ห้องสมุดกรมพัฒนาที่ดิน

ผลงานฉบับเต็ม

เรื่อง

ระบบตัวแทนการให้บริการเว็บไซต์หน่วยงาน สำนักงานพัฒนาที่ดินเขต (Reverse Proxy)

ของ
นายภูวดล แสงทอง
ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ ตำแหน่งเลขที่ ๓๖๐
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน

ขอประเมินเพื่อแต่งตั้งให้ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ชำนาญการ
ตำแหน่งเลขที่ ๓๖๐
สังกัด กลุ่มระบบเครือข่ายและคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

ห้องสมุดกรมพัฒนาที่ดิน

ห้องสมุดกรมพัฒนาที่ดิน
วันที่ 13 พ.ย. 2561
เลขหมู่ ๐๐๕.๘
๒๖๘๕๕
เลขทะเบียน b100577

ผลงานฉบับเต็ม

เรื่อง

ระบบตัวแทนการให้บริการเว็บไซต์หน่วยงาน สำนักงานพัฒนาที่ดินเขต (Reverse Proxy)

ของ
นายภูวดล แสงทอง
ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ ตำแหน่งเลขที่ ๓๖๐
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน

ขอประเมินเพื่อแต่งตั้งให้ดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ชำนาญการ
ตำแหน่งเลขที่ ๓๖๐
สังกัด กลุ่มระบบเครือข่ายและคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

คำนำ

ในปัจจุบัน หน่วยงานภาครัฐมีการนำเทคโนโลยีดิจิตอลเข้ามาเสริมศักยภาพการทำงานของบุคลากร เพิ่มประสิทธิภาพการดำเนินงานและยกระดับการให้บริการประชาชนเป็นหลัก เว็บไซต์ถือเป็นสื่ออิเล็กทรอนิกส์ที่สำคัญในการเข้าถึงการให้บริการของภาครัฐ ทำให้ประชาชนได้รับความสะดวกรวดเร็วในการใช้บริการที่ทั่วถึงและเท่าเทียมกัน โดยมีศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งถือเป็นศูนย์กลางการจัดการด้านเทคโนโลยีสารสนเทศ รับผิดชอบในการดูแล และจัดการเว็บไซต์หน่วยงานภายในกรมพัฒนาที่ดินทั้งหมดในส่วนกลางและส่วนภูมิภาค ส่งเสริมและสนับสนุนให้ทุกหน่วยงานปรับปรุงข้อมูลข่าวสาร องค์ความรู้ ผลงานวิชาการ บริการ e-Service ต่าง ๆ ภายในเว็บไซต์ของหน่วยงานต่าง ๆ ให้มีข้อมูลที่เป็นประโยชน์และเป็นปัจจุบัน

ระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต (Reverse Proxy) พัฒนาขึ้นโดยทำหน้าที่ให้บริการต่าง ๆ แทนเครื่องแม่ข่ายเว็บไซต์ส่วนภูมิภาคจริง ซึ่งจะทำให้ลดปริมาณของการส่งผ่านข้อมูลภายในเครือข่าย ทำให้เครื่องแม่ข่ายเว็บไซต์ไม่ต้องทำงานหนัก และยังเป็นเครื่องมือเพื่อลดช่องโหว่ของเว็บไซต์ เพื่อป้องกันการโจมตีของเว็บไซต์ได้

ผู้จัดทำ จึงได้รวบรวมข้อมูล หลักการวิเคราะห์ การออกแบบ กระบวนการพัฒนา และการบริหารจัดการเว็บเซิร์ฟเวอร์ ขึ้นเพื่อใช้เป็นเอกสารอ้างอิงสำหรับข้าราชการและเจ้าหน้าที่ รวมทั้งผู้ที่มีความสนใจในการพัฒนาระบบตัวแทนการให้บริการเว็บไซต์ สามารถนำไปใช้ต่อยอดเพื่อใช้ในการบริการเว็บไซต์ มีประสิทธิภาพ ต่อไป

ภูวดล แสงทอง
กุมภาพันธ์ ๒๕๖๑

ห้องสมุดกรมพัฒนาที่ดิน

สารบัญ

ห้องสมุดกรมพัฒนาที่ดิน

สารบัญ (ต่อ)

ห้องสมุดกรมพัฒนาที่ดิน

สารบัญภาพ

หน้า

สารบัญภาพ (ต่อ)

หน้า

สารบัญภาพ (ต่อ)

หน้า

บทที่ ๑
บทนำ

๑.๑ ชื่อผลงาน ระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต (Reverse Proxy)

๑.๒ บทนำ / ความสำคัญของปัญหา

ในปัจจุบัน หน่วยงานภาครัฐมีการนำเทคโนโลยีดิจิตอลเข้าไปเสริมศักยภาพการทำงานของบุคลากร โดยการประยุกต์ใช้ไอซีที เพื่อเพิ่มประสิทธิภาพการดำเนินงานภาครัฐและยกระดับการให้บริการประชาชนเป็นหลัก เว็บไซต์ถือเป็นสื่ออิเล็กทรอนิกส์ที่สำคัญในการเข้าถึงการให้บริการของภาครัฐ ทำให้ประชาชนได้รับความสะดวกรวดเร็วในการใช้บริการที่ทั่วถึงและเท่าเทียมกัน กรมพัฒนาที่ดินจึงส่งเสริมและสนับสนุนให้ทุกหน่วยงานจัดทำเว็บไซต์ขึ้น เพื่อให้บริการข้อมูล การให้บริการวิชาการเป็นทั้ง MIS GIS ข่าวประชาสัมพันธ์ กิจกรรมงานของหน่วยงานสู่ประชาชนทั่วไป

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) ซึ่งถือเป็นศูนย์กลางการจัดการด้านเทคโนโลยีสารสนเทศ รับผิดชอบในการดูแล และจัดการเว็บไซต์หน่วยงานภายในกรมพัฒนาที่ดินทั้งหมดในส่วนกลางและส่วนภูมิภาค ส่งเสริมและสนับสนุนให้ทุกหน่วยงานปรับปรุงข้อมูลข่าวสาร องค์ความรู้ ผลงานวิชาการ บริการ e-Service ต่าง ๆ ภายในเว็บไซต์ของหน่วยงานให้มีข้อมูลที่เป็นประโยชน์และเป็นปัจจุบัน พร้อมเผยแพร่ออกสู่เกษตรกรและสาธารณชน เพื่อให้เจ้าหน้าที่ เกษตรกร และผู้รับบริการ สามารถเข้าถึงข้อมูลข่าวสารจากเว็บไซต์ได้อย่างสะดวกและรวดเร็ว จากอุปกรณ์ต่าง ๆ ที่ต่อกับอินเทอร์เน็ตได้ทุกที่ทุกเวลา เป็นการยกระดับในการพัฒนา และการดำเนินงานรัฐบาลอิเล็กทรอนิกส์ให้บรรลุเป้าหมายของกรมพัฒนาที่ดิน

เว็บไซต์หน่วยงานในส่วนภูมิภาคส่วนใหญ่เป็นข้อมูลในรูปแบบคงที่ (Data Static) แสดงผลอย่างเดียวโดยไม่มีการโต้ตอบระหว่างผู้ใช้งานกับเว็บไซต์ เช่น ข้อมูลเอกสารเผยแพร่ ข้อมูลแสดงผลรูปภาพ เมื่อผู้ใช้งานเรียกดูข้อมูลบนเว็บไซต์ส่วนภูมิภาคผ่านระบบอินเทอร์เน็ต ระบบจะส่งข้อมูลคำขอแพ็กเกต (Packet) มายังไฟร์วอลล์ (Firewall) ส่วนกลาง (ตั้งอยู่ ณ ห้องควบคุมระบบ Network ศทส.) เพื่อตรวจสอบแพ็กเกต ตามนโยบายการให้บริการ (Policy) จากนั้น จะส่งแพ็กเกตคำขอไปยังเครื่องแม่ข่ายเว็บไซต์ของหน่วยงานส่วนภูมิภาคเพื่อประมวลผล แล้วจึงส่งแพ็กเกจตอบกลับไปยังผู้สนใจผ่านระบบเครือข่ายอินทราเน็ตของกรมพัฒนาที่ดิน และหากมีการรับ-ส่งแพ็กเกตคำขอที่เหมือนกันในช่วงเวลาเดียวกัน พบว่าเครื่องแม่ข่ายเว็บไซต์ของหน่วยงานส่วนภูมิภาคต้องทำงานหนัก เพราะประมวลผลซ้ำ ๆ ทุกครั้งที่มีการส่งคำขอ

ในขณะเดียวกัน การป้องกันการโจมตี ด้วยการติดตั้งไฟร์วอลล์ระหว่างเครือข่ายภายนอกและเว็บเซิร์ฟเวอร์ เพื่อทำหน้าที่ตรวจสอบความถูกต้องของการรับ-ส่งระหว่างต้นทาง (Source) และปลายทาง (Destination) สามารถป้องกันได้ส่วนหนึ่ง แต่ไม่สามารถป้องกันการโจมตีผ่านช่องโหว่ของชุดคำสั่ง (Source Code) เว็บไซต์ ซึ่งอยู่นอกเหนือการตรวจสอบของไฟร์วอลล์กรองแพ็กเกต (Packet Filtering) จึงทำให้กลุ่มผู้ไม่ประสงค์ดีพยายามเข้าถึงระบบโดยไม่ได้รับอนุญาต รวมถึง ทำให้ระบบหยุดให้บริการด้วยวิธีการต่าง ๆ อันส่งผลต่อภาพลักษณ์ของหน่วยงาน ผู้ไม่ประสงค์ดีอาจมีจุดประสงค์แตกต่างกันไปตามเวลา และสถานการณ์ เช่น เพื่อข่มขู่เรียกค่าไถ่ หรือเพื่อแอบซ่อนช่องการโจมตีที่แท้จริง และใช้เว็บไซต์ของเราเป็นฐานในการโจมตีเว็บไซต์อื่น ๆ ซึ่งแนวโน้มภัยคุกคามผ่านช่องทางอินเทอร์เน็ตมีเพิ่มขึ้นอย่างต่อเนื่องทุกปี

ด้วยเหตุผลนี้ จึงได้พัฒนาระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต (Reverse Proxy) ขึ้น เพื่อจำลองเครื่องคอมพิวเตอร์ที่ทำหน้าที่ให้บริการต่าง ๆ แทนเครื่องแม่ข่ายเว็บไซต์จริงที่ตั้งอยู่ในอินเทอร์เน็ต ซึ่งทำหน้าที่สำหรับเก็บข้อมูลเว็บไซต์ที่ผู้ใช้บริการได้เรียกข้อมูลมาจากอินเทอร์เน็ต โดยผ่านทาง Web Browser ทำให้ผู้ใช้บริการรายต่อไปที่ต้องการค้นหาข้อมูลเดิมซ้ำกับที่มีผู้อื่นเรียกใช้บริการไว้สามารถที่จะเรียกดูข้อมูลจาก Reverse Proxy ได้โดยตรง ไม่ต้องค้นหาข้อมูลจากแม่ข่ายเว็บไซต์จริงอีก ซึ่งจะทำให้ลดปริมาณของการส่งผ่านข้อมูลโดยตรง (data-stream) ลงไป ทำให้เครื่องแม่ข่ายเว็บไซต์ไม่ต้องทำงานหนัก และ Reverse Proxy ยังสามารถปรับปรุงชุดคำสั่งให้กับเครื่องแม่ข่ายเว็บไซต์ เพื่อลดช่องโหว่ของเว็บไซต์ เป็นเครื่องมือเบื้องต้นใช้ในการป้องกันการโจมตีของเว็บไซต์ได้

๑.๓ วัตถุประสงค์

๑.๓.๑ เพื่อลดช่วงเวลาในการรับ-ส่งข้อมูล (Load) เว็บไซต์มาแสดงผล ของเครื่องแม่ข่ายเว็บไซต์ผ่านระบบเครือข่ายอินทราเน็ต เพิ่มประสิทธิภาพในการให้บริการเว็บไซต์หน่วยงานพัฒนาที่ดิน

๑.๓.๒ เพื่อเป็นเครื่องมือที่ใช้ในจัดการป้องกันการโจมตีจากผู้บุกรุกภายนอกเครือข่ายกรมพัฒนาที่ดิน ได้ทันท่วงทีเมื่อได้รับการแจ้งเตือนภัยทางอินเทอร์เน็ต เหตุการณ์การโจมตี และป้องกันความเสี่ยง ไม่ให้มีผลกระทบต่อการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต สำหรับผู้ใช้งานเครือข่ายภายในกรมพัฒนาที่ดิน

๑.๔ ขอบเขตการศึกษา

๑.๔.๑ ศึกษาระบบปฏิบัติการ (Operation System) CentOS เพื่อให้ทราบความต้องการของระบบ ขั้นตอนการติดตั้ง การกำหนดค่าระบบปฏิบัติการให้สามารถเชื่อมต่อและใช้งานร่วมกับระบบเครือข่ายภายในของกรมพัฒนาที่ดิน การติดตั้งการกำหนดค่าโปรแกรมพื้นฐานที่จำเป็นของระบบ การตรวจสอบปรับปรุงเวอร์ชั่นระบบปฏิบัติการ เพื่อให้สามารถใช้งานได้เต็มประสิทธิภาพ

๑.๔.๒ ศึกษาโปรแกรมอรรถประโยชน์ (Utility Software)เอนจิ้นเอ็ก (Nginx) เพื่อนำมาใช้ทำงานร่วมกับระบบทั้งหมดได้อย่างเหมาะสมและมีความเข้ากัน โดยพิจารณาทั้งในด้านการทำงานร่วมกับระบบปฏิบัติการและโปรแกรมอื่น ๆ ที่เกี่ยวข้อง เรียงลำดับขั้นตอนการติดตั้งโปรแกรม การกำหนดค่า (configuration) โปรแกรม ให้สามารถใช้งานร่วมกับระบบเครือข่ายของกรมพัฒนาที่ดิน พร้อมทั้งศึกษาข้อจำกัดของโปรแกรม เพื่อให้สามารถพัฒนาระบบได้มีประสิทธิภาพ

๑.๔.๓ ศึกษาการจัดการเครื่องแม่ข่ายเสมือน (Virtualization) เพื่อให้ทราบขั้นตอนวิธีการติดตั้ง การเข้าถึง การจัดการควบคุม และการกำหนดค่าให้สามารถเชื่อมต่อระบบเครือข่ายของ กรมพัฒนาที่ดิน เพื่อสามารถติดตั้งระบบปฏิบัติการที่พัฒนาระบบให้มีประสิทธิภาพได้

๑.๔.๔ ศึกษาการจัดการระบบพร็อกซี่ ให้ทราบถึงหลักการทำงานของระบบ เพื่อสามารถออกแบบและการวิเคราะห์ระบบให้มีประสิทธิภาพได้

๑.๔.๕ ศึกษาการจัดการไฟร์วอลล์ ให้ทราบวิธีการบริหารจัดการอุปกรณ์ เพื่อปรับปรุงการกำหนดค่า(configuration) ให้มีประสิทธิภาพได้

๑.๔.๖ ศึกษาการจัดการช่องโหว่ของเว็บไซต์ที่สามารถนำมาปรับปรุงชุดคำสั่งโปรแกรมเพื่อปิดกันช่องโหว่ได้

๑.๔.๗ ศึกษา วิเคราะห์ และออกแบบระบบเครือข่ายของกรมพัฒนาที่ดิน เพื่อให้รองรับกับการเชื่อมโยงของระบบ

๑.๔.๘ ศึกษา วิเคราะห์รูปแบบ และข้อมูลของเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต

๑.๕ ความรู้ทางวิชาการหรือแนวคิดที่ใช้ในการดำเนินการ

๑.๕.๑ ความรู้ด้านบริหารจัดการระบบปฏิบัติการ (Operation System) Community Enterprise Operating System (CentOS)

๑.๕.๒ ความรู้ด้านบริหารจัดการโปรแกรมอรรถประโยชน์ (Utility Software) Nginx

๑.๕.๓ ความรู้ด้านบริหารเครื่องแม่ข่ายเสมือน (Virtualization)

๑.๕.๔ ความรู้ด้านการจัดการพร็อกซี่ (Proxy)

๑.๕.๕ ความรู้ด้านบริหารจัดการอุปกรณ์ ไฟร์วอลล์

๑.๕.๖ ความรู้ด้านภัยคุกคาม การโจมตี และช่องโหว่ของเว็บไซต์

๑.๕.๗ ความรู้ด้านบริหารจัดการระบบเครือข่ายของกรมพัฒนาที่ดิน

๑.๕.๘ ความรู้เกี่ยวกับข้อมูลของเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต

๑.๖ สรุปสาระและขั้นตอนการดำเนินการ

พัฒนาระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต (Reverse Proxy) ขึ้นเพื่อจำลองเครื่องคอมพิวเตอร์ทำหน้าที่ให้บริการต่าง ๆ แทนเครื่องแม่ข่ายเว็บไซต์จริง ที่ตั้งอยู่ในอินเทอร์เน็ต ซึ่งทำหน้าที่สำหรับเก็บข้อมูลที่ผู้ใช้บริการได้เรียกข้อมูลมาจากอินเทอร์เน็ต โดยผ่านทาง web browser ทำให้ผู้ใช้บริการรายต่อไปที่ต้องการค้นหาข้อมูลเดิมซ้ำกับที่มีผู้อื่นเรียกใช้บริการไว้ สามารถที่จะเรียกดูข้อมูลจาก Reverse Proxy ได้โดยตรง ไม่ต้องค้นหาข้อมูลจากแม่ข่ายเว็บไซต์จริงอีก ซึ่งจะทำให้ลดระยะเวลาของการส่งผ่านข้อมูลโดยตรง (data-stream) ลงไป ทำให้เครื่องแม่ข่ายเว็บไซต์ไม่ต้องทำงานหนัก และ Reverse Proxy ยังสามารถปรับปรุงชุดคำสั่งให้กับเครื่องแม่ข่ายเว็บไซต์ เพื่อลดช่องโหว่ของเว็บไซต์ เป็นเครื่องมือเบื้องต้นใช้ในการป้องกันการโจมตีของเว็บไซต์ได้

ขั้นตอนการดำเนินการ

๑.๖.๑ วางแผนออกแบบระบบเครือข่าย จัดเตรียมโปรแกรม (Software) เพื่อทำระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต พร้อมกำหนดคุณลักษณะของโปรแกรม รวมทั้งรวบรวมข้อมูล และช่องโหว่ของเว็บไซต์หน่วยงาน

๑.๖.๒ ติดตั้งปรับปรุงชุดคำสั่งโปรแกรมที่เกี่ยวข้องกับระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต และปรับปรุงชุดคำสั่งของอุปกรณ์ระบบเครือข่าย

๑.๖.๓ เปิดการใช้งานระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต

๑.๗ ส่วนของงานที่ผู้เสนอเป็นผู้ปฏิบัติ

วิเคราะห์และออกแบบระบบ ประกอบด้วย การศึกษาระบบตัวแทนการให้บริการเว็บไซต์ ระบบคอมพิวเตอร์และเครือข่ายกรมพัฒนาที่ดิน เว็บไซต์หน่วยงานในส่วนภูมิภาคของกรมพัฒนาที่ดิน ติดตั้งระบบปฏิบัติการ โปรแกรมอรรถประโยชน์ ปรับปรุงการกำหนดค่าระบบปฏิบัติการ โปรแกรมอรรถประโยชน์อุปกรณ์ระบบเครือข่าย ให้สามารถรองรับการทำงานของระบบ ให้ระบบสามารถทำงานได้เต็มประสิทธิภาพสัดส่วน ๑๐๐%

๑.๘ ระยะเวลาและสถานที่ดำเนินการ

ระยะเวลา : ระหว่างเดือน มกราคม ๒๕๖๐ - สิงหาคม ๒๕๖๐

สถานที่ดำเนินการ : ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน

๑.๙ ผู้ดำเนินการ

ชื่อ นายภูวดล แสงทอง **ตำแหน่ง** นักวิชาการคอมพิวเตอร์ปฏิบัติการ

มีหน้าที่จัดทำ รวบรวมข้อมูล ศึกษา วิเคราะห์ ออกแบบ พัฒนาระบบ ทดสอบระบบและปรับปรุงระบบให้พร้อมใช้งาน ปฏิบัติงาน ๑๐๐%

๑.๑๐ ผลสำเร็จของงาน (เชิงปริมาณ/คุณภาพ)

เชิงปริมาณ : มีระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต

เชิงคุณภาพ : เพิ่มประสิทธิภาพในการให้บริการเว็บไซต์ ลดช่องโหว่ที่เป็นช่องทางในการโจมตีเว็บไซต์ ลดการทำงานของเครื่องแม่ข่าย และลดจำนวนข้อมูลที่ส่งผ่านในระบบเครือข่าย

๑.๑๑ การนำไปใช้ประโยชน์

นำระบบที่พัฒนาสำเร็จแล้วมาติดตั้ง และเชื่อมต่อระบบเครือข่ายกรมพัฒนาที่ดิน ประชาชนและผู้สนใจเว็บไซต์หน่วยงานในส่วนภูมิภาคสามารถใช้บริการเว็บไซต์ได้มีประสิทธิภาพยิ่งขึ้น และลดช่องโหว่ในการพยายามโจมตีเว็บไซต์ของผู้ไม่ประสงค์ดี

บทที่ ๒
แนวคิดและทฤษฎีที่เกี่ยวข้อง

ในการพัฒนาระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต จำเป็นต้องมีความรู้และทฤษฎีพื้นฐานเพื่อที่จะได้นำมาพัฒนาระบบให้เป็นไปตามความต้องการ ในบทนี้ จะกล่าวถึง วงจรการพัฒนาระบบ และองค์ประกอบพื้นฐานในการจัดทำระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต ซึ่งประกอบด้วย ด้านระบบปฏิบัติการ (Operation System) ด้านโปรแกรมอรรถประโยชน์ ด้านการจัดการเครื่องแม่ข่ายเสมือน (Virtualization) ด้านการจัดการเซอวิสพร็อกซี่ (Proxy) ด้านการจัดการไฟร์วอลล์ (Firewall) ด้านการจัดการเว็บไซต์และช่องโหว่ของเว็บไซต์ ด้านและการจัดการระบบเครือข่าย ที่มีส่วนเกี่ยวข้องในการพัฒนาระบบ

๒.๑ ความหมายของวงจรพัฒนาบริหารงานคุณภาพ PDCA

PDCA คือ วงจรการบริหารงานคุณภาพ ย่อมาจาก ๔ คำ ได้แก่ Plan (วางแผน), Do (ปฏิบัติ), Check (ตรวจสอบ) และ Act (การดำเนินการให้เหมาะสม) ซึ่งวงจร PDCA สามารถประยุกต์ใช้ได้กับทุก ๆ เรื่อง นับตั้งแต่กิจกรรมส่วนตัว เช่น การปรุงอาหาร การเดินทางไปทำงานในแต่ละวัน การตั้งเป้าหมายชีวิต และการดำเนินงานในระดับบริษัท ซึ่งรายละเอียดในแต่ละขั้นตอนมี ดังนี้

๒.๑.๑ P = Plan (ขั้นตอนการวางแผน)

ขั้นตอนการวางแผนครอบคลุมถึงการกำหนดกรอบหัวข้อที่ต้องการปรับปรุงเปลี่ยนแปลง ซึ่งรวมถึงการพัฒนาสิ่งใหม่ ๆ การแก้ปัญหาที่เกิดขึ้นจากการปฏิบัติงาน ฯลฯ พร้อมกับพิจารณาว่ามีความจำเป็นต้องใช้ข้อมูลใดบ้างเพื่อการปรับปรุงเปลี่ยนแปลงนั้น โดยระบุวิธีการเก็บข้อมูลและกำหนดทางเลือกในการปรับปรุงให้ชัดเจน ซึ่งการวางแผนจะช่วยให้กิจการสามารถคาดการณ์สิ่งที่เกิดขึ้นในอนาคต และช่วยลดความสูญเสียต่าง ๆ ที่อาจเกิดขึ้นได้ ทั้งในด้านแรงงาน วัตถุดิบ ชั่วโมงการทำงาน เงิน และเวลา

๒.๑.๒ D = Do (ขั้นตอนการปฏิบัติ)

ขั้นตอนการปฏิบัติ คือ การลงมือปรับปรุงเปลี่ยนแปลงตามทางเลือกที่ได้กำหนดไว้ในขั้นตอนการวางแผน ซึ่งในขั้นตอนนี้ต้องมีการตรวจสอบระหว่างการปฏิบัติด้วยว่าได้ดำเนินไปในทิศทางที่ตั้งใจหรือไม่ เพื่อทำการปรับปรุงเปลี่ยนแปลงให้เป็นไปตามแผนการที่ได้วางไว้

๒.๑.๓ C = Check (ขั้นตอนการตรวจสอบ)

ขั้นตอนการตรวจสอบ คือ การประเมินผลที่ได้รับจากการปรับปรุงเปลี่ยนแปลง เพื่อให้ทราบว่า ในขั้นตอนการปฏิบัติงานสามารถบรรลุเป้าหมายหรือวัตถุประสงค์ที่ได้กำหนดไว้หรือไม่ แต่สิ่งสำคัญก็คือ ต้องรู้ว่าจะตรวจสอบอะไรบ้างและบ่อยครั้งแค่ไหน เพื่อให้ข้อมูลที่ได้จากการตรวจสอบเป็นประโยชน์สำหรับขั้นตอนถัดไป

๒.๑.๔ A = Action (ขั้นตอนการดำเนินงานให้เหมาะสม)

ขั้นตอนการดำเนินงานให้เหมาะสมจะพิจารณาผลที่ได้จากการตรวจสอบ ซึ่งมีอยู่ ๒ กรณี คือ ผลที่เกิดขึ้นเป็นไปตามแผนที่วางไว้ หรือไม่เป็นไปตามแผนที่วางไว้ หากเป็นกรณีแรก ก็ให้นำแนวทางหรือกระบวนการปฏิบัตินั้นมาจัดทำให้เป็นมาตรฐาน พร้อมทั้งหาวิธีการที่จะปรับปรุงให้ดียิ่งขึ้นไปอีก ซึ่งอาจหมายถึง สามารถบรรลุเป้าหมายได้เร็วกว่าเดิม หรือเสียค่าใช้จ่ายน้อยกว่าเดิม หรือทำให้คุณภาพดียิ่งขึ้นก็ได้

แต่ถ้าหากเป็นกรณีที่สอง คือ ผลที่ได้ไม่บรรลุวัตถุประสงค์ตามแผนที่วางไว้ ควรนำข้อมูลที่รวบรวมไว้มาวิเคราะห์และพิจารณาว่าควรจะดำเนินการอย่างไร เช่น มองหาทางเลือกใหม่ที่น่าจะเป็นไปได้ ใช้ความพยายามให้มากขึ้นกว่าเดิม ขอความช่วยเหลือจากผู้รู้ หรือเปลี่ยนเป้าหมายใหม่ เป็นต้น (ความหมายของ PDCA, ๒๕๕๘: ออนไลน์)

ภาพที่ ๒ – ๑ วงจร PDCA (Paul Haining, ๒๕๖๐. Online: ๑)

๒.๒ ระบบปฏิบัติการ (Operation System : OS)

เป็นส่วนหนึ่งของซอฟต์แวร์ระบบมีความสำคัญในการทำงานของคอมพิวเตอร์ โดยจะเริ่มทำงานตั้งแต่บูตเครื่องขึ้นมาหลังจากรอมได้ทำการจัดแจงอุปกรณ์แล้วก็พร้อมที่จะรับคำสั่งจากผู้ใช้งาน เป็นซอฟต์แวร์ที่ใช้ในจัดการระบบก่อนพร้อมใช้งาน ขณะการใช้งาน และหลังจากใช้งานจนเครื่องดับ สามารถจัดแจงการทำงานและควบคุมการทำงานของอุปกรณ์ที่เชื่อมต่อได้ทั้งหมดหากไม่รู้จักอุปกรณ์ชนิดใดก็จะทำการแจ้งเตือนเพื่อหาไดรเวอร์เพื่อรองรับการใช้งานต่อไป นอกจากระบบปฏิบัติการนี้ยังรองรับการใช้งานโปรแกรมชนิดอื่นอย่างเช่นโปรแกรมประยุกต์ต่าง ๆ ด้วย

ดังนั้นระบบปฏิบัติการ คือ ซอฟต์แวร์ชนิดหนึ่งที่ทำหน้าที่ในการควบคุมคอมพิวเตอร์ และพร้อมทำตามคำสั่งของผู้ใช้งาน โดยจะแสดงผลกับอุปกรณ์ชนิดต่าง ๆ ที่ติดตั้งไว้และเชื่อมต่อ

ตัวอย่างระบบปฏิบัติการที่เราใช้งานกันอยู่ อย่างเช่น Windows ๘ windows ๑๐ ซึ่งเป็นระบบปฏิบัติการของ Microsoft จะมี แมคอินทอส ของทาง Apple หรือระบบปฏิบัติการใช้งานแบบฟรีอย่าง linux จากหลายค่ายเพราะมีผู้พัฒนาแยกย่อยมากมาย อย่างเช่น CestOS Ubuntu นอกจากในคอมพิวเตอร์แล้ว ระบบปฏิบัติยังใช้กับอุปกรณ์พกพา เช่น มือถือ แท็บเล็ต อย่าง iOS Android ที่ผู้ใช้มือถือคุ้นเคยกันดี

๒.๒.๑ หน้าที่ของระบบปฏิบัติการ

เริ่มต้นเปิดเครื่องคอมพิวเตอร์จนกระทั่งรอมทำงานตรวจสอบอุปกรณ์ควบคุมภายในต่าง ๆ จากนั้นก็จะส่งต่อให้ระบบปฏิบัติการทำงานโดยจะถูกเก็บไว้ในฮาร์ดดิสก์ โดยจะทำการติดตั้งก่อนหน้าจากทางร้านหรือว่าทางผู้ผลิตหรือเราสามารถที่จะติดตั้งเอง โดยระบบปฏิบัติการสามารถทำหน้าที่ได้ ดังนี้

๒.๒.๑.๑ การจัดการไฟล์ ในเครื่องคอมพิวเตอร์เรามีไฟล์ต่าง ๆ มากมาย ทั้งเกิดจากระบบปฏิบัติการเอง โปรแกรมชนิดอื่น หรือเกิดจากการใช้งานของเราเอง ซึ่งมีไฟล์เป็นจำนวนมากหากไม่จัดจะยากต่อการค้นหา เหมือนหนังสือที่อยู่ตามชั้น หากเก็บไว้อย่างเป็นระเบียบมีการจัดหมวดหมู่ที่ดีก็จะง่ายต่อการขึ้นหากว่ากางไม่มีการจัดระเบียบ โดยไฟล์เองก็จะมีการแบ่งเป็นหมวดหมู่ ไดเรคทรอรี่ จะมีการระบุชื่อไฟล์ไว้ และเมื่อต้องการแฟ้มข้อมูลเหล่านี้ก็จะนำออกมาใช้ได้ จะมีการจัดการเก็บไฟล์แบบลำดับ

๒.๒.๑.๒ การจัดการฮาร์ดแวร์ เมื่อเข้าสู่ระบบแล้ว ระบบปฏิบัติการจะทำการติดต่อสื่อสารกับอุปกรณ์ที่เชื่อมต่อทั้งหมด และจะทำหน้าที่ควบคุม และทำงานเมื่อผู้ใช้งานสั่งระบบปฏิบัติการก็จะส่งให้อุปกรณ์ต่าง ๆ ทำงานติดต่อกับผู้ใช้งาน เมนูหรือว่าสิ่งต่าง ๆ ไว้สำหรับการโต้ตอบต่อผู้ใช้งานในเดสท็อป ในการติดต่อกับผู้ใช้งานสามารถที่จะติดต่อผ่านอักษรด้วยการพิมพ์คำสั่ง อย่างเช่น ระบบ DOS Linux ที่ไม่ได้ทำการติดตั้งโหมดกราฟฟิก หรือการใช้กราฟฟิก อย่าง Windows ในยุคปัจจุบัน

๒.๒.๒ รูปแบบการทำงานของระบบปฏิบัติการ

เนื่องจากระบบปฏิบัติการนั้นสามารถที่จะทำงานได้หลายรูปแบบและความสามารถที่หลากหลาย ดังนี้

๒.๒.๒.๑ Single – User Processing เป็นระบบที่ใช้งานได้เพียงคนเดียวเท่านั้น และใช้งานได้เพียงงานเดียว ต้องให้คนใช้งานเสร็จ และโปรแกรมเสร็จก่อนค่อยให้คนอื่นเข้ามาใช้งานได้ อย่างเช่น ระบบ DOC

๒.๒.๒.๒ Multiuser Processing เป็นระบบปฏิบัติการที่สามารถใช้งานได้หลายคนพร้อมกัน โดยขึ้นอยู่กับอุปกรณ์การใช้งานเป็นหลักอย่างเช่น การเชื่อมต่อผ่านเทอร์มินัล ส่วนมากจะเป็นระบบปฏิบัติการ Linux Unix

๒.๒.๒.๓ Single tasking เป็นระบบปฏิบัติการที่ใช้งานได้ครั้งละ ๑ โปรแกรม หากจะทำงานโปรแกรมอื่นต้องรอให้โปรแกรมปัจจุบันเสร็จเสียก่อน

๒.๒.๒.๔ Multitasking เป็นความสามารถที่สำคัญและมีประโยชน์ในการใช้งานมาก โดยสามารถใช้งานโปรแกรมพร้อมกันได้หลายโปรแกรม จึงทำให้มีความสะดวกในการใช้งานได้หลายงาน โดยไม่ต้องรอให้โปรแกรมเสร็จก่อน โดยใช้หน่วยความจำในการจัดการของแต่ละโปรแกรม อย่างเช่น เปิดเพลงพิมพ์งานไปด้วย โดยระบบปฏิบัติการจะทำงานร่วมกับโปรแกรมเหล่านั้นให้ทำงานอย่างเป็นระบบ ปัจจุบันระบบปฏิบัติการสามารถรองรับการทำงานในรูปแบบ Multitasking หมดแล้ว (ระบบปฏิบัติการ Operating System. ๒๕๕๘: ออนไลน์)

๒.๒.๓ เซนต์โอเอส (CentOS)

CentOS เป็นลีนุกซ์ในระดับ Enterprise ที่มีเป้าหมายหลักในเรื่องของความ stable เพื่อให้ใช้กับงานในระดับองค์กร CentOS แตกต่างจากลีนุกซ์ตัวอื่น ๆ ที่ค่อนข้างจะมีการเปลี่ยนแปลงบ่อย และมักจะใส่ feature ที่ยังไม่ stable ลงไป ดังนั้นการที่ CentOS ให้ความสำคัญในเรื่องของความ stable จึงทำให้ผู้ใช้งานสามารถมุ่งความสนใจในเรื่องของ application โดยลดความกังวลในส่วนของ OS ลงไป

CentOS ย่อมาจาก (Community ENTerprise Operating System) เป็นลีนุกซ์ที่พัฒนามาจากต้นฉบับ RedHat Enterprise Linux (RHEL) โดยที่ CentOS ได้นำเอาซอร์สโค้ดต้นฉบับของ RedHat มาทำการคอมไพล์ใหม่ โดยการพัฒนายังเน้นพัฒนาเป็นซอฟต์แวร์ Open Source โดยเป็นลิขสิทธิ์แบบ GNU General Public License ในปัจจุบัน CentOS Linux ถูกนำมาใช้ในการทำ Web Hosting กันอย่างกว้างขวาง เนื่องจากเป็นระบบปฏิบัติการที่มีต้นแบบจาก RedHat ที่มีความแข็งแกร่งสูง การติดตั้งแพ็กเกจย่อยภายในสามารถใช้ได้ทั้ง RPM, TAR, APT หรือใช้คำสั่ง YUM ในการอัปเดทซอฟต์แวร์แบบอัตโนมัติ

๒.๒.๓.๑ เหตุผลที่ควรเลือกใช้ CentOS สำหรับองค์กรเหมาะสมที่จะนำระบบตัวลีนุกซ์ตัวนี้มาทำเป็น เซิร์ฟเวอร์ใช้งานภายในองค์กร เหตุผลหลักในการนำระบบนี้มาใช้งาน คือ

๑) เพื่อประหยัดงบประมาณขององค์กร เนื่องจาก CentOS เป็นซอฟต์แวร์ Open Source องค์กรไม่จำเป็นต้องจ่ายค่าลิขสิทธ์ซอฟต์แวร์

