Обнаружение атак. Система RealSecure

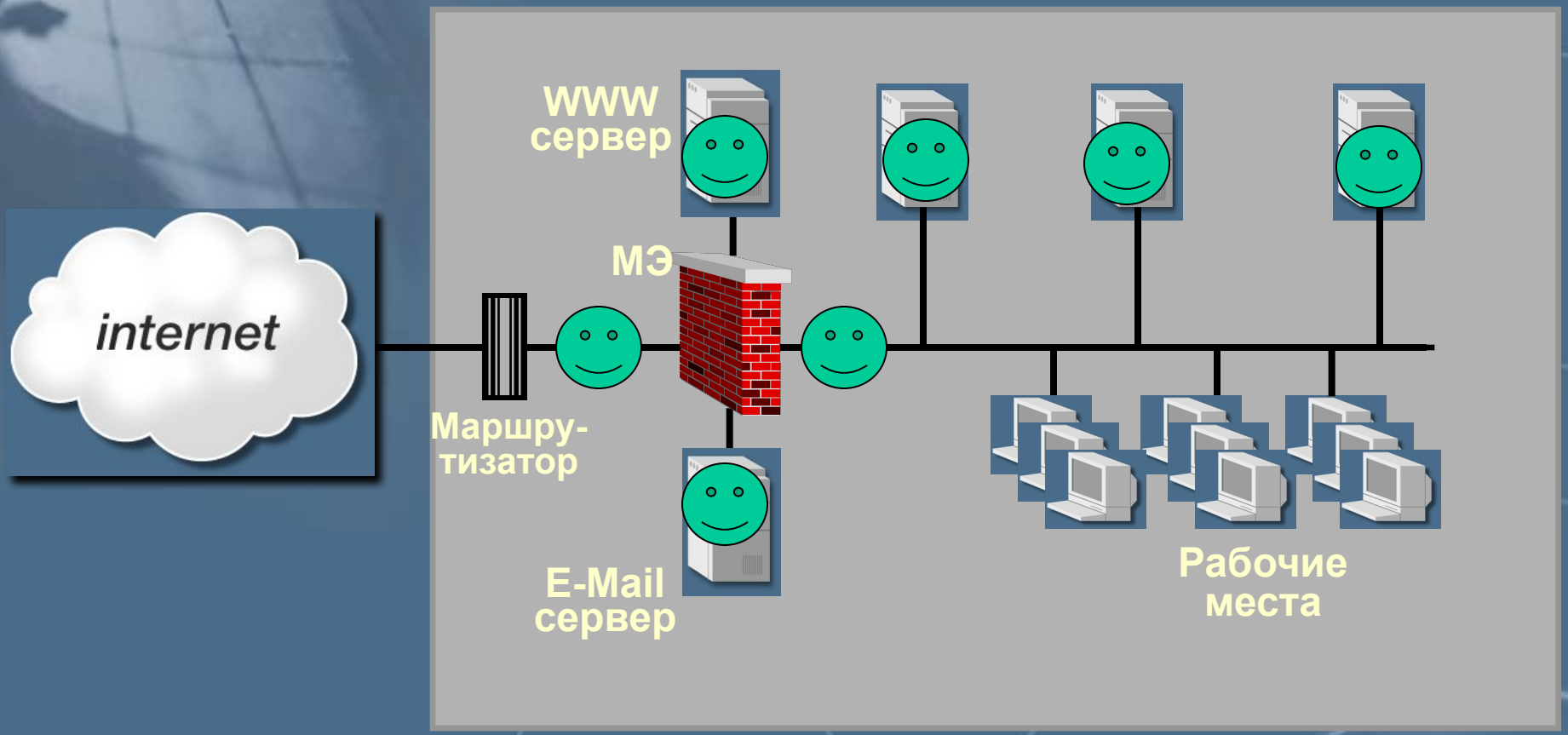
Средства защиты сетей

- МЭ
- Средства анализа защищённости
- Средства обнаружения атак

Архитектура систем обнаружения атак

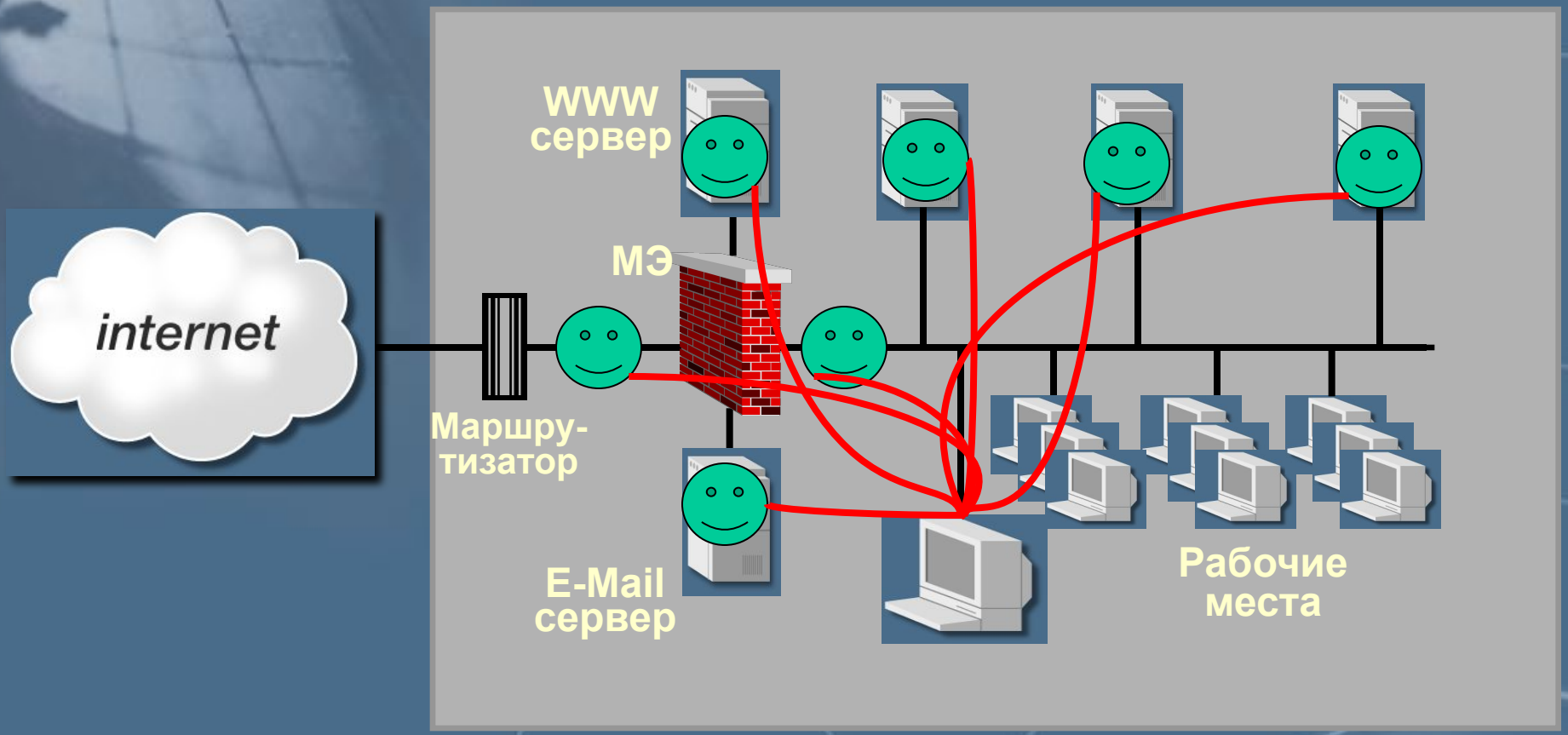
- Модуль слежения
- Модуль управления

Архитектура систем обнаружения атак



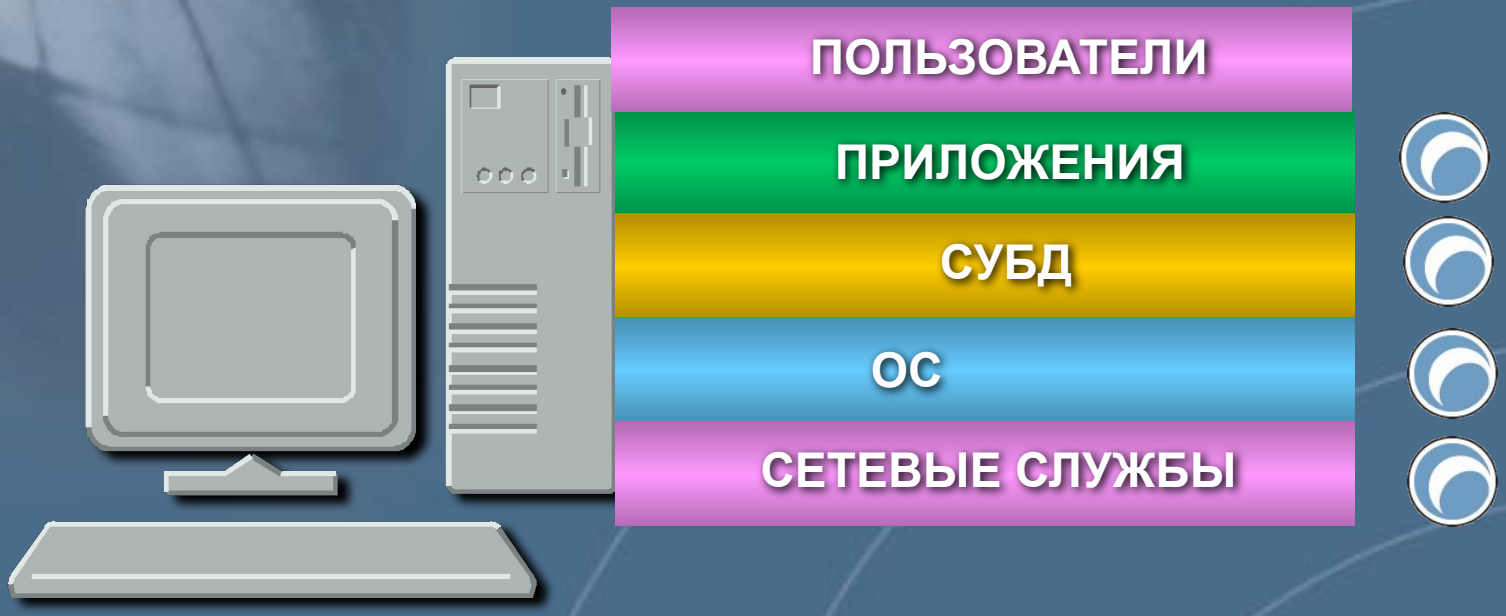
Сенсоры

Архитектура систем обнаружения атак



Управляющие компоненты

