Средства обнаружения атак

Раздел 2 – Тема 14

Средства защиты сетей

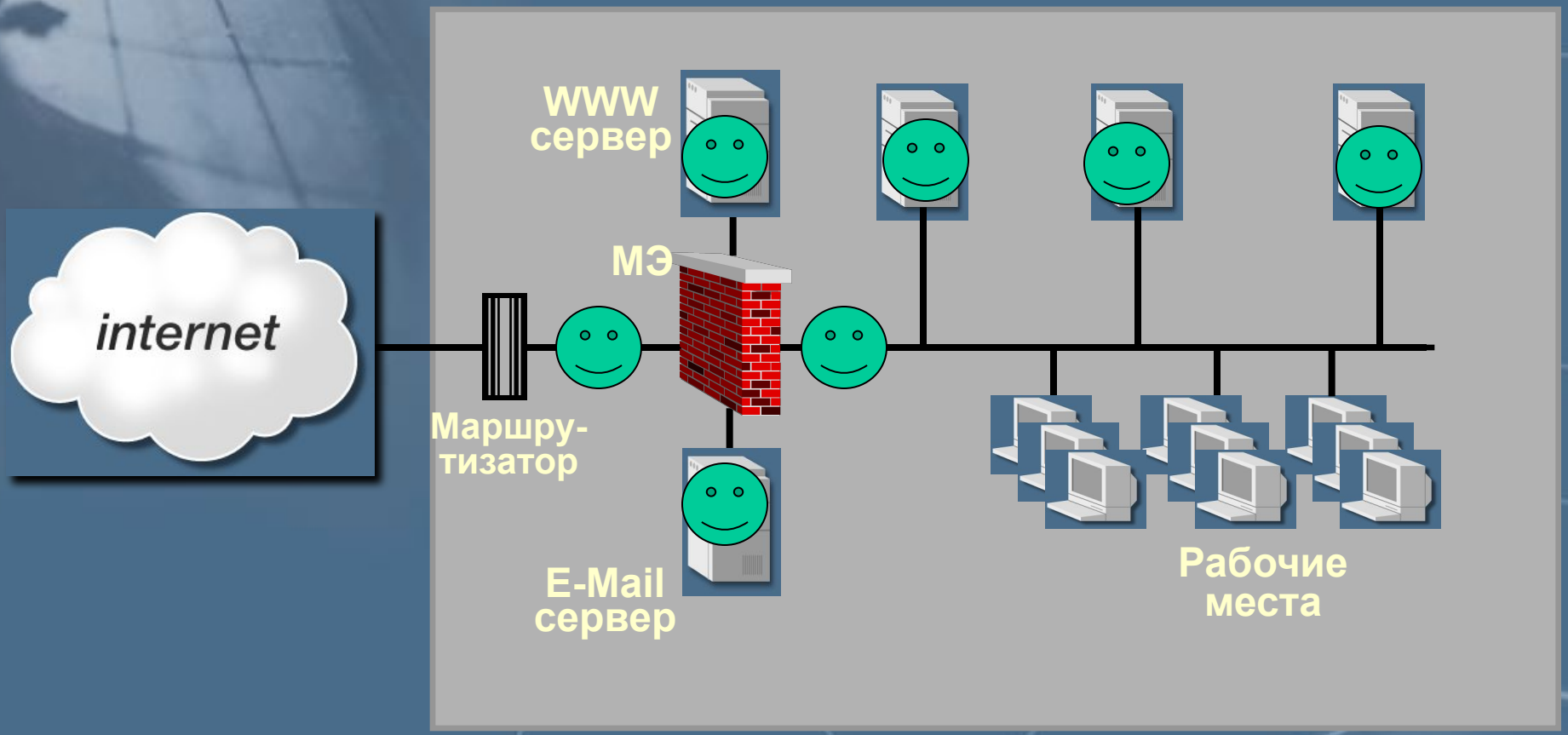
- МЭ
- Средства анализа защищённости
- Средства обнаружения атак

Архитектура систем обнаружения атак

- Модуль слежения
- Модуль управления

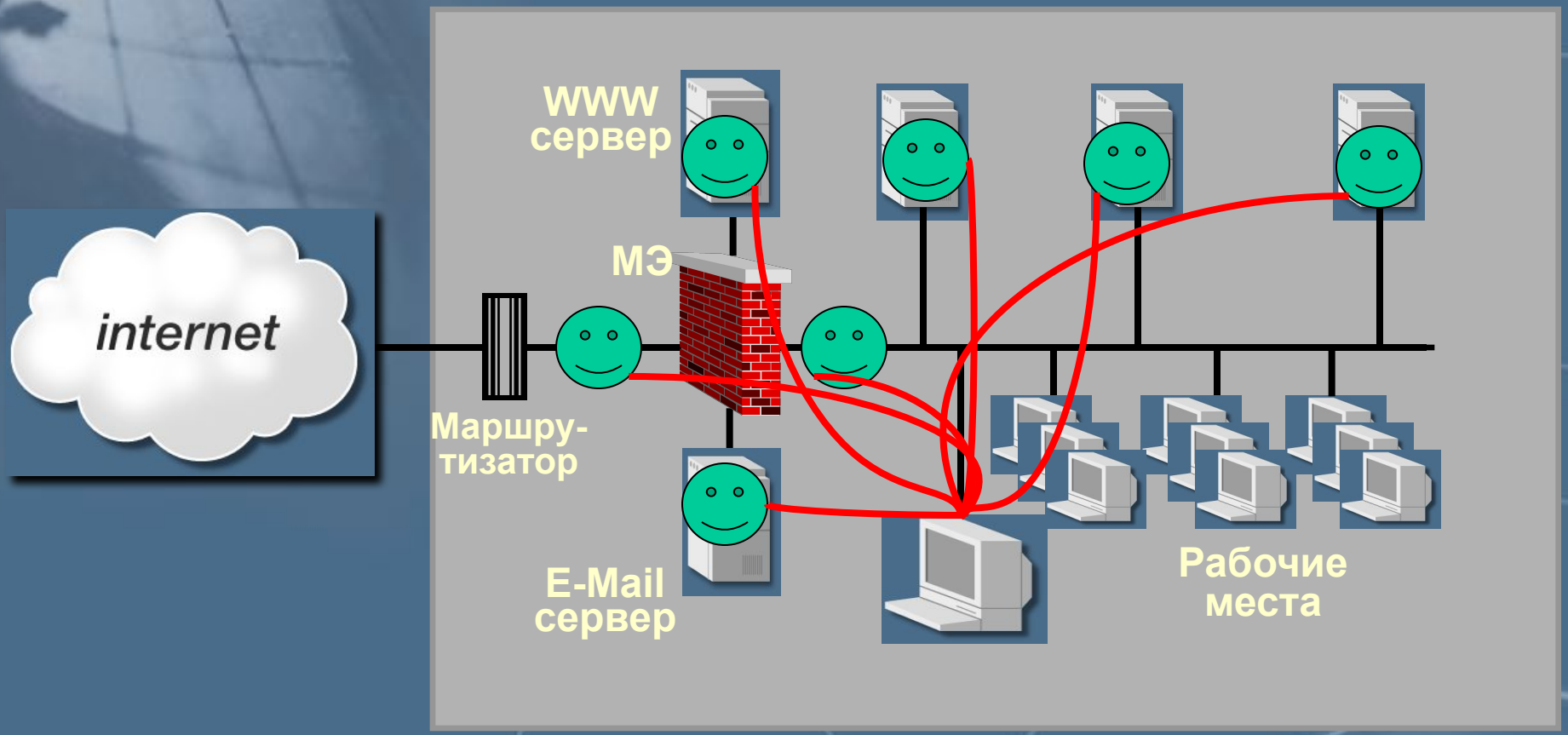
- Системы на базе узла
- Системы на базе сегмента

