ZyXEL

Next-Gen Unified Security Gateway

ZyXEL

www.zyxel.co.th

คู่มือการตั้งค่า USG Series

Performance Series

- USG40-UTM
- USG60-UTM
- USG60W-UTM

Advanced Series

- USG110-UTM
- USG310-UTM

Default Setting	
IP Address:	192.168.1.1
User:	admin
Password:	1234

CALL CENTER 24Hr
0 2832 0600

ZyXEL (Thailand) Co.,Ltd.

สำนักงานใหญ่ : 1/1 หมู่ 2 ถนนราชพฤกษ์ ตำบลบางรักน้อย อำเภอเมือง จังหวัดนนทบุรี 11000 โทร 0 2831 5315 แฟกซ์ 0 2831 5395

ศูนย์บริการสาขาถนนรัตนาธิเบศร์ : 25/46 หมู่ 8 ถนนรัตนาธิเบศร์ อำเภอเมือง จังหวัดนนทบุรี 11000

17-65-100-009084T

Next-Gen Unified Security Gateway
Performance Series

● USG40-UTM ● USG60-UTM ● USG60W-UTM

Next-Gen Unified Security Gateway
Advanced Series

● USG110-UTM ● USG310-UTM

Default Setting	
IP Address:	192.168.1.1
User:	admin
Password:	1234

Default Physical Port

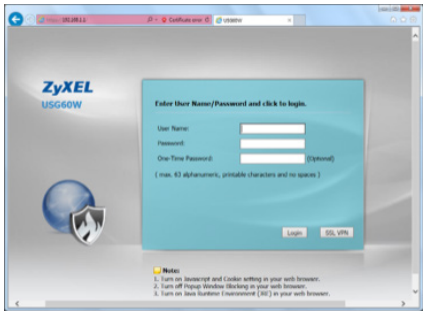
PORT / INTERFACE	P1	P2	P3	P4	P5	P6	P7	P8
• USG40	wan1	lan1	lan1	lan1	opt			
• USG40W	wan1	lan1	lan1	lan1	opt			
• USG60	wan1	wan2	lan1	lan1	lan1	lan1		
• USG60W	wan1	wan2	lan1	lan1	lan1	lan1		
• ZyWALL 110 • USG110 • USG210	wan1	wan2	opt	lan1	lan1	lan1	dmz	
• ZyWALL 310 • ZyWALL 1100 • USG310 • USG1100 • USG1900	ge1	ge2	ge3	ge4	ge5	ge6	ge7	ge8

Default Physical Port

ZONE / INTERFACE	WAN	LAN1	LAN2	DMZ	OPT	NO DEFAULT ZONE
• USG40	WAN1 WAN1_PPP	LAN1	LAN2	DMZ	OPT OPT_PPP	
• USG40W	WAN1 WAN1_PPP	LAN1	LAN2	DMZ	OPT OPT_PPP	
• USG60	WAN1 WAN1_PPP WAN2 WAN2_PPP	LAN1	LAN2	DMZ		
• USG60W	WAN1 WAN1_PPP WAN2 WAN2_PPP	LAN1	LAN2	DMZ		
• ZyWALL 110 • USG110 • USG210	WAN1 WAN1_PPP WAN2 WAN2_PPP	LAN1	LAN2	DMZ	OPT OPT_PPP	
• ZyWALL 310 • ZyWALL 1100 • USG310 • USG1100 • USG1900	GE1 GE1_PPP GE2 GE2_PPP	GE3	GE4	GE5		GE3_PPP GE4_PPP GE5_PPP GE6 GE6_PPP GE7 GE7_PPP GE8 GE8_PPP

การ Login เพื่อตั้งค่า USG Series

1. เชื่อมต่อพอร์ต LAN หรือ LAN1 ของอุปกรณ์ แล้วเปิดหน้า Web Browser แล้วเข้าไปที่ https://192.168.1.1 จะปรากฏหน้า Login



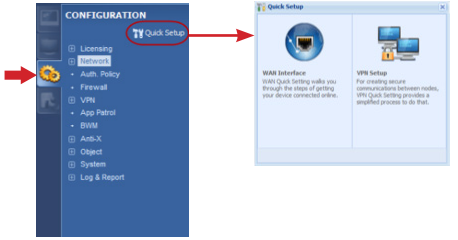
2. ใส่ Username และ Password เป็น admin และ 1234 ตามลำดับ (ค่า Default) จากนั้นกด Login จะปรากฏหน้า Installation Setup Wizard โดยให้เลือก Go to Dashboard เพื่อเข้าสู่หน้าการตั้งค่าของอุปกรณ์

โดยหน้าหลักของอุปกรณ์จะแสดงแถบเมนูด้วยกัน 3 ส่วน คือ

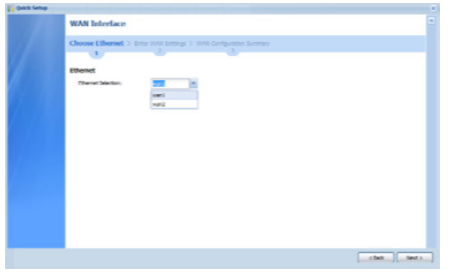
1. **แถบเมนูหลัก** ประกอบไปด้วยเมนู Dashboard, Monitor, Configuration และ Maintenance
2. **หน้าต่างหลัก** จะแสดงสถานะ การทำงานของอุปกรณ์รวมถึงภาพจำลองสถานะการเชื่อมต่อของอุปกรณ์
3. **แถบเครื่องมือ** ประกอบไปด้วย ปุ่ม Logout, Console หรือ Help เพื่อแสดงรายละเอียดของเมนูต่างๆ

การ Login เพื่อตั้งค่า USG Series

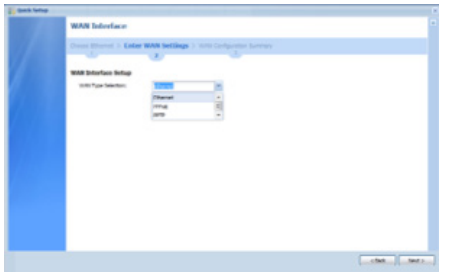
ไปยังแถบเมนู Configuration เลือก Quick Setup จะปรากฏการตั้งค่า 2 รูปแบบ คือ WAN Interface และ VPN Setup ให้เลือก WAN Interface



เลือก Interface wan1 หรือ wan2 เพื่อเชื่อมต่ออินเตอร์เน็ต โดยหากเชื่อมต่อ Modem/Router ที่พอร์ต P1 คือ wan1 หรือ พอร์ต P2 คือ wan2



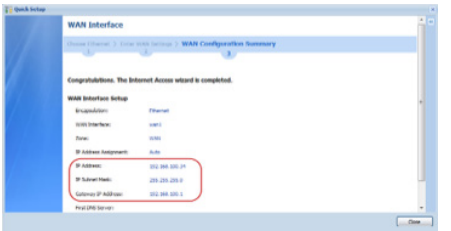
การตั้งค่าการเชื่อมต่ออินเตอร์เน็ต สามารถเชื่อมต่อได้ 3 รูปแบบ คือ Ethernet, PPPoE และ PPTP



