ระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเทอร์เน็ต
กรณีศึกษา สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ

INTERNET AUTHENTICATION SYSTEM
CASE STUDY: GEO-INFORMATICS AND SPACE TECHNOLOGY DEVELOPMENT AGENCY

โดย

วิศวะ เจนจบ

WISSAWA JENJOB

อาจารย์ที่ปรึกษา

ดร. ปานวิทย์ ธุวะนุติ

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ2
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ 2 ปีการศึกษา 2555

INTERNET AUTHENTICATION SYSTEM
CASE STUDY GEO-INFORMATICS AND SPACE TECHNOLOGY DEVELOPMENT AGENCY

WISSAWA JENJOB

A REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS OF THE COURSE
INDEPENDENT STUDY 2
MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
2/ 2012

หัวข้อ	ระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเทอร์เน็ต กรณีศึกษา สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ
นักศึกษา	นายวิศวะ เจนจบ
รหัสนักศึกษา	53660517
ปริญญา	วิทยาศาสตร์มหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	เทคโนโลยีระบบสารสนเทศ
ปีการศึกษา	2555
อาจารย์ที่ปรึกษา	ดร. ปานวิทย์ ธุวะนุติ

บทคัดย่อ

โครงการจัดทำระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเทอร์เน็ตภายในสำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน) จัดทำขึ้นเพื่อลดปัญหาคอขวดในการส่งข้อมูลของระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเทอร์เน็ตระบบเดิมให้สามารถใช้งานได้อย่างมีประสิทธิภาพยิ่งขึ้น ระบบใหม่ที่ได้จัดทำนี้ใช้เทคนิคการทำงานร่วมกันระหว่างไฟร์วอล์ (Firewall) และไดเร็คทอรี่เพื่อเก็บข้อมูลในการควบคุมและจัดการ การเข้าถึงทรัพยากรบนโดเมน (Active Directory) เพื่อตรวจสอบสิทธิ์ในการใช้งานอินเทอร์เน็ตในสำนักงานฯ ด้วยวิธีการนี้ทำให้ได้ระบบพิสูจน์ตัวตนที่สะดวกต่อการใช้งานและมีความเร็วในการใช้งานอินเตอร์เน็ตเพิ่มขึ้น เนื่องจากระบบที่พัฒนาขึ้นสามารถลดการวางอุปกรณ์เพื่อขวางระบบเครือข่ายทำให้อุปกรณ์บนเครือข่ายไม่ทำงานซ้ำซ้อนกัน แนวคิดในการพัฒนาระบบดังกล่าวนี้ สามารถนำไปใช้เป็นแนวทางในการพัฒนาและเพิ่มประสิทธิภาพให้กับระบบเครือข่ายภายในองค์กรเพื่อลดค่าใช้จ่ายในการจัดหาอุปกรณ์เครือข่ายโดยสามารถใช้อุปกรณ์ที่มีอยู่เดิมให้เกิดประโยชน์สูงสุดได้เป็นอย่างดี

Title	INTERNET AUTHENTICATION SYSTEM CASE STUDY: GEO-INFORMATICS AND SPACE TECHNOLOGY DEVELOPMENT AGENCY
Student	Mr. Wissawa Jenjob
Student ID	53660517
Degree	Master of Science
Program	Information Technology
Major	Information System Technology
Year	2555
Advisor	Dr.panwit Thuwanuti

ABSTRACT

The development of Internet Authentication System Case Study: Geo-Informatics and Space Technology Development Agency (Public Organization) is created to reduce the delay of data transmission through the exist internet authentication system. The new system is developed by using the integration capabilities of Firewall device and Active Directory to authenticate for the internet access. Using this advanced technique, the powerful internet authentication system is derived. The system provides high speed data transmission without delaying since it reduces the use of redundant devices for blocking network access. This concept gives an idea of making full and efficiency use of available network resources, which can be utilized to establish a low-cost and high- efficiency network system in other organizations.

กิตติกรรมประกาศ

การพัฒนาระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเทอร์เน็ต กรณีศึกษาสำนักงานพัฒนาเทคโนโลยีอวกาศ และภูมิสารสนเทศ ประสบความสำเร็จลุล่วงได้ด้วยดี ด้วยความอนุเคราะห์และคำปรึกษาจากหลายฝ่าย ผู้จัดทำจึงขอขอบคุณในความช่วยเหลือ ดังนี้

ขอขอบคุณ อาจารย์ที่ปรึกษา ดร. ปานวิทย์ ธุวะนุติ ที่ให้คำปรึกษาเกี่ยวกับการเชื่อมต่อระบบและการนำอุปกรณ์ทางด้านเครือข่ายมาประยุกต์ใช้งานร่วมกัน เป็นแนวทางให้ผู้ใช้งานอินเทอร์เน็ตทำการพิสูจน์ตัวตนก่อนการใช้งานและก่อให้เกิดแนวคิดในการทำระบบนี้ขึ้น

ขอขอบคุณ คุณยรรยง ลูกศร หัวหน้าฝ่ายบริหารเครือข่ายและการสื่อสาร สำนักงานพัฒนาเทคโนโลยีอวกาศ และภูมิสารสนเทศ ที่ให้ความสนับสนุนการจัดทำระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเทอร์เน็ตเพื่อนำไปใช้งานในองค์กร โดยชี้แนะการตั้งค่าอุปกรณ์ทางด้านเครือข่ายและอนุญาตให้ใช้งานอุปกรณ์ทางด้านเครือข่ายของสำนักงานสำหรับการจัดทำระบบทำระบบพิสูจน์ตัวตนด้วย

ขอบคุณรุ่นพี่ เพื่อนร่วมชั้นเรียน สาขาเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุก ๆ คน ที่ให้ความช่วยเหลือ และให้คำแนะนำต่าง ๆ ตลอดจนให้กำลังใจในการศึกษาเสมอมา

คุณงามความดีอันใดที่เกิดประโยชน์ต่อเอกสารการศึกษาอิสระฉบับนี้ ข้าพเจ้าขอมอบให้แก่บิดาและมารดา อันเป็นที่รักและเคารพยิ่งของข้าพเจ้า ตลอดจนครูอาจารย์ที่เคารพทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้ให้แก่ข้าพเจ้า

วิศวะ เจนจบ

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญรูป

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

ระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเทอร์เน็ต กรณีศึกษาสำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ เพื่อการแก้ปัญหาที่เกิดขึ้นกับการใช้งานระบบพิสูจน์ตัวตนระบบเดิมให้มีประสิทธิภาพมากยิ่งขึ้น

1.1 ความเป็นมาของโครงการ

ปัจจุบันมีการนำระบบสารสนเทศมาใช้เพื่อเพิ่มประสิทธิภาพการทำงานในองค์กรมากขึ้น องค์กรภาครัฐและองค์กรภาคเอกชนล้วนให้ความสำคัญกับระบบสารสนเทศทั้งสิ้น เห็นได้ชัดจากการจัดตั้งแผนกสารสนเทศเพื่อบริหารจัดการงานด้านสารสนเทศในองค์กร งานด้านการบริหารเครือข่ายเป็นงานหนึ่งในแผนกสารสนเทศที่มีความสำคัญเช่นกัน โดยมีหน้าที่บริหารเครือข่ายให้ผู้ใช้งานภายในองค์กรสามารถใช้งานเครือข่ายได้อย่างเต็มประสิทธิภาพและสอดคล้องกับ พ.ร.บ. ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ 2550 ด้วยปัจจัยดังกล่าว การบริหารเครือข่ายที่ดีและมีประสิทธิภาพจำเป็นต้องตรวจสอบการเข้าใช้งานอินเทอร์เน็ตของผู้ใช้งานภายในระบบเสมอ ทั้งนี้เพื่อประโยชน์ในการตรวจสอบช่องสัญญาณอินเทอร์เน็ต (Internet Bandwidth) และการอ้างอิงเพื่อการฟ้องร้องทางกฎหมาย

ระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตระบบเดิมเป็นระบบที่สำนักงานฯ ได้ทำการจัดซื้อระบบมาใช้งาน ระบบดังกล่าวประกอบด้วยอุปกรณ์ระบบพิสูจน์ตัวตน (Authentication) ล็อก (Log) และการจัดการผู้ใช้งาน (User Management) ซึ่งระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตระบบเดิมนี้จะวางขวางระบบเครือข่าย โดยติดตั้งในตำแหน่งที่อยู่ก่อนไฟร์วอลล์ (Firewall) หลัก ก่อให้เกิดปัญหาที่ระบบ กล่าวคือ เมื่อมีการส่งข้อมูลที่มีขนาดใหญ่ เช่น ข้อมูลภาพถ่ายจากดาวเทียม ข้อมูลดังกล่าวจะถูกส่งไปยังปลายทางได้ช้าลง และก่อให้เกิดปัญหาการแมพไอพีแอดเดรส (Map IP address) ภายในสำนักงานฯ ซึ่งโดยปกติจะทำการผูกไอพีแอดเดรสภายนอกกับภายในไว้ที่ไฟร์วอลล์หลัก การที่ระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตระบบเดิมมีไฟร์วอลล์อยู่ภายในตัวระบบ จึงทำให้ไม่สามารถใช้งานไอพีแอดเดรสที่ผูกกันได้ ต้องติดต่อประสานงานเพื่อแจ้งบริษัทผู้รับผิดชอบระบบให้มาดำเนินการแก้ไข นอกจากนี้ ระบบดังกล่าวมีฐานข้อมูลผู้ใช้ในระบบการจัดการข้อมูลผู้ใช้ที่ไม่เชื่อมต่อกัน ทำให้สำนักงานฯ ซึ่งมีที่ตั้งอยู่ 3

สาขา และทุกสาขามีระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตระบบเดิมติดตั้งอยู่ไม่สามารถเชื่อมโยงข้อมูลผู้ใช้ร่วมกันได้ เมื่อมีการเพิ่มข้อมูลผู้ใช้งานเข้าสู่ระบบจะต้องทำการเพิ่มข้อมูลให้กับทุกสาขาทุกครั้ง ก่อให้เกิดความไม่สะดวกในการใช้งาน เนื่องจากฐานข้อมูลผู้ใช้ทั้ง 3 สาขาไม่สามารถสำเนาถึงกัน ตลอดจนการตรวจสอบล็อกการใช้งานเพื่อช่วยในการแก้ไขปัญหาที่เกิดจากการใช้งานระบบเครือข่ายไม่สามารถทำได้โดยตรง เช่น เมื่อมีการใช้งานแบนด์วิธ (Bandwidth) มากเกินไปทำให้ระบบไม่สามารถส่งข้อมูลได้ตามต้องการของผู้ใช้ ในกรณีนี้สำนักงานฯ จำเป็นต้องติดต่อประสานงานไปยังบริษัทผู้ดูแลระบบเพื่อแจ้งขอตรวจสอบข้อมูลล็อก การใช้งานแบนด์วิธในแต่ละเครื่องโดยที่สำนักงานฯ ไม่สามารถตรวจสอบข้อมูลล็อกเองได้

จากปัญหาดังกล่าว จึงได้มีแนวคิดในการพัฒนาระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตโดยใช้อุปกรณ์ไฟร์วอลล์หลัก คือ Fortigate 620b Application Firewall เพื่อพิสูจน์ตัวตนและสร้างระบบการจัดการข้อมูลผู้ใช้ (User Management) ขึ้นใหม่ โดยใช้แอคทีฟไดเร็กทอรี (Active Directory) ของ Microsoft Windows เก็บข้อมูลรายชื่อผู้ใช้งานและทำการสำเนาข้อมูลผู้ใช้งานทุกสาขา ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านของตัวเองได้ และระบบไฟร์วอลล์สามารถที่จะระบุตัวตนผู้ใช้งานอินเตอร์เน็ตที่มีการใช้งานอินเทอร์เน็ตจำนวนมากได้ด้วยความรวดเร็ว ลดการนำอุปกรณ์วางขวางระบบ ทำให้เกิดการโอเวอร์เฮด (Over Head) น้อยลงด้วยความสามารถของตัวไฟร์วอลล์เองที่มีทรูพุต (Throughput) สูง จึงแก้ปัญหาของการส่งข้อมูลที่มีขนาดใหญ่ได้

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

1.2.1 เพื่อแก้ไขปัญหาเดิมที่เกิดขึ้นจากการใช้งานระบบระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตเดิมขององค์กร

1.2.2 เพื่อวิเคราะห์และออกแบบระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตระบบใหม่

1.2.3 เพื่อพัฒนาระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตที่ง่ายต่อการใช้งาน แก้ปัญหางานด้านเครือข่ายให้มีประสิทธิภาพมากขึ้น

1.2.4 เพื่ออำนวยความสะดวกให้แก่เจ้าหน้าที่ดูแลระบบในการค้นหาข้อมูลการใช้งานอินเทอร์เน็ตของเจ้าหน้าที่ภายในหน่วยงาน ให้สามารถค้นหาได้อย่างรวดเร็ว

1.2.5 เพื่อใช้งานอุปกรณ์ในสำนักงานให้เกิดความคุ้มค่าสูงสุด ลดค่าใช้จ่ายในการจัดซื้อและค่าบำรุงรักษารายปี

1.2.6 เพื่อให้เป็นไปตาม พ.ร.บ. ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ 2550

1.3 ขอบเขตของโครงการ

1.3.1 ออกแบบสถาปัตยกรรมและโครงสร้างพื้นฐานของระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ต

1.3.2 สร้างระบบจัดเก็บบัญชีรายชื่อผู้ใช้ด้วยแอคทีฟไดเร็กทอรีและเชื่อมต่อระบบแอพพลายแอนซ์ไฟร์วอลล์ (Appliance Firewall) เข้ากับแอคทีฟไดเร็กทอรี

1.3.3 สร้างการทำสำเนาข้อมูลบัญชีรายชื่อของเจ้าหน้าที่ภายในแอคทีฟไดเร็กทอรีของสำนักงานฯ ทุกสาขา

1.3.4 ออกแบบและพัฒนาเว็บแอปพลิเคชั่นสำหรับการกรอกข้อมูลในการเข้าใช้อินเทอร์เน็ตและเว็บแอปพลิเคชั่นสำหรับการเปลี่ยนรหัสผ่านของผู้ใช้

1.4 ขั้นตอนของการดำเนินการ

1.4.1 ศึกษาความเป็นไปได้ในการพัฒนาระบบระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตด้วยอุปกรณ์ Fortigate Appliance Firewall ร่วมกับแอคทีฟไดเร็กทอรี

1.4.2 ออกแบบสถาปัตยกรรมและโครงสร้างพื้นฐานของระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ต

1.4.3 สร้างโดเมนคอนโทรลเลอร์ (Domain Controller) เพื่อใช้งานแอคทีฟไดเร็กทอรี ซึ่งเป็นไดเร็กทอรีเซอร์วิส (Directory Service) สำหรับจัดเก็บรายชื่อผู้ใช้งาน รวมทั้งรหัสผ่านบน Microsoft Windows Server 2003

1.4.4 สร้างหน่วยจัดการ (Organization Unit) เพื่อจัดเก็บบัญชีรายชื่อของผู้ใช้งานไว้เป็นกลุ่ม ๆ

1.4.5 เชื่อมต่อ Fortigate Appliance Firewall กับแอคทีฟไดเร็กทอรีเพื่อให้แอพพลาย-แอนซ์ไฟร์วอลล์สื่อสารกับแอคทีฟไดเร็กทอรีได้

1.4.6 ออกแบบและพัฒนาเว็บแอปพลิเคชั่นสำหรับติดต่อกับแอคทีฟไดเร็กทอรีโดยตรงเพื่อให้ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านเองได้

1.4.7 ออกแบบและพัฒนาส่วนติดต่อผู้ใช้ในการล็อกอินให้ใช้งานง่ายและมีความน่าสนใจ โดยสามาถนำข่าวสารสำคัญภายในสำนักงานแสดงด้วยได้

1.4.8 สร้างการทำสำเนาข้อมูลบัญชีรายชื่อของเจ้าหน้าที่ภายในแอคทีฟไดเร็กทอรีของสำนักงานฯ ทุกสาขา

1.4.9 ทดสอบระบบ

1.4.10 วิเคราะห์ผลจากการทดสอบและสรุปผลการทดสอบ

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 ได้ระบบระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตที่สะดวกต่อการใช้งาน

1.5.2 แก้ไขปัญหาความเร็วในการใช้งานอินเทอร์เน็ตที่ช้าเนื่องจากการวางขวางของระบบเดิม

1.5.3 สามารถตรวจสอบล็อกได้เองโดยไม่จำเป็นต้องแจ้งบริษัทผู้รับผิดชอบดูแลอุปกรณ์เพื่อขอให้ถอดข้อมูลที่ต้องการ

1.5.4 สามารถแก้ไขหน้าล็อกอิน (Login) ได้เอง สามารถเพิ่มข่าวสำคัญได้โดยไม่ต้องแจ้งบริษัท

1.5.5 ข้อมูลบัญชีรายชื่อของผู้ใช้งานมีการทำสำเนาข้อมูลไว้เหมือนกันในทุกเครื่องที่ให้บริการไดเร็กทอรีเซอร์วิสจึงทำให้การแก้ไขข้อมูลรหัสผ่านเหมือนกันจึงเกิดความสะดวกในการปฏิบัติงานต่างสาขา

1.5.6 ลดค่าใช้จ่ายในการบำรุงรักษาอุปกรณ์รายปี

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

2.1 ไฟร์วอลล์

ไฟร์วอลล์ คือ เครื่องมือที่ใช้ในการป้องกันเน็ตเวิร์ก (Network) จากการสื่อสารทั่วไปที่ไม่ได้รับอนุญาตโดยเครื่องมือนี้อาจจะเป็นฮาร์ดแวร์ (Hardware) หรือ ซอฟต์แวร์ (Software) หรือทั้งสองรวมกันขึ้นอยู่กับวิธีการ หรือ สถาปัตยกรรมไฟร์วอลล์ (Firewall Architecture) ที่ใช้ ไฟร์วอลล์เป็นเครื่องมือที่ทำหน้าที่รักษาความปลอดภัยในเชิงการป้องกัน (Protect) ซึ่งจะทำหน้าที่ควบคุมการเข้าถึงเน็ตเวิร์ก (Access Control) โดยอาศัยกฎพื้นฐาน (Rule Base) ปัญหาความปลอดภัยของเน็ตเวิร์ก คือ การควบคุมการเข้าถึงระบบหรือข้อมูลภายในเน็ตเวิร์กซึ่งก่อนที่จะเกิดการเข้าถึงตรรกะ (Logical Access) ได้นั้น ต้องทำการสร้างการเชื่อมต่อตรรกะ (Logical Connection) และการเชื่อมต่อนั้นต้องใช้โปรโตคอล (Protocol) ดังนั้นไฟร์วอลล์จึงจะทำหน้าที่ตรวจสอบการเชื่อมต่อภายในเครือข่ายให้เป็นไปตามกฎ

2.1.1 คุณสมบัติของไฟร์วอลล์

คุณสมบัติทั่วไปของไฟร์วอลล์ นั้นจะมีอยู่ 3 อย่างด้วยกันคือ

2.1.1.1 Protect ไฟร์วอลล์ เป็นเครื่องมือที่ทำงานในเชิงการป้องกัน โดยกลุ่มข้อมูล (Packet) ที่สามารถผ่านเข้า-ออกได้นั้น จะต้องเป็นกลุ่มข้อมูลที่ไฟร์วอลล์ เห็นว่าปลอดภัย หากกลุ่มข้อมูลใดที่ไฟร์วอลล์ เห็นว่าไม่ปลอดภัย ไฟร์วอลล์จะไม่อนุญาตให้ผ่าน โดยการตัดสินว่ากลุ่มข้อมูลปลอดภัยหรือไม่นั้นขึ้นอยู่กับ กฎพื้นฐานที่ผู้ดูแลระบบคอมพิวเตอร์ (Administrator) ได้กำหนดไว้

2.1.1.2 Access Control ไฟร์วอลล์ จะควบคุมการเข้าถึงของเครื่องผู้ใช้งานต่างๆ ให้เป็นไปตามกฎพื้นฐานตามที่ผู้ดูแลระบบคอมพิวเตอร์ได้กำหนดไว้

2.1.1.3 Rule Base ไฟร์วอลล์ จะทำการควบคุมการเข้าถึงโดยอาศัยการเปรียบเทียบคุณสมบัติของกลุ่มข้อมูลที่จะผ่านเข้า-ออก กับกฎพื้นฐานที่ผู้ดูแลระบบคอมพิวเตอร์ได้กำหนดไว้ หากพบว่าไม่มีกฎห้ามไว้ก็จะอนุญาตให้ผ่านไปได้ แต่ถ้ามีกฎข้อใดข้อหนึ่งห้ามจะไม่ยอมให้ผ่าน

2.1.2 ประเภทของไฟร์วอลล์

ประเภทของไฟร์วอลล์แบ่งตามเทคโนโลยีที่ใช้ในการตรวจสอบและควบคุมได้ 3 ชนิด คือ

2.1.2.1 Packet Filtering เป็นไฟร์วอลล์พื้นฐานที่ควบคุมข้อมูลจราจรบนระบบเครือข่ายให้เป็นไปตามทางที่เหมาะสมเพียงทางเดียว โดยอาศัยการตรวจสอบข้อมูลที่ปรากฏ

อยู่เปรียบเทียบกับเงื่อนไขที่กำหนดไว้ไฟร์วอลล์ประเภทนี้ส่วนมากจะติดตั้งอยู่บนเราท์เตอร์ (Router) จึงเรียกไฟร์วอลล์ชนิดนี้ว่า Screening Router

ข้อดีของ Screening Router

- ราคาถูกเพราะเป็นคุณสมบัติที่มีในเราท์เตอร์อยู่แล้ว
- หากเน็ตเวิร์กไม่ใหญ่มากนักสามารถใช้งานแทนไฟร์วอลล์ได้
- การใช้ Screening Router ควบคู่กับไฟร์วอลล์จะช่วยแบ่งภาระของไฟร์วอลล์ได้มากยิ่งขึ้น
- สามารถใช้ป้องกันบางประเภทที่ไฟร์วอลล์ไม่สามารถป้องกันได้

ข้อเสียของ Screening Router

- การใช้งานยาก และไม่มีมาตรฐานกลาง
- ไม่สามารถกำหนดกฎที่ซับซ้อนได้ และมีความสามารถจำกัด
- อาจทำให้เน็ตเวิร์กช้าได้

2.1.2.2 Circuit-Level (Stateful Inspection Firewall) เป็นไฟร์วอลล์ที่ทำงานโดยที่สามารถเข้าใจสถานะของการสื่อสารทั้งกระบวนการ โดยแทนที่จะดูข้อมูลจากเฮดเดอร์ (Header) เพียงอย่างเดียว Stateful Inspection ไฟร์วอลล์ จะนำเอาส่วนข้อมูลของแพกเกต (Packet) (Message Content) และข้อมูลที่ได้จากแพกเกตก่อนหน้านี้ที่ได้ทำการบันทึกเอาไว้ นำมาพิจารณาด้วย จึงทำให้สามารถระบุได้ว่าแพกเกตใดเป็นแพกเกตที่ติดต่อเข้ามาใหม่หรือว่าเป็นส่วนหนึ่งของการเชื่อมต่อที่มีอยู่แล้ว ตัวอย่าง ผลิตภัณฑ์ทางการค้าที่ใช้ Stateful Inspection Technology ได้แก่ Check Point Firewall-1 Cisco Secure Pix Firewall SunScreen Secure Net และส่วนที่เป็น Open Source แจกฟรี ได้แก่ NetFilter ใน Linux (Iptables ในลีนุกซ์เคอร์เนล 2.3 เป็นต้นไป)

ข้อดีของ Stateful Inspection ไฟร์วอลล์

- ใช้งานง่าย เพราะถูกออกแบบมาทำหน้าที่ไฟร์วอลล์โดยเฉพาะ
- ประสิทธิภาพสูง เพราะถูกออกแบบมาทำหน้าที่ไฟร์วอลล์โดยเฉพาะ
- สามารถทำ IDS เพื่อป้องกันการโจมตีได้
- การกำหนด Access Ruleทำได้ง่าย
- สามารถเพิ่มบริการอื่นๆได้
- มีความสามารถในการทำ Authentication
- การสื่อสารระหว่าง Firewall กับ Administration Console มีความปลอดภัยสูง

ข้อเสียของ Stateful Inspection ไฟร์วอลล์

- ราคาแพง
- มีความเสี่ยงต่อการถูกเจาะระบบในระดับระบบปฏิบัติการ (Operation System) ที่ตัวไฟร์วอลล์ติดตั้ง

- ผู้ใช้จำเป็นต้องอาศัยผู้ผลิตค่อนข้างมาก โดยเฉพาะไฟร์วอลล์ประเภทอุปกรณ์เครือข่ายสื่อสาร (Network Appliance) คือ เป็นทั้งซอฟต์แวร์และฮาร์ดแวร์

2.1.2.3 Application Level Firewall (Proxy) เป็นโปรแกรมประยุกต์ (Application Programme) ที่ทำงานอยู่บนไฟร์วอลล์ที่ตั้งอยู่ระหว่างเน็ตเวิร์กสองเน็ตเวิร์ก ทำหน้าที่เพิ่มความปลอดภัยของระบบเน็ตเวิร์กโดยการควบคุมการเชื่อมต่อระหว่างเน็ตเวิร์กภายในและภายนอก พร็อกซี (Proxy) จะช่วยเพิ่มความปลอดภัยได้มากเนื่องจากมีการตรวจสอบข้อมูลถึงในระดับของแอพพลิเคชันเลเยอร์ (Application Layer) ลักษณะการทำงานของแอพพลิเคชันเลเยอร์ไฟร์วอลล์นั้น คือ เมื่อไคลเอนต์ (Client) ต้องการใช้บริการภายนอก ไคลเอนต์จะทำการติดต่อไปยังพร็อกซีก่อนไคลเอนต์จะเจรจาต่อรอง (Negotiate) กับพร็อกซี เพื่อให้พร็อกซีติดต่อไปยังเครื่องปลายทางให้เมื่อพร็อกซีติดต่อไปยังเครื่องปลายทางให้แล้วจะมีการเชื่อมต่อ (Connection) สองการเชื่อมต่อคือ ไคลเอนต์กับพร็อกซี และพร็อกซี กับเครื่องปลายทาง โดยที่พร็อกซีจะทำหน้าที่รับข้อมูลและส่งต่อข้อมูลให้ในสองทิศทาง ทั้งนี้พร็อกซีจะทำหน้าที่ในการตัดสินใจว่าจะให้มีการเชื่อมต่อกันหรือไม่หรือจะส่งต่อแพกเกตให้หรือไม่

ข้อดีของ Application Level Firewall (Proxy)

- สามารถควบการติดต่อสื่อสารระหว่างอินเตอร์เน็ต (Internet) กับเน็ตเวิร์กในระดับแอพพลิเคชัน (Application) เท่านั้น ทำให้ลดความเสี่ยงที่จะถูกคุกคามในระดับเน็ตเวิร์ก-เลเยอร์ (Network Layer)

- สามารถเพิ่มหน้าที่อย่างอื่นเข้าไปได้ เช่นการควบคุมการเข้าใช้งานเว็บไซต์ที่ไม่ต้องการได้

- สามารถทำการแคชข้อมูลไว้ที่ตัวพร็อกซีสำหรับข้อมูลที่ใช้บ่อย ทำให้เพิ่มความเร็วในการใช้งานในครั้งต่อไป

- การใช้งานแบนด์วิธมีประสิทธิภาพสูงขึ้น

- มีความสามารถในการตรวจสอบผู้ใช้ (User Authentication)

- มีความสามารถในการกลั่นกรองเนื้อหาได้ (Content Filtering)

ข้อเสียของ Application Level Firewall (Proxy)

- ใช้ได้กับแอพพลิเคชันบางตัวเท่านั้น

- ไม่สามารถใช้งานกับแอพพลิเคชันที่ต้องการการสื่อสารโดยตรงจากต้นจนจบ

- เสี่ยงต่อการละเมิดความเป็นส่วนตัว

- จำเป็นต้องมีพร็อกซีหลายตัวหากต้องการใช้งานหลายแอพพลิเคชัน

- อาจเป็นสาเหตุให้เกิดปัญหาคอขวดได้

- เสี่ยงต่อการโดนโจมตีแบบ Denial of Service (DoS)

2.1.2.4 ความแตกต่างของ Hardware Firewall และ Software Firewall Hardware Firewall เป็นอุปกรณ์ที่มีความเร็วในการทำงานสูงและมีความปลอดภัยสูงและมีทรูพุทที่สูง เนื่องจากการออกแบบฮาร์ดแวร์ที่ถูกออกแบบมาโดยเฉพาะ การโจมตีจึงทำได้ยากและไม่คุ้มค่าที่นักเจาะระบบคอมพิวเตอร์ (Hacker) จะทำการเจาะระบบ เพราะ Hardware Firewall นั้นถูกพัฒนาด้วยวิธีการเฉพาะสำหรับฮาร์ดแวร์นั้น ๆ จึงจำเป็นต้องมีความรู้ความเข้าใจในกระบวนการของฮาร์ดแวร์ในระดับล่างสุด Hardware Firewall จึงเหมาะอย่างยิ่งเพื่อใช้ประโยชน์ ดังนี้

- เป็นจุดผ่านของโซน (Zone) ของเซิร์ฟเวอร์ฟาร์ม Server Farm
- เป็นจุดผ่านทางของแพกเกตที่ต้องมีการเข้ารหัส (Encryption) ที่วิ่งผ่าน Local-Area Connection เช่น IPSec ซึ่งเป็นการใช้ประโยชน์จากการออกแบบในลักษณะ ASIC หรือ Application Specific Integrated Circuit
- เป็นตัวป้องกันโซนที่มีลักษณะของการถูกโจมตีแบบไม่หลากหลาย เนื่องจากเป็นโซนของการให้บริการหรือขอรับบริการกับโลกภายนอกแบบคาดเดาได้ โดยส่วนมากคือเซิร์ฟเวอร์ฟาร์ม เช่น FTP Server และ Web Server อาจจะกล่าวได้ว่า ความแข็งแกร่งและความรวดเร็วของ Hardware Firewall เหมาะสมเป็นอย่างยิ่งกับการปกป้องพื้นที่สำคัญที่มีการให้บริการในลักษณะของการให้บริการซ้ำๆ อย่างเซิร์ฟเวอร์ฟาร์ม Software Firewall มีข้อดี คือ ความหลากหลาย ซึ่งจุดนี้คือจุดแข็งของไฟร์วอลล์ชนิดนี้ทำให้ Software Firewall นั้นเหมาะสำหรับการใช้งานโดยส่วนมาก ดังนี้
- เป็นประตูกั้นระหว่างผู้ใช้งานภายในองค์กร กับระบบเครือข่ายภายนอก เช่น อินเตอร์เน็ตซึ่งมีวิธีการจู่โจมระบบในรูปแบบใหม่ ๆ รายวันไฟร์วอลล์ที่จะมารับมือกับการคุกคามต่าง ๆ เหล่านี้จึงแทบจะต้องปรับเปลี่ยนกันแบบรายวัน
- เป็นประตูกั้นระหว่างผู้ใช้ (User) กับ ผู้ใช้ด้วยกันเอง เช่นกั้นระหว่าง Wireless LAN User กับ Wired LAN User เหตุผลที่ Software Firewall เหมาะสำหรับการปกป้องในรูปแบบนี้เพราะภัยที่มากับพฤติกรรมการใช้งานของผู้ใช้นั้นค่อนข้างมีความหลากหลาย ยากแก่การคาดเดาและยังเป็นพื้นที่ที่ไม่มีกฎเกณฑ์ตายตัวและควบคุมได้ยาก จึงต้องใช้ไฟร์วอลล์ที่สามารถปรับตัวได้ดีและเร็วแบบซอฟแวร์ซึ่งสามารถทำงานร่วมกับ Third Party Solution ได้มากมายไม่ว่าจะเป็น Anti-Virus Engine ชั้นนำเพื่อให้เกิดความปลอดภัยอย่างสมบูรณ์ที่สุด

2.2 ระบบปฏิบัติการวินโดวส์เซิร์ฟเวอร์ 2003

ระบบปฏิบัติการ Windows Server 2003 เป็นระบบปฏิบัติการที่ออกแบบและพัฒนาขึ้นเพื่อรองรับการให้บริการ (Services) ต่างๆ กับผู้ใช้มากมาย ไม่ว่าจะเป็นบริการผ่านทางอินเตอร์เน็ตหรืออินทราเน็ต (Intranet) เช่น บริการไฟล์แชร์ (File Server) บริการเว็บไซต์ (Web Server) บริการ

ควบคุมเครื่องพิมพ์ (Print Server) บริการฐานข้อมูลไดเร็กทอรี่ (Directory Server) นอกจากนี้ยังมีบริการอีกมากมายที่ไม่ได้กล่าวถึงในที่นี้ซึ่งสามารถตรวจสอบได้จาก http://www.microsoft.com ระบบปฏิบัติการ Windows Server 2003 มีความแข็งแกร่งเพียงพอที่จะรองรับงานเชิงธุรกิจและรับแอพพลิเคชันใหญ่ๆได้ โดยมีแนวคิดหลักของระบบปฏิบัติการดังนี้

2.2.1 การขยายออกได้ (Extensibility) ตัวระบบมีความยืดหยุ่นและง่ายต่อการเพิ่มขยายเพื่อรองรับความต้องการในอนาคตของผู้ใช้งานได้

2.2.2 การเคลื่อนย้ายได้ (Portability) สามารถเคลื่อนย้ายไปทำงานในแพลตฟอร์ม (Platform) ของตัวประมวลผล (Processor) อื่นได้

2.2.3 แอพพลิเคชันที่ทำงานภายใต้ Windows Server 2003 ต้องสามารถใช้ประโยชน์จากเครื่องคอมพิวเตอร์ที่มีหลายตัวประมวลผลได้อย่างเต็มประสิทธิภาพ (Multiprocessing and Scalability)

