Межсетевые экраны

Контроль доступа

- Два абонента взаимодействуют через сеть: как обеспечить контроль доступа на этом уровне?

Контроль доступа

- Фильтрация на уровне сети
  - Сетевой периметр
- Фильтрация на уровне сервиса

Межсетевой экран

- Концепция межсетевых экранов появилась в конце 80 годов 20 века
- Типы межсетевых экранов в историческом порядке:
  - пакетные фильтры
  - прокси прикладного уровня
  - МСЭ с контролем состояния

Пакетные фильтры

- Решение принимается для каждого пакета индивидуально
- Как правило, используются только поля заголовков сетевого и транспортного уровня
- Пример: **ipfwadm** в Linux 1.xx

Пакетные фильтры

- Если пакет не прошел фильтрацию, что делать?

Пакетные фильтры

- Пример правила:

ipfwadm -I -a accept -S 192.168.100.0/24 -D 0/0

Прокси прикладного уровня

- Реализуют протокол (или его подмножество) прикладного уровня
  - SMTP
  - DNS
  - FTP
  - HTTP

Прокси прикладного уровня

- Решение можно принимать вплоть до конкретного действия на уровне протокола прикладного уровня
- Необходим соответствующий прокси и перенастройка сервера и/или клиента
- Примеры: **mod_security**, **squid**, **fwtk**

Прокси прикладного уровня

- Пример правила:

http-gw: permit-hosts: 192.168.*.*

Контроль состояния

- Прозрачное “понимание” сессии на транспортном или прикладном уровне
- Решение можно принимать на любом уровне
- Необходима прозрачная реализация прикладных протоколов

Контроль состояния

- Как реагировать на сетевом уровне на нарушение на уровне приложения?

Контроль состояния

- Пример правила:

iptables -A INPUT -i eth0 -p icmp --icmp-type echo-request -j ACCEPT

Другие проблемы

- Многопользовательские системы
- Динамические IP адреса
- Производительность и DoS