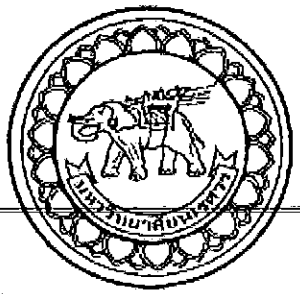


ศึกษาระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์กรณีศึกษา มหาวิทยาลัยนเรศวร

A STUDY OF THE COMPUTER NETWORK SECURITY SYSTEM AT NARESUAN UNIVERSITY

นายนราพงษ์ ทิพย์สุทะ รหัส 43370469

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาหลักสูตรปริญญาวิศวกรรมศาสตร์บัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร
ปีการศึกษา 2546

ใบรับรองโครงงานวิศวกรรม

หัวข้อโครงงาน	ศึกษาระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์กรณีศึกษามหาวิทยาลัยนเรศวร
ผู้ดำเนินโครงงาน	นายนราพงษ์ ทิพย์สุทะ รหัส 43370469
อาจารย์ที่ปรึกษา	อาจารย์ ดร.สุชาติ แย้มเม่น
สาขา	วิศวกรรมคอมพิวเตอร์
ภาควิชา	วิศวกรรมไฟฟ้าและคอมพิวเตอร์
ปีการศึกษา	2546

.....

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร อนุมัติให้โครงงานฉบับนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตรวิศวกรรมศาสตร์บัณฑิต สาขาวิศวกรรมคอมพิวเตอร์คณะกรรมการสอบโครงงานวิศวกรรม

.....ประธานกรรมการ
(อาจารย์ ดร. สุชาติ แย้มเม่น)

.....กรรมการ
(อาจารย์ ดร.พนมขวัญ ริยะมงคล)

.....กรรมการ
(อาจารย์พงศ์พันธ์ กิจสนาโยธิน)

หัวข้อโครงงาน	ศึกษาระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์กรณีศึกษามหาวิทยาลัยนเรศวร
ผู้ดำเนินโครงงาน	นายนราพงษ์ ทิพย์สุทะ รหัส 43370469
อาจารย์ที่ปรึกษา	อาจารย์ ดร.สุชาติ แย้มเม่น
สาขา	วิศวกรรมคอมพิวเตอร์
ภาควิชา	วิศวกรรมไฟฟ้าและคอมพิวเตอร์
ปีการศึกษา	2546

บทคัดย่อ

ในปัจจุบันเรื่องของความปลอดภัยของเครือข่ายเป็นเรื่องที่ผู้คนให้ความสนใจกันมากขึ้นเนื่อง จากการเจริญเติบโตของอินเทอร์เน็ตและความเสี่ยงต่อเรื่องของความปลอดภัยจึงสูงขึ้น ไฟร์วอลล์เป็นสิ่งหนึ่งซึ่งช่วยในการรักษาความปลอดภัย แต่ด้วยไฟร์วอลล์ที่มีอยู่ในปัจจุบันยังมีข้อจำกัดในการนำมาใช้ในเครือข่ายจึงได้มีแนวคิดในการศึกษาไฟร์วอลล์หลายๆชนิดซึ่งเป็นการศึกษาข้อดีและข้อด้อยของไฟร์วอลล์ที่มีความสามารถแตกต่างกัน

เพื่อศึกษาวิเคราะห์สถานภาพของระบบเครือข่ายคอมพิวเตอร์วิเคราะห์ปัญหาของระบบเครือข่ายมหาวิทยาลัยนเรศวร โดยใช้ข้อมูลจากการศึกษาวิเคราะห์ข้อมูลนโยบายการบริการและปัญหาการใช้งานจากผู้ดูแลระบบเครือข่ายและผู้ใช้งานทั่วไป เพื่อเป็นแนวทางในการพัฒนาและออกแบบระบบเครือข่ายคอมพิวเตอร์ต่อไป

Project Title	A study of the computer network security system at Naresuan University
Name	Mr. Narapong Tipsuta ID. 43370469
Project Advisor	Mr.Dr. Suchart Yammen
Major	Computer Engineering
Department	Electrical and Computer Engineering
Academic Year	2003

ABSTRACT

Nowadays, the risk of network security is more concerned because internet has started showing up in all fact of everyday life. The connection to internet becomes as common as a telephone for most of the population. Firewall is a method used for securing data and resources on a network by limiting network traffic between users and external threats or the Internet, current firewall architectures have some limitation of using.

The result of this project is an analysis of analyzing the problem of network infrastructure system by using the evaluated database from service policies and the emerging problems from the view of network system administrators, and general users. The ways for developing and designing the network system are also discussed.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้สำเร็จได้ด้วยดี เนื่องจากได้รับการแนะนำสนับสนุนและให้คำปรึกษาเป็นอย่างดีจากอาจารย์สุชาติ แย้มแม่น, อาจารย์ภานุพงศ์ สอนคม อาจารย์ที่ปรึกษา ปริญญานิพนธ์ซึ่งต้องขอขอบพระคุณเป็นอย่างสูง รวมทั้งอาจารย์ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร ทุกท่าน ที่ให้การอบรมสั่งสอนวิชาความรู้แก่คณะผู้จัดทำมาโดยตลอด

ขอขอบพระคุณอาจารย์ วัฒนา เชี่ยวสุวรรณ รักษาการในตำแหน่งผู้อำนวยการศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์ที่ได้กรุณาให้ใช้ห้องคอมพิวเตอร์ที่เป็นประโยชน์ต่อการศึกษาค้นคว้าโครงงานนี้และขอขอบคุณฝ่ายควบคุมระบบเครือข่ายคอมพิวเตอร์ที่ให้ความอนุเคราะห์ข้อมูล และขอขอบคุณเพื่อนๆนิสิตคณะมนุษยศาสตร์ เอกอังกฤษ ที่ให้ความร่วมมือเป็นอย่างดียิ่งในทุกด้าน

สุดท้ายนี้ ขอขอบพระคุณเป็นอย่างสูงสำหรับบุคคลที่สำคัญที่สุดที่ทำให้คณะผู้จัดทำมีวันนี้ คือ บิดา-มารดา ผู้เป็นที่เคารพรักยิ่งของคณะผู้จัดทำ ซึ่งท่านให้การอบรมสั่งสอน เลี้ยงดู และให้โอกาสในการศึกษาอย่างเต็มที่ จึงขอกราบขอบพระคุณมา ณ ที่นี้

นราพงษ์ ทิพย์สุทะ

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

บทที่ 1
บทนำ

ในบทนี้เป็นการแนะนำส่วนประกอบการทำงานอย่างคร่าวๆของโครงงานนี้ซึ่งประกอบไปด้วย ที่มาและความสำคัญของโครงงาน วัตถุประสงค์ในการทำโครงงานนี้ ขอบเขตของโครงงานที่สามารถทำได้ในส่วนนี้ ระยะเวลาที่ในการดำเนินงานของแต่ละขั้นตอน ผลที่คาดว่าจะได้รับจากโครงงาน และการใช้งบประมาณในการดำเนินงาน บทนี้มีเพื่อบอกความจำเป็นในการทำโครงงานดังที่จะกล่าวดังต่อไปนี้

1.1 ที่มาและความสำคัญของโครงงาน

อินเตอร์เน็ตเป็นเครือข่ายคอมพิวเตอร์ขนาดใหญ่ ที่เชื่อมโยงเอาเครือข่าคอมพิวเตอร์ย่อยๆ ทั่วโลกเข้าด้วยกันมีการแลกเปลี่ยนข่าวสารกันตลอด 24 ชั่วโมง การติดต่อสื่อสารกัคอมพิวเตอร์ในอีกซีกโลกหนึ่งจะง่ายพอๆกับการคุยกับคอมพิวเตอร์ที่อยู่ในห้องติดกัน เมื่อไรก็ตามที่คอมพิวเตอร์เชื่อมต่อเข้ากับอินเตอร์เน็ตก็เปรียบเสมือนกับการติดต่อสื่อสารทั่วโลก ซึ่งจะนำข้อมูลมจากคอมพิวเตอร์เครื่องอื่นมาสู่คอมพิวเตอร์ ปัจจุบันนี้หลายๆองค์กรได้เชื่อมต่อระบบเครือข่ายของตนเพื่อนำองค์กรของตนเข้าสู่อินเตอร์เน็ต เพื่อรองรับการติดต่อสื่อสารและการค้นคว้าหาข้อมูลต่างๆการเชื่อมต่อเข้าสู่ระบบอินเตอร์เนตทำให้เกิดช่องว่างด้านความปลอดภัย เปิดโอกาสให้ผู้ประสงค์ร้ายเข้ามาทำลาย หรือ โจรกรรมคอยฉวยโอกาสนี้ในการโจรกรรมหรือทำลายข้อมูลระหว่างการทำธุรกรรแม้กระทั่งการทำลายระบบเครือข่ายขององค์กร วิธีการป้องกันการบุกรุกจากผู้ไม่ประสงค์ดีดังกล่าว คือการติดตั้งระบบรักษาความปลอดภัยให้กับเครือข่ายคอมพิวเตอร์ซึ่งแนวทางป้องกันอย่างหนึ่งก็คือใช้ไฟร์วอลล์เป็นตัวหลักในป้องกันการบุกรุกระบบเครือข่ายทั้งจากภายนอกและภายในระบบเครือข่าย

ผู้เสนอโครงงานจึงมีแนวคิดที่จะจัดทำโครงงานศึกษาระบบป้องกันการบุกรุกระบบเครือข่ายภายในของมหาวิทยาลัยให้มีความปลอดภัยและมีเสถียรภาพมากขึ้น

1.2 วัตถุประสงค์ของโครงงาน

1. เพื่อศึกษาการทำงานของระบบรักษาความปลอดภัยโดยใช้ไฟร์วอลล์บนเครือข่ายคอมพิวเตอร์ รวมทั้งโครงสร้างของระบบรักษาความปลอดภัยบนเครือข่ายอินทราเน็ตชนิดต่างๆ และข้อดี ข้อเสียของระบบรักษาความปลอดภัย
2. เปรียบเทียบการทำงานของไฟร์วอลล์เพื่อให้สามารถเลือกไฟร์วอลล์ที่เหมาะสมกับระบบเครือข่ายคอมพิวเตอร์ได้
3. เพื่อศึกษาโครงสร้างระบบเครือข่ายคอมพิวเตอร์ และ ระบบรักษาความปลอดภัยของระบบเครือข่ายของมหาวิทยาลัยนเรศวร
4. เพื่อนำเสนอแนวความคิดและรูปแบบการป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยนเรศวร โดยใช้ไฟร์วอลล์

1.3 ขอบข่ายของโครงงาน

1. ศึกษาการทำงานของระบบเครือข่ายคอมพิวเตอร์ที่ใช้ โพรโตคอลทีซีพี /ไอพี (TCP/IP Protocol)
2. ศึกษาพฤติกรรมการบุกรุกทางเครือข่ายคอมพิวเตอร์และรูปแบบการโจมตีในแบบต่างๆ
3. ศึกษาคุณลักษณะของไฟร์วอลล์ ประเภทของไฟวอลล์ รูปแบบการทำงานต่างๆของไฟร์วอลล์ รวมถึงข้อดี ข้อเสียของแต่ละแบบเพื่อใช้เป็นข้อมูลในการเลือกใช้ไฟร์วอลล์ให้เหมาะสมกับระบบเครือข่าย
4. ศึกษาโครงสร้างระบบเครือข่ายคอมพิวเตอร์และระบบความรักษาปลอดภัยของระบบเครือข่ายของมหาวิทยาลัยนเรศวร
5. เพื่อนำเสนอแนวความคิดและรูปแบบการป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยนเรศวร โดยใช้ไฟร์วอลล์

1.4 ขั้นตอนการดำเนินงาน

กิจกรรม	ปี 2545		ปี 2546									
	พ.ย	ธ.ค	ม.ค	ก.พ	มี.ค.	เม.ย.	พ.ค	มิ.ย	ก.ค	ส.ค	ก.ย	ต.ค
1. เขียนโครงร่างการทำงานและการนำเสนอ	←	→										
2. ศึกษาและค้นคว้าข้อมูลของการสื่อสารระหว่างระบบเครือข่ายคอมพิวเตอร์ที่ใช้โพรโตคอล(TCP/IP)	←	→										
3. ศึกษาพฤติกรรมการบุกรุกทางเครือข่ายคอมพิวเตอร์และรูปแบบการโจมตีในแบบต่างๆของผู้ประสงค์ร้าย			←	→	→							
4. ศึกษารายละเอียดและการทำงานของไฟร์วอลล์(Firewall) ชนิดต่างๆ			←	→	→	→	→					
5. ศึกษาโครงสร้างระบบเครือข่ายของมหาวิทยาลัยนเรศวร						←	→	→	→			
6. จัดทำบทสรุปของโครงงาน									←	→	→	

1.5 ผลที่คาดว่าจะได้รับ

1. เข้าใจถึงปัญหาข้อบกพร่องของระบบเครือข่ายในปัจจุบัน
2. มีความรู้ความเข้าใจถึงการทำงานของไฟล์วอลล์และการใช้งานไฟร์วอลล์ชนิดต่างๆ
3. สามารถเลือกใช้ไฟร์วอลล์ได้อย่างเหมาะสมกับระบบเครือข่าย
4. เป็นกรณีศึกษาระบบรักษาความปลอดภัยบนระบบเครือข่ายให้กับระบบเครือข่ายของมหาวิทยาลัยนเรศวร

1.6 งบประมาณที่ใช้ นิสิต: คน: 1000 บาท

1. ค่าวัสดุและค่าอุปกรณ์		1000 บาท
	รวม	1000 บาท

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

2.1 นโยบายการใช้งานคอมพิวเตอร์ภายใต้ระบบเครือข่ายคอมพิวเตอร์

นโยบายการใช้งานระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศมหาวิทยาลัยนเรศวร ประกอบด้วย

1) ระบบความปลอดภัยของทรัพยากรข้อมูลกลาง

มหาวิทยาลัยนเรศวร กำหนดการจัดการ การเก็บรักษา และป้องกันความปลอดภัยของทรัพยากรข้อมูลกลาง หรือฐานข้อมูลร่วม จากการละเมิดสิทธิในการสืบค้นข้อมูล หรือใช้งานข้อมูลโดยไม่ได้รับอนุญาต การดำเนินการดังกล่าวเป็นหน้าที่ของ System Administrator ขึ้นตรงกับศูนย์ควบคุมเครือข่ายและฝึกอบรม กองแผนงาน สำนักงานอธิการบดี มหาวิทยาลัยนเรศวร ทั้งนี้ผู้ใช้งานที่ได้รับสิทธิในการสืบค้นข้อมูล สามารถป้องกันรักษาทรัพยากรข้อมูลที่มีคุณค่าได้ในเครื่องคอมพิวเตอร์ส่วนบุคคลหรืออาจแสดงคำร้องเพื่อการป้องกันพิเศษจากเจ้าหน้าที่ผู้รับผิดชอบได้

2) ทรัพยากรข้อมูลอื่น ๆ

ทรัพยากรข้อมูลที่สร้างสรรค์และจัดเก็บในระบบเครือข่ายคอมพิวเตอร์ย่อยๆ ได้แก่ Department และ Faculty Network ของแต่ละหน่วยงาน คณะ สำนัก สถาบัน กำหนดให้มีอิสระในการจัดการเก็บรักษา และป้องกันความปลอดภัยของทรัพยากรข้อมูลเฉพาะของเครือข่ายภายในหน่วยงานดังกล่าวเป็นหน้าที่ของเจ้าหน้าที่ผู้รับผิดชอบระบบคอมพิวเตอร์ของแต่ละหน่วยงาน คณะสำนัก สถาบันในสังกัดมหาวิทยาลัยนเรศวร

3) ทรัพยากรข้อมูลเฉพาะ

โดยทั่วไปแล้วทรัพยากรข้อมูลที่จัดเก็บไว้ในระบบเครือข่ายคอมพิวเตอร์ทั้งของแต่ละหน่วยงาน คณะ สำนัก สถาบัน และเครือข่ายกลาง NU Net นับเป็นทรัพยากรข้อมูลลับเฉพาะเพื่อการใช้สำหรับกิจกรรมภายในมหาวิทยาลัยนเรศวรอยู่แล้ว นอกเสียจากว่าบุคคล หน่วยงาน คณะ สำนัก สถาบันผู้เป็นเจ้าของข้อมูลมีความประสงค์จะเปิดเผย กระจายข้อมูลดังกล่าวให้เป็นสาธารณะ หากพ้นจากความประสงค์ดังกล่าวแล้ว มหาวิทยาลัยถือว่าทรัพยากรข้อมูลทุกอย่างเป็นความลับเฉพาะ ซึ่งจัดไว้บริการสำหรับบุคลากรที่ได้รับสิทธิในการสืบค้นและใช้งานข้อมูลตาม Account หรือ Username และ Password ที่ได้จัดเตรียมไว้ให้เท่านั้น นอกเหนือไปจากนี้ให้เป็นดุลยพินิจของ System Administrator กรณีทรัพยากรข้อมูลลับเฉพาะของ Nu Net หรือเจ้าหน้าที่

ผู้รับผิดชอบระบบคอมพิวเตอร์ของแต่ละหน่วยงานที่จะพิจารณาให้บุคคลได้สืบค้นและเรียกใช้ข้อมูลลับเฉพาะเป็นคร่าว ๆ ไปตามร้องขอ

4) การควบคุมดูแลตรวจสอบ

การควบคุมดูแลตรวจสอบการสืบค้นและใช้งานทรัพยากรข้อมูลกลาง NU Net ให้เป็นไปตามกระบวนการและกิจกรรมเชิงวิชาการสอดคล้องกับนโยบายการบริหารและบริการการศึกษาของมหาวิทยาลัยนเรศวร ดังนั้น System Administrator จะพิจารณาถอดถอน Account หรือ Username และ Password ออกจากสิทธิของผู้ใช้ใดๆ ต่อเมื่อ

พบว่าการใช้งานทรัยากรข้อมูลอย่างผิดกฎหมาย อาทิการทำซ้ำโปรแกรมคอมพิวเตอร์ที่เข้าข่ายละเมิดทรัพย์สินทางปัญญาหรือการใช้งานโปรแกรมคอมพิวเตอร์ที่ละเมินสิทธิบัตรอนุญาตใช้งานพบว่าการใช้งานทรัพยากรข้อมูลมีความเสี่ยง หรือเป็นภายต่อทรัพยากรข้อมูลของระบบหรือผู้ใช้อื่นๆ ที่เป็นสมาชิกในระบบ อาทิไวรัสคอมพิวเตอร์ หรือการแพร่กระจายข้อมูลในเชิงทำลายต่างๆ พบว่าการใช้งานทรัพยากรข้อมูลไม่เหมาะสมขัดต่อนโยบายใดๆ ของมหาวิทยาลัย

5) ความรับผิดชอบของผู้ใช้

การสืบค้นและเรียกใช้ทรัพยากรข้อมูลของ NU Net เป็นสิทธิเศษจัดเตรียมไว้เฉพาะบุคลากรสังกัดมหาวิทยาลัยนเรศวร ได้แก่ อาจารย์ เจ้าหน้าที่ และนิสิต ทั้งนี้สิทธิดงกล่าวอาจมอบหมายเป็นกรณีพิเศษให้กับบุคคลภายนอก โดยเป็นไปตามดุลยพินิจของผู้บริหาร สอดคล้องกับนโยบายของมหาวิทยาลัย อย่างไรก็ตามบุคลากรที่ได้รับสิทธิในการใช้งาน พึงกอปรไปด้วยความรับผิดชอบในการใช้งานทรัพยากรข้อมูล

6) วัตถุประสงค์ของสถาบัน

การจัดเตรียมระบบเครือข่าย NU Net เพื่อการแลกเปลี่ยนและใช้งานทรัพยากรข้อมูลร่วมกัน เพื่อ การบริหารและบริการการศึกษา สนับสนุนกิจกรรมเชิงวิชาการ การเรียนการสอน การค้นคว้าวิจัย รวมทั้งการบริการสังคมตามนโยบายมหาวิทยาลัย ทรัพยากรข้อมูลในระบบ NU Net มิได้จัดเตรียมไว้เพื่อการใช้งานในเชิงพาณิชย์ใดๆ ทั้งสิ้น

7) ความปลอดภัย

ผู้ใช้ต้องมีความรับผิดชอบต่อความปลอดภัยของข้อมูลและอุปกรณ์ระบบเครือข่าย NU Net

7.1) ผู้ใช้จะต้องได้รับ Account หรือ Username และ Password เป็นสิทธิของการสืบค้นและใช้งานทัพยากรข้อมูลเป็นเฉพาะตนและไม่ควรนำไปเผยแพร่เป็นสาธารณะ

7.2) ผู้ใช้พึงสงวนสิทธิการใช้งาน โดยการเปลี่ยน Password ด้วยตนเองอยู่เนื่อง ๆ

7.3) ผู้ใช้ควรทำความเข้าใจระดับป้องกันรักษาความปลอดภัยของข้อมูล

7.4) ผู้ใช้พึงระวังความเสียหายและการสูญเสียทรัพยากรข้อมูลจากไวรัสคอมพิวเตอร์ และโปรแกรมเชิงทำลายอื่นๆ รวมทั้งศึกษาขั้นตอนในการป้องกัน อาทิติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ ประจำเครื่องคอมพิวเตอร์ส่วนบุคคล เป็นต้น

8) การใช้งานโดยถูกต้องตามกฎหมาย

การใช้งานทรัพยากรข้อมูลระบบเครือข่าย NU Net ให้เป็นไปตามกฎหมายเท่านั้น ตัวอย่างของการใช้งานผิดกฎหมาย ได้แก่

8.1) การข่มขู่ผู้อื่นโดยจงใจ

8.2) การจงในทำลายอุปกรณ์ โปรแกรม หรือข้อมูลของผู้อื่น

8.3) การจงใจก่อกวนหรือตรวจสอบการใช้งานข้อมูลผู้อื่นโดยไม่รับอนุญาต

8.4) การทำซ้ำโปรแกรมหรือวัสดุที่มีการสงวนสิทธิการใช้ตามใบอนุญาตใช้งาน

9) การใช้งานอย่างมีจริยธรรม

ทรัพยากรข้อมูลของระบบเครือข่าย NU Net ควรมีการใช้งานอย่างสอดคล้องเหมาะสมกับ "ศักดิ์" และ "สิทธิ" ของบุคลากรสังกัดมหาวิทยาลัยนเรศวร ตัวอย่างของการใช้งานผิดจริยธรรม ได้แก่

9.1) การใช้งานที่ละเมิดต่อระบบความปลอดภัยของระบบ

9.2) การใช้งานโดยไม่ได้รับ Account หรือ Username และ Password ซึ่งเป็นการแสดงสิทธิการในการใช้งานไม่ถูกต้อง

9.3) การลักลอบใช้ Account หรือ Username และ Password ของบุคคลอื่น ๆ

9.4) การใช้งานข้อมูล Multimedia หรือการสื่อสารข้อมูลซึ่งต้องอาศัย Bandwidth หรือกินพื้นที่เส้นทางเดินข้อมูลสูง ๆ อย่างมาก (Overuse) หรือตลอดเวลาแต่ เพียงผู้เดียว ขาดการวิเคราะห์ในสิทธิการใช้งานของผู้อื่น

9.5) การใช้งานทรัพยากรข้อมูลเพียงวัตถุประสงค์เฉพาะตน หรือเชิงพาณิชย์ หรือเชิงใดๆ ที่ขัดต่อนโยบายหรือแนวทางของมหาวิทยาลัย

9.6) การใช้งานทรัพยากรข้อมูลโดยขาดความซื่อสัตย์

9.7) การละเมินทรัพย์สินทางปัญญา

9.8) การละเมินกฎหรือข้อปฏิบัติในการใช้งานระบบเครือข่าย

9.9) การละเมิดสิทธิของผู้ใช้อื่น ๆ

10) การใช้งานอย่างสร้างสรรค์

ทรัพยากรข้อมูลระบบเครือข่าย NU Net สามารถนำไปใช้ให้เกิดประโยชน์ได้หลายทางรวมทั้งผู้ใช้สามารถบำรุงรักษาอุปกรณ์และข้อมูลในระบบเครือข่าย NU Net ได้หลายวิธี ได้แก่

ตรวจสอบ Hard disk ในเครื่องคอมพิวเตอร์ส่วนบุคคล และหมั่นลบไฟล์ข้อมูล ที่ไม่ใช้งานแล้ว หรือ Temp File ออก เพื่อเพิ่มเนื้อที่การเก็บข้อมูลใน Hard disk

การสื่อสารข้อมูล Online เป็นเวลานานๆ (Overuse) หลีกเลี่ยงการใช้พื้นที่เก็บข้อมูลส่วนกลางเฉพาะตนเองมากๆ คำนึงเมื่อต้องการพิมพ์เอกสารหรือใส่ใจต่อกระบวนการอำนวยให้เกิดความสะดวกในการใช้ ทรัพยากรข้อมูลกลางแก่ผู้ใช้อื่น ๆ ด้วย

ใช้งานอรรถประโยชน์จากระบบเครือข่ายปฏิสัมพันธ์อย่างเหมาะสมพอควร

11) จดหมายลูกโซ่ (Chain Letter)

ทรัพยากรข้อมูลระบบเครือข่าย NU Net จัดเตรียมได้สำหรับหน่วยงาน คณะสำนัก สถาบัน อาจารย์ เจ้าหน้าที่ และนิสิต ในสังกัดมหาวิทยาลัยนเรศวร เพื่อวัตถุประสงค์ในการบริหารและบริการการศึกษา การสื่อสารผ่านจดหมายอิเลคทรอนิกส์ จัดเตรียมไว้เพื่ออำนวยความสะดวกในกิจกรรมเชิงวิชาการ รวมทั้งการเผยแพร่ข้อมูลที่ถูกต้องสมควร ทั้งนี้จดหมายลูกโซ่ และ/หรือ จดหมายที่ไม่มีข้อความอันเป็นสาระต่าง ๆ เป็นสิ่งที่ต้องห้ามของนโยบายการใช้งานระบบเครือข่ายของมหาวิทยาลัย หากมีการตรวจพบการเผยแพร่จดหมายลูกโซ่ หรือจดหมายที่ไม่มีข้อความอันเป็นสาระใน Account หรือ Username และ Password ของผู้มีสิทธิใช้งานคนใดคณะกรรมการลงทะเบียน Account หรือ Username และ Password ด้วยการประสานงานของ System Administrator ผู้รับผิดชอบระบบเครือข่าย NU Net และเจ้าหน้าที่ผู้รับผิดชอบระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน คณะ สำนักสถาบัน จะทำการเตือนเป็นลายลักษณ์อักษร หากยังพบพฤติกรรมการใช้งานทรัพยากรข้อมูลดังเดิมอีกคณะกรรมการจะทำงานยกเลิกสิทธิในการใช้งานต่อไป

12) การเล่นเกมส์คอมพิวเตอร์

มหาวิทยาลัยจัดเตรียมระบบเครือข่าย NU Net สำหรับหน่วยงาน คณะ สำนัก สถาบัน อาจารย์ เจ้าหน้าที่ และนิสิต ในสังกัดมหาวิทยาลัยนเรศวร เพื่อวัตถุประสงค์ในการสืบค้นและใช้งานทรัพยากรข้อมูลร่วมกันเพื่อการบริหารและบริการศึกษารวมทั้งกิจกรรมเชิงวิชาการอื่นๆ การเล่นเกมส์คอมพิวเตอร์ด้วยการใช้อุปกรณ์ระบบเครือข่ายและทรัพยากรอื่นๆ ของมหาวิทยาลัย เป็นสิ่งต้องห้าม หากผู้รับผิดชอบระบบเครือข่าย NU Net และเจ้าหน้าที่ผู้รับผิดชอบระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานคณะ สำนัก สถาบัน จะทำการตักเตือนเป็นลายลักษณ์อักษร

13) ข้อควรละเว้น

การละเมิดนโยบายดังกล่าว โดยเฉพาะการละเมิดนโยบายการใช้งานทรัพยากรข้อมูลระบบเครือข่าย NU Net อย่างถูกกฎหมายและมีจริยธรรม นับว่าเป็นการละเมิดรุนแรง ผู้ละเมิดจะถูกพิจารณาว่าปฏิบัติขัดแย้งต่อนโยบายมหาวิทยาลัย และอาจสูญเสียสิทธิในการสืบค้นและใช้งานทรัพยากรข้อมูลได้ ทั้งนี้การใช้งานทรัพยากรข้อมูลที่ผิดกฎหมาย อาจถูกดำเนินการโดยหน่วยงาน

ด้านกฎหมายของรัฐ นโยบายดังกล่าวสามารถเป็นผลในหน่วยงานของสภามหาวิทยาลัย สภาอาจารย์ สภาลูกจ้าง สภานิสิตสมาคมนิสิตเก่ามหาวิทยาลัยนเรศวร อีกด้วย

14) นโยบายลงทะเบียนเพื่อรับ Account หรือ Username และ Password

14.1) ความหมายของคำที่เกี่ยวข้องในการลงทะเบียน

14.1.1) ผู้มีสิทธิ : หน่วยงาน คณะ สำนัก สถาบัน อาจารย์ เจ้าหน้าที่ นิสิต ในสังกัดมหาวิทยาลัยนเรศวร

14.1.2) สิทธิที่ได้รับ : Account หรือ Username และ Password เพื่ออนุญาตในการสืบค้นและใช้งานทรัพยากรข้อมูลระบบเครือข่าย NU Net

14.1.3) การได้มาซึ่งสิทธิ : ผู้มีสิทธิแสดงความจำนงค์ต่อเจ้าหน้าที่ผู้รับผิดชอบของแต่ละ หน่วยงาน คณะ สำนัก สถาบัน สังกัดมหาวิทยาลัยนเรศวร เป็นผู้พิจารณาอนุมัติตามขั้นตอนของหน่วยงาน คณะ สำนัก และสถาบัน

14.2) คณะกรรมการอนุมัติ Account หรือ Username และ Password

มหาวิทยาลัยจะแต่งตั้งคณะอนุกรรมการควบคุม และตรวจสอบการใช้งานระบบเครือข่ายคอมพิวเตอร์ มีจำนวนไม่เกิน 7 คน เพื่อทำหน้าที่พิจารณาอนุมัติ Account หรือ Username และ Password ให้แก่ผู้มีสิทธิตามที่แสดงความจำนงค์ เพื่อสามารถสืบค้นและใช้งานทรัพยากรข้อมูลระบบเครือข่าย NU Net โดยมีขอบเขตในการพิจารณาอนุมัติ ดังนี้

14.2.1) ตรวจสอบความจำนงค์ในการสืบค้นและใช้งานทรัพยากรข้อมูลระบบเครือข่าย NU Net ของผู้มีสิทธิตามรายละเอียดที่ได้แสดงไว้ในใบคำร้องของ Account หรือ Username และ Password

14.2.2) อนุมัติการลงทะเบียน Account หรือ Username และ Password เมื่อพิจารณาเห็นว่าเหมาะสม

14.2.3) ไม่อนุมัติการลงทะเบียน Account หรือ Username และ Password เมื่อพิจารณาเห็นว่าไม่เหมาะสม

14.2.4) ให้คำแนะนำถึงบริการการสืบค้นและใช้งานทรัพยากรข้อมูลระบบเครือข่าย NU Net ที่จัดเตรียมไว้ในปัจจุบันหรือบริการที่จะเกิดมีขึ้นในอนาคต

14.2.5) แสดงนโยบายการใช้งานทรัพยากรข้อมูลระบบเครือข่าย NU Net ให้ผู้มีสิทธิที่ได้รับ Account หรือ Username และ Pass word ทราบเพื่อการปฏิบัติอย่างสอดคล้องและถูกต้อง

15) นโยบายการแลกเปลี่ยนหรือใช้ Account หรือ Username และ Password ร่วมกัน

การอนุญาตให้มีการใช้สิทธิในการสืบค้นและใช้งานทรัพยากรข้อมูลระบบเครือข่าย NU Net โดยการลงทะเบียน Account หรือ Username และ Password ร่วมกันกับผู้ที่ไม่ได้รับสิทธิหรือไม่ผ่านการลงทะเบียนและอนุมัติจากคณะกรรมการลงทะเบียน Account หรือ Username และ Password ทั้งสิ้น หากมีการตรวจพบการใช้งานที่ละเมิดนโยบายดังกล่าวคณะกรรมการจะเพิกถอนสิทธิในการสืบค้นและใช้งานทันที รวมทั้งความเสียหายใด ๆ ก็ตามที่เกิดจากการละเมิดนโยบายให้เป็นความรับผิดชอบของผู้ที่ได้รับสิทธิที่จะต้องชดใช้ต่อความเสียหายนั้น ๆ

16) นโยบายการยกเลิก Account หรือ Username และ Password

การยกเลิกดังกล่าวหมายถึงการยกเลิกสิทธิในการสืบค้นและใช้งานทรัพยากรข้อมูลระบบเครือข่าย NU Net ซึ่งจะดำเนินการต่อเมื่อ

16.1) พบว่า Account หรือ Username และ Password ที่ได้ลงทะเบียนอนุญาตให้ใช้งานได้ ไม่มีการใช้งานต่อเนื่องเป็นเวลา 60 วัน

16.2) พบว่าผู้ได้รับ Account หรือ Username และ Password หมดสภาพการเป็นบุคลากรสังกัดมหาวิทยาลัยนเรศวร อาทิ อาจารย์ หรือเจ้าหน้าที่ที่ลาออก นิสิตที่ลาออกระหว่างการศึกษานิสิตที่สำเร็จการศึกษา เป็นต้น การยกเลิก Account หรือ Username และ Password จะดำเนินการภายใน 30 วัน นับจากวันหมดสภาพ

17) นโยบายการรวบรวมเก็บรักษาข้อมูล

ด้วยเทคโนโลยีการสื่อสารข้อมูลระบบเครือข่าย NU Net อำนวยให้ผู้มีสิทธิใช้งานและได้รับ Account หรือ Username และ Password ทุกคนสามารถสืบค้นและเรียกใช้งานทรัพยากรข้อมูลได้โดยสะดวกบนโปรแกรมคอมพิวเตอร์ที่ติดตั้งอยู่ในปัจจุบัน เพื่อสนับสนุนกิจกรรมเชิงวิชาการที่เป็นหน้าที่การงานประจำวัน ผู้ใช้สามารถสืบค้น เรียกใช้งาน รวมทั้งเก็บรวบรวมข้อมูลที่เป็นประโยชน์การบริหารและบริการการศึกษาได้ในระบบเครือข่าย Nu Net ยกเว้นข้อมูลที่เป็นส่วนบุคคลหรือไม่เกี่ยวข้องกับกิจกรรมเชิงวิชาการ มหาวิทยาลัยไม่อนุญาตให้มีการรวบรวมจัดเก็บไว้ในพื้นที่เก็บข้อมูลของระบบเครือข่าย NU Net นอกเสียจากผู้ใช้จะรวบรวมจัดเก็บไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคลของตนเท่านั้น อย่างไรก็ตามข้อมูลที่รวบรวมและจัดเก็บจะต้องได้รับการดูแลจาก System Administrator เพื่อป้องกันความปลอดภัยของข้อมูลโดยรวม ข้อมูลของผู้ใช้งานอื่น ๆ และระบบเครือข่าย NU Net ออกจากข้อมูลหรือโปรแกรมที่อาจเป็นอันตรายได้

18) นโยบายการใช้จดหมายอิเลคทรอนิกส์เพื่อการสื่อสารข้อมูล

จดหมายอิเลคทรอนิกส์ (Electronic Mail : E-mail) นับเป็นวิธีการสื่อสารและแหล่งข้อมูลสำคัญสำหรับการบริหารและบริการศึกษา ที่จะสามารถอำนวยประโยชน์ในกิจกรรมเชิงวิชาการได้ดีเป็นอย่างยิ่ง และด้วยสภาพแวดล้อมของสังคมสารสนเทศในปัจจุบัน จดหมายอิเลคทรอนิกส์ถือเป็นองค์ประกอบสำคัญของการดำเนินงานและหน้าที่ในประจำวัน การรับ ข ส่งจดหมายอิเลคทรอนิกส์ เป็นการสื่อสารตรงจากบุคคลถึงบุคคล ภายในกลุ่มสื่อสารขนาดเล็ก เฉพาะ

กิจ ข้อมูลในจดหมายและกลุ่มในการสื่อสารมีการจำกัดตนเองด้วยวัตถุประสงค์ในการติดต่อ นโยบายการใช้จดหมายอิเลคทรอนิกส์ของมหาวิทยาลัย สนับสนุนการติดต่อสื่อสารที่อำนวยประโยชน์ เป็นช่องทางของการได้รับข่ายสารที่มีคุณค่าเป็นช่องทางการสื่อสารที่สะดวกและประหยัดมาทางหนึ่ง การใช้จดหมายอิเลคทรอนิกส์เพื่อการอื่น ๆ โดยเฉพาะการรับ-ส่งข้อมูลอันไม่เป็นสาระนับเป็นการกระทำที่ไม่สมควร แสดงถึงผู้ใช้งานขาดสำนึกรับผิดชอบต่อระบบเครือข่าย NU Net ซึ่งเป็นทรัพยากรที่จัดสรรขั้นมาเพื่อการใช้งานร่วมกันของบุคลากรสังกัดมหาวิทยาลัยนเรศวร

19) ข้อแนะนำในการใช้จดหมายอิเลคทรอนิกส์

19.1) จดหมายอิเลคทรอนิกส์ไม่ควารใช้สำหรับการติดต่อสื่อสารในระดับกลุ่มขนาดใหญ่ หรือ Mass Communication เพื่อการแจ้งข้อมูลต่อสาธารณะ อันไม่ได้ระบุผู้รับข้อมูลที่ถูกต้องมีจำนวนแน่นอน

19.2) จดหมายอิเลคทรอนิกส์ไม่ควรใช้สำหรับการติดต่อเพื่อวัตถุประสงค์ในเชิงพาณิชย์ หรือวัตถุประสงค์ใด ๆ ที่ไม่เป็นการสนับสนุนกิจกรรมเชิงวิชาการตามนโยบายของมหาวิทยาลัยรวมทั้งรายชื่อที่อยู่ที่สามารถติดตอกันบนเครือข่าย NU Net หรือ Mailing List ก็ไม่สมควรเปิดเผยต่อสาธารณะ ในกรณีที่ไม่ใช่การติดต่อสื่อสารที่สอดคล้องกับนโยบายของมหาวิทยาลัย

19.3) ศูนย์ควบคุมเครือข่ายและฝึกอบรมคอมพิวเตอร์ สำนักงานอธิการบดี มหาวิทยาลัยนเรศวร มีการดำเนินการให้บริการ Electronic Bulletin Board สำหรับการกระจายข้อมูลเพื่อติดต่อสื่อสารในระดับกลุ่มขนาดใหญ่ หรือ Mass Communication

19.4) การใช้จดหมายอิเลคทรอนิกส์ ควรมีการดำเนินการอย่างถูกต้องเหมาะสมสอดคล้องกับนโยบายเรื่องสิทธิ ความรับผิดชอบและการใช้งานทรัพยากรข้อมูลระบบเครือข่าย NU Net

20) นโยบายการใช้จดหมายอิเลคทรอนิกส์เพื่อการสำรวจวิจัย

ความหมายของการสำรวจวิจัย หมายถึงการศึกษาเฉพาะในเรื่องใดเรื่องหนึ่ง และมีผลลัพท์ของการศึกษาจะเป็นข้อมูลหรือสามารถนำไปประยุกต์ใช้เพื่อการบริการสังคมภายในหรือภายนอกมหาวิทยาลัยนเรศวร ต่อไปได้ หากผู้มีสิทธิสืบค้นและใช้งานทรัพยากรข้อมูลระบบเครือข่าย NU Net มีความประสงค์ต้องการใช้จดหมายอิเลคทรอนิกส์เพื่อการสำรวจวิจัย หัวข้อแนวทาง รวมทั้งเวลาที่ต้องการใช้อุปกรณ์และทรัพยากรของมหาวิทยาลัยไปในกิจดังกล่าว เพื่อป้องกันการเสี่ยงต่อความเสียหายของระบบเครือข่าย NU Net และ/หรือสถานะทางการเงิน การจ้างงาน ภาพลักษณ์และชื่อเสียงของมหาวิทยาลัย เมื่อคณะกรรมการพิจารณาอนุมัติแล้วจึงจะสามารถดำเนินการใช้จดหมายอิเลคทรอนิกส์เพื่อการสำรวจวิจัยต่อไปได้

ข้อกำหนดในจดหมายอิเลคทรอนิกส์ที่ทำการส่งออกไปที่กลุ่มเป้าหมายเพื่อการสำรวจวิจัยจะต้องระบุแสดงรายการดังต่อไปนี้ทุกครั้ง

ชื่อ – สกุล และสังกัดของผู้ดำเนินการสำรวจวิจัย

วัตถุประสงค์ของการสำรวจวิจัย

ระบุต่อกลุ่มเป้าหมายในการติดต่อว่าการให้ความร่วมมือในการตอบแบบสอบถามเป็นความสมัครใจ ไม่มีการบังคับใดๆ ทั้งสิ้น

ผู้ดำเนินการสำรวจวิจัยไม่สามารถอ้างอิงความสัมพันธ์ใด ๆ กับมหาวิทยาลัยนเรศวร

21) นโยบายการติดตั้งอุปกรณ์เพิ่มเติมบนเครือข่าย NU Net

มหาวิทยาลัยนเรศวร ดำเนินการติดตั้งระบบเครือข่าย NU Net ด้วยแผนการสนับสนุนการใช้งานเทคโนโลยีสารสนเทศ เพื่ออำนวยประโยชน์ด้านการบริหารและบริการศึกษา ตามนโยบายของมหาวิทยาลัย โดยคำนึงจำนวนของหน่วยงาน คณะ สำนัก สถาบัน อาจารย์ เจ้าหน้าที่ นิสิต ในสังกัดมหาวิทยาลัยนเรศวร ผู้มีสิทธิใช้งาน คำนึงถึงอัตราเติบโตของบุคลากร คำนึงถึงความต้องการการสืบค้นใช้งานทรัพยากรข้อมูล และคำนึงถึงประสิทธิภาพของระบบเครือข่าย NU Net เพื่อสามารถบริการข้อมูลอย่างเหมาะสมอยู่เสมอ

อย่างไรก็ตามหากงาน/คณะ/สำนัก/สถาบันอาจารย์/เจ้าหน้าที่/นิสิตในสังกัดมหาวิทยาลัยนเรศวร ผู้มีสิทธิสืบค้นใช้งานทรัพยากรข้อมูลระบบเครือข่าย NU Net มีความประสงค์ต้องการติดตั้งอุปกรณ์เพิ่มเติมบนเครือข่าย NU Net เพื่อการเพิ่มศักยภาพในการทำงานของตนหรือเพื่อให้บริการ ข้อมูลร่วมภายในระบบเครือข่ายย่อยของหน่วยงาน/สำนักแล้ว ข้อให้มีการดำเนินการดังต่อไปนี้

21.1) แสดงความจำนงต่อผู้บริหารศูนย์ควบคุมเครือข่าย NU Net พร้อมกรอกแบบฟอร์มเพื่อการติดตั้ง และแสดงรายการอุปกรณ์ที่จะติดตั้งเพิ่มเติมระบบเครือข่าย NU Net

21.2) หน่วยงาน คณะ สำนัก สถาบัน หรือบุคลากรผู้ยื่นคำร้องขอติดตั้งอุปกรณ์เพิ่มเติมบนระบบเครือข่าย NU Net ต้องมีความรับผิดชอบต่อความปลอดภัยของระบบเครือข่าย NU Net อย่างเต็มที่ อาทิระบบการทำงานของอุปกรณ์จะต้องสอดคล้องกับการทำงานของระบบเครือข่าย NU Net หรือการงานอุปกรณ์ที่ติดตั้งใหม่จะต้องไม่มีความเสี่ยงต่อการสูญเสียทรัพยากรข้อมูลเดิมของระบบเครือข่าย NU Net หรือการติดตั้งอุปกรณ์ใหม่จะไม่รบกวนการสืบค้นและใช้งานทรัพยากรข้อมูลของผู้ใช้อื่น ๆ บนเครือข่าย NU Net เป็นต้น

21.3) หน่วยงาน คณะ สำนัก สถาบัน หรือบุคลากรผู้ยื่นคำร้องขอติดตั้งอุปกรณ์เพิ่มเติมบนระบบเครือข่าย NU Net ดังกล่าว จะต้องรับผิดชอบในการติดตั้งดำเนินการบำรุงรักษาอุปกรณ์ ด้วยตนเอง

21.4) ศูนย์ควบคุมเครือข่ายมีอำนาจตรวจสอบการใช้งาน และเพิกถอนคำอนุญาตให้ติดตั้งอุปกรณ์เพิ่มเติมนั้นออกจากระบบเครือข่าย NU Net ได้หากพบพฤติกรรมการใช้งานไม่เหมาะสม ขัดแย้งต่อนโยบายของมหาวิทยาลัย

22) นโยบายการทำซ้ำโปรแกรมคอมพิวเตอร์

มหาวิทยาลัยนเรศวรกำหนดนโยบายการใช้งานโปรแกรมคอมพิวเตอร์ตามพระราชบัญญัติทรัพย์สินทางปัญญา และสนับสนุนการจัดซื้อโปรแกรมคอมพิวเตอร์พร้อมใบอนุญาตใช้งานอย่างถูกต้องตามกฎหมายทุกประการ สำหรับหน่วยงาน คณะ สำนัก ในสังกัดมหาวิทยาลัยนเรศวรหากเกิดกรณีหรือพฤติกรรมใด ๆ ที่แสดงความจงใจในการใช้งานที่เข้าข่ายละเมิดทรัพย์สินทางปัญญา อาทิ การซ้ำโปรแกรมคอมพิวเตอร์นอกเหนือไปจากใบอนุญาตใช้งานจากเจ้าของลิขสิทธิ์ เป็นต้นมหาวิทยาลัยจะไม่รับผิดชอบต่อกระทำดังกล่าว และให้เป็นความผิดชอบของหน่วยงาน คณะ สำนัก และ/หรือผู้ดำเนินการต่อไปเอง

23) นโยบายการบริการสถานที่และอุปกรณ์เพื่อสืบค้นข้อมูล

มหาวิทยาลัยนเรศวร ดำเนินการให้บริการ Account หรือ Username และ Password เพื่อให้สามารถสืบค้นและงานข้อมูลนอกเหนือไปจากระบบเครือข่าย NU Net ได้แก่ระบบอินเตอร์เน็ทรวมทั้งข้อมูลสาธารณะจากระบบเครือข่ายคอมพิวเตอร์อื่น ๆ ทั้งนี้กำหนดการใช้งานให้อยู่ในขอบเขตของการบริหารและบริการศึกษา พร้อมทั้งได้มีการจัดเตรียมสถานที่และอุปกรณ์ให้สามารถสืบคุ้นข้อมูลได้อีกด้วย โดยมีข้อปฏิบัติดังนี้

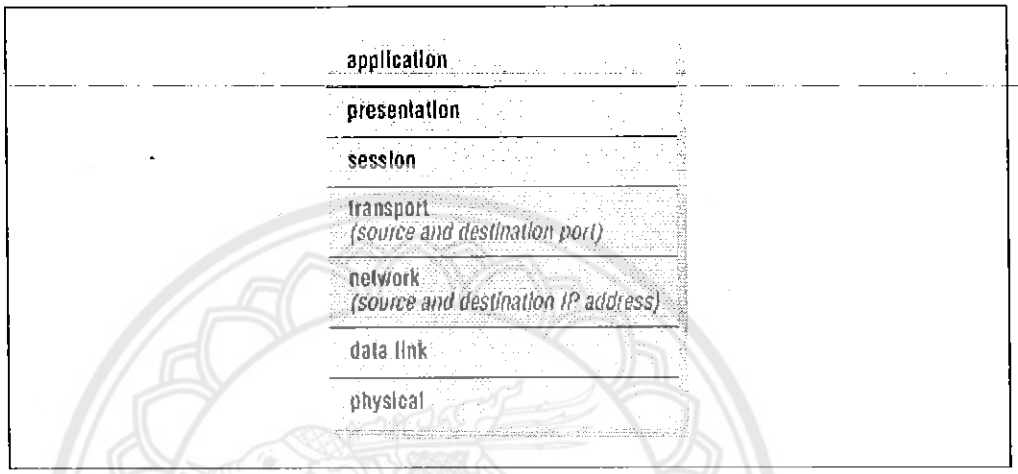
หน่วยงาน คณะ สำนัก หรือสถาบัน จัดเตรียมสถานที่และอุปกรณ์จำเป็นในการสืบค้นข้อมูล อาทิ เครื่องคอมพิวเตอร์ลูกข่าย เครื่องพิมพ์ เป็นต้น ให้เป็นบริการสาธารณะสำหรับบุคลากร อาจารย์ เจ้าหน้าที่ และนิสิต ในสังกัด สะดวกต่อการสืบคุ้นข้อมูลเพื่อประยุกต์ใช้ในกิจกรรมวิชาการได้

สถานที่และอุปกรณ์ที่จัดไว้ให้สืบคุ้นข้อมูลนี้สำหรับการสืบค้นเชิงวิชาการเท่านั้น หากพบการใช้ข้อมูลที่ไม่เป็นไปตามนโยบายของมหาวิทยาลัย เจ้าหน้าที่ผู้ดูแลระบบคอมพิวเตอร์สามารถตักเตือนผู้ใช้ได้ รวมทั้งการใช้งานอันละเลยต่อจริยธรรมที่ผู้ใช้ควรมี อาทิ การครอบครองสถานที่และอุปกรณ์เป็นเวลานาน ในขณะที่มีผู้ใช้คนอื่นรอใช้งานอยู่ หรือการเรียกใช้ข้อมูลที่ต้องการอาศัยทรัพยากรเครือข่ายสูงในเวลาที่มีการใช้งานร่วมกันของผู้ใช้คนอื่นจำนวนมากบนเครือข่าย

2.2 แบบจำลองสำหรับอ้างอิงแบบโอเอสไอ

การเชื่อมต่อคอมพิวเตอร์หลายๆเครื่องเข้าด้วยกัน จนเกิดเป็นระบบเครือข่ายคอมพิวเตอร์ซึ่งสามารถรับส่งข้อมูลระหว่างคอมพิวเตอร์เครื่องหนึ่งไปสู่คอมพิวเตอร์อีกเครื่องหนึ่งที่ต่างระบบต่างยี่ห้อกันได้จำเป็นจะต้องมีมาตรฐานในการสื่อสารหน่วยงานกำหนมาตรฐานสากล คือ

International Standards Organization หรือ ISO จึงกำหนดโครงสร้างทั้งหมดที่จำเป็นต้องใช้ในการรับส่งข้อมูลขึ้น ซึ่งเป็นสถาปัตยกรรมแบบระบบเปิด (Open System) เรียกว่า Open Systems Interconnection หรือเรียกสั้นๆว่า โอเอสไอ โมเด็ล (OSI Model)โอเอสไอ โมเด็ล กำหนดมาตรฐานการสื่อสารข้อมูลจากระบบคอมพิวเตอร์หนึ่งไปยังอีกระบบหนึ่ง โดยแบ่งออกเป็น 7 ชั้นซึ่งคอมพิวเตอร์จะมีชั้นการสื่อสาร 7 ชั้นเหมือนกัน



รูปที่ 2-1 การรับส่งข้อมูลของแบบจำลองอ้างอิงโอเอสไอทั้ง 7 ชั้น

(ที่มา : http://www.defcon1.org/e-books/ch15_03.htm)

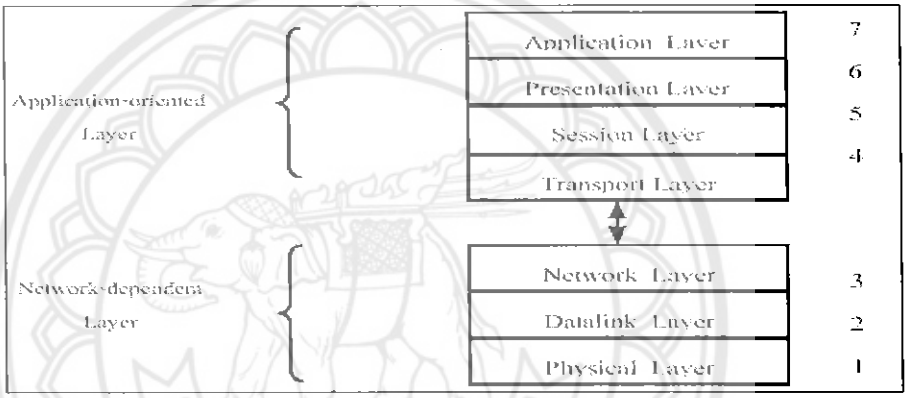
ในแต่ละเลเยอร์จะเสมือนเชื่อมต่ออยู่กับชั้นที่เทียบเท่ากันของคอมพิวเตอร์อีกด้านหนึ่ง เช่นชั้นทรานสปอร์ต จะติดต่อสื่อสารกับชั้นทรานสปอร์ต และ ชั้นแอปพลิเคชั่นจะติดต่อกับชั้นแอปพลิเคชั่นของคอมพิวเตอร์อีกฝั่งหนึ่งเท่านั้น แต่จริงๆแล้วมีสายส่งข้อมูลที่เชื่อมต่ออยู่ที่ชั้นที่ 1 หรือชั้นล่างสุดเพียงชั้นเดียว

ในการติดต่อรับส่งข้อมูล ผู้ใช้จะทำการรับส่งข้อมูลผ่านทางชั้นที่ 7 คือ ชั้นแอปพลิเคชั่น ซึ่งอยู่ด้านบนสุดของ โอเอสไอ โมเด็ลเท่านั้น แล้วส่งข้อมูลให้ต่อกับชั้นที่ 6 เรื่อยไปจนถึงชั้นล่างสุดแล้วจึงส่งต่อให้กับชั้นล่างสุดของคอมพิวเตอร์ผู้รับไล่ขึ้นไปจนถึงชั้นที่ 7 ตามลำดับ เนื่องจากการติดต่อรับส่งข้อมูลจะกระโดดข้ามไปส่งให้ชั้นอื่นที่ไม่อยู่ติดกันไม่ได้ แต่ละชั้นที่ทำหน้าที่รับส่งข้อมูลจะติดต่อรับส่งข้อมูลกับชั้นที่ติดอยู่กับตัวเองเท่านั้น ชั้นแอปพลิเคชั่นจะส่งให้ชั้นเซสชั่น โดยไม่ผ่านชั้นพรีเซนเทชั่นไม่ได้ประโยชน์ในการแบ่งเป็นชั้น คือ การกำหนดการติดต่อระหว่างชั้นทำได้โดยไม่ต้องคำนึงถึงการเปลี่ยนแปลงในชั้นอื่นๆ

ในทางทฤษฎี แต่ละชั้นของการรับส่งข้อมูลจะมีฟังก์ชันการทำงานที่แน่นอน และแยกออกจากกัน สามารถที่จะนำแต่ละชั้นของแต่ละบริษัทมาเชื่อมต่อกันได้อย่างไม่มีขีดจำกัด แต่ในทางปฏิบัตินั้นโอเอสไอโมเด็ล จะแบ่งออกเป็น 2 กลุ่มใหญ่ๆ คือ กลุ่มแรกได้แก่ 4 ชั้นด้านบน คือ ชั้น 7,

6, 5 และ 4 ทำหน้าที่เชื่อมต่อกับส่งข้อมูลระหว่างผู้ใช้กับแอปพลิเคชั่น ให้รับส่งข้อมูลกับฮาร์ดแวร์ที่อยู่ชั้นล่างได้อย่างถูกต้อง เรียกว่าชั้นแอปพลิเคชั่นโอเรียนเต็ด โดย 4 ชั้นบนนี้มักจะเป็น ซอฟต์แวร์ของบริษัทใดบริษัทหนึ่งรวมอยู่เป็นโปรแกรมเดียวจะแยกออกจากกันเป็นชั้นๆเพื่อใช้โปรแกรมของบริษัทอื่นได้ลำบาก หรือในบางกรณีก็อาจทำไม่ได้

กลุ่มที่สองจะเป็นชั้นล่างได้แก่ชั้น 3, 2 และ1 ทำหน้าที่เกี่ยวกับการรับส่งข้อมูลผ่านสายส่งและควบคุมการรับส่งข้อมูล ตรวจสอบข้อผิดพลาด รวมทั้งเลือกเส้นทางที่ใช้ในการรับส่งข้อมูล ซึ่งจะเกี่ยวกับฮาร์ดแวร์เป็นหลัก เรียกว่า ชั้นเน็ตเวิร์กดีเพนเดนท์ ซึ่งในส่วนนี้เกี่ยวข้องกับฮาร์ดแวร์และโปรแกรมควบคุมฮาร์ดแวร์เป็นหลัก ทำให้สามารถแยกแต่ละชั้นออกจากกันได้ง่าย และใช้ผลิตภัณฑ์ของต่างบริษัทกันในแต่ละชั้นได้อย่างไม่มีปัญหา



รูปที่ 2-2 แสดงการแบ่งเลเยอร์ระดับบน-เลเยอร์ระดับล่าง
(ที่มา: เปิดโลก TCP/IP และโปรโตคอลของอินเตอร์เน็ต สุวัฒน์ ปุณณชัยยะ)

2.3 หน้าที่การทำงานของแต่ละชั้น

ชั้นที่ 1: ชั้นฟิสิคัล (Physical Layer)

ทำการรับส่งข้อมูลในรูปแบบ"บิต" (bit) โดยไม่พิจารณาเรื่องความหมายข้อมูล การรับส่งจะส่งข้อมูล "0" หรือ "1" ผ่านสายส่งข้อมูลจริงโดยสามารถกำหนดคุณสมบัติทางกายภายของฮาร์ดแวร์ที่ใช้เชื่อมต่อระหว่างคอมพิวเตอร์ทั้ง 2 ระบบได้ว่าจะใช้สายส่งข้อมูลแบบไหนข้อต่อหรือปลั๊กที่ใช้ในการรับส่งข้อมูล ใช้ความต่างศักย์ไฟฟ้าเท่าใด ความเร็วในการส่งข้อมูลเป็นเท่าใดสัญญาณที่ใช้รับส่งข้อมูลในสายมีรูปร่างอย่างไร หากการรับส่งข้อมูลมีปัญหาเนื่องจากฮาร์ดแวร์ เช่นสายสัญญาณที่ใช้รับส่งข้อมูลขาด,อุปกรณ์เสียหาย ก็จะเป็นหน้าที่ของชั้นที่ 1 ที่จะตรวจสอบและแจ้งข้อผิดพลาดนั้นให้ชั้นอื่นๆที่อยู่เหนือขึ้นไปทราบ

ชั้นที่ 2: ชั้นดาต้าลิงก์ (Data link Layer)

ทำหน้าที่จัดการและรับส่งข้อมูลในระดับฮาร์ดแวร์โดยแปลคำสั่งที่ได้รับจากชั้นที่ 3ให้เป็นคำสั่งควบคุมฮาร์ดแวร์ ตรวจสอบและแก้ไขข้อผิดพลาดในการรับส่งข้อมูล

ชั้นที่ 3: ชั้นเน็ตเวิร์ก (Network Layer)

ทำหน้าที่เลือกหรือกำหนดเส้นทางที่จะใช้ในการรับส่งข้อมูลระหว่างเครือข่าย และส่งผ่านข้อมูลที่ได้รับไปสู่ปลายทาง ในชั้นนี้จะมองเห็นข้อมูลทั้งหมดเป็นแพ็คเก็ตหรือเฟรม ซึ่งเป็นการผนึกคำสั่งและไดอะล็อกต่างๆ ไว้ภายใน มีเพียงแอดเดรสของผู้รับ, ผู้ส่ง,ลำดับการรับส่งและส่วนของข้อมูลเท่านั้นที่ในชั้นนี้จะมองเห็น ดังนั้นตัวเนื้อหาของข้อมูลจะไม่มีผลใดๆในการรับส่งข้อมูลเลย ไม่ว่าข้อมูลในระดับสูงจะเป็นวีดีโอ,ภาพ,เสียงหรือข้อมูลอื่นใดก็ตาม นอกจากนี้ยังทำการ Call Setup หรือเรียกติดต่อคอมพิวเตอร์ปลายทางก่อนการรับส่งข้อมูล และทำการ Call Clearing หรือยกเลิกการติดต่อเมื่อการรับส่งข้อมูลจบลงแล้ว ในกรณีที่การรับส่งข้อมูลนั้นต้องมีการติดต่อกันก่อน(Hand shaking)

ชั้นที่ 4: ชั้นทรานสปอร์ต (Transport Layer)

เป็นรอยต่อระหว่างการรับส่งข้อมูลของซอฟต์แวร์กับฮาร์ดแวร์นำข้อมูลในระดับสูงมาแปลงให้รับส่งได้ในระดับฮาร์ดแวร์ เช่น แปลงค่าหรือชื่อของคอมพิวเตอร์ในเครือข่าย (Mac address) ให้เป็นหมายเลขเครือข่าย พร้อมทั้งเป็นชั้นที่ควบคุมการรับส่งข้อมูลจากปลายด้านส่งถึงปลายด้านรับตลอดเส้นทางตามจังหวะที่กำหนดไว้ในชั้นที่ 5 เช่นไม่ส่งข้อมูลเร็วเกินไปจนฝั่งผู้รับไม่สามารถรับข้อมูลได้ทัน เป็นการควบคุมคุณภาพของการรับส่งข้อมูลให้มีมาตรฐานในระดับที่ตกลงกันของทั้งสองฝ่าย ทำหน้าที่ตัดข้อมูลออกเป็นส่วนย่อยๆ ให้เหมาะกับลักษณะการทำงานของฮาร์ดแวร์ที่ใช้ในเครือข่ายเช่นหากข้อมูลที่ได้รับจากชั้นที่ 5 มีความยาวเกินกว่าที่เครือข่ายจะส่งได้ ชั้นที่ 4 จะตัดข้อมูลออกเป็นส่วนย่อยๆ แล้วส่งไปให้ผู้รับ ข้อมูลที่ได้รับปลายทางก็จะถูกนำมาต่อกันที่ชั้นที่ 4 ของด้านผู้รับ แล้วจึงส่งต่อให้ชั้นที่ 5 นำไปใช้ต่อไป

ชั้นที่ 5: ชั้นเซสชั่น (Session Layer)

ทำหน้าที่ควบคุม "จังหวะ" ในการรับส่งข้อมูลของคอมพิวเตอร์ทั้งสองด้าน ที่รับส่งแลกเปลี่ยนข้อมูลกันให้มีความสอดคล้อง (Synchronization) และกำหนดวิธีที่ใช้รับส่งข้อมูล เช่น อาจจะเป็นในลักษณะสลับกันส่งฝ่ายหนึ่งรับ อีกฝ่ายหนึ่งส่ง (Half Duplex) หรือรับส่งข้อมูลพร้อมกันทั้งสองฝ่าย (Full Duplex) โดยจะมองข้อมูลเสมือนเป็นประโยคที่สนทนาโต้ตอบกัน เช่น เมื่อผู้รับได้รับข้อมูลส่วนแรกจากผู้ส่ง ก็จะโต้ตอบกลับไปให้ผู้ส่งรู้ว่าได้รับข้อมูลส่วนแรกเรียบร้อยแล้วและพร้อมที่จะรับข้อมูลส่วนที่สองต่อไป

ชั้นที่ 6: ชั้นพรีเซนเทชั่น (Presentation Layer)

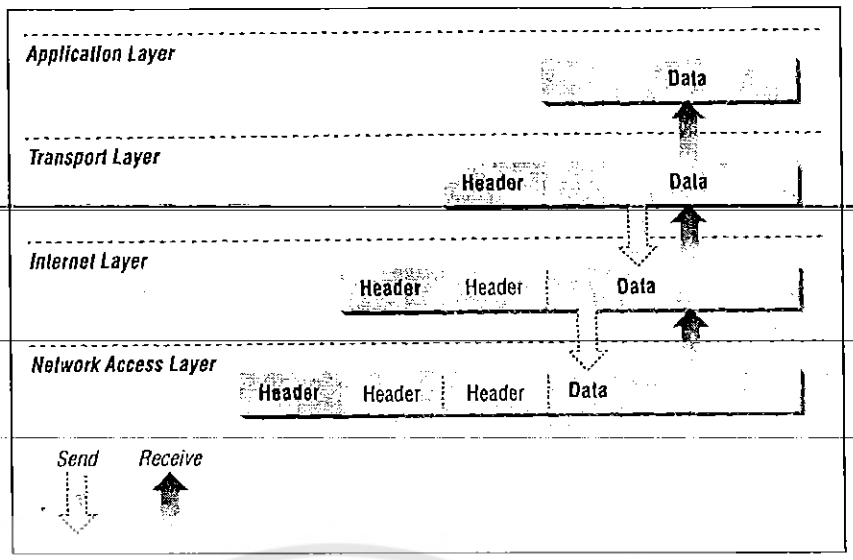
เป็นชั้นที่ทำหน้าที่ตกลงกับคอมพิวเตอร์อีกฝั่งหนึ่งว่ามีขั้นตอนและข้อบังคับอย่างไรในการรับส่งข้อมูล เนื่องจากรูปแบบของข้อมูลจะเป็นคำสั่งที่มีกฎ (Syntax) บังคับอย่างแน่นอน เช่น ในการคัดลอกไฟล์ จะต้องสร้างไฟล์ใหม่ขึ้นมาจากนั้นจึงเปิดไฟล์ แล้วจึงรับข้อมูลจากปลายทางมาเก็บลงในไฟล์ที่สร้างใหม่นี้ นอกจากนี้ยังทำหน้าที่แปลความหมายของคำสั่งที่ได้รับจากชั้นที่ 7 ให้เป็นคำสั่งระดับปฏิบัติการส่งให้ชั้นที่ 5 ต่อไปอีกด้วย

ชั้นที่ 7: ชั้นแอปพลิเคชั่น (Application Layer)

เป็นชั้นสูงสุด ที่รับคำสั่งต่างๆ จากผู้ใช้ นำมาแปลความหมายและทำงานตามคำสั่งที่ได้รับในระดับโปรแกรมประยุกต์ เช่น แปลความหมายของการกดปุ่มเมาส์ให้เป็นคำสั่งในการคัดลอกไฟล์ หรือดึงข้อมูลมาแสดงผลบนจอภาพ ซึ่งการแปลคำสั่งจะต้องแปลออกมาให้ถูกกฎ (Syntax) ที่ใช้ในระบบคอมพิวเตอร์นั้นๆ ตัวอย่างเช่น ถ้ามีการคัดลอกไฟล์ ชื่อไฟล์จะต้องยาวไม่เกินจำนวนที่ระบบปฏิบัติการใช้อยู่ และต้องประกอบด้วยตัวอักษรตามที่กำหนด รวมไปถึงฟังก์ชันที่ใช้ในการรับส่งข้อมูลระหว่างชั้นที่ 7 กับชั้นที่ 6 ด้วย

โดยการรับส่งข้อมูลใน โอเอสไอ โมเดลนี้ข้อมูลจากบนสุดคือชั้นที่ 7 จะถูกส่งลงไปในชั้นถัดไปจนกระทั่งถึงชั้นที่ 1 โดยข้อมูลเดิมจะผนึกรวมกับข้อมูลที่ใช้ควบคุมของแต่ละชั้นซ้อนๆกันไปเป็นลำดับ เช่น ข้อมูลจากชั้นแอปพลิเคชั่น คือ แอปพลิเคชั่นดาต้า เมื่อถูกส่งลงไปยังชั้นถัดไป ก็จะถูกผนึกด้วยแอปพลิเคชั่นเฮดเดอร์ และทั้ง แอปพลิเคชั่นเฮดเดอร์ และแอปพลิเคชั่นดาต้าจะถูกรวมกันเป็นข้อมูลของ ชั้นพรีเซนเทชั่น ซึ่งก็จะถูกผนึกด้วยชั้นพรีเซนเตชั่นอีกครั้ง

ก่อนที่จะส่งต่อไปที่ข้อมูลให้กับชั้นถัดไป แต่ละชั้นจะผนึกเฮดเดอร์ของตัวเองก่อนส่งต่อชั้นถัดไป จนกระทั่งถึงชั้นล่างสุด ชั้นฟิสิคัล ซึ่งจะทำการส่งข้อมูลให้ถึงปลายทาง และข้อมูลที่ปลายทางได้รับ จะถูกนำมาแยกเฮดเดอร์ที่เพิ่มเข้ามานี้ออกทีละชั้นจนกระทั่งถึงชั้นบนสุด ก็จะได้แอปพลิเคชั่นดาต้าที่ผู้ส่งส่งให้แก่ผู้รับ

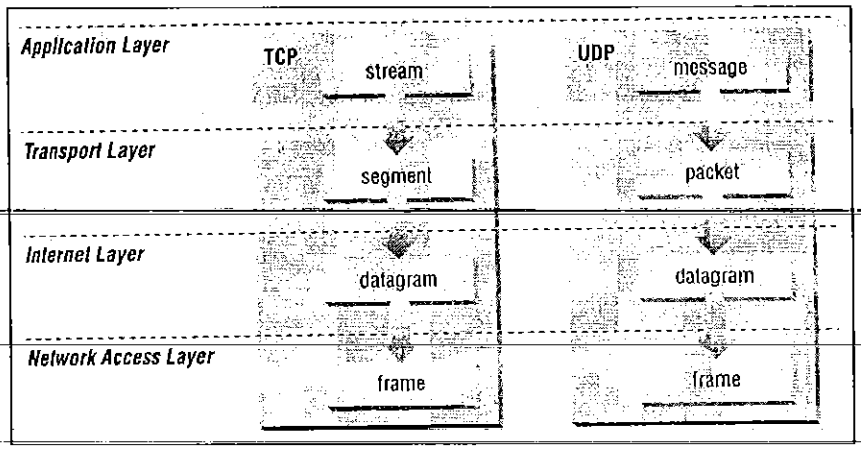


รูปที่ 2-3 การรับส่งข้อมูลของทีซีพี/ไอพี ในโอเอสไอโมเด็ล
(ที่มา: โครงสร้างและหลักการทำงานเบื้องต้น อานันท์ สีห์พิทักษ์เกียรติ)

2.4 ทีซีพี/ไอพี

TCP/IP (Transmission Control Protocol / Internet Protocol) เป็นมาตรฐานที่เกิดขึ้นก่อนโอเอสไอโมเด็ล ทีซีพี/ไอพีได้ถือกำเนิดขึ้นบนเครือข่ายอาร์พาเน็ต (ARPANET) ซึ่งต่อมาได้ขยายการเชื่อมต่อทั่วโลกเป็นเครือข่ายอินเทอร์เน็ต ทำให้มาตรฐานของทีซีพี/ไอพี เป็นที่ยอมรับกว้างขวางและเนื่องจากเป็นโพรโตคอลที่ใช้ได้ฟรีโดยไม่ต้องเสียค่าลิขสิทธิ์ จึงทำให้มีจำนวนผู้ใช้งานเพิ่มขึ้นจำนวนมากจนถือเป็นมาตรฐานที่มีผู้ใช้รับส่งข้อมูลมากที่สุดในปัจจุบัน

มาตรฐาน ทีซีพี/ไอพี นี้ไม่ได้เป็นไปตามรูปแบบของโอเอสไอโมเด็ลเนื่องจากโอเอสไอโมเด็ลถูกออกแบบโดยองค์กรขนาดใหญ่ซึ่งใช้เวลานานในการออกแบบตลอดจนการรับรองมาตรฐานต่างกับทีซีพี/ไอพี ซึ่งถูกออกแบบด้วยความต้องการอันเร่งด่วนของรัฐบาลสหรัฐฯ จึงทำให้การพัฒนาทีซีพี/ไอพีมีเงื่อนไขในด้านความต้องการที่ต่างจากโอเอสไอโมเด็ลทีซีพี/ไอพีมีการแบ่งจำนวนชั้นที่ใช้รับส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ออกเป็นเพียง 4 ชั้น เรียกว่า ทีซีพี/ไอพีสแตก



รูปที่ 2-4 ทีซีพี/ไอพี โพรโตคอลเมื่อเทียบกับโอเอสไอโมเด็ล
(ที่มา: โครงสร้างและหลักการทำงานเบื้องต้น อานันท์ สีห์พิทักษ์เกียรติ)

1. ทีซีพี/ไอพีสแตก

ชั้นที่ 1: เน็ตเวิร์กอินเตอร์เฟซ (Network Interface)

เป็นชั้นที่ควบคุมฮาร์ดแวร์การรับส่งข้อมูลผ่านเครือข่าย ซึ่งเทียบได้กับชั้นที่ 1 และชั้นที่ 2 ของโอเอสไอโมเด็ล ในชั้นนี้จะทำหน้าที่เชื่อมต่อกับฮาร์ดแวร์และควบคุมการรับส่งข้อมูลในระดับฮาร์ดแวร์ของเครือข่ายทีซีพี/ไอพี ไม่ได้กำหนดรูปแบบของการเชื่อมต่อในระดับนี้ไว้ใหม่แต่ได้ใช้มาตรฐานที่มีอยู่เดิมที่กำหนดไว้ก่อน ซึ่งที่ใช้กันอยู่จะเป็นตามมาตรฐานของ IEEE เช่น IEEE 802.3 จะเป็นการเชื่อมต่อผ่านLAN แบบ Ethernet LAN หรือ IEEE 802.5 จะเป็นการเชื่อมต่อผ่าน LAN แบบ Token Ring เป็นต้น ตัวอย่างการทำงานได้แก่ การเพิ่มเฮดเดอร์เข้าไปในดาต้าแกรมเพื่อให้กลายเป็นเฟรมแล้วส่งไปตามเครือข่าย

ชั้นที่ 2: ชั้นอินเทอร์เน็ต (Internet Layer)

ในชั้นนี้มีหน้าที่ส่งผ่านข้อมูลระหว่างเครือข่าย ทำการหาเส้นทางการส่ง หน้าที่ของชั้นนี้เทียบเท่ากับชั้นเน็ตเวิร์กและชั้นดาต้าลิงก์ของโอเอสไอโมเด็ล โดยมีโพรโตคอลที่ทำงานเป็นกลไกสำคัญในชั้นนี้คือไอพีนอกจากนี้ยังมีโพรโตคอลที่ทำงานอยู่ในชั้นนี้อีก 2 ชนิด คือ ไอซีเอ็มพี (Internet Control Message Protocol, ICMP) และเออาร์พี (Address Resolution Protocol, ARP)

ชั้นที่ 3: ชั้นทรานสปอร์ต (Transport Layer)

รับผิดชอบการส่งข้อมูลจากจุดต้นทางไปจนถึงปลายทาง หากเปรียบเทียบกับโอเอสไอโมเด็ลก็สามารถเทียบได้กับชั้นเซสชั่นรวมกับชั้นทรานสปอร์ตนั่นเอง โดยมีซ็อคเก็ตเป็นจุดปลายในการสื่อสาร ซึ่งซ็อคเก็ตนี้ประกอบไปด้วยหมายเลขของคอมพิวเตอร์และหมายเลขพอร์ตของเครื่อง

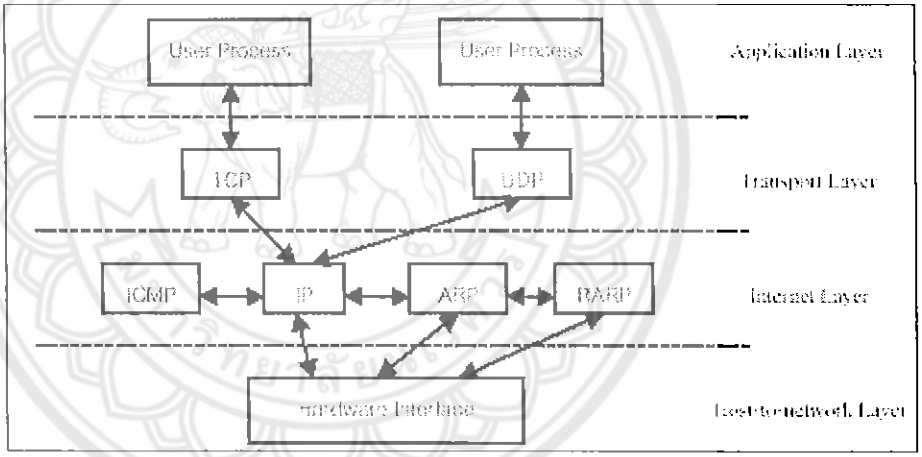
ที่ต้องการส่งข้อมูลไปถึง บริการหลักในชั้นนี้มีอยู่ 2 แบบ คือ คอนเน็คชั่นโอเรียนเต็ด โดยผ่านทีซีพี และ คอนเน็คชั่นเลส ซึ่งผ่านยูดีพี

ชั้นที่ 4 : ชั้นแอปพลิเคชั่น (Application Layer)

ชั้นนี้รองรับการทำงานของแอปพลิเคชั่นต่างๆ ที่ทำงานอยู่ในเครื่องต้นทางและปลายทาง การทำงานของแอปพลิเคชั่นต่างๆมีการติดต่อกันตามแต่ละโพรโตคอลเฉพาะแล้วแต่แอปพลิเคชันที่ใช้งาน การทำงานในชั้นนี้เทียบได้กับชั้นแอปพลิเคชั่นรวมกับชั้นพรีเซนเทชั่นของโอเอสไอโมเด็ล

2. ชุดของทีซีพี/ไอพี โพรโตคอล

ชุดของทีซีพี/ไอพีโพรโตคอล นอกจากมีโพรโตคอลทีซีพีและไอพีแล้ว ยังมีโพรโตคอลอื่นๆอีกดังภาพแสดงความสัมพันธ์ของชุดโพรโตคอลโดยแบ่งตามชั้น



รูปที่ 2-5 ความสัมพันธ์ของชุดโพรโตคอล

(ที่มา: เปิดโลก TCP/IP และโปรโตคอลของอินเตอร์เน็ต สุวัฒน์ ปุณณชัยยะ)

2.5 โพรโตคอล

1. โพรโตคอลทีซีพี

เป็นโพรโตคอลแบบคอนเน็คชั่นโอเรียนเต็ดซึ่งจะรับประกันการรับ-ส่งข้อมูลมีความน่าเชื่อถือ หน้าที่ของการทำงานของทีซีพีในการรับส่งข้อมูลมี 6 อย่าง ดังนี้

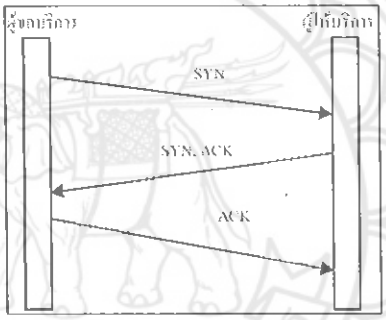
1. ควบคุมการรับส่งข้อมูล (Basic Data Transfer)
2. ความน่าเชื่อถือในการรับส่งข้อมูล (Reliability)
3. ควบคุมการไหลของข้อมูล (Flow Control)

4. การทำมัลติเพล็ก (Multiplexing)

5. ควบคุมการเชื่อต่อ (Connection)

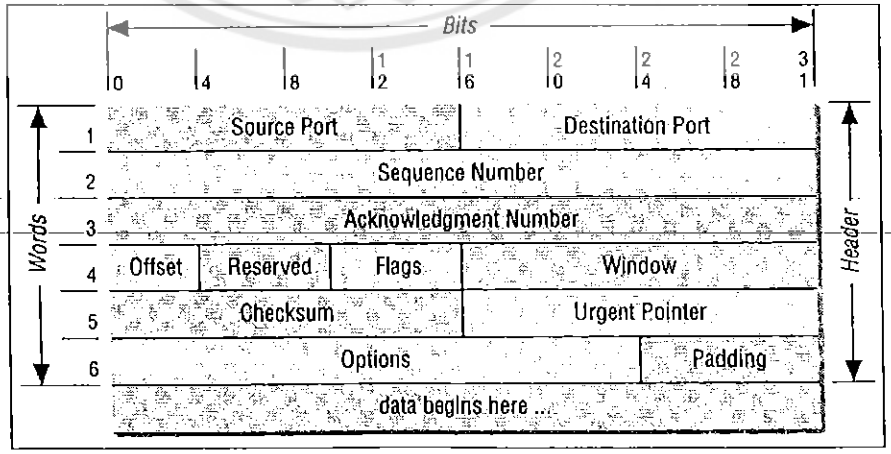
6. ความปลอดภัยในการรับส่งข้อมูล (Security)

การทำงานที่สำคัญอย่างหนึ่งของทีซีพี คือการทำ "3-way Handshake" ซึ่งเป็นการระบวนการเริ่มต้นในการสร้างการเชื่อมต่อในชั้นทรานสปอร์ต กล่าวคือ ในการติดต่อกันระหว่างระบบเครือข่ายต้องมีการสร้างการเชื่อมต่อไปยังระบบที่ให้บริการก่อน โดยผู้ขอบริการส่งสัญญาณ SYN เพื่อขอบริการจากนั้นผู้ให้บริการจะส่งสัญญาณ ACK เพื่อตอบรับการเชื่อต่อที่ร้องขอมา จึงจะเริ่มต้นส่งข้อมูลได้การเชื่อมต่อแบบ 3-way handshake นี้เป็นการตรวจสอบความพร้อมของทั้งฝ่ายส่งและฝ่ายรับและการกำหนดค่าเริ่มต้นของพารามิเตอร์ต่างๆของทั้งสองฝ่ายให้ตรงกัน หลังจากกระบวนการทำ 3-way handshake สิ้นสุด ทั้งสองฝ่ายจึงสามารถรับและส่งข้อมูลระหว่างกันได้



รูปที่ 2-6 3-way handshakes

(ที่มา: เปิดโลก TCP/IP และโปรโตคอลของอินเตอร์เน็ต สุวัฒน์ ปุณณชัยยะ)



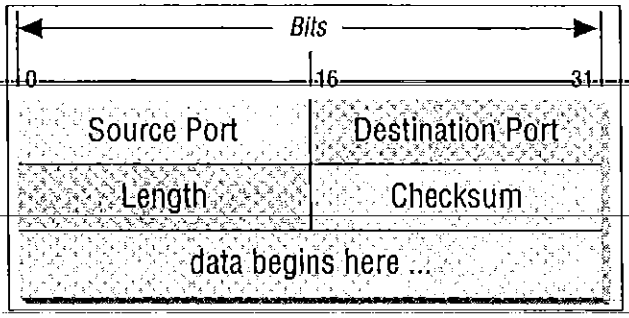
รูปที่ 2-7 ส่วนประกอบของทีซีพี เฮดเดอร์

(ที่มา: โครงสร้างและหลักการทำงานเบื้องต้น อานันท์ สีห์พิทักษ์เกียรติ)

เฮดเดอร์ของทีซีพี

- Source port (16-bit) พอร์ตที่โปรแกรมผู้ส่งใช้ส่งข้อมูล
- Destination port (16-bit) พอร์ตทางฝั่งผู้รับที่ข้อมูลถูกส่งไป
- Sequence number (32-bit) บอกตำแหน่งของข้อความที่ถูกแบ่งเมื่อข้อมูลมีขนาดใหญ่เกินกว่าที่ระบบกำหนด ใช้ในการเรียงลำดับข้อมูลเมื่อถึงผู้รับ
- Acknowledgement number (32-bit) บอก Sequence number ที่ควรจะเป็น
- Data offset (4-bit) นำขนาดของ Header คำนวณหาตำแหน่งเริ่มต้นของข้อมูล
- Reserved (6-bit) สงวนไว้สำหรับใช้ในอนาคต แต่เนื่องจากไม่เคยถูกใช้ จึงเซ็ทค่าเป็นศูนย์
- URG flag ถ้ามีค่าเป็น "1" Urgent Pointer จะชี้อยู่ที่ข้อมูลที่มี flag บอกว่า "urgent"
- ACK flag ถ้ามีค่าเป็น "1" แสดงว่าแพ็คเก็ต2เป็นแพ็คเก็ตตอบรับ เมื่อมีผู้ส่งส่งการร้องขอการติดต่อข้อมูลออกไป
- PSH flag ถ้ามีค่าเป็น "1" มีการใช้ push function
- RST flag ถ้ามีค่าเป็น "1" เป็นการเริ่มต้นการติดต่อใหม่
- SYN flag ถ้ามีค่าเป็น "1" แสดงถึง Sequence number เกิดขึ้นในจังหวะเดียวกัน
- FIN flag ถ้ามีค่าเป็น "1" ผู้ส่ง ส่งข้อมูลเสร็จสิ้น
- Window (16-bit) จำนวนบล๊อคของข้อมูลที่ผู้รับสามารถรับได้ในขณะหนึ่ง
- Checksum (16-bit) เป็นการคำนวณเพื่อตรวจสอบความถูกต้องของข้อมูลทั้งในส่วนเฮดเดอร์และเนื้อหา
- Urgent Pointer (16-bit) ถ้า URG flag มีค่าเป็น "1" พอยเตอร์จะชี้ไปยังที่ซึ่งเก็บ Urgent Data โดยฟิลด์นี้จะถูกเรียกใช้จากโปรแกรมที่อยู่เหนือทีซีพีในสแตก
- ออปชัน (Option) ความยาวไม่คงที่เช่นเดียวกับออปชันในเฮดเดอร์ของไอพี หน้าที่หนึ่งของออปชันคือการกำหนดขนาดใหญ่สุดของเซกเมนต์ (Segment) และเนื่องจากความยาวที่ไม่แน่นอนของออปชันทำให้ต้องมี padding เพื่อเติมขนาดให้เต็ม 32-bit

2. โพรโตคอลยูดีพี

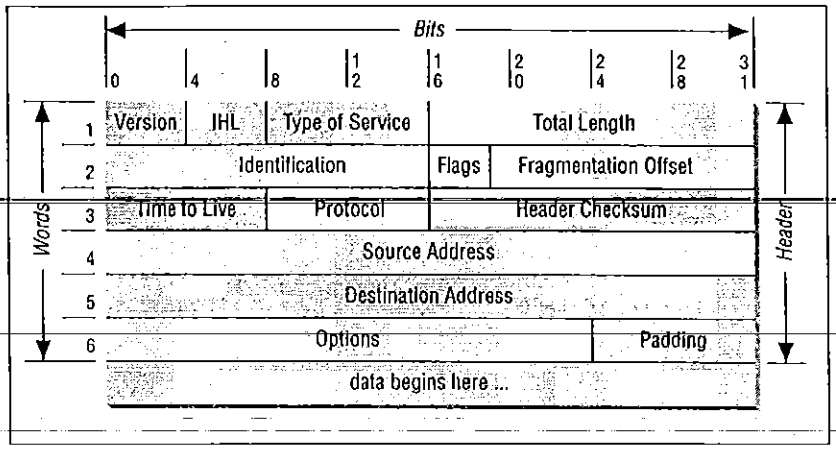


รูปที่ 2-8 ส่วนประกอบของยูดีพี เฮดเดอร์ ทุกฟิลด์มีขนาด 16-bit
(ที่มา: โครงสร้างและหลักการทำงานเบื้องต้น อานันท์ สีห์พิทักษ์เกียรติ)

มีการทำงานคล้ายกับทีซีพี คือ จัดการเกี่ยวกับการสื่อสารระหว่างเครื่อง แต่เป็นแบบคอนเน็คชั่นเลส คือ ทั้งฝ่ายส่งและฝ่ายรับไม่จำเป็นต้องอาศัยการสร้างช่องทางเชื่อมต่อกัน และไม่รับรองว่าข้อมูลที่ส่งไปจะไปถึงปลายทางหรือไม่ และอาจซ้ำซ้อนหรือผิดลำดับได้ แต่ข้อดีของโพรโตคอลนี้คือโอเวอร์เฮดต่ำ

3. โพรโตคอลไอพี

ไอพีเป็นโพรโตคอลที่จัดการเกี่ยวกับแอดเดรสของแต่ละแพ็คเก็ต เพื่อให้การส่งแพ็คเก็ตต่างๆไปยังเป้าหมายได้ถูกต้อง การทำงานของไอพีเป็นเพียงการส่งข้อมูลไปยัง เครื่องเป้าหมายเท่านั้น ไม่มีการส่งสัญญาณของบริการ หรือสัญญาณให้บริการระหว่างกันเหมือนทีซีพี กล่าวคือเป็นการเชื่อมต่อแบบคอนเน็คชั่นเลส โดยปล่อยให้โพรโตคอลในชั้นที่เหนือขึ้นไปมีหน้าที่จัดการเรื่องความถูกต้อง การหาเส้นทางของข้อมูลจะทำในระดับของไอพีนี้ โดยพิจารณาแต่ละแพคเก็ตแยกออกจากกัน ในข้อมูลของโพรโตคอลไอพีจะมีข้อมูลของหมายเลขไอพีปลายทางที่จะส่งข้อมูลไปและเมื่อถึงเครือข่ายปลายทางแล้วจะมี กลไกแปลงหมายเลขไอพีให้เป็นหมายเลขฮาร์ดแวร์ประจำเครื่องที่ถูกต้องอีกทีหนึ่งด้วยโพรโตคอล เออาร์พี



