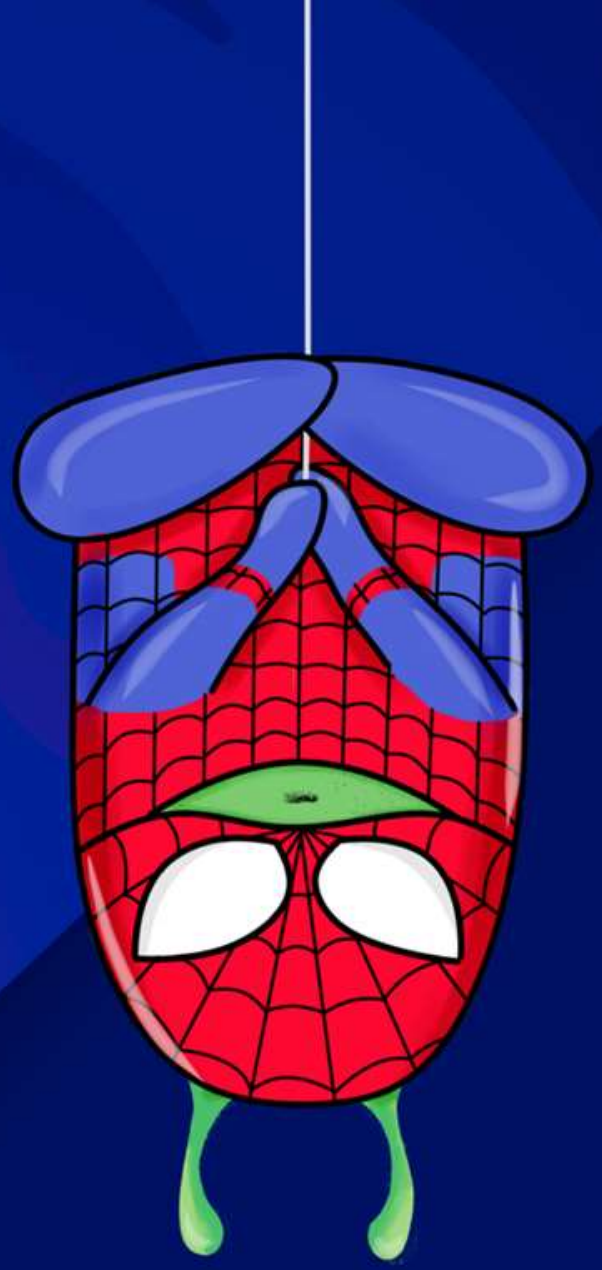
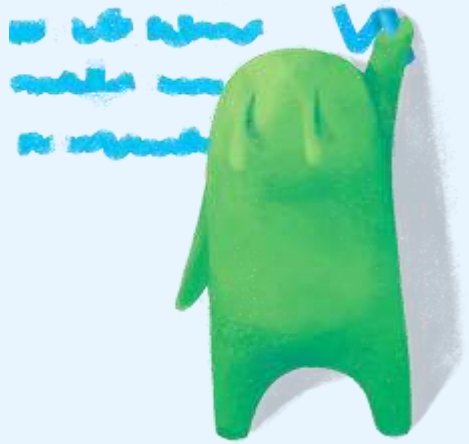
Firewall



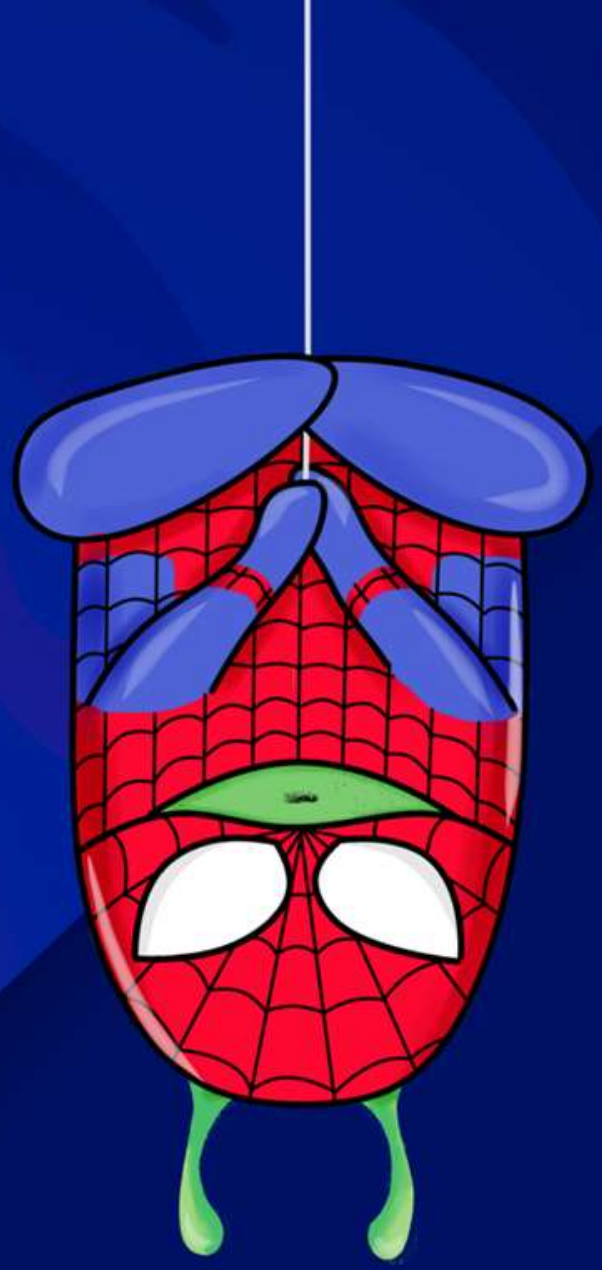
Спикер:
Роман Козлов

Firewall



- Iptables - что такое и зачем он нужен
- INPUT - защита системы linux
- FORWARD - защита транзитного трафика
- OUTPUT - защита от скомпрометированных сервисов
- Established/Related/Invalid/New и концепция statefull firewall, contrack
- Дополнительные цепочки
- Работа с адрес-листами

