# Защищенные сети Secure Networks

Сентябрь 2005

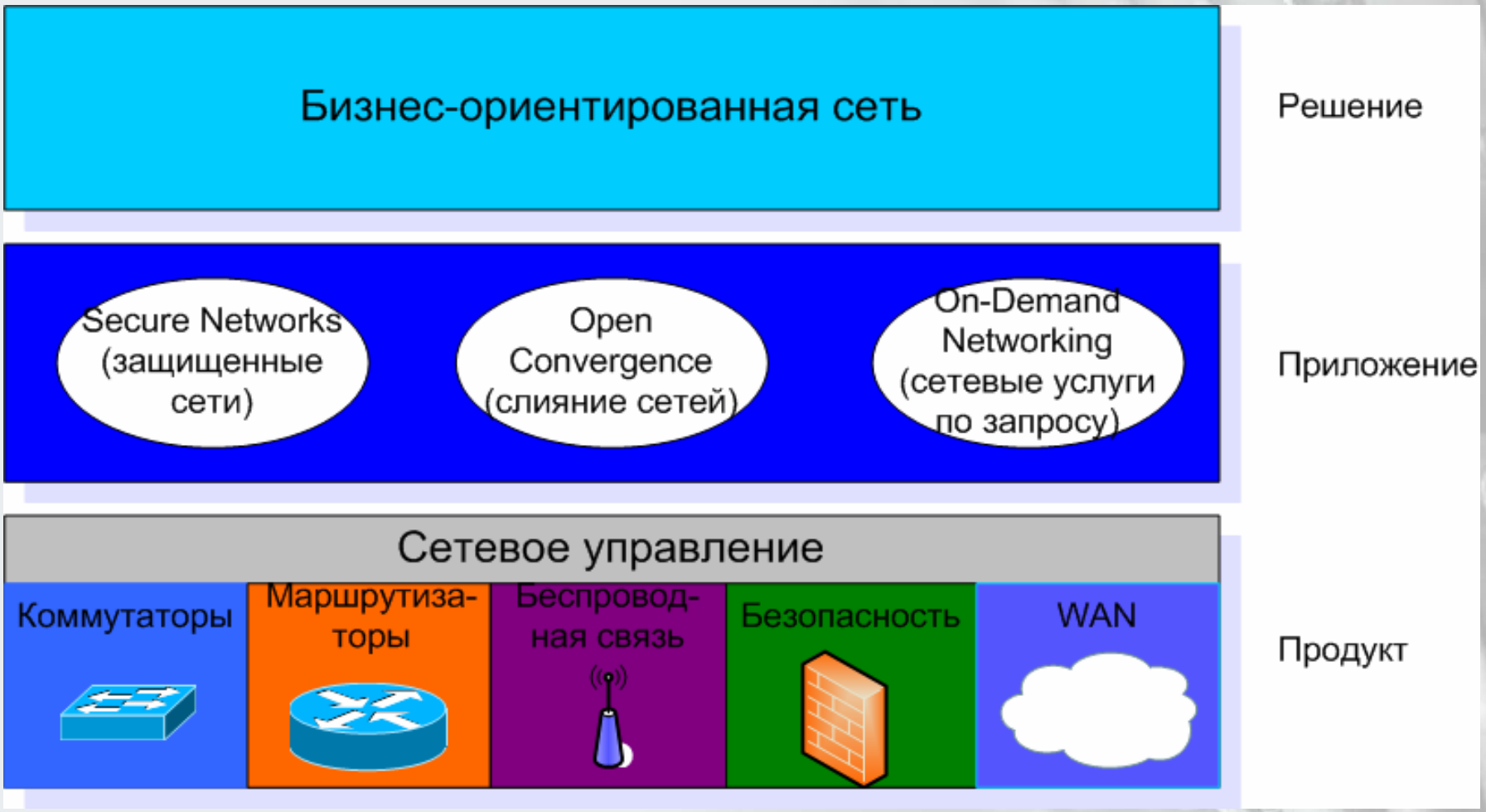

1-й Голутвинский пер., 3/5, стр. 1. Тел./факс(095) 705-90-30. http://www.ecoprog.ru

# ОГЛАВЛЕНИЕ




1-й Голутвинский пер., 3/5, стр. 1. Тел./факс(095) 705-90-30. http://www.ecoprog.ru

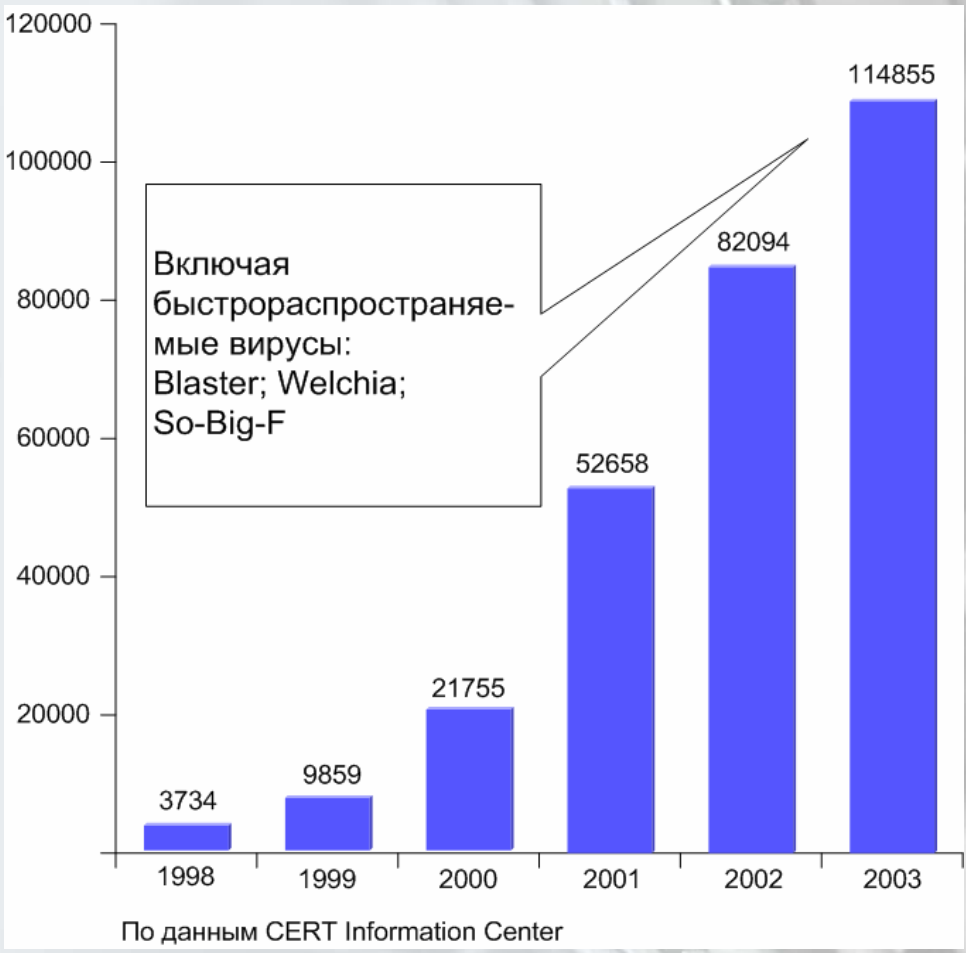
# Корпоративные решения Enterasys



# Количество инцидентов нарушения безопасности имеет тенденцию удвоения

**При этом:**

- Более 60% корпораций были взломаны
- Около 10% даже не поняли как это было сделано
- Более 80% понесли финансовые потери
- Более 20% уязвимостей были связаны с «человеческим фактором»
- Около 70% атак были инициированы из сети компании



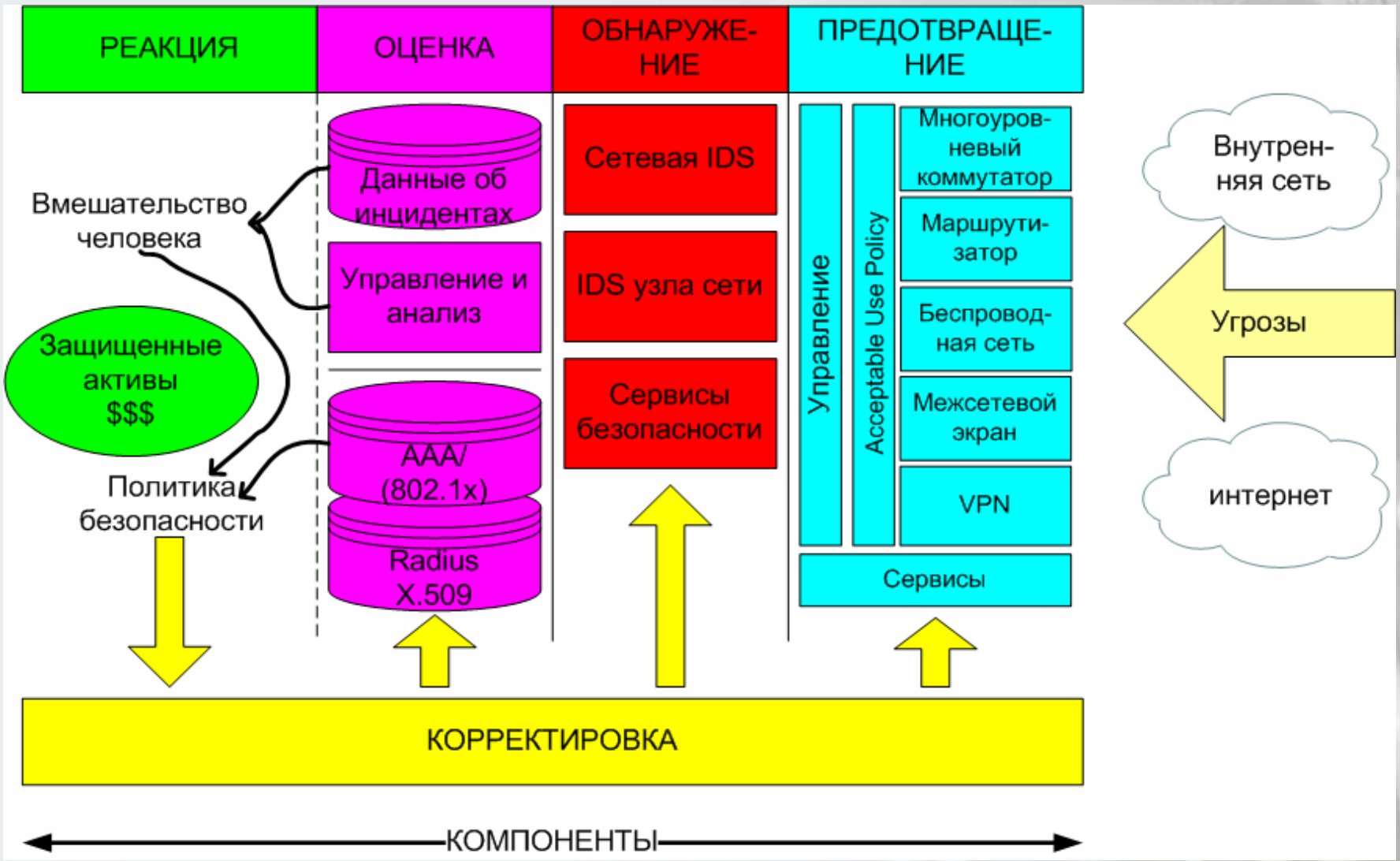
# Сравнение скоростей вирусных атак

| | Code Red | Slammer |
|---|---|---|
| Заражаемость в час | 1,8 компьютера | 420 компьютеров |
| Время удвоения кол-ва зараженных компьютеров | 37 минут | 8,5 секунд |
| Время заражения всех жертв | 24 часа | 30 минут |

# Требования к современным защищенным сетям

- Максимально быстрое автоматизированное распознавание, локализация и реакция на внутренние и внешние угрозы в точке возникновения атаки;
- Централизованное управление политиками безопасности;
- Защищенность сети на всем протяжении от уровня ядра до уровня доступа и конечных пользователей;
- Сбережение инвестиций.