รูปที่ 2-9 ส่วนประกอบของไอพี เฮดเดอร์

(ที่มา: โครงสร้างและหลักการทำงานเบื้องต้น อานันท์ สีห์พิทักษ์เกียรติ)

- Version (4-bit) เวอร์ชันของไอพี ถ้าเวอร์ชันต่างกัน รูปแบบของข้อมูลในเฮดเดอร์จะต่างกัน และไม่สามารถใช้ร่วมกันได้ ปัจจุบันมีเพียงถึงเวอร์ชัน 4 สำหรับไอพีเวอร์ชันถัดไป เรียกว่า "IPV6"
- Internet Header Length, IHL (4-bit) บอกความยาวในส่วนของเฮดเดอร์ ทำให้โปรแกรมสามารถคำนวณและทราบได้ว่าส่วนของข้อมูลเริ่มต้นที่บิตใด
- Type of Service (8-bit) บอกลำดับความสำคัญก่อนหลังของแพ็กเก็ต แต่เนื่องจากยังไม่มีการใช้ในไอพีเวอร์ชัน 4 นี้ จึงมีค่าเป็น 0s
- Datagram Length (8-16bit) บอกความยาวของทั้งดาต้าแกรมมีขนาด 8-bit หรือมากถึง 65,535 ไบต์(16-bit) หากลบออกด้วย IHL ก็จะสามารถทราบความยาวในส่วนของเนื้อหาได้
- Identification (16-bit) เป็นฟิลด์ที่บ่งชี้ว่าดาต้าแกรมนี้มาจากข้อความใด ในกรณีที่ข้อความมีขนาดใหญ่เกินจากที่กำหนด ต้องแบ่งออกให้เป็นดาต้าแกรมย่อย แต่ไม่ได้บอกลำดับของดาต้าแกรม
- Flags (3-bit) เป็นตัวที่บอกว่าดาต้าแกรมนี้ได้มาจากการแฟรกเมนเทชั่นหรือไม่
- Time to Live, TTL (8-bit) ตัวกำหนดระยะเวลายาวนานที่สุด ที่ดาต้าแกรมจะอยู่ในเครือข่าย
- Protocol (8-bit) ชนิดของโพรโตคอลของข้อมูลที่อยู่ในดาต้าแกรม
- Header Checksum (16-bit) เช็คความถูกต้องของข้อมูลส่วนเฮดเดอร์
- Source Address (32-bit) หมายเลขไอพีของผู้ส่งดาต้าแกรม
- Destination Address (32-bit) หมายเลขไอพีของดาต้าแกรมที่ถูกส่งไป

- ออปชัน เช่น Control, Reserved, Debugging หรือ Measurement
- Padding เนื่องจากออปชันมีขนาดไม่แน่นอน จึงนำแพดดิงมาทำให้ดาต้าแกรมมีขนาด32บิต

4. โพรโตคอลไอซีเอ็มพี (Internet Control Message Protocol)

การแจ้งเตือนหรือแสดงข้อความจากระบบ เพื่อบอกให้ผู้ใช้ทราบว่าเกิดอะไรขึ้นในการส่งผ่านข้อมูลนั้น ซึ่งปัญหาส่วนมากคือส่งไปไม่ได้ หรือปลายทางรับข้อมูลไม่ได้ ข้อความที่ไอซีเอ็มพีส่งนั้นแบ่งออกได้ 2 แบบคือ ข้อความแจ้งข้อผิดพลาด และ ข้อความเรียกขอข้อมูลเพิ่ม คำสั่ง ping หรือ trace route ก็เป็นคำสั่งหนึ่งของ ไอซีเอ็มพี คำสั่งที่สำคัญของ ไอซีเอ็มพี

- **ping** จะใช้ echo request และ echo reply message เพื่อตัดสินว่ามีการติดต่อกันจริงระหว่างสองเครือข่าย
- **Source quenches message** ใช้บอกผู้ส่ง เมื่อส่งข้อมูลในอัตราเร็วเกินกว่าที่ผู้รับ สามารถรับได้ทัน
- **redirect message** เราเตอร์ใช้ในการบอกเราเตอร์ตัวอื่นๆ เมื่อพบเส้นทางไปสู่ปลายทางที่ดีกว่า
- **Time exceeded message** เราเตอร์ใช้ในการบอกอุปกรณ์อื่นๆ หากแพ็คเก็ตถูกทิ้งไป เช่นเดียวกับทีซีพีและยูดีพี ไอซีเอ็มพี ใช้ไอพีโพรโตคอลในการส่งผ่านข้อมูลออกสู่เครือข่าย

5. โพรโตคอลเออาร์พี (Address Resolution Protocol)

ถูกเรียกใช้งานโดยโพรโตคอลไอพีเพื่อช่วยแปลงหมายเลขไอพีไปเป็นหมายเลขไอพีปลายทางตัวอย่างเช่น เว็บเซิร์ฟเวอร์เครื่องหนึ่งเชื่อมต่ออยู่ในเครือข่ายอินเทอร์เน็ต และในการเชื่อมต่อนี้ต้องอาศัยNetwork Interface Card (NIC) หรือ LAN card ติดตั้งอยู่ LAN card นี้จะมีหมายเลขเฉพาะประจำฮาร์ดแวร์ ที่ไม่ซ้ำใคร เพื่อใช้อ้างอิงการส่งข้อมูลในเครือข่าย แต่เมื่อมาใช้งานโพรโตคอล ทีซีพี/ไอพี ก็จะต้องมีการกำหนดหมายเลขไอพีหมายเลขประจำตัวเพื่อใช้อ้างอิงกัน และโพรโตคอลเออาร์พีจะทำหน้าที่แปลงค่าหมายเลขไอพีให้เป็นหมายเลขฮาร์ดแวร์จริงให้ในระดับการทำงานที่ชั้นอินเทอร์เน็ตเวิร์ก ซึ่งกลไกในการแปลงนี้เรียกว่า address resolution

2.6 บริการของ ทีซีพี/ไอพี

1. เทลเน็ต

เป็นโปรแกรมบน UNIX ที่อนุญาตให้ผู้ใช้เข้าสู่ระบบได้ แม้จะอยู่นอกพื้นที่ของเครือข่าย เทลเน็ตถูกนำมาพัฒนาให้สามารถใช้ได้บนหลายระบบปฏิบัติการ เช่น ผู้ใช้สามารถเข้าสู่ระบบได้ ถึงแม้จะเรียกใช้จาก Window NT แต่ยังคงใช้คำสั่งของ UNIX ในการดำเนินการต่างๆ การใช้งาน เทลเน็ตถูกนำมาใช้อยู่บนพอร์ต 23

2. เอฟทีพี

เช่นเดียวกับเทลเน็ตเป็นบริการ (Service) ที่ใช้สำหรับรับ-ส่งไฟล์ สามารถเข้าสู่ระบบได้แม้จะอยู่ในพื้นที่อื่นภายนอกเครือข่าย ด้วยการใช้ Username และPassword รวมถึง Anonymous ซึ่งอนุญาตให้ผู้ใดก็ตามสามารถใช้บริการนี้ได้ FTP ถูกนำมาใช้บริการอยู่บนพอร์ต 21

3. ดีเอ็นเอส

ทำหน้าที่แปลงข้อมูลชื่อโดเมนเนม หรือชื่อเว็บไซต์ทั้งหลายให้เป็นหมายเลขไอพี

4. เอสเอ็มทีพี

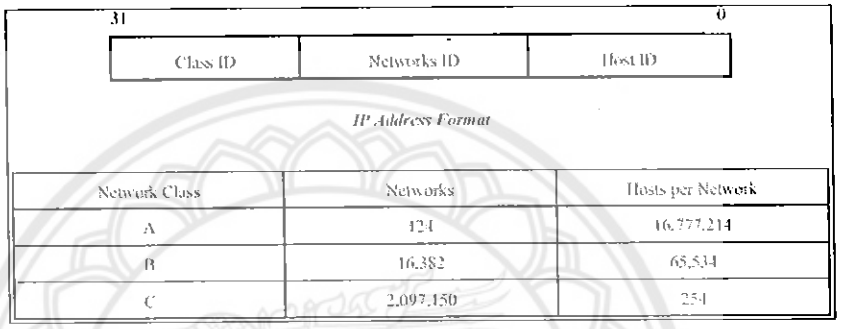
เป็นบริการสำหรับการส่งและรับอีเมล์ โดยจะถูกเรียกใช้ขณะที่โปรแกรมคอมพิวเตอร์ของด้านผู้ใช้งาน ส่งเมล์มาที่ MTA3 (Mail Transfer Agent) และใช้รับส่งอีเมล์ระหว่าง MTA ด้วยกัน สำหรับการใช้เมล์บนเครื่องที่ผู้ใช้ใช้อ่านเมล์ไม่ได้ต่อกับเครื่องที่มีเมล์บ๊อกซ์ตลอดเวลา อาจจะดาวน์โหลดเมล์มาเก็บไว้ที่เครื่องของตัวเอง โดยใช้โพรโตคอล POP (Post Office Protocol) และ IMAP (Internet Message Access Protocol) ได้

2.7 รูปแบบและการกำหนดแอดเดรสของ ทีซีพี/ไอพี

ในหัวข้อนี้จะได้อธิบายรูปแบบการกำหนดแอดเดรสของโพรโตคอลทีซีพี/ไอพี ซึ่งลักษณะ แอดเดรสของโพรโตคอล นี้ค่าของแอดเดรสของเครื่องในระบบเครือข่ายจะไม่ซ้ำกันเลย โดยเรียกเลขนี้ว่าหมายเลขไอพี เป็นเลข 32 บิตซึ่งแบ่งเป็นคลาส ตามหลักในการพิจารณาที่จะได้กล่าวต่อไปนี้

1. การแบ่งคลาสเน็ตเวิร์ก

เนื่องจากหมายเลขแอดเดรสของคอมพิวเตอร์เครื่องใดๆนั้น จะต้องสามารถบอกถึงความแตกต่างระหว่างตัวเรื่องเอง ตลอดจนเครือข่ายที่คอมพิวเตอร์นั้นเชื่อมต่ออยู่ด้วย หมายเลขไอพีจึงแบ่งแยกออกเป็น2 ส่วน ได้แก่ ส่วนที่แสดงหมายเลขของโฮสต์และส่วนที่เป็นหมายเลขของเครือข่ายการแบ่งคลาสของแอดเดรสทำได้โดยพิจารณาจำนวนบิตของ 2 ส่วนประกอบข้างต้น ซึ่งมีการแบ่งออกเป็น 5 คลาส แต่มีการใช้เพียง 3 คลาสแรก คือ คลาส A, คลาส B และ คลาส C ส่วนคลาส D และคลาส E ถูกสงวนไว้สำหรับจุดประสงค์พิเศษ



Network Class	Networks	Hosts per Network
A	124	16,777,214
B	16,382	65,534
C	2,097,150	254

รูปที่ 2-10 คลาส, จำนวนเครือข่าย และจำนวนโฮสต์ของแต่ละคลาส
(ที่มา: เปิดโลก TCP/IP และโปรโตคอลของอินเตอร์เน็ต สุวัฒน์ ปุณณชัยยะ)

2. การทำซับน็ต (Sub netting)

การทำซับเน็ตเป็นการเปลี่ยนแปลงการใช้หมายเลขของเครื่องโฮสต์และหมายเลขของเครือข่ายในระดับท้องถิ่นโดยในทางตรรก คือ การเลื่อนเส้นแบ่งที่แยกหมายเลขเครื่อง และหมายเลขของเครือข่ายที่อยู่ ในหมายเลขไอพีโดยที่ปริมาณของหมายเลขโฮสต์และ หมายเลขเครือข่ายจะแปรผกผันกัน ยกตัวอย่างเช่น หากมีปริมาณของเครือข่ายมาก ก็จะทำให้เครื่องใดๆที่จะต่อ กับระบบเครือข่ายหนึ่งๆน้อยลง เป็นต้น ในการปฏิบัติการทำซับเน็ตทำโดยการทำซับเน็ตมาสก์ (Subnet Mask) คือตัวเลขจำนวน 32 บิต มาทำการ AND กับหมายเลขไอพีตัวอย่างเช่นกำหนดหมายเลขไอพีเป็น 192.168.5.13 และซับเน็ตมาสก์คือ 255.255.255.0 จะได้เป็น 192.168.5.0จะเห็นว่าหากพิจารณาโดยไม่มีการทำซับเน็ตแล้วจะได้หมายเลขของเน็ตเวิร์คคือ161.246 และหมายเลขประจำเครื่องคือ 5.13 แต่ผลที่ได้จากการทำซับเน็ตจะได้หมายเลขเน็ตเวิร์ค เป็น 192.168.5.0 และหมายเลขเครื่องคือ 13 หรืออาจกล่าวได้ว่า คอมพิวเตอร์เครื่องนี้มีหมายเลขเครื่องเท่ากับ 13 และอยู่บนเครือข่ายย่อยหมายเลข 192.168.52.6 หมายเลขพอร์ต เนื่องจากในเวลาใดๆสามารถมีโพรเซสของผู้ใช้สามารถใช้ยูดีพีหรือทีซีพีได้พร้อมกันหลายๆโพรเซส ดังนั้นจึงต้องมีวิธีแยกแยะว่าข้อมูลเป็นของโพรเซสใด ซึ่งวิธีที่ทีซีพีและยูดีพีใช้ คือการใช้หมายเลขพอร์ตเมื่อ

โพรเซสของเครื่องไคลเอนต์ต้องการที่จะติดต่อกับเซิร์ฟเวอร์ ไคลเอนต์จะต้องติดต่อแต่ล่าพังรู้หมายเลขอินเตอร์เนต 32 บิต เพียงอย่างเดียวนั้นไม่เพียงพอ เพราะว่าสามารถติต่อกับโฮสต์ได้เพียงอย่างเดียวแต่ไม่สามารถเจาะจงโพรเซสที่จะทำการติดต่อได้ ดังนั้ นเพื่อแก้ปัญหานี้ทั้งทีซีพีและยูดีพี ได้มีการกำหนดหมายเลขพอร์ตมาตรฐาน (well-known ports) ซึ่งเป็นที่รู้จักกัน เช่น ทุกๆ ระบบทีซีพี/ไอพี จะกำหนดพอร์ต 23 เป็นพอร์ตบริการของเทลเน็ตเป็นต้น

เมื่อทีซีพีหรือยูดีพี กำหนดหมายเลขพอร์ตที่ไม่ซ้ำกันให้โพรเซสของผู้ใช้ เราเรียกหมายเลขพอร์ตนี้ว่ าหมายเลขพอร์ตชั่วคราว (ephemeral port numbers) เมื่อไคลเอนต์เลิกใช้หมายเลขพอร์ตนี้แล้วสามารถกำหนดหมายเลขพอร์ตนี้ให้ไคลเอนต์อื่นได้ โพรเซสที่ได้รับหมายเลขพอร์ตชั่วคราวนี้จะไม่สนใจว่ามีค่าเท่าไร แต่เป็นหน้าที่ของอีกโพรเซสหนึ่งที่ต่อกันที่ต้องสนใจเพราะต้องส่งข้อมูลกลับมาที่พอร์ตนี้ในทีซีพี และ ยูดีพี นั้น หมายเลขพอร์ตตั้งแต่ 1-1023 เป็นพอร์ตที่สงวนไว้สำหรับหมายเลขพอร์ตมาตรฐาน

2.8 ไฟร์วอลล์

1. หน้าที่ของไฟรวอลล์

จุดประสงค์ของการมีระบบไฟร์วอลล์ในเครือข่ายก็เพื่อป้องกันการเข้าสู่ระบบจากผู้บุกรุกภายนอก และปล่อยให้เฉพาะผู้ใช้ที่มีสิทธิถูกต้องในการใช้ระบบคอมพิวเตอร์ทำงานได้ตามปกติ ไฟร์วอลล์มีหน้าที่กว้าง แต่โดยหลัก ๆ แล้วอาจแบ่งกลไกการทำงานได้เป็นสองส่วนคือ

- ส่วนที่ทำหน้าที่ ขวางกั้นข้อมูลโปรแกรมหรือผู้ใช้ Network traffic ที่ไม่ได้รับการอนุญาตไว้ก่อนล่วงหน้า (Forbidden) จะไม่สามารถเข้ามาในระบบโดยผ่านไฟร์วอลล์ได้
- ส่วนที่อนุญาตให้ ข้อมูล โปรแกรม หรือผู้ใช้ Network traffic ที่ไม่ได้รับการห้ามไว้ (Permitted) จะสามารถเข้ามาในระบบผ่านไฟร์วอลล์ได้

ไฟร์วอลล์บางชนิดจะเน้นที่การขวางกั้น Traffic แต่ไฟร์วอลล์แบบอื่นๆจะเน้นการให้ Traffic ผ่านไปได้แต่สิ่งที่ควรจำไว้คือไฟร์วอลล์จะนำ นโยบายควบคุมการเข้าถึง (Access control policy) ไปดำเนินการ ไฟร์วอลล์จะเป็นเสมือนสวิทซ์ปิดเปิดที่จะทำหน้าที่ควบคุมการอนุญาตให้เครือข่ายภายนอกติดต่อกับเครือข่ายภายในได้

2. ฟังก์ชันของไฟร์วอลล์

- มีกฎการควบคุมการเข้าถึง
- อนุญาตให้เฉพาะผู้ที่มีสิทธิ์ผ่านเข้าไปได้
- ช่วยป้องกันการเข้าถึงของผู้ที่ไม่ได้รับอนุญาต
- ช่วยปกป้องข้อมูลไม่ให้เกิดการรั่วไหล
- มีการเก็บ Log file ที่เป็นข้อมูลการไหลเข้าออกของข้อมูล
- ไฟร์วอลล์ป้องกันตัวเองและส่วนที่ควรแก่การป้องกันอันตราย มันสามารถรองรับการเข้าถึงของหลายๆ Server ได้ และสามารถให้การเข้าถึงที่ดีได้

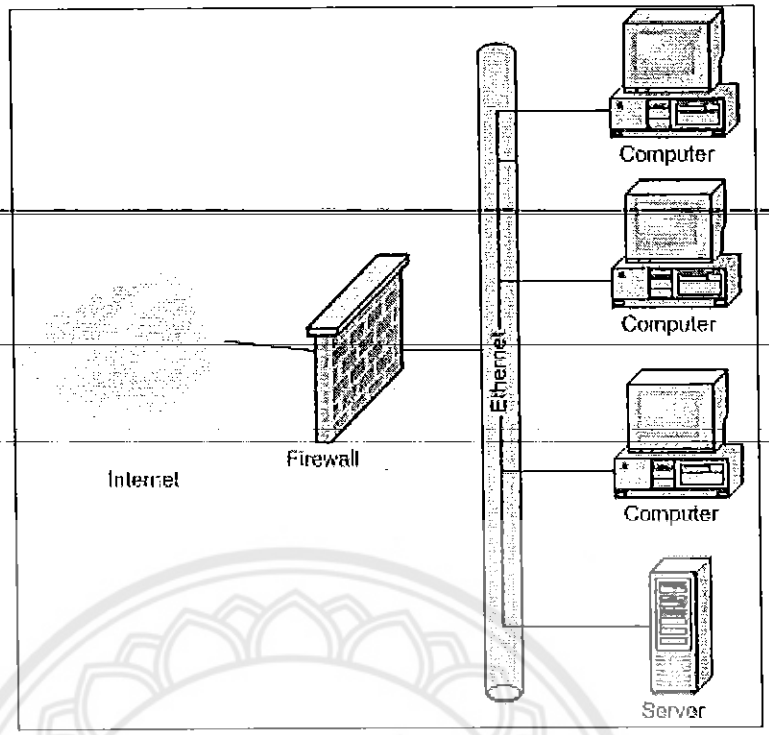
3. คุณสมบัติของไฟร์วอลล์

- เป็นระบบการรักษาความปลอดภัยที่ทำงานอยู่ตลอดเวลา (Always Invoked)
- เป็นระบบที่ไม่สามารถจะทำการดัดแปลงแก้ไขได้โดยง่ายจากผู้ไม่ประสงค์ดี (Tamper Proof)
- เป็นระบบที่มีขนาดเล็กและมีการทำงานที่ไม่สลับซับซ้อนมากนัก ซึ่งทำให้ง่ายต่อการวิเคราะห์และตรวจสอบขีดความสามารถในการรักษาความปลอดภัยของระบบไฟร์วอลล์

2.9 ประเภทของไฟร์วอลล์

1. เกตเวย์ไฟร์วอลล์ (Gateway Firewall) หรือไฟร์วอลล์ (Firewall)

ไฟร์วอลเป็นระบบหรือกลุ่มของระบบป้องกันที่บังคับใช้นโยบายการรักษาความปลอดภัยระหว่างเครือข่ายกับเครือข่าย หรือเครือข่ายกับอินเทอร์เน็ต ไฟร์วอลล์เป็นตัวกำหนดว่าบริการของเครือข่ายภายในชนิดใดบ้างที่เข้าถึงได้จากภายนอก และบริการภายนอกในขณะที่เข้าถึงได้จากผู้ใช้ภายใน ไฟร์วอลสามารถที่จะป้องกันการโจมตีจากภายนอกเครือข่ายได้ โดยจะกรองข้อมูล (หมายเลขไอพี สับเน็ตพอร์ต ฯลฯ) และอนุญาตให้ผู้ใช้ที่มีข้อมูลที่น่าไว้ใจเท่านั้น ผ่านเข้ามาในระบบเครือข่ายของเราวิธีการของไฟร์วอลล์ จะจำกัดให้มีการผ่านเข้าออกได้ ที่จุดเดียว (Controlled point) และป้องกันผู้บุกรุกที่พยายามจะเข้ามาในเครือข่าย ดังนั้นการรับส่งข้อมูลทั้งหมดต้องผ่านไฟร์วอลล์ซึ่งเป็นด่านสำหรับตรวจสอบแพ็คเก็ต ไฟร์วอลล์มีหน้าที่ตัดสินใจว่าจะอนุญาตให้แพ็คเก็ตนั้นผ่านไปหรือไม่ ซึ่งการตัดสินใจนี้ ขึ้นอยู่กับกฎเกณฑ์ที่กำหนดไว้ สอดคล้องกับนโยบายขององค์กร



รูปที่ 2-11 ไฟร์วอลล์กั้นระหว่างอินเตอร์เน็ตกับเน็ตเวิร์กภายใน

(ที่มา: www.thaicert.nectec.or.th/)

2. สิ่งที่ไฟร์วอลล์สามารถทำได้

- เป็นจุดสำคัญของการตัดสินใจเพื่อรักษาความปลอดภัย เนื่องจากเป็นจุดเดียวที่เครือข่ายติดต่อกับเครื่องภายนอกเครือข่าย
- สามารถตรวจสอบ และเก็บรายละเอียดกิจกรรมต่างๆ ระหว่างเครือข่ายภายใน และเครือข่าย
  ภายนอก เพราะในการติดต่อทุกครั้งต้องผ่านไฟร์วอลล์
- สามารถกำหนดกฎเกณฑ์ นโยบายในการอนุญาต หรือไม่อนุญาตในการใช้บริการต่างๆ ภายในเครือข่าย
- มีการตรวจตราบริการต่างๆ ทำงานได้อย่างถูกต้อง

3. สิ่งที่ไฟร์วอลล์ไม่สามารถทำได้

- ไฟร์วอลล์ไม่สามารถป้องกันผู้บุกรุกที่ อยู่ภายในเครือข่าย(Internal Network)
- ไฟร์วอลล์ไม่สามารถป้องกันการโจมตีที่ไม่ได้ผ่านไฟร์วอลล์ เช่น ผู้ใช้ภายในเครือข่ายมีการ
- เชื่อมต่อกับอินเทอร์เน็ตในทางอื่น ซึ่งไม่ผ่านไฟร์วอลล์ โดยที่ผู้ดูแลระบบไม่รับทราบ เช่น

การ Dial-up ไปยังอินเทอร์เน็ตจากเครื่องคอมพิวเตอร์ส่วนตัวที่อยู่ภายในเครือข่าย

- ไม่สามารถป้องกันไวรัสหรือ Trojan Horse ได้ เพราะไฟร์วอลล์ไม่สามารถตรวจสอบรายละเอียดข้อมูลที่อยู่ภายในแพ็คเก็ตว่ามีไวรัสหรือไม่

2.10 เพอร์ซันนอลไฟร์วอลล์ (Personal Firewall)

เป็นซอฟต์แวร์แอปพลิเคชั่นออกแบบมาเพื่อผู้ใช้ทั่วไปที่มีการเชื่อมต่อแบบ "always-on" อย่างเช่น ดีเอสแอล หรือ เคเบิลโมเด็ม โดยพื้นฐานการทำงานเป็นลักษณะเดียวกับเกตเวย์ไฟร์วอลล์ คือ ตรวจสอบข้อมูลเข้าออก ต่างกันที่เพอร์ซันนอลไฟร์วอลล์ จะทำงานบนเครื่องคอมพิวเตอร์เครื่องหนึ่งไม่ได้ทำงานในระดับเครือข่าย มีลักษณะการทำงานคล้ายโปรแกรมประเภทป้องกันไวรัส เพอร์ซันนอลไฟร์วอลล์จึงได้รับความสนใจ เนื่องจากความเสี่ยงของการถูกบุกรุกในปัจจุบันนั้นเพิ่มมากขึ้น

1. รูปแบบการทำงานของไฟร์วอลล์

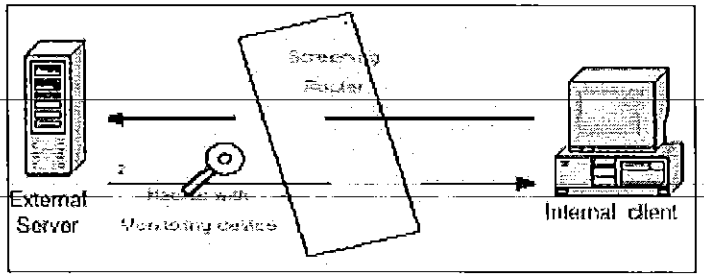
เราสามารถแบ่งรูปแบบการทำงานของไฟร์วอลล์ออกได้เป็น 3 ประเภท ตามกลวิธีในการป้องกันเครือข่ายออกจากเครือข่ายอื่นๆ สำหรับการทำงานบนเราเตอร์ในเลเยอร์ระดับล่าง จะใช้วิธีการกรองแพ็คเก็ต โดยอาศัยข้อมูลในส่วนเฮดเดอร์ เรียกว่า "แพ็คเก็ตฟูลเตอร์ริ่ง" (Packet Filtering) ส่วนการทำงานในเลเยอร์ระดับสูง ซึ่งจะมีพร็อกซีเซิร์ฟเวอร์คอยตรวจสอบเนื้อหาภายในแพ็คเก็ตและแสดงผลการตรวจสอบ เรียกว่า "พร็อกซีเซิร์ฟเวอร์เกตเวย์" และประเภทสุดท้าย จะเก็บสถานการณ์ทำงานไว้เป็นลำดับขั้น คือ "สเตทฟูลอินสเป็คชัน"

2. แพ็คเก็ตฟูลเตอร์ริ่ง (Packet-Filtering)

เป็นวิธีที่ใช้กันอย่างแพร่หลาย หลักการทำงานคือ ไฟร์วอลล์จะกรองแพ็คเก็ตโดยพิจารณาแพ็คเก็ตที่เข้าออกตามกฎที่ตั้งไว้ การตัดสินใจกรองแพ็คเก็ตเหล่านี้จะยึดข้อมูลที่อยู่ในเฮดเดอร์ของแพ็คเก็ตตัวนั้นๆ เช่น แอดเดรสต้นทาง แอดเดรสปลายทาง พอร์ตหรือโพรโตคอล เมื่อแพ็คเก็ตแต่ละแพ็คเก็ตเข้ามาสู่ไฟร์วอลล์ จะนำมาเทียบกับกฎ หากเข้ากับกฎใดกฎหนึ่ง ก็จะดูว่ากฎนั้นสั่งให้ส่งแพ็คเก็ตต่อไปหรือดร็อปแพ็คเก็ตนั้นทิ้งไป และหากไม่เข้ากับกฎใดเลย ก็จะพิจารณาว่าค่าดีฟอลต์เป็นอะไร ให้ส่งหรือดร็อป

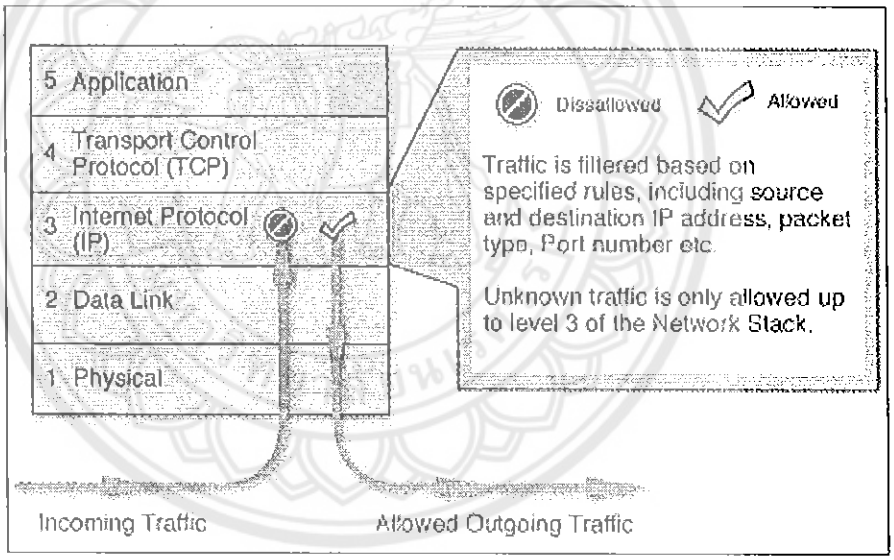
แพ็คเก็ตฟูลเตอร์ริ่ง เป็นการทำงานในชั้นเน็ตเวิร์ก วิธีการนี้เป็นวิธีที่ง่ายและทำงานได้รวดเร็วที่สุด แต่จุดอ่อนคือ ความยากในการกำหนดกฎต่างๆ ให้รัดกุมและการติดต่อกันระหว่างโฮสต์ต้นทางและโฮสต์ปลายทางได้โดยตรง อาจส่งผลให้ข้อมูลต่างๆ ของโฮสต์ปลายทาง รวมทั้ง

โฮสต์อื่นๆ ที่ติดต่ออยู่กับโฮสต์ปลายทางถูกโจมตีได้ไฟร์วอลล์แบบนี้สามารถต่อต้านการโจมตีได้หลายชนิด เช่น IP spoofing, Source Routing Attack, Tiny Fragmentation Attack



รูปที่ 2-12 รูปแบบการทำงานของแพ็คเก็ตฟูลเตอร์ริ่ง

(ที่มา: www.thaicert.nectec.or.th/)



รูปที่ 2-13 Packet-Filtering path ของ TCP/IP model

(ที่มา: www.thaicert.nectec.or.th/)

ไฟร์วอลล์ใช้ข้อมูลเหล่านี้ในการตัดสินใจว่าจะทำอย่างไรกับแพ็คเก็ตดังกล่าว ไฟร์วอลล์จะทำการใดๆก็ตามกับ แพ็คเก็ตนั้นขึ้นอยู่กับนโยบายทางด้านความมั่นคงของเครือข่ายในองค์กรนั้น เช่น ไฟร์วอลล์สามารถที่จะโยนแพ็คเก็ตทิ้งได้หากแพ็คเก็ตที่มันรับมานั้นเป็นแพ็คเก็ตที่มีเลขที่อยู่ต้นทางมาจากคอมพิวเตอร์บางเครื่องที่ไม่ได้รับอนุญาตให้ส่งข้อมูลมายังเครือข่ายที่ไฟร์วอลล์ปกป้องอยู่ เป็นต้น

ไฟร์วอลล์ระดับเครือข่ายที่พัฒนาขึ้นในระยะหลังนี้มีความสามารถที่จะจดจำสถานะของการเชื่อมต่อระหว่างคอมพิวเตอร์สองเครื่องที่สื่อสารกันผ่านไฟร์วอลล์ได้นอกจากนี้มันยังสามารถเก็บบันทึกข้อมูลกาเชื่อมต่อเหล่านี้เอาไว้ได้อีกด้วยถ้าผู้บริหารเครือข่ายต้องการ เราอาจจะให้มันบันทึกข้อมูลสัมภาระที่แพ็คเก็ตขนมา(payload) ก็สามารถทำได้ ข้อมูลเหล่านี้มีประโยชน์มากต่อการบริหารเครือข่ายขององค์กรทั้งในแง่ของการป้องกันการโจมตีที่มาจากเครือข่ายภายนอก การป้องกันการบ่อนทำลายที่มาจากภายในเครือข่ายการค้นหาต้นต่อหรือระบุตัวผู้บุกรุก การเก็บสถิติของการใช้บริการของระบบคอมพิวเตอร์เพื่อการพัฒนาการให้บริการที่ดีขึ้น และอื่นๆอีกมามายนอกเหนือจากความสามารถที่กล่าวไปแล้ว ความแตกต่างที่สำคัญของไฟร์วอลล์ระดับเน็ตเวิร์คอย่างหนึ่งคือมันจะนำทางการติดต่อที่ผ่านมันโดยตรง ดังนั้นจึงควรใช้ไฟรวอลล์แบบนี้ถ้าต้องการการขวางกั้น IP address ที่กำหนดได้อย่างถูกต้องไฟร์วอลล์ระดับเน็ตเวิร์คมีแนวโน้มที่จะทำงานได้เร็วมากและเข้าใจง่ายสำหรับผู้ใช้ และผู้ใช้มักไม่รู้ว่ามีไฟร์วอลล์แบบนี้อยู่ในเครือข่ายของตนด้วยซึ่งก็เป็นสิ่งที่ดีที่ผู้ใช้คอมพิวเตอร์พึงปรารถนา

ข้อเสียของแพ็คเก็ตฟูลเตอร์ริ่ง

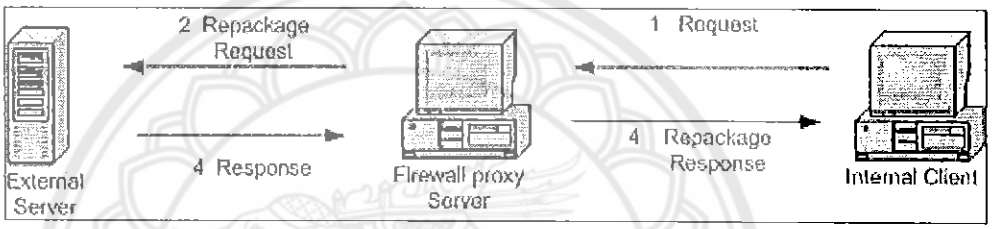
- มีความสามารถน้อยในการจะป้องกันความปลอดภัยให้เครือข่ายเพราะ ไฟร์วอลล์แบบนี้อาจถูกบุกรุกได้ง่าย
- ไม่สามารถตรวจสอบ Packet Filtering Rules ว่ามีประสิทธิภาพแค่ไหน
- ถ้า Filtering Rules มีความซับซ้อนมากก็ยากที่จะจัดการดูแล

เนื่องจากการติดต่อระหว่างเครือข่ายกับอินเทอร์เน็ตเป็นแบบ Direct Access ดังนั้นจึงจำเป็นต้องมี Advanced Authentication measures สำหรับทุก Host ถึงแม้ว่าแพ็คเก็ตฟูลเตอร์ริ่งไฟร์วอลล์จะมีข้อเสียมาก แต่ในความเป็นจริงแล้วจะมีการประยุกต์นำแพ็คเก็ตฟูลเตอร์ริ่งไฟร์วอลล์ไปรวมกับไฟร์วอลล์แบบอื่นๆเพื่อเพิ่งประสิทธิภาพให้กับระบบ ไฟร์วอลล์ให้มากขึ้น

3. พร็อกซีเซิร์ฟเวอร์เกตเวย์ (Proxy-Server Gateway)

พร็อกซีทำงานอยู่ในเลเยอร์ระดับสูง เป็นโปรแกรมแอปพลิเคชั่นที่ ทำงานอยู่ระหว่างสองเครือข่าย โดยจะทำงานในลักษณะของการส่งข้อมูลต่อให้ เมื่อแพ็คเก็ตมาถึง พร็อกซีจะแยกข้อมูลส่วนที่เป็นเฮดเดอร์ของแพ็คเก็ตออก เหลือแต่ส่วนของข้อมูลในส่วนของชั้นแอปพลิเคชั่น เช่น หากเป็นข้อมูลเว็ป พร็อกซีจะแยกเฮดเดอร์ออกเหลือแต่ส่วนโพรโตคอล HTTP จากนั้นก็จะนำเฮดเดอร์มาพิจารณากับกฎต่างๆ ที่กำหนดเอาไว้ หากเป็นไปตามกฎที่ให้ส่งต่อ ก็จะนำข้อมูล HTTP นั้นมาประกอบเป็นแพ็คเก็ตขึ้นมาใหม่ แล้วส่งต่อตามฟังก์ชันการหาเส้นทางจากการที่พร็อกซี เพิ่ม

ความสามารถในการติดตามและควบคุมการผ่านเข้าออกของแพ็คเก็ตระหว่างเครือข่าย คือ เมื่อผู้ใช้ภายในต้องการส่งข้อมูลไปยังเครื่องใดเครื่องหนึ่งในอินเทอร์เน็ต จะต้องส่งผ่านมาให้กับพร็อกซี เมื่อพร็อกซีได้รับและ ตรวจสอบว่าเป็นไปตามกฎแล้ว พร็อกซีจึงจะส่งข้อมูลต่อให้อินเทอร์เน็ตอีกทีหนึ่ง เสมือนกับเป็นการส่งมาจากผู้ใช้ภายในโดยตรง การทำงานแบบนี้ ทำให้การติดต่อระหว่างผู้ใช้ภายในกับภายนอก ไม่ต้องติดต่อก็โดยตรง ผู้ดูแลระบบสามารถมองเห็นเหตุการณ์ที่เกิดขึ้นบริเวณแกตเวย์ แต่พร็อกซีจะต้องรับภาระอย่างหนัก ทำให้ประสิทธิภาพในการติดต่อระหว่างเครือข่ายลดลง ทำงานช้า แต่มีความปลอดภัยมากกว่าเนื่องจากมีการพิจารณาข้อมูลถึงระดับแอปพลิเคชั่นทั้งนี้ไฟร์วอลล์จะส่งต่อได้เฉพาะโพรโตคอลที่ไฟร์วอลล์รู้จักเท่านั้น



รูปที่ 2-14 รูปแบบการทำงานของพร็อกซีเซิร์ฟเวอร์เกตเวย์

(ที่มา: www.thaicert.nectec.or.th/)

พร็อกซีเซิร์ฟเวอร์เกตเวย์แบ่งออกได้เป็น 2 ประเภท

4. เซอร์กิต-เลเวล เกตเวย์ (Circuit – Level Gateway)

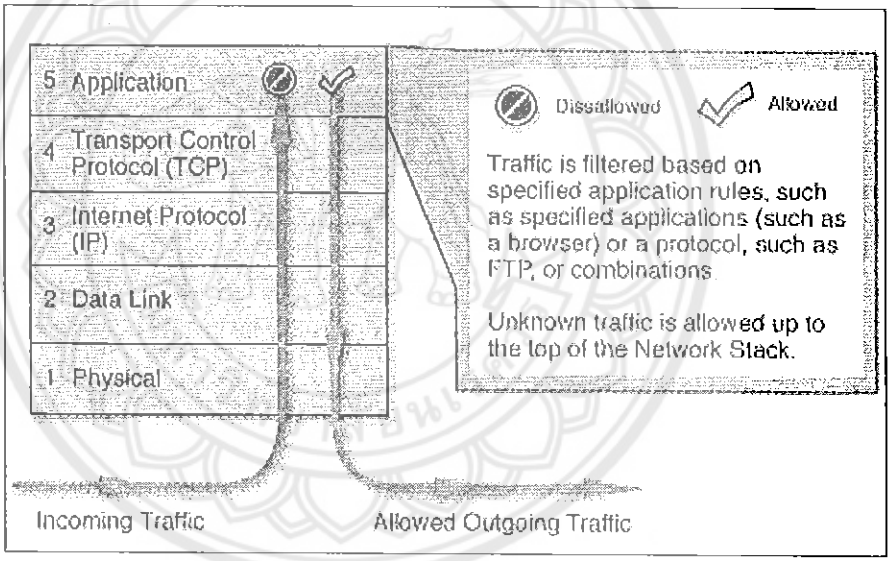
เป็นพร็อกซีที่ ทำการควบคุมการติดต่อกันระหว่างเครือข่ายภายในและภายนอกโดยไม่มีช่องว่างกล่าวคือ จะมีวงจรเสมือน (Virtual Circuit) อยู่ระหว่างโฮสต์ภายในเครือข่ายกับพร็อกซีเซิร์ฟเวอร์ เมื่อมีการร้องขอการติดต่อ (Request) จากเครือข่ายภายใน แพ็คเก็ตจะถูกส่งให้วงจรเสมือน ผ่านไปยังพร็อกซีเซิร์ฟเวอร์ซึ่งจะส่งการร้องขอการติดต่อไปยังอินเทอร์เน็ต หลังจากทำการแปลงหมายเลขไอพีเรียบร้อยแล้ว ในทำนองเดียวกัน การตอบรับ (Response) จากอินเทอร์เน็ต จะถูกส่งมายังพร็อกซีเซิร์ฟเวอร์ผ่านวงจรเสมือน ก่อนส่งกลับให้โฮสต์ต้นทาง โดยในการติดต่อนี้เครือข่ายภายนอกจะไม่สามารถมองเห็นโฮสต์ใดๆ ภายในเครือข่ายได้เลย การติดต่อแบบนี้จะใช้ในกรณีที่ผู้ใช้ภายในเครือข่ายกับอินเทอร์เน็ตไว้ใจได้เท่านั้น

5. แอปพลิเคชั่น-เลเวล เกตเวย์ (Application – Level Gateway)

สำหรับแอปพลิเคชั่นเกตเวย์ นอกจากจะทำงานเช่นเดียวกับวงจรเสมือนแล้ว ยังเพิ่มความสามารถในการตรวจสอบแพ็คเก็ตด้วย ไม่ว่าจะเป็นส่วนของเฮดเดอร์หรือเนื้อหาข้อมูลภายใน

แพ็คเก็ตเพื่อหยุดยั้งการส่งข้อมูลจากภายนอก หากมีข้อมูลจากแฮ็กเกอร์แอบซ่อนอยู่ภายในแพ็คเก็ต นอกจากนี้แอปพลิเคชั่นเกตเวย์ยังสนับสนุนการให้บริการ สำหรับโพรโตคอลแบบต่างๆ คือ เทลเน็ต , เอฟทีพี, เอชทีทีพี และ เอสเอ็มทีพี โดยที่ผู้ดูแลระบบจะต้องทำการติดตั้งในพร็อกซีแยกสำหรับแต่ละการให้บริการ

ไฟร์วอลล์จะทำหน้าที่เป็นตัวแทนของเครื่องลูกข่ายเรียกขอข้อมูลจากเซิร์ฟเวอร์ภายนอกเอง ระบบนี้มีความปลอดภัยค่อนข้างสูง การทำงานข้อมูลจะถูกตรวจสอบที่ระดับ แอปพลิเคชันเลเยอร์ของโอเอสไอโมเดลหรือระดับ แอปพลิเคชันเลเยอร์ของทีซีพีไอพีโมเดลส่วนมากให้ในรูปแบบของพร็อกซี (proxy) ซึ่งเป็นตัวกลางในการรับส่งข้อมูล ซึ่งจะทำให้ช้ากว่าแบบ แพ็คเก็ตฟูลเตอร์ริ่งเกตเวย์แต่มีความปลอดภัยมากกว่า ระบบนี้จะสนับสนุนการบันทึกการติดต่อ และความปลอดภัยของผู้ใช้



รูปที่ 2-15 Application layer gateway path ของ TCP/IP model

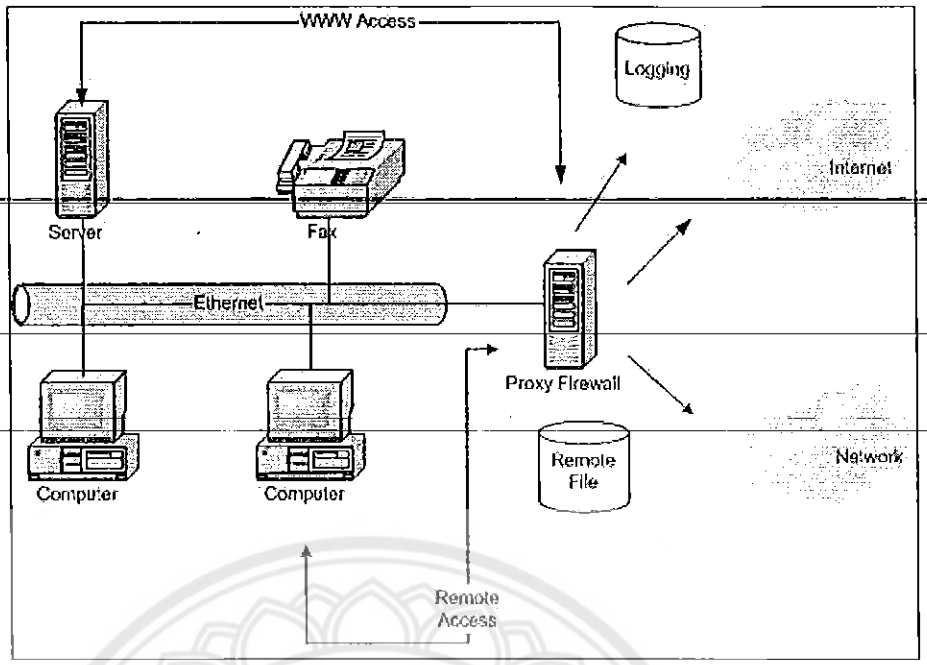
(ที่มา: www.thaicert.nectec.or.th/)

ระบบคอมพิวเตอร์ที่มีโปรแกรมประเภทพร็อกซีทำงานอยู่(โดยปกติมักมีมากกกว่าหนึ่งตัว)พร็อกซีคือโปรแกรมซึ่งทำหน้าที่เป็นตัวแทนดูแลการจราจรที่วิ่งผ่านไปมาระหว่างเครือข่ายที่ได้รับการปกป้องกับเครือข่ายภายนอกพร็อกซีจะเข้าใจเฉพาะโพรโตคอลที่มันถูกออกแบบมาให้ใช้งานได้ด้วยเท่านั้น ตัวอย่างเช่น พร็อกซี สำหรับโพรโตคอลเอฟทีพีก็จะเข้าใจเฉพาะโพรโตคอลเอฟทีพีเท่านั้น การออกแบบให้พร็อกซีเข้าใจโพรโตคอลแบบใดแบบหนึ่งก็เพื่อให้การติดตั้ง การเก็บข้อมูลการทำงานของโพรโตคอลและ การบริหารระบบสามารถกระทำได้สะดวกง่ายดายอีก

ทั้งพร็อกซีลักษณะนี้มักมีประสิทธิภาพดีกว่าพร็อกซีที่เข้าใจหลายๆโพรโตคอลเพราะผู้ออกแบบสามารถเอาจุดเด่นของโพรโตคอลนั้นมาใช้ได้เต็มที่โดยไม่ต้องคำนึงถึงว่าจะเกิดผลกระทบใดๆ

โดยทั่วไปจะเป็นโฮสต์ที่รันพร็อกซีเซิร์ฟเวอร์ที่ไม่ให้อนุญาตให้มีการติดต่อผ่าน ระหว่างเน็ตเวิร์คโดยตรง และทำการบันทึกการติดต่อที่รัดกุมและตรวจสอบการติดต่อสื่อสารที่ผ่านมัน เนื่องจากพร็อกซีแอปพลิเคชั่นเป็นส่วนประกอบที่เป็นซอฟท์แวร์ที่รันบนไฟร์วอลล์มันจะทำงานทางด้านการบันทึกการติดต่อรายละเอียดของการจราจรบนเครือข่ายได้ดีมาก และทำหน้าที่เกี่ยวกับการควบคุมการเข้าใช้ระบบ(access control) นอกจากนี้ยังมีพร็อกซีที่สามารถทำหน้าที่ในการแปลงเลขที่อยู่เครือข่าย (network address translator) กล่าวคือ เมื่อแพ็คเก็ตจะผ่านออกจากเครือข่ายขององค์กรพร็อกซีจะทำการเปลี่ยนค่าเลขที่อยู่ต้นทางของแพ็คเก็ตให้เป็นค่าที่กำหนดไว้ ซึ่งโดยปกติก็คือค่าเลขที่อยู่ของไฟร์วอลล์นั่นเอง เมื่อระบบที่ปลายทางต้องการติดต่อกลับมาที่ต้นทางไฟร์วอลล์ก็จะได้รับแพ็คเก็ตและเมื่อได้ตรวจสอบความปลอดภัยหรือทำการบันทึกรายละเอียดของแพ็คเก็ตแล้วไฟร์วอลล์ก็อาจส่งไฟร์วอลล์ต่อไปให้ระบบคอมพิวเตอร์ปลายทางตัวจริงที่ควรได้รับแพ็คเก็ตนั้นอีกที เนื่องจากการติดต่อเข้ามาทางเดียวและออกไปทางอื่นๆ หลังจากที่ผ่านแอปพลิเคชันที่ทำการป้องกันการเริ่มต้นการติดต่ออย่างมีประสิทธิภาพการเปลี่ยนเลขที่อยู่ต้นทางของแพ็คเก็ตนั้นช่วย ให้ไฟร์วอลล์ทำหน้าที่ป้องกันการรุกรานจากเครือข่ายภายนอกได้ดีขึ้น เพราะผู้บุกรุกไม่สามารถรู้ได้เลยว่าเลขที่อยู่ที่แท้จริงของเครือข่ายและระบบคอมพิวเตอร์คืออะไร การใช้แอปพลิเคชันนี้ในบางกรณี จะมีผลกระทบต่อประสิทธิภาพการทำงานและอาจทำให้ยากต่อการเข้าใจไฟร์วอลล์ระดับแอปพลิเคชันรุ่นแรก ๆ อย่างไฟร์วอลล์ที่ใช้ TIS firewall toolkit เป็นชุดเครื่องมือที่ประกอบด้วยพร็อกซีสำหรับโปรแกรมที่ใช้โพรโตคอลเทลเน็ต, rogin(remote login),เอฟทีพี,เอชทีทีพี(Hypertext Transfer Protocol), X-Windows และ NNTP (Network News Transfer Protocol) ซึ่งผู้ใช้ปลายทาง(end user)จะใช้งานยากและต้องอาศัยการฝึกสอน ส่วนไฟร์วอลล์ระดับแอปพลิเคชันสมัยใหม่จะใช้งานได้ง่ายมากไฟร์วอลล์ประเภทนี้จะให้รายงานการตรวจสอบ ที่ให้รายละเอียดมากกว่าและบังคับใช้การรักษาความปลอดภัยที่เข้มงวดกว่าไฟร์วอลล์ระดับเน็ตเวิร์ค ผู้ดูแลระบบสามารถที่จะเลือกได้ว่าส่วนใดที่ต้องการการเข้ารหัส และส่วนใดไม่มีความจำเป็นที่จะต้องทำเช่นนั้น

นอกจากการใช้พร็อกซีเกตเวย์ แล้วยังสามารถใช้พร็อกซีไฟร์วอลล์ ซึ่งส่วนมากจะเป็นระบบคอมพิวเตอร์เดี่ยวๆ (Isolated Machine) ที่ทำหน้าที่เฉพาะอย่างใดอย่างหนึ่ง โดยจะมีโปรแกรม หรือ ฟังก์ชันต่างๆอยู่น้อยที่สุด ทั้งนี้เพื่อจุดประสงค์ที่ว่าหากมีผู้บุกรุกเข้ามาในระบบก็จะไม่มีทรัพยากรใดๆที่สามารถนำมาใช้ได้ในการทำอันตรายต่อระบบ ระบบ Proxy Firewall นั้นมักจะนำมาใช้ทำหน้าที่อย่างใดอย่างหนึ่งเท่านั้น เช่น ใช้ในการบันทึกการเข้ามาใช้ทรัพยากรต่างๆในระบบ



รูปที่ 2-16 ระบบเครือข่ายที่มีพร็อกซีไฟร์วอลล์

(ที่มา: www.thaicert.nectec.or.th/)

จากรูปจะเห็นได้ว่าในการที่ระบบเครือข่ายย่อยที่มีพร็อกซีไฟร์วอลล์กั้นอยู่นั้น จะสามารถรักษาความปลอดภัยให้กับระบบภายในได้เป็นอย่างดี เพราะว่าในการติดต่อข้อมูลข่าวสารหรือการใช้งานของไฟล์ต่างๆนั้นจะมีพร็อกซีไฟร์วอลล์ทำหน้าที่แทนระบบเครือข่ายแทบทั้งหมดแม้กระทั่งการเข้าสู่ www หรือการทำ Remote Access ก็จะต้องใช้บริการของพร็อกซีไฟร์วอลล์ซึ่งจะทำหน้าที่แทนและเป็นตัวกลางระหว่างระบบเครือข่ายภายในและระบบเครือข่ายภายนอกทั้งหมด

ข้อดีของแอปพลิเคชันเกยเวย์ที่ไม่อนุญาตให้มีการติดต่อโดยตรงระหว่างเครือข่ายกับอินเทอร์เน็ต คือ

- สามารถปิดบังข้อมูลได้ เพราะการติดต่อผ่าน Application Gateway ทำให้ไม่จำเป็นต้องประกาศชื่อของ Site system ภายในเครือข่าย เพราะชื่อ Host ของ Application Gateway เป็นเพียงที่เดียวเท่านั้นที่จำเป็นต้องประกาศให้รู้ในเครือข่ายอินเทอร์เน็ต ซึ่งจะช่วยเพิ่มความปลอดภัยให้กับข้อมูลต่าง ๆ ภายในเครือข่าย
- ตรวจสอบการเข้าสู่เครือข่ายได้อย่างมีประสิทธิภาพ เพราะการติดต่อผ่านApplication Gateway ทำให้เราสามารถตรวจสอบการติดต่อทุกชนิดก่อนที่เข้าถึง Host ภายใน ซึ่งจะเพิ่มประสิทธิภาพในการรักษาความปลอดภัยให้มากขึ้น

- คุ้มค่าในการติดตั้ง เพราะ software หรือ hardware สำหรับการตรวจสอบการเข้าสู่เครือข่ายจำเป็นต้องติดตั้งบน Application Gateway เท่านั้น
- ลดความซับซ้อนของ Filtering rules เนื่องจาก แทนที่ Router จะทำการติดต่อระหว่างเครือข่ายอินเตอร์เน็ตกับ Site ต่าง ๆ ที่กำหนดไว้เฉพาะ ก็จะกำหนดให้ Router กลั่นกรองการติดต่อจากภายนอกโดยอนุญาตให้การติดต่อเข้าสู่เครือข่ายเฉพาะที่กำหนดใน Application Gateway เท่านั้น นอกจากนั้นให้ปฏิเสธการติดต่อ

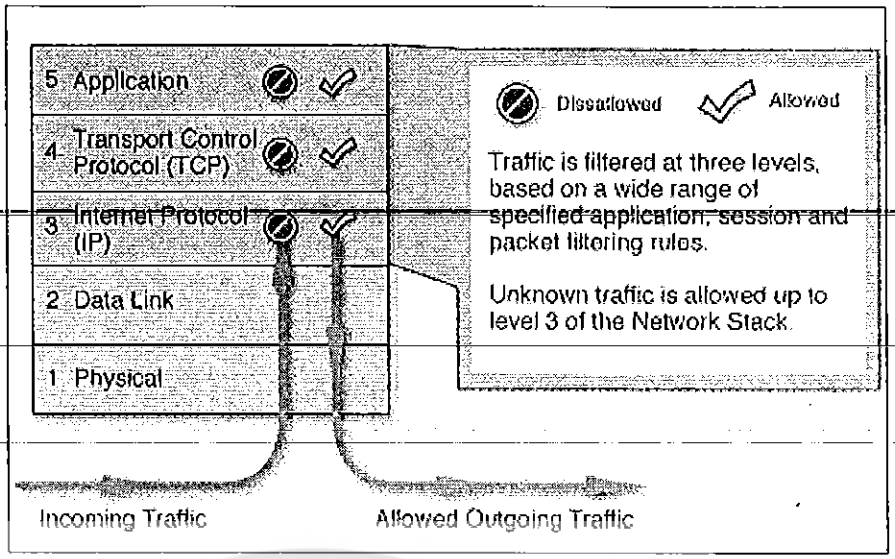
6. สเตทฟูลอินสเป็คชั่นหรือไดนามิกแพ็คเก็ตฟูลเตอร์ริ่ง

เป็นรูปแบบการทำงานแบบใหม่ ซึ่งปรับปรุงมาจากแพ็คเก็ตฟูลเตอร์ริ่งอย่างเดิมซึ่งจะตัดสินใจโดยดูข้อมูลในส่วนของเฮดเดอร์เท่านั้น และจะพิจารณาเฉพาะแพ็คเก็ตนั้นๆ โดยไม่ได้คำนึงถึงแพ็คเก็ตก่อนหน้านี้ส่วนสเตทฟูลอินสเป็คชั่นจะเอาข้อจำกัดนี้ ทั้งในส่วนของข้อมูลที่ใช้ในการตัดสินใจ โดยจะดูถึงข้อมูลในส่วนของ Payload ด้วย และจะคำนึงถึงส่วนของแพ็คเก็ตอื่นๆ ที่อยู่ก่อนหน้านี้ประกอบในการตัดสินใจ ทำให้ความสามารถในการตัดสินใจมากขึ้น เพราะรู้ข้อมูลมากขึ้น โดยเพิ่มตารางเก็บสถานะ เช่น เมื่อส่งข้อมูลให้อินเทอร์เน็ต ตารางสถานะจะเก็บหมายเลขพอร์ตต้นทาง หมายเลขพอร์ตปลายทาง การเก็บนี้เรียกว่า "Saving the state" เมื่อมีแพ็คเก็ตที่เป็นการตอบรับ ก็จะนำแพ็คเก็ตที่รับมานั้น เปรียบเทียบกับ "Saved state" ข้อมูลตรงกันที่เก็บไว้ว่ามี

การทำงานของสเตทฟูลอินสเป็คชั่น จะมีการติดตามสถานะ(State) การทำงานของการเชื่อมต่อแบบ ทีซีพี ซึ่งเป็นผลให้สามารถดูรูปแบบการทำงานได้ทั้งกระบวนการ ไม่ได้ดูเพียงข้อมูลในแต่ละแพ็คเก็ต โดยสามารถดูลักษณะการเชื่อมต่อ การโต้ตอบของแต่ละโพรโตคอลที่มีลักษณะที่แตกต่างกันโดยสามารถแยกแยะโพรโตคอลที่ถูกต้องกับโพรโตคอลที่ไม่ถูกต้องออกจากกันได้ นอกจากนี้สเตทฟูลอินสเป็คชั่นยังมีความปลอดภัยมากกว่าเพราะสามารถจะปิดพอร์ตที่มีหมายเลขมากกว่า 1,024 ได้เนื่องจากการเชื่อมต่อแบบ ทีซีพี อย่างเช่นเว็บนั้น แม้เมื่อเริ่มแรกจะติดต่อกันโดยผ่านพอร์ต 80 แต่หลังจากที่ติดต่อกันแล้ว จะมีการใช้หมายเลขพอร์ตแบบสุ่ม โดยมีหมายเลขมากกว่า 1,024 ซึ่งทำให้ไฟร์วอลล์แบบแพ็คเก็ตฟูลเตอร์ริ่งจำเป็นต้องเปิดพอร์ตที่มีหมายเลขมากกว่า 1,024 ไว้ตลอดเวลา แต่สเตทฟูลจะเปิดพอร์ตเฉพาะเวลาที่มีการเชื่อมต่อผ่านพอร์ตนั้นๆ เท่านั้น หากแพ็คเก็ตถูกตรวจสอบแล้วว่าไม่เป็นไปตามกฎก็จะปิดพอร์ตนั้นทันที สำหรับข้อจำกัดของสเตทฟูลอินสเป็คชั่น คือ ไม่รู้จักการทำงานในระดับแอปพลิเคชั่น และยังคงเป็นการติดต่อระหว่างผู้ใช้ภายในกับภายนอกโดยตรงดังนั้นไฟร์วอลล์ที่ดี จึงมักจะนำวิธีการหลายๆวิธีเข้ามาใช้ด้วยกัน เช่น ใช้พร็อกซีเซิร์ฟเวอร์และและสเตทฟูลอินสเป็คชั่นทำงานร่วมกัน

	Packet Filter	Stateful Inspection	พร็อกซีเซิร์ฟเวอร์ Gateways
ข้อดี	• ประสิทธิภาพดี • ง่ายในการ implement • ไม่ขึ้นกับแอปพลิเคชั่ น (Application Independent)	• ประสิทธิภาพดี • เปิดพอร์ตเฉพาะเมื่อมีการติดต่อ • สนับสนุนเกือบทุกบริการ	• ไม่เปิดเผยหมายเลขไอพีภายใน • พิจารณาเนื้อหาของข้อมูลด้วย • มี User Authentication • เก็บรายละเอียด log ได้มาก
ข้อเสีย	• เปิดเผยหมายเลขไอพีภายใน • มี การเปิดช่องว่างทิ้งไว้ถาวร • No User Authentication • ใช้การเชื่อมต่อโดยตรงกับภายนอก	• No User Authentication • ใช้การเชื่อต่อโดยตรงกับภายนอก • เปิดเผยหมายเลขไอพีภายใน	• ประสิทธิภาพต่ำกว่า • ต้องมีพร็อกซี สำหรับทุกๆแอปพลิเคชั่นที่ใช้ • ไม่มี การป้องกันในระดับชั้นที่ต่ำกว่าชั้นแอปพลิเคชั่น • เปิดเผยระบบปฏิบัติการ

ตารางที่ 2-1 เปรียบเทียบรูปแบบการทำงานของไฟร์วอลทั้ง 3 ประเภท



รูปที่ 2-17 Stateful Inspection path ของ TCP/IP model

(ที่มา: www.thaicert.nectec.or.th/)

การทำงานในรูปแบบของ packet OSI model จะทำงานในระดับ network layer แล้ว INSPECT Engine จะเข้าไปทำงานต่อโดยจะทำการตรวจสอบวิเคราะห์ พิจารณาข้อมูลรายละเอียด เช่น port number ,source ,destination address เป็นต้น จาก ทุกๆ application layer ของแต่ละ packet และจะนำข้อมูลเหล่านี้ไปเก็บไว้ใน dynamic state tables เพื่อใช้สำหรับการเปรียบเทียบในการคอนเน็กกลับเข้ามา และเมื่อมี การตอบรับกลับมาของ packet ข้อมูลที่ก็ถูกนำไปเปรียบเทียบกับข้อมูลรายละเอียดที่เก็บไว้อยู่แล้วใน Dynamic State Table ว่าตรงกันหรือไม่ถ้าตรงก็จะยอมให้ผ่านเข้าไป ถ้าไม่ตรงก็จะไม่ยอมรับ

การทำงานในรูปแบบของ TCP/IP model เมื่อ packet ถูกส่งเข้ามา จะถูกตรวจสอบในระดับชั้น Internet Protocol (IP) ถ้าถูกต้อง ก็จะถูกส่งผ่านเข้าไปในระดับชั้น Transport Control Protocol (TCP) และถ้าการตรวจสอบข้อมูลถูกต้อง ก็จะส่งผ่านเข้าไปในระดับชั้น Application และสามารถส่งต่อเข้าไปในระบบได้ แต่ถ้า packet ถูกตรวจสอบว่าข้อมูลนั้นไม่ถูกต้องในแต่ละระดับชั้นก็จะถูกส่งกลับมาออกทันที โดยไม่ต้องมีการตรวจสอบในชั้นอื่นอีกต่อไป

เมื่อการคอนเน็กในแต่ละครั้งนั้นจบลง ก็จะปิดการใช้งานเซอร์วิซนั้นด้วย เนื่องจากมันอาจจะเป็นช่องทางที่เปิดให้ผู้บุกรุกเข้าโจมตีได้ Firewall แบบนี้จะให้ประสิทธิภาพในการทำงานที่สูง มีความปลอดภัยสูงกว่า 2 แบบ

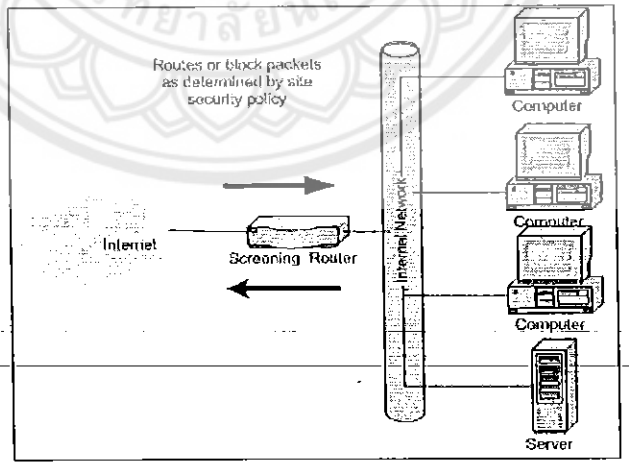
2.11 สถาปัตยกรรมของไฟร์วอลล์

ซิงเกิลบ็อกซ์ (Single Box)

1. สกรีนนิ่ง เราเตอร์ (Screening Router)

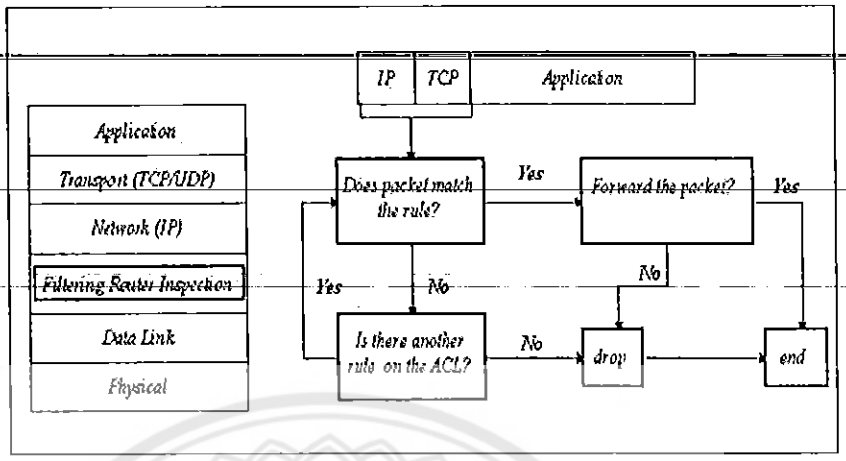
สกรีนนิ่งเราเตอร์ คือ อุปกรณ์ที่ใช้ในการตรวจสอบว่า ข้อมูลในรูป Data Packets นั้นจะถูกส่งไปที่ใดและมาจากไหน และได้รับอนุญาตอย่างถูกต้องหรือไม่ตัวสกรีนนิ่งเราเตอร์ จะมีข้อมูลที่เรียกว่า Routing Table เพื่อเอาไว้ตรวจสอบข้อมูลที่ถูกส่งผ่านทั้งเข้ามาในระบบเครือข่ายและออกไปจากระบบเครือข่าย การตรวจสอบนั้นสามารถทำได้โดยการตรวจดู Address ที่ Headers ของข้อมูลที่ในรูป Packet Data แล้วเปรียบเทียบกับข้อมูล Address ที่มีอยู่ก่อนแล้วใน Routing Table

สกรีนนิ่งเราเตอร์เป็นส่วนประกอบพื้นฐาน ในไฟร์วอลล์เกือบทุกประเภท สกรีนนิ่งเราเตอร์คือ commercial router ที่ใช้กันอยู่ หรือเป็นเพียง host-based router ที่มีความสามารถในการกรองข้อมูลก็ได้ ใช้งานง่าย และได้รับความนิยมมากที่สุด เพราะว่าเราเตอร์โดยส่วนใหญ่ที่ใช้กันอยู่ในปัจจุบันนี้จะมีความสามารถในการดัก Traffic ระหว่างจุดปลายทางหรือระหว่างเน็ตเวิร์กได้อยู่แล้วสกรีนนิ่งเราเตอร์ทำงานใน Network level และจะใส่ข้อมูลว่าให้ผ่านหรือไม่ไปในเฮดเดอร์ของ ทีซีพีไอทีเพ็ตเกตไฟร์วอลล์ ในลักษณะนี้ รวดเร็วที่สุด มีความยืดหยุ่นมาก และราคาก็ค่อนข้างถูก แต่ยังขาดความสามารถที่จะให้รายละเอียดของข้อมูลที่ปล่อยผ่านไปอยู่ วิธีนี้จึงไม่มั่นคง และง่ายสำหรับผู้โจมตีแต่ทั้งนั้นก็ขึ้นกับซอร์ฟแวร์ที่ติดตั้งไว้ที่เซิร์ฟเวอร์ด้วยว่ามีระบบรักษาความปลอดภัยที่ดีเพียงใด และผู้เชี่ยวชาญหลายท่าน มักจะไม่ใช้วิธีนี้ อย่างเดียวในการป้องกันระบบ แต่บางแห่งก็อาจมีเพียงแคสกรีนนิ่งเราเตอร์ที่กั้นระหว่างเน็ตเวิร์กภายในกับภายนอกอินเตอร์เน็ต



รูปที่ 2-18 สกรีนนิ่ง เราเตอร์

(ที่มา: www.thaicert.nectec.or.th/)



รูปที่ 2-19 Filtering Routers or Screening Router

(ที่มา: www.firewall.com/)

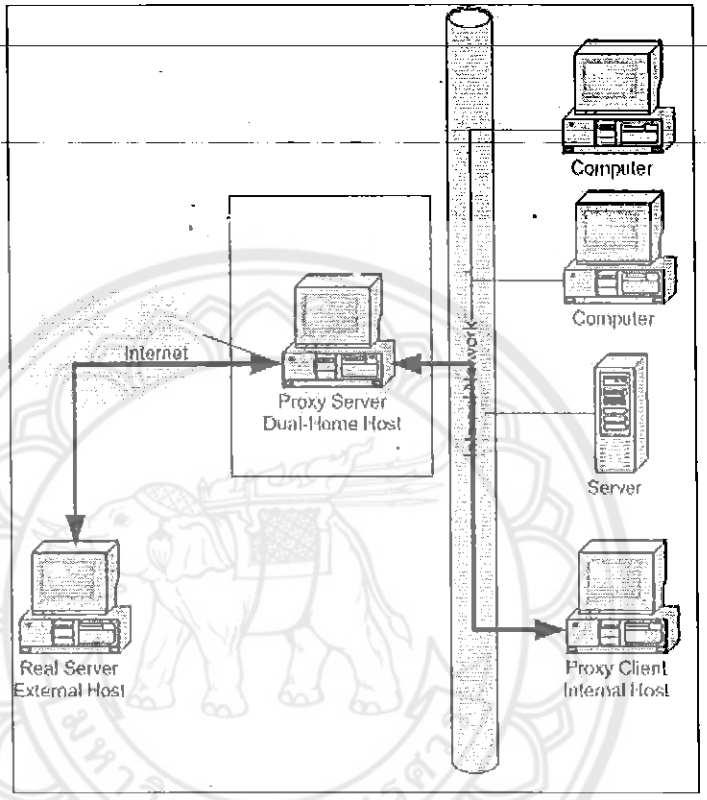
2. ดูอัล – โฮม โฮสต์ (Dual-Home Host)

ไฟร์วอลล์ระดับแอปพลิเคชั่นที่เรียกว่าดูอัล-โฮมโฮสต์เป็นโฮสต์ที่รันพร็อกซีซอฟท์แวร์ที่มีการรักษาความปลอดภัยที่สูงมาก มีสอง Network interface ซึ่งแต่ละอันก็จะอยู่อีกเน็ตเวิร์ค หนึ่งและขวางกั้นการติดต่อสื่อสารที่ผ่านมันทั้งหมด

ดูอัล-โฮมโฮสต์เป็น การ implement firewall อีกรูปแบบหนึ่งที่ได้รับความนิยมใช้กันมาก มันจะทำตัวเสมือนเป็น complete block ระหว่าง internet กับเน็ตเวิร์คภายใน โดยไม่ใช้การติดต่อแบบทีซีพีไอพี ผู้ดูแลระบบสามารถกำหนดได้ว่าจะให้มีการเข้าระบบได้อย่างไร ทั้งโดยกำหนดที่แอปพลิเคชั่นซึ่งการดักแบบนี้เป็นแบบ "อะไรที่ไม่ได้อนุญาต ถือว่าห้ามผ่าน" ซึ่งทำให้ผู้ใช้สามารถติดต่ออินเตอร์เน็ตได้เฉพาะ แอปพลิเคชั่นที่อนุญาต เท่านั้น หรือ การให้ user login เข้าระบบ ซึ่งวิธีนี้จะทำให้ผ้โจมตีผู้ที่สามารถเจาะรหัสของผู้ใช้คนใดคนหนึ่ง ที่ตั้ง password ไว้ไม่ดีสามารถเจาะเข้าสู่ระบบทั้งหมดได้ และส่วนที่อันตรายที่สุดก็คือส่วนที่เป็นโฮสต์เนื่องจากเป็นส่วนที่ติดต่อกับอินเตอร์เน็ตโดยตรง แต่ผู้ดูแลระบบก็ยังสามารถที่จะตรวจดูได้ว่าผู้ใช้คนใดที่ทำให้เกิดความเสียหาย และทำอะไรไว้บ้าง

แต่ถ้ามีการกำหนดดูอัล-โฮมโฮสต์ไม่ให้มีการติดต่อโดยตรงของผู้ใช้ จะทำให้การควบคุมทำได้ง่ายขึ้น นอกจากนั้นซอร์ฟแวร์ระบบ ที่นำมาใช้กับดูอัล-โฮมโฮสต์มีข้อดีตรงที่ง่ายในการปรับเปลี่ยนการเก็บ log รวมทั้ง keep track การใช้ แอปพลิเคชั่นใดๆของ ผู้ใช้ที่ telnet login เข้ามา การเจาะทะลุเข้า ดูอัล-โฮมโฮสต์จะทำให้สามารถทำโอเปอร์เรชั่นได้เกือบทั้งหมด

จุดอ่อนที่สำคัญที่สุดของ ดูอัล-โฮมโฮสต์คือ เมื่อความล้มเหลวของระบบเกิดขึ้น ทำให้ระบบทั้งหมดเปิด ซึ่งทำให้ค่าตัวแปรบางอย่างที่สำคัญต่อความปลอดภัยของระบบถูกแก้ได้ สำหรับระบบ UNIX-based dual homed gateway โดยทั่วไป รวมทั้ง TCP/IP routing จะถูกทำให้ใช้การไม่ได้โดยการแก้ตัวแปรใน kernel ของมันที่ชื่อว่า ip forwarding



รูปที่ 2-20 ดูอัล-โฮม โฮสต์

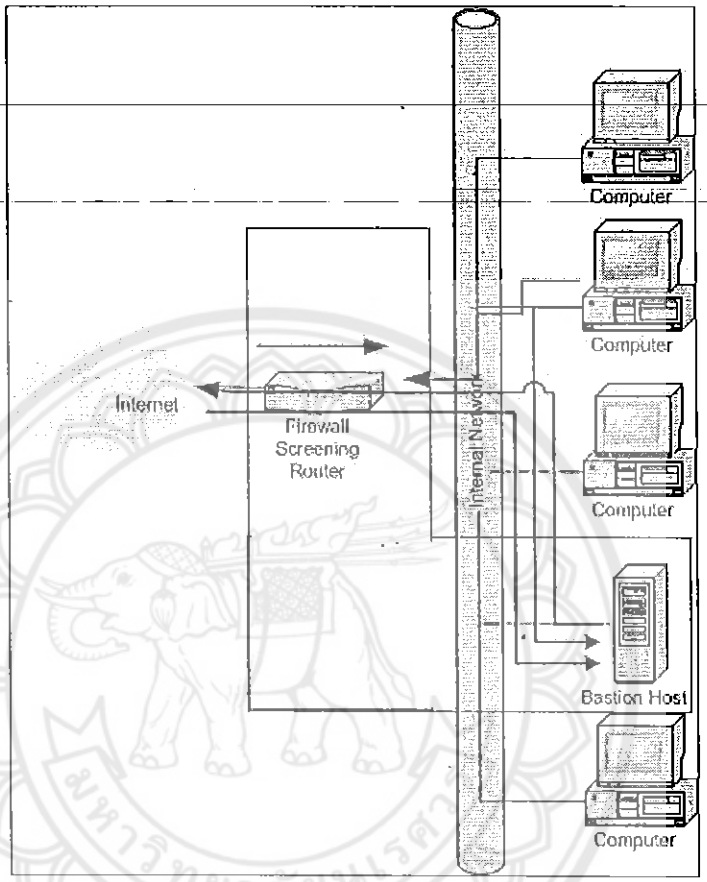
(ที่มา: www.thaicert.nectec.or.th/)

มัลติเพิล-เพอโพส บ็อกซ

3. สกรีนนิ่งโฮสต์ อาร์คิเทคเจอร์ (Screening Host Architecture)

ประกอบไปด้วยไฟร์วอลล์ประเภทแพ็คเก็ตฟูลเตอร์ริ่งและเบสชันโฮสต์(Bastion Host) โดยเบสชันโฮสต์เป็นคอมพิวเตอร์พิเศษ ที่อนุญาตให้มีการเชื่อมต่อกับเครือข่ายภายนอก ซึ่งจะทำหน้าที่เป็นพร็อกซีที่จะส่งแพ็คเก็ตต่อไปยังเครื่องอื่นๆในเครือข่าย ดังนั้นหากมีการบริการใดๆในระบบ เบสชันโฮสต์จะต้องรู้จักโพรโตคอลนั้นๆ เบสชันโฮสต์จะต้องมีการพิสูจน์สิทธิ์ (Authentication) ที่เหมาะสม โดยในการเริ่มใช้งาน แพ็คเก็ตจะถูกฟูลเตอร์โดยแพ็คเก็ตฟูลเตอร์ริ่งเราเตอร์ก่อนตามกฎที่กำหนดว่าควรจะอนุญาตหรือไม่หากอนุญาตจะต้องขอพิสูจน์ สิทธิ์กับเบสชันโฮสต์ แล้วให้เบสชันโฮสต์เป็นตัวกลางจัดการเชื่อมต่ออีกครั้งหนึ่ง ข้อเสียของโครงสร้างแบบนี้

ขึ้นอยู่กับการทำงานของฟูลเตอร์ริ่งเราเตอร์ หากมีการทำงานผิดพลาด เบสชันโฮสต์ จะให้บริการทุกการเชื่อมต่อ ส่งผลให้ เครือข่ายภายในถูกโจมตีได้ จึงไม่ควรให้บริการที่มีความเสี่ยงสูง เช่น เว็บเซิร์ฟเวอร์

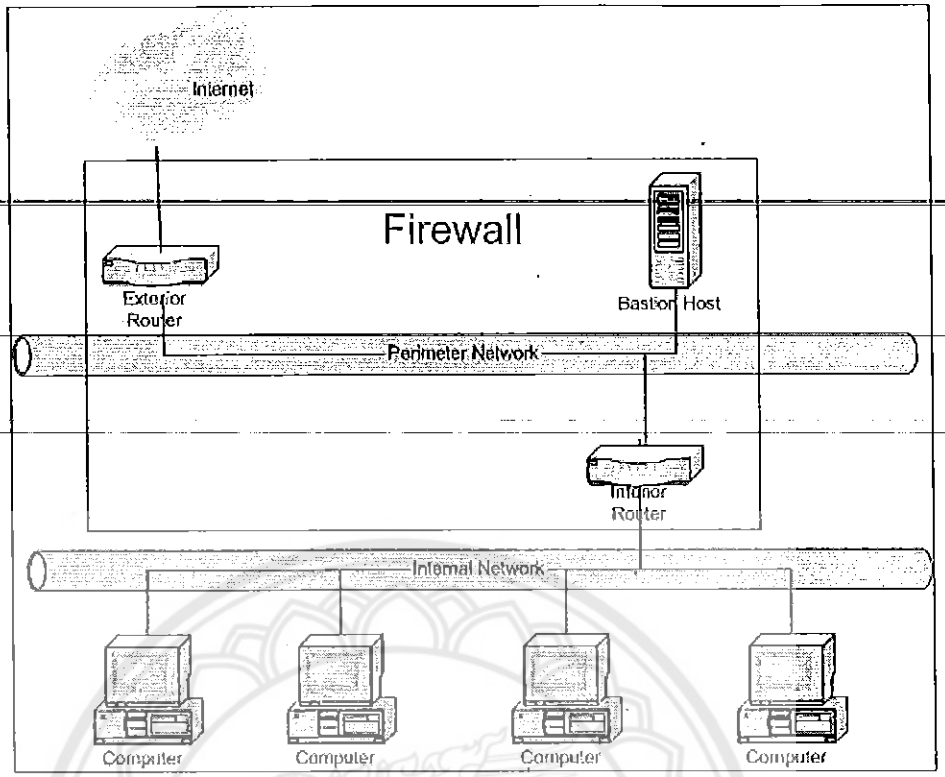


รูปที่ 2-21 สกรีนนิ่งโฮสต์ อาร์คิเทคเจอร์

(ที่มา: www.thaicert.nectec.or.th/)

4. สกรีนสับเน็ตอาร์คิเทคเจอร์ (Screened Subnet Architecture)

ต่างจากสถาปัตยกรรมสกรีนนิ่งโฮสต์ ตรงที่ส่วนของเบสชันโฮสต์จะมีการแบ่งเครือข่ายภายในออกจากเครือข่ายที่ให้บริการซึ่งให้ความปลอดภัยมากกว่า ในกรณีนี้จะมีไฟร์วอลล์ถึงสองตัว คือ เราเตอร์ภายนอกและเราเตอร์ภายใน เราเตอร์ภายในจะทำหน้าที่ป้องกันไม่ให้เครือข่ายภายในถูกโจมตี เมื่อภายนอกถูกเจาะทะลนอกจากนั้นยังป้องกันไม่ให้โจมตีจากเครือข่ายภายในได้อีกด้วย นั่นคือภายในจะกรองทั้งแพ็คเก็ตที่มาจากอินเทอร์เน็ตและเบสชันโฮสต์ นอกจากนี้ยังมีการเพิ่มชั้นของเพอริมิเตอร์ขึ้นอีกระหว่างเราเตอร์ภายนอกและภายใน เพื่อป้องกันผู้ประสงค์ร้ายไม่ให้เข้าถึงเครือข่ายภายใน



รูปที่ 2-22 สกรีนสับเน็ตอาร์คิเทคเจอร์

(ที่มา: www.thaicert.nectec.or.th/)

นอกจากนี้ยังมีเครือข่าย DMZ (De-militarize zone) คือการวางโฮสต์ที่ไม่น่าเชื่อถือหรือมีความปลอดภัยต่ำ (Untrusted Host) ไว้ภายในไฟร์วอลล์ แต่อยู่นอกเครือข่ายภายใน ซึ่งการทำเช่นนี้ไฟร์วอลล์จะทำการเชื่อมต่อกับสามเครือข่ายและการทำเช่นนี้เป็นการเพิ่มประสิทธิภาพ ความปลอดภัยความน่าเชื่อถือและความสามารถในการนำโฮสต์ที่ไม่น่าเชื่อถือ แต่ไม่ได้เพิ่มระดับของความปลอดภัยในการเข้าถึงจากโฮสต์ที่อยู่ในเครือข่ายภายใน โฮสต์ที่ไม่น่าเชื่อถือมีจุดประสงค์ต่างๆกัน เช่น FTP Server และเว็บไซต์สาธารณะ จะถูกนำมาไว้ในเครือข่าย DMZ เป็นการสร้างเครือข่ายบริการสาธารณะ

2.12 พื้นฐานสำหรับการบุกรุกระบบคอมพิวเตอร์

สคริปต์ซีจีไอ(CGI Script) การใช้งานสคริปต์ซีจีไอไม่ปลอดภัย เนื่องจากผู้บุกรุกสามารถสอดแทรกโปรแกรมแปลกปลอมผ่านเข้าไปกับฟิลด์ที่รับอินพุตให้ทำงานจากเชลล์ได้ซึ่งโปรแกรมแปลกปลอมนั้นสามารถซ่อนไว้โดยการกำหนดตัวแปรแทนได้ช่องโหว่ที่เป็นที่รู้จักกันดีตัวหนึ่งคือ phf ซึ่งเป็นไลบรารีที่มากับ httpd ของ NCSA

การบุกรุกผ่านทางเว็บเซิร์ฟเวอร์ เว็บเซิร์ฟเวอร์หลายตัวที่สามารถเขียนตัวเองได้ เช่น IIS มีจุดบกพร่องในการระบุชื่อของไฟล์สามารถเรียกได้โดยใช้ "../" (เป็นการย้อนกลับไปในไดเรกทอรีนอกหนึ่งชั้น) ทำให้สามารถเข้าไปเรียกใช้ได้ทุกไดเรกทอรีในระบบไฟล์ช่องทางการบุกรุกอื่นๆ เช่นใช้บัฟเฟอร์โอเวอร์โฟลว์

การบุกรุกผ่านทางโดเมนเนมเซิร์ฟเวอร์(DNS) ช่องโหว่เกิดจากโดเมนเนมเซิร์ฟเวอร์(Domain Name Server) มีการทำงานแบบรีเคอร์ซีฟ(Recursive) โดยส่งคำถามไปยังโดเมนเนมเซิร์ฟเวอร์ที่อยู่ในลำดับขั้นที่สูงขึ้นไปผู้บุกรุกอาจส่งคำร้องขอเข้าไปยังโดเมนเนมเซิร์ฟเวอร์ตัวแรก ซึ่งโดเมนเนมเซิร์ฟเวอร์ตัวนั้นจะส่งคำถามขึ้นไปยังโดเมนเนมเซิร์ฟเวอร์ในลำดับสูงขึ้นถัดไปผู้บุกรุกสามารถปลอมที่อยู่ทางอินเตอร์เน็ตให้เป็นโดเมนเนมเซิร์ฟเวอร์ที่ตอบสนองตัวแรกและส่งคำตอบผิดๆ กลับมาทำให้โปรแกรมที่เป็นผู้ถามในลำดับแรกได้รับคำตอบที่ผิดๆ ไปซึ่งอาจเกิดการติดต่อไปยังเครื่องที่ผู้บุกรุกจัดเตรียมไว้ก่อนแล้วได้

Remote Procedure Call (RPC) RPC อนุญาตให้สามารถรันโปรแกรมบนเครื่องคอมพิวเตอร์เครื่องอื่นได้เป็นอันตรายอย่างยิ่งเมื่อผู้บุกรุกเข้ามารันโปรแกรมที่เครื่องเป้าหมาย เช่น ลงโปรแกรม Back door เอาไว้เพื่อเป็นช่องทางในการเข้าไปยังเครื่องเป้าหมายอีกครั้ง ซึ่ง RPC ในเวอร์ชันเก่าๆ จะมีการกำหนดสิทธิ์เป็น full control

การบุกรุกผ่านโพรโตคอล SMTP (Send mail) Sendmail เป็นโปรแกรมที่ใช้กันอย่างแพร่หลายและซับซ้อนโปรแกรมหนึ่งซึ่งมีข้อบกพร่องอยู่มาก ในประวัติศาสตร์มีผู้บุกรุกพบบักที่เกิดจากการใช้คำสั่ง DEBUG หรือฟีเจอร์ WIZ ที่ซ่อนไว้เป็นตัวช่วยเจาะระบบผ่านทาง SMTP

Sadmind และ mountd Sadmind ถูกใช้งานอยู่ในระบบ SUN Solaris อนุญาตให้ผู้ดูแลระบบสามารถทำการควบคุมเครื่องเซิร์ฟเวอร์จากระยะไกลได้ส่วน mountd มีการอนุญาตให้มีการแชร์ไฟล์ระหว่างเครือข่าย ซึ่งเป็นช่องทางให้ผู้บุกรุกสามารถลงโปรแกรม เช่น DDOS (Distributed Denial Of Service) เพื่อโจมตีเครื่องเป้าหมายเครื่องอื่นได้

การเปิดแชร์ไฟล์ เครื่องคอมพิวเตอร์ที่มีการเปิดแชร์ไฟล์เอาไว้เช่นในNetworkneighborhood (Windows),Appleshare (Macintosh) และ NFS(Unix) อาจเป็นช่องทางให้ผู้บุกรุกเข้าไปเอาข้อมูลที่สำคัญออกมา เช่น อีเมล์ เอกสารสำคัญที่เก็บเอาไว้ในเครื่องคอมพิวเตอร์หรือได้ Account และรหัสผ่านสำหรับล็อกอินไปยังเซิร์ฟเวอร์อื่นได้Account ที่ไม่มีรหัสผ่าน หรือรหัสผ่านที่ง่ายต่อการเดาเมื่อผู้บุกรุกทราบว่ามี Username นั้นอยู่จริงๆ ภายในระบบ จะทำการเชื่อมต่อไปยังเครื่องคอมพิวเตอร์ หรือเซิร์ฟเวอร์เป้าหมายโดยทำการล็อกอินด้วย Usernameนั้น และทำการเดารหัสผ่าน หรือในบางครั้ง ระบบจะไม่มีการถามรหัสผ่าน สามารถเข้าไปในระบบได้เลย นับว่าเป็นอันตรายอย่างยิ่ง

