

# Средства обнаружения атак

Раздел 2 – Тема 14

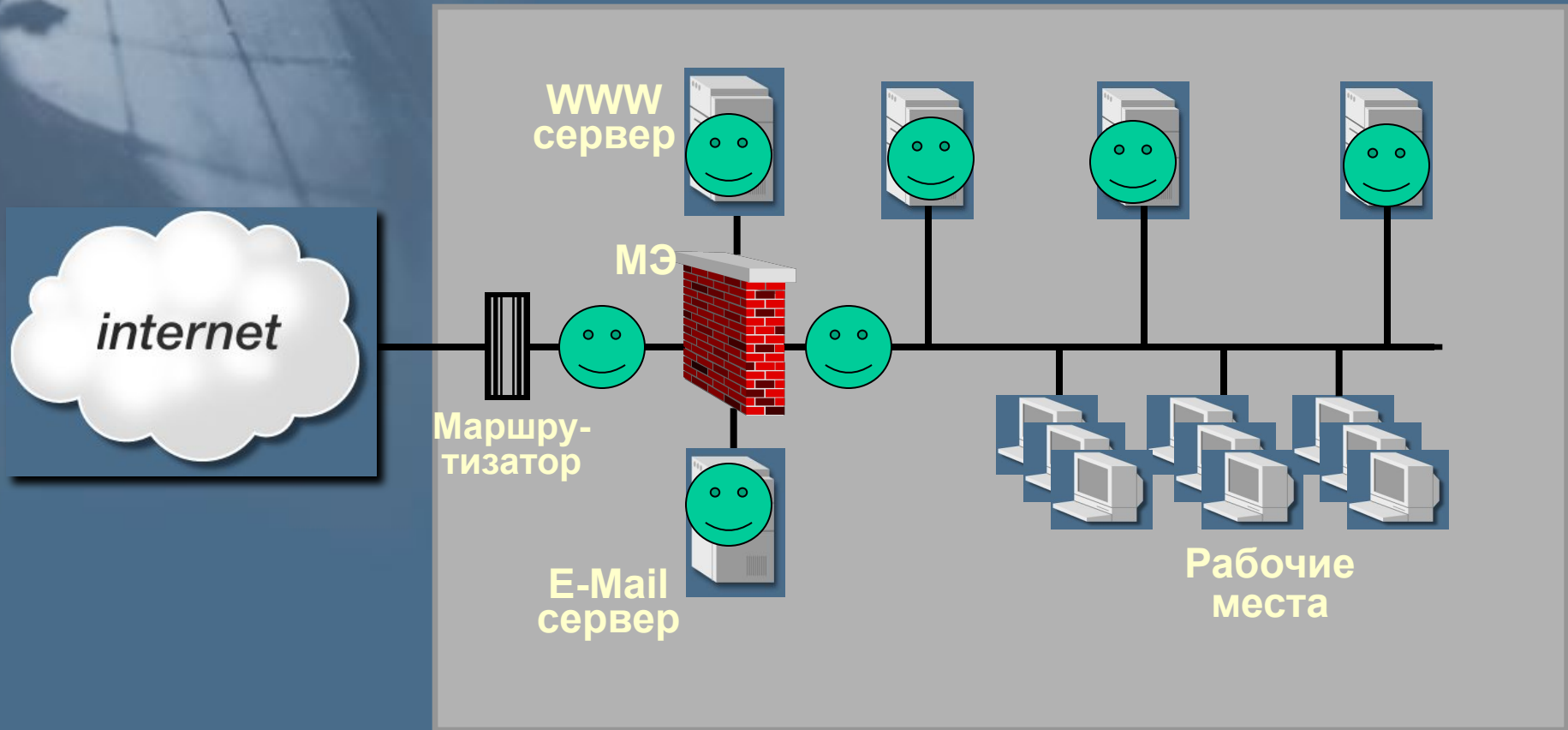
# Средства защиты сетей

- МЭ
- Средства анализа защищённости
- Средства обнаружения атак

# Архитектура систем обнаружения атак

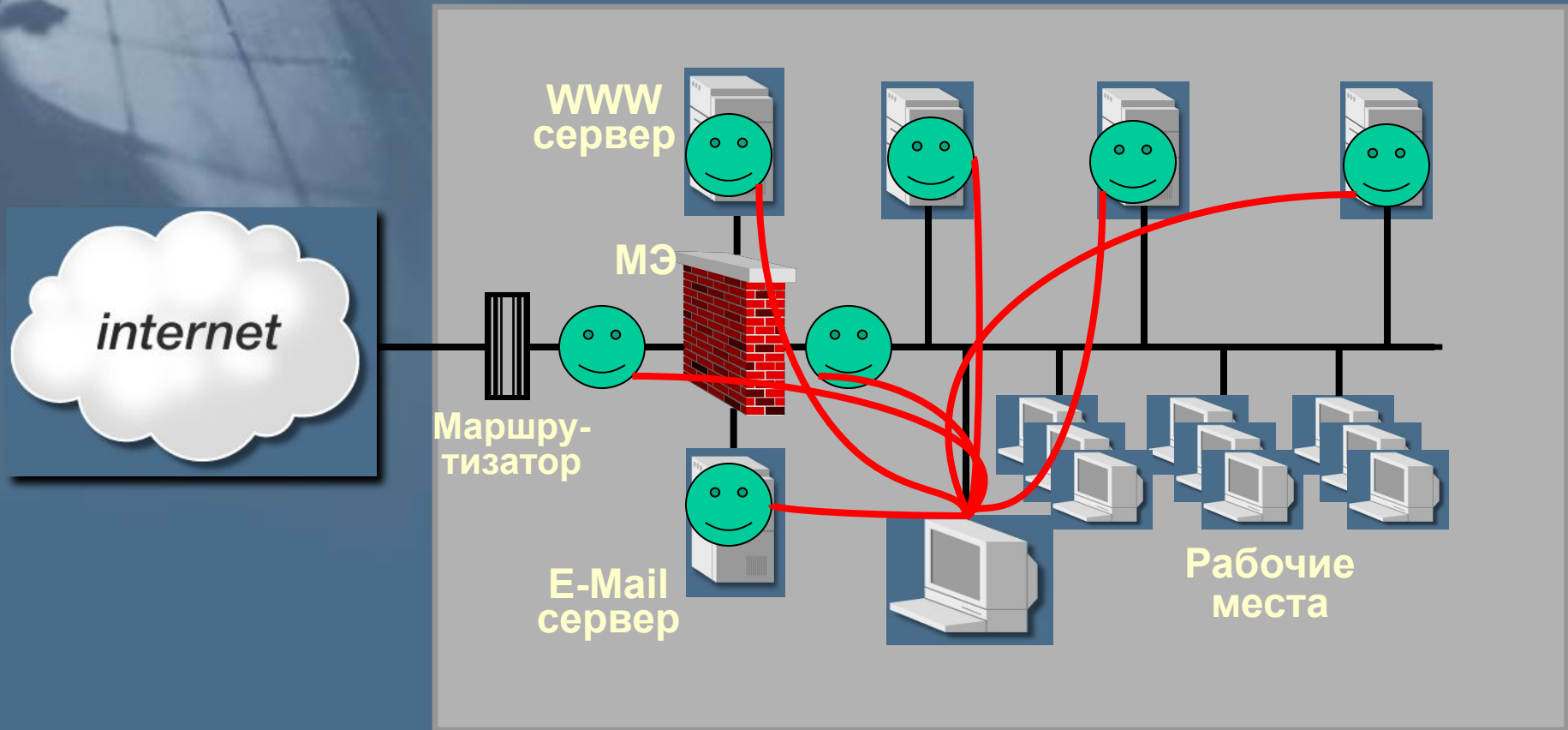
- Модуль слежения
- Модуль управления
  
- Системы на базе узла
