Administração de Sistemas

Orlando Sousa

Aula 6

Listas de controlo de acesso (ACLs)
NAT

Listas de controlo de acesso

- Permite filtrar tráfego (efectua testes aos pacotes de dados. Ex: nega ou permite em função do endereço ou tipo de tráfego)
- Permite restringir a utilização da rede para certos serviços e/ou dispositivos
- Cada interface do router, pode ter duas listas de acesso por protocolo, uma para entrada e outra para saída de tráfego
- Não se pode apagar uma linha da ACL (Apenas toda a lista)

REGRAS:

- É efectuado de uma forma sequencial: linha1, linha2, linha3, etc. (Colocar as linhas mais restritivas no topo da lista!)
- A procura é feita até que uma linha faça *matching* (as outras linhas serão ignoradas)
- **Existe um "deny" implícito no fim de todas as listas de acesso** (se não for efectuado *matching* até essa linha, então o pacote de dados será descartado).

Tipos de ACLs

- Standard (1-99, 1300-1999)
  - Usado para filtrar pacotes de uma dada origem (permite ou nega o tráfego a um conjunto de protocolos baseado no endereço de rede/subrede/máquina)
  - Devem ser colocadas o mais próximo possível do “destino”
- Extended (100-199, 2000-2699)
  - Usado para filtrar pacotes baseados na sua origem e destino
  - Filtra pelo tipo de protocolo (Ex: IP, TCP, UDP, etc.) e pelo número da porta
  - Também permite ou nega o tráfego com mais granularidade
  - Devem ser colocadas o mais próximo possível da “origem”

Nota: Também podem ser utilizados nomes para fazer referência às listas (em “substituição” dos números)

Comandos para manuseamento de ACLs

- Standard

Acrescentar uma linha a uma lista:

access-list número-lista {permit | deny} **endereço_origem** {máscara}

Activar uma lista de acesso numa interface do router (para "entrada" ou "saída"):

ip access-group número-lista {in | out}

- Extended

Acrescentar uma linha a uma lista:

access-list número-lista {permit | deny} protocolo **endereço_origem** {máscara} **endereço-destino** {máscara}

Activar uma lista de acesso numa interface do router (para "entrada" ou "saída"):

ip access-group número-lista {in | out}

- Listas com nome

ip access-list standard|extended nome_lista (depois colocar as linhas necessárias para a lista)

ip access-group nome-lista {in | out}

- Remoção de uma lista de acesso:

no access-list número-lista

no ip access-group número-lista in|out (remove uma ACL de uma interface)

- Comandos para consulta de listas:

show ip interfaces

show access-lists [número]

show ip access-list [número]

Máscaras nas ACLs

- São utilizadas para identificar os intervalos de endereços IP. Funcionam de forma contrária às máscaras de subrede (Cada 0 deve fazer *matching*, cada 1 deve ser ignorado).
- Para calcular a máscara da lista faz-se o seguinte:
  - Identificar o valor decimal de cada *byte* da máscara de subrede
  - Subtrair a 255 o valor encontrado

Exemplo: Obter a máscara utilizada numa lista para a máscara de subrede 255.255.248.0

Primeiro byte: 255-255=0
Segundo byte: 255-255=0
Terceiro byte: 255-248=7
Quarto byte: 255-0=255
A máscara a utilizar na lista será: **0.0.7.255**

Nota: Atente aos valores obtidos:
Máscara da subrede (255.255.248.0): **11111111.11111111.11111000.00000000**
Máscara da lista (0.0.7.255): **00000000.00000000.00000111.11111111**

Exemplos: Listas *Standard*

- **Exemplo 1:** Cria uma lista de acesso que permite todo o tráfego excepto da rede 10.0.0.0. A lista é aplicada à interface Ethernet0.

  Router(config)**#access-list 1 deny 10.0.0.0 0.255.255.255**
  Router(config)**#access-list 1 permit any**
  Router(config)**#interface Ethernet0**
  Router(config-if)**#ip access-group 1 out**

- **Exemplo 2:** Rejeita todo o tráfego excepto da máquina 10.12.12.14 e aplica a lista à interface Serial0

  Router(config)**#access-list 2 permit 10.12.12.16**
  Router(config)**#interface Serial0**
  Router(config-if)**#ip access-group 2 in**

Exemplo: Restringir o acesso via telnet ao router

- Numa ligação via telnet ao router, este associa a ligação com uma linha para terminal virtual (VTY). Por defeito suporta 5 telnets (0-4).

```
Router(config)# access-list 99 permit 192.168.1.0 0.0.0.255
Router(config)# line vty 0 4
Router(config-line)# access-class 99 in
```

