FIREWALL

- Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.

- Os firewalls têm sido a linha de frente da defesa na segurança de rede há mais de 25 anos. Eles colocam uma barreira entre redes internas protegidas e controladas que podem ser redes externas confiáveis ou não, como a Internet.

- Um firewall pode ser um hardware, software ou ambos.

- Firewall stateless: firewall sem estado de conexão, quando não há uso de conntrack, não é possível fazer NAT/Redirecionamento de portas;

- Firewall statefull: firewall com estado de conexão, todos os pacotes (fluxos) são registrados na conntrack e portanto é possível saber o estado da conexão (nova, estabelecida, desconhecida, ...), a contagem de bytes, o timeout, quais dados foram usados na alteração de redirecionamento de portas e/ou alteração do IP de origem;

FIREWALL

- forward: quando um pacote entra em uma interface de rede para sair em outra interface de rede;
- input: quando um pacote entra em uma interface com destino a um IP do próprio Linux (loopback);
- output: quando um pacote é criado no Linux para ser entregue no próprio Linux (input) ou entregue por uma interface de rede a algum host remoto;
- Por padrão os sistemas não preenchem nenhuma regra em nenhuma das etapas de controle do firewall;
- Você deve inserir a regra em alguma etapa;
- Quando um pacote IP chega em uma etapa com regras, as regras são processadas na ordem de cima
- para baixo;

FIREWALL

- Cada regra é composta de verificação e ação:

- Não ausência de verificação a ação é executada;

- Na presença de verificação única, é necessária que ela seja satisfeita para que a ação seja executada;
- Na presença de várias verificações, todas devem ser satisfeitas para que a ação seja executada;
- Se a verificação (ou verificações) não forem satisfeitas, a próxima regra será analisada até o final da lista;

- Não havendo regras, aplica-se a política da etapa;

- Política: cada etapa possui uma política, que irá dar tratamento aos pacotes IPs que não encontraram regras para tratá-los;

- Opções: DROP ou ACCEPT
- Padrão: ACCEPT - os pacotes passam para a próxima etapa;

FIREWALL

- Os pacotes IPs passam por vários tratamentos:
- Fragmentação/desfragmentação;
- Registro de detalhes em tabela de conexões - CONNTRACK;
- Alterações nos cabeçalhos (TOS, TTL, redirecionamento de porta);
- Alterações de IP de origem (NAT: DNAT, MASQUERADE e NETMAP);
- Marcações internas;
- Desvio de roteamento;
- Destruição silenciosa (ignora-se o processamento do pacote);
- Destruição com retorno (resposta TCP-RST, ICMP-*);
- Conntrack: tabela que mantém o registro de todos os fluxos passando pelo roteadores;

FIREWALL

- O ato de registro da conexão na base de dados conntrack ocorre entre a etapa raw/PREROUTING e mangle/PREROUTING;
- Caso a etapa raw/PREROUTING aplique a ação NOTACK no pacote, ele não será registrado na conntrack e ficará em modo stateless, impossibilidade de sofrer alterações de porta e origem;

- Alterações de destino (DNAT) funcionam apenas em nat/PREROUTING;
- Alterações de origem (NAT) funcionam apenas em ROUTING (ip rule) e nat/POSTROUTING;
- Alterações no IP de origem são mapeados na conntrack, uma nova porta de origem e ip de origem são definidos para a conexão, e o pacote é alterado e enviado adiante;

- Quando o pacote retorna para o Linux, contendo em seu destino o IP e porta atribuidos pelo NAT, uma consulta na conntrack é realizada para descobrir qual os dados originais do pacote
- para a reescrita, esse processo é realizado entre raw/PREROUTING e mangle/PREROUTING;
- Apenas pacotes com estato NEW (primeiro pacote de cada fluxo) pode sofrer alterações de destino/origem;

FIREWALL

- Quando um pacote IP chega em uma etapa com regras, as regras são processadas na ordem de cima para baixo;
- Cada regra é composta de verificação e ação:
- Não ausência de verificação a ação é executada;

