CHƯƠNG 4
ACL, NAT/PAT, IPTABLES

THS. TRẦN THỊ DUNG
DUNGTT@UIT.EDU.VN

1

NỘI DUNG

- Khái niệm access list
- Cơ chế hoạt động của ACL
- Phương pháp cấu hình ACL
- Các phương pháp ánh xạ địa chỉ
- Iptables trong Linux

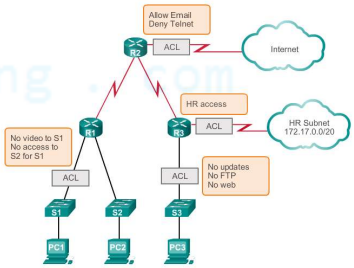
2

Khái niệm ACL

- ACL là một danh sách các dòng cho phép hay cấm các gói tin ra/vào một router.
- ACL phân tích các gói tin đến và đi để tiến hành chuyển tiếp hoặc hủy gói tin dựa trên các tiêu chí như địa chỉ IP nguồn/đích, giao thức.
- Hay còn gọi là Packet filtering

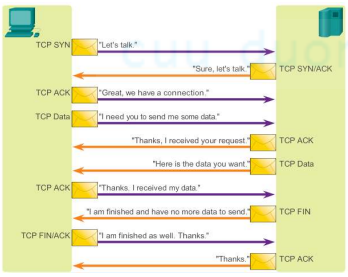
3

Khái niệm ACL



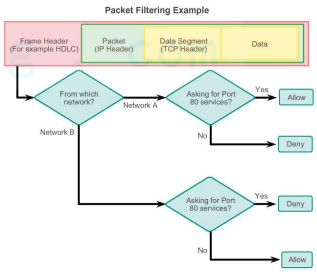
4

Một TCP Conversation



5

Ví dụ



6

NỘI DUNG

- Khái niệm access list
- Cơ chế hoạt động của ACL
- Phương pháp cấu hình ACL
- Các phương pháp ánh xạ địa chỉ
- Iptables trong Linux

7

Hoạt động của ACL

Inbound ACL

Lọc những gói tin đến một interface của router, trước khi router định tuyến đến một interface khác

Outbound ACL

Lọc những gói tin sau khi router định tuyến/chuyển tiếp ra một interface

8

Các loại ACL trên thiết bị Cisco

ACL chuẩn - Standard ACLs

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Standard ACLs filter IP packets based on the source address only.

ACL mở rộng - Extended ACLs

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

Extended ACLs filter IP packets based on several attributes, including the following:
- Source and destination IP addresses
- Source and destination TCP and UDP ports
- Protocol type/ Protocol number (example: IP, ICP, UDP, TCP, etc.)

9

Hoạt động của Inbound ACL

Nếu inbound ACL được đặt tại một interface, các gói tin sẽ được kiểm tra trước khi được định tuyến.

Nếu một gói tin phù hợp với một dòng ACL có kết quả là permit thì gói tin đó sẽ được định tuyến.

Nếu một gói tin phù hợp với một dòng ACL có kết quả là deny, router sẽ hủy gói tin đó.

Nếu một gói tin không phù hợp các dòng của ACL, nó sẽ được hiểu là "implicitly denied" và bị hủy.

10

Hoạt động của Outbound ACL

Gói tin được định tuyến trước khi được đưa đến interface để ra khỏi router.

Nếu outbound interface không có ACL, gói tin sẽ được đẩy ra khỏi interface đó.

Nếu outbound interface có ACL, gói tin sẽ được kiểm tra trước khi bị đẩy ra khỏi interface đó.

Nếu một gói tin phù hợp với một dòng ACL có kết quả là permit thì gói tin đó sẽ được đẩy ra khỏi interface.

11

Hoạt động của Outbound ACL

Nếu một gói tin phù hợp với một dòng ACL có kết quả là deny, gói tin bị hủy.

Nếu một gói tin không phù hợp các dòng của ACL, nó sẽ được hiểu là "implicitly denied" và bị hủy.

12

Hoạt động của standard ACL

Standard ACLs chỉ kiểm tra địa chỉ nguồn và không kiểm tra các phần còn lại

13

Hoạt động của Extended ACL

The ACL kiểm tra địa chỉ nguồn, số port nguồn, và giao thức trước sau đó mới đến địa chỉ đích, port đích để ra quyết định là permit hay deny.

14

Wildcard Masks in ACLs

Giới thiệu về ACL Wildcard Mask

- Wildcard masks là một chuỗi 32 bit để xác định phần địa chỉ IP phù hợp với yêu cầu matching:
  - Wildcard mask bit 0 – so sánh với các bit trong địa chỉ IP.
  - Wildcard mask bit 1 – bỏ qua phần bit trong địa chỉ IP.

15

Ví dụ Wildcard Mask

Example 1

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.	00000000.00000000.00000000.00000000
Result	192.168.1.1	11000000.10101000.00000001.00000001

Example 2

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	255.255.255.255	11111111.11111111.11111111.11111111
Result	0.0.0.0	00000000.00000000.00000000.00000000

Example 3

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.255	00000000.00000000.00000000.11111111
Result	192.168.1.0	11000000.10101000.00000001.00000000

16

Ví dụ Wildcard Mask

Example 1

	Decimal	Binary
IP Address	192.168.16.0	11000000.10101000.00010000.00000000
Wildcard Mask	0.0.15.255	00000000.00000000.00001111.11111111
Result Range	192.168.16.0 to 192.168.31.255	11000000.10101000.00010000.00000000 to 11000000.10101000.00011111.11111111

Example 2

	Decimal	Binary
IP Address	192.168.1.0	11000000.10101000.00000001.00000000
Wildcard Mask	0.0.254.255	00000000.00000000.11111110.11111111
Result	192.168.1.0	11000000.10101000.00000001.00000000
	All odd numbered subnets in the 192.168.0.0 major network	

17

Cách tính Wildcard mask

Cách dễ nhất là lấy 255.255.255.255 trừ subnet mask.