IMAP และ **POP** เป็นโพรโตคอลที่อนุญาตให้ผู้ใช้งานไม่ว่าจะอยู่ที่ไหนก็ตามสามารถเข้ามาอ่านอีเมล์จากเมล์เซิร์ฟเวอร์ได้เป็นช่องทางให้ผู้บุกรุกสามารถผ่านเข้าไปถึงเมล์เซิร์ฟเวอร์ในระบบโดยไม่ถูกกันจากไฟร์วอลล์

Simple Network Management Protocol (SNMP) อุปกรณ์จำพวกเราเตอร์ สวิตช์ ฮับ หรืออุปกรณ์ที่เปิดให้มีควบคุม และบริหารในเครือข่ายระยะใกล้ และไกลได้มักจะมีการตั้งค่ารหัสผ่านของผู้ดูแลระบบ เป็นค่าเดิมจากโรงงานที่ผลิตนับเป็นช่องทางให้ผู้บุกรุกเข้ามาควบคุมระบบเครือข่ายขององค์กรได้

2.13 การสำรวจระบบและรวบรวมข้อมูลเพื่อการโจมตีของผู้บุกรุก

Ping sweeps การส่งคำสั่ง ping ไปยังเครื่องแบบสุ่มเพื่อค้นหาว่ามีเครื่องใดเปิดให้บริการอยู่ค้นหาตำแหน่ง โฮสต์ที่ต้องการและตรวจสอบการเข้าถึงได้การกระทำในทำนองนี้อาจใช้โพรโตคอลอื่นๆ เช่น SNMP sweep สามารถนำมาใช้เพื่อตรวจสอบดูตารางการจัดเส้นทาง (routing table) ของเราเตอร์ที่ไม่รักษาความปลอดภัยเพื่อเรียนรู้รายละเอียดเกี่ยวกับโทโปโลยี (Topology) ของเครือข่ายขององค์กรเป้าหมาย

TCP scan การเข้าไปตรวจดูพอร์ตทีซีพีว่ามีช่องทางใดที่เปิดให้บริการอยู่และเป็นช่องที่ผู้บุกรุกสามารถใช้เจาะระบบเข้าไปได้รูปแบบในการสแกนพอร์ตต่างๆ เป็นไปได้ทั้งการสแกนพอร์ตแบบต่อเนื่อง (เรียงตามหมายเลขพอร์ตที่เป็นไปได้) แบบสุ่มและแบบกำหนดหมายเลขพอร์ตที่ต้องการสแกนไว้ล่วงหน้า

OS identification กระทำโดยการส่งแพ็กเก็ตไอซีเอ็มพี (ICMP) หรือทีซีพี (TCP) ไปยังเครื่องเป้าหมายทำให้ผู้บุกรุกทราบชนิด และเวอร์ชันของระบบปฏิบัติการและชนิดของเครื่อง

TraceRoute โปรแกรม TraceRoute สามารถเปิดเผยหมายเลขเครือข่ายและเราเตอร์ในเส้นทางไปสู่โฮสต์ที่ระบุ

Finger โพรโตคอล Finger สามารถเปิดเผยข้อมูลในรายละเอียดเกี่ยวกับผู้ใช้ (ชื่อล็อกอิน หมายเลขโทรศัพท์เวลาที่ล็อกอินครั้งสุดท้าย เป็นต้น) ของโฮสต์ที่ระบุได้

DNS Server เซิร์ฟเวอร์ดีเอ็นเอสสามารถเข้าถึงรายการไอพีแอดเดรสของโฮสต์และชื่อโฮสต์ที่ตรงกันได้

Whois โพรโตคอล Whois เป็นบริการข้อมูลชนิดหนึ่งที่สามารถให้ข้อมูลเกี่ยวกับโดเมน DNS ทั้งหมดและผู้ดูแลระบบที่รับผิดชอบแต่ละโดเมน อย่างไรก็ตาม ข้อมูลนี้มักจะล่าสมัย

SYN Flood เป็นการโจมตีโดยการส่งแพ็คเก็ต TCP ที่ตั้งค่า SYN บิตไว้ไปยังเป้าหมาย เสมือนกับการเริ่มต้นร้องขอการติดต่อแบบ TCP ตามปกติ (ผู้โจมตีสามารถปลอมไอพีของ source address ได้) เครื่องที่เป็นเป้าหมายก็จะตอบสนองโดยการส่ง SYN-ACK กลับมายัง source ip address ที่ระบุไว้ ซึ่งผู้โจมตีจะควบคุมเครื่องที่ถูกระบุใน source ip address ไม่ให้ส่งข้อมูลตอบกลับ ทำให้เกิด

สภาวะ half-open ขึ้นที่เครื่องเป้าหมาย หากมีการส่ง SYN flood จำนวนมาก ก็จะทำให้คิวของการให้บริการของเครื่องเป้าหมายเต็ม ทำให้ไม่สามารถให้บริการตามปกติได้ นอกจากนี้ SYN flood ที่ส่งไปจำนวนมาก ยังอาจจะทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่อีกด้วย

ICMP Flood เป็นการส่งแพ็คเก็ต ICMP จำนวนมากไปยังเป้าหมาย ทำให้เกิดการใช้งานแบนด์วิดธ์เต็มที่

UDP Flood เป็นการส่งแพ็คเก็ต UDP จำนวนมากไปยังเป้าหมาย ซึ่งทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่และ/หรือทำให้ทรัพยากรของเป้าหมายถูกใช้ไปจนหมด โดยจะส่ง UDP packet ไปยัง port ที่กำหนดไว้ เช่น 53 (DNS)

Smurf ผู้โจมตีจะส่ง ICMP Echo Request ไปยัง broadcast address ในเครือข่ายที่เป็นตัวกลาง (ปกติจะเรียกว่า amplifier) โดยปลอม source ip address เป็น ip address ของระบบที่ต้องการโจมตี ซึ่งจะทำให้เครือข่ายที่เป็นตัวกลางส่ง ICMP Echo Reply กลับไปยัง ip address ของเป้าหมายทันที ซึ่งทำให้มีการใช้งานแบนด์วิดธ์อย่างเต็มที่

Fraggle เป็นอีกรูปแบบหนึ่งของการโจมตีแบบ Smurf โดยผู้โจมตีจะส่ง UDP Echo Request (UDP port 7) ไปยัง broadcast address ของ amplifier network โดยปลอม source ip address ไปเป็น ip address ของเป้าหมาย ซึ่งทำให้มีการใช้งานแบนด์วิดธ์อย่างเต็มที่ และ/หรือทำให้มีการใช้ทรัพยากรของเป้าหมายจนหมดไป ซึ่งการโจมตียังสามารถใช้ได้กับ UDP, TCP services อื่น เช่น Chargen อีกด้วย

2.14 ศึกษารูปแบบ การโจมตีในรูปใหม่ๆ

การโจมตีนั้นแบ่งเป็น 3 ส่วนคือ Deployment, Use และ Impact

1. Deployment รูปแบบการโจมตีตั้งแต่ช่วงปี 1999 จะเริ่มจากการเจาะเข้าไปในระบบที่มีช่องโหว่ แล้วจึงติดตั้งโปรแกรมที่ทำหน้าที่เป็น DDoS ลงไปในระบบดังกล่าว ดังนั้นจึงสามารถพบเห็นการเพิ่มขึ้นของการโจมตีแบบอัตโนมัติ การเลือกเป้าหมายนั้นมีทั้งแบบสุ่ม (blind targeting) และการเลือกเป้าหมายแบบเจาะจง (selective targeting) เช่น ระบบปฏิบัติการวินโดวส์และเราเตอร์ นอกจากนี้ยังพบว่าช่วงเวลาที่ใช้ระหว่างการค้นพบช่องโหว่ใหม่กับการคิดค้น exploit tool ออกมาเพื่อใช้งานช่องโหว่นั้นมีช่วงเวลาที่สั้นลง

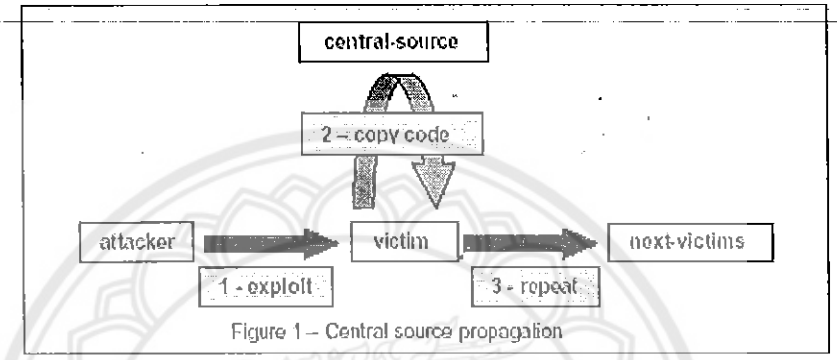
Automation เช่นเดียวกับรูปแบบการโจมตีอื่น การโจมตีแบบ DoS ในช่วงแรก จะใช้วิธีเจาะเข้าไปในระบบที่มีช่องโหว่จากนั้นจึงติดตั้งเครื่องมือด้วยตัวเอง ภายหลังได้มีการคิดค้นเครื่องที่ช่วยทำงานเหล่านี้ให้โดยอัตโนมัติ จุดเริ่มต้นของการโจมตีมักจะเริ่มจากการสแกนไปยังระบบของเป้าหมาย ซึ่งสแกนเนอร์จะแสดงรายชื่อโฮสต์ที่มีช่องโหว่ จากนั้นก็จะใช้ automated tool หรือเครื่องมือที่ใช้ในการรัน exploit บนโฮสต์ที่มีช่องโหว่ เพื่อครอบครองโฮสต์ดังกล่าว จากนั้นจึงจะติดตั้งเครื่องมือสำหรับโจมตีต่อไป

หากพิจารณาในรายละเอียดจะพบว่า เครื่องมือของผู้โจมตีจะก่อให้เกิดแพ็กเก็ตจำนวนมาก โดยอาศัยเครือข่ายที่ตอบรับกับ IP direct broadcast packet เช่น ผู้โจมตีสร้างแพ็กเก็ตจำนวนมากจาก Microsoft Internet Information Server (IIS) ที่มีช่องโหว่ซึ่งอนุญาตให้รันคำสั่งใน HTTP request ได้ ในปัจจุบันผู้โจมตีได้พัฒนาเครื่องมือที่สามารถสั่งงานโดยอัตโนมัติตั้งแต่เริ่มการสแกน การทำ exploit (หรือหาประโยชน์จากช่องโหว่ของระบบ) และติดตั้งเครื่องมือสำหรับโจมตี เครื่องมืออย่าง T0rnkit ถือได้ว่าเป็นเครื่องมือที่ประสบความสำเร็จมากตัวหนึ่ง แต่เครื่องมือแบบนี้ไม่มีคุณสมบัติในการกระจายตัวโดยอัตโนมัติแต่อย่างใด อย่างไรก็ตามก็มีหนอนอินเทอร์เน็ตบางตัว เช่น Ramen หรือ Nimda ที่สามารถสแกน การทำ exploit ติดตั้งเครื่องมือสำหรับโจมตี และกระจายตัวต่อไปโดยอัตโนมัติ ซึ่งปัจจุบันได้เริ่มมีการนำเครื่องมือลักษณะดังกล่าวมาใช้งานด้วย

การกระจายตัวแบบอัตโนมัติมีด้วยกัน 3 รูปแบบ คือ

1. Central source propagation

กลไกการกระจายตัวแบบนี้จะต้องใช้ระบบที่ถูก Compromised เรียบร้อยแล้ว จากนั้นจึงติดตั้งเครื่องมือหรือ attacker toolkit จากส่วนกลาง โดยมี script ที่ทำหน้าที่ควบคุมการติดตั้งและเริ่มวงจรเพื่อโจมตีที่อื่นต่อไป กลไกการรับส่งไฟล์จะใช้โพรโตคอล HTTP, FTP และ RPC เป็นส่วนใหญ่ ตัวอย่างที่เห็นได้ชัดคือ หนอนอินเทอร์เน็ตที่ชื่อ 1i0n

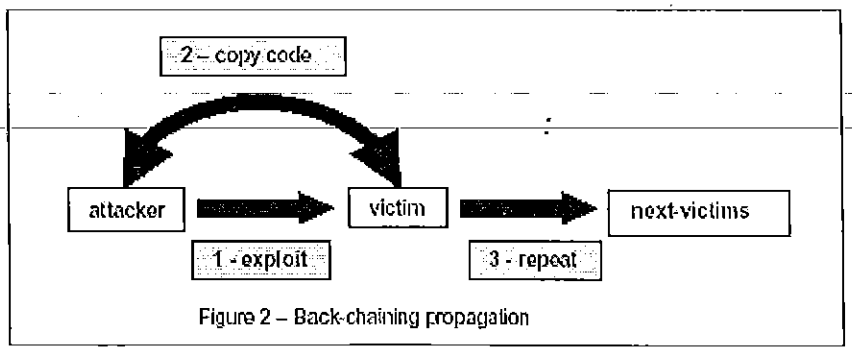


รูปที่ 2-23 Central source propagation

(ที่มา: www.thaicert.nectec.or.th/)

2. Back-chaining propagation

กลไกการกระจายตัวแบบนี้จะต้อง compromise ไปยังเป้าหมายจาก attacker host แล้วจึงส่งต่อ attacker tool ไปยังเครื่องที่ถูก compromised ไปแล้วดังกล่าว ในบางกรณี attack tool จะสามารถเปิด port เพื่อรอรับ connection สำหรับขนส่งไฟล์ข้ามเครือข่าย หรือใช้ TFTP ข้อดีของการกระจายตัวแบบนี้คือสามารถคงอยู่ได้นานกว่าเพราะไม่มี single point of failure ตัวอย่างที่เห็นได้ชัดเจนกว่าหนอนอินเทอร์เน็ตที่ชื่อ ramen

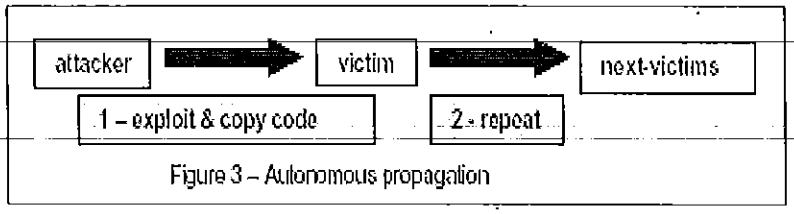


รูปที่ 2-24 Back-chaining propagation

(ที่มา: www.thaicert.nectec.or.th/)

3. Autonomous propagation

ตัวอย่างที่เห็นได้ชัดเจนคือ Code red และ Morris ซึ่งเป็นหนอนอินเทอร์เน็ตที่กระจายตัวในปี 1988 การ exploit จะผสมกลไกการกระจายตัวเข้าไปด้วย ดังนั้นจึงไม่มีการรับส่งไฟล์จากภายนอกแต่อย่างใด



รูปที่ 2-25 Autonomous propagation
(ที่มา: www.thaicert.nectec.or.th/)

ในที่นี้ไม่ได้รวมการกระจายตัวผ่านทางไฟล์แนบ (attachment) ของอี-เมล์ เข้ามาเป็นวิธีในการกระจายตัว เพราะการกระจายตัวผ่านทางอี-เมล์ดังกล่าวจำเป็นต้องได้รับการกระตุ้นโดยผู้ใช้งานเสียก่อน (ปัจจุบันมีไวรัสบางตัวที่ต้องการกระตุ้นจากผู้ใช้เพียงเล็กน้อย เช่น Nimda, Goner ที่ผู้ใช้แค่เพียงคลิ้กที่ subject ของอี-เมล์ก็สามารถกระจายตัวไปได้ ซึ่งอาศัยช่องโหว่ของโปรแกรม Microsoft Internet Explorer ในขณะที่ไวรัสแบบเก่าจำเป็นต้องได้รับการกระตุ้น โดยการรันไฟล์ที่แนบมาโดยผู้ใช้อย่างชัดเจน) ปัจจุบันจะเห็นการโจมตีที่มากขึ้นผ่านทางอี-เมล์ โดยพยายามลวงผู้ใช้งานให้เข้าใจผิดเกี่ยวกับชื่อไฟล์ที่แนบมาด้วย อย่างไรก็ตามการโจมตีในรูปแบบดังกล่าวถือได้ว่าเป็นการโจมตีแบบ social engineering ซึ่งไม่ได้ใช้เทคโนโลยีที่ซับซ้อนมากขึ้นแต่อย่างใด

พื้นฐานการโจมตีเป้าหมาย

การโจมตีแบบอัตโนมัติในหัวข้อด้านบนนั้นมักจะกระทำกับระบบปฏิบัติการที่เป็นยูนิกซ์เท่านั้น แต่เนื่องจากจำนวนผู้ใช้ระบบปฏิบัติการวินโดวส์ที่เพิ่มขึ้น และจำนวนช่องโหว่ที่เพิ่มมากขึ้น ทำให้ end-user กลายเป็นเป้าหมายของการเจาะเข้าไปเพื่อติดตั้ง DoS tool ในที่นี้จะพูดถึงรูปแบบในการเลือกเป้าหมายซึ่งมี 2 รูปแบบด้วยกันคือ การเลือกเป้าหมายแบบสุ่มและการเลือกเป้าหมายแบบเจาะจง

หนอนอินเทอร์เน็ตที่กระจายตัวได้ด้วยตัวเองอย่าง Code Red, Code Red II และ Nimda ใช้วิธีการเลือกเป้าหมายแบบสุ่ม ซึ่งเป้าหมายที่สุ่มได้จะมีขนาดใหญ่ แต่เน้นหนักเฉพาะเป้าหมายที่อยู่ในเครือข่ายใกล้เคียงกันเท่านั้น ซึ่งบรรดาเครื่องมือหรือหนอนเหล่านี้ใช้หลักการพื้นฐานของการสุ่มค่าตัวเลขขึ้นมา ปัจจุบันมีการโจมตีทั้งต่อยูนิกซ์และวินโดวส์ การโจมตีที่มีพื้นฐานการเลือก

เป้าหมายแบบสุ่มปกติแล้วจะทำเองโดยอัตโนมัติ และในช่วงของการโจมตีจะใช้มนุษย์มาเกี่ยวข้องเพียงเล็กน้อยหรือน้อยมาก ความสำเร็จของการโจมตีจะถูกจำกัดไว้ในระดับหนึ่ง เพราะเครื่องมือที่ใช้มักจะถูกออกแบบให้โจมตีช่องโหว่ในไม่กี่รูปแบบเท่านั้น

การโจมตีที่มีพื้นฐานการเลือกเป้าหมายแบบเจาะจงมักจะไม่ใช้งานที่เป็นอัตโนมัติมากนัก และการเลือกเป้าหมายจะไม่ขึ้นอยู่กับช่องโหว่ด้วย เกณฑ์การเลือกเป้าหมายขึ้นอยู่กับลักษณะการเชื่อมต่อเครือข่าย แบนด์วิดธ์ที่มีการใช้งาน และแบนด์วิดธ์ที่เหลืออยู่มากกว่า เพราะผู้โจมตีจะใช้เป็นส่วนหนึ่งของการโจมตี DoS แบบกระจายหรือ DDoS แต่ในปัจจุบันผู้โจมตีมักจะไม่ค่อยให้ความสนใจต่อเกณฑ์การเลือกเป้าหมายมากนัก ซึ่งจะเห็นว่าการเลือกเป้าหมายที่เป็น end-user ที่ใช้ระบบปฏิบัติการวินโดวส์กำลังเพิ่มจำนวนขึ้นสำหรับการเลือกเป้าหมายทั้งสองรูปแบบ และจากการพัฒนารวมทั้งการนำโค้ดมาใช้ใหม่ ทำให้เครื่องมือสำหรับโจมตีมีความสามารถในการโจมตีช่องโหว่ที่มีอย่างมากมายของวินโดวส์ ส่งผลให้มีการใช้งานเครื่องเหล่านั้นอย่างกว้างขวางสาเหตุที่ผู้โจมตีมุ่งเป้าไปยังผู้ที่ใช้วินโดวส์ก็เนื่องจาก ผู้ใช้ส่วนใหญ่ไม่มีความรู้เกี่ยวกับ security ไม่ทราบวิธีป้องกันตัวเองจากการโจมตี ซึ่งแตกต่างจากผู้เชี่ยวชาญหรือผู้ดูแลระบบที่ยังสามารถป้องกันตัวเองได้ในระดับหนึ่ง

การเลือกเราเตอร์เป็นเป้าหมาย

มีการเพิ่มจำนวนของการโจมตีที่มุ่งเป้าไปที่เราเตอร์มากขึ้น เนื่องจากผู้ผลิตบางรายได้มีการตั้งค่า Default password ไว้ หรือมีการติดตั้งที่ไม่ดีพอ ซึ่งทำให้ผู้บุกรุกสามารถครอบครองเราเตอร์ได้ มีเอกสารที่แสดงคำสั่งที่ควรจะถูกรันภายหลังจากผู้บุกรุกสามารถครอบครองเราเตอร์ได้เพื่อแก้ไข configuration ของเราเตอร์ ผู้บุกรุกมักจะใช้เราเตอร์เป็นจุดในการสแกนระบบ หรือใช้เป็น proxy เพื่อติดต่อไปยัง IRC หรือใช้เป็นจุดในการสร้าง flooding DoS attack

เราเตอร์เป็นเป้าหมายที่นิยมกันของผู้โจมตี เนื่องจากเป็นจุดที่มักจะอยู่นอกเหนือ Security policy และไม่ได้รับการป้องกันเท่าที่ควร นอกจากนี้ยังมีโอกาสที่จะถูกค้นพบยังมีน้อยความสำคัญของเราเตอร์เริ่มมีบทบาทมากขึ้นสำหรับการโจมตีแบบ DoS ซึ่งอยู่บนพื้นฐานของการโจมตีโดยตรงไปยัง routing protocols ที่เชื่อมเครือข่ายระหว่างกันบนอินเทอร์เน็ต

ความสามารถของเครื่องมือ

การโจมตีที่ดีจะพยายามลดเวลาที่จะใช้ในการเข้าโจมตี เพราะช่วงเวลาตั้งแต่มีการค้นพบช่องโหว่พร้อมกับการเข้าใช้ช่องโหว่(Exploit) จนถึงการที่ผู้ดูแลระบบนำ patch มาติดตั้งเพื่อป้องกันระบบนั้นมีช่วงเวลาที่สั้นลง และเนื่องจากการที่มีเครื่องมือสำหรับโจมตีเป็นจำนวนมากทำให้การพัฒนาเครื่องมือเพื่อเข้าใช้งานช่องโหว่ใหม่ๆ ได้ตลอด นอกจากนี้ยังมีกลุ่มคนซึ่งมักจะชุม

สร้างเครื่องมือสำหรับโจมตีใหม่ๆ ออกมาเรื่อยๆ เพื่อสร้างคุณค่าให้กับกลุ่มของตัวเอง เครื่องมือที่ถูกเผยแพร่สู่สาธารณะมักจะใช้ประโยชน์ไม่ค่อยได้เนื่องจากเก่าเกินไป แต่ผู้พัฒนาก็พยายามที่จะออกแบบเครื่องมือเพื่อเพิ่มอายุการใช้งานให้มากขึ้น

2. Use ยังคงเห็นการโจมตีแบบ DoS รูปแบบเก่า คือโจมตีจากที่เดียวไปยังเป้าหมายหลายแห่งพร้อมกัน

Control Channels รูปแบบการโจมตีแบบ DoS ในก่อนหน้านี้จะเป็นการส่งคำสั่งควบคุมการโจมตีจากเครื่องควบคุม (intruder) ไปยัง agent หรือตัวกลาง (ซึ่งถูก compromise และติดตั้งเครื่องมือไว้แล้ว) เพื่อส่งแพ็กเก็ตจำนวนมากไปยังเป้าหมายพร้อมๆ กัน โดยทั่วไปตัวกลางจะเปิด port เพื่อรอรับคำสั่งโจมตีจากผู้ควบคุม และเช่นเดียวกันเครื่องควบคุมก็จะเปิด port ไว้เพื่อให้ตัวกลางรายงานค่าไอพีแอดเดร็สของตัวกลางเข้ามา โดยปกติค่า port ที่ใช้จะเป็นค่าที่แน่นอน และเป็น port ที่มีค่าสูงๆ

ตัวอย่างแสดงการใช้ Port ของ **Trinoo**

ผู้โจมตี --> เครื่องที่ทำหน้าที่ควบคุม; destination port 27665/tcp
เครื่องที่ทำหน้าที่ควบคุม --> ตัวกลาง; destination port 27444/udp
ตัวกลาง --> เครื่องที่ทำหน้าที่ควบคุม; destination port 31335/udp

เครื่องมืออื่นๆ อย่างเช่น Stacheldraht สามารถเข้ารหัสคำสั่งที่ใช้ในการสื่อสารได้ เพื่อป้องกันการถูกตรวจสอบจาก sniffer หรือ IDS

ก่อนหน้านี้เมื่อเครือข่ายถูกโจมตีด้วย DoS มักจะถูกตรวจสอบและขัดขวางได้ง่าย เนื่องจากเครื่องที่ทำหน้าที่เป็นตัวกลางจะต้องทำหน้าที่รักษารายชื่อของเครื่องที่ทำหน้าที่ควบคุม ซึ่งก็คือรายชื่อไอพีแอดเดร็สของเครื่องเหล่านั้น เพื่อส่งแพ็กเก็ตไปลงทะเบียนกับเครื่องที่ทำหน้าที่ควบคุม ดังนั้นหากสามารถขัดขวางการทำงานของเครื่องที่ทำหน้าที่เป็นตัวกลางได้ ก็จะสามารถตรวจสอบได้ว่าเครื่องที่ทำหน้าที่ควบคุมมีไอพีใดบ้าง ในขณะเดียวกันเครื่องที่ทำหน้าที่เป็นเครื่องควบคุมก็จะมีรายชื่อไอพีของเครื่องที่เป็นตัวกลางอยู่ การค้นพบเครื่องที่ทำหน้าที่ควบคุมก็จะนำไปสู่การขัดขวางการโจมตีได้ และเนื่องจากทั้งเครื่องที่ทำหน้าที่ควบคุมและเครื่องที่เป็นตัวกลางจะต้องเปิด port เพื่อรอรับ connection มันจึงสามารถถูกค้นพบได้โดย network scanner นอกจากนี้ช่องทางการสื่อสารที่ใช้ระหว่างผู้โจมตีกับเครื่องที่ทำหน้าที่ควบคุม และเครื่องที่ทำหน้าที่ควบคุมกับเครื่องที่เป็นตัวกลาง จะสามารถถูกค้นพบและดักจับได้ด้วยเครื่องมือที่คอยจับตาดูเครือข่าย เช่น Intrusion detection System (IDS)

ข้อบกพร่องของเครื่องมือโจมตีแบบ DoS รุ่นเก่า ทำให้มันไม่สามารถถูกใช้งานได้อย่างแพร่หลาย ไม่ว่าจะเป็นขั้นตอน deployment ซึ่งต้องอาศัยเวลา หรือแม้แต่การทำ automate deployment ก็ตาม การถูกค้นพบเพียงเครื่องเดียวอาจจะทำให้กระบวนการที่ทำมาทั้งหมดนั้นไม่สามารถใช้งานได้เลย ดังนั้นในปัจจุบันนี้จะพบเห็นแต่เพียงขั้นตอนของการ deployment ของเครื่องมือต่างๆ เท่านั้น ในปัจจุบันพบว่าผู้บุกรุกได้ใช้โพรโตคอล Internet Relay Chat (IRC) เป็นช่องทางหลักของการสื่อสารเพิ่มมากขึ้น ซึ่งได้เปลี่ยนรูปแบบในการควบคุมการโจมตี โดยทำหน้าที่เป็นเครื่องที่ทำหน้าที่ควบคุมแทน ซึ่งมีข้อดีเนื่องจากสามารถรันบ็อท (bots) บนเครือข่าย IRC ได้ ทำให้ลดการพึ่งพามนุษย์ลงไปได้

การใช้เครือข่ายและโพรโตคอล IRC ทำให้ยากในการตรวจสอบที่มาของการโจมตีแบบ DDoS เนื่องจากเครื่องที่ทำหน้าที่เป็นตัวกลางสามารถส่งข้อมูลออกไปยังเครือข่าย IRC โดยใช้ port มาตรฐานได้ เช่น port 6667/tcp ซึ่งในกรณีนี้ตัวกลางไม่จำเป็นต้องเปิด port รอรับ connection ดังนั้นการใช้ network scanner ตรวจสอบก็ไม่สามารถตรวจจับได้ เมื่อผู้โจมตีต้องการสื่อสารไปยังเครื่องตัวกลางก็จะติดต่อไปยัง IRC server และใช้ช่องทางการสื่อสารของ IRC เพื่อควบคุมการทำงานของเครื่องตัวกลาง ซึ่งโดยปกติแล้วถ้าเครือข่ายมีนโยบายการรักษาความปลอดภัยที่ดีพอ เช่น การห้ามใช้งาน IRC port ก็จะสามารถดักจับและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตได้ แต่โดยทั่วไปแล้วมักจะมีการอนุญาตให้ใช้งาน IRC เนื่องจากเป็นความต้องการของผู้ใช้การสืบสวนหาผู้โจมตีที่ใช้ช่องทางการควบคุมผ่านเครือข่ายและโพรโตคอล IRC นั้น ส่วนใหญ่มักจะไม่ประสบความสำเร็จ เพราะหากมีการค้นพบเครื่องที่ทำหน้าที่เป็นตัวกลางแล้ว การสืบสวนต่อไปมักจะสิ้นสุดลงที่ IRC server และทราบเพียงชื่อ channel ที่ใช้ในการควบคุมเท่านั้นเอง

ExecutionDoSAttacks จากการเปลี่ยนแปลงของการโจมตีแบบ DoS การเพิ่มขึ้นของผู้ใช้อินเทอร์เน็ตทั้ง end-user/องค์กร และประสบการณ์ของการโจมตี จะเห็นได้ว่ามีการเพิ่มจำนวนของการโจมตีแบบ DDoS ขนาดใหญ่มากขึ้นเรื่อยๆ เครือข่ายขนาดใหญ่มีแบนด์วิดธ์และทรัพยากรที่มากขึ้น การโจมตีที่เกิดขึ้นก็ได้อาศัยทรัพยากรที่มากมายเหล่านี้ด้วย การทำ packet filtering หรือ rate limiting นั้นสามารถหยุดยั้งการโจมตีได้บางรูปแบบเท่านั้น ผู้โจมตีได้พยายามใช้โพรโตคอลหรือบริการที่มักจะอนุญาตให้ใช้งานเป็นพาหนะในการขนถ่ายข้อมูลผ่านไป การทำ packet filtering หรือ rate limiting โดยใช้วิธี anomalous (การตรวจจับโดยอาศัยหลักการสังเกตุความผิดปกติของเหตุการณ์ที่เกิดขึ้น โดยเปรียบเทียบกับเหตุการณ์ที่เป็นปกติ) เองก็ทำได้ยาก แต่อย่างไรก็ตามการใช้วิธีการทั้ง packet filtering และ rate limiting ก็ทำให้งานของผู้โจมตียากขึ้นไปอีกระดับหนึ่ง

การปลอมไอพีแอดเดรสในการโจมตีแบบ DoS มักจะไม่จำเป็น เพราะจำนวนเครื่องที่ใช้เป็น source ในการโจมตีมักจะมีจำนวนมากมาย ซึ่งอาจจะอยู่ในคนละ AS (autonomous system) กันก็ได้ และส่วนใหญ่มักจะถูกครอบครองได้อย่างง่ายดาย

3. Impact Increased Blast zone ปกติผลกระทบของการโจมตีแบบ DoS มักจะขึ้นกับความสามารถในการใช้งานทรัพยากรที่ยังหลงเหลืออยู่ มีวิธีและเครื่องมือมากมายที่สามารถทำลายเครือข่ายที่มีทรัพยากรเหลือเฟือได้ นอกจากนี้ยังมีผลกระทบข้างเคียงที่เกิดจากการโจมตีที่ไม่เกี่ยวข้องกับการใช้งานทรัพยากรหรือ resource

ตัวอย่างที่เห็นได้ชัดเจนคือ ระบบการบันทึกล็อกซึ่งโดยปกติจะบันทึกข้อมูลที่เกี่ยวข้องกับเครือข่ายลงในระบบ เมื่อมีการกระจายของไวรัสบางตัว เช่น Code red, Nimda, Netsky, Sasser ก็อาจจก่อให้เกิดปัญหากับระบบบันทึกข้อมูลซึ่งต้องบันทึกข้อมูลจำนวนมาก จนพื้นที่สำหรับเก็บข้อมูลมีไม่เพียงพอซึ่งอาจจะมีผลต่อการทำงานของระบบโดยรวมได้สำหรับเครือข่ายที่เชื่อมต่อเครือข่ายอื่นผ่านทาง upstream network ที่มีการคิดค่าใช้จ่ายจากจำนวนข้อมูลที่ถูกส่งผ่าน ก็จะได้รับผลกระทบจากการโจมตีแบบ DoS ซึ่งจะก่อให้เกิดมีการส่งผ่านข้อมูลจำนวนมาก ทำให้อาจจะมีปัญหากับค่าใช้จ่ายที่ตามมาได้ ปัจจุบันมีความนิยมในการใช้งาน web hosting มากขึ้น ซึ่งหมายถึงการโจมตีต่อเว็บไซต์แห่งเดียว ก็จะทำให้เกิดผลกระทบต่อเว็บไซต์อื่นๆ ที่ใช้บริการอยู่บนเครื่องเดียวกันได้

เวลาที่เหมะสำหรับการโจมตี

เหตุการณ์ต่างๆ ที่เกิดขึ้น เช่น Code Red, Nimda, Netsky, Sasser ต่างแสดงให้เห็นว่าเครื่องมือที่ทำงานแบบอัตโนมัติเหล่านี้สามารถก่อให้เกิดการโจมตีแบบ DoS ได้ในหลายๆ ส่วนของอินเทอร์เน็ต การ scan และกระจายตัวของไวรัสเหล่านี้ไม่ใช่ปัญหาหลัก แต่ผลข้างเคียงที่เกิดขึ้นกลับกลายเป็นปัญหาหลัก โดยส่วนใหญ่ปัญหาจะเกิดขึ้นภายในเครือข่ายท้องถิ่น (local network) นอกจากนี้ยังไม่น่าเชื่อว่าจะมีอุปกรณ์บางตัวที่ได้รับผลกระทบจากไวรัสเหล่านี้ เช่น printer, DSL modem เหตุการณ์ที่เกิดขึ้นทั้งหมดนั้นสามารถทำให้ระบบที่เชื่อมต่อกับอินเทอร์เน็ตหยุดการทำงานไปได้อย่างง่ายดาย

2.15 การสแกนพอร์ต (Port Scanning)

เป็นหนึ่งในเทคนิคที่โด่งดังที่สุดที่ผู้โจมตีใช้ในการค้นหาบริการที่พวกเขาจะสามารถเจาะผ่านเข้าไปยังระบบๆได้ โดยปกติแล้วทุก ๆ ระบบที่ต่อเข้าสู่ระบบ LAN หรือระบบอินเทอร์เน็ตจะเปิดบริการทั้งที่อยู่บนพอร์ตที่เป็นที่รู้จักและที่ไม่เป็นที่รู้จัก สำหรับการทำ Port Scanning นั้น ผู้

โจมตีจะสามารถค้นหาข้อมูลได้มากมายจากระบบของเป้าหมาย ได้แก่ บริการอะไรบ้างที่กำลังรันอยู่ ผู้ใช้คนไหนเป็นเจ้าของบริการเหล่านั้น สนับสนุนการล็อกอินด้วย anonymous หรือไม่ และบริการด้านเครือข่ายมีการทำ authentication หรือไม่ การทำ Port Scanning ทำได้โดยการส่งข้อความหนึ่งไปยังแต่ละพอร์ต ณ เวลาหนึ่ง ๆ ผลลัพธ์ที่ตอบสนองออกมาจะแสดงให้เห็นว่าพอร์ตนั้น ๆ ถูกใช้อยู่หรือไม่ และสามารถทดสอบดูเพื่อหาจุดอ่อนต่อไปได้หรือไม่ Port Scanners มีความสำคัญต่อผู้ชำนาญด้านความปลอดภัยของเครือข่ายมากเพราะว่ามันสามารถเปิดเผยจุดอ่อนด้านความปลอดภัยที่มีความเป็นไปได้ของระบบเป้าหมาย

การ Scan ต่อไปนี้เป็นรูปแบบมาตรฐานสำหรับเครื่องมือ Port Scanning ที่ทำงานโดยอัตโนมัติ เช่น Nmap และ Nessus

Address Resolution Protocol (ARP) scans จะตรวจหาอุปกรณ์ที่ทำงานในเครือข่ายโดยการส่งชุดของ ARP broadcasts และเพิ่มค่าของฟิลด์ที่บรรจุ IP address ของเป้าหมายในแต่ละ broadcast packet การ scan ชนิดนี้จะได้รับผลตอบสนองจากอุปกรณ์ที่มี IP บนเครือข่ายออกมาในรูปแบบของ IP address ของแต่ละอุปกรณ์ การ scan แบบนี้จึงทำการ map out ได้ทั้งเครือข่ายอย่างมีประสิทธิภาพ

The Vanilla TCP connect scan เป็นเทคนิคการ scan แบบพื้นฐานและง่ายที่สุด คือจะใช้ connect system call ของระบบปฏิบัติการไปบนระบบเป้าหมายเพื่อเปิดการเชื่อมต่อไปยังทุก ๆ พอร์ตที่เปิดอยู่ การ scan ชนิดนี้สามารถจับได้ง่ายมาก โดยล็อก (log) ต่าง ๆ ของระบบที่เป็นเป้าหมายจะแสดงการร้องขอการเชื่อมต่อ (connection requests) และข้อความแสดงข้อผิดพลาด (error messages) สำหรับบริการที่ตอบรับการเชื่อมต่อนั้น

The TCP SYN (Half Open) scans เทคนิคนี้บางครั้งถูกเรียกว่า half open เพราะว่าระบบที่ทำการโจมตีไม่ได้ปิดการเชื่อมต่อที่ได้เปิดไว้ scanner จะส่ง SYN packet ไปยังเป้าหมายและรอการตอบสนอง ถ้าพอร์ตถูกเปิดไว้เป้าหมายก็จะส่ง SYN/ACK กลับมา แต่ถ้าพอร์ตถูกปิดอยู่ เป้าหมายก็จะส่ง RST กลับมา วิธีการ scan รูปแบบนี้ยากต่อการตรวจจับ ปกติเครื่องที่เป็นเป้าหมายจะทำหน้าที่ปิดการเชื่อมต่อที่เปิดไว้ และส่วนใหญ่จะไม่มีระบบการล็อกที่เหมาะสมในการตรวจจับการ scanชนิดนี้

The TCP FIN scan เทคนิคนี้สามารถที่จะทะลุผ่านไฟล์วอลล์ ส่วนใหญ่, packet filters, แต่ละโปรแกรมตรวจจับการ scan ไปได้โดยไม่ถูกตรวจพบ เพราะระบบที่ทำการโจมตีจะส่ง FIN packets

ไปยังระบบของเป้าหมาย สำหรับพอร์ตต่าง ๆ ที่ปิดอยู่จะตอบสนองกลับไปด้วย RST ส่วนพอร์ตที่เปิดจะไม่สนใจ packets เหล่านั้นเลย ดังนั้นเครื่องที่ทำการโจมตีก็จะได้ข้อมูลว่ามันได้รับRSTจากพอร์ตไหนบ้างและไม่ได้RSTจากพอร์ตไหนบ้าง

The TCP Reverse Ident scan เป็นเทคนิคที่สามารถตรวจหาชื่อของเจ้าของแต่ละโพรเซสที่เป็นการเชื่อมต่อด้วย TCP บนเครื่องเป้าหมาย การ scan ชนิดนี้จะทำให้ระบบที่ทำการโจมตีสามารถเชื่อมต่อเข้าไปยังพอร์ตที่เปิดอยู่และใช้ ident protocol ในการค้นหาว่าใครเป็นเจ้าของโพรเซสบนเครื่องเป้าหมายได้

The TCP XMAS ถูกใช้เพื่อหาพอร์ตบนเครื่องเป้าหมายที่อยู่ในสถานะ listening โดยจะส่ง TCP packet ที่มี flag เป็น URG, PSH และ FIN ใน TCP header ไปยังพอร์ตของเครื่องเป้าหมาย ถ้าพอร์ต TCP ของเครื่องเป้าหมายปิดอยู่ พอร์ตนั้นก็จะส่ง RST กลับมา

The TCP NULL scan เทคนิคนี้จะส่ง TCP packet ที่มี sequence number แต่ไม่มี flag ออกไปยังเครื่องเป้าหมาย ถ้าพอร์ตปิดอยู่จะส่ง กลับมา RST packet กลับมา แต่ถ้าพอร์ตเปิดอยู่

The TCP ACK scan เป็นเทคนิคที่ใช้ค้นหาเว็บไซต์ที่เปิดบริการอยู่ แต่ปฏิเสธการตอบสนองต่อ ICMP ping หรือค้นหากฎ (rule) หรือนโยบาย (policy) ต่าง ๆ ที่ตั้งไว้ที่ไฟล์วอลล์เพื่อตรวจสอบดูว่าไฟล์วอลล์สามารถกรอง packet อย่างง่าย ๆ หรือเทคนิคชั้นสูง โดยการ scan แบบนี้จะใช้ TCP packet ที่มี flag เป็น ACK ส่งไปยังพอร์ตเครื่องปลายทาง ถ้าพอร์ตเปิดอยู่ เครื่องเป้าหมายจะส่ง RSTกลับมาแต่ถ้าปิดอยู่ก็จะไม่สนใจpacketนั้น

The FTP Bounce Attack ใช้โพรโตคอล ftp สำหรับสร้างการเชื่อมต่อบริการ ftp ของ proxy วิธีการ scan แบบนี้ ผู้โจมตีจะสามารถซ่อนตัวอยู่หลัง ftp server และ scan เป้าหมายอื่น ๆ ได้โดยไม่ถูกตรวจจับ ดังนั้น ftp servers ส่วนใหญ่จะมีการ disable บริการของ ftp เพื่อความปลอดภัยของระบบ

The UDP ICMP port scan ใช้โพรโตคอล UDP ในการ scan หาพอร์ตหมายเลขสูง ๆ โดยเฉพาะในระบบSolarisแต่จะช้าและไม่น่าเชื่อถือ

The ICMP ping-sweeping scan จะใช้คำสั่ง ping เพื่อกวาดดูว่ามีระบบไหนที่เปิดใช้งานอยู่ เครือข่ายส่วนใหญ่จึงมีการกรองหรือ disabledโพรโตคอล ICMP เพื่อความปลอดภัยของระบบ

1.การปิดพอร์ต

การปิดพอร์ต คือ การไม่ยอมรับการติดต่อเข้ามายังพอร์ตนั้นๆ เช่นเดียวกับการเปิดพอร์ต เราไม่สามารถปิดพอร์ตนั้นโดยตรงได้ด้วยโอสต์ทั่วไปหากจะปิดพอร์ต จะต้องหยุดการทำงานของแอปพลิเคชั่นก่อนแล้วพอร์ตจะถูกปิดไปเอง หรือสามารถทำได้โดยผ่านไฟร์วอลล์ เราเตอร์ หรืออุปกรณ์ Layer 4 Switch

2. การเปิดพอร์ต

สามารถกำหนดได้เพียงส่วนที่อยู่ในระดับไอพี คือ หมายเลขไอพี สับเน็ตมาสก์ และ เกตเวย์เท่านั้น จะไม่สามารถกำหนดได้ว่าจะเปิดปิดพอร์ตใดบ้าง การที่พอร์ตใดจะเปิดให้บริการเป็นเซิร์ฟเวอร์พอร์ตนั้นจะต้องมีแอปพลิเคชั่นทำงานอยู่บนพอร์ตนั้นเสมอ คือมีโปรแกรมที่รับหน้าที่โต้ตอบและจัดการการสื่อสารที่มายังพอร์ตนั้น จึงอาจเปรียบได้ว่าพอร์ตก็คือแอปพลิเคชั่น การที่มีพอร์ตเปิดอยู่ก็หมายถึงการมีแอปพลิเคชั่นทำงานอยู่นอกจากแอปพลิเคชั่นจะเปิดพอร์ตเพื่อใช้งานแล้ว ระบบปฏิบัติการที่อาศัย ทีซีพี/ไอพี ก็จะต้องเปิดพอร์ตเพื่อใช้ในกิจการของระบบปฏิบัติการด้วย โดยที่ผู้ใช้ไม่รู้ตัว เพราะเป็นการใช้งานภายในของระบบปฏิบัติการและผู้ผลิตคิดว่าผู้ใช้ไม่จำเป็นต้องรู้ จึงทำให้ผู้ใช้ถูกบุกรุกจากพอร์ตเหล่านี้ด้วย ซึ่งเมื่อเริ่มใช้แอปพลิเคชั่นมาก เครื่องคอมพิวเตอร์ของเราก็จะเริ่มเปิดพอร์ตมากขึ้น ซึ่งเป็นการเปิดช่องทางให้ผู้อื่นติดต่อเข้ามาได้มากขึ้นตามไปด้วย

1. พอร์ตที่เปิดไว้โดยไม่ได้ตั้งใจ

การเปิดพอร์ตเป็นการเปิดแบบลอจิคัลและมองไม่เห็น ดังนั้นหากไม่ทำการตรวจสอบโอสต์ของเราให้ดี จะไม่ทราบว่ามีพอร์ตใดเปิดอยู่ ส่วนใหญ่เกิดจากแอปพลิเคชั่นอื่นๆ มาเปิดพอร์ตบนโฮสต์เราโดยที่เราไม่เคยติดตั้งเข้าไปด้วยเลย โดยแอปพลิเคชั่นเหล่านี้ได้มาตั้งแต่ขั้นตอนการติดตั้งระบบปฏิบัติการซึ่งผู้ผลิตคาดว่าผู้ใช้ต้องการใช้แอปพลิเคชั่นเหล่านั้น ผู้ใช้สามารถตรวจสอบว่ามีแอปพลิเคชั่นใดบ้างที่ทำงานอยู่โดยที่เราไม่ต้องการ ให้หยุดการทำงานของแอปพลิเคชั่นเหล่านั้น พอร์ตก็จะถูกปิดไปเอง

2. พอร์ตของระบบปฏิบัติการ

เป็นพอร์ตที่จำเป็นสำหรับระบบปฏิบัติการนั้นๆ หากไม่เปิดพอร์ตเปล่านี้ระบบปฏิบัติการก็จะไม่สามารถทำงานได้อย่างสมบูรณ์ เช่น ไมโครซอฟท์ วินโดวส์ เอ็นที จะต้องใช้พอร์ต 135-139 ของ ทีซีพี ในการทำงานพอร์ตประเภทนี้จะไม่สามารถปิดลงได้

เนื่องจากแอปพลิเคชั่นที่ใช้งานพอร์ตนั้นเป็นส่วนหนึ่งของระบบปฏิบัติการ ข้อเสียอย่างมาก็คือ นอกจากผู้ใช้จะไม่สามารถปิดพอร์ตเหล่านี้ได้ ยังเป็นการบอกผู้บุกรุกอีกด้วยว่าใช้ระบบปฏิบัติการอะไร และทำให้ผู้บุกรุกสามารถโจมตีได้ง่ายขึ้น

3. พอร์ตที่เปิดแบบสุ่ม

เกิดจากแอปพลิเคชั่นบางประเภทที่มีการใช้งานพอร์ตมากกว่า 1 พอร์ต โดยมีหมายเลขพอร์ตที่คงที่ไว้เป็นหลัก 1 พอร์ต ส่วนพอร์ตที่จะเปิดเป็นการชั่วคราวนี้ ไคลเอนต์และเซิร์ฟเวอร์จะมีการตกลงกันเพื่อเปลี่ยนไปสื่อสารกันที่พอร์ตนั้นๆ ซึ่งการเปิดพอร์ตประเภทนี้มีปัญหาคือ

- พอร์ตจะปิดลงเมื่อการใช้งานเสร็จสิ้น แต่หากแอปพลิเคชั่นทำงานผิดพลาดหรือหยุดลงกลางคัน พอร์ตก็อาจจะถูกเปิดค้างทิ้งไว้
- การไม่มีหมายเลขพอร์ตแน่นอน ทำให้ควบคุมและตรวจสอบได้ยาก หากพอร์ตที่ใช้บังเอิญตรงกับพอร์ตที่อันตรายซึ่งใช้โดยโปรแกรมประเภทโทรจัน
- หากมีการนำไฟร์วอลล์มาใช้ งาน การกำหนดกฎสำหรับไฟร์วอลล์จะทำได้ยาก เพราะกฎของไฟร์วอลล์จะตั้งอยู่บนพื้นฐานของการใช้พอร์ตเป็นหลัก

2.16 ตารางการโจมตี (Type of Attacks)

ประเภทของการคุกคาม (Type of Threat)	คำอธิบาย (Description)	รูปแบบการคุกคาม (Form of Threat)
การเปลี่ยนแปลงข้อมูลระหว่างส่ง	การเปลี่ยนแปลงของทรานส์แอ็กชัน(Transaction)ข้ามระบบเครือข่าย	หาจุดอ่อนของโพรโตคอลการสื่อสาร
Denial of Service	การโจมตีที่ทำให้เซิร์ฟเวอร์หรือระบบเครือข่ายแย่ลง	หาจุดอ่อนเกี่ยวกับระบบความปลอดภัยของโพรโตคอลการสื่อสาร และระบบปฏิบัติการ
การขโมยข้อมูล	การโจมตีที่ผลคือถูกขโมยข้อมูลผู้โจมตีสามารถเข้าใช้บริการต่างๆ เช่น เครื่องคอมพิวเตอร์ได้	หาจุดอ่อนเกี่ยวกับระบบความปลอดภัยของตัวแอพพลิเคชัน ระบบปฏิบัติการ และเครื่องโฮสต์
การเข้าไปยุ่งกับข้อมูล(data tampering)	การแปลงเปลี่ยนของหน้าสถานะต่างๆเช่น ข้อมูลสุขภาพ, ทรานสคริปต์ (transcripts) ของนักเรียน	หาจุดอ่อนเกี่ยวกับระบบความปลอดภัยบนเซิร์ฟเวอร์ เพื่อดัดแปลงหน้าเว็บเพจ หรือข้อมูลในฐานข้อมูล
การSpoof(Spoofing)	การปลอมแปลงหมายเลขไอพี เพื่อมีสิทธิในการเข้าใช้ทรัพยากรหรือการปลอมตัวเป็นผู้อื่นในการอีเมล์	หาจุดอ่อนของโพรโตคอลการสื่อสารที่จะยอมให้ผู้โจมตีปลอมตัวเป็นคนอื่นได้
การSniff(Sniffing)	การจับตาดูทราฟฟิก (traffic) ของระบบเครือข่าย เพื่อดูข้อมูลหรือรหัสผ่าน	ทราฟฟิกของระบบเครือข่ายถูกส่งเป็นข้อความต้นฉบับเลยอ่านได้ชัดเจน รหัสผ่านและข้อมูลต่างๆสามารถถูกนำไปใช้ได้
ไวรัส (Virus)	โปรแกรมที่ประสงค์ร้ายอาจประกอบด้วยคอมโพเนนท์ที่ไม่อันตรายหรืออันตรายก็ได้	ความสะดวกของโปรแกรมที่ดาวน์โหลด(download) มา

ตารางที่ 2-2 ประเภทการโจมตี

หรืออาจจำแนกตามจุดประสงค์ของการคุกคามได้ดังนี้

จุดประสงค์การคุกคาม (Threat Purpose)	การคุกคาม (Threats)	ผลกระทบ (Consequence)	มาตรการรับมือ (Countermeasures)
ความถูกต้อง (Integrity)	- การเปลี่ยนแปลงข้อมูล - ม้าโทรจัน(Trojan horse)	- การเปลี่ยนแปลงข้อมูล	Cryptographic Checksum
	- การแปลงข้อมูลระหว่างส่ง	- ม้าโทรจัน(Trojan horse) - การแปลงข้อมูลระหว่างส่ง	
ความลับความเป็นส่วนตัว (Confidentiality)	- การแอบดูข้อมูลบนเน็ต - ขโมยข้อมูล	- ข้อมูลสูญหาย - สูญเสียความเป็นส่วนตัว	การเข้ารหัส (Encryption) Web proxies
Denial Of Service	- การทำลายThreads - การฟลัดดิ้ง(Flooding) - การทำให้หน่วยความจำเต็ม - โจมตีดีเอ็นเอเซิร์ฟเวอร์ (DNS Server) เพื่อปล่อยให้เครื่องโคดเดี่ยว	- ภาวะแตกแยก (Disruptive) - ทำให้ผู้ใช้ทำงานไม่เสร็จ - ทำให้รำคาญ	ยากที่จะป้องกัน
การพิสูจน์ตน (Authentication)	- การปลอมตัวเป็นผู้ใช้ที่มีสิทธิ์ - การปลอมแปลงเอกสาร	- เชื่อว่าข้อมูลที่ผิดนั้นถูกต้อง - การแสดงอย่างผิดๆ	Cryptographic Technique
	ข้อมูลปลอมลายเซ็น	ของผู้ใช้	

ตารางที่ 2-3 จุดประสงค์การโจมตี

2.17 ทฤษฎีการทดสอบไฟร์วอลล์

1. หลักการทดสอบ Firewall

จุดประสงค์ของการทดสอบก็เพื่อตรวจสอบว่าไฟร์วอลล์ทำงานได้อย่างที่เราต้องการหรือไม่ทำงานอย่างมีประสิทธิภาพเพียงไร โดยควรจะต้องทำสิ่งเหล่านี้วัดความสามารถของไฟร์วอลล์ในด้านต่าง ๆ คือ

- ด้านความปลอดภัย (Security)
- ด้านการจัดการ (Management)
- ด้านประสิทธิภาพ (Performance)
- ฟังก์ชันของไฟร์วอลล์ เช่น
  - การกรองแพ็กเก็ต (packet filtering)
  - การเก็บล็อก (logging)
  - ความสามารถในการแจ้งเตือน (alert capability) เมื่อเกิดเหตุการณ์ผิดปกติ

จากนั้น นำข้อมูลที่ได้ไปทำการเปรียบเทียบข้อเด่นข้อด้อยของไฟร์วอลล์แต่ละตัว

2. ด้านความปลอดภัย (Security)

เป็นด้านที่มีความสำคัญที่สุดในการทดสอบไฟร์วอลล์ เพราะจุดประสงค์ของไฟร์วอลล์ก็คือ การรักษาความปลอดภัย ซึ่งการทดสอบด้านนี้ จะเป็นการตรวจสอบหาจุดบกพร่องในการรักษาความปลอดภัยของไฟร์วอลล์ในการทดสอบความปลอดภัยของผลิตภัณฑ์ไฟร์วอลล์นี้ จะทำการทดสอบ 2 ส่วนด้วยกันคือ

- การทดสอบการโจมตีโดยใช้ Denial of Services (DoS) ซึ่งเป็นการโจมตีที่ทำให้โฮสต์ที่ถูกโจมตีไม่สามารถทำงานได้ตามปกติ แล้วดูว่าไฟร์วอลล์สามารถรับมือกับการโจมตีได้หรือไม่ โดยจะทำการโจมตีไปยังโฮสต์ที่อยู่หลังไฟร์วอลล์ และไฟร์วอลล์โฮสต์แล้วพิจารณาว่า ไฟร์วอลล์มีปฏิกิริยาต่อการโจมตีอย่างไร แจ้งเตือนหรือไม่
- การทดสอบความปลอดภัยโดยใช้การสแกนเพื่อตรวจสอบ(Scanning)ซึ่งเป็นการใช้โปรแกรมจำพวกพอร์ตสแกนเนอร์(PortScanner),โปรแกรมสำรวจช่องโหว่(VunerabilityScanner)ที่จะนำมาใช้ในการทดสอบมีทั้งที่รันบนวินโดว์(Windows-based Scanner) และ ที่รันบนยูนิกซ์(Unix-based Scanner) การสแกนเพื่อตรวจสอบ ต่อไป โดยเราจะพิจารณาว่าเมื่อทำการสแกนโฮสต์ที่ติดตั้งไฟร์วอลล์หรือโฮสต์หลังไฟร์วอลล์แล้วไฟร์วอลล์มีผลอย่างไรกับการสแกนนั้นๆ เช่น ทำให้

สแกนไม่ได้คือไม่มีข้อมูลใดๆตอบสนองกลับกลับไปเลย หรืออาจมีข้อมูลตอบสนองเพียงบางส่วน หรืออาจได้รับข้อมูลตามปกติเหมือนไม่มีไฟร์วอลล์ป้องกันก็เป็นได้

3. ด้านการจัดการ (Management)

การจัดการและการคอนฟิกก็เป็นปัจจัยสำคัญอย่างหนึ่งที่จะต้องคำนึงถึง เพราะการมีระบบไฟร์วอลล์ที่สามารถจัดการ และตั้งค่าได้ง่ายจะทำให้สะดวกสำหรับผู้ดูแลระบบ และยังทำให้เกิดความผิดพลาดน้อยลงในการเซ็ตค่าต่าง ๆ ด้วย ในทางตรงข้าม ถ้ามีความซับซ้อนมากในการจัดการก็อาจจะทำให้เกิดความผิดพลาดในการปรับตั้งค่าให้กับไฟร์วอลล์ ซึ่งจะนำไปสู่ช่องโหว่

ในการโจมตีในการทดสอบด้านการจัดการของผลิตภัณฑ์ไฟร์วอลล์นี้ จะทำการทดสอบ

1. ความยากง่ายในการติดตั้ง มี GUI ช่วยสำหรับการติดตั้งหรือไม่
2. ความยากง่ายในการคอนฟิก มี GUI สำหรับการปรับตั้งค่าหรือไม่

4. ด้านประสิทธิภาพ (Performance)

การวัดประสิทธิภาพของไฟร์วอลล์ ก็เพื่อที่จะทำให้มั่นใจได้ว่า ตัวไฟร์วอลล์จะไม่ไปถ่วงการส่งข้อมูลผ่านทางสายอินเทอร์เน็ตที่ค่อนข้างช้าอยู่แล้วให้ช้าลงไปอีกก่อนจะเริ่มทำการวัดประสิทธิภาพจะต้องทำการ ping ไปที่เครื่องเป้าหมาย (ที่มีไฟร์วอลล์) ก่อน เพื่อให้ CPU มีการทำงานอย่างเต็มประสิทธิภาพก่อน เราจะส่งแพ็กเก็ตไปเรื่อย ๆ จนกระทั่ง CPU utilization เท่ากับ 100 เปอร์เซ็นต์ แล้วเราสามารถพิจารณาประสิทธิภาพของไฟร์วอลล์จากจำนวนแพ็กเก็ตที่ไฟร์วอลล์รองรับได้เมื่อ CPU utilization เท่ากับ 100 เปอร์เซ็นต์

ไฟร์วอลล์ที่มีประสิทธิภาพดี ควรส่งถ่ายข้อมูลได้อย่างรวดเร็ว ไม่ควรเกิดปัญหาคอขวดของเครือข่าย อาจจะวัดโดยใช้ FTP หรือ ping

2.18 ทดสอบฟังก์ชันของไฟร์วอลล์

- **การกรองแพ็กเก็ต (packet filtering)**

เพื่อทำการทดสอบว่าไฟร์วอลล์ทำงานได้ถูกต้องตามที่ต้องการหรือไม่ เป็นไปตามการปรับตั้งค่าของเราหรือเปล่า โดยขั้นตอนแรกต้องตั้งกฎที่จะให้ไฟร์วอลล์ทำตามขึ้นมาก่อน และสำหรับแต่ละกฎจะต้องระบุขอบเขตภายในกฎตัวอย่างกฎเช่น "อนุญาตให้แพ็กเก็ตที่เป็นทีซีพีผ่านจากโฮสต์ใดๆ ไปยังเว็บเซิร์ฟเวอร์ผ่านพอร์ต 80 " เราก็จะแบ่งการทดสอบเป็น 3 ขอบเขตคือ

1. การส่งแพ็กเก็ตที่เป็นทีซีพีไปยังเว็บเซิร์ฟเวอร์ ผ่านพอร์ตน้อยกว่า 80
2. การส่งแพ็กเก็ตที่เป็นทีซีพีไปยังเว็บเซิร์ฟเวอร์ ผ่านพอร์ต 80
3. การส่งแพ็กเก็ตที่เป็นทีซีพีไปยังเว็บเซิร์ฟเวอร์ ผ่านพอร์ตมากกว่า 80

จากนั้นสำหรับแต่ละขอบเขต ก็ให้สร้างการทดสอบที่อยู่ภายในขอบเขตนั้นๆ โดยจะต้องทำการตรวจสอบว่าไฟร์วอลล์จะปฏิเสธหรือส่งต่อทุกๆ แพ็กเก็ตสำหรับแต่ละขอบเขตโดยทั้งนี้ในฟังก์ชัน

- **การเก็บล็อก (logging)**

ทำการตรวจสอบถึงความยากง่ายในการจัดการล็อกไฟล์ เพราะกฎข้อหนึ่งของการบริการความปลอดภัยของระบบก็คือ การจัดให้มีล็อกไฟล์ของระบบ และต้องจัดให้มีการใช้งานข้อมูลที่บันทึกไว้อย่างสม่ำเสมอ และนอกจากนี้ยังต้องมีการจัดการใช้ข้อมูลล็อกไฟล์ได้อย่างมีประสิทธิภาพ เนื่องจากล็อกไฟล์ส่วนมากจะเป็นเท็กซ์ไฟล์ขนาดใหญ่ ซึ่งการหาแนวโน้มสำคัญๆ จากข้อมูลเหล่านี้เป็นเรื่องที่ยาก ดังนั้นจึงควรจะมีเครื่องมือที่จะอ่านข้อมูลภายในล็อกไฟล์เหล่านี้ และสรุปข้อมูลต่างๆ ออกมาแสดงในรูปแบบของกราฟหรือตาราง เพื่อให้สามารถทำความเข้าใจได้ง่ายขึ้นโดยในส่วนนี้ เราจะพิจารณาว่า ไฟร์วอลล์แต่ละตัวมีเครื่องมือที่จะอ่านข้อมูลจากล็อกไฟล์ และทำการสรุปออกมาในรูปกราฟฟิกหรือไม่

- **ความสามารถในการแจ้งเตือน (alert capability)**

โดยตรวจดูว่า ไฟร์วอลล์สามารถเตือนผู้ดูแลระบบ เมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น ได้หรือไม่ โดยจะตรวจสอบว่า สามารถแจ้งเตือนผ่านสื่อดังนี้คือ อีเมลล์, เพจเจอร์, SMS Messageและ ICQ

2.19 การโจมตีโฮสต์หลังไฟร์วอลล์ด้วย DoS

โดยทั่วไปแล้ว การโจมตีเป้าหมายด้วย DoS จะมีจุดประสงค์เพื่อให้เซิร์ฟเวอร์ผู้ให้บริการต่างๆ(เช่น เว็บเซิร์ฟเวอร์ (Web Server)) หยุดทำงาน หรือทำงานได้ช้าลง ซึ่งผู้ดำเนินการเซิร์ฟเวอร์เหล่านี้จะติดตั้งไฟร์วอลล์เอาไว้ และจะให้เซิร์ฟเวอร์ผู้ให้บริการอยู่ในส่วนของ DMZ นั่นหมายความว่าเซิร์ฟเวอร์เหล่านี้เป็นโฮสต์ที่อยู่หลังไฟร์วอลล์

ในการโจมตีเมื่อยิง DoS มาที่เซิร์ฟเวอร์แล้ว เราจะพิจารณาผลที่เกิดขึ้นดังนี้

- อาการของโฮสต์หลังไฟร์วอลล์ที่ถูกยิง (เซิร์ฟเวอร์ผู้ให้บริการ) ซึ่งอาการที่อาจเกิดได้มีดังนี้
  - เครื่องแฮงก์ ต้องบูตเครื่องใหม่
  - เครื่องช้าลงมาก ทำอะไรไม่ได้
  - มีการใช้ซีพียู (CPU Usage) เป็น 100% อยู่ชั่วขณะหนึ่งแล้วกลับสู่สภาพเดิม
  - ไม่มีอาการใดๆเกิดขึ้น
- การแจ้งเตือนของไฟร์วอลล์โฮสต์

2.20 การโจมตีไฟร์วอลล์โฮสต์ด้วย DoS

ในบางครั้งผู้บุกรุกมุ่งโจมตีไปที่เครื่องไฟร์วอลล์ เพื่อทำให้ไฟร์วอลล์หยุดทำงานหรืออ่อนแอลงแล้วจะสามารถเข้าไปหาประโยชน์หรือเข้าไปสร้างความเสียหายที่เน็ตเวิร์ก และโฮสต์ภายในต่อไปได้ ซึ่งประเด็นนี้น่าสนใจที่ว่า ไฟร์วอลล์ที่เราใช้มีการจัดการอย่างไรกับปัญหานี้ ไฟร์วอลล์จะปฏิบัติตนอย่างไรเมื่ออยู่ในภาวะถูกโจมตีด้วย DoSในการโจมตีเมื่อเรายิง DoS ไปที่ไฟร์วอลล์โฮสต์แล้ว เราจะพิจารณาผลที่เกิดขึ้นดังนี้

- ปฏิกิริยาของไฟร์วอลล์โฮสต์ที่ถูกยิง ดังนี้
  - ไฟร์วอลล์คงอยู่ได้และปฏิบัติหน้าที่ได้ตามปกติ
  - ไฟร์วอลล์หยุดการทำงาน แต่ก่อนหยุดไม่สามารถปฏิบัติตามนโยบายป้องกันเน็ตเวิร์กภายในเมื่อพบสิ่งผิดปกติ (เช่น ปิด/เปิดเซอร์วิส)
  - ไฟร์วอลล์หยุดการทำงาน แต่ก่อนหยุดยังสามารถปฏิบัติตามนโยบายป้องกันเน็ตเวิร์กภายในเมื่อพบสิ่งผิดปกติ ไฟร์วอลล์ทำงานได้ช้าลง
- การแจ้งเตือนของไฟร์วอลล์โฮสต์
  - ไฟร์วอลล์โฮสต์มีการแจ้งเตือนว่าถูกโจมตีหรือไม่

2.21 ระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์ (Intrusion Detection System: IDS)

ระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์เป็นกระบวนการตรวจสอบเครือข่ายและระบบคอมพิวเตอร์เมื่อมีการละเมิดกฎการรักษาความปลอดภัยโดยระบบตรวจจับผู้บุกรุกระบบประกอบด้วยหน้าที่หลัก 3 ประการ คือ รวบรวมข้อมูลเหตุการณ์ที่เกิดขึ้นไว้ในเรคอร์ดมีตัววิเคราะห์ในการตรวจจับผู้บุกรุกและส่วนตอบโต้ผู้บุกรุกคำว่า **ผู้บุกรุก** หมายถึง ผู้ที่ชอบหาช่องโหว่ของโปรแกรมและเจาะเข้าไปในระบบคอมพิวเตอร์รวมทั้งหมายถึงแฮ็กเกอร์ คือ ผู้ที่ชอบเข้าไปศึกษาบางสิ่งบางอย่างในระบบ

การพูดถึง Misuse Detection และ Intrusion Detection ข้อแตกต่างระหว่าง 2 อย่าง คือ เราพิจารณาวิเคราะห์ส่วนของเครือข่ายโดยสังเกตถึงกิจกรรมของผู้ใช้งานน่าจะใช้ Misuse Detection แต่ถ้าสนใจการโจมตีจากภายนอกหรือผู้บุกรุกใช้ Intrusion Detection จะเหมาะสมกว่า

ข้อแตกต่างอีกอย่างคือ ถ้าผู้ใช้มีสิทธิในเครือข่ายจะเป็น Misuse Detection แต่ถ้าไม่มีสิทธิเราใช้ Intrusion Detection

1. ความจำเป็นที่ต้องมีระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์

เป็นที่รู้กันดีว่าระบบคอมพิวเตอร์ และเครือข่ายมีการออกแบบที่ไม่ค่อยปลอดภัยมากนักทำให้ผู้บุกรุกมีโอกาสที่จะบุกรุกระบบได้ง่ายแม้ว่ามีไฟร์วอลล์ (Firewall) อยู่แล้วก็ตามแต่ก็ไม่สามารถป้องกันการบุกรุก 100 เปอร์เซ็นต์เนื่องจากไฟร์วอลล์เป็นการป้องกันระหว่างระบบคอมพิวเตอร์ภายในเครือข่าย (Internal networks) กับระบบภายนอก (Internet) หากผู้บุกรุกเป็น คน ภายในไฟร์วอลล์เอง ก็ไม่สามารถป้องกันได้ ดังนั้นการมีไฟร์วอลล์เปรียบเสมือนการมีรั้วกั้นรอบบ้านและระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์เปรียบเสมือนการติดตั้งกล้องวีดีโอคอยตรวจสอบ สิ่งผิดปกติทำให้การป้องกันระบบทำได้ดียิ่งขึ้น

2. ข้อดีและข้อเสียของระบบตรวจจับผู้บุกรุก

ข้อดีของระบบตรวจจับผู้บุกรุก

1. การตอบสนองทันทีทันใด

การวิเคราะห์การบุกรุกนั้น หากเป็นผู้เชี่ยวชาญที่มีความรู้ความเข้าใจด้านเน็ตเวิร์กและโพรโตคอลเป็นอย่างดีก็จะวิเคราะห์ได้โดยอาศัยเครื่องมือเพียงเล็กน้อยเท่านั้น คือ ใช้เครื่องมือทำการจัดเก็บบันทึกข้อมูลทั้งหมด ที่มีการสื่อสารกันบนเน็ตเวิร์ก แล้วนำข้อมูลที่ได้เหล่านั้นมาวิเคราะห์โดยพฤติกรรมและความสัมพันธ์ ก็จะสามารถหาสิ่งผิดปกติที่เกิดขึ้นได้ แต่การวิเคราะห์ในลักษณะดังกล่าวจะกระทำได้ก็ต่อเมื่อได้เกิดเหตุการณ์ไปแล้ว เนื่องจากการวิเคราะห์จะเป็นไปในลักษณะการวิเคราะห์ข้อมูลย้อนหลัง ไม่สามารถจะ

กระทำได้ในทันที ซึ่ง IDS จะช่วยแก้ไขข้อ บกพร่องในส่วนนี้ เพราะ IDS สามารถตรวจจับได้ทันทีที่มีความผิดปกติเกิดขึ้น และช่วยให้ทำการแก้ไขได้ทันท่วงที การทำงานพื้นฐานของ IDS จะเหมือนกับการที่ทำโดยคน เพียงแต่ IDS นั้นทำงานโดยอัตโนมัติและการทำงานอยู่ตลอดเวลาไม่มีหยุดจึงสามารถตอบสนองต่อสิ่งผิดปกติได้รวดเร็วกว่าซึ่งถ้าให้คนมานั่งตรวจจับก็ไม่สามารถทำได้ตลอดเวลา

2. การมีฐานความรู้ของการวิเคราะห์

จากที่ได้กล่าวมาข้างต้น การที่จะตรวจจับสิ่งผิดปกติและแยกแยะกิจกรรมเหล่านั้นออกจากการสื่อสารข้อมูลตามปกติได้นั้นจะต้องอาศัยความชำนาญ และเข้าใจในรูปแบบของการสื่อสารข้อ มูลและการ 2 บุกรุกเป็นอย่างดี นั่นคือทักษะที่จำเป็นของนักวิเคราะห์การบุกรุก (Intrusion Analyst) ซึ่งผู้เชี่ยวชาญในระดับที่จะทำงานเช่นนี้ได้มีไม่มากนัก ประกอบกับเทคนิคและกลวิธีในการบุกรุกหรือก่อกวนนั้นได้พัฒนาขึ้นทุกวันวิธีการตรวจจับและวิเคราะห์จำเป็นต้องพัฒนาตามให้สอดคล้อง กันจึงจะตรวจจับได้อย่างมีประสิทธิผล ซึ่งในส่วนนี้ผู้เชี่ยวชาญเองก็อาจจะทำได้ไม่ดีเท่า IDS สามารถช่วยแบ่งเบาภาระของนักวิเคราะห์ลงได้มาก โดยหากรู้รูปแบบพฤติกรรมแน่ชัดว่าเป็นการมุ่งร้ายก็ให้จัดเก็บข้อมูลรูปแบบเหล่านี้ใน IDS เสีย เมื่อมีกิจกรรมดังกล่าวเกิดขึ้นในเน็ตเวิร์ก IDSก็สามารถตรวจพบได้ทันที และเมื่อค้นพบรูปแบบใหม่ก็จัดเก็บลงใน IDS อีก ทำให้ IDS เสมือนมีฐานความรู้ในการวิเคราะห์การบุกรุกได้ดีในระดับหนึ่ง และขีดความสามารถก็จะเพิ่มขึ้นเรื่อย ๆตามปริมาณของรูปแบบที่เก็บอยู่ในฐานความรู้นั่นเอง หากมีการบำรุงรักษาฐานความรู้ในตัว IDS ได้ดีและนำ IDS ไปใช้ในจุดที่เหมาะสมแล้ว การบุกรุกที่ไม่ใช่เทคนิคใหม่ล่าสุดจริง ๆก็แทบจะไม่สามารถเล็ดรอดสายตา IDSไปได้ ถึงขั้นนี้แล้วแม้ว่าจะเป็น IDS แบบธรรมดา ๆก็มีความสามารถมากกว่าผู้บริหารระบบทั่วไปเสียอีกสำหรับนักวิเคราะห์ แล้วเมื่อมี IDS จะทำให้ไม่ต้องห่วงหน้าพะวงหลัง เพราะการบุกรุกที่สามารถตรวจจับได้ง่าย ๆก็สามารถตรวจพบได้โดย IDS อย่างน้อย IDS ก็ช่วยกลั่นกรองข้อมูลเบื้องต้นได้ในระดับหนึ่งและแบ่งเบาภาระได้พอสมควร

3. การช่วยตรวจสอบข้อบกพร่องของระบบป้องกันอื่น ๆ

เน็ตเวิร์กของผู้ใช้อาจมีการป้องกันการบุกรุกอยู่แล้วโดยใช้ไฟร์วอลล์ (Firewall) อย่างไรก็ตามไฟร์วอลล์มิใช่เครื่องมือที่จะป้องกันการบุกรุกได้โดยอัตโนมัติ จะต้องอาศัยผู้ที่บริหารระบบกำหนดกฎให้เหมาะสมกับการใช้งาน อีกประการหนึ่ง ถึงแม้จะมีการตั้งกฎที่เหมาะสมแล้วก็ตาม แต่กฎเหล่านั้นอาจไม่สามารถป้องกันการบุกรุกได้ การบริหารไฟร์วอลล์ที่ดีก็ควรจะมีการตรวจสอบย้อนหลัง (Audit) และการทดสอบการเจาะระบบ

(Penetration Test) เพื่อเป็นการสอบทานระบบอีกครั้งหนึ่ง IDS สามารถช่วยได้มาก โดยติดตั้ง IDS ไว้หลังไฟร์วอลล์ และทำการทดสอบเจาะระบบด้วยวิธีต่าง ๆเพื่อดูว่าจะมีเทคนิคใดที่สามารถเจาะผ่านไฟร์วอลล์ได้บ้าง และหากมีแพ็กเกจใดผ่านเข้าไปได้ IDSก็จะตรวจพบ ทำให้ผู้บริหารระบบสามารถปรับปรุงกฎให้รัดกุมมาก

2. ข้อเสียของระบบตรวจจับผู้บุกรุก

ถึงแม้ IDS จะมีประโยชน์ค่อนข้างมากในการช่วยรักษาความปลอดภัยและการเตือนภัยล่วงหน้าแต่ก็มีข้อเสียอยู่หลายประการซึ่งผู้ที่จะนำไปใช้จะต้องตระหนักไว้

1. การละเมิดความเป็นส่วนบุคคล

เนื่องจาก IDS มีพื้นฐานจากการนำข้อมูลทั้งหมดที่สื่อสารกันมาทำการวิเคราะห์ ซึ่งข้อมูลเหล่านั้นจะต้องครอบคลุมถึงข้อมูลทั่วไปที่มีการสื่อสารกันตามปกติ และการที่จะทราบว่ามีความผิดปกติหรือไม่นั้นก็จะต้องอ่านข้อมูลทั้งหมดด้วยดังนั้นไม่ว่าจะมีกิจกรรมใดๆที่เกิดขึ้นในเน็ตเวิร์ก ไม่ว่าจะเป็นการท่องเว็บการดาวน์โหลดข้อมูลการแชทคุยกันไอซีคิว อี-เมล์ และกิจกรรมอื่นๆที่สื่อสารข้อมูลผ่านเน็ตเวิร์ก ก็จะสามารถถูกเปิดอ่านได้จาก IDS นั่นหมายความว่า IDS สามารถนำไปใช้ในทางที่ผิดเพื่อละเมิด 3 สิทธิส่วนบุคคลได้ การทำงานของ IDS เปรียบเสมือนการที่ตำรวจต้องการตรวจสอบและดักจับผู้ไม่หวังดีที่คอยโทรศัพท์ก่อกวนชาวบ้านในหมู่บ้าน และเพื่อการนี้ตำรวจจึงต้องทำการดักฟังโทรศัพท์ของทุกคนที่อยู่ในหมู่บ้านนั้น ซึ่งอาจจะมีเพียงหนึ่งในพันที่เป็นผู้ร้าย แต่ตำรวจผู้ทำหน้าที่ดักฟังก็จะรู้ความลับของคนทุกคน บางทีการที่มีคนดักฟังความลับของทุกคนอาจเป็นอันตรายกว่าการโดนผู้ร้ายก่อกวนก็เป็นได้ดังนั้นการนำ IDS มาติดตั้งในเน็ตเวิร์กจะต้องได้รับการอนุมัติจากหน่วยงานอย่างถูกต้องแล้วเท่านั้น และผู้ทำหน้าที่ในด้านนี้จะต้องเป็นผู้ที่ได้รับความไว้วางใจและมีความรับผิดชอบสูงในอันที่จะไม่ละเมิดสิทธิส่วนบุคคลของคนอื่น และหากเห็นข้อมูลใดๆก็จะต้องไม่เปิดเผยข้อมูลเหล่านั้นแก่บุคคลนั้น โดยทั่วไปแล้วการติดตั้งอุปกรณ์ที่สามารถอ่านข้อมูลของผู้อื่นบนเน็ตเวิร์กได้นั้นจะเป็นข้อห้ามอันดับต้นๆในนโยบายรักษาความปลอดภัยเลยทีเดียว สิ่งที่เป็นข้อสังเกต คือ การกระทำในลักษณะนี้ยากต่อการป้องกันในทางเทคนิค ดังนั้นหน่วยงานโดยทั่วไปจึงต้องกำหนดเป็นข้อห้ามในนโยบายความปลอดภัยและมีบทลงโทษสำหรับผู้ที่ละเมิดในขั้นรุนแรง

2. การตอบโต้อัตโนมัติ

IDS ที่มีจำหน่ายอยู่ในท้องตลาดจะมีส่วนหนึ่งที่ให้ผู้ใช้สามารถกำหนดการดำเนินการอย่างหนึ่งอย่างใดเมื่อตรวจพบการบุกรุกเกิดขึ้น เช่น ส่งจดหมายเตือนผู้ดูแลระบบ เรียกวิทยุติดตามตัว ส่งคำสั่งไปยังไฟร์วอลล์เพื่อจำกัดการเข้าออกของข้อมูล และสิ่งที่สำคัญที่สุดซึ่งอาจจะส่งผลเสีย หายใหญ่หลวงต่อเจ้าของได้ก็คือ การโจมตีกลับไปยังต้นกำเนิดของการบุกรุก (counter attack) โดยที่ IDS เองก็จะรู้จักวิธีการโจมตีแบบต่างๆดีอยู่แล้ว จึงมิใช่เรื่องยากเย็นแต่อย่างใดที่จะทำการโจมตีผู้อื่น ผู้ผลิตจึงมักเพิ่มเติมส่วนนี้ให้แก่ IDS เสมือนหนึ่งการติดอาวุธๆไว้ให้ต่อกรกับแฮ็กเกอร์ เลยทีเดียวผู้ดูแลระบบบางส่วนอาจรู้สึกสะใจและ คิดว่าเหมาะสมแล้วกับการโจมตีกลับไปยังแฮ็กเกอร์เหล่านั้นให้หลาบจำจะได้ไม่พยายามมาข้องแวะอีก เป็นนโยบายการรักษาความปลอดภัยแบบตาต่อตาฟันต่อฟัน และเชื่อว่าหากกำหนดให้การโจมตีกลับเป็นไปอย่างอัตโนมัติแล้ว น่าจะทำให้ปลอดภัยมากขึ้น ในค่ำคืนที่เงียบสงบใครจะไปรู้ว่า IDS อาจจะกำลังต่อกรอยู่กับแฮ็กเกอร์ ที่พยายามแอบเข้ามาในระบบอย่างสุดกำลัง และสู้ยิบตาเพื่อรักษามิให้แฮ็กเกอร์ บุกรุกเข้ามาในเน็ตเวิร์กได้ ในโลกแห่งความเป็นจริงแล้วการตัดสินใจว่าผู้ใดเป็นแฮ็กเกอร์ อย่างชัดเจนมิได้ทำได้โดยง่ายและในเวลาอันรวดเร็ว การที่กำหนดให้ IDS ทำการตอบโต้กลับไปในทันทีโดยมีข้อมูล เพียงผิวเผินนั้น นอกจากจะไม่ช่วยให้เน็ตเวิร์กของเราปลอดภัยแล้ว ยังจะทำให้เรากลายไปเป็นแฮ็กเกอร์ ที่คอยโจมตีผู้อื่นเสียเอง ยกตัวอย่างความเสียหาย เช่น

- การวิเคราะห์ผิดพลาดเข้าใจว่ากิจกรรมที่เกิดขึ้นเป็นการบุกรุกและ IDS ก็ดำเนินการโจม ตีกลับไปในทันที กรณีนี้ผู้บริสุทธิ์ก็จะถูกโจมตีจาก IDS ของเราโดยที่ไม่รู้เรื่องใด ๆ
- การวิเคราะห์ถูกต้องแต่แอดเดรสของต้นทางเป็นแอดเดรสปลอมกรณีนี้หาก IDSไม่มีกลไกในการสอบทานแอดเดรสที่มีประสิทธิภาพอาจไม่สามารถแยกแยะได้ว่าต้นทางของการโจมตีแท้จริงนั้นเป็นที่ไหนและเมื่อทำการโจมตีกลับไปก็อาจจะมิใช่ตัวการที่แท้จริงและเหตุการณ์จะเลว ร้ายยิ่งขึ้นหากแอดเดรสที่ปลอมมานั้นเป็นของหน่วยงานทางความมั่นคงหรือหน่วยงานทางทหาร และเมื่อนั้นผู้ดูแลระบบอาจจะตระหนักได้ว่า IDS ตัวเดียวอาจจะทำให้เขาต้องเข้าไปนอนในคุกหลายคืน เทคนิคการปลอมแอดเดรสลักษณะนี้อาจ
เป็นการยืมมือ IDS ของเราไปโจมตีผู้อื่นอีกทอดหนึ่งได้เป็นอย่างดี
- การวิเคราะห์แอดเดรสที่ถูกต้อง และการโจมตีกลับไปก็ตรงไปยังแฮ็กเกอร์ อย่างถูกต้องตามที่ต้องการ แต่ผลที่ได้ก็เพียงอาจจะทำให้แฮ็กเกอร์ หยุดความพยายามไปชั่วขณะเท่านั้น อีกไม่นานก็จะหาวิธีกลับมาใหม่ และไม่เกิดผลใดๆเลย

นอกจากจะเป็นการยั่วยุให้มีความรุนแรงมากขึ้นเท่านั้น สิ่งสำคัญที่ผู้ทำหน้าที่ด้านความปลอดภัยและผู้บริหารระบบควร จะตระหนักไว้ให้จงหนักคือท่านไม่มีสิทธิพิเศษที่จะไปตอบโต้ผู้บุกรุก โดยการโจมตีกลับไม่ว่าในกรณีใด สิ่งที่ท่านจะทำได้ดีที่สุด คือทำระบบให้แข็งแรงมั่นคงและปลอดภัยที่สุดเท่านั้น นั่นคือ ปิดประตูบ้านให้แน่น ตรวจตราอย่างรัดกุมและใช้งานเท่าที่จำเป็น ส่วนผู้ที่กระทำผิดเหล่านั้นควรจะปล่อยให้เป็นไปตามกฎหมายและกระบวนการยุติธรรมจะดีที่สุด เพราะการตอบโต้การกระทำที่ผิดกฎหมายด้วยวิธีที่ผิดกฎหมายจะทำให้เรากลายเป็นจำเลยไปด้วยในที่สุด

3. การเตือนภัยที่ผิดพลาด

ข้อที่ 3 อาจไม่ใช่ข้อเสียที่สำคัญของการใช้ IDS หากผู้ใช้มีความรู้ในการใช้งานที่ดีพอและเข้าใจหลักการวิเคราะห์การบุกรุกของ IDS ได้ดี อย่างที่ได้กล่าวแล้วข้างต้น ก็คือ อาจจะมีกิจกรรมปกติหลายอย่างที่มีลักษณะใกล้เคียงหรือบางครั้งเหมือนกับการพยายามบุกรุก ซึ่งแน่นอนว่าหาก IDS ได้ถูกกำหนดให้ ตรวจจับกิจกรรมประเภทดังกล่าวแล้วก็จะมีการเตือนในทันทีที่ ตรวจพบและเป็นหน้าที่ของนักวิเคราะห์ที่จะทำการสืบค้นข้อมูลด้านอื่นๆ มาประกอบการวินิจฉัยอีกครั้งหนึ่งว่าพฤติกรรมดังกล่าวที่ตรวจพบนั้นเป็นการบุกรุกหรือไม่อย่างไร IDS ที่ถูกกำหนดให้มีความไวเป็นพิเศษมักจะสามารถตรวจจับพฤติกรรมที่ก้ำกึ่งนั้นได้มากเป็นพิเศษ ตัวอย่างเช่น IDS ได้ถูกกำหนดไว้ว่า เมื่อได้รับ Ping Packet จากแอดเดรสเดิมติดต่อกัน 10 แพ็กเกจภายใน 30 วินาที ให้เตือนว่าเป็น การพยายามโจมตีโดยเทคนิค Ping Flood เป็นต้น หากเน็ตเวิร์กดังกล่าวเป็นเน็ตเวิร์กที่ใช้งานโดยวิศวกรระบบและมีการทดสอบการ Ping บ่อย ๆก็อาจจะทำให้ IDS เตือนอยู่แทบตลอด เวลาโดยไม่ได้มีการบุกรุกที่แท้จริงการเตือนโดยมิได้มีการบุกรุกจริงนั้น อาจจะดูเหมือนว่าไม่ส่งผลเสียหายประการใดและน่าจะเกิดประโยชน์เสียด้วยซ้ำเพราะจะทำให้ผู้ดูแลระบบมีความตื่นตัดตลอด เวลาแต่ในความเป็นจริงแล้วธรรมชาติของมนุษย์มีแนวโน้มจะละเลยต่อสิ่งเหล่านี้ หากมีการเตือนแล้ว ไม่มีการบุกรุกจริงบ่อยครั้งเข้าความน่าเชื่อถือของ IDS ก็จะลดลงตามลำดับ และเมื่อมีความพยายามบุกรุกจริงก็จะไม่ได้ให้ความสนใจเท่าที่ควรและไม่ได้หาทางป้องกันอย่างเหมาะสม นั่นคือ IDS จะกลายเป็นเด็กเลี้ยงแกะที่เวลาหมาป่าเข้ามาจริงก็ไม่มีผู้ใดรับฟัง ดูเผิน ๆอาจจะเหมือน ว่ายังดีกว่าการไม่มี IDS เสียเลยแต่การมี IDS อยู่ในระบบโดยไม่ได้นำมาปรับแต่ง อย่างเหมาะสม และเชื่อมั่นว่า IDS สามารถจะคอยระแวดระวังและเก็บหลักฐานต่าง ๆไว้ให้นั้นจะทำให้ผู้บริหารระบบนิ่งนอนใจและคลายความเคร่งครัดในการปฏิบัติงานลง อาจจะถึงขั้นหย่อนยานกว่าการป้องกันในระดับปกติที่ไม่มี IDSได้ นอกจากนี้การปล่อยให้ IDS มีการเตือนอย่างไม่เหมาะสมจะทำให้เกิดข้อมูล