- Системы на базе сегмента

# Архитектура систем обнаружения атак



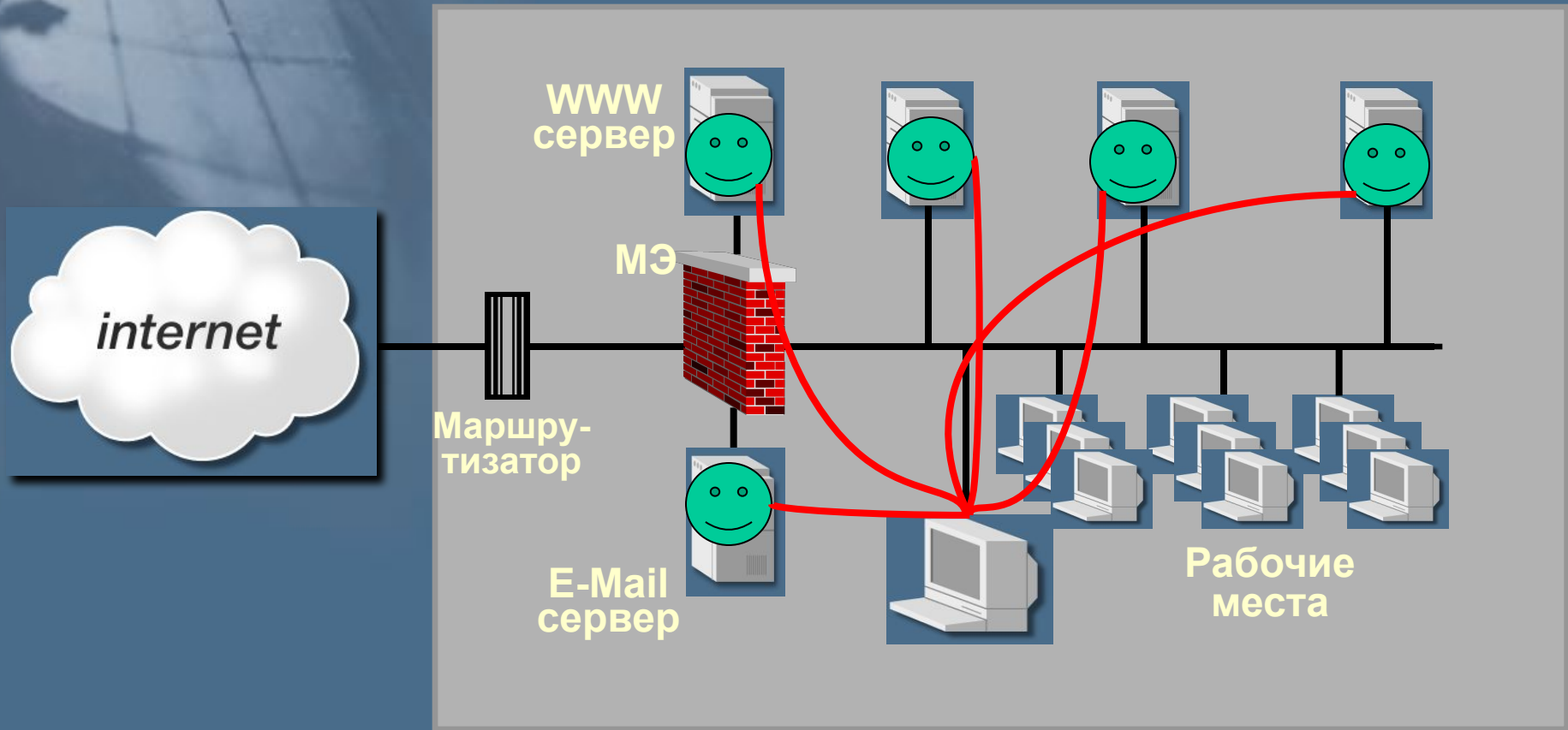
Сенсоры

# Архитектура систем обнаружения атак



Управляющие компоненты

# Системы обнаружения атак на базе узла



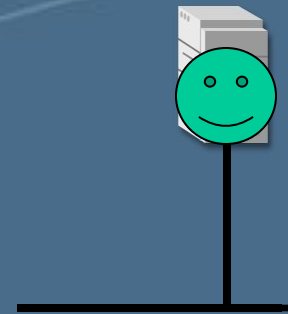
# Системы обнаружения атак на базе узла

## Источники данных:

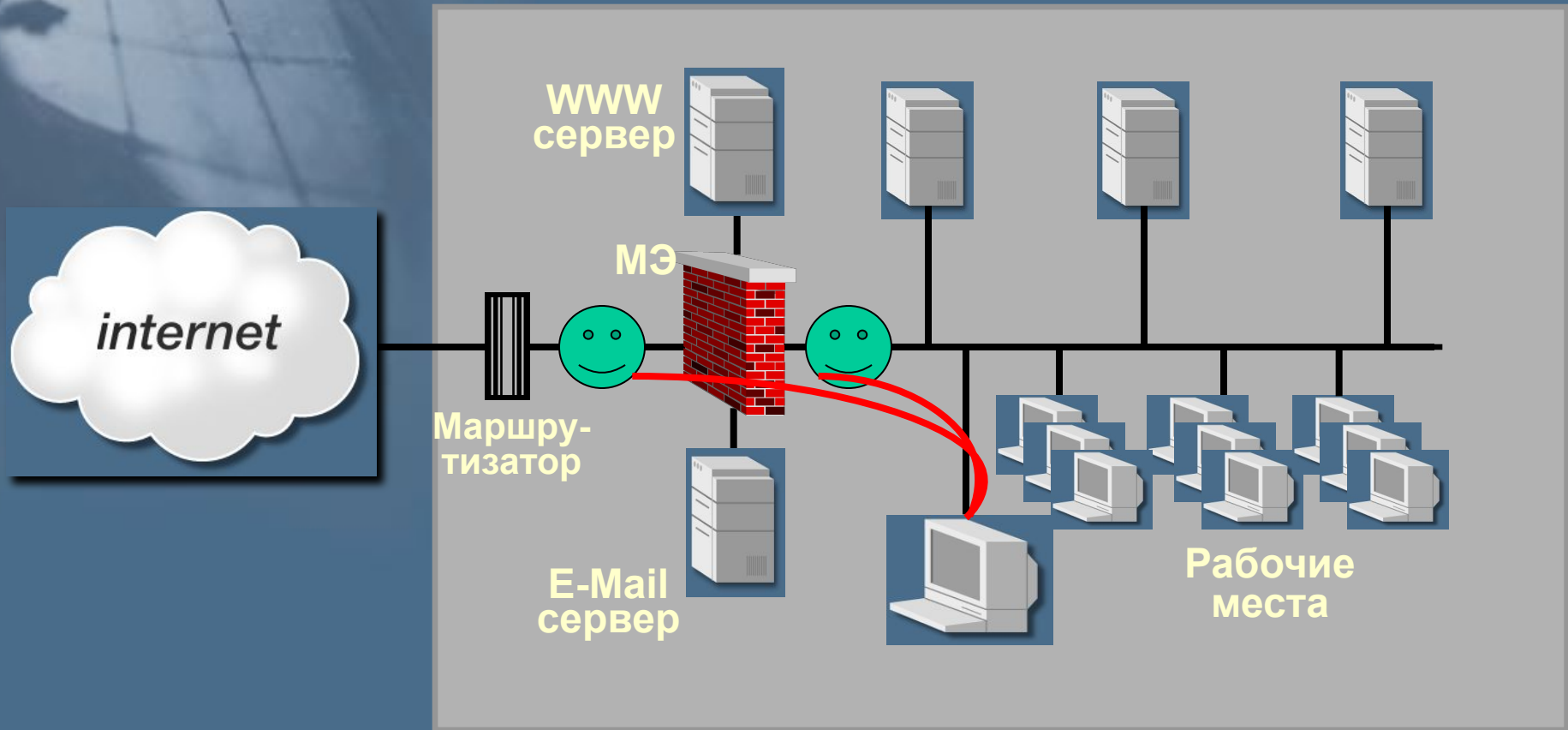