Iptables - что такое и зачем он нужен



Спикер:
Роман Козлов

iptables - ЧТО ТАКОЕ И ЗАЧЕМ ОН НУЖЕН

- Iptables/ip6tables — утилита командной строки, является стандартным интерфейсом управления работой межсетевого экрана (брандмауэра) netfilter для Linux
- Для использования утилиты iptables требуются привилегии суперпользователя (root)
- Иногда под словом iptables имеется в виду и сам межсетевой экран netfilter
- Базируется На основе правил, которые анализируются последовательно до тех пор, пока не будет найдено первое совпадение
- Правила брандмауэра Iptables упорядочены в таблицы: filter, nat, mangle, raw, security
- Просмотр состояния IPTABLES (версия iptables –v)
- iptables -L -n -v

iptables - ЧТО ТАКОЕ И ЗАЧЕМ ОН НУЖЕН

iptables структурно состоит из **таблиц**, в которые входят **цепочки**, в свою очередь содержащие наборы **правил**

RAW	MANGLE	NAT	FILTER	SECURITY
PREROUTING	PREROUTING	PREROUTING	INPUT	INPUT
OUTPUT	INPUT	OUTPUT	FORWARD	FORWARD
	FORWARD	POSTROUTING	OUTPUT	OUTPUT
	OUTPUT			
	POSTROUTING			

iptables

Просмотр таблиц и цепочек

```
iptables [-t имя таблицы] [-L имя цепочки]
```

```
root@msk-r01:~# iptables -L INPUT -t filter -v --line-numbers
Chain INPUT (policy ACCEPT 10 packets, 1710 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      748 54900 ACCEPT     all  --  any    any     anywhere             anywhere             ctstate RELATED,ESTABLISHED
2        0     0 DROP       all  --  any    any     anywhere             anywhere             ctstate INVALID
3        0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:ssh
4        0     0 DROP       all  --  ens3   any     anywhere             anywhere
root@msk-r01:~#
```

```
iptables -S [-t имя таблицы]
```

```
root@msk-r01:~# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -m conntrack --ctstate INVALID -j DROP
-A INPUT -i ens3 -p icmp -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -i ens3 -j DROP
```

Добавление правил

```
iptables -t таблица действие цепочка дополнительные_параметры
```

iptables – ОСНОВНЫЕ ДЕЙСТВИЯ

-A - добавить правило в цепочку

-D - удалить правило

-I - вставить правило с нужным номером

-L - вывести все правила в текущей цепочке

-S - вывести все правила в формате ввода правил

-F - очистить все правила

-N - создать цепочку

-X - удалить цепочку

-P - установить действие по умолчанию для цепочки

! - отрицание перед условием (кроме)

iptables ДЕЙСТВИЯ ПО УМОЛЧАНИЮ

- Во всех таблицах iptables есть правило по умолчанию – что делать с пакетами после обработки всеми правилами в данной цепочке
- Возможно изменить действие по умолчанию используя –P
- Прежде чем менять действие по умолчанию на DROP – добавьте разрешающие правила в соответствующую цепочку

```
root@msk-r01:~# iptables -S -t raw
-P PREROUTING ACCEPT
-P OUTPUT ACCEPT
```

```
root@msk-r01:~# iptables -S -t mangle
-P PREROUTING ACCEPT
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-P POSTROUTING ACCEPT
```

```
root@msk-r01:~# iptables -S -t nat
-P PREROUTING ACCEPT
-P INPUT ACCEPT
-P OUTPUT ACCEPT
-P POSTROUTING ACCEPT
```

```
root@msk-r01:~# iptables -S -t filter
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
```

iptables adds

Установка iptales

```
apt install iptables
```

Установка утилиты сохранения правил

```
apt install iptables-persistent
systemctl enable netfilter-persistent.service
systemctl status netfilter-persistent.service
```

Сохранение текущих правил

```
netfilter-persistent save
```

Сохранение всех правил iptables в файл

```
iptables-save > имя_файла.txt
```

Загрузка всех правил iptables из файла

```
Iptables-restore < имя_файла.txt
```

iptables –t filter

01

Работа по принципу «Если-ТО»

02

Упорядочены в цепочки

03

Существуют предопределенные цепочки

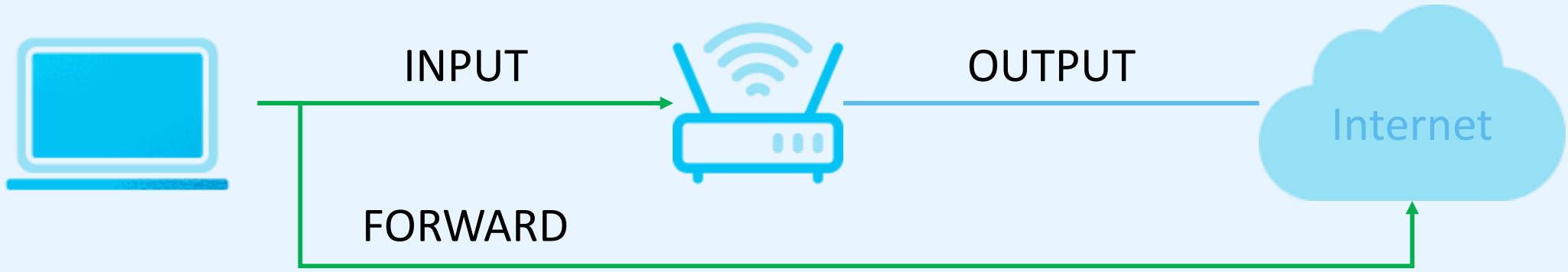
04

Пользователи могут создавать собственные цепочки

iptables –t filter -l

Это предопределенные цепочки

- **INPUT** (Пакеты предназначенные HOST)
- **FORWARD** (Транзитные пакеты через HOST)
- **OUTPUT** (Пакеты сгенерированные HOST)



iptables –j (ДЕЙСТВИЯ)