๒) เพื่อนำมาทำเซิร์ฟเวอร์บริการงานต่าง ๆ ในองค์กร ซึ่งภายใน CentOS มีแพ็กเกจย่อยที่นำมาใช้ทำเซิร์ฟเวอร์สำหรับใช้งานในองค์กรจำนวนมากอาทิ เช่น

- Web Server (Apache)
- FTP Server (ProFTPd / VSFTPd)
- Mail Server (Sendmail / Postfix / Dovecot)
- Database Server (MySQL / PostgreSQL)
- File and Printer Server (Samba)
- Proxy Server (Squid)
- DNS Server (BIND)
- DHCP Server (DHCPd)
- Antivirus Server (ClamAV)
- RADIUS Server (FreeRADIUS)
- Control Panel (ISPConfig)

๓) เพื่อนำมาทำเป็นระบบเซิร์ฟเวอร์สำหรับจ่าย Private IP Address แจกเครื่องลูกข่ายในองค์กร รวมทั้งตั้งเป็นระบบเก็บ Log Files ผู้ใช้งาน เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ปี ๒๕๕๐

๒.๒.๓.๒ ข้อจำกัดของ CentOS

หน่วยความจำขั้นต่ำของเครื่องที่จะติดตั้ง CentOS ๖.๓ ได้นั้น ต้องมีขนาด ๓๑๒ MB สำหรับ Text Mode ส่วนการติดตั้งใน Text Mode จะไม่สามารถแก้ไขพาร์ติชันของดิสก์และเลือกชุดซอฟต์แวร์ได้ต้องเลือกติดตั้งในโหมด GUI เท่านั้น ซึ่งเป็นโหมดดีฟอลต์อยู่แล้วตอนบู๊ตจากแผ่นดีวีดี หน่วยความจำขั้นต่ำต้องใช้เพื่อติดตั้งโหมด GUI คือ ๖๕๒ MB (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), ๒๕๕๕: ออนไลน์)

๒.๓ ด้านโปรแกรมอรรถประโยชน์

โปรแกรมอรรถประโยชน์ (utility program / software) เรียกสั้น ๆ ว่า ยูทิลิตี เป็นโปรแกรมประเภทหนึ่งที่ทำงานบนระบบปฏิบัติการ คุณสมบัติการใช้งานนั้นค่อนข้างหลากหลาย ส่วนมากใช้เพื่อบำรุงรักษาและเพิ่มประสิทธิภาพการทำงานของคอมพิวเตอร์ ช่วยสนับสนุน เพิ่ม หรือขยายขีดความสามารถของโปรแกรมที่ใช้งานให้มีประสิทธิภาพมากขึ้น ยูทิลิตี้แบ่งออกเป็นสองชนิดคือ โปรแกรมอรรถประโยชน์สำหรับระบบปฏิบัติการ (OS utility program) และโปรแกรมอรรถประโยชน์อื่น ๆ (stand-alone utility program) (โปรแกรมอรรถประโยชน์, ออนไลน์)

๒.๓.๑ เว็บเซิร์ฟเวอร์และเอนจิ้นเอ็ก (Nginx)

Nginx มาจากคำว่า Engine-X (เอนจิ้นเอ็ก) เป็น Web Server ที่มีประสิทธิภาพดี และกำลังนิยมอยู่ในปัจจุบัน ถูกคิดค้นขึ้นมาเพื่อให้สามารถที่จะรองรับการทำงานได้มากกว่า Apache นั่นเอง และนอกจากนี้แล้วตัว Nginx ยังมีโมดูลเสริมเข้ามาที่เพียงพอต่อการใช้งานทั่วไป และเป็นซอฟแวร์แบบ Open Source ที่สามารถใช้งานได้ฟรี โดยมีทั้งเวอร์ชั่นที่รองรับทั้งระบบ Linux และระบบ Windows

๒.๓.๒ ความเป็นมาของ Nginx

Nginx พัฒนาโดย อิกอร์ซิสโซอีฟ และเปิดให้ใช้งานในปี ๒๕๔๗ เอ็นจินเอ็กซ์เป็นที่รู้จักในแง่การมีประสิทธิภาพสูง ความมีเสถียรภาพ มีการใช้งานทรัพยากรระบบต่ำ ในตอนแรก Nginx ไม่โด่งดังนัก เนื่องจากผู้พัฒนาไม่เขียนเอกสารที่เป็นภาษาอังกฤษเลย ทำให้ผู้ใช้งานมีอยู่ในวงแคบ คือ แถบ ๆ รัสเซียเท่านั้น ต่อมาเมื่อคนเริ่มรู้จักมากขึ้น ก็มีการแปลเอกสารไว้ให้สามารถดูตัวอย่างได้ แต่ยังไม่เป็นเอกสารอย่างเป็นทางการเท่าไรนัก ต้องอาศัยประสบการณ์บ้างเล็กน้อยในการอ่าน

จุดเด่นของเจ้าตัว Nginx คือ มีประสิทธิภาพมากกว่าเจ้าตัว Apache ด้วยการที่ใช้ทรัพยากรของเครื่องน้อยกว่า เช่น RAM และ CPU ทำให้ Server ทำงานได้มากยิ่งขึ้น แต่เนื่องมาจากว่าการ config ที่ค่อนข้างจะยุ่งยากรวมไปถึงการใช้งานบางอย่างที่ไม่ได้รองรับเหมือนกันกับตัว Apache ทำให้ตัว Nginx ถูกใช้งานเพียงบางอย่าง เช่น การทำเว็บไซต์เกี่ยวกับดาวน์โหลด การทำเว็บไซต์เกี่ยวกับพวก streaming การทำเว็บไซต์อัปโหลด ซึ่งจะมีพื้นที่สามารถรองรับจำนวนของผู้ใช้ได้มากกว่านั่นเอง

๒.๓.๓ การใช้งาน Nginx

การใช้งานจริงจะใช้ผสมข้อดีของ Nginx Web Server กับ Apache Web Server เข้าด้วยกัน คือ ให้ Nginx เป็นตัวรับ Request แล้วส่งไปให้กับ Apache เพื่อประมวลผล PHP และนำผลลัพธ์นั้นมาแสดงให้ ส่วนตัว Nginx นั้น หลัก ๆ แล้วจะนำมาใช้กับพวกไฟล์ Media ต่าง ๆ เช่น รูปภาพ วิดีโอ มากกว่า เนื่องจากการประมวลผลนั้นตัว Nginx ไม่สามารถทำได้โดยตรงต้องเรียกผ่าน fcgi (Fast CGI) อีกทีหนึ่ง (ทำได้เช่นกัน แต่จะ config ยากกว่าส่งให้ Apache ประมวลผล)

ข้อดีของ Nginx

- รองรับมาตรฐานในด้านความปลดภัย HTTP/2
- รับรองการทำงาน HTTP ได้ครบถ้วน
- ไฟล์ที่เป็น static จะประมวลผลได้เร็วกว่า Apache
- ทำงานแบบ Asynchronous โดยไม่มีการหยุดรออะไรทั้งนั้นแยก ๆ กันไปทำงานทันที จึงใช้ทรัพยากรน้อยกว่าทำงานได้เร็วกว่า รองรับจำนวนผู้ใช้งานได้มากกว่า Apache

ข้อเสียของ Nginx

- การ config ที่ค่อนข้างจะยุ่งยากกว่า Apache เนื่องจากการออกแบบที่ค่อนข้างต้องการประสิทธิภาพที่สูงทำให้ต้องตัดการประมวลผลที่เป็นด้วยตัวเองออกไป แล้วไปให้โปรเซสอื่นหรือระบบอื่นจัดการประมวลผลแบบ Dynamic ให้แทน เช่น FastCGI, SCGI, uWSGI, memcache
- การบำรุงรักษายากกว่า Apache เนื่องจาก Nginx ได้มีการออกแบบให้เป็นโมดูลเช่นกันแต่ไม่ได้ยืดหยุ่นมาก ถ้าจะต้องการเพิ่มหรือแก้ไขโมดูลต่าง ๆ จะไม่ค่อยสะดวก
- การเอาไปทำงานได้หลายแพลตฟอร์ม ยังพอร์ตไปไม่ครบนัก ติดตั้งไม่ง่ายนัก การทำงานร่วมกับองค์ประกอบอื่นยังต้องตั้งค่าอีกเยอะ ต่างกับ Apache ที่พอร์ตไปทุกที่ได้ง่ายกว่า (เว็บเซิร์ฟเวอร์และเอนจิ้นเอ็ก, ออนไลน์)

๒.๔ ด้านการจัดการพร็อกซี่ (Proxy)

พร็อกซี่เป็นเครื่องมือในการควบคุมทราฟฟิค (traffic) ชนิดหนึ่ง ซึ่งทำงานที่ระดับของแอพพลิเคชั่นในลักษณะที่เป็นตัวกลางในการสื่อสารระหว่างไคลเอนต์กับเซิร์ฟเวอร์ โดยทำหน้าที่ป้องกันไม่ให้มีการสื่อสารโดยตรงระหว่างไคลเอนต์กับเซิร์ฟเวอร์ แต่ยังคงให้ไคลเอนต์สามารถใช้งานแอพพลิเคชั่นบนเซิร์ฟเวอร์ได้ตามปกติ และผู้ใช้ซึ่งใช้งานแอพพลิเคชั่นนั้น ๆ จะไม่ได้รับผลกระทบแต่อย่างใด

๒.๔.๑ ลักษณะการทำงาน

โดยปกติทั่วไปแล้วการสื่อสารระหว่างไคลเอนต์กับเซิร์ฟเวอร์นั้น จะต้องมีการเชื่อมต่อหรือคอนเน็คชั่น (Connection) เกิดขึ้นระหว่างไคลเอนต์กับเซิร์ฟเวอร์อยู่ตลอดเวลาที่สื่อสารกันอยู่ จุดสำคัญอยู่ตรงที่การที่เชื่อมต่อโดยตรงนั้นจะมีความเสี่ยงหลายประการตามที่ได้กล่าวมาแล้วในข้างต้น จึงมีการนำ Proxy เข้ามาก่อน

หน้าที่ในการทำงานของพร็อกซี่ คือ เป็นตัวกลางรับข้อมูลจากไคลเอนต์มาแล้วทำการส่งต่อไปยังเซิร์ฟเวอร์ และรับข้อมูลที่ตอบกลับจากเซิร์ฟเวอร์กลับมายังไคลเอนต์ที่ทำการร้องขอ และจะทำหน้าที่นี้อยู่ตลอดเวลาที่ไคลเอนต์และเซิร์ฟเวอร์นั้นติดต่อกัน ซึ่งการที่มีพร็อกซี่มาเป็นตัวกลางระหว่างไคลเอนต์กับเซิร์ฟเวอร์นั้น ทำให้โฮสต์ทั้งคู่ไม่จำเป็นต้องติดต่อกันโดยตรง เพียงแค่ติดต่อกับตัวกลางคือพร็อกซี่เท่านั้น และการทำงานของแอพพลิเคชั่นทั้งสองฝั่งยังคงทำได้เช่นเดิม

๒.๔.๒ ขั้นตอนการนำ Proxy เข้ามาใช้งาน

๒.๔.๒.๑ การเริ่มต้นทำงานของแอพพลิเคชั่นโดยทั่วไป เริ่มจากการที่แอพพลิเคชั่นบนไคลเอนต์ขอรับข้อมูลจากเซิร์ฟเวอร์ตามโปรโตคอลในแอพพลิเคชั่นเลเยอร์ที่กำหนดไว้ เช่น เว็บบราวเซอร์กับเว็บเซิร์ฟเวอร์ จะใช้โปรโตคอล HTTP ในการสื่อสารระหว่างกัน

๒.๔.๒.๒ เมื่อเว็บเซิร์ฟเวอร์ได้รับการขอข้อมูลจากบราวเซอร์แล้ว ก็จะตอบรับกลับไปและเริ่มการติดต่อสื่อสารกัน และทั้งฝั่งไคลเอนต์และเซิร์ฟเวอร์ก็จะทำการติดต่อสื่อสารกันตามที่โปรโตคอล HTTP กำหนดจนจบการสื่อสารเซสชั่น (Session) นั้น อย่างไรก็ตามโปรโตคอล HTTP นั้นจะต้องอาศัย TCP ในการรับส่งข้อมูลระหว่างไคลเอนต์กับเซิร์ฟเวอร์ นั่นหมายถึงไคลเอนต์จะต้องสามารถติดต่อกับเซิร์ฟเวอร์ได้ด้วย TCP เสียก่อน เนื่องจาก TCP เป็นโปรโตคอลเลเยอร์ที่อยู่ภายใต้ HTTP อีกเลเยอร์หนึ่ง ดังนั้นในสภาวะการทำงานปกติของ HTTP บราวเซอร์จะต้องสามารถติดต่อกับเซิร์ฟเวอร์โดยตรงเสมอ นั่นคือในสภาวะการทำงานปกตินั้นแพ็คเก็ตของ TCP/IP จะต้องสามารถส่งถึงกันระหว่างโฮสต์ทั้งคู่ได้

๒.๔.๒.๓ เมื่อนำพร็อกซี่มาใช้งานจะต้องติดตั้งตรงจุดที่คั่นกลางระหว่างไคลเอนต์กับเซิร์ฟเวอร์ เพื่อเป็นตัวกลาง โดยที่พร็อกซี่จะต้องมี ๒ อินเตอร์เฟส โดยอินเตอร์เฟสหนึ่งต่ออยู่กับเน็ตเวิร์กของไคลเอนต์และอีกอินเตอร์เฟสหนึ่งต่ออยู่กับเซิร์ฟเวอร์ ซึ่งหากพิจารณาที่พร็อกซี่แล้วจะเห็นว่าสามารถติดต่อได้โดยตรงกับทั้งไคลเอนต์และเซิร์ฟเวอร์ แต่สำหรับไคลเอนต์และเซิร์ฟเวอร์จะติดต่อได้แต่เพียงกับพร็อกซี่เท่านั้น

ในลักษณะที่มีพร็อกซี่มาคั่นกลางระหว่างเน็ตเวิร์กทั้งสองนั้น การสื่อสารระหว่างไคลเอนต์และเซิร์ฟเวอร์ด้วยวิธีการเดิมโดยใช้ HTTP เช่นเดิมเหมือนกับมีการสื่อสารกันโดยตรงนั้นย่อมไม่สามารถจะกระทำได้ เพราะการสื่อสารในเลเยอร์ล่างของ TCP/IP นั้นไม่สามารถทำได้สำเร็จ ดังนั้นจึงจำเป็นต้องมีการปรับปรุงแก้ไขโปรโตคอลให้สามารถรองรับการสื่อสารที่มีตัวกลางมาถ่ายทอดข้อมูลได้ โดยให้ในระดับ TCP/IP นั้นกำหนดให้เพียงโฮสต์แต่ละฝั่งสามารถติดต่อกับพร็อกซี่เท่านั้น ส่วนในระดับ HTTP นั้นพร็อกซี่จะทำการส่งต่อระหว่างทั้งสองฝั่งให้ดูประหนึ่งว่าสามารถติดต่อกันได้โดยตรง ซึ่งจุดสำคัญของพร็อกซี่ก็จะอยู่ตรงนี้เอง อาจจะกล่าวโดยสรุปคือพร็อกซี่จะทำให้โฮสต์ไม่สามารถติดต่อกันได้ โดยโปรโตคอล TCP/IP แต่จะสามารถติดต่อกันได้ด้วยโปรโตคอลในระดับแอพพลิเคชั่นเลเยอร์

อย่างที่กล่าวข้างต้น คือ แอพพลิเคชั่นที่ใช้งานพร็อกซี่นั้นจะต้องมีการแก้ไขในระดับแอพพลิเคชั่นในบางส่วน เพื่อให้สามารถสื่อสารผ่านพร็อกซี่ได้ ดังเช่นเว็บบราวเซอร์ หากจะทำการสื่อสารกันโดยผ่านพร็อกซี่นั้นก็จะต้องทำการปรับแต่งเพื่อให้บราวเซอร์ทราบว่าจะให้ติดต่อกับเว็บไซต์โดยผ่านพร็อกซี่หรือจะติดต่อกับเว็บเซิร์ฟเวอร์โดยตรง จะได้ทำการสื่อสารกันได้ถูกต้องและเมื่อบราวเซอร์ต้องการจะติดต่อไปยังเว็บเซิร์ฟเวอร์ใดก็เพียงแต่ส่งคำขอไปยังพร็อกซี่เท่านั้น หลังจากนั้นก็เป็นภาระของพร็อกซี่ในการไปติดต่อกับเว็บเซิร์ฟเวอร์ตัวจริง แล้วจึงจะนำผลที่ได้จากเว็บเซิร์ฟเวอร์ตอบกลับมายังบราวเซอร์

เมื่อปรับแต่งให้บราวเซอร์ทำการสื่อสารผ่านพร็อกซี่ การทำงานจะมีการเปลี่ยนแปลงไป คือ จากเดิมเมื่อเว็บบราวเซอร์ต้องการติดต่อกับเว็บเซิร์ฟเวอร์ก็จะส่งคำขอในระดับแอพพลิเคชั่น ซึ่งในกรณีนี้ คือ HTTP ไปยังเซิร์ฟเวอร์ปลายทาง แต่สำหรับในระดับเน็ตเวิร์กนั้นแพ็กเก็ตของคำขอดังกล่าวจะมี IP แอดเดรสของปลายทางคือพร็อกซี่แค่นั้น ไม่ว่าเว็บบราวเซอร์จะติดต่อไปยังเว็บเซิร์ฟเวอร์ซึ่งตัวอยู่ที่ใด แพ็คเก็ตจริง ๆ ก็จะเดินทางไปแค่พร็อกซี่เท่านั้น ในขณะเดียวกันพร็อกซี่ก็คอยโต้ตอบในระดับของ HTTP กลับไปยังไคลเอนต์ประหนึ่งว่าตนเองเป็นเว็บเซิร์ฟเวอร์ปลายทางจริง

โดยทั่วไปพร็อกซี่ที่พบเห็นว่ามีการนำมาใช้งานมากที่สุดก็คือ เว็บพร็อกซี่ แต่จริง ๆ แล้วยังมีแอพพลิเคชั่นอีกหลายชนิดที่สามารถใช้พร็อกซี่ได้เช่น เมล์พร็อกซี่ FTP พร็อกซี่ เป็นต้น ซึ่งหากแอพพลิเคชั่นที่ใช้งานอยู่ปกติไม่สามารถปรับแต่งให้ใช้พร็อกซี่ได้ เช่น FTP ก็จำเป็นต้องติดตั้งโปรแกรมพร็อกซี่ไคลเอนต์ (Proxy Client) เพื่อใช้งานกับโปรแกรม FTP เพื่อทำหน้าที่ดัดแปลงโปรโตคอลเดิมให้รองรับการสื่อสารผ่านพร็อกซี่ให้ได้ (เรืองไกร รังสิพล. ๒๕๔๕ : ๓๕ - ๓๗)

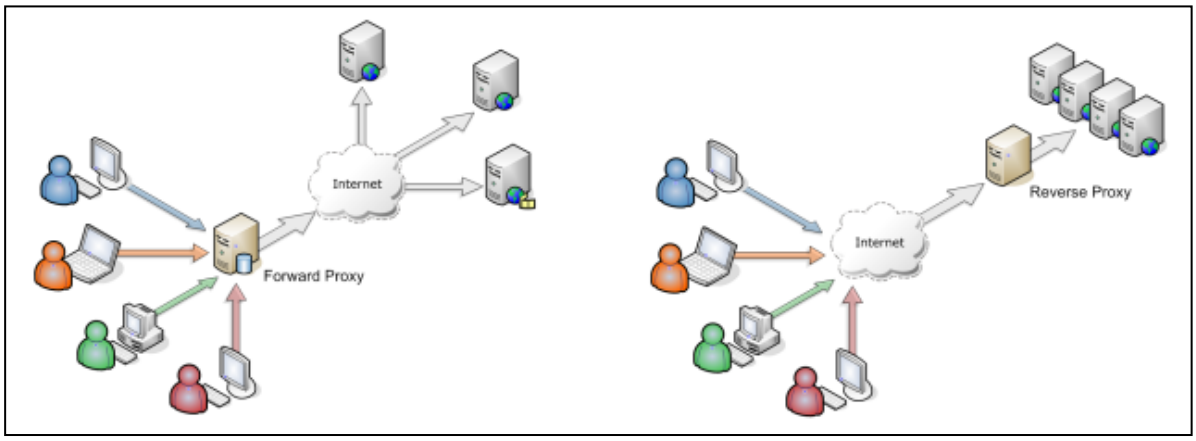
๒.๕ Reverse Proxy

การบริการ Proxy caches ซึ่ง Squid สามารถติดตั้งให้ทำงานใน ๓ รูปแบบหลัก ดังนี้

๒.๕.๑ Standard Proxy Cache ใช้สำหรับเก็บ cache ของ static web pages จำพวก html และรูปภาพ โดยทั่วไปมักจะถูกใช้งานใน network ภายในองค์กร โดยที่ web pages ต่าง ๆ ที่ถูกเรียกผ่าน local network เป็นครั้งที่สอง web browser จะแสดงผล web pages นั้นผ่าน proxy cache แทนที่ไปดึงข้อมูลจาก web server มาแสดงผล (ประหยัด bandwidth และเพิ่มความเร็วในการแสดงผล)

๒.๕.๒ Transparent Cache ความสามารถหลัก ๆ เหมือนกับการติดตั้งแบบ standard proxy cache จะแตกต่างกันที่การติดตั้งแบบ transparent cache ไม่จำเป็นต้องปรับแต่ง web browser ให้สามารถใช้งาน proxy cache โดยที่ transparent cache จะทำหน้าที่คอยกรอง HTTP traffic (on port 80) แล้วตรวจสอบว่า request นั้นมีอยู่ใน cache หรือไม่ ถ้าไม่มีก็จะทำการส่งต่อไปยัง web server ของ web pages นั้น (สำหรับ Linux การใช้งาน transparent cache จะใช้ควบคู่ไปกับ iptables ในการกรอง HTTP traffic)

๒.๕.๓ Reverse Proxy Cache สำหรับ reverse proxy cache จะทำหน้าที่แตกต่างกับ standard และ transparent caches โดยที่ reverse proxy cache จะทำหน้าที่ลดภาระของ web server แทนที่การลด network bandwidth ของฝั่ง client กล่าวคือ reverse proxy cache ถูกติดตั้งอยู่หน้า web server (ระหว่าง internet และ web server) คอยจัดการ traffic ที่เกิดขึ้นทั้งหมดก่อนจะถึง web server ป้องกัน traffic ที่เพิ่มขึ้นโดยไม่พึงประสงค์ (ซึ่งอาจจะโดนโจมตีจาก hacker เป็นต้น) อีกทั้งยังลดภาระของ web server อีกทางหนึ่ง (วิธีติดตั้ง Reverse Proxy ด้วย Squid, ๒๕๕๑: ออนไลน์)



ภาพที่ ๒ – ๒ การเปรียบเทียบรูปแบบการเชื่อมโยงระหว่าง Forward proxy และ Reverse Proxy (Mark Allen, ๒๕๖๐: ออนไลน์)

๒.๕.๔ การกำหนดชุดคำสั่งโปรแกรม Nginx เพื่อให้บริการ Reverse Proxy สำหรับการให้บริการเว็บไซต์ โดยการกำหนดค่าไฟล์ที่พาร์ท (path) /etc/nginx/conf.d โดยกำหนเชื่อไฟล์ต้องตามด้วย .conf เพื่อให้โปรแกรมสามารถแสดงผลได้อย่างถูกต้อง ตัวอย่างเช่น
/etc/nginx/conf.d/www.mydomain.com.conf
สำหรับเว็บไซต์ www.mydomain.com มีคำอธิบายในไฟล์เบื้องต้นดังนี้

```
upstream BackendServer {
 server 192.168.146.100:80; } <----- เครื่องแม่ข่ายเว็บไซต์จริง
server {
listen 80; <----- การกำหนด Port ที่ให้บริการบนเครื่อง Reverse Proxy
server_name   www.mydomain.com; <----- การกำหนด Domain ที่สนใจ
location / {
```

proxy_pass http://BackendServer; <----- การกำหนดให้ Request ส่งไปที่ Backend server

}

} (คมกริช คำสวัสดิ์. 2559: 11)

๒.๖ ด้านการจัดการเครื่องแม่ข่ายเสมือน (Virtualization)

เวอร์ชวลไลซ์เซชั่น คือ “เทคโนโลยีสำหรับการจำลองสภาพแวดล้อมให้เสมือนมีคอมพิวเตอร์หลายเครื่องทำงานอยู่ภายในคอมพิวเตอร์เครื่องหลัก” โดยอาศัยการทำงานของซอฟต์แวร์ด้านเวอร์ชวลไลเซชั่นเป็นตัวจัดการในเรื่องต่าง ๆ ไม่ว่าจะเป็นเรื่องของการใช้ฮาร์ดแวร์ ระบบปฏิบัติการ ระบบไฟล์ ระบบเครือข่าย และไฟร์วอลล์ ให้กับระบบเสมือนแต่ละตัว ทำให้การเชื่อมต่อระบบจากภายนอกไม่สามารถแยกได้ว่ากำลังติดต่อกับระบบเสมือนหรือระบบจริง

ในเรื่องของการจัดการระบบปฏิบัติการที่หลากหลายให้สามารถทำงานบนฮาร์ดแวร์ชุดเดียวกันได้นั้น ระบบปฏิบัติการหลักที่รองรับระบบปฏิบัติการอื่น ๆ มีชื่อเรียกแตกต่างกันออกไปตามเจ้าของผลิตภัณฑ์ ชื่อที่พบเห็นกันได้บ่อย ๆ ก็คือ Hypervisor, Domain ๐ และ Host OS ส่วนระบบปฏิบัติการที่ถูกจำลองขึ้นมานั้นจะถูกเรียกว่า Guest OS หรือ Domain U ซึ่งในระบบที่ถูกจำลองขึ้นนี้จะมีระบบไฟล์, ระบบเครือข่าย และไฟร์วอลล์แยกจากเครื่องหลัก นั่นก็คือ ทุกอย่างแยกออกมาอย่างอิสระจาก Host OS

ความเป็นมาของเวอร์ชวลไลเซชั่น (Virtualization)

Virtualization คำนี้เริ่มใช้กันมาตั้งแต่ปี ๑๙๖๐ โดยมีการใช้งานในกลุ่มของคอมพิวเตอร์เมนเฟรม ดังนั้น จึงไม่เป็นที่รู้จักแพร่หลาย จนต้องรอคอยให้ความสามารถของฮาร์ดแวร์และซอฟต์แวร์มาลงตัวเอาในปี ๒๐๐๐ ปีนี้เองที่ทำให้ทุกคนได้รู้จัก VMWare เพราะมาพร้อมกับคุณสมบัติที่เรียกว่า Full Virtualization นี่คือการสร้างระบบเสมือนอย่างเต็มรูปแบบเริ่มตั้งแต่การจำลอง BIOS ไปถึงฮาร์ดแวร์ทุกตัวบนเครื่องคอมพิวเตอร์

เมื่อความก้าวหน้าของเทคโนโลยีด้านฮาร์ดแวร์เพิ่มสูงมากขึ้นเรื่อย ๆ ทำให้กระแสของการทำ virtualization เติบโตตามไปแบบไร้ขีดจำกัด โดยเฉพาะจำนวน CORE ของซีพียูที่นับวันก็จะมีจำนวนมากขึ้น ทำให้สามารถตอบสนองการจำลองระบบได้อย่างเต็มรูปแบบ และที่มากไปกว่านั้นก็คือ ราคาของหน่วยความจำความเร็วสูงอย่าง RAM ก็ถูกลงมากจนไม่ใช่ข้อจำกัดด้านการลงทุนด้านนี้อีกต่อไป (Agent 47. ๒๕๕๘: ออนไลน์)

๒.๗ ด้านการจัดการไฟร์วอลล์ (Firewall)

ไฟร์วอลล์ (Firewall) คือ ระบบรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ ซึ่งจะทำหน้าที่เปิดและปิดการเข้าถึงจากภายนอก (เช่น จากอินเทอร์เน็ต) เข้าถึงเครือข่ายภายใน (เช่น เครือข่ายภายในองค์กรหรือคอมพิวเตอร์ส่วนตัว) ได้ อาจพูดได้ว่าไฟร์วอลล์ก็เหมือนยามหน้าประตูของคอมพิวเตอร์ ซึ่งการเข้าถึงจากภายนอกจะต้องผ่านให้ไฟร์วอลล์ตรวจสอบก่อนว่า สามารถเข้าระบบเครือข่ายภายในได้หรือไม่ โดยไฟร์วอลล์จะมีการกำหนดกฎระเบียบบังคับใช้เฉพาะเครือข่าย ซึ่งหมายความว่า หากการเข้าถึงนั้นถูกต้องตามที่ไฟร์วอลล์กำหนดไว้ ก็จะเข้าถึงเครือข่ายได้ หากไม่ตรงก็จะเข้าถึงไม่ได้ (หรือที่เรียกกันว่า Default deny นั่นเอง)

ยุคที่ ๑ Access Control Lists (การกำหนดเงื่อนไขเข้าถึงเครือข่ายภายใน)

ในช่วงต้น Firewall จะทำงานโดยใช้การกำหนดเงื่อนไขเข้าถึงเครือข่ายภายใน หรือ Access Control Lists (ACLs) โดยเฉพาะในเราเตอร์ส่วนใหญ่ ACLs คือ กฎระเบียบที่เขียนขึ้นมาเพื่อตรวจสอบการเข้าถึงจากภายนอกว่า อนุญาตให้เข้าถึงเครือข่ายภายในได้หรือไม่ เช่น การเข้าถึงจากภายนอกของ IP address 172.168.2.2 จะเข้าใช้เครือข่ายภายในไม่ได้ หรือแม้แต่การอนุญาตให้ port 80 ของ IP address 172.168.2.2 เข้าถึงเว็บเซิร์ฟเวอร์ IP 10.10.10.201 ได้

ACLs มีประโยชน์ตรงที่สามารถกำหนดได้ว่าต้องการให้ส่วนใดเข้าถึงบ้าง และยังมีประสิทธิภาพสูง แต่ว่าไม่สามารถอ่าน packet headers ก่อนหน้าได้ ACLs จะทำหน้าที่เพียงแค่อ่านข้อมูลการเข้าถึงเท่านั้น ดังนั้นการคัดกรองการเข้าถึงจากภายนอกโดยใช้ ACLs เพียงอย่างเดียวจึงไม่เพียงพอต่อการป้องกันการคุกคามข้อมูลภายในจากภายนอกได้

ยุคที่ ๒ Proxy firewalls

Proxy firewalls จะทำหน้าที่เป็นตัวกลาง โดยจะรับคำขอเข้าถึงข้อมูลภายใน โดยอ้างตัวเองว่าเป็นเครือข่ายภายใน หลังจากที่ตรวจสอบคำขอแล้วให้เข้าถึงข้อมูลภายในได้ ก็จะส่งข้อมูลไปให้เครือข่ายภายใน เครือข่ายภายในก็จะส่งข้อมูลกลับมาให้ Proxy แล้ว Proxy ก็จะทำให้ข้อมูลนั้นส่งไปให้ภายนอก โดยใช้ชื่อของ Proxy server กระบวนการนี้ Proxy firewall จะทำหน้าที่เป็นสื่อกลางระหว่างเครือข่ายภายในกับภายนอกไม่ให้เชื่อมต่อกันโดยตรง Proxy firewall สามารถตรวจสอบข้อมูลได้ทั้งหมด และยังทำหน้าที่คัดกรองให้ด้วย โดยอ้างอิงจากข้อมูลระดับย่อย การทำ Access Control จึงเป็นที่น่าสนใจของเหล่าแอดมิน เครือข่ายต่าง ๆ แต่อย่างไรก็ตามแอพพลิเคชั่นแต่ละตัวก็ต้องมี proxy เป็นของตัวเองในระดับแอพพลิเคชั่น (application-level) Proxy-firewalled เองก็เผชิญปัญหาด้านประสิทธิภาพของการเข้าถึงข้อมูล และข้อจำกัดด้านการรองรับแอพพลิเคชั่นต่าง ๆ รวมไปถึงการทำงานทั่วไปด้วย ซึ่งปัญหาเหล่านี้จะนำไปสู่ปัญหาด้านการควบคุมข้อมูล ซึ่งอาจทำให้ถูกดึงข้อมูลภายในออกไปภายนอกได้ นี่จึงเป็นเหตุผลที่ว่าทำไมจึงไม่ค่อยใช้ proxy firewalls กัน แม้ว่า Proxy firewall จะเป็นที่นิยมมากในช่วงปี ๑๙๙๐ ปัญหาด้านประสิทธิภาพและการควบคุมข้อมูลก็ทำให้อัตราการนำ proxy firewalls ไปใช้ในเครือข่ายภายในลดลงไปมาก

ยุคที่ ๓ Stateful Inspection firewalls

Stateful inspection หรือ stateful filtering เป็น Firewall ในยุคที่ ๓ ของเทคโนโลยี Firewall โดยที่ Stateful filtering จะทำหน้าที่ ๒ อย่าง หน้าที่แรก คือ แบ่งการเข้าถึงโดยใช้พอร์ทปลายทาง (destination port) เช่น tcp/80 = HTTP และหน้าที่ที่สอง คือ ติดตามสถานะการเข้าถึงข้อมูลโดยดูแลการโต้ตอบระหว่างภายในกับภายนอกตั้งแต่เริ่มต้นจนสิ้นสุดการเชื่อมต่อ

หน้าที่ทั้งสองที่กล่าวไปข้างต้น จะช่วยให้การทำงานของการควบคุมการเข้าถึงให้มีประสิทธิภาพมากขึ้น stateful inspection firewalls ไม่เพียงแต่เปิดปิดการเข้าถึงจากภายนอก โดยอ้างอิงจาก port กับ protocol เท่านั้น แต่ยังดูที่ประวัติย้อนหลังของ packet ในตารางสถานะ packet ด้วย เมื่อ stateful firewalls รับ packet มา ก็จะตรวจสอบในตารางสถานะของ packet ว่าเคยเชื่อมต่อกับระบบแล้วหรือยัง หรือแม้แต่ตรวจดูว่า packet นั้นมาจาก host ภายในหรือไม่ หากว่าไม่พบข้อมูลใด ๆ packet ก็จะถูกส่งไปตรวจสอบตามกฎระเบียบการเข้าถึงข้อมูลภายใน

Firewall แบบ stateful filtering จะโปร่งใส และให้ผู้ใช้งานควบคุมได้ โดยการเพิ่มการป้องกันที่ซับซ้อนให้กับโครงสร้างข้อมูล แต่ stateful firewalls ก็ยังเผชิญปัญหาด้านการรับมือกับซอฟต์แวร์แอพพลิเคชั่นที่มีการเปลี่ยนแปลงบ่อยอย่างเช่น SIP หรือ H.323

ยุคที่ ๔ Unified Threat Management (UTM)

Unified Threat Management (UTM) ก็คือ การรวบรวมการทำงานของ stateful inspection firewalls, แอนตี้ไวรัส, และ IPS ไว้ในที่เดียวกัน ต่อมา UTM ก็มีฟังก์ชั่นการรักษาความปลอดภัยเครือข่ายเพิ่มขึ้น

UTMs จะต้องอาศัยการทำงานของ Firewall แบบ stateful inspection ซึ่งจะปูทางการทำงานให้ UTM เพราะฟังก์ชั่นการทำงานต่าง ๆ ของ UTM จะทำงานตามระบบรักษาความปลอดภัยที่วางไว้ ดังนั้น หากเงื่อนไข access control วางมาดี การทำงานต่าง ๆ ใน Firewall ในเครือข่ายก็จะดีตามด้วย ถึงแม้ว่า UTMs จะมีฟังก์ชั่นด้านความปลอดภัยหลาย ๆ อันรวมกัน แต่เทคโนโลยี access control เบื้องต้นของ Firewall ก็ยังเหมือนเดิม

ยุคที่ ๕ Next-generation firewalls (Firewall ยุคล่าสุด)

