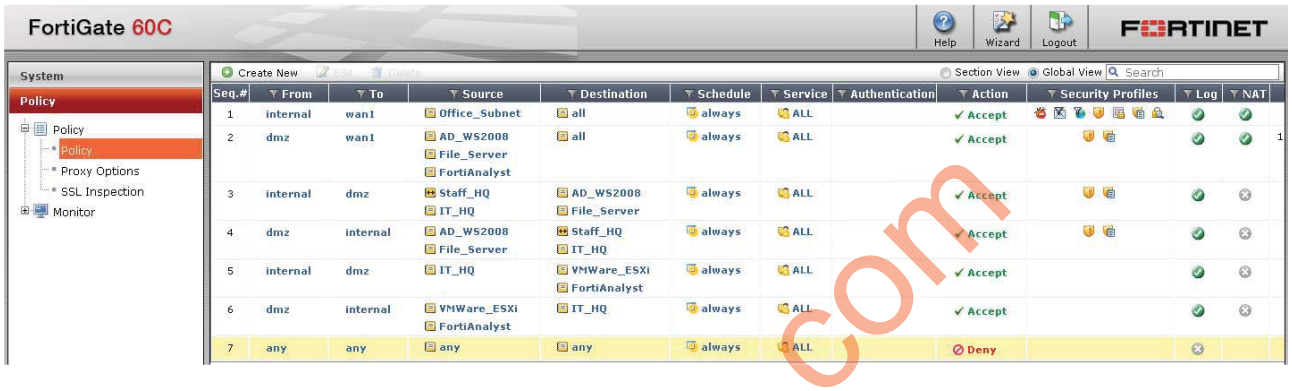
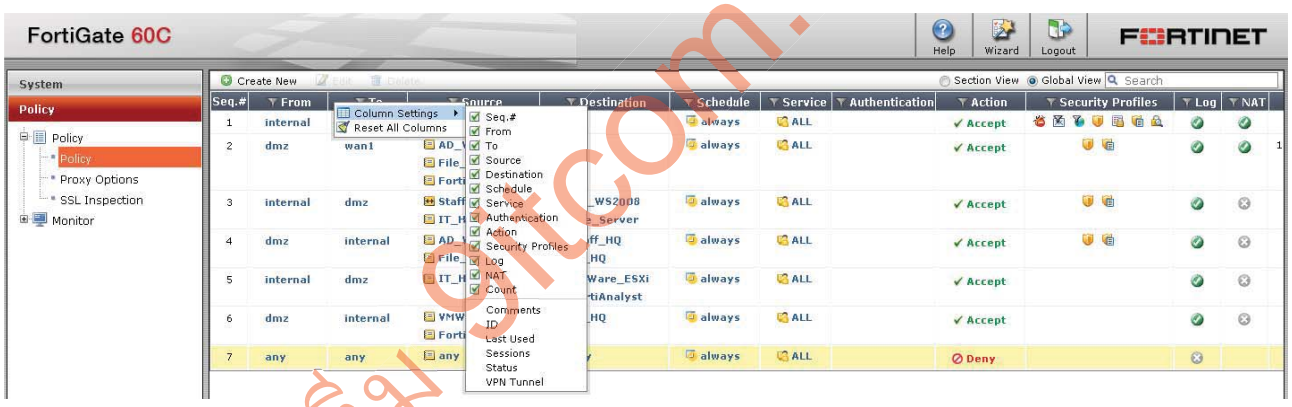
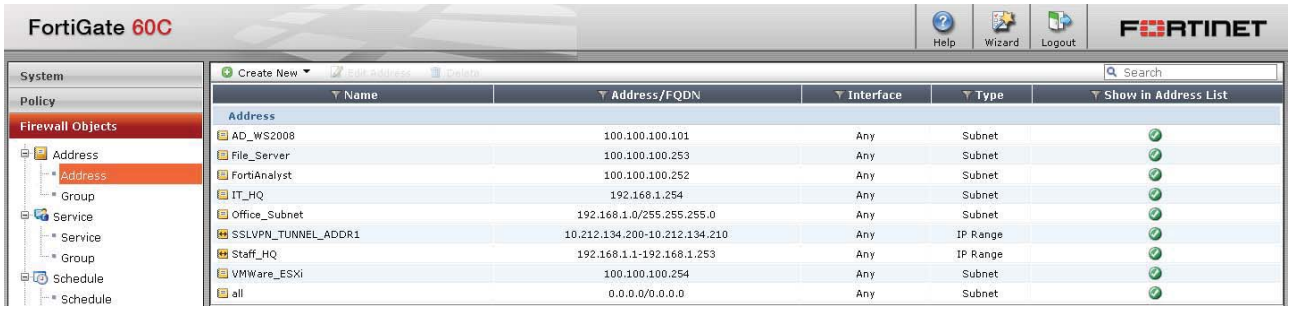


