ECOPROG
consulting, engineering, management

ЗАЩИЩЕННЫЕ СЕТИ
SECURE NETWORKS

Январь 2007

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

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.

ECOPROG
consulting, engineering, management

АРХИТЕКТУРА РЕШЕНИЯ SECURE NETWORKS

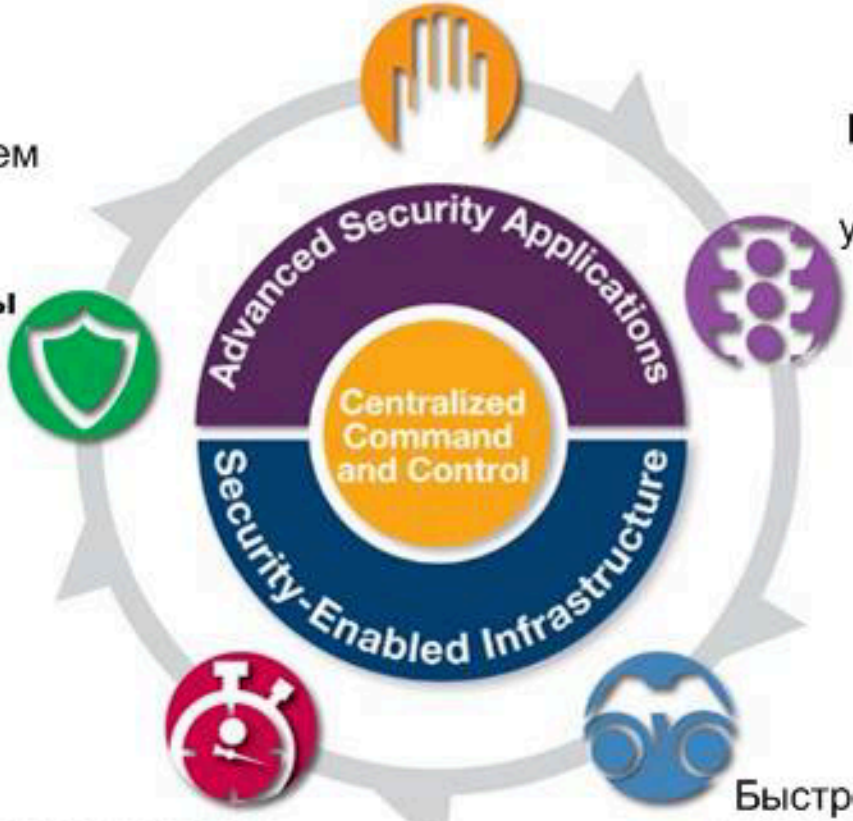
- Инфраструктура с поддержкой функций информационной безопасности
- Централизованное управление и контроль
- Средства информационной безопасности

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

СИСТЕМНЫЙ ПОДХОД К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Установка и внедрение политик использования сети

Оценка конечных систем пользователей для обеспечения **проактивной защиты**



Контроль доступа для всех пользователей, устройств и приложений

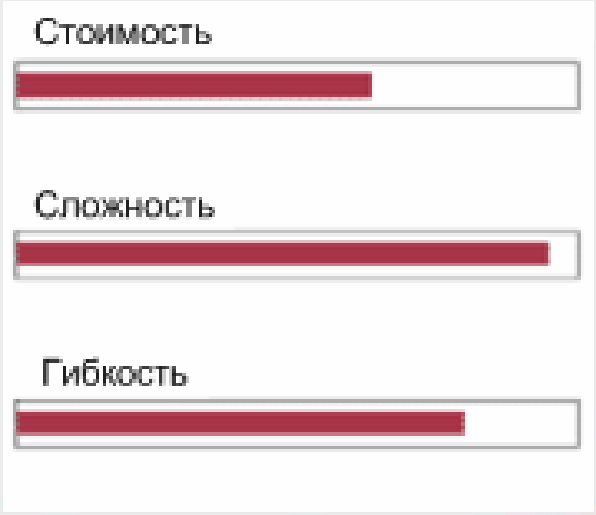
Автоматическая реакция на инциденты

Быстрое **обнаружение и локализация инцидентов** или аномального поведения во всей сети

ПОДДЕРЖКА И ВНЕДРЕНИЕ ПОЛИТИК

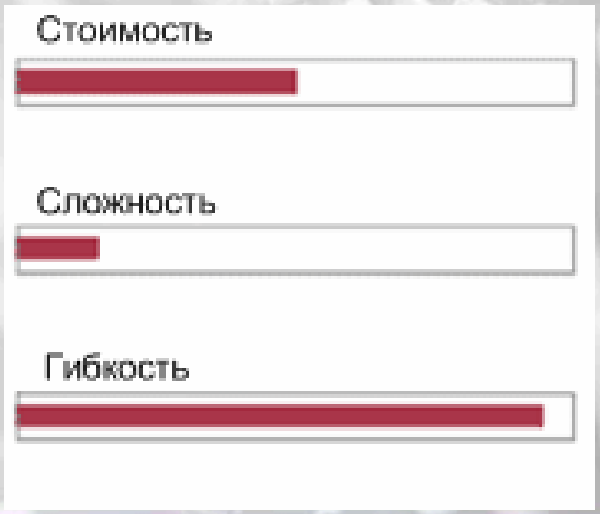
Традиционный подход

- Необходимо внедрение специализированного ПО для поддержки политик
- Установка серверов политик «в разрыв» сети
- У различных производителей различные понятия о политиках



Системный подход

- Поддержка политик интегрирована в сетевое оборудование
- Внедрение политик повсеместно в сети
- Централизованное управление политиками

