**NetFlow**

Netflow предоставляет возможность анализа сетевого трафика на уровне сеансов, делая запись о каждой транзакции TCP/IP. Информация не столь подробна, как предоставляемая tcpdump'ом, но представляет довольно подробную статистику.

Netflow имеет три основных компонента:

* сенсор;
* коллектор;
* система обработки и представления данных.

**Сенсор** — демон, который слушает сеть и фиксирует данные сеанса. Также как Snort или любая другая система обнаружения вторжений, сенсор должен иметь возможность подключиться к хабу, "зеркалированному" порту коммутатора или любому другому устройству, для просмотра сетевого трафика. Если вы используете систему пакетной фильтрации на базе BSD или Linux, то это превосходное место для сенсора Netflow, так как весь трафик будет проходить через эту точку. Сенсор будет собирать информацию о сеансах и сбрасывать ее в коллектор.

**Коллектор** — второй демон, который слушает на UDP порту, указанному вами и осуществляет сбор информации от сенсора. Полученные данные он сбрасывает в файл для дальнейшей обработки. Различные коллекторы сохраняют данные в различных форматах.

Наконец, **система обработки** читает эти файлы и генерирует отчеты в форме, более удобной для человека. Эта система должна быть совместима с форматом данных, предоставляемых коллектором.