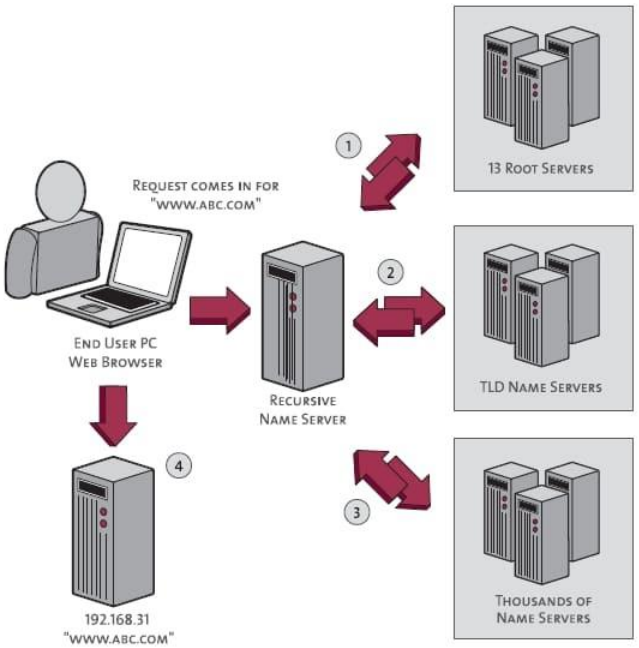
คู่มือการใช้งาน
ระบบป้องกันความปลอดภัยการให้บริการ DNS

DNS ย่อมากจาก Domain Name System ทำหน้าที่แปลง Domain Name ไปสู่ IP Address ซึ่งเป็นค่าตัวเลขที่ Browsers ใช้ในการโหลดหน้า Internet ทุกอุปกรณ์ที่เชื่อมต่อกับอินเตอร์เน็ตจะมีเลข IP Address ซึ่งใช้สำหรับเป็นชื่อสำหรับให้อุปกรณ์อื่นๆ ใช้ในการระบุตัวตน ซึ่งจะทำให้ผู้ใช้งานสามารถพิมพ์ข้อความลงบนเบราว์เซอร์เว็บไซต์เป็นชื่อของเว็บนั้นๆ เช่น kru.ac.th, fst.kru.ac.th, google.com, yahoom.comหรือ sanook.com เป็นต้น เพื่อทำเปิดหน้าเว็บไซต์ที่ต้องการขึ้นมา แทนที่จะพิมพ์ IP Address ของทุกๆ Website แทน



ภาพ การทำงานของระบบ DNS Server
ที่มา https://techforteam.com/blog/dns-server/

การจัดการ DNS และ DHCP ด้วยอุปกรณ์ Infoblox

Infoblox เป็นบริษัทด้าน IT Automation และ Network Security จากสหรัฐอเมริกาที่สามารถตอบโจทย์การทำธุรกิจในยุคดิจิทัล โดยการเชื่อมต่อ Network ไม่ว่าจะเป็นอุปกรณ์ IoT, Machine Learning, Blockchain เป็นต้น Infoblox ได้ก่อตั้งขึ้นในปี 1999 ที่เมืองชิคาโก ทางบริษัทมีโซลูชั่นด้านความปลอภัยของ Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) และ IP address management ซึ่งทั้งสามส่วนนี้รวมเรียกกันว่า DDI ซึ่ง DDI ย่อมาจากระบบ DNS , DHCP และ IP Address Management เป็นระบบ Service ที่มีความสำคัญมาก ทำหน้าที่เชื่อมโยงทุกสิ่งในระบบ Network เข้าหากัน สามารถใช้จัดการ IP Address ขององค์กรแบบอัตโนมัติทั้ง IPv4 และ IPv6 ทั้งที่เป็น Physical และ Virtual Systems ให้ความสะดวกกับผู้ดูแลระบบ ทำให้แก้ปัญหา Network ได้อย่างรวดเร็วกว่าการจัดการแบบเดิม

ประโยชน์ที่ได้รับจากการใช้งาน Infoblox DNS & DHCP

ทำให้ใช้งานของผู้ใช้ รวมทั้งอุปกรณ์ที่เข้าใช้งานระบบเครือข่ายมีความน่าเชื่อถือได้มากขึ้น (Hardening OS) ช่วยเพิ่มประสิทธิภาพในการทำงานได้สูงสุดไม่สามารถ Root Access ได้ ทั้งยังได้รองรับการทำงานผ่านอุปกรณ์ผ่าน Certified Common Criteria EAL2 มีความสามารถในการป้องกันช่องโหว่ของอุปกรณ์ รวมทั้งการ Update Antivirus ความจุ (Capacity) รองรับการบริหารจัดการแบบ Centralize management ในกรณีที่มีอุปกรณ์หลายๆ ตัว สามารถใช้ประโยชน์จากระบบ IP Tracking ได้แบบ Real Time เพื่อตรวจสอบข้อมูลว่า IP Address ที่แจกไป รวมถึงสามารถบริหาร IP Address ที่ยังไม่ถูกใช้งานได้อย่างไม่มีข้อขัดข้อง รองรับ HA และ DHCP Fail Over เพื่อรองรับการทำงานกรณีที่เกิดปัญหา สามารถออกรายงานเชิงสถิติเพื่อเสนอต่อผู้บริหารด้วย Infoblox reporter Network Design เป็นต้น

ระบบการบริหารจัดการและควบคุมการใช้งาน DHCP และ IP Address ของหลาย ๆ หน่วยงานมักจะถูกออกแบบให้ใช้บนเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ (Server) เพื่อ Control และ Management โดยจะพบปัญหา ดังนี้

1) ระบบปฏิบัติการเป็นเครื่อง Server ทำให้ต้อง Hardening Server เนื่องจาก Server มี Vulnerability ค่อนข้างมากและต้องมีการ Update Anti-virus อยู่ตลอด

2) ไม่สามารถกำหนดการแจก IP Address หรือจำกัดการใช้งานที่แน่นอนได้เนื่องจากระบบ Server ไม่รองรับการกำหนดค่าการแจก IP Address ที่แน่นอน

3) การใช้บริหาร Server ที่ซับซ้อนต้องใช้บุคลากรที่มีความเชี่ยวชาญในการใช้งาน

4) ระยะเวลาที่ใช้ในการ Manage ต่อ 1 IP คิดตามค่าเฉลี่ยค่อนข้างนาน

5) ไม่มีระบบ HA รองรับกรณีที่เครื่อง Server ที่ใช้ในการแจก DHCP เกิดปัญหาเนื่องจากการแจก IP Address ที่มากขึ้นทำให้การทำงานของเครื่อง Server หนักขึ้น บางครั้ง Server เกิดอาการ Hang และ Restart ตัวเองบ่อยๆ โดยที่ทางผู้ดูแลระบบ (Administrator) ไม่ทราบสาเหตุ โดยต้องแก้ปัญหาโดยการเพิ่ม RAM หรือ CPU ของเครื่องเพื่อให้รองรับการใช้งานได้ ซึ่งไม่สามารถประเมินการทำงานที่แท้จริงได้ กรณีที่มีการตั้งเครื่อง Server เพื่อแจก DHCP หลายๆ เครื่อง ข้อมูลไม่มีการ Synchronize กันเนื่องจากต้องแยกบริหารจัดการ Server แต่ละเครื่อง เป็นต้น

6) ข้อมูล IP Address ระบบไม่มีการ Update แบบ Real time การทำ Policy เพื่อแยกแจก IP Address ตามชนิดของอุปกรณ์ทำได้ยาก กรณีที่เกิดปัญหาและต้อง Restore จาก Back up ข้อมูลที่นำมาใช้ไม่ up to date และนี่เป็นเพียงปัญหาที่พบบ่อยจากการใช้งาน Server ช่วยในการจดจำและบริหารจัดการ IP Address

7) IP ADDRESS MANAGEMENT (IPAM) ระบบบริหารจัดการ IP Address หรือ IP Address Management นั้น ในปัจจุบันมีส่วนช่วยในการบริหารจัดการ IP Address ให้เป็นไปได้ง่ายขึ้น เมื่อต้องก้าวเข้าสู่ยุคของ IPv6 เป็นไปได้ยากที่เราจะ Manage IP ผ่านระบบ Manual อย่างเดิมแล้วไม่เกิดข้อผิดพลาด ทำให้ผู้ดูแลระบบการแจก IP ต้องทำงานที่ซับซ้อนมากยิ่งขึ้น

ประโยชน์และบทบาทในการดูแลระบบ

1) User มีการ request เพื่อขอ IP Address 3-7 IP ต่อ 1 คน การ Manage ผ่านระบบ Manual เป็นได้ได้ช้าด้วยปริมาณ IP Address ที่เพิ่มขึ้น บางครั้งอาจเกิดข้อผิดพลาด อัตราการขยายตัวของ IP Address มีจำนวนเพิ่มมากขึ้นตลอดเวลา

2) Mobility and IP device growth

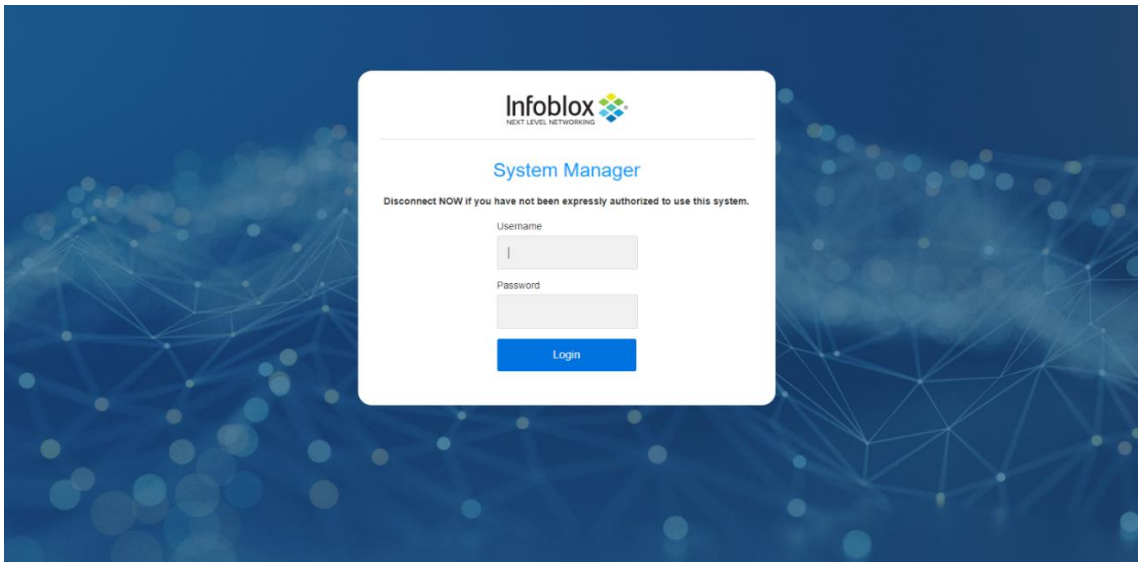
3) IPv6 and DNSSEC

4) Data center virtualization

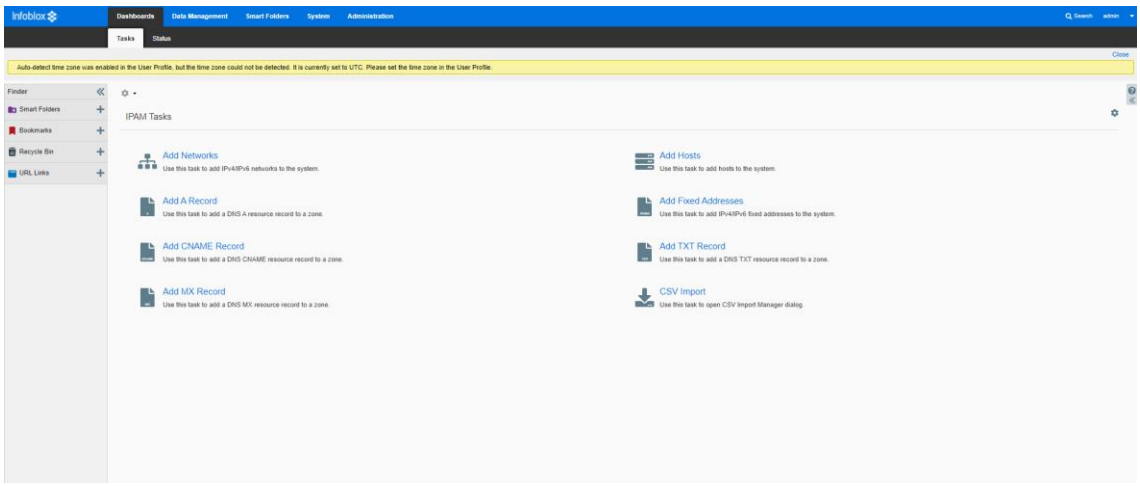
5) การทำ Capacity และ Inventory planning เพื่อรองรับการขยายตัวของธุรกิจ

