НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ РТК

Межсетевой экран ССПТ-2

Новопашенный А.Г.
andr@rusnet.ru

Санкт-Петербург
29.02.2012

Основные характеристики МЭ ССПТ-2

- ССПТ-2: аппаратно-программный МЭ экспертного уровня
-
- Аппаратное решение на базе стандартной аппаратной платформы
- Встроенная управляющая операционная система – FreeBSD
- Несколько вариантов исполнения устройства (количество и скорость интерфейсов, аппаратная база)
- Скрытый режим работы устройства в сети

Технические характеристики ССПТ-2

Фильтрующие интерфейсы	От 2 до 5 Eth 10/100 От 2 до 5 Eth 10/100/1000 2 Eth 10 GE
Форматы кадров	Ethernet II, IEEE 802.3/LLC, IEEE 802.3 Raw, IEEE 802.3-SNAP IEEE 802.1p/q (VLAN)
Управление (локальное и удаленное)	консоль, COM, Ethernet командная строка, WEB
Уровни фильтрации	Канальный, сетевой (NAT) транспортный (инспекция состояний), прикладной

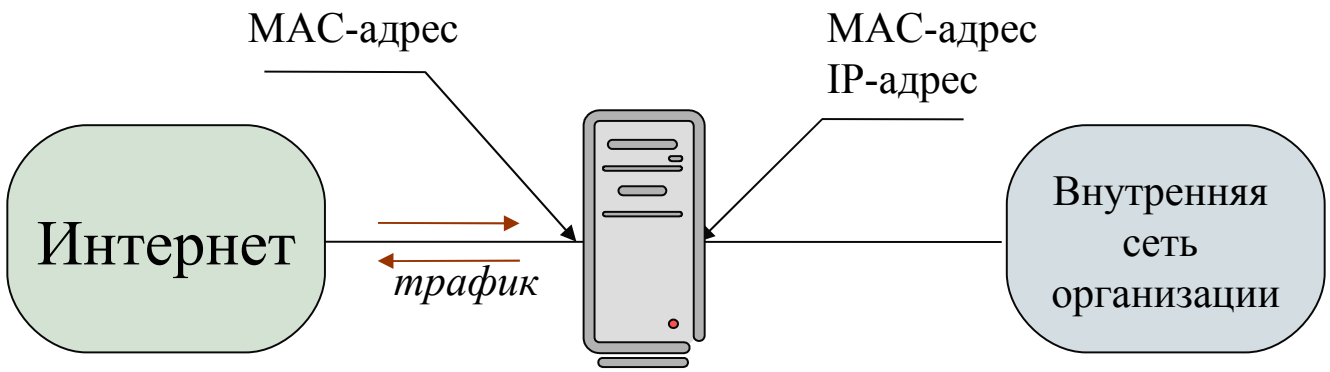
Основные функциональные характеристики

1. Многоуровневая скрытая фильтрация пакетов по совокупности критериев.
2. Контроль транспортных соединений (до 40000 TCP сессий) на основе проверки соответствия каждого пакета контексту выбранной сессии.
3. Трансляция сетевых адресов (режим NAT) для сокрытия структуры внутренней сети с выделением «демилитаризованной зоны».
4. Блокировка компьютерных flood-атак на основе фильтрация аномальной активности сетевых потоков данных.
5. «Зеркалирование» трафика на заданный интерфейс для анализа и проверки с использованием специальных средств контроля.
6. Горячее резервирование для создания систем фильтрации высокой готовности и отказоустойчивости.

Основные функциональные характеристики

1. Выгрузка журналов регистрации по протоколам FTP и SYSlog.
2. Защита канала управления с использованием алгоритма ГОСТ 28147-89 .
3. Аутентификация и авторизация администратора с помощью протокола RADIUS.
4. Контроль доступа к порту управления на основе списка доверенных сетевых адресов.
5. Синхронизация таймера операционной системы по протоколу NTP.