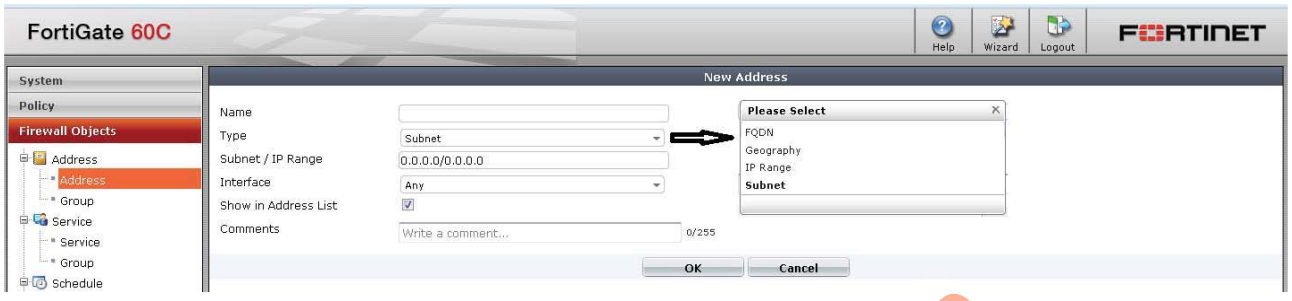


หัวข้อที่ควรทราบ

1. Policy นั้นใช้สำหรับสร้าง Firewall Policy ซึ่งจะมี Address ,User Identify ,Device Indentify
2. สำหรับการอ่าน Policy นั้น FortiGate จะมี Option ให้ผ่านได้ 2 แบบ
   a. Session View จะเป็นการอ่าน Policy ตาม Interface เช่น Intrenal => Wan1
   b. Global View จะเป็นการอ่าน Policy ตาม Sequent การทำงานของ Firewall

หมายเหตุ : สำหรับการ View ทั้ง 2 แบบสามารถเพิ่ม Filed ได้ ที่ใช้งานบ่อยๆได้แก่ ID ,Count ,Status





หัวข้อที่ควรทราบ Firewall Objects (Address)

1. สำหรับสร้าง Object ที่เป็น Address ขึ้นมาสำหรับไปใช้งานใน Firewall Policy

   a. FQDN คือ Fully Qualified Domain Name เช่น facebook.com ,youtube.com

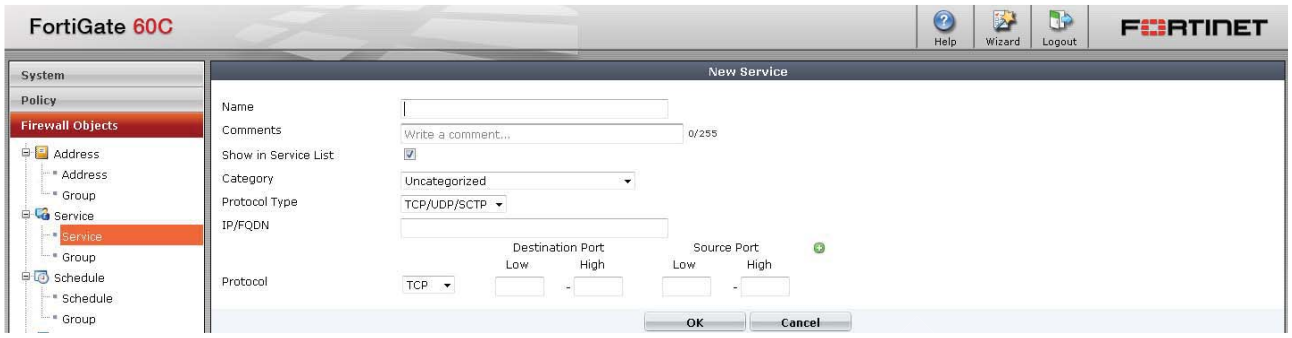
   b. Geography คือ IP Address ที่ถูก Assign ให้ประเทศต่างๆ

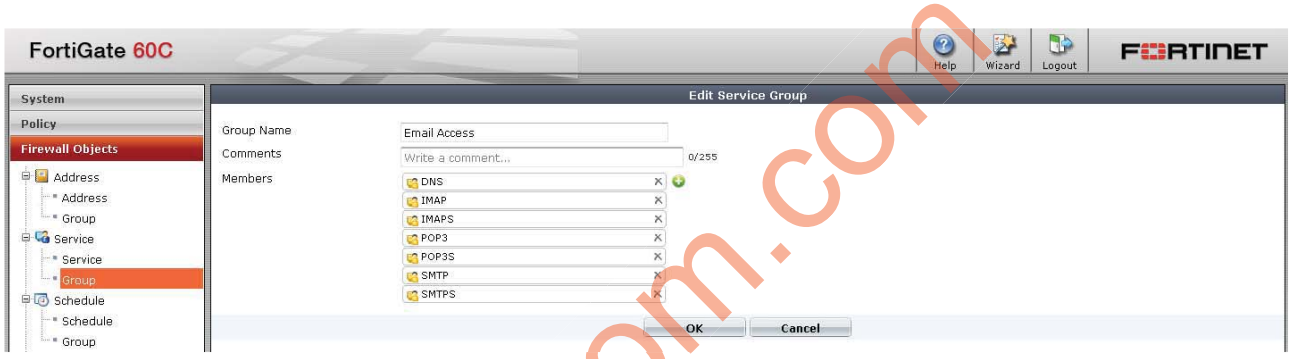
   c. IP-Range คือ ช่วงของ IP Address เช่น 192.168.100.1-192.168.1.50

   d. Subnet คือ กลุ่มของ IP Address ทั้งหมายเลข Subnet เช่น 192.168.100.0/24

หมายเหตุ :

