

Защищенные сети Secure Networks

Сентябрь 2005

ОГЛАВЛЕНИЕ

Предпосылки

Концепция Secure Networks

Состав решения

Пример реализации

Преимущества решения

Корпоративные решения Enterasys

Бизнес-ориентированная сеть

Решение

Secure Networks
(защищенные
сети)

Open
Convergence
(слияние сетей)

On-Demand
Networking
(сетевые услуги
по запросу)

Приложение

Сетевое управление

Коммутаторы



Маршрутиза-
торы



Беспровод-
ная связь



Безопасность



WAN

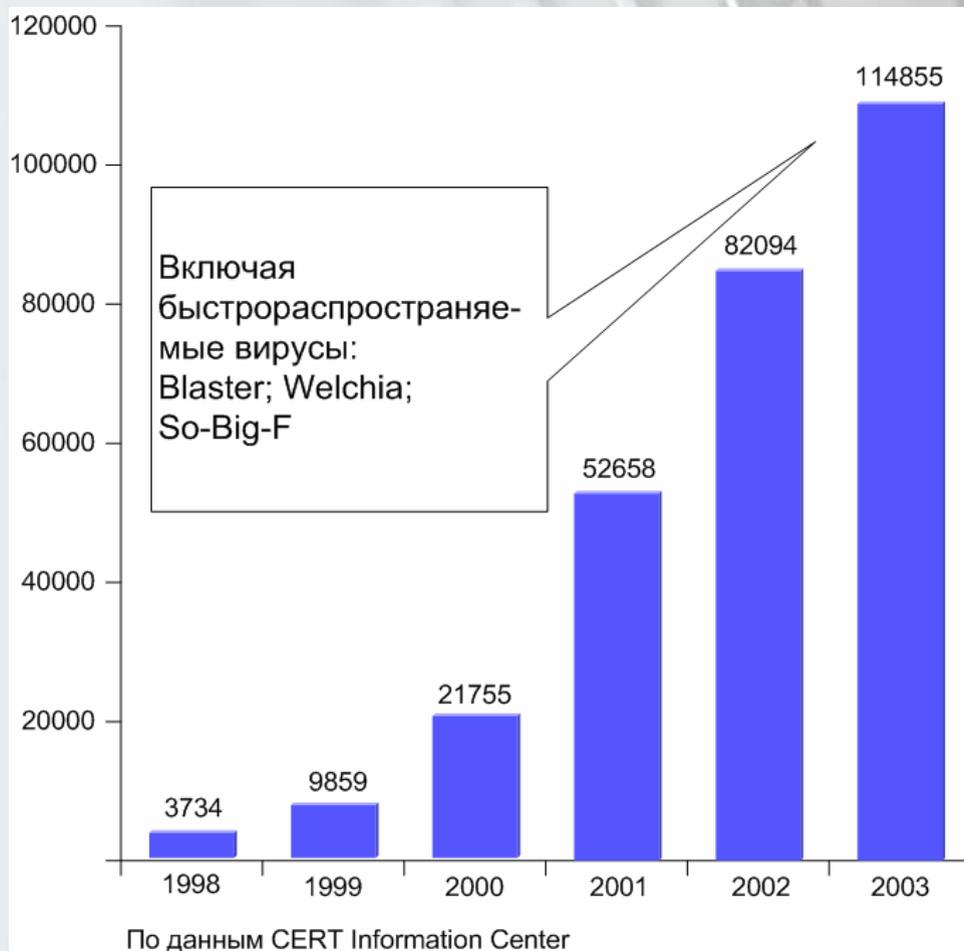


Продукт

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



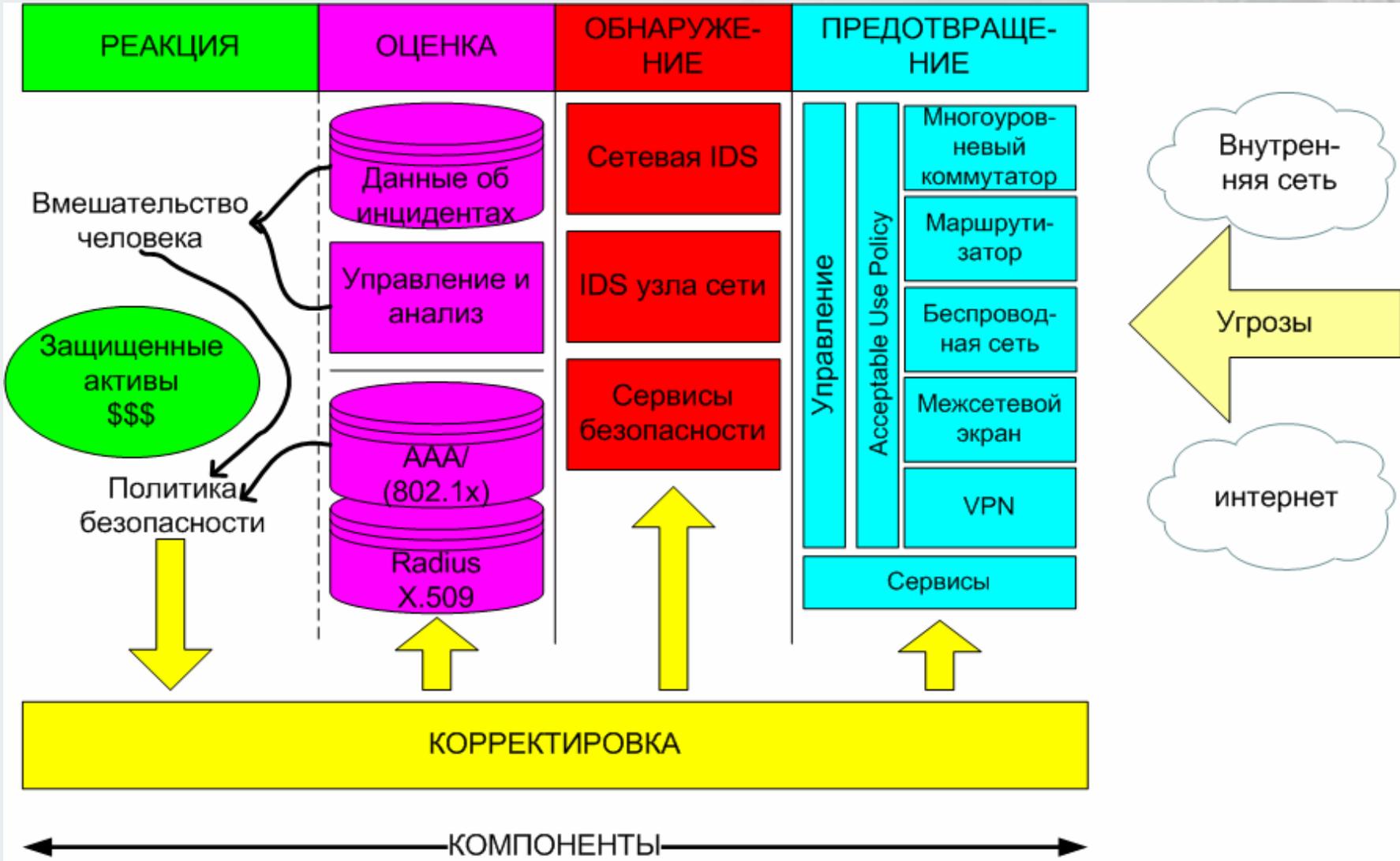
Сравнение скоростей вирусных атак

	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

Предпосылки

Концепция Secure Networks

Состав решения

Пример реализации

Преимущества решения

Концепция Secure Networks

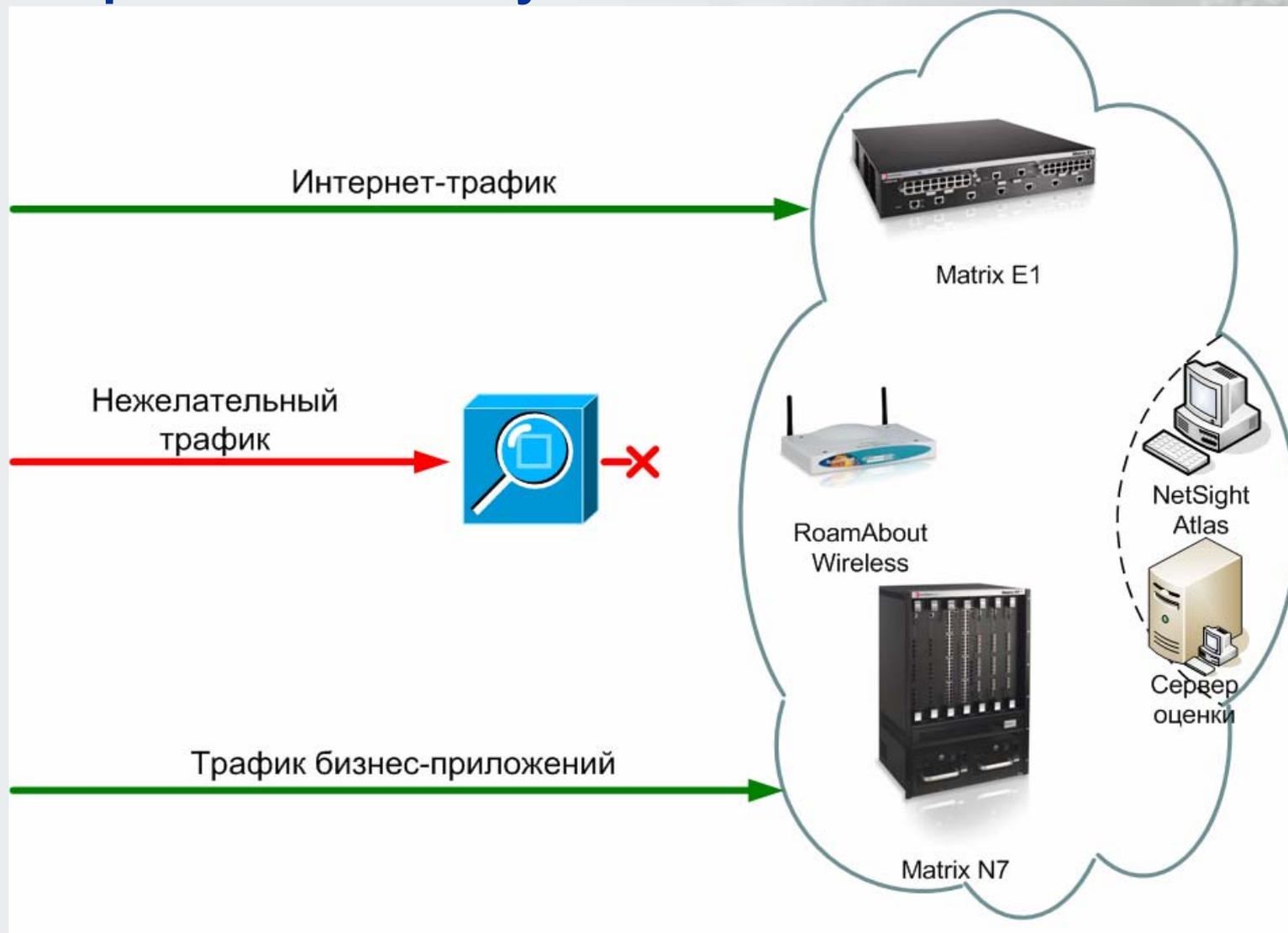
РЕШЕНИЕ

- **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)