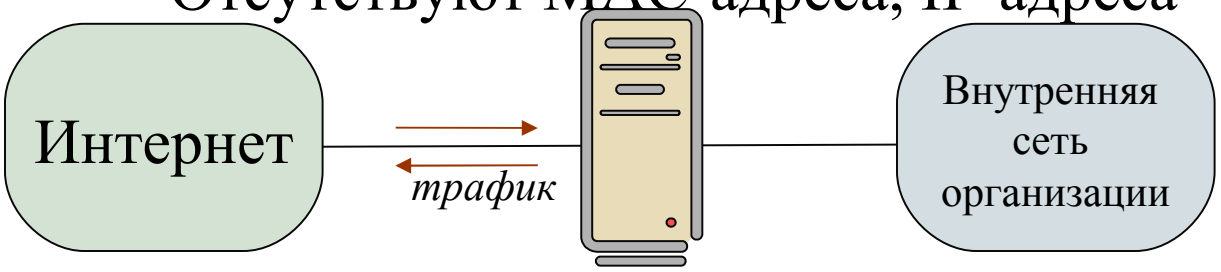
Скрытый режим работы ССПТ-2 в сети. Особенности применения в корпоративных сетях



Архитектура ССПТ-2:

прозрачен для трафика

Отсутствуют MAC-адреса, IP-адреса

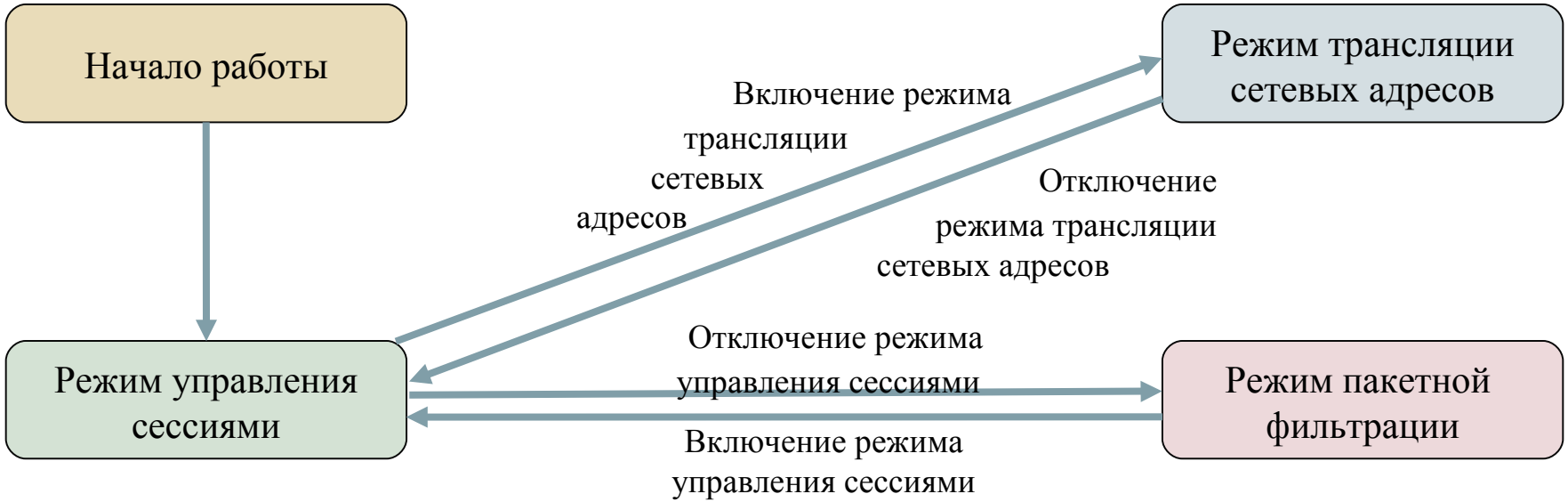


Преимущества:

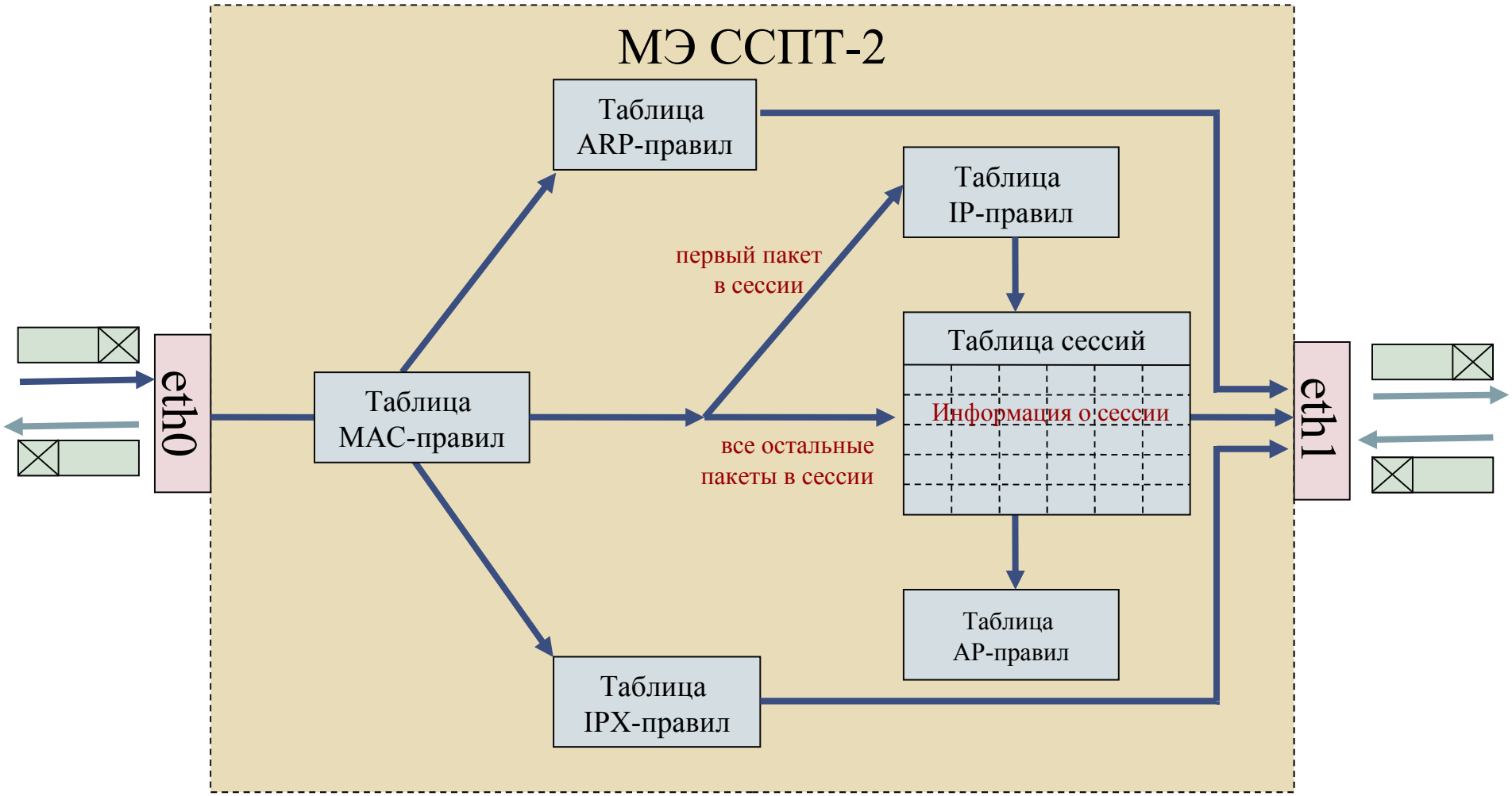
- простота интеграции в существующую сетевую инфраструктуру
- защищённость от деструктивных воздействий на средства безопасности

Режимы фильтрации ССПТ-2

- ССПТ-2 способен осуществлять фильтрацию в следующих режимах:
- Режим пакетной фильтрации
- Режим управления сессиями
- Режим трансляции сетевых адресов



Управление сессиями (инспекция состояний)



Управление сессиями. Детали и преимущества

Преимущества механизма управления сессиями:

- Контроль хода TCP-соединения
- Контроль данных прикладных протоколов
- Блокировка атак, связанных с некорректной установкой флагов TCP
- Автоматическое открытие клиентских портов, необходимых для текущего соединения
- Создание одного правила для одного потока данных

Основные параметры сессии, хранящаяся в таблице сессий:

- интерфейсы, MAC-, IP-адреса и порты взаимодействующих сторон
- номера родительской и дочерней сессий
- текущее состояние сессии
- протокол транспортного и прикладного уровней
- информация о контексте прикладного протокола
- номера TCP-последовательностей для последнего принятого пакета
- имя пользователя, которому принадлежит данная сессия
- время начала, время последней активности и значение таймаута неактивности сессии
- количество пакетов и байт, прошедших от клиента к серверу и обратно
- параметры подсчета интенсивности пакетов в сессии
- номер порта трансляции при использовании режима NAT

Фильтрация прикладных протоколов

Идентификация основных прикладных протоколов независимо от порта сервиса

Протокол HTTP:

- фильтрация по адресам WEB-серверов
- фильтрация по именам (фрагментам) файлов
- фильтрация по методу запроса

Протокол SMTP:

- фильтрация по почтовым адресам отправителя и получателя

Протокол FTP:

- фильтрация по командам **put, get**
- фильтрация по именам (фрагментам) файлов
- фильтрация по имени/паролю пользователя

Сервисы SQL:

- фильтрация по SQL-запросам

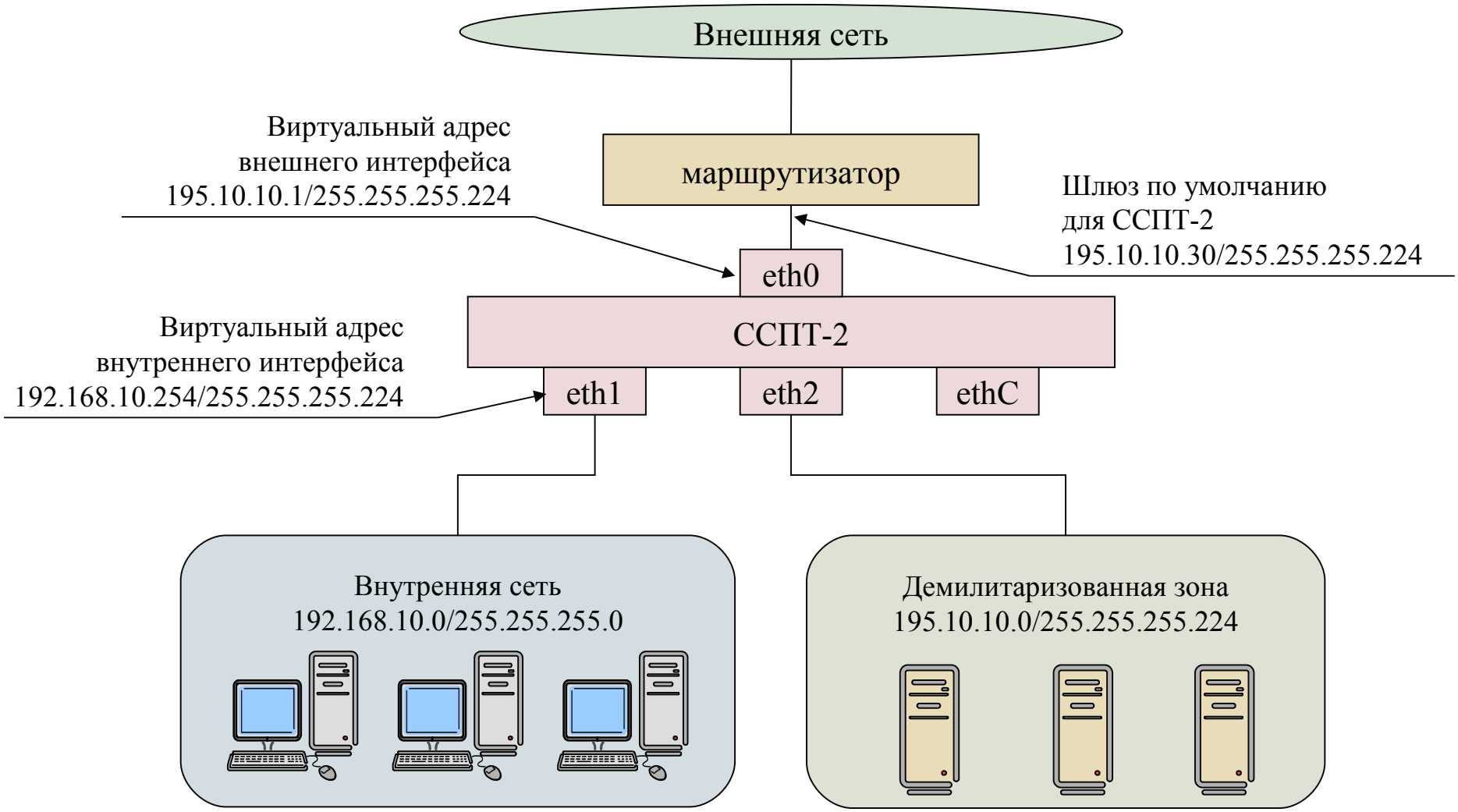
Для перечисленных, а также любых других прикладных протоколов:

- фильтрация любой символьной ASCII-последовательности (до 255 символов)
- фильтрация любой байт-последовательности (до 16 байт)

