1. 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.

2. Cite os tipos de firewall e explique.
Existem basicamente dois tipos de firewalls:

- => Nível de aplicação - Este tipo de firewall analisam o conteúdo do pacote para tomar suas decisões de filtragem. 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.
-

3. Sobre as características do iptables assinale a alternativa incorreta:

Letra d

4. Quais são os chains padrões e o que são? Fale o funcionamento de cada um. (Correção não foi especificado mas só os chains padrões da tabela Filter já era a resposta esperada)

Na tabela filter, há 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.

Na tabela NAT, há, também, 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 .

-

Na tabela mangle, há 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*.

5. Explique os tipos de NAT.

Tipos de NAT:

NAT – Serve para controlar a tradução de endereços das maquinas que atravessam o roteamento Linux.

SNAT – Aplicada quando queremos alterar o endereço de origem do pacote.

Aqui nós utilizamos para fazer o mascaramento.

DNAT – Aplicada quando desejamos alterar o endereço de destino do pacote.