Sessão 3: Firewall

As atividades desta sessão serão realizadas na máquina virtual *FWGW1-G*, com pequenas exceções apontadas pelo enunciado dos exercícios.

1) Trabalhando com *chains* no *iptables*

O Netfilter é um *framework* provido pelo kernel Linux que permite que várias operações relacionadas à rede sejam implementadas através de *handlers* customizados. Ele provê diversas funções e operações que permitem filtragem de pacotes, tradução de endereços de rede e portas, bem como a capacidade de proibir que pacotes cheguem a pontos sensíveis da rede.

O `iptables` é a ferramenta em espaço de usuário que permite a gerência do Netfilter. Há vários conceitos centrais ao `iptables`, como:

- Tabelas:
  - *Filter*: filtragem de pacotes.
  - *NAT*: tradução de endereços.
  - *Mangle*: marcação de pacotes e QoS.
- Chains:
  - INPUT: entrada no firewall propriamente dito.
  - OUTPUT: saída do firewall propriamente dito.
  - FORWARD: passagem através do firewall.
  - PREROUTING: decisões pré-roteamento; presente apenas nas tables *NAT* e *Mangle*.
  - POSTROUTING: decisões pós-roteamento; presente apenas nas tables *NAT* e *Mangle*.
- Alvos:
  - ACCEPT: aceita o pacote.
  - DROP: descarta o pacote sem informar o remetente.
  - REJECT: rejeita o pacote e notifica o remetente.
  - LOG: loga o pacote nos registros do `iptables`.
- Manipulação de regras:
  - A: adiciona a regra ao final da *chain* (*append*).
  - I: insere a regra no começo da *chain* (*insert*).
  - D: apaga a regra (*delete*).
  - L: listas as regras de uma dada *chain* (*list*).
  - P: ajusta a política padrão de uma *chain* (*policy*).
  - F: apaga todas as regras da *chain* (*flush*).
- Padrões de casamento:

  - `-s`: IP de origem do pacote.
  - `-d`: IP de destino do pacote.
  - `-i`: interface de entrada.
  - `-o`: interface de saída.
  - `-p`: protocolo, que pode ser dos tipos TCP, UDP e ICMP.
- Módulos adicionais para casamento de pacotes (*extended packet matching modules*) podem ser habilitados com a opção `-m` ou `--match`. Destacamos:
  - `conntrack`: quando habilitado, permite acesso ao controle de estados de conexões; normalmente invocado por `-m conntrack --ctstate` ou para um *subset* de suas funções, `-m state --state`. Estados válidos incluem INVALID, NEW, ESTABLISHED, RELATED e UNTRACKED.
  - `icmp`: possibilita filtrar tipos específicos de ICMP, via *flag* `--icmp-type`.
  - `mac`: possibilita filtragem por endereço físico de origem, via *flag* `--mac-source`.
  - `multiport`: permite especificação de até 15 portas dentro de uma mesma regra, separadas por vírgula, ou um *range* com a sintaxe `porta:porta`. Pode-se especificar portas de origem (`--sports`), destino (`--dports`) ou ambas (`--ports`).
  - `tcp`: habilita as opções `--source-port` (ou `--sport`), `--destination-port` (ou `--dport`), `--tcp-flags` (*flags válidas*: SYN, ACK, FIN, RST, URG, PSH, ALL e NONE), `--syn` e `--tcp-option` para pacotes TCP.
  - `udp`: habilita as opções `--source-port` (ou `--sport`), `--destination-port` (ou `--dport`) para pacotes UDP.

1. Primeiro, vamos testar a filtragem simples (*stateless*) no `iptables`. Faça login na máquina *FWGW1-G* como `root` e mude a política padrão da *chain* OUTPUT para DROP. Em seguida, tente conectar-se à porta 80/HTTP de um host remoto na Internet. É possível?
2. Agora, crie uma regra na *chain* OUTPUT que permita a saída de pacotes na porta 80/HTTP (não se esqueça também de permitir consultas DNS à porta 53/UDP, se estiver utilizando um nome e não um endereço IP) e tente conectar-se novamente. Qual o resultado?
3. Mude a política padrão da *chain* INPUT também para DROP. Ainda é possível conectar-se?
4. Finalmente, crie uma regra apropriada na *chain* INPUT e teste o sucesso na conexão HTTP.