Example 1

```
  255.255.255.255
- 255.255.255.000
  000.000.000.255
```

Example 2

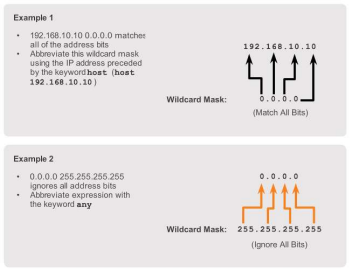
```
  255.255.255.255
- 255.255.255.240
  000.000.000.015
```

Example 3

```
  255.255.255.255
- 255.255.252.000
  000.000.003.255
```

18

Wildcard Mask Keywords



19

Ví dụ Wildcard Mask Keywords

Example 1:

```
R1(config)#access-list 1 permit 0.0.0.0 255.255.255.255
R1(config)#access-list 1 permit any
```

Example 2:

```
R1(config)#access-list 1 permit 192.168.10.10 0.0.0.0
R1(config)#access-list 1 permit host 192.168.10.10
```

20

Hướng dẫn tạo ACLs

- Sử dụng tại router ở giữa internal network và external network như mạng Internet.
- Sử dụng tại router ở giữa 2 network mà mình cần phải kiểm soát việc truy cập dữ liệu.
- Cấu hình ACL tại các router biên.

21

Hướng dẫn tạo ACLs

- Một ACL/protocol – IPv4/IPv6.
- Một ACL/direction - ACLs kiểm soát một hướng tại một interface => cần có 2 ACL nếu muốn kiểm soát dữ liệu trên cả 2 hướng ra/vào một interface.
- Một ACL/interface - ACLs kiểm soát một interface, ví dụ GigabitEthernet 0/0.

22

Hướng dẫn tạo ACLs

Guideline	Benefit
Base your ACLs on the security policy of the organization.	This will ensure you implement organizational security guidelines.
Prepare a description of what you want your ACLs to do.	This will help you avoid inadvertently creating potential access problems.
Use a text editor to create, edit and save ACLs.	This will help you create a library of reusable ACLs.
Test your ACLs on a development network before implementing them on a production network.	This will help you avoid costly errors.

23

Vị trí đặt ACLs trên router

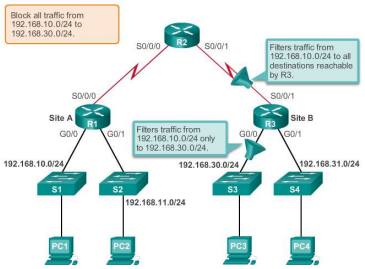
Extended ACLs – gần nguồn.

Standard ACLs – gần đích.

Ngoài ra có thể phụ thuộc vào: sự kiểm soát của admin, băng thông và dễ dàng cấu hình hay không.

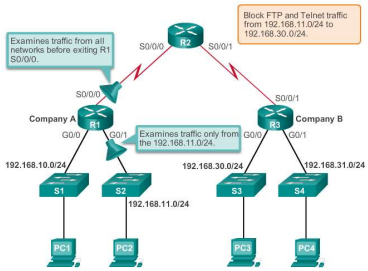
24

Ví dụ: Vị trí của Standard ACL



25

Ví dụ: Vị trí của Extended ACL



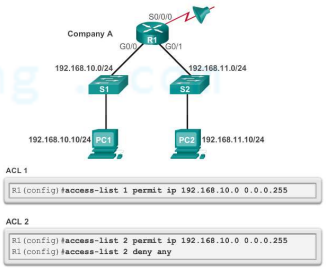
26

NỘI DUNG

- Khái niệm access list
- Cơ chế hoạt động của ACL
- Phương pháp cấu hình ACL
- Các phương pháp ánh xạ địa chỉ
- Iptables trong Linux

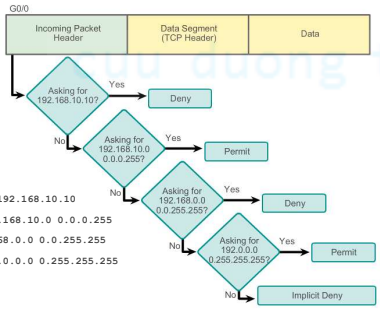
27

Cấu hình Standard ACL



28

Cấu hình Standard ACL



Example ACL

```
access-list 2 deny host 192.168.10.10
access-list 2 permit 192.168.10.0 0.0.0.255
access-list 2 deny 192.168.0.0 0.0.255.255
access-list 2 permit 192.0.0.0 0.255.255.255
```

29

Cấu hình tạo Standard ACL

Cú pháp câu lệnh hoàn chỉnh:

- `Router(config)# access-list access-list-number deny permit remark source [ source-wildcard ] [ log ]`

Để xóa ACL, sử dụng câu lệnh **`no access-list`**.

30

Áp dụng Standard ACLs vào interface

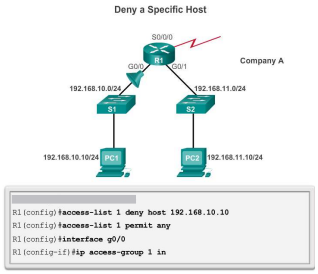
Sau khi tạo ACL, nó cần được đặt vào một interface theo chiều in/out với câu lệnh **ip access-group** trong mode interface:

```
Router(config-if)# ip access-group { access-list-number | access-list-name } { in | out }
```

