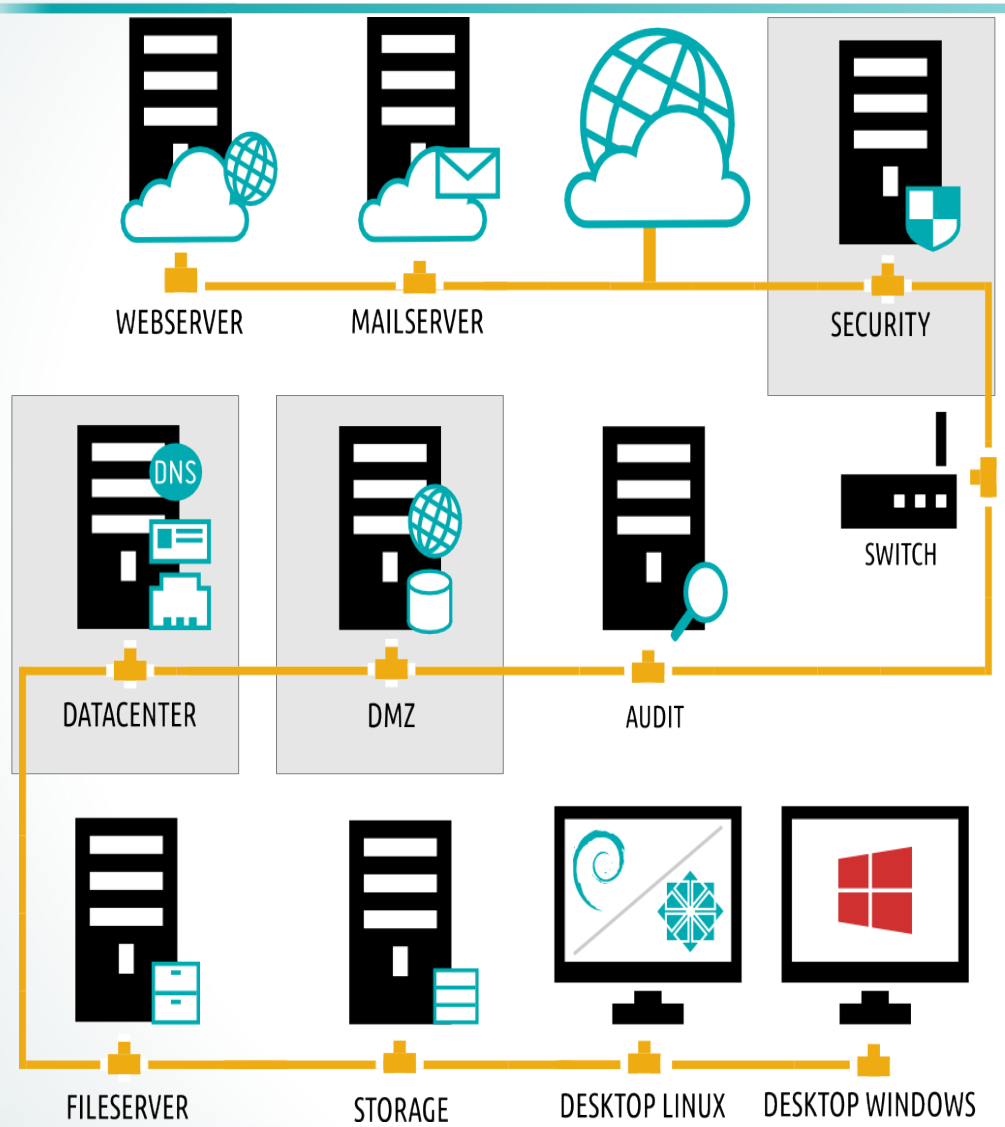

4LINUX
FREE SOFTWARE SOLUTIONS

Só na 4Linux você aprende MUITO MAIS!

Firewall Linux

iT EXPERIENCE



Nesta Aula:

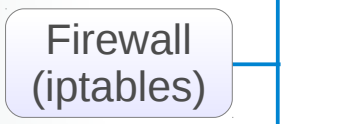
- Security – Local

  Acesso pelo VirtualBox

  SO: Debian Linux

Firewall Linux

- Existem basicamente dois tipos de Firewall:



Firewall de Rede → Conhecido como Firewall de Borda tem a função de Gerenciar todos os pacotes que entram e saem da Rede; (INPUT / OUTPUT / NAT)

Firewall de Host → Configurado localmente em cada servidor sua principal função é gerenciar a troca de pacotes do Host com a Rede Interna ou Externa. (INPUT / OUTPUT)

Firewall Linux

Iptables:

- O iptables é um firewall em nível de pacotes e funciona baseado no endereço/porta de origem/destino do pacote, prioridade;

- Ele funciona através da comparação de regras para saber se um pacote tem ou não permissão para passar;

- Possuí 2 Políticas: ACCEPT ou DROP;

- Possuí 5 tabelas: Filter , Nat, Mangle, Raw e Security;

- Possuí 5 Chains: INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING.

Firewall Linux

- Explorando o Iptables:

```
1# iptables -L  (Padrão: Filter)
2# iptables -L -t filter
3# iptables -L -t nat
4# iptables -L -t mangle
5# iptables -L -t raw
6# iptables -L -t security
```

O comando **iptables** tem a função gerenciar um firewall no Linux. Com ele criamos regras, visualizamos regras, deletamos regras, definimos políticas.

-L → (list) – Listar Regras Ativas

-t → (table) – Define uma das 4 tabela do Iptables (Filter, Nat, Mangle e Raw).

