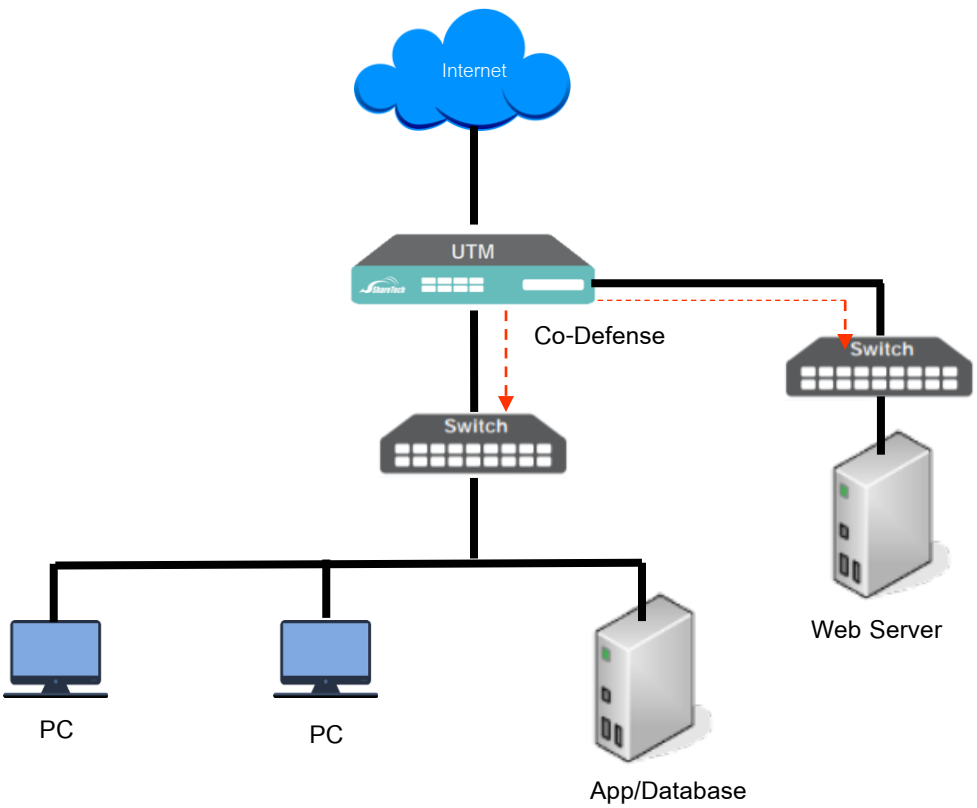
Co-Defense Switch



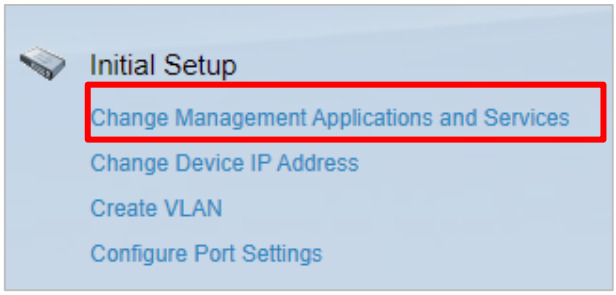
ต.ย Network Diagram

Support : support.th@nit.co.th
Sales : rung@nit.co.th
Mobile : 081=985-6916
Web : www.netinfortech.co.th
Line : nit.sharetech

Co-Defense Switch เป็นอีกหนึ่ง Function ของ Next Gen UTM Firewall ที่ช่วยให้ Firewall สามารถตรวจสอบ และป้องกันความเสี่ยง ที่ผ่านอุปกรณ์ Switch ก่อนผ่านมาถึง Firewall จะมีขั้นตอนการตั้งค่าดังนี้

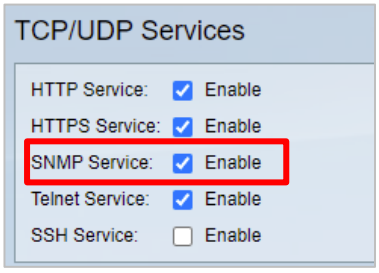
❑ Cisco Switch

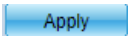
1.เปิด SNMP service บน Switch ที่ต้องการให้ทำงานร่วมกันกับ Firewall สำหรับคู่มือจะใช้ Switch Cisco เป็นตัวอย่าง