# Непрерывное обеспечение безопасности сети



# ОГЛАВЛЕНИЕ

# Концепция Secure Networks

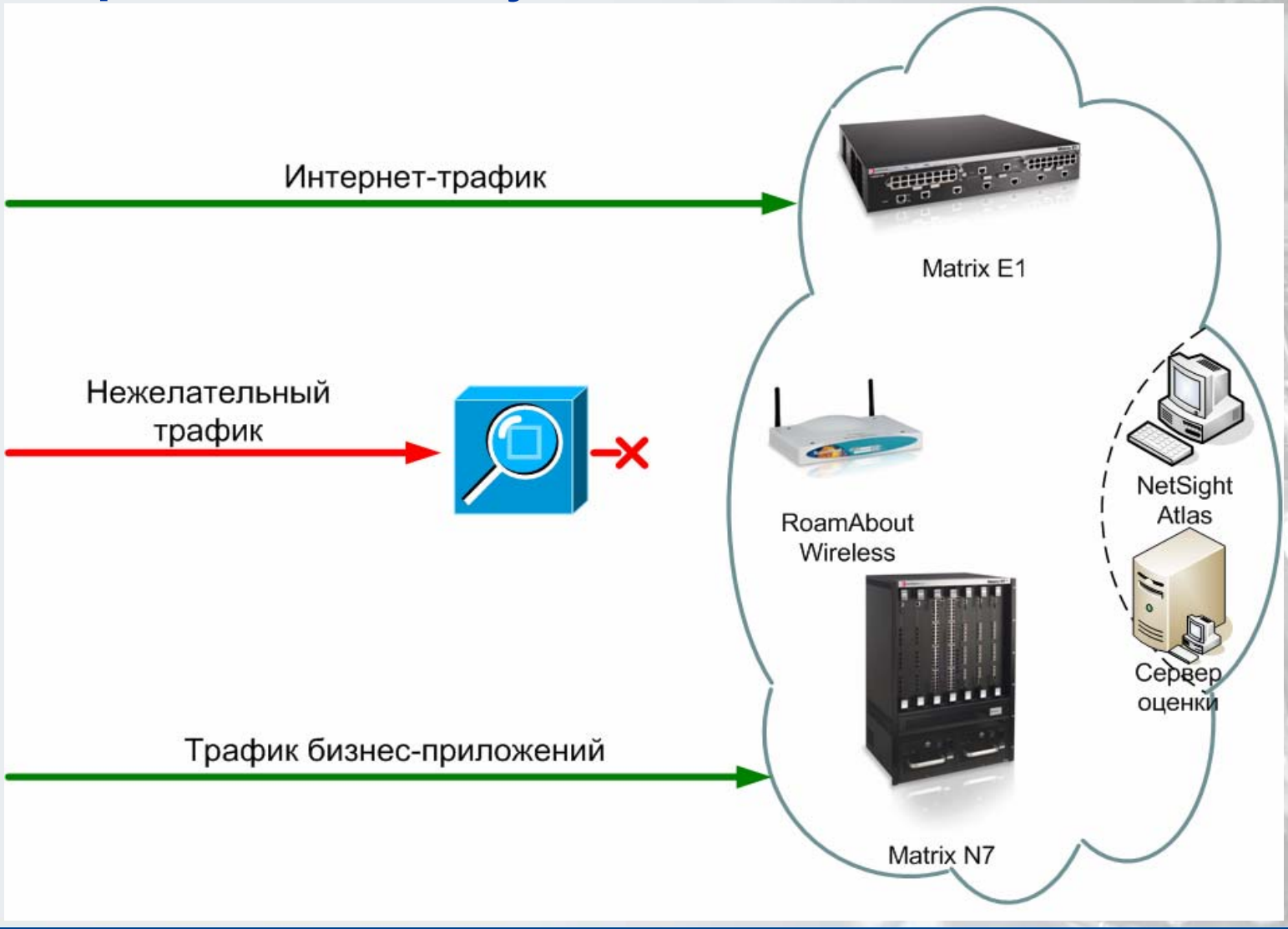
## РЕШЕНИЕ

- Acceptable Use Policy (политика правильного применения)
- Dynamic Intrusion Response (адаптивная реакция на вторжения)
- Trusted End-System (доверенная конечная система)
- Secure Application Provisioning (обеспечение безопасной работы приложений)
- Secure Guest Access (безопасный гостевой доступ)
- Single Sign-On (единая аутентификация)

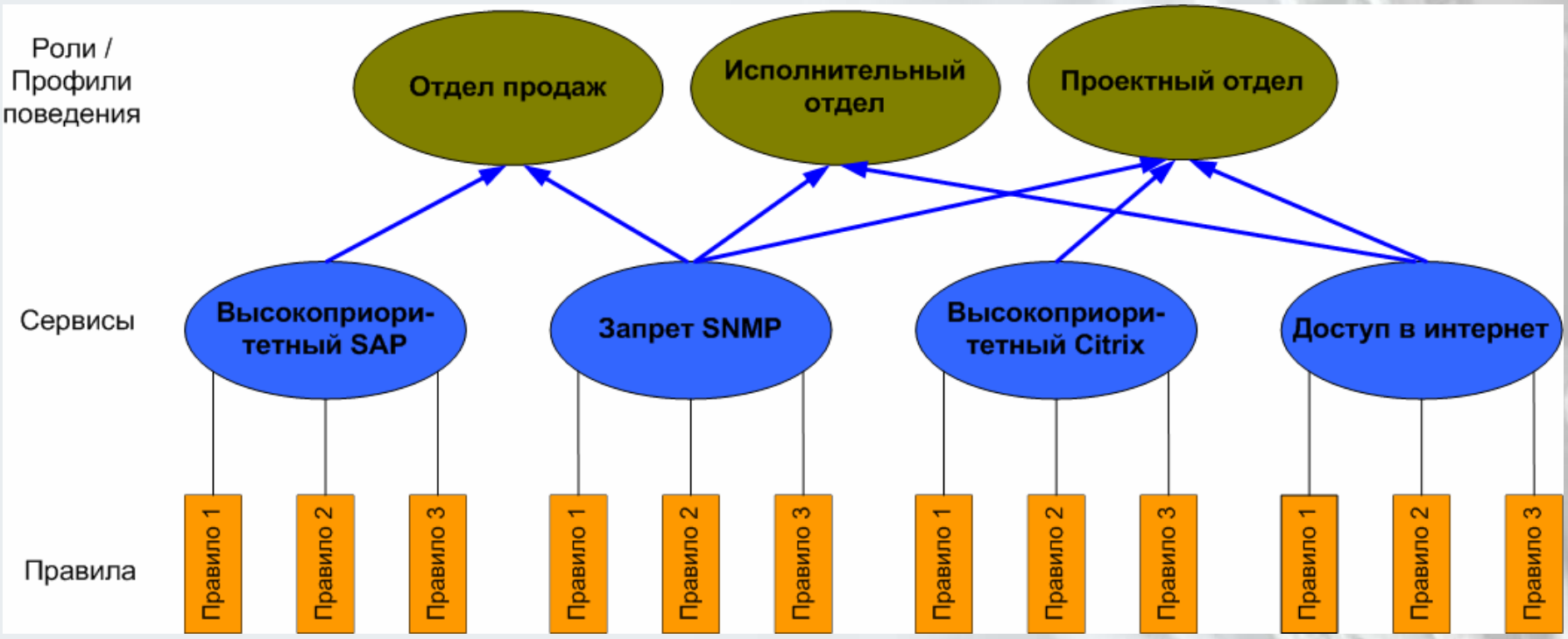
## ПРИМЕНЕНИЕ

- Distribution Layer Security (безопасность уровня распределения)
- Secure Data Center (защищенное хранилище данных)
- Secure Convergence (защищенное слияние сетей)
- Secure Wireless (защищенная беспроводная сеть)