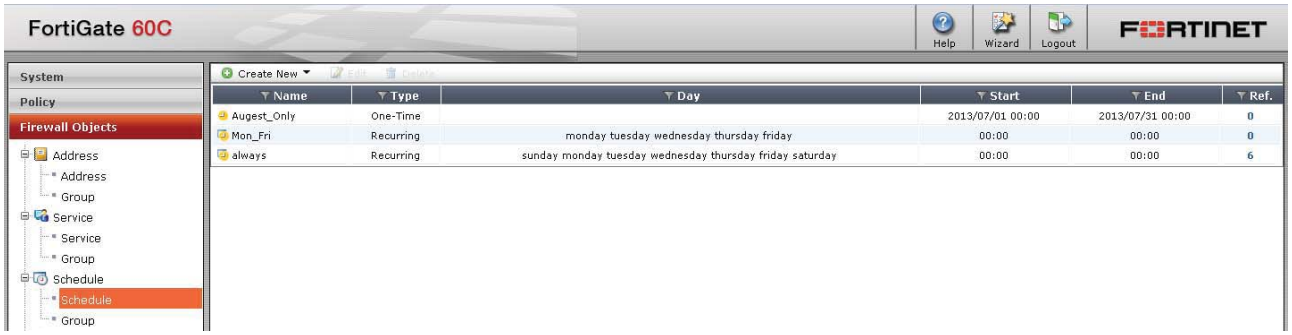
ตัวเลือก Interface กรณีมีการเลือกไว้ Object Address นี้จะสามารถใช้งานได้ต่อเมื่อเลือก Interface นั้นๆ ขึ้นมาใช้งานใน Firewall Policy กรณี ต้องการใช้งานรวมๆ ให้เลือกเป็น “Any”

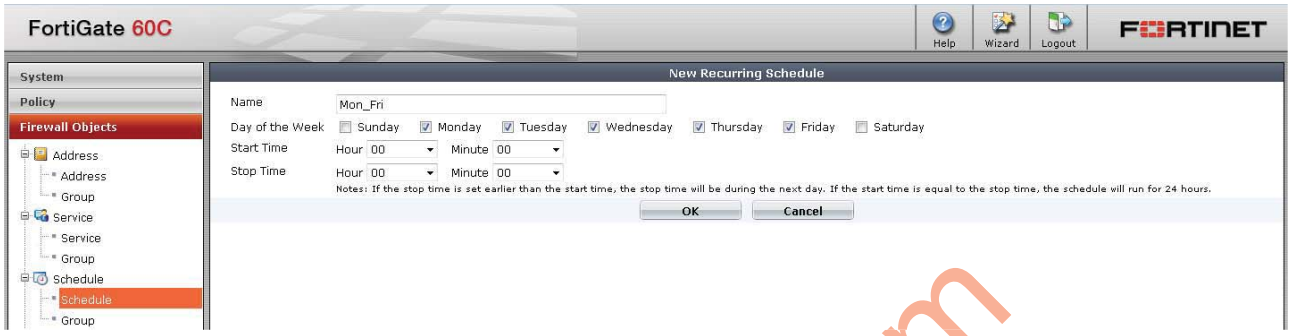


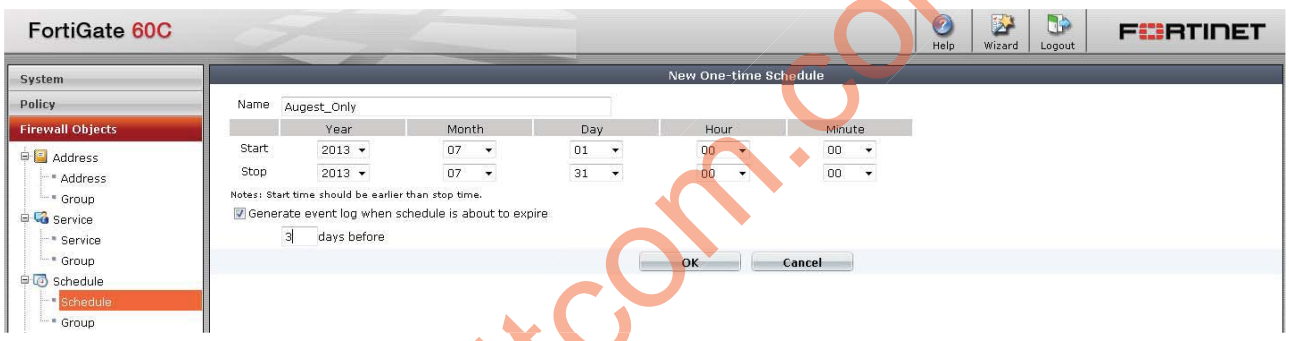


หัวข้อที่ควรทราบ Firewall Objects (Service)

สำหรับการสร้าง Object ที่เป็น Service นั้นโดยส่วนใหญ่ FortiGate จะมี Service มาตรฐานที่เป็น Pre-Define มาให้แล้ว แต่กรณีต้องการสร้าง Custom Service ขึ้นมาใช้งานเองใน Service Object ก็สามารถที่จะสร้างขึ้นมาได้ โดย กำหนดชื่อ รวมถึง Protocol ใช้งาน และ Source Port ,Destination Port เองตาม Custom Service ที่ลูกค้าต้องการใช้งาน กรณีที่ต้องการรวม Service หลายๆ ตัวเข้าเป็น Group นั้นก็สามารถทำขึ้นมาได้โดยการ Create “Group Service” และรวม Service หลายๆตัวเข้าด้วยกัน