- Каждое правило имеет действие - что делать, когда пакет сопоставлен (попал под это правило)
- Принимать (ACCEPT)
- Отбрасывать (DROP) или отклонять (REJECT) - и отправлять сообщение отклонения icmp
- JUMP и RETURN в/из пользовательских цепочек
- И другое

```
root@msk-r01:~# iptables -A INPUT -j
ACCEPT    DROP      FORWARD   INPUT     LOG       OUTPUT    REJECT    ULOG
```

iptables –m comment

```
iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT -m comment --comment "ACCEPT ESTABLISHED RELATED PACKET IN INPUT"
```

```
root@msk-r01:~# iptables -S -t filter
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment "ACCEPT ESTABLISHED RELATED PACKET IN INPUT" -j ACCEPT
-A INPUT -m conntrack --ctstate INVALID -m comment --comment "DROP INVALID PACKET IN INPUT" -j DROP
-A INPUT -i ens3 -p icmp -m comment --comment "ACCEPT PING OTHER ICMP TO HOST" -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -m comment --comment "ACCEPT SSH CONNECTION TO HOST" -j ACCEPT
-A INPUT -i ens3 -m comment --comment "DROP ALL TO HOST" -j DROP
```

```
root@msk-r01:~# iptables -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED /* ACCEPT ESTABLISHED RELATED PACKET IN INPUT */
DROP       all  --  anywhere             anywhere             ctstate INVALID /* DROP INVALID PACKET IN INPUT */
ACCEPT     icmp --  anywhere             anywhere             /* ACCEPT PING OTHER ICMP TO HOST */
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh /* ACCEPT SSH CONNECTION TO HOST */
DROP       all  --  anywhere             anywhere             /* DROP ALL TO HOST */
```

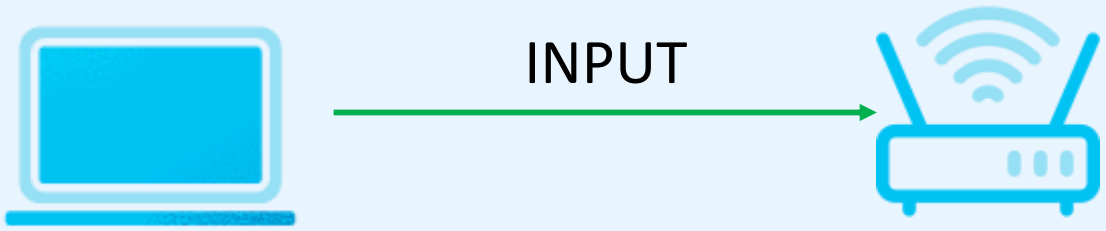
СОВЕТ. Чтобы улучшить читаемость правил iptables, можно упорядочить их последовательно по цепочкам и добавить комментарии.

INPUT - защита системы Linux

Спикер:
Роман Козлов

iptables -t filter -A INPUT

- Защищает службы на linux хосте – ssh, web, vpn, proxy и прочие
- Либо из Интернета, либо из внутренней сети



iptables -t filter -A INPUT

- **Правило открывающее доступ к SSH на серер с интерфейса ens3 (в данном случае интерфейс из WAN)**
  ```
  iptables -t filter -A INPUT -i ens3 -p tcp --dport 22 -j ACCEPT
  ```
- **Правило разрешающее установленные и связанные соединения***
  ```
  iptables -I INPUT 1 -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment
  "ACCEPT ESTABLISHED RELATED PACKET IN INPUT" -j ACCEPT
  ```
- **Правило открывающее доступ к icmp на сервере с внешнего интерфейса**
  ```
  iptables -t filter -A INPUT -i ens3 –p icmp -j ACCEPT
  ```
- **Правило запрещающее весь остальной трафик**
  ```
  iptables -t filter -A INPUT -i ens3 -j DROP
  ```
- **Не забываем сохранить правила**
  ```
  - netfilter-persistent save
  ```

iptables -t filter -A INPUT

iptables -t filter -L INPUT -n

```
root@msk-r01:~# iptables -t filter -L INPUT -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           ctstate RELATED,ESTABLISHED /* ACCEPT ESTABLISHED RELATED PACKET IN INPUT */
DROP       all  --  0.0.0.0/0            0.0.0.0/0           ctstate INVALID /* DROP INVALID PACKET IN INPUT */
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           /* ACCEPT PING OTHER ICMP TO HOST */
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22 /* ACCEPT SSH CONNECTION TO HOST */
DROP       all  --  0.0.0.0/0            0.0.0.0/0           /* DROP ALL TO HOST */
```