Để bỏ ACL ra khỏi interface, sử dụng câu lệnh **no ip access-group**

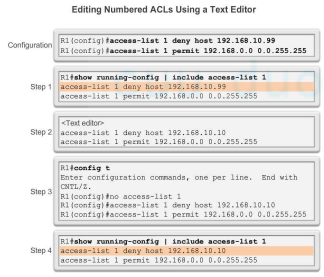
31

Cấu hình Standard ACL hoàn chỉnh



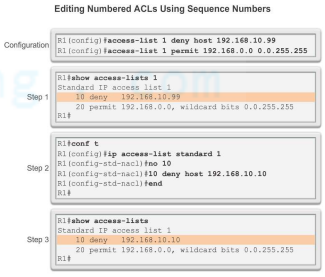
32

Thay đổi Standard ACL



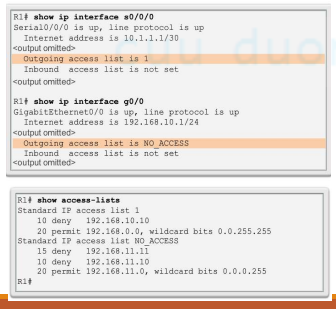
33

Thay đổi Standard ACL



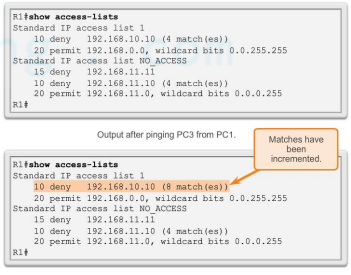
34

Kiểm tra ACLs



35

Kiểm tra ACL



36

Securing VTY ports with a Standard IPv4 ACL

Configuring a Standard ACL to Secure a VTY Port

Filtering Telnet or SSH traffic is typically considered an extended IP ACL function because it filters a higher level protocol. However, because the **access-class** command is used to filter incoming or outgoing Telnet/SSH sessions by source address, a standard ACL can be used.

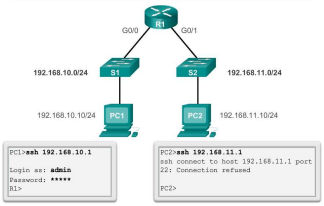
```
Router(config-line)# access-class access-list-number { in [ vrf-also ] | out }
```

37

Securing VTY ports with a Standard IPv4 ACL

Verifying a Standard ACL used to Secure a VTY Port

```
R1#show access-lists
Standard IP access list 21
    10 permit 192.168.10.0, wildcard bits 0.0.0.255 (2 matches)
    20 deny   any (1 match)
R1#
```




```
PC1>ssh 192.168.10.1

Login as: admin
Password: *****
R1>
```

```
PC2>ssh 192.168.11.1
ssh connect to host 192.168.11.1 port
22: Connection refused

PC2>
```

38

Extended ACLs

Extended ACLs can filter on:

- Source address
- Destination address
- Protocol
- Port numbers

39

Extended ACLs

Using Port Numbers

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

Using Keywords

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

40

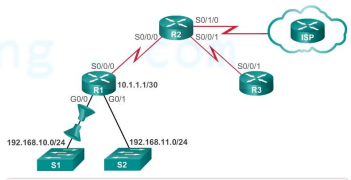
Cấu hình Extended ACLs

Phương pháp cấu hình tương tự Standard ACL nhưng cú pháp phức tạp hơn.

```
access-list access-list-number {deny | permit | remark}
protocol source [source-wildcard] [operator operand]
[port port-number or name] destination [destination-wildcard]
[operator operand] [port port-number or name][established]
```

41

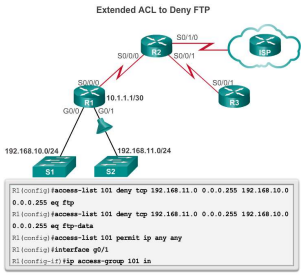
Áp dụng Extended ACLs vào Interfaces




```
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)#access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)#interface g0/0
R1(config-if)#ip access-group 103 in
R1(config-if)#ip access-group 104 out
```

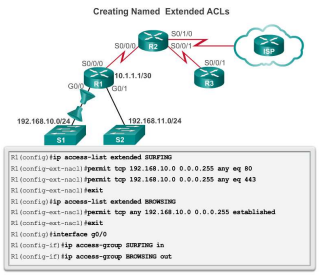
42

Ví dụ cấu hình Extended ACLs



43

Cấu hình Đặt tên Extended ACLs



44

Kiểm tra Extended ACLs

```
R1#show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
R1#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<output omitted for brevity>
  Outgoing access list is BROWSING
  Inbound  access list is SURFING
<output omitted for brevity>
```

45

Thay đổi Extended ACLs

Một extended ACL có thể được thay đổi với 2 phương pháp:

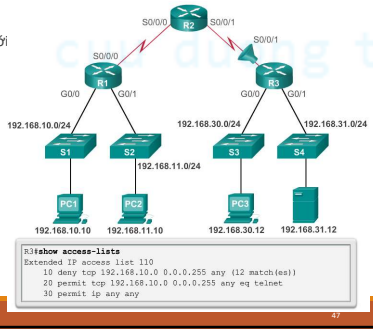
1 - Text editor

2 – Sequence numbers

46

Ví dụ cấu hình ACLs sai - 1

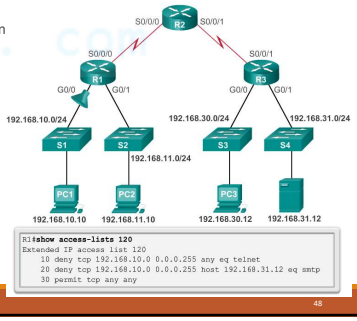
Host 192.168.10.10 không kết nối được với 192.168.30.12.