Firewall Linux

Tabelas:

- São os locais usados para armazenar as Chains e Regras de nosso Firewall:

Filter → Regras responsáveis por determinar tudo que entra e sai da máquina local. Muito usada em Firewall de Host;

NAT → Usada para dados que gera outra conexão, como mascarar a Internet, Redirecionar Requisições. Essencial para Firewall de Rede;

Mangle → Utilizada para alterações especiais de pacotes, como marcação para QOS e balanceamento de link;

Firewall Linux

Tabelas:

- Novas Tabelas:

RAW → Marca pacotes para rastreio posterior, utilizada para configurar exeções, o que faz dela importante é ela ficar no topo de todas as outras tabelas, sendo a primeira a processar o pacote;

Security → Usada para regras de rede para Controle Obrigatório de Acesso (MAC - Mandatory Access Control), específica para integração com o SELINUX.

Firewall Linux

Chains:

- As Chains são locais onde as regras são armazenadas de acordo com sua tabela;

```
Filter→ INPUT ,  OUTPUT , FORWARD

NAT   → PREROUTING , POSTROUTING , INPUT , OUTPUT

Mangle→ PREROUTING , POSTROUTING , INPUT , OUTPUT, FORWARD

RAW   →  PREROUTING  , OUTPUT

Security →  INPUT  , OUTPUT, FORWARD
```

As Chains podem ser embutidas ou criadas pelo usuário.

Firewall Linux

Política e Regras:

- Cada Chain possuí uma política padrão que vai determinar que tipo de regras você irá criar na Chain;

Política ACCEPT→ Cria-se regras de Bloqueio de Pacotes;

Política DROP → Cria-se regras de Liberação de Pacotes;

Qual política é mais eficaz?

É mais fácil saber tudo o que precisa ser bloqueado ou tudo que minha empresa precisa que seja liberado?

Firewall Linux

- Definindo Política nas Chains:

```
1# iptables -t filter -S
2# iptables -t nat -S
3# ping 127.0.0.1
4# iptables -t filter -P INPUT DROP
5# iptables -t filter -S
6# iptables -t filter -nL
7# ping 127.0.0.1
```

Política DROP → Tudo está negado exceto o que for liberado em regras de ACCEPT.

Política ACCEPT → Tudo está liberado exceto o que for negado em regras de DROP.

-P → (policy) – Define a Política da Chain

-S → (list-rules) – Lista a Regras de todas as chains ou uma em específico.

Firewall Linux

- Definindo Política nas Chains:

```
1# iptables -t filter -S
2# iptables -t nat -S
3# ping 127.0.0.1
4# iptables -t filter -P INPUT DROP
5# iptables -t filter -S
6# iptables -t filter -nL
7# ping 127.0.0.1
```

Política DROP → Tudo está negado exceto o que for liberado em regras de ACCEPT.

Política ACCEPT → Tudo está liberado exceto o que for negado em regras de DROP.

-P → (policy) – Define a Política da Chain

-S → (list-rules) – Lista a Regras de todas as chains ou uma em específico.

Firewall Linux

- Definindo Regras:

iptables	-t filter -A INPUT	-d 127.0.0.1	-j ACCEPT
	A	B	C

A → Onde a regra será armazenada, ou seja, checada. Sempre indicamos a tabela e a Chain.

B → A regra em si. As informações que passamos na regra são: Origem e Destino do Pacote, Porta do Serviço, Protocolo, etc.

C → A ação da Regra, ou seja, o destino do pacote. Se o pacote será aceito, negado, redirecionado, etc.

Firewall Linux

- Definindo Regras na Tabela Filter

```
1# iptables -t filter -A INPUT -d 127.0.0.1 -j ACCEPT
```

Tudo que entrar no Servidor Security com destino ao Localhost (127.0.0.1) será liberado.

```
2# iptables -t filter -nL

3# iptables -t filter -S INPUT

4# ping 127.0.0.1

5# ping 192.168.X.1

6# iptables -t filter -nL --line-numbers
```

-A → (append) – Adiciona uma regra do Final da lista de Regras já criadas;

-I → (insert) - Adiciona uma regra no começo da lista de Regras já criadas;

-d → (destination) – Específica o destino do Pacote.

Firewall Linux

Sobrevivendo no Iptables

```
1# iptables -t filter -nL --line-numbers
2# iptables -t filter -D INPUT 1
3# iptables -t filter -nL
4# iptables -t filter -A INPUT -j ACCEPT
5# iptables -t filter -nL
6# iptables -t filter -F
7# iptables -t filter -nL
8# iptables -t filter -A INPUT -j ACCEPT
```

-D → (delete) – Deleta uma regra de uma Chain;

-F → (flush) – Deleta todas as regras das Chains de uma tabela;

Firewall Linux

Sobrevivendo no Iptables

```
# iptables-save
# iptables-save > /root/firewall
# iptables -t filter -F
# iptables -t filter -nL
# cat /root/firewall
# iptables-restore /root/firewall
# iptables -t filter -nL
# iptables -t filter -F
```

Todas as regras de firewall são criadas na memória, portanto uma vez que a máquina reinicie tudo é perdido.

O iptables não tem um arquivo de configuração, ele oferece dois comandos para que você posso salvar as regras e ativar na inicialização:

iptables-save → Salva as regras num arquivo.