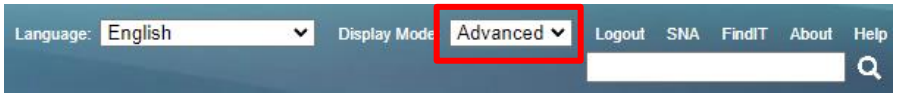
1.1 คลิกที่ Change Management Application and Service

1.2 จะเปิดหน้าจอให้คลิกเครื่องหมายถูกที่ SNMP

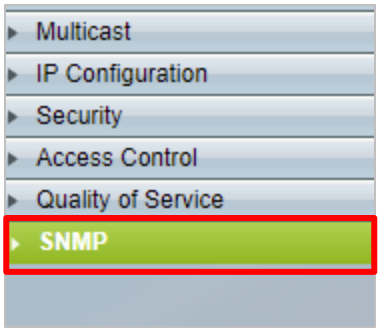


1.3 กดปุ่ม 

1.4 เลือกการ Setting แบบ Advanced ที่เมนู Display Mode

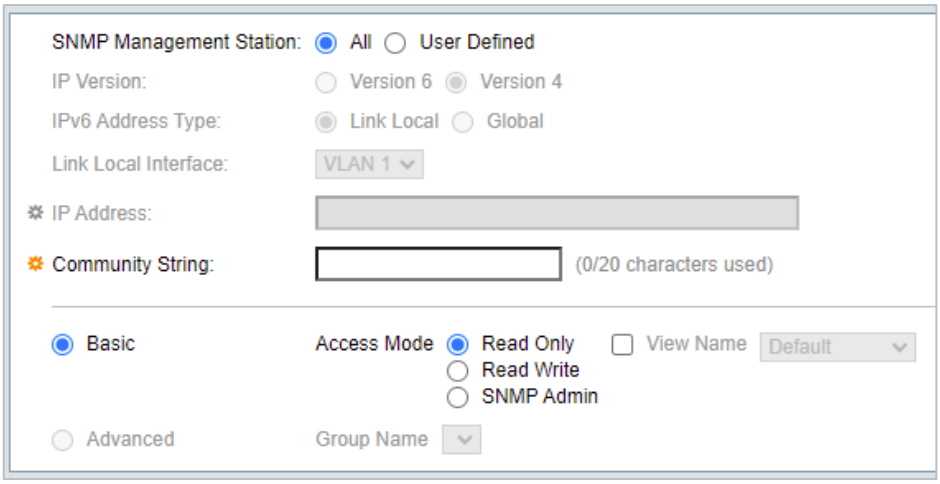


1.5 คลิกที่เมนู SNMP



1.6 คลิกที่เมนู Communities เพื่อสร้าง Public/Private Communities

1.7 กดปุ่ม Add... จะเปิดหน้าให้สร้าง Communities

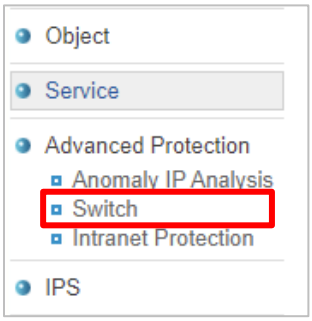


- SNMP Management Station ให้เลือก All
- Communities String ให้ใส่ Public
- Access Mode เลือก Read Only
- กดปุ่ม Apply
- ให้สร้าง Communities สำหรับ Private ในหน้าจอเดียวกัน
- Access Mode เลือก Read Write
- กดปุ่ม Apply

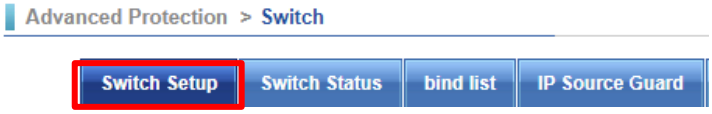
- กดปุ่ม Save ทุกครั้งเมื่อมีการ Setting