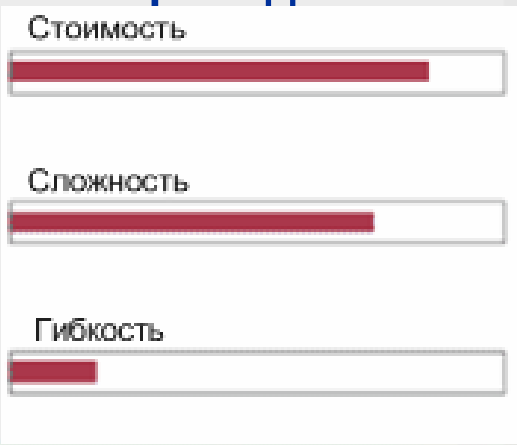


1-й Голутвинский пер., 3/5, стр. 1. Тел./факс: (095) 705-90-30. http://www.ecoprog.ru

КОНТРОЛЬ ДОСТУПА

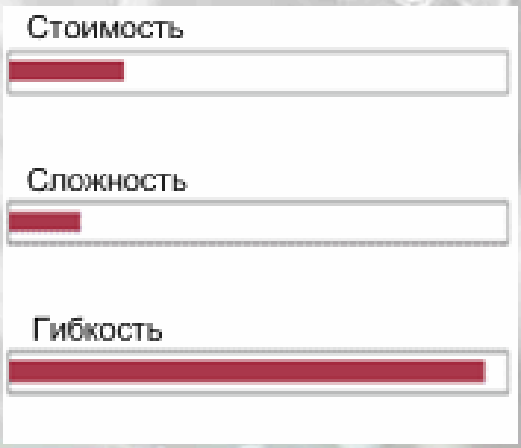
Традиционный подход

- Поддержка одного вида аутентификации
- Ограниченная поддержка конечных систем
- Управление контролем доступа не зависит от управления политиками
- Различные возможности на проводных и беспроводных сетях



Системный подход

- Поддержка разнообразных видов аутентификации
- Полная поддержка конечных систем
- Интегрированное управление контролем доступа и политиками
- Возможности контроля доступа не зависят от среды передачи

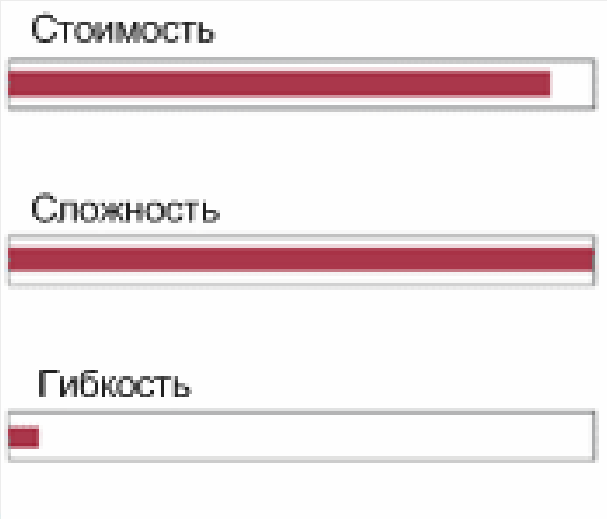


1-й Голутвинский пер., 3/5, стр. 1. Тел./факс: (095) 705-90-30. http://www.ecoprog.ru

ОБНАРУЖЕНИЕ И ЛОКАЛИЗАЦИЯ ИНЦИДЕНТОВ

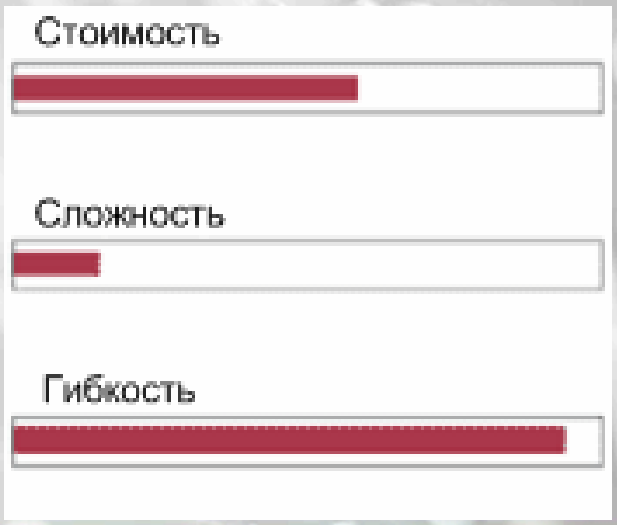
Традиционный подход

- Распределенные программно-аппаратные комплексы (ПАК) обнаружения вторжений без корреляции событий по источнику инцидентов
- Требует ручного поиска источника инцидентов



Системный подход

- Консолидированное и централизованное обнаружение вторжений средствами сетевого оборудования и ПАК
- Автоматическое распознавание источника инцидентов



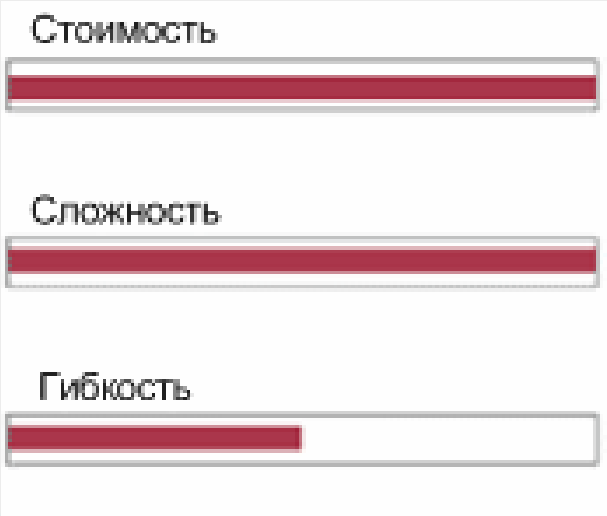
1-й Голутвинский пер., 3/5, стр. 1. Тел./факс: (095) 705-90-30. http://www.ecoprog.ru