Архитектура систем обнаружения атак



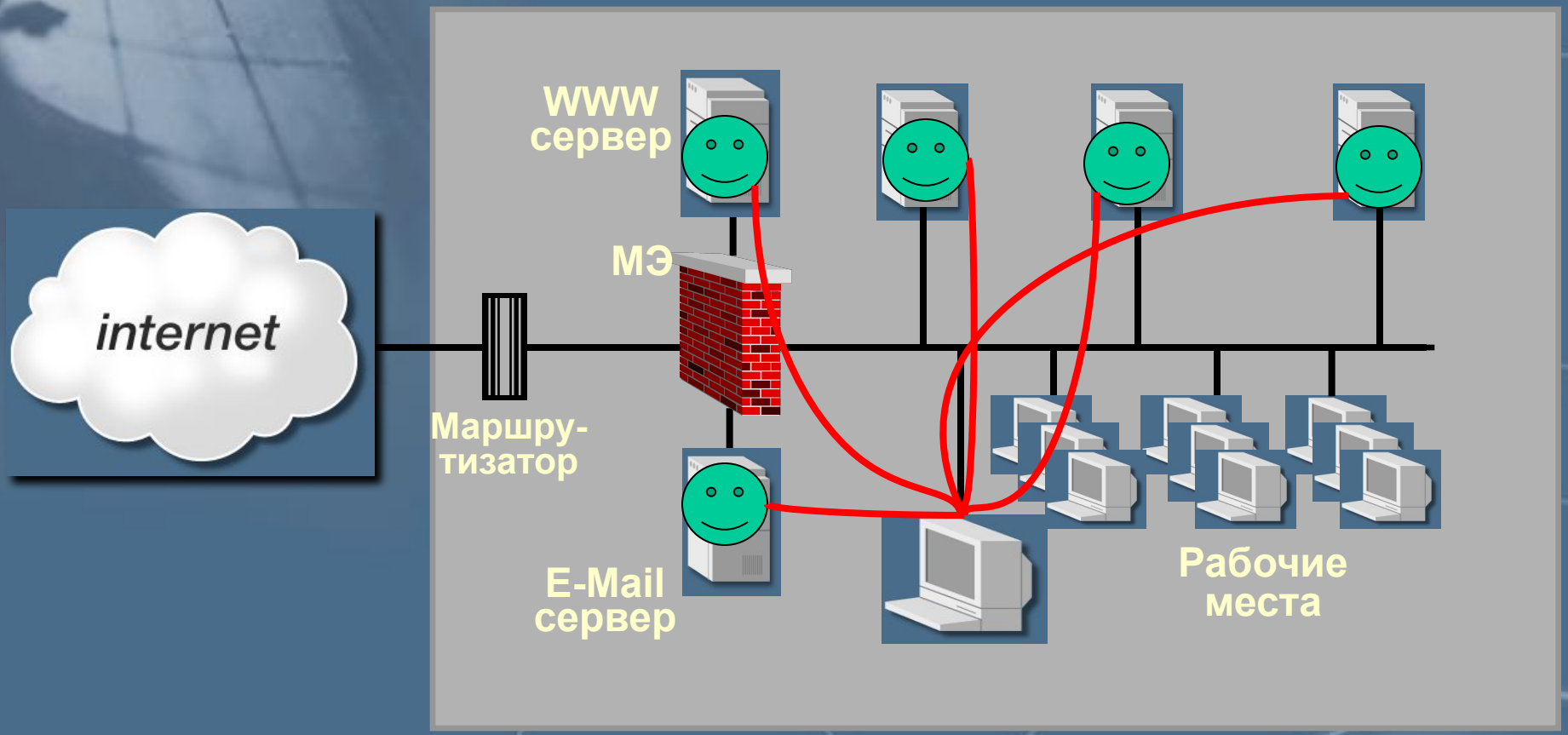
Сенсоры

Архитектура систем обнаружения атак

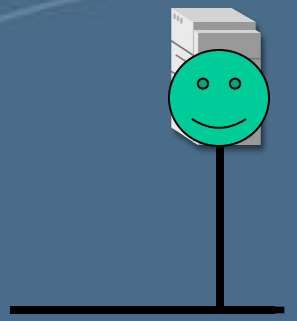


Управляющие компоненты

Системы обнаружения атак на базе узла



Системы обнаружения атак на базе узла

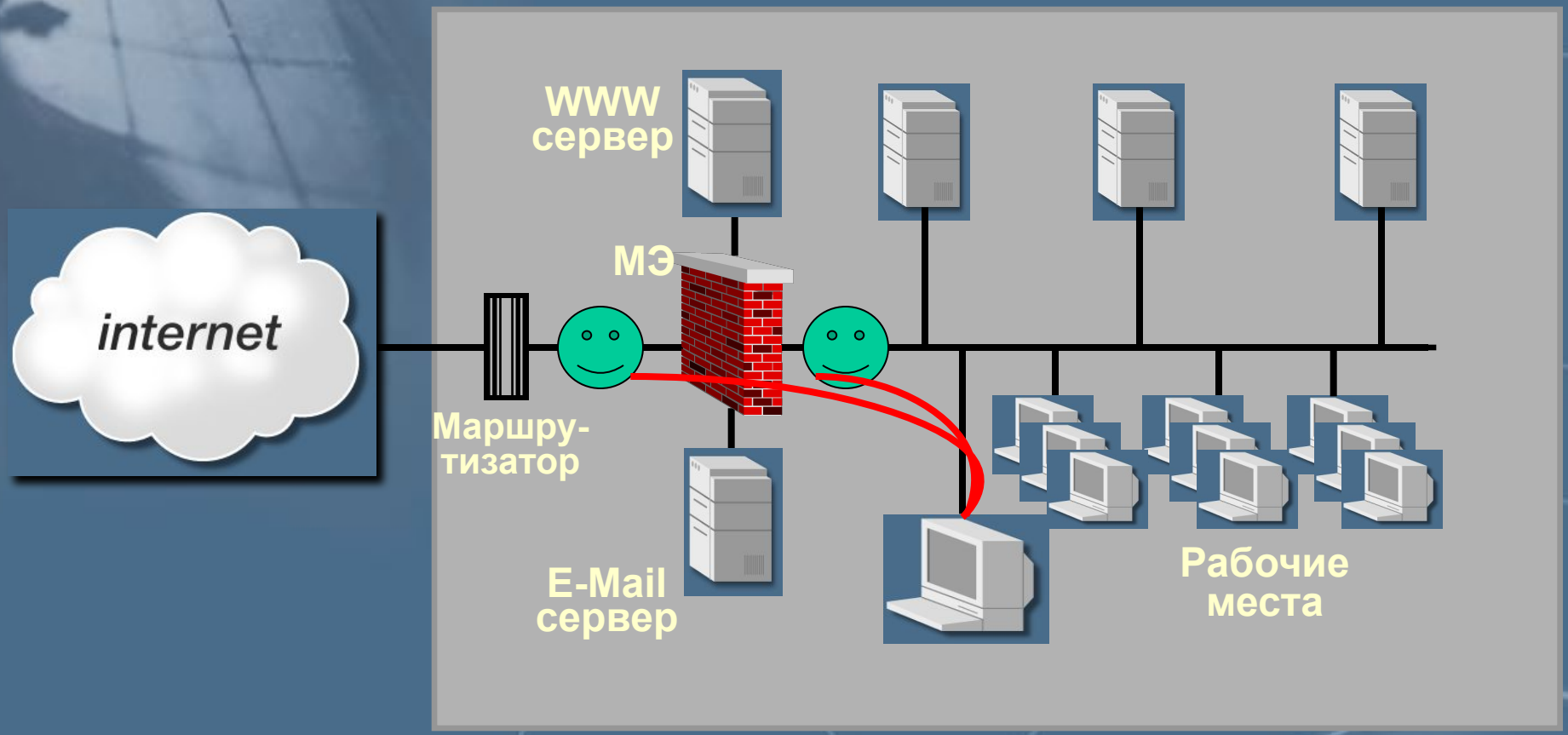


Источники данных:

- Журналы аудита
- Действия пользователей

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

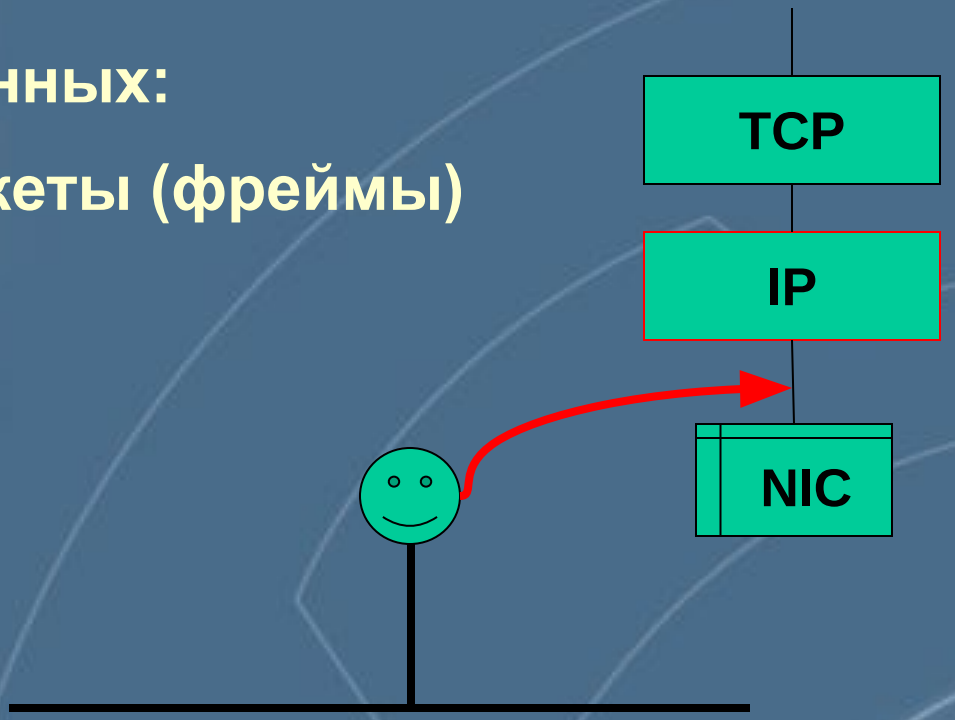
Системы обнаружения атак на базе сети



Системы обнаружения атак на базе сети

Источник данных:

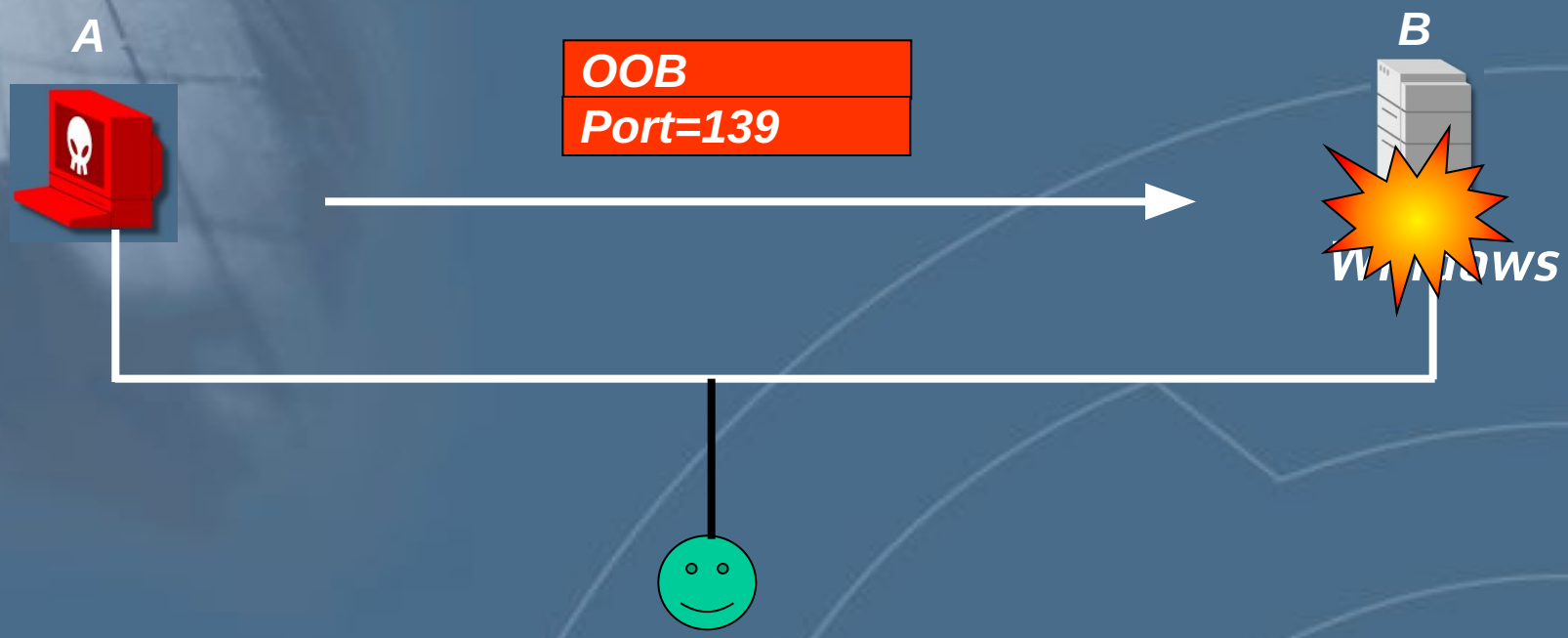
- **Сетевые пакеты (фреймы)**



Принципы работы систем обнаружения атак

- Обнаружение аномалий
- Анализ сигнатур

Анализ сигнатур



- Атака “WinNuke”

Сигнатуры «State-less» (однопакетные)

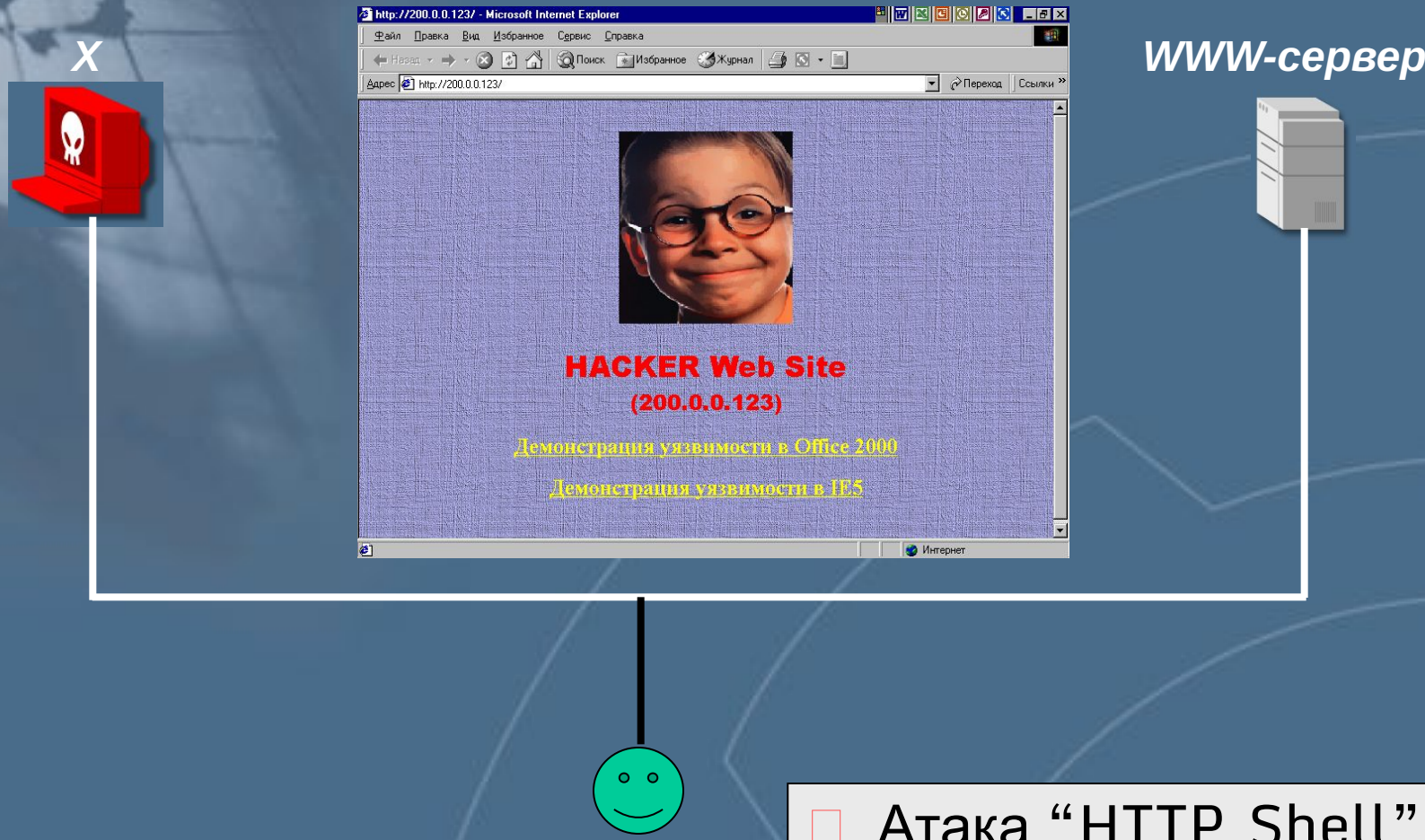
Анализ сигнатур

SYN	Узел А
SYN	Узел А
SYN	Узел А
SYN	Узел А
SYN	**Узел А**

- Атака “SynFlood”