Классификация систем обнаружения атак



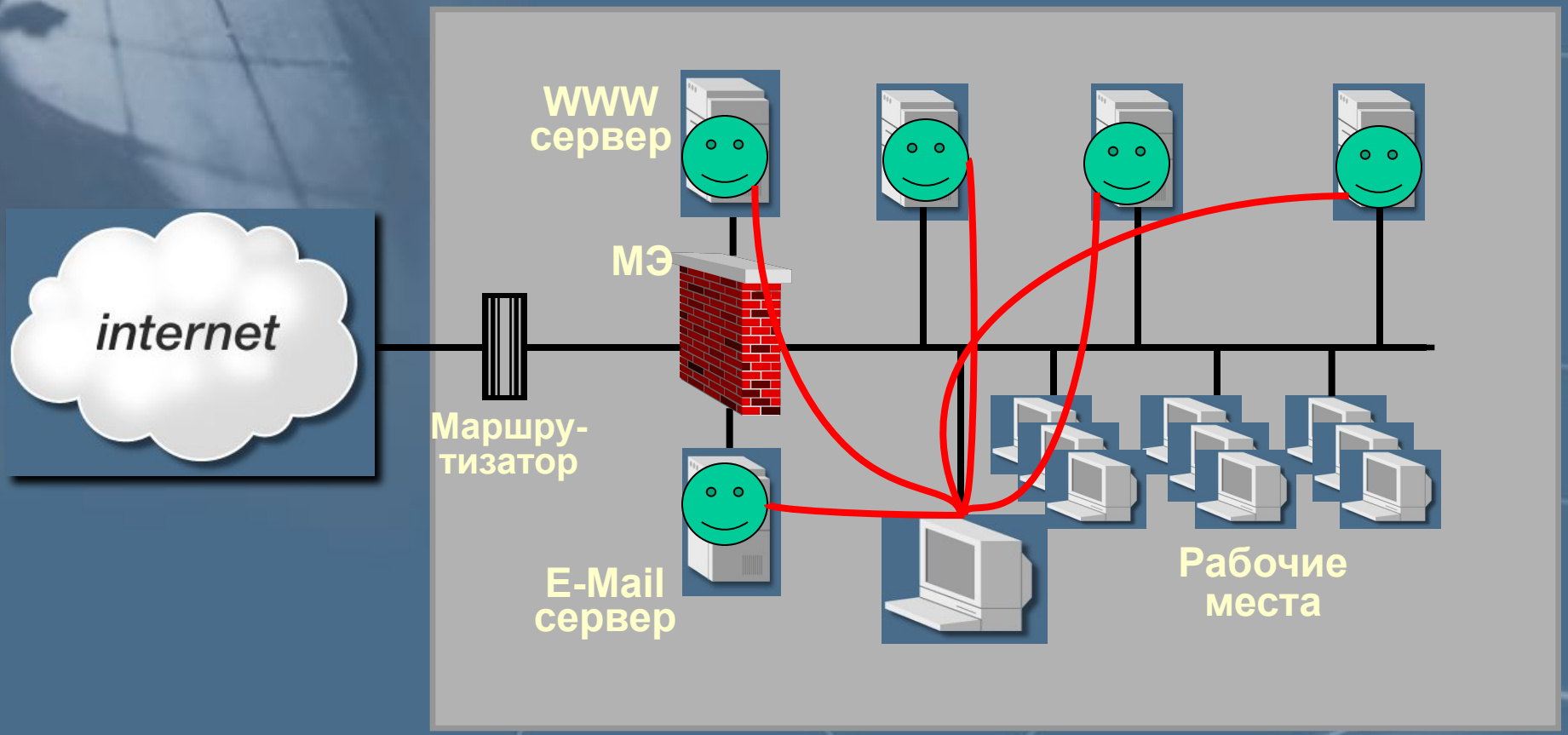
По уровням информационной инфраструктуры

Классификация систем обнаружения атак

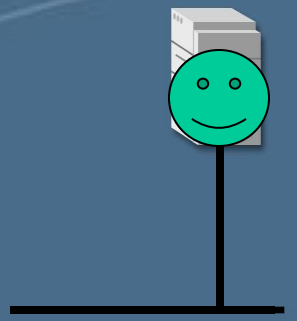
- Системы на базе узла
- Системы на базе сегмента

По принципу реализации

Системы обнаружения атак на базе узла



Системы обнаружения атак на базе узла

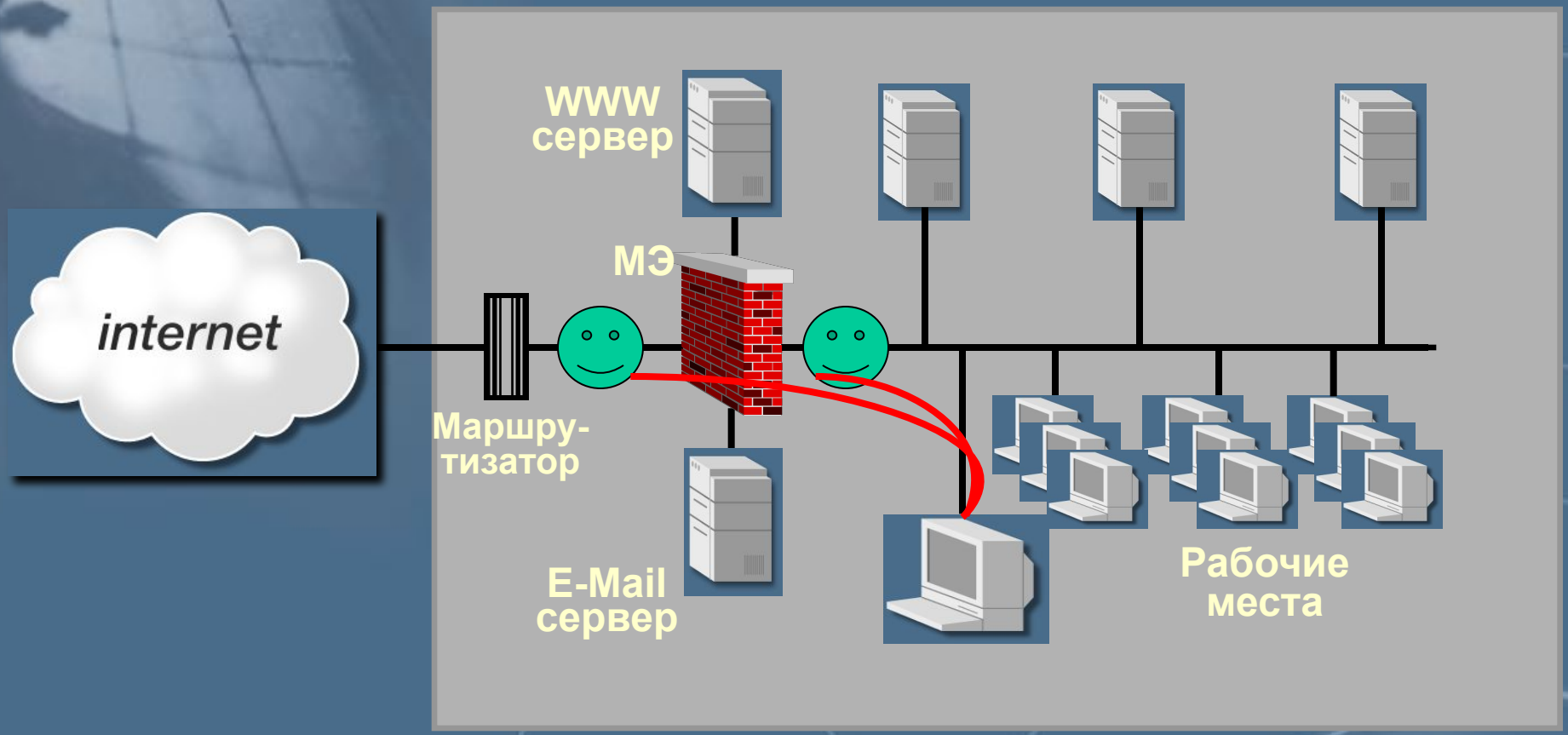


Источники данных:

- Журналы аудита
- Действия пользователей

Необязательно:
Сетевые пакеты (фреймы), направленные к узлу и от узла

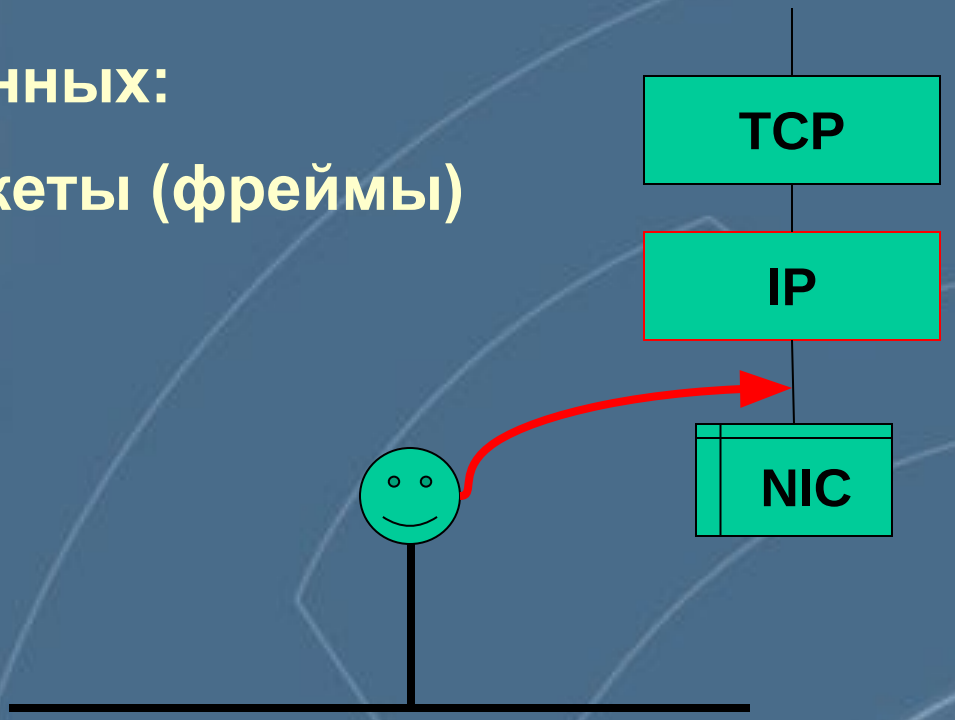
Системы обнаружения атак на базе сети



Системы обнаружения атак на базе сети

Источник данных:

- **Сетевые пакеты (фреймы)**



Классификация систем обнаружения атак

- **Обнаружение аномалий**
- **Анализ сигнатур**

По технологии обнаружения

Системы обнаружения атак

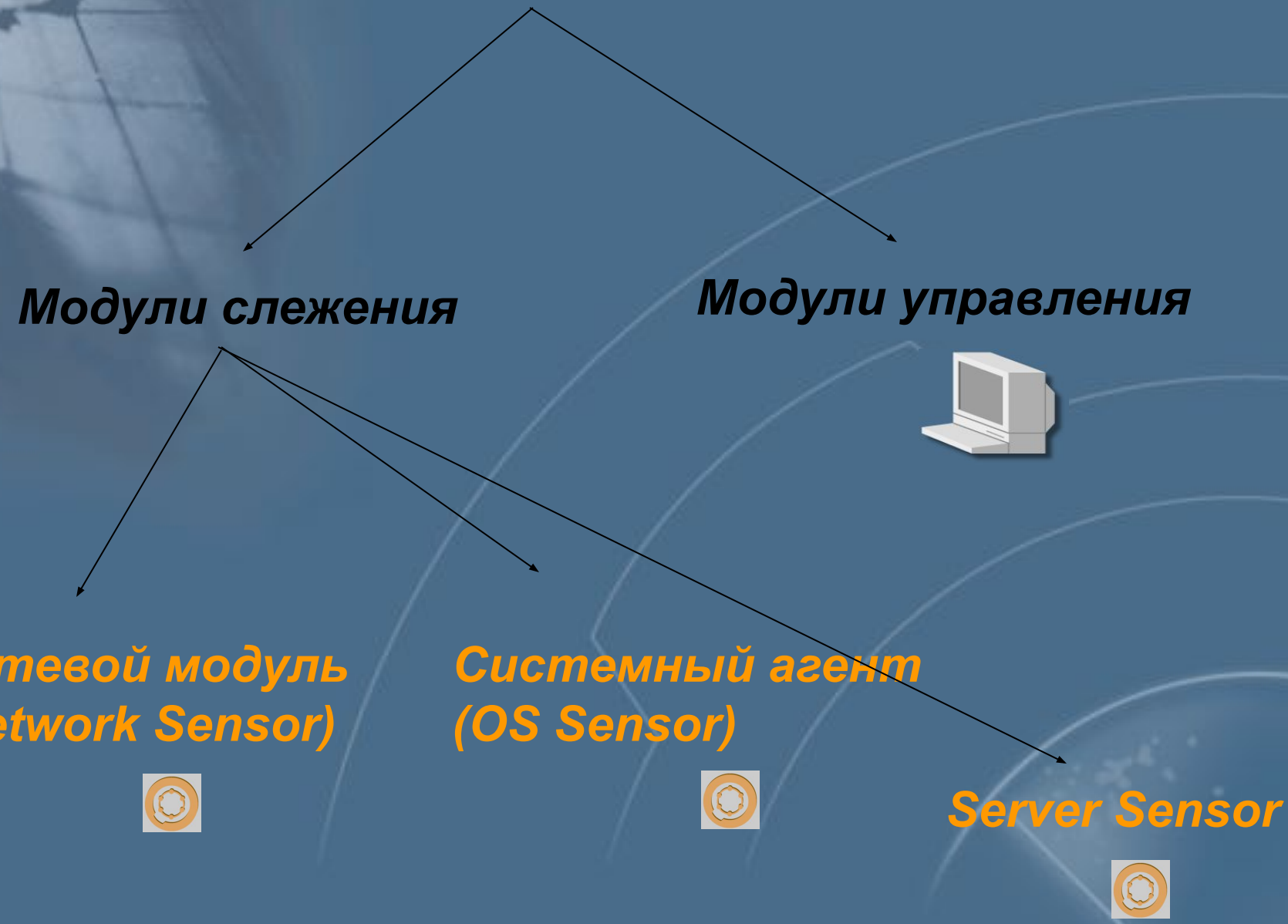
	Net Prowler	Secure IDS	eTrust Intrusion Detection	RealSecure	Snort
Производитель	Axent Technologies	Cisco Systems	Computer Associates	Internet Security Systems	Нет
Платформа	Windows NT	Защищенная версия Solaris	Windows NT	Windows NT (2000)	Unix
Технология обнаружения	Сигнатуры атак	Сигнатуры атак	Сигнатуры атак	Сигнатуры атак	Сигнатуры атак
Принцип реализации	На базе сети	На базе сети	На базе сети + возможности МЭ	На базе сети и на базе узла	На базе сети