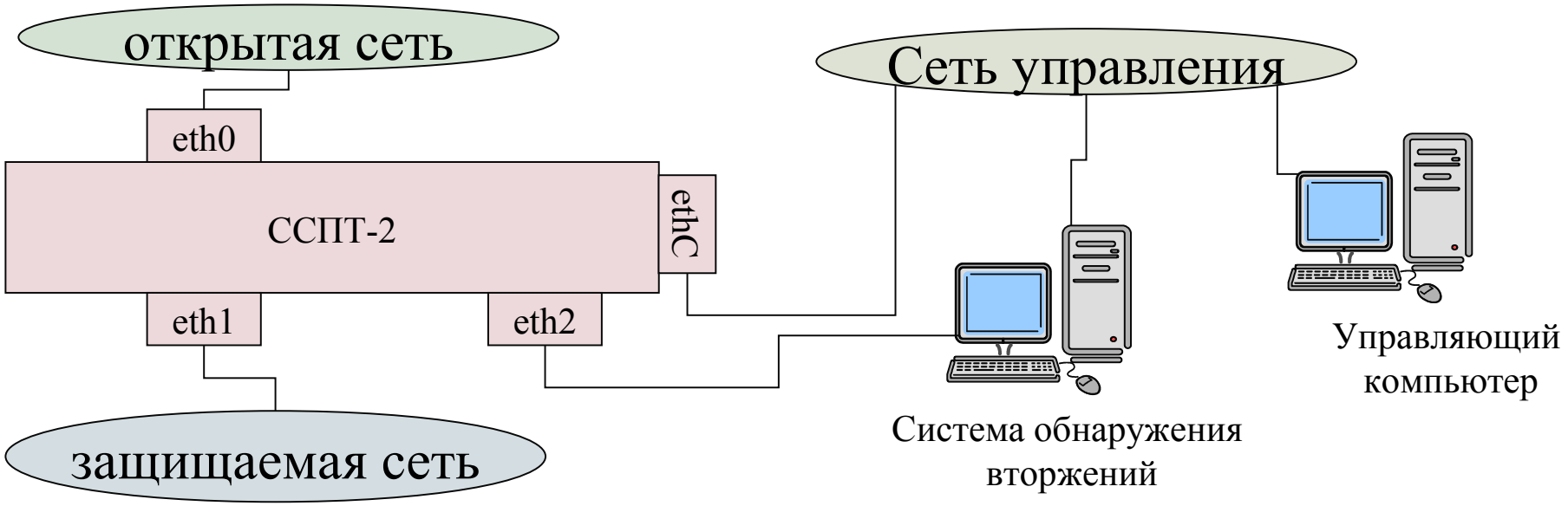
Выполнение следующих действий

- пропуск пакета
- удаление пакета и сессии
- регистрация пакета и сессии

Режим трансляции сетевых адресов (NAT) и аутентификация сетевых пользователей с сохранением скрытности