iptables -S -t filter

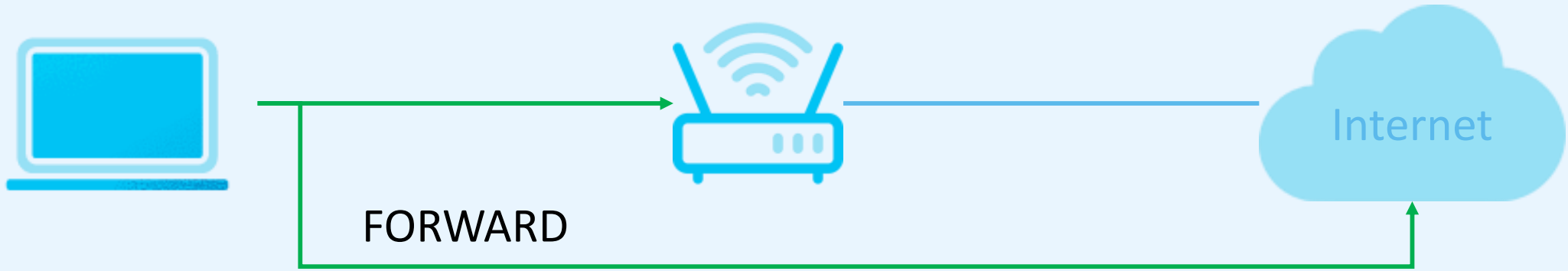
```
root@msk-r01:~# iptables -S -t filter
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment "ACCEPT ESTABLISHED RELATED PACKET IN INPUT" -j ACCEPT
-A INPUT -m conntrack --ctstate INVALID -m comment --comment "DROP INVALID PACKET IN INPUT" -j DROP
-A INPUT -i ens3 -p icmp -m comment --comment "ACCEPT PING OTHER ICMP TO HOST" -j ACCEPT
-A INPUT -i ens3 -p tcp -m tcp --dport 22 -m comment --comment "ACCEPT SSH CONNECTION TO HOST" -j ACCEPT
-A INPUT -i ens3 -m comment --comment "DROP ALL TO HOST" -j DROP
```

FORWARD – защита транзитного трафика

Спикер:
Роман Козлов

iptables -t filter -A FORWARD

- Содержит правила, управляющие пакетами, проходящими через HOST
- FORWARD контролирует трафик транзитный трафик
- С помощью цепочки FORWARD мы защищаем локальные сети, ограничиваем доступ в интернет, защищаем виртуальные машины и контейнеры



iptables -t filter -A FORWARD

- **Правило открывающее доступ ЧЕРЕЗ внешний интерфейс ens3(WAN) с внутреннего интерфейса ens4(LAN)**

```
iptables -t filter -A FORWARD -i ens4 -o ens3 -j ACCEPT
```

- **Правило разрешающее установленные и связанные соединения***

```
iptables -I FORWARD 1 -m conntrack --ctstate RELATED,ESTABLISHED -m comment --
comment "ACCEPT ESTABLISHED RELATED PACKET IN FORWARD" -j ACCEPT
```

- **Правило запрещающее транзитный трафик с ens3(WAN) интерфейса в локальную сеть, кроме dst-nat***

```
iptables –t filter -A FORWARD -i ens3 -m conntrack  ! --ctstate DNAT -j DROP
```

- **Не забываем сохранить правила**

```
- netfilter-persistent save
```

iptables -t filter -A FORWARD

iptables -L FORWARD -n -v

```
root@msk-r01:~# iptables -L FORWARD -n -v
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate RELATED,ESTABLISHED /* ACCEPT ESTABLISHED RELATED PACKET IN FORWARD */
    0     0 ACCEPT     all  --  ens4   ens3    0.0.0.0/0            0.0.0.0/0
    0     0 DROP       all  --  ens3   *       0.0.0.0/0            0.0.0.0/0           ! ctstate DNAT
```

iptables -S -t filter

```
root@msk-r01:~# iptables -S -t filter
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment "ACCEPT ESTABLISHED RELATED PACKET IN INPUT" -j ACCEPT
-A INPUT -m conntrack --ctstate INVALID -m comment --comment "DROP INVALID PACKET IN INPUT" -j DROP
-A INPUT -i ens3 -p icmp -m comment --comment "ACCEPT PING OTHER ICMP TO HOST" -j ACCEPT
-A INPUT -i ens3 -p tcp -m tcp --dport 22 -m comment --comment "ACCEPT SSH CONNECTION TO HOST" -j ACCEPT
-A INPUT -i ens3 -m comment --comment "DROP ALL TO HOST" -j DROP
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment "ACCEPT ESTABLISHED RELATED PACKET IN FORWARD" -j ACCEPT
-A FORWARD -i ens4 -o ens3 -j ACCEPT
-A FORWARD -i ens3 -m conntrack ! --ctstate DNAT -j DROP
```

iptables -t filter -A FORWARD

- **Правило запрещающее выход из локальной сети по SMTP и SMB протоколам**
  ```
  iptables -I FORWARD 2 -s 172.30.0.0/22 -i ens4 -o ens3 -p tcp -m multiport  --dports 25,445 -j DROP
  ```

- **Правило разрешающее выход по наиболее используемым портам во внешнюю сеть по протоколу tcp**
  ```
  iptables -I FORWARD 3 -s 172.30.0.0/22 -i ens4 -o ens3 -p tcp-m multiport  --dports 80,443,8080,993,995,465,587 -j ACCEPT
  ```