Neste exemplo, apenas é permitido tráfego da rede 192.168.1.0/24

Exemplos: Listas *Extended*

- **Exemplo 1: Não encaminha tráfego TCP de qualquer host da rede 10.0.0.0 para a rede 11.12.0.0. Aplica a lista à interface Serial0**

```
Router(config)#access-list 111 deny tcp 10.0.0.0 0.255.255.255 11.12.0.0 0.0.255.255
Router(config)#access-list 111 permit ip any any
Router(config)#int Serial0
Router(config-if)#ip access-group 111 in
```

- **Exemplo 2: Esta lista impede todos os *telnets* do host 192.168.1.25**

```
Router(config)# access-list 102 deny tcp host 192.168.1.25 any eq 23
Router(config)# access-list 102 permit tcp any any
```

- **Exemplo 3:**

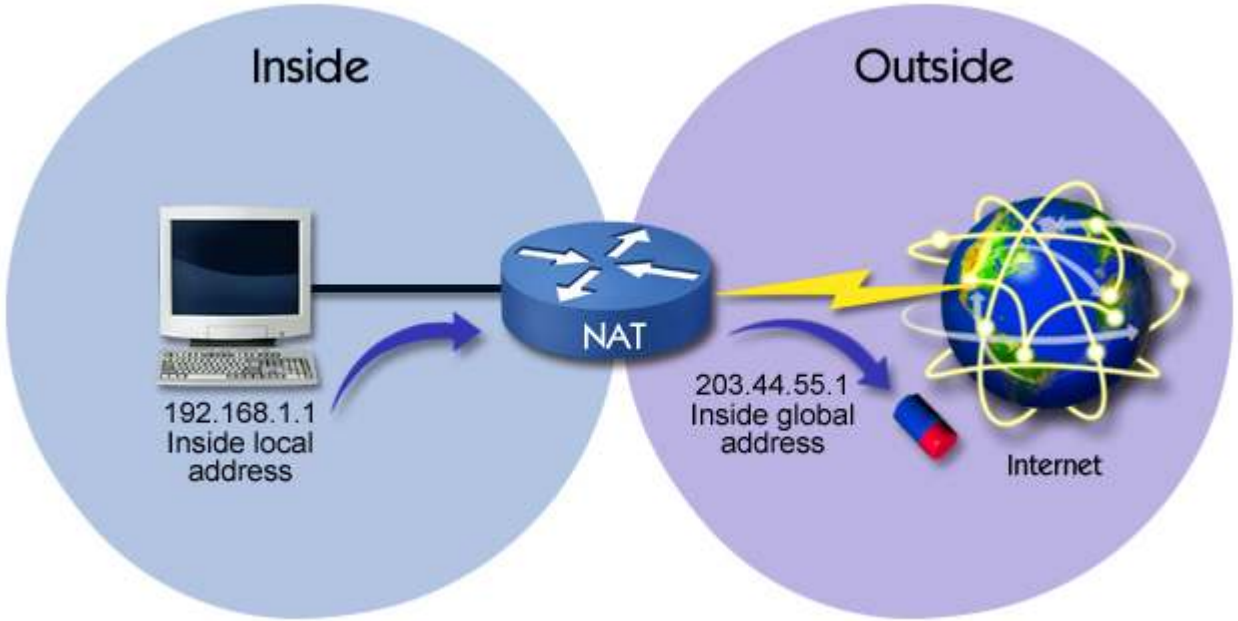
```
Router(config)# access-list 101 permit tcp
        host 199.199.199.1
        host 200.200.200.1 eq dns
Router(config)# access-list 101 permit udp
        any host 200.200.200.1 eq dns
Router(config)# access-list 101 permit tcp
        any host 200.200.200.2 eq www
Router(config)# access-list 101 permit icmp
        any 200.200.200.0 0.0.0.255
Router(config)# access-list 101 permit tcp
        any host 200.200.200.3 eq smtp
Router(config)# access-list 101 permit udp
        host 201.201.201.2
        host 201.201.201.1 eq rip
Router(config)# interface Ethernet0
Router(config-if)# ip address 201.201.201.1 255.255.255.0
Router(config-if)# ip access-group 101 in
```

Exemplo: ACL com nome

```
Router(config)# ip access-list extended fica_de_fora
Router(config-ext-acl)# permit tcp
                        any 172.16.0.0 0.0.255.255
                        established log
Router(config-ext-acl)# permit udp
                        any host 172.16.1.1 eq dns log
Router(config-ext-acl)# permit tcp
                        172.17.0.0 0.0.255.255
                        host 176.16.1.2 eq telnet log
Router(config-ext-acl)# permit icmp
                        any 176.16.0.0 0.0.255.255
                        echo-reply log
Router(config-ext-acl)# deny ip any any log
Router(config)# interface Ethernet0
Router(config-if)# ip access-group fica_de_fora
```