2.2.4 ความเชื่อถือได้และความทนทาน (Reliability and Robustness) ระบบปฏิบัติการมีเสถียรภาพสูง สามารถป้องกันข้อผิดพลาดอันเกิดจากกระบวนการภายในและจากแอพพลิเคชันภายนอกได้ ระบบจะต้องอยู่ในสถานะที่สามารถควบคุมได้ตลอดเวลา หากเกิดข้อผิดพลาดขึ้นระบบต้องสามารถรายงานได้อย่างถูกต้องและความผิดพลาดของแอพพลิเคชันจะต้องไม่มีผลต่อการทำงานของระบบปฏิบัติการโดยรวม นอกจากนี้ ระบบปฏิบัติการยังต้องมีอำนาจเต็มที่ในการควบคุมแอพพลิเคชัน ได้แก่ การสั่งหยุดแอพพลิเคชันที่ทำให้เกิดปัญหาต่อระบบและสามารถเรียกค้นทรัพยากรระบบทั้งหมด เช่น หน่วยความจำให้กลับมาคืนสู่ระบบได้

2.2.5 มีระบบรักษาความปลอดภัยที่ดี (Security) ระบบต้องสามารถตรวจสอบผู้ใช้ก่อนเขาใช้งานระบบได้ รวมทั้งติดตามการใช้งานของผู้ใช้ได้ และสามารถกำหนดสิทธิต่างๆในการใช้งานทรัพยากรของระบบได้

2.2.6 ตัวระบบต้องทำงานได้ในความเร็วสูงสุดเท่าที่ทำได้ ในแพลตฟอร์มทางฮาร์ดแวร์ที่มีอยู่ (Performance) หากผู้ใช้งานเคยใช้ระบบปฏิบัติการก่อนหน้านี้แล้ว คือ Windows Server - 2000 ผู้ใช้จะเกิดความเคยชินในการใช้งานระบบปฏิบัติการ Windows Server 2003 เพราะ Windows Server 2003 เป็นเวอร์ชัน (Version) ที่ได้รับการพัฒนาต่อจาก Windows Server 2000 นั่นเองแต่ Windows Server 2003 ได้ทำการปรับปรุงและแก้ไขปัญหาต่างๆ ที่เกิดขึ้นกับระบบปฏิบัติการตัวก่อนหน้านี้ซึ่ง Windows Server 2003 เป็นระบบปฏิบัติการที่มีประสิทธิภาพสูงและมีความปลอดภัยในด้านการรักษาความปลอดภัยสูงเช่นกัน ระบบปฏิบัติการ Windows Server - 2003 มีชุดของเซิร์ฟเวอร์หลายแบบด้วยกัน ขณะที่ชุดของเซิร์ฟเวอร์ทั้งหมดยังรองรับและสนับสนุนเครื่องลูกข่ายที่เป็น Windows 2000 Professional และ Windows XP Professional ด้วยเช่นกัน ซึ่งชุดของ Windows Server 2003 มีดังต่อไปนี้

- Windows Server 2003, Standard Edition

- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Datacenter Edition
- Windows Server 2003, Web Edition

2.3 Windows Server 2003 Server Roles

โดยทั่วไปนั้น หลังจากทำการติดตั้ง Windows Server 2003 การทำงานของเครื่องเซิร์ฟเวอร์จะเป็นแบบ เซิร์ฟเวอร์ส่วนตัวไม่ต้องแชร์กับผู้อื่น (Standalone Server) และเป็นสมาชิกของเวิร์กกรุ๊ป (Workgroup) โดยจะยังไม่ได้เป็นสมาชิกของโดเมน (Domain) จากนั้นเมื่อทำการการติดตั้งแอคทีฟไดเร็กทอรีเสร็จเรียบร้อย และมีการเพิ่มเครื่องเซิร์ฟเวอร์ Windows Server 2003 เข้าเป็นสมาชิกของโดเมนจะมีบทบาทสองบทบาทที่เครื่องเซิร์ฟเวอร์จะเป็นได้ คือ Member Server คือ เซิร์ฟเวอร์ที่เป็นสมาชิกของโดเมน (Domain Member) และเซิร์ฟเวอร์ที่เป็นโดเมนคอนโทรลเลอร์ (Domain Controller)

2.3.1 บทบาทของเครื่องเซิร์ฟเวอร์ Windows Server 2003 ในการใช้งานรูปแบบต่างๆ

2.3.1.1 เครื่องเซิร์ฟเวอร์ Windows Server 2003 ที่ไม่เป็นสมาชิกของโดเมน จะเรียกเซิร์ฟเวอร์แบบนี้ว่าสแตน อโลน เซิร์ฟเวอร์ (Stand-Alone Server) ซึ่งจะเป็นสมาชิกของเวิร์กกรุ๊ปและจะเก็บฐานข้อมูลของผู้ใช้ไว้ที่เครื่องตัวเองในไฟล์ชื่อว่า Security Accounts Manager: SAM

2.3.1.2 เครื่องเซิร์ฟเวอร์ Windows Server 2003 ที่เป็นสมาชิกของโดเมน จะมีบทบาท 2 บทบาท คือ เซิร์ฟเวอร์ที่เป็นสมาชิกของโดเมน (Domain Member Server) และเซิร์ฟเวอร์ที่เป็นโดเมนคอนโทรลเลอร์ (Domain Controller)

2.3.2 Member Server คือ เซิร์ฟเวอร์ที่เป็นสมาชิกของโดเมนเหมาะสำหรับการใช้งานเป็น File/Print Server Application Server Database Server และWeb Server เพราะสามารถที่จะบริหารจัดการได้โดยผ่านโดเมนคอนโทรลเลอร์ โดยเซิร์ฟเวอร์ที่เป็นสมาชิกของโดเมนนั้นจะเก็บฐานข้อมูลของผู้ใช้ไว้ที่ตัวเองเรียกว่า Security Accounts Manager: SAM แต่สามารถที่จะถูกควบคุมผ่านทางโดเมนได้

2.3.3 โดเมนคอนโทรลเลอร์ คือ เซิร์ฟเวอร์ที่ทำหน้าที่จัดเก็บฐานข้อมูลของโดเมน (Domain Database) และจัดการการสื่อสารระหว่างผู้ใช้กับโดเมน และยังทำหน้าที่ให้บริการตรวจสอบการล็อกออน (Logon Authentication) เข้าโดเมนของเครื่องคอมพิวเตอร์ลูกข่าย (Client Computer) และ ผู้ใช้

2.3.3.1 หน้าที่ของโดเมนคอนโทรลเลอร์ในโดเมน

ในแต่ละโดเมนนั้น จะต้องมีโดเมนคอนโทรลเลอร์ อย่างน้อย 1 ตัวโดยเซิร์ฟเวอร์ที่เป็นโดเมนคอนโทรลเลอร์จะมีหน้าที่มี 3 อย่างดังนี้

- ให้บริการและตรวจสอบการเข้าใช้ของผู้ใช้
- ให้บริการและจัดการการให้บริการไดเร็คทอรีเซอร์วิส (Directory Service)
- เก็บและจัดการฐานข้อมูลแอคทีฟไดเร็กทอรี (Active Directory Database)

2.3.3.2 บทบาทของโดเมนคอนโทรลเลอร์ในโดเมน

เครื่องเซิร์ฟเวอร์ Windows Server 2003 ที่เป็นโดเมนคอนโทรลเลอร์ในโดเมนนั้นจะมีบทบาท 3 บทบาท ด้วยกัน ดังนี้

- Operations Master Roles รูปแบบแอคทีฟไดเร็กทอรีโดเมน (Active Directory - Domain) นั้นจะรองรับการทำ Multi Master Replication Model คือ การแลกเปลี่ยนข้อมูลระหว่างโดเมนคอนโทรลเลอร์ทุกๆ ตัวจะมีระดับชั้นการทำงานเท่ากัน แต่จะมีโดเมนคอนโทรลเลอร์หนึ่งตัวที่ทำหน้าที่เป็น Operations Master ซึ่งจะทำหน้าที่ให้บริการการร้องขอการเปลี่ยนแปลงต่างๆ ของแอคทีฟไดเร็กทอรีแก่โดเมนคอนโทรลเลอร์ตัวอื่นๆ โดยในแต่ละฟอเรสต์ (Forest) นั้นจะมี Operations Master Roles จำนวน 5 อย่างด้วยกัน ซึ่ง Operations Master Roles จะถูกกำหนดให้กับโดเมนคอนโทรลเลอร์เครื่องใดเครื่องหนึ่ง หรือหลายเครื่องก็ได้

- Forest-Wide Operation Master Roles เป็นบทบาท Operations Master Roles ประเภทหนึ่งที่ถูกกำหนดให้กับโดเมนคอนโทรลเลอร์ได้เพียงเครื่องเดียวในแต่ละฟอเรสต์ ซึ่งมีอยู่ 2 ชนิด คือ Schema Master จะทำหน้าที่ควบคุมการอัพเดตและการเปลี่ยนแปลงแก้ไขโครงสร้าง (Schema) ในแต่ละฟอเรสต์และ Domain Naming Master จะทำหน้าที่ควบคุมการเพิ่มหรือลบโดเมนในแต่ละฟอเรสต์

- Domain-Wide Operation Master Roles เป็นบทบาท Operations Master Roles อีกประเภทที่ถูกกำหนดให้กับโดเมนคอนโทรลเลอร์ได้เพียงเครื่องเดียวในแต่ละโดเมน ซึ่งมีอยู่ 3 ชนิด คือ Relative Identifier (RID) Master ทำหน้าที่สร้าง Relative Identification (RID) ให้กับโดเมนคอนโทรลเลอร์ทุกตัวในโดเมน การมี RID Master นั้น ก็เพื่อรับประกันว่าหมายเลข Security ID ของออบเจกต์ (Object) ทุกๆ ตัวในแต่ละโดเมนมีค่าไม่ซ้ำกัน และ PDC Emulator-Master ทำหน้าที่จำลองตัวเป็น PDC ของ Windows NT4.0 เพื่อให้สามารถทำการซิงโครไนซ์ (Synchronize) บัญชีผู้ใช้ (User Account) และรหัสผ่าน (Password) กับ BDC ของ Windows NT4.0 ได้ นอกจากนี้ยังทำหน้าที่จำลองตัวเป็น PDC ของ Windows NT 4.0 เพื่อให้เครื่องไคลเอนต์ที่เป็น Windows 95/98 สามารถใช้งานได้ตามปกติ ในกรณีที่ ต่อมาได้ทำการอัพเดต Windows NT4.0 BDC ไปเป็น Windows Server 2003 บทบาทการเป็น PDC Emulator จะยังคงอยู่ แต่ว่าการทำหน้าที่จะเปลี่ยนไป คือ เมื่อผู้ใช้ทำการเปลี่ยนรหัสผ่านบนโดเมนคอนโทรลเลอร์ตัวใดๆ ก็ตาม โดเมน-คอนโทรลเลอร์ตัวนั้นจะทำการส่งสัญญาณไปยัง เซิร์ฟเวอร์ที่เป็น PDC Emulator จากนั้นจะทำ

การเรพลิเคท (Replicate) ไปยังโดเมนคอนโทรลเลอร์อื่นๆ ทุกตัวภายในโดเมน เมื่อผู้ใช้ทำการล็อกออนด้วยรหัสผ่านใหม่ที่โดเมนคอนโทรลเลอร์ตัวอื่น ซึ่งอาจจะยังไม่ได้รับการ เรพลิเคท โดเมนคอนโทรลเลอร์ตัวนั้นจึงยังไม่รู้ว่ารหัสผ่านมีการเปลี่ยนแปลง แต่ก่อนที่โดเมนคอนโทรลเลอร์จะแจ้งผู้ใช้ว่าใส่รหัสผ่านผิด โดเมนคอนโทรลเลอร์ตัวนั้นจะถามไปยัง เซิร์ฟเวอร์ที่เป็น PDC Emulator ก่อน ซึ่งเซิร์ฟเวอร์ที่เป็น PDC Emulator จะทราบว่ามีการเปลี่ยนรหัสผ่านและแจ้งกลับไปยังโดเมนคอนโทรลเลอร์ตัวที่สอบถามมา ดังนั้นโดเมนคอนโทรลเลอร์ก็จะทราบว่ามีการเปลี่ยนรหัสผ่าน จึงยอมให้ผู้ใช้ล็อกออนเข้าใช้งานด้วยรหัสผ่านตัวใหม่ได้ ส่วน Infrastructure Master ทำหน้าที่ติดตามการเปลี่ยนแปลงสมาชิกของกรุ๊ปต่างๆ และคอยอัพเดตการเปลี่ยนแปลงดังกล่าวให้กับยังโดเมนคอนโทรลเลอร์ทุกตัวในโดเมน เพื่อให้โดเมนคอนโทรลเลอร์มีข้อมูลที่ทันสมัยเสมอ

นอกจาก Forest-Wide Operation master Roles และ Domain-Wide Operation master Roles แล้วในแต่ละฟอเรสต์จะต้องมีโกลบอลแค็ตตาล็อกเซิร์ฟเวอร์ (Global Catalog Server) คือ เซิร์ฟเวอร์ที่ทำหน้าที่เก็บรวบรวมค่าต่างๆ ของแอตทริบิวต์ (Attribute) ที่สำคัญและถูกใช้งานบ่อยของแต่ละออบเจ็กต์ โกลบอลแค็ตตาล็อกเซิร์ฟเวอร์จะทำหน้าที่เพิ่มความรวดเร็วในการค้นหาออบเจ็กต์ในฟอเรสต์ โดยในแต่ละฟอเรสต์จะต้องมีโกลบอลแค็ตตาล็อกเซิร์ฟเวอร์อย่างน้อย 1 เครื่องโดยค่าดีฟอลท์ (Default) นั้น เครื่องโดเมนคอนโทรลเลอร์เครื่องแรกของฟอเรสต์จะทำหน้าที่เป็นโกลบอลแค็ตตาล็อกเซิร์ฟเวอร์โดยอัตโนมัติแต่มีข้อกำหนดของการทำหน้าที่เป็นโกลบอลแค็ตตาล็อกเซิร์ฟเวอร์ คือ ในกรณีที่มีโดเมนคอนโทรลเลอร์มากกว่า 1 เครื่อง โดเมนคอนโทรลเลอร์ที่ทำหน้าที่ เป็นโกลบอลแค็ตตาล็อกเซิร์ฟเวอร์ จะต้องเป็นโดเมนคอนโทรลเลอร์คนละตัวกับที่ทำหน้าที่เป็น Infrastructure Master เนื่องจากโดยดีฟอลท์นั้น เครื่องโดเมนคอนโทรลเลอร์เครื่องแรกของโดเมนจะทำหน้าที่เป็นโกลบอลแค็ตตาล็อกเซิร์ฟเวอร์โดยอัตโนมัติ แต่อย่างไรก็ตามเราสามารถเปลี่ยนเครื่องโดเมนคอนโทรลเลอร์ที่ทำหน้าที่เป็นโกลบอลแค็ตตาล็อกเซิร์ฟเวอร์ในภายหลังได้ นอกจากนี้ยังสามารถเพิ่มเครื่องโดเมนคอนโทรลเลอร์ให้ทำหน้าที่เป็นโกลบอลแค็ตตาล็อกเซิร์ฟเวอร์ได้ตามความเหมาะสม

2.3.4 DNS Services และรูปแบบชื่อโดเมนของแอคทีฟไดเรคทอรี่ในการทำงานของ Windows Server 2003 ตัวของ Domain Name System (DNS) จัดเป็นเซอร์วิสที่จะต้องมีควบคู่กับตัวของแอคทีฟไดเรคทอรี่ โดยก่อนที่จะลงมือติดตั้งแอคทีฟไดเรคทอรี่ จำเป็นต้องศึกษาว่า DNS นั้นมีบทบาทกับการทำงานของแอคทีฟไดเรคทอรี่อย่างไร

2.4 Domain Name System (DNS)

อินเตอร์เน็ต คือ เครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่มีคอมพิวเตอร์ทั่วโลกจำนวนมากเชื่อมต่อกันโดยแต่ละเครื่องในระบบอินเตอร์เน็ตมีระเบียบวิธีสื่อสารระหว่างกันได้ด้วย

อินเตอร์เน็ตโปรโตคอล (Internet Protocol: IP) และอ้างอิงถึงกันและกันจากชุดหมายเลขอินเตอร์เน็ตโปรโตคอลซึ่งเป็นชุดหมายเลขที่จำเป็นต้องกำหนดให้มีประจำแต่ละเครื่องคอมพิวเตอร์ในเครือข่ายอินเตอร์เน็ต มีลักษณะเป็นกลุ่มตัวเลข 4 กลุ่มประกอบกันที่คั่นด้วยดอท (.) เช่น 203.146.189.21 และไม่ซ้ำกันในแต่ละเครื่องเพื่อให้การสื่อสารระหว่างคอมพิวเตอร์มีการอ้างอิงไปยังแต่ละเครื่องได้อย่างถูกต้องมีประสิทธิภาพ

เนื่องจากปริมาณคอมพิวเตอร์ในเครือข่ายมีแนวโน้มเพิ่มขึ้นมาก ทำให้การจะเข้าถึงเครื่องคอมพิวเตอร์ซึ่งเป็นแหล่งข้อมูลต่างๆนั้นผ่านทางการจดจำหมายเลขเครื่องเป็นเรื่องที่ยากลำบากสำหรับผู้ใช้ จึงเกิดระบบ DNS ขึ้นมาเสริมระเบียบวิธีเดิมที่สื่อสารด้วยอินเตอร์เน็ตโปรโตคอลโดยตรงเพื่อเอื้ออำนวยให้ผู้ใช้เข้าถึงเครื่องคอมพิวเตอร์ที่กระจายอยู่ในเครือข่ายอินเตอร์เน็ตผ่านทางการจำชื่อโดเมนที่เป็นชุดตัวอักษรแทนเช่น www.gistda.or.th

จากการที่มีระบบโดเมนเข้ามาเสริมกิจกรรมต่างๆที่จะเกิดขึ้นในเครือข่ายอินเตอร์เน็ตจึงต้องอิงอาศัย อยู่กับการทำงานของระบบโดเมนเป็นลำดับแรก จึงอาจจะกล่าวได้ว่าระบบโดเมนเป็นระบบที่สำคัญมากต่อการดำเนินไปของกิจกรรมในเครือข่ายอินเตอร์เน็ต ซึ่งหากระบบโดเมนไม่ทำงานเว็บบราวเซอร์ (Web Browser) ซึ่งเป็นช่องทางเชื่อมต่อสู่โลกอินเตอร์เน็ตให้แก่ผู้ใช้จะไม่สามารถค้นหาเว็บไซต์ (Web Site) พบและผู้ใช้จะไม่สามารถรับหรือส่งอีเมล์ (e-Mail) ได้

2.4.1 ลักษณะโครงสร้างข้อมูลและองค์ประกอบของระบบโดเมน

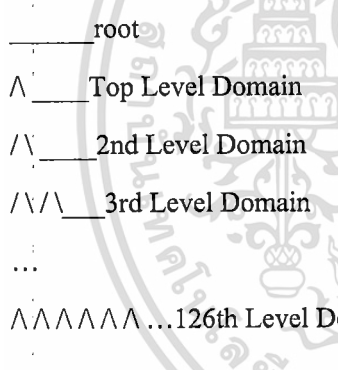
ในขณะที่เครือข่ายอินเตอร์เน็ตประกอบไปด้วยคอมพิวเตอร์จำนวนมากมายเชื่อมต่อกันและเลขที่อยู่ไอพี (IP Address) สามารถทำให้เครื่องคอมพิวเตอร์ระบุตัวตนระหว่างกันในอินเตอร์เน็ตได้ ชื่อโดเมนก็ทำให้เลขที่อยู่ไอพีกลายสภาพไปเป็นตัวอักษรอีกทีหนึ่งเพื่อให้ผู้ใช้ง่ายต่อการจดจำ ระบบโดเมนจึงเป็นที่อยู่ของข้อมูลเกี่ยวกับชื่อโดเมนและเลขที่อยู่ไอพีที่เป็นคู่ของกันและกัน โดยการทำงานของระบบนี้คือ สืบค้นชื่อโดเมนไปหาหมายเลขเครื่องคอมพิวเตอร์หรือเลขที่อยู่ไอพีอันเป็นที่อยู่ของข้อมูลปลายทางอย่างมีขั้นตอน ในขณะที่ชื่อโดเมนซึ่งเช่นเดียวกันกับเลขที่อยู่ไอพีซึ่งทำหน้าที่ระบุที่อยู่ของข้อมูลปลายทางจะต้องมีลักษณะเป็นเอกลักษณ์ไม่ซ้ำซ้อนกันเพื่อประสิทธิภาพในการเข้าถึงข้อมูลอย่างเป็นระบบระเบียบ

ในระบบโดเมนจึงประกอบด้วยชุดข้อมูลจำเพาะของแต่ละโดเมนจำนวนมหาศาลที่ประกอบไปด้วยสิ่งที่จำเป็นต่อกระบวนการสืบค้น โดยชุดข้อมูลจำเพาะของแต่ละชื่อโดเมนซึ่งจะอยู่ในรูปเท็กซ์ไฟล์ (Text File) เหล่านั้นถูกเรียกว่า โซนไฟล์ (Zone File) การจัดระเบียบโซนไฟล์จำนวนมหาศาลเพื่อประสิทธิภาพในการสืบค้นของระบบโดเมนทำในลักษณะเป็นฐานข้อมูลแบบกระจาย โดยแบ่งจัดเก็บโซนไฟล์ ตามโครงสร้างเป็นแบบลำดับชั้น (Hierarchical) ไล่จากลำดับบนสุดซึ่งเป็นฐานข้อมูลร่วมของกระบวนการสืบค้นทั้งระบบมีชื่อเฉพาะว่ารูท ซิสเต็ม (Root System) ประกอบด้วยเซิร์ฟเวอร์จำนวน 13 ตัวโดยแต่ละตัวจะมีข้อมูลเหมือนกันเพื่อรองรับการทำงานของกันและกัน และเพื่อประสิทธิภาพให้แก่การทำงานถามตอบของ DNS เป็นไปได้

อย่างรวดเร็วยิ่งขึ้น โดยเมื่อมีการถามหาข้อมูลมายังรูทซิสเต็ม ใน 13 ตัวนี้ที่อยู่ใกล้ผู้ถามที่สุดจะเป็นผู้ตอบ

ถัดจากรูท ซิสเต็ม ไปจึงเริ่มจากหน่วยชื่อที่มีลักษณะทั่วไป ไปหาลำดับล่างสุดที่เป็นหน่วยชื่อที่มีลักษณะเฉพาะเกิดรูปลักษณ์โครงสร้างฐานข้อมูลทั้งระบบคล้ายต้นไม้กลับหัว (Tree) โดยเรียกทั้งโครงสร้างนี้ว่า Domain Name Space หรือ เรียกสั้นๆว่า Name Space โดยโครงสร้างการจัดลำดับข้อมูลแบบนี้สะท้อนออกไปยังรูปแบบเดียวกันกับการเขียนชื่อโดเมนซึ่งในแต่ละชื่อเป็นการไล่จากหน่วยชื่อทางขวาที่มีลักษณะทั่วไปคั่นไปหาหน่วยชื่อที่อยู่ทางซ้ายที่มีลักษณะเฉพาะขึ้นเรื่อย โดยชื่อแต่ละหน่วยจะคั่นด้วยดอท (.)

การแตกลำดับชั้นลงไปตามโครงสร้างนี้สามารถมีได้สูงสุด 127 ชั้น และแต่ละชั้นมีตัวอักษร (Character) ได้มากสุด 63 ตัวอักษรโดยชั้นที่อยู่ล่างสุดซึ่งอาจเป็นชั้นที่สองไปจนถึงชั้นที่ 127 จะเป็นชื่อที่เจาะจงถึงเครื่องนั้นๆ ในขณะที่ชั้นอื่นๆก่อนถึงชั้นล่างสุดจะเป็นชื่อรากในแต่ละลำดับ การแตกลำดับชั้นลงไปมากมายเช่นนี้ทำให้ ชื่อโดเมนผันแปรต่างๆกันออกไปได้มากมายยิ่งขึ้น เช่น



ในแต่ละลำดับชั้นที่ถัดจากรูท ซิสเต็ม จะประกอบไปด้วยจุดแตกย่อย (Node) ซึ่งเป็นชื่อโดเมนหน่วยขวาสุด (โดเมนระดับบนสุด) จะเป็นชื่อที่รวมของโซนไฟล์ของชื่อโดเมนที่อยู่ภายใต้จุดแตกย่อยชื่อโดเมนนั้นๆ เช่น Node .com จะเป็นศูนย์รวมของโซนไฟล์ของชื่อโดเมนต่างๆที่อยู่ภายใต้ .com เช่น Amazon.com Ebay.com

การเป็นที่รวมของโซนไฟล์ในจุดแตกย่อยหนึ่งๆนี้เรียกว่าโซนซึ่งในแต่ละโซนจะมีเนมเซิร์ฟเวอร์ แบบ Authority Name Server ประจำการอยู่ทำหน้าที่คอยตอบคำถาม ให้แก่รีโซลเวอร์หรือเนมเซิร์ฟเวอร์ที่เป็น Recursive Name Server ผู้ดูแลการทำงานของเนมเซิร์ฟเวอร์รวมทั้งฐานข้อมูลที่ประกอบไปด้วยโซนไฟล์ของ เนมเซิร์ฟเวอร์ต่างๆ คือ ผู้ดูแลฐานข้อมูลโดเมน (Registry) ซึ่งสามารถบริหารฐานข้อมูลนั้นได้อย่างอิสระภายใต้การกำดูแลของ ICANN ทำให้จุดแตกย่อยของโซนนั้นๆ สามารถแตกย่อยโครงสร้างข้อมูลภายในจุดแตกย่อยนั้นๆ เพื่อจัดเก็บโซนไฟล์ ออกไปได้อีกเป็นหลายๆสาขา (Leaf) ตัวอย่าง >>> .th >>> .co.th

ลักษณะโครงสร้างต้นไม้เช่นนี้ช่วยให้โดเมนในหน่วยงานหรือองค์กรใดๆไม่จำเป็นต้องเก็บรักษาสำเนาข้อมูลชื่อโดเมนที่มีอยู่ทั้งหมด หากแต่ระบบสามารถเชื่อมถึงกันทางเครือข่ายเพื่อสืบค้นและแลกเปลี่ยนข้อมูลรวมทั้งใช้ฐานข้อมูลของแต่ละลำดับชั้นร่วมกันโดยอัตโนมัติ

2.4.2 การทำงานของระบบโดเมน

งานหลักของ ระบบโดเมน คือเก็บข้อมูลของ DNS และตอบคำถามเมื่อได้รับคำร้องจากระบบ โดยบริการสืบค้นชื่อกระทำในหลายแบบโดยมีบริการส่วนใหญ่ คือ

- Standard Name Resolution คือกระบวนการใช้ชื่อโดเมนสืบค้นเลขที่อยู่ไอพี
- Reverse Name Resolution คือกระบวนการใช้เลขที่อยู่ไอพี สืบค้นชื่อโดเมน
- Electronic Mail Resolution กระบวนการกำหนดจุดหมายในการส่งอีเมล์จากอีเมล์ที่จะใช้ในการส่ง

ขั้นตอนในการสืบค้นที่อยู่ของแหล่งข้อมูล ดำเนินไปในลักษณะของไคลเอ็นท์ เซิร์ฟเวอร์ (Client – Server) ในกระบวนการทำงานของระบบโดเมนแบบมาตรฐาน (Standard Name Resolution) ภายในโครงสร้างต้นไม้ของระบบโดเมน เป็นการทำงานประสานกันระหว่าง Authority Name Server ซึ่งเป็น เนมเซิร์ฟเวอร์ ที่ประจำอยู่แต่ละโซน รวมไปถึงเนมเซิร์ฟเวอร์ที่ถูกมอบหมาย (Delegate) ให้ตอบคำถามเกี่ยวกับชื่อโดเมนภายใต้ชื่อ Node นั้นๆ และ Resolver ซึ่งเป็นโปรแกรมสืบค้นชื่อที่ประจำอยู่ในเครื่องของผู้ใช้

กระบวนการสืบค้นชื่อจะเริ่มต้นจากการทำงานของรีโซลเวอร์ซึ่งได้รับคำสั่งค้นหามาจากผู้ใช้โดยรีโซลเวอร์จะเริ่มต้นสืบค้นจากภายในแคช (Catch) ซึ่งเป็นที่เก็บข้อมูลของชื่อที่อยู่ของแหล่งข้อมูลชั่วคราวที่อาศัยอยู่ในเครื่องของผู้ใช้เอง ซึ่งหากค้นเจอจะทำให้รีโซลเวอร์ทำเวลาในการค้นหาแหล่งที่อยู่ได้ดี

กรณี รีโซลเวอร์ค้นข้อมูลในแคชแล้วไม่พบรีโซลเวอร์จะมีปกติตั้งต้นถามไปยัง Authority Name Server ที่ประจำอยู่ ณ รูท ซิสเต็ม ซึ่งเป็นฐานข้อมูลร่วมระดับบนสุดที่อย่างน้อยที่สุดสามารถแนะนำเส้นทางให้แก่ รีโซลเวอร์ได้เพื่อให้รีโซลเวอร์ได้ถามไปยังเนมเซิร์ฟเวอร์อื่นๆต่อไปกรณีที่ Authority Name Server ที่ประจำอยู่ ณ รูท ซิสเต็ม ไม่รู้คำตอบ

รีโซลเวอร์จะสืบค้นตามคำแนะนำของ Authority Name Server ในระบบเรื่อยๆ จนกว่าจะพบเนมเซิร์ฟเวอร์ที่เป็นของแหล่งข้อมูลเป้าหมาย ซึ่งจะให้คำตอบสุดท้ายเป็นหมายเลขประจำเครื่องอันเป็นแหล่งข้อมูลที่ผู้ใช้ต้องการเข้าถึงยังผลให้เครื่องผู้ใช้สามารถติดต่อกับเครื่องแหล่งข้อมูลได้ในที่สุด

การถามจะตั้งต้นที่โดเมนระดับกว้าง ได้แก่ รูท (Root) แล้วจึงเป็นโดเมนระดับบนสุดที่สุดก่อนแล้วไล่ความเฉพาะลงมาเรื่อยๆ กระบวนการทำงานแบบนี้ที่รีโซลเวอร์ทำการค้นหาคำตอบเองเป็นหลักด้วยการติดต่อกับเนมเซิร์ฟเวอร์เรื่อยๆจนกว่าจะเจอเนมเซิร์ฟเวอร์ ที่เป็นปลายทางเรียกว่า Iterative Resolution

อย่างไรก็ตามยังมีลักษณะการสืบค้นแบบ Recursive Resolution ซึ่งเป็นกระบวนการที่รีโซลเวอร์ พึ่งพาการทำงานของเนมเซิร์ฟเวอร์เป็นหลักโดย ในการทำงาน Resolver ทำการส่งคำถามไปยังเนมเซิร์ฟเวอร์ เพียงครั้งเดียว หากกรณี Authority Name Server ตัวนั้นไม่รู้คำตอบก็จะทำการสืบค้นต่อให้แก่ รีโซลเวอร์โดย Authority Name Server นั้นจะต้องมีคุณสมบัติเป็นผู้ค้นหาคำตอบได้ด้วย เรียกว่า Recursive Name Server ในขณะที่ รีโซลเวอร์ในกระบวนการสืบค้นแบบนี้ก็จะต้องเป็นแบบ Stub Resolver ซึ่งมีลักษณะที่ Recursive Name Server ยอมรับ จึงจะทำให้กระบวนการสืบค้นชื่อแบบ Recursive Resolution นี้ดำเนินไปได้

ในทำงานในรูปแบบ Recursive resolution มักเป็นกระบวนการที่ใช้กันแบบภายในองค์กรที่อาจให้มี Local Name Server ช่วย อำนวยความสะดวกให้รีโซลเวอร์ภายในเครื่องของผู้ใช้งานในองค์กร อย่างไรก็ตามเมื่อ Local Name Server นั้นๆต้องเข้าสู่โครงสร้างข้อมูลระบบโดเมนภายนอก ก็มักจะเป็นกระบวนการสืบค้นแบบ Iterative Resolution ปรกติ จึงกล่าวได้ว่าในกระบวนการแบบ Standard Name Resolution อาจมีทั้งลักษณะการทำงานแบบ Iterative resolution และ Recursive resolutionประกอบกัน

โดเมนของ DNS และโดเมนของ แอคทีฟไดเร็กทอรีนั้นมีรูปแบบของชื่อโดเมนที่เหมือนกันทุกอย่าง คือ ใช้ความแตกต่างของ Namespace ในการจำแนกชื่อเครื่องคอมพิวเตอร์ โดยเครื่องคอมพิวเตอร์ระบบเน็ตเวิร์กของ Windows Server 2003 ใช้ DNS ในการค้นหาโดเมนคอนโทรลเลอร์ และเครื่องคอมพิวเตอร์ตัวอื่นๆ ที่ทำหน้าที่ให้บริการ

ชื่อโดเมนและชื่อเครื่องคอมพิวเตอร์จะแสดงในรูปของ Resource Record ในชื่อที่เป็นแบบ DNS Namespace และแสดงในลักษณะของออบเจ็คในแอคทีฟไดเร็กตอรีในชื่อแบบ Active Directory Namespace ซึ่ง DNS Server จะเก็บชื่อของเครื่องคอมพิวเตอร์ แบบเดียวกับที่เก็บในรายชื่อเครื่องคอมพิวเตอร์ในแอคทีฟไดเร็กทอรีซึ่งเราเรียกชื่อแบบที่เป็น Domain DNS Name นี้ว่า Primary DNS Suffix กับเครื่องคอมพิวเตอร์ที่เข้าเป็นสมาชิกในโดเมนของแอคทีฟไดเร็กทอรี

เราอาจจะพูดได้ว่า เครื่องคอมพิวเตอร์ใช้ชื่อแบบ DNS Namespace กับชื่อแบบ Active Directory Namespace เป็นชื่อเดียวกัน ยกตัวอย่างเช่น เครื่องคอมพิวเตอร์ชื่อ Client1 เมื่อเข้าเป็นสมาชิกในโดเมนชื่อ Abc.com ดังนั้นชื่อเครื่องคอมพิวเตอร์ Client1 แบบ Fully Qualified Domain Name (FQDN) ก็คือ Client1.Abc.com

การรวมเอา DNS และ แอคทีฟไดเร็กทอรีเป็นงานที่สำคัญที่สุดเนื่องจากเครื่องไคลเอนต์ในระบบเน็ตเวิร์กของ Windows Server 2003 จะต้องติดต่อไปทำการล๊อกออน กับโดเมนคอนโทรลเลอร์ของโดเมน หรือการติดต่อเพื่อขอกับบริการต่างๆ ของแอคทีฟไดเร็กทอรีจากโดเมนคอนโทรลเลอร์ ซึ่งการที่เครื่องไคลเอนต์จะสามารถติดต่อกับโดเมนคอนโทรลเลอร์ได้นั้นจะต้องอาศัยการทำงานกับ DNS ในการแปลงชื่อของโดเมนคอนโทรลเลอร์ให้เป็นหมายเลข IP Address ก่อน