RealSecure - система обнаружения атак в реальном времени

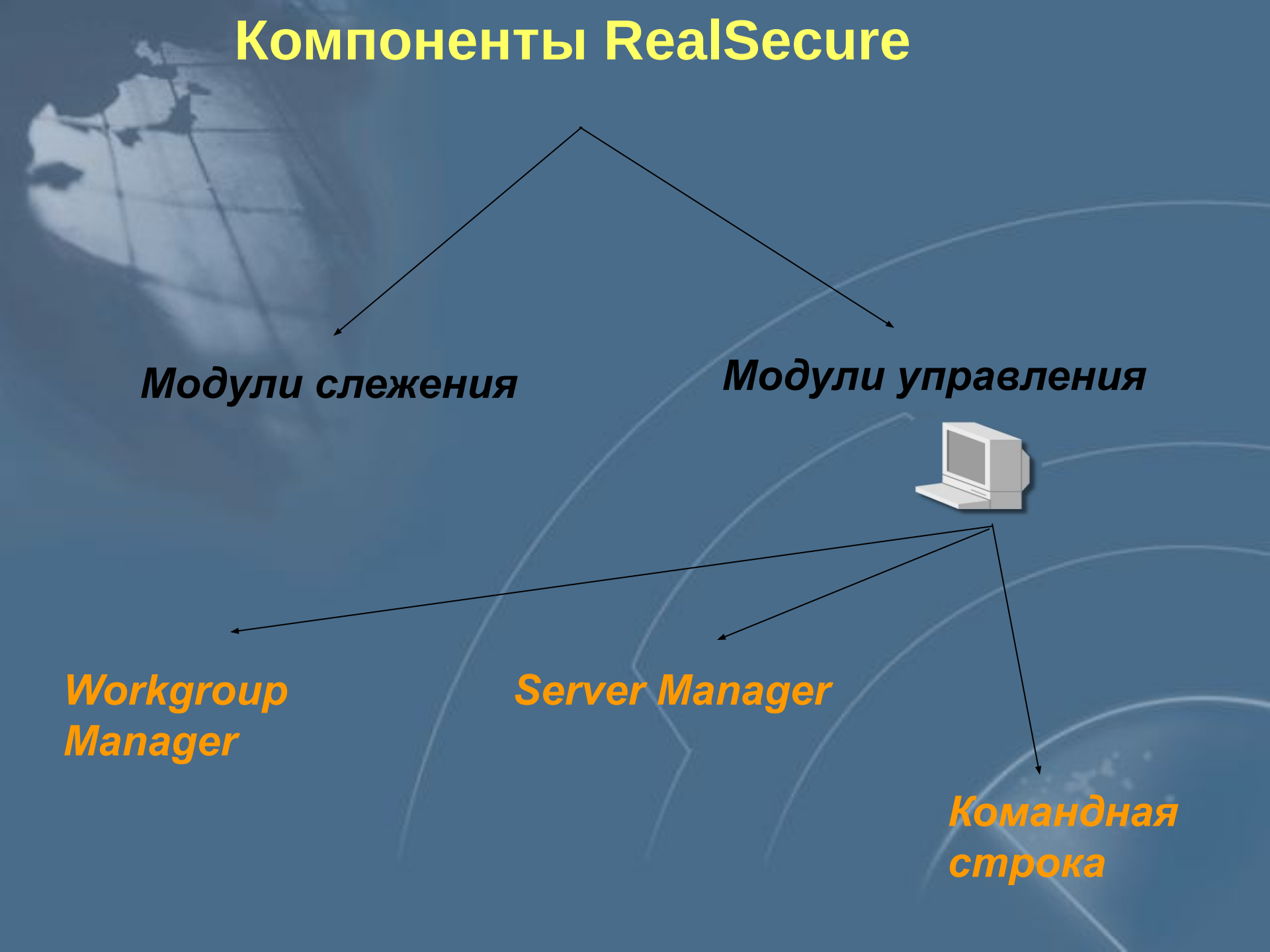
- *Устанавливается в сетевом сегменте или на отдельном узле*

- *Просматривает весь трафик сегмента или действия пользователя конкретного узла*
- *Анализирует трафик с целью обнаружения атак и других событий, связанных с безопасностью*
- *В случае обнаружения предпринимает ответные действия*

Компоненты RealSecure



Компоненты RealSecure



Компоненты RealSecure

Модули управления

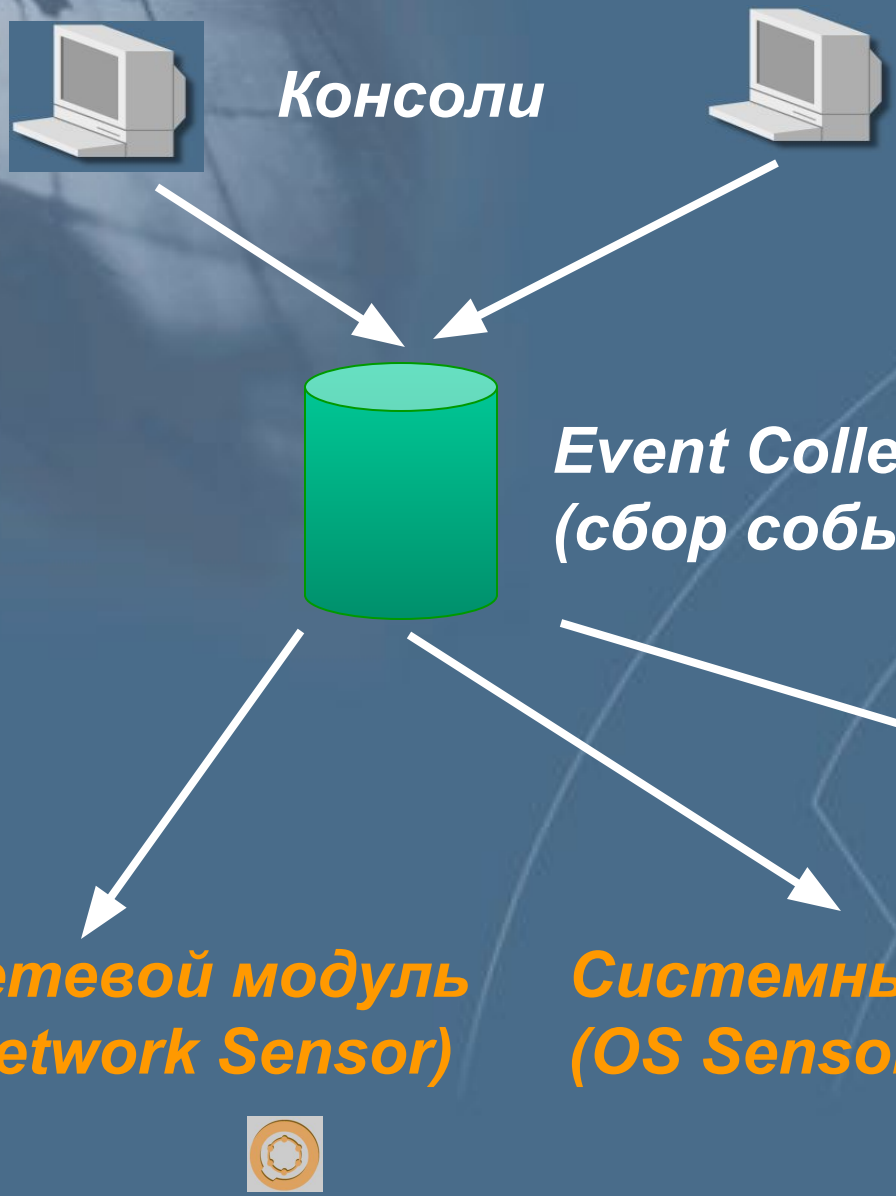
Server Manager

Командная строка

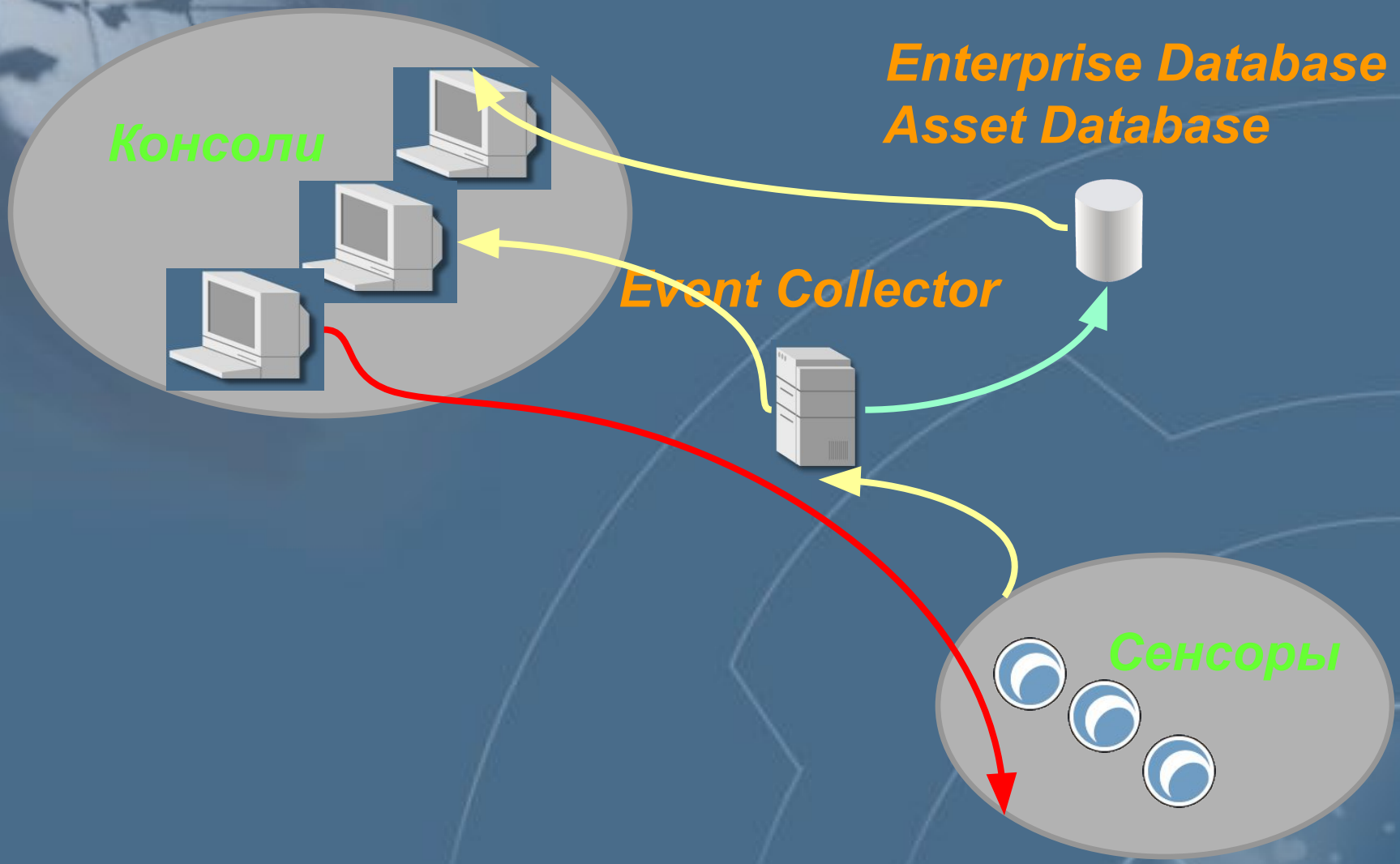
Workgroup Manager

- ***Event Collector***
- ***Enterprise Database***
- ***Asset Database***
- ***Console***

