- Использует нейронные сети
- Автоматически категоризует новые сайты
- Распределяет сайты по категориям SurfControl



SurfControl®
Enterprise Threat Protection

SurfControl Web Filter Border Manager
Обзор

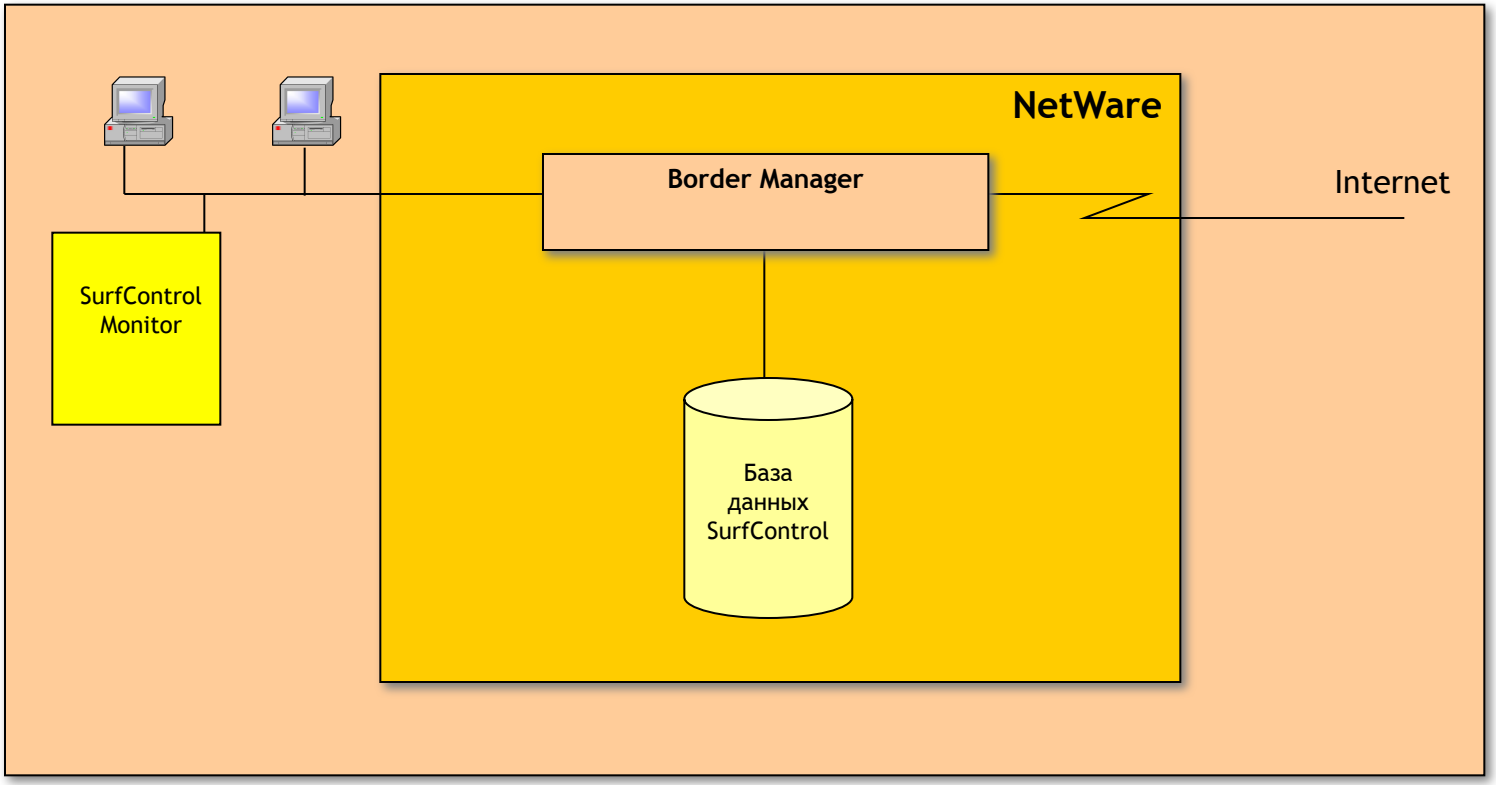
SurfControl®
Enterprise Threat Protection

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

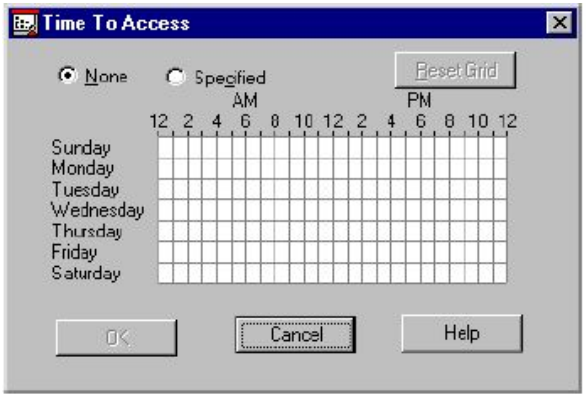
SurfControl®
Enterprise Threat Protection

