Безопасность в IP-телефонии

Костюкович Н.Ф.

К типичным угрозам можно отнести:

- **отказ в обслуживании;**
- **подмена номера;**
- **взлом аккаунтов и генерация дорогого международного трафика через ТфОП от имени абонента со взломанным аккаунтом;**
- **несанкционированное изменение конфигурации;**
- **мошенничество со счетом;**
- **перепродажа трафика;**
- **прослушивание трафика;**
- **прослушивание переговоров и др.**

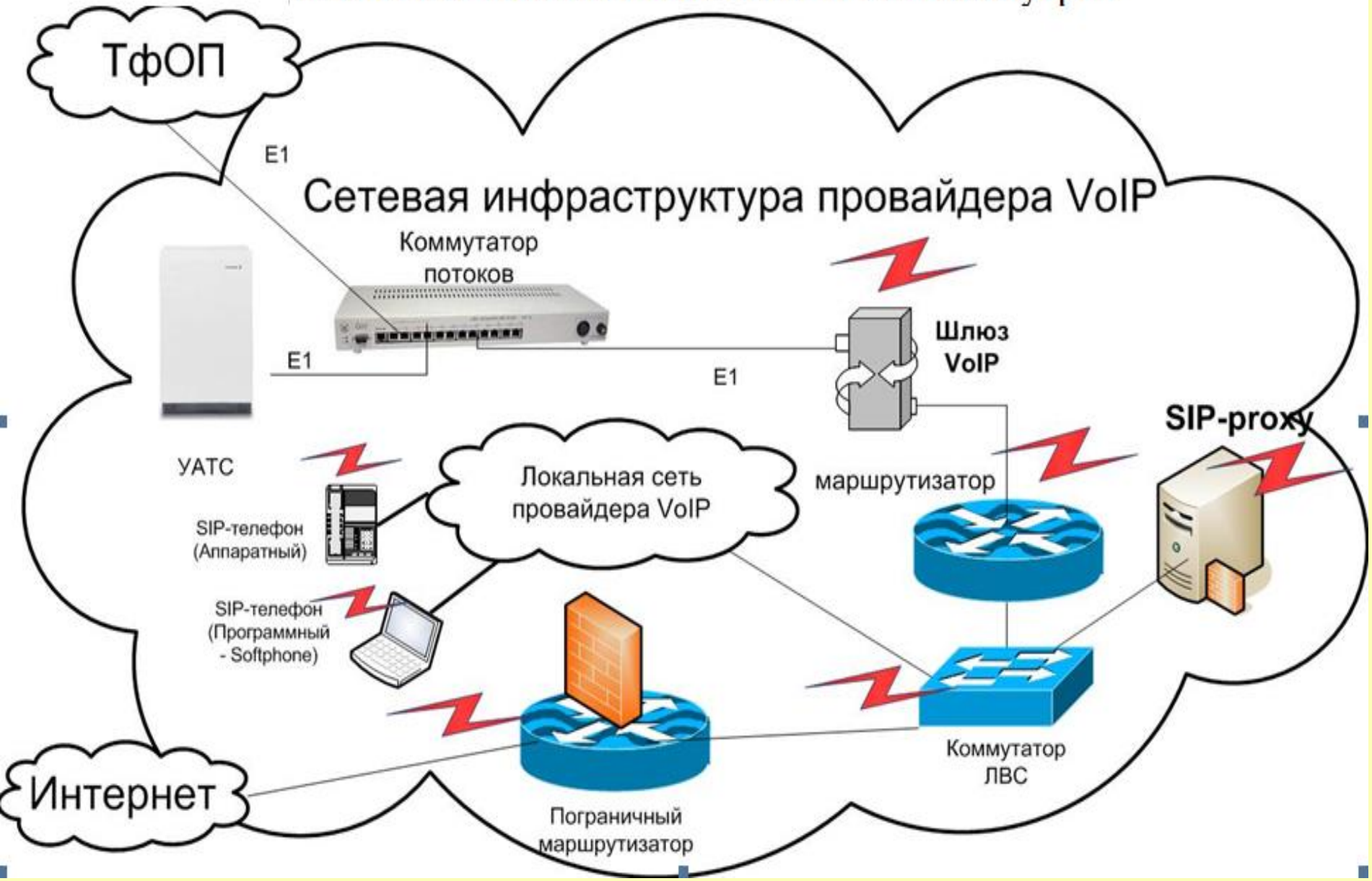
Угрозы могут быть направленны как на объекты сетевой инфраструктуры:

- **коммутаторы,**
- **маршрутизаторы,**
- **шлюзы**

так и на конечные устройства:

- **терминала пользователей,**
- **серверы VoIP**

Схема возможных источников и объектов угроз



1) Программное обеспечение (ПО) пограничного маршрутизатора сети Интернет, который должен в этой схеме выполнять функции файерволла для предотвращения несанкционированных проникновений.