ECOPROG
consulting, engineering, management

АВТОМАТИЧЕСКАЯ РЕАКЦИЯ

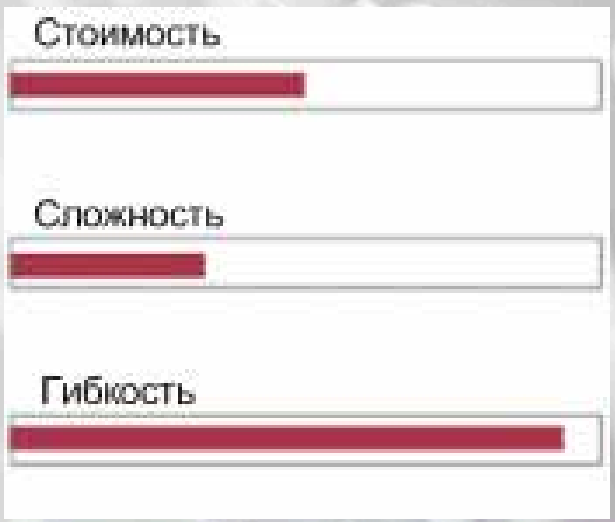
Традиционный подход

- Ограниченное количество вариантов реакции на угрозы
- Устранение угрозы требует вмешательства администратора
- Ограничение трафика ненадежной рабочей станции пределами одной VLAN



Системный подход

- Гибкие настройки процесса реагирования на угрозы
- Полностью автоматическая реакция на угрозы
- Безопасная изоляция ненадежной рабочей станции



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

ECOPROG
consulting, engineering, management

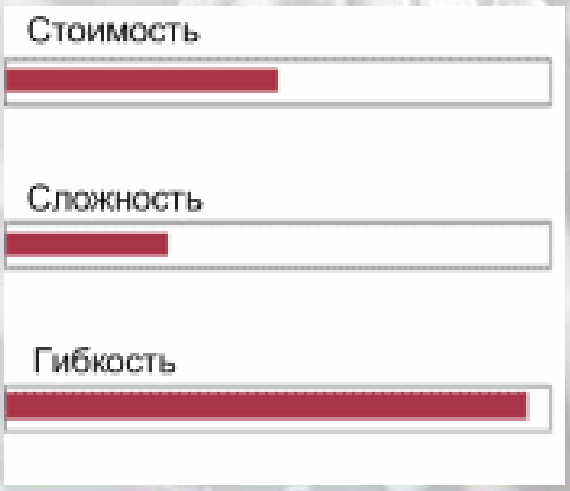
ПРОАКТИВНАЯ ЗАЩИТА

Традиционный подход

- Программно-аппаратные системы предотвращения вторжений
- Функционал фирменных технологий безопасности ограничен возможностями ОС устройства
- Политики не распространяются на уровень доступа

Системный подход

- Встроенное гибкое управление безопасностью на уровне доступа
- Открытая технология оценки для всех конечных станций
- Единая политика карантина для всей сети
- Эффективное управление изменениями настроек безопасности



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

СОСТАВ АРХИТЕКТУРЫ SECURE NETWORKS

Инфраструктура с поддержкой функций информационной безопасности

- ✓Коммутаторы
- ✓Маршрутизаторы
- ✓Беспроводная связь

Централизованное управление и контроль

- ✓NetSight Console
- ✓NetSight Policy Manager
- ✓NetSight Automated Security Manager

Средства информационной безопасности

- ✓Dragon Security Suite
- ✓Enterasys Sentinel

ECOPROG
consulting, engineering, management

ИНФРАСТРУКТУРА С ПОДДЕРЖКОЙ ФУНКЦИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Коммутаторы

- SecureStack A
- SecureStack B
- SecureStack C
- Matrix N-Series
- Matrix E-Series
- RoamAbout Wireless Switch

Маршрутизаторы

- Matrix X Secure Core Router
- XSR 1800
- XSR 3000

Беспроводная связь

- RoamAbout Access Point
- RoamAbout Multimode Radio Card

Security-Enabled Infrastructure

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

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ И КОНТРОЛЬ

Базовый модуль

- NetSight Console – мониторинг и управление оборудованием Enterasys

Подключаемые модули

- NetSight Policy Manager – управление политиками
- NetSight Automated Security Manager – обработка инцидентов безопасности
- NetSight Inventory Manager – управление изменениями, инвентаризация
- NetSight Router Services Manager – управление маршрутизаторами

Centralized Command & Control

ECOPROG
consulting, engineering, management

NETSIGHT CONSOLE

- обеспечивает управление оборудованием, мониторинг и локализацию неисправностей, автоматическое обнаружение устройств, управление событиями, журналирование, поддержку приложений;
- обеспечивает управление портами, устройствами, классами устройств, пользователями;
- поддержка подключаемых модулей для расширения функциональных возможностей;
- поддержка следующих операционных систем:
  - Windows XP, 2000, 2003 Server;
  - Solaris 2.8, 2.9
  - RedHat Linux ES, WS, SUSE Linux