1. เชื่อมต่อแบบ Ethernet

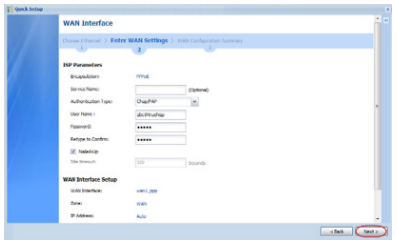
หลังจากเลือกการเชื่อมต่อแบบ Ethernet แล้วสามารถตั้งค่าให้รับ IP Address อัตโนมัติ (Auto) หรือ ทำการกำหนดค่า IP Address (Static) ได้

หากสามารถเชื่อมต่อได้สำเร็จจะได้รับ IP ดังรูป

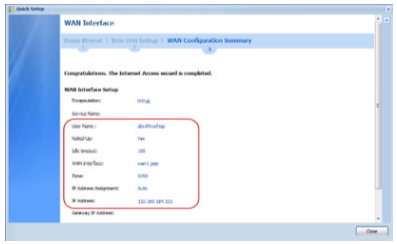


2.เชื่อมต่อแบบ PPPoE

หลังจากเลือกการเชื่อมต่อแบบ PPPoE จะปรากฏหน้าการตั้งค่าการเชื่อมต่ออินเตอร์เน็ตโดยทำการกรอก username และ password ที่ได้รับจากผู้ให้บริการ

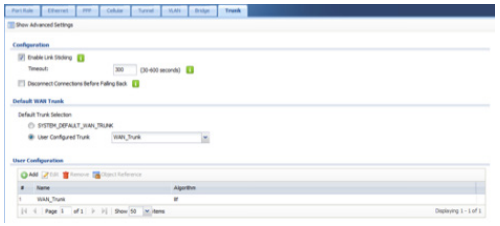


หากทำการเชื่อมต่อได้สำเร็จจะได้รับ IP Address จากผู้ให้บริการ ดังรูป



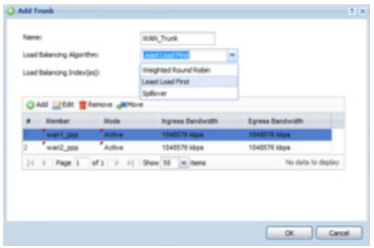
การตั้งค่า Trunk หรือ Load Balancing

ไปที่เมนู Network >> Interface >> Trunk เพื่อทำการกำหนด Interface ต่างๆ ให้เป็นสมาชิกของ WAN_TRUNK โดยการเลือก Edit หรือทำการ Add เข้าไปใหม่



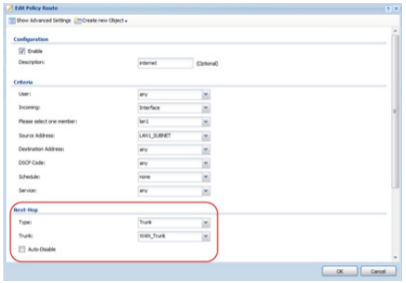
เมื่อทำการ Edit หรือ Add มาแล้วจะสามารถกำหนด Algorithm ได้ว่าต้องการให้เป็น Load Balance รูปแบบใด สามารถเลือกได้ 3 แบบ คือ Weighted Round Robin, Least Load First หรือ Spillover และสามารถกำหนดได้ว่าต้องการให้ Interface ใดบ้างอยู่บน WAN_TRUNK นี้บ้าง

แต่ละ Interface เลือกโหมดได้เป็น Active และ Passive โหมด Active คือ Interface นั้นจะทำงานอยู่ ส่วน Passive นั้นคือ Interface นั้นจะทำงานเป็น Back-up Interface



การตั้งค่า Policy Route

การกำหนด Policy Route เพื่อสร้างเส้นทางของ Packet ที่จะเชื่อมต่ออินเตอร์เน็ต ไปที่เมนู Network >> Routing >> Policy Route



จากรูปตัวอย่างกำหนดว่าเมื่อมี Packet จากพอร์ต Interface lan 1 ที่มี IP เป็น LAN_SUBNET จะไปที่ใดๆ ก็ตาม (Destination Address – any) ให้ไปออกที่พอร์ต WAN_TRUNK เป็นต้น

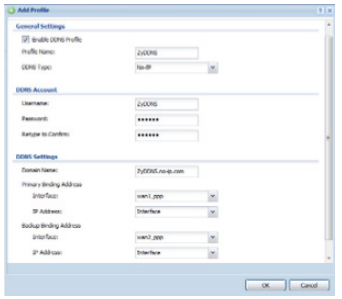
การตั้งค่า Port Role

เป็นการกำหนดการหน้าที่การทำงานของพอร์ตต่างๆ ซึ่งจากรูป P3, P4 จะหน้าที่เป็น LAN1 โดย P5 และ P6 จะทำหน้าที่เป็น LAN2 และ DMZ ตามลำดับ

**USG310, USG1100 และ USG1900 ไม่รองรับ Port Role*

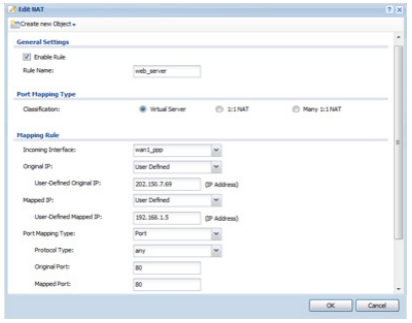
การตั้งค่า Dynamic DNS

ไปที่เมนู Network >> DDNS เพื่อทำการสร้าง Profile โดยการ Add ขึ้นมา โดยใส่ Account ของ Dynamic DNS ลงไป จากนั้นจึงใส่ชื่อ Domain เลือก Interface ที่ต้องการเอาชื่อ Domain ไปผูกไว้



การตั้งค่า NAT

ไปที่เมนู Network >> NAT เพื่อตั้งค่าการ Forward Port หรือ Map IP ต่างๆ โดยกด Add ขึ้นมาเพื่อทำการกำหนด Policy

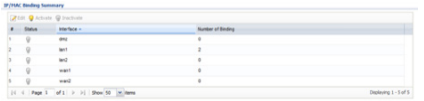


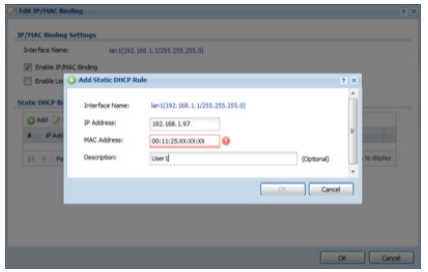
1. Port Forwarding Incoming Interface เป็น Interface ที่ Packet เข้ามา และกำหนด Original IP เป็น any จากนั้นจึงกำหนด IP ของเครื่องภายในในหัวข้อ Mapped IP รวมถึงกำหนด Port ที่ต้องการ Forward เข้ามาด้วย