ในลักษณะที่เป็นการบุกรุกจริงและการเตือนผิดพลาดผสมกันอยู่อาจทำให้การเตือนที่เป็นของจริงถูกกลบไปและยากต่อการสังเกต อย่าลืมว่าแฮ็กเกอร์ ที่มีความสามารถจะทิ้งร่องรอยของการบุกรุกไว้เพียงเล็กน้อยอาจจะมีเพียง 2-3 ร่องรอยเท่านั้นที่ IDS สามารถตรวจพบได้ หากร่องรอยเหล่านี้ถูกนำไปผสมปนเปกับการตรวจจับอื่นๆอีกนับพัน ย่อมมีโอกาสสูงที่จะถูกมองเลยไปโดยไม่มีผู้ใดให้ความสนใจ

2.22 พฤติกรรมโดยทั่วไปของผู้บุกรุก

ประกอบด้วยขั้นตอนสำคัญ 3 ขั้นซึ่งจำเป็น และเป็นพื้นฐานทั่วไปของการบุกรุก

1. การแกะรอย (Foot printing)

เป็นการรวบรวมข้อมูลของเครื่องเป้าหมายที่ต้องการให้ได้มากที่สุด โดยเฉพาะช่องโหว่ที่มีอยู่บนเน็ตเวิร์ก ทำให้ทราบโพรไฟล์ (Profile) ของเครื่องเป้าหมายที่เชื่อมต่ออยู่กับอินเตอร์เน็ต (Internet) ทั้งในส่วนของเน็ตเวิร์กภายในหรืออินทราเน็ต (Intranet) และเอ็กซ์ทราเน็ต (Extranet) รวมทั้งการให้บริการการเชื่อมต่อจากระยะไกล (remote access)

ประกอบด้วย 3 ขั้นตอนย่อย ดังนี้

1. กำหนดขอบเขตของการแกะรอย เป็นการพิจารณาว่าต้องการแกะรอยเน็ตเวิร์กทั้งองค์กรหรือสนใจเฉพาะบางส่วนโดยค้นหาข้อมูลจากแหล่งข้อมูลที่เปิดเผยได้ (Open Source Search) ทำให้ทราบข้อมูลบางอย่างที่น่าสนใจได้ เช่นนโยบายด้านการรักษาความปลอดภัย ซึ่งบ่งบอกให้ทราบ ถึงกลไกการรักษาความปลอดภัยที่ใช้งานอยู่ปัจจุบัน ชื่อผู้ติดต่อและอีเมล์แอดเดรสหรือตำแหน่ง ที่ตั้ง
2. การรวบรวมรายละเอียดต่างๆ ของเน็ตเวิร์กเป้าหมาย โดยหาชื่อโดเมนและเน็ตเวิร์กที่เกี่ยวโยงกับเครื่องเป้าหมาย แล้วเรียกใช้โปรแกรม เช่น whois (เป็นโปรแกรมที่ใช้หา ข้อมูลว่า มีใครใช้งานอยู่ในระบบบ้าง) ดูโดเมนเนมของระบบ และค้นหาค่ากำหนดของเครื่องที่ทำงานอยู่ในเน็ตเวิร์ก เช่น ชื่อเครื่อง รุ่นของระบบปฏิบัติการ ชื่อผู้ใช้ทั้งหมดในระบบ
3. การสำรวจเน็ตเวิร์ก โดยพยายามสำรวจเส้นทางที่แพ็กเกจไอพี เริ่มส่งจากเครื่องต้นทางไปถึงปลายทาง

2. การสแกนเพื่อตรวจสอบ

เปรียบเสมือนการเคาะกำแพงเพื่อสำรวจหาประตูบ้านและหน้าต่าง (ช่องโหว่) โดยการแกะรอยจะทำให้ได้ไอพีแอดเดรส และข้อมูลเกี่ยวกับเน็ตเวิร์กของเครื่องเป้าหมายผ่านการทางสอบถามจากฐานข้อมูล whois ส่วนต่อมาคือ ทำการตรวจสอบว่าเครื่องคอมพิวเตอร์ปลายทางใดบ้างที่ เปิด

อยู่และสามารถเข้าถึงได้โดยตรงผ่านทางอินเตอร์เน็ตและถ้าเป็นไปได้ควรทราบด้วยว่า มีหมายเลขพอร์ตใดเปิดอยู่บ้าง โดยการใช้เครื่องมือและเทคนิคต่างๆเช่น ping sweeps, port scans และ automated discovery tool

3. การค้นหาและรวบรวมรายละเอียด (Enumeration)

เป็นการค้นหาบัญชีผู้ใช้หรือค้นหาทรัพยากรที่แชร์ไว้ ซึ่งข้อแตกต่างสำคัญระหว่างเทคนิคการรวบรวมข้อมูลและเบาะแสกับการค้น หาและรวบรวมรายละเอียดต่างๆ คือ ระดับหรือความร้ายแรงของการบุกรุก หมายความว่ามีการเปิดคอนเน็กชันไปยังเครื่องปลายทาง โดยตรงและมีการส่งคำถามถามไปด้วย เมื่อแฮ็กเกอร์ทราบชื่อแอคเคานต์ของผู้ใช้ที่ถูกต้องหรือทราบชื่อแชร์โฟลเดอร์ ผู้บุกรุกจะพยายามทำการคาดเดารหัสผ่าน หรือค้นหาจุดบกพร่องของสิทธิที่เซตไว้ที่แชร์โฟลเดอร์นั้นๆเมื่อผู้บุกรุกสามารถเข้าไปเป็นผู้ใช้ทั่วไปแล้วก็สามารถหาช่องทางขยายสิทธิ์ ให้ได้เป็นผู้ดูแลระบบประเภทของข้อมูลที่แฮ็กเกอร์ต้องการรวบรวบสามารถแบ่งออกเป็น 3 กลุ่มใหญ่ คือรายชื่อทรัพยากรในเน็ตเวิร์ก เช่น ชื่อแชร์โฟลเดอร์, รายชื่อแอคเคานต์ของผู้ใช้และรายชื่อกลุ่ม และ ชื่อแอพพลิเคชัน

2.23 รูปแบบของระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์

1. วิธีเปรียบเทียบพฤติกรรมผู้ใช้กับรูปแบบการบุกรุกที่รู้จัก (Misuse Intrusion Detection)

วิธีเปรียบเทียบพฤติกรรมผู้ใช้กับรูปแบบการบุกรุกที่รู้จักประกอบด้วย การเก็บบันทึกและการระบุรูปแบบของการบุกรุกซึ่งอาจบุกรุกจากจุดอ่อนของระบบหรือการละเมิดกฎรักษาความปลอดภัยโดยมีตัวตรวจจับคอยดูแลกิจกรรมต่างๆที่กระทำในปัจจุบันว่าเหมือนกับพฤติกรรม การบุกรุกที่เคยเกิดขึ้นหรือได้รับรายงานว่าเป็นการบุกรุกหรือไม่ในบางระบบมีการใช้กฎ (Rule-based expert system) โดยตั้งกฎขึ้นจากพฤติกรรมที่น่าสงสัย เช่นการ login ล้มเหลวเกินกว่า 3 ครั้งต่อเนื่องกันในเวลา5นาที ถือว่าพยายามบุกรุกและข้อมูลที่ใช้ตรวจสอบจะถูกนำมาเปรียบเทียบกับกฎ (Rules) ที่มีอยู่สังเกตว่ามีการนำข้อมูลทางเวลาเข้ามาพิจารณาด้วย การตรวจจับการบุกรุกโดยวิธีนี้สามารถมีการแก้ไขกฎหรือเพิ่มกฎได้ในระบบที่เป็นปัญญาประดิษฐ์ (Artificial Intelligence)ระบบอาจทำการแก้ไขกฎหรือเพิ่มกฎได้ด้วยตนเองข้อเสียของวิธีเปรียบเทียบ พฤติ กรรมผู้ใช้กับรูปแบบการบุกรุกที่รู้จัก คือ

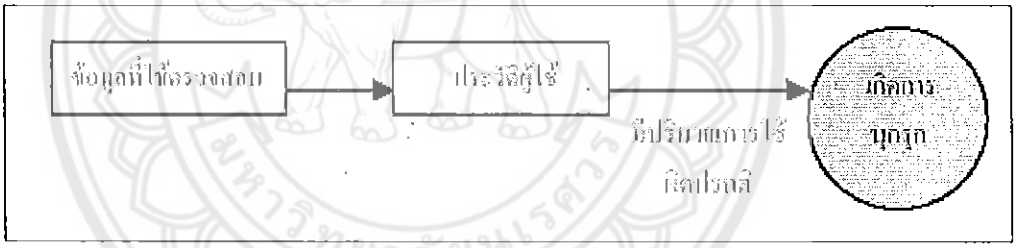
1. ประสิทธิภาพของระบบการตรวจจับชนิดนี้ขึ้นอยู่กับรูปแบบการบุกรุกที่ระบบรู้จัก
2. มีข้อจำกัดในเรื่องจำนวนของรูปแบบในการบุกรุก ซึ่งหากเป็นการบุกรุกที่ระบบไม่รู้จักมาก่อนจะทำให้ไม่สามารถตรวจจับการบุกรุกได้

2. วิธีตรวจสอบการใช้งานระบบที่ผิดปรกติ (Anomaly Intrusion Detection)

วิธีตรวจสอบการใช้งานทรัพยากรระบบที่ผิดปรกติตั้งอยู่บนสมมติฐานว่าการกระทำใดๆ ที่เป็นการบุกรุกจะต้องมีการใช้งานระบบอย่างผิดปรกติ โดยมีกระบวนการเก็บประวัติพฤติกรรมการใช้งานของผู้ใช้ และสังเกตการทำงานเกิดขึ้นของผู้ใช้ว่าเมื่อเข้ามาในระบบได้กระทำสิ่งใดบ้าง แล้วรายงานเก็บเป็นประวัติซึ่งสามารถใช้เป็นข้อมูลตรวจสอบในการนำมาเปรียบเทียบว่าพฤติกรรมในปัจจุบันมีการใช้งานระบบที่ผิดปรกติกว่าประวัติพฤติกรรมของผู้ใช้เดิมมากน้อยเพียงใด หากมีปริมาณการใช้ในปริมาณมากผิดปรกติจึงถือว่าเกิดการบุกรุก

ปัญหาของการตรวจจับโดยวิธีตรวจสอบการใช้งานระบบที่ผิดปรกติ คือ

1. อาจมีพฤติกรรมการใช้งานทรัพยากรระบบของผู้ใช้ที่ผิดปรกติเกิดขึ้นแต่ไม่ได้เป็นการบุกรุกระบบ ทำให้ระบุสถานะผิดพลาด
2. ตรวจไม่พบการบุกรุกระบบเนื่องจากการบุกรุกนั้นไม่ได้ใช้ทรัพยากรระบบอย่างผิดปรกติ
3. หากผู้บุกรุกค่อยๆเปลี่ ยนพฤติกรรมการใช้งานไปทีละเล็ กละน้อยระบบจะไม่ สามารถตรวจจับความผิดปรกติได้มีปริมาณการใช้ผิดปรกติ



รูปที่ 2-26 การทำงานของการตรวจจับผู้บุกรุกโดยวิธีตรวจสอบการใช้งานระบบที่ผิดปรกติ (ที่มา: http://www.thaicert.nectec.or.th/)

วิธีการตัดสินใจของลักษณะการบุกรุก

ใช้สถิติในการวิเคราะห์หาความผิดปกติ (Statistical Anomaly Detection)

จะใช้การเก็บเป็นสถิติจากพฤติกรรมใช้งานปกติ โดยมีตัวแปรที่ต้องสนใจ คือ ยูสเซอร์, กรุ๊ป, เวิร์กสเตชัน, เซิร์ฟเวอร์, ไฟล์ (File), การ์ดเครือข่าย (Network Adapter) และอื่นๆ พื้นฐานคือถ้ามีการใช้งานผิดปกติไปจากเดิมนั่นเองอาทิ เช่น เวลาที่เข้าใช้งานโปรแกรมที่ใช้เป็นต้น

ข้อดี คือ

- เข้าใจได้ง่ายอาศัยสถิติเข้าช่วย
- จำนวนของตัวแปรในรูปแบบที่ใช้ไม่มากนักทำให้ใช้หน่วยความจำในการจัดเก็บน้อย
- สถิติที่ได้ขึ้นอยู่กับเวลาโดยมีการหาค่าเฉลี่ย ค่าน้ำหนัก และตัวแปรภายใน

- พฤติกรรมโดยรวมอย่างง่าย คือ failed login ทำให้ผู้ใช้งานเข้าใจง่าย

ข้อเสีย คือ

- ยังรวมไปถึงข้อมูลที่อาจจะไม่ต้องทำเป็นสถิติด้วย
- รวมค่าจากหลายตัวแปรอาจจะทำให้ได้สถิติไม่ถูกต้อง
- ไม่มีมาตรฐานที่แน่นอนรองรับ
- พฤติกรรมของผู้ใช้งานแต่ละคนไม่เหมือนกัน
- แฮ็กเกอร์ผู้ที่รู้สถิติจะเข้าใจและพยายามหลีกเลี่ยงการตรวจสอบและเปลี่ยนไปใช้วิธีการอื่นแทน
- ผู้โจมตีอาจจะให้หลาย account ในการแสดงพฤติกรรมที่แตกต่างหลีกเลี่ยงการตรวจจับได้
- ค่าเฉลี่ยเวลาที่ใช้ในการแสดงพฤติกรรมเพื่อโจมตีแตกต่างกัน

2.24 ระบบตรวจจับผู้บุกรุกโดยวิธีการตรวจสอบการใช้งานระบบที่ผิดปรกติ

แบ่งออกเป็น 3 ส่วนหลักคือ

1. ส่วนเก็บข้อมูลพฤติกรรมผู้ใช้งาน
2. ส่วนเก็บข้อมูลและวิเคราะห์พฤติกรรมผู้ใช้งาน
3. ส่วนตอบสนองการวิเคราะห์ ทำการรายงานผลการวิเคราะห์เมื่อพบพฤติกรรมการใช้งานที่ผิดปรกติไป

1. ส่วนเก็บข้อมูลพฤติกรรมผู้ใช้งาน

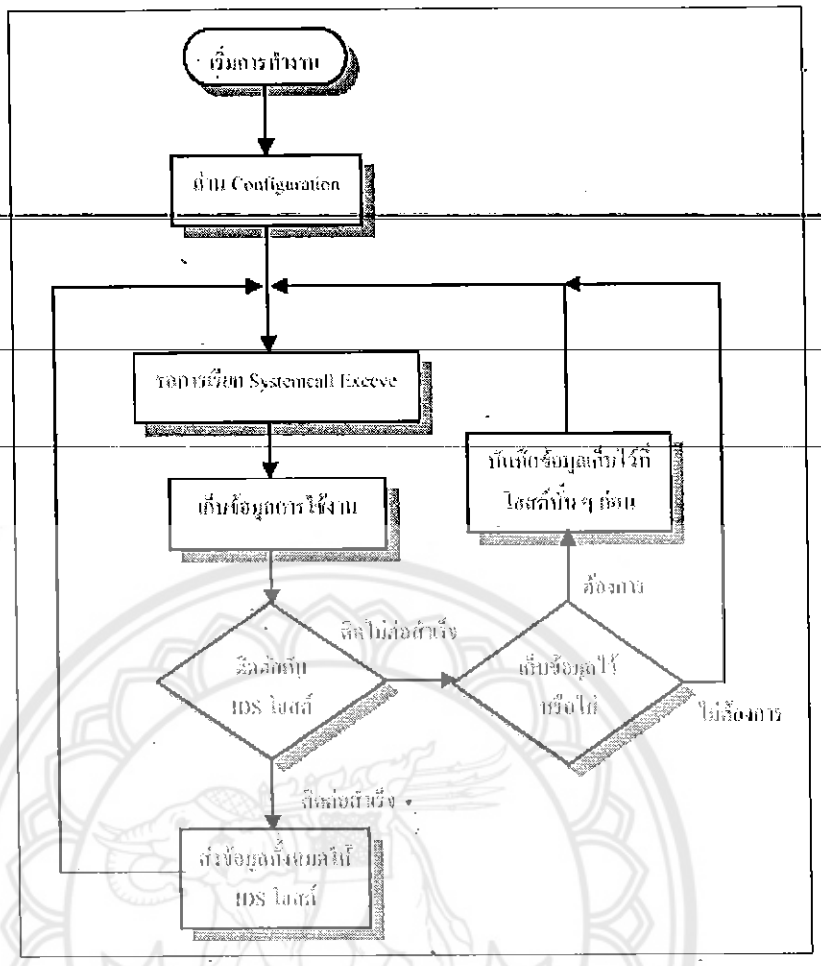
ส่วนเก็บข้อมูลพฤติกรรมผู้ใช้งานจะถูกติดตั้งอยู่ที่โฮสต์ที่ต้องการวางระบบตรวจจับผู้บุกรุกไว้โดยการทำงานคือจะทำการติดตามการใช้งานผ่านทางการเรียกใช้ซิสเต็มคอลล์ execve โดยปรกติซิสเต็มคอลล์ตัวนี้จะถูกเรียกใช้งานเมื่อทำการรันไฟล์โปรแกรมต่างๆ ซึ่งจะมีการส่งทั้งคำสั่งและอาร์กิวเมนต์(argument)ของคำสั่งนั้นๆเข้ามาให้ซิสเต็มคอลล์จากหลักการทำงานดังกล่าวสามารถดักจับข้อมูลการใช้งานของผู้ใช้โดยดูที่ลักษณะของคำสั่งที่ใช้และลำดับการใช้งานของคำสั่งได้ โดยโหลดโมดูลเข้าไปเพื่อทำหน้าที่ดังกล่าวโดยลักษณะการทำงานของโมดูลจะเป็น ไปตาม Flowchart

ลักษณะข้อมูลที่ส่งไปให้ IDS โฮสต์จะเก็บเป็นโครงสร้างดังนี้

```
struct execInfor {
int uid; // หมายเลขประจำตัวผู้ใช้งาน
char pathname[PATH_LEN]; // ตำแหน่งไฟล์ที่เรียกใช้งาน
char command[MAX_COMM_LEN]; // คำสั่งและอาร์กิวเมนต์
unsigned long startTime; // เวลาที่ทำการเรียกคำสั่ง  };
```

หากสังเกตจะพบว่าทั้งๆที่ส่วนของข้อมูลเกี่ยวกับการใช้งานของผู้ใช้นั้นมีมากมายแต่เรานำมาใช้เพียงเท่านี้เพราะส่วนวิเคราะห์ของระบบเราต้องการข้อมูล เพียงแค่นี้เท่านั้นถ้าเราเก็บข้อมูลมากไปก็จะทำให้สิ้นเปลืองทรัพยากรระบบและระบบจะทำงานช้าลงเพราะต้องเก็บข้อมูลทุกๆ คำสั่งที่ใช้งานของผู้ใช้ทุกคนที่กำลังใช้งานอยู่และหากสังเกตในอีกแง่หนึ่งก็จะพบว่าสิ่งที่ทำการเก็บนั้นคล้ายกับข้อมูลที่อยู่ในล็อกไฟล์ pacct แต่ความจริงแล้วต่างกันเพราะ

1. การเก็บข้อมูลคำสั่งที่ใช้งานของล็อกไฟล์ pacct เก็บเฉพาะคำสั่งที่เรียกใช้งานเท่านั้น ข้อมูลที่เหลือเช่น ออปชัน และอาร์กิวเมนต์ต่าง ๆ จะไม่ถูกเก็บไว้ทำให้ได้ข้อมูลพฤติกรรมการใช้งานที่ไม่ครบถ้วน
2. การเก็บข้อมูลใน pacct จะทำขึ้นเมื่อโพรเซสนั้นๆ จบการทำงานแล้วเท่านั้น



รูปที่ 2-27 ขั้นตอนการทำงานของส่วนเก็บข้อมูลพฤติกรรม

(ที่มา: http://www.thaicert.nectec.or.th/)

ดังนั้นเพื่อให้ได้ข้อมูลที่ ใกล้เคียงกับพฤติกรรมผู้ใช้และมีความถูกต้องมากที่สุดและข้อมูลที่ได้มาเป็นข้อมูลที่สามารถใช้ในการวิเคราะห์ได้จริงๆ จึงใช้วิธีการเก็บข้อมูลด้วยการติดตามการทำงานของซิสเต็มคอลล์ดังที่กล่าวมา

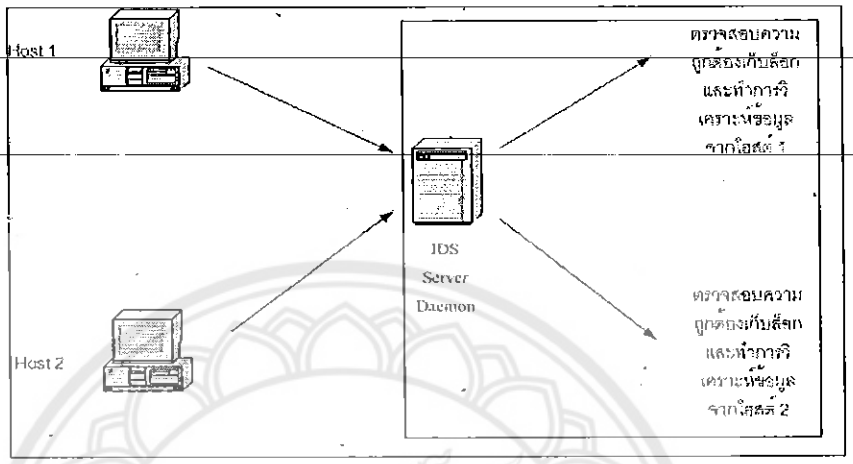
2. ส่วนเก็บข้อมูลและวิเคราะห์พฤติกรรมผู้ใช้งาน

ส่วนเก็บข้อมูลและวิเคราะห์พฤติกรรมผู้ใช้งานจะถูกติดตั้งอยู่ที่ฝั่ง IDS โฮสต์ในส่วนนี้เป็นหน้าที่ของ IDS เดมอนโดยมีหน้าที่ 3 ส่วน คือ

1. ส่วนตรวจสอบความถูกต้องของพฤติกรรมผู้ใช้งาน ทำการตรวจสอบความถูกต้องของข้อมูลที่เก็บใน IDS โฮสต์
2. ส่วนเก็บข้อมูลพฤติกรรมผู้ใช้งาน ทำการรับข้อมูลพฤติกรรมการใช้งานที่ส่งมาจาก

โฮสต์ต่างๆและเก็บไว้ใน IDS โฮสต์

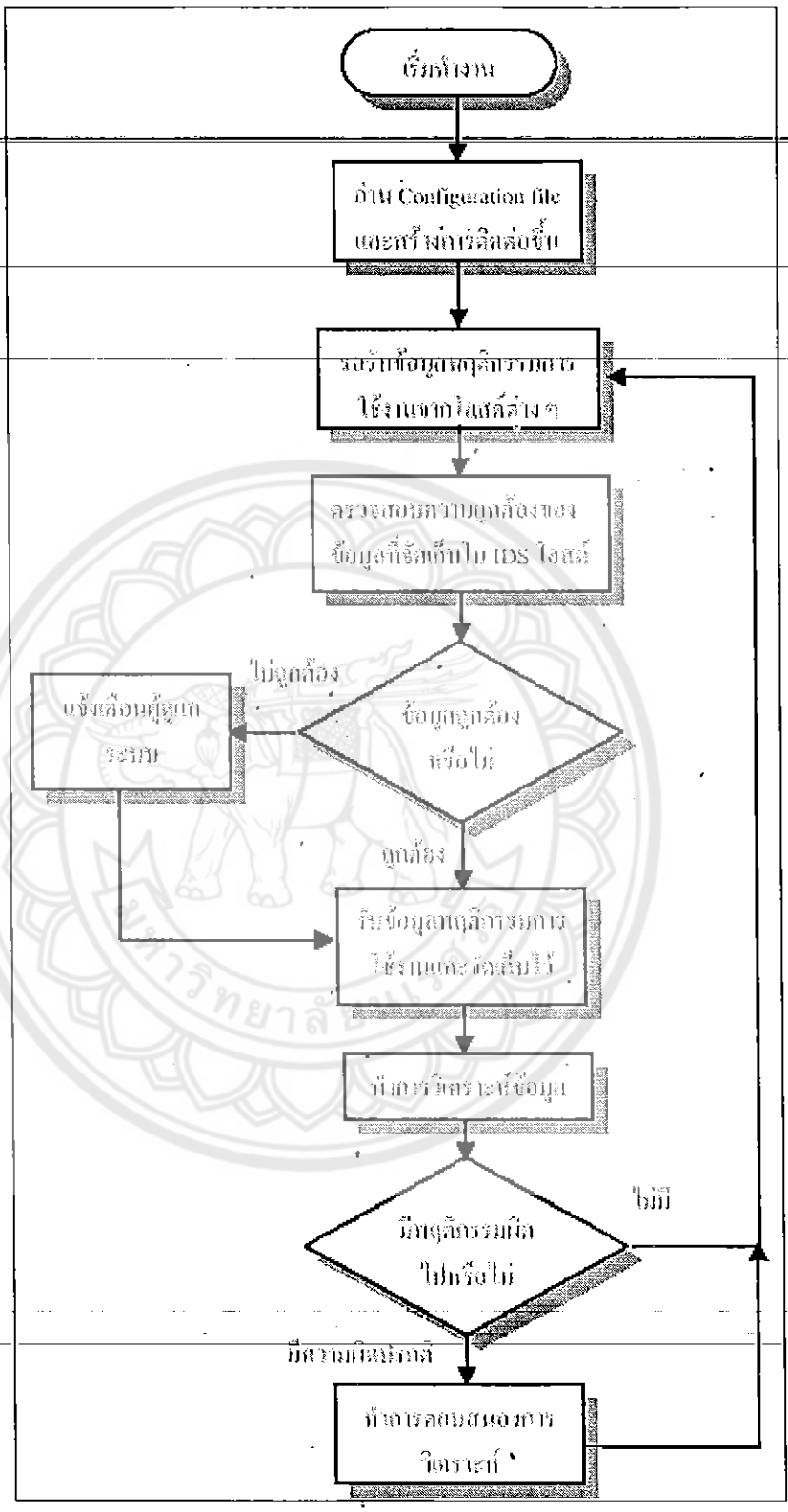
3. ส่วนการวิเคราะห์พฤติกรรมผู้ใช้งาน นำข้อมูลในฐานข้อมูลมาผ่านกระบวนการวิเคราะห์และทำการตอบสนองการวิเคราะห์ โดยส่วนการตอบสนองการวิเคราะห์จะขอแยกหัวข้อออกไป



รูปที่ 2-28 ภาพรวมของส่วนเก็บข้อมูลและวิเคราะห์พฤติกรรมผู้ใช้งาน

(ที่มา: http://www.thaicert.nectec.or.th/)

การทำงานของ IDS เซิร์ฟเวอร์เดมอนมีลำดับการทำงานดังนี้



รูปที่ 2-29 ขั้นตอนการทำงานของส่วนเก็บข้อมูลและวิเคราะห์พฤติกรรมผู้ใช้งาน

(ที่มา: http://www.thaicert.nectec.or.th/)

ส่วนตรวจสอบความถูกต้องของข้อมูลพฤติกรรมผู้ใช้งาน

ในส่วนนี้จะทำการสร้าง MD (Message digest) ของฐานข้อมูลแต่ละคนแยกออกเป็น ไฟล์ออกมาอีกส่วนหนึ่งโดยแต่ละคนก็จะมี MD คนละ 1 ไฟล์ เหตุผลที่ต้องทำ MD ของแต่ละคนแยกกันคนละไฟล์คือ ในส่วนของ MD นี้จะมีการแก้ไขในทุกครั้งที่มีการเก็บข้อมูลใหม่ซึ่งแน่นอนว่าในช่วงเวลาเดียวกันนั้นต้องมีผู้ใช้งานที่ใช้งานพร้อมๆ กันหลายคนดังนั้นถ้าเราทำการรวม MD ของแต่ละคนเข้าเป็นไฟล์เดียวก็จะเกิดปัญหาในการอัปเดทส่วน MD ที่จะใช้งานซ้อนกัน โดยอัลกอริทึมที่ใช้ในการสร้าง MD คืออัลกอริทึม MD5 มีความยาว 128 บิต

ส่วนเก็บข้อมูลพฤติกรรมผู้ใช้

โครงสร้างข้อมูลที่ใช้เก็บข้อมูลพฤติกรรมที่ส่วน IDS โฮสต์มีลักษณะดังนี้

```
struct userLog {
        char pathname[PATH_LEN];
        char command[MAX_COMM_LEN];
        unsigned long startTime;
        };
```

ลักษณะการแยกเก็บข้อมูลนั้นผู้ใช้แต่ละคนที่มาจากแต่ละโฮสต์นั้นจะแยกตามหมายเลขไอพีแอดเดรสและหมายเลขประจำตัวผู้ใช้ที่ส่งมาพร้อมกับข้อมูล ยกตัวอย่างเช่น ข้อมูลพฤติกรรมผู้ใช้ที่มีหมายเลข ประจำตัว 501 มาจากโฮสต์ที่มีหมายเลขไอพีแอดเดรสเป็น 161.246.2.201 ข้อ มูลพฤติกรรมจะถูกเก็บอยู่ในไดเรกทอรีทีมีชื่อเป็น “161.246.10.21” และชื่อไฟล์ “501” โดยข้อ มูลจะถูกเก็บเป็นเรคอร์ดต่อกันไปเรื่อยๆ

ส่วนการวิเคราะห์ข้อมูล

ลักษณะการวิเคราะห์ข้อมูลทำการวิเคราะห์ลักษณะการใช้งานคำสั่งโดยดูจากอาร์กิวเมนต์ และลำดับการใช้งานคำสั่งในส่วนการวิเคราะห์ข้อมูลจะแบ่งเป็น 2 ขั้นตอนคือ

1. ขั้นตอนเตรียมข้อมูลเพื่อการวิเคราะห์

เป็นขั้นตอนที่เตรียมข้อมูลพฤติกรรมที่ รับมาให้อยู่ในรูปแบบที่เหมาะสมและง่ายต่อการวิเคราะห์โดยวิธีการคือนำข้อมูลคำสั่งที่เก็บอยู่ในฟิล์ดข้อมูล command [MAX_COMM_LEN] แล้วแทนที่อาร์กิวเมนต์ที่ไม่ใช่ออปชัน (อาร์กิวเมนต์ที่เป็นออปชันจะขึ้นต้นด้วยตัวอักษร ‘-‘) ด้วยข้อความ “<f>” เหตุผลต้องเปลี่ยนแปลงข้อมูลดังกล่าวออกไปเนื่องมาจากว่าสิ่งที่บอกถึงพฤติกรรมของผู้ใช้งานจะเป็นอาร์กิวเมนต์ที่เป็นออปชันเสียมากกว่า ยกตัวอย่างเช่น เมื่อเราใช้คำสั่ง emacs ซึ่งเป็นโปรแกรมเท็กซ์เอดิเตอร์โดยเรียกจากเชลล์

#emacs –nw a.txt b.txt

ชื่อไฟล์ที่ตามหลังออปชันนั้นจะไม่แทนถึงพฤติกรรมผู้ใช้มากนักเพราะในแต่ละครั้งที่ผู้ใช้เรียกโปรแกรมนี้ขึ้นใช้งานก็มักจะเปลี่ยนชื่อไฟล์ที่เรียก แต่ออปชันยังคงเดิม ดังนั้นจากคำสั่งที่ผู้ใช้งานป้อนเข้ามาเมื่อผ่านส่วนขั้นตอนการเตรียมข้อมูลเพื่อการวิเคราะห์แล้วก็จะได้เป็นข้อความดังนี้ emacs –nw <f> <f> แต่การเตรียมข้อมูลด้วยวิธีนี้ยังมีจุดอ่อนคือมีบางคำสั่งที่ออปชันการใช้งานนั้นอาจไม่ได้ขึ้นต้นด้วยตัวอักษร '-'เช่น คำสั่ง tar เป็นต้น

#tar xvfz global-4.2.tar.gz

เมื่อผ่านขั้นตอนการเตรียมข้อมูลเพื่อการวิเคราะห์ผลลัพธ์ที่ได้คือ tar <f> <f> <f> เห็นได้ว่าออปชัน 'xvfz' นั้นหายไปด้วยเพราะไม่ได้ขึ้นต้นด้วยตัวอักษร '-' แต่อย่างไรก็ตามคำสั่งที่ใช้ออปชันที่ไม่ได้ขึ้นต้นด้วยตัวอักษร '-' มีอยู่เป็นส่วนน้อย

2. ขั้นตอนการวิเคราะห์ข้อมูล

วิธีการที่ใช้วัดค่าความเหมือนจะใช้การวัดค่าความเหมือน (similarity measure) ของข้อมูล โดยค่าค่านี้จะมีค่ามากเมื่อข้อมูลคู่ที่นำมาเปรียบเทียบนั้นมีความคล้ายกันมาก และมีค่าน้อยลงเมื่อข้อมูลคู่นั้นๆ มีความต่างกันออกไปโดยค่ายิ่งมากก็ยิ่งแสดงว่าคล้ายกันมากและในทางกลับกันถ้าข้อมูลมีความต่างกันมากก็จะมีค่าน้อยลง

โดยอัลกอริทึมความเหมือนที่ใช้มีขั้นตอนดังนี้

ให้ Seq1, Seq2 แทนลำดับข้อมูลชุดที่ 1 และ 2 ตามลำดับ

Seqi (i), แทนข้อมูลตัวที่ i ใน Seqj

ให้ c เป็นค่าคงที่มีค่าเริ่มต้นที่ 1 และ Sim แทนค่าความเหมือนมีค่าเริ่มต้นที่ 0

เริ่มขั้นตอนการเปรียบเทียบความเหมือนของลำดับ Seq1, Seq2

1. ในแต่ละตำแหน่งของ i ในลำดับที่ทำการเปรียบเทียบ

- ถ้า Seq1 (i) = Seq2 (i) ให้ Sim:=Sim+c และเพิ่มค่าโดย c:=c+1

- ถ้าไม่เท่ากันให้ค่า c=1

2. หลังจากทุกตำแหน่งทำการเปรียบเทียบแล้วค่า Sim ที่ได้มาคือค่าความเหมือนของลำดับทั้งสอง คะแนนค่าความเหมือนจะมีค่าระหว่าง 0 ถึง n*(n+1)/2 โดย n คือความยาวของลำดับที่ทำการตรวจสอบ ยกตัวอย่างเพื่อให้เห็นภาพได้ชัดขึ้นดังนี้

ให้ Seq1 = { "ls", "- -color", "<f>", "vi" , "<f>"}

และ Seq2 = { "ls", "-p" , "<f>", "cat", "<f>"}

จะได้ค่าความเหมือนของลำดับทั้งสองดังตารางโดยการเปรียบเทียบลำดับทั้งสองดูจากซ้ายไปขวา

Seq1		ls	- -color	<f>	vi	<f>	คะแนนหลังการเปรียบเทียบ
Seq2		ls	-p	<f>	cat	<f>	
C	ค่าเริ่มต้น=1	1	2	1	2	1	-
C	ค่าเริ่มต้น=0	0	1	1	2	2	3

ตารางที่ 2-4 แสดงการคำนวนค่าความเหมือนของลำดับ

จะได้ว่าลำดับทั้งสองนี้มีค่าความเหมือน 3

3. ค่าความเหมือนของลำดับ Seqi ลำดับเดียวกับเซตของลำดับ L ได้ดังนี้

Sim (Seqi, L) = max Seqj L {Sim (Seqi, Seqj)}

หมายความว่าค่าความเหมือนของลำดับ Seqi เมื่อเปรียบเทียบกับเซตของลำดับ L แล้วคือค่า Sim ที่มีค่ามากที่สุดเมื่อทำการเปรียบเทียบ Seqi กับทุกๆ ลำดับในเซต L จากอัลกอริทึมด้านบนได้แสดงให้เห็นว่าในการทำการวิเคราะห์นั้นต้องมีลำดับอยู่ 2 ชุดนำมาเปรียบเทียบกัน เมื่อนำมาเปรียบเทียบกับลักษณะของฐานข้อมูลพฤติกรรมผู้ใช้งานของเราแล้วเราจะแบ่งฐานข้อมูล ออกเป็น 2 ส่วนคือ

1. ฐานข้อมูลการใช้งานในช่วงระยะเวลาปัจจุบัน
2. ฐานข้อมูลการใช้งานในช่วงระยะเวลาที่ผ่านมา

แล้วนำฐานข้อมูลทั้ง 2 มาเปรียบเทียบค่าความเหมือนกันโดยในอัลกอริทึมขั้นตอนที่ 3 จะต้องนำลำดับพฤติกรรมการใช้งานในช่วงระยะเวลาปัจจุบันจำนวน1 ลำดับมาทำการเปรียบ เทียบกับฐานข้อมูลการใช้งานในช่วงระยะเวลาที่ผ่านมาทั้งหมดแล้วหาค่าสูงสุด และเมื่อได้ค่านั้นๆ ก็นำมาบวกเก็บไว้และทำการหาค่าความเหมือนของลำดับต่อไปของฐานข้อมูลการใช้งานในช่วงระยะเวลาปัจจุบันกับฐานข้อมูลการใช้งานในช่วงระยะเวลาที่ผ่านมาทั้งหมด จนกระทั่งสิ้นสุดข้อมูลของฐานข้อมูลการใช้งานในช่วงระยะเวลาปัจจุบัน ค่ารวมที่ได้คือค่าความเหมือนของพฤติกรรมการใช้งานในช่วงระยะเวลาปัจจุบันเทียบกับช่วงระยะเวลาที่ผ่านมา ซึ่งเราใช้ ค่าค่านี้ในการวัดการเปลี่ยนแปลงไปของพฤติกรรมของผู้ใช้ แต่ละคนหากค่านี้มีค่าสูงแสดงว่าพฤติกรรมผู้ใช้คนนั้นๆ ค่อนข้างคงที่ แต่ถ้าหากค่านี้มีค่าต่ำแสดงว่าพฤติกรรมของผู้ใช้มีการเปลี่ยนแปลงและหากมี ค่าต่ำมากจนถึงระดับหนึ่งที่เราตั้งไว้ก็จะแสดงว่าพฤติกรรมผู้ใช้คนนั้นมีพิรุธ เข้าข่ายการบุกรุกจากอัลกอริทึมข้างบนสังเกตได้ว่ามีตัวแปรที่สำคัญอยู่ 4 ตัวแปรคือ

1. จำนวนสมาชิกใน Seq แต่ละ Seq
2. จำนวนข้อมูลที่ใช้เปรียบเทียบจากฐานข้อมูลการใช้งานในช่วงระยะเวลาปัจจุบัน

3. จำนวนข้อมูลที่ใช้เปรียบเทียบจากฐานข้อมูลการใช้งานในช่วงระยะเวลาที่ผ่านมา

4. ค่าต่ำสุดที่ยอมรับได้ของการเปลี่ยนแปลงพฤติกรรม

ซึ่งค่าทั้ง 4 นี้จำเป็นต้องมีการปรับให้เหมาะสมในแต่ละระบบ

3. ส่วนตอบสนองการวิเคราะห์

เป็นส่วนที่ถูกเรียกใช้เมื่อระบบตรวจจับได้ว่ามี ผู้ใช้ที่มีพฤติกรรมเปลี่ยนไปจนถึงระดับที่ผิดปรกติโดยจะแบ่งการทำงานเป็น 2 ประเภทคือ

1. ทำการเก็บล็อกไว้ใน IDS โฮสต์ โดยระบบจะมีอยู่ 2 ชนิดคือ

- Blacklist เก็ บข้อมูลผู้ใช้งานที่เข้าข่ายมีพฤติ กรรมการบุกรุกในขณะนั้นและเมื่อพฤติกรรมของผู้ใช้คนนั้นๆ เปลี่ยนแปลงไปในทางที่ดีขึ้นจนมีค่าพฤติกรรมที่เกินค่าที่กำหนดไว้ก็จะถูกลบออกจากรายชื่อนี้ โครงสร้างของไฟล์นี้จะเป็นเรคอร์ดต่อๆ กัน โดยมีโครงสร้างดังนี้

```
struct blackUser{
int uid; // uid ของผู้ใช้
char hostIP[20]; // หมายเลขไอพีแอดเดรสที่ผู้ใช้ใช้งานอยู่
float score; // ค่าคะแนนการบุกรุก
unsigned long detectTime; // เวลาที่ตรวจพบการบุกรุก }
```

- Eventlist เก็บข้อมูลเหตุการณ์ต่างๆ ทั้งหมดที่เกิดขึ้นเช่นมีผู้ใช้เริ่มมีพฤติกรรมเข้าข่ายการบุกรุกมีผู้ใช้ที่มีพฤติกรรมดีขึ้นที่เปลี่ยนสถานะจากผู้บุกรุกเป็นผู้ใช้ปรกติ มีความผิดพลาดจากการตรวจสอบความถูกต้องของฐานข้อมูลเป็นต้น ไฟล์นี้มีโครงสร้างเป็นเท็กซ์ไฟล์ปรกติ

2. แจ้งเตือนผู้ดูแลระบบ โดยการส่งข้อความเตือนไปยังผู้ดูแลระบบ

บทที่ 3

วิธีดำเนินการศึกษาวิจัย

3.1 วิธีดำเนินการวิจัย

ในการศึกษาค้นคว้า ระบบเครือข่ายคอมพิวเตอร์มหาวิทยาลัยนเรศวร ผู้วิจัยได้กำหนดขั้นตอนการดำเนินการวิจัยตามลำดับ ดังนี้

3.1.1 วิธีการเก็บรวบรวมข้อมูล

1.การเก็บรวบรวมข้อมูลปฐมภูมิ

1.1 เก็บข้อมูลเกี่ยวกับนโยบายด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัยนเรศวรจากคณะสำนักและหน่วยงาน

1.2 เก็บข้อมูลด้านแนวทางการวิเคราะห์ระบบเครือข่าย การเลือกใช้เทคโนโลยีที่เกี่ยวข้องและแนวทางความปลอดภัยของระบบเครือข่ายรวมทั้งปัญหาและอุปสรรคในการพัฒนาระบบเครือข่าย

1.3 เก็บข้อมูลปัญหาและปัจจัยที่ส่งผลกระทบต่อการใช้งานระบบเครือข่ายคอมพิวเตอร์

2.การเก็บรวบรวมข้อมูลทุติยภูมิ

โดยทำการเก็บรวบรวมข้อมูลเพื่อประกอบการวิเคราะห์และออกแบบระบบเครือข่ายคอมพิวเตอร์ดังนี้

2.1 นโยบายการใช้งานคอมพิวเตอร์ภายใต้ระบบเครือข่ายคอมพิวเตอร์

3.1.2 การสร้างเครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล

1.แบบสัมภาษณ์ปากเปล่า (สอบถาม)

การจัดทำแบบสัมภาษณ์ผู้ดูแลระบบเครือข่ายแต่ละ สำนักและหน่วยงานเพื่อสอบถามถึงความคิดเห็นเกี่ยวกับการใช้บริการระบบเครือข่ายคอมพิวเตอร์และความต้องการใช้เทคโนโลยีสารสนเทศของหน่วยงาน

3.2 ขั้นตอนการศึกษาวิจัย

ผู้วิจัยได้กำหนดขั้นตอนการดำเนินงานวิจัย โดยการศึกษาและวิเคราะห์ 2 ขั้นตอนดังนี้

3.2.1 ขั้นตอนการศึกษาวิเคราะห์ระบบงานปัจจุบัน (Existing Systems Analysis) และความต้องการของหน่วยงาน (Requirement Definition)

โดยการศึกษาค้นคว้าจากเอกสารที่เกี่ยวข้อง และการสัมภาษณ์ ผู้ดูแลระบบเครือข่าย และผู้ใช้งานทั่วไป ประกอบด้วย

1. ด้านสถานภาพของระบบเครือข่ายคอมพิวเตอร์
2. ด้านความต้องการใช้งานระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ
3. ด้านการพัฒนาระบบงานด้านสารสนเทศของหน่วยงาน
4. ด้านสถานะภาพปัญหา อุปสรรคและความต้องการใช้งานเทคโนโลยีสารสนเทศ

3.2.2 ขั้นการวิเคราะห์และออกแบบระบบในภาพรวม (Conceptual Analysis and Design)

ทำการวิเคราะห์ระบบเครือข่าย โดยใช้หลักประสิทธิภาพ (Efficiency) ความสามารถในการใช้งานระบบเครือข่าย (Network Availability) ความเชื่อถือได้ของระบบ (Reliability) การมีระบบสำรอง (Redundancy) การคำนึงถึงช่วงเวลาที่สามารถใช้งานระบบเครือข่ายได้ (Network Uptime) การจัดเตรียมข้อมูลให้แก่ผู้ใช้งานระบบ และการคำนึงถึงประสิทธิผลในด้านค่าใช้จ่าย (Cost Effectiveness) รวมทั้งการเก็บค่าสถิติเกี่ยวกับการใช้งาน ซึ่งประกอบด้วย

1. การวิเคราะห์โครงสร้างของระบบเครือข่ายคอมพิวเตอร์โดยกำหนดขอบเขตการวิเคราะห์ออกเป็น 4 ส่วน
2. การออกแบบระบบเครือข่ายคอมพิวเตอร์โดยใช้ข้อมูลจากการศึกษาวิเคราะห์
3. การกำหนดแผนการปรับปรุงและติดตั้งระบบเพื่อสนองความต้องการใช้เทคโนโลยีสารสนเทศของมหาวิทยาลัยในอนาคต

3.3 กรรมวิธีการดำเนินงาน

3.3.1 การศึกษาวิเคราะห์ระบบงานปัจจุบัน (Existing Systems Analysis) และความต้องการของหน่วยงาน (Requirement Definition)

เป็นการสำรวจและศึกษาระบบการทำงานในปัจจุบัน โดยการศึกษาค้นคว้าข้อมูลจากเอกสารที่เกี่ยวข้อง รวมทั้งการสำรวจและสัมภาษณ์เพื่อให้ได้มาซึ่งข้อมูลเพื่อพิจารณาสภาพปัญหาที่ต้องการใช้ระบบเครือข่ายคอมพิวเตอร์มาช่วย รวมทั้งพิจารณาความเหมาะสมของการนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้งานโดยพิจารณาคุณลักษณะของระบบงาน ปัญหาที่เกิดขึ้นและปัจจัยต่างๆที่ประสบแล้วจึงพิจารณาแนวทางในการแก้ปัญหาที่เป็นไปได้ นอกจากนี้ยังทำการกำหนดความต้องการของผู้ใช้ (User) ที่ชัดเจน เป็นการศึกษาความต้องการนำระบบคอมพิวเตอร์มาช่วยงานในระบบงานต่างๆ

บทที่ 4
ผลการวิเคราะห์ข้อมูล

ผลการวิเคราะห์สถานภาพของระบบเครือข่ายคอมพิวเตอร์

4.1 การออกแบบและติดตั้ง

จากการวิเคราะห์ด้านการออกแบบระบบเครือข่ายคอมพิวเตอร์มหาวิทยาลัยนเรศวรพบว่า มหาวิทยาลัย ได้กำหนดให้เกิดการพัฒนาระบบเทคโนโลยีสารสนเทศของหน่วยงานต่างๆอย่างเป็นรูปแบบแนวทางเดียวกัน อันจะนำมาซึ่งความสามารถใช้งานทรัพยากรข้อมูลร่วมกันและแลกเปลี่ยนข้อมูลบนระบบปฏิบัติการเดียวกัน สามารถบริหารและจัดการระบบความปลอดภัยของข้อมูลได้สะดวกและมีประสิทธิ สามารถกำหนดแนวทางในการพัฒนาอย่างต่อเนื่องชัดเจน การออกแบบติดตั้ง NU Net ระยะที่ 1 ถึงระยะที่ 7 มหาวิทยาลัยนเรศวรได้ดำเนินการติดตั้งระบบตามลำดับ ดังนี้

4.1.1 การติดตั้งระบบเครือข่ายคอมพิวเตอร์ระยะที่ 1 (พ.ศ. 2539)

ในปีแรกของการติดตั้งเป็นการวางโครงสร้างพื้นฐานการสื่อสารข้อมูลภายในมหาวิทยาลัยด้วยการดำเนินโครงข่ายสายสัญญาณใยแก้วนำแสง (Fiber Optic) โดยทำการวางเครือข่ายหลัก (ATM Campus Backbone) ความเร็ว 155 Mbps เชื่อมระหว่างอาคารมิ่งขวัญสำนักงานอธีการบดีไปยังคณะหน่วยงานต่างๆรวม 7 กลุ่มอาคาร ดังนี้

1. อาคารมิ่งขวัญ
2. กลุ่มอาคารคณะวิทยาศาสตร์
3. กลุ่มอาคารคณะวิศวกรรมศาสตร์
4. กลุ่มอาคารคณะเกษตรศาสตร์ฯ
5. กลุ่มอาคารคณะเภสัชศาสตร์
6. อาคารคณะมนุษยศาสตร์
7. สำนักหอสมุด

4.1.2 การติดตั้งระบบเครือข่ายคอมพิวเตอร์ระยะที่ 2 (พ.ศ. 2540)

เป็นการติดตั้งระบบการสื่อสารข้อมูลระดับ Building Backbone ด้วยเทคโนโลยี Ethernet ความเร็ว 10 Mbps (LAN) เชื่อมต่อภายในกลุ่มอาคารทั้ง 7 กลุ่ม โดยทำการติดตั้งอุปกรณ์และระบบดังนี้

1. ติดตั้งระบบ Intranet และ Internet เพื่อให้บริการ จำนวน 700 Network Outlets ให้บริการอินเตอร์เน็ตสำหรับคณาจารย์และข้าราชการภายในมหาวิทยาลัยที่ความเร็ว 64 Kbps

2. ติดตั้งระบบ Web Server เพื่อให้บริการข้อมูลของมหาวิทยาลัย
3. ติดตั้งระบบ Electronic Mail Servers สำหรับคณาจารย์และข้าราชการภายในมหาวิทยาลัย
4. จัดตั้งศูนย์ควบคุมระบบเครือข่ายคอมพิวเตอร์ ณ ชั้น 3 อาคารมิ่งขัญญ์
5. จัดตั้งศูนย์บริการให้คำปรึกษาแนะนำการใช้งาน NU Net Help Desk

4.1.3 การติดตั้งระบบเครือข่ายคอมพิวเตอร์ระยะที่ 3 (พ.ศ.2541)

เป็นการเพิ่มขยาย Bandwidth ของเส้นทางการสื่อสาร (Internet Link) จาก 64 Kbps ในภาคเรียนที่ 1 และเพิ่มเป็น 512 Kbps ภาคเรียนที่ 2 โดยมีจุดมุ่งหมายให้บริการอินเตอร์เน็ตแก่นิสิตทุกคนภายในมหาวิทยาลัย และได้ทำการปรับปรุงติดตั้งระบบ ดังนี้

1. ปรับปรุงและติดตั้งระบบเครือข่ายส่วนกลางโดยการเพิ่มจุดสืบค้นและติดตั้งเครื่องคอมพิวเตอร์ให้บริการยังคณะและหน่วยงานต่างๆ
2. ปรับปรุงและติดตั้งระบบเครือข่ายส่วนย่อยคือหน่วยงานและคณะต่างๆรวมทั้งศูนย์วิทยบริการและวิทยาเขตสารสนเทศพะเยา 9 แห่ง
3. จัดทำ Username และ Password เพื่อมอบให้แก่นิสิตทุกคนเพื่อให้สามารถบริการข้อมูล Intranet, Internet และ e-mail โดยมี User ประมาณ 12,000 คน
4. เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์กับระบบเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษาของทบวงมหาวิทยาลัย (Uni Net)
5. จัดการอบรมการใช้งานพร้อมคู่มือการใช้การใช้งานระบบ NU Net
6. ให้บริการ Remote Access คือบริการการใช้ระบบเครือข่ายผ่านหมายเลขโทรศัพท์ รวม 32 คู่สาย โดยนิสิตและบุคลากรทุกคนมีสิทธิ์ใช้งานภายใต้นโยบายของมหาวิทยาลัย

4.1.4 การติดตั้งระบบเครือข่ายคอมพิวเตอร์ระยะที่ 4 (พ.ศ.2542)

ในการติดตั้งระบบเครือข่ายคอมพิวเตอร์ระยะที่ 4 นี้เป็นการติดตั้งเพื่อปรับปรุงระบบการให้บริการมีประสิทธิภาพมากขึ้น และเป็นการติดตั้งขยายบริการไปยังอาคารที่ก่อสร้างใหม่ ดังนี้

1. การปรับเพิ่มขนาดความเร็วในการรับส่งข้อมูลจากเดิม 512 Kbps เป็น 768 Kbps เพื่อรองรับการใช้งานของของ User จำนวน 15,000 คน
2. เพิ่มจำนวนคู่สายบริการ Remote Access จำนวน 32 คู่สาย รวมเป็น 64 คู่สาย
3. เชื่อมต่อระบบเครือข่ายไปยังศูนย์วิทยบริการและสถาบันสมทบ รวม 11 แห่ง
4. ติดตั้งระบบเครือข่ายคอมพิวเตอร์เชื่อมต่อไปยังหอพักข้าราชการและนิสิต

5. ติดตั้งระบบเครือข่ายคอมพิวเตอร์เชื่อมต่อจากคณะวิศวกรรมศาสตร์ไปยังอาคารปฏิบัติการพลังงานแสงอาทิตย์
6. ติดตั้งและขยายจุดให้บริการคอมพิวเตอร์ภายในอาคารต่างๆ

4.1.5 การติดตั้งระบบเครือข่ายคอมพิวเตอร์ระยะที่ 5 (พ.ศ.2543)

ในการติดตั้งระบบเครือข่ายคอมพิวเตอร์ระยะที่ 5 นี้ เป็นการติดตั้งเพื่อปรับปรุงระบบการให้บริการมีประสิทธิภาพมากขึ้น และเป็นการติดตั้งขยายบริการไปยังอาคารที่ก่อสร้างใหม่ ดังนี้

1. ปรับปรุงขนาดความเร็วในการรับส่งข้อมูลจาก 768 Kbps เป็น 1Mbps เพื่อรองรับจำนวน User 18,000 คน
2. เพิ่มจำนวนคู่สายบริการ Remote Access จำนวน 64 คู่สาย รวมเป็น 94 คู่สาย
3. เชื่อมต่อระบบเครือข่ายไปยังศูนย์วิทยบริการและสถาบันสมทบเพิ่มเติม รวมเป็น 13 แห่ง
4. ติดตั้งระบบเครือข่ายคอมพิวเตอร์ไปยังอาคารใหม่ที่ก่อสร้างแล้วเสร็จ จำนวน 3 อาคาร ได้แก่ อาคารคณะวิทยาศาสตร์ใหม่ อาคารคณะแพทยศาสตร์ และ อาคารศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร (CITCOMS)
5. ติดตั้งเครื่องคอมพิวเตอร์ให้แก่คณะและหน่วยงานต่างๆ
6. ติดตั้งและขยายจุดให้บริการคอมพิวเตอร์ภายในอาคารต่างๆ

4.1.6 การติดตั้งระบบเครือข่ายคอมพิวเตอร์ระยะที่ 6 (พ.ศ.2544)

ในการติดตั้งระบบเครือข่ายคอมพิวเตอร์ระยะที่ 6 นี้ เป็นการติดตั้งเพื่อปรับปรุงระบบการให้บริการมีประสิทธิภาพมากขึ้น และเป็นการติดตั้งขยายบริการไปยังอาคารที่ก่อสร้างใหม่ ดังนี้

1.ปรับปรุงขนาดความเร็วในการรับส่งข้อมูลจาก 1Mbps เป็น 1.5 Mbps เพื่อรองรับจำนวน User 22,000 คน
2. เพิ่มจำนวนคู่สายบริการ Remote Access จำนวน 94 คู่สาย รวมเป็น 120 คู่สาย
3. ทำการเชื่อมต่อระบบเครือข่ายไปยังศูนย์วิทยบริการและสถาบันสมทบเพิ่มเติม รวมเป็น 15 แห่ง
4. ทำติดตั้งระบบเครือข่ายคอมพิวเตอร์ไปยังอาคารใหม่ที่ก่อสร้างแล้วเสร็จ จำนวน 3 อาคาร ได้แก่ อาคารกิจกรรม อาคารอเนกประสงค์
5. ติดตั้งเครื่องคอมพิวเตอร์ให้แก่ห้องปฏิบัติการคอมพิวเตอร์คณะต่างๆ
6. ติดตั้งและขยายจุดให้บริการคอมพิวเตอร์ภายในอาคารต่างๆ

7. ทำการย้ายศูนย์ควบคุมระบบเครือข่ายจากอาคารมิ่งขวัญมายังอาคารศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร(CITCOMS)

4.1.7 การติดตั้งระบบเครือข่ายคอมพิวเตอร์ระยะที่ 7 (พ.ศ.2545)

ในการติดตั้งระบบเครือข่ายคอมพิวเตอร์ระยะที่ 7 นี้ เป็นการติดตั้งเพื่อปรับปรุงระบบการให้บริการมีประสิทธิภาพมากขึ้น และเป็นการติดตั้งขยายบริการไปยังอาคารที่ก่อสร้างใหม่ ดังนี้

1.ปรับปรุงขนาดความเร็วในการรับส่งข้อูลจาก 1.5Mbps เป็น 3 Mbps เพื่อรองรับจำนวน User 28,325 คน

2. เพิ่มจำนวนคู่สายบริการ Remote Access จำนวน 150 คู่สาย รวมเป็น 270 คู่สาย
3. ทำการเชื่อมต่อระบบเครือข่ายไปยังศูนย์วิทยบริการและสถาบันสมทบเพิ่มเติม รวมเป็น 16 แห่ง
4. ทำการปรับปรุงและติดตั้งระบบการรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์
5. ติดตั้งเครื่องคอมพิวเตอร์ให้แก่ห้องปฏิบัติการคอมพิวเตอร์คณะต่างๆ
6. ทำการติดตั้งและขยายจุดให้บริการคอมพิวเตอร์ภายในอาคารต่างๆ
7. ทำการติดตั้งระบบปฏิบัติการและระบบสารสนเทศเพื่อการบริหารงาน

4.2 การเลือกใช้เทคโนโลยีที่เกี่ยวข้อง

4.2.1 เทคโนโลยีระบบเครือข่าย

จากการวิเคราะห์ข้อมูลการเลือกใช้เทคโนโลยีที่เกี่ยวข้อง พบว่าการติดตั้งระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย ได้เลือกใช้เทคโนโลยี Asynchronous Transfer Mode (ATM) เพื่อสร้างทางด่วนของข้อมูลที่ความเร็วสูงสุด 155 Mbps (OC-3) เชื่อมทางด่วนข้อมูลด้วยสายเคเบิลใยแก้วนำแสง 12 แกน รวมทั้งการติดต่อกับเครือข่ายระยะไกล (Remote Campus) มีการพัฒนา Gateway เพื่อให้ระบบสามารถพัฒนาถึง Wide Area Network และต่อเชื่อมข้อมูลบนเครือข่ายอินเตอร์เน็ต

ซึ่งจากการศึกษาพบว่าเหตุผลที่เลือกใช้เทคโนโลยี ATM เนื่องจากในปี 2539 ที่เริ่มทำการติดตั้งระบบนั้นมีเทคโนโลยีเพียง 2 แบบให้เลือกคือ FDDI กับ ATM และมหาวิทยาลัยได้เลือกแบบ ATM เนื่องจากเป็นเทคโนโลยีใหม่ล่าสุดที่มีความเร็วขนาด 155 Mbps และสามารถสร้าง Virtual circuit ได้มากกว่า FDDI คือในขนาด 155 Mbps สามารถสร้างท่อการเชื่อมต่อขยายเพิ่มขึ้นได้มากกว่า ส่วน FDDI มีข้อจำกัดด้านความเร็วเพียง 100 Mbps และต้องทำการเชื่อมต่อแบบ Ring จึ่งจะสามารถใช้งานได้สมบูรณ์

4.2.2 ระบบปฏิบัติการ

มหาวิทยาลัยนเรศวรได้เลือกใช้ระบบปฏิบัติการที่มีความสะดวกและง่ายต่อการใช้งาน คือ ระบบปฏิบัติการ Windows NT ซึ่งจากการศึกษาข้อมูลพบว่าเหตุผลที่เลือกใช้เนื่องจากงบประมาณของมหาวิทยาลัยมีจำกัด และข้อจำกัดด้านบุคลากรที่สามารถใช้ระบบปฏิบัติการอื่นได้ จึงเลือกใช้ระบบดังกล่าว ดังจะแสดงผลสำรวจการติดตั้งระบบปฏิบัติการต่าง ๆ ในตารางต่อไปนี้

ลำดับ	หน่วยงาน	ระบบปฏิบัติการ
1	คณะศึกษาศาสตร์	Windows 9x, Windows NT, Windows 2000
2	คณะมนุษยศาสตร์ฯ	Windows 9x, Windows NT, Windows 2000
3	คณะวิทยาศาสตร์	Windows 9x, Windows NT, Windows 2000, Unix,Linux
4	คณะเกษตรศาสตร์ฯ	Windows 9x, Windows NT, Windows 2000
5	คณะเภสัชศาสตร์	Windows 9x, Windows NT, Windows 2000
6	คณะวิศวกรรมศาสตร์	Windows 9x, Windows NT, Windows 2000, Unix,Linux
7	คณะแพทยศาสตร์	Windows 9x, Windows NT, Windows 2000
8	คณะทันตแพทยศาสตร์	Windows 9x, Windows NT, Windows 2000
9	คณะสหเวชศาสตร์	Windows 9x, Windows NT, Windows 2000
10	คณะพยาบาลศาสตร์	Windows 9x, Windows NT, Windows 2000
11	คณะวิทยาศาสตร์การแพทย์	Windows 9x, Windows NT, Windows 2000

ตารางที่ 4-1 แสดงการติดตั้งระบบปฏิบัติการของคณะและหน่วยงาน

ลำดับ	หน่วยงาน	ระบบปฏิบัติการ
12	คณะสถาปัตยกรรมศาสตร์	Windows 9x, Windows NT, Windows 2000
13	สถาบันวิจัยทางวิทยาศาสตร์	Windows 9x, Windows NT, Windows 2000
14	สุขภาพ	Windows 9x, Windows NT, Windows 2000, Unix,Linux
15	สำนักหอสมุด	Windows 9x, Windows NT, Windows 2000
16	ศูนย์ควบคุมระบบเครือข่ายฯ	Windows 9x, Windows NT, Windows 2000
17	วิทยาเขตสารสนเทศพะเยา	Windows 9x, Windows NT, Windows 2000
18	บัณฑิตวิทยาลัย	Windows 9x, Windows NT, Windows 2000
19	ศูนย์วิทยบริการจังหวัด	Windows 9x, Windows NT, Windows 2000
20	กำแพงเพชร	Windows 9x, Windows NT, Windows 2000
21	ศูนย์วิทยบริการจังหวัดแพร่	Windows 9x, Windows NT, Windows 2000
22	ศูนย์วิทยบริการจังหวัดอุตรดิตถ์	Windows 9x, Windows NT, Windows 2000
23	ศูนย์วิทยบริการจังหวัดเพชรบูรณ์	Windows 9x, Windows NT, Windows 2000
24	ศูนย์วิทยบริการจังหวัดสุโขทัย	Windows 9x, Windows NT, Windows 2000
25	ศูนย์วิทยบริการจังหวัดตาก	Windows 9x, Windows NT, Windows 2000
26	ศูนย์วิทยบริการจังหวัดอุทัยธานี	Windows 9x, Windows NT, Windows 2000
27	ศูนย์วิทยบริการจังหวัดนครสวรรค์	Windows 9x, Windows NT, Windows 2000
28	ศูนย์วิทยบริการจังหวัดเชียงใหม่	Windows 9x, Windows NT, Windows 2000
29	ศูนย์วิทยบริการจังหวัด	Windows 9x, Windows NT, Windows 2000
30	ศูนย์วิทยบริการจังหวัด โรงพยาบาลพุทธชินราช พิษณุโลก	Windows 9x, Windows NT, Windows 2000
31	วิทยาลัยพยาบาลบรมราชชนนี	Windows 9x, Windows NT, Windows 2000
32	พุทธชินราช	Windows 9x, Windows NT
	โรงพยาบาลอุตรดิตถ์	
	วิทยาลัยพยาบาลบรมราชชนนี อุตรดิตถ์	

ตารางที่ 4-1 แสดงการติดตั้งระบบปฏิบัติการของคณะและหน่วยงาน(ต่อ)

4.2.3 หลักและวิธีการวางระบบแบบกระจายศูนย์

1. การแบ่งจำนวน Server ในแต่ละคณะ ขึ้นอยู่กับความจำเป็นในการใช้งาน และจำนวนผู้ใช้ (User) ของแต่ละคน

2. ทำการแยก Windows Networking Domain ออกเป็นระดับคณะ (Faculty Network) เพื่อทำการกระจายบริหาร ระบบออกไปสู่หน่วยงานย่อย และในแต่ละคณะจะมีผู้ควบคุมระบบเครือข่ายเป็นของตนเอง โดยมี Internet Domain เป็น "nu.ac.th" และระดับคณะจะกำหนดเป็น Sub Domain เช่น คณะวิศวกรรมศาสตร์ เป็น "eng.nu.ac.th"

3. ในแต่ละ Windows Networking Domain จะติดตั้ง Web Server เป็นของตนเอง และ URL อ้างอิงตาม Domain และ Sub-domain เช่น http://www.eng.nu.ac.th

4. กระจายการบริหารออกเป็นระดับคณะ(Faculty Network) โดยใช้ e-mail Address เป็นระบบเดียวกัน คือ user@nu.ac.th และมีการติดตั้งระบบ Web Base e-mail ให้บริการด้วย

4.3 การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานภายใน

4.3.1 การจัดแบ่ง Windows Networking Domain Name

ระบบเครือข่ายคอมพิวเตอร์ภายในมหาวิทยาลัย มีการติดตั้งระบบเครือข่ายและอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่าย ระบบปฏิบัติการ และระบบการสื่อสาร E-mail ให้บริการทุกกลุ่มอาคารและศูนย์ควบคุมเครือข่ายคอมพิวเตอร์ตั้งอยู่ ณ สำนักงานอธิการบดี เชื่อมเข้าสู่กลุ่มอาคารต่าง ๆ รวมทั้งศูนย์วิทยบริการ สถาบันสมทบ และวิทยาเขต โดยมีการแบ่ง Windows Networking Domain Name ตามคณะและหน่วยงานหลักดังตาราง ซึ่งในรายงานการวิจัยฉบับนี้จะเรียกว่า "Domain Name"

Domain Name	หน่วยงานภายใต้ Domain Name
President	หน่วยงานในสังกัดสำนักงานธิการบดี
Agriculture	คณะเกษตรศาสตร์ทรัพยากรธรรมชาติ และสิ่งแวดล้อม
Education	คณะศึกษาศาสตร์
Engineering	คณะวิศวกรรมศาสตร์
Human social	คณะมนุษยศาสตร์และสังคมศาสตร์
Pharmaceutical	คณะเภสัชศาสตร์
Science	คณะวิทยาศาสตร์
Medicine	คณะแพทยศาสตร์ และวิทยาศาสตร์การแพทย์ คณะทันตแพทย์ศาสตร์ คณะสหเวชศาสตร์ และคณะพยาบาลศาสตร์
Payao	วิทยาเขตสารสนเทศพะเยา
SERT	ศูนย์วิจัยและฝึกอบรมพลังงานแสดงอาทิตย์
Naresuan	ตั้งขึ้นใหม่เพื่อรองรับนโยบายการรวมศูนย์ ตั้งแต่ปีการศึกษา 2545 เพื่อให้บริการทุกหน่วยงานภายในมหาวิทยาลัย

ตารางที่ 4-2 แสดงการแบ่ง Windows Networking Domain Name

ที่	Domain	ชื่อเครื่อง Server	ลักษณะของ Software	รายละเอียด
1	Agriculture	agi-01-svr	NOS : windows NT 4.0 Server	ทำหน้าที่เป็น Primary Domain Controller
		agi-02-msg	NOS : windows NT 4.0 Server	ทำหน้าที่ Backup Domain Controller, Mail Server, Web Server
			App. : Exchange 5.5 Server	
			And Internet Information Server	
			NOS : Windows 2000 Server	ทำหน้าที่ Proxy Server
		agi-03-prx	App. : Proxy 2.0 Server	เครื่องบริการเฉพาะทาง
		agi-04-map	Windows 2000 server	
			NOS : windows NT 4.0 primary	ทำหน้าที่เป็น Primary Domain Controller และ Mail Server
2	Education	edu-01-svr	App. : Exchange 5.5 Server	
			NOS : windows NT 2000 server	ทำหน้าที่เป็น Backup Domain Controller และ Web Server
		edu-02-svr	App. : Internet Information Server	
			NOS : windows NT 2000 Server	ทำหน้าที่เป็น Proxy Server
		edu-03-prx	App. : Proxy 2.0 Server	
			NOS : windows NT 2000 Server	ทำหน้าที่เป็น Media Server
		edu-media-svr	App. : Real Server	

ตารางที่ 4-3 แสดงรายการเครื่องคอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการที่ให้บริการในแต่ละ Windows networking domain

ที่	Domain	ชื่อเครื่อง Server	ลักษณะของ Software	รายละเอียด
3	Engineering	eng-01-svr	NOS : windows NT 4.0 Server	ทำหน้าที่เป็น Primary Domain Controller
			NOS : windows NT 4.0 Server	
		eng-02-msg	App. : Exchange 5.5 Server	ทำหน้าที่ Backup Domain Controller และ Mail Server
			NOS : Windows NT 2000Server	
		eng-03-prx	App. : Proxy 2.0 Server	ทำหน้าที่ Proxy Server
4	Human social	hss-o1-svr	NOS : windows NT 4.0 Server	ทำหน้าที่เป็น Primary Domain Controller
			NOS : windows NT 4.0 Server	
		hss-02-msg	App. : Exchange 5.5 Server	ทำหน้าที่เป็น Backup Domain Controller และ Mail Server
			NOS : windows NT 4.0 Server	
		hss-04-svr	App. : Apache	ทำหน้าที่เป็น Backup Domain Controller และ Web Server
5	Medicine	data-01	NOS : windows NT 4.0 Server	
			NOS : windows NT 4.0 Server	ทำหน้าที่เป็น Proxy Server
		med-01-svr	App. : Internet Information Server	
			NOS : windows NT 4.0 Server	
		med-02-msg	App. : Exchange 5.5 Server	ทำหน้าที่เป็น Mail server

ตารางที่ 4-3 แสดงรายการเครื่องคอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการที่ให้บริการในแต่ละ Windows networking domain (ต่อ)

ที่	Domain	ชื่อเครื่อง Server	ลักษณะของ Software	รายละเอียด
		med-04-net	NOS : windows NT 2000Server App. : Proxy 2.0 Server	ทำหน้าที่ Proxy Server
		med-05-net	NOS : windows NT 2000Server App. : Proxy 2.0 Server	ทำหน้าที่ Proxy Server
		med-2000-svr	NOS : windows NT 2000Server	ทำหน้าที่ Proxy Server
		NS	NOS : windows NT 4.0 Server	ทำหน้าที่เป็น Primary Domain Controller
6	Payao	py-01-svr	NOS : windows NT 2000Server	ทำหน้าที่เป็น Master Domain Controller
		py-02-svr	NOS : windows NT 2000Backup App. : Exchange 2000 Server	ทำหน้าที่เป็น Domain Controller และ Mail Server
		py-03-svr	NOS : windows NT 2000Server App. : ISA 2000 Server	ทำหน้าที่เป็น Proxy Server
7	Pharmaceutical	Graduate	NOS : windows NT 4.0 Server	ให้บริการข้อมูลแก่นิสิตระดับปริญญาโท
		Monkey	NOS : windows NT 4.0 Server	ให้บริการเก็บข้อมูลในคณะ
		pha-01-svr	NOS : windows NT 4.0 Server App. : Internet Information Server	ทำหน้าที่เป็น Primary Domain controller และ web server

ตารางที่ 4-3 แสดงรายการเครื่องคอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการที่ให้บริการในแต่ละ Windows networking domain (ต่อ)

ที่	Domain	ชื่อเครื่อง Server	ลักษณะของ Software	รายละเอียด
			NOS : windows NT 4.0 Server	
		pha-02-msg	App. : Exchange 5.5 Server	ทำหน้าที่เป็น Backup Domain Controller และ Mail Server
		pha-03-svr	NOS : windows NT 4.0 Server	
			NOS : windows NT 2000Server	
		pha-05-prx	App. : Proxy 2.0 Server	
		phadbms	NOS : windows NT 4.0 Server	
			NOS : windows NT 2000Server	
8	Science	is	App. : Internet Information Server	
		sci-01-svr	NOS : windows NT 4.0 Server	
			NOS : windows NT 4.0 Server	
		sci-02-msg	App. : Exchange 5.5 Server	
			NOS : windows NT 2000Server	
		sci-03-prx	App. : Proxy 2.0 Server	
			NOS : windows NT 2000 Server	
		sci-04-svr	App. : Exchange 5.5 Server	

ตารางที่ 4-3 แสดงรายการเครื่องคอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการที่ให้บริการในแต่ละ Windows networking domain (ต่อ)

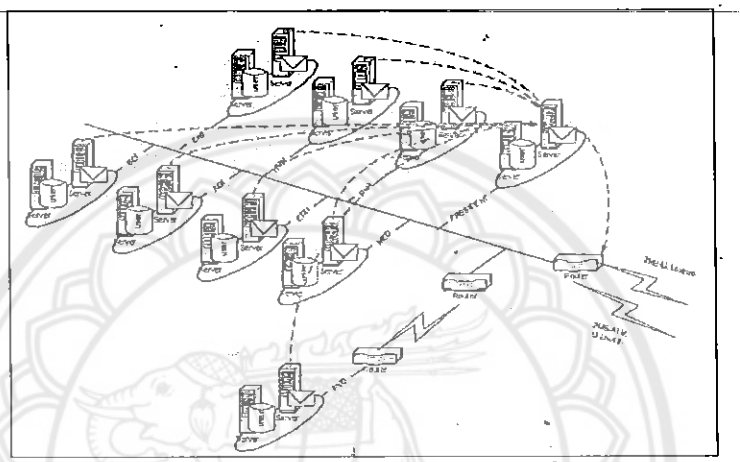
ที่	Domain	ชื่อเครื่อง Server	ลักษณะของ Software	รายละเอียด
9	SERT		NOS : windows NT 4.0 primary App.: Internet Information Server	ทำหน้าที่เป็น wab server
10	President		NOS : windows NT 4.0 primary App.: Steel Belt Radius	ทำหน้าที่เป็น domain controller และ RADIUS Server
			NOS: windows NT 2000server App.: SQL 7.0 Server	ทำหน้าที่เป็น Proxy Server
			NOS: windows NT 2000server App.: Internet Information Server	ทำหน้าที่เป็น Wab server สำหรับกองบริการ
			NOS: windows NT2000server App.: DNS, WINS, DHCP (came with NOS)	ทำหน้าที่เป็น DNS, WINS, DHCP เพื่อให้บริการภายในเครือข่าย
			NOS: windows NT 2000server App.: ISA 2000 Server	ทำหน้าที่เป็น Proxy และ Firewall ภายในเครือข่าย
			NOS: windows NT 2000server App.: Proxy 2.0 Server	ทำหน้าที่เป็น Proxy Server
			NOS: windows NT 4.0 server App.: Proxy 2.0 Server	ทำหน้าที่เป็น Proxy Server ภายนอกเครือข่าย

ที่	Domain	ชื่อเครื่อง Server	ลักษณะของ Software	รายละเอียด
			NOS : windows NT 4.0 server.	
		Oop-02-msg	App.: Exchange 5.5 server	ทำหน้าที่เป็น mail Server
			NOS : windows NT 4.0 server	
		Oop-05-svr	App.: Steel belt radius	
			NOS: windows NT 2000server	ทำหน้าที่เป็น Radius Server สำหรับหอพักหญิง
		Oop-08-str	App.: Steel Belt Radius	
		Oop-13-ip	NOS: windows NT 4.0 Server	NT Server (วิทยาเขตสารสนเทศพะเยา(
			NOS: windows NT 4.0 Server	
		www-01-svr	App.: Internet Information Server	ทำหน้าที่เป็น Wab server หลักของมหาวิทยาลัย
			NOS: windows NT4.0 Server	
		www-02-mail	App.: Internet Information Server	ทำหน้าที่เป็น Web Server สำหรับนิสิต
		www-03-mail	NOS: windows NT4.0 Server	เป็น Web base Email
		www-04-svr	NOS: windows NT2000server	ทำหน้าที่เป็น File server
			NOS: windows NT2000server	
		lib-01-svr	App.: Internet information server	ทำหน้าที่เป็น Web Server สำหรับสำนักหอสมุด
			NOS: windows NT 2000server	
		lib-02-prx	App.:ISA 2000 Server	ทำหน้าที่เป็น Proxy Server
11	Naresuan	nu-phs-1 and nu-phs-2	NOS: windows NT 2000server	ACD and ADC backup + Exchange 2000 Server

ตารางที่ 4-3 แสดงรายการเครื่องคอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการที่ให้บริการในแต่ละ Windows networking domain (ต่อ)

4.3.2 การให้บริการภายในระบบเครือข่ายคอมพิวเตอร์แบบท้องถิ่น (Local Area Network) ของมหาวิทยาลัยนเรศวร

มหาวิทยาลัยนเรศวรได้จัดบริการระบบเครือข่ายคอมพิวเตอร์แบบท้องถิ่น โดยแบ่งแยก Windows Networking Domain ตามคณะ/หน่วยงาน และทำการเชื่อมโยง Domain (Trust Domain) แต่ละ Domain เข้าด้วยกัน ดังรูปต่อไปนี้



รูปที่ 4-1 แสดงการเชื่อมโยง Domain (Trust Domain)
(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

4.3.3 ระบบการพิสูจน์ตัวตนของผู้ใช้งาน (Authentication System)

ระบบเครือข่ายคอมพิวเตอร์ (Nu Net) ได้ใช้ระบบการพิสูจน์ตัวตนของผู้ใช้งาน (Authentication System) ของ Microsoft Windows NT 4.0 Server โดยแบ่งการให้บริการออกเป็น 11 Windows Networking Domain เพื่อให้บริการแลกเปลี่ยนข้อมูลและการสื่อสารระหว่างกันของผู้ใช้บริการ

4.3.4 ระบบการให้บริการจดหมายอิเล็กทรอนิกส์ (E-mail)

ระบบการให้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) บนระบบเครือข่ายของมหาวิทยาลัยนเรศวร ได้ดำเนินการให้บริการผ่านระบบปฏิบัติการของ Microsoft Exchange 5.5 โดยทำการกระจายการให้บริการไปตามหน่วยงานหรือ Domain โดยแยก Windows Networking Domain ละ 1 ระบบ (Exchange's Site)

4.3.5 ลักษณะการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์

ปัจจุบันมหาวิทยาลัย มีศูนย์กลางการเชื่อแต่ละระบบเครือข่ายคอมพิวเตอร์ 2 แห่ง คือ อาคารมิ่งขวัญ และอาคารศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร (CITCOMS) ซึ่งอาคารมิ่งขวัญจะเชื่อมต่อกับคณะ/หน่วยงานต่าง ๆ ด้วยเทคโนโลยี ATM และอาคาร CITCOMS ซึ่งจะเชื่อมต่อกับคณะวิชาต่าง ๆ ด้วยเทคโนโลยี Gigabit Ethernet รวมทั้งทำหน้าที่เชื่อมต่อให้บริการไปยังศูนย์วิทยบริการวิทยาเขตสารสนเทศ โดยมีจำนวนเครื่องคอมพิวเตอร์ใช้งาน และให้บริการภายในเครือข่ายประมาณ 4,175เครื่อง

ในศึกษาวิเคราะห์สถานภาพระบบเครือข่ายคอมพิวเตอร์ขึ้น จะแบ่งกายวิเคราะห์ออกเป็นกลุ่มสาขาวิชา ตามรูปแบบการบริหารจัดการของมหาวิทยาลัย 3 กลุ่มสาขาวิชา และหน่วยงานในสังกัดสำนักงานอธิการบดี ดังนี้

1) กลุ่มสาขาทางด้านมนุษยศาสตร์และสังคมศาสตร์
2) กลุ่มสาขาวิชาทางด้านวิทยาศาสตร์สุขภาพ
3) กลุ่มสาขาวิชาทางด้านวิทยาศาสตร์เทคโนโลยี
4) หน่วยงานสังกัดสำนักงานอธิการบดี

กลุ่มสาขาวิชา	สถานภาพการเชื่อมต่อ
กลุ่มสาขาวิชาทางด้านมนุษยศาสตร์และสังคมศาสตร์	ประกอบด้วย 3คณะวิชา - คณะมนุษย์ศาสตร์ฯ ต่อเชื่อมกับศูนย์กลางเครือข่ายอาคารมิ่งขวัญ - ด้วย ATM จำนวน 1link - คณะศึกษาศาสตร์ ต่อเชื่อมกับศูนย์กลางเครือข่ายอาคาร CITCOMS ด้วย GB Ethernet 1 Link และอาคารมิ่งขวัญ ด้วย ATM 1 link - บัณฑิตวิทยาลัยต่อเชื่อมกับ ศูนย์กลางระบบเครือข่ายผ่าน คณะศึกษาศาตร์ ด้วย Fast Ethernet - ศูนย์วิทยบริการ และสนับสนุนสมทบ 15 แห่ง เชื่อมต่อกับศูนย์กลางระบบเครือข่ายผ่านวงจรสื่อสารความเร็วสูง (Frame Relay) ของการสื่อสารแห่งประเทศไทย

กลุ่มสาขาวิชา	สถานภาพการเชื่อมต่อ
กลุ่มสาขาวิชาทางด้านวิทยาศาสตร์สุขภาพ	ประกอบด้วย 7คณะวิชา - คณะทันตแพทยศาสตร์ และคณะพยาบาลศาสตร์ - คณะเภสัชศาสตร์ และสหเวชศาสตร์ คณะวิทยาศาสตร์การแพทย์ และสถาบันวิจัยทางวิทยาศาสตร์สุขภาพ เชื่อมต่อกับ ศูนย์กลางระบบเครือข่ายอาคารมิ่งขวัญ ด้วย ATM จำนวนคณะละ 1 Link - คณะแพทยศาสตร์ เชื่อมต่อกับศูนย์กลางระบบเครือข่ายอาคารมิ่งขวัญ ผ่านคณะวิทยาศาสตร์การแพทย์ด้วย Fast Ethernet
กลุ่มสาขาวิชาทางด้านวิทยาศาสตร์เทคโนโลยี	ประกอบด้วย 4คณะวิชา - คณะเกษตรศาสตร์ฯ เชื่อมต่อศูนย์กลางเครือข่ายอาคารมิ่งขวัญ ด้วย ATM 1 Link เชื่อมกับอาคาร CITCOMS ด้วย GB Ethernet 1 Link - คณะวิศวกรรมศาสตร์ เชื่อมต่อกับศูนย์กลางระบบเครือข่ายอาคารมิ่งขวัญด้วย ATM จำนวน 1 Link - คณะสถาปัตยกรรมศาสตร์ เชื่อมต่อกับศูนย์กลางระบบเครือข่ายผ่านคณะวิศวกรรมศาสตร์ ด้วย Fast Ethernet - คณะวิทยาศาสตร์ เชื่อมต่อกับศูนย์กลางระบบเครือข่าย ผ่านคณะวิศวกรรมศาสตร์ ด้วย ATM จำนวน 1 Link
หน่วยงานสังกัดสำนักงานอธิการบดี	- ประกอบด้วยหน่วยงานในสังกัดสำนักงานอธิการบดี - อาคารมิ่งขวัญ เป็นศูนย์กลางระบบเครือข่ายเชื่อมต่อกับคณะวิชาต่างๆด้วยเทคโนโลยี ATM แล้วเชื่อมต่อไปยัง CITCOMS เพื่อทำหน้าที่เป็น Backup Link - อาคาร CITCOMS เป็นศูนย์กลางระบบเครือข่ายเชื่อมต่อกับคณะวิชาต่าง ๆด้วยเทคโนโลยี GB Ethernet
	- ศูนย์วิจัยพลังงานแสงอาทิตย์ จะเชื่อมต่อกับศูนย์กลางระบบเครือข่ายผ่านคณะวิทยาศาสตร์ ด้วย ATM จำนวน 1 Link - สำนักหอสมุด เชื่อมต่อกับศูนย์กลางระบบเครือข่าย อาคารมิ่งขวัญ

ตารางที่ 4-4 แสดงข้อมูลการเชื่อต่อระบบเครือข่ายคอมพิวเตอร์แบ่งตามกลุ่มสาขาวิชา

กลุ่มสาขาวิชา	สถานภาพการเชื่อมต่อ
	ด้วย ATM จำนวน 1Link
	- วิทยาเขตสารสนเทศพะเยา เชื่อมต่อกับมหาวิทยาลัยด้วยวงจรเช่า ขนาด 2 Mbps มีเครือข่ายภายใน (LAN) เป็น GB Ethernet

ตารางที่ 4-4 แสดงข้อมูลการเชื่อต่อระบบเครือข่ายคอมพิวเตอร์แบ่งตามกลุ่มสาขาวิชา(ต่อ)

ลำดับ	คณะวิชา	จำนวนเครื่อง
1	คณะมนุษยศาสตร์และสังคมศาสตร์	269
2	คณะศึกษาศาสตร์	166
3	คณะทันตแพทย์ศาสตร์	155
4	คณะพยาบาลศาสตร์	55
5	คณะแพทย์ศาสตร์	173
6	คณะเภสัชศาสตร์	183
7	คณะสหเวชศาสตร์	63
8	คณะวิทยาศาสตร์การแพทย์	29
9	สถาบันวิจัยวิทยาศาสตร์สุขภาพ	30
10	คณะวิทยาศาสตร์	490
11	คณะเกษตรศาสตร์ทรัพยากรธรรมชาติและสิ่งแวดล้อม	197
12	คณะวิศวกรรมศาสตร์	458
13	บัณฑิตวิทยาลัย	46
14	บัณฑิตวิทยาลัย	54
15	ศูนย์บริการ 11แห่ง	220
16	สถาบันสมทบ 4แห่ง	200
17	ศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร (CISCOMS)	750
18	ศูนย์วิจัยและฝึกอบรมพลังงานแสงอาทิตย์	16

ตารางที่ 4-5 แสดงจำนวนเครื่องคอมพิวเตอร์

ลำดับ	คณะวิชา	จำนวนเครื่อง
19	หน่วยงานสังกัดสำนักงานอธิการบดี	280
20	วิทยาเขตสารสนเทศจังหวัดพะเยา	152
21	สำนักหอสมุด	79
22	หอพักนิสิต	45
23	หอพักบุคลากร	65
	รวมทั้งสิ้น	4,175

ตารางที่ 4-5 แสดงจำนวนเครื่องคอมพิวเตอร์(ต่อ)

4.4 ผลการวิเคราะห์โครงสร้างของระบบเครือข่ายคอมพิวเตอร์

จากการศึกษาวิเคราะห์พบว่าระบบโครงสร้างพื้นฐานของระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยนเรศวร ที่ได้ทำการติดตั้งระบบเครือข่ายคอมพิวเตอร์ระยะที่ 1 เมื่อ พ.ศ 2539 .เป็นการตั้งตั้งเครือข่ายแบบท้องถิ่น 7 กลุ่มอาคารหลักแต่ยังไม่สามารถใช้งานอินเตอร์เน็ตได้ และในปี พ.ศ 2540 . เป็นการติดตั้ง Building Backbone เชื่อมต่อสัญญาณการสื่อสารข้อมูลภายในอาคาร และเชื่อต่อสัญญาณการสื่อสารข้อมูลกับผู้ให้บริการอินเตอร์เน็ตภายนอก คือบริษัท สามารถคอร์ปปอเรชั่น จำกัด ด้วยความเร็วในการรับสงข้อมูล 64 Kbps และในปี 2541 – 2545 เป็นติดตั้งระบบเครือข่ายขยายเพิ่มเติมไปยังอาครที่ก่อสร้างใหม่จนครบทุกอาคาร และมีการขยายเพิ่มความเร็วในการรับส่งข้อมูล (Bandwidth) จาก 64 kbps เพิ่มเป็น 3 Mbps ในปี 2545 ซึ่งเป็นการเจริญเติบโตที่รวดเร็วอย่างมาก ทำให้มหาวิทยาลัยมีการพัฒนาการจัดการเรียนการสอนและการใช้งานข้อมูลอย่างรวดเร็วอย่างมาก ทำให้มหาวิทยาลัยนเรศวรยังได้ทำการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์เพื่อให้บริการอินเตอร์เน็ตไปยังวิทยาเขต ศูนย์วิทยบริการ และสถาบันสมทบของมหาวิทยาลัยทุกแห่ง และเนื่องจากมีความพร้อมด้านโครงสร้างพื้นฐาน จึงทำให้ทุกหน่วยงานในมหาวิทยาลัยมีแนวโน้มการใช้ความเร็วในการรับส่งข้อมูลเพิ่มสูงขึ้นตามมา และมีลักษณะการใช้งานอินเตอร์เน็ตเพื่อการสืบค้นฐานข้อมูลทางวิชาการจากทั้งแห่งภายในและภายนอกมหาวิทยาลัย ที่มีลักษณะเป็นสื่อมัลติมีเดีย และมีแนวโน้มการใช้งาน e-Learning เพิ่มมากขึ้นรวมทั้งการใช้ระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยมีพัฒนาการของระบบโครงสร้างพื้นฐานโดยการขยายการเชื่อมต่อแบบต่างๆ ซึ่งในการวิเคราะห์ครั้งนี้ผู้วิจัยจะแยกการระบบเครือข่าย NU NET ตามส่วนการเชื่อต่อเป็น 4 ส่วน ดังนี้