- **Этот маршрутизатор является первым объектом угроз из сети Интернет.**
- **Но вследствии недостаточной защиты на маршрутизаторе, эти угрозы будут направлены на все устройства в данной сети, поддерживающие протокол IP.**

2) Коммутатор ЛВС может как предотвращать часть угроз, например, с помощью ограничения и изоляции трафика в данной сети с помощью виртуальных подсетей – VLAN и правильно организованной защиты на базе списков доступа (ACL – Access List Classes), так и служить источником угроз, в случае недостаточно настроенной защиты.

3) SIP-телефоны могут быть источниками угроз как вследствие умышленных действий сотрудников компании провайдера VoIP, так и вследствие недостаточной защиты этих телефонов (путем взлома паролей доступа к настройкам SIP-телефона).

- **С таких телефонов можно совершать телефонные звонки как через сеть Интернет, так и через сеть оператора ТфОП**

4) Устройтва серверной инфраструктуры провайдера VoIP (SIP-proxy, шлюз VoIP).

- SIP-сервер, позволяет производить регистрацию телефонных абонентов как в своей локальной сети, так и предоставлять услуги телефонии внешним абонентам, находящимся как в сети ТфОП, так и в сети IP.
- SIP-сервер является основным элементов сети VoIP, реализующим управление телефонными вызовами как в IP-сети, так и в ТфОП.

- **Именно на него в первую очередь направляются угрозы из сети Интернет :**
- **сканирование портов 5060, 5061, закрепленных за протоколом SIP,**
- **подбор паролей доступа к Web-управлению SIP-сервером, что позволяет регистрировать сторонних абонентов, разрешать им вызовы в любую сеть – ТфОП или IP,**
- **а также совершать любые другие не санкционированные действия.**

- **По этой причине требуется особое отношение к защите управления SIP-сервером, что обычно не входит в стандартное ПО обычных маршрутизаторов и требует дополнительных расходов на приобретение, настройку и последующее сопровождение специализированного ПО.**
- **Например, ПО SBC (Session Border Controller — пограничный контроллер сессий).**

- **Рассмотрим механизм реализации достаточно распространенной угрозы, заключающейся во взломе учетной записи абонента VoIP и некоторые меры защиты от таких угроз.**

Использование взломанной учетной записи может преследовать цели:

- **нанесение материального ущерба абоненту, аккаунт которого взломали;**
- **получение собственной выгоды взломщиком, например, в случае, если дорогие международные звонки направлены на номера, зарегистрированные как платные.**

Объектами таких угроз являются:

- **Терминалы пользователей с «ненадежными» логинами/паролями (пароли по умолчанию);**
- **SIP-серверы с аккаунтами абонентов, управляемыми, например, через (веб-интерфейсы).**

- **Проникновение в сетевую инфраструктуру провайдера VoIP происходит достаточно известными способами:**

- **Сначала с IP-адресов, закрепленных часто за различными зарубежными подставными прокси серверами, сканируются порты провайдера VoIP, наиболее часто используемые для проникновения (80-HTTP, 445, 1433, 771 и др.) с целью проникнуть через эти порты в различные устройства провайдера VoIP и похитить логины/пароли доступа к услугам SIP-телефонии или к Web-управлению устройств VoIP.**

- **При достижении этой цели с удаленных устройств запускаются запросы на услуги, например, платных зарубежных номеров (дорогие услуги медицинских, юридических консультаций, и т.п.).**
- **Протокол SIP по своим технологическим возможностям поддерживает соединения типа точка-много-точек, что позволяет одновременно организовать несколько вызовов по разным номерам абонентов Б, при этом номер абонента А будет указан один и тот.**

- **т.к. похищенный аккаунт абонента А является разрешенным для сети провайдера VoIP, то устройства, маршрутизация на которых настроена на пропуск вызовов с этого номера в сеть ТфОП, спокойно пропустят эти вызовы.**
- **АТС в сети оператора ТфОП по своим технологическим возможностям не способна различить – кто и как часто набирает номера абонента Б – реальное устройство в сети провайдера VoIP или это номер сгенерирован удаленным устройством по протоколу SIP.**

