การทำ ACL บน Router CISCO

นายเกรียงศักดิ์ นามโคตร (Mr.Jodoi) เรียบเรียง

Access Control List (ACL) คือ การกรอง packet ที่จะเข้าออก Router ให้เป็นไปตามเงื่อนไขที่เราต้องการ และมีส่วนช่วยในเรื่องของ IT Security แต่มีข้อเสียคือไปเพิ่ม load cpu ให้กับ Router เพราะหน้าที่หลักของ Router คือการพา packet ไปให้ถูกเส้นทางหรือการหาเส้นทาง ไม่ใช่ทำหน้าที่กรอง packet และการตั้งค่า ACL ที่ผิดพลาด จะส่งผลให้ Network มีปัญหาได้ การกรอง packet ควรจะเป็นหน้าที่ของ Firewall มากกว่า แต่สำหรับ Network ที่ไม่ใหญ่มาก หรือบริษัทที่มีงบประมาณน้อย การทำ ACL บน Router นั้นก็เป็นทางเลือกหนึ่งที่น่าสนใจ และ ACL ยังเป็นหัวข้อหนึ่งสำหรับผู้ที่ต้องสอบ Cert. CCNA

การ config ACL บน Router CISCO นั้น ทำได้ 2 วิธีการ คือวิธีการแบบตัวเลข และวิธีการแบบชื่อ (Name ACL) ในที่นี่จะสอนเฉพาะวิธีการแบบตัวเลขเท่านั้น

ACL แบ่งเป็น 2 ประเภท คือ

1) ACL แบบ Standard ใช้ตัวเลข 1-99

2) ACL แบบ Extended ใช้ตัวเลข 100-199

Standard ACL

Standard ACL จะกรอง traffic เฉพาะ source address เท่านั้น ตัวเลขที่ใช้คือเลข 1-99 (เฉพาะ protocol IP) โดยมีรูปแบบการ config ดังนี้

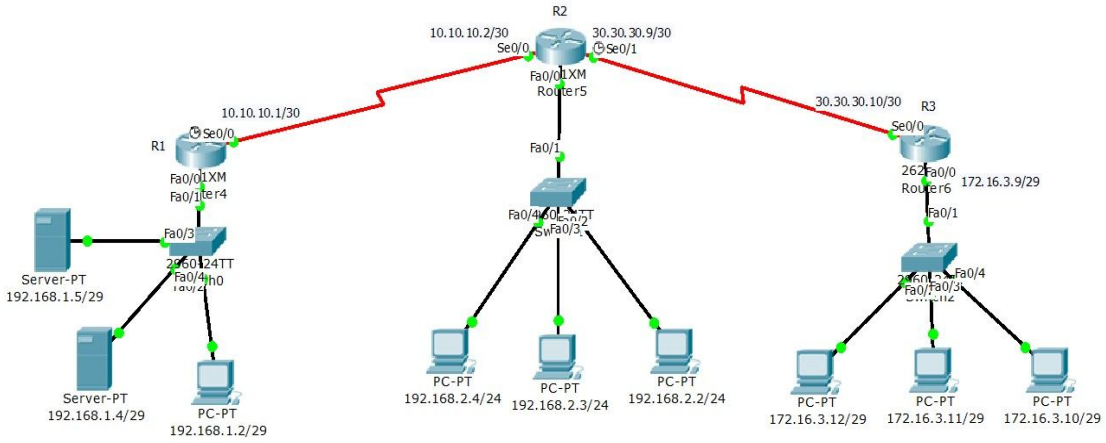
Router(config)#access-list access-number permit,deny,remark Source Address Wildcard

(deny คือห้าม packets ผ่าน ,permit คืออนุญาตให้ packets forward ผ่านได้, remark คือ comment)

(Source Address ถ้า IP เดียวใส่ IP ตัวนั้น แต่ถ้าทั้งวง ให้ใส่เป็น Network IP)

ตัวอย่างโจทย์

1) จาก Network Diagram ห้าม IP 192.168.2.2 และ 172.16.3.8/29 ทั้งวง เข้ามาที่ Router R1



การ config มี 2 ขั้นตอน

ขั้นตอนที่1 คือการประกาศ ACL จากโจทย์สามารถ config ได้ดังนี้

R1(config)#access-list 1 deny 192.168.2.2 0.0.0.0

หรือ

R1(config)#access-list 1 deny host 192.168.2.2

(ในกรณี ห้ามเพียง IP เดียว นิยมใช้คำว่า host)

R1(config)#access-list 1 deny 172.16.3.8 0.0.0.7

(ในกรณี ห้ามทั้งSubnet ให้ใส่เป็น Network IP การคำนวณ NetworK IP และค่า wildcard หาอ่านได้ในบทความเรื่อง IP Address)

R1(config)#access-list 1 permit any

(ต้องมีบรรทัดนี้ปิดท้ายเพื่ออนุญาตให้เงื่อนไขอื่น ที่ไม่ตรงกับด้านบนสามารถผ่านได้เนื่องจากจะมีบรรทัด access-list 1 deny any ซ่อนอยู่ การจัดเรียงบรรทัดต้องเรียงให้ถูกต้องเพราะACL จะอ่าน config จากบนลงล่าง) เมื่อ show config ดู จะต้องเป็นดังนี้

R1#show running-config

!