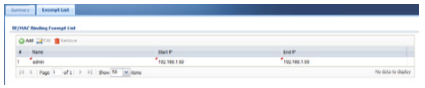
2. Mapped IP จะคล้ายกับแบบแรกแต่เพิ่มส่วนของการกำหนด Original IP เข้าไปว่าจะทำการผูก Public IP เข้ากับ Private IP ใด

การตั้งค่า IP/MAC Binding

ไปที่เมนู Network >> IP/MAC Binding เพื่อทำการผูก MAC Address ของเครื่อง Client เข้ากับ IP Address ถ้า MAC Address กับ IP Address ไม่ตรงกันก็จะไม่สามารถใช้งานได้ แต่จะสามารถทำการยกเว้นได้ในช่วง IP Address ที่เราทำการกำหนดลงไปว่าไม่ต้องทำการผูกกับ MAC Address ในหัวข้อ Exempt List

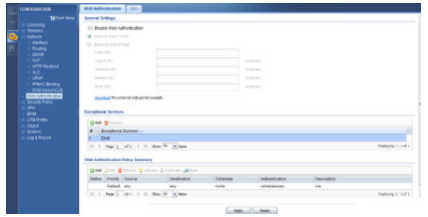




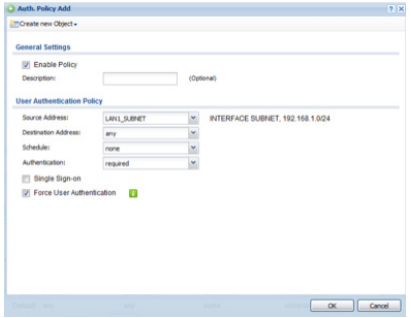


การตั้งค่า Web Authentication

ไปที่เมนู Network >> Web Authentication เพื่อตั้งนโยบายของการระบุตัวตนของผู้ใช้งาน โดยจะใช้การอ้างอิงจาก Auth. Method ที่สร้างขึ้น

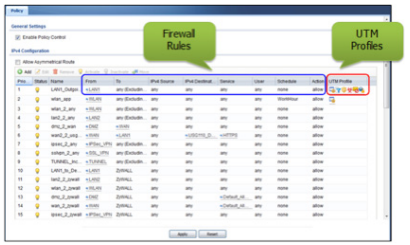


กด Add เพื่อเพิ่ม Policy การตั้งค่าระบุตัวตน โดยกำหนดจาก Source Address



การตั้งค่า Policy Control

ไปที่เมนู Security Policy >> Policy Control ใน Next Generation USG จะมีการรวมฟังก์ชั่น Firewall Rule และ การตั้งค่าจัดการ UTM เข้าด้วยกันโดยรูปแบบการตั้งค่า Policy control จะแบ่งเป็น 2 ส่วน ดังนี้

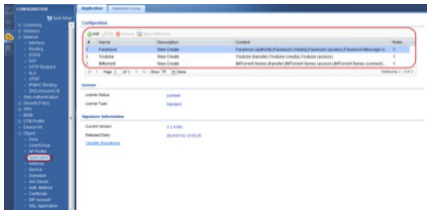


Policy Control จะเป็นการกำหนดสิทธิ์การเข้าถึงโซนต่างๆ ของแต่ละโซน หรือแต่ละเครื่อง โดยลำดับของPolicy ที่สร้างขึ้นมานั้นจะทำงานจากข้อแรกไปเรื่อยๆ จนถึงข้อสุดท้าย

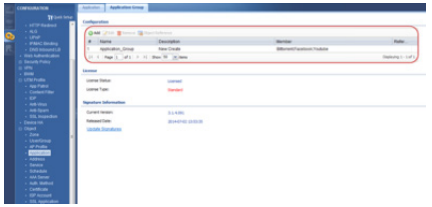
การตั้งค่า UTM Profiles

App Patrol Profile เป็นรูปแบบ Profile ที่ใช้สำหรับจัดการการทำงาน Application ต่างๆ โดยมีวิธีการสร้างดังนี้

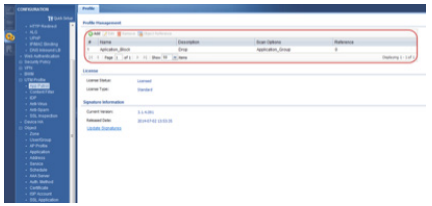
1. App Patrol Profile เป็นรูปแบบ Profile ที่ใช้สำหรับจัดการการทำงาน Application ต่างๆ โดยมีวิธีการสร้างดังนี้



2. สามารถนำ Application ที่เราสร้างขึ้นรวบรวมเป็น Application Group ได้ดังรูป

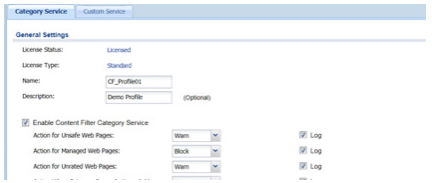


3. สร้าง App Patrol Profile เพื่อกำหนดการ drop สำหรับ Application Group ที่ได้ทำการสร้างขึ้นมา

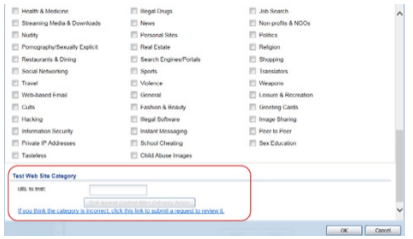


Content Filter Profile

ไปที่เมนู UTM Profile >> Content Filter รูปแบบ Profile ที่กำหนดให้ User สามารถใช้งานหรือไม่สามารถใช้งาน Website บาง Website ได้ จะแบ่งออกเป็นสองส่วน คือ Category Service สามารถเลือกเป็นหัวข้อได้เลยว่าต้องการ Block Website ที่มีเนื้อหาในเรื่องใดๆ บ้าง อีกส่วนคือ Custom Service โดยต้องกำหนดเองว่าจะ Block Website ใดหรือจะให้ Website ใดใช้งานได้

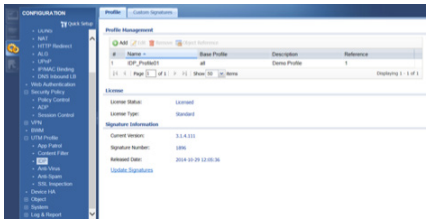


สำหรับรูปแบบของ Category Service สามารถตรวจสอบหมวดหมู่ได้ว่าอยู่ในกลุ่มไหน ที่หัวข้อ Test Web Site Category



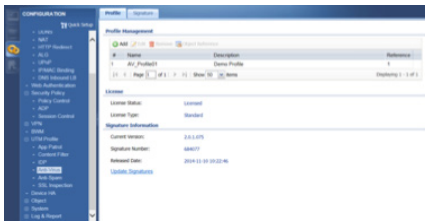
IDP Profile

ไปที่เมนู UTM Profile >> IDP เพื่อเปิดการใช้งาน IDP โดยจำการตรวจสอบตาม Policy ที่ได้ตั้งไว้คล้ายๆ กับ Anti-Virus โดยจะดูจาก Policy ของ Signature ที่ได้ตั้งไว้ว่าจะ Drop หรือ Allow Signature ใดบ้าง



