Exercício 3a – Filtros Anti-Spoofing

Objetivo: Implementar na rede do ISP filtros anti-spoofing.

Cenário: Os endereços das interfaces físicas, o protocolo de roteamento interno e o iBGP já estão configurados.

Antes de configurar as sessões e-BGP e obter acesso às redes externas, aplique no roteadores do AS filtros de proteção que impediram que seus clientes enviem pacotes para a Internet com endereços IP falsos (*spoofing*). Importante destacar que quanto mais próximo do cliente mais restritiva devem ser as regras aplicadas. Dentro desse conceito, nos roteadores que atuam como "concentrador", juniper e mikrotik_clientes, deve-se habilitar o `rp_filter` e filtrar a entrada de pacotes apenas de IPs das redes dos clientes. Nas bordas, recomenda-se apenas adicionar filtro de bogons.

1. Primeiro, configure nos roteadores de borda do AS os filtros anti-spoofing IPv4. Esses filtros irão descartar pacotes cujo endereço de origem seja de prefixos de uso reservado, que não devem ser utilizados na Internet, e permitirá o envio de pacotes de endereços válidos.

   Para realizar essa tarefa execute os seguintes comandos no roteador mikrotik_borda:

```
> /ip firewall address-list
  add address=0.0.0.0/8 list=FILTRO-BOGONS-V4
  add address=10.0.0.0/8 list=FILTRO-BOGONS-V4
  add address=100.64.0.0/10 list=FILTRO-BOGONS-V4
  add address=127.0.0.0/8 list=FILTRO-BOGONS-V4
  add address=169.254.0.0/16 list=FILTRO-BOGONS-V4
  add address=172.16.0.0/12 list=FILTRO-BOGONS-V4
  add address=192.0.0.0/24 list=FILTRO-BOGONS-V4
  add address=192.0.2.0/24 list=FILTRO-BOGONS-V4
  add address=192.168.0.0/16 list=FILTRO-BOGONS-V4
  add address=198.18.0.0/15 list=FILTRO-BOGONS-V4
  add address=198.51.100.0/24 list=FILTRO-BOGONS-V4
  add address=203.0.113.0/24 list=FILTRO-BOGONS-V4
  add address=224.0.0.0/3 list=FILTRO-BOGONS-V4

> /ip firewall filter
  add action=drop chain=forward in-interface=ether2 \
src-address-list=FILTRO-BOGONS-V4
  add action=drop chain=forward in-interface=ether3 \
src-address-list=FILTRO-BOGONS-V4
  add action=drop chain=forward in-interface=ether4 \
src-address-list=FILTRO-BOGONS-V4
```

   No roteador cisco execute os seguintes comandos para criar os filtros:

```
# configure terminal
# ip access-list extended FILTRO-BOGONS-V4
# deny ip 0.0.0.0 0.255.255.255 any
# deny ip 10.0.0.0 0.255.255.255 any
# deny ip 100.64.0.0 0.63.255.255 any
# deny ip 127.0.0.0 0.255.255.255 any
# deny ip 169.254.0.0 0.0.255.255 any
# deny ip 172.16.0.0 0.15.255.255 any
# deny ip 192.0.0.0 0.0.0.255 any
# deny ip 192.0.2.0 0.0.0.255 any
# deny ip 192.168.0.0 0.0.255.255 any
# deny ip 198.18.0.0 0.1.255.255 any
# deny ip 198.51.100.0 0.0.0.255 any
# deny ip 203.0.113.0 0.0.0.255 any
# deny ip 224.0.0.0 31.255.255.255 any
# permit ip any any

# interface GigabitEthernet0/0.3XX4
# ip access-group FILTRO-BOGONS-V4 in
# interface GigabitEthernet0/0.3XX5
# ip access-group FILTRO-BOGONS-V4 in
# interface GigabitEthernet0/0.3XX9
```

```
# ip access-group FILTRO-BOGONS-V4 in
# exit
# exit
```

2. O filtro de endereços inválidos no IPv6 difere do filtro IPv4. No IPv4 bloqueia-se as poucas faixas de endereços inválidos e permite-se toda a faixa de endereços válidos. No IPv6, como a quantidade de endereços válidos na Internet é apenas uma pequena parte dos endereços existentes (12,5%) é mais eficiente criar regras que liberem as faixas válidas e bloqueiem todas as demais.