2) Firewall *stateful*

Não é conveniente nem manutenível criar regras como fizemos na atividade (1) — para cada regra de saída, ter que existir uma regra de entrada correspondente. Podemos usar a capacidade do `iptables` de monitorar estados de conexões a nosso favor, já que ele é um firewall *stateful*.

1. Remova as regras da chain INPUT. Em seguida crie uma regra genérica que permita que conexões estabelecidas sejam autorizadas através do firewall. Em seguida, tente estabelecer uma conexão HTTP. Foi possível?
2. Qual seria, então, a diferença entre filtros de pacotes *stateless* e *stateful*?

3) Configurando o firewall *FWGW1-G*: tabela *filter*

A partir desta atividade o roteiro está dividido em duas grandes partes. Na primeira, o aluno programará um controle de pacotes para permitir a comunicação entre os *hosts* descritos na topologia do laboratório. Na segunda parte, programará a tradução de pacotes. Se precisar, retorne à imagem constante da atividade (2) da sessão 1 — Configuração preliminar das máquinas.

A tabela a seguir mostra uma listagem com a descrição dos serviços a serem disponibilizados pelos servidores da DMZ, cuja permissão de acesso será configurada nas atividades a seguir.

Tabela 1. Serviços de rede disponíveis na DMZ

Servidor	Serviço	Protocolo	Porta	Descrição
LinServer-G	SSH	TCP	22	Serviço de login remoto
LinServer-G	Postfix	TCP	25	Servidor de mensagens
LinServer-G	Apache	TCP	80	Servidor de páginas web
LinServer-G	Courier	TCP	110	Servidor POP3
LinServer-G	PostgreSQL	TCP	5432	Servidor de banco de dados
LinServer-G	Bind	UDP	53	Servidor DNS
LinServer-G	NTP	UDP	123	Servidor de hora
WinServer-G	FTP	TCP	21	Servidor de arquivos
WinServer-G	IIS	TCP	80	Servidor de páginas web
WinServer-G	IIS	TCP	443	Servidor de páginas web
WinServer-G	RDP	TCP	3389	Serviço de conexão remota
WinServer-G	NTP	UDP	123	Servidor de hora

A realização desta atividade é fundamental para a realização das demais atividades deste curso. A política de filtro de pacotes será a mais restritiva possível, permitindo somente as conexões previamente definidas no firewall. Dessa forma, a política padrão é negar todos os pacotes que chegarem, saírem e/ou atravessarem o firewall.

A cada item será necessário verificar a configuração corrente do firewall. Para listar as regras das tabelas *input* e *nat* do firewall, respectivamente, use os comandos:

```
# iptables -L -vn
# iptables -t nat -L -vn
```

Caso cometa um erro, você pode apagar todas as regras das tabelas *input* e *nat* do firewall, respectivamente, com os comandos:

```
# iptables -F
# iptables -t nat -F
```

Use o comando `tcpdump` para testar o funcionamento de suas regras.

1) Configuração preliminar

1. O primeiro passo, antes de mesmo começar a mexer no firewall, é ter uma maneira de gravar suas regras. Iremos instalar o pacote `iptables-persistent` para atingir esse objetivo; mas, antes de começar, garanta que seu firewall não possui regras e que as políticas de entrada/saída são permissivas:

   ```
   # iptables -P INPUT ACCEPT
   # iptables -P OUTPUT ACCEPT
   # iptables -F
   ```

   ```
   # iptables -L
   Chain INPUT (policy ACCEPT)
   target     prot opt source               destination

   Chain FORWARD (policy ACCEPT)
   target     prot opt source               destination

   Chain OUTPUT (policy ACCEPT)
   target     prot opt source               destination
   ```

2. Agora, instale o pacote `iptables-persistent` para tornar suas configurações de firewall permanentes mesmo após o `reboot` da máquina.

