ผลงานเรื่องที่ ๓

ผลงานฉบับเต็ม

เรื่อง

คู่มือการบริหารจัดการระบบสารสนเทศและคอมพิวเตอร์ กรมพัฒนาที่ดิน

ของ

นางจันทร์เพ็ญ ลาภจิตร
นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ ตำแหน่งเลขที่ ๑๘๒
ศูนย์สารสนเทศ กรมพัฒนาที่ดิน

ขอประเมินเพื่อแต่งตั้งให้ดำรงตำแหน่งนักวิเคราะห์นโยบายและแผนเชี่ยวชาญ
ตำแหน่งเลขที่ ๑๘๒
ผู้เชี่ยวชาญด้านสารสนเทศ
ศูนย์สารสนเทศ กรมพัฒนาที่ดิน
กระทรวงเกษตรและสหกรณ์

สารบัญ

หน้า

สารบัญภาพ

ภาพ **หน้า**

ภาพ **หน้า**

ภาพ **หน้า**

ภาพ **หน้า**

ภาพ **หน้า**

บทที่ ๑
บทนำ

๑. ความสำคัญของปัญหา

กรมพัฒนาที่ดินได้นำระบบสารสนเทศและคอมพิวเตอร์ เข้ามาใช้ในการเพิ่มประสิทธิภาพการปฏิบัติงานของกรมฯ และการให้บริการสำหรับประชาชน โดยมีสถาปัตยกรรมระบบเครือข่ายกรมพัฒนาที่ดิน เป็นแบบดาว (Star Topology) ประกอบด้วย ระบบเครือข่ายหลักส่วนกลาง (CLN : Central Local Area Network) และระบบเครือข่ายส่วนภูมิภาค (RLN : Regional Local Area Network) เชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตผ่านสื่อกลางหลายประเภท เช่น เฟรมรีเลย์ (Frame Relay) , MPLS , ADSL) มีการนำเอาเทคโนโลยีทางด้านระบบภาพ+เสียง+ข้อมูล (Multimedia) เช่น ระบบโทรศัพท์ผ่านไอพี (IP Phone) , ระบบถ่ายทอดสัญญาณวีดีโอ (Video Streaming) , ระบบกระจายสัญญาณ (Broadcasting), ระบบการประชุมสัญญาณวีดีโอ (Video Conference) ฯลฯ เข้ามาใช้งาน มีระบบฐานข้อมูลที่ ให้บริการทั้งภายในและภายนอกองค์กร ผ่านช่องทางการบริการข้อมูลเครือข่ายของผู้ให้บริการ (ISP: Internet Service Provider) โดยมีการเชื่อมโยงและแลกเปลี่ยนข้อมูลเข้ากับระบบบริการแผนที่และข้อมูลทางแผนที่และผลผลิต จากโครงการจัดทำแผนที่เพื่อการบริหารทรัพยากรธรรมชาติและทรัพย์สิน ของกระทรวงเกษตรและสหกรณ์ ที่ให้บริการสืบค้นข้อมูลแผนที่ภาพถ่ายทางอากาศสี และมีการเชื่อมโยงกับเครือข่ายกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารภายใต้โครงการพัฒนาเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ ซึ่งต้องใช้ความเชี่ยวชาญ ความรู้ความสามารถ ประสบการณ์และความชำนาญด้านระบบสารสนเทศและคอมพิวเตอร์อย่างสูง เพื่อช่วยในการวิเคราะห์ ตัดสินใจ วางแผนและแก้ไขปัญหาทางด้านระบบเครือข่าย ที่มีความยุ่งยาก ซับซ้อน และมีผลกระทบในวงกว้าง

การจัดการงานระบบสารสนเทศและคอมพิวเตอร์ของกรมพัฒนาที่ดิน ให้เกิดความปลอดภัยและมีเสถียรภาพ เป็นส่วนสำคัญในการทำให้งานด้านเทคโนโลยีสารสนเทศอื่นๆ เป็นไปได้อย่างราบรื่นและส่งผลต่อความเชื่อมั่นของระบบทั้งหมด จึงมีความจำเป็นอย่างยิ่งที่จะต้องเฝ้าระวังและปรับแต่งค่าการทำงาน ให้สามารถใช้งานได้ตลอดเวลา ผ่านทางเครื่องมือสำหรับบริหารความปลอดภัยด้านต่างๆที่เกี่ยวข้อง ประกอบด้วย ด้านการเฝ้าระวังและดูแล (Watchdog &Monitor) ด้านการเก็บข้อมูลการใช้งาน (Log) ด้านการบริหารเครื่องมือจากระยะไกล (Remote Management) ด้านการพัฒนาใช้งาน SNMP (Simple Network Protocol) ด้านการวิเคราะห์รูปแบบการให้บริการเครือข่าย (Network Bandwidth Shaping & QOS) ด้านการควบคุมการใช้งานเครือข่าย (Network Filtering) เพื่อให้สอดคล้องตามแผนแม่บทเทคโนโลยีสารสนเทศของกรมพัฒนาที่ดิน และตรงตามข้อกำหนดของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งสามารถดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ซึ่งการบริหารจัดการระบบดังกล่าว เป็นงานที่มีความยุ่งยาก ซับซ้อน เนื่องจากจะต้องทำความเข้าใจด้านวิชาการกฎหมายคอมพิวเตอร์ และมีทักษะขั้นสูงในระบบงานอื่นที่เกี่ยวข้อง เพื่อให้สามารถวิเคราะห์ ออกแบบ วางแผน กำหนดคุณสมบัติและค่าคอนฟิกกูเรชั่น (Configuration) บนอุปกรณ์ในส่วนของฮาร์ดแวร์ (Hardware) และซอฟท์แวร์ (Software) ที่ปัจจุบัน ที่มีความสลับซับซ้อนได้อย่างครบถ้วน อันจะส่งผลให้การใช้งานของระบบสารสนเทศและคอมพิวเตอร์ของกรมพัฒนาที่ดินเป็นไปตามวัตถุประสงค์ มีเสถียรภาพและความปลอดภัยสูงสุด

การบูรณาการข้อมูลภาครัฐ (Government Data Integration) เพื่อหาแนวทางในการปฏิบัติงานร่วมกันระหว่างระบบ (Interoperability) ของหน่วยงานภาครัฐ ให้สามารถแลกเปลี่ยนเชื่อมโยงข้อมูล เพื่อการปฏิบัติงานร่วมระหว่างระบบต่างๆที่แตกต่างกัน ผ่านทางเทคโนโลยีบริการด้านเวป (Web Services) ซึ่งสอดคล้องกับนโยบายของกรมพัฒนาที่ดิน ที่ได้นำงานบริการประชาชนและข้อมูลเผยแพร่ด้านการพัฒนาที่ดิน มาให้บริการผ่านเว็บไซต์บริการต่างๆของกรมพัฒนาที่ดิน อาทิเช่น www.ldd.go.th , mordin.ldd.go.th , lddmapserver.ldd.go.th ฯลฯ ในการขอรับบริการหรือเชื่อมโยงบริการผ่านระบบ Web Service ในการจัดทำระบบสารสนเทศและคอมพิวเตอร์ เพื่อรองรับงานบริการดังกล่าวนั้น จำเป็นจะต้องมีความรู้ ความชำนาญและประสบการณ์ทางด้าน ต่างๆที่เกี่ยวข้อง เช่น บริการด้านเวป (Web Service) โปรโตคอล (Protocol) พอร์ท (Port) การบริหารจัดการฐานข้อมูล (Database Management System) ภาษาและเครื่องมือในการออกแบบและพัฒนา (Language Utility and Develop Tool) และมีทักษะขั้นสูงในการประยุกต์ระบบงานต่างๆเข้าด้วยกัน เพื่อให้สามารถวิเคราะห์ ออกแบบ วางแผน กำหนดค่าคอนฟิกกูเรชั่น (Configuration) ของระบบเทคโนโลยีสารสนเทศบริการได้อย่างถูกต้อง

ดังนั้นเพื่อให้การบริหารจัดการระบบสารสนเทศและคอมพิวเตอร์ มีประสิทธิภาพ จึงได้จัดทำคู่มือการบริหารจัดการระบบสารสนเทศและคอมพิวเตอร์ กรมพัฒนาที่ดิน (LDD Manual Management Information Systems and Computer) ขึ้น เพื่อให้ผู้รับผิดชอบ/ผู้ปฏิบัติงาน มีความรู้ความเข้าใจเกี่ยวกับวิธีการ Configuration ระบบสารสนเทศ ระบบเครือข่าย ตลอดจน วิธีการแก้ไขปัญหาแนวทางการดำเนินงานระบบเทคโนโลยีสารสนเทศกรมพัฒนาที่ดิน ให้มีความน่าเชื่อถือ และมีเสถียรภาพ

๒. วัตถุประสงค์

๒.๑ เพื่อจัดทำคู่มือการบริหารจัดการระบบสารสนเทศและคอมพิวเตอร์ กรมพัฒนาที่ดิน

๒.๒ เพื่อให้ผู้ปฏิบัติงานใช้เป็นคู่มือในการดำเนินงานด้านระบบสารสนเทศและคอมพิวเตอร์ ให้มีประสิทธิภาพและประสิทธิผล

๓. ขอบเขตการศึกษา

๓.๑ ศึกษา วิเคราะห์ มาตรการรักษาความปลอดภัยระบบเครือข่ายของกรมพัฒนาที่ดิน ระบบ Authentication รายละเอียดการทำงานและการกำหนดค่าระบบพร็อกซี่ (Proxy) ระบบ ไฟล์วอลล์ (Firewall) ระบบตรวจสอบการบุกรุก (Intrusion Detection System) ระบบ Intrusion Prevention System และระบบควบคุมการเข้าถึงระบบ/ข้อมูล (Access Control) ศึกษามาตรฐานการจัดการความปลอดภัยระบบสารสนเทศ (Information Security Management)

๓.๒ ศึกษา วิเคราะห์ องค์ประกอบขั้นตอนและมาตรฐานการจัดทำบริการด้านเวป (web service) บริการด้านแอปพลิเคชั่น (application service) บริการด้านฐานข้อมูล (database service) บริการด้านจดหมายอิเลกทรอนิกส์ (e-mail service) บริการด้านป้องกันไวรัส (antivirus service) การบริหารจัดการโดเมน (domain service) รายละเอียดการใช้งานพอร์ท (port) และโปรโตคอล (protocol) ของแต่ละบริการ (service)

๓.๓ ศึกษา วิเคราะห์ แนวความคิดด้านเครื่องจักรเสมือน (Virtual Machine Concept) แนวคิดการสร้างเครื่องคอมพิวเตอร์เสมือนบน ฮาร์ดแวร์เพียงชุดเดียว ซึ่งสามารถทำงานได้เสมือนกับว่ามี

คอมพิวเตอร์หลายๆเครื่อง โดยมีการแยกการทำงานของระบบต่างๆได้อย่างเป็นอิสระต่อกัน มาตรฐานของเครื่องจักรเสมือน (Virtual Machine) และรูปแบบการใช้งานของเครื่องแม่ข่ายบริการ ในปัจจุบันของกรมพัฒนาที่ดิน

๓.๔ รวบรวมข้อมูลศึกษา วิเคราะห์ ในข้อ ๓.๑ – ๓.๓ ข้อมูลการปฏิบัติงานระบบสารสนเทศคอมพิวเตอร์ของกรมพัฒนาที่ดิน ข้อมูลอุปกรณ์สารสนเทศต่างๆ ที่นำมาใช้งาน และออกแบบการจัดทำรูปเล่ม การเรียงลำดับเนื้อหา ของคู่มือการบริหารจัดการระบบสารสนเทศคอมพิวเตอร์ กรมพัฒนาที่ดิน

๓.๕ จัดทำคู่มือการบริหารจัดการระบบสารสนเทศคอมพิวเตอร์ กรมพัฒนาที่ดิน ตั้งแต่การวางโครงสร้างของส่วนประกอบต่างๆสำหรับระบบฯ การออกแบบระบบฯ การติดตั้งระบบฯ การกำหนดค่าคุณลักษณะของอุปกรณ์เครือข่าย การกำหนดค่าคุณลักษณะของเครื่องแม่ข่ายบริการ (Server) การกำหนดมาตรการรักษาความปลอดภัยในส่วนของเครือข่ายและฐานข้อมูล การจัดการด้านงานบริการต่างๆ สำหรับเครื่องแม่ข่ายบริการ (Server Service) การจัดทำเอกสารอธิบายรายละเอียดในแต่ละขั้นตอน การจัดทำแผนภาพแสดงเครือข่าย (Network Diagram) และแผนภาพแสดงการไหลของข้อมูล (Data Flow Diagram) เพื่ออธิบายโครงสร้างระบบเครือข่าย การจัดทำรายละเอียดการทำงานและขั้นตอนการบริหารระบบงานของเครื่องแม่ข่ายบริการทั้งหมด การจัดทำรายละเอียดการทำงานและขั้นตอนการบริหารระบบเครือข่ายและอุปกรณ์พร้อมทั้งกระบวนการตรวจสอบประสิทธิภาพการทำงานของระบบสารสนเทศคอมพิวเตอร์

๔. ระยะเวลาและสถานที่ดำเนินการ

ระยะเวลา : ระหว่างเดือนตุลาคม ๒๕๕๔ - พฤษภาคม ๒๕๕๕

สถานที่ดำเนินการ : ศูนย์สารสนเทศ กรมพัฒนาที่ดิน

๕. ผู้ดำเนินการ

นางจันทร์เพ็ญ ลาภจิตร ตำแหน่ง นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ

มีหน้าที่ จัดทำคู่มือการบริหารจัดการระบบสารสนเทศคอมพิวเตอร์ กรมพัฒนาที่ดิน ปฏิบัติงาน ๑๐๐%

๖. ประโยชน์ที่จะได้รับ

๖.๑ นำไปใช้ในการการบริหารจัดการระบบสารสนเทศและคอมพิวเตอร์ ของกรมพัฒนาที่ดิน ให้มีความปลอดภัยและมีประสิทธิภาพสูงสุด

๖.๒ นำไปใช้ในการวิเคราะห์ แก้ไขปัญหา และปรับปรุงระบบสารสนเทศและคอมพิวเตอร์ ของกรมพัฒนาที่ดิน ให้สามารถบริการระบบสารสนเทศได้อย่างต่อเนื่อง สามารถใช้ในการประเมินและวางแผน การพัฒนาระบบสารสนเทศและคอมพิวเตอร์ ของกรมพัฒนาที่ดิน ให้รองรับงานและการบริการสารสนเทศตามแผนงาน การพัฒนาระบบสารสนเทศและคอมพิวเตอร์ ที่กรมพัฒนาที่ดินวางไว้ในอนาคต

๖.๓ นำไปใช้เป็นเอกสารประกอบการศึกษา ค้นคว้า อ้างอิง ทางด้านระบบสารสนเทศและคอมพิวเตอร์ สำหรับเจ้าหน้าที่และหน่วยงานที่เกี่ยวข้อง

บทที่ ๒
การวิเคราะห์และออกแบบระบบ

ในการดำเนินการวิเคราะห์และออกแบบ ระบบบริหารจัดการสารสนเทศและคอมพิวเตอร์ กรมพัฒนาที่ดิน (LDD Management Information Systems and Computer) มีกระบวนการในการดำเนินการที่เป็นขั้นตอน โดยได้มีการศึกษาวิเคราะห์มาตรการรักษาความปลอดภัยระบบเครือข่ายที่เหมาะสม วิเคราะห์ระบบการลงชื่อเข้าระบบ (Authentication) วิเคราะห์รายละเอียดการทำงานและการกำหนดค่าพร็อกซี่ (Proxy) วิเคราะห์ระบบ ไฟล์วอลล์ (Firewall) วิเคราะห์ระบบตรวจสอบและป้องกันการบุกรุก (Intrusion Detection System & Intrusion Prevention System) วิเคราะห์ระบบจดหมายอิเล็กทรอนิกส์ (Electronic Mail) วิเคราะห์ระบบควบคุมการเข้าถึงข้อมูล (Access Control) ตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพัฒนาที่ดิน วิเคราะห์ระบบการทำงานของเครื่องแม่ข่ายสำหรับงานบริการเว็บไซต์ โดยมีวัตถุประสงค์เพื่อให้ระบบสารสนเทศและคอมพิวเตอร์ของกรมพัฒนาที่ดินมีความเหมาะสม มีประสิทธิภาพ ครอบคลุมการทำงานต่าง ๆ ที่กำหนดไว้ ให้สามารถดำเนินงานได้อย่างต่อเนื่องและป้องกันภัยคุกคามต่าง ๆ ได้ พร้อมทั้งปฏิบัติตามเจตนารมณ์ของพระราชกฤษฎีกาการกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ มาตรา ๖ และมาตรา ๙ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ ของหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

ในขั้นตอนการวิเคราะห์และออกแบบ เพื่อกำหนดรายละเอียดการติดตั้ง และการดำเนินการบริหารจัดการระบบสารสนเทศ กรมพัฒนาที่ดิน (LDD Management Information Systems) นั้น ได้แบ่งขั้นตอนการวิเคราะห์และออกแบบ เป็นหัวข้อตามรายละเอียดต่าง ๆ ดังต่อไปนี้

๒.๑ การวิเคราะห์และออกแบบการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Acceptable use Analysis and Design)

๒.๒ การวิเคราะห์และออกแบบการใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟล์วอลล์ (Firewall Analysis and Design)

๒.๓ การวิเคราะห์และออกแบบการใช้งานระบบตรวจจับและป้องกันผู้บุกรุก (Intrusion Detection System : IDS and Intrusion Prevention System : IPS Analysis and Design)

๒.๔ การวิเคราะห์และออกแบบการใช้งานอินเตอร์เน็ต (Internet Analysis and Design)

๒.๕ การวิเคราะห์และออกแบบการเข้าถึง (Access Control Analysis and Design)

๒.๖ การวิเคราะห์และออกแบบการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail Analysis and Design)

๒.๑ การวิเคราะห์และออกแบบการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Acceptable Use Analysis and Design)

๒.๑.๑ องค์ประกอบของระบบสารสนเทศกับความมั่นคงปลอดภัย

ระบบสารสนเทศ (Information System : IS) นั้นสามารถทำงานได้โดยอาศัยองค์ประกอบหลายส่วน ได้แก่ ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) ข้อมูล (Data) บุคลากร (People) ขั้นตอนการทำงาน (Procedure) และเครือข่ายคอมพิวเตอร์ (Network) องค์ประกอบแต่ละส่วนจะมีหน้าที่ต่างกันไปในการนำข้อมูลเข้าสู่ระบบประมวลผลเพื่อสร้างสารสนเทศที่เป็นประโยชน์ และแสดงผลสารสนเทศเหล่านั้นออกทางหน่วยแสดงผลชนิดต่าง ๆ ซึ่งหมายความว่าองค์ประกอบแต่ละส่วนมีหน้าที่ในการทำงานแตกต่างกัน ดังนั้นจึงต้องการความมั่นคงปลอดภัยแตกต่างกันไป ดังนี้

๒.๑.๑.๑ ซอฟต์แวร์ (Software) ในโครงการพัฒนาซอฟต์แวร์ใด ๆ ย่อมต้องอยู่ภายใต้เงื่อนไขของการบริหารโครงการ นั่นคือ ภายใต้เวลา ต้นทุน และกำลังคนที่จำกัด ดังนั้น ส่วนใหญ่จะพบว่าการเพิ่มความปลอดภัยให้กับซอฟต์แวร์ มักจะทำภายหลังจากพัฒนาซอฟต์แวร์เสร็จแล้ว ไม่ได้ทำในตอนต้นของกระบวนการพัฒนา จึงทำให้ซอฟต์แวร์มีจุดอ่อน ง่ายต่อการจู่โจม ซึ่งแน่นอนว่าหากจู่โจมหรือสร้างความเสียหายให้กับซอฟต์แวร์แล้ว ก็จะส่งผลต่อข้อมูลของระบบด้วย

๒.๑.๑.๒ ฮาร์ดแวร์ (Hardware) นโยบายความมั่นคงปลอดภัยที่มีต่อฮาร์ดแวร์นั้นจะใช้นโยบายเดียวกับสินทรัพย์ที่จับต้องได้ขององค์กร นั่นคือ การป้องกันฮาร์ดแวร์จากการลักขโมยหรือภัยอันตรายต่าง ๆ เช่น การใส่กุญแจอุปกรณ์ชนิดต่าง ๆ ที่สามารถทำได้ การจำกัดการใช้งานอุปกรณ์เหล่านั้น หรือการจัดสถานที่ที่ปลอดภัยให้กับอุปกรณ์หรือฮาร์ดแวร์ เป็นต้น การป้องกันการเข้าถึงอุปกรณ์หรือฮาร์ดแวร์ต่าง ๆ จะช่วยลดโอกาสเข้าถึงหรือการสร้างความเสียหายให้กับสารสนเทศได้ระดับหนึ่ง

๒.๑.๑.๓ ข้อมูล (Data) ข้อมูล/สารสนเทศเป็นทรัพยากรที่มีค่ามากในองค์กร และเป็นเป้าหมายหลักของการโจมตีโดยเจตนา ถึงแม้ว่าระบบสารสนเทศในปัจจุบันมีระบบฐานข้อมูลที่มีเครื่องมือรักษาความมั่นคงปลอดภัยในเบื้องต้นไว้เป็นส่วนใหญ่แล้วก็ตาม แต่การป้องกันที่แน่นหนาขึ้นก็มีความจำเป็นสำหรับข้อมูลที่เป็นความลับ ซึ่งต้องอาศัยทั้งนโยบายความปลอดภัยและกลไกป้องกันที่ดีควบคู่กัน

๒.๑.๑.๔ บุคลากร (People) คือภัยคุกคามต่อความมั่นคงปลอดภัยของสารสนเทศที่ถูกมองข้ามมากที่สุด เนื่องจากถึงแม้ว่าองค์กรจะมีระบบรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีประสิทธิภาพมากเพียงใดก็ตาม แต่หากบุคลากรผู้เกี่ยวข้องไม่มีจิตสำนึก หรือมีความตระหนักถึงความปลอดภัย โดยเฉพาะหากบุคลากรไม่มีจรรยาบรรณในอาชีพก็เป็นจุดอ่อนที่ดีที่สุดของการโจมตี เนื่องจากผู้ไม่หวังดีสามารถเกลี้ยกล่อมให้บุคลากรดังกล่าวเปิดระบบให้ได้โดยไม่จำเป็นต้องใช้เครื่องมือใด ๆ เลย นอกจากนี้ บุคลากรอาจถูกหลอกลวงเพื่อให้ข้อมูลบางอย่างแก่มิจฉาชีพได้ จึงทำให้มีการศึกษาถึงเรื่องนี้กันอย่างจริงจัง เรียกว่า **“Social Engineering”** ซึ่งเป็นการป้องกันการหลอกลวงบุคลากร เพื่อเปิดเผยข้อมูลบางอย่างที่ทำให้เข้าสู่ระบบได้ โดยอาศัยพฤติกรรมที่เป็นจุดอ่อนของบุคลากรในการหลอกลวง

๒.๑.๑.๕ ขั้นตอนการทำงาน (Procedure) เป็นอีกหนึ่งองค์ประกอบด้านความปลอดภัยที่ถูกมองข้าม โดยหากมิจฉาชีพทราบถึงขั้นตอนการทำงานอย่างใดอย่างหนึ่งครบถ้วนแล้ว ก็จะสามารถค้นหาจุดอ่อนเพื่อกระทำการอันก่อให้เกิดความเสียหายทั้งต่อองค์กรและลูกค้าขององค์กรได้

๒.๑.๑.๖ เครือข่ายคอมพิวเตอร์ (Network) การเชื่อมต่อระหว่างคอมพิวเตอร์และระหว่างเครือข่ายคอมพิวเตอร์ ทำให้เกิดอาชญากรรมและภัยคุกคามคอมพิวเตอร์ชนิดใหม่จำนวนมาก

โดยเฉพาะการเชื่อมต่อระบบสารสนเทศเข้ากับเครือข่ายอินเตอร์เน็ต จัดว่ามีความเสี่ยงต่อภัยคุกคามสูงมาก ดังนั้น องค์กรที่มีการเชื่อมต่อระบบสารสนเทศเข้ากับอินเตอร์เน็ตจึงควรเพิ่มมาตรการรักษาความมั่นคงปลอดภัยที่แน่นหนาขึ้น

๒.๑.๒ วงจรการออกแบบระบบความมั่นคงปลอดภัยของสารสนเทศ

๒.๑.๒.๑ การสำรวจ (Investigation) โดยนำรายละเอียดในเบื้องต้นมาทำการสำรวจ กล่าวคือ ทำการเก็บข้อมูลเพื่อนำมาวิเคราะห์ปัญหา กำหนดขอบเขต เป้าหมาย และวัตถุประสงค์ของระบบฯ รวมถึงเงื่อนไขอื่น ๆ ในการดำเนินงาน ตลอดจนการศึกษาความเป็นไปได้ที่จะดำเนินงานด้วย

๒.๑.๒.๒ การวิเคราะห์ (Analysis) เป็นขั้นตอนที่นำข้อมูลจากการสำรวจมาทำการศึกษาเพิ่มเติม ถึงภัยคุกคามในปัจจุบันและวิธีป้องกันตามที่ได้ระบุไว้ในนโยบายความมั่นคงปลอดภัยเบื้องต้น วิเคราะห์ประเด็นด้านกฎหมายที่เกี่ยวข้องกับวิธีการหรือมาตรการป้องกัน พระราชบัญญัติว่าด้วยกรกระทำผิดทางคอมพิวเตอร์ ซึ่งรวมถึงกฎหมายสิทธิส่วนบุคคล (Privacy)

๒.๑.๒.๓ การออกแบบระดับตรรกะ (Logical Design) เป็นขั้นตอนการจัดทำโครงร่างของระบบความมั่นคงปลอดภัยของสารสนเทศ ตรวจสอบและจัดทำนโยบายหลักที่จะนำไปใช้ นอกจากนี้ยังต้องจัดทำแผนรับมือเหตุการณ์ไม่คาดคิด (Incident Response Action Plan) โดยในแผนงานจะต้องสามารถตอบคำถามต่าง ๆ ได้ดังนี้

๑) การทำงานของระบบจะสามารถดำเนินงานต่อไปได้อย่างไรในกรณีที่เกิดความเสียหาย

๒) ต้องดำเนินการอย่างไรเมื่อถูกโจมตี

๓) จะต้องฟื้นฟูระบบอย่างไรหลังจากได้รับความเสียหาย

๒.๑.๒.๔ การออกแบบระดับกายภาพ (Physical Design) เป็นขั้นตอนการกำหนดเทคโนโลยีสารสนเทศที่จะนำมาสนับสนุนโครงร่างระบบความมั่นคงปลอดภัยที่ได้ออกแบบไว้ในเฟสที่ผ่านมา โดยจะต้องมีการประเมินเทคโนโลยีดังกล่าว พร้อมสร้างทางเลือกของเทคโนโลยีที่จะนำมาใช้ แล้วนำมาคัดเลือกทางเลือกที่ดีและเหมาะสมที่สุด ซึ่งในกระบวนการดังกล่าวอาจพบว่าต้องมีการแก้ไขโครงร่างที่ได้ออกแบบไว้ ทั้งนี้ เนื่องจากอาจมีการเปลี่ยนแปลงบางอย่างที่เห็นว่าเหมาะสมกว่า

๒.๑.๓ การจารกรรมหรือการรุกล้ำ (Espionage or Trespass)

๒.๑.๓.๑ การจารกรรม (Espionage) เป็นการกระทำซึ่งใช้อุปกรณ์อิเล็กทรอนิกส์หรือตัวบุคคลในการจารกรรมสารสนเทศที่เป็นความลับ ผู้จารกรรมจะใช้วิธีการต่าง ๆ เพื่อเข้าถึงสารสนเทศที่จัดเก็บไว้ และรวบรวมสารสนเทศดังกล่าวโดยไม่ได้รับอนุญาต ซึ่งก็คือ การรวบรวมข้อมูล/สารสนเทศโดยผิดกฎหมายนั่นเอง อย่างไรก็ตาม มิจฉาชีพสามารถรวบรวมสารสนเทศไปใช้ประโยชน์ได้โดยถูกกฎหมาย เช่น การทำวิจัยทางการตลาดผ่านทางเว็บไซต์ จัดว่าเป็นวิธีการรวบรวมสารสนเทศที่ถูกกฎหมาย ในยุคแรกจึงมีผู้หาผลประโยชน์จากสารสนเทศด้วยวิธีดังกล่าวจำนวนมาก อย่างไรก็ตาม การกระทำดังกล่าวจัดว่าไม่มีจริยธรรมในการประกอบอาชีพ และต่อมาได้มีการกำหนดให้เป็นการกระทำที่ผิดกฎหมาย

อีกกรณีหนึ่งของการจารกรรมข้อมูลหรือการรุกล้ำเพื่อให้ได้สารสนเทศของผู้อื่นมา คือ “**Industrial Espionage**” เป็นการใช้เทคนิคที่ถูกกฎหมายแต่ก้ำกึ่งกับความไม่ชอบธรรม เพื่อรวบรวมสารสนเทศสำคัญหรือความลับทางการค้าของคู่แข่งเพื่อนำมาหาผลประโยชน์ แย่งชิงความ

ได้เปรียบในอุตสาหกรรม เทคโนโลยีที่ใช้เพื่อการจารกรรมสารสนเทศอาจเป็นไปได้ทั้งเทคโนโลยีชั้นสูง หรืออาจไม่ต้องใช้เทคโนโลยีใดเลยก็ได้ เช่น กรณีที่เรียกว่า **“Should Surfing”** คือ การแอบมองดูข้อมูลส่วนตัวของผู้อื่นขณะทำธุรกรรมผ่านตู้ ATM โดยเป็นการแอบมองจากด้านหลังหรือในระยะไกล เป็นต้น โดยกรณี Shoulder Surfing นั้น ยังรวมถึงการแอบมองหรือรวบรวมข้อมูลของผู้อื่นจากโต๊ะทำงาน เครื่องคอมพิวเตอร์ที่ผู้อื่นกำลังใช้งาน ตลอดจนแอบฟังการสนทนาทางโทรศัพท์ด้วย

๒.๑.๓.๒ การรุกล้ำ (Trespass) คือ การกระทำที่ทำให้ผู้รุกล้ำสามารถเข้าสู่ระบบเพื่อรวบรวมสารสนเทศที่ต้องการได้โดยไม่ได้รับอนุญาต การควบคุมการกระทำลักษณะดังกล่าว สามารถทำได้โดยการจำกัดสิทธิ์และพิสูจน์ตัวจนผู้เข้าสู่ระบบทุกครั้งว่าเป็นบุคคลที่ได้รับอนุญาตจริง (Authentication) เป็นกลไกการควบคุมที่สามารถป้องกันภัยคุกคามชนิดนี้ได้ในระดับหนึ่ง ต่อไปนี้เป็นตัวอย่างภัยคุกคามประเภท Espionage และ Trespass ที่รู้จักกันเป็นอย่างดี

๒.๑.๓.๓ แฮคเกอร์ (Hacker) หมายถึง บุคคลผู้ซึ่งใช้และสร้างซอฟต์แวร์คอมพิวเตอร์ขึ้นมา เพื่อช่วยให้ตนสามารถเข้าถึงสารสนเทศของผู้อื่นอย่างผิดกฎหมาย แฮคเกอร์บางกลุ่มอาจต้องการเพียงทดสอบความรู้ความสามารถของตนในการเข้าถึงสารสนเทศผู้อื่นเท่านั้น โดยไม่ได้มีเป้าหมายเพื่อขโมยหรือทำลายสารสนเทศและระบบ อย่างไรก็ตาม มีแฮคเกอร์บางกลุ่ม ที่มีเป้าหมายเพื่อขโมยสารสนเทศของผู้อื่นด้วย โดยการใช้ทักษะและกลลวงต่าง ๆ แฮคเกอร์กลุ่มนี้จึงเป็นภัยคุกคามต่อองค์กรอย่างมาก

๒.๑.๓.๔ Script Kiddies คือ แฮคเกอร์มือใหม่ ที่ไม่มีความชำนาญ เป็นผู้ที่ใช้ซอฟต์แวร์หรือโปรแกรมที่ Expert Hacker เขียนไว้มาใช้โจมตีหรือก่อกวนระบบผู้อื่น

๒.๑.๓.๕ Packet Monkeys คือ Script Kiddies ที่ใช้โปรแกรมอัตโนมัติโจมตีระบบแบบปฏิเสธการให้บริการ (Distributed Denial – of – Service) ทำให้ระบบไม่สามารถให้บริการแก่ผู้ใช้ตามคำร้องขอที่ส่งมาได้ ซึ่งบางครั้งทำให้ผู้ใช้เข้าใจผิดว่าระบบล้มเหลว โดยไม่สามารถทราบได้เลยว่าระบบกำลังถูกโจมตี

๒.๑.๓.๖ แครกเกอร์ (Cracker) คือ ผู้ที่ทำลายหรือทำซ้ำซอฟต์แวร์รักษาความมั่นคงปลอดภัยของระบบอื่น การทำลายระบบรักษาความมั่นคงปลอดภัยของระบบสารสนเทศผู้อื่น จัดว่าเป็นการสร้างความเสียหายให้เกิดขึ้น ดังนั้น แครกเกอร์จึงแตกต่างกับแฮคเกอร์ด้วยเหตุผลดังกล่าว นั่นคือ “แฮคเกอร์” มีเป้าหมายเพื่อทดสอบความสามารถหรือต้องการความท้าทายโดยการเจาะระบบให้สำเร็จ (ไม่รวมกรณีสร้างความเสียหายแก่สารสนเทศของระบบด้วย) ส่วน “แครกเกอร์” มีจุดประสงค์หลัก คือ ต้องการทำลายระบบรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์หรือระบบสารสนเทศ อย่างไรก็ตาม ภัยคุกคามทั้งสองจัดว่าเป็นอาชญากรรมคอมพิวเตอร์เหมือนกัน

๒.๑.๔ การโจมตีเครือข่าย

เครือข่ายเป็นเทคโนโลยีที่มีความเสี่ยงสูงมาก ถ้าไม่มีการควบคุมหรือป้องกันที่ดี การโจมตีหรือการบุกรุกเครือข่าย หมายถึงความพยายามที่จะเข้าใช้ระบบ (Access Attack) การแก้ไขข้อมูลหรือระบบ (Modification Attack) การทำให้ระบบไม่สามารถใช้การได้ (Deny of Service Attack) และการทำให้ข้อมูลเป็นเท็จ (Repudiation Attack) ซึ่งจะกระทำโดยผู้ประสงค์ร้าย ผู้ที่ไม่มีสิทธิ์ หรืออาจเกิดจากความไม่ตั้งใจของผู้ใช้เอง ต่อไปนี้เป็นรูปแบบ ต่าง ๆ ที่ผู้ไม่ประสงค์ดีพยายามที่จะบุกรุกเครือข่ายเพื่อลักลอบข้อมูลที่สำคัญหรือเข้าใช้ระบบโดยไม่ได้รับอนุญาต

๒.๑.๔.๑ การโจมตีรหัสผ่าน

การโจมตีรหัสผ่าน (Password Attack) หมายถึง การโจมตีที่ผู้บุกรุกพยายามเดารหัสผ่านของผู้ใช้คนใดคนหนึ่ง ซึ่งวิธีการเดานั้นก็มีหลายวิธี เช่น บรู๊ทฟอร์ธ (brute –Force) , โทรจันฮอร์ส (Trojan horse) , ไอพีสปูฟิง , แพ็กเก็ตสนิฟเฟอร์ เป็นต้น การเดาแบบบรู๊ทฟอร์ช หมายถึง การลองผิดลองถูกรหัสผ่านเรื่อย ๆ จนกว่าจะถูก บ่อยครั้งที่การโจมตีแบบบรู๊ทฟอร์ธใช้การพยายามล็อกอินเข้าใช้รีซอร์สของเครือข่าย โดยถ้าทำสำเร็จผู้บุกรุกก็จะมีสิทธิ์เหมือนกับเจ้าของแอ็คเคาท์นั้น ๆ

๒.๑.๔.๒ การโจมตีแบบ Man-in-the-Middle

การโจมตีแบบ Man-in-the-Middle นั้นผู้โจมตีต้องสามารถเข้าถึงแพ็กเก็ตที่ส่งระหว่างเครือข่ายได้ เช่น ผู้โจมตีอาจอยู่ที่ ISP ซึ่งสามารถตรวจจับแพ็กเก็ตที่รับส่งระหว่างเครือข่าย ภายในและเครือข่ายอื่น ๆ โดยผ่าน ISP การโจมตีนี้จะใช้แพ็กเก็ตสนิฟเฟอร์เป็นเครื่องมือเพื่อขโมยข้อมูล หรือใช้เซสชั่นเพื่อแอ็กเซสเครือข่ายภายใน หรือวิเคราะห์การจราจรของเครือข่ายหรือผู้ใช้

๒.๑.๔.๓ การโจมตีแบบ DOS

การโจมตีแบบดีไนล์ออฟเซอร์วิส หรือ DOS (Denial-of-Service) หมายถึง การโจมตีเซิร์ฟเวอร์โดยการทำให้เซิร์ฟเวอร์นั้นไม่สามารถให้บริการได้ ซึ่งโดยปกติจะทำโดยการใช้รีซอร์สของเซิร์ฟเวอร์จนหมด หรือ ถึงขีดจำกัดของเซิร์ฟเวอร์ ตัวอย่างเช่น เว็บ เซอร์เวอร์ และเอฟทีพีเซิร์ฟเวอร์ การโจมตีจะทำได้โดยการเปิดการเชื่อมต่อ (Connection) กับเซิร์ฟเวอร์จนถึงขีดจำกัดของเซิร์ฟเวอร์ ทำให้ผู้ใช้คนอื่น ๆ ไม่สามารถเข้ามาใช้บริการได้ การ โจมตีแบบนี้อาจใช้โปรโตคอลที่ใช้บนอินเตอร์เน็ตทั่ว ๆ ไป เช่น TCP(Transmission Control Protocol) หรือ ICMP (Internet Control Message Protocol) การโจมตีแบบแบบดีไนล์ออฟเซอร์วิส เป็นการโจมตีจุดอ่อนของระบบหรือเซิร์ฟเวอร์มากกว่าการโจมตีจุดบกพร่อง (Bug) หรือช่องโหว่ของระบบการรักษาความปลอดภัย

๒.๑.๔.๔ โทรจันฮอร์ส เวิร์ม และไวรัส

คำว่า “ โทรจันฮอร์ส (Trojan Horse) ” นี้เป็นคำที่มาจากสงครามโทรจัน ระหว่างทรอย (Troy) และ กรีก (Greek) ซึ่งเปรียบถึงม้าโครงไม้ที่ชาวกรีกสร้างทิ้งไว้แล้วซ่อนทหารไว้ข้างในแล้วถอนทัพกลับ พอชาวโทรจันออกมาดูเห็นม้าโครงไม้ทิ้งไว้ และคิดว่าเป็นของขวัญที่กรีซทิ้งไว้ให้จึงนำกลับเข้าเมืองไปด้วย พอตกดึกทหารกรีกที่ซ่อนอยู่ในม้าโครงไม้นี้ก็ออกมาเปิดประตูให้กับทหารกรีกเข้าไปทำลายเมืองทรอย สำหรับในความหมายคอมพิวเตอร์แล้ว โทรจันฮอร์ส หมายถึง โปรแกรมที่ทำลายระบบคอมพิวเตอร์โดยแฝงมากับโปรแกรมอื่น ๆ เช่น เกม สกรีนเซฟเวอร์ เป็นต้น ซึ่งผู้ใช้อาจจะดาวน์โหลดโปรแกรมต่าง ๆ เหล่านี้มา แต่เมื่อติดตั้งแล้วรันโปรแกรมโทรจันฮอร์สที่แฝงมาด้วยก็จะทำลายระบบคอมพิวเตอร์ เช่น ลบไฟล์ต่าง ๆ หรืออาจสร้างแบ็คดอร์ให้กับโปรแกรมอื่นเข้ามาทำลายระบบก็ได้

๒.๑.๕ มาตรการป้องกันการโจมตีจากผู้บุกรุก

๒.๑.๕.๑ ใช้ Intrusion Detection ดักจับผู้บุกรุกจากภายนอก

๒.๑.๕.๒ ตรวจหาช่องโหว่ภายใน Network

๒.๑.๕.๓ กำหนดระดับความปลอดภัยให้เหมาะสมกับ Server

๒.๑.๕.๔ ควบคุมแพ็กเก็ตเข้า – ออกด้วย เพื่อกรอง Network กราฟิกขององค์กรได้ทั้ง ขาเข้าและขาออก

๒.๑.๕.๕ เพื่อเพิ่มความปลอดภัยยิ่งขึ้น

๒.๑.๕.๖ ป้องกันการเข้าใช้งานที่ไม่ได้รับอนุญาตด้วยการตรวจสอบข้อมูลใน Network

๒.๑.๕.๗ ป้องกันเซิร์ฟเวอร์ที่เกี่ยวกับเว็บ อีเมล์ และแอปพลิเคชันอื่น ๆ จากการโจมตี

๒.๑.๖ รูปแบบการรักษาความมั่นคงปลอดภัยที่ออกแบบ

จากการดำเนินการจัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร ของกรมพัฒนาที่ดิน พ.ศ.๒๕๔๗ – ๒๕๔๙ ได้มีการพัฒนาและออกแบบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อป้องกันให้ระบบฯ มีความปลอดภัย และสามารถรองรับการทำงานได้ตลอดเวลา โดยแบ่งการรักษาความมั่นคงปลอดภัยระบบฯ ออกเป็น ๒ ส่วน ดังนี้

๒.๑.๖.๑ การรักษาความมั่นคงปลอดภัยของเครือข่าย

๑) การออกแบบการใช้งานเครือข่ายแบบ Vlan เพื่อป้องกันการรบกวนการทำงานของเครือข่าย

๒) การออกแบบสถาปัตยกรรมการเชื่อมต่อของอุปกรณ์เครือข่ายหลักแบบชั้น เพื่อให้เกิดเสถียรภาพในการทำงาน

๓) การออกแบบการตั้งค่า Access List Control บนอุปกรณ์เครือข่ายเพื่อควบคุมการใช้งาน IP Address และ Protocol ของเครื่องคอมพิวเตอร์ลูกข่าย

๔) การออกแบบการใช้งาน Proxy เพื่อลดปริมาณ Traffic ของการใช้งาน Internet

๕) การออกแบบสถาปัตยกรรมป้องกันการบุกรุกเครือข่ายจากภายนอกผ่านทางระบบ Firewall และระบบ IPS

๒.๑.๖.๒ การรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์

๑) การออกแบบการใช้งานระบบป้องกันไวรัส เพื่อแก้ปัญหา Malware ต่าง ๆ

๒) การออกแบบการใช้งานระบบ Virtual Machine Server (เครื่องแม่ข่ายเสมือน) เพื่อแก้ปัญหาการใช้งาน Hardware ไม่เข้ากันกับระบบปฏิบัติการ (Compatible) ลดเวลาการ Downtime ของเครื่องแม่ข่าย และช่วยให้การ Backup สามารถทำได้อย่างรวดเร็ว

๒.๒ การวิเคราะห์และออกแบบการใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟล์วอลล์ (Firewall Analysis and Design)

Firewall คือ ระบบที่ประกอบไปด้วยฮาร์ดแวร์ ซอฟต์แวร์ หรือทั้งสองอย่างที่ถูกออกแบบมาเพื่อป้องกัน Network จากการเข้าใช้งานที่ไม่ได้รับอนุญาต Firewall มีวิธีการออกแบบได้หลายรูปแบบ เช่น Bastion Host , Perimeter Network ซึ่งจำแนกเป็นแบบ Three-Homed และ Back –To-Back Firewall ใช้หลักการกรองแพ็กเก็ตข้อมูลและการกรองชนิดอื่นๆ เพื่อควบคุมการใช้งาน Network

Firewall หมายถึง กำแพงกันไฟ ซึ่งสร้างไว้ป้องกันไฟที่ไหม้จากบริเวณหนึ่งลุกลามไปบริเวณอื่น เพราะฉะนั้นถ้ามาใช้กับระบบ Network ก็มีประโยชน์คล้าย ๆ กัน โดยมันจะช่วยป้องกันอันตรายที่มาจากอินเทอร์เน็ต โดยปกติ Firewall จะถูกติดตั้งในจุดที่ Network ภายในจะติดต่อกับอินเทอร์เน็ต

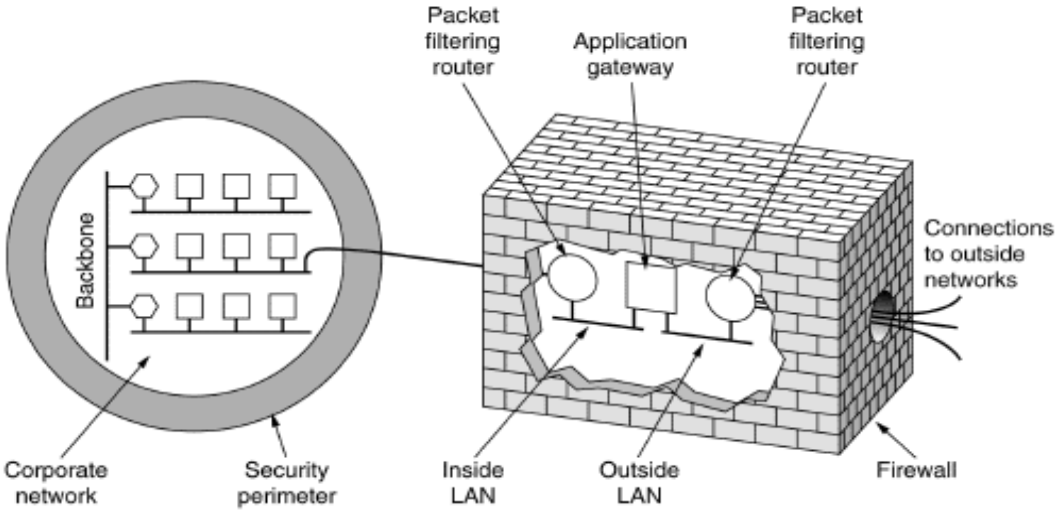
ผลิตภัณฑ์ Firewall ส่วนใหญ่ต้องมีความสามารถหลัก ๆ คือ เป็นจุดควบคุม Network ทราฟฟิกที่จะเข้ามาใน Network ภายในขององค์กร และเป็นจุดควบคุม Network ทราฟฟิกจากภายใน

องค์กรที่จะออกไปใช้งานอินเทอร์เน็ต โดยที่ Firewall ต้องบังคับให้ Network ทราฟฟิกเหล่านี้เป็นไปตามกฎและนโยบายความปลอดภัยที่องค์กรกำหนด

ความสามารถในการเชื่อมต่อเครื่องคอมพิวเตอร์ใดๆ เข้ากับคอมพิวเตอร์เครื่องอื่นได้ในทุกที่ที่ต้องการเป็นความสามารถที่มีทั้งผลดีและผลเสีย นอกเหนือจากอันตรายจากการรั่วไหลของข้อมูลแล้ว ยังมีอันตรายที่มากับข้อมูลที่ถูกใส่เข้ามาในระบบด้วยนั่นก็คือ ไวรัส และอันตรายจากโปรแกรมอันตรายต่าง ๆ ที่เข้ามาทำลายการรักษาความปลอดภัย ทำอันตรายกับข้อมูลที่มีค่า และทำให้สิ้นเปลืองเวลาอันมีค่ายิ่งของผู้ดูแลระบบที่พยายามที่จะทำให้ระบบอยู่ในสภาพที่ดี โดยทั่วไปโปรแกรมอันตรายเหล่านี้มักจะเกิดขึ้นจากพนักงานที่ไม่มีความระมัดระวังในการใช้งานหรือพนักงานที่พยายามจะสร้างสถานการณ์เลวร้ายให้เกิดขึ้นในองค์กร

ผลที่ตามมาคือ จำเป็นจะต้องมีกลไกที่จัดการเก็บรักษาข้อมูลที่ดีเอาไว้ในขณะที่กำจัดข้อมูลที่ไม่ดีออกไปจากระบบคอมพิวเตอร์ คือการใช้ Firewall

Firewall เป็นการปรับตัวของวิธีการรักษาความปลอดภัย ซึ่งบังคับให้ทุกคนเข้าหรือออกจากองค์กรโดยผ่านประตูหรือเส้นทางที่จัดเตรียมไว้ให้เท่านั้น ซึ่งจะทำให้ระบบสามารถตรวจสอบข้อมูลที่จะส่งเข้าหรือออกจากองค์กรได้ ดังรูปแสดงรายละเอียดส่วนประกอบของ Firewall ซึ่งประกอบด้วย packet filler จำนวน ๒ ตัว และ application gateway ดังที่แสดงในรูปต่อไปนี้



ภาพที่ ๑ รายละเอียดส่วนประกอบของ Firewall

Firewall ในลักษณะนี้ประกอบด้วยสองส่วน คือ เราเตอร์สองตัวที่ทำการตรวจสอบแพ็กเก็ตข้อมูล packet filtering และ application gateway ข้อมูลทุกแพ็กเก็ตจะต้องถูกส่งผ่านเราเตอร์สองตัว ซึ่งทำหน้าที่ในการกรองข้อมูลและจะต้องผ่าน application gateway เพื่อที่จะได้สามารถส่งข้อมูลออกไปนอกระบบหรือเข้ามาในระบบได้ โดยไม่มีเส้นทางอื่นให้เลือก

Packet filter แต่ละตัวคือเราเตอร์มาตรฐานทั่วไปที่ติดตั้งหน้าที่พิเศษเข้าไปด้วย นั่นคือการตรวจสอบข้อมูลที่ถูกส่งเข้ามาหรือส่งออกไป แพ็กเก็ตที่มีลักษณะถูกต้องตามข้อกำหนดจะถูกส่งต่อไปได้ตามปกติ ส่วนที่ไม่ผ่านข้อกำหนดก็จะถูกทำลายทิ้งไป ซึ่งเราเตอร์ที่อยู่ด้านในระบบ LAN จะทำหน้าที่

กรองข้อมูลที่จะถูกส่งออกไป ส่วนเราเตอร์ตัวที่อยู่นอกระบบ LAN จะทำหน้าที่ตรวจสอบแพ็กเก็ตที่จะถูกส่งเข้ามาในระบบ LAN แพ็กเก็ตที่ผ่านการตรวจขั้นต้นจากเราเตอร์ทั้งขาเข้าและขาออกจะถูกส่งไปตรวจสอบอีกขั้นตอนหนึ่งที่ application gateway การที่ต้องติดตั้งเราเตอร์ไว้สองตัวก็เพื่อให้แน่ใจได้ว่าจะไม่มีแพ็กเก็ตใดสามารถเดินทางเข้าหรือออกจากระบบได้โดยไม่ถูกตรวจสอบจาก application gateway เนื่องจากไม่มีเส้นทางอื่นให้เลือก โดยทั่วไปจะทำงานโดยอาศัยการกำหนดเงื่อนไขผ่านตารางข้อมูลที่ผู้ดูแลระบบเป็นผู้กำหนดขึ้นใช้งานตารางข้อมูลเหล่านี้ประกอบด้วยข้อมูลสามชนิด คือ จะแสดงที่อยู่ของที่มาของข้อมูลและเป้าหมายที่จะถูกส่งออกไปซึ่งเป็นสถานที่ที่ได้รับการตรวจสอบและอนุญาตให้ใช้งานได้ รวมทั้งที่อยู่ของผู้ส่งและผู้รับที่ไม่อนุญาตให้ใช้งานผ่านระบบเครือข่ายขององค์กร และกฎเกณฑ์ที่จะนำมาใช้ว่าจะต้องทำอย่างไรกับแพ็กเก็ตข้อมูลที่จะส่งออกนอกระบบหรือส่งเข้ามาในระบบ

ในกรณีทั่วไปที่สร้างขึ้นมาสำหรับระบบ TCP/IP ที่อยู่ของผู้ส่งและที่อยู่ของผู้รับประกอบด้วย IP address และหมายเลข Port ที่ใช้ (เป็นตัวกำหนดบริการที่เรียกใช้จากโพรโตคอล TCP/IP เช่น Port ๒๓ คือ telnet Port ๗๙ คือ finger และ Port ๑๑๙ คือ USENET เป็นต้น) องค์กรสามารถกั้นแพ็กเก็ตที่เดินทางเข้ามาสำหรับทุก IP address ที่ต้องใช้บริการใน Port ใดก็ได้ ด้วยวิธีการนี้บุคคลที่อยู่นอกองค์กรจะไม่สามารถ log-in เข้ามาใช้งานในระบบได้โดยการเรียกใช้บริการ telnet จาก Port ๒๓ ได้ยิ่งกว่านี้ องค์กรยังสามารถป้องกันไม่ให้พนักงานในองค์กรมัวแต่อ่านข่าวใน USERNET ทั้งวันโดยไม่ทำงานได้โดยการปิด Port ๑๑๙

การกั้นไม่ให้ส่งข้อมูลออกไปนั้นเป็นการทำงานที่ซับซ้อนกว่าเพราะว่าไซต์ส่วนใหญ่จะใช้ Port มาตรฐาน ยิ่งกว่านี้บริการที่สำคัญบางอย่าง เช่น FTP (file transfer protocol) หมายเลข Port จะถูกกำหนดให้ใช้ด้วยการเปลี่ยนแปลงหมายเลขไปเรื่อยๆ นอกจากนี้การกั้นการเชื่อมต่อ TCP นั้น ยากยิ่งขึ้นไปอีก เช่น การกั้นแพ็กเก็ต UDP นั้นยากมากเพราะไม่ทราบว่าแพ็กเก็ตนั้นจะทำอะไร Packet filter ส่วนใหญ่จึงไม่อนุญาตให้ใช้ UDP เลย

ส่วนที่สองของ Firewall คือ application gateway แทนที่จะมองดูที่ข้อมูลดิบที่ส่งมาในแพ็กเก็ตแต่เพียงอย่างเดียวเกตเวย์จะทำงานในระดับชั้นสื่อสารโปรแกรมประยุกต์ ตัวอย่างเช่น เมล์เกตเวย์ (mail gateway) สามารถที่จะจัดตั้งขึ้นมาเพื่อตรวจสอบแต่ละข่าวสารที่อยู่ในเมล์ทุกฉบับทั้งขาเข้าและขาออกเมล์แต่ละฉบับจะถูกตรวจสอบจากข้อมูลที่ปรากฏอยู่ใน header field หรือขนาดของข่าวสาร หรือแม้กระทั่งเนื้อหาที่อยู่ในเมล์ เช่น ในหน่วยที่ตั้งทางทหารถ้าหากตรวจพบว่ามีคำว่า “นิวเคลียร์” “ระเบิด” หรืออื่น ๆ เกตเวย์ก็สามารถที่จะแจ้งเตือนไปยังผู้รับผิดชอบได้เพื่อหาทางจัดการกับเมล์ฉบับนี้

โดยทั่วไปแล้ว Firewall แบ่งออกเป็น ๒ ประเภท คือ

๒.๒.๑ Application Layer Firewall

เป็นFirewallที่ทำงานในระดับแอพพลิเคชันเลเยอร์ (Application Layer Firewall) นั้นบางทีก็เรียกว่า “พร็อกซี่ (Proxy Firewall)” คือ โปรแกรมที่รันบนระบบปฏิบัติการทั่ว ๆ ไป เช่น วินโดวส์ เซิร์ฟเวอร์หรือยูนิกซ์ หรืออาจจะเป็นฮาร์ดแวร์ที่ติดตั้งซอฟต์แวร์พร้อมใช้งานแล้วก็ได้ Firewall จะมีเน็ตเวิร์คการ์ดหลายการ์ด เพื่อสำหรับเชื่อมต่อกับ เครือข่ายต่าง ๆ นโยบายการรักษาความปลอดภัยจะเป็นสิ่งที่กำหนดว่าทราฟฟิกใด สามารถถ่ายโอนระหว่างเครือข่ายใดได้บ้าง ถ้านโยบายไม่ได้ระบุอย่างชัดเจนว่า ทราฟฟิกไหนที่อนุญาตให้ผ่านได้ Firewall ก็จะไม่ส่งผ่านหรือละทิ้งแพ็กเก็ตนั้นทันที นโยบายนั้นจะถูกบังคับใช้โดยพร็อกซี่ใน Firewall ระดับแอพพลิเคชันนั้นทุก ๆ โปรโตคอลที่อนุญาตให้ผ่านได้

จะต้องมีพร็อกซี่สำหรับโปรโตคอลนั้น พร็อกซี่ที่ดีที่สุดนั้นจะเป็นพร็อกซี่ที่ออกแบบมาสำหรับจัดการกับโปรโตคอลนั้นโดยเฉพาะ Firewall ที่ทำงานในระดับแอพพลิเคชั่นปัจจุบันส่วนใหญ่จะมีพร็อกซี่สำหรับโปรโตคอลที่นิยมใช้ เช่น HTTP , SMTP , FTP และ Telnet เป็นต้น ถ้าโปรโตคอลไหนไม่มีพร็อกซี่ก็ไม่สามารถผ่าน Firewall ได้ นอกจากนี้ Firewall ประเภทนี้ยังสามารถซ่อนแอดเดรสหรือหมายเลขของระบบภายในได้ เนื่องจากการเชื่อมต่อทั้งหมดจะสิ้นสุดที่ Firewall ดังนั้นเครื่องที่อยู่ภายนอกจะมองเห็นเฉพาะหมายเลขไอพีของ Firewall เท่านั้น ถ้าผู้บุกรุกไม่รู้โครงสร้างภายในโอกาสที่จะเจาะระบบได้ก็น้อยลง

๒.๒.๒ Packet Filtering Firewall

เป็นแพ็กเก็ตฟิลเตอร์ริ่ง Firewall (Packet Filtering Firewall) อาจเป็นได้ทั้งซอฟต์แวร์หรือฮาร์ดแวร์ที่ทำหน้าที่กรองแพ็กเก็ตที่ผ่าน Firewall โดยใช้นโยบายการรักษาความปลอดภัยที่กำหนดไว้ แพ็กเก็ตฟิลเตอร์ริ่ง Firewall นั้นจะอนุญาตให้มีการเชื่อมต่อโดยตรงระหว่างไคลเอนท์และเซิร์ฟเวอร์ ดังนั้น Firewall ประเภทนี้จะทำงานค่อนข้างเร็วกว่าแบบแอพพลิเคชัน Firewall เนื่องจากไม่ต้องสร้างคอนเน็กชันใหม่ เราท์เตอร์โดยทั่วไปจะมีหลักการทำงานคือ เมื่อได้รับแพ็กเก็ตมาก็จะตรวจสอบหมายเลขไอพีของเครื่องปลายทาง หลังจากนั้นเราท์เตอร์ก็จะตรวจเช็คเราท์ติ้งเทเบิ้ล (Routing Table) เพื่อค้นหาเราท์เตอร์หรือโฮสต์ปลายทางที่จะส่งต่อไป ส่วนขั้นตอนการกรองแพ็กเก็ตของ Firewall นั้นจะทำก่อนที่จะส่งผ่านแพ็กเก็ตนี้ แพ็กเก็ตจะถูกกรองตามรายการควบคุมการเข้าถึง (Access Control List หรือ ACL) แต่ละรายการของ ACL จะประกอบด้วยฟิลด์ของเฮดเดอร์ของไอพีแพ็กเก็ตและการอนุญาตหรือไม่อนุญาตให้ผ่าน

๒.๒.๓ รูปแบบไฟล์วอลล์ ที่ออกแบบ

จากการวิเคราะห์ Firewall ที่เหมาะสมในการนำมาใช้งาน ได้ออกแบบเป็นรูปแบบผสมโดยการใช้Application Firewall ร่วมกับ Hardware Firewall ซึ่งใช้รูปแบบการวางโครงสร้างประเภท Bastion Host Firewall โดยมีการใช้เครื่องคอมพิวเตอร์ ๑ เครื่อง ทำหน้าที่เป็น Firewall ขั้นกลางจุดเชื่อมต่อ ระหว่างเครือข่ายภายในของกรมฯและเครือข่ายภายนอก (อินเทอร์เน็ต) และใช้ Hardware Box ขั้นกลางจุดเชื่อมต่อ ระหว่างเครือข่ายภายนอก (อินเทอร์เน็ต) ที่ต้องการเรียกเข้ามาใช้งานเครื่องแม่ข่ายบริการของกรมฯ

ข้อดีของระบบ

มีภาระการดูแลและจัดการน้อย และมีความยืดหยุ่นในการใช้งาน

ข้อจำกัดของระบบ

๑) ลักษณะการทำงาน เป็นการป้องกันแบบจุดเดียว (Single Point of Defense) ซึ่งต้องรักษาความปลอดภัยเครื่องคอมพิวเตอร์และ Firewall Box ที่ติดตั้งระบบ มิฉะนั้นอาจถูกโจมตีจากภายนอก และจากเครือข่ายภายในที่ไม่มีมาตรการป้องกัน

๒) ถ้าเครื่องที่ทำหน้าที่เป็น Firewall ถูกเจาะได้ ก็จะสามารถเข้าถึงระบบเครือข่ายภายในทันที (Single Point of Failure)

๓) ประสิทธิภาพในการรองรับปริมาณ Traffic ของระบบเครือข่ายสามารถรองรับได้ในระดับหนึ่ง ในกรณีที่ระบบเครือข่ายมีการขยายตัว จะต้องมีการ upgrade ระบบ หรือหาระบบอื่นที่มีความสามารถสูงกว่ามาทดแทน

๒.๓ การวิเคราะห์และออกแบบการใช้งานระบบตรวจจับและป้องกันผู้บุกรุก (IDS : Intrusion Detection System and IPS : Intrusion Prevention System IPS Analysis and Design)

๒.๓.๑ ระบบการตรวจจับการบุกรุก (Intrusion Detection System : IDS)

ระบบการตรวจจับการบุกรุก หรือ IDS (Intrusion Detection System) เป็นเครื่องมือสำหรับการรักษาความปลอดภัยอีกประเภทหนึ่งที่ใช้สำหรับตรวจจับความพยายามที่จะบุกรุกเครือข่าย โดยระบบแจ้งเตือนผู้ดูแลระบบเมื่อมีการบุกรุกหรือพยายามที่จะบุกรุกเครือข่าย IDS นั้นไม่ใช่ระบบที่ใช้ป้องกันการบุกรุกแต่เป็นระบบที่คอยแจ้งเตือนภัยเท่านั้น ถ้าเปรียบกับระบบการรักษาความปลอดภัยของรถ IDS ก็อาจจะเปลี่ยนได้กับระบบกันขโมย ซึ่งระบบนี้จะส่งสัญญาณเมื่อมีการตรวจพบความพยายามที่จะขโมยรถ เช่น การงัดประตู หรือกระจก แต่ระบบนี้ไม่สามารถป้องกันไม่ให้รถถูกขโมยได้ อย่างไรก็ตามโดยธรรมชาติแล้วขโมยจะพยายามหลีกเลี่ยงรถที่ติดตั้งระบบนี้ ระบบเครือข่ายก็เช่นกัน ถ้ามีระบบตรวจจับและแจ้งสัญญาณเตือนการบุกรุก เหล่ามิจฉาชีพมักจะหลีกเลี่ยงการบุกรุกเครือข่ายนี้

๒.๓.๑.๑ IDS แบ่งออกเป็น ๒ ประเภท คือ Host-Based IDS และ Network-Based IDS โดย โฮสต์เบสไอดีเอส นั่นคือ ระบบที่ติดตั้งที่โฮสต์เฝ้าระวังและตรวจจับความพยายามที่จะบุกรุกโฮสต์นั้น ส่วนเน็ตเวิร์ค เบสไอดีเอส นั่นคือ ระบบที่ตรวจดูแพ็กเก็ตที่วิ่งอยู่ในเครือข่าย และแจ้งเตือนถ้าพบหลักฐานที่คาดว่าจะเป็นการบุกรุกเครือข่าย

๑) Host-Based IDS

โฮสต์เบสไอดีเอสเป็นซอฟต์แวร์ที่รันบนโฮสต์ โดยปกติแล้ว IDS ประเภทนี้จะวิเคราะห์ล็อก (Log) เพื่อค้นหาข้อมูลเกี่ยวกับการบุกรุก ในระบบยูนิกซ์นั้นล็อกที่ IDS จะตรวจสอบ เช่น Syslog, Messages , Lastlog และ Wtmp เป็นต้น ส่วนในวินโดว์นั้น IDS ก็จะตรวจสอบอีเวนต์ล็อกต่าง ๆ เช่น System, Application และ Security เป็นต้น โดยปกติ IDS จะอ่านเหตุการณ์ใหม่ที่เกิดขึ้นในล็อกและเปรียบเทียบกับกฎที่ตั้งไว้ก่อนหน้า ถ้าตรงก็จะแจ้งทันที ดังนั้นการที่ IDS จะตรวจจับการบุกรุกได้ระบบจะต้องบันทึกเหตุการณ์ต่าง ๆ ที่สำคัญที่เกิดขึ้นกับระบบในล็อกไฟล์ มิฉะนั้น IDS ก็ไม่มีข้อมูลที่จะใช้ในการวิเคราะห์

๒) Network-Based IDS

เน็ตเวิร์คเบสไอดีเอส คือ ซอฟต์แวร์พิเศษที่รันบนคอมพิวเตอร์เครื่องหนึ่งแยกต่างหาก IDS ประเภทนี้จะมีเน็ตเวิร์คที่ทำงานในโหมดที่เรียกว่า “โพรมิสเซียส (Promiscuous Mode)” ซึ่งในโหมดนี้เน็ตเวิร์คการ์ดที่รันในโหมดธรรมดานั้น จะรับเอาเฉพาะแพ็กเก็ตที่มีที่อยู่ปลายทางตรงกับเครื่องเท่านั้น เมื่อทุก ๆ แพ็กเก็ตส่งผ่านไปให้แอพพลิเคชัน IDS จะวิเคราะห์ข้อมูลในแพ็กเก็ตเหล่านั้นกับกฎที่ได้ตั้งไว้ก่อนหน้า ถ้าตรงกับกฎก็จะแจ้งเตือนทันที

๒.๓.๑.๒ การแจ้งเตือนภัย IDS

IDS จะรายงานเฉพาะสิ่งที่กำหนดให้รายงานเท่านั้น มีอยู่สองสิ่งที่ผู้ดูแลระบบจะต้องคอนฟิกให้กับ IDS สิ่งแรกคือ ซิกเนเจอร์ของการบุกรุก สิ่งที่สองคือเหตุการณ์ที่ผู้ดูแลระบบให้ความสำคัญหรือเหตุการณ์ที่คาดว่าจะเป็นผลไปสู่การบุกรุกในภายหน้า ซึ่งเหตุการณ์ต่าง ๆ เหล่านี้อาจเป็นทราฟฟิกที่ไม่ปกติหรืออาจเป็นบางข้อความในล็อก

๒.๓.๑.๓ การสำรวจเครือข่าย

เหตุการณ์ที่เป็นการสำรวจเครือข่ายเป็นการพยายามของผู้บุกรุกที่จะรวบรวมข้อมูลเกี่ยวกับระบบเครือข่ายก่อนที่จะโจมตีจริง ๆ เช่น IP Scans, Port Scans, Trojan Scans, Vulnerability Scans, File Snooping

๒.๓.๑.๔ การโจมตี

การโจมตีเครือข่ายหรือระบบนั้นควรให้ลำดับความสำคัญสูงสุด เมื่อ IDS รายงานเหตุการณ์นี้ผู้ดูแลระบบต้องตอบสนองกับเหตุการณ์นี้ทันทีเพื่อป้องกันการสูญเสียมากกว่านี้ บางครั้ง IDS อาจแยกแยะระหว่างการโจมตีจริง ๆ กับการสแกนหาจุดอ่อน เนื่องจากเหตุการณ์ทั้งสองนั้น IDS จะตรวจพบซิกเนเจอร์ของการโจมตีเหมือนกัน ผู้ดูแลระบบอาจต้องวิเคราะห์ข้อมูลเพิ่มเติม การสแกนหาจุดอ่อนนั้น IDS จะรายงานการโจมตีหลายๆ รูปแบบในช่วงเวลาสั้น ๆ กับระบบใดระบบหนึ่ง ส่วนการโจมตีจริงนั้นอาจมีการรายงานการโจมตีแค่รูปแบบเดียวกับระบบใดระบบหนึ่งเหตุการณ์ที่น่าสงสัยหรือผิดปกติเหตุการณ์อื่น ๆ ที่ผิดปกติและไม่ได้จัดอยู่ในประเภทต่าง ๆ ที่กล่าวมาข้างต้นถือว่าเป็นเหตุการณ์ที่น่าสงสัยว่าอาจมีการโจมตีเครือข่ายเกิดขึ้น ซึ่งผู้ดูแลระบบต้องวิเคราะห์และสืบหาสาเหตุของเหตุการณ์ที่ว่านี้ต่อ ตัวอย่างเช่น บางโฮสต์อาจส่งแพ็กเก็ตที่มีข้อมูลส่วนหัวผิดไปจากที่กำหนดในมาตรฐาน ซึ่งเหตุการณ์นี้อาจเกิดขึ้นเนื่องจากการโจมตีแบบ
ใหม่ หรือเน็ตเวิร์คการ์ดเครื่องส่งอาจเสีย

๒.๓.๒ ระบบการป้องกันการบุกรุก (Intrusion Prevention System: IPS)

ระบบที่คอยป้องกันการบุกรุก (Intrusion Prevention System) Intrusion Prevention System (IPS) คือ ระบบที่คอยตรวจจับการบุกรุกของผู้ที่ไม่ประสงค์ดี รวมไปถึงข้อมูลจำพวกไวรัสด้วย โดยสามารถทำการวิเคราะห์ข้อมูลทั้งหมดที่ผ่านเข้าออกภายในเครือข่ายว่า มีลักษณะการทำงานที่เป็นความเสี่ยงที่ก่อให้เกิดความเสียหายต่อระบบเครือข่ายหรือไม่ เมื่อตรวจพบข้อมูลที่มีลักษณะการทำงานที่เป็นความเสี่ยงต่อระบบเครือข่ายก็จะทำการป้องกันข้อมูลดังกล่าวนั้น ไม่ให้เข้ามาภายในเครือข่ายได้ โดยสามารถแบ่งประเภทของ IPS ได้ดังนี้ คือ

๒.๓.๒.๑ แบ่งตามแพลตฟอร์ม (Network / Host based)

วิธีการแบ่งประเภทตามแพลตฟอร์ม จะแบ่งออกได้เป็น ๒ ประเภท คือ Network Intrusion Prevention Systems (NIPS) และ Host Intrusion Prevention Systems (HIPS) ซึ่ง NIPS เฝ้ามองทราฟฟิกภายในระบบเน็ตเวิร์กว่า มีการมุ่งประสงค์ร้ายจากภายนอกที่น่าสงสัยหรือไม่ หรือว่ามีกิจกรรมภายในเน็ตเวิร์กที่น่าสงสัยหรือไม่ ถ้าพบก็จะปิดกั้นเครือข่ายที่น่าสงสัยเหล่านั้น ส่วน HIPS นั้นจะถูกติดตั้งให้อยู่ที่เครื่องโฮสต์หน้าที่โดยทั่วไปคือ เฝ้ามองส่วนของการร้องขอ (request) ของระบบแล้วปิดกั้นการร้องขอที่ไม่เหมาะสม ในส่วนของ NIPS นั้นจะแจ้งเตือนปัญหาและป้องกันในส่วนของสภาพแวดล้อมของเครือข่าย ในขณะที่ HIPS จะเจาะจงไปยังเครื่องโฮสต์เครื่องใดเครื่องหนึ่งเท่านั้น

๒.๓.๒.๒ แบ่งตาม attack timeline

เป็นการแบ่งตามความสามารถในการตรวจจับการโจมตีแบบ “zero-day” ซึ่งขึ้นอยู่กับฐานข้อมูลที่มี แต่ถ้าไม่มีการอัพเดตเพิ่มเติมนั้น ในกรณีนี้การโจมตี “zero-day” เป็นการโจมตีที่ไม่สามารถตรวจจับได้ แล้ว เมื่อสามารถแยกแยะรูปแบบการโจมตีได้แล้วจึงเรียกว่าการโจมตีที่สามารถตรวจจับได้ ดังนั้นการตรวจจับการโจมตีที่ไม่สามารถตรวจจับได้ แต่เดิมจะช่วยให้ความสามารถใน

การป้องกันของ IPS เพิ่มมากขึ้น ในขณะที่การตรวจจับการโจมตีที่สามารถตรวจจับได้นั้น ทำให้แยกความแตกต่างของชนิดและรูปแบบการโจมตีได้แบบจำเพาะเจาะจงได้มากขึ้น

๒.๓.๒.๓ รูปแบบการใช้งานระบบตรวจจับและป้องกันผู้บุกรุก ที่ออกแบบ

จากการวิเคราะห์ระบบตรวจจับและป้องกันผู้บุกรุก ที่เหมาะสมในการนำมาใช้งาน ได้ออกแบบเป็นรูปแบบ Network Intrusion Prevention Systems (NIPS) และ Host Intrusion Prevention Systems (HIPS) โดยรูปแบบ NIPS มีการใช้งานผ่านทางเครื่องคอมพิวเตอร์ ๑ เครื่อง ทำหน้าที่เป็น IPS ที่ทำงานร่วมกับ Firewall ที่ขั้นกลางจุดเชื่อมต่อ ระหว่างเครือข่ายภายในของกรมฯและเครือข่ายภายนอก (อินเทอร์เน็ต) และใช้ HIPS ที่ติดตั้งมากับระบบป้องกันไวรัสในเครื่องคอมพิวเตอร์ แม่ข่ายทำหน้าที่เป็น IPS ขั้นกลางจุดเชื่อมต่อเครือข่ายภายนอก (อินเทอร์เน็ต) ที่ต้องการเรียกเข้ามาใช้งานเครื่องแม่ข่ายบริการของกรมฯ

๒.๔ การวิเคราะห์และออกแบบการใช้งานอินเตอร์เน็ต (Internet Analysis and Design)

ในการใช้งาน Internet ได้มีการวิเคราะห์และออกแบบโดยใช้มาตรการทำงานของอุปกรณ์เครือข่ายที่ใช้กันอยู่ในปัจจุบัน เพื่อให้ระบบฯ สามารถใช้งานได้อย่างมีประสิทธิภาพและมีเสถียรภาพ โดยมีการออกแบบระบบที่ใช้งาน ดังนี้คือ

๒.๔.๑ NAT (Network Address Translation)

NAT : คือ กระบวนการแปลงค่า Source IP Address หรือ Destination IP Address หรือ Source Port ในส่วนหัวของแพ็กเก็ตเพื่อให้แพ็กเก็ตนั้นวิ่งเข้าหรือออกตามตารางเส้นทางที่ได้ออกแบบไว้ NAT แบ่งเป็น ๒ ชนิดใหญ่ ๆ ได้แก่ Static NAT และ Dynamic NAT

๒.๔.๑.๑ Static NAT

Static NAT หรือตามมาตรฐาน RFC-๓๐๒๒ เรียกว่า NAT (ไม่มีคำว่า Static นำหน้า) คือ การแม็ปเพื่อแปลงค่าไอพีแอดเดรสระหว่างไอพีภายใน (private ip) กับไอพีจริง (public ip) แบบหนึ่งต่อหนึ่ง เพื่อให้คอมพิวเตอร์ที่อยู่บนอินเตอร์เน็ตมองเห็นคอมพิวเตอร์ในเครือข่ายภายในหน่วยงานที่ใช้ไอพีภายใน (private ip) ตัวอย่างเช่น หน่วยงานแห่งหนึ่งได้รับจัดสรรไอพีแอดเดรสช่วง ๒๐๐.๑.๑.๐ – ๒๐๐.๑.๑.๒๕๕ และออกแบบให้เว็บเซิร์ฟเวอร์สมารถมองเห็นได้จากอินเตอร์เน็ตผ่านไอพีแอดเดรสหมายเลข ๒๐๐.๑.๑.๕ แต่ผู้ดูแลระบบกำหนดค่าไอพีแอดเดรสที่เครื่องเว็บเซิร์ฟเวอร์เป็นไอพีภายในหมายเลข ๑๙๒.๑๖๘.๙๙.๓ ไม่ได้กำหนดเป็นไอพีจริง ดังนั้นเมื่อต้องการให้คอมพิวเตอร์ที่อยู่บนอินเตอร์เน็ตสื่อสาร กับเว็บเซิร์ฟเวอร์เครื่องนี้ได ก็จะต้องกำหนดค่าคอนฟิกเกี่ยวกับ Static NAT บน Firewall เพื่อทำการแม๊ประหว่าง ๒๐๐.๑.๑.๕ กับ ๑๙๒.๑๖๘.๙๙.๓ หลังจากที่ได้สร้างตาราง Static NAT บน Firewall แล้ว เมื่อแพ็กเก็ตที่ถูกสร้างโดยเว็บเซิร์ฟเวอร์ซึ่งมีไอพีแอดเดรสหมายเลข ๑๙๒.๑๖๘.๙๙.๓ จะถูกส่งไปยังอินเตอร์เน็ต โดยแพ็กเก็ตจะวิ่งออกจากเครื่องต้นทางผ่าน Firewall เมื่อแพ็กเก็ตมาถึง Firewall ก่อนที่ Firewall จะเริ่มส่งแพ็กเก็ตดังกล่าวออกไป Firewall จะแปลง (Translate) ค่า Source IP Address จาก ๑๙๒.๑๖๘.๙๙.๓ ให้เป็น ๒๐๐.๑.๑.๕ ก่อน จากนั้นจึงค่อยส่งออกไปสู่อินเตอร์เน็ต เมื่อมีการตอบกลับจากโฮสต์ที่อยู่บนอินเตอร์เน็ตก็จะมีการส่งแพ็กเก็ตที่ระบุว่าให้ส่งกลับมายังไอพีแอดเดรสปลายทางหมายเลข ๒๐๐.๑.๑.๕ และขณะที่แพ็กเก็ตวิ่งเข้ามาถึง Firewall Firewall ก็จะแปลง (Translate) ค่า Destination IP Address ให้กลับมาเป็น ๑๙๒.๑๖๘.๙๙.๓ เพื่อที่แพ็กเก็ตดังกล่าวจะได้วิ่งเข้ามาถึงเครื่องเว็บเซิร์ฟเวอร์ได้ และหากหน่วยงานแห่งนี้มี Mail Server ตั้งอยู่

ภายใน โดยผู้ดูแลระบบกำหนดค่าไอพีแอดเดรสให้เป็น ๑๙๒.๑๖๘.๙๙.๗ และมีการกำหนดที่ Firewall ในตาราง NAT ให้อินเตอร์เน็ตมองเห็นเป็น ไอพีจริงหมายเลข ๒๐๐.๑.๑.๔ ทุกครั้งที่มีการส่งอีเมล์ออกไปยังอินเตอร์เน็ตแพ็กเก็ตที่ถูกสร้างโดยเครื่อง Mail Server นี้ จะถูกแปลงไอพีแอดเดรสต้นทางให้เป็น ๒๐๐.๑.๑.๔ โดย Firewall ก่อนที่จะส่งออกไปยังอินเตอร์เน็ต และเมื่อมีแพ็กเก็ตที่มาจากอินเตอร์เน็ตส่งเข้ามายัง Mail Server ไอพีแอดเดรส ๒๐๐.๑.๑.๔ เมื่อแพ็กเก็ตวิ่งเข้ามาถึง Firewall ซึ่งเป็นด่านหน้ามันจะถูกแปลงให้มีปลายทางเป็นไอพีแอดเดรส ๑๙๒.๑๖๘.๙๙.๗ เพื่อที่แพ็กเก็ตนี้จะได้เดินทางมาถึงเครื่อง Mail Server ที่ใช้ไอพีภายใน เห็นได้ว่า Firewall มีการสร้างตารางคงที่เพื่อแม๊ปค่าระหว่างไอพีภายในกับไอพีจริงแต่ละคู่ด้วยค่าไอพีแอดเดรสที่คงที่ เลยเป็นที่มาของคำว่า “Static NAT”

๒.๔.๑.๒ Dynamic NAT หรือ Internet Share

Static NAT หรือตามมาตรฐาน RFC-๓๐๒๒ เรียกว่า NAPT (Network Address Port Translation) และภาษาของผู้ใช้ทั่วไปเรียกว่า Internet Share คือการแม็ปเพื่อแปลงค่าไอพีแอดเดรสระหว่างไอพีภายใน (private ip) หนึ่งหมายเลข โดยใช้ค่าตัวเลข Source Port เข้ามาร่วมด้วย เพื่อให้ แพ็กเก็ตที่ถูกสร้างจากเครื่องที่ใช้ไอพีภายในหมายเลขต่าง ๆมีค่า Source IP Address เป็นค่าไอพีจริง ก่อนที่จะถูกส่งออกไปยังอินเตอร์เน็ต เพื่อทำให้แพ็กเก็ตขากลับ สามารถวิ่งกลับมายัง Network ต้นทางได้อย่างถูกต้อง ตัวอย่างเช่น หน่วยงานแห่งหนึ่งเชื่อมต่อกับ ISP และได้ไอพีจริงมาเพียงหมายเลขเดียว อุปกรณ์ที่ทำหน้าที่เป็นเราเตอร์ (หรือ Firewall) ซึ่งมีอินเตอร์เฟสด้านนอกเป็นไอพีจริง สมมติว่าเป็นหมายเลข ๒๐๐.๒.๒.๕ ส่วนอินเตอร์เฟสด้านในเป็นไอพีภายในหมายเลข ๑๙๒.๑๖๘.๑.๑ เมื่อคอมพิวเตอร์ในเครือข่าย LAN ภายใน ต้องการท่องเว็บในอินเตอร์เน็ต ก็จะมีการส่งแพ็กเก็ตออกไป เช่น ๑๙.๒.๑๖๘.๑.๒ ส่ง TCP packet ไปที่ www.sanook.com โดยใช้ Source Port หมายเลข ๑๐๒๔ เมื่อแพ็กเก็ตมาถึง Firewall ตัว Firewall จะแปลงค่า Source IP Address ให้เป็นค่าไอพีแอดเดรสขาออกของ Firewall (ซึ่งเป็นไอพีจริงหมายเลข ๒๐๐.๒.๒.๕) และแปลค่า Source Port ให้เป็นค่า Source Port ของ Firewall ว่างอยู่ เช่น แปลงให้เป็นหมายเลข ๔๐๐๑ แล้วจึงส่งแพ็กเก็ตออกไปสู่อินเตอร์เน็ต เมื่อมีแพ็กเก็ตตอบกลับก็จะเป็นแพ็กเก็ตที่มายัง ๒๐๐.๒.๒.๕ Port ๔๐๐๑ Firewall ก็จะเปิดตาราง NAT ในหน่วยความจำ ทำให้ทราบว่า TCP Session นี้เป็นของเครื่อง ๑๙๒.๑๖๘.๑.๒ จากนั้น Firewall ก็จะทำการแปลงค่า Destination IP และ Destination Port ให้เป็น ๑๙๒.๑๖๘.๑.๒ และ ๑๐๒๔ ตามลำดับ ในทำนองเดียวกันเครื่อง ๑๙๒.๑๖.๑.๙ และ ๑๙๒.๑๖๘.๑.๔ ก็ต้องการติดต่อกับอินเตอร์เน็ตเช่นกัน Firewall จะใช้กลไกเดียวกันนี้ในการจดจำว่า Session ใดเป็นของไอพีแอดเดรสก็ติดต่อกับเซิร์ฟเวอร์บนอินเตอร์เน็ตหลายแห่งหมายเลข Source Port ของ Firewall จะถูกใช้ได้สูงสุดประมาณไม่เกิน Port ๖๕๕๓๕ ดังนั้นหาก Session ใดไม่มีการใช้งานแล้วก็จะถูกลบออกจากตาราง NAT ที่อยู่ในหน่วยความจำ เพื่อที่หมายเลข Port เดิม (บน Firewall) จะได้ถูกนำมาใช้ใหม่ในลักษณะที่เป็นพลวัตร จึงเป็นที่มาขอคำว่า “Dynamic NAT”

๒.๔.๒ Proxy

Proxy เป็นชื่อเรียกอุปกรณ์ที่ทำงานเป็น Web Cache อย่างไรก็ตามหาก Network ของเราออกแบบให้มีการใช้งาน Proxy ก็จำเป็นอย่างยิ่งที่จะต้องมีความเกี่ยวข้องกับการกำหนดกฎบน Firewall ในทางปฏิบัติเราสามารถใช้คอมพิวเตอร์ ที่ติดตั้งโปรแกรม ISA (Microsoft Internet Security and Acceleration Server) เพื่อทำงานเป็น Proxy

Proxy (หรือ Web Cache) คืออุปกรณ์หรือเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นตัวกลางระหว่างเครื่องไคลเอนต์ และเว็บเซิร์ฟเวอร์ในการร้องขอและจัดส่งหน้าเว็บเพจ ตัวอย่างเช่น เมื่อ user ๑ (ซึ่งอยู่บนNetworkที่ใช้ Proxy) ต้องการเข้าชมเว็บไซต์ www.sanook.com คำร้องขอหน้าเว็บเพจจะถูกส่งไปยัง Proxy จากนั้น Proxy จะร้องขอหน้าเว็บเพจของ www.sanook.com ให้ user๑ แทน เมื่อ www.sanook.com ส่งหน้าเว็บเพจกลับมา Proxy จะเก็บหน้าเว็บเพจดังกล่าวไปบน cache พร้อมทั้งส่งหน้าเว็บเพจดังกล่าวมาให้ user๑ จากนั้นหากมีผู้ใช้คนอื่น เช่น user๒ ต้องการหน้าเว็บเพจของ www.sanook.com ก็จะส่งคำร้องขอไปยัง www.sanook.com แต่เนื่องจากเป็นNetworkที่กำหนดให้มีการใช้ proxy ดังนั้นคำร้องขอนี้จะถูกส่งไปยังที่ Proxy แทน เมื่อ Proxy ได้รับการร้องขอดังกล่าว ก็จะมองหาว่าสิ่งที่ผู้ใช้ต้องการมีอยู่ใน cache หรือไม่ หากมีอยู่ก็จะส่งข้อมูลที่อยู่ใน cache ไปให้ แต่ถ้าไม่มีก็จะส่งคำร้องขอไปยังเว็บเซิร์ฟเวอร์

ประโยชน์ของ Proxy มี ๒ คุณลักษณะ คือ

๒.๑.๒.๑ เพื่อความเร็วในการดาวน์โหลดหน้าเว็บเพจ เนื่องจากหากหน้าเว็บเพจ รูปภาพหรือไฟล์ที่ร้องขอมีอยู่ใน cache ของ Proxy อยู่แล้วก็ไม่จำเป็นต้องดาวน์โหลดจากใหม่จากอินเตอร์เน็ต ความเร็วในการส่งหน้าเว็บเพจก็จะเร็วเท่ากับความเร็วของระบบ LAN เพราะ Proxy มักจะได้รับการติดตั้งไว้บน LAN เดียวกันกับผู้ใช้

๒.๑.๒.๒ เพื่อประหยัดแบนด์วิดธ์ เพราะหากมีผู้ใช้หลาย ๆ คนดาวน์โหลดหน้าเว็บเพจ รูปภาพ หรือไฟล์เดียวกันโดยไม่มีการใช้ Proxy จะทำให้ต้องใช้แบนด์วิดธ์ในการดาวน์โหลดค่อนข้างมาก ซึ่งแปรผันตามจำนวนผู้ใช้ แต่ถ้าหากเราใช้ Proxy แล้วหน้าเว็บเพจรูป หรือไฟล์จะถูกดาวน์โหลดจาเพียงครั้งเดียวแล้วถูกเก็บไว้ที่ cache ของ Proxy ผู้ใช้ที่ร้องขอไปทีหลังก็จะได้รับข้อมูลจาก cache ของ Proxy แทน ทำให้ประหยัดแบนด์วิดธ์เพราะไม่ต้องร้องขอและดาวน์โหลดข้อมูลใหม่

Proxy มักจะใช้ Port หมายเลข ๘๐๘๐ หรือหมายเลข ๓๑๒๘ ดังนั้น การคอนฟิกเน็คเวิร์กเกี่ยวกับ Proxy แบ่งเป็น ๒ กลุ่มใหญ่ ๆ ได้แก่ การระบุค่า Proxy โดยตรงที่บราวเซอร์ และการทำ Auto Redirect (หรือเรียกว่า transparent proxy)

๒.๔.๓ รูปแบบการใช้งานระบบ Internet ที่ออกแบบ

จากการวิเคราะห์ข้อมูลระบบ Internet ที่เหมาะสมในการนำมาใช้กับกรมพัฒนาที่ดิน ซึ่งมีเครื่องแม่ข่ายที่ให้บริการด้าน web service และเครื่องลูกข่ายที่ขอรับบริการใช้งาน Internet จำนวนมาก จึงได้ออกแบบระบบฯที่มารองรับการใช้งานเป็นแบบ Static NAT โดยให้มีการทำงานผ่านทาง Public IP ที่กำหนดสำหรับการใช้งาน Internet ของลูกข่าย และทำการ NAT ชนิดหนึ่งต่อหนึ่ง สำหรับเครื่องแม่ข่ายบริการเพื่อรองรับการเรียกใช้งานจากภายนอก จากนั้นจะทำการติดตั้งเครื่องแม่ข่ายที่ให้บริการด้าน Proxy และให้เครื่องลูกข่ายทุกเครื่องต้องใช้งาน Internet ผ่านทาง Proxy เพื่อประหยัดแบนวิทช์เครือข่าย และสามารถกำหนด Policy ของการใช้งาน Internet ได้

๒.๕ การวิเคราะห์และออกแบบการเข้าถึง (Access Control Analysis and Design)

เป็นการวิเคราะห์และออกแบบมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบสารสนเทศและคอมพิวเตอร์ที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลขององค์กร โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ ที่มีความจำเป็นต้องเข้าออกห้องศูนย์คอมพิวเตอร์

๒.๕.๑ การวิเคราะห์และออกแบบการเข้าออกห้องควบคุมระบบ Network (ห้อง Server)

กำหนดให้มีแนวปฏิบัติดังนี้

๒.๕.๑.๑ ผู้ดูแลระบบ จัดระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นสัดส่วนชัดเจน เช่น ส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย (Server Zone) เป็นต้น

๒.๕.๑.๒ ผู้ดูแลระบบ ต้องทำการกำหนดสิทธิ์บุคคลในการเข้า-ออกห้อง Server โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการติดประกาศ *"ระเบียบการเข้าออกห้อง Server"* พร้อมระบุรายชื่อเจ้าหน้าที่ที่ได้รับการกำหนดสิทธิ์ไว้อย่างชัดเจน

๒.๕.๑.๓ กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้อง มีความจำเป็นต้องเข้า-ออกห้อง Server ต้องแจ้งที่กลุ่มระบบเครือข่ายและคอมพิวเตอร์ และกรอกแบบฟอร์มขอเข้าใช้งานเครื่องแม่ข่าย ณ ห้องควบคุมระบบ (ห้อง Server) ก่อน โดยมีมาตรการการควบคุมอย่างรัดกุม เจ้าหน้าที่กลุ่มระบบเครือข่ายและคอมพิวเตอร์ ควบคุมการปฏิบัติงานระหว่างอยู่ในห้องควบคุมระบบ

๒.๕.๒ การวิเคราะห์และออกแบบการเข้าถึงระบบเทคโนโลยีสารสนเทศ

กำหนดให้มีแนวปฏิบัติดังนี้

๒.๕.๒.๑ ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ให้แก่ผู้ใช้

๒.๕.๒.๒ เจ้าของข้อมูล และ เจ้าของระบบ จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งาน ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๒.๕.๒.๓ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๕.๓ การวิเคราะห์และออกแบบการเข้าถึงข้อมูลของผู้ใช้

กำหนดให้มีแนวปฏิบัติดังนี้

๒.๕.๓.๑ การลงทะเบียนเจ้าหน้าที่ใหม่ กำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อเปลี่ยนตำแหน่งงานภายในองค์กร ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน เป็นต้น

๒.๕.๓.๒ การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ กำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ การกำหนดชื่อผู้ใช้ต้องเป็นหนึ่งเดียวคือไม่ซ้ำกัน

๒.๕.๓.๓ กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๒.๕.๓.๔ ผู้ใช้ต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

๒.๕.๓.๕ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงการทำลายข้อมูลแต่ละประเภทชั้นความลับ ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณต้องทำการเข้ารหัส (Encryption) ทีเป็นมาตรฐานสากล กำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๒.๕.๔ แนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอก

กำหนดให้มีแนวปฏิบัติดังนี้

๒.๕.๔.๑ มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้าองค์กรนั้นต้องมีการดูแลและการจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

๒.๕.๔.๒ การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น ไม่เปิดพอร์ตและโมเด็มที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๒.๕.๔.๓ การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการ ตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

๒.๖ การวิเคราะห์และออกแบบการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail Analysis and Design)

จดหมายอิเล็กทรอนิกส์ (E-Mail) คือ การส่งข้อความหรือข่าวสารจากบุคคลหนึ่งไปยังบุคคล อื่น ๆ ผ่านทางคอมพิวเตอร์และระบบเครือข่ายเหมือนกับการส่งจดหมาย แต่อยู่ในรูปแบบของสัญญาณข้อมูลที่เป็นอิเล็กทรอนิกส์ โดยเปลี่ยนการนำส่งจดหมายจากบุรุษไปรษณีย์มาเป็นโปรแกรม และเปลี่ยนจากการใช้เส้นทางจราจรคมนาคมทั่วไป มาเป็นช่องสัญญาณรูปแบบต่างๆ ที่เชื่อมต่อระหว่างเครือข่ายคอมพิวเตอร์ ซึ่งจะตรงเข้ามาสู่ Mail Box ที่ถูกจัดสรรใน Server ของผู้รับปลายทางทันที

๒.๖.๑ โปรโตคอลที่ใช้ในการสื่อสารข้อมูลด้านอีเมล์ในระบบเครือข่ายอินเทอร์เน็ต ประกอบด้วย

๒.๖.๑.๑ SMTP (Simple Message Transfer Protocol) ทำหน้าที่ส่งอีเมล์จากเซิร์ฟเวอร์ของผู้ส่งไปยังเมล์เซิร์ฟเวอร์ของผู้รับ

๒.๖.๑.๒ POP (Post Office Protocol) กระบวนการส่งเมล์จะสิ้นสุดเมื่อผู้ส่งสั่งให้เมล์ไคลเอนท์ส่งข้อมูลไปถึงเมล์เซิร์ฟเวอร์ของผู้รับและอีเมล์นั้นจะถูกจัดเก็บไว้ในเมล์บ็อกซ์ของผู้รับที่เครื่องเมล์เซิร์ฟเวอร์

๒.๖.๑.๓ IMAP (Internet Message Access Protocol) คือ โปรโตคอลที่ใช้ในการจัดการเมล์บ็อกซ์ ในการใช้งาน E-Mail จำเป็นจะต้องมี E-Mail Address ซึ่งเปรียบเหมือนที่อยู่ทางอินเตอร์เน็ตของแต่ละคน จะแทนด้วยชื่อหรือรหัสที่ใช้แทนตัว แล้วตามด้วยชื่อของ Mail Server ที่ให้บริการ เช่น cit_๕@ldd.go.th โดยทั่วไป E-Mail Address จะประกอบด้วย User ID ใช้เป็นชื่อหรือ

รหัสประจำตัวของผู้ใช้บริการแต่ละคน เครื่องหมาย @ และDomain Name ของ Mail Server ที่ใช้บริการ

๒.๖.๒ ประเภทของจดหมายอิเลคทรอนิกส์ที่ทำให้ระบบฯเกิดปัญหา

๒.๖.๒.๑ Spam mail คือ จดหมายอิเลคทรอนิกส์ที่ผู้ส่งส่วนใหญ่มีความประสงค์ที่จะโฆษณาสินค้าหรือบริการที่ตัวเองมี

๒.๖.๒.๒ Chain mail คือ เป็นจดหมายอิเลคทรอนิกส์ที่มีข้อความเหมือนจดหมายลูกโซ่ที่เราเคยได้รับโดยทั่วไป เนื้อหาก็จะเป็นเรื่องคำเตือนเกี่ยวกับไวรัส หรือเรื่องอื่น ๆ แต่ที่สำคัญคือ บอกว่าให้ส่งข้อความนี้ให้กับคนที่รู้จัก

๒.๖.๒.๓ Bomb mail คือ การก่อกวนผู้รับจดหมายอิเลคทรอนิกส์ หรือระบบจดหมายอิเลคทรอนิกส์ของเครือข่าย โดยส่งจดหมายอิเลคทรอนิกส์เป็นจำนวนมาก ๆ ไปยังผู้รับจดหมายอิเลคทรอนิกส์หรือระบบจดหมายอิเลคทรอนิกส์

๒.๖.๒.๔ Mail Virus เป็นจดหมายอิเลคทรอนิกส์ที่มี Attached File เป็นไวรัสที่ติดมากับจดหมายอิเลคทรอนิกส์ด้วย ซึ่งไวรัสนี้สามารถ Execute ได้เมื่อผู้อ่านคลิกเพื่อเปิดไฟล์นั้น

๒.๖.๒.๕ Hoax mail เป็นรูปแบบหนึ่งของการก่อกวนที่มีผลต่อผู้ใช้คอมพิวเตอร์จำนวนมาก โดยไวรัสหลอกลวงพวกนี้จะมาในรูปของจดหมายอิเล็กทรอนิกส์ การส่งข้อความต่อ ๆ กันไปผ่านทางโปรแกรมรับส่งข้อความ หรือห้องสนทนาต่าง ๆ ซึ่งสามารถสร้างความวุ่นวายให้เกิดขึ้นได้มากหรือ น้อยเพียงใด ก็ขึ้นกับเทคนิค และการใช้จิตวิทยาของผู้สร้างข่าวขึ้นมา

๒.๖.๓ Mail Spam / Bomb คืออะไร

Spam mail คือ อีเมล์ที่เราไม่ต้องการ เป็นประเภทหนึ่งของ Junk mail จุดประสงค์ของ Spam mail นั้น ผู้ส่งส่วนใหญ่ต้องการโฆษณาบริการต่าง ๆ ที่ตัวเองมี ส่วนจุดประสงค์หลักของ Bomb mail คือ การก่อกวนผู้รับหรือระบบเมล์ของเครื่องข่ายนั้น โดยทั่วไป Spam Mail เป็นการส่งอีเมล์แต่ละฉบับไปหาคนจำนวนมาก ส่วน Bomb mail เป็นการเมล์จำนวนมากไปหาคน ๆ หนึ่งหรือระบบเมล์ใดระบบเมล์หนึ่ง

๒.๖.๔ วิธีการป้องกัน Spam

การส่งอีเมล์เป็นการสื่อสารที่เสียค่าใช่จ่ายน้อยและสามารถเข้าถึงกลุ่มผู้บริโภคได้จำนวนมาก ผู้ที่สร้าง SPAM ก็คือพวกที่ต้องการเข้าถึงกลุ่มผู้บริโภคให้ได้มากที่สุดเพื่อจุดประสงค์ในการโฆษณาขายสินค้า , ประชาสัมพันธ์ ทางธุรกิจของตน จึงใช้วิธีการให้ได้มาซึ่งอีเมล์แอดเดรสของกลุ่มผู้บริโภคที่เป็นกลุ่มเป้าหมาย ซึ่งอาจเป็นได้จากหลายกรณี เช่น การที่เราส่งต่ออีเมล์ต่าง ๆ การใช้อีเมล์แอดเดรสในการสมัครสมาชิกของกลุ่มข่าว (newsgroup) หรือสมัครสมาชิกของเว็บไซต์ต่าง ๆ เป็นต้น

SPAM เกิดจากการที่ผู้สร้าง SPAM รู้จักอีเมล์แอดเดรสของเรา ดังนั้นการป้องกันที่ต้นเหตุที่ดีที่สุด คือการป้องกันไม่ให้คนอื่นที่ไม่จำเป็นหรือไม่เกี่ยวข้องในติดต่อรู้จักอีเมล์แอดเดรสของเรา แต่ถ้าหากเราไม่สามารถป้องกันที่ต้นเหตุได้ตั้งแต่แรก และเคยได้รับ SPAM อีเมล์มาแล้ว เราก็ต้องหันมาป้องกันที่ปลายเหตุ โดยใช้ความสามารถของอีเมล์ไคลเอ็นท์ เช่น Microsoft Outlook ในการกรอง SPAM อีเมล์หรือ/และร่วมกับความสามารถของอีเมล์เซิร์ฟเวอร์ เช่น Microsoft Exchange หรือ ซอฟต์แวร์ Anti-spam เพิ่มเติมตามความเหมาะสม โดยออกแบบการป้องกัน SPAM ดังนี้ ใช้ Outlook ในการกรองอีเมล์

SPAM หลีกเลี่ยงการตอบอีเมล์ SPAM และไม่ควรส่งต่ออีเมล์ประเภท Chain e-mail หรือ Forward mail

๒.๖.๕ การออกแบบการใช้งานจดหมายอิเล็กทรอนิกส์

จากการวิเคราะห์ ได้ออกแบบให้ระบบฯ ใช้งานผ่านทาง Anti-virus Gateway คือ ระบบการป้องกันและกำจัดไวรัสคอมพิวเตอร์ ณ ต้นทางเข้าของอีเมล์ เป็นระบบกำจัดไวรัสแบบรวมศูนย์ นั่นคือเป็นระบบที่กำจัดไวรัสก่อนที่จะเข้าถึง อีเมล์ Box หรือ อีเมล์ Server ของท่าน ซึ่งระบบ Anti-virus Gateway นี้ อาจจะรวมไปถึงการป้องกันและตรวจสอบจดหมายขยะ (SPAM) ด้วยระบบการทำงานของ Anti-virus Gateway นี้จะทำการตรวจสอบไวรัสจากอีเมล์ทุกฉบับทั้งส่งเข้าและส่งออกไป เพื่อตรวจจับและฆ่าไวรัสที่มีปนมากับอีเมล์ต่าง ๆ รวมถึงที่ปนมากับไฟล์ที่แนบไปด้วย หากอีเมล์ฉบับใดติดไวรัส ก็จะมีการแจ้งเตือนไปยังผู้ส่ง รวมถึงจะมีรายงานให้กับผู้ดูแลระบบเป็นรายวัน รายสัปดาห์ และ รายเดือนอีกด้วย ซึ่งจะทำให้บริการนี้เป็นบริการที่อำนวยความสะดวกและความปลอดภัยให้หน่อยงานต่างๆ ที่ใช้อีเมล์ในการติดต่อสื่อสารข้อมูลได้ทำงานอย่างปลอดภัย

บทที่ ๓
ขั้นตอนการติดตั้งและบริหารจัดการระบบ

ศูนย์สารสนเทศ กรมพัฒนาที่ดิน ได้มีการจัดแบ่งหมวดหมู่การดำเนินงานด้านระบบสารสนเทศและคอมพิวเตอร์ ออกตามลักษณะของงานและอุปกรณ์ที่เกี่ยวข้อง เป็น ๒ ส่วน คือ

๓.๑ การติดตั้งและบริหารงานระบบด้านเครือข่าย (Installation and Operation of the Network) ประกอบด้วย

๓.๑.๑ งานด้านการบริหารจัดการเครือข่าย โดยใช้ระบบแลนเสมือน (Virtual LAN)

๓.๑.๒ งานด้านการควบคุมเครือข่าย โดยใช้ระบบรายการควบคุมการเข้าถึงแอสเซ็ทคอนโทรลิส (Access List Control)

๓.๑.๓ งานด้านการรักษาความปลอดภัยเครือข่าย โดยใช้ระบบอุปกรณ์ด่านกันบุกรุก (Hardware Firewall)

๓.๒ การติดตั้งและบริหารงานระบบด้านคอมพิวเตอร์ (Installation and Operation of the Computer) ประกอบด้วยรูปแบบเสมือน **(**Virtual)

๓.๒.๑ งานด้านการรักษาความปลอดภัยคอมพิวเตอร์ โดยใช้ระบบส่วนชุดคำสั่งด่านกันบุกรุก (Software Firewall)

๓.๒.๒ งานด้านการรักษาความปลอดภัยคอมพิวเตอร์ โดยใช้ชุดคำสั่งป้องกันไวรัสในทางคอมพิวเตอร์ (Software Antivirus)

๓.๒.๓ งานด้านการบริหารจัดการคอมพิวเตอร์ โดยใช้ระบบเครื่องแม่ข่ายเสมือน (Virtual Machine (VM))

๓.๒.๔ งานด้านการบริการโดยใช้ระบบบริหารจัดการการตัดสินใจเชิงพื้นที่ (Executive Information System: EIS ด้านการพัฒนาที่ดิน)

รายละเอียดขั้นตอนและวิธีการปฏิบัติงานของระบบทั้ง ๒ ส่วนนั้น ต้องทำงานที่เกี่ยวข้องและสัมพันธ์กัน ไม่ได้มีการแบ่งแยกเป็นส่วนใดส่วนหนึ่งอย่างสิ้นเชิง เนื่องจากทุกระบบถือเป็นองค์ประกอบที่ทำให้ระบบสารสนเทศและคอมพิวเตอร์ กรมพัฒนาที่ดิน ทำงานได้อย่างมีประสิทธิภาพและมีเสถียรภาพ

๓.๓ แผนภาพการบริหารระบบสารสนเทศและคอมพิวเตอร์ กรมพัฒนาที่ดิน

๓.๑ การติดตั้งและบริหารระบบด้านเครือข่าย (Installation and Operation of the Network)

๓.๑.๑ งานด้านการบริหารจัดการเครือข่าย โดยใช้ระบบแลนเสมือน (Virtual LAN)

๓.๑.๑.๑ การติดตั้งระบบ Vlan

VLAN คือ การแบ่งกลุ่มของสวิตช์ภายในเลเยอร์ ๒ ที่ไม่ขึ้นกับ ลักษณะทางกายภาพ ใดๆกล่าวแบบง่าย ๆ ก็คือ เราไม่จำเป็นที่จะต้องนำสวิตช์มาต่อกันเป็นทอดๆ เพื่อจัดกลุ่มของสวิตช์ว่าสวิตช์กลุ่มนี้คือ กลุ่มเดียวกัน แต่เราสามารถที่จะจัดกลุ่มให้ สวิตช์ที่อยู่ห่างไกลกันออกไปนั้น เป็นสมาชิกของสวิตช์อีกกลุ่มหนึ่งทางแนวตรรกะ (Logical Design) ได้ในกระบวนการทำงานของสวิตช์ เลเยอร์ ๒

นั้น ถึงแม้ว่าตัวสวิตซ์เองจะสามารถลดปริมานของ โดเมนปะทะ (Collision Domain) ไปได้ ให้เหลือเพียง ๑ Collision Domain ต่อ ๑ พอร์ทของสวิตซ์ แล้วก็ตาม แต่ทว่า ทุกพอร์ทของสวิตซ์นั้น ก็ยังคงมี บรอดคาสท์โดเมน (Broadcast Domain) อยู่ดี ซึ่งหากว่าเรานำสวิตซ์มาต่อกันหลาย ๆ จุด และมีการใช้งานบรอดคาสท์โดเมนขึ้นมา นั่นหมายถึงว่า ก็ยังคงที่จะมีทราฟฟิก (Traffic) ที่เป็นส่วนเกินออกมาอยู่ดี ซึ่งทราฟฟิกจำพวกนี้จะเป็นตัวที่ทำให้ระบบเน็ตเวิร์กเกิดความล่าช้า และสิ้นเปลือง CPU ในการประมวลผลของอุปกรณ์ดีไวซ์ต่าง ๆ โดยไม่จำเป็น ซึ่งการทำ VLAN นี้ จะมาช่วยแก้ปัญหาตรงจุดนี้ได้ เนื่องจากในการทำ VLAN นี้ จะเป็นการจำกัดวงของบรอดคาสท์โดเมนให้อยู่ภายในพอร์ท หรือ ดีไวซ์ที่เรากำหนดเท่านั้น ซึ่งทราฟฟิกจะไม่ถูกส่งผ่านไปยังบรอดคาสท์โดเมนอื่น ๆ หากไม่มีการคอนฟิกหรือปรับแต่งเพิ่มเติม และในทางการรักษาความปลอดภัยในระบบเครือข่ายนั้น ทุกพอร์ทของสวิตซ์นั้น ถือว่าเป็นบรอดคาส์ทโดเมนเดียวกัน ซึ่งทราฟฟิกที่วิ่งออกมาจากพอร์ทของสวิตซ์ทุกพอร์ทนั้น สามารถที่จะมองเห็นเฟรมข้อมูลนั้นได้ หากว่ามีใครสักคนหนึ่งทำตัวเป็น สนิฟเฟอร์โหมด (Sniffer Mode) เพื่อดักจับข้อมูลไปได้ แต่หากเมื่อมีการทำ VLAN แล้ว เราสามารถที่จะควบคุมทราฟฟิกให้อยู่ในเฉพาะขอบเขตที่เราต้องการได้ เช่น ต้องการให้ สวิตซ์พอร์ทที่ ๑-๕ ของสวิตซ์ ๑ ซึ่งอยู่ชั้นที่ ๑ เป็นสมาชิกเดียวกันกับ สวิตซ์พอร์ทที่ ๖-๘ ของสวิตซ์ ๓ ที่อยู่ชั้นที่ ๓ ก็เป็นได้ โดยที่ ทราฟฟิกจะไม่ถูกส่งออกไปยังพอร์ทอื่น ๆ ของสวิตซ์ตัวมันเองและสวิตซ์ตัวอื่นอีก ซึ่งเป็นมาตรการในการรักษาความปลอดภัยเบื้องต้นของระบบเน็ตเวิร์ก

ในการติดตั้งระบบ Vlan นั้น จะต้องเข้าไปกำหนดในอุปกรณ์ Switch แบบ Managed ซึ่งกรมพัฒนาที่ดินมีการใช้งาน Cisco Switch เป็นอุปกรณ์หลักในการควบคุมเครือข่ายของกรมฯ โดยในขั้นแรกจะต้องรวบรวมข้อมูลของหน่วยงานทั้งหมด ว่ามีจำนวนทั้งสิ้นกี่หน่วยงาน เพื่อมาจัดทำแผนงานการสร้าง Vlan ให้ครบตามจำนวนหน่วยงาน จากนั้นจึงเข้าไปกำหนดค่า Configuration ในอุปกรณ์ Switch ตามชุดคำสั่ง ดังต่อไปนี้

```
C๖๕๐๖-๒๕๕๗#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
C๖๕๐๖-๒๕๕๗(config)#vlan ๔๐๐
C๖๕๐๖-๒๕๕๗(config-vlan)#name Test
C๖๕๐๖-๒๕๕๗(config-vlan)#
% Applying VLAN changes may take few minutes.  Please wait...
C๖๕๐๖-๒๕๕๗#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
C๖๕๐๖-๒๕๕๗(config)#interface vlan ๔๐๐
C๖๕๐๖-๒๕๕๗(config-if)#ip address ๑๐.๑.๔๐.๒๕๔ ๒๕๕.๒๕๕.๒๕๕.๐
C๖๕๐๖-๒๕๕๗(config-if)#description ## Vlan for Testing ##
C๖๕๐๖-๒๕๕๗(config-if)#
C๖๕๐๖-๒๕๕๗#show interfaces vlan ๔๐๐
Vlan๔๐๐ is administratively down, line protocol is down
  Hardware is EtherSVI, address is fc๕b.๓๙๑๖.๑๕๐๐ (bia fc๕b.๓๙๑๖.๑๕๐๐)
  Description: ## Vlan for Testing ##
  Internet address is ๑๐.๑.๔๐.๒๕๔/๒๔
  MTU ๑๕๐๐ bytes, BW ๑๐๐๐๐๐๐ Kbit, DLY ๑๐ usec,
```

reliability ๒๕๕/๒๕๕, txload ๑/๒๕๕, rxload ๑/๒๕๕
Encapsulation ARPA, loopback not set
Keepalive not supported
ARP type: ARPA, ARP Timeout ๐๔:๐๐:๐๐
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: ๐/๗๕/๐/๐ (size/max/drops/flushes); Total output drops: ๐
Queueing strategy: fifo
Output queue: ๐/๔๐ (size/max)
๕ minute input rate ๐ bits/sec, ๐ packets/sec
๕ minute output rate ๐ bits/sec, ๐ packets/sec
L๒ Switched: ucast: ๔๔๑ pkt, ๓๓๕๑๖ bytes - mcast: ๐ pkt, ๐ bytes
L๓ in Switched: ucast: ๐ pkt, ๐ bytes - mcast: ๐ pkt, ๐ bytes
L๓ out Switched: ucast: ๐ pkt, ๐ bytes - mcast: ๐ pkt, ๐ bytes
๐ packets input, ๐ bytes, ๐ no buffer
Received ๐ broadcasts (๐ IP multicasts)
๐ runts, ๐ giants, ๐ throttles
๐ input errors, ๐ CRC, ๐ frame, ๐ overrun, ๐ ignored
๐ packets output, ๐ bytes, ๐ underruns
๐ output errors, ๐ interface resets
๐ output buffer failures, ๐ output buffers swapped out

จากชุดคำสั่งเป็นการสร้าง Vlan ๔๐๐ สำหรับใช้ทดสอบการทำงาน ซึ่งในการกำหนด Vlan นั้น จะต้องให้ครบตามจำนวนของหน่วยงาน เนื่องจากจะต้องกำหนด IP Address ของแต่ละหน่วยงานอยู่คนละเครือข่ายกัน เพื่อป้องกันปัญหาจาก broadcasting รบกวน และกรณีที่เครื่องใดเครื่องหนึ่งในเครือข่ายเกิดปัญหาแล้วส่งผลกระทบกับเครือข่ายทั้งหมด

๓.๑.๑.๒ การบริหารจัดการเครือข่าย โดยใช้ระบบแลนเสมือน (Virtual LAN)

ในการบริหารจัดการเครือข่ายนั้น มีความจำเป็นที่จะต้องทำการแบ่งแยกเครือข่ายแต่ละหน่วยงานออกจากกัน เพื่อให้สามารถบริหารจัดการแต่ละเครือข่ายได้อย่างเป็นเอกภาพและไม่เกิดปัญหาการรบกวนการทำงานของระบบเครือข่ายรวม โดยเครื่องมือที่ช่วยในการบริหารจัดการที่เป็นสากลและใช้งานกันอย่างแพร่หลาย คือการแบ่งแยกเครือข่ายผ่านทางระบบวีแอลเอเอ็น (VLAN) หรือแลนเสมือน (Virtual LAN) ซึ่งเป็นฟังก์ชัน (Function) มาตรฐานสำหรับการจัดการอุปกรณ์สวิทช์ในชั้นสื่อสารระดับ ที่ ๒ (Managed Switch Layer ๒) ที่มีการใช้งานอยู่ในปัจจุบัน

วีแอลเอเอ็น (VLAN) คือ การแบ่งกลุ่มเครือข่ายของสวิตช์ภายในเลเยอร์ ๒ ที่ไม่ขึ้นกับลักษณะทางกายภาพใดๆ แต่สามารถจัดกลุ่มให้ทางแนวตรรกะ (Logical Design) ซึ่งการทำวีแอลเอเอ็น (VLAN) นี้ ช่วยแก้ปัญหาการใช้งานบรอดคาสท์โดเมน(Broadcast Domain) เนื่องจากในการทำวีแอลเอเอ็น (VLAN) นี้ เป็นการจำกัดขนาดวงของบรอดคาสท์โดเมนให้อยู่ภายในพอร์ทหรือดีไวซ์ (device) ที่กำหนด ถือเป็นมาตรการในการรักษาความปลอดภัยเบื้องต้นของระบบเครือข่าย

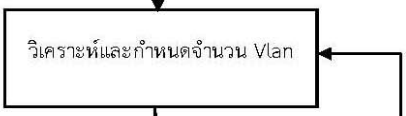
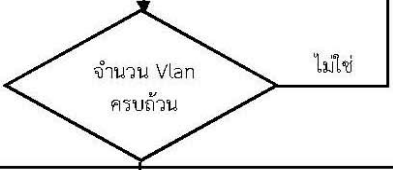
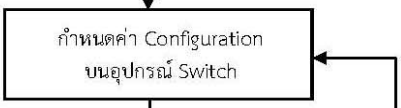
ศูนย์สารสนเทศ กรมพัฒนาที่ดิน ได้แบ่งการทำงานวีแอลเอเอ็น (VLAN) ออกเป็น ๒ ประเภท คือ วีแอลเอเอ็น (VLAN) จำแนกตามหน่วยงาน และวีแอลเอเอ็น (VLAN) จำแนกตามภารกิจเฉพาะด้าน

สำหรับ วีแอลเอเอ็น (VLAN) ที่มีการใช้งานในปัจจุบันมีจำนวน ๓๒ วีแอลเอเอ็น (VLAN) ได้แก่

๑. VLAN ๑ = Native VLAN
๒. VLAN ๒ = DMC Zone
๓. VLAN ๓ = ห้องอบรม
๔. VLAN ๔ = ผู้บริหาร
๕. VLAN ๕ = สำนักงานเลขานุการกรม
๖. VLAN ๖ = กองการเจ้าหน้าที่
๗. VLAN ๗ = กองคลัง
๘. VLAN ๘ = กองแผนงาน
๙. VLAN ๙ = กองสำรวจดินและวิจัยทรัพยากรดิน
๑๐. VLAN ๑๐ = สำนักวิทยาศาสตร์เพื่อการพัฒนาที่ดิน
๑๑. VLAN ๑๑ = สำนักเทคโนโลยีการสำรวจและทำแผนที่
๑๒. VLAN ๑๒ = กองนโยบายและแผนการใช้ที่ดิน
๑๓. VLAN ๑๓ = กองวิจัยและพัฒนาการจัดการที่ดิน
๑๔. VLAN ๑๔ = สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน
๑๕. VLAN ๑๕ = กองเทคโนโลยีชีวภาพทางดิน
๑๖. VLAN ๑๗ = หมอดินอาสา
๑๗. VLAN ๑๘ = หญ้าแฝก
๑๘. VLAN ๑๙ = ตรวจสอบภายใน
๑๙. VLAN ๒๔ = สำนักผู้เชี่ยวชาญ
๒๐. VLAN ๒๕ = อาคารปุ๋ยหมัก
๒๑. VLAN ๒๖ = ห้องประชุม
๒๒. VLAN ๒๘ = IPPhone
๒๓. VLAN ๒๙ = Video Conference
๒๔. VLAN ๓๐ = ศูนย์สารสนเทศ
๒๕. VLAN ๓๓ = กล้อง CCTV
๒๖. VLAN ๕๓ = ระบบ LDD Hot Spot
๒๗. VLAN ๕๔ = ระบบ LDD Hot Spot
๒๘. VLAN ๕๕ = ระบบ LDD Hot Spot
๒๙. VLAN ๗๐ = โครงการ GIN
๓๐. VLAN ๙๑ = NAS
๓๑. VLAN ๓๐๐ = Firewall
๓๒. VLAN ๓๐๑ = Firewall

ในการติดตั้งระบบ วีแอลเอเอ็น (VLAN) ต้องกำหนดค่าคอนฟิกูเรชั่น (Configuration) ให้กับอุปกรณ์สวิทช์(Switch) ยี่ห้อซิสโก้ (Cisco) ทุกเครื่องที่มีการต่อเชื่อม ซึ่งประกอบด้วยอุปกรณ์กระจายสัญญาณแบบหลัก (Core Switch) ยี่ห้อซิสโก้ (Cisco) รุ่น ๖๕๐๖ อุปกรณ์กระจายสัญญาณแบบกระจาย (Distributed Switch) ยี่ห้อซิสโก้ (Cisco) รุ่น ๓๖๕๐ และ อุปกรณ์กระจายสัญญาณแบบเข้าถึง (Access Switch) ยี่ห้อซิสโก้ (Cisco) รุ่น ๒๙๖๐ ขั้นตอนแรกในการเริ่มต้นใช้งานจะต้องใช้วิธีการเขียนระบุคำสั่งบนบรรทัดคำสั่ง (Command Line) ผ่านทางคอนโซล พอร์ต (Console Port) เพื่อกำหนดค่าคอนฟิกกูเรชั่น (Configuration) จากนั้นเมื่อกำหนดค่าการทำงานเบื้องต้นเรียบร้อยแล้ว จึงใช้วิธีการ Remote ผ่านทางเครือข่าย ซึ่งง่ายต่อการควบคุมและตรวจสอบว่าการกำหนดค่าต่าง ๆ ของระบบครบถ้วน

แผนผังแสดงขั้นตอนและวิธีการปฏิบัติงาน ระบบ VLAN

ลำดับที่	ผังกระบวนการ	รายละเอียดงาน
		
๑		๑. วิเคราะห์โครงสร้างหน่วยงานและจำนวนเครือข่ายที่ใช้งานของกรมพัฒนาที่ดินเพื่อกำหนดจำนวน VLAN ที่ใช้งาน
๒		๒. ตรวจสอบจำนวน VLAN ว่าครบถ้วนหรือไม่ ถ้ายังไม่ครบให้กลับไปทำขั้นตอนที่ ๑ ถ้าครบแล้วให้ไปทำขั้นตอนที่ ๓
๓		๓. กำหนดค่า Configuration สำหรับแต่ละ VLAN ลงบนอุปกรณ์ Switch ที่ใช้งาน
๔		๔. ทดสอบการทำงานของแต่ละ VLAN บนอุปกรณ์ Switch ว่าสามารถใช้งานได้หรือไม่ ถ้าไม่สามารถใช้งานให้กลับไปทำขั้นตอนที่ ๓ ถ้าใช้งานได้แล้วให้ไปทำขั้นตอนที่ ๕
๕		๕. กำหนดค่า Configuration การเชื่อมต่อ VLAN บนเครื่องคอมพิวเตอร์
๖		๖. ทดสอบการเชื่อมต่อเข้ามายังเครือข่ายของกรมพัฒนาที่ดินว่าสามารถใช้งานได้หรือไม่ ถ้าไม่สามารถใช้งานให้กลับไปทำขั้นตอนที่ ๕ ถ้าใช้งานได้แล้วให้ไปทำขั้นตอนที่ ๗
๗		๗. บันทึกค่า Configuration ลงบนอุปกรณ์ Switch ที่เชื่อมต่อทั้งหมด
		

ขั้นตอนการติดตั้งและดำเนินการ

๑) เชื่อมสายโรลโอเวอร์ (Rollover) ผ่านคอนโซล พอร์ต (Console Port) ของอุปกรณ์สวิทซ์(Switch) ยี่ห้อซิสโก้ (Cisco) เข้ากับเครื่องคอมพิวเตอร์ควบคุมระบบฯ

๒) ติดต่อกับระบบผ่านทางโปรโตคอลรูปแบบซีเคียวร์ชีล (Secure Shell)

๓) ระบบให้ระบุรหัสผู้ใช้งาน (User) และรหัสผ่าน (Password) ที่ใช้งานให้ใช้ค่าเริ่มต้น อุปกรณ์ยี่ห้อซิสโก้ (Cisco) ที่กำหนดมาจากโรงงาน จากนั้นให้กำหนดค่าหมายเลขอ้างอิงในการติดต่อสื่อสาร (IP Address) สำหรับส่วนต่อประสาน (Interface) ที่เป็นช่องทางการควบคุม (Managed Port) กำหนดค่ารหัสผู้ใช้งาน (User) และเปิดให้สามารถใช้งานรหัสผ่าน (Enable Password) ที่ใช้งาน จากนั้นให้บันทึก (Save) และเริ่มต้นระบบใหม่ (Restart) ระบบฯ เมื่อสามารถเชื่อมต่ออุปกรณ์ผ่านทางเครือข่ายแบบมีสาย (LAN) ได้แล้ว ให้เข้าสู่ระบบ (Log-in) เข้าไปในระบบ เพื่อทำการตั้งค่าคอนฟิกกูเรชั่น (Configuration) ระบบ วีแอลเอเอ็น (VLAN) ต่อไป

๓.๑.๒ งานด้านการควบคุมเครือข่าย โดยใช้ระบบรายการควบคุมการเข้าถึงแอสเซ็ทคอนโทรลิส (Access List Control)

๓.๑.๒.๑ การตั้งค่า Access List Control บนอุปกรณ์เครือข่าย

Access Control List (ACL) คือ การกรอง packet ที่จะเข้าออก Router หรือ Switch Layer ๓ ให้เป็นไปตามเงื่อนไขที่เราต้องการ และมีส่วนช่วยในเรื่องของ IT Security แต่มีข้อเสียคือไปเพิ่ม load cpu ให้กับ Router เพราะหน้าที่หลักของ Router คือการพา packet ไปให้ถูกเส้นทาง หรือการหาเส้นทาง ไม่ใช่ทำหน้าทีกรอง packet และการตั้งค่า ACL ทีผิดพลาด จะส่งผลให้ Network มีปัญหาได้ การกรอง packet ควรจะเป็นหน้าที่ของ Firewall มากกว่า แต่สำหรับ Network ที่ไม่ใหญ่มาก การทำACL บน Router นั้นเป็นทางเลือกหนึ่งที่สามารถทำได้

การ Configuration ACL บน Router หรือ Switch Layer ๓ นั้น ทำได้ ๒ วิธีการ คือวิธีการแบบตัวเลข และวิธีการแบบชื่อ (Name ACL) โดยมีรูปแบบการกำหนดค่า Configuration ในอุปกรณ์ ตามชุดคำสั่ง ดังต่อไปนี้

```
ip access-list extended vlan๑๑
deny   udp any any eq ๑๙๐๐
deny   tcp any any eq ๑๙๐๐
deny   ip host ๒๓๙.๒๕๕.๒๕๕.๒๕๐ any
deny   ip any host ๒๓๙.๒๕๕.๒๕๕.๒๕๐
deny   ip ๑๙๒.๑๖๘.๐.๐ ๐.๐.๒๕๕.๒๕๕ any
deny   ip any ๑๙๒.๑๖๘.๐.๐ ๐.๐.๒๕๕.๒๕๕
permit ip any host ๒๐๓.๑๔๘.๒๕๐.๑๘๙
permit ip host ๑๐.๑.๑๑.๒๕๒ any
permit ip host ๑๐.๑.๑๑.๒๕๓ any
permit ip host ๑๐.๑.๑๑.๒๕๔ any
deny   tcp any any eq ๑๙๓๕
permit ip host ๑๐.๑.๑๑.๑ ๑๐.๐.๐.๐ ๐.๒๕๕.๒๕๕.๒๕๕
permit tcp host ๑๐.๑.๑๑.๑๐๗ host ๑๐.๑.๑.๑๑๑
```

deny tcp any any eq ๔๔๕
permit tcp any any eq ๕๕๔
permit tcp any any eq ๑๗๕๕
permit tcp any any eq ๑๙๓๕
permit tcp any any eq ๒๖๓๘
permit tcp any any eq ๓๓๘๙
permit tcp any any eq ๕๐๖๐
permit tcp any any eq ๕๐๖๑
permit tcp any any eq ๘๐๐๕
permit tcp any any eq ๘๐๘๐
permit tcp any any eq ๘๐๘๑
permit tcp any any eq ๘๔๔๓
permit tcp any any eq ๘๘๘๘
permit tcp any any eq ๙๐๙๐
permit udp any any eq ๘๐๘๐
permit udp any any eq ๘๘๘๘
permit udp any any eq ๙๙๙๙
deny tcp any any eq ๕๙๓
deny tcp any any eq ๖๖๖๗
deny udp any any eq ๑๓๕
deny udp any any range ๒๐๐๐ ๖๕๕๓๕
deny tcp any any range ๒๐๐๐ ๖๕๕๓๕
permit tcp host ๑๐.๑.๑๑.๑๐ any eq ๑๘๖๓
permit tcp host ๑๐.๑.๑๑.๑๑ any eq ๑๘๖๓
permit tcp host ๑๐.๑.๑๑.๒๘ any eq ๑๘๖๓
permit tcp host ๑๐.๑.๑๑.๔๙ any eq ๑๘๖๓
permit tcp host ๑๐.๑.๑๑.๖๙ any eq ๑๘๖๓
permit tcp host ๑๐.๑.๑๑.๑๓๒ any eq ๑๘๖๓
permit ip ๑๐.๑.๑๑.๐ ๐.๐.๐.๒๕๕ host ๕๘.๑๔๗.๗๙.๑๓๖
permit ip ๑๐.๑.๑๑.๐ ๐.๐.๐.๒๕๕ host ๒๐๓.๑๔๔.๑๙๔.๔๕
permit ip ๑๐.๑.๑๑.๐ ๐.๐.๐.๒๕๕ host ๒๐๒.๑๔๒.๒๐๐.๑๓๑
permit ip ๑๐.๑.๑๑.๐ ๐.๐.๐.๒๕๕ host ๖๑.๑๙.๒๔๙.๑๐๓
permit ip ๑๐.๑.๑๑.๐ ๐.๐.๐.๒๕๕ host ๒๐๓.๑๑๓.๙.๑๐๔
permit ip ๑๐.๑.๑๑.๐ ๐.๐.๐.๒๕๕ host ๒๐๓.๑๑๓.๙.๑๐๕
permit ip ๑๐.๑.๑๑.๐ ๐.๐.๐.๒๕๕ host ๒๐๒.๖๐.๑๙๙.๔๔
permit ip ๑๐.๑.๑๑.๐ ๐.๐.๐.๒๕๕ host ๒๐๓.๑๔๖.๒๕๐.๒๐๐
permit ip host ๑๐.๑.๑๑.๒๒๒ ๑๐.๐.๐.๐ ๐.๒๕๕.๒๕๕.๒๕๕

จากชุดคำสั่งเป็นการสร้าง ip access-list extended vlan ๑๑ สำหรับสำนักวิทยาศาสตร์เพื่อการพัฒนาที่ดิน จากนั้นจะนำชุดคำสั่งของ ACL นี้ไปประกาศกำหนดไว้ใน Vlan ๑๑ เพื่อควบคุมการใช้งานของหน่วยงานให้เป็นไปตามที่กำหนด ทั้งในส่วนของ IP Address ที่อนุญาตให้ใช้งาน และ Protocol ที่อนุญาตให้ใช้งาน ทั้งนี้จะต้องสร้าง ACL ให้กับทุกหน่วยงานเพื่อให้เป็นไปตามมาตรฐานเดียวกัน

๓.๑.๒.๒ การควบคุมเครือข่ายโดยใช้ระบบแอสเซ็ทคอนโทรลิส (AccessList Control(ACL))

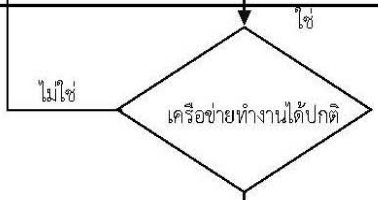
การควบคุมเครือข่ายผ่านทางอุปกรณ์สวิทซ์ในชั้นสื่อสารระดับที่ ๓ (Managed Switch Layer ๓) และอุปกรณ์เร้าเตอร์ (Router) ยี่ห้อซิสโก้ (Cisco) เพื่อให้มีปริมาณข้อมูลผ่านช่องทางของเครือข่ายในช่วงเวลาหนึ่งๆในปริมาณที่เหมาะสม และจำกัดการใช้งานให้เป็นไปตามข้อกำหนด จึงได้มีการนำระบบแอสเซ็ทคอนโทรลิส (Access List Control) ซึ่งเป็นฟังก์ชั่นการทำงานของอุปกรณ์ยี่ห้อซิสโก้ (Cisco) มาใช้ในการควบคุมเครือข่าย ให้สามารถทำงานได้อย่างมีประสิทธิภาพ

การทำงานของแอสเซ็ทคอนโทรลิส (Access List Control) คือ การกรองแพ็กเกต (packet) ที่เข้าออก อุปกรณ์เร้าเตอร์ (Router) หรือ สวิทซ์ในชั้นสื่อสารระดับที่ ๓ ให้เป็นไปตามเงื่อนไขที่กำหนดเพื่อควบคุมการ ใช้งานและช่วยในเรื่องของการรักษาความปลอดภัยเครือข่าย แต่มีข้อเสียคือเพิ่มภาระการหน่วยประมวลกลาง (Load central processing unit) ให้กับ อุปกรณ์เร้าเตอร์ (Router) เพราะหน้าที่หลักของอุปกรณ์เร้าเตอร์ (Router) คือการนำพาแพ็กเกต (packet) ไปให้ถูกเส้นทางหรือการหาเส้นทาง ไม่ใช่ทำหน้าที่กรองแพ็กเกต(packet) และการตั้งค่าแอสเซ็ทคอนโทรลิส (Access List Control) ที่ผิดพลาด อาจส่งผลให้เครือข่ายมีปัญหาได้ แต่การทำ แอสเซ็ทคอนโทรลิส (Access List Control) บนอุปกรณ์เครือข่ายสวิทซ์ในชั้นสื่อสารระดับที่ ๓ นั้น เป็นทางเลือกหนึ่งที่ใช้ในการควบคุมเครือข่ายให้มีการทำงานได้อย่างมีเสถียรภาพเพิ่มขึ้น

ศูนย์สารสนเทศ กรมพัฒนาที่ดิน มีการนำระบบ แอสเซ็ทคอนโทรลิส (Access List Control) มาใช้งานร่วมกับระบบวีแอลเอเอ็น (VLAN) เพื่อควบคุมการ ใช้งานระบบเครือข่ายของกรมพัฒนาที่ดินให้เป็นไปตามข้อกำหนดที่วางไว้ ได้แก่การควบคุมหมายเลขอ้างอิงในการติดต่อสื่อสาร (IP Address) ของแต่ละวีแอลเอเอ็น (VLAN) การควบคุมการใช้งานทีซีพีพอร์ต (TCP Port) และยูดีพีพอร์ต (UCP Port) และการควบคุมการเชื่อมต่อระหว่างแต่ละ วีแอลเอเอ็น (VLAN)

แผนผังแสดงขั้นตอนและวิธีการปฏิบัติงาน

ระบบ Access Control List (ACL)

ลำดับที่	ผังกระบวนการ	รายละเอียดงาน
		
๑		๑. วิเคราะห์ปริมาณข้อมูลที่ผ่านช่องทางของเครือข่าย ค่า IP Address ค่า TCP Port และ UCP Port ของแต่ละ VLAN ที่ใช้งานของกรมพัฒนาที่ดิน เพื่อกำหนด ACL Policy
๒		๒. ตรวจสอบจำนวน ACL Policy ว่าครบถ้วนหรือไม่ ถ้ายังไม่ครบให้กลับไปทำขั้นตอนที่ ๑ ถ้าครบแล้วให้ไปทำขั้นตอนที่ ๓
๓		๓. กำหนดค่า Configuration ACL Policy ลงบนอุปกรณ์เครือข่าย Switch Layer ๓ และ Router ที่ใช้งาน
๔		๔. ทดสอบการทำงานของแต่ละ ACL Policy ที่กำหนดบนอุปกรณ์ ว่าสามารถใช้งานได้หรือไม่ ถ้าไม่สามารถใช้งานให้กลับไปทำขั้นตอนที่ ๓ ถ้าใช้งานได้แล้วให้ไปทำขั้นตอนที่ ๕
๕		๕. ทดสอบการทำงานของระบบเครือข่ายของกรมพัฒนาที่ดิน เมื่อใช้งานร่วมกับ ACL Policy ว่าสามารถใช้งานได้ปกติหรือไม่ ถ้าไม่สามารถใช้งานให้กลับไปทำขั้นตอนที่ ๓ ถ้าใช้งานได้แล้วให้ไปทำขั้นตอนที่ ๖
๖		๗. บันทึกค่า Configuration ลงบนอุปกรณ์เครือข่ายที่เชื่อมต่อทั้งหมด
		

ขั้นตอนการติดตั้งและดำเนินการ

๑) ติดต่อกับระบบผ่านทางโปรโตคอลซีเคียวร์ชีล (Secure Shell) บนเครื่องคอมพิวเตอร์ควบคุมระบบ

๒) ระบบจะให้ระบุรหัสผู้ใช้งาน (User) และรหัสผ่าน (Password) ที่ใช้งานให้ใช้ค่าที่ได้กำหนดไว้

๓) ทำการตั้งค่าคอนฟิกกูเรชั่น (Configuration) ระบบเอซีแอล (ACL) ตามขั้นตอนต่อไป

๓.๑.๓ งานด้านการรักษาความปลอดภัยเครือข่าย โดยใช้ระบบอุปกรณ์ด่านกันบุกรุก (Hardware Firewall)

การรักษาความปลอดภัยเครือข่ายเป็นสิ่งที่มีความสำคัญเป็นอย่างมาก และต้องปฏิบัติเป็นอันดับแรกในการวางระบบเครือข่าย โดยเครื่องมือมาตรฐานที่นำมาใช้งานคือระบบด่านกันบุกรุก (Firewall) ซึ่งมีทั้งแบบอุปกรณ์ที่เป็นส่วนเครื่อง (Hardware) และชุดคำสั่งที่เป็นส่วนชุดคำสั่ง (Software) โดยที่ความสามารถหลักของด่านกันบุกรุก (Firewall) ทั้ง ๒ แบบ คือ เป็นจุดควบคุมข้อมูลจากเครือข่ายภายนอกหรือเครือข่ายอินเทอร์เน็ต ที่เข้ามาในเครือข่ายภายในขององค์กร และเป็นจุดควบคุมข้อมูลจากเครือข่ายภายในองค์กร ที่ออกไปใช้งานเครือข่ายภายนอกหรือเครือข่ายอินเทอร์เน็ต โดยที่ด่านกันบุกรุก (Firewall) ต้องบังคับให้ข้อมูลเครือข่ายเหล่านี้เป็นไปตามกฎและนโยบายความปลอดภัยที่องค์กรกำหนด

Firewall หมายถึง กำแพงกันไฟ ซึ่งสร้างไว้ป้องกันไฟที่ไหม้จากบริเวณหนึ่งลุกลามไปบริเวณอื่น เพราะฉะนั้นเมื่อนำมาใช้กับระบบเครือข่ายจะมีลักษณะการทำงานที่คล้ายกัน โดยทำหน้าที่ป้องกันอันตรายที่มาจากอินเทอร์เน็ต ซึ่งตำแหน่งการติดตั้งด่านกันบุกรุก (Firewall) จะถูกติดตั้งในจุดที่เครือข่าย ภายในติดต่อกับเครือข่ายภายนอกหรือเครือข่ายอินเทอร์เน็ต

ศูนย์สารสนเทศ กรมพัฒนาที่ดิน ได้นำอุปกรณ์ด่านกันบุกรุก (Hardware Firewall) มาใช้งานร่วมกับระบบชุดคำสั่งด่านกันบุกรุก (Software Firewall) โดยระบบอุปกรณ์ด่านกันบุกรุก (Hardware Firewall) ที่นำมาใช้งานคืออุปกรณ์ยี่ห้อซิสโก้ Cisco รุ่น เอเอสเอ๕๕๔๐ (ASA ๕๕๔๐) ซึ่งเป็นผลิตภัณฑ์ อุปกรณ์ด่านกันบุกรุก (Hardware Firewall) ที่สามารถทำงานตั้งแต่ชั้นสื่อสารระดับที่ ๓ (Layer ๓) ชั้นเครือข่าย (Network) ไปจนถึงชั้นสื่อสารระดับที่ ๗ (Layer ๗) ชั้นโปรแกรมประยุกต์ (Application) เพื่อรักษาความปลอดภัยระบบเครือข่ายของกรมพัฒนาที่ดิน ให้เป็นไปตามข้อกำหนดที่วางไว้ ได้แก่ การควบคุมการเรียกใช้งานเว็บไซต์ (Website) ที่เป็นอันตราย การควบคุมการใช้งานการบริการอินเตอร์เน็ต (Internet Service) การควบคุมการใช้งานเครือข่ายทางสังคม (Social Network) การควบคุมการบรรจุลง (Download) ข้อมูล การควบคุมการบุกรุกจากใช้งานจากเครือข่ายอินเทอร์เน็ต และการควบคุมโปรโตคอล (Protocol) การเชื่อมต่อระหว่างเครือข่ายอินเทอร์เน็ตกับเครือข่ายภายในของกรมพัฒนาที่ดินตามที่มีหน่วยงานร้องขอ

๓.๑.๓.๑ การติดตั้งระบบ Hardware Firewall

การกำหนดค่า Configuration ของระบบฯ ขั้นตอนแรกในการเริ่มต้นใช้งานจำเป็นจะต้องใช้วิธีการเขียนระบุคำสั่งบน Command Lind ผ่านทาง Console Port ของอุปกรณ์ เพื่อกำหนดค่า IP Address และ User Permission ที่ในการใช้เชื่อมต่อกับระบบฯ จากนั้นเมื่อสามารถ

ติดต่อผ่านทางเครือข่าย LAN กับระบบฯได้แล้ว จึงใช้การเชื่อมต่อผ่านเครือข่าย เพื่อ Download และติดตั้ง GUI (Graphic User Interface) Application และกำหนดค่า Configuration ผ่านทางโปรแกรม Cisco ASDM Launcher ซึ่งจะง่ายต่อการควบคุมและตรวจสอบว่า การกำหนดค่าต่าง ๆ เป็นไปตามที่กรมพัฒนาที่ดินได้กำหนดไว้ครบถ้วนหรือไม่ เนื่องจากการทำงานของโปรแกรม จะแสดงค่าการกำหนดต่าง ๆ เป็นรูปภาพพร้อมคำอธิบาย ส่วนในการทำงานเบื้องหลังของโปรแกรมจะแปลงค่าที่กำหนดไว้ทั้งหมด ไปเป็น Source Code บน Command Lind เพื่อควบคุมการทำงานบนระบบอีกครั้งหนึ่ง

ขั้นตอนการติดตั้ง

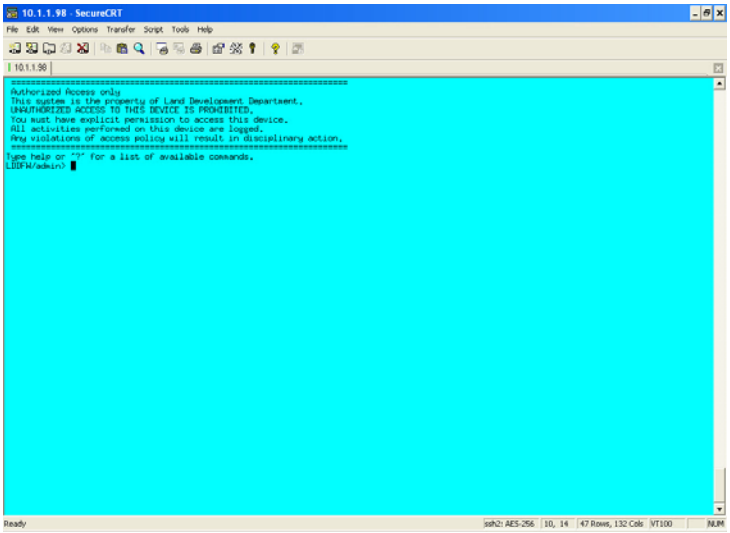
๑) เชื่อมสาย Rollover ผ่าน Console Port ของอุปกรณ์ ASA เข้ากับเครื่องคอมพิวเตอร์ควบคุมระบบฯ

๒) ติดต่อกับระบบผ่านทางโปรแกรม SSH (Secure Shell)

๓) ระบบจะให้ระบุ User Password ที่ใช้งาน ให้ใช้ค่าเริ่มต้น Cisco ที่มาจากโรงงาน

ภาพที่ ๒ การระบุ Username เพื่อเชื่อมต่อระบบ

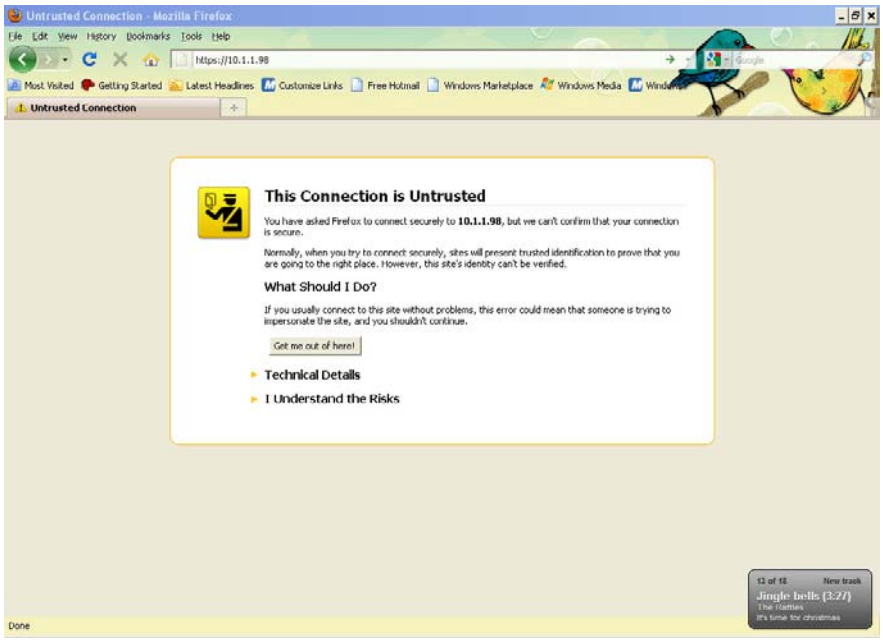
๔) ให้กำหนดค่า IP Address สำหรับ Interface ที่เป็น Managed Port กำหนดค่า User และ Enable Password ที่จะใช้งาน จากนั้นให้ Save และ Restart ระบบฯ



ภาพที่ ๓ การใช้โปรแกรม SSH เชื่อมต่อระบบ

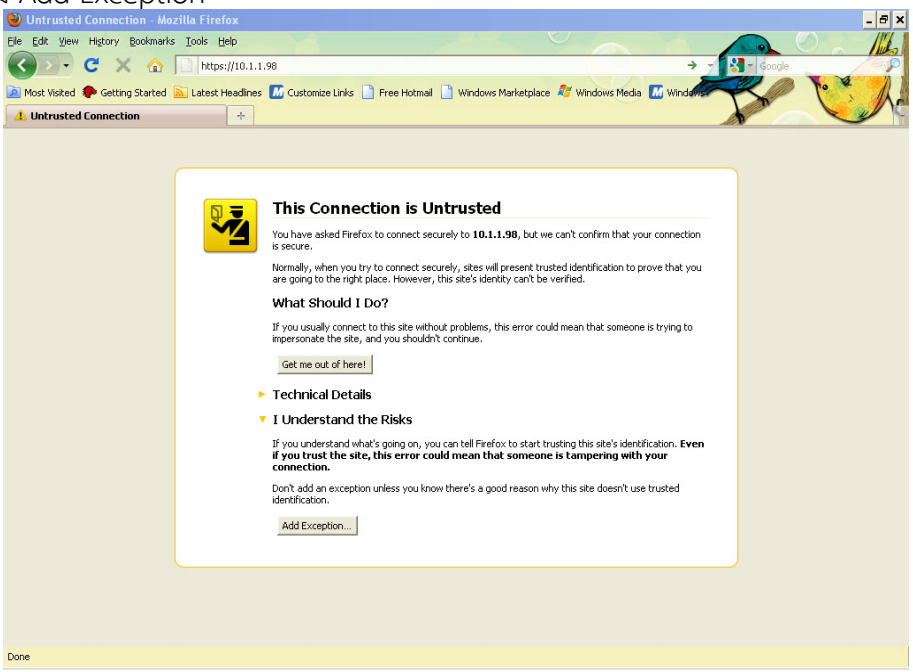
เมื่อสามารถเชื่อมต่อผ่านทางเครือข่าย LAN ได้แล้ว ต่อสาย LAN เข้ากับ Port Managementของอุปกรณ์ ASA จากนั้นให้ Log-In เข้าไปในระบบฯ เพื่อDownload Application ASDM Launcher ที่ใช้ในการควบคุมแบบ GUI (Graphic User Interface) มาติดตั้ง ไว้ที่เครื่องคอมพิวเตอร์ ที่ควบคุมระบบฯ ตามขั้นตอนดังต่อไปนี้

๕) เปิดโปรแกรม Internet Browser และระบุ URL ไปที่ IP Management ของระบบ



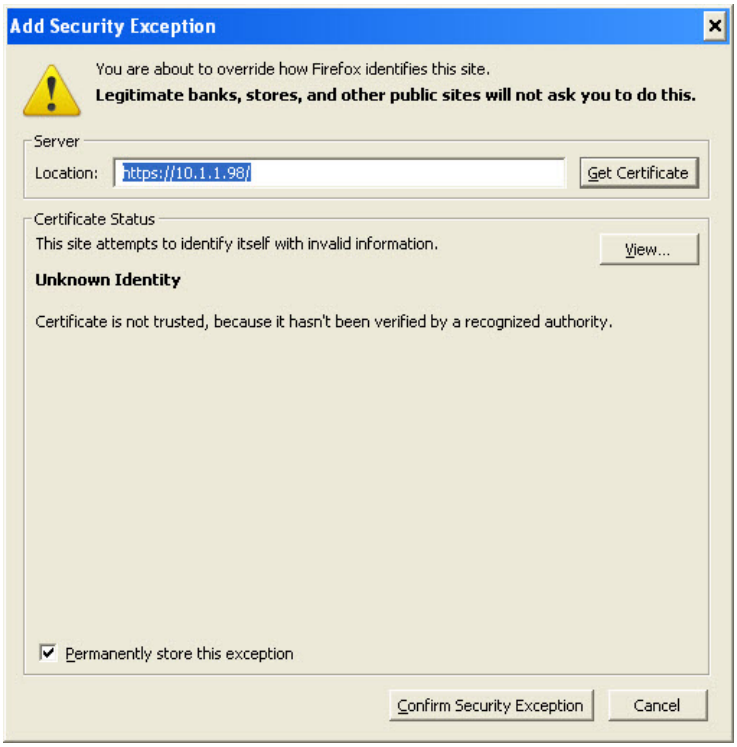
ภาพที่ ๔ การใช้โปรแกรม Internet Browser เชื่อมต่อระบบ

๖) ปรากฏหน้าต่าง Untrusted Connection ให้เลือก I Understand the Risks จากนั้นกดปุ่ม Add Exception



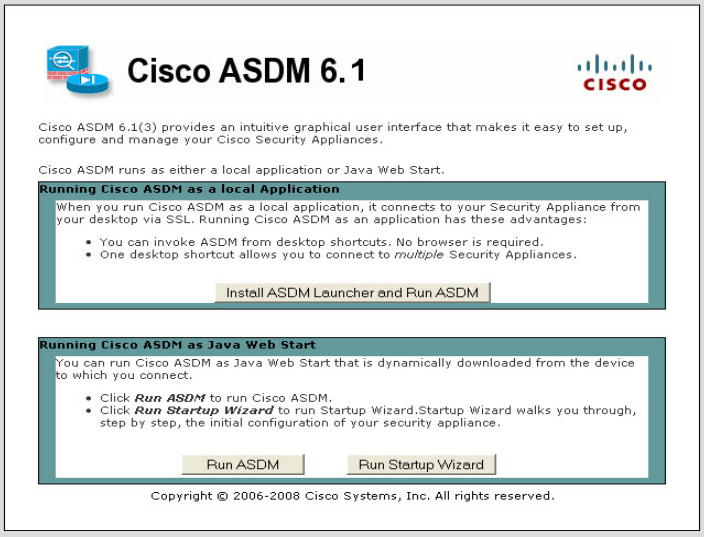
ภาพที่ ๕ การใช้โปรแกรม Internet Browser เชื่อมต่อระบบ

๗) ปรากฏหน้าต่าง Add Security Exception ให้กดปุ่ม Get Certificate จากนั้นกดปุ่ม Confirm Security Exception

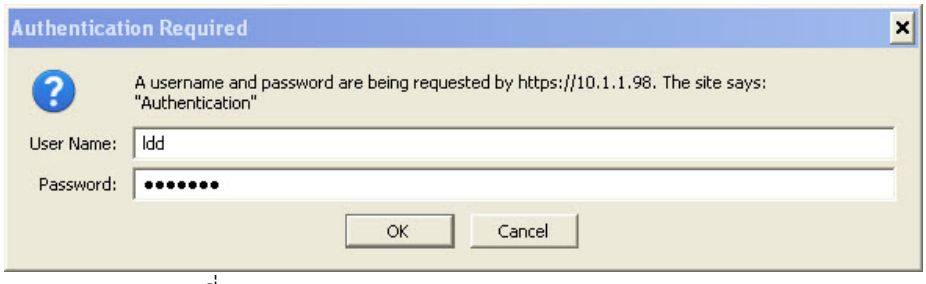


ภาพที่ ๖ การ Confirm Security Exception

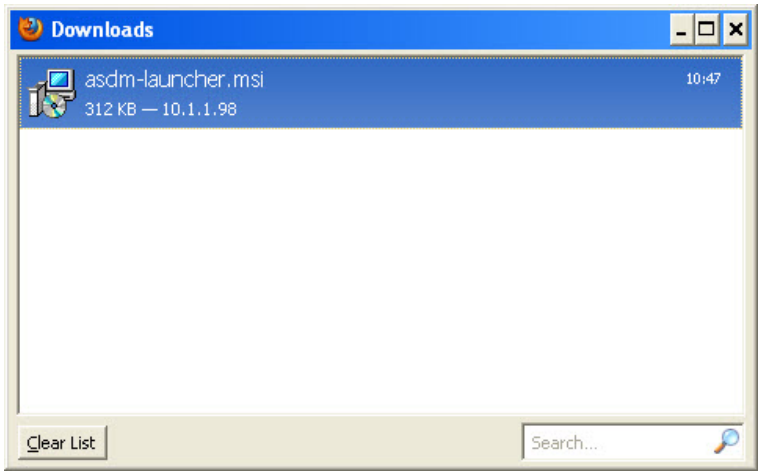
๘) ปรากฏหน้าต่าง Cisco ASDM ๖.๑ ให้กดปุ่ม Install ASDM Launcher and run ASDM จะ ปรากฏหน้าต่าง Authentication Required ให้ระบุ User และPassword ที่สามารถเรียกใช้งานระบบ จากนั้นจะเป็นการ Download File ชื่อ ASDM- Launcher.MSI ซึ่งเป็นไฟล์ที่ใช้ในการติดตั้ง มาเก็บไว้ในเครื่อง ให้คลิ้กที่ไฟล์เพื่อเริ่มต้นการติดตั้ง จนจบขั้นตอนตามภาพด้านล่าง



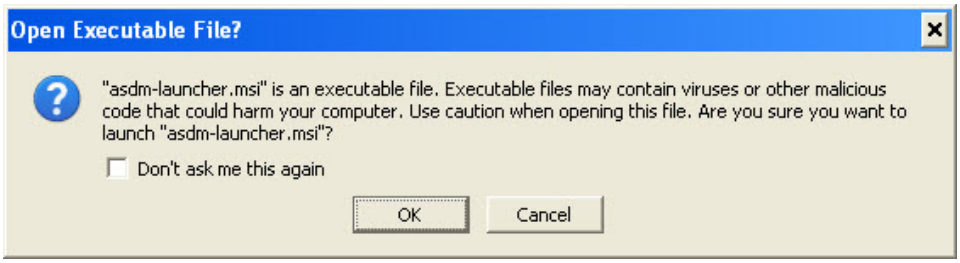
ภาพที่ ๗ การ Install ASDM Launcher



ภาพที่ ๘ การ Authentication ASDM Launcher

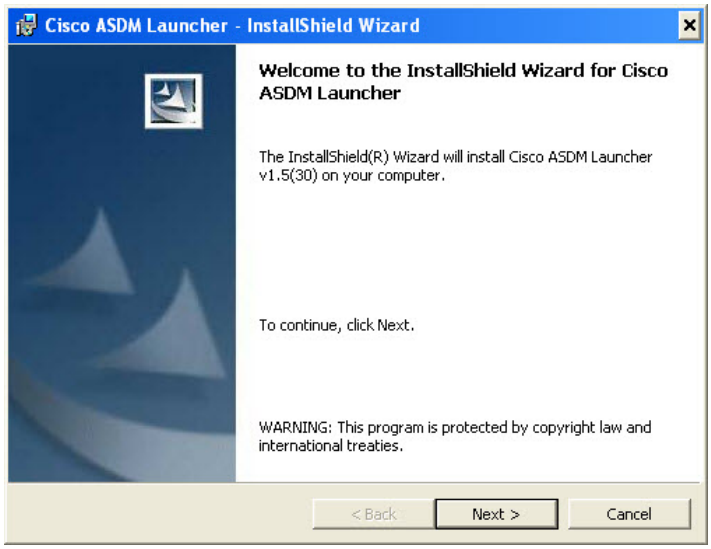


ภาพที่ ๙ ผลการ Download ASDM Launcher

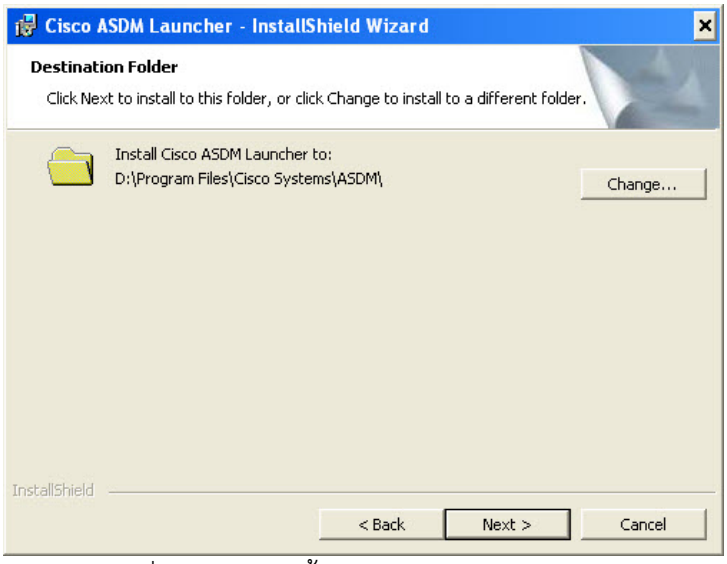


ภาพที่ ๑๐ การ Open Executable File

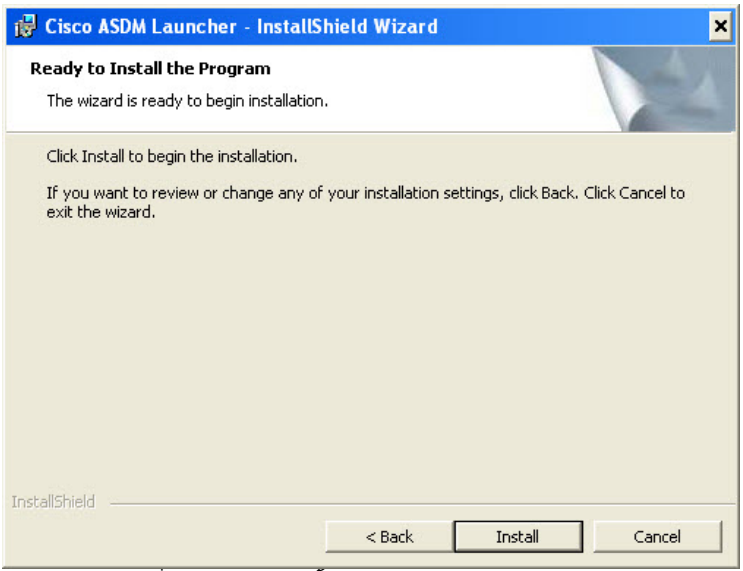
ภาพที่ ๑๑ Security Warning



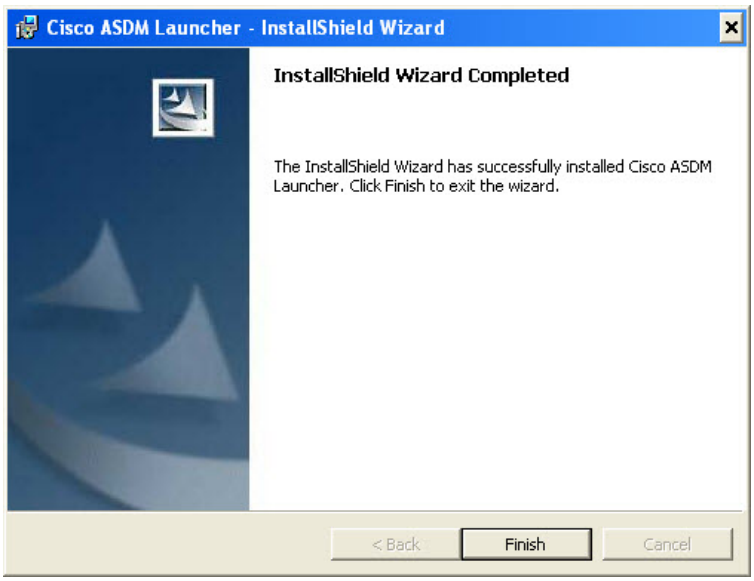
ภาพที่ ๑๒ การติดตั้งโปรแกรม ASDM Launcher



ภาพที่ ๑๓ การติดตั้งโปรแกรม ASDM Launcher



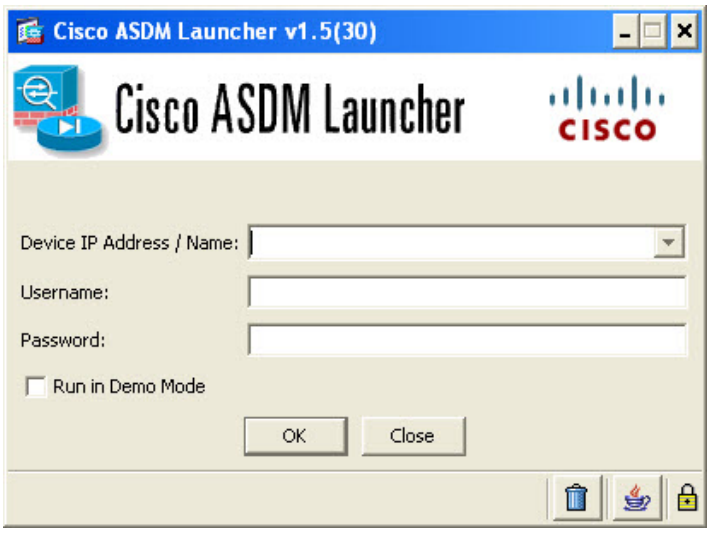
ภาพที่ ๑๔ การติดตั้งโปรแกรม ASDM Launcher



ภาพที่ ๑๕ ผลการติดตั้งโปรแกรม ASDM Launcher

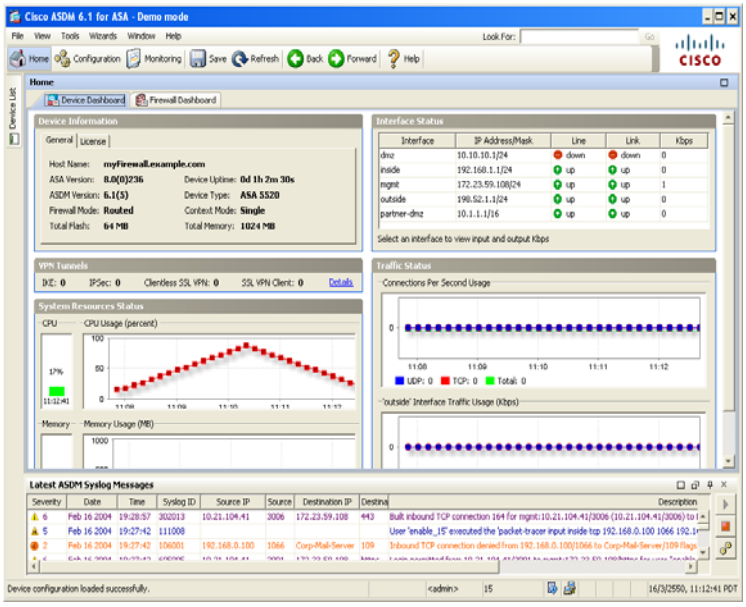
ในการกำหนดค่า Configuration ต่าง ๆ จะมีลักษณะการกำหนดอยู่ ๒ รูปแบบ คือ กำหนดให้ Packet ผ่านได้ และกำหนดให้ Packet ผ่านไม่ได้ ซึ่งการจะกำหนดให้ผ่านหรือไม่ให้ผ่านขึ้นอยู่กับ Policy ที่กรมพัฒนาที่ดินวางไว้ และความจำเป็นที่ใช้ในการติดต่อสื่อสารระหว่างเครือข่ายต่าง ๆ ที่กำหนดขึ้นมา เช่นการติดต่อระหว่างอุปกรณ์ IPPhone ใช้ Protocol H.๓๒๓ Port ๑๗๑๙ และ ๑๗๒๐ การให้บริการของเครื่องแม่ข่ายที่ต้องใช้งาน เช่นการให้บริการเครื่องแม่ข่ายเมล์ ใช้ Protocol SMTP Port ๒๕ การให้บริการเครื่องแม่ข่ายเวปใช้ Protocol HTTP Port ๘๐ หรือการให้บริการเครื่องแม่ข่าย DNS ใช้ Protocol HTTP Port ๕๓ โดยมีขั้นตอนตัวอย่างการกำหนดค่าต่าง ๆ โดยสังเขป ดังนี้

๙) เรียกโปรแกรม Cisco ASDM Launcher ขึ้นมาใช้งาน ระบบฯ จะให้ระบุ IP ของระบบฯที่จะเข้าใช้งาน และต้องระบุ User และPassword ที่มีสิทธิเรียกใช้งาน



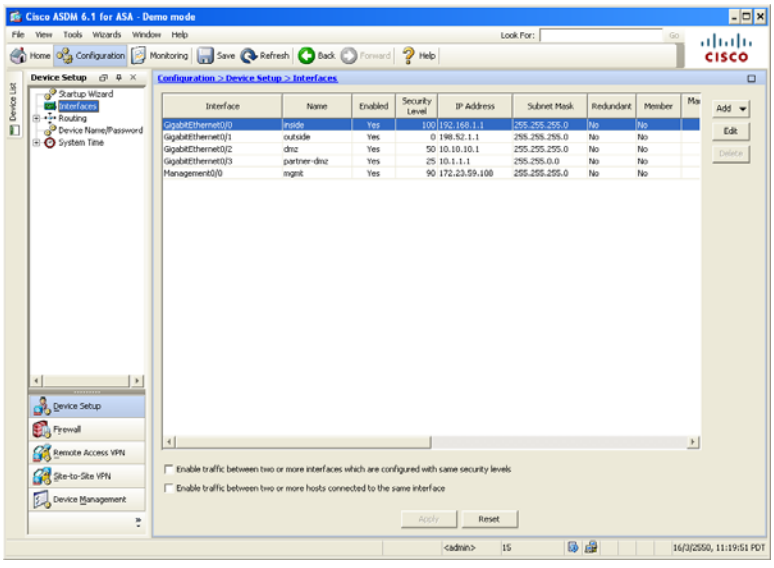
ภาพที่ ๑๖ การเรียกใช้งานโปรแกรม ASDM Launcher

๑๐) ปรากฏหน้าต่าง Cisco ASDM ๖.๑ ขึ้นมาดังรูป



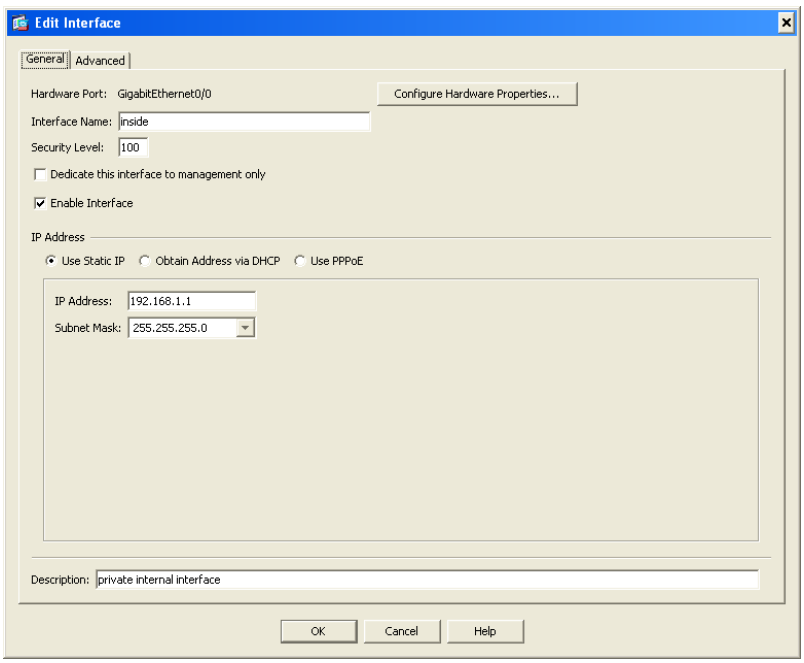
ภาพที่ ๑๗ การใช้ งานโปรแกรม Cisco ASDM ๖.๑ for ASA

๑๑) เลือกแถบเมนู Configuration จากนั้นในช่องด้านซ้ายมือ เลือก Device Setup และเลือกเมนูย่อยมาที่ Interface เพื่อให้กำหนดค่า Zone ต่าง ๆ ของกรมพัฒนาที่ดิน ตามที่ได้ออกแบบไว้ (เป็นการกำหนดค่าเครือข่ายต่าง ๆ ให้ระบบ)



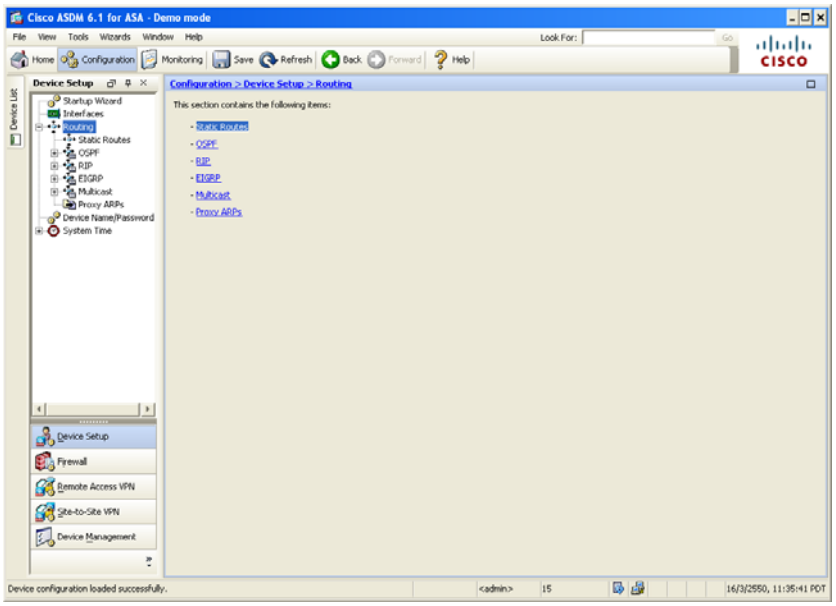
ภาพที่ ๑๘ การกำหนดค่า Interface Cisco ASDM ๖.๑ for ASA

๑๒) การกำหนดค่า Zone ต่างๆของระบบฯ ทำได้โดยในส่วนของรายการ Interface ของจอแสดงด้านขวา ให้ดับเบิ้ลคลิ้กเลือก Interface ที่ต้องการกำหนดจากนั้นจะปรากฏหน้าต่าง Edit Interfaceให้ระบุค่าคุณสมบัติตามที่ได้ออกแบบไว้ จากนั้นกดปุ่ม OK



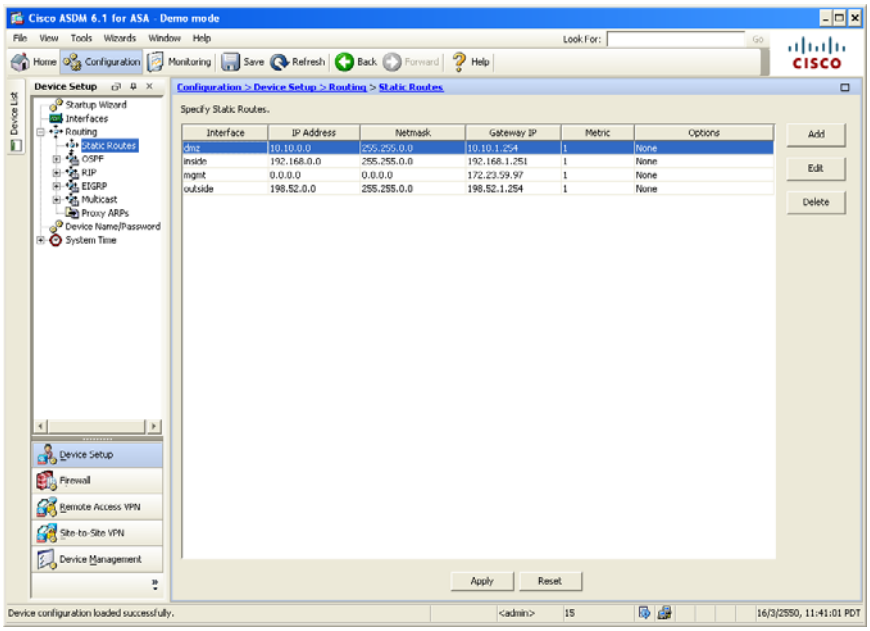
ภาพที่ ๑๙ การกำหนดค่า Interface Cisco ASDM ๖.๑ for ASA

๑๓) เลือกแถบเมนู Configuration จากนั้นในช่องด้านซ้ายมือ เลือก Device Setup และเลือกเมนูย่อยมาที่ Routing เพื่อให้กำหนดค่า Routing Table ต่าง ๆ ของกรมพัฒนาที่ดินตามที่ได้ออกแบบไว้ (เป็นการระบุเส้นทางการ Route ของแต่ละเครือข่าย)

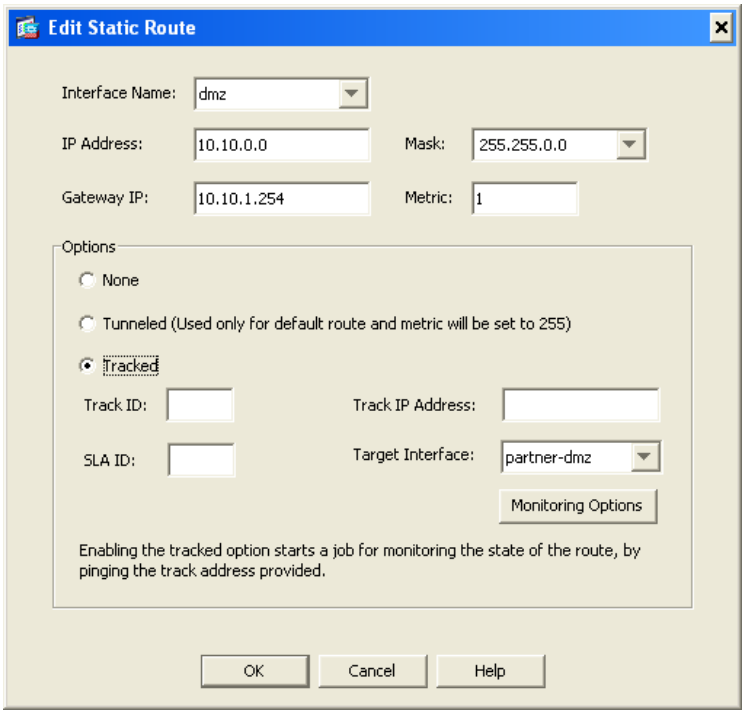


ภาพที่ ๒๐ การกำหนดค่า Routing Cisco ASDM ๖.๑ for ASA

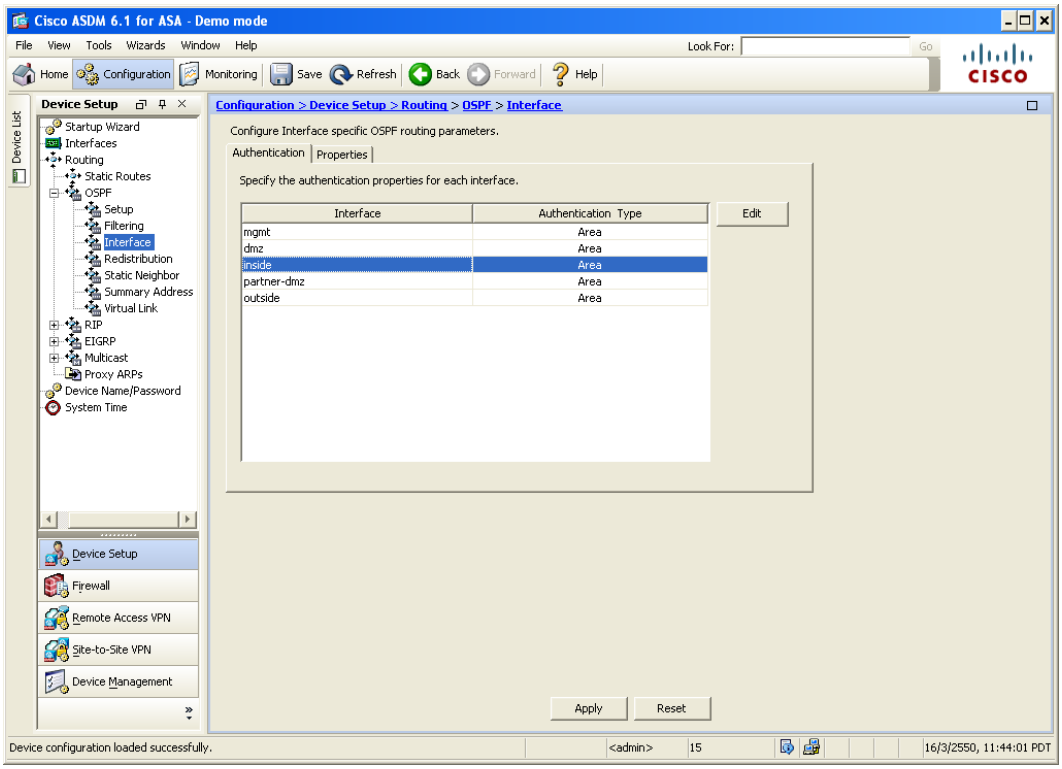
๑๔) การกำหนดค่า Routing ต่าง ๆ ของระบบฯ ทำได้โดยในส่วนของรายการ Routing ของจอแสดงด้านซ้ายมือให้เลือก Routing Protocol ที่ต้องการ จากนั้น ให้ดับเบิ้ลคลิ้กเลือก Interface ที่ต้องการกำหนดด้านขวามือ จากนั้นจะปรากฏหน้าต่าง Edit Protocol Routeให้ระบุค่าคุณสมบัติตามที่ได้ออกแบบไว้ จากนั้นกดปุ่ม OK



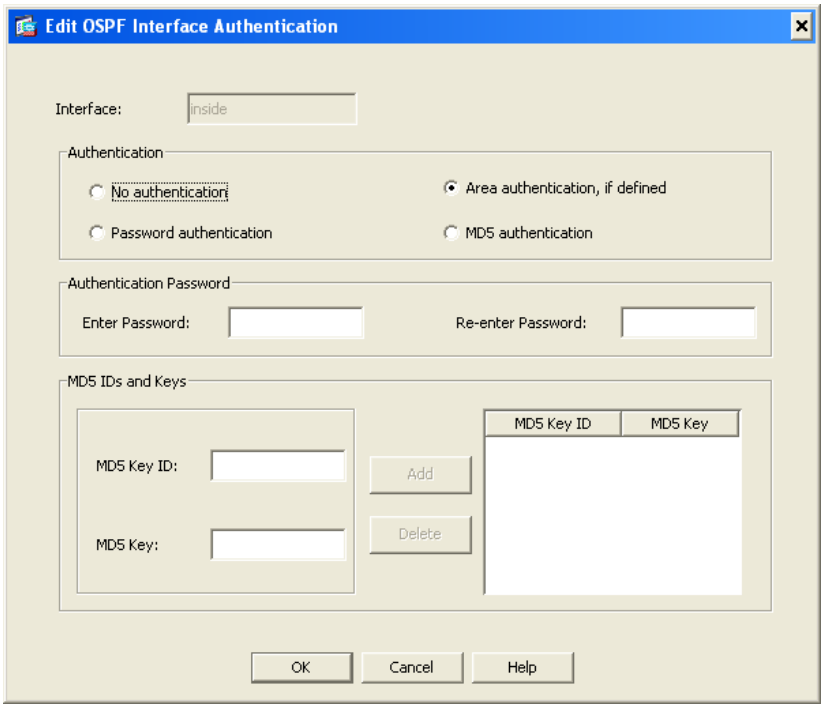
ภาพที่ ๒๑ การกำหนดค่า Routing Protocol Cisco ASDM ๖.๑ for ASA



ภาพที่ ๒๒ การกำหนดค่า Routing Protocol Cisco ASDM ๖.๑ for ASA

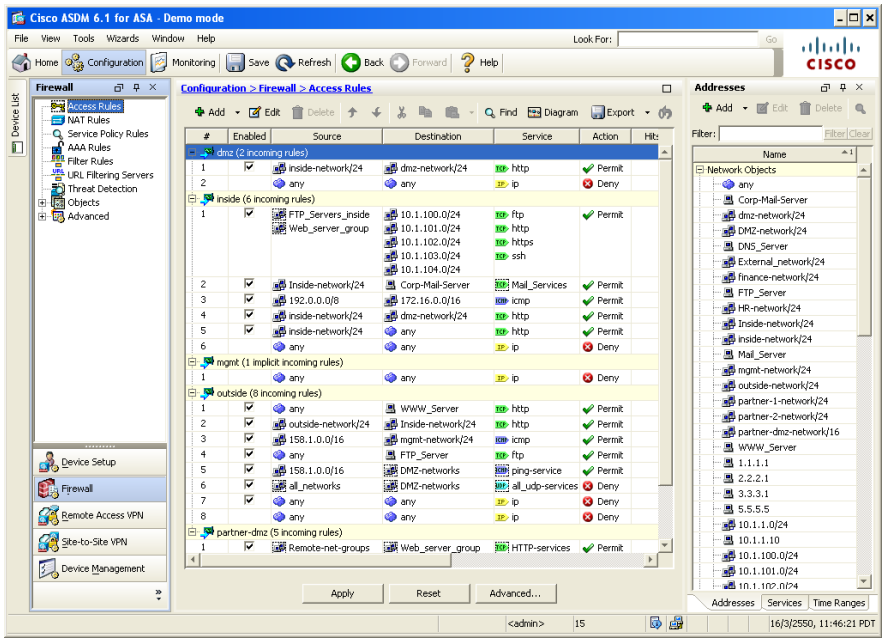


ภาพที่ ๒๓ การกำหนดค่า Routing Protocol Cisco ASDM ๖.๑ for ASA



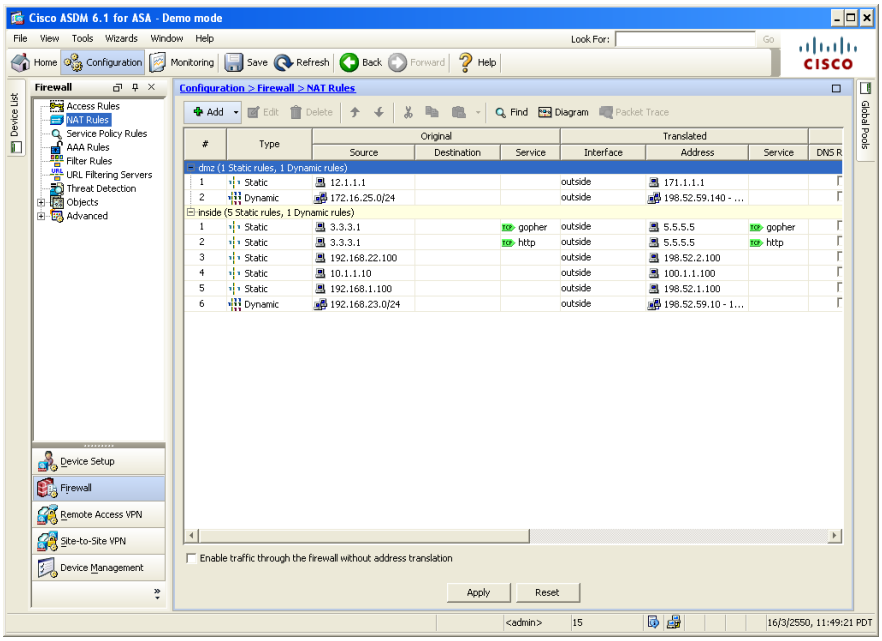
ภาพที่ ๒๔ การกำหนดค่า Routing Protocol Cisco ASDM ๖.๑ for ASA

๑๕) เลือกแถบเมนู Configuration จากนั้นในช่องด้านซ้ายมือ เลือก Firewall และเลือกเมนูย่อยมาที่ Access Rules เพื่อให้กำหนดค่า Access Rules ต่าง ๆ ของกรมพัฒนาที่ดิน ตามที่ได้ออกแบบไว้ (เป็นการกำหนดค่า Packet Permission ให้แต่ละเครือข่าย ตาม Policy ที่ได้มีการออกแบบไว้)



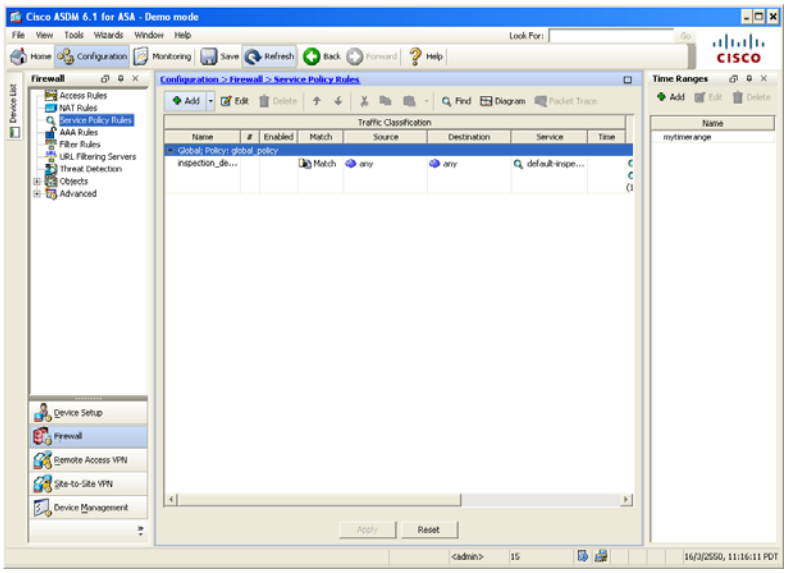
ภาพที่ ๒๕ การกำหนดค่า Access Rules Cisco ASDM ๖.๑ for ASA

๑๖) เลือกแถบเมนู Configuration จากนั้นในช่องด้านซ้ายมือ เลือก Firewall และเลือกเมนูย่อยมาที่ NAT (Network Address Translate) Rules เพื่อให้กำหนดค่า NAT Rule ต่าง ๆ ของกรมพัฒนาที่ดิน ตามที่ได้ออกแบบไว้ (เป็นการกำหนดค่าให้เครื่องแม่ข่ายบริการ สำหรับให้บริการเครือข่ายภายนอก)



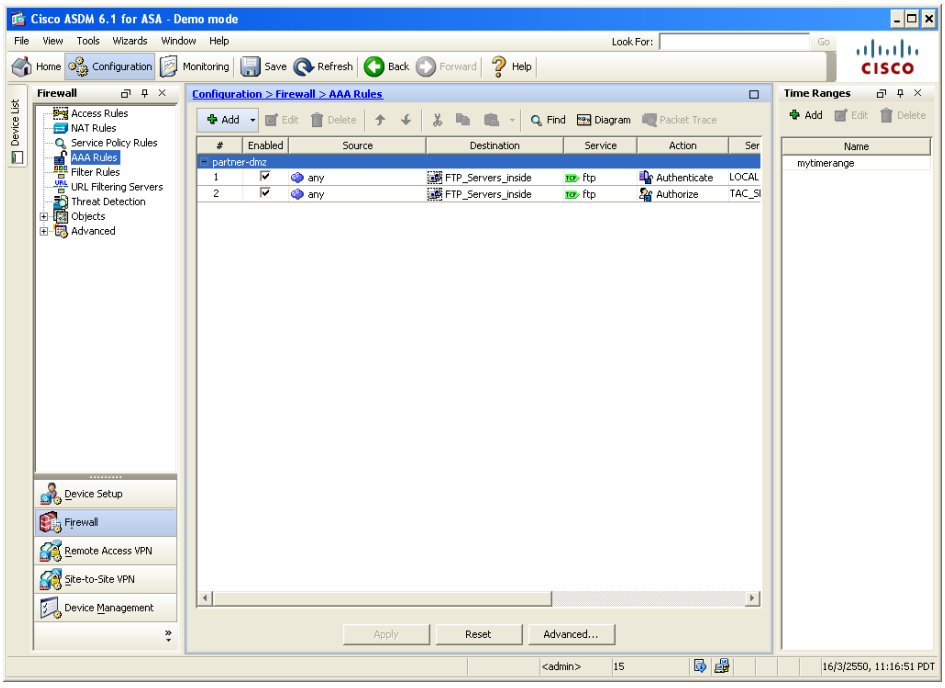
ภาพที่ ๒๖ การกำหนดค่า NAT Rules Cisco ASDM ๖.๑ for ASA

๑๗) เลือกแถบเมนู Configuration จากนั้นในช่องด้านซ้ายมือ เลือก Firewall และเลือกเมนูย่อยมาที่ Service Policy Rules เพื่อให้กำหนดค่า Service Policy Rule ต่าง ๆ ของ กรมพัฒนาที่ดิน ตามที่ได้ออกแบบไว้



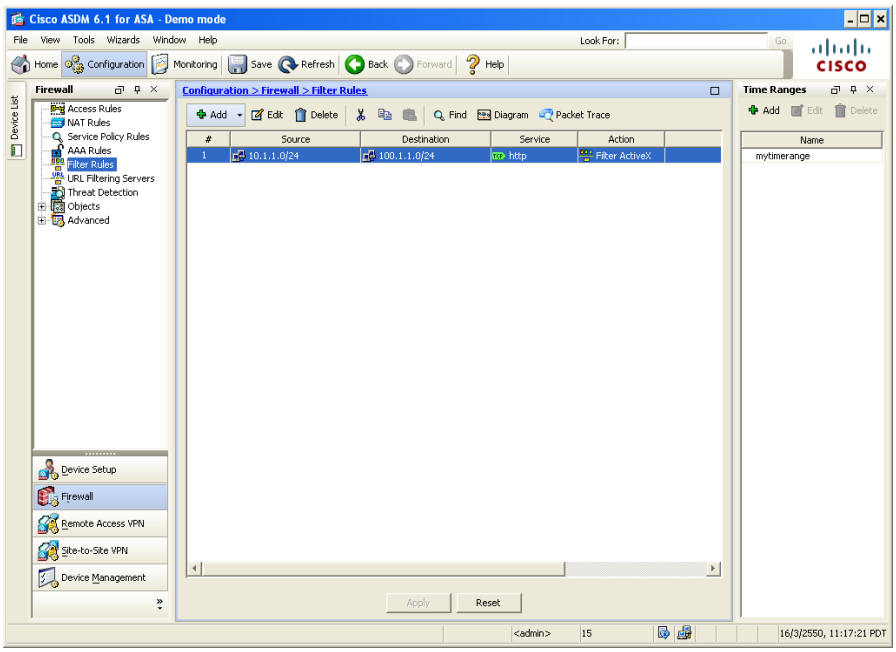
ภาพที่ ๒๗ การกำหนดค่า Service Policy Rules Cisco ASDM ๖.๑ for ASA

๑๘) เลือกแถบเมนู Configuration จากนั้นในช่องด้านซ้ายมือ เลือก Firewall และเลือกเมนูย่อยมาที่ AAA Rules เพื่อให้กำหนดค่า AAA Rule ต่าง ๆ ของกรมพัฒนาที่ดิน ตามที่ได้ออกแบบไว้ (เป็นการกำหนดรูปแบบการ Authentication ของระบบ)



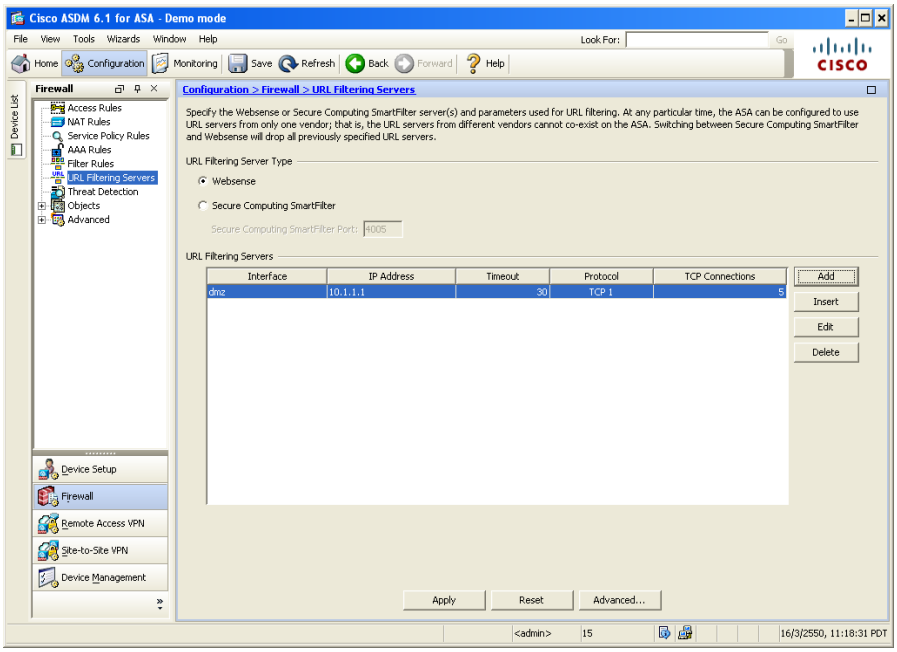
ภาพที่ ๒๘ การกำหนดค่า AAA Rules Cisco ASDM ๖.๑ for ASA

๑๙) เลือกแถบเมนู Configuration จากนั้นในช่องด้านซ้ายมือ เลือก Firewall และเลือกเมนูย่อยมาที่ Filter Rules เพื่อให้กำหนดค่า Filter Rule ต่าง ๆ ของกรมพัฒนาที่ดิน ตามที่ได้ออกแบบไว้ (เป็นการกำหนดตัวคัดกรองย่อย เพื่อใช้ในการทำงานตาม Policy)



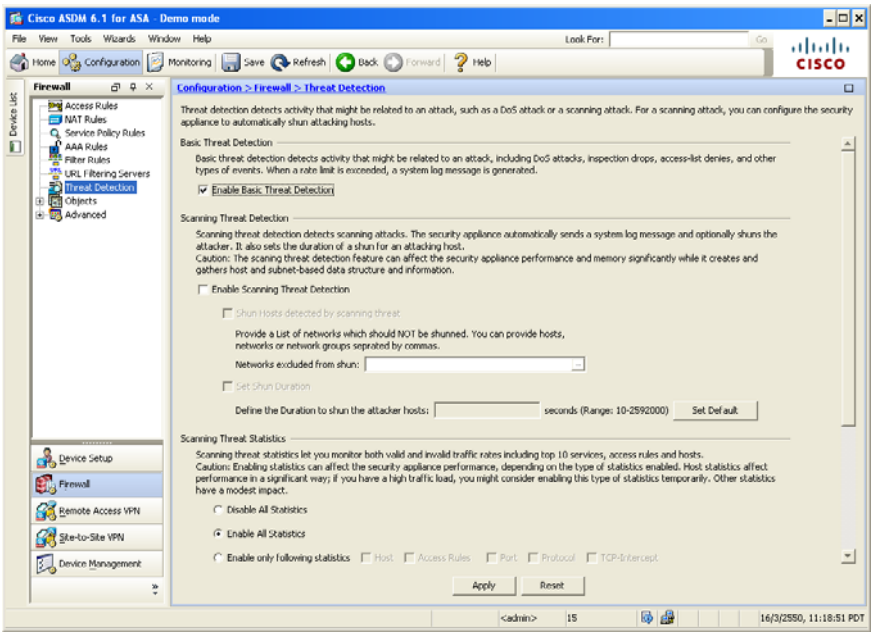
ภาพที่ ๒๙ การกำหนดค่า Filter Rules Cisco ASDM ๖.๑ for ASA

๒๐) เลือกแถบเมนู Configuration จากนั้นในช่องด้านซ้ายมือ เลือก Firewall และเลือกเมนูย่อยมาที่ URL Filtering Servers เพื่อให้กำหนดค่า URL Filter Rule ต่าง ๆ ของกรมพัฒนาที่ดิน ตามที่ได้ออกแบบไว้ (เป็นการกำหนดตัวคัดกรองย่อย เพื่อใช้ในการเรียกDomain Name ผ่าน Browser ตาม Policy)



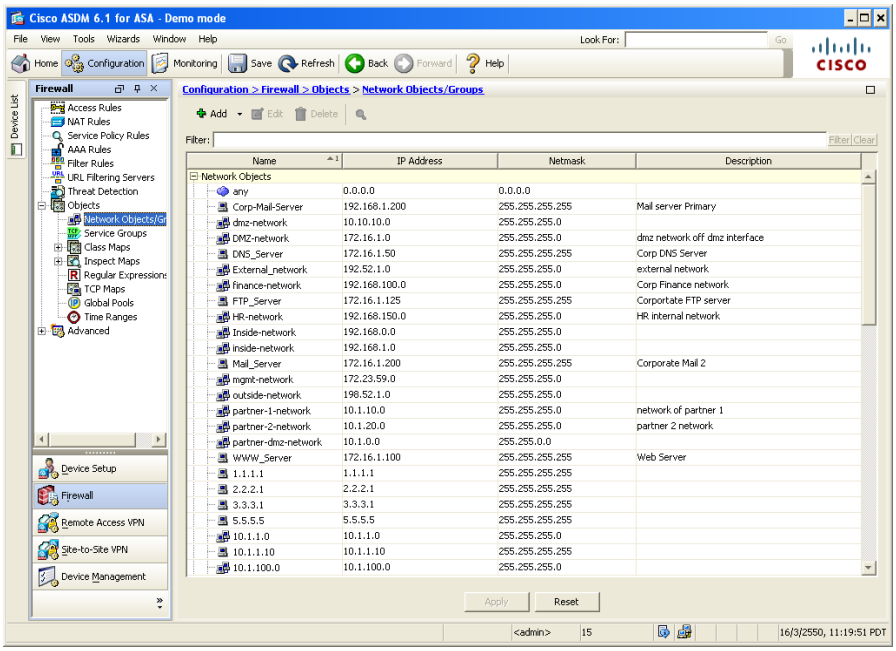
ภาพที่ ๓๐ การกำหนดค่า URL Filtering Servers Cisco ASDM ๖.๑ for ASA

๒๑) เลือกแถบเมนู Configuration จากนั้นในช่องด้านซ้ายมือ เลือก Firewall และเลือกเมนูย่อยมาที่ Threat Detection เพื่อให้กำหนดค่า Threat Detect Rule ของกรมพัฒนาที่ดิน ตามที่ได้ออกแบบไว้ (เป็นการกำหนดค่าการตรวจสอบรูปแบบไวรัส)



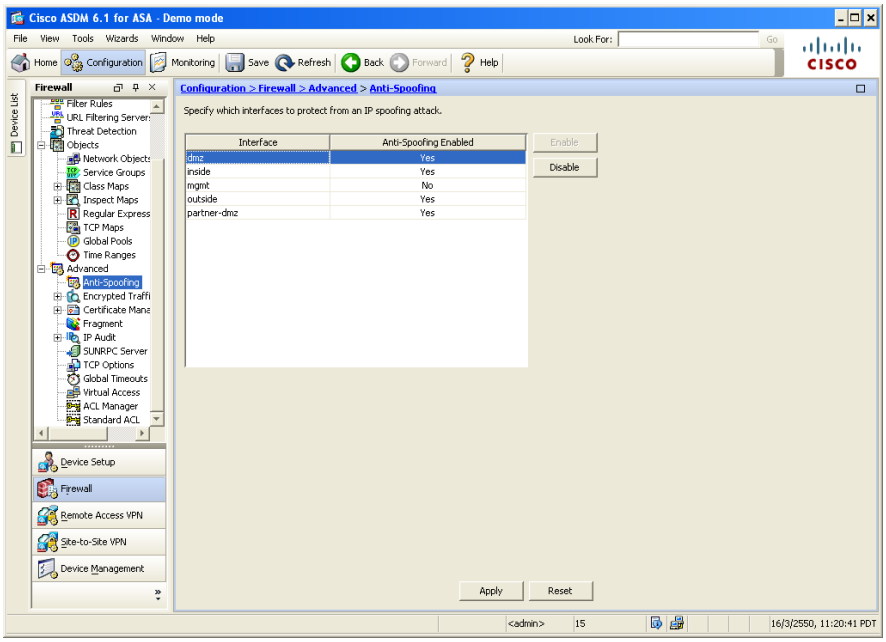
ภาพที่ ๓๑ การกำหนดค่า Threat Detection Cisco ASDM ๖.๑ for ASA

๒๒) เลือกแถบเมนู Configuration จากนั้นในช่องด้านซ้ายมือ เลือก Firewall และเลือกเมนูย่อยมาที่ Objects เพื่อให้กำหนดค่า Objects ต่าง ๆ ของกรมพัฒนาที่ดิน ตามที่ได้ออกแบบไว้ (เป็นการกำหนดค่า Objects ที่นำมาใช้งานตาม Policy)



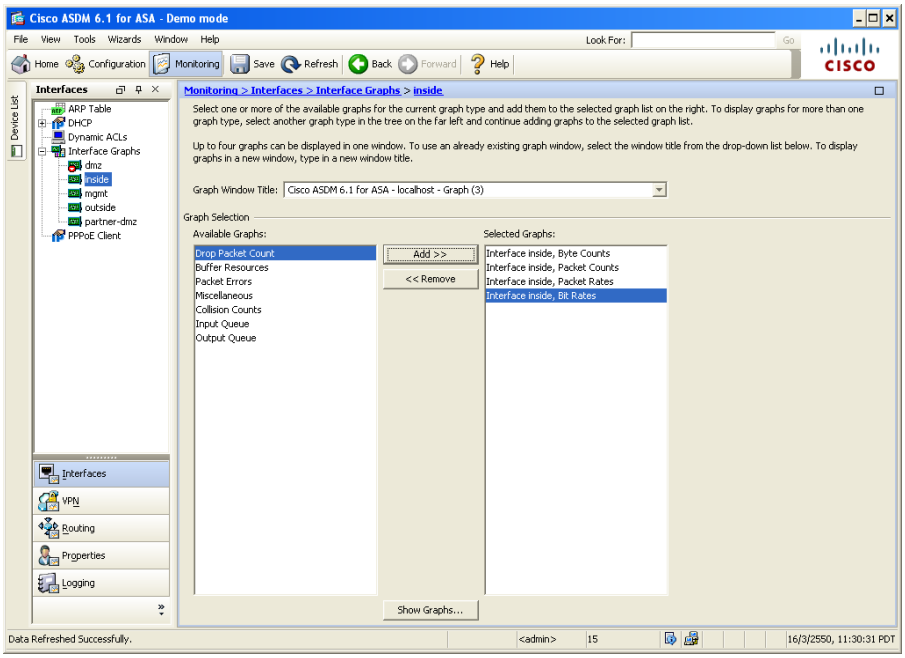
ภาพที่ ๓๒ การกำหนดค่า Objects Cisco ASDM ๖.๑ for ASA

๒๓) เลือกแถบเมนู Configuration จากนั้นในช่องด้านซ้ายมือ เลือก Firewall และเลือกเมนูย่อยมาที่ Advanced เพื่อให้กำหนดค่าคำสั่งระดับ Advanced Rule ต่าง ๆ ของกรมพัฒนาที่ดิน ตามที่ได้ออกแบบไว้

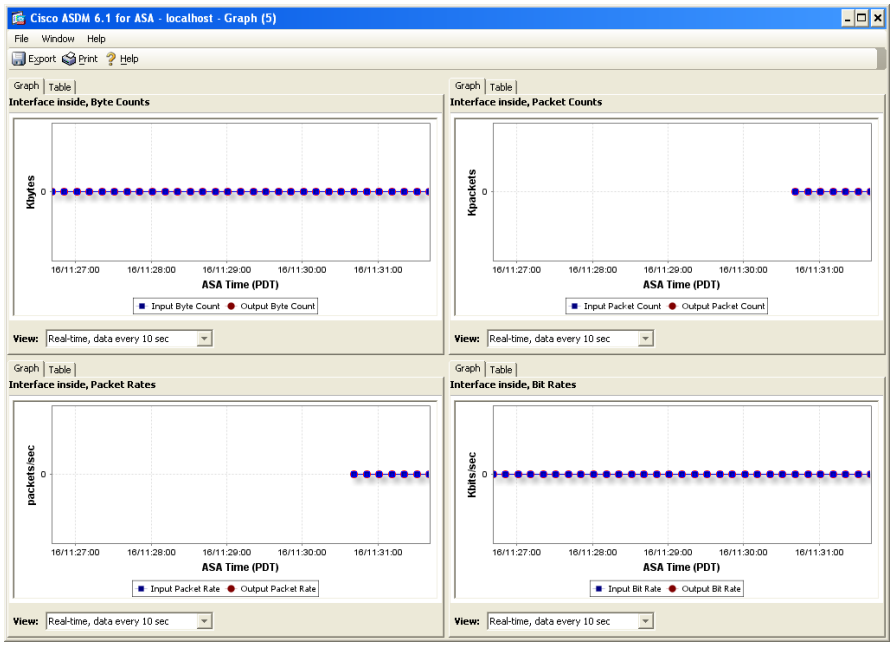


ภาพที่ ๓๓ การกำหนดค่า Advanced Rule Cisco ASDM ๖.๑ for ASA

๒๔) เลือกแถบเมนู Monitoring จากนั้นในช่องด้านซ้ายมือ เลือก Interface Graphs และเลือกเมนูย่อยมาที่ Interface ที่ต้องการ Monitor ในจอด้านขวามือช่อง Available Graphs กำหนดสิ่งที่ต้องการตรวจสอบ จากนั้นกด Show Graphs เพื่อใช้ในการตรวจสอบ Monitoring

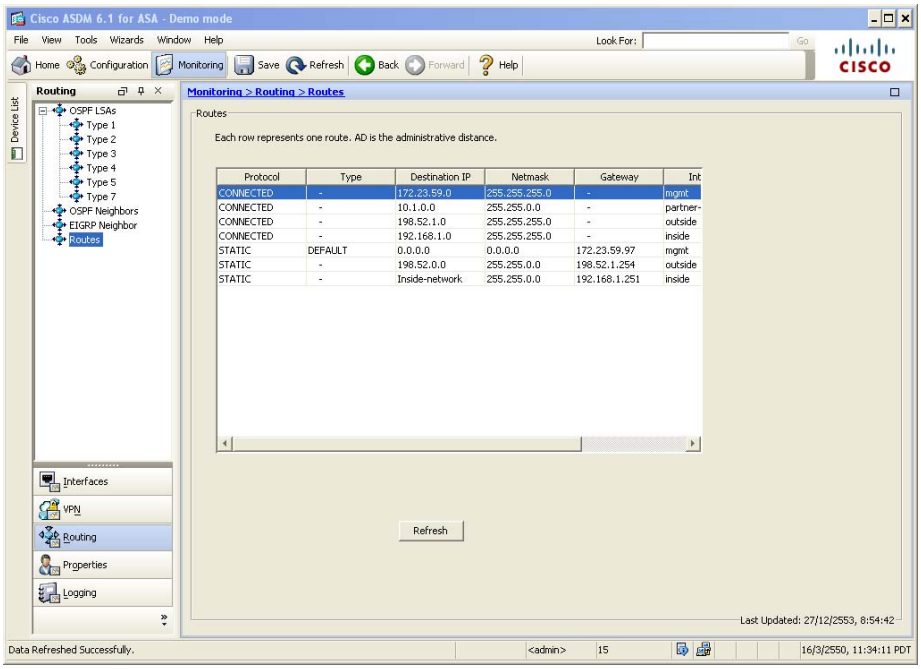


ภาพที่ ๓๔ การกำหนดค่า Monitor Interface Cisco ASDM ๖.๑ for ASA



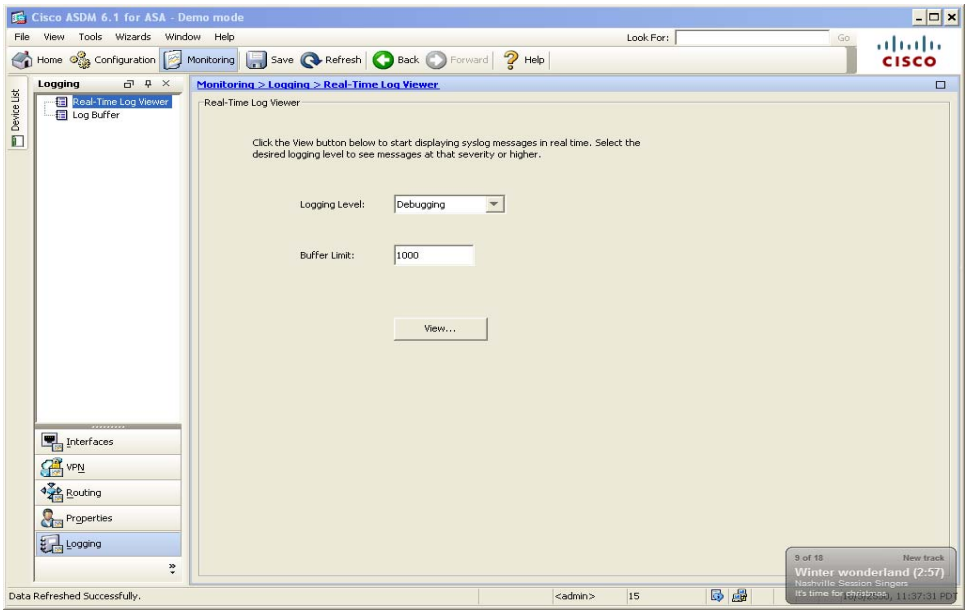
ภาพที่ ๓๕ การกำหนดค่า Monitor Interface Cisco ASDM ๖.๑ for ASA

๒๕) เลือกแถบเมนู Monitoring จากนั้นในช่องด้านซ้ายมือ เลือก Routing และเลือกเมนูย่อยมาที่ Routes ในจอด้านขวามือ จะแสดงค่า Routing ทั้งหมดที่กำหนดไว้เพื่อทำการตรวจสอบ

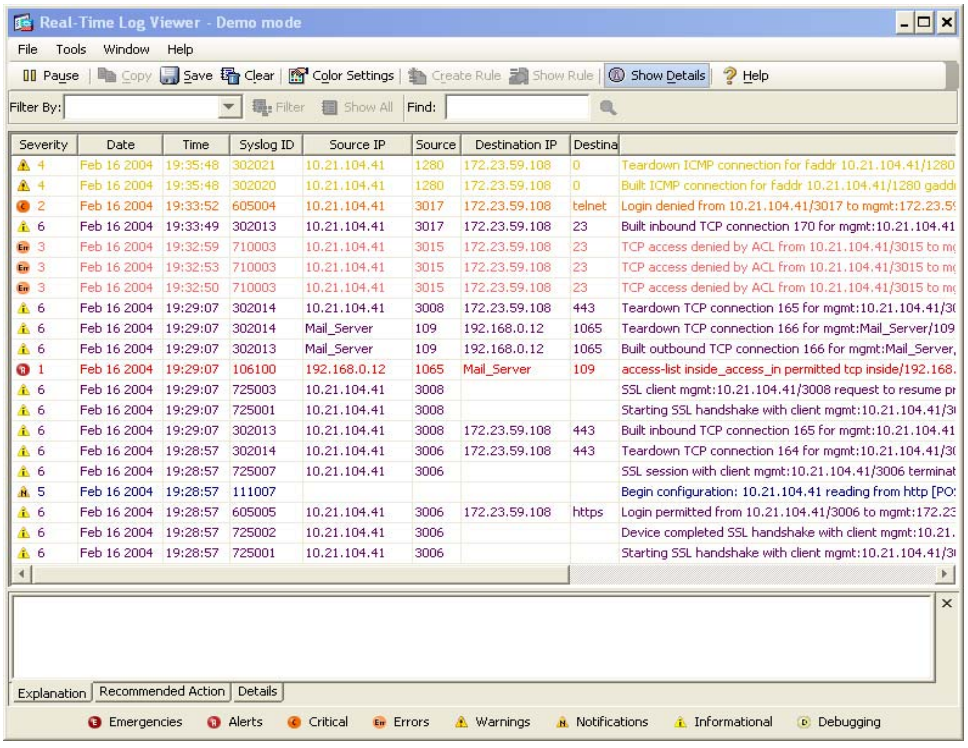


ภาพที่ ๓๖ การกำหนดค่า Monitor Routing Cisco ASDM ๖.๑ for ASA

๒๖) เลือกแถบเมนู Monitoring จากนั้นในช่องด้านซ้ายมือ เลือก Logging และเลือกเมนูย่อยมาที่ Real-Time Log Viewer ในจอด้านขวามือ จะแสดงค่า Logging Level ให้ระบุ Level ของ Log ที่ต้องการ Monitor จากนั้นกดปุ่ม View

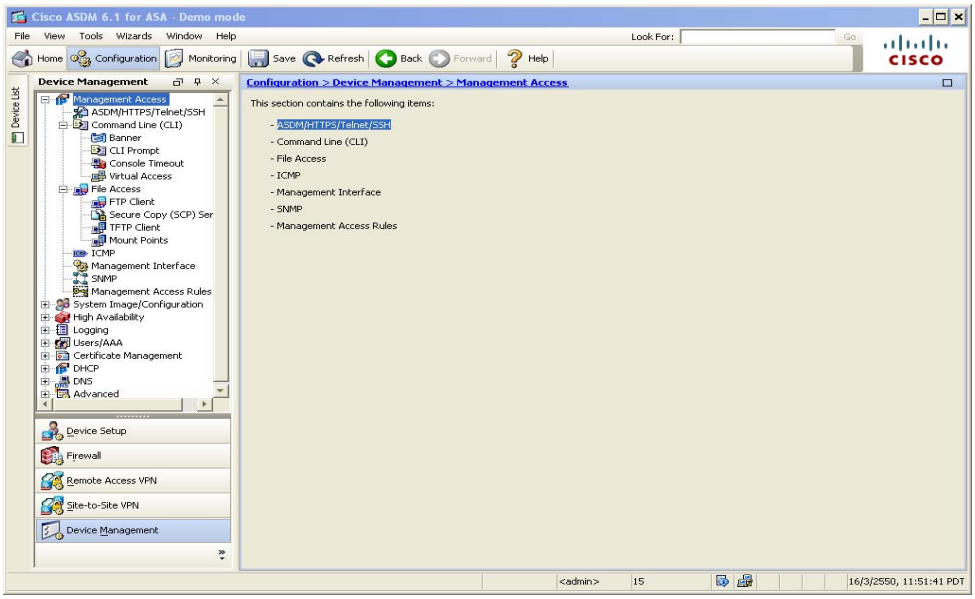


ภาพที่ ๓๗ การกำหนดค่า Monitor Logging Cisco ASDM ๖.๑ for ASA



ภาพที่ ๓๘ การกำหนดค่า Monitor Logging Cisco ASDM ๖.๑ for ASA

๒๗) เลือกแถบเมนู Configuration จากนั้นในช่องด้านซ้ายมือ เลือก Device Management และเลือกเมนูย่อยมาที่ Management Access เพื่อกำหนดค่าการจัดการย่อย เช่น ASDM/HTTPS/Telnet/SSH , Command Line , File Access , ICMP, Management Interface , SNMP , Management Access Rules เพื่อใช้ในการตรวจสอบระบบ



ภาพที่ ๓๙ การกำหนดค่า Device Management Cisco ASDM ๖.๑ for ASA

แผนผังแสดงขั้นตอนและวิธีการปฏิบัติงาน

ระบบ Hardware Firewall

ลำดับที่	ผังกระบวนการ	รายละเอียดงาน
	เริ่มต้น	
๑	วิเคราะห์และกำหนด Firewall Policy	๑. วิเคราะห์การใช้งานเครือข่าย ค่า Service ที่จำเป็นต้องใช้งาน ค่า Protocol ที่จำเป็นต้องใช้งาน ช่องทางการเชื่อมต่อที่ใช้งานของกรมพัฒนาที่ดิน เพื่อกำหนด Firewall Policy
๒	Firewall Policy ครบถ้วน ไม่ใช่	๒. ตรวจสอบจำนวน Firewall Policy ว่าครบถ้วนหรือไม่ ถ้ายังไม่ครบให้กลับไปทำขั้นตอนที่ ๑ ถ้าครบแล้วให้ไปทำขั้นตอนที่ ๓
๓	ใช่ กำหนดค่า Configuration บนอุปกรณ์ Hardware Firewall	๓. กำหนดค่า Configuration Firewall Policy ลงบนอุปกรณ์เครือข่าย Hardware Firewall
๔	Firewall Policy สามารถใช้งานได้ ไม่ใช่	๔. ทดสอบการทำงานของแต่ละ Firewall Policy ที่กำหนดบนอุปกรณ์ ว่าสามารถใช้งานได้หรือไม่ ถ้าไม่สามารถใช้งานได้ให้กลับไปทำขั้นตอนที่ ๓ ถ้าใช้งานได้แล้วให้ไปทำขั้นตอนที่ ๕
๕	ใช่ เครือข่ายทำงานได้ปกติ ไม่ใช่	๕. ทดสอบการทำงานของระบบเครือข่ายของกรมพัฒนาที่ดินเมื่อใช้งานร่วมกับ Firewall Policy ว่าสามารถใช้งานได้ปกติหรือไม่ ถ้าไม่สามารถใช้งานได้ให้กลับไปทำขั้นตอนที่ ๓ ถ้าใช้งานได้แล้วให้ไปทำขั้นตอนที่ ๖
๖	ใช่ บันทึกค่า Configuration บนอุปกรณ์ Switch	๖. บันทึกค่า Configuration ลงบนอุปกรณ์ Hardware Firewall
	สิ้นสุด	

ขั้นตอนการติดตั้งและดำเนินการ

๑) เชื่อมสายโรลโอเวอร์ (Rollover) ผ่านคอนโซล พอร์ต (Console Port) ของอุปกรณ์ด่านกันบุกรุก (Hardware Firewall) เข้ากับเครื่องคอมพิวเตอร์ควบคุมระบบฯ

๒) ติดต่อกับระบบผ่านทางโปรโตคอลรูปแบบซีเคียวร์ชีล (Secure Shell)

๓) ระบบให้ระบุรหัสผู้ใช้งาน (User) และรหัสผ่าน (Password) ที่ใช้งานให้ใช้ค่าเริ่มต้น ยี่ห้อซิสโก้ (Cisco) ที่กำหนดมาจากโรงงาน จากนั้นกำหนดค่าหมายเลขอ้างอิงในการติดต่อสื่อสาร (IP Address) สำหรับส่วน ต่อประสาน (Interface) ที่เป็นช่องทางการควบคุม (Managed Port) กำหนดค่ารหัสผู้ใช้งาน (User) และเปิดให้สามารถใช้งานรหัสผ่าน (Enable Password) ที่ใช้งานเพื่อกำหนดค่าสิทธิ์ (Permission) ที่ในการใช้เชื่อมต่อกับระบบ จากนั้นเมื่อสามารถติดต่อผ่านทางเครือข่ายแลน (LAN) กับระบบได้แล้ว จึงใช้การเชื่อมต่อผ่านเครือข่าย เพื่อ บรรจุลง (Download) และติดตั้งโปรแกรมส่วนต่อประสานกราฟฟิกกับผู้ใช้ (Graphical user interface (GUI) และการกำหนดตั้งค่าคอนฟิกกูเรชั่น (Configuration) ผ่านทางโปรแกรมซิสโก้ เอเอสดีเอ็มรันเชอร์ (Cisco ASDM Launcher) เพื่อทำการกำหนดค่าคอนฟิกกูเรชั่น (Configuration) ระบบ อุปกรณ์ด่านกันบุกรุก (Hardware Firewall) ต่อไป

๓.๒ การติดตั้งและบริหารงานระบบด้านคอมพิวเตอร์ (Installation and Operation of the Computer) ประกอบด้วยรูปแบบเสมือน (Virtual)

๓.๒.๑ งานด้านการรักษาความปลอดภัยคอมพิวเตอร์ โดยใช้ระบบส่วนชุดคำสั่งด่านกันบุกรุก (Software Firewall)

ศูนย์สารสนเทศ กรมพัฒนาที่ดิน นำระบบชุดคำสั่งด่านกันบุกรุก (Software Firewall) มาใช้งานร่วมกับระบบ อุปกรณ์ด่านกันบุกรุก (Hardware Firewall) เพื่อรักษาความปลอดภัยระบบเครือข่ายให้เป็นไปตามข้อกำหนดที่วางไว้ ได้แก่ การควบคุมการเรียกใช้งานเว็บไซต์ บริการต่างๆของกรมพัฒนาที่ดิน การควบคุมการใช้งานอินเตอร์เน็ต ผ่านทางเครื่องบริการแทน (Proxy Server) และการควบคุมการเชื่อมต่อระหว่างเครือข่ายภายในของกรมพัฒนาที่ดินกับวีแอลเอเอ็น (VLAN) ของเครื่องแม่ข่ายบริการ

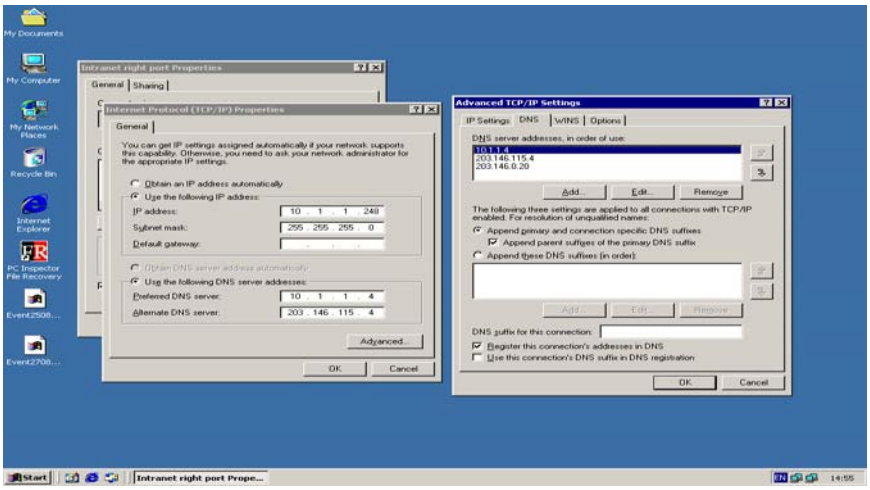
ระบบชุดคำสั่งด่านกันบุกรุก (Software Firewall) ที่นำมาใช้งานคือไมโครซอฟ อินเตอร์เน็ต ซีเคียวริตี้ แอนด์ เอคแซวเรชั่น เซฟเวอร์ (Microsoft Internet Security and Acceleration Server (ISA Server)) ซึ่งเป็นผลิตภัณฑ์โปรแกรมประยุกต์ด่านกันบุกรุก (Application Firewall) และแคชชิ่งเซฟเวอร์ (Caching Server) ของบริษัทไมโครซอฟท์ที่ทำงานบนระบบปฏิบัติการวินโดว์เซฟเวอร์ (Windows Server) ซึ่งมีความสามารถในด้านการควบคุม การใช้งานแบบกำหนดนโยบาย (Policy Based) และมีความสามารถด้านการทำเป็นแคชชิ่งเซฟเวอร์ (Caching Server) เพื่อให้การบริการแทน (Proxy Service) ได้

๓.๒.๑.๑ การติดตั้งระบบ Software Firewall

Microsoft Internet Security and Acceleration Server (ISA Server) เป็นผลิตภัณฑ์ Application Firewall และ Catching Server ของบริษัทไมโครซอฟร์ สำหรับองค์กรที่ทำงานบนระบบปฏิบัติการ Windows Server ซึ่งมีความสามารถในด้านการควบคุม การใช้งานแบบกำหนดนโยบาย (Policy Based) ทำให้ระบบเครือข่ายมีประสิทธิภาพโดยรวมสูงขึ้น และมีความสามารถด้านการจัดการเครือข่ายโดยที่ ISA Server มี ๒ เอดิชัน ซึ่งถูกออกแบบมาเพื่อให้เหมาะกับการใช้งานในรูปแบบต่าง ๆ ขององค์กร ไม่ว่าจะติดตั้งในรูปแบบแยกองค์ประกอบต่างๆ ออกจากกันหรือในรูปแบบรวม Firewall และ Catching Server ในแม่ข่ายเครื่องเดียวและสามารถจัดการเกี่ยวกับความปลอดภัยและการเข้าใช้งานอินเทอร์เน็ตได้ด้วยคอนโซลเดียว

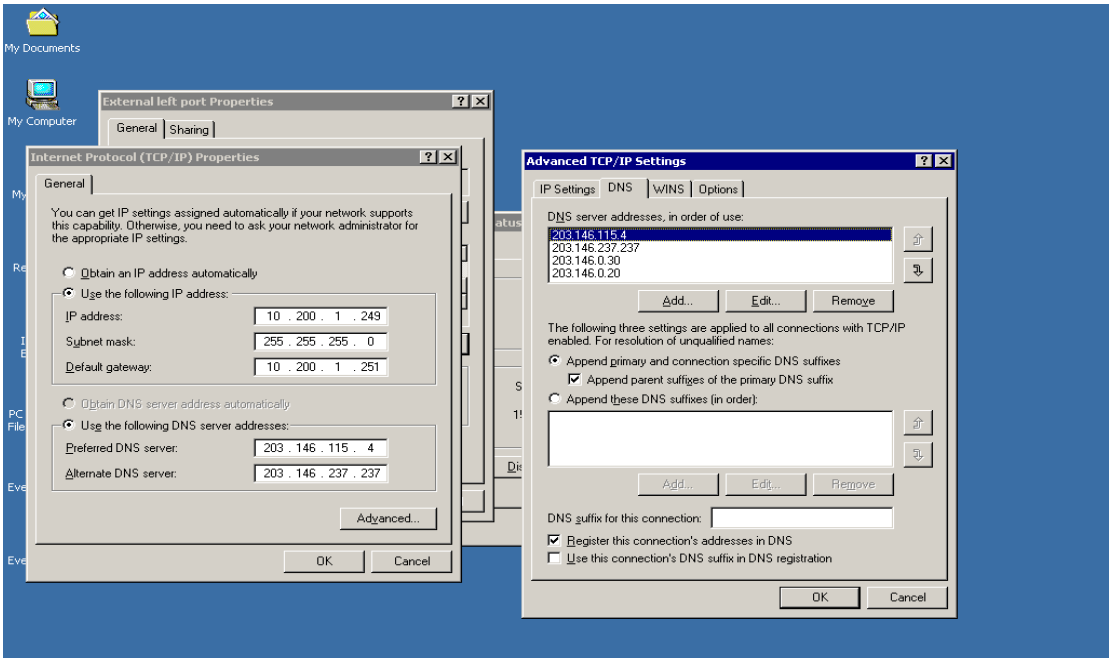
๓.๒.๑.๒ การกำหนดค่า Configuration ISA Server

๑) กำหนด IP Address ของกรมพัฒนาที่ดิน โดยคลิกขวาที่ My Network Places แล้วเลือก Intranet right port properties แล้วคลิกที่ Internet Protocol Properties ใส่ IP address เป็น ๑๐.๑.๑.๒๔๘ และสามารถเพิ่ม DNS Server โดยคลิกปุ่ม Advanced แล้วคลิกปุ่ม add เพื่อเพิ่ม address ของ DNS Server



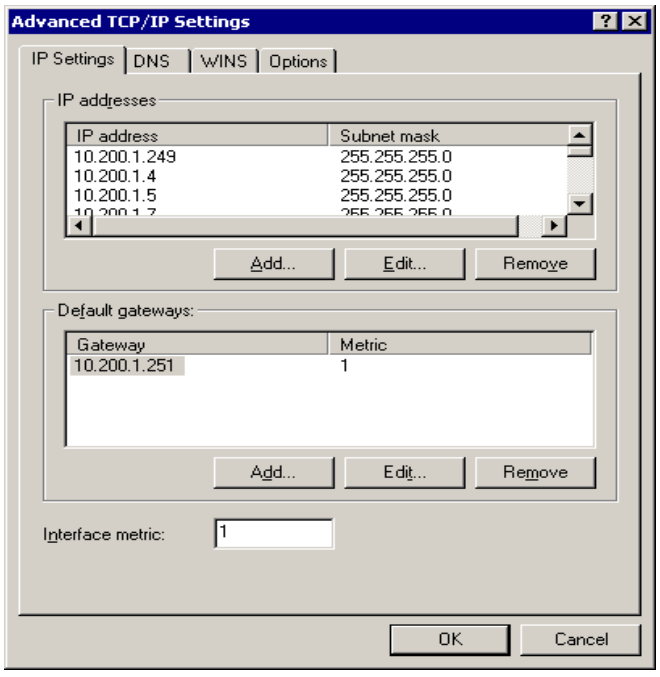
ภาพที่ ๔๐ การกำหนดค่า DNS Server

๒) ที่ External port Properties กำหนด IP address เป็น ๑๐.๒๐๐.๑.๒๔๙ และ DNS Server เป็น ๒๐๓.๑๔๖.๑๑๕.๔



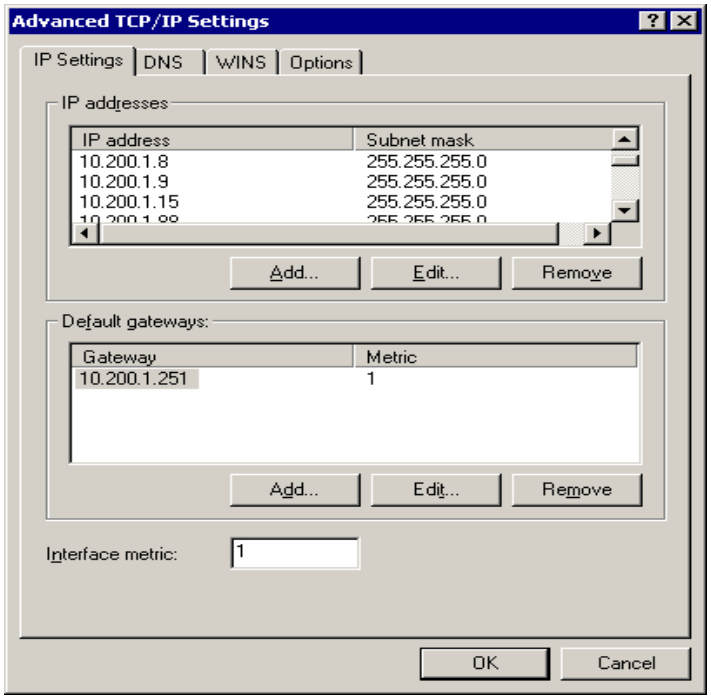
ภาพที่ ๔๑ การกำหนดค่า DNS Server

๓) ที่ Advanced TCP/IP Settings สามารถเพิ่ม IP address ได้โดยกดปุ่ม Add และ gateway เป็น ๑๐.๒๐๐.๑.๒๕๑



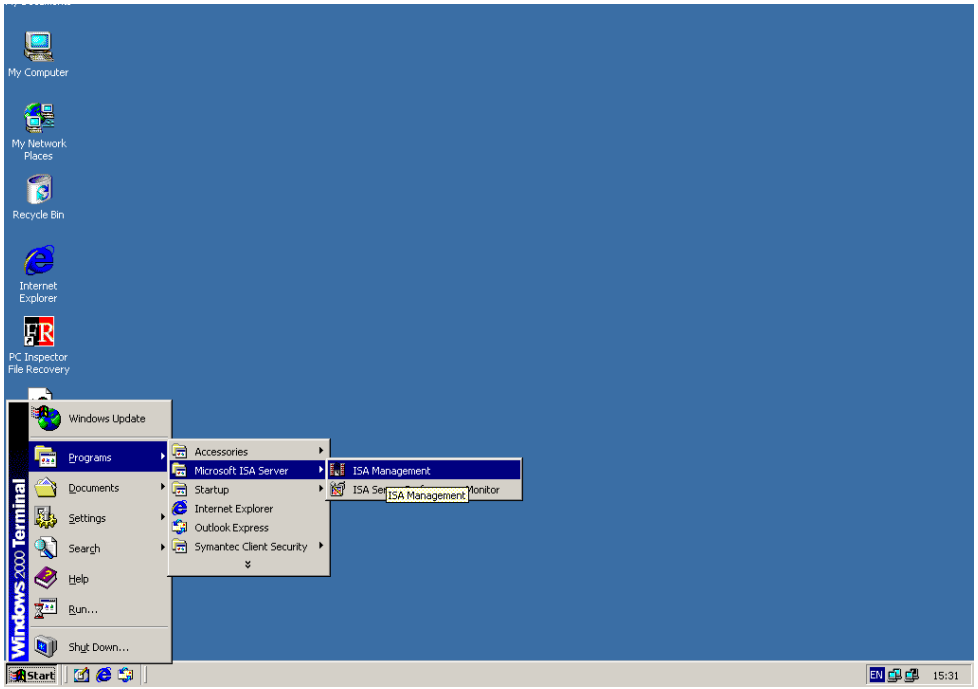
ภาพที่ ๔๒ การกำหนดค่ากำหนดค่า IP

๔) ที่ Advanced TCP/IP Settings สามารถลบ IP address ได้โดยกดปุ่ม Remove และแก้ไขโดยกดปุ่ม Edit



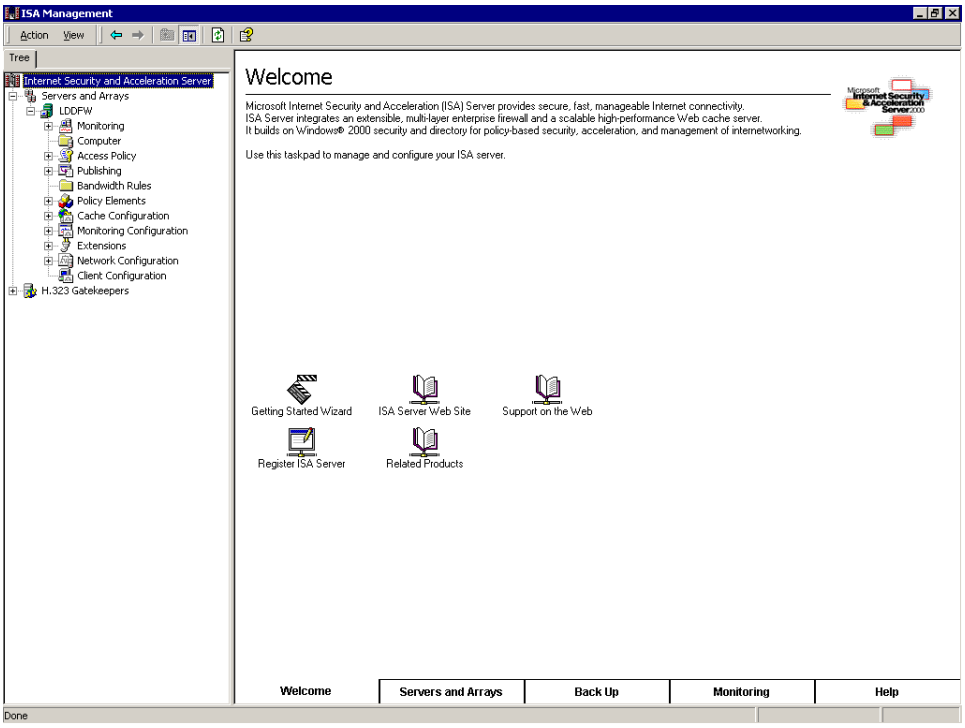
ภาพที่ ๔๓ การกำหนดค่ากำหนดค่า IP

๕) เปิดโปรแกรม ISA Management โดยคลิกที่ปุ่ม Start > Programs > Microsoft > ISA Server > ISA Management



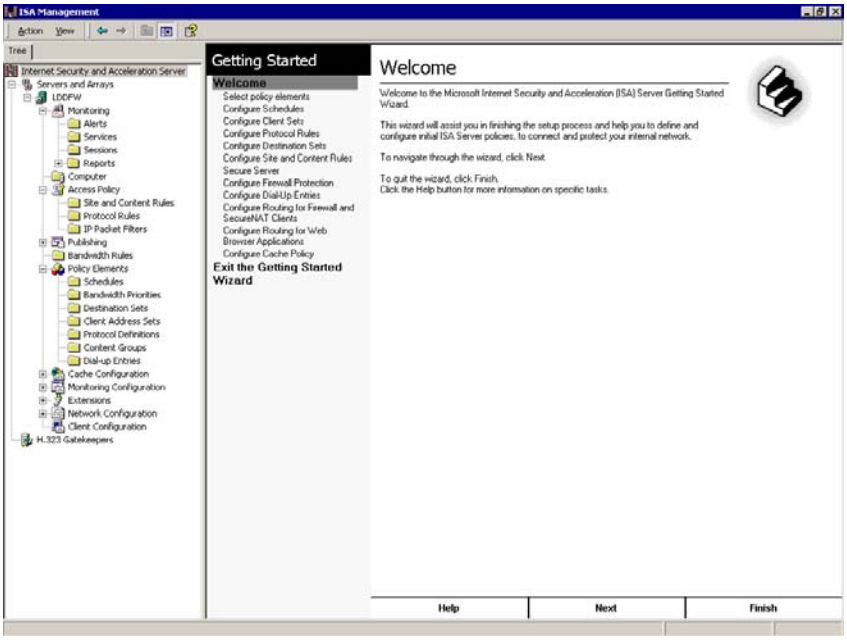
ภาพที่ ๔๔ การใช้งานโปรแกรม ISA

๖) จะปรากฏหน้าต่างโปรแกรม ISA Management เพื่อใช้กำหนดค่าของ ISA Server ในการป้องกันความปลอดภัย เช่น กำหนด policy security (นโยบายที่ใช้เพื่อป้องกันความปลอดภัย) แล้วให้คลิกที่ปุ่ม Getting Started Wizard



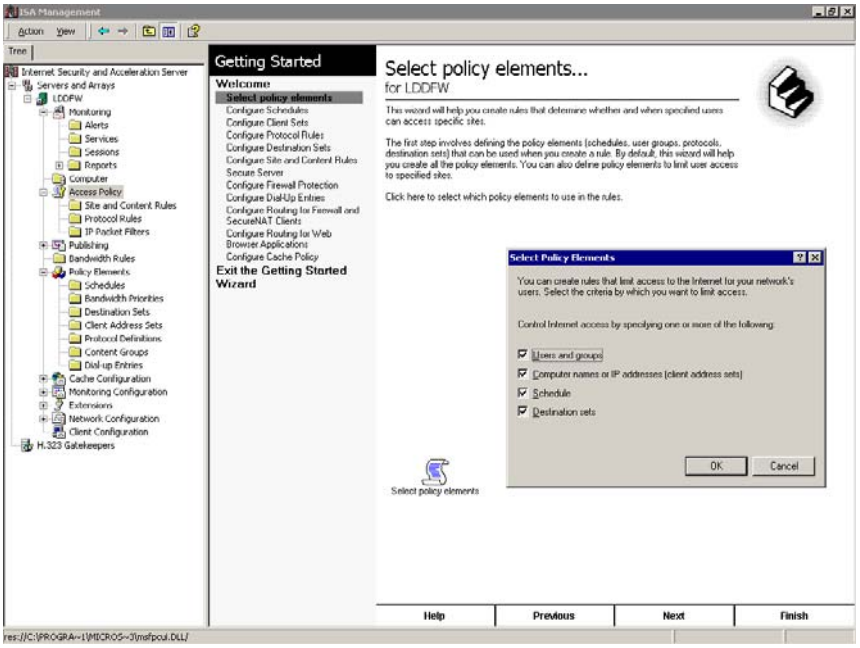
ภาพที่ ๔๕ การใช้งานโปรแกรม ISA

๗) จะปรากฏหน้าต่างโปรแกรมดังรูป



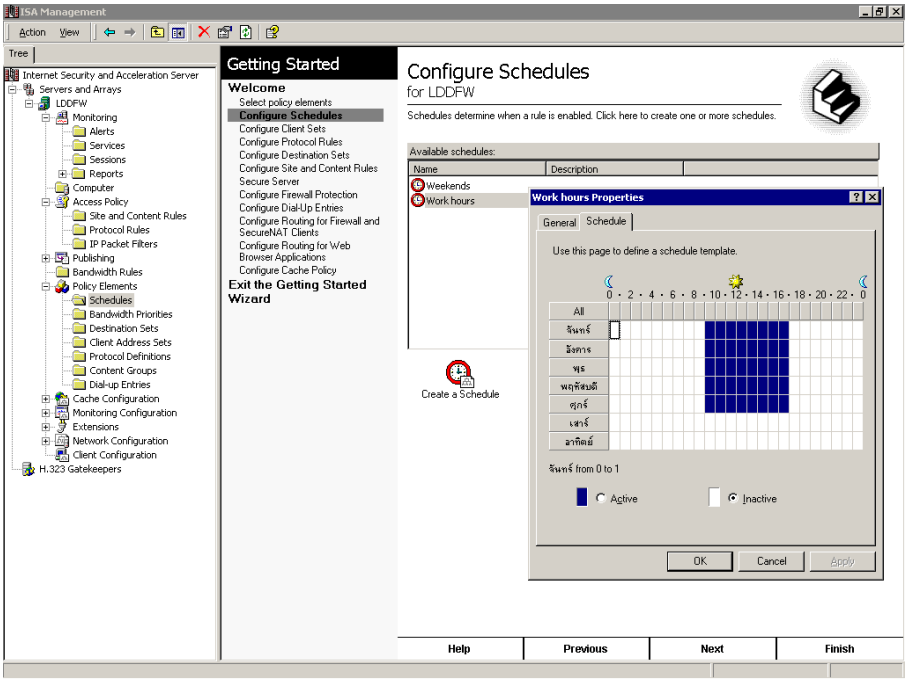
ภาพที่ ๔๖ การใช้งานกำหนดค่าโปรแกรม ISA

๘) ให้คลิกที่ Select policy elements เพื่อคลิกเลือกนโยบายที่ใช้ควบคุมในการ access ข้อมูลใน Internet (ในที่นี้เลือกทุกช่อง แล้วคลิกปุ่ม OK)



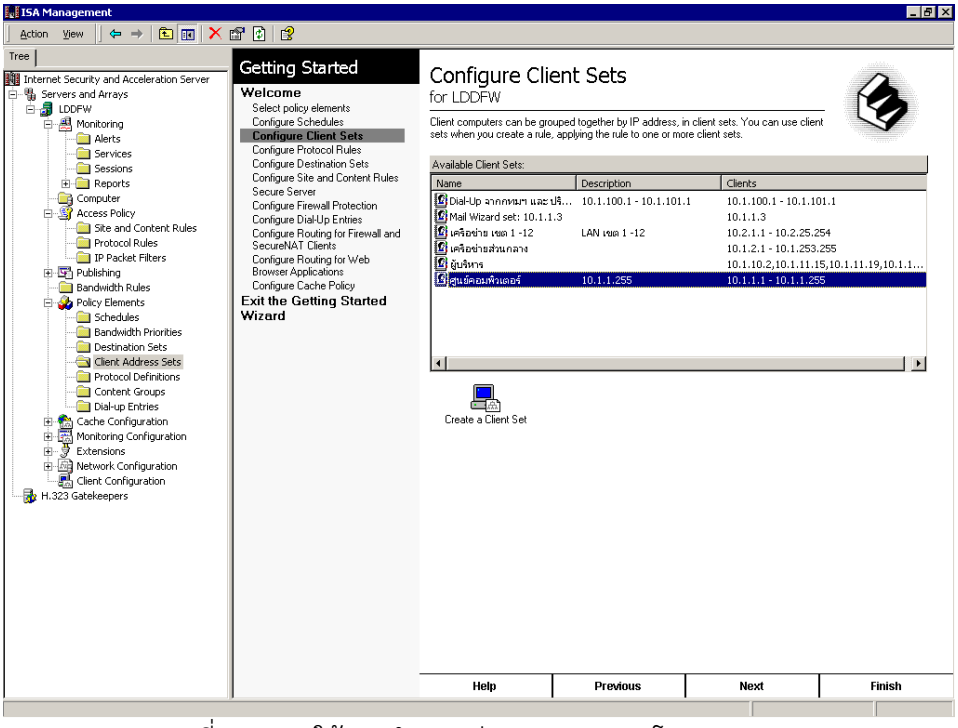
ภาพที่ ๔๗ การใช้งานกำหนดค่า Policy Element โปรแกรม ISA

๙) ให้คลิกที่ Configure Schedulers และที่ work hours คลิกขวาเลือก work hours Properties เพื่อกำหนดตารางเวลาในการทำงานโดยคลิกเลือกเซลล์ในวันและเวลาที่ต้องการ จากนั้นเลือกปุ่มเรดิโอตามเงื่อนไข ซึ่งมี ๒ อย่างคือ เลือก Active เพื่อเพิ่มช่วงวันและเวลานั้นเข้าไปในตารางเวลาใช้งาน หรือ เลือก Inactive เพื่อยกเลือกวันและเวลานั้นในตารางเวลาใช้งาน



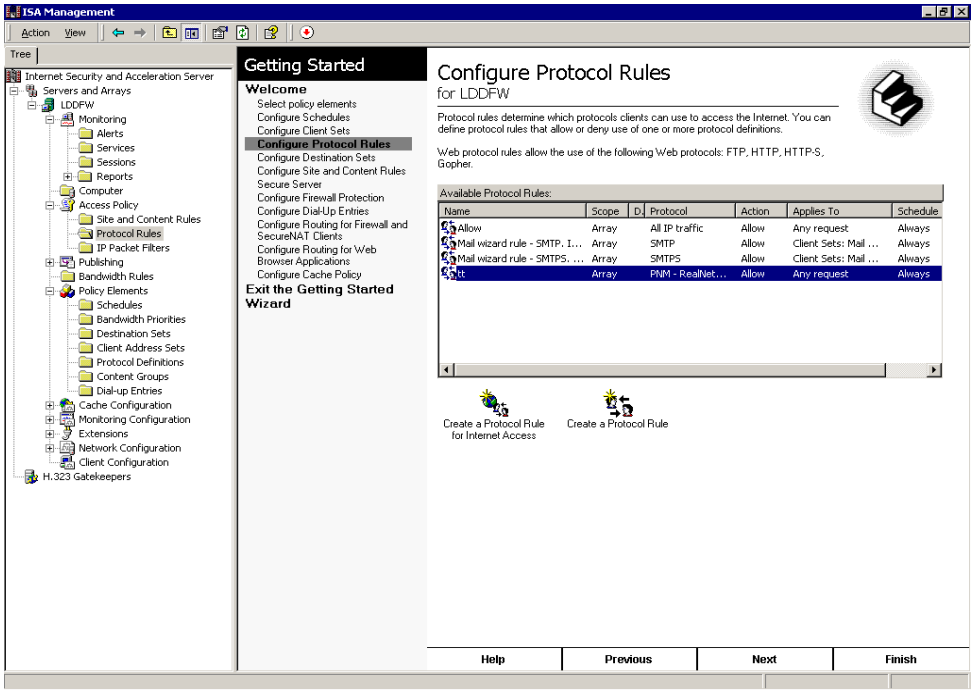
ภาพที่ ๔๘ การใช้งานกำหนดค่า Schedule โปรแกรม ISA

๑๐) ให้คลิกที่ Configure Client Sets เพื่อกำหนดกลุ่มของเครื่องลูกโดยระบุ IP address



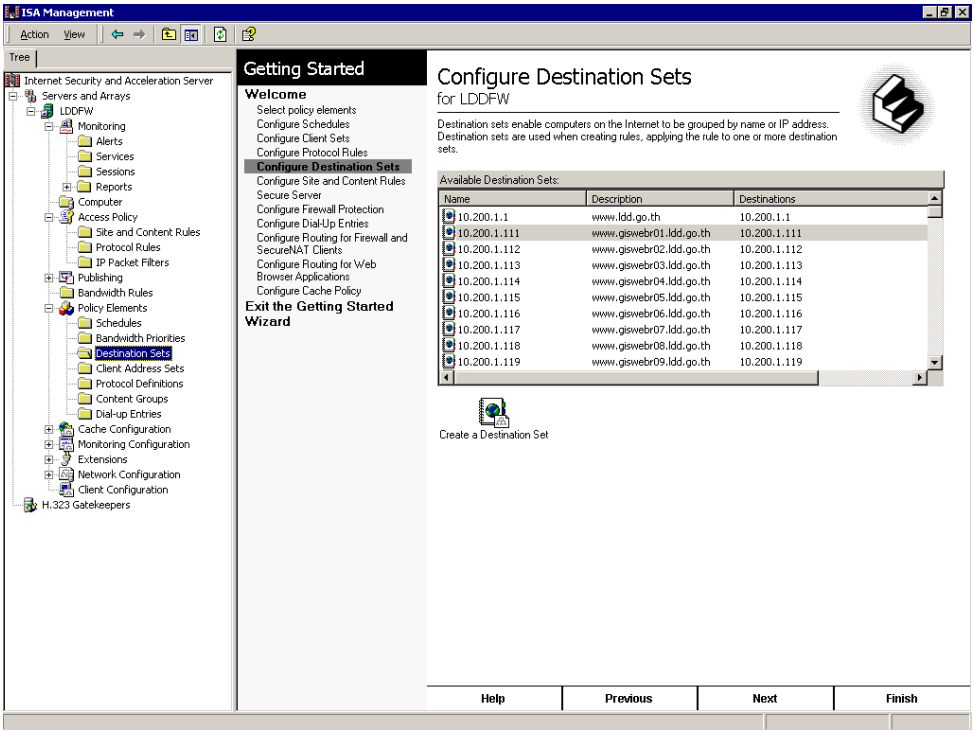
ภาพที่ ๔๙ การใช้งานกำหนดค่า Client Sets โปรแกรม ISA

๑๑) ให้คลิกที่ Configure Protocol Rules เพื่อกำหนดกฎที่อนุญาตให้เครื่องลูกใดบ้างใช้งาน



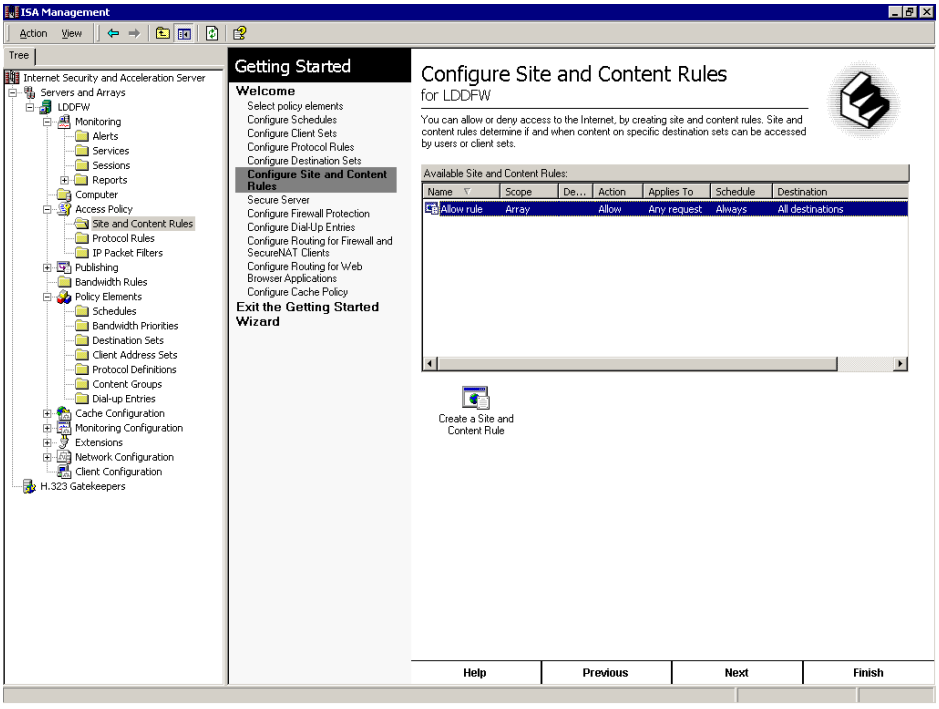
ภาพที่ ๕๐ การใช้งานกำหนดค่า Protocol Rules โปรแกรม ISA

๑๒) ให้คลิกที่ Configure Destination Sets เพื่อกำหนด Destination Sets ที่ต้องการ



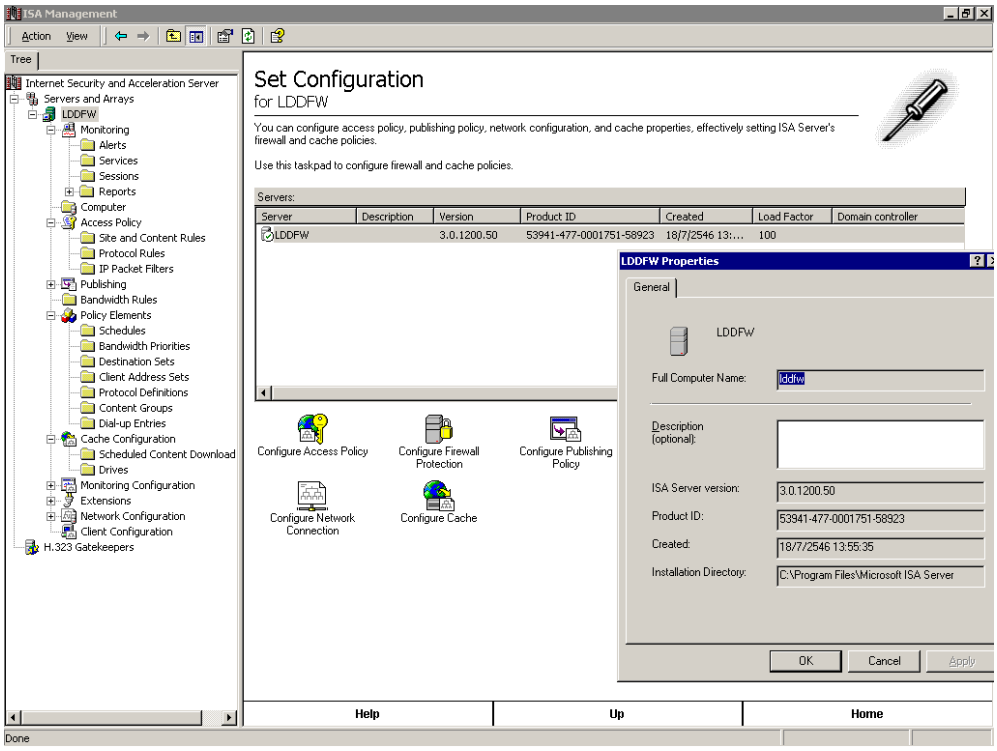
ภาพที่ ๕๑ การใช้งานกำหนดค่า Destination Sets โปรแกรม ISA

๑๓) ให้คลิกที่ Configure Site and Content Rules เพื่อกำหนดกฎที่อนุญาตหรือปฏิเสธให้ใช้งาน Internet



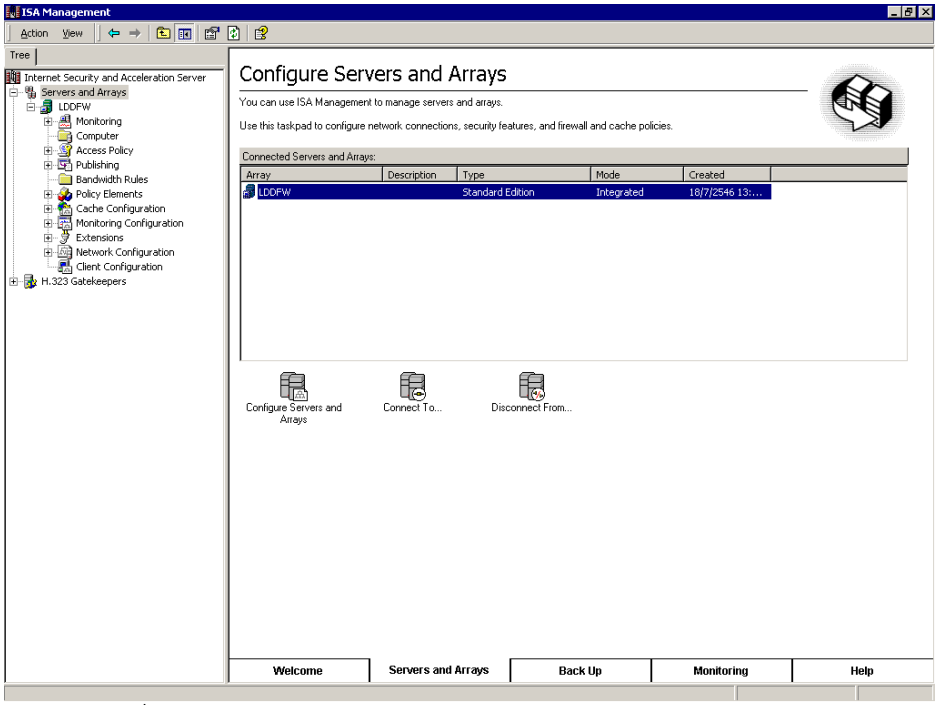
ภาพที่ ๕๒ การใช้งานกำหนดค่า Site and Content Rules โปรแกรม ISA

๑๔) ที่ Set Configuration เพื่อใช้กำหนด access policy, network configuration และ cache properties



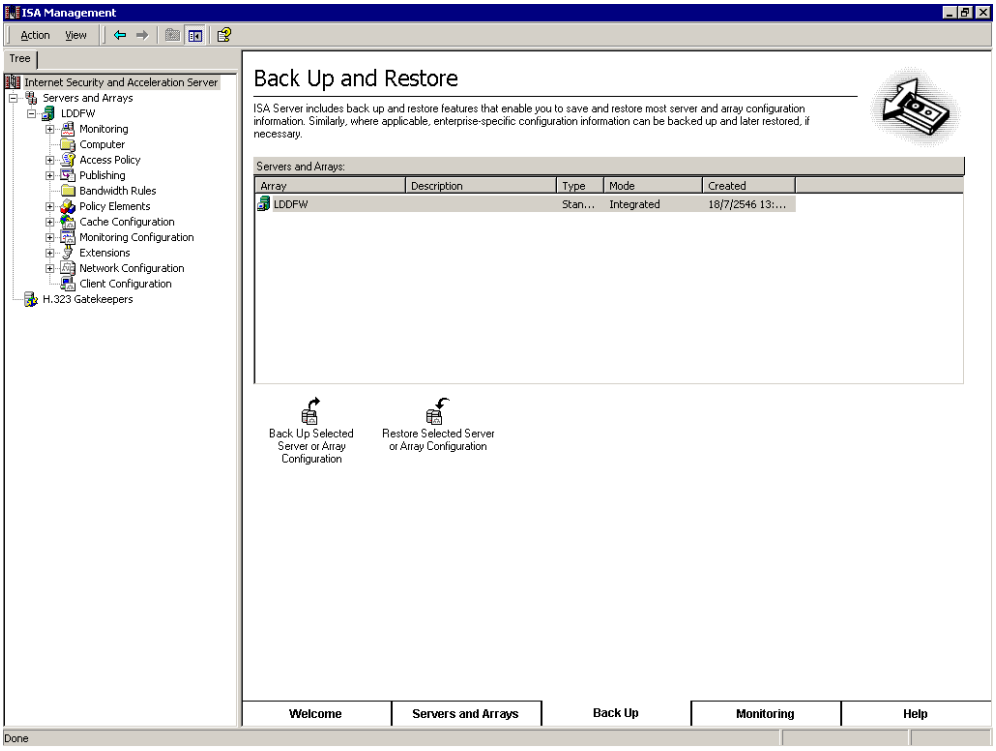
ภาพที่ ๕๓ การใช้งานกำหนดค่า Configuration โปรแกรม ISA

๑๕) คลิกที่ Servers and Arrays เพื่อกำหนดค่า network connection, security และ policy



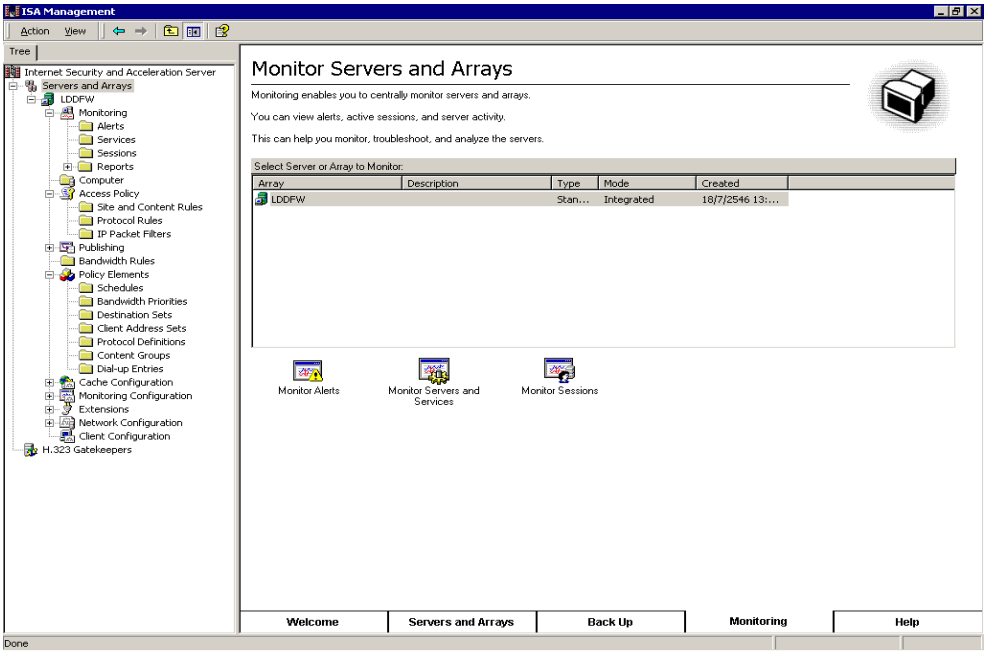
ภาพที่ ๕๔ การใช้งานกำหนดค่า Servers and Arrays โปรแกรม ISA

๑๖) ที่ Internet Security and Acceleration Server ให้คลิกขวาเลือก Back Up and Restore เพื่อใช้กำหนดค่า Configure ของการ Back Up และ Restore



ภาพที่ ๕๕ การใช้งานกำหนดค่าBackup and Restore โปรแกรม ISA

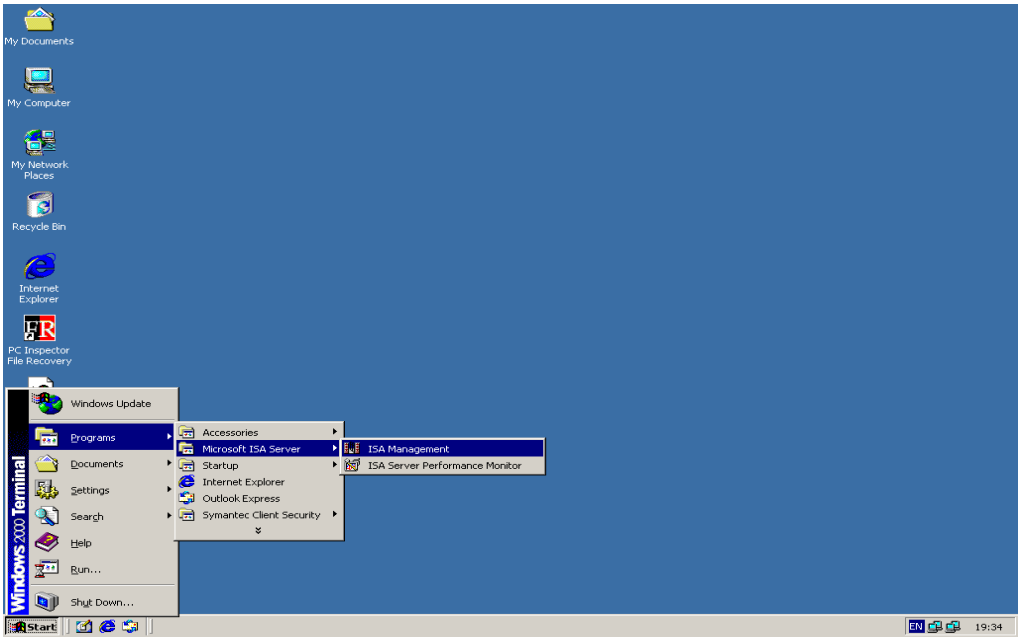
๑๗) ที่ Servers and Arrays คลิกขวาเลือก Monitor Servers and Arrays เพื่อใช้ดูคำเตือน (Alerts) , sessions ที่ทำงานอยู่ซึ่งช่วยในการจัดการและวิเคราะห์การทำงานของ Server



ภาพที่ ๕๖ การใช้งานกำหนดค่า Monitor Servers and Arrays โปรแกรม ISA

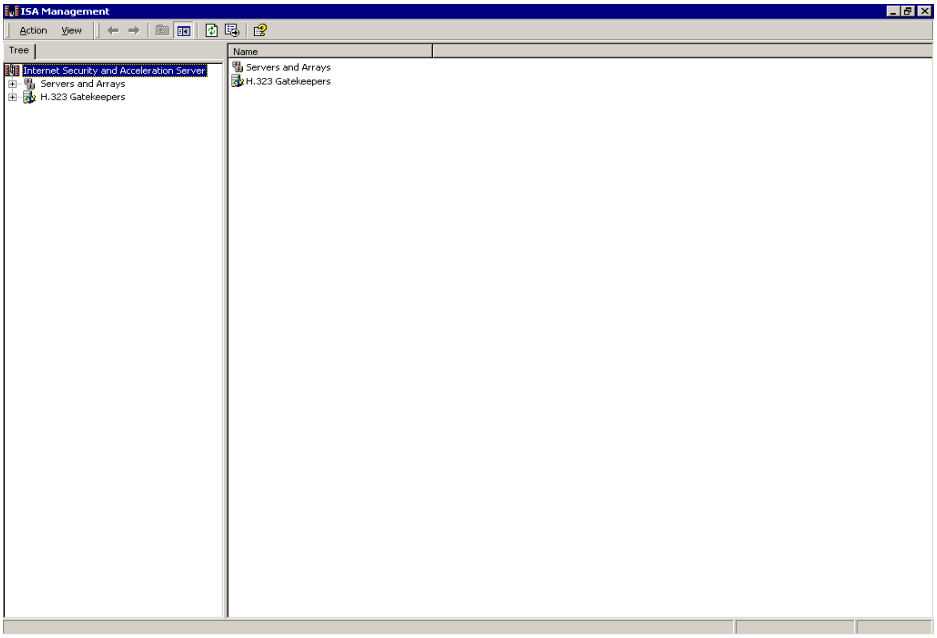
๓.๒.๑.๓ การใช้งานโปรแกรม

๑) เปิดโปรแกรม ISA Server โดยคลิกไปที่ Program > Microsoft ISA Server > ISA Management



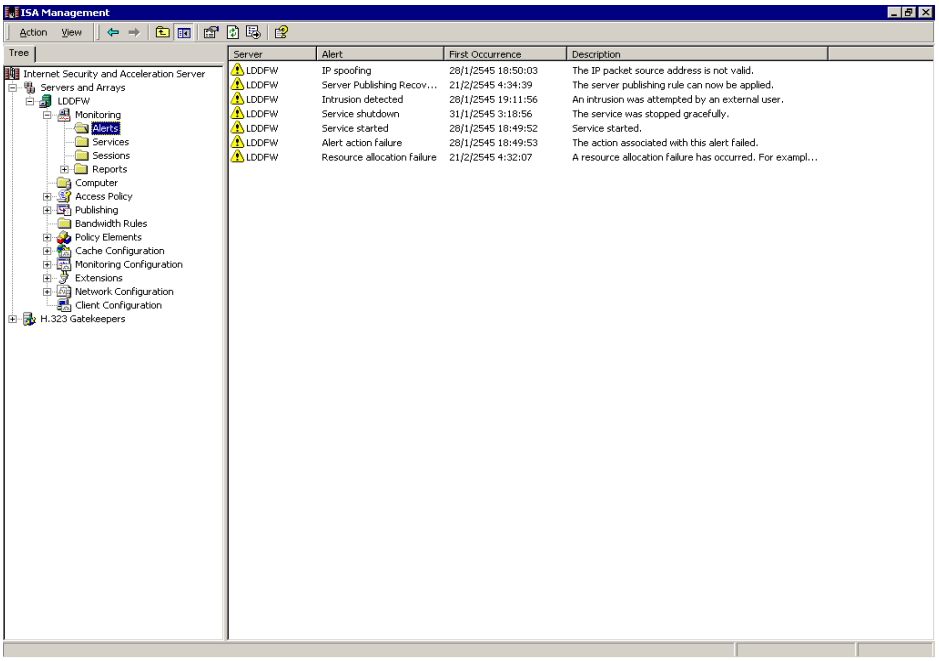
ภาพที่ ๕๗ การเรียกใช้งานโปรแกรม ISA (๑)

๒) เมื่อเปิด ISA Management แล้วจะปรากฏภาพดังรูป ให้คลิกไปที่ Server and Arrays



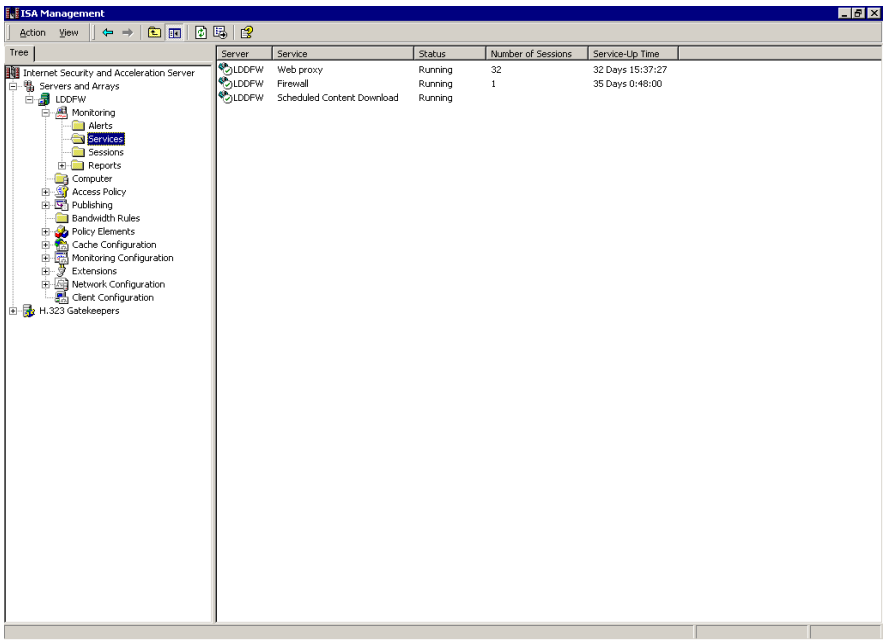
ภาพที่ ๕๘ การเรียกใช้งานโปรแกรม ISA (๒)

๓) แล้วให้คลิกที่ LDDFW > Monitoring > Alerts เพื่อใช้ดูสิ่งที่โปรแกรมเตือนเกี่ยวกับการทำงานต่าง ๆ



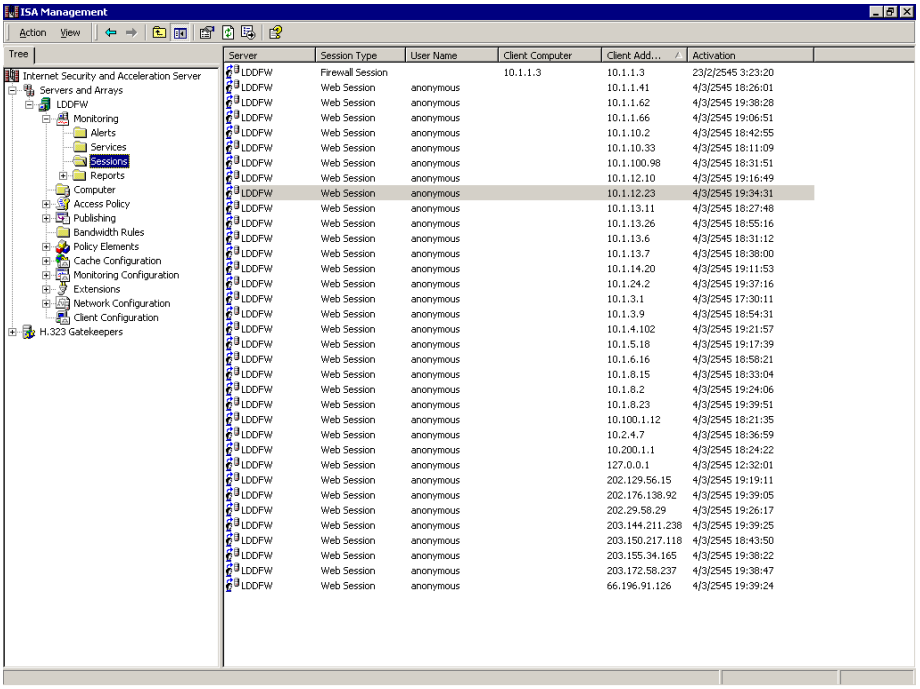
ภาพที่ ๕๙ การเรียกใช้งานโปรแกรม ISA (๓)

๔) คลิกที่ Services เพื่อดูบริการที่มีและ Services ที่ทำงานบ้าง และสามารถสตาร์ทและสต็อปเซอร์วิสต่าง ๆ ได้โดยเลือกที่เซอร์วิสที่ต้องการ แล้วคลิกขวาเลือกป๊อปอัปเมนู Start , Stop หรือ Restart เนื่องจากเซอร์วิส ISA Server Control Service เป็นเซอร์วิสที่เซอร์วิสอื่นๆ ต้องใช้งานด้วย



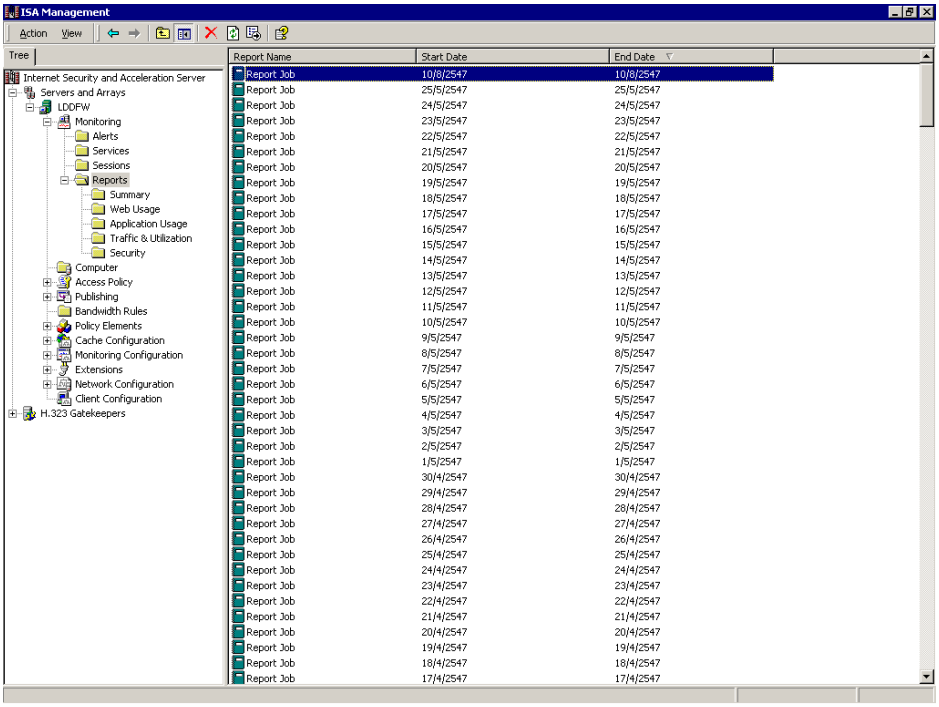
ภาพที่ ๖๐ การเรียกใช้งานโปรแกรม ISA (๔)

๕) คลิกที่ Sessions เพื่อใช้ดู Sessions ใดที่กำลังทำงานอยู่บ้าง



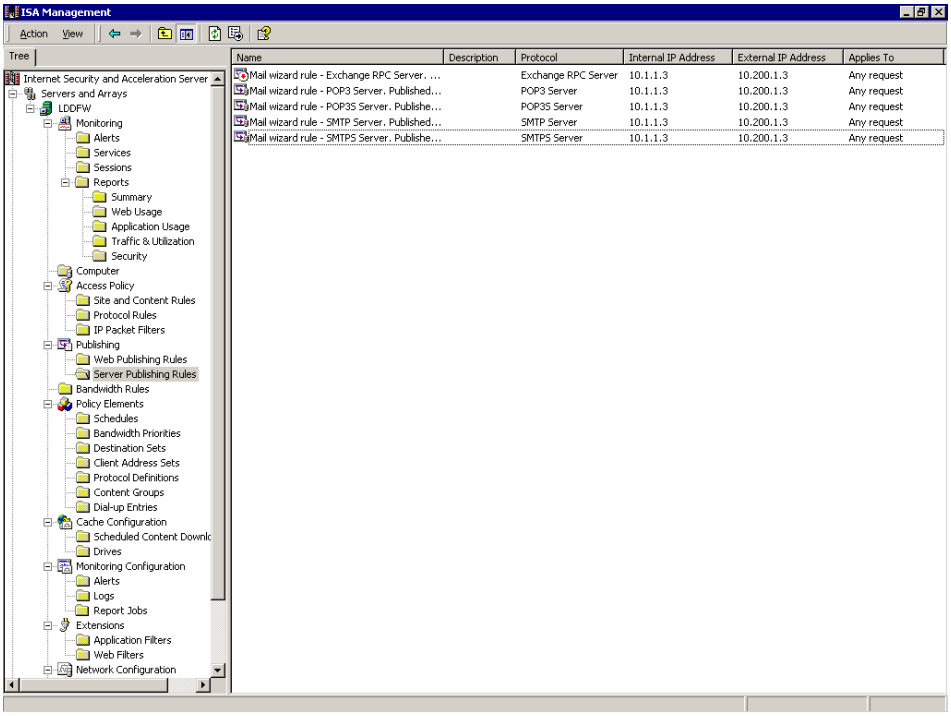
ภาพที่ ๖๑ การเรียกใช้งานโปรแกรม ISA (๕)

๖) คลิกที่ Reports เพื่อดูรายงานที่ต้องการดู โดยใน detail pane ฝั่งขวาเลือก Report Job ที่คุณได้สร้างไว้ก่อนหน้านี้แล้วดับเบิลคลิกหรือคลิกขวาแล้วเลือกป๊อปอัปเมนู Open จะมีรายงานแสดงใน web browser



ภาพที่ ๖๒ การเรียกใช้งานโปรแกรม ISA (๖)

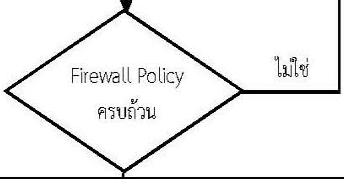
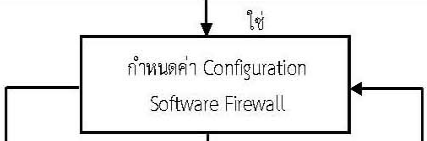
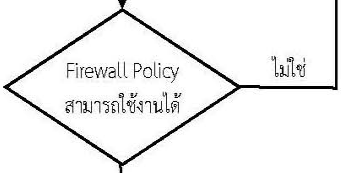
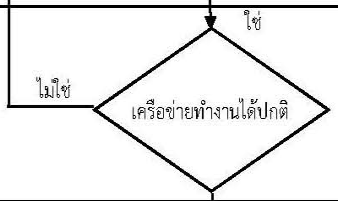
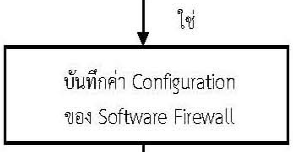
๗) คลิกที่ Server publishing rules เพื่อใช้ดูกฎต่าง ๆ ที่ใช้ในการป้องกันการใช้งาน Internet



ภาพที่ ๖๓ การเรียกใช้งานโปรแกรม ISA (๗)

แผนผังแสดงขั้นตอนและวิธีการปฏิบัติงาน

ระบบ Software Firewall

ลำดับที่	ผังกระบวนการ	รายละเอียดงาน
		
๑		๑. วิเคราะห์การใช้งานเครือข่าย การควบคุมการเรียกใช้งาน Website บริการต่าง ๆ ของกรมพัฒนาที่ดิน การควบคุมการใช้งาน Internet ผ่านทาง Proxy Service และการควบคุมการเชื่อมต่อระหว่างเครือข่ายภายในกับเครื่องแม่ข่ายของกรมพัฒนาที่ดิน เพื่อกำหนด Firewall Policy
๒		๒. ตรวจสอบจำนวน Firewall Policy ว่าครบถ้วนหรือไม่ ถ้ายังไม่ครบให้กลับไปทำขั้นตอนที่ ๑ ถ้าครบแล้วให้ไปทำขั้นตอนที่ ๓
๓		๓. กำหนดค่า Configuration Firewall Policy ลงบนโปรแกรม Software Firewall ที่ติดตั้งอยู่บนเครื่องแม่ข่ายควบคุม
๔		๔. ทดสอบการทำงานของแต่ละ Firewall Policy ที่กำหนดบนอุปกรณ์ว่าสามารถใช้งานได้หรือไม่ ถ้าไม่สามารถใช้งานได้ให้กลับไปทำขั้นตอนที่ ๓ ถ้าใช้งานได้แล้วให้ไปทำขั้นตอนที่ ๕
๕		๕. ทดสอบการทำงานของระบบเครือข่ายของกรมพัฒนาที่ดินเมื่อใช้งานร่วมกับ Firewall Policy ว่าสามารถใช้งานได้ปกติหรือไม่ ถ้าไม่สามารถใช้งานได้ให้กลับไปทำขั้นตอนที่ ๓ ถ้าใช้งานได้แล้วให้ไปทำขั้นตอนที่ ๖
๖		๖. บันทึกค่า Configuration ของการกำหนดโปรแกรม Software Firewall
		

ขั้นตอนการติดตั้งและดำเนินการ

๑) ติดตั้งวินโดว์เซฟเวอร์ ๒๐๐๓ (Windows Server ๒๐๐๓) บนเครื่องคอมพิวเตอร์ควบคุมระบบ

๒) ทำการติดตั้งโปรแกรมไอเอสเอ ๒๐๐๖ (ISA ๒๐๐๖) เมื่อติดตั้งเสร็จให้เริ่มต้นระบบใหม่ Restart เครื่อง

๓) เปิดโปรแกรมไอเอสเอ ๒๐๐๖ (ISA ๒๐๐๖) จากนั้นกำหนดค่าตั้งค่าคอนฟิกกูเรชั่น ตามที่ได้กำหนดไว้

๓.๒.๒ งานด้านการรักษาความปลอดภัยคอมพิวเตอร์ โดยใช้ชุดคำสั่งป้องกันไวรัสในทางคอมพิวเตอร์ (Software Antivirus)

ศูนย์สารสนเทศ กรมพัฒนาที่ดิน นำโปรแกรมป้องกันไวรัสในทางคอมพิวเตอร์ (Antivirus) มาใช้ โดยการติดตั้งบนเครื่องคอมพิวเตอร์ทั้งหมด เพื่อรักษาความปลอดภัยของระบบคอมพิวเตอร์จากการถูกโจมตีโดยไวรัสในทางคอมพิวเตอร์ หรือโปรแกรมประสงค์ร้ายต่างๆ (Malware) โดยเป็นไปตามข้อกำหนดด้านการรักษาความปลอดภัยที่วางไว้ ได้แก่ การป้องกันการติดไวรัสในทางคอมพิวเตอร์ จากไฟล์อันตรายต่างๆ การสแกนตรวจหาไวรัสในทางคอมพิวเตอร์ แบบตลอดเวลา (Real Time) การปรับปรุงฐานข้อมูลไวรัสในทางคอมพิวเตอร์แบบอัตโนมัติ และการป้องกันไวรัสในทางคอมพิวเตอร์ ที่บนเครื่องแม่ข่ายบริการทั้งหมด

โปรแกรมป้องกันไวรัสในทางคอมพิวเตอร์ (Antivirus) ที่นำมาใช้คือโปรแกรมอีเอสอีที เอ็นพอยท์ ซีเคียวริตี้ (ESET Endpoint Security) ซึ่งเป็นผลิตภัณฑ์ป้องกันไวรัสในทางคอมพิวเตอร์ (Antivirus) ของบริษัท ESET ที่ทำงานบนระบบปฏิบัติการ Windows มีความสามารถในด้านการควบคุมการป้องกันไวรัสในทางคอมพิวเตอร์ ทั้งหมด รวมทั้งมีฟังก์ชั่นด้านการป้องกันการบุกรุกจากโปรแกรมที่ไม่ประสงค์ดี (Intrusion Prevent System) การใช้งานแบบกำหนดนโยบาย (Policy Based) และมีความสามารถด้านการทำเป็นแอนตี้ไวรัสเซฟเวอร์ (Antivirus Server) เพื่อให้บริการแอนตี้ไวรัส (Antivirus) ได้

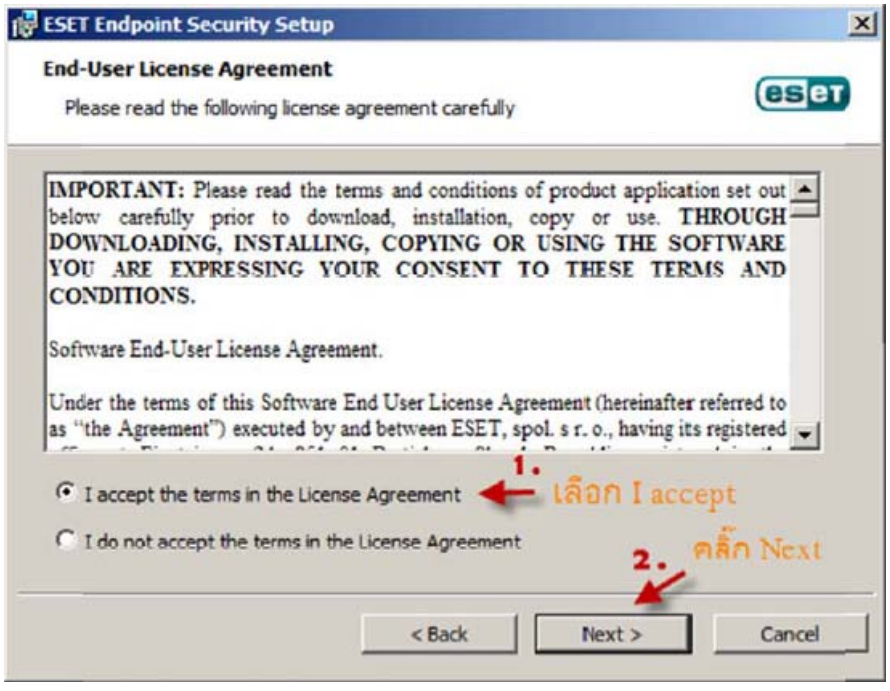
๓.๒.๒.๑ ขั้นตอนการติดตั้งและดำเนินการ

ขั้นตอนในการติดตั้งและดำเนินการโปรแกรมอีเอสอีที เอ็นพอยท์ ซีเคียวริตี้ (ESET Endpoint Security) เพื่อให้โปรแกรมสามารถทำงานบนเครื่องคอมพิวเตอร์ได้ ให้ปฏิบัติตามขั้นตอนดังต่อไปนี้

๑) เปิดโปรแกรมการติดตั้ง จะปรากฏหน้าจอยืนยันการติดตั้ง ให้กด Next

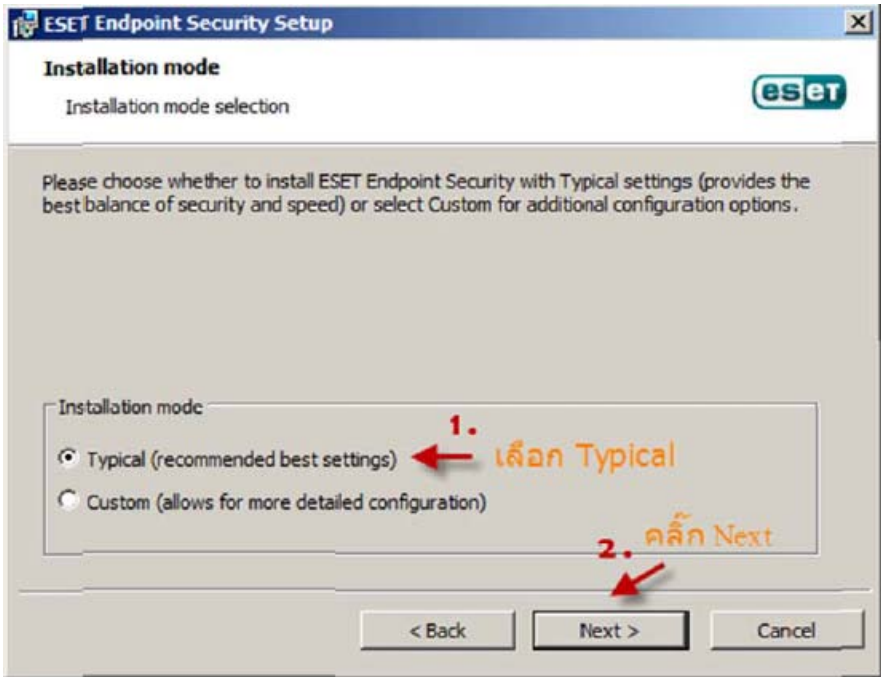
ภาพที่ ๖๔ การติดตั้งโปรแกรม ESET Endpoint Security

๒) หน้าจอแสดงข้อกำหนด ให้ทำเครื่องหมายที่ปุ่ม I Accept จากนั้นกด Next



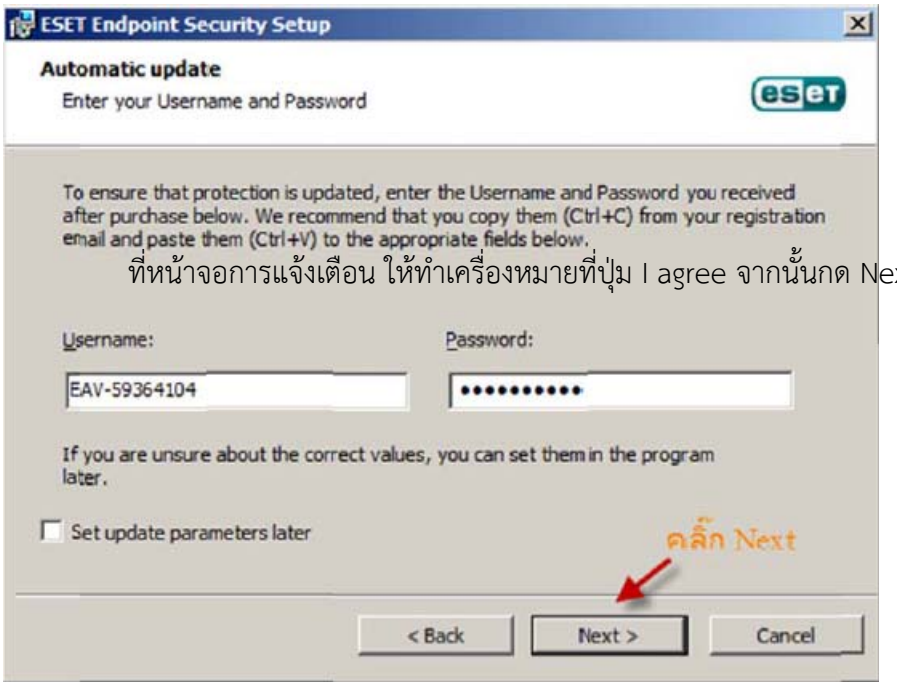
ภาพที่ ๖๕ ข้อกำหนดโปรแกรม ESET Endpoint Security

๓) หน้าจอโหมดการติดตั้ง ให้ทำเครื่องหมายที่ปุ่ม Typical จากนั้นกด Next



ภาพที่ ๖๖ โหมดการติดตั้งโปรแกรม

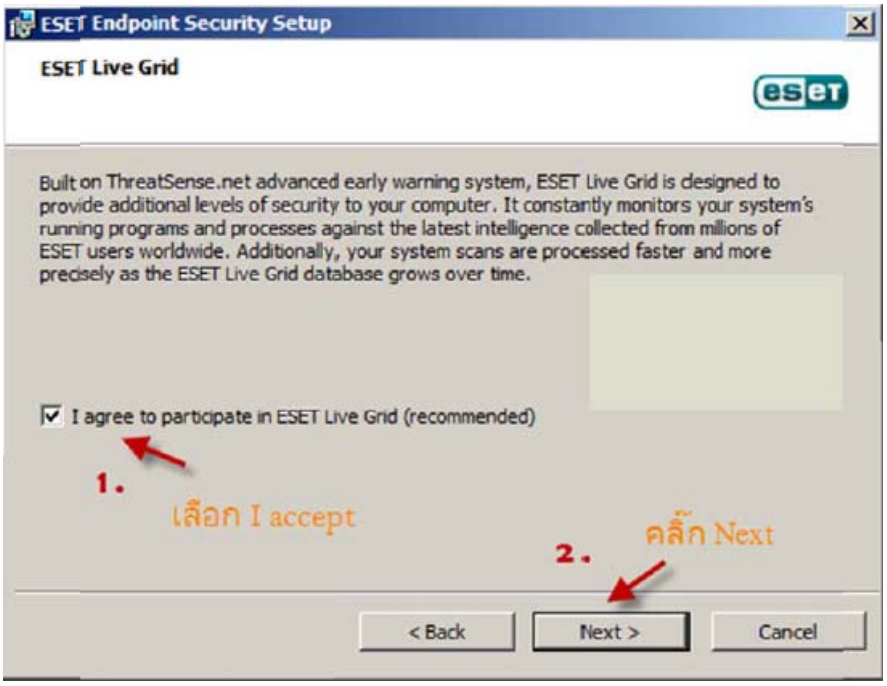
๔) หน้าจอยืนยันสิทธิของโปรแกรม ให้ระบุรหัสผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของกรมพัฒนาที่ดิน จากนั้นกด Next



ที่หน้าจอการแจ้งเตือน ให้ทำเครื่องหมายที่ปุ่ม I agree จากนั้นกด Next

ภาพที่ ๖๗ การยืนยันสิทธิของโปรแกรม

๕) หน้าจอการเชื่อมโยงข้อมูลเชิงวิเคราะห์ที่รวบรวมข้อมูลในการป้องกันไวรัส ให้คลิ๊ก Next

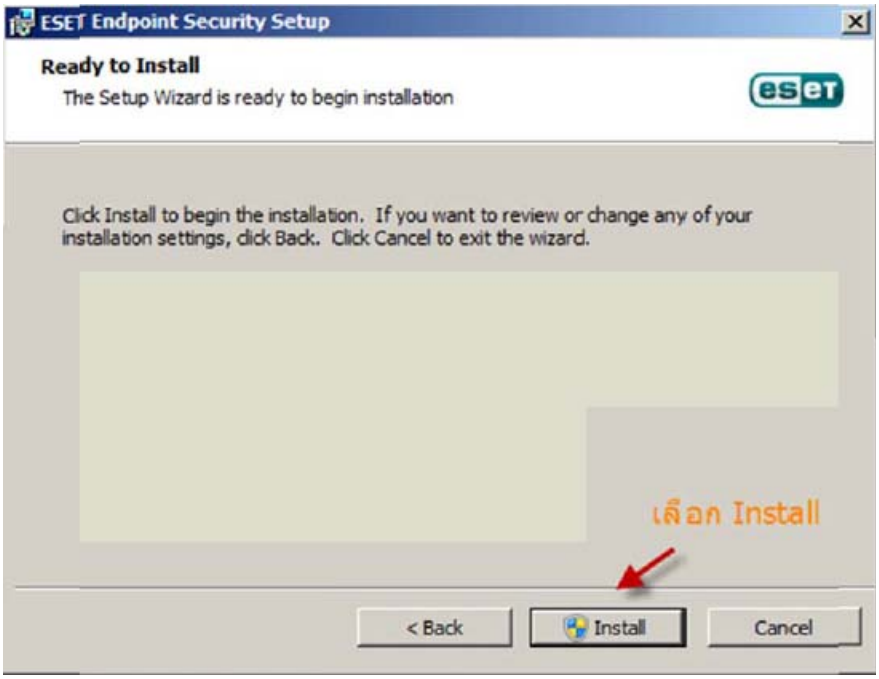


ภาพที่ ๖๘ การเชื่อมโยงข้อมูลเชิงวิเคราะห์ที่รวบรวมข้อมูลในการป้องกันไวรัส

๖) หน้าจอตรวจจับโปรแกรมประสงค์ร้าย ให้เลือกที่ Enable detection จากนั้นกด Next

ภาพที่ ๖๙ การตรวจจับโปรแกรมประสงค์ร้าย

๗) หน้าเตรียมพร้อมในการติดตั้งโปรแกรม ให้คลิ๊ก Install เพื่อติดตั้งโปรแกรม



ภาพที่ ๗๐ การติดตั้งโปรแกรม

๘) เมื่อปรากฏหน้าจอยืนยันการติดตั้งเสร็จสิ้น ให้กดปุ่ม Finish จากนั้นให้เริ่มต้นระบบใหม่ (Restart) เครื่องคอมพิวเตอร์เพื่อให้เซอวิส (Service) ต่างๆของโปรแกรมทำงานได้อย่างสมบูรณ์

ภาพที่ ๗๑ การยืนยันการติดตั้งเสร็จสิ้น

๓.๒.๒.๒ การบริหารจัดการระบบป้องกันไวรัส

๑) ติดตั้งโปรแกรมป้องกันไวรัสบนเครื่องแม่ข่ายบริการทั้งหมด

๒) จัดทำแผน Backup/Recovery พร้อมดำเนินการทดสอบทุกเดือน

๓) ในส่วนของเครื่องแม่ข่ายให้ป้องกันการ Boot จากอุปกรณ์ภายนอกด้วยการ BIOS ให้ Boot จาก Hard disk เป็นอันดับแรกเสมอ

๔) ไม่เปิดโปรแกรม Browser เพื่อเรียกใช้งาน Internet ยกเว้นการเข้า Website ของ Microsoft

๕) ติดตามความเคลื่อนไหว การเตือนภัยและข้อแนะนำต่างๆ อย่างใกล้ชิดจาก Website ป้องกัน Virus

๖) พยายามติดตามความเคลื่อนไหวของการปรับปรุงในส่วนรักษาความปลอดภัยของโปรแกรม ที่ใช้งานผ่านเครือข่าย

๗) สแกนไวรัสอย่างสม่ำเสมอ โดยตั้งค่าให้ทำงานแบบออโตเมติก อย่างน้อยสัปดาห์ละ ๑ ครั้ง

๓.๒.๓ การบริหารจัดการคอมพิวเตอร์ โดยใช้ระบบเครื่องแม่ข่ายเสมือน (Virtual Machine: VM)

๓.๒.๓.๑ การใช้งานระบบ Virtual Machine Server (เครื่องแม่ข่ายเสมือน)

การใช้งานระบบเครื่องแม่ข่ายเสมือน (Virtual Machine (VM)) นั้น ต้องเข้าใจความหมายของคำว่าเวอร์ชวลไลเซชั่น (Virtualization) ซึ่งหมายถึง การจำลองเครื่องเสมือนด้วยซอฟต์แวร์ ที่ทำให้คอมพิวเตอร์หนึ่งเครื่อง สามารถทำงานเป็นเครื่องเสมือนหลายๆ ระบบได้ โดยแต่ละระบบมีทรัพยากรหน่วยความจำ ฮาร์ดดิสก์ และอุปกรณ์เครือข่ายเสมือนที่เป็นอิสระต่อกัน เครื่องเสมือนแต่ละเครื่อง จึงสามารถมีระบบปฏิบัติการและซอฟต์แวร์เป็นของตนเองโดยอิสระ และแต่ละเครื่องทำการคัดลอก (copy) ข้อมูลระบบปฏิบัติการ (operating system) ถูกติดตั้งสู่เครื่องแม่ข่ายเสมือน (Virtual machine) เครื่องแม่ข่ายเสมือน (Virtual Machine) คือระบบปฏิบัติการที่ทำให้สามารถใช้ซอฟต์แวร์เพื่อจำลองการทำงานของคอมพิวเตอร์เครื่องอื่น เสมือนมีคอมพิวเตอร์ ๒ เครื่อง หรือมากกว่านั้น ซ้อนกันอยู่ในคอมพิวเตอร์เพียงเครื่องเดียว ประโยชน์ของการจำลองในลักษณะนี้ เช่น ใช้ในการทดสอบการลงโปรแกรมใหม่ๆ เพราะการทำงานเสมือนเป็นคอมพิวเตอร์อีกตัวหนึ่ง ซึ่งถ้าเกิดความผิดพลาดใดๆ จะไม่มีผลต่อตัวระบบปฏิบัติการคอมพิวเตอร์ระบบหลัก ในภาพรวมของไฮเปอร์ไวเซอร์ (Hypervisor) มีแฟ้มเอกสารหลัก (main file) ดังนี้ Configuration file, Virtual disk file, NVRAM setting fileและLog file

เวอร์ชวลไลเซชั่น (Virtualization) แบ่งออกได้เป็น ๒ ประเภท คือ

๑. โฮส ออฟเปอเรติ่ง ซิสเต็ม เบส Host Operating System-Based

เวอร์ชวลไลเซชั่น (Virtualization) ประเภทนี้ ต้องใช้ระบบปฏิบัติการ (Operating System) ประเภทวินโดว์ (Windows) หรือ (ลีนุกซ์) Linux เพื่อใช้ในการติดตั้งบนเครื่องคอมพิวเตอร์ตัวอย่างเช่น โปรแกรม วีเอ็มแวร์เซฟเวอร์ (VMware Server) โปรแกรมวีเอ็มแวร์เวิคสเตชั่น (VMware Workstation)

๒. เบสเมทเทิลไฮเปอร์ไวเซอร์ Bare-Metal Hypervisor

เบส เมทเทิล ไฮเปอร์ ไวเซอร์ซิสเต็ม (Bare-metal hypervisor system) เป็นระบบ (system) ที่ไม่จำเป็นต้องใช้ระบบปฏิบัติการ (operating system) ในการติดตั้ง เพราะ

ตัวไฮเปอร์ไวเซอร์ (Hypervisor) คือ ระบบปฏิบัติการ (operating system) ด้วยตัวมันเองอยู่แล้ว จึงสามารถใช้งานได้ทันที

ศูนย์สารสนเทศ กรมพัฒนาที่ดิน นำระบบเครื่องแม่ข่ายเสมือน (Virtual Machine: VM) มาใช้แทนเครื่องแม่ข่ายเดิมที่มีอายุการใช้งานมาเป็นเวลานาน และใช้กับเครื่องแม่ข่ายบริการที่ติดตั้งใหม่ เพื่อลดค่าใช้จ่าย โดยการลดจำนวนเซิร์ฟเวอร์ฮาร์ดแวร์ที่ต้องใช้งาน ลดการใช้พลังงานจากการใช้คอมพิวเตอร์หลายๆเครื่อง ลดค่าไฟ ลดค่าบำรุงรักษา ช่วยให้การจัดสรรทรัพยากรภายในเครื่องเป็นไปได้อย่างคุ้มค่า ช่วยให้สามารถประมวลผลหลายๆแพลตฟอร์ม (platform) บนเครื่องเดียวกันได้ และช่วยลดเวลาในการติดตั้งระบบปฏิบัติการและแอบพลิเคชั่น ในการสร้างแม่ข่ายเสมือน (Virtual Machine) โดยการสำเนาหรือโคลน (Clone) จากแม่แบบเครื่อง แม่ข่ายเสมือน (Virtual Machine Template) ระบบเครื่องแม่ข่ายเสมือน (Virtual Machine: VM) ที่นำมาใช้คือโปรแกรม วีเอ็มแวร์ (VMware) ที่สามารถทำงานแบบโฮส ออฟเปอเรติ่ง ซิสเต็มเบส เวอร์ชวลไลเซชั่น (Host Operating System-Based Virtualization) บนระบบปฏิบัติการวินโดว์เซฟเวอร์ (Windows Server) และสามารถทำงานแบบเบสเมทเทิลไฮเปอร์ไวเซอร์ (Bare-Metal Hypervisor) ที่มีระบบปฏิบัติการเป็นของตนเองได้ รวมทั้งมีฟังก์ชั่นช่วยให้การทำงานของเวอร์ชวลเมชชีนเซอวิส (Virtual Machine Service) มีความสะดวกในการติดตั้งและบริหารงาน

๓.๒.๓.๒ คุณสมบัติและประโยชน์ของ Virtual Machines

๑) **Isolation:** ระบบปฏิบัติการ และ ระบบปฏิบัติการหลายๆ ชนิด สามารถทำงานได้อยู่บนคอมพิวเตอร์ เพียงเครื่องเดียว โดยที่แต่ละระบบปฏิบัติการ ทำงานแยกกันอยู่อย่างอิสระ

๒) **Standardization:** ฮาร์ดแวร์ที่แสดงอยู่ใน Virtual Machine นั้นจะถูกแสดงในลักษณะที่มาตรฐาน ซึ่งหมายถึง Virtual Machine ที่ทำงานอยู่นั้น จะมองฮาร์ดแวร์ตัวใดๆ ก็ตามเหมือนกันทั้งหมด ไม่ว่ามันจะแตกต่างกันในเชิงฮาร์ดแวร์จริงเพียงใด

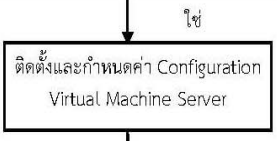
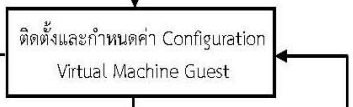
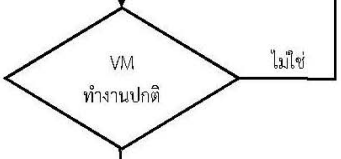
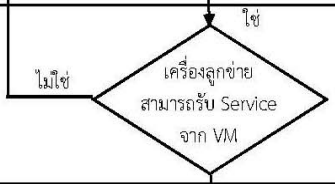
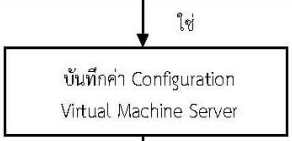
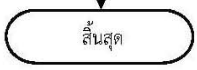
๓) **Consolidation:** หลักการของ Virtual Machines นั้นยังเป็นส่วนหนึ่งของการสนับสนุนการใช้งานที่เรียกว่า consolidation หรือการรวม และขจัดสิ่งที่ไม่จำเป็นออก รวมทั้งการใช้งานฮาร์ดแวร์ให้มีประสิทธิภาพมากยิ่งขึ้น ซึ่งการ consolidation นี้เอง ทำให้การบริการจัดการง่ายขึ้น

๔) **Ease of Testing:** การทำการทดสอบ ไม่ว่าจะเป็นการทดสอบระบบซอฟต์แวร์ใหม่ บนระบบปฏิบัติการที่ต่างกันหรือเหมือนกัน ทำได้ง่ายและไม่กวน production system เลย

๕) **Mobility:** การย้ายตัวระบบปฏิบัติการที่เป็น Virtual Machine นั้นทำได้ง่ายมาก เช่นการย้ายข้ามฮาร์ดแวร์ไปทำงานที่เครื่องอื่น นอกจากนั้น คุณสมบัติการทา snapshot และ rollback ยังเป็นการเพิ่มความสามารถในการกู้ข้อมูล และ เพิ่ม availability โดยรวมให้ระบบ

แผนผังแสดงขั้นตอนและวิธีการปฏิบัติงาน

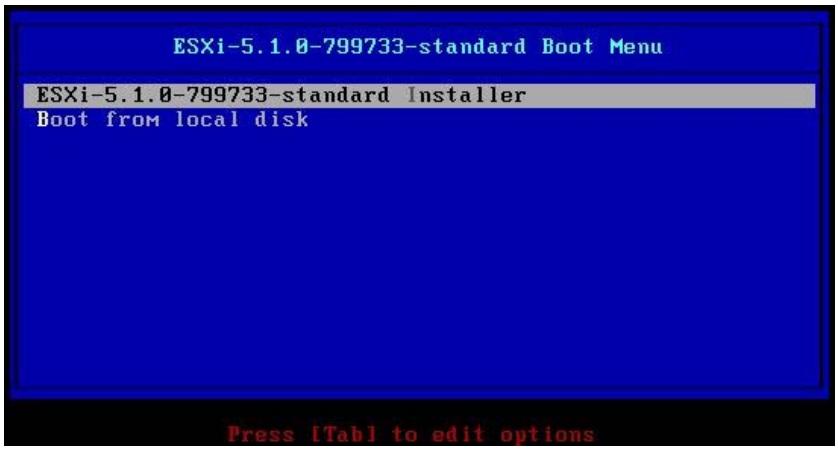
ระบบ Virtual Machine Server (VM)

ลำดับที่	ผังกระบวนการ	รายละเอียดงาน
		
๑		๑. วิเคราะห์คุณสมบัติและจำนวนเครื่องแม่ข่ายบริการของกรมพัฒนาที่ดิน เพื่อกำหนดเครื่องแม่ข่ายเสมือน (Virtual Machine : VM) ทั้งในส่วนของ Server และ Guest ที่นำมาใช้งาน
๒		๒. ตรวจสอบจำนวน VM Server และ Guest ว่าครบถ้วนหรือไม่ ถ้ายังไม่ครบ ให้กลับไปทำขั้นตอนที่ ๑ ถ้าครบแล้วให้ไปทำขั้นตอนที่ ๓
๓		๓. ติดตั้งและกำหนดค่า Configuration Virtual Machine Server
๔		๔. ติดตั้งและกำหนดค่า Configuration Virtual Machine Quest
๕		๕. ทดสอบการทำงานของแต่ละ Virtual Machine Quest ที่ติดตั้งว่าสามารถใช้งานได้หรือไม่ ถ้าไม่สามารถใช้งานได้ให้กลับไปทำขั้นตอนที่ ๔ ถ้าใช้งานได้แล้วให้ไปทำขั้นตอนที่ ๖
๖		๖. ทดสอบการรองรับบริการของเครื่องลูกข่ายเมื่อติดต่อมายังเครื่องแม่ข่ายที่เป็น Virtual Machine Quest ว่าสามารถใช้งานได้ปกติหรือไม่ ถ้าไม่สามารถใช้งานได้ให้กลับไปทำขั้นตอนที่ ๔ ถ้าใช้งานได้แล้วให้ไปทำขั้นตอนที่ ๗
๗		๗. บันทึกค่า Configuration ระบบเครื่องแม่ข่ายเสมือน (Virtual Machine : VM)
		

ขั้นตอนการติดตั้งและดำเนินการ

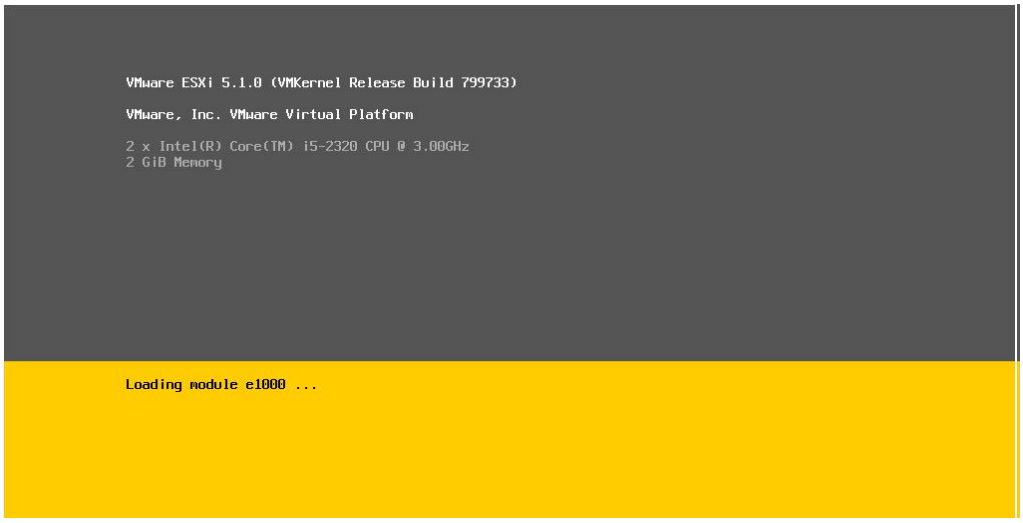
ขั้นตอนในการติดตั้งโปรแกรมวีเอ็มแวร์ (VMware) รุ่น อีเอสเอ็กไอเวอร์ชั่น ๕.๑ (ESXi ๕.๑) บนเครื่องคอมพิวเตอร์ควบคุมระบบ สามารถดำเนินการตามขั้นตอนดังต่อไปนี้

๑) ใส่แผ่นติดตั้งโปรแกรมพร้อมตั้งค่าบูตแผ่นซีดีที่เครื่องคอมพิวเตอร์ควบคุมระบบ จะขึ้นหน้าจออีเอสเอ็กไอบูทเมนู (ESXi Boot Menu) ให้เลือกข้อแรก สำหรับการติดตั้งอีเอสเอ็กไอ (EXSi)



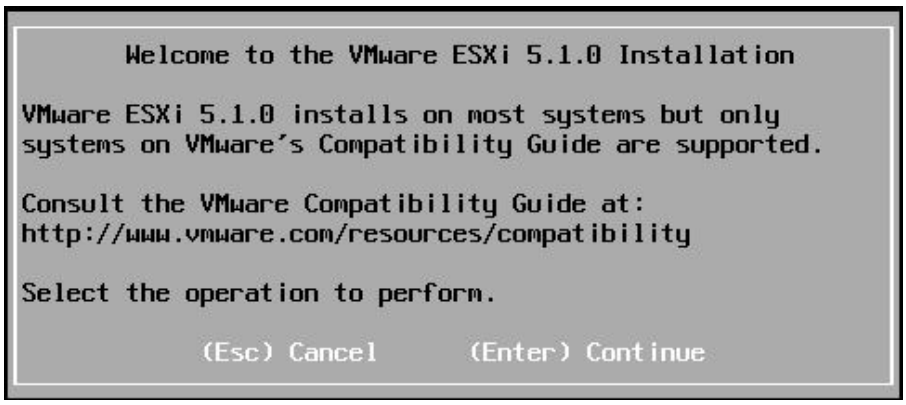
ภาพที่ ๗๒ การติดตั้งโปรแกรมวีเอ็มแวร์ (VMware)

๒) โปรแกรมจะแสดงรายละเอียดของเวอร์ชั่นของโปรแกรม รายละเอียดของเครื่องแม่ข่ายที่จะติดตั้ง พร้อมโหลดค่าโมดูลต่างๆที่จะต้องใช้ในการติดตั้ง



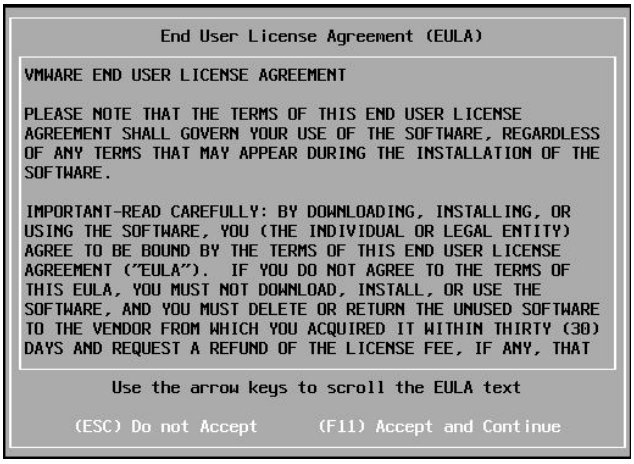
ภาพที่ ๗๓ หน้าจอแสดงรายละเอียดของเวอร์ชั่นของโปรแกรม

๓) เข้าสู่หน้าจอต้อนรับสู่การติดตั้ง วีเอ็มแวร์ (VMware) เวอร์ชั่นอีเอสเอ็กไอ ESXi เลือก (Enter) Continue



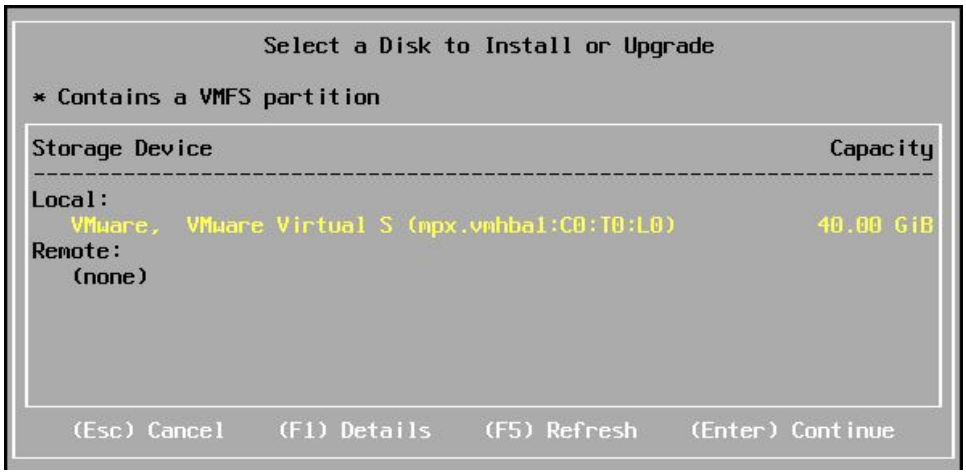
ภาพที่ ๗๔ หน้าจอต้อนรับสู่การติดตั้ง วีเอ็มแวร์ (VMware)

๔) แสดงรายละเอียดข้อตกลงต่างๆของโปรแกรม เลือก (F11) Accept and continue



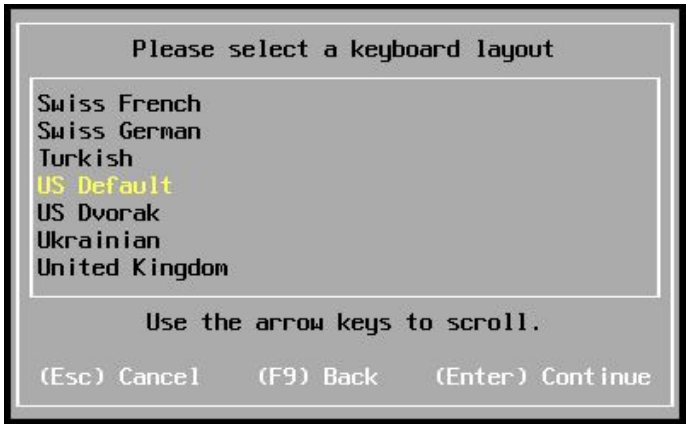
ภาพที่ ๗๕ หน้าจอแสดงรายละเอียดข้อตกลงต่างๆของโปรแกรม

๕) เลือกฮาร์ดดิสที่จะใช้ในการติดตั้ง โดยโปรแกรมจะแสดงชื่อและขนาดของฮาร์ดดิสก์ เลือก (Enter)



ภาพที่ ๗๖ หน้าจอแสดงแสดงชื่อและขนาดของฮาร์ดดิสก์

๖) เลือกรูปแบบของคีย์บอร์ด (Keyboard) ที่จะใช้งาน เลือก (Enter) Continue

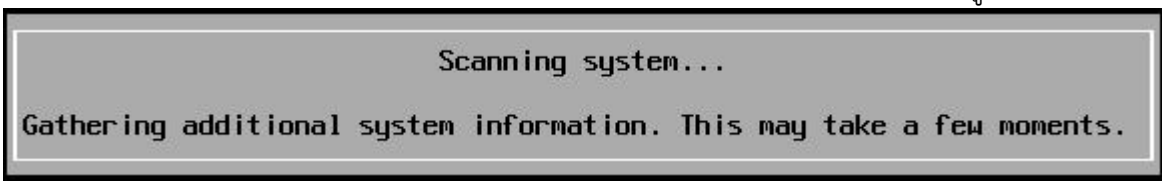


ภาพที่ ๗๗ รูปแบบของคีย์บอร์ด (Keyboard) ที่จะใช้งาน

๗) กำหนดรหัสผ่านของ Root เสร็จแล้ว เลือก (Enter) Continue

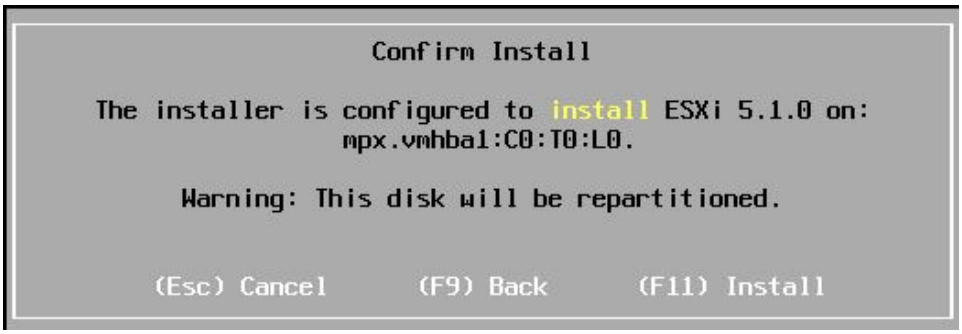
ภาพที่ ๗๘ การกำหนดรหัสผ่านของ Root

๘) โปรแกรมเริ่มทำการสแกนไฟล์ระบบที่จะใช้ในการติดตั้ง ใช้เวลาสักครู่



ภาพที่ ๗๙ โปรแกรมเริ่มทำการสแกนไฟล์ระบบที่จะใช้ในการติดตั้ง

๙) หลังจากนั้นโปรแกรมจะขึ้นหน้าต่างยืนยันการติดตั้ง หากต้องการติดตั้งจริงให้เลือก (F11) install

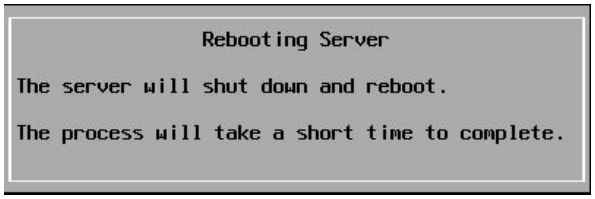


ภาพที่ ๘๐ หน้าต่างยืนยันการติดตั้ง

๑๐) เริ่มการติดตั้ง ใช้เวลาพอประมาณ และหลังจากติดตั้งเสร็จแล้ว จะขึ้นหน้าให้เริ่มต้นระบบใหม่ (Restart) ระบบ ๑ ครั้ง เลือก (Enter) Reboot

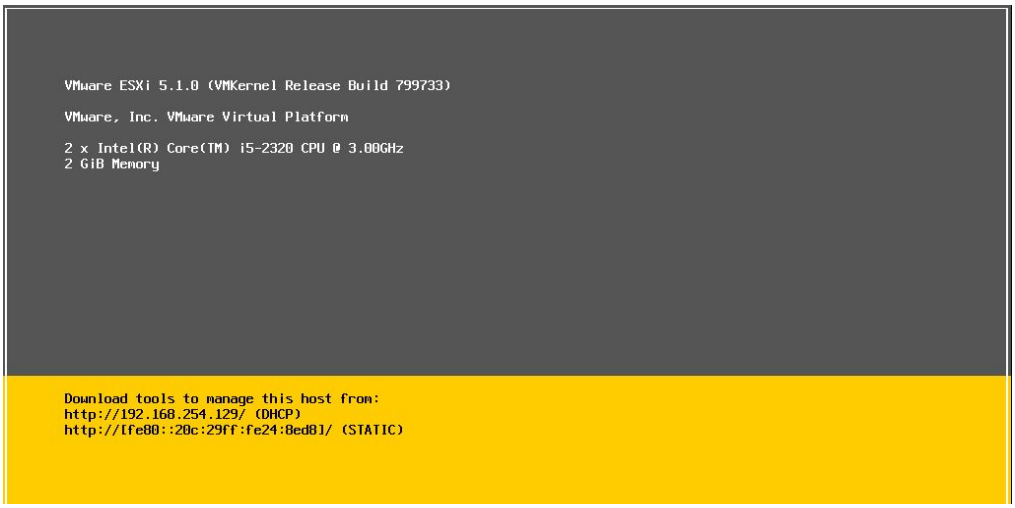
ภาพที่ ๘๑ หน้าจอแสดงสถานะเริ่มการติดตั้ง

๑๑) เครื่องแม่ข่ายเริ่มเริ่มต้นระบบใหม่ (Reboot)



ภาพที่ ๘๒ เครื่องแม่ข่ายเริ่มเริ่มต้นระบบใหม่ (Reboot)

๑๒) หลังจากรีสตาร์ทแล้ว โปรแกรมจะแสดงรายละเอียดของระบบพร้อมทั้งลิงค์ยูอาร์แอล (URL) ที่ใช้ดาวน์โหลดโปรแกรมวีสเฟียร์ ไคลเอนต์ (VSphere Client)

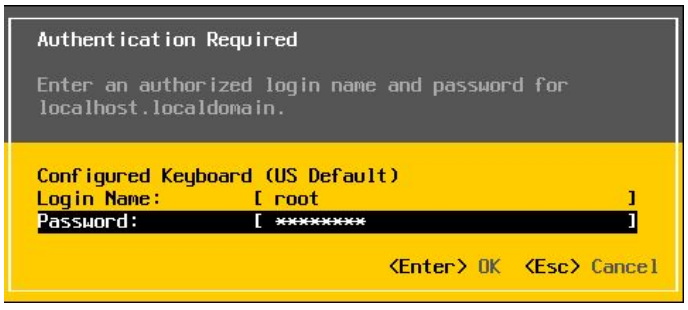


ภาพที่ ๘๓ โปรแกรมจะแสดงรายละเอียดของระบบ

๑๓) หากผู้ใช้งานต้องการที่จะเข้าไปตั้งค่าไอพีใหม่ หรือตั้งค่าอื่นๆ โปรแกรมจะแสดงฟังค์ชั่นที่ใช้ในการตั้งค่าดังภาพ สามารถกดปุ่ม (F2) Customize System ได้

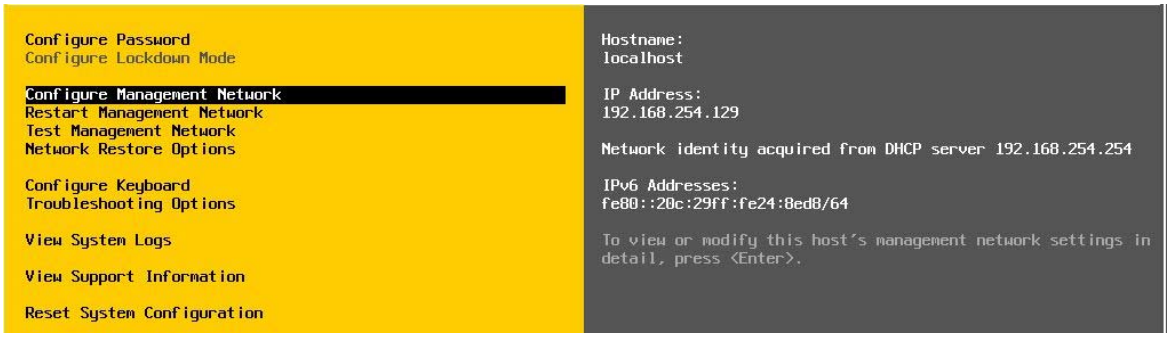
ภาพที่ ๘๔ โปรแกรมแสดงฟังค์ชั่นที่ใช้ในการตั้งค่า

๑๔) โปรแกรมจะแสดงช่องใส่รหัสผ่านที่ได้กำหนดไว้ตอนต้นของการติดตั้ง โดยค่าเริ่มต้น (Default) ของ ชื่อลงบันทึกเข้า (login Name) คือ root และใส่รหัสผ่านเรียบร้อยแล้ว เลือก <Enter> OK



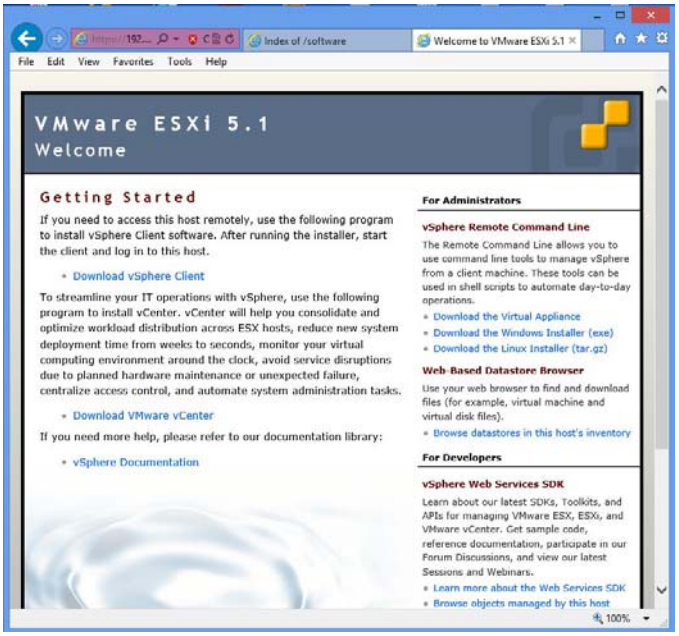
ภาพที่ ๘๕ โปรแกรมแสดงช่องใส่รหัสผ่าน

๑๕) แสดงหน้าการตั้งค่าแต่ละประเภท ผู้ใช้งานสามารถเลือกการตั้งค่าต่างๆได้ตามต้องการ



ภาพที่ ๘๖ แสดงหน้าการตั้งค่าแต่ละประเภท

๑๖) หลังจากตั้งค่าเรียบร้อยแล้ว ให้ไปยังเครื่องคอมพิวเตอร์ สำหรับใช้ในการติดตั้งโปรแกรมวีสเฟียร์ VSphere เปิดเบราว์เซอร์ (Browser) แล้วพิมพ์ยูอาร์แอล (Uniform Resource Locator (URL)) ของเครื่องแม่ข่ายที่ได้กำหนดค่าไว้ แล้วจะขึ้นหน้าต่างดังภาพคลิก Download vSphere client คลิกเพื่อบรรจุลง (Download) และติดตั้งลงเครื่องให้เรียบร้อย

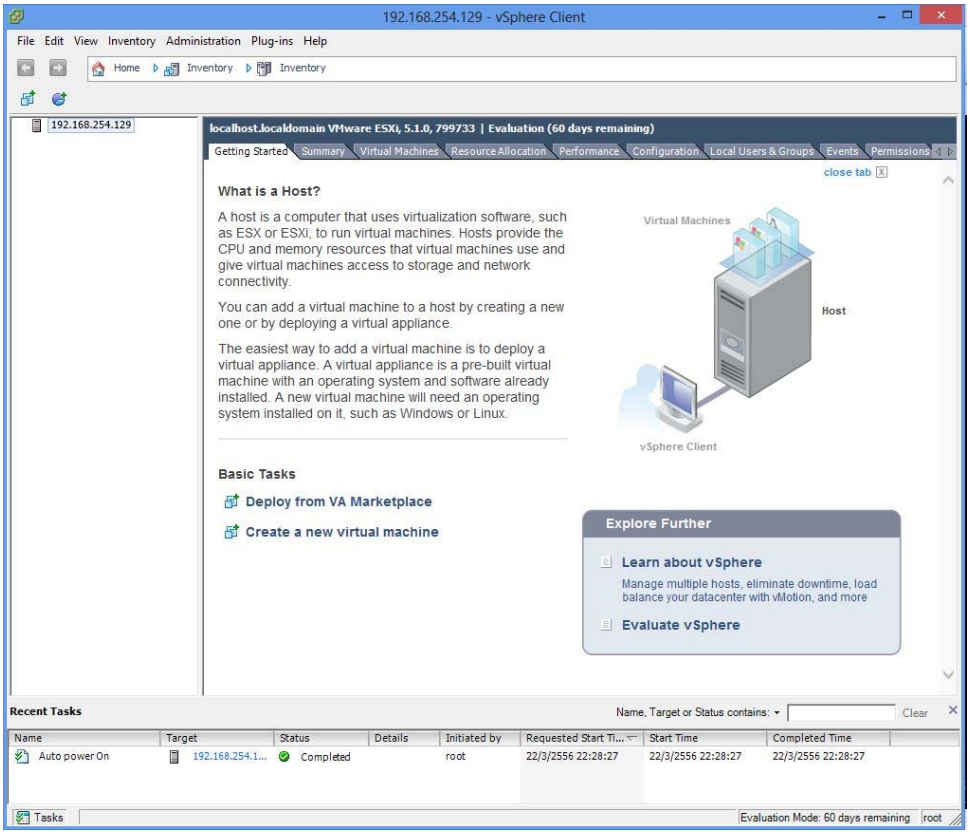


ภาพที่ ๘๗ หน้าต่างแสดงการ Download vSphere client

๑๗) หลังจากติดตั้งแล้วจะขึ้นหน้าดังภาพ เพื่อเข้าใช้ในการสร้างเครื่องแม่ข่ายเสมือน (Guest OS) ต่อไป

ภาพที่ ๘๘ แสดงหน้าจอเครื่องแม่ข่ายเสมือน (Guest OS)

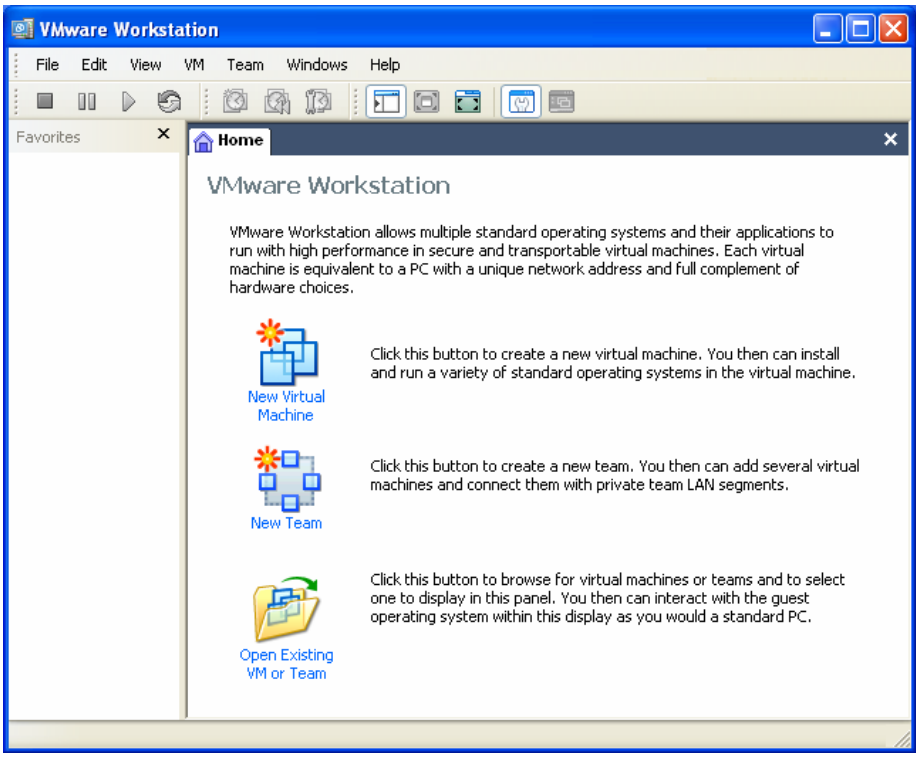
๑๘) แสดงหน้าต่างของโปรแกรมอีเอสเอ็กไอ(EXSi) ผ่านวีสเฟียร์ ไคลเอนต์ (vSphere Client)



ภาพที่ ๘๙ แสดงหน้าต่างโปรแกรมอีเอสเอ็กไอ(EXSi) ผ่านวีสเฟียร์ ไคลเอนต์ (vSphere Client)

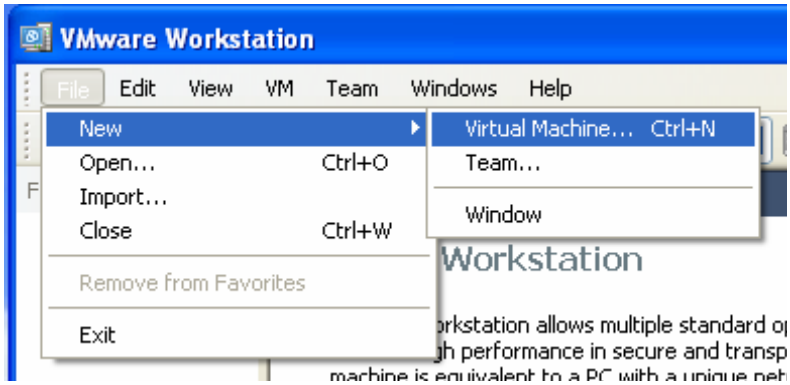
๓.๒.๓.๓ ตัวอย่างการกำหนดค่าสำหรับ Virtual Machines VMware

๑) เมื่อลงโปรแกรมและเปิดการใช้งานก็จะปรากฏโปรแกรมดังภาพที่ ๖๔

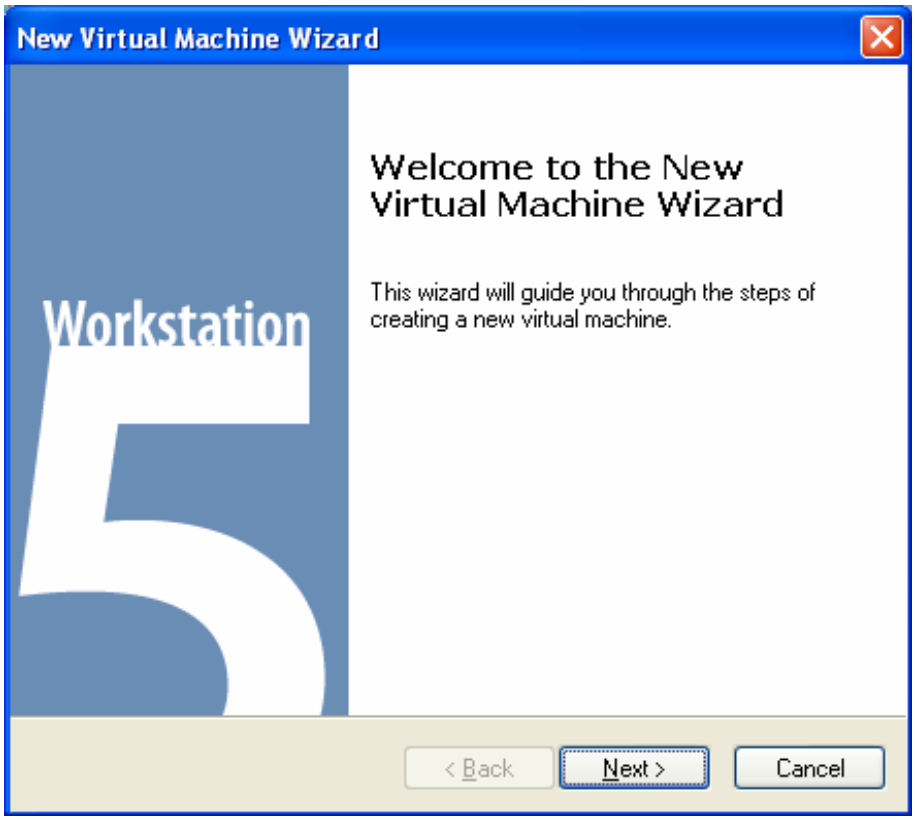


ภาพที่ ๙๐ หน้าต่างของโปรแกรม VMware

๒) เมื่อลงโปรแกรมเสร็จแล้วให้สร้าง VM โดยเลือกที่ Menu File > New > Virtual Machine ตามภาพที่ ๓ -๖๔ แล้วจะได้หน้าต่าง Welcome ตามภาพที่ ๓ -๖๕

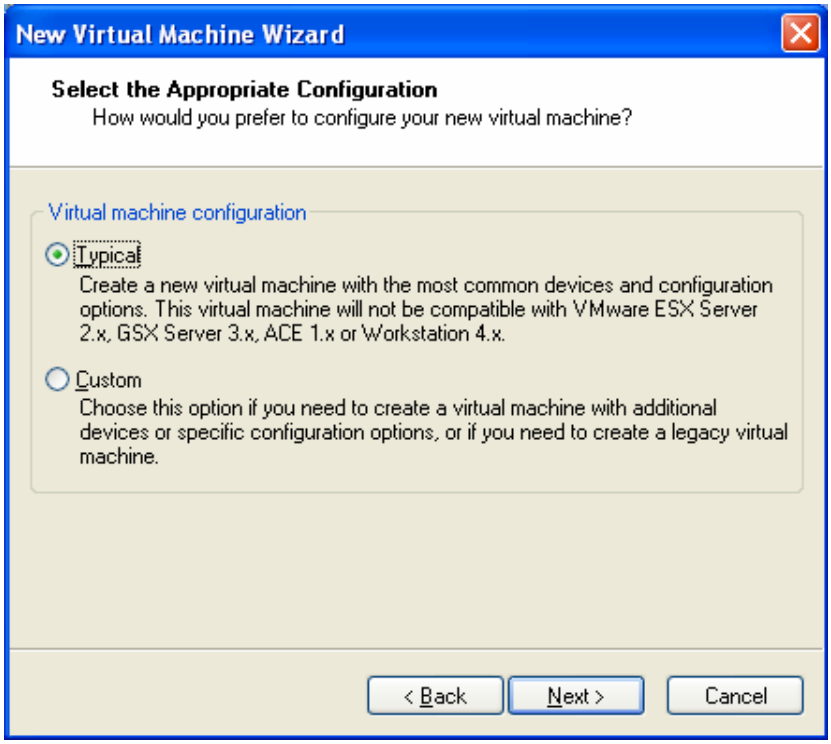


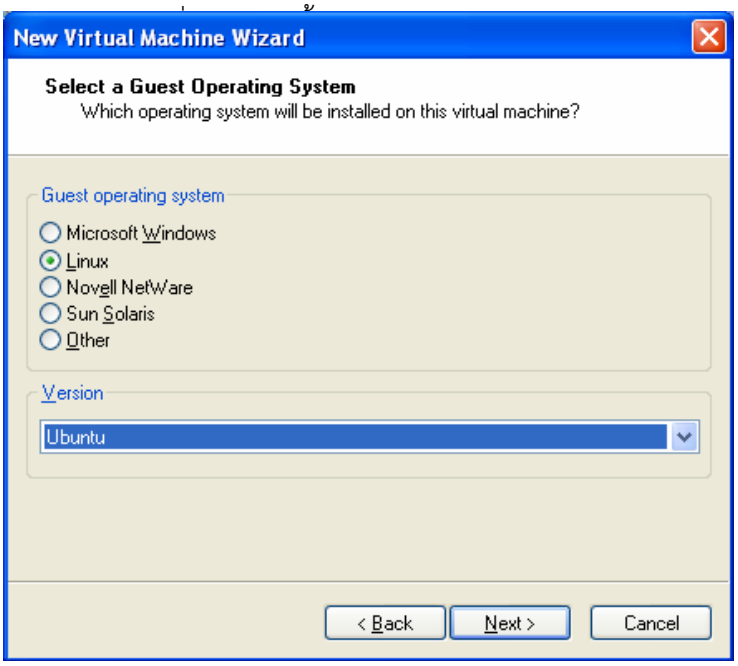
ภาพที่ ๙๑ การสร้าง Virtual Machine ใหม่



ภาพที่ ๙๒ หน้าต่าง Welcome Windows

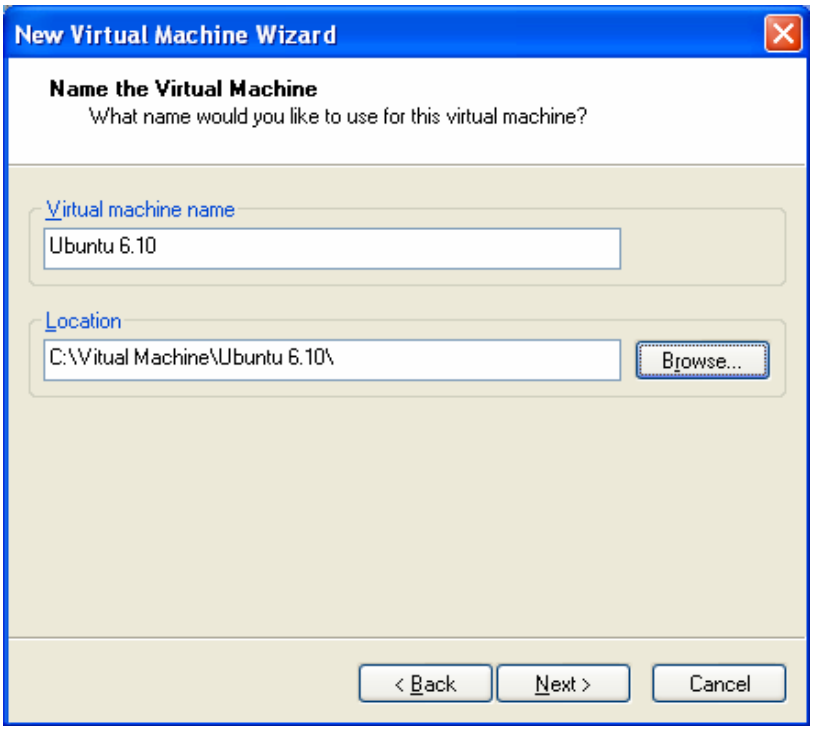
๓) เมื่อเข้ามาที่หน้าต่าง Welcome Windows กด Next เข้าหน้าต่าง Appropriate Configuration จากนั้นกด Next

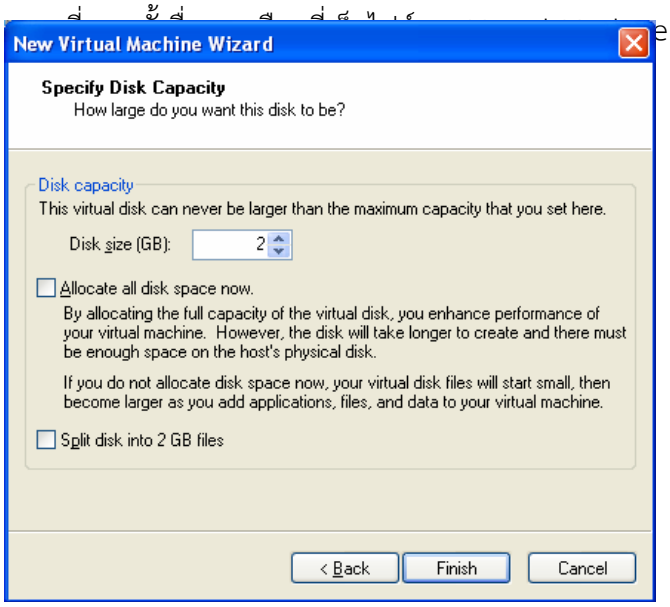




ภาพที่ ๙๔ การเลือก Guest Operating System หรือ OS ที่ต้องการลง

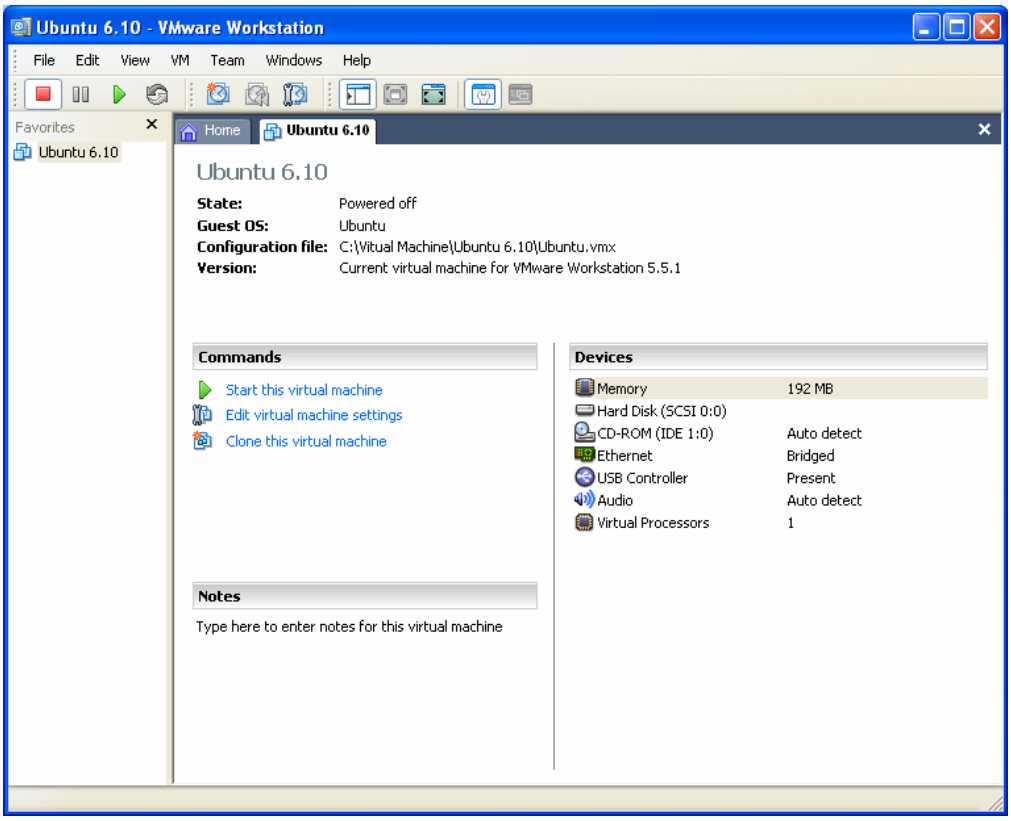
๔) ขั้นตอนนี้เป็นการเลือก OS ที่ต้องการสร้างเป็น VM ภายในเครื่อง ซึ่งจะทดสอบการลงเป็น Ubuntu ๖.๑ เมื่อเลือกเสร็จแล้วก็ต้องตั้งชื่อให้กับ Virtual Machine ที่จะสร้างและเลือกที่เก็บไฟล์ของ VM โดย Default จะเก็บอยู่ที่ C:\Documents and Settings\xxx\My Documents\My Virtual Machines แต่อันนี้จะเลือกเก็บไว้ที่อื่นตามภาพที่ ๖๙ กด next ต่อไปก็จะเป็นการกำหนดค่าของ Disk ที่ต้องการให้ VM ใช้โดย Default จะเป็น ๘ GB แต่จะกำหนดให้เป็น ๒ GB ตามขนาดการใช้งาน ตามภาพที่ ๗๐



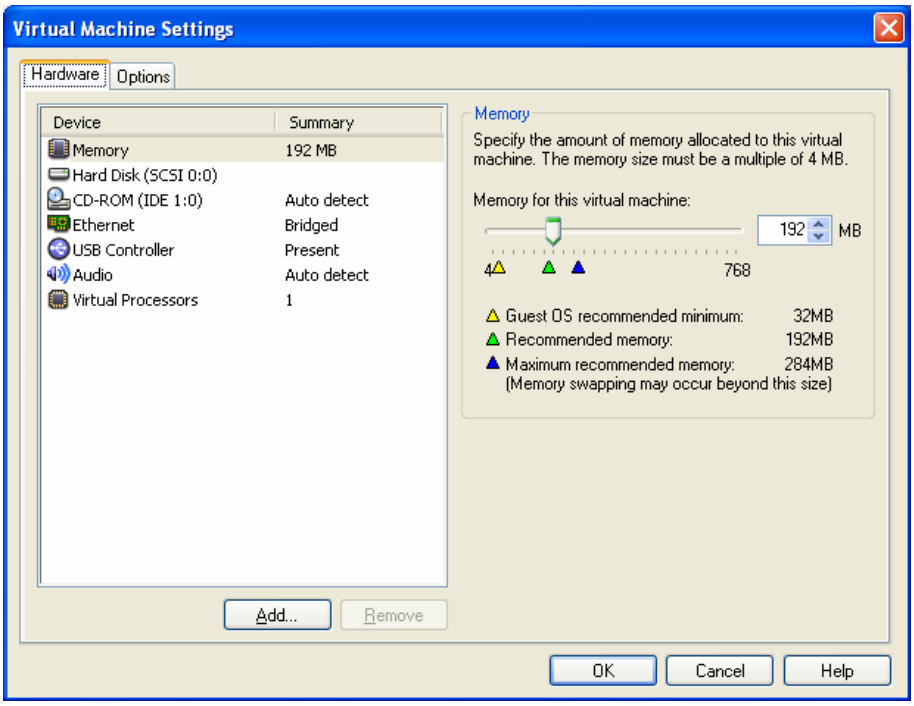


ภาพที่ ๙๖ การกำหนดค่าของ Disk ที่ต้องการใช้เป็น Virtual Machine

๕) เมื่อตั้งค่าเบื้องต้นเสร็จแล้วก็จะกลับมาที่ Menu ตามเดิมดังภาพที่ ๑๐ สามารถตั้งค่าเพิ่มเติมได้โดยการเลือกไปที่ Edit virtual machine setting ก็จะเข้าสู่หน้าต่าง Virtual Machine Settings ดังภาพที่ ๗๑



ภาพที่ ๙๗ หน้าจอ Menu หลังจากที่สร้าง VM เสร็จแล้ว

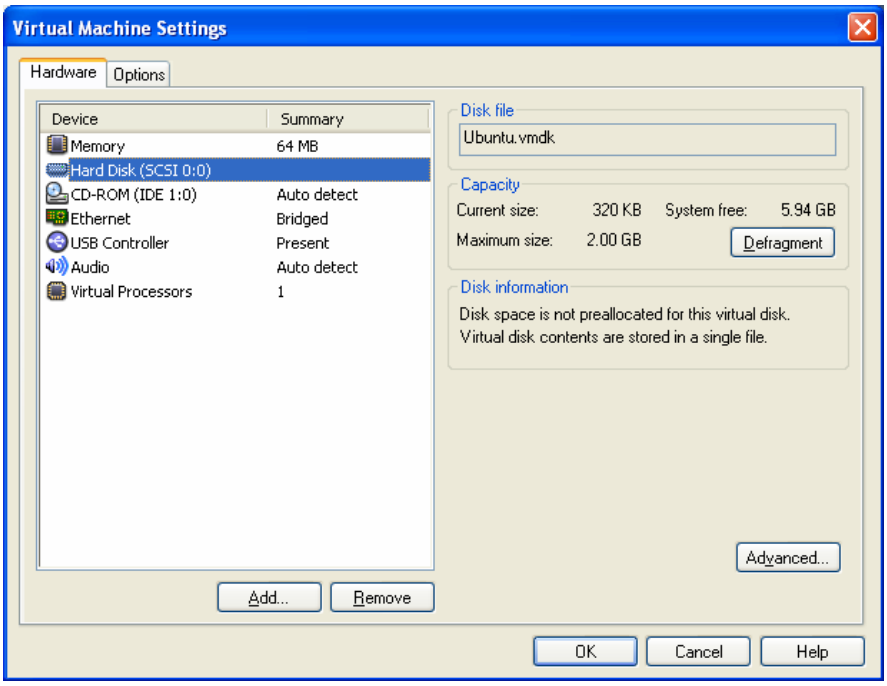


ภาพที่ ๙๘ หน้าต่าง Edit virtual machine setting

๖) ที่หน้าต่างของ Edit virtual machine setting เราจะพบว่าอุปกรณ์ที่ต้องการแก้ไขจะเป็นรายชื่ออยู่ทางซ้ายมือและค่าที่สามารถปรับเปลี่ยนได้จะอยู่ทางขวามือ โดยเราสามารถปรับเปลี่ยนฮาร์ดแวร์ของ VM ได้ ๗ อย่างคือ

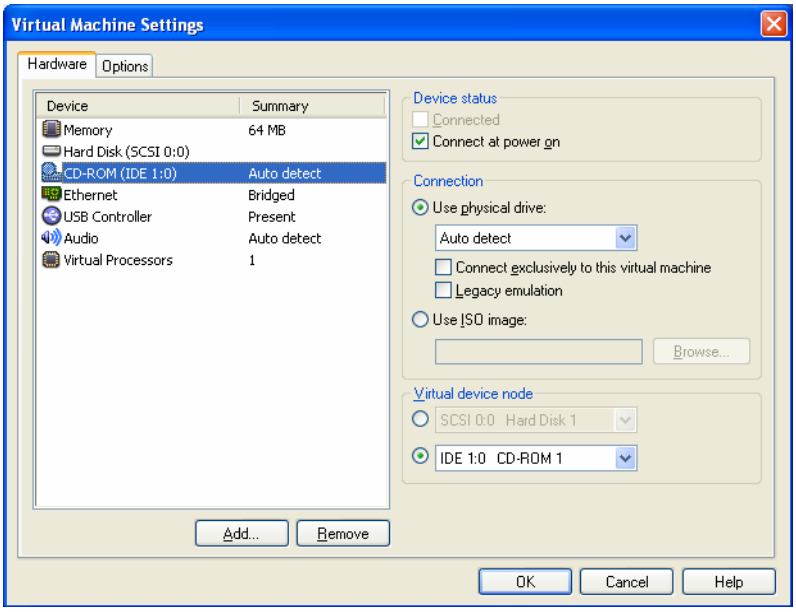
๑ Memory = RAM ที่ Host ต้องการแบ่งให้ VM ใช้

๒ Hard Disk = เป็นการแบ่ง Hard Disk ของเครื่องไปเป็น Disk ของ VM



ภาพที่ ๙๙ หน้าต่าง Setting ในส่วนของ Hard Disk

๗) CD Rom = CD Rom ของ VM เพื่อให้ VM สามารถใช้งาน CD Rom ที่อยู่ที่เครื่องที่ (Host)



ภาพที่ ๑๐๐ หน้าต่าง Setting ในส่วนของ CD-ROM

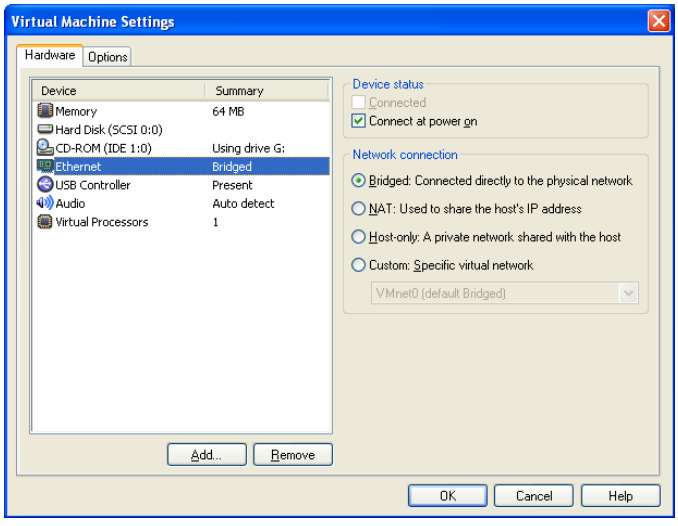
๘) Ethernet = LAN card ของ VM เป็นการกำหนดรูปแบบการต่อระบบ Network ดังต่อไปนี้

(๑) Bridged เป็นการต่อ LAN card ของ VM ออกไปที่ LAN card ของเครื่องHostโดย ip ของ VM ที่ใช้งานจะเป็นคนละ ip กับเครื่องHost และสามารถทำให้เครื่องคอมเครื่องอื่นที่อยู่ใน Network สามารถติดต่อกับ VM เครื่องนี้ได้

(๒) NAT คล้ายกับการต่อแบบ Bridge แต่ ip ของ VM ที่ต่อออกไปที่ด้านนอกเครื่องคอมพิวเตอร์คอมเครื่องอื่นจะมองเป็น ip เดียวกับเครื่องHost

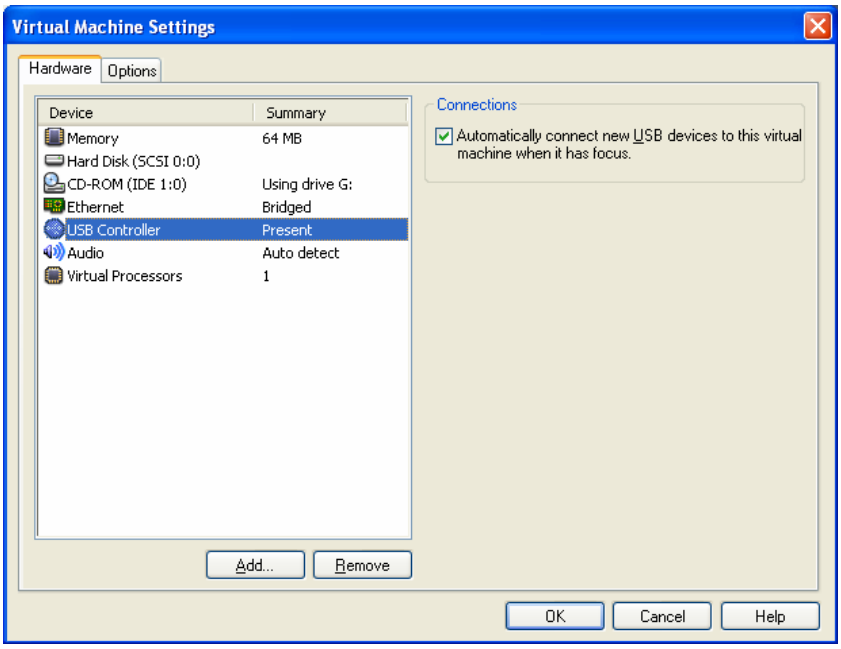
(๓) Host-only เป็นการต่อใช้งานเฉพาะ VM กับเครื่องHost เท่านั้น

(๔) Custom เป็นการเลือกการเชื่อมต่อกับระบบ Network ภายนอกในกรณีที่มีการใช้งาน LAN card ของทั้ง VM และเครื่องHostหลาย card



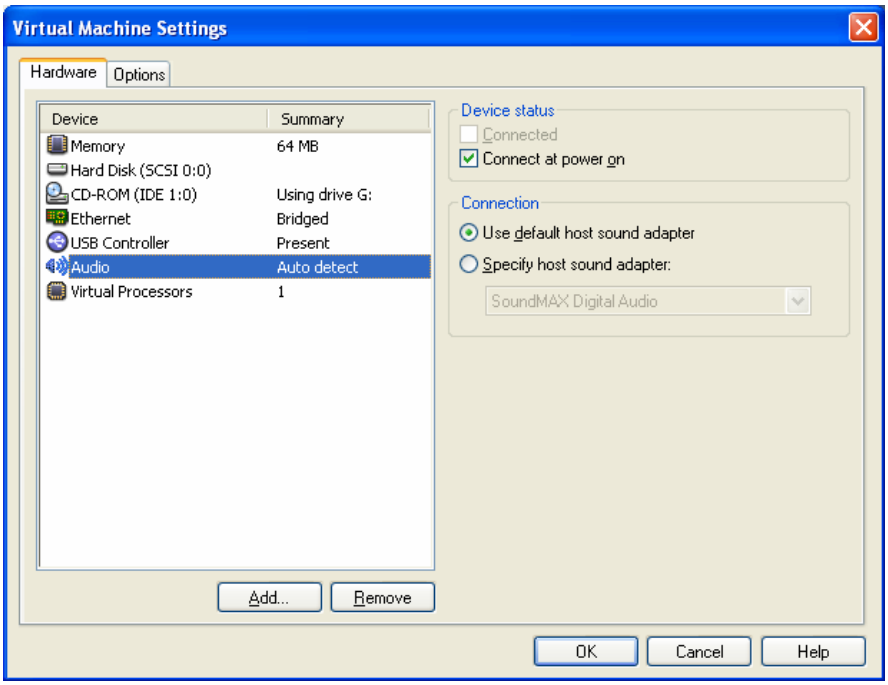
ภาพที่ ๑๐๑ หน้าต่าง Setting ในส่วนของ Ethernet

๙) USB Controller = เป็นการกำหนดให้ VM สามารถใช้งานอุปกรณ์ USB ที่ทำการต่อเข้ามาในระบบได้เมื่อมีการต่ออุปกรณ์เข้ามาที่เครื่อง Host



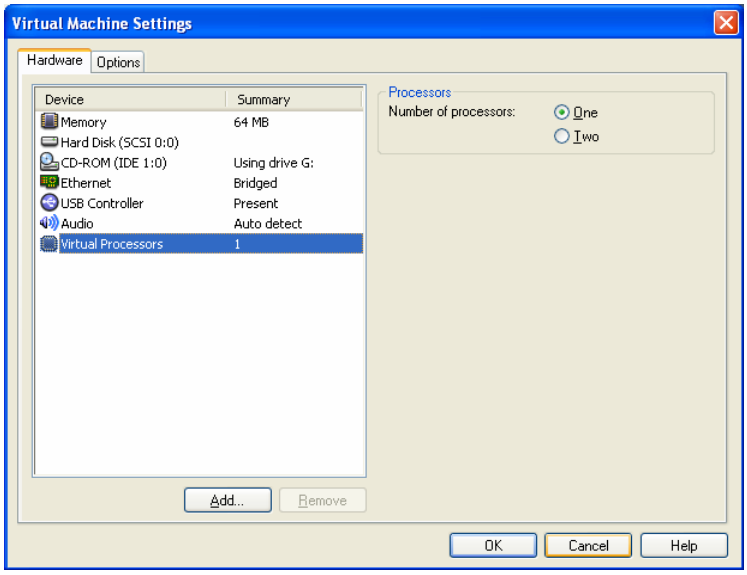
ภาพที่ ๑๐๒ หน้าต่าง Setting ในส่วนของ USB Controller

๑๐) Audio = เป็นการกำหนดให้ VM ใช้ Sound card ของ Host



ภาพที่ ๑๐๓ หน้าต่าง Setting ในส่วนของ Audio

๑๑) Virtual Processors = เป็นการกำหนดว่าต้องการให้ VM มี Processor (CPU) กี่ตัวเพื่อใช้ในการประมวลผลเพื่อทดสอบการใช้งานแบบ Multi-Processors



ภาพที่ ๑๐๔ หน้าต่าง Setting ในส่วนของ Virtual Processors

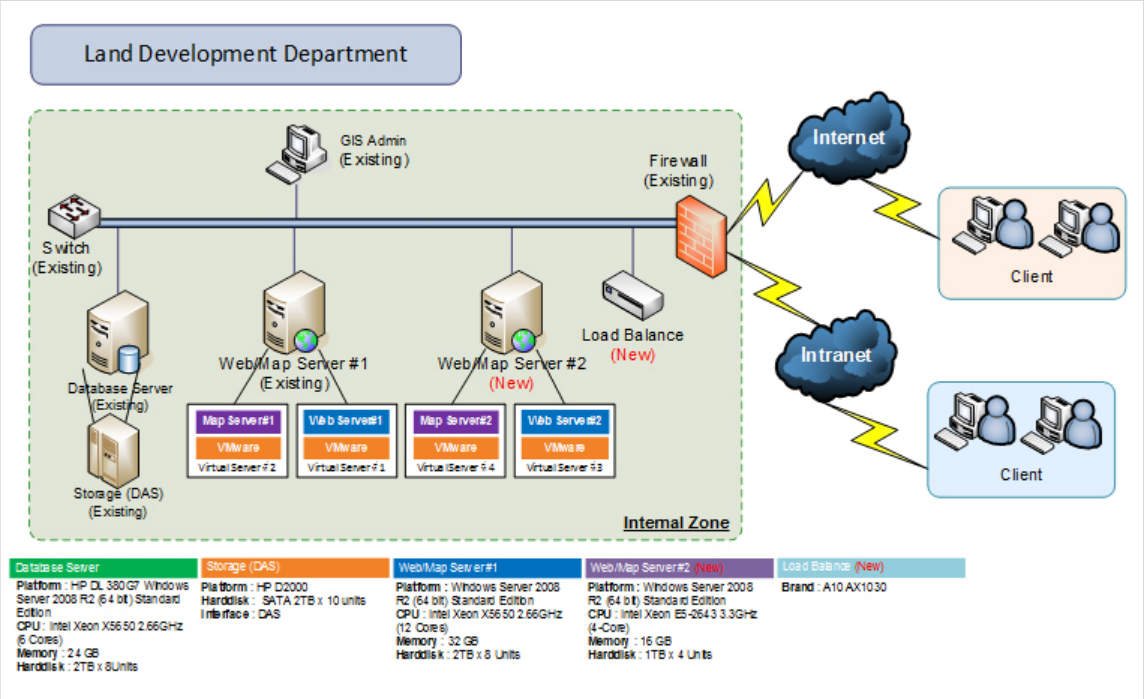
๓.๒.๔ การบริการโดยใช้ระบบบริหารจัดการการตัดสินใจเชิงพื้นที่ (Executive Information System: EIS ด้านการพัฒนาที่ดิน)

๓.๒.๔.๑ การติดตั้งและใช้งานระบบการบริหารจัดการการตัดสินใจเชิงพื้นที่ (Executive Information System-EIS) ผ่านทาง Virtual Machine และการบริหารระบบผ่านทางเครื่องมือกระจายการทำงาน (Load Balancing)

ศูนย์สารสนเทศ กรมพัฒนาที่ดิน ได้นำระบบเทคโนโลยีทางด้านการจัดการข้อมูลเชิงพื้นที่ มาใช้ในการบริหารจัดการกิจกรรมต่าง ๆ โดยระบบดังกล่าว จะเป็นการผสมผสานเทคโนโลยี ทั้งในรูปแบบของระบบสารสนเทศภูมิศาสตร์ และการบริหารจัดการฐานข้อมูล ตลอดจนการพัฒนาโปรแกรมประยุกต์ ที่มีการใช้เทคโนโลยีสารสนเทศภูมิศาสตร์ทำงานในรูปแบบของเว็บแอพพลิเคชั่น (Web Application) ในแต่ละโปรแกรมผู้ใช้งานสามารถเข้าถึง เรียกดู และสืบค้นข้อมูล ผ่านทางช่องการอินเตอร์เน็ต หรือ สมาร์ทโฟน (Smart Phone) ได้

๑) ภาพรวมของระบบ (System Overview)

เป็นการอธิบายถึงภาพรวมของการทำงานของระบบคอมพิวเตอร์ระบบการบริหารจัดการการตัดสินใจเชิงพื้นที่ (Executive Information System-EIS ด้านการพัฒนาที่ดิน) พร้อมทั้งอธิบายถึงหน้าที่การทำงานของเครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่ายและอุปกรณ์เกี่ยวเนื่อง ดังนี้



ภาพที่ ๑๐๕ ภาพรวมของระบบ (System Overview)

จากภาพรวมของระบบบริหารจัดการการตัดสินใจเชิงพื้นที่ (Executive Information System : EIS ด้านการพัฒนาที่ดิน) ประกอบด้วย

๑.๑) เครื่องคอมพิวเตอร์แม่ข่ายสำหรับ Database จำนวน ๑ เครื่อง ทำหน้าที่จัดเก็บข้อมูลของระบบงานทั้งส่วนที่เป็น MIS และ GIS ลงในระบบฐานข้อมูล (RDBMS) โดยเชื่อมต่อกับ Storage HP D๒๖๐๐และให้บริการทั้งผู้ใช้งานบนเครือข่าย

๑.๒) เครื่อง Load Balance จำนวน ๑ เครื่อง ทำหน้าที่กระจายงานของเครื่อง web server ใน virtual server ที่ ๑ และ ๓

๑.๓) เครื่องคอมพิวเตอร์แม่ข่ายสำหรับ Web/Mapจำนวน ๒ เครื่อง ทำหน้าที่ให้บริการใน ๒ ส่วน คือ ระบบงานที่ให้บริการผู้ใช้งานบนเครือข่ายภายในองค์กร (Intranet) และระบบงานที่ให้บริการผู้ใช้งานบนเครือข่ายอินเตอร์เน็ต (Internet) โดยตัวเครื่องคอมพิวเตอร์แม่ข่ายจะมีการแบ่งทำ Virtualization (VMware)เพื่อแบ่ง Virtual Server โดยแบ่งตามหน้าที่การทำงาน ซึ่งมีรายละเอียด ดังนี้

๑.๓.๑) Virtual Server ที่ ๑ ทำหน้าที่เป็นเครื่อง Web Server ๑

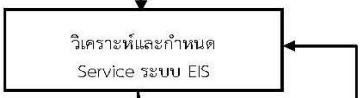
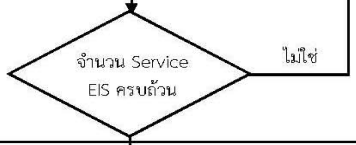
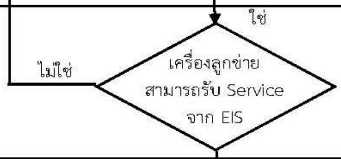
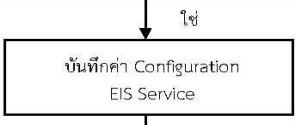
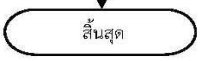
๑.๓.๒) Virtual Server ที่ ๒ ทำหน้าที่เป็นเครื่อง Map Server โดยติดตั้งซอฟต์แวร์โปรแกรมจัดการและจัดเก็บข้อมูลสารสนเทศทางภูมิศาสตร์ สำหรับให้บริการระบบงานทั้ง Intranet และ Internet

๑.๓.๓) Virtual Server ที่ ๓ ทำหน้าที่เป็นเครื่อง Web Server ๓

๑.๓.๔) Virtual Server ที่ ๔ ทำหน้าที่เป็นเครื่อง Map Server โดยติดตั้งซอฟต์แวร์โปรแกรมจัดการและจัดเก็บข้อมูลสารสนเทศทางภูมิศาสตร์ สำหรับให้บริการระบบงานทั้ง Intranet และ Internet

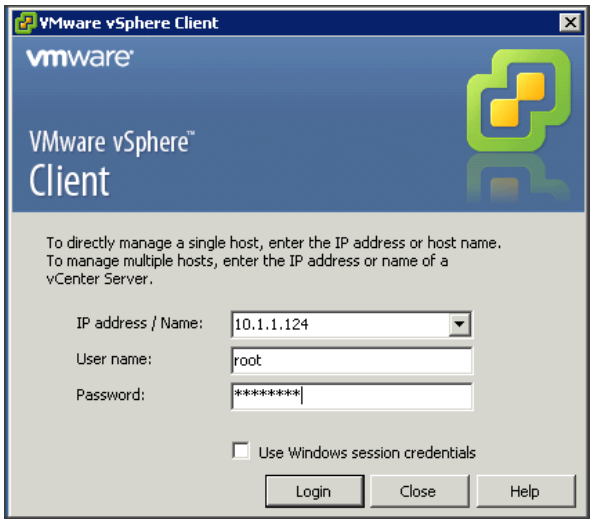
แผนผังแสดงขั้นตอนและวิธีการปฏิบัติงาน

ระบบ Executive Information System (EIS)

ลำดับที่	ผังกระบวนการ	รายละเอียดงาน
		
๑		๑. วิเคราะห์รูปแบบการทำงานด้านแผนภาพกราฟฟิกและข้อมูลอื่น ๆ ที่นำมาใช้ในการตัดสินใจของผู้รับบริการระบบ ศึกษา Service ที่เกี่ยวข้องรวมทั้งความต้องการทั้งหมดของระบบในการบริหาร Service ดังกล่าว ให้สามารถทำงานได้อย่างมีประสิทธิภาพ เพื่อกำหนดค่า Service ที่ต้องใช้งาน
๒		๒. ตรวจสอบจำนวน Service EIS ที่ต้องใช้งานว่าครบถ้วนหรือไม่ ถ้ายังไม่ครบให้กลับไปทำขั้นตอนที่ ๑ ถ้าครบแล้วให้ไปทำขั้นตอนที่ ๓
๓		๓. กำหนดค่า Configuration Service EIS ที่ต้องการรวมทั้ง Requirement ต่าง ๆ ที่ใช้งาน
๔		๔. ติดตั้งเครื่องแม่ข่ายควบคุมระบบ (EIS Server) จากนั้นติดตั้ง Service EIS
๕		๕. ทดสอบการทำงานของเครื่องควบคุมระบบ (EIS Server) ว่าสามารถทำงานได้เป็นปกติหรือไม่ ถ้าไม่สามารถใช้งานได้ให้กลับไปทำขั้นตอนที่ ๔ ถ้าใช้งานได้แล้วให้ไปทำขั้นตอนที่ ๖
๖		๖. ทดสอบการรับบริการของเครื่องลูกข่ายเมื่อติดต่อมายังเครื่องแม่ข่าย EIS Server ว่าสามารถใช้งานได้ปกติหรือไม่ ถ้าไม่สามารถใช้งานได้ให้กลับไปทำขั้นตอนที่ ๔ ถ้าใช้งานได้แล้วให้ไปทำขั้นตอนที่ ๗
๗		๗. บันทึกค่า Configuration ของระบบบริหารจัดการการตัดสินใจเชิงพื้นที่ (Executive Information System : EIS)
		

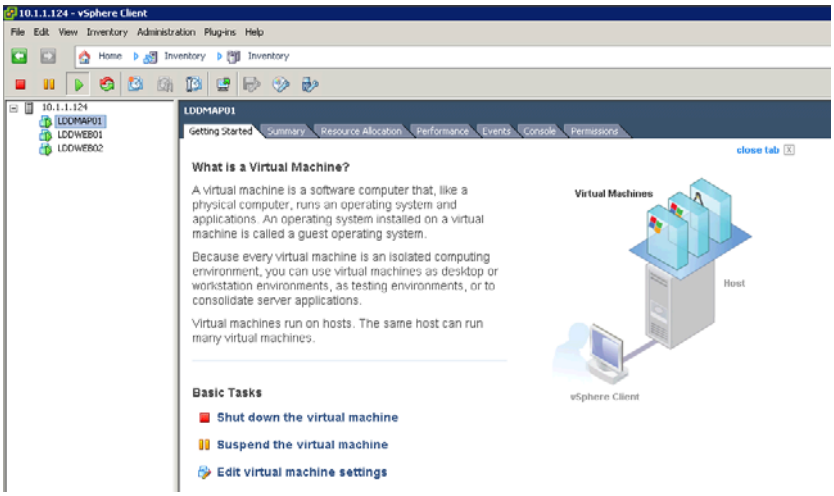
๒) การใช้งานผ่านโปรแกรมVMware vSphere Client

๒.๑) Login ด้วย User : root / password



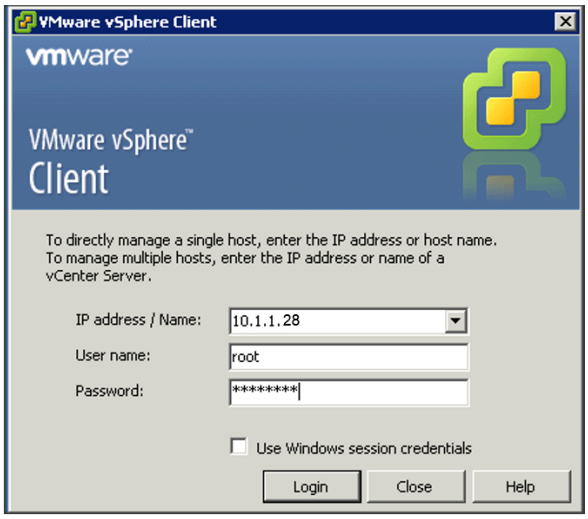
ภาพที่ ๑๐๖ หน้าต่างการ Login ระบบ EIS

๒.๒) จากนั้นไปที่ Basic task > Start vm โดยเปิดเครื่อง LDDMAP๐๑, LDDWEB๐๑ ตามลำดับ



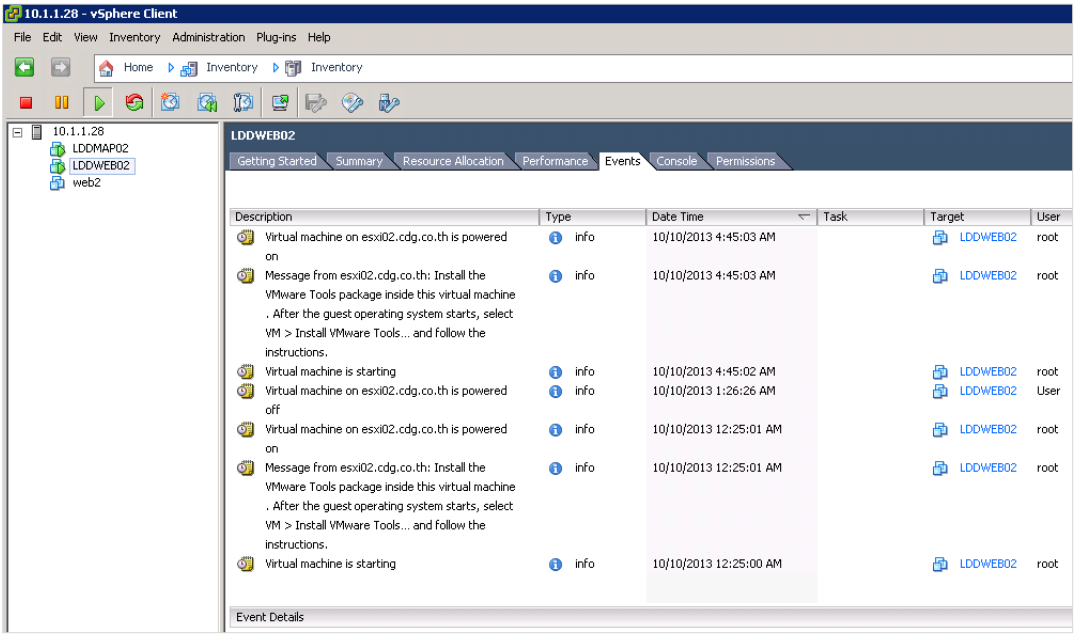
ภาพที่ ๑๐๗ การ Start vm ระบบ EIS

๒.๓) ที่เครื่อง Database เปิดโปรแกรม VMware vSphere Client จากนั้น Login ด้วย User : root / P@ssword



ภาพที่ ๑๐๘ หน้าต่างการ Login ระบบ EIS (๒)

๒.๔) จากนั้นไปที่ Basic task > Start vmโดยเปิดเครื่อง LDDMAP๐๒, LDDWEB๐๒ ตามลำดับ



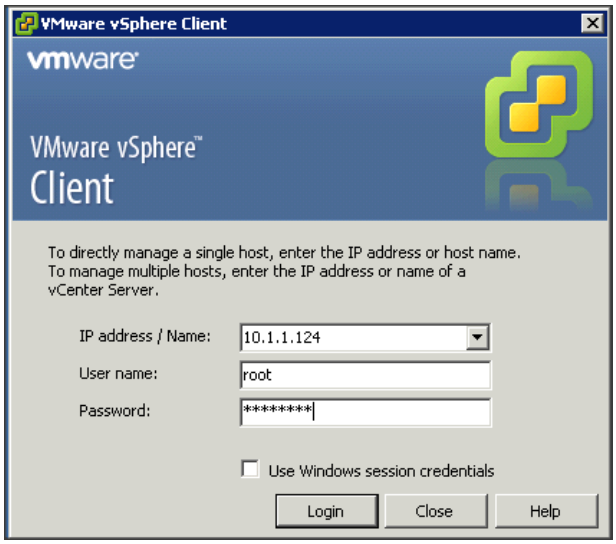
ภาพที่ ๑๐๙ การ Start vm ระบบ EIS (๒)

๓) การปิดเครื่อง ให้ทำการ Shutdown เครื่องตามลำดับ ดังนี้

๓.๑) ทำการ Remote Desktop หรือเปิด Console ผ่าน VMware vSphere Client ที่เครื่อง Web Server #๑ และ Web Server #๒ จากนั้นสั่ง Shutdown

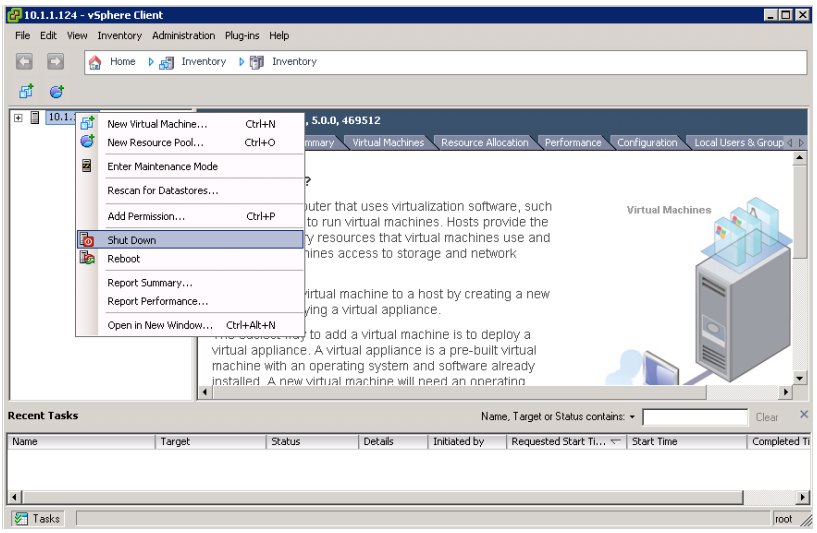
๓.๒) ทำการ Remote Desktop หรือเปิด Console ผ่าน VMware vSphere Client เครื่อง Map Server #๑และ Map Server #๒จากนั้นสั่ง Shutdown

๓.๓) ที่เครื่อง Database เปิดโปรแกรม VMware vSphere Client จากนั้น Login ด้วย User : root / password



ภาพที่ ๑๑๐ หน้าต่างการ Login ระบบ EIS (๓)

๓.๔) จากนั้นคลิกขวาที่ “๑๐.๑.๑.๑๒๔” เลือก Shutdown เพื่อ Shutdown เครื่อง Web / Map Server

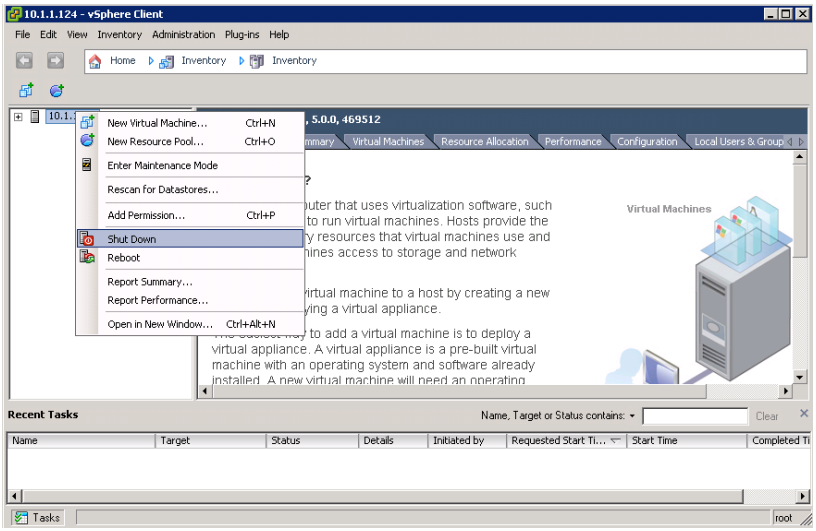


ภาพที่ ๑๑๑ การ Shutdown เครื่อง Web

๓.๕) ที่เครื่อง Database เปิดโปรแกรม VMware vSphere Client จากนั้น Login ด้วย User : root / P@ssword

ภาพที่ ๑๑๒ หน้าต่างการ Login ระบบ EIS (๔)

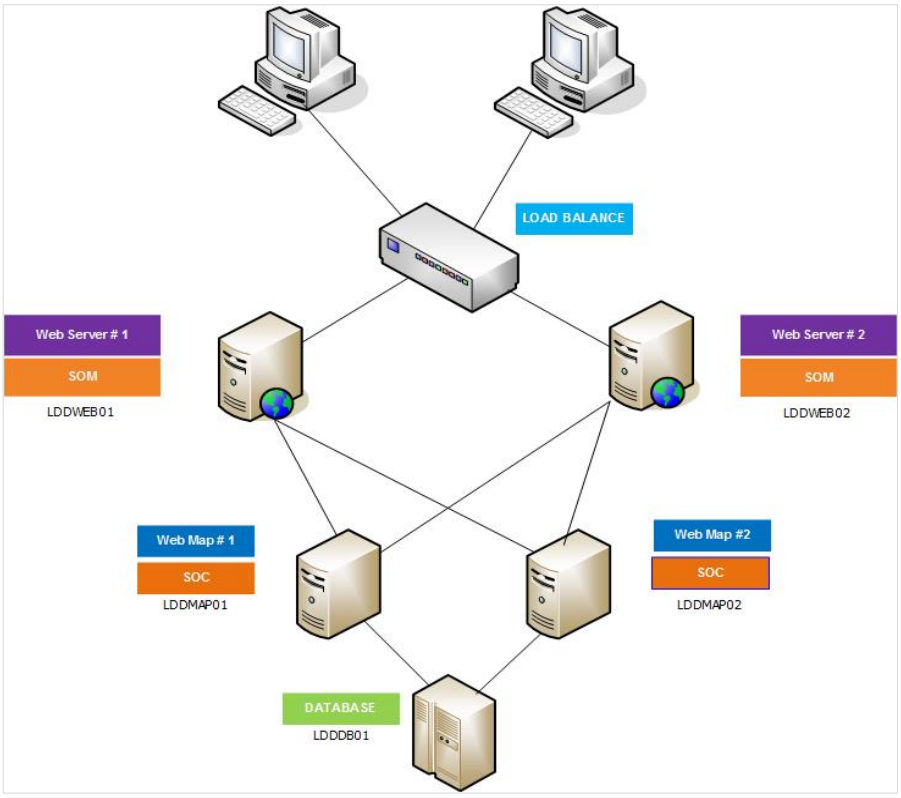
๓.๖) จากนั้นคลิกขวาที่ “๑๐.๑.๑.๒๘” เลือก Shutdown เพื่อ Shutdown เครื่อง Web / Map Server



ภาพที่ ๑๑๓ การ Shutdown เครื่อง Web (๒)

๓.๗) สั่ง Shutdown Database Server เมื่อเครื่อง Database ดับ จึงปิด Storage HP D๒๖๐๐

๔) ขั้นตอนการบริหารจัดการระบบ (Operating Procedure)



ภาพที่ ๑๑๔ หลักการการทำงานเบื้องต้นของระบบ

ภายในเครื่อง Web Server จะประกอบไปด้วย ๒ ส่วน คือ Web application และ SOM(ArcGIS ServerObject Manager) ซึ่ง SOM จะมีหน้าที่คอยรับการร้องขอ Map Service จาก Web application จากนั้นจะส่งข้อมูลที่ได้รับมาไปให้ Map Server ภายในเครื่อง Map Server จะมี SOC (ArcGIS Server ObjectContainer) รอรับงานจาก SOM เมื่อได้รับงานก็จะทำการประมวลผลโดยอาศัยข้อมูลแผนที่ใน Database จากนั้นจึงส่งงานกลับไปหา SOM เพื่อส่งกลับไปยัง Web application อีกครั้งหนึ่ง และมีเครื่อง Load Balance สำหรับกระจายงานเครื่อง Web Server ทั้งสอง เพื่อแบ่งภาระการทำงานของเครื่อง

๔.๑) ลำดับการ Stop / Start Service เพื่อแก้ไขกรณีเกิดปัญหาในการใช้งานระบบจากที่ได้อธิบายถึงหลักการทำงานของระบบไว้แล้ว แสดงให้เห็นว่า Service ต่างๆในแต่ละเครื่องมีการทำงานเชื่อมโยงกันอยู่ จึงต้องมีลำดับในการ Start / Stop Service ซึ่งมีลำดับดังนี้

๔.๑.๑) การ StopService

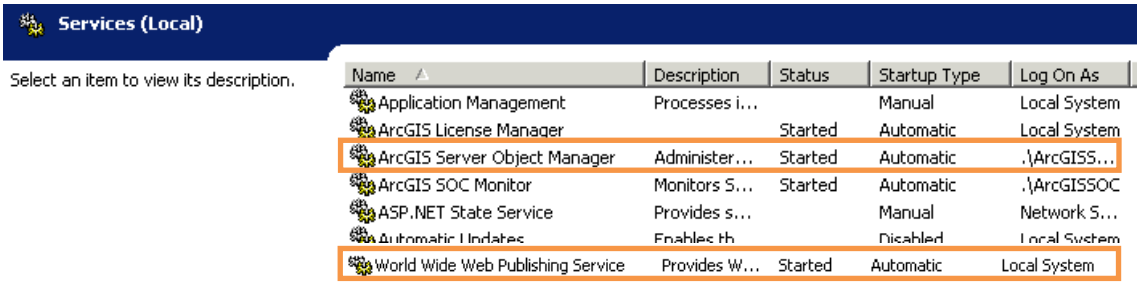
- Stop Service “ArcGIS Server Object Manager” ที่เครื่อง Web Server ทั้ง ๒ เครื่อง
- Stop Service “ArcGIS SOC Monitor” ที่เครื่อง Map Server ทั้ง ๒ เครื่อง
- Stop Service “SQL Server (LDDDB)” ที่เครื่อง Database Server

๔.๑.๒) การ StartService

- Start Service “SQL Server (LDDDB)” ที่เครื่อง Database Server
- Start Service “ArcGIS SOC Monitor” ที่เครื่อง Map Server ทั้ง ๒ เครื่อง
- Start Service “ArcGIS Server Object Manager” ที่เครื่อง Web Server ทั้ง ๒ เครื่อง

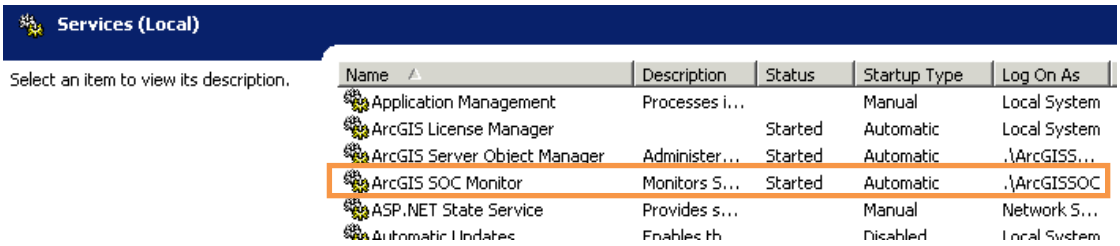
๔.๒) วิธีการในการ Stop / Start Service ในแต่ละเครื่อง มีรายละเอียดดังนี้

๔.๒.๑) เครื่อง Web Server # ๑ และ Web Server # ๒ ไปที่ Services จากนั้นคลิกขวาที่ArcGIS Server Object Manager, World Wide Web Publishing Serviceแล้วเลือก Start เพื่อ Start Service หรือ Stop เพื่อ Start Service



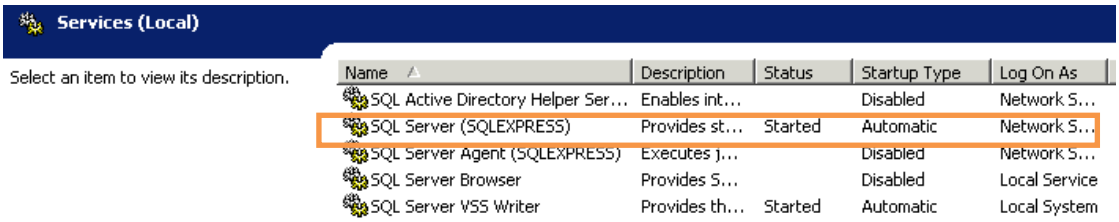
ภาพที่ ๑๑๕ การ Configuration ระบบ EIS

๔.๒.๒) เครื่อง Map Server#๑ และ Map Server #๒ ไปที่ Services จากนั้นคลิกขวาที่ArcGIS SOC Monitor แล้วเลือก Start เพื่อ Start Service หรือ Stop เพื่อ Start Service



ภาพที่ ๑๑๖ การ Configuration ระบบ EIS (๒)

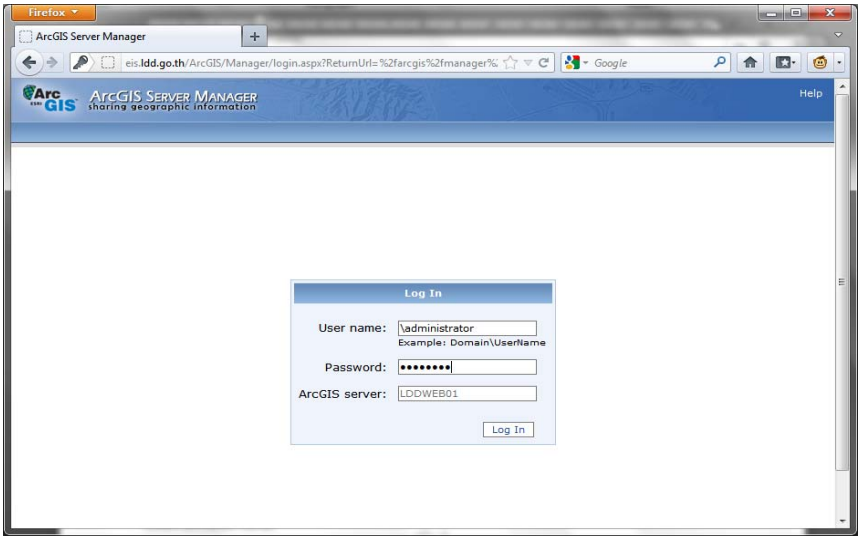
๔.๒.๓) เครื่อง Database Server ไปที่ Services จากนั้นคลิกขวาที่ SQL Server (LDDDB) แล้วเลือก Start เพื่อ Start Database หรือ Stop เพื่อ Start Database



ภาพที่ ๑๑๗ การ Configuration ระบบ EIS (๓)

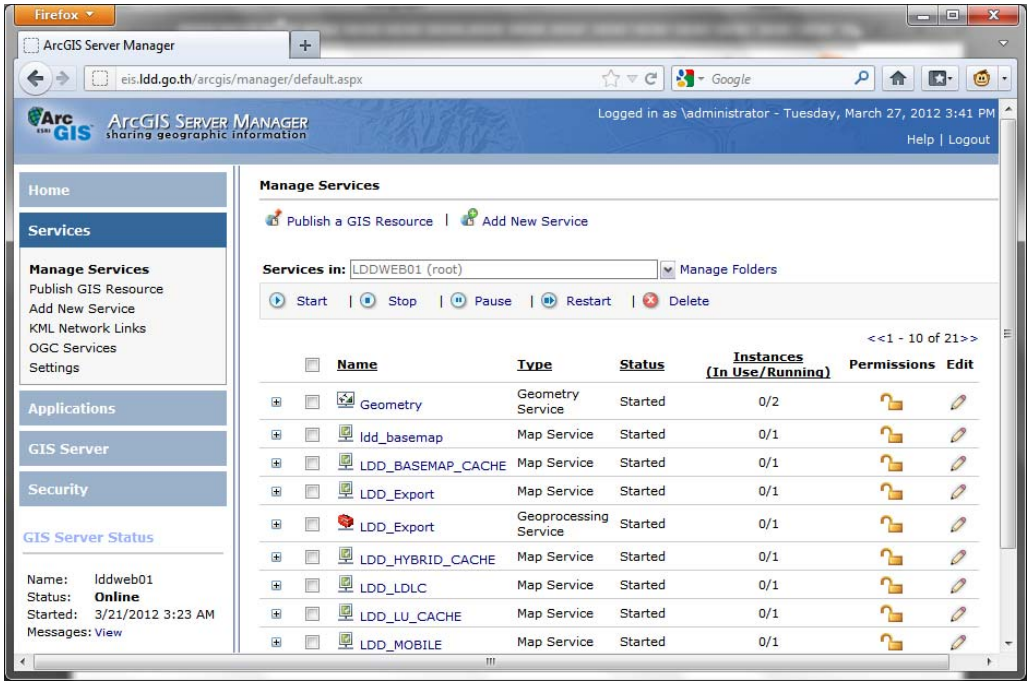
๔.๓) การจัดการ Map Service ผ่าน ArcGIS Server Manager

๔.๓.๑) เปิด Web browser เข้าไปที่ URL : http://<lddweb๐๑ หรือlddweb๐๒>/arcgis/manager จากนั้น Login ด้วย User / Password : Administrator / @ldd#adm



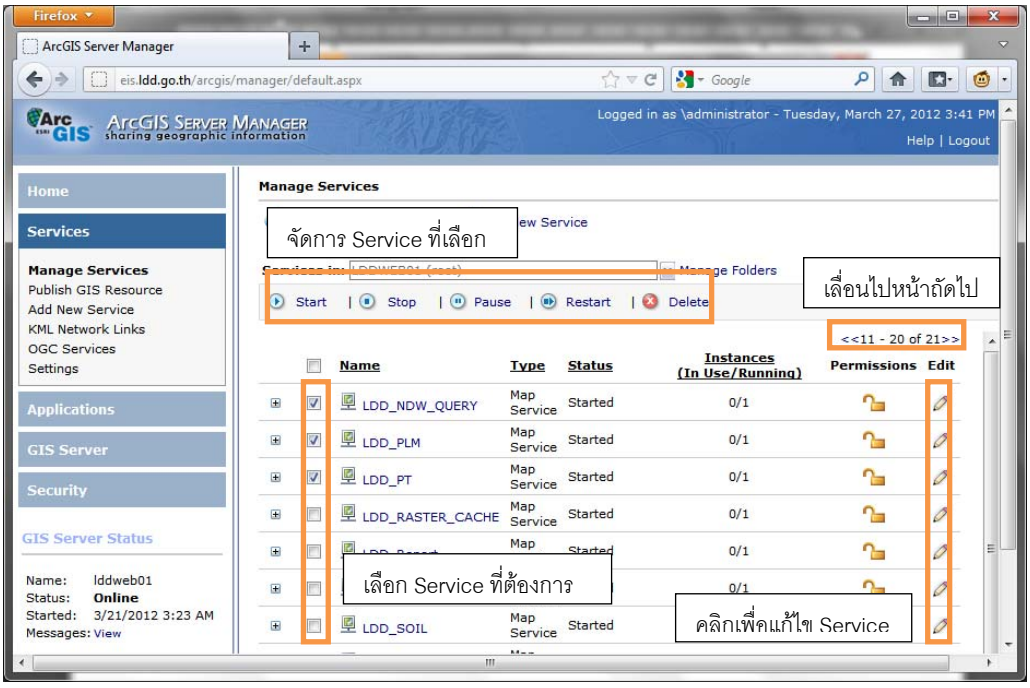
ภาพที่ ๑๑๘ การ Configuration ระบบ EIS (๔)

๔.๓.๒ ที่เมนูด้านซ้าย เลือก Services> Manage Services จะปรากฏรายการ Service ดังรูป



ภาพที่ ๑๑๙ การ Configuration ระบบ EIS (๕)

๔.๓.๓) จากหน้าต่างนี้สามารถสั่ง Stop, Start, Restart, Delete และ แก้ไข Map service



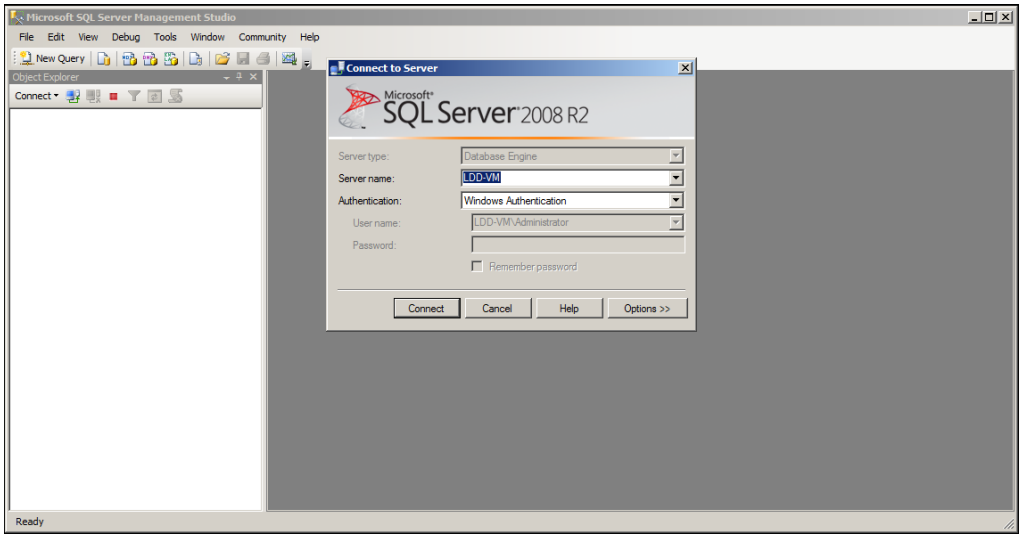
ภาพที่ ๑๒๐ การ Configuration ระบบ EIS (๖)

๕) Backup and Restore

อธิบายถึงวิธีการสำรองข้อมูล Database สำรองระบบปฏิบัติการของเครื่อง Web / Map Server และวิธีการสำรองConfigure file ของซอฟต์แวร์ ArcGIS Server ดังนี้

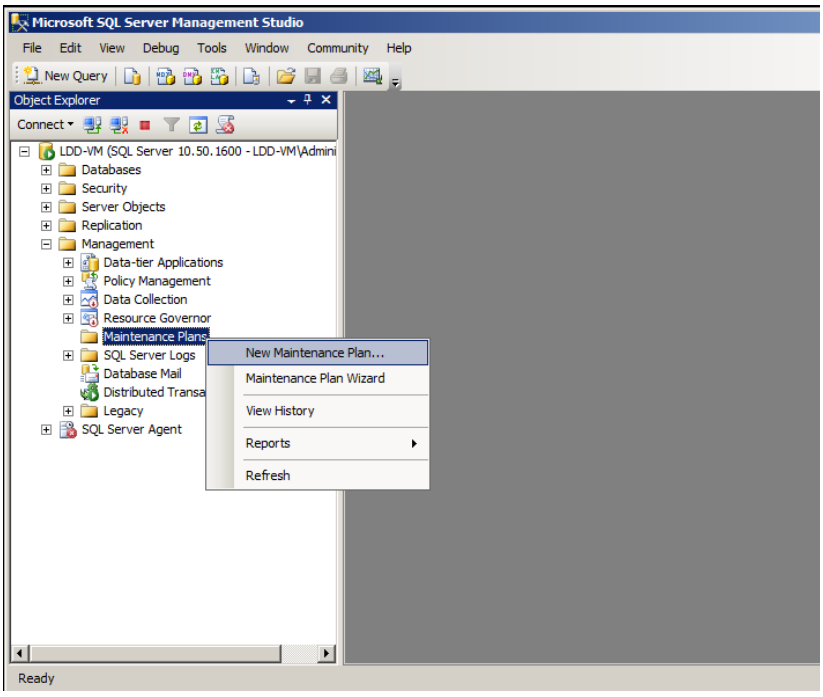
๕.๑) ขั้นตอนการสร้าง Schedule สำหรับBackup Database

๕.๑.๑) เปิดโปรแกรม “Microsoft SQL Server Management Studio” ที่ Authentication เลือก “Windows Authentication” ดังภาพ จากนั้นคลิก Connect



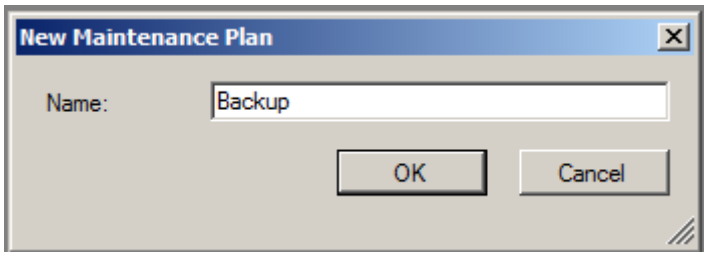
ภาพที่ ๑๒๑ การ Configuration ระบบ EIS (๗)

๕.๑.๒) จากนั้นไปที่ Management > Maintenance Plans แล้วคลิกขวา เลือก “New Maintenance Plan...”



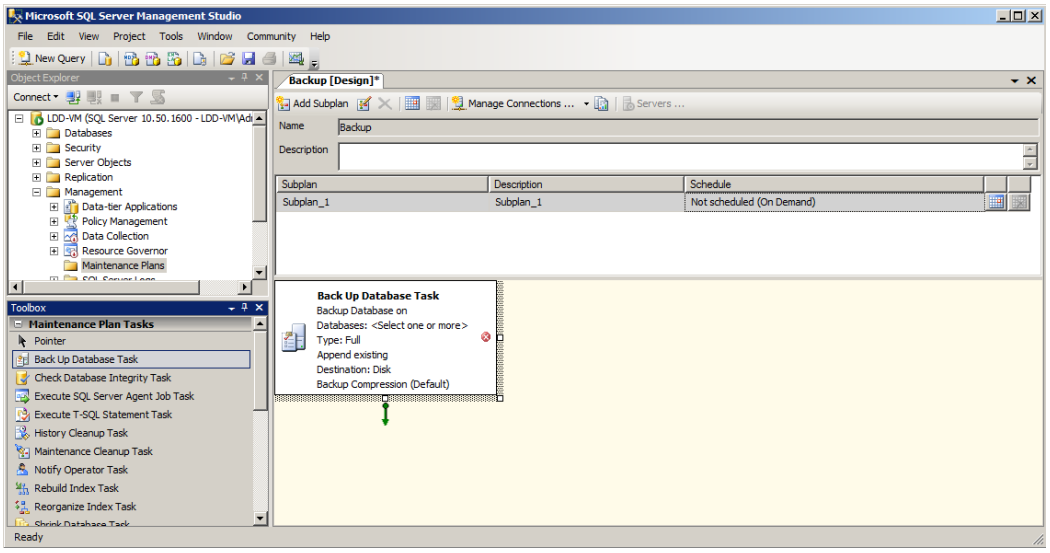
ภาพที่ ๑๒๒ การ Configuration ระบบ EIS (๘)

๕.๑.๓) ตั้งชื่อจากนั้นคลิก OK



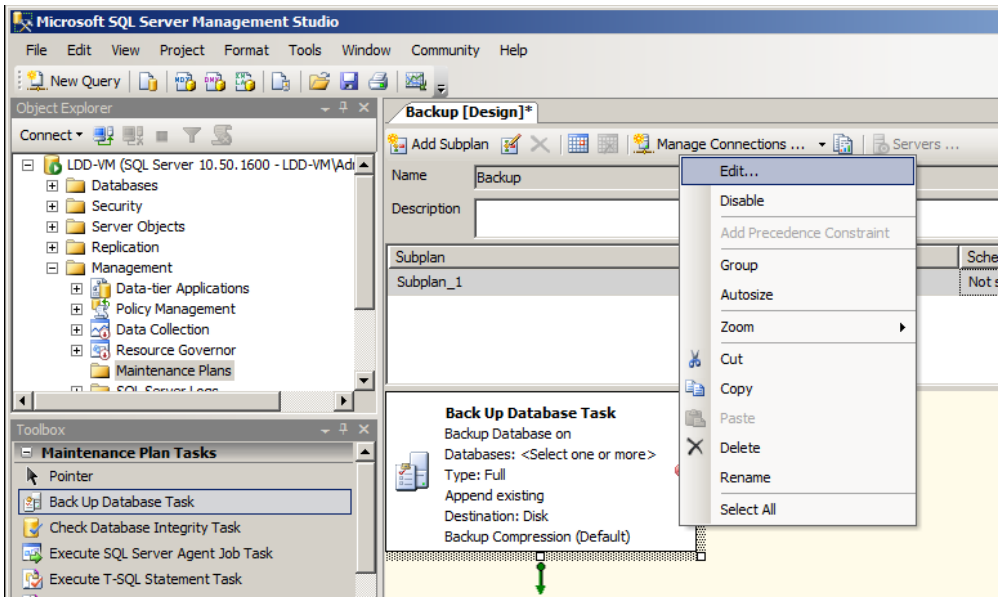
ภาพที่ ๑๒๓ การ Configuration ระบบ EIS (๙)

๕.๑.๔) ดับเบิ้ลคลิกที่“Back Up Database Task”จะปรากฏดังภาพ



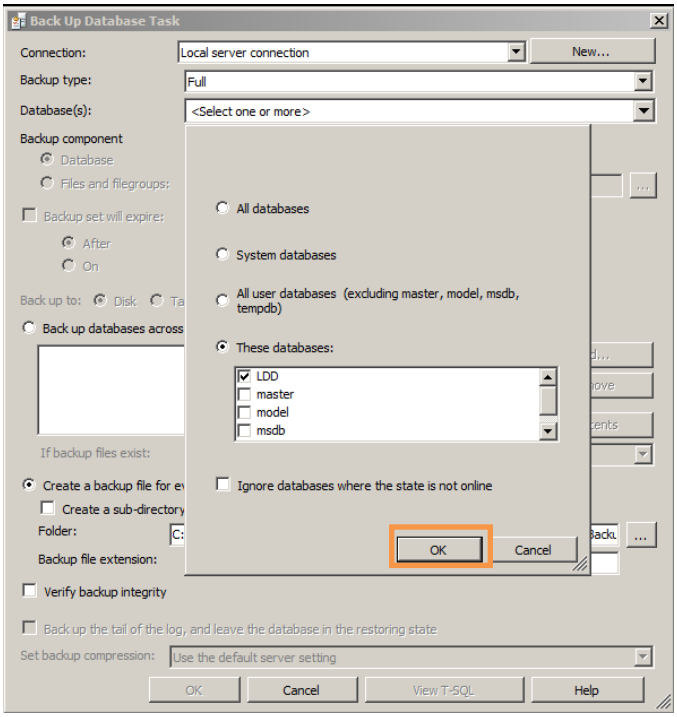
ภาพที่ ๑๒๔ การ Configuration ระบบ EIS (๑๐)

๕.๑.๕) คลิกขวาที่กรอบ “Back Up Database Task” เลือก Edit



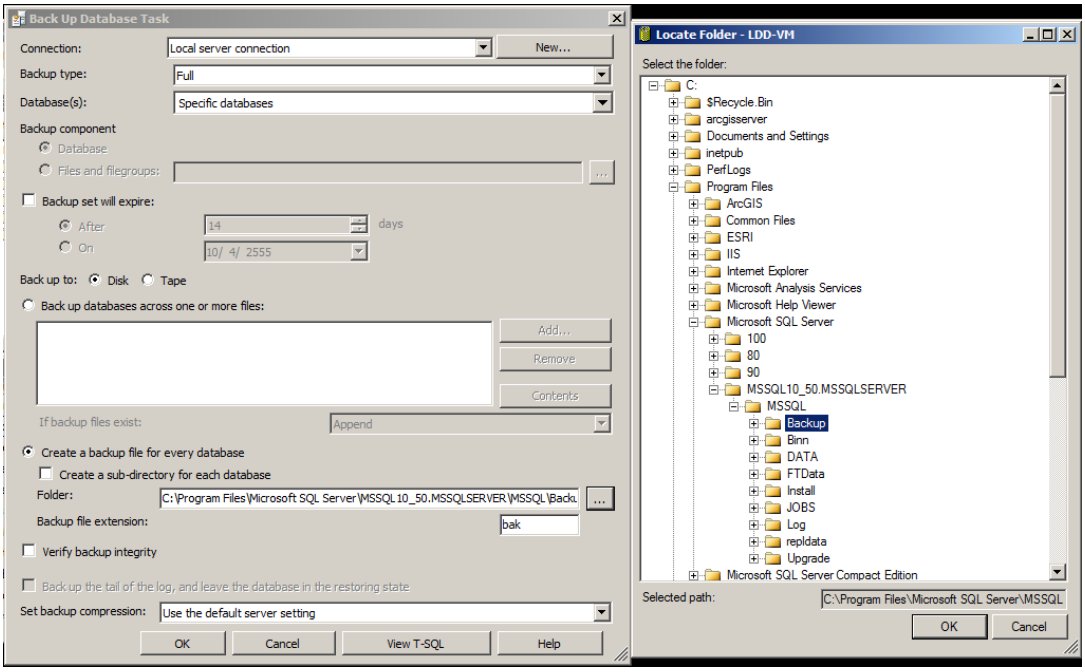
ภาพที่ ๑๒๕ การ Configuration ระบบ EIS (๑๑)

๕.๑.๖) ที่ Backup type เลือก Full ที่ Database(s) เลือก LDD และ sde จากนั้นคลิก OK



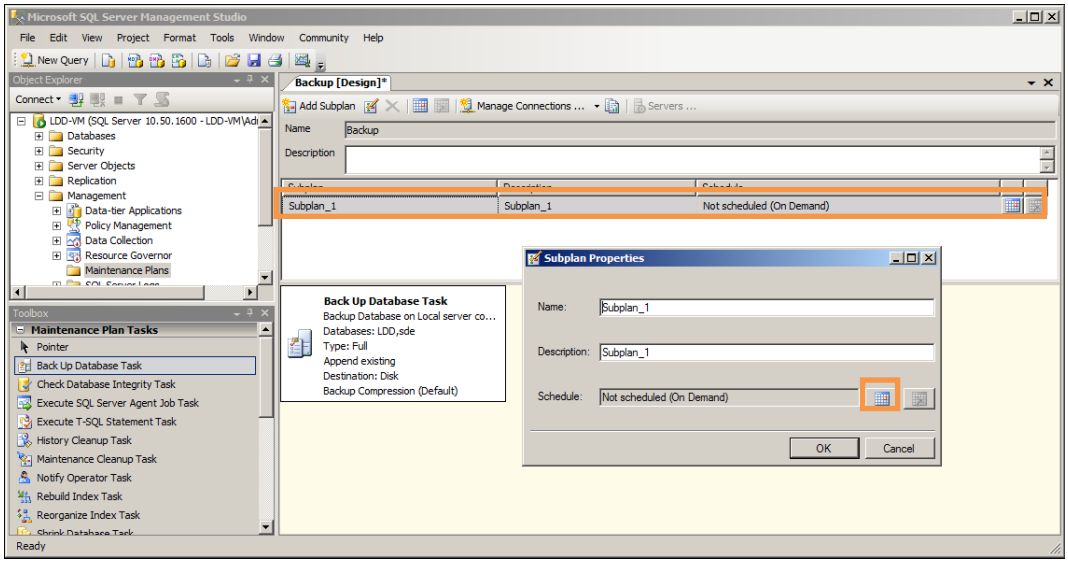
ภาพที่ ๑๒๖ การ Configuration ระบบ EIS (๑๒)

๕.๑.๗) จากนั้น คลิกปุ่ม “...” ปรากฏหน้าต่างย่อยทางด้านขวาเพื่อเลือกที่เก็บไฟล์ Backup เมื่อเลือกได้แล้วคลิก OK ๒ ครั้ง



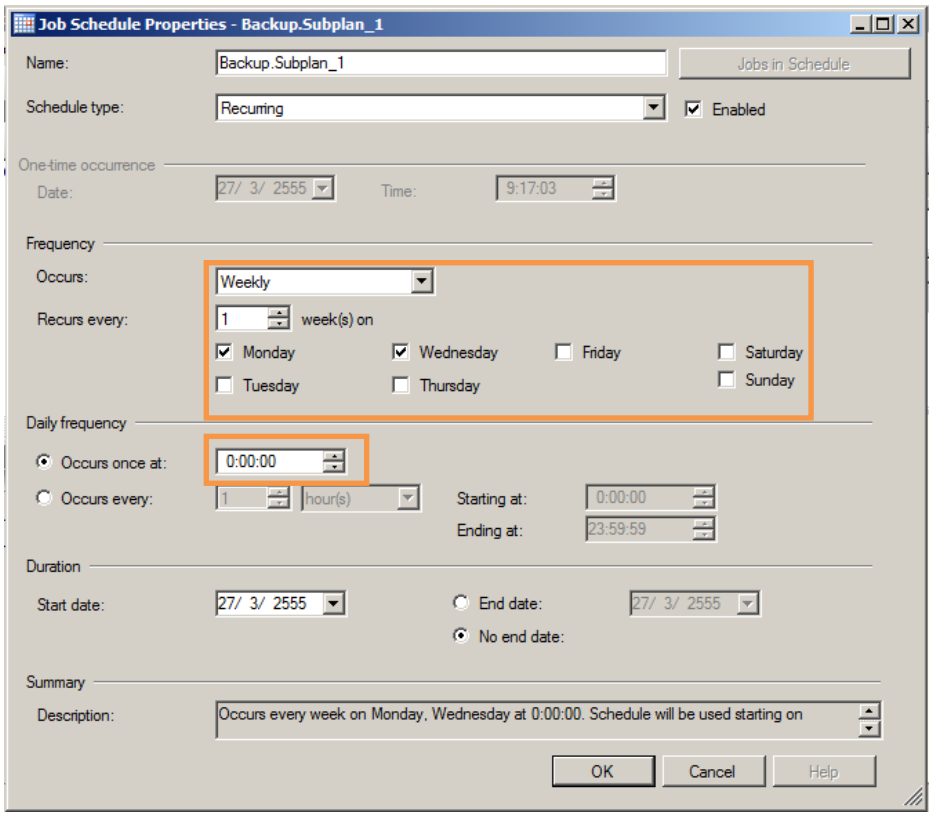
ภาพที่ ๑๒๗ การ Configuration ระบบ EIS (๑๓)

๕.๑.๘) ดับเบิ้ลคลิกที่ Subplan_๑ จะปรากฏหน้าต่างย่อยดังรูป คลิกปุ่ม 



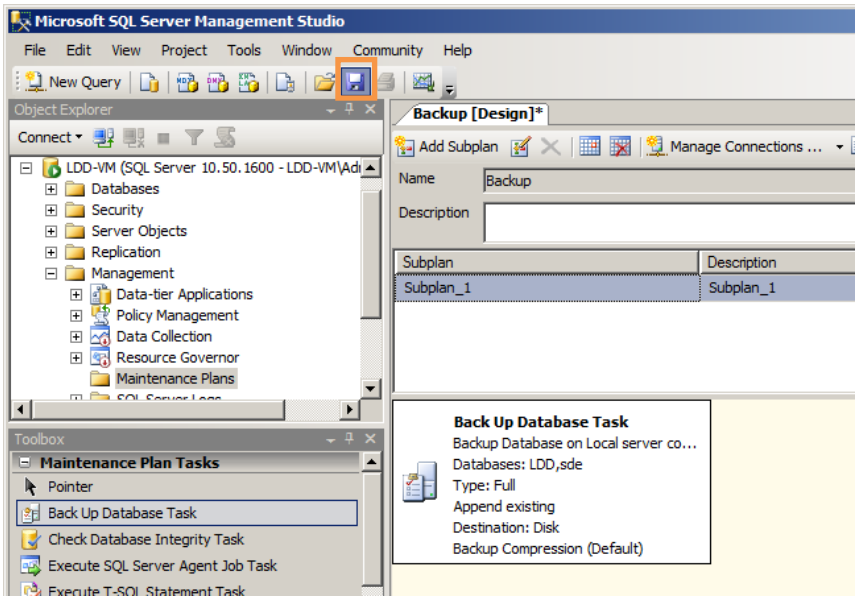
ภาพที่ ๑๒๘ การ Configuration ระบบ EIS (๑๔)

๕.๑.๙) ทำการตั้งค่าวันและเวลาในการ Backup จากนั้น คลิก OK



ภาพที่ ๑๒๙ การ Configuration ระบบ EIS (๑๕)

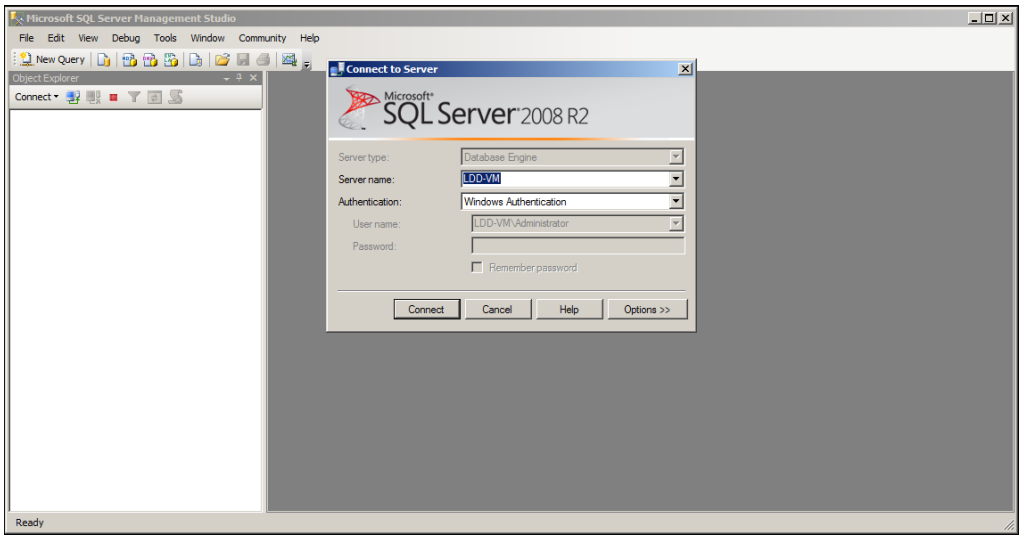
๕.๑.๑๐) จากนั้นคลิกที่  เพื่อทำการบันทึกการตั้งค่า เป็นอันเสร็จสิ้น



ภาพที่ ๑๓๐ การ Configuration ระบบ EIS (๑๖)

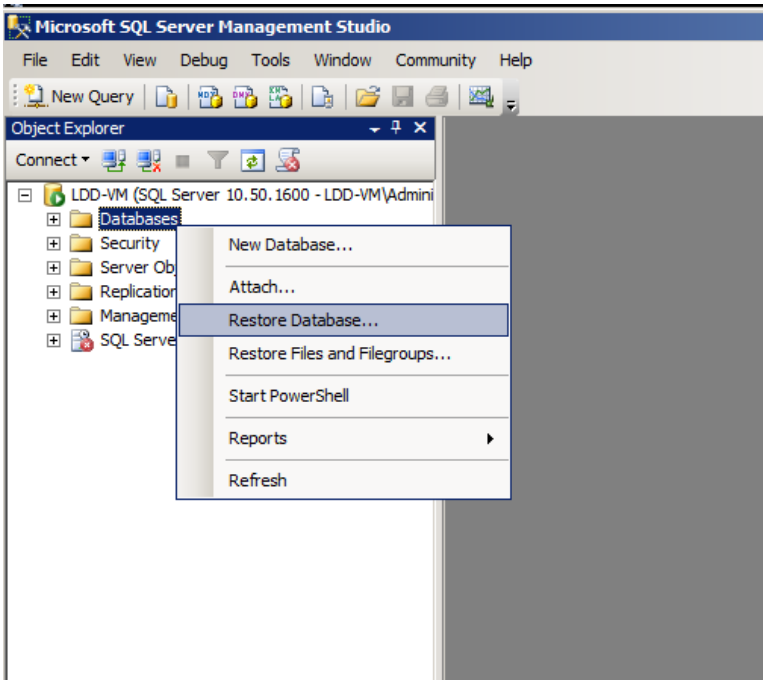
๖) ขั้นตอนการ Restore Database

๖.๑) เปิดโปรแกรม “Microsoft SQL Server Management Studio” ที่ Authentication เลือก “Windows Authentication” ดังภาพ จากนั้นคลิก Connect



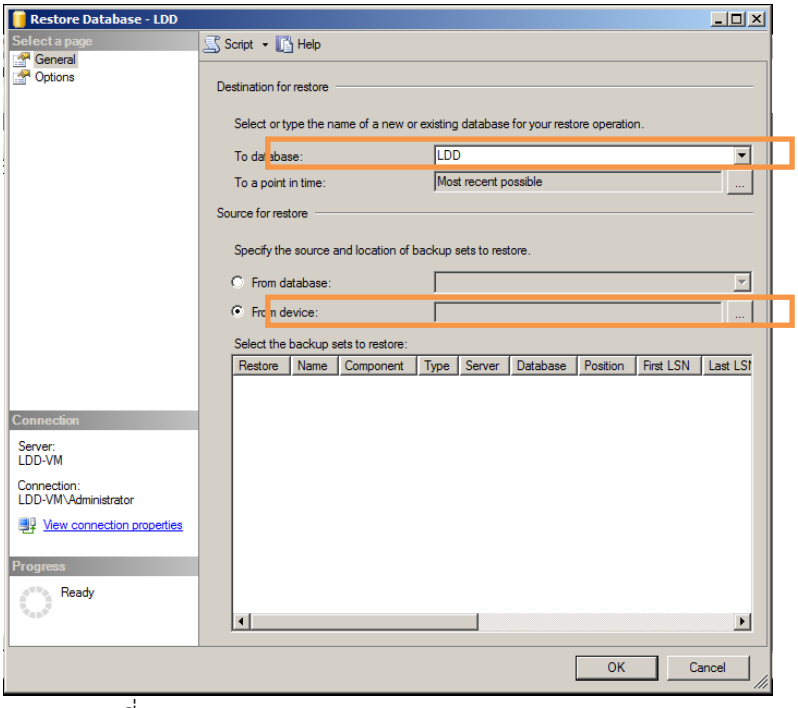
ภาพที่ ๑๓๑ การ Configuration ระบบ EIS (๑๗)

๖.๒) คลิกขวาที่ Databases เลือก Restore Database...



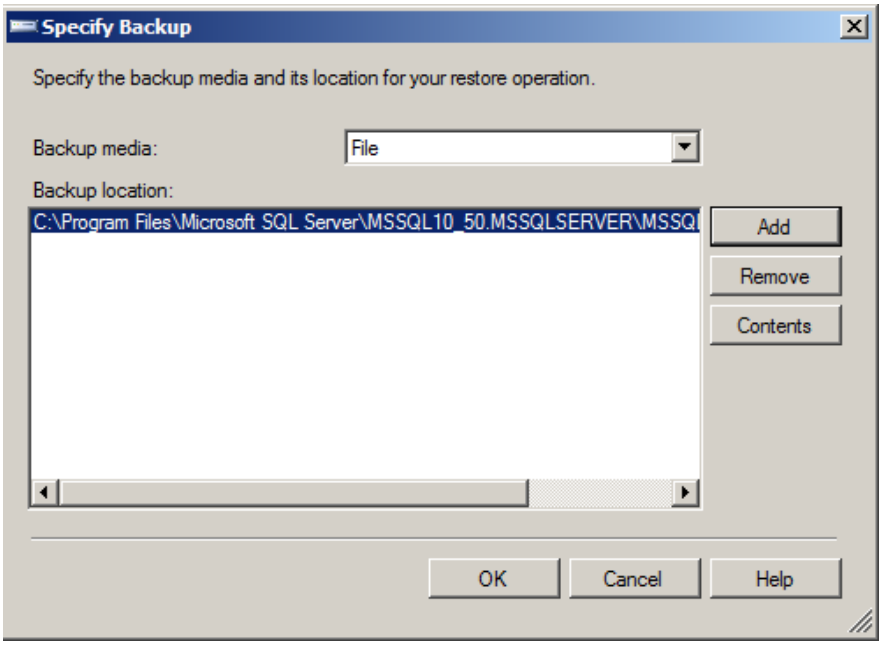
ภาพที่ ๑๓๒ การ Configuration ระบบ EIS (๑๘)

๖.๓) จะปรากฏหน้าต่างใหม่ดังภาพที่ To database ให้เลือก Database ที่ต้องการจะ Restore ที่ Source for restore เลือก From device จากนั้นคลิกปุ่ม ... เพื่อเลือกไฟล์ Backup



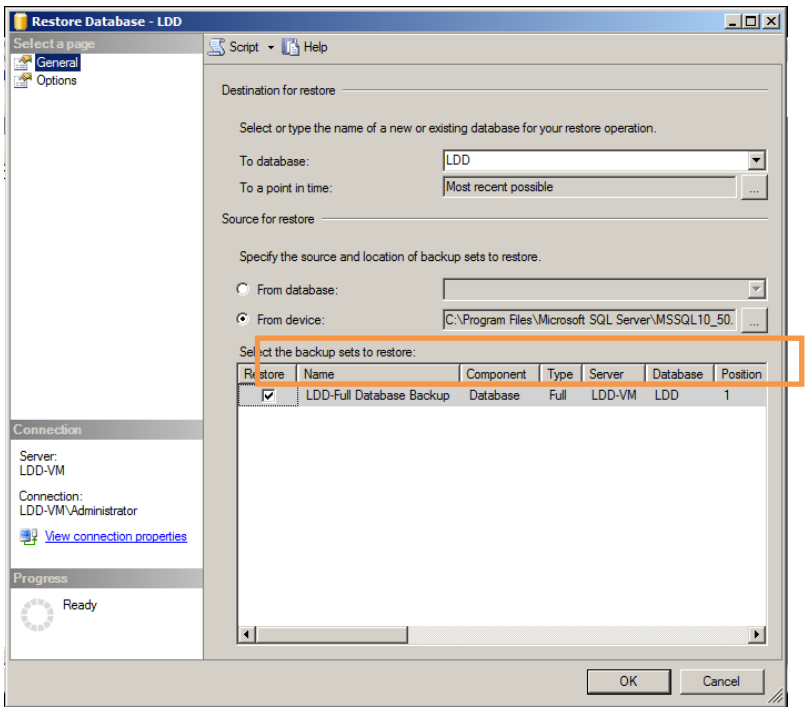
ภาพที่ ๑๓๓ การ Configuration ระบบ EIS (๑๙)

๖.๔) คลิก Add จากนั้นเลือกไฟล์ Backup ที่ต้องการจะ Restore เสร็จแล้ว คลิก OK



ภาพที่ ๑๓๔ การ Configuration ระบบ EIS (๒๐)

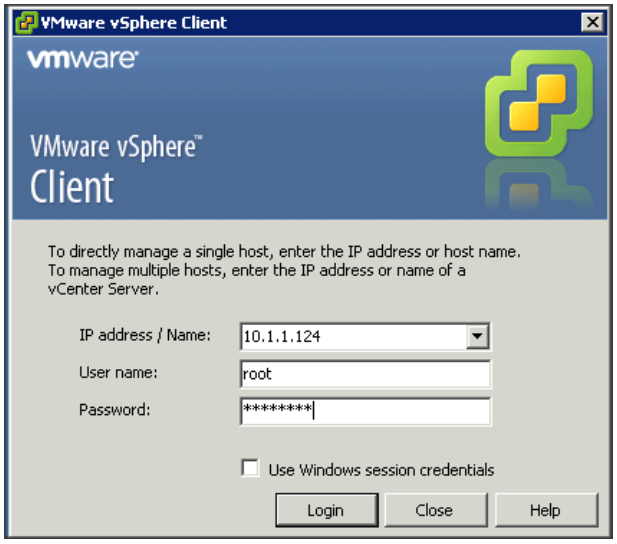
๖.๕) เลือกข้อมูลที่จะทำการ Restore จากไฟล์ Backup ดังรูป จากนั้นคลิก OK โปรแกรมจะเริ่มทำการ Restore Database จนเสร็จ



ภาพที่ ๑๓๕ การ Configuration ระบบ EIS (๒๑)

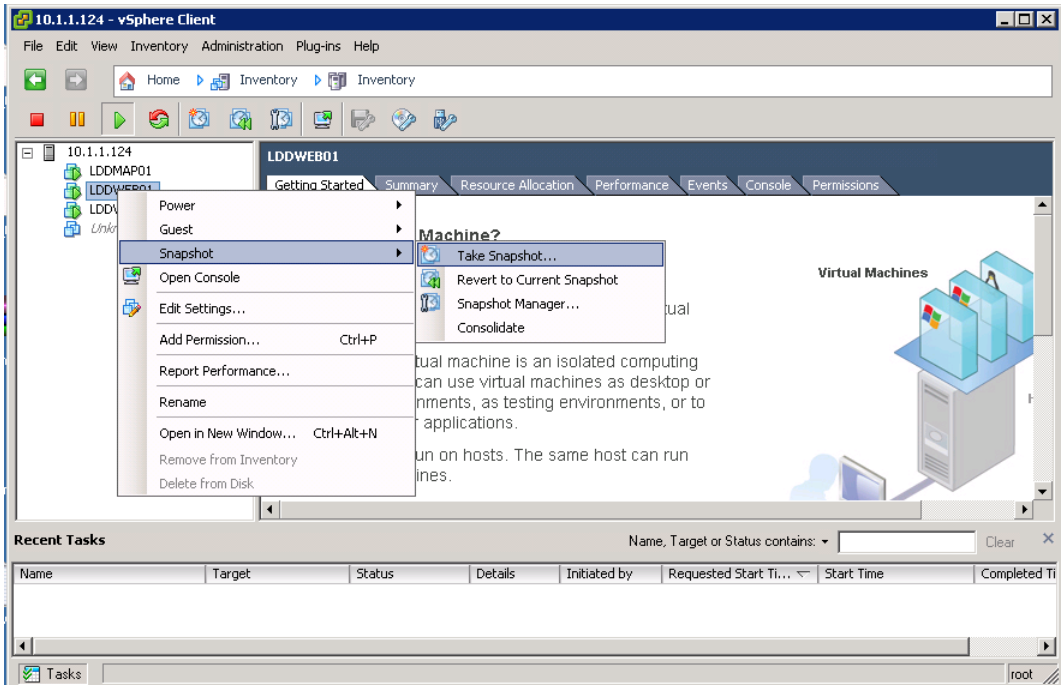
๗) วิธีการทำ Snap shot เพื่อ Backup เครื่อง Web Server และ Map Server

๗.๑) ที่เครื่อง Database เปิดโปรแกรม VMware vSphere Client จากนั้น Login ด้วย User : root / passwordที่เครื่อง ๑๐.๑.๑.๑๒๔ หรือ Login ด้วย User : root / P@ssword ที่เครื่อง ๑๐.๑.๑.๒๘



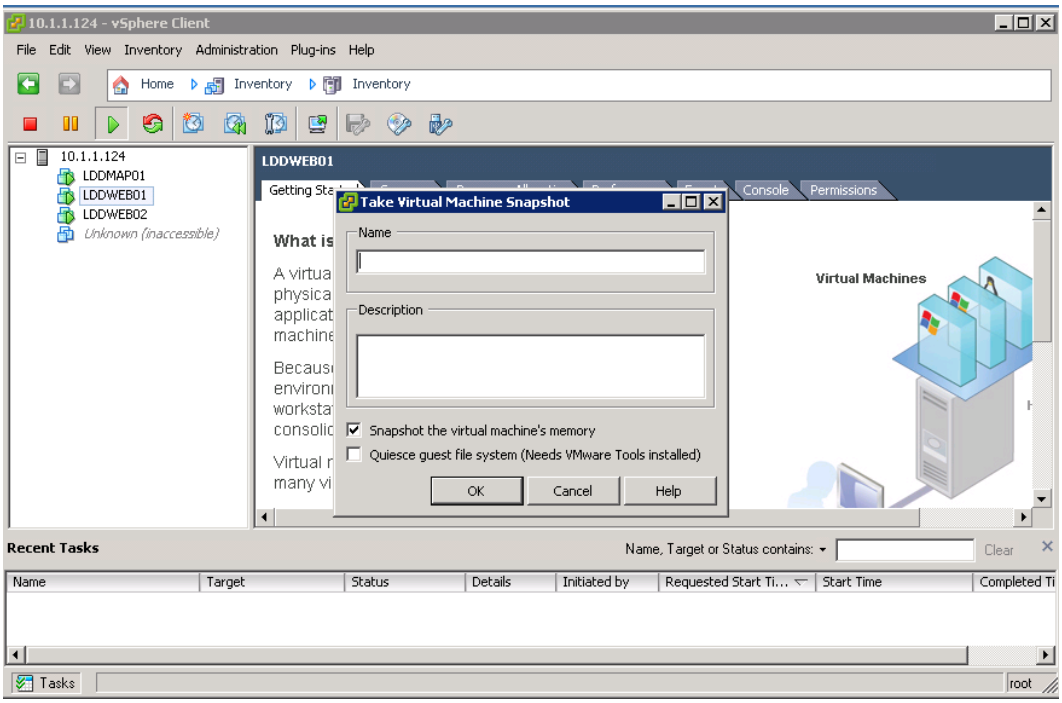
ภาพที่ ๑๓๖ หน้าต่างการ Login ระบบ EIS (๕)

๗.๒) คลิกขวาที่ VM ที่ต้องการทำ Snap shot เลือก Snapshot > Take Snapshot



ภาพที่ ๑๓๗ การ Snapshot ระบบ EIS

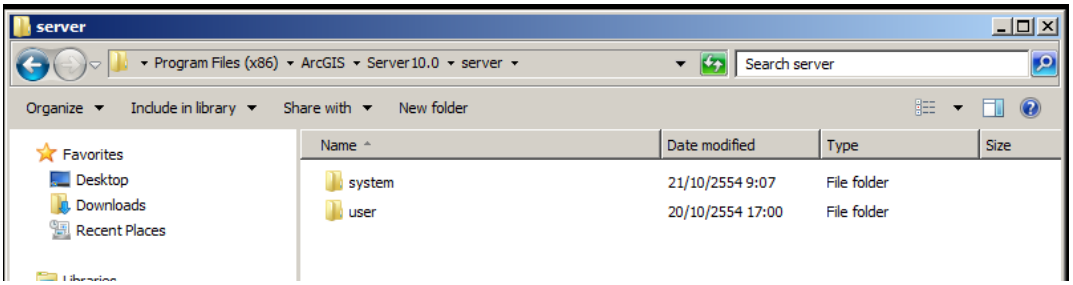
๗.๓) ตั้งชื่อและใส่ Description จากนั้นคลิก OK โปรแกรมจะเริ่มทำการจัดเก็บ Snapshot



ภาพที่ ๑๓๘ การ Snapshot ระบบ EIS (๒)

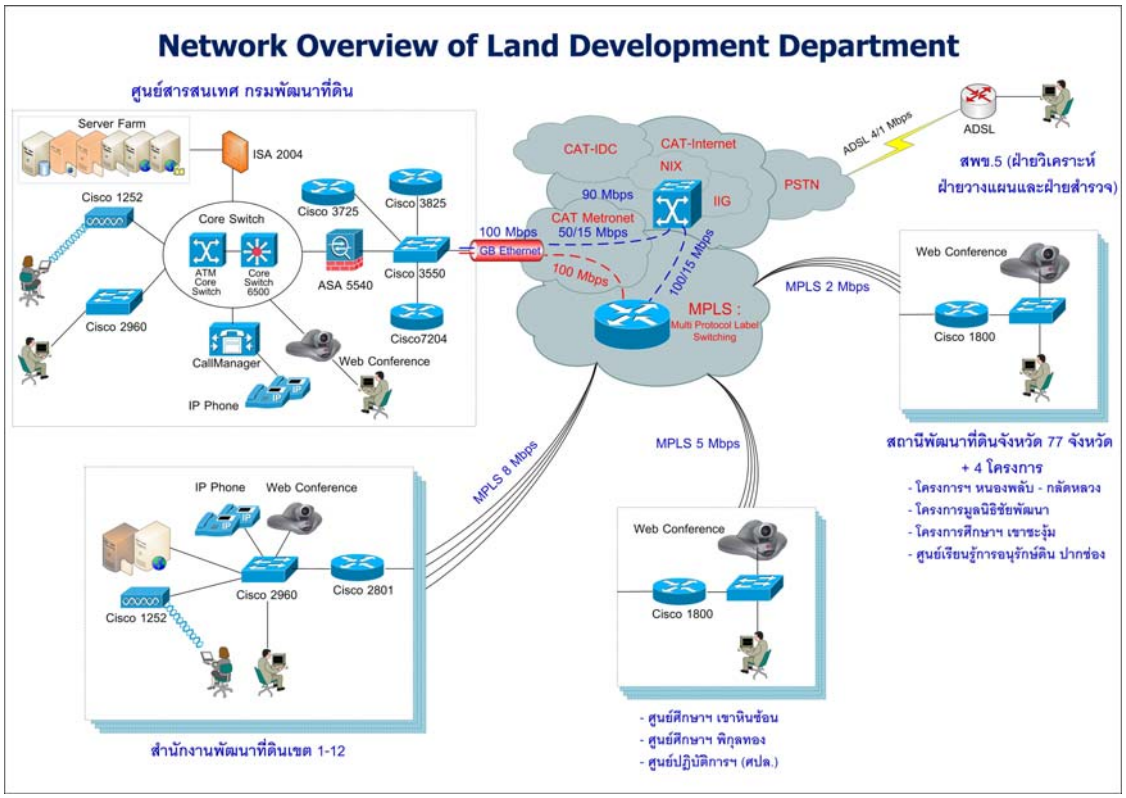
๘) วิธีการสำรองConfigure file ของซอฟต์แวร์ ArcGIS Server

๘.๑) เข้าไปที่ Path : C:\Program Files(x๘๖)\ArcGIS\Server๑๐.๐\server จากนั้นทำการ Copy โฟลเดอร์ “user” ออกมาเก็บสำรองไว้

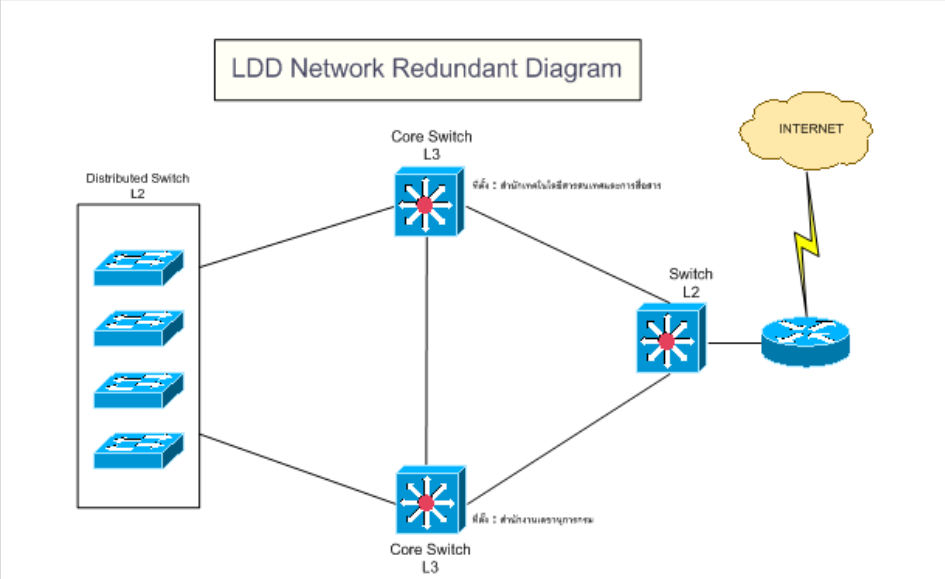


ภาพที่ ๑๓๙ การสำรองConfigure file ระบบ EIS

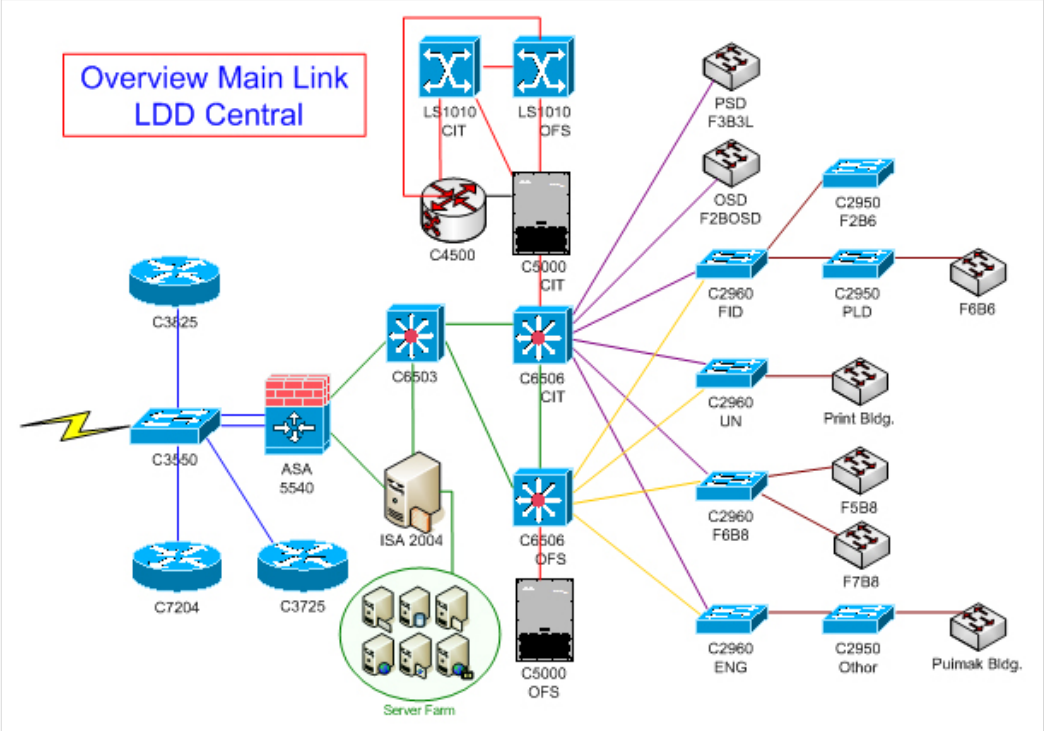
๓.๓ แผนภาพการบริหารระบบสารสนเทศและคอมพิวเตอร์ กรมพัฒนาที่ดิน



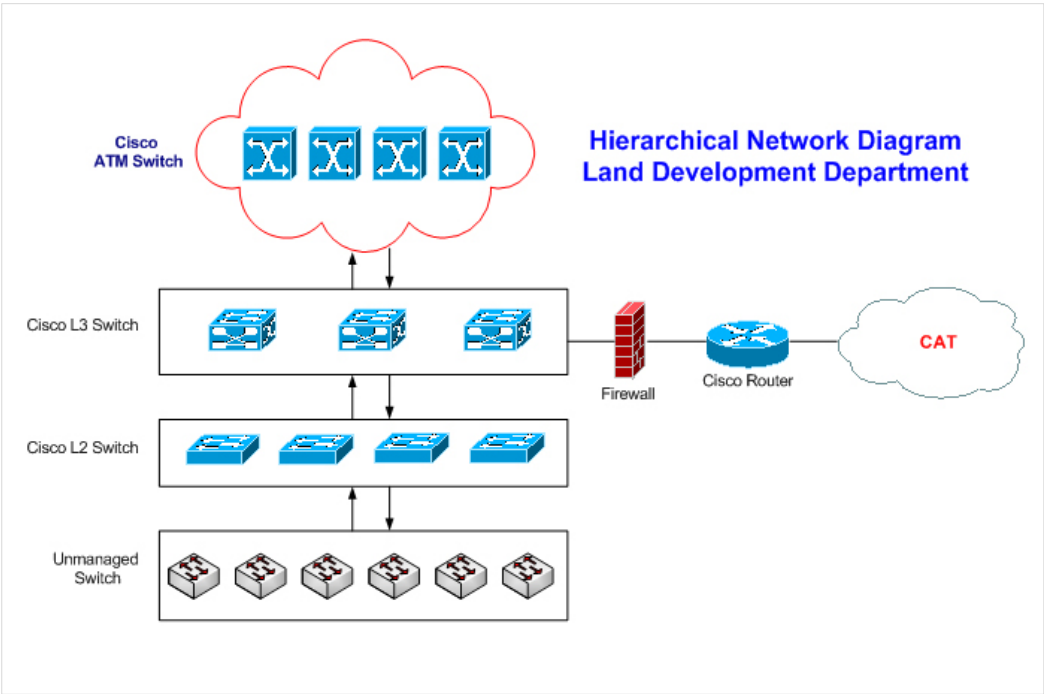
ภาพที่ ๑๔๐ ภาพรวมระบบสารสนเทศและคอมพิวเตอร์ กรมพัฒนาที่ดิน



ภาพที่ ๑๔๑ ภาพระบบ Redundant อุปกรณ์ Switch กรมพัฒนาที่ดิน



ภาพที่ ๑๔๒ ภาพรวมการเชื่อมต่ออุปกรณ์เครือข่าย กรมพัฒนาที่ดิน



ภาพที่ ๑๔๓ ภาพการเชื่อมต่อของอุปกรณ์เครือข่ายแบบชั้น กรมพัฒนาที่ดิน

บทที่ ๔
สรุปและข้อเสนอแนะ

๔.๑ สรุป

จากผลการดำเนินงาน กรมพัฒนาที่ดินจะมีคู่มือการบริหารจัดการระบบสารสนเทศและคอมพิวเตอร์ กรมพัฒนาที่ดิน (LDD Manual Management Information Systems and Computer) ตรงตามวัตถุประสงค์ที่ตั้งไว้ เพื่อให้ผู้รับผิดชอบ/ผู้ปฏิบัติงาน ได้มีความรู้ความเข้าใจเกี่ยวกับวิธีการ Configuration ระบบสารสนเทศ ระบบเครือข่าย ตลอดจน วิธีการแก้ไขปัญหาแนวทางการดำเนินงานระบบเทคโนโลยีสารสนเทศกรมพัฒนาที่ดิน ให้มีความน่าเชื่อถือ และมีเสถียรภาพ ทั้งเป็นการเพิ่มศักยภาพและความสามารถในการควบคุม , การจัดระเบียบและการบริหารระบบสารสนเทศและคอมพิวเตอร์ ให้มีประสิทธิภาพมากขึ้น ช่วยแก้ไขปัญหาในกรณีที่เจ้าหน้าที่ที่รับผิดชอบงานโดยตรงไม่สามารถมาปฏิบัติงานได้ โดยมีการสรุปรายละเอียดของระบบสารสนเทศและคอมพิวเตอร์ ดังต่อไปนี้

๔.๑.๑ ระบบเครือข่ายกรมพัฒนาที่ดิน (LDD Network System)

ระบบฯ มีความสามารถให้บริการเชื่อมต่อเข้าสู่ระบบเครือข่าย Internet ได้อย่างสะดวก สามารถเพิ่มขยาย พื้นที่จุดบริการเครือข่ายได้ในอนาคต ทำหน้าที่ควบคุมการรับส่งข้อมูลและแอพพลิเคชั่นผ่านทางการเชื่อมต่อระบบเครือข่ายอย่างมีประสิทธิภาพ รวมทั้งมีระบบควบคุม Firewall IDS IPS ที่รองรับการรักษาความปลอดภัย โดยมี Policy Filter ที่สามารถกำหนดขั้นตอนการป้องกันภัยคุกคามจากการใช้งานได้อย่างยืดหยุ่นภายใต้กลยุทธ์ด้านการรักษาความปลอดภัยแบบป้องกันตนเองที่สามารถกำหนดได้ด้วยตนเอง พร้อมทั้งมีระบบการบริหารจัดการที่ครบวงจร โดยมีฟังก์ชั่นควบคุมการเข้าใช้งาน ฟังก์ชั่นการตรวจสอบสถานะอุปกรณ์ ฟังก์ชั่นการตรวจสอบสถานะผู้ใช้งาน ฟังก์ชั่นการบำรุงรักษาและการเก็บบันทึกข้อมูลการใช้งานทั้งหมด รวมทั้งฟังก์ชั่นที่จำเป็น เพื่อช่วยให้ผู้ดูแลระบบฯ สามารถกำหนดคุณสมบัติและตรวจสอบสถานการณ์ทำงานของระบบเครือข่ายกรมพัฒนาที่ดิน (LDD Network System) ได้อย่างรวดเร็วและมีประสิทธิภาพ

๔.๑.๒ ระบบคอมพิวเตอร์บริการ กรมพัฒนาที่ดิน (LDD Server Service System)

ระบบมีประสิทธิภาพในด้านการให้บริการในด้านต่างๆ ดังต่อไปนี้

๑) การบริการระบบควบคุมโดเมน (Domain Controller) และบริการเครือข่าย (Network service) มีการควบคุมการใช้งานแบบรวมศูนย์ โดยศูนย์สารสนเทศ ให้บริการสำหรับหน่วยงานและผู้ที่มาขอรับบริการของกรมพัฒนาที่ดินส่วนกลาง

๒) การบริการระบบเวป (Web Service) ผ่านช่องทางเครือข่ายของกรมพัฒนาที่ดิน เพื่อให้ข้าราชการ พนักงานและบุคคลภายนอก สามารถเรียกใช้งานบริการดังกล่าว เพื่อเผยแพร่ข้อมูลของกรมพัฒนาที่ดิน โดยให้บริการทางด้านระบบบริหารจัดการสารสนเทศ (Management Information System : MIS) ข้อมูลทางด้านแผนที่ (Geographic Information System : GIS) ข้อมูลทางด้านการช่วยในการตัดสินใจเชิงแผนที่ (Executive Information System : EIS) และการนำเสนอผลงานวิจัยของกรมพัฒนาที่ดิน

๓) การบริการระบบเมล์ (Mail Service) ผ่านช่องทางเครือข่ายของกรมพัฒนาที่ดิน เพื่อให้ข้าราชการ พนักงาน สามารถเรียกใช้งานบริการดังกล่าว เพื่อเป็นช่องทางในการติดต่อสื่อสาร ผ่านทางโครงข่ายอินทราเน็ต (Intranet) และอินเตอร์เน็ต (Internet)

๔.๑.๓ จุดเด่นของระบบสารสนเทศและคอมพิวเตอร์ กรมพัฒนาที่ดิน

๑) ความสะดวกสบาย (Comfortable) : รองรับการทำงานร่วมกับอุปกรณ์สารสนเทศได้หลากหลายประเภท เช่น Notebook, Smartphone , Tablet และอุปกรณ์อื่นที่รองรับการเรียกเข้าใช้งานระบบเครือข่าย Internet ได้อย่างสะดวก รวดเร็ว

๒) ช่วยการเพิ่มผลผลิต (Productivity) : การเชื่อมต่อกับระบบสารสนเทศและคอมพิวเตอร์ กรมพัฒนาที่ดิน เป็นช่องทางหนึ่งให้ผลการทำงานสำเร็จมากขึ้น เนื่องจากได้รับสิทธิการเข้าถึงสำหรับผู้ใช้งาน เพื่อเข้าสู่อินเทอร์เน็ตและข้อมูลที่ต้องการของตนได้

๓) มีความปลอดภัย (Security) : การควบคุมและการจัดการการเข้าถึงระบบสารสนเทศและคอมพิวเตอร์ กรมพัฒนาที่ดิน มีระบบรักษาระบบความปลอดภัยที่แข็งแกร่ง เพื่อให้สามารถอนุญาตเฉพาะบุคคลที่ระบุและให้ใช้งานได้เฉพาะที่ระบบฯกำหนดไว้เท่านั้น

๔) เพิ่มเสถียรภาพและความน่าเชื่อถือ ให้กับระบบงานบริการต่าง ๆ ของกรมพัฒนาที่ดิน

๔.๒ ปัญหาและอุปสรรค

ในการจัดทำคู่มือการบริหารจัดการระบบสารสนเทศและคอมพิวเตอร์ กรมพัฒนาที่ดิน (LDD Manual Management Information Systems and Computer) ให้ครอบคลุมการทำงานของระบบฯ ทั้งหมดของกรมพัฒนาที่ดิน เป็นเรื่องที่มีความยุ่งยาก ซับซ้อน เนื่องจาก ระบบสารสนเทศและคอมพิวเตอร์ ของกรมพัฒนาที่ดิน มีขนาดใหญ่ มีการให้บริการทั้งในส่วนของเครือข่ายและเครื่องแม่ข่ายบริการ ที่มีปริมาณมาก ดังนั้นในการเขียนคู่มือจึงได้นำเสนอในส่วนที่เป็นหัวใจหลักของระบบฯ ที่มีความสำคัญและไม่สามารถหยุดทำงานได้ เนื่องจากจะส่งผลกับการทำงานโดยรวมของระบบฯ ซึ่งอาจจะทำให้ขาดรายละเอียดในการกำหนดค่าของระบบย่อยบางส่วนไป

๔.๓ ข้อเสนอแนะ

เนื่องจากระบบสารสนเทศและคอมพิวเตอร์ กรมพัฒนาที่ดิน ได้มีการปรับปรุงและพัฒนามาอย่างต่อเนื่อง ทั้งในส่วนของฮาร์ดแวร์ (Hardware) และซอฟแวร์ (Software) เพื่อให้ทันสมัยและรองรับการบริการสารสนเทศสมัยใหม่ ที่ต้องการความสามารถของระบบฯ ค่อนข้างสูง ดังนั้นข้อมูลในคู่มือบางส่วนอาจมีการเปลี่ยนแปลงตามอุปกรณ์หรือระบบใหม่ที่มีการติดตั้งเพิ่มเติมเข้ามา เพื่อให้ตรงตามการให้บริการของกรมฯ ที่เปลี่ยนไป โดยจะต้องมีการปรับปรุงรายละเอียดข้อบังคับในการใช้งานต่างๆ ของระบบ ทุกครั้งที่มีการเปลี่ยนแปลงค่าคุณลักษณะของงานการบริการระบบต่าง ๆ ภายในกรมฯ ซึ่งจะส่งผลให้คู่มือการบริหารจัดการระบบสารสนเทศและคอมพิวเตอร์ กรมพัฒนาที่ดิน (LDD Manual Management Information Systems and Computer) มีความทันสมัยและน่าเชื่อถือ

ภาคผนวก ก

การกำหนดค่าคอนฟิคกูเรชั่นของอุปกรณ์สวิชต์หลัก
(Core Switch Configuration)

การกำหนดค่าคอนฟิคกูเรชั่นของอุปกรณ์สวิชต์หลัก

(Core Switch Configuration)

Current configuration : ๑๖๙๒๙๔ bytes

!

upgrade fpd auto

version ๑๒.๒

service nagle

no service pad

service timestamps debug datetime msec localtime show-timezone

service timestamps log datetime msec localtime show-timezone

service password-encryption

service counters max age ๕

!

hostname C๖๕๐๖-CIT

!

boot-start-marker

boot-end-marker

!

enable secret ๕ ๑adym$fwFUsTc๔uitIgZ๙OXfFr๑๑

!

username technical privilege ๑๕ password ๗ ๐๓๓๔๕๓๑๙๐๙๐๒๒๕๔๕

username supong privilege ๑๕ password ๗ ๐๙๕F๕B๑๙๑๖๐B๑๐

username ldd privilege ๑๕ password ๗ ๑๕๑E๐F๐๘๒๔๗B๖๘๗๖

aaa new-model

aaa authentication login vty group tacacs+ local

aaa authentication dot๑x default group radius local

aaa authorization exec vty group tacacs+ local

!

aaa session-id common

clock timezone BKK ๗

call-home

  alert-group configuration

```
  alert-group diagnostic
  alert-group environment
  alert-group inventory
  alert-group syslog
 profile "CiscoTAC-๑"
   no active
   no destination transport-method http
   destination transport-method email
   destination address email callhome@cisco.com
   destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
   subscribe-to-alert-group diagnostic severity minor
   subscribe-to-alert-group environment severity minor
   subscribe-to-alert-group syslog severity major pattern ".*"
   subscribe-to-alert-group configuration periodic monthly ๑๙ ๑๖:๑๓
   subscribe-to-alert-group inventory periodic monthly ๑๙ ๑๕:๕๘
ip subnet-zero
!
!
!
ip multicast-routing
no ip domain-lookup
ip name-server ๑๐.๑.๑.๔
vtp domain LDD
vtp mode transparent
mls ip slb purge global
mls netflow interface
no mls flow ip
mls cef error action reset
!
crypto pki trustpoint TP-self-signed-๑๓๑๔
 enrollment selfsigned
```

```
 subject-name cn=IOS-Self-Signed-Certificate-๑๓๑๔
 revocation-check none
 rsakeypair TP-self-signed-๑๓๑๔
!
redundancy
 keepalive-enable
 mode sso
 main-cpu
  auto-sync running-config
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan ๑-๔๐๙๔ priority ๔๐๙๖
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
dot๑x system-auth-control
fabric timer ๑๕
!
vlan internal allocation policy ascending
vlan access-log ratelimit ๒๐๐๐
!
vlan ๒
 name Server
!
vlan ๓
 name Training
!
vlan ๔
 name GIS
!
vlan ๕
 name Management
```

```
!
vlan ๖
 name Secretary
!
vlan ๗
 name Personal
!
vlan ๘
 name Finance
!
vlan ๙
 name Planing
!
vlan ๑๐
 name SoilSurvey
!
vlan ๑๑
 name SoilAnalysis
!
vlan ๑๒
 name Catographic
!
vlan ๑๓
 name LandUse
!
vlan ๑๔
 name Conservation
!
vlan ๑๕
 name Engineer
!
vlan ๑๖
```

```
 name OFI
!
vlan ๑๗
 name Mordin
!
vlan ๑๘
 name IRV
!
vlan ๑๙
 name ONR
!
vlan ๒๐
 name WiFi
!
vlan ๒๑
 name Audit
!
vlan ๒๒
 name Dial-in
!
vlan ๒๓
 name Original
!
vlan ๒๔
 name Expert
!
vlan ๒๕
 name OSB
!
vlan ๒๖
 name Meeting-Room
!
```

```
vlan ๒๘
 name IPP
!
vlan ๒๙
 name VDO_Conf
!
vlan ๓๐
 name CIT
!
vlan ๓๓
 name CCTV
!
vlan ๕๓
 name hotspot_aruba
!
vlan ๕๔
 name hotspot_other
!
vlan ๕๕
 name hotspot_gateway
!
vlan ๖๖
 name test_hsrp
!
vlan ๗๐
 name GIN
!
vlan ๗๗
 name LDD-Region-Manage
!
vlan ๘๐
 name ldd-guest
```

```
!
vlan ๘๘
 name support
!
vlan ๙๐
 name DMZ
!
vlan ๙๑
 name NAS
!
vlan ๙๙
 name Proxy
!
vlan ๑๐๐
 name proxy๓
!
vlan ๑๙๙
 name proxy๒
!
vlan ๒๐๐
 name link_๔๕๐๐
!
vlan ๒๐๒
 name Link_๖๕๐๐
!
vlan ๓๐๐
 name Firewall_Management
!
vlan ๓๐๑
 name lan_to_firewall
!
!
```

```
!
interface Port-channel๑
 description ## Connect to C๖๕๐๖-OFS B๓RF๒ ##
 switchport
 switchport trunk encapsulation dot๑q
 switchport mode trunk
 switchport nonegotiate
!
interface Port-channel๒
 description ## Connect to C๖๕๐๖-๒๕๕๗ ##
 switchport
 switchport trunk encapsulation dot๑q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet๑/๑
 description ## Ether Channel Connect to C๖๕๐๖-OFS ##
 switchport
 switchport trunk encapsulation dot๑q
 switchport mode trunk
 switchport nonegotiate
 channel-group ๑ mode on
!
interface GigabitEthernet๑/๒
 description ## Ether Channel Connect to C๖๕๐๖-OFS ##
 switchport
 switchport trunk encapsulation dot๑q
 switchport mode trunk
 switchport nonegotiate
 channel-group ๑ mode on
!
interface GigabitEthernet๑/๓
```

```
 description ## Connect to ๒๙๖๐ ENG Rack BENG F๒ ##
 switchport
 switchport trunk encapsulation dot๑q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet๑/๔
 description ## Connect to ๒๙๕๐T UN Rack BUN F๒ ##
 switchport
 switchport trunk encapsulation dot๑q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet๑/๕
 description ## Connect to ๒๙๕๐ FID Rack B๖ F๓ ##
 switchport
 switchport trunk encapsulation dot๑q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet๑/๖
 description ## Connect to ๒๙๕๐ Land Rack B๘ F๖ ##
 switchport
 switchport trunk encapsulation dot๑q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet๑/๗
 description ## Ether Channel Connect to C๖๕๐๖-๒๕๕๗ ##
 switchport
 switchport trunk encapsulation dot๑q
 switchport mode trunk
```

```
 switchport nonegotiate
 channel-group ๒ mode on
!
interface GigabitEthernet๑/๘
 description ## Ether Channel Connect to C๖๕๐๖-๒๕๕๗ ##
 switchport
 switchport trunk encapsulation dot๑q
 switchport mode trunk
 switchport nonegotiate
 channel-group ๒ mode on
!
interface GigabitEthernet๑/๙
 no ip address
 shutdown
!
interface GigabitEthernet๑/๑๐
 no ip address
!
interface GigabitEthernet๑/๑๑
 no ip address
 shutdown
!
interface GigabitEthernet๑/๑๒
 no ip address
 shutdown
!
interface GigabitEthernet๑/๑๓
 no ip address
 shutdown
!
interface GigabitEthernet๑/๑๔
 no ip address
```

```
 shutdown
!
interface GigabitEthernet๑/๑๕
 no ip address
 shutdown
!
interface GigabitEthernet๑/๑๖
 no ip address
 shutdown
!
interface GigabitEthernet๑/๑๗
 no ip address
 shutdown
!
interface GigabitEthernet๑/๑๘
 no ip address
 shutdown
!
interface GigabitEthernet๑/๑๙
 no ip address
 shutdown
!
interface GigabitEthernet๑/๒๐
 no ip address
 shutdown
!
interface GigabitEthernet๑/๒๑
 no ip address
 shutdown
!
interface GigabitEthernet๑/๒๒
 no ip address
```

```
 shutdown
!
interface GigabitEthernet๑/๒๓
 no ip address
 shutdown
!
interface GigabitEthernet๑/๒๔
 no ip address
 shutdown
!
interface GigabitEthernet๒/๑
 description ## HP Blade Right Port ๒๐ ##
 switchport
 switchport trunk encapsulation dot๑q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet๒/๒
 description ## Link Call Manager ๑๐.๑.๒๘.๒๕๐ ##
 switchport
 switchport access vlan ๒๘
 switchport mode access
!
interface GigabitEthernet๒/๓
 description ## Link S/W Allied ๘ Ports ADMST_Kreing FL.๒ ##
 switchport
 switchport access vlan ๕
 switchport mode access
!
interface GigabitEthernet๒/๔
 description ## Link S/W UN ๒๙๖๐ port ๒๔ ##
 switchport
```

```
 switchport trunk encapsulation dot๑q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet๒/๕
 description ## Link A/P Room ADMST_Anusorn Fl.๒ ##
 switchport
 switchport access vlan ๕
 switchport mode access
!
interface GigabitEthernet๒/๖
 description ## Link to room front toilet fl.๑ bl.๓L ##
 switchport
 switchport access vlan ๒๕
 switchport mode access
!
interface GigabitEthernet๒/๗
 description ## S/W CCTV Rack๔ ##
 switchport
 switchport access vlan ๓๓
 switchport mode access
!
interface GigabitEthernet๒/๘
 description ## Aruba Port ๒ from left ##
 switchport
 switchport access vlan ๕๓
 switchport mode access
!
interface GigabitEthernet๒/๙
 description ## Aruba Port ๓ from left ##
 switchport
 switchport access vlan ๕๔
```

```
 switchport mode access
!
interface GigabitEthernet๒/๑๐
 description ## Connect PSD_HRM ##
 switchport
 switchport access vlan ๗
 switchport mode access
!
interface GigabitEthernet๒/๑๑
 description ## Server FID๑๐๑ ๑๐.๑.๗.๑ ##
 switchport
 switchport access vlan ๘
 switchport mode access
!
interface GigabitEthernet๒/๑๒
 description ## S/W TP-Link Rack ๖ : port ๒๔ ##
 switchport
 switchport access vlan ๒
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet๒/๑๓
 description ## Vlan๓๐ to CCTV Control Room B๖ F๑ IP ๑๐.๑.๓๐.๒๐๐ ##
 switchport
 switchport access vlan ๓๐
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet๒/๑๔
 description ## Aruba Port ๔ from left ##
 switchport
 switchport access vlan ๕๕
```

```
 switchport mode access
!
interface GigabitEthernet๒/๑๕
 description ## Link Firewall ๑๐.๑.๑.๑๕ : port ๑ ##
 switchport
 switchport access vlan ๒
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet๒/๑๖
 description ## HP Blade left Port ๒๑ ##
 switchport
 switchport access vlan ๒
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet๒/๑๗
 description ## Vlan๒๘ to S/W IPPhone CIT Server Room Rack๑ ##
 switchport
 switchport access vlan ๒๘
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet๒/๑๘
 description ## Vlan๑๒ to D-Link ๑๒๒๖G P๒๔ CIT Server Room Rack๑ ##
 switchport
 switchport access vlan ๑๒
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet๒/๑๙
 description ## Vlan๔ to A/P ADB Room B๓L F๒ ##
```

```
 switchport
 switchport access vlan ๔
 switchport mode access
!
interface GigabitEthernet๒/๒๐
 description ## Vlan๔ to S/W Technical Support Room CIT F๑ ##
 switchport
 switchport access vlan ๔
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet๒/๒๑
 description ## A/P Aruba ##
 switchport
 switchport access vlan ๕๓
 switchport mode access
!
interface GigabitEthernet๒/๒๒
 description ## connect S/W Vlan ๓ Peach&Tok room ##
 switchport
 switchport access vlan ๓
 switchport mode access
!
interface GigabitEthernet๒/๒๓
 description ## A/P Aruba ##
 switchport
 switchport access vlan ๕๓
 switchport mode access
!
interface GigabitEthernet๒/๒๔
 description ## A/P Aruba ##
 switchport
```

```
 switchport access vlan ๕๓
 switchport mode access
!
interface GigabitEthernet๒/๒๕
 description ## Link Proxy : ๑๐.๑.๑.๒ : port ๒ ##
 switchport
 switchport access vlan ๒
 switchport mode access
!
interface GigabitEthernet๒/๒๖
 description ## Switch TP-Link Open Rack ##
 switchport
 switchport access vlan ๒
 switchport mode access
!
interface GigabitEthernet๒/๒๗
 description ## Vlan๑๑ to S/W OSD Rack BOSD F๒ ##
 switchport
 switchport access vlan ๑๑
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet๒/๒๘
 description ## Vlan๗ to S/W PSD B๓L F๓ ##
 switchport
 switchport access vlan ๗
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet๒/๒๙
 description ## Connect to Cisco ๕๐๐๐ P๓/๙ CIT Server Room Rack๒ ##
 switchport
```

```
 switchport trunk encapsulation dot๑q
 switchport mode trunk
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet๒/๓๐
 description ## oss๑๐๑ & olp๑๐๑ ##
 switchport
 switchport access vlan ๒
!
interface GigabitEthernet๒/๓๑
 description ## LDDHOTSPOT Lobby ##
 switchport
 switchport access vlan ๕๓
 switchport mode access
!
interface GigabitEthernet๒/๓๒
 description ## Port S/W Vlan ๔ Peach&Tok Room ##
 switchport
 switchport access vlan ๔
 switchport mode access
!
interface GigabitEthernet๒/๓๓
 description ## Switch ๓COM Rack WEB LDD ##
 switchport
 switchport access vlan ๒
 switchport mode access
!
interface GigabitEthernet๒/๓๔
 description ** Qcenter **
 switchport
 switchport access vlan ๑๑
```

```
 switchport mode access
!
interface GigabitEthernet๒/๓๕
 description ## S/W TP-Link : Open Rack ๑: Port ๒๔ ##
 switchport
 switchport access vlan ๒
 switchport mode access
!
interface GigabitEthernet๒/๓๖
 description ## S/W TP-Link : Open Rack ๒: Port ๒๔ ##
 switchport
 switchport access vlan ๒
 switchport mode access
!
interface GigabitEthernet๒/๓๗
 description ## ASA๕๕๔๐ Porto/๓ or Cat๓๕๕๐ Porto/๓ ##
 switchport
 switchport access vlan ๒
 switchport mode access
!
interface GigabitEthernet๒/๓๘
 description ## Broadcast ๑๐.๑.๑.๑๔๕and ๑๐.๑.๑.๑๔๖ _ VMnet๒ ##
 switchport
 switchport access vlan ๒
 switchport mode access
!
interface GigabitEthernet๒/๓๙
 description ## Proxy Internal ๑๐.๑.๑.๒ ##
 switchport
 switchport access vlan ๒
 switchport mode access
!
```

```
interface GigabitEthernet๒/๔๐
 switchport
 switchport access vlan ๓๐๑
 switchport mode access
!
interface GigabitEthernet๒/๔๑
 switchport
 switchport access vlan ๓๐๑
 switchport mode access
!
interface GigabitEthernet๒/๔๒
 description ## Link Proxy port ๑ : ๑๐.๙๙.๑.๓ ##
 switchport
 switchport access vlan ๙๙
 switchport mode access
!
interface GigabitEthernet๒/๔๓
 description ##  Ether Channel Connect to C๖๕๐๖-๒๕๕๗ ##
 switchport
 switchport trunk encapsulation dot๑q
 switchport mode trunk
 switchport nonegotiate
 channel-group ๒ mode on
!
interface GigabitEthernet๒/๔๔
 description ##  Ether Channel Connect to C๖๕๐๖-๒๕๕๗ ##
 switchport
 switchport trunk encapsulation dot๑q
 switchport mode trunk
 switchport nonegotiate
 channel-group ๒ mode on
!
```

```
interface GigabitEthernet๒/๔๕
 description ## Link S/W SMC VDO Conf R๔ Port ๒๕ ##
 switchport
 switchport access vlan ๒๙
 switchport mode access
!
interface GigabitEthernet๒/๔๖
 description ## PF LDD Region Server ESXI ๑๐.๑.๗๗.๒๐๐ ##
 switchport
 switchport trunk encapsulation dot๑q
 switchport mode trunk
 switchport nonegotiate
 spanning-tree portfast trunk
!
interface GigabitEthernet๒/๔๗
 switchport
 switchport trunk encapsulation dot๑q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet๒/๔๘
 description ## Cisco C๓๕๖๐-CIT Port ๒๔ ##
 switchport
 switchport trunk encapsulation dot๑q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet๕/๑
 no ip address
 shutdown
!
interface GigabitEthernet๕/๒
```

```
 no ip address
 shutdown
!
interface Vlan๑
 description ## Vlan Cisco ##
 ip address ๑๐.๑.๑๐๐.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๑๐๐.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๒
 description ## Vlan Server ##
 ip address ๑๐.๑.๑.๑๐๐ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
!
interface Vlan๓
 description ## Vlan Training ##
 ip address ๑๐.๑.๒.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๒.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๔
 description ## Vlan GIS ##
 ip address ๑๐.๑.๓.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๓.๒๕๔
 standby priority ๒๐๐
```

```
!
interface Vlan๕
 description ## Vlan Management ##
 ip address ๑๐.๑.๔.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๔.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๖
 description ## Vlan Secretary ##
 ip address ๑๐.๑.๕.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๕.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๗
 description ## Vlan Personal ##
 ip address ๑๐.๑.๖.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๖.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๘
 description ## Vlan Finance ##
 ip address ๑๐.๑.๗.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๗.๒๕๔
 standby priority ๒๐๐
```

```
!
interface Vlan๙
 description ## Vlan Planing ##
 ip address ๑๐.๑.๘.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๘.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๑๐
 description ## Vlan SoilSurvey ##
 ip address ๑๐.๑.๙.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๙.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๑๑
 description ## Vlan SoilAnalysis ##
 ip address ๑๐.๑.๑๐.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๑๐.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๑๒
 description ## Vlan Catographic ##
 ip address ๑๐.๑.๑๑.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๑๑.๒๕๔
 standby priority ๒๐๐
```

```
!
interface Vlan๑๓
 description ## Vlan Landuse ##
 ip address ๑๐.๑.๑๒.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๑๒.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๑๔
 description ## Vlan Conservation ##
 ip address ๑๐.๑.๑๓.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๑๓.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๑๕
 description ## Vlan Engineer ##
 ip address ๑๐.๑.๑๔.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๑๔.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๑๖
 description ## Vlan OFI ##
 ip address ๑๐.๑.๑๕.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๑๕.๒๕๔
 standby priority ๒๐๐
```

```
!
interface Vlan๑๗
 description ## Vlan Mordin ##
 ip address ๑๐.๑.๑๖.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๑๖.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๑๘
 description ## Vlan IRV ##
 ip address ๑๐.๑.๑๗.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๑๗.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๑๙
 description ## Vlan ONR ##
 ip address ๑๐.๑.๑๘.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๑๘.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๒๐
 description ## Vlan WiFi ##
 ip address ๑๐.๑.๑๙.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๑๙.๒๕๔
 standby priority ๒๐๐
```

```
!
interface Vlan๒๑
 description ## Vlan Audit ##
 ip address ๑๐.๑.๒๐.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๒๐.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๒๒
 description ## Vlan Demo ##
 ip address ๑๐.๑.๒๑.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 shutdown
 standby ip ๑๐.๑.๒๑.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๒๓
 description ## Vlan Original ##
 ip address ๑๙๑.๒.๑.๒๕๓ ๒๕๕.๒๕๕.๐.๐
 no ip proxy-arp
 ip pim sparse-mode
 shutdown
 standby ip ๑๙๑.๒.๑.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๒๔
 description ## Vlan Expert ##
 ip address ๑๐.๑.๒๔.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
```

```
 standby ip ๑๐.๑.๒๔.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๒๕
 description ## Vlan Soil-Biotech ##
 ip address ๑๐.๑.๒๕.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๒๕.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๒๖
 description ## Vlan Meeting-Room ##
 ip address ๑๐.๑.๒๖.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๒๖.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๒๘
 description ## Vlan IPPhone ##
 ip address ๑๐.๑.๒๘.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 standby ip ๑๐.๑.๒๘.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๒๙
 description ## Vlan VDO Conference ##
 ip address ๑๐.๑.๒๙.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๒๙.๒๕๔
```

```
 standby priority ๒๐๐
!
interface Vlan๓๐
 description ## Vlan CIT ##
 ip address ๑๐.๑.๓๐.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๓๐.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๓๓
 description ## Vlan CCTV ##
 ip address ๑๐.๑.๓๓.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๓๓.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๕๕
 description ## Vlan Hotspot Gateway ##
 ip address ๑๐.๑.๕๕.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๕๕.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๗๐
 description ## Vlan GIN ##
 ip address ๑๐.๑.๗๐.๒๕๔ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
!
```

```
interface Vlan๗๗
 description ## Vlan LDD Region Management ##
 ip address ๑๐.๑.๗๗.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
 standby ip ๑๐.๑.๗๗.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๘๐
 description ## Vlan for LDD Guest ##
 ip address ๑๐.๘๐.๘๐.๒๕๔ ๒๕๕.๒๕๕.๒๕๕.๐
 ip access-group vlan๘๐ in
 no ip proxy-arp
 ip pim sparse-mode
!
interface Vlan๘๘
 description ## Vlan technical support ##
 ip address ๑๐.๑.๘๘.๒๕๔ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
!
interface Vlan๙๐
 no ip address
 ip pim sparse-mode
 shutdown
!
interface Vlan๙๑
 description ## Vlan NAS ##
 ip address ๑๐.๑.๙๑.๒๕๔ ๒๕๕.๒๕๕.๒๕๕.๐
!
interface Vlan๙๙
 description ## Vlan Proxy External ##
```

```
 ip address ๑๐.๑.๙๙.๒๕๔ ๒๕๕.๒๕๕.๒๕๕.๐
 no ip proxy-arp
 ip pim sparse-mode
!
interface Vlan๑๐๐
 ip address ๑๐.๙๘.๑.๒๕๔ ๒๕๕.๒๕๕.๒๕๕.๐
!
interface Vlan๑๙๙
 description ## Vlan Proxy External๒ ##
 ip address ๑๐.๙๙.๑.๒๕๔ ๒๕๕.๒๕๕.๒๕๕.๐
!
interface Vlan๒๐๐
 ip address ๑๐.๑๐.๑.๑๗ ๒๕๕.๒๕๕.๒๕๕.๒๔๐
 no ip proxy-arp
 ip pim sparse-mode
!
interface Vlan๒๐๒
 ip address ๑๐.๑๐.๑.๖๕ ๒๕๕.๒๕๕.๒๕๕.๒๔๐
 no ip proxy-arp
 ip pim sparse-mode
!
interface Vlan๓๐๐
 description ## Firewall_Management ##
 ip address ๑๐.๑.๒๐๓.๒๕๓ ๒๕๕.๒๕๕.๒๕๕.๐
 standby ip ๑๐.๑.๒๐๓.๒๕๔
 standby priority ๒๐๐
!
interface Vlan๓๐๑
 description ## link Core Switch to Firewall ##
 ip address ๑๐.๕.๕.๑๔ ๒๕๕.๒๕๕.๒๕๕.๒๔๘
 standby ip ๑๐.๕.๕.๑๒
!
```

```
ip classless
ip route ๐.๐.๐.๐ ๐.๐.๐.๐ ๑๐.๕.๕.๙
!
!
no ip http server
ip http authentication local
ip http secure-server
ip pim rp-address ๑๐.๕.๕.๒
ip tacacs source-interface Vlan๑
!

ip access-list extended virusblock
 permit ip host ๑๐.๑.๑๐.๒๐๑ any
 permit ip host ๑๐.๑.๑๐.๒๐๒ any
 permit ip host ๑๐.๑.๑๐.๒๐๓ any
 permit ip host ๑๐.๑.๑๐.๒๐๔ any
 permit ip host ๑๐.๑.๑๐.๒๐๕ any
ip access-list extended vlan๑๐
 permit ip any host ๖๑.๙๐.๒๐๔.๑๗๓
 permit ip host ๑๐.๑.๑๐.๑ any
 permit ip any host ๑๐.๑.๑๐.๑
 deny   udp any any eq ๑๙๐๐
 deny   tcp any any eq ๑๙๐๐
 deny   ip host ๒๓๙.๒๕๕.๒๕๕.๒๕๐ any
 deny   ip any host ๒๓๙.๒๕๕.๒๕๕.๒๕๐
 deny   ip ๑๙๒.๑๖๘.๐.๐ ๐.๐.๒๕๕.๒๕๕ any
 deny   ip any ๑๙๒.๑๖๘.๐.๐ ๐.๐.๒๕๕.๒๕๕
 permit ip host ๑๐.๑.๑๐.๒๐๐ any
 permit ip any host ๒๐๓.๑๔๘.๒๕๐.๑๘๙
 permit ip host ๑๐.๑.๑๐.๑๓๑ ๑๐.๐.๐.๐ ๐.๒๕๕.๒๕๕.๒๕๕
 permit ip any host ๑๐.๑.๑.๑
 permit ip ๑๐.๑.๑๐.๐ ๐.๐.๐.๒๕๕ ๑๙๙.๔๗.๒๑๘.๐ ๐.๐.๐.๒๕๕
```

permit ip ๑๐.๑.๑๐.๐ ๐.๐.๐.๒๕๕ ๑๙๙.๔๗.๒๑๖.๐ ๐.๐.๐.๒๕๕
permit ip host ๑๐.๑.๑๐.๑ ๑๐.๐.๐.๐ ๐.๒๕๕.๒๕๕.๒๕๕
permit ip host ๑๐.๑.๑๐.๖ ๑๐.๐.๐.๐ ๐.๒๕๕.๒๕๕.๒๕๕
permit ip host ๑๐.๑.๑๐.๗๗ any
permit ip host ๑๐.๑.๑๐.๒๕๒ any
permit ip host ๑๐.๑.๑๐.๒๕๓ any
permit ip host ๑๐.๑.๑๐.๒๕๔ any
deny tcp any any eq ๑๙๓๕
permit ip host ๑๐.๑.๑๐.๑๕๐ any
deny tcp any any eq ๔๔๕
permit tcp any any eq ๕๕๔
permit tcp any any eq ๑๗๕๕
permit tcp any any eq ๑๙๓๕
permit tcp any any eq ๒๖๓๘
permit tcp any any eq ๓๓๘๙
permit tcp any any eq ๘๐๐๕
permit tcp any any eq ๘๐๘๐
permit tcp any any eq ๘๐๘๑
permit tcp any any eq ๘๔๔๓
permit tcp any any eq ๘๘๘๘
permit tcp any any eq ๙๐๙๐
permit tcp any any eq ๙๙๙๙
permit udp any any eq ๕๕๔
permit udp any any eq ๑๗๕๕
permit udp any any eq ๑๙๓๕
permit udp any any eq ๒๙๖๗
permit udp any any eq ๓๘๒๙๓
permit udp any any eq ๓๙๙๙๙
permit udp any any eq ๗๓๕๐
permit udp any any eq ๗๓๕๑
permit udp any any eq ๗๓๕๒
permit udp any any eq ๗๓๕๓

permit udp any any eq ๘๐๘๐
permit udp any any eq ๘๘๘๘
permit udp any any eq ๙๙๙๙
deny   tcp any any eq ๕๙๓
deny   tcp any any eq ๖๖๖๗
deny   udp any any eq ๑๓๕
deny   udp any any range ๒๐๐๐ ๖๕๕๓๕
deny   tcp any any range ๒๐๐๐ ๖๕๕๓๕
permit ip ๑๐.๑.๑๐.๐ ๐.๐.๐.๒๕๕ host ๕๘.๑๔๗.๗๙.๑๓๖
permit ip ๑๐.๑.๑๐.๐ ๐.๐.๐.๒๕๕ host ๒๐๓.๑๔๔.๑๙๔.๔๕
permit ip ๑๐.๑.๑๐.๐ ๐.๐.๐.๒๕๕ host ๒๐๒.๑๔๒.๒๐๐.๑๓๑
permit ip ๑๐.๑.๑๐.๐ ๐.๐.๐.๒๕๕ host ๖๑.๑๙.๒๔๙.๑๐๓
permit ip ๑๐.๑.๑๐.๐ ๐.๐.๐.๒๕๕ host ๒๐๓.๑๑๓.๙.๑๐๔
permit ip ๑๐.๑.๑๐.๐ ๐.๐.๐.๒๕๕ host ๒๐๓.๑๑๓.๙.๑๐๕
permit ip ๑๐.๑.๑๐.๐ ๐.๐.๐.๒๕๕ host ๒๐๒.๖๐.๑๙๙.๔๔
permit ip ๑๐.๑.๑๐.๐ ๐.๐.๐.๒๕๕ host ๒๐๓.๑๔๖.๒๕๐.๒๐๐
permit ip host ๑๐.๑.๑๐.๒๒๒ ๑๐.๐.๐.๐ ๐.๒๕๕.๒๕๕.๒๕๕
permit ip host ๑๐.๑.๑๐.๒ ๑๐.๐.๐.๐ ๐.๒๕๕.๒๕๕.๒๕๕
permit ip host ๑๐.๑.๑๐.๓ ๑๐.๐.๐.๐ ๐.๒๕๕.๒๕๕.๒๕๕
permit ip host ๑๐.๑.๑๐.๔ ๑๐.๐.๐.๐ ๐.๒๕๕.๒๕๕.๒๕๕
permit ip host ๑๐.๑.๑๐.๕ ๑๐.๐.๐.๐ ๐.๒๕๕.๒๕๕.๒๕๕
permit ip host ๑๐.๑.๑๐.๗ ๑๐.๐.๐.๐ ๐.๒๕๕.๒๕๕.๒๕๕
permit ip host ๑๐.๑.๑๐.๘ ๑๐.๐.๐.๐ ๐.๒๕๕.๒๕๕.๒๕๕
permit ip host ๑๐.๑.๑๐.๙ ๑๐.๐.๐.๐ ๐.๒๕๕.๒๕๕.๒๕๕

!
logging ๑๐.๑.๑.๑๖๖
no cdp advertise-v๒
snmp-server community comro RO
tacacs-server host ๑๐.๑.๑.๙๙ timeout ๕
tacacs-server directed-request
tacacs-server key ๗ ๑๓๐๙๑๓๑๖๑๘๐๙๐๗๓๘๒E๓๐

```
!
radius-server host ๑๐.๑.๑.๙๙ auth-port ๑๘๑๒ acct-port ๑๘๑๓ key ๗
๑๓๐๙๑๓๑๖๑๘๐๙๐๗๓๘๒E๓๐
radius-server source-ports ๑๖๔๕-๑๖๔๖
!
control-plane
!
!
dial-peer cor custom
!
!
line con ๐
line vty ๐ ๔
 authorization exec vty
 login authentication vty
line vty ๕ ๑๕
!
mac-address-table static ๐๐๑a.๗๐๓๔.๒๗๔๕ vlan ๙ drop
mac-address-table static ๐๐๑a.๗๐๓๔.๒b๕๑ vlan ๙ drop
mac-address-table static ๖๐๒๑.c๐b๙.ccb๘ vlan ๓๐ drop
mac-address-table static ๘๘๓๒.๙b๖๐.cb๒๕ vlan ๓๐ drop
!
End
```

ภาคผนวก ข

การกำหนดค่าคอนฟิคกูเรชั่นของอุปกรณ์นำทาง
(Router Configuration)

การกำหนดค่าคอนฟิคกูเรชั่นของอุปกรณ์นำทาง
(Router Configuration)

```
Current configuration : ๘๙๗๗ bytes
version ๑๕.๒
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname c๓๙๒๕-ldd
!
boot-start-marker
boot-end-marker
!
!
logging buffered ๕๑๒๐๐ warnings
no logging console
!
no aaa new-model
clock timezone BKK ๗ ๐
!
ipv๖ unicast-routing
ipv๖ cef
!
no ip domain lookup
ip domain name yourdomain.com
ip cef
multilink bundle-name authenticated
!
!
crypto pki token default removal timeout ๐
!
```

```
crypto pki trustpoint TP-self-signed-๒๗๘๗๙๒๖๔๐๘
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-๒๗๘๗๙๒๖๔๐๘
 revocation-check none
 rsakeypair TP-self-signed-๒๗๘๗๙๒๖๔๐๘
!
!
license udi pid C๓๙๐๐-SPE๑๐๐/K๙ sn FOC๑๘๓๙๓JJ๒
!
interface Embedded-Service-Engine๐/๐
 no ip address
 shutdown
!
interface GigabitEthernet๐/๐
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE ๐/๐$ ## C๓๕๕๐
Port ๑๙ ##
 ip address ๑๐.๒๐๐.๑.๒๕๑ ๒๕๕.๒๕๕.๒๕๕.๐
 ip access-group blockweb in
 ip access-group blockweb out
 ip virtual-reassembly in
 load-interval ๓๐
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet๐/๑
 description Trunk port on CAT  Switch ## C๓๕๕๐ Port ๑ ##
 no ip address
 ip access-group blockweb in
 ip access-group blockweb out
 no ip redirects
 ip directed-broadcast
```

```
 no ip proxy-arp
 ip pim sparse-mode
 ip flow ingress
 load-interval ๓๐
 duplex auto
 speed auto
!
interface GigabitEtherneto/๑.๑๐
 description Connect to CAT Internet
 encapsulation dot๑Q ๕๑๒
 ip address ๖๑.๑๙.๕๒.๒๒๒ ๒๕๕.๒๕๕.๒๕๕.๒๕๒
 ip flow ingress
 ip virtual-reassembly in
 ipv๖ address ๒๐๐๑:C๓๘:๙๐๐๗:๑๓::๙๙๓๑:๒/๖๔
!
interface GigabitEtherneto/๒
 description To_FW_Dell
 ip address ๖๑.๑๙.๙๘.๒๐๑ ๒๕๕.๒๕๕.๒๕๕.๐
 duplex auto
 speed auto
 ipv๖ address ๒๐๐๑:C๓๘:๙๐๔๖:FFFF:FFFF::๑/๘๐
 ipv๖ enable
!
ip forward-protocol nd
!
ip http server
ip http access-class ๒๓
ip http authentication local
ip http secure-server
ip http timeout-policy idle ๖๐ life ๘๖๔๐๐ requests ๑๐๐๐๐
!
ip route ๐.๐.๐.๐ ๐.๐.๐.๐ ๖๑.๑๙.๕๒.๒๒๑
```

```
ip route ๑๐.๐.๐.๐ ๒๕๕.๐.๐.๐ ๖๑.๑๙.๙๘.๒๐๒
ip route ๑๐.๒๕๕.๒๕๕.๐ ๒๕๕.๒๕๕.๒๕๕.๒๔๐ ๖๑.๑๙.๙๘.๒๐๒ name
DNS_CAT_LDD
ip route ๖๑.๑๙.๙๘.๘๐ ๒๕๕.๒๕๕.๒๕๕.๒๕๕ ๖๑.๑๙.๙๘.๒๐๒
ip route ๖๑.๑๙.๙๘.๑๒๒ ๒๕๕.๒๕๕.๒๕๕.๒๕๕ ๖๑.๑๙.๙๘.๒๐๒
ip route ๖๑.๑๙.๙๘.๑๒๕ ๒๕๕.๒๕๕.๒๕๕.๒๕๕ ๖๑.๑๙.๙๘.๒๐๒
ip route ๖๑.๑๙.๙๘.๑๒๖ ๒๕๕.๒๕๕.๒๕๕.๒๕๕ ๖๑.๑๙.๙๘.๒๐๒
ip route ๖๑.๑๙.๙๘.๑๒๗ ๒๕๕.๒๕๕.๒๕๕.๒๕๕ ๖๑.๑๙.๙๘.๒๐๒
ip route ๖๑.๑๙.๙๘.๑๕๐ ๒๕๕.๒๕๕.๒๕๕.๒๕๕ ๖๑.๑๙.๙๘.๒๐๒
ip route ๖๑.๑๙.๙๘.๑๕๑ ๒๕๕.๒๕๕.๒๕๕.๒๕๕ ๖๑.๑๙.๙๘.๒๐๒
ip route ๖๑.๑๙.๙๘.๑๕๒ ๒๕๕.๒๕๕.๒๕๕.๒๕๕ ๖๑.๑๙.๙๘.๒๐๒
ip route ๖๑.๑๙.๙๘.๑๙๑ ๒๕๕.๒๕๕.๒๕๕.๒๕๕ ๖๑.๑๙.๙๘.๒๐๒
ip route ๑๗๒.๑๗.๑.๐ ๒๕๕.๒๕๕.๒๕๕.๒๔๘ ๖๑.๑๙.๙๘.๒๐๒
ip route ๑๙๒.๑๖๘.๗๐.๐ ๒๕๕.๒๕๕.๒๕๕.๐ ๖๑.๑๙.๙๘.๒๐๒
ip route ๑๙๒.๑๖๘.๗๑.๐ ๒๕๕.๒๕๕.๒๕๕.๐ ๖๑.๑๙.๙๘.๒๐๒
!
ip access-list extended blockweb
 deny   ip any host ๗๔.๑๑๔.๑๓.๙
 deny   ip host ๗๔.๑๑๔.๑๓.๙ any
 deny   ip any host ๑๔๑.๑๐๑.๑๑๘.๕๘
 deny   ip any host ๑๔๑.๑๐๑.๑๑๘.๕๙
 deny   ip any host ๑๗.๑๔๙.๑๖๐.๔๙
 deny   ip any host ๑๗.๒๕๑.๒๐๐.๗๐
 deny   ip any host ๑๙๒.๓๓.๑๔.๓๐
 deny   tcp any range ๑๓๗ ๑๓๙ any
 permit ip any any
!
ipv๖ route ๒๐๐๑:C๓๘:๙๐๔๖::/๔๘ GigabitEtherneto/๒
FE๘๐::CoEA:E๔FF:FE๘๗:๓E๖๙
ipv๖ route ::/๐ GigabitEtherneto/๑.๑๐ ๒๐๐๑:C๓๘:๙๐๐๗:๑๓::๙๙๓๑:๑
!
no cdp run
```

```
!
!
control-plane
!
!
!
line con ๐
 login local
line aux ๐
line ๒
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v๑๒๐ ssh
 stopbits ๑
line vty ๐ ๔
 privilege level ๑๕
 login local
 transport input telnet ssh
line vty ๕ ๑๕
 privilege level ๑๕
 login local
 transport input telnet ssh
!
scheduler allocate ๒๐๐๐๐ ๑๐๐๐
end
```