Next-generation firewalls (NGFWs) ถูกออกแบบขึ้นมาให้ต่อสู้กับแอพพลิเคชั่นและมัลแวร์ที่ซับซ้อนขึ้นทุกวัน นักพัฒนาแอพพลิเคชั่นซอฟต์แวร์ หรือมัลแวร์ ต่างก็ทำพลาดในการตั้งค่าการเข้าถึงแบบ long-standing port-based เพราะใช้เทคนิคการเลี่ยงตัว port ในการพัฒนาโปรแกรมซอฟต์แวร์ ทุกวันนี้มัลแวร์ต่าง ๆ ก็เลยแฝงตัวติดอยู่กับแอพพลิเคชั่นเข้าไปยังเครือข่ายภายใน แล้วก็สร้างเครือข่ายระหว่างตัวมัลแวร์ในเครือข่ายภายในอีกที NGFWs จะทำหน้าที่เป็นแพลทฟอร์มด้านความปลอดภัยที่จะช่วยตรวจสอบการเข้าใช้เครือข่ายจากภายนอก (Onestopwareblogger. ๒๕๖๐: ออนไลน์)

๒.๘ ด้านการจัดการเว็บไซต์และช่องโหว่ของเว็บไซต์

๒.๘.๑ HTTP และ HTTPS

๒.๘.๑.๑ เฮชทีทีพี (Hypertext Transfer Protocol : HTTP) เป็นโปรโตคอลที่อยู่ในชั้นแอพพลิเคชั่นของชุดโปรโตคอล TCPIP ซึ่งจะเป็นตัวกำหนดรูปแบบการร้องขอไฟล์ของลูกข่าย (เว็บบราวเซอร์) จากเว็บเซิร์ฟเวอร์ และรูปแบบการถ่ายโอนไฟล์จากเว็บเซิร์ฟเวอร์ไปยังลูกข่าย กระบวนการนั้นจะเริ่มที่ทางฝั่งลูกข่าย โดยผู้ใช้คลิกที่ลิงค์ในเว็บเพจ หรือพิมพ์ยูอาร์แอล (Uniform Resource Locator : URL) ในช่องที่อยู่ แอดเดส (Address) ของเว็บบราวเซอร์ หลังจากนั้น เว็บบราวเซอร์จะส่งการร้องขอเฮชทีทีพี รีเควส (HTTP Request) ผ่านเครือข่ายไปยังเว็บเซิร์ฟเวอร์ เมื่อเว็บเซิร์ฟเวอร์ได้รับการร้องขอ ก็จะค้นหาไฟล์ที่กำหนดในยูอาร์แอล ซึ่งถ้าพบก็จะตอบกลับเฮชทีทีพี เรสปอนส์ (HTTP Response) พร้อมกับไฟล์นั้นกลับไปยังฝั่งลูกข่ายเว็บ บราวเซอร์ เมื่อได้รับไฟล์เว็บเพจที่ร้องขอไปก็จะแสดงไฟล์นั้นให้ผู้ใช้ดู โปรโตคอลเฮทีทีพีนั้นไม่ได้กำหนดรูปแบบการแสดงผลให้ผู้ใช้ดู ซึ่งหน้าที่นี้เป็นของเว็บบราวเซอร์ ดังนั้น เว็บบราวเซอร์ที่ต่างกันอาจแสดงเว็บเพจไม่เหมือนกันก็ได้

๒.๘.๑.๒ เฮชทีทีพีเอส (Hypertext Transfer Protocol : HTTPS) ปัจจุบันก็ได้มีการพัฒนาโปรโตคอลแทนเฮทีทีพี ที่สามารถเข้ารหัสข้อมูลได้ซึ่งก็คือ โปรโตคอลเฮชทีทีพีเอส HTTPS (Hypertext Transfer Protocol Over Secure Socket Layer) ซึ่งพัฒนาโดยเน็ตสเคป (Netscape) เพื่อสำหรับการเข้ารหัสข้อมูลที่รับส่งระหว่างเว็บเซิร์ฟเวอร์และบราวเซอร์ มีการเข้ารหัสข้อมูล โดยปกติแล้ว เฮชทีทีพีเอสจะใช้พอร์ต 443 แทนพอร์ต 80 โดยเวอร์ชั่นแรกนั้น จะใช้การเข้ารหัสแบบอาร์เอสเอ (RCA) ที่ใช้คีย์ขนาด ๔๐ บิต ซึ่งก็ถือว่าปลอดภัยเพียงพอในช่วงแรก ๆ ตัวอย่างที่เห็นได้ทั่วไปในการใช้งานเฮชทีทีพีเอส เช่น เมื่อไปเยี่ยมชมเว็บไซต์อีคอมเมิร์ซเพื่อสั่งซื้อสินค้าออนไลน์ ในช่วงของการเลือกดูสินค้านั้นก็จะใช้โปรโตคอล

เฮชทีทีพี ซึ่งไม่จำเป็นต้องมีการเข้ารหัส แต่เมื่อจะสั่งซื้อสินค้าและจ่ายเงินด้วยบัตรเครดิต ยูอาร์เอลของเว็บเพจนั้น ก็จะเปลี่ยนมาเป็นขึ้นต้นด้วย https:// ซึ่งเมื่อมีการรับส่งข้อมูลก็จะมีการเข้ารหัสข้อมูลเหล่านั้น

เว็บทั่วไปจะใช้โปรโตคอล เฮชทีทีพี ในการรับส่งเอกสารเฮชทีเอ็มแอล (Hypertext Markup Language : html) ระหว่างเว็บเซิร์ฟเวอร์ และบราวเซอร์ ซึ่งโปรโตคอลนี้จะรับส่งข้อมูลในรูปแบบเคลียร์เท็กซ์ ทำให้การสื่อสารไม่ปลอดภัย โดยเฉพาะสำหรับการรับส่งข้อมูลที่สำคัญ เช่น หมายเลขบัตรเครดิต หรือยูสเซอร์เนม และพาสเวิร์ด สำหรับเข้าใช้ระบบต่าง ๆ เนื่องจากคนอื่นอาจเฝ้าดูข้อมูลที่วิ่งผ่านเครือข่ายอยู่ก็ได้ ส่วนเว็บโปรโตคอลเวอร์ชั่นที่รองรับเอสเอสแอล (Secure Socket Layer : SSL) คือ เฮชทีทีพี ซึ่งเป็นโปรโตคอลที่ถือว่าปลอดภัยสำหรับการสื่อสารผ่านอินเทอร์เน็ต (จตุชัย แพงจันทร์. ๒๕๕๘: ๒๑๐ , ๒๑๔)

๒.๘.๒ รหัสสถานะเฮชทีทีพี (HTTP Status Code)

คือ โค๊ดมาตรฐานที่แสดงขึ้นมาจากการตอบสนองของเว็บเซิร์ฟเวอร์บนเว็บไซต์ต่าง ๆ ที่อยู่บนอินเทอร์เน็ต หรือเรียกง่าย ๆ ว่าโค๊ดแสดงสถานะของ เฮชทีทีพี โค๊ดต่าง ๆ เหล่านี้จะช่วยให้เราวินิจฉัยและให้ทราบถึงปัญหาต่าง ๆ ที่เกิดขึ้นเมื่อหน้าเว็บ หรือทรัพยากรต่าง ๆ เช่น รูปภาพ ข้อความ วิดีโอ ฯลฯ ที่ไม่สามารถโหลดได้อย่างเป็นปกติ รหัสสถานะ การให้ของเฮชทีทีพี และประโยคที่เป็นคำอธิบายเหตุผลว่าเกิดอะไรขึ้นกับข้อผิดพลาดนี้

- **2xx การร้องขอสำเร็จ** รหัสสถานภาพกลุ่มนี้ หมายถึง การดำเนินการที่ร้องขอได้รับแล้ว เป็นที่เข้าใจแล้ว และได้ยอมรับแล้ว ใช้แสดงว่าการร้องขอจากเครื่องลูกข่ายได้ดำเนินการสำเร็จแล้ว ตัวอย่างเช่น 200 OK เป็นรหัสตอบรับมาตรฐานสำหรับการร้องขอที่สำเร็จ 201 Created การร้องขอได้ดำเนินการแล้ว เป็นต้น
- **3xx การเปลี่ยนทาง** รหัสสถานภาพกลุ่มนี้ หมายถึง เครื่องลูกข่ายอาจต้องมีการกระทำอื่นเพิ่มเติม เพื่อที่จะทำการร้องขอนั้นให้สำเร็จ แสดงว่าโปรแกรมพร็อกซีผู้ใช้จำเป็นต้องมีการดำเนินการอื่นเพิ่มเติม ซึ่งอาจทำได้เองโดยไม่จำเป็นต้องโต้ตอบกับผู้ใช้ ถ้าคำสั่งร้องขอครั้งที่สองเป็น GET หรือ HEAD นอกจากนี้ พร็อกซีผู้ใช้ไม่ควรเปลี่ยนทางมากกว่าห้าครั้ง เพราะว่าการทำเช่นนั้นอาจถูกพิจารณาว่าเป็นวงลูปไม่รู้จบ ตัวอย่างเช่น 306 Switch Proxy แจ้งไปยังเครื่องลูกข่ายว่าควรเปลี่ยนพร็อกซีที่ใช้ ปัจจุบันเลิกใช้งานแล้ว
- **4xx ความผิดพลาดจากเครื่องลูกข่าย** รหัสสถานภาพกลุ่มนี้ หมายถึง การร้องขอจากเครื่องลูกข่ายไม่เป็นที่ยอมรับ หรือไม่สามารถทำตามการร้องขอนั้นได้ เครื่องแม่ข่ายจะถือว่าเป็นความผิดพลาดของเครื่องลูกข่าย ตัวอย่างเช่น 400 Bad Request ข้อความร้องขอที่ส่งมามีความผิดพลาดทางไวยากรณ์ หรือไม่สามารถทำตามการร้องขอนั้นได้
- **5xx ความผิดพลาดจากเครื่องแม่ข่าย** รหัสสถานภาพกลุ่มนี้ หมายถึง เครื่องแม่ข่ายไม่สามารถให้บริการได้ แม้ว่าการร้องขอจะส่งมาอย่างถูกต้อง เครื่องให้บริการพบกับข้อผิดพลาดบางประการ ซึ่งทำให้ไม่สามารถทำตามการร้องขอที่ส่งมา ตัวอย่างเช่น 500 Internal Server Error ข้อความแสดงความผิดพลาดแบบทั่วไป (Bundit Nuntates, ๒๕๕๗: ออนไลน์)

๒.๘.๓ SQL Injection

SQL Injection เป็นเทคนิคที่ใช้ประโยชน์จากส่งคำสั่ง SQL ผ่านทางเว็บแอพพลิเคชันเพื่อไปโจมตีระบบฐานข้อมูลหลังบ้าน โดยอาศัยช่องโหว่ของการใส่ข้อมูล input ของผู้ใช้ที่สามารถตรวจสอบรูปแบบการโจมตีได้อย่างจำกัด แฮ็คเกอร์รู้ดีว่านักเขียนโปรแกรมจะนำข้อมูลที่ผู้ใช้ input ลงไป ไปใช้เป็นส่วน

หนึ่งของคำสั่ง SQL เพื่อส่งไปยังระบบฐานข้อมูล จึงได้แอบฝังคำสั่ง SQL บางอย่างลงไปใน input เหล่านั้นด้วย ส่งผลให้แฮ็คเกอร์สามารถดึงข้อมูล หรือเปลี่ยนแปลงแก้ไขข้อมูลในระบบฐานข้อมูลตามคำสั่ง SQL ที่แอบฝังลงไปได้ทันที ยกตัวอย่างง่าย ๆ ที่พบเห็นบ่อย ๆ คือ “OR 1=1” ที่นิยมใช้เพื่อบายพาสการพิสูจน์ตัวตน ปกติแล้วหน้าพิสูจน์ตัวตนจะมีช่องให้ใส่ชื่อผู้ใช้และรหัสผ่าน ซึ่งนักเขียนโปรแกรมก็จะนำข้อมูลที่ผู้ใช้กรอกลงไป ไปตรวจสอบกับระบบฐานข้อมูลโดยใช้ คำสั่ง SELECT * FROM authen_db WHERE username=‘suthee’ and password=‘12345678’; เพื่อเช็คดูว่าในฐานข้อมูลการพิสูจน์ตัวตน (authen_db) มีชื่อผู้ใช้และรหัสผ่านตรงตามที่ผู้ใช้กรอกลงไปหรือไม่ ซึ่งเมื่อแฮ็คเกอร์รู้ว่าต้องมีการนำข้อมูลที่ผู้ใช้กรอกลงไป (ในที่นี้คือ suthee และ 12345678) ส่งไปยังระบบฐานข้อมูลโดยตรง จึงได้แอบฝังคำสั่ง SQL ลงไปเพื่อหลีกเลี่ยงการตรวจสอบ คือ การใส่ชื่อผู้ใช้เป็น “admin” และรหัสผ่านเป็น “‘ OR ‘1’=‘1” ส่งผลให้คำสั่ง SQL ที่ใช้ตรวจสอบเพื่อพิสูจน์ตัวตนก็จะกลายเป็น SELECT * FROM authen_db WHERE username=‘admin’ and password=‘’ OR ‘1’=‘1’; ผลลัพธ์ที่ได้ คือ แฮ็คเกอร์สามารถลงชื่อเข้าใช้เป็น “admin” ได้ทันที เนื่องจากด้านหลังมีนิพจน์ OR 1=1 ทำให้คำสั่ง SQL ดังกล่าวเป็นจริงเสมอ นอกจากการบายพาสการพิสูจน์ตัวตนแล้ว SQL Injection ยังสามารถดึงข้อมูล, เปลี่ยนแปลงแก้ไข, ลบข้อมูล หรือทำลายฐานข้อมูลทั้งหมด ขึ้นอยู่กับคำสั่ง SQL ที่แอบฝังลงไปได้เช่นกัน" (TechTalkThai, ๒๕๕๗: ออนไลน์)

๒.๙ ด้านการจัดการระบบเครือข่ายคอมพิวเตอร์

๒.๙.๑ นิยามของระบบเครือข่าย

แลน (Local Area Network : LAN) แปลว่า ระบบเครือข่ายบริเวณเฉพาะที่เป็นระบบเครือข่ายคอมพิวเตอร์ซึ่งมีขนาดเล็ก นิยมใช้ภายในห้องหรือสถานที่เดียวกัน สำหรับระบบเครือข่ายแบบ LAN (แลน) ในแลนหนึ่งวงจะต้องมีหนึ่งไอพีซับเน็ต ดังนั้น อุปกรณ์เครือข่าย (อย่างเช่น คอมพิวเตอร์) ที่อยู่แลนวงเดียวกันจะต้องมีไอพีแอดเดรสอยู่ในซับเน็ตเดียวกัน ซึ่งนั่นหมายความว่า อุปกรณ์เครือข่ายเหล่านี้จะต้องมีหมายเลขเน็ตเวิร์คแอดเดรส และบรอดคาสต์แอดเดรสเป็นหมายเลขเดียวกัน

แวน (Wide Area Network : WAN) แปลว่า “ระบบเครือข่ายบริเวณกว้าง” เป็นระบบเครือข่ายคอมพิวเตอร์ที่มีการเชื่อมต่อของแลนตั้งแต่สองวงขึ้นไป และต้องอยู่ห่างไกลกันในคนละสถานที่ หรือพื้นที่ อย่างเช่น การเชื่อมต่อระหว่างมหาวิทยาลัย คนละวิทยาเขตซึ่งอยู่กันคนละเมือง นอกจากนี้ระบบเครือข่ายแวนจะเกี่ยวข้องกับไอพีแอดเดรสหลาย ๆ ซับเน็ต ดังนั้น อุปกรณ์ เราท์เตอร์ (ซึ่งมีหน้าที่ในการส่งข้อมูลแพ็กเก็ตข้ามระหว่างซับเน็ต) จะถูกใช้ในกรณีนี้

อินทราเน็ต (Intranet) หมายถึง “ระบบเครือข่ายเชื่อมต่อกันภายใน” เป็นระบบเครือข่ายคอมพิวเตอร์ที่มีการเชื่อมต่อกันเองภายในองค์กรเดียวกัน ซึ่งอาจจะประกอบไปด้วยแลนหลาย ๆ วงต่อเชื่อมกันภายในสถานที่เดียวกัน หรือแลนหลาย ๆ วงที่อยู่ห่างไกลกันคนละเมืองต่อเชื่อมกันผ่านแวน

เอ็กซ์ทราเน็ต (Extranet) หมายถึง “ระบบเครือข่ายเชื่อมต่อกันภายนอก” เป็นระบบเครือข่ายคอมพิวเตอร์อินทราเน็ต ที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ ซึ่งมักจะเป็นอินเทอร์เน็ต หรืออาจจะเป็นระบบเครือข่ายคอมพิวเตอร์อินทราเน็ต ที่เชื่อมต่อถึงกันโดยผ่านอินเทอร์เน็ต อย่างเช่น วีพีเอ็น(Private Public Network : VPN)

อินเทอร์เน็ต (Internet) หมายถึง “ระบบเครือข่ายที่เชื่อมโยงถึงกันทั่วโลก” เป็นระบบเครือข่ายที่มีการเชื่อมต่อกันทั่วโลก ดังนั้น ภายในระบบเครือข่ายอินเทอร์เน็ตจะประกอบไปด้วยแวนต่างๆ ที่เชื่อมโยงกันทั่วโลก นั่นหมายความว่า อินเทอร์เน็ตเป็นระบบเครือข่ายที่ใหญ่ที่สุดในโลก และมีเพียงเครือข่าย

ห้องสมุดกรมพัฒนาที่ดิน

เดียวเท่านั้นในโลกใบนี้ จึงกล่าวได้ว่าอินเทอร์เน็ตเป็นเครือข่ายสาธารณะ (Public Network)" (สานนท์ ฉิมพรี. ๒๕๕๒ : ๕)

๒.๙.๒ ไอพี แอดเดรส (IP Address) คือ หมายเลขที่สามารถระบุแยกแยะความแตกต่างของเครื่อง**คอมพิวเตอร์** และอุปกรณ์เครือข่ายต่าง ๆ ที่มีการเชื่อมต่อในเครือข่ายเดียวกัน หรือจะเป็นการเชื่อมต่อนอกเครือข่ายก็ได้เช่นกัน อย่างที่กล่าวมาแล้วในตอนต้นว่า ไอพี แอดเดรส เปรียบได้ดังเลขที่บ้าน ในการตั้งไอพี แอดเดรส จะตั้งไม่ให้ซ้ำกันอย่างเด็ดขาด เพราะถ้าซ้ำกันจะทำให้เกิดความสับสนในการติดต่อสื่อสารภายในเครือข่าย ซึ่งนี่เองเลยมีหน่วยงานที่ออกมากำหนดเรื่องของการตั้งค่า ไอพี แอดเดรส ขึ้นมา (ไอพี แอดเดรส IP Address. ออนไลน์)

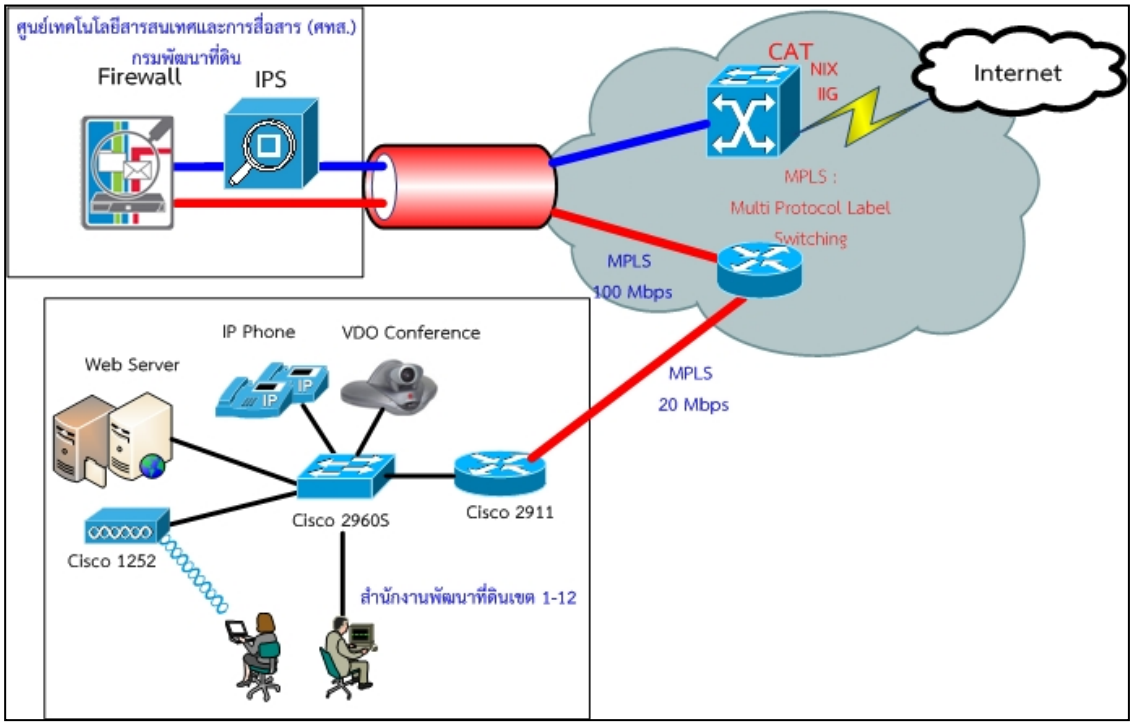
๒.๙.๓ พอร์ต (Port)

คอมพิวเตอร์ที่ใช้โปรโตคอล TCPIP ส่วนใหญ่จะมีแอพพลิเคชันหลายตัวที่ใช้โปรโตคอล TCP/IP ในการสื่อสารกับเครื่องอื่น ซึ่งโปรโตคอล TCP/IP จะจัดการส่งข้อมูลไปยังแอพพลิเคชั่นที่เหมาะสม เพื่อให้ TCP/IP สามารถรองรับหลายแอพพลิเคชั่นในเครื่องเดียว จึงมีการใช้พอร์ตและซ๊อกเก็ต (Port and Socket) เพื่อช่วยในการแยกแยะแอพพลิเคชั่นต่าง ๆ แอพพลิเคชั่นแต่ละตัวที่จะรับส่งข้อมูลผ่านเครือข่าย จะใช้หมายเลขพอร์ตตั้งแต่ 0 ถึง 65,536 ดังนั้น เพื่อให้ส่งข้อมูลถูกต้อง แอพพลิเคชั่นที่รันในเครื่องเดียวกันจะต้องใช้หมายเลขพอร์ตที่ต่างกัน เพื่อช่วยลดความสับสน "อันที่นิยมใช้กันทั่วไป ส่วนใหญ่จะถูกกำหนดให้ใช้หมายเลขพอร์ตใดพอร์ตหนึ่ง ซึ่งองค์กรที่ทำหน้าที่กำหนด หมายเลขนี้คือ IANA (Internet Assigned Numbers Authority) หมายเลขพอร์ตเหล่านี้จะถูกตีพิมพ์ใน REC 1700 (จตุชัย แพงจันทร์. ๒๕๕๘ : ๒๘๐)

ห้องสมุดกรมพัฒนาที่ดิน

บทที่ ๓
การวิเคราะห์และออกแบบกระบวนการจัดทำระบบ

ขั้นตอนการพัฒนาระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต มีขั้นตอนในส่วนของการสร้างเครื่องแม่ข่ายเสมือน (Visual Machine) การติดตั้งโปรแกรมที่เกี่ยวข้อง และการปรับปรุงระบบเครือข่ายเพื่อให้การพัฒนาระบบเป็นไปตามที่ได้กำหนดไว้ ดังนี้



ภาพที่ ๓ – ๑ รูปแบบการเชื่อมต่อระบบเครือข่ายในปัจจุบันที่ให้บริการเว็บไซต์

๓.๑ ขั้นตอนการให้บริการเว็บไซต์ของหน่วยงานส่วนภูมิภาค กรมพัฒนาที่ดิน ในปัจจุบัน

กรมพัฒนาที่ดินมีการว่าจ้างบริษัท กสท โทรคมนาคม จำกัด (มหาชน) เพื่อใช้บริการด้านการเชื่อมต่ออินเทอร์เน็ต และเชื่อมต่อระบบเครือข่ายระหว่างหน่วยงานส่วนกลางกับหน่วยงานส่วนภูมิภาค ผ่านมาตรฐานเอ็มพีแอลเอส (Multiprotocol Label Switching : MPLS) ซึ่งการให้บริการเว็บไซต์ของหน่วยงานส่วนภูมิภาค กรมพัฒนาที่ดิน สำหรับบุคคลที่สนใจและอยู่ภายนอกเครือข่ายกรมพัฒนาที่ดิน จะมีการเชื่อมต่อโดยอุปกรณ์ที่มีหน้าที่แตกต่าง และมีขั้นตอนดังนี้

ขั้นตอนที่ ๑ เมื่อมีผู้สนใจเรียกใช้งานเว็บไซต์ จากอุปกรณ์หรือคอมพิวเตอร์ที่อยู่ภายนอกเครือข่ายกรมพัฒนาที่ดิน คอมพิวเตอร์เครื่องดังกล่าวจะส่งข้อมูลความต้องการเรียกใช้งานเว็บไซต์ บรรจุลงไปในแพ็กเก็ต (Packet) และส่ง Packet ในระบบเครือข่ายไปยังไอเอสพี (Internet service provider :ISP) ที่มีเชื่อมต่ออยู่ และISP จะส่ง Packet ผ่านการเชื่อมต่ออินเทอร์เน็ต มายัง ISP บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

ขั้นตอนที่ ๒ เมื่ออุปกรณ์เครือข่ายที่ของ ISP บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ได้รับ Packet ดังกล่าว จะทำการตรวจสอบและส่ง Packet ดังกล่าวไปยังอุปกรณ์เครือข่ายของ กรมพัฒนาที่ดิน ผ่านมาตรฐาน MPLS

ขั้นตอนที่ ๓ เมื่ออุปกรณ์เครือข่าย กรมพัฒนาที่ดิน ส่วนกลาง ได้รับ Packet ดังกล่าวจะทำการตรวจสอบความผิดปกติในการส่ง Packet โดยอุปกรณ์ IPS เมื่อ Packet นั้นไม่มีความผิดปกติ จะทำการส่งต่อไปยังอุปกรณ์ไฟร์วอลล์ และไฟร์วอลล์ซึ่งมีหน้าที่ในการทำเอ็นเอที (Network address translation : NAT) คือการเปลี่ยน Public ไอพีแอดเดส (IP address) ไปเป็น Private IP address ที่ใช้ในเชื่อมต่อระบบเครือข่ายภายใน กรมพัฒนาที่ดิน เมื่อเสร็จสิ้นกระบวนการ NAT แล้วจะทำการส่ง Packet ผ่านอุปกรณ์ต่าง ๆ ภายใน กรมพัฒนาที่ดิน เพื่อส่งข้อมูลไปยังเครื่องแม่ข่ายเว็บไซต์ของหน่วยงานส่วนภูมิภาค กรมพัฒนาที่ดิน

ขั้นตอนที่ ๔ เมื่อเครื่องแม่ข่ายเว็บไซต์ของหน่วยงานส่วนภูมิภาค กรมพัฒนาที่ดิน ได้รับ Packet จะทำการประมวลผล Packet ที่ได้รับ และทำการสร้างข้อมูลเพื่อตอบกลับตามความต้องการ บรรจุลงไปยัง Packet และส่ง Packet ดังกล่าวกลับไปยังอุปกรณ์เครือข่าย กรมพัฒนาที่ดิน ส่วนกลาง

ขั้นตอนที่ ๕ เมื่ออุปกรณ์เครือข่าย กรมพัฒนาที่ดิน ส่วนกลาง ได้ Packet ดังกล่าว อุปกรณ์ไฟร์วอลล์ จะทำการ NAT เป็น Public IP address และส่ง Packet ไปยัง ISP บริษัท กสท โทรคมนาคม จำกัด (มหาชน) เพื่อส่งข้อมูลเครื่องลูกข่าย

ขั้นตอนที่ ๖ เมื่ออุปกรณ์เครือข่าย บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ได้รับ Packet แล้วก็จะส่ง Packet กลับไปยัง ISP ของเครื่องลูกข่าย และส่งข้อมูลไปยังเครื่องลูกข่าย เมื่อเครื่องลูกข่ายได้รับ Packet จะแปลง Packet ที่ได้รับเป็นข้อมูลเพื่อให้แสดงผลข้อมูล เป็นเสร็จสิ้นข้อมูลกระบวนการให้เว็บไซต์ของหน่วยงานส่วนภูมิภาค กรมพัฒนาที่ดิน ในปัจจุบัน ตามภาพที่ ๓ – ๑

๓.๒ การวิเคราะห์ระบบ

เครื่องแม่ข่ายเว็บไซต์ของหน่วยงานส่วนภูมิภาค กรมพัฒนาที่ดิน ติดตั้งอยู่ที่สำนักงานพัฒนาที่ดินเขต เชื่อมต่อระบบเครือข่ายส่วนภูมิภาคและส่วนกลางผ่านระบบอินทราเน็ตของกรมพัฒนาที่ดิน ตามมาตรฐาน MPLS การเชื่อมต่อระหว่างส่วนกลางกับสำนักงานพัฒนาที่ดินเขต สามารถใช้ท่อวงจรที่มีความเร็ว ๒๐ Mbps ท่อวงจรดังกล่าว ใช้งานร่วมกับการใช้งานต่าง ๆ เช่น การใช้งานระบบ e-Service ของกรมฯ การใช้งานระบบภายนอก กรมพัฒนาที่ดิน การใช้งานทั่วไปเพื่อเชื่อมต่ออินเทอร์เน็ต และมีอุปกรณ์ที่ทำหน้าที่ปกป้องรักษาความปลอดภัยทางระบบเครือข่ายและอินเทอร์เน็ต ประกอบด้วย ไฟร์วอลล์ และไอพีเอส ทำการตรวจสอบการส่งผ่านข้อมูลตามหน้าที่และคุณสมบัติของอุปกรณ์ เพื่อรักษาความปลอดภัยทางระบบเครือข่ายและอินเทอร์เน็ตของ กรมพัฒนาที่ดิน ซึ่งทำให้การให้บริการเว็บไซต์ของหน่วยงานในส่วนภูมิภาคทำได้อย่างมีประสิทธิภาพ

๓.๓ ปัญหาที่เกิดขึ้นในปัจจุบัน

เว็บไซต์หน่วยงานในส่วนภูมิภาค กรมพัฒนาที่ดิน ส่วนใหญ่เป็นข้อมูลในรูปแบบคงที่ (Data Static) แสดงผลอย่างเดียวโดยไม่มีการโต้ตอบระหว่างผู้ใช้งานกับเว็บไซต์ เช่น ข้อมูลเอกสารเผยแพร่ ข้อมูลแสดงผลรูปภาพ เมื่อผู้ใช้งานเรียกดูข้อมูลบนเว็บไซต์ส่วนภูมิภาคผ่านระบบอินเทอร์เน็ต ระบบจะส่งข้อมูลคำขอ Packet มายังไฟร์วอลล์ ส่วนกลาง (ตั้งอยู่ ณ ห้องควบคุมระบบ Network ศทส.) เพื่อตรวจสอบแพ็กเกต ตามนโยบายการให้บริการ (Policy) จากนั้น จะส่งแพ็กเกตคำขอไปยังเครื่องแม่ข่ายเว็บไซต์ของหน่วยงานส่วน

ภูมิภาคเพื่อประมวลผล แล้วจึงส่งแพ็กเกจตอบกลับไปยังผู้สนใจ ผ่านระบบเครือข่ายอินทราเน็ตของกรมฯ และหากมีการรับ-ส่งแพ็กเกตคำขอที่เหมือนกันในช่วงเวลาเดียวกัน พบว่า เครื่องแม่ข่ายเว็บไซต์ของหน่วยงานส่วนภูมิภาคต้องทำงานหนัก เพราะประมวลผลซ้ำ ๆ ทุกครั้งที่มีการส่งคำขอ

ในขณะเดียวกัน การป้องกันการโจมตีด้วยการติดตั้งไฟร์วอลล์ระหว่างเครือข่ายภายนอกและเว็บเซิร์ฟเวอร์ เพื่อทำหน้าที่ตรวจสอบความถูกต้องของการรับ-ส่งระหว่างต้นทาง (Source) และปลายทาง (Destination) สามารถป้องกันได้ส่วนหนึ่ง แต่ไม่สามารถป้องกันการโจมตีผ่านช่องโหว่ของชุดคำสั่ง (Source Code) เว็บไซต์ ซึ่งอยู่นอกเหนือการตรวจสอบของไฟร์วอลล์กรองแพ็กเกต (Packet Filtering) จึงทำให้กลุ่มผู้ไม่ประสงค์ดีพยายามเข้าถึงระบบโดยไม่ได้รับอนุญาต รวมถึงทำให้ระบบหยุดให้บริการด้วยวิธีการต่าง ๆ อันส่งผลต่อภาพลักษณ์ของหน่วยงาน ผู้ไม่ประสงค์ดีอาจมีจุดประสงค์แตกต่างกันไปตามเวลา และสถานการณ์ เช่น เพื่อข่มขู่เรียกค่าไถ่ หรือเพื่อแอบซ่อนช่องการโจมตีที่แท้จริง และใช้เว็บไซต์ของเราเป็นฐานในการโจมตีเว็บไซต์อื่น ๆ ซึ่งแนวโน้มภัยคุกคามผ่านช่องทางอินเทอร์เน็ตมีเพิ่มขึ้นอย่างเนื่องทุกปี

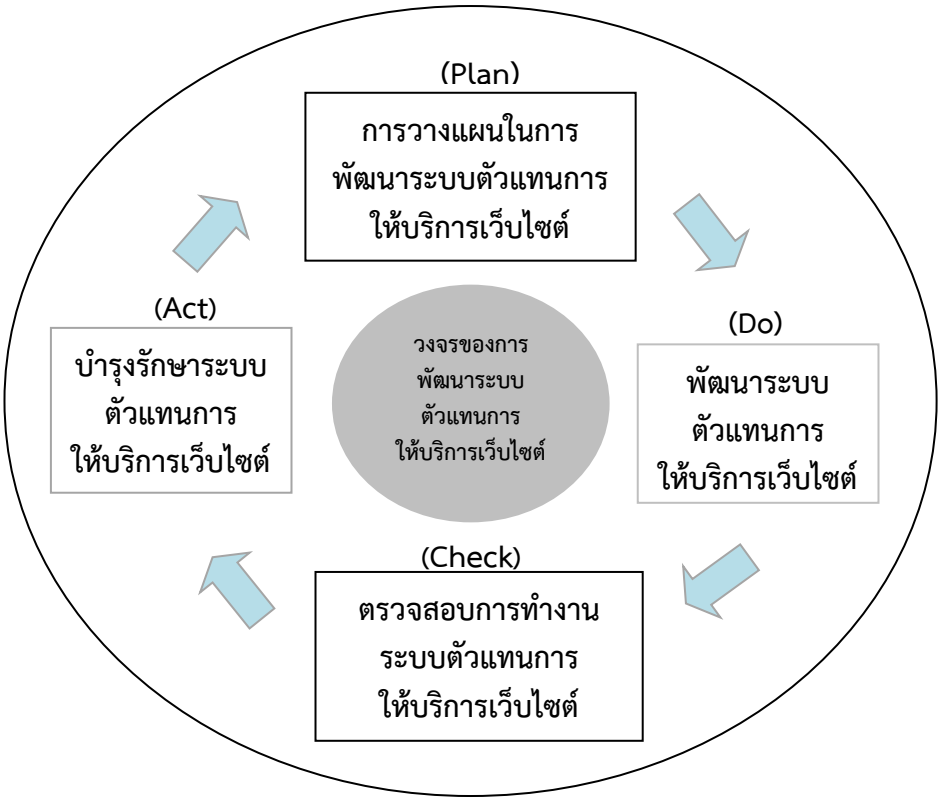
๓.๔ ความจำเป็นในการพัฒนาระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต

จากปัญหาที่เกิดขึ้นดังกล่าว จึงได้พัฒนาระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต รีเวิสพร็อกซี่ (Reverse Proxy) ขึ้น เพื่อจำลองเครื่องคอมพิวเตอร์ที่ทำหน้าที่ให้บริการต่าง ๆ แทนเครื่องแม่ข่ายเว็บไซต์จริงที่ตั้งอยู่ในอินเทอร์เน็ต ซึ่งทำหน้าที่สำหรับเก็บข้อมูลที่ผู้ใช้บริการได้เรียกข้อมูลมาจากอินเทอร์เน็ต โดยผ่านทางเว็บบราวเซอร์ (Web Browser) ทำให้ผู้ใช้บริการรายต่อไปที่ต้องการค้นหาข้อมูลเดิมซ้ำกับที่มีผู้อื่นเรียกใช้บริการไว้ สามารถที่จะเรียกดูข้อมูลจากรีเวิสพร็อกซี่ได้โดยตรง ไม่ต้องค้นหาข้อมูลจากแม่ข่ายเว็บไซต์จริงอีก ซึ่งทำให้ลดช่วงเวลาในการรับ-ส่งข้อมูล (Load) เว็บไซต์มาแสดงผล ทำให้ผู้ใช้งานสามารถเข้าถึงได้เร็วขึ้น และรีเวิสพร็อกซี่ยังสามารถปรับปรุงชุดคำสั่งให้กับเครื่องแม่ข่ายเว็บไซต์ เพื่อลดช่องโหว่ของเว็บไซต์ เป็นเครื่องมือเบื้องต้นใช้ในการป้องกันการโจมตีของเว็บไซต์ได้