- Журналы аудита
- Действия пользователей

## Необязательно:

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



# Системы обнаружения атак на базе сети

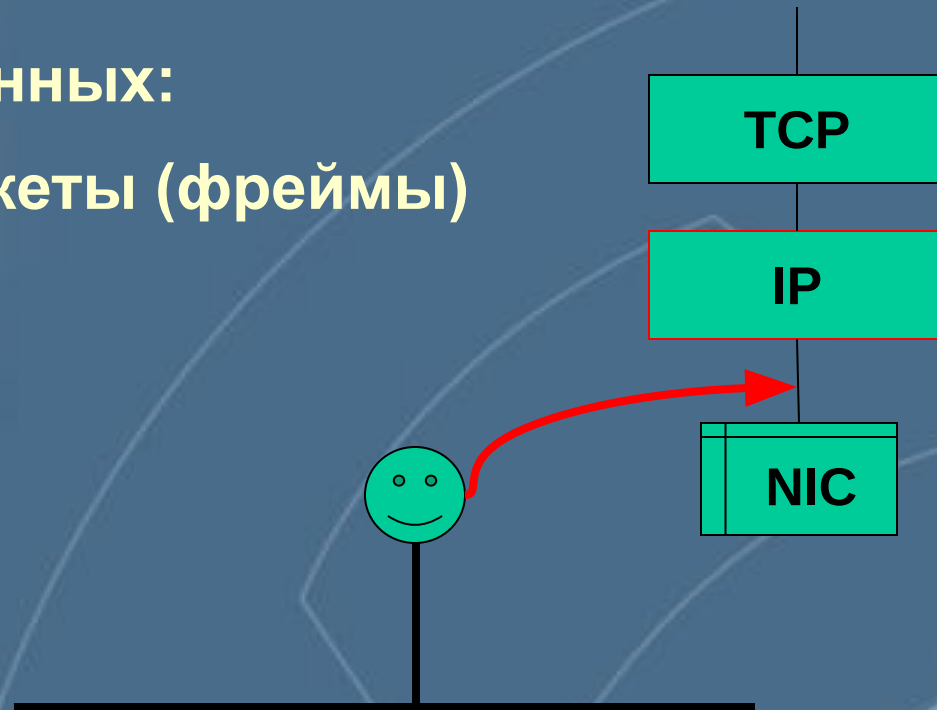




# Системы обнаружения атак на базе сети

Источник данных:

- Сетевые пакеты (фреймы)