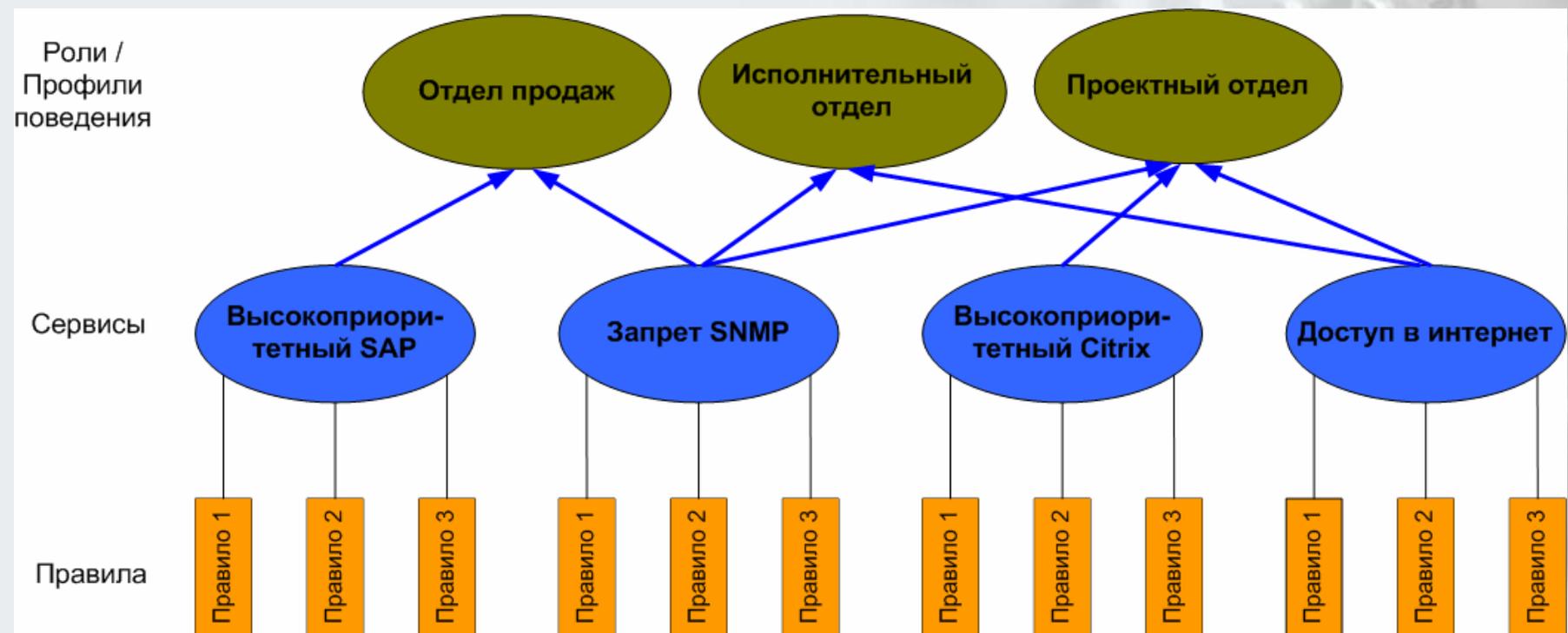
ПРИМЕНЕНИЕ

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

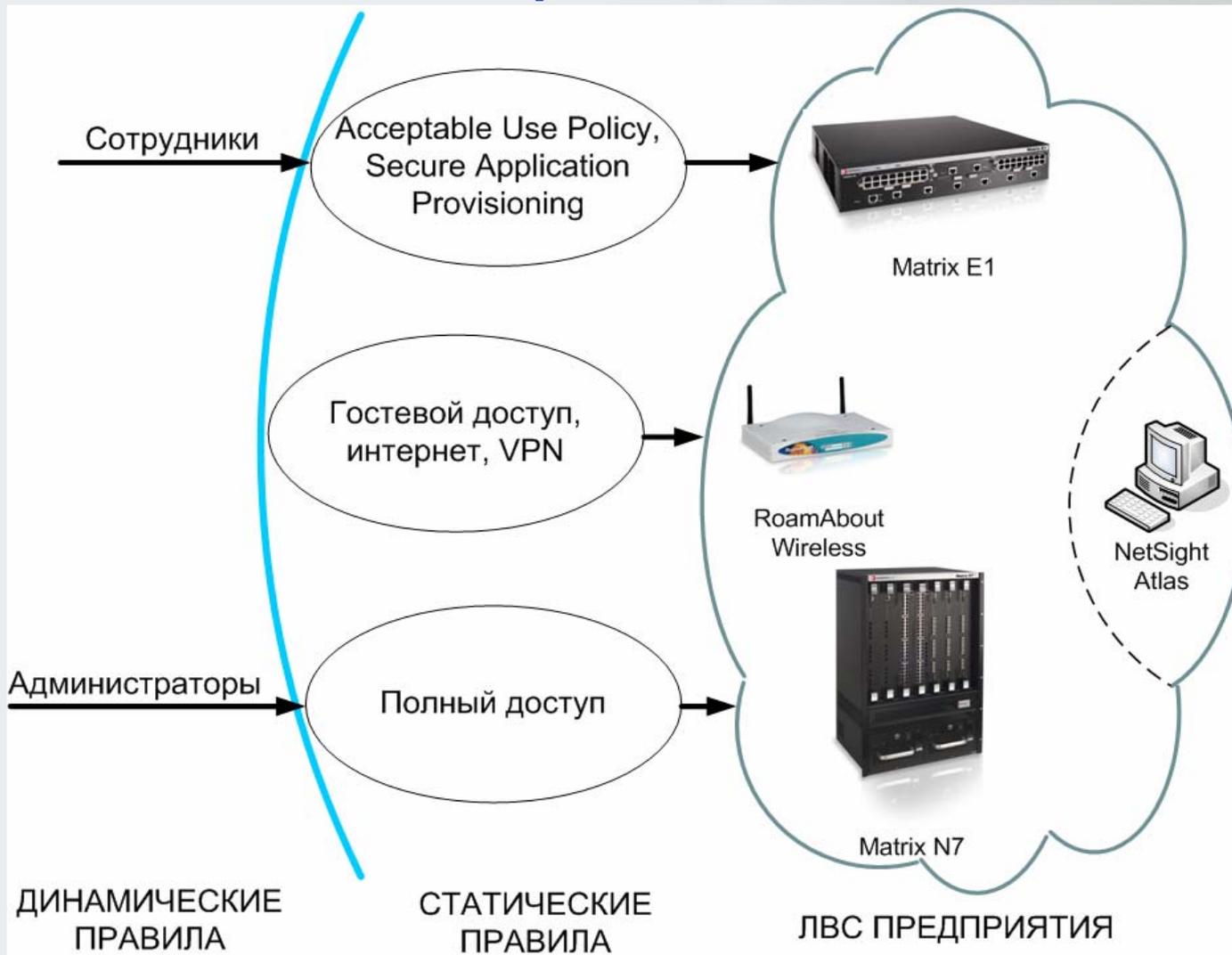
Acceptable Use Policy



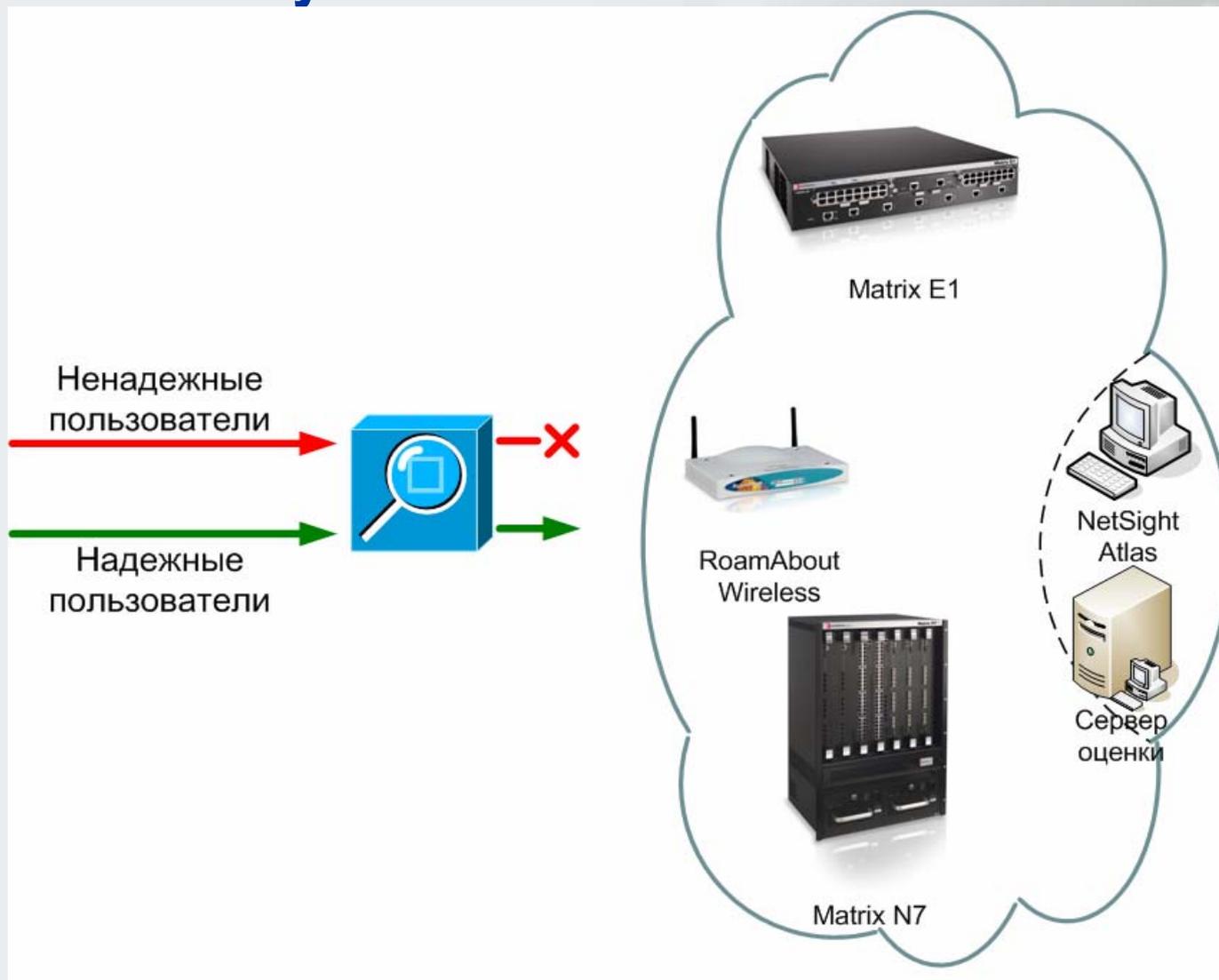
Бизнес-ориентированный подход к построению ЛВС



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.

