

Este material é parte integrante do curso de FIREWALL do prof. Uirá Ribeiro e é protegido por direitos autorais e não pode ser copiado, distribuído em parte ou ao todo sem a expressa autorização do autor.

Tabela Nat

1. 06_tabela_nat

1.1 Tabela Nat



Este material é parte integrante do curso de FIREWALL do prof. Uirá Ribeiro e é protegido por direitos autorais e não pode ser copiado, distribuído em parte ou ao todo sem a expressa autorização do autor.

1.2 Agenda da Aula

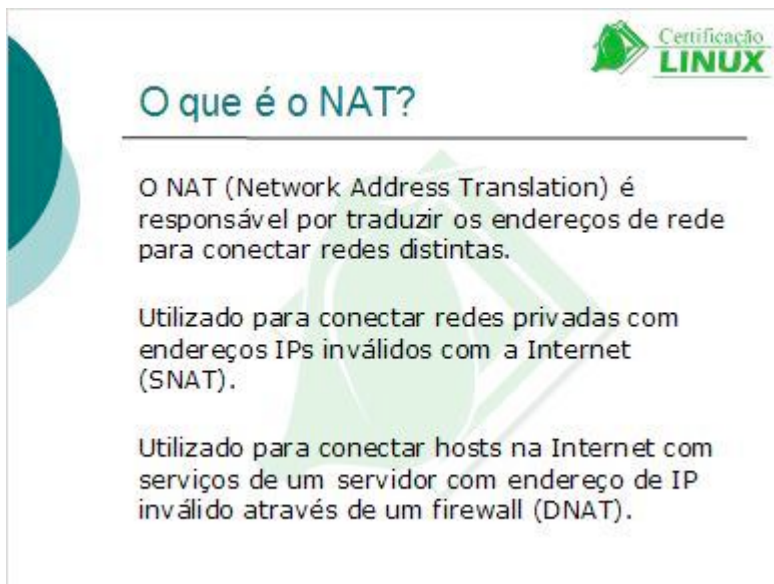


The slide features a teal circular graphic on the left and a green Linux logo in the top right corner. The title 'Agenda da Aula' is centered at the top. Below it, on the left, is a red circular logo with a white 'L' and the text 'Linux fundamentais' underneath. To the right of this logo is a bulleted list item.

Agenda da Aula

- Como alterar os pacotes para interligar redes distintas

1.3 O que é o nat



The slide features a teal circular graphic on the left and a green Linux logo in the top right corner. The title 'O que é o NAT?' is centered at the top. Below the title, there are three paragraphs of text explaining NAT.

O que é o NAT?

O NAT (Network Address Translation) é responsável por traduzir os endereços de rede para conectar redes distintas.

Utilizado para conectar redes privadas com endereços IPs inválidos com a Internet (SNAT).

Utilizado para conectar hosts na Internet com serviços de um servidor com endereço de IP inválido através de um firewall (DNAT).

Este material é parte integrante do curso de FIREWALL do prof. Uirá Ribeiro e é protegido por direitos autorais e não pode ser copiado, distribuído em parte ou ao todo sem a expressa autorização do autor.

1.4 Redes privadas




Redes privadas

Devido à escassez de endereços IPs válidos, as redes privadas fazem uso de faixas de endereços consideradas inválidas, que não podem ser roteados na Internet.

Essas faixas de IPs são:

- 192.168.0.0/16
- 10.0.0.0/8
- 172.16.0.0/12

1.5 Nat




Nat

O papel principal do NAT é fazer uma tradução dos IPs de redes privadas para endereços válidos (caso mais comum).

Desta forma o netfilter altera o IP de origem ou destino no cabeçalho dos pacotes para que as redes privadas possam se conectar com a Internet e vice-versa.

Este material é parte integrante do curso de FIREWALL do prof. Uirá Ribeiro e é protegido por direitos autorais e não pode ser copiado, distribuído em parte ou ao todo sem a expressa autorização do autor.

1.6 *Ip conntrack*




Ip conntrack

Para conseguir fazer essa tradução de endereços, o Kernel mantém uma tabela chamada `ip_conntrack` com os detalhes de cada conexão em:

```
/proc/net/ip_conntrack
```

Esse registro possibilita que o netfilter controle as traduções de endereços.

1.7 *Tipos de tradução*




Tipos de tradução

O nat pode trabalhar de 4 maneiras diferentes

- 1:1 - um IP privado é traduzido para um IP público.
- 1:N - um IP privado é traduzido para vários IPs públicos. Utilizado quando existe várias conexões para um host com IP privado.
- N:1 - vários IPs privados são traduzidos para 1 IP público.
- N:N - muitos IPs privados são traduzidos para muitos IPs públicos.

