Firewall

План

- Что такое Firewall
- Основная задача Firewall
- Как работает Firewall
- Виды Firewall
- Типичные возможности
- Проблемы, не решаемые с помощью Firewall

Что такое Firewall

Межсетевой экран или сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

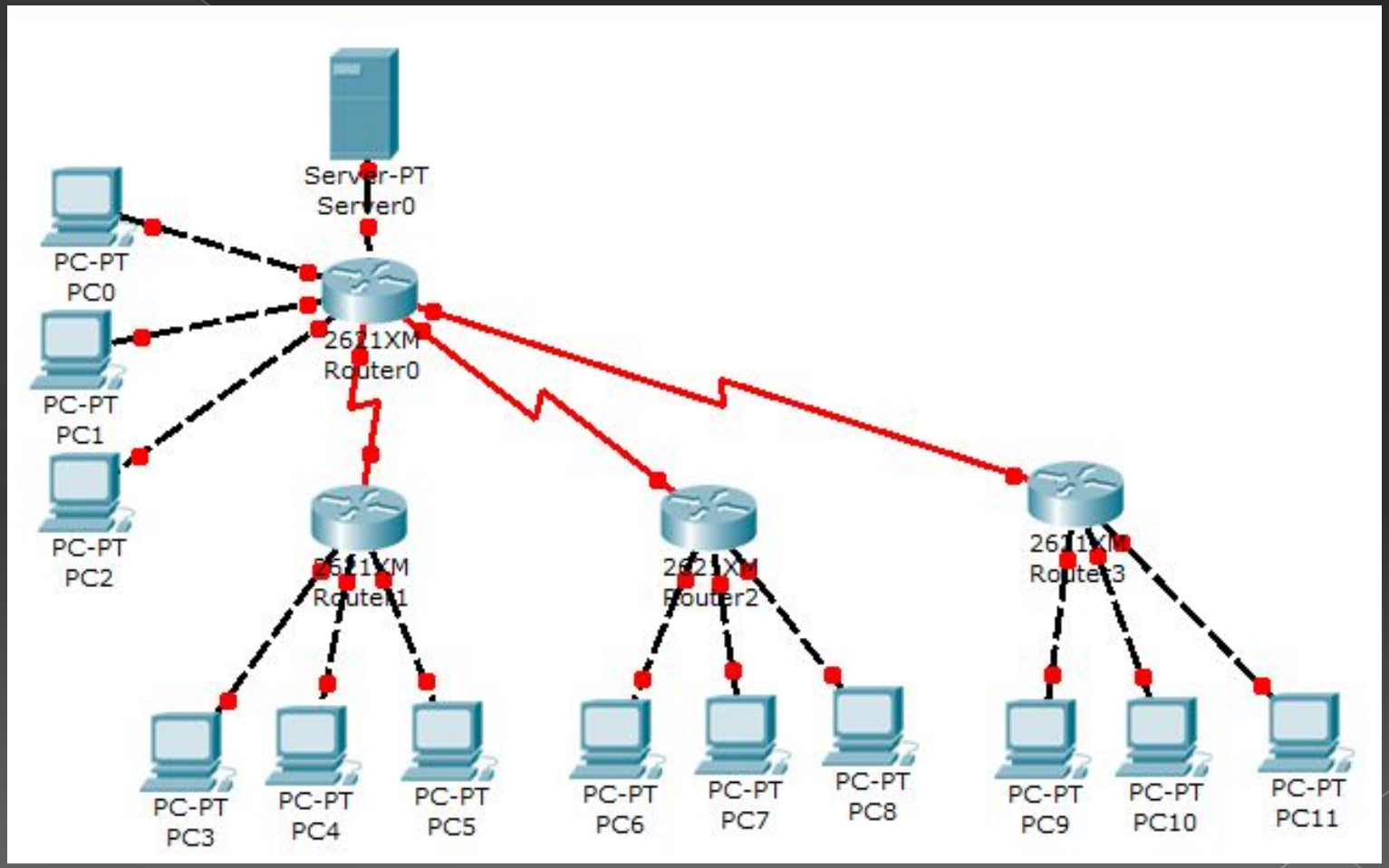
Основная задача Firewall

- Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

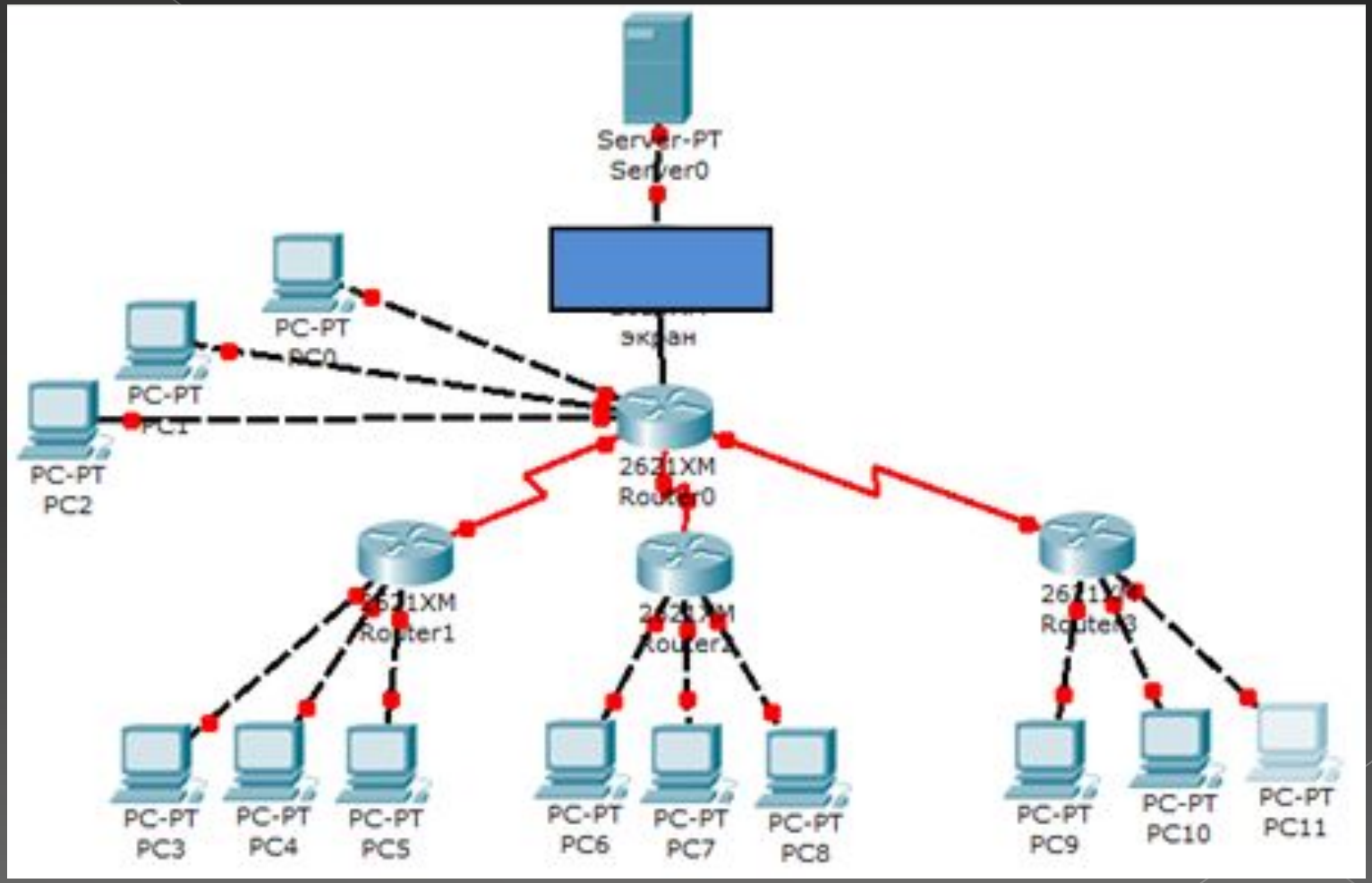
Как работает Firewall

Firewall контролирует порты и проходящие через них пакеты. Важной функцией Firewall является наблюдение за всеми установленными и запущенными приложениями. У брандмауэра есть набор правил, как встроенных по умолчанию, так и задаваемых самим пользователем.