Сигнатуры «State-based» (анализ таблиц)

Анализ сигнатур



- Атака “HTTP_Shell”

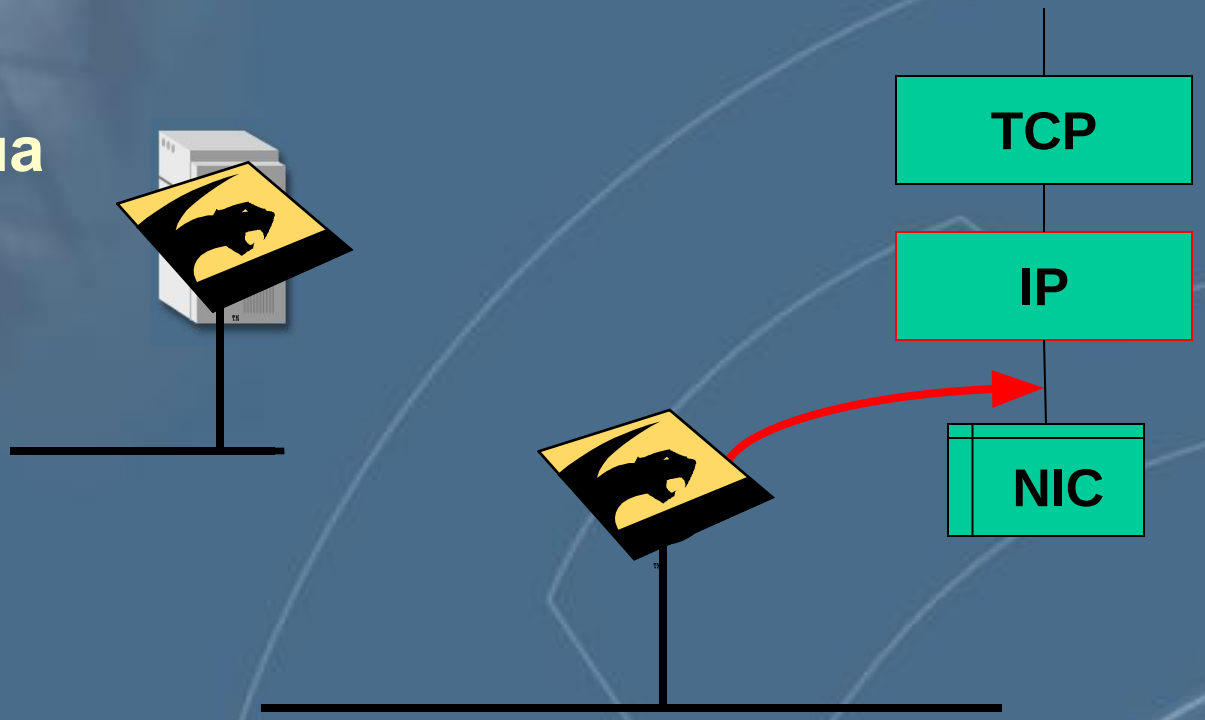
Сигнатуры «Stream-oriented» (сборка сегментов)

