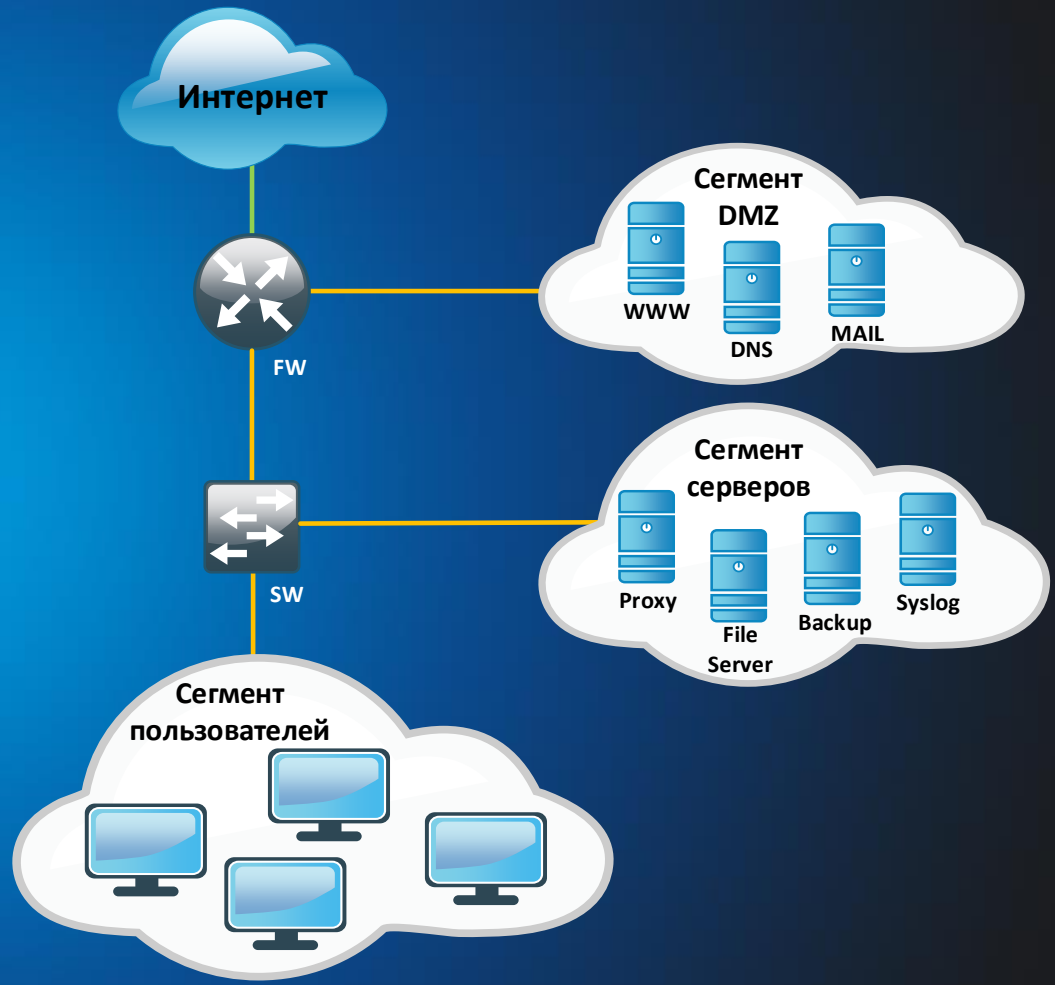

NetSkills
online IT school

“Linux для начинающих”
Базовый курс
7. Межсетевой экран

NetSkills
online IT school

7. Linux для начинающих. Базовый курс. Межсетевой экран

1. Доступ в Интернет организуется через NAT
2. Пользователи подключены через proxy сервер
3. Корпоративная почта организована на своем почтовом сервере MAIL
4. Корпоративный сайт и внутренние веб ресурсы расположены на веб сервере WWW
5. В сети функционирует программный шлюз FW, представляющий собой сервер с ОС Linux, на котором расположен DHCP сервер
6. В сети так же есть первичный и вторичный DNS сервера
7. В качестве сетевого хранилища используется файловый сервер File Server
8. На сервер Backup собираются резервные копии со всех остальных серверов
9. Различные события с серверов собираются на сервер логирования Syslog