47

Ví dụ cấu hình ACLs sai - 2

Mạng 192.168.10.0 /24 không thể dung TFTP đến mạng 192.168.30.0 /24

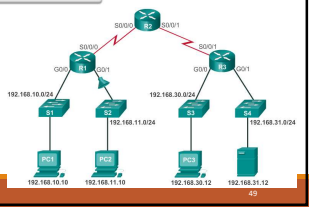


48

Ví dụ cấu hình ACLs sai - 3

Mạng 192.168.11.0 /24 có thể Telnet đến 192.168.30.0 /24 nhưng đúng ra là không được phép.

```
R1#show access-lists 130
Extended IP access list 130
    10 deny tcp any eq telnet any
    20 deny tcp 192.168.11.0 0.0.0.255 host 192.168.31.12 eq smtp
    30 permit tcp any any (12 match(es))
```

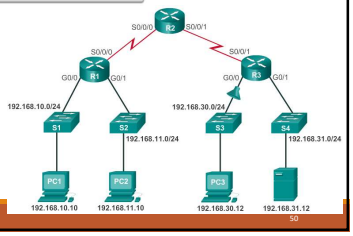


49

Ví dụ cấu hình ACLs sai - 4

192.168.30.12 có thể Telnet đến 192.168.31.12, nhưng đúng ra là không được phép.

```
R3#show access-lists 140
Extended IP access list 140
    10 deny tcp host 192.168.30.1 any eq telnet
    20 permit ip any any (5 match(es))
```



50

NỘI DUNG

- Khái niệm access list
- Cơ chế hoạt động của ACL
- Phương pháp cấu hình ACL
- Các phương pháp ánh xạ địa chỉ
- Iptables trong Linux

51

Khái niệm về NAT

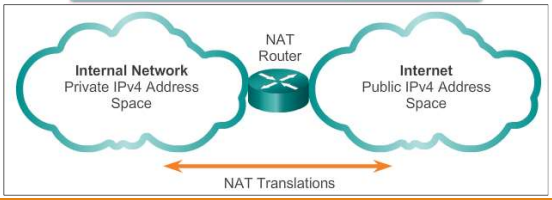
- Được thiết kế để tiết kiệm địa chỉ IP
- Cho phép mạng nội bộ sử dụng địa chỉ IP private
- Địa chỉ IP private sẽ được chuyển đổi sang địa chỉ IP public để có thể được định tuyến trên Internet
- Mạng riêng được tách biệt và giấu kín IP nội bộ.
- Thường sử dụng trên router biên của mạng một cửa.

52

Khái niệm về NAT (tt.)

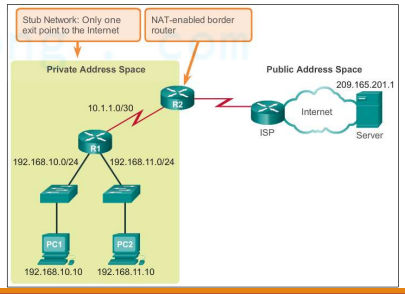
Private Internet addresses are defined in RFC 1918:

Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16



53

Khái niệm về NAT (tt.)



54

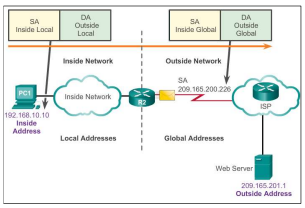
Các thuật ngữ về NAT

Inside network là tập hợp cacs thiết bị sử dụng IP private

Outside network là tất cả các mạng bên ngoài khác.

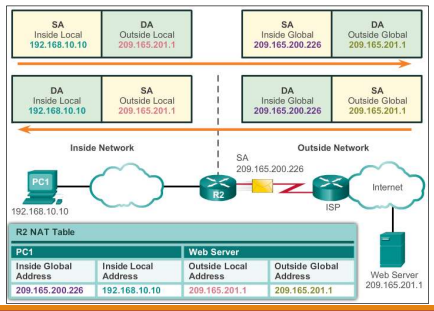
NAT bao gồm 4 loại địa chỉ:

- Inside local address
- Inside global address
- Outside local address
- Outside global address



55

Các thuật ngữ về NAT (tt.)



56

Các loại NAT

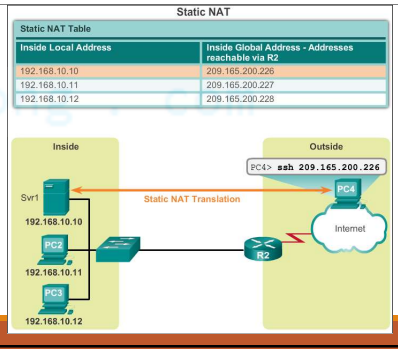
Static NAT

- Static NAT là ánh xạ một – một giữa địa chỉ local và địa chỉ global.
- Loại ánh xạ này được cấu hình bởi admin và thường cố định, không đổi.
- Static NAT rất có ích khi trong một mang có một server và server này có thể được truy cập từ bên ngoài..
- Admin có thể truy cập từ đến server sử dụng SSH trỏ đến địa chỉ global của server.

57

Các loại NAT

Static NAT (tt.)



58

Các loại NAT

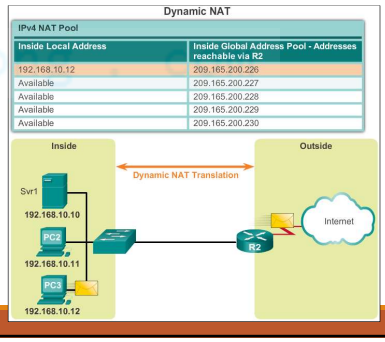
Dynamic NAT

- Dynamic NAT sử dụng một dải địa chỉ public và gán cho các máy bên trong mạng inside theo kiểu first-come, first-served.
- Khi một thiết bị bên mạng inside yêu cầu truy cập ra bên ngoài, Dynamic NAT gán cho nó một địa chỉ public có trong dải địa chỉ.
- Dynamic NAT yêu cầu phải có đủ địa chỉ public để có thể đáp ứng với số lượng user trong mạng inside.

59

Các loại NAT

Dynamic NAT (tt.)



60

Các loại NAT

Port Address Translation

- Port Address Translation (PAT) có thể ánh xạ nhiều địa chỉ IP private sang một địa chỉ IP public.
- PAT sử dụng thêm port nguồn để phân biệt các luồng dữ liệu của các client khác nhau trong mạng internal.

