Firewall

O que é um Firewall:

É uma barreira inteligente entre duas redes, sendo que só trafegam nessas redes o tráfego autorizado pelo firewall. Esse tráfego autorizado é examinado em tempo real sendo que a seleção dele é feita conforme a política do firewall.

Existem basicamente dois tipos de firewalls:

- => Nível de aplicação - Este tipo de firewall analisam o conteúdo do pacote para tomar suas decisões de filtragem. Firewalls deste tipo são mais intrusivos (pois analisam o conteúdo de tudo que passa por ele) e permitem um controle relacionado com o conteúdo do tráfego. Alguns firewalls em nível de aplicação combinam recursos básicos existentes em firewalls em nível de pacotes combinando as funcionalidade de controle de tráfego/controle de acesso em uma só ferramenta. Servidores proxy, como o squid, são um exemplo deste tipo de firewall.
- => Nível de pacotes - Este tipo de firewall toma as decisões baseadas nos parâmetros do pacote, como porta/endereço de origem/destino, estado da conexão, e outros parâmetros do pacote. O firewall então pode negar o pacote (DROP) ou deixar o pacote passar (ACCEPT). O iptables é um excelente firewall que se encaixa nesta categoria.

Na configuração do Firewall utilizaremos o Iptables. O iptables suporta vários protocolos sendo que no seu pacote mais recente o ip6tables traz suporte ao IPv6, sendo que é uma maneira de configuração muito estável, fácil de administrar, pode ser feita através de scripts e confiável.

Características do IPTABLES:

.: Suporte aos protocolos TCP, UDP, ICMP

.: Pode se especificar portas de endereço e de destino.

.: Suporta módulos externos como FTP e IRC

.: Suporta um número ilimitado de regras por CHAINS (correntes).

.: Pode se criar regras de proteção contra ataques diversos

.: Suporte para roteamento de pacotes e redirecionamento de portas.

.: Suporta vários tipos de NAT, como o SNAT e DNAT e mascaramento.

.: Pode priorizar tráfego para determinados tipos de pacotes.

Para configurar o iptables, precisamos saber das regras e das políticas.

Regras do Firewall

TABELAS DO IPTABLES

- *fil*ter - Esta é a tabela padrão, contém 3 chains padrões:
-
    - INPUT - Consultado para dados que chegam a máquina
    - OUTPUT - Consultado para dados que saem da máquina
    - FORWARD - Consultado para dados que são redirecionados para outra interface de rede ou outra máquina.

  Os chains *INPUT* e *OUTPUT* somente são atravessados por conexões indo/se originando de localhost.

  OBS: Para conexões locais, somente os chains *INPUT* e *OUTPUT* são consultados na tabela filter.
-
- nat - Usada para dados que geram outra conexão (masquerading, source nat, destination nat, port forwarding, proxy transparente são alguns exemplos). Possui 3 chains padrões:
-
    - PREROUTING - Consultado quando os pacotes precisam ser modificados logo que chegam. É o chain ideal para realização de DNAT e redirecionamento de portas .
    - OUTPUT - Consultado quando os pacotes gerados localmente precisam ser modificados antes de serem roteados. Este chain somente é consultado para conexões que se originam de IPs de interfaces locais.
    - POSTROUTING - Consultado quando os pacotes precisam ser modificados após o tratamento de roteamento. É o chain ideal para realização de SNAT e IP Masquerading .
-
- mangle - Utilizada para alterações especiais de pacotes (como modificar o tipo de serviço (TOS) ou outros detalhes que serão explicados no decorrer do capítulo. Possui 5 chains padrões:
-
    - INPUT - Consultado quando os pacotes precisam ser modificados antes de serem enviados para o chain *INPUT* da tabela *filter*.
    - FORWARD - Consultado quando os pacotes precisam ser modificados antes de serem enviados para o chain *FORWARD* da tabela *filter*.
    - PREROUTING - Consultado quando os pacotes precisam ser modificados antes de ser enviados para o chain *PREROUTING* da tabela *nat*.
    - POSTROUTING - Consultado quando os pacotes precisam ser modificados antes de serem enviados para o chain *POSTROUTING* da tabela *nat*.
    - OUTPUT - Consultado quando os pacotes precisam ser modificados antes de serem enviados para o chain *OUTPUT* da tabela *nat*.

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.

NAT – 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.

Basicamente o IPTABLES tem as seguintes políticas:

- DROP: Nega pacote e não manda um pacote de volta para o emitente.

- ACCEPT: Aceita o pacote

- REJECT: Nega pacote e manda um pacote de volta do tipo host-unreachable (Host Inalcançável)

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