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

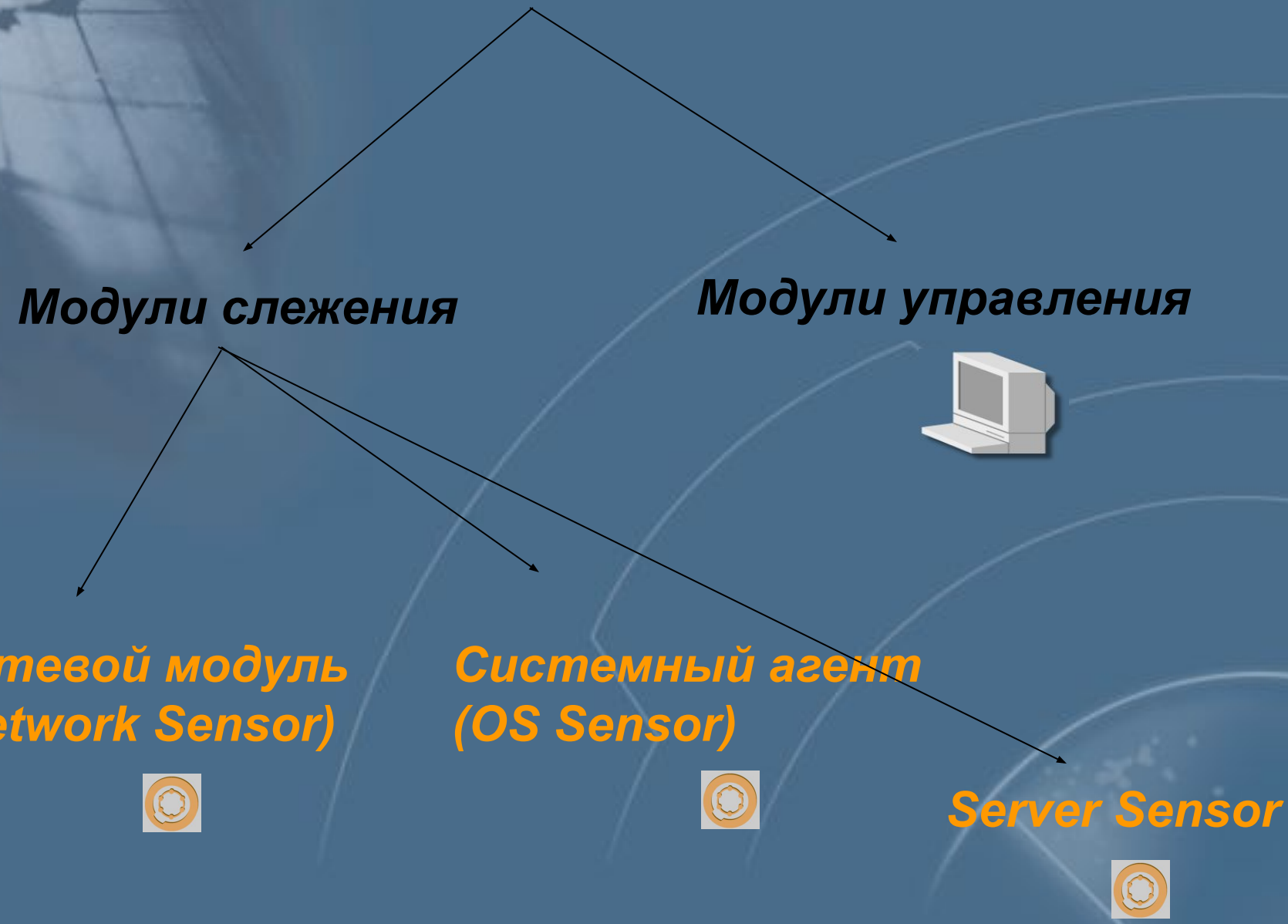
Система обнаружения атак RealSecure

На базе узла

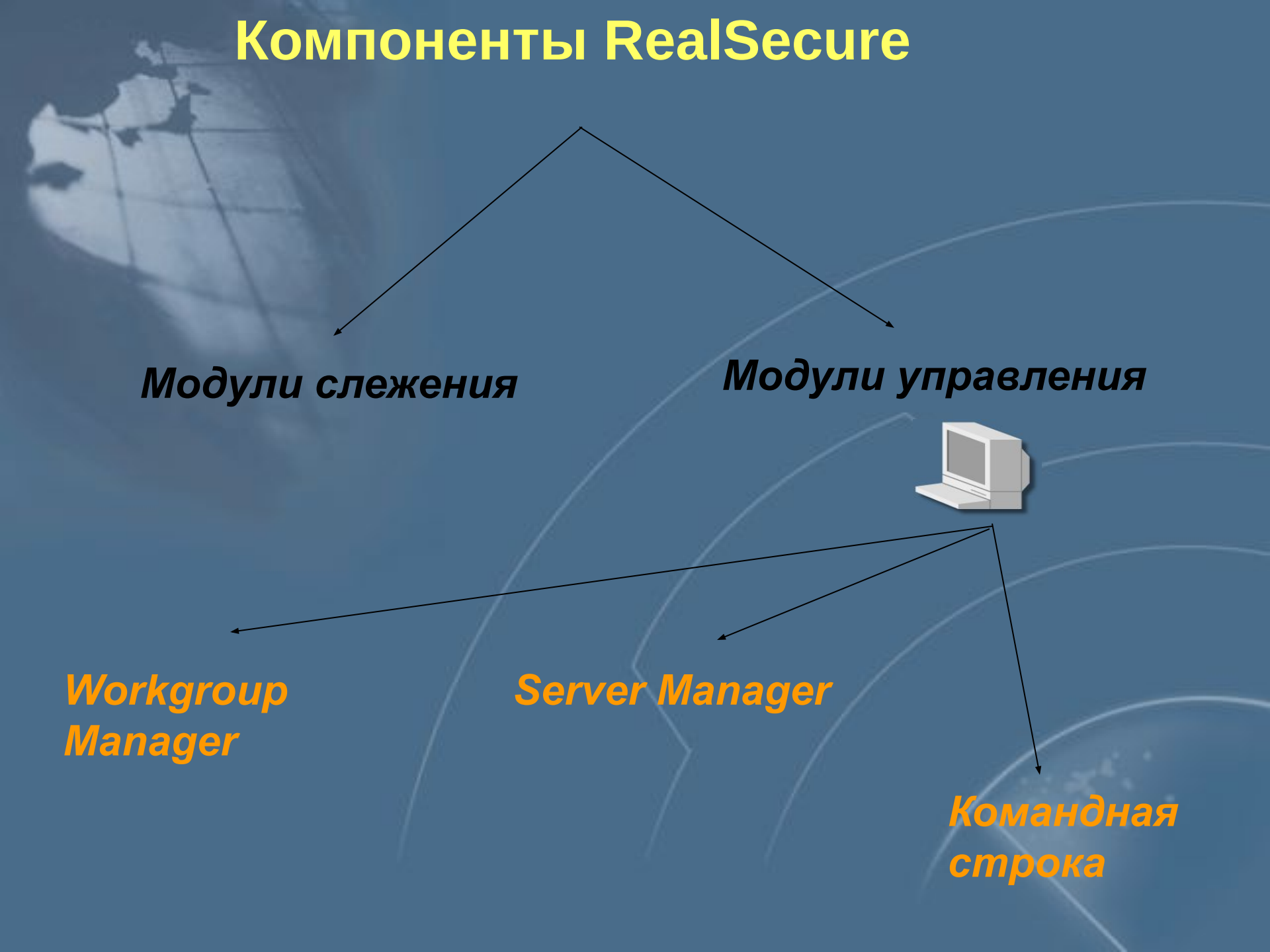


На базе сети

Компоненты RealSecure



Компоненты RealSecure