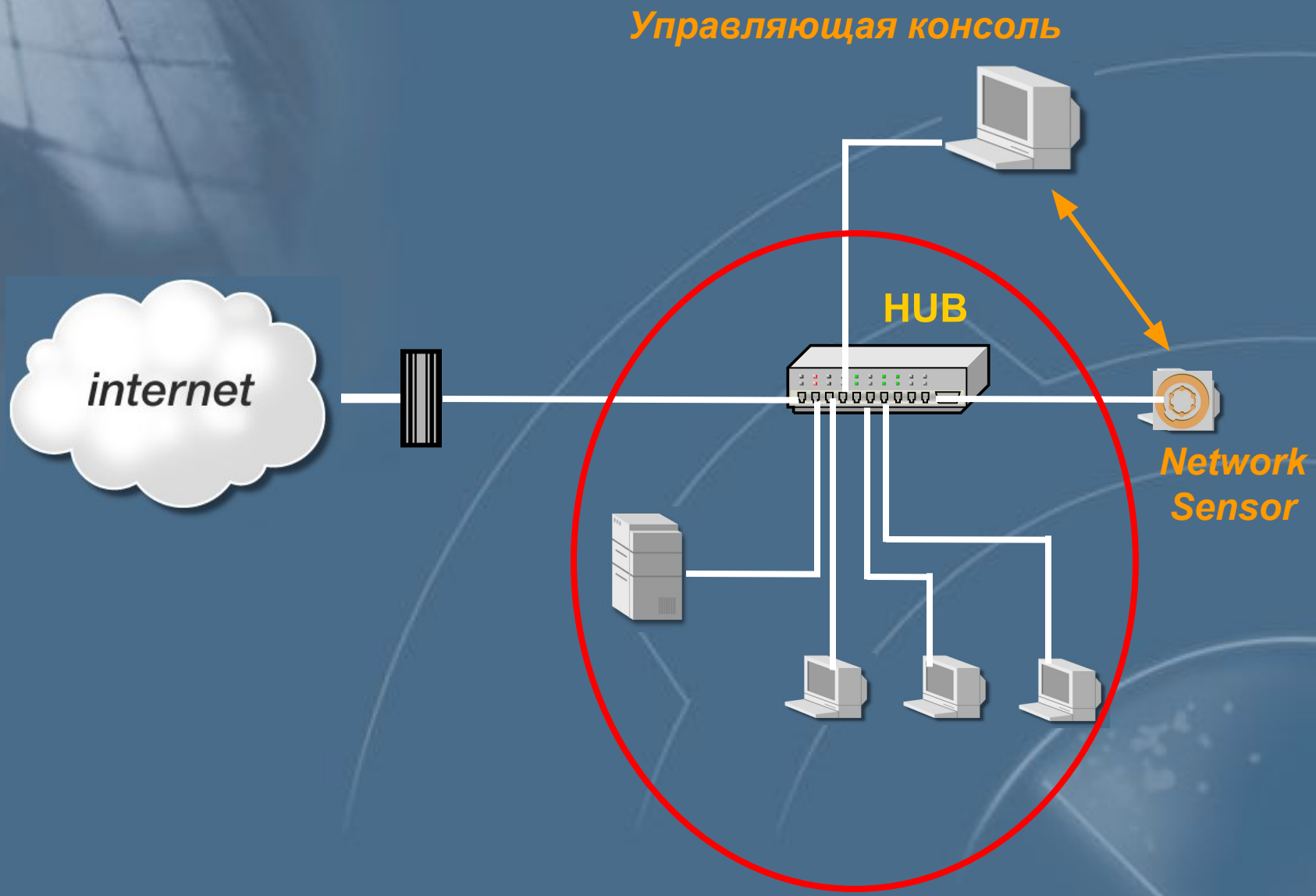
Компоненты RealSecure версии 6.0



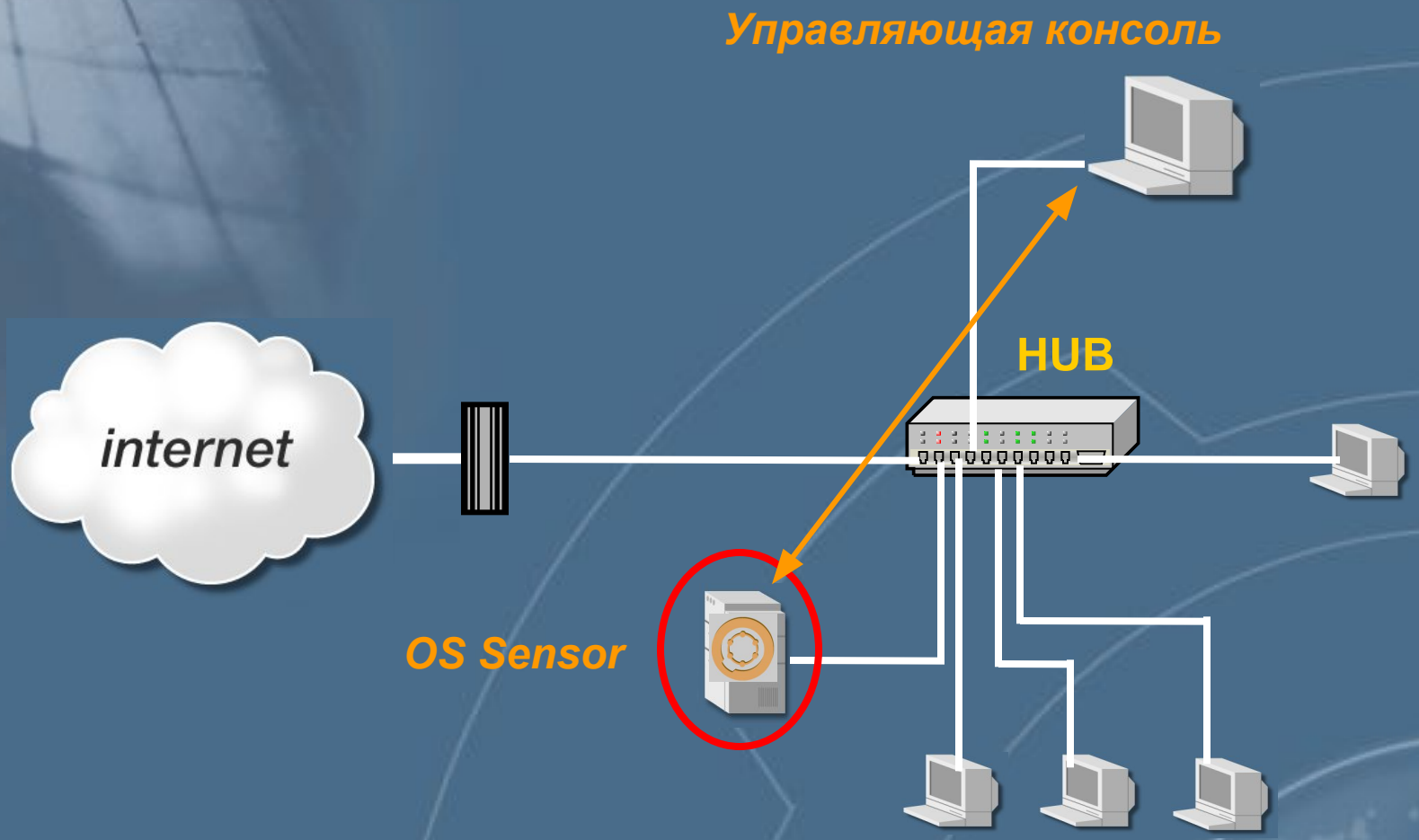
Архитектура



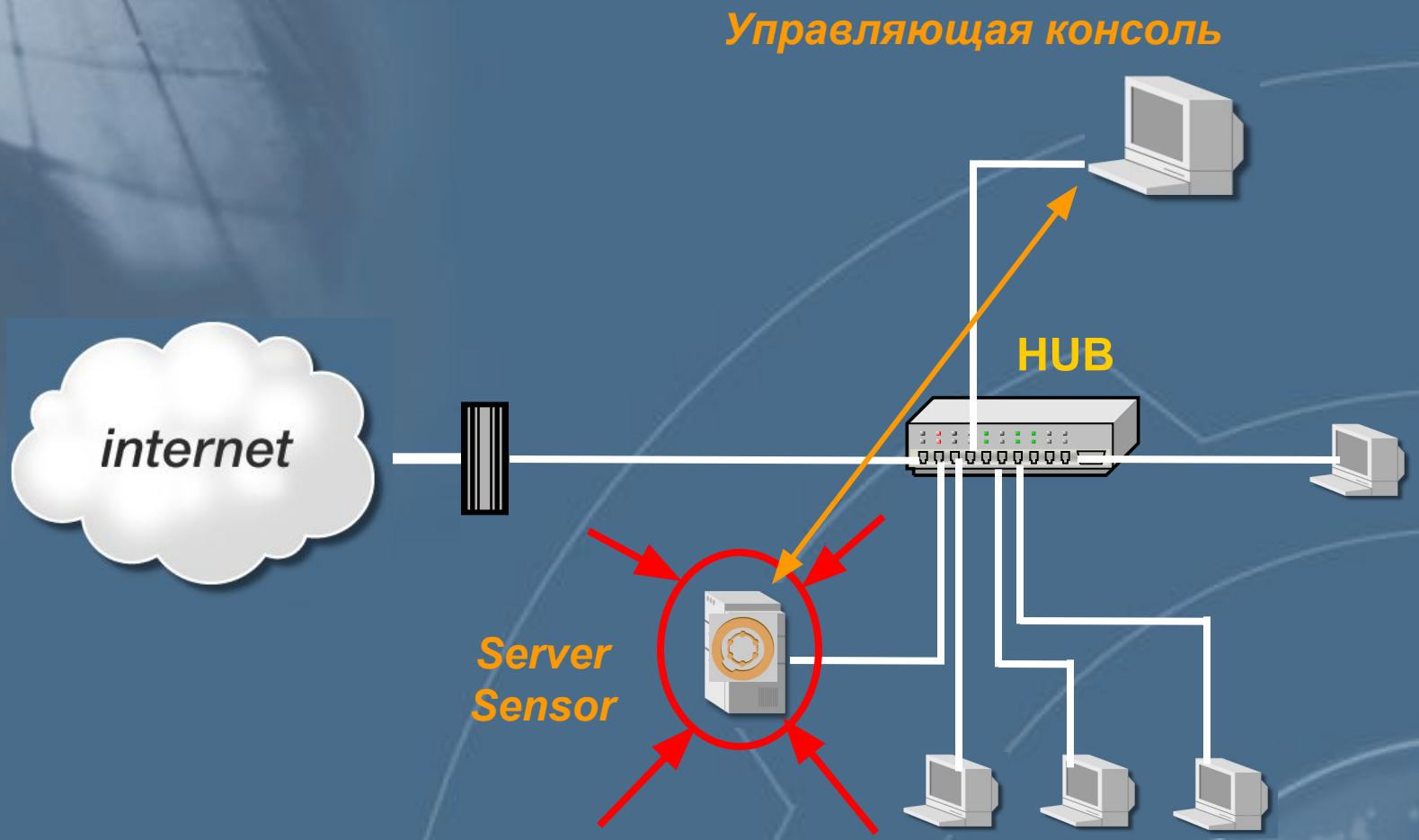
Расположение сетевого модуля



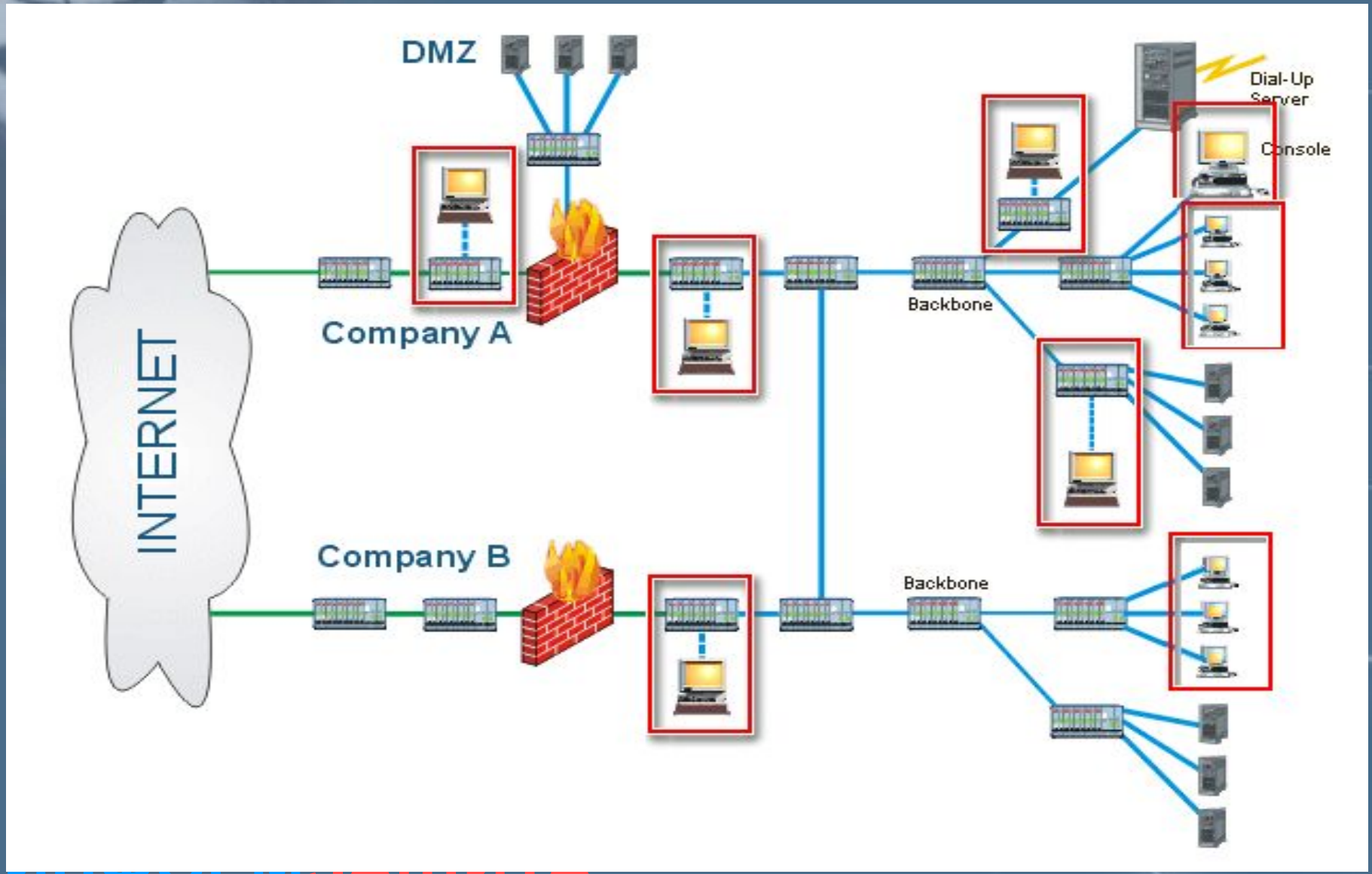
Расположение системного агента



Расположение Server Sensor



Примеры размещения RealSecure



Категории контролируемых событий

- *Атаки*
  - *Уровня сети (Сканирование портов, SYN Flood, Ping of Death)*
  - *Уровня СУБД (MS SQL Server)*
  - *Уровня приложений (Атаки на MS IIS, MS Exchange)*
- *Установленные соединения*
  - *TELNET, FTP, SMTP*
- *Пользовательские события*
  - *HTTP – запросы, содержимое почтовых сообщений*

