**Entendendo IPTABLES

PREROUTING e POSTROUTING**

Quando o assunto é firewall logo se pensa em usar um Linux com iptables. O que não falta são tutoriais pela Internet que ensinam como instalar e configurar um firewall no Linux usando o iptables. Infelizmente muita gente se confunde quando o assunto é a chain PREROUTING e POSTROUTING da tabela NAT do Netfilter.

A proposta deste post é justamente explicar o que acontece com o pacote quando passa por uma dessas chains.

A figura abaixo mostra a estrutura interna de um firewall **Netfilter / Iptables**:



***PREROUTING***

Logo que o pacote chega ele é modificado, isso acontece antes do roteamento do pacote, isto é, antes do pacote ser entregue a uma máquina destino interna. É usado em regras de DNAT e Redirecionamento de porta.

Vamos analisar o cenário abaixo, onde estamos fazendo um DNAT, ou seja, toda requisição feita para o IP 200.164.30.20 na porta 80 será repassado para o IP da rede interna 192.168.2.100.



A requisição vem da Internet com destino 200.164.30.20:80.

No nosso firewall a porta 80 esta desabilitada, neste caso o pacote seria “dropado”, mas como temos essa regra de IPTABLES:

iptables -t nat -A PREROUTING -d 200.164.30.20 -p tcp --dport 80 -j DNAT --to 192.168.2.100

Neste caso todo pacote com destino 200.164.30.20:80 será repassado para 192.168.2.100:80, porém isso acontece antes de qualquer roteamento. Veja a figura abaixo que mostra o que acontece logo que o pacote chega no firewall:



Como o nosso firewall conhece a rede 192.168.2.0/24 o pacote será repassado para o IP 192.168.2.100 na porta 80. Note que o roteamento foi o último procedimento realizado. Neste caso não seria lógico realizar o roteamento primeiro já que o DST possui o mesmo IP do firewall (200.164.30.20).

***POSTROUTING***

Os pacotes precisam ser modificados após o roteamento. É usado em regras de SNAT e IP MASQUERADING.

Neste post vou usar o MASQUERADING para explicar como funciona o POSTROUTING.

Segue abaixo a descrição tirada do FOCALINUX do que seria o MASQUERADING:

“O IP Masquerading é um tipo especial de SNAT usado para conectar a sua rede interna a internet quando você recebe um IP dinâmico de seu provedor”.

Veja o cenário abaixo:



A máquina 192.168.2.100 pretende acessar a INTERNET, mas para isso é preciso ter uma regra de MASQUERADING no Firewall, onde o mesmo mascara todo acesso da máquina de origem para que saia para a Internet com o IP do próprio Firewall. A regra do iptables seria assim:

iptables -t nat -A POSTROUTING -s 192.168.2.100 -o eth0 -j MASQUERADE

A requisição vem de uma máquina interna da rede (192.168.2.100) com destino (dst) [www.google.com](http://www.google.com/).

Veja a figura abaixo que mostra o que acontece logo que o pacote chega no firewall:



Quando o pacote chegar no Firewall vai ser repassado para o Gateway padrão do Firewall que está configurado na placa de rede com saída para a Internet. No segundo momento, logo depois do roteamento, o pacote bate na chain POSTROUTING da nossa regra de iptables e o mesmo é modificado para que possa navegar na Internet com um IP válido, no nosso caso o IP do Firewall (200.164.30.20).

É fundamental entender o fluxo do pacote quando o mesmo passa pelo Netfilter. Postrouting e Prerouting são chains que poucos entendem. Espero que com este post as dúvidas possam ter sido esclarecidas sobre o assunto.