

# Интеграция системы Перехват в существующую сеть

Для работы системы Перехват требуется получать данные об исходящем HTTP и SMTP трафике. Модули системы, которые получают данные, называются *сенсоры*. Есть два сенсора – почтовый сенсор и веб сенсор. Оба сенсора могут находиться на одной машине (рекомендуется для упрощения настройки), но при необходимости могут быть и разнесены по разным машинам).

## Почтовый сенсор

Почтовый сенсор выполняет перехват SMTP и POP3 почты. (При этом, перехват POP3 почты, скорее исторически сложившаяся возможность. POP3 почта, как правило, входящая, а не исходящая. Но можно контролировать и ее).

Сенсор может работать как будучи интегрированным в почтовый сервер Exim (через который должна проходить исходящая почта) так и в режиме «сниффера» (мы рекомендуем этот метод).

При работе сенсора в составе МТА Exim, требуется, чтобы вся исходящая почта проходила через этот почтовый сервер. Для этого, либо все рабочие машины должны быть настроены на отсылку почты через этот сервер, либо, если исходящая почта идет через уже существующий корпоративный сервер, он должен быть настроен на использование Exim сервера в качестве smarthost'a.

При рекомендуемом режиме работы в режиме сниффера, он должен быть расположен так, чтобы машина с сенсором могла «слышать» исходящий трафик. Возможны следующие варианты:

- Сенсор устанавливается на почтовом сервере (это возможно если он работает под UNIX-подобной ОС).
- Сенсор устанавливается на одном из роутеров. (те же требования).
- Сенсор устанавливается на отдельную машину, которая конфигурируется в режиме бриджа и «прозрачно» встраивается между внешним роутером организации и роутером провайдера. Переконфигурация роутеров не требуется.
- Сенсор устанавливается на отдельную машину, подключенную к monitoring порту свитча, если в нем поддерживается эта функция.

## Веб сенсор

Встроен в HTTP проху идущий в составе системы Перехват. Для подключения требуется, чтобы исходящий HTTP трафик проходил через этот прокси сервер. Для этого либо рабочие станции настраиваются на использование прокси-сервера перехвата, либо, если используется существующий корпоративный прокси сервер, то он настраивается на использование прокси-сервера перехвата в качестве вышестоящего (parent) прокси. Возможно использование в режиме transparent прокси. В этом случае не требуется перенастройка рабочих станций, а файрвол на машине с прокси-сервером настраивается для выполнения редиректа трафика TCP/80 на прокси сервер.