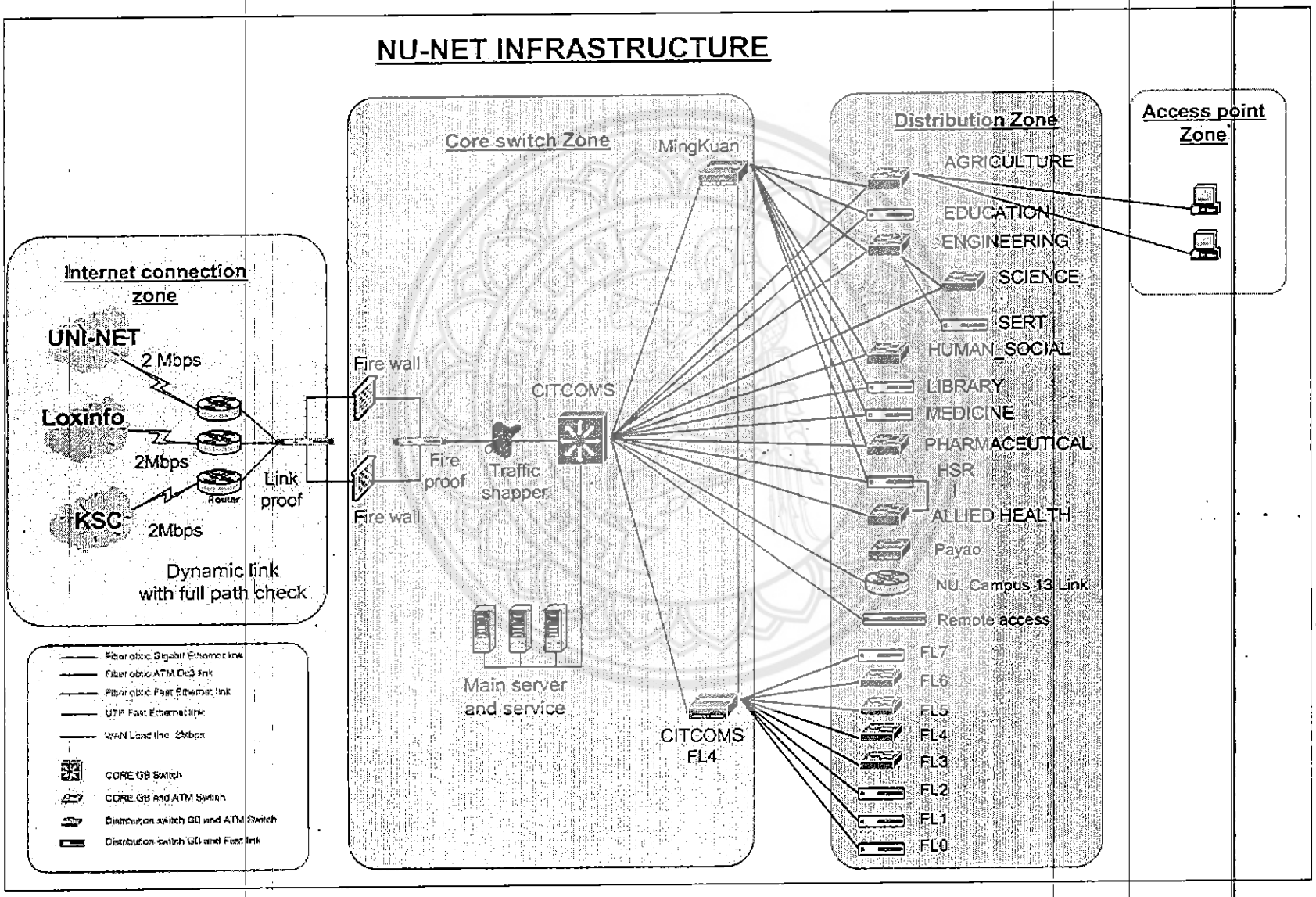
1) ส่วนการเชื่อมต่อระบบเครือข่ายภายนอก (Internet Connection Zone) ขอบเขต ตั้งแต่ ผู้ให้บริการอินเตอร์เน็ต (ISP) ถึง Router ตัวแรกที่ใช้ในการเชื่อมต่อ

2) ส่วนการเชื่อมต่อหลัก (Core Switch Zone) ขอบเขตตั้งแต่ Router ตัวแรกถึงที่เชื่อมต่อกับ ISP ถึง Main Switch อาคารมิ่งขวัญ และอาคาร CITCOMS ชั้น 4

3) ส่วนกระจาย (Distribution Zone) ขอบเขตตั้งแต่สายสัญญาณจนถึง Switch ที่ใช้เชื่อมไปยังปลายทางคือคณะวิชา และหน่วยงานต่าง ๆ

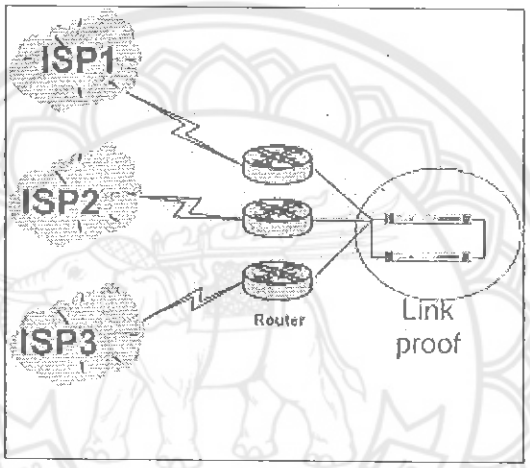
4) ส่วนเชื่อมต่อ (Access Point Zone) ขอบเขต ตั้งแต่การเชื่อมต่อออกจาก Switch ของ Distributor Zone ถึงเครื่องคอมพิวเตอร์ของผู้ใช้งาน

สำหรับโครงสร้างการเชื่อมต่อของระบบเครือข่ายคอมพิวเตอร์ มีรายละเอียดดังภาพต่อไปนี้


NU-NET INFRASTRUCTURE
Internet connection zone
UNI-NET
2 Mbps
Loxinfo
2Mbps
KSC
2Mbps
Router
Link proof
Dynamic link with full path check
Fire wall
Fire wall
Fire proof
Traffic shapper
CITCOMS
Core switch Zone
MingKuan
Main server and service
CITCOMS FL4
Distribution Zone
AGRICULTURE
EDUCATION
ENGINEERING
SCIENCE
SERT
HUMAN_SOCIAL
LIBRARY
MEDICINE
PHARMACEUTICAL
HSR
I
ALLIED HEALTH
Payao
NU_Campus 13 Link
Remote access
FL7
FL6
FL5
FL4
FL3
FL2
FL1
FL0
Access point Zone
CORE GB Switch
CORE GB and ATM Switch

4.4.1 ส่วนที่ 1 ส่วนการเชื่อมต่อระบบเครือข่ายภายนอก (Internet Connection Zone)

เป็นส่วนที่ใช้ในการเชื่อมต่อกับอินเตอร์เน็ต(Internet) ภายนอกมหาวิทยาลัย โดยได้ทำการเชื่อมต่อระบบเครือข่ายกับผู้ให้บริการอินเตอร์เน็ต (ISP) 2 ราย เพื่อสลับการเชื่อมต่อในสภาวะที่การเชื่อมต่อสายใดสายหนึ่งไม่สามารถใช้งานได้คือ ระบบเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา (UNINET) ขนาดความเร็วในการรับส่งข้อมูล 2 Mbps โดยทำการเชื่อมต่อแบบ Interface ATM OC-3 และบริษัท Lox info ขนาดความเร็วในการรับส่งข้อมูล 2 Mbps โดยทำการเชื่อมต่อแบบ Interface V35 และมีการ Routing BGP Version 4 ดังรูป

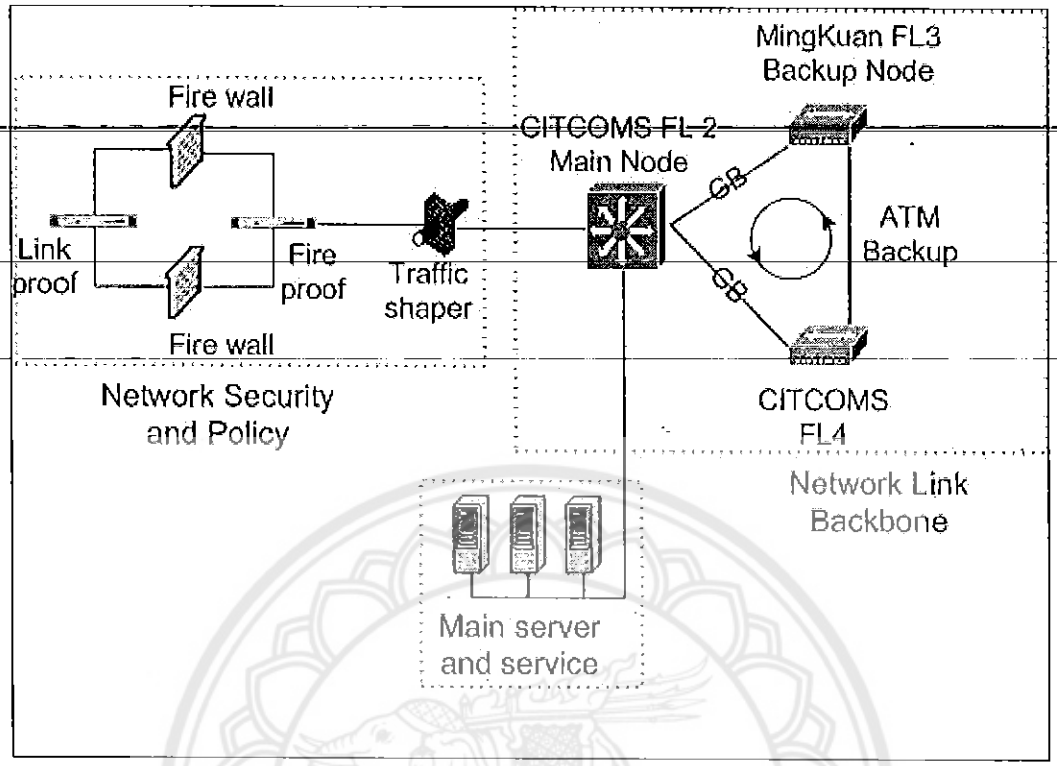


รูปที่ 4-2 การเชื่อมต่อระบบเครือข่ายภายนอก

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

4.4.2 ส่วนที่ 2 ส่วนที่การเชื่อมต่อหลัก (Core Switch Zone)

เป็นส่วนของการเชื่อมต่อหลักจากภายนอกมหาวิทยาลัยและจากหน่วยงานภายในมหาวิทยาลัย การเชื่อมต่อหลักนี้จะทำหน้าที่ในการเชื่อมต่อระบบเครือข่ายทั้งหมดของมหาวิทยาลัยเข้าสู่ระบบบริหารจัดการเครือข่ายส่วนกลาง โดยมีศูนย์กลางในการเชื่อมต่อ 2 แห่งคือ การเชื่อมต่อไปยังอาคารมิ่งขวัญ โดยใช้ Gigabit Ethernet บนสายใยแก้วนำแสง แบบ Single Mode และการเชื่อมต่อไปยังอาคาร CITCOMS ชั้น 2 โดยใช้ Gigabit Ethernet บนสายใยแก้วนำแสงแบบ Multimode
ดังรูป



รูปที่ 4-3 ความสัมพันธ์ส่วนการเชื่อมต่อหลัก

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

โครงสร้างของส่วนการเชื่อมต่อหลักประกอบไปด้วยอุปกรณ์ดังนี้

1. Load balance firewall (Radware Fireproof)
2. Firewall

Watchguard Firewall II

Watchguard Firewall 2500

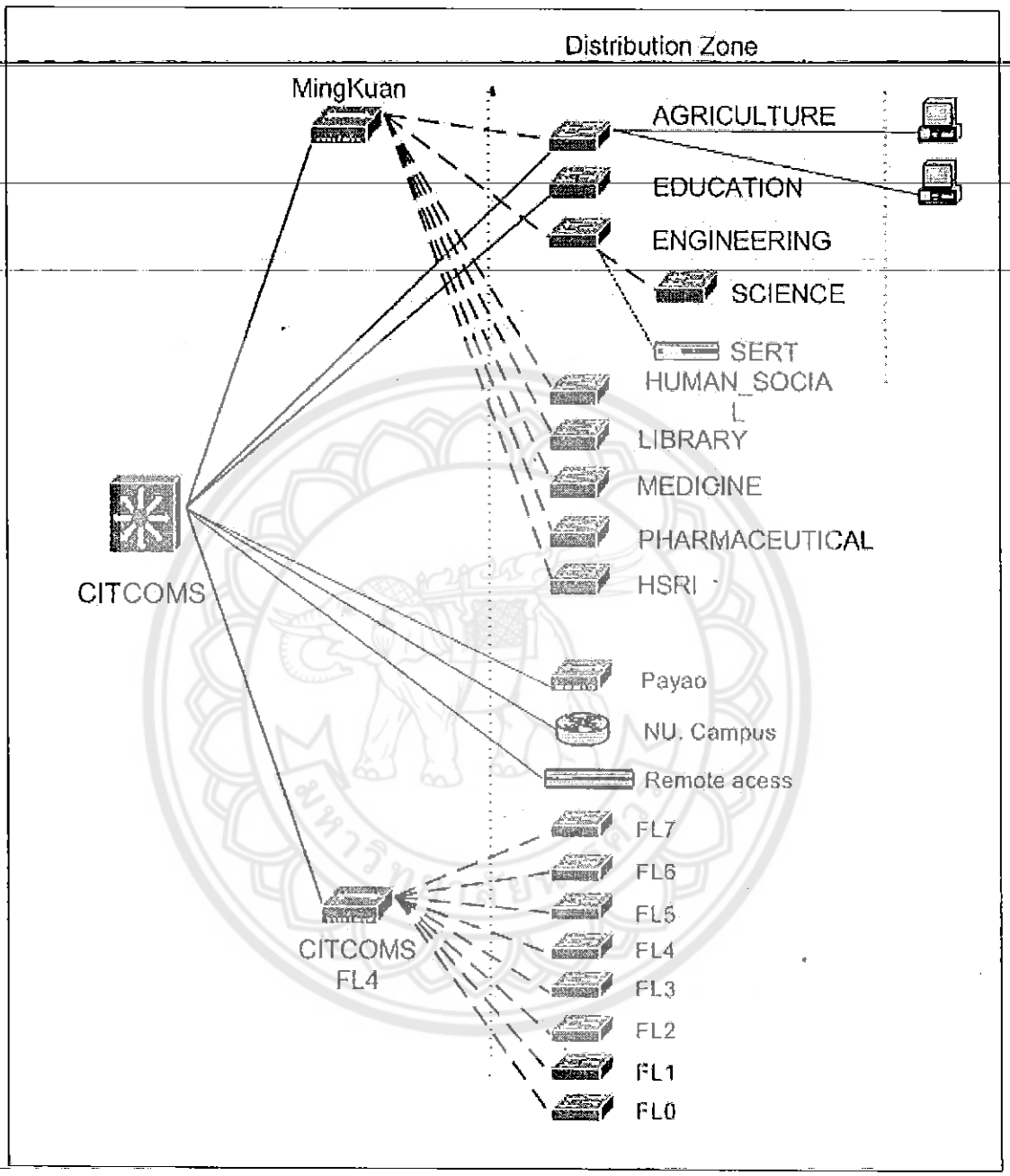
3. Traffic shaper (Allot AC301)
4. Core switch
   - Alcatel Omi switch S/R CPM MPX
   - 4 port GB Single mode
   - 4 port GB Multi mode
   - 64 port 10/100 Mbps

5. Main Switch Mingkuan floor 3
   - Alatel Omi switch CPU MPM 1G
   - 2 port GB Single mode
   - 10 port ATM OC-3
   - 12 Port 100 Mbps
6. Main Switch CITCOMS floor 3
   - Alcatel Omi switch CPU MPM 1G
   - 2 port GB Multimode
   - 16 port ATM OC-3
   - 96 port 10 Mbps

4.4.3 ส่วนที่ 3 ส่วนกระจาย (Distribution Zone)

เป็นส่วนเชื่อจาก Core Switch เพื่อทำหน้าที่กระจายสัญญาณไปยังคณะ/หน่วยงานต่าง ๆ ภายในมหาวิทยาลัย ได้แก่

1. คณะเกษตรศาสตร์ ทรัพยากรธรรมชาติและสิ่งแวดล้อม
2. คณะศึกษาศาสตร์
3. คณะวิศวกรรมศาสตร์
4. คณะวิทยาศาสตร์
5. คณะมนุษย์ศาสตร์และสังคมศาสตร์
6. สำนักหอสมุด
7. คณะแพทยศาสตร์
8. คณะเภสัชศาสตร์
9. สถาบันวิจัยทางวิทยาศาสตร์สุขภาพ
10. ศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสารทั้ง 8 ชั้น
11. วิทยาเขตสารสนเทศพะเยา
12. ศูนย์วิทยาบริการ 11 แห่ง และ
13. สถาบันสมทบ 4 แห่ง



รูปที่ 4-4 ความสัมพันธ์ส่วนของการกระจายการเชื่อมต่อ

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

แสดงการเชื่อมต่อด้วยสายใยแก้วน้ำแสง ณ อาคารมิ่งขวัญ และอาคาร CITCOM ชั้น 2 เป็นส่วนของ Distribution Zone ที่ใช้งานในปัจจุบัน แล่ะบางส่วนเป็นการติดตั้งไว้เพื่อเป็นระบบสำรอง

Distribution Zone	Fiber Optic To CITCOMS	Fiber Optic to Mingkuan
คณะเกษตรศาสตร์ฯ	GB	สำรอง ATM
คณะศึกษาศาสตร์	GB	ไม่ได้ใช้
คณะวิศวกรรมศาสตร์	ไม่มี	ATM
คณะวิทยาศาสตร์	ไม่มี	ATM เชื่อมจาก ENG.
คณะมนุษยศาสตร์ฯ	ไม่มี	ATM
สำนักหอสมุด	ไม่มี	ATM
คณะแพทย์ศาสตร์	ไม่มี	ATM
คณะเภสัชศาสตร์	ไม่มี	ATM
สถาบันวิจัยวิทยาศาสตร์สุขภาพ	ไม่มี	ATM
วิทยาเขตสารสนเทศพะเยา	100 Mbps UTP Commit Rate 2 Mbps	ไม่มี
ศูนย์วิทยบริการและสถาบันสมทบ	100 Mbps Commit Rate 64kbps	ไม่มี
Remote access	100 Mbps UTP Rate per user 56kbps 2 Mbps	ไม่มี
CITCOMS ทั้ง 8ชั้น	ATM	ไม่มี

ตารางที่ 4-6 รายละเอียดการเชื่อมต่อของ Core Switch

Distribution Zone	CITCOMS ชั้น 2(Core)	Mingluan (Core)	คณะวิศวกรรมศาสตร์
คณะเกษตรศาสตร์ฯ	12	12	ไม่มี
คณะศึกษาศาสตร์	12	12	ไม่มี
คณะวิศวกรรมศาสตร์	ไม่มี	12	ไม่มี
คณะวิทยาศาสตร์	ไม่มี	ไม่มี	12
คณะมนุษยศาสตร์ฯ	ไม่มี	12	ไม่มี
สำนักหอสมุด	ไม่มี	12	ไม่มี
คณะแพทย์ศาสตร์	ไม่มี	12	ไม่มี
คณะเภสัชศาสตร์	ไม่มี	12	ไม่มี
สถาบันวิจัยวิทยาศาสตร์สุขภาพ	ไม่มี	12	ไม่มี
CITCOMS ชั้น 4	6	12	ไม่มี
ศูนย์วิจัยพลังงานแสงอาทิตย์	ไม่มี	ไม่มี	6

ตารางที่ 4-7 ตารางแสดงส่วนเชื่อมต่อของ Distribution Zone ที่เชื่อมต่อกันด้วยสาย Fiber Optic

Distribution Zone	Switch (Slot)	GB (port)	ATM (port)	Port			
				(10)	(100)	(10FB)	(100FB)
คณะเกษตรศาสตร์ฯ	9slot	2 SM	1/1	24	ไม่มี	ไม่มี	ไม่มี
คณะศึกษาศาสตร์	Stack	2 SM	ไม่มี	ไม่มี	24	ไม่มี	ไม่มี
คณะวิศวกรรมศาสตร์	9slot	ไม่มี	3/8	ไม่มี	ไม่มี	8	8
คณะวิทยาศาสตร์	9slot	ไม่มี	1	ไม่มี	32	ไม่มี	8
คณะมนุษยศาสตร์ฯ	9slot	ไม่มี	1	12	32	ไม่มี	ไม่มี
สำนักหอสมุด	Pizza	ไม่มี	1	12	ไม่มี	ไม่มี	ไม่มี
คณะแพทย์ศาสตร์	Stack	ไม่มี	1	32	ไม่มี	ไม่มี	ไม่มี
คณะเภสัชศาสตร์	9slot	ไม่มี	1	24	ไม่มี	ไม่มี	ไม่มี
สถาบันวิจัยวิทยาศาสตร์สุขภาพ	Stack	ไม่มี	1	ไม่มี	24	ไม่มี	ไม่มี
ศูนย์วิจัยพลังงานแสงอาทิตย์	Pizza	ไม่มี	ไม่มี	ไม่มี	24	ไม่มี	1
CITCOMS Floor 0	Stack	ไม่มี	1	12	ไม่มี	ไม่มี	ไม่มี
CITCOMS Floor 1	Stack	ไม่มี	1	32	ไม่มี	ไม่มี	ไม่มี
CITCOMS Floor 2	Stack	ไม่มี	1	32	ไม่มี	ไม่มี	ไม่มี
CITCOMS Floor 3 - 1	9slot	ไม่มี	2/2	96	ไม่มี	ไม่มี	ไม่มี
CITCOMS Floor 3 - 2	Stack	ไม่มี	1	96	ไม่มี	ไม่มี	ไม่มี
CITCOMS Floor 4 - 1	9slot	2MM	7/8	96	ไม่มี	ไม่มี	ไม่มี
CITCOMS Floor 4 - 2	9slot	ไม่มี	1/2	128	ไม่มี	ไม่มี	ไม่มี
CITCOMS Floor 5	9slot	ไม่มี	1/8	108	32	ไม่มี	ไม่มี
CITCOMS Floor 6	9slot	ไม่มี	1/8	150	ไม่มี	ไม่มี	ไม่มี
CITCOMS Floor 7	Stack	ไม่มี	1	32	ไม่มี	ไม่มี	6

ตารางที่ 4-8 ความสัมพันธ์รายละเอียดของอุปกรณ์ Switch ในส่วน Distribution Zone ของคณะ/หน่วยงานที่เชื่อมต่อกับระบบเครือข่ายหลักของมหาวิทยาลัย

จากตารางข้างต้น เป็นการแสดงรายละเอียดของการเชื่อมต่อในส่วนของ Distribution Zone ที่มีการเชื่อต่อด้วย Fiber Optic โดยมีบางส่วนที่ไม่ได้เชื่อมต่อผ่าน Fiber Optic เช่น วิทยาเขตสารสนเทศ

ศูนย์วิทยบริการ และสถาบันสมทบได้ทำการเช่าสายสัญญาณความเร็วสูงจากการสื่อสารแห่งประเทศไทยในรูปแบบ Frame Relay และใช้ Router (CISCO 3600) กระจายไปยัง Router (CISCO 800) ของวิทยาเขตสารสนเทศ ศูนย์วิทยบริการ และสถาบันสมบททุนแห่ง ด้วยขนาดความเร็วในการรับส่งข้อมูล 64 kbps ถึง 2 Mbps ดังนี้

1) การให้บริการวิทยาเขตสารสนเทศพะเยา ใช้การเชื่อต่อผ่านสายสัญญาณชนิด Frame Relay ของการสื่อสารแห่งประเทศไทยโดยมีผู้ให้บริการอินเตอร์เน็ต คือ UNI NET เป็นผู้ให้บริการ โดยใช้การเชื่อมต่อขนาด 2 Mbps ผ่านอุปกรณ์ Router (CISCO 2500)

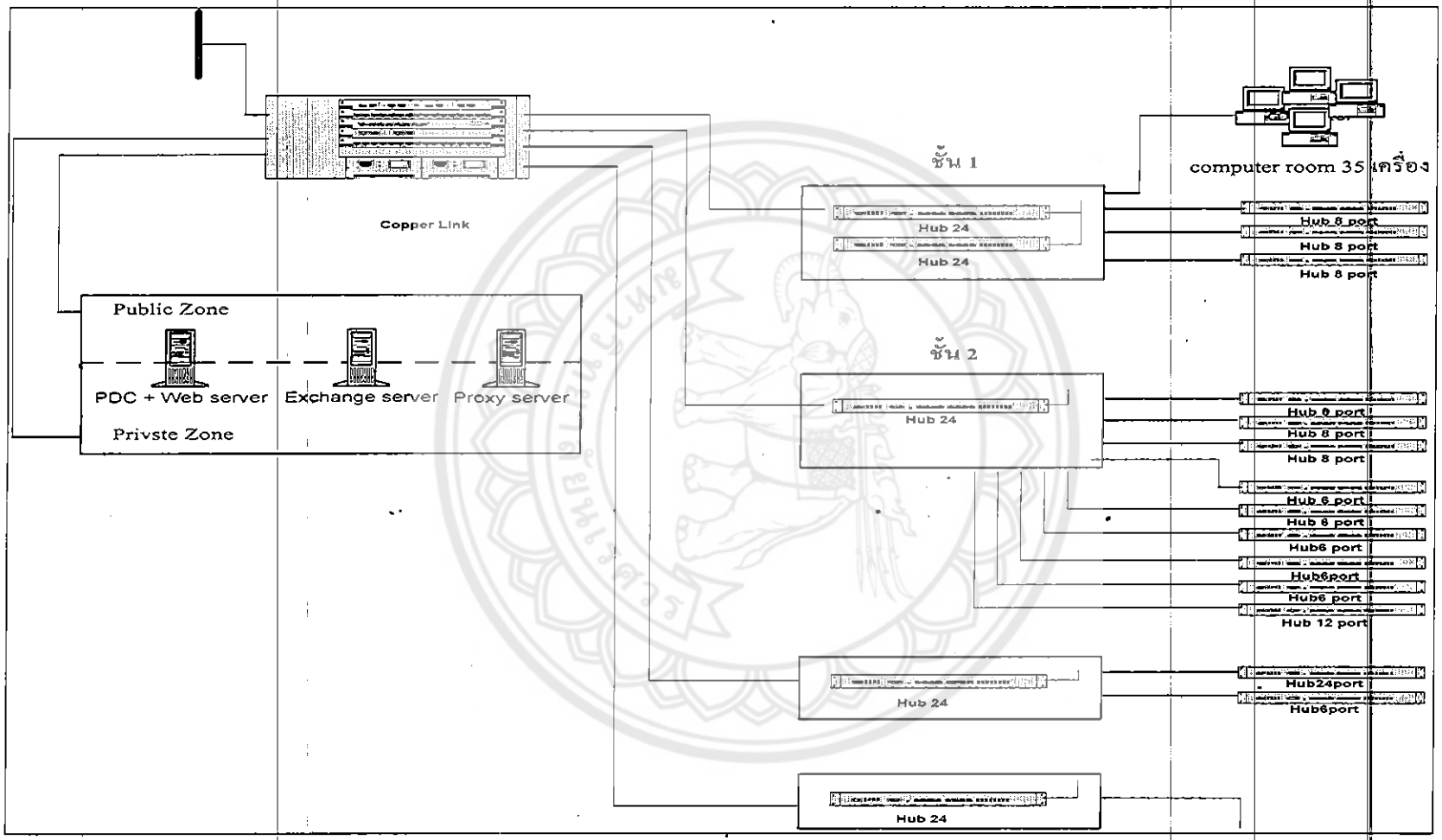
2) การให้บริการศูนย์วิทยาบริการ และสถาบันสมทบ 13 แห่ง ยกเว้นศูนย์วิทยบริการเชียงใหม่และศูนย์วิทยบริการกรุงเทพฯ ประกอบด้วย

2.1วิทยาลัยนาฏศิลป์สุโขทัย
2.2โรเรียนพิจิตรวิทยาคม
2.3โรงเรียนวิทยานุกูลนารี
2.4โรงเรียนอุตรดิตถ์ครุณี
2.5โรงเรียนนารีรัตน์แพร่
2.6โรงเรียนอุทัยธานีวิทยาคม
2.7โรงเรียนกำแพงเพชรวิทยาคม
2.8โรงเรียนนครสวรรค์
2.9โรงเรียนตากวิทยาคม
2.10 โรงพยาบาลอุตรดิตถ์
2.11 วิทยาลัยพยาบาลบรมราชชนนี อุตรดิตถ์
2.12โรงพยาบาลพุทธชินราชพิษณุโลก
2.13วิทยาลัยพยาบาลบรมราชชนนี พุทธชินราช

3) การให้บริการ Remote Access เป็นการให้บริการระบบเครือข่ายผ่านระบบโทรศัพท์แก่ผู้ใช้งานทุกคนของมหาวิทยาลัย ในปัจจุบันมีคู่สายให้บริการ 270 คู่สายอัตโนมัติ แบ่งเป็นการให้บริการคู่สาย แบบ ISDN PRI จำนวน 150 คู่สาย และแบบ Trucking Access R2 120 คู่สาย

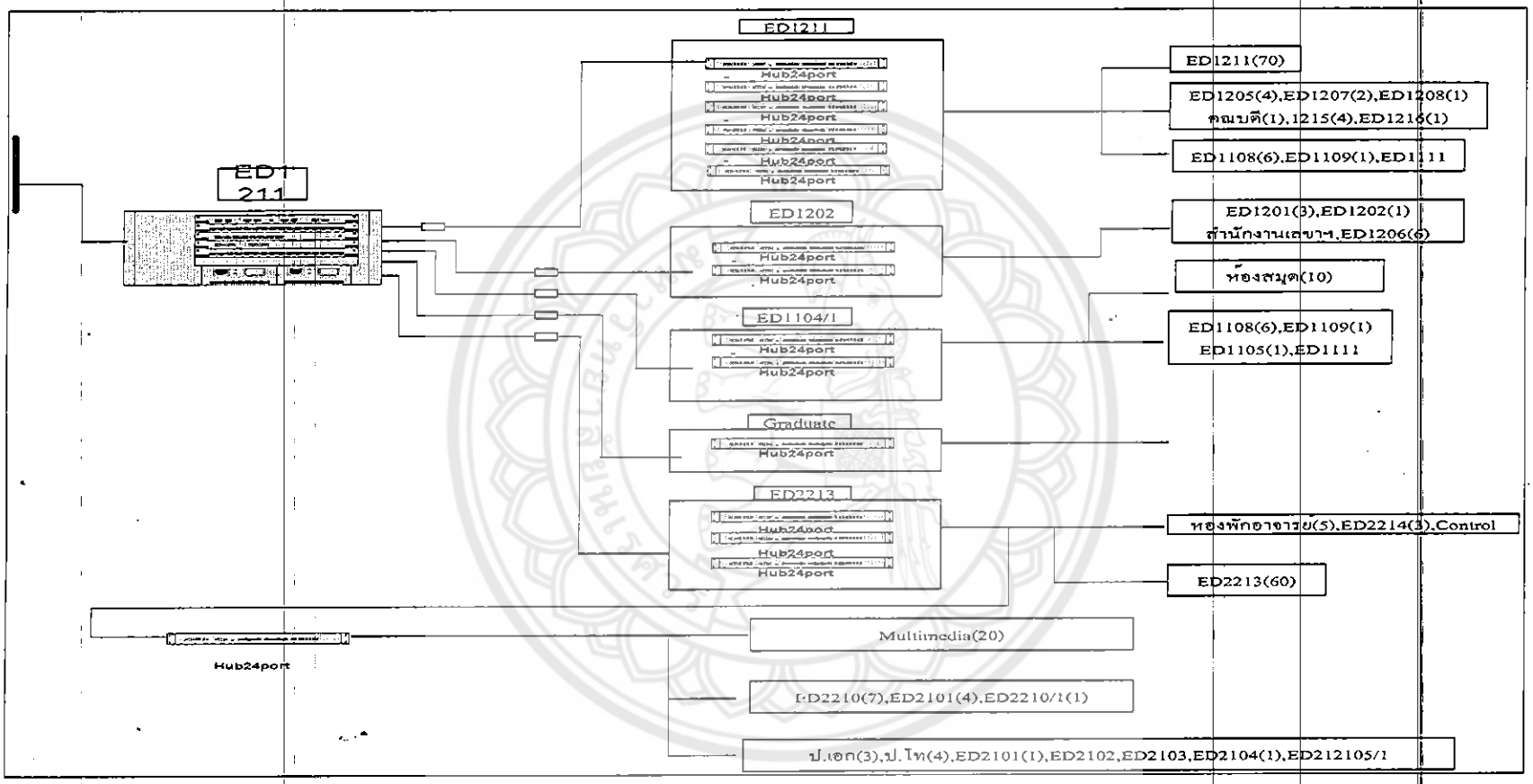
4.4.4 ส่วนที่ 4 ส่วนของการเชื่อมต่อ (Access Point Zone)

ส่วนของการ์ดเชื่อมต่อไปนี้ คือส่วนที่เชื่อมต่อจาก Switch ไปยังจุด Outlet เพื่อเชื่อมต่อไปยังอุปกรณ์กระจายสัญญาณ (Hub) หรือเครื่องคอมพิวเตอร์ของคณะ/หน่วยงานต่างๆซึ่งมีรายละเอียดการกระจายสัญญาณไปยังคณะ/หน่วยงานหลักๆดังนี้



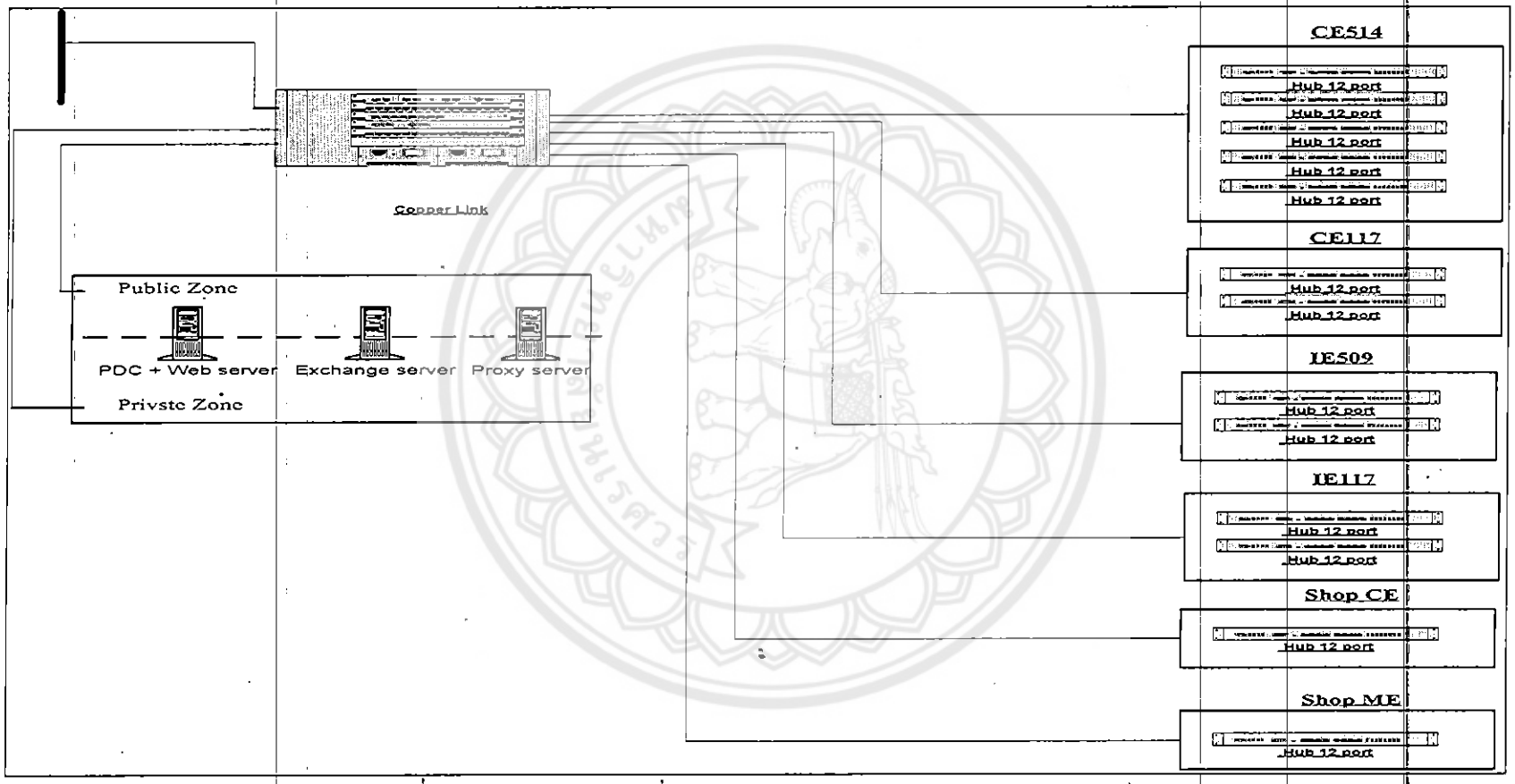
รูปที่ 4-5 ความสัมพันธ์การเชื่อมต่อไปยังจุดใช้งานของคณะเกษตรศาสตร์

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์ (2546), แผนแม่บทเทคโนโลยีสารสนเทศ. มหาวิทยาลัยนเรศวร)



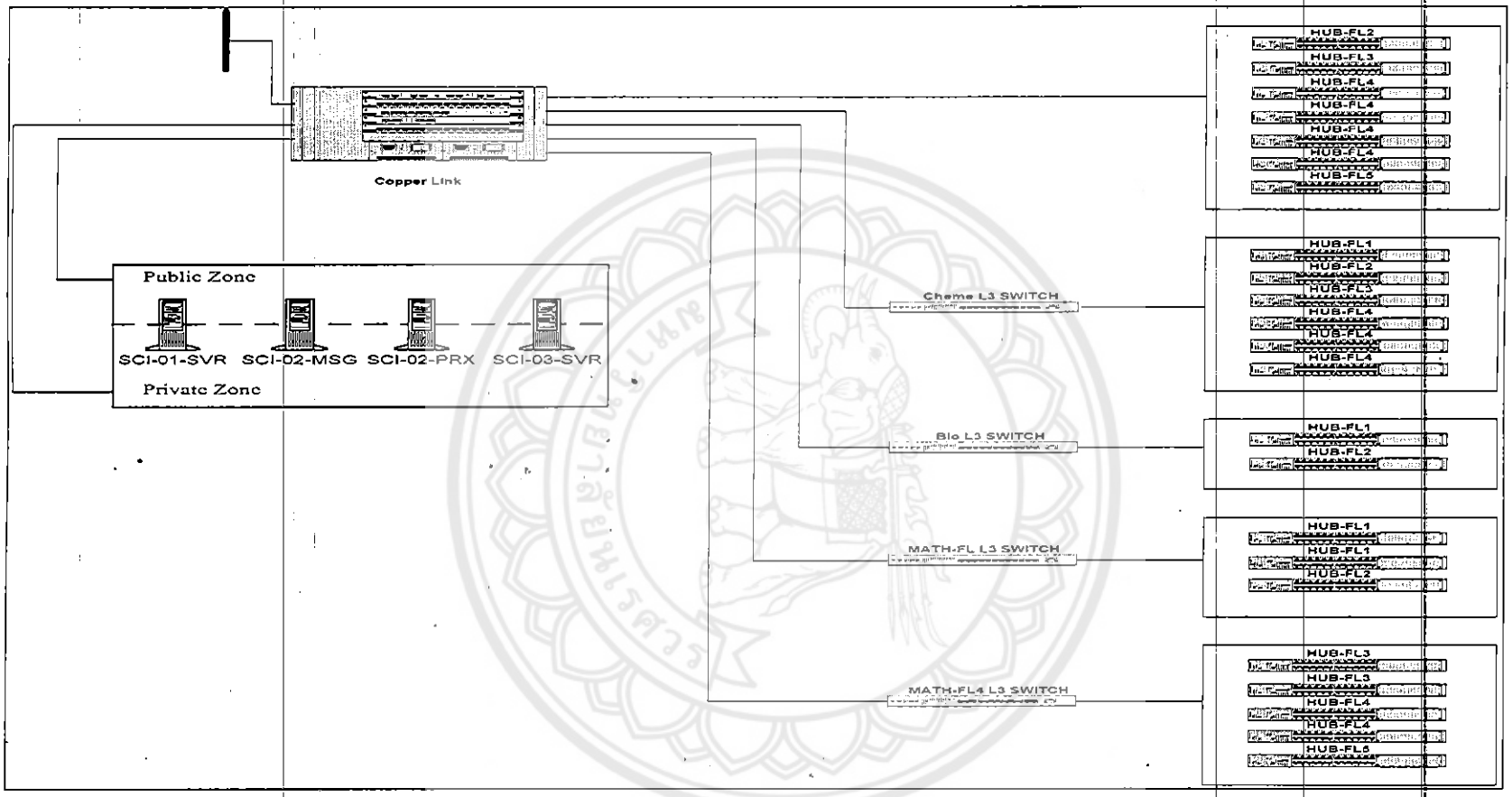
รูปที่ 4-6 ความสัมพันธ์การเชื่อมต่อไปยังจุดใช้งานของคณะศึกษาศาสตร์

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์ (2546), แผนแม่บทเทคโนโลยีสารสนเทศ. มหาวิทยาลัยนเรศวร)



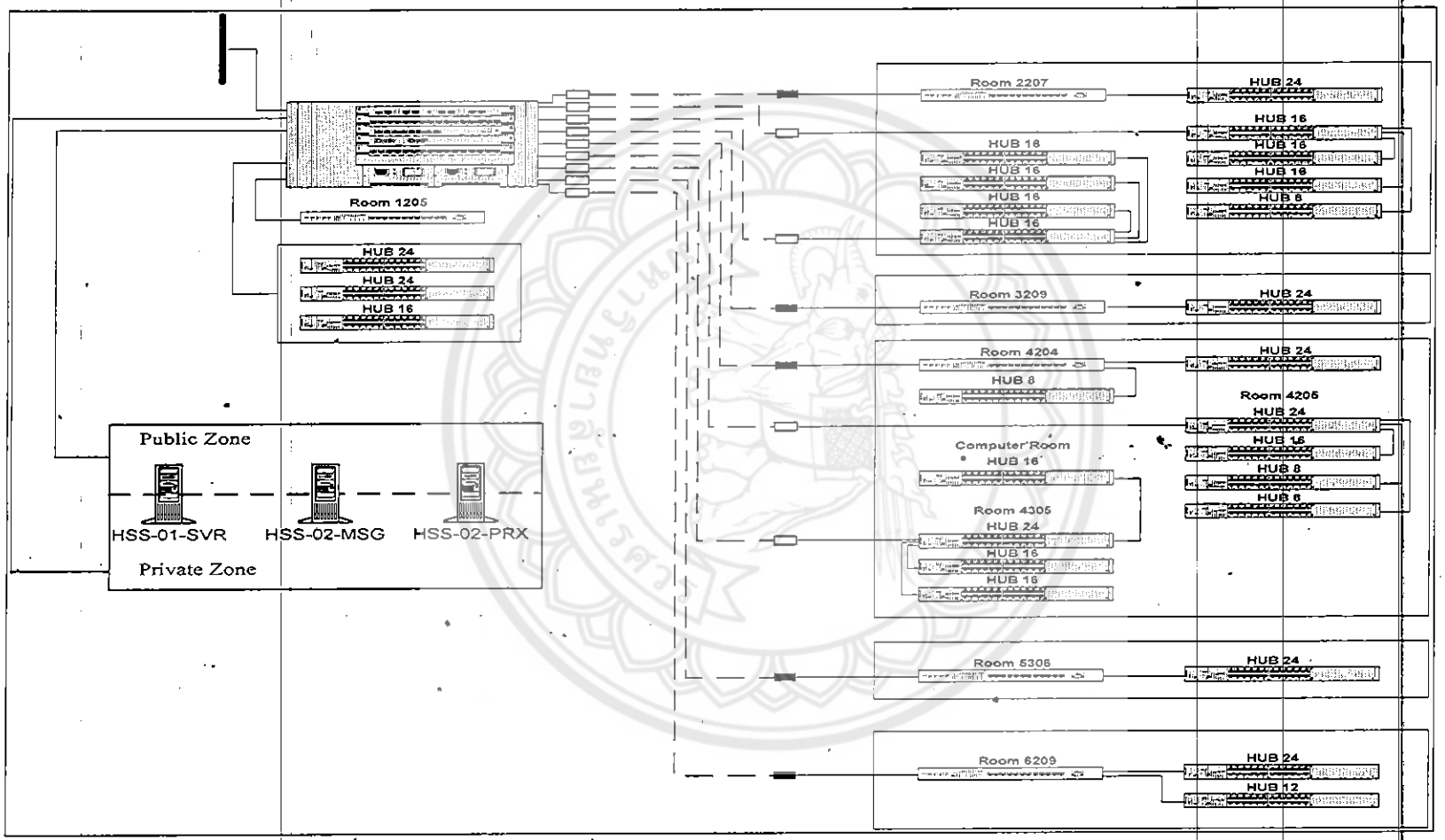
รูปที่ 4-7 ความสัมพันธ์การเชื่อมต่อไปยังจุดใช้งานของคณะวิศวกรรมศาสตร์

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์ (2546), แผนแม่บทเทคโนโลยีสารสนเทศ. มหาวิทยาลัยนเรศวร)



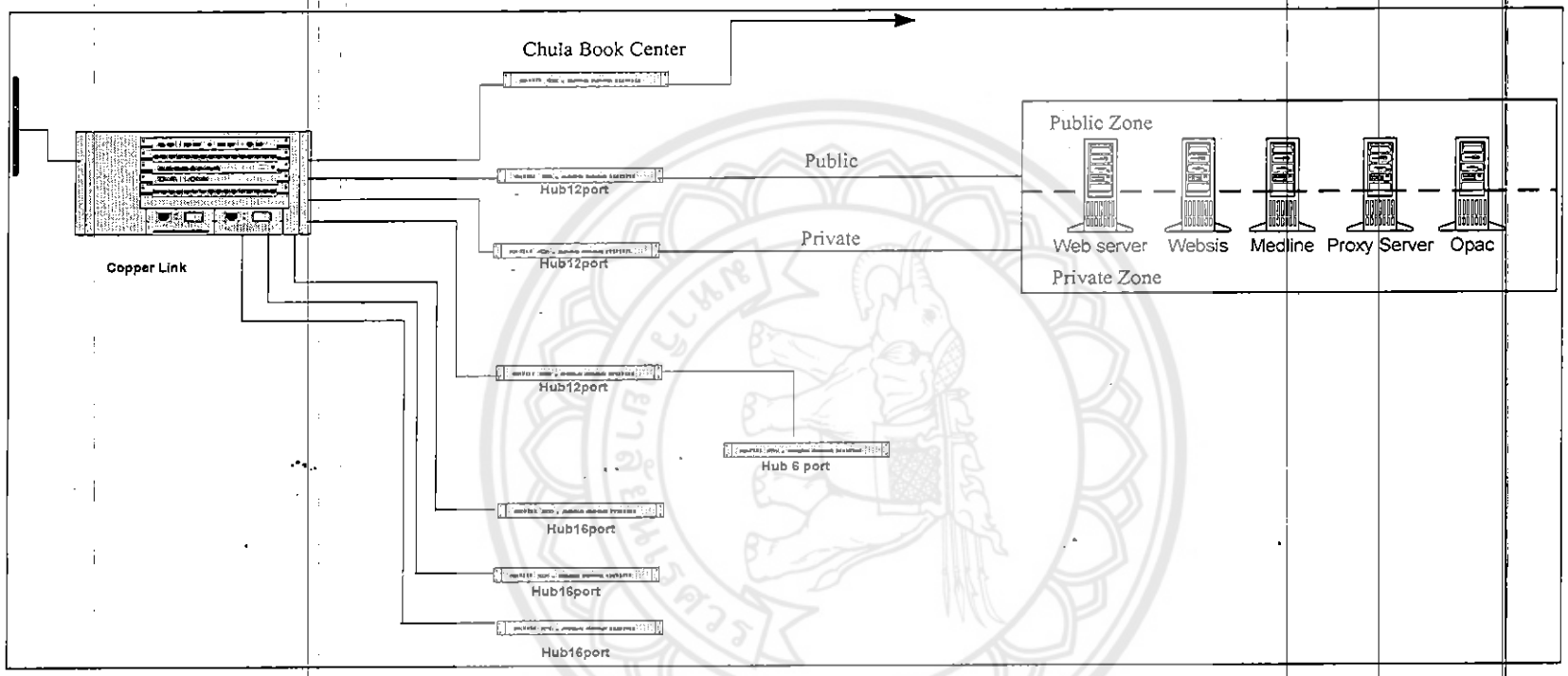
รูปที่ 4-8 ความสัมพันธ์การเชื่อมต่อไปยังจุดใช้งานของคณะวิทยาศาสตร์

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์ (2546), แผนแม่บทเทคโนโลยีสารสนเทศ. มหาวิทยาลัยนเรศวร)



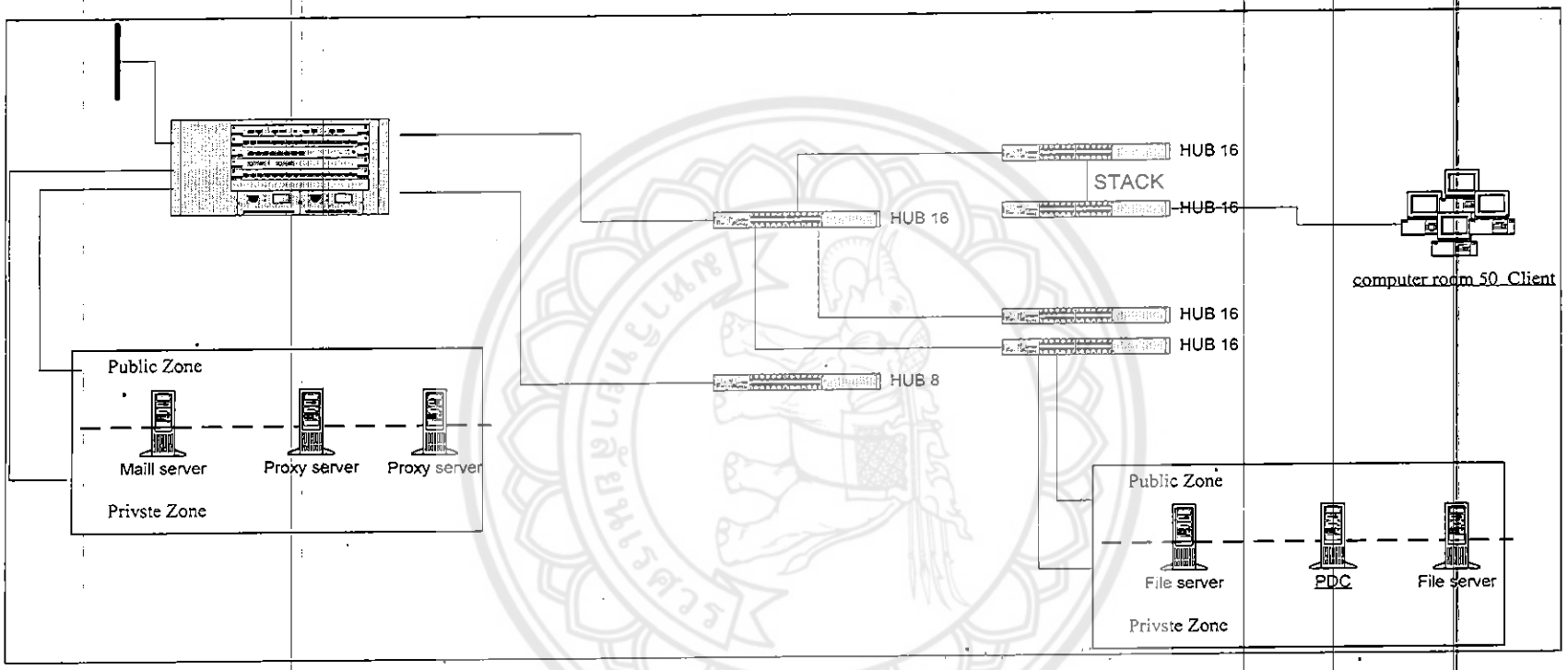
รูปที่ 4-9 ความสัมพันธ์การเชื่อมต่อไปยังจุดใช้งานของคณะมนุษยศาสตร์และสังคมศาสตร์

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์ (2546), แผนแม่บทเทคโนโลยีสารสนเทศ. มหาวิทยาลัยนเรศวร)



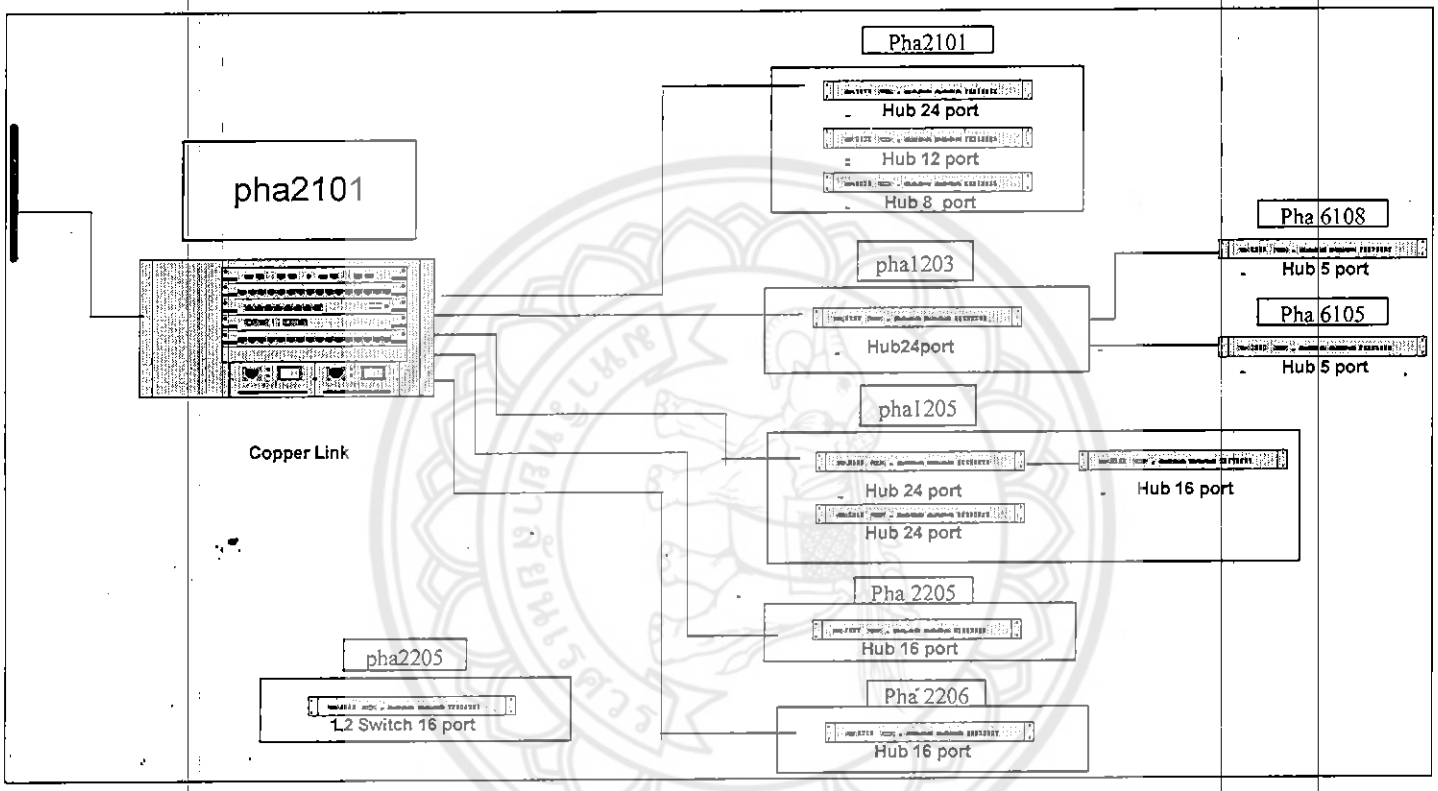
รูปที่ 4-10 ความสัมพันธ์การเชื่อมต่อไปยังจุดใช้งานของสำนักหอสมุด

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์ (2546), แผนแม่บทเทคโนโลยีสารสนเทศ. มหาวิทยาลัยนเรศวร)



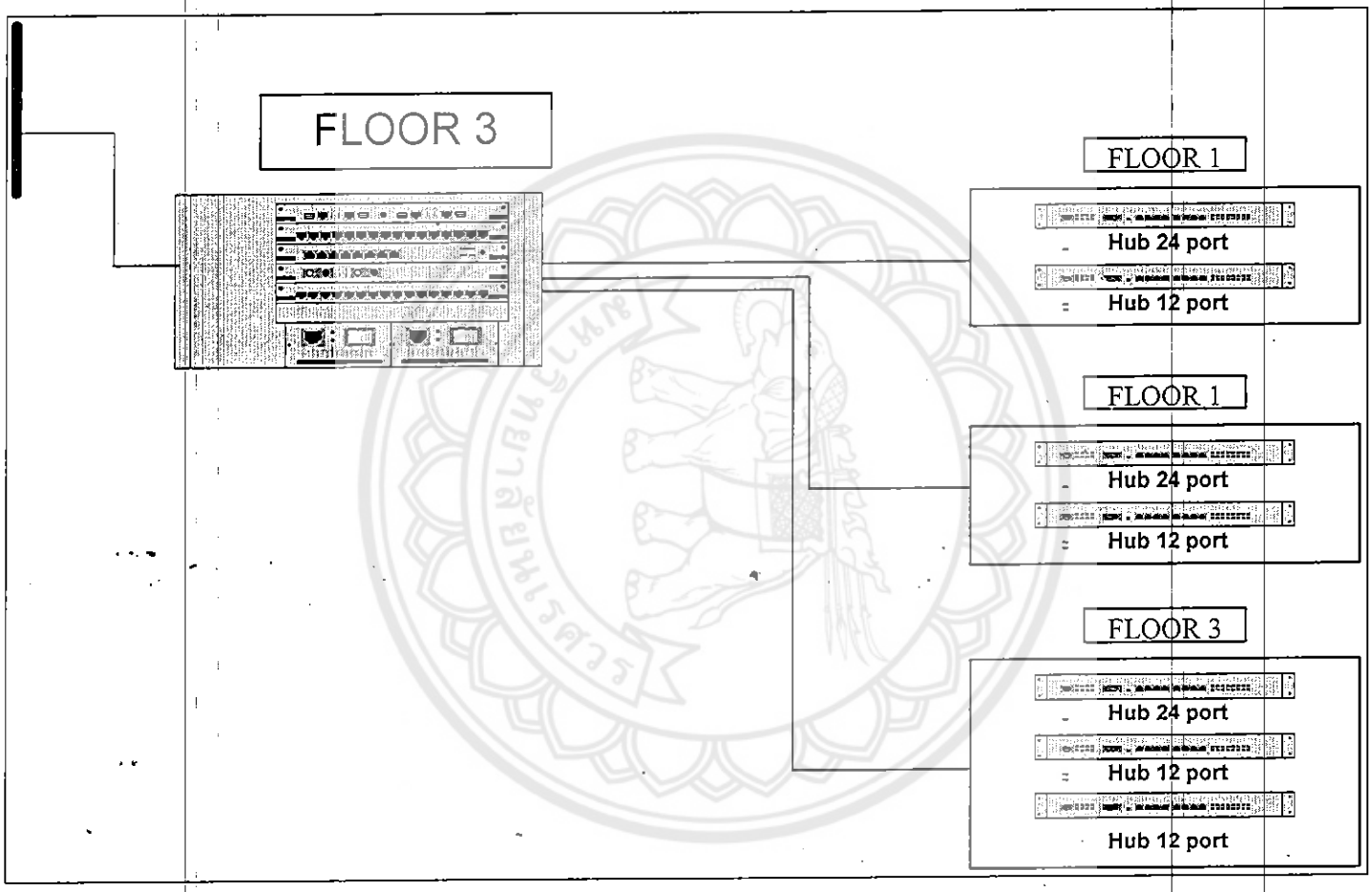
รูปที่ 4-11 ความสัมพันธ์การเชื่อมต่อไปยังจุดใช้งานของคณะแพทยศาสตร์

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์ (2546), แผนแม่บทเทคโนโลยีสารสนเทศ. มหาวิทยาลัยนเรศวร)



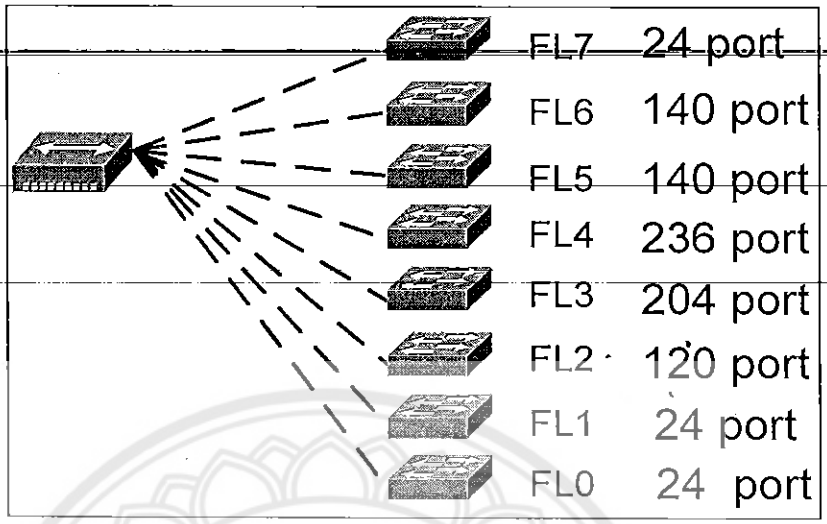
รูปที่ 4-12 ความสัมพันธ์การเชื่อมต่อไปยังจุดใช้งานของคณะเภสัชศาสตร์

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์ (2546), แผนแม่บทเทคโนโลยีสารสนเทศ. มหาวิทยาลัยนเรศวร)



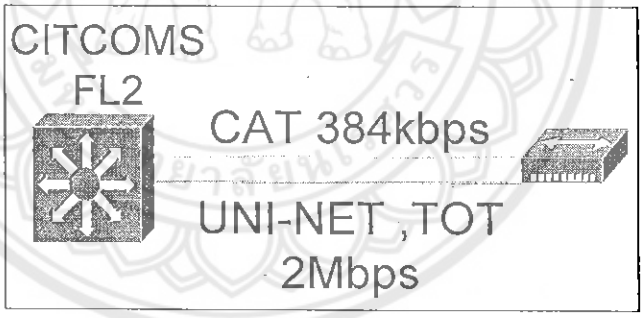
รูปที่ 4-13 ความสัมพันธ์การเชื่อมต่อไปยังจุดใช้งานของสถาบันวิจัยทางวิทยาศาสตร์สุขภาพ

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์ (2546), แผนแม่บทเทคโนโลยีสารสนเทศ. มหาวิทยาลัยนเรศวร)



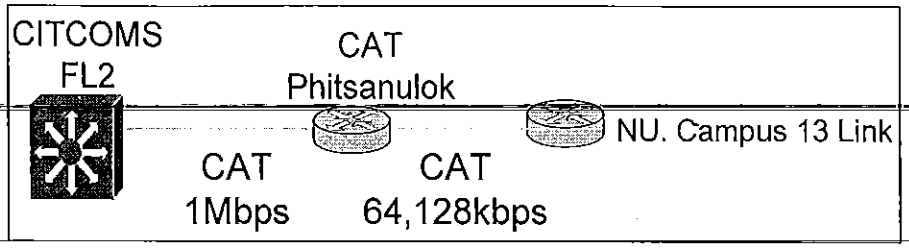
รูปที่ 4-14 ความสัมพันธ์การเชื่อมต่อไปยังจุดใช้งานของศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร(CITCOMS) ทั้ง 8 ชั้น

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)



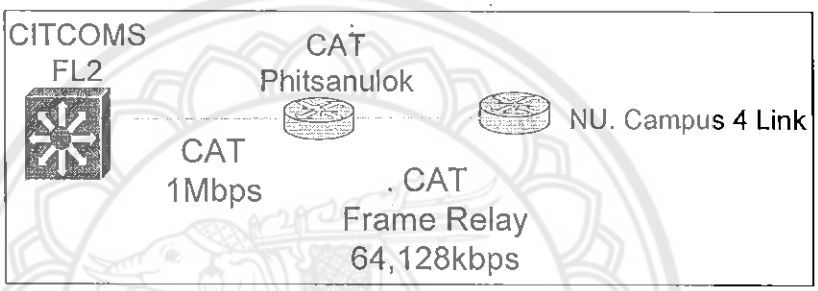
รูปที่ 4-15 ความสัมพันธ์การเชื่อมต่อไปยังวิทยาเขตสารสนเทศพะเยา

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)



รูปที่ 4-16 ความสัมพันธ์การเชื่อมต่อไปยังศูนย์วิทยบริการ

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)



รูปที่ 4-17 ความสัมพันธ์การเชื่อมต่อไปยังสถาบันสมทบ 4 แห่ง

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

4.5 การวิเคราะห์ปัญหาและปัจจัยที่ส่งผลกระทบต่อระบบเครือข่ายคอมพิวเตอร์

เพื่อให้การวิเคราะห์ปัญหาและปัจจัยที่ส่งผลกระทบต่อระบบเครือข่ายคอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพ จึงได้แบ่งส่วนการวิเคราะห์ปัญหาและอุปสรรค์ออกเป็น 4 ส่วน ด้วยกัน คือ

1. ส่วน **Internet Connection Zone** คือระบบเครือข่ายคอมพิวเตอร์ส่วนที่เชื่อมต่อกับผู้ให้บริการอินเตอร์เน็ต(ISP)
2. **ส่วน Core Switch Zone** คือส่วนที่เป็นระบบบริหารจัดการ การเชื่อมต่อ และการกระจายสัญญาณส่วนกลางของศูนย์ควบคุมระบบเครือข่ายคอมพิวเตอร์
3. **ส่วน Distribution Zone** คือส่วนที่เป็นการการเชื่อมต่อจากส่วนกลางไปยัง Core Switch ของคณะ/หน่วยงานต่างๆ
4. **ส่วน Access Point Zone** คือส่วนที่เป็นการเชื่อมต่อหลัง Core Switch หรือส่วนที่เป็นการใช้งานของผู้ใช้บริการระบบเครือข่ายคอมพิวเตอร์

จากการแบ่งส่วนเพื่อวิเคราะห์สถานภาพและปัญหาอุปสรรคที่เกิดขึ้นต่อระบบเครือข่ายดังกล่าวข้างต้น จึงสามารถสรุปปัญหาและปัจจัยที่ส่งผลกระทบต่อการใช้งาน ดังนี้

4.5.1 ปัญหาส่วนที่ 1 Internet Connection Zone

ปัญหาที่สำรวจพบ

1. ปัญหาระบบเครือข่าย NU Net ไม่สามารถติดต่อกับระบบเครือข่ายอินเตอร์เน็ตภายนอกได้ เป็นผลให้ผู้ใช้งานไม่สามารถรับส่งข้อมูลได้ และข้อมูลของผู้ใช้บริการที่มีการติดต่อสื่อสารในช่วงนั้นอาจสูญหาย โดยมีสาเหตุดังนี้

ผู้ให้บริการอินเตอร์เน็ต (ISP) บางรายไม่สามารถให้บริการได้ในช่วงเวลานั้นๆ ข้อจำกัดของระบบการหาเส้นทางการเชื่อมต่อกับระบบอินเตอร์เน็ตของ BGP Protocol สามารถตรวจสอบสถานภาพการเชื่อมต่อระหว่างเครือข่าย NU Net กับอุปกรณ์ Router ของผู้ให้บริการอินเตอร์เน็ตของมหาวิทยาลัยเพียงรายเดียวเท่านั้น

สายสัญญาณเชื่อมต่ออินเตอร์เน็ตไปยังต่างประเทศ ซึ่งมีการสื่อสารแห่งประเทศไทยเป็นผู้ให้บริการเพียงรายเดียว เป็นผลให้หากระบบของการสื่อสารแห่งประเทศไทยมีเหตุขัดข้องจะทำให้ไม่สามารถเชื่อมต่อกับระบบเครือข่ายต่างประเทศได้

2. ปัญหา Bandwidth ไม่เพียงพอต่อความต้องการการใช้งาน เมื่อมีผู้เข้ามาใช้งานจำนวนมากจะให้การเชื่อมต่อระบบอินเตอร์เน็ตช้ามาก เช่น การเปิด Web Page หรือการ Download ข้อมูลโดยมีสาเหตุ ดังนี้

มีความต้องการใช้งานอินเตอร์เน็ตสูงมาก ปัจจุบันมีจำนวน User account ทั้งหมดประมาณ 28,325 Account ปริมาณ Bandwidth ที่ได้รับจากผู้ให้บริการทั้งสองราย รวมกันแล้วมีขนาด 4 Mbps และจากการ Monitor Bandwidth พบว่าปริมาณใช้งานสูงในช่วงเวลา 8.00 – 03.00 น.

เนื่องจากจำนวนเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่าย NU Net ประมาณ 4,175 เครื่อง สามารถเทียบอัตราส่วนเป็น เครื่องคอมพิวเตอร์ 1 เครื่อง Bandwidth 0.71 Kbps ทั้งนี้ในแต่ละคณะมีโครงการเพิ่มจำนวนเครื่องให้บริการแก่นิสิตอย่างต่อเนื่อง

4.5.2 ปัญหาส่วนที่ 2 Core Switch Zone

ปัญหาที่สำรวจพบ

1. ปัญหาอุปการณ์เชื่อมต่อเครือข่ายหลักไม่สามารถให้บริการได้ เป็นผลให้ผู้ใช้บริการไม่สามารถติดต่อสื่อสารกับเครือข่ายภายนอกได้ โดยมีสาเหตุดังนี้

เนื่องจากระบบเดิมมีการออกแบบให้เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้หมายเลขไอพีจริง อยู่ใน IP SUBNET เดียวกันทำให้เมื่อมีเครื่องคอมพิวเตอร์แม่ข่ายเครื่องใดเครื่องหนึ่งเกิดปัญหา เช่น การติดไวรัสคอมพิวเตอร์ ก็จะทำให้เกิดการกระจายตัวของไวรัส และปล่อยข้อมูลจำนวนมากออกมา ซึ่งจะเกิดผลกระทบกับเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมดใน IP SUBNET เดียวกัน รวมทั้งส่งผลกระทบต่ออุปกรณ์ในการเชื่อมต่อเครือข่ายหลักของมหาวิทยาลัย

เนื่องจากเดิมมีการออกแบบให้คอมพิวเตอร์แม่ข่ายตามคณะวิชาต่างๆสามารถใช้หมายเลขไอพีจริงได้ เพื่องเชื่อมต่อกับระบบอินเตอร์เน็ตโดยตรง เกิดช่องโห่วของระบบความปลอดภัย เป็นช่องทางในการโจมตีจากภายนอกได้ง่าย

2. ปัญหาการให้บริการ Mail Server มีผลกระทบให้เกิดปัญหาเกี่ยวกับการรับส่ง E-mail โดยมีสาเหตุดังนี้

เครื่อง Mail Server ที่ให้บริการอยู่มีอายุการใช้งานมานาน ทำให้เกิดปัญหา เช่น พื้นที่เก็บข้อมูล (Free space) ไม่เพียงพอต่อการเก็บที่เพิ่มขึ้น อุปกรณ์ภายในเสื่อมสภาพ ไม่สามารถใช้งานได้อย่างเต็มประสิทธิภาพ เครื่อง Mail Server ไม่ทำการแลกเปลี่ยน (Replication) ข้อมูลระหว่างกันได้ไม่สามารถรองรับชุดโปรแกรม (Software) รุ่นใหม่เช่น Window 2000 Server, Exchange 2000 Server เป็นต้น

กระจาย Mail Server ไปตามคณะและหน่วยงาน Mail Server แต่ละคณะวิชามีนโยบายการบริหารจัดการและการรักษาความปลอดภัยบนเครื่องแม่ข่ายแตกต่างและเนื่องจากระบบเครือข่าย NU Net มีการเชื่อมต่อกับ ระบบเครือข่ายอินเตอร์เน็ตเพียงจุดเดียว ณ ห้องแม่ข่ายหลักของมหาวิทยาลัยแต่เครื่อง Mail Server กระจายอยู่ตามคณะ ซึ่งหากการเชื่อมต่อระหว่างคณะกับห้องแม่ข่ายหลักไม่สามารถติดต่อกันได้ เช่น หนูกัดสายสื่อสัญญาณ จะเป็นผลให้ผู้ใช้บริการเครือข่ายในคณะนั้นๆ ไม่สามารถรับ e-mail ได้

ปัญหาผู้ดูแลระบบเครือข่าย ผู้ดูแลระบบส่วนกลางไม่สามารถเข้าไปดำเนินการแก้ไขปัญหาที่คณะหรือหน่วยงานนอกเวลาราชการได้ ทำให้เกิดการล่าช้าในการแก้ปัญหา และผู้ดูแลระบบเครือข่ายของคณะและหน่วยงานต่างๆมีหน้าที่รับผิดชอบหลายด้านจึงไม่มีเวลาในการควบคุมดูแลการให้บริการของเครื่องแม่ข่าย

MISSING

5.ปัญหาการให้บริการ DNS Server โดยมีสาเหตุ ดังนี้

5.1 DNS Server หลักมีเพียงเครื่องเดียว ทำให้เกิดความเสี่ยงต่อการให้บริการสูง

5.2 DNS Server ปัจจุบันเครื่องที่มหาวิทยาลัยใช้ทำหน้าที่นี้ เป็นครื่องคอมพิวเตอร์ที่ออกแบบมาสำหรับทำงานแบบ Desktop ไม่ได้ออกแบบมาสำหรับทำงานเป็นเครื่องคอมพิวเตอร์แม่ข่ายโดยเฉพาะ ซึ่งทำให้เกิดปัญหาการให้บริการ

6. ปัญหาอุปกรณ์ Core Switch มีอายุการใช้งานนาน และไม่มีระบบสำรอง เมื่อเกิดปัญหาทำให้ไม่สามารถใช้งานได้ทั้งระบบ

4.5.3 ปัญหาส่วนที่ 3 Distribution Zone

ปัญหาที่สำรวจพบ

1. ปัญหาผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ (Administrator) บางส่วนไม่มีความรู้ความเข้าใจเกี่ยวกับระบบเครือข่ายอย่างเพียงพอ โดยมีสาเหตุดังนี้

ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ของคณะต่างๆมีความรับผิดชอบหลายด้านจึงทำให้ไม่สามารถดูแล และจัดการ คอมพิวเตอร์แม่ข่ายตามคณะวิชาได้อย่างเต็มที่ เช่น การ update service pack และการ update virus pattern เป็นต้น

เทคโนโลยีมีความก้าวหน้าและเปลี่ยนแปลงอย่างรวดเร็ว ผู้ดูแลระบบเครือข่ายของไม่ได้รับการพัฒนาให้มีความรู้เท่าทันเทคโนโลยีและจากการสำรวจพบว่ามีการกระทำบางอย่างโดยรู้เท่าไม่ถึงการณ์ เช่น การนำโปรแกรมอื่นไปใช้งานในที่เครื่องแม่ข่าย และการเก็บข้อมูลอื่นๆที่ไม่เกี่ยวข้องในเครื่องแม่ข่ายเป็นผลให้เครื่องต้องรับภาระหนักและส่งผลกระทบให้ทำงานผิดพลาด

2. ปัญหาการเชื่อมต่อสื่อสัญญาณจากคณะต่างๆมายังส่วนกลางคืออาคาร CITCOMS ซึ่งการเชื่อมต่อสื่อสัญญานจากคณะต่างๆมายังส่วนกลาง ส่วนใหญ่การเชื่อมต่อด้วยสื่อสัญญาณ ATM ขนาด 155 Mbps เส้นทางเดียวกันนั้น ซึ่งหากเส้นทางดังกล่าวขาดการติดต่อ คณะนั้นก็จะขาดการติดต่อกับหน่วยงานอื่นได้ ซึ่งต้องใช้เวลานานในการเชื่อมต่อ และมีค่าใช้จ่ายในการเชื่อมต่อแต่ละครั้งสูง

4.5.4 ปัญหาส่วนที่ 4 Access Point Zone

ปัญหาที่สำรวจพบ

1. ปัญหาการขยายการเชื่อมต่อของระบบเครือข่ายภายในคณะ/หน่วยงาน โดยมีสาเหตุมาจากคณะหรือหน่วยงานจัดหาอุปกรณ์ในส่วนของ Access Point ที่ไม่สามารถทำงานร่วมกับอุปกรณ์หลักของมหาวิทยาลัยได้ และคณะวิชาจัดหาอุปกรณ์แล้วต่อเชื่อมแบบพ่วง (Chain hub/switch) ทำให้เกิดปัญหาในด้านประสิทธิภาพของเครือข่าย
2. ปัญหาการขาดความรู้ความเข้าใจในการใช้บริการเครือข่ายของผู้ใช้บริการระบบเครือข่ายคอมพิวเตอร์ โดยมีสาเหตุมาจากผู้ใช้บริการบางรายไม่มีความรู้พื้นฐานทางคอมพิวเตอร์และไม่ได้รับการอบรมพัฒนาให้มีความสามารถ หรือไม่ได้ใช้งานเครือข่ายคอมพิวเตอร์เป็นเวลานาน หลังจากที่ได้รับการอบรมการใช้บริการเครือข่ายคอมพิวเตอร์
3. ปัญหาการขาดนโยบายการใช้งานอินเตอร์เน็ต และไม่มีบทลงโทษอย่างจริงจังต่อผู้กระทำความผิดที่ก่อให้เกิดความเสียหายต่อระบบเครือข่ายคอมพิวเตอร์ และผู้ดูแลระบบเครือข่ายบางหน่วยงานต้องการทดลองและเรียนรู้การทำงานของระบบเครือข่ายจนเป็นเหตุให้ระบบมีความเสียหายเกิดขึ้น

4.5.5 ค่าสถิติเกี่ยวกับการใช้งาน

การวิเคราะห์ระบบเครือข่ายต้องมีการวางแผนเก็บรวบรวมข้อมูลในรูปแบบของสถิติการใช้งานระบบเครือข่าย (Network Statistics) เพื่อนำมาใช้ประกอบการวิเคราะห์ประสิทธิภาพข้อมูลสถิติที่ดีควรถูกเก็บรวบรวมผ่านทางฮาร์ดแวร์เรียกว่าอุปกรณ์ตรวจสอบประสิทธิภาพ (Performance Monitor)

1. ซอฟต์แวร์สำหรับการวิเคราะห์ค่าสถิติ (Statistical Analysis System) ที่รวบรวมข้อมูลดิบจากแหล่งต่างๆแล้วนำมาวิเคราะห์ด้วยวิธีทางสถิติ เช่น

การใช้โปรแกรม MRTG (Multi Router Traffic Grapher) เพื่อตรวจสอบคุณภาพการเชื่อมต่อระบบเครืออข่ายคอมพิวเตอร์ ซึ่งสามารถทำได้หลายระดับ เช่น ทำการตรวจสอบในส่วนของการเชื่อมต่อภายนอกหรือการเชื่อมต่อกับผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider) ทำการตรวจสอบในส่วนของการกระจายการเชื่อมต่อไปยังคณะและหน่วยงานต่างๆภายในมหาวิทยาลัย (Distribution Zone) เพื่อวัดสถิติหรือปริมาณการใช้ Bandwidth ของมหาวิทยาลัย

การใช้โปรแกรม Bricks เพื่อ ตรวจสอบความเร็วในการเชื่อมต่อของอุปกรณ์ Gigabit Ethernet เปรียบเทียบ ATM

2. ซอฟต์แวร์บันทึกเหตุการณ์ (Log files) ทำหน้าที่เก็บรวบรวมและบันทึกเพื่อนำมาวิเคราะห์ภายหลัง เช่น บันทึกรายงานการทำงาน (Transaction Logs) บันทึกการส่งข้อมูล (Message logs) และบันทึกทางเดิน (Line traces) เช่น

การใช้โปรแกรม Log files เพื่อบันทึก Transaction ของระบบฐานข้อมูลบุคลากรซึ่งจะเก็บบันทึกกิจกรรมที่เกิดขึ้นในระบบฐานข้อมูลบุคลากรทำให้ผู้ดูแลระบบทราบเวลา และการกระทำของบุคคลใดบุคคลหนึ่ง ที่เข้ามาในระบบ

การใช้โปรแกรม Log files เพื่อบันทึก Transaction ของเครื่องแม่ข่ายให้บริการอินเตอร์เน็ตของคณะและหน่วยงาน หรือเครื่องแม่ข่ายให้บริการ e-mail เพื่อให้ทราบตัวบุคคล เวลา และการกระทำของบุคคลที่เข้ามาใช้งานเครื่องแม่ข่าย

3. การใช้ซอฟต์แวร์เพื่อการทำ Quality of Service

4.5.6 แนวทางการแก้ไขปัญหาส่วนที่ 1 Internet Connection Zone

1.จากปัญหาระบบเครือข่ายคอมพิวเตอร์ไม่มีเสถียรภาพเนื่องจากเกิดปัญหาจากการเชื่อมต่อระดับต่างๆ เช่น การเชื่อมต่อผู้ให้บริการอินเต่อร์เน็ต การเชื่อมต่อกันระหว่างอาคารภายในมหาวิทยาลัย และการเชื่อมต่อภายในอาคาร ทำให้ต้องมีการออกแบบระบบใหม่ที่แก้ปัญหาดังกล่าวให้มีความเสถียรภาพและน่าเชื่อถือ (Reliability) และส่วนเชื่อมต่อภายนอกเป็นส่วนที่ต้องไม่มีจุดอ่อน หรือจุดที่หยุดทำงานแล้วระบบหยุดทำงานทั้งหมด (Single point of frailer) สามารถรักษาการเชื่อมต่อไว้ได้ตลอดเวลา และจะต้องมีความสามารถในการตรวจสอบเส้นทางว่าเส้นทางการเชื่อมต่อใดยังใช้งานได้ และเส้นทางใดเกิดปัญหาการเชื่อมต่อ และระบบการตรวจสอบต้องมีความรวดเร็วและสามารถตรวจสอบได้ทันที จึงต้องมีระบบการตรวจสอบสถานะของระบบการเชื่อมต่อ เช่น การใช้ระบบการติดตามตรวจสอบ (Monitoring) ของโปรแกรม MRTG

2.ส่วนเชื่อมต่อภายนอก (Internet Connection Zone) ระบบเครือข่ายคอมพิวเตอร์แบบเดิมของมหาวิทยาลัยเป็นรูปแบบของ Static Link ซึ่งเป็นการใช้งานได้ระดับหนึ่ง การออกแบบระบบใหม่ต้องเป็นแบบ Dynamic Link ซึ่งเป็นการใช้งานเส้นทางได้ประโยชน์สูงสุด

3.ส่วนเชื่อมต่อภายนอกต้องมีความยืดหยุ่นสูงเนื่องจากเป็นส่วนของการเชื่อมต่ออันดับแรกที่สำคัญที่สุด หากส่วนนี้เกิดปัญหาผู้ใช้งานจะไม่สามารถใช้งานอินเตอร์เน็ตได้ การออกแบบให้มีความยืดหยุ่นสูงโดยการมีเส้นทางสำรองและมีการนำเส้นทางสำรองมาใช้งานได้โดยอัตโนมัติ เมื่อเส้นทางใดเส้นทางหนึ่งเกิดปัญหาโดยไม่ต้องการหยุดการทำงานของระบบเครือข่าย และผู้ใช้งานยังใช้งานได้

ตามปกติโดยที่ไม่รู้สึกว่าระบบเครือข่ายมีปัญหาเกิดขึ้น โดยการติดตั้งอุปกรณ์ Link Proof เพื่อทำการหน้าที่ในการบริหารจัดการ Bandwidth โดยอัตโนมัติ

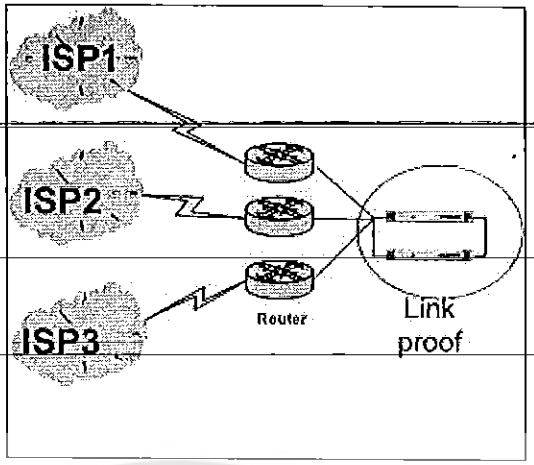
4.5.6.1 สรุปการวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์

การวิเคราะห์และออกแบบระบบเครือข่ายคอมพิวเตอร์ในส่วนเชื่อมต่อภายนอก คือการติดตั้งอุปกรณ์ Link Prof หลัง Router ที่เชื่อมต่อกับผู้ให้บริการอินเตอร์เน็ต เพื่อรองรับความต้องการดังที่ได้กล่าวมาแล้ว คือ

1. ต้องมีระบบสลับการเชื่อมต่ออัตโนมัติเมื่อสายสัญญาณขาด
2. ต้องสามารถตรวจสอบการเชื่อมต่อถึงปลายทางได้ (Full past check)
3. เป็นการเชื่อมต่อแบบไม่ระบุเส้นทาง (Dynamic Link)
4. สามารถเชื่อมต่อกับผู้ให้บริการ Internet ได้อย่างน้อย 4 ราย
5. ต้องสามารถทำ Load Balance Link ได้ เพื่อให้ใช้งาน Bandwidth ได้อย่างคุ้มค่า
6. สามารถระบุเส้นทางที่เชื่อมต่อได้ว่า Link มีการเชื่อมต่อที่เร็วที่สุด

ข้อดี ของระบบคือ ระบบจะมีเสถียรภาพมากกว่าเดิมเพราะว่าการเชื่อมต่อต่างๆจะไม่ขาด คือเมื่อ Link ใดขาดจะมีการสลับไปใช้ Link อื่นอย่างอัตโนมัติสามารถทำ Load Balance Link ซึ่งเป็นการใช้ Bandwidth อย่างคุ้มค่าที่สุดและสามารถระบุ Link ที่เร็วที่สุดที่ใช้ในการเชื่อมต่อได้โดยคุณสมบัติของ Link proof จะทำให้ระบบมีเสถียรภาพขึ้นและทำให้ระบบไม่ขาดการติดต่อสื่อสาร

ข้อเสีย ของระบบคือ หากอุปกรณ์ Link proof ขัดข้องจะทำให้ระบบขาดการเชื่อมต่อกับภายนอกทั้งหมด ซึ่งมีทางป้องกันได้ และหากใช้เวลาในการติดต่อ Server ภายนอกมหาวิทยาลัยในครั้งแรกนานกว่าเพราะต้องรอการตรวจสอบความเร็วในการเชื่อมต่อว่า Link ใดมีการเชื่อมต่อที่เร็วที่สุด



