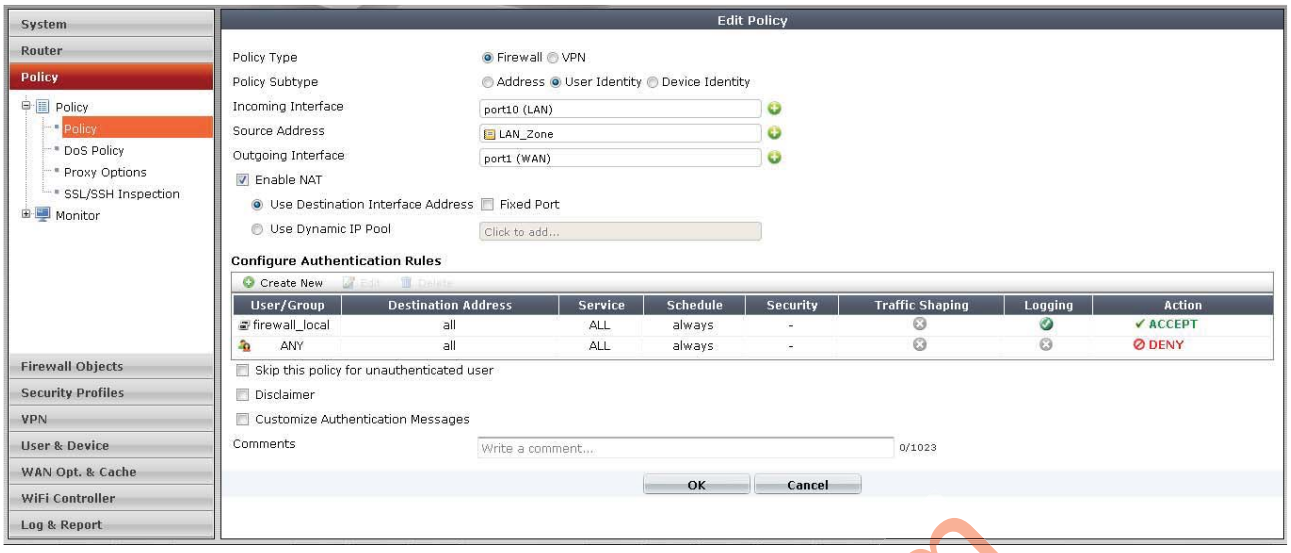
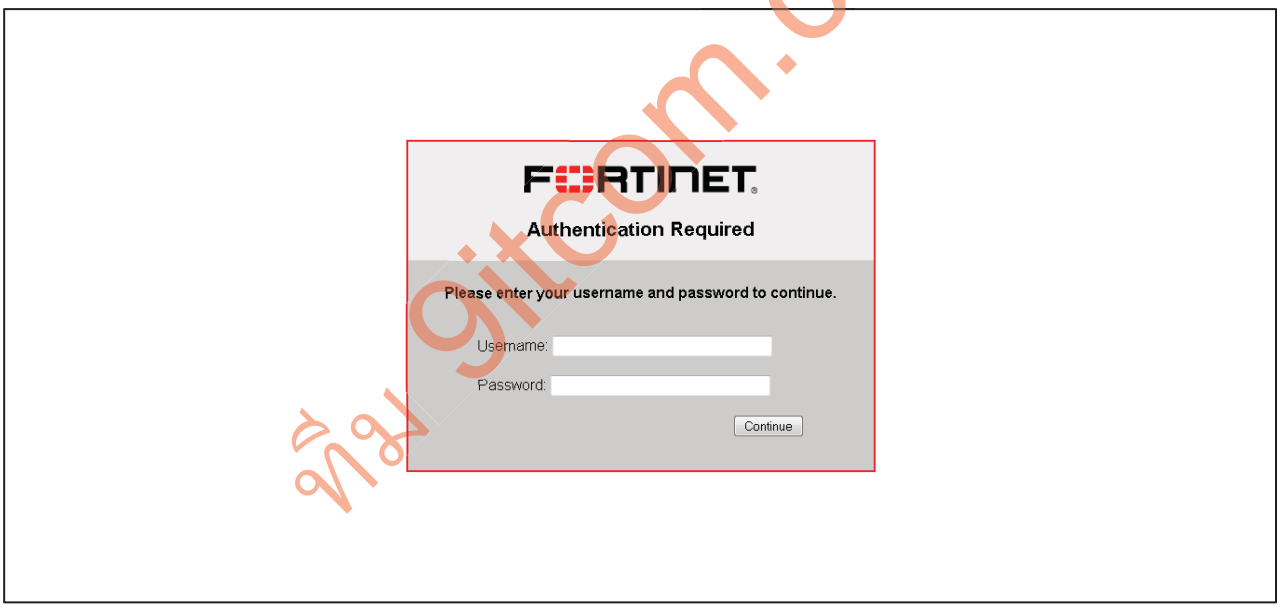
ขั้นตอนที่ 3 : เขียน Policy Auth ด้วย Local User