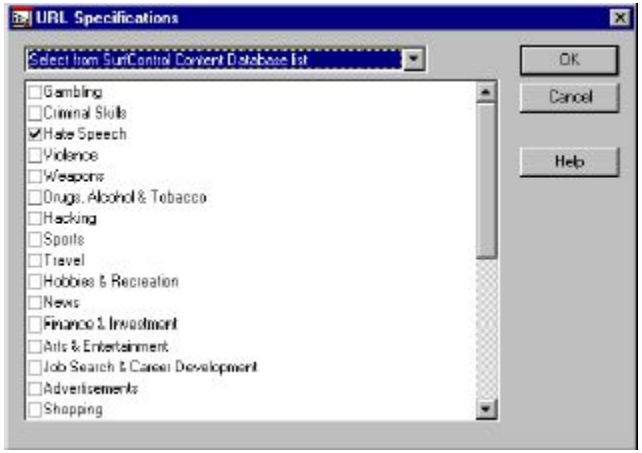
Архитектура сети



SurfControl®
Enterprise Threat Protection

Настройка





SurfControl®
Enterprise Threat Protection

SurfControl FireWall-1
Обзор

SurfControl
Enterprise Threat Protection

Компоненты

Linux
Windows

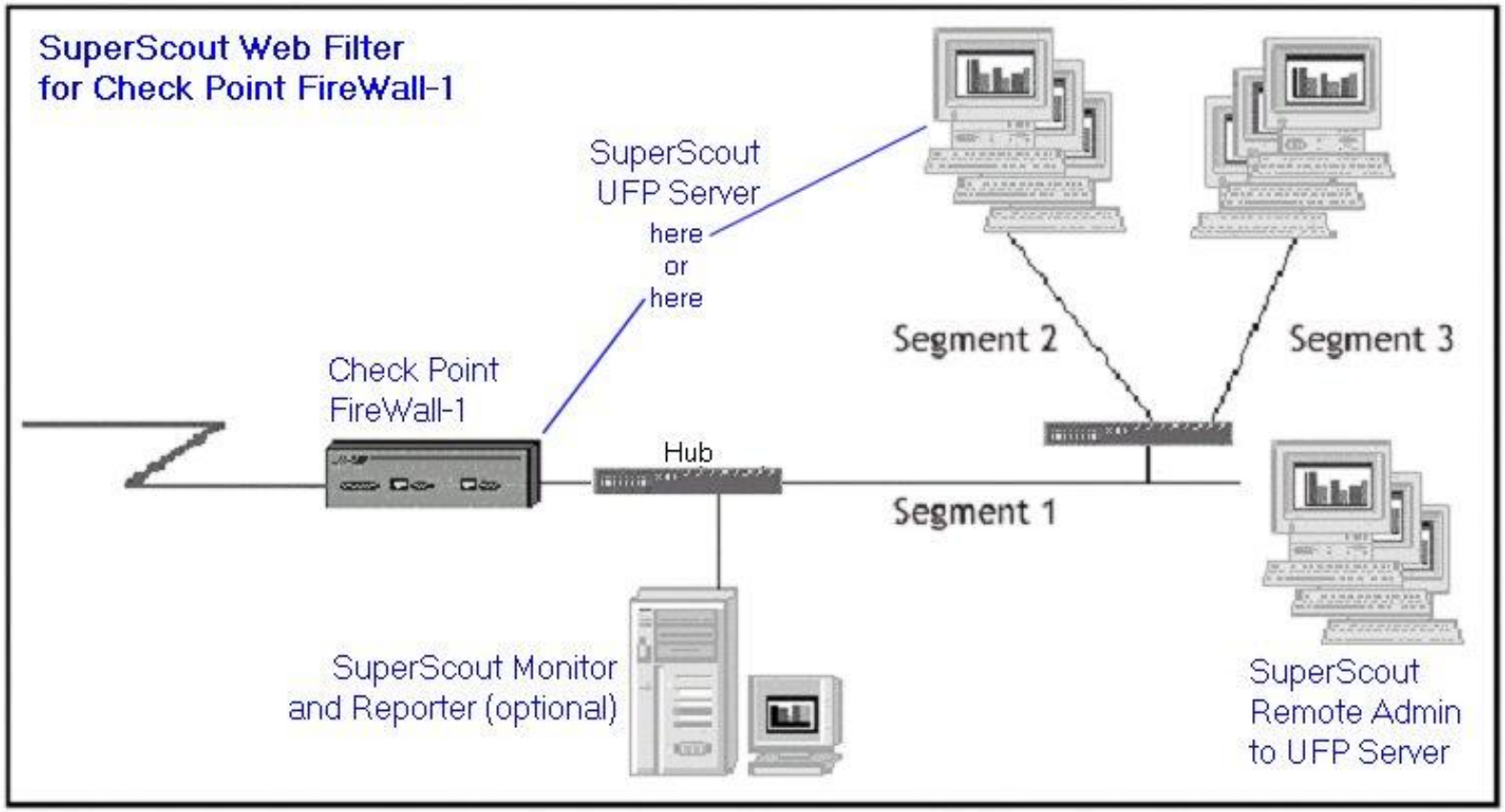
- SurfControl UFP Server
  - Протокол UFP
  - Блокировка на основе URL

Windows

- SurfControl Monitor and Reporter
  (опционально)
  - Мониторинг
    - По пользователям и по сайтам
    - Real-Time Monitor
  - Отчеты
    - Более 50 отчетов