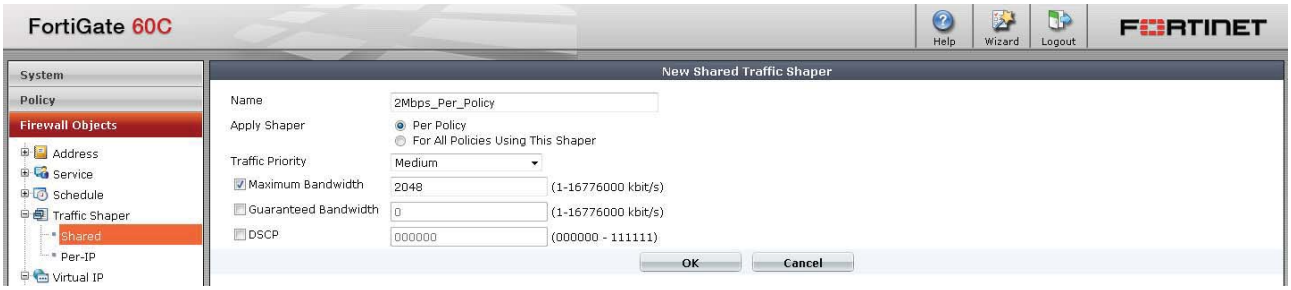


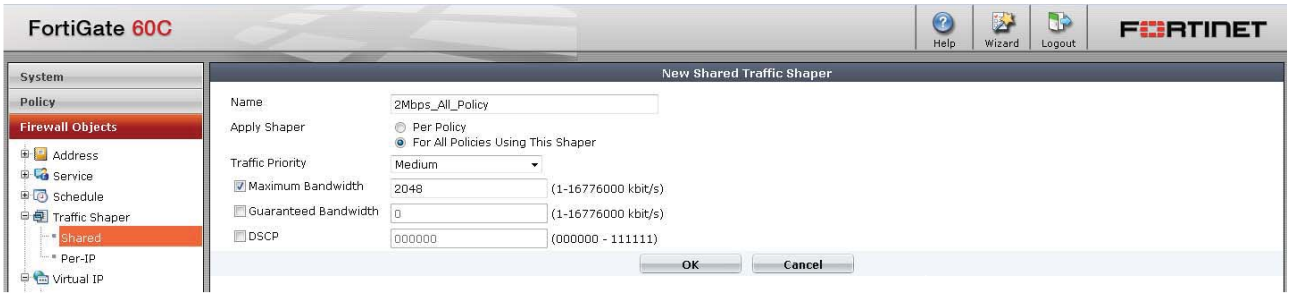


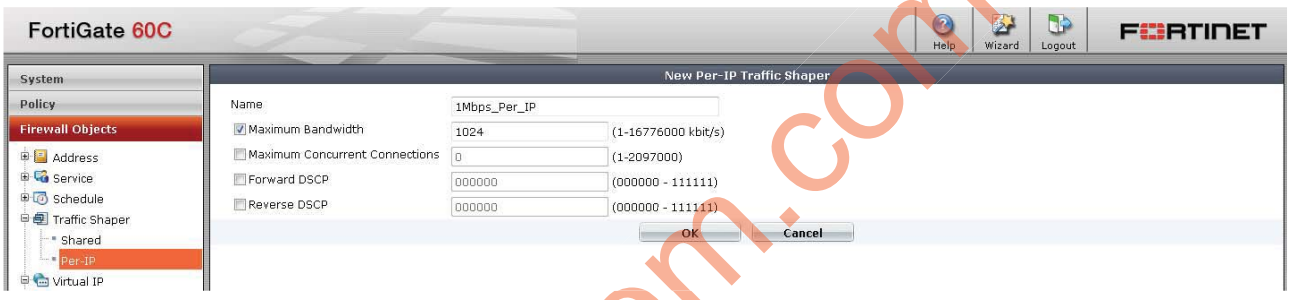


หัวข้อที่ควรทราบ Firewall Objects (Schedule)

สำหรับการสร้าง Object ที่เป็น Schedule นั้นโดย ค่ามาตรฐานของ FortiGate จะมี “Always” มาให้ใช้งานเป็นค่าเริ่มต้น สำหรับกรณีที่ลูกค้าต้องการสร้าง Schedule ขึ้นมาเพื่อให้ Firewall ทำงานสำหรับ Policy นั้นๆตามช่วงเวลาที่เราก็หมดขั้นมาเอาห็สามารถทำได้ โดย FortiGate นั้นจะรองรับรูปแบบการสร้าง Schedule ทั้งแบบ “Recurring” ช่วงเวลานั้นๆตลอดไป และ แบบ One-Time คือช่วงเวลาตามที่กำหนดเท่านั้น และสำหรับ Object Schedule นั้นก็สามารถที่จะรวบเป็น Group ได้