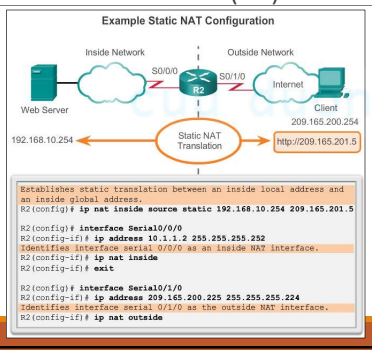
61

Cấu hình Static NAT

- 2 bước cơ bản để cấu hình static NAT:
  - Tạo ánh xạ giữa địa chỉ inside và địa chỉ outside .
  - Xác định interface nào thuộc về mạng inside, interface nào thuộc outside.

62

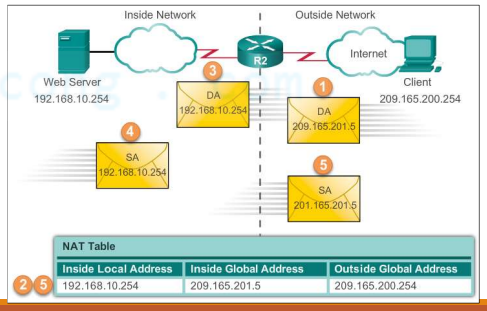
Cấu hình Static NAT (tt.)




```
Establishes static translation between an inside local address and
an inside global address.
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5

R2(config)# interface Serial0/0/0
R2(config-if)# ip address 10.1.1.2 255.255.255.252
Identifies interface serial 0/0/0 as an inside NAT interface.
R2(config-if)# ip nat inside
R2(config-if)# exit

R2(config)# interface Serial0/1/0
R2(config-if)# ip address 209.165.200.225 255.255.255.224
Identifies interface serial 0/1/0 as the outside NAT interface.
R2(config-if)# ip nat outside
```

63

Cấu hình Static NAT (tt.)



64

Kiểm tra Static NAT

The static translation is always present in the NAT table.

```
R2# show ip nat translations
Pro Inside global  Inside local   Outside local  Outside global
--- 209.165.201.5  192.168.10.254  ---            ---
R2#
```

The static translation during an active session.

```
R2# show ip nat translations
Pro Inside global Inside local   Outside local    Outside global
--- 209.165.201.5 192.168.10.254 209.165.200.254  209.165.200.254
R2#
```

65

Configuring Static NAT

Kiểm tra Static NAT (tt.)

```
R2# clear ip nat statistics

R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0
Hits: 0  Misses: 0
<output omitted>
```

Client PC establishes a session with the web server

```
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 2, occurred 00:00:14 ago
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0
Hits: 5  Misses: 0
<output omitted>
```

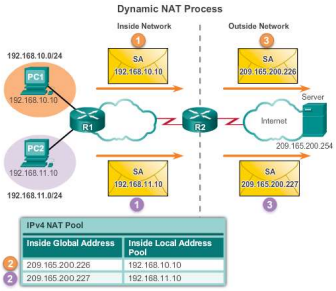
66

Cấu hình Dynamic NAT

Dynamic NAT Configuration Steps	
Step 1	Define a pool of global addresses to be used for translation. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
Step 2	Configure a standard access list permitting the addresses that should be translated. **access-list** *access-list-number* **permit** *source* [*source-wildcard*]
Step 3	Establish dynamic source translation, specifying the access list and pool defined in prior steps. **ip nat inside source list** *access-list-number* **pool** *name*
Step 4	Identify the inside interface. **interface** *type number* **ip nat inside**
Step 5	Identify the outside interface. **interface** *type number* **ip nat outside**

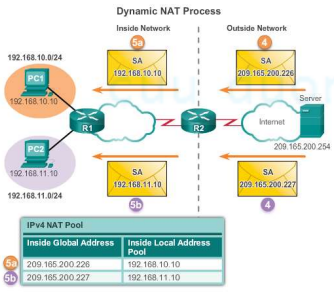
67

Cấu hình Dynamic NAT (tt.)



68

Cấu hình Dynamic NAT (tt.)



69

Kiểm tra Dynamic NAT

Verifying Dynamic NAT with show ip nat translations

```
R2# show ip nat translations
Pro Inside global     Inside local  Outside local Outside global
--- 209.165.200.226  192.168.10.10 ---           ---
--- 209.165.200.227  192.168.11.10 ---           ---
R2#
R2# show ip nat translations verbose
Pro Inside global     Inside local  Outside local Outside global
--- 209.165.200.226  192.168.10.10 ---           ---
    create 00:17:25, use 00:01:54 timeout:86400000, left
23:58:05, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 32, lc_entries: 0
--- 209.165.200.227    192.168.11.10      ---     ---
    create 00:17:22, use 00:01:51 timeout:86400000, left
23:58:08, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 34, lc_entries: 0
R2#
```

70

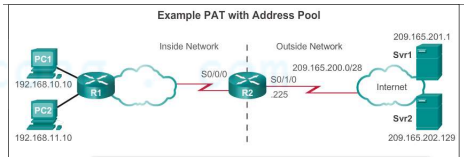
Kiểm tra Dynamic NAT (tt.)