SurfControl®
Enterprise Threat Protection

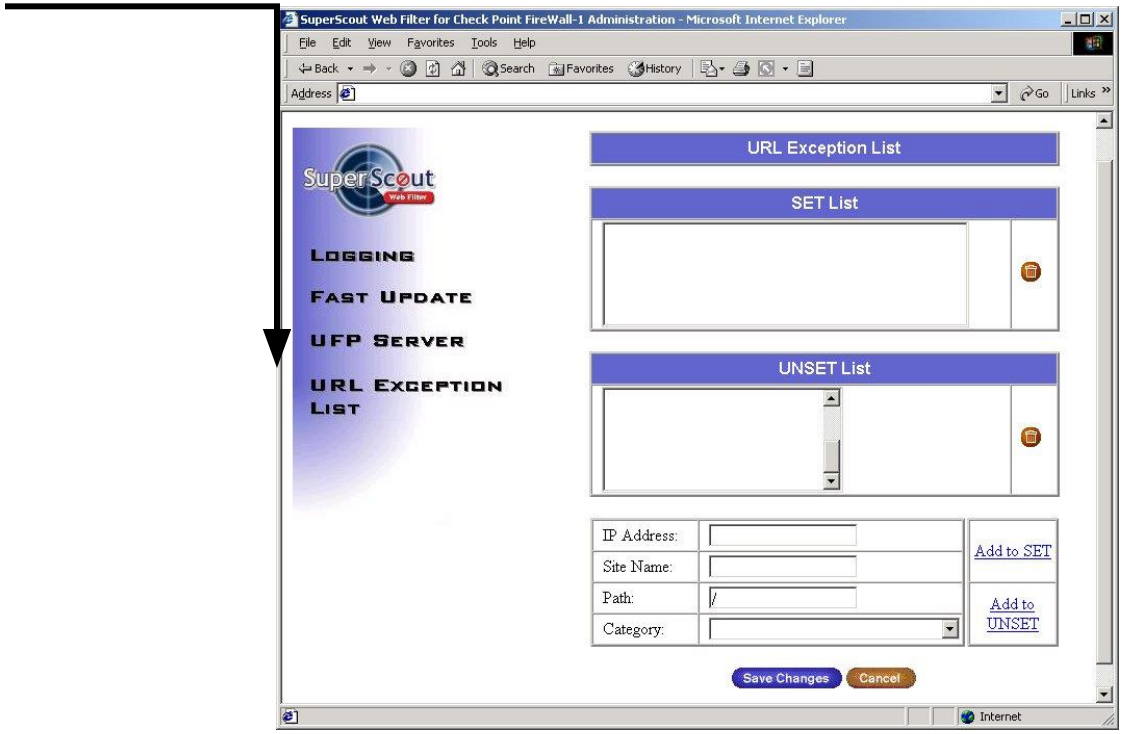
Конфигурация сети



SurfControl®
Enterprise Threat Protection

SurfControl UFP Server

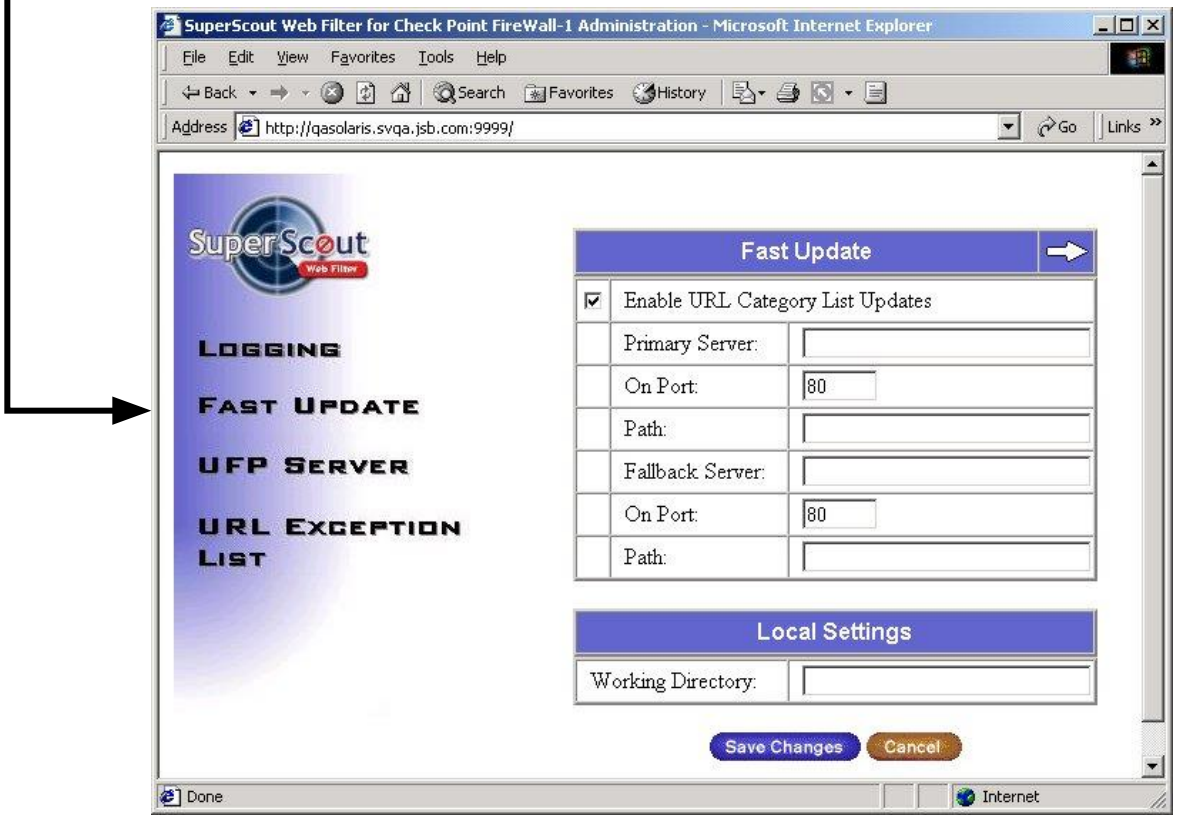
- Удаленное администрирование через браузер