2.5 Active Directory Microsoft Windows Server 2003

แอคทีฟไดเร็กทอรีเป็นเครื่องมือตัวหนึ่งที่มีมาพร้อมกับ Microsoft windows 2003 server ทุกรุ่นโดยใช้ทำหน้าที่จัดการกับทรัพยากรในระบบ ทั้งการจัดเก็บข้อมูลในรูปของออบเจ็ค การคอนฟิก (Config) และการควบคุมการให้บริการโครงสร้างพื้นฐานของแอคทีฟไดเร็กทอรี โดยมีโครงสร้างพื้นฐานอยู่ด้วยกันสองรูปแบบที่เรียกว่า โครงสร้างแบบตรรกะและโครงสร้างแบบฟิสิคัล (Physical) ซึ่งผู้ที่ทำหน้าที่ดูแลควรจะได้เข้าใจโครงสร้างทั้งสองลักษณะดังกล่าวนี้ก่อน เพราะจะทำให้สามารถกำหนดรูปแบบและวิธีการทำงานกับแอคทีฟไดเร็กทอรีได้อย่างเหมาะสม โดยโครงสร้างแบบตรรกะนั้นจะพูดถึงแอคทีฟไดเร็กทอรีในแง่ของการติดตั้งการบริหารและการจัดการกับทรัพยากร เช่น ทะเบียนผู้ใช้ (User Account) กรุ๊ป (Group) คอมพิวเตอร์แอคเคาท์ (Computer Account) รวมถึงเครื่องพิมพ์และแชร์โฟลเดอร์ (Public Share Folder) ซึ่งแอคทีฟ-ไดเร็กทอรีจะแสดงในรูปของออบเจ็ค โดเมนเนม โดเมนทรีและฟอเรสต์ ซึ่งถ้าเราเข้าใจโครงสร้างของแอคทีฟไดเร็กทอรีในลักษณะนี้จะช่วยให้เราสามารถติดตั้ง ควบคุม และวิเคราะห์เพื่อหาแนวทางการแก้ปัญหาต่างๆ ได้ ส่วนโครงสร้างแบบฟิสิคัลนั้น จะพูดถึงแอคทีฟไดเร็กทอรีในแง่ของการติดต่อสื่อสารระหว่างเครื่องในระบบเน็ตเวิร์ก ซึ่งประกอบด้วย โดเมนคอนโทรลเลอร์และไซต์ (Site) ซึ่งผลที่เกิดจากการกำหนดโครงสร้างของแอคทีฟไดเร็กทอรีให้เป็นแบบนี้ก็คือ การควบคุมเงื่อนไขของการทำเรพลิเคท (Replicate) รวมทั้งการลดปริมาณความหนาแน่นในช่องทางสื่อสารของระบบเครือข่าย ที่เกิดจากกระบวนการล็อกออน ของเครื่องไคลเอนท์

2.5.1 ประโยชน์ที่ได้รับการใช้งานแอคทีฟไดเร็กทอรี

แอคทีฟไดเร็กทอรีจัดเป็นเครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลต่างๆ เกี่ยวกับยูสเซอร์แอคเคานท์, คอมพิวเตอร์แอคเคานท์ และทรัพยากรที่มีในเครือข่าย และกำหนดวิธีการให้ผู้ใช้รวมไปถึงโปรแกรมต่างๆ สามารถติดต่อเข้ามาใช้ข้อมูลทั้งในการค้นหา การเรียกดู และการกำหนดวิธีการเข้าไปใช้งาน การอนุญาต หรือไม่อนุญาตในการทำงานของผู้ใช้บางรายแอคทีฟไดเร็กทอรีช่วยให้การจัดการกับข้อมูลสามารถทำได้จากศูนย์กลาง (Centralize Management) คือ สามารถสั่งควบคุมการทำงานของทั้งระบบจากจุดใดจุดหนึ่งในระบบได้ เพราะข้อมูลของทั้งระบบจะถูกเก็บและสามารถเปลี่ยนแปลงได้จากการสั่งงานบนตัวของแอคทีฟไดเร็กทอรีนอกจากนั้นเรายังสามารถแบ่งเบาภาระงานบางอย่างของผู้ดูแลระบบ ออกไปยังผู้ที่ได้รับมอบหมาย ให้ทำงานบางอย่างภายใต้สิทธิที่ได้รับ เมื่อเราติดตั้ง Active Directory ของ Windows Server 2003 แล้วทรัพยากรในระบบที่มีอยู่เดิมทั้งหมดก็สามารถเข้าใช้งานและสั่งการลงไป โดยมีการตรวจสอบเพื่อความปลอดภัยของระบบได้ โดยอาศัยการพิจารณาเป็นออบเจกต์ที่จัดเก็บในโครงสร้างแบบมีลำดับชั้น ที่สำคัญที่สุดคือ โครงสร้างแบบฟิสิคัล ของแอคทีฟไดเร็กทอรีช่วยให้เราสามารถควบคุมปริมาณข้อมูลที่มีในระบบเน็ตเวิร์กได้อีกด้วย เพราะสามารถกำหนดเงื่อนไขในการล็อกออนของเครื่องไคลเอนท์

ว่าจะต้องขอทำการตรวจสอบ จากเครื่องโดเมนคอนโทรลเลอร์ที่อยู่ใกล้เคียงกับเครื่องไคลเอนต์ของผู้ใช้และยังสามารถควบคุมการเรพลิเคทบนเครื่องโดเมนคอนโทรลเลอร์ได้

2.5.2 โครงสร้างแบบตรรกะของแอคทีฟไดเร็กทอรี

โครงสร้างแบบตรรกะของ แอคทีฟไดเร็กทอรีจะมององค์ประกอบต่างๆ ในรูปของออบเจกต์ ที่จัดเก็บในโครงสร้างแบบมีลำดับชั้น โดยออบเจกต์ที่พูดถึงก็คือ รายชื่อผู้ใช้และทรัพยากรที่มีในระบบ เน็ตเวิร์ก เช่น เครื่องคอมพิวเตอร์ เครื่องพิมพ์ รวมไปถึงออบเจกต์ต่างๆ ที่ใช้เก็บรวมรวมข้อมูลของออบเจกต์อื่นๆ เข้าด้วยกันให้เป็นหมวดหมู่ โครงสร้างแบบตรรกะจะประกอบไปด้วย

2.5.2.1 ออบเจกต์ คือ หน่วยข้อมูลพื้นฐานในโครงสร้างแบบตรรกะของแอคทีฟไดเร็กทอรี โดยมีการแบ่งออกเป็นคลาส (Class) ต่าง เช่น คลาสรายชื่อผู้ใช้, คลาสเครื่องคอมพิวเตอร์ เป็นต้นโดยที่ออบเจกต์ที่มีในแต่ละคลาสก็จะมีแอตทริบิวต์ที่อาจจะเหมือนกันหรือแตกต่างกันเป็นส่วนประกอบพื้นฐาน เพื่อให้สามารถเข้าใจได้ง่ายขึ้นขอยกตัวอย่างดังนี้ สมมติว่าเรากำลังพูดถึง CPU ตัวของ CPU ก็คือ ออบเจกต์นั่นเอง ซึ่งถ้าจะให้ทราบถึงรายละเอียดของตัว CPU เราก็ต้องระบุรายละเอียดเพิ่มเติม เช่น ยี่ห้ออินเทล รุ่น Corei7 ความเร็ว 2 GHz มีขนาดของแคช 1 MB ซึ่งเหล่านี้ก็คือแอตทริบิวต์ของออบเจกต์ CPU นั่นเอง

2.5.2.2 ออกาไนเซชันนอล ยูนิต (Organizational Units หรือ OU) เพื่อให้การจัดการกับออบเจกต์มีระเบียบมากขึ้น แอคทีฟไดเร็กทอรีจึงได้นำเอาแนวคิดของการเก็บออบเจกต์ที่มีความเกี่ยวข้องในการทำงานมาเก็บรวบรวมไว้ในคอนเทนเนอร์ เพื่อจะได้ง่ายต่อการควบคุมและกำหนดบทบาทความรับผิดชอบ ให้กับผู้มีหน้าที่ดูแลได้เป็นสัดส่วน เราจึงมีการใช้งาน OU เพื่อทำหน้าที่เป็นคอนเทนเนอร์ เพื่อให้เข้าใจได้ง่ายขึ้นให้นึกถึงว่าทำไม เราต้องสร้างโฟลเดอร์เพื่อเก็บไฟล์ข้อมูลในเครื่องคอมพิวเตอร์

2.5.2.3 โดเมน จัดว่าเป็นยูนิตหลักของการทำงานในโครงสร้างแบบตรรกะของแอคทีฟไดเร็กทอรีในแต่ละโดเมนใช้เก็บรวบรวมเงื่อนไขในการควบคุมออบเจกต์และแลกเปลี่ยนการใช้ข้อมูลของ แอคทีฟไดเร็กทอรีกำหนดนโยบายเกี่ยวกับความปลอดภัย และการแลกเปลี่ยนการใช้งานทรัพยากรกับโดเมนอื่นๆ ซึ่งเราพอจะสรุปเป็นข้อๆ ได้ดังนี้

- กำหนดของเขตของผู้ดูแลในการบริหารและจัดการ
- ช่วยในด้านการกำหนดระดับความปลอดภัยในการใช้งานทรัพยากรของระบบ
- ใช้กำหนดเงื่อนไขการทำเรพลิเคท

2.5.2.4 โดเมนทรี (Domain Trees) โดเมนหลายๆ โดเมนที่นำมาใช้งานร่วมกันโดยกำหนดความสัมพันธ์แบบมีลำดับชั้นนี้ เราเรียกว่า “โดเมนทรี” โดยโดเมนถูกสร้างขึ้นก่อนเรียกว่า “โดเมนแม่” (Parent Domain) ส่วนโดเมนที่สร้างเพิ่มเติมในภายหลัง ในลักษณะลำดับชั้นเรียกว่า โดเมนลูก (Child Domain) โดยเอกลักษณ์ของโดเมนลูกก็คือ จะมีการสืบทอดลักษณะของ

ชื่อมาจากโดเมนแม่ตามลักษณะของชื่อที่เป็นแบบ DNS Name ยกตัวอย่างเช่น โดเมนแม่ชื่อว่า gistda.or.th ดังนั้นตัวของโดเมนลูกก็จะมีชื่อตามลักษณะของตัวแม่คือเป็น server1.gistda.or.th หรือเป็น server2.gistda.or.th เป็นต้น

2.5.2.5 ฟอเรสต์ คือกลุ่มของโดเมนทรีที่มีการใช้งานร่วมกันอยู่ โดยมีลักษณะคล้ายๆกับโดเมนทรี แต่ว่าไม่จะเป็นต้องมีการสืบทอดลักษณะชื่อกันตามรูปแบบชื่อที่เป็น DNS Name เช่นอาจจะเป็นชื่อโดเมน ABC.COM กับ XYZ.NET เป็นต้น ซึ่งทั้งสองชื่อก็เป็นชื่อที่อยู่ในฟอเรสต์ของบริษัทเดียวกัน แต่มีข้อที่ควรจำก็คือ โดเมนแรกของฟอเรสต์นั้นเราจะมีคำเรียกเฉพาะว่าเป็น ฟอเรสต์ รูท โดเมน (Forest Root Domain) เพื่อใช้แสดงให้ทราบถึงลักษณะโดเมนที่มีสิทธิในการทำงานเหนือโดเมนอื่นๆ ทั้งหมดในฟอเรสต์ โครงสร้างแบบฟิสิคัลของแอคทีฟ-ไดเร็กทอรี โครงสร้างแบบฟิสิคัลของ แอคทีฟไดเร็กทอรีนั้นจะถูกใช้ ในมุมมองที่แตกต่างไปจากโครงสร้างแบบที่เป็นตรรกะ โดยเราจะใช้โครงสร้างในการทำงานนี้กับตัวเครื่องที่เป็นไคลเอนต์และเซิร์ฟเวอร์มีการส่งข้อมูลผ่านเน็ตเวิร์กกันอย่างไร ซึ่งผลที่ได้ก็คือ เราสามารถกำหนดให้มีการส่งข้อมูลได้อย่างเหมาะสม ไม่ทำให้ช่องทางสื่อสารของระบบคับคั่ง โดยเราสามารถพิจารณาโครงสร้างแบบ Physical ได้เป็นลักษณะต่างๆ ดังนี้

- โดเมนคอนโทรลเลอร์ คือ เครื่องที่ติดตั้ง Windows Server 2003, Windows Server 2000 หรือ Windows NT เพื่อใช้ทำหน้าที่เป็นเซอร์วิส ที่เรียกว่าไดเร็กทอรีเซอร์วิสในโดเมนคอนโทรลเลอร์แต่ละเครื่องจะมีส่วนที่ใช้เก็บข้อมูลและสามารถเรพลิเคทกันและกันเพื่อให้ข้อมูลตรงกันอยู่เสมอ นอกจากนั้นโดเมนคอนโทรลเลอร์หนึ่งเครื่องก็สามารถให้บริการได้ในหนึ่งโดเมนเท่านั้น แต่ในทางกลับกัน ในหนึ่งโดเมนมีโดเมนคอนโทรลเลอร์ได้หลายเครื่อง

- ไซต์ คือกลุ่มของเครื่องคอมพิวเตอร์ ที่ติดต่อกันบนระบบเน็ตเวิร์กที่มีประสิทธิภาพที่ดี โดยจะต้องมีโดเมนคอนโทรลเลอร์ อย่างน้อยหนึ่งตัวภายใจแต่ละไซต์ทำหน้าที่ให้บริการซึ่งประโยชน์ที่ได้รับก็คือสามารถลดปริมาณข้อมูลที่ใช้ติดต่อระหว่างไคลเอนต์กับโดเมนคอนโทรลเลอร์ที่ อยู่ต่างไซต์กันในเวลาที่มีการล็อกออน เพราะเครื่องไคลเอนต์จะติดต่อกับเครื่องโดเมนคอนโทรลเลอร์ที่อยู่ในไซต์เดียวกัน นอกจากนั้นก็เพื่อให้เราสามารถควบคุมการเรพลิเคทข้อมูลระหว่างเครื่องโดเมนคอนโทรลเลอร์ที่อยู่คนละไซต์ หลักการทำงานของ แอคทีฟไดเร็กทอรี ในส่วนนี้ จะแนะนำให้รู้จักการทำงานของ แอคทีฟไดเร็กทอรีในมุมมองของการทำหน้าที่เป็นไดเร็กทอรีเซอร์วิสซึ่งการทำความเข้าใจเกี่ยวกับการทำงานของแอคทีฟไดเร็กทอรีจะช่วยให้เราสามารถแก้ปัญหาต่างๆ ที่เกิดขึ้นได้อย่างถูกต้องและเหมาะสม แนวคิดเกี่ยวกับการทำงานของไดเร็กทอรีเซอร์วิสสำหรับในองค์กรขนาดใหญ่ ซึ่งมีทรัพยากรจำนวนมากทั้ง แชร์โฟลเดอร์และเครื่องพิมพ์ ซึ่งมาจากหลายๆ แหล่งการที่ผู้ใช้งานจะสามารถทราบถึงรายละเอียดทั้งหมดนั้นคงเป็นไปได้ยาก ยกตัวอย่างเช่นผู้ใช้ต้องการทราบว่ามีเครื่องพิมพ์ที่สามารถพิมพ์เอกสารสีที่มี ความละเอียดสูงในบริษัทหรือไม่ในกรณีที่ผู้ใช้จะสามารถหาข้อมูลได้จากที่ไหน และอีกกรณีก็คือ

ถ้าต้องการส่งพัสดุไปให้ผู้รับที่ทำงานในสาขาที่ต่างจังหวัด แต่เราไม่ทราบว่าจะต้องจ่าหน้าถึงผู้รับซึ่งอยู่เลขที่เท่าไหร่ ถนนอะไรเราจะสามารถสอบข้อมูลเหล่านี้ได้จากที่ได้ ในจุดนี้ จึงเป็นที่มาของการนำเอาแนวคิดที่เกี่ยวกับการใช้งานไดเร็กทอรีเซอร์วิสเข้ามาช่วยในการปฏิบัติงาน โดย Microsoft เรียกไดเร็กทอรีเซอร์วิสของตนเองว่า แอคทีฟไดเร็กทอรีเซอร์วิส (Active Directory Service)โดยบทบาทของ แอคทีฟไดเร็กทอรีที่มีใน Windows Server 2003 นั้นยังสามารถช่วยกำหนดรูปแบบในการทำงานหลายๆ ด้านให้กับผู้ดูแลระบบ โดยเริ่มตั้งแต่การกำหนดวิธีการตรวจสอบผู้ใช้งานว่ามีสิทธิในการเข้าสู่ระบบหรือไม่และสามารถใช้งานทรัพยากรอะไรที่มีอยู่ได้บ้าง รวมไปถึงการติดตั้งโปรแกรมตามลักษณะงานการกำหนดสภาพแวดล้อมในการทำงานกับเครื่องคอมพิวเตอร์ของผู้ใช้ โดยผู้ดูแลระบบสามารถกำหนดเงื่อนไขต่างๆ เหล่านี้ได้ทั้งหมดที่จุดเดียว โดยไม่ต้องเสียเวลาไปกำหนดทีละเครื่องและยังสามารถลดปริมาณการส่งข้อมูลไปบนระบบเน็ตเวิร์ก ซึ่งเกิดจากการติดต่อระหว่างเครื่องคอมพิวเตอร์ได้ด้วย

2.5.3 รูปแบบการบริหารระบบของแอคทีฟไดเร็กทอรี

ใน Windows Server 2003 นั้น ได้อำนวยความสะดวกให้กับผู้ดูแลระบบ ด้วยการติดตั้งเครื่องมือจำนวนมาก เพื่อให้สามารถใช้ควบคุมและจัดการกับข้อมูลได้จากศูนย์กลาง เพราะข้อมูลทั้งหมดที่ทำจะถูกเก็บลงในฐานข้อมูลเดียวกันและในทางกลับกันก็อาจจะมองว่า เราสามารถแยกการควบคุมและการบริการออกเป็นหลายๆ ส่วนก็ได้ เพื่อความสะดวกในการทำงานกับฐานข้อมูลที่มีขนาดใหญ่

2.5.4 การจัดการกับแอคทีฟไดเร็กทอรี

แอคทีฟไดเร็กทอรี มีเครื่องมือหลายตัวเพื่อใช้ในการจัดการกับทรัพยากรจากศูนย์กลาง การที่แอคทีฟไดเร็กทอรีสามารถทำงานในลักษณะที่ว่านี้ได้ เพราะมีเหตุผลดังนี้

แอคทีฟไดเร็กทอรีเก็บข้อมูลต่างๆ ไว้ในออบเจกต์ซึ่งออบเจกต์เหล่านั้นก็จะมีข้อมูลที่เกี่ยวกับทรัพยากร ที่มีในระบบ ดังนั้นผู้ดูแลระบบเพียงคนเดียวก็สามารถดูแลและควบคุมทรัพยากรที่มีในระบบได้ผ่านทางเครื่องมือของ แอคทีฟไดเร็กทอรีเอง แอคทีฟไดเร็กทอรีสามารถค้นหาข้อมูลได้โดยการใช้งานผ่านโปรโตคอลแอล-แด็บ (Lightweight Directory Access Protocol: LDAP) ดังนั้นมันจึงเป็นเรื่องที่ง่ายสำหรับผู้ดูแลระบบที่จะเลือกดูและค้นหาข้อมูลของ แอคทีฟ-ไดเร็กทอรีเพราะเครื่องมือต่างๆ ที่มีให้รองรับการทำงานบนโปรโตคอล แอล-แด็บ แอคทีฟไดเร็กทอรีอนุญาตให้เราเก็บรวบรวมออบเจกต์ต่างๆ ที่มีลักษณะของการกำหนดเงื่อนไขความปลอดภัยคล้ายกัน หรือต้องการรับบริการจากแอคทีฟไดเร็กทอรีเหมือนกัน มาเก็บรวมเข้าด้วยกันภายในออร์แกไนเซชันยูนิต (Organization Unit: OU) ซึ่งการเก็บรวบรวมออบเจ็ค ต่างๆ ไว้ใน OU นั้น นอกจากจะช่วยให้ข้อมูลต่างๆ ถูกจัดเก็บได้อย่างเป็นระเบียบแล้ว เรายังสามารถใช้เงื่อนไขเกี่ยวกับการทำงานของกรุ๊ปโพลิซี (Group Policy) และการทำดีลิเกทคอนโทรล (Delegate Control) เข้ามาช่วยในการทำงานได้อีกด้วย และสามารถกำหนดเงื่อนไขการทำงานด้วยกรุ๊ปโพลิซี โดยการทำงาน

ในส่วนของกรุ๊ปโพลิซี นั้น สามารถกำหนดได้ตั้งแต่ระดับของไซต์ โดเมน และ OU โดยกรุ๊ปโพลิซี สามารถควบคุมและกำหนดสภาพแวดล้อมการทำงานได้ทั้งสมาชิกที่อยู่ใน OU ทั้งยูสเซอร์แอค-เคานท์และคอมพิวเตอร์แอคเคานท์ แอคทีฟไดเร็กทอรีช่วยให้การมอบหมายงานในส่วนของผู้ดูแลระบบ ไปยังผู้ใช้งานทั่วไปได้โดยไม่จำเป็นต้องกำหนดให้ผู้ใช้คนนั้นๆ เป็นสมาชิกในกลุ่มของผู้ดูแลระบบอีกต่อไป ซึ่งลักษณะของการทำงานดังกล่าว คล้ายคลึงกับการกำหนดสิทธิ์ให้กับผู้ใช้งานสามารถที่จะอ่านหรือเขียนข้อมูลลงบนไฟล์ได้ ซึ่งเราเรียกการทำงานในส่วนนี้ว่าการทำ ดีลิเกทคอนโทรล ลักษณะของการทำดีลิเกทคอนโทรล ช่วยให้เราสามารถกำหนดวิธีการทำงานในลักษณะต่างๆ ได้แก่ สามารถกำหนดเพอร์มิชชั่น (Permission) แบบฟูลคอนโทรล (Full Control) เพื่อให้ผู้ดูแลระบบในแต่ละส่วนสามารถจัดการกับระบบที่ตนเองดูแลได้อย่างเต็มที่และไม่อนุญาตให้ผู้ดูแลระบบในส่วนงานอื่น เข้ามายุ่งเกี่ยวด้วย สามารถกำหนดสิทธิในการแก้ไขได้ถึงระดับ แอตทริบิวต์ของออบเจกต์ภายใน OU ที่ดูแลนั้นๆเช่น สามารถเปลี่ยนชื่อ นามสกุล ที่อยู่ หมายเลขโทรศัพท์ และรีเซ็ตรหัสผ่านของผู้ใช้ทุกคนใน OU นั้นๆ และสามารถกำหนดสิทธิตามลักษณะงาน เช่นสามารถรีเซ็ตรหัสผ่านให้กับผู้ใช้ทุกคนในโดเมนไม่ว่าจะอยู่ใน OU ใดก็ตาม

2.6 แอล-แด็บ (Lightweight Directory Access Protocol: LDAP)

แอล-แด็บ เป็นโปรโตคอลที่พัฒนามาจาก Protocol X.500 ซึ่งใช้ในการเข้าถึงและอัพเดท (Update) ข้อมูลของไดเร็กทอรี (Directory) ซึ่งไดเร็กทอรี ที่จริงก็อาจเรียกได้ว่าเป็นฐานข้อมูลแบบพิเศษที่บรรจุรายละเอียดของออบเจกต์ต่างๆ เช่น ผู้ใช้ โปรแกรมประยุกต์ ไฟล์ เครื่องพิมพ์และอื่นๆ รวมทั้งข้อมูลความปลอดภัยของออบเจกต์เหล่านี้ด้วย โดยข้อแตกต่างของไดเร็กทอรีกับฐานข้อมูลปกติ ได้แก่

- โอเปอเรชั่น (Operation): ในไดเร็กทอรีจะเน้นที่การเข้าถึงข้อมูลหรือ อ่านข้อมูล มากกว่าอัพเดท หรือ เขียนข้อมูล ในขณะที่ฐานข้อมูลทั่วไปจะเน้นการอัพเดทมากกว่า

- ทรานแซคชั่น (Transaction): ในฐานข้อมูลจะรองรับการทำทรานแซคชั่นหรือการอัพเดทข้อมูลสองจุดที่ต้องสอดคล้องกัน แบบออลออน็อตติง (All-or-Nothing) เช่นการโอนเงินจากบัญชีหนึ่ง ไปอีกบัญชีหนึ่งที่ต้องการความสมบูรณ์ ทั้ง 2 ฝั่ง หรือไม่ก็ไม่ต้องทำเลย ในขณะที่ไดเร็กทอรีที่เน้นการอ่านอย่างเดียว อาจจะไม่ต้องการความสอดคล้องกันของข้อมูลนัก เช่นเมื่อมีการเปลี่ยนที่อยู่ระหว่างคน ในหน่วยงานหนึ่งๆ ก็ต้องมีการแก้ไขสถานที่ติดต่อของคนนั้น ซึ่งตรงนี้อาจจะไม่จำเป็นต้องทำทันที

- Data Accuracy: ไดเร็กทอรี อาจจะมีข้อจำกัดในการจัดเก็บข้อมูลที่ไม่สมบูรณ์ เช่น มีแต่ชื่อไม่มีที่อยู่ แต่ยังคงสามารถปรับคุณสมบัติเหล่านี้ได้ในบางไดเร็กทอรีเซอร์วิส

- Query: ไดเร็กทอรีไม่สนับสนุนการสืบค้นแบบ Query String (SQL, Structured Query Language) แม้ไดเร็กทอรี จะมีคุณสมบัติด้อยกว่าฐานข้อมูลหลายประการ แต่เนื่องจากโปรโตคอลที่ใช้ในการเข้าถึงไดเร็กทอรี เช่น แอล-แด็บ มีความเร็วในการเข้าถึงข้อมูลสูง และก็ทำให้โปรแกรมประยุกต์ที่ทำงานบนโปรโตคอลเหล่านี้สามารถเข้าถึงข้อมูลอย่างรวดเร็ว ทำให้ระบบไดเร็กทอรีเป็นที่ยอมรับ และนำมาใช้งานทั่วไป นอกจากประโยชน์ในการค้นหาข้อมูลได้อย่างรวดเร็วแล้ว ไดเร็กทอรียังเป็นโครงสร้างข้อมูลที่แสดงให้ผู้ใช้เห็นข้อมูลทั้งหมดได้จากมุมมองเดียว (Single Logical View) แม้ว่าแท้จริงแล้ว ข้อมูลเหล่านั้นอาจถูกเก็บแยกกันอยู่อย่างกระจัดกระจายตาม Host ต่างๆบน Distributed System ซึ่งข้อดีต่างๆ เหล่านี้ ทำให้มีการพัฒนาโปรแกรมประยุกต์ที่ใช้ไดเร็กทอรีเซอร์วิส ออกมามากมาย และแอล-แด็บ ก็คือหนึ่งในมาตรฐานที่ใช้จัดการ การรับส่งข้อมูลระหว่างแอพพลิเคชั่น เซิร์ฟเวอร์ ที่เก็บไดเร็กทอรีเหล่านี้ กับ ไคลเอ็นท์ แอพพลิเคชั่นที่เป็นฝ่ายเรียกดูข้อมูลจากไดเร็กทอรี

อีกหนึ่งสาเหตุที่จำเป็นต้องมีมาตรฐานในการเข้าถึงข้อมูลในไดเร็กทอรี นั้นก็เพื่อให้การพัฒนา โปรแกรมประยุกต์ที่ใช้ติดต่อกับไดเร็กทอรี เซิร์ฟเวอร์นั้นมีความยืดหยุ่นขึ้น โดยผู้พัฒนาโปรแกรมสามารถเรียกใช้ API (Application Programming Interface) เพื่อติดต่อกับไดเร็กทอรีเซอร์วิสได้ โดยไม่ต้องทราบวิธีการเข้าถึงโดยละเอียด เช่น โครงสร้างของไดเร็กทอรี หรือ ชนิดของข้อมูล (Data Type) ภายใน หรือไม่จำเป็นต้องปรับแก้ โปรแกรมประยุกต์ใหม่ หากมีความต้องการชนิดของข้อมูลใหม่ๆ เป็นต้น นอกเหนือจากที่กล่าวมาข้างต้นแล้ว การมีมาตรฐานเดียวกัน ทำให้ผู้ผลิตโปรแกรมประยุกต์และอุปกรณ์เน็ตเวิร์กที่รองรับการใช้งานไดเร็กทอรีเซอร์วิส มีระเบียบวิธีที่ชัดเจนเป็นกลางทำให้การติดต่อระหว่างโปรแกรมประยุกต์จากต่างผู้ผลิต หรือต่างแพลทฟอร์ม นั้นเป็นไปได้อย่างรวดเร็ว ถูกต้อง และปลอดภัย โดยไม่ต้องทราบข้อมูลที่ใช้ในการติดต่อ เช่น แพลทฟอร์มที่ใช้Host Name หรือ IP address เช่นเดียวกับการที่เราต้องมี TCI/IP, HTTP, FTP, RPC หรือ ORB เป็นมาตรฐานที่ใช้อยู่ทั่วโลก

แอล-แด็บ เป็นมาตรฐานที่ได้รับการยอมรับอย่างกว้างขวาง และมีผู้ผลิตโรแกรมประยุกต์อยู่หลายราย เช่น OpenLDAP IBM Oracle และMicrosoft ซึ่งผลิตภัณฑ์ที่ได้รับความนิยม ได้แก่ Slapd ของ University of Michigan และ Openldap ไดเร็กทอรี เซิร์ฟเวอร์ของ Netscape แอคทีฟไดเร็กทอรีของ Microsoft, Novell Directory Services (NDS) ของ Novell, Sun Directory Services (SDS) ของ Sun และ Internet Directory Server (IDS) ของ Lucent

LDAP ได้รับการออกแบบมาให้อยู่บน TCP/IP Layer ที่มีเพียง 4 Layer ทำให้มีความต้องการทรัพยากรน้อยกว่าแด็บ (DAP) ของมาตรฐาน X.500 อย่างไรก็ตาม หากมีความต้องการติดต่อกันระหว่างแอล-แด็บ ไคลเอ็นท์ (LDAP Client) กับ X.500 Server จำเป็นจะต้องมีการติดต่อผ่านช่องทางที่เรียกว่า แอล-แด็บ เซิร์ฟเวอร์ (LDAP Server) ซึ่งจะต้องมีความเข้าใจทั้ง TCP/IP และโอเอสไอ โมเดล (OSI Model) ในขณะที่ LDAP Client ไม่จำเป็นต้องทำความเข้าใจกับโอเอสไอ

เลเยอร์ (OSI Layer) และไม่ต้องประมวลผลตามแอล-แด็บที่มีความซับซ้อน และโอเวอร์เฮดสูง สำหรับระบบที่ไม่มีการใช้ X.500 ก็ สามารถมีเพียงแอล-แด็บ ไคลเอ็นท์ กับ แอล-แด็บ เซิร์ฟเวอร์ ซึ่งเรียกว่า แอล-แด็บ สแตน อโลน เซิร์ฟเวอร์ (LDAP Stand-Alone Server) แอล-แด็บ ไดเร็กทอรี มีการจัดโครงสร้างแบบลำดับชั้น (Hierarchical) โดยข้อมูลจะถูกบรรจุอยู่ในเอนทรี (Entry) ซึ่งแต่ละเอนทรีจะประกอบด้วยแอตทริบิวต์ ในรูปของ = โดยประเภทจะถูกกำหนดไว้ด้วย Object Identifier (OID)

เอนทรีจะถูกจัดไว้เป็นลำดับชั้นด้วยชื่อเฉพาะ (Distinguished name: DN) โดย Entry ใดๆ ที่อยู่ใต้เอนทรีอื่นจะมีชื่อเฉพาะของเอนทรีอื่นเป็นข้อความที่ตามหลัง (Suffix) เอนทรี นั้น

โครงสร้างของไดเร็กทอรี จะระบุชื่อเฉพาะและระบุว่า แต่ละเอนทรีจะประกอบไปด้วย แอตทริบิวต์ใดบ้าง โดยกำหนดโครงสร้างจะกำหนดข้อมูลเหล่านี้ไว้ในออบเจกต์คลาส (Object class) ซึ่งได้แก่ลิสต์ (List) ของ แมนดาทอรี (Mandatory) กับ ออบชั่นนัล (Optional) แอตทริบิวต์ วิธีการเปรียบเทียบแอตทริบิวต์ ชนิดและขนาดของข้อมูลที่อนุญาต ซึ่งทุกๆ Entry จะต้องเชื่อมโยงไว้กับออบเจกต์คลาสหนึ่ง คลาสรายละเอียดเพิ่มเติมของ Schema File มีอยู่ในหัวข้อ LDAP Schema

แอตทริบิวต์ ส่วนใหญ่จะมีการใช้ตัวอักษรย่อระบุประเภท ซึ่งได้แก่ uid = User id, cn = Common Name, sn = Surname, l = Location, ou = Organizational Unit, o = Organization, dc = Domain Component, st = State, c = Country, etc. โดยข้อมูลเพิ่มเติมในส่วนนี้สามารถหาได้จาก RFC2256