ขั้นตอนการเพิ่ม DNS ด้วย Infoblox

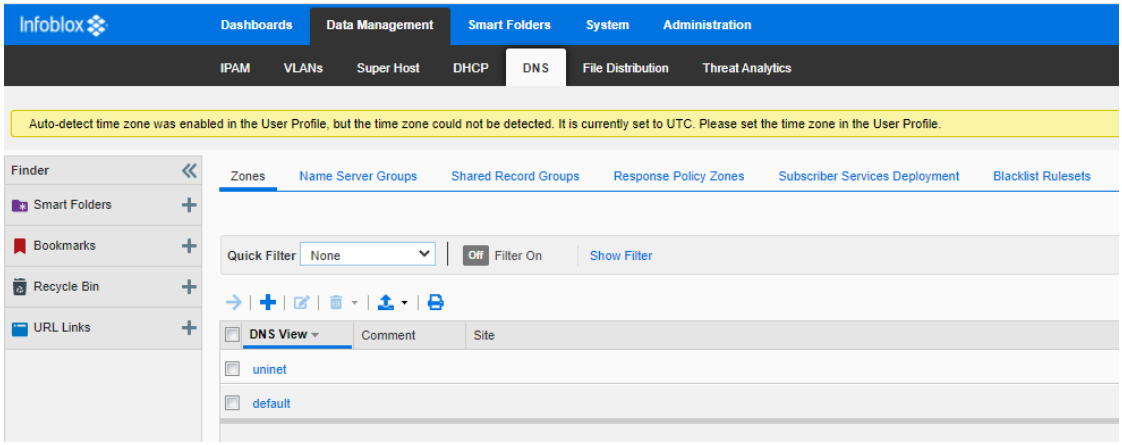
1. ล็อคอินเข้าระบบบริหารจัดการ Infoblox



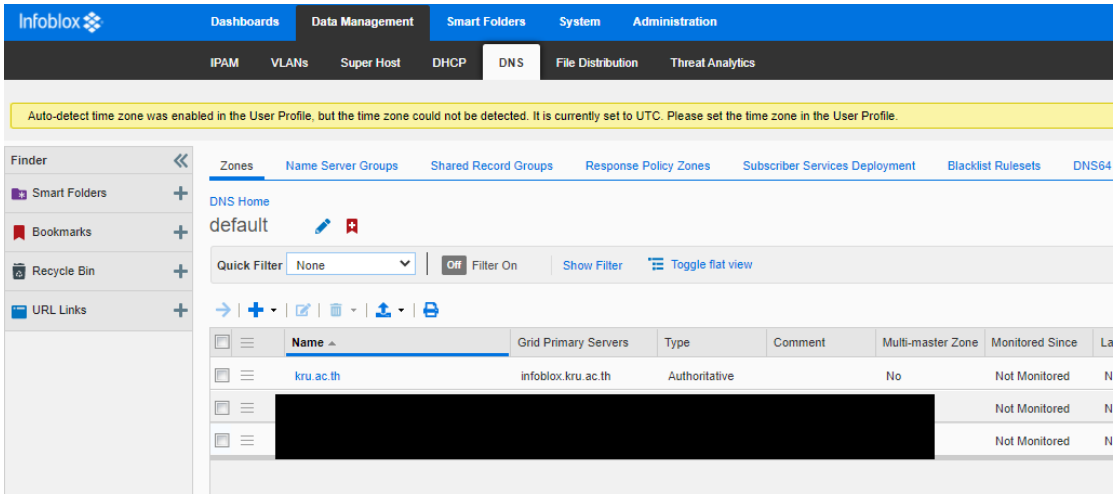
2. เมื่อล็อคอินเข้าสู่ระบบจะปรากฏหน้าต่างดังรูป



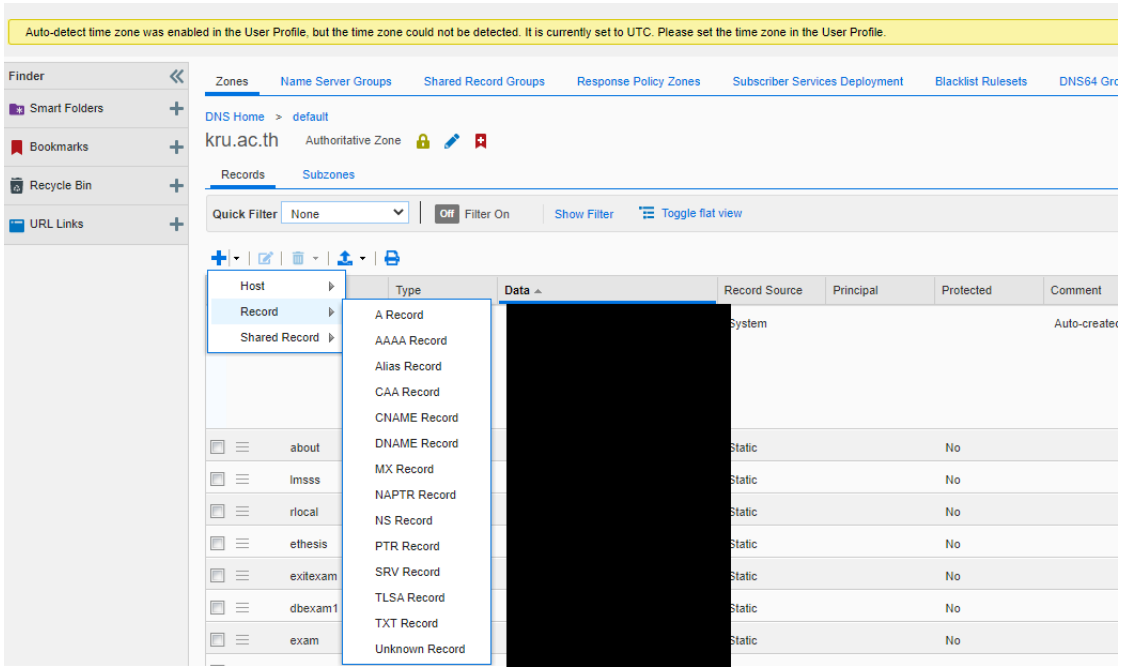
3. เลือกแท็บเมนู Data Management > DNS ตามรูป



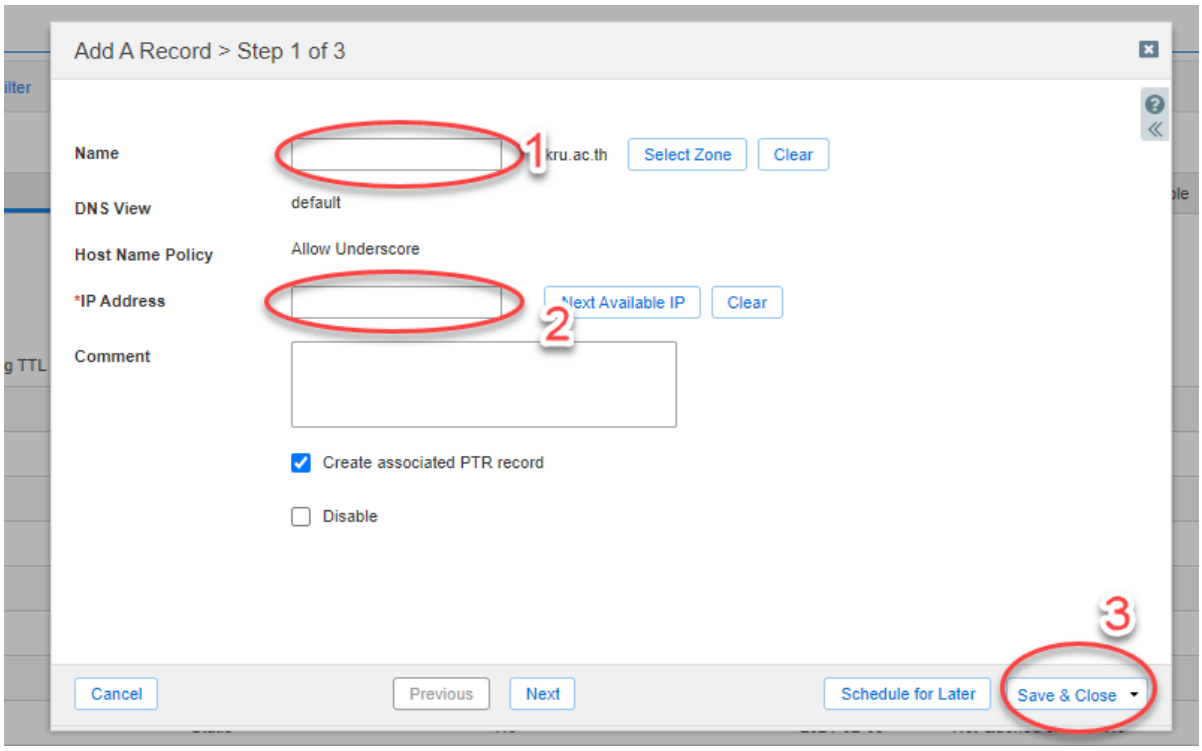
4. เลือก kru.ac.th



5. เลือกเพิ่ม Record > A Record ตามภาพ



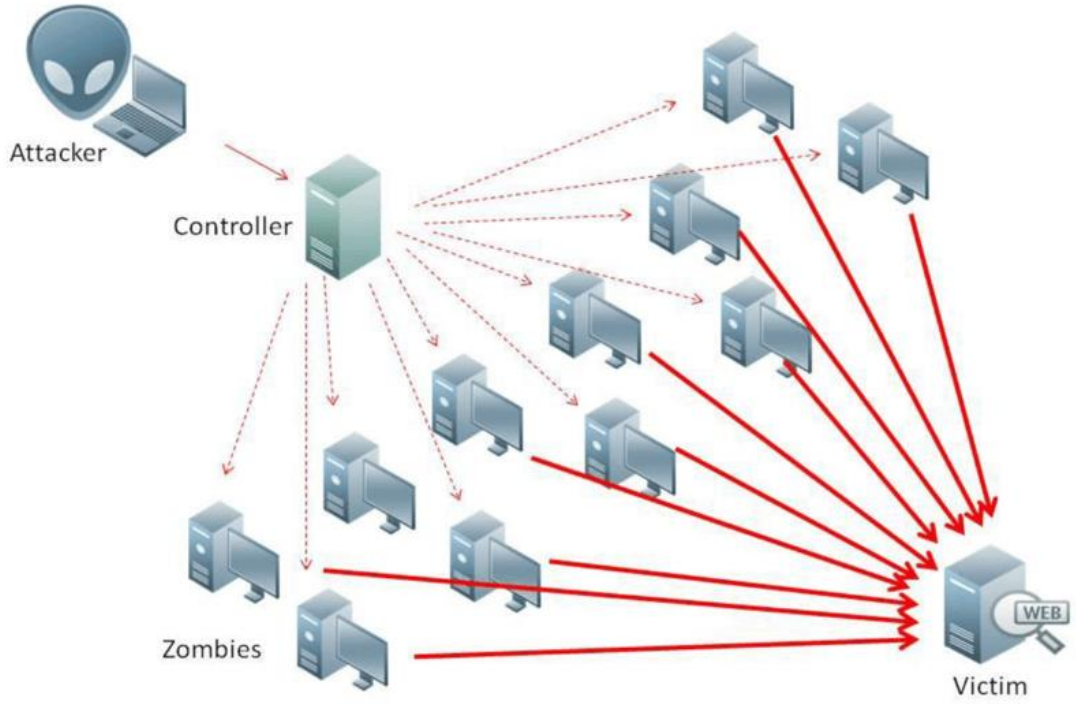
6. ช่องที่ 1 กำหนดชื่อ DNS ช่องที่ 2 ใส่ Ip address ช่องที่ 3 บันทึกและเสร็จสิ้น



คู่มือการใช้งาน

ระบบป้องกันการโจมตี DDOS

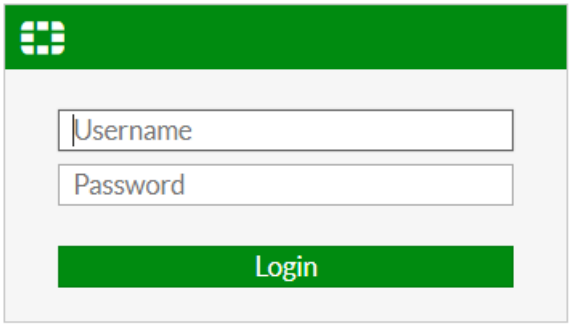
DOS เป็นการโจมตีแบบ denial of service สามารถเข้าใจได้ง่ายและมีประสิทธิภาพมาก ผู้โจมตีพยายามทำให้ service ของไซต์นั้นไม่สามารถทำงานได้โดยการส่งคำร้องขอ (requests) หรือหยุดการทำงานในขณะนั้น เช่น ถ้าคุณมีเซิร์ฟเวอร์รับส่งเมลที่สามารถรับและส่งเมล 100 ข้อความในหนึ่งวินาที ผู้โจมตีก็เพียงแต่ส่งข้อความไปยังเซิร์ฟเวอร์นั้น 200 ข้อความต่อหนึ่งวินาที อาจทำให้การติอต่อสื่อสารกับภายนอกจะถูกตัดขาดหรืออาจทำให้เมลเซิร์ฟเวอร์อาจหยุดการตอบรับทั้งหมด โดยทั่วไปผู้โจมตีจะโจมตีเป้าหมายที่เด่นชัด เช่น เว็ปเซิร์ฟเวอร์ หรือเป้าหมาย ที่เป็นโครงสร้างพื้นฐาน เช่น เราเตอร์ (router) และการเชื่อมโยงของเน็ตเวิร์ค เป็นต้น