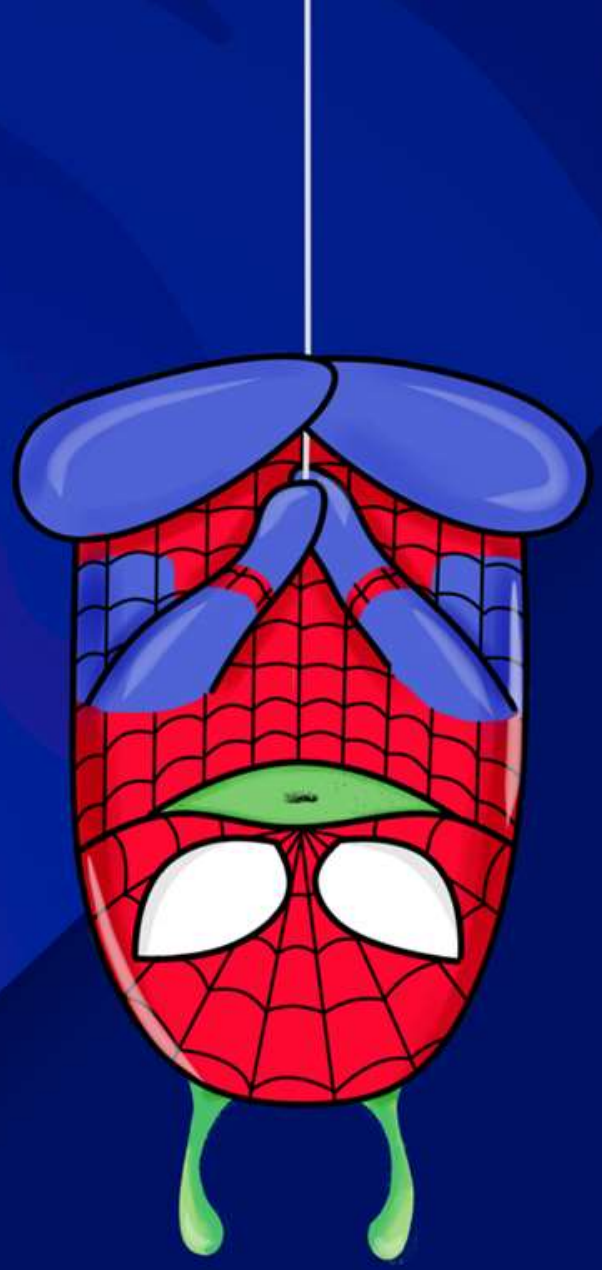
- **Правило разрешающее выход по наиболее используемым портам во внешнюю сеть по протоколу udp**
  ```
  iptables -I FORWARD 4 -s 172.30.0.0/22 -i ens4 -o ens3 -p udp -m multiport  --dports 80,443,8080,993,995,465,587 -j ACCEPT
  ```

- **Правило запрещающее выход по всем остальным протоколам**
  ```
  iptables -I FORWARD 5 -i ens4 -o ens3 -j DROP
  ```

НАИБОЛЕЕ ЧАСТО ИСПОЛЬЗУЕМЫЕ СЛУЖБЫ

Port	Service
80/tcp	HTTP
443/tcp/udp	HTTPS
22/tcp	SSH
23/tcp	Telnet
20,21/tcp	FTP
25,143,110,993,995,465,587/tcp	MAIL
445/TCP	SMB

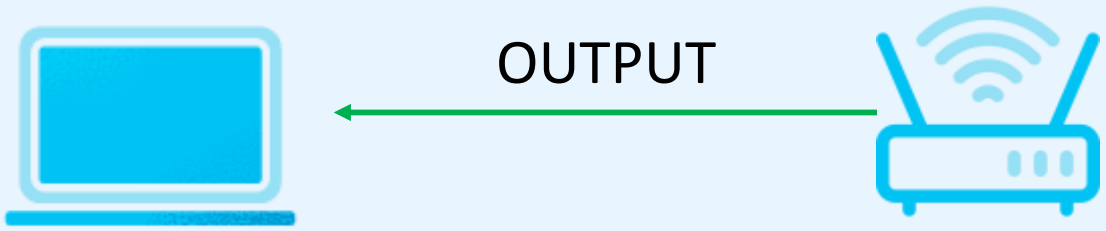
OUTPUT – защита от скомпрометированных сервисов



Спикер:
Роман Козлов

iptables -t filter -A OUTPUT

- OUTPUT – защищает от пакетов сгенерированных HOST
- В модульной операционной системе могут быть ситуации, когда злоумышленник скомпрометировал какую-то определённую службу на host – без полного доступа к операционной системе



iptables -t filter -A OUTPUT

- **Правило разрешающее установленные и связанные соединения* от Linux HOST**
  ```
  iptables -A OUTPUT -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment
  "ACCEPT ESTABLISHED RELATED PACKET FROM OUTPUT" -j ACCEPT
  ```

- **Правило разрешающее icmp трафик с сервера**
  ```
  iptables -t filter -A OUTPUT -p icmp -j ACCEPT
  ```

- **Правило разрешающее трафик с src-port(порт источника) 22, 80, 443 TCP**
  ```
  iptables -t filter -A OUTPUT -p tcp -m multiport --sports 22,80,443 -j ACCEPT
  ```

- **Правило разрешающее трафик для DNS службы**
  ```
  iptables -I OUTPUT 3 -p udp --dport 53 -j ACCEPT
  ```

- **Правило запрещающее весь остальной трафик с linux host**
  ```
  iptables -t filter -A OUTPUT -j DROP
  ```