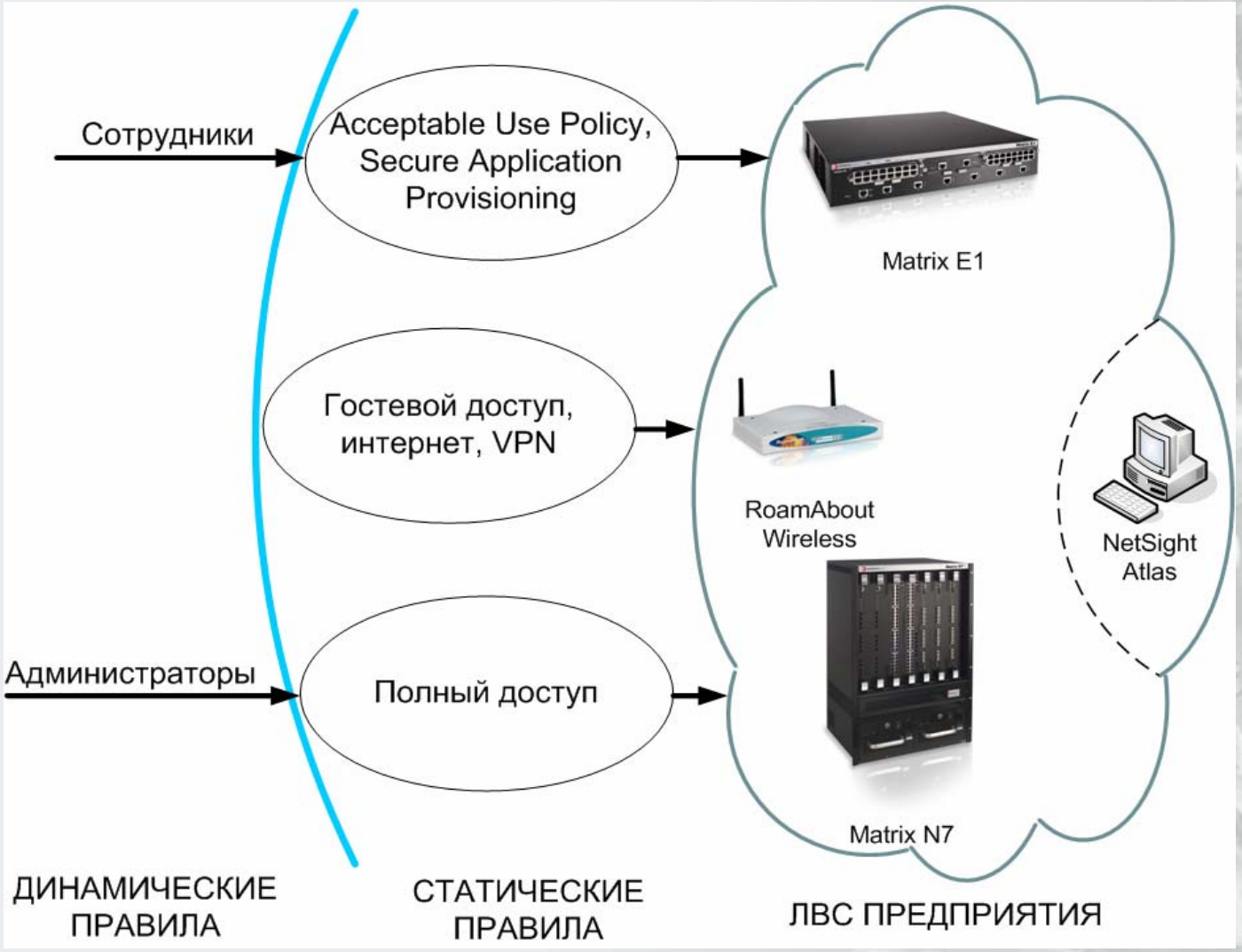
# Acceptable Use Policy



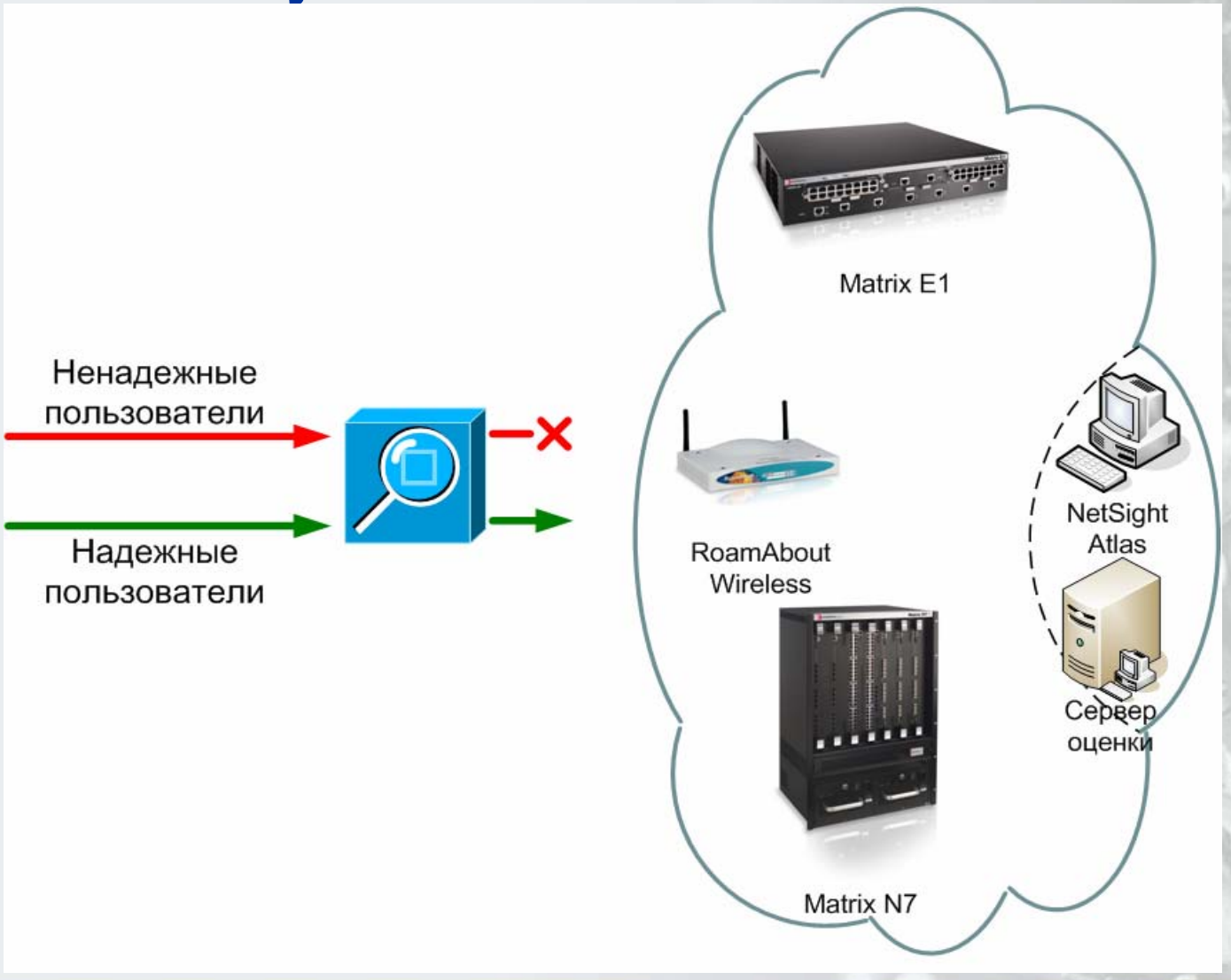
# Бизнес-ориентированный подход к построению ЛВС



# Dynamic Intrusion Response



# Trusted End-System



# Secure Application Provisioning

- Применение политики безопасности и соглашения о качестве сервиса в рамках всей сети;
- Назначение приоритета приложениям и сервисам, исходя из того кто именно к ним обращается;
- Гарантия необходимого уровня QoS для критичных для бизнеса приложений и сервисов;
- Назначение наивысшего приоритета наиболее важным приложениям и сервисам и низшего приоритета менее важным.

# Secure Guest Access

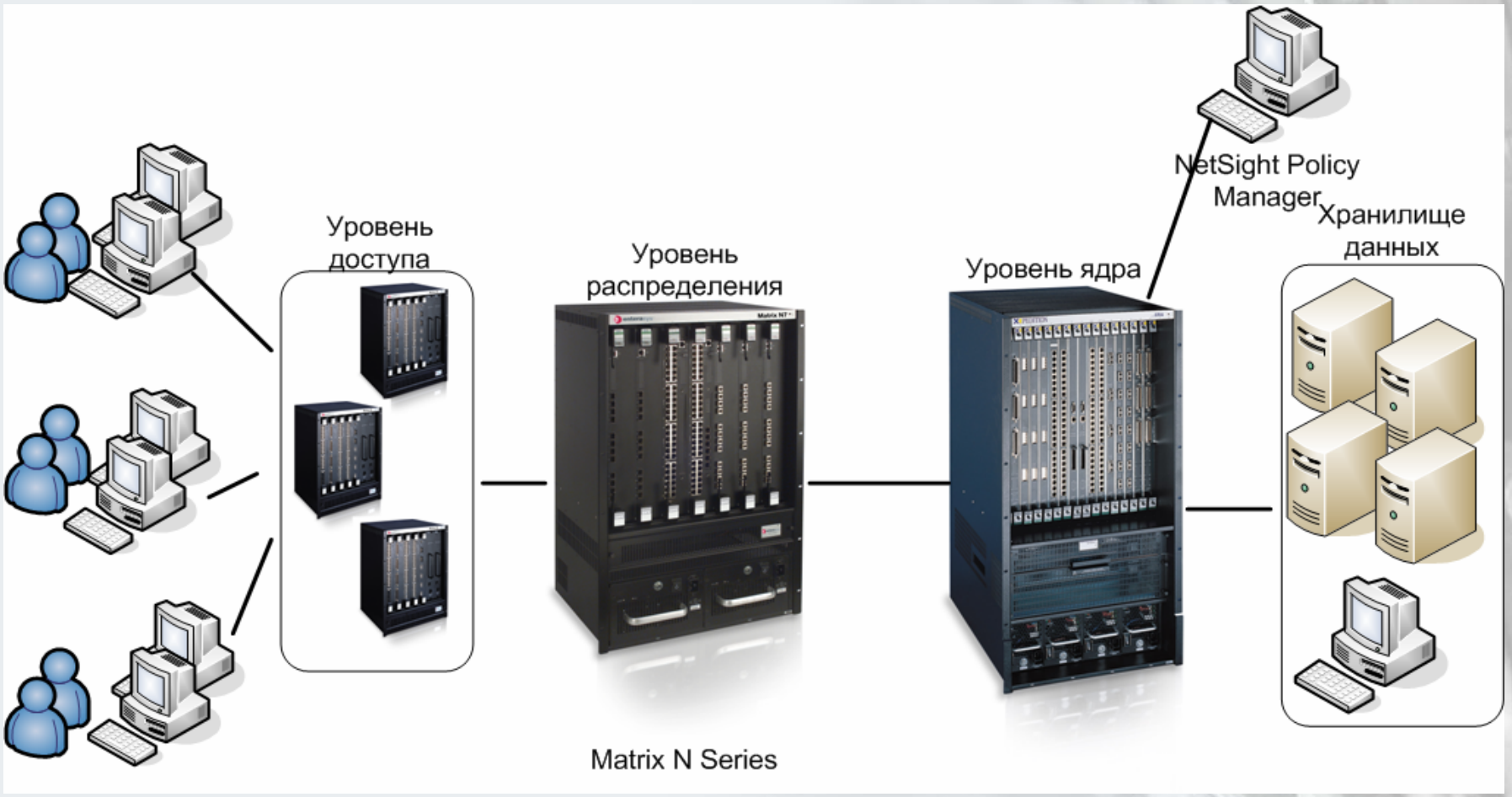
- Предоставление гостю компании доступа к определенным ресурсам (например, интернет), в то же время защищая интеллектуальную собственность компании от угроз;
- Повышение уровня мобильности сотрудников, предоставляя им доступ к ресурсам корпоративной сети в том месте, где они им нужны;
- Повышение продуктивности бизнеса гарантированием доступа тем людям, от которых напрямую зависит деятельность компании – партнерам, консультантам, удаленным сотрудникам.