# Принципы работы систем обнаружения атак



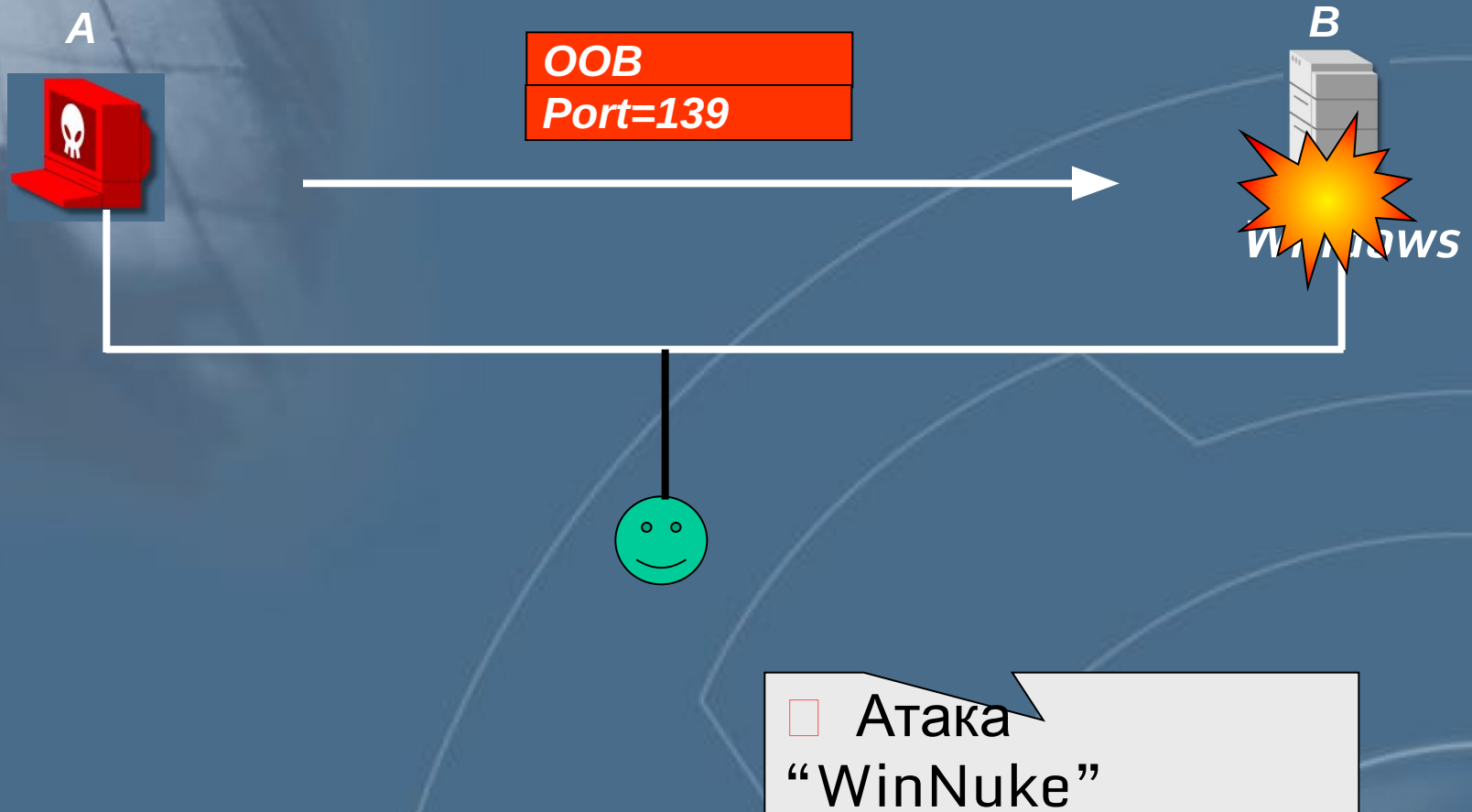
Обнаружение аномалий



Анализ сигнатур



# Анализ сигнатур



Сигнатуры «State-less» (однопакетные)

# Анализ сигнатур



SYN	Узел А
SYN	Узел А
SYN	Узел А
SYN	Узел А
SYN	Узел А

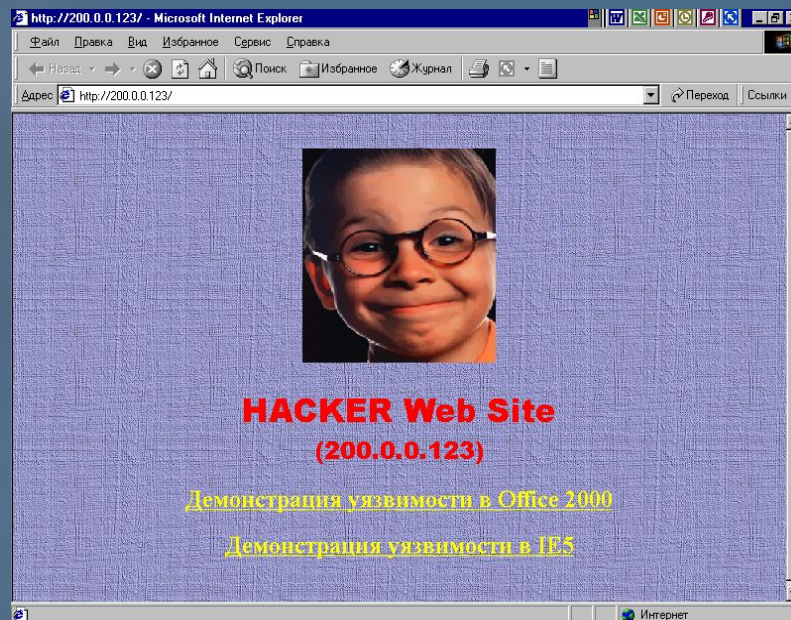


□ Атака  
“SynFlood”

Сигнатуры «State-based» (анализ таблиц)

# Анализ сигнатур

X



WWW-сервер



Атака “HTTP\_Shell”

Сигнатуры «Stream-oriented» (сборка сегментов)

# Системы обнаружения атак

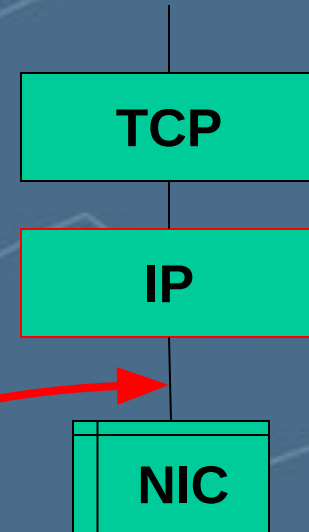
	Net Prowler	Secure IDS	eTrust Intrusion Detection	RealSecure	Snort
Производитель	Axent Technologies	Cisco Systems	Computer Associates	Internet Security Systems	Net
Платформа	Windows NT	Защищенная версия Solaris	Windows NT	Windows NT (2000)	Unix
Технология обнаружения	Сигнатуры атак	Сигнатуры атак	Сигнатуры 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