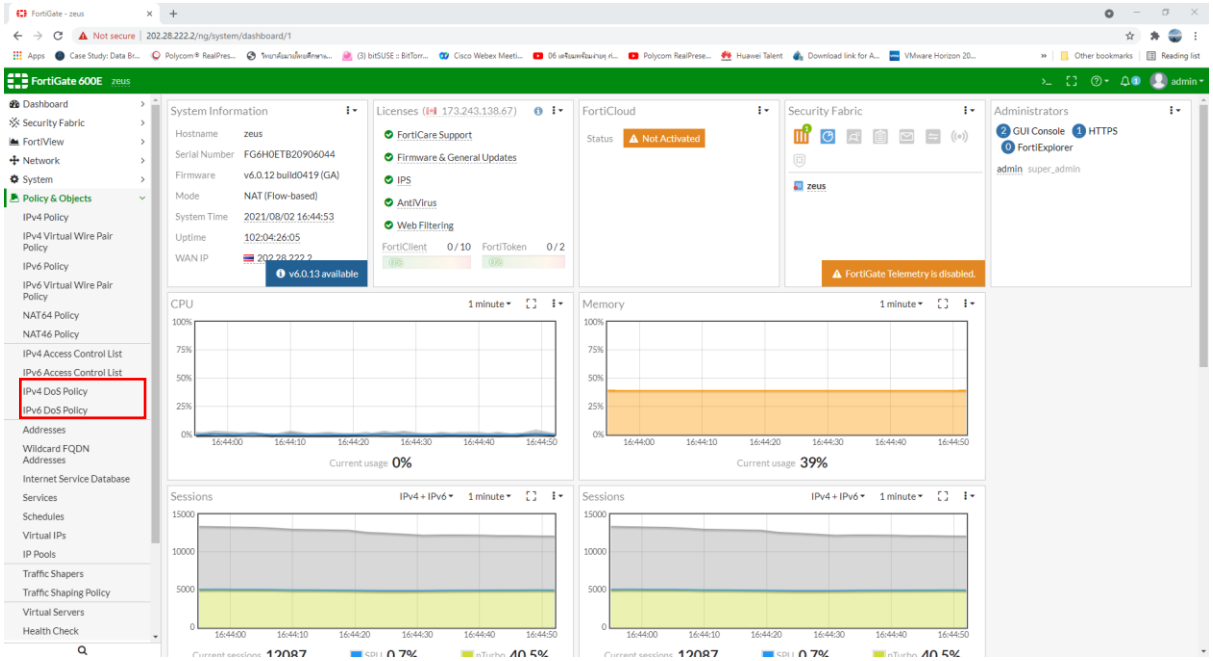
ภาพ แสดงลักษณะการโจมตีแบบ DOS (denial of service)
ที่มา http://www2.crma.ac.th/itd/CertDetail.asp?ID=00059

ขั้นตอนการใช้งานระบบป้องกันการโจมตี DDOS มีขั้นตอน ดังนี้

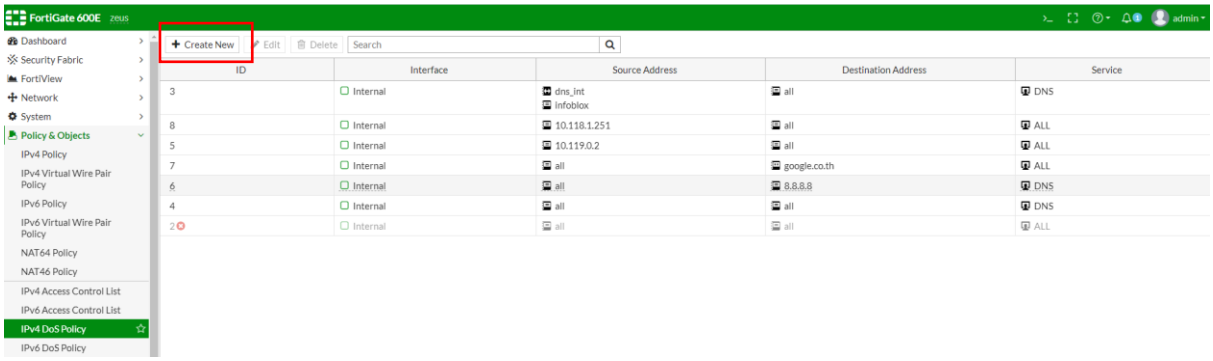
1. ล็อคอินเข้าระบบบริหารจัดการ Fortigate Appliance



2. เมื่อล็อคอินเข้าสู่ระบบจะปรากฏหน้าต่างดังรูป



3. เลือกแท็บเมนู Policy & Objects > IPV4 Dos Policy ตามรูป



4. เลือก กำหนดค่า ต่าง ๆ ตามรูป

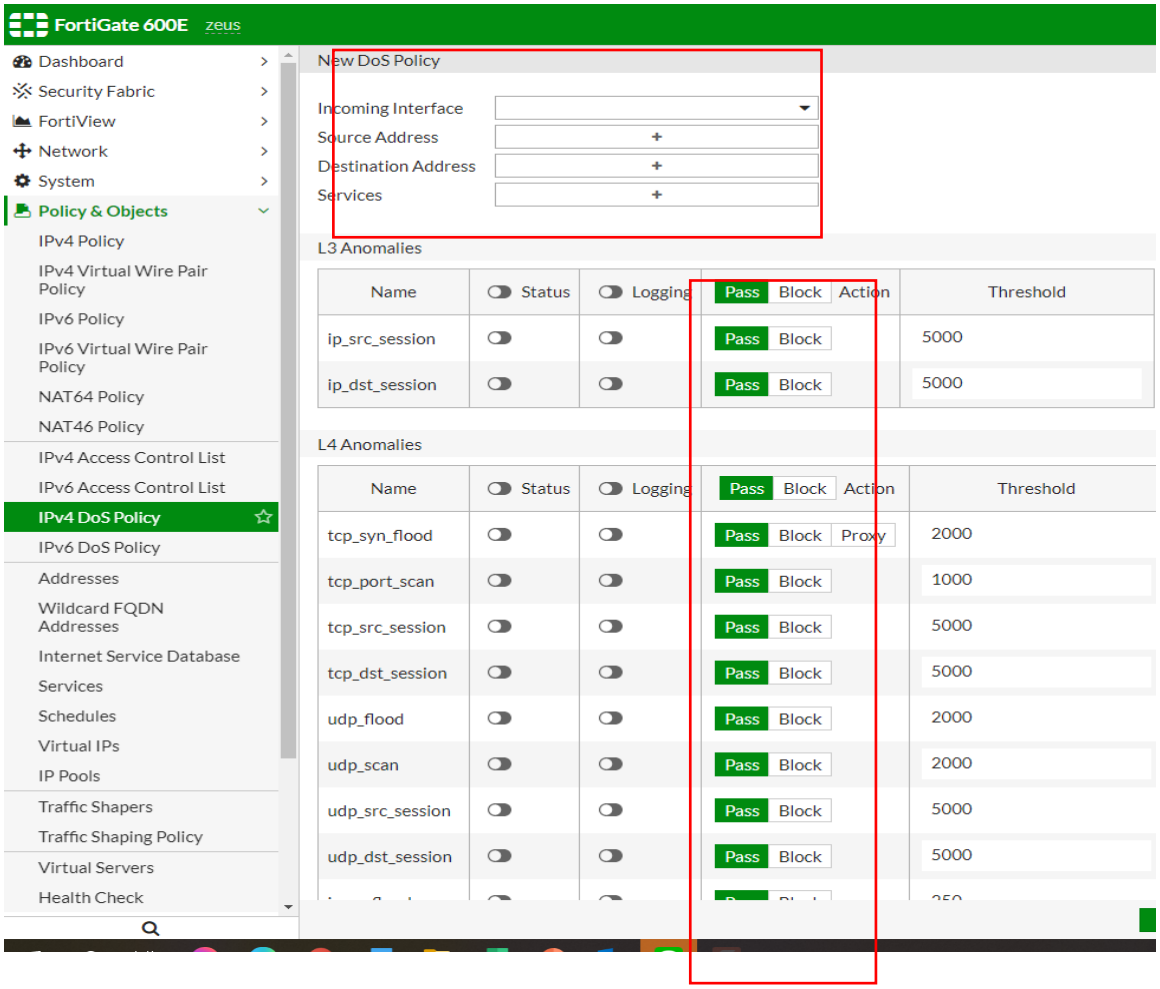
จะประกฎหน้าต่างดังภาพ

ช่องที่ 1 ใส่ Interface ขาใน

ช่องที่ 2 ใส่ IP Address ต้นทาง

ช่องที่ 3 ใส่ IP Address ปลายทาง

ช่องที่ 4 ใส่ Service หรือ Application ที่ต้องการป้องกัน



5. เลือกตั้งค่า policy สำหรับการป้อง DOS Attack

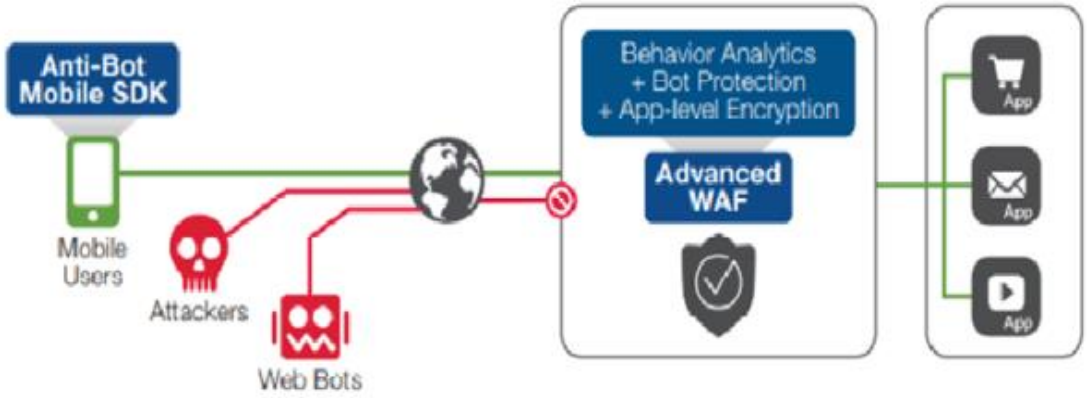
คู่มือการใช้งาน
ระบบการป้องกันการโจมตีผ่านเว็บ (Web Application Firewall : WAF)

Web Application Firewall (WAF) เป็นเครื่องมือที่ใช้ป้องกัน Web application จากการโจมตีผ่านทาง Application Layer เช่น Cross-site scripting (XSS), SQL Injection และ Cookie Poisoning และอื่นๆ ซึ่งช่องทางแรกที่จะถูกโจมตีก็คือ Website หรือ Application ที่เป็นด่านหน้าในการรองรับการใช้งานจากผู้ใช้ ซึ่งหากถูกผู้ไม่หวังดีสามารถโจมตีระบบเข้ามาได้ จะสามารถเข้าถึงข้อมูลสำคัญที่เก็บไว้ในฐานข้อมูลได้ การที่มี WAF ติดตั้งอยู่และวางไว้ถูกที่ถูกเวลาจะช่วยให้สามารถป้องกันการโจมตีระบบได้

WAF ทำงานได้อย่างไร

หลักการที่ WAF ป้องกัน Web App ของคุณคือ การกรองข้อมูล, การ Monitoring และการ Block Traffic แปลกปลอมที่เป็น HTTP/HTTPS ที่ส่งมายัง Web Application ของคุณ และก็ป้องกันไม่ให้ข้อมูลส่งออกจาก Application โดยการใช้ Policy หลาย ๆ Policy เข้ามาช่วยวิเคราะห์หรือพิจารณาว่าTraffic ไหนผิดปกติ และ Traffic ไหนปลอดภัย Proxy Server จะทำหน้าที่ป้องกันข้อมูลของ Client ที่สามารถรั่วไหลออกได้ แต่ WAF จะทำหน้าที่ตรงกันข้ามกับ Proxy Server เรียกว่าเป็น Reverse Proxy มีหน้าที่ป้องกันไม่ให้ Traffic ที่ดูแล้วน่าจะเป็นภัยคุกคามต่อ Client เข้าถึงข้อมูลภายในของ Web Application Server ได้

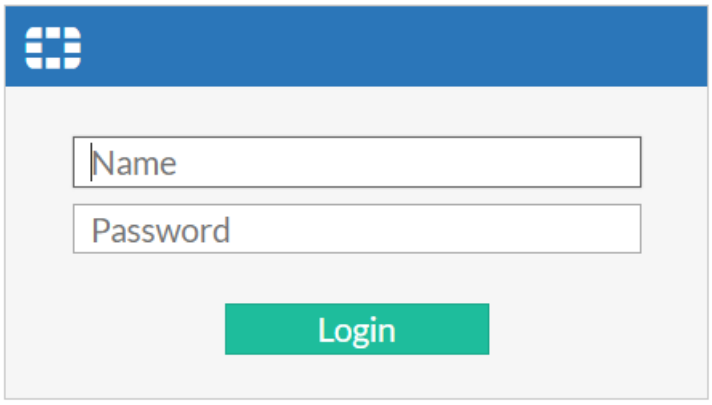
ผลิตภัณฑ์ WAF ในตลาดมีอยู่หลากหลายรูปแบบเลย ไม่ว่าจะเป็น Software, Appliance หรือบริการแบบ Delivered as a service ส่วนของ Policy เองก็สามารถปรับค่าได้ตามต้องการให้เหมาะสมกับ Web Application ของคุณ ถึงแม้ว่า WAF หลาย ๆ เจ้า จะสามารถ Update Policy ได้อยู่บ่อยๆ เพื่อให้พร้อมกับภัยคุกคามรูปแบบใหม่ ๆ บางรายถึงขั้นมีการใช้ Machine Learning ในการ Enable ให้ WAF Update ได้แบบอัตโนมัติ การที่มี Feature แบบนี้จะช่วยให้ลดปัญหาที่ยุ่งยากในการ Update Policy ได้ และทำให้มั่นใจว่า WAF จะสามารถป้องกันภัยคุกคามชนิดใหม่ๆ ได้