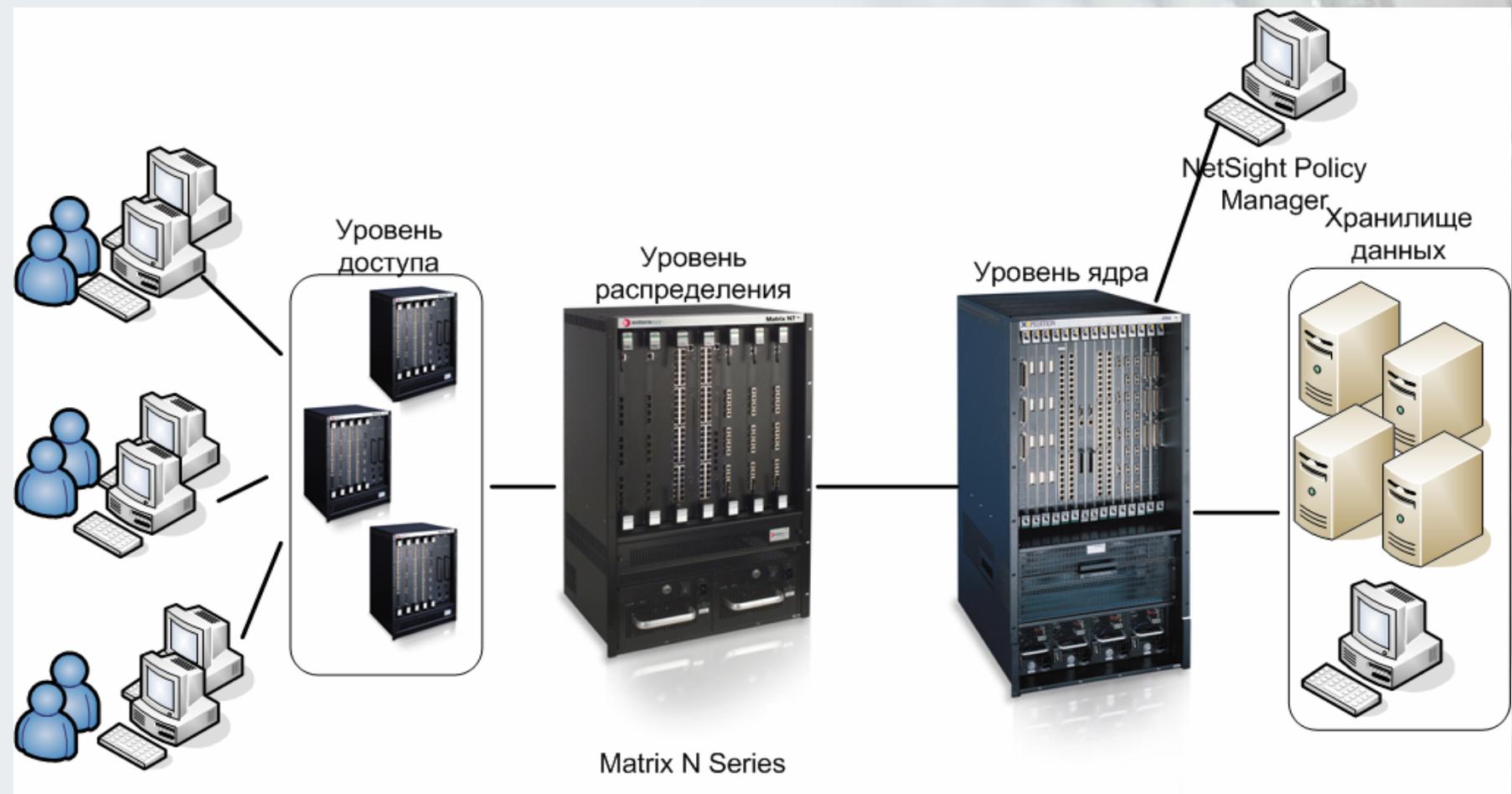
Secure Guest Access

- 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.

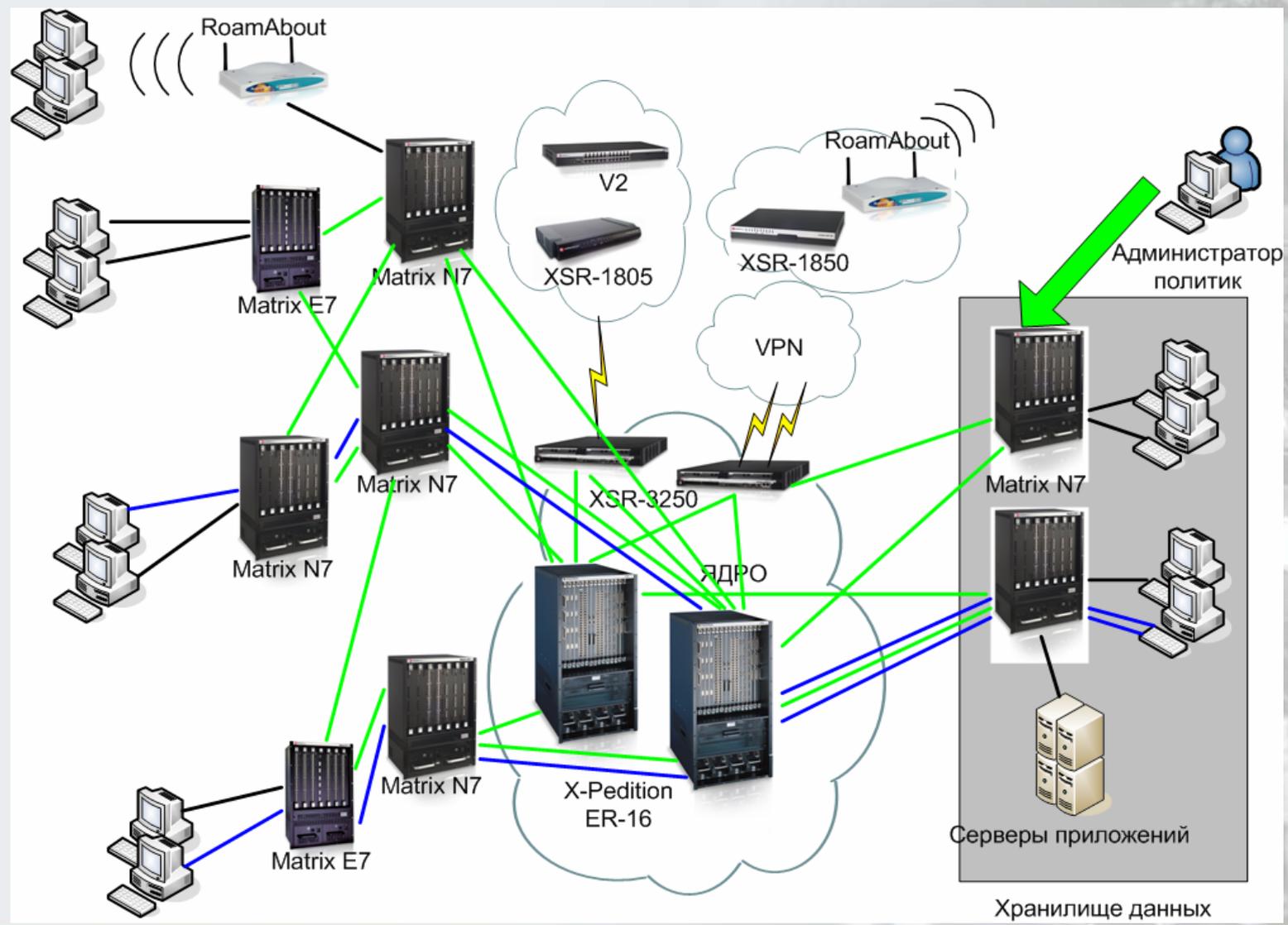
Single Sign-On

- 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.