**Модули слежения**

**Модули управления**

**Сетевой модуль  
(Network Sensor)**



**Системный агент  
(OS Sensor)**



**Server Sensor**





# Компоненты RealSecure

*Модули слежения*

*Модули управления*



*Workgroup  
Manager*

*Server Manager*

*Командная  
строка*

# Компоненты RealSecure

## Модули управления



*Server Manager*



*Командная строка*

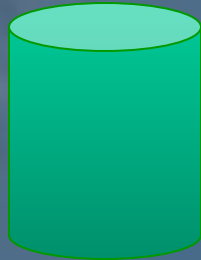
## Workgroup Manager

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

# Архитектура



**Консоли**



**Event Collector**  
(сбор событий с сенсоров)

**Сетевой модуль**  
(Network Sensor)



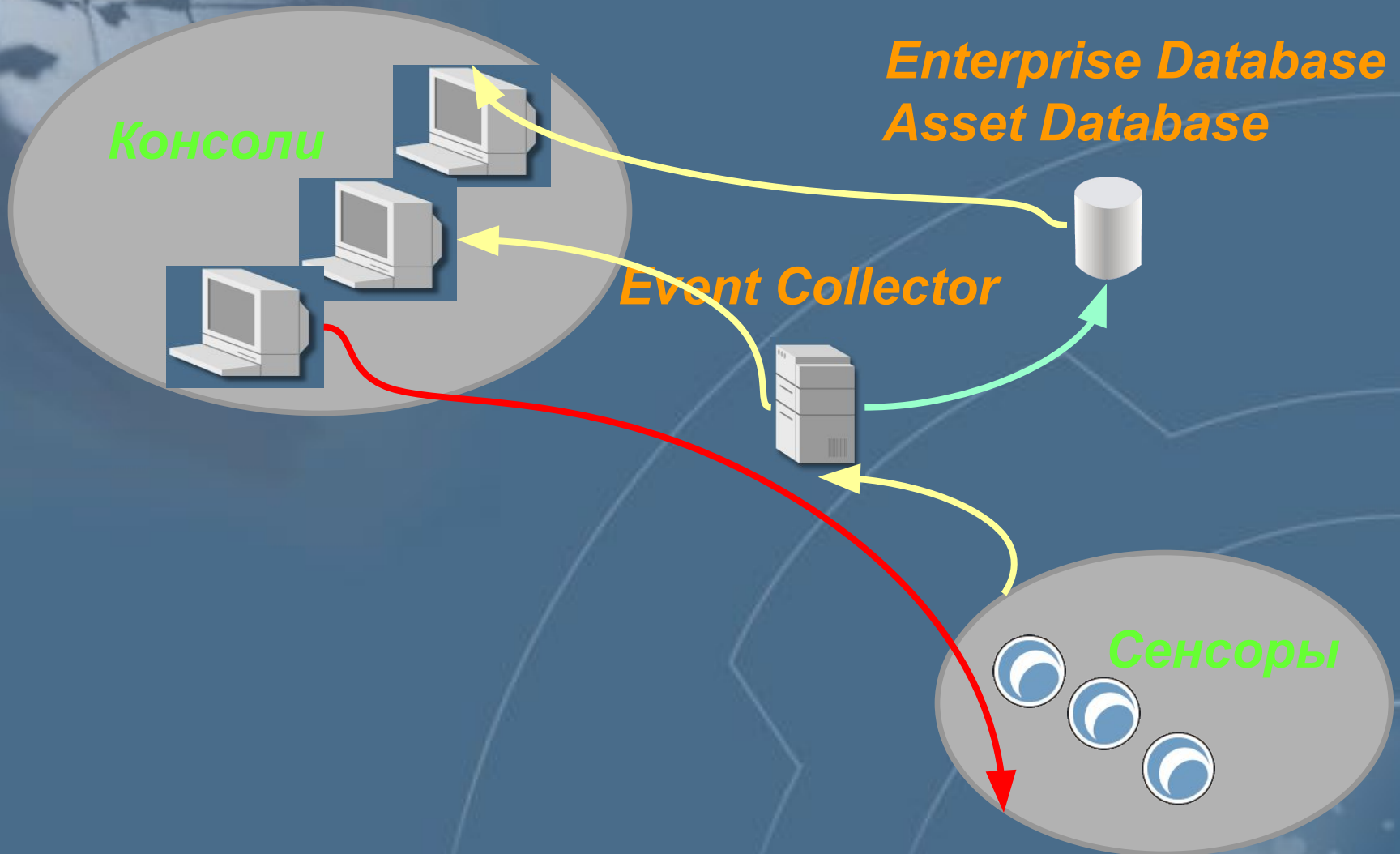
**Системный агент**  
(OS Sensor)