จากนั้น User จะติดหน้า Firewall Auth

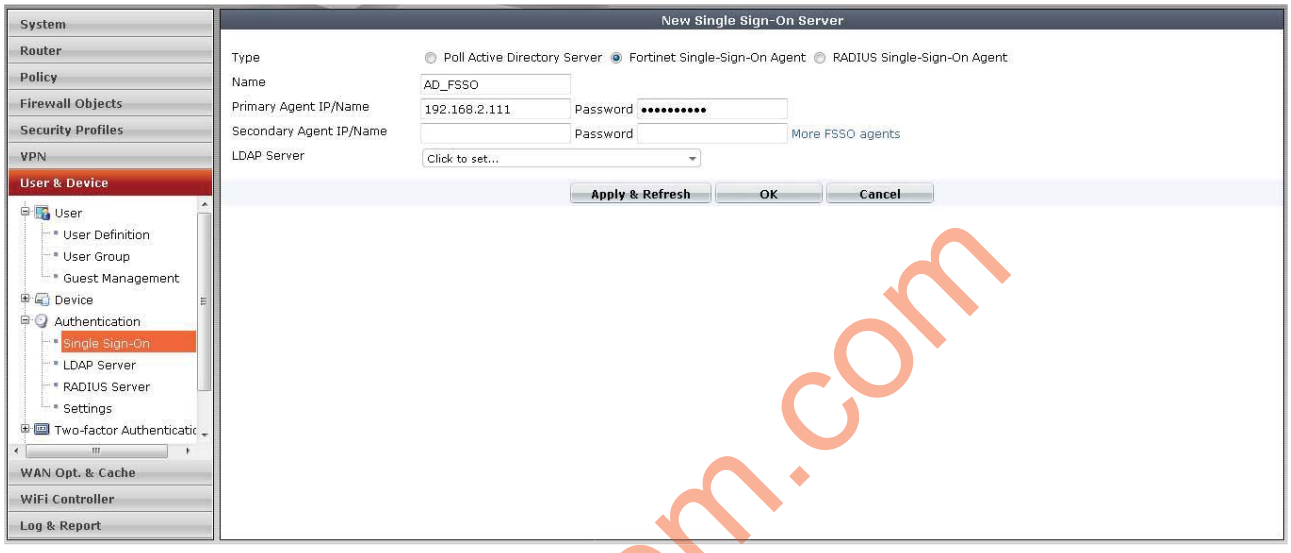


Fortinet Single Sign On (FSSO)

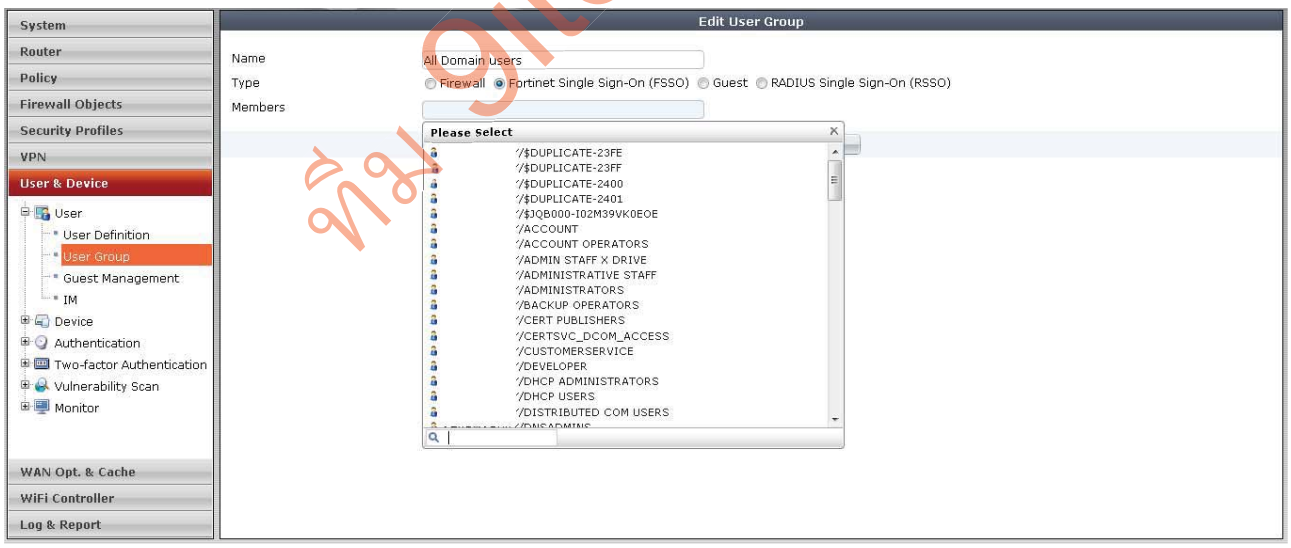
การรับค่าของการ Sign On User กับ Windows AD เข้ามาและตัว FortiGate จะรับทราบ Event นั้นๆ

และสามารถปล่อย User ออกได้เลยโดยไม่ต้อง Auth กับตัว Firewall อีก 1 ครั้ง

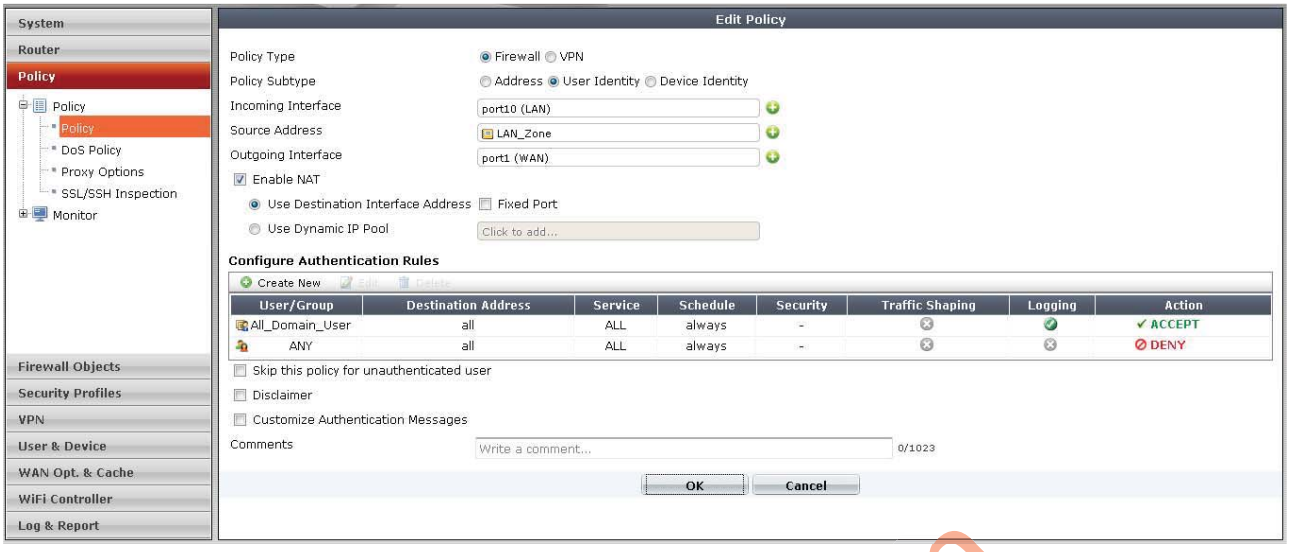
ขั้นตอนที่ 1: สร้าง Connector กับตัว Windows AD