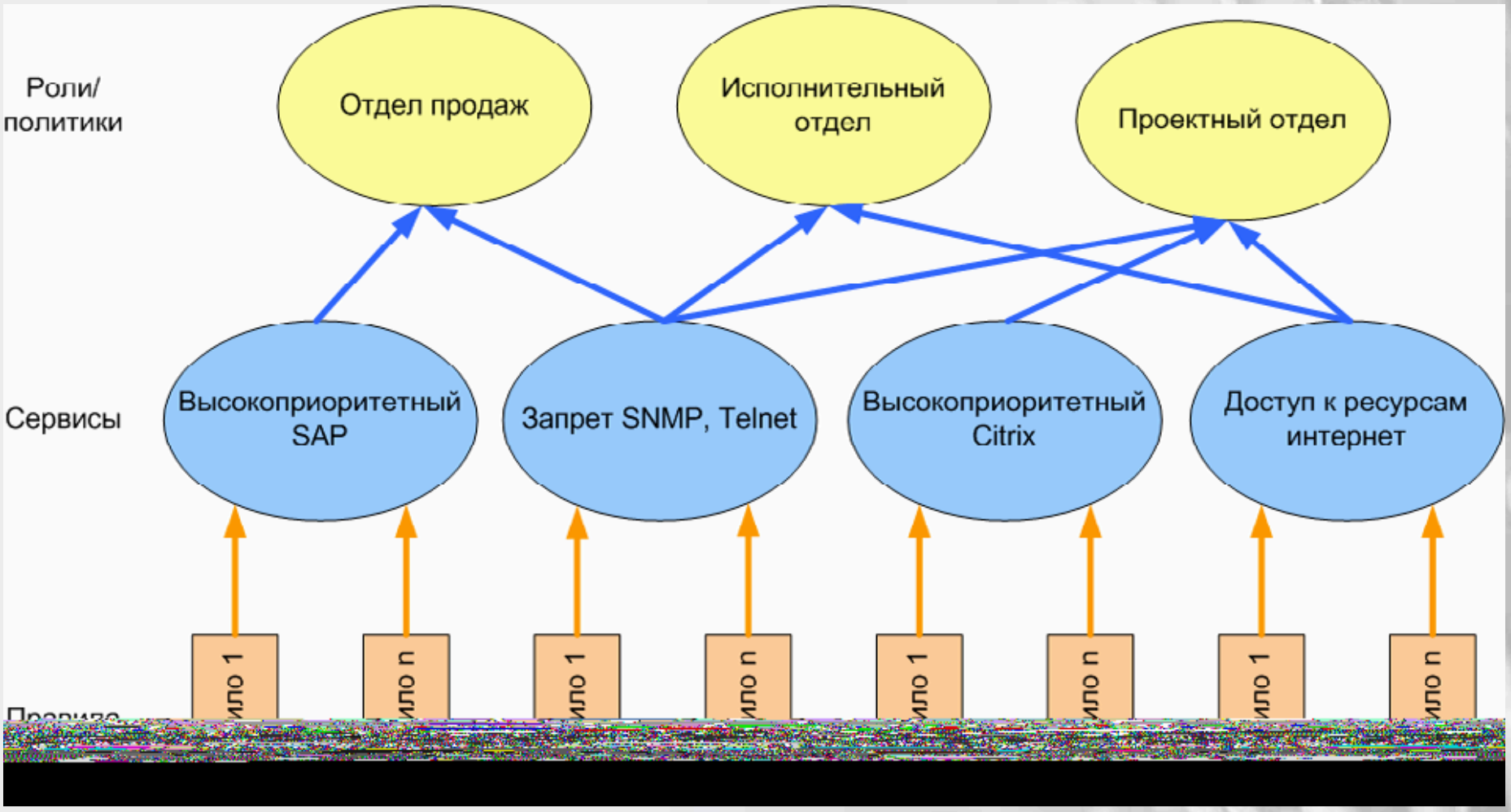
1-й Голутвинский пер., 3/5, стр. 1. Тел./факс: (095) 705-90-30. http://www.ecoprog.ru

NETSIGHT POLICY MANAGER

- установление соответствия между бизнес-задачами пользователей и ИТ-сервисами;
- управление учетными записями пользователей с использованием ролей пользователей;
- поддержка различных протоколов аутентификации, включая 802.1x, RADIUS, аутентификацию по MAC-адресу;
- позволяет работать сети в режиме «распределенного межсетевого экрана»;
- применение политик одним нажатием клавиши на всем протяжении сети;
- поддержка нескольких политик, обеспечивающих QoS, CoS, ограничение полосы пропускания, VLAN, фильтрацию;
- обеспечение средств аудита (event log).