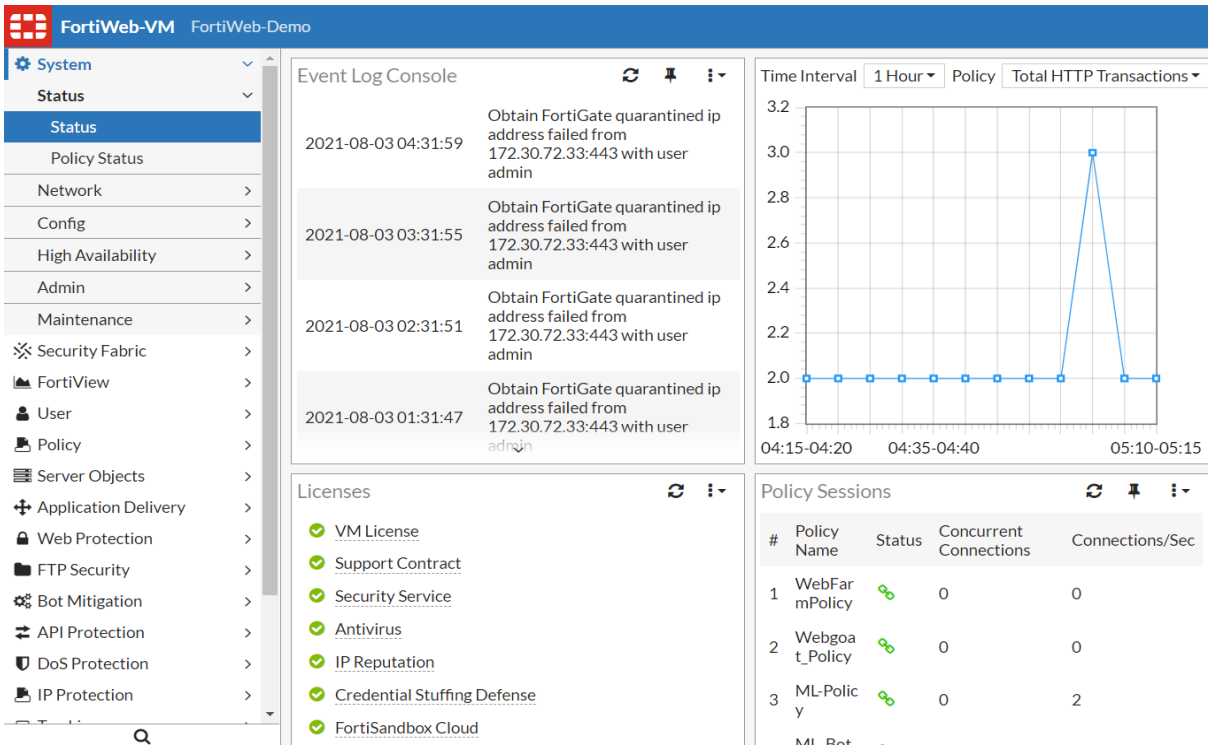
ภาพ แสดงการทำงานของ Web Application Firewall (WAF)
ที่มา WWW.F5.COM

ขั้นตอนการบริหารจัดการ Web Application Firewall

1. ล็อคอินเข้าระบบบริหารจัดการ Fortiweb Vitual Appliance

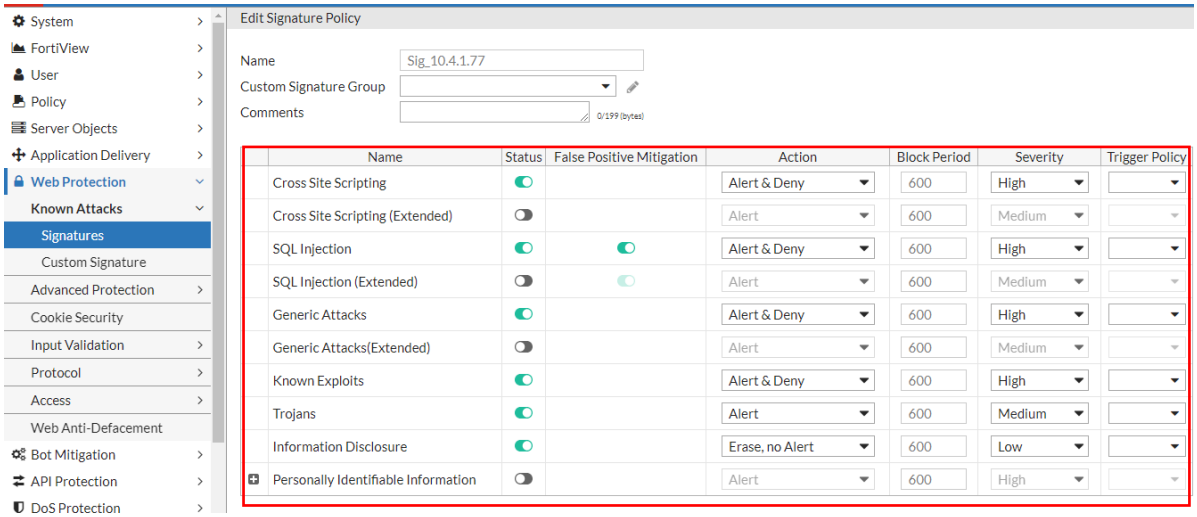


2. เมื่อล็อคอิน เข้าสู่ระบบแล้ว จะปรากฏ ดังภาพด้านล่าง



3. เมื่อต้องการ สร้าง Policy สำหรับป้องกัน Website โดยสามารถทำตาม วิธีการ ด้านล่าง ทำการสร้าง Signature โดยเลือก Web Protection → Know Attacks → Signature โดยมี Action คือ

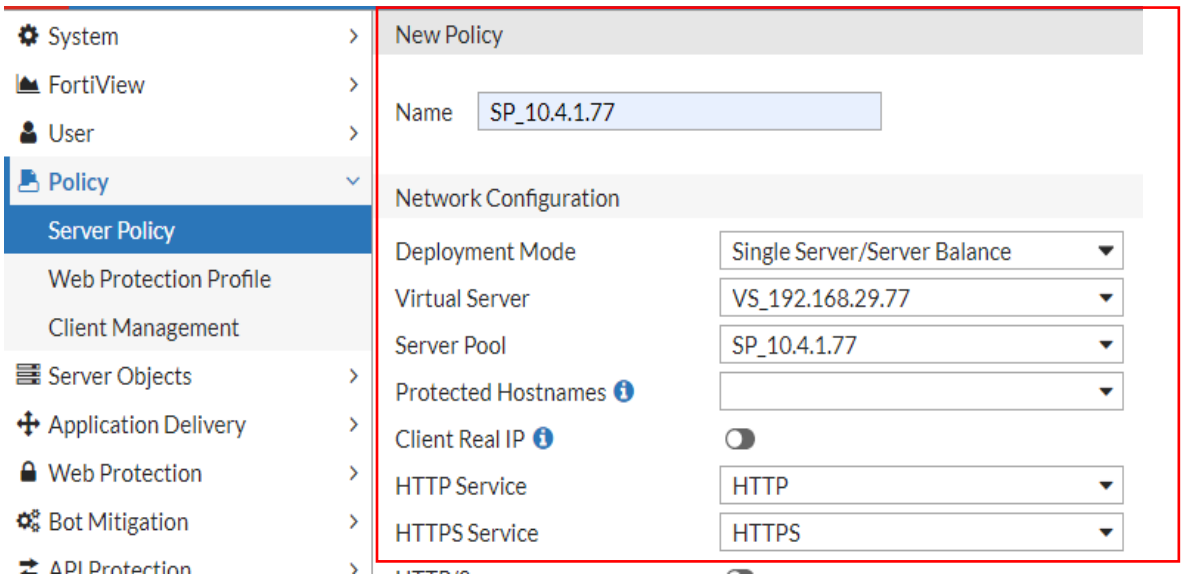
- Alert คือ Accept the request ของ client และ ส่ง log /or email
- Alert & Deny คือ Block the request ของ client และ ส่ง log /or email
- Deny (no log) คือ Block the request ของ client
- Period Block คือ Block the request ของ client เป็นเวลา 1 ถึง 600 หน่วยเป็นวินาที
- Redirect คือ Request ของ client zจะถูกส่งไปยัง web server อื่นที่ถูกระบุไว้
- Send HTTP Response คือ Block and reply to the client



4. เมื่อต้องการ สร้าง Policy สำหรับป้องกัน Website โดยสามารถทำตาม วิธีการ ด้านล่าง

สร้าง Server Policy โดยเลือก Policy → Server Policy → Create New โดยมีค่า parameter ที่ต้องใส่คือ

- Name ใส่ชื่อของ Server Policy
- Deployment Mode เลือก Single Server/Server Blance
- Virtual Server เลือก VS_192.168.29.77
- Server Pool เลือก SP_10.4.1.77
- HTTP Service เลือก HTTP
- HTTPS Service เลือก HTTPS
- Web Protection Profile เลือก WP_10.4.1.77
- Monitor Mode เลือก enable เมื่อต้องการให้ Fortiweb ทำการ simulate protection (มี log ขึ้นตาม action ที่ถูกกำหนดเช่น block แต่จะไม่มีการ block เกิดขึ้นจริง)



Fortiweb สามารถทำการป้องกัน web server เบื้องต้นได้แล้ว โดยสามารถให้ Firewall เปลี่ยน DNAT จาก 10.4.177 มาเป็น 192.168.29.77 เพื่อให้ http traffic ผ่าน Fortiweb เพื่อทำการกรอง traffic ก่อนเรียกไปยัง web server (Client จะไม่มีการติดต่อโดยตรงกับ web server)

คู่มือการใช้งาน
การควบคุมการใช้งาน Network Access Control (NAC)

Network Access Control (NAC) คือ คอมพิวเตอร์เครือข่ายหรอโซลูชันที่ใช้ชุดของโปรโตคอลเพื่อกำหนดและดำเนินนโยบายที่อธิบายถึงวิธีการรักษาความปลอดภัยในการเข้าถึงเครือข่ายโหนดโดยอุปกรณ์เมื่อพยายามเข้าถึงเครือข่าย NAC อาจรวมกระบวนการแก้ไขอัตโนมัติเข้ากับระบบเครือข่ายทำให้โครงสร้างพื้นฐานของเครือข่าย เช่น เราเตอร์สวิตช์และไฟร์วอลล์สามารถทำงานร่วมกับเซิร์ฟเวอร์ส่วนหลังและอุปกรณ์คอมพิวเตอร์ของผู้ใช้ปลายทางเพื่อให้แน่ใจว่าระบบข้อมูลทำงานอย่างปลอดภัย ก่อนที่จะอนุญาตให้ใช้งานร่วมกันได้ รูปแบบพื้นฐานของ NAC คือ 802.1X มาตรฐานการควบคุมการเข้าถึงเครือข่ายมีจุดมุ่งหมายเพื่อทำสิ่งที่ชื่อมีความหมาย ควบคุมการเข้าถึงไฟล์เครือข่าย ด้วยนโยบายต่างๆ รวมถึงการตรวจสอบนโยบายการรักษาความปลอดภัยของอุปกรณ์ปลายทางก่อนการรับเข้าและการควบคุมหลังการรับเข้าซึ่งผู้ใช้และอุปกรณ์สามารถไปที่เครือข่ายได้และทำอะไรได้บ้าง

เป้าหมายของ NAC

เนื่องจาก NAC เป็นผลิตภัณฑ์รักษาความปลอดภัยที่เกิดขึ้นใหม่คำจำกัดความจึงมีทั้งการพัฒนาและการโต้เถียง เป้าหมายที่ครอบคลุมของแนวคิดสามารถกลั่นได้ดังนี้

การบรรเทาของการโจมตีแบบศูนย์วัน

1) การอนุญาตการรับรองความถูกต้องและการบัญชีของการเชื่อมต่อเครือข่ายการเข้ารหัสการรับส่งข้อมูลไปยังเครือข่ายไร้สายและแบบใช้สายโดยใช้โปรโตคอลสำหรับ 802.1X เช่น EAP-TLS, EAP-PEAP หรือ EAP-MSCHAP

2) การควบคุมตามบทบาทของผู้ใช้อุปกรณ์แอปพลิเคชันหรือการตรวจสอบความปลอดภัยหลังการโพสต์การทำงานอัตโนมัติด้วยเครื่องมืออื่น ๆ เพื่อกำหนดบทบาทเครือข่ายตามข้อมูลอื่น ๆ เช่นช่องโหว่ที่ทราบสถานะการแหกคุกเป็นต้น

3) ประโยชน์หลักของโซลูชั่น NAC คือ การป้องกันสถานีปลายทางที่ไม่มีโปรแกรมป้องกันไวรัสแพตช์หรือซอฟต์แวร์ป้องกันการบุกรุกโฮสต์จากการเข้าถึงเครือข่ายและทำให้คอมพิวเตอร์เครื่องอื่นเสี่ยงต่อการปนเปื้อนข้ามของ เวิร์มคอมพิวเตอร์.

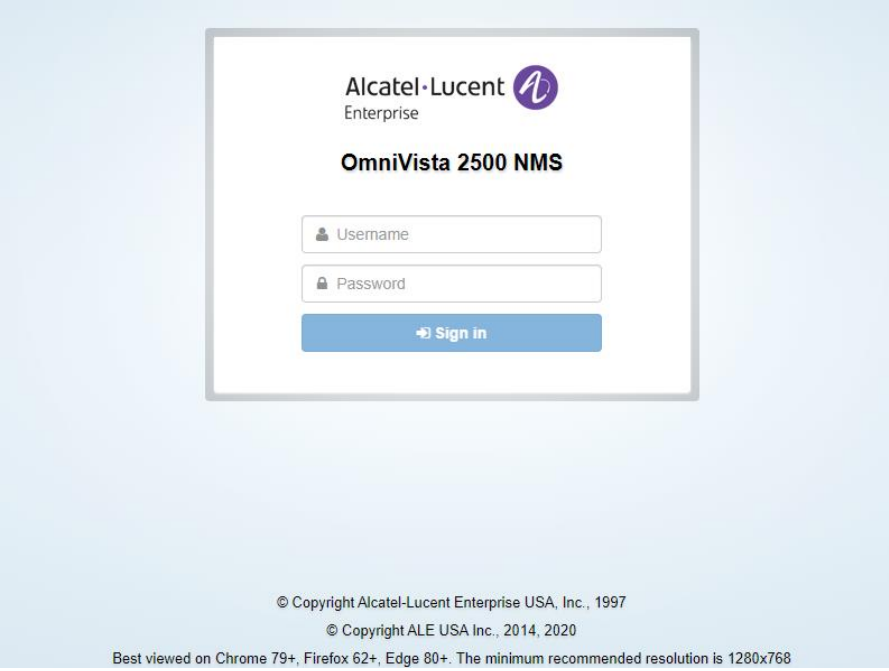
การบังคับใช้นโยบาย

โซลูชัน NAC อนุญาตให้ผู้ให้บริการเครือข่ายกำหนดนโยบายเช่นประเภทของคอมพิวเตอร์หรือบทบาทของผู้ใช้ที่ได้รับอนุญาตให้เข้าถึงพื้นที่ของเครือข่ายและบังคับใช้ในสวิตช์เราเตอร์และศูนย์กลางเครือข่าย การจัดการข้อมูลประจำตัวและการเข้าถึงในกรณีที่เครือข่าย IP ทั่วไปบังคับใช้นโยบายการเข้าถึงในแง่ของ ที่อยู่ IP, สภาพแวดล้อม NAC พยายามที่จะทำตาม รับรองความถูกต้อง ข้อมูลประจำตัวของผู้ใช้อย่างน้อยสำหรับสถานีปลายทางของผู้ใช้เช่นแล็ปท็อปและคอมพิวเตอร์เดสก์ท็อป