ขั้นตอนที่ 2: สร้าง User Group ที่ Link กับ FSSO



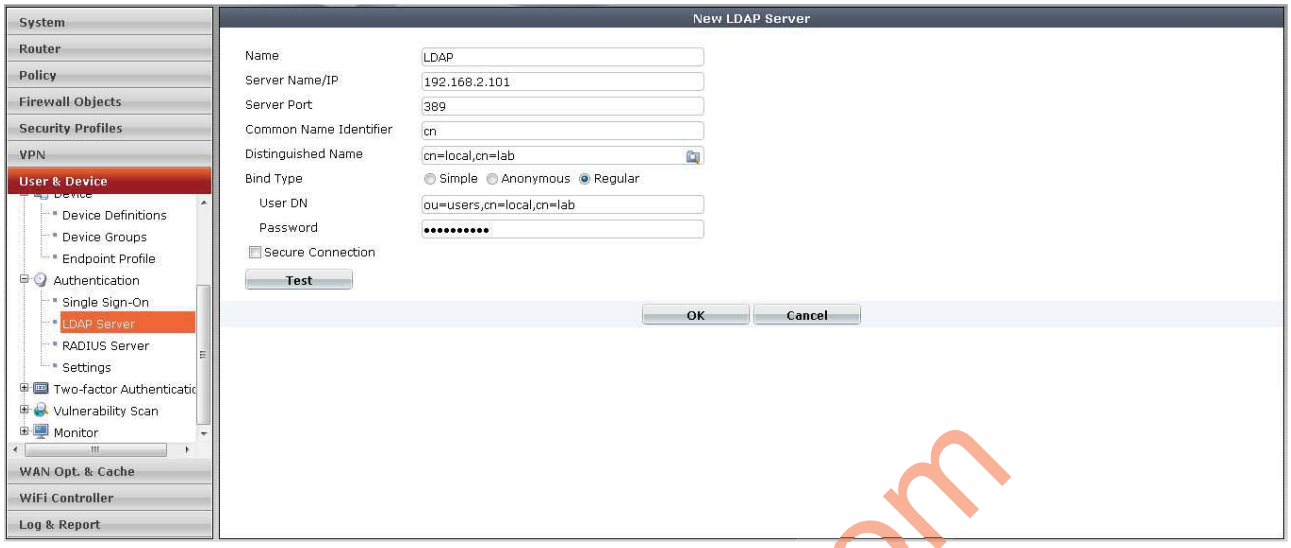
ขั้นตอนที่ 3: สร้าง Policy Auth โดยใช้ User Group ที่รับมาจาก FSSO