- **Не забываем сохранить правила**
  ```
  - netfilter-persistent save
  ```

iptables -t filter -A OUTPUT

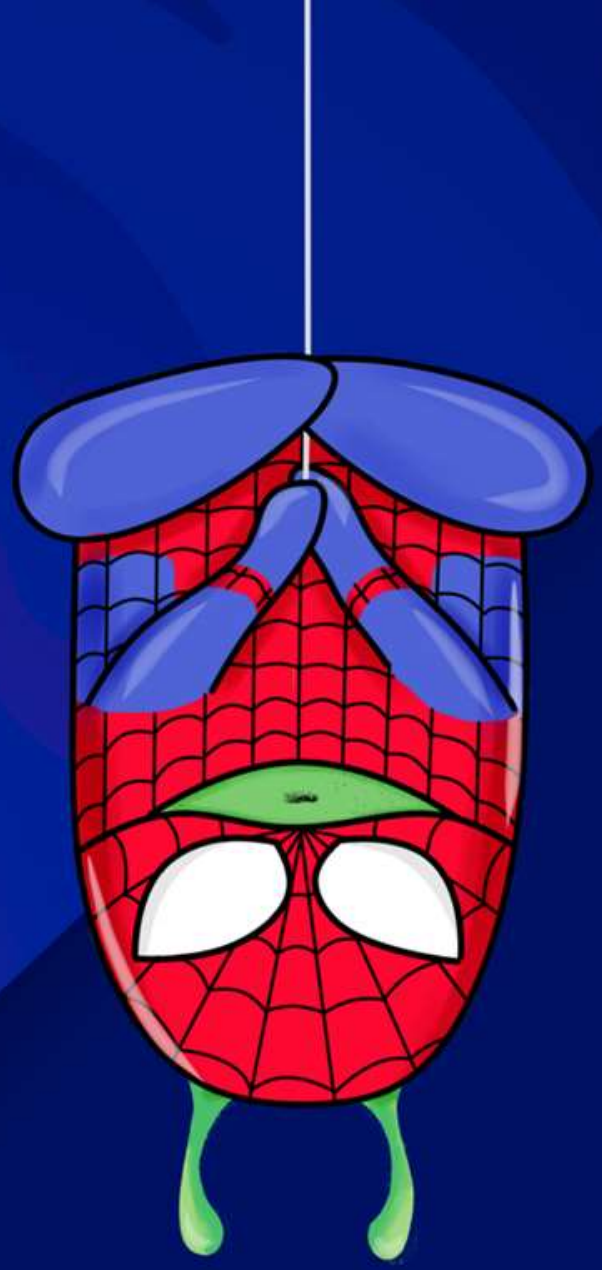
iptables -L OUTPUT -n -v

```
root@msk-r01:~# iptables -L OUTPUT -n -v
Chain OUTPUT (policy ACCEPT 3351 packets, 404K bytes)
 pkts bytes target     prot opt in     out     source               destination
  316 33840 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate RELATED,ESTABLISHED /* ACCEPT ESTABLISHED RELATED PACKET FROM OUTPUT */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           multiport sports 22,80,443
    1   327 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

iptables -S -t filter