Este material é parte integrante do curso de FIREWALL do prof. Uirá Ribeiro e é protegido por direitos autorais e não pode ser copiado, distribuído em parte ou ao todo sem a expressa autorização do autor.

1.8 Chains do nat




Chains do nat

Na tabela nat podem ser utilizadas 3 chains:

- PREROUTING - "pega" os pacotes antes deles serem roteados.
- POSTROUTING - "pega" os pacotes após serem roteados.
- OUTPUT - "pega" os pacotes que saem dos processos locais do firewall.

1.9 Ações do nat




Ações do nat

Os pacotes da tabela nat podem sofrer 4 ações possíveis:

- DNAT - destination nat. Utilizado para alterar o IP de destino dos cabeçalhos dos pacotes.
- SNAT - source nat. Utilizado para alterar o IP de origem dos cabeçalhos dos pacotes.
- MASQUERADE - Utilizado para mascarar as conexões. Geralmente usado para IPs dinâmicos.
- REDIRECT - Utilizado para redirecionar portas em um mesmo host.

Este material é parte integrante do curso de FIREWALL do prof. Uirá Ribeiro e é protegido por direitos autorais e não pode ser copiado, distribuído em parte ou ao todo sem a expressa autorização do autor.

1.10 SNAT




SNAT

O SNAT geralmente é utilizado para alterar os endereços de origem dos pacotes para dar acesso à Internet aos hosts de uma rede privada.

- A chain do SNAT é a POSTROUTING.

1.11 Ip Forward



Ip Forward


Para fazer uso do nat é preciso habilitar o recurso de encaminhamento de pacotes do Kernel.

Para isto, é preciso alterar o arquivo `/proc/sys/net/ipv4/ip_forward`:

```
echo 1> /proc/sys/net/ipv4/ip_forward
```


Este material é parte integrante do curso de FIREWALL do prof. Uirá Ribeiro e é protegido por direitos autorais e não pode ser copiado, distribuído em parte ou ao todo sem a expressa autorização do autor.

1.12 Ip Forward




Ip Forward

É importante saber que o `ip_forward` precisa ser colocado no arquivo `/etc/sysctl.conf` para que a configuração fique permanente após o reinício do firewall adicionando a seguinte linha:

```
net.ipv4.ip_forward = 1
```

1.13 Compartilhar Internet para um host




Compartilhar Internet para um host

Para compartilhar a Internet para um host apenas (1:1) utilizando um IP válido fixo:


```
iptables -t nat -A POSTROUTING -s 192.168.0.20 -d 0/0 -j SNAT --to 200.251.153.57
```

Este material é parte integrante do curso de FIREWALL do prof. Uirá Ribeiro e é protegido por direitos autorais e não pode ser copiado, distribuído em parte ou ao todo sem a expressa autorização do autor.

1.14 Compartilhar Internet para




Compartilhar Internet para uma rede




Para compartilhar a Internet para uma rede apenas (N:1) utilizando um IP válido fixo:

```
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j SNAT --to 200.251.153.58
```

1.15 Compartilhar Internet para



Compartilhar Internet para uma rede usando vários IPs válidos




Para compartilhar a Internet para uma rede apenas (N:N) utilizando mais de um IP válido fixo:

```
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j SNAT --to 200.251.153.57-200.251.153.60
```


Este material é parte integrante do curso de FIREWALL do prof. Uirá Ribeiro e é protegido por direitos autorais e não pode ser copiado, distribuído em parte ou ao todo sem a expressa autorização do autor.

1.16 Conectando redes privadas




Conectando redes privadas

O netfilter pode ser utilizado para conectar redes privadas:

```
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j SNAT --to 172.19.0.1
```

1.17 Masquerading




Masquerading

O masquerade é uma situação especial do SNAT em que os IPs válidos são dinâmicos, utilizados em conexões ppp, ADSL, cabo, GSM, etc.

Da mesma forma que o SNAT, o Masquerading precisa do ip_forward habilitado.

Este material é parte integrante do curso de FIREWALL do prof. Uirá Ribeiro e é protegido por direitos autorais e não pode ser copiado, distribuído em parte ou ao todo sem a expressa autorização do autor.

1.18 Masquerading




Masquerading

Para habilitar o compartilhamento da conexão ppp com toda a rede interna:

```
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o ppp0 -j MASQUERADE
```

1.19 Masquerading



Masquerading


Você pode especificar protocolos e serviços que serão compartilhados:

```
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -p tcp --dport 80 -j MASQUERADE
```

Acima, somente a porta 80 será liberada.

Este material é parte integrante do curso de FIREWALL do prof. Uirá Ribeiro e é protegido por direitos autorais e não pode ser copiado, distribuído em parte ou ao todo sem a expressa autorização do autor.