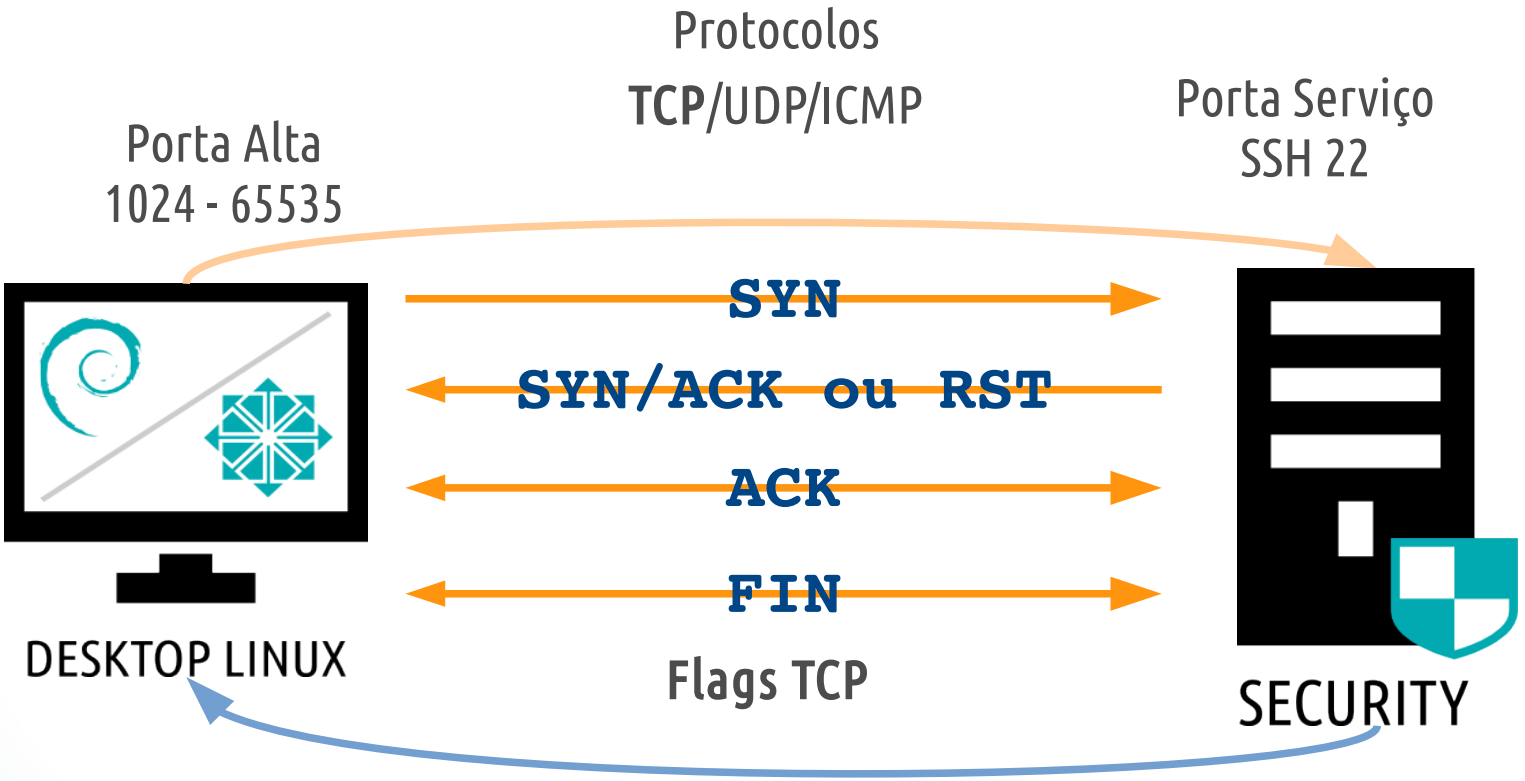
iptables-restore → Ativa as regras armazenadas pelo iptables-save.

Firewall Linux

- Construindo um Firewall:
  - Antes de iniciar a construção de um Firewall é importante dominar alguns conceitos de Rede:
    - Como funciona uma Conexão baseada em Cliente e Servidor;
    - Portas e Protocolos dos Principais Serviços da Rede;

Firewall Linux

Como funciona uma Conexão baseada em Cliente e Servidor?



Firewall Linux

SSH Ativo:

 # tcpdump -n -i eth0 host 192.168.200.35 and port 22

IP 192.168.200.35.62939 > 192.168.200.1.22: **Flags [S]**, seq 1470916950, win 65535

IP 192.168.200.1.22 > 192.168.200.35.62939: **Flags [S.]**, seq 1431520632, ack 1470916951, win 14480

IP 192.168.200.35.62939 > 192.168.200.1.22: **Flags [.]**, **ack** 1, win 65535

IP 192.168.200.35.62939 > 192.168.200.1.22: **Flags [F.]**, seq 1809, ack 1512, win 65535

SSH Desligado:

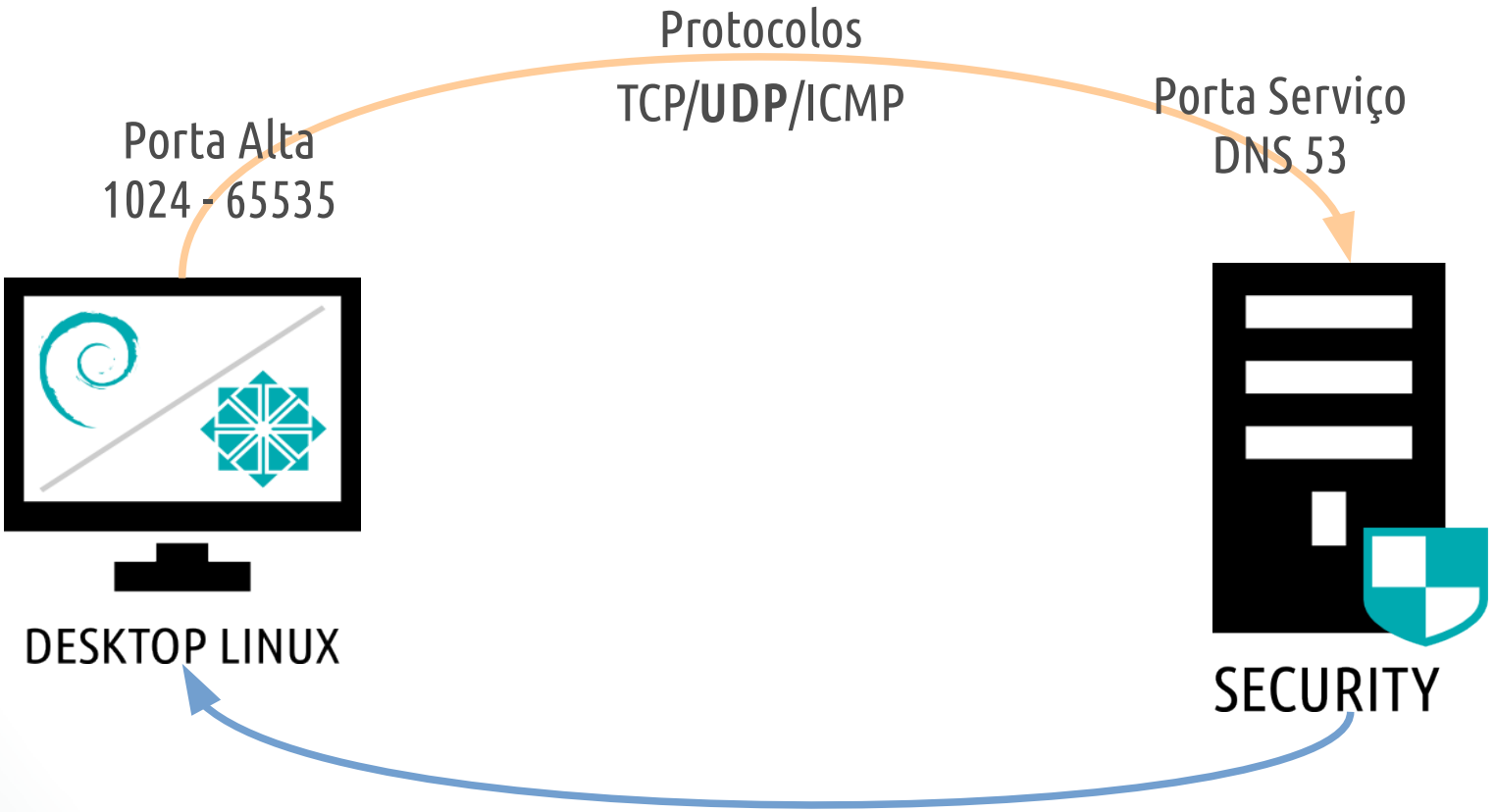
 # tcpdump -n -i eth0 host 192.168.200.35 and port 22

IP 192.168.100.35.62946 > 192.168.100.1.22: **Flags [S]**, seq 2848827145, win 65535, options

IP 192.168.100.1.22 > 192.168.100.35.62946: **Flags [R.]**, seq 0, ack 2848827146, win 0, length 0

Firewall Linux

Como funciona uma Conexão baseada em Cliente e Servidor?



Firewall Linux

DNS Ativo:

 # tcpdump -n -i eth0 port 53

IP 192.168.100.35.57067 > 201.6.2.140.53: 61682+ A? google.com. (28)

IP 201.6.2.140.53 > 192.168.100.35.57067: 61682 11/4/4 A 74.125.234.68, A 74.125.234.72, A 74.125.234.78, A 74.125.234.73, A 74.125.234.66, A 74.125.234.67, A 74.125.234.64, A 74.125.234.71, A 74.125.234.65, A 74.125.234.70, A 74.125.234.69 (340)

DNS Desligado:

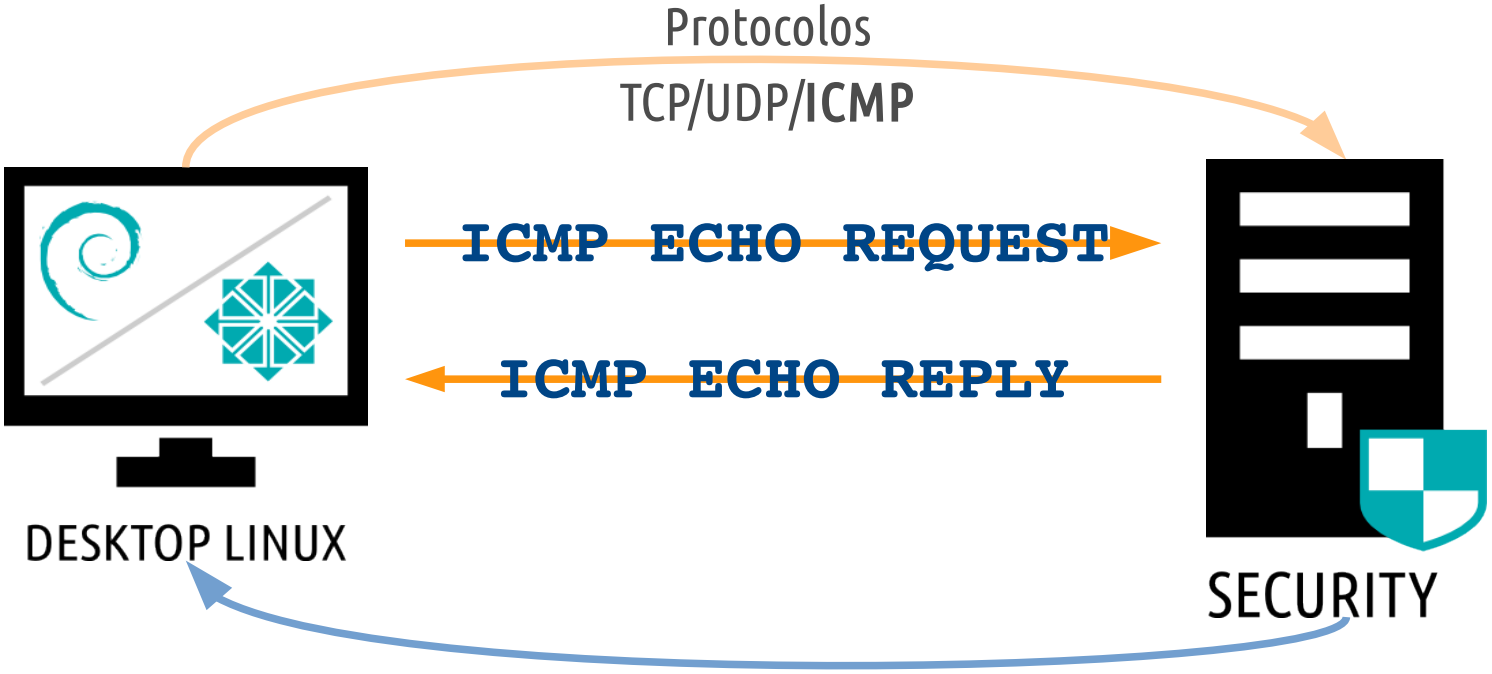
 # tcpdump -n -i eth0 port 53

IP 192.168.100.1.47619 > 66.118.142.41.53: 65307+ A? google.com. (28)

IP 66.118.142.41.53 > 192.168.100.1.47619: 65307 Refused- 0/0/0 (28)

Firewall Linux

Como funciona uma Conexão baseada em Cliente e Servidor?




```
# tcpdump -n -i eth0  icmp
16:01:44.190864 IP 192.168.100.18 > 4.2.2.2: ICMP echo request, id 2721, seq 1, length 64
16:01:44.334131 IP 4.2.2.2 > 192.168.100.18: ICMP echo reply, id 2721, seq 1, length 64
```

Firewall Linux

Portas e Protocolos dos Principais Serviços da Rede:

```
1# cat /etc/services
```

SSH	22/tcp	POP3	110/tcp
HTTP	80/tcp	POP3S	995/tcp
HTTPS	443/tcp	IMAP	143/tcp
DNS	53/udp	IMAPs	993/tcp
SMTP	25/tcp	LDAP	389/tcp
SMTPS	465/tcp	OPENVPN	1194/udp
FTP	21/tcp		

Firewall Linux

- Construindo um Firewall:

1ª → Definir a Política das Chains da Tabela Filter;

```
1# iptables -t filter -P INPUT DROP
2# iptables -t filter -P OUTPUT DROP
3# iptables -t filter -P FORWARD DROP
4# iptables -t filter -nL
5# ping 4.2.2.2
6# ssh 127.0.0.1
```

Firewall Linux

2ª → Liberar acesso ao loopback – 127.0.0.1

```
1# iptables -t filter -A INPUT -d 127.0.0.1 -j ACCEPT
```

Tudo que entrar no Servidor Security com destino ao Localhost (127.0.0.1) será liberado.

```
2# iptables -t filter -A OUTPUT -d 127.0.0.1 -j ACCEPT
```

Tudo que sair do Servidor Security com destino ao Localhost (127.0.0.1) será liberado.

```
3# iptables -t filter -nL --line-numbers

4# ssh 127.0.0.1

5# ping 127.0.0.1
```

Firewall Linux

3ª → Liberar Ping do Firewall para Internet e Rede LAN

```
1# iptables -t filter -A OUTPUT -p icmp -d 0/0 -j ACCEPT
```

Tudo que sair do Servidor Security sendo protocolo ICMP (ping) com destino a qualquer lugar será liberado.

```
2# iptables -t filter -A INPUT -p icmp --icmp-type 0 -s 0/0 -j ACCEPT
```

Tudo que entrar no Servidor Security sendo protocolo ICMP do Tipo 0 (echo reply) vindo de qualquer lugar será liberado.

```
3# iptables -t filter -nL --line-numbers
```

```
4# ping 8.8.8.8
```

Tente da máquina física pingar o Firewall – Não será permitido!

Firewall Linux

4ª → Liberar Consulta DNS a partir do Firewall

```
1# iptables -t filter -A OUTPUT -p udp -s 200.100.50.X  -d 0/0
--dport 53 -j ACCEPT
```

Tudo que sair do Servidor Security sendo protocolo UDP com destino a qualquer lugar na porta 53 (DNS) será liberado.

```
2# iptables -t filter -A INPUT -p udp -s 0/0 --sport 53 -d
200.100.50.X -j ACCEPT
```

Tudo que entrar sendo protocolo UDP vindo de qualquer lugar pela porta 53 no Servidor Security será liberado.

```
3# iptables -t filter -nL --line-numbers
```

```
4# ping google.com
```

Firewall Linux

5ª → Permitir Acesso a Internet pelo Firewall

```
1# iptables -t filter -A OUTPUT -p tcp -m multiport -s 200.100.50.X -d 0/0 --dport 80,443 -j ACCEPT
```

Tudo que sair do Servidor Security sendo protocolo TCP com destino a qualquer lugar nas portas 80 e 443 (http e https) será liberado.

```
2# iptables -t filter -A INPUT -p tcp -m multiport -s 0/0 --sport 80,443 -d 200.100.50.X -j ACCEPT
```