❑ Firewall

2. เข้า Firewall และคลิกที่เมนู Advanced Protection

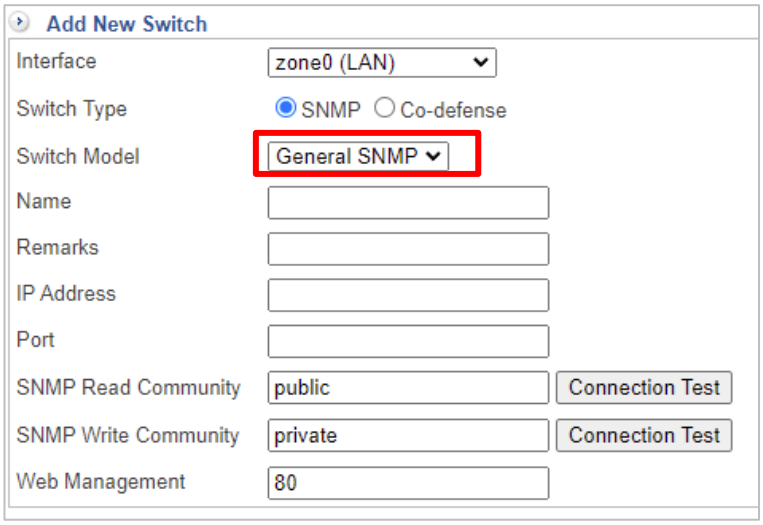


2.1 คลิกที่เมนู Switch Setup



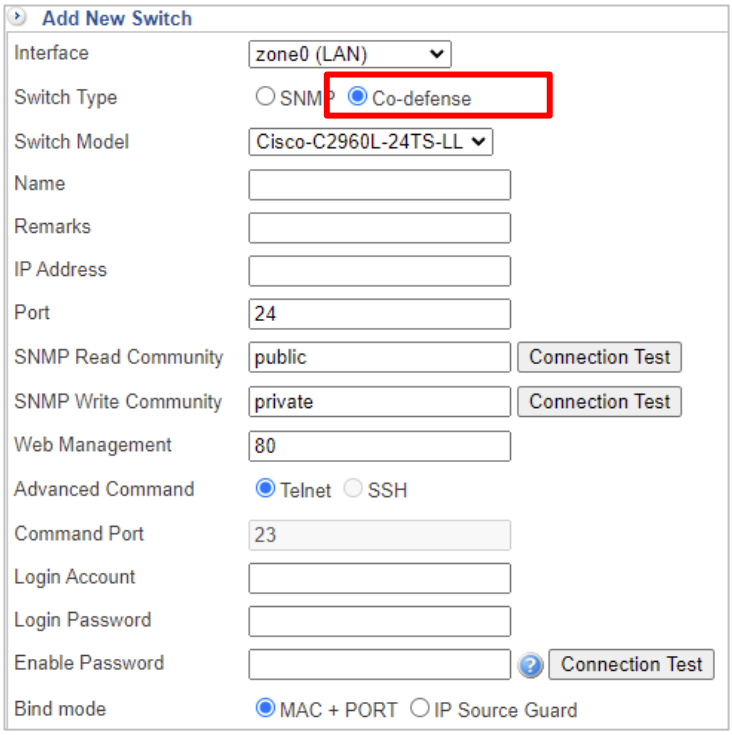
2.2 กดปุ่ม 

2.3 จะเปิดหน้าเพื่อติดตั้งค่า เลือก Switch type SNMP



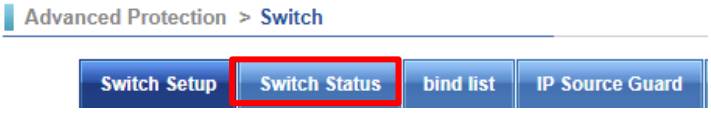
- Interfaces ให้เลือก zone ที่ Switch ต่ออยู่เช่น zone0 (LAN)
- Switch Type SNMP สำหรับ L2 switch ที่เป็น Management สามารตรวจสอบ และ Close port บน switch ด้วย Firewall ได้
- ให้เลือก Model ของ Switch ที่รองรับแต่ถ้าไม่มีใน List ให้เลือก General SNMP
- Name ให้ใส่ชื่อที่สื่อความหมายเช่น Core-SW, SW-FL1
- Remarks เป็นการขยายความว่า Switch นี้ติดตั้งอยู่ที่ไหน
- IP Address ให้ใส่ IP Address ของ Switch
- Port ให้ใส่จำนวน Port ของ Switch เช่น 8, 16, 20, 24
- SNMP Read Community ให้ใส่ public ตามที่สร้างในหัวข้อ 1 (กดปุ่มทดสอบ Connection Test) ถ้า Fail ให้เช็คที่ Switch
- SNMP Write Community ให้ใส่ private และทดสอบ
- กดปุ่ม 

2.3 ติดตั้งค่า เลือก Switch type Co-Defense

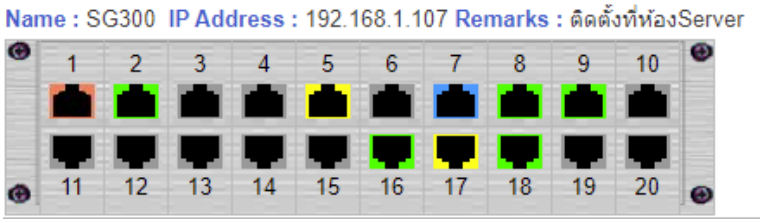


- Interfaces ให้เลือก zone ที่ Switch ต่ออยู่เช่น zone0 (LAN)