Механизмы реагирования RealSecure

Разрыв соединения

Реконфигурация межсетевого экрана

Выполнение программы, определённой пользователем

Отправка сообщения

- *На консоль*
- *По протоколу SNMP*
- *По E-mail*

Регистрация события в БД

Расширенная регистрация с возможностью последующего воспроизведения

Network Sensor

Особенности:

- обнаружение в реальном режиме времени

- независимость от операционной системы

- обнаружение атак до достижения ею цели

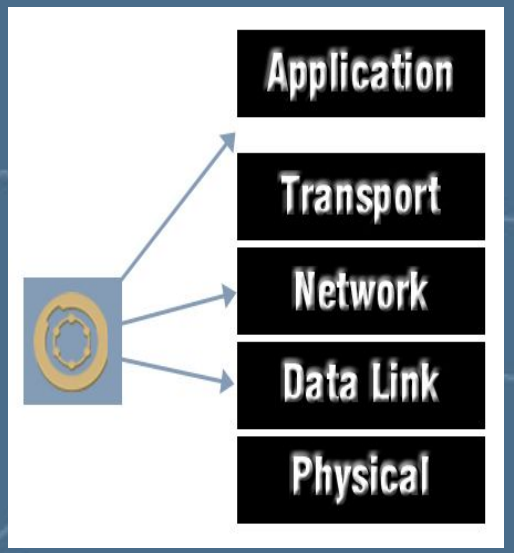
- невозможность обнаружения (Stealth-режим)

RealSecure и межсетевые экраны

- Модемы
- Атаки через «туннели»
- Атаки со стороны авторизованных пользователей
- Атаки на межсетевые экраны