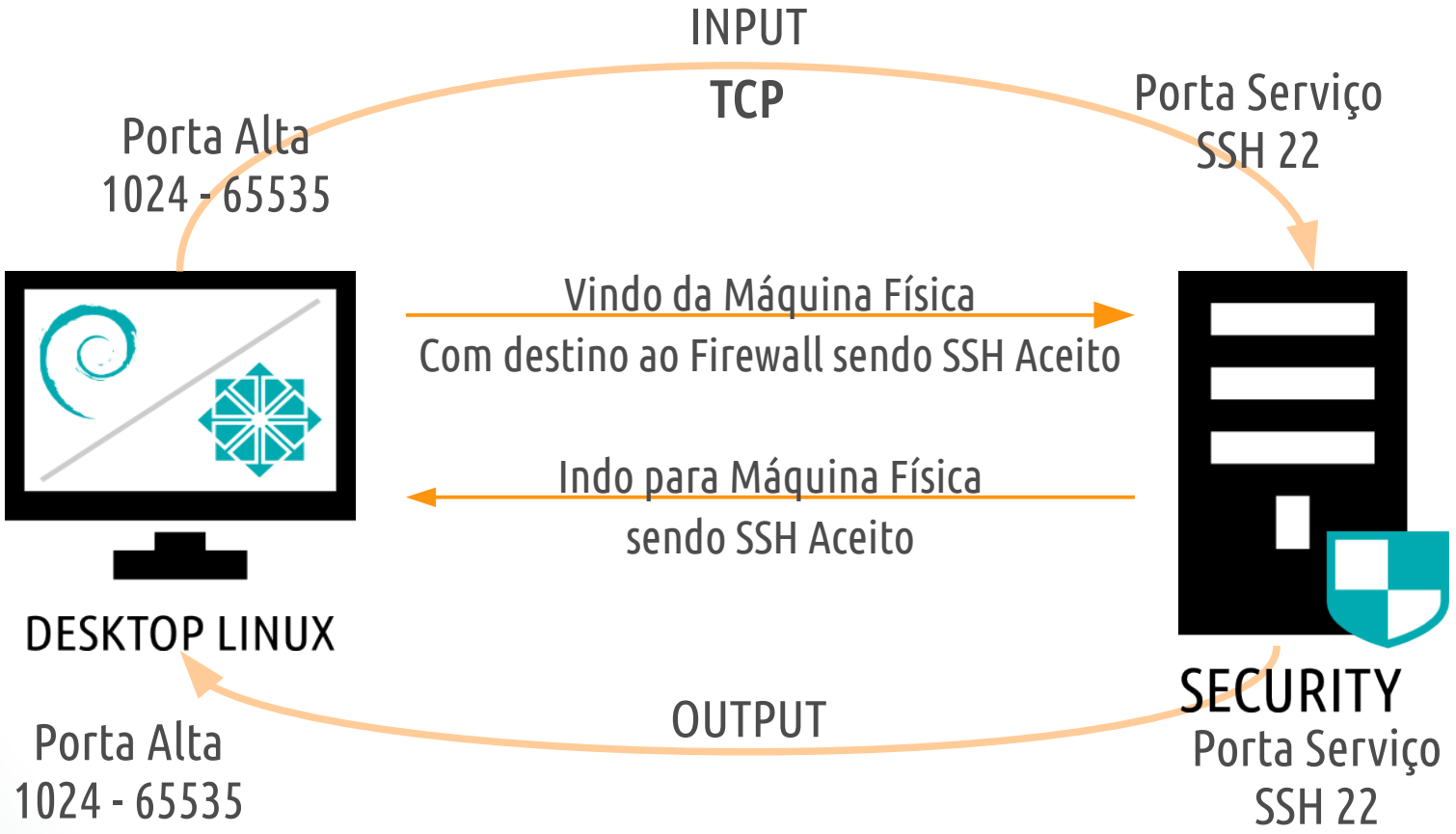
Tudo que entrar sendo protocolo TCP vindo de qualquer lugar pelas portas 80 e 443 no Servidor Security será liberado.

```
3# iptables -t filter -nL --line-numbers
```

```
4# apt-get update
```

Laboratório Dexter

- Libere Acesso SSH da Máquina Física para O Firewall:



Laboratório Dexter

- Libere Acesso SSH da Máquina Física para O Firewall:

```
1# iptables -t filter -A INPUT -p tcp -s 192.168.200.X -d
200.100.50.X --dport 22 -j ACCEPT
```

Tudo que entrar vindo da Máquina Física sendo protocolo TCP com destino ao Servidor Security na porta 22 (SSH) será liberado.

```
2# iptables -t filter -A OUTPUT -p tcp -s 200.100.50.X –sport
22 -d 192.168.200.X -j ACCEPT
```