# Single Sign-On

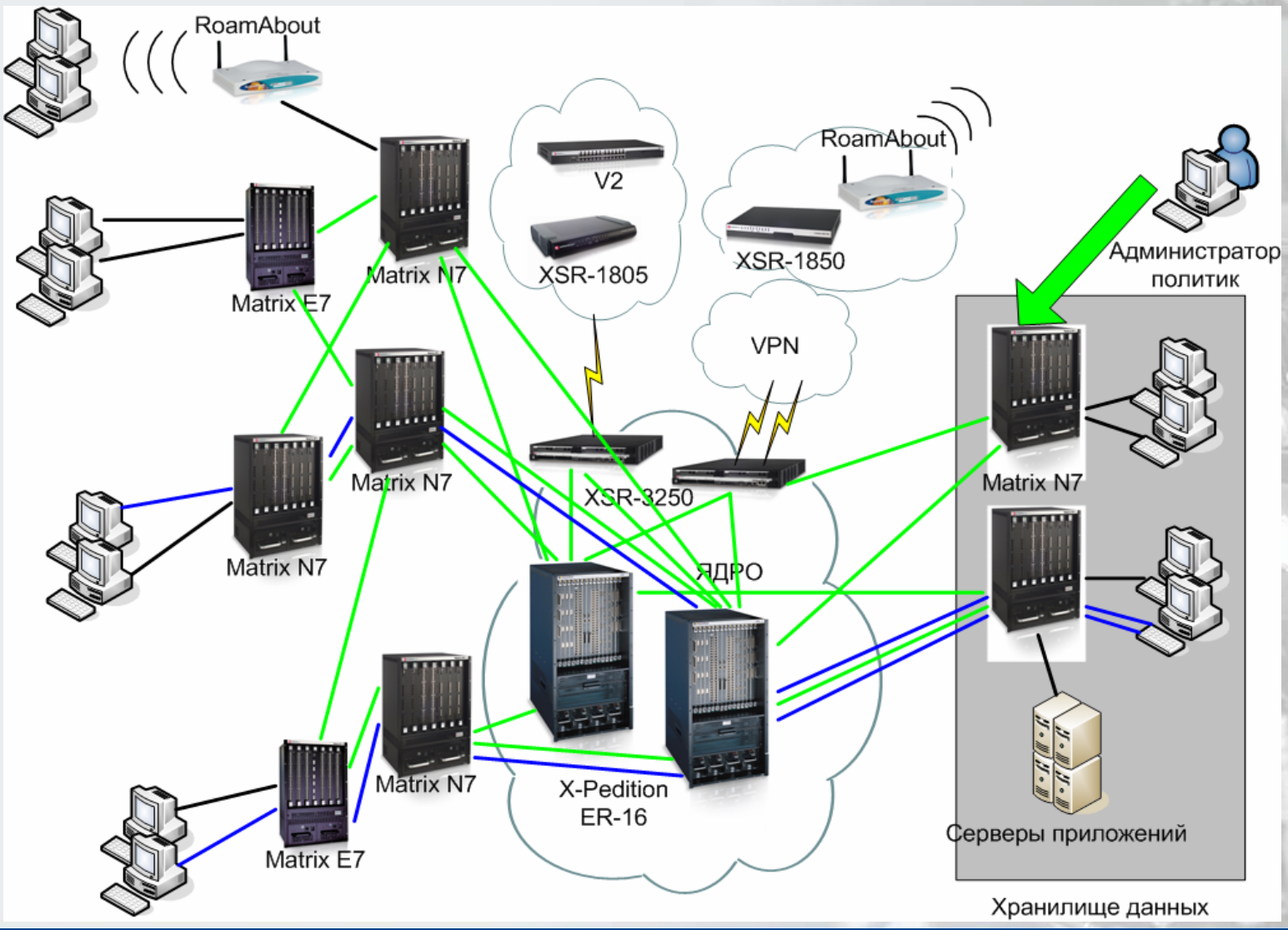
- Обеспечение одновременной аутентификации пользователя там, где ему это требуется – в Active Directory, в сети, в приложениях;
- Гарантия эффективного управления центральными ресурсами;
- Уменьшение влияния «человеческого фактора» при настройке прав доступа;
- Блокировка ресурсов для пользователей с неправильной или украденной аутентификационной информацией;
- Упрощение администрирования систем разделения прав доступа;
- Обеспечение быстрого доступ аутентифицированных пользователей лишь с одним паролем.


1-й Голутвинский пер., 3/5, стр. 1. Тел./факс(095) 705-90-30. http://www.ecoprog.ru

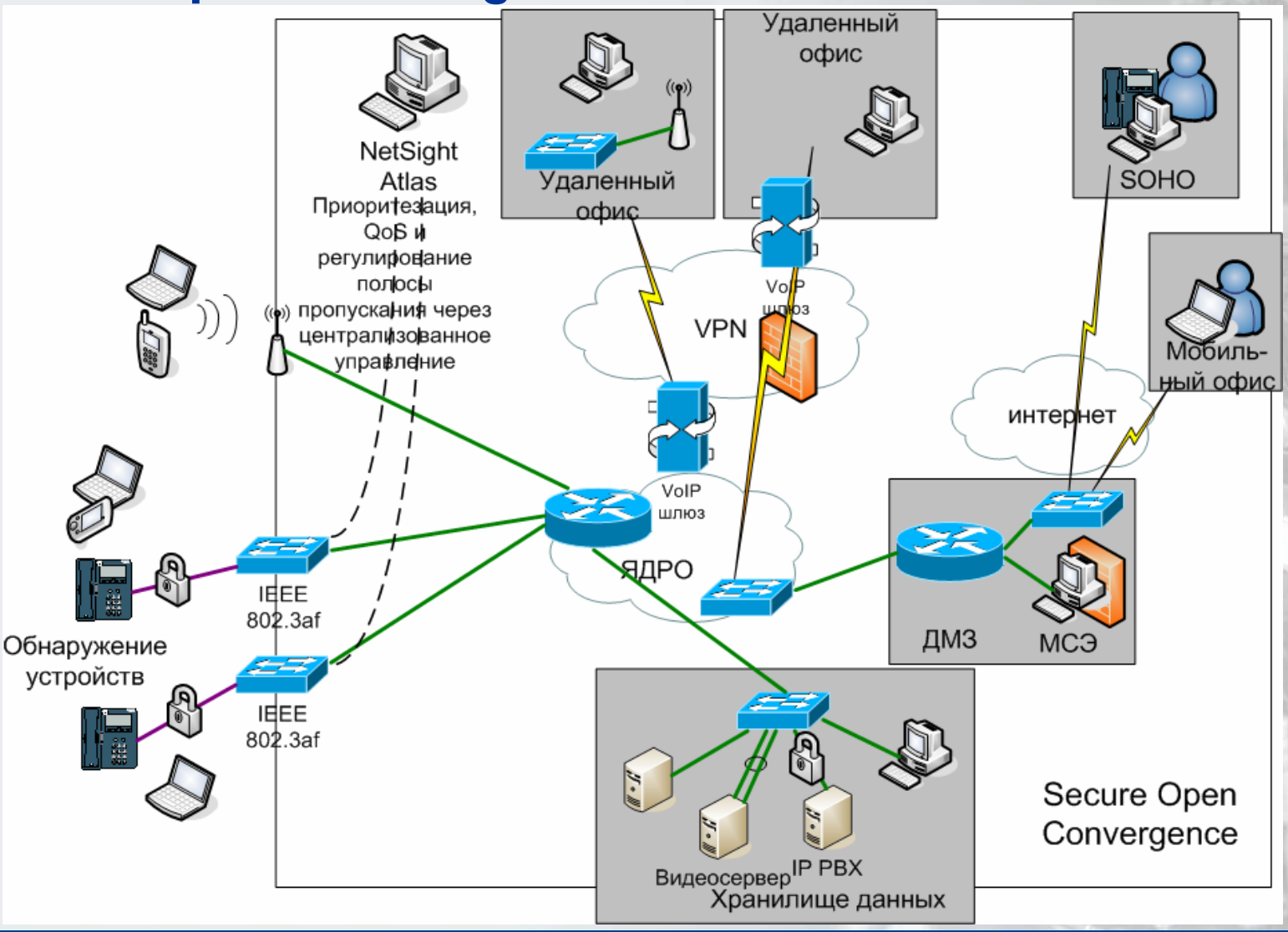
# Distribution Layer Security



# Secure Datacenter



# Secure Open Convergence



# Secure Wireless

- Защищенный периметр сети, полная совместимость с проводной сетью
- Эффективное вложение средств
- Гибкость внедрения вычислительных систем и приложений
- Решение от одного из лидеров беспроводной связи


1-й Голутвинский пер., 3/5, стр. 1. Тел./факс(095) 705-90-30. http://www.ecoprog.ru

# ОГЛАВЛЕНИЕ

# Состав решения Secure Networks

- NetSight Atlas Console
- NetSight Policy Manager
- NetSight Automated Security Manager
- Dragon IDS и IPS
- Активное сетевое оборудование (коммутаторы Matrix, маршрутизаторы XSR, беспроводные решения RoamAbout)

# NetSight Atlas Console

- Консоль управления сетью
- Корпоративная система управления сетями и элементный менеджер
- Одновременное управление группами сетевых объектов
- Расширение возможностей дополнительными модулями NetSight Atlas
- Поддержка различных платформ