Компоненты RealSecure

Модули управления

Server Manager

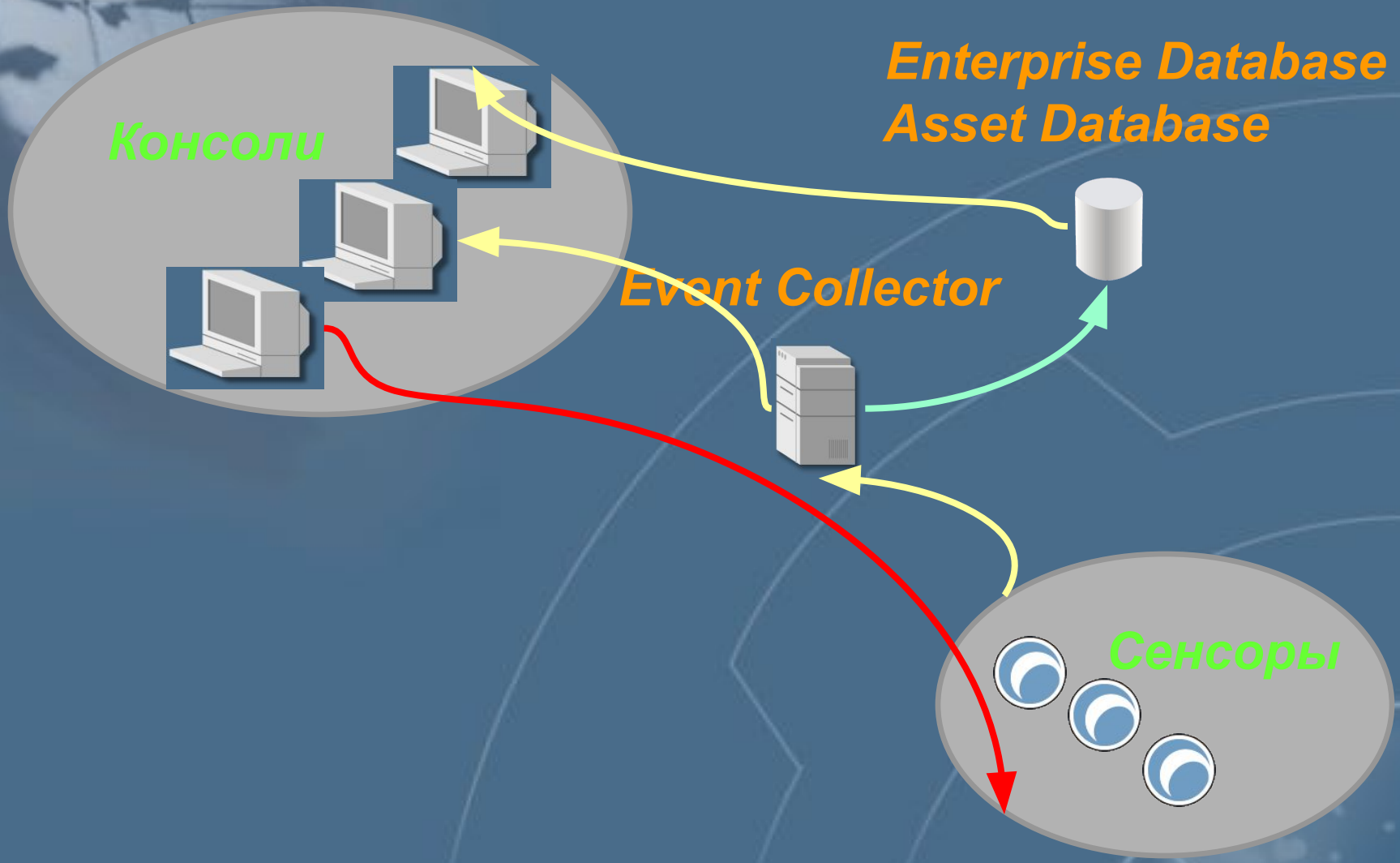
Командная строка

Workgroup Manager

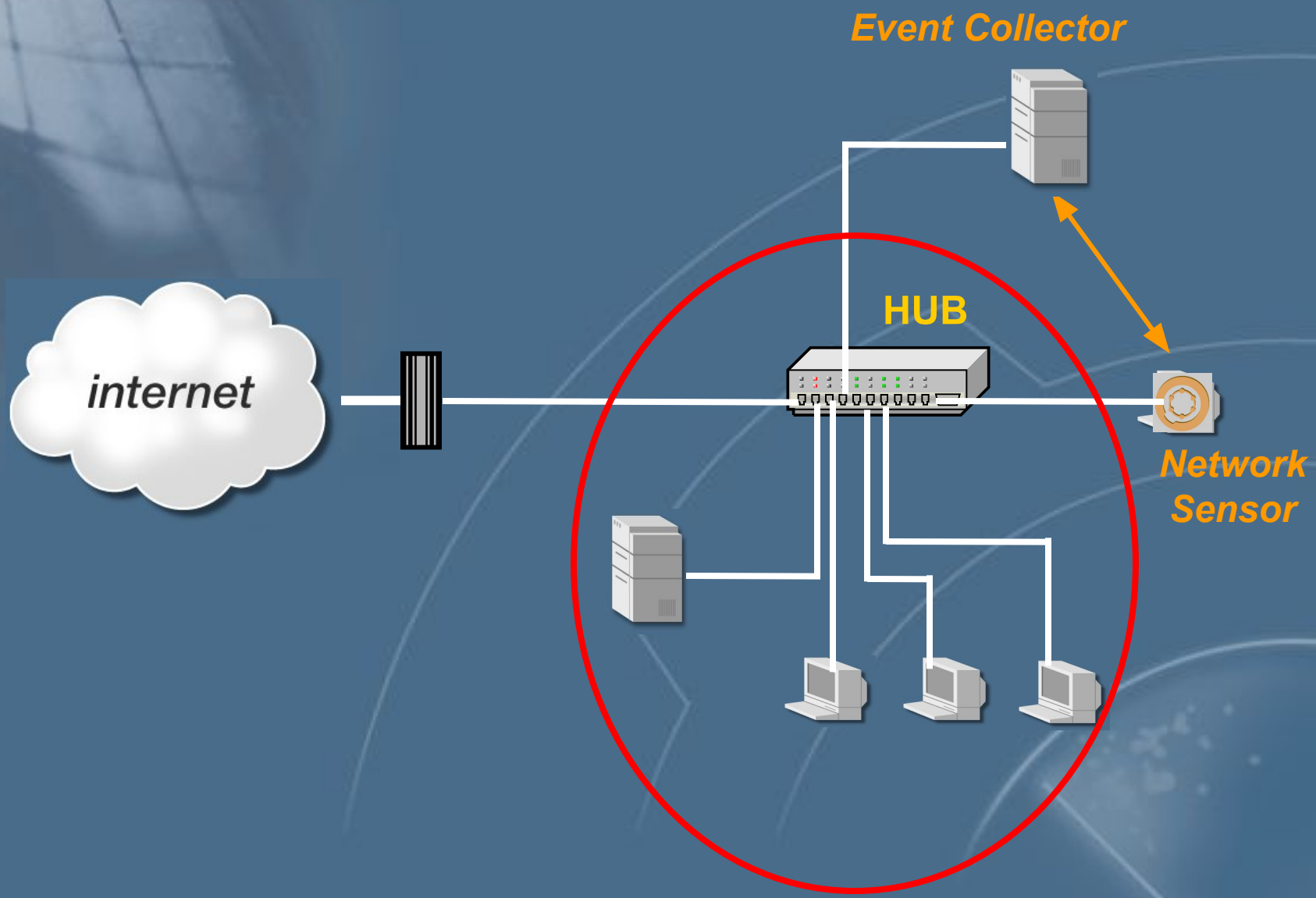
- ***Event Collector***
- ***Enterprise Database***
- ***Asset Database***
- ***Console***