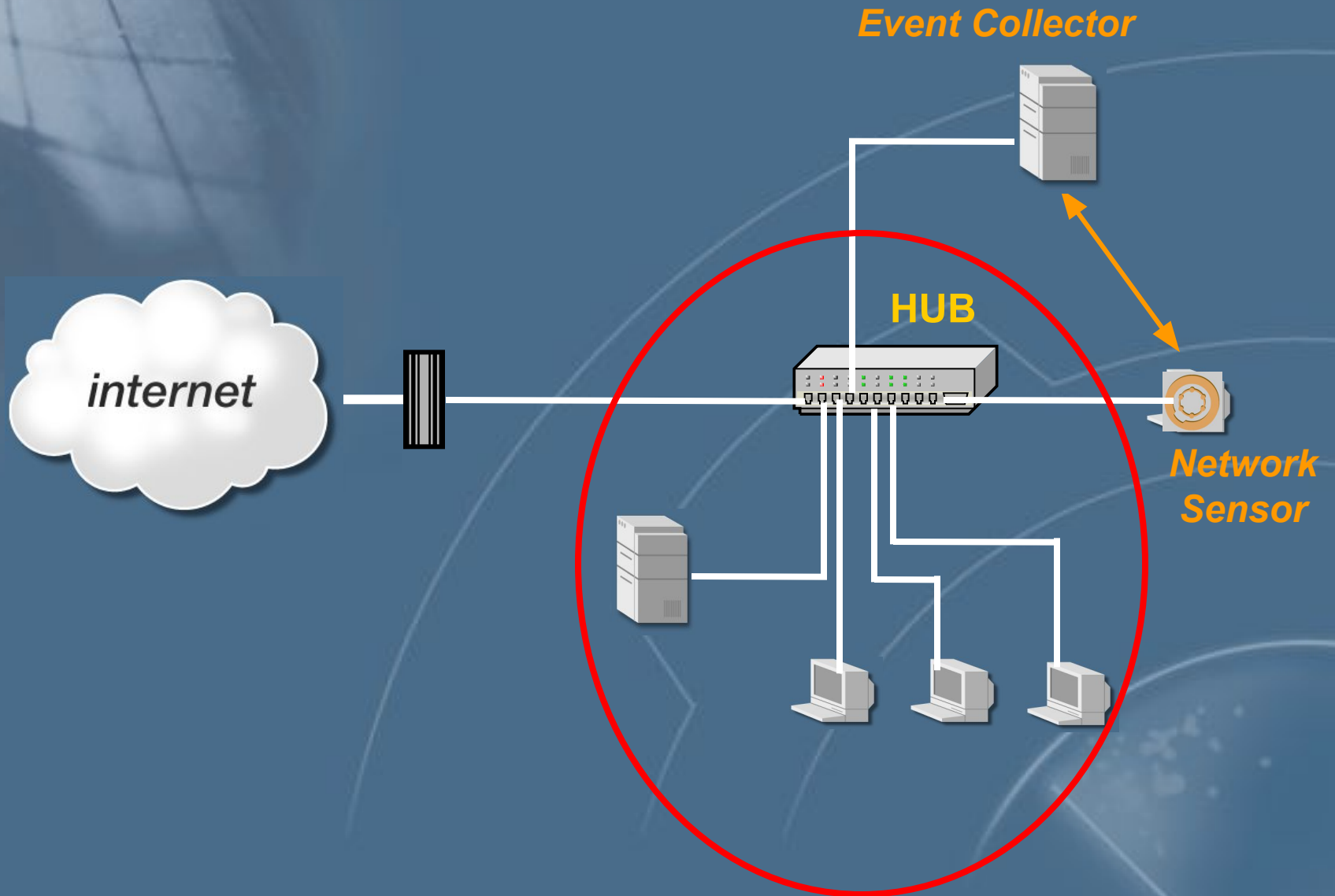
**Server Sensor**



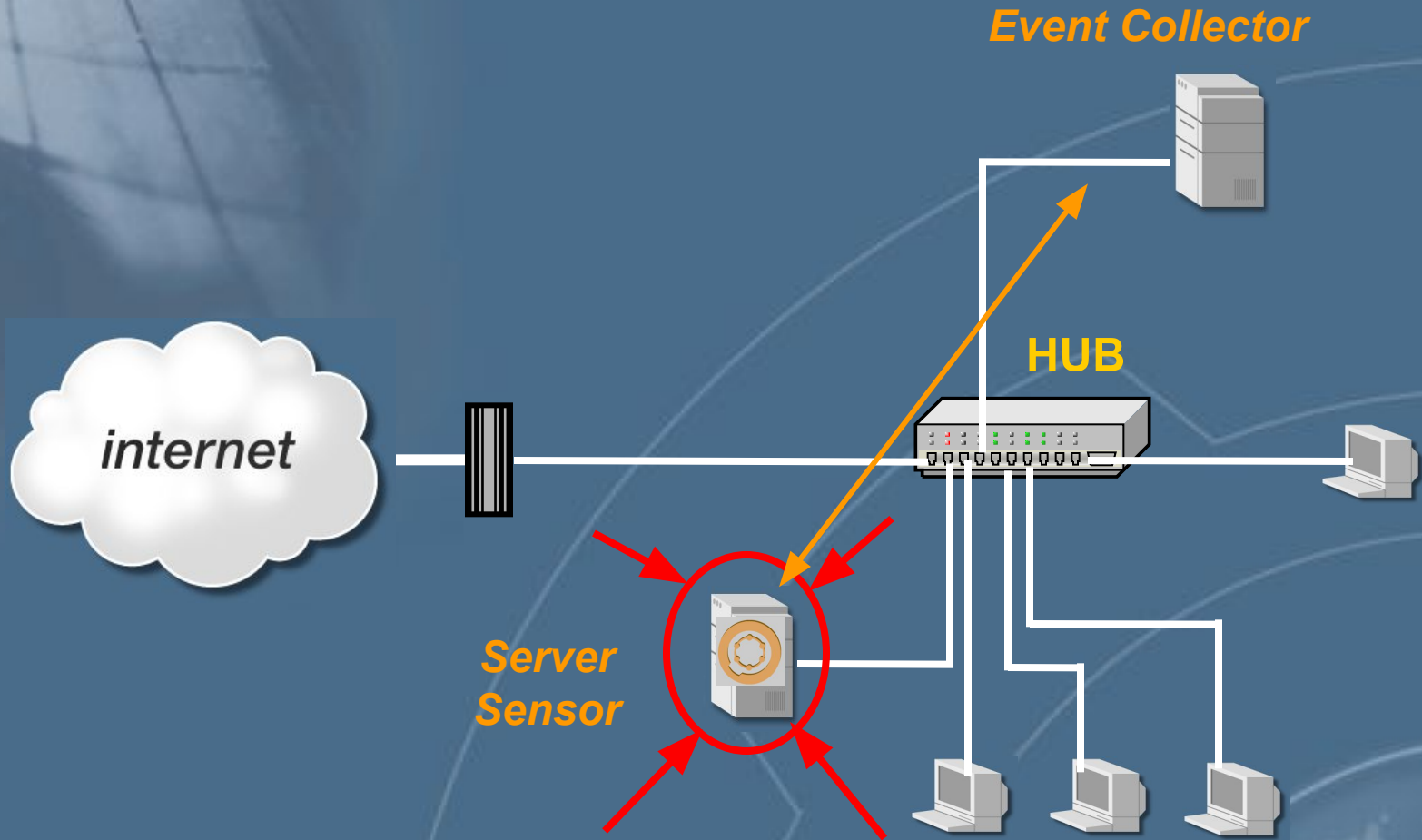
# Взаимодействие компонентов



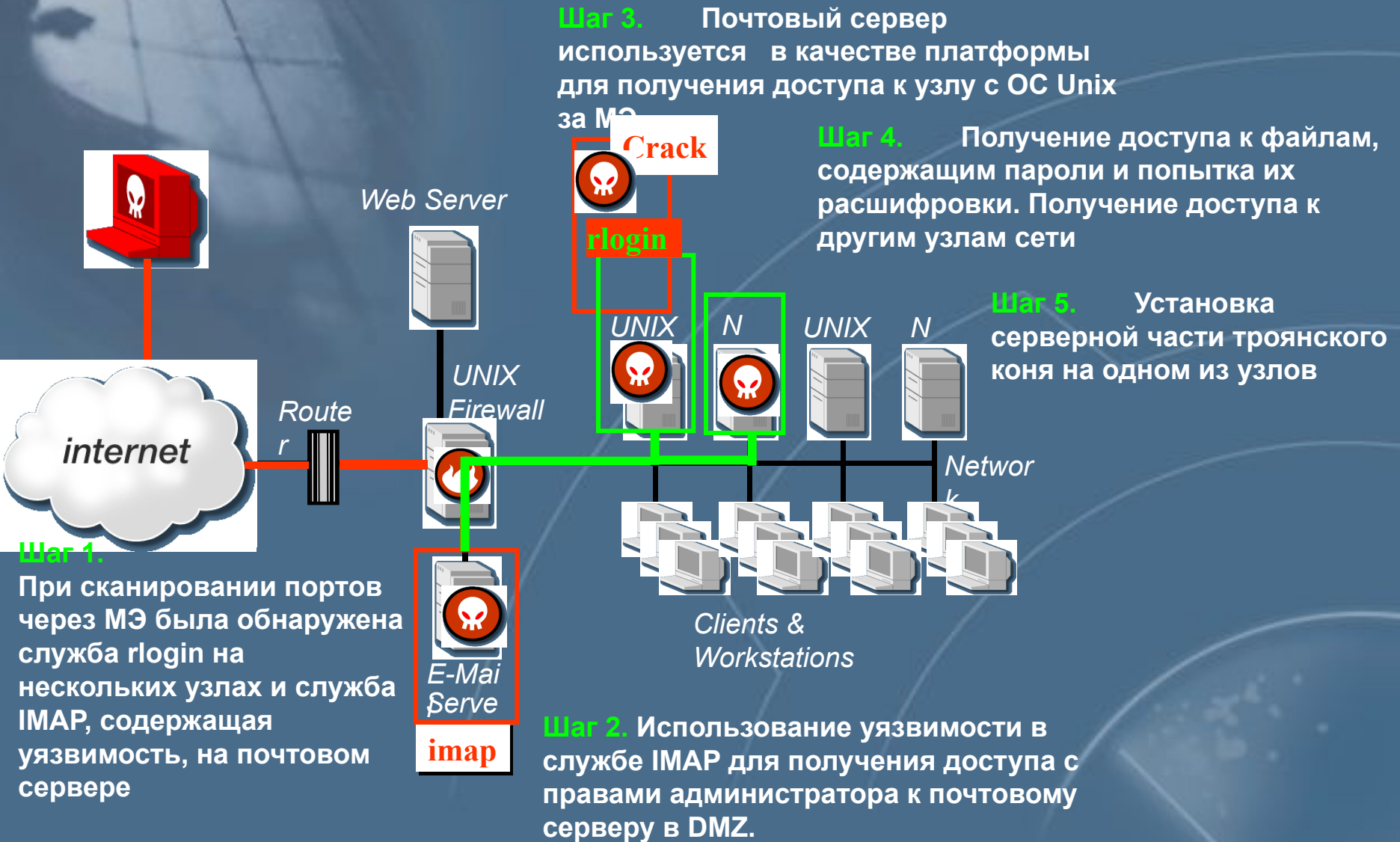
# Расположение сетевого модуля



# Расположение Server Sensor



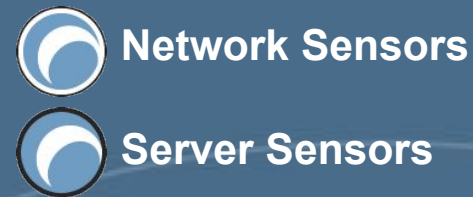
# Пример атаки



# Пример атаки: Сеть + RealSecure

## Шаг 3.

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



