คู่มือการใช้งาน Virtual Firewall FortiGate

สารบัญ

เนื้อหา หน้า

Dashboard FORTIGATE....3

Network Interface FORTIGATE....3

Policy FORTIGATE....4

SSL VPN FORTIGATE....13

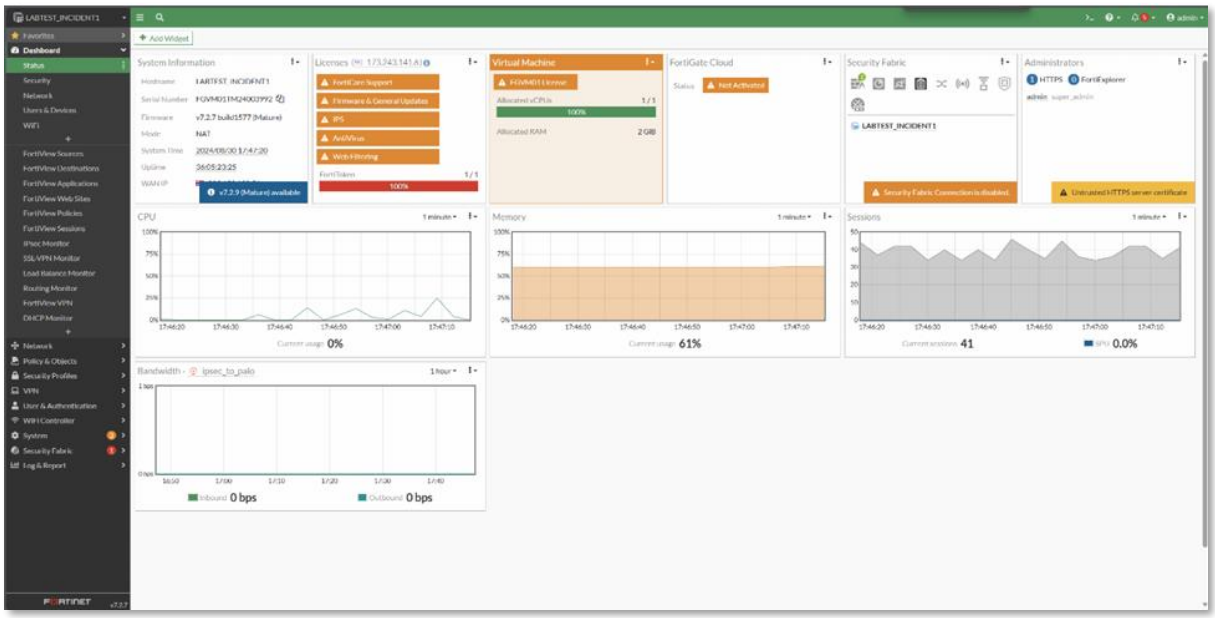
Log & Report FORTIGATE....20

TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

Firewall: FortiGate

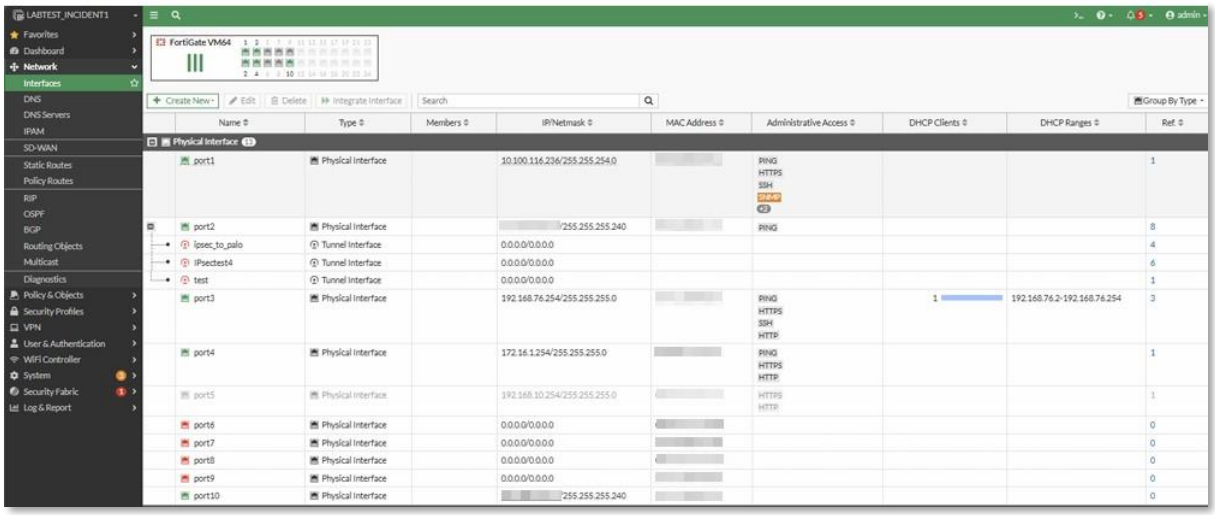
Dashboard FORTIGATE

Dashboard > Status คือหน้าหลักเมื่อเข้าใช้งานระบบ vFW FortiGate จะแสดงข้อมูลภาพรวมของ Firewall



Network Interface FORTIGATE

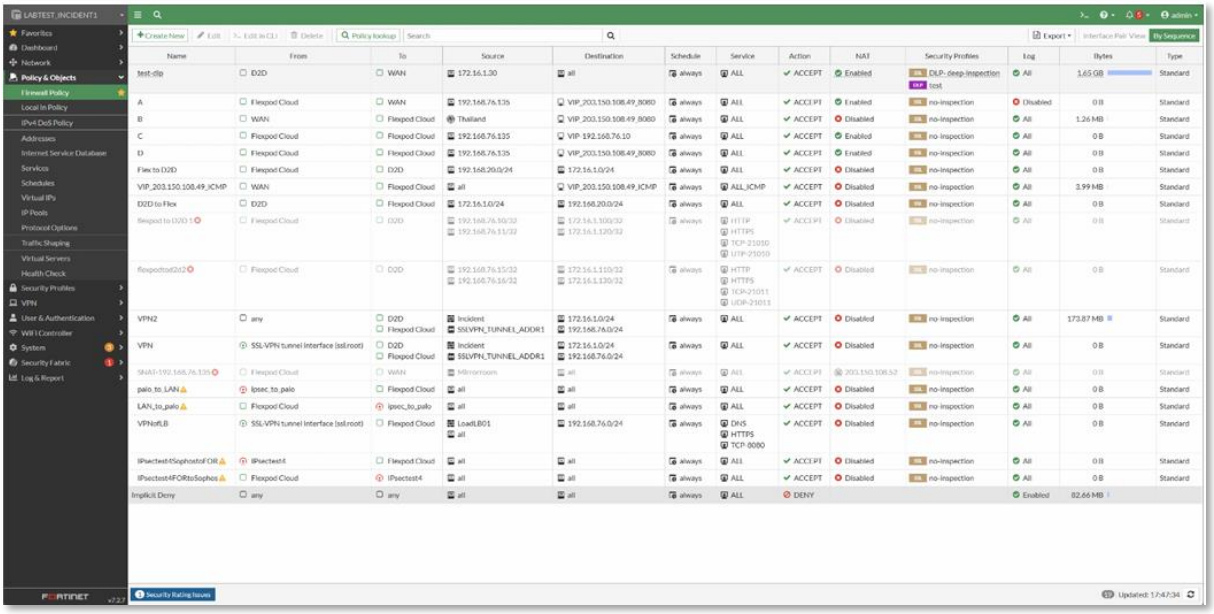
เมนู Network > Interface ใช้แสดง Interface ที่เชื่อมต่อกับ IP Network หรือ VLAN ต่างๆ รวมถึง IPSEC ที่เชื่อมอยู่ภายใต้ Firewall ด้วย



TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

Policy FORTIGATE

เข้าเมนู Policy & Objects > Firewall Policy เพื่อดูหรือตั้งค่า Policy ต่างๆ โดยลำดับการทำงานของ Policy จะเรียงลำดับเริ่มจาก ลำดับบนสุด > ลำดับล่างสุด ในการสร้าง Policy จะแบ่งเป็น Policy ขาเข้า **Inbound Policy [DNAT]** และ ขาออก **Outbound [SNAT]**



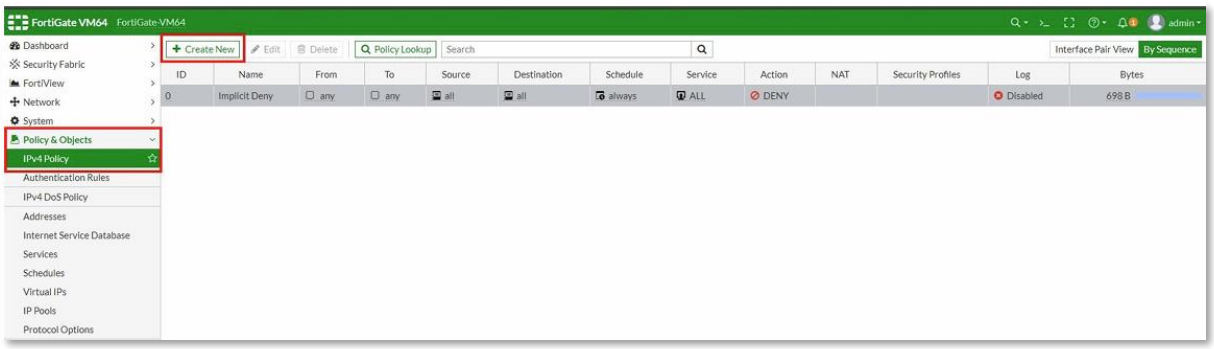
Policy ขาออก / Outbound Policy [SNAT]