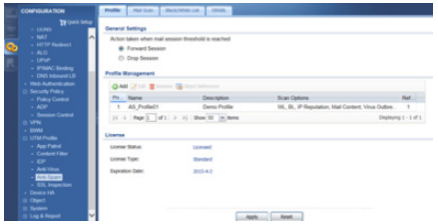
Anti-Virus Profile

ไปที่เมนู UTM Profile >> Anti-Virus เพื่อกำหนดการตั้งค่า Anti-Virus Profile โดยอ้างอิงจาก signature ในการตรวจสอบ

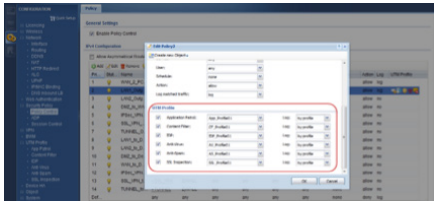


Anti-Spam Profile

ไปที่เมนู UTM Profile >> Anti-Spam เพื่อทำการตั้งค่าการตรวจสอบ e-mail ต่างๆ โดยตรวจสอบได้ 2 โปรโตคอล คือ SMTP, POP3 สามารถตรวจสอบได้ทั้งจาก Black List & White List รวมถึง DNS Black List (DNSBL) ใน Black List & White List นั้นต้องทำการกำหนดเอง โดยกำหนดได้เป็น Subject, IP Address, E-mail Address, Mail Header ส่วน DNSBL จะเป็นการตรวจสอบจาก Server ภายนอก

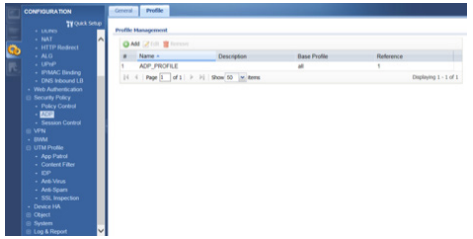


ซึ่งหลังจากได้ทำการสร้าง UTM Profile เสร็จเรียบร้อยแล้ว สามารถนำ Profile ต่างๆ นั้นมาจัดการใน Policy Control ได้ ที่เมนู Security Policy >> Policy Control



การตั้งค่า ADP

ไปที่เมนู Security Policy >> ADP เพื่อใช้งาน ADP ซึ่งจะคล้ายกับการทำงานของ IDP เพียงแต่ว่าจะสามารถใช้ได้ฟรีอยู่แล้ว จะเป็น Signature เก่าที่มีมานานแล้ว พวก Port Scan, Flood ต่างๆ จะไม่สามารถอัพเดต Signature ได้ซึ่งต่างกับ IDP ที่จะเป็น Signature ใหม่ๆ



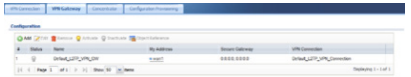
การตั้งค่า VPN

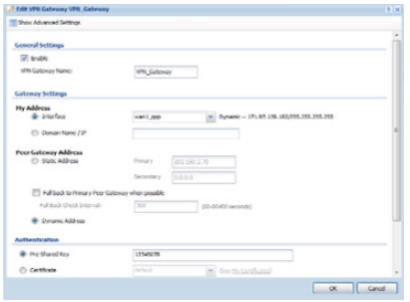
1. แบบ IPSec

1.1 การตั้งค่า IPSec VPN

ไปที่เมนู VPN >> IPSec VPN เพื่อทำการกำหนด Policy ของ VPN การตั้งค่าต่างๆ นั้นทำตามขั้นตอนดังนี้

- ไปที่เมนู VPN >> IPSec VPN >> VPN Gateway เพื่อทำการกำหนด Policy การ connect ของขา WAN กำหนด WAN ฝั่งเรา กำหนด WAN อีกฝั่งหนึ่ง หรือ จะกำหนดเป็น Dynamic Address เพื่อทำเป็นรูปแบบ Remote Access (Server Role)กำหนด Pre-Shared Key และ Phase1 Algorithm ให้เหมือนกันทั้งสองฝั่ง

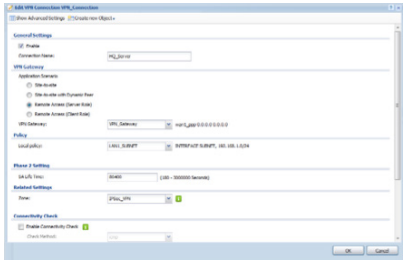




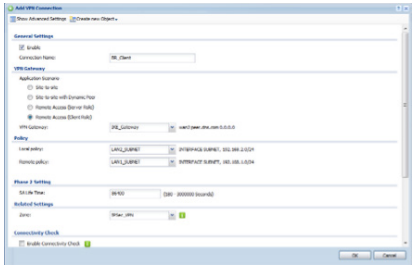
- ไปที่เมนู VPN >> IPSec VPN >> VPN Connection เพื่อทำการกำหนด Policy การ connect ของ LAN ทั้งสองฝั่ง โดยเลือก VPN Gateway ที่เราสร้างขึ้นมาเมื่อซักครู่นี้ รวมถึงกำหนด Algorithm ของ Phase 2 ให้ตรงกันทั้งสองฝั่ง

ตัวอย่างการตั้งค่าระหว่าง HQ และ BR โดยใช้รูปแบบ Remote Access (Server Role) และ Rmote Access (Client Role)

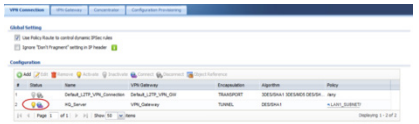
- Remote Access (Server Role)



- Remote Access (Client Role)



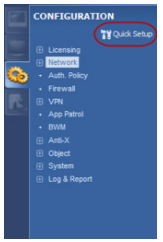
- ซึ่งหาก VPN Tunnel เชื่อมต่อได้สำเร็จจะปรากฏสัญลักษณ์การเชื่อมต่อดังรูป



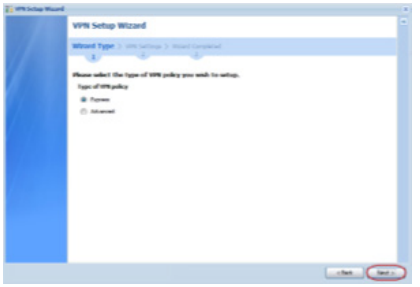
1.2 การตั้งค่า IPSec VPN Auto Configuration Provisioning

IPSec VPN Auto Configuration Provisioning เป็นการรับการตั้งค่า VPN จาก VPN Server มายัง Client โดยจะใช้งานควบคู่กับ Software IPSec VPN Client ซึ่งขั้นตอนดังนี้