## 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.

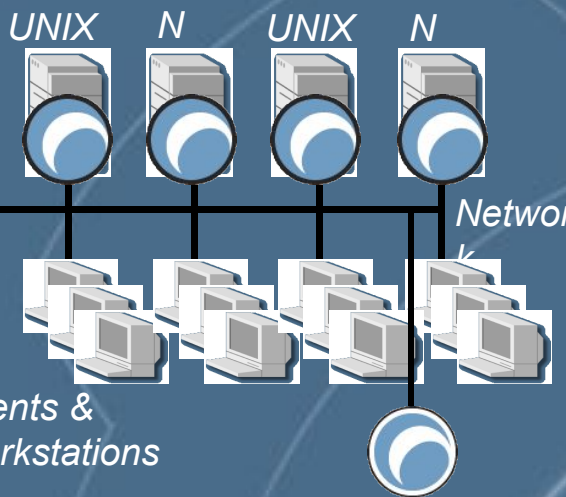


## Шаг 2.

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

## 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



# 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*

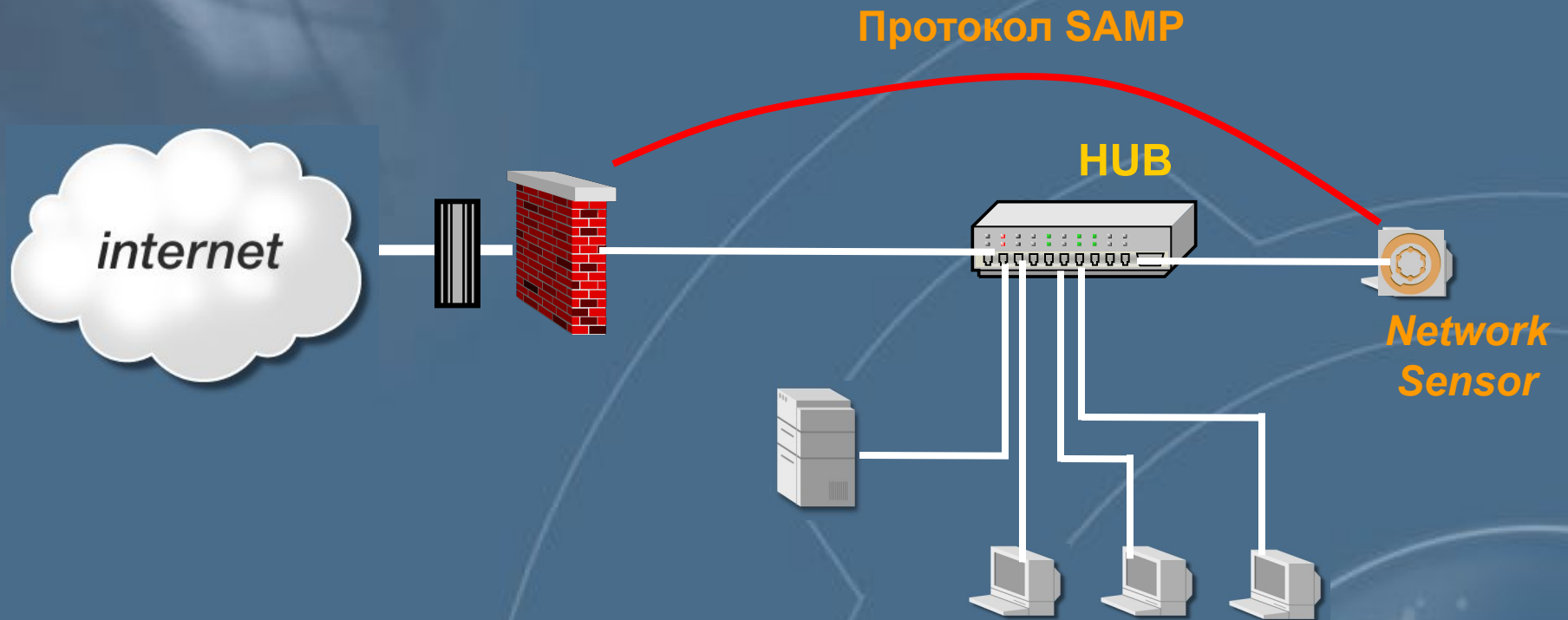
*Расширенная регистрация с возможностью последующего воспроизведения*