```
root@msk-r01:~# iptables -S -t filter
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment "ACCEPT ESTABLISHED RELATED PACKET IN INPUT" -j ACCEPT
-A INPUT -m conntrack --ctstate INVALID -m comment --comment "DROP INVALID PACKET IN INPUT" -j DROP
-A INPUT -i ens3 -p icmp -m comment --comment "ACCEPT PING OTHER ICMP TO HOST" -j ACCEPT
-A INPUT -i ens3 -p tcp -m tcp --dport 22 -m comment --comment "ACCEPT SSH CONNECTION TO HOST" -j ACCEPT
-A INPUT -i ens3 -m comment --comment "DROP ALL TO HOST" -j DROP
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment "ACCEPT ESTABLISHED RELATED PACKET IN FORWARD" -j ACCEPT
-A FORWARD -s 172.30.0.0/22 -i ens4 -o ens3 -p tcp -m multiport --dports 25,445 -j DROP
-A FORWARD -s 172.30.0.0/22 -i ens4 -o ens3 -p tcp -m multiport --dports 80,443,8080,993,995,465,587 -j ACCEPT
-A FORWARD -s 172.30.0.0/22 -i ens4 -o ens3 -p udp -m multiport --dports 80,443,8080,993,995,465,587 -j ACCEPT
-A FORWARD -i ens4 -o ens3 -p icmp -j ACCEPT
-A FORWARD -i ens4 -o ens3 -j DROP
-A FORWARD -i ens3 -m conntrack ! --ctstate DNAT -j DROP
-A OUTPUT -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment "ACCEPT ESTABLISHED RELATED PACKET FROM OUTPUT" -j ACCEPT
-A OUTPUT -p icmp -j ACCEPT
-A OUTPUT -p tcp -m multiport --sports 22,80,443 -j ACCEPT
-A OUTPUT -j DROP
```

Established/Related/Invalid/New и концепция statefull firewall, contrack



Спикер:
Роман Козлов

statefull firewall — это firewall, который отслеживает полное состояние активных сетевых подключений

statefull firewall — это firewall, "запоминающий" состояние соединения, либо генерирующий динамические правила для прохождения пакетов, которые (правила) после определенного промежутка времени «удаляются»

conntrack

- Компонент netfilter, обеспечивающий отслеживание состояния соединений и классификацию пакетов с точки зрения принадлежности к соединениям, что позволяет netfilter осуществлять полноценную stateful-фильтрацию трафика

- Как и netfilter, система conntrack является частью ядра Linux

- Отслеживание состояний отдельных соединений с тем, чтобы классифицировать каждый пакет либо как относящийся к уже установленному соединению, либо как открывающий новое соединение. При этом понятие «состояние соединения» искусственно вводится для протоколов, в которых оно изначально отсутствует (UDP, ICMP)

conntrack

- При работе же с протоколами, поддерживающими состояния (например, TCP), conntrack активно использует эту возможность, тесно взаимодействуя с базовой сетевой подсистемой ядра Linux

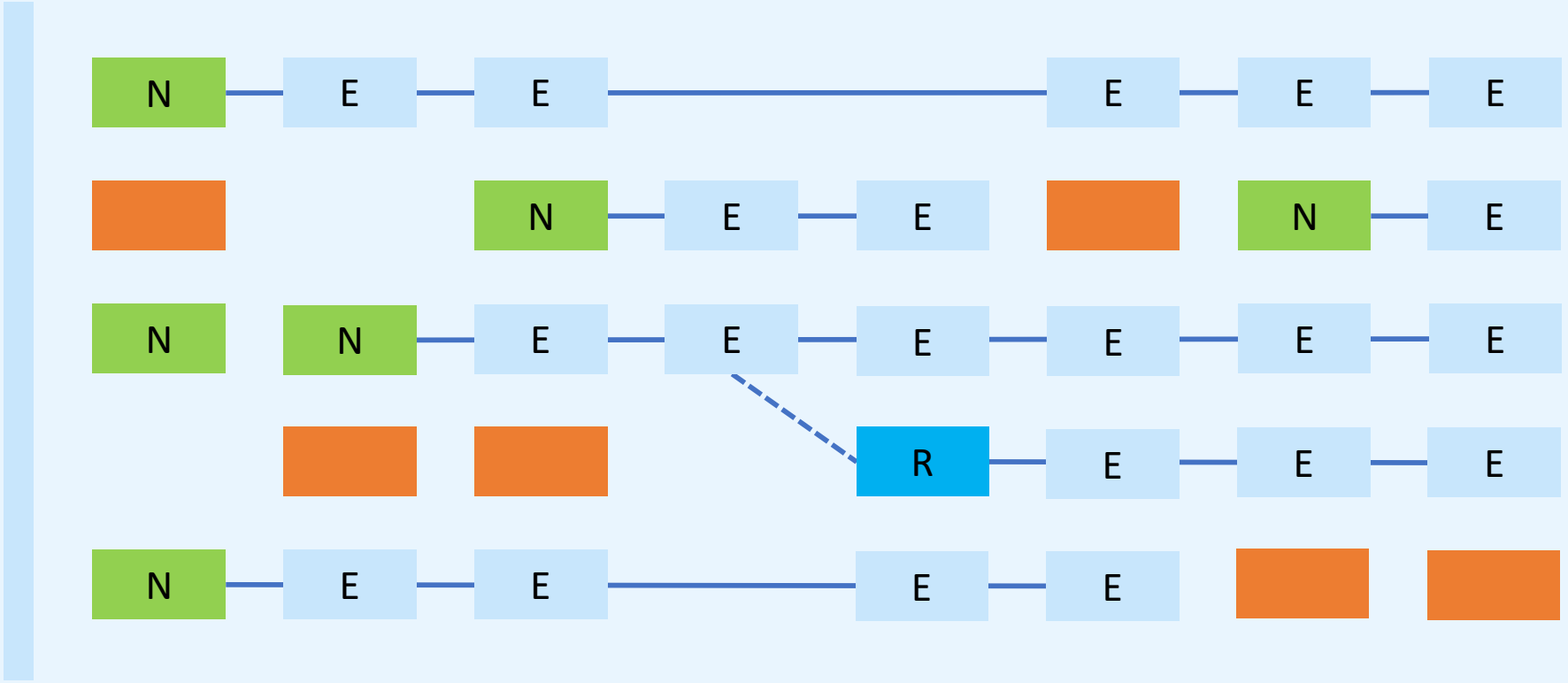
- Отслеживание связанных соединений, например, ICMP-ответов на TCP и UDP-пакеты

- Для правильной обработки сложных протоколов(FTP, SIP) conntrack использует специальные модули (conntrack helpers), которые анализируют трафик и «выхватывают» информацию протокола о новых соединениях (например, порт, на который оно будет открыто), что позволяет обеспечить их корректную фильтрацию, маршрутизацию, шейпинг и пропускание через NAT

iptables –a input/forward/output-m conntrack --ctstate

- **NEW** - пакет открывает новое соединение – все правила пишут относительно новых соединений
- **ESTABLISHED** - пакет принадлежит к уже открытому соединению
- **RELATED** - пакет открывает новое соединение, но оно имеет отношение к уже имеющемуся соединению
- **INVALID** - пакет не принадлежит ни к одному из известных соединений
- **UNTRACKED** - отслеживание состояния соединения для данного пакета было отключено. Обычно оно отключается с помощью действия NOTRACK в таблице raw
- **DNAT** - показывает, что к данному соединению применена операция подмены адреса назначения
- **SNAT** - показывает, что к данному соединению применена операция подмены адреса источника

CONNECTIONS



N - New R - Releated E - Estalished - Invalid

iptables –a -m conntrack --ctstate

- **Правило разрешающее установленные и связанные соединения в цепочке INPUT**
  ```
  iptables -I INPUT 1 -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment
  "ACCEPT ESTABLISHED RELATED PACKET IN FORWARD" -j ACCEPT
  ```

- **Правило разрешающее установленные и связанные соединения в цепочке FORWARD**
  ```
  iptables -I FORWARD 1 -m conntrack --ctstate RELATED,ESTABLISHED -m comment --
  comment "ACCEPT ESTABLISHED RELATED PACKET IN FORWARD" -j ACCEPT
  ```

- **Правило разрешающее установленные и связанные соединения в цепочке OUTPUT**
  ```
  iptables -A OUTPUT -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment
  "ACCEPT ESTABLISHED RELATED PACKET FROM OUTPUT" -j ACCEPT
  ```

- **Правило запрещающее INVALID соединения в цепочке INPUT с интерфейса ens3(WAN)**
  ```
  iptables -I INPUT 2 –I ens3 -m conntrack --ctstate INVALID-m comment --comment
  “DROP INVALID PACKET IN INPUT" -j DROP
  ```

- **Правило запрещающее INVALID соединения в цепочке FORWARD с интерфейса ens3(WAN)**

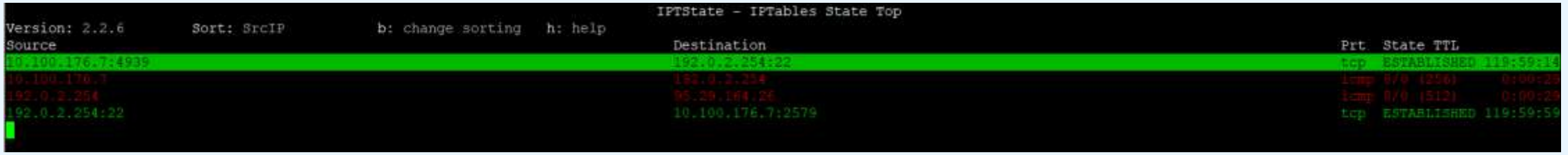
- ```
  iptables -I FORWARD 2 –I ens3 -m conntrack --ctstate INVALID-m comment --comment
  “DROP INVALID PACKET IN INPUT" -j DROP
  ```
  ```