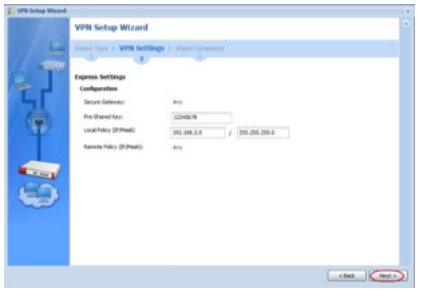
- ไปที่เมนู Quick Setup จะปรากฏการตั้งค่า 2 รูปแบบ คือ WAN Interface และ VPN Setup



- เลือก VPN Setup จะปรากฏ VPN Setup Wizard เลือก VPN Settings for Configuration Provisioning



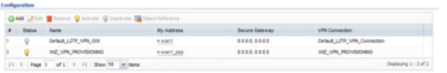
- ทำการระบุรหัสผ่าน (Pre-Shared Key) และ IP Address ฝั่งภายใน (Local Policy) กด “Next “



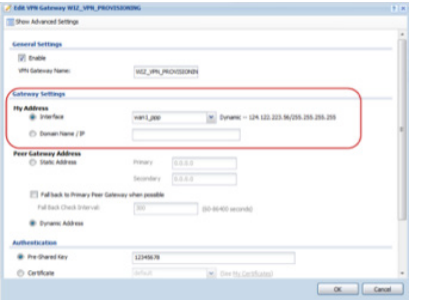
- สรุปข้อมูลการตั้งค่าทั้งหมด ทำการกด “Save” เพื่อบันทึกค่า

- จบขั้นตอนการตั้งค่า กด “Close” เพื่อปิดการตั้งค่า

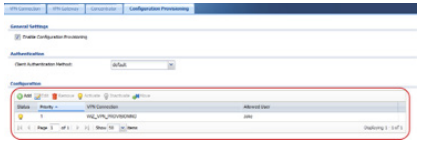
- ไปยังเมนู VPN >> IPSec VPN จะเห็นได้ว่าในส่วนของ VPN Gateway จะมีการสร้าง Object ชื่อ “WIZ_VPN_PROVISIONING”



- ทำการตรวจสอบการตั้งค่าว่าตรงตามข้อมูลที่ตั้งค่าไว้หรือไม่ เช่น ในส่วน VPN Gateway >> Gateway Settings >> My Address ต้องทำการเลือก Interface ให้ถูกต้อง

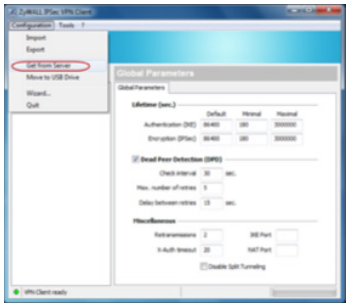


- ไปที่เมนู Configuration Provisioning เพื่อกำหนดนโยบายการอนุญาตของการขอรับการใช้งาน เช่น อนุญาตให้ชื่อผู้ใช้ “Joke” รับการตั้งค่า VPN ได้



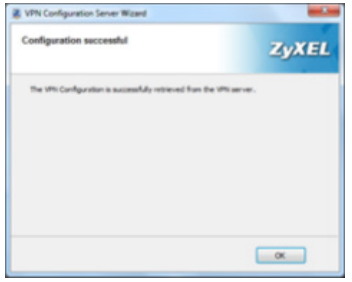
- ไปเปิดโปรแกรม IPSec VPN Client ไปที่เมนู Configuration >> Get from Server

- เปิดโปรแกรม IPSec VPN Client ไปที่เมนู Configuration >> Get from Server

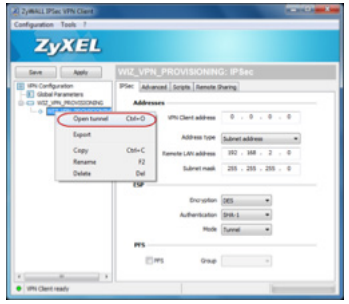


- ใส่ Gateway ของ VPN Server ระบุชื่อผู้ใช้และรหัสผ่าน

- เสร็จสิ้นกระบวนการรับการตั้งค่าจาก VPN Server

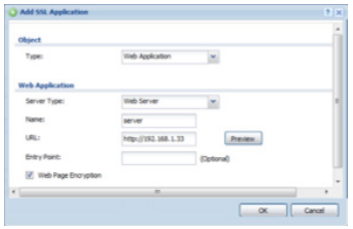


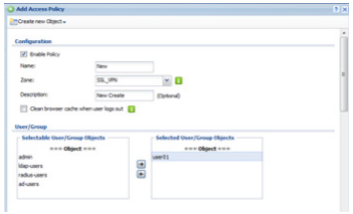
- ทำการเชื่อมต่อ VPN โดยทำการ Open tunnel

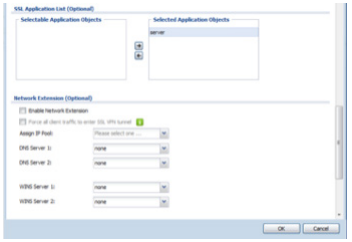


2. แบบ SSL

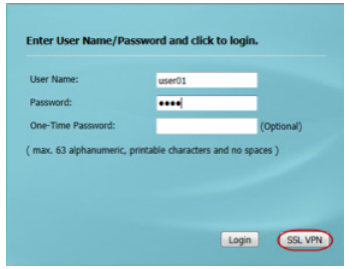
ไปที่เมนู VPN >> SSL VPN >> Access Privilege เพื่อทำการกำหนด Application ที่จะทำ SSL โดยการตั้งชื่อกำหนดสิทธิ์ของ User และกำหนด Application ที่เราต้องการ

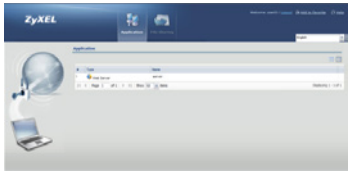






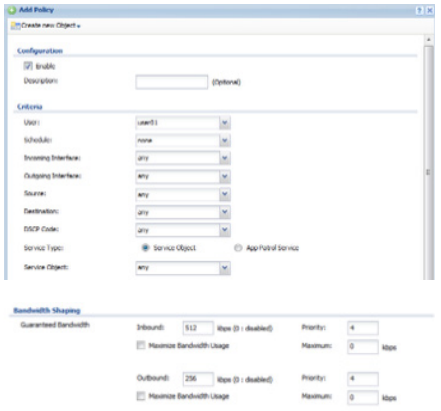
- เมื่อทำการใช้งานก็ใส่ Username และ Password ของ User ที่จะใช้งานลงไปพร้อมทั้งเลือกด้วยว่าจะ Login เป็น SSL แล้วก็กด Login ก็จะสามารถใช้งาน SSL ได้





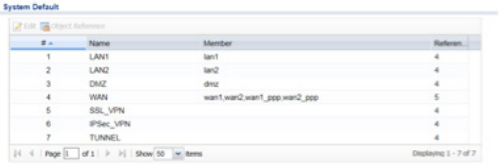
การตั้งค่า BWM

เป็นการจัดสรรแบนด์วิดธ์การใช้งานของผู้ใช้แต่ละคน โดยสามารถระบุการบริการได้จาก Service object ที่สร้างขึ้นเอง หรือ App Patrol Service ที่มีอยู่แล้ว