1.20 DNAT




DNAT

O DNAT é responsável por trocar os endereços de destino dos pacotes. É utilizado para prover acesso à aplicações e serviços da Internet para algum host na rede interna com IP inválido.

O DNAT usa a chain PREROUTING.

1.21 DNAT



DNAT

Neste exemplo toda conexão proveniente da Internet para a porta 80 será enviada para um webserver:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 192.168.0.15
```

Este material é parte integrante do curso de FIREWALL do prof. Uirá Ribeiro e é protegido por direitos autorais e não pode ser copiado, distribuído em parte ou ao todo sem a expressa autorização do autor.

1.22 DNAT para balanceamento




DNAT para balanceamento

O DNAT pode ser usado para balancear a carga entre dois ou mais servidores.

Imagine o cenário com 3 servidores web com IPs 192.168.0.2, 192.168.0.3 e 192.168.0.4.

No DNS apenas um IP válido será usado para acessar os 3 servidores através de um firewall: 200.123.123.123

1.23 DNAT




DNAT

No exemplo o IP 200.123.123.123 está configurado na eth0. Para fazer o load balance entre os 3 servidores:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 192.168.0.2-192.168.0.4
```

Este material é parte integrante do curso de FIREWALL do prof. Uirá Ribeiro e é protegido por direitos autorais e não pode ser copiado, distribuído em parte ou ao todo sem a expressa autorização do autor.

1.24 DNAT




DNAT

E para que a rede interna possa acessar o servidor web, é necessário fazer um DNAT adicional

```
iptables -t nat -A OUTPUT -d 200.123.123.123 -p tcp --dport 80 -j DNAT --to 192.168.0.2-192.168.0.4
```

1.25 REDIRECT




REDIRECT

O REDIRECT é utilizado para redirecionar os pacotes de uma porta para outra porta em um mesmo host.

Geralmente utilizado para redirecionar as conexões para um servidor proxy, como o squid.

Este material é parte integrante do curso de FIREWALL do prof. Uirá Ribeiro e é protegido por direitos autorais e não pode ser copiado, distribuído em parte ou ao todo sem a expressa autorização do autor.

1.26 REDIRECT




REDIRECT

Neste exemplo, todas as conexões para a porta 80 serão direcionadas para a porta 3128 do squid:

```
iptables -t nat -A PREROUTING -s 192.168.0.0/24 -p tcp --dport 80 -j REDIRECT --to-port 3128
```

1.27 REDIRECT

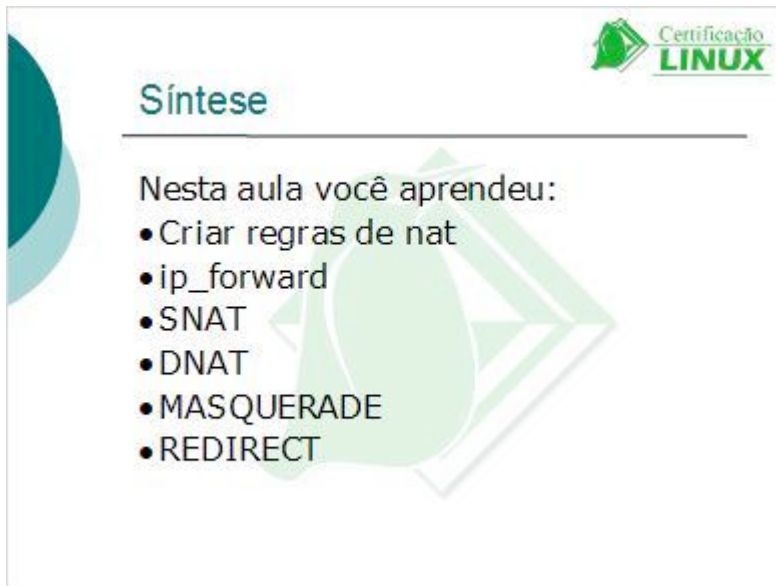


REDIRECT

Veja que o REDIRECT para um proxy squid só pode ser usado quando ele está em modo transparente, sem autenticação de usuários.

Este material é parte integrante do curso de FIREWALL do prof. Uirá Ribeiro e é protegido por direitos autorais e não pode ser copiado, distribuído em parte ou ao todo sem a expressa autorização do autor.

1.28 Síntese



The slide features a teal circular graphic on the left and a large, faint green Linux logo in the background. The title 'Síntese' is underlined. The text 'Nesta aula você aprendeu:' is followed by a bulleted list of topics.

Síntese

Nesta aula você aprendeu:

- Criar regras de nat
- ip_forward
- SNAT
- DNAT
- MASQUERADE
- REDIRECT