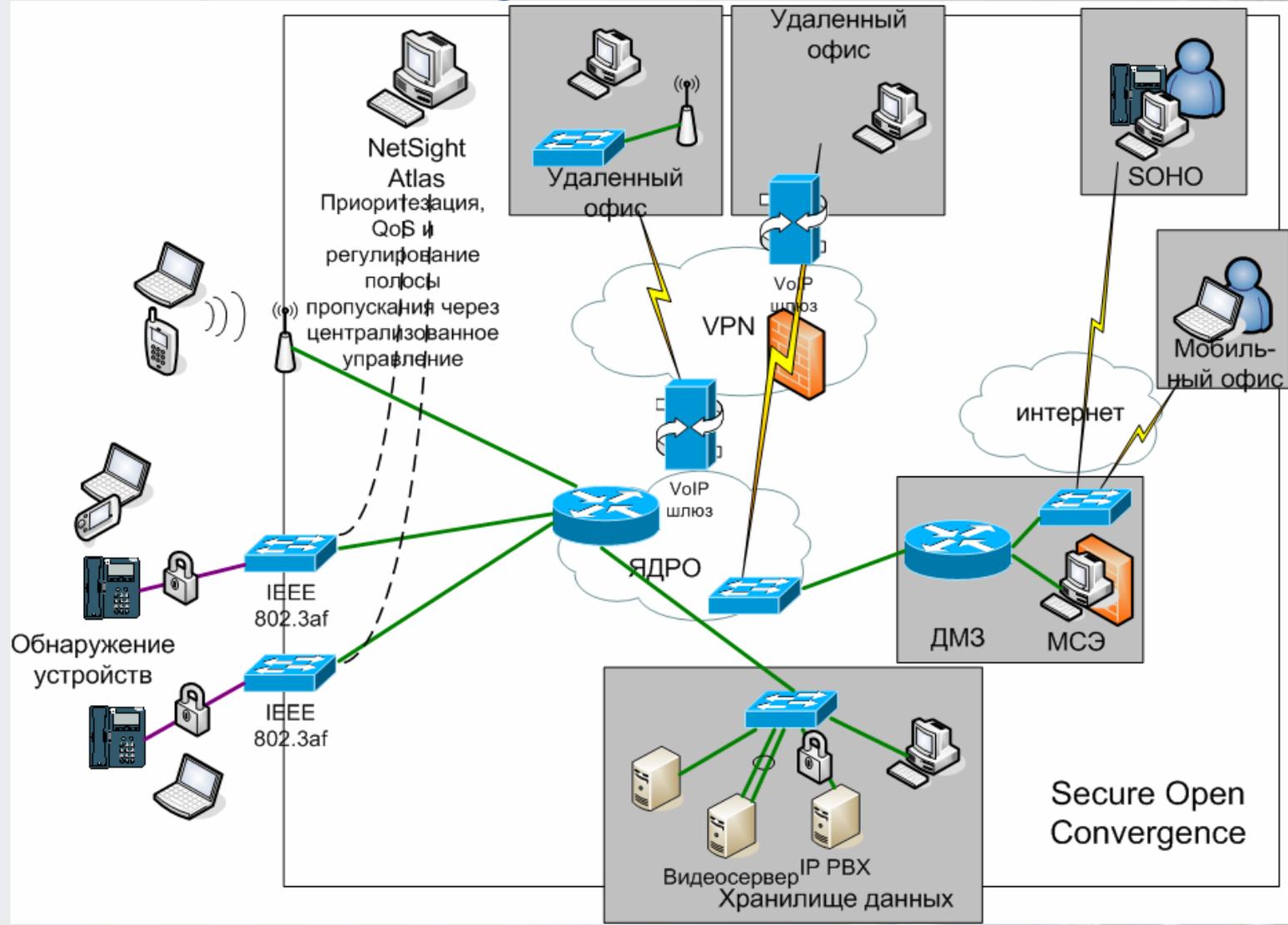
Distribution Layer Security



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

ОГЛАВЛЕНИЕ

Предпосылки
Концепция Secure Networks
Состав решения
Пример реализации
Преимущества решения