Архитектура

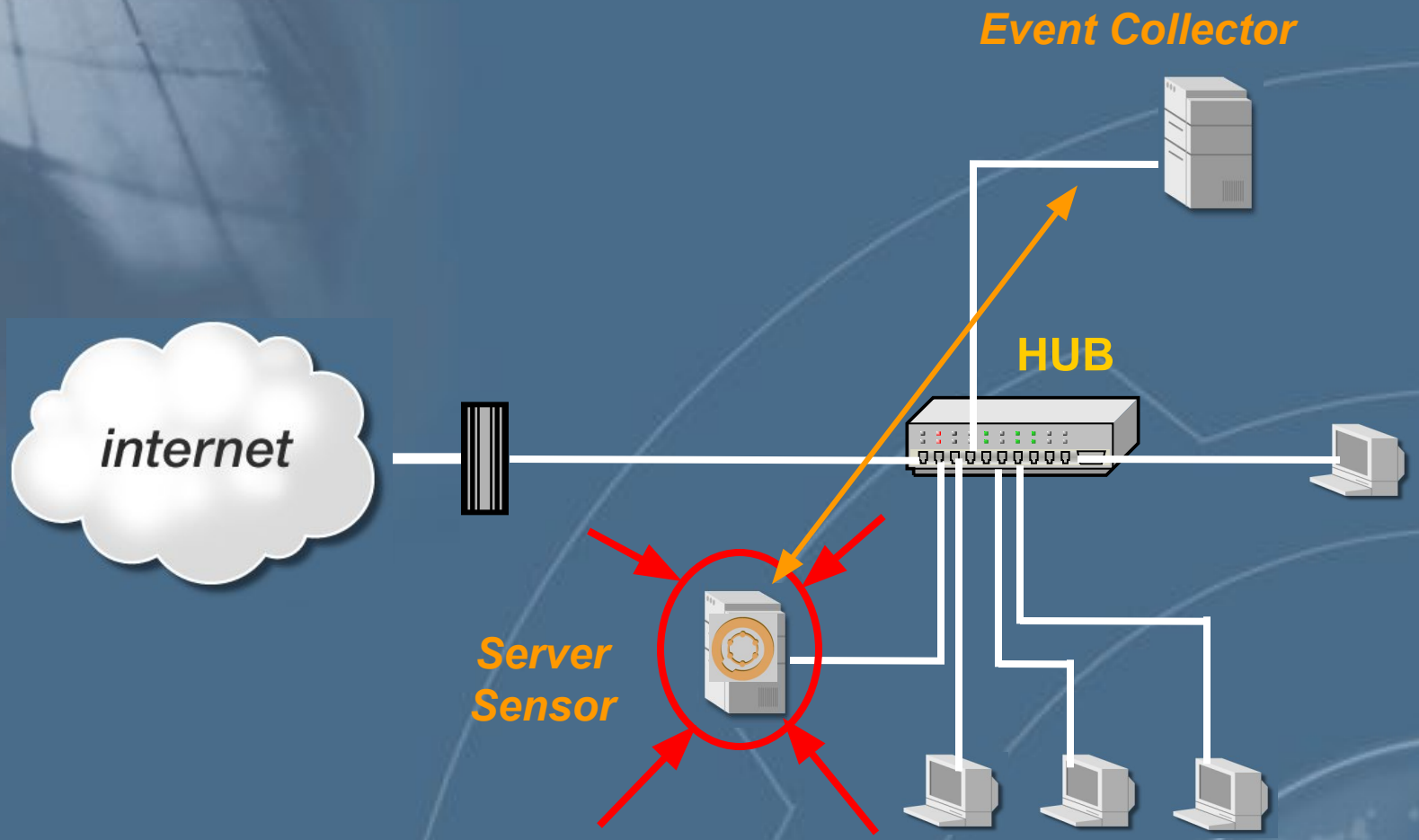
Взаимодействие компонентов



Расположение сетевого модуля



Расположение Server Sensor



Пример атаки

Шаг 1.
При сканировании портов через МЭ была обнаружена служба rlogin на нескольких узлах и служба IMAP, содержащая уязвимость, на почтовом сервере

Шаг 2. Использование уязвимости в службе IMAP для получения доступа с правами администратора к почтовому серверу в DMZ.

Шаг 3. Почтовый сервер используется в качестве платформы для получения доступа к узлу с ОС Unix за МЭ

Шаг 4. Получение доступа к файлам, содержащим пароли и попытка их расшифровки. Получение доступа к другим узлам сети

Шаг 5. Установка серверной части троянского коня на одном из узлов

Пример атаки: Сеть + RealSecure

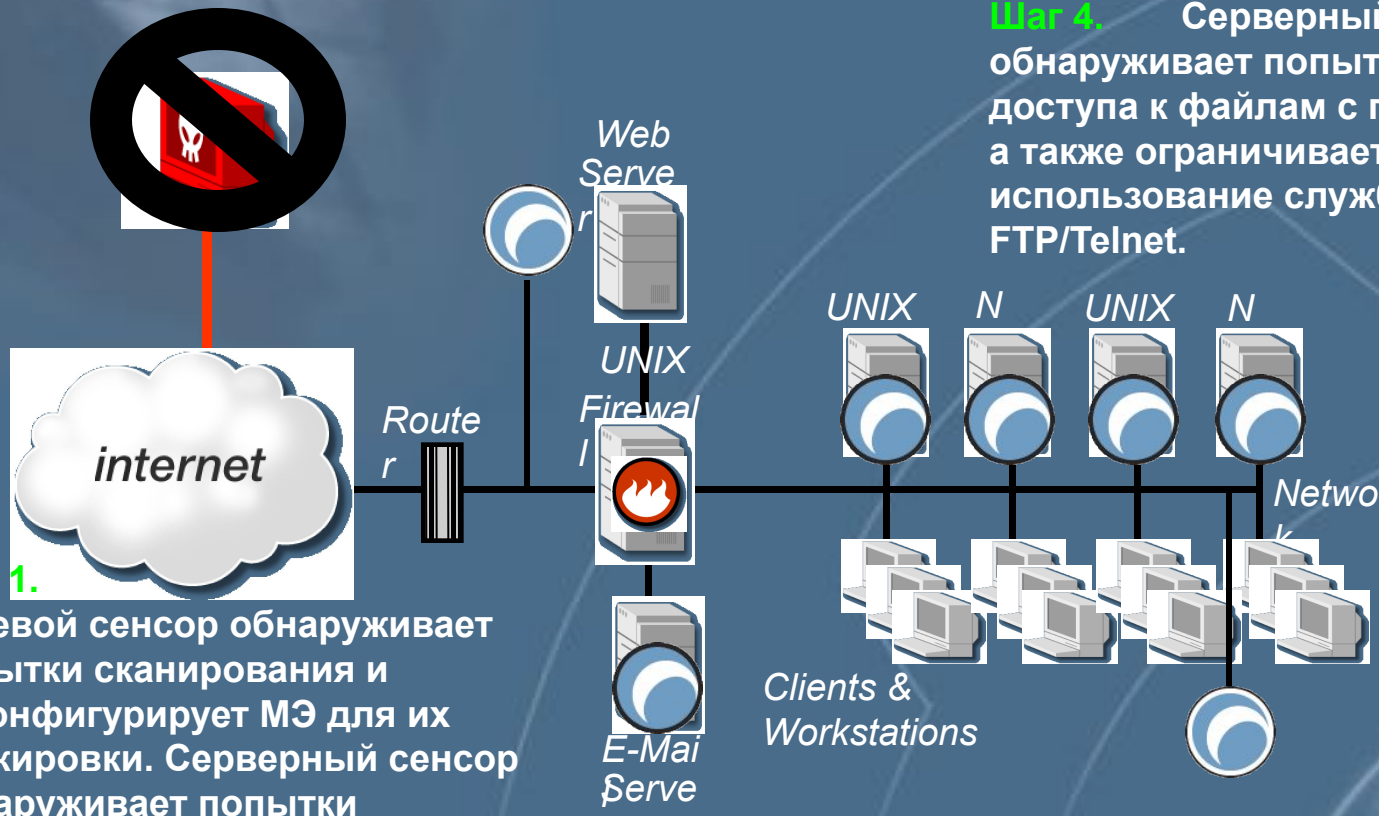
Шаг 3.
Серверный сенсор оповещает о попытках подключения со стороны узла из DMZ или блокирует такие попытки.