การกำหนด Zone

ไปที่เมนู Object >> Zone เป็นการกำหนดโซนที่อยู่ให้กับ Interface ต่างๆ ซึ่งจะมีผลในการตั้งค่าใน Policy Control

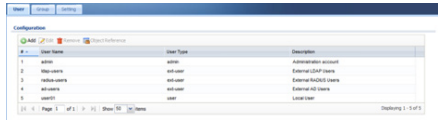


การตั้งค่า User/Group

ไปที่เมนู Object >> User/Group เพื่อทำการ Add User หรือทำการรวมกลุ่ม User รวมถึงการกำหนด Policy การ Logon ของ User และการ Force Authentication

1. User

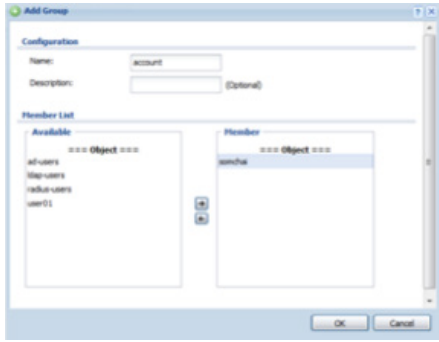
ที่เมนู User สามารถกด Add เพื่อทำการ Add User ได้เลย User จะมี 5 แบบ คือ admin, limited-admin, User, guest, และ ext-User โดย admin จะมีสิทธิ์ในการตั้งค่าทั้งหมด limited-admin มีสิทธิ์แค่เข้ามาดูค่า configuration ต่างๆ แต่ไม่มีสิทธิ์แก้ไข ส่วนที่เหลือจะเป็น User สำหรับ Logon เพื่อกำหนดสิทธิ์ใช้งานต่างๆ



เมื่อทำการ Add ขึ้นมาแล้วก็แค่กำหนด Username Password แล้วก็เลือกประเภทของ User ที่ต้องการ ส่วนที่เป็น Re-Authentication time จะหมายความว่าถ้าหมดเวลาที่กำหนดแล้ว User จะต้องทำการ Logon ใหม่อีกครั้ง ส่วนที่เป็น Lease Time จะคล้ายกัน ต่างกันที่ว่าจะสามารถต่อเวลาออกไปได้โดยไม่ต้องทำการ Logon ใหม่

2. Group

จะเป็นการจับ User ที่มีอยู่ให้มาอยู่เป็นกลุ่มเดียวกันเพื่อจะให้ง่ายในการกำหนด Policy ต่างๆของ User ที่ต้องการให้มีลักษณะการใช้งานเหมือนๆ กัน จากรูปกรอบทางซ้ายคือ User ที่สามารถที่จะกำหนดเข้าไปอยู่ใน Group ได้ กรอบทางด้านขวาคือ User ที่เป็นสมาชิกของ Group นี้อยู่



3. Setting

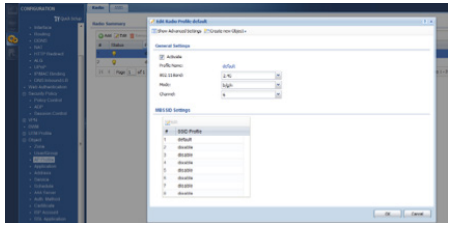
เมนูนี้จะเป็นการตั้งค่าการ Logon ของ User ต่างๆ ดังนี้

- Miscellaneous setting เป็นการเพิ่ม Lease Time อัตโนมัติ กับตั้งว่าถ้า User ไม่มีการใช้งานนานกี่นาทีจะทำการ Logout ออกอัตโนมัติ
- User Logon Setting กำหนดจำนวน User ที่ Logon เข้ามาได้พร้อมๆกัน หัวข้อแรกเป็นการกำหนด User Admin อีกหัวข้อเป็นการกำหนด User อื่นๆ
- User Lockout Setting กำหนดจำนวนครั้งที่ User จะพยายาม Logon ถ้า Logon ผิดตามจำนวนที่กำหนด จะโดยล็อคไม่ให้ทำการ Logon เป็นจำนวนเวลาที่กำหนด

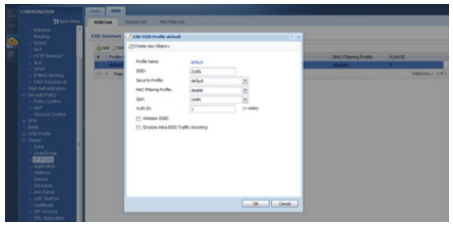
การตั้งค่า AP Profile

ในส่วนของ AP Profile จะประกอบไปด้วยสองส่วนหลักๆ คือ

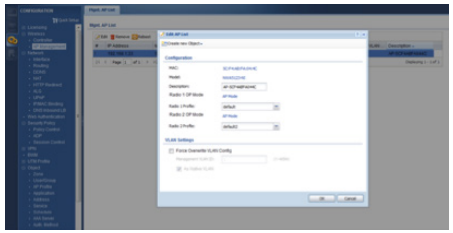
Radio Profile เป็น Profile ที่เอาไว้ตั้งค่าต่าง ๆ ของ AP Mode เช่น ย่านความถี่ 2.4GHz หรือ 5GHz และช่องสัญญาณที่เลือกใช้ (Channel ID) รวมทั้ง SSID Profile ที่จะนำมาใช้งานกับ Radio Profile ซึ่ง 1 Radio Profile สามารถกำหนดให้ใช้งาน SSID ได้ถึง 8 SSIDs (Multi SSID) ในเวลาเดียวกัน



SSID Profile เป็น Profile ที่มีไว้สำหรับเก็บค่า SSID ที่ต้องการเพื่อนำไปใช้ใน Radio Profile และยังสามารถกำหนดค่า Security ของ Wireless โดยเรียกใช้งานจาก Security Profile และ MAC filter Profile รวมทั้งสามารถระบุ VLAN ID และ QoS ให้กับ SSID นั้น ๆ ได้ด้วย



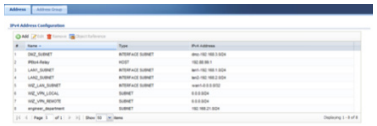
ซึ่งหลังจากได้ทำการสร้าง Radio Profile เสร็จเรียบร้อยแล้ว สามารถนำ Radio Profile นั้นมาใช้งานกับ AP ที่ต้องการ ที่เมนู Wireless >> AP Management

