Trabalho prático 2

Segurança
2019/2020

David Caneira 2018010614

NAT:

ip nat pool users 193.137.79.1 193.137.79.1 prefix-length 24

ip nat inside source list 1 pool users

ip nat outside (comando colocado na interface FastEthernet 1/1 para a nat “exterior”)

ip nat inside (comando colocado na interface FastEthernet0/0 para a nat “interior”)

Logging:

login block-for 60 attempts 2 within 30

login delay 10

login on-failure log

login on-success log

logging trap notifications

logging 193.137.78.1

Autenticação:

aaa new-model

aaa authorization console

aaa authorization exec default local

aaa authentication login default local group radius

aaa accounting exec default start-stop group radius

radius-server host 193.137.78.1 auth-port 1812 acct-port 1813 key secret

Firewall PC1:

Permissão de operações tcp, udp e icmp do interior para o exterior

Acesso à Internet a partir do PC1 deve estar vedado todos os fins de semana

ip access-list extended f0/0_in

permit ip 192.168.1.0 0.0.0.255 193.137.78.0 0.0.0.255 reflect users_internal timeout 300

deny ip 192.168.1.0 0.0.0.255 any time-range vedado (comando usado para bloquear o acesso à Internet todos os fins de semana. nâo podem ser feitas ligações de dentro para fora e vice-versa)

permit udp 192.168.1.0 0.0.0.255 any reflect users_udp timeout 300

permit icmp 192.168.1.0 0.0.0.255 any reflect users_icmp timeout 300

permit tcp 192.168.1.0 0.0.0.255 any reflect users_tcp timeout 300

deny ip any any

ip access-list extended f0/0_out

evaluate users_internal

evaluate users_tcp

evaluate users_udp

evaluate users_icmp

deny ip any any

O comando "reflect" faz com que quando chega tráfego permitido, o router cria acess-lists para aceitar tráfego de retorno nos pontos evaluate especificados.

Firewall XP e Server:

Portos fechados para o exterior e PC1

Permissão de operações TCP, UDP e ICMP para o exterior

Acesso aos serviços FTP a partir da rede PC1

Deve permitir acesso HTTP, SMTP, POP/IMAP a todo o mundo

Permitir queries DNS a partir do PC1, com portos abertos e funcionais

```
ip access-list extended e1/0_in
 remark XP
 permit udp host 193.137.78.1 any reflect xp_udp timeout 300
 dynamic xptelnet permit icmp host 193.137.78.1 host 8.8.8.8
 deny   icmp host 193.137.78.1 host 8.8.8.8
permit icmp host 193.137.78.1 any reflect xp_icmp timeout 300
 permit tcp host 193.137.78.1 any reflect xp_tcp timeout 300
 remark SRV
 evaluate userstosrv_ftp
 evaluate srv_http
 evaluate srv_smtp
 evaluate srv_pop
 evaluate srv_imap
 evaluate srv_dns
 deny   ip any any
ip access-list extended e1/0_out
 evaluate xp_icmp
 evaluate xp_udp
 evaluate xp_tcp
 remark SRV
 permit tcp 192.168.1.0 0.0.0.255 host 193.137.78.2 eq ftp reflect userstosrv_ftp
timeout 300
```

Anti-spoofing

O tráfego vindo de redes privadas e endereços multicast na interface de entrada de R1 é negado

```
ip access-list extended anti-spoofing
 remark Filtro Anti-spoofing
 deny   ip 193.137.78.0 0.0.0.255 any
 deny   ip 224.0.0.0 15.255.255.255 any
 deny   ip 127.0.0.0 0.255.255.255 any
 deny   ip host 0.0.0.0 any
```

```
deny   ip 10.0.0.0 0.255.255.255 any
deny   ip 172.16.0.0 0.15.255.255 any
deny   ip 192.168.0.0 0.0.255.255 any
permit ip any any
```