Server Sensor

Обнаружение атак на всех уровнях на конкретный узел сети



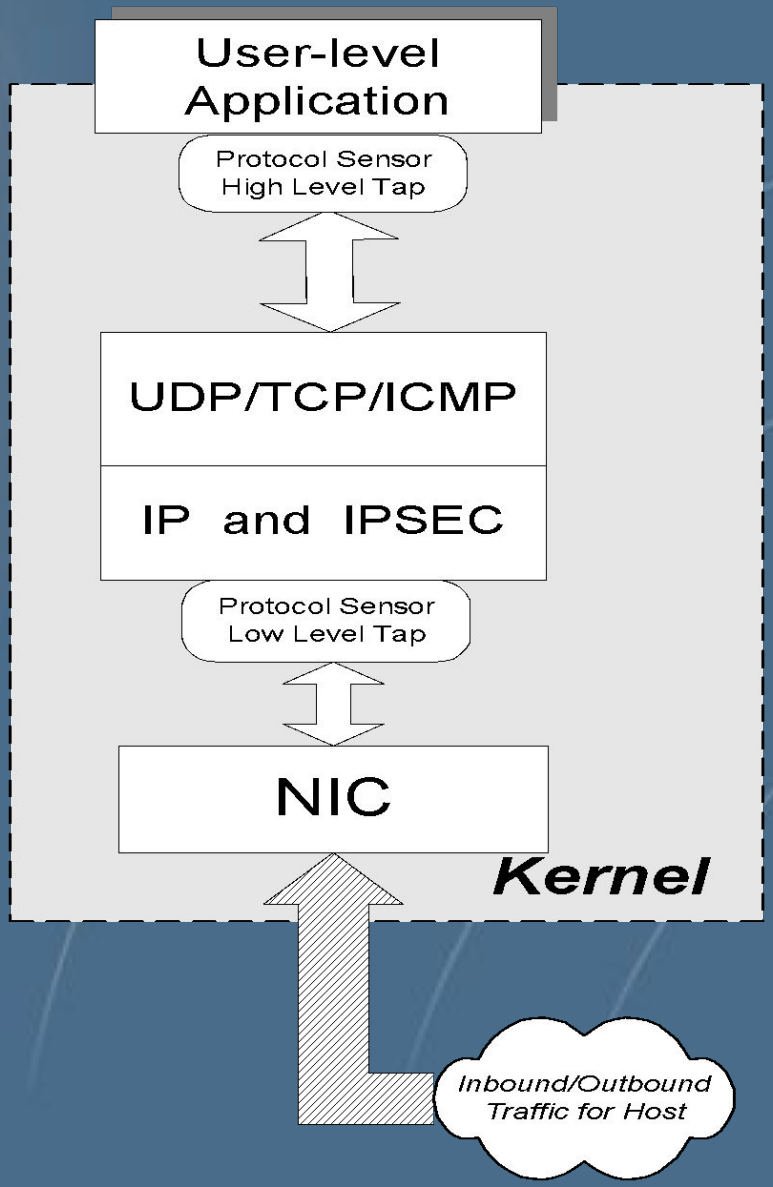
Особенности:

- *производительность*
- *обнаружение всех атак*
- *работа в коммутируемых сетях*
- *работают в сетях с шифрованием*

Функции персонального межсетевого экрана

Server Sensor

3. High Module



2. Стек TCPIP

1. Low Module

Что делает управляющая консоль?

Предоставляет интерфейс для конфигурирования модулей слежения

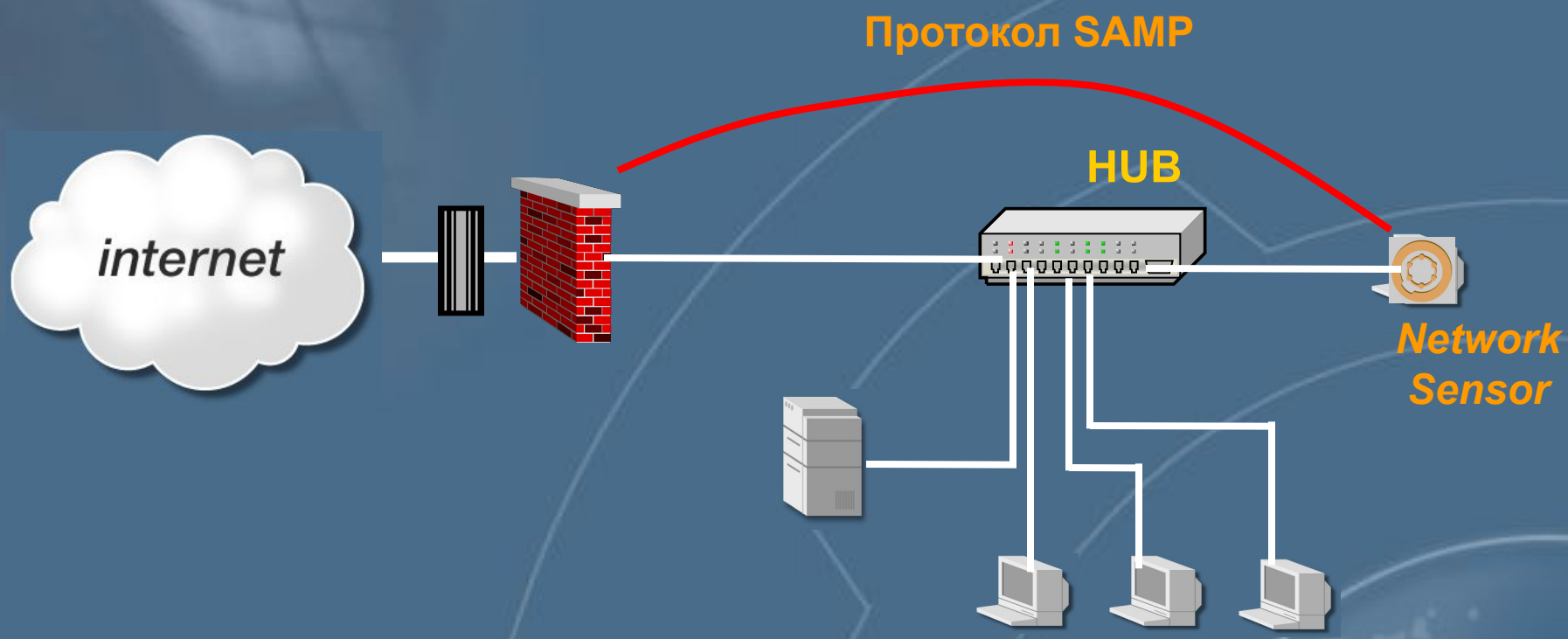
На консоль поступают сообщения от модулей слежения и данные, записанные модулями слежения