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

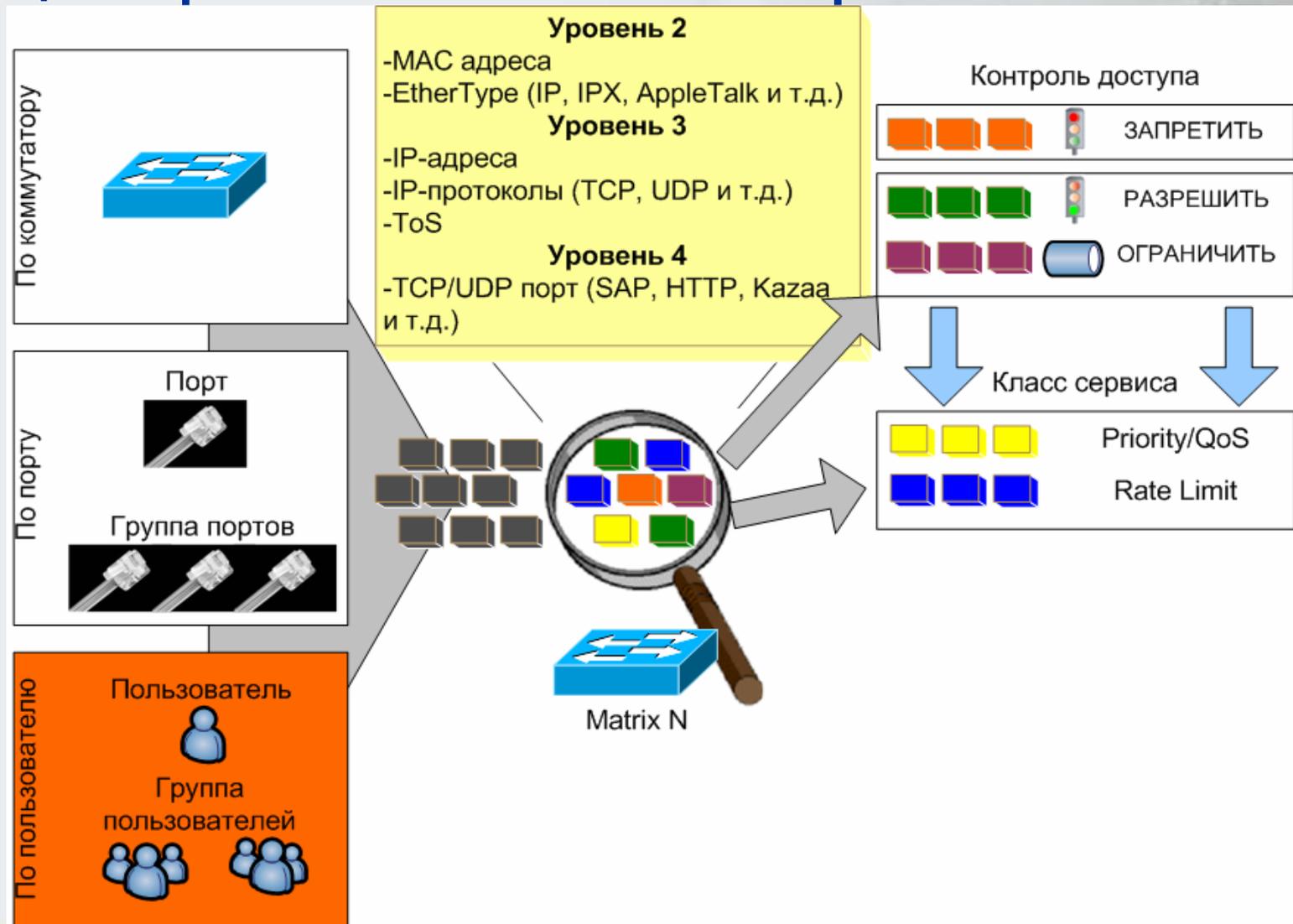
NetSight Policy Manager

- **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**

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

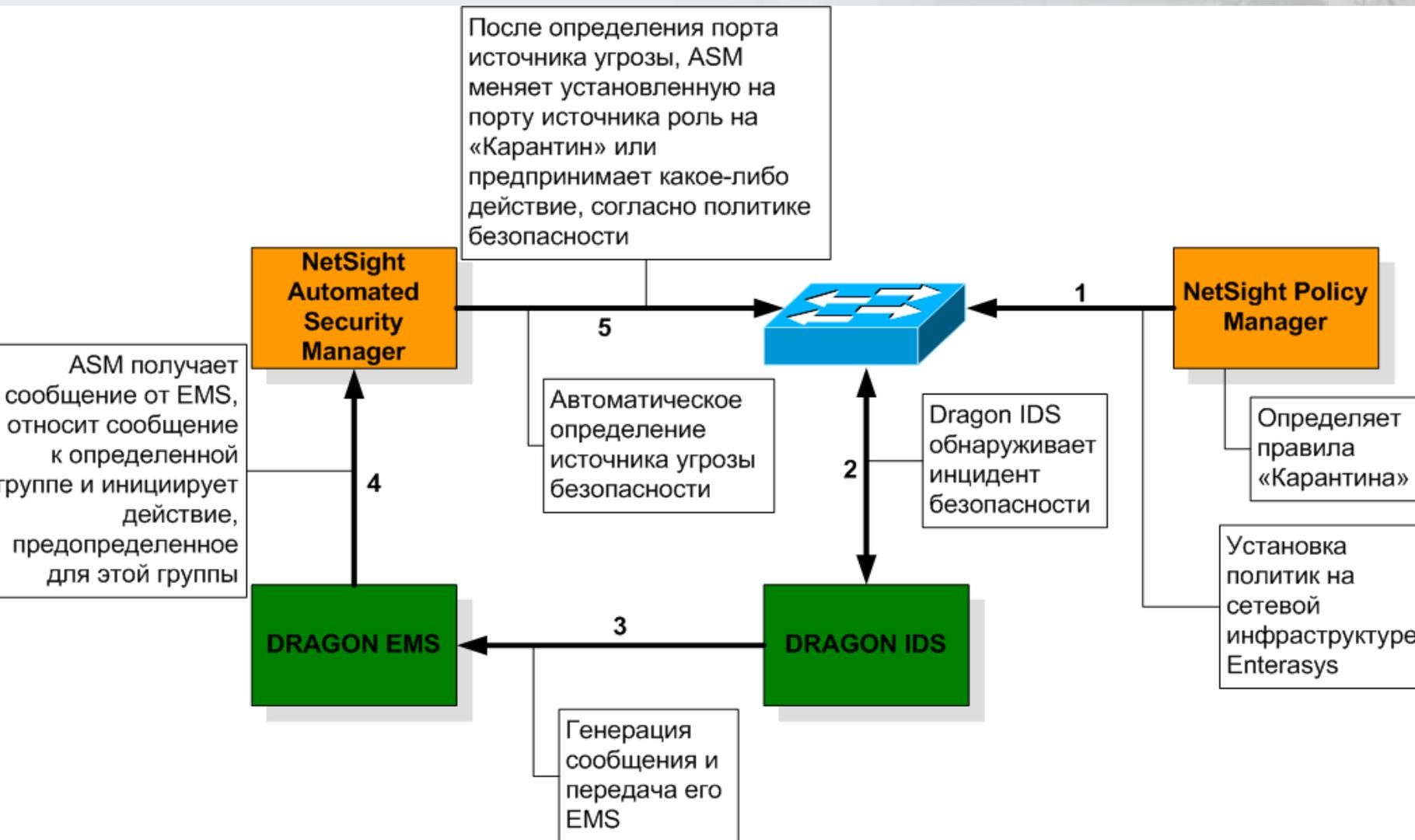
Функционирование сети на основе ролей



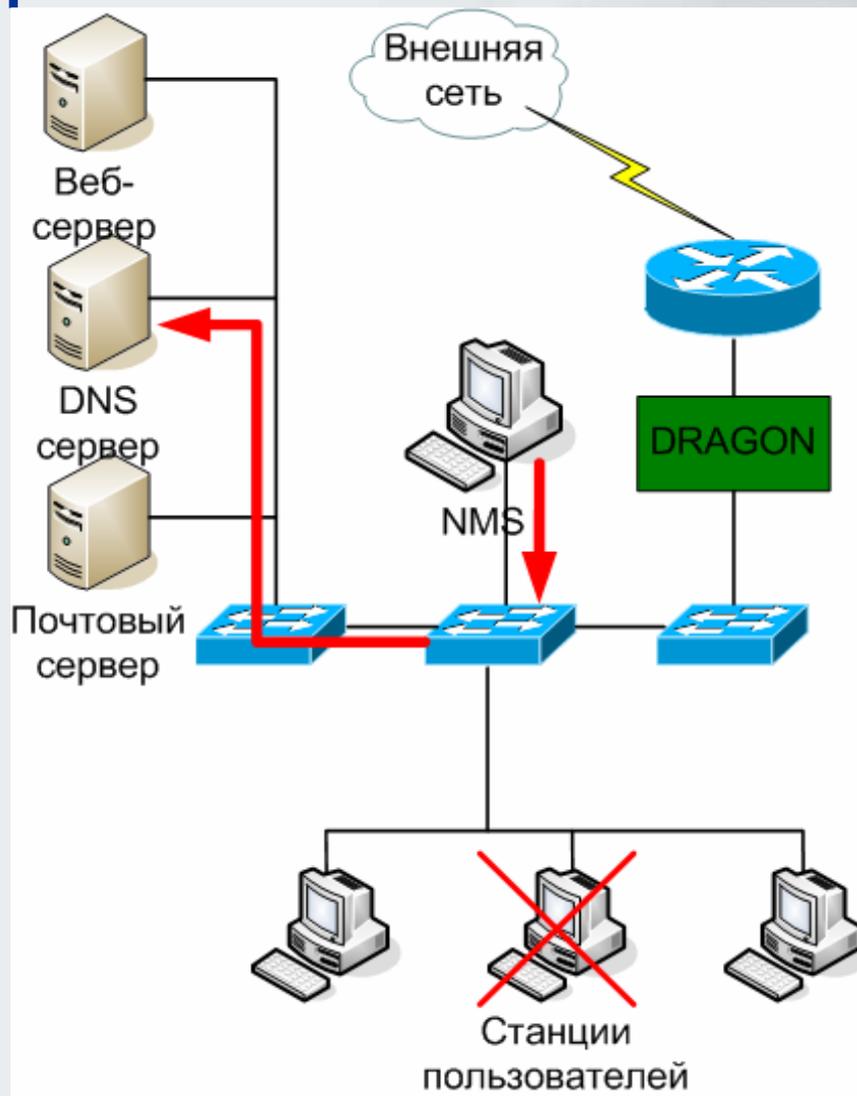
Dragon IDS

- **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

Dragon Enterprise Management Server

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

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

Предпосылки
Концепция Secure Networks
Состав решения
Пример реализации
Преимущества решения