รูปที่ 4-18 การเชื่อมต่อระบบเครือข่ายภายนอก

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

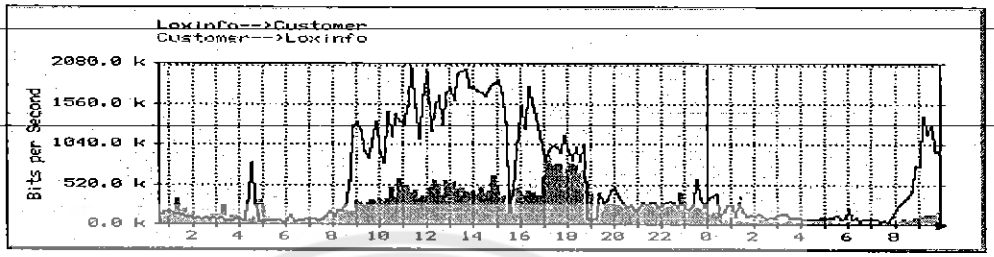
การกำหนดโครงร่างส่วนการเชื่อมต่อระบบเครือข่ายภายนอก (Internet Connection Zone) สำหรับการสื่อสารข้อมูล เพื่อเป็นส่วนที่ใช้ในการเชื่อมต่อกับอินเตอร์เน็ตภายนอกมหาวิทยาลัย และสลับการเชื่อมต่อในสภาวะที่เชื่อมต่อสายใดไม่สามารถใช้งานได้ โดยมีการเชื่อมต่อจะเชื่อมต่อกับผู้ให้บริการอินเตอร์เน็ตภายนอก (ISP) สามรายคือ

1. Uni Net ใช้การเชื่อมต่อแบบ Interface ATM OC-3
2. ISP เอกชนใช้การเชื่อมต่อแบบ Interface V35 (Loxinfo)
3. ISP เอกชนใช้การเชื่อมต่อแบบ Interface V35 (KSC)

สาเหตุที่ต้องออกแบบให้มีผู้ใช้บริการอินเตอร์เน็ต 3 ราย เนื่องจากบริการของ Uni Net เป็นบริการที่ทบวงมหาวิทยาลัยได้จัดให้แก่สถาบันการศึกษา แต่ยังไม่ได้มาตรฐานด้านคุณภาพ และยังมีเสถียรภาพเพียงพอในการใช้งาน ทำให้เกิดปัญหาการให้บริการเป็นประจำจึงไม่สามารถคาดหวังในการใช้งานได้สำหรับผู้ให้บริการอินเตอร์เน็ตเอกชนต้องมี 2 ราย เพื่อใช้เป็นระบบสำรองการใช้งานหากเส้นทางใดเกิดเสียหายหรือมีข้อผิดพลาด ระบบก็ยังสามารถให้บริการต่อไปได้ แต่อาจมีปัญหาการรับส่งข้อมูลช้าลง

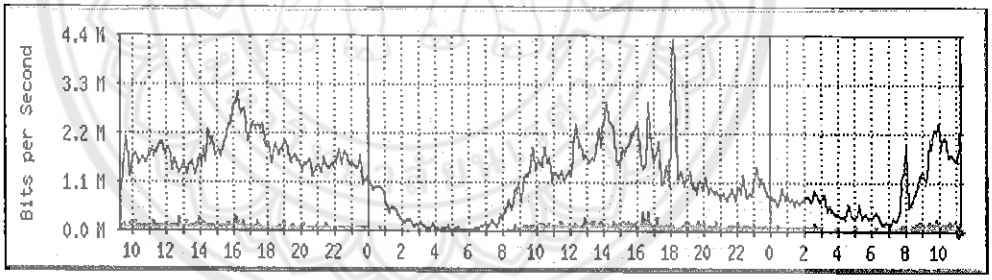
4.5.6.2 การเปรียบเทียบส่วน Internet Connection Zone ด้วยโปรแกรม MRTG

การเปรียบเทียบการใช้บริการระบบก่อนการติดตั้งอุปกรณ์ Link Proof เพื่อทำหน้าที่ Load balance link และแสดงถึงสถิติหลังการทดลองติดตั้งแล้ว ดังนี้



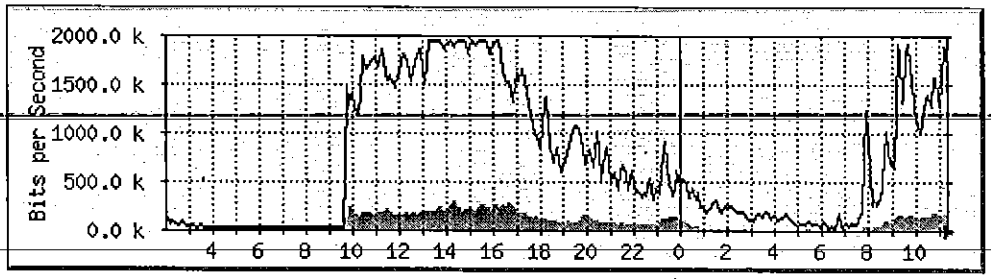
รูปที่ 4-19 กราฟการติดตั้งอุปกรณ์ Link Proof ของ ISP รายที่ 1

จากภาพแดงการใช้งานก่อนการติดตั้งอุปกรณ์ Link Proof เพื่อทำหน้าที่เป็น Load Balance Link ณ วันที่ 1 สิงหาคม 2546 ของบริษัท Loxinfo http://corp.loxinfo.co.th/



รูปที่ 4-20 กราฟการติดตั้งอุปกรณ์ Link Proof ของ Uni Net

จากภาพแสดงปริมาณการใช้งานก่อนการติดตั้งอุปกรณ์ LinkProof เพื่อทำหน้าที่ Load Balance Link ณ วันที่ 1 สิงหาคม 2546 ของ UniNet http://seenet.uni.net.th:555/nu/router/7200/202.28.31.613.html



รูปที่ 4-21 กราฟการติดตั้งอุปกรณ์ Link Proof ของ ISP รายที่ 2

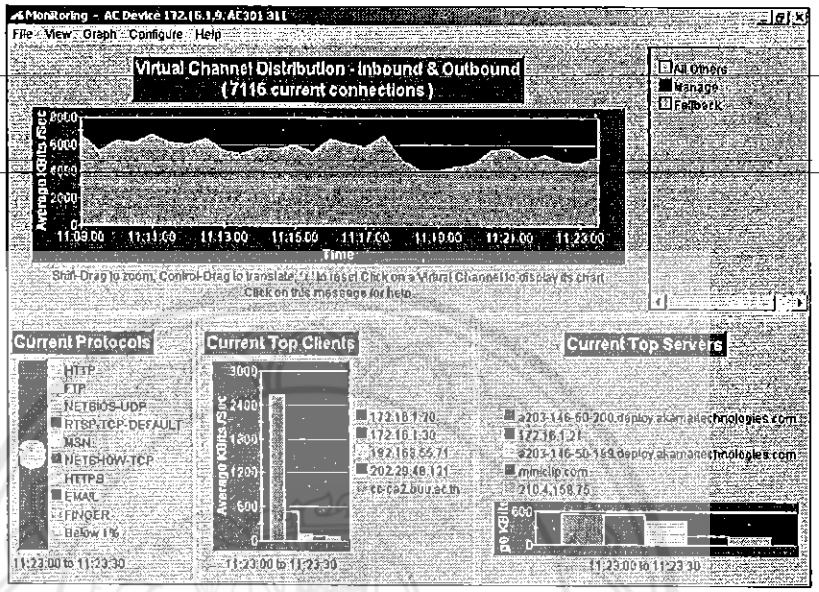
จากภาพแสดงปริมาณการใช้งานหลังการติดตั้งอุปกรณ์ Link Proof เพื่อทำหนาที่ Load Balance Link ณ วันที่ 1 สิงหาคม 2546 ของบริษัท Uni Net

http://nctmgr.ksc.net.th/mrtg/branch/phitsanulok/nu.html

จากรูปที่ 4-19 และ 4-20 และ 4-21 แสดงให้เห็นได้อย่างชัดเจนว่ามีการกระจายตัวของช่องสัญญาณทั้ง 3 ISP อย่างเหมาะสมทั้งขาเข้าและขาออก ซึ่งแสดงให้เห็นว่าสามารถใช้ช่องสัญญาณได้คุ้มค่า และช่วยให้เสถียรภาพ โดยการสลับการเชื่อมต่อในกรณีที่เกิดเหตุขัดข้องจะเป็นไปโดยอัตโนมัติ

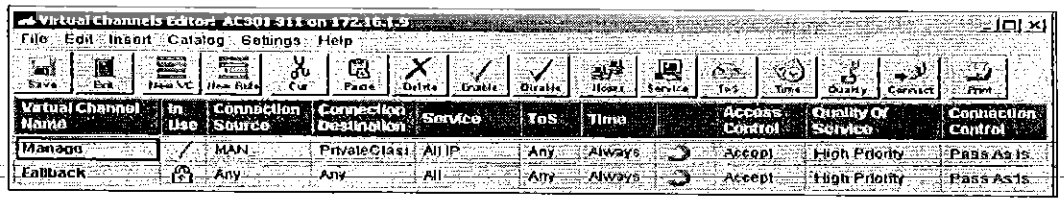
4.5.6.3 การทำ Quality of Service ของระบบการเชื่อมต่อกับระบบภายนอก

การทำ Quality of Service โดยใช้ Software ของอุปกรณ์ Traffic Shaper แสดงดังรูปต่อไปนี้



รูปที่ 4-22 การทำ Quality of Service

ด้านบน(สีเขียว)เป็นลักษณะการใช้งานแบบ Non Qos ซึ่งจะมาสามารถแสดงและกำหนดการใช้งานได้ ส่วนด้านล่างซ้ายมือเป็นการทำ Qos ของระบบการเชื่อมต่อกับภายนอก ซึ่งสามารถบอกถึงการใช้งานได้ และการกำหนดการใช้งาน ทั้งขนาด ช่องสัญญาณ ลำดับก่อนหลังและการรับประกันขนาดช่องสัญญาณ สำหรับบริการที่สำคัญ



รูปที่ 4-23 การตั้งค่าของ Quality of Service

จากภาพแสดงหน้าจอของวิธีการตั้งค่า Quality of Service ของระบบการติดตามตรวจสอบระบบ โดยมีความหมายของการตั้งค่าต่างๆ ดังนี้

1. Virtual Channel name คือชื่อของกฎต่างๆ ที่ผู้ดูแลระบบได้ตั้งค่าไว้
2. In use คือการกำหนดเป็นสภาวะ Enable หรือ Disable
3. Connection Source คือต้นทางการส่ง
4. Connection destination คือส่งถึงปลายทาง
5. Service คือรูปแบบการให้บริการ (port layer 4)
6. ToS (Type of Service) คือการกำหนดการใช้งานโดย Packet ToS ที่ส่ง
7. Time คือเวลาการให้บริการ
8. Access คือสถานการณ์ที่ให้บริการ
9. Qos (Quality of Service) คือกำหนดการให้บริการ หรือ Bandwidth Priority
10. Connection Control คือการทำ Traffic redirect

4.5.6.4 แนวทางการแก้ไขปัญหาส่วนที่ 2 Core Switch Zone

1.การแก้ไขปัญหาอุปกรณ์เชื่อมต่อเครือข่ายหลักไม่สามารถให้บริการได้ต้องทำการปรับรื้อระบบ IP Address ใหม่เพื่อให้เป็นระบบที่มีความปลอดภัยสูง และจะมีการมอบ IP จริงให้แก่หน่วยงานที่ขออนุญาตเป็นลายลักษณ์อักษร โดยผู้ดูแลระบบส่วนกลางต้องคอยติดตามตรวจสอบตลอดเวลา

2.การแก้ไขปัญหาระบบ Mail Server ต้องทำการย้ายเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ e-mail จากคณะและหน่วยงานต่างๆ มาติดตั้ง ณ ส่วนกลางทั้งหมด เพื่อความสะดวกในการดูแลและบำรุงรักษา และต้องทำการ Upgrade เครื่องคอมพิวเตอร์แม่ข่ายให้มีประสิทธิภาพการรองรับการทำงานได้ ทั้งพื้นที่เก็บข้อมูล (Free space) และ Software และต้องมีการพัฒนาผู้ดูแลระบบเครือข่ายส่วนกลางและคณะให้มีความสามารถเพิ่มขึ้น สำหรับอำนาจหน้าที่และความรับผิดชอบของผู้ดูแลระบบเครือข่ายระดับหน่วยงานและคณะยังคงเดิม คือสามารถ Access เข้ามาแก้ไขปรับปรุงข้อมูลบน Mail Server ของคณะตนเองได้ตามปรกติ เพื่อให้เกิดความคล่องตัวในการใช้งาน

3.การแก้ไขปัญหาการให้บริการ Domain Controller หรือคอมพิวเตอร์แม่ข่าย การให้บริการเก็บบัญชีรายชื่อผู้ใช้ สิทธิการใช้งาน ต้องทำการย้ายเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ Domain Controller จากคณะและหน่วยงานต่างๆ มาติดตั้ง ณ ส่วนกลางทั้งหมด เพื่อความสะดวกในการดูแลและบำรุงรักษา ทั้งพื้นที่เก็บข้อมูล (Free space) และการแก้ไขปัญหา Trust relationship ระหว่าง

Domain โดยการ Upgrade Software ให้เป็น Window 2000 Server หรือ Exchange 2000 Server และต้องมีการพัฒนาผู้ดูแลระบบเครือข่ายส่วนกลางให้มีความสามารถเพิ่มขึ้น

4.การแก้ไขปัญหาการให้บริการ ISA: Internet Securities and Accelerator หรือเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ตรวจสอบข้อมูล เข้าและออก แปลงหมายเลขไอพีภายใน ให้เป็นหมายเลขไอพีจริง ต้องทำการ Upgrade เครื่องคอมพิวเตอร์แม่ข่ายให้มีประสิทธภาพรองรับการทำงานได้ และต้องจัดหาเครื่องคอมพิวเตอร์แม่ข่ายเพิ่มขึ้นเพื่อทำหน้าที่เป็น Web Caching

5.การแก้ไขปัญหาการให้บริการ DNS Server โดยการจัดหาเครื่องคอมพิวเตอร์แม่ข่ายเพิ่มขึ้นและเพื่อทำหน้าที่ DNS Server

6.การแก้ไขปัญหาส่วนการเชื่อมต่อหลัก ที่ทำหน้าที่ในการเชื่อมต่อระบบเครือข่ายทั้งมหาวิทยาลัยเข้าสู่ส่วนกลาง ต้องทำการออกแบบระบบให้มีความต้องและเชื่อถือได้ (Reliability) ส่วนเชื่อมต่อหลัก (Core Switch Zone) ต้องมีระบบสำรองการทำงาน (Backup System) เพื่อป้องกันการทำงานที่ผิดพลาด ต้องมีการเชื่อมต่ออย่างน้อย 2 เส้นทาง และมีระบบตรวจสอบการเชื่อมต่อว่ายังใช้งานอยู่ได้และสลับการเชื่อมต่ออัตโนมัติหากเกิดการผิดพลาดขึ้น และต้องมีส่วนประกอบความต้องการดังนี้

6.1 การออกแบบต้องมีระบบรักษาความปลอดภัยที่ป้องกันการบุกรุกได้ และรองรับการใช้งานของมหาวิทยาลัย

6.2 ต้องรองรับการจัดสรร Bandwidth ที่ตรงกับการใช้งานของมหาวิทยาลัย

6.3 ต้องเป็นอุปกรณ์ที่ออกแบบมาเฉพาะสำหรับรักษาความปลอดภัย

6.4 Core Switch ต้องเป็น Layer 3 GB Switch ทั้งมหาวิทยาลัย

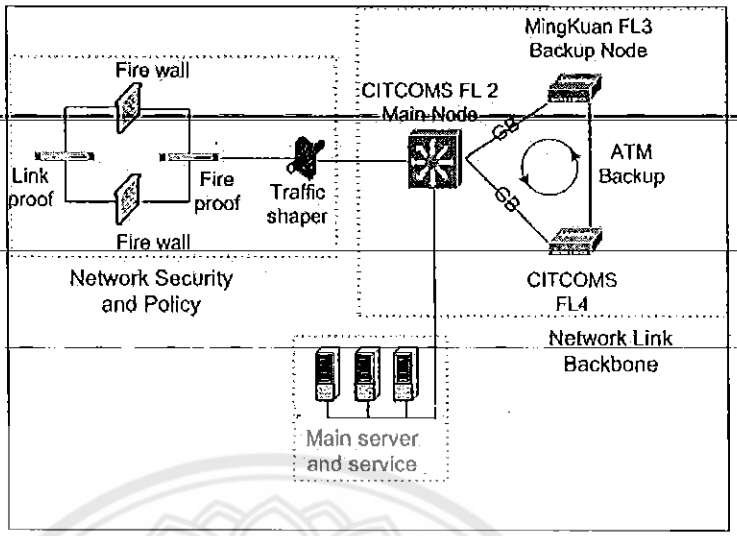
6.5 การเชื่อมต่อ Main Switch แต่ละ Node ใช้ Fiber optic

6.6 การเชื่อมต่อต้องมีการทำ Link สำรองไว้

6.7 เครื่อง Server และบริการต่างๆ ที่ทางมหาวิทยาลัยมีต้องอยู่ภายใต้การควบคุมของ Core Switch

6.8 เครื่อง Server และการให้บริการต่างๆ ต้องรองรับการทำงานในระบบ IP base เท่านั้น

จากข้อมูลดังกล่าวข้างต้นจึงจำเป็นต้องปรับปรุงระบบในส่วนการเชื่อมต่อหลักใหม่เพื่อให้รองรับการทำงานการใช้งานในอนาคตจึงได้ปรับปรุงโครงสร้างระบบเครือข่ายส่วนเชื่อมต่อหลักดังรูป



รูปที่ 4-24 แสดงภาพการเชื่อมต่อของส่วนเชื่อมต่อหลัก

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

ส่วน Network Security and Policy เป็นส่วนที่ต้องการอุปกรณ์เฉพาะด้านเพื่อเสถียรภาพการทำงาน ซึ่งประกอบไปด้วยอุปกรณ์ Firewall, Load Balance Firewall, Traffic shaper อุปกรณ์ในส่วนนี้จะทำหน้าที่กำหนด Policy ตรวจสอบและกำหนดขนาด Bandwidth

ส่วน Network link backbone เป็นแกนกลางในการเชื่อมต่อระบบทั้งมหาวิทยาลัย ซึ่งเชื่อมไปยังคณะต่างๆ และเป็นจุดรวมบริการทุกชนิดของมหาวิทยาลัย โดยมี Layer 3 Switch เป็น Core Switch หลัก และเชื่อมด้วย GB ไปยัง Backup Node หลัก 2 Node คือ อาคารมิ่งขวัญชั้น 3 และอาคาร CITCOMS ชั้น 4 ซึ่งมี ATM ทำหน้าที่เป็น Backup ซึ่งกันและกัน

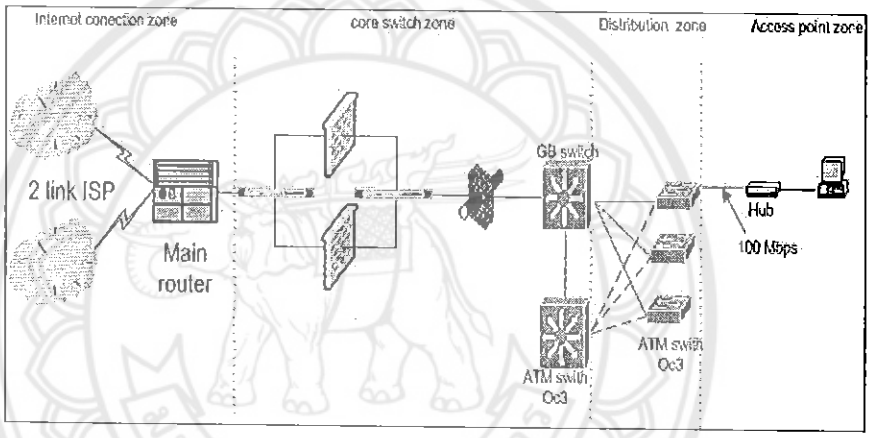
ส่วนของ Main Server and Service เป็นส่วนของการให้บริการหลักของมหาวิทยาลัย เมื่อทำการปรับปรุงแล้วจะมีข้อดีและข้อเสีย ดังนี้

ข้อดี เมื่อปรับปรุงระบบเสร็จแล้ว จะรับรองการทำงานของระบบทั้งมหาวิทยาลัย ซึ่งจะควบคุมดูแลโดยผู้ดูแลระบบส่วนกลาง ส่วนการเชื่อมต่อนี้จะไม่มีการขาดการเชื่อมต่อ เนื่องจากมีการทำระบบ Link สำรองไว้แล้ว

ข้อเสีย มีส่วนที่ต้องให้การดูแลเป็นพิเศษ และมีอุปกรณ์บางชนิดที่หยุดทำงานไม่ได้คือ Core Switch และ fireproof ซึ่งควรต้องมีอุปกรณ์สำรอง หรือมีการซ้อมรับสถานการณ์ต่างๆ ไว้ล่วงหน้า

การกำหนดโครงร่างส่วนการเชื่อมต่อหลัก (Core Switch Zone) นี้เป็นส่วนหลักในการเชื่อมต่อจากส่วนเชื่อมต่อระบบภายนอก ทำหน้าที่ในการเชื่อมต่อระบบเครือข่ายทั้งมหาวิทยาลัยเข้าสู่ส่วนกลาง โดยการเชื่อมต่อการสื่อสารจากอาคารมิ่งขวัญโดยใช้ GB Ethernet บนสายใยนำแสงแบบ Single Mode

สำหรับการออกแบบในส่วนการเชื่อมต่อหลักระหว่างอาคาร CITCOMS ไปยังอาคารหรือหน่วยงานต่างๆ ภายในมหาวิทยาลัย รวมทั้งวิทยาเขต สถาบันสมทบ และศูนย์วิทยบริการนั้น ต้องทำการปรับปรุงอุปกรณ์ Core Switch ของแต่ละหน่วยงาน โดยการโยกย้ายอุปกรณ์ switching ตัวเก่าของคณะใหญ่ๆไปใช้ในหน่วยงานเล็กๆ และจัดซื้อ Core Switch ตัวใหม่ที่เป็นเทคโนโลยี Gigabit Ethernet มาใช้ในคณะใหญ่ๆต่อไป จะทำให้เพิ่มประสิทธิภาพของระบบได้



รูปที่ 4-25 โครงร่างการเชื่อมต่อหลัก

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

โครงสร้างของส่วนการเชื่อมต่อหลักประกอบไปด้วยอุปกรณ์ดังนี้

1. Load balance firewall (Radware Fireproof)
2. Firewall:
   - Watchguard Firewall II
   - Watchguard Firewall 2500
3. Traffic shaper (Allot AC301)
4. Core Switch
   - Omi Switch S/R CPM MPX
   - 4 port GB Single Mode

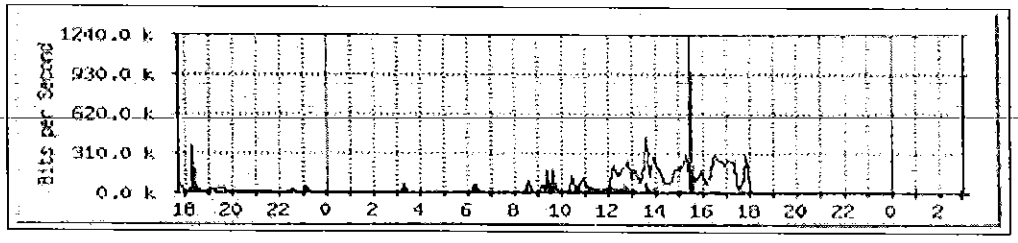
- 4 port GB Multi Mode
- 64 port 10/100 Mbps

5. Main Switch Mingkuan floor 3
   - Omi Switch CPU MPM 1G
   - 2 port GB Single Mode
   - 10 port ATM OC-3
   - 12 port 100 Mbps
6. Main Switch CITCOMS floor 2
   - Omi Switch CPU MPM 1G
   - 2 port GB Multimode
   - 16 port ATM OC-3
   - 96 port 10 Mbps

4.5.6.5 การประเมินเพื่อตรวจสอบคุณภาพการเชื่อมต่อด้วยโปรแกรม MRTG

1. การเปรียบเทียบส่วนเชื่อมต่อ Core Switch Zone ไปยัง Distribution Zone ด้วยโปรแกรม MRTG (Multi Router Traffic Grapher)

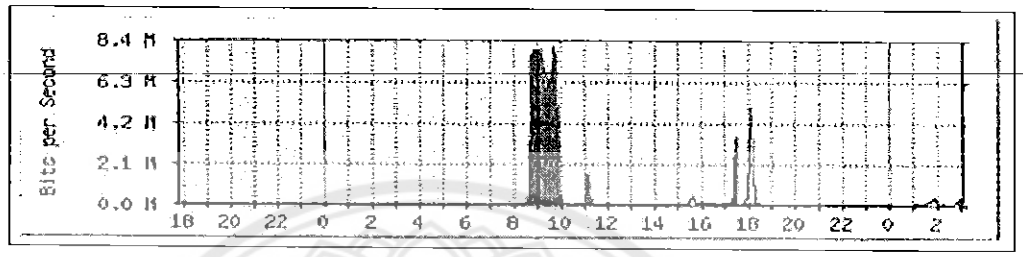
ในการตวจสอบการเชื่อมต่อด้วย MRTG สรุปผลได้ว่า ไม่สามารถบอกความแตกต่างได้อย่างชัดเจน เพราะในขณะที่ทำการวัดนี้มีปริมาณการใช้งานที่ไม่มากพอที่จะทำการวัดได้ตลอดเวลา ดังนั้นผลการทดสอบนี้ จึงเป็นเพียงการบันทึกการใช้งานตามปกติเท่านั้น หากต้องการตรวจสอบขนาดช่องสัญญาณจริงที่ใช้งานได้ จะตรวจสอบด้วย Brick Software จะเห็นถึงความแตกต่างของช่องสัญญาณมากกว่า



รูปที่ 4-26 การใช้งานช่องสัญญาณของคณะศึกษาศาสตร์

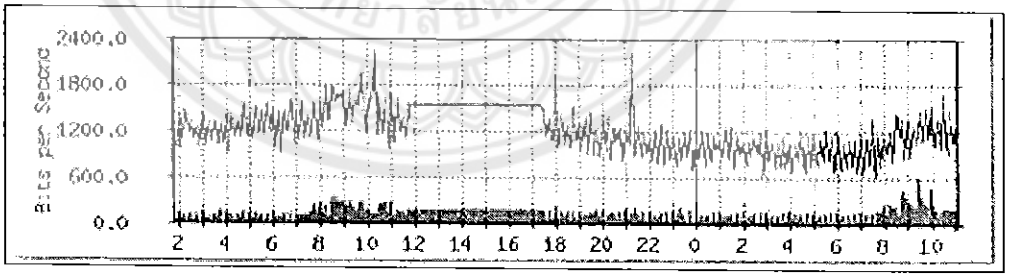
(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

จากภาพความสัมพันธ์การทดสอบสถิติการใช้งานช่องสัญญาณระบบเครือข่ายคอมพิวเตอร์ของคณะศึกษาศาสตร์ ณ วันที่ 1 สิงหาคม 2546 จะเห็นว่ามีการใช้สัญญาณเพื่อออกไปสู่ภายนอกประมาณ 1 Kbps ถึง 400 Kbps และมีการใช้ช่องสัญญาณเพื่อรับเข้าข้อมูลสู่ภายในมหาวิทยาลัยประมาณ 1 Kbps ถึง 1,240 Kbps



รูปที่ 4-27 การใช้งานช่องสัญญาณของคณะแพทย์ศาสตร์
(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

จากภาพความสัมพันธ์การทดสอบสถิติการใช้งานช่องสัญญาณระบบเครือข่ายคอมพิวเตอร์ของคณะแพทย์ศาสตร์ ณ วันที่ 1 สิงหาคม 2546 จะเห็นว่ามีการใช้สัญญาณเพื่อออกไปสู่ภายนอกประมาณ 1 Kbps ถึง 5 Mbps และมีการใช้ช่องสัญญาณเพื่อรับเข้าข้อมูลสู่ภายในมหาวิทยาลัยประมาณ 1 Kbps ถึง 8 Mbps



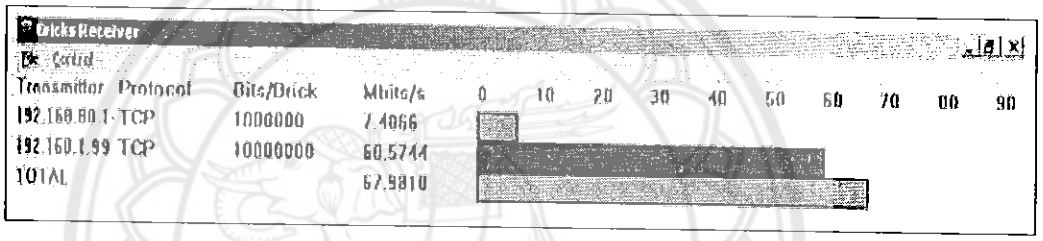
รูปที่ 4-28 การใช้งานช่องสัญญาณของคณะเกษตรศาสตร์ฯ
(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

จากภาพความสัมพันธ์การทดสอบสถิติการใช้งานช่องสัญญาณระบบเครือข่ายคอมพิวเตอร์ของคณะเกษตรศาสตร์ฯ ณ วันที่ 1 สิงหาคม 2546 จะเห็นว่ามีการใช้สัญญาณเพื่อออกไปสู่ภายนอกประมาณ 1 Kbps ถึง 2,300 Kbps และมีการใช้ช่องสัญญาณเพื่อรับเข้าข้อมูลสู่ภายใน

มหาวิทยาลัยประมาณ 1 Kbps ถึง 600 Kbps ซึ่งจะเห็นได้ว่าคณะเกษตรศาสตร์มีการใช้ช่อง สัญญาณสูงกว่าคณะอื่น เนื่องจากอุปกรณ์ Core Switch หลักใช้แบบ GB Ethernet

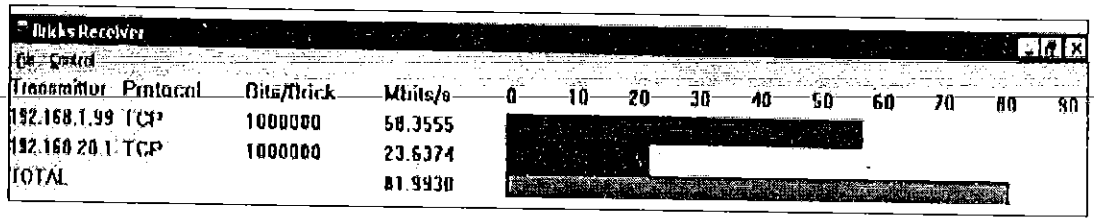
4.5.6.6 ผลการทดลองความเร็วในการเชื่อมต่อของ GB กับ ATM ด้วยโปรแกรม Bricks

โปรแกรม Brick เป็นโปรแกรมที่ใช้สร้าง Packet รับ-ส่งระหว่าง Brick Receiver ในขนาดช่องสัญญาณสูงสุดของช่องสัญญาณที่ทำได้ และค่าที่วัดได้เป็นขนาดของช่องสัญญาณที่ทำได้โดยทดสอบใช้การทดสอบใช้ Brick Receiver นี้ได้ติดตั้งที่ศูนย์กลางเครือข่าย CITCOMS เพื่อทำการทดสอบไปยังคณะเกษตรศาสตร์ฯ ซึ่งเป็นการเชื่อมต่อด้วยระบบ GB โดยเปรียบเทียบกับคณะแพทย์ศาสตร์และคณะมนุษย์ศาสตร์และคณะสังคมศาสตร์ ซึ่งเป็นการเชื่อมต่อด้วยระบบ ATM ซึ่งได้ผลดังนี้



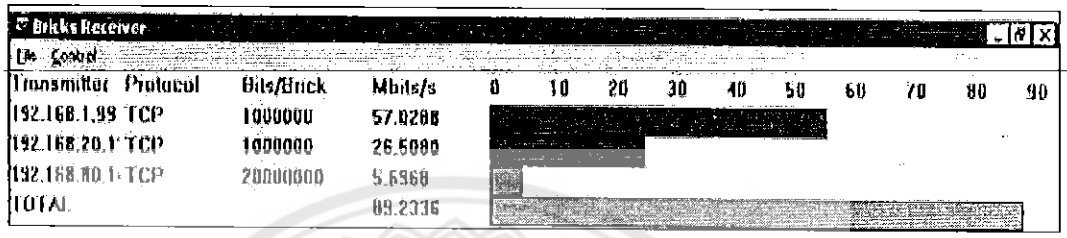
รูปที่ 4-29 ผลการทดสอบเปรียบเทียบระหว่างคณะเกษตรศาสตร์ฯกับคณะแพทย์ศาสตร์
(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

จากภาพแสดงให้เห็นการทดลองความเร็วในการรับส่งข้อมูลของคณะเกษตรศาสตร์ฯ (สีแดง) ที่เชื่อมต่อด้วยอุปกรณ์ Core Switch ที่เป็น GB มีค่าความเร็วเท่ากับ 60.5744 Mbits/s และความเร็วในการรับส่งข้อมูลของคณะแพทย์ศาสตร์ (สีเขียว) ที่เชื่อมต่อด้วย ATM มีค่าความเร็วเท่ากับ 7.4066 Mbits/s



รูปที่ 4-30 ผลการทดสอบเปรียบเทียบระหว่างคณะเกษตรศาสตร์ฯกับคณะมนุษยศาสตร์ฯ
(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

จากภาพแสดงให้เห็นการทดลองความเร็วในการรับส่งข้อมูลของคณะเกษตรศาสตร์ฯ (สีแดง) ที่เชื่อมต่อด้วยอุปกรณ์ Core Switch ที่เป็น GB มีค่าความเร็วเท่ากับ 58.3555 Mbits/s และความเร็วในการรับส่งข้อมูลของคณะมนุษยศาสตร์ฯ (สีน้ำเงิน) ที่เชื่อมต่อด้วย ATM มีค่าความเร็วเท่ากับ 23.6374 Mbits/s



รูปที่ 4-31 ผลการทดสอบเปรียบเทียบระหว่างคณะเกษตรศาสตร์ฯกับคณะมนุษยศาสตร์ฯ และคณแพทย์ศาสตร์
(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

จากภาพแสดงให้เห็นการทดลองความเร็วในการรับส่งข้อมูลของคณะเกษตรศาสตร์ฯ (สีแดง) ที่เชื่อมต่อด้วยอุปกรณ์ Core Switch ที่เป็น GB มีค่าความเร็วเท่ากับ 57.0288 Mbits/s และความเร็วในการรับส่งข้อมูลของคณะมนุษยศาสตร์ฯ (สีน้ำเงิน) ที่เชื่อมต่อด้วย ATM มีค่าความเร็วเท่ากับ 26.5080 Mbits/s และความเร็วในการรับส่งข้อมูลของคณะแพทย์ศาสตร์ (สีเขียว) ที่เชื่อมต่อด้วย ATM มีค่าความเร็วเท่ากับ 5.6968 Mbits/s

4.5.6.7 แนวทางการแก้ไขปัญหาส่วนที่ 3 Distribution Zone

1. การแก้ไขปัญหาด้านบุคลากร ต้องมีการพัฒนาความรู้ความสามารถของบุคลากรอยู่ตลอดเวลา เพื่อให้มีความรู้ความสามารถบริหารจัดการระบบได้อย่างมีประสิทธิภาพ และต้องมีการแบ่งหน้าที่ความรับผิดชอบงานกันอย่างชัดเจน เพื่อเป็นการกำหนดขอบเขตการทำงาน โดยมีระบบการตรวจสอบและติดตามประเมินผลการทำงานผู้ดูแลระบบเครือข่าย

2. การแก้ไขปัญหาส่วนกระจาย (Distribution Zone) ซึ่งเป็นส่วนที่มีการปรับจาก Core Switching ซึ่งเดิมมีเพียงชุดเดียวซึ่งง่ายต่อการจัดการแต่ต้องมีการสำรองอุปกรณ์หากเกิดความผิดพลาด แต่ในการออกแบบระบบใหม่นี้ ควรใช้ Core Switching ซึ่งเป็นแบบ Dual CPU ซึ่งสามารถสลับการทำงานได้อย่างง่ายและสะดวก ส่วนกระจายในระบบเดิมของคณะวิชาและหน่วยงานบางแห่งเป็นระบบ

ที่ไม่สามารถสลับการใช้งานได้ ดังนั้น switching ของคณะและหน่วยงานบางแห่งจะไม่สามารถรองรับการทำงานให้จะต้องมีการปรับปรุงระบบใหม่ โดยการเปลี่ยน Switch ใหม่ที่มีคุณสมบัติแบบ Dual CPU แต่ระบบโครงสร้างการเชื่อมต่อของเครือข่ายยังคงเดิมทุกประการ จึงเป็นการลงทุนเพิ่มบางส่วนและใช้ระบบโครงสร้างพื้นฐานเดิมที่ได้ติดตั้งมาอย่างดีได้อย่างเหมาะสม การปรับปรุงระบบเพื่อแก้ปัญหาส่วนกระจายนี้ ต้องกำหนดการเชื่อมต่อดังนี้

2.1 อุปกรณ์ switching ของทุกคณะต้องเป็นอุปกรณ์ที่มีมาตราฐานเดียวกับ Core Switch หลักของมหาวิทยาลัยซึ่งอยู่ภายใต้การดูแลของมหาวิทยาลัย

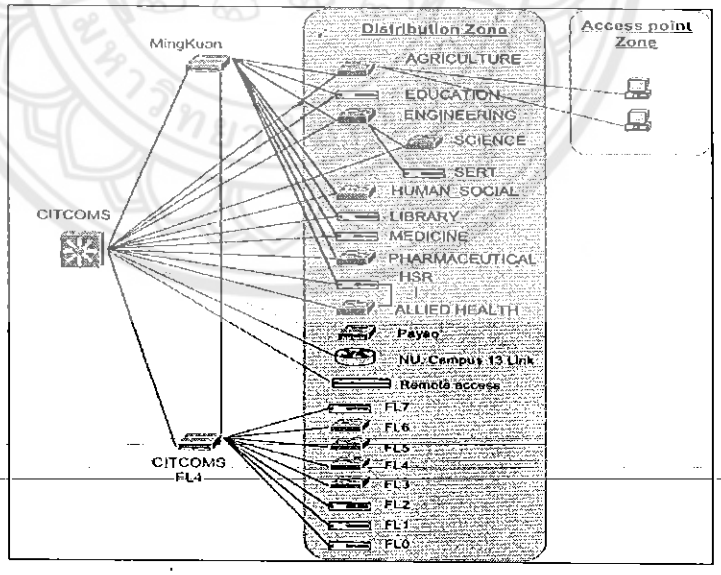
2.2 การเชื่อมต่อกับทุกคณะและหน่วยงาน กำหนดให้เป็น Gigatbit Ethernet

2.3 สื่อสัญญาณที่เชื่อมไปยังคณะและหน่วยงานกำหนดให้เป็นสายสัญญาณใยแก้วนำแสง (Fiber optic)

2.4 ทุกคณะและหน่วยงานต้องมีเส้นทางการเชื่อมต่อสำรองเป็นแบบ (Fast Ethernet) หรือ ATM OC-3

2.5 การกำหนด VLAN และการเชื่อมต่อออกภายนอกมหาวิทยาลัยทั้งหมด มหาวิทยาลัยจะเป็นผู้จัดสรรให้

จากความต้องการดังกล่าว ผู้วิจัยจึงได้นำมาออกแบบส่วนกระจาย ดังรูป

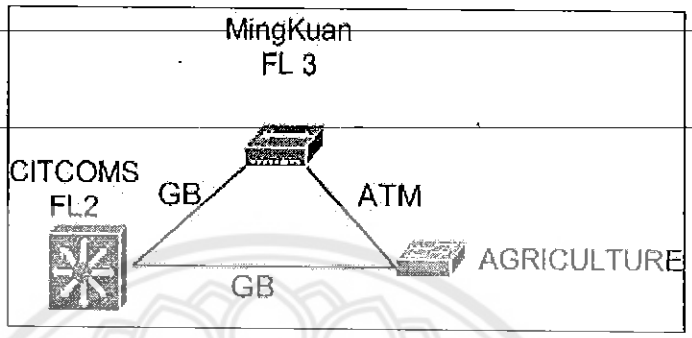


รูปที่ 4-32 การกำหนดโครงสร้างระบบเครือข่ายคอมพิวเตอร์เบื้องต้น

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

โดยมีรายละเอียดการเชื่อมต่ออุปกรณ์และระบบของคณะวิชา และหน่วยงานต่างๆดังนี้

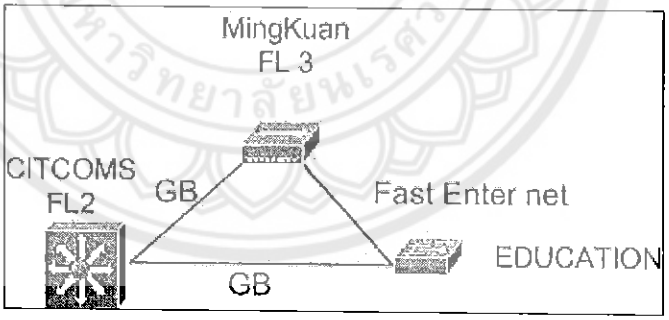
1.คณะเกษตรศาสตร์ มีการเชื่อมต่อหลักกับศูนย์กลางเครือข่ายเป็น GB Ethernet และการเชื่อมต่อสำรองคือ ATM OC-3 ไปที่อาคารมิ่งขวัญ



รูปที่ 4-33 การออกแบบการเชื่อมต่อของคณะเกษตรศาสตร์

(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

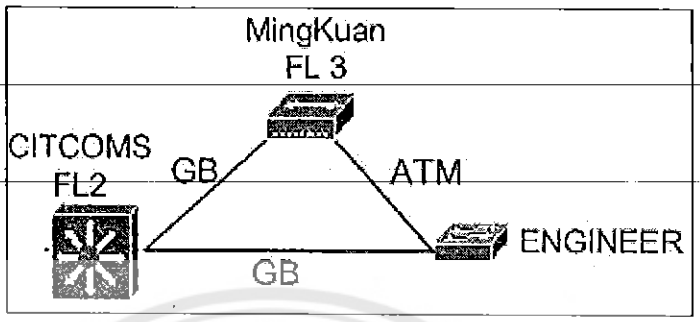
2. คณะศึกษาศาสตร์ มีการเชื่อมต่อหลักกับศูนย์กลางเครือข่ายเป็น GB Ethernet และการเชื่อมต่อสำรองคือ ATM OC-3 ไปที่อาคารมิ่งขวัญ



รูปที่ 4-34 การออกแบบการเชื่อมต่อของคณะศึกษาศาสตร์

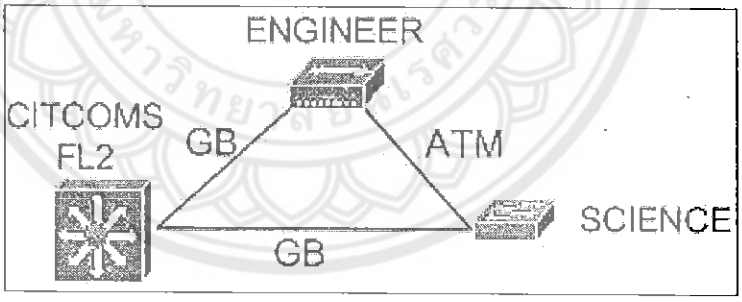
(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

3.คณะวิศวกรรมศาสตร์ มีการเชื่อมต่อหลักกับศูนย์กลางเครือข่ายเป็น GB Ethernet และการเชื่อมต่อสำรองคือ ATM OC-3 ไปที่อาคารมิ่งขวัญ



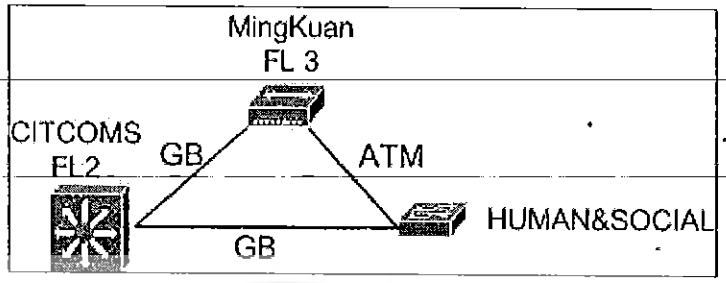
รูปที่ 4-35 การออกแบบการเชื่อมต่อของคณะวิศวกรรมศาสตร์
(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

4.คณะวิทยาศาสตร์ มีการเชื่อมต่อหลักกับศูนย์กลางเครือข่ายเป็น GB Ethernet และการเชื่อมต่อสำรองคือ ATM OC-3 ไปที่คณะวิศวกรรมศาสตร์



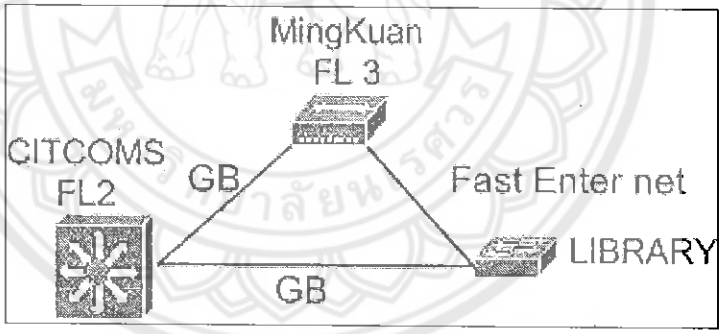
รูปที่ 4-36 การออกแบบการเชื่อมต่อของคณะวิทยาศาสตร์
(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

5.คณะมนุษยศาสตร์และคณะสังคมศาสตร์ มีการเชื่อมต่อหลักกับศูนย์กลางเครือข่ายเป็น GB Ethernet และการเชื่อมต่อสำรองคือ ATM OC-3 ไปที่อาคารมิ่งขวัญ



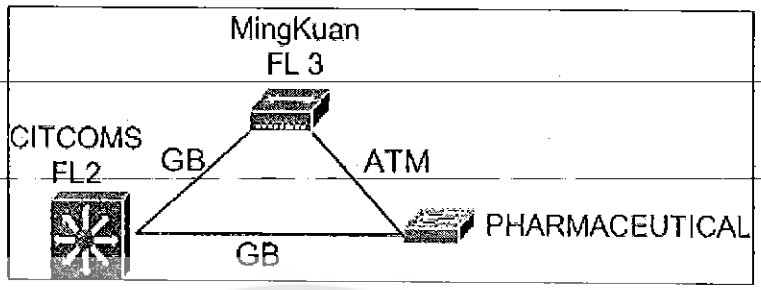
รูปที่ 4-37 การออกแบบการเชื่อมต่อของคณะมนุษยศาสตร์และคณะสังคมศาสตร์
(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

6.สำนักหอสมุด มีการเชื่อมต่อหลักกับศูนย์กลางเครือข่ายเป็น GB Ethernet และการเชื่อมต่อสำรองคือ ATM OC-3 ไปที่อาคารมิ่งขวัญ



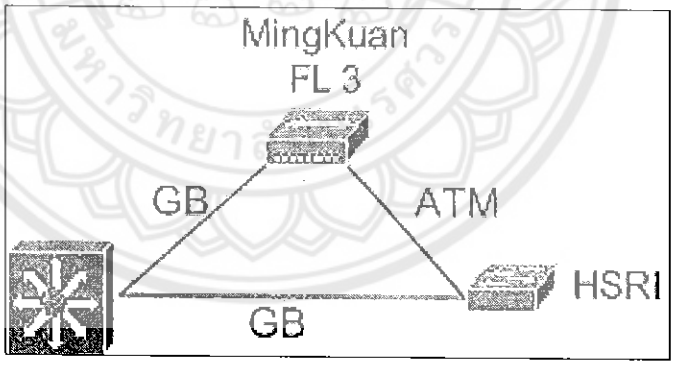
รูปที่ 4-38 การออกแบบการเชื่อมต่อของสำนักหอสมุด
(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

7.คณะเภสัชศาสตร์ มีการเชื่อมต่อหลักกับศูนย์กลางเครือข่ายเป็น GB Ethernet และการเชื่อมต่อสำรองคือ ATM OC-3 ไปที่อาคารมิ่งขวัญ



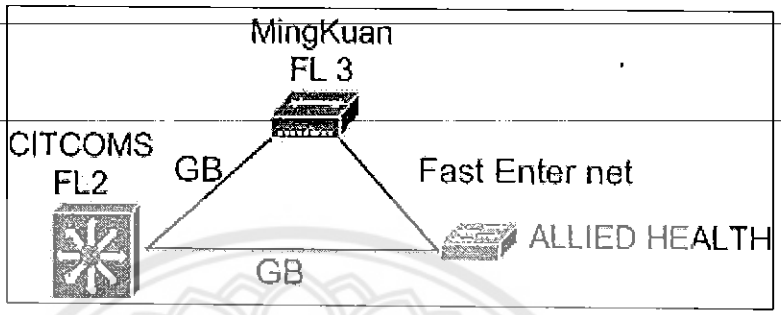
รูปที่ 4-39 การออกแบบการเชื่อมต่อของคณะเภสัชศาสตร์
(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

8.สถาบันวิจัยทางวิทยาศาสตร์สุขภาพ มีการเชื่อมต่อหลักกับศูนย์กลางเครือข่ายเป็น GB Ethernet และการเชื่อมต่อสำรองคือ ATM OC-3 ไปที่อาคารมิ่งขวัญ



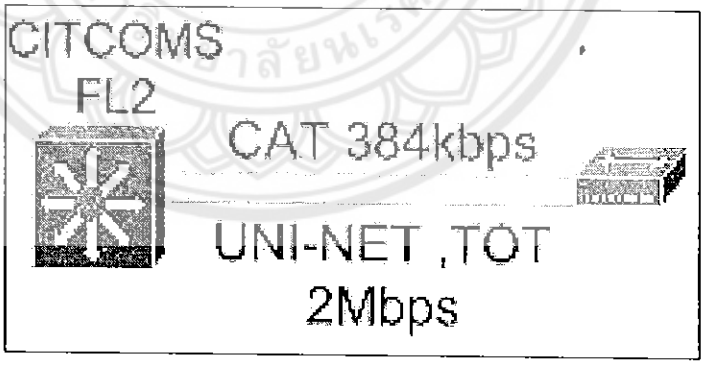
รูปที่ 4-40 การออกแบบการเชื่อมต่อของสถาบันวิจัยทางวิทยาศาสตร์สุขภาพ
(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

9.กลุ่มอาคารวิทยาศาสตร์สุขภาพมีการเชื่อมต่อหลักหลังจากคณะสหเวชศาสตร์เข้ากับศูนย์กลางเครือข่ายเป็น GB Ethernet และการเชื่อมต่อสำรองคือ Fast Ethernet ของสถาบันวิจัยทางวิทยาศาสตร์สุขภาพที่เชื่อมต่อมาจากอาคารมิ่งขวัญ และอาคาร CITCOMS



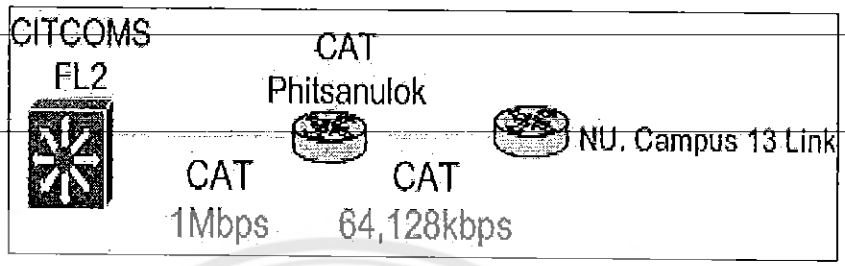
รูปที่ 4-41 การออกแบบการเชื่อมต่อของกลุ่มอาคารวิทยาศาสตร์สุขภาพ
(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

10.วิทยาเขตสารสนเทศพะเยา มีการเชื่อมต่อหลักกับศูนย์กลางเครือข่ายเป็น Lead line 2 Mbps และการเชื่อมต่อคือ VDO Conference ขนาด 384 kbps



รูปที่ 4-42 การออกแบบการเชื่อมต่อของวิทยาเขตสารสนเทศพะเยา
(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

11. ศูนย์วิทยบริการและสถาบันสมทบ 15 แห่ง มีการเชื่อมต่อหลักกับศูนย์กลางเครือข่ายเป็น Lead line 1 Mbps ไปยังการสื่อสารแห่งประเทศไทยจังหวัดพิษณุโลกแล้วมีการกระจายไปยังศูนย์วิทยบริการและสถาบันสมทบ 15 แห่ง ด้วย Bandwidth 64 และ 128 kbps

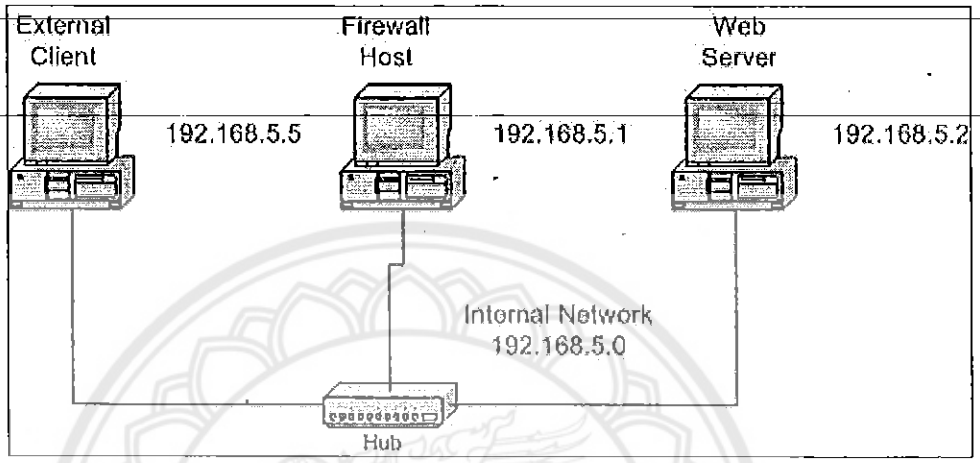


รูปที่ 4-43 การออกแบบการเชื่อมต่อของศูนย์วิทยบริการและสถาบันสมทบ
(ที่มา: ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, มหาวิทยาลัยนเรศวร)

4.6 คุณลักษณะของผลิตภัณฑ์การทำงานไฟร์วอลล์ที่นำมาทดสอบและการคอนฟิกกูเรชัน

4.6.1 เน็ตเวิร์กโทโพโลยี (Network Topology)

4.6.1.1 เน็ตเวิร์กโทโพโลยีสำหรับทดสอบเอนเตอร์ไพรส์ไฟร์วอลล์



รูปที่ 4-44 เน็ตเวิร์กโทโพโลยี สำหรับทดสอบเอนเตอร์ไพรส์ไฟร์วอลล์

สำหรับเน็ตเวิร์กโทโพโลยีที่วางขึ้นมาเพื่อทำการทดสอบนั้นประกอบด้วยเครื่อง 3 เครื่อง คือ

1. ไคลเอ็นต์ภายนอก (External Client)

เป็นไคลเอ็นต์ที่ไม่ได้อยู่ในเครือข่ายภายใน (internal network) โดยจุดประสงค์หลักของเครื่องนี้คือใช้เพื่อทำการโจมตีไฟร์วอลล์โฮสต์ และโฮสต์หลังไฟร์วอลล์ โดยมีสเป็กของเครื่องเป็นดังนี้

- ซีพียู: Intel(R) Pentium(R) 4 CPU 1.80 GHz
- หน่วยความจำ :256 เมกกะไบต์
- การ์ดแลนความเร็ว :10/100 เมกกะบิตต่อวินาที (Mbps) 1 ใบ
- ระบบปฏิบัติการ :RedHat 9.0 และ Window XP Professional service pack1

2. ไฟร์วอลล์โฮสต์ (Firewall Host)

เป็นเครื่องเซิร์ฟเวอร์ที่เป็นไฟร์วอลล์โฮสต์โดยจุดประสงค์หลักของเครื่องนี้คือใช้เพื่อเป็น ไฟร์วอลล์ในการป้องกันเครือข่ายภายในโดยมีสเป็กของเครื่องเป็นดังนี้

- ซีพียู: Intel(R) Celeron(TM)
- หน่วยความจำ :384 เมกกะไบต์
- การ์ดแลนความเร็ว :10/100 เมกกะบิตต่อวินาที 1 ใบ
- ระบบปฏิบัติการ :Window 2000 Server

ทั้งนี้เครื่องไฟร์วอลล์โฮสต์ได้ถูกได้ใช้สวิทช์เพื่อเชื่อมต่อระหว่าง 2 เครือข่ายด้วยกัน

3. ไคลเอ็นต์ภายใน (Internal Client)

เป็นไคลเอ็นต์ที่อยู่ในเครือข่ายภายใน โดยจุดประสงค์หลักของเครื่องนี้คือ ใช้เป็นเว็บเซิร์ฟเวอร์(Web Server) เพื่อให้บริการโดยมีสเป็กของเครื่องเป็นดังนี้

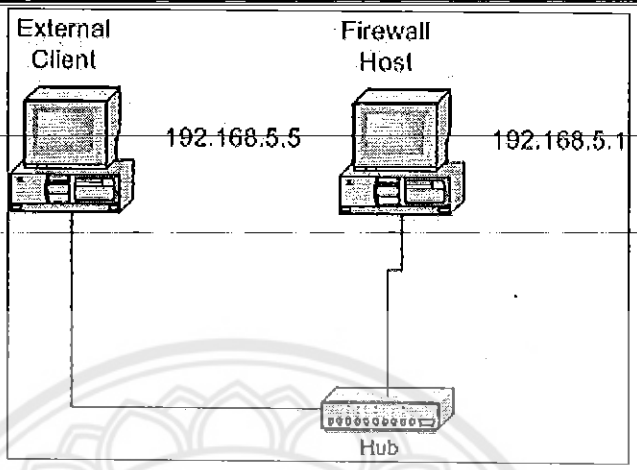
- ซีพียู :Pentium III 800 MHz
- หน่วยความจำ :640 เมกกะไบต์
- การ์ดแลนความเร็ว :10/100 เมกกะบิตต่อวินาที 1 ใบ
- ระบบปฏิบัติการ :Window 2000 Server

วิธีการเชื่อมต่อ

ใช้ Switch 5-Port 10/100 Mbps เพื่อทำการเชื่อมต่อดังนี้

1. สายที่ 1 ต่อระหว่างไคลเอ็นต์ภายนอกกับไฟร์วอลล์โฮสต์ สำหรับเหตุที่เชื่อมต่อกันด้วยคือเชื่อมต่อกันด้วยสวิทซ์ความเร็ว100MHzก็ได้โดยระบุไอพีแอดเดรสของการ์ดแลนดังนี้
   - ไคล์เอ็นต์ภายนอก:192.168.5.5
   - ไฟร์วอลล์โฮสต์: 192.168.5.1
2. สายที่ 2 ต่อระหว่างไฟร์วอลล์โฮสต์กับไคลเอ็นต์ภายใน โดยระบุไอพีแอดเดรสของการ์ดแลนดังนี้
   - ไฟร์วอลล์โฮสต์: 198.168.5.1
   - ไคลเอ็นต์ภายใน :198.168.5.2

4.6.1.2 เน็ตเวิร์กโทโพโลยีสำหรับทดสอบเพอร์ซันนอลไฟร์วอลล์



รูปที่ 4-45 เน็ตเวิร์กโทโพโลยีสำหรับเพอร์ซันนอลไฟร์วอลล์

สำหรับเน็ตเวิร์กโทโพโลยีที่วางขึ้นมาเพื่อทำการทดสอบนั้น ประกอบด้วยเครื่อง 2 เครื่อง คือ

1. ไคลเอ็นต์ภายนอก (External Client)

เป็นไคลเอ็นต์ที่ไม่ได้อยู่ในเครือข่ายภายใน (internal network) โดยจุดประสงค์หลักของเครื่องนี้คือใช้เพื่อทำการโจมตีไฟร์วอลล์โฮสต์ โดยมีสเป็กของเครื่องเป็นดังนี้

- ซีพียู: Intel(R) Pentium(R) 4 CPU 1.80 GHz
- หน่วยความจำ :256 เมกกะไบต์
- การ์ดแลนความเร็ว :10/100 เมกกะบิตต่อวินาที (Mbps) 1 ใบ
- ระบบปฏิบัติการ :Window XP Professional

2. เพอร์ซันนอลไฟร์วอลล์ (Personal Firewall)

เป็นเครื่องเซิร์ฟเวอร์ที่เป็นไฟร์วอลล์โฮสต์โดยจุดประสงค์หลักของเครื่องนี้คือใช้เพื่อเป็นไฟร์วอลล์ในการป้องกันเครื่องคอมพิวเตอร์ส่วนบุคคล (personnel computer) โดยมีสเป็กของเครื่องเป็นดังนี้

- ซีพียู: Intel(R) Celeron(TM)
- หน่วยความจำ :384 เมกกะไบต์
- การ์ดแลนความเร็ว :10/100 เมกกะบิตต่อวินาที 1 ใบ

- ระบบปฏิบัติการ :Window 2000 Server

วิธีการเชื่อมต่อ

ต่อการ์ดแลนของทั้ง 2 เครื่องเข้ากับเน็ตเวิร์ก 192.168.5.0 โดยระบุไอพีแอดเดรสของการ์ดแลนดังนี้

- ไคล์เอ็นต์ภายนอก :192.168.5.5
- ไฟร์วอลล์โฮสต์: 192.168.5.1

4.7 ผลิตภัณฑ์ไฟร์วอลล์ที่นำมาศึกษา

ไฟร์วอลล์ที่เรานำมาทดสอบมีทั้งประเภทแอพพลิเคชันพรอกซี (Application Proxy) และประเภทสเตตฟูลอินสเป็กชัน (Stateful Inspection) และมีทั้งเอนเตอร์ไพรส์ไฟร์วอลล์ (Enterprise Firewall) และเพอร์ซันนอลไฟร์วอลล์ (Personal Firewall)

4.7.1 Zone Alarm Pro V.3.0

4.7.1.1 คุณลักษณะของ Zone Alarm Pro

- ความต้องการของระบบ (System Requirement)
  - อินเทล พีซี หรือเทียบเท่า
  - ระบบโปรเซสเซอร์ 486 ขึ้นไป
  - ระบบปฏิบัติการวินโดว์ 98/ME/NT/2000/XP
  - RAM 8 เมกะไบต์ (MB)
  - เนื้อที่ว่างฮาร์ดดิส 10 เมกะไบต์
- เป็นผลิตภัณฑ์เชิงการค้า (Commercial product) ซึ่งที่เรามาใช้นี้ เป็นการดาวน์โหลดมาทดลองใช้เท่านั้น
- Zone Alarm Pro มี 4 ส่วนหลักๆที่ใช้ต่อสู้กับการคุกคามบนอินเตอร์เน็ต ดังนี้

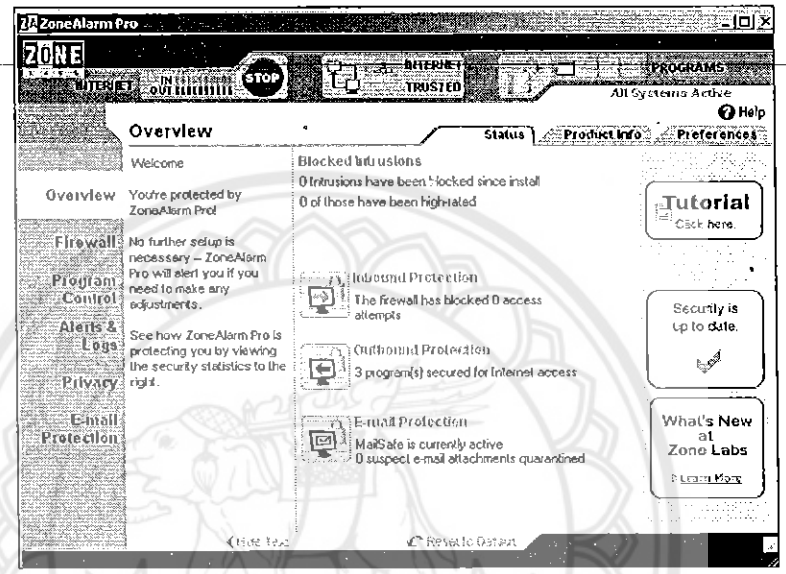
  - ไฟร์วอลล์

  - ส่วนควบคุมโปรแกรม จะป้องกันโปรแกรมจำพวกโทรจันไม่ให้เข้ามาฝังตัวและติดตั้งอยู่ในเครื่องคอมพิวเตอร์ได้

  - การรักษาความเป็นส่วนตัว คือจะป้องกันเครื่องจากความวุ่นวายของ cookieและการป๊อปอัพ (Pop up) โฆษณาต่างๆ และยังป้องกันเครื่องจากสคริปต์ และวัตถุฝัง ตัวต่างๆ จากเว็บเพจ

- การป้องกันอีเมล์ ปกป้องเครื่องจากหนอนอินเตอร์เน็ต และไวรัส ทั้งที่รู้จักแล้ว และยังไม่รู้จักซึ่งจะมากับอีเมล์ได้

- ใช้งานง่าย พร้อมทั้งมี Wizard ช่วยในการคอนฟิกกูเรชัน อีกทั้งในการปรับแต่งค่าต่างๆ ก็ทำได้ง่ายดาย และเข้าใจง่าย

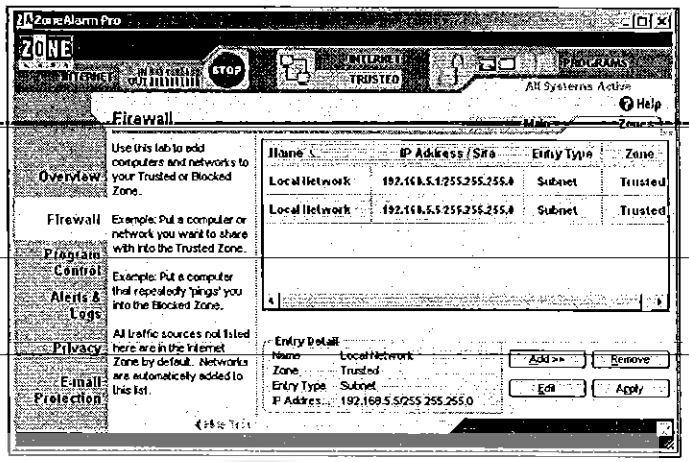


รูปที่ 4-46 โปรแกรมZone Alarm Pro

4.7.1.2 การคอนฟิก Zone Alarm Pro V3.1.0

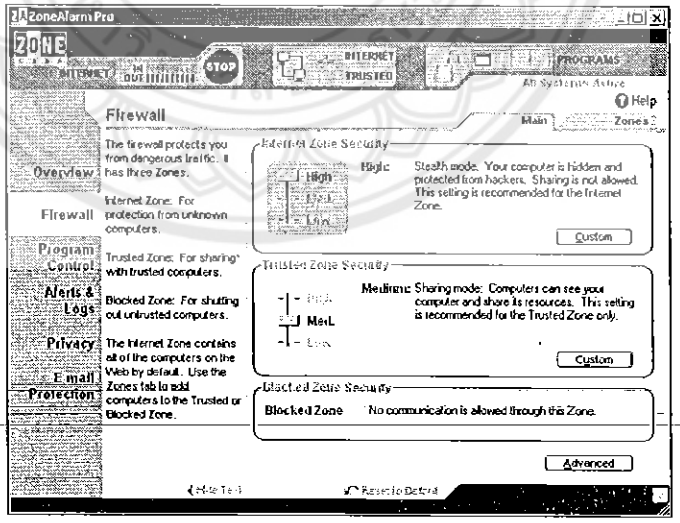
ในการปรับแต่งค่าต่างๆ ในโปรแกรม จะอธิบายตามจุดต่างๆ ที่เราให้ความสนใจ นั่นคือทางด้านความปลอดภัย ดังนี้

- เซ็ตค่าเน็ตเวิร์กของเราตามเน็ตเวิร์กโทโพโลยี โดยให้เน็ตเวิร์กภายนอกคือเน็ตเวิร์ก และเน็ตเวิร์กภายในคือเน็ตเวิร์กที่เราสร้างขึ้นใหม่ตามโทโพโลยี พร้อมทั้งเชื่อถือเน็ตเวิร์กภายในไว้ด้วย

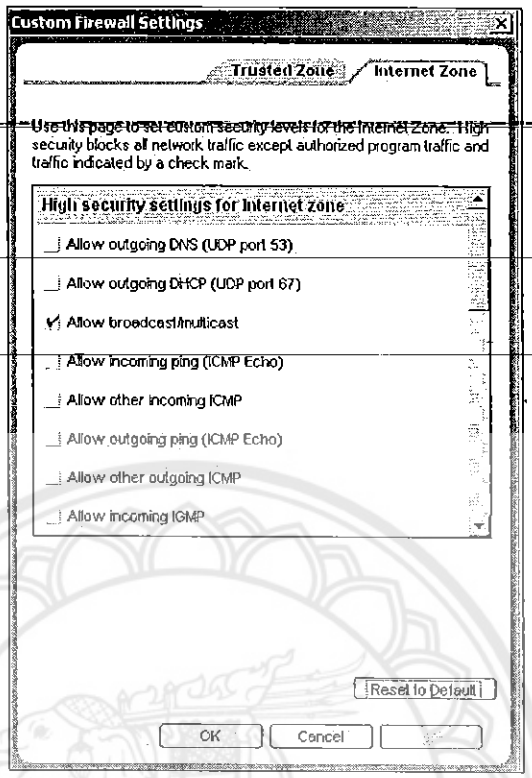


รูปที่ 4-47 ค่าเน็ตเวิร์กโซนที่ได้ติดตั้งเข้าไป

- ทำการตั้งค่าการรักษาความปลอดภัยของไฟร์วอลล์ สำหรับความปลอดภัยจากอินเตอร์เน็ต เน็ตเวิร์ก เลือกแบบกลาง (Medium) และยังเข้าไปปรับแต่งเพิ่มเติมได้อีก โดยการกดปุ่ม Custom เพื่อเลือกตั้งค่าเพิ่มเติมเอง แล้วเลือกเช็คดังรูปที่ 4-47 เพื่อบล็อกพอร์ตเกี่ยวกับ NetBIOS ซึ่งเป็นจุดอ่อนที่เป็นเป้าหมายของผู้บุกรุกในการโจมตีด้วย DoS ส่วนมากส่วนเช็คที่สองนั้นเป็นการบล็อกการ Ping เข้ามากจากภายนอก



รูปที่ 4-48 การตั้งค่าไฟร์วอลล์



รูปที่ 4-49 การตั้งค่าไฟร์วอลล์เลือกเอง

4.7.2 Tiny Personal Firewall

4.7.2.1 คุณลักษณะของTiny Personal Firewall

เป็นเทคโนโลยีด้านความปลอดภัยแบบส่วนตัวที่ใช้งานง่าย ซึ่งป้องกันพีซีจากผู้บุกรุกได้อย่างเต็มรูปแบบ ใช้ได้ดีทั้งเครื่องที่ต่ออยู่ในระบบเน็ตเวิร์กขององค์กรและเครื่องแสตนอโลน (Stand Alone)ซึ่งติดต่อกับอินเตอร์เน็ตด้วยการใช้บริการจากISP ต่างๆ Tiny Personal Firewall มีคุณสมบัติที่สำคัญดังนี้

- ความต้องการของระบบ

  - 586 Pentium Class
  - RAM 16 เมกะไบต์
  - เนื้อที่ว่างบนฮาร์ดดิสต์ 1 เมกะไบต์
  - ระบบปฏิบัติการวินโดว์ 9x/2000/ME/NT/XP

- **การกรองแอพพลิเคชัน (Application Filter)**

เพื่อที่จะป้องกันม้าโทรจันและแอพพลิเคชันที่พิสูจน์ความถูกต้องไม่ได้ Tiny Personal Firewall จึงมีการกรองแอพพลิเคชัน ซึ่งจะมีwizard ที่จะตรวจจับเมื่อมีแอพพลิเคชันพยายาม bind พอร์ตเพื่อการติดต่อสื่อสาร มันจะสร้างกฎการกรอง ที่ขึ้นอยู่กับอินพุตของผู้ใช้ด้วย คือผู้ใช้สามารถอนุญาตแอพพลิเคชันนั้นจากกฎการกรองได้ และจะมีการเก็บดาต้าเบสของแอพพลิเคชันทั่วๆไปว่าใช้พอร์ตไหนเป็นปกติไว้ด้วย

- **แอดเดรสที่เชื่อถือได้ (Trusted Address)**

ผู้ใช้สามารถกำหนดกฎการกรองได้เอง โดยอาจกำหนดแอดเดรสที่เชื่อถือได้เป็น IPเดียว หรือเป็นช่วงของ IP หรือจะเชื่อถือทั้งเน็ตเวิร์กใดๆได้เลย

- การบริหารจัดการทางไกล

สามารถทำการคอนฟิกนโยบายความปลอดภัยต่างๆได้จากระยะไกล

4.7.2.2 การคอนฟิก Tiny Personal Firewall

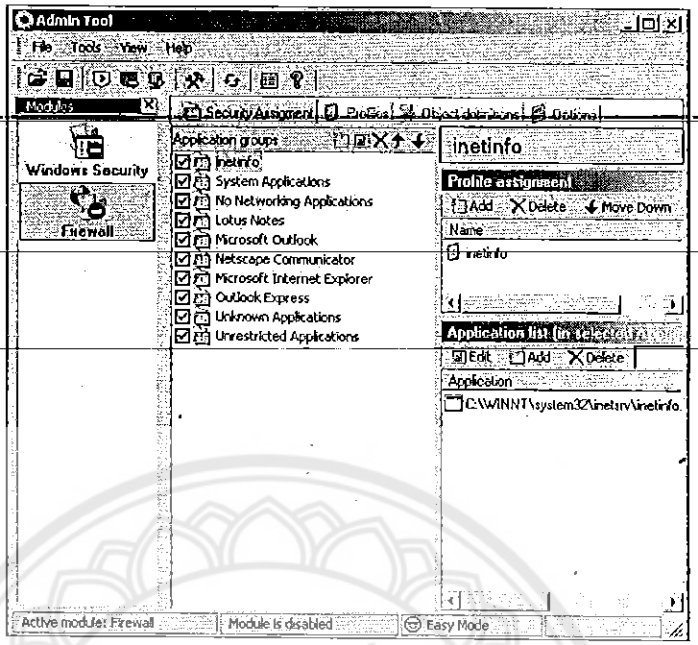
ในการปรับแต่งค่าต่างๆ ในโปรแกรม จะอธิบายตามจุดต่างๆ ที่เราให้ความสนใจ นั่นคือทางด้านความปลอดภัย ดังนี้

- ทำการตั้งค่าการรักษาความปลอดภัยของไฟร์วอลล์ โดยสามารถเลือกโหมดการทำงานได้ 3 โหมด

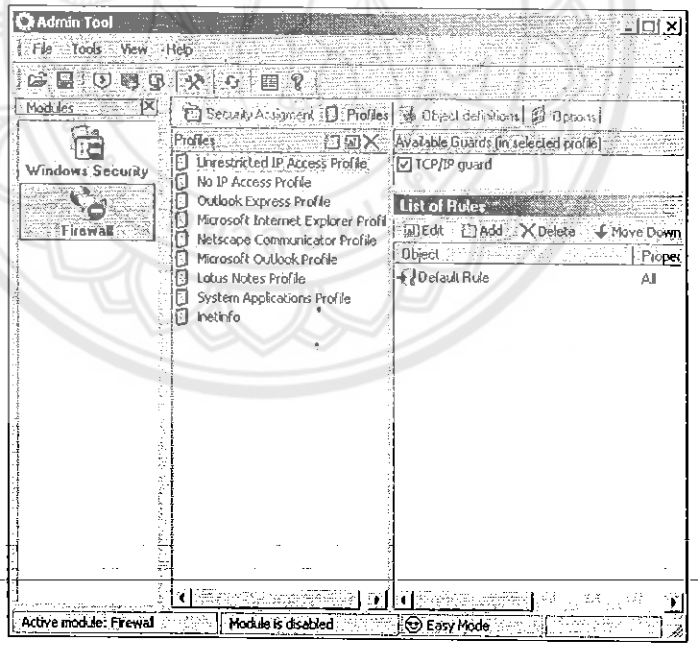
- Don't Bother Me คือถ้าพฤติกรรมที่เข้ามาไม่ตรงกับกฎที่ระบุไว้ Tiny Personal Firewall ก็จะไม่ขึ้นหน้าจอให้สร้างกฎใหม่

- Ask Me First คือถ้าพฤติกรรมที่เข้ามาไม่ตรงกับกฎที่ระบุไว้ Tiny Personal Firewall ก็จะขึ้นหน้าจอให้ผู้ใช้งานตัดสินใจ

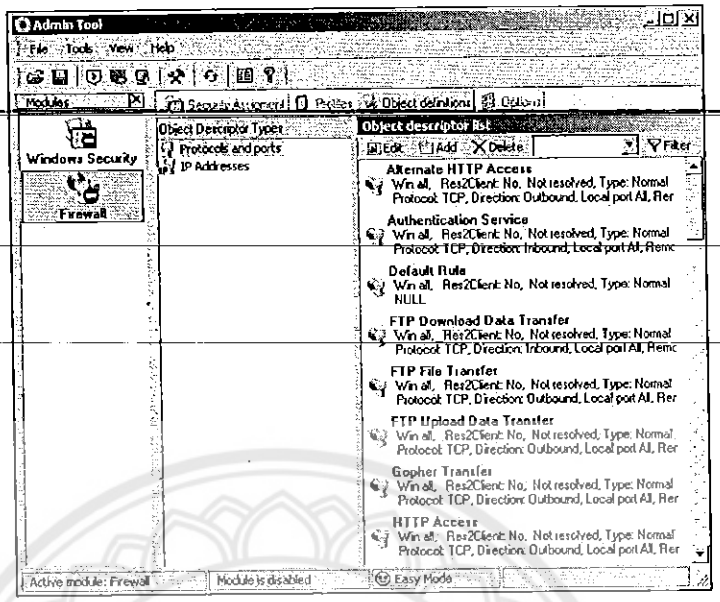
- Cut Me off คืองดการใช้งานเน็ตเวิร์ก จะใช้ออปชั่นนี้ก็ต่อเมื่อไม่ต้องการใช้งานเน็ตเวิร์ก เพื่อเพิ่มความปลอดภัยให้มากที่สุด



รูปที่ 4-50 การเลือกโหมดการทำงานของ Tiny Personal Firewall



รูปที่ 4-51 แสดงหน้าจอปรับตั้งค่าไฟร์วอลล์



รูปที่ 4-52 การเพิ่มนโยบายให้กับไฟร์วอลล์

4.7.3 WatchGuard Firewall

WatchGuard Firewall มีส่วนประกอบหลักๆ 4 ส่วนดังนี้

- **LiveSecurity Service**

  เป็นการรักษาได้ง่ายความปลอดภัยของเครือข่ายของการจัดการ การบริการเชื่อมต่อโดยอัตโนมัติกับ WatchGuard

- **Control Center**

  -Policy Manager ใช้ให้การออกแบบ, แก้ไข, และจัดการส่วนอิเล็กโทรนิคของนโยบาย ความปลอดภัยเครือข่าย

  -Firebox Monitors เป็นการผสม WatchGuard กับ Monitoring ของเครื่องมือที่ติดตามเข้าไปในส่วนติดต่อผู้ใช้งานเดี่ยว

  -LogViewer – แสดงสถิติของข้อมูลล็อก

- **Security Suite**

  -User authentication เป็นความน่าเชื่อถือผู้ใช้

  -Network address translation การแปลตำแหน่งที่อยู่เครือข่าย

  -Remote user virtual private networking ผู้ใช้ระยะไกลการทำเครือข่าย

  -Branch office virtual private networking การทำเครือข่ายส่วนตัว

-Selective Web-site blocking การบล็อกเว็บไซด์

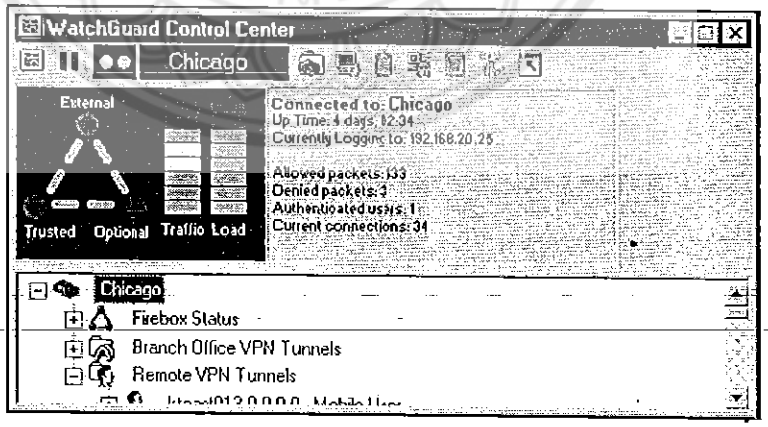
- **Security appliance**

4.7.3.1 คุณลักษณะของ WatchGuard Firewall

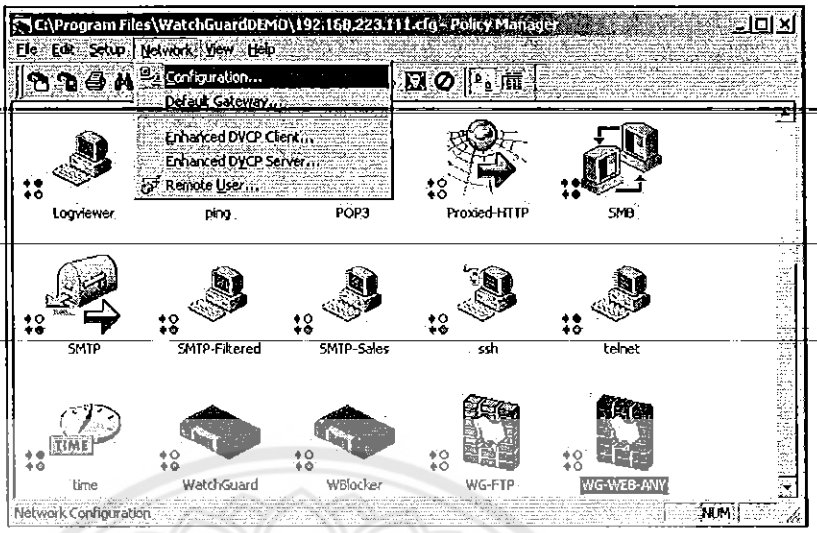
- เป็นไฟร์วอลล์เต็มรูปแบบ
- ประกอบด้วยเทคโนโลยีทางความปลอดภัยมากมายทั้ง NAT, VPNs, เพอร์ซันนอลไฟร์วอลล์
- สามารถจัดการจากทางไกลได้ (Remote Administration)
- มี security policy ที่จัดการง่าย
- มีการจัดเก็บลงล็อกไฟล์
- มีการแจ้งเตือน

4.7.3.2 หน้าที่หลักที่สำคัญของ WatchGuard

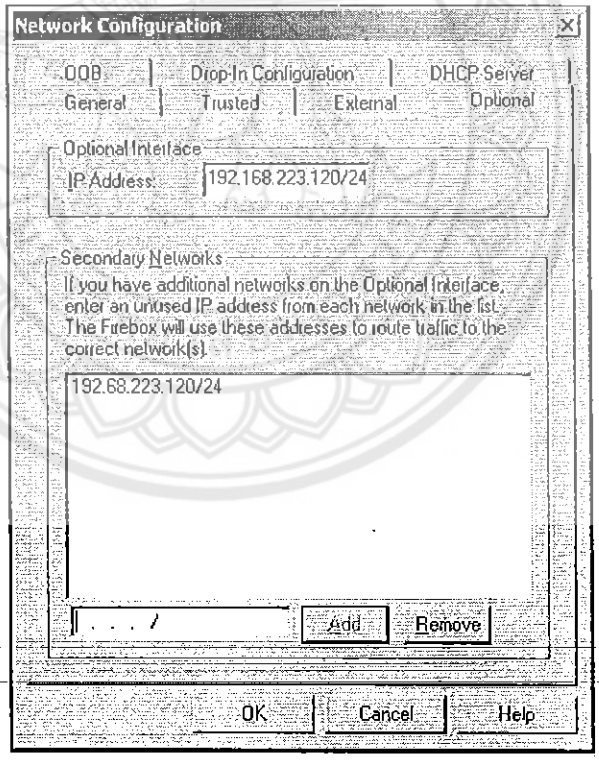
- WatchGuard มีความสามารถป้องกันทรัพยากรเครือข่ายทั้งหมด
- สามารถป้องกันการต่อต้านการโจมตีและการเข้าถึงที่ไม่ได้รับอนุญาติ
- สามารถจัดการกับระบบของยูสเซอร์ได้
- สามารถสร้างการทำ Private IP เชื่อมต่อและใช้งานอินเทอร์เน็ตได้ (NAT)
- การจำลองเครือข่ายภายในบนเครือภายนอกอย่างเช่นอินเตอร์เน็ต (Virtual Private Network)



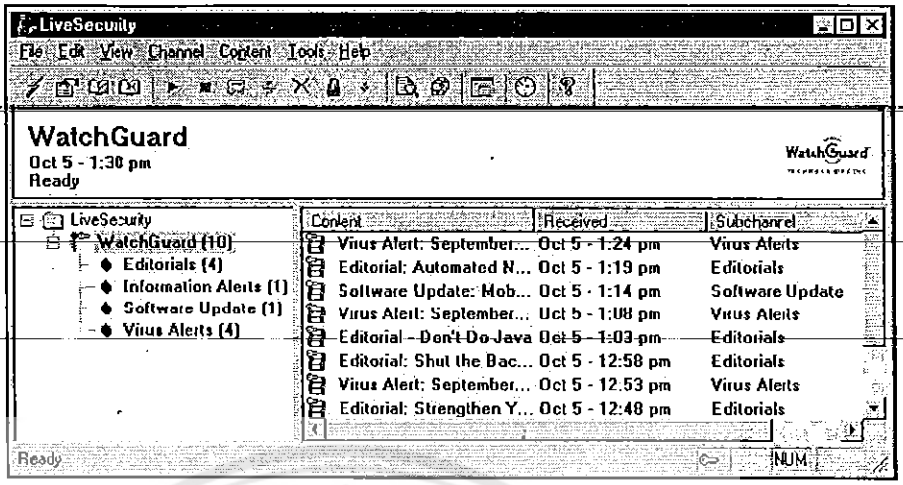
รูปที่ 4-53 WatchGuard Control Center (Front Panel, Firebox and Status)



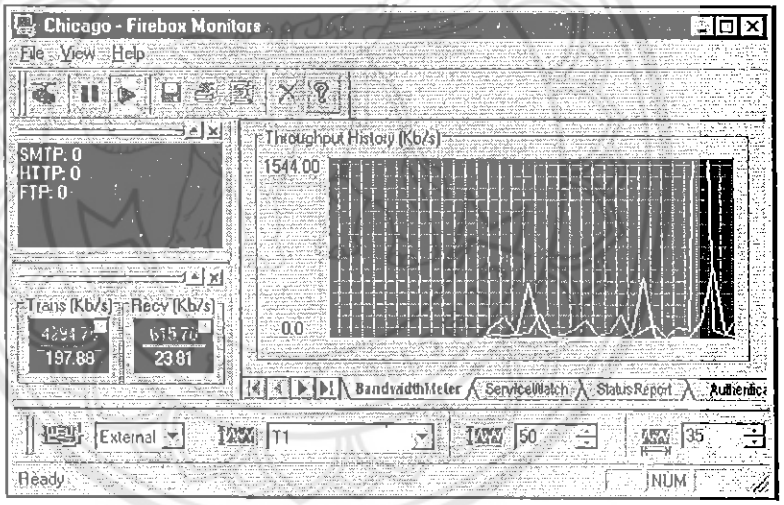
รูปที่ 4-54 การคอนฟิกกูเรชันเน็ตเวิร์กให้กับไฟร์วอลล์



รูปที่ 4-55 การคอนฟิกกูเรชันเน็ตเวิร์ก ออฟชัน อินเทอร์เฟส



รูปที่ 4-56 WatchGuard Control Center



รูปที่ 4-57 Monitionsของ WatchGuard

4.7.3.3 ความต้องการของระบบ (Window Platform)

- ระบบปฏิบัติการ Microsoft Windows NT 4.0 (SP3 & SP4),Window 2000 Server
- ฮาร์ดแวร์แพลทฟอร์ม WatchGuard VPN-1 Appliances,ODS SecureCom 8000 family Alcatel (Xylan) switches,Nortel ARN, ASN, BN and System 5000 routers,Nortel Contivity switches
- เนื้อที่ว่างบนฮาร์ดดิสต์ 40 เมกะไบต์
- RAM 64 เมกะไบต์