   Para isso, no roteador mikrotik_borda execute os seguintes comandos:

```
> /ipv6 firewall address-list
  add address=2001:500::/30 list=FILTRO-BOGONS-V6
  add address=2001::/32 list=FILTRO-BOGONS-V6
  add address=2001::/16 list=FILTRO-BOGONS-V6
  add address=2001:678::/29 list=FILTRO-BOGONS-V6
  add address=2001:c00::/23 list=FILTRO-BOGONS-V6
  add address=2001:13c7:6000::/36 list=FILTRO-BOGONS-V6
  add address=2001:13c7:7000::/36 list=FILTRO-BOGONS-V6
  add address=2001:43f8::/29 list=FILTRO-BOGONS-V6
  add address=2002::/16 list=FILTRO-BOGONS-V6
  add address=2003::/16 list=FILTRO-BOGONS-V6
  add address=2400::/12 list=FILTRO-BOGONS-V6
  add address=2600::/12 list=FILTRO-BOGONS-V6
  add address=2610::/23 list=FILTRO-BOGONS-V6
  add address=2620::/23 list=FILTRO-BOGONS-V6
  add address=2800::/12 list=FILTRO-BOGONS-V6
  add address=2a00::/12 list=FILTRO-BOGONS-V6
  add address=2801::/24 list=FILTRO-BOGONS-V6
  add address=2c00::/12 list=FILTRO-BOGONS-V6
  add address=4d0c::/16 list=FILTRO-BOGONS-V6
  add address=fe80::/10 list=FILTRO-BOGONS-V6
> /ipv6 firewall filter
  add action=drop chain=forward in-interface=ether2 \
src-address=2001:db8::/32
  add action=drop chain=forward in-interface=ether3 \
src-address=2001:db8::/32
  add action=drop chain=forward in-interface=ether4 \
src-address=2001:db8::/32
  add chain=forward in-interface=ether2 src-address-list=FILTRO-BOGONS-V6
  add chain=forward in-interface=ether3 src-address-list=FILTRO-BOGONS-V6
  add chain=forward in-interface=ether4 src-address-list=FILTRO-BOGONS-V6
  add action=drop chain=forward in-interface=ether2
  add action=drop chain=forward in-interface=ether3
  add action=drop chain=forward in-interface=ether4
> /
```

No roteador cisco execute os seguintes comandos para criar os filtros anti-spoofing IPv6:

```
# configure terminal
# ipv6 access-list FILTRO-BOGONS-V6
# deny ipv6 2001:db8::/32 any
# permit ipv6 2001:500::/30 any
# permit ipv6 2001::/32 any
# permit ipv6 2001::/16 any
# permit ipv6 2001:0678::/29 any
# permit ipv6 2001:0c00::/23 any
# permit ipv6 2001:13c7:6000::/36 any
# permit ipv6 2001:13c7:7000::/36 any
# permit ipv6 2001:43f8::/29 any
# permit ipv6 2002::/16 any
# permit ipv6 2003::/16 any
# permit ipv6 2400::/12 any
# permit ipv6 2600::/12 any
# permit ipv6 2610::/23 any
# permit ipv6 2620::/23 any
# permit ipv6 2800::/12 any
# permit ipv6 2a00::/12 any
# permit ipv6 2801:0000::/24 any
# permit ipv6 2c00::/12 any
# permit ipv6 4d0c::/16 any
# permit ipv6 fe80::/10 any
# deny ipv6 any any

# interface GigabitEthernet0/0.3XX4
# ipv6 traffic-filter FILTRO-BOGONS-V6 in
# interface GigabitEthernet0/0.3XX5
# ipv6 traffic-filter FILTRO-BOGONS-V6 in
# interface GigabitEthernet0/0.3XX9
# ipv6 traffic-filter FILTRO-BOGONS-V6 in
# exit
# exit
```

3. No roteador cisco é preciso executar o seguinte comando para salvar as configurações:

```
# copy running-config startup-config
```

4. Nos roteadores mikrotik_clientes e juniper os filtros anti-spoofing devem ser mais restritivos, permitindo apenas o encaminhamento de pacotes cujo endereço de origem pertença aos prefixos alocados para os clientes. Além disso, deve-se habilitar a função rp-filter.

   No roteador mikrotik_clientes execute os seguintes comandos para criar os filtros para a rede IPv4:

```
> /ip firewall filter
  add chain=forward in-interface=ether3 src-address=102.XX.8.2/32
  add chain= forward in-interface=ether4 src-address=102.XX.1.2/28
  add chain=forward in-interface=ether5 src-address=102.XX.2.2/32
  add action=drop chain=forward in-interface=ether3
  add action=drop chain=forward in-interface=ether4
  add action=drop chain=forward in-interface=ether5
> /ip settings set rp-filter=strict
> /
```

No roteador juniper os comandos a serem executados são os seguintes:

```
# edit
# set firewall family inet filter CLIENTES-DOMESTICOS-V4 term ANTI-SPOOFING
from source-address 102.XX.24.1/32
# set firewall family inet filter CLIENTES-DOMESTICOS-V4 term ANTI-SPOOFING
then accept
# set firewall family inet filter CLIENTES-DOMESTICOS-V4 term DEFAULT then
discard

# set firewall family inet filter CLIENTES-CORP-V4 term ANTI-SPOOFING from
source-address 102.XX.17.0/28
# set firewall family inet filter CLIENTES-CORP-V4 term ANTI-SPOOFING then
accept
# set firewall family inet filter CLIENTES-CORP-V4 term DEFAULT then discard

# set interfaces ge-0/0/0 unit 3XX6 family inet rpf-check
# set interfaces ge-0/0/0 unit 3XX6 family inet filter input CLIENTES-
DOMESTICOS-V4

# set interfaces ge-0/0/0 unit 3XX7 family inet rpf-check
# set interfaces ge-0/0/0 unit 3XX7 family inet filter input CLIENTES-CORP-
V4
# commit
```