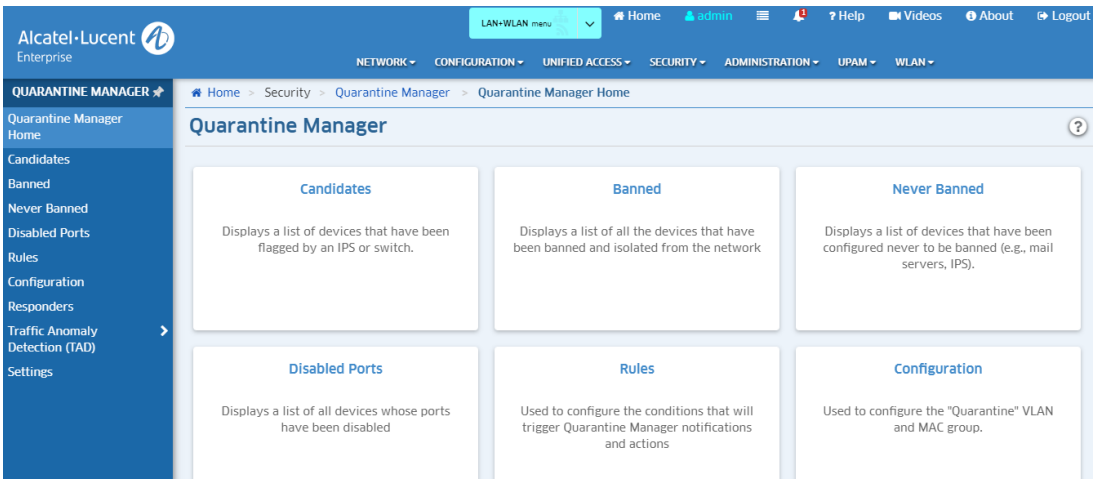
ขั้นตอนการใช้งาน

การบริหารจัดการเครื่องคอมพิวเตอร์แปลกปลอม ที่เข้ามาในระบบเครือข่ายนั้น สามารถใช้ความสามารถของ Feature เช่น Quarantine Management ใน Alcatel-Lucene มาใช้ได้ โดยมีวิธีการดังนี้

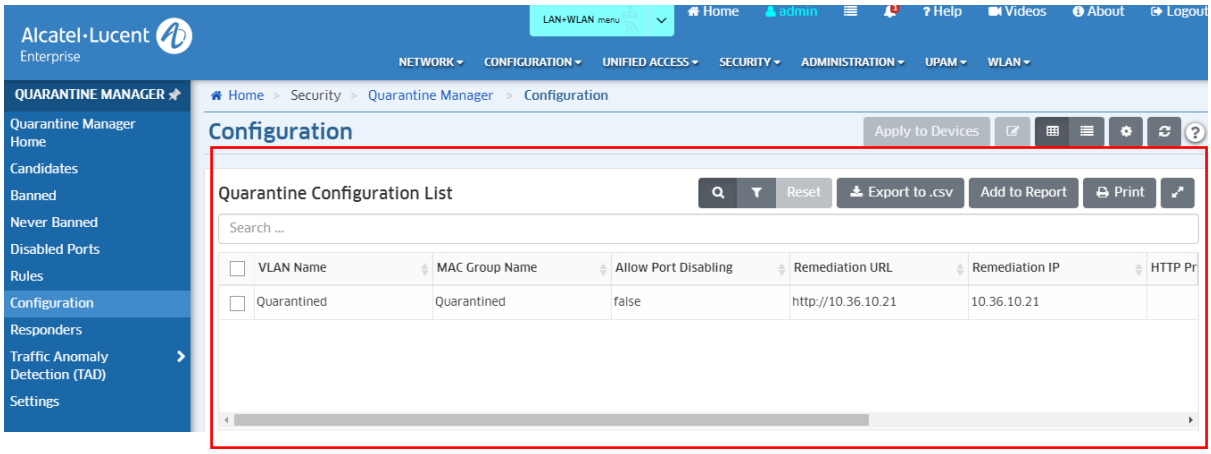
1. ทำการ Log-in เข้าสู่ระบบ OminVista 2500 NMS ผ่าน Browser ต่าง ๆ และทำการ กรอก User name และ Password เพื่อเข้าไปบริหารจัดการ



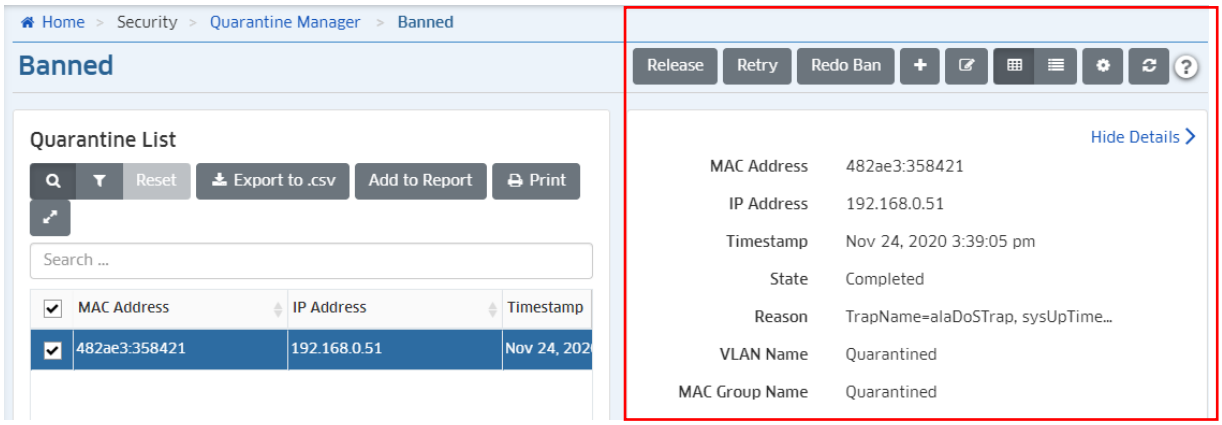
2. หลังจากทำการ Login แล้ว จะปรากฏหน้าจอ ดังภาพ ด้านล่าง



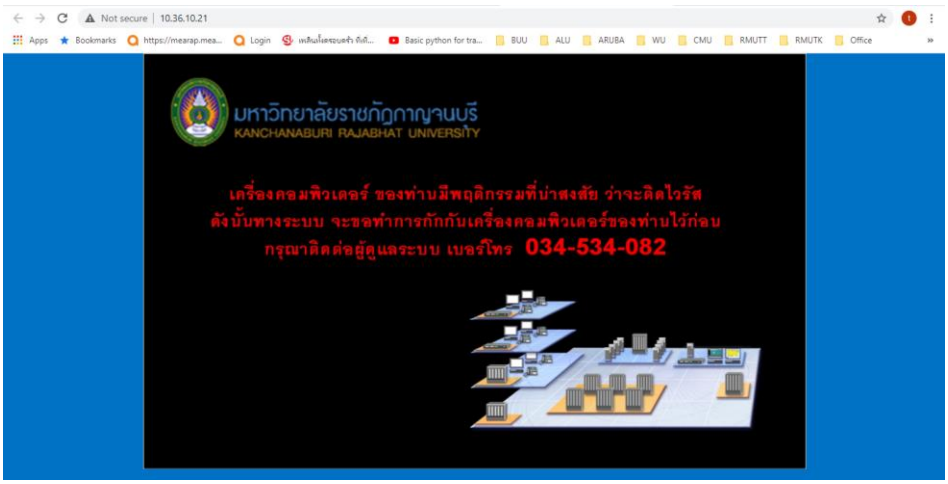
3. เลือกเมนู Configuration เพื่อกำหนด นโยบายสำหรับควบคุมเครื่องคอมพิวเตอร์แปลกปลอม หรือกำหนด Action เช่น Block หรือ Quarantine (กักขัง) เครื่องที่เชื่อมต่อแปลกปลอม



4. เลือกเมนู Banded เพื่อตรวจดูเครื่องคอมพิวเตอร์แปลกปลอมที่ ตรงกับนโยบาย (Policy) จะได้ตามภาพด้านล่าง

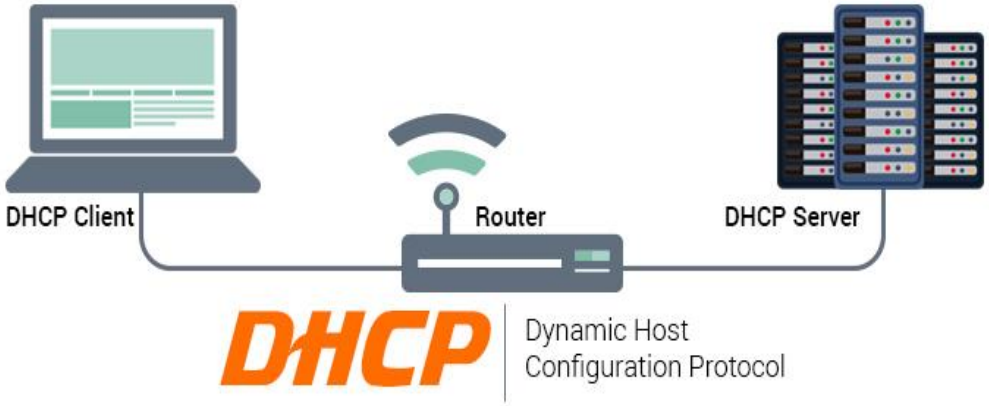


5. กรณีที่เครื่องคอมพิวเตอร์แปลกปลอมหรือคอมพิวเตอร์ในเครือข่าย เข้าเกณฑ์ตามกฎนโยบาย (Policy) สามารถที่ให้ Alcatel-Lucene Quarantine Manager ทำการแสดงหน้า Page (Notification Page) เพื่อแจ้งเตือนให้เข้าเกณฑ์ตามกฎนโยบาย (Policy) หรือผิด Policy ได้ ดังภาพด้านล่าง



คู่มือการใช้งาน
ระบบบริหารจัดการ IP Address

DHCP เป็นเครื่องมือการจัดการเครือข่ายที่ทำงานร่วมกับสองโปรโตคอล ได้แก่ Transmission Control Protocol (TCP) และ Internet Protocol (IP)ซึ่งทั้งสองนี้จำเป็นต้องมีเพื่อเชื่อมต่ออุปกรณ์เข้าด้วยกันและเชื่อมต่อกับเครือข่าย



ภาพ การทำงานของระบบบริหารจัดการ IP Address
ที่มา https://www.bestinternet.co.th/

หน้าที่หลักของ DHCP คือ ทำให้การจัดการและการกำหนดค่า IP Address ทั่วทั้งเครือข่ายเป็นไปโดยอัตโนมัติดังนั้นผู้ดูแลระบบจึงไม่จำเป็นต้องกำหนด IP Address ด้วยตนเองทุกครั้งที่อุปกรณ์จะเชื่อมต่อ เซิร์ฟเวอร์ DHCP ยังรับผิดชอบการกำหนดค่าเซิร์ฟเวอร์โดเมน (DNS) และเน็ตมาสก์เครือข่ายย่อย รวมถึงเกตเวย์เริ่มต้นอีกด้วย

เซิร์ฟเวอร์ DHCP จัดว่าเป็นเครื่องมือการจัดการที่สามารถอธิบายตัวเองได้ค่อนข้างชัดเจน เซิร์ฟเวอร์ที่ใช้ DHCP และอุปกรณ์กำหนดให้เชื่อมต่อกับเครือข่ายด้วย IP Address แบบไดนามิก รวมถึงการกำหนดค่าข้อมูลเครือข่ายอื่นๆ ซึ่งทั้งหมดนี้ มันสามารถจัดการได้โดยที่ผู้ดูแลระบบไอทีไม่ต้องจำเป็นต้องมีส่วนร่วมมากนัก ในธุรกิจขนาดเล็กหรืออุปกรณ์ภายในบ้าน เซิร์ฟเวอร์ DHCP นั้นมีอยู่ในเราเตอร์ได้ ในขณะที่ธุรกิจขนาดใหญ่อาจจะใช้ในรูปแบบคอมพิวเตอร์เครื่องเดียวหรือเซิร์ฟเวอร์เพื่อทำหน้าที่เป็นเซิร์ฟเวอร์ DHCP โดยเฉพาะ

DHCP ทำงานยังไง?

