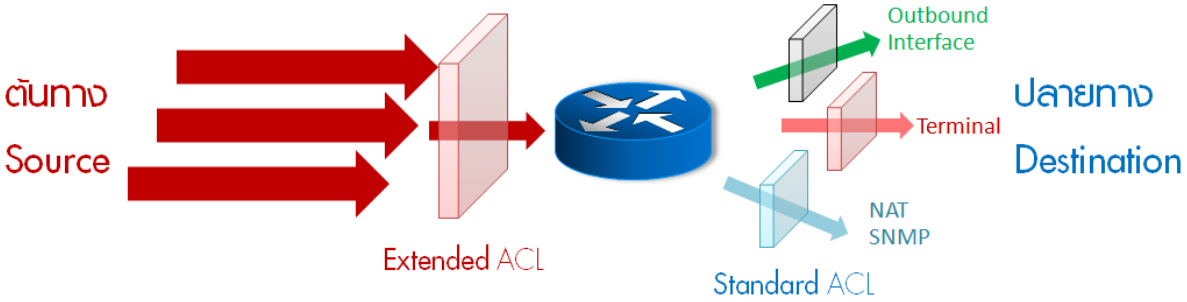
หลักการตั้งค่า Access-List

และความผิดพลาดที่ผู้ตั้งค่ามักลืมนึกถึง

Access Control List (ACL) เป็นชุดเงื่อนไขที่กำหนดแพ็กเก็ตข้อมูลที่เราสนใจ บนเราท์เตอร์ เพื่อนำไปใช้ในรูปแบบต่างๆ เช่น ควบคุมแพ็กเก็ตที่เข้าหรือออกจากอินเตอร์เฟส หรือนำไปใช้กับฟีเจอร์ยอดนิยมอย่าง NAT เป็นต้น ซึ่งมีหลักการที่ผู้ตั้งค่าควรคำนึงอยู่ 3 ประการ ดังนี้

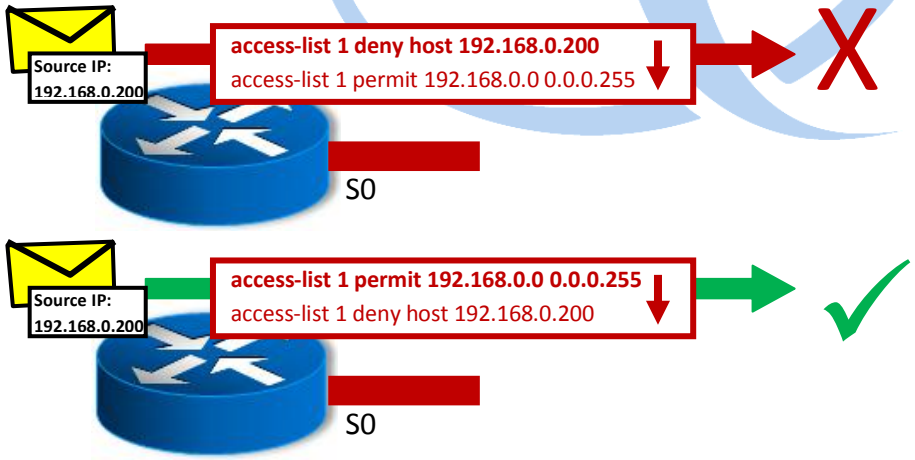
1 **นำ ACL แบบ Extended ไปใช้กับอินเตอร์เฟสขาเข้าเราท์เตอร์** (Source) **และนำแบบ Standard ไปใช้กับอินเตอร์เฟสขาออก** (Destination)



นอกจากไม่ทำให้หน่วงการประมวลผลบนเราท์เตอร์แล้ว ยังมีผลในแง่ความปลอดภัยด้วย คือทำให้กรองแพ็กเก็ตที่ไม่ต้องการได้อย่างเด็ดขาด หากปล่อยให้เข้ามาในเราท์เตอร์แล้ว อาจทำให้แพ็กเก็ตดังกล่าวหาช่องทาง หรืออินเตอร์เฟสอื่นที่มีช่องโหว่อ้อมไปหาปลายทางได้อีก

ซิสโก้จึงใช้คำว่า “Extended near Source, Standard near Destination”