# NetSight Policy Manager

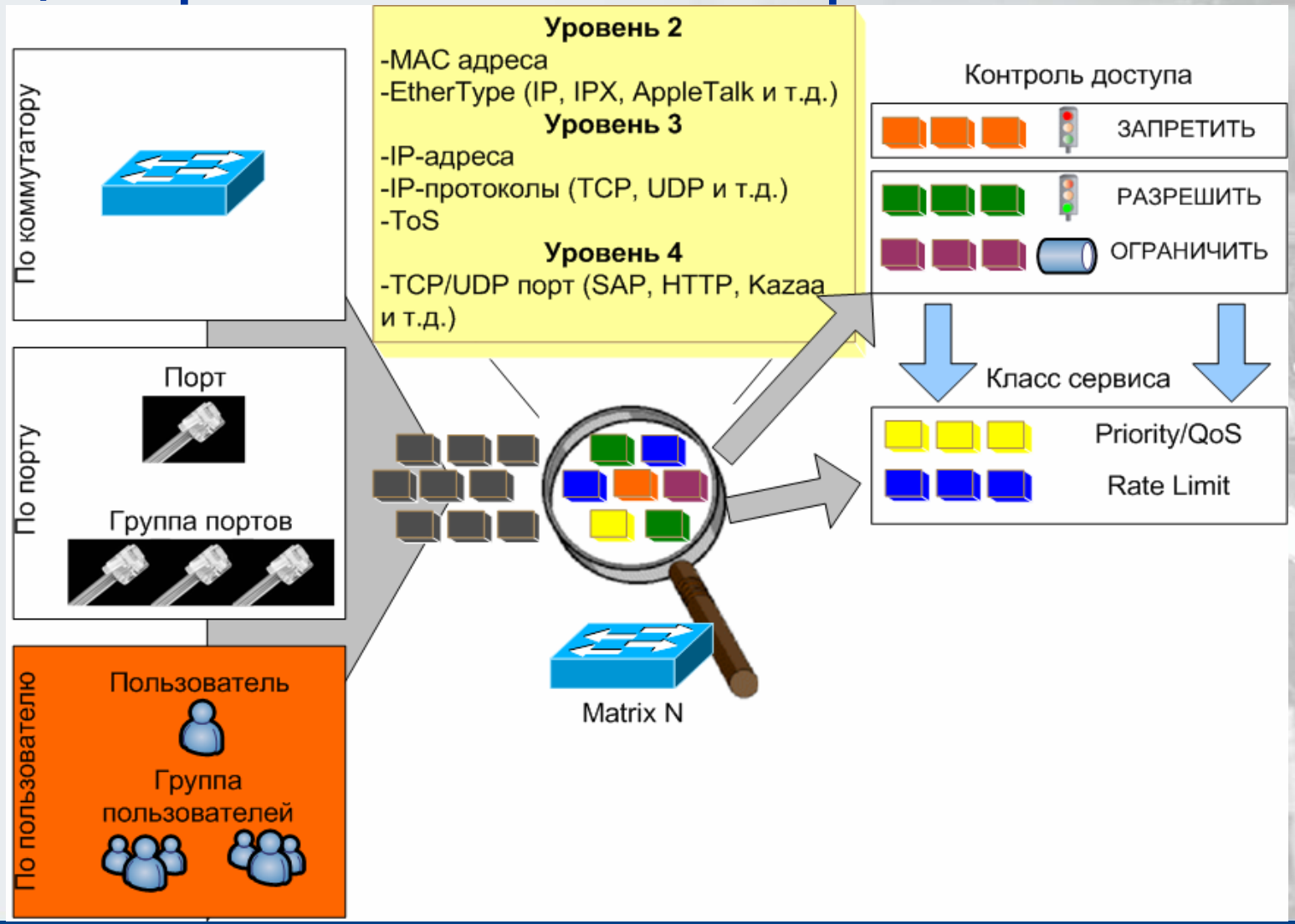
- Защита инвестиций
- Экономия времени и ресурсов за счет автоматизации
- Надежная и защищенная связь с пользователями сети
- Уменьшение сложности вычислительной инфраструктуры
- Удобный графический интерфейс на основе JAVA


1-й Голутвинский пер., 3/5, стр. 1. Тел./факс(095) 705-90-30. http://www.ecoprog.ru

# NetSight Automated Security Manager

- Дополнительная защита с помощью передовой системы поиска пользователей и компьютеров
- Ключевой элемент системы Secure Networks
- Корпоративная система управления сетями и комплекс защиты от вторжений
- Поддержка различных платформ – Windows 2000, 2003 Server и XP; Solaris v2.7, 2.8; Linux Red Hat v9 и Linux Enterprise ES v3

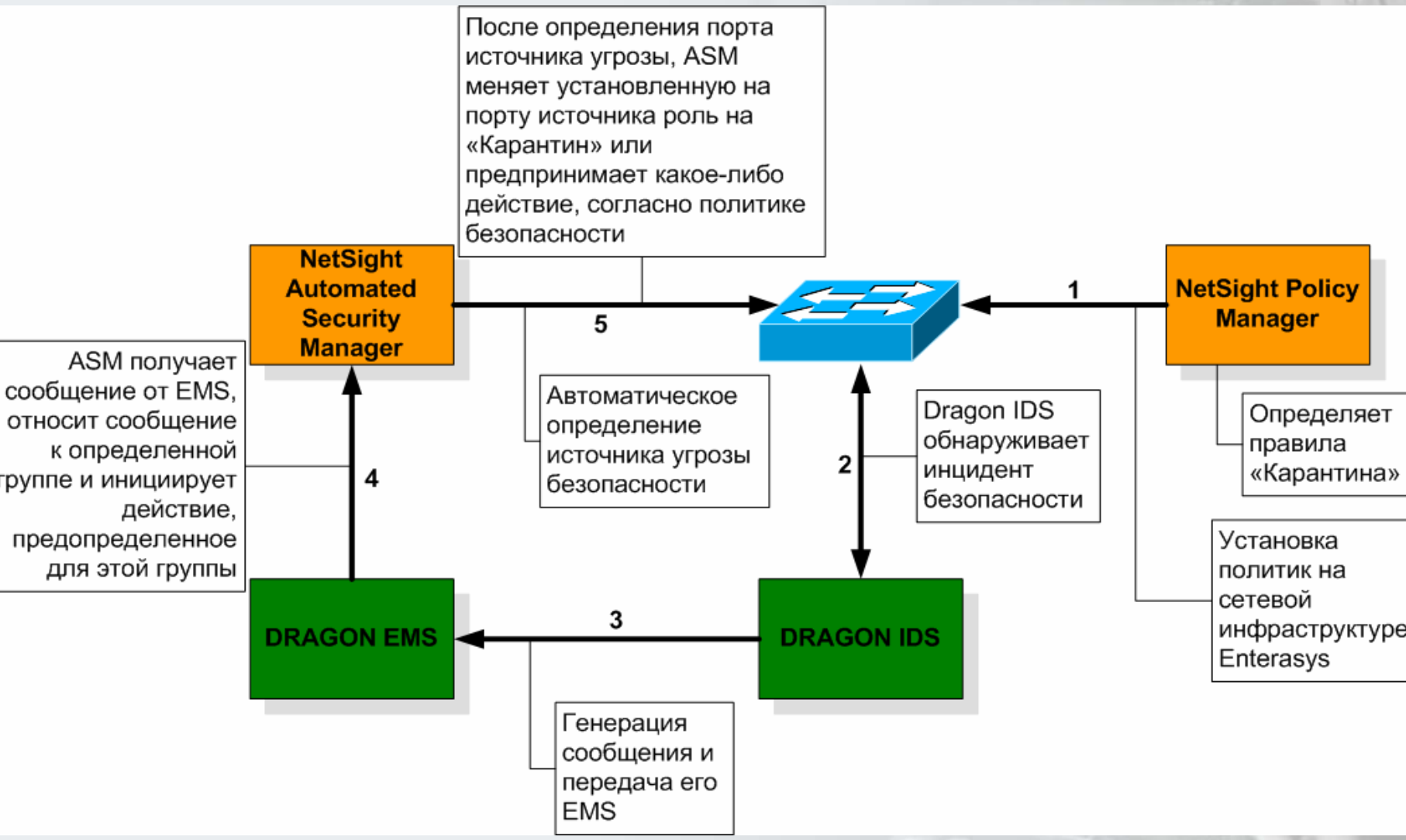
# Функционирование сети на основе ролей



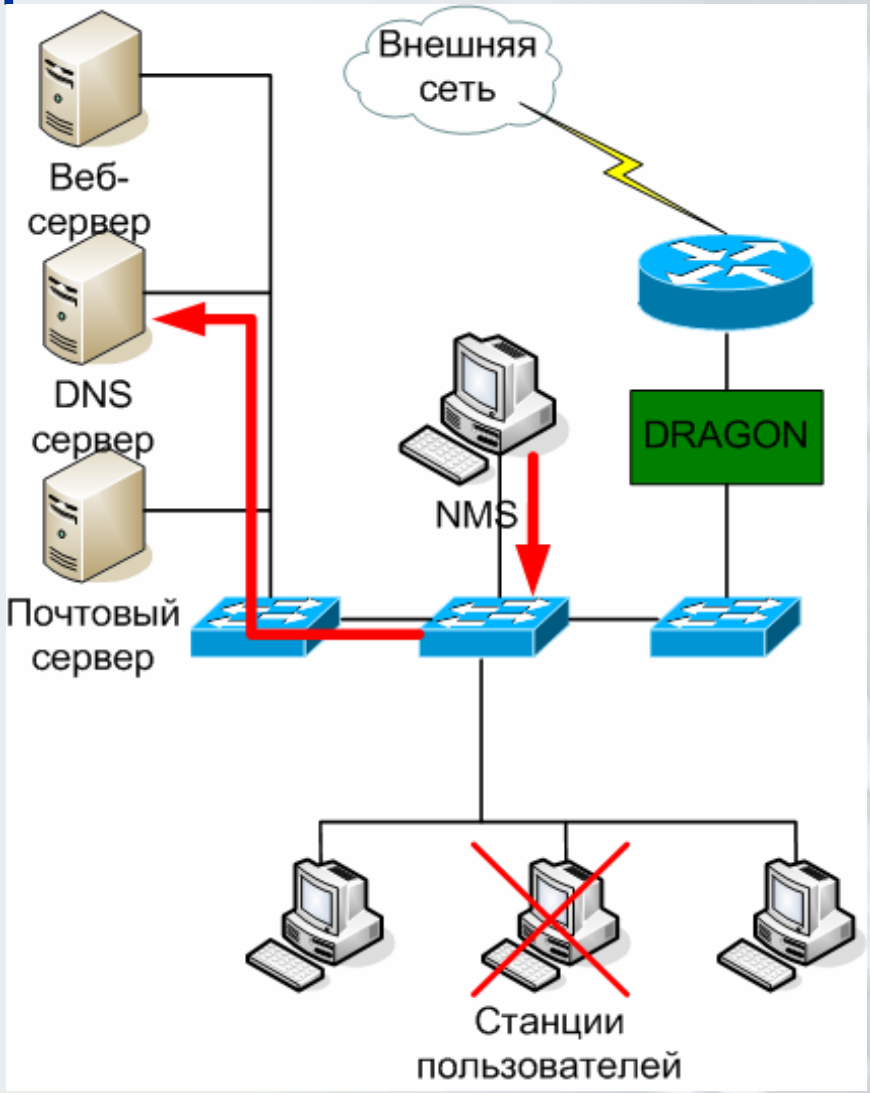
# Dragon IDS

- Dragon Network Sensor
- Dragon Host Sensor
- Dragon Enterprise Management Server
- Dragon Remote Site Appliance