- Na presença de verificação única, é necessária que ela seja satisfeita para que a ação seja executada;
- Na presença de várias verificações, todas devem ser satisfeitas para que a ação seja executada;
- Se a verificação (ou verificações) não forem satisfeitas, a próxima regra será analisada até o final da lista;

- Não havendo regras, aplica-se a política da etapa;
- Política: cada etapa possui uma política, que irá dar tratamento aos pacotes IPs que não encontraram regras para tratá-los;
- Opções: DROP ou ACCEPT Padrão: ACCEPT - os pacotes passam para a próxima etapa;

FIREWALL

- No uso de nomes DNS (FQDN), o iptables irá resolver o nome, pegar o primeiro IP e
- inserir no netfilter, se o site possuir múltiplos IPs no DNS ou mudar de IP no DNS, a regra não fica sabendo!
- só é possível verificar a interface de saída após a etapa de roteamento;

- Principais ações:
- ACCEPT: pula o pacote para próxima etapa;
- DROP: destrói o pacote silenciosamente;
- REJECT: destrói o pacote e envia um retorno para o remetente:
- TCP: tcp-reset;
- Demais: ICMP
- SNAT: altera o endereço de origem para um IP específico;
- MASQUERADE: altera o endereço IP de origem para o IP da interface de saida (consulta o ip de destino em: ip route get 8.8.8.8 e usa o src do retorno como IP de origem);
- NETMAP: cria um mapa de SNAT baseado nos bits finais de um prefixo de rede;
- DNAT: altera o destino e/ou porta (nat/PREROUTING);
- REDIRECT: altera a porta (nat/PREROUTING);
- LOG: envia um registro de log com os detalhes do pacote para o buffer de logs

FIREWALL

- O firewall pode incorporar software, hardware ou combinar ambos. São diversos os tipos de firewall. Por isso, apenas saber o que é firewall não é suficiente. É necessário analisar o ambiente para escolher o melhor tipo. Veja os três principais.

- Firewall de inspeção de estado
- Um tipo muito comum de firewall é o de inspeção de estado, também considerado o firewall tradicional.

- Com base em critérios técnicos, como estados, portas específicas ou protocolos, ele permite ou bloqueia o tráfego. Suas decisões de filtragem determinam se os dados podem chegar no usuário.

- O administrador, ao configurar o computador e a ferramenta, estabelece previamente esses critérios. Mas o firewall também toma decisões de forma autônoma com base nas interações anteriores, Por exemplo, os tipos de tráfego que causaram interrupções no passado serão filtrados no futuro.

FIREWALL

- O firewall de proxy é muito semelhante com uma barreira física real, pois atua como intermediário entre redes externas e computadores. É o “guarda no portão”, que examina e avalia os dados recebidos antes de permitir a passagem para o usuário.

- Os servidores proxy podem ter desvantagens, principalmente por interferir em dados que não são uma ameaça, o que gera atrasos. Eles podem, porém, oferecer recursos adicionais, como segurança de conteúdo e armazenamento em cache, pois evita conexões diretas de fora da rede.

- O firewall de próxima geração (NGFW) combina recursos de um firewall tradicional e de sistemas de prevenção de invasões de rede. Ele vai além da filtragem de pacotes e é a solução mais adequada para se manter atualizado quanto às ameaças mais modernas.

- Empresas e redes sofisticadas utilizam o NGFW para para examinar e identificar perigos específicos em nível mais granular. Para tanto, outros recursos que vão além do padrão de firewall (inspeção stateful). Veja alguns:

FIREWALL

- Reconhece e controla aplicações para detectar e bloquear aplicativos nocivos;
- Adota técnicas que lidam com ameaças à segurança em evolução;
- Atualiza caminhos para incluir feeds futuros de informação;
- Previne invasão integrada.
- Existe, também, o NGFW focado em ameaças. Além de tudo que um NGFW tradicional oferece, ele tem detecção e remediação avançadas de ameaças.

- Assim, o profissional consegue saber os recursos em maior risco, pois reconhece o contexto de forma completa. Ele também pode reagir rapidamente aos ataques cibernéticos, pois utiliza automação de segurança inteligente.

- O NGFW focado em ameaças pode, ainda, detectar as atividades evasivas e suspeitas, que se relacionam com eventos de rede e endpoint. Sua atuação completa reduz bastante o tempo entre detecção e limpeza. Assim, contribui para uma melhor administração do ambiente.

- Além de aprender o que é firewall, é muito importante identificar o tipo mais adequado à infraestrutura empresarial. Nem sempre, essa avaliação é fácil, motivo pelo qual a assistência de especialistas pode ajudar bastante os gestores.

FIREWALL

- A invenção do firewall deve ser encarada como um processo em andamento. O motivo disso é que ela está em constante evolução, e vários criadores participaram do seu desenvolvimento e evolução.

- Do final dos anos 80 até meados dos anos 90, cada criador expandiu vários componentes e versões relacionados aos firewalls antes que eles se tornassem o produto usado como base para todos os firewalls modernos.

- Brian Reid, Paul Vixie e Jeff Mogul

- No final da década de 80, Mogul, Reid e Vixie trabalhavam na Digital Equipment Corp (DEC) no desenvolvimento de tecnologia de filtragem de pacotes que se tornaria valiosa em futuros firewalls. Isso levou ao conceito de inspecionar conexões externas antes de entrar em contato com computadores em uma rede interna. Embora alguns possam considerar esse filtro de pacotes como o primeiro firewall, tratava-se de uma tecnologia de componentes que sustentava os verdadeiros sistemas de firewall que estavam por vir.

FIREWALL

- David Presotto, Janardan Sharma, Kshitiji Nigam, William Cheswick e Steven Bellovin

- Do final dos anos 80 até o início dos anos 90, vários funcionários da AT&T Bell Labs pesquisaram e desenvolveram o conceito inicial do firewall de gateway em nível de circuito. Esse foi o primeiro firewall a inspecionar e permitir conexões contínuas, em vez de reautorizar repetidamente após cada pacote de dados. Presotto, Sharma e Nigam desenvolveram o gateway em nível de circuito entre 1989 e 1990 e foram seguidos pelo trabalho de Cheswick e Bellovin com tecnologia de firewall em 1991.

- Marcus Ranum

- Entre 1991 e 1992, na DEC, Ranum inventou os proxies de segurança, que se tornaram um componente vital do primeiro produto de firewall de camada de aplicativo: o Secure External Access Link (SEAL) baseado em proxy, de 1991. Essa foi uma expansão do trabalho de Reid, Vixie e Mogul na DEC e foi o primeiro firewall lançado comercialmente.

FIREWALL

- Gil Shwed e Nir Zuk

- Entre 1993 e 1994, na Check Point, o fundador da empresa, Gil Shwed, e um prolífico desenvolvedor, Nir Zuk, tiveram papéis significativos no desenvolvimento do primeiro produto de firewall fácil de usar e amplamente adotado: o Firewall-1. Gil Shwed inventou e registrou a patente nos EUA da inspeção com estado, em 1993. Isso foi seguido pelo trabalho de Nir Zuk em uma interface gráfica fácil de usar para o Firewall-1 de 1994, que foi vital na adoção mais ampla de firewalls em empresas e residências para o futuro em perspectiva.

- Esses desenvolvimentos foram essenciais para moldar o produto de firewall que conhecemos hoje. Cada um foi usado de alguma forma em muitas soluções de segurança virtual.

FIREWALL

- O que um firewall faz e contra o que ele pode proteger? O conceito de firewall de segurança de rede destina-se a restringir a superfície de ataque da rede a um único ponto de contato.
- Em vez de cada host em uma rede ser exposto diretamente à internet global, primeiro todo o tráfego deve entrar em contato com o firewall.
- Como isso também funciona da maneira inversa, o firewall pode filtrar e bloquear o tráfego não permitido, de entrada ou de saída.
- Além disso, os firewalls são usados para criar uma trilha de auditoria de tentativas de conexão de rede, a fim de promover a conscientização de segurança.
- Como a filtragem de tráfego pode ser um conjunto de regras estabelecido pelos proprietários de uma rede privada, isso cria casos de uso personalizados para firewalls.

Os casos de uso populares envolvem o gerenciamento dos seguintes itens:

- Infiltração de agentes mal-intencionados: conexões indesejadas de uma fonte de comportamento estranho podem ser bloqueadas. Isso pode evitar espionagem e ameaças persistentes avançadas.
- Controles para pais: os pais podem impedir que seus filhos vejam conteúdo explícito na Web.
- Restrições de navegação na Web no local de trabalho: os empregadores podem impedir que os funcionários usem as redes da empresa para acessar determinados serviços e conteúdo, como mídia social.
- Intranet controlada nacionalmente: os governos nacionais podem bloquear o acesso de residentes internos a conteúdo e serviços da Web que são potencialmente dissidentes à liderança de uma nação ou a seus valores.

FIREWALL

- No entanto, os firewalls são menos eficazes nos seguintes aspectos:

- Identificar explorações de processos de rede legítimos: os firewalls não preveem a intenção humana. Portanto, não podem determinar se uma conexão "legítima" é destinada a fins mal-intencionados. Por exemplo, a fraude de endereço IP (falsificação de IP) ocorre porque os firewalls não validam os IPs de origem e destino.
- Impedir conexões que não passam pelo firewall: firewalls em nível de rede, por si sós, não impedirão a atividade interna mal-intencionada. Os firewalls internos, assim como aqueles baseados em host, precisarão estar presentes além do firewall de perímetro, para particionar a rede e retardar a propagação de "incêndios" internos.
- Fornecer proteção adequada contra malware: embora as conexões com código mal-intencionado possam ser interrompidas se não forem permitidas, uma conexão considerada aceitável ainda pode levar essas ameaças à sua rede. Se um firewall ignorar uma conexão como resultado de configuração incorreta ou exploração, um pacote de proteção antivírus ainda será necessário para limpar qualquer malware que penetrar.

FIREWALL

- A configuração e a manutenção adequadas do firewall são essenciais para manter sua rede e seus dispositivos protegidos. Veja algumas dicas para orientar suas práticas de segurança de rede de firewall:

- Sempre atualize seus firewalls o mais rápido possível

- Use proteção antivírus:

- Limite portas e hosts acessíveis com uma lista de permissões:

- Tenha redundâncias de rede ativas para evitar tempo de inatividade: backups de dados para hosts de rede e outros sistemas essenciais podem evitar perda de dados e produtividade durante um incidente.

FIREWALL

- /home/raphael/iptables-clear.sh
- #!/bin/bash

- # servidores DNS:
- # - Policy DROP:
- iptables -t filter -P FORWARD DROP
- # - Servidores DNS (request):
- iptables -t filter -A FORWARD -p udp --dport 53 -d 8.8.8.8 -j ACCEPT
- iptables -t filter -A FORWARD -p udp --dport 53 -d 8.8.4.4 -j ACCEPT
- iptables -t filter -A FORWARD -p udp --dport 53 -d 1.1.1.1 -j ACCEPT
- iptables -t filter -A FORWARD -p udp --dport 53 -d 1.0.0.1 -j ACCEPT
- # - Servidores DNS (reply):
- iptables -t filter -A FORWARD -p udp --sport 53 -s 8.8.8.8 -j ACCEPT
- iptables -t filter -A FORWARD -p udp --sport 53 -s 8.8.4.4 -j ACCEPT
- iptables -t filter -A FORWARD -p udp --sport 53 -s 1.1.1.1 -j ACCEPT
- iptables -t filter -A FORWARD -p udp --sport 53 -s 1.0.0.1 -j ACCEPT

OBRIGADO