Сеть без сетевого экрана



Сеть с сетевым экраном



Виды Firewall

Сетевые экраны подразделяются на различные типы в зависимости от следующих характеристик:

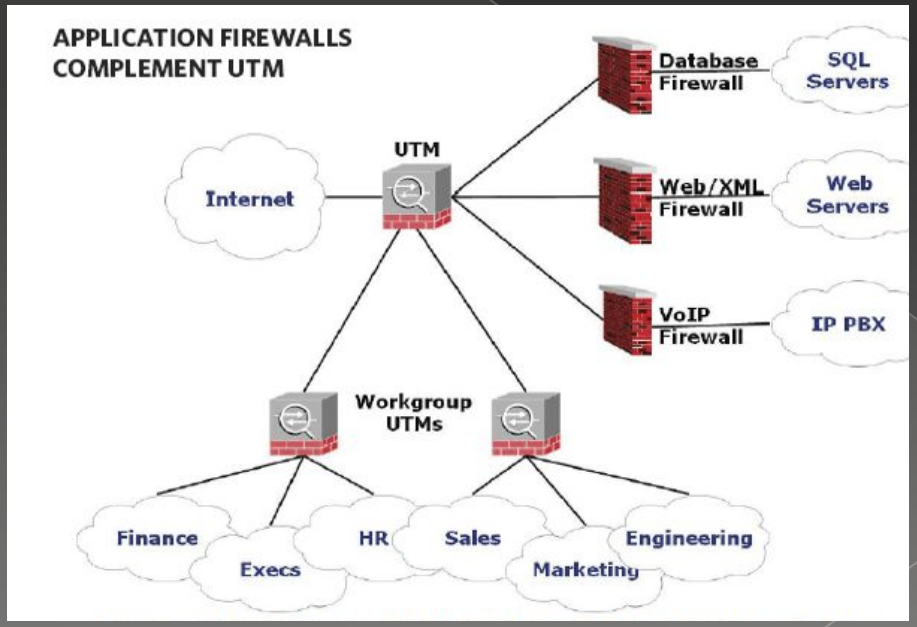
- обеспечивает ли экран соединение между одним узлом и сетью или между двумя или более различными сетями;
- на уровне каких сетевых протоколов происходит контроль потока данных;
- отслеживаются ли состояния активных соединений или нет.

Виды Firewall в зависимости от охвата контролируемых потоков

- традиционный сетевой (или межсетевой) экран
- персональный сетевой экран
- вырожденный случай

Виды Firewall в зависимости от уровня, на котором происходит контроль доступа

- сетевой уровень
- сеансовый уровень (также известные как stateful)
- уровень приложений



Виды Firewall в зависимости от отслеживания активных соединений

- stateless (простая фильтрация)
- stateful, stateful packet inspection (SPI) (фильтрация с учётом контекста)

Типичные возможности

- фильтрация доступа к заведомо незащищенным службам;
- препятствование получению закрытой информации из защищенной подсети, а также внедрению в защищенную подсеть ложных данных с помощью уязвимых служб;
- контроль доступа к узлам сети;
- может регистрировать все попытки доступа как извне, так и из внутренней сети, что позволяет вести учёт использования доступа в Интернет отдельными узлами сети;
- регламентирование порядка доступа к сети;
- уведомление о подозрительной деятельности, попытках зондирования или атаки на узлы сети или сам экран;

Проблемы, не решаемые с помощью Firewall

- не защищает узлы сети от проникновения через «люки» (англ. back doors) или уязвимости ПО;
- не обеспечивает защиту от многих внутренних угроз, в первую очередь — утечки данных;
- не защищает от загрузки пользователями вредоносных программ, в том числе вирусов;

Спасибо за внимание