2.6.1 หน้าที่การทำงานของไดเร็กทอรี เซิร์ฟเวอร์ใน แอล-แด็บ

ไดเร็กทอรี เซิร์ฟเวอร์ ในโปรโตคอลแอล-แด็บนี้ จะมีระบบการทำงานที่เป็นการบริหารงานจากส่วนกลางในส่วนกลางนี้จะมีการแบ่งหน้าที่การทำงานออกเป็นส่วน ๆ (เปรียบเทียบได้กับสมุดหน้าเหลืองที่มีการเก็บข้อมูลไว้เป็นหมวดหมู่) เมื่อผู้ใช้ (ไคลเอ็นท์ หลาย ๆ เครื่อง) ต้องการเข้ามาใช้งานในส่วนที่ต้องการแอล-แด็บ เซิร์ฟเวอร์ ก็จะกระจายข้อมูลไปให้ไคลเอ็นท์ได้อย่างรวดเร็ว เมื่อไคลเอ็นท์ ต้องการค้นหาข้อมูลสามารถทำได้อย่างสะดวกรวดเร็วได้เช่นกันจะเห็นได้ว่าไดเร็กทอรี จะทำงานคล้ายกับฐานข้อมูลที่มีการจำกัดชนิดของข้อมูลที่จะทำการเก็บลงในไดเร็กทอรี ข้อมูลที่จะทำการเก็บลงจะต้องมีการตรวจสอบความถูกต้องด้วย แต่ความจริงแล้วไดเร็กทอรี มีความแตกต่างจากฐานข้อมูลตรงที่ไดเร็กทอรี จะมีการใช้งานอย่างไม่จำกัดเตรียมรับกับสถานการณ์ที่ไคลเอ็นท์เข้ามาใช้งานมาก ๆ เครื่องเซิร์ฟเวอร์ที่ให้การบริการอยู่ก็สามารถรองรับการทำงานได้ จะเห็นได้ว่าในปัจจุบันนี้ในองค์กรต่าง ๆ ได้มีการนำ ไดเร็กทอรีเซิร์ฟเวอร์มาใช้กันอย่างแพร่หลายเพราะสามารถควบคุมการเข้าใช้งาน ในระบบต่าง ๆ ในการเข้าถึงข้อมูลของเซิร์ฟเวอร์รวมถึงการรักษาความปลอดภัยแต่ไดเร็กทอรีเซิร์ฟเวอร์ จะเหมาะกับงานที่มีการอ่าน

มากกว่าการบันทึกข้อมูลไดเร็กทอรีจึงออกแบบมาให้สามารถรองรับการทำงานจากไคลเอ็นท์ได้หลายแพลทฟอร์มพร้อมกัน

2.6.2 ขั้นตอนการทำงานของแอล-แด็บ

แอล-แด็บจะทำงานแบบ ไคลเอ็นท์ เซิร์ฟเวอร์ โดยทางไคลเอ็นท์ จะมีการลงโปรแกรมไว้เมื่อต้องการข้อมูลจากเซิร์ฟเวอร์ก็จะทำการส่งการร้องขอ โดยจะผ่านโปรโตคอลทีซีพี/ไอพี (TCP/IP) เมื่อทางเซิร์ฟเวอร์ได้รับร้องขอ แล้ว จะทำการประมวลผลตามที่ไคลเอ็นท์ต้องการและส่งผลลัพธ์กลับไปให้ ไคลเอ็นท์ แอล-แด็บ ไม่เพียงแค่ทำงานแบบไคลเอ็นท์เซิร์ฟเวอร์เท่านั้นยังสามรถทำงานแบบเมสเซจโอเรียนเต็ด (Messages-Oriented)ได้อีก โดยที่ เมสเซจโอเรียนเต็ดหมายถึงการติดต่อสื่อสารระหว่าง ไคลเอ็นท์เซิร์ฟเวอร์ ที่จะมีการส่งสาร (Messages) เป็นการร้องขอไปยังเซิร์ฟเวอร์และเมื่อ เซิร์ฟเวอร์ ได้รับก็จะส่งผลลัพธ์กลับมาในรูปของสารไปให้ไคลเอ็นท์ เราจะเรียกการส่งแบบนี้ว่าซีรี่ แอล-แด็บ เมสเสจ (Series Ldap Message)

บทที่ 3
วิธีการดำเนินงาน

ในบทนี้จะกล่าวถึงวิธีการออกแบบและดำเนินงานสร้างระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ต กรณีศึกษาสำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ โดยขั้นตอนการดำเนินงานแบ่งออกเป็น 4 ส่วน ดังนี้

3.1 ศึกษาระบบการทำงานของสำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ

3.1.1 ประวัติของสำนักงานฯ

ประเทศไทยได้เข้าร่วมโครงการ NASA ERTS-1 ซึ่งเป็นดาวเทียมสำรวจทรัพยากรดวงแรกของโลก เมื่อวันที่ 14 กันยายน พ.ศ.2514 ภายใต้การดำเนินงานของโครงการสำรวจทรัพยากรธรรมชาติด้วยดาวเทียม สำนักงานคณะกรรมการวิจัยแห่งชาติ โดย ทำหน้าที่ประสานงาน จัดหาข้อมูลดาวเทียม ดำเนินการวิเคราะห์ข้อมูล ถ่ายทอดเทคโนโลยี ตลอดจนจัดหาทุนฝึกอบรม ดูงาน และการประชุมทั้งระดับประเทศและนานาชาติ ด้วยผลสำเร็จของโครงการจึงได้มีการเปลี่ยนสถานภาพโครงการฯ เป็นหน่วยงานระดับกองชื่อ กองสำรวจทรัพยากรธรรมชาติด้วยดาวเทียม ใน พ.ศ.2522 และใน พ.ศ.2525 ได้ดำเนินการจัดตั้งสถานีรับสัญญาณดาวเทียมขึ้นที่เขตลาดกระบัง กรุงเทพมหานคร นับเป็นสถานีรับแห่งแรกในภูมิภาคเอเชียตะวันออกเฉียงใต้ เมื่อปี 2541 รัฐบาลมีนโยบายปฏิรูประบบราชการเพื่อให้การทำงานคล่องตัวขึ้น จึงได้ประกาศใช้พระราชบัญญัติองค์การมหาชน พ.ศ.2542 และด้วยความสำคัญของการใช้เทคโนโลยีด้านการสำรวจข้อมูลระยะไกลและระบบสารสนเทศภูมิศาสตร์ในการพัฒนาประเทศ ใน พ.ศ.2543 กระทรวงวิทยาศาสตร์เทคโนโลยีและสิ่งแวดล้อมได้จัดตั้งหน่วยงานใหม่โดยรวมกองสำรวจทรัพยากรธรรมชาติด้วยดาวเทียม สำนักงานคณะกรรมการวิจัยแห่งชาติ และฝ่ายประสานงานและส่งเสริมการพัฒนาระบบสารสนเทศภูมิศาสตร์ ศูนย์ข้อมูลข้อสนเทศ สำนักงานปลัดกระทรวงวิทยาศาสตร์เทคโนโลยีและสิ่งแวดล้อม ตามพระราชกฤษฎีกา เมื่อวันที่ 2 พฤศจิกายน พ.ศ.2543 ในนามของ " สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน) " ตั้งแต่วันที่ 3 พฤศจิกายน พ.ศ.2543 สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน) มีตัวย่อว่า "สทอภ." และมีชื่อภาษาอังกฤษ "Geo-Informatics

and Space Technology Development Agency (Public Organization) - GISTDA" เป็นหน่วยงานของรัฐในรูปแบบองค์การมหาชน ซึ่งมุ่งเน้นการบริหารและดำเนินงานอย่างมีประสิทธิภาพ เพื่อบริการข้อมูลภูมิสารสนเทศ บริการวิชาการต่าง ๆ ตลอดจนการวิจัยและพัฒนาเทคโนโลยีอวกาศให้เป็นประโยชน์ต่อประชาชน

3.1.2 พันธกิจของสำนักงานฯ

สำนักงานมีพันธกิจหลัก ดังนี้

- ผลิต จัดหา รวบรวม วิเคราะห์ และจัดทำคลังข้อมูลจากดาวเทียมสำรวจทรัพยากรและภูมิสารสนเทศเพื่อการพัฒนาประเทศ

- ให้บริการข้อมูล และให้คำปรึกษาด้านเทคโนโลยีอวกาศและภูมิสารสนเทศทั้งในประเทศและระดับสากล

- การพัฒนาเครือข่ายความร่วมมือและการให้บริการด้านเทคโนโลยีอวกาศและภูมิสารสนเทศในระดับสากลทั้งในและต่างประเทศ

- พัฒนาขีดความสามารถในการให้บริการ การสร้างอุตสาหกรรมต่อเนื่อง การสร้างมูลค่าเพิ่มและหารายได้โดยไม่แสวงหากำไรจากการบริการ (ทั้งด้านวิชาการและข้อมูล)

- พัฒนาบุคลากรด้านเทคโนโลยีอวกาศและภูมิสารสนเทศทั้งในและต่างประเทศ

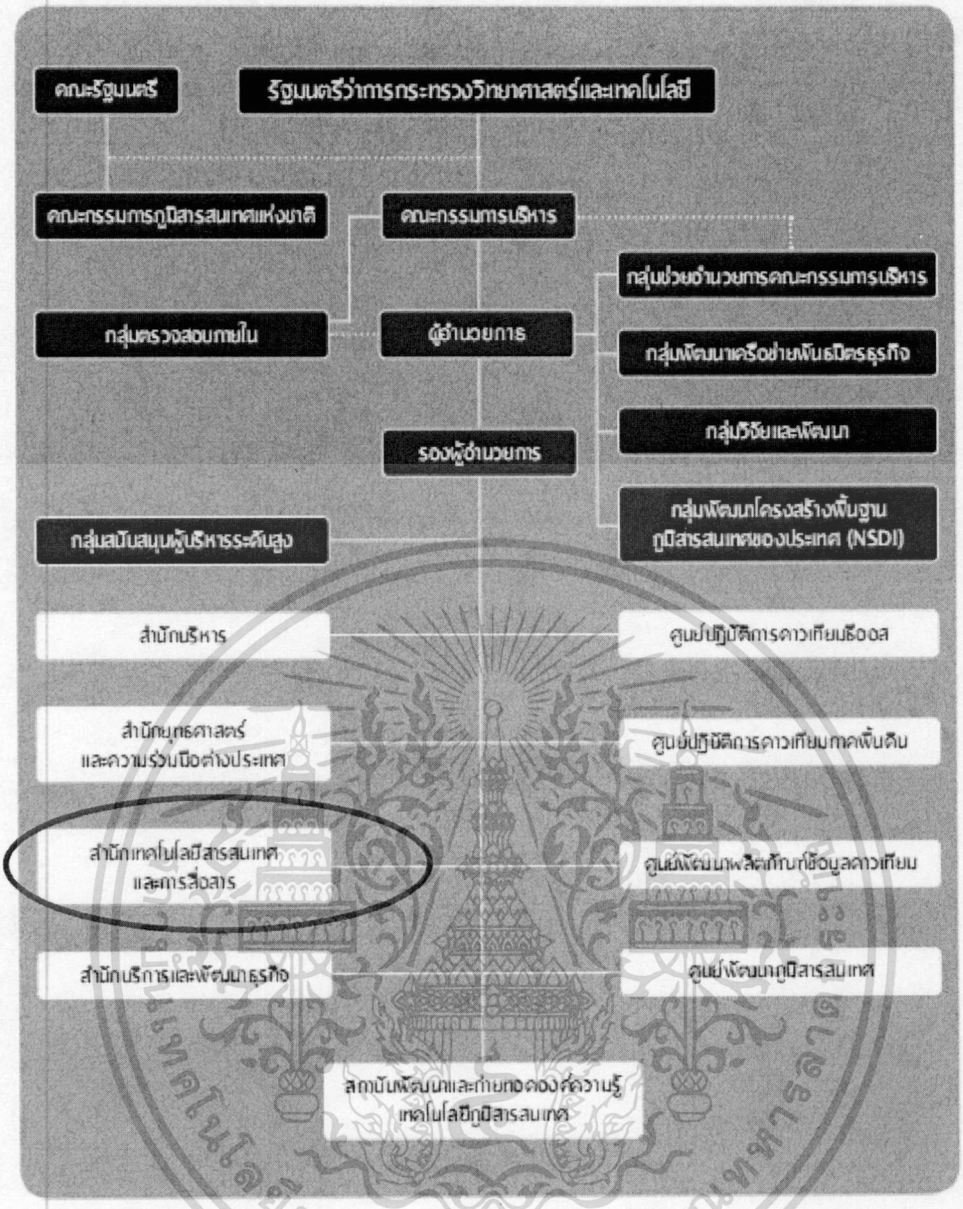
- วิจัยและพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศและระบบดาวเทียมสำรวจทรัพยากร

- การพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีภูมิสารสนเทศ

จากพันธกิจ ดังกล่าวจะเห็นได้ว่าสำนักงานฯ ระบบเครือข่ายอินเตอร์มีบทบาทสำคัญอย่างยิ่งต่อการพัฒนาองค์กรให้บรรลุพันธกิจที่กำหนดไว้ สำนักงานฯจึงจำเป็นต้องมีระบบเครือข่ายอินเตอร์ความเร็วสูงเพื่อให้สามารถส่งผ่านข้อมูลภูมิสารสนเทศที่มีขนาดใหญ่ได้อย่างมีประสิทธิภาพ

3.1.3 โครงสร้างสำนักงานฯ

สำนักงานฯ ประกอบไปด้วย 4 ศูนย์ 4 สำนัก 1 สถาบัน และ 6 กลุ่ม โดยหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศขององค์กร คือ สำนักเทคโนโลยีสารสนเทศและการสื่อสาร รับผิดชอบเกี่ยวกับการบริหารจัดการและพัฒนาระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ การจัดทำแผนแม่บทและแผนปฏิบัติการเทคโนโลยีสารสนเทศ ของ สทอภ. รวมถึงจัดซื้อจัดหาอุปกรณ์คอมพิวเตอร์และอุปกรณ์ให้เพียงพอและมีประสิทธิภาพ ดังรูปที่ 3.1

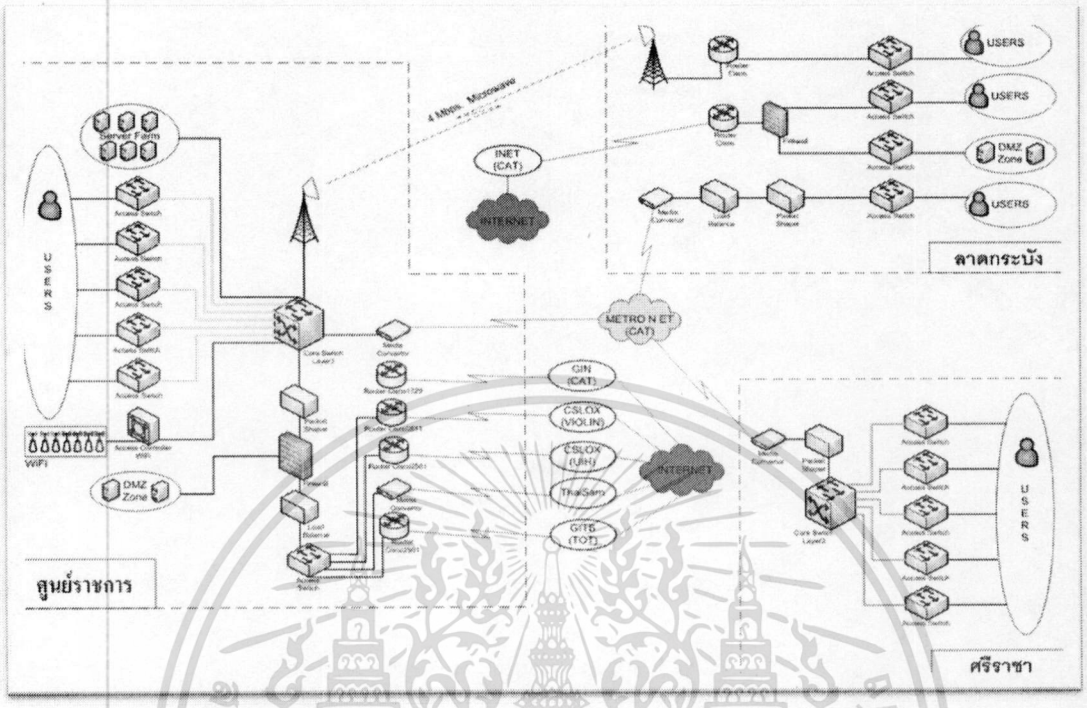


รูปที่3.1 แสดงผังโครงสร้างองค์กร

3.1.4 ระบบเครือข่ายสำนักงานฯ

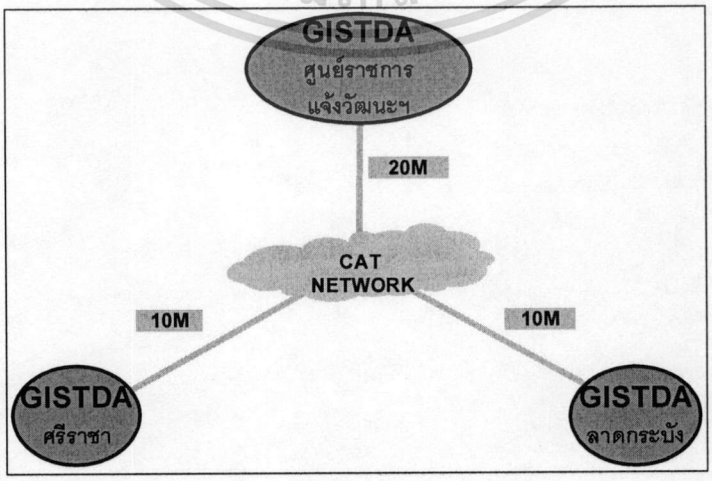
สำนักงานฯ มีสำนักงานใหญ่อยู่ที่ศูนย์ราชการแจ้งวัฒนะและอีก 2 สำนักงานย่อย คือ ศูนย์ควบคุมดาวเทียมภาคพื้นดินลาดกระบัง ตั้งอยู่ที่เขตลาดกระบัง กรุงเทพฯ และศูนย์ปฏิบัติการดาวเทียมธีออส ตั้งอยู่ที่ อ.ศรีราชา จ. ชลบุรี โดยมีการเชื่อมโยงเครื่องข่ายของสำนักงานถึงกันทั้ง 3 แห่งผ่านเครือข่ายวงจรเช่าของบริษัท กสท.โทรคมนาคม ในด้านการใช้งานอินเตอร์เน็ต สำนักงานใหญ่ศูนย์ราชการแจ้งวัฒนะมีเส้นทางการเชื่อมต่ออินเตอร์เน็ตอยู่ 5 เส้นทาง ซึ่งเส้นทางหลักที่ใช้งานปัจจุบันคือ Cslox Info และศูนย์ควบคุมดาวเทียมภาคพื้นดินลาดกระบังมีการใช้

เส้นทางออกสู่อินเตอร์เน็ต 1 เส้นทางคือ INET ส่วนศูนย์ปฏิบัติการดาวเทียมธีออสนั้น ใช้เส้นทางออกสู่อินเตอร์เน็ตโดยผ่านศูนย์ราชการแจ้งวัฒนะ ดังรูปที่ 3.2



รูปที่ 3.2 แสดงระบบเครือข่ายสำนักงานฯ

และเครือข่ายวงจรเช่าของบริษัท กสท.โทรคมนาคม มีแบนด์วิธ ดังนี้ จากศูนย์ราชการแจ้งวัฒนะไปยังเครือข่าย Metro Net ของ CAT มีแบนด์วิธ 20 Mbps จากศูนย์ควบคุมดาวเทียมภาคพื้นดินลาดกระบังไปยังเครือข่าย Metro Net ของ CAT มีแบนด์วิธ10 Mbps และศูนย์ปฏิบัติการดาวเทียมธีออส ไปยังเครือข่าย Metro Net ของ CAT มี แบนด์วิธ 10 Mbps ดังรูปที่ 3.3

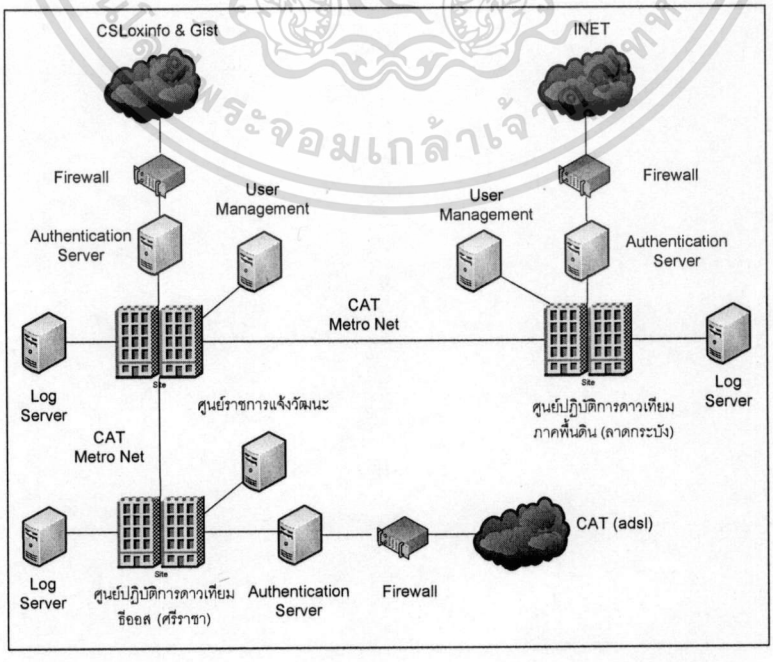


รูปที่ 3.3 GISTDA Metro NET (CAT Telecom)

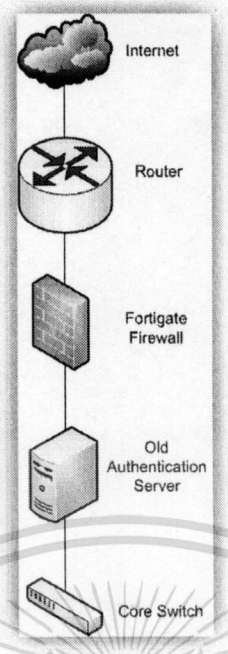
3.2 ศึกษาสถาปัตยกรรมการเชื่อมต่อระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตเดิม

ระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตของสำนักงานฯ เดิมนั้น ได้ทำการจัดซื้ออุปกรณ์สำเร็จรูปจากบริษัทภายนอกให้เข้ามาติดตั้งอุปกรณ์สำหรับการพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตจำนวน 3 ชุด โดยติดตั้งระบบที่สำนักงานใหญ่ ศูนย์ราชการ ถนนแจ้งวัฒนะ 1 ชุด สถานีรับสัญญาณดาวเทียมภาคพื้นดินลาดกระบัง 1 ชุด และศูนย์ปฏิบัติการดาวเทียมธีออส 1 ชุด เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ รองรับการใช้งานของเจ้าหน้าที่ทั้งหมดประมาณ 300 คนทั่วทั้งองค์กร แต่ทั้งนี้ ศูนย์ปฏิบัติการดาวเทียมธีออสไม่ได้มีการใช้งานระบบพิสูจน์ตัวตนดังกล่าว เพราะเส้นทางการเชื่อมต่ออินเตอร์เน็ตมีความเร็วต่ำและได้เลือกใช้เส้นทางการออกอินเตอร์เน็ตผ่านศูนย์ราชการแจ้งวัฒนะแทน โดยวิ่งผ่าน link Fiber Optic 1G เครือข่าย Uninet โดยภาพรวมของการติดตั้งอุปกรณ์ระบบเดิม ดังรูปที่ 3.4

ทั้งนี้ ตำแหน่งติดตั้งเซิร์ฟเวอร์เพื่อพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตระบบเดิมทั้ง 3 สาขาติดตั้งในลักษณะขวางระบบ เมื่อผู้ใช้เข้าสู่กระบวนการใช้งานอินเตอร์เน็ต จะต้องผ่านอุปกรณ์ Core Switch และผ่านการพิสูจน์ตัวตนกับเครื่องเซิร์ฟเวอร์ที่ติดตั้งอยู่ในลักษณะวางขวางระบบ จากนั้นผู้ใช้งานจะผ่าน Policy ของไฟร์วอลล์ก่อนจะไปทำการค้นหาเส้นทางที่เราท์เตอร์เพื่อออกสู่อินเตอร์เน็ต ดังรูปที่ 3.5



รูปที่ 3.4 แสดงภาพรวมของการติดตั้งอุปกรณ์ระบบเดิม



รูปที่ 3.5 ตำแหน่งติดตั้งเซิร์ฟเวอร์สำหรับพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตระบบเดิมทั้ง 3 สาขา

3.3 ศึกษาปัญหาระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตระบบเดิม

จากการศึกษาระบบพิสูจน์ตัวตนระบบเดิมที่สำนักงานฯใช้งานพบปัญหาที่สำคัญ ดังนี้

- ค่าบำรุงรักษาระบบรายปีมีราคาสูง จากค่าอุปกรณ์ 1,965,590 บาท ค่าบำรุงรักษารายปี 899,228 บาท
- ฐานข้อมูลผู้ใช้งาน ถูกจัดเก็บแยกกัน 3 ที่ คือ ศูนย์ราชการแจ้งวัฒนะ สถานีรับสัญญาณดาวเทียมภาคพื้นดินลาดกระบัง และศูนย์ปฏิบัติการดาวเทียมธีออส ทำให้เกิดความซ้ำซ้อนของข้อมูล
- ไม่สามารถทำสำเนาข้อมูลระหว่างฐานข้อมูลผู้ใช้งานทั้ง 3 ศูนย์ได้
- ไม่สามารถค้นหารายชื่อผู้ใช้ที่ทำการเชื่อมต่ออินเตอร์เน็ตได้ด้วยผู้ดูแลระบบขององค์กรต้องแจ้งเจ้าหน้าที่บริษัทดำเนินการให้เท่านั้น
- ระบบเดิมมีไฟร์วอลล์ในตัวอุปกรณ์ ไอพีแอดเดรสที่ทำการแมปไอพีภายในกับไอพีภายนอกไว้จำเป็นต้องมาทำการแมปซ้ำที่อุปกรณ์พิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตระบบ

เดิมอีกครั้งโดยทำการแจ้งเจ้าหน้าที่บริษัทดำเนินการให้ จึงทำให้เกิดความไม่สะดวกต่อการปฏิบัติงาน

- ระบบเดิมระบบเดิมมีทรูพุท 1 Gbps ซึ่งมีค่าทรูพุทที่น้อยมากเมื่อเทียบกับอุปกรณ์ไฟร์วอลล์ที่จะนำมาทำระบบพิสูจน์ตัวตนระบบใหม่

- ระบบเดิมไม่สามารถเพิ่มข่าวสารประกาศภายในสำนักงานฯได้ด้วยผู้ดูแลระบบขององค์กรโดยจะต้องแจ้งเจ้าหน้าที่บริษัทดำเนินการให้ทุกครั้ง ซึ่งก่อเกิดความไม่สะดวกในการปฏิบัติงาน

3.4 ดำเนินงานสร้างระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตใหม่

หลังจากได้ศึกษาระบบเครือข่ายสำนักงานฯ ศึกษาสถาปัตยกรรมการเชื่อมต่อระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตเดิม และพบปัญหาจากการใช้งานระบบเดิมแล้วนั้น ในขั้นนี้เป็นขั้นตอนการออกแบบพัฒนาระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตใหม่เพื่อแก้ไขปัญหาการใช้งานจากระบบดังกล่าว โดยมีขั้นตอน ดังนี้

3.4.1 กำหนดความต้องการของระบบ (System Requirement Specification)

จากปัญหาที่พบจากระบบเดิมพบว่า ระบบใหม่ที่จะพัฒนาขึ้นมีความต้องการแบ่งออกเป็น 2 ประเภท คือ ความต้องการที่เป็นฟังก์ชันการทำงาน (Functional Requirements) และความต้องการที่ไม่เป็นฟังก์ชันการทำงาน (Non-Functional Requirements)

3.4.1.1 ความต้องการระบบด้านฟังก์ชัน (Functional Requirements)

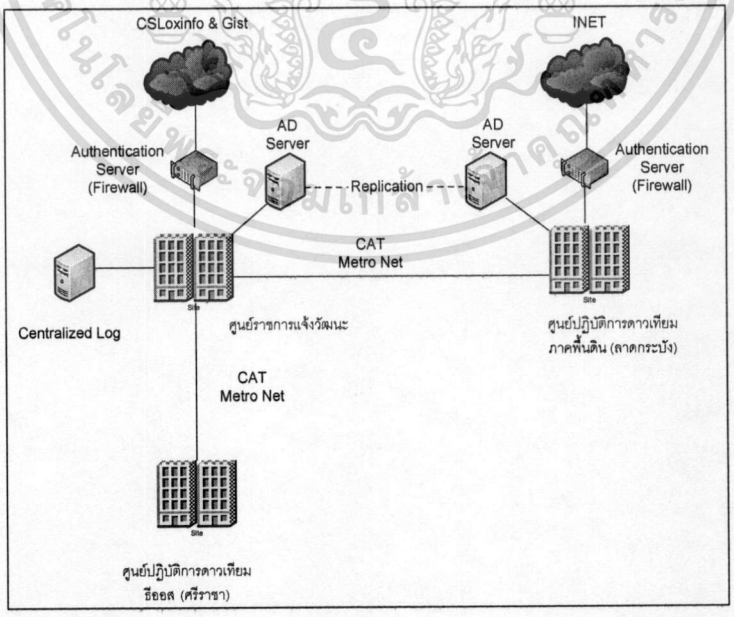
- ระบบจะต้องปิดกั้นการใช้งานอินเตอร์เน็ตสำหรับผู้ที่ยังไม่ลงทะเบียนได้
- ระบบสามารถแสดงข่าวสารของสำนักงานผ่านหน้าเว็บลงทะเบียนเข้าใช้ได้
- ระบบสามารถบันทึกข้อมูลของสมาชิกที่ละทะเบียนไว้ได้
- ระบบสามารถระบุข้อมูลเลขที่อยู่ไอพีของเจ้าหน้าที่ ที่ทำการเชื่อมต่ออินเตอร์เน็ตได้
- ระบบสามารถแสดงข้อมูลการใช้งานอินเตอร์เน็ตได้
- ระบบสามารถระบุข้อมูลปริมาณการใช้งานอินเตอร์เน็ตเป็นปัจจุบันได้
- ระบบจะต้องสามารถตรวจสอบรายการใช้งานของผู้ใช้งานย้อนหลังได้ โดยตรวจสอบจากเลขที่อยู่ไอพี หรือ รายชื่อของผู้ใช้งาน
- ระบบสามารถแก้ไขข้อมูลรหัสผ่านโดยตรงจากผู้ใช้

3.4.1.2 ความต้องการระบบที่ไม่เกี่ยวกับฟังก์ชั่น (Non-Functional Requirements)

- ระบบสามารถทำงานได้ 24 ชั่วโมง
- ระบบสามารถทำการกู้คืนข้อมูลได้ภายในเวลาไม่เกิน 30 นาที
- ระบบล่มได้ไม่เกิน 5 ครั้งต่อปี
- ระบบสามารถค้นหาข้อมูล ภายใน 10 วินาที
- ระบบสามารถทำงานผ่านระบบเครือข่ายได้
- ระบบสามารถสำเนาบัญชีรายชื่อผู้ใช้ไว้ต่างสาขาได้
- ระบบจะต้องมีความถูกต้องของข้อมูล เพื่อนำไปใช้ในทางกฎหมายได้

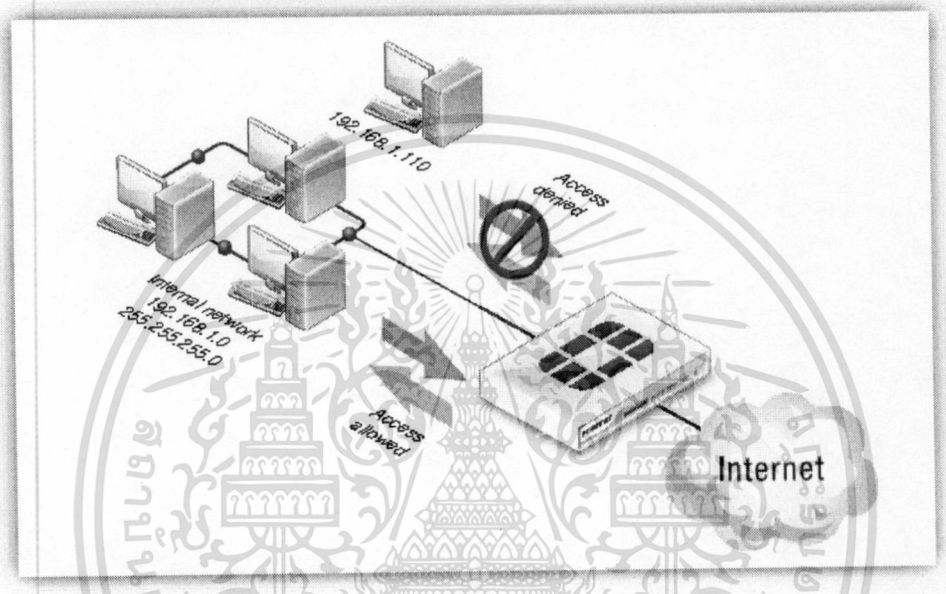
3.4.2 ออกแบบสถาปัตยกรรมระบบ (Architecture Design)

เพื่อตอบสนองความต้องการระบบข้างต้น จึงได้ทำการออกแบบการจัดเก็บข้อมูลรายชื่อผู้ใช้งานให้จัดเก็บบนระบบปฏิบัติการวินโดวส์ 2003 โดยใช้แอคทีฟไดเร็กทอรี เป็นตัวจัดเก็บ และได้มีการติดตั้ง โดเมนคอนโทรลเลอร์ จำนวน 2 ตัว โดยทำงานในลักษณะ Multi-Master Replicationเครื่องโดเมนคอนโทรลเลอร์ตัวที่ 1 จะติดตั้งไว้ ที่สำนักงานใหญ่และเครื่องที่ 2 จะทำการติดตั้งไว้ ณ สถานีควบคุมดาวเทียมภาคพื้นดินลาดกระบัง เชื่อมต่อกันด้วยระบบเครือข่าย Lease Line แบนด์วิธ 10 Mbps ส่วนศูนย์ปฏิบัติการดาวเทียมธีออสจะออกสู่อินเตอร์เน็ตโดยผ่านศูนย์ราชการแจ้งวัฒนะ และจะมีการเก็บล็อกการใช้งานทั้ง 3 สาขาที่ศูนย์ราชการแจ้งวัฒนะ โดยภาพรวมการติดตั้งอุปกรณ์ของระบบใหม่ (กรณีศึกษา) แสดงดังรูปที่ 3.6