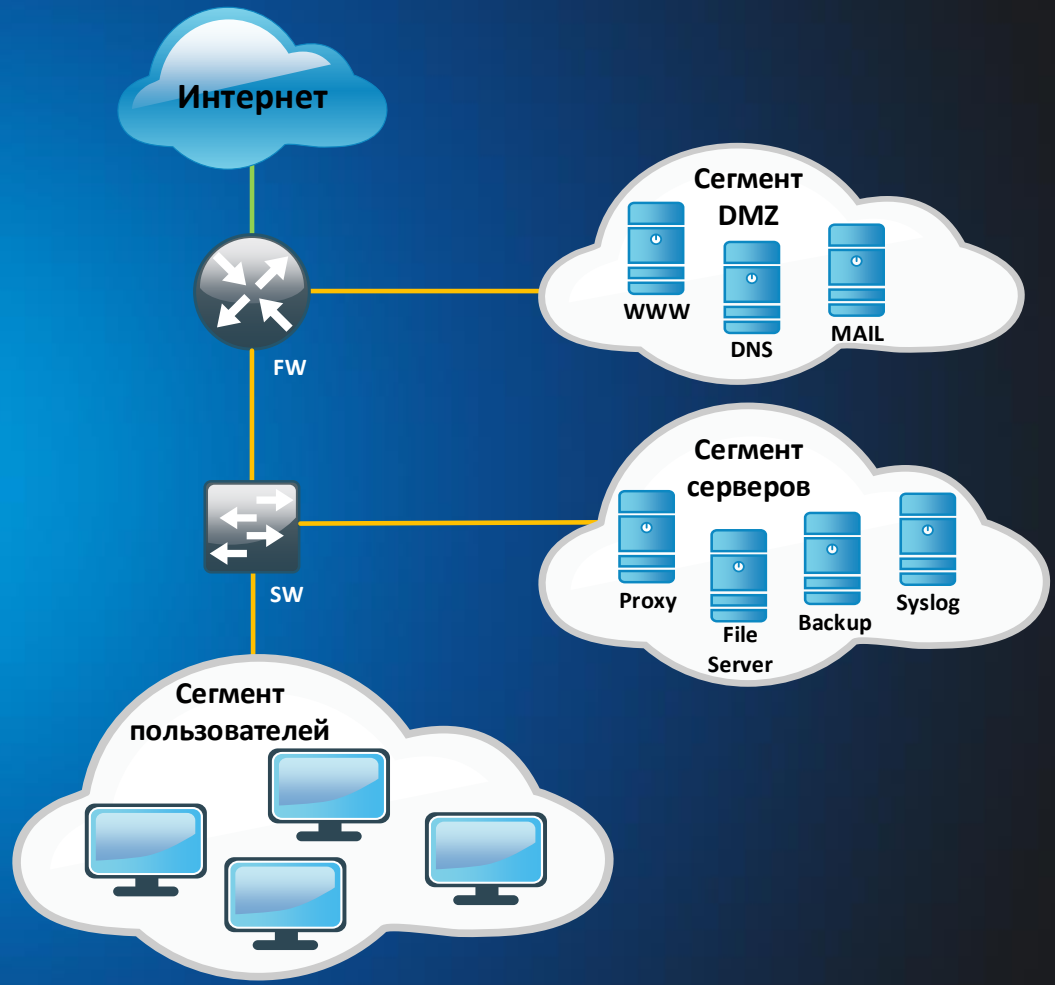
NetSkills
online IT school

7. Linux для начинающих. Базовый курс. Межсетевой экран

DMZ – сегмент серверов, которые будут доступны как из внутренней сети, так и из внешней.

Сервера – сегмент серверов, которые работают только во внутренней сети

Пользователи – это пользователи



NetSkills
online IT school

7. Linux для начинающих. Базовый курс. Межсетевой экран

Адреса сетей

Сегмент DMZ (фиолетовая сеть) – 192.168.250.0/24

Сегмент серверов (оранжевая сеть) – 192.168.251.0/24

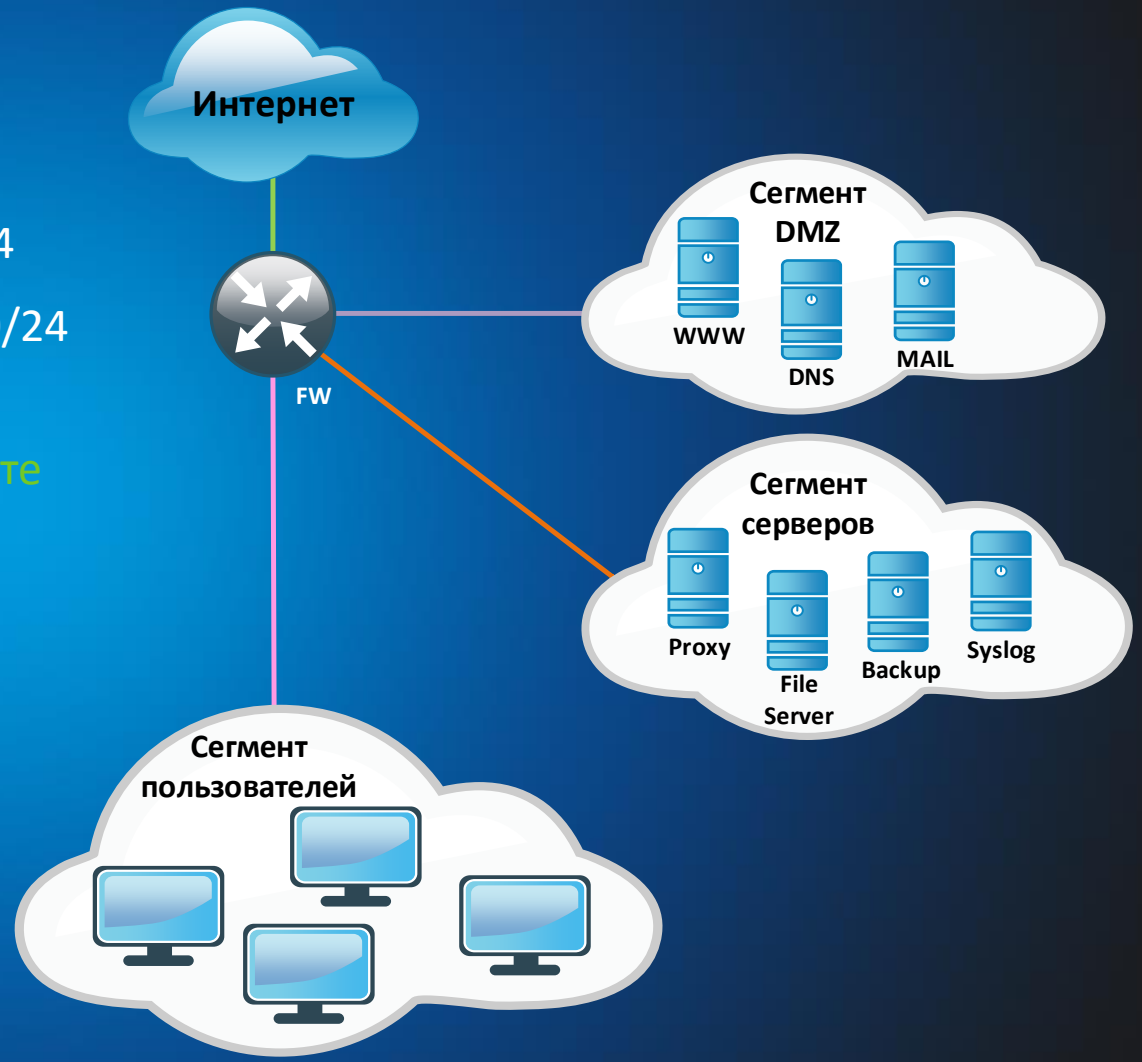
Сегмент пользователей (розовая сеть) – 192.168.252.0/24

Адреса сетевых интерфейсов шлюза в каждом сегменте

Сегмент DMZ (фиолетовая сеть) – 192.168.250.1

Сегмент серверов (оранжевая сеть) – 192.168.251.1

Сегмент пользователей (розовая сеть) – 192.168.252.1



NetSkills
online IT school

7. Linux для начинающих. Базовый курс. Межсетевой экран

NAT – это механизм, позволяющий преобразовывать ip адреса транзитных пакетов.

Подробнее про NAT можно прочитать здесь, или посмотреть видеоурок, посвященный этой теме.

Netfilter – межсетевой экран в Linux.
Для управления им используется утилита iptables.

NetSkills
online IT school

7. Linux для начинающих. Базовый курс. Межсетевой экран

Правило — состоит из критерия, действия и счетчика.

Критерий — логическое выражение, в котором указываются свойства пакета или соединения.

Действие — что нужно сделать с пакетом или соединением, если они подпадают под критерий правила.

Счетчик — ведет учет количества пакетов, которые попали под критерий данного правила.

NetSkills
online IT school

7. Linux для начинающих. Базовый курс. Межсетевой экран

Цепочка — упорядоченная последовательность правил. Цепочки можно разделить на пользовательские и базовые.

Базовая цепочка — цепочка, создаваемая по умолчанию при инициализации таблицы.

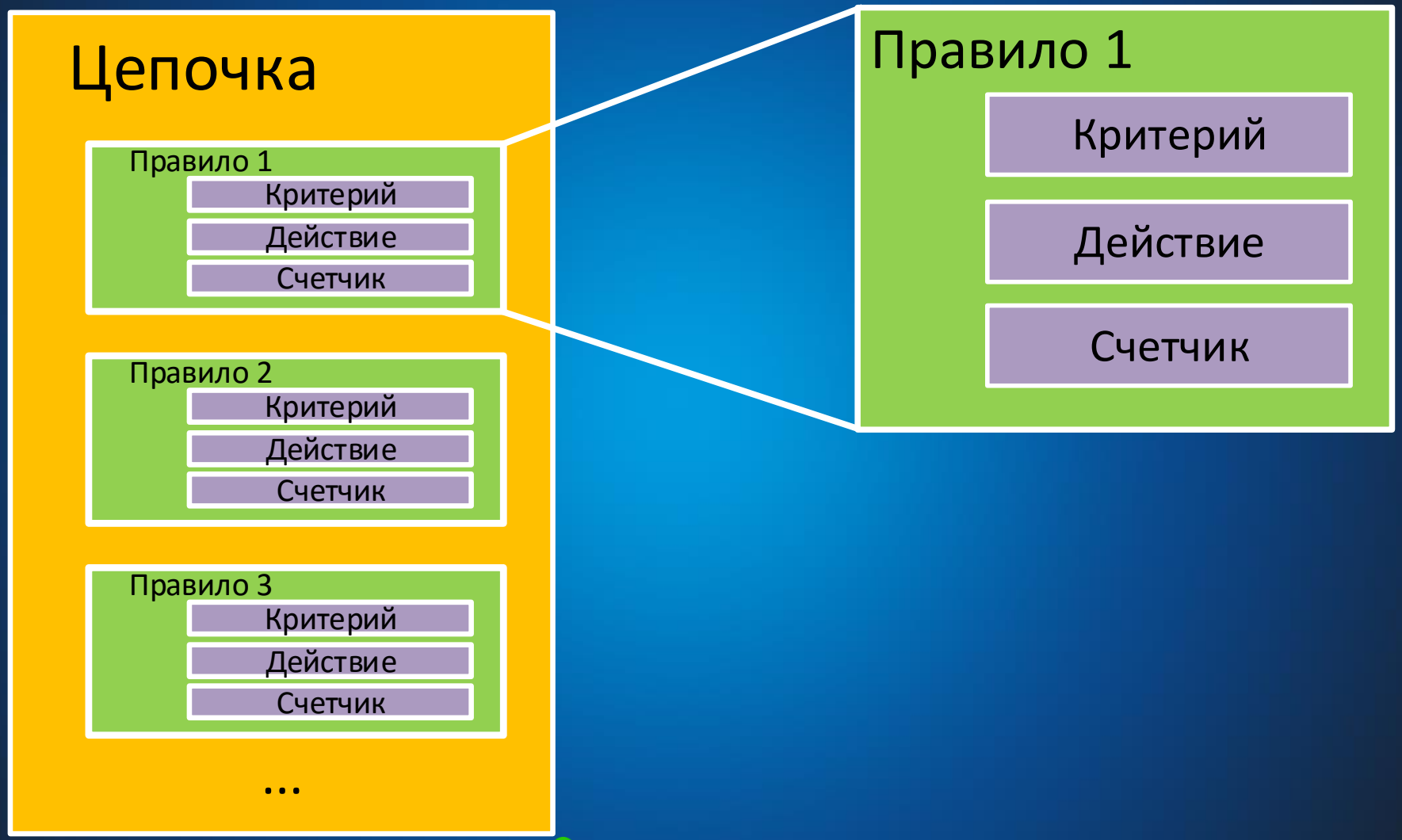
Пользовательская цепочка — цепочка, созданная пользователем.

Таблица — совокупность базовых и пользовательских цепочек, объединенных общим функциональным назначением.

7. Linux для начинающих. Базовый курс. Межсетевой экран

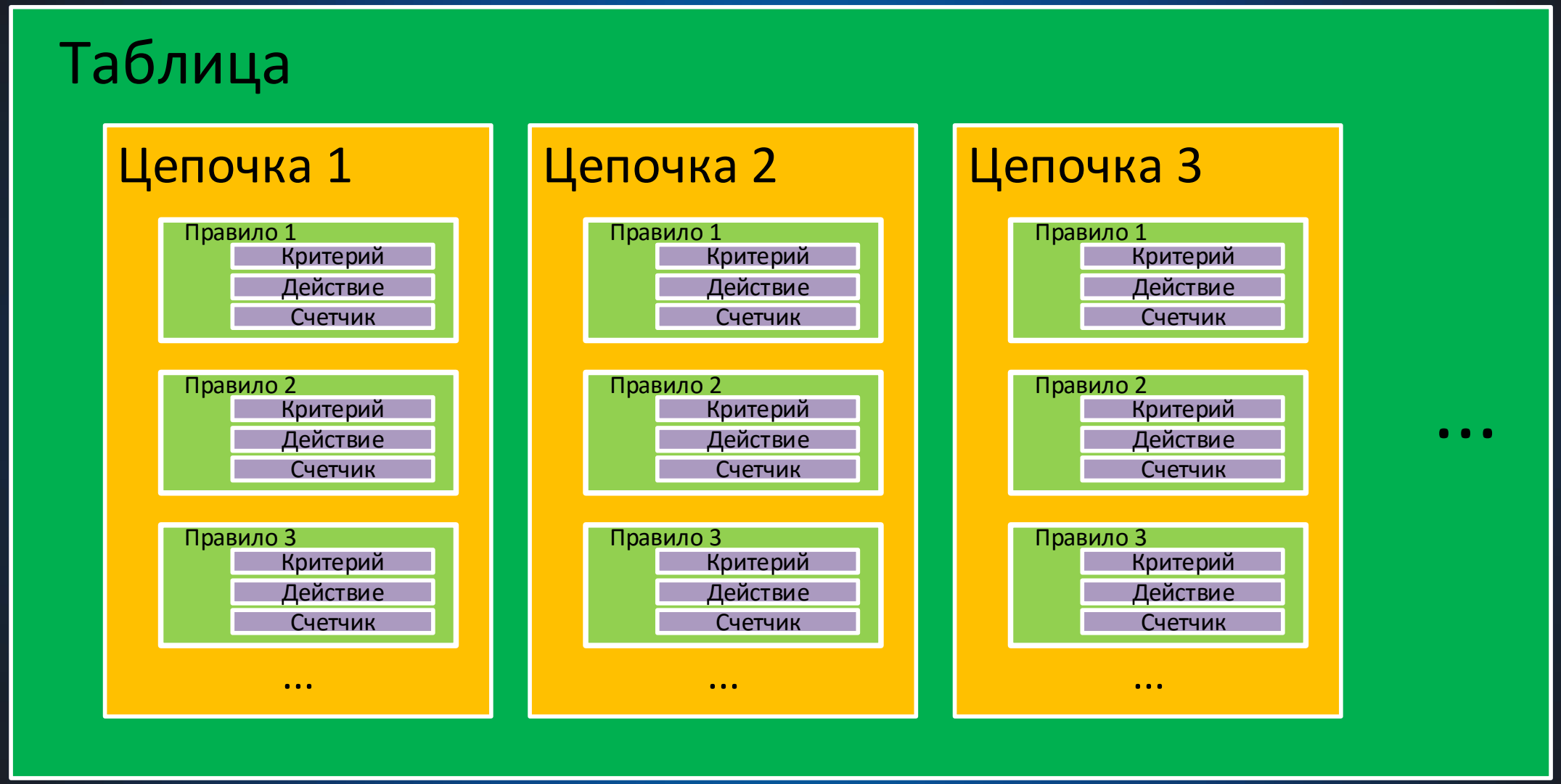
NetSkills
online IT school

7. Linux для начинающих. Базовый курс. Межсетевой экран



NetSkills
online IT school

7. Linux для начинающих. Базовый курс. Межсетевой экран



NetSkills
online IT school

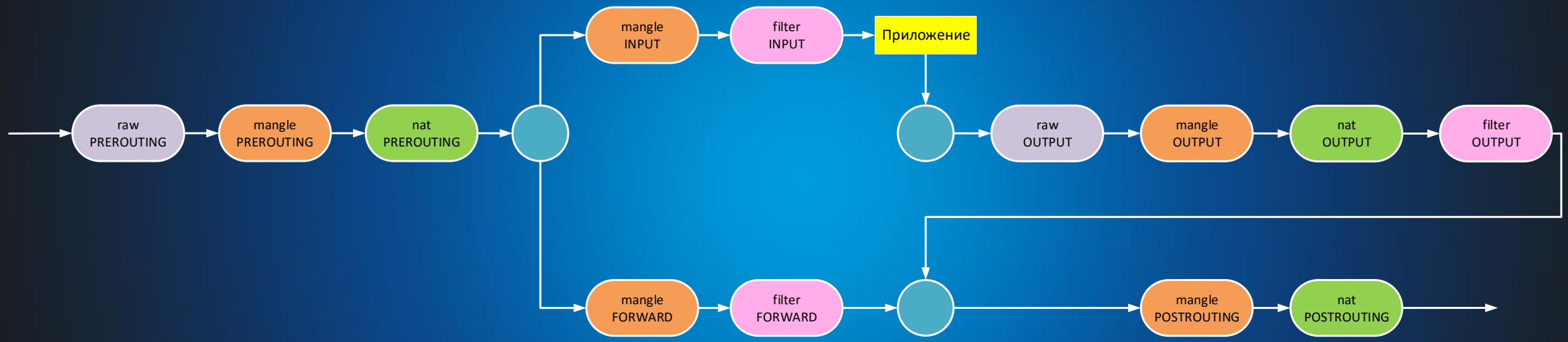
7. Linux для начинающих. Базовый курс. Межсетевой экран

Таблицы
raw — пакет проходит данную таблицу до передачи системе определения состояний.
mangle — содержит правила модификации (обычно полей заголовка) IP-пакетов.
nat — предназначена для подмены адреса отправителя или получателя.
filter — основная таблица, используется по умолчанию если название таблицы не указано. Используется для фильтрации пакетов.

Цепочки
PREROUTING — для изначальной обработки входящих пакетов
INPUT — для входящих пакетов, адресованных непосредственно локальному компьютеру
FORWARD — для проходящих (маршрутизируемых) пакетов
OUTPUT — для пакетов, создаваемых локальным компьютером (исходящих)
POSTROUTING— для окончательной обработки исходящих пакетов
Также можно создавать и уничтожать собственные цепочки при помощи утилиты iptables.

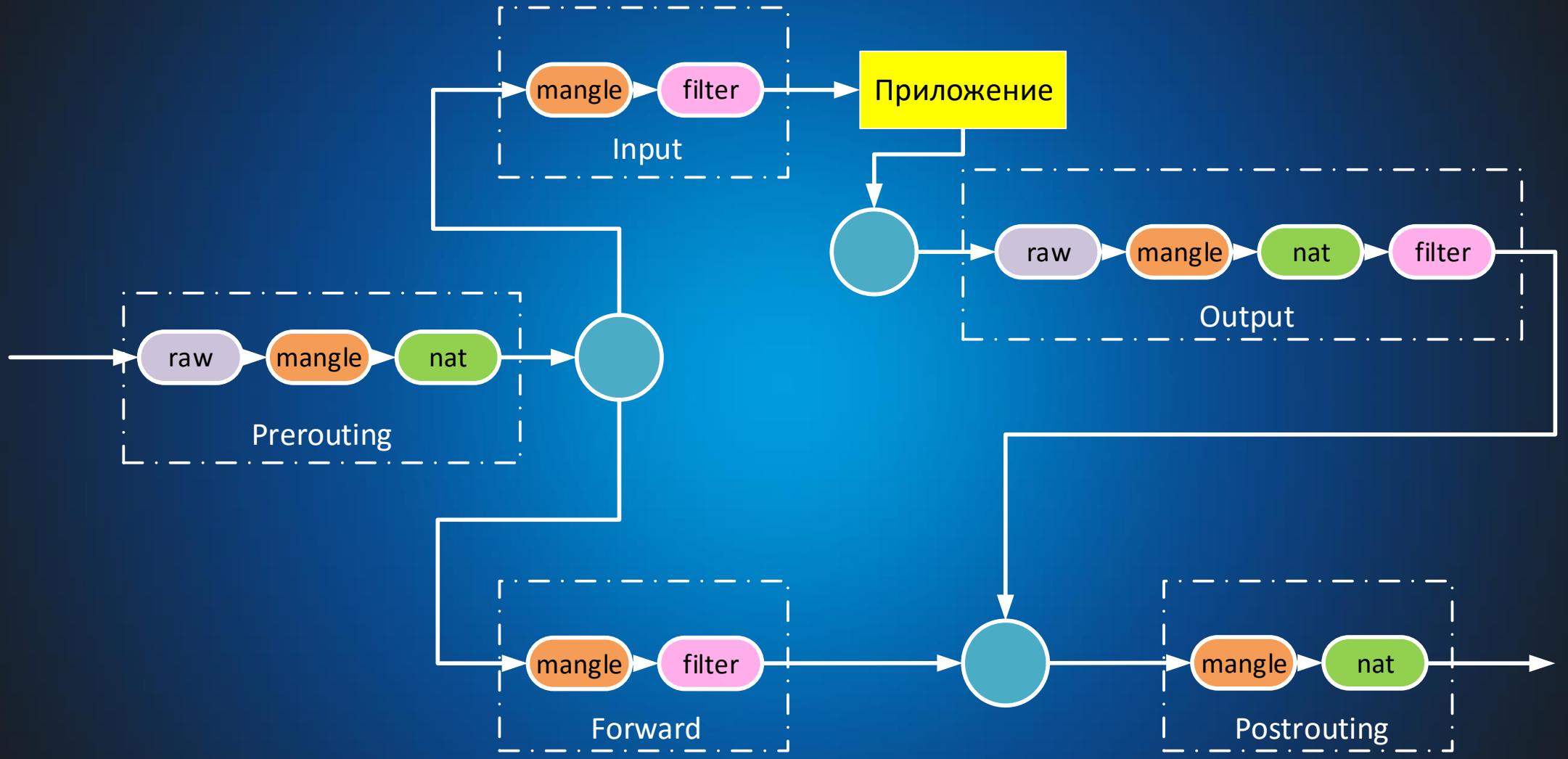
NetSkills
online IT school

7. Linux для начинающих. Базовый курс. Межсетевой экран



NetSkills
online IT school

7. Linux для начинающих. Базовый курс. Межсетевой экран



NetSkills
online IT school

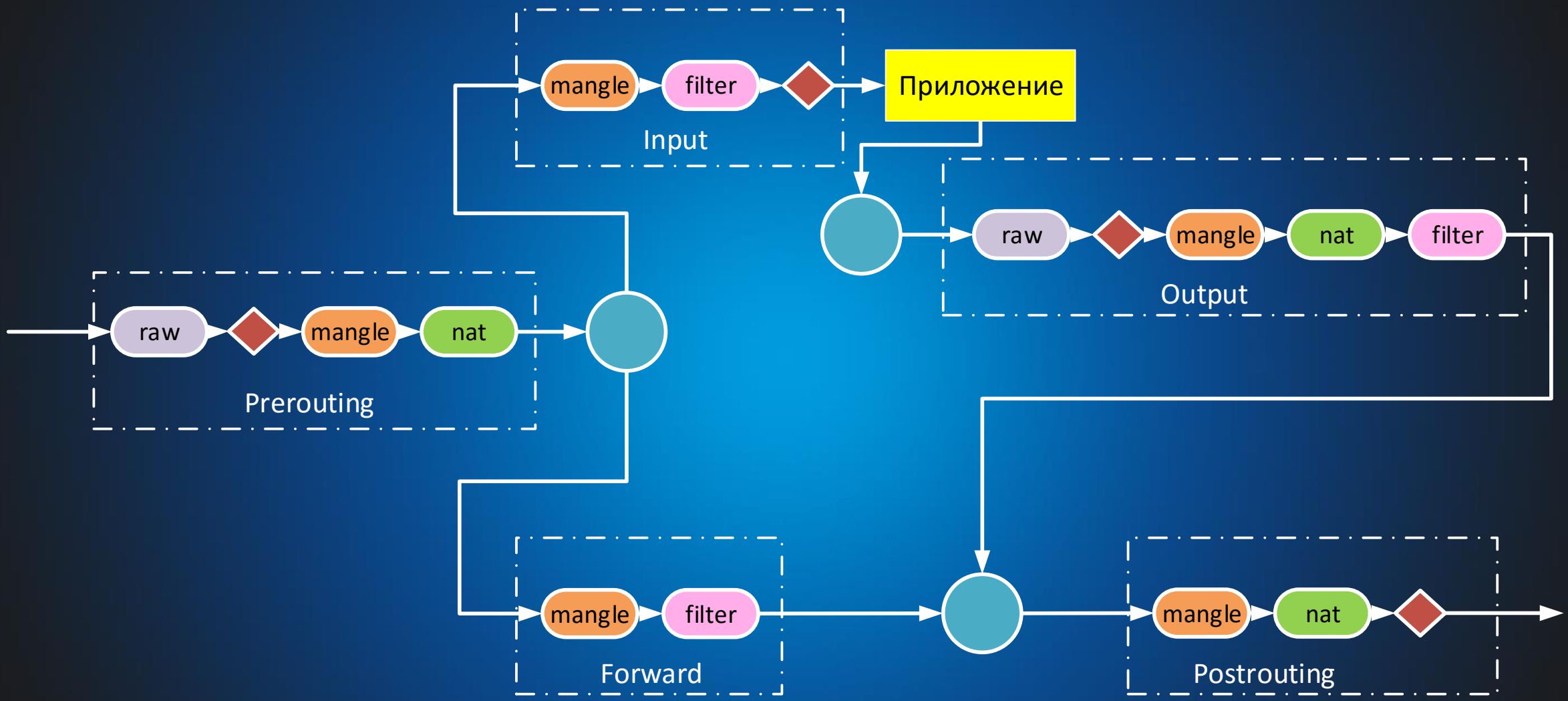
7. Linux для начинающих. Базовый курс. Межсетевой экран

Механизм определения состояний (state machine, connection tracking, conntrack) - позволяет определить какому соединению принадлежит пакет.

Типы состояний:
NEW – новое соединение
ESTABLISHED – уже установленное соединение
RELATED – дополнительное к уже существующему соединению
INVALID – другое соединение

NetSkills
online IT school

7. Linux для начинающих. Базовый курс. Межсетевой экран



NetSkills
online IT school

7. Linux для начинающих. Базовый курс. Межсетевой экран

Дополнительные ссылки

1. Утилита nmcli
2. Курс молодого бойца. Настройка NAT
3. Chkconfig и service

NetSkills
online IT school