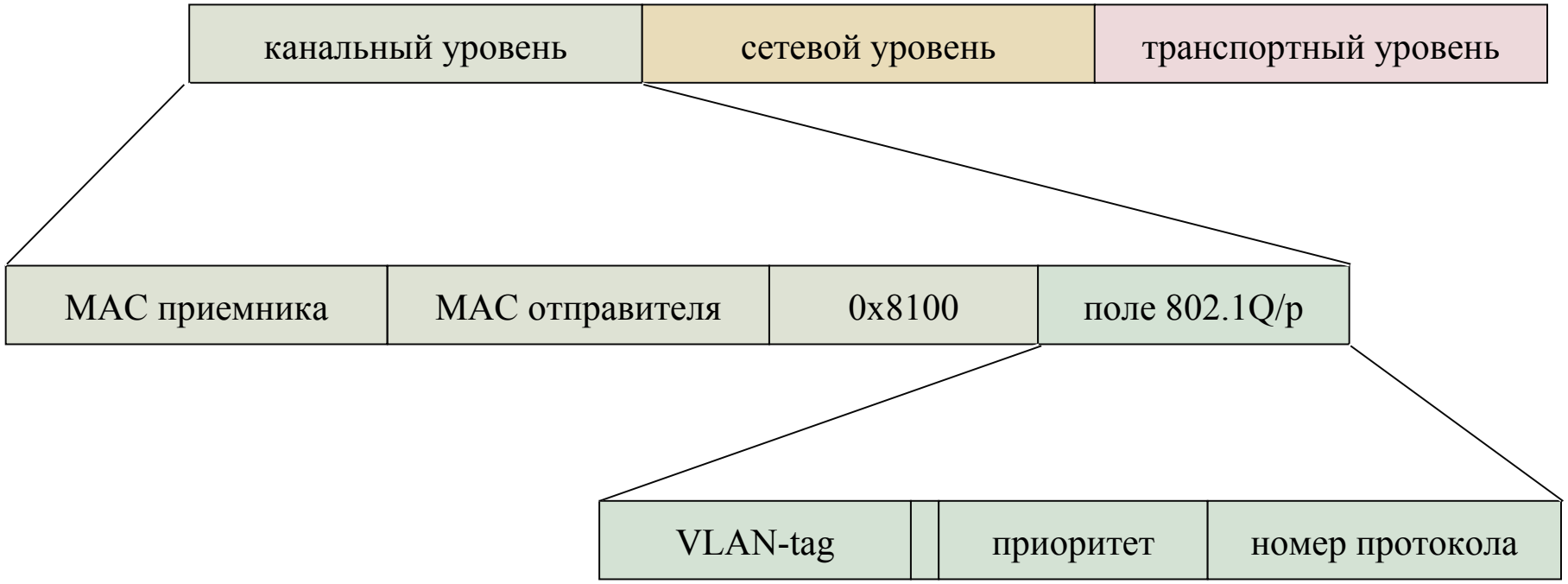


Система обнаружения и противодействия сетевым атакам



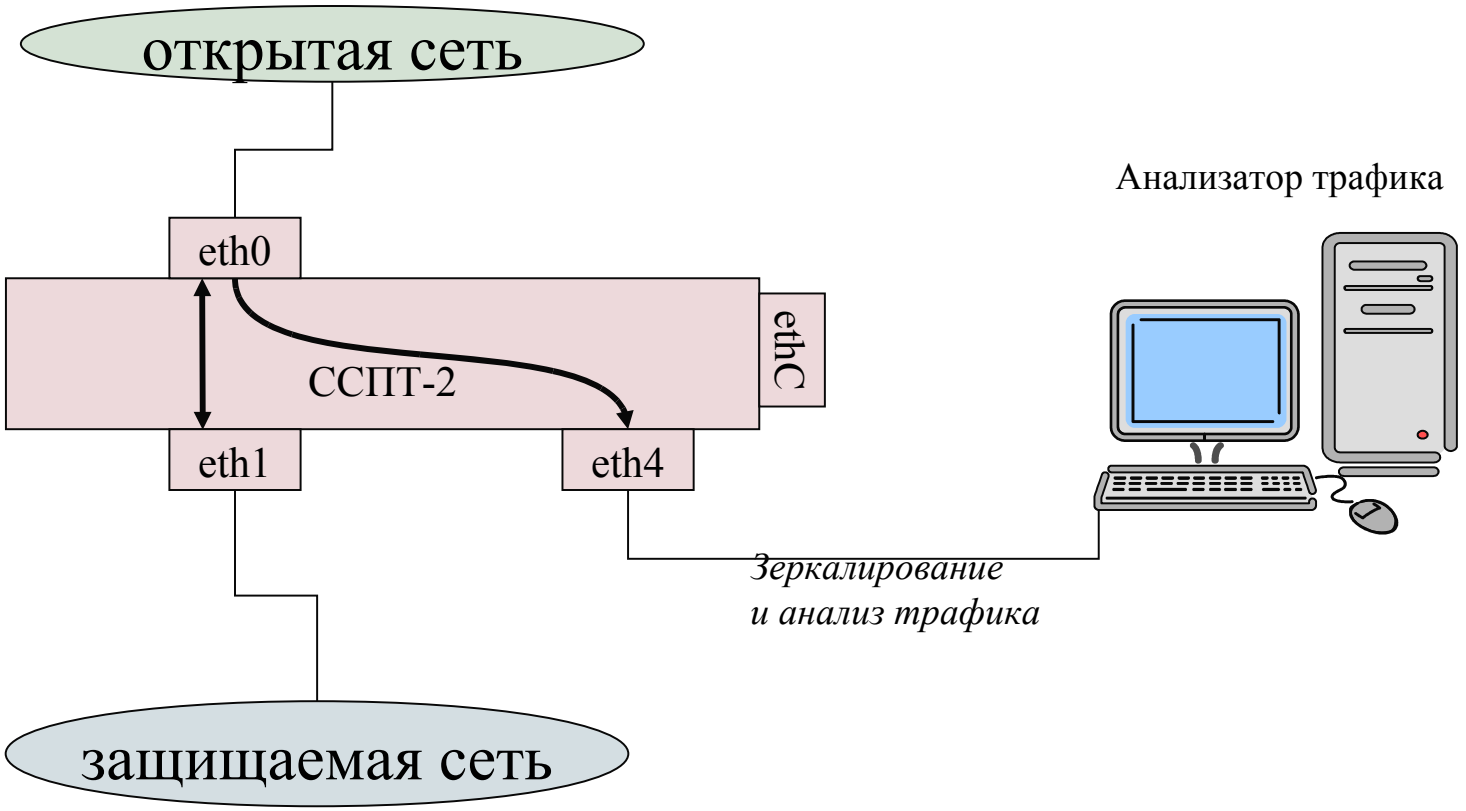
- Встроенный механизм обнаружения и блокировки атак типа «отказ в обслуживании»
- IDS: Intrusion Detection System, система обнаружения вторжений
- IPS: Intrusion Protection System, система противодействия вторжениям, динамическая генерация правил фильтрации на основе отчетов IDS
- IDS = IPS + МЭ