# Функционирование Dragon IDS



# Совместная работа UPN и IDS



# Dragon Network Sensor

- Настраиваемые сигнатуры
- Контроль различных интерфейсов
- Дефрагментация IP и восстановление потока данных TCP/UDP
- Декодирование протоколов
- Защита от атак DoS, направленных на системы защиты
- Принятие контрмер на уровне отдельных событий
- Динамическое изменение конфигурации
- Защита от сканирования

# Dragon Host Sensor

- Предотвращение от вторжений на прикладном уровне
- Анализ протоколов
- Анализ реестра и журнала событий Windows
- Обнаружение служб TCP/UDP
- Мониторинг ядра
- Интерфейс для подключения пользовательских модулей


1-й Голутвинский пер., 3/5, стр. 1. Тел./факс(095) 705-90-30. http://www.ecoprog.ru

# Dragon Enterprise Management Server

- Веб-интерфейс управления
- Непрерывное обновление сигнатур
- Управление на системном уровне
- Создание пользовательских сигнатур
- Анализатор событий
- Сводные отчеты
- Реконструкция сеансов


1-й Голутвинский пер., 3/5, стр. 1. Тел./факс(095) 705-90-30. http://www.ecoprog.ru

# Dragon Remote Site Appliance

- Сетевой детектор вторжений для филиалов компании
- Платформа XSR
- Простота локальной установки и удаленного управления

# Активное сетевое оборудование

- Коммутаторы Matrix – в зависимости от серии в той или иной мере поддерживают опции безопасности, от поддержки аутентификации в коммутаторах серии V2 и A2 до полного функционала в N-серии
- Маршрутизаторы XSR – высокопроизводительные маршрутизаторы для создания защищенного ядра
- Беспроводная связь RoamAbout – точки доступа для организации защищенных беспроводных сетей

# Выгоды от Secure Networks для бизнеса

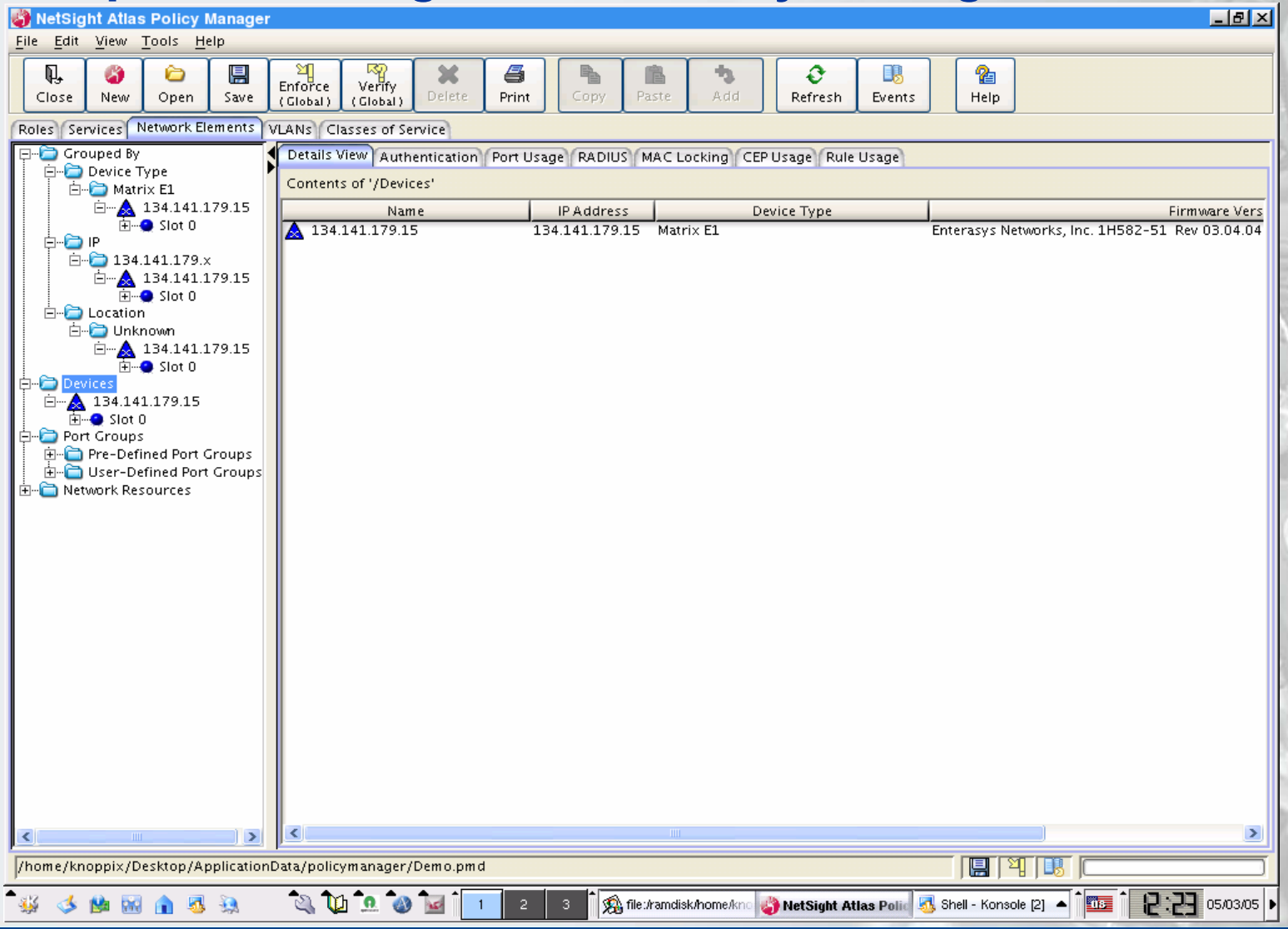
- Обеспечивает постепенное, обоснованное вложение средств в сетевую безопасность
- Обеспечение надежного защищенного доступа для пользователей изнутри и снаружи сети, основанного на их роли внутри организации
- Уменьшение сложности сетевой инфраструктуры и рисков внедрением активной автоматизированной системы сетевой безопасности
- Позволяет адаптировать сеть любой компании к реальным потребностям ее бизнеса
- Способствует эффективному внедрению новых приложений
- Применимо уже сегодня с использованием линейки продуктов Enterasys

# ОГЛАВЛЕНИЕ

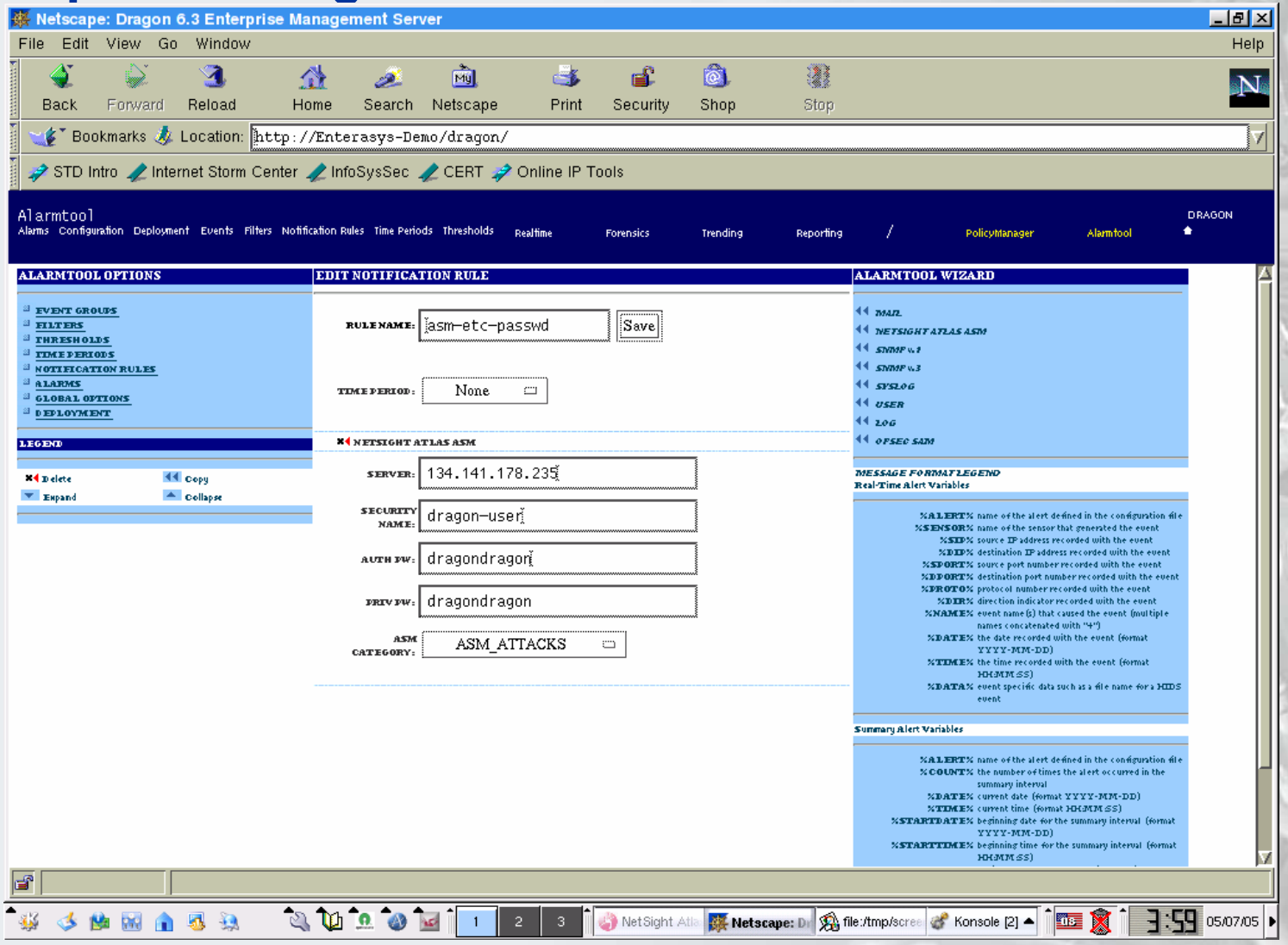



1-й Голутвинский пер., 3/5, стр. 1. Тел./факс(095) 705-90-30. http://www.ecoprog.ru