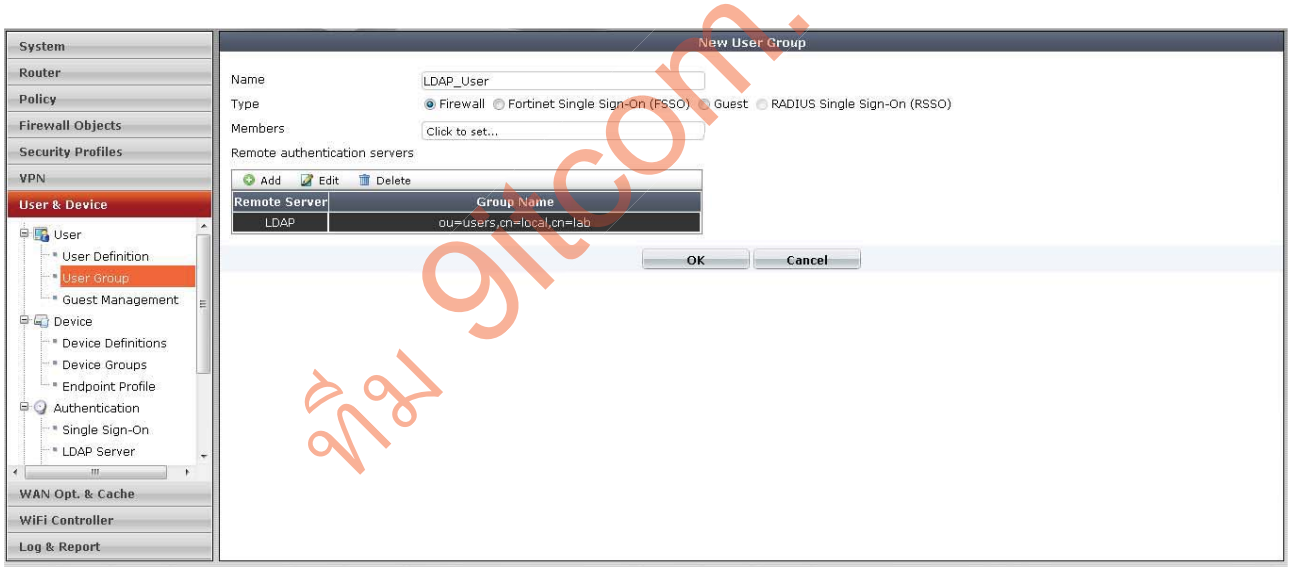
จากนั้น User จะติดหน้า Firewall Auth

LDAP User

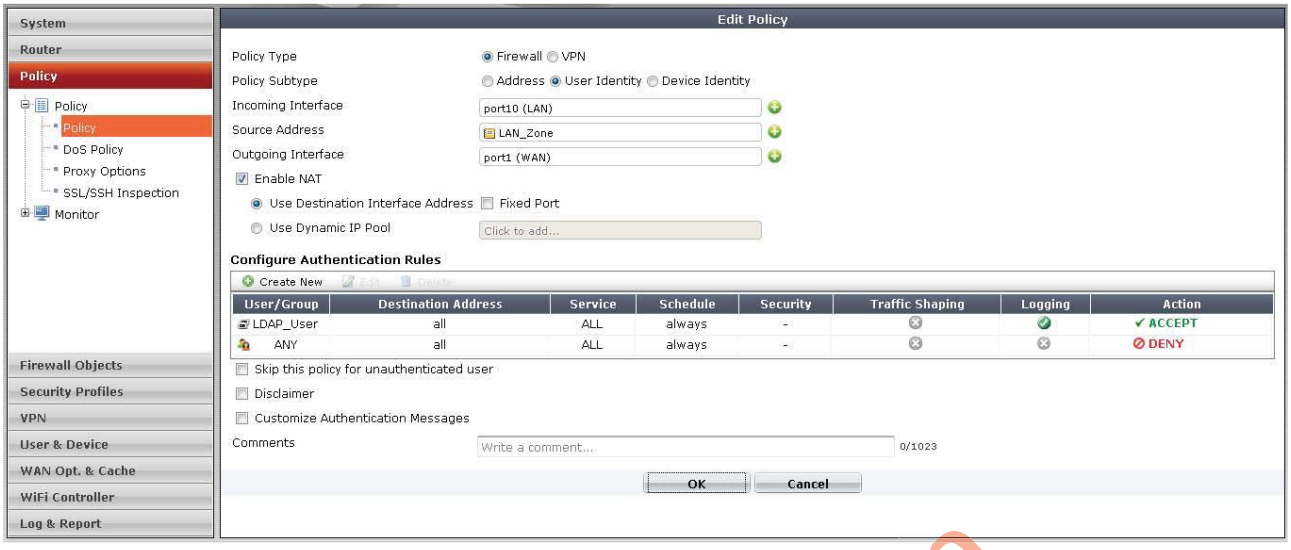
ขั้นตอนที่ 1 : สร้าง Connector ของ FortiGate กับ LDAP



ขั้นตอนที่ 2 : สร้าง User Group เพื่อใช้งาน User ที่ได้จาก LDAP



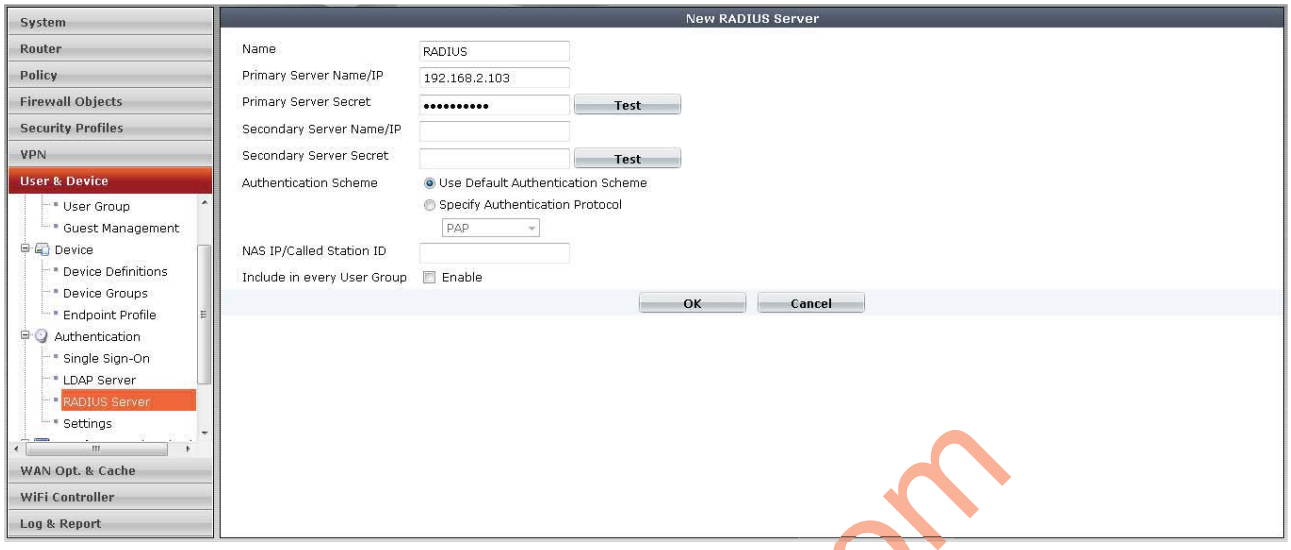
ขั้นตอนที่ 3: สร้าง Policy Auth โดยใช้ User Group ที่รับมาจาก LDAP