NAT (Network Address Translation)

- Permite ligar uma rede privada à Internet. Não necessita de um endereço IP "público" para cada máquina
- O Router transforma o endereço privado num endereço público e vice-versa
- Situações mais comuns de utilização:
  - É necessário utilizar endereços privados já que o ISP não forneceu IPs suficientes
  - Estando a usar endereços públicos, muda-se de ISP e o novo ISP não suporta os endereços actuais
  - A fusão de empresas/departamentos que estão a usar o mesmo espaço de endereçamento
  - Necessita "dar" o mesmo IP a várias máquinas, de modo a que do exterior sejam vistas como "uma" (ex: para balanceamento de carga)



Tipos de NAT

- Endereços privados
  - Classe A: 10.0.0.0-10.255.255.255
  - Classe B: 172.16.0.0-172.31.255.255
  - Classe C: 192.168.0.0-192.168.255.255

Tipos de NAT:

- **Estático:** Cada ip interno é associado a um ip público. O mapeamento é manual
- **Dinâmico:** O mapeamento é automático. O router tem uma *pool* de endereços para efectuar o mapeamento
- **Overload with PAT(Port Address Translation)**: Um único endereço público pode estar associado a vários endereços privados. A “separação” é feita através da utilização de uma porta para cada *host*.

Comandos NAT Estático

Router(config)# **ip nat inside source static** Endereço_Interno Endereço_público

Router(config)# **ip nat outside source static** Endereço_público Endereço_interno

Definir as interfaces "inside" e "outside":

Router(config)# **interface** type [slot_#/]port_#
Router(config-if)# **ip nat inside|outside**

Comandos de consulta:

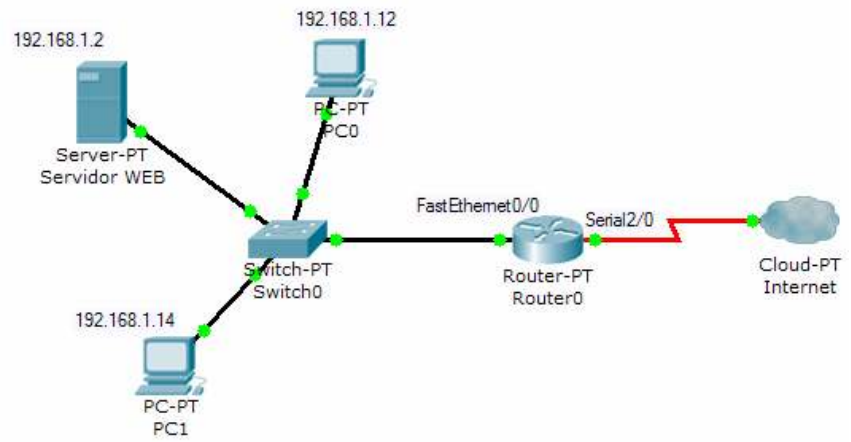
show ip nat translations

show ip nat statistics

debug ip nat

Exemplo

Router(config)# **ip nat inside source static**
192.168.1.2 200.200.200.1
Router(config)# **interface FastEthernet0/0**
Router(config-if)# **ip nat inside**
Router(config-if)# **exit**
Router(config)# **interface Serial2/0**
Router(config-if)# **ip nat outside**



Comandos NAT Dinâmico

1-Definir os endereços internos que usarão NAT:

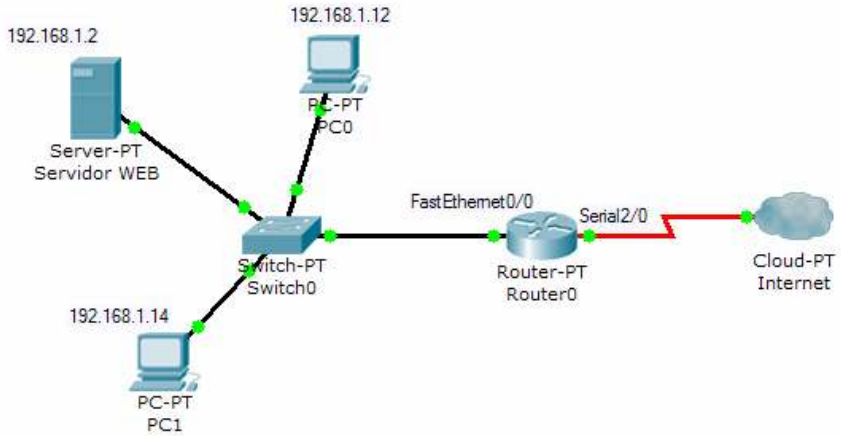
Router(config)# **ip nat inside source**
list número_lista_standard(ACL)
pool nome_da_pool