Настройка NetSight Atlas Policy Manager

NetSight Atlas Policy Manager

File Edit View Tools Help

Close New Open Save Enforce (Global) Verify (Global) Delete Print Copy Paste Add Refresh Events Help

Roles Services **Network Elements** VLANs Classes of Service

Details View Authentication Port Usage RADIUS MAC Locking CEP Usage Rule Usage

Contents of '/Devices'

Name	IP Address	Device Type	Firmware Vers
134.141.179.15	134.141.179.15	Matrix E1	Enterasys Networks, Inc. 1H582-51 Rev 03.04.04

/home/knoppix/Desktop/ApplicationData/policymanager/Demo.pmd

file://ramdisk/home/kno NetSight Atlas Polic Shell - Konsole [2] 12:23 05/03/05

Настройка Dragon IDS

NetScape: Dragon 6.3 Enterprise Management Server

File Edit View Go Window Help

Back Forward Reload Home Search Netscape Print Security Shop Stop

Bookmarks Location:

STD Intro Internet Storm Center InfoSysSec CERT Online IP Tools

Alarmtool

Alarms Configuration Deployment Events Filters Notification Rules Time Periods Thresholds Realtime Forensics Trending Reporting / PolicyManager Alarmtool DRAGON

ALARMTOOL OPTIONS	EDIT NOTIFICATION RULE	ALARMTOOL WIZARD
<ul style="list-style-type: none"> [-] EVENT GROUPS [-] FILTERS [-] THRESHOLDS [-] TIME PERIODS [-] NOTIFICATION RULES [-] ALARMS [-] GLOBAL OPTIONS [-] DEPLOYMENT <p>LEGEND</p> <p>[-] Delete [-] Copy [-] Expand [-] Collapse</p>	<p>RULENAME: <input type="text" value="asm-etc-passwd"/> <input type="button" value="Save"/></p> <p>TIME PERIOD: <input type="text" value="None"/></p> <hr/> <p>NETSIGHT ATLAS ASM</p> <p>SERVER: <input type="text" value="134.141.178.235"/></p> <p>SECURITY NAME: <input type="text" value="dragon-user1"/></p> <p>AUTH PW: <input type="text" value="dragondragon1"/></p> <p>PRIV PW: <input type="text" value="dragondragon"/></p> <p>ASM CATEGORY: <input type="text" value="ASM_ATTACKS"/></p>	<ul style="list-style-type: none"> [-] MAIL [-] NETSIGHT ATLAS ASM [-] SNMP v.1 [-] SNMP v.3 [-] SYSLOG [-] USER [-] LOG [-] OFSEC SAM <p>MESSAGE FORMAT LEGEND Real-Time Alert Variables</p> <p>%ALERT% name of the alert defined in the configuration file %SENSOR% name of the sensor that generated the event %SID% source IP address recorded with the event %DIP% destination IP address recorded with the event %SPORT% source port number recorded with the event %DPORT% destination port number recorded with the event %PROT% protocol number recorded with the event %DIR% direction indicator recorded with the event %NAME% event name(s) that caused the event (multiple names concatenated with "4") %DATE% the date recorded with the event (format YYYY-MM-DD) %TIME% the time recorded with the event (format HH:MM:SS) %DATA% event specific data such as a file name for a MIDS event</p> <p>Summary Alert Variables</p> <p>%ALERT% name of the alert defined in the configuration file %COUNT% the number of times the alert occurred in the summary interval %DATE% current date (format YYYY-MM-DD) %TIME% current time (format HH:MM:SS) %STARTDATE% beginning date for the summary interval (format YYYY-MM-DD) %STARTTIME% beginning time for the summary interval (format HH:MM:SS)</p>

1 2 3 NetSight Atlas Netscape: Dr file://tmp/screen Konsole [2] 3:59 05/07/05

Настройка Automated Security Manager

NetSight Atlas Console and Automated Security Manager - Database "Default"

File Edit Tools Applications Help

ASM Mode: Search And Respond
Activity Count: 0

My Network (1) Properties Map VLAN Compass Interface Summary

Automated Security Manager

Operation Mode

- Disabled
- Search Only
- Search And Respond

Statistics **Configure**

Current: Since (05/07/2005 04:22:11 PM)

Search Pending: 0 Average Search Time (sec): 0
Action Taken: 0 Incident Rate: N/A
Awaiting Confirm: 0

Activity Monitor

Filter

Show Threat Details Show Action Details Show Excluded (0 entries for excluded ports) **Test...**

Incide...@	Icon	Status	Date/Time	Sender ID	Sender Name	Event Category	Si

Cancel Search Confirm Response Undo Action Delete Table Entry ASM Options... Configure...

Close Help

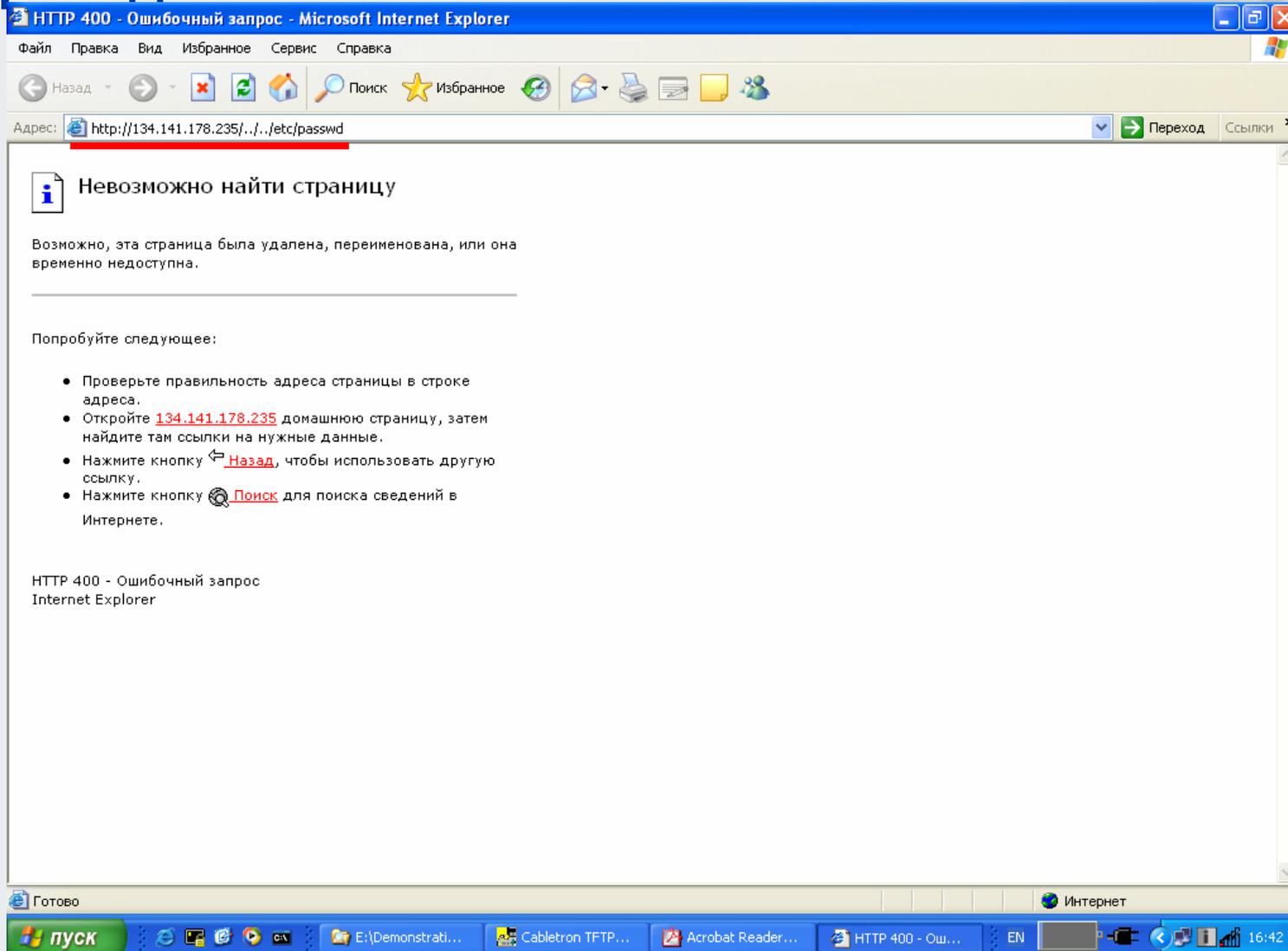
Acknowledge Severity Category Date/Time Host IP Address User Name Type Event Information