SurfControl®
Enterprise Threat Protection

SurfControl UFP Server

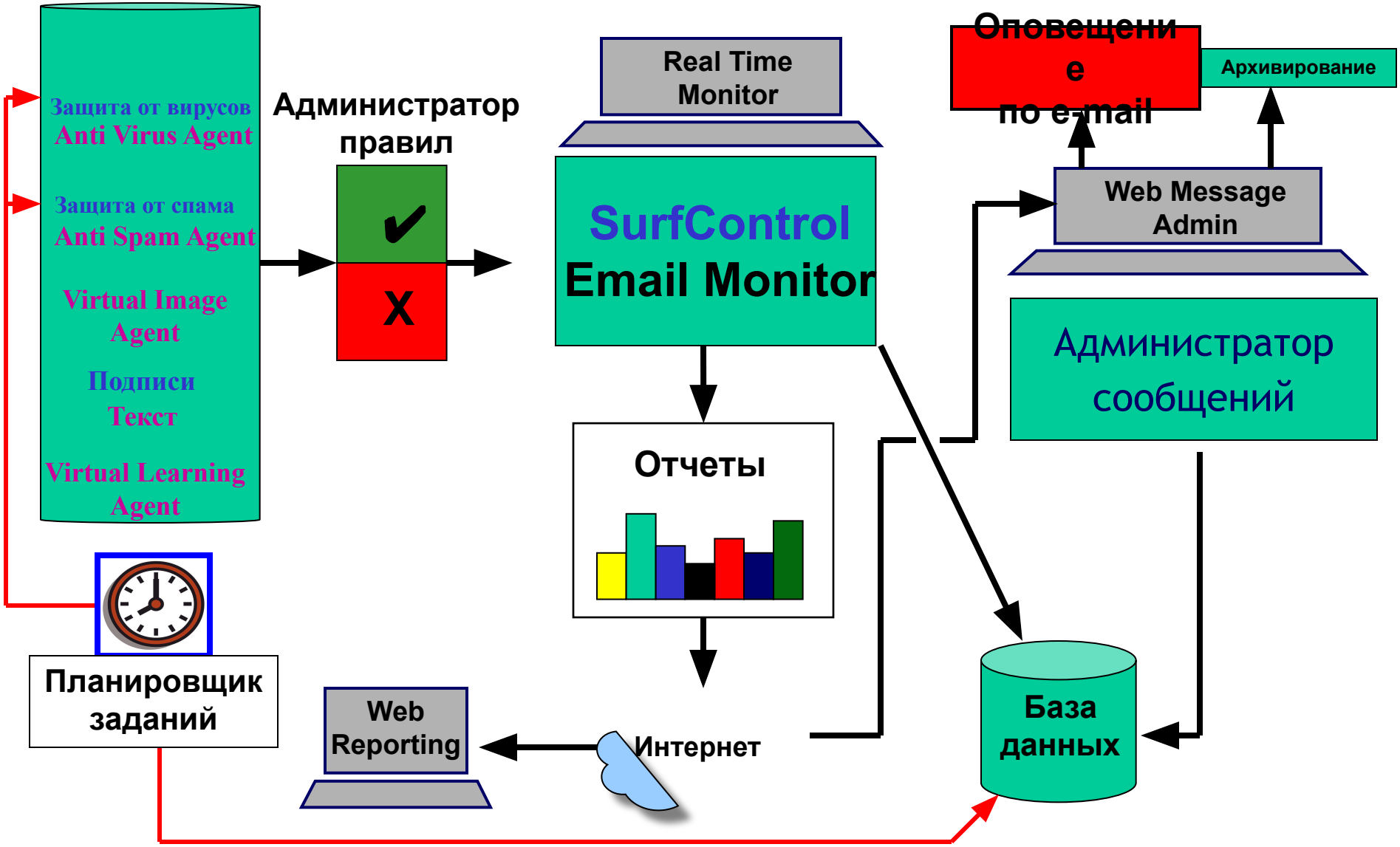
- Обновление базы данных по расписанию



SurfControl®
Enterprise Threat Protection

SurfControl E-mail Filter
Обзор

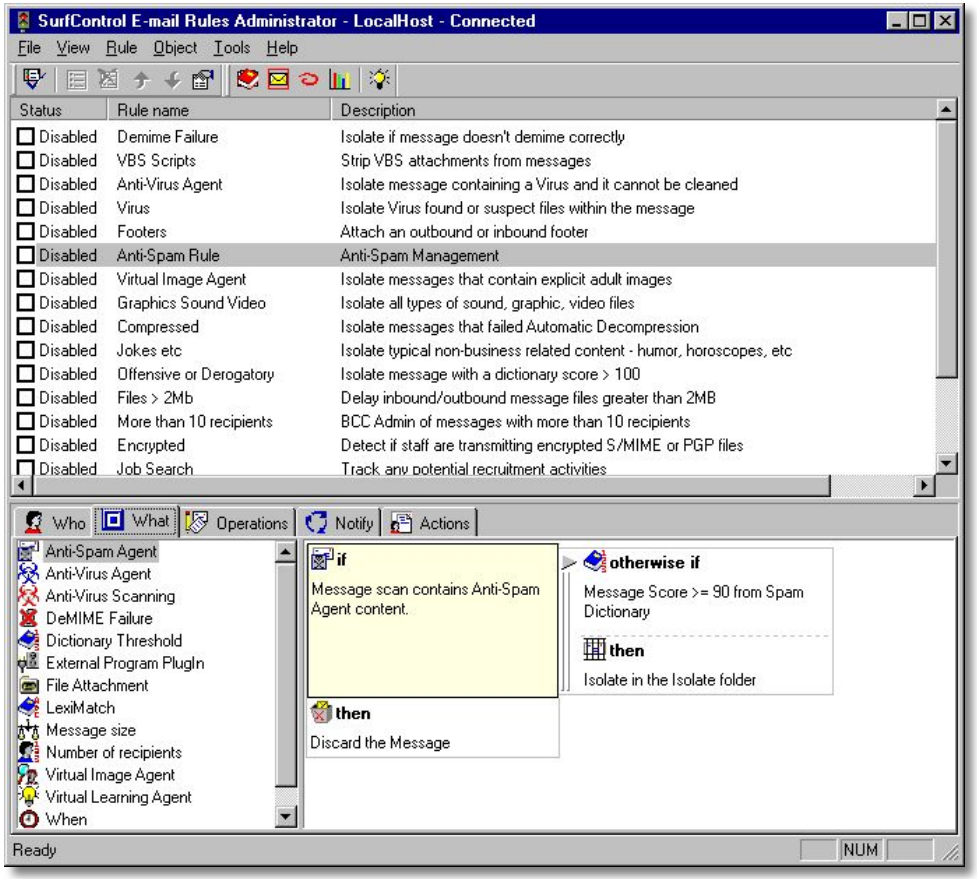
SurfControl Email Filter



SurfControl®
Enterprise Threat Protection

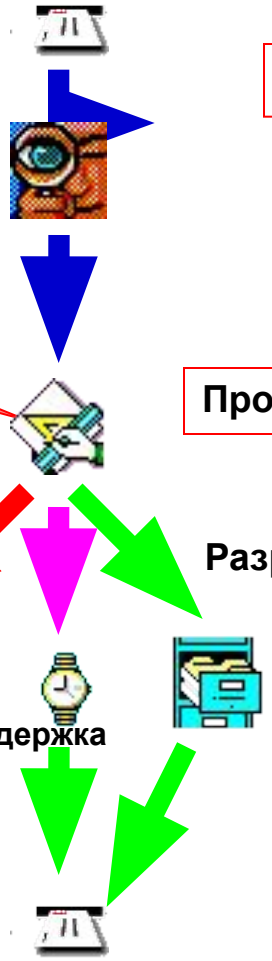
Администратор правил E-Mail Filter

- Простота использования



SurfControl®