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

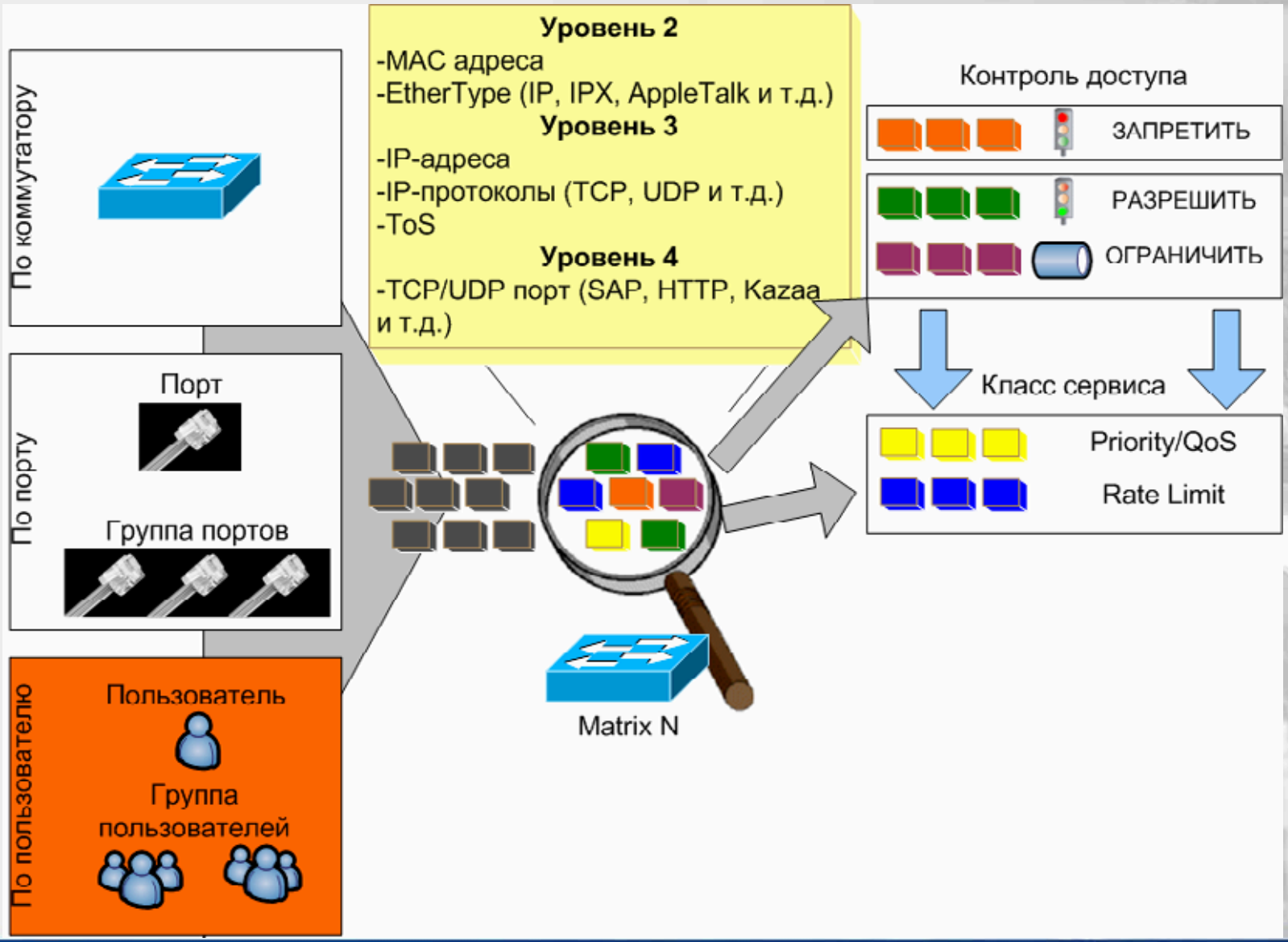
СООТВЕТСТВИЕ БИЗНЕС-ЗАДАЧ И ИТ-СЕРВИСОВ



РОЛИ И ПОЛИТИКИ В SECURE NETWORKS

- роли пользователей, описанные в NetSight Policy Manager, являются наглядным представлением политик, применяемых на сетевых устройствах;
- роли описывают список ИТ-сервисов и его свойства, к которым имеет доступ пользователь или группа пользователей в соответствии с предопределенными правилами;
- роли могут назначаться для пользователя, группы пользователей, физического порта, группы портов или для устройства;
- после анализа сетевого траффика коммутатором, предпринимается действие, описанное в настройках роли (блокирование, разрешение, ограничение пределами одной VLAN, ограничение полосы пропускания, применение правил приоритезации).

ПРИНЦИП РАБОТЫ СЕТИ СЕТИ НА ОСНОВЕ РОЛЕЙ



NETSIGHT AUTOMATED SECURITY MANAGER

- идентификация физического местоположения источника атаки;
- обеспечение функционирования ИТ-сервисов компании во время инцидентов безопасности методом изоляции источника атаки;
- ограничение угроз с применением политик Secure Networks;
- поддержка изменения политики/роли пользователя в зависимости от конфигурации его рабочей станции;
- возможность назначения политики каждому пользователю для более гибкой настройки сервисов и предотвращения атак;
- журналирование событий, система отчетов;
- обеспечение гибкого контроля на уровне портов устройств по типу события или угрозы.

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

ECOPROG
consulting, engineering, management

СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

SC MAGAZINE AWARDS 2006 EUROPE WINNER

Dragon Security Suite

- Dragon Intrusion Defense – решение по обнаружению и предотвращению вторжений в сетевую инфраструктуру
  - Dragon Enterprise Management Server – сервер управления системой предотвращения вторжений
  - Dragon Network Intrusion Detection & Prevention – система обнаружения и предотвращения вторжений
  - Dragon Host Sensor – хост-сенсор
  - Web Server Intrusion Prevention – сенсор для веб-серверов
- Dragon Network Defense – решение по обнаружению аномалий сетевого трафика и управлению системой сетевой безопасности;

Enterasys Sentinel Proactive Prevention

- Enterasys Sentinel Trusted Access Manager and Gateway – система доверенного доступа к ресурсам корпоративной сети

Advanced Security Applications

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

ECOPROG
consulting, engineering, management

DRAGON ENTERPRISE MANAGEMENT SERVER

- распределенная клиент-серверная архитектура;
- централизованное управление лицензиями для сенсоров;
- автоматическое обновление сигнатур атак;
- встроенный редактор для ручной настройки сигнатур;
- анализ событий в реальном масштабе времени и во временном интервале;
- группировка событий по различным параметрам для упрощения анализа;
- реконструкция соединений с возможностью анализа пакетов данных;
- соответствует требованиям стандартов ГОСТ 29216-91 и 50628-95.

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

DRAGON NETWORK INTRUSION DETECTION AND PREVENTION

- защита сети от злоумышленников и предотвращение их повторного появления;
- гигабитная производительность работы при одновременном декодировании протоколов, анализе сигнатур и поведения пользователей;
- поддержка нескольких виртуальных сенсоров на одном физическом устройстве;
- анализ VoIP-протоколов для обнаружения атак;
- поддержка расширенных возможностей по написанию сигнатур (статистические данные, шаблоны, отслеживание состояния сессии);
- идентификация и блокирование атак с применением фрагментированного трафика;
- разрыв TCP-сессий с отправкой ICMP unreachable;
- предотвращение сканирования сетей с генерацией ложных ответов.