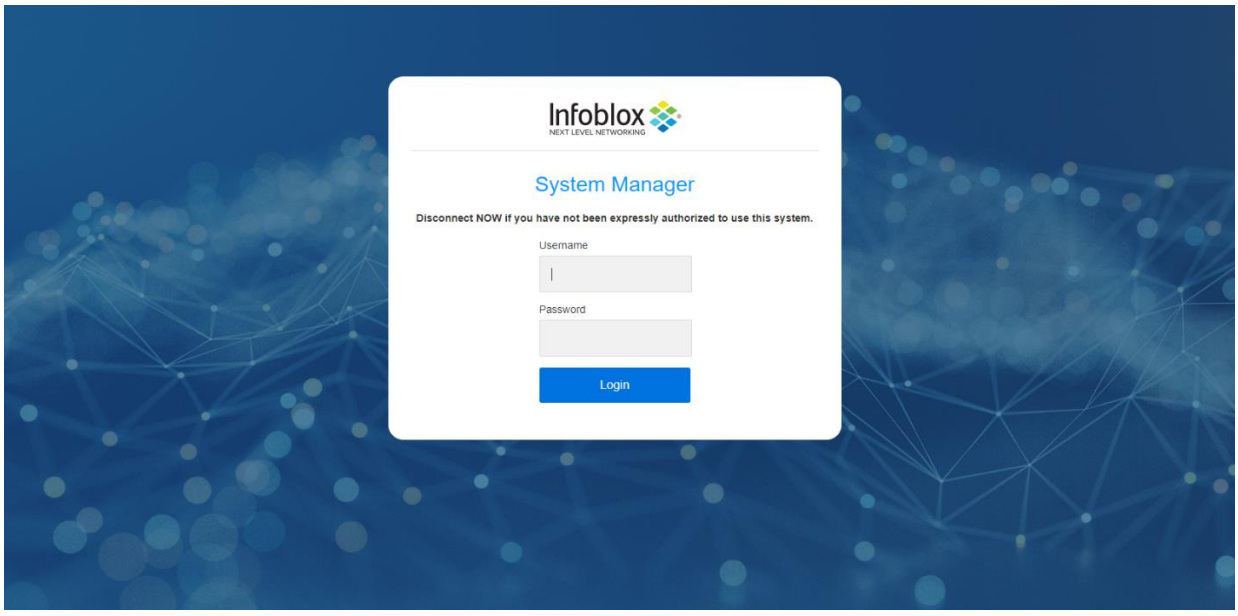
DHCP ทำงานโดยใช้รูปแบบไคลเอนต์ – เซิร์ฟเวอร์ โดยมีเซิร์ฟเวอร์DHCP ทำหน้าที่เป็นโฮสต์ในขณะที่อุปกรณ์ที่เชื่อมต่อกับเครือข่ายเป็นไคลเอนต์ (Client) ทันทีที่ลูกค้าทำการส่งคำขอไปยังเครือข่าย สำหรับที่อยู่ IP โฮสต์จะกำหนด IP Address โดยนำมาจากรายการของตัวเลือกที่มีอยู่ ซึ่งนี่จะทำให้การสื่อสารระหว่างอุปกรณ์และเครือข่ายเกิดขึ้น

ข้อดีหลักของ DHCP

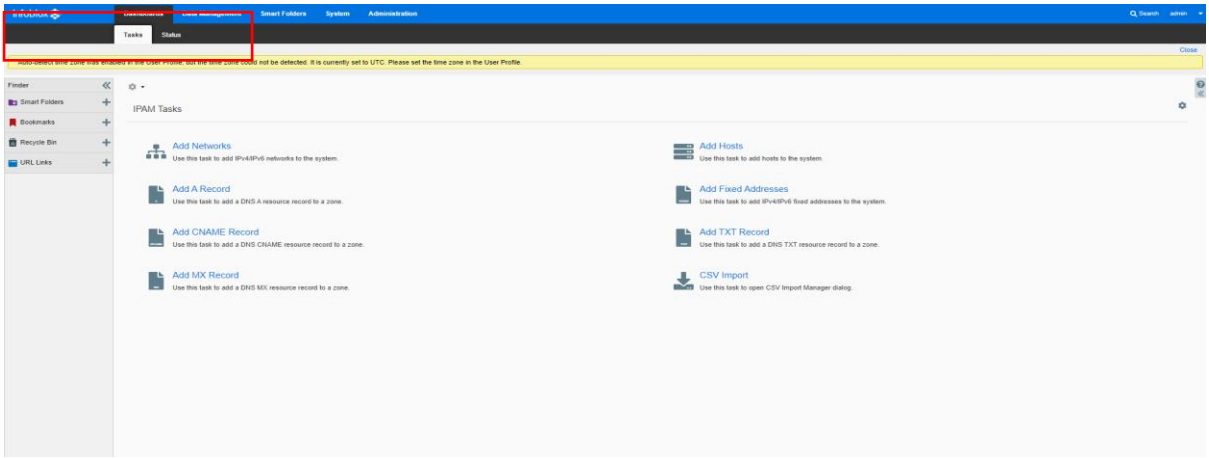
ประโยชน์หลักอย่างหนึ่งของการใช้เซิร์ฟเวอร์ DHCP เมื่อเทียบกับโซลูชั่นของระบบเครือข่ายอื่นๆ คือ การตั้งค่าเครือข่าย TCP/IP ได้เร็วกว่า นอกจากนี้ยังง่ายต่อการจัดการเครือข่าย เนื่องจาก การทำงานที่ไม่ยุ่งยาก เพราะเซิร์ฟเวอร์จะกำหนด IP Address เองโดยอัตโนมัติ ดังนั้นพนักงานไอทีจึงไม่จำเป็นต้องทำด้วยตัวเองพนักงานไอทีจะมีเวลาทำงานและสามารถช่วยเหลืองานด้านอื่นๆ ได้มากกว่า การที่จะต้องมาคอยเสียเวลาจัดการกับระบบเครือข่ายที่ง่ายแต่ช่างสิ้นเปลืองทรัพยากรและเวลา ประโยชน์อีกอย่างหนึ่งของการใช้เครือข่าย DHCP คือการเกิดปัญหาระหว่างอุปกรณ์นั้น เป็นไปได้น้อยมากเนื่องจากเซิร์ฟเวอร์จะกำหนดIP Address แทนมนุษย์จึงมั่นใจได้ว่าอุปกรณ์ทั้งสองเครื่องจะถูกตั้งค่าเหมือนกันอย่างแน่นอน

ขั้นตอนการเพิ่ม DNS ด้วย Infoblox

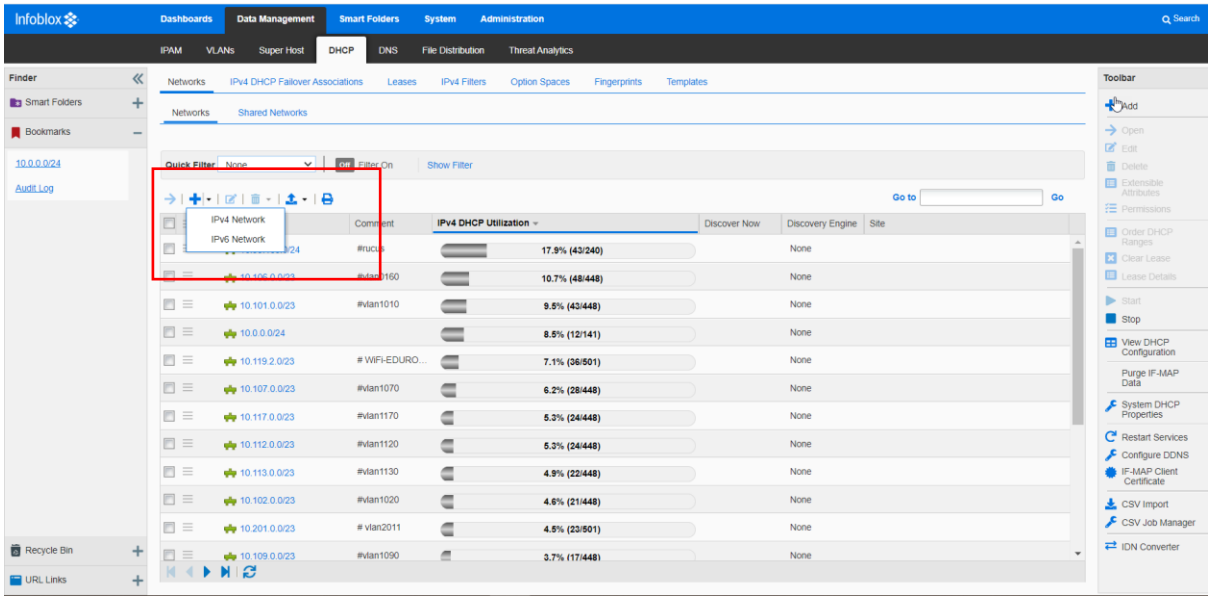
1. ล็อคอินเข้าระบบบริหารจัดการ Infoblox



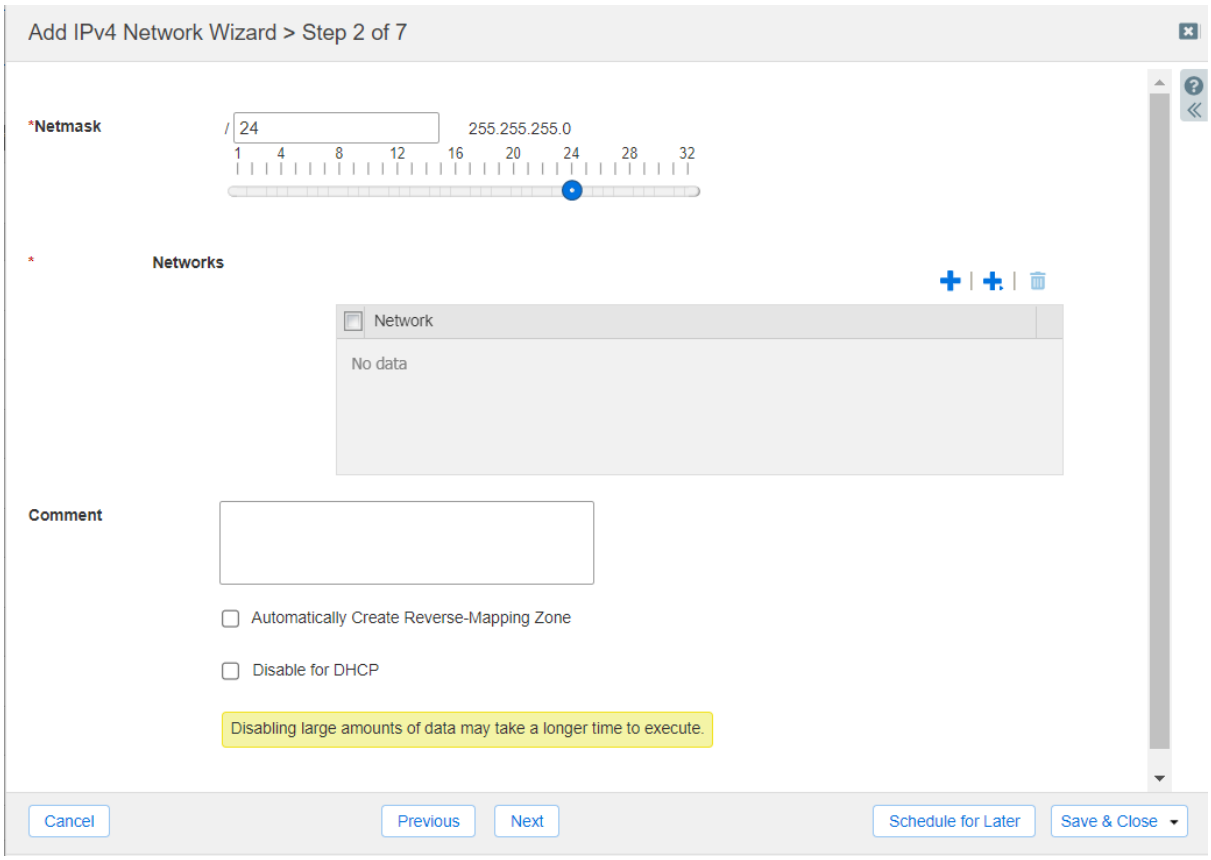
2. เมื่อล็อคอินเข้าสู่ระบบจะปรากฏหน้าต่างดังรูป



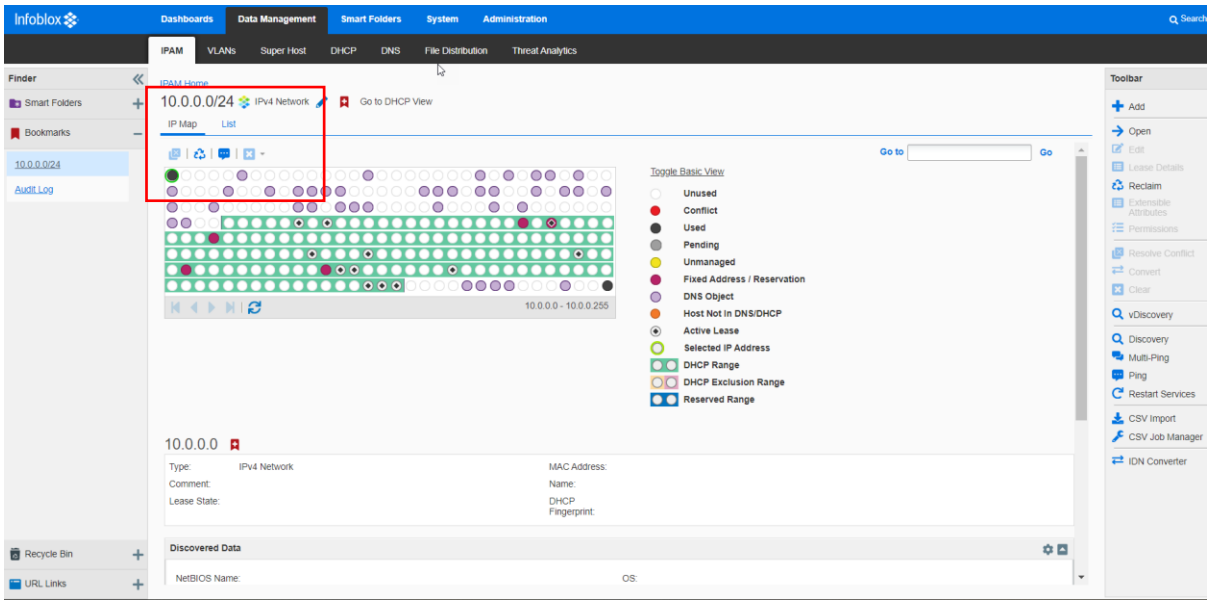
3. เลือกติดตั้ง DHCP Service โดยไปเมนู Disk Management -> DHCP -> + และ เมนู IP v4 Network จะได้ภาพ ด้านล่าง