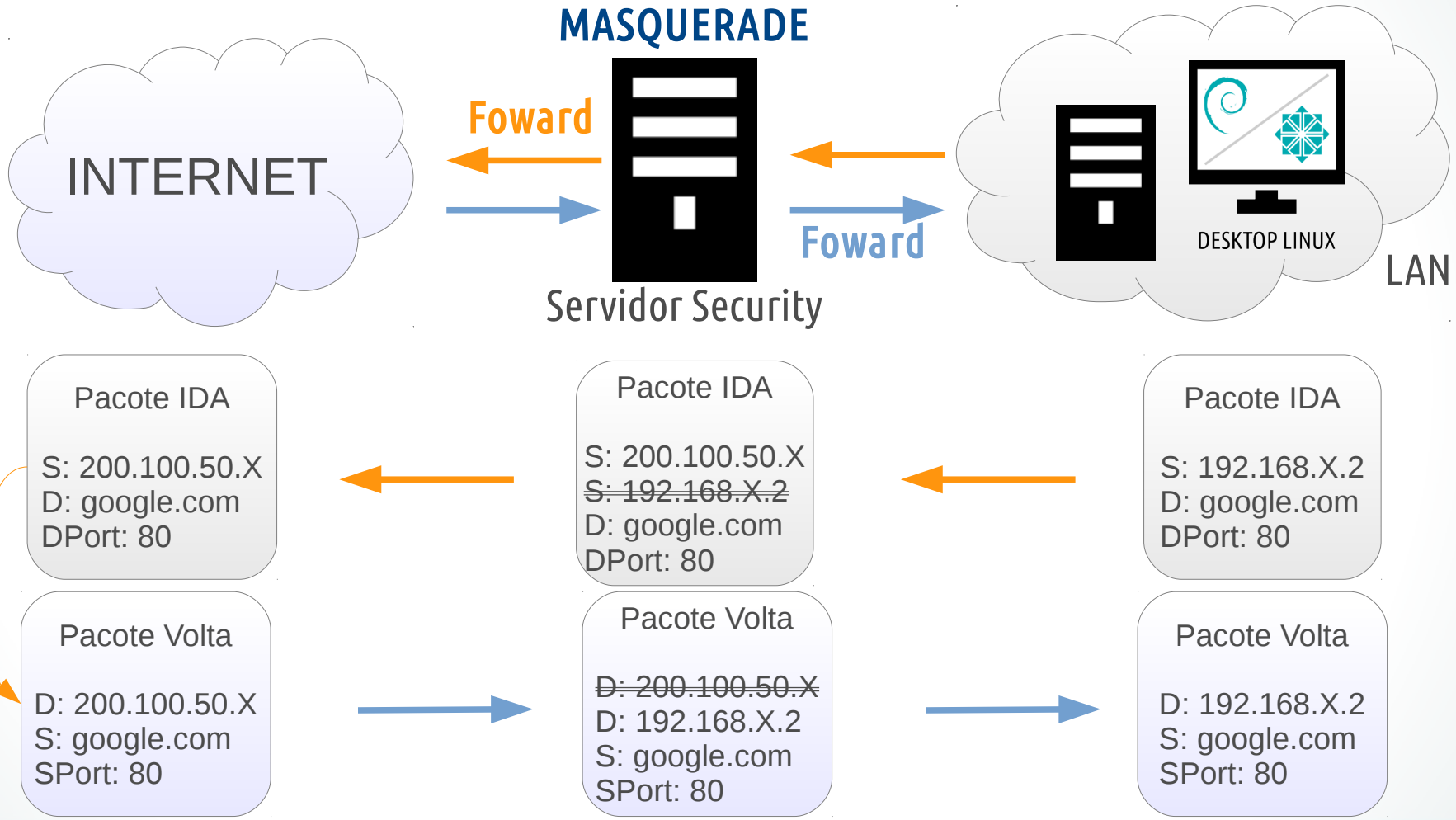
Tudo que sair sendo protocolo TCP saindo do Servidor Security na porta 22 com destino a Máquina Física será liberado.

```
3# iptables -t filter -nL --line-numbers
```

Tente da Máquina Física acessar o Firewall por SSH – Será permitido!

Firewall Linux

Como funciona o Compartilhamento de Internet?



Firewall Linux

- Para trabalhar com MASQUERADE, NAT ou até mesmo roteamento de pacotes por tabela de roteamento é necessário ativar o repasse de pacotes entre placas fisicamente no kernel:

```
1# vim /etc/sysctl.conf
   28 net.ipv4.ip_forward=1
2# sysctl -p
3# cat /proc/sys/net/ipv4/ip_forward
```

Firewall Linux

7ª → Libere Acesso a Internet para as Máquinas da LAN

```
1# iptables -t nat -A POSTROUTING -s 192.168.X.0/24  -d 0/0 -j MASQUERADE
```

Tudo vier da Rede Interna com destino a Internet será MASCARADO

```
2# iptables -t filter -A FORWARD -p tcp -m multiport -s
192.168.X.0/24 -d 0/0 --dport 80,443 -j ACCEPT
```

Tudo que vier da Rede Interna com destino a Internet nas portas 80 443 eu permito o repasse de pacotes

```
3# iptables -t filter -A FORWARD -p tcp -m multiport -s 0/0
--sport 80,443 -d 192.168.X.0/24  -j ACCEPT
```

Tudo que vier da Internet nas portas 80 e 443 com destino a Rede Interna eu permito o repasse de pacotes

Firewall Linux

8ª → Libere Acesso a Consulta DNS para as Máquinas da LAN

```
1# iptables -t filter -A FORWARD -p udp -s 192.168.X.0/24 -d 0/0
--dport 53 -j ACCEPT
```

Tudo que vier da Rede Interna com destino a Internet na porta 53 eu permito o repasse de pacotes

```
2# iptables -t filter -A FORWARD -p udp -s 0/0 --sport 53 -d
192.168.X.0/24 -j ACCEPT
```

Tudo que vier da Internet na porta 53 com destino a Rede Interna eu permito o repasse de pacotes

Tente do Servidor DataCenter acessar a Internet – Será permitido!

