Segundo a Cisco, um firewall é um dispositivo de segurança da rede que monitora o tráfego dela e, de acordo com as regras definidas, decide permitir ou bloquear tráfegos específicos. Ele pode ser um hardware, software ou ambos.

Statefull X Stateless: Em uma regra Statefull, os dispositivos da intranet podem iniciar comunicação externa com qualquer servidor que não foi previamente bloqueado, após iniciada a comunicação e verificadas as regras do firewall, ele mantem informações a respeito dela em uma tabela, que será usada para permitir o retorno das informações vindas dos servidores externos. A regra Statefull não permite que um servidor externo comunique com um interno sem que a mesma esteja associada a um pacote na tabela de informações. Um dos problemas da regra é permitir que um dispositivo interno se comunique com qualquer dispositivo externo, e se a resposta estiver de acordo com o especificado no pacote que iniciou a comunicação, ele aceita o retorno, mesmo que seja de um servidor malicioso. Já na regra Stateless, não existe uma tabela para relacionar a comunicação externa com a interna, é tudo considerado novo. Existem regras para definir quais servidores externos podem se comunicar com os internos. O problema é que aceita a comunicação de ambos os lados, o que permite serviços externos iniciarem a comunicação, mesmo que ela não tenha sido solicitada.

Políticas(regras) de Firewall: Definem permissão ou negação de serviço, as regras são compostas por origem (quem vai iniciar a comunicação), destino (Com quem a origem vai se comunicar) e serviço/porta (tipo de conexão a ser realizada). No geral, não é viável liberar destino por destino, então a liberação é feita para todos, e é criada outra regra bloqueando os destinos que não devem ser acessados.

O firewall lê as regras top-down, até encontrar a regra que se aplica a comunicação atual. Então caso a primeira regra bloqueie um determinado servidor, e a segunda permita o acesso de todos os servidores, o servidor terá seu acesso negado, visto que o firewall encontrou a regra 1 primeiro, ela se aplicava ao caso, ele seguiu ela e parou ali, sem nem mesmo consultar a segunda.

NAT (Network Address Translation): Usado para mascarar os IP da LAN, o NAT é o serviço que traduz o IP privado de cada máquina, para um IP público, usado por toda a rede local. O servidor externo recebe esse IP público e envia a resposta para ele, após o firewall receber essa resposta, ele envia para a máquina na rede que fez a solicitação. Para isso, o firewall mantem os dados de origem e destino das solicitações.

SNAT (Source NAT): Mascara o endereço de origem.

DNAT (Destination NAT): Mascara o endereço de destino.

VPN (Virtual Private Network): A VPN site to site cria um túnel para questões de segurança na comunicação, precisa que ambos os firewall estejam configurados iguais, precisa de uma pre-shared key que é uma senha compartilhada entre as duas

pontas, possui também o protocolo IKE, que é um protocolo de troca de chaves, esse protocolo pode ser encontrado em 2 versões, a versão 2 possui mais segurança e features a mais e caso seja encontrado o uso da versão 1 é recomendável atualizá-lo. Pode possuir criptografia e autenticação. Na área de troca de chaves de criptografia, um ótimo exemplo são os grupos Diffie–Hellman, onde quanto maior o grupo, mais segurança você terá, porem maior o custo de processamento. O termo Key lifetime refere-se ao tempo de vida das chaves. A comunicação é dividida em Phase 1 e Phase 2. A Phase 1 se refere a comunicação entre um firewall e outro, através dos IP públicos. Enquanto a Phase 2 se refere a comunicação entre as redes privadas por trás do firewall. A Phase 2 não funciona se a Phase 1 estiver com problemas, entretanto a Phase 1 pode funcionar mesmo que a Phase 2 não esteja. A VPN também precisa de regras estabelecidas, para permitir as comunicações entre as partes. As configurações para a Phase 1 e Phase 2 não precisam ser iguais, mas a configuração nos firewall

envolvidos sim.

NAT na VPN: O NAT traversal é quando o IP é mascarado para trafegar no VPN, ocorre após ser habilitado e é usado para evitar falha na comunicação, por exemplo, devido ao IP da rede ser igual dos dois lados. Também existe uma configuração para evitar o uso de NAT dentro da VPN, para que seja mantido o IP privado no tráfego pelo túnel, o nome varia de acordo com o fornecedor do firewall, podendo ser NO-NAT, NNAT ou NAT EXEMPT, porem a função deles é a mesma.

Como um firewall lê uma regra: Após receber uma solicitação direta, o firewall verifica se tem uma rota para o IP alvo. Caso pra uma solicitação exista uma regra de DNAT ou SNAT, ele primeiro aplica a regra, alterando o IP e depois testa se possui uma rota pra esse IP alterado.