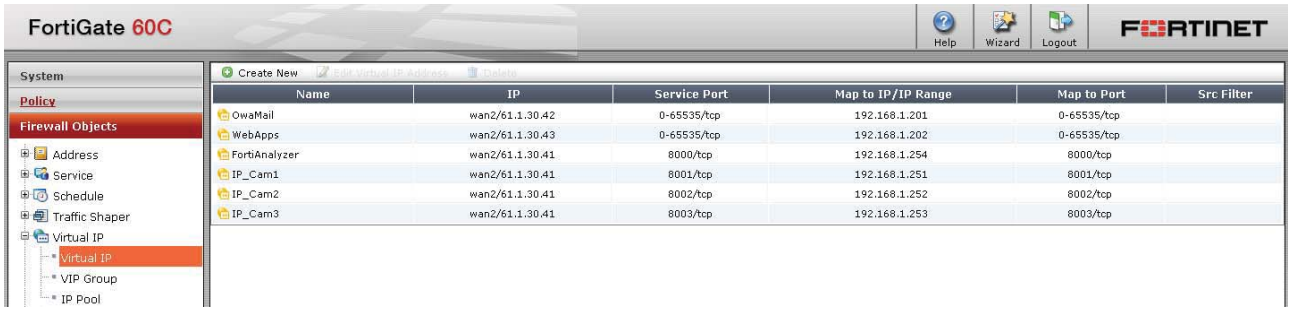


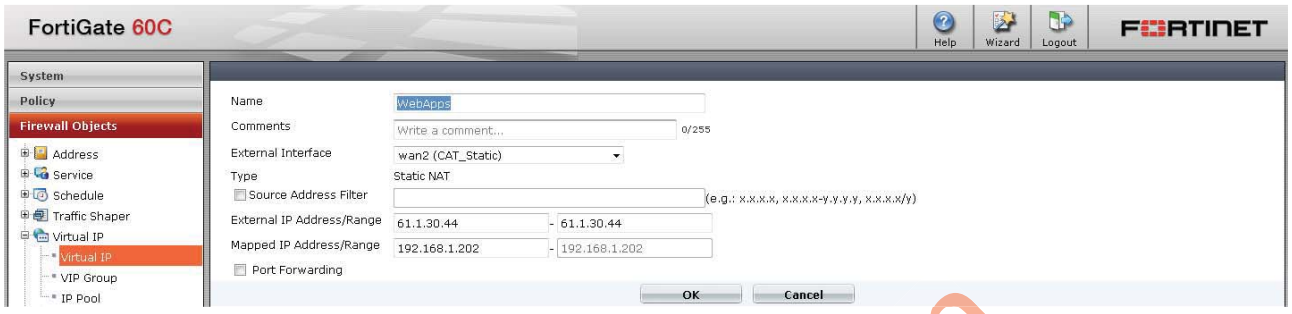


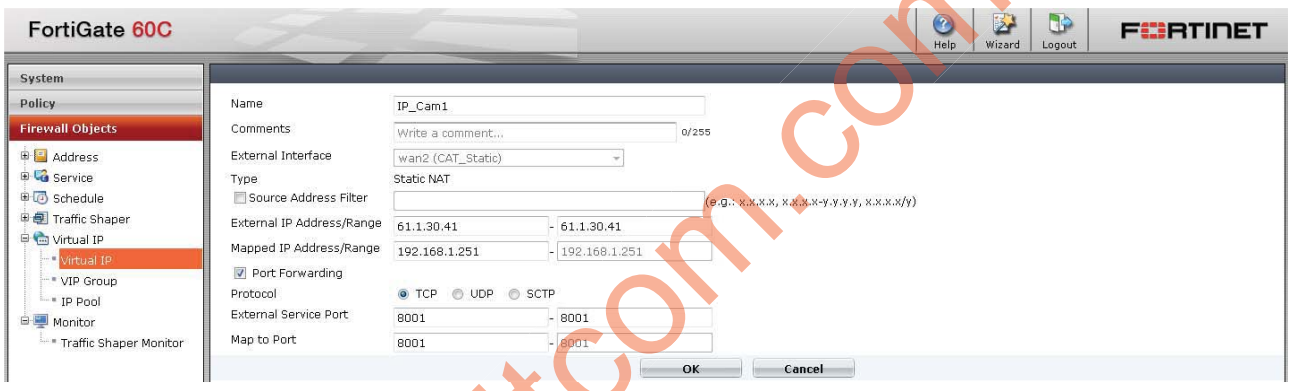


หัวข้อที่ควรทราบ Firewall Objects (Traffic Shaper)

สำหรับการสร้าง Object ที่เป็น Traffic Shaper นั้นจะมีอยู่ด้วยกัน 2 แบบ “Shared ,Per IP” โดยสำหรับ Shared นั้นจะแบ่งย่อยเป็น “Per Policy” กรณีนำไปใช้งานจะเป็น Traffic ที่ถูกนำไปใช้งานเฉพาะ Policy นั้นๆ เท่านั้น ส่วน “For All Policy” นั้นจะเป็นท่อ Traffic Shaper ที่ใช้งานร่วมกันทุก Policy ที่ใช้งาน Object Traffic Shaper ตัวนี้ คือ รวมกันไปทุก Policy ในท่อนี้เพียงท่อเดียว สำหรับ Per IP นั้นจะเป็น Object Traffic Shaper ที่ใช้งานลักษณะต่อ IP จะใช้ Traffic Maximum ได้เท่านั้นถ้ามีการนำ Object Traffic Shaper “Per IP” นั้นๆ ไปใช้งานใน Firewall Policy







