РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук
Кафедра прикладной информатики и теории вероятностей

Презентация №13

iptables: Углубленный Анализ Межсетевого Экрана Linux

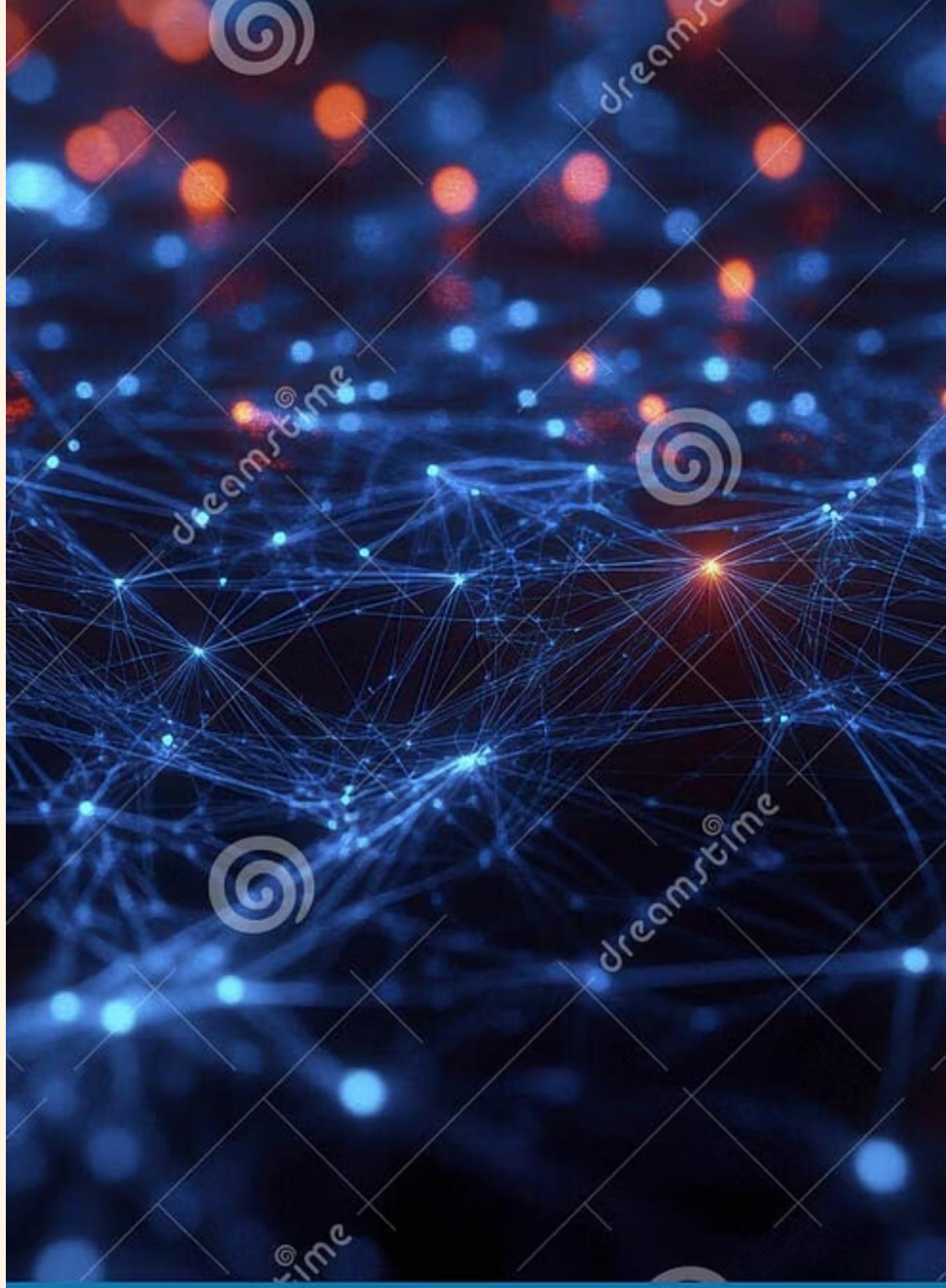
Студент: Эйвази Мани

Группа: НПИбд-03-24

Студенческий билет №: 1032245107

iptables: Углубленный Анализ Межсетевого Экрана Linux

Комплексное руководство для системных администраторов и инженеров по безопасности