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

ECOPROG
consulting, engineering, management

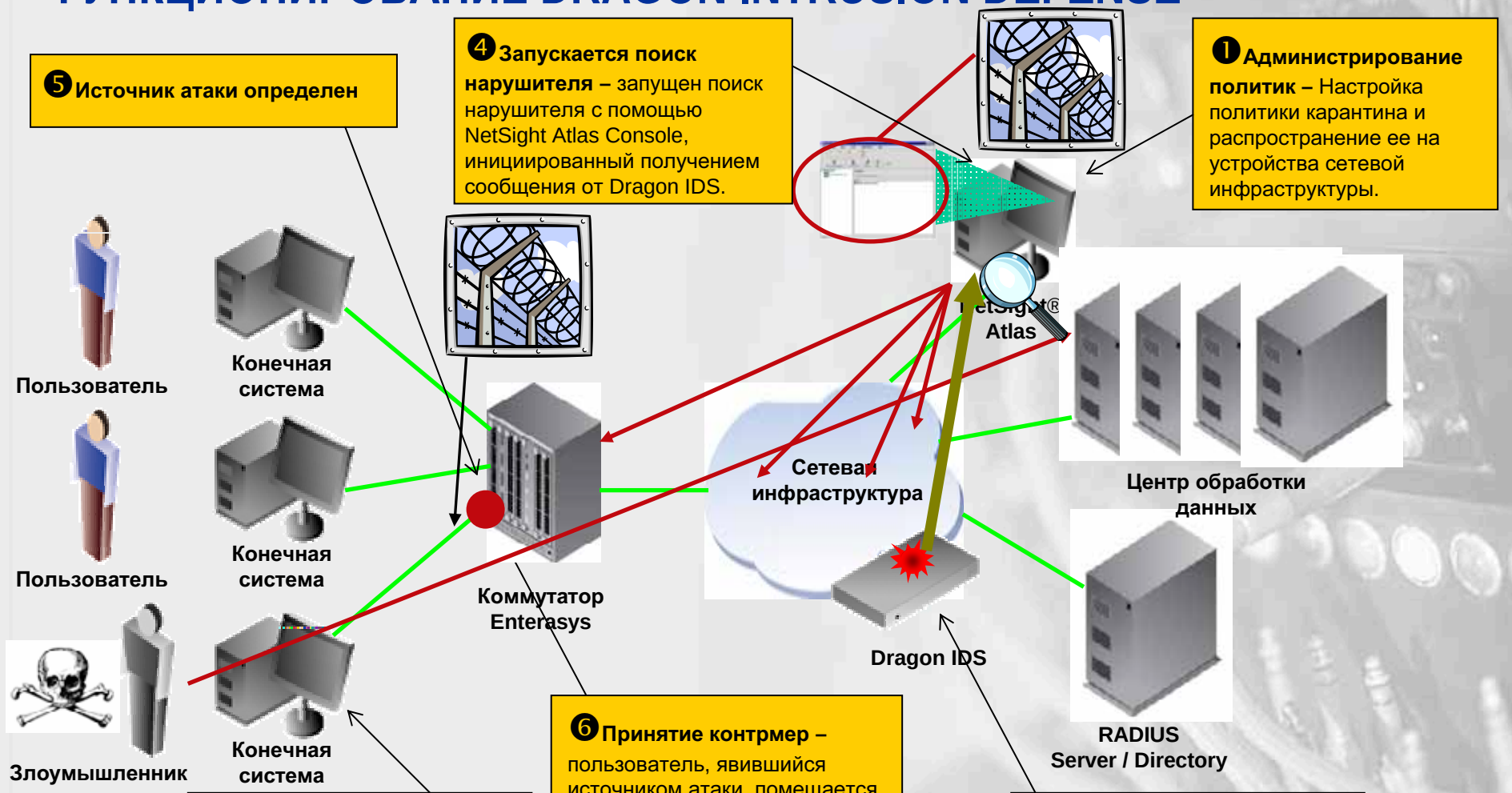
DRAGON HOST SENSOR AND WEB SERVER INTRUSION PREVENTION

- предотвращение атак на популярные веб-серверы Microsoft IIS и Apache;
- мониторинг атрибутов разрешений на доступ к файлам (u+g+o);
- контроль целостности файлов с помощью MD5-хэша;
- сигнатурный анализ файлов и каталогов;
- мониторинг журнала событий (event log) Windows;
- анализ доступа к ключам реестра Windows;
- мониторинг открытых TCP и UDP портов (защита от «черных ходов»);
- обнаружение инцидентов, связанных с превышением полномочий;
- наличие интерфейса для самостоятельной разработки модулей с использованием технологии Microsoft .NET.