# Обнаружение атак и МЭ

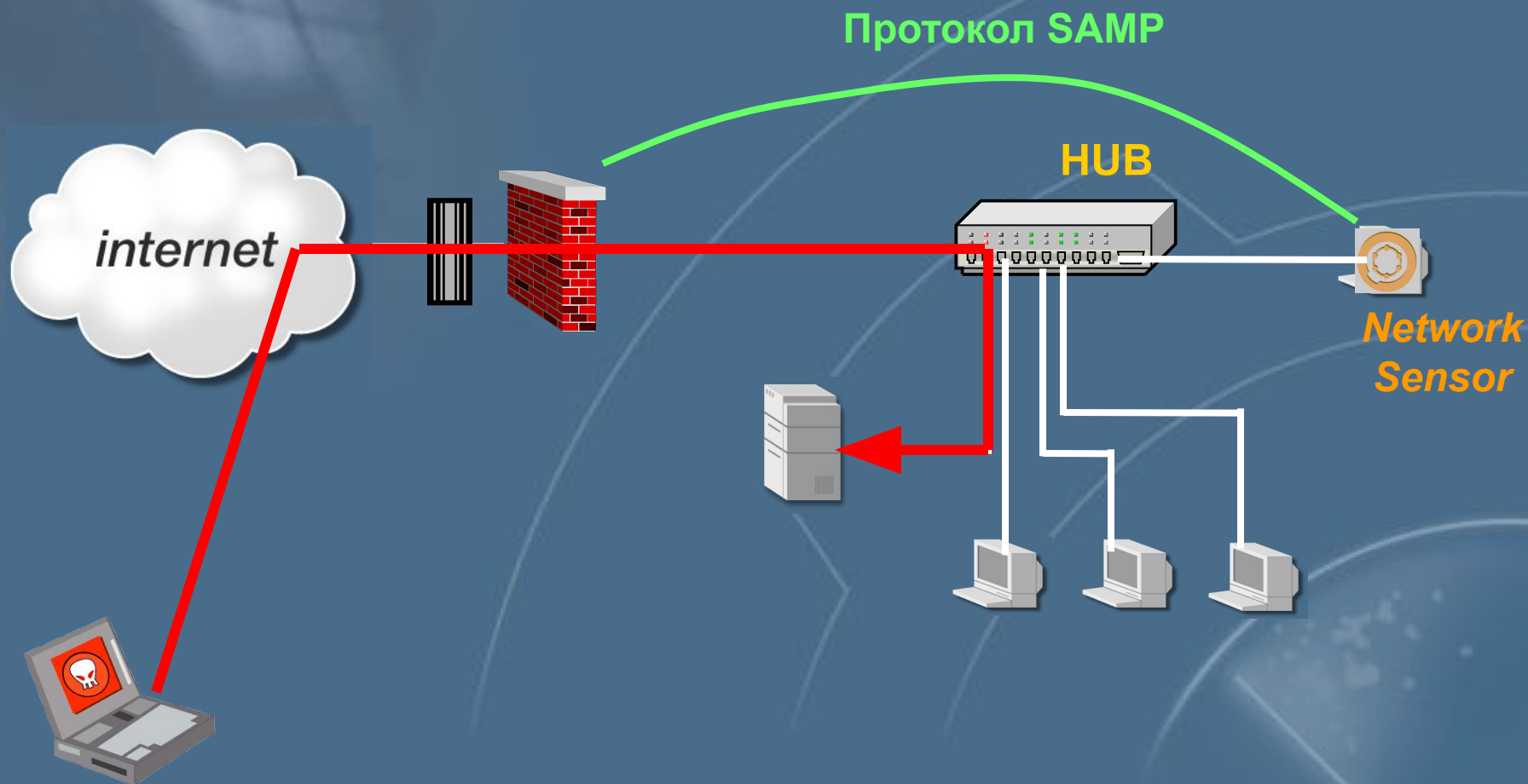
- Использование OPSec SDK, предоставляющих необходимые API
- Применение открытых протоколов
  - CVP(Content Vectoring Protocol)
  - UFP (URL Filter Protocol)
  - SAMP (Suspicious Activity Monitoring Protocol)
- Использование языка INSPECT

Концепция OPSec

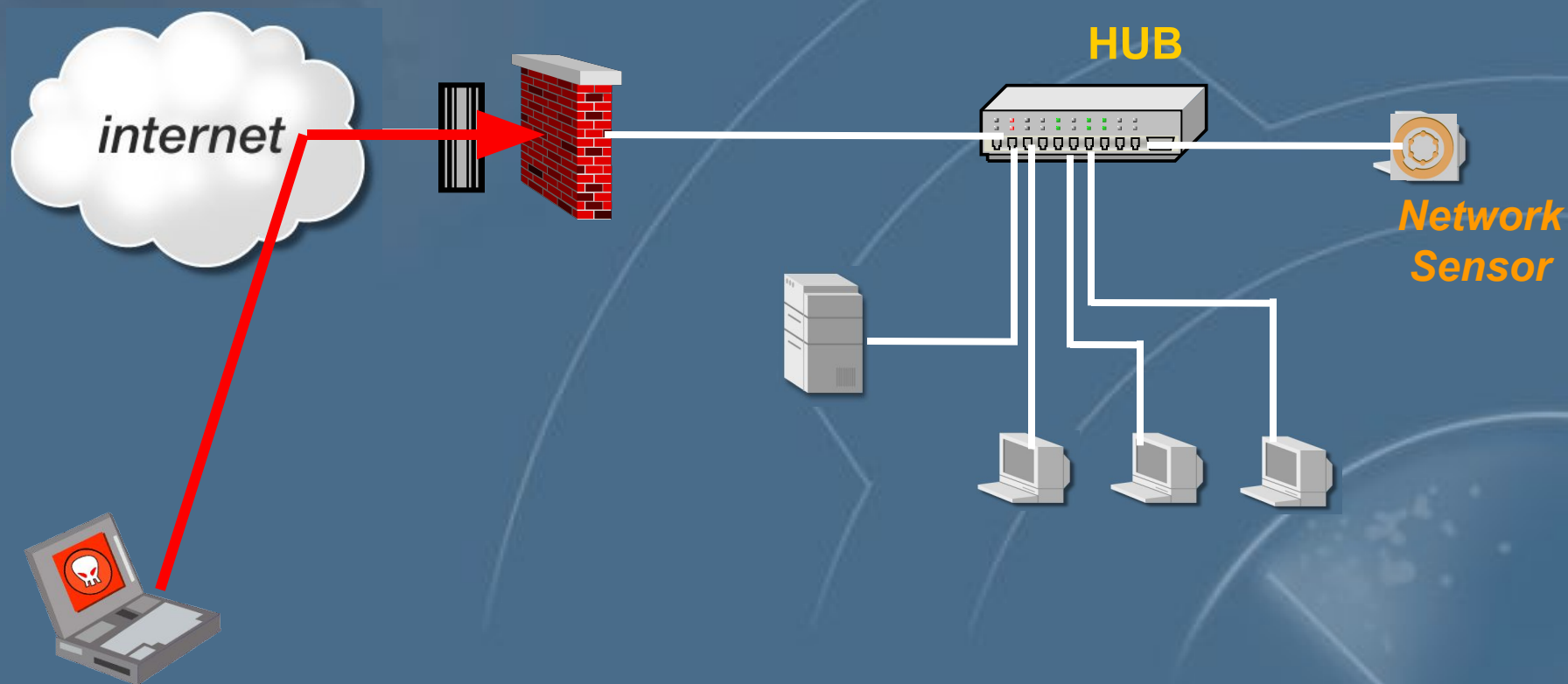
# Реконфигурация МЭ



# Реконфигурация МЭ



# Реконфигурация МЭ



# Практическая работа 12

Работа с программой RealSecure

The background is a solid blue color. In the top-left corner, there is a faint, semi-transparent image of a globe showing continents and latitude/longitude lines. Overlaid on the blue background are several white, curved lines that suggest a network or data flow, starting from the bottom right and curving upwards and to the left.

# 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`

IP	TCP UDP ICMP
----	--------------------

`./snort -vd`

IP	TCP UDP ICMP	Данные
----	--------------------	--------

`./snort -vde`

Ethernet	IP	TCP UDP ICMP	Данные
----------	----	--------------------	--------

# 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