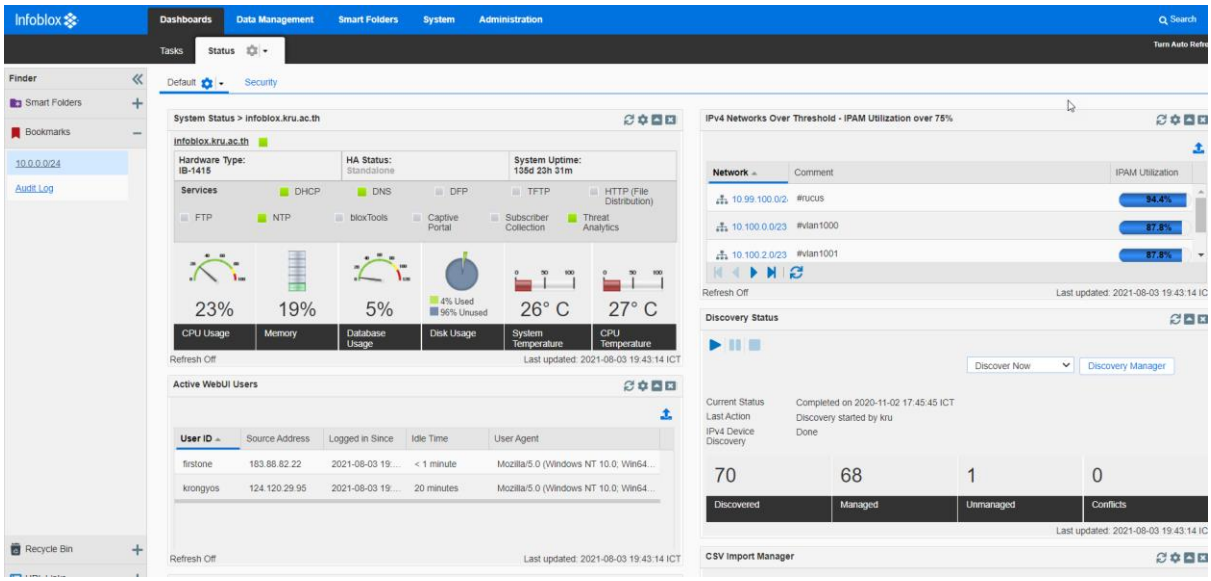
4. กำหนด IP Address ที่ต้องการ แล้วเลือก Save



5. เมื่อมีการแจก IP Address ในระบบ DHCP ที่กำหนดแล้ว สามารถตรวจดู IP Address ที่แจกได้ โดยไปยัง เมนู Disk Management -> IPAM -> เลือก Subnet ที่ต้องการ



6. หากต้องการตรวจดู (Resource Monitor) สามารถ ไปยังเมนู Dashboard -> Status จะได้ภาพ ตามด้านล่าง

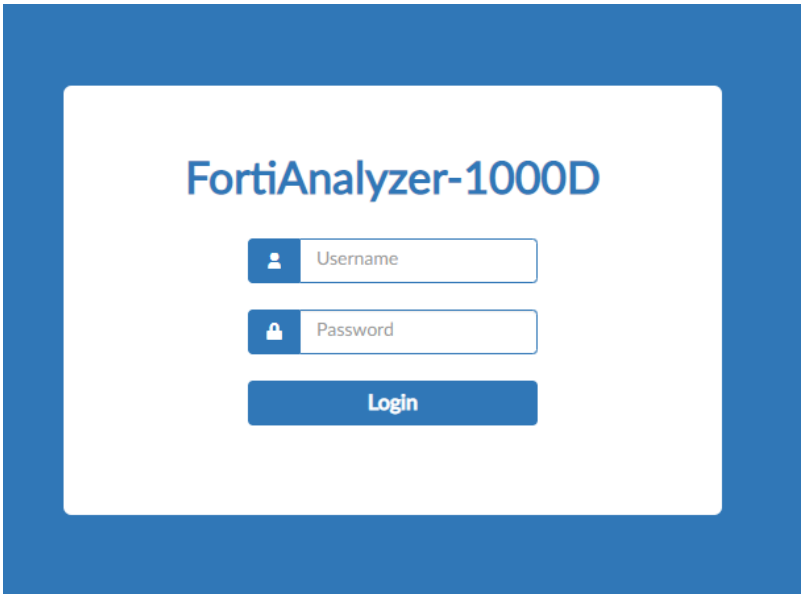


คู่มือการรายผลการใช้งานระบบเครือข่าย
Forti Analyzer-1000D

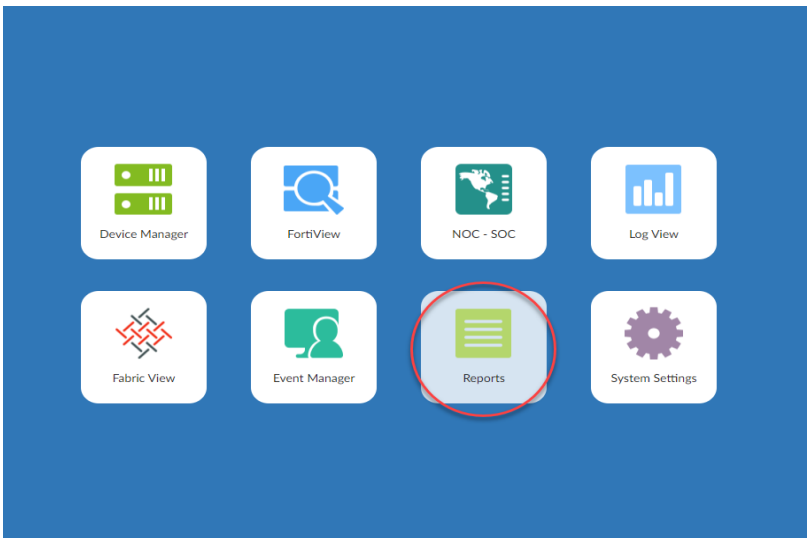
Forti Analyzer Centralized log & analysis appliance เป็นระบบจัดเก็บ Log แบบศูนย์กลาง ทำให้เห็นภัยคุกคามต่างๆ ได้อย่างทันที่ รวมถึงแจ้งเตือนละวิเคราะห์ ทำให้ผู้ใช้งานสามารถมองเห็นต้นต่อของภัยคุกคามที่เข้ามาในระบบ และทำสำคัญคือการเก็บรักษา Log File จาก FortiGate ตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 รวมถึงล่าสุด ฉบับแก้ไข พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มีขั้นตอนการดังนี้

ขั้นตอนการใช้งานระบบ Forti Analyzer-1000D

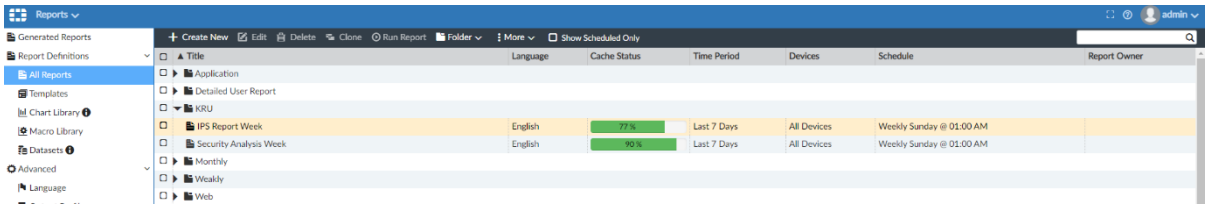
1. ล็อคอินเข้าระบบ FortiAnalyzer-1000D



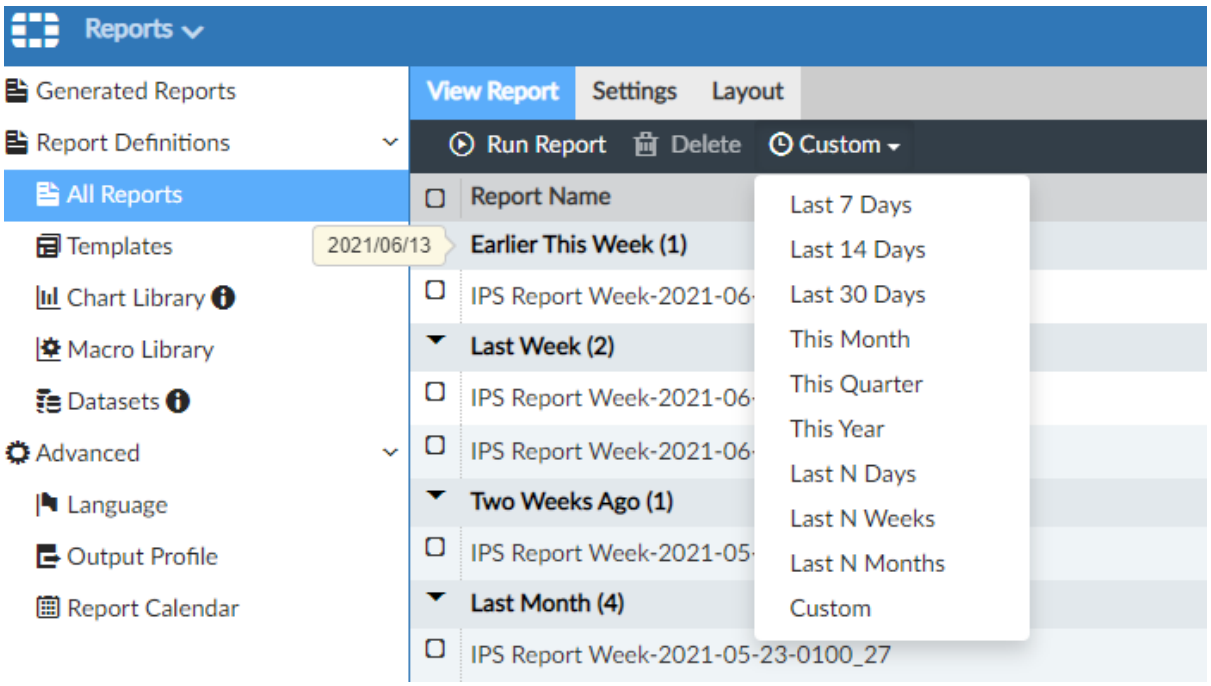
2. เลือก Report ตามภาพ



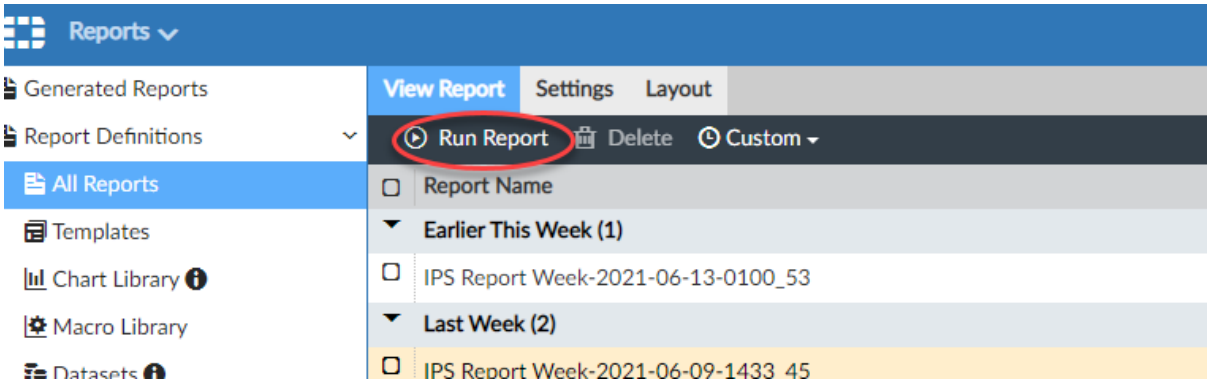
3. เลือก IPS Report Week ตามภาพ



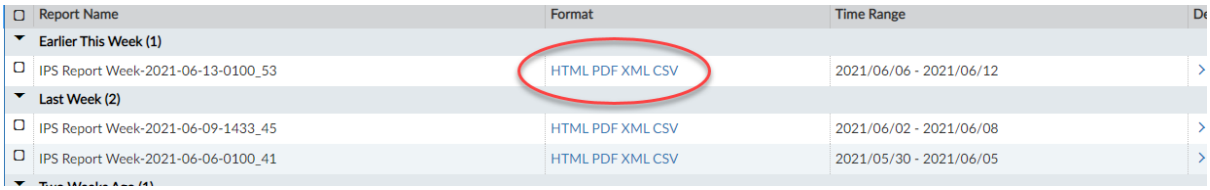
4. เลือก Custom ตามภาพ เพื่อกำหนดช่วงเวลาที่ต้องการดู Report