Step 1: เริ่มที่ตรวจสอบ Interface เครื่องที่ต้องการว่าอยู่ที่ Interface ใด โดยดูได้จากแถบ Network >> Interface

Step 2: ให้เริ่มดู Zone ที่ต้องการทำ ตัวอย่างเช่น:

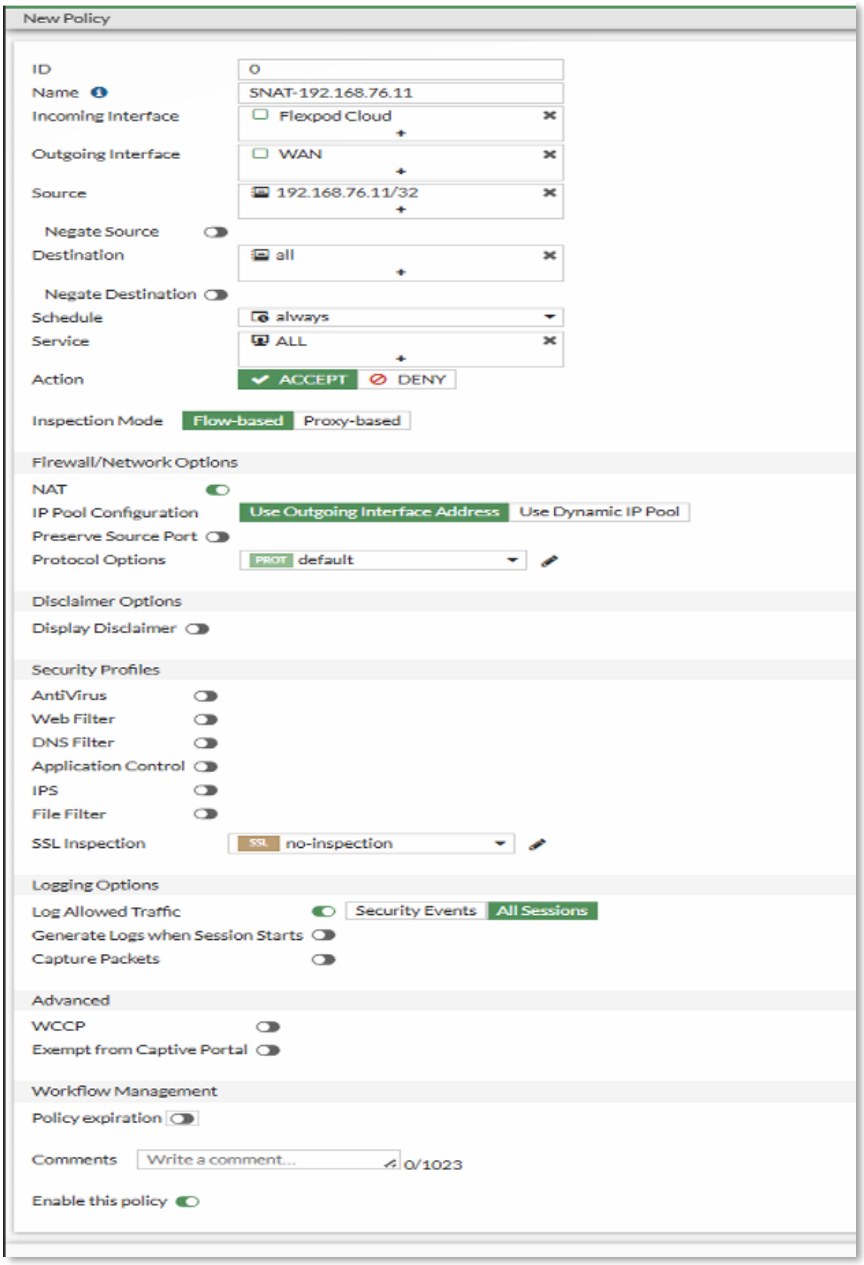
ต้องการให้เครื่อง IP: 192.168.76.11 ออก Internet ได้ zone Flexpod Cloudและ Interface port3

Step 3: Create Policy โดยเลือกแถบ Policy & Object > Firewall Policy



TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

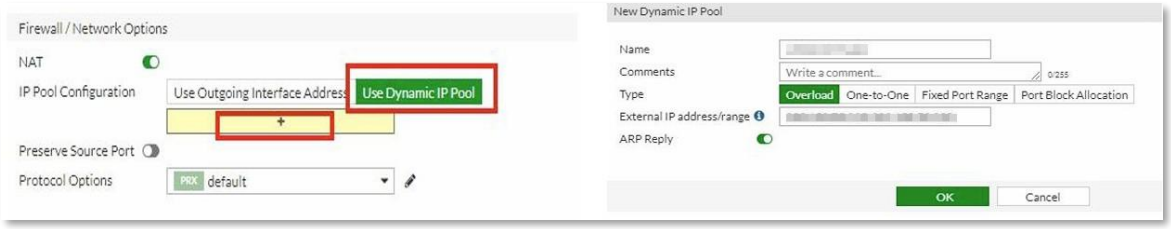
Step 4: Create policy SNAT



TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

ในหน้าต่าง **New Policy** ให้กรอกข้อมูลดังนี้

- **Name:** ตั้งชื่อให้กับ **Policy** ให้สื่อถึงการใช้งานตาม **IP** เช่น **SNAT-192.168.76.11** เป็นต้น
- **Incoming Interface:** เลือก **Interface** ที่ **Traffic** จะเข้ามา (เช่น **Flexpod Cloud).**
- **Outgoing Interface:** เลือก **Interface** ที่ **Traffic** จะออกไป (เช่น **WAN).**
- **Source:** ระบุแหล่งที่มาของ **Traffic (IP Address, Subnet,** หรือ **Object)** หากยังไม่มีจะต้องสร้าง **Object** ก่อน
- **Destination:** ระบุปลายทางของ **Traffic (IP Address, Subnet,** หรือ **Object)** หากยังไม่มีจะต้องสร้าง **Object** ก่อน
- **Schedule:** กำหนดเวลาที่ **Policy** จะทำงาน (เช่น **Always** หากต้องการให้ทำงานตลอดเวลา).
- **Service:** เลือกประเภทบริการที่ต้องการควบคุม (เช่น **HTTP, HTTPS,** หรือ **All** หากต้องการควบคุมทุก **Service)** หากยังไม่มีจะต้องสร้าง **Object** ก่อน
- **Security Profile** กรณีลูกค้ามีการใช้งานพวก **Feature App control** หรือ **Web filter** เป็นต้น
- **Logging Option** การเก็บ **Log** ให้เลือกเก็บแบบ **All Session**
- **Action:** เลือก **Allow** เพื่ออนุญาต หรือ **Deny** เพื่อปฏิเสธ **Traffic**
- **ID** ไม่จำเป็นต้องกรอก โดยหลังจาก **Create New Policy ID** จะเริ่มนับต่อจาก **ID** ล่าสุดที่ถูกสร้างขึ้นมา

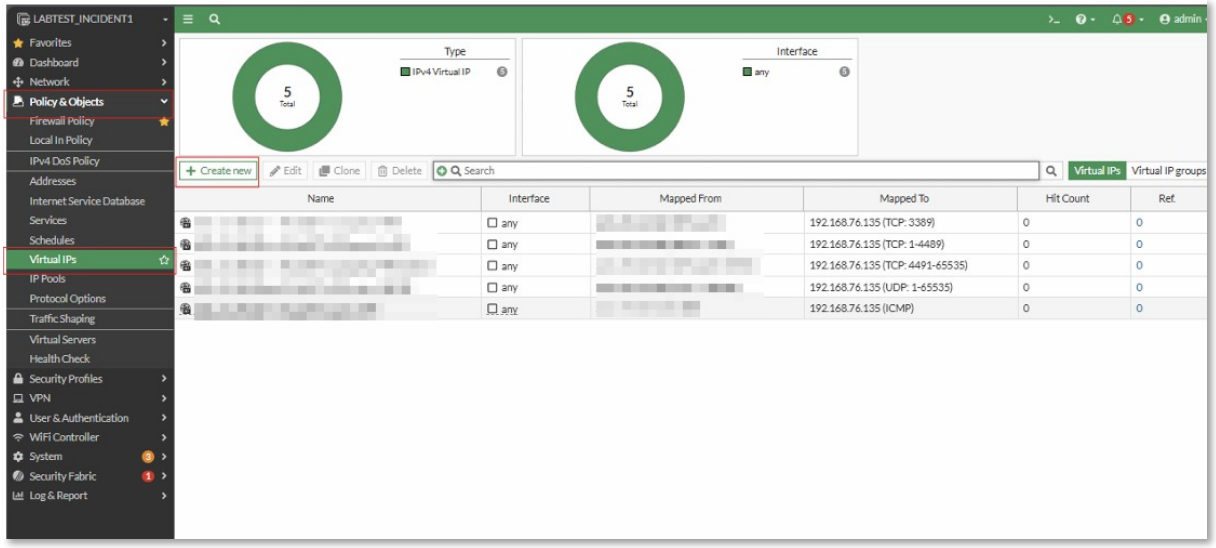


- **NAT:** เปิดใช้งานหากต้องการทำ **Network Address Translation.**
  โดยการ **NAT** จะเป็นการเปลี่ยน **IP source** เดิมให้เป็น **IP** ใหม่ ที่นี้จะเลือกใช้งานเป็น **IP interface** ตาม **interface**
  outgoing ในขอ **2** จะออกเป็น **IP 203.150.79.227** ทั้งนี้หากต้องการ **NAT** เปน **IP** อื่นๆตามที่ทางลูกค้า **request**
  ให้เลือก **Dynamic pool** แล้วจึงสร้าง **pool public** ใหม่หากยังไม่มี **object**
- หากกำหนดค่าต่างๆ เรียบร้อยแล้ว อย่าลืมที่จะ **Enable Policy**