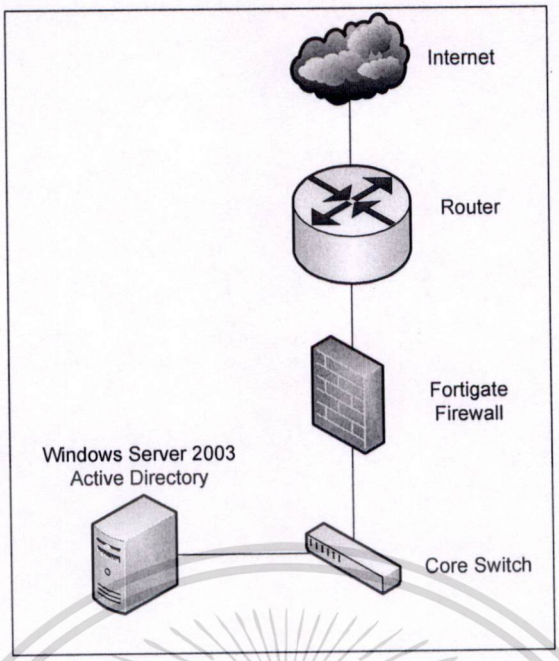
รูปที่ 3.6 แสดงภาพรวมการติดตั้งอุปกรณ์ของระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตระบบใหม่

สำนักงานฯ มีการใช้งานอุปกรณ์ไฟร์วอลล์แบบ Appliance ซึ่งอุปกรณ์ดังกล่าวนี้ติดตั้งอยู่ในลักษณะวางขวางระบบเครือข่าย เมื่ออุปกรณ์ไฟร์วอลล์ติดตั้งอยู่ลักษณะดังกล่าว ผู้จัดทำโครงการจึงได้ลดการวางอุปกรณ์ที่ขวางระบบเครือข่ายลง โดยใช้งานอุปกรณ์ไฟร์วอลล์ในการพิสูจน์ตัวตนควบคู่ไปกับการทำหน้าที่เป็นอุปกรณ์ไฟร์วอลล์ เพื่อให้เกิดความคุ้มค่าของการลงทุน จึงได้ตัดเอาเซิร์ฟเวอร์พิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตแบบทั่ว ๆไป ออกจากระบบเครือข่าย เพื่อให้มีทรูพุทที่สูงขึ้นและไม่เกิดคอขวดจากการวางเซิร์ฟเวอร์ขวางระบบ ดังรูปที่ 3.7



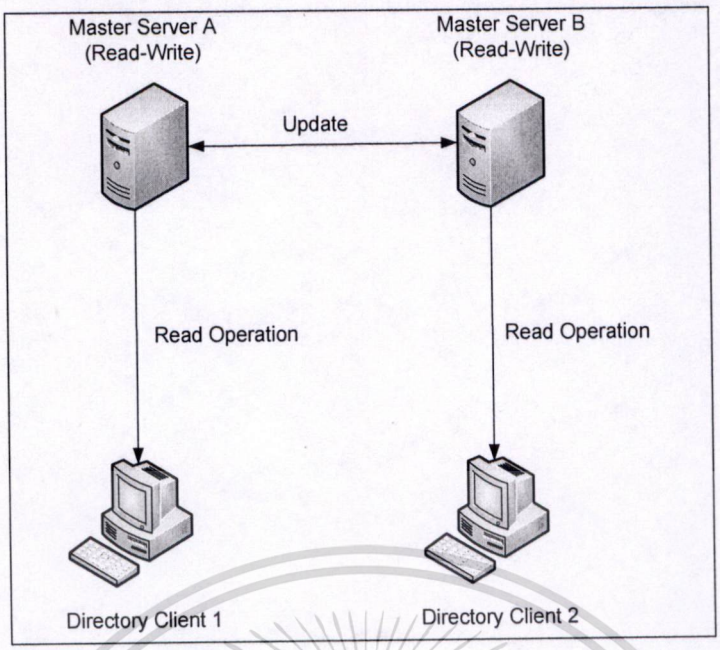
รูปที่ 3.7 แสดงการนำ Firewall Fortigate มาใช้งานในระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ตระบบใหม่

เนื่องจากสำนักงานฯมี License ของ Windows Server 2003 และแอคทีฟไดเร็กทอรีของ Windows Server 2003 และมีความปลอดภัยสูง สะดวกในการบริหารจัดการ ผู้จัดทำโครงการจึงเลือกจัดเก็บข้อมูลบัญชีรายชื่อผู้ใช้งานอินเตอร์เน็ตของสำนักงานทั้งหมดโดยมีไม่ต่ำกว่า 300 รายชื่อบนแอคทีฟไดเร็กทอรี ดังรูปที่ 3.8



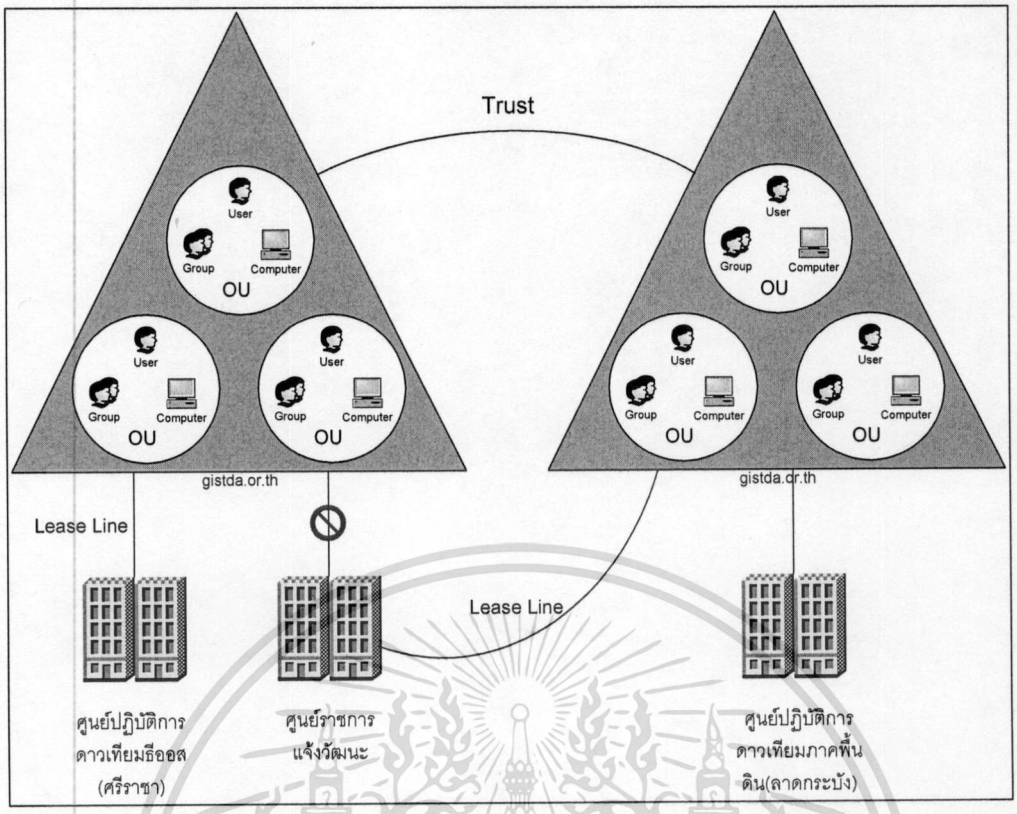
รูปที่ 3.8 แสดงระบบพิสูจน์ตัวตนระบบใหม่ที่ออกแบบให้ใช้งานร่วมกับแอคทีฟไดเร็กทอรี

จากการใช้แอคทีฟไดเร็กทอรี เก็บข้อมูลผู้ใช้งานของสำนักงานฯ เพื่อให้ข้อมูลมีความเหมือนกันทั้ง 2 สำนักงานฯ จึงได้มีการทำการสำเนาบัญชีรายชื่อของผู้ใช้งานไว้ทั้ง 2 ที่เหมือนกัน การทำสำเนารายชื่อบน แอคทีฟไดเร็กทอรี นั้น จะทำผ่านโดเมนเดียวกัน คือ authenticatin.gistda.or.th เมื่อมีการเปลี่ยนแปลงแก้ไขข้อมูลรายชื่อผู้ใช้งานบนเซิร์ฟเวอร์ฝั่งใดก็ตาม ภายในระยะเวลา 15 วินาทีข้อมูลจะมีการส่งการเปลี่ยนแปลงไปยังอีกเครื่องหนึ่งเสมอ ดังนั้นอุปกรณ์ไฟร์วอลล์ที่ทำหน้าที่พิสูจน์ตัวตนสามารถที่จะใช้บัญชีรายชื่อจากเครื่องใดก็ได้ เพราะมีข้อมูลเหมือนกัน เสมือนมีเครื่องสำรองในการให้บริการและเป็นการเพิ่มความต่อเนื่องของระบบ ดังรูปที่ 3.9



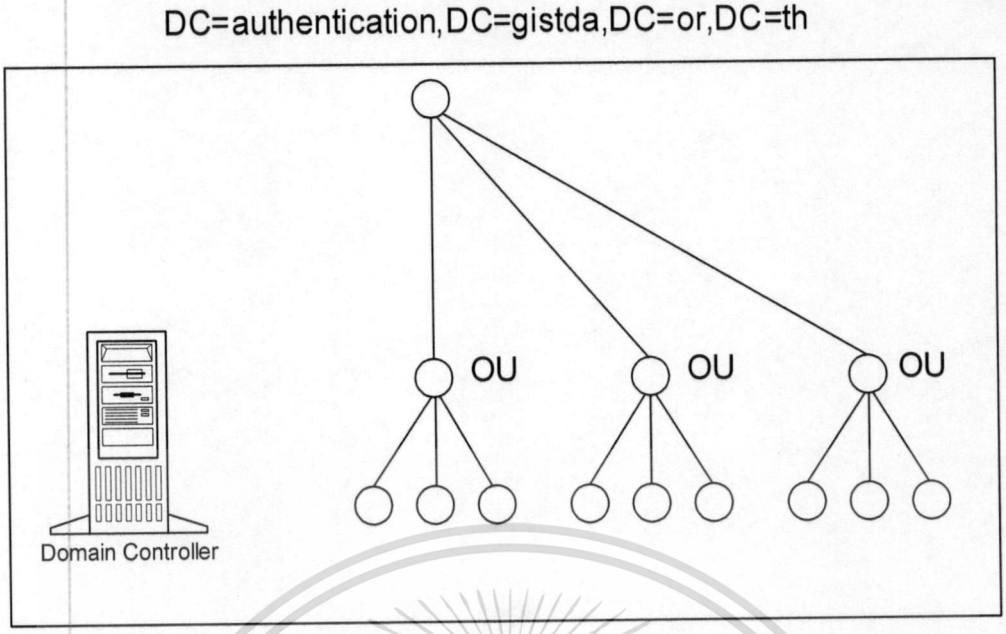
รูปที่ 3.9 แสดงระบบการทำสำเนาข้อมูลรายชื่อผู้ใช้ของ แอคทีฟไดเร็กทอรี เซิร์ฟเวอร์

การใช้งานเครื่องแอคทีฟไดเร็กทอรี ที่เก็บข้อมูลรายชื่อผู้ใช้งานอินเตอร์เน็ตในสำนักงานนั้นมีการเรียกใช้งาน ดังนี้ ศูนย์ราชการแจ้งวัฒนะและศูนย์ปฏิบัติการดาวเทียมธีออสใช้งานแอคทีฟไดเร็กทอรี ณ เครื่องให้บริการที่ศูนย์ราชการแจ้งวัฒนะ ส่วนศูนย์ควบคุมดาวเทียมภาคพื้นดินลาดกระบังใช้งานแอคทีฟไดเร็กทอรี ณ เครื่องให้บริการที่ศูนย์ควบคุมดาวเทียมลาดกระบัง เมื่อเครื่องแอคทีฟไดเร็กทอรี ณ ศูนย์ราชการแจ้งวัฒนะไม่สามารถให้บริการได้ เนื่องจากเหตุขัดข้องต่าง ๆ และผู้ใช้งานต้องการออกสู่อินเตอร์เน็ต โดยจะต้องทำการพิสูจน์ตัวตนก่อนการใช้งาน ผู้ดูแลระบบสามารถเลือกเปลี่ยนเลขที่อยู่ไอพีของเครื่องแอคทีฟไดเร็กทอรีที่ให้บริการตรวจสอบรายชื่อเป็นเครื่องให้บริการที่ศูนย์ควบคุมดาวเทียมลาดกระบังผ่าน Leased Line ได้ ดังรูปที่ 3.10



รูปที่ 3.10 แสดงการสำเนาข้อมูลและการเรียกใช้งาน

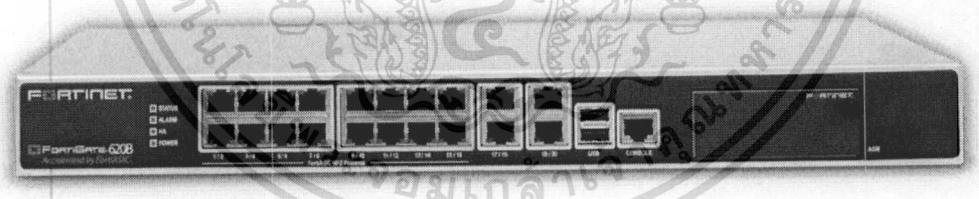
เนื่องจากการจัดเก็บรายชื่อผู้ใช้งานของระบบเดิมนั้น ไม่ได้มีการแยกกลุ่มผู้ใช้งาน จึงทำให้การค้นหาว่าผู้ใช้งานอยู่ส่วนงานไหนเป็นไปด้วยความยากลำบาก ผู้จัดทำโครงการจึงได้นำ Organization Unit (OU) เข้ามาใช้งาน บนแอคทีฟไดเร็กทอรี โดยแยก OU ออกไปตามสำนัก/ศูนย์ต่าง ๆ ซึ่งมีทั้งหมด 9 สำนัก/ศูนย์ และแต่ละสำนักก็จะมี OU ย่อยลงไปอีกในระดับฝ่ายและงาน ดังรูปที่ 3.11



รูปที่ 3.11 แสดงการจัดกลุ่มบัญชีรายชื่อผู้ใช้งานตาม Organization Unit

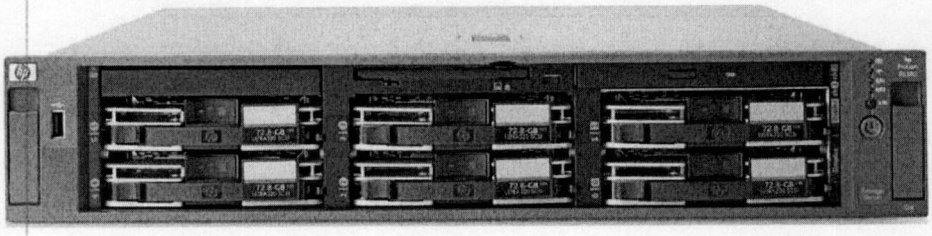
3.4.3 กำหนดข้อมูลจำเพาะให้กับฮาร์ดแวร์และซอฟต์แวร์

อุปกรณ์ที่ใช้ในการทำระบบพิสูจน์ตัวตนจะใช้ไฟร์วอลล์หลักของสำนักงานฯ ยี่ห้อ Fortinet รุ่น Fortigate Firewall 620B และอุปกรณ์ Server ยี่ห้อ HP ProLiant DL 380 และอุปกรณ์เก็บ log ยี่ห้อ Fortinet รุ่น Forti Analyzer 1000C ดังรูปที่ 3.12 - 3.15

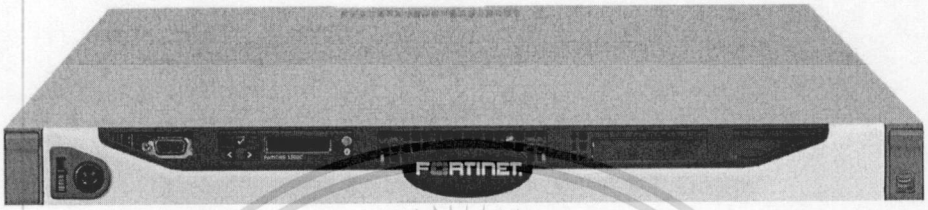


รูปที่ 3.12 แสดงอุปกรณ์ Firewall สำหรับการทำการพิสูจน์ตัวตน ยี่ห้อ Fortinet รุ่น Fortigate 620B

รูปที่ 3.13 แสดงอุปกรณ์ Firewall สำหรับการทำการพิสูจน์ตัวตน ยี่ห้อ Fortinet รุ่น Fortigate 1000



รูปที่ 3.14 แสดงอุปกรณ์คอมพิวเตอร์ ยี่ห้อ HP รุ่น ProLiant DL380



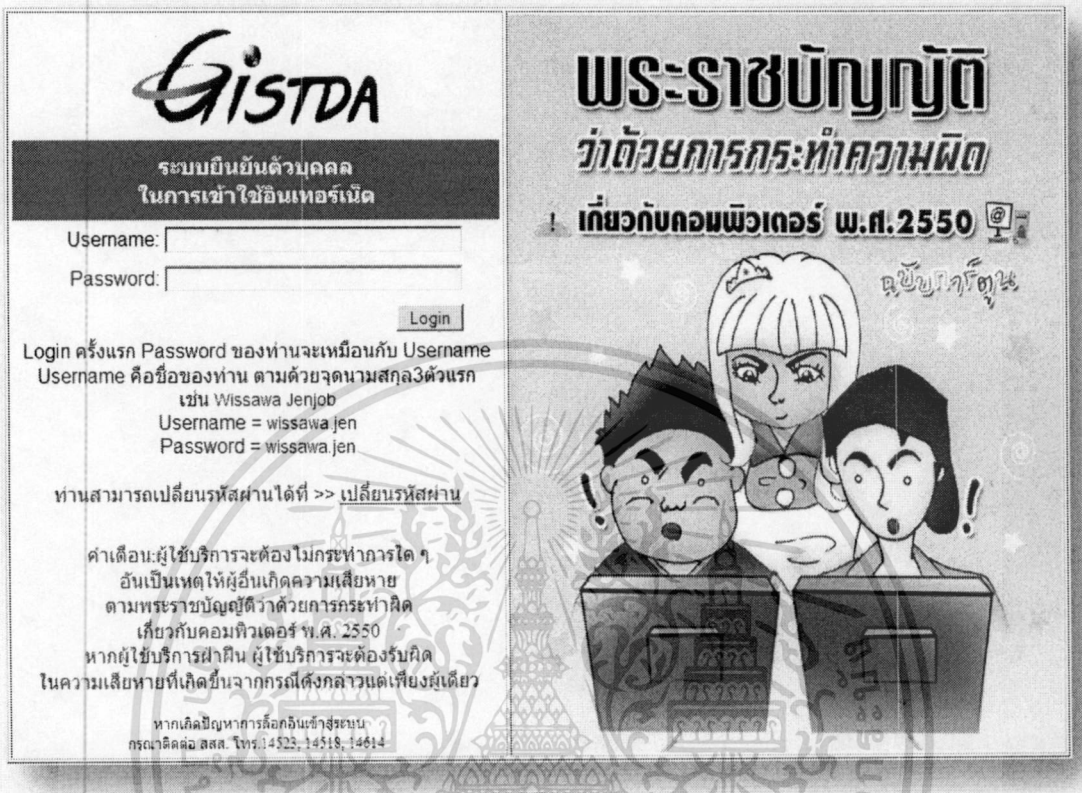
รูปที่ 3.15 แสดงอุปกรณ์บันทึกข้อมูลการจราจรทางคอมพิวเตอร์ ยี่ห้อ Fortinet รุ่น FortiAnalyzer 1000C

3.4.4 ออกแบบส่วนต่อประสานกับผู้ใช้ (User Interface Design)

ส่วนติดต่อผู้ใช้งานขณะล็อกอินของระบบเดิมมีส่วนป้อนข้อมูลอยู่ด้านซ้ายและมีส่วนของการใส่ภาพประกาศข่าวสารของสำนักงานฯ อยู่ด้านขวาและมีเมนูของการเปลี่ยนรหัสผ่าน ดังรูปที่ 3.16

รูปที่ 3.16 แสดงส่วนต่อประสานกับผู้ใช้ (ระบบเดิม)

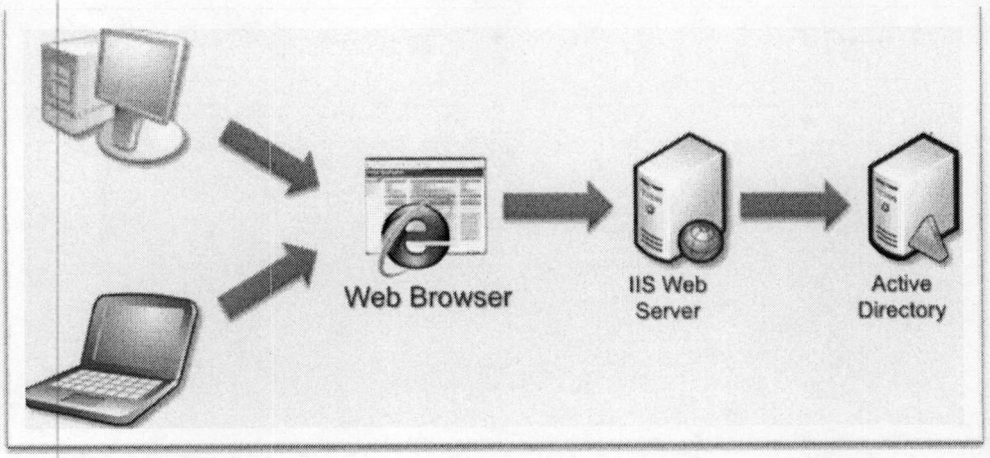
ส่วนต่อประสานผู้ใช้งานขณะล็อกอินของระบบใหม่ออกแบบให้มีส่วนป้อนข้อมูลผู้ใช้ (Username) และพาสเวิร์ด (Password) ของผู้ใช้งานอยู่ด้านซ้าย และส่วนของการใส่ภาพประกาศข่าวสารของสำนักงานอยู่ด้านขวา และมีเมนูของการเปลี่ยนรหัสผ่าน ดังรูปที่ 3.17



รูปที่ 3.17 แสดงส่วนต่อประสานกับผู้ใช้ (ระบบใหม่)

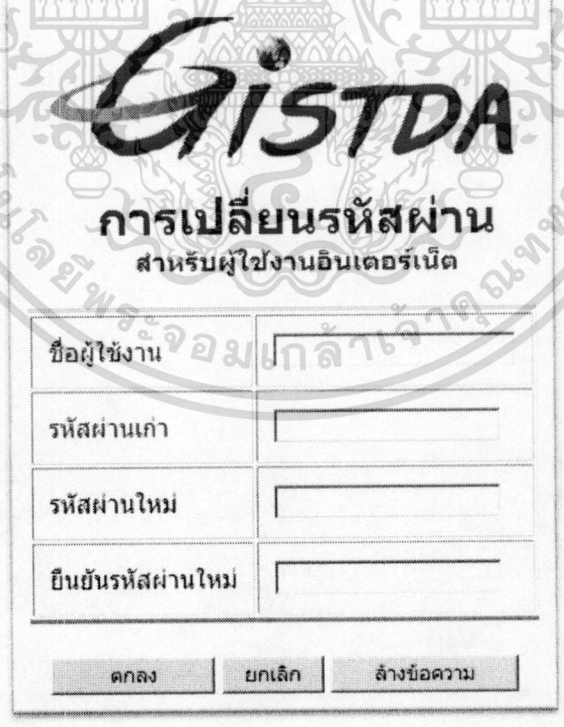
3.4.5 ออกแบบวิธีการเปลี่ยนรหัสผ่านส่วนตัวของผู้ใช้งานระบบฯ

การเปลี่ยนรหัสผ่านของผู้ใช้งานนั้น หลังจากที่ผู้ดูแลระบบสร้าง บัญชีรายชื่อและรหัสผ่านให้กับผู้ใช้แล้ว เพื่อความปลอดภัย ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านเองได้โดยใช้งานผ่านเว็บเพจ โดยจะมีการติดตั้งเว็บเซิร์ฟเวอร์บนเครื่องแอคทีฟไดเร็กทอรี ทั้ง 2 เครื่อง เพื่อให้บริการเปลี่ยนรหัสผ่านผ่านเว็บ ดังรูปที่ 3.18



รูปที่ 3.18 แสดงรูปแบบการเปลี่ยนรหัสผ่านส่วนตัวของผู้ใช้งานผ่านเว็บเพจของระบบใหม่

ในการออกแบบส่วนต่อประสานกับผู้ใช้งานเพื่อการเปลี่ยนรหัสผ่านนั้น มีฟอร์มให้ผู้ใช้กรอก ดังนี้ ชื่อผู้ใช้งาน รหัสผ่านเก่า รหัสผ่านใหม่ และฟอร์มของการยืนยันรหัสผ่านใหม่ เมื่อผู้ใช้กรอกข้อมูลถูกต้อง แอคทีฟไดเร็กทอรี จะทำการแก้ไขข้อมูลรหัสผ่านตามรหัสผ่านใหม่ที่ผู้ใช้ป้อนข้อมูลเข้ามา ดังรูปที่ 3.19



รูปที่ 3.19 แสดงรูปแบบการเปลี่ยนรหัสผ่านส่วนตัวของผู้ใช้งานระบบใหม่

3.4.6 ขั้นตอนการขอลงทะเบียนใช้งานอินเตอร์เน็ตสำหรับเข้าใช้งานระบบพิสูจน์ตัวตนฯ

เมื่อพัฒนาระบบพิสูจน์ตัวตนระบบใหม่แล้วเสร็จ ขั้นตอนสุดท้ายที่ต้องดำเนินการเพื่อให้ผู้ใช้งานอินเตอร์เน็ตสามารถใช้งานระบบใหม่ที่พัฒนาขึ้นได้อย่างมีประสิทธิภาพ คือ การออกแบบและกำหนดขั้นตอนการขอใช้งานอินเตอร์เน็ต ซึ่งได้ออกแบบขั้นตอนการขอใช้งานไว้ตามลำดับดังนี้

3.4.6.1 เจ้าหน้าที่สำนักงานฯ กรอกเอกสารลงทะเบียนผู้ใช้อินเตอร์เน็ต

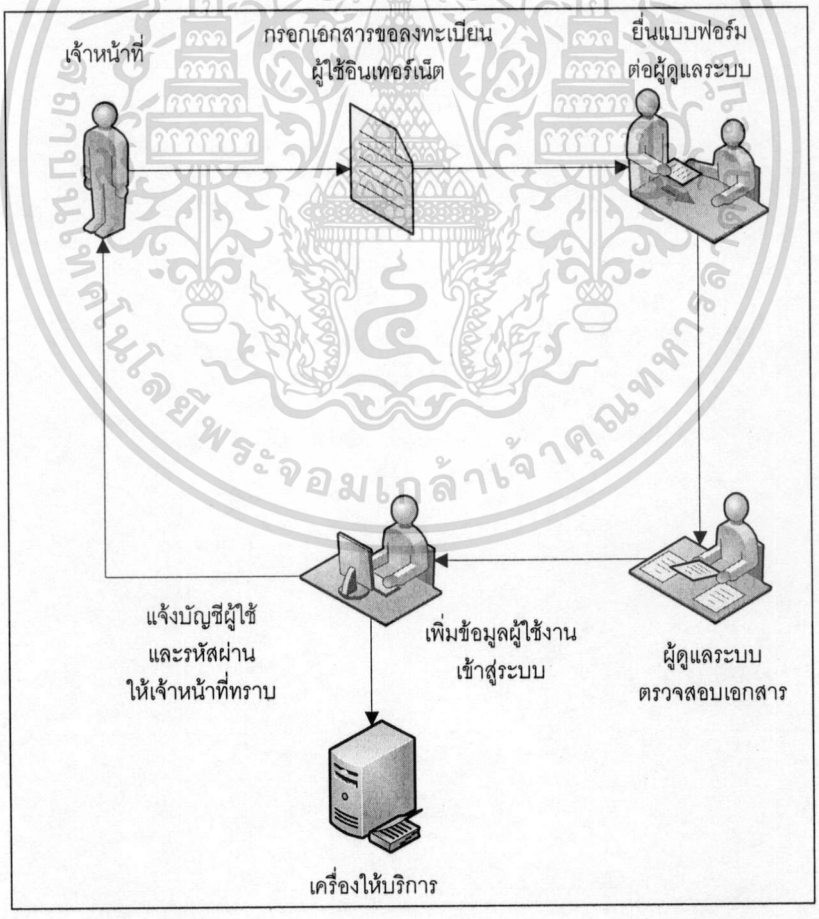
3.4.6.2 เจ้าหน้าสำนักงานฯ ยื่นแบบฟอร์มต่อผู้ดูแลระบบ

3.4.6.3 ผู้ดูแลระบบตรวจสอบเอกสารและความถูกต้องของเอกสาร

3.4.6.4 ผู้ดูแลระบบเพิ่มข้อมูลผู้ใช้งานเข้าสู่ระบบ

3.4.6.5 ผู้ดูแลระบบแจ้งเจ้าหน้าที่ทราบเกี่ยวกับบัญชีผู้ใช้

ขั้นตอนการขอใช้งาน แสดงดังรูปที่ 3.20 และฟอร์มการขอใช้งาน แสดงดังรูปที่ 3.21



รูปที่ 3.20 แสดงขั้นตอนการขอลงทะเบียนใช้งานอินเตอร์เน็ต

แบบฟอร์มขอทะเบียนผู้ใช้ระบบอินเทอร์เน็ตของ สทอภ.

วันที่..... เดือน ..... พ.ศ. .....

เรียน หัวหน้าฝ่ายบริหารเครือข่ายและการสื่อสาร สำนักเทคโนโลยีสารสนเทศและการสื่อสาร

ข้าพเจ้า ❑ นาย ❑ นาง ❑ นางสาว ❑ อื่น ๆ ระบุ .....

ชื่อ (ภาษาไทย).....นามสกุล.....

ชื่อ (ภาษาอังกฤษ) .....นามสกุล.....

ตำแหน่ง.....

สังกัด ฝ่าย / กลุ่ม.....

สำนัก / ศูนย์.....

มีความประสงค์ขอทะเบียนผู้ใช้ระบบอินเทอร์เน็ตของ สทอภ. โดยยอมรับข้อกำหนดและความรับผิดภายใต้ พรบ. ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ๒๕๕๐ ทุกประการ

ลงชื่อ.....

ผู้ขอทะเบียน

ลงชื่อ.....

ผู้บังคับบัญชา

– ส่วนของเจ้าหน้าที่ _____

กำหนดทะเบียนผู้ใช้อินเทอร์เน็ตคือ.....

ตั้งแต่วันที่..... เดือน ..... พ.ศ. ..... ถึง วันที่..... เดือน ..... พ.ศ. .....

ลงชื่อ.....