- **Цели у подобного рода взлома, как правило, финансовые.**
- **Предварительно можно зарегистрировать платный телефонный номер и совершить звонок на него с каждого из обнаруженных SIP-аккаунтов.**
- **Взлом целевого SIP-сервера может нести и более серьезные последствия, так как злоумышленник получает контроль над аутентификацией и тарификацией пользователей, а также маршрутизацией звонков.**

- **Технологически подобный сценарий проникновения может быть реализован с компьютера, находящегося в любой географической точке земли. Важно только наличие доступа с этого компьютера в сеть Интернет.**
- **Система прокси серверов и C&C-серверов (Command and Control - командование и управление), реализующих данные сценарии, получила название – БотНет (сеть роботов).**
- **Наибольшее количество активных C&C серверов бот-сетей располагается в США (631). На втором месте - Британские Виргинские Острова – 237. Нидерланды -154. Россия -125, Германия – 95, Корея - 81 и Швейцария – 77.**

- **Такой робот-сервер может создавать десятки и сотни вызовов в секунду по заранее введенным платным номерам Б, подставляя в качестве номера А, номера и логины/пароли из взломанных аккаунтов.**
- **При таком проникновении исходный IP-адрес компьютера, с которого был запущен подобный сценарий проникновения, скрывается и вместо него прокси-сервер подставляет свои адреса, что затрудняет поиск злоумышленников.**

Методы защиты от рассмотренных угроз

- **Наибольшую опасность рассмотренная угроза представляет для провайдера VoIP, т.к. наносит ему значительный материальный ущерб.**
- **По этой причине провайдер VoIP в первую очередь заинтересован в использовании методов защиты от таких угроз с целью снижения материального ущерба.**

Традиционные методы защиты с помощью ACL-списков на пограничном маршрутизаторе, или коммутаторе ЛВС в случае услуг VoIP не дают достаточного эффекта по следующим причинам:

- **Списки ACL обычно основаны на анализе информации в заголовках уровня L2/L3/L4, не затрагивая анализа прикладных протоколов, например – SIP.**
- **Значения IP-адресов, с которых производится проникновение в сеть провайдера VoIP, не остаются постоянными и заранее неизвестны провайдеру VoIP.**

ACL (Access Control List) – список контроля доступа, который определяет, кто может получать доступ к объекту, и какие операции разрешено или запрещено проводить над объектом.

ACL являются основой систем фильтрации (ограничения прав доступа).

ACL также можно использовать для целей, отличных от фильтрации IP-трафика, например, для назначения классов обслуживания, а также для фильтрации протоколов, отличных от IP.

ACL представляет собой таблицу, содержащую записи, определяющие права пользователя.

ACL представляет собой последовательность условий проверки параметров пакетов данных на разных уровнях модели OSI.

В частности, коммутатор проверяет информацию в кадрах на совпадение с критериями фильтрации, определенными в ACL, и выполняет над пакетами одно из действий:

- **Permit ("Разрешить")**
- **Deny ("Запретить").**

Критерии фильтрации могут быть определены на основе следующей информации, содержащейся в пакете:

- **порт коммутатора;**
- **MAC/ IP-адрес;**
- **тип Ethernet / тип протокола в заголовке IP;**
- **VID/VLAN;**
- **CoS;**
- **порт TCP/ UDP (тип приложения);**
- **первые 80 байт пакета, включая поле данных…**

Можно использовать разрешение или запрет доступа различным типам файлов, таким как FTP или HTTP.

Список доступа ACL составляется из условий, которые определяют, следует ли пакеты принимать или отклонять во входных и выходных интерфейсах маршрутизатора.

Если ACL отсутствует на маршрутизаторе, то все проходящие через маршрутизатор пакеты будут иметь доступ к сети.

В Cisco IOS (**I**nternetwork **O**perating **S**ystem — Межсетевая Операционная Система) **есть следующие типы ACL:**

- **Стандартные (только IP-адрес источника)**
- **Расширенные (IP-адреса, № протокола, порт TCP/UDP)**
- **Именованные (любое символическое имя).**

Каждый список на роутере имеет уникальный номер/имя, который идентифицирует тип созданного списка доступа.

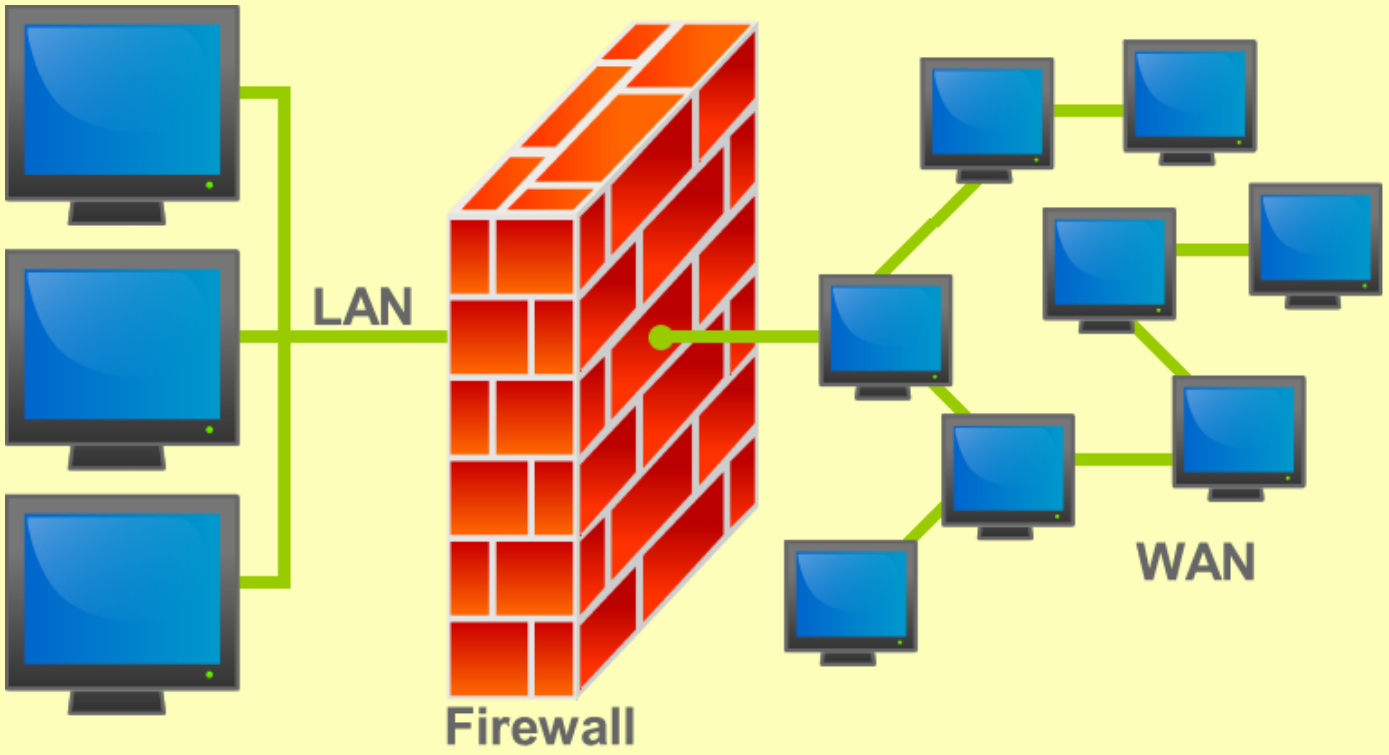
- **Но если знаешь «вредоносный» IP-адрес, то внести его в ACL не сложно.**
- **Главное как его определить.**
- **Для этого существуют технологии DPI.**
- **Deep Packet Inspection (DPI) — технология накопления статистических данных, проверки и фильтрации сетевых пакетов по их содержимому**

- **Поэтому лучшую защиту обеспечивают методы, основанные на более глубоком анализе входящих пакетов, например, с использованием технологий DPI.**
- **Программное обеспечение, поддерживающее DPI, позволяет анализировать содержимое SIP-запросов, определяя адреса абонентов Б и частоту вызовов от абонентов А.**
- **Благодаря этой информации можно построить алгоритмы анализа аномалий во входящем трафике.**

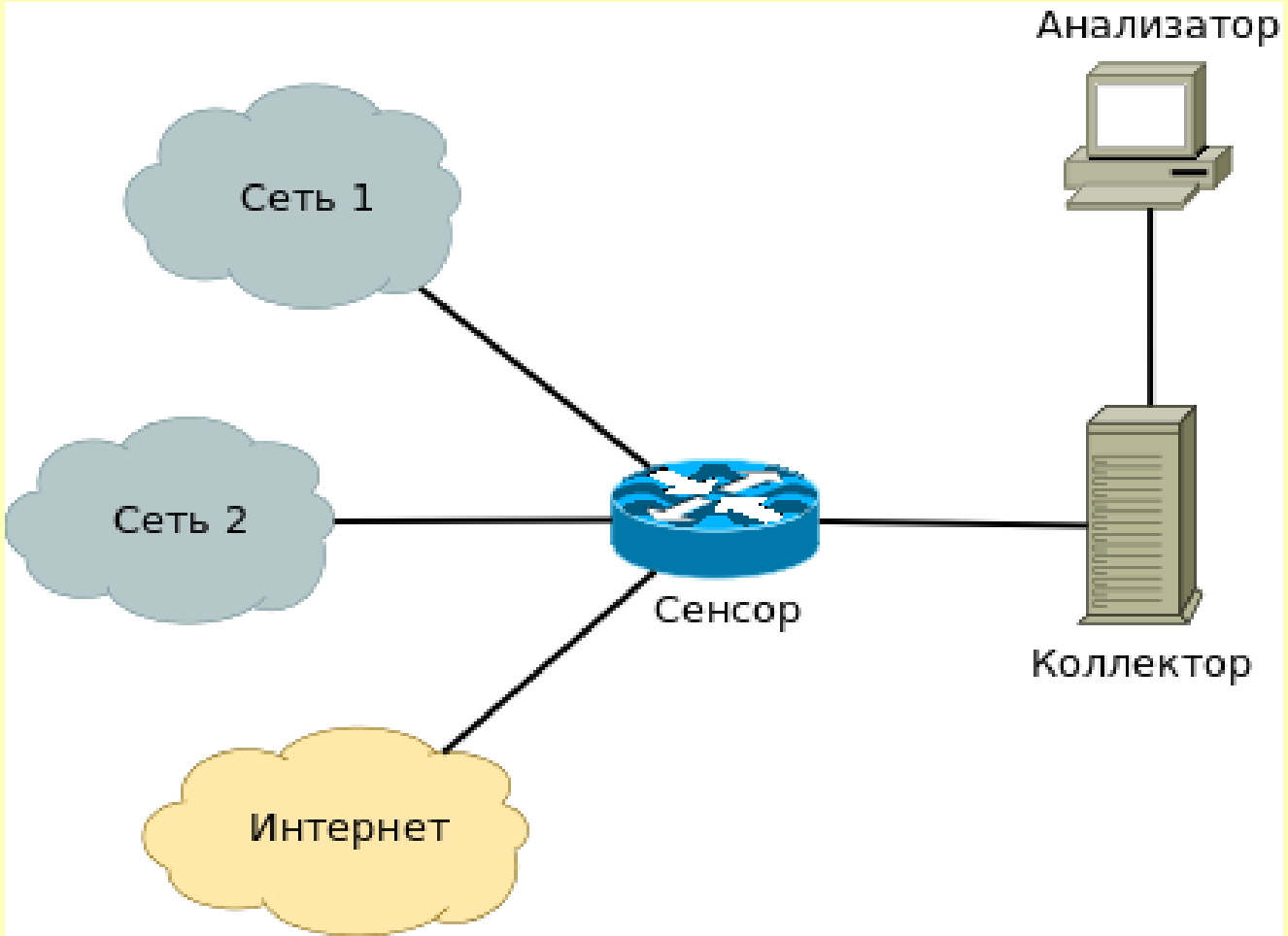
- **Например, если вызовы от одного и того же абонента А поступают чаще чем 2…3 вызова в секунду, можно сделать вывод, что абонентом А является не реальный терминал, а программа-робот из какой-либо Бот-Нет.**
- **Остается только определить IP-адрес, с которого поступили данные вызовы и заблокировать вызовы с этих IP-адресов, например, внеся их в списки ACL.**

- **Подобное ПО имеется на множестве специализированных для VoIP сетей файрволлах, например, на базе SBC-контроллеров.**
- **Однако, по причине высокой стоимости такого ПО, требующего достаточной квалификации администратора, многие провайдеры VoIP пренебрегают такой защитой, за что впоследствии придется расплачиваться материальным ущербом, нанесенным взломом аккаунтов.**

Расположение сетевого экрана (Firewall) в сети.



Для организации защиты требуется реализовать систему анализа сетевого трафика следующего вида



Сенсор работает в одном из нескольких режимов:

- **Режим “шунтирования” – когда только отсылается копия пакета на коллектор**
- **“строгий” режим - в этом случае все новые соединения анализируются коллектором**
- **“умный” режим – в этом режиме только определённая часть пакетов отсылаются на анализ коллектору**

Коллектор позволяет анализировать содержимое пакетов, определять адреса устройств создающих аномальный трафик и включать эти адреса в ACL.

FIN

СПАСИБО

за

ВНИМАНИЕ