Enterprise Threat Protection

Правила



E-Mail помещается во входную очередь

Проверка на соответствие правилам

Разрешить

E-Mail располагается в очереди на отправку

Задержка

Изоляция

Удаление

Добавляется автоматическая подпись

SurfControl®
Enterprise Threat Protection

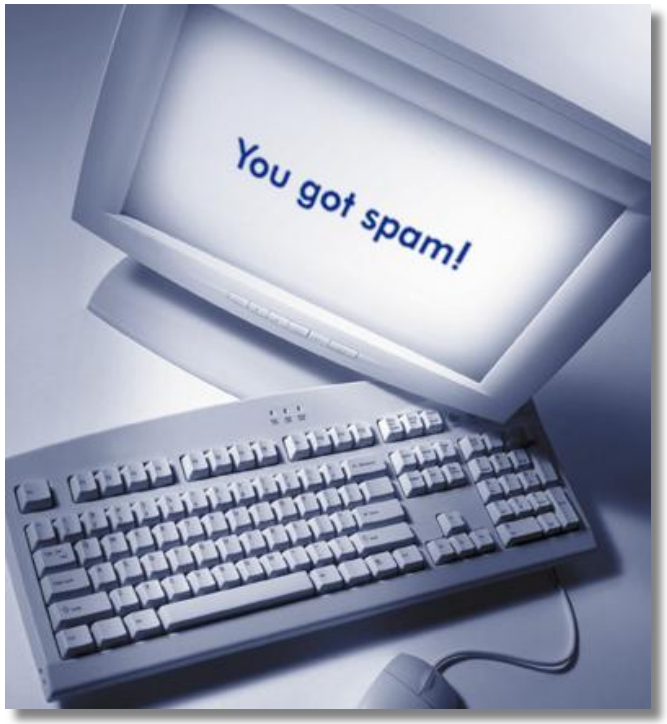
Anti Virus Agent

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

SurfControl®
Enterprise Threat Protection

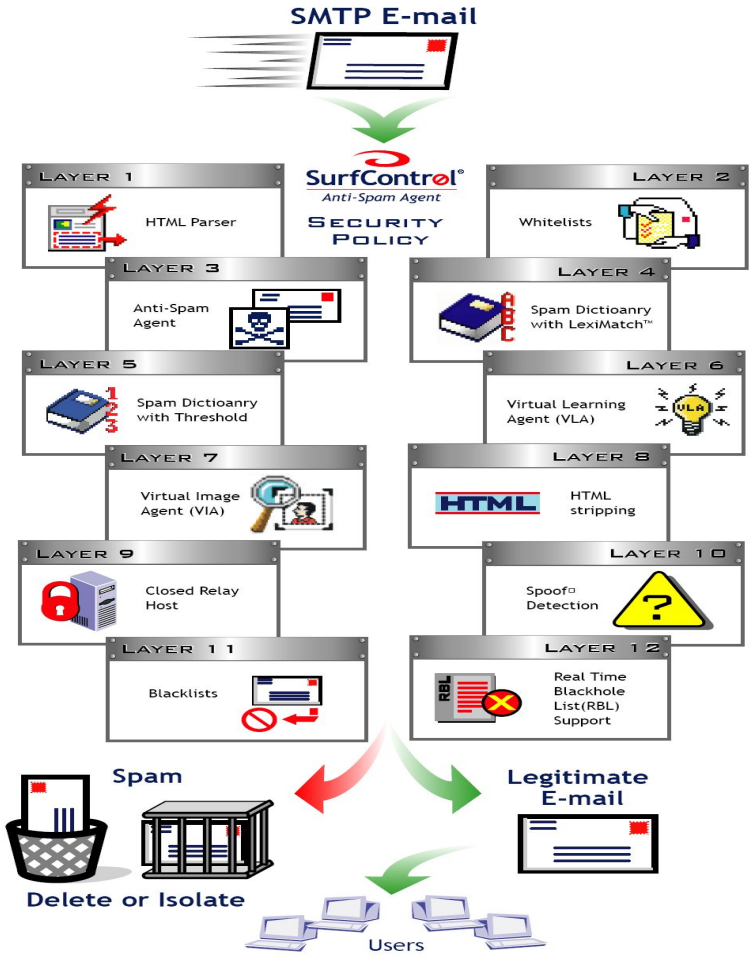