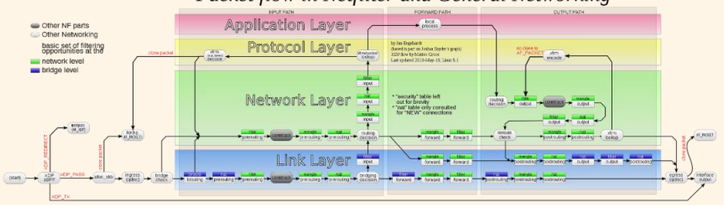
Архитектура Netfilter и Роль iptables

Netfilter *— это фреймворк в ядре Linux, предоставляющий хуки для перехвата и обработки сетевых пакетов на различных этапах их жизненного цикла. Он является основой для функциональности межсетевого экрана, NAT и других сетевых операций.*

iptables *выступает в качестве инструмента пользовательского пространства, который позволяет администраторам взаимодействовать с фреймворком Netfilter. С его помощью определяются правила, управляющие поведением сетевого трафика.*

Эта синергия обеспечивает мощный и гибкий механизм для контроля над сетевой безопасностью системы Linux.

Packet flow in Netfilter and General Networking



Таблицы iptables: Разделение Функционала

Filter

Основная таблица для фильтрации пакетов (ACCEPT, DROP, REJECT). Определяет, какие пакеты будут разрешены или запрещены.

NAT (Network Address Translation)

Используется для трансляции IP-адресов и портов. Включает SNAT (исходящий) и DNAT (входящий) для сокрытия или перенаправления трафика.

Mangle

Предназначена для изменения заголовков IP-пакетов (например, TTL, TOS) или установки меток для последующей обработки.

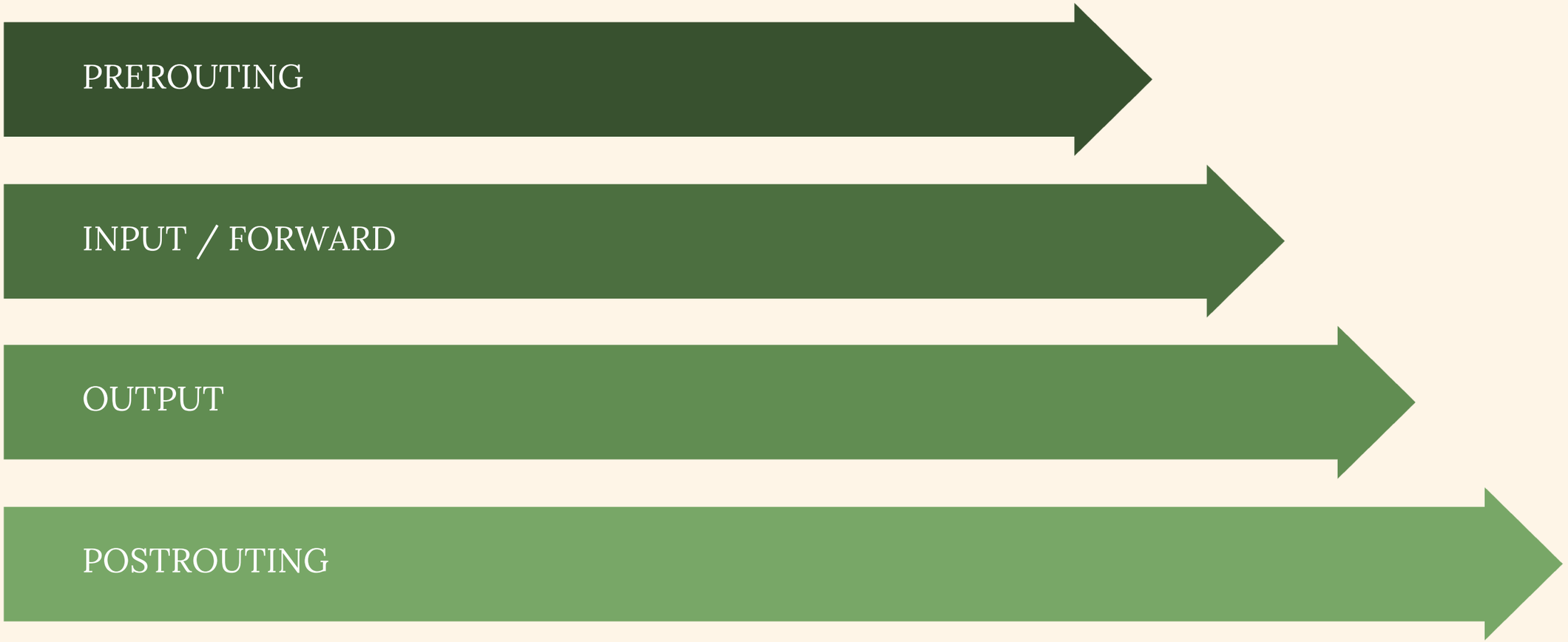
Raw

Используется для отключения отслеживания соединений (conntrack) для определенных пакетов, что может быть полезно для высокопроизводительных систем.