Verifying Dynamic NAT with show ip nat statistics

```
R2# clear ip nat statistics

PC1 and PC2 establish sessions with the server

R2# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 0 extended)
Peak translations: 6, occurred 00:27:07 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 4
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NAT-POOL1 refcount 2
 pool NAT-POOL1: netmask 255.255.255.224
start 209.165.200.226 end 209.165.200.240
type generic, total addresses 15, allocated 2 (13%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
R2#
```

71

Cấu hình PAT: Address Pool



Define a pool of public IPv4 addresses under the pool name NAT-POOL2.
R2(config)# **ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask 255.255.255.224**
Define which addresses are eligible to be translated.
R2(config)# **access-list 1 permit 192.168.0.0 0.0.255.255**
Bind NAT-POOL2 with ACL 1.
R2(config)# **ip nat inside source list 1 pool NAT-POOL2 overload**

Identify interface serial 0/0/0 as an inside NAT interface.
R2(config)# **interface Serial0/0/0**
R2(config-if)# **ip nat inside**

Identify interface serial 0/1/0 as the outside NAT interface.
R2(config)# **interface Serial0/1/0**
R2(config-if)# **ip nat outside**

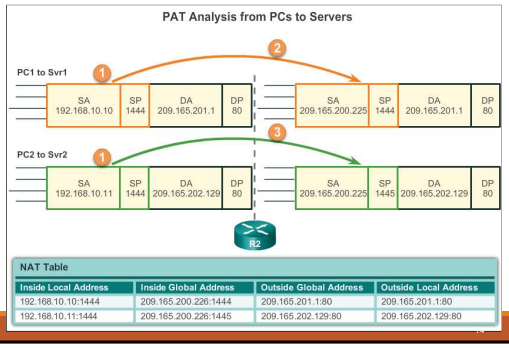
72

Cấu hình PAT: Single Address

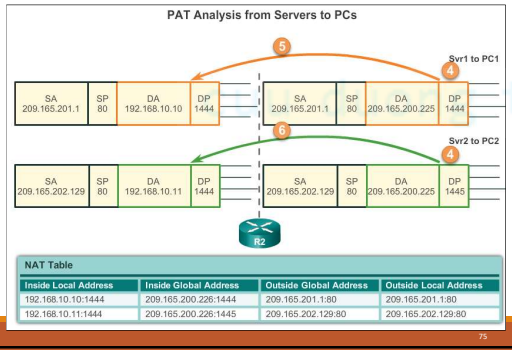
Step 1	Define a standard access list permitting the addresses that should be translated. **access-list** *access-list-number* **permit** *source* [*source-wildcard*]
Step 2	Establish dynamic source translation, specifying the ACL, exit interface and overload options. **ip nat inside source list** *access-list-number* **interface** *type number* **overload**
Step 3	Identify the inside interface. **interface** *type number* **ip nat inside**
Step 4	Identify the outside interface. **interface** *type number* **ip nat outside**

73

Phân tích PAT



Phân tích PAT (tt.)



75

Kiểm tra PAT

Verifying PAT Translations

```
R2# show ip nat translations
Pro Inside global          Inside local       Outside local      Outside global
tcp 209.165.200.226:51839  192.168.10.10:51839 209.165.201.1:80   209.165.201.1:80
tcp 209.165.200.226:42558  192.168.11.10:42558 209.165.202.129:80 209.165.202.129:80
R2#
```

76

NỘI DUNG

- Khái niệm access list
- Cơ chế hoạt động của ACL
- Phương pháp cấu hình ACL
- Các phương pháp ánh xạ địa chỉ
- Iptables trong Linux

77

Iptables là gì?

- Là một thành phần mặc định có chức năng như một firewall trong hệ điều hành Linux
- Iptables gồm 2 phần:
  - Netfilter trong kernel
  - Iptales ở user space: chịu trách nhiệm giao tiếp giữa người dùng và netfilter

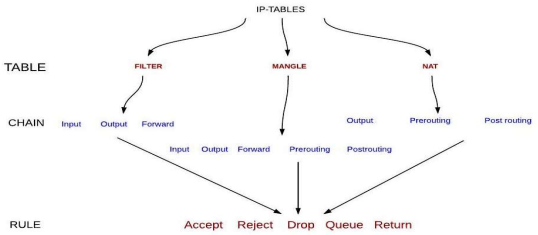
78

Chức năng của Iptables

- Sử dụng làm firewall cho cho các dịch vụ mạng như: mail server , web server , DNS server.
- Triển khai NAT
- Có khả năng phân tích packet một cách hiệu quả , cho phép firewall theo dõi kết nối có liên quan
- Tính năng lọc gói (packet filtering) dựa trên các thành phần của các Header. Từ đó giúp hệ thống ngăn chặn các cuộc tấn công từ bên ngoài và bảo mật hệ thống nội bộ.

79

Hoạt động của Iptables



80

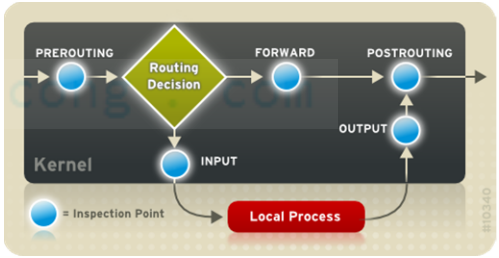
Hoạt động của Iptables (tt.)

Iptable tổ chức phân loại dựa theo cách thức xử lý gói tin. Các gói tin này được xử lý qua các **Bảng** (trong mỗi bảng có phân biệt dạng gói tin đi vào- INPUT, đi ra- OUTPUT hoặc chuyển tiếp- Forward hay cách thức biến đổi địa chỉ nguồn, đích- PREROUTING, POSTROUTING,... và người ta gọi nó là chain. Trong mỗi chain sẽ có những luật- rule để quyết định xử lý gói tin như thế nào: cho phép-accept, từ chối-reject, bỏ đi-drop,...). Trong thực tế bảng FILTER và NAT được sử dụng nhiều nhất.

- FILTER: lọc gói tin vào ra trên Server (đóng vai trò như một firewall)
- NAT: cho ánh xạ 1 địa chỉ IP thành nhiều
- MANGLE: biến đổi Type of Service bits trên header của gói tin TCP

81

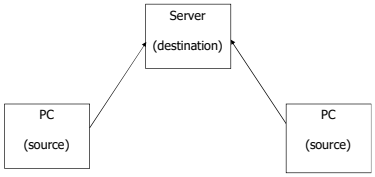
Hoạt động của Iptables (tt.)