Anti-Spam Agent

- Фильтрация спама на сетевом шлюзе.
- Увеличение скорости работы сети и почтового сервера.
- Минимизирует влияние спама на производительность.
- Максимизирует безопасность.
- 100% точность.



SurfControl®
Enterprise Threat Protection

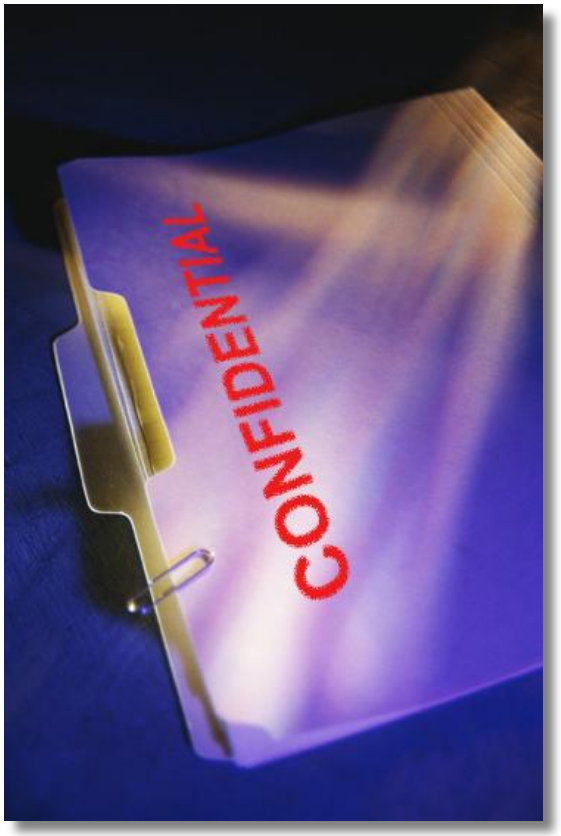
12 уровней защиты от спама



SurfControl®
Enterprise Threat Protection

Virtual Learning Agent

- Защищает от утечки конфиденциальной информации.