Network Sensors

Server Sensors

Шаг 4. **Серверный сенсор обнаруживает попытки доступа к файлам с паролями а также ограничивает использование служб FTP/Telnet.**

Шаг 5. **Сетевой и серверный сенсор обнаруживают попытки установки или использования серверных частей троянских коней**



Шаг 1.
Сетевой сенсор обнаруживает попытки сканирования и реконфигурирует МЭ для их блокировки. Серверный сенсор обнаруживает попытки подключения к портам и блокирует ответы на них.

Шаг 2. **Сетевой сенсор обнаруживает атаку на службу IMAP. Серверный сенсор блокирует исходящие соединения, направленные во внутреннюю сеть**

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*

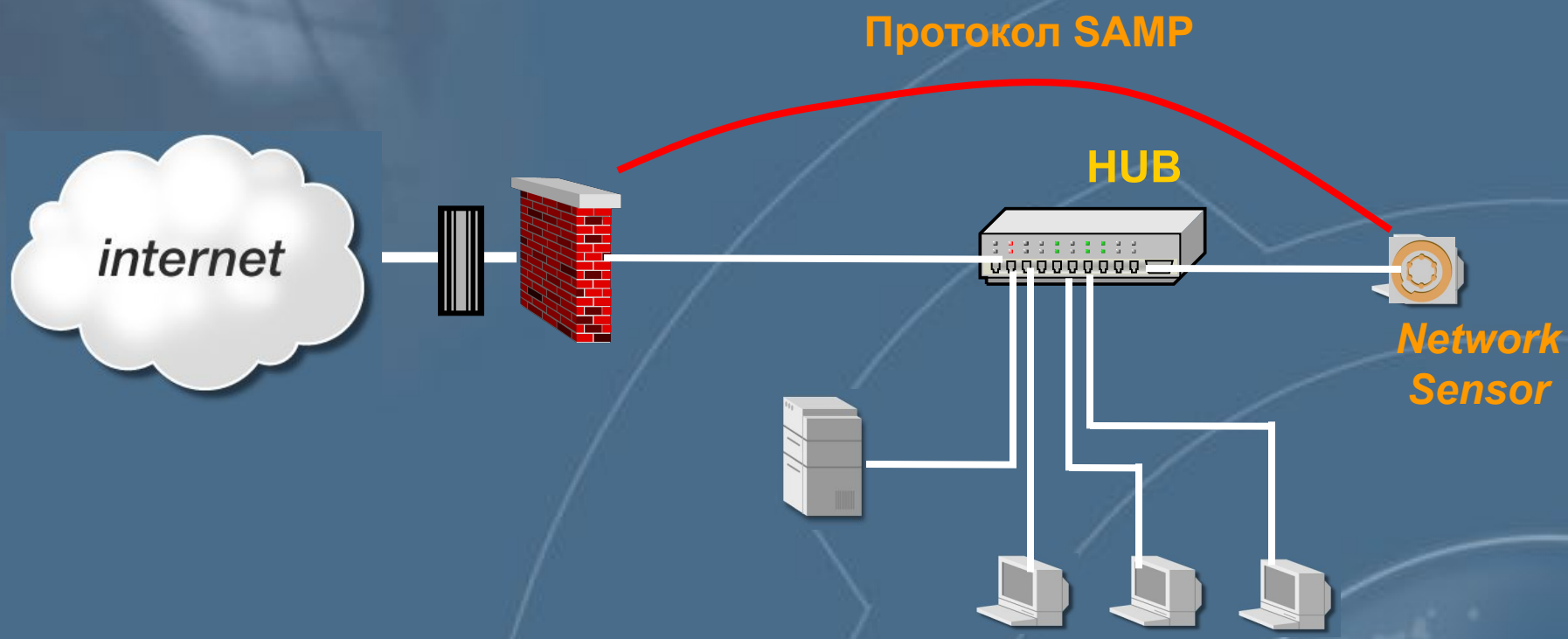
Регистрация события в БД

Расширенная регистрация с возможностью последующего воспроизведения

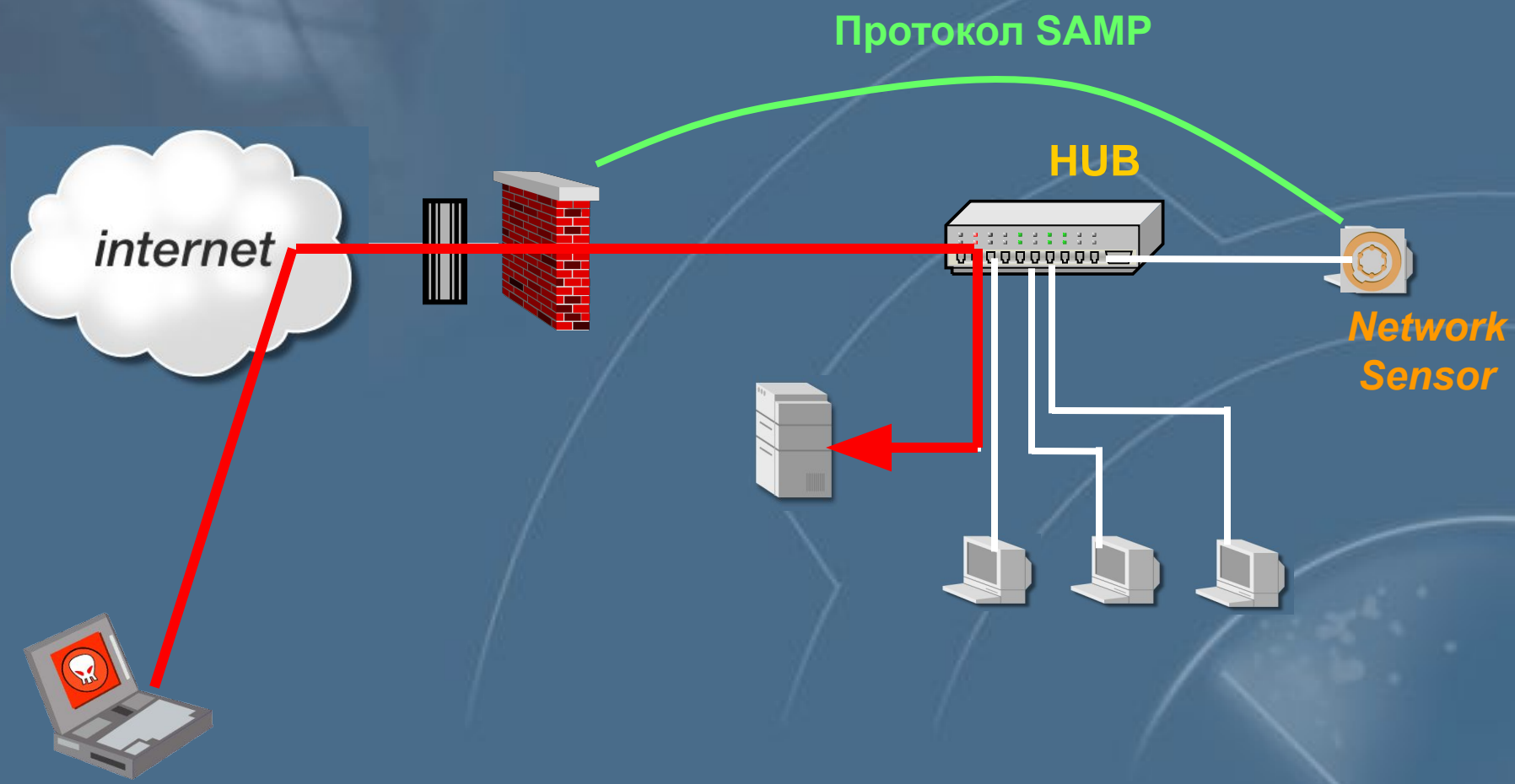
Обнаружение атак и МЭ

- Использование OPSec SDK, предоставляющих необходимые API
- Применение открытых протоколов
  - CVP(Content Vectoring Protocol)
  - UFP (URL Filter Protocol)
  - SAMP (Suspicious Activity Monitoring Protocol)
- Использование языка INSPECT

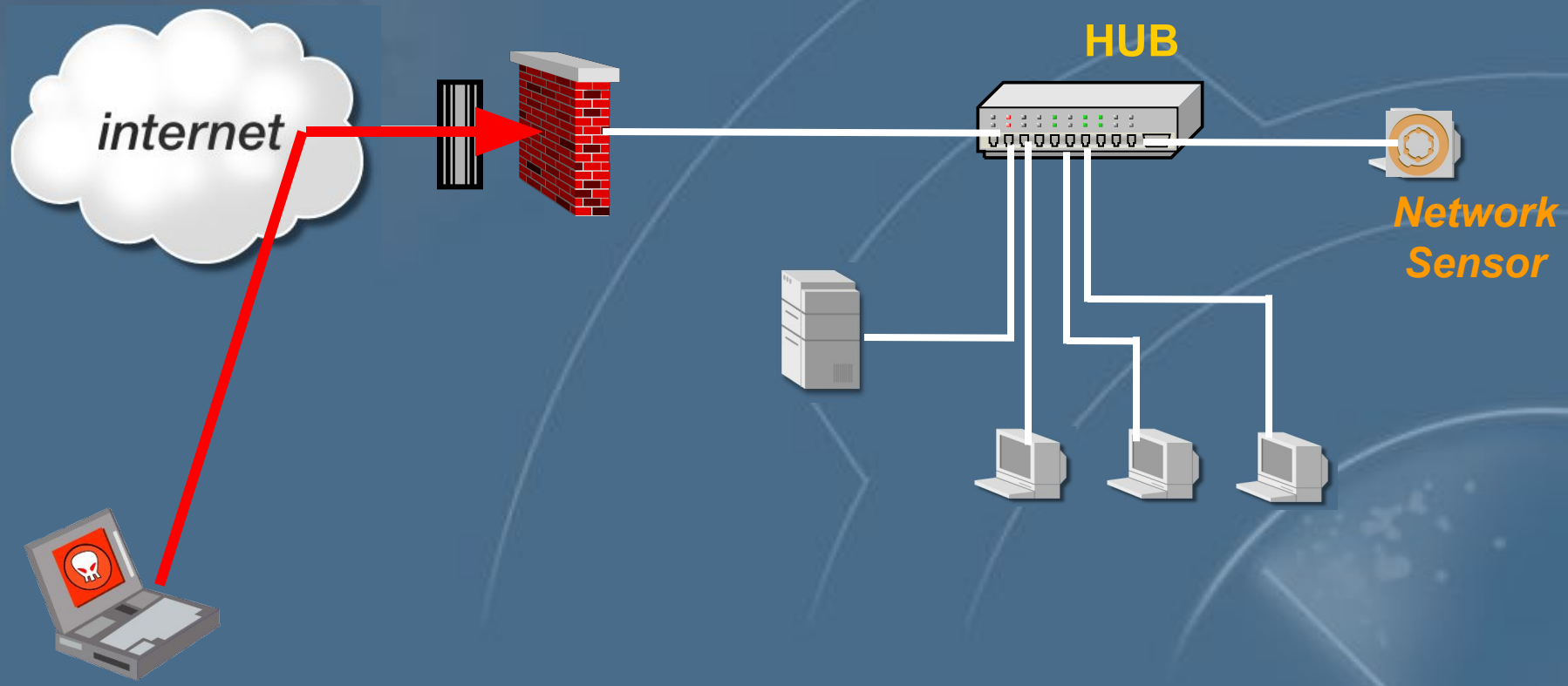
Реконфигурация МЭ



Реконфигурация МЭ



Реконфигурация МЭ



Практическая работа 12

Работа с программой RealSecure

Система обнаружения атак Snort

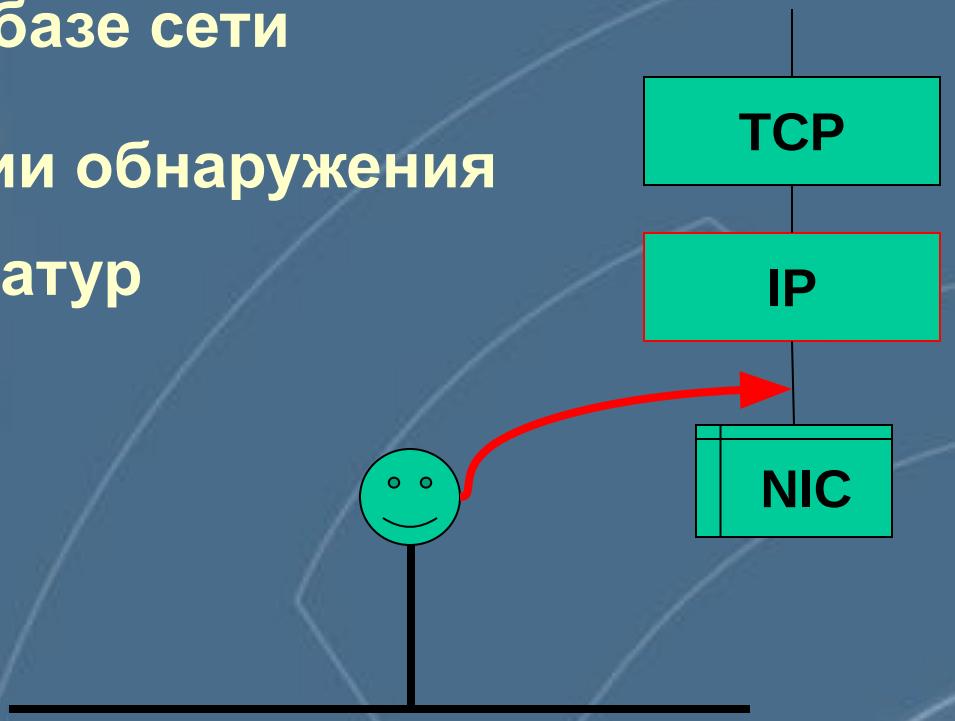
Архитектура

По принципу реализации

- **Система на базе сети**

По технологии обнаружения

- **Анализ сигнатур**



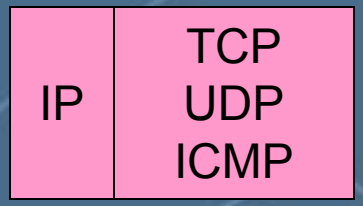
Режимы работы

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

Sniffer Mode

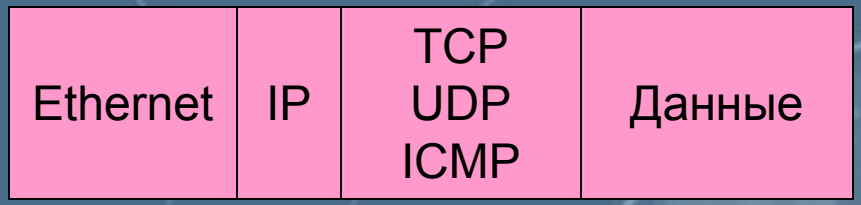
Вывод на экран содержимого пакетов

```
./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)

Практическая работа 13

Работа с программой Snort