Фильтрация виртуальных локальных сетей 802.1q

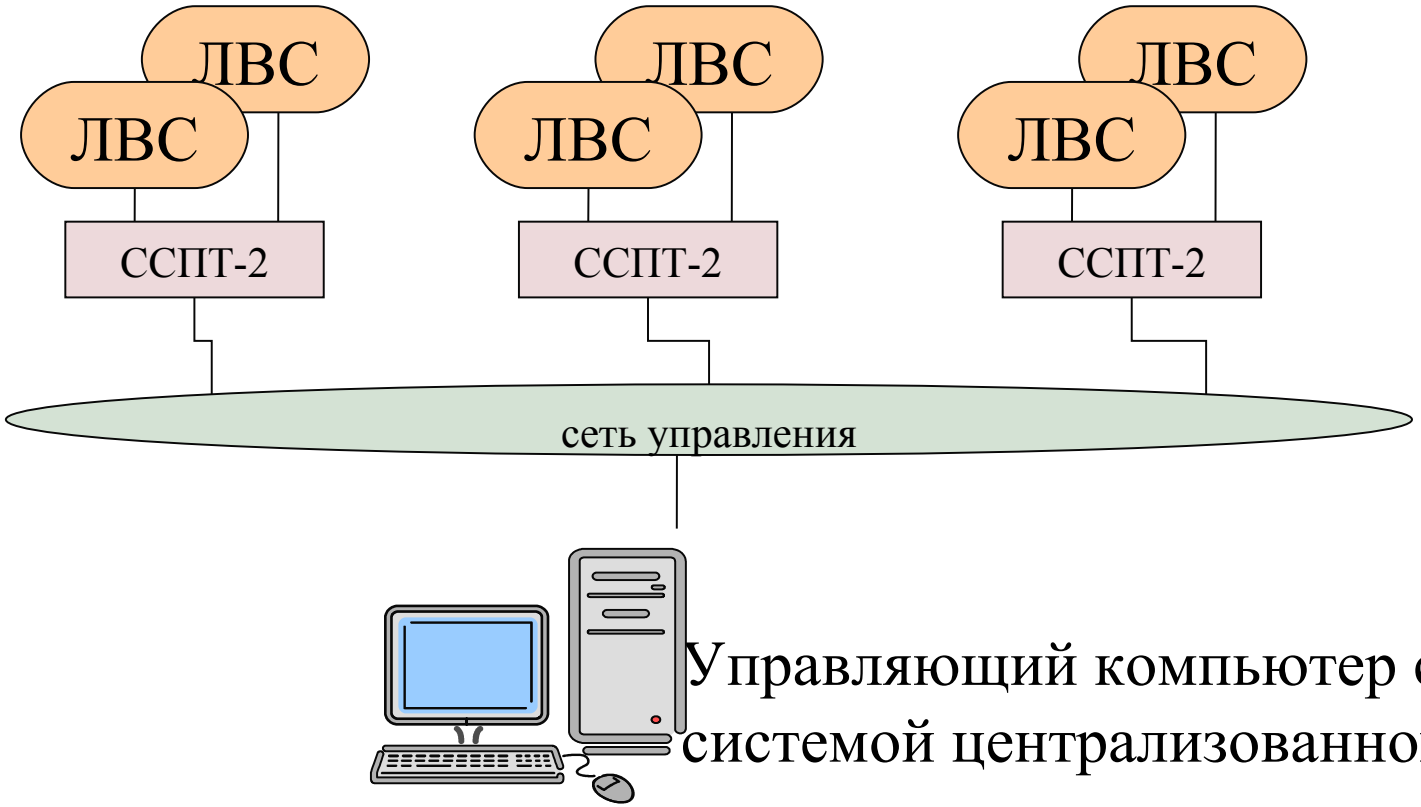


- **Предусматриваются следующие возможности:**
- формирование групп виртуальных локальных сетей (ВЛВС, VLAN)
- Задание правил фильтрации для каждой из групп
- Построение собственных политик безопасности для различных ВЛВС