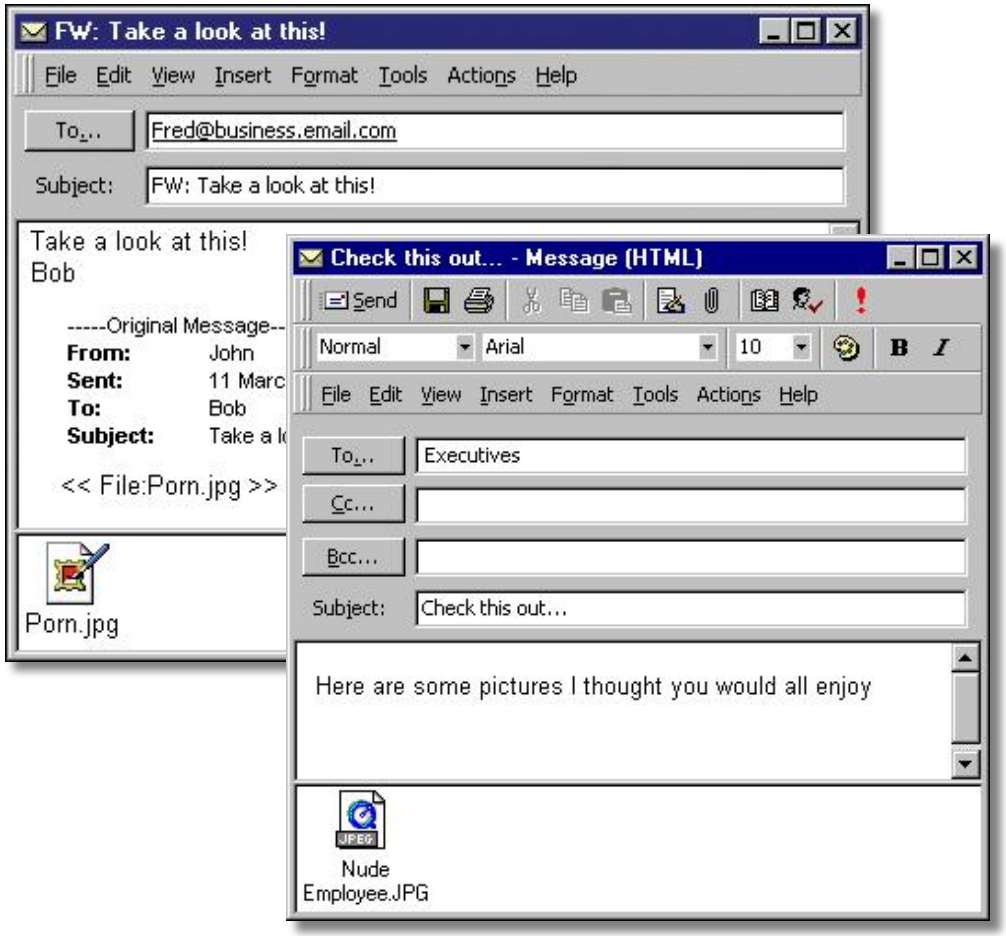


- Обучается на основе документов пользователя.