หัวหน้าฝ่ายบริหารเครือข่ายและการสื่อสาร

รูปที่ 3.21 แสดงแบบฟอร์มการขอลงทะเบียนผู้ใช้ระบบอินเตอร์เน็ตของสำนักงานฯ

3.4.7 การเพิ่มข้อมูลผู้ใช้เข้าสู่ระบบพิสูจน์ตัวตนระบบใหม่

ขั้นตอนการเพิ่มข้อมูลผู้ใช้เข้าสู่ระบบพิสูจน์ตัวตนระบบใหม่ สามารถสรุปได้โดยใช้แผนภาพกิจกรรม (Activity Diagram) แสดงลำดับกิจกรรมของการทำงาน (Work Flow) และแสดง

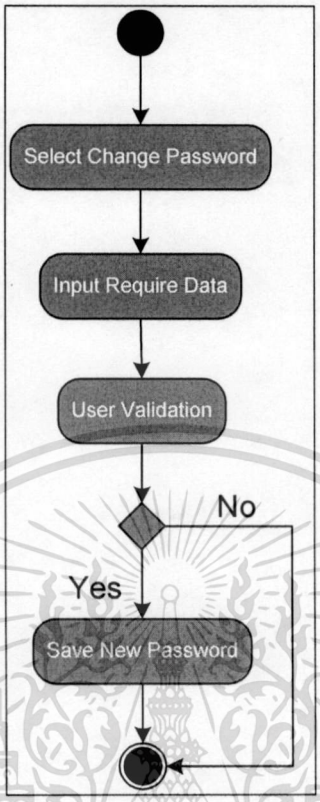
ทางเลือกที่เกิดขึ้น แผนภาพกิจกรรมจะแสดงขั้นตอนการทำงานในการปฏิบัติการ โดยประกอบไปด้วยสถานะต่างๆ ที่เกิดขึ้นระหว่างการทำงาน และผลจากการทำงานในขั้นตอนต่าง ๆ ดังรูปที่ 3.22-3.24

วงกลมสีดำ คือ จุดเริ่มต้น เรียก Initial State

วงกลมสีดำ มีวงล้อมอีกชั้น คือ จุดสิ้นสุด เรียก Final State

รูปที่ 3.22 แสดงการเพิ่มข้อมูลผู้ใช้งานอินเตอร์เน็ตใหม่เข้าสู่ระบบ โดยผ่านแอคทีฟไดเร็กทอรี

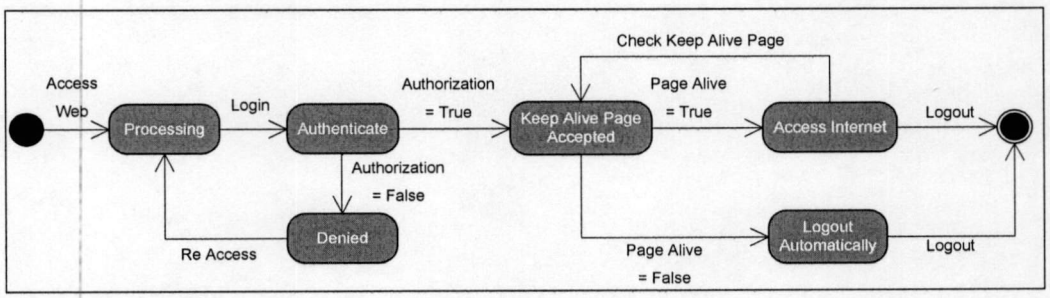
3.4.8 Activity Diagram การเปลี่ยนรหัสผ่าน



รูปที่ 3.23 แสดงการเปลี่ยนรหัสผ่านส่วนตัวของผู้ใช้งานระบบผ่าน Webpage

3.4.9 รายละเอียดของการทำงานของระบบในแต่ละช่วง

State Chart Diagram เป็นแผนภาพที่แสดงให้เห็นถึงปฏิสัมพันธ์ (Interaction) ระหว่างออบเจ็กต์ State Chart Diagram จะเน้นที่การแสดงให้เห็นถึงสถานะ (State) การเปลี่ยนสถานะ (Transition) ที่มีต่อเหตุการณ์ (Event) ที่เกิดขึ้นในช่วงชีวิตของออบเจ็กต์ 1 ช่วง



รูปที่ 3.24 แสดง State Chart Diagram

บทที่ 4

การทดสอบและผลการทดสอบ

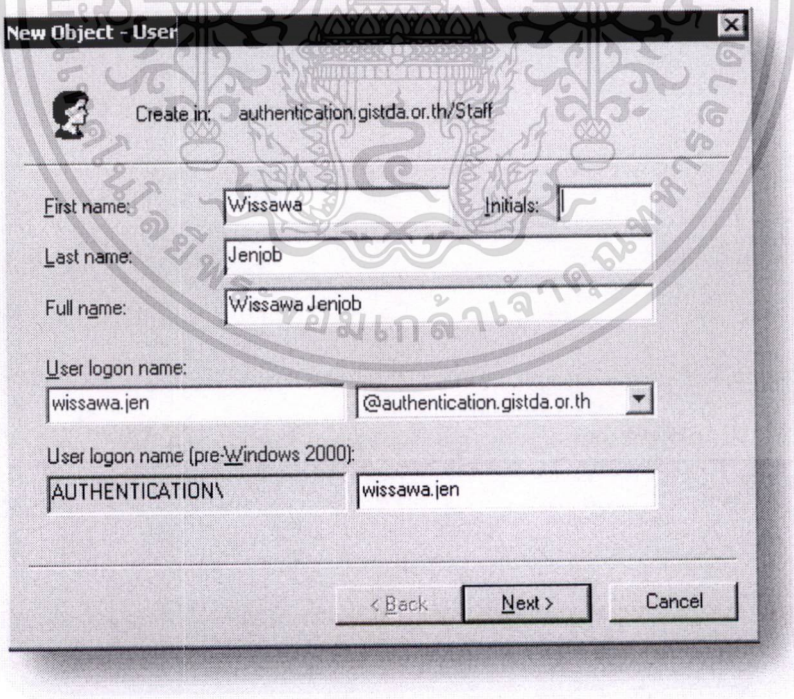
ในบทนี้จะเป็นการทดสอบการทำงานทั้งหมดของระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเทอร์เน็ต ระบบใหม่ที่ได้ออกแบบและพัฒนาขึ้น

4.1 การทดสอบการเพิ่มข้อมูลผู้ใช้งาน

4.1.1 การเพิ่มข้อมูลบัญชีผู้ใช้งาน เข้าสู่ระบบแอคทีฟไดเร็กทอรีผ่านเครื่องเซิร์ฟเวอร์ AUTHEN-1 ด้วย User = wissawa.jen

4.1.1.1 ส่วนของการเพิ่มรายชื่อผู้ใช้งานลงในแอคทีฟไดเร็กทอรี มีขั้นตอน ดังนี้

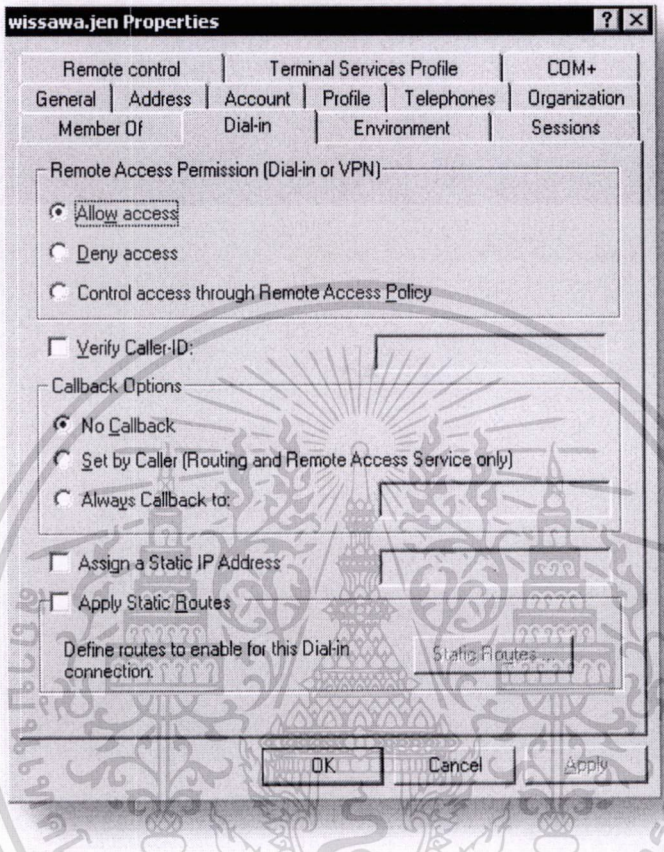
- ที่ Windows Server 2003 เลือก Administrative Tools เลือก Active Directory User and Computers และทำการเลือก New User ดังรูปที่ 4.1
- ให้เพิ่มข้อมูลผู้ใช้งานเข้าสู่ระบบ ประกอบด้วย First name, Last name, และสำคัญตรงช่องของ User logon name: ในการทดสอบนี้ User logon name = wissawa.jen



รูปที่ 4.1 แสดงการเพิ่มข้อมูลบัญชีรายชื่อผู้ใช้งานบนแอคทีฟไดเร็กทอรีเซิร์ฟเวอร์ AUTHEN-1

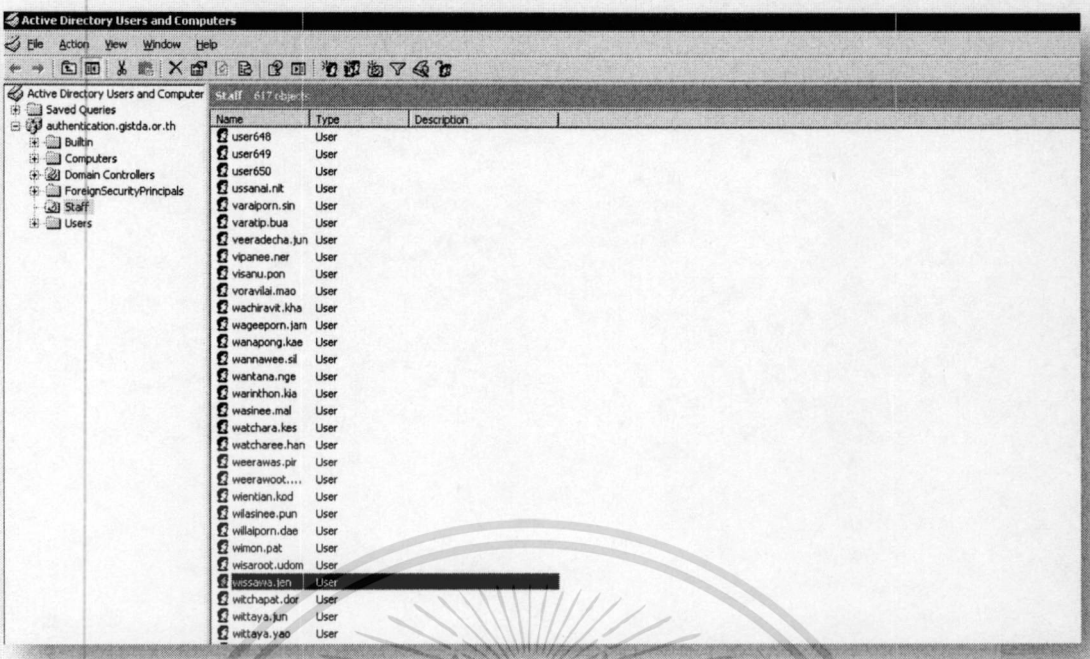
4.1.1.2 ส่วนของการอนุญาตให้ผู้ใช้งานใช้งานรายชื่อได้ มีขั้นตอนดังนี้

- เมื่อทำการเพิ่มรายชื่อผู้ใช้งานลงในแอคทีฟไดเร็กทอรีเรียบร้อยแล้ว ให้เลือกที่ Properties ของผู้ใช้งาน และเลือก Allow access ดังรูปที่ 4.2



รูปที่ 4.2 แสดงการอนุญาตให้ผู้ใช้งานใช้งานรายชื่อได้

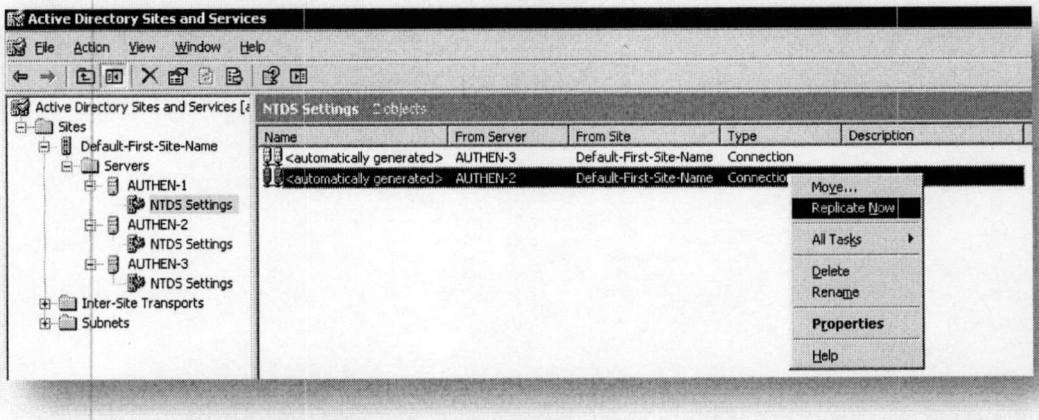
เมื่อข้อมูลผู้ใช้เพิ่มเข้าสู่ระบบแล้ว ระบบจะแสดงรายชื่อของเจ้าหน้าที่ที่ได้ทำการเพิ่มเข้าสู่ระบบ ดังรูปที่ 4.3



รูปที่ 4.3 แสดงรายชื่อผู้ใช้ ที่ทำการเพิ่มเข้าสู่ระบบเครื่อง AUTHEN-1

4.2 การทดสอบการทำสำเนาบัญชีรายชื่อผู้ใช้งาน

การทำสำเนาบัญชีรายชื่อผู้ใช้งานระหว่างเซิร์ฟเวอร์ AUTHEN-1 และ AUTHEN-2 โดยปกติแอคทีฟไดเร็กทอรีจะทำสำเนาถึงกันแบบอัตโนมัติประมาณ 15 วินาที บน Windows Server 2003 หากการทำสำเนาบัญชีรายชื่อระหว่างเซิร์ฟเวอร์ AUTHEN-1 และ AUTHEN-2 สำเร็จ สามารถทดสอบการเรพลิเคทได้ทันที โดยสามารถทดสอบได้ตามขั้นตอนดังนี้ บนเครื่อง Windows Server 2003 -> Administrative Tools -> Active Directory Sites and Services -> Sites -> Default-First-Site-Name -> Servers -> AUTHEN-1 -> NTDS Setting -> Right Click From Server -> AUTHEN-2 -> Replicate Now ดังรูปที่ 4.4

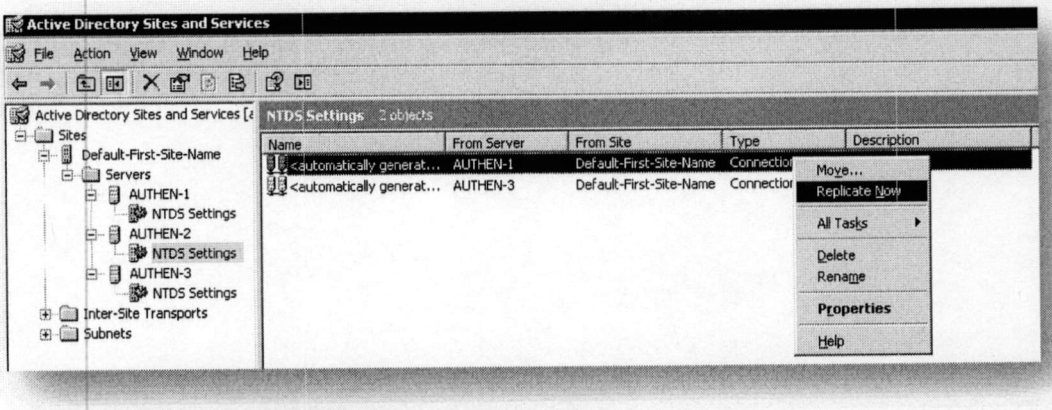


รูปที่ 4.4 แสดงการทดสอบการทำสำเนาบัญชีรายชื่อผู้ใช้งานระหว่างเซิร์ฟเวอร์ AUTHEN-1 และ AUTHEN-2 บน แอคทีฟไดเร็กทอรีไซต์และเซอร์วิส บนเครื่อง AUTHEN-1

ผลจากการทดสอบบนเครื่อง AUTHEN-1 เรพลิเคทจากเซิร์ฟเวอร์ AUTHEN-2 ผลลัพธ์ที่ได้หากเรพลิเคทสำเร็จจะพบหน้าต่างแจ้งผล Active Directory has replicated the connections. ดังรูปที่ 4.5

รูปที่ 4.5 แสดงการผลทดสอบการทำสำเนาบัญชีรายชื่อผู้ใช้งานระหว่างเซิร์ฟเวอร์ AUTHEN-1 และ AUTHEN-2บนเครื่อง AUTHEN-1

ทดสอบการเรพลิเคทระหว่างเซิร์ฟเวอร์ AUTHEN-1 และ AUTHEN-2 บน แอคทีฟไดเร็ก-ทอรีไซต์และเซอร์วิส บนเครื่อง AUTHEN-2 ดังรูปที่ 4.6



รูปที่ 4.6 แสดงการทดสอบการทำสำเนาบัญชีรายชื่อผู้ใช้งานระหว่างเซิร์ฟเวอร์ AUTHEN-1 และ AUTHEN-2 บน แอคทีฟไดเร็กทอรี ไซต์และเซอร์วิส บนเครื่อง AUTHEN-2

ผลจากการทดสอบบนเครื่อง AUTHEN-1 เรพลิเคทจากเซิร์ฟเวอร์ AUTHEN-2 ผลลัพธ์ที่ได้ หากเรพลิเคทสำเร็จจะพบหน้าต่างแจ้งผล Active Directory has replicated the connections. ดังรูปที่ 4.7

รูปที่ 4.7 แสดงการผลทดสอบการทำสำเนาบัญชีรายชื่อผู้ใช้งาน ระหว่างเซิร์ฟเวอร์ AUTHEN-1 และ AUTHEN-2

4.3 การทดสอบการพิสูจน์ตัวตนสำหรับอินเตอร์เน็ตผ่านอุปกรณ์ไฟร์วอลล์ Fortigate620B (ศูนย์ราชการแจ้งวัฒนะ)

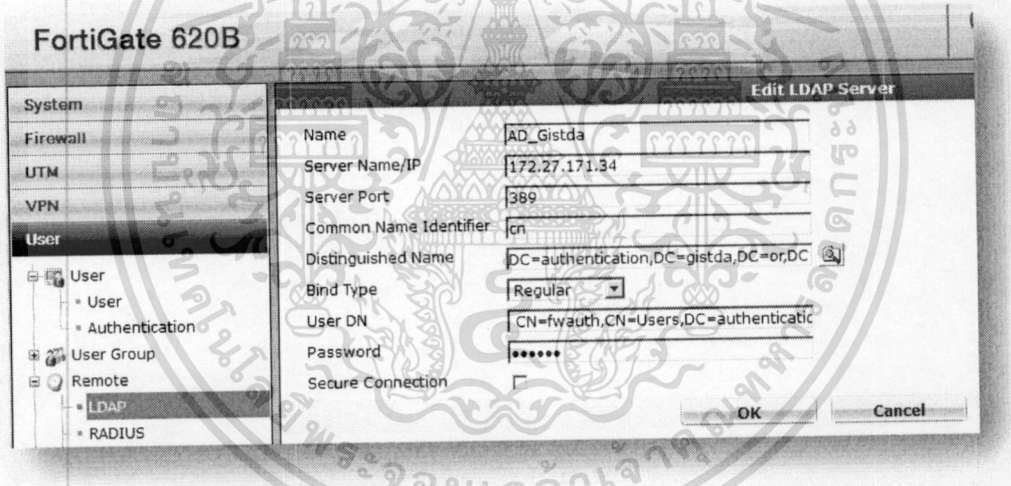
4.3.1 ส่วนของการตั้งค่า แอล-แด็บเซิร์ฟเวอร์บนอุปกรณ์ Firewall Fortigate 620B

firmwareที่ใช้ คือ รุ่น FG620B-4.00-build441

4.3.1.1 ทำการสร้างผู้ใช้ในบนแอคทีฟไดเร็กทอรี 1 ผู้ใช้เพื่อให้อุปกรณ์ Fortigate - Firewall สามารถเรียกใช้ผู้ใช้ที่สร้างไว้อยู่แล้วในแอคทีฟไดเร็กทอรีเพื่อมาทำการพิสูจน์ตัวตนในการทดสอบนี้ได้สร้างชื่อ User : fwauth , Password : fwauth1

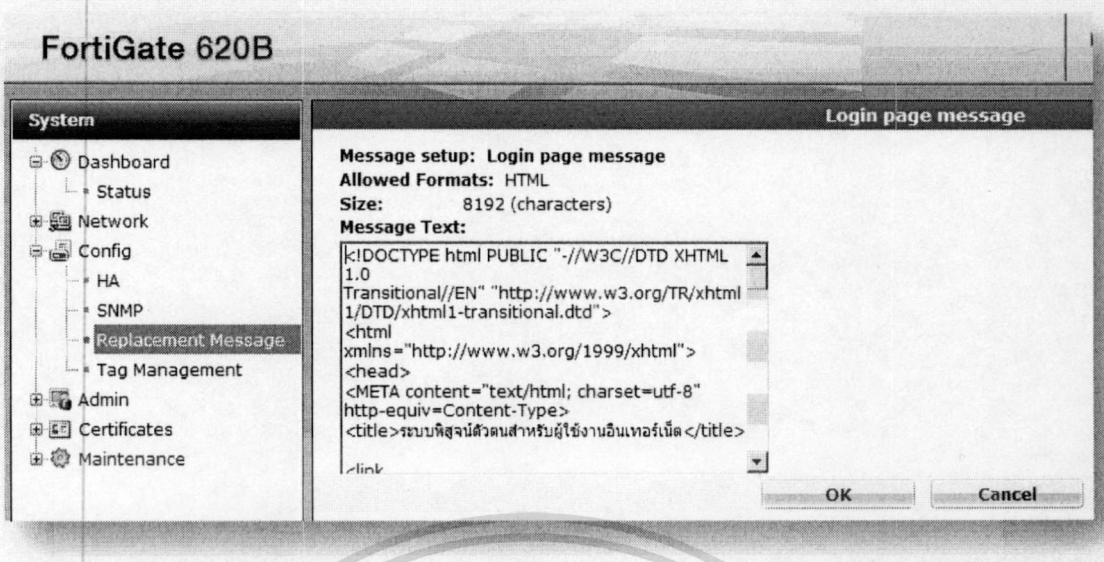
4.3.1.2 ทำการล็อกอินเข้าไปที่ตัวไฟร์วอลล์ Fortigate620B จากนั้นเข้าไปที่เมนู User -> Remote -> LDAP คลิกเลือกที่เมนู Create New และทำการใส่ค่าต่างๆ ดังนี้ ดังรูปที่ 4.8

- Name: AD_Gistda และ Server Name/IP: 172.27.171.34 (หมายเลขไอพีแอดเดรสของเครื่องแอคทีฟไดเร็กทอรีเครื่องที่ 1 ติดตั้งที่ศูนย์ราชการแจ้งวัฒนะ)
- Server Port: 389 และ Common Name Identifier: cn
- Distinguished Name: dc=authentication,dc=gistda,dc=or,dc=th (แอคทีฟ-ไดเร็กทอรีที่ Promote ขึ้น มีชื่อโดเมนเนมว่า authentication.gistda.or.th)
- Bine Type: Regular
- User DN: cn=fwauth,cn=users,dc=authentication,dc=gistda,dc=or,dc=th (อ้างอิงตามผู้ใช้ที่ได้สร้างไว้ในขั้นตอนที่ 1.1)



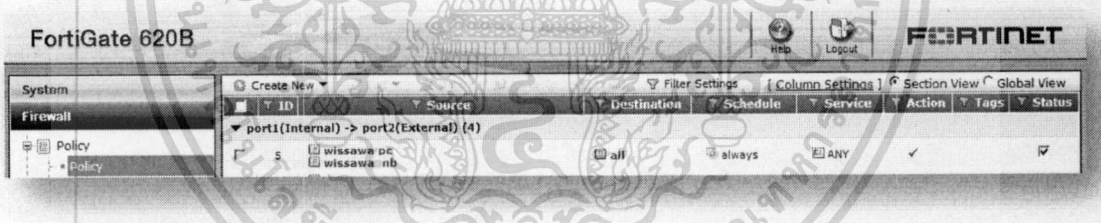
รูปที่ 4.8 แสดงการเพิ่มไอพีของเครื่องแอคทีฟไดเร็กทอรีเข้าสู่บนอุปกรณ์ไฟร์วอลล์ Fortigate620B ด้วยโปรโตคอล แอล-แด็บ

เมื่อทำการตั้งค่าการเชื่อมต่อแอคทีฟไดเร็กทอรีด้วยโปรโตคอลแอล-แด็บ บนตัวอุปกรณ์ไฟร์วอลล์ เสร็จเรียบร้อยแล้ว จากนั้นจึงทำการสร้างหน้าต่างล็อกอินด้วยเอกสาร HTML เพื่อแสดงผลให้ผู้ใช้งานป้อนค่า ชื่อผู้ใช้และพาสเวิร์ดก่อนการเชื่อมต่ออินเทอร์เน็ต โดยการเลือกเมนู System -> Config -> Replacement Message -> Login page message โดยสามารถพิมพ์เอกสาร HTML ลงไปในหน้าต่างได้ในช่อง Message Text: ดังรูปที่ 4.9



รูปที่ 4.9 แสดงการแก้ไขไฟล์ HTML สำหรับ Login Page บนอุปกรณ์ไฟร์วอลล์ Fortigate620B

ในส่วนของการสร้าง Policy บนอุปกรณ์ไฟร์วอลล์ Fortigate 620B ด้วย firmware ที่ใช้คือรุ่น FG620B-4.00-build441 นั้นทำได้โดยการเลือกเมนู Firewall -> Policy -> Policy และทำการเลือก Create New ดังรูปที่ 4.10



รูปที่ 4.10 แสดงการตั้งค่าไฟร์วอลล์ โพลิซี (Firewall Policy) เพื่อให้ไฟร์วอลล์ทำหน้าที่พิสูจน์ทราบตัวตน

4.3.2 ส่วนของการอนุญาตให้ผู้ใช้งานใช้งานรายชื่อได้ ดังรูปที่ 4.11 ซึ่งมีขั้นตอนดังนี้

4.3.2.1 ในการทดสอบ ณ ศูนย์ราชการแจ้งวัฒนะได้ทำการวางตำแหน่งอุปกรณ์ไฟร์วอลล์ให้ทำงานในลักษณะทรานส์พาเรนท์ ไฟร์วอลล์ (Transparent- Firewall) โดยวางขวางระบบซึ่ง Port1 (Internal) จะเป็นขาที่ต่อเน็ตเวิร์กภายในและ Port2 (External) จะเป็นขาที่ต่อเน็ตเวิร์กภายนอก

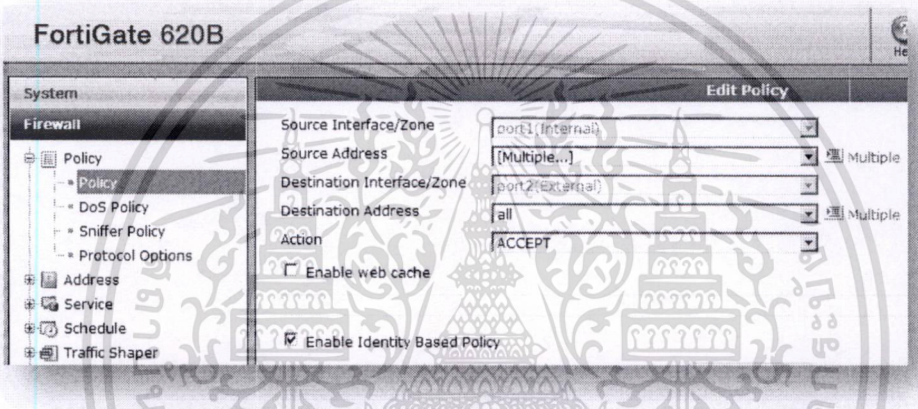
4.3.2.2 ตั้งค่า Source Interface/Zone เป็น Port1(Internal)

4.3.2.3 เลือกผู้ใช้งานตามหมายเลขไอพีแอดเดรสของเครื่องที่จะให้ทำการพิสูจน์ตัวตนก่อนการใช้งานอินเทอร์เน็ตภายนอกด้วยการเลือกหัวข้อ [Multiple…] และทำการเลือกหมายเลขไอพีที่ต้องการ ในการทดสอบนี้เลือก IP 172.27.104.60

4.3.2.4 ทำการตั้งค่า Destination Interface/Zone เป็น Port2 (External)

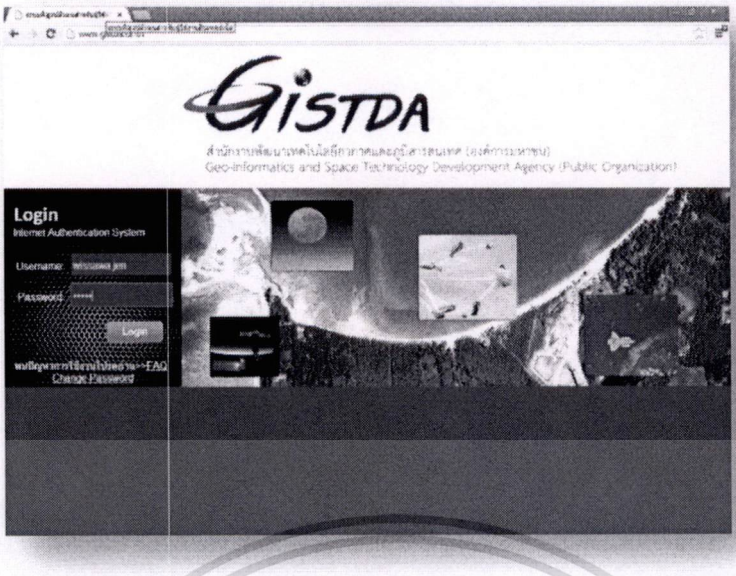
4.3.2.5 ในส่วนของ Action ให้เลือก ACCEPT

4.3.2.6 คลิกเลือกในช่อง Enable Identity Based Policy เพื่อทำการเปิดใช้งานการพิสูจน์ตัวตนด้วยอุปกรณ์ไฟร์วอลล์



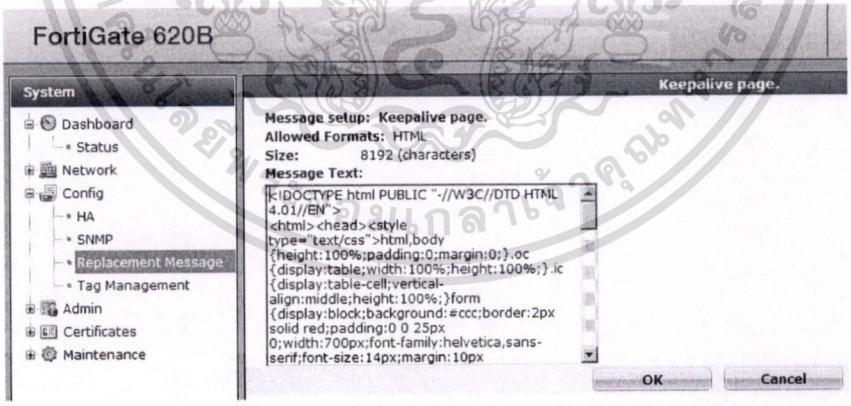
รูปที่ 4.11 แสดงการตั้งค่า Identity Based Policy บนอุปกรณ์ไฟร์วอลล์ Fortigate

เมื่อนำไอพีตรงตามโพลิซี เปิดเว็บเบราเซอร์ เนื่องจากอุปกรณ์ไฟร์วอลล์อยู่ในลักษณะขวางระบบและทำการ Enable Identity Based Policy เพื่อทำการเปิดใช้งานการพิสูจน์ตัวตนด้วยอุปกรณ์ไฟร์วอลล์แล้วผู้ใช้จะพบกับเอกสาร HTML จากการออกแบบหน้าเว็บเพจ ที่ได้ทำการใส่ลงไปบนไฟร์-วอลล์ ในส่วนของหน้าต่างข้อความล็อกอิน (Login Page Message) ก่อนหน้านี้แสดงขึ้นมา ดังรูปที่ 4.12



รูปที่ 4.12 แสดงหน้าต่างการล็อกอินและทำการล็อกอินโดยใช้บัญชีรายชื่อจากเครื่องเซิร์ฟเวอร์AUTHEN-1

จากนั้นทดสอบใส่เอกสาร HTML สำหรับ Keepalive page สำหรับใช้เป็นหน้าเว็บเพจคงสถานะของการเข้าใช้งานอินเตอร์เน็ต หากผู้ใช้งานปิดหน้าต่างดังกล่าวผู้ใช้งานจะไม่สามารถใช้งานอินเตอร์เน็ตได้ สำหรับหน้าต่างนี้ได้ออกแบบให้สามารถกดออกจากระบบได้ ดังรูปที่ 4.13



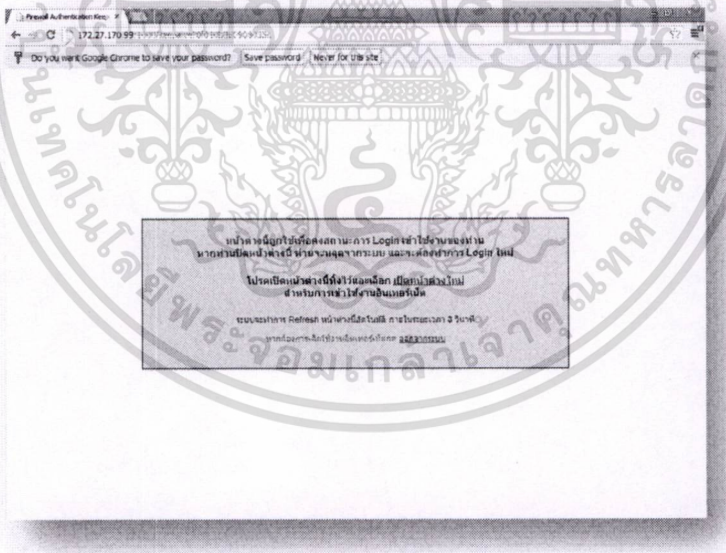
รูปที่ 4.13 แสดงการแก้ไขไฟล์ HTML สำหรับ Keepalive Page บนอุปกรณ์ไฟร์วอลล์

หลังจากล็อกอินผ่านแล้วหน้าต่างคงสถานการณ์เข้าใช้งานอินเตอร์เน็ตจะปรากฏซึ่งในหน้าจอนี้ประกอบด้วยรายละเอียดต่างๆ ดังนี้

- ข้อความแจ้งเตือนผู้ใช้งานอินเตอร์เน็ตให้เปิดหน้าต่างคงสถานะของการใช้งานอินเตอร์เน็ตทิ้งไว้

- ระยะเวลาในการรีเฟรช (Refresh) ตั้งไว้ที่ 20 วินาที เมื่อครบ 20 วินาทีแล้ว Java Script ที่ถูกเขียนในเอกสาร HTML จะทำการเรียก url ของ Keepalive Page ดังมีลักษณะของ url ดังนี้ location.href="http://172.27.170.99:1000/keepalive?050d07010a0b035c"; เพื่อทำการส่งข้อมูลเซสชัน (Session) ที่ยังเชื่อมต่ออยู่แก่อุปกรณ์ไฟร์วอลล์เพื่อไม่ให้ไฟร์วอลล์ทำการตัดเซสชันดังกล่าว ผู้ใช้งานจึงยังคงเล่นอินเตอร์เน็ตต่อไปได้ หมายเลขเซสชันที่ผู้ใช้ทำการเชื่อมต่อกับอุปกรณ์ไฟร์วอลล์ คือ 050d07010a0b035c

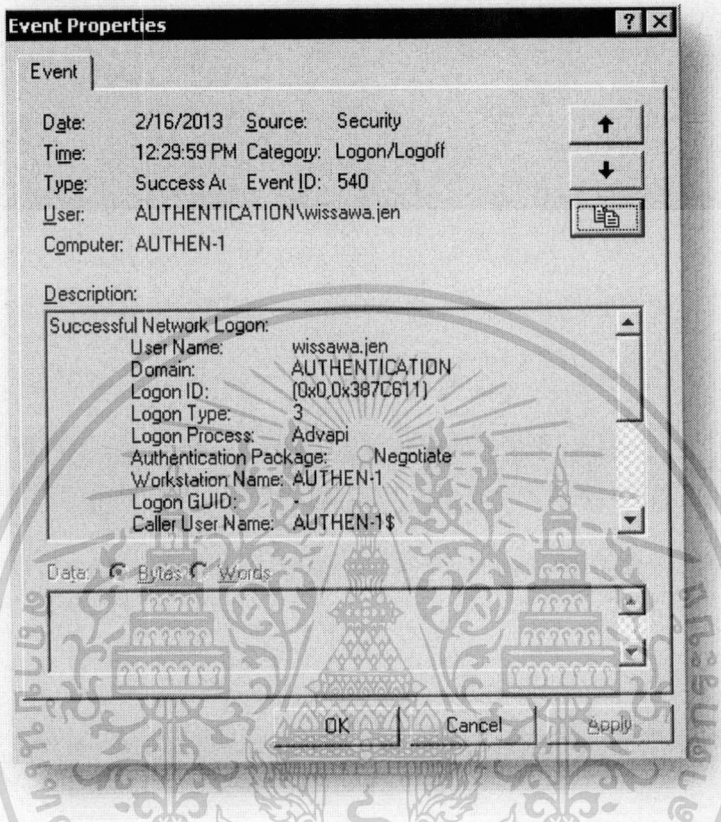
- ในส่วนลอง HTML Hyperlinks “ออกจากระบบ”
จะเป็นการเรียกเพจล็อกเอาท์ (logout) ของอุปกรณ์ Fortigate Firewall ซึ่งเป็นเว็บเพจที่ไม่สามารถแก้ไขได้โดยเรียกเว็บด้วยไอพีของอุปกรณ์ตามด้วยคำว่า logout? จากนั้นต่อด้วยหมายเลขเซสชัน เช่น http://172.27.170.99:1000/logout?050d07010a0b035c เพื่อแจ้งให้ Fortigate Firewall ทำการตัดเซสชันนี้ และหากต้องการใช้งานอินเตอร์เน็ตจะต้องทำการล็อกอินใหม่ ดังรูปที่ 4.14



รูปที่ 4.14 แสดงหน้าต่างคงสถานการณ์เข้าใช้งานอินเตอร์เน็ตหลังจากล็อกอินผ่านแล้ว

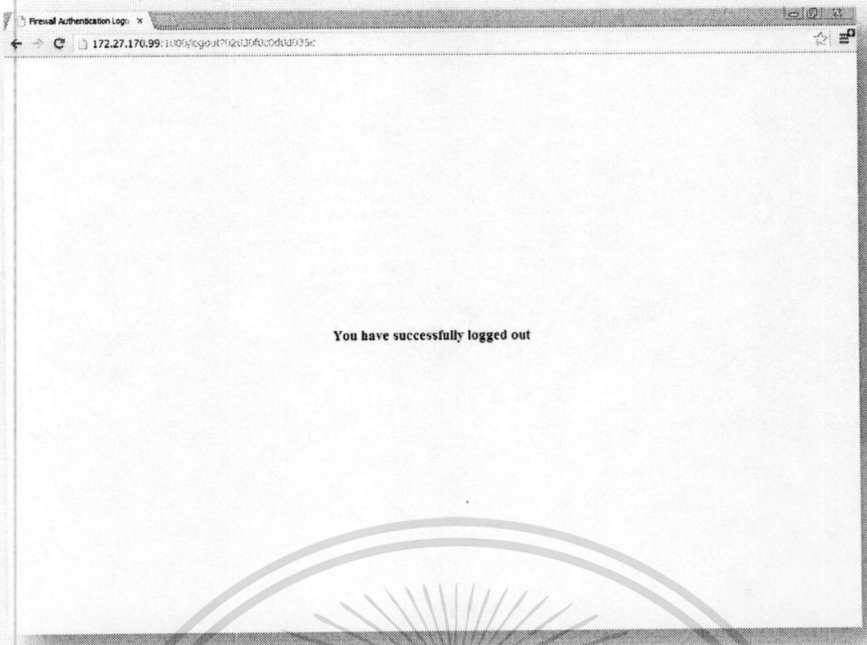
- หน้าต่าง Event Viewer ของ Windows Server 2003 R2 ในส่วนของ Security จะพบกับหน้าจอนี้ซึ่งประกอบด้วยการแสดงผลลัพธ์ของการล็อกออนใช้งานบัญชีรายชื่อบนแอคทีฟ-ไดเร็กทอรีด้วย Event ID: 540 ซึ่ง ID นี้จะแจ้งเหตุการณ์ของ Network Logon จากผลการทดสอบใช้ชื่อผู้ใช้ wissawa.jen ในการล็อกอินหน้า Login Page นั้น ในส่วนของ ผู้ใช้ในหน้าต่างนี้ก็แสดง

รายชื่อ wissawa.jen และมี Type เป็น Success Audit ซึ่งแสดงว่าสามารถทำการล็อกอินใช้งานได้ และเครื่องที่ให้บริการก็แสดงในส่วนของ Workstation Name ซึ่งแสดงชื่อเครื่องให้บริการ คือ AUTHEN-1 ดังรูปที่ 4.15



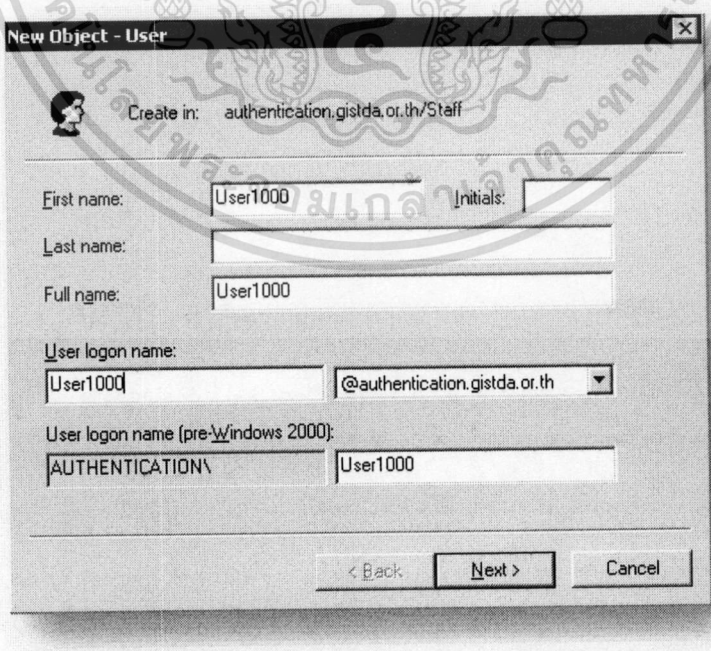
รูปที่ 4.15 แสดงการล็อกอินผ่านการใช้งานบัญชีรายชื่อบนเครื่อง AUTHEN-1

เมื่อทดสอบการกดปุ่ม “ออกจากระบบ” ผลลัพธ์ที่ได้จะพบกับหน้าต่างแสดงข้อความว่าได้ออกจากระบบเรียบร้อยแล้วด้วยข้อความ You have successfully logged out ดังรูปที่ 4.16



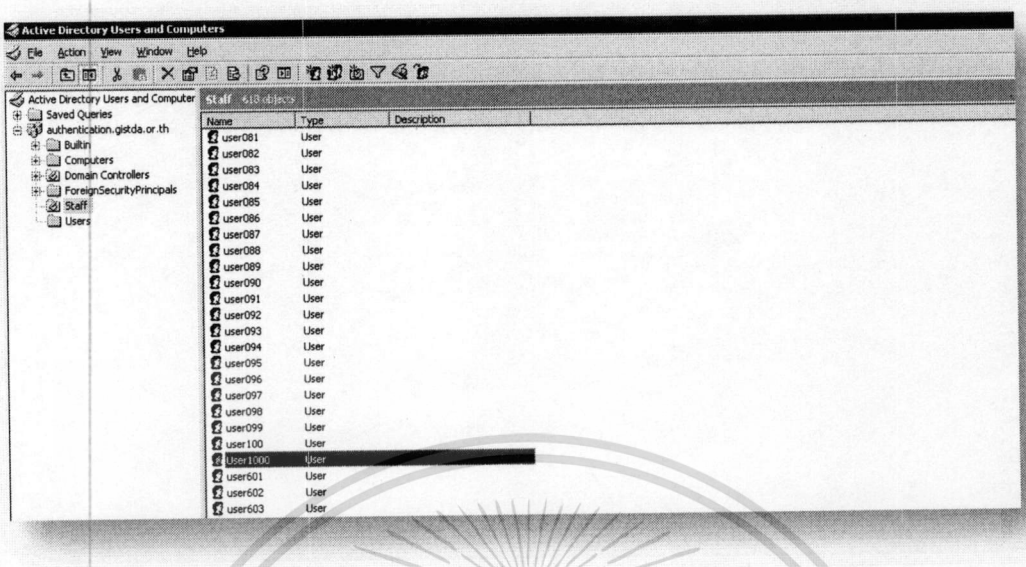
รูปที่ 4.16 แสดงการล็อกเอาท์ออกจากระบบ

ทดสอบเพิ่มข้อมูลผู้ใช้งานเข้าสู่ระบบ ประกอบด้วย First name, Last name, และ User logon -name: ในการทดสอบนี้ User logon name = User1000 บนเครื่อง AUTHEN-2 โดยตัวเครื่องถูกติดตั้งที่ศูนย์ควบคุมดาวเทียมภาคพื้นดินลาดกระบัง ดังรูปที่ 4.17



รูปที่ 4.17 แสดงการเพิ่มข้อมูลบัญชีผู้ใช้งานเข้าสู่ระบบผ่านแอคทีฟไดเร็กทอรีผ่านเครื่องเซิร์ฟเวอร์ AUTHEN-2 ด้วย User = User1000

เมื่อทำการเพิ่มผู้ใช้งานแล้วจะพบกับรายชื่อผู้ใช้งาน ดังรูปที่ 4.18



รูปที่ 4.18 แสดงรายชื่อผู้ใช้ที่ทำการเพิ่มเข้าสู่แอคทีฟไดเร็กทอรี

เนื่องจากการทดสอบข้างต้นได้ทำการสร้างผู้ใช้ในแอคทีฟไดเร็กทอรีขึ้นมา 1 ผู้ใช้เพื่อให้อุปกรณ์ Fortigate Firewall สามารถเรียกใช้ ผู้ใช้ ที่สร้างไว้อยู่แล้วในแอคทีฟไดเร็กทอรีเพื่อมาทำการพิสูจน์ตัวตน ในการทดสอบนี้ได้สร้างชื่อ User : fwauth , Password : fwauth1 ไว้เรียบร้อยแล้วจากเครื่อง 172.27.171.34 และเนื่องจากเครื่องทั้ง 2 มีการทำการสำเนาบัญชีรายชื่อซึ่งกัน จึงทำให้ User : fwauth , Password : fwauth1 ปรากฏบนเครื่อง AUTHEN-2 ด้วย ดังรูปที่ 4.19 จึงทำการล็อกอินเข้าไปที่ตัวไฟร์วอลล์ Fortigate620B จากนั้นเข้าไปที่เมนู User -> Remote -> LDAP คลิกเลือกที่เมนู Create New และทำการใส่ค่าต่างๆดังนี้

- Name : AD_Gistda
- Server Name/IP : 172.27.191.10

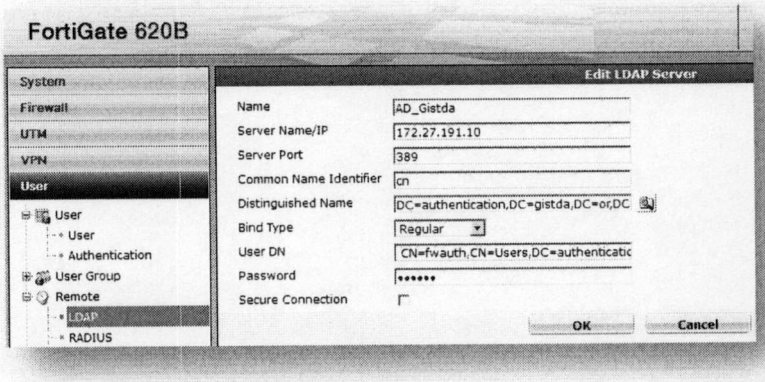
(หมายเลข IP Address ของเครื่องแอคทีฟไดเร็กทอรีเครื่องที่ 2 ติดตั้งศูนย์ควบคุมดาวเทียมภาคพื้นดิน)

- Server Port : 389
- Common Name Identifier : cn
- Distinguished Name : dc=authentication,dc=gistda,dc=or,dc=th

(Active Direcotory ที่ Promote ขึ้น มีชื่อโดเมนเนมว่า authentication.gistda.or.th)

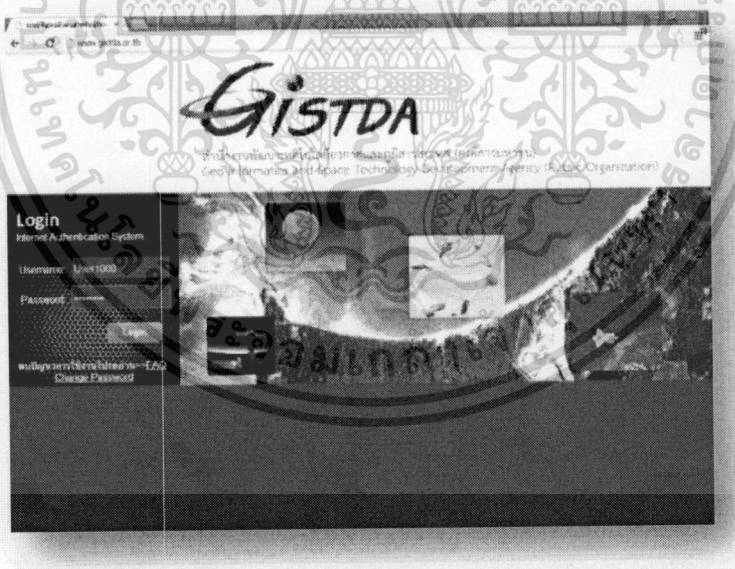
- Bine Type : Regular
- User DN : cn=fwauth,cn=users,dc=authentication,dc=gistda,dc=or,dc=th

(อ้างอิงตาม User ที่ได้สร้างไว้ ในขั้นตอนที่ 1.1)



รูปที่ 4.19 แสดงการแก้ไขค่าคอนฟิกพารามิเตอร์อุปกรณ์ไฟร์วอลล์ Fortigate 620B โดยใช้บัญชีรายชื่อจากเครื่องเซิร์ฟเวอร์AUTHEN-2 IP Address = 172.27.191.10 ณ สถานีควบคุมดาวเทียมลาดกระบัง

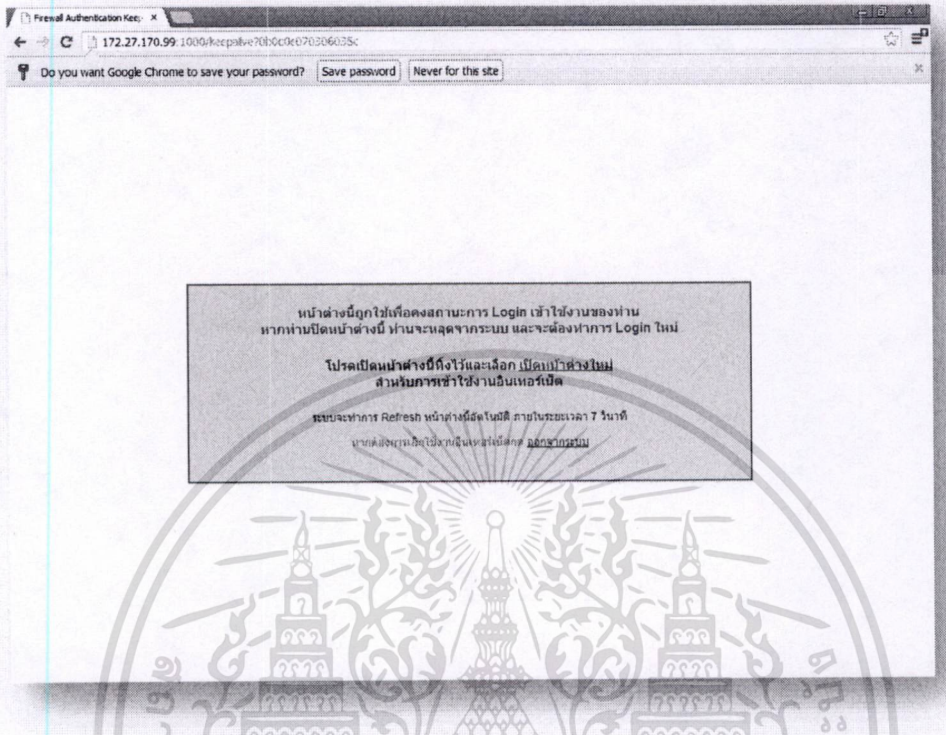
เมื่อนำไอพีตรงตามโพลิซีเปิดเว็บเบราเซอร์ เนื่องจากอุปกรณ์ไฟร์วอลล์อยู่ในลักษณะขวางระบบ และทำการ Enable Identity Based Policy เพื่อทำการเปิดใช้งานการพิสูจน์ตัวตนด้วยอุปกรณ์ไฟร์วอลล์แล้วผู้ใช้จะพบกับเอกสาร HTML จากการออกแบบหน้าเว็บเพจ ที่ได้ทำการใส่ลงไปไฟร์วอลล์ในส่วนของ Login Page Message ก่อนหน้านี้แสดงขึ้นมา ดังรูปที่ 4.20



รูปที่ 4.20 แสดงหน้าต่างการล็อกอินและทำการล็อกอินโดยใช้บัญชีรายชื่อจากเครื่องเซิร์ฟเวอร์ AUTHEN-2

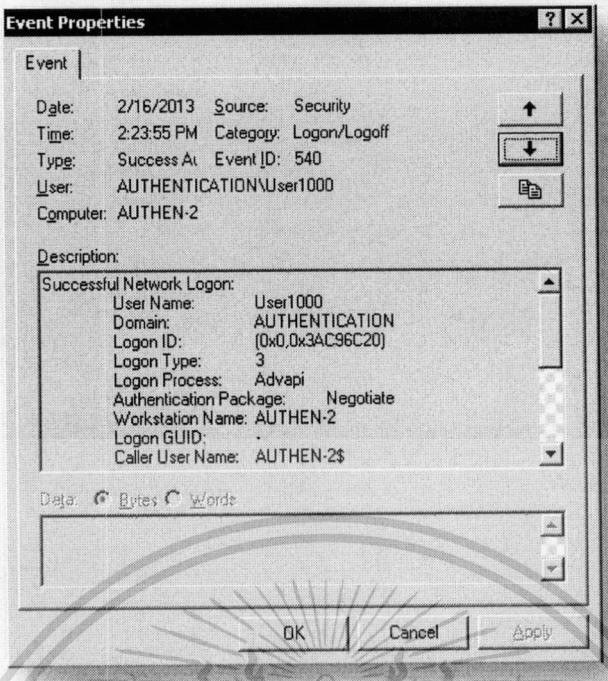
เพจล็อกเอาท์ (logout) ของอุปกรณ์ Fortigate Firewall ซึ่งเป็นเว็บเพจที่ไม่สามารถแก้ไขได้ โดยเรียกเว็บด้วยไอพีของอุปกรณ์ตามด้วยคำว่า logout? จากนั้นต่อด้วยหมายเลขเซสชัน

เช่น http://172.27.170.99:1000/logout?050d07010a0b035c เพื่อแจ้งให้ Fortigate Firewall ทำการตัดเซสชันนี้ และหากต้องการใช้งานอินเตอร์เน็ตจะต้องทำการล็อกอินใหม่ ดังรูปที่ 4.21



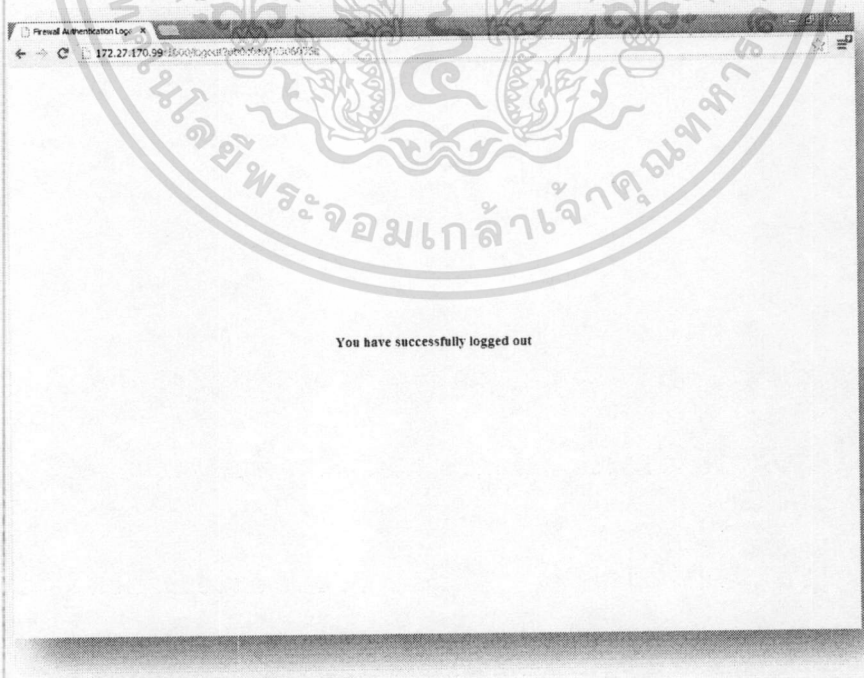
รูปที่ 4.21 เพจล็อกเอาท์

หน้าต่าง Event Viewer ของ Windows Server 2003 R2 ในส่วนของ Security ของเครื่อง AUTHEN-2 จะพบกับหน้าจอนี้ซึ่งประกอบด้วยการแสดงผลลัพธ์ของการล็อกออนใช้งานบัญชีรายชื่อบนแอคทีฟไดเร็กทอรีด้วย Event ID: 540 ซึ่ง ID นี้จะแจ้งเหตุการณ์ของ Network Logon จากผลการทดสอบใช้ username = User1000 ในการล็อกอินหน้า Login Page นั้น ในส่วนของผู้ใช้ในหน้าต่างนี้ก็แสดงรายชื่อ User1000 และมี Type เป็น Success Audit ซึ่งแสดงว่าสามารถทำการล็อกอินใช้งานได้ และ เครื่องที่ให้บริการก็แสดงในส่วนของ Workstation Name ซึ่งแสดงชื่อเครื่องให้บริการคือ AUTHEN-2 ดังรูปที่ 4.22



รูปที่ 4.22 แสดงการล็อกอินผ่านการใช้งานบัญชีรายชื่อบนเครื่อง AUTHEN-2

เมื่อทดสอบการออกจากระบบ User1000 ก็สามารถที่จะทำการออกจากระบบได้ เช่นเดียวกับ User = wissawa.jen ที่ได้ทำการทดสอบบนเครื่อง AUTHEN-1 ดังรูปที่ 4.23



รูปที่ 4.23 แสดงการล็อกเอาท์ออกจากระบบ

4.4 การทดสอบการทดสอบการพิสูจน์ตัวตนสำหรับอินเทอร์เน็ตผ่านอุปกรณ์ไฟร์วอลล์ Fortigate1000 (ศูนย์ควบคุมดาวเทียมภาคพื้นดินลาดกระบัง)

4.4.1 ส่วนของการตั้งค่าแอล-แด็บ เซิร์ฟเวอร์ บนอุปกรณ์ไฟร์วอลล์ Fortigate 1000

4.4.1.1 ผู้ใช้ในแอคทีฟไดเร็กทอรีสร้างไว้อยู่แล้ว เพื่อให้อุปกรณ์ไฟร์วอลล์ Fortigate 1000 สามารถเรียกใช้ ผู้ใช้ ที่สร้างไว้อยู่แล้วในแอคทีฟไดเร็กทอรีเพื่อมาทำการพิสูจน์ตัวตนในการทดสอบนี้ได้สร้างชื่อ User: fwauth , Password : fwauth1

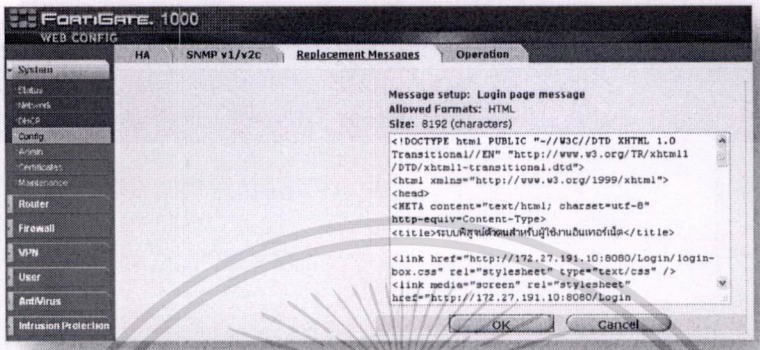
4.4.1.2 ทำการ Login เข้าไปที่ตัวไฟร์วอลล์ Fortigate 1000 จากนั้นเข้าไปที่เมนู User -> Remote -> LDAP คลิกเลือกที่เมนู Create New และทำการใส่ค่าต่างๆ ดังนี้ ดังรูปที่ 4.24

- Name : AD_Gistda
- Server Name/IP : 172.27.191.10 (หมายเลขไอพีแอดเดรสของเครื่องแอคทีฟไดเร็กทอรีเครื่องที่ 2 ติดตั้งที่ศูนย์ควบคุมดาวเทียมภาคพื้นดินลาดกระบัง)
- Server Port : 389
- Common Name Identifier : cn
- Distinguished Name : dc=authentication,dc=gistda,dc=or,dc=th (แอคทีฟไดเร็กทอรีที่Promote ขึ้น มีชื่อโดเมนเนมว่า authentication.gistda.or.th)
- Bine Type : Regular

รูปที่ 4.24 แสดงการเพิ่มไอพีของเครื่องแอคทีฟไดเร็กทอรีเข้าสู่บนอุปกรณ์ไฟร์วอลล์ Fortigate 1000 ด้วยโปรโตคอลแอล-แด็บ

4.4.2 User DN : cn=fwauth,cn=users,dc=authentication,dc=gistda,dc=or,dc=th (อ้างอิงตาม User ที่ได้สร้างไว้ในขั้นตอนที่ 1.1) เมื่อทำการตั้งค่าการเชื่อมต่อแอคทีฟไดเร็กทอรีด้วยโปรโตคอลแอล-แด็บ บนตัวอุปกรณ์ไฟร์วอลล์เสร็จเรียบร้อยแล้ว จากนั้นจึงทำการ

สร้างหน้าต่างล็อกอินด้วยเอกสาร HTML เพื่อแสดงผลให้ผู้ใช้งานป้อนค่า username และ password ก่อนการเชื่อมต่ออินเทอร์เน็ต โดยการเลือกเมนู System -> Config -> Replacement Message -> Login page message โดยสามารถพิมพ์เอกสาร HTML ลงไปในหน้าต่างได้ในช่อง Message Text: ดังรูปที่ 4.25



รูปที่ 4.25 แสดงการแก้ไขไฟล์ HTML สำหรับ Login Page บนอุปกรณ์ไฟร์วอลล์ Fortigate 1000

4.4.3 ส่วนของการอนุญาตให้ผู้ใช้งานใช้งานรายชื่อได้ มีขั้นตอน ดังนี้ ดังรูปที่ 4.26

4.4.3.1 ในการทดสอบ ได้ทำการวางตำแหน่งอุปกรณ์ไฟร์วอลล์ให้ทำงานในลักษณะวางขวางระบบ และทำ NAT ไอพีขานอก ซึ่ง Internal จะเป็นขาที่ต่อเน็ตเวิร์กภายใน และ External จะเป็นขาที่ต่อเน็ตเวิร์กภายนอก

4.4.3.2 ให้ทำการตั้งค่า Source Interface/Zone เป็น Internal

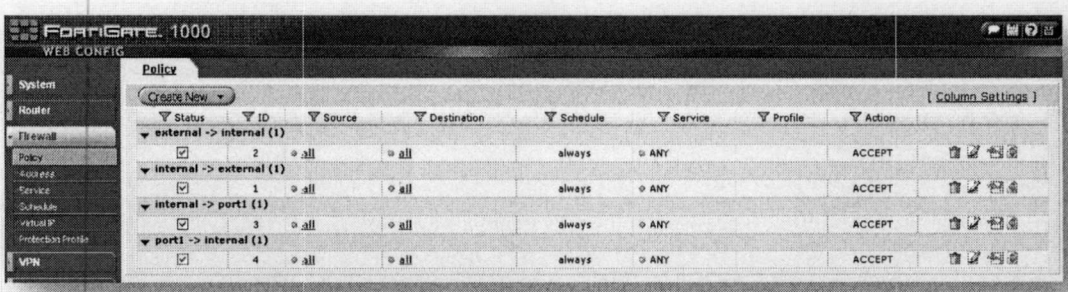
4.4.3.3 ทำการเลือกผู้ใช้งานตามหมายเลขไอพีแอดเดรสของเครื่องเจ้าหน้าที่ที่จะให้ทำการพิสูจน์ตัวตนก่อนการใช้งานอินเทอร์เน็ตภายนอกด้วยการเลือกหัวข้อ All เพื่อเลือกทั้งหมด

4.4.3.4 ให้ทำการตั้งค่า Destination Interface/Zone เป็น External

4.4.3.5 ทำการตั้งค่า Destination Address เป็น all

4.4.3.6 ในส่วนของ Action ให้เลือก ACCEPT

4.4.3.7 คลิกเลือกในช่อง Authentication เพื่อทำการเปิดใช้งานการพิสูจน์ตัวตนด้วยอุปกรณ์ Firewall

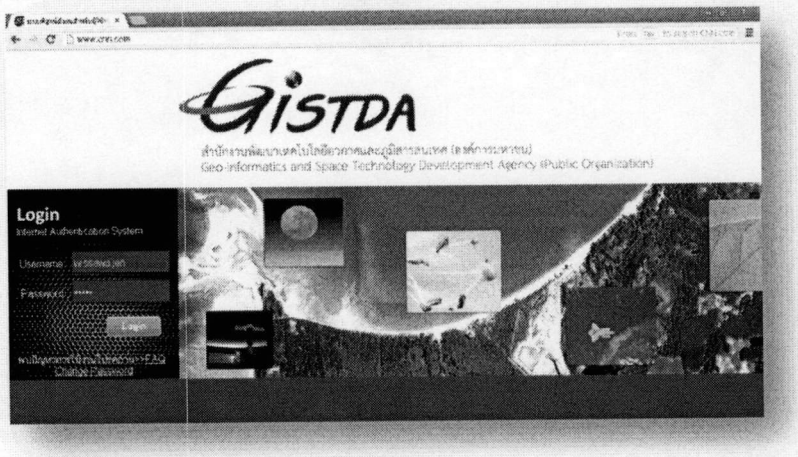


รูปที่ 4.26 แสดงการตั้งค่าไฟร์วอลล์ โพลิซี (Firewall Policy) เพื่อให้ไฟร์วอลล์ทำหน้าที่พิสูจน์ทราบตัวตน

เมื่อนำไอพีตรงตามโพลิซีเปิดเว็บเบราเซอร์ เนื่องจากอุปกรณ์ไฟร์วอลล์อยู่ในลักษณะขวางระบบ และทำการเปิดใช้งานการพิสูจน์ตัวตนด้วยอุปกรณ์ไฟร์วอลล์แล้ว ผู้ใช้จะพบกับเอกสาร HTML จากการออกแบบหน้าเว็บเพจที่ได้ทำการใส่ลงไปไฟร์วอลล์ในส่วนของ Login page message ก่อนหน้านี้แสดงขึ้นมา ดังรูปที่ 4.27

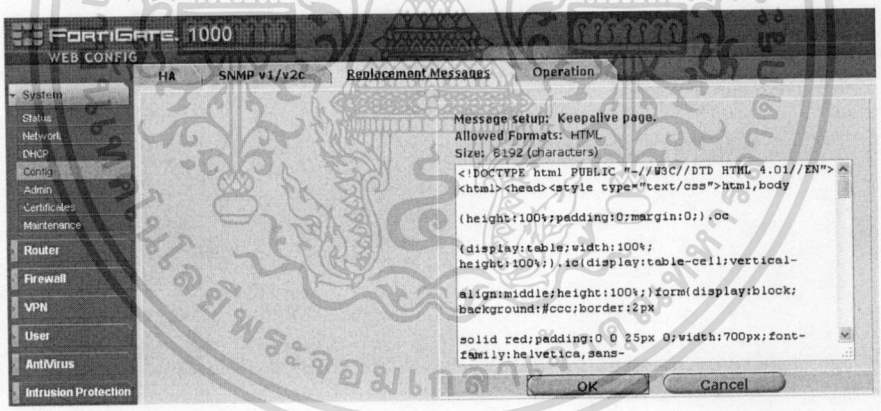
รูปที่ 4.27 แสดงการตั้งค่าโพลิซี และการ Enable Authentication บนอุปกรณ์ไฟร์วอลล์ Fortigate 1000

เมื่อนำไอพีตรงตามโพลิซี เปิดเว็บเบราเซอร์ เนื่องจากอุปกรณ์ไฟร์วอลล์อยู่ในลักษณะขวางระบบและทำการ Enable Identity Based Policy เพื่อทำการเปิดใช้งานการพิสูจน์ตัวตนด้วยอุปกรณ์ไฟร์วอลล์แล้ว ผู้ใช้จะพบกับเอกสาร HTML จากการออกแบบหน้าเว็บเพจ ที่ได้ทำการใส่ลงไปไฟร์วอลล์ในส่วนของหน้าต่างข้อความล็อกอิน (Login Page Message) ก่อนหน้านี้แสดงขึ้นมา ดังรูปที่ 4.28



รูปที่ 4.28 แสดงหน้าต่างการล็อกอินและทำการล็อกอินโดยใช้บัญชีรายชื่อจากเครื่องเซิร์ฟเวอร์ AUTHEN-2

จากนั้นทดสอบใส่เอกสาร HTML สำหรับ Keepalive page สำหรับใช้เป็นหน้าเว็บเพจคงสถานะของการเข้าใช้งานอินเตอร์เน็ต หากผู้ใช้งานปิดหน้าต่างดังกล่าวผู้ใช้งานจะไม่สามารถใช้งานอินเตอร์เน็ตได้ สำหรับหน้าต่างนี้ได้ออกแบบให้สามารถกดออกจากระบบได้ ดังรูปที่ 4.29



รูปที่ 4.29 แสดงการแก้ไขไฟล์ HTML สำหรับ Keepalive Page บนอุปกรณ์ไฟร์วอลล์ Fortigate 1000

ในหน้าจอนี้ประกอบด้วย

- ข้อความแจ้งเตือนผู้ใช้งานอินเตอร์เน็ตให้เปิดหน้าต่างคงสถานะของการใช้งานอินเตอร์เน็ตทิ้งไว้

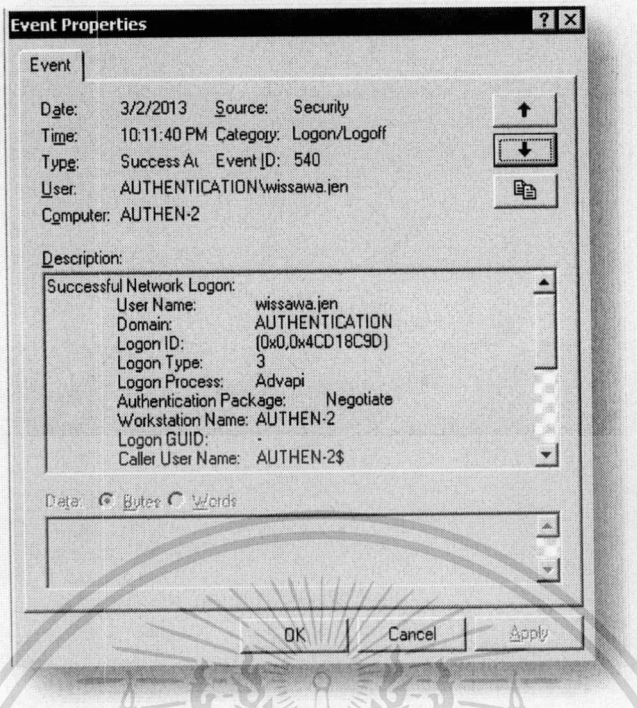
- ระยะเวลาในการรีเฟรช ตั้งไว้ที่ 20 วินาที เมื่อครบ 20 วินาทีแล้ว Java Script ในเอกสาร HTMLจะทำการเรียก location.href="http://172.27.191.253:1000/keepalive?07050b0500030b1b";