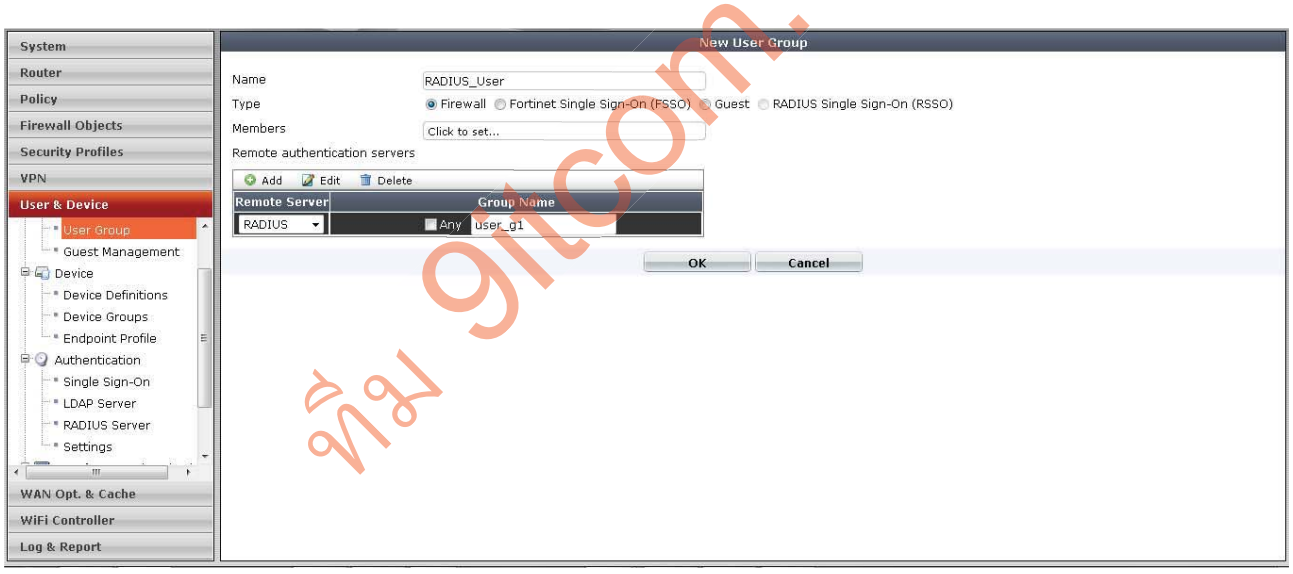
จากนั้น User จะติดหน้า Firewall Auth

LDAP User

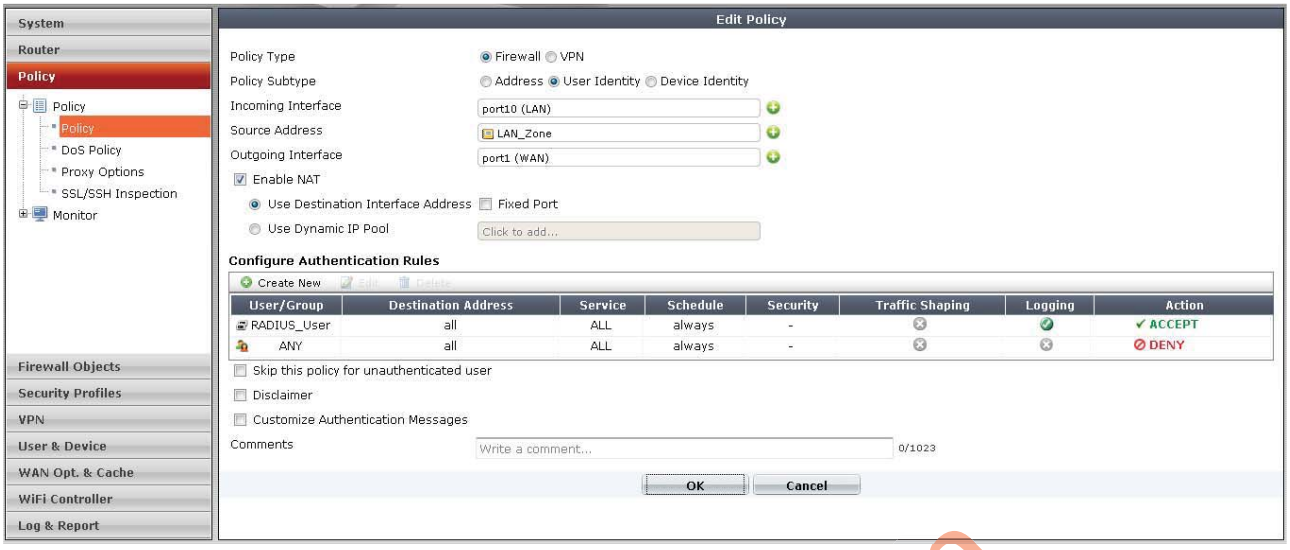
ขั้นตอนที่ 1 : สร้าง Connector ของ FortiGate กับ RADIUS



ขั้นตอนที่ 2 : สร้าง User Group เพื่อใช้งาน User ที่ได้จาก RADIUS (ต้องกำหนด Group Name)