หัวข้อที่ควรทราบ Firewall Objects (VIP)

สำหรับการสร้าง Object ที่เป็น VIP นั้นจะมีอยู่ด้วยกัน 2 แบบ คือ “Static NAT 1:1” คือจาก Real IP ภายนอกมาเป็น Private IP ภายในโดยตรง “Static NAT 1:1” และ สำหรับอีกแบบจะเป็นลักษณะการ Forward Port เข้ามาที่ Private IP ภายใน IP ต่างๆ เฉพาะ Port ใด Port หนึ่ง หรืออาจจะทำการ Forward Port เป็นช่วงเข้ามาหา Private IP ภายในก็ได้กรณี Apps หรือ Server นั้นๆ ต้องการ

หมายเหตุ

Real IP ที่ได้ Assign มาสำหรับตัวอย่างนี้

	Subnet ID	Host Addresses	Subnet Broadcast
9157	61.1.30.40	61.1.30.41 - 61.1.30.46	61.1.30.47

เบื้องต้นเกี่ยวกับ Security Profile (UTM Profile)

การทำการตรวจสอบของ Security Profile ของ FortiGate มี 2 แบบ Flow Based ,Proxy Based โดย Flow Based ตรวจสอบเป็น Packets ส่วน Proxy Based จะตรวจสอบแบบ Complete Content

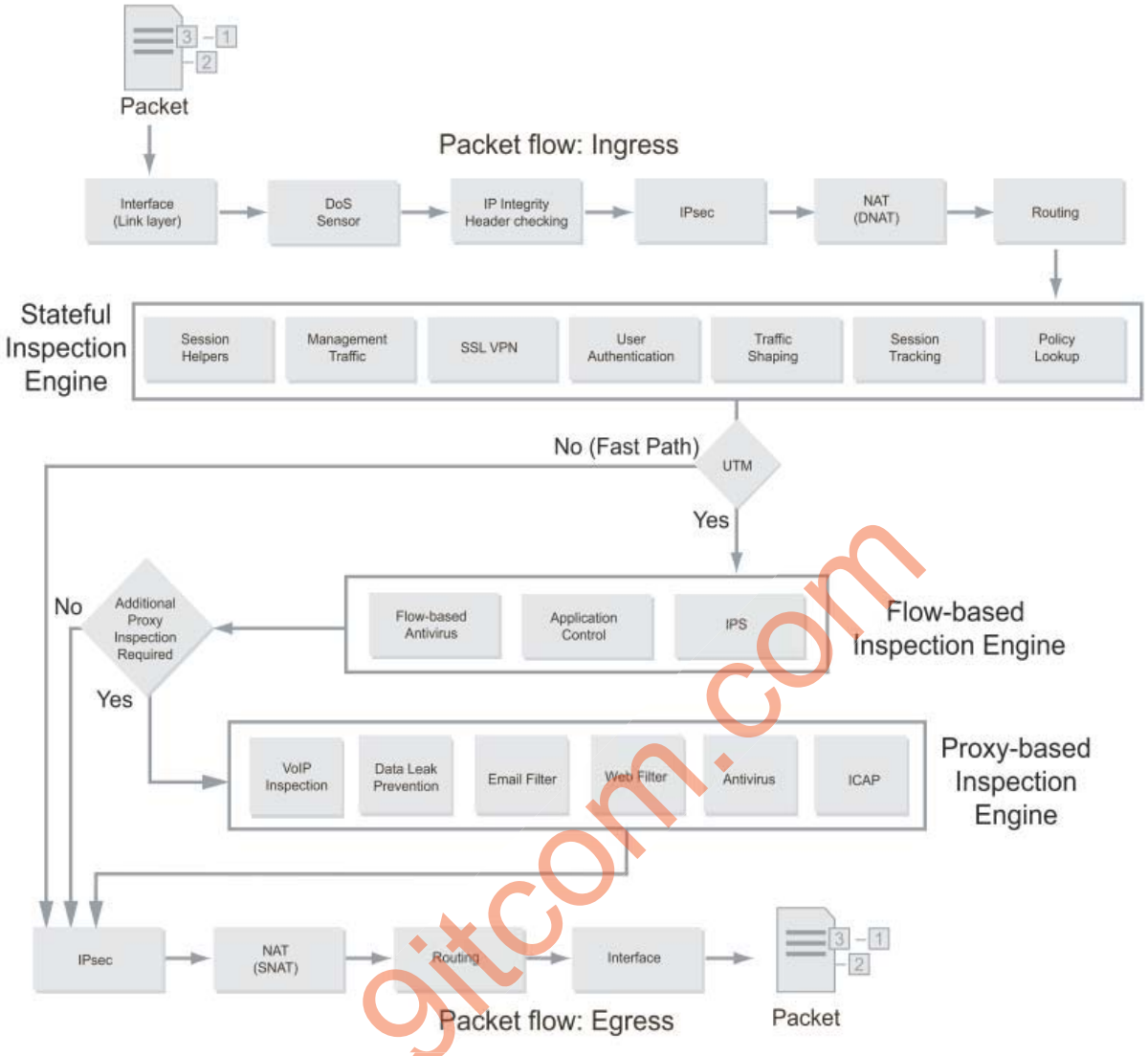
Feature	Stateful	Flow	Proxy
Inspection unit per session	first packet	selected packets	complete content
Memory, CPU required	low	medium	high
Level of threat protection	good	better	best