4.7.3.4 คุณลักษณะของ **WatchGuard Firewall**

- ให้การบริหารระบบความปลอดภัยองค์กร เช่น มีการเลือกอนุญาติการเข้าสู่เครือข่ายทั้งจากการเข้าถึงทางไกล และจากผู้ใช้ภายในองค์กร มีการกำหนดสิทธิด้วยขั้นตอนทางเทคนิคชั้นสูง เพื่อปกป้องข้อมูลสำคัญขององค์กร ให้ความมั่นใจ และมั่นคงในการสื่อสาร หรือส่งผ่านข้อมูลบนเครือข่ายสาธารณะดังเช่นบนอินเตอร์เน็ต ทำหน้าที่เป็น gateway เพื่อตรวจสอบความผิดปกติ หรือปัญหาต่างๆ ที่จะเกิดขึ้นกับข้อมูลบนเครือข่าย เช่น ไวรัส หรือแฮกเกอร์ และป้องกันการทำลายระบบ เป็นต้น
- มีการควบคุมการเข้าสู่เครือข่าย ซึ่งจะทำให้ทราบว่ามีข้อมูลอะไรส่งเข้า-ออกบนเครือข่าย พร้อมกำหนดนโยบายด้านความปลอดภัย กระจายการเข้าถึงเครือข่าย ป้องกันการทำลายระบบ และมีฟังก์ชั่นการ log-in และสัญญาณเตือนที่ก้าวล้ำ
- มีการกำหนดสิทธิในการเข้าถึงเครือข่ายด้วยกัน 3 ประเภท คือ User Authentication, Client Authentication และ Transparent Session Authentication
- มีการรักษาความปลอดภัยข้อมูลที่มีประสิทธิภาพ เช่น การตรวจหาไวรัส, การตรวจสอบ URL, Java and ActiveX, Stripping Mail (SMTP) Support และ FTP Support
- มีการเปลี่ยน IP บนเครือข่าย
- มี Reporting Module ที่ช่วยตรวจสอบข้อมูล และแสดงออกมาในรูปของรายงาน
- มีคุณสมบัติแบบ VPN ที่ให้การเชื่อมต่อระหว่างเครือข่ายที่มีความปลอดภัย
- มี LDAP Account Management
- มีการป้องกันการเจาะเข้าสู่ระบบ

- มี High Availability Module ที่ให้การทำงานที่ต่อเนื่องของระบบ, รับประกันการใช้งานในส่วนของ VPN ที่สำคัญจะไม่ถูกรบกวน และหยุดชะงัก, ช่วยให้การใช้งาน และการบริหารระบบเป็นไปโดยง่าย และช่วยให้มีการบำรุงรักษา gateway ได้ตลอดเวลา
- ป้องกันความปลอดภัยจากอันตรายที่อาจจะเกิดขึ้นทั้งภายในและภายนอกเครือข่าย
- ตรวจสอบสิทธิ์ของผู้ใช้เครือข่าย
- สนับสนุนแอพพิลเคชั่นกว่า 150 เครือข่าย และบริการต่าง ๆ จากภายนอก
- ปกปิดข้อมูลเพื่อป้องกันการเปลี่ยน address บนเครือข่าย
- ป้องกันความปลอดภัยจากไวรัส อันตรายจากสิ่งที่ไม่เป็นที่ต้องการอันแฝงมาจากที่อื่น

4.7.4 Linux Kernel Firewalls-IPtables

เป็นทูล Built-In ของลีนุกซ์ที่มีเคอร์เนลตั้งแต่ 2.4 เป็นต้นไปใช้ สำหรับสร้างควบคุมและตรวจสอบกฎเกณฑ์ในการกรองข้อมูลที่ ผ่านไปมาระหว่างเน็ตเวิร์กภายนอกและเน็ตเวิร์กภาย ในและยังป้องกันเน็ตเวิร์กและข้อมูลสำคัญๆ จากผู้ที่ไม่ได้รับอนุญาตที่แอบเข้ามาในระบบเน็ตเวิร์กของระบบ

4.7.4.1 คุณลักษณะของ IPtables

- Intel 386-486 ขึ้นไป ยิ่งสูงก็จะมีประสิทธิภาพทางด้านการประมวลผลมากขึ้น
- RAM ไม่ควรต่ำกว่า 8 เมกะไบต์
- ระบบบัส (BUS) แบบ ISA, ELSAหรือ VESA
- เนื่อที่ว่างบนฮาร์ดดิสต์ไม่ควรต่ำกว่า 5 เมกะไบต์

4.7.4.2 หน้าที่หลักที่สำคัญของ IPtables ที่ต้องทำ คือ

- ให้สิทธิข้อมูลที่ ได้รับอนุญาตให้เข้ามาถึงที่หมายได้และปฏิเสธข้อมูลที่ไม่ ได้รับอนุญาตให้เข้ามาในเน็ตเวิร์ก หรือเครื่องคอมพิวเตอร์ภายในเน็ตเวิร์ก
- ให้บริการในลักษณะของยามรักษาการอิเล็กทรอนิกส์ ที่คอยหยุดความพยายามของแฮกเกอร์หรือบุคคลใดก็ตามที่พยายามเจาะเข้ามายังเน็ตเวิร์กของเราจากเครื่องคอมพิวเตอร์ที่ไม่รู้จัก (Untrusted Computer) บนเน็ตเวิร์กภายนอก

4.7.4.3 สร้างไฟร์วอลล์ โดยใช้ IPtables

กำหนดกฎ

```
# ========================================================================
# ปิด ipchains
modprobe –r ipchains

# load module ต่างๆ
modprobe ip_tables
modprobe iptable_filter
modprobe iptable_nat
modprobe conntrack
modprobe conntrack_ftp

#enable forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward
# ========================================================================

# เคลียร์กฎที่มีอยู่ออกทั้งหมด
iptables -F
iptables -X
iptables -Z

# เคลียร์ที่เทเบิล nat ด้วย
iptables -t nat -F
iptables -t nat -X
iptables -t nat -Z

# policy
iptables -P INPUT DROP
```

```
iptables -P FORWARD DROP

## เครื่อง firewall สามารถออกได้อย่างอิสระ
iptables -P OUTPUT ACCEPT
# ================================================================================

# constant variables
IN_IF="eth0"
EX_IF="eth1"
IN_HOST="192.168.5.0/24"
FW_ADDR_IN="192.168.5.1"
FW_ADDR_EX="192.168.5.5"
NET_ADDR="161.246.39.0"
BROADCAST="192.168.5.255"
IN_NET_ADDR="192.168.5.0"
IN_BROADCAST="192.168.5.255"
IN_WEB_ADDR="192.168.5.2"
EX_WEB_ADDR="192.168.5.2"
IN_MAIL_ADDR="192.168.5.2"
EX_MAIL_ADDR="192.168.5.2"
CLASS_A="10.0.0.0/8"
CLASS_B="172.16.0.0/12"
CLASS_C="192.168.0.0/16"
CLASS_D_MULTICAST="224.0.0.0/4"
CLASS_E_RESERVED_NET="240.0.0.0/5"
LOOPBACK="127.0.0.0/8"
#
================================================================================
```

```
# protect chain มีไว้ตรวจสอบรูปแบบแพ็กเก็ตต่างๆ ที่เข้ามาภายใน
iptables –N PROTECT
## ป้องกันการ attack
### land attack
#### ด้วยการห้ามแพ็กเก็ตที่มี source address = destination address = firewall address
iptables -A PROTECT -s $FW_ADDR_EX -d $FW_ADDR_EX -j DROP

### smurf attack
#### ด้วยการห้ามส่งแพ็กเก็ตมาที่ net address และ broadcast address
iptables -A PROTECT -d $NET_ADDR -j DROP
iptables -A PROTECT -d $BROADCAST -j DROP
iptables -A PROTECT -d $IN_NET_ADDR -j DROP
iptables -A PROTECT -d $IN_BROADCAST -j DROP

### fragments
#### บันทึก log เก็บไว้ก่อน จึงค่อย drop
iptables -A PROTECT -f -m limit -j LOG --log-prefix "FRAGMENTS: "
iptables -A PROTECT -f -j DROP

## ป้องกันการ attack โดยอาศัย icmp
### ping flood
#### โดยการจำกัดปริมาณการ ping (icmp echo-request)
iptables -A PROTECT -p icmp --icmp-type echo-request -m limit \--limit 3/s --limit-burst 15 -j
ACCEPT
iptables -A PROTECT -p icmp --icmp-type echo-request -j DROP

### icmp timestamp attack
iptables -A PROTECT -p icmp --icmp-type timestamp-request –j DROP
```

```
## icmp logging
### เพื่อใช้ตรวจสอบว่ามี icmp packet รูปแบบใดอีกหรือเปล่าที่ต้องป้องกัน
iptables -A PROTECT -p icmp -m limit -j LOG --log-prefix "ICMP: "
### ยอมรับ icmp packet รูปแบบอื่นๆ ที่ไม่ใช่ ping
iptables -A PROTECT -p icmp -j ACCEPT

## ป้องกันการ attack โดยอาศัย udp
### diagnostic port attack
#### disable small services at "/etc/inetd/conf"
#### และ drop แพ็กเก็ตที่ใช้ small services port
#### 7-echo
#### 9-discard
#### 13-daytime
#### 19-chargen
#### 37-time
iptables -A PROTECT -p udp -m multiport --sport 7,9,13,19,37 -j DROP
iptables -A PROTECT -p udp -m multiport --dport 7,9,13,19,37 -j DROP

## udp logging
### เพื่อใช้ตรวจสอบว่ามี udp packet รูปแบบใดอีกหรือเปล่าที่ควรยอมรับ
iptables -A PROTECT -p udp -m limit -j LOG --log-prefix "UDP: "
iptables -A PROTECT -p udp -j DROP

## ป้องกันการ attack โดยอาศัย tcp
### trojans
### โดยการบันทึก log ไว้แล้ว drop ทิ้ง
#### deepthroat
iptables -A PROTECT -p tcp -m multiport --dport 41,999,2140,3150,6670,6771,60000 \
-m limit -j LOG --log-prefix "DeepThroat: "
```

```
iptables -A PROTECT -p tcp -m multiport --dport 41,999,2140,3150,6670,6771,60000 \
-j DROP
```

subseven

```
iptables -A PROTECT -p tcp -m multiport --dport 2773,6711,6712,6713,7215,27374,27573,54283 \-
m limit -j LOG --log-prefix "SubSeven: "
iptables -A PROTECT -p tcp -m multiport --dport 2773,6711,6712,6713,7215,27374,27573,54283 \-j
DROP
```

netbus

```
iptables -A PROTECT -p tcp -m multiport --dport 12345,12346,20034 \
-m limit -j LOG --log-prefix "NetBus: "
iptables -A PROTECT -p tcp -m multiport --dport 12345,12346,20034 \-j DROP
```

back orifice (bo)

```
iptables -A PROTECT -p tcp -m multiport --dport 8787,31337,54320 \-m limit -j LOG --log-prefix
"Back Orifice: "
iptables -A PROTECT -p tcp -m multiport --dport 8787,31337,54320 \-j DROP
```

diagnostic port attack

```
iptables -A PROTECT -p tcp -m multiport --sport 7,9,13,19,37 -j DROP
iptables -A PROTECT -p tcp -m multiport --dport 7,9,13,19,37 -j DROP
```

syn flood

โดยการจำกัดปริมาณ syn packet

```
iptables -A PROTECT -p tcp --syn -m limit --limit 3/s --limit-burst 15 -j ACCEPT
iptables -A PROTECT -p tcp --syn -j DROP
```

tcp logging

เพื่อใช้ตรวจสอบว่ามี tcp packet รูปแบบใดอีกหรือเปล่าที่ควรยอมรับ

```
iptables -A PROTECT -p tcp -m limit -j LOG --log-prefix "TCP: "
iptables -A PROTECT -p tcp -j DROP

## logging
iptables -A PROTECT -m limit -j LOG --log-prefix "OTHERS: "
iptables -A PROTECT -j DROP
# ================================================================

# input chain
## drop invalid and illegal packets
iptables -A INPUT -m unclean -j DROP
iptables -A INPUT -m state --state INVALID -j DROP

## allow unlimited traffic on the loopback interface.
iptables -A INPUT -i lo -j ACCEPT

## ยอมรับแพ็กเก็ตทั้งหมดจาก internal network
iptables -A INPUT -i $IN_IF -s $IN_HOST -j ACCEPT

## drop แพ็กเก็ตที่ร้องขอการเชื่อมต่อจากภายนอกทั้งหมด
## คือ ไม่อนุญาติให้ภายนอกสร้างการเชื่อมต่อได้
iptables -A INPUT -i $EX_IF -m state --state NEW -j DROP
## ป้องกันการปลอมแปลง ip (spoofing)
### เครื่องภายนอกไม่มีทางใช้ ip address เดียวกับเครื่องไฟร์วอลล์ได้
iptables -A INPUT -i $EX_IF -s $FW_ADDR_EX -j DROP

### เครื่องภายนอกไม่มีทางใช้ private ip ได้
iptables -A INPUT -i $EX_IF -s $CLASS_A -j DROP
iptables -A INPUT -i $EX_IF -s $CLASS_B -j DROP
```

```
iptables -A INPUT -i $EX_IF -s $CLASS_C -j DROP
iptables -A INPUT -i $EX_IF -s $CLASS_D_MULTICAST -j DROP
iptables -A INPUT -i $EX_IF -s $CLASS_E_RESERVED_NET -j DROP

### เครื่องภายนอกไม่มีทางใช้ loopback address ได้
iptables -A INPUT -i $EX_IF -s $LOOPBACK

## ยอมรับแพ็กเก็ตจากภายนอก
## ที่เป็นส่วนหนึ่งของการเชื่อมต่อที่สร้างโดยเครื่องไฟร์วอลล์เอง
iptables -A INPUT -i $EX_IF -m state --state ESTABLISHED -j ACCEPT

## RELATED packet jump to PROTECT
iptables -A INPUT -i $EX_IF -m state --state RELATED -j PROTECT
# ==========================================================================

# forward chain
## drop invalid and illegal packets
iptables -A FORWARD -m unclean -j DROP
iptables -A FORWARD -m state --state INVALID -j DROP

# (from external to internal network)
## ป้องกันการปลอมแปลง ip (spoofing)
### เครื่องภายนอกไม่มีทางใช้ ip address เดียวกับเครื่องไฟร์วอลล์ได้
iptables -A FORWARD -i $EX_IF -o IN_IF -s $FW_ADDR_EX -j DROP

### เครื่องภายนอกไม่มีทางใช้ private ip ได้
iptables -A FORWARD -i $EX_IF -o $IN_IF -s $CLASS_A -j DROP
iptables -A FORWARD -i $EX_IF -o $IN_IF -s $CLASS_B -j DROP
iptables -A FORWARD -i $EX_IF -o $IN_IF -s $CLASS_C -j DROP
```

```
iptables -A FORWARD -i $EX_IF -o $IN_IF -s $CLASS_D_MULTICAST -j DROP
iptables -A FORWARD -i $EX_IF -o $IN_IF -s $CLASS_E_RESERVED_NET -j DROP

### เครื่องภายนอกไม่มีทางใช้ loopback address ได้
iptables -A FORWARD -i $EX_IF -o $IN_IF -s $LOOPBACK

## ยอมรับแพ็กเก็ตที่เป็นส่วนหนึ่งของการเชื่อมต่อที่สร้างโดยภายในเอง
iptables -A FORWARD -i EX_IF -o $IN_IF -m state --state ESTABLISHED -j ACCEPT

#(from external to server)
## ยอมให้ภายนอกใช้บริการ web and mail server
iptables -A FORWARD -i EX_IF -o $IN_IF -d $IN_WEB_ADDR -p tcp --dport 80 -m state –state
NEW -j PROTECT
iptables -A FORWARD -i EX_IF -o $IN_IF -d $IN_MAIL_ADDR -p tcp --dport 25 -m state –state
NEW -j PROTECT

#(from external to internal host)
## drop แพ็กเก็ตที่ร้องขอการเชื่อมต่อจากภายนอกทั้งหมด
## คือ ไม่อนุญาติให้ภายนอกสร้างการเชื่อมต่อได้
iptables -A FORWARD -i $EX_IF -o $IN_IF -d $IN_HOST -m state --state NEW -j DROP

## RELATED packet jump to PROTECT
iptables -A FORWARD -i $EX_IF -o $IN_IF -m state --state RELATED -j PROTECT

# (from internal network to external)
## ป้องกัน trojans
## โดยการบันทึก log ไว้ แล้ว drop ทิ้ง
### deepthroat
```

```
iptables -A FORWARD -i $IN_IF -o $EX_IF -p tcp -m multiport --sport
41,999,2140,3150,6670,6771,60000 \-m limit -j LOG --log-prefix "DeepThroat: "
Iptables -A FORWARD -i $IN_IF -o $EX_IF -p tcp -m multiport --sport
41,999,2140,3150,6670,6771,60000 \-j DROP

### subseven
iptables -A FORWARD -i $IN_IF -o $EX_IF -p tcp -m multiport --sport
2773,6711,6712,6713, 7215,27374,27573,54283 \-m limit -j LOG --log-prefix "SubSeven:"
iptables -A FORWARD -i $IN_IF -o $EX_IF -p tcp -m multiport --sport
2773, 6711, 6712, 6713,7215,27374, 27573, 54283 \-j DROP

### netbus
iptables -A FORWARD -i $IN_IF -o $EX_IF -p tcp -m multiport --sport 12345,12346,20034 \-m
limit -j LOG --log-prefix "NetBus: "
iptables -A FORWARD -i $IN_IF -o $EX_IF -p tcp -m multiport --sport 12345,12346,20034 \-j
DROP

### back orifice (bo)
iptables -A FORWARD -i $IN_IF -o $EX_IF -p tcp -m multiport --sport 8787,31337,54320 \
-m limit -j LOG --log-prefix "Back Orifice: "
iptables -A FORWARD -i $IN_IF -o $EX_IF -p tcp -m multiport --sport 8787,31337,54320 \
-j DROP

## ยอมรับแพ็กเก็ตจากภายนอกออกสู่ภายนอกทั้งหมด
## แต่บันทึก log ไว้ก่อน เผื่อไว้ใช้ตรวจสอบ
iptables -A FORWARD -i $IN_IF -o $EX_IF -m limit -j LOG --log-prefix "FORWARD-OUT: "
iptables -A FORWARD -i $IN_IF -o $EX_IF -j ACCEPT
# ================================================
# output chain
```

```
## ป้องกัน trojans
## โดยการบันทึก log ไว้ แล้ว drop ทิ้ง
### deepthroat
iptables -A OUTPUT -p tcp -m multiport --sport 41,999,2140,3150,6670,6771,60000 \
-m limit -j LOG --log-prefix "DeepThroat: "
iptables -A OUTPUT -p tcp -m multiport --sport 41,999,2140,3150,6670,6771,60000 \
-j DROP

### subseven
iptables -A OUTPUT -p tcp -m multiport --sport 2773,6711,6712,6713,7215,27374,27573,54283 \-m
limit -j LOG --log-prefix "SubSeven: "
iptables -A OUTPUT -p tcp -m multiport --sport 2773,6711,6712,6713,7215,27374,27573,54283 \-j
DROP

### netbus
iptables -A OUTPUT -p tcp -m multiport --sport 12345,12346,20034 \-m limit -j LOG --log-prefix
"NetBus: "
iptables -A OUTPUT -p tcp -m multiport --sport 12345,12346,20034 \-j DROP

### back orifice (bo)
iptables -A OUTPUT -p tcp -m multiport --sport 8787,31337,54320 \-m limit -j LOG --log-prefix
"Back Orifice: "
iptables -A OUTPUT -p tcp -m multiport --sport 8787,31337,54320 \-j DROP

## ยอมรับแพ็กเก็ตที่ออกจากเครื่องไฟร์วอลล์ทั้งหมด
## แต่บันทึก log ไว้ก่อน เผื่อไว้ใช้ตรวจสอบ
iptables -A OUTPUT -m limit -j LOG --log-prefix "OUTPUT: "
iptables -A OUTPUT -j ACCEPT
# ==========================================
```

 # NAT

snat

iptables -t nat -A POSTROUTING -s $IN_HOST -i $IN_IF -o $EX_IF -j SNAT --to $FW_ADDR_EX

dnat

web server

iptables -t nat -A PREROUTING -d $EX_WEB_ADDR -p tcp --dport 80 -j DNAT --to $IN_WEB_ADDR

mail server

iptables -t nat -A PREROUTING -d $EX_MAIL_ADDR -p tcp --dport 25 -j DNAT --to $IN_MAIL_ADDR

4.7.5 Sonic wall Firewall PRO 300

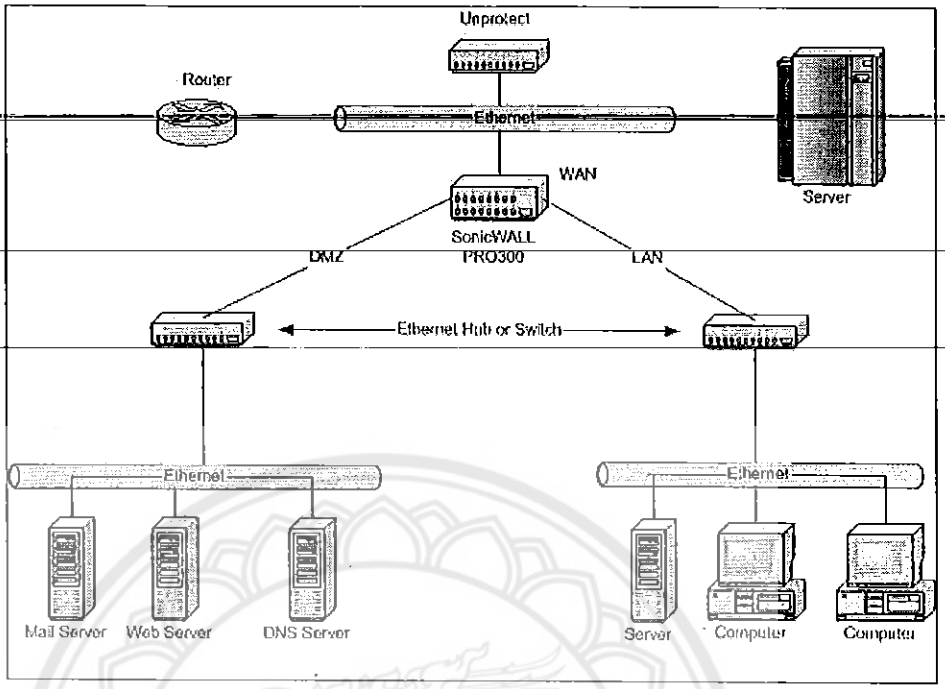
เป็นผลิตภัณฑ์ที่มีความสามารถในเรื่องความปลอดภัยในระบบอินเตอร์เน็ต ซึ่งป้องกันการการบุกรุก โดยสามารถจัดการการคอนฟิกกูเลชันได้โดยง่ายรับรององค์กรขนาดเล็กและองค์กรขนาดใหญ่ มีคุณสมบัติที่สำคัญดังนี้

4.7.5.1 คุณสมบัติของไฟร์วอลล์

- ระบบโปรเซสเซอร์ 233 MHz Strong ARM RISC with a CyberSentry Security
- RAM 64 MB
- Flash memory 4 MB
- WAN interface One10/100 Base-T autosensing
- LAN interface One10/100 Base-T autosensing

- **Intranet Firewalling**

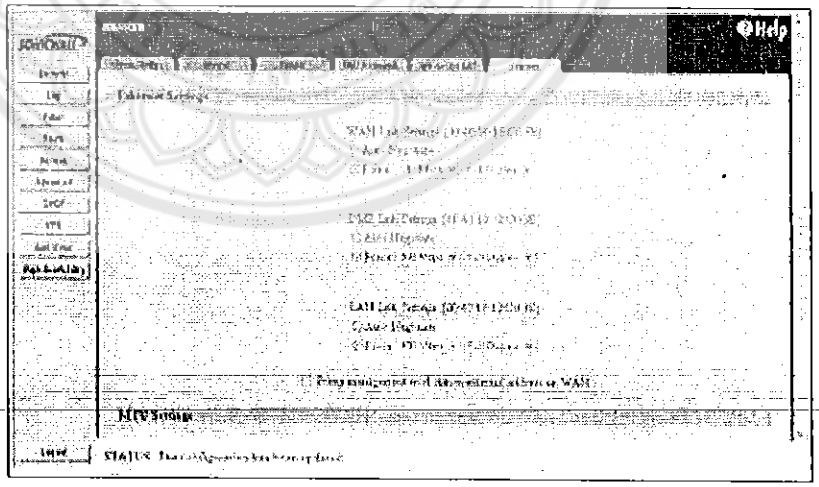
ลักษณะสำคัญของ Sonicwall เข้าถึง โฮสต์ที่เป็น WAN interface จากระบบเครือข่าย LAN โดยโฮสต์ที่อยู่กับเน็ตเวิร์กเดียวกันกับ WAN interface ของตัวไฟร์วอลล์และรวมไปถึง Router ดังรูป



รูปที่ 4-58 Intranet firewall diagram

(ที่มา: The Complete Reference Firewalls Mc Graw Hill)

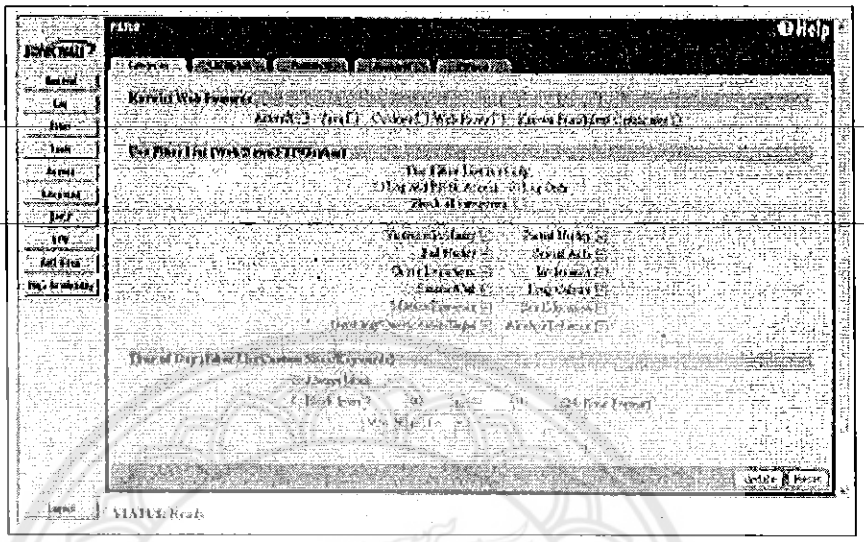
- **Ethernet Setting**



รูปที่ 4-59 Ethernet Setting

(ที่มา: The Complete Reference Firewalls Mc Graw Hill)

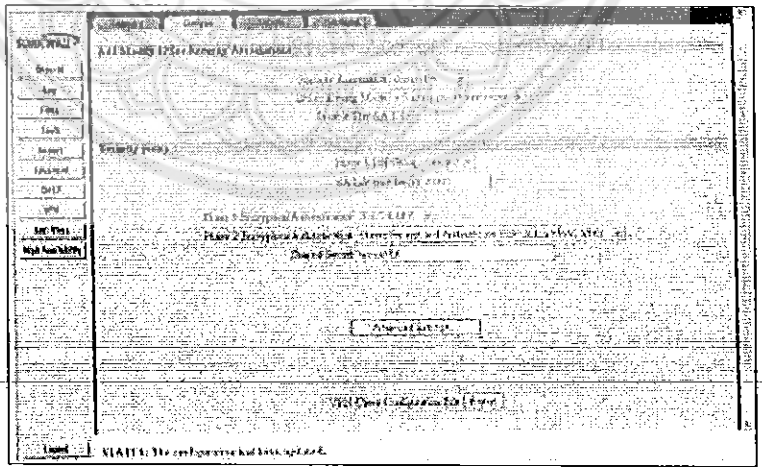
- **Filtering**



รูปที่ 4-60 Categories Tab

(ที่มา: The Complete Reference Firewalls Mc Graw Hill)

- VPN



รูปที่ 4-61 ความสัมพันธ์การคอนฟิก VPN

(ที่มา: The Complete Reference Firewalls Mc Graw Hill)

4.7.5.2 การคอนฟิกกูเรชัน Sonicwall

การคอนฟิก Sonicwall สามารถทำได้โดยการตั้งค่า, การเพิ่มกฎนโยบาย, การเพิ่มการบริการ และการเพิ่มหรือการแก้ไขยูสเซอร์ ในส่วนของ Network access rules ก็จะปฏิบัติตามการเพิ่มนโยบาย และลบนโยบายของความปลอดภัยและจะคอนฟิกได้ง่ายโดย GUI

4.7.5.3 คุณลักษณะที่สำคัญของ Sonicwall

- Sonicwall มีความสามารถป้องกันทรัพยากรเครือข่ายได้อย่างดี
- สามารถป้องกันการต่อต้านการโจมตีและการเข้าถึงที่ไม่ได้รับอนุญาติ
- สามารถแจกไอพีแอดเดรสไปยังเครื่องลูกข่ายได้(DHCP)
- สามารถสร้างการทำ Private IP เชื่อมต่อและใช้งานอินเทอร์เน็ตได้ (NAT)
- สนับสนุนการทำโพรโตคอลของไพรเวตเน็ตเวิร์ก(Virtual Private Network)

4.7.6 Internet Securities and Accelerator 2000 Server (ISA Server)

4.7.6.1 คุณลักษณะของ ISA Server

เป็นซอฟต์แวร์ที่รวบรวมเอาความสามารถด้านความปลอดภัยคือ ทำหน้าที่เป็นไฟล์วอลล์ Intrusion Detection และ Content Filtering มีความสามารถของพร็อกซี่และการบริหารแบนวิดธ์เข้าอยู่ในตัวเดียวกัน และยังมีการอิมพลีเมนต์ใช้งานได้โดยง่าย

4.7.6.2 ความต้องการของระบบ

- CPU Pentium-II 300 MHz
- RAM 256 MB
- พื้นที่ว่างบนฮาร์ดดิสก์อย่างต่ำ 20 MB
- ระบบปฏิบัติ Window 2000 Server ที่ติดตั้ง Service Pack 1 ขึ้นไป
- ฮาร์ดดิสก์ที่มีพาร์ติชั่นเป็นแบบ NTFS
- เน็ตเวิร์กอะแดปเตอร์ 3 การ์ดสำหรับเน็ตเวิร์กแต่ละเซกเมนต์

4.7.6.3 การติดตั้ง ISA Server

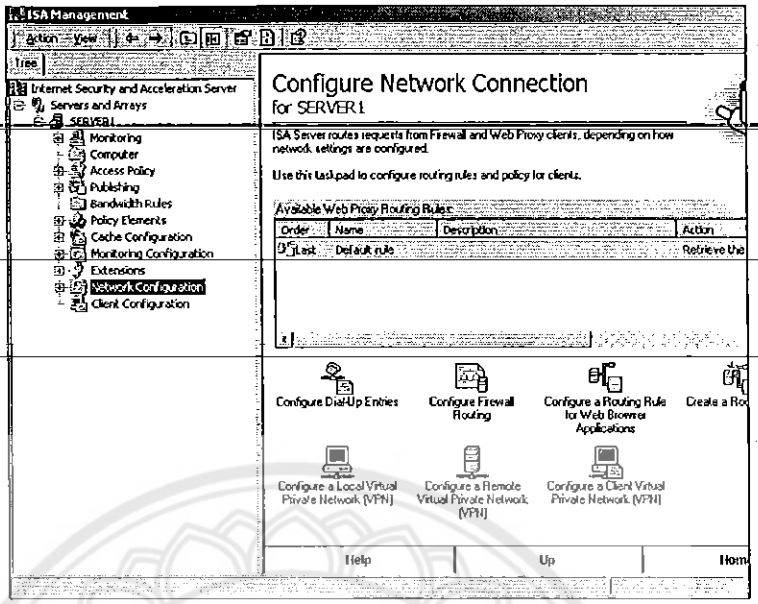
- ติดตั้งระบบปฏิบัติการ Window 2000 Server และติดตั้ง Service Pack ล่าสุดลงไปการดำเนินการในส่วนนี้จะใช้เวลาประมาณ 1 ชั่วโมงและจะต้องมีการรีบู๊ตคอมพิวเตอร์หลายครั้ง
- ทดสอบการผลการติดตั้งระบบปฏิบัติการว่าสามารถทำงานได้ตามปกติ โดยตรวจสอบใน Event Viewer ในส่วนของ System Log ว่ามีรายการแจ้งข้อผิดพลาดใดๆหรือไม่
- ทดสอบการทำงานของเน็ตเวิร์กว่าทำงานได้ตามปกติ โดย Ping ไปยังโฮสต์ที่อยู่บนแต่ละเซกเมนต์และเราเตอร์ รวมไปถึง Ping ไปยัง ISP ที่เชื่อมต่ออยู่
- ทดสอบการเชื่อมต่อกับอินเตอร์เน็ต อาจจะใช้วิธีง่ายโดยการทดลองบราวส์เว็บ

4.7.6.4 การ คอนฟิกกูเรชัน ISA Server

การควบคุม ISA Server นั้นทำได้โดยผ่านโปรแกรม ISA Management เป็นเสมือนคอนโซลควบคุมการทำงานทั้งหมดของ ISA Server เนื่องจากคอมโพเนนต์ที่มีใน ISA Server นั้นมีค่อนข้างมากและมีความสัมพันธ์เกี่ยวข้องกับการทำงานด้วยกันทั้งสิ้น การกำหนดค่าต่าง ๆ ลงไปที่คอมโพเนนต์โดยตรงอาจจะเข้าใจได้ยากพอสมควร ในการเรียกใช้งานครั้งแรกโปรแกรมจะมี Wizard เพื่อช่วยให้การกำหนดค่าต่าง ๆ นั้นครบถ้วนและทำได้ง่ายขึ้นโดยผ่านเมนูที่จะระบุหน้าที่และความต้องการในการกำหนด เช่นกำหนดตารางเวลา กำหนดกลุ่มของไคลเอนต์ กำหนดค่าของการต่ออินเตอร์เน็ตโดย Dial-Up เป็นต้น และเมื่อเลือกผ่านเมนูก็จะเข้าถึงคอมโพเนนต์เกี่ยวกับเรื่องต้องการในทันที ซึ่งจะแตกต่างจากการกำหนด Configuration

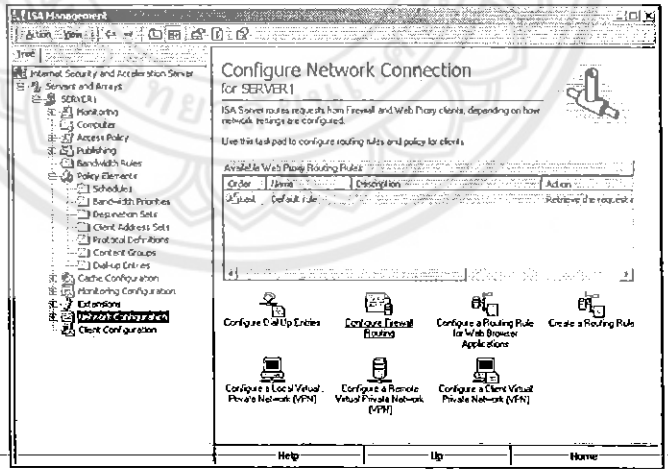
1. กำหนด IP Address ของแต่ละโซน เพื่อให้ ISA Server ทราบว่าส่วนใดเป็น Internal network ส่วนใดเป็น DMZ และส่วนใดเป็น External network โดยการกำหนดที่คอมโพเนนต์ของ Network Configuration

   ในส่วนของ Network Configuration นั้นจะมี 3 คอมโพเนนต์หลักก็คือ Routing, Local Address Table และ Local Domain Table ในเบื้องต้นให้กำหนดเฉพาะ Local Addrese Table เพื่อระบุ IP Address ของ Internal network และ DMZ เสียก่อน โดยการเลือกคอมโพเนนต์จากโฟลเดอร

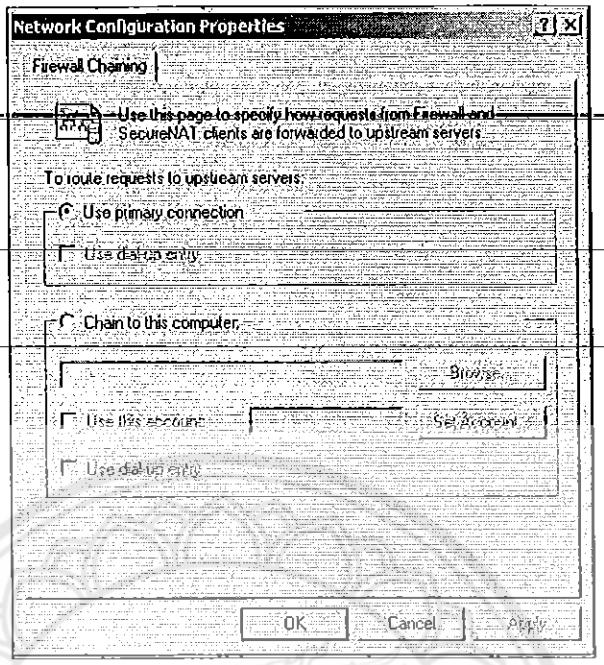


รูปที่ 4-62 หน้าจอคอนโซลเมื่อเลือกคอมโพเนนต์ของ Network Configuration

2. กำหนดทิศทางการเราต์แพ็คเก็ตจากโฮสต์ที่อยู่ภายใน DMZ และ Internal network โดยการเลือกโฟลเดอร์ Network Configuration และคลิกไอคอน Configure Firewall Routing



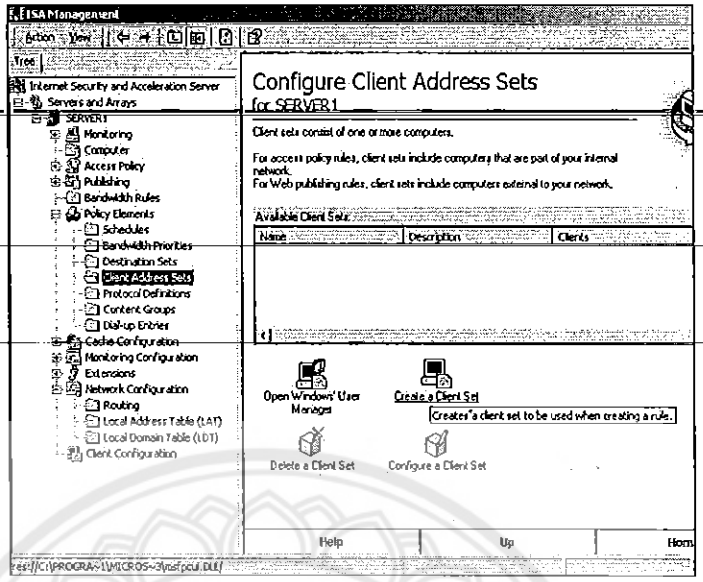
รูปที่ 4-63 หน้าจอหลักของ Network Configuration



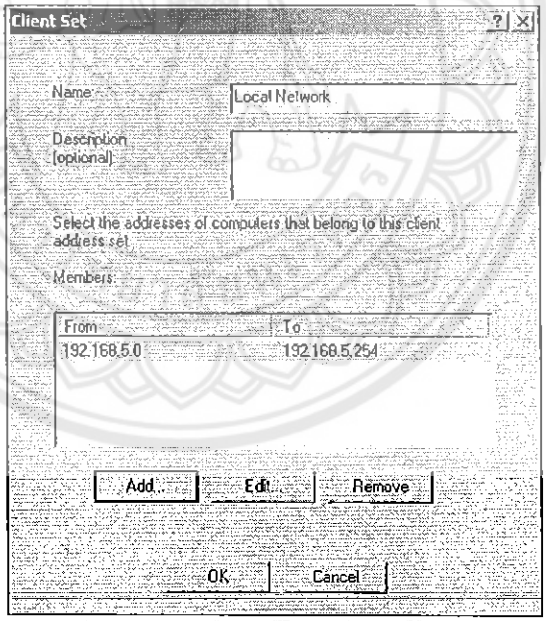
รูปที่ 4-64 หน้าจอ การกำหนด Firewall Routing

เนื่องจาก ISA Server นี้เชื่อมต่อมกับอินเตอร์เน็ตโดยผ่านเราเตอร์โดยตรงไม่ได้ผ่าน Dial-Up Connection หรือผ่านไปยังคอมพิวเตอร์อื่น ดังนั้นจะต้องกำหนดออปชั่นของ to route requests to upstream servers เป็น Use primary Connection

3. กำหนด Client Address Set ซึ่งหมายถึงกลุ่มของโฮสต์ที่ใช้งานเป็นไคลเอนต์ เพื่อสำหรับใช้อ้างอิงถึงโฮสต์ที่อยู่ใน Internal network เนื่องจากในการกำหนดแอคเซสรูมมักจะต้องเรียกอ้างอิงถึง Client Set อยู่เสมอ



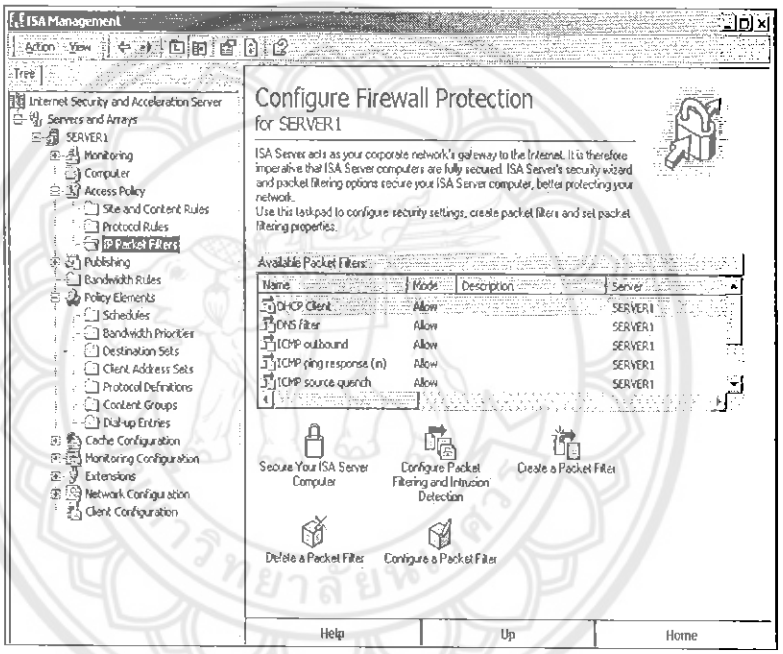
รูปที่ 4-65 หน้าจอของหลักของ Client Address Sets



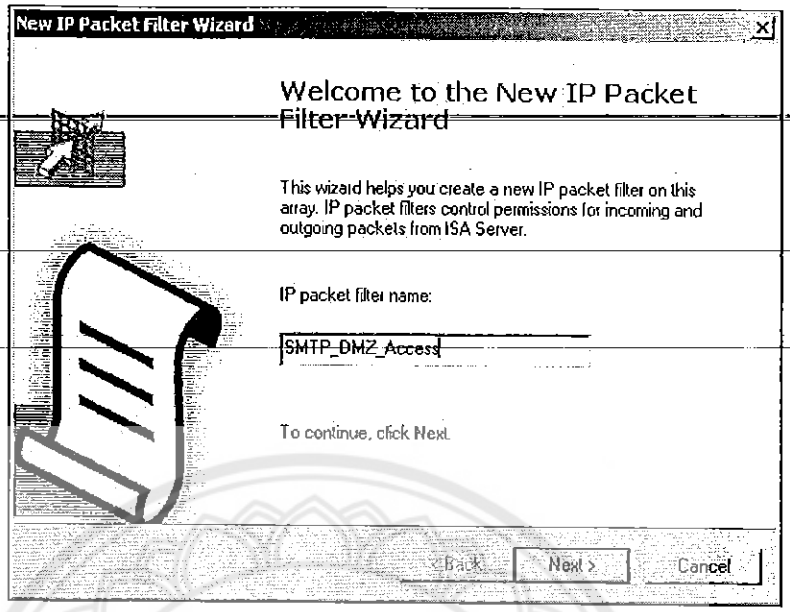
รูปที่ 4-66 หน้าจอสำหรับป้อนค่าเข้าไปใน Client Address Sets

โดยกำหนดชื่อของกลุ่ม Client Address Sets ซึ่งในตัวอย่างนี้คือ Internal network ที่มี IP Address อยู่ในช่วงตั้งแต่ 192.168.1.254 – 192.206.1.0 หลังจากจัดเก็บข้อมูลเรียบร้อยแล้วต่อไปหากมีการกำหนดค่าใดที่ต้องระบุ Address ของโฮสต์แล้ว จะปรากฏ Internal network ให้เลือกอยู่เสมอ

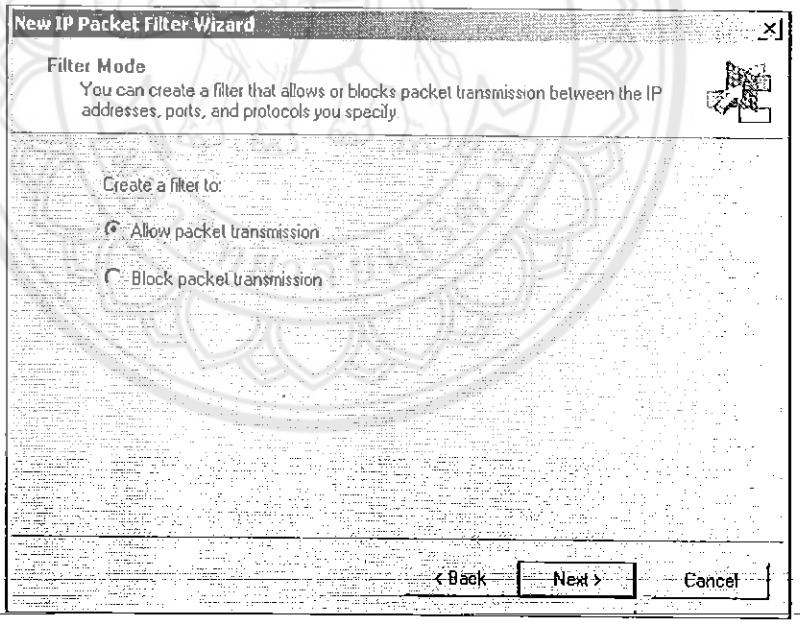
4. นำแอคเซสรูลที่มากำหนดลงใน Policy ของ ISA Server หลังจากได้ทำการกำหนดเกี่ยวกับ Internal network เป็นการเรียบร้อยแล้ว ก็จะเป็นการกำหนดแอคเซสรูลให้สามารถเข้าไปใช้บริการเซิร์ฟเวอร์ต่าง ๆ ที่อยู่ใน DMZ ตามที่ต้องการ



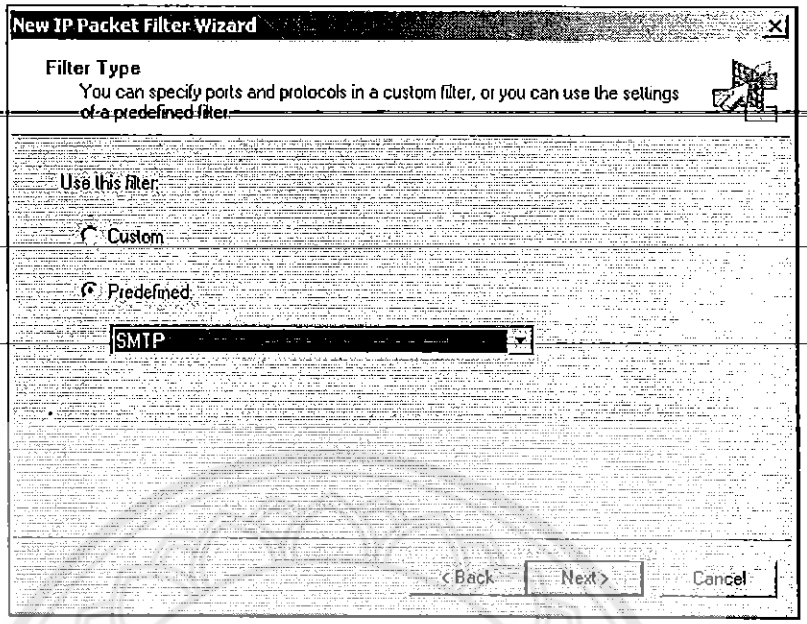
รูปที่ 4-67 หน้าจอสำหรับจัดการเกี่ยวกับ IP Packet Filter



รูปที่ 4-68 หน้าจอ Wizard สำหรับช่วยในการกำหนด Rules



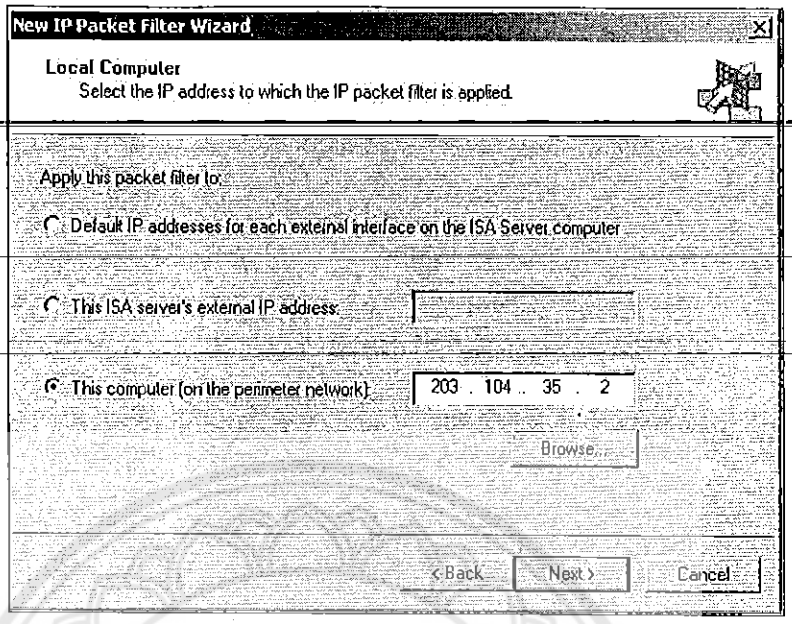
รูปที่ 4-69 การเลือกโหมดของการฟิลเตอร์ว่าจะเป็น Allow หรือ Block



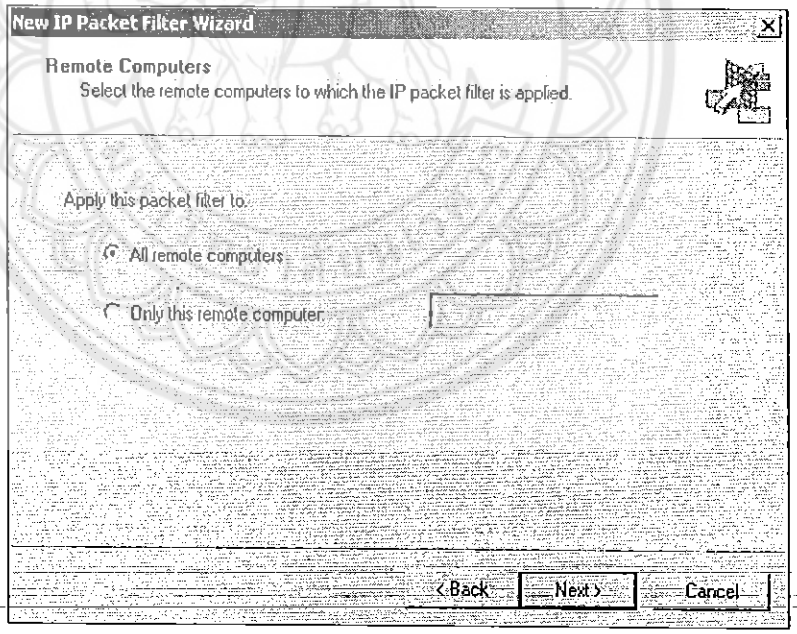
รูปที่ 4-70 การเลือกลักษณะของการฟิลเตอร์

ในการกำหนด IP Packet Filter นั้นจะเริ่มต้นด้วยการเลือกโหมดของการฟิลเตอร์เสียก่อนว่าแอคเซสรูลนี้จะกำหนดเพื่ออนุญาตหรือปิดกั้นแพ็คเก็ต หลังจากนั้นก็จะเลือกลักษณะของแพ็คเก็ตที่จะทำการฟิลเตอร์ว่าจะเป็นโปรโตคอลอะไร มีรายละเอียดของแพ็คเก็ตอย่างไร โดย ISA Server ได้ กำหนดรูปแบบของโปรโตคอลที่มีการใช้งานเป็นประจำเป็นไว้ล่วงหน้าแล้ว

ดังเช่นจากตัวอย่างข้างต้นเราสามารถเลือกรูปแบบการฟิลเตอร์ของ SMTP ได้จากที่กำหนดไว้ล่วงหน้าโดยใช้ออปชั่น Predefined ได้ทันที นอกจากนี้ยังมีโปรโตคอลอื่น ๆ ที่ได้กำหนดเอาไว้แล้ว เช่น POP3, HTTP, DNS เป็นต้น ช่วยให้การกำหนดแอคเซสรูลทำได้ง่ายขึ้น หากรูปแบบการฟิลเตอร์ใดไม่มีกำหนดไว้ ก็จะต้องเลือกแบบ Custom ซึ่งจะต้องกำหนดคุณลักษณะของแพ็คเก็ตทั้งหมดด้วยตนเอง

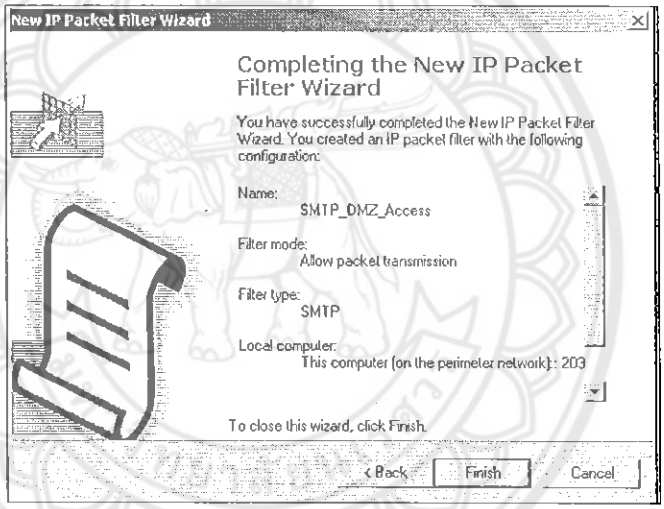


รูปที่ 4-71 หน้าจอเลือก Local Computer



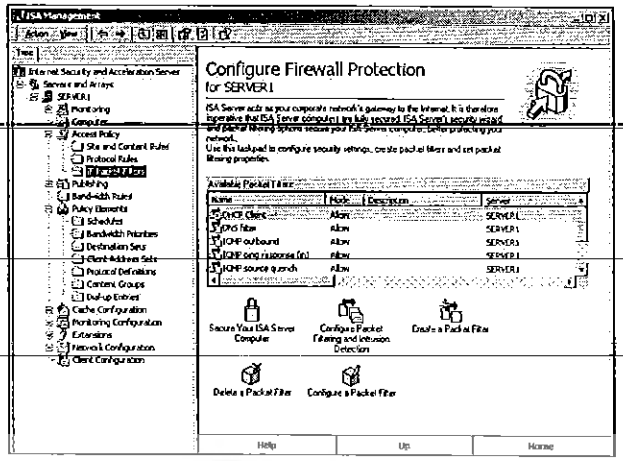
รูปที่ 4-72 หน้าจอเลือก Remote Computer

5. หลังจากกำหนดลักษณะของการฟิลเตอร์แล้วลำดับสุดท้ายจะเป็นการกำหนด IP Address ต้นทางและปลายทางของแอคเซสรูล สำหรับ ISA Server แล้วอาจจะเรียกแตกต่างจากที่เข้าใจกันทั่วไปคือ Source และ Destination แต่จะเรียกว่า Local Computer และ Remote Computer แทน สำหรับแอคเซสรูลของ SMTP ก็ระบุ IP Address ของ SMTP Server คือ 203.140.35.2ลงไป และสำหรับ Remote Computer นั้นให้กำหนด All remote computer นั่นหมายถึงอนุญาตให้โฮสต์ใด ๆ ก็ตามสามารถแอคเซสเข้ามาได้เพราะจะทำให้สามารถรับอีเมล์จากอินเตอร์เน็ตได้ หลังจากเลือก Local และ Remote Computer เรียบร้อยแล้วก็เป็นเสร็จขั้นตอนการกำหนด IP Packet Filter หน้าจากจะปรากฏข้อมูลสรุปสิ่งที่ได้กำหนดไว้



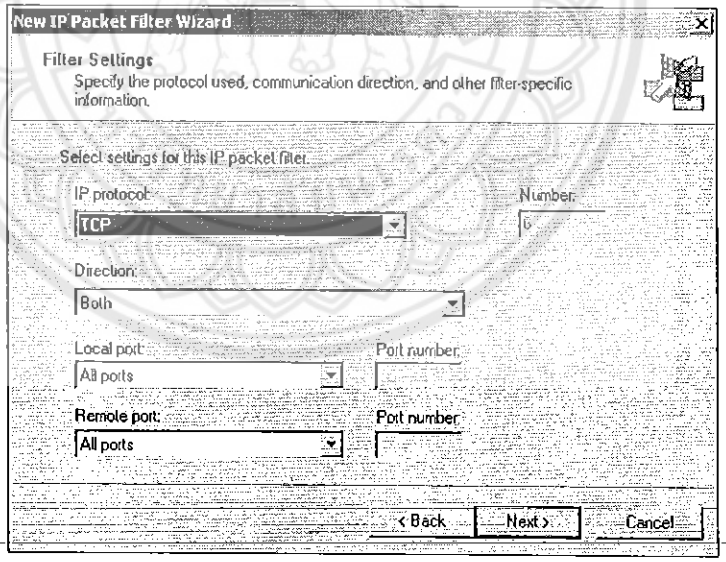
รูปที่ 4-73 หน้าจอเมื่อการกำหนด IP Packet Filter เสร็จสมบูรณ์

6. สำหรับแอคเซสรูลของเซิร์ฟเวอร์อื่น ๆ ที่อยู่ใน DMZ ไม่ว่าจะเป็น POP3, HTTP, FTP รวมทั้งการบริการอย่างที่จำเป็นต่อการทำงานของเซิร์ฟเวอร์เอง เช่น DNS Query ก็ให้นำลักษณะการใช้งานทั้งหมดนั้นมากำหนดเป็นแอคเซสรูลใน IP Packet Filter เช่นเดียวกับของ SMTP Server เพียงแต่เปลี่ยนโปรโตคอลและ Local Computer ให้เป็นของแต่ละเซิร์ฟเวอร์ จนครบของทุกเซิร์ฟเวอร์

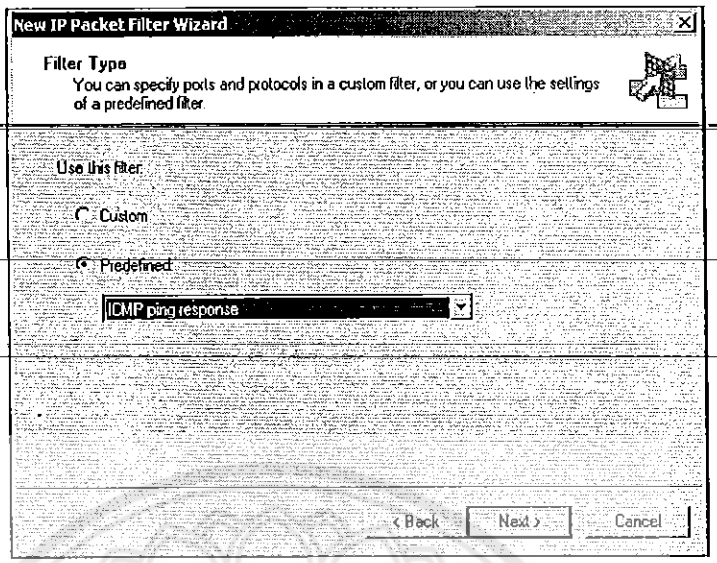


รูปที่ 4-74 IP Packet Filter ที่ครอบคลุมทุกเซิร์ฟเวอร์ใน DMZ

7. หาก IP Packet Filter ใดไม่มีการกำหนด Predefined Filter Type แล้วจะต้องกำหนดเองแบบ Custom นั้นจะต้องมีข้อมูลเสียก่อนว่าแอพพลิเคชั่นที่จะให้บริการนั้นใช้โปรโตคอลอะไร TCP/IP (TCP, UDP หรือ ICMP)



รูปที่ 4-75 หน้าจอสำหรับกำหนด Filter Type
สำหรับโปรโตคอลที่ไม่ได้มีการกำหนดไว้ล่วงหน้า



รูปที่ 4-76 หน้าจอตัวอย่างการกำหนด Filter Type สำหรับโปรแกรม Ping

8. กำหนดแอคเซสรูลให้กับไคลเอนต์ที่อยู่ใน Internal network ในส่วนของ Internal network นั้น นอกจากจะสามารถควบคุมโดยผ่าน IP Packet Filter ซึ่งเป็นการควบคุมในระดับต่ำแล้ว ISA Server ยังมีส่วนเพิ่มเติมเพื่อการควบคุมใน Internal network ให้มีประสิทธิภาพและสะดวกมากขึ้น เป็นโอกาสให้สามารถกำหนดแอคเซสรูลในระดับแอพพลิเคชั่นได้ โดยผ่านการกำหนดใน 2 ส่วนคือ Protocol Rules และ Site and Content Monitoring

4.7.7 Firewall with FreeBSD 4.8

4.7.7.1 การ Kernel Options

การ Recompiler kernel ในกรณีที่สงสัยเกี่ยวกับ เรื่อง configuring the FreeBSD Kernel ต้องเพิ่ม option ต่อไปนี้ ใน ไฟล์ kernel configuration

Options IPFIREWALL

ทำให้เกิดมี Kernel's firewall code.

Options IPFIREWALL_VERBOSE

ส่ง Logged packets ไปยัง system logger.

Options IPFIREWALL_VERBOSE_LIMIT= 100

จำกัด จำนวนที่จะบันทึก เพื่อป้องกันมิให้ log file ต้องมี แต่ ข้อมูลซ้ำๆกัน 100นี้ เป็นเลข ที่สมเหตุสมผลแล้ว ซึ่งสามารถปรับเอา ตามความต้องการได้

Options IPDIVERT

ให้มี divert sockets

Options TCP_DROP_SYNFIN

Option นี้ ทำให้ TCP packets ที่มี SYN and FIN ไม่ได้รับการพิจารณาอันนี้ จะป้องกันการตรวจจับ TCP/IP stack โดย nmap แต่ก็จะทำให้ RFC 1644ไม่ได้รับการสนับสนุน ซึ่ง ไม่ แนะนำ ทำผ่านเครื่อง web server.

4.7.7.2 แก้ไขไฟล์ /etc/rc.conf เพื่อให้ firewall ทำงาน

ทำการต้องแก้ไขเพิ่มเติมไฟล์ /etc/rc.conf เพื่อบอกให้รู้เกี่ยวกับ firewall ก็แค่เพิ่มบรรทัด

```
firewall_enable="YES"
firewall_script="/etc/firewall/fwrules"
natd_enable="YES"
natd_interface="tun"0
natd_flags="-dynamic"
```

รายละเอียดเพิ่มเติม โปรดดูจากไฟล์ /etc/defaults/rc.conf ในระบบปฏิบัติการ FreeBSD 4.8

4.7.7.3 ปิด Network address translation ของ PPP

คุณสมบัติพิเศษเรื่อง Network addresses translation (NAT) ของ PPP อยู่แล้วก็ได้ ถ้าเป็นเช่นนั้น ขอให้ปิดสมบัตินั้นเสีย เพื่อทำหน้าที่นั้นแทนถ้ากำหนดให้ PPP เริ่มทำงานโดยอัตโนมัติ ไว้แล้ว ซึ่งก็เพียงสามสี่บรรทัด คล้ายๆกันนี้:

```
ppp_enable="YES"

ppp_mode="auto"

ppp_nat="YES"

ppp_profile="profile"
```

4.7.7.4 ชุดกฎระเบียบ สำหรับ firewall

Restart และให้ firewall ทำงาน สร้าง directory/ etc/firewall .และเข้าไปสู่ Directory นั้น แล้วแก้ไขไฟล์ fwrules ตามที่ระบุไว้ในไฟล์ rc.conf โปรดสังเกตุด้วยว่า ชื่อไฟล์แรกนั้น กำหนดเป็นอะไรก็ได้ ในไฟล์หลังนั่น แล้วก็ปรับให้ตรงกัน

Firewall ตัวอย่าง ซึ่ง บอกรายละเอียด

```
# Firewall rules

# written by Marc Silver (marcs@draenor.org)

# http://draenor.org/ipfw

# freely distributable

# Define the firewall command (as in /etc/rc.firewall) for easy

# Reference.  Helps to make it easier to read.

fwcmd="/sbin/ipfw"
```

```
# บังคับลบทุกๆกฎก่อน

$fwcmd -f flush

# divert ทุกๆ packets ผ่าน tunnel interface ที่ใช้โดยโปรแกรม PPP.

$fwcmd add divert natd all from any to any via tun0

# อนุญาตให้ data ทั้งหมด จาก network card ของเรา และ localhost. ให้แก้ไข

$fwcmd add allow ip from any to any via lo0

$fwcmd add allow ip from any to any via fxp0

# อนุญาต ให้ ต่อได้ทั้งหมด ที่ได้เริ่มขึ้นมาแล้วนั้น

$fwcmd add allow tcp from any to any out xmit tun 0setup

# เมื่อต่อติดแล้ว, อนุญาต ให้ เปิดรอ ได้

$fwcmd add allow tcp from any to any via tun 0established

# อนุญาตให้ทุกคน ต่อ ผ่าน บริการในเครื่องนี้ เพียง ssh และ apache เท่านั้น

$fwcmd add allow tcp from any to any  80setup

$fwcmd add allow tcp from any to any  22setup

# ส่ง RESET ไปยัง ident packets ทั้งหมด

$fwcmd add reset log tcp from any to any  113in recv tun0

# อนุญาตให้ถามออกไป DNS จำเพาะ name server ที่ระบุไว้เท่านั้น

ก็แทนจุดๆ ด้วยหมายเลข IP  ของ nameserver

$fwcmd add allow udp from any to x.x.x.x 53 out xmit tun0
```

 # อนุญาต ให้เข้ามา พร้อมคำตอบ

$fwcmd add allow udp from x.x.x.x 53 to any in recv tun0

 # อนุญาตให้ ICMP

$fwcmd add allow icmp from any to any

 # ที่เหลือก็ปฏิเสธทั้งหมด

$fwcmd add deny log ip from any to any

Firewall ที่ใช้งานได้แล้ว และอนุญาตให้เรียกใช้บริการทั้งสอง port คือ 80&22 พร้อมทั้ง log ความ พยายามอื่นๆที่เพียรต่อเข้ามา ไว้ด้วย

4.12.5 การติดตั้งและใช้งานไฟวอล์ลของ **FreeBSD**

การติดตั้ง

1.ต้องทำการคอนฟิกเคอร์เนลในไฟล์คอนฟิกของเคอร์เนลและคอมไพเคอร์เนลด้วยออฟชันต่อไปนี้

options IPFIREWALL

options IPFIREWALL_FORWARD

options IPFIREWALL_VERBOSE

options IPFIREWALL_VERBOSE_LIMIT=128

2. เมื่อทำการคอมไพเรียบร้อยแล้วต้องเข้าไปเพิ่มคำสั่งต่อไปนี้ในไฟล์ /etc/rc.conf

firewall_enable="YES" # Set to YES to enable firewall functionality

firewall_script="/etc/rc.firewall" # Which script to run to set up the firewall

firewall_type="OPEN" # Firewall type (see /etc/rc.firewall)

firewall_quiet="NO" # Set to YES to suppress rule display

firewall_logging="NO" # Set to YES to enable events logging

firewall_flags="" # Flags passed to ipfw when type is a file

จากนั้นทำการ Restart เครื่องใหม่

3. เมื่อเข้าระบบได้แล้วก็ลองตรวจสอบเน็ตเวิคร์ก่อนว่าสมบูรณ์ดีใหม่ลอง ping เครื่องต่างๆในระบบของว่าเจอไหมถ้าทุกอย่างปกติ ก็ข้ามขั้นต้อนนี้ไปไปได้เลย ซึ่งมันก็คือขึ้นขั้นตอนทำให้ไฟวอลล์ยอมให้ทุกเพคเกจของข้อมูลผ่านได้ใช้คำสั่ง

#ipfw add 65000 pass all from any to any

คำสั่งดูกฎของไฟวอล์ลทั้งหมด

#ipfw show

ซึ่งผลการรันจะออกมาแบบนี้

00100 4174 551308 allow ip from any to any via lo0

00200 0 0 deny ip from any to 127.0.0.0/8

00300 0 0 deny ip from 127.0.0.0/8 to any

00400 367703 255889440 allow ip from 192.168.0.0/24 to 192.168.0.0/24

00500 224956 89416080 allow tcp from any to any via tun0

00700 59377 6800555 fwd 127.0.0.1,8080 tcp from any to any 80

65000 160037 70649800 allow ip from any to any

65535 0 0 deny ip from any to any

4.7.7.6 กฎของไฟวอลล์ อธิบายดังต่อไปนี้

#ipfw add 65000 pass all from any to any

คำสั่งนี้เป็นการเพิ่มกฎของไฟวอล์ลที่ 65000 คือยอมให้เพคเกจทุกอย่างผ่านไปได้ ถ้าดูด้วยคำสั่ง ipfw show ก็จะมีกฎหมายเลข 65000

65000 160037 70649800 allow ip from any to any

ลืมบอกไปอย่างหนึ่งว่ากฎพื้นฐานของไฟวอล์ลของ FreeBSD จะมีกฎหมายเลข 65535 ดังนี้

65535 0 0 deny ip from any to any

ซึ่งก็คือไม่ยอมให้เพคเกจใดผ่านนี่ก็คือสาเหตุว่าทำไมถ้าคอมไฟเดอร์แนลให้ใช้ไฟวอล์ลแล้วบูตเครื่องเลยทำให้ การทำงานทางเน็ตเวิคร์ทำงานไม่ได้เลย

ต่อมาว่าด้วยเรื่องหมายเลขของกฎมีความสำคัญตรงที่เป็นลำดับการทำงานกฎใหนที่หมายเลขของกฎ น้อยก็จะสำคัญมาก FreeBSD จะมองจากหมายเลขน้อยมาหามา อย่างเช่นถ้าเราใช้คำส่ง ipfw show แล้วขึ้นกฎดังนี้

65000 160037 70649800 allow ip from any to any

65535 0 0 deny ip from any to any

ก็หมายความว่าจะทำตามกฎหมายเลข 65000 ก่อนคือยอมให้ทุกเพคเกจผ่าน แล้วค่อยทำตาม 65535 คือไม่ยอมให้ทุกเพคเกจผ่านดูเลขที่อยู่หลังหมายเลขกฎคือเพคเกจที่วิ่งออกและวิ่งเข้าตามลำดับของกฎนั้นๆ เราสามารถเคลียให้เป็น 0 ได้ด้วยคำสั่ง

 # ipfw zero 65000

หมายถึงการเคลียการนับของเพคเกจของกฎหมายเลข 65000 ให้เป็นศูนย์ เรื่องการลบกฎของไฟวอลล์ใช้คำสั่ง delete เช่นคำสั่ง

 # ipfw delete 65000

หมายถึงการลบกฎหมายเลข 65000 ซึ่งถ้าตาม ipfw show นี้

65000 160037 70649800 **allow ip from any to any**

ก็จะลบทุกลบการยอมให้ทุกเพคเกจผ่านไปไปได้ซึ่งถ้าไม่กฎใดๆ

การเพิ่มกฎของไฟวอล์ลใช้คำสั่ง add เช่นคำสั่ง

4.7.7.7 ออฟชันที่เกี่ยวกับการยอมรับและปฏิเสธเพคเกจ

reject

ออฟชันนี้ปฏิเสธเพคเกจและส่ง ICMP host หรือบอกกล่าวทาง host ที่ร้องขอว่าไม่สามารถให้บริการได้

allow

ออฟชันนี้ยอมให้ทุกเพคเกจผ่านไปได้

deny

ออฟชันนี้ปฏิเสธเพคเกจและไม่ส่ง ICMP host หรือไม่บอกกล่าวทาง host ที่ร้องขอว่าไม่สามารถให้บริการได้

count

นับเพคเกจแต่ไม่ผ่านกฎที่ให้ออฟชันนี้แต่จะให้ใช้กฎของไฟวอลล์ข้อต่อไปเลย

ออฟชันของโปรโตคอลของไฟวอลล์

all

หมายถึงทุกโปรโตคอล

icmp

หมายถึงโปรโตคอล ICMP อาจจะงงเพราะตัวเองก็ยังไม่ค่อยเข้าใจ โปรโตคอลนี้ใช้ในคำสั่ง ping

tcp

หมายถึงโปรโตคอล tcp อันนี้คงไม่ต้องพูดหลายอย่างใช้โปรโตคอลนี้ เช่น http , mail , ircd

udp

หมายถึงโปรโตคอล udp อันนี้คงตรงข้ามกับ tcp เช่น DNS

4.7.7.8 การตรวจสอบ log file ของ friewall

โดยปรกติดแล้ว friewall ของ FreeBSD จะไม่ไม่ทำการเก็บ log file หากต้องการต้องคอมไพ kernel ให้มี option ต่อไปนี้

options IPFIREWALL_VERBOSE

options IPFIREWALL_VERBOSE_LIMIT=128

ซึ่งค่านี้

IPFIREWALL_VERBOSE # ค่านี้หมายถึงการติดตั้งให้ firewall เก็บ logfile

IPFIREWALL_VERBOSE_LIMIT=128 # หมายถึงจำนวนบรรทัดที่จะใช้เก็บค่าของ logfile สำหรับกฎของ firewall นั่นๆ

ถึงตรงนี้แล้วบางคนอาจไม่ได้ติดตั้งก็ตรวจสอบได้จากคำสั่ง

sysctl -a | grep net.inet.ip.fw.verbose

ถ้าได้ผลรัน

net.inet.ip.fw.verbose: 0 # เป็นศูนย์หมายถึงไม่ทำการติดตั้ง

net.inet.ip.fw.verbose_limit: 0 # เป็นจำนวนบรรทัดที่ใช้เก็บข้อมูลใน logfile

ซึ่งสามารถทำการตั้งค่าใหม่ได้ด้วยคำสั่ง

sysctl net.inet.ip.fw.verbose=1

sysctl net.inet.ip.fw.verbose_limit=1024

คำสั่ง sysctl เป็นคำสั่งปรับแต่งค่าตัวแปรของ kernel

4.7.8 ไฟร์วอลล์ในระบบปฏิบัติการ Windows 2000

เนื่องจากปัญหาด้านความปลอดภัยที่ค่อนข้างต่ำในระบบปฏิบัติการ Windows 95, 98, Me ซึ่งส่วนมากจะใช้ในระบบคอมพิวเตอร์ส่วนบุคคล ทำให้ไมโครซอฟต์ต้องทำการปรับปรุงระดับความปลอดภัยของ windows 2000 ให้ดีกว่าระบบเดิมหลายด้าน รวมทั้งระบบไฟร์วอลล์ โดยระบบไฟร์วอลล์ของ windows 2000 จะเป็นแบบ packet filtering ดังนั้นการตั้งกฎของไฟร์วอลล์นั้นต้องมีความรู้เกี่ยวกับการทำงานของ TCP/IP protocol

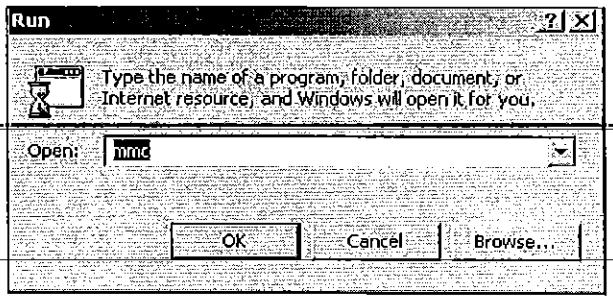
MMC (Microsoft Management Console)

mmc เป็นโปรแกรมของผู้ดูแลระบบ (administrator account) สำหรับช่วยในการวางแนวทางและขอบเขตของผู้ใช้งาน (User) หรือกลุ่มของผู้ใช้งาน (Group) ตามระบบและระเบียบที่ administrator ต้องการ ภายในโปรแกรมจะประกอบด้วยโมดูลหลักๆ ของการจัดระบบ ที่เรียกว่า snap-ins เช่น activeX Control , Certificates, Component services, Device Manager เป็นต้น ในบทความนี้จะไม่กล่าวถึงรายละเอียดของ mmc

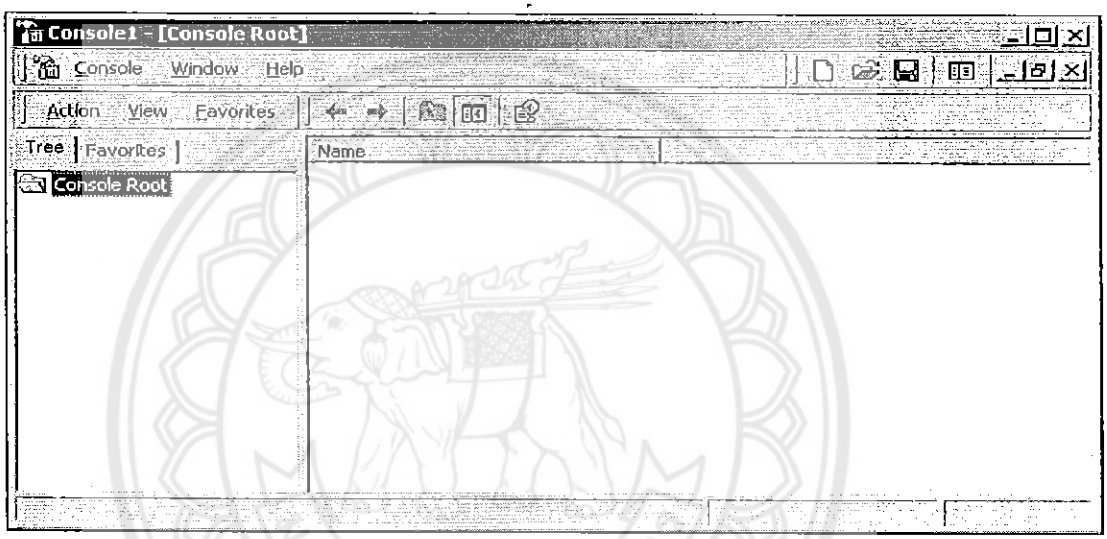
mmc มี snap-ins เพื่อสร้างระบบความปลอดภัยของระบบเครือข่ายในระดับไอพี ที่เรียกว่า IP Security หน้าที่ของ snap-ins นี้คือการสร้างไฟร์วอลล์ให้กับเครื่องผ่านการสร้างกฎที่มีรูปแบบ เดียวกันกับ packet filtering firewall

4.7.8.1 เริ่มต้นการสร้างระบบไฟร์วอลล์

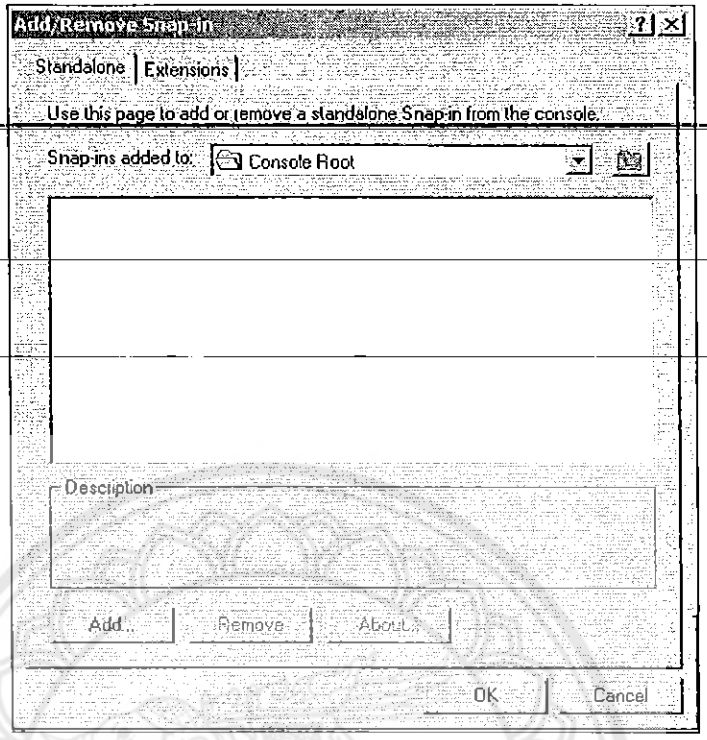
ในส่วนนี้จะกล่าวขึ้นตัวอย่างการสร้างกฎ และการทดลองใช้งานกฎของ IP firewall ใน IP security snap-ins โดยขั้นตอนหลักๆ มีดังนี้



รูปที่ 4-77 ใส่คำสั่ง mmc



รูปที่ 4-78 เลือก เมนู Console Root



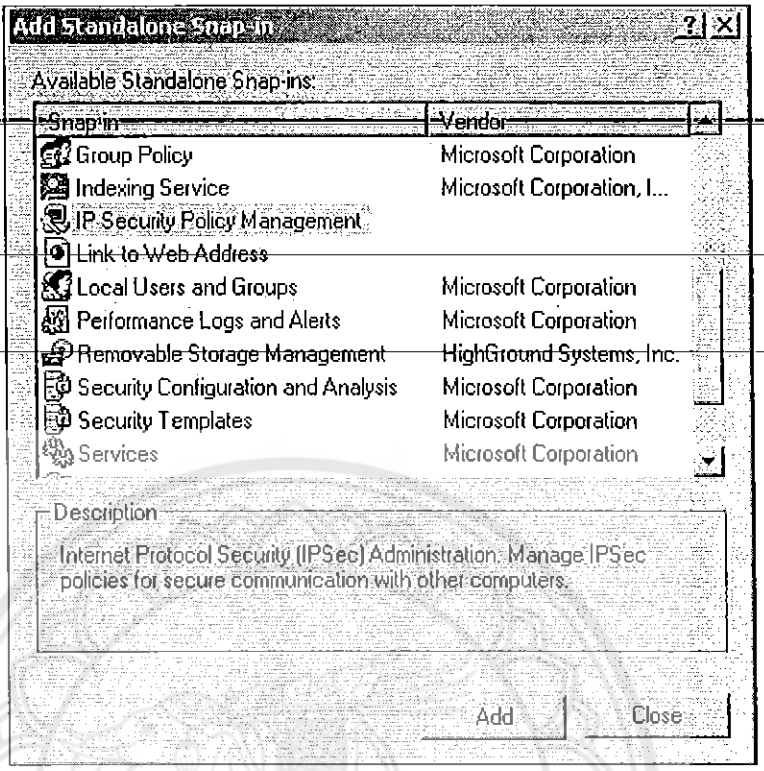
รูปที่ 4-79 Add/Remove Snap-in

4.7.8.2 การเพิ่ม IP secuirty snap-ins ใน mmc console

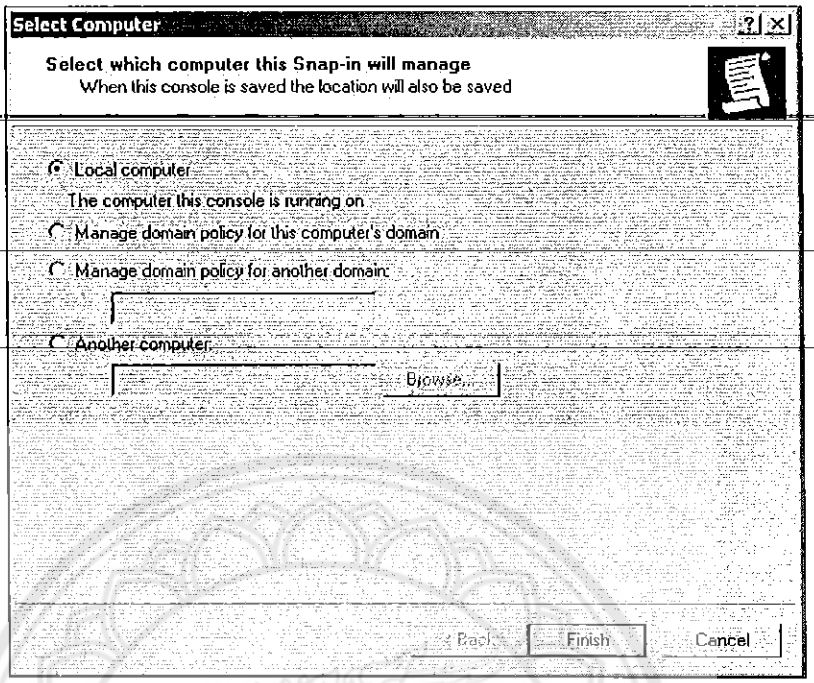
1. เรียกใช้งาน mmc โดยเลือก: Start ใน task bar -> Run -> ใส่คำสั่ง mmc

2. เลือก เมนู Console -> เลือก Add/Remove Snap-in -> กดปุ่ม Add

3. เลือก "IP Security Policy Management" ใน add standalone Snap-In block-> กดปุ่ม Add เมื่อเข้าสู่ Select Computer กดปุ่ม Finish และ กดปุ่ม Close ใน add standalone Snap-In block และ กดปุ่ม Ok ใน Add/Remove Snap-in Block

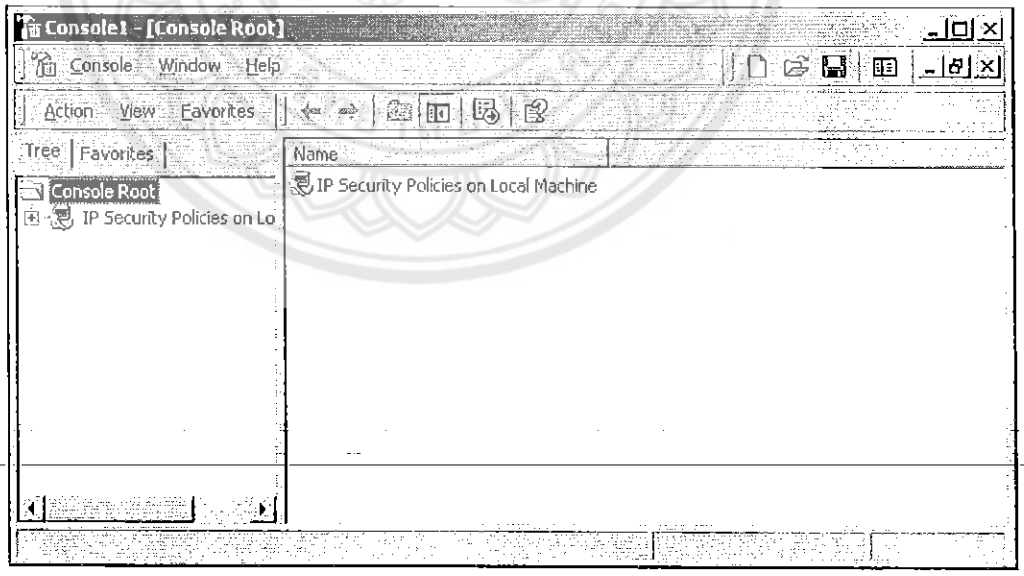


รูปที่ 4-80 Add Standalone Snap-in



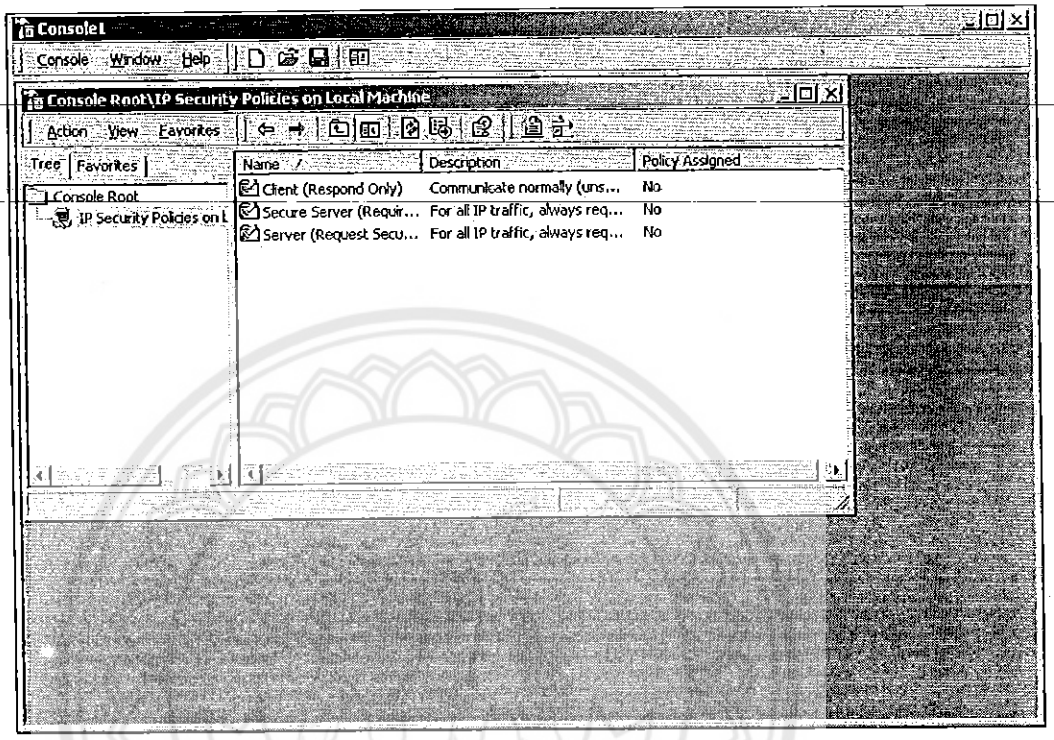
รูปที่ 4-81 ทำการเลือก Local computer

4. หลังจากขั้นตอนข้างต้นจะได้ผลดังนี้



รูปที่ 4-82 Console 1

5. คลิ้กไอคอน IP Secuirty Policies on Local Machine ทางด้านซ้าย แล้วด้านขวาจะแสดงกฎ (Windows จะเรียกว่า Policy) ของไฟร์วอลล์ โดยทั่วไปแล้ว windows จะให้กฎพื้นฐานมาสามชุด