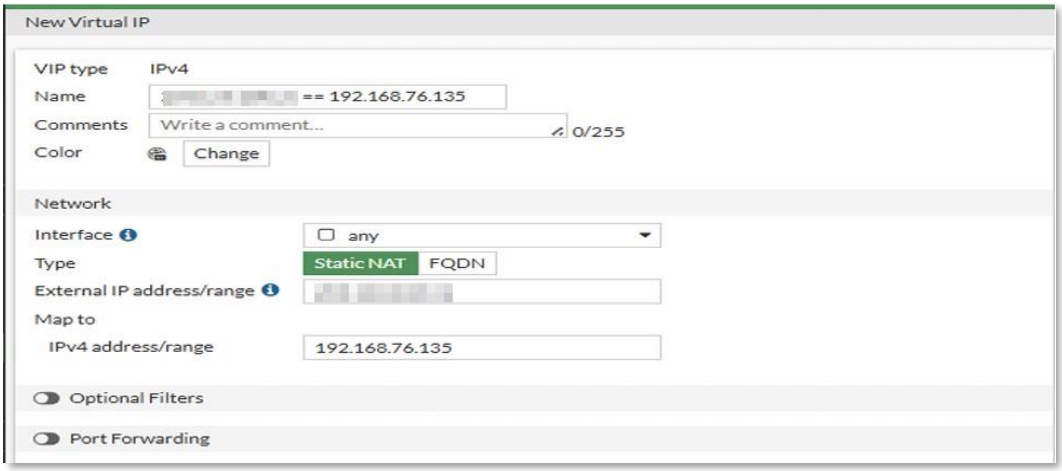
TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

Policy ขาเข้า Inbound Policy [DNAT]

Step 1: สร้าง Virtual IP (VIP) โดยการ MAP IP [WAN] เข้ากับ IP [LAN] โดยไปยังแถบ Policy & Object > Virtual IPs จากนั้นเลือก Create



- การ **MAP IP** จะได้ผลออกมาเป็น **Object** ที่ภายในมีการ **Forward packet** จาก ขา **WAN** ไปยัง ขา **LAN**



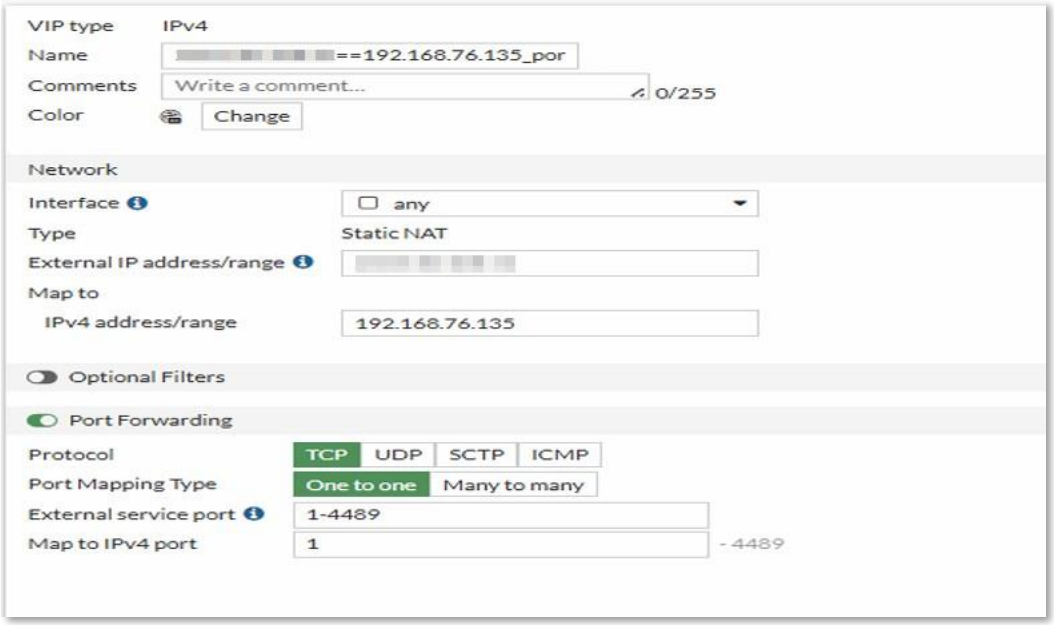
*** ในหัวข้อ **External IP** จะเป็น **IP WAN** ที่เราต้องการใช้งาน **MAP** กับ **LAN IP address**

TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

Step 2: กรณีหากลูกค้าต้องการจะทำ port forwarding ให้ดำเนินการ MAP เหมือนขั้นตอนปกติ แต่จะเพิ่มในส่วนของ Port Forwarding

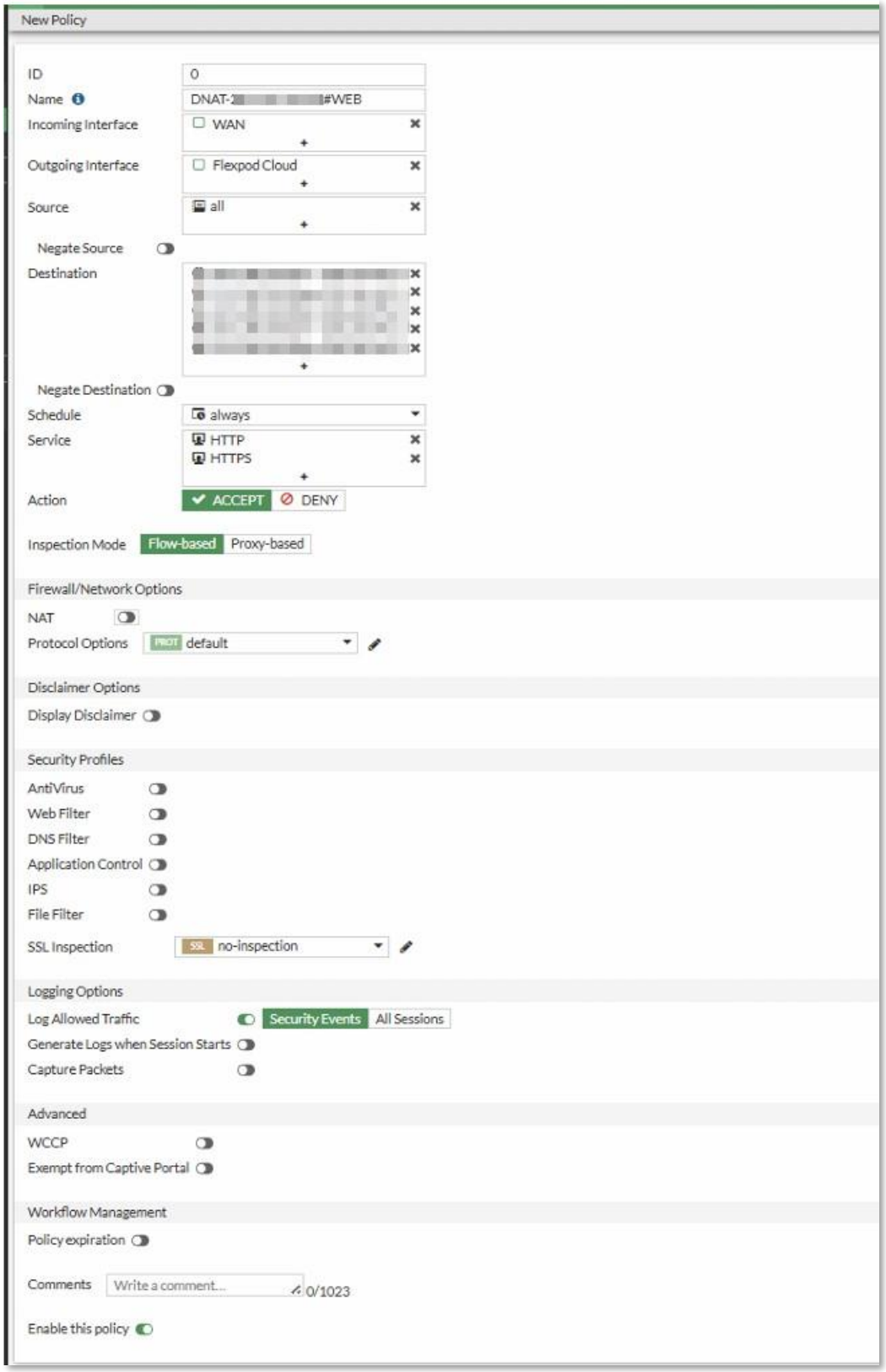
โดยส่วน Port Forwarding จะมีให้เลือกส่วน 4 ส่วน

- **Protocol:** ชนิดของ Protocol ที่ต้องการ Forward Port
- **Port Mapping Type:** ประเภทของการ Mapping Port ปกติจะเลือก one to one
- **External service port:** Port ที่จะเรียกเข้ามาจากภายนอก
- **Map to IPv4 port:** Port ที่ต้องการ Forward ต่อ



TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

Step 3: สร้าง **Policy** สำหรับ **VIP** ที่กำหนดไว้ จะเริ่มในส่วนของการ **Create Policy**



TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

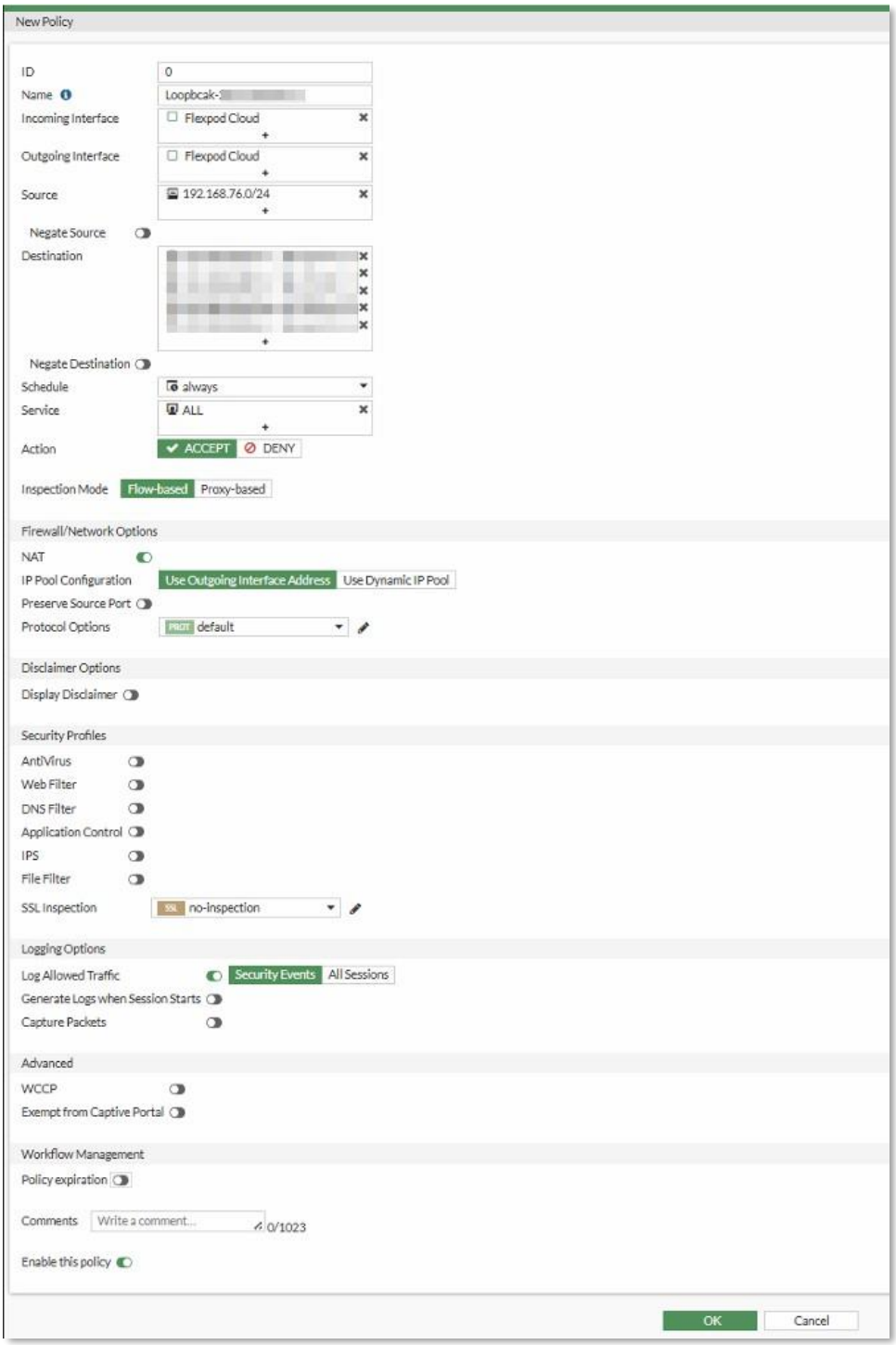
โดยในหน้าต่าง **New Policy** ให้กรอกข้อมูลดังนี้:

- **ID** ไม่จำเป็นต้องกรอก โดยหลังจาก **Create New Policy ID** จะเริ่มนับต่อจาก **ID** ล่าสุดที่ถูกสร้างขึ้นมา
- **Name:** ตั้งชื่อให้กับ **Policy**
- **Incoming Interface:** เลือก **Interface** ที่ **Traffic** จะเข้ามา (เช่น **WAN).**
  โดยปกติของ **Policy DNAT** ส่วนใหญ่จะเข้ามาจาก **Interface Wan** แต่ก็สามารถเข้ามาจาก **Interface** อื่นๆได้ เช่น **LAN** จะเป็นส่วนของ **Policy Loopback**
- **Outgoing Interface:** เลือก **Interface** ที่ **Traffic** จะออกไป (เช่น **Flexpod Cloud).**
  จะต้องเลือกจาก **Interface** ที่เครื่องปลายทางอยู่เช่น **192.168.76.135** อยู่ **Flexpod Cloud** เป็นต้น
- **Source:** ระบุแหล่งที่มาของ **Traffic (IP Address, Subnet,** หรือ **Object).** หากยังไม่มีจะต้องสร้าง **Object** ก่อน
- **Destination:** ระบุปลายทางของ **Traffic (IP Address, Subnet,** หรือ **Object).** หากยังไม่มีจะต้องสร้าง **Object** ก่อน
- **Schedule:** กำหนดเวลาที่ **Policy** จะทำงาน (เช่น **Always** หากต้องการให้ทำงานตลอดเวลา).
- **Service:** เลือกประเภทบริการที่ต้องการควบคุม (เช่น **HTTP, HTTPS,** หรือ **All** หากต้องการควบคุมทุก **Service).** หากยังไม่มีจะต้องสร้าง **Object** ก่อน
- **Security Profile** กรณีลูกค้ามีการใช้งานพวก **Feature App control** หรือ **Web filter**
  การใช้งาน **Feature** ต่างๆ *** มีข้อควรระวัง คือหากมีการเปิดใช้อาจส่งผลกระทบต่อการใช้งานเพราะอาจมีบาง **feature** ที่เป็นการ **block service** เป็นต้น
- **Logging Option** การเก็บ **Log** ให้เลือกเก็บแบบ **All Session**
- **Action:** เลือก **Allow** เพื่ออนุญาต หรือ **Deny** เพื่อปฏิเสธ **Traffic**
- **NAT:** เปิดใช้งานหากต้องการทำ **Network Address Translation.**
  โดยการ **NAT** จะเป็นการเปลี่ยน **IP source** เดิมให้เป็น **IP** ใหม่ หากมีการเปิดใช้งาน **source** ดังกล่าวจะถูกเปลี่ยนเป็น **IP** ตามที่กำหนด และ บางทีอาจจะทำให้ไม่ทราบ **Source IP** ที่แท้จริงที่เรียกเข้ามาได้
- หากกำหนดค่าต่างๆ เรียบร้อยแล้ว อย่าลืมที่จะ **Enable Policy** เป็นอันเรียบร้อย

TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

Step 4: Policy Loopback

กรณีที่เครื่องอยู่ภายใต้ **Firewall** เดียวกัน เรียกมายัง **IP Public** ของที่ภายใต **Firewall** เดียวกัน เช่นกัน โดยลักษณะของ **Policy** จะสร้างคลายๆของ **Policy DNAT** แต่จะแตกตางที่ **Source Interface** จะเป็น **Interface** ภายใต้ **Firewall** ไม่ใช้ **WAN** และ มีการ **NAT Source** เพิ่มเพื่อให้สามารถเรียกไปยัง **IP Public** ที่อยู่ภายใต้ **Firewall** เดียวกันได้



TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

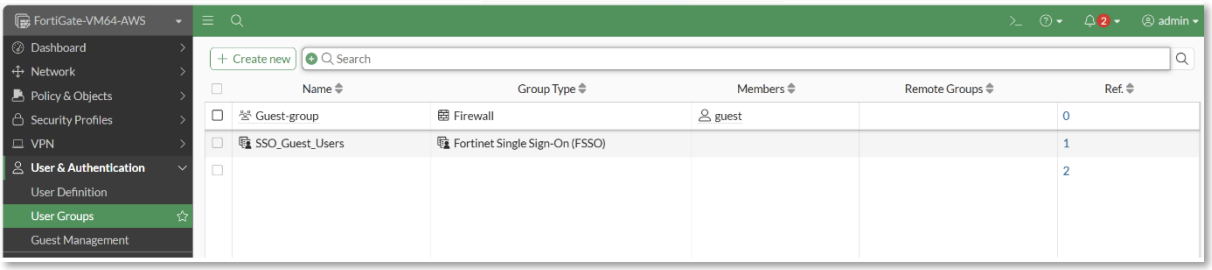
โดยในหน้าตาง **New Policy** ให้กรอกข้อมูลดังนี้:

- **ID** ไม่จำเป็นต้องกรอก โดยหลังจาก **Create New Policy ID** จะเริ่มนับต่อจาก **ID** ล่าสุดที่ถูกสร้างขึ้นมา
- **Name:** ตั้งชื่อให้กับ **Policy**
- **Incoming Interface:** เลือก **Interface** ที่ **Traffic** จะเข้ามา (เช่น **Flexpod Cloud).**
  โดยปกติของ **Policy DNAT** ส่วนใหญ่จะเข้ามาจาก **Interface Wan** แต่ก็สามารถเข้ามาจาก **Interface** อื่นๆได้ เช่น **LAN** จะเป็นส่วนของ **Policy Loopback**
- **Outgoing Interface:** เลือก **Interface** ที่ **Traffic** จะออกไป (เช่น **Flexpod Cloud).**
  จะต้องเลือกจาก **Interface** ที่เครื่องปลายทางอยู่เช่น 192.168.76.135 อยู่ **Flexpod Cloud** เป็นต้น
- **Source:** ระบุแหล่งที่มาของ **Traffic (IP Address, Subnet,** หรือ **Object).** หากยังไม่มีจะต้องสร้าง **Object** ก่อน
- **Destination:** ระบุปลายทางของ **Traffic (IP Address, Subnet,** หรือ **Object).** หากยังไม่มีจะต้องสร้าง **Object** ก่อน
- **Schedule:** กำหนดเวลาที่ **Policy** จะทำงาน (เช่น **Always** หากต้องการให้ทำงานตลอดเวลา).
- **Service:** เลือกประเภทบริการที่ต้องการควบคุม (เช่น **HTTP, HTTPS,** หรือ **All** หากต้องการควบคุมทุก **Service).**
- **Security Profile** กรณีลูกค้ามีการใช้งานพวก **Feature App control** หรือ **Web filter**
  การใช้งาน **Feature** ต่างๆ *** มีข้อควรระวัง คือหากมีการเปิดใช้อาจส่งผลกระทบต่อการใช้งานเพราะอาจมีบาง **feature** ที่เป็นการ **block service** เป็นต้น
- **Logging Option** การเก็บ **Log** ให้เลือกเก็บแบบ **All Session**
- **Action:** เลือก **Allow** เพื่ออนุญาต หรือ **Deny** เพื่อปฏิเสธ **Traffic**
- **NAT:** เปิดใช้งานหากต้องการทำ **Network Address Translation.**
  โดยการ **NAT** จะเป็นการเปลี่ยน **IP source** เดิมให้เป็น **IP** ใหม่ให้เป็น วง **Network** ภายใต้ **Firewall** เพื่อให้สามารถเรียกไปยังปลายทางที่เป็น **IP Public** ที่อยู่ภายใต้ **Firewall** เดียวกันได้ ตัวอย่างเช่น 192.168.76.135 **NAT** 192.168.76.254 เป็นต้น
- หากกำหนดค่าต่างๆ เรียบร้อยแล้ว อย่าลืมที่จะ **Enable Policy** เป็นอันเรียบร้อย

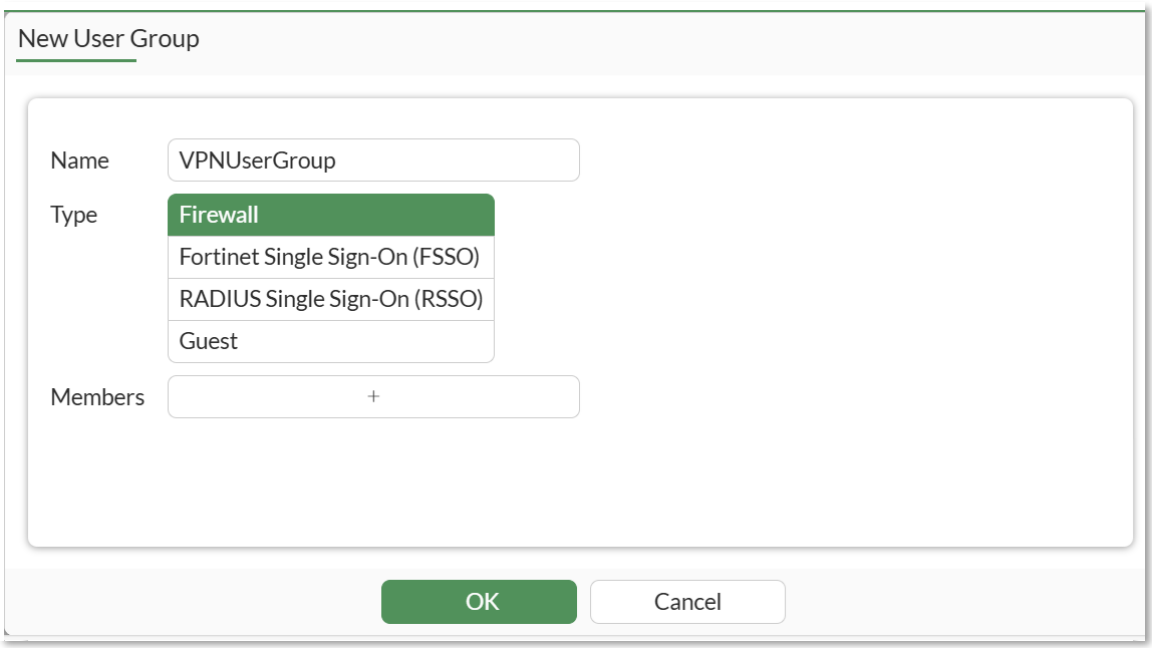
TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

SSL VPN FORTIGATE

Step 1: เริ่มต้นด้วยการสร้าง User VPN Group User & Authentication > User Groups > Create New

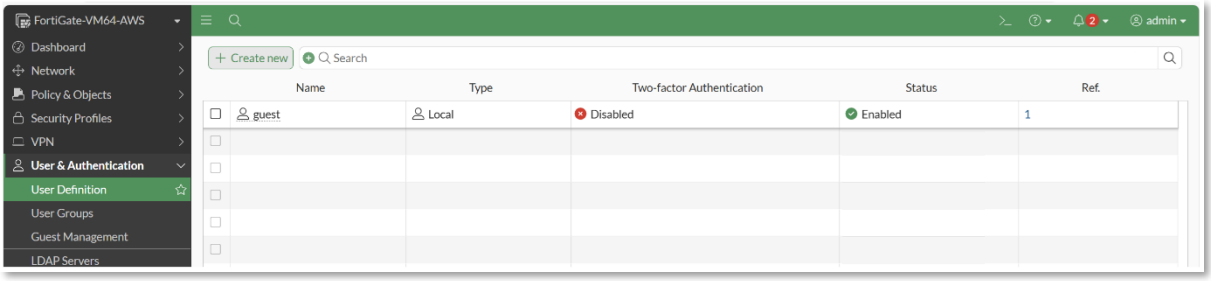


- กำหนดชื่อ **Group >** จากนั้นกดที่ **OK**

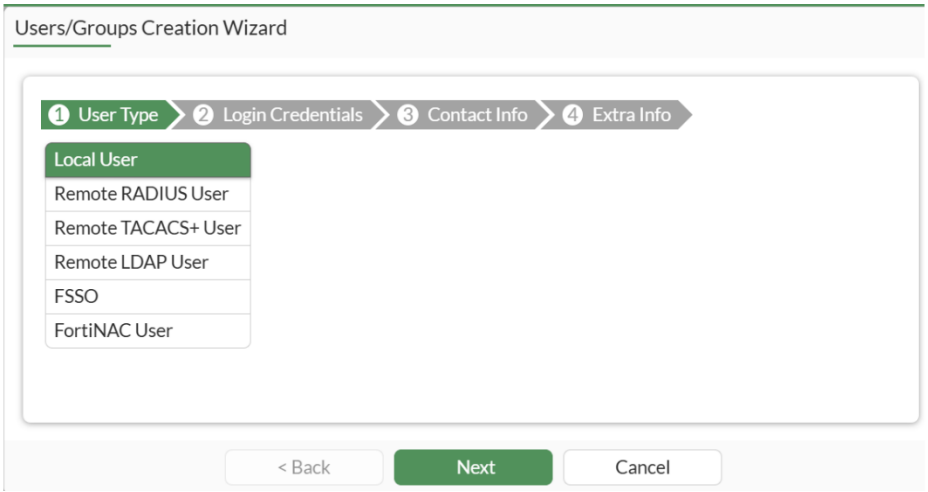


TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

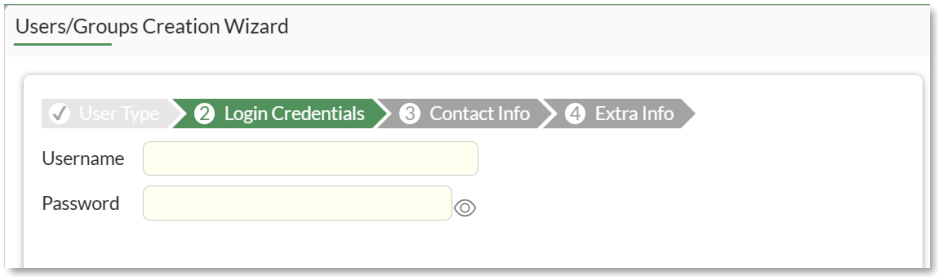
Step 2: สร้าง User ใหม่ ไปที่ User & Authentication > User Definition > Create New

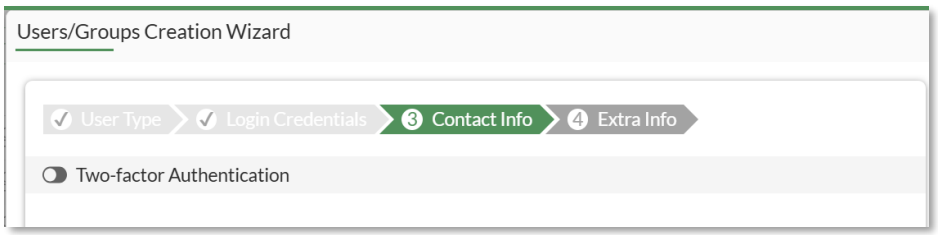


- เลือกไปที่ Local User > Next



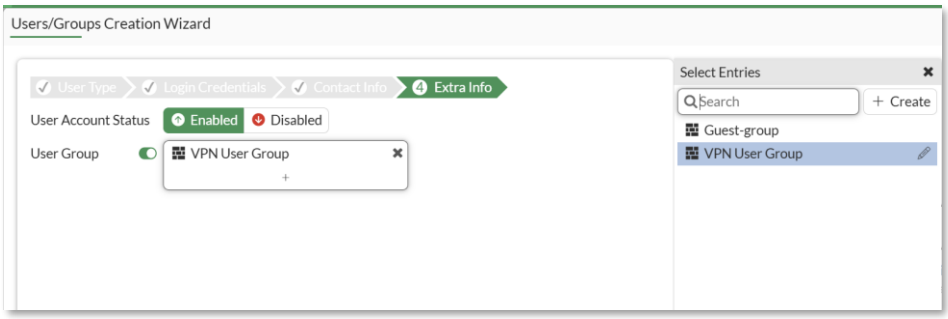
- กำหนด **Username / Password** ให้เรียบร้อย **> Next //** หาไม่มี **2FA** ให้ **Next** ข้ามไปก่อนได้เลย