SurfControl®
Enterprise Threat Protection

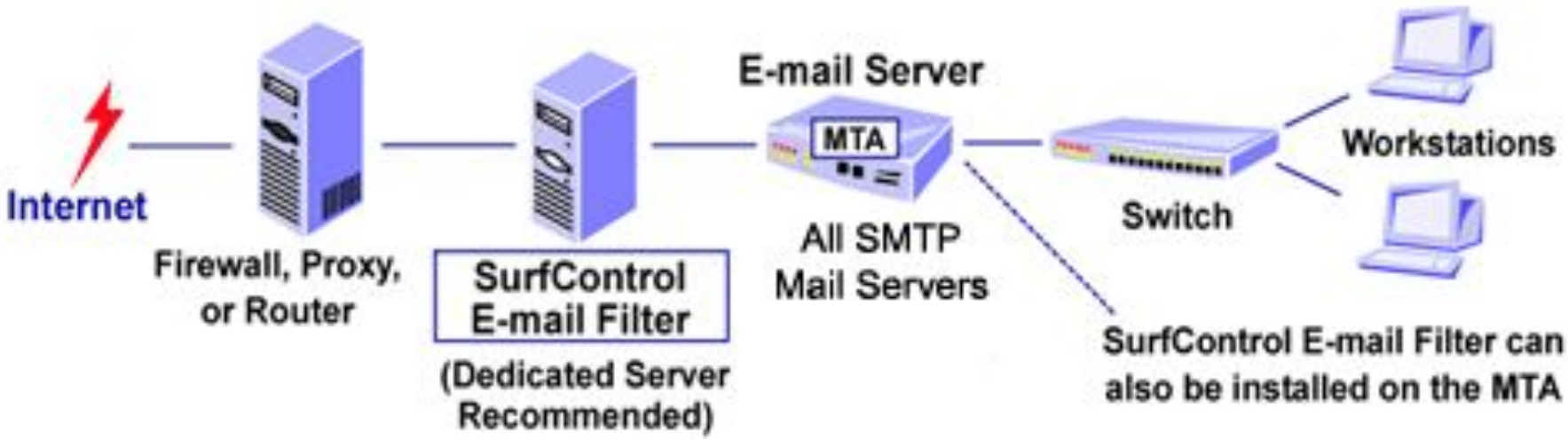
Virtual Image Agent

- Удаляет эротические фотографии из e-mail
- Использует искусственный интеллект



SurfControl®
Enterprise Threat Protection

Конфигурация сети



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

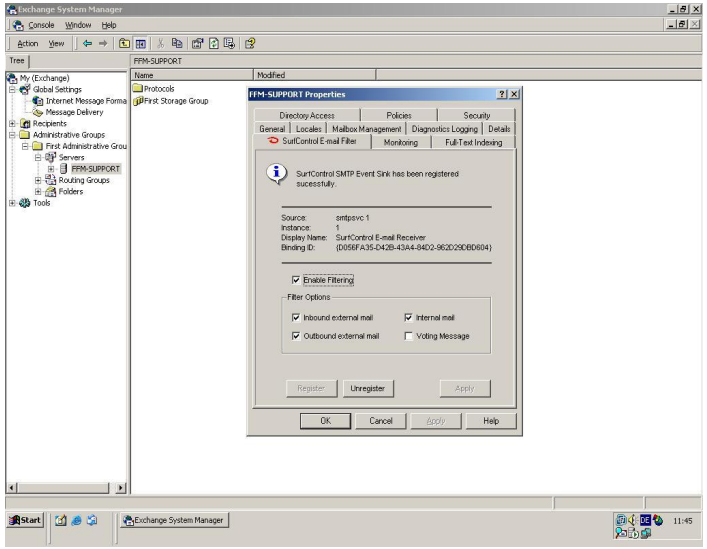
SurfControl®
Enterprise Threat Protection

SurfControl E-mail Filter для Exchange

SurfControl®
Enterprise Threat Protection

MS Exchange - SEF Plug-In

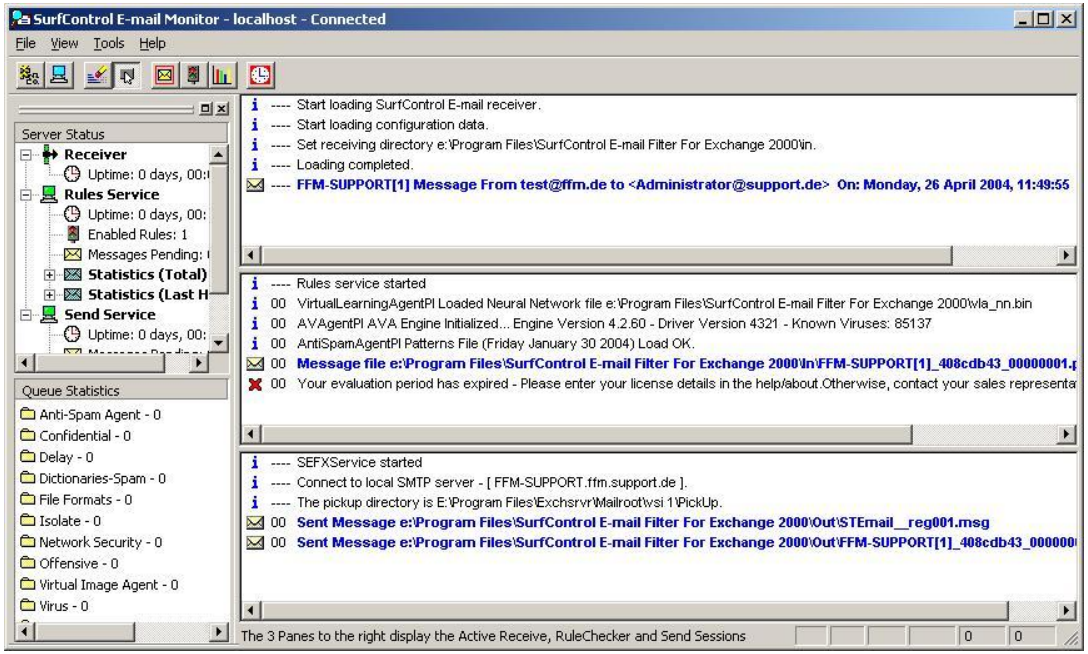
- Дополняет стандартные фильтры MS Exchange
- Пользователь сам выбирает, какие письма проверяются e-mail фильтром



SurfControl®
Enterprise Threat Protection

E-mail Filter Monitor

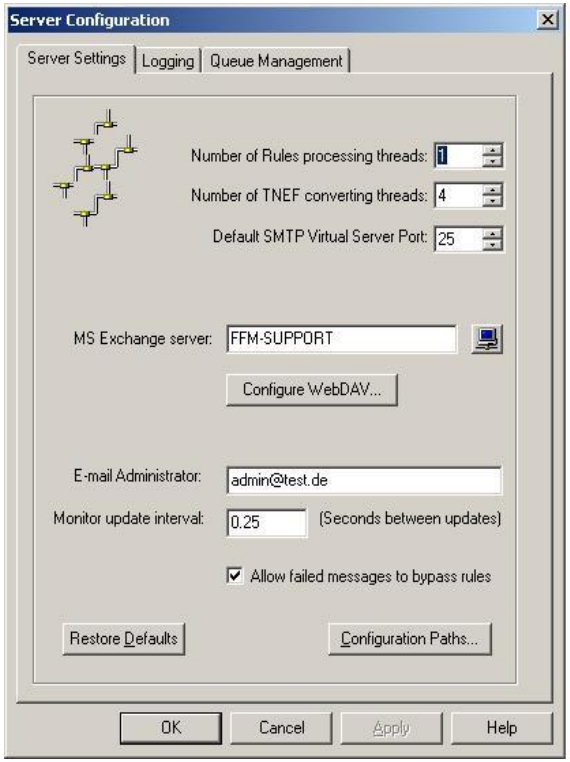
- Возможность слежения за потоком сообщений



SurfControl®
Enterprise Threat Protection

Настройка сервера

- Настройка взаимодействия с Exchange
- Использование WebDAV



SurfControl®
Enterprise Threat Protection

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 MB	Минимум 512 MB
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

SurfControl®
Enterprise Threat Protection

Спасибо за внимание