Laboratório Dexter

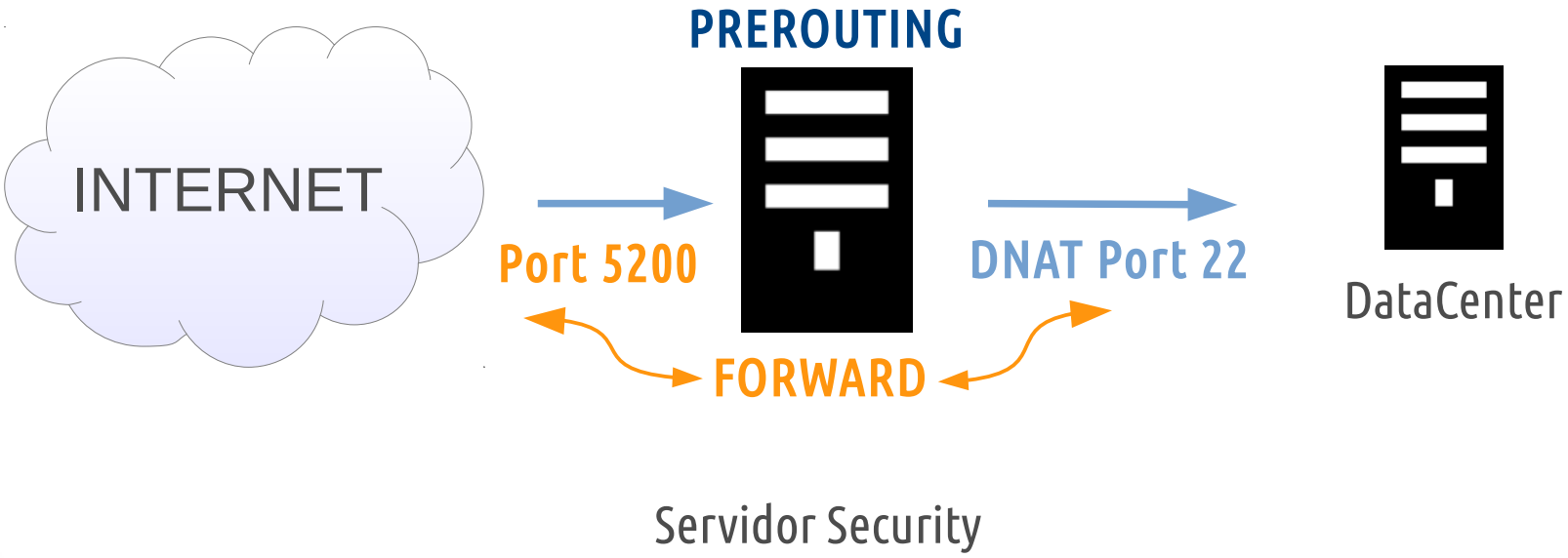
- Libere Repasse de Pacotes para os Serviços mais comuns para a Rede Interna:

```
for PORT in  80 443 25 110 143 993 995 21 20

do

   iptables -A FORWARD -p tcp -s 192.168.X.0/24  --sport
1024:65535  -d 0/0 --dport $PORT -j ACCEPT

 iptables -A FORWARD -p tcp  -s 0/0 --sport $PORT -d
192.168.X.0/24 --dport 1024:65535 -j ACCEPT

done
```

Tente do Servidor DataCenter validar as regras acima!

Firewall Linux

Como funciona o Redirecionamento de Portas?



Firewall Linux

10ª → Redirecione o Serviço SSH para os Servidores Internos

Porta 52000 → Servidor DataCenter → Porta 22

Porta 53000 → Servidor DMZ → Porta 22

Porta 54000 → Servidor Audit → Porta 22

Porta 55000 → Servidor FileServer → Porta 22

Porta 56000 → Servidor Storage → Porta 22

Firewall Linux

10ª → Redirecione o Serviço SSH para os Servidores Internos

```
1# iptables -t nat -A PREROUTING -p tcp -s 0/0 -d 200.100.50.X
--dport 52000 -j DNAT --to 192.168.X.2:22
```

Tudo que vier da Internet com destino ao Servidor Security na porta 52000 será redirecionado ao Servidor DataCenter na porta 22

```
2# iptables -t filter -A FORWARD -p tcp -s 0/0 -d 192.168.X.2
--dport 22 -j ACCEPT
```

Tudo que vier da Internet com destino ao DataCenter na porta 22 eu permito o repasse de pacotes

```
3# iptables -t filter -A FORWARD -p tcp -s 192.168.X.2 --sport
22 -d 0/0 -j ACCEPT
```

Laboratório Dexter

- Conclua a Regra de Redirecionamento do SSH para os Servidores da Dexter:

```
for SERVER in  2 3 4 5 6
do
iptables -t nat -A PREROUTING -p tcp -s 0/0 -d 200.100.50.X
--dport 5$SERVER'000' -j DNAT --to 192.168.X.$SERVER:22
iptables -t filter -A FORWARD -p tcp -s 0/0 -d 192.168.X.
$SERVER --dport 22 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -s 192.168.X.$SERVER
--sport 22 -d 0/0 -j ACCEPT
done
```

Pergunta LPI

Você implementou algumas regras de Firewall, e o próprio Firewall está saindo para a internet, porém qualquer máquina atrás do firewall não consegue conectar. Qual deve ser o problema?

A. Os usuários são ingênuos, precisa mostrar como se faz.

B. A política da Chain OUTPUT é DROP, precisa ser ACCEPT para deixar o tráfego de saída chegar ao host.

C. Encaminhamento de IP está desativado no / proc/sys/net/ipv4.

D. Se o firewall pode se conectar à Internet, os sistemas por trás dele estão OK. O problema deve ser em outro lugar.

Pergunta LPI

Você implementou algumas regras de Firewall, e o próprio Firewall está saindo para a internet, porém qualquer máquina atrás do firewall não consegue conectar. Qual deve ser o problema?

A. Os usuários são ingênuos, precisa mostrar como se faz.

B. A política da Chain OUTPUT é DROP, precisa ser ACCEPT para deixar o tráfego de saída chegar ao host.

C. Encaminhamento de IP está desativado no / proc/sys/net/ipv4.

D. Se o firewall pode se conectar à Internet, os sistemas por trás dele estão OK. O problema deve ser em outro lugar.

Resposta: C


4LINUX
FREE SOFTWARE SOLUTIONS