2- Criar a pool de endereços públicos a usar:

Router(config)# **ip nat pool** nome_da_pool
Endereço_público_inicial
Endereço_público_final
netmask máscara_subrede

Exemplo (Configuração de NAT dinâmico para os dois PCs)

Router(config)# **ip nat inside source list 1 pool minha-pool**
Router(config)# **access-list 1 permit 192.168.1.12 0.0.0.0**
Router(config)# **access-list 1 permit 192.168.1.14 0.0.0.0**
Router(config)# **ip nat pool minha-pool 200.200.200.2**
200.200.200.3 netmask 255.255.255.0
Router(config)# **interface FastEthernet0/0**
Router(config-if)# **ip nat inside**
Router(config-if)# **exit**
Router(config)# **interface Serial2/0**
Router(config-if)# **ip nat outside**



Comandos PAT

1-Definir os endereços internos que usarão NAT:

Router(config)# **ip nat inside source**
list número_lista_standard(ACL)
pool nome_da_pool **overload**

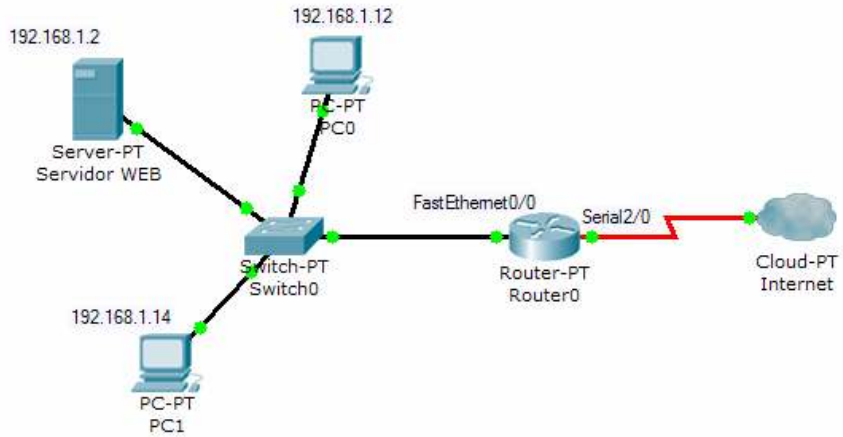
2- Criar a pool de endereços públicos a usar:

Router(config)# **ip nat pool** nome_da_pool
Endereço_público_inicial
Endereço_público_final
netmask máscara_subrede

Nota: Pode-se utilizar mais do que um endereço. Se for apenas utilizado 1, então tem de utilizar o mesmo no “inicio” e no “fim”.

Exemplo

Router(config)# **ip nat inside source list 1 pool**
minha-pool overload
Router(config)# **access-list 1 permit 192.168.1.12 0.0.0.0**
Router(config)# **access-list 1 permit 192.168.1.14 0.0.0.0**
Router(config)# **ip nat pool minha-pool 200.200.200.2**
200.200.200.2
netmask 255.255.255.0
Router(config)# **interface FastEthernet0/0**
Router(config-if)# **ip nat inside**
Router(config-if)# **exit**
Router(config)# **interface Serial2/0**
Router(config-if)# **ip nat outside**



Distribuição de carga

Permite distribuir a carga por várias máquinas.

1- Definir os endereços dos dispositivos que oferecem o serviço:

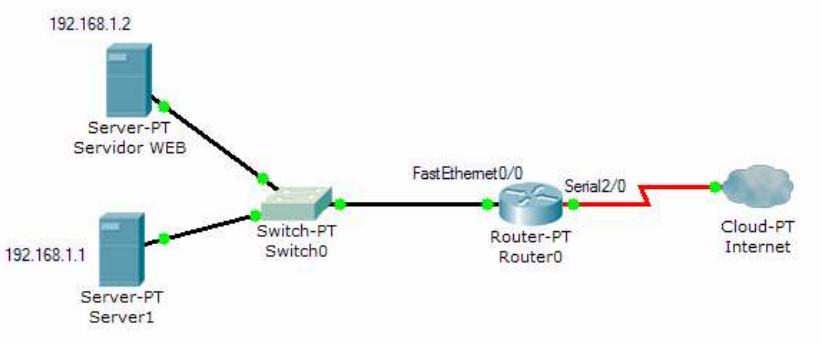
Router(config)# ip nat pool nome_da_pool
Endereço_Inicial
Endereço_final
prefix-length tamanho_máscara_subrede
type rotary