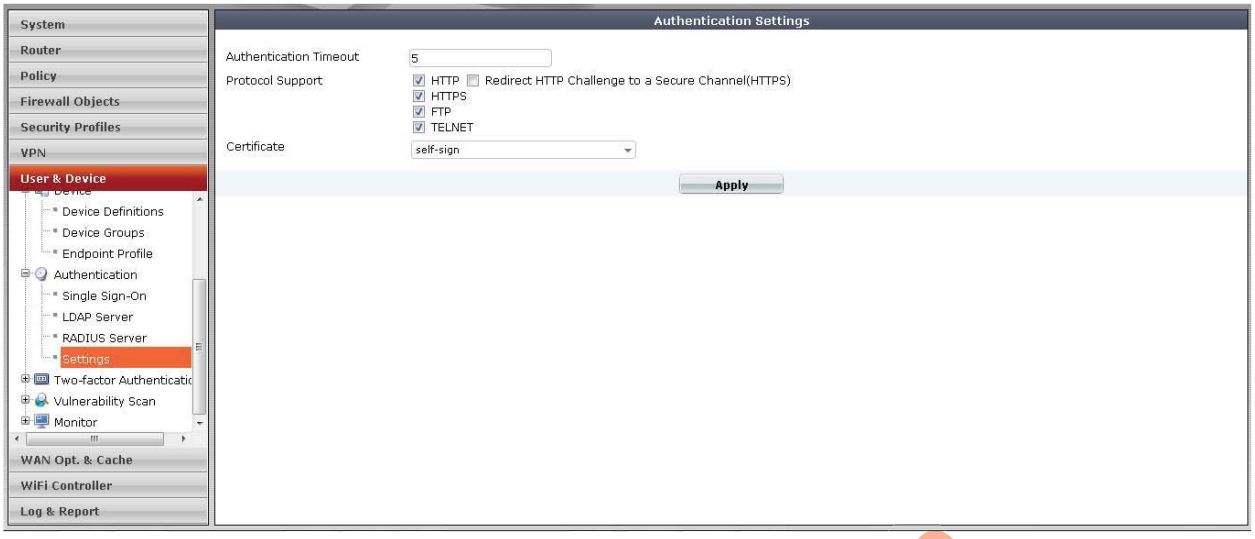


ขั้นตอนที่ 3: สร้าง Policy Auth โดยใช้ User Group ที่รับมาจาก LDAP



จากนั้น User จะติดหน้า Firewall Auth

การกำหนดค่า Auth Time-Out ของ Global



Config Auth OverDrive เพื่อกำหนดให้ User บางกลุ่มสามารถ Auth ได้มากกว่า 1 Session

FortiGate # config system global

FortiGate (global) # set policy-auth-concurrent 1

FortiGate (global) # end

FortiGate # config user group

FortiGate (group) # edit Manager

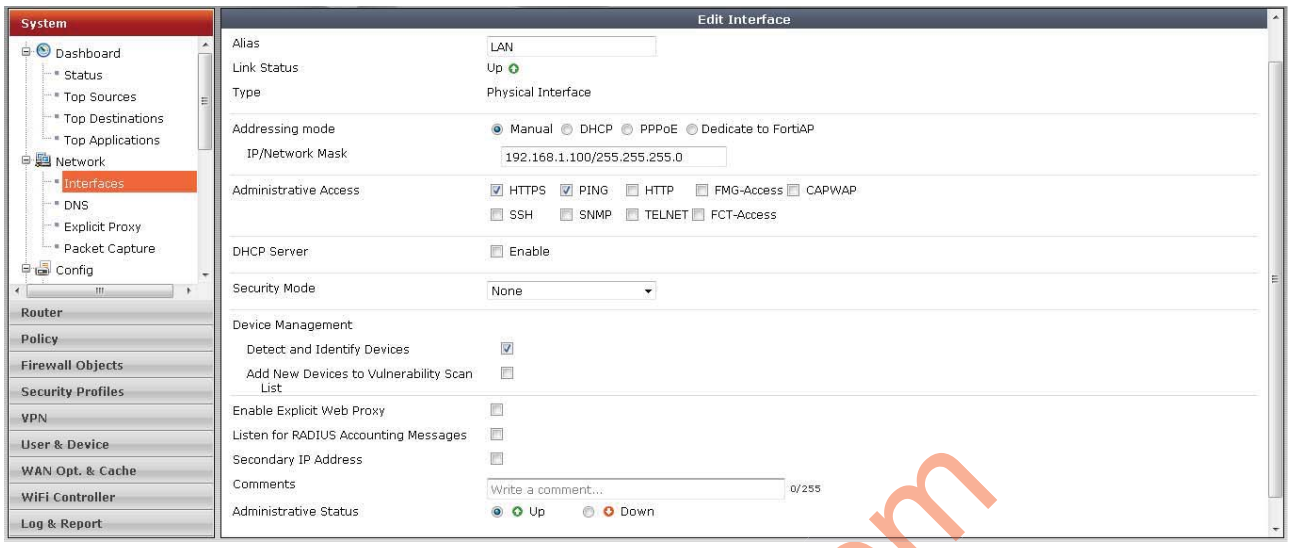
FortiGate (Manager) # set auth-concurrent-override enable