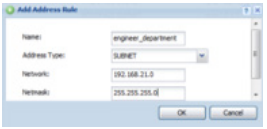


ภาพโครงสร้างการตั้งค่าเพื่อเปิดใช้งาน Wireless โดยใช้ AP Profile ในการจัดการ

การตั้งค่า Address

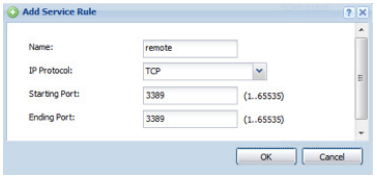
ไปที่เมนู Object >> Address ทำการกำหนด IP Address ต่างๆ เป็นชื่อที่ต้องการ เพื่อนำไปใช้ตั้งค่า Policy ในหัวข้ออื่นต่อไป สามารถรวมหลายๆ Address Object เข้าด้วยกันเป็นกลุ่มเพื่อกำหนด Policy ได้เช่นกัน แต่ละ Object ที่สร้างขึ้นมานั้นกำหนด IP ได้หลายแบบ เช่น Host, Range, Subnet, Interface IP, Interface subnet, และ Interface gateway





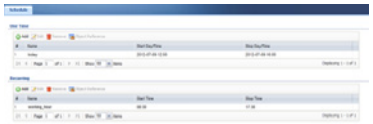
การตั้งค่า Service

ไปที่เมนู Object >> Service เป็นการกำหนด Port ของ Service เป็นชื่อต่างๆ โดยจะมีเป็น Default Port กำหนดมาบางส่วนอยู่แล้วซึ่งเป็น Port มาตรฐาน ถ้ามี Application อื่นที่ใช้งานก็สามารถ Add เพิ่มเข้าไปได้ รวมถึงสามารถรวมหลาย Service เป็นกลุ่มได้เช่นเดียวกัน



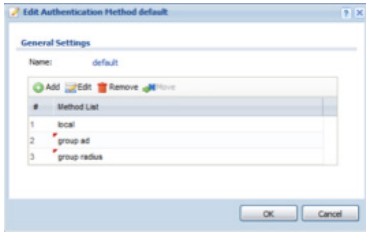
การตั้งค่า Schedule

ไปที่เมนู Object >> Schedule ทำการกำหนดตารางเวลาเพื่อที่จะนำไปใช้กับ Policy ต่างๆ สามารถกำหนดได้เป็นใช้งานเพียงครั้งเดียว (One Time) หรือว่าให้มีการทำงานซ้ำๆ (Recurring)



การตั้งค่า Auth. Method

ไปที่เมนู Object >> Auth. Meth เพื่อกำหนดว่าจะให้อุปกรณ์ไปตรวจสอบ Username Password จากที่ใดก่อนไม่ว่าจะเป็น Local, AD, LDAP, Radius

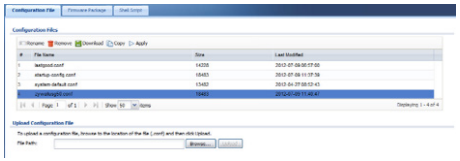


การตั้งค่าเวลา/วันที่

ไปที่เมนู System >> Date/Time สามารถตั้งได้ทั้งแบบตั้งค่าเองหรือว่า Sync กับ Time Server

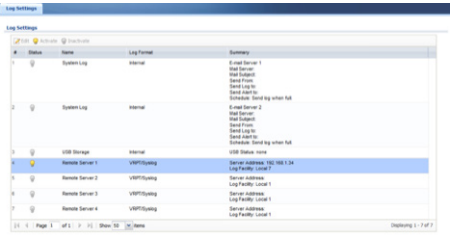
การตั้งค่าไฟล์ config

ไปที่เมนู Maintenance >> File Manager เพื่อทำการบันทึกไฟล์ Configuration ต่างๆ ทุกครั้งที่มีการแก้ไขค่า ค่าที่แก้ไขจะถูกบันทึกลงไฟล์ “startup-config.conf” โดยอัตโนมัติ เราสามารถบันทึกไฟล์นี้เป็นไฟล์ Backup ของเราเองได้โดยการคลิ๊กที่ startup-config ให้เป็นแถบสีฟ้า จากนั้นกด Copy แล้วเปลี่ยนชื่อตามต้องการ กด OK ก็จะปรากฏชื่อไฟล์ที่เรานั้นบันทึกไปขึ้นมาอีกบรรทัด ถ้าต้องการ Download เก็บไว้ในคอมพิวเตอร์ก็คลิ๊กที่ไฟล์ที่ต้องการ จากนั้นกด Download จะ Upload ไฟล์จากในคอมพิวเตอร์ก็ Browse ไปที่ไฟล์ที่เราต้องการ จากนั้นก็กด Upload ไฟล์ก็จะไปปรากฏในตาราง ต้องการให้ไฟล์นั้นทำงาน ก็คลิ๊กที่ไฟล์นั้น แล้วจึงกด Run ไฟล์นั้นก็จะทำงานแทนไฟล์ Config เดิม



การตั้งค่า Log

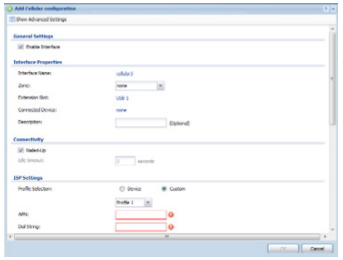
ไปแถบเมนูหลัก Monitor >> Log จะมีหน้าที่แสดง Log สถานะของอุปกรณ์ ส่วนการตั้งค่า Log ให้ไปแถบเมนูหลัก Configuration >> Log settings จะเป็นการตั้งค่าเพื่อให้อุปกรณ์ส่ง Log ออกไปภายนอกได้ทั้ง e-mail และ SysLog Server



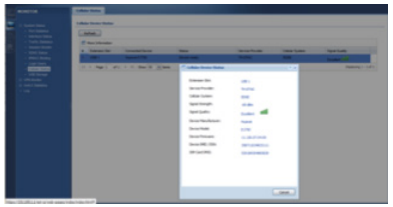
การตั้งค่า e-mail Log ให้กด Modify ที่ข้อ 1 System Log เมื่อเข้าไปแล้วก็ทำการตั้งว่าจะส่งไปที่ e-mail ใด แล้วต้องการให้ส่งหัวข้อใดบ้าง สามารถส่งไปได้ 2 Mail Server ส่วนที่เป็น SysLog Server ให้ Modify ที่หัวข้อ Remote Server เมื่อเข้าไปที่หน้าตั้งค่าแล้ว ก็กำหนด IP ของ Server ที่ต้องการส่ง Log ไปเก็บ แล้วเลือกหัวข้อที่ต้องการ

การตั้งค่าการใช้งาน 3G

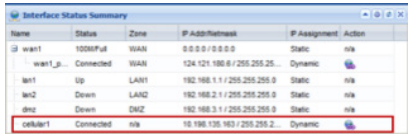
เชื่อมอุปกรณ์ Aircard ผ่านทาง USB Port แล้วไปที่เมนู configuration > Network > interface > Cellular > Add แล้วทำการใส่ค่า APN และ Dial String ของผู้ให้บริการ