5. เลือก Run Report ตามภาพ เพื่อสร้าง Report

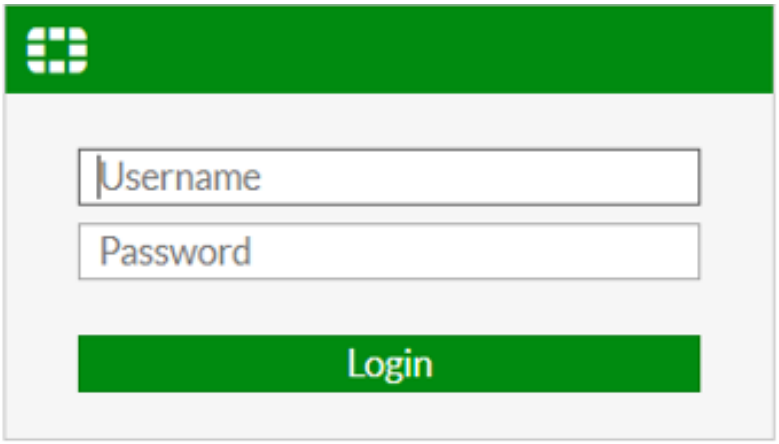


6. เลือกนามสกุลไฟล์ Report ที่เราต้องการ เป็นอันเสร็จสิ้นการดึง Report

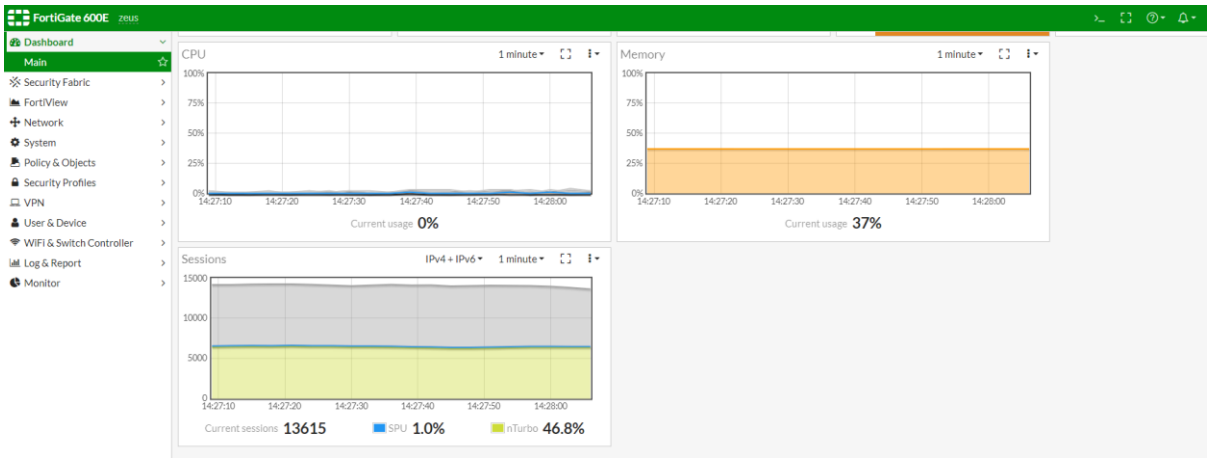


ขั้นตอนการ Map Ip address และตั้งค่า Policy ด้วย Firewall FortiGate 600E

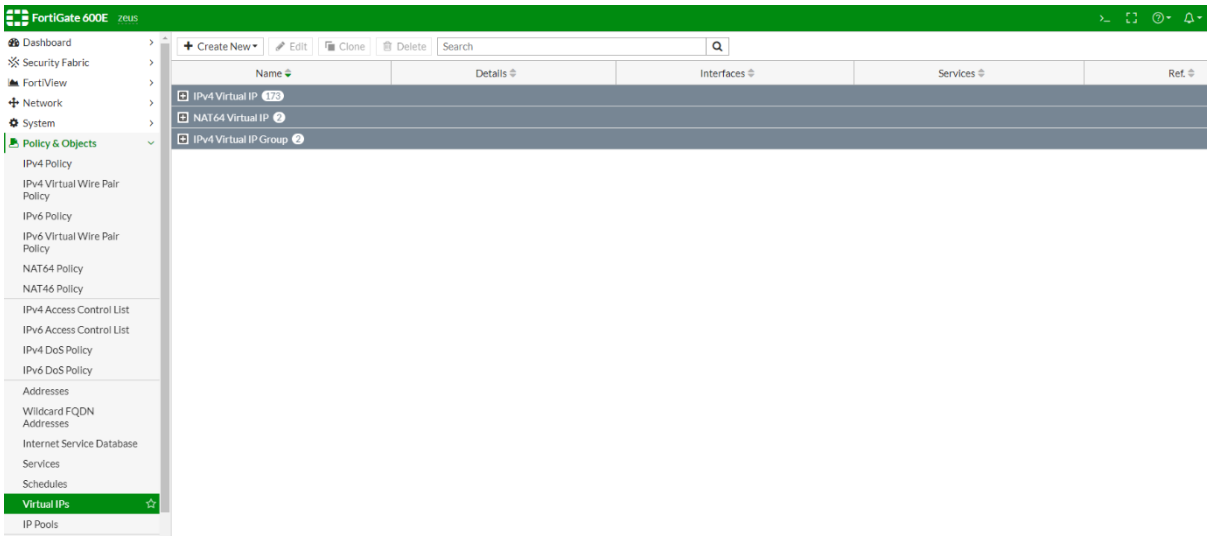
1. ล็อคอินเข้าระบบบริหารจัดการ Firewall FortiGate 600E



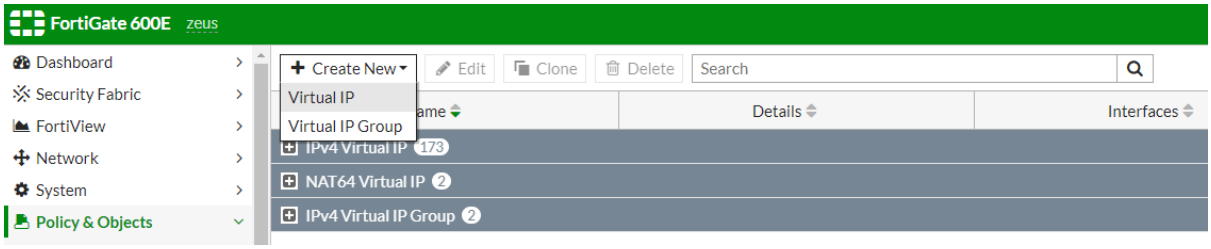
2. ล็อคอินเสร็จแล้วจะปรากฏหน้าต่างดังภาพ



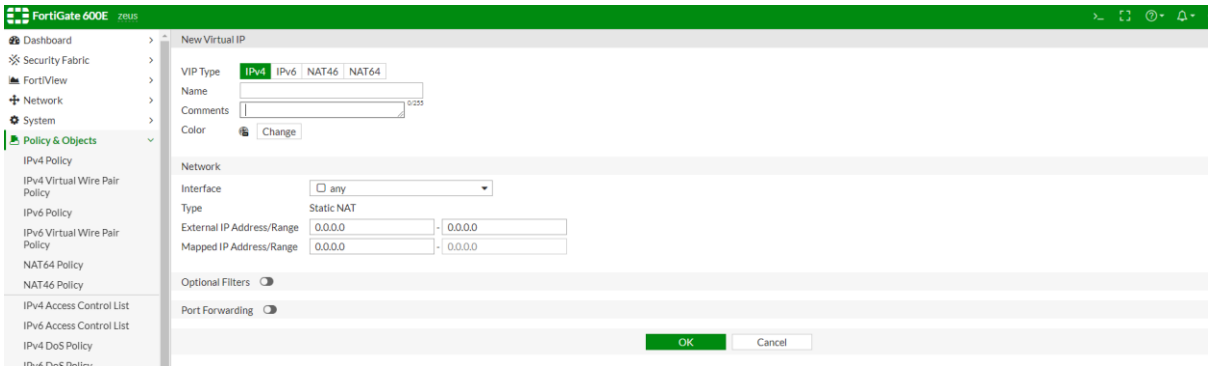
3. แท็บเมนูด้านซ้ายเลือก Policy & Objects > Virtual IPs



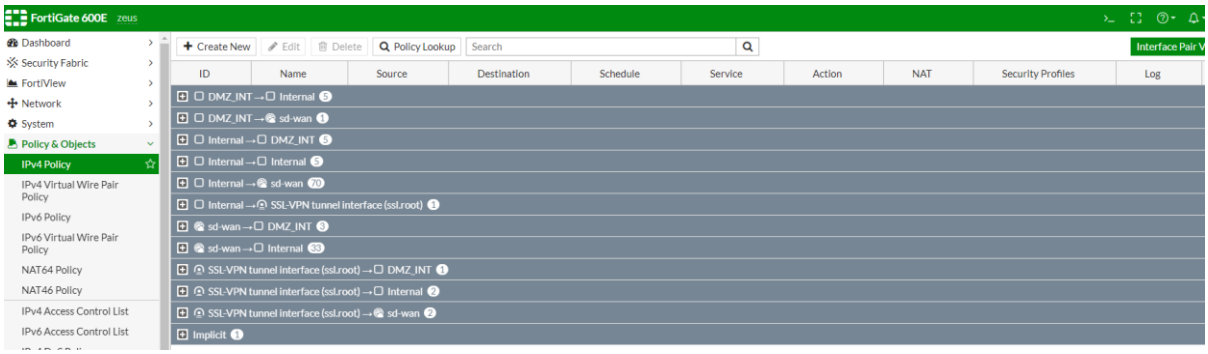
4. เลือก Create New > Virtual IP ตามภาพ



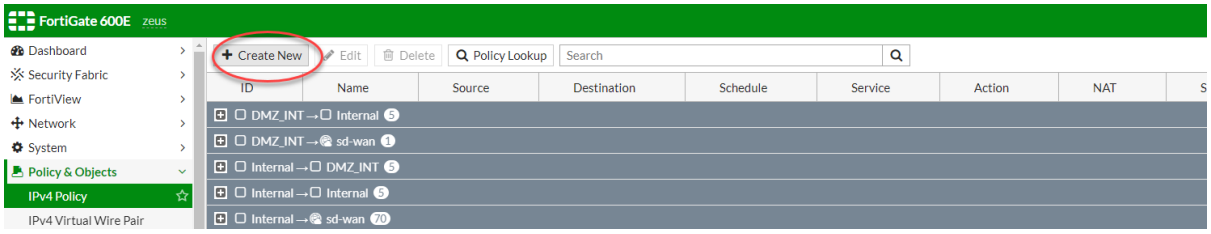
5. จะปรากฏหน้าต่างดังภาพ จากนั้นให้ใส่ชื่อ กำหนด interface และใส่ Ip ขานอก ขาใน เรียบร้อยกด OK เพื่อเสร็จสิ้น การ Map IP Address



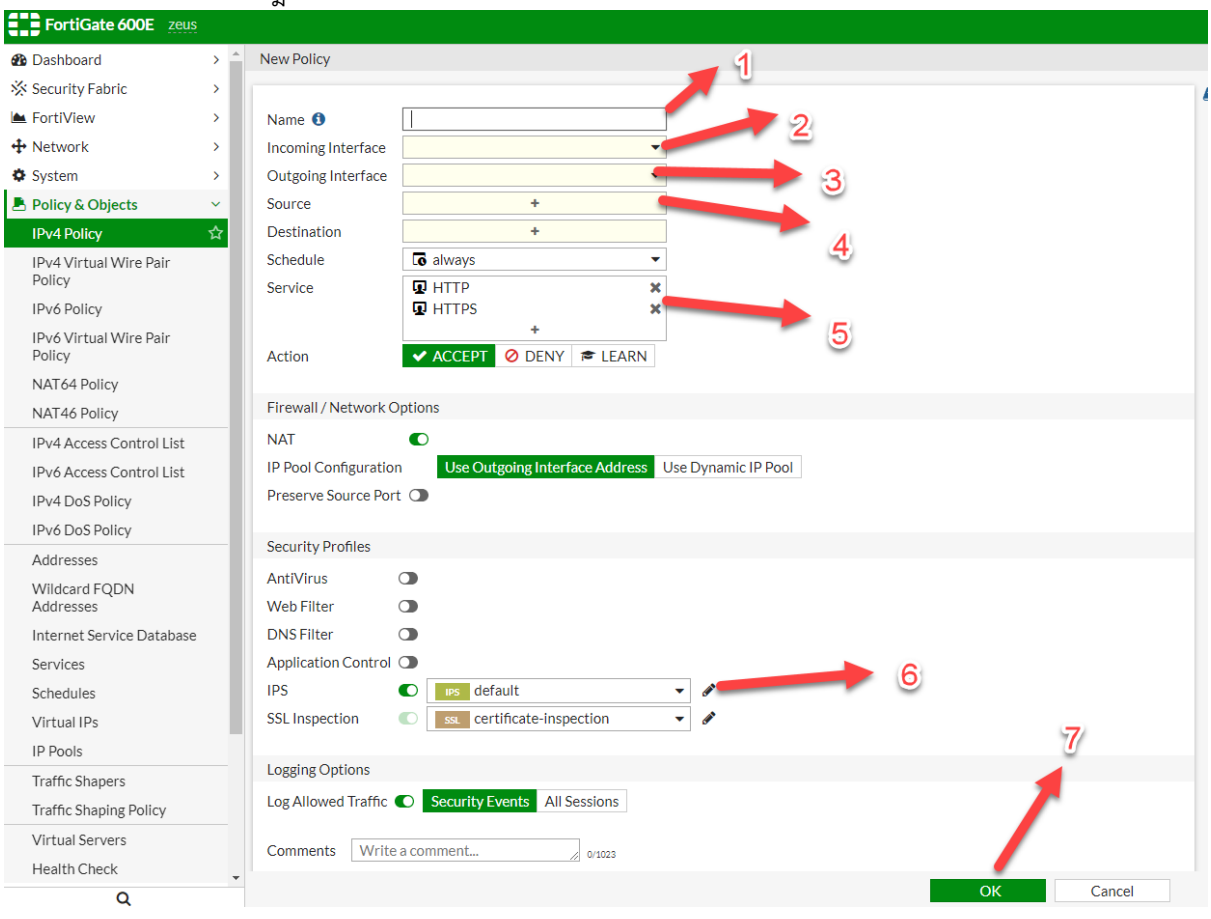
6. เลือก Ipv4 Policy เพื่อตั้งค่า Policy



7. เลือก Create New เพื่อสร้าง Policy



8. จะประกฏหน้าต่างดังภาพ



ช่องที่ 1 ใส่ชื่อ Policy แล้วแต่เราจะกำหนด

ช่องที่ 2 ใส่ Interface ขานอก

ช่องที่ 3 ใส่ Interface ขาใน

ช่องที่ 4 เลือกชื่อที่เราได้ Map IP Address นำมาใส่ในช่องนี้

ช่องที่ 5 กำหนด Service ที่เราต้องการ ตามภาพคือการเปิดใช้ port 80 และ port 443

ช่องที่ 6 เปิดใช้ระบบ IPS เพื่อช่วยป้องกันการโจมตี เช่น DDOS และยังสามารถเก็บข้อมูลการโจมตีต่าง ๆ ไปยังระบบ FortiAnalyzer-1000D ให้เราสามารถมาตรวจสอบย้อนหลังได้อีกด้วย