2 **ตั้งเงื่อนไขที่จำเพาะที่สุดไว้บรรทัดบนสุดก่อน เพราะเราท์เตอร์อ่านเงื่อนไขจากบนลงล่าง**



คำว่า “อ่านจากบนลงล่าง” คือ เราท์เตอร์จะเอาข้อมูลของแพ็กเก็ตมาไล่เทียบจากเงื่อนไขบรรทัดบนสุดก่อน **ถ้าเข้าเงื่อนไข ก็เป็นอันจบ ไม่ต้องอ่านบรรทัดต่อมา** จึงสำคัญเป็นอย่างยิ่งที่ต้องกำหนดเงื่อนไขที่จำเพาะ (รายโฮส หรือรายกลุ่มไอพี) ก่อนเงื่อนไขที่กว้างกว่า (เช่น เป็นเครือข่าย) เป็นต้น

ซิสโก้อธิบายด้วยประโยคที่ว่า “First match determines whether accepts or rejects the packet”

3 อย่าลืมเงื่อนไขสุดท้าย “permit ip any any” ถ้าตั้งชุดเงื่อนไขแบบ Deny เฉพาะบางกลุ่ม

หลักการของ Access-List คือ อนุญาตเฉพาะแพ็กเก็ตที่เข้าเงื่อนไขเท่านั้น โดยถือว่าถ้าแพ็กเก็ตไม่ตรงกับเงื่อนไขใดในชุดนี้ ถือว่าต้องปฏิเสธแพ็กเก็ตนั้นโดยปริยาย **(ซิสโก้ใช้คำว่า Implicit Deny)** (บางคนจึงสอนให้จำว่า Access-List ที่ตั้งขึ้น จะมีเงื่อนไขสุดท้ายซ่อนอยู่คือ Deny any any เสมอ)

ด้วยเหตุผลดังกล่าว และเจตนาในการใช้ จึงแบ่งการตั้งค่า Access-List ได้เป็นสองสไตล์ ได้แก่ การอนุญาตเฉพาะบางกลุ่ม (Allow by rule) กับการบล็อกเฉพาะบางกลุ่ม (Deny by exception) ซึ่งเชื่อหรือไม่ว่า ก รณีหลังผู้ตั้งค่ามักลืมสั่งอนุญาตแพ็กเก็ตที่เหลือที่ไม่เข้าเงื่อนไข (ด้วยคำสั่งอย่าง permit ip any any เป็นต้น) ทำให้แพ็กเก็ตอื่นโดนบล็อกการติดต่อบนอินเตอร์เฟสเดียวกันไปด้วยโดยไม่ได้ตั้งใจ

หมายเหตุ: *สำหรับ Acces-list แบบ Extended ที่เราจะใช้เสมือนเป็น Firewall ก่อนเข้าเราท์เตอร์นั้น มีคำแนะนำด้านความปลอดภัยว่า ถึงแม้ Access-list จะมีคุณสมบัติเป็น Implicit Deny (ปฏิเสธการสื่อสารแบบอื่นทั้งหมดที่ไม่เข้าเงื่อนไขข้างต้น) แต่ก็ควรใส่เงื่อนไขสุดท้ายเป็น access-list 1xx deny ip any any* ***log*** *เพื่อให้แน่ใจว่า เราท์เตอร์จะบันทึก Log ของการสื่อสารขาเข้าที่ไม่เข้าเงื่อนไขที่กำหนด เพื่อใช้ตรวจสอบผ่าน Syslog ในภายหลังได้*

ตัวอย่าง:

access-list 100 deny tcp any range 0 65535 any range 0 65535 ***log***

access-list 100 deny ip any any ***log***

(เพื่อให้บันทึก log การสื่อสารที่ไม่เข้าเงื่อนไขทั้งระดับ ip และ tcp ซึ่งสามารถแสดงบันทึก syslog ที่เราท์เตอร์เก็บไว้ได้ด้วยคำสั่ง show logging หรือจะตั้งค่า logging x.x.x.x โดยที่ x.x.x.x เป็นเครื่องที่เปิด Syslog Server เพื่อเรียกอ่านย้อนหลังก็ได้)