82

CÁC LOẠI CHAIN TRONG BẢNG FILTER

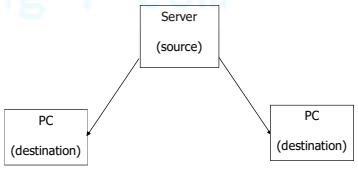
INPUT: gói tin đi từ máy bất kỳ nào vào Server.



83

CÁC LOẠI CHAIN TRONG BẢNG FILTER (tt.)

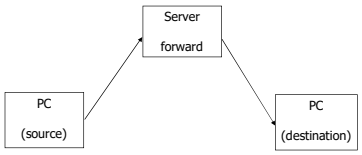
OUTPUT: gói tin đi từ Server đến máy bất kỳ nào.



84

CÁC LOẠI CHAIN TRONG BẢNG FILTER (tt.)

FORWARD: gói tin đi vào 1 card mạng này của Server và được chuyển qua card mạng khác (cũng trên server đó) để đi ra 1 mạng khác.



85

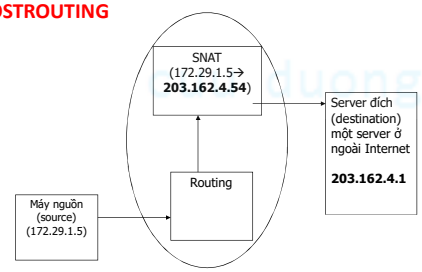
CÁC LOẠI CHAIN TRONG BẢNG NAT

- **POSTROUTING:** Thực hiện việc NAT sau khi gói tin đã đi qua bộ định tuyến (routing) của Server (hay còn gọi là SNAT – Source NAT).
  - Trong đó, **MASQUERADE** là trường hợp đặc biệt của SNAT, dùng trong trường hợp IP public thay đổi liên tục (PAT – port addess translating).
- **PREROUTING:** Thực hiện việc NAT trước khi gói tin đi qua bộ định tuyến (routing) của Server. Bảng này còn biết với tên gọi là **DNAT (Destination NAT).**

86

CÁC LOẠI CHAIN TRONG BẢNG NAT (tt.)

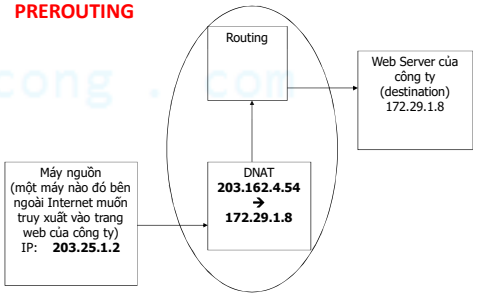
POSTROUTING



87

CÁC LOẠI CHAIN TRONG BẢNG NAT (tt.)

PREROUTING



88

Target

- **ACCEPT:** iptables chấp nhận chuyển data đến đích.
- **DROP**: iptables hủy những packet.
- **LOG**: thông tin của packet sẽ gởi vào syslog daemon và iptables tiếp tục xử lý luật tiếp theo trong bảng mô tả luật.

89

Target (tt.)

- **REJECT**: iptable sẽ hủy các packet va gởi thông báo cho sender.
- **DNAT**: thay đổi địa chỉ đích của packet. Tùy chọn là *--to-destination ipaddress.*
- **SNAT**: thay đổi địa chỉ nguồn của packet. Tùy chọn là *--to-source <address>[-address][:<port>-<port>]*
- **MASQUERADING:** được sử dụng để thực hiện kỹ thuật PAT

90

Các options trong câu lệnh iptables

Lệnh switching quan trọng	Ý nghĩa
`-t <table>`	Nếu bạn không chỉ định rõ là tables nào , thì filter table sẽ được áp dụng. Có ba loại table là filter, nat, mangle.
`-j <target>`	Nhảy đến một chuỗi target nào đó khi gói dữ liệu phù hợp quy luật hiện tại .
`-A`	Nối thêm một quy luật nào đó vào cuối chuỗi (chain).
`-F`	Xóa hết tất cả mọi quy luật trong bảng đã chọn .
`-p <protocol-type>`	Phù hợp với giao thức (protocols) , thông thường là `icmp`, `tcp`, `udp`, và `all` .
`-s <ip-address>`	Phù hợp IP nguồn
`-d <ip-address>`	Phù hợp IP đích
`-i <interface-name>`	Phù hợp điều kiện INPUT khi gói dữ liệu đi vào firewall
`-o <interface-name>`	Phù hợp điều kiện OUTPUT khi gói dữ liệu đi ra khỏi firewall .

91

Sử dụng bảng Filter làm firewall

Đây là cách thêm rule từ cửa sổ gõ lệnh của Linux. Chúng ta cũng có thể để nó trong file script (/etc/sysconfig/iptables) và thực thi file này bằng lệnh /etc/init.d/iptables restart

iptables –A INPUT –p icmp --icmp-type any -j ACCEPT

- -A: thêm 1 rule.
- -p: chỉ ra giao thức sử dụng (icmp, tcp, udp,..)
- --icmp-type: kiểu icmp (echo-request, echo-reply, all…)
- -j : chuyển hướng tới 1 cách xử lý (ACCEPT, REJECT, DROP,…) hoặc một đích nào đó (1 chain mới, một kiểu NAT: DNAT, SNAT,…)

92

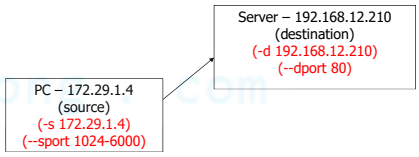
Sử dụng bảng Filter làm firewall (tt.)