FortiGate (Manager) # set auth-concurrent-value 2

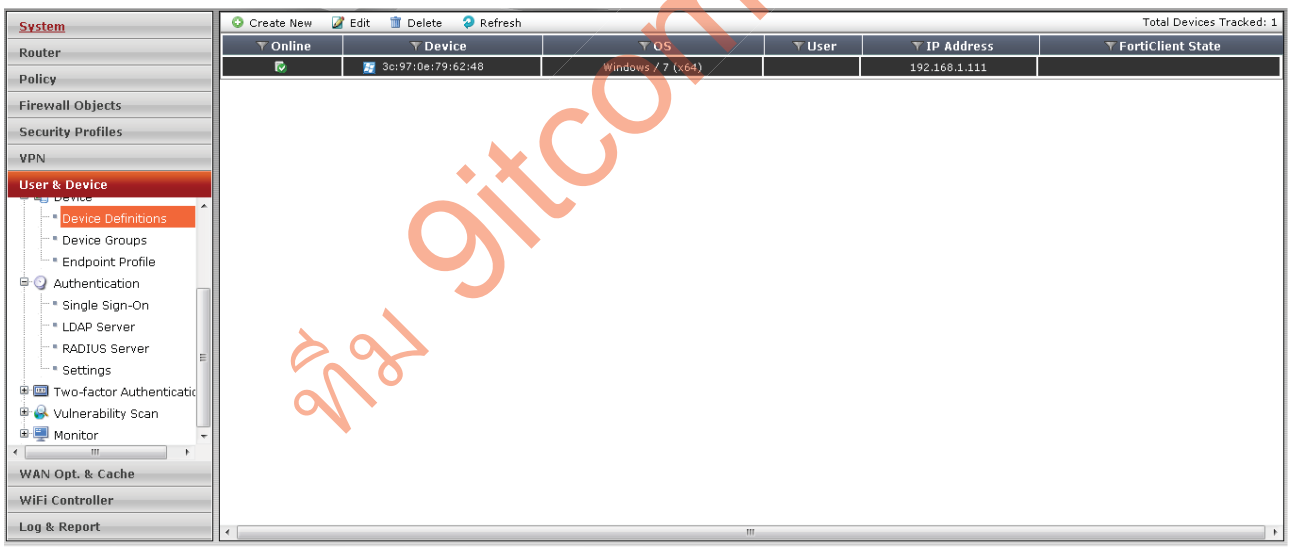
FortiGate (Manager) # end

Device Auth

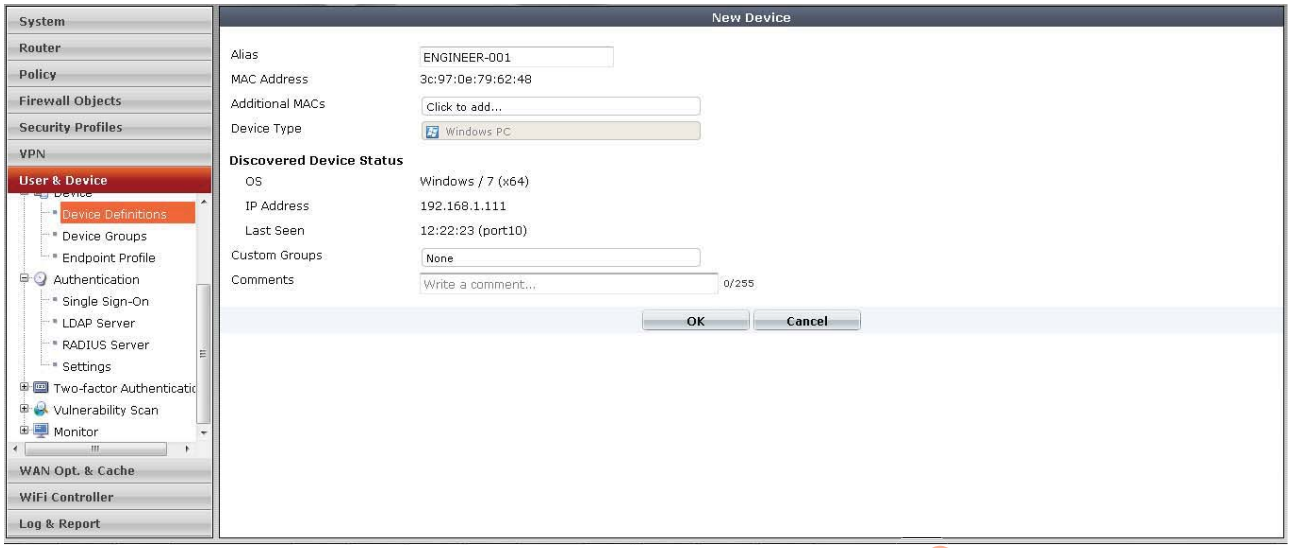
ขั้นตอนที่ 1 : เปิด Device Detect ที่ Interface ที่ต้องการทำ Policy



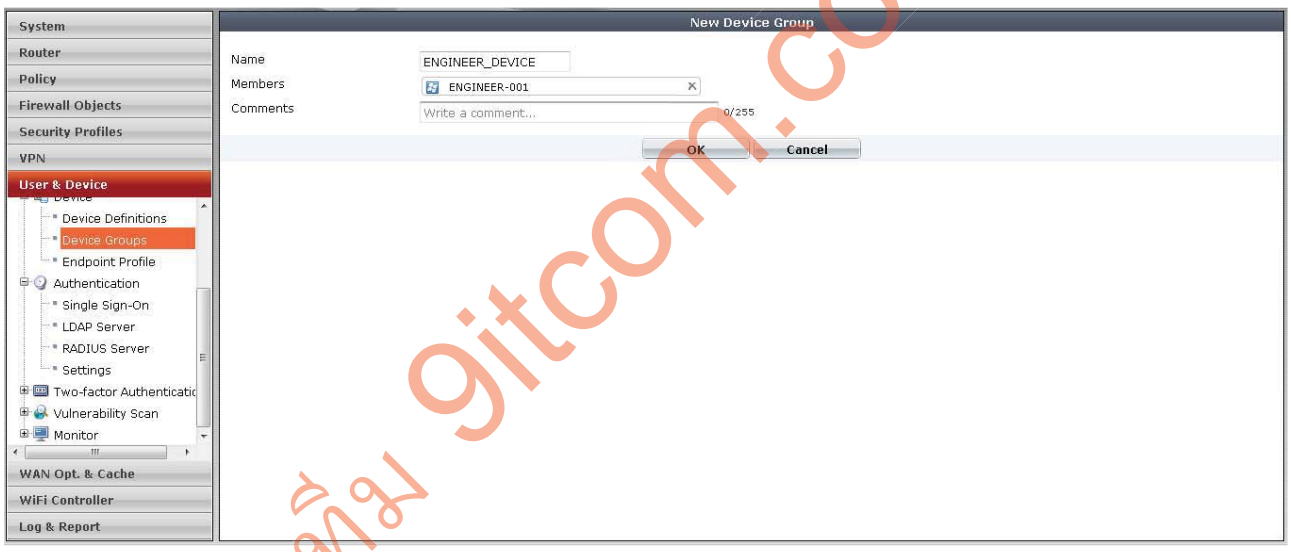
ขั้นตอนที่ 2 : FortiGate จะสามารถ Detect Device ได้