   ```
   # apt-get install iptables-persistent
   ```

   Na instalação do pacote, quando perguntado, responda:

   Tabela 2. Configurações do iptables-persistent

Pergunta	Resposta
Salvar as regras IPv4 atuais?	Sim
Salvar as regras IPv6 atuais?	Sim

3. Isso feito, basta dar início ao processo de configuração do firewall. Ao inserir um conjunto de regras com as quais você esteja satisfeito, é possível gravá-las de forma fácil com o comando:

```
# iptables-save > /etc/iptables/rules.v4
```

4. Se cometer qualquer erro durante o processo de configuração, você pode recarregar o conjunto de regras salvo no arquivo `/etc/iptables/rules.v4` com o comando:

```
# systemctl restart netfilter-persistent.service
```

2) Configuração do acesso ao firewall

Vamos primeiramente permitir acesso administrativo ao firewall por SSH, bem como pacotes ICMP para testes de conectividades.

1. Primeiro, torne as políticas do firewall restritivas, ajustando a política das *chains* INPUT e FORWARD para DROP.
2. Teste o funcionamento do firewall. Na máquina *LinServer*, por exemplo, tente enviar um pacote ICMP para a máquina *FWGW1-G*.
3. Agora, adicione as seguintes regras ao firewall:
   - Permita todo o tráfego na interface *loopback*, e rejeitar qualquer pacote vindo da rede 127.0.0.0/8 que não seja para a interface `lo` com `icmp-port-unreachable`
   - Permita conexões destinadas ao firewall (*chain* INPUT) cujo estado seja relacionado ou estabelecido.
   - Permita gerência via `ssh` do firewall *FWGW1-G* a partir de máquinas da Intranet.
   - Permita que pacotes ICMP oriundos das redes DMZ/Intranet cheguem ao firewall *FWGW1-G*.
4. Realize o teste de conexão do passo (2) novamente, e verifique que suas configurações funcionaram.
5. Se quiser, use o PuTTY (https://www.putty.org/) ou Cygwin (http://www.cygwin.com/), nas máquinas *WinClient-G* ou sua máquina física, para conectar-se à máquina *FWGW1-G* e testar sua configuração.

3) Configuração do acesso Intranet > DMZ

Agora, vamos configurar o firewall para permitir pacotes originados na Intranet que atravessem o firewall com destino aos serviços da DMZ. Verifique a lista de serviços a serem permitidos na tabela 7 — "Serviços de rede disponíveis na DMZ".

1. Adicione regras à *chain* FORWARD da tabela *filter* que permitam que o serviços da tabela referenciada acima possam ser acessados a partir da Intranet.
2. Teste sua configuração acessando o servidor web IIS instalado na máquina *WinServer-G*, e acessando-o a partir da máquina *WinClient-G*.

4) Configuração do acesso DMZ/Intranet > Internet

Agora, vamos configurar o acesso da DMZ e Intranet para a Internet. Para isso, teremos que permitir que pacotes originados nessas redes atravessem o firewall via interface de rede *outbound*.

1. Adicione regras à *chain* FORWARD da tabela *filter* que permitam que as redes DMZ e Intranet possam acessar qualquer serviço na Internet, via quaisquer protocolos.
2. Teste sua configuração acessando uma página da Internet a partir da máquina *LinServer-G*.

5) Configuração do acesso Internet > DMZ

Finalmente, o último passo é permitir que requisições vindas da Internet possam acessar alguns serviços publicados pela DMZ.

Como dois serviços das máquinas *LinServer-G* e *WinServer-G* operam nas mesmas portas (80/TCP e 123/UDP), teremos que fazer uma técnica de PAT (*port address translation*) para que ambos possam ser atingidos. O primeiro passo será feito aqui, nas regras da *chain* FORWARD; na próxima atividade, em que configuraremos o DNAT, será realizada a parte de tradução de portas.

Tabela 3. Serviços publicados pela DMZ para a Internet

Servidor	Serviço	Protocolo	Porta do serviço	Porta Internet
LinServer-G	Postfix	TCP	25	25
LinServer-G	Apache	TCP	80	80
LinServer-G	Courier	TCP	110	110
LinServer-G	Bind	UDP	53	53
LinServer-G	NTP	UDP	123	123
WinServer-G	FTP	TCP	21	21
WinServer-G	IIS	TCP	80	8080
WinServer-G	IIS	TCP	443	443
WinServer-G	NTP	UDP	123	8123

O teste deste configuração será feito na próxima atividade, em que configuraremos o NAT.

As regras de DNAT que inseriremos na atividade a seguir entrarão na *chain* PREROUTING, ou pré-roteamento. Isso significa dizer que os números de porta Internet mostrados acima serão traduzidos para os números das porta de serviço **ANTES** que as regras da *chain* FORWARD sejam processadas.

Tenha isso em mente ao decidir quais números de porta utilizar nas regras de repasse deste exercício.

1. Adicione regras à *chain* FORWARD da tabela *filter* que permitam que a Internet consiga acessar os serviços publicados pelas máquinas da DMZ, de acordo com as especificações acima.

4) Configurando o firewall *FWGW1-G*: tabela *nat*

O principal objetivo desta atividade é demonstrar o entendimento do funcionamento dos tipos de NAT e aplicá-los em uma simulação de caso real.

Utilizando os conceitos aprendidos, será necessário configurar o NAT no firewall *FWGW1-G* para permitir que as máquinas da rede local e da DMZ consigam acessar a Internet. Também será necessária a configuração do NAT para publicação dos serviços da DMZ para a Internet.

1) Configuração do SNAT: DMZ/Intranet > Internet

1. Antes de configurar o SNAT para acesso DMZ/Intranet > Internet, será necessário remover a configuração de *masquerading* preexistente, que fizemos na sessão 1. Edite o arquivo `/etc/rc.local` e remova ou comente a linha:

```
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

2. Da mesma forma, remova essa regra do firewall, já que configuraremos outras regras, mais específicas, em seu lugar a seguir.

```
# iptables -t nat -L POSTROUTING -vn --line-number
Chain POSTROUTING (policy ACCEPT 2 packets, 104 bytes)
num   pkts bytes target     prot opt in     out     source
destination
1       70  5922 MASQUERADE  all  --  *      enp0s3    0.0.0.0/0
0.0.0.0/0
```

```
# iptables -t nat -D POSTROUTING 1
```

3. Agora sim, tudo pronto. Insira uma regra no firewall que faça tradução dos endereços das redes DMZ/Intranet via *masquerading*, permitindo assim seu acesso à Internet.
4. Teste sua configuração. Acesse, por exemplo, a máquina *LinServer-G* e tente acessar um site na Internet.

2) Configuração do DNAT: Internet > DMZ

1. Agora, vamos configurar o DNAT, que irá permitir acesso pela Internet aos serviços publicados pela DMZ. Comece fazendo as regras para a máquina *LinServer-G*, que não exige PAT.
2. Agora, teste sua configuração. Primeiro, instale o servidor web Apache na máquina *LinServer-G*; a seguir, em sua máquina física, acesso o IP público da máquina *FWGW1-G* na porta 80/TCP e verifique que de fato é exibida no navegador a página web instalada no *LinServer-G*.
3. Faça o mesmo processo para a configuração do DNAT da máquina *WinServer-G*. Atente-se para o fato de que duas portas internat, 80/TCP e 123/UDP, serão acessadas através das portas externas 8080/TCP e 8123/UDP respectivamente. Configure o PAT de acordo.

4. Teste sua configuração. Em sua máquina física, acesso o IP público da máquina *FWGW1-G* na porta 8080/TCP e verifique que de fato é exibida no navegador a página web do servidor IIS instalada na máquina *WinServer-G*.

6) Revisão final da configuração do firewall *FWGW1-G*

Salve a configuração feita até aqui e reinicie o firewall com os comandos:

```
# hostname
FWGW1-A

# iptables-save > /etc/iptables/rules.v4
# systemctl restart netfilter-persistent.service
```

Revise se todos os pontos abordados até aqui foram contemplados. Que outras regras interessantes poderiam ser incluídas na configuração desse firewall?