Ví Dụ 1: tham khảo file iptables mẫu.

```
*filter  // Dùng bảng filter, nếu muốn dùng bảng nat thì khai báo: *nat

:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -i eth0 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp --icmp-type any -j ACCEPT
-A INPUT -p 50 -j ACCEPT
-A INPUT -p 51 -j ACCEPT
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

93

Sử dụng bảng Filter làm firewall (tt.)



Ví Dụ 2: thêm 1 rule cấm máy 172.29.1.4 truy xuất Server.

-A INPUT –s 172.29.1.4 –d 192.168.12.210 –j REJECT

Nếu muốn cấm đường mạng 192.168.11.0/24 truy cập Server ta khai báo

-A INPUT –s 192.168.11.0/24 –d 192.168.12.210 –j REJECT

94

Sử dụng bảng Filter làm firewall (tt.)

Ví Dụ 3: thêm 1 rule cấm máy 172.29.1.8 truy xuất đến dịch vụ web trên Server, nhưng vẫn cho phép truy xuất tất cả các dịch vụ khác.

-A INPUT –s 172.29.1.8 –d 192.168.12.210 –p tcp –m tcp --dport 80 –j REJECT

- --dport : port của máy đích (máy Server, đối với gói tin đi vào).
- --sport : port của máy nguồn (máy trạm, đối với gói tin đi vào server).

Ví Dụ 4: thêm 1 rule cấm máy 172.29.1.8 truy xuất đến dịch vụ **ssh** trên Server, nhưng vẫn cho phép truy xuất tất cả các dịch vụ khác.

-A INPUT –s 172.29.1.8 –d 192.168.12.210 –p tcp –m tcp --dport 22 –j REJECT

95

Sử dụng bảng Filter làm firewall (tt.)

Ví Dụ 5: giả sử trên máy server có 2 card mạng: eth0, eth1 và ta chỉ áp dụng firewall trên card mạng thứ nhất (eth0) thì khai báo như sau:

-A INPUT *–i eth0* –s 172.29.1.10 –d 192.168.12.210 –j REJECT

Nếu không chỉ rõ dùng card mạng nào (không có –i eth0) thì ngầm định là áp dụng cho tất cả các card mạng có trên máy server.

Với tham số:

-i để chỉ card mạng đối với hướng dữ liệu đi vào (INPUT)

Ví dụ : -i eth0, -i eth1

-o để chỉ card mạng đối với hướng dữ liệu đi ra (OUTPUT)

Ví dụ : -o eth0, -o eth1

96

Ví Dụ 5: thêm 1 rule cấm máy 172.29.1.9 dùng port từ 1024 đến 5000 truy xuất đến dịch vụ **ssh** trên Server, nhưng vẫn cho phép truy xuất đến ssh nếu dùng ngoài dãy port bị cấm.

-A INPUT –s 172.29.1.9 –d 192.168.12.210 –p tcp –m tcp --dport 1024:5000 --dport 22 –j REJECT

Ví Dụ 9: Cấm máy tính có ip 172.29.11.2 truy vấn DNS Server và không phép máy 172.29.11.2 được phép làm secondary (backup dns) cho Server.

-A INPUT –s 172.29.11.2 –d 192.168.12.210 –p udp –m udp --dport 53 –j REJECT

-A INPUT –s 172.29.11.2 –d 192.168.12.210 –p tcp –m tcp --dport 53 –j REJECT

97

Sử dụng bảng Filter làm firewall (tt.)

Ví Dụ 7: Cấm máy tính có ip 172.29.12.2 truy xuất đến server dùng giao thức UDP, những vẫn cho phép máy này truy xuất những dịch vụ dùng giao thức khác như TCP, ICMP,…

-A INPUT –s 172.29.12.2 –d 192.168.12.210 –p udp –m udp –j REJECT

Ví Dụ 8: Cấm máy tính có ip 172.29.11.2 truy vấn DNS Server nhưng vẫn cho phép máy 172.29.11.2 được phép làm secondary (backup dns) cho Server.

-A INPUT –s 172.29.11.2 –d 192.168.12.210 –p udp –m udp --dport 53 –j REJECT

98

Sử dụng bảng Filter làm firewall (tt.)

Ví Dụ 9: Cấm máy tính có ip 172.29.11.1 **ping** tới Server. Trước dòng:
-A INPUT -p icmp --icmp-type any -j ACCEPT

Ta khai báo:

-A INPUT –s 172.29.11.1 -p icmp --icmp-type any -j REJECT

Ví Dụ 10: Có thể dùng cách phủ định (! Dấu chấm thang) trong rule. Ví dụ cấm tất cả các máy trừ IP 172.29.11.1 được phép truy cập web.

-A INPUT –s ! 172.29.11.1 -p tcp -m tcp --dport www -j REJECT

99

Cách sử dụng bảng NAT

Trong file (/etc/sysconfig/iptables), ở cuối file khai báo như sau: *nat

sau từ *nat sẽ là các rule của bảng NAT

Lưu ý : Dùng lệnh #sysctl -w net.ipv4.ip_forward=1

hoặc dùng lệnh #echo "1" /proc/sys/net/ipv4/ipforward

Ví Dụ 1: NAT 1 IP thật 203.162.5.2 cho đường mạng 192.168.10.0/24 được phép đi ra ngoài Internet trực tiếp

-A POSTROUTING -o eth0 -s 192.168.10.0/24 -j SNAT --to 203.162.5.2

-o : là card mạng đi ra Internet của Router

100

Cách sử dụng bảng NAT (tt.)

Ví Dụ 2: dùng masquerade để NAT ip thật thay đổi (adsl, dialup).

-A POSTROUTING -o ppp0 -j MASQUERADE

ppp0 : là interface của modem hoặc adsl trên router

Ví Dụ 3: NAT 1 IP thật 203.162.5.2 cho máy web server 172.29.1.2 được phép public.

-A PREROUTING -p tcp --dport 80 -i eth0 -j DNAT --to 172.29.1.2:80

101