Console Policy Inventory Automated Security Traps Syslog

0%

NetSight Netscape file://tmp/ Konsole Com.en 4:29 05/07/05

Проведение атаки



HTTP 400 - Ошибочный запрос - Microsoft Internet Explorer

Файл Плавка 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

Готово Интернет

пуск E:\Demonstrati... Cabletron TFTP... Acrobat Reader... HTTP 400 - Ош... EN 16:42

Обнаружение атаки

NetSight Atlas Console and Automated Security Manager - Database 'Default'

File Edit Tools Applications Help

ASM Mode: Search And Respond
Activity Count: 1

My Network (1)
 All Devices (1)
 Grouped By (1)
 Not Polled Devices
 134.141.179.15

Properties Map VLAN Compass Interface Summary

Device Access Date/Time Port

IP Address	Display Name	Device Type	Status	Uptime	Firmware	Boot PROM	Base MAC	Chassis
134.141.179.15	134.141.179.15	1H582-51	Contact Established	0 Days 0:42:59.12	03.04.04.1	01.04.00	00:01:F4:8A:F1:40	

Acknowledge	Severity	Date/Time	User Name	Type	Information
<input type="checkbox"/>	Info	05/09/2005 02:57:1...	root	Event	1: 134.141.179.15 SNMP Set Success. ifAdminStatus.5 [2]
<input type="checkbox"/>	Info	05/09/2005 02:57:1...	root	Event	1: Matched rule asm-etc-passwd for 134.141.179.15/5. Action is Disable Port.
<input type="checkbox"/>	Info	05/09/2005 02:57:0...	root	Event	1: Search for 134.141.179.235 from SNMPv3 Inform received 05/09/2005 02:57:07 PM
<input type="checkbox"/>	Info	05/09/2005 02:57:0...	root	Event	1: 2005-05-09 14:57:07 134.141.178.235 [134.141.178.235]: INFORM, SNMPv3, user dragon-user, con.
<input type="checkbox"/>	Info	05/09/2005 02:56:0...	root	Event	Created rule "asm-etc-passwd"
<input type="checkbox"/>	Info	05/09/2005 02:54:1...	root	Event	Automated Security Manager set to search and respond.
<input type="checkbox"/>	Info	05/09/2005 02:54:0...	root	Event	NetSight Atlas Console launched. Automated Security Manager is currently disabled.

Console Policy Inventory Automated Security Traps Syslog

0%

1 2 3 NetSight Netscape NetSight file:/tmp/... Konsense 3:5 05/09/05



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.

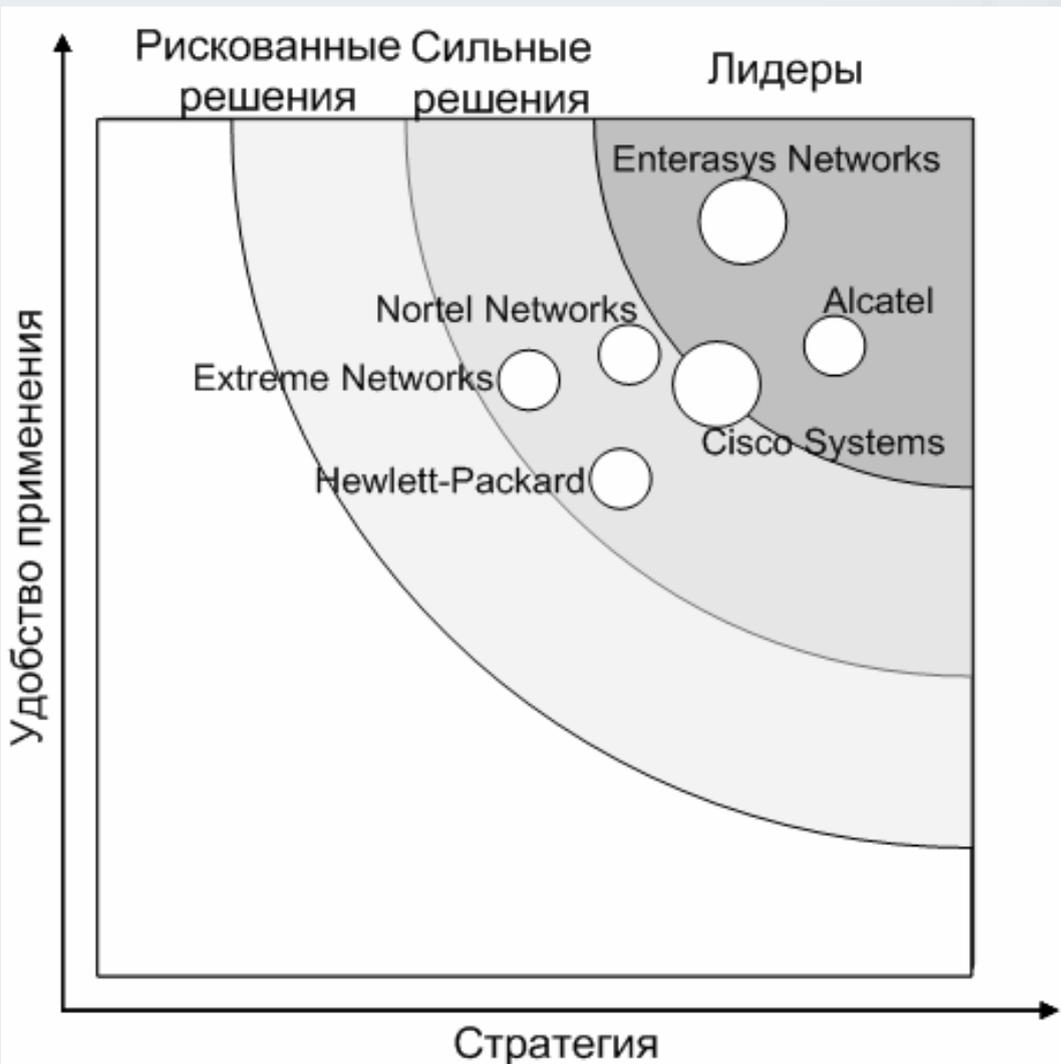
HTTP 400 - Ошибочный запрос
Internet Explorer

Подключение по локальной сети
Сетевой кабель не подключен

ОГЛАВЛЕНИЕ

- Предпосылки
- Концепция Secure Networks
- Состав решения
- Пример реализации
- Преимущества решения**

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.