เพื่อทำการส่งข้อมูลเซสชันที่ยังเชื่อมต่ออยู่แก่อุปกรณ์ไฟร์วอลล์เพื่อไม่ให้ไฟร์วอลล์ทำการตัดเซสชันดังกล่าว ผู้ใช้งานจึงยังคงเล่นอินเทอร์เน็ตต่อไปได้ หมายเลขเซสชันที่ผู้ใช้ทำการเชื่อมต่อกับอุปกรณ์ไฟร์วอลล์ คือ 07050b0500030b1b ดังรูปที่ 4.30

- ในส่วนลอง HTML Hyperlinks "ออกจากระบบ" นี้จะเป็นการเรียกเพจ logout ของอุปกรณ์ Fortigate Firewall ซึ่งเป็นเว็บเพจที่ไม่สามารถแก้ไขได้ โดย เรียกเว็บด้วยไอพีของอุปกรณ์ตามด้วยคำว่า logout? จากนั้นต่อด้วยหมายเลขเซสชัน เช่น http://172.27.191.253:1000/logout?07050b0500030b1b เพื่อแจ้งให้ Fortigate Firewall ทำการตัด เซสชันนี้ และหากต้องการใช้งานอินเตอร์เน็ตจะต้องทำการล็อกอินใหม่

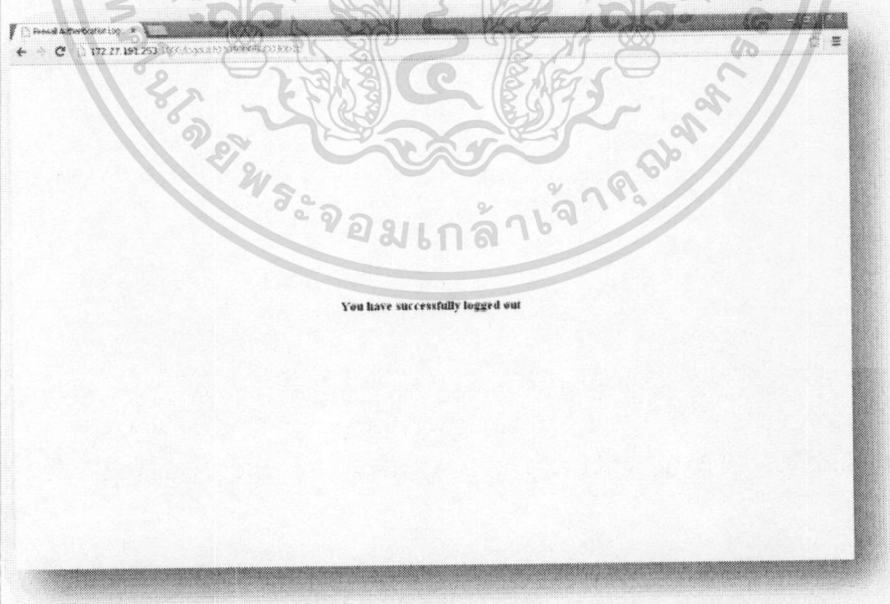
รูปที่ 4.30 แสดงหน้าต่างคงสถานการณ์เข้าใช้งานอินเตอร์เน็ตหลังจากล็อกอินผ่านแล้ว

หน้าต่าง Event Viewer ของ Windows Server 2003 R2 ในส่วนของ Security จะพบกับหน้าจอนี้ซึ่งประกอบด้วยการแสดงผลลัพธ์ของการล็อกออนใช้งานบัญชีรายชื่อบนแอคทีฟ-ไดเร็กทอรีด้วย Event ID: 540 ซึ่ง ID นี้จะแจ้งเหตุการณ์ของ Network Logon จากผลการทดสอบใช้ username wissawa.jen ในการล็อกอินหน้า Login Page นั้น ในส่วนของ User ในหน้าต่างนี้ก็แสดงรายชื่อ wissawa.jen และมี Type เป็น Success Audit ซึ่งแสดงว่าสามารถทำการล็อกอินใช้งานได้ และเครื่องที่ให้บริการก็แสดงในส่วนของ Workstation Name ซึ่งแสดงชื่อเครื่องให้บริการคือ AUTHEN-2 ดังรูปที่ 4.31



รูปที่ 4.31 แสดงการล็อกอินผ่านการใช้งานบัญชีรายชื่อบนเครื่อง AUTHEN-2

เมื่อทดสอบการกดปุ่ม “ออกจากระบบ” ผลลัพธ์ที่ได้จะพบกับหน้าต่างแสดงข้อความว่าได้ออกจากระบบเรียบร้อยแล้วด้วยข้อความ You have successfully logged out ดังรูปที่ 4.32



รูปที่ 4.32 แสดงการล็อกเอาท์ ออกจากระบบ จากเครื่องไฟร์วอลล์ Fortigate 1000

เนื่องจากการทดสอบข้างต้นได้ทำการสร้างผู้ใช้ในแอคทีฟไดเร็กทอรีขึ้นมา 1 ผู้ใช้เพื่อให้อุปกรณ์ Fortigate Firewall สามารถเรียกใช้ผู้ใช้ที่สร้างไว้อยู่แล้วในแอคทีฟไดเร็กทอรีเพื่อมาทำการพิสูจน์ตัวตน ในการทดสอบนี้ได้สร้างชื่อ User : fwauth , Password : fwauth1 ไว้เรียบร้อยแล้ว จากเครื่อง 172.27.171.341.2 ทำการ Login เข้าไปที่ตัว Firewall Fortigate 1000 จากนั้นเข้าไปที่เมนู User -> Remote -> LDAP คลิกเลือกที่เมนู Create New และทำการใส่ค่าต่างๆ ดังนี้ ดังรูปที่ 4.33

- Name : AD_Gistda

-Server Name/IP : 172.27.171.34 (หมายเลขไอพีแอดเดรสของเครื่องแอคทีฟไดเร็กทอรีเครื่องที่ 2 ติดตั้งศูนย์ราชการแจ้งวัฒนะ)

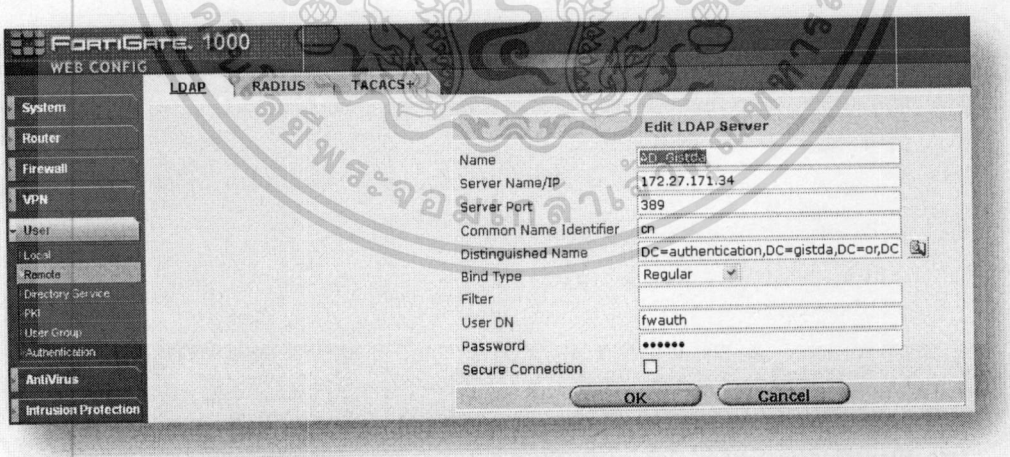
- Server Port : 389

- Common Name Identifier : cn

- Distinguished Name : dc=authentication,dc=gistda,dc=or,dc=th (แอคทีฟไดเร็กทอรีที่ Promote ขึ้น มีชื่อโดเมนเนมว่า authentication.gistda.or.th)

- Bine Type : Regular

- User DN : cn=fwauth,cn=users,dc=authentication,dc=gistda,dc=or,dc=th (อ้างอิงตามผู้ใช้ ที่ได้สร้าง ไว้ในขั้นตอนที่ 1.1)



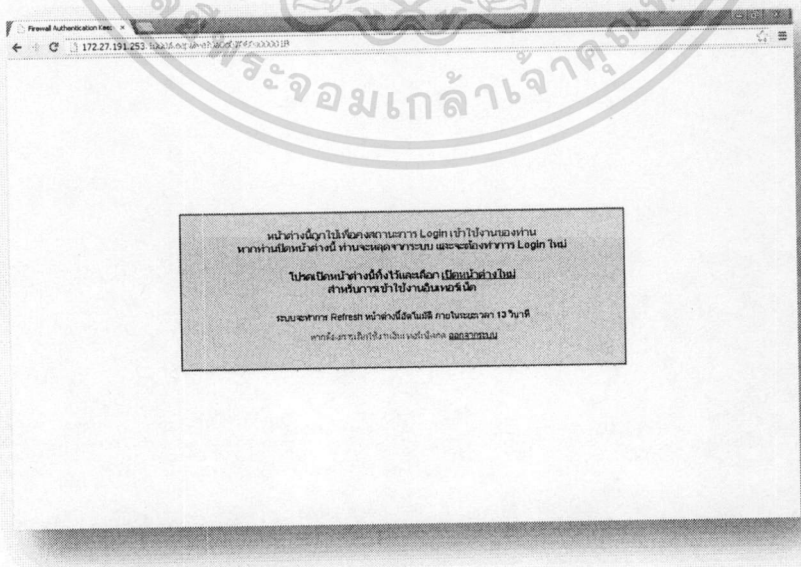
รูปที่ 4.33 แสดงการแก้ไขค่าคอนฟิกพารามิเตอร์อุปกรณ์ไฟร์วอลล์ Fortigate 1000 โดยใช้บัญชีรายชื่อจากเครื่องเซิร์ฟเวอร์ AUTHEN-1

เมื่อนำไอพีที่อยู่ด้าน Source Address เปิดเว็บเบราเซอร์ เนื่องจากอุปกรณ์ไฟร์วอลล์อยู่ในลักษณะขวางระบบ และทำการเปิดใช้งานการพิสูจน์ตัวตนด้วยอุปกรณ์ไฟร์วอลล์แล้ว

ผู้ใช้จะพบกับเอกสาร HTML จากการออกแบบหน้าเว็บเพจ ที่ได้ทำการใส่ลงไปไฟร์วอลล์ ในส่วนของ Login page message ก่อนหน้านี้แสดงขึ้นมา ดังรูปที่ 4.34

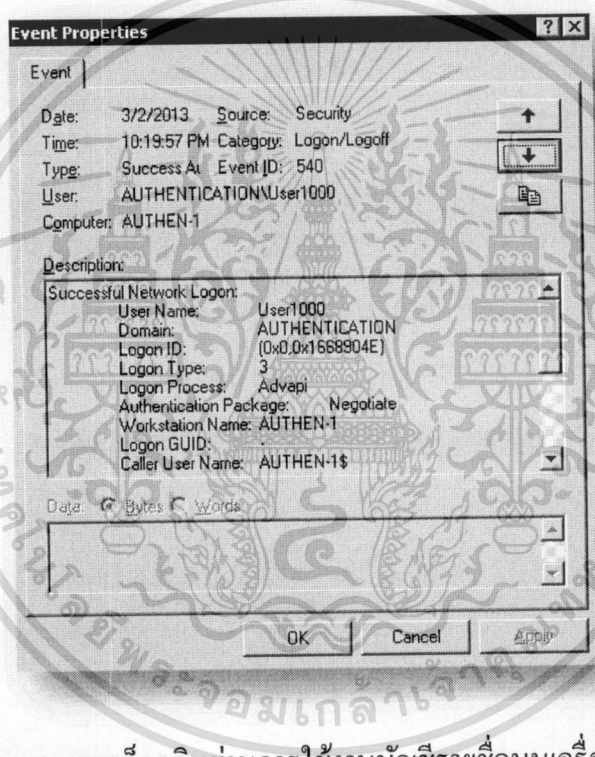
รูปที่ 4.34 แสดงหน้าต่างการล็อกอินและทำการล็อกอินโดยใช้บัญชีรายชื่อจากเครื่องเซิร์ฟเวอร์ AUTHEN-1

เพจล็อกเอาท์ (logout) ของอุปกรณ์ Fortigate Firewall ซึ่งเป็นเว็บเพจ ที่ไม่สามารถแก้ไขได้โดยเรียกเว็บด้วยไอพีของอุปกรณ์ตามด้วยคำว่า logout? จากนั้นต่อด้วยหมายเลขเซสชัน เช่น http://172.27.170.99:1000/logout?050d07010a0b035c เพื่อแจ้งให้ Fortigate Firewall ทำการตัดเซสชันนี้ และหากต้องการใช้งานอินเตอร์เน็ตจะต้องทำการล็อกอินใหม่ ดังรูปที่ 4.35



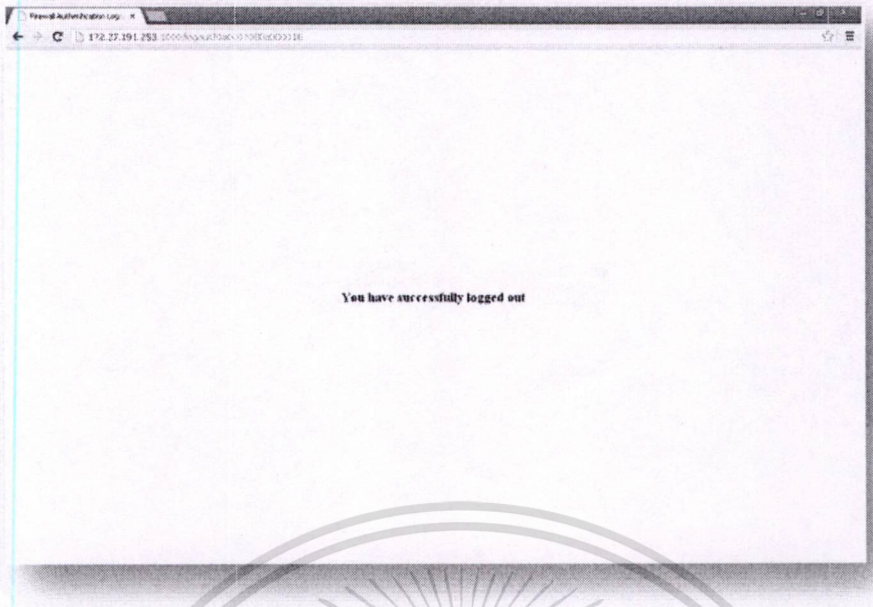
รูปที่ 4.35 แสดงหน้าต่างคงสถานการณ์เข้าใช้งานอินเตอร์เน็ตหลังจากล็อกอินผ่านแล้ว

หน้าต่าง Event Viewer ของ Windows Server 2003 R2 ในส่วนของ Security ของเครื่อง AUTHEN-1 จะพบกับหน้าจอนี้ซึ่งประกอบด้วยการแสดงผลลัพธ์ของการล็อกออนใช้งานบัญชีรายชื่อบน แอคทีฟไดเร็กทอรีด้วย Event ID: 540 ซึ่ง ID นี้จะแจ้งเหตุการณ์ของ Network Logon จากผลการทดสอบใช้ username = User1000 ในการล็อกอินหน้า Login Page นั้น ในส่วนของ User ในหน้าต่างนี้ก็แสดงรายชื่อ User1000 และมี Type เป็น Success Audit ซึ่งแสดงว่าสามารถทำการล็อกอินใช้งานได้ และ เครื่องที่ให้บริการก็แสดงในส่วนของ Workstation Name ซึ่งแสดงชื่อเครื่องให้บริการคือ AUTHEN-1 ดังรูปที่ 4.36



รูปที่ 4.36 แสดงการล็อกอินผ่านการใช้งานบัญชีรายชื่อบนเครื่อง AUTHEN-1

เมื่อทดสอบการกดปุ่ม “ออกจากระบบ” ผลลัพธ์ที่ได้จะพบกับหน้าต่างแสดงข้อความว่าได้ออกจากระบบเรียบร้อยแล้วด้วยข้อความ You have successfully logged out ดังรูปที่ 4.37

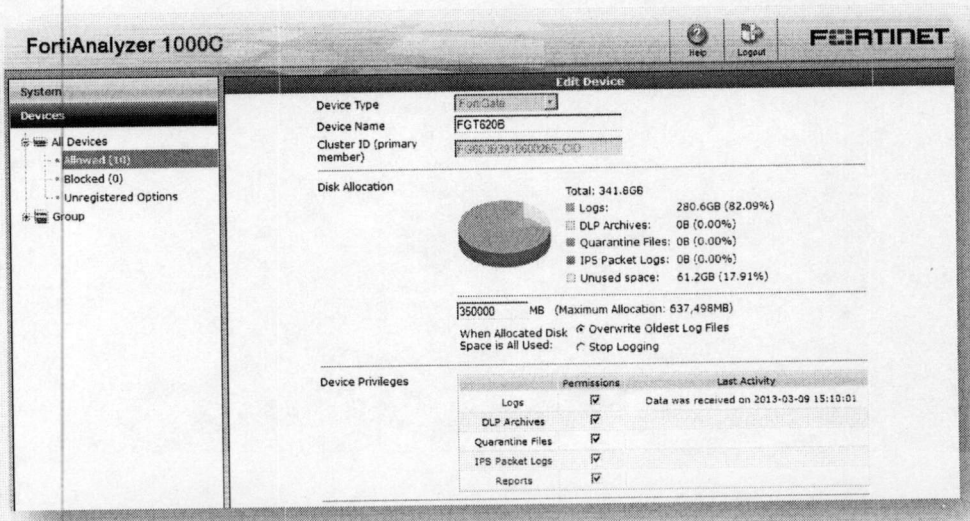


รูปที่ 4.37 เมื่อทดสอบการออกจากระบบ User1000 ก็สามารถที่จะทำการออกจากระบบได้ เช่นเดียวกับ User = wissawa.jen ที่ได้ทำการทดสอบบนเครื่อง AUTHEN-2

4.5 การทดสอบอ่าน Log File จาก FortiAnalyzer 1000C

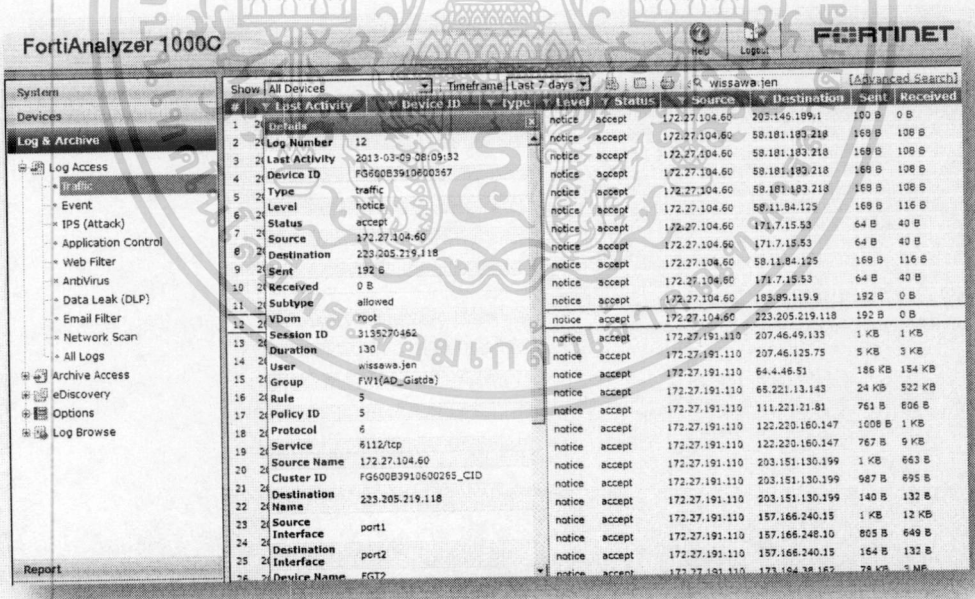
การเพิ่มอุปกรณ์ Fortigate Firewall เข้าสู่อุปกรณ์เก็บ Log FortiAnalyzer 1000C มีขั้นตอน ดังนี้ ดังรูปที่ 4.38

- Device Type = FortiGate ซึ่งเป็นรุ่น Device ของอุปกรณ์ Firewall
- Device Name = ชื่อของอุปกรณ์
- ในส่วน Disk Allocation สามารถกำหนดได้ถึง Maximum Allocation เมื่อ Log File ถึงค่าที่กำหนดก็จะทำการเขียนทับไฟล์เดิม
- Device Privileges ให้กำหนดเชคบ็อกซ์ที่ Logs



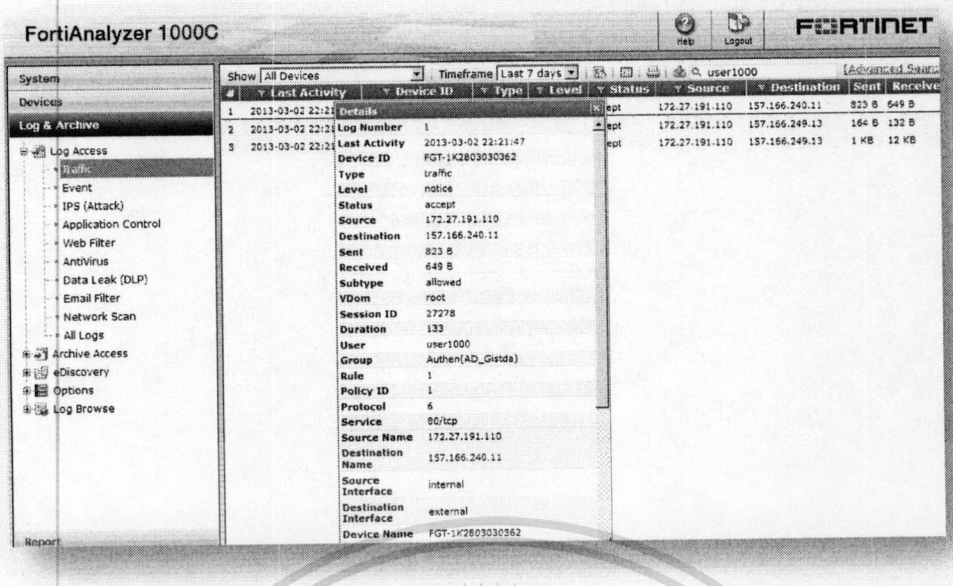
รูปที่ 4.38 การเพิ่มอุปกรณ์ Fortigate Firewall เข้าสู่อุปกรณ์เก็บ Log FortiAnalyzer 1000C

ผลการทดสอบการค้นหา Network Traffic จาก User wissawa.jen ผลลัพธ์ที่ได้จาก log แสดงให้ทราบระยะเวลาของการเชื่อมต่อ Source IP และ Destination IP และ Status ของการเชื่อมต่อ ดังรูปที่ 4.39



รูปที่ 4.39 ผลการทดสอบการค้นหา Network Traffic จาก User wissawa.jen ผลลัพธ์ที่ได้จาก log

ผลการทดสอบการค้นหา Network Traffic จาก User = User1000 ผลลัพธ์ที่ได้จาก log แสดงให้ทราบระยะเวลาของการเชื่อมต่อ Source IP และ Destination IP และ Status ของการเชื่อมต่อ ดังรูปที่ 4.40



รูปที่ 4.40 ผลการทดสอบการค้นหา Network Traffic จาก User = User1000

4.6 การทดสอบเปลี่ยนรหัสผ่านโดยผู้ใช้งานผ่านเว็บ

ทดสอบทำการเลือก Change Password บนหน้าต่างล็อกอิน จะพบกับหน้าต่างการเปลี่ยนรหัสผ่านสำหรับผู้ใช้งานอินเตอร์เน็ตปรากฏขึ้น ดังรูปที่ 4.41

ทดสอบเปลี่ยนรหัสผ่านของ Username = wissawa.jen ด้วย password จาก 12345 เป็น12345678 เมื่อกรอกข้อมูลในช่องครบแล้วเลือกตกลง ระบบจะทำการเปลี่ยนรหัสผ่านตามรหัสผ่านใหม่

รูปที่ 4.41 แสดงการทดสอบเปลี่ยนรหัสผ่าน ของผู้ใช้งานอินเตอร์เน็ต

เมื่อทำการเปลี่ยนรหัสผ่านสำเร็จ ระบบจะแจ้งให้ผู้ใช้งานทราบว่ารหัสผ่านได้รับการแก้ไขแล้วและผู้ใช้สามารถกลับไปหน้าล็อกอินจากหน้าเพจนี้ได้ โดยเลือกลิงค์ “กลับไปหน้าล็อกอิน” ดังรูปที่ 4.42

รูปที่ 4.42 แสดงกรณีเปลี่ยนรหัสผ่านสำเร็จ

ทดสอบใส่รหัสเดิมไม่ถูกต้องทำให้ไม่สามารถแก้ไขรหัสผ่านได้ ระบบจะแจ้งให้ทราบว่าไม่สามารถแก้ไขรหัสผ่าน และให้ตรวจสอบการป้อนข้อมูล สามารถกดปุ่ม “Back” เพื่อกลับไปหน้าการใส่ข้อมูลอีกครั้งได้ ดังรูปที่ 4.43

รูปที่ 4.43 กรณีเปลี่ยนรหัสผ่านไม่สำเร็จ

4.7 การเปรียบเทียบระบบเดิมที่ใช้เครื่องแม่ข่ายกับระบบใหม่

การเปรียบเทียบระบบเดิมที่ใช้เครื่องแม่ข่ายกับระบบใหม่ที่นำอุปกรณ์ฮาร์ดแวร์ไฟร์วอลล์ร่วมกับแอคทีฟไดเร็กทอรีทำระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเทอร์เน็ต ดังแสดงในตารางที่ 4.1

หัวข้อเปรียบเทียบ	เซิร์ฟเวอร์สำหรับพิสูจน์ตัวตนแบบเดิม	แอพไพล์แอนซ์ ไฟร์วอลล์ร่วมกับแอคทีฟไดเร็กทอรี
ทรูพุทของอุปกรณ์	1Gbps	16 Gbps
การติดตั้ง	วางขวางระบบ (ต่อจากอุปกรณ์ไฟร์วอลล์)	วางขวางระบบ
การเปลี่ยนรหัสผ่านของผู้ใช้	เปลี่ยนได้	เปลี่ยนได้
การตรวจสอบล็อกไฟล์	ต้องติดต่อบริษัทผู้ให้บริการ	ตรวจสอบล็อกไฟล์ได้ทันที
ข้อมูลล็อกที่ได้	Login Time, User Name, IP Address	Login Time, User Name, IP Address, Source Port, Destination Port, Source IP, Destination IP, Protocol
ความคงทนของระบบ	เกิดอาการค้างบ่อย ต้องทำการรีเซต	7*24
การทำสำเนาข้อมูล	ไม่มีการทำสำเนาข้อมูลผู้ใช้งาน	ทำสำเนาถึงกันทุกๆ 15 วินาทีหลังการเปลี่ยนแปลงแก้ไข
การแมพไอพี	ต้องแจ้งบริษัท	สามารถทำได้ทันที
การประกาศข่าวสาร	ต้องแจ้งบริษัท	อัพโหลดไฟล์ข้อมูลประกาศได้ทันที
ค่าบำรุงรักษารายปี	ค่าอุปกรณ์พิสูจน์ตัวตน 899,228 บาท ค่าไฟร์วอลล์ที่ต้อง MA ตามปกติ 400,000 บาท	400,000 บาท

ตารางที่ 4.1 เปรียบเทียบระบบเดิมที่ใช้เครื่องแม่ข่ายกับระบบใหม่ที่นำอุปกรณ์ฮาร์ดแวร์ไฟร์วอลล์ร่วมกับแอคทีฟไดเร็กทอรีทำระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเทอร์เน็ต

บทที่ 5
สรุปผลและข้อเสนอแนะ

จากการจัดทำระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ต กรณีศึกษาสำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน) สามารถสรุปผลการดำเนินงาน รวมถึงข้อเสนอแนะได้ ดังนี้

5.1 สรุปผลการทดลอง

5.1.1 การเพิ่มบัญชีรายชื่อผู้ใช้งาน สามารถที่จะทำการเพิ่มจากเครื่องเซิร์ฟเวอร์ใดก็ได้ เนื่องจากแอคทีฟไดเร็กทอรีมีการสำเนาข้อมูลบัญชีรายชื่อผู้ใช้งานไว้ทุกเครื่องเหมือนกันทั้งหมด หากเครื่องให้บริการบัญชีรายชื่อผู้ใช้งานเครื่องใด ไม่สามารถให้บริการได้ ผู้ดูแลระบบสามารถเลือกเปลี่ยนไปใช้เครื่องให้บริการอื่นเพื่อความต่อเนื่องของระบบ

5.1.2 การสำเนาข้อมูลบัญชีรายชื่อผู้ใช้งาน เนื่องจากระบบมีการเชื่อมโยงกันข้ามสำนักงานระบบเครือข่ายจึงจำเป็นที่จะต้องมีความเสถียรสูง จากการทดลองระบบของสำนักงานฯ ทั้ง 3 สาขา เชื่อมต่อกันด้วย Lease Line หากผู้ดูแลระบบ ต้องการทำสำเนาบัญชีรายชื่อผู้ใช้งานระหว่างสำนักงานฯ ก็สามารถที่จะทำการสำเนาข้อมูลบัญชีรายชื่อผู้ใช้งานได้ทันที หากเครื่องให้บริการบัญชีรายชื่อผู้ใช้งาน ณ สำนักงานฯใดเสียสามารถเลือกเปลี่ยนไปใช้เครื่องให้บริการ ณ สาขาอื่น ผ่าน Lease Line ได้

5.1.3 การพิสูจน์ทราบตัวตนก่อนการใช้งานอินเตอร์เน็ต สามารถทำได้ดีด้วยคุณสมบัติที่เพิ่มขึ้นบนเฟิร์มแวร์(Firmware) รุ่นใหม่ ๆ ของอุปกรณ์ไฟร์วอลล์ จึงทำให้การพิสูจน์ตัวตนทำได้รวดเร็วและลดคอขวดของการวางเครื่องแม่ข่ายสำหรับทำระบบพิสูจน์ตัวตนสำหรับผู้ใช้งานอินเตอร์เน็ต ข้างหน้าไฟร์วอลล์ลงไปได้

5.2 ปัญหาและอุปสรรค

5.2.1 หากเครื่องโดเมนคอนโทรลเลอร์ ณ สำนักงานใด ๆ เสียและไม่สามารถใช้งานได้ด้วยการซ่อมแซมระบบ หากจำเป็น ต้องติดตั้งระบบปฏิบัติการใหม่ จำเป็นที่จะต้องมีความรู้ความเข้าใจในการบริหารจัดการโดเมนคอนโทรลเลอร์ สำนักงานใดที่เครื่องโดเมนคอนโทรลเลอร์ ยังให้บริการได้จะต้องทำการโอนย้ายบทบาทยืดหยุ่นหนึ่งต้นแบบการดำเนินงาน (Flexible Single Master Operations: FSMO) ไปยังเครื่องนั้นแล้วการติดตั้งโดเมนคอนโทรลเลอร์ใหม่ เพื่อทำการ

จัดสร้าง Multi-Master Replication หากไม่โอนย้ายบทบาท FSMO ก่อนจะไม่สามารถทำสำเนาบัญชีรายชื่อผู้ใช้งานข้ามสำนักงานได้

5.2.2 ผู้ใช้งานที่ทำการล็อกอินผ่านแล้ว ผู้ใช้จะพบกับหน้าต่าง ซึ่งปรากฏอยู่บนแทบใหม่ของเว็บบราวเซอร์ ซึ่งผู้ใช้งานอินเทอร์เน็ตจะต้องเปิดหน้าต่างนี้ทิ้งไว้ เพื่อให้สามารถเข้าใช้งานอินเตอร์เน็ตได้อย่างต่อเนื่อง และด้วยการที่เว็บบราวเซอร์รุ่นใหม่ ๆที่ถูกปรับปรุงขึ้นมีการใช้งานแท็บ จึงทำให้หน้าต่างคงสถานะการเข้าใช้งานอินเตอร์เน็ตปรากฏอยู่บนแท็บ และผู้ใช้งานมักจะเผลอปิดแท็บคงสถานะการใช้งานลงทำให้ไม่สามารถใช้งานอินเตอร์เน็ตได้ เพราะอุปกรณ์ไฟร์วอลล์ตรวจสอบตามเวลาแล้วไม่พบหน้าต่างคงสถานะการใช้งานอินเตอร์เน็ตไฟร์วอลล์จะตัดผู้ใช้ออกจากระบบพิสูจน์ตัวตนและผู้ใช้จะต้องทำการล็อกอินใหม่

บรรณานุกรม

ชัยนันท์ กมลวดี. 2546 . **เจาะลึกเพิ่มพลังเครือข่ายเต็มพิกัดด้วย Directory Services**. กรุงเทพฯ: เอส.พี.ซี. บุ๊คส์.

บัณฑิต จามรภูติ. 2548 . **คู่มือ Windows Server 2003 ภาคปฏิบัติเล่ม 1**. พิมพ์ครั้งที่ 8. เชียงใหม่: Bandhit.

Fortinet Inc. 2013 . **Fortinet Technical Documentation**. Retrieved January 6, 2013, from http://docs.fortinet.com/fgt40mr3.html

Microsoft. 2012 . **Windows Server 2003**. Retrieved November 15, 2012, from http://technet.microsoft.com/en-us/windowsserver/bb512919.aspx

Paul Cociuba. 2009 . **Setting Up the IIS 6 Password Change Site - IISADMPWD**. Retrieved May 15, 2010, from http://blogs.msdn.com/b/friis/archive/2009/03/24/setting-up-the-iis-6-password-change-site-iisadmpwd.aspx

ประวัติผู้เขียน

ชื่อ – นามสกุล	นายวิศวะ เจนจบ
ประวัติการศึกษา	
ปริญญาตรี	มหาวิทยาลัยเทคโนโลยีราชมงคลล้านนา วิทยาเขตภาคพายัพ
ประกาศนียบัตรวิชาชีพชั้นสูง	วิทยาลัยเทคนิคเชียงใหม่
ประกาศนียบัตรวิชาชีพ	วิทยาลัยเทคนิคเชียงใหม่