- Switch Type Co-Defense จะใช้สำหรับ L3 switch Management สามารถตรวจสอบ และป้องกันกับหลาย Function บน Firewall เช่น IPS
- ให้เลือก Model ของ Switch ที่รองรับมีใน List
- Name ให้ใส่ชื่อที่สื่อความหมายเช่น Core-SW, SW-FL1
- Remarks เป็นการขยายความว่า Switch นี้ติดตั้งอยู่ที่ไหน
- IP Address ให้ใส่ IP Address ของ Switch
- Port ให้ใส่จำนวน Port ของ Switch เช่น 8, 16, 20, 24
- SNMP Read Community ให้ใส่ public ตามที่สร้างในหัวข้อ 1 (กดปุ่มทดสอบ Connection Test) ถ้า Fail ให้เช็คที่ Switch
- SNMP Write Community ให้ใส่ private และทดสอบ
- Advanced Command ให้เลือก Telnet หรือ SSH ขึ้นอยู่กับ Switch อนุญาตในการ Remote เพื่อบริหารจัดการ
- Login Account / Login Password / Enable Password เป็น Username และ Password ของ Switch เมื่อใส่ข้อมูลให้ทดสอบ Connection Test ด้วย
- Bind mode เลือก Mode การตรวจสอบด้วย MAC + IP หรือ IP Source Guard เพื่อป้องกัน
- กดปุ่ม 

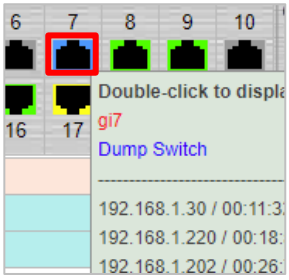
2.4 เมนู Switch Status สำหรับดู Packet / Traffic /Status ที่เกิดขึ้นบน Switch



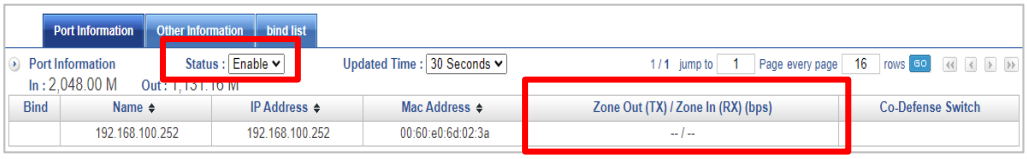
2.5 คลิกที่เมนู Switch Status จะแสดงรูปของ Switch



-ใช้ Mouse ชี้ที่ Port จะเห็น IP Address และ Mac address ของอุปกรณ์ที่เสียบอยู่ที่ Port นั้นๆ