ชนิดของ Security Profile กับลักษณะการตรวจสอบ

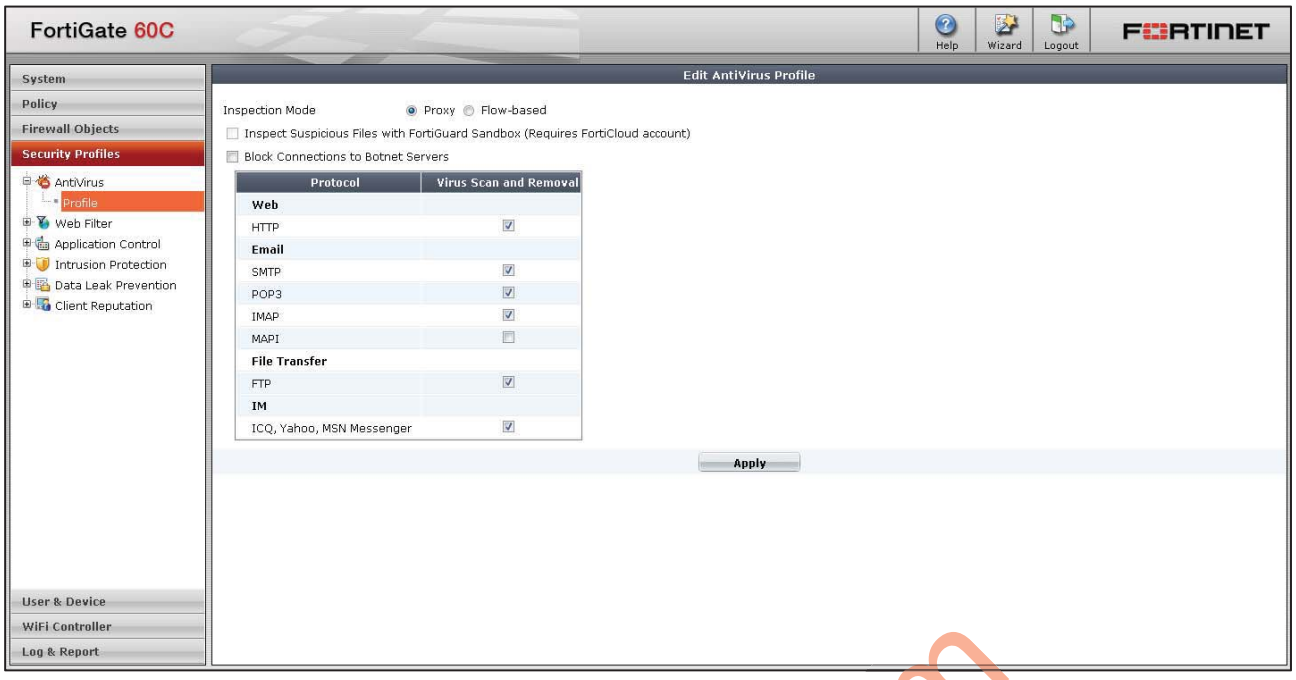
FortiOS security functions and security layers

Security Function	Stateful	Flow	Proxy
Firewall	ü		
IPsec VPN	ü		
Traffic Shaping	ü		
User Authentication	ü		
Management Traffic	ü		
SSL VPN	ü		
Intrusion Prevention		ü	
Flow-based Antivirus		ü	
Application Control		ü	
VoIP inspection			ü
Proxy Antivirus			ü
Email Filtering			ü
Web Filtering (Antispam)			ü
Data Leak Prevention			ü