๓.๕ ออกแบบกระบวนการจัดทำระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต

๓.๕.๑ ข้อกำหนดทั่วไป

กิจกรรมในการพัฒนาระบบซึ่งประกอบด้วยขั้นตอน ๔ ขั้น คือ วางแผน-ปฏิบัติ-ตรวจสอบ-ปรับปรุงการดำเนินกิจกรรม แนวทางที่ใช้ในมาตรฐานฉบับนี้จะใช้กระบวนการ Plan-Do-Check-Act หรือ P-D-C-A มาประยุกต์ใช้ตามแสดงในภาพที่ ๓ - ๒



ภาพที่ ๓ – ๒ แผนภาพแสดงวงจรการพัฒนาระบบตัวแทนการให้บริการเว็บไซต์ Plan-Do-Check-Act

๓.๕.๒ การบริหารจัดการระบบตัวแทนการให้บริการเว็บไซต์

๓.๕.๒.๑ การวางแผนในการพัฒนาระบบตัวแทนการให้บริการเว็บไซต์ (Plan) หมายความรวมถึงการกำหนดเป้าหมาย ความต้องการของระบบ รวมถึงขอบเขตการพัฒนาระบบ ในการดำเนินงานวิธีการและขั้นตอนที่จำเป็น เพื่อให้การดำเนินงานบรรลุเป้าหมาย ในการวางแผนจะต้องทำความเข้าใจกับเป้าหมายวัตถุประสงค์ให้ชัดเจน โดยปฏิบัติ ดังนี้

๑) กำหนดเป้าหมายของระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต โดยพิจารณาถึงโครงสร้างและองค์ประกอบของเว็บไซต์

๒) กำหนดความต้องการของระบบ โดยพิจารณาอุปกรณ์และเครื่องมือที่ใช้ลักษณะการเชื่อมต่อระบบเครือข่าย สถานที่ตั้ง และเทคโนโลยี จะต้องมีองค์ประกอบดังนี้

๒.๑) อุปกรณ์และเครื่องที่เลือกใช้ พิจารณาจากทรัพยากรที่ติดตั้งอยู่ ณ ห้องควบคุมระบบเครือข่าย Network กรมพัฒนาที่ดิน ซึ่งมีอยู่ ไม่มีค่าใช้จ่ายในการพัฒนาระบบ มีความเสถียรและมีประสิทธิภาพ จึงเลือกใช้เครื่องแม่ข่ายในลักษณะเครื่องแม่ข่ายเสมือน เนื่องจากระบบที่พัฒนาไม่มีการประมวลผลที่ซับซ้อน จึงแบ่งทรัพยากรที่กรมพัฒนาที่ดิน มีอยู่ก็เพียงพอต่อการพัฒนาระบบ เลือกใช้ระบบปฏิบัติการ เซ็นโอเอส เวอร์ชั่น ๗ (CentOS7) เนื่องจากมีความเสถียร ไม่มีค่าใช้จ่าย และเลือกใช้โปรแกรมเว็บเซิร์ฟเวอร์เอนจิ้นเอ็ก (Nginx) เนื่องจากเป็นโปรแกรมเว็บเซิร์ฟเวอร์ที่เกิดขึ้นใหม่ โดยนำข้อเสียจากโปรแกรมเว็บเซิร์ฟเวอร์ตัวอื่นมาเป็นตัวอย่างในการพัฒนาโปรแกรมให้มีความเสถียรยิ่งขึ้น

๒.๒) การวางแผนกำหนดค่าโปรแกรมอรรถประโยชน์ เพื่อลดปริมาณการรับ-ส่งข้อมูลในระบบเครือข่ายให้เหมาะสมกับการให้บริการ

๒.๓) การวางแผนกำหนดค่าโปรแกรมอรรถประโยชน์ เพื่อลดช่องโหว่การโจมตีเว็บไซต์ของระบบให้เหมาะสมกับการให้บริการ

๓) การวางแผนเพื่อปรับปรุงรูปแบบการเชื่อมโยงระบบเครือข่ายการให้บริการเว็บไซต์ การปรับปรุงการกำหนดค่าอุปกรณ์ ไฟร์วอลล์ เพื่อให้ระบบสามารถใช้งานได้เต็มประสิทธิภาพ

๔) รูปแบบการประเมินผลระบบตัวแทนการให้บริการเว็บไซต์

๓.๕.๒.๒ พัฒนาระบบตัวแทนการให้บริการเว็บไซต์ (Do) ควรปฏิบัติ ดังนี้

๑) จัดทำระบบตัวแทนการให้บริการเว็บไซต์ตามแผนที่ได้กำหนดไว้

๑.๑) สร้างเครื่องแม่ข่ายเสมือน (Visual Machine)

๑.๒) ติดตั้งระบบปฏิบัติการเซ็นโอเอส เวอร์ชั่น ๗ (CentOS7)

๑.๓) กำหนดค่าการทำงานของระบบตัวแทนการให้บริการเว็บไซต์ (Reverse Proxy) โดยการติดตั้งและกำหนดค่าผ่านโปรแกรมเอนจิ้นเอ็ก (Nginx)

๒) ปรับปรุงการกำหนดค่าโปรแกรมอรรถประโยชน์ เพื่อลดการรับ-ส่งข้อมูลในระบบเครือข่ายตามแผนที่ได้กำหนดไว้

๓) ปรับปรุงการกำหนดค่าโปรแกรมอรรถประโยชน์ เพื่อลดช่องโหว่การโจมตีเว็บไซต์ของระบบตามแผนที่ได้กำหนดไว้

๔) กำหนดค่าอุปกรณ์ที่เกี่ยวข้องในระบบเครือข่ายให้เป็นไปตามรูปแบบการเชื่อมโยงตามแผนที่ได้กำหนดไว้

๓.๕.๒.๓ ตรวจสอบการทำงานระบบตัวแทนการให้บริการเว็บไซต์ (Check) ควรปฏิบัติดังนี้

๑) ตรวจจับข้อผิดพลาดในการแสดงผลเว็บไซต์

๑.๑) ตรวจสอบข้อผิดพลาดจากการแสดงผลเว็บไซต์

๑.๒) เฝ้าระวังและตรวจสอบผลของการปรับปรุงระบบเครือข่ายที่เกี่ยวข้องกับการเปลี่ยนแปลง

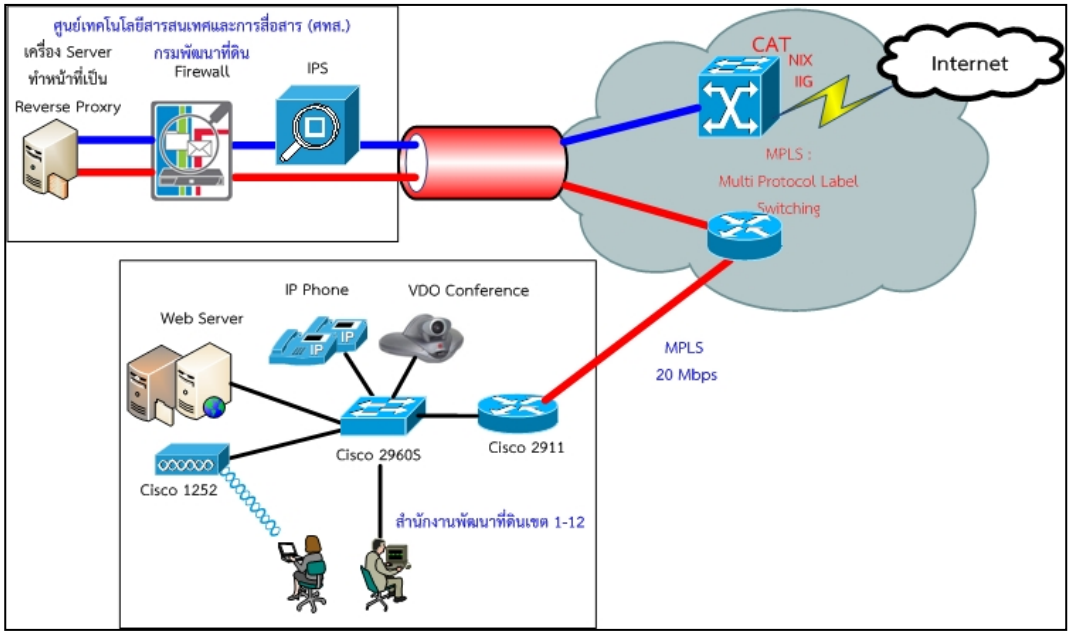
๒) ดำเนินการทบทวนความสัมฤทธิผลของระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต ได้แก่ ช่วงเวลาที่เปลี่ยนแปลงไปในดาวน์โหลดข้อมูล เป็นต้น

๓.๕.๒.๔ บำรุงรักษาระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต (Act) ควรปฏิบัติ ดังนี้

๑) ปรับปรุงระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต

๒) ตรวจสอบว่าการปรับปรุงที่ทำไปแล้วนั้นบรรลุตามวัตถุประสงค์ที่กำหนดไว้หรือไม่

๓) จัดทำเอกสารที่ใช้ในการบำรุงรักษาระบบตัวแทนการให้บริการเว็บไซต์



ภาพที่ ๓ – ๓ รูปแบบการเชื่อมต่อระบบเครือข่ายที่ให้บริการผ่านระบบตัวแทนการให้บริการเว็บไซต์ (Reverse Proxy)

๓.๖ ขั้นตอนการให้บริการเว็บไซต์ของหน่วยงานส่วนภูมิภาค กรมพัฒนาที่ดิน ผ่านระบบตัวแทนการให้บริการเว็บไซต์ (Reverse Proxy)

การให้บริการเว็บไซต์ของหน่วยงานส่วนภูมิภาค กรมพัฒนาดิน สำหรับบุคคลที่สนใจและอยู่ภายนอกเครือข่ายกรมพัฒนาที่ดิน โดยผ่านระบบตัวแทนการให้บริการเว็บไซต์ (Reverse Proxy) จะมีการเชื่อมต่อโดยอุปกรณ์ที่มีหน้าที่แตกต่างและมีขั้นตอนดังนี้

ขั้นตอนที่ ๑ เมื่อมีผู้สนใจเรียกใช้งานเว็บไซต์ จากอุปกรณ์หรือคอมพิวเตอร์ที่อยู่ภายนอกเครือข่ายกรมพัฒนาที่ดิน คอมพิวเตอร์เครื่องดังกล่าวจะส่งข้อมูลความต้องการเรียกใช้งานเว็บไซต์ บรรจุลงไปในแพ็กเก็ต (Packet) และส่ง Packet ในระบบเครือข่ายไปยังไอเอสพี (Internet service provider :ISP) ที่มีเชื่อมต่ออยู่ และISP จะส่ง Packet ผ่านการเชื่อมต่ออินเทอร์เน็ต มายัง ISP บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

ขั้นตอนที่ ๒ เมื่ออุปกรณ์เครือข่ายที่ของ ISP บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ได้รับ Packet ดังกล่าว จะทำการตรวจสอบและส่ง Packet ดังกล่าวไปยังอุปกรณ์เครือข่ายของ กรมพัฒนาที่ดิน ผ่านมาตรฐาน MPLS

ขั้นตอนที่ ๓ เมื่ออุปกรณ์เครือข่ายกรมพัฒนาที่ดิน ส่วนกลาง ได้รับ Packet ดังกล่าวจะทำการตรวจสอบความผิดปกติในการส่ง Packet โดย IPS เมื่อ Packet นั้นไม่มีความผิดปกติ จะทำการส่งต่อไปยังอุปกรณ์ไฟร์วอลล์เพื่อทำการ NAT เมื่อเสร็จสิ้นจะทำการส่ง Packet ผ่านอุปกรณ์ต่าง ๆ ภายใน กรมพัฒนาที่ดิน เพื่อส่งข้อมูลไปยังเครื่องแม่ข่ายตัวแทนการให้บริการเว็บไซต์ (Reverse Proxy)

ขั้นตอนที่ ๔ เมื่อเครื่องแม่ข่าย Reverse Proxy ของหน่วยงานส่วนภูมิภาคกรมพัฒนาที่ดิน ซึ่งทำหน้าที่ลักษณะเดียวกันกับเครื่องแม่ข่ายตัวจริง ได้รับ Packet แล้ว ทำการประมวลผลข้อมูล โดยตรวจสอบต่าง ๆ เช่น ความถูกต้องของข้อมูล ลักษณะของข้อมูลที่ไม่มีความเสี่ยง ตามข้อกำหนด (Policy) และทำการตรวจสอบว่าความต้องการของข้อมูลที่เครื่องลูกข่ายต้องการนั้น มีไฟล์แคช (Cache) ข้อมูลเก็บอยู่หรือไม่ ถ้า

ไม่มีจะส่งข้อมูลความต้องการดังกล่าวไปยังเว็บไซต์จริง เมื่อเครื่องแม่ข่ายจริงได้รับความต้องการแล้ว เครื่องแม่ข่ายจะประมวลผล และส่งข้อมูลตามความต้องการกลับมายังเครื่อง Reverse Proxy เหมือนกับการทำงานระหว่างเครื่องแม่ข่ายให้บริการเครื่องลูกข่าย เมื่อเครื่อง Reverse Proxy ได้รับข้อมูลที่สมบูรณ์แล้ว จะทำจัดเก็บข้อมูลในไฟล์ Cache ถ้าเกิดมีการเรียกใช้ข้อมูลเว็บไซต์ในลักษณะเดียวกัน เครื่อง Reverse Proxy จะไม่ต้องทำการข้อมูลไปยังเครื่องแม่ข่ายจริง แต่จะนำข้อมูลที่เก็บอยู่ในไฟล์ Cache จัดทำชุดข้อมูลและส่งกลับไปยังเครื่องลูกข่ายที่ต้องการข้อมูลได้เอง หลังจากที่เครื่อง Reverse Proxy จัดทำข้อมูลเสร็จสิ้นและจัดส่งกลับไปในรูปแบบ Packet ส่งไปยังอุปกรณ์เครือข่าย กรมพัฒนาที่ดิน ส่วนกลาง

ขั้นตอนที่ ๕ เมื่ออุปกรณ์เครือข่าย กรมพัฒนาที่ดิน ส่วนกลาง ได้รับ Packet แล้ว อุปกรณ์ไฟร์วอลล์ จะทำการ NAT เป็น Public IP address และส่ง Packet ไปยัง ISP บริษัท กสท โทรคมนาคม จำกัด (มหาชน) เพื่อส่งข้อมูลเครื่องลูกข่าย

ขั้นตอนที่ ๖ เมื่ออุปกรณ์เครือข่าย บริษัท กสท โทรคมนาคม จำกัด (มหาชน) ได้รับ Packet แล้วจะส่ง Packet กลับไปยัง ISP ของเครื่องลูกข่าย เพื่อส่งข้อมูลไปยังเครื่องลูกข่าย เมื่อเครื่องลูกข่ายได้รับ Packet จะแปลง Packet ที่ได้รับ เป็นข้อมูลเพื่อให้แสดงผลข้อมูล เป็นเสร็จสิ้นข้อมูลกระบวนการให้เว็บไซต์ของหน่วยงานส่วนภูมิภาคผ่านระบบตัวแทนการให้บริการเว็บไซต์ (Reverse Proxy) ตามภาพที่ ๓ – ๓

บทที่ ๔
การพัฒนาระบบ

การพัฒนาระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต ดำเนินงานตามการวางแผนที่ได้กำหนดไว้ และจัดหาอุปกรณ์และเครื่องมือที่ใช้ในการพัฒนา โดยจัดสรรจากทรัพยากรเดิมที่มีอยู่ จัดหาและติดตั้งโปรแกรมจากแหล่งที่มีความน่าเชื่อถือและปลอดภัย เพื่อป้องกันการถูกแนบไฟล์ไม่พึงประสงค์ ซึ่งอาจเป็นช่องทางการถูกโจมตีในอนาคต รวมถึงชุดคำสั่งที่นำมาปรับใช้กับโปรแกรมต้องศึกษาและเข้าใจรายละเอียดเพื่อทำไปใช้ในการพัฒนาระบบได้อย่างมีประสิทธิภาพ

๔.๑ อุปกรณ์และเครื่องมือที่ใช้

ในการพัฒนาระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต ใช้อุปกรณ์และโปรแกรมสำหรับสนับสนุนการดำเนินการ ดังนี้

๔.๑.๑ เครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาระบบ ประกอบด้วย CPU I๗-๓๗๗๐ , HDD ขนาดความจุ ๑๕๐ GB, RAM ขนาด ๔ GB

๔.๑.๒ โปรแกรมสนับสนุน ประกอบด้วย ระบบปฏิบัติการ Windows ๗, โปรแกรม VMware vSphere Client โปรแกรม putty, โปรแกรม WinSCP, โปรแกรม Google Chrome

๔.๑.๓ เครื่องสนับสนุนการติดตั้งเซิร์ฟเวอร์ เป็นเครื่องแม่ข่ายที่ได้ติดตั้งอีเอสเอ็กไอ เซิร์ฟเวอร์เวอร์ชั่น ๕.๕ (ESXi Server Version ๕.๕ standard :ESXi) สำหรับใช้ในการติดตั้งระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต ที่มี CPU จำนวน ๑ CPU,จำนวน ๘ Core ต่อ CPU , HDD ขนาดความจุ ๕๐ GB, และ RAM ขนาด ๔ GB

๔.๑.๔ โปรแกรมที่ใช้ในการพัฒนาระบบประกอบด้วย ระบบปฏิบัติการเซ็นโอเอส เวอร์ชั่น ๗ (CentOS 7) และโปรแกรมเอนจิ้นเอ็ก (Nginx)

๔.๒ ขั้นตอนการติดตั้งและบริหารจัดการระบบ

๔.๒.๑ ทำการสร้างเครื่องแม่ข่ายเสมือน (Visual Machine) บน ESXi ของ กรมพัฒนาที่ดิน

๔.๒.๒ ทำการติดตั้งระบบปฏิบัติการ CentOS 7 บนเครื่องแม่ข่ายเสมือน ทำการเชื่อมต่อระบบเครือข่ายของ กรมพัฒนาที่ดิน และปรังปรุงระบบปฏิบัติการให้เป็นปัจจุบัน

๔.๒.๓ ทำการติดตั้งโปรแกรม Nginx เป็นโปรแกรมที่ทำหน้าที่เว็บเซอรวิส ซึ่งกำหนดให้เป็นบริการพร็อกซีของเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต

๔.๒.๓.๑ ติดตั้งโปรแกรมเอนจิ้นเอ็ก และปรับปรุงการกำหนดค่าโปรแกรมอรรถประโยชน์เพื่อลดการรับ-ส่งข้อมูลในระบบเครือข่าย

๔.๒.๓.๒ ปรับปรุงการกำหนดค่าโปรแกรมอรรถประโยชน์ ให้สามารถแทนการเรียกใช้งานเว็บไซต์

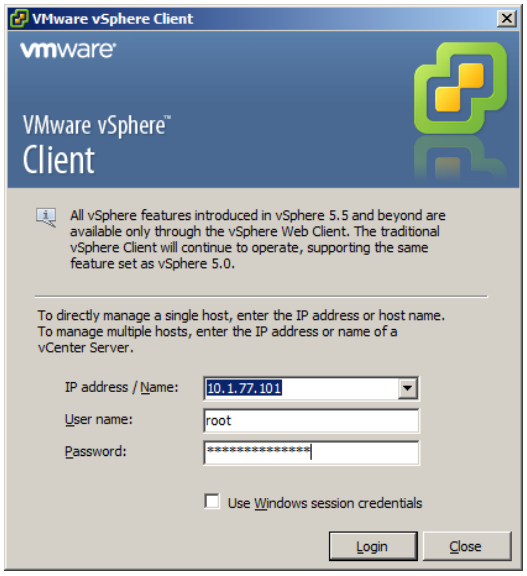
๔.๒.๓.๓ ปรับปรุงการกำหนดค่าโปรแกรมอรรถประโยชน์ เพื่อลดการรับ-ส่งข้อมูล และลดช่องโหว่การโจมตีเว็บไซต์ของระบบ

๔.๒.๔ ทำการปรับปรุงการกำหนดค่าอุปกรณ์ ไฟร์วอลล์ ให้สามารถรองรับการพัฒนาระบบนี้ได้

๔.๓ การดำเนินการติดตั้ง

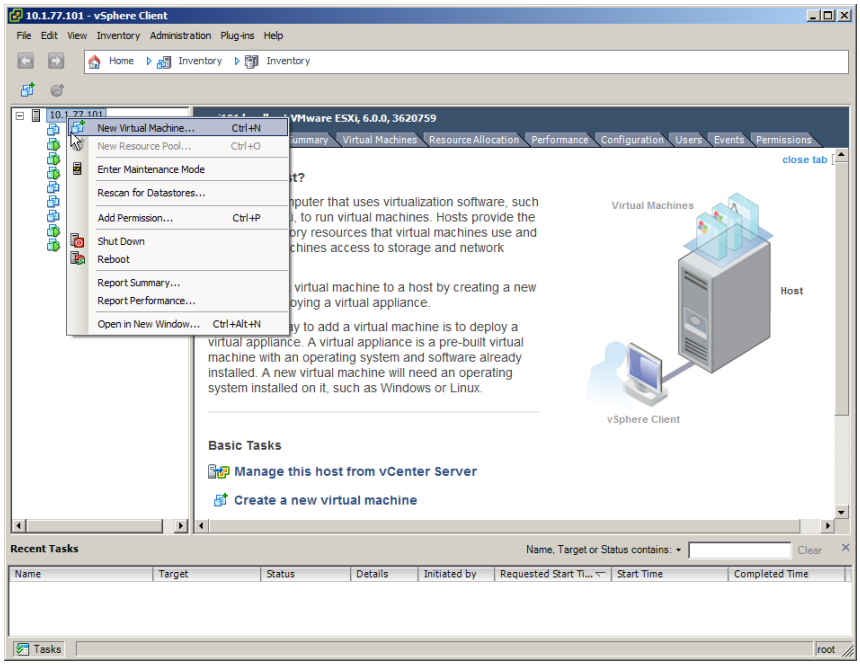
๔.๓.๑ การสร้างเครื่องแม่ข่ายเสมือน(Visual Machine)

๔.๓.๑.๑ นำเครื่องคอมพิวเตอร์สนับสนุนเรียกใช้โปรแกรม VMware vSphere Client เพื่อเชื่อมต่อ โดยใส่ค่าไอพีแอดเดรส (IP Address) 10.1.77.101 **ชื่อผู้ใช้** (Username) root และ**รหัสผ่าน** (Password) ที่ได้รับสิทธิในการบริหารจัดการเครื่องแม่ข่าย ESXi



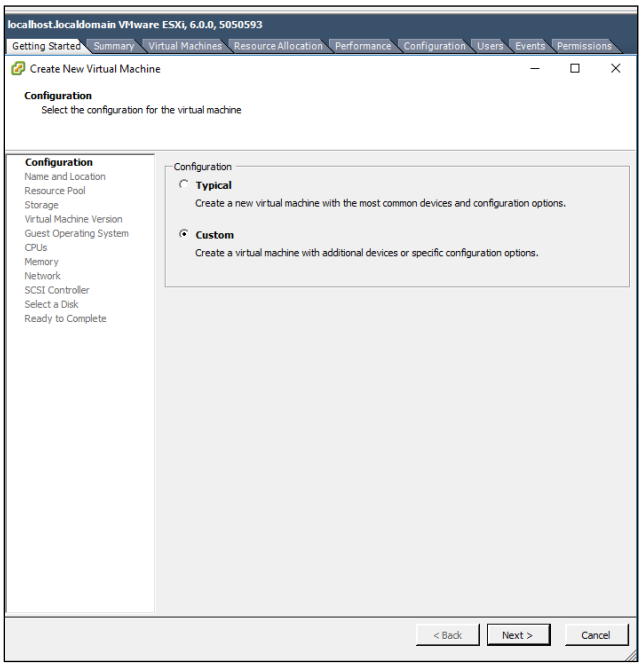
ภาพที่ ๔ – ๑ การระบุไอพีแอดเดรส ชื่อผู้ใช้ และรหัสผ่าน เพื่อเชื่อมต่อเครื่องแม่ข่าย ESXi

๔.๓.๑.๒ การคลิกขวาที่รูปเครื่องแม่ข่าย 10.1.77.101 และเลือก New Virtual Machine



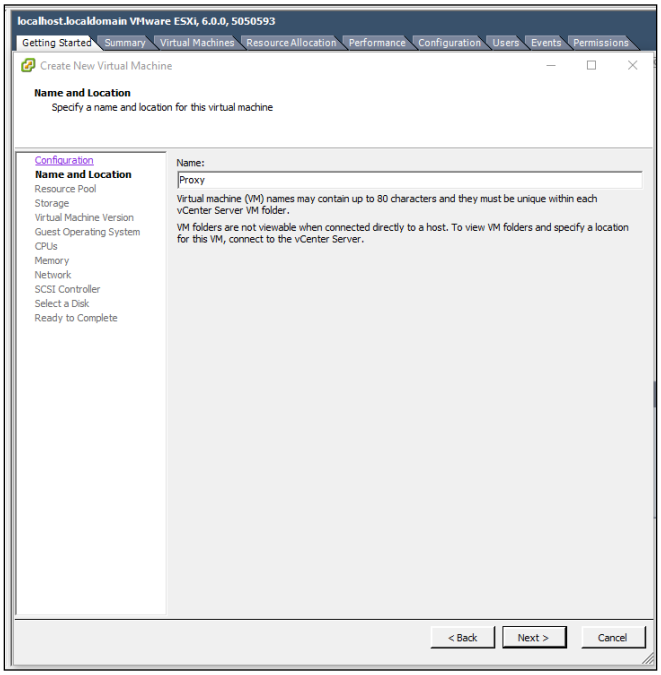
ภาพที่ ๔ – ๒ การเลือก New Virtual Machine เพื่อสร้างเครื่องข่ายเสมือน

๔.๓.๑.๓ กำหนดค่าลักษณะการคอนฟิกูเรชัน (configuration) โดยเลือกรูปแบบกำหนดค่าเอง เลือก Custom เพื่อที่สามารถกำหนดรายละเอียดการติดตั้งตามรูปแบบที่ต้องการ



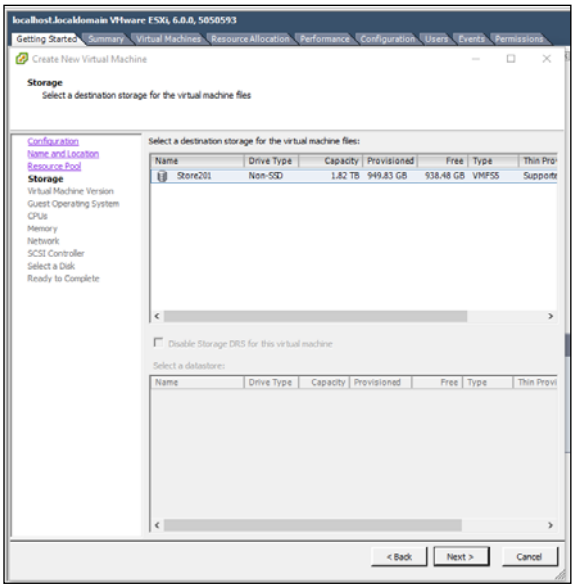
ภาพที่ ๔ – ๓ การเลือกลักษณะการคอนฟิกูเรชัน

๔.๓.๑.๔ กำหนดค่าชื่อเครื่องแม่ข่ายเสมือนโดยใช้ชื่อ Proxy



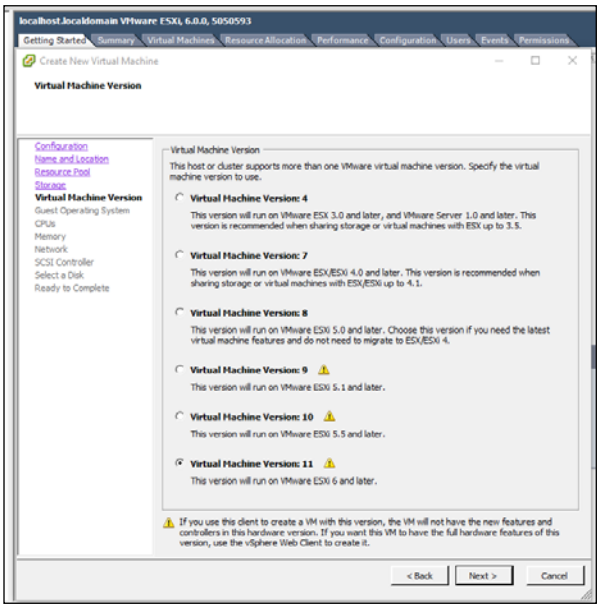
ภาพที่ ๔ – ๔ การกำหนดค่าชื่อเครื่องแม่ข่ายเสมือน

๔.๓.๑.๕ กำหนดค่าพื้นที่จัดเก็บ (Storage) ของเครื่องแม่ข่ายเสมือน โดยเลือก Store201



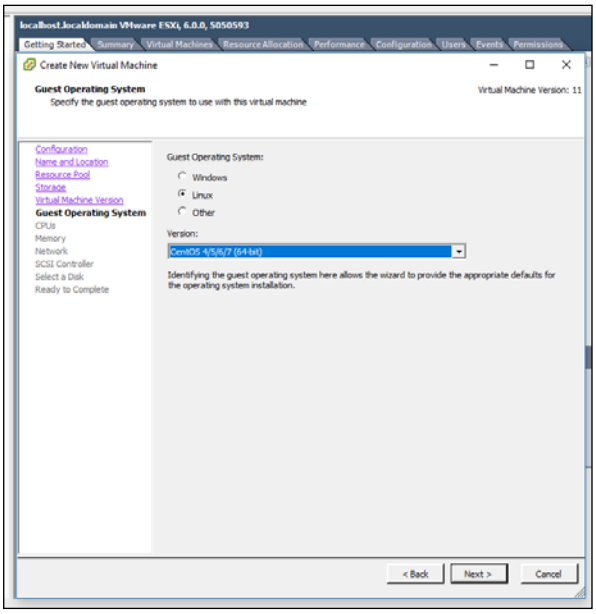
ภาพที่ ๔ – ๕ การเลือกพื้นที่จัดเก็บ

๔.๓.๑.๖ การกำหนดค่าเวอร์ชั่นเครื่องแม่ข่ายเสมือน Virtual Machine ที่ต้องการติดตั้งโดยเลือกเป็นเวอร์ชั่น Virtual Machine Version 11 ซึ่งเป็น Version ล่าสุด



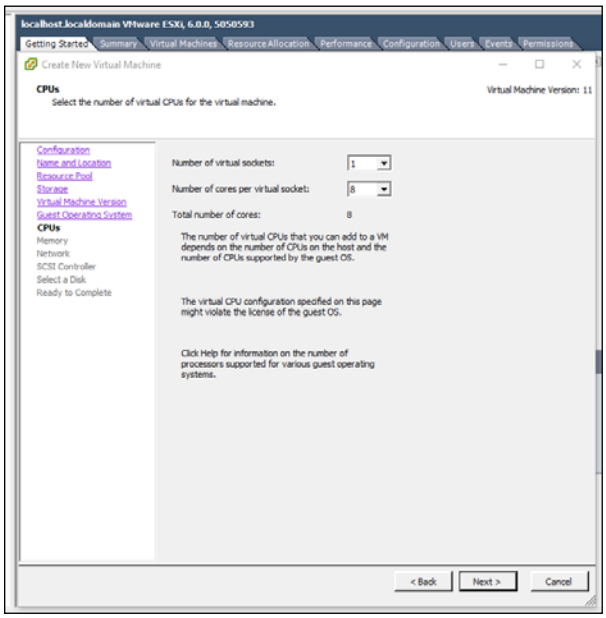
ภาพที่ ๔ – ๖ การกำหนดค่าเวอร์ชั่นเครื่องแม่ข่ายเสมือน

๔.๓.๑.๗ การกำหนดค่าระบบปฏิบัติการของเครื่องแม่ข่ายเสมือนที่ติดตั้งโดยกำหนดค่าเป็น CentOS 4/5/6/7 (64bit)



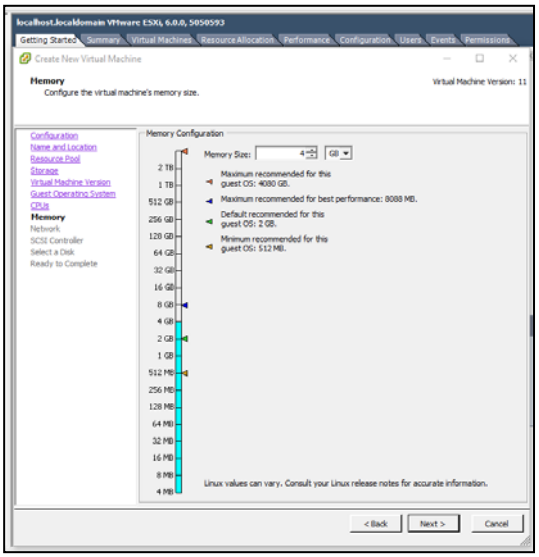
ภาพที่ ๔ – ๗ การกำหนดค่าระบบปฏิบัติการของเครื่องแม่ข่ายเสมือนที่ทำการติดตั้ง

๔.๓.๑.๘ การกำหนดค่าจำนวนซีพียู (CPUs) และจำนวนคอร์ต่อซีพียู (Core of CPU) ของเครื่องแม่ข่ายเสมือน กำหนดจำนวนซีพียูให้ค่าเท่ากับ ๑ ซีพียู และจำนวนคอร์ต่อซีพียูเท่ากับ ๘ คอร์ด



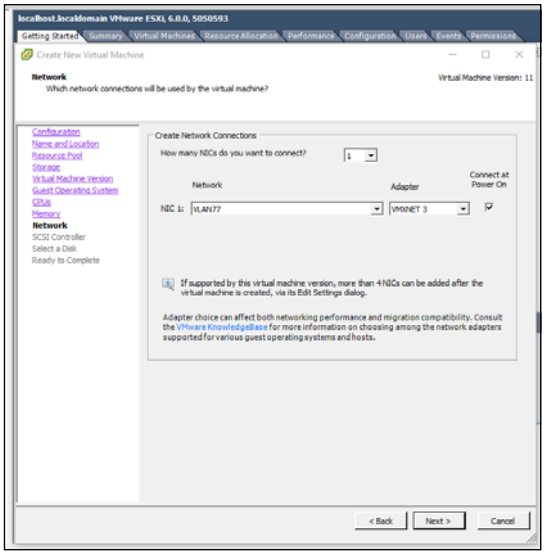
ภาพที่ ๔ – ๘ การกำหนดค่าจำนวนซีพียู (CPUs) และจำนวนคอร์ต่อซีพียู (Core of CPU) ของเครื่องแม่ข่ายเสมือน

๔.๓.๑.๙ การกำหนดค่าขนาดเมมโมรี่ (Memory) ของระบบปฏิบัติการของเครื่องแม่ข่ายเสมือน กำหนดค่าขนาด ๔ GB



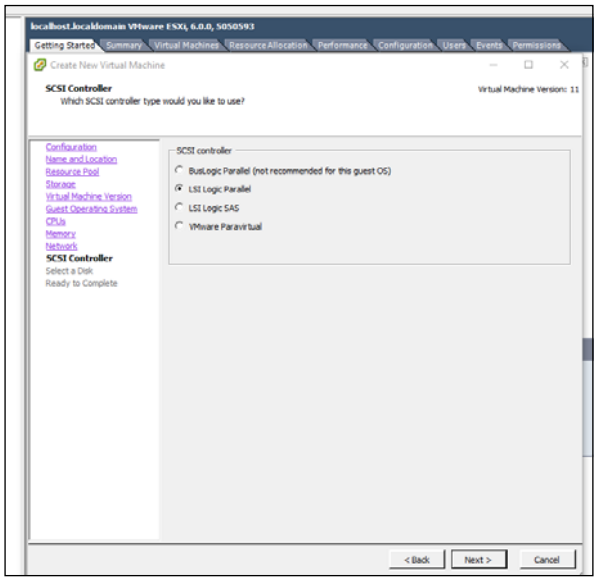
ภาพที่ ๔ – ๙ การกำหนดค่าขนาดเมมโมรี่ (Memory) ของระบบปฏิบัติการเครื่องแม่ข่ายเสมือน

๔.๓.๑.๑๐ การกำหนดค่าจำนวนอินเตอร์เฟส (interface) ที่ใช้ในการเชื่อมต่อระบบเครือข่ายและวีแลน (Vlan) ที่เครื่องแม่ข่ายเสมือนเชื่อมต่อระบบเครือข่าย โดยเลือกจำนวนการ์ดเน็ตเวิร์ค NICs จำนวน ๑ interface และกำหนดค่า VLAN77 เพื่อใช้ในการเชื่อมต่อกับวีแลนหมายเลข ๗๗ ของกรมพัฒนาที่ดินที่ได้ประกาศใช้ไว้ และเลือก Adapter ที่ใช้ในการเชื่อมต่อกับเครื่องแม่ข่ายเสมือนเท่ากับ VMXNET 3 และเลือกทำเครื่องหมายคลิก Connect at Power On เพื่อทุกครั้งที่ทำการเปิดเครื่องเน็ตเวิร์คจะเชื่อมต่อระบบเครือข่าย



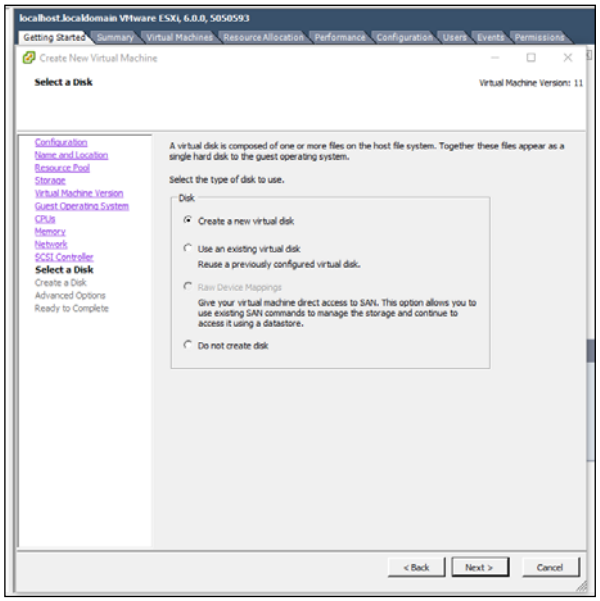
ภาพที่ ๔ – ๑๐ การเลือกจำนวน interface การเชื่อมต่อระบบเครือข่ายเครื่องแม่ข่ายเสมือน

๔.๓.๑.๑๑ การกำหนดค่ารูปแบบลักษณะการเชื่อมต่อและควบคุม (SCSI Controller) ดิสก์ (Disk) ระบบปฏิบัติการของเครื่องแม่ข่ายเสมือน โดยกำหนดค่ารูปแบบเป็น LSI logic Parallel



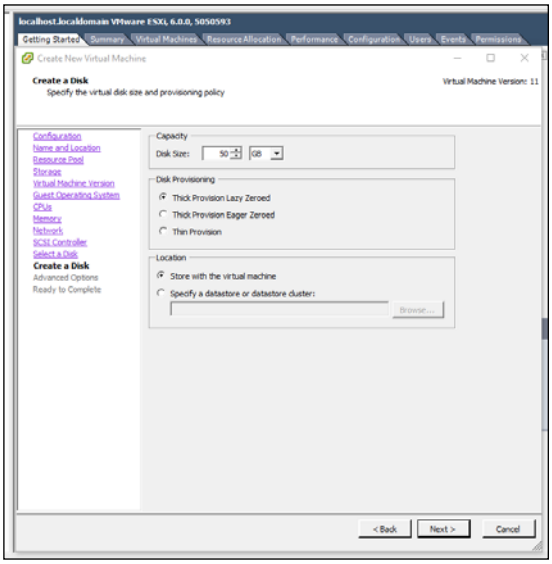
ภาพที่ ๔ – ๑๑ การกำหนดค่ารูปแบบลักษณะการเชื่อมต่อและควบคุมดิสก์ระบบปฏิบัติการของเครื่องแม่ข่ายเสมือน

๔.๓.๑.๑๒ การกำหนดค่าใช้งานลักษณะของดิสก์ (Disk) ระบบปฏิบัติการของเครื่องแม่ข่ายเสมือน โดยกำหนดค่าลักษณะการสร้างใหม่ คือ Create a new virtual disk



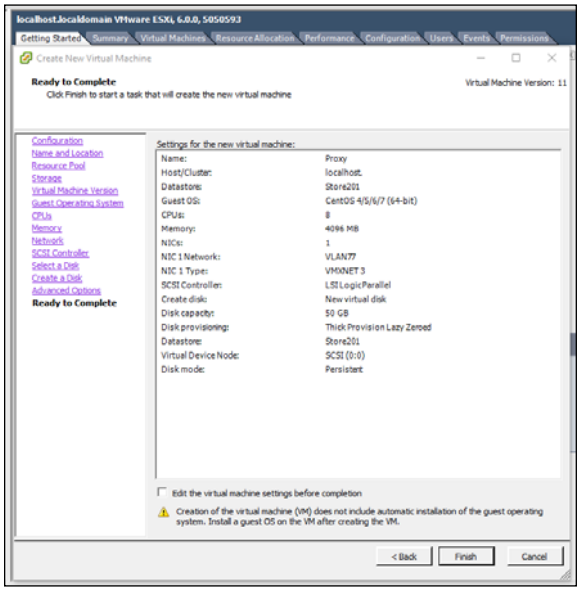
ภาพที่ ๔ – ๑๒ การกำหนดค่าใช้งานลักษณะของดิสก์ (Disk) ระบบปฏิบัติการของเครื่องแม่ข่ายเสมือน

๔.๓.๑.๑๓ การกำหนดค่าขนาดของพื้นที่ดิสก์ระบบปฏิบัติการของเครื่องแม่ข่ายเสมือนโดยกำหนดค่าให้มีขนาดพื้นที่เท่ากับ ๕๐ GB กำหนดรูปแบบ Disk Provisioning เป็นรูปแบบ Think Provision Lazy Zeroed และกำหนดค่าสถานที่จัดเก็บข้อมูล (Location) คือ Store with the virtual machine



ภาพที่ ๔ – ๑๓ การกำหนดค่าขนาดของพื้นที่ดิสก์ระบบปฏิบัติการของเครื่องแม่ข่ายเสมือน

๔.๓.๑.๑๔ หน้าจอแสดงผลสรุปการกำหนดค่าเครื่องแม่ข่ายเสมือนเพื่อทบทวนการกำหนดค่าต่าง ๆ การสร้าง Virtual Machine โดยกด Finish เป็นการเริ่มสร้างเครื่องแม่ข่ายเสมือนที่ได้กำหนดไว้

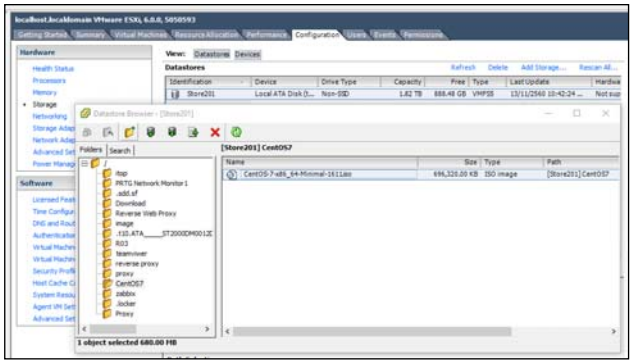


ภาพที่ ๔ – ๑๔ หน้าจอแสดงผลสรุปการกำหนดค่าเครื่องแม่ข่ายเสมือน

๔.๓.๒ การติดตั้งระบบปฏิบัติการเซนต์โอเอสเวอร์ชั่น ๗

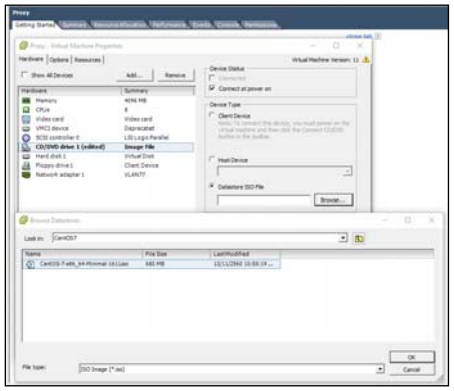
ทำการดาวน์โหลดไฟล์อิมเมจ (Image) ของระบบระบบปฏิบัติการเซนต์โอเอสเวอร์ชั่น ๗ ตาม URL: http://mirror1.ku.ac.th/CentOS-cd-dvd/CentOS-7-x86_64-Minimal-1161.iso โดยให้ทำการ ดาวน์โหลดไฟล์ เป็นไฟล์รูปแบบ Minimal Install ซึ่งจะทำให้ระบบปฏิบัติการมีขนาดเล็กและจะติดตั้งเฉพาะตัวระบบปฏิบัติการ และเครื่องมือที่จำเป็นเท่านั้น ทำให้ลดความเสี่ยงจากโปรแกรมต่างที่ไม่ได้ใช้งาน และมีความปลอดภัยกว่าที่ติดตั้งแบบเต็มรูปแบบ (Full)

๔.๓.๓.๓ ทำการนำเข้าไฟล์อิมเมจ (Image) ที่ใช้ในการติดตั้ง จัดเก็บที่เครื่องแม่ข่าย ESXi ที่หัวข้อ configuration > Datastores > storage201() > CentOS7



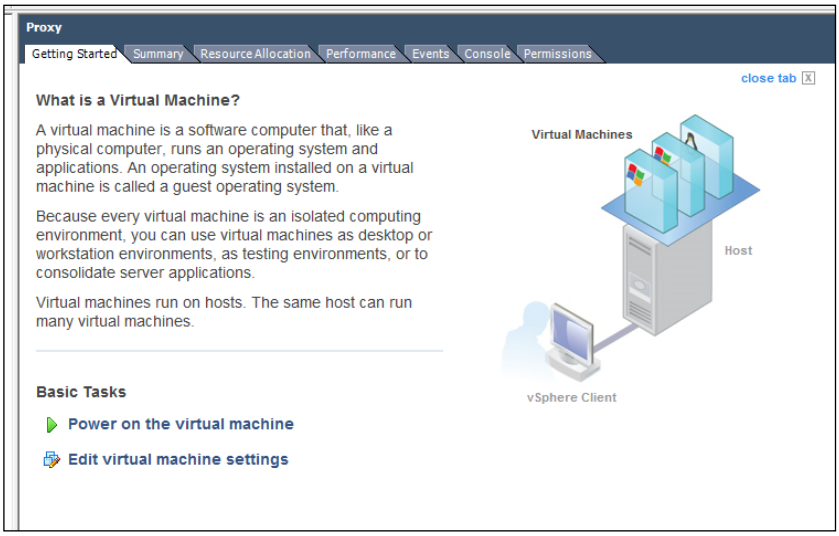
ภาพที่ ๔ – ๑๕ การนำไฟล์ Image ที่ใช้ในการติดตั้ง จัดเก็บที่เครื่อง ESXi

๔.๓.๓.๔ ทำการตั้งค่าเรียกใช้งาน Image เพื่อติดตั้ง CentOS7 โดย click ขวาที่เครื่องแม่ข่ายเสมือนที่ได้สร้างไว้ในขั้นตอนที่ ๑.๑ เลือก Setting > CD/DVD drive > Datastore ISO File > Browse ทำการเลือกไฟล์ Image ที่ทำการ upload ไว้ click OK



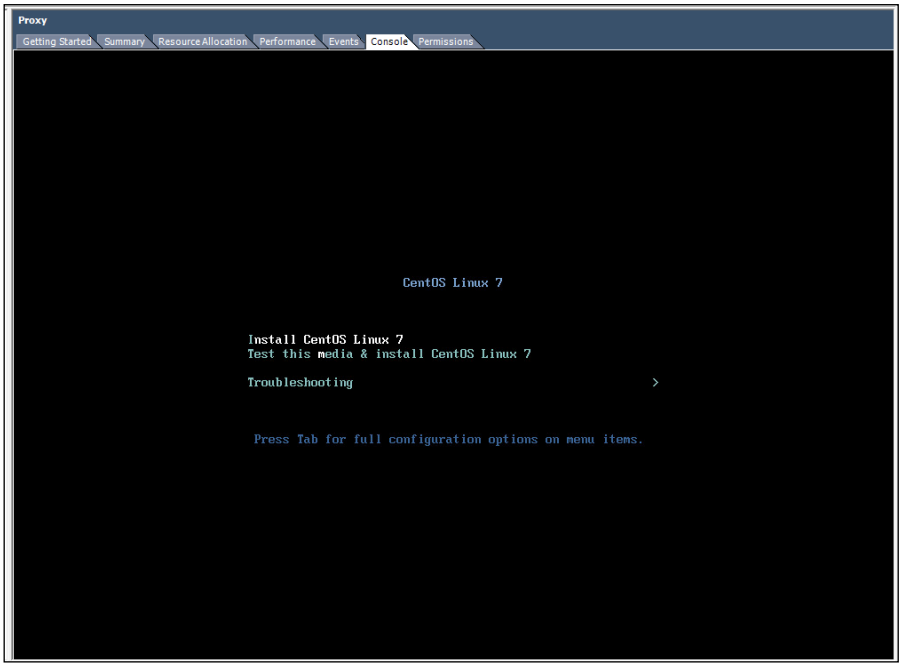
ภาพที่ ๔ – ๑๖ การกำหนดค่าเรียกใช้งาน Image เพื่อติดตั้ง เซนต์โอเอสเวอร์ชั่น ๗

๔.๓.๓.๕ ทำการเปิดเครื่องแม่ข่ายเสมือน เพื่อเริ่มต้นติดตั้งระบบปฏิบัติการเซนต์โอเอสเวอร์ชั่น ๗ โดยกดเลือกแถบบาร์ Getting started และคลิกเลือกข้อมูล Power on the virtual machine เพื่อเปิดเครื่องแม่ข่ายเสมือน



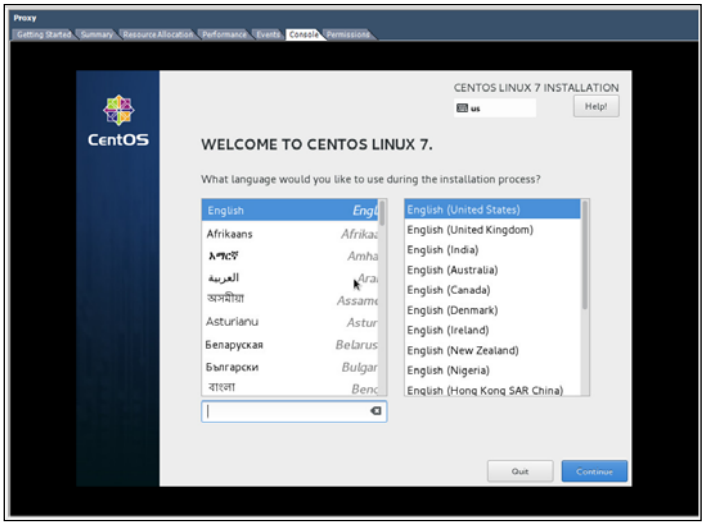
ภาพที่ ๔ – ๑๗ การเปิดเครื่องแม่ข่ายเสมือน

๔.๓.๓.๖ ทำการเลือกแถบบาร์ Console เพื่อควบคุมเครื่องแม่ข่ายเสมือนในการติดตั้งระบบ ปฏิบัติการ และ เลือก Install CentOS Linux 7 แล้วกด Enter เพื่อเริ่มต้นติดตั้ง



ภาพที่ ๔ – ๑๘ จอภาพแสดงการเริ่มต้นขั้นตอนติดตั้งระบบปฏิบัติการ

๔.๓.๓.๗ เข้าสู่หน้าจอ ต้อนรับการติดตั้งระบบปฏิบัติการทำการเลือกภาษอังกฤษ English เพื่อใช้ในกระบวนการติดตั้งระบบ แล้วกดปุ่ม Continue

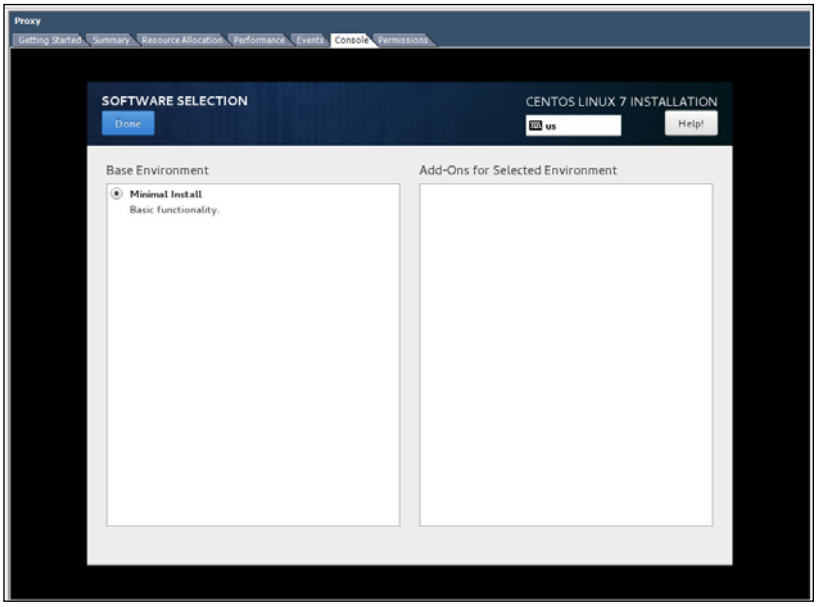


ภาพที่ ๔ – ๑๙ จอภาพแสดงเข้าสู่หน้าจอ ต้อนรับการติดตั้งระบบปฏิบัติการ

๔.๓.๓.๘ ทำการกำหนดค่าเวลาและช่วงเวลา (Time Zone) ของระบบปฏิบัติการ โดยกำหนดค่าเป็นเวลาปัจจุบันและเลือกทวีป Region เป็น Asia เมืองเป็น Bangkokแล้วทำการกดปุ่ม Done

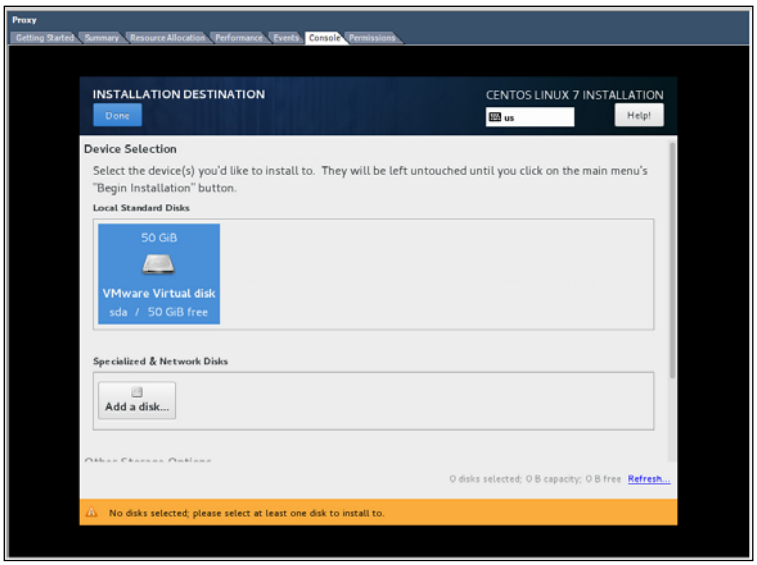
ภาพที่ ๔ – ๒๐ จอภาพแสดงการกำหนดค่าเวลาและช่วงเวลา

๔.๓.๓.๙ แสดงรายละเอียดการเลือกติดตั้งโปรแกรมที่ติดตั้งพร้อมกับระบบปฏิบัติการ และทำการกดปุ่ม Done



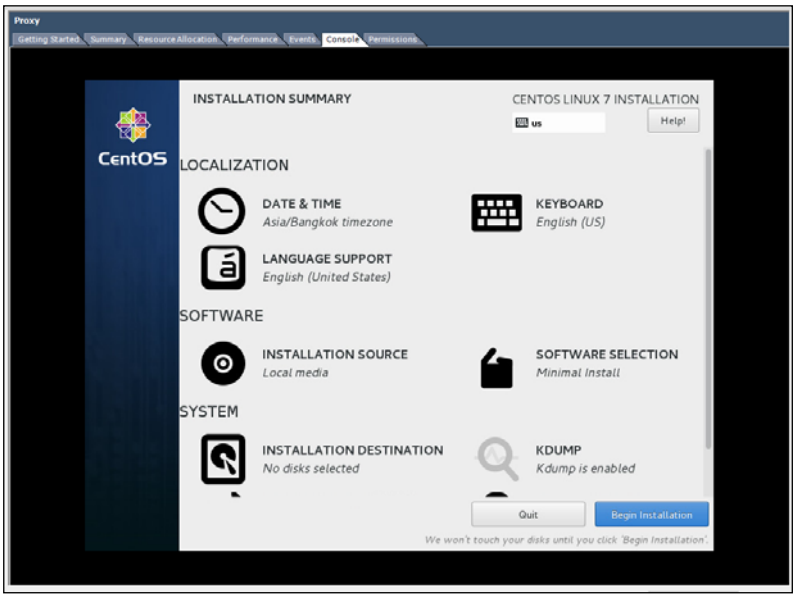
ภาพที่ ๔ – ๒๑ จอภาพแสดงรายละเอียดการเลือกติดตั้งโปรแกรมพร้อมกับระบบปฏิบัติการ

๔.๓.๓.๑๐ ทำการเลือกดิสก์ Disk ที่ต้องการติดตั้ง โดยเลือกดิสก์ VMware virtual disk และทำการกดปุ่ม Done



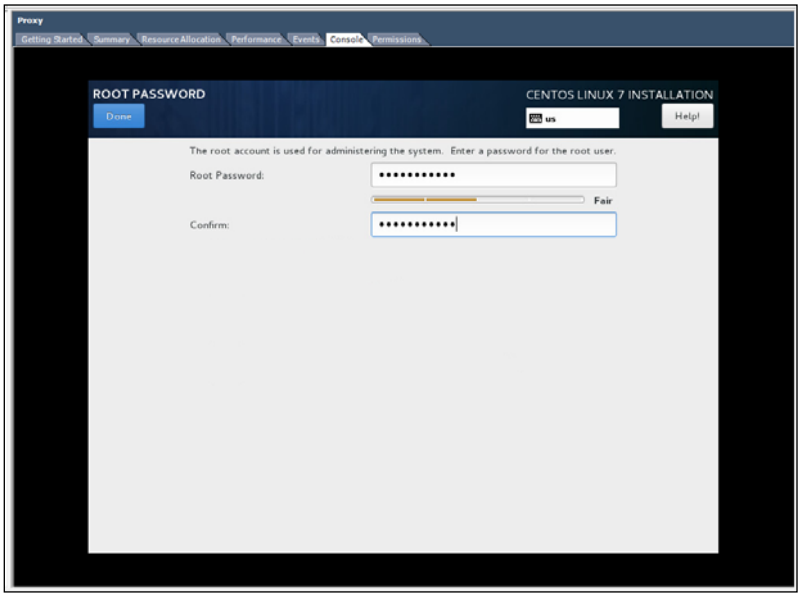
ภาพที่ ๔ – ๒๒ จอภาพแสดงการเลือก Disk ที่ต้องการติดตั้ง

๔.๓.๓.๑๑ แสดงสรุปการกำหนดค่าระบบปฏิบัติการ กดปุ่ม Begin Installation เพื่อเริ่มขั้นตอนการติดตั้ง



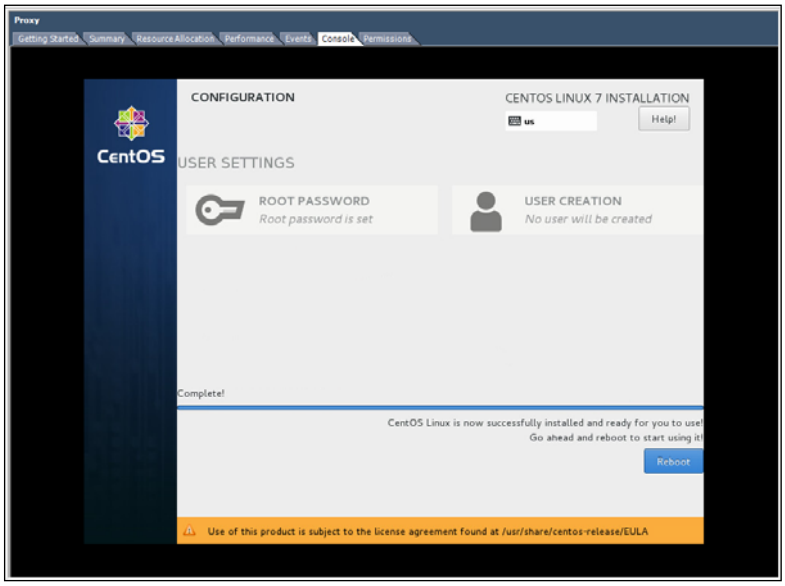
ภาพที่ ๔ – ๒๓ จอภาพแสดงการตรวจสอบการกำหนดค่าให้ถูกต้องก่อนการติดตั้ง

๔.๓.๓.๑๒ ทำการกำหนดค่ารหัสผ่าน (password) ของผู้ใช้สิทธิผู้ดูแลระบบ (root) แล้วกดปุ่ม Done



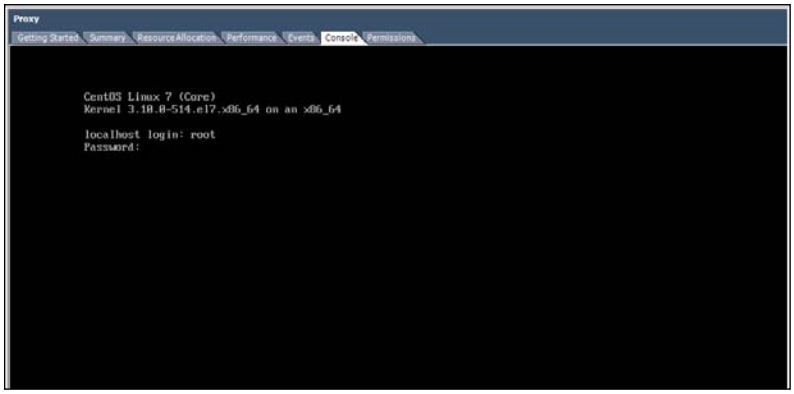
ภาพที่ ๔ – ๒๔ จอภาพแสดงการกำหนดค่ารหัสผ่าน ของผู้ใช้สิทธิผู้ดูแลระบบ

๔.๓.๓.๑๓ แสดงผลเสร็จสิ้นการติดตั้งระบบปฏิบัติการและทำการกด Reboot เพื่อเริ่มต้นระบบปฏิบัติการใหม่



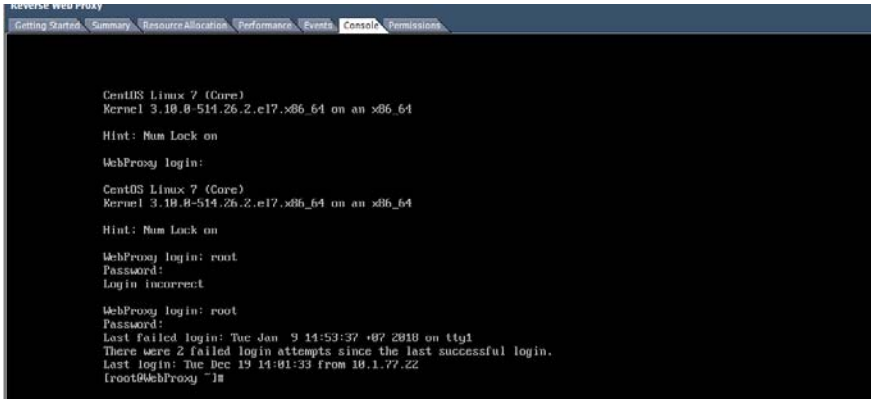
ภาพที่ ๔ – ๒๕ จอภาพแสดงผลเสร็จสิ้นการติดตั้งระบบปฏิบัติการ

๔.๓.๓.๑๔ หลังจากระบบปฏิบัติการเริ่มต้นใหม่ (Reboot) แล้ว ระบบปฏิบัติการพร้อมใช้งาน



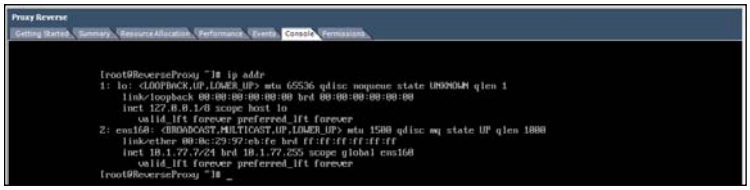
ภาพที่ ๔ – ๒๖ จอภาพแสดงผลการเริ่มต้นระบบปฏิบัติการ

๔.๓.๓.๑๕ ทำการกรอกชื่อผู้ใช้งาน (user) และรหัสผ่าน (password) เพื่อเข้าสู่ระบบ



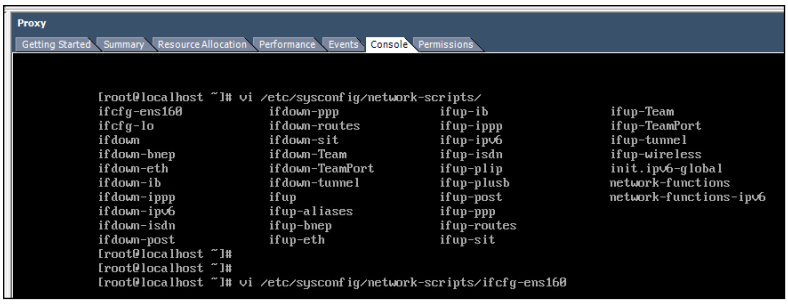
ภาพที่ ๔ – ๒๗ จอภาพแสดงการกรอกชื่อผู้ใช้งานและรหัสผ่านเพื่อเข้าสู่ระบบ

๔.๓.๓.๑๖ การกำหนดค่าไอพีแอสเดส (IP address) การตรวจสอบสถานะการเชื่อมต่อของการ์ดเครือข่าย (Interface Network Card) และชื่อไฟล์ที่ใช้สำหรับควบคุมการ์ดเครือข่าย ที่ใช้ในการเชื่อมโยงระบบเครือข่ายเพื่อนำไปใช้ในการกำหนดค่าเพื่อเชื่อมต่อระบบ โดยใช้คำสั่ง ip addr



ภาพที่ ๔ – ๒๘ จอภาพแสดงการตรวจสอบสถานะการ์ดเครือข่าย (Interface Network card)

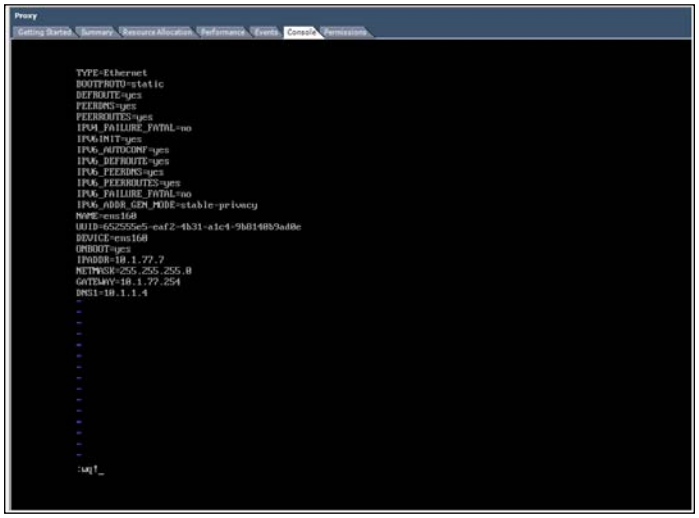
๔.๓.๓.๑๗ กำหนดค่าไฟล์ ifcfg-ens160 เพื่อกำหนดค่าไฟล์คอนฟิกควบคุมการ์ดเครือข่าย ใช้โปรแกรม vi โดยใช้คำสั่ง vi /etc/sysconfig/network-scripts/ifcfg-ens160



ภาพที่ ๔ – ๒๙ จอภาพแสดงการใช้คำสั่งกำหนดค่าไฟล์ควบคุมการ์ดเครือข่าย

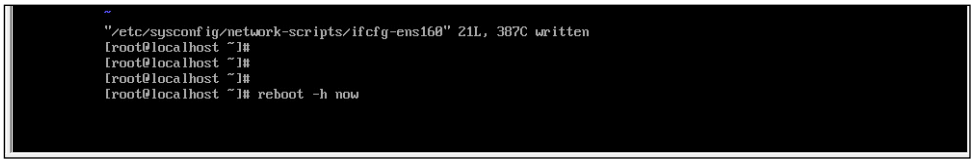
๔.๓.๓.๑๘ การกำหนดค่าไฟล์คอนฟิกควบคุมการ์ดเครือข่าย (Interface Network card) เพื่อเชื่อมต่อระบบเครือข่ายของกรมพัฒนาที่ดินและทำการจัดเก็บค่า (Save) ซึ่งกำหนดให้เครื่องแม่ข่ายรีเวิสพร็อกซี่ ไอพี 10.1.77.67 โดยปรับปรุงและเพิ่มชุดคำสั่งดังนี้

TYPE=Ethernet
BOOTPROTO=static
ONBOOT=yes
IPADDR=10.1.77.67
NETMASK=255.255.255.0
GATEWAY=10.1.77.254
DNS1=10.1.1.4



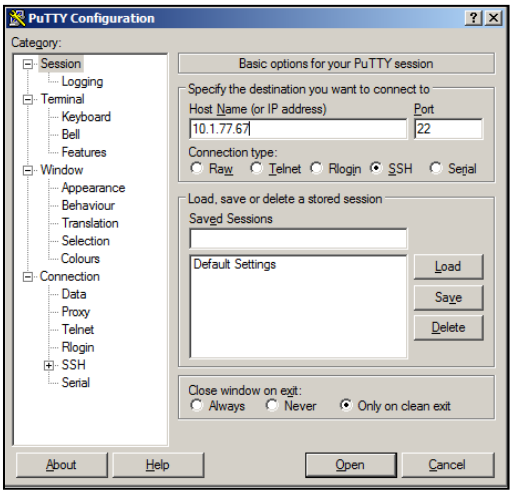
ภาพที่ ๔ – ๓๐ จอภาพแสดงการกำหนดค่าไฟล์คอนฟิกควบคุมการ์ดเครือข่าย

๔.๓.๓.๑๙ ทำการใช้คำสั่งรีสตาร์ทระบบปฏิบัติการ (Restart) เพื่อให้การกำหนดค่าไฟล์คอนฟิกควบคุมการ์ดเครือข่ายมีผลที่ได้กำหนดค่าโดยใช้คำสั่ง reboot -h now



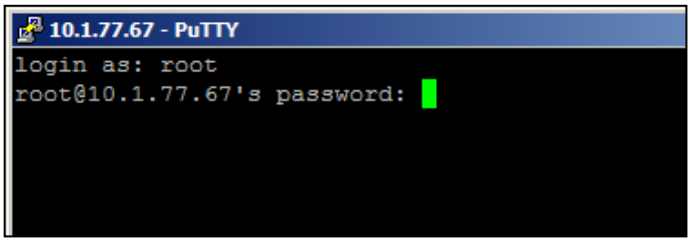
ภาพที่ ๔ – ๓๑ จอภาพแสดงการใช้คำสั่งรีสตาร์ทระบบปฏิบัติการ

๔.๓.๓.๒๐ หลังจากรีสตาร์ทระบบปฏิบัติการ แล้วทำการใช้โปรแกรม Putty เชื่อมต่อไปยังเครื่อง แม่ข่ายพร็อกซี่ 10.1.77.67 port หมายเลข 22 จากเครื่องสนับสนุนเพื่อการกำหนดค่าคอนฟิกและทดสอบการเชื่อมต่อแม่ข่ายพร็อกซี่ผ่านช่องทางโปรโตคอล (Protocol) ซีเคียวเชล (Secure Shell :SSH) โดยกำหนดไอพีแอดเดส 10.1.77.67 port หมายเลข 22 และคลิก Open



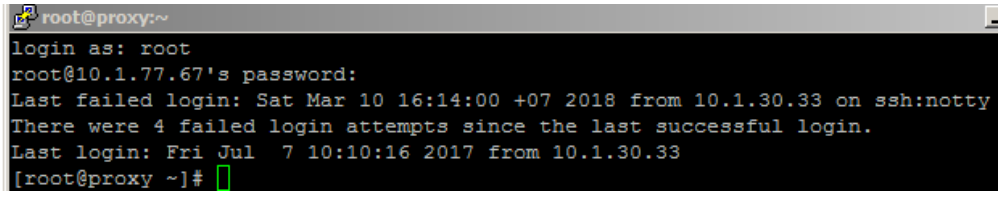
ภาพที่ ๔ – ๓๒ การใช้โปรแกรม Putty เชื่อมต่อไปยังเครื่องแม่ข่ายพร็อกซี่

๔.๓.๓.๒๑ ทำการเข้าสู่ระบบ (Login) โดยการกรอกชื่อผู้ใช้งานและรหัสผ่าน



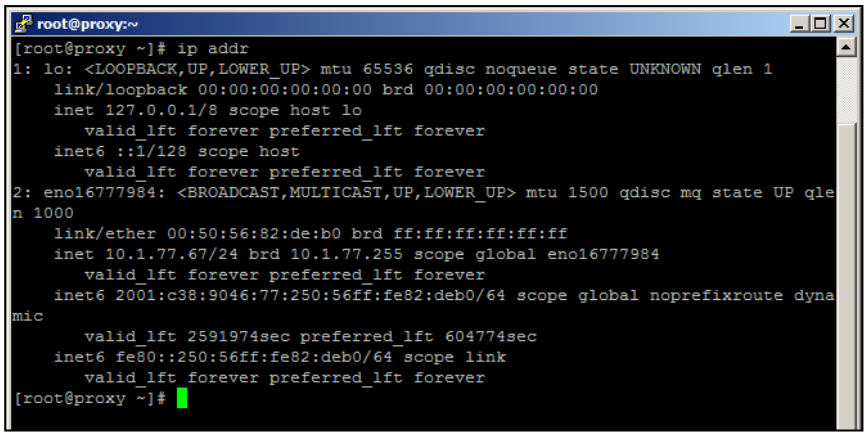
ภาพที่ ๔ – ๓๓ จอภาพแสดงการเข้าสู่ระบบโดยการกรอกชื่อผู้ใช้งานและรหัสผ่าน

๔.๓.๓.๒๒ เสร็จสิ้นการเข้าสู่ระบบ (Login) โดยขึ้นสถานะ # คือพร้อมรับคำสั่งต่อไป



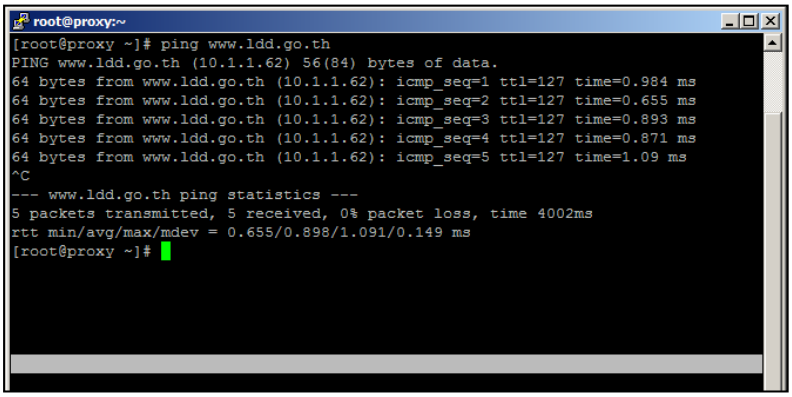
ภาพที่ ๔ – ๓๔ จอภาพแสดงการเสร็จสิ้นการเข้าสู่ระบบ (Login)

๔.๓.๓.๒๓ ทำการตรวจสอบสถานะไฟล์คอนฟิกควบคุมการ์ดเครือข่าย ที่แสดงผลหลังจากการปรับปรุงค่า โดยใช้คำสั่ง ip addr



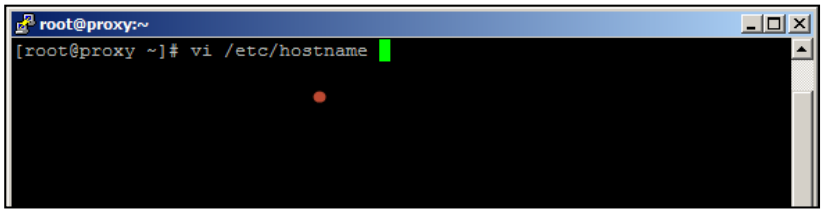
ภาพที่ ๔ – ๓๕ จอภาพแสดงการตรวจสอบสถานะไฟล์คอนฟิกควบคุมการ์ดเครือข่าย

๔.๓.๓.๒๔ การทดสอบการเชื่อมต่อระบบเครือข่ายโดยใช้คำสั่ง ping ไปยังเครื่อง www.ldd.go.th พบว่ามีการ reply กลับมาสามารถใช้งานได้ โดยใช้คำสั่ง ping www.ldd.go.th



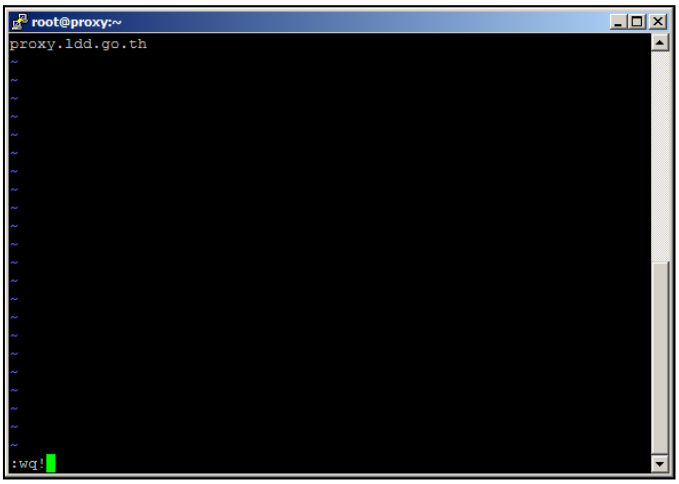
ภาพที่ ๔ – ๓๖ จอภาพแสดงการทดสอบการเชื่อมต่อระบบเครือข่าย

๔.๓.๓.๒๕ ทำการกำหนดค่าไฟล์ hostname เพื่อกำหนดค่าชื่อเครื่องระบบปฏิบัติการ โดยใช้คำสั่ง vi/etc/hostname



ภาพที่ ๔ – ๓๗ จอภาพแสดงการใช้คำสั่งเพื่อกำหนดค่าไฟล์ hostname

๔.๓.๓.๒๖ ทำการกำหนดค่าไฟล์ hostname ชื่อเครื่อง และทำการ Save โดยแก้ไขการกำหนดค่าไฟล์คือ proxy.ldd.go.th

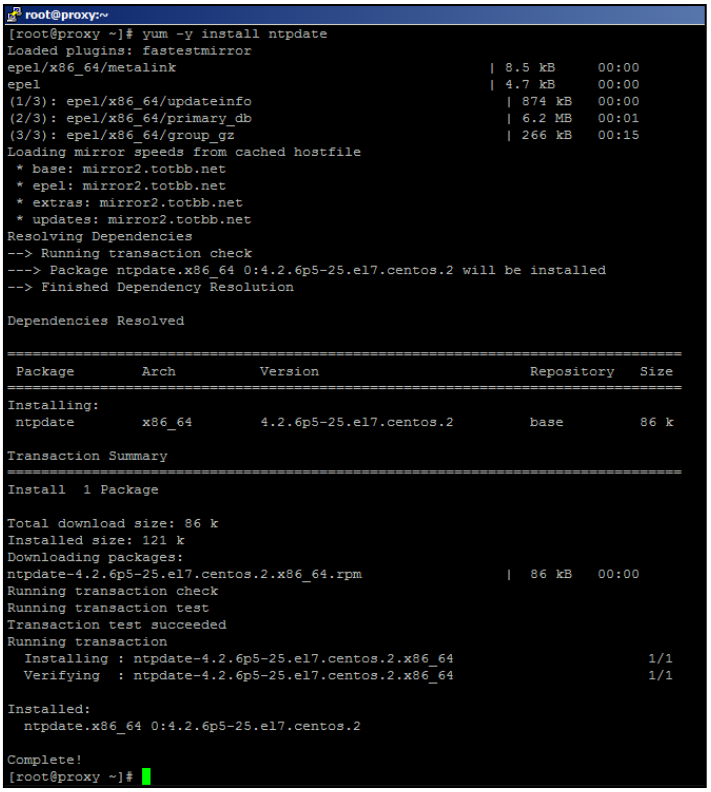


ภาพที่ ๔ – ๓๘ จอภาพแสดงการกำหนดค่าไฟล์ hostname

๔.๓.๓.๒๗ ทำการสร้างชื่อผู้ใช้งานและกำหนดค่ารหัสผ่าน เพิ่มเติมชื่อผู้ใช้งานคือ proxy และรหัสผ่าน โดยการใช้คำสั่ง adduser proxy และรหัสผ่าน passwd proxy เพื่อใช้สิทธิ์ในการควบคุมระบบปฏิบัติการ

ภาพที่ ๔ – ๓๙ จอภาพแสดงการสร้างชื่อผู้ใช้งานและกำหนดค่ารหัสผ่าน

๔.๓.๓.๒๘ ทำการติดตั้งโปรแกรม NTPdate และทำการซิงก์ (sync) เวลา NTP server ของกรมพัฒนาที่ดิน เพื่อให้เวลาเครื่องรีเวิสพร็อกซี่มีเวลาที่ตรงกันกับเครื่อง NTP ของกรมพัฒนาที่ดิน โดยใช้คำสั่ง yum -y install ntpdate และใช้คำสั่ง ntpdate ntp.ldd.go.th

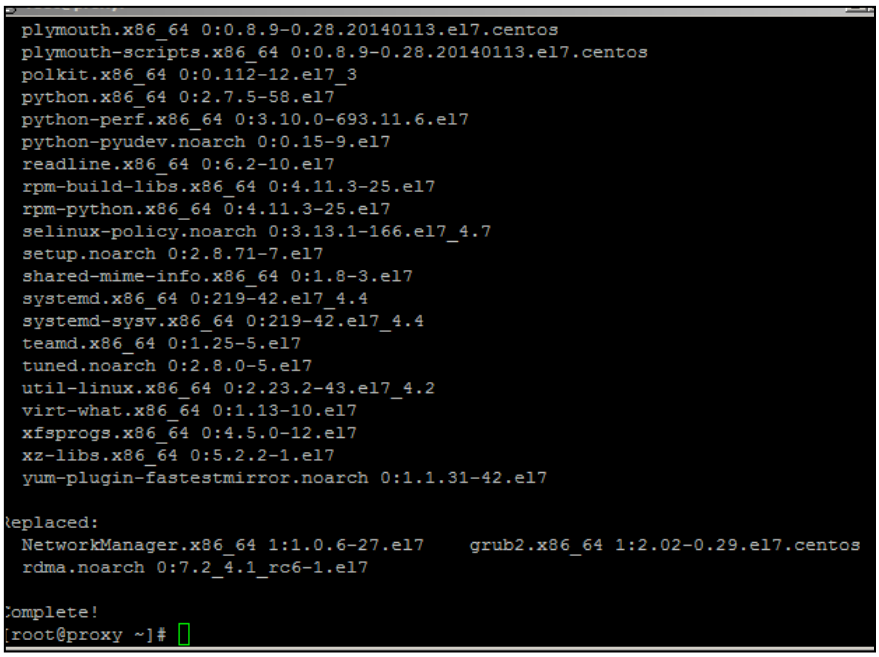


ภาพที่ ๔ – ๔๐ จอภาพแสดงการติดตั้งโปรแกรม NTPdate

ภาพที่ ๔ – ๔๑ จอภาพแสดงการกำหนดค่าให้ซิงก์เวลากับ NTP server กรมพัฒนาที่ดิน

๔.๓.๓.๒๙ ทำการปรับปรุงระบบปฏิบัติการให้เป็นปัจจุบัน โดยทำการอัปเดทระบบปฏิบัติการให้เป็นเวอร์ชั่นล่าสุด เมื่อเสร็จการดาวน์โหลด และติดตั้งเรียบร้อยและทำการรีสตาร์ดระบบปฏิบัติการ โดยใช้คำสั่ง yum -y update

ภาพที่ ๔ – ๔๒ จอภาพแสดงการอัปเดทระบบปฏิบัติการให้เป็นเวอร์ชั่นล่าสุด

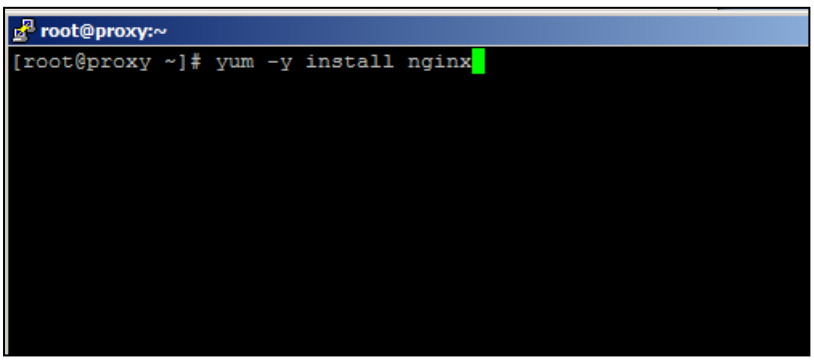


ภาพที่ ๔ – ๔๓ จอภาพแสดงการเสร็จสิ้นการอับเดทระบบปฏิบัติการ

๔.๓.๓ การติดตั้ง โปรแกรม Nginx และปรับปรุงค่า Configuration ของ firewall

โปรแกรม Nginx เป็นโปรแกรมที่ทำหน้าที่เว็บเซอวิส (Web Service) ซึ่งถูกพัฒนาจากการนำข้อด้อยของโปรแกรม apache มาพัฒนาเพื่อให้มีประสิทธิภาพ และในปัจจุบัน มีการนิยมนำโปรแกรม Nginx มาใช้เป็นเว็บ Web Service, Load Balancing และ Reverse proxy การทำงานของ Reverse proxy จะทำหน้าที่เป็นเครื่องแม่ข่ายเพื่อให้บริการเว็บไซต์แทนเครื่องแม่ข่ายเว็บไซต์จริง และทำหน้าเป็นเครื่องลูกข่าย เพื่อนำไปนำข้อมูลเว็บไซต์ของเครื่องแม่ข่ายเว็บไซต์จริง มาเก็บไว้และนำไปแสดงผล นอกจากจะทำให้ลดภาระเครื่องแม่ข่ายแล้ว แต่ยังสามารถกำหนดแนวนโยบาย เพื่อปกป้องลักษณะการโจมตีผ่านการเชื่อมต่อเว็บไซต์ ได้อีกอย่างด้วย

๔.๓.๑.๑ ทำการติดตั้งโปรแกรมเอนจิ้นเอ็ก โดยการใช้คำสั่ง yum -y install Nginx



ภาพที่ ๔ – ๔๔ จอภาพแสดงการใช้คำสั่งเพื่อทำการติดตั้งโปรแกรม Nginx

```
 Verifying  : perl-Filter-1.49-3.el7.x86_64
 Verifying  : perl-Text-ParseWords-3.29-4.el7.noarch
 Verifying  : 1:nginx-mod-mail-1.12.2-1.el7.x86_64

nstalled:
 nginx.x86_64 1:1.12.2-1.el7

ependency Installed:
 fontconfig.x86_64 0:2.10.95-11.el7                  fontpackage
 gperftools-libs.x86_64 0:2.4-8.el7                  libX11.x86_
 libXau.x86_64 0:1.0.8-2.1.el7                       libXpm.x86_
 libpng.x86_64 2:1.5.13-7.el7_2                      libunwind.x
 libxslt.x86_64 0:1.1.28-5.el7                       lyx-fonts.n
 nginx-filesystem.noarch 1:1.12.2-1.el7              nginx-mod-h
 nginx-mod-http-perl.x86_64 1:1.12.2-1.el7           nginx-mod-h
 nginx-mod-stream.x86_64 1:1.12.2-1.el7              perl.x86_64
 perl-Encode.x86_64 0:2.51-7.el7                     perl-Export
 perl-File-Temp.noarch 0:0.23.01-3.el7               perl-Filter
 perl-HTTP-Tiny.noarch 0:0.033-3.el7                 perl-PathTo
 perl-Pod-Perldoc.noarch 0:3.20-4.el7                perl-Pod-Si
 perl-Scalar-List-Utils.x86_64 0:1.27-248.el7        perl-Socket
 perl-Text-ParseWords.noarch 0:3.29-4.el7            perl-Time-H
 perl-constant.noarch 0:1.27-2.el7                   perl-libs.x
 perl-parent.noarch 1:0.225-244.el7                  perl-podlat
 perl-threads-shared.x86_64 0:1.43-6.el7

omplete!
root@proxy ~]#
```

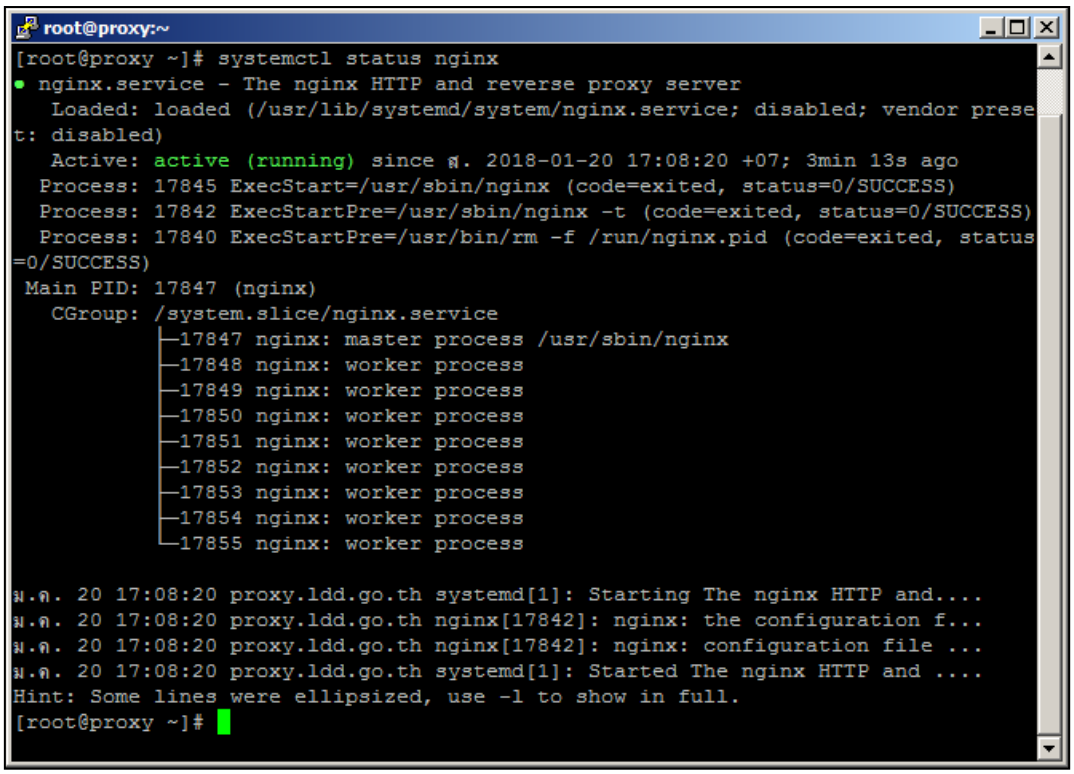
ภาพที่ ๔ – ๔๕ จอภาพแสดงเสร็จสิ้นการดาวน์โหลดแล้วติดตั้งโปรแกรม

๔.๓.๑.๒ ทำการเปิดใช้งานโปรแกรมเอนจิ้นเอ็ก โดยใช้คำสั่ง systemctl start Nginx

```
root@proxy:~
[root@proxy ~]#  systemctl start  nginx
[root@proxy ~]#
```

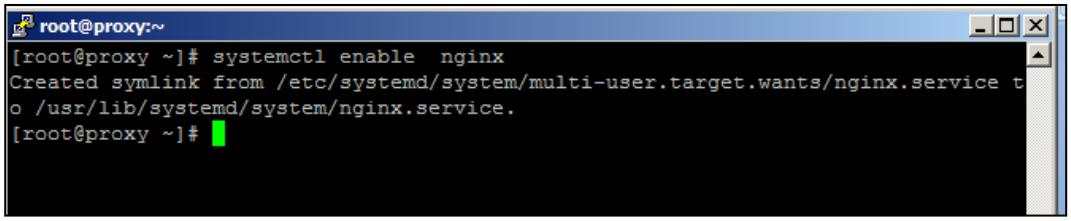
ภาพที่ ๔ – ๔๖ จอภาพแสดงการใช้คำสั่งเพื่อเปิดใช้งานโปรแกรม Nginx

๔.๓.๑.๓ ทำการตรวจสอบสถานะ การทำงานของโปรแกรม Nginx โดยใช้คำสั่ง systemctl status Nginx



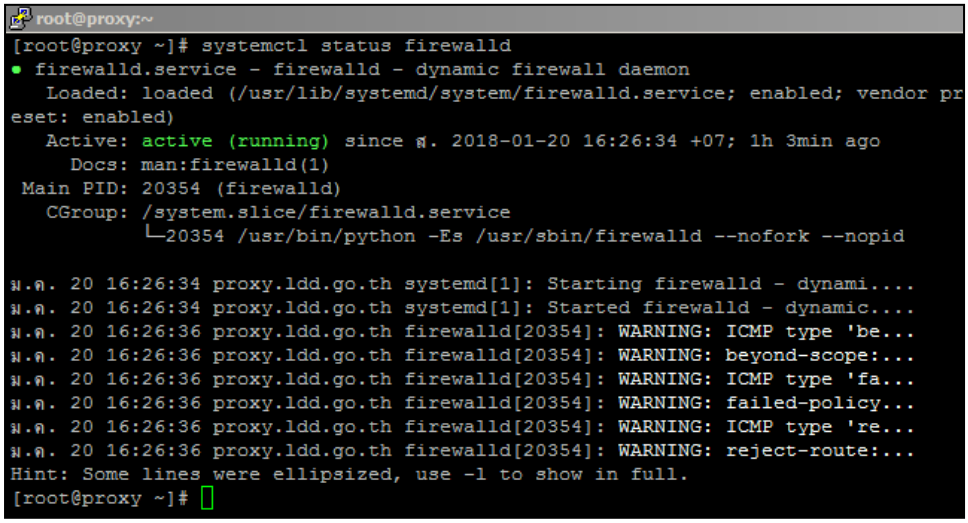
ภาพที่ ๔ – ๔๗ จอภาพแสดงการใช้คำสั่งเพื่อตรวจสอบสถานะโปรแกรม Nginx

๔.๓.๑.๔ ทำการกำหนดค่าให้โปรแกรมเอนจิ้นเอ็ก เปิดใช้งานโปรแกรมหลังจากการเริ่มต้นระบบปฏิบัติการใหม่ทุกครั้ง (Boot) โดยใช้คำสั่ง systemctl enable Nginx



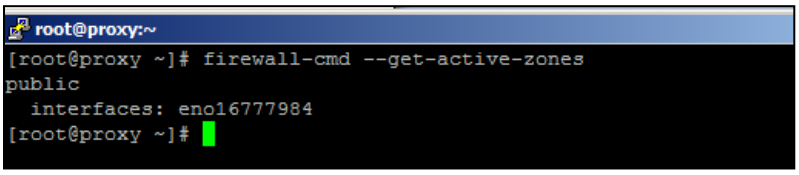
ภาพที่ ๔ – ๔๘ จอภาพแสดงการใช้คำสั่งกำหนดค่าให้โปรแกรม Nginx เปิดใช้งานหลังจากการเริ่มต้นระบบปฏิบัติการ

๔.๓.๑.๕ ทำการตรวจสอบสถานะการทำงานไฟร์วอลล์ ของระบบปฏิบัติการโดยใช้คำสั่ง systemctl status firewall



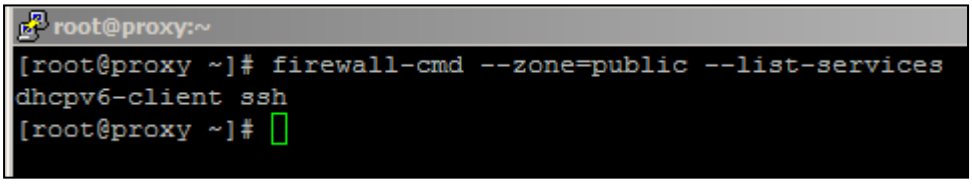
ภาพที่ ๔ – ๔๙ จอภาพแสดงการตรวจสอบการทำงานสถานะไฟล์วอลล์ของระบบปฏิบัติการ

๔.๓.๑.๖ ทำการตรวจสอบโซนการเชื่อมต่อ (zone) ที่การ์ดเชื่อมต่อระบบเครือข่ายเชื่อมต่ออยู่ โดยใช้คำสั่ง firewall-cmd --get-active-zones



ภาพที่ ๔ – ๕๐ จอภาพแสดงการตรวจสอบ zone ที่การ์ดเชื่อมต่อระบบเครือข่าย

๔.๓.๑.๗ ทำการตรวจสอบเซอวิส เชื่อมต่อ zone ที่การ์ดเชื่อมต่อระบบเครือข่ายเชื่อมต่อเปิดอยู่ โดยใช้คำสั่ง firewall-cmd --zone=public --list-services

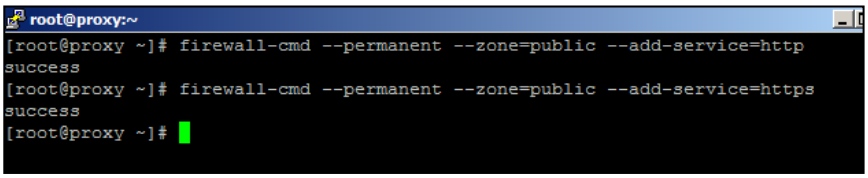


ภาพที่ ๔ – ๕๑ จอภาพแสดงการตรวจสอบเซอวิส ที่มีการเชื่อมต่อ zone ต่าง ๆ

๔.๓.๑.๘ ทำการปรับปรุงค่า Configuration ของ firewall เพื่อให้เซอวิส http และ https สามารถเชื่อมต่อได้ โดยใช้คำสั่ง firewall-cmd --permanent --zone=public --add-service=http และ firewall-cmd --permanent --zone=public --add-service=https อธิบายได้ ดังนี้

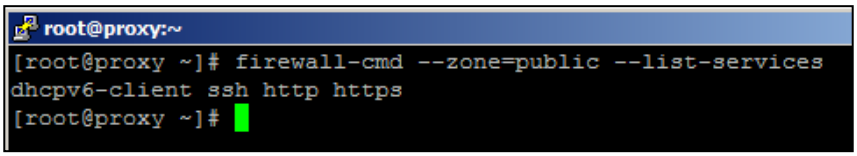
firewall-cmd --permanent กำหนดค่าสร้างช่องทางถาวร --zone=public ในโซน public --add-service=http กำหนดค่าให้เพิ่มเซอวิส http

firewall-cmd --permanent กำหนดค่าสร้างช่องทางถาวร --zone=public ในโซน public --add-service=http กำหนดค่าให้เพิ่มเซอวิส https



ภาพที่ ๔ – ๕๒ จอภาพแสดงการใช้คำสั่งปรับปรุงค่าคอมฟิกไฟร์วอลล์เพื่อให้เซอวิสสามารถเชื่อมต่อได้

๔.๓.๑.๙ ทำการตรวจสอบเซอวิส http และ https สามารถเชื่อมต่อ zone ที่การ์ดเชื่อมต่อระบบเครือข่ายเชื่อมต่ออยู่ได้ โดยใช้คำสั่ง firewall-cmd --zone=public --list-services



ภาพที่ ๔ – ๕๓ จอภาพแสดงการตรวจสอบเซอวิส ที่มีการเชื่อมต่อ zone ต่าง ๆ

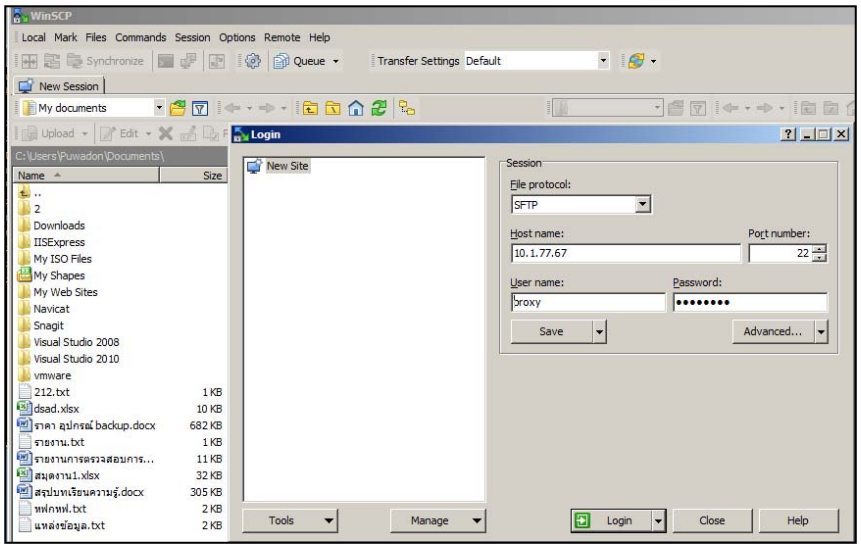
๔.๓.๑.๑๐ ทำการทดสอบการเรียกใช้งานเว็บไซต์ไปยังเครื่อง Reverse Proxy ให้บริการ โดยใช้เครื่องสนับสนุนเรียกใช้งานเว็บไซต์ที่ URL : 10.1.77.67

ภาพที่ ๔ – ๕๔ จอภาพแสดงการทดสอบการเรียกใช้งานเว็บไซต์ไปยังเครื่องแม่ข่ายให้บริการ

๔.๓.๔ การปรับปรุงการกำหนดค่าโปรแกรมอรรถประโยชน์

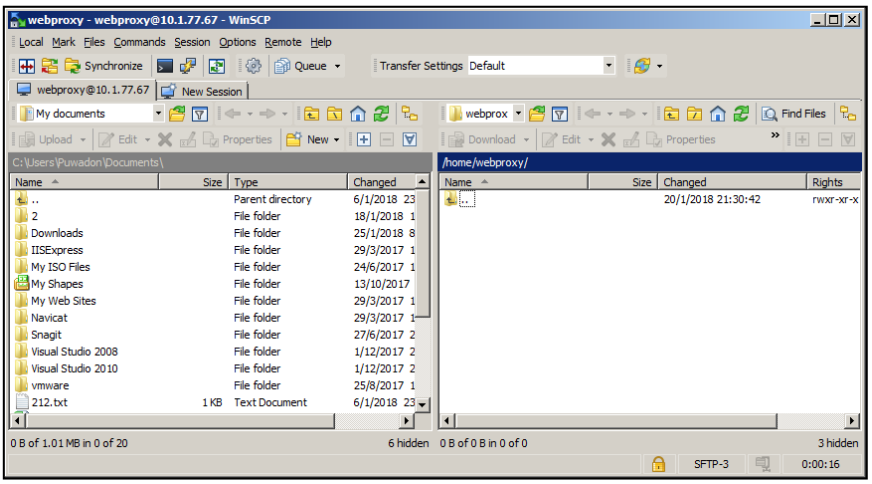
การที่ทำให้ Reverse Proxy สามารถแทนการเรียกใช้งานเว็บไซต์ตามแผนที่ได้กำหนดไว้ จะต้องมีการปรับปรุง โดยยกตัวอย่างเฉพาะการปรับปรุงให้รองรับสำหรับเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต ๓ เท่านั้น เนื่องจากวิธีการปรับปรุงสำหรับเว็บไซต์สำนักพัฒนาที่ดินเขตอื่นจะทำในรูปแบบคล้ายๆกัน แต่มีรายละเอียดปลีกย่อยที่คล้ายกัน ขึ้นอยู่กับความเหมาะสมของเว็บไซต์

๔.๓.๔.๑ ทำการใช้โปรแกรม WinSCP เชื่อมต่อไปยังเครื่องแม่ข่ายพร็อกซี่ 10.1.77.67 ชื่อผู้ใช้งาน (user) : proxy และรหัสผ่าน (password) redssadawd จากเครื่องสนับสนุน



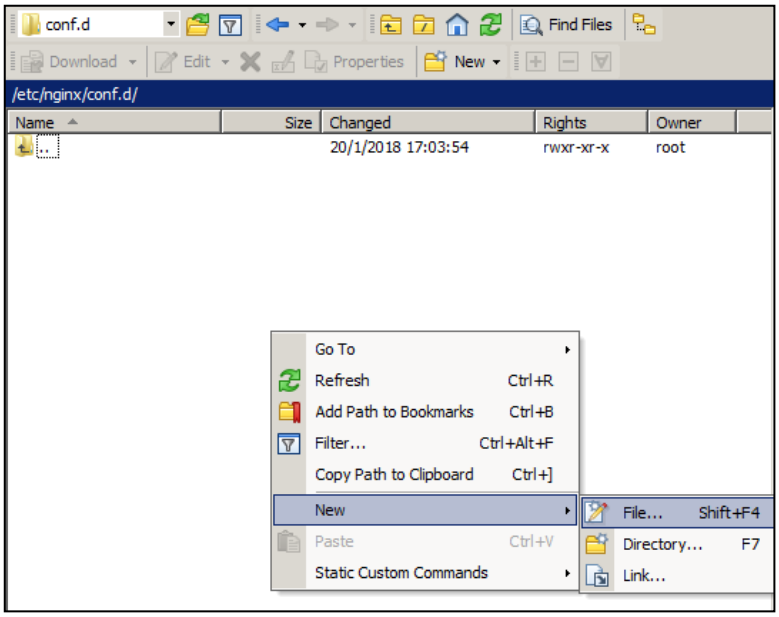
ภาพที่ ๔ – ๕๕ การใช้โปรแกรม WinSCP เชื่อมต่อไปยังเครื่องแม่ข่ายพร็อกซี่

๔.๓.๔.๒ ผลการเชื่อมต่อเครื่องแม่ข่ายพร็อกซี ด้วยโปรแกรม WinSCP สำเร็จ จะแสดงผลเป็นหน้าต่าง ๒ หน้าต่าง คือฝั่งเครื่องคอมพิวเตอร์สนับสนุนซึ่งอยู่ฝั่งซ้าย และเครื่องแม่ข่ายพร็อกซีซึ่งอยู่ฝั่งขวา



ภาพที่ ๔ – ๕๖ ผลการเชื่อมต่อเครื่องแม่ข่ายพร็อกซี ด้วยโปรแกรม WinSCP สำเร็จ

๔.๓.๔.๓ การกำหนดค่าให้โปรแกรมเอนจิ้นเอ็ก (Ngnix) ให้สามารถรองรับลักษณะการทำงานรูปแบบพร็อกซี่ (proxy) ของเว็บไซต์ในหน่วยงานส่วนภูมิภาค โดยการสร้างไฟล์คอนฟิกกูเรชั่นแยกตามเครื่องแม่ข่ายที่อยู่ตามพัฒนาที่ดินเขต เช่น ไฟล์คอนฟิกกูเรชั่นของเว็บไซต์หน่วยงานพัฒนาที่ดินเขต ๓ กำหนดค่าที่ชื่อว่า r03.ldd.go.th.conf โดยจัดเก็บไฟล์ดังกล่าวที่พาร์ท (path) /etc/nginx/conf.d เพื่อให้งานในการบริหารจัดการกำหนดค่าเว็บไซต์ ตัวอย่างเช่น การสร้างไฟล์สำหรับเว็บไซต์ของสำนักงานพัฒนาที่ดินเขต ๓ ที่พาร์ท (path) /etc/Nginx/conf โดยใช้สร้างชื่อไฟล์ /etc/Nginx/conf.d/r03.ldd.go.th.conf โดยทำการคลิกขวาแล้วเลือก New>Fire และตั้งชื่อไฟล์ r03.ldd.go.th.conf



ภาพที่ ๔ – ๕๗ การสร้างไฟล์ Configuration เว็บไซต์สำหรับเว็บไซต์ของสำนักงานพัฒนาที่ดินเขต ๓

๔.๓.๔.๔ ทำการกำหนดชุดคำสั่งไฟล์สำหรับเว็บไซต์ของสำนักงานพัฒนาที่ดินเขต ๓ โดยกำหนดชุดคำสั่งดังนี้

```
upstream r03.ldd.go.th{ server 10.2.3.1:80; }
server {
listen 80;
server_name r03.ldd.go.th;
location / {
proxy_pass http://r03.ldd.go.th;
        }
}
```

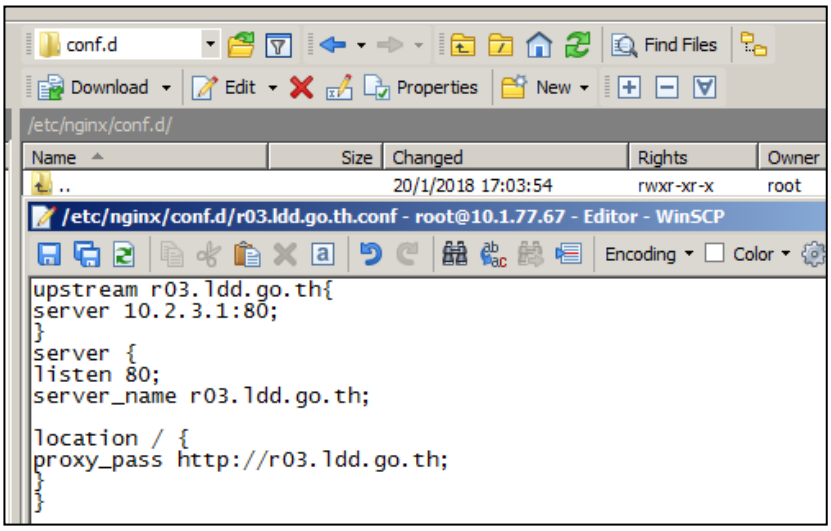
อธิบายได้ดังนี้

upstream หมายถึง การกำหนดค่า ถ้ามีการเรียกใช้เว็บไซต์สำนักงานพัฒนาที่ดินเขต ๓ ให้ดึงข้อมูลมาแสดงจากเครื่องหมายเลขไอพีแอดเดส 10.2.3.1

listen หมายถึง การกำหนดค่า Port การให้บริการ

server_name หมายถึง การกำหนดค่าชื่อเครื่อง

proxy_pass หมายถึง การกำหนดค่าให้เรียกสามารถเรียกได้เฉพาะคำนั้นเท่านั้น



ภาพที่ ๔ – ๕๘ ไฟล์ชุดคำสั่งสำหรับเว็บไซต์ของสำนักงานพัฒนาที่ดินเขต ๓

๔.๓.๔.๕ ทำการปรับปรุงค่าไฟล์ /etc/Nginx/conf.d/r03.ldd.go.th.conf ในส่วนของลักษณะการจัดเก็บชื่อไฟล์โดยกำหนดค่าชื่อล็อกไฟล์ (log file) และตำแหน่งที่จัดเก็บที่

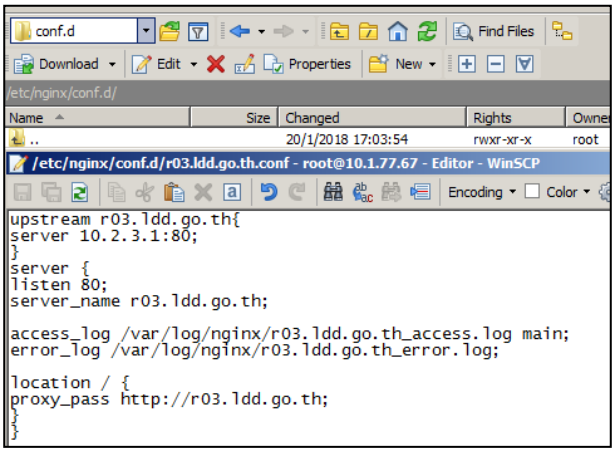
access_log /var/log/Nginx/r03.ldd.go.th_access.log main;

error_log /var/log/Nginx/r03.ldd.go.th_error.log;

อธิบายได้ดังนี้

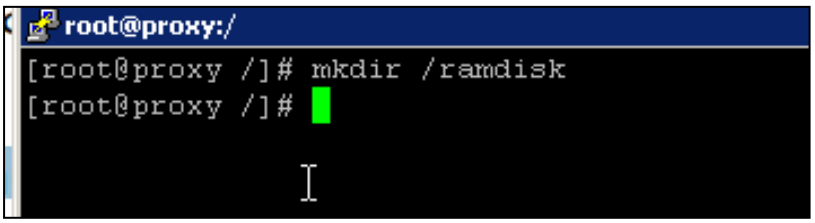
access_log การกำหนดค่าล๊อกไฟล์ การใช้งานปกติ ตำแหน่งที่จัดเก็บ พาร์ท /var/log/Nginx/ และกำหนดค่าชื่อไฟล์ r03.ldd.go.th_access.log

error_log การกำหนดค่าล๊อกไฟล์ ผิดปกติ ปกติ ตำแหน่งที่จัดเก็บ พาร์ท /var/log/Nginx/ และกำหนดค่าชื่อไฟล์ r03.ldd.go.th_error.log



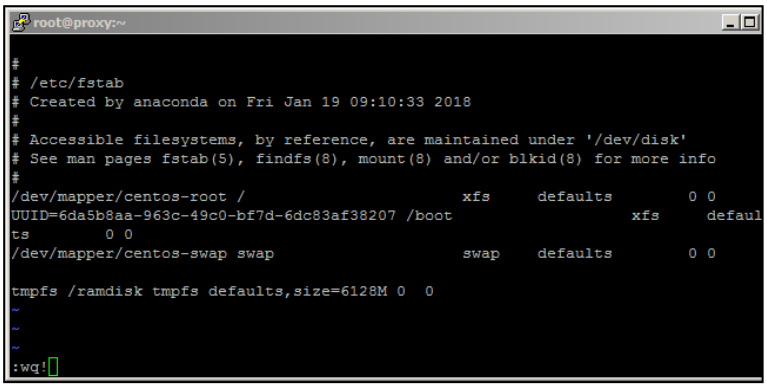
ภาพที่ ๔ – ๕๙ การเพิ่มกำหนดค่า Log ในไฟล์ชุดคำสั่งสำหรับเว็บไซต์ของสำนักงานพัฒนาที่ดินเขต ๓

๔.๓.๔.๖ การเพิ่มประสิทธิภาพการในการแสดงผลเว็บไซต์โดยกำหนดค่าแรมดิสก์ (Ram disk) เพื่อนำเอาจำนวนพื้นที่ส่วนหนึ่งไปทำ Ram disk เพื่อใช้งานเป็น Caching ไฟล์ เนื่องจาก RAM มีความเร็วในการอ่าน (Read) สูง ในกรณีนี้กำหนดค่า Ramdisk ขนาด ๖๑๒๘ MB เริ่มจากการใช้คำสั่งสร้างพาร์ท ramdisk โดยใช้คำสั่ง mk /ramdisk



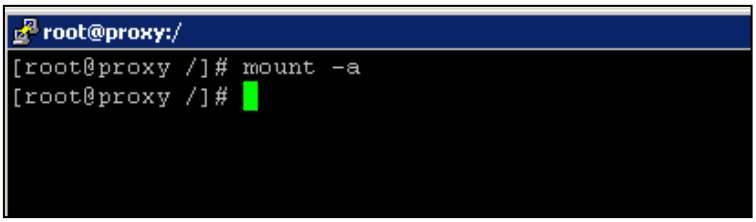
ภาพที่ ๔ – ๖๐ จอภาพแสดงการใช้คำสั่งในการตรวจสอบความถูกต้องของชุดคำสั่ง

๔.๓.๔.๗ ทำการกำหนดค่าขนาดพาร์ทข้อมูล Ram disk ให้มีขนาด ๖๑๒๘ MB โดยการกำหนดค่าไฟล์ชุดคำสั่ง /etc/fstab โดยเพิ่มชุดคำสั่งtmpfs/ramdisk tmpfs defaults,size=6128M 0 0



ภาพที่ ๔ – ๖๑ จอภาพแสดงการกำหนดค่าขนาดของพาร์ทข้อมูล Ram disk

๔.๓.๔.๘ ทำการปรับปรุงค่าดิสก์ที่ระบบปฏิบัติการเชื่อมต่อ (Remount) ที่ได้รับการแก้ไขโดยใช้คำสั่ง mount -a



ภาพที่ ๔ – ๖๒ จอภาพแสดงการปรับปรุงค่าดิสก์ที่ระบบปฏิบัติการเชื่อมต่อ

4.3.4.9 การกำหนดค่าให้โปรแกรม Nginx จัดเก็บไฟล์แคชข้อมูลเว็บไซต์ ในรูปแบบ Ram disk โดยทำการเพิ่มชุดไฟล์คำสั่ง /etc/Nginx/conf.d/r03.ldd.go.th.conf

proxy_cache_path /ramdisk/cache_r03.ldd.go.th levels=1:2
keys_zone=cache_cache_r03.ldd.go.th:128m
max_size=32m inactive=10m use_temp_path=off ;

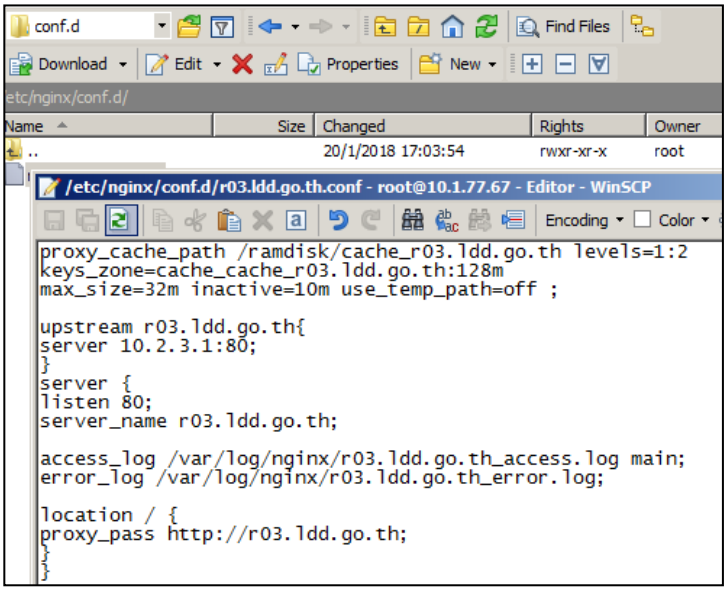
อธิบายได้ดังนี้

proxy_cache_path คือ การกำหนดค่าพาร์ทที่เก็บข้อมูลไฟล์แคชที่
ramdisk/cache_r03.ldd.go.th

keys_zone คือ การกำหนดค่าชุดคำสั่งหลักให้จัดเก็บขนาดสูงสุด ๑๒๘ MB

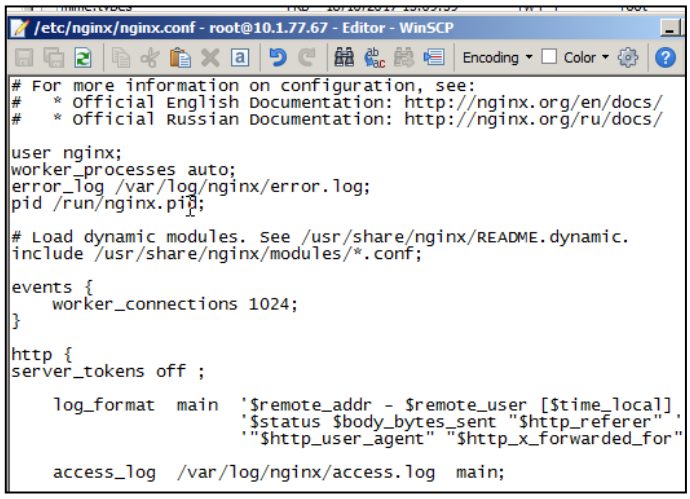
max_size คือ การกำหนดค่าไฟล์ที่มีการจัดเก็บขนาดใหญ่สุดเท่ากับ ๓๒ MB

inactive คือ เวลาที่จำค่าในแต่ละไฟล์คือ ๑๐ นาที



ภาพที่ ๔ – ๖๓ การกำหนดค่าให้โปรแกรม Nginx จัดเก็บไฟล์แคชข้อมูลเว็บไซต์

๔.๓.๔.๑๐ การปรับตั้งค่าให้โปรแกรม Nginx ไม่แสดงผลเวอร์ชั่นของโปรแกรม เพื่อลดช่องโหว่ในการโจมตีผ่านระบบเครือข่าย โดยกำหนดค่า Server Tokens ไฟล์ /etc/nginx/nginx.conf โดยกำหนดค่า แก้ไขชุดคำสั่งให้เป็น server_tokens off

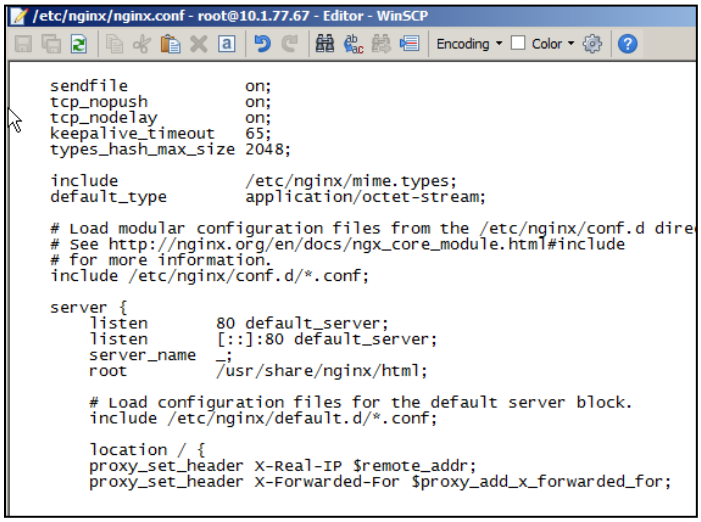


ภาพที่ ๔ – ๖๔ การปรับตั้งค่าให้โปรแกรม Nginx ไม่แสดงผลเวอร์ชั่นของโปรแกรม

๔.๓.๔.๑๑ การปรับตั้งค่าให้ส่งค่าในส่วนหัว (Header) ของแพ็กเก็ตที่ได้รับจากการเรียกใช้งานเว็บไซต์ เพื่อส่งค่าเป็นไอพีแอสเดสชุดเดิมที่ได้รับ โดยกำหนดค่าไฟล์ /etc/nginx/nginx.conf โดยกำหนดไฟล์ชุดคำสั่ง

proxy_set_header X-Real-IP $remote_addr;

proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;

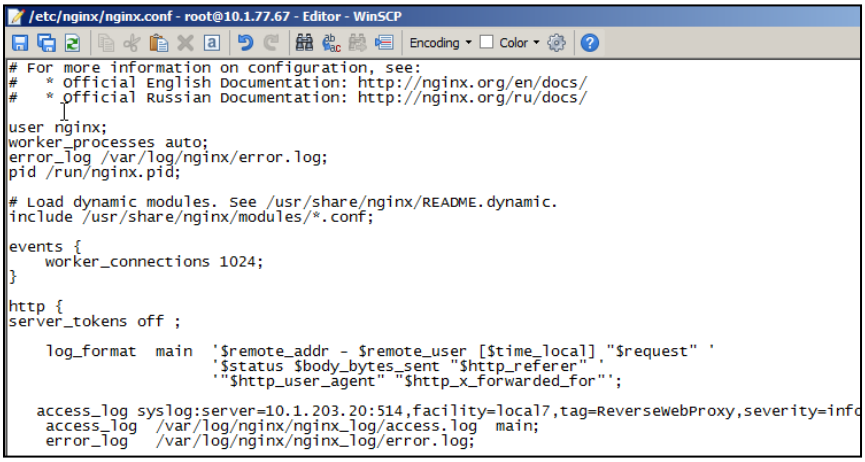


ภาพที่ ๔ – ๖๕ การปรับตั้งค่าให้โปรแกรม Nginx ส่งค่าไอพีแอสเดสชุดเดิม

๔.๓.๔.๑๒ การกำหนดค่าให้โปรแกรม Nginx ส่งค่าล็อกไฟล์ log file การใช้ไปยังศูนย์กลางการจัดเก็บล็อกไฟล์ (centralized log) โดยกำหนดค่าไฟล์ /etc/Nginx/Nginx.conf โดยกำหนดค่า

ไฟล์ชุดคำสั่ง access_log
syslog:server=10.1.203.20:514,facility=local7,tag=ReverseWebProxy,severity=info;
อธิบายได้ดังนี้

access_log syslog:server=10.1.203.20:514 กำหนดค่าส่งล็อกไฟล์ไปเครื่องหมายเลขไอพีแอดเดส 10.1.203.20 หมายเลขพอร์ต 514 facility=local7 แหล่งกำเนิดของข้อมูลล็อก tag=ReverseWebProxy ใส่เครื่องหมายว่า ReverseWebProxy severity=info; แสดงถึงระดับความสำคัญของเหตุการณ์

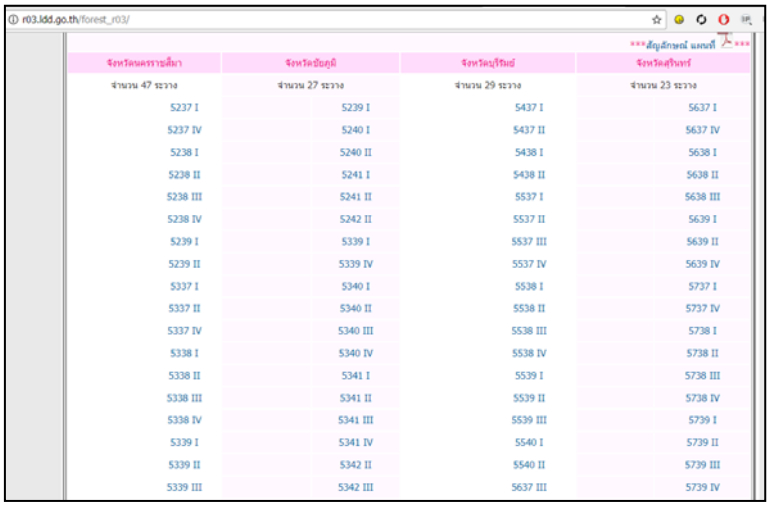


ภาพที่ ๔ – ๖๖ การกำหนดค่าให้โปรแกรม Nginx ส่งค่าล็อกไฟล์

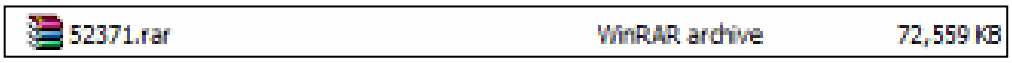
๔.๓.๕ ปรับปรุงการกำหนดค่าโปรแกรม Nginx เพื่อเพิ่มประสิทธิภาพในการรับ-ส่งข้อมูล และลดช่องโหว่การโจมตีเว็บไซต์ของระบบ

๔.๓.๕.๑ เพื่อเพิ่มประสิทธิภาพในการรับ-ส่งข้อมูล ตามแผนที่ได้กำหนดไว้ โดยวิเคราะห์ถึงความเหมาะสมในแต่เว็บไซต์เนื่องจาก แต่ละเว็บไซต์มีการนำเว็บดังกล่าวไปใช้งานแตกต่างเช่น เว็บไซต์สำนักพัฒนาที่ดินเขต ๓ มีการนำเว็บไซต์ใช้ด้านเผยแพร่ข้อมูลแผนที่เป็นจำนวนมาก และลักษณะไฟล์มีขนาดใหญ่ ซึ่งทำให้ผู้ใช้งานต้องดาวน์โหลดไฟล์ข้อมูลดังกล่าว เหมือน ๆ กันหลายครั้งจึงทำให้ มีการรับ-ส่งข้อมูลเดิมจากส่วนภูมิภาคมายังส่วนกลาง ส่งผลให้ประสิทธิภาพในการรับ-ส่งข้อมูลอื่น ๆ ลดลง และผู้ใช้บริการอินเทอร์เน็ตจะต้องใช้เวลาในการดาวน์โหลดนานกว่า เครื่องแม่ข่ายที่ให้บริการอยู่ส่วนกลาง

ภาพที่ ๔ – ๖๗ จอภาพแสดงเมนูดาวน์โหลดแผนที่ป่าไม้ถาวรของเว็บไซต์สำนักพัฒนาที่ดินเขต ๓



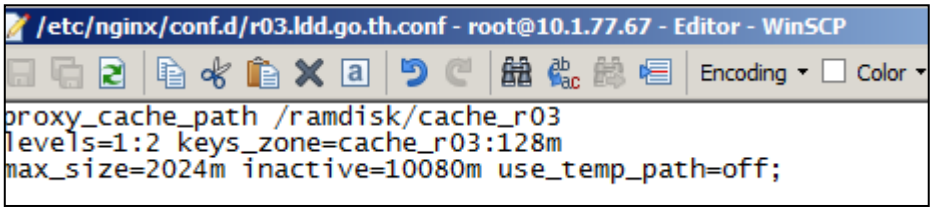
ภาพที่ ๔ – ๖๘ จอภาพแสดงเมนูดาวน์โหลดภาพแผนที่ป่าไม้ถาวรตามมติคณะรัฐมนตรี
ของเว็บไซต์สำนักพัฒนาที่ดินเขต ๓



ภาพที่ ๔ – ๖๙ ไฟล์ตัวอย่างแผนที่พื้นที่ป่าจำแนกจังหวัดนครราชสีมา

ซึ่งจากกวิเคราะห์ลักษณะการให้บริการเว็บไซต์สำนักพัฒนาที่ดินเขต ๓ ส่วนใหญ่จะไม่มีการเปลี่ยนแปลง และประกาศการจัดซื้อจัดจ้างเป็นลิงก์ไปที่ จัดซื้อจัดจ้างของกรมพัฒนาที่ดิน จึงแก้ไขชุดคำสั่งเพื่อเพิ่มประสิทธิภาพในการรับ-ส่งข้อมูล โดยการกำหนดค่าชุดคำสั่ง จาก

proxy_cache_path /ramdisk/cache_r03
levels=1:2keys_zone=cache_cache_r03.ldd.go.th:128m
max_size=32m inactive=10m use_temp_path=off ;
เป็น
proxy_cache_path /ramdisk/cache_r03
levels=1:2 keys_zone=cache_r03:128m
max_size=2024m inactive=10080m use_temp_path=off;



ภาพที่ ๔ – ๗๐ การแก้ไขชุดคำสั่ง เพื่อเพิ่มประสิทธิภาพในการรับ-ส่งข้อมูล

๔.๓.๕.๒ ทำการแก้ไขชุดคำสั่ง เพื่อลดช่องโหว่การโจมตีเว็บไซต์ โดยการกำหนดค่าชุดคำสั่ง

๑) ชุดคำสั่งให้สามารถ block method อื่นๆที่ไม่ใช่ GET และ POST

```
# Block HEAD | GET | POST
 if ($request_method !~ ^(HEAD|GET|POST)$ ) {
     return 405;
  }
```

อธิบายได้ดังนี้ ถ้าเป็น HTTP Request ที่มีไม่ใช่ลักษณะ การ GET และ POST ให้ทำการคืนค่าไปแสดงผลเว็บไซต์เป็น รหัส error 405

๒) ชุดคำสั่งให้สามารถป้องกันการโจมลักษรณะ SQL injections

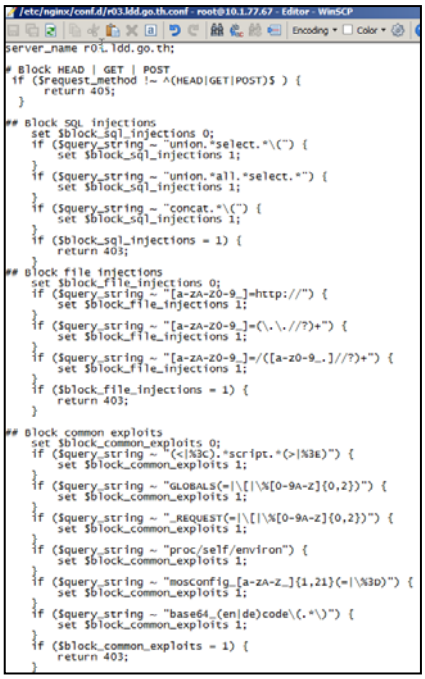
```
## Block SQL injections
    set $block_sql_injections 0;
    if ($query_string ~ "union.*select.*\(") {
        set $block_sql_injections 1;
    }
    if ($query_string ~ "union.*all.*select.*") {
        set $block_sql_injections 1;
    }
    if ($query_string ~ "concat.*\(") {
        set $block_sql_injections 1;
    }
    if ($block_sql_injections = 1) {
        return 403;
    }
```

อธิบายได้ดังนี้ หากเครื่องแม่ข่าย Web Server โดนการโจมตีที่มีลักษณะเป็น SQL injections ให้ทำการส่งคืนค่าโดยแสดงผลเว็บไซต์เป็น รหัส error 403

๓) ชุดคำสั่งให้สามารถป้องกันการโจมตีลักษณะ file injections

```
## Block file injections
    set $block_file_injections 0;
    if ($query_string ~ "[a-zA-Z0-9_]=http://") {
        set $block_file_injections 1;
    }
    if ($query_string ~ "[a-zA-Z0-9_]=(\.\.//?)+") {
        set $block_file_injections 1;
    }
    if ($query_string ~ "[a-zA-Z0-9_]=/([a-z0-9_.]//?)+") {
        set $block_file_injections 1;
    }
    if ($block_file_injections = 1) {
        return 403;
    }
```

อธิบายได้ดังนี้ หากเครื่องแม่ข่าย Web Server โดนการโจมตีที่มีลักษณะเป็น file injections ให้ทำการส่งคืนค่าโดยแสดงผลเว็บไซต์เป็น รหัส error 403



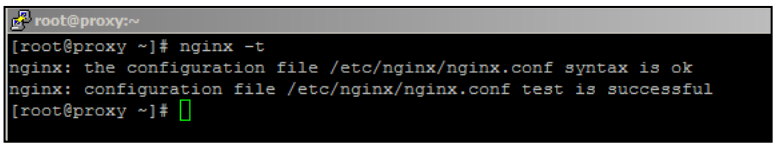
ภาพที่ ๔ – ๗๑ การกำหนดค่าปิดกันการโจมตีของไฟล์ชุดคำสั่ง

๔.๓.๕.๓ การปรับปรุงไฟล์ชุดคำสั่ง ของโปรแกรม Nginx จะยังไม่มีผลจากการแก้ไขทันที ต้องดำเนินการขั้นตอนต่อไป โดยต้องตรวจสอบชุดคำสั่งที่มีการแก้ไขว่าถูกต้องหรือไม่ ตามที่โปรแกรมสามารถที่จะอ่านค่า และนำไปใช้ได้หรือไม่ โปรแกรมจึงมีคำสั่งที่ให้ตรวจสอบก่อนว่าชุดคำสั่งดังกล่าวถูกหรือไม่ โดยใช้คำสั่ง nginx -t ถ้าชุดคำสั่งที่ได้รับการแก้ไขถูกต้องก็จะแจ้งข้อความดังนี้

nginx: the configuration file /etc/nginx/nginx.conf syntax is ok

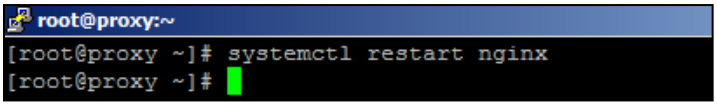
nginx: configuration file /etc/nginx/nginx.conf test is successful

แสดงว่าชุดคำสั่งที่ได้รับการแก้ไขนั้นสามารถนำไปใช้ได้



ภาพที่ ๔ – ๗๒ จอภาพแสดงการใช้คำสั่งในการตรวจสอบความถูกต้องของชุดคำสั่ง

๔.๓.๕.๔ หลังจากตรวจสอบชุดคำสั่ง โดยใช้คำสั่ง nginx -t มีข้อมูลถูกต้องแล้ว ต้องทำการ รีสตาร์ทโปรแกรม เพื่อให้ชุดคำสั่งที่มีการเปลี่ยนแปลงมีผล โดยใช้คำสั่ง systemcrl restart nginx

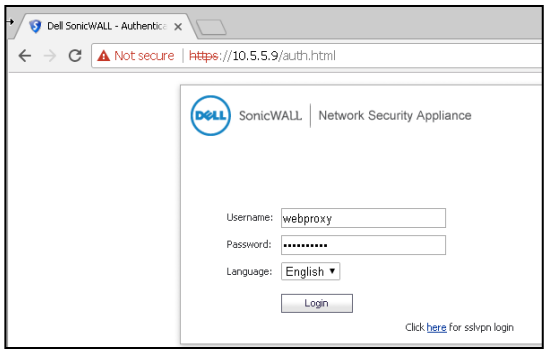


ภาพที่ ๔ – ๗๓ จอภาพแสดงการใช้คำสั่ง restart โปรแกรมเพื่อให้ชุดคำสั่งที่มีการเปลี่ยนแปลงมีผล

๔.๔ การปรับปรุงการกำหนดค่าอุปกรณ์เครือข่ายที่เกี่ยวข้อง

การปรับปรุงระบบอุปกรณ์เครือข่ายนั้นมีการ เปลี่ยนแปลงการเชื่อมโยงอยู่หนึ่งอุปกรณ์คือ อุปกรณ์ไฟล์วอลล์ซึ่งทำหน้าที่ในการตรวจสอบการส่ง-รับข้อมูลแพ็คเก็ต (packet) ให้ถูกต้องการ และฟังก์ชันการทำเน็ตเวิร์ค แอดเดรส ทรานสเลชั่น (Network address translation : NAT) จึงต้องดำเนินการปรับปรุง ไฟล์วอลในส่วนของการเน็ตเวิร์ค แอดเดรส ทรานสเลชั่น ยกตัวอย่าง การปรับปรุงเว็บไซต์สำนักงานพัฒนาที่ดินเขต ๓

๔.๔.๑ เข้าสู่เว็บไซต์ควบคุมอุปกรณ์ไฟร์วอลล์ เข้าสู่ URL://10.5.5.9/auth.html และทำการกรอกชื่อผู้ใช้และรหัสผ่านเพื่อเข้าสู่ระบบ

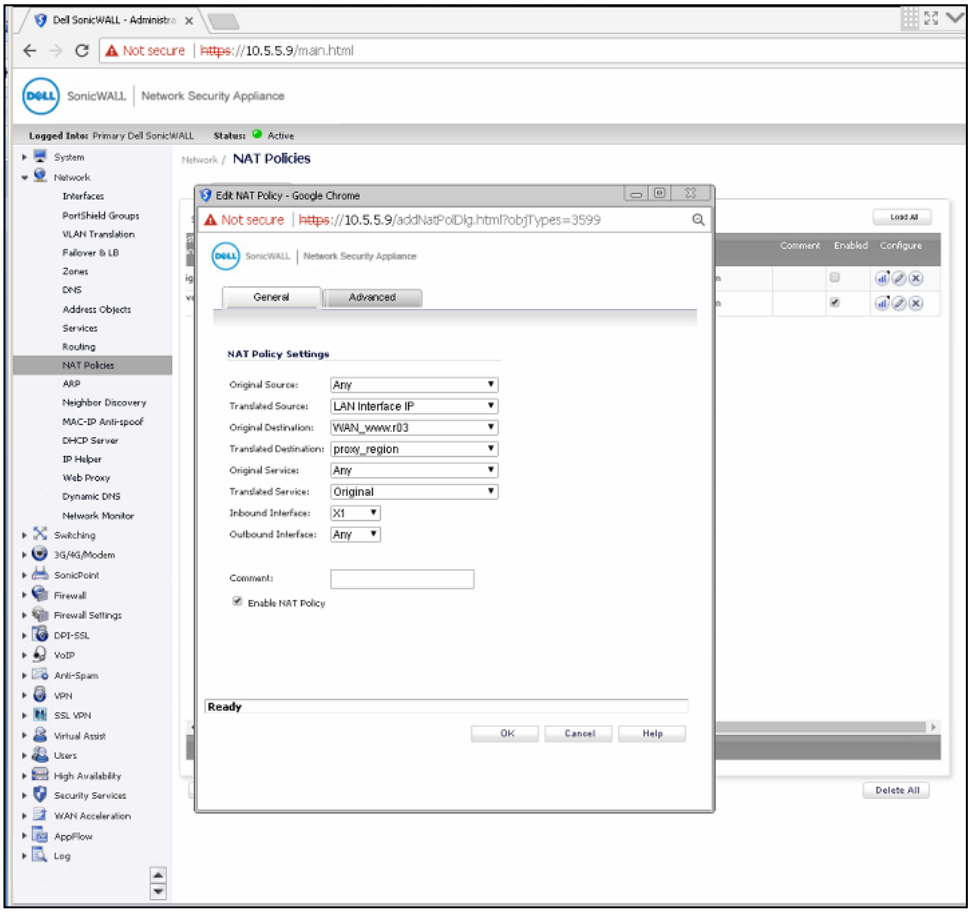


ภาพที่ ๔ - ๗๔ การเข้าสู่เว็บไซต์ควบคุมอุปกรณ์ไฟร์วอลล์

๔.๔.๒ ทำการสร้าง หมายเลขของอุปกรณ์ (Address Object) ที่ใช้สำหรับอ้างอิงในการปรับปรุงฟังก์ชันการทำ NAT ที่ส่วนของการสร้างหมายเลขของอุปกรณ์ใหม่ กำหนดค่า ชื่อเครื่อง proxy_region ของรีเวิสพร็อกซี่ โซนคือ LAN และ หมายเลขไอพีแอดเดส 10.1.77.67 โดยการกำหนดค่าที่ Network>Address Object>Add.. และกำหนดค่า Name: proxy_region, Zone Assignment: LAN, Type: HOST และ IP Address: 10.1.77.67

ภาพที่ ๔ – ๗๕ การสร้างหมายเลขของอุปกรณ์

๔.๔.๓ ทำการปรับการปรุงการกำหนดค่าฟังก์ชัน NAT ในส่วนการให้บริการเว็บไซต์สำนักงานพัฒนาที่ดินเขต ๓ โดยปรับเปลี่ยนในส่วน อุปกรณ์เครื่องแม่ข่ายปลายทาง (Translated Destination) เปลี่ยนเป็น proxy_region



ภาพที่ ๔ – ๗๖ การปรับการปรุงการกำหนดค่าฟังก์ชัน NAT

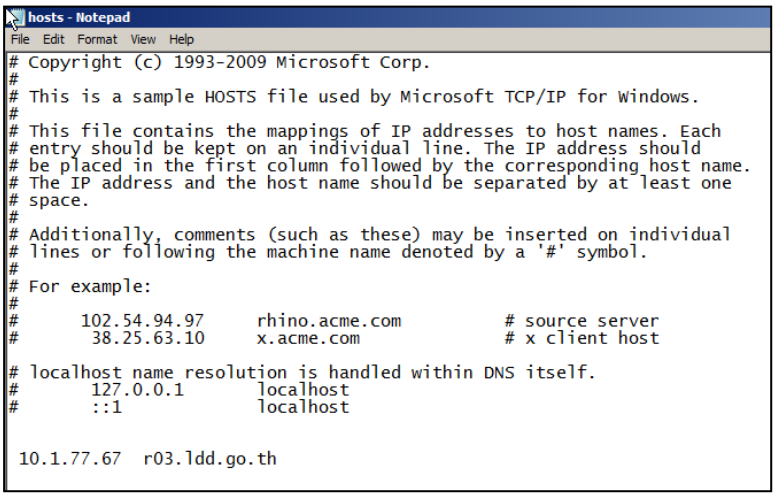
บทที่ ๕
การตรวจสอบการทำงานและการบำรุงรักษาระบบ

หลังจากติดตั้งระบบตัวแทนการให้บริการเว็บไซต์สำนักงานพัฒนาที่ดินเขตเรียบร้อยแล้ว ดำเนินการตรวจสอบการทำงานระบบตัวแทนการให้บริการเว็บไซต์สำนักงานพัฒนาที่ดินเขต (Check) และบำรุงรักษาระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต (Act) เพื่อให้ระบบสามารถใช้งานได้อย่างมีประสิทธิภาพ โดยมีขั้นตอน ดังนี้

๕.๑ การตรวจสอบการทำงานระบบตัวแทนการให้บริการเว็บไซต์สำนักงานพัฒนาที่ดินเขต (Check) ปฏิบัติดังนี้

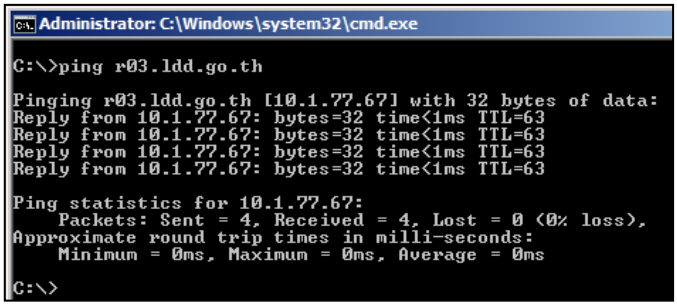
๕.๑.๑ การตรวจสอบความถูกต้อง โดยการทดสอบการใช้งานเว็บไซต์สำนักงานพัฒนาที่ดินเขต ๓ เพื่อให้เครื่องคอมพิวเตอร์ที่ใช้สำหรับสนับสนุน สามารถทดสอบการเรียกใช้งานเว็บไซต์จากเครื่องคอมพิวเตอร์ภายในหน่วยงาน

๕.๑.๒ ทดสอบจากเครื่องคอมพิวเตอร์ที่เชื่อมต่อระบบเครือข่ายภายในกรมพัฒนาที่ดิน โดยนำเครื่องคอมพิวเตอร์ที่ใช้สำหรับสนับสนุน เชื่อมต่อกับระบบเครือข่ายภายในของกรมพัฒนาที่ดิน และกำหนดค่าไฟล์ hosts ของเครื่องคอมพิวเตอร์ ให้สามารถเรียกเว็บไซต์สำนักงานพัฒนาที่ดินเขต ๓ เป็นเครื่องแม่ข่าย Reverse Proxy โดยการปรับเปลี่ยนกำหนดค่าไฟล์ C:\Windows\System32\drivers\etc\hosts เพิ่มชุดคำสั่ง 10.1.77.67 r03.ldd.go.th



ภาพที่ ๕ - ๑ ไฟล์ Hosts ที่ถูกเพิ่มชุดคำสั่ง

๕.๑.๓ ทำการทดสอบติดต่อไปยังเครื่องแม่ข่ายเว็บไซต์สำนักงานเขตพัฒนาที่ดินเขต ๓ r03.ldd.go.th เพื่อทดสอบว่าเว็บไซต์ r03.ldd.go.th ต้องติดต่อไปยังเครื่อง Reverse Proxy โดยใช้คำสั่ง ping r03.ldd.go.th ซึ่งเครื่องคอมพิวเตอร์ที่สนับสนุนใช้ไอพีแอดเดส 10.1.77.67 เพื่อจะติดต่อไปยังเครื่องแม่ข่ายเว็บไซต์ r03.ldd.go.th

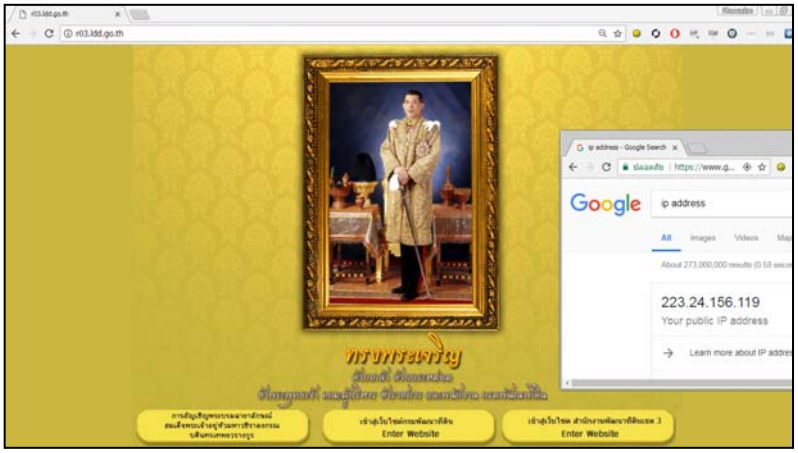


ภาพที่ ๕ – ๒ จอภาพแสดงการทดสอบโดยการ ping เครื่องแม่ข่ายเว็บไซต์สำนักงานเขตพัฒนาที่ดินเขต ๓

๕.๑.๔ ทดสอบเรียกใช้งานเว็บไซต์พัฒนาที่ดินเขต ๓ โดยนำเครื่องคอมพิวเตอร์ที่ใช้สำหรับสนับสนุน เชื่อมต่อกับระบบอินเตอร์เน็ตจากภายในกรมพัฒนาที่ดิน ใช้โปรแกรม Google chrome และเรียกใช้งานเว็บไซต์ r03.ldd.go.th เว็บไซต์สามารถแสดงผลเป็นปกติ

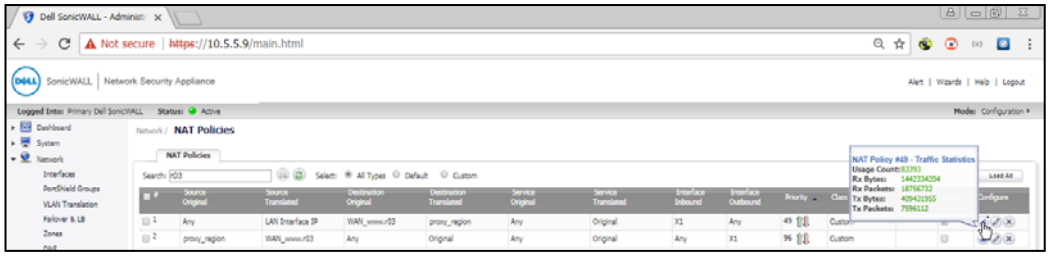
ภาพที่ ๕ – ๓ จอภาพแสดงเว็บไซต์พัฒนาที่ดินเขต ๓ จากคอมพิวเตอร์ภายในเครือข่าย

๕.๑.๕ ทดสอบจากเครื่องคอมพิวเตอร์ที่เชื่อมต่อระบบเครือข่ายภายนอกกรมพัฒนาที่ดิน โดยนำเครื่องคอมพิวเตอร์ที่ใช้สำหรับสนับสนุน เชื่อมต่อกับระบบอินเตอร์เน็ตจากภายนอกกรมพัฒนาที่ดิน ทดสอบเรียกใช้งานเว็บไซต์พัฒนาที่ดินเขต ๓ โดยเรียกใช้โปรแกรม Google chrome และเรียกเว็บไซต์ r03.ldd.go.th เว็บไซต์สามารถแสดงผลเป็นปกติ



ภาพที่ ๕ – ๔ จอภาพแสดงผลเว็บไซต์พัฒนาที่ดินเขต ๓ จากคอมพิวเตอร์เชื่อมต่ออินเตอร์เน็ต

๕.๑.๖ เฝ้าระวังและตรวจสอบผลของการปรับปรุงระบบเครือข่ายที่เกี่ยวข้องกับการเปลี่ยนแปลง ได้ตรวจสอบขั้นตอนการเฝ้าระวังสามารถตรวจสอบได้จากจำนวน packet ที่มีการรับ-ส่งข้อมูลผ่านฟังก์ชันเน็ตเวิร์ค แอดเดรส ทรานสเลชั่น ว่ามีจำนวนที่ต้องเปลี่ยนแปลงอยู่เสมอ

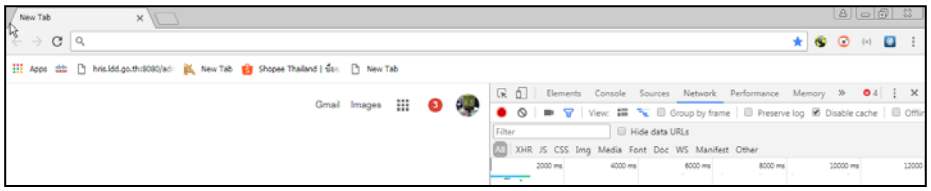


ภาพที่ ๕ – ๕ การตรวจสอบจำนวนแพ็กเก็ตที่มีการรับ-ส่งข้อมูล

๕.๑.๗ ดำเนินการทบทวนความสัมฤทธิผลของระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต ได้แก่ ช่วงเวลาที่เปลี่ยนแปลงไปในดาวน์โหลดข้อมูล

การทดสอบเพื่อได้รู้ว่าแม่ข่ายเสมือนรีเวิสพร็อกซี่สามารถช่วยลดเวลาในการดาวน์โหลดข้อมูล เพื่อให้ได้เปรียบเทียบการใช้งาน ต้องทดสอบโดยเครื่องคอมพิวเตอร์ที่เชื่อมต่อระบบเครือข่ายส่วนกลาง และได้แก้ไขไฟล์ Hosts ให้เรียกใช้งานเว็บไซต์ผ่านระบบตัวแทนการให้บริการเว็บไซต์ และทำตามขั้นตอนดังนี้

๕.๑.๗.๑ กำหนดโปรแกรม Google chrome ทำการกำหนดค่า Disable cache เพื่อไม่ให้โปรแกรมจำข้อมูลที่เคยได้ดาวน์โหวดไว้ โดยกำหนดที่ Google chrome console > network > Disable cache ทำเครื่องถูกที่ช่อง Disable cache



ภาพที่ ๕ – ๖ การกำหนดค่าโปรแกรม google chrome

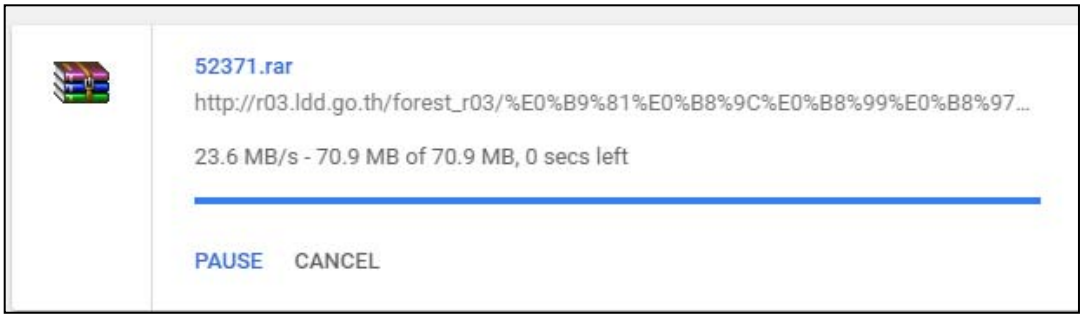
๕.๑.๗.๒ เลือกไฟล์ดาวน์โหลด คือ ไฟล์แผนที่ป่าไม้ถาวรจำแนก จ.นครราชสีมา 52371.rar จากเว็บไซต์สำนักงานพัฒนาที่ดินเขต ๓

ภาพที่ ๕ – ๗ จอภาพแสดงเมนูดาวน์โหลดภาพแผนที่ป่าไม้ถาวรตามมติคณะรัฐมนตรี ของเว็บไซต์สำนักพัฒนาที่ดินเขต ๓

๕.๑.๗.๓ อัตราความเร็วในการดาวน์โหลดแผนที่ จะได้อัตราความเร็วที่ ๖๘.๔ KB/s

ภาพที่ ๕ – ๘ อัตราความเร็วในการดาวน์โหลดรูปภาพแผนที่ในครั้งแรก

๕.๑.๗.๔ เมื่อเสร็จสิ้นการดาวน์โหลดแผนที่ในครั้งแรก ทำการลบไฟล์ที่ดาวน์โหลด และทำการดาวน์โหลดไฟล์อีกครั้ง ซึ่งจะได้อัตราความเร็วในการดาวน์โหลดแผนที่ ที่ ๒๓.๖ MB/s ซึ่งเป็นอัตราความเร็วที่เร็วกว่าในครั้งแรก จึงสรุปได้ว่า ช่วงเวลาที่เปลี่ยนแปลงไปในดาวน์โหลดข้อมูล มีอัตราความเร็วที่ดีกว่า



ภาพที่ ๕ – ๙ อัตราความเร็วในการดาวน์โหลดรูปภาพแผนที่ในครั้งที่สอง

๕.๒ บำรุงรักษาและปรับปรุงระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต (Act) ปฏิบัติดังนี้

หลังจากระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต เป็นไปตามแผนที่กำหนดไว้ เมื่อ ศทส. ได้รับการแจ้งเตือนจากศูนย์เตือนภัยต่าง ๆ ว่ามีเป้าหมายในการโจมตีผ่าน ช่องทางการควบคุมระบบบริหารจัดการเนื้อหาของเว็บไซต์ (Content Management System : CMS) ของโปรแกรม joomla ดังนั้น เพื่อลดความเสี่ยงภัยจากโจมตีผ่านทางอินเตอร์เน็ต จึงดำเนินการปิดช่องทางการเข้าถึงผ่านการเชื่อมต่ออินเตอร์เน็ต โดยกำหนดค่าเพิ่มเติมในระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต ในที่นี้ยกตัวอย่าง เว็บไซต์สำนักงานพัฒนาที่ดินเขต ๔ โดยดำเนินการดังนี้

๕.๒.๑ ตรวจสอบพบว่า ช่องทางการควบคุมระบบบริหารจัดการเว็บไซต์ CMS โปรแกรม joomla ของเว็บไซต์สำนักงานเขตพัฒนาที่ดินเขต ๔ จะสามารถเข้าถึงได้โดยเรียกใช้เว็บไซต์ r04.ldd.go.th/homer04/administrator จึงได้ทำการปิดกั้นการเข้าถึงผ่านการเชื่อมต่ออินเตอร์เน็ต โดยเพิ่มชุดคำสั่งในไฟล์ /etc/ngnix/conf.d/r04.conf เพิ่มการกำหนดค่า ดังนี้

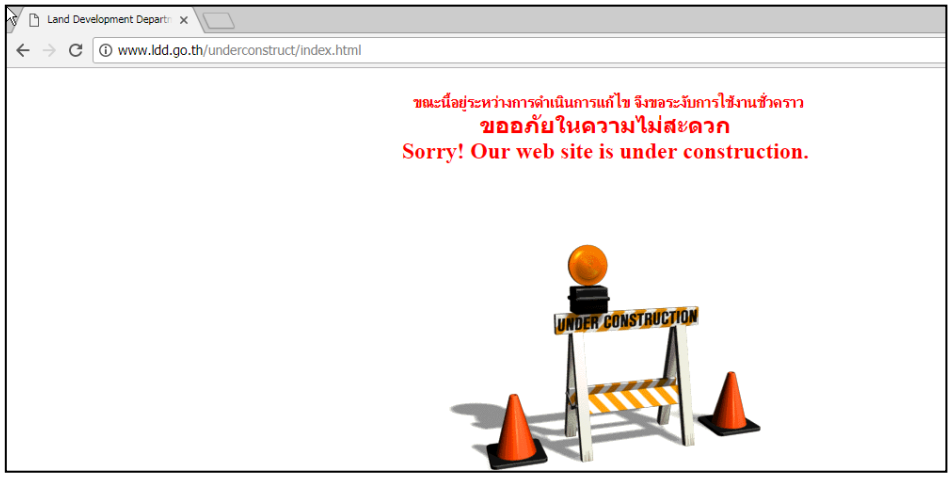
```
location ~* ^/homer04/administrator/ {
if ($request_uri ~* "/homer04/administrator/") {
  rewrite^/homer04/administrator/$http://www.ldd.go.th/underconstruct/
     index.html redirect;
  rewrite ^ http://www.ldd.go.th/underconstruct/index.html redirect;    } }
```

```
    }
  }

   location ~* ^/homer04/administrator/ {
   if ($request_uri ~* "/homer04/administrator/") {
        rewrite ^/homer04/administrator/$ http://www.ldd.go.th/underconstruct/index.html redirect;
        rewrite ^ http://www.ldd.go.th/underconstruct/index.html redirect;
#       return 404;
    }
  }
```

ภาพที่ ๕ – ๑๐ การเพิ่มกำหนดค่าปิดกั้น ไฟล์ชุดคำสั่งสำหรับเว็บไซต์ของสำนักงานพัฒนาที่ดินเขต ๔

๕.๒.๒ หากมีผู้บุกรุกจากภายนอกกรมฯ พยายามเรียกใช้งาน CMS ของเว็บไซต์สำนักงานพัฒนาที่ดินเขต ๔ URL http://r04.ldd.go.th/homer04/administrator ระบบ Reverse Proxy จะส่งค่าการร้องขอไปเรียกเว็บไซต์ (redirect) www.ldd.go.th/underconstruction/index.html แทน ทำให้ผู้ บุกรุกไม่สามารถเข้าสู่หน้า CMS ของเว็บไซต์สำนักงานพัฒนาที่ดินเขต ๔ ได้



ภาพที่ ๕ – ๑๑ จอภาพแสดงเว็บไซต์ www.ldd.go.th/underconstruct/index.html

บทที่ ๖
สรุปและข้อเสนอแนะ

ระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต พัฒนาขึ้นเพื่อช่วยเพิ่มประสิทธิภาพในการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต และลดช่องโหว่การโจมตีเว็บไซต์และภัยต่าง ๆ จากอินเตอร์เน็ต โดยระบบมีเทคโนโลยี แรมดิสก์ (Ram disk) เพื่อช่วยเพิ่มความเร็วในการแสดงข้อมูลเว็บไซต์ และมีการปรับปรุงชุดคำสั่งแตกต่างกัน เพื่อให้เหมาะสมกับการให้บริการเว็บไซต์ ซึ่งมีความคล่องตัว ในการเปลี่ยนแปลงชุดคำสั่งที่อาจเปลี่ยนแปลงได้ในอนาคตจากช่องโหว่การโจมตีเว็บไซต์ หรือภัยต่าง ๆ ที่เกิดขึ้นได้จากทางอินเตอร์เน็ต หรือจากการเปลี่ยนแปลงโครงสร้างเว็บไซต์ เป็นต้น จากการดำเนินงานระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต สามารถให้บริการได้อย่างมีประสิทธิภาพ และตรงตามวัตถุประสงค์ของโครงการ

๖.๑. ความยุ่งยากในการดำเนินการ/ ปัญหา/ อุปสรรค

๖.๓.๑ การออกแบบและพัฒนาเว็บไซต์ของหน่วยงานพัฒนาที่ดินเขต ถูกออกแบบและพัฒนาขึ้นโดยใช้องค์ประกอบที่แตกต่างกัน เช่น ภาษาที่ใช้ในการพัฒนา และฐานข้อมูลที่ใช้งาน เพื่อให้ตรงกับความต้องการของผู้รับบริการ และความถนัดของผู้พัฒนาเว็บไซต์ เช่น การนำเว็บไซต์มาใช้เผยแพร่ข้อมูลแผนที่ให้กับบุคคลากรภายในสำนักงานพัฒนาที่ดินเขต ดังนั้น การจัดทำระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต จึงต้องศึกษาวิเคราะห์และออกแบบระบบ เพื่อรองรับการทำงานและการแสดงผลของเว็บไซต์ให้สมบูรณ์และมีประสิทธิภาพ

๖.๓.๒ การกำหนดชุดคำสั่งเพิ่มเติมเพื่อลดช่องโหว่ของเว็บไซต์ หรือเพื่อปกป้องการโจมตีจากเครือข่ายอินเตอร์เน็ต ต้องตรวจสอบให้ดีก่อนว่าชุดคำสั่งที่จะนำไปใช้นั้นสามารถแสดงผลเว็บไซต์ได้เป็นไปตามปกติ แต่ถ้าชุดคำสั่งมีผลในการแสดงผล และเป็นช่องโหว่หรือภัยที่สำคัญ ต้องประสานไปยังผู้พัฒนาเว็บไซต์หรือผู้รับผิดชอบเว็บไซต์ เพื่อทำการเปลี่ยนแปลงกรรมวิธีในการแสดงผล หรือต้องช่วยหาแนวทางเพื่อให้เว็บไซต์ทำงานได้ตามปกติ

๖.๒. ผลที่ได้รับ

๖.๓.๑ มีระบบ Reverse Proxy ที่ช่วยในการลดช่วงเวลาในการรับ-ส่งข้อมูล (Load) เว็บไซต์มาแสดงผล เพื่อเพิ่มประสิทธิภาพในการให้บริการเว็บไซต์หน่วยงานพัฒนาที่ดิน สำหรับผู้สนใจเว็บไซต์ที่อยู่ภายนอก กรมพัฒนาที่ดิน จากการใช้เทคโนโลยี Ram disk ที่นำประสิทธิภาพในการอ่าน เขียนข้อมูลแรม (Remote Access Memory : RAM) ได้อย่างรวดเร็วนำมาเก็บข้อมูลไฟล์ Cache ของไฟล์ข้อมูลเว็บไซต์ที่ให้บริการ

๖.๓.๒ มีระบบ Reverse Proxy ที่ใช้เป็นเครื่องมือในจัดการป้องกันการโจมตีจากผู้บุกรุกภายนอกเครือข่ายกรมพัฒนาที่ดิน ได้ทันท่วงทีเมื่อได้รับการแจ้งเตือนภัยทางอินเทอร์เน็ต เหตุการณ์การโจมตี และป้องกันความเสี่ยง ไม่ให้มีผลกระทบต่อการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต สำหรับผู้ใช้งานเครือข่ายภายในกรมพัฒนาที่ดิน หากผู้บุกรุกจากเครือข่ายภายนอก พยามยามเข้าถึงช่องทางการ

บริหารจัดการเว็บไซต์ ระบบ Reverse Proxy จะทำการปิดกั้น เพื่อไม่ให้เข้าถึงช่องทางดังกล่าว โดยระบบจะทำการเปลี่ยนเส้นทาง (Redirect) ไปยังอีกเว็บไซต์หนึ่ง ตามที่ได้กำหนดค่าไว้

๖.๓. ข้อเสนอแนะ

๖.๓.๑ จัดให้มีบุคลากรทำหน้าที่ติดตามช่องโหว่ การโจมตีเว็บไซต์ และภัยต่าง ๆ จากอินเตอร์เน็ต ที่อาจจะมีผลกระทบกับการให้บริการเว็บไซต์ของหน่วยงานพัฒนาที่ดินเขต เพื่อหาวิธีหรือแนวทางการป้องกัน ที่สามารถนำมาใช้ในการปรับปรุงการกำหนดชุดคำสั่งของระบบตัวแทนการให้บริการเว็บไซต์หน่วยงาน สำนักงานพัฒนาที่ดินเขต ได้ทันท่วงที

๖.๓.๒ เว็บไซต์หน่วยงานสถานีพัฒนาที่ดิน เก็บอยู่ภายใต้เครื่องแม่ข่ายของเว็บไซต์สำนักงานพัฒนาที่ดินเขต ในการปรับปรุงเว็บไซต์หรือข้อมูลแต่ละครั้ง ต้องทำการปรับปรุงการเชื่อมต่อผ่านช่องทาง FTP Server การบริหารจัดการเนื้อหาเว็บไซต์ (Content Management System : CMS) หรือช่องทางอื่น ๆ ซึ่งมีความเสี่ยงที่อาจจะถูกผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลได้ จึงเสนอให้มีอุปกรณ์ หรือเครื่องมือที่มีลักษณะเป็นช่องทางในการเข้าถึงอย่างปลอดภัยจากภายนอกเครือข่าย เช่น วีพีเอ็น (Virtual Private Network : VPN) ก่อนที่จะทำการปรับปรุงเว็บไซต์หรือเปลี่ยนแปลงข้อมูล

๖.๓.๓ จัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ และบังคับใช้ให้หน่วยงานภายใน กรมพัฒนาที่ดินพัฒนาเว็บไซต์เป็นไปตามข้อกำหนด และมีบุคลากรที่มีความรู้ด้านการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ ทำหน้าที่ตรวจสอบว่าหน่วยงานได้พัฒนาเว็บไซต์เป็นไปตามมาตรฐาน รวมถึงการเฝ้าระวังภัยที่จะเกิดขึ้นจากการโจมตีบนระบบเครือข่าย ถึงช่องโหว่ของเว็บไซต์ที่พึ่งค้นพบและมีผลกับเว็บไซต์ภายในหน่วยงาน เพื่อแจ้งเตือนไปยังผู้แล รวมถึงปิดกั้นหรือปกป้องภัยที่อาจจะส่งผลกับเว็บไซต์ของหน่วยงานได้

๖.๓.๔ การโจมตีเว็บไซต์มีการพัฒนาขึ้นอยู่ตลอดเวลา ระบบตัวแทนการให้บริการเว็บไซต์หน่วยงานสำนักงานพัฒนาที่ดินเขต ก็เป็นส่วนหนึ่งที่สามารถลดช่องโหว่การโจมตีเว็บไซต์ได้ แต่ต้องติดตามภัยต่าง ๆ ที่มีการพัฒนาและต้องหาชุดคำสั่งเพื่อปรับปรุงให้สามารถปกป้องภัยได้ ถ้าสามารถจัดหาอุปกรณ์ที่สามารถปกป้องและมีการอัพเดทเครื่องมือเป็นอัตโนมัติ เช่น เว็บแอพพิเคชั่นไฟล์วอลล์ (Web Application Firewall) ก็จะสามารถลดความเสี่ยง และเพิ่มประสิทธิภาพในการให้บริการได้

บรรณานุกรม

คมกริช คำสวัสดิ์. ๒๕๕๙. **การใช้งาน Reverse Proxy โดย NGINX บน CentOS7**. กรุงเทพฯ: สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน).

ความหมายของ PDCA. ๒๕๕๕. (Online). https://sites.google.com/site/pumpkin2555/khwampdca, ๙ กุมภาพันธ์ ๒๕๖๑.

จตุชัย แพงจันทร์. ๒๕๕๘. **Master in Security 3rd Edition.** นนทบุรี. ไอดีซี พรีเมียร์ จำกัด.

โปรแกรมอรรถประโยชน์. (Online). https://th.wikipedia.org/wiki/โปรแกรมอรรถประโยชน์, ๙ กุมภาพันธ์ ๒๕๖๑.

ระบบปฏิบัติการ Operating System. ๒๕๕๘. (Online). www.thaiwebsocial.com/2015/09/ระบบปฏิบัติการหรือ-os-คืออะไร, ๙ กุมภาพันธ์ ๒๕๖๑.

เรืองไกร รังสิพล. ๒๕๔๕. **เปิดโลก Firewall และ Internet Security.** กรุงเทพมหานคร: โปรวิชั่น.

เว็บเซิร์ฟเวอร์และเอนจิ้นเอ็ก. (Online). http://www.softmelt.com/article.php?id=631, ๙ กุมภาพันธ์ ๒๕๖๑.

วิธีติดตั้ง Reverse Proxy ด้วย Squid. ๒๕๕๑. (Online). https://thanadet.wordpress.com/2008/11/29/วิธีติดตั้ง-reverse-proxy-ด้วย-squid, ๙ กุมภาพันธ์ ๒๕๖๑.

สานนท์ ฉิมพรี. ๒๕๕๒. **เขียนโปรแกรมและเรียนรู้เครือข่ายคอมพิวเตอร์ด้วย Ubuntu + Perl.** นนทบุรี: ไอดีซี พรีเมียร์ จำกัด.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). ๒๕๕๕. **ลีนุกส์และเซนต์โอเอส Operating System.** (Online). https://www.etda.or.th/content/1344.html, ๙ กุมภาพันธ์ ๒๕๖๑.

ไอพี แอดเดรส IP Address. (Online). http://www.เกร็ดความรู้.net/ip-address, ๙ กุมภาพันธ์ ๒๕๖๑.

Agent 47. ๒๕๕๘. Virtualization technology คืออะไร (Online). http://kraison-comp.blogspot.com, ๙ กุมภาพันธ์ ๒๕๖๑.

Bundit Nuntates. ๒๕๕๗. **HTTP Status Code – รวมความหมายของ Error Code บน Web Browser.** (Online). https://gunoob.com/http-status-code-404-403-500, ๙ กุมภาพันธ์ ๒๕๖๑.

Mark Allen. ๒๕๖๐. **The Advantages of Using a Forward and Reverse Proxy.** (Online). https://pro2col.com/advantages-using-forward-reverse-proxy, ๙ กุมภาพันธ์ ๒๕๖๑

Onestopwareblogger. ๒๕๖๐. **ไฟร์วอลล์ คืออะไร?.** (Online). blog.onestopware.com/ไฟร์วอลล์-คืออะไร, ๙ กุมภาพันธ์ ๒๕๖๑.

Paul Haining. ๒๕๖๐. **How a construction approach to safety can benefit everyone.** (Online). http://blog.usa.skanska.com/category/education, ๙ กุมภาพันธ์ ๒๕๖๑.

บรรณานุกรม (ต่อ)

Saixiii. ๒๕๖๐. **Proxy คืออะไร พร็อกซี่ ทำหน้าที่เป็นศูนย์กลางในการรับส่งข้อมูล.** (Online). https://saixiii.com/what-is-proxy, ๙ กุมภาพันธ์ ๒๕๖๑.

TechTalkThai. ๒๕๕๗. **SQL Injection กับความเชื่อผิดๆ.** (Online). https://www.techtalkthai.com/fallacy-of-sql-injection, ๙ กุมภาพันธ์ ๒๕๖๑.

Theerapat Montrisart. ๒๕๕๐. **เอกสารประกอบการฝึกอบรม Linux System Administration.** กรุงเทพฯ: MyComputer Training Center.

ภาคผนวก

ไฟล์ชุดคำสั่งหลักของโปรแกรม Nginx

etc/nginx/ngnix.conf

```
# For more information on configuration, see:
#   * Official English Documentation: http://nginx.org/en/docs/
* Official Russian Documentation: http://nginx.org/ru/docs/
user webproxy;
ชื่อผู้ใช้งานที่มีสิทธิเชื่อมโยงโปรแกรมกับระบบปฏิบัติการ
worker_processes auto;
pid /run/nginx.pid;
# Load dynamic modules. See /usr/share/nginx/README.dynamic
#  include /usr/share/nginx/modules/*.conf;
events {
    worker_connections 768;
}
http {
 server_tokens off;
ปิดการแสดงผลเวอร์ชันของโปรแกรม
    log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';
การกำหนดรูปไฟล์ log ว่าเก็บข้อมูล log ใดบ้าง
   access_log
syslog:server=10.1.203.20:514,facility=local7,tag=ReverseWebProxy,severity=info;
การกำหนดส่งค่า log ไปยัง centralized log  กรมพัฒนาที่ดิน
    access_log  /var/log/nginx/nginx_log/access.log  main;
    error_log   /var/log/nginx/nginx_log/error.log;
    sendfile            on;
    tcp_nopush          on;
    tcp_nodelay         on;
    types_hash_max_size 2048;
    gzip                off;
## Size Limits & Buffer Overflows
## the size may be configured based on the needs.
    client_header_buffer_size 1k;
```

```
    client_body_buffer_size 100k;
    client_max_body_size 100K;
    large_client_header_buffers 2 1k;
 การกำหนดขนาดขอบเขตไฟล์ที่ใช้ในการเชื่อมต่อ
## Timeouts definition ##
    client_body_timeout   10;
    client_header_timeout 10;
    keepalive_timeout     5 5;
    send_timeout          10;
การกำหนดเวลาใช้ในการเชื่อมต่อ
## End ##
    include             /etc/nginx/mime.types;
#    default_type        application/octet-stream;
    # Load modular configuration files from the /etc/nginx/conf.d directory.
    # See http://nginx.org/en/docs/ngx_core_module.html
    # for more information.
      include /etc/nginx/conf.d/*.conf;
การกำหนดให้อ่านไฟล์ใน path /etc/nginx/conf.d ซึ่งเป็นจัดเก็บไฟล์ของแต่ละเว็บไซต์
#      include /etc/nginx/block.d/*.conf;
 }
```

ไฟล์ชุดคำสั่งของเว็บไซต์ โดยยกตัวอย่างไฟล์ชุดคำสั่งสำหรับเว็บไซต์สำนักงานพัฒนาที่ดินเขต 1

```
# Server R01
 proxy_cache_path /ramdisk/cache_r01 levels=1:2 keys_zone=cache_r01:64m
max_size=512m inactive=20m  use_temp_path=off;
การกำหนดขนาดของไฟล์ที่จัดเก็บใน แรมดิสก์ (ramdisk)
## Limit Request
#limit_req_zone $binary_remote_addr zone=r03:32m rate=1000r/s;
#limit_req_zone $binary_remote_addr zone=notvalid:10m rate=10r/s;
server  {
  listen  80;
  server_name  r01.ldd.go.th;
การกำหนดถ้ามีการเรียกใช้งานเว็บไซต์ r01.ldd.go.th ที่ port ให้เรียกชุดคำสั่งจากไฟล์นี้
# Closing Slow Connections
  client_body_timeout 30s;
  limit_conn perip 10;
  limit_conn perserver 100;
# Block HEAD | GET | POST
 if ($request_method !~ ^(HEAD|GET|POST)$ ) {
                return 405;
  }
การกำหนดให้อนุญาตเรียกใช้ method ได้เฉพาะ  HEAD,GET และ POST นอกเหนือจากนี้ให้ส่งค่าเป็น
Http status code 405
 ## Block SQL injections
    set $block_sql_injections 0;
    if ($query_string ~ "union.*select.*\(") {
        set $block_sql_injections 1;
    }
    if ($query_string ~ "union.*all.*select.*") {
        set $block_sql_injections 1;
    }
    if ($query_string ~ "concat.*\(") {
        set $block_sql_injections 1;
    }
    if ($block_sql_injections = 1) {
        return 403;
    }
```

การกำหนดให้ เมื่อมีการเชื่อมต่อที่มีลักษณะการโจมตีรูปแบบ SQL injections ที่ ส่งค่าเป็น Http status code 403

```
## Block file injections
    set $block_file_injections 0;
    if ($query_string ~ "[a-zA-Z0-9_]=http://") {
        set $block_file_injections 1;
    }
    if ($query_string ~ "[a-zA-Z0-9_]=(\.\.//?)+") {
        set $block_file_injections 1;
    }
    if ($query_string ~ "[a-zA-Z0-9_]=/([a-z0-9_.]//?)+") {
        set $block_file_injections 1;
    }
    if ($block_file_injections = 1) {
        return 403;
    }
```

การกำหนดให้ เมื่อมีการเชื่อมต่อที่มีลักษณะการโจมตีรูปแบบ SQL injections ที่ ส่งค่าเป็น Http status code 403

```
## Block common exploits
    set $block_common_exploits 0;
    if ($query_string ~ "(<|%3C).*script.*(>|%3E)") {
        set $block_common_exploits 1;
    }
    if ($query_string ~ "GLOBALS(=|\[|\%[0-9A-Z]{0,2})") {
        set $block_common_exploits 1;
    }
    if ($query_string ~ "_REQUEST(=|\[|\%[0-9A-Z]{0,2})") {
        set $block_common_exploits 1;
    }
    if ($query_string ~ "proc/self/environ") {
        set $block_common_exploits 1;
    }
    if ($query_string ~ "mosConfig_[a-zA-Z_]{1,21}(=|\%3D)") {
        set $block_common_exploits 1;
    }
    if ($query_string ~ "base64_(en|de)code\(.*\)") {
        set $block_common_exploits 1;
```

```
    }
    if ($block_common_exploits = 1) {
        return 403;
    }
```

การกำหนดให้ เมื่อมีการเชื่อมต่อที่มีลักษณะการโจมตีรูปแบบ common exploits ที่ ส่งค่าเป็น Http status code 403

```
   access_log      /var/log/nginx/r01/r01_access.log;
   error_log       /var/log/nginx/r01/r01_error.log;
```

การกำหนดค่าจัดเก็บไฟล์ log

```
  location / {
      proxy_pass http://10.2.1.1/;
      proxy_redirect          off;
```

การกำหนดค่าเชื่อมไปต่อยังเครื่องแม่ข่ายสำนักงานพัฒนาที่ดินเขต ๑

```
#Header
      proxy_set_header Host $host;
      proxy_set_header X-Real-IP $remote_addr;
      proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
      proxy_connect_timeout 60;
      proxy_send_timeout 60;
      proxy_read_timeout 60;
      proxy_buffering on;
      proxy_buffers 128 64k;
      proxy_cache cache_r01;
      proxy_cache_valid  200 302 30m;
      proxy_cache_valid  404      1m;
```

การกำหนดค่าขอบเขตของไฟล์ Header ที่อนุญาตให้สามารถเชื่อมต่อ

```
#       limit_req zone=r03;
  }
}
```