ССПТ-2: зеркалирование трафика



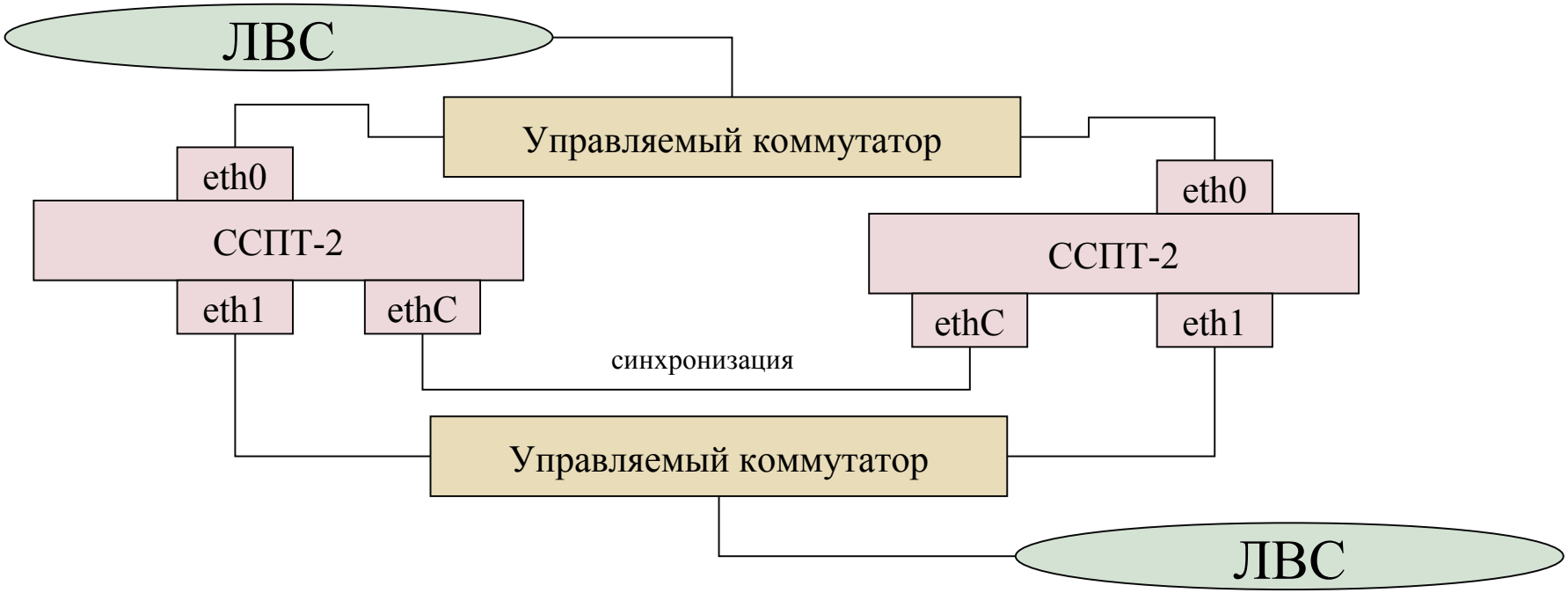
Система централизованного управления



Управляющий компьютер с системой централизованного управления

- Мониторинг состояний и полнофункциональное управление
- Платформы Windows и Unix
- Использование SNMP или специализированного протокола

Система высокой готовности: «Горячий резерв».



Особенности режимов резервирования:

- без сохранения состояний
- «активный/резервный» (собственный протокол и Spanning Tree Protocol)
- «активный/активный» (агрегирование каналов коммутаторов

ГОСУДАРСТВЕННЫЙ РЕЕСТР сертифицированных средств защиты информации

№ 2141

МЭ ССПТ-2 - по 3 классу для МЭ и 3 уровню контроля НДВ (может использоваться для защиты информации в ИСПДн до 1 класса включительно)

Срок действия Сертификата 23.07.2013

Контактная информация

Организация:НПО РТК, системы безопасности

Адрес:194064, Санкт-Петербург, Тихорецкий пр., 21

Телефон:(812)552-0660

E-mail:info@npo-rtc.ru