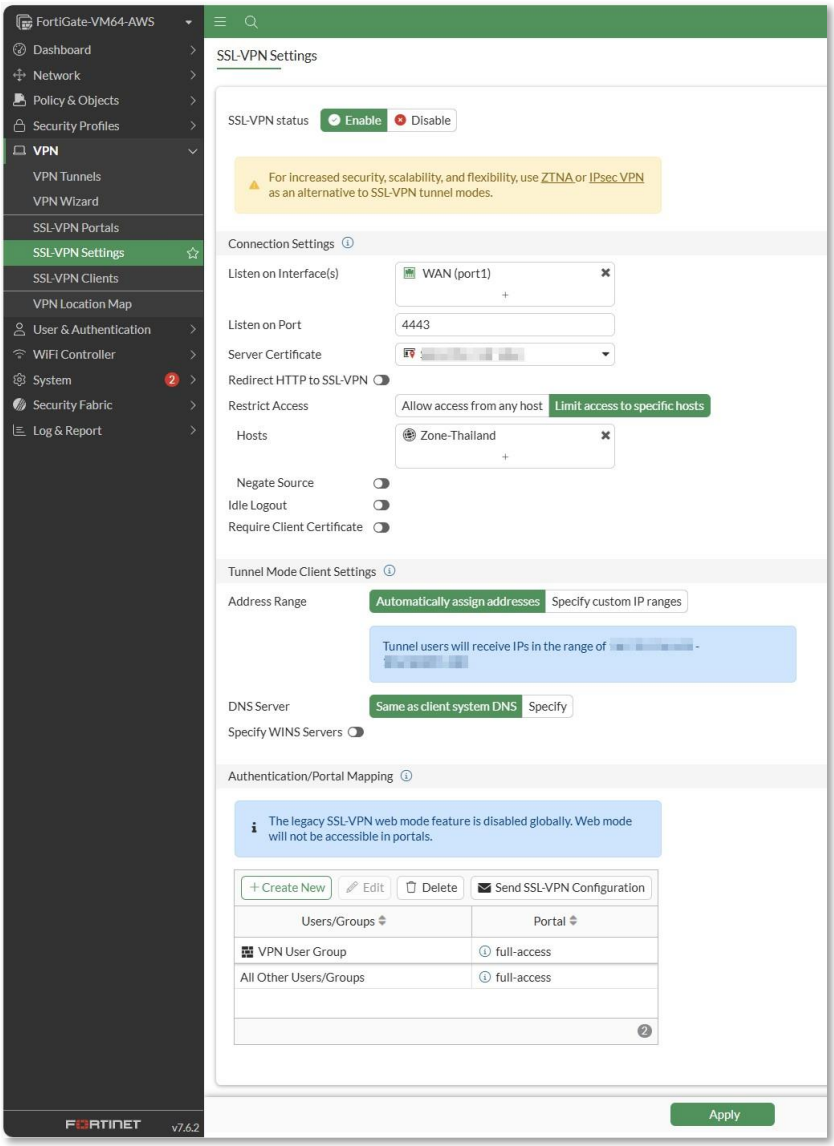


TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

- เลือก **Enable** กดเลือก **User Group** เป็น **group** ที่สร้างไว้ตอน **Step 1** แล้วกด **OK** เป็นอันเสร็จสมบูรณ์ ในการสร้าง **User VPN**

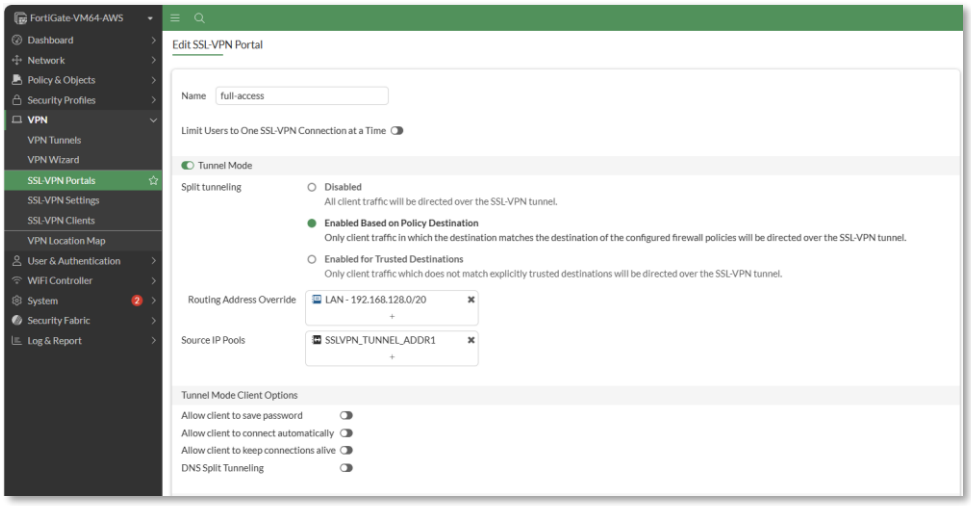


Step 3: ที่ **SSL-VPN Setting** ตรง **Authentication/Portal Mapping** กด **Create New Group** ที่เราสร้างแล้วเลือก **Full Access**



TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

- ไปที่หน้า SSL-VPN Portal กดที่ full access แล้วกด edit จากนั้น Enable Split Tunneling ออก แล้วกด OK



Step 4: สร้าง Policy สำหรับการใช้งาน SSL-VPN โดยในหน้าต่าง New Policy ให้กรอกข้อมูลดังนี้:

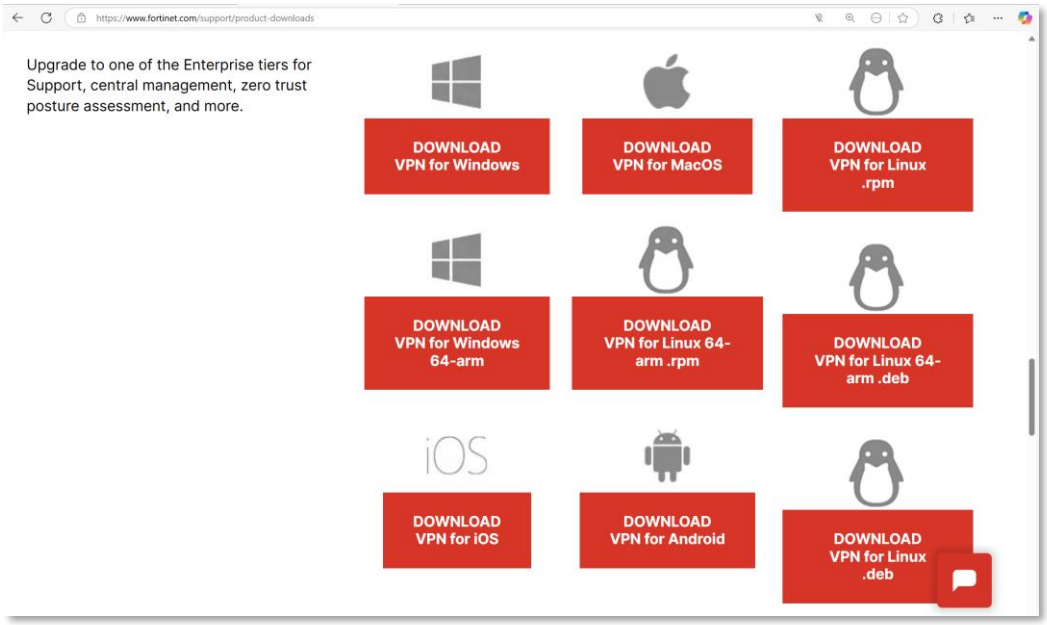
- ID ไม่จำเป็นต้องกรอก โดยหลังจาก Create New Policy ID จะเริ่มนับต่อจาก ID ล่าสุดที่ถูกสร้างขึ้นมา
- Name: ตั้งชื่อให้กับ Policy ให้สื่อถึงการใช้งานตาม IP เช่น VPN TO CLOUD เป็นต้น
- Incoming Interface: เลือก Interface ที่ Traffic จะเข้ามา (เช่น SSL-VPN tunnel interface (ssl.root)). โดยปกติของ Policy ของ SSL VPN จะเลือก SSL-VPN tunnel interface (ssl.root) เป็น Interface
- Outgoing Interface: เลือก Interface ที่ Traffic จะออกไป (เช่น Flexpod Cloud). จะต้องเลือกจาก Interface ที่เครื่องปลายทางอยู่เช่น 192.168.76.0/24 อยู่ Flexpod Cloud
- Source: ระบุแหล่งที่มาของ Traffic (IP Address, Subnet, หรือ Object). หากยังไม่มีจะต้องสร้าง Object ก่อน
- Destination: ระบุปลายทางของ Traffic (IP Address, Subnet, หรือ Object). หากยังไม่มีจะต้องสร้าง Object ก่อน
- Schedule: กำหนดเวลาที่ Policy จะทำงาน (เช่น Always หากต้องการให้ทำงานตลอดเวลา).
- Service: เลือกประเภทบริการที่ต้องการควบคุม (เช่น HTTP, HTTPS, หรือ All หากต้องการควบคุมทุก Service).
- Logging Option การเก็บ Log ให้เลือกเก็บแบบ All Session
- Action: เลือก Allow เพื่ออนุญาต หรือ Deny เพื่อปฏิเสธ Traffic
- หากกำหนดค่าต่างๆ เรียบร้อยแล้ว อย่าลืมที่จะ Enable Policy เป็นอันเรียบร้อย

TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

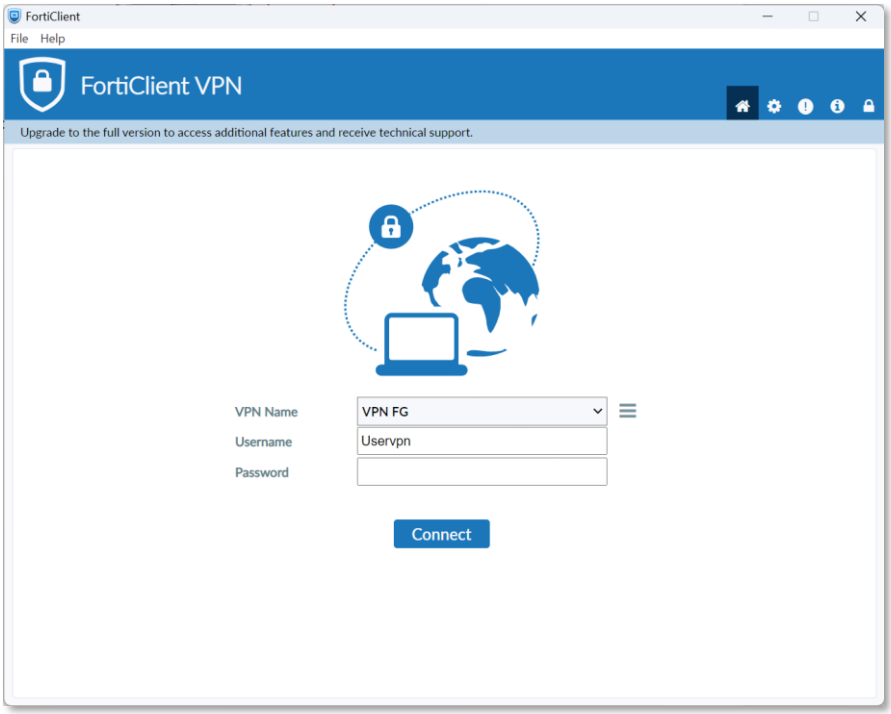
FortiClient VPN

Download Client VPN จาก https://www.fortinet.com/support/product-downloads

- เลือก Product Download > Forticlient VPN Only



- หลังจากติดตั้ง Forticlient ที่เป็น Program สำหรับการ VPN เรียบร้อยแล้ว
- เลือก แถบ 3 ขีด > Add a new Connection



TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

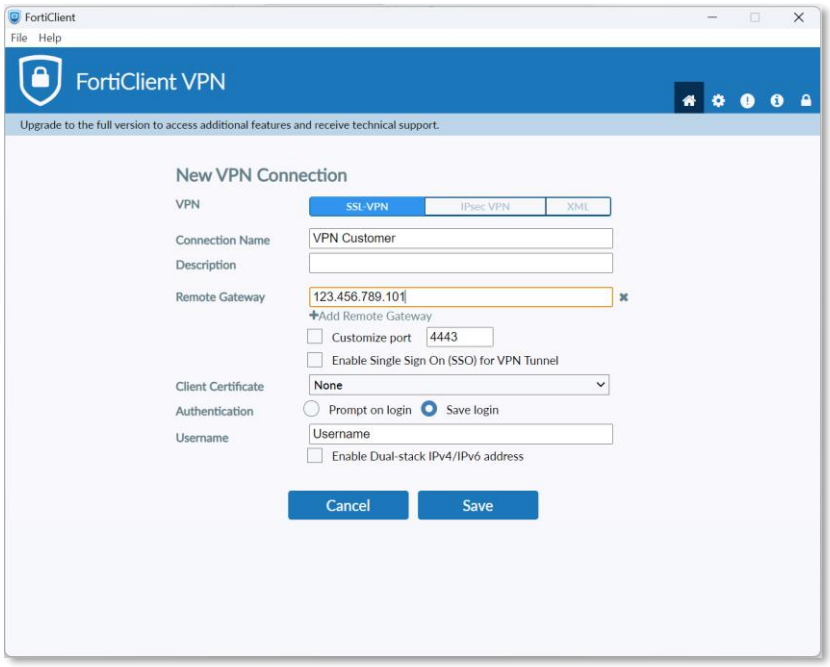
- กำหนดค่า **SSL-VPN Connection** ตามที่ระบบ **Firewall** กำหนดไว้ดังนี้

  1) Connection Name: CPN customer

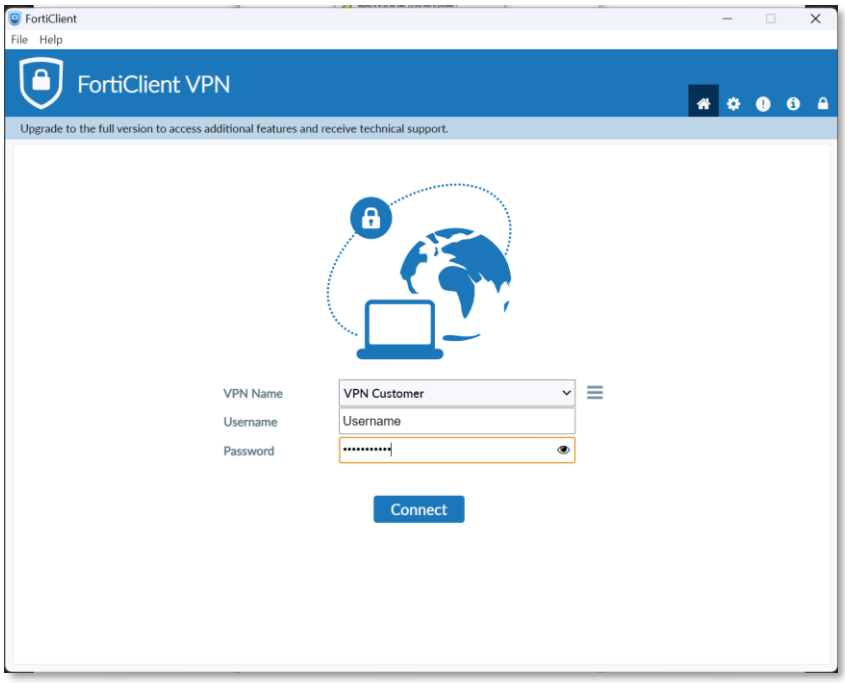
  2) Remote Gateway: xxx.xxx.xxx.xxx (IP Public ของ Firewall)

  3) ทำเครื่องหมายถูกที่ช่อง **Customize port** และระบุค่าเป็น **4443**

  4) คลิกปุ่ม **Save**

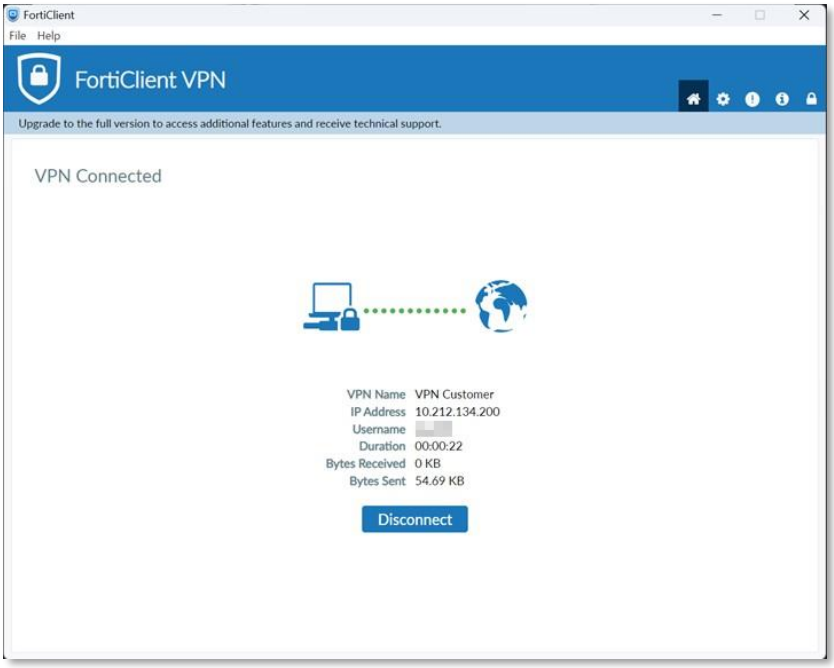


- กรอก **Username** และ **Password** ที่ใช้ **Login** เข้าเครื่องคอมพิวเตอร์ที่ทำงาน
- คลิกปุ่ม **Connect**



TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

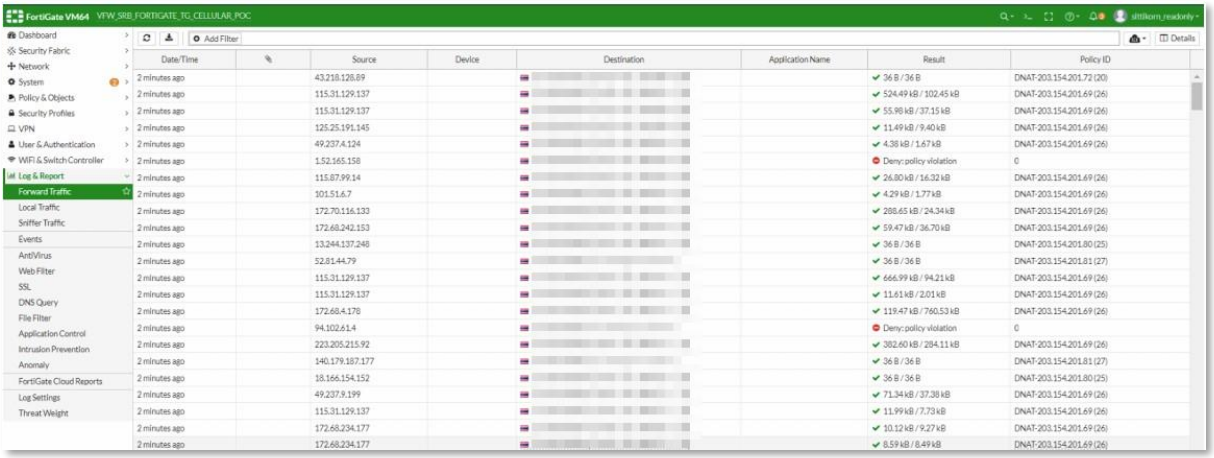
- หาก **Config SSL VPN** ถูกต้อง และ **Login** สำเร็จจะได้ผลตามรูปด้านล่าง



TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

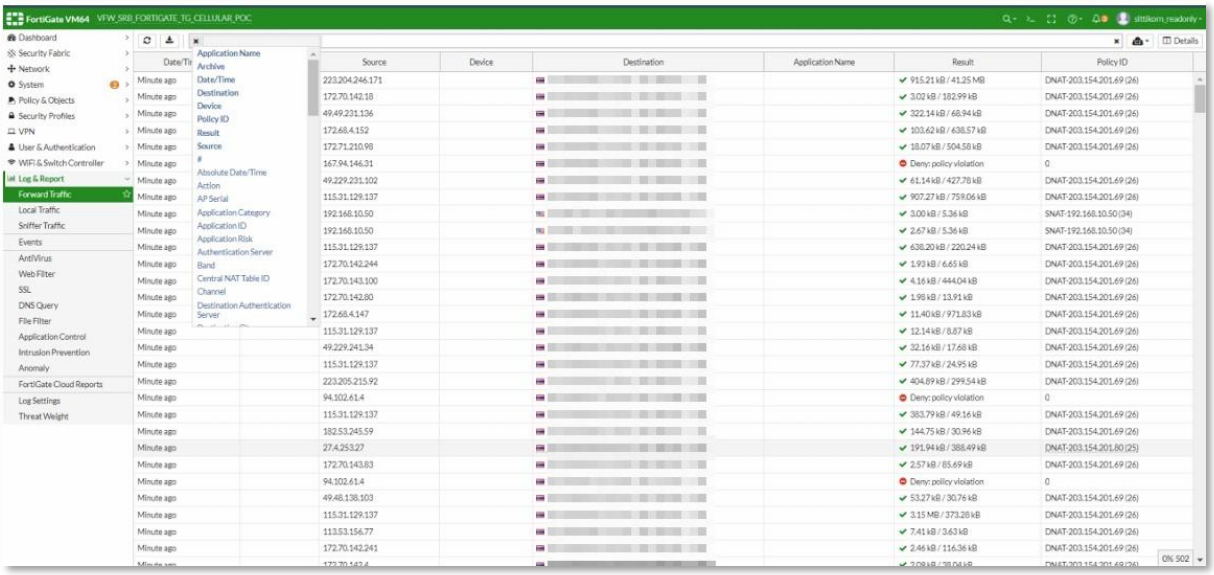
Log & Report FORTIGATE

Step 1: ในการดู **Log** จะเข้ามาที่แถบ **Log&Report > Forward Traffic** โดยจะโชว์ **Log** ขึ้นมาดังภาพ



Step 2: ตัวอย่างการใช้แถบค้นหาข้อมูล

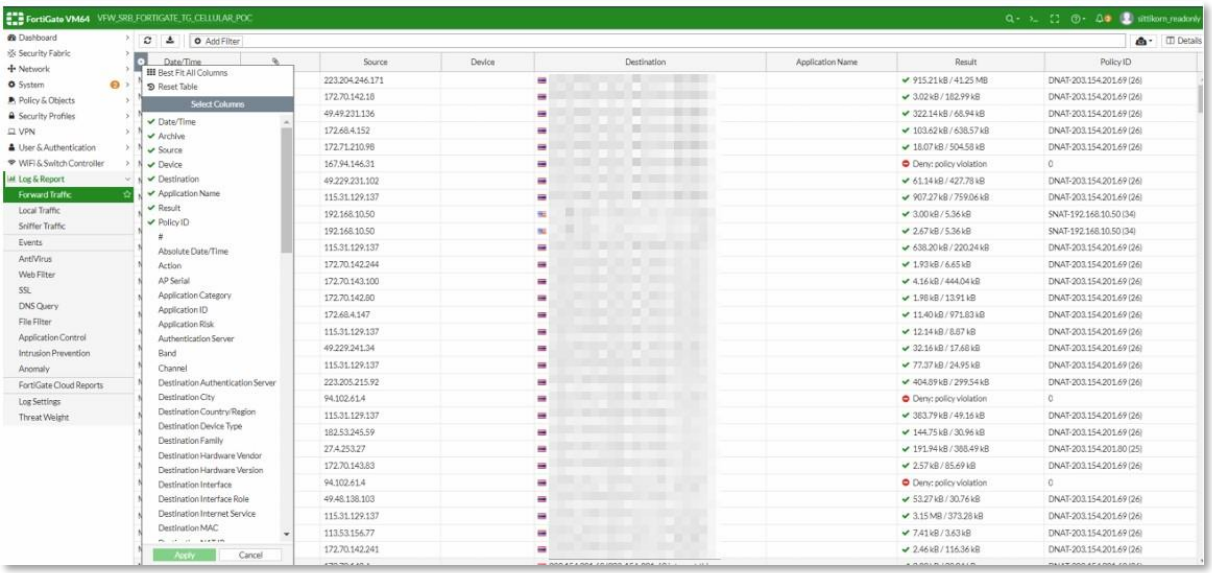
ในแถบค้นหาสามารถกด **add filter** เพื่อกำหนดขอบเขตการค้นหาได้ จะมีหัวข้อให้เลือกดังภาพ



TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770

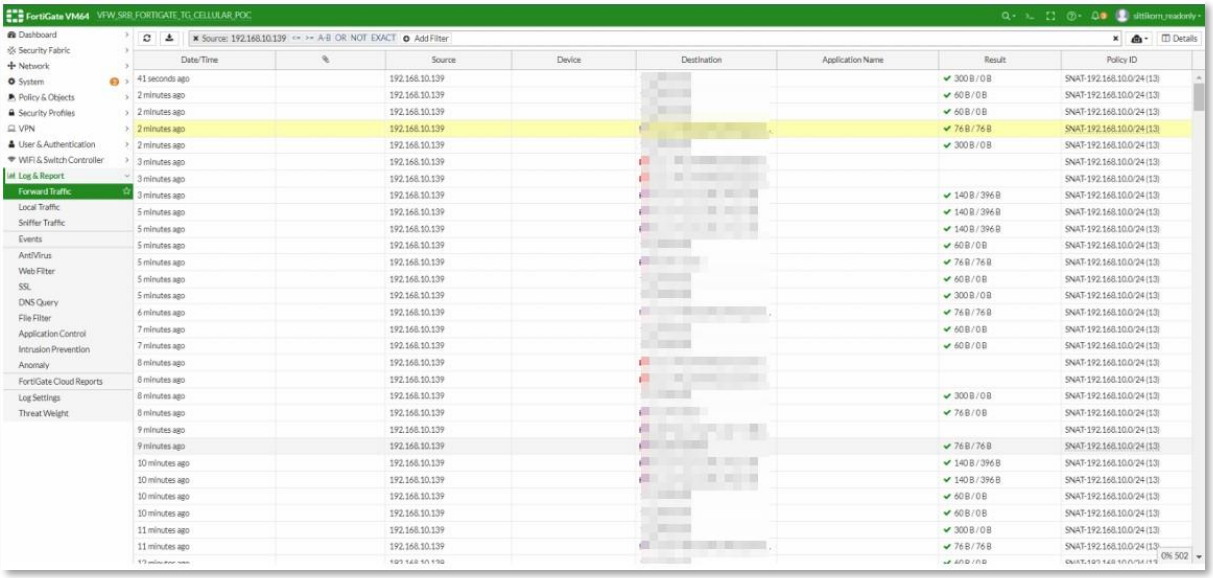
ตัวอย่างการใช้แถบค้นหาข้อมูล

สามารถ คลิกขวาที่แถบ **column** เพื่อทำการเพิ่ม/ลด **column** ที่ต้องการแสดงได้



ตัวอย่างการใช้แถบค้นหาข้อมูล

ตัวอย่างการค้นหาโดยกำหนด **filter** เป็น **IP source**



TEL +66 2017 7777
FAX +66 2017-7778
CALL CENTER +66 2017 7770