Firewall
Tipos de NAT:
NAT – Serve para controlar a tradução de endereços das maquinas que atravessam o roteamento Linux, A tradução de endereços tem inúmeras utilidades, uma delas é o Masquerading, onde máquinas de uma rede interna podem acessar a Internet através de uma máquina Linux, redirecionamento de porta, proxy transparente, etc. Esta seção abordará os tipos de NAT, exemplos de como criar rapidamente uma conexão IP masquerading e entender como a tradução de endereços funciona no iptables.

SNAT – Aplicada quando queremos alterar o endereço de origem do pacote. Aqui nós utilizamos para fazer o mascaramento. OBS: Somente a Chain POSTROUTING pode ser usada na ação SNAT.

DNAT – Aplicada quando desejamos alterar o endereço de destino do pacote. Esta ação é utilizada para fazer redirecionamento de portas, redirecionamento de servidor, load balance e proxy.

Na Prática para criar uma regra de Firewall:
Ativar o roteamento

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

Verificar se a Distro Linux está com o iptables ativo ou possui o modulo iptables.
#modprobe iptables
Criar um script de firewall e dar permissão de execução
#vim firewall.sh
#chmod +x firewall.sh
Após inserir todas as regras rodar o script
#./firewall.sh
Liberar acesso da interface para receber ping
`iptables -A INPUT -i XXX -p icmp -j ACCEPT onde XXX é a interface`
Liberar acesso a uma porta
iptables -I INPUT -i eth1 -p tcp -s 0/0 --dport XX -j ACCEPT onde XX é a porta
Redirecionamento de IP com portas
iptables -t nat -A PREROUTING -s 0/0 -p tcp -ZZZ.ZZZ.ZZZ.ZZZ--dport YYY -j DNAT --to XXX.XXX.XXX.XXX