Security

Применяет метки безопасности SELinux к пакетам, обеспечивая интеграцию с расширенными механизмами безопасности.

Цепочки (Chains): Путь Пакета



Пакеты проходят через определенные цепочки в зависимости от их направления и типа (входящие, исходящие, пересылаемые). Каждая цепочка содержит набор правил, которые обрабатываются последовательно. Встроенные цепочки являются фундаментальной частью маршрутизации пакетов в ядре Linux.

Правила и Критерии Фильтрации

Структура Правила

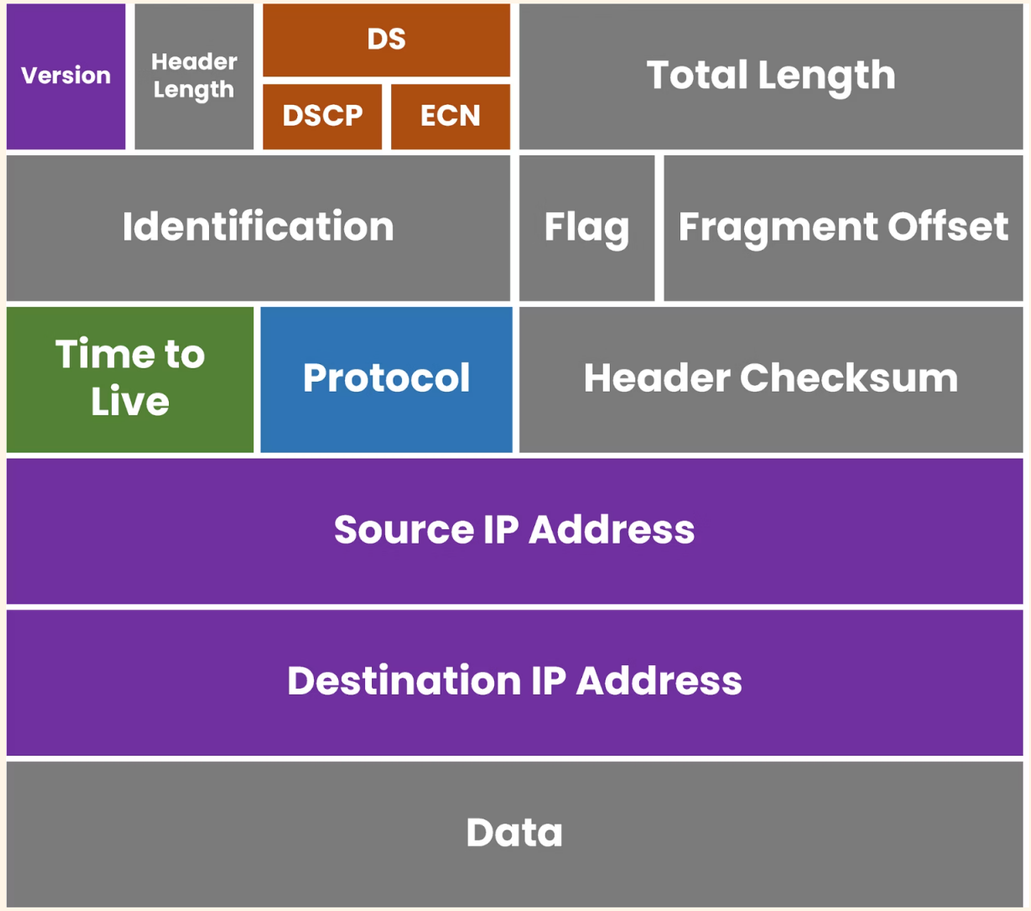
Каждое правило iptables состоит из нескольких компонентов:

- ***Таблица:*** *Определяет контекст применения правила (filter, nat, mangle и т.д.).*
- ***Цепочка:*** *Указывает, в какой точке обработки пакета правило должно быть применено (INPUT, OUTPUT, FORWARD).*
- ***Критерии:*** *Условия, которым должен соответствовать пакет.*
- ***Действие:*** *Что происходит с пакетом, если он соответствует критериям.*