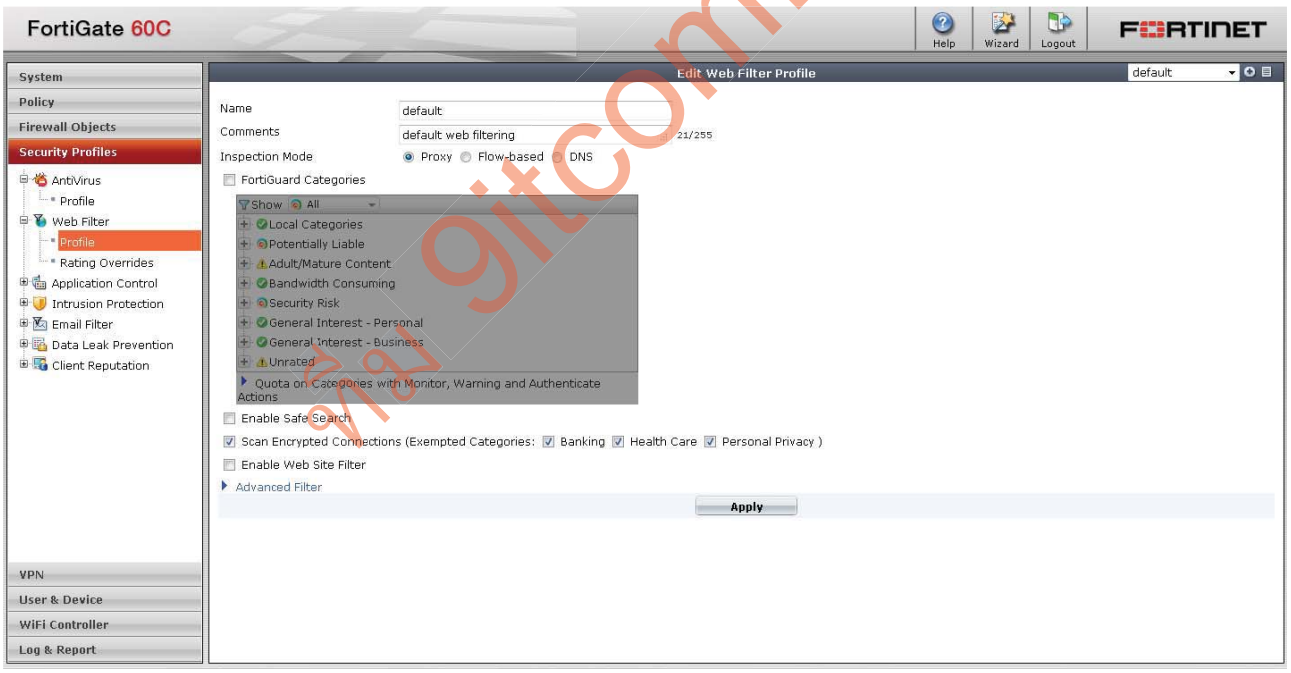
Packet flow



โครงสร้างการทำงาน Packets Flow ภายใน FortiGate

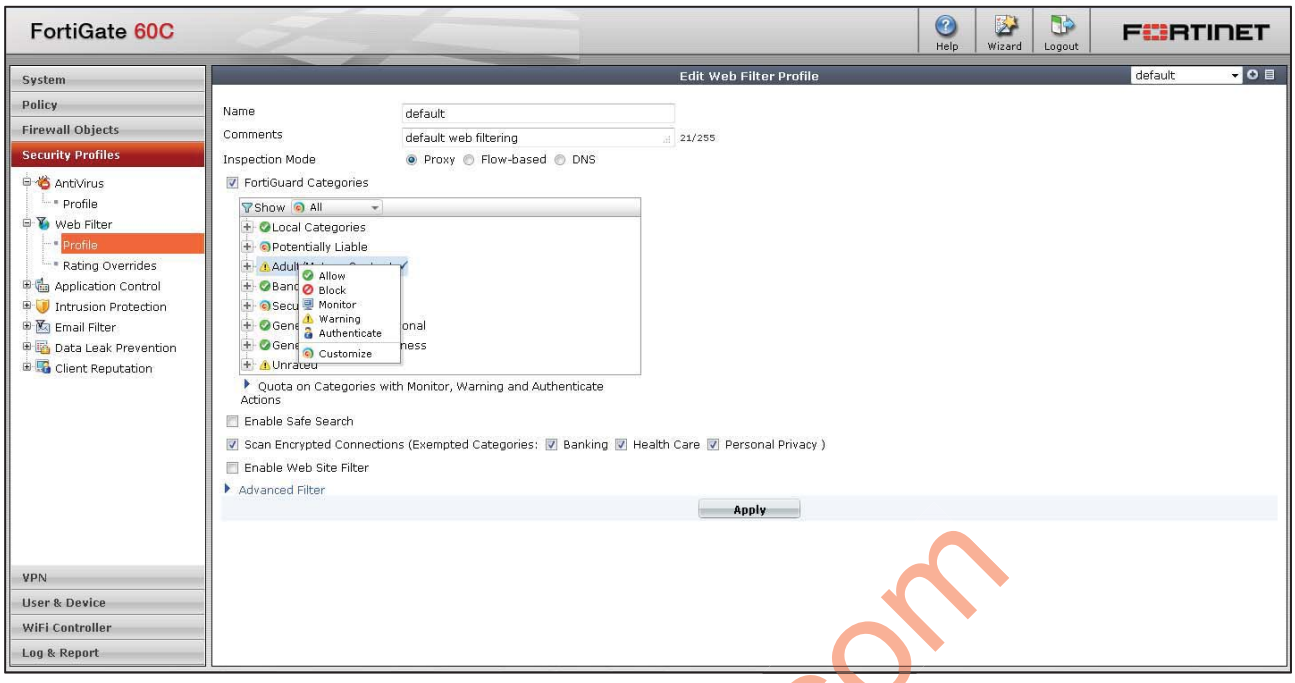


สำหรับ AntiVirus Security Profile นั้นจะรองรับการ Scan ทั้ง 2 แบบ คือ Flow Base และ Proxy Base และจะสามารถเลือกได้ว่าจะให้ Scan ที่ Protocol ไหนบ้าง สามารถเลือกตามการใช้งานที่เหมาะสมได้



สำหรับ WebFilter นั้นจะสามารถใช้งานส่วนของ FortiGuard Categories เลยก็ได้ อาจจะเพิ่ม URL บางตัวเข้าใน WebSite Filter หรือ อาจจะใช้งานเฉพาะ WebSite Filter ก็สามารถทำได้

ตัวอย่างการใช้ FortiGuard ทำการ Block WebSite ไม่เหมาะสมทั้ง Categories



ทดสอบเปิด WebSite ที่เกี่ยวกับ Alcohol โดยใช้ Action = Block (http://www.johnniewalker.com)