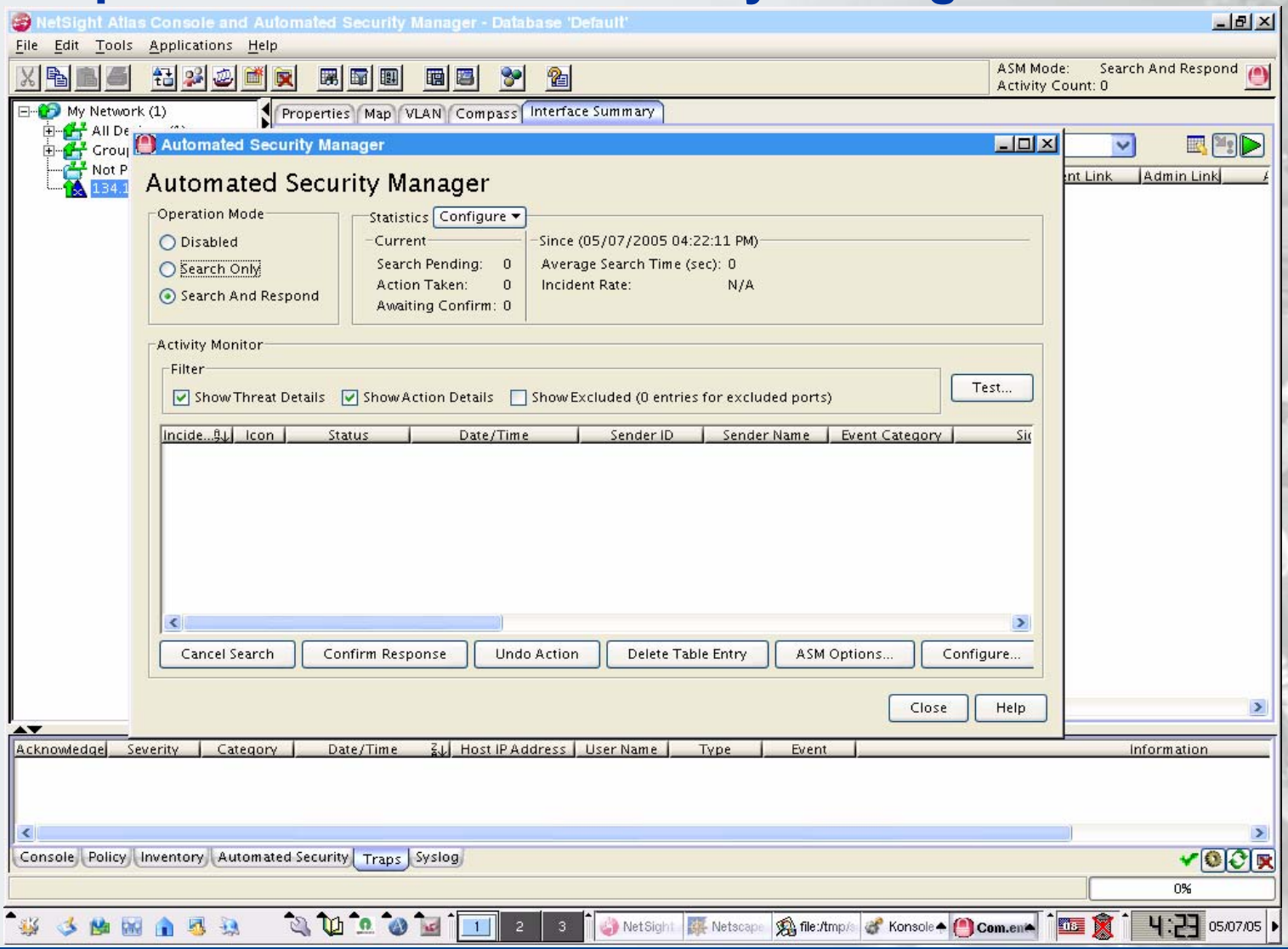
# Настройка NetSight Atlas Policy Manager