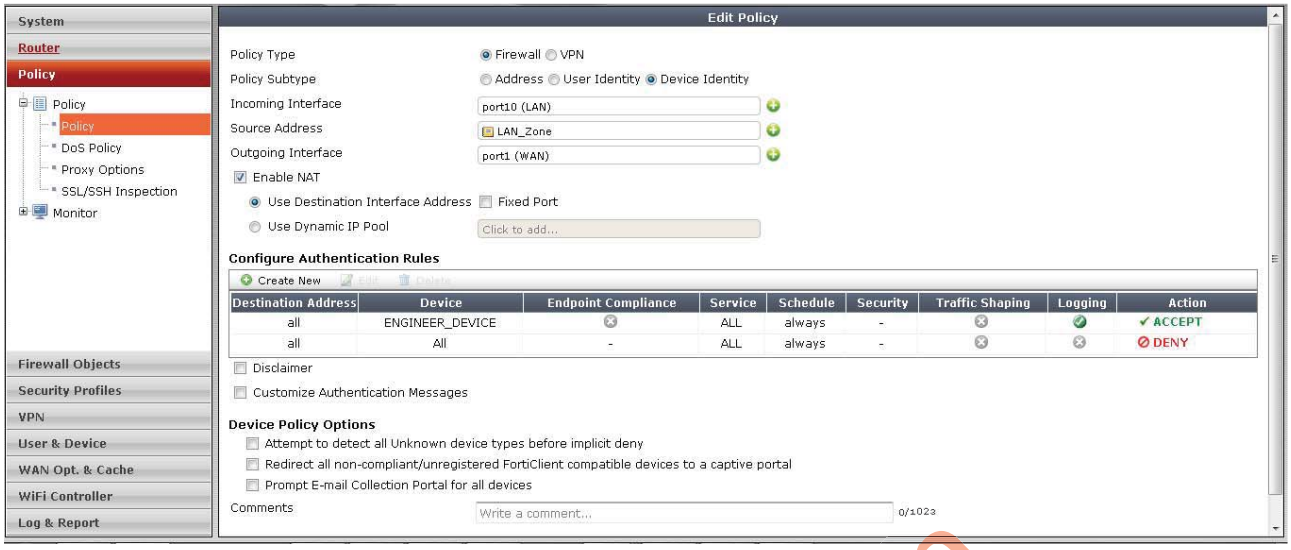
ขั้นตอนที่ 3 : ตั้งชื่อ Device

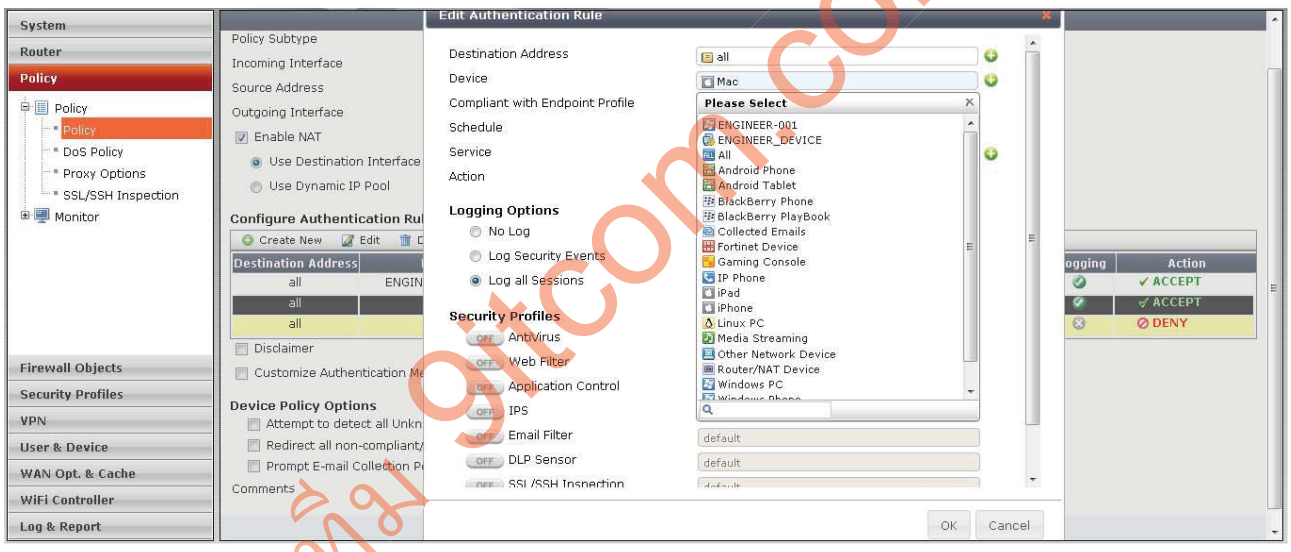


ขั้นตอนที่ 4 : นำ Device มาจัด Group



ขั้นตอนที่ 5 : เขียน Policy ที่ Auth ด้วย Device หรือ ใช้ Pre-Define Device Signature ก็ได้





การส่ง Log ไปเก็บที่ FortiAnalyzer