

Firewall

Versão: 1.3

Data: 23/07/2024

Conceitos Gerais

- Sendo um firewall o ponto de conexão com a Internet, tudo o que chega à rede interna deve passar por ele.
- O firewall é o responsável pela aplicação de regras de segurança que podem ter objetivos desde o controle de acesso até o registro do tráfego para auditoria.
- É um mecanismo de segurança obrigatório em um projeto de segurança.
- Cada tipo de firewall possui características e funcionalidades específicas, sendo importante escolher o modelo ideal para cada necessidade.

Tipos de Firewall

1. Firewall de filtragem estática de pacotes (também conhecido como firewall sem estado - *stateless*):

- **Função:** Filtragem básica de dados na camada 3 (rede) e 4 (transporte) do modelo OSI.
- **Funcionamento:** Bloqueia ou permite o tráfego com base em regras predefinidas (IP, portas, protocolos).
- **Vantagens:** Simples, eficiente para filtragem básica.
- **Desvantagens:** Regras manuais limitam a flexibilidade, não inspeciona o conteúdo dos pacotes.
- **Ideal para:** Redes pequenas com baixo risco de ataques.

Em contraste ao Firewall com/mantém estado (*stateful*).

2. Firewall de gateway (cria “circuito”):

- **Função:** Filtragem na camada 5 (sessão) do modelo OSI / camada 4 (transporte) do modelo TCP/IP.
- **Funcionamento:** Monitora o *handshake* TCP para validar conexões entre dispositivos internos e externos.
- **Vantagens:** Monitoramento rápido de conexões TCP, identifica ameaças com eficiência.
- **Desvantagens:** Requer combinação com outros dispositivos de segurança para proteção completa (por exemplo, IDS/IPS)

- **Ideal para:** Redes com tráfego TCP significativo e necessidade de monitoramento de conexões.

3. Firewall de *proxy* (também conhecido como *firewall de aplicação*):

- **Função:** Filtragem na camada 7 (aplicação) do modelo OSI.
- **Funcionamento:** Atua como intermediário entre a rede interna e externa, filtrando dados de protocolos como HTTP, FTP e DNS.
- **Vantagens:** Alto nível de segurança para aplicações específicas.
- **Desvantagens:** Implementação complexa, exige grande quantidade de regras, pode gerar lentidão na rede.
- **Ideal para:** Redes que manipulam dados confidenciais e exigem controle granular do tráfego de aplicações.

4. WAF (*Web Application Firewall*):

- **Camada de atuação:** Camada 7 (aplicação) do modelo OSI.
- **Função:** Analisa e filtra o tráfego web em busca de ataques específicos direcionados a aplicações web, como injeção de SQL, cross-site scripting (XSS) e ataques de força bruta.
- **Vantagens:**
 - Proteção contra ataques específicos de aplicações web.
 - Monitoramento e detecção de ataques em tempo real.
 - Possibilidade de bloquear ataques automaticamente.
- **Desvantagens:**
 - Proteção limitada a ataques de aplicações web.
 - Pode gerar falsos positivos, bloqueando tráfego legítimo.
 - Implementação complexa, exige conhecimento técnico para configuração.

5. Firewall de última geração (NGFW - *Next-Generation Firewall*):

- **Função:** “Combina as funcionalidades dos firewalls anteriores com recursos avançados contra ataques cibernéticos modernos”. Diversas camadas analisadas, tudo em um.
- **Funcionamento:** Filtragem granular de pacotes em todas as camadas, inspeção profunda de pacotes, IPS, antivírus, controle de aplicativos, VPN e outras funções.
- **Vantagens:** Proteção completa contra diversos tipos de ameaças, incluindo malware e ataques na camada 7.
- **Desvantagens:** Alto custo, implementação complexa, exige expertise para gerenciamento.
- **Ideal para:** Grandes empresas e organizações com alto nível de exigência de segurança.

Extra: a inspeção profunda com DPI (*Deep Packet Inspection*); OPNsense (NGFW, sandbox e IPS)

Firewall iptables

- Firewall IPTables:
<https://www.guiafoca.org/guiaonline/seguranca/ch05.html>
- Tabelas:
<https://www.guiafoca.org/guiaonline/seguranca/ch05.html#fw-iptables-tabelas>
- Chains: os Chains são locais onde as regras do firewall definidas pelo usuário são armazenadas. Existem dois tipos de chains: os embutidos (como os chains INPUT, OUTPUT e FORWARD) e as criados pelo usuário. Os nomes dos chains embutidos devem ser especificados sempre em maiúsculas (note que os nomes dos chains são case-sensitive, ou seja, o chain input é completamente diferente de INPUT).

Mais referências

- <https://ubuntu.com/server/docs/security-firewall>
- <http://www.guiafoca.org/cgs/guia/avancado/ch-fw-iptables.html>
- <https://ostec.blog/seguranca-perimetro/firewall-stateful-stateless>
- <https://help.ubuntu.com/community/UFW>

Práticas

Faça sempre um teste após inserir uma regra

Para cada item a seguir, execute um comando e verifique a saída em tela aos realizar o teste de conexão.

Manipulando Chains, adicionando regras:

<https://www.guiafoca.org/guiaonline/seguranca/ch05s02.html>

Simular abertura de portas e conexões:

1. Abrindo socket/port: `sudo nc -l <IP> <NUMERO_PORTA>`
2. Teste de conexão: `telnet <IP> <NUMERO_PORTA>`
3. Exemplo: `sudo nc -l localhost 22`

Restrição de acesso web para todos

4. Crie uma regra no iptables para negar o acesso por qualquer IP de origem que tente acessar a porta 80 do seu computador.
5. Agora crie uma regra que libere a porta 80 somente para 1 IP específico de origem e negue para todo o resto.

Restrição de ping

1. Crie uma regra que negue o ping (ICMP) vindo de quaisquer IPs.

Redirecionamento de portas

1. Crie um redirecionamento da porta 3333 para a porta 22 do SSH. Qualquer IP de origem que tenha como destino a sua máquina na porta 3333 deve ter seu fluxo redirecionado para a porta 22.
2. Adicione uma regra que registre o LOG para a regra anterior.

Aplicação de ToS

1. Utilize a tabela mangle para criar uma regra de espera mínima com base no campo TOS do IPv4. **Para este passo, não é necessário gerar tráfego para testar, mostre somente a regra na tabela mangle.**
 - a. “Espera Mínima: É especificado através de Minimize-Delay, 16 ou 0x10”
 - b. <https://www.guiafoca.org/guiaonline/seguranca/ch05s05.html>

Negando tudo e liberando somente o necessário

1. Limpe as regras
2. Troque a política da chain INPUT na tabela filter (tabela padrão caso não informe a flag -t) para DROP
3. Libere as portas 22, 80 e 443 para todos (qualquer IP origem)

Registrando

1. Crie uma regra que registra em LOG os acessos à porta 22 e outro para a porta 80