5. Os filtros para a rede IPv6 são similares aos da rede IPv4.

   Para configurá-los no roteador mikrotik-clientes execote os seguintes comandos:

```
> /ipv6 firewall filter
  add chain=forward in-interface=ether3 src-address=4d0c:XX:800::/56
  add chain=forward in-interface=ether4 src-address=4d0c:XX:1::/48
  add chain=forward in-interface=ether5 src-address=4d0c:XX:2::2/128
  add action=drop chain=forward in-interface=ether3
  add action=drop chain=forward in-interface=ether4
  add action=drop chain=forward in-interface=ether5
> /
```

Obs.: Os roteadores mikrotik não apresentam a função rp-filter para redes IPv6.

No roteador juniper execute os seguintes comando:

```
# edit
# set firewall family inet6 filter CLIENTES-DOMESTICOS-V6 term ANTI-SPOOFING
from source-address 4d0c:XX:8800:0::/56
# set firewall family inet6 filter CLIENTES-DOMESTICOS-V6 term ANTI-SPOOFING
then accept
# set firewall family inet6 filter CLIENTES-DOMESTICOS-V6 term DEFAULT then
discard

# set firewall family inet6 filter CLIENTES-CORP-V6 term ANTI-SPOOFING from
source-address 4d0c:XX:8001:0::/48
# set firewall family inet6 filter CLIENTES-CORP-V6 term ANTI-SPOOFING then
accept
# set firewall family inet6 filter CLIENTES-CORP-V6 term DEFAULT then
discard

# set interfaces ge-0/0/0 unit 3XX6 family inet6 rpf-check
# set interfaces ge-0/0/0 unit 3XX6 family inet6 filter input CLIENTES-
DOMESTICOS-V6

# set interfaces ge-0/0/0 unit 3XX7 family inet6 rpf-check
# set interfaces ge-0/0/0 unit 3XX7 family inet6 filter input CLIENTES-CORP-
V6
# commit
```

Exercício 3b – Gerência da Porta 25

Objetivo: Implementar na rede do ISP filtros de gerência da porta 25/TCP.

Cenário: Os endereços das interfaces físicas, o protocolo de roteamento interno e o iBGP já estão configurados.

Outro filtro importante de ser configurado é o que impede a saída de tráfego da rede dos clientes domésticos com destino à porta 25/TCP, com o intuito de evitar o envio de spams. Nesse exercício abordaremos apenas como criar o filtro que impede o encaminhamento de pacotes com destino a porta 25 e não será tratada nenhuma configuração referente ao servidor de e-mail.

1. Este filtro também deve ser configurado o mais próximo a rede dos clientes domésticos atuando apenas sobre as interfaces que conectam este tipo de cliente.

   Para realizar a configuração no roteador mikrotik_cliente execute os seguintes comandos:

```
> /ip firewall filter
  add chain=forward action=drop src-address=0.0.0.0/0 dst-address=0.0.0.0/0 \
dst-port=25 protocol=tcp in-interface=ether3 place-before=0

> /ipv6 firewall filter
  add chain=forward action=drop src-address=::/0 dst-address=::/0 \
dst-port=25 protocol=tcp in-interface=ether3 place-before=0
```

   No roteador juniper os comandos devem ser os seguintes:

```
> edit
# set firewall family inet filter CLIENTES-DOMESTICOS-V4 term PORTA-25 from
address 0.0.0.0/0
# set firewall family inet filter CLIENTES-DOMESTICOS-V4 term PORTA-25 from
protocol tcp
# set firewall family inet filter CLIENTES-DOMESTICOS-V4 term PORTA-25 from
port smtp
# set firewall family inet filter CLIENTES-DOMESTICOS-V4 term PORTA-25 then
discard
# insert firewall family inet filter CLIENTES-DOMESTICOS-V4 term PORTA-25
before term ANTI-SPOOFING

# set firewall family inet6 filter CLIENTES-DOMESTICOS-V6 term PORTA-25 from
address ::/0
# set firewall family inet6 filter CLIENTES-DOMESTICOS-V6 term PORTA-25 from
next-header tcp
# set firewall family inet6 filter CLIENTES-DOMESTICOS-V6 term PORTA-25 from
port smtp
# set firewall family inet6 filter CLIENTES-DOMESTICOS-V6 term PORTA-25 then
discard
# insert firewall family inet6 filter CLIENTES-DOMESTICOS-V6 term PORTA-25
before term ANTI-SPOOFING
# commit
```