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

ECOPROG
consulting, engineering, management

ФУНКЦИОНИРОВАНИЕ DRAGON INTRUSION DEFENSE



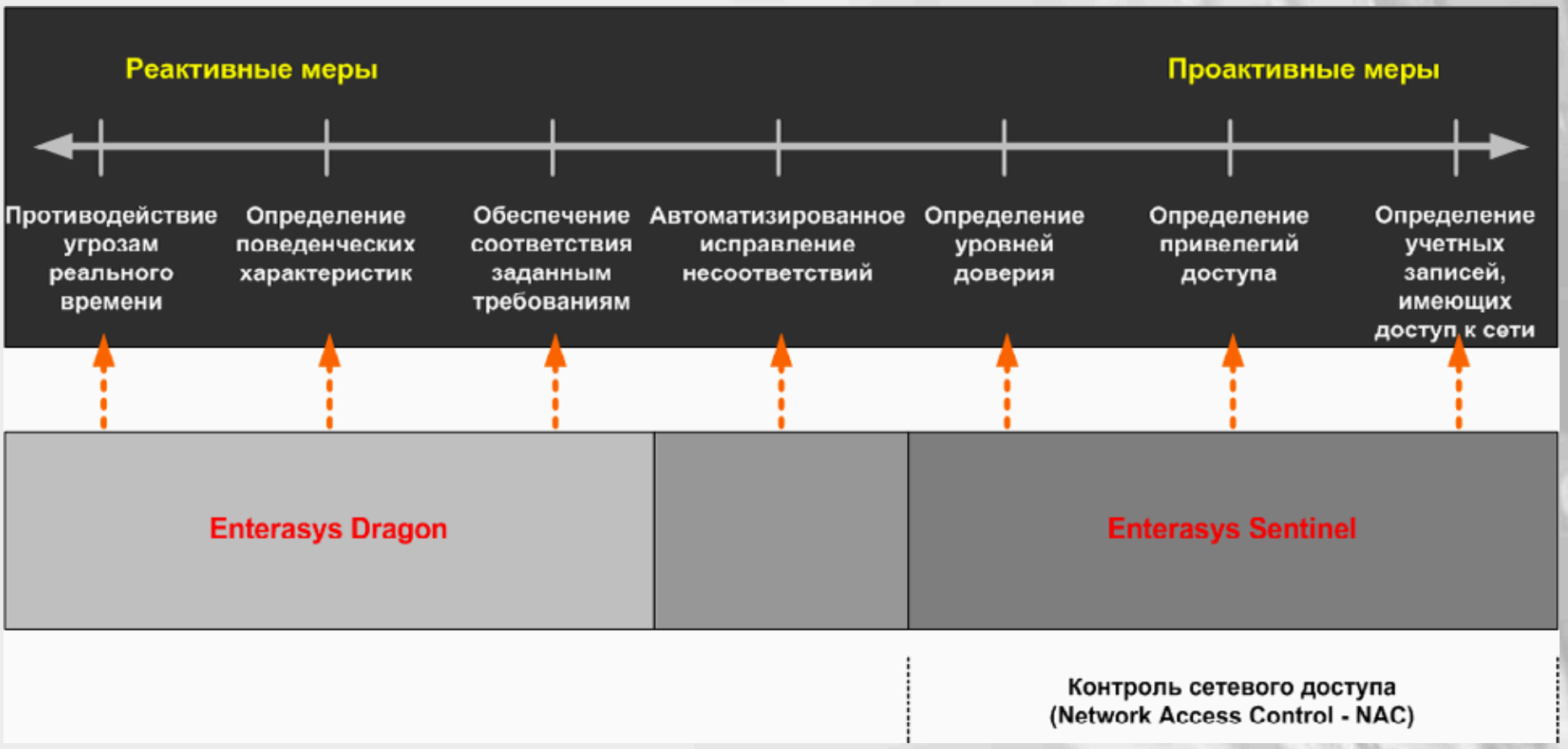
1-й Голутвинский пер., 3/5, стр. 1. Тел./факс: (095) 705-90-30. http://www.ecoprog.ru

DRAGON NETWORK DEFENSE

- Решение состоит из Security Command Console, Behavioral Flow Processor и Behavioral Flow Sensor
- Позволяет создавать и распространять сетевые политики и политики безопасности с одной консоли;
- Мониторинг уязвимостей;
- Анализ потоков данных для предотвращения “zero day” атак, сетевых червей, вирусов, DDoS-атак;
- Более 10000 сигнатур различных сетевых событий доступны через автоматическую систему обновлений;
- Возможности интеллектуальной обработки событий позволяют генерировать реакцию на инциденты, которые не описаны в сигнатурах;
- Генерация отчетов об инцидентах безопасности, автоматическая приоритезация событий, помощь в устранении последствий инцидентов;
- Поддержка широкого спектра оборудования и ПО сторонних разработчиков (CISCO, Check Point, Nokia, Netscreen, ISS, Network Associates, McAfee, SNORT, SourceFire, Microsoft);
- Интеграция с NetSight Automated Security Manager.

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

СПЕКТР ВОЗМОЖНОСТЕЙ SECURE NETWORKS



КОНТРОЛЬ СЕТЕВОГО ДОСТУПА (NAC)

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

ECOPROG
consulting, engineering, management

ENTERASYS SENTINEL TRUSTED ACCESS GATEWAY AND MANAGER

Trusted Access Gateway

- Программно-аппаратный комплекс
- Специализированный модуль для Matrix N
- Защищенная версия ОС Linux
- RADIUS-прокси
  - Аутентификация (802.1X, MAC, веб)
  - Авторизация (динамические политики/назначение VLAN)
- Сервисы оценки
  - Nessus
  - Lockdown

Trusted Access Manager

- Программный комплекс с клиент-серверной архитектурой
- Версии для Windows, Linux, Solaris
- Конфигурирование Trusted Access Gateway (домены безопасности, серверы оценки, AAA, MAC locking)
- Мониторинг рабочих станций (статус, авторизация, статистика сканирования)

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

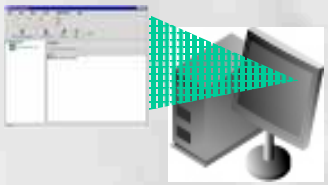
ECOPROG
consulting, engineering, management

ПРИМЕР NAC БЕЗ ИСПОЛЬЗОВАНИЯ АГЕНТОВ

❻ **Назначение политики –** в случае несоответствия параметров конечной системы пользователя требованиям политики безопасности, к системе применяется политика “Quarantine”; в ином случае производится реаутентификация и применение соответствующей политики в соответствии с настройками RADIUS Server.

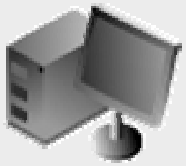
❶ **Администрирование политик –** Основными шагами настройки политик являются описания ролей “Assessing”, “Quarantine” и “Failsafe”. Далее политики распространяются и активизируются в точках применения политик сетевой инфраструктуры.