Пример: `iptables -A INPUT -s 192.168.1.1 -p tcp --dport 22 -j ACCEPT`

Основные Критерии

- `--source (-s)`*: IP-адрес источника.*
- `--destination (-d)`*: IP-адрес назначения.*
- `--protocol (-p)`*: Протокол (tcp, udp, icmp, all).*
- `--dport`*: Порт назначения (для TCP/UDP).*
- `--in-interface (-i)`*: Входящий сетевой интерфейс.*
- `--out-interface (-o)`*: Исходящий сетевой интерфейс.*



Действия (Targets) iptables

ACCEPT

Разрешить пакету пройти. Обработка правила завершается.

DROP

Молча отбросить пакет. Отправитель не получает уведомления.

REJECT

Отклонить пакет и отправить отправителю ошибку (напр., ICMP port unreachable).

LOG

Записать информацию о пакете в системный журнал (syslog), затем продолжить обработку правил.

SNAT / DNAT

Source/Destination NAT. Изменение IP-адреса источника или назначения соответственно.

MASQUERADE

Динамический SNAT, используется для скрытия внутренней сети за внешним IP-адресом маршрутизатора.

RETURN

Прекратить обработку пакета в текущей цепочке и вернуться к вызывающей цепочке.

Отслеживание Соединений (conntrack)

*Механизм **conntrack** позволяет iptables отслеживать состояния сетевых соединений. Это критически важно для создания stateful (сохраняющих состояние) межсетевых экранов, которые более надежны и безопасны, чем stateless (без сохранения состояния).*

Без отслеживания состояний, каждое правило проверялось бы для каждого пакета независимо, что значительно усложнило бы настройку и снизило бы безопасность.

NEW

Пакет является частью нового соединения.

ESTABLISHED

Пакет принадлежит уже установленному соединению.

RELATED

Пакет связан с существующим соединением (напр., FTP-data).

INVALID

Пакет не может быть идентифицирован или принадлежит к некорректному соединению.

Базовые Сценарии Настройки

01

Запрет/Разрешение Входящих

Настройка политики по умолчанию для цепочки INPUT на DROP, затем явное разрешение необходимых портов (например, HTTP, HTTPS).

```
iptables -P INPUT DROP
```

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

02

Разрешение SSH

Предоставление доступа по SSH только с доверенных IP-адресов для повышения безопасности.

```
iptables -A INPUT -p tcp --dport 22 -s 192.168.1.0/24 -j ACCE
```

03

Настройка NAT (Маскарадинг)

Позволяет машинам в частной сети выходить в интернет через один публичный IP-адрес.

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

04

Простой Файервол

Комбинация разрешающих правил для известных сервисов и отброса всего остального входящего трафика.

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED
-j ACCEPT
```

Сохранение и Восстановление Правил

Правила iptables, установленные вручную или с помощью скриптов, по умолчанию не сохраняются при перезагрузке системы.

Для сохранения используется утилита `iptables-save`*, которая выводит текущий набор правил в стандартный вывод. Эти правила могут быть сохранены в файл:*

```
iptables-save > /etc/iptables/rules.v4
```

Для восстановления правил из файла используется `iptables-restore`*:*

```
iptables-restore < /etc/iptables/rules.v4
```

Автоматизация

Современные дистрибутивы Linux используют службы, такие как `iptables` *или* `netfilter-persistent`*, для автоматического сохранения и восстановления правил при загрузке/выключении системы. Необходимо убедиться, что эти службы активированы.*

Заключение и Перспективы

iptables остается мощным и широко используемым инструментом для управления межсетевым экраном в Linux, предлагая детальный контроль над сетевым трафиком.

Современное Состояние

Несмотря на появление более новых технологий, таких как `nftables`, iptables до сих пор является стандартом де-факто во многих системах и сетях.

Переход на nftables

`nftables` *представляет собой более гибкую и унифицированную систему для фильтрации пакетов, которая постепенно заменяет iptables. Знание iptables все еще является ценным активом, так как многие концепции переходят в* `nftables`.

Практические Рекомендации

Начинайте с простых правил, постепенно усложняя их. Всегда тестируйте изменения в безопасной среде и обеспечьте возможность отката. Регулярно просматривайте и обновляйте правила межсетевого экрана.

Спасибо за внимание