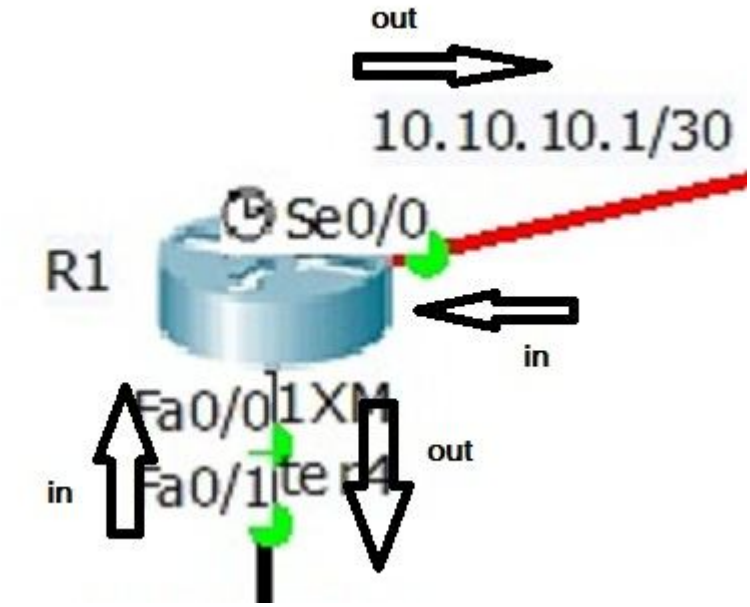
access-list 1 deny host 192.168.2.2

access-list 1 deny 172.16.3.8 0.0.0.7

access-list 1 permit any

!

ขั้นตอนที่2 คือการ enable ACL ที่ interface ให้ดูที่ Source IP ว่าวิ่งเข้าRouter หรือ วิ่งออกจากRouter โดย packet ที่เข้า Router จะเป็น in และ packet ที่ออกจาก Router จะเป็น out



จากโจทย์ IP ที่สนใจ คือ IP 192.168.2.2 และ 172.16.3.8/29 อยู่ทางขวามือของ Router R1 ดังนั้นถ้าทำการ on ACL ที่ interface s0/0 จะเป็น in เพราะ packet วิ่งเข้าRouter R1 แต่ถ้าทำการon ACL ที่ interface f0/0 จะเป็น out เพราะ packet วิ่งออกจากRouter R1 แต่ควรจะ on ACL ที่ interface s0/0 จึงจะถูกต้องเพราะโจทย์บอกว่าห้ามเข้ามาที่ Router R1 ดังนั้นconfig ได้ดังนี้

R1(config)#interface s0/0

R1(config-if)#ip access-group 1 in

เมื่อ show config ดู จะต้องเป็นดังนี้

R1#show running-config

!

interface Serial0/0

ip address 10.10.10.1 255.255.255.252

ip access-group 1 in

clock rate 128000

!

การตรวจสอบ acl ใน Router CISCO นั้น นอกจากจะใช้การ show running-config แล้วยังสามารถใช้command show access-lists เช่น

R1#show access-lists

Standard IP access list 1

deny host 192.168.2.2

deny 172.16.3.8 0.0.0.7

permit any

และถ้าต้องการดูว่าinterface ใด ทำACL ไว้หรือไม่ จะใช้command show ip interface เช่น

R1#show ip interface s0/0

Outgoing access list is not set

Inbound access list is 1

ให้สังเกตตรงบรรทัด Outgoing และ Inbound ถ้ามีการทำACL ไว้จะแสดงตัวเลขของACL

จุดที่ต้องระวังในการทำACL บน Router CISCO คือ การปรับแต่งหรือแก้ไขACL นั้น ควรจะทำการcopy ACL ของเดิมไว้ก่อน เนื่องจาก เมื่อทำการลบACL บรรทัดใดบรรทัดหนึ่ง ACL ที่เป็น number เดียวกันจะหายทั้งหมด ถ้าไม่มีความชำนาญจริงไม่ควร remote แก้ไขเด็ดขาด

หวังว่าบทความนี้คงจะก่อให้เกิดประโยชน์ไม่มากก็น้อยสำหรับผู้ที่ทำงานอยู่กับอุปกรณ์Cisco นะครับ ติดตามตอนที่ 2 Extended ACL เร็วๆนี้ครับ

สนับสนุนโดย http://www.jodoi.com