Enterasys NetSight® Policy Manager

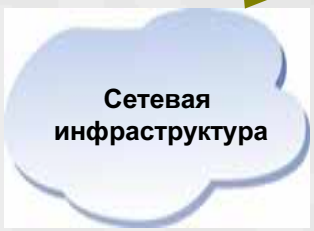


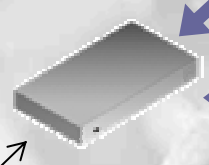
❺ **Оценка –** Trusted Access Gateway осуществляет запрос к серверу оценки, чтобы он просканировал конечную систему на соответствие корпоративной политике безопасности.

Сервер оценки



Сетевая инфраструктура





Пользователь

Конечная система

Коммутатор Enterasys

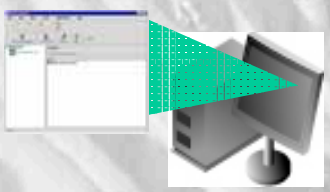
Enterasys Sentinel™ Trusted Access Gateway (RADIUS-прокси)

RADIUS Server / Directory

❸ **Доступ –** конечная система пользователя пытается подключиться к сети.

❹ **Запрос аутентификации –** MAC-адрес клиента появился на коммутаторе с поддержкой политик, временно применена роль “Assessing”, для того чтобы сервер оценки мог проверить клиента на соответствие корпоративной политике безопасности.

❷ **Настройка Trusted Access Gateway –** изменения, касающиеся процессов аутентификации и оценки сохраняются на шлюзах.



Enterasys Sentinel™ Trusted Access Manager

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

ПРОВЕРКА ЦЕЛОСТНОСТИ СИСТЕМЫ БЕЗ ИСПОЛЬЗОВАНИЯ АГЕНТОВ

С помощью сервера оценки

- Nessus
  - Сканирование уязвимостей
  - Параметры антивируса
  - Реестр Windows
  - Файловая система Linux
- Lockdown
  - Сканирование уязвимостей
  - Параметры антивируса
  - Реестр Windows
  - Файловая система Linux

Технология Java/ActiveX

- Sygate
  - Java-апплет
  - Параметры антивируса и персонального брандмауэра, наличие заплаток
- Zone Labs
  - ActiveX-компонент
  - Параметры антивируса и персонального брандмауэра, наличие заплаток, версия ПО, шаблон политики безопасности

ПРОВЕРКА ЦЕЛОСТНОСТИ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ АГЕНТОВ

«Тонкий агент»

- Lockdown
  - Параметры антивируса, персонального брандмауэра, шаблонов политик безопасности
  - Сканирование реестра Windows
  - Поддержка Windows, Mac OS X

«Толстый агент»

- Обычные атрибуты
  - Параметры антивируса, персонального брандмауэра, шаблонов политик безопасности, версии ПО
  - Поддержка Windows
- Sygate
  - Принудительное использование 802.1X
- Zone Labs
  - Принудительное использование 802.1X
- Microsoft Network Access Protection
  - Принудительное использование DHCP, VPN, 802.1X, IPSec

ECOPROG
consulting, engineering, management

ПРИМЕР NAC С ИСПОЛЬЗОВАНИЕМ АГЕНТОВ

❻ Назначение политики – в случае несоответствия параметров конечной системы пользователя требованиям политики безопасности, к системе применяется политика “Quarantine”; в ином случае производится реаутентификация и применение соответствующей политики в соответствии с настройками RADIUS Server.

❶ Администрирование политик – Основными шагами настройки политик являются описания ролей “Assessing”, “Quarantine” и “Failsafe”. Далее политики распространяются и активизируются в точках применения политик сетевой инфраструктуры.

Enterasys NetSight® Policy Manager

❺ Оценка – конечная система пользователя оценивается на сервере оценки (с использованием EAP) на соответствие с корпоративной политикой безопасности.

Сервер оценки (RADIUS-прокси)

Шунт

Сетевая инфраструктура

Без EAP

Enterasys Sentinel™ Trusted Access Gateway (RADIUS-прокси)

RADIUS Server / Directory

Пользователь

Конечная система

Коммутатор Enterasys

❸ Доступ – Конечная система пользователя с установленным агентом пытается подключиться к сети с использованием 802.1X.

❹ Запрос на аутентификацию по 802.1X – MAC-адрес клиента появился на коммутаторе с поддержкой политик. Запрос на аутентификацию по 802.1X высылается на Trusted Access Gateway и перенаправляется на сервер оценки.

❷ Настройка Trusted Access Gateway – изменения, касающиеся процессов аутентификации и оценки сохраняются на шлюзах.

Enterasys Sentinel™ Trusted Access Manager

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

ECOPROG
consulting, engineering, management

ИНТЕГРАЦИЯ DRAGON И ENTERASYS SENTINEL

❺ Отклик на угрозу – Контрмеры применяются только к порту источника атаки (применение политики карантина, отключение порта и т.п.).

❶ Конфигурация политики карантина – Задание настроек политики карантина и ее распространение по корпоративной сетевой инфраструктуре.

Enterasys NetSight® Policy Manager

Nessus

lockdown

Сервер оценки

Пользователь

Конечная система

Коммутатор Enterasys

Сетевая инфраструктура

Enterasys Sentinel™ Trusted Access Gateway (RADIUS-прокси)

RADIUS Server / Directory

❷ Обнаружение инцидента – Инцидент безопасности, возникающий в сетевой инфраструктуре, немедленно обнаруживается.

Enterasys Dragon® Intrusion and Network Defense

❻ Оповещение ASM/TAM – MAC-адрес источника угрозы блокируется на всех Trusted Access Gateway.

Enterasys Sentinel™ Trusted Access Manager

❸ Оповещение об инциденте – Факт нарушения политики безопасности передается к Automated Security Manager, на котором сконфигурировано правило реагирования на инцидент.

Enterasys NetSight® Automated Security Manager

❹ Генерация контрмер – Точное обнаружение местоположения источника угрозы, применение предопределенного правила к сетевому порту источника атаки.

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

ВАШИ ВОПРОСЫ

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

СПАСИБО ЗА ВНИМАНИЕ !

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