เมื่อตั้งค่าเสร็จเรียบร้อยให้ทำการตรวจสอบสถานะของสัญญาณ และ การเชื่อมต่อ ดังภาพ



ตรวจสอบสถานะ การเชื่อมต่อ Monitor > Interface status



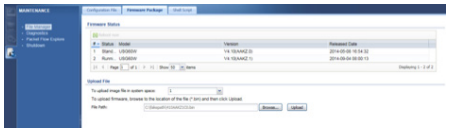
*สามารถตรวจสอบ Aircard ที่รองรับ (3G Card Support) ได้ที่ **www.zyxel.co.th** แล้วเลือกผลิตภัณฑ์ที่ต้องการตรวจสอบ*

APPENDIX

การ Upgrade Firmware

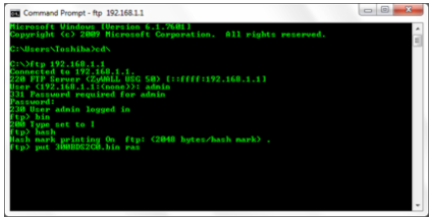
1. ผ่าน Web GUI

ไปที่เมนู Maintenance >> File Manager >> Firmware Package เลือก system space ที่จะทำการ upload เนื่องจากอุปกรณ์รองรับการทำงาน Dual firmware จากนั้นก็ Browse ไฟล์ที่ต้องการ (.bin) แล้วก็กด Upload รอจนอุปกรณ์ Reboot จนเสร็จสิ้น

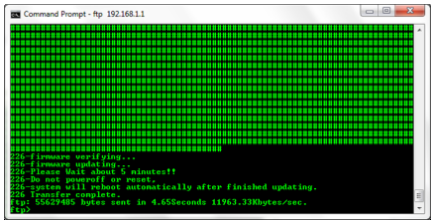


2. ผ่าน FTP

- เปิดหน้า Command Prompt แล้วเข้าไปยัง Directory ที่ไฟล์ Firmware อยู่จากตัวอย่างจะอยู่ที่ c:\
- พิมพ์คำสั่ง ftp < IP Address> จากตัวอย่างคือ ftp 192.168.1.1
- ใส่ Username Password เช่นเดียวกับที่ Login ผ่านทางหน้า Web GUI
- พิมพ์คำสั่ง bin
- พิมพ์คำสั่ง hash
- พิมพ์คำสั่ง put <ชื่อไฟล์> ras จากตัวอย่างเป็น put 300BDS2C0.bin ras



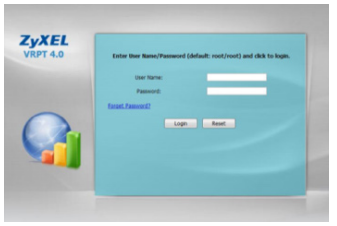
- เมื่อเสร็จแล้วจะปรากฏข้อความดังรูป รอจนอุปกรณ์ reboot เสร็จ



**ข้อแนะนำ* ระหว่างอุปกรณ์ทำการ Reboot อยู่ห้ามปิด Power หรือ Reset เป็นอันขาด ให้รอจน Reboot เสร็จสิ้น จะใช้เวลาประมาณ 5 นาที ในการ Reboot*

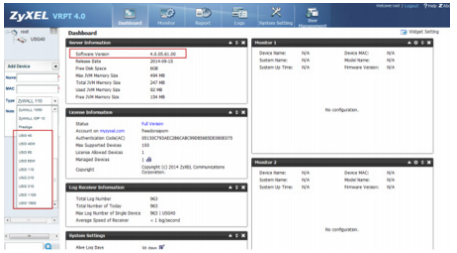
การใช้งานร่วมกับ Vantage Report

ไปที่เมนู Configuration >> Log Setting เพื่อทำการตั้งค่าให้อุปกรณ์ทำการส่ง Log ไปยัง SysLog Server หรือเครื่องที่ลง Vantage Report ไว้นั้นเอง ที่ Vantage Report ทำการ Register และทำการ Add Device ก็สามารถรับ Log จากอุปกรณ์ได้



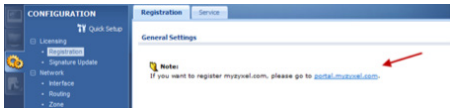
เมื่อติดตั้งโปรแกรม Vantage Report เรียบร้อยแล้ว ให้เรียกใช้งานที่ http://localhost:8080/vrpt จะปรากฏหน้าต่างรูป Username และ Password จะเป็น root จากนั้นจึงทำการ Register ที่เมนู system setting >> Registration โดย Account ที่ใช้นั้นจะเป็น Account ของ myzyxel.com จากนั้นก็ Add Device โดยคลิ๊กขวาที่เมนู root ที่อยู่ทางด้านซ้ายสุด จะปรากฏดังภาพ คือใส่ชื่อที่เราต้องการ นำ MAC Address ตัวแรกของอุปกรณ์มาใส่โดยดูได้จากหน้า Status ของอุปกรณ์ หรือใต้อุปกรณ์ แล้วเลือก Type ให้ตรงกับรุ่นที่ใช้

สุดท้ายไปที่ Logs >> Log Viewer ทำการ Search เพื่อดูว่ามี Log มาหรือไม่ เมื่อมี Log มาแล้วให้รออีกซักระยะหนึ่งก็จะมีกราฟปรากฏขึ้นในหัวข้ออื่นๆ ต่อไป

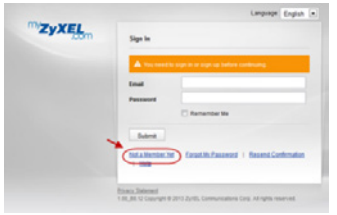


การ Register อุปกรณ์และ License

ไปที่เมนู Licensing >> Registration กด link portal.myzyxel.com เพื่อเข้าสู่ Web myZyXEL.com ในการลงทะเบียนอุปกรณ์



ทำการสมัคร Account เพื่อเข้าสู่ระบบของ myZyXEL.com



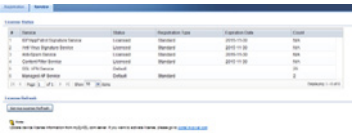
เมื่อ login เข้าระบบได้เรียบร้อย

ให้ทำการลงทะเบียนอุปกรณ์ที่เมนู Device Registration โดยกรอกข้อมูล MAC Address ตัวแรก และ Serial Number ของตัวอุปกรณ์

ลงทะเบียน Service license ที่เมนู Service Registration

ทำการ Activate License Service ของอุปกรณ์ที่เมนู Device Management จึงเสร็จสิ้นขั้นตอนการลงทะเบียนใช้งาน License Service

กลับมาที่ตัวอุปกรณ์ USG เพื่อตรวจสอบส Status ของ License ว่าถูกต้องหรือไม่ ที่เมนู Licensing >> Registration >> Service หากยังไม่ถูกต้องให้ทำการกด Service License Refresh



การ Update Signature

ไปที่เมนู Licensing >> Signature update เพื่อกำหนดช่วยเวลาที่ต้องการที่จะให้อุปกรณ์ทำการ Download Signature ใหม่ๆ มา หรือจะให้ Download ในทันทีเลยก็ได้โดยกดที่ Update Now