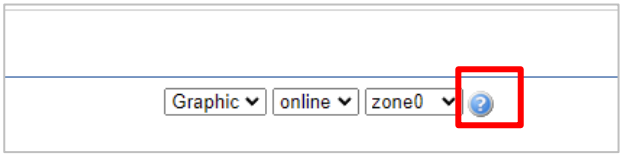


- การดู Traffic ของเครื่องคอมพิวเตอร์ให้ ดับเบิลคลิกที่ Port ที่ต้องการดู

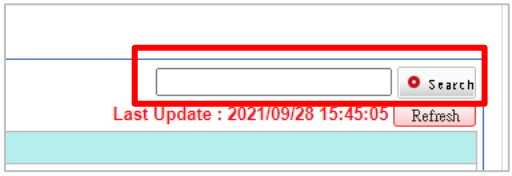


ถ้าเราเห็นว่า Port นี้ใช้งาน (Traffic) สูงผิดปกติให้เปลี่ยน Status จาก Enable เป็น Close แค่นี้ก็จบปิด Port ให้ให้เครื่องคอมพิวเตอร์ที่ต่ออยู่เชื่อมต่อกับเครือข่ายได้

- ความหมายของสีที่แสดงสามารถดูความหมายโดยคลิกที่ ?

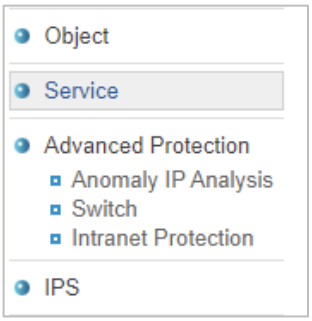


- สามารถค้นหา IP Address ว่าเสียบอยู่กับ Switch / Port ไหนได้

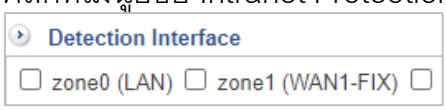


2.7 การสั่งให้ Switch ป้องกันความเสี่ยงที่เกิดขึ้น จากการตรวจสอบด้วย IPS

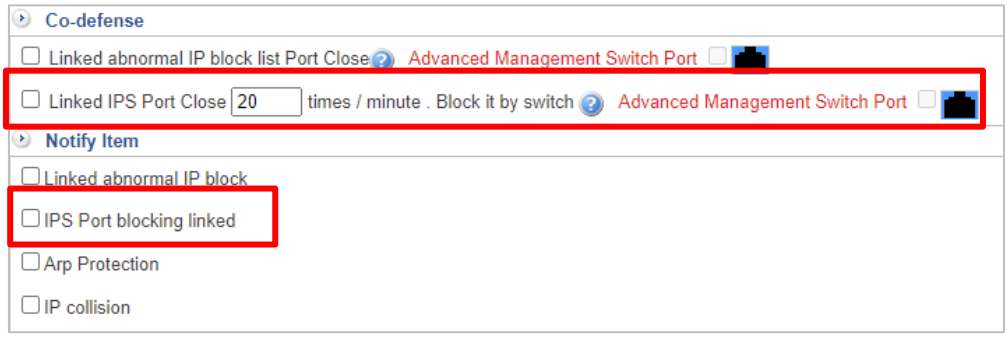
- เข้าเมนู Advanced Protection



- คลิกที่เมนูย่อย Intranet Protection และกดเครื่องหมายถูกที่ Zone0



- ให้คลิกเครื่องหมายถูกตามรูป



- กดปุ่ม 

- ถ้ามีความเสี่ยงเกิดขึ้น Switch จะถูก Close Port เฉพาะ Port ที่มีความเสี่ยง สามารถดู Lock ได้จาก Switch Status หรือ Lock Status

ข้อระมัดระวัง

การ Setting ให้ Firewall ทำการ Close Port เมื่อมีการรับส่งข้อมูลที่สูง และผิดปกติ บางครั้งอาจจะจับผิด เนื่องจากบาง Application อาจต้องใช้งานที่สูง และถ้าไป Close port ที่ต่อกับ Firewall จะทำให้ ออกอินเตอร์เน็ตไม่ได้