Позволяет формировать отчёты на основе собранных данных

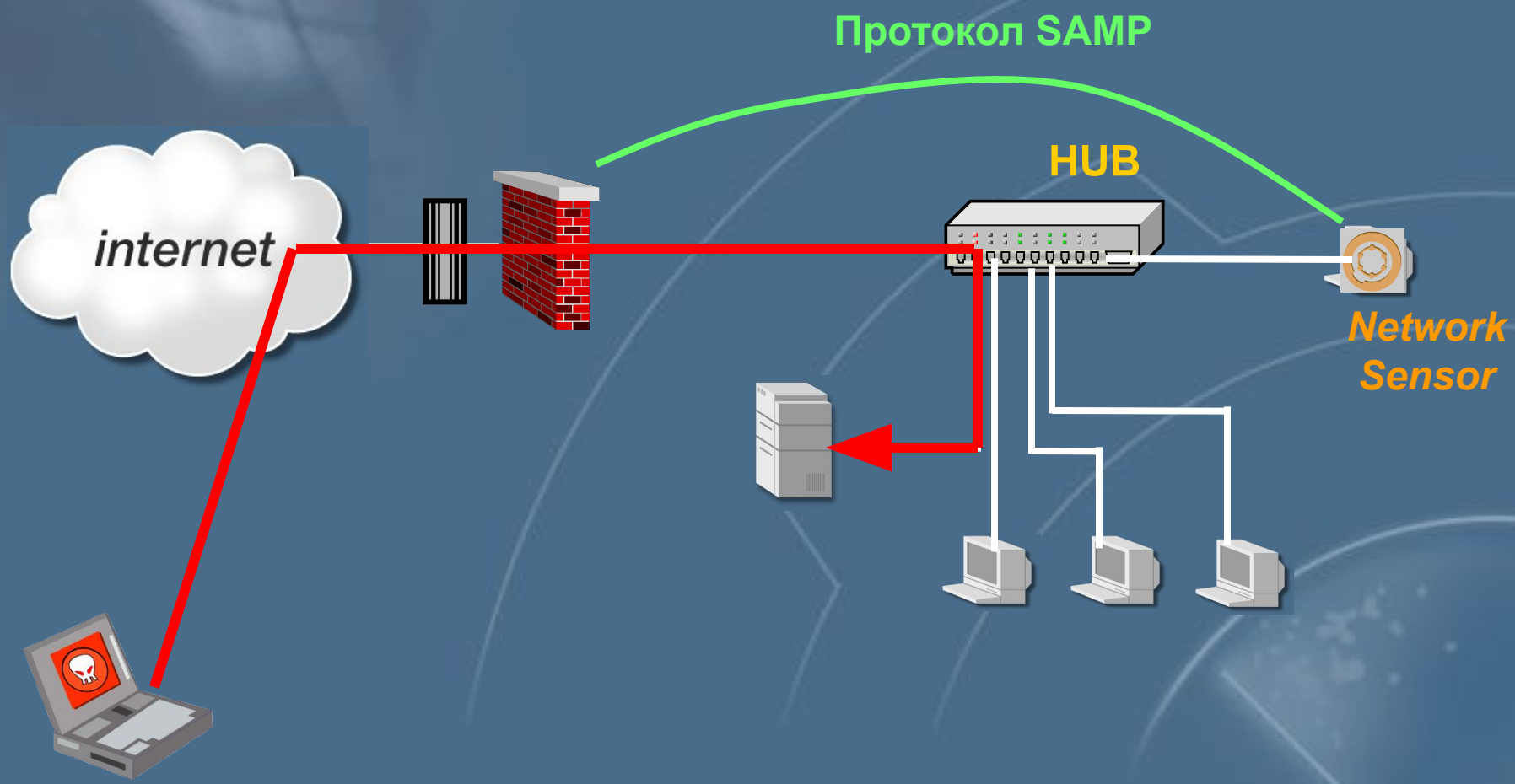
Концепция OPSec

- Использование OPSec SDK, предоставляющих необходимые API
- Применение открытых протоколов
  - CVP(Content Vectoring Protocol)
  - UFP (URL Filter Protocol)
  - SAMP (Suspicious Activity Monitoring Protocol
  - LEA (Log Export API)
  - OMI (Object Management Interface)
- Использование языка INSPECT

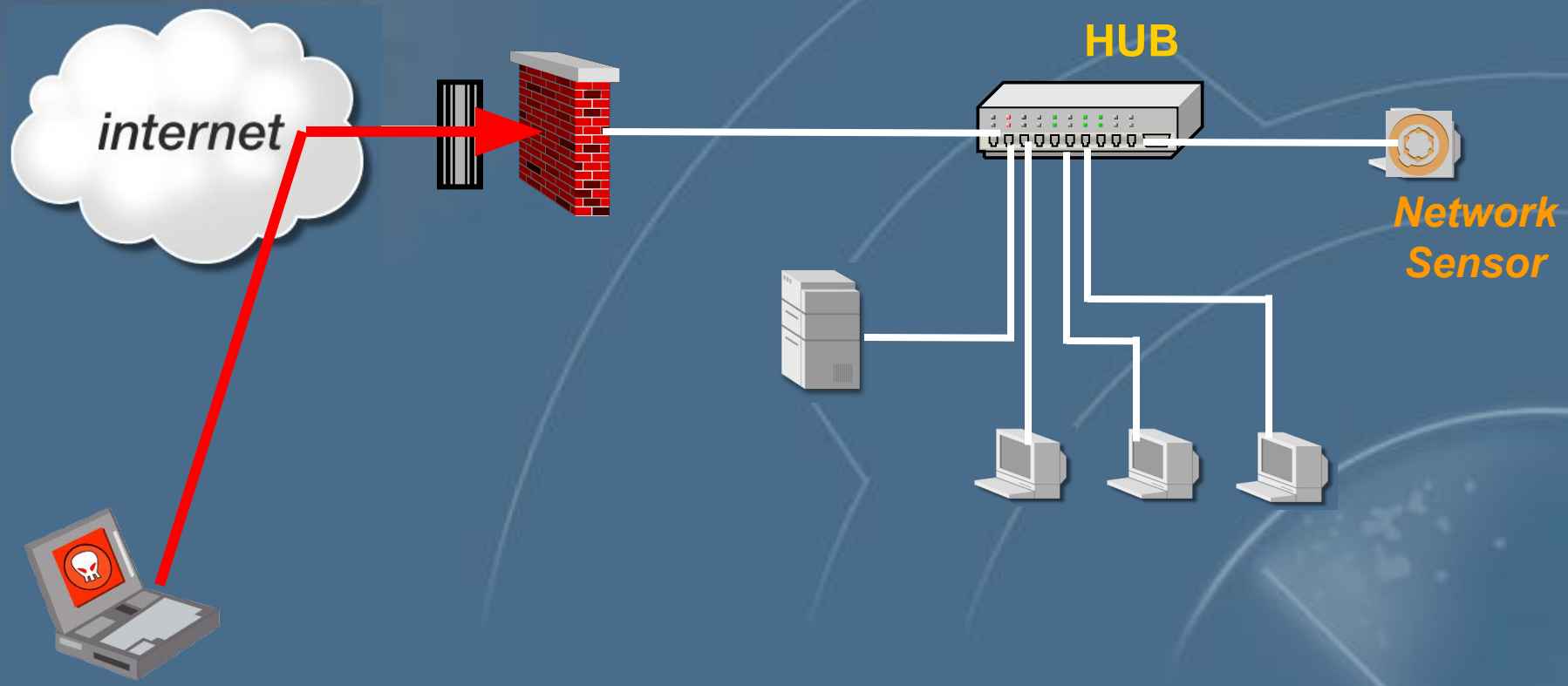
Реконфигурация МЭ



Реконфигурация МЭ



Реконфигурация МЭ



Система обнаружения атак Snort

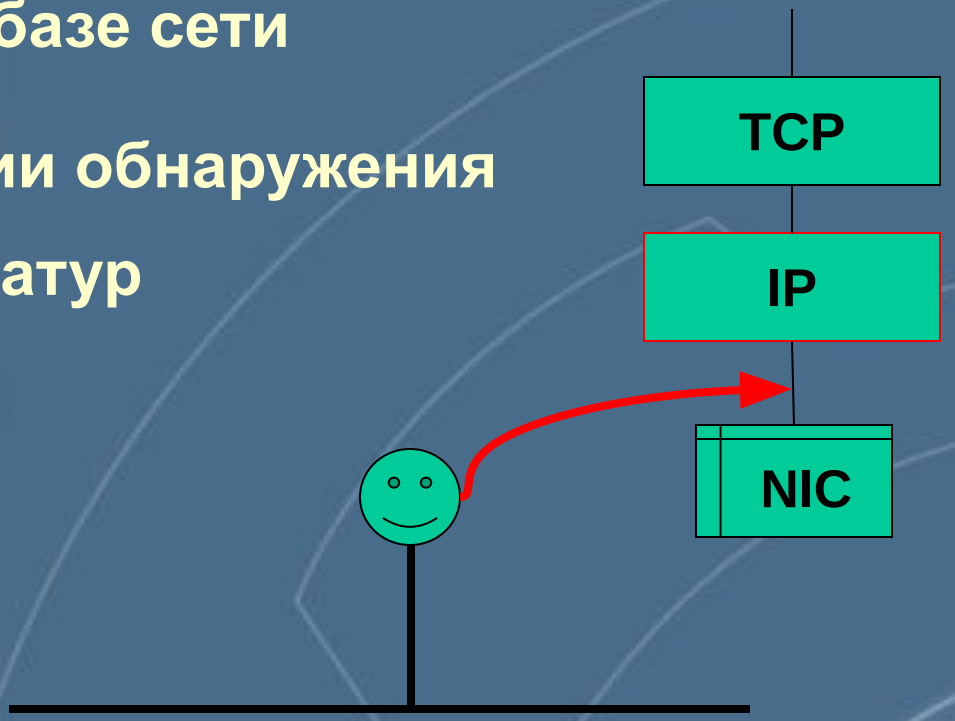
Архитектура

По принципу реализации

- **Система на базе сети**

По технологии обнаружения

- **Анализ сигнатур**



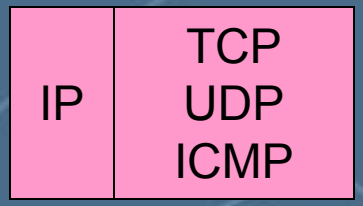
Режимы работы

- **Sniffer Mode**
- **Packet Logger**
- **Intrusion Detection System**

Sniffer Mode

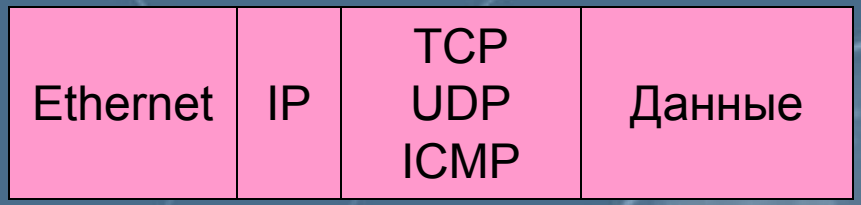
Вывод на экран содержимого пакетов

```
./snort -v
```




```
./snort -vd
```


```
./snort -vde
```



Packet Logger

Запись содержимого пакетов в файл

```
./snort -vde -l
./log
```

подкаталог log в текущем каталоге

Intrusion Detection System

Обнаружение событий

```
./snort –vde –l ./log – c
snort.conf
```

Правила срабатывания (контролируемые события)