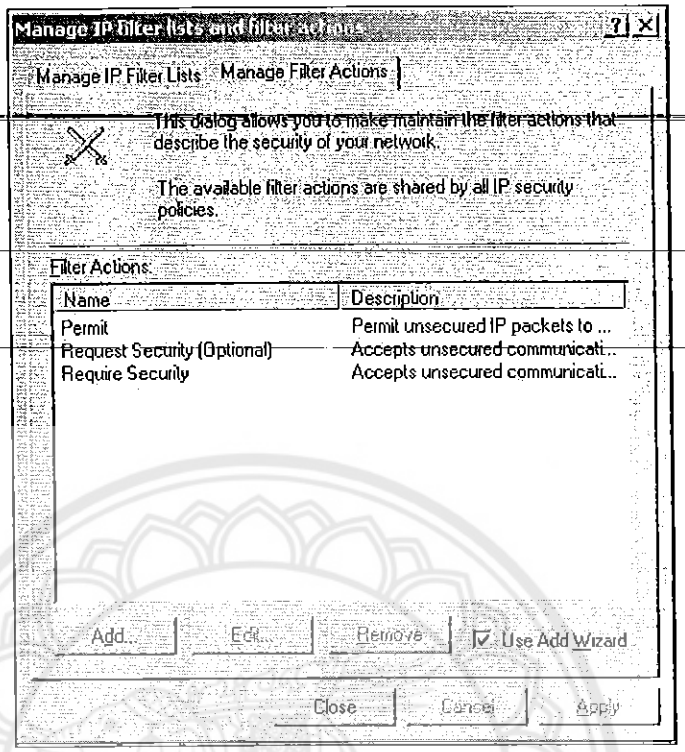


รูปที่ 4-83 ความสัมพันธ์ของกฎ 3 ชุด

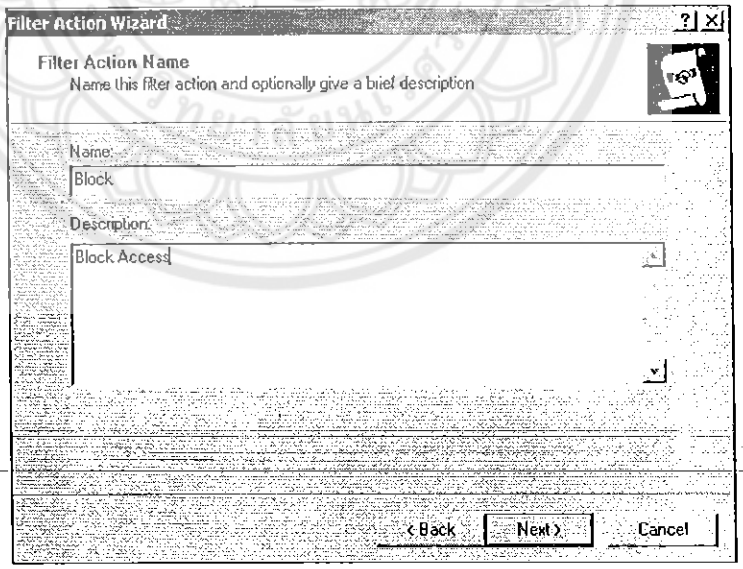
4.7.8.3 การเพิ่ม Block action ให้กับ Firewall

ในระบบไฟร์วอลล์ของ IP -Security มีรูปแบบ action ที่จะอนุญาต หรือ ยกเลิกแพ็จเกจ ตามกฎของไฟร์วอลล์ แต่ใน windows ไม่มี action ของการยกเลิก (Block) เป็นค่าปริยาย ดังนั้นจึงต้องมีการเพิ่มส่วนนี้เข้าไปเพื่อสะดวกต่อการสร้างกฎของไฟร์วอลล์ โดยมีขั้นตอนดังนี้

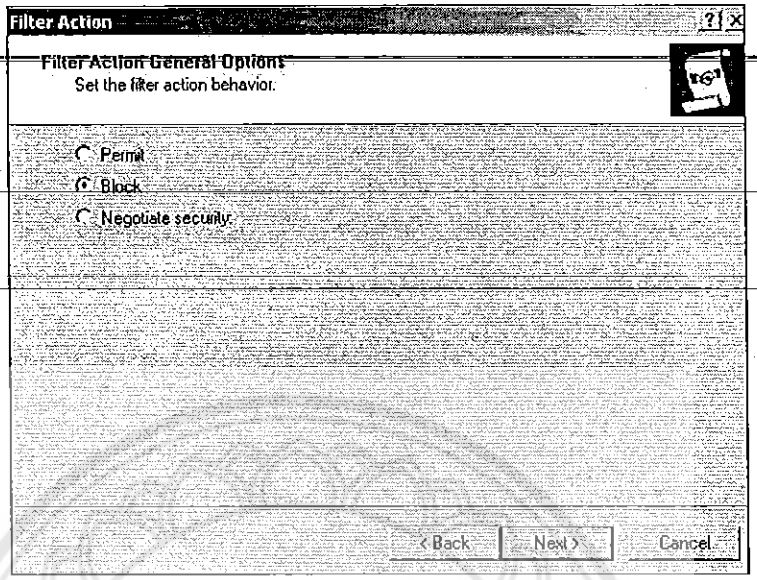
1. คลิ้กขวาไอคอน IP Secuirty Policies on Local Machine ทางด้านซ้าย -> เลือก Manage IP Filter Lists and Filter Actions -> เลือกแท็ป Manage Filter Actions -> กดปุ่ม Add แล้วจะเข้ามายัง Filter Action Wizard-> กดปุ่ม Next -> ใส่ชื่อเป็น "Block" และคำอธิบายเป็น "Block Access" -> กดปุ่ม Next -> เลือก radio-button เป็น"Block" -> Next : ไฟร์วอลล์ในบทความนี้เป็นแบบธรรมดา ดังนั้นไม่ต้องสนใจ option อื่น ๆ กด Next จนกว่าจะพบปุ่ม Finish แล้วจึงกดปุ่ม Finish



รูปที่ 4-84 Manage IP Filter Lists and Filter Actions



รูปที่ 4-85 Filter Action Wizard

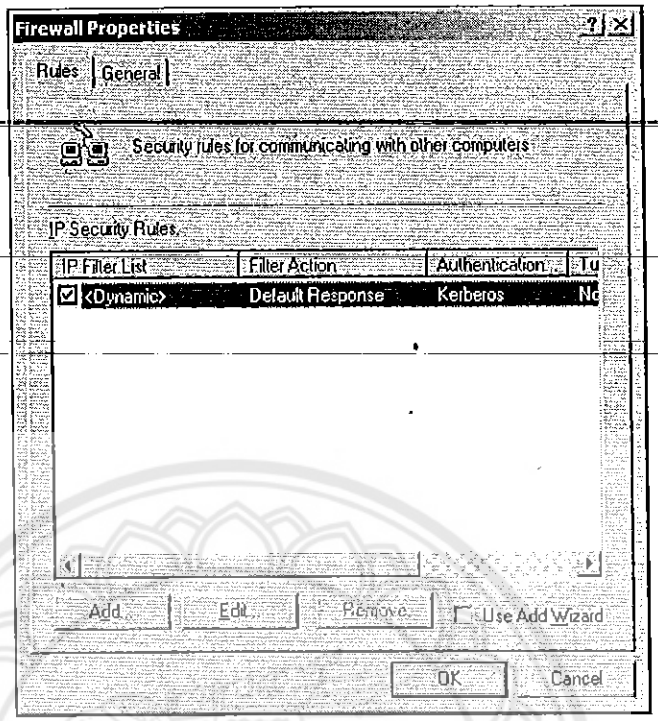


รูปที่ 4-86 Filter Action

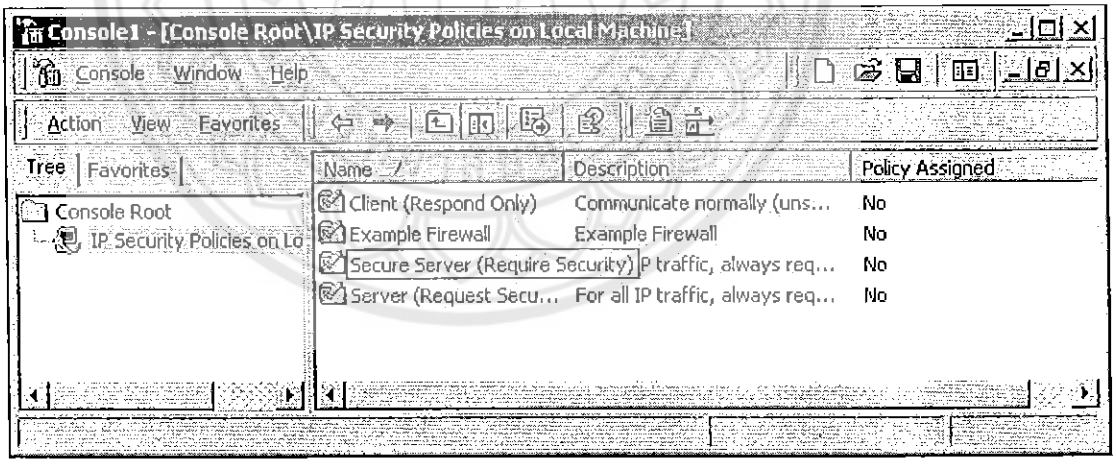
4.7.8.4 ออกแบบกฎของไฟร์วอลล์

คลิ้กขวาไอคอน IP Sccuirty Policies on Local Machine ทางด้านซ้าย -> เลือก Create IP Security Policy -> กดปุ่ม Next -> ใส่ชื่อ เป็น "Example Firewall" คำอธิบายคือ "Example Firewall" -> กดปุ่ม Next จนกว่าจะพบปุ่ม Finish แล้วจึงกดปุ่ม Finish เนื่องจากค่าปริยายที่ให้มามีความเหมาะสมกับการตั้งค่า firewall อยู่แล้ว

หมายเหตุ :หากเครื่องที่ติดตั้ง firewall เป็นเครื่องที่ไม่เกี่ยวข้องกับโดเมนใดๆ เลย โปรแกรมจะแจ้งเตือนให้กดปุ่ม Yes ได้ทันที



รูปที่ 4-87 Firewall Properties



รูปที่ 4-88 Console Root\IP Security Policies on local Machine

4.7.8.5 การเพิ่ม Filter packet ให้กับไฟร์วอลล์

หลังจากการสร้างกฎของไฟร์วอลล์ จำเป็นต้องเพิ่มส่วนของ Filter Action ให้กับไฟร์วอลล์เพื่อสร้างกฎในการอนุญาตหรือ ยกเลิกแพ็กเกจ ซึ่งในที่นี้จะยกสองตัวอย่างของการตั้งค่าไฟร์วอลล์ดังนี้คือ

1. ป้องกัน ICMP Denial of services : การบุกรุกแบบนี้เกิดขึ้นจากเครื่องได้รับแพ็กเกจแบบ ICMP มากจนทำให้เครื่องหยุดทำงาน ดังนั้นกฎของไฟร์วอลล์ต้องตั้งกฎที่ว่าจะไม่ยอมรับแพ็จเกจ แบบ ICMP การตั้งค่ามีขึ้นตอนดังนี้ จากข้อ C ในหน้าจอ Firewall Properties -> **ยกเลิกการใช้งาน Use Add Wizard** ->กดปุ่ม Add -> จะปรากฏรายชื่อของ Filter สองชุด คือ All IP Traffic และ All ICMP Traffic เลือก All ICMP Traffic -> กดแท็ป "Filter Action" -> เลือก Blocked -> กด OK -> กด Close สามารถทดสอบว่ากฎนี้ใช้งานได้จริงหรือไม่ โดยการทดสอบจากการ ping หากไม่มีการตอบกลับแสดงว่าไฟร์วอลล์นั้นใช้งานได้จริง

หมายเหตุ :

- การเรียกใช้งาน Firewall rule : ในหน้าจอ Console คลิ้กขวาที่ไอคอนของกฎที่ต้องการใช้ แล้วเลือก Assign
- เนื่องจาก windows 2000 ไม่สามารถแยกแยะ ICMP ในระดับลึก เช่น ICMP แบบ echo หรือ ICMP แบบ reply เป็นต้น ดังนั้นจาก ตัวอย่าง 1 จะพบปัญหาตรงที่เครื่องไม่สามารถ ping ออกสู่ภายนอกได้

2. กฎการเปิดพอร์ต 80: เช่นเดียวกับ การสร้างกฎในข้อ 1 โดยการเพิ่ม Filter rule ใหม่ให้กับไฟร์วอลล์ และสร้าง IP filter ใหม่โดยใช้กฎที่ว่า "ยอมรับแพ็จเกจ ทุกตัวที่มาจากภายนอก ที่มีพอร์ต 80" ซึ่งจะให้ชื่อ fiter นี้ว่า example

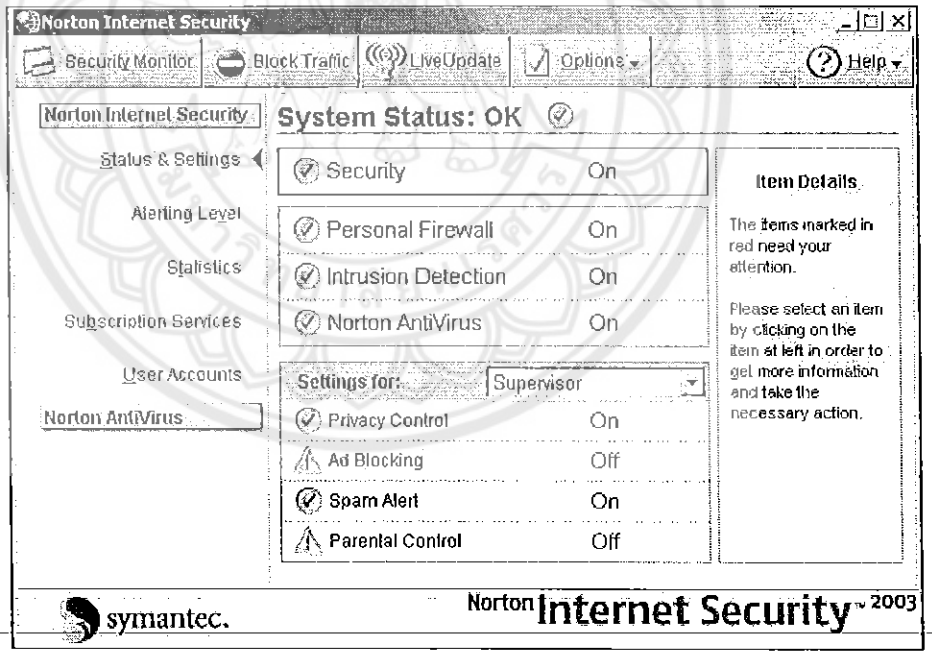
3. กฎการปิดพอร์ต NetBIOS : โดยปกติ Windows 2000 จะเปิดการใช้งานพอร์ต tcp139 เพื่อใช้ในการแชร์ไฟล์ต่างๆ หาก ผู้ใช้มิได้เปลี่ยนแปลงค่าปริยายหลังจากการติดตั้ง windows ระบบจะแชร์ไฟล์ทั้งหมดในเครื่อง เช่น Drive C ($C) เป็นต้น การแชร์ไฟล์โดยไม่มีการป้องกันโดยการใช้ password จะทำให้เครื่องเสี่ยงต่อการบุกรุกจากไวรัสได้ นอกจากนั้นในเครื่องคอมพิวเตอร์ส่วนตัวไม่ควรมีการเปิดใช้งานพอร์ตดังกล่าวโดยเด็ดขาด รูปแบบการตั้งค่าจะเหมือนกับในตัวอย่าง D.2 แต่กฎของ Filter จะต่างกันคือ ใน filter propertiers : source address = Any IP Address , Destination Address = My IP Address , Protocol = TCP , From any port ,To this port = 139 ตามลำดับ และต้องสร้าง Action เป็น Block

4.7.9 Norton Internet security

4.7.9.1 คุณลักษณะของ Norton Internet Security

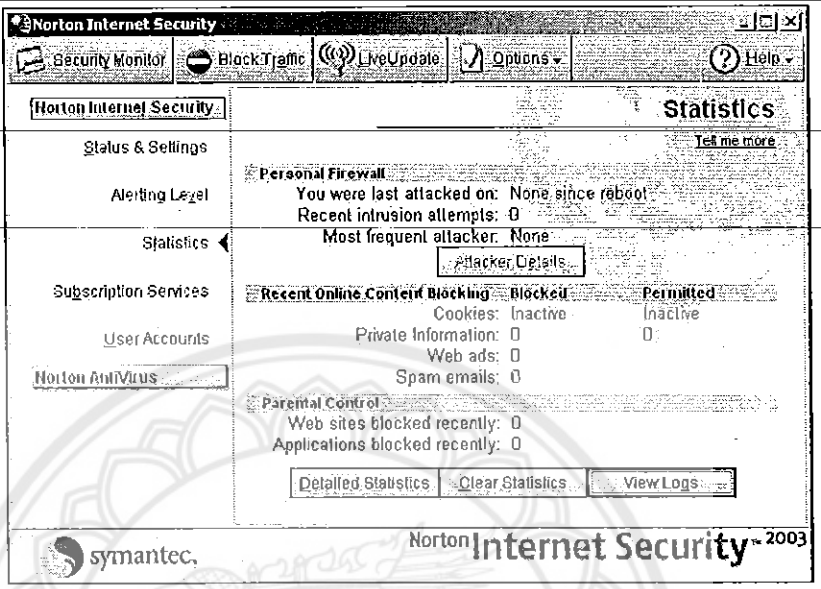
- ความต้องการของระบบ (System Requirement)
  - CPU จะต้องมีความเร็วขั้นต่ำเท่ากับ Pentium 150 MHz ขึ้นไป
  - หน่วยความจำขั้นต้ำ 64เมกะไบต์
  - ฮาร์ดดิสก์ไม่ต่ำกว่า 85เมกะไบต์
  - ระบบปฏิบัติการ Window 95B,98,98SE,ME,NT4.0,Window 2000,Window XP
  - บราวเซอร์เวอร์ชั่นต่ำสุด IE4.01 และ MiSE Service Pack 1

- Norton Internet Security มีหน้าจอคอนโซล แบ่งออกเป็น 2 ส่วน คือ
  - ส่วนที่เป็นเมนูของฟังก์ชั่นต่างๆที่ทีอยู่ใน NIS
  - ส่วนที่เป็นข้อมูลสถานะของ NIS ในปัจจุบันที่เกี่ยวข้องกับฟังก์ชันที่ผู้ใช้เลือก



รูปที่ 4-89 หน้าจอคอนโซลของ NIS

4.7.9.2 การคอนฟิกของ Norton Internet Security



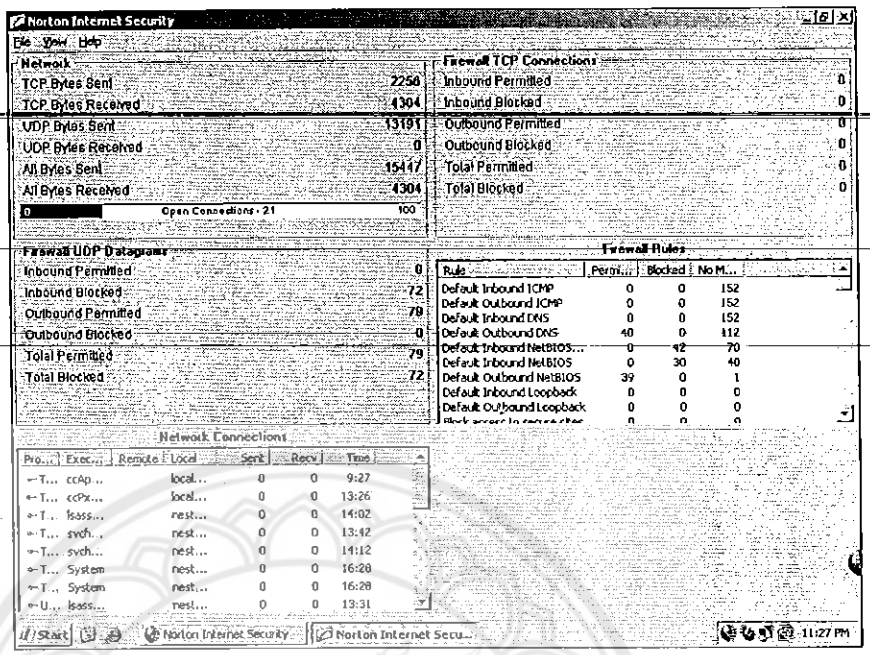
รูปที่ 4-90 หน้าจอแสดงสถานะของ เพอร์ซันแนลไฟร์วอลล์

Personal Firewall

You were last attacked on เวลาที่มีการ โจมตีมายังเครื่องคอมพิวเตอร์นี้ครั้งสุดท้าย

Resent intrusion attempts จำนวนความพยายามในการเจาะระบบเข้ามาครั้งล่าสุด

Most frequent attacker โฮสต์ที่พยายามเจาะระบบเข้ามาบ่อยที่สุด



รูปที่ 4-91 หน้าจอแสดงสถิติและสถานะของเน็ตเวิร์กโดยละเอียด

Network เป็นข้อมูลสรุปของปริมาณการรับ-ส่ง โดยจำแนกเป็นของโปรโตคอล UDP และ TCP เป็นข้อมูลรวมทั้งหมด

Firewall TCP Connections แสดงรายละเอียดการสื่อสารเฉพาะของ TCP โดยจะแสดงทั้งในส่วนของการสื่อสารทั้งที่ได้รับอนุญาติ (Permitted) และไม่ได้รับอนุญาติ (Blocked) ทั้งที่เป็นการสื่อสารเข้า (Inbound) และการสื่อสารขาออก (Outbound)

Firewall UDP Datagram แสดงสถิติเช่นเดียวกับของ TCP แต่เป็นโพรโตคอล UDP

Firewall Rules แสดงสถิติของการทำงานของไฟร์วอลล์ในการเปรียบเทียบลักษณะของทราฟฟิคกับแอคเซสรูลที่กำหนดไว้ในไฟร์วอลล์

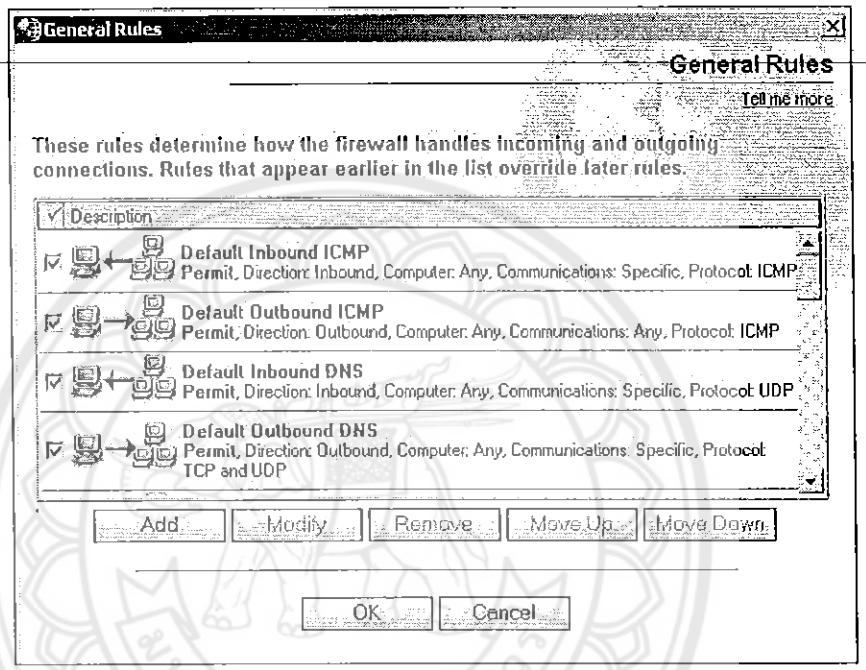
Network Connections แสดง **Connections** ในปัจจุบันซึ่งโปรแกรมที่ทำงานอยู่ภายในเครื่องของผู้ใช้เปิดไว้เพื่อใช้ในการสื่อสารกับผู้อื่น

4.7.9.3 การกำหนดแอคเซสรูล

แอคเซสรูลของ NIS แบ่งออกได้เป็น 2ส่วนและกำหนดไว้จุดเดียวกัน

Outbound access การควบคุมทราฟฟิคขาออก

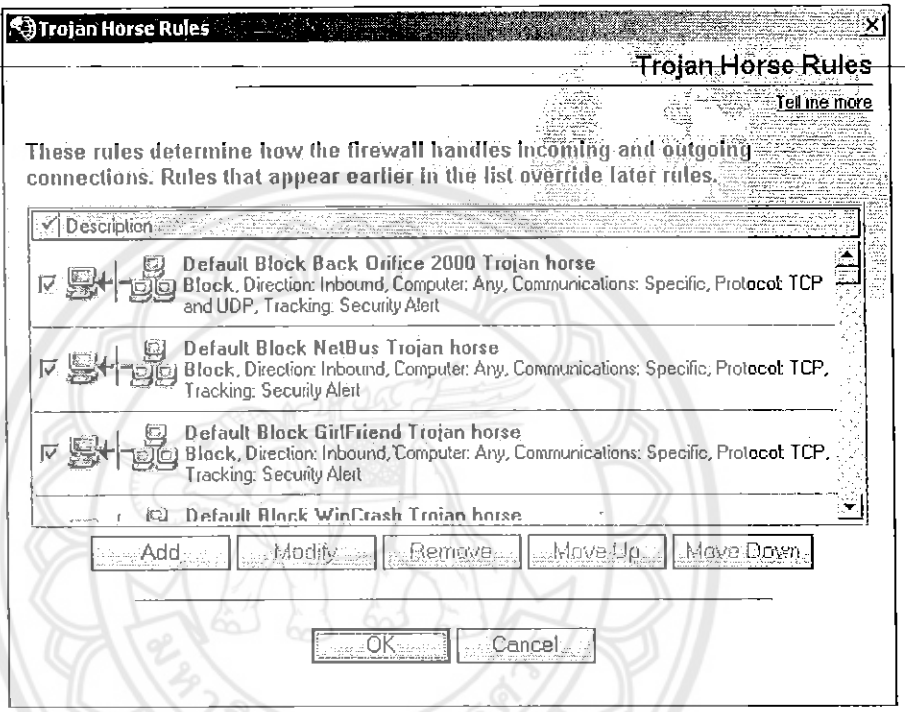
Inbound access การควบคุมทราฟฟิคขาเข้า



รูปที่ 4-92 เมนู System-wide Settings สำหรับกำหนดกฎ

4.7.9.4 การป้องกันโปรแกรมม้าโทรจัน

NIS ได้แยกส่วนของการกำหนดแอคเซสรูลสำหรับป้องกันโปรแกรมม้าโทรจันไว้แยกอีกเมนูหนึ่งซึ่งที่จริงแล้วนั้นก็เป็นอีกแอคเซสรูลของไฟร์วอลล์เหมือนกับการกำหนดใน System -Wide Setting



รูปที่ 4-93 รายละเอียดของ Trojan horse Settings

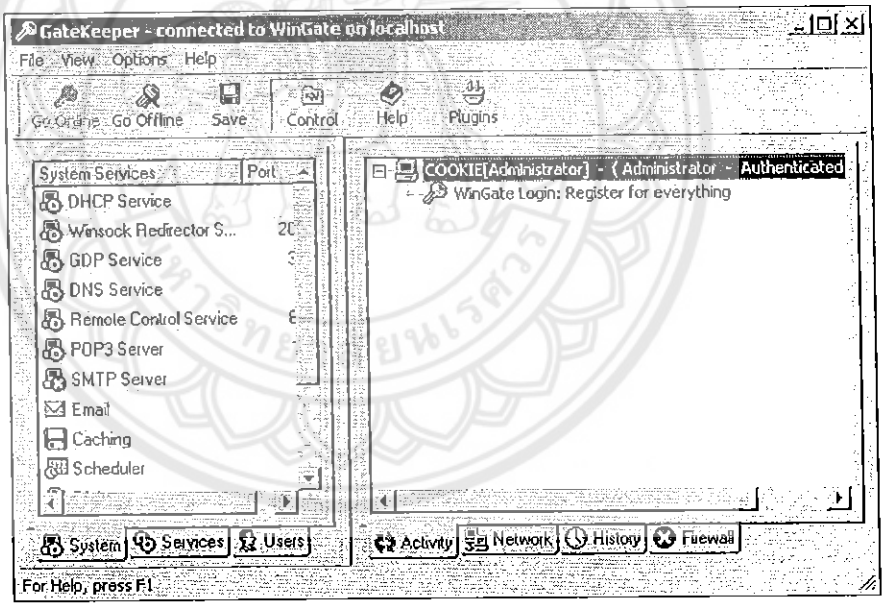
4.7.10 WinGate Server

1. คุณลักษณะของ WinGate

- เป็นโปรแกรมสำหรับการแชร์อินเตอร์เน็ต
- ไฟร์วอลล์
- NAT (Network Address Translator)
- สามารถจัดการจากทางไกลได้ (Remote Administration)
- มีการจัดเก็บลงล็อกไฟล์

2. WinGate มีส่วนหลักๆดังนี้

GateKeeper คือส่วนที่ติดต่อผู้ใช้สำหรับ WinGate ใช้รวมทุกการคำนวณบน Wingate รวมทั้งการจัดการค่าที่คอนฟิกกูเรชัน ไว้ซึ่งถูกออกแบบเข้าใจได้ง่ายมาก



รูปที่ 4-94 GateKeeper ของ WinGate

3.การคอนฟิกกูเรชัน Firewall ของ WinGate

Firewall Modes

- **Low: Allows servers to run behind firewall**

  ยอมให้Telnet, WWW, FTP, SMTP, NNTP, เครื่องแม่ข่าย POP3

  ยอมให้ TCP & UDP 1024 - 4096

  ยอมให้ TCP & UDP บนส่วนติดต่อภายใน

- **Medium: For games and Internet applications**

  ยอมให้ TCP & UDP 1024 - 4096

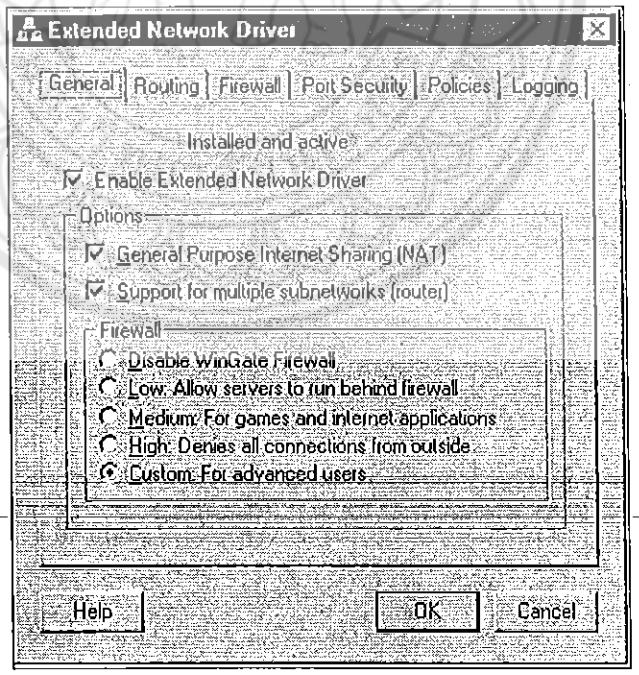
  ยอมให้ TCP & UDP บนส่วนติดต่อภายใน

- **High: Denies all connections from the outside**

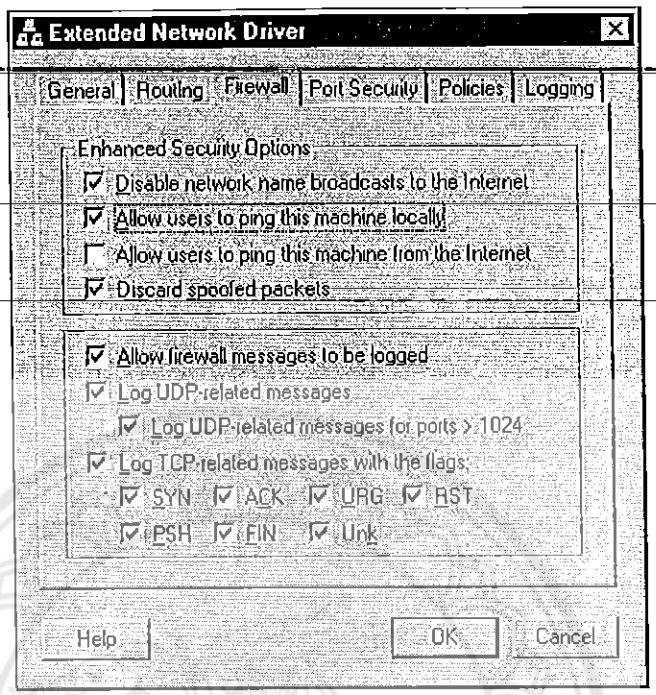
  ยอมให้ TCP & UDP บนส่วนติดต่อภายใน

- **Custom: For advanced users**

  การตั้งค่าความเคยชินใดๆที่เพิ่มจะประยุกต์ได้รวมทั้งการตั้งค่าของโหมดล่าสุดที่สิ่งนั่นถูกเลือก



รูปที่ 4-95 WinGate สนับสนุนเครือข่ายที่ขยาย



รูปที่ 4-96 การสนับสนุนเครือข่ายขยาย-ไฟร์วอลล์

4. ความต้องการของระบบ (Window Platform)

- ระบบปฏิบัติการ Microsoft 98, ME, Windows 2000, Xp
- RAM 64 เมกะไบต์
- โมเด็ม 56 K
- ฮาร์ดดิสก์ไม่ต่ำกว่า 60 เมกะไบต์

4.8 การทดสอบไฟร์วอลล์

เพอร์ซันนอลไฟร์วอลล์

4.8.1 การทดสอบเพอร์ซันนอลไฟร์วอลล์ Zone Alarm Pro

ระบบปฏิบัติการที่ทำการทดสอบ : วินโดว์2000 เซิร์ฟเวอร์

1. การโจมตีเพอร์ซันนอลไฟร์วอลล์ Zone Alarm Pro ด้วย DoS

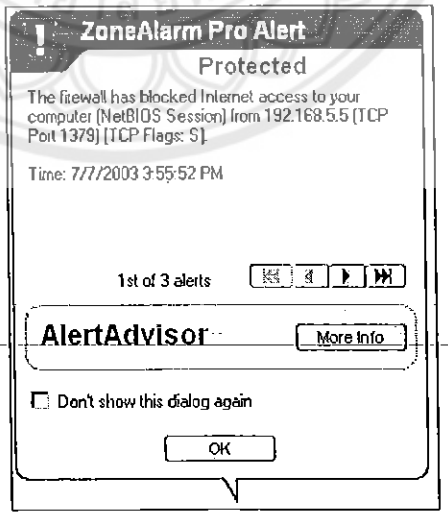
การป้องกันตัวของ Zone Alarm Pro จากการโจมตีด้วย DoS

จากการคอนฟิกให้ไฟล์วอลล์สำหรับโซนอินเตอร์เน็ตมีค่าเป็น med โปรแกรมจะทำการบล็อกพอร์ต NetBios ขาเข้า (135,137-139,445) เอาไว้โดยอัตโนมัติพร้อมกับตั้งค่าให้บล็อกพอร์ต TCP หมายเลข 10 เอาไว้แล้ว (หากเลือกค่าเป็น Low นั่นคือไฟร์วอลล์ไม่ทำงาน จะไม่มีการบล็อกพอร์ตใดๆ)

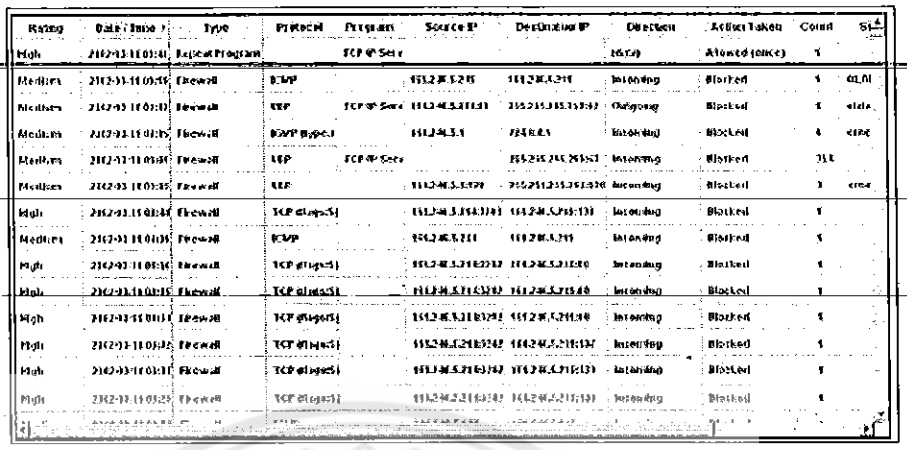
2. โจมตีด้วย killwin.c DoS ไฟล์นี้โดยดีฟอลท์จะโจมตีไปที่พอร์ต NetBios Session นั่นคือพอร์ต 139 ซึ่งระบบปฏิบัติการวินโดว์ทั่วไป จะเปิดพอร์ตนี้เอาไว้

ผลการโจมตี

- Zone Alarm ทำการบล็อกเอาไว้ได้ โดยจะแจ้งเตือนขึ้นมาดังรูปที่ 4-98 แล้วเก็บเป็นล็อกไว้ดังรูปที่ 4-99
- ไฟร์วอลล์โฮสต์ทำงานได้ตามปกติ



รูปที่ 4-97 แสดงการแจ้งเตือนของ ZoneAlarm



Rating	Date / Time	Type	Protocol	Program	Source IP	Destination IP	Direction	Action Taken	Count	St
High	2012-03-11 01:01:41	Rejected Program		TCP IP Serv			Incoming	Allowed (once)	1	
Medium	2012-03-11 01:01:39	Firewall	ICMP		[redacted]	[redacted]	Incoming	Blocked	1	01:01
Medium	2012-03-11 01:01:37	Firewall	UDP	TCP IP Serv	[redacted]	[redacted]	Outgoing	Blocked	1	01:01
Medium	2012-03-11 01:01:35	Firewall	ICMP Type=3		[redacted]	[redacted]	Incoming	Blocked	1	01:01
Medium	2012-03-11 01:01:33	Firewall	UDP	TCP IP Serv		[redacted]	Incoming	Blocked	318	
Medium	2012-03-11 01:01:31	Firewall	UDP		[redacted]	[redacted]	Incoming	Blocked	1	01:01
High	2012-03-11 01:01:29	Firewall	TCP flags=S		[redacted]	[redacted]	Incoming	Blocked	1	
Medium	2012-03-11 01:01:27	Firewall	ICMP		[redacted]	[redacted]	Incoming	Blocked	1	
High	2012-03-11 01:01:25	Firewall	TCP flags=S		[redacted]	[redacted]	Incoming	Blocked	1	
High	2012-03-11 01:01:23	Firewall	TCP flags=S		[redacted]	[redacted]	Incoming	Blocked	1	
High	2012-03-11 01:01:21	Firewall	TCP flags=S		[redacted]	[redacted]	Incoming	Blocked	1	
High	2012-03-11 01:01:19	Firewall	TCP flags=S		[redacted]	[redacted]	Incoming	Blocked	1	
High	2012-03-11 01:01:17	Firewall	TCP flags=S		[redacted]	[redacted]	Incoming	Blocked	1	
High	2012-03-11 01:01:15	Firewall	TCP flags=S		[redacted]	[redacted]	Incoming	Blocked	1	

รูปที่ 4-98 รายละเอียดการเก็บล็อกกิ้ง (Logging) ที่ได้แจ้งเตือนไว้

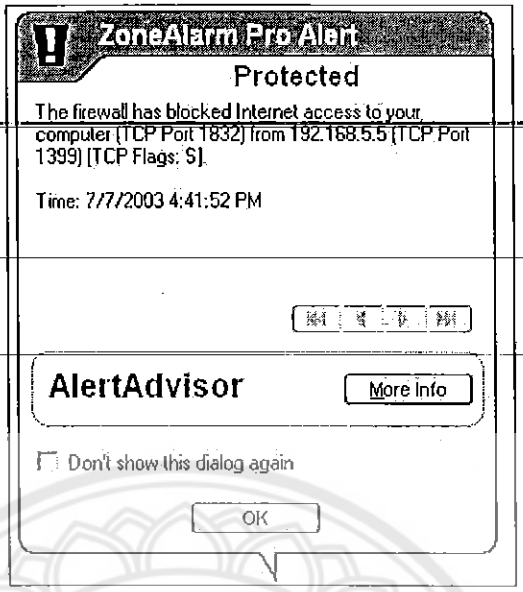
3. โจมตีด้วย synflood.c

จะสั่งให้โจมตีไปที่พอร์ต 10

ผลการโจมตี

- เครื่องไม่ตอบสนองใดๆ หยุดการทำงานไป จนกว่าจะหยุดโจมตี
- ถ้าพอร์ตที่ถูกโจมตีนั้นถูกสั่งบล็อกเอาไว้ก่อนหน้านี้แล้ว เมื่อการโจมตีหยุดลง

Zone Alarm จึงแจ้งเตือนขึ้นมาดัง รูปที่ 4-99 ว่ามีการโจมตีที่พอร์ตหมายเลข 139 แต่ถ้าไม่ได้บล็อกเอาไว้ก่อนจะไม่มีการแจ้งเตือนใดๆ



รูปที่ 4-99 แสดงการแจ้งเตือนของ Zone Alarm

4. การสแกนเพอร์ซันนอลไฟร์วอลล์ Zone Alarm

ทำการคอนฟิกให้เพอร์ซันนอลไฟร์วอลล์ Zone Alarmทำงานในโหมด Med หลังจากนั้นใช้ Nmap เพื่อสแกนพอร์ต ได้ผลลัพธ์ของการสแกตพอร์ตออกมาคือ

- Port 23, 80 ปิดอยู่
- Port อื่นๆ ที่เหลือถูกฟิลเตอร์
- Nmap ไม่สามารถตรวจหาระบบปฏิบัติการได้

4.8.2 การทดสอบ Tiny Personal Firewall

ระบบปฏิบัติการที่ทำการทดสอบ : วินโดว์2000

1. การโจมตี Tiny Personal Firewall ด้วย DoS

การป้องกันตัวของ Tiny Personal Firewall จากการโจมตีด้วย DoS

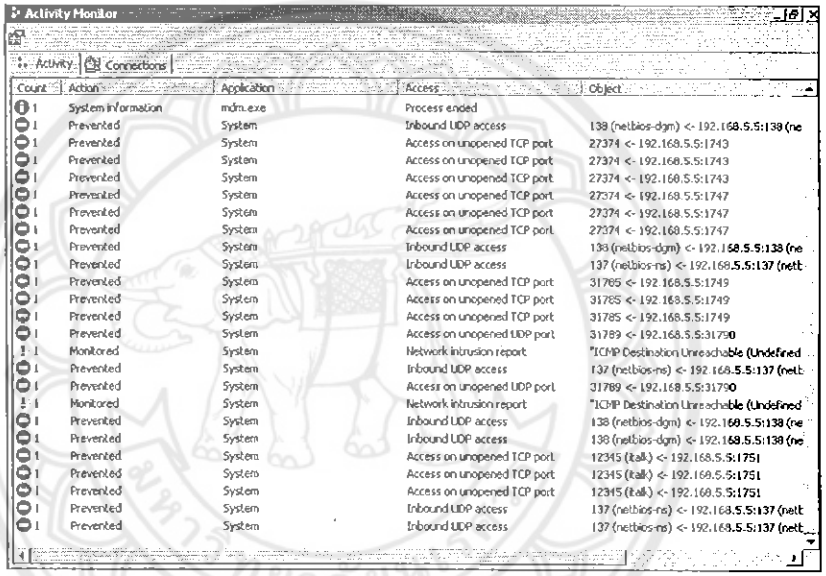
โดยดีฟอลต์ โปรแกรมจะทำการบล็อกพอร์ต NetBios ขาเข้า (135,137-139,445) เอาไว้โดยอัตโนมัติ หากเลือกให้ไฟร์วอลล์ทำงานอยู่ และไม่สามารถเปิดปิดพอร์ตเกี่ยวกับ NetBios เองได้ โดยเราจะเลือกโหมดการทำงานของไฟร์วอลล์ (เลือก Ask me first) คือให้แจ้ง และให้ผู้ใช้ตัดสินใจว่าจะปฏิเสธ (Deny) หรืออนุญาต (Permit) และทำการบล็อกพอร์ต TCP หมายเลข 10

2. โจมตีด้วย killwin.c

DoS ไฟล์นี้โดยดีฟอลท์จะโจมตีไปที่พอร์ต NetBios Session นั่นคือพอร์ต 139 ซึ่งระบบปฏิบัติการวินโดว์ทั่วไป จะเปิดพอร์ตนี้เอาไว้

ผลการโจมตี

- มีการแจ้งถามเช่นใน ดังรูป 4-100ให้ผู้ใช้ตัดสินใจ แต่ถึงแม้จะอนุญาตก็จะไม่เกิดผลเสียอะไร เนื่องจากแพ็กเก็ตที่มานั้นหมดอายุไปก่อนแล้ว
- ไฟร์วอลล์โฮสต์ทำงานได้ตามปกติ



รูปที่ 4-100 แสดงการแจ้งเตือน และถามความเห็นของผู้ใช้เมื่อถูกโจมตีที่พอร์ต137, 138

3. โจมตีด้วย Synflood.c

สั่งให้ทำการโจมตีไปที่พอร์ต TCP หมายเลข 10

ผลการโจมตี

- เครื่องไม่ตอบสนองใดๆ จนกว่าจะหยุดโจมตี
- แจ้งเตือนขึ้นทันทีที่เครื่องกลับมาทำงานอีกครั้ง แต่จะแจ้งเป็นพอร์ตหมายเลข 10 แทน
- ไม่ว่าพอร์ตที่ถูกโจมตีนั้น จะเปิดหรือปิดอยู่ ถ้า ไม่ได้รับการอนุญาตหรือบล็อกเอาไว้ในกฎการกรอง Tiny จะแจ้งเตือนทันทีที่กลับมาทำงานใหม่ได้อีกครั้ง

4. การสแกน Tiny Personal Firewall

ทำการคอนฟิกให้ Tiny Personal Firewall ทำงานในโหมด Ask Me First หลังจากนั้นใช้ Nmap เพื่อสแกนพอร์ต ได้ผลลัพธ์ของการสแกนพอร์ตออกมาคือ

- Port 139 เปิดอยู่
- Port 23, 80 ปิดอยู่
- Port อื่นๆ ที่เหลือถูกฟิลเตอร์
- Nmap สามารถตรวจหาระบบปฏิบัติการได้

4.8.3 ไฟร์วอลล์ในระบบปฏิบัติการ Windows 2000

1. การโจมตี ไฟร์วอลล์ในระบบปฏิบัติการ Windows 2000 ด้วย DoS

การป้องกันตัวของ ไฟร์วอลล์ในระบบปฏิบัติการ Windows 2000 จากการโจมตีด้วย DoS

โดยปกติ Windows 2000 จะเปิดการใช้งานพอร์ต tcp139 เพื่อใช้ในการแชร์ไฟล์ต่างๆ หากผู้ใช้มิได้เปลี่ยนแปลงค่าปริยายหลังจากการติดตั้ง windows ระบบจะแชร์ไฟล์ทั้งหมดในเครื่อง เช่น Drive C ($C) เป็นต้น การแชร์ไฟล์โดยไม่มีการป้องกันโดยการใช้ password จะทำให้เครื่องเสี่ยงต่อการบุกรุกจากไวรัสได้ นอกจากนั้นในเครื่องคอมพิวเตอร์ส่วนตัวไม่ควรมีการเปิดใช้งานพอร์ตดังกล่าวโดยเด็ดขาด

2. โจมตีด้วย killwin.c

DoS ไฟล์นี้โดยดีฟอลท์จะโจมตีไปที่พอร์ต NetBios Session นั่นคือพอร์ต 139 ซึ่งระบบปฏิบัติการวินโดว์ทั่วไป จะเปิดพอร์ตนี้เอาไว้

ผลการโจมตี

- ไม่เกิดผลเสียอะไรเนื่องจากแพ็กเก็ตที่มานั้นหมดอายุไปก่อนแล้ว
- ไฟร์วอลล์โฮสต์ทำงานได้ตามปกติ
- มีการแสดงผลการโจมตี ที่ Log viewer ของโปรแกรม

3. โจมตีด้วย Synflood.c

สั่งให้ทำการโจมตีไปที่พอร์ต TCP หมายเลข 10

ผลการโจมตี

- เครื่องไม่ตอบสนองใดๆ จนกว่าจะหยุดโจมตี
- ไม่มีแจ้งเตือนขึ้นเลย
- ไม่ว่าพอร์ตที่ถูกโจมตีนั้น จะเปิดหรือปิดอยู่ ก็ไม่เกิดอาการอะไรเกิดขึ้น

4. การสแกน ไฟร์วอลล์ในระบบปฏิบัติการ Windows 2000

ทำการคอนฟิกให้ ไฟร์วอลล์ ในระบบปฏิบัติการ Windows 2000 ทำงานในโหมด Firewall หลังจากนั้นใช้ Nmap เพื่อสแกนพอร์ต ได้ผลลัพธ์ของการสแกนพอร์ตออกมาคือ

- Port 135,139 เปิดอยู่
- Port 445, 8000 ปิดอยู่
- Port อื่นๆ ที่เหลือถูกฟิลเตอร์
- Nmap ไม่สามารถตรวจหาระบบปฏิบัติการได้

4.8.4 Norton Internet security 2003

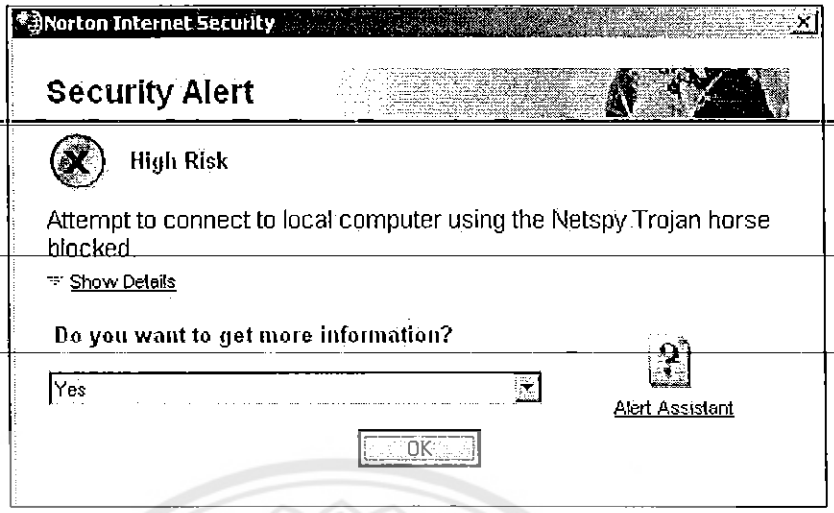
การโจมตี Norton Internet security 2003 ด้วย DoS

1. โจมตีด้วย killwin.c

DoS ไฟล์นี้โดยดีฟอลท์จะโจมตีไปที่พอร์ต NetBios Session นั่นคือพอร์ต 139 ซึ่งระบบปฏิบัติการวินโดว์ทั่วไป จะเปิดพอร์ตนี้เอาไว้

ผลการโจมตี

- มีการแจ้งถามเช่นใน ดังรูป 4-101 ให้ผู้ใช้ตัดสินใจ แต่ถึงแม้จะอนุญาตก็จะไม่เกิดผลเสียอะไร เนื่องจากแพ็กเก็ตที่มานั้นหมดอายุไปก่อนแล้ว
- ไฟร์วอลล์โฮสต์ทำงานได้ตามปกติ



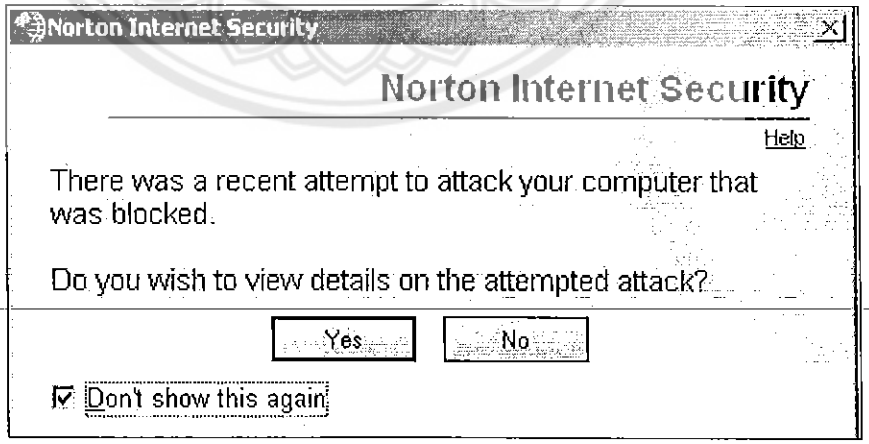
รูปที่ 4-101 Norton จะถามให้ไวรัสผ่านเข้าไปได้ไหม

3. โจมตีด้วย Synflood.c

สั่งให้ทำการโจมตีไปที่พอร์ต TCP หมายเลข 10

ผลการโจมตี

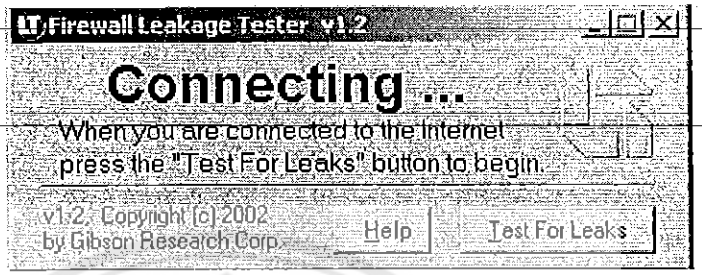
- เครื่องไม่ตอบสนองใดๆ จนกว่าจะหยุดโจมตี
- มีแจ้งเตือนขึ้นและไฟร์วอลล์ทำงานช้าลง



รูปที่ 4-102 มีการโจมตีเกิดขึ้น

4. การเจาะไฟร์วอลล์ Norton Internet security 2003

ทำการคอนฟิกให้ ไฟร์วอลล์ ใน Norton Internet security 2003ทำงานในโหมด Firewall หลังจากนั้นใช้ โปรแกรม LeakTest เพื่อเจาะระบบไฟร์วอลล์ ได้ผลลัพธ์คือ



รูปที่ 4-103 โปรแกรม LeakTest ขณะกำลังทดสอบการเชื่อมต่อ

รูปที่ 4-104 LeakTest สามารถเจาะผ่านไฟร์วอลล์ได้สำเร็จ

4.8.5สรุปผลการทดสอบผลิตภัณฑ์ไฟร์วอลล์ชนิดเพอร์ซันนอลไฟร์วอลล์

1. สรุปผลการโจมตีด้วย DoS

จากการทดลองโจมตีไฟร์วอลล์ทั้งสองตัวด้วย Killwin.c ปรากฏว่าไฟร์วอลล์ทั้งห้าตัวสามารถต้านทานได้ เนื่องจาก

- **สำหรับ Zone Alarm** นั้นได้มีการตั้งค่าเอาไว้ให้บล็อกพอร์ตเกี่ยวกับ NetBios ซึ่งหากไม่ตั้งค่าเช่นนี้ ไฟร์วอลล์โฮสต์ก็จะแครชทันทีเนื่องจากถูกโจมตีด้วย Killwin
- **สำหรับ Tiny Personal Firewall** นั้น บล็อกพอร์ตเกี่ยวกับNetBios เป็นดีฟอลต์โดยผู้ใช้ไม่สามารถปรับเปลี่ยนได้เลย
- สำหรับ ไฟร์วอลล์ในระบบปฏิบัติการ **Windows 2000**นั้น บล็อกพอร์ตเกี่ยวกับNetBios เป็นดีฟอลต์โดยผู้ใช้ไม่สามารถปรับเปลี่ยนได้
- สำหรับ **Norton Internet security 2003**นั้น บล็อกพอร์ตเกี่ยวกับ NetBios เป็นดีฟอลต์โดยผู้ใช้สามารถปรับเปลี่ยนได้โดยการกำหนดเอง
- สำหรับ **IPTABLE Linux** นั้น บล็อกพอร์ตเกี่ยวกับ NetBios เป็นดีฟอลต์โดยผู้ใช้ไม่สามารถปรับเปลี่ยนได้

ส่วนผลจากการโจมตีด้วย Synflood.c นั้นผลิตภัณฑ์ไม่สามารถต้านทานได้ทั้งหมด และมีลักษณะที่เหมือนกัน จึงไม่นำมาเป็นนัยสำคัญในการตัดสินใจ

	Zone Alarm	TINY	Win 2000	Norton	IPTABLE
Killwin.c	A	A	A	A	A
Synflood.c	B	C	C	B	C

ตารางที่ 4-9 สรุปการโจมตี DoS ไปยังเพอร์ซันนอลไฟร์วอลล์

A: ปกติ

B: ตอบสนองช้ามากๆ

C: หยุดทำงานไม่ตอบสนองใดๆ

หมายเหตุ จากตาราง การทดลองได้ทำการคอนฟิกกูเรชันให้บล็อกพอร์ต TCP หมายเลข 10 และ 139 และโจมตี killwin และ Synflood ไปยังพอร์ต 139 และ 10 ตามลำดับ

2. สรุปผลการโจมตีด้วยการสแกนพอร์ต

จากการทดลองในการสแกนพอร์ตโฮสต์ที่ทำการติดตั้งเพอร์ซันนอลไฟร์วอลล์ โดยใช้ Nmap และ Leak Test จะทำการสรุปผลการทดลองดังนี้ ทั้งเพอร์ซันนอลไฟร์วอลล์ ให้ผลการสแกนพอร์ตที่ไม่ตรงกับความเป็นจริงโดยสิ้นเชิง กล่าวคือ

- สำหรับ ZoneAlarm

พอร์ต 23, 80 ที่เปิดอยู่, Nmap ตรวจสอบพบว่าพอร์ตนี้ปิด

ส่วนพอร์ตอื่นๆ ที่เหลือ, Nmap ตรวจสอบพบว่าพอร์ตถูกฟิลเตอร์ (ไม่รู้ว่าเปิดหรือปิด)

- สำหรับ Tiny Personal Firewall

พอร์ต 23, 80 ที่เปิดอยู่, Nmap ตรวจสอบพบว่าพอร์ตนี้ปิด

พอร์ต 139 ที่ deny ไว้, Nmap ตรวจสอบพบว่าพอร์ตนี้เปิด

ส่วนพอร์ตอื่นๆ ที่เหลือ, Nmap ตรวจสอบพบว่าพอร์ตถูกฟิลเตอร์

-สำหรับ ไฟร์วอลล์ในระบบปฏิบัติการ Windows 2000

พอร์ต 135,139 เปิดอยู่

พอร์ต 445, 8000 ปิดอยู่

พอร์ต อื่นๆ ที่เหลือถูกฟิลเตอร์

ส่วนพอร์ตอื่นๆ ที่เหลือ, Nmap ตรวจสอบพบว่าพอร์ตถูกฟิลเตอร์

-สำหรับ Norton และ Linux

ใช้โปรแกรม Leak Test เจาะระบบออกมาจากไฟร์วอลล์ โดยทำงานคล้าย Black office

ผลปรากฏว่า Leak Test สามารถเจาะได้ทั้ง Norton และ IPTABLE

ส่วนการตรวจจับระบบปฏิบัติการพบว่า

- **ZoneAlarm** สามารถปิดบังระบบปฏิบัติการได้
- **Tiny Personal Firewall** ไม่สามารถปิดบังระบบปฏิบัติการได้
- **-สำหรับ ไฟร์วอลล์ในระบบปฏิบัติการ Windows 2000** ไม่สามารถปิดบังระบบปฏิบัติการได้
- **-สำหรับ Norton** สามารถปิดบังระบบปฏิบัติการได้
- **-IPTABLE** ไม่สามารถปิดบังระบบปฏิบัติการได้

เพราะฉะนั้นโดยภาพรวมแล้ว การปิดบังร่องรอยของโฮสต์ที่ทำการติดตั้งเพอร์ซันนอลไฟร์วอลล์ Zone Alarm และ Norton ได้ผลลัพธ์เป็นที่น่าพอใจกว่าโฮสต์ที่ทำการติดตั้ง Tiny Personal Firewall, Window2000, IPTABLE เนื่องจากผลลัพธ์ของการสแกนพอร์ตพบว่าไฟร์วอลล์ทั้งหมดทำให้

ผลการสแกนพอร์ตไม่ตรงกับความเป็นจริงโดยสิ้นเชิง แต่สำหรับการตรวจจับระบบปฏิบัติการพบว่า Zone Alarm และ Norton สามารถปิดบังระบบปฏิบัติการได้ แต่ Tiny Personal Firewall, Window2000, IPTABLE ทำไม่ได้

เอนเตอร์ไพรส์ไฟร์วอลล์

4.8.6 การทดสอบไฟร์วอลล์ WatchGuard

ระบบปฏิบัติการที่ทำการทดสอบไฟร์วอลล์โฮสต์: วินโดว์ NT

ระบบปฏิบัติการที่ทำการทดสอบโฮสต์หลังไฟร์วอลล์: วินโดว์2000 เซิร์ฟเวอร์

1. การโจมตี WatchGuard ด้วย DoS

โจมตี killwin.c

- กรณีทดสอบโฮสต์หลังไฟร์วอลล์โจมตีไปที่พอร์ต 80 (เปิดพอร์ต 80 สำหรับโปรโตคอล http ที่โฮสต์หลังไฟร์วอลล์)

ผลการโจมตี

- โฮสต์หลังไฟร์วอลล์ และไฟร์วอลล์โฮสต์ ทำงานตามปกติ
- มีการแจ้งเตือนการบุกรุกเครื่องไฟร์วอลล์ที่พอร์ต 80
- แม้จะโจมตีที่พอร์ตอื่นๆ ที่ไม่ได้อนุญาต ก็ยังคงทำงานปกติ

กรณีทดสอบไฟร์วอลล์โฮสต์

โจมตีไปที่พอร์ต 139

ผลการโจมตี

- ไฟร์วอลล์โฮสต์ทำงานตามปกติ
- มีการแจ้งเตือนการบุกรุกเครื่องไฟร์วอลล์ที่พอร์ต 139

2. โจมตี synflood.c

- **กรณีทดสอบโฮสต์หลังไฟร์วอลล์**

  โจมตีไปที่พอร์ต 80 (เปิดพอร์ต 80 สำหรับโปรโตคอล http ที่โฮสต์หลังไฟร์วอลล์)

ผลการโจมตี

- ไฟร์วอลล์โฮสต์ทำงานตามปกติ
- มีการแจ้งเตือนการบุกรุกเครื่องไฟร์วอลล์ที่พอร์ต 80

- กรณีทดสอบไฟร์วอลล์โฮสต์

  โจมตีไปที่พอร์ต 80

ผลการโจมตี

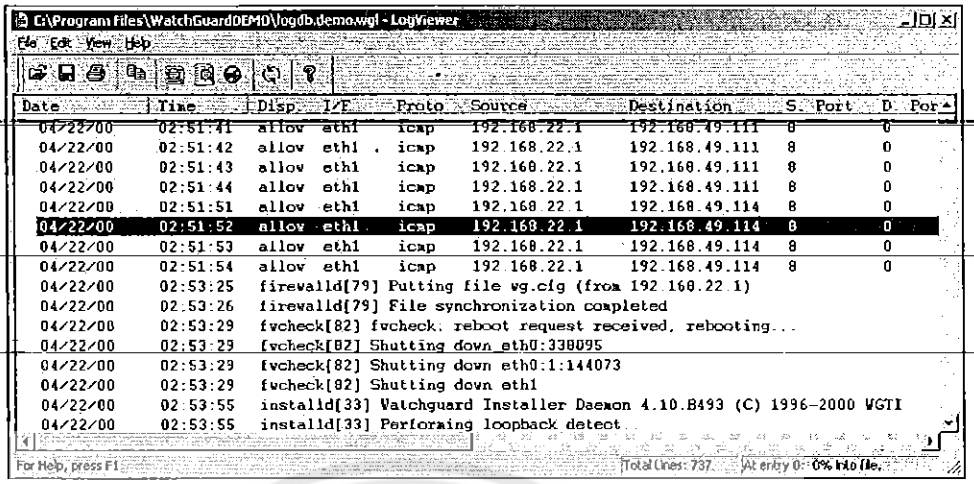
- ไฟร์วอลล์โฮสต์ทำงานตามปกติ
- มีการแจ้งเตือนการบุกรุกเครื่องไฟร์วอลล์ที่พอร์ต 80 หลังจากกลับมาทำงานอีกครั้ง
- ไม่ว่าจะโจมตีไปที่พอร์ตใดๆ ก็หยุดไม่ทำงานแม้จะไม่อนุญาตให้ใครเข้าถึงเครื่องไฟร์วอลล์ได้เลย

การสแกน WatchGuard

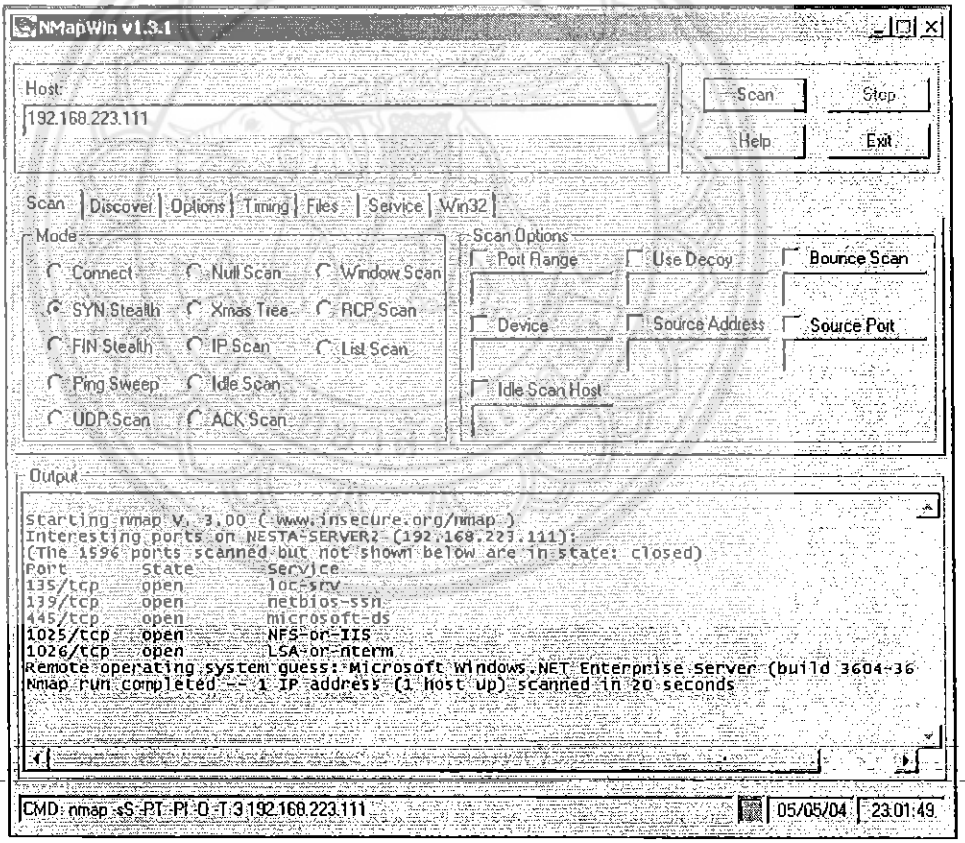
3. ใช้ Nmap เพื่อสแกนพอร์ตโฮสต์ที่ติดตั้ง WatchGuard

ได้ผลลัพธ์ของการสแกนพอร์ตออกมาคือ

- Port 135,139 เปิดอยู่
- Port 445, 1025 เปิดอยู่
- Port อื่นๆ ที่เหลือถูกฟิลเตอร์
- Nmap สามารถตรวจหาระบบปฏิบัติการได้



รูปที่ 4-105 Logviewer ของ WatchGuard



รูปที่ 4-106 การสแกน WatchGuard ด้วย Nmap

4.8.7 การทดสอบ Internet Security and Acceleration, ISA Server

1. การโจมตี ISA Server ด้วย DoS

โจมตี killwin.c

- กรณีทดสอบโฮสต์หลังไฟร์วอลล์โจมตีไปที่พอร์ต 80 (เปิดพอร์ต 80 สำหรับโปรโตคอล http ที่โฮสต์หลังไฟร์วอลล์)

ผลการโจมตี

- โฮสต์หลังไฟร์วอลล์ และไฟร์วอลล์โฮสต์ ทำงานตามปกติ
- มีการแจ้งเตือนการบุกรุกเครื่องไฟร์วอลล์ที่พอร์ต 80 ที่ ISA Management
- แม้จะโจมตีที่พอร์ตอื่นๆ ที่ไม่ได้อนุญาต ก็ยังคงทำงานปกติ

กรณีทดสอบไฟร์วอลล์โฮสต์

โจมตีไปที่พอร์ต 139

ผลการโจมตี

- ไฟร์วอลล์โฮสต์ทำงานตามปกติ
- มีการแจ้งเตือนการบุกรุกเครื่องไฟร์วอลล์ที่พอร์ต 139 ที่ ISA Management
- แม้จะโจมตีที่พอร์ตอื่นๆ ที่ไม่ได้อนุญาต ก็ยังคงทำงานปกติแต่จะทำงานช้ามากๆ

2. โจมตี synflood.c

- กรณีทดสอบโฮสต์หลังไฟร์วอลล์

  โจมตีไปที่พอร์ต 80 (เปิดพอร์ต 80 สำหรับโปรโตคอล http ที่โฮสต์หลังไฟร์วอลล์)

ผลการโจมตี

- ไฟร์วอลล์โฮสต์ทำงานตามปกติแจ่จะทำงานช้าลง
- มีการแจ้งเตือนการบุกรุกเครื่องไฟร์วอลล์ที่พอร์ต 139 ที่ ISA Management
- ถ้าโจมตีไปพอร์ตที่ไม่ได้อนุญาตไว้ โฮสต์หลังไฟร์วอลล์จะปลอดภัย

- กรณีทดสอบไฟร์วอลล์โฮสต์

  โจมตีไปที่พอร์ต 80

ผลการโจมตี

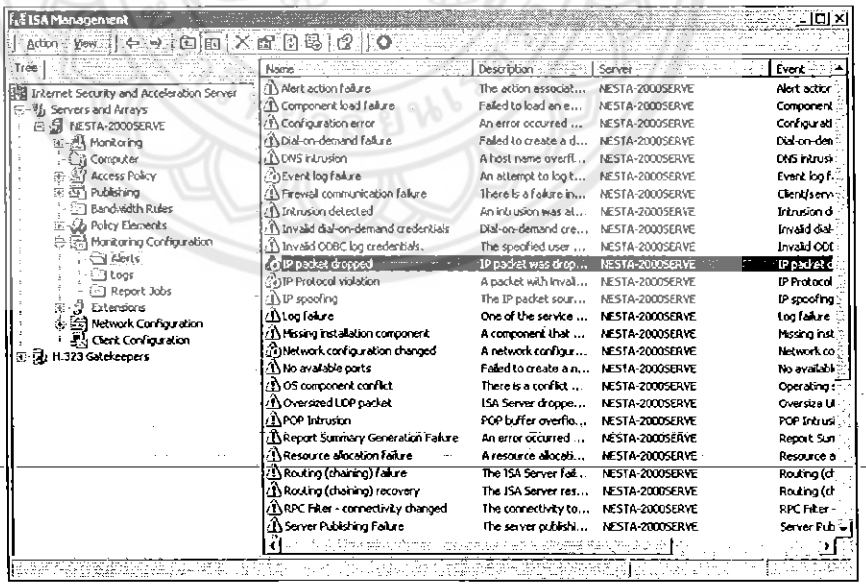
- ไฟร์วอลล์โฮสต์ทำงานตามปกติ
- มีการแจ้งเตือนการบุกรุกเครื่องไฟร์วอลล์ที่พอร์ต 80 หลังจากกลับมาทำงานอีกครั้ง
- ไม่ว่าจะโจมตีไปที่พอร์ตใดๆ ก็ไม่หยุดทำงาน แม้จะไม่อนุญาตให้ใครเข้าถึงเครื่องไฟร์วอลล์ได้เลยและทำงานช้า

3. การสแกน ISA Server

ใช้ Nmap เพื่อสแกนพอร์ตโฮสต์ที่ติดตั้ง ISA Server

ได้ผลลัพธ์ของการสแกนพอร์ตออกมาคือ

- Port 135,139 เปิดอยู่
- Port 445, 1025 เปิดอยู่
- Port อื่นๆ ที่เหลือถูกฟิลเตอร์
- Nmap สามารถตรวจหาระบบปฏิบัติการได้



รูปที่ 4-107 ความสัมพันธ์การเตือนของ ISA เป็น Log Viewer

4.8.8 การทดสอบ Wingate

ระบบปฏิบัติการที่ทำการทดสอบ : วินโดว์ 2000 เซิร์ฟเวอร์

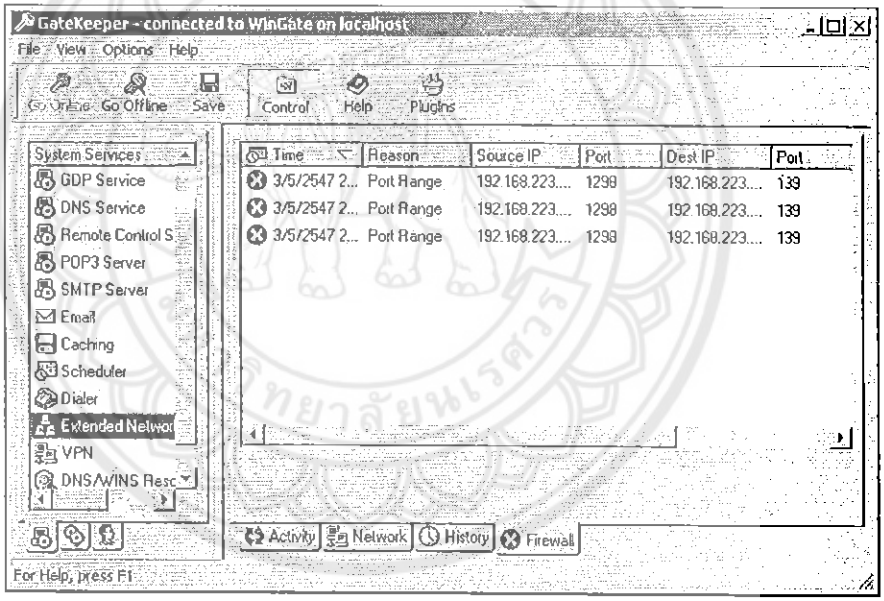
1. การโจมตี Wingate ด้วย Dos

โจมตีด้วย killwin.c

โจมตีไปที่พอร์ต 139

ผลการโจมตี

- ถ้าบล็อกพอร์ต 139 เอาไว้แล้ว (หรือไม่ได้อนุญาตพอร์ตนี้) จะเครื่องจะทำงานปกติ พร้อมแจ้งเตือนดังรูปที่ 4-108
- ถ้าอนุญาตพอร์ต 139 เอาไว้ เมื่อถูกโจมตี เครื่องจะตอบสนองช้ามาก จนต้องบูตใหม่



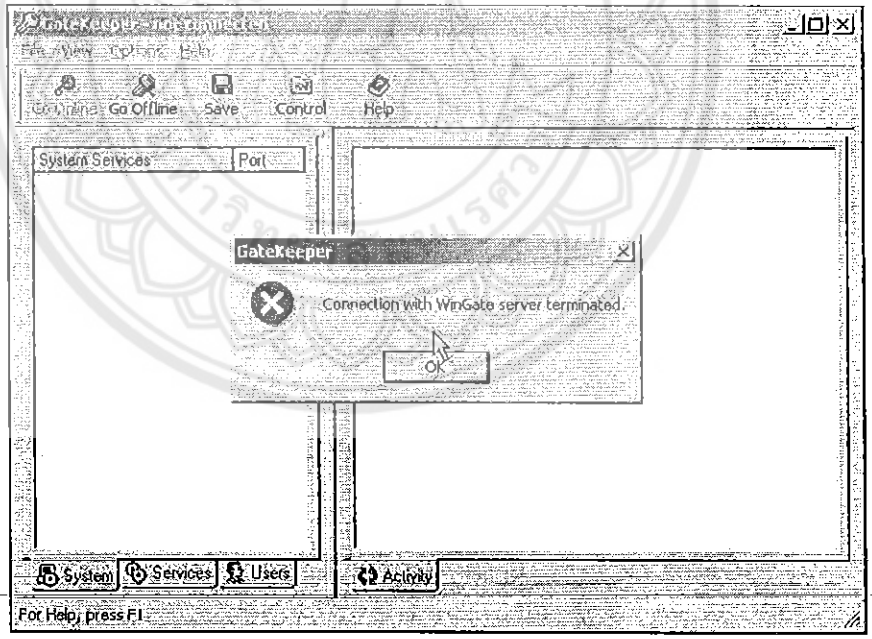
รูปที่ 4-108 การแจ้งเตือนการโจมตีที่พอร์ต 139 ของ Wingate

2. โจมตีด้วย synflood.c

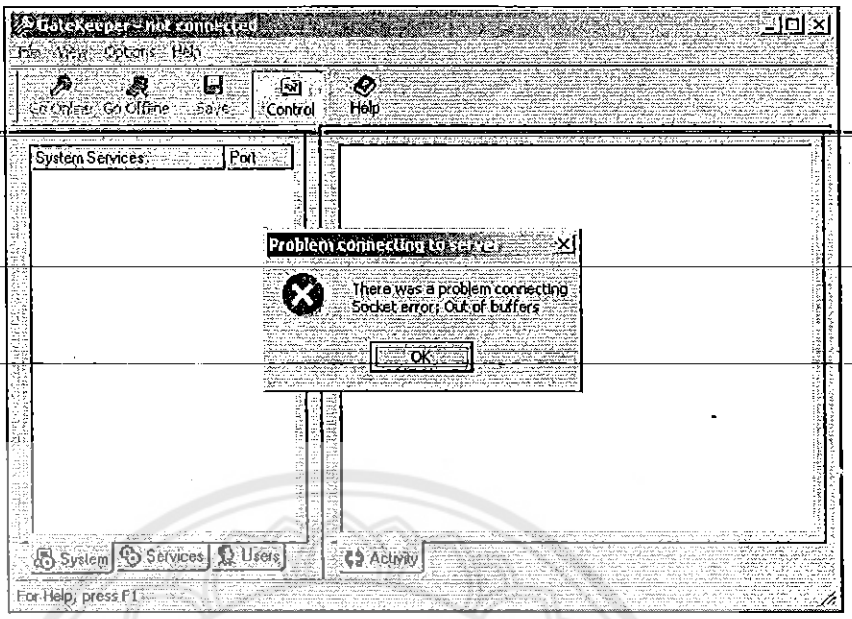
โจมตีไปที่พอร์ต 10

ผลการโจมตี

- ถ้าอนุญาตพอร์ต 10 เอาไว้ เมื่อถูกโจมตี เครื่องจะไม่ตอบสนองใดๆ หยุดทำงาน
- ถ้าบล็อกพอร์ต 10 เอาไว้ (หรือไม่ได้อนุญาต) เครื่องจะเป็นปกติ ก็ต่อเมื่อปริมาณแพ็กเก็ตที่ยิงมามีไม่มากนัก (ไม่เกิน 1 แสนแพ็กเก็ต) หากปริมาณแพ็กเก็ตที่ยิงมามีจำนวนมากๆ จะทำให้ WinGate ซึ่งจะทำการแจ้งเตือนสำหรับทุกๆ แพ็กเก็ตที่เข้ามานั้นทำงานหนักจนดึงซีพียูมาใช้งาน 100 % เครื่องจะตอบสนองช้ามากๆ จนต้องปิดWinGate ทิ้งไป หรือWinGate ปิดตัวเองไป ดังรูปที่ 4-109 และเมื่อเปิดขึ้นมาใหม่ก็ยังเกิดปัญหาบัฟเฟอร์เต็ม ไม่สามารถเข้า WinGate ได้ ดังรูปที่ 4-110 อีกทั้งขณะที่ WinGate กำลังแจ้งเตือนมากเกินไป (Over Alert) อยู่นั้น จะไม่ป้องกันพอร์ตที่บล็อกเอาไว้
- แม้ว่า WinGate จะมีปัญหาปิดตัวเองไป แต่ยังคงรักษาค่าเซอร์วิสหรือพอร์ตต่างๆ ที่ตั้งเอาไว้ได้



รูปที่ 4-109 WinGate ปิดตัวเองเนื่องจากเตือนมากเกินไป เพราะการโจมตีด้วย synflood

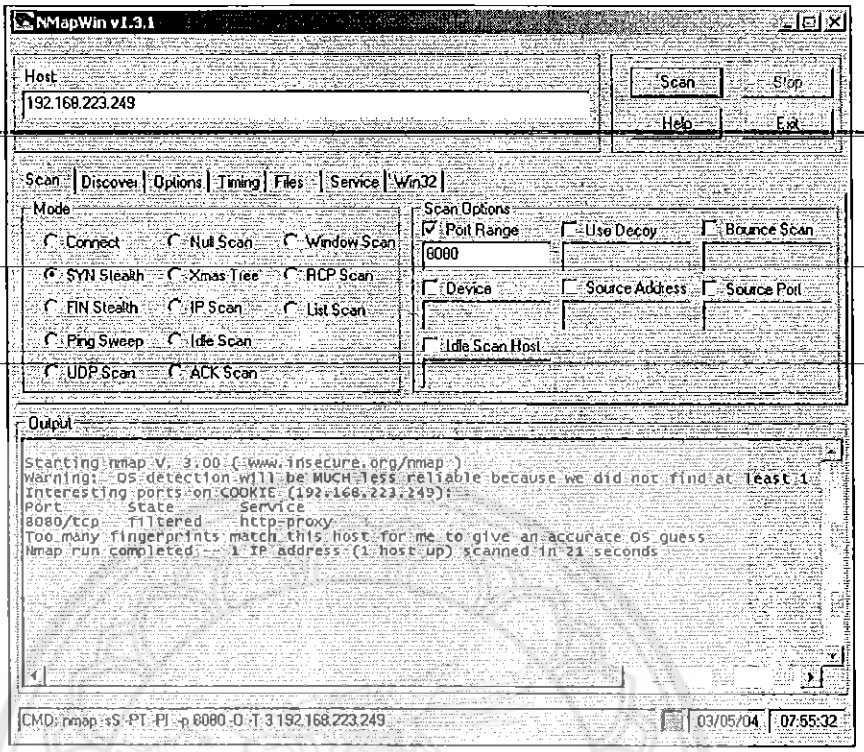


รูปที่ 4-110 WinGate ไม่สามารถเปิดขึ้นใหม่ได้ เนื่องจากบัฟเฟอร์เต็ม

3. การสแกน WinGate

ใช้ Nmapเพื่อสแกนพอร์ตโฮสต์ที่ติดตั้ง WinGate ได้ผลลัพธ์ของการสแกนพอร์ตออกมาคือ

- Port 80 เปิดอยู่
- Port อื่นๆ ที่เหลือถูกฟิลเตอร์
- Nmap ไม่สามารถตรวจหาระบบปฏิบัติการได้



รูปที่ 4-111 Nmapเพื่อสแกนพอร์ตโฮสต์ที่ติดตั้ง WinGate

4.8.9 Firewalling with FreeBSD 4.8 และ IP Table Linux

1. การโจมตี Firewalling with FreeBSD 4.8 และ IP Table Linux ด้วย DoS

โจมตี killwin.c

- กรณีทดสอบโฮสต์หลังไฟร์วอลล์โจมตีไปที่พอร์ต 80 (เปิดพอร์ต 80 สำหรับโปรโตคอล http ที่โฮสต์หลังไฟร์วอลล์)

ผลการโจมตี

- โฮสต์หลังไฟร์วอลล์ และไฟร์วอลล์โฮสต์ ทำงานตามปกติ
- ไม่มีการแจ้งเตือน เนื่องจากเป็นพอร์ตที่อนุญาตเอาไว้
- มีการแจ้งเตือนแต่จะไปแสดงที่ ไฟล์ Log ของระบบ

กรณีทดสอบไฟร์วอลล์โฮสต์

โจมตีไปที่พอร์ต 139

ผลการโจมตี

- ไฟร์วอลล์โฮสต์ทำงานตามปกติ

2. โจมตี synflood.c

- **กรณีทดสอบโฮสต์หลังไฟร์วอลล์**

  โจมตีไปที่พอร์ต 80 (เปิดพอร์ต 80 สำหรับโปรโตคอล http ที่โฮสต์หลังไฟร์วอลล์)

ผลการโจมตี

- โฮสต์หลังไฟร์วอลล์ และไฟร์วอลล์โฮสต์ ไม่ตอบสนองใดๆ
- ถ้าโจมตีไปพอร์ตที่ไม่ได้อนุญาตไว้ โฮสต์หลังไฟร์วอลล์จะปลอดภัย แต่เครื่องไฟร์วอลล์จะหยุดการทำงานช้าลง
- มีการแจ้งเตือนแต่จะไปแสดงที่ ไฟล์ Log ของระบบ

- กรณีทดสอบไฟร์วอลล์โฮสต์

  โจมตีไปที่พอร์ต 80

ผลการโจมตี

- ไฟร์วอลล์โฮสต์หยุดทำงาน ไม่ตอบสนอง
- มีการแจ้งเตือนแต่จะไปแสดงที่ ไฟล์ Log ของระบบ
- ไม่ว่าจะโจมตีไปที่พอร์ตใดๆ ก็หยุดทำงานทุกครั้ง แม้จะไม่อนุญาตให้ใครเข้าถึงเครื่องไฟร์วอลล์ได้

3. การเจาะระบบ Firewalling with FreeBSD 4.8 และ IP Table Linux

ใช้ Leak Test เพื่อสแกนพอร์ตโฮสต์ที่ติดตั้ง Firewall with FreeBSD 4.8 และ IP Table Linux ได้ผลลัพธ์ของการสแกนพอร์ตออกมาคือ โปรแกรม Teak Test สามารถเจาะผ่านไฟร์วอลล์ทั้งคู่ได้ และ Nmap สามารถตรวจหาระบบปฏิบัติการได้

4.8.10 สรุปผลการทดสอบผลิตภัณฑ์ไฟร์วอลล์ชนิดเอนเตอร์ไพรส์ไฟร์วอลล์

1. สรุปผลการโจมตีด้วย DoS

WatchGuard และ ISA Server ดีกว่า Wingate และ FreeBSD เนื่องจาก Wingate มีปัญหาเรื่องการแจ้งเตือนมากเกินไปเมื่อถูก โจมตี ด้วย Synflood และช่วงเวลานั้นก็เป็นช่องโหว่ให้โจมตีที่พอร์ตอื่นๆ ซึ่งถูกบล็อกเอาไว้ได้ส่วน WatchGuard แม้จะหยุดทำงานไปแต่ยังคงป้องกันพอร์ตอื่นๆ และเครื่องภายในไว้ได้และเมื่อกลับมาทำงานใหม่ก็ทำงานต่อได้อย่างปกติ ผิดกับ Wingate ที่กลับมาทำงานใหม่ไม่ได้เพราะบัฟเฟอร์หมด ต้องบูตเครื่องใหม่เท่านั้น

	ISA Server	FreeBSD	Wingate	WatchGuard
Killwin.c	A	A	A	A
Synflood.c	B	C	D	B

ตารางที่ 4-10 สรุปการโจมตี DoS ไปยังเอนเตอร์ไพร์สไฟร์วอลล์

A: ปกติ

B: ตอบสนองