Сетевые экраны и фильтрация трафика

Фильтрация (filtering) -- запрет или разрешение прохождения входящих или исходящих пакетов по выбранным критериям.

В качестве объекта фильтрации выступает пакет. Может выполняться по IP-адресам, по портам, по содержимому и так далее.

Сетевой (межсетевой) экран (firewall, по-немецки brandmauer) -- запрет или разрешение доступа к определенным категориям сетевых ресурсов (как правило централизованным или внешним).

Сетевой экран в основном выполняет фильтрацию, но это более общее понятие. Классификация сетевых экранов:

1. Packet Firewalls -- просто пропускают или отбрасывают пакеты. Работают на третьем уровне (очень редко на втором).

2. Stateful Firewalls -- способны следить (tracking) за состоянием TCP соединений, то есть выполнять инспекцию (inspection) трафика. Работают на третьем и четвертом уровнях.

3. Application Gateway Firewalls -- способны следить за сообщениями протоколов прикладного уровня (например, HTTP), то есть выполнять глубокую инспекцию – DPI (Deep Packet Inspection). Работают на третьем -- седьмом уровнях