2- Definir os endereços públicos dos dispositivos que são usados para aceder ao serviço:

Router(config)# ip nat inside destination
list número_lista_standard pool nome_da_pool

Exemplo (As respostas aos pedidos efectuados para 200.200.200.1 são efectuadas por dois servidores: 192.168.1.1 e 192.168.1.2)

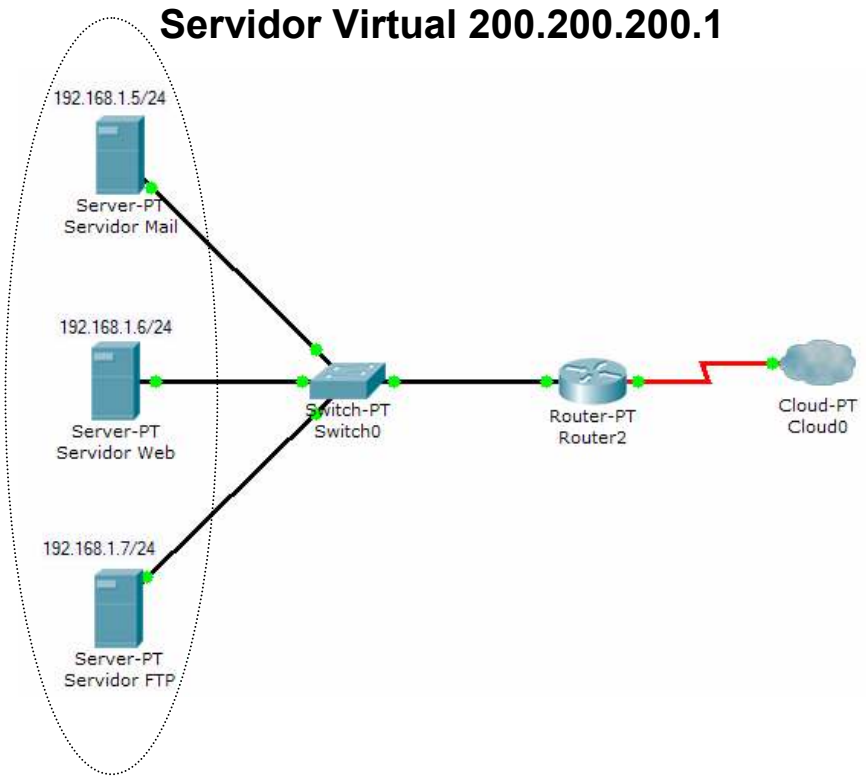
Router(config)# **ip nat pool servidores-web**
192.168.1.1 192.168.1.2
prefix-length 24 type rotary
Router(config)# **ip nat inside destination list 1**
pool servidores-web
Router(config)# **access-list 1 permit 200.200.200.1**
Router(config)# **interface FastEthernet0/0**
Router(config-if)# **ip nat inside**
Router(config-if)# **exit**
Router(config)# **interface Serial2/0**
Router(config-if)# **ip nat outside**



Redireccionamento de portas

- Utiliza PAT estático
- Um “servidor virtual” é usado para aceder a vários servidores/serviços (que podem estar na mesma máquina e/ou em máquinas diferentes)
- Cada servidor/serviço utiliza uma porta diferente

Exemplo




```
Router(config)# ip nat inside source static tcp 192.168.1.6 80  200.200.200.1 80
Router(config)# ip nat inside source static tcp 192.168.1.7 21  200.200.200.1 21
Router(config)# ip nat inside source static tcp 192.168.1.7 20  200.200.200.1 20
Router(config)# ip nat inside source static tcp 192.168.1.5 25  200.200.200.1 25
Router(config)# interface FastEthernet0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface Serial2/0
Router(config-if)# ip nat outside
```

Bibliografia

IBM Redbook : TCP/IP Tutorial and Technical Overview
http://www.redbooks.ibm.com/abstracts/gg243376.html

Internetworking Technology Handbook
http://www.cisco.com/en/US/tech/tk1330/tsd_technology_support_technical_reference_book09186a00807594e5.html

Access Control Lists and IP Fragments
http://www.cisco.com/en/US/tech/tk1330/tsd_technology_support_technical_reference_book09186a00807594e5.html

How Network Address Translation Works
http://computer.howstuffworks.com/nat.htm/printable