conntrack / iptstate

Инструменты для просмотра состояния conntrack в linux

```
apt install conntrack
apt install iptstate
```

```
iptstate
```




```
conntrack -L
```

```
root@msk-r01:~# conntrack -L
tcp      6 431911 ESTABLISHED src=10.100.176.7 dst=192.0.2.254 sport=4939 dport=22 src=192.0.2.254 dst=10.100.176.7 sport=22 dport=4939 [ASSURED] mark=0 use=1
icmp     1 29 src=192.0.2.254 dst=95.29.164.26 type=8 code=0 id=2 [UNREPLIED] src=95.29.164.26 dst=192.0.2.254 type=0 code=0 id=2 mark=0 use=1
icmp     1 29 src=10.100.176.7 dst=192.0.2.254 type=8 code=0 id=1 src=192.0.2.254 dst=10.100.176.7 type=0 code=0 id=1 mark=0 use=1
tcp      6 431999 ESTABLISHED src=192.0.2.254 dst=10.100.176.7 sport=22 dport=2579 src=10.100.176.7 dst=192.0.2.254 sport=2579 dport=22 [ASSURED] mark=0 use=1
conntrack v1.4.6 (conntrack-tools): 4 flow entries have been shown.
```

Показывает все активные соединения

Возможно очищать активные соединения

Дополнительные цепочки

Спикер:
Роман Козлов

iptables –n

В ситуации большого количества однотипных правил, возможно оптимизировать прохождение трафика с использованием дополнительных цепочек

Например, при наличии таких правил будет происходить последовательная проверка в том числе и для не TCP трафика:

```
-A FORWARD -i ens4 -o ens3 -p tcp --dport 80 -j ACCEPT
-A FORWARD -i ens4 -o ens3 -p tcp --dport 443 -j ACCEPT
-A FORWARD -i ens4 -o ens3 -p tcp --dport 8080 -j ACCEPT
-A FORWARD -i ens4 -o ens3 -p tcp --dport 993 -j ACCEPT
-A FORWARD -i ens4 -o ens3 -p tcp --dport 995 -j ACCEPT
```

Чтобы избежать этого, можно создать отдельную цепочку с общими условиями – FORWARD входящие и исходящие интерфейсы и tcp

```
iptables -A FORWARD -p tcp -i ens4 -o ens3 -j FWD_TCP_IN_ENS3_OUT_ENS4
```

iptables –n

Изменить цепочку в правилах

```
-A FWD_TCP_IN_ENS3_OUT_ENS4 -p tcp --dport 80 -j ACCEPT
-A FWD_TCP_IN_ENS3_OUT_ENS4 -p tcp --dport 443 -j ACCEPT
-A FWD_TCP_IN_ENS3_OUT_ENS4 -p tcp --dport 8080 -j ACCEPT
-A FWD_TCP_IN_ENS3_OUT_ENS4 -p tcp --dport 993 -j ACCEPT
-A FWD_TCP_IN_ENS3_OUT_ENS4 -p tcp --dport 995 -j ACCEPT
-A FWD_TCP_IN_ENS3_OUT_ENS4 -j RETURN
```

В конце может быть возврат в исходную цепочку или DROP/REJECT

iptables -n

```
iptables -L FWD_TCP_IN_ENS3_OUT_ENS4 -n -v
```

```
root@msk-r01:~# iptables -L FWD_TCP_IN_ENS3_OUT_ENS4 -n -v
Chain FWD_TCP_IN_ENS3_OUT_ENS4 (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:8080
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:993
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:995
    0     0 RETURN     all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

```
iptables -S -t filter
```

```
-A FWD_TCP_IN_ENS3_OUT_ENS4 -p tcp -m tcp --dport 80 -j ACCEPT
-A FWD_TCP_IN_ENS3_OUT_ENS4 -p tcp -m tcp --dport 443 -j ACCEPT
-A FWD_TCP_IN_ENS3_OUT_ENS4 -p tcp -m tcp --dport 8080 -j ACCEPT
-A FWD_TCP_IN_ENS3_OUT_ENS4 -p tcp -m tcp --dport 993 -j ACCEPT
-A FWD_TCP_IN_ENS3_OUT_ENS4 -p tcp -m tcp --dport 995 -j ACCEPT
-A FWD_TCP_IN_ENS3_OUT_ENS4 -j RETURN
```

Работа с адрес-листами

Спикер:
Роман Козлов

ipset

IPSET инструмент для работы с большим количеством IP-адресов и сетевых портов в iptables

Список в специальном формате, который передается iptables при настройке

Для использования входа только с определенных IP можно использовать отдельные цепочки или инструмент ipset

ipset

Установка

```
apt install ipset
```

Создание нового списка

```
ipset -N admin nethash
```

Заполняем список

```
ipset -A admin 192.0.2.254
ipset -A admin 172.30.0.0/16
ipset -A admin 198.51.100.254
ipset -A admin 203.0.113.254
```

Разрешение доступа к SSH только с адрес-листа amin

```
iptables -A INPUT -p tcp -m tcp --dport 22 -m set --match-set admin src -j
ACCEPT
```

ipset

`ipset -L name`

```
root@msk-r01:~# ipset -L admin
Name: admin
Type: hash:net
Revision: 7
Header: family inet hashsize 1024 maxelem 65536 bucketsize 12 initval 0x2a2b9a59
Size in memory: 696
References: 1
Number of entries: 5
Members:
172.30.0.0/16
192.0.0.254
198.51.100.254
203.0.113.254
192.0.2.254
```