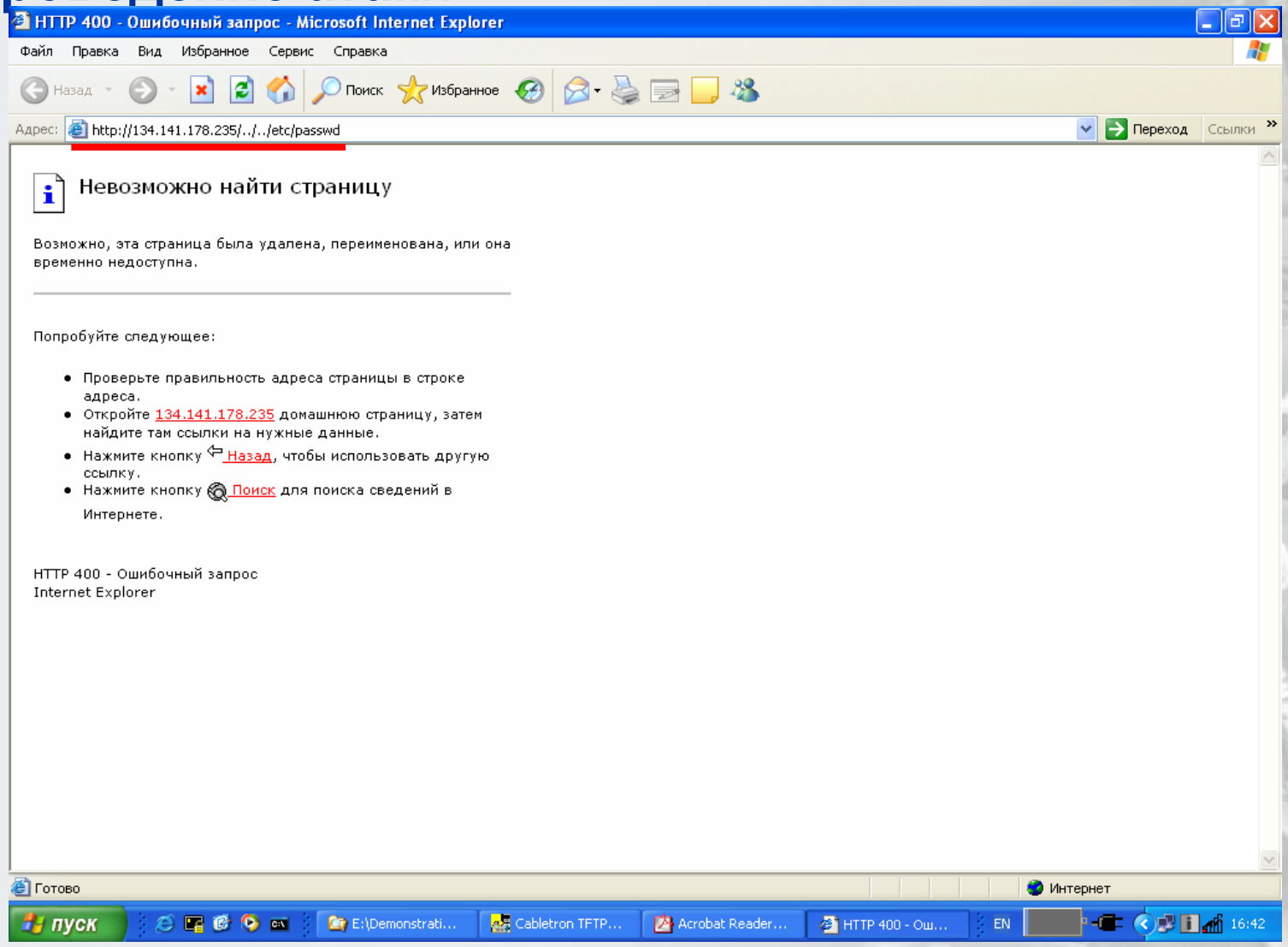
# Настройка Dragon IDS



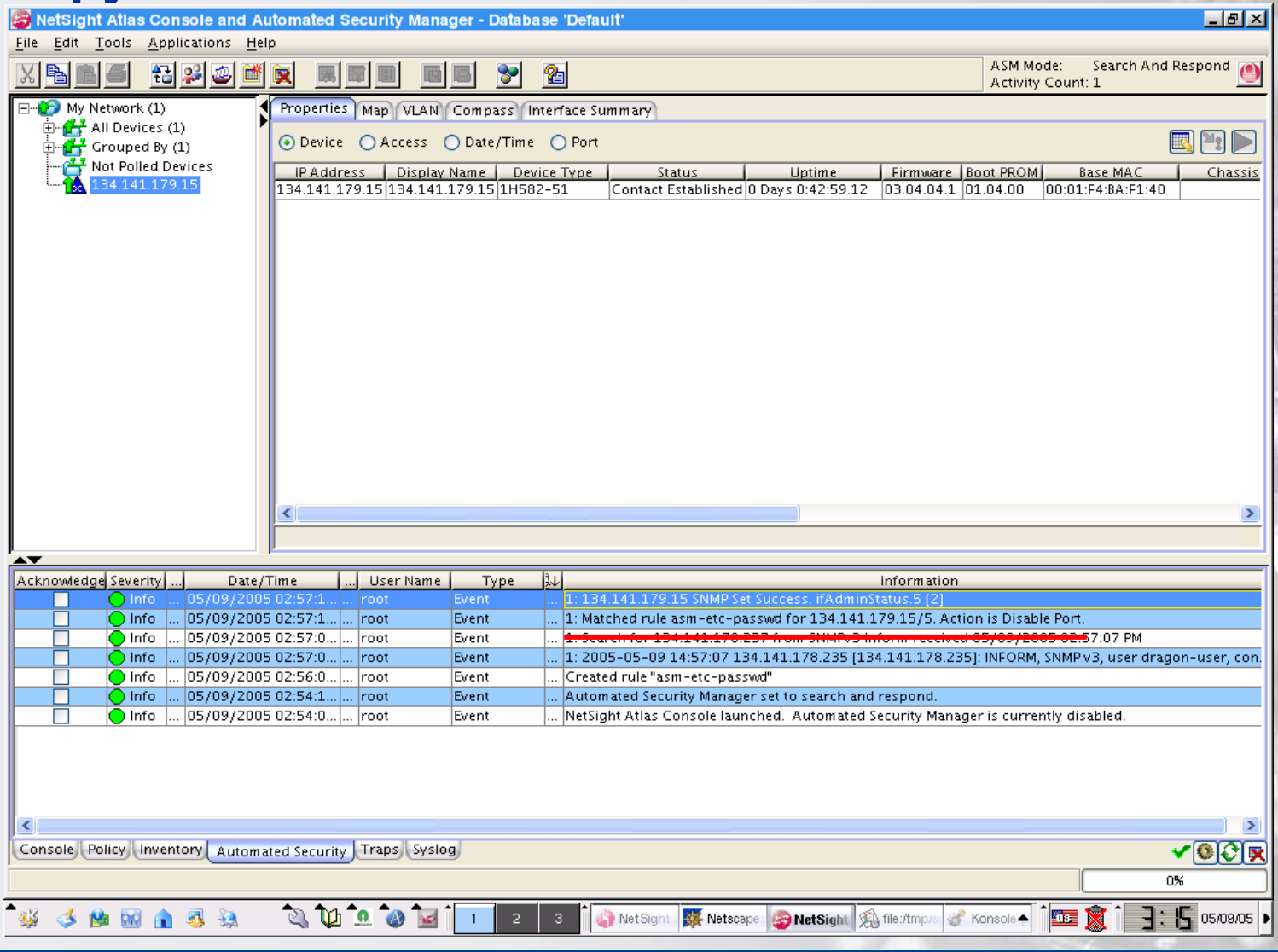
# Настройка Automated Security Manager

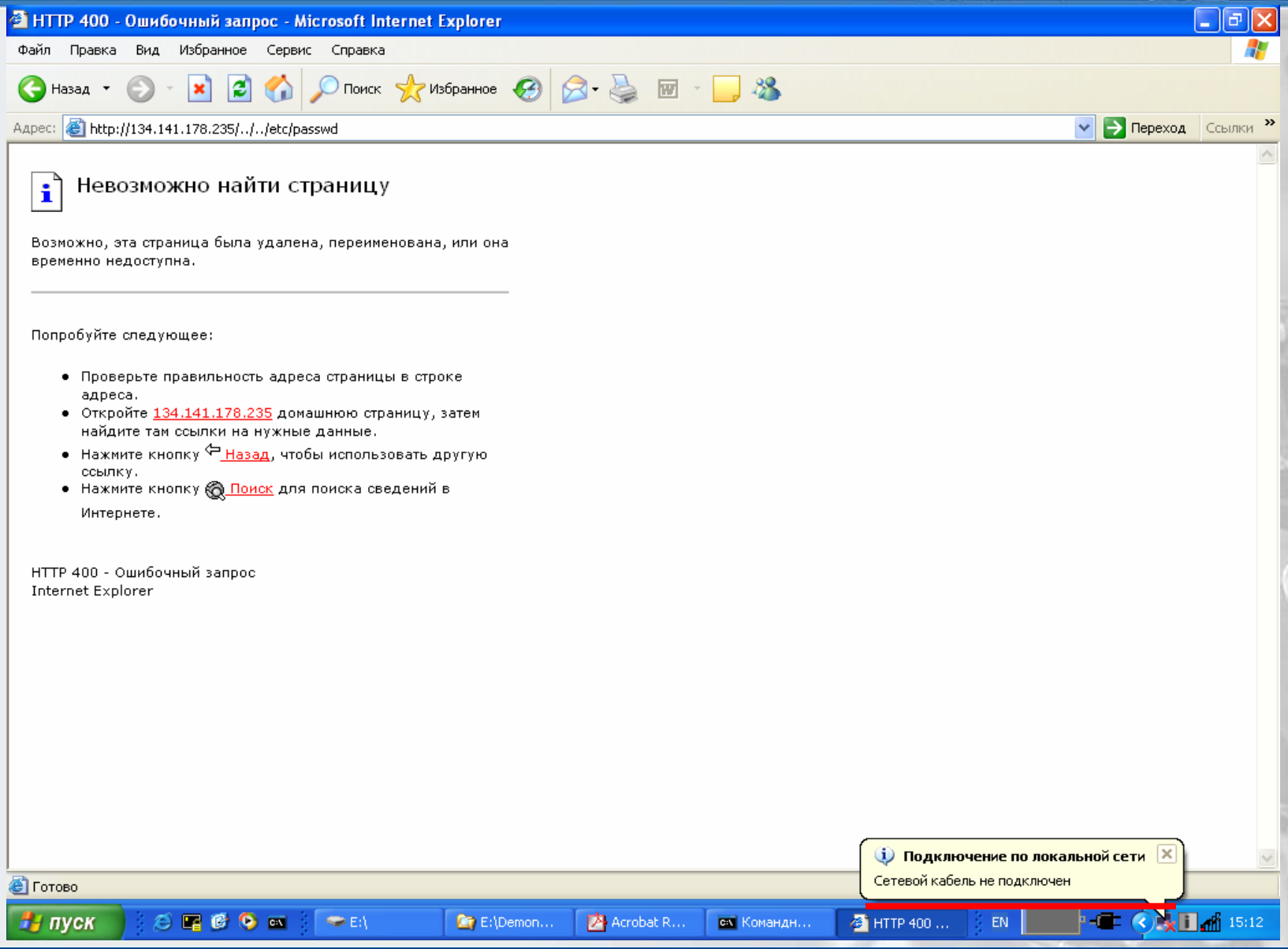


# Проведение атаки



# Обнаружение атаки



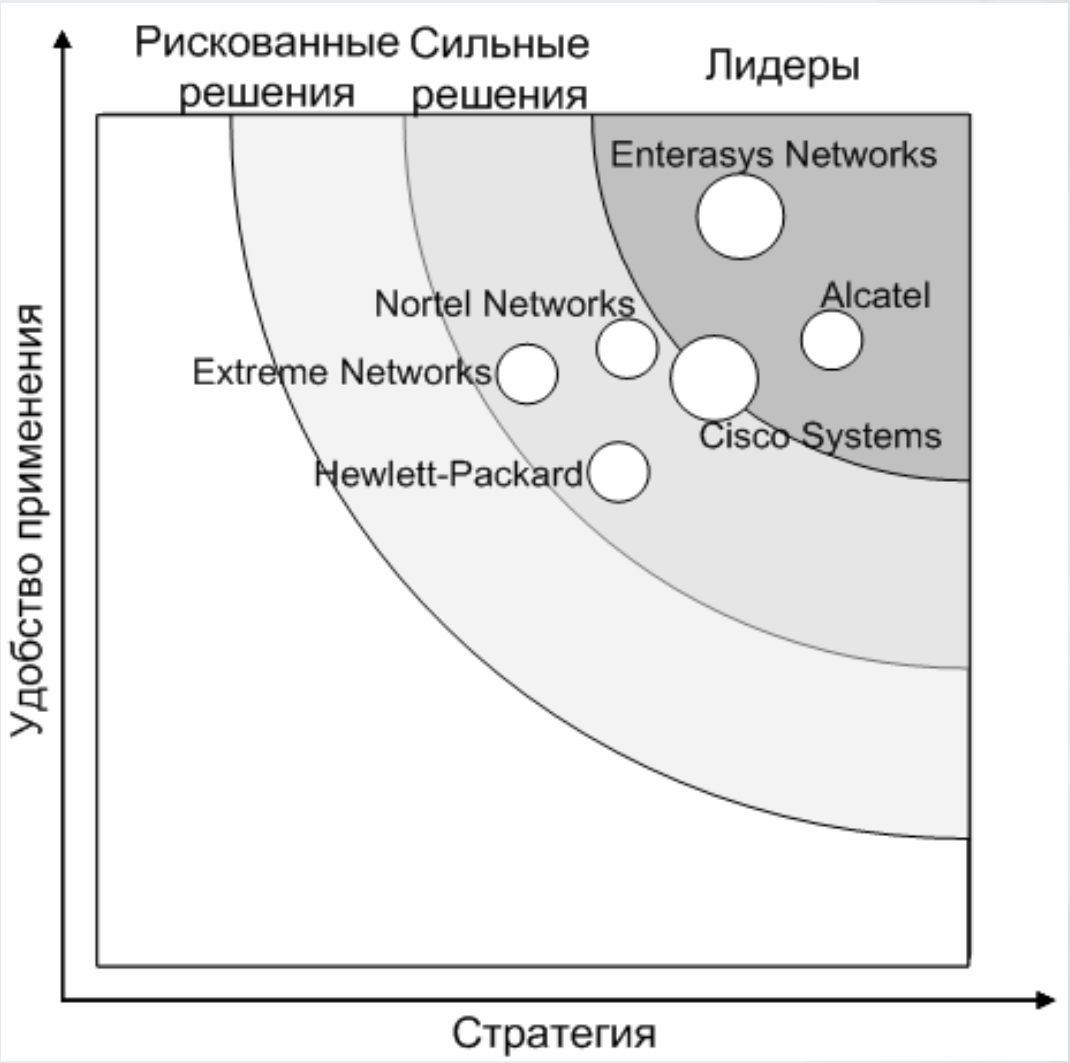

HTTP 400 - Ошибочный запрос - Microsoft Internet Explorer
Файл Правка Вид Избранное Сервис Справка
Назад
Поиск
Избранное
Адрес: http://134.141.178.235/../../etc/passwd
Переход
Ссылки
Невозможно найти страницу
Возможно, эта страница была удалена, переименована, или она временно недоступна.
Попробуйте следующее:
Проверьте правильность адреса страницы в строке адреса.
Откройте 134.141.178.235 домашнюю страницу, затем найдите там ссылки на нужные данные.
Нажмите кнопку Назад, чтобы использовать другую ссылку.
Нажмите кнопку Поиск для поиска сведений в Интернете.
HTTP 400 - Ошибочный запрос
Internet Explorer
Подключение по локальной сети
Сетевой кабель не подключен
Готово
пуск
E:\
E:\Demon...
Acrobat R...
Командн...
HTTP 400 ...
EN
15:12

# ОГЛАВЛЕНИЕ




1-й Голутвинский пер., 3/5, стр. 1. Тел./факс(095) 705-90-30. http://www.ecoprog.ru

# Рынок корпоративных систем безопасности




«Enterasys – безоговорочный лидер рынка»

-- «Securing the Campus Network»

Forrester Report, 29.09.2004

# Преимущества решения Secure Networks

- Автоматическое обнаружение угрозы в масштабе реального времени;
- Автоматическая локализация источника угрозы и реакция на нее в точке возникновения;
- Централизованное бизнес-ориентированное управление правилами доступа к ресурсам ЛВС;
- Централизованное управление качеством обслуживания;
- Предоставление гостевого доступа.

# Secure Networks – выгодное решение

## Выгоды для бизнеса:

- Уменьшение затрат на эксплуатацию и администрирование;
- Минимизация внешних и внутренних угроз (кражи, потеря конфиденциальности, прерывание бизнеса);
- Экономически оправданное решение в приобретении и использовании;

## Выгоды для ИТ:

- Централизованный контроль и управление корпоративными политиками безопасности;
- Автоматизированное диагностирование, локализация, отклик и предотвращение угроз;
- Распределенное управление и детальный контроль за сетевой инфраструктурой;
- Интеграция в существующую ИТ-инфраструктуру;
- Масштабируемость.


1-й Голутвинский пер., 3/5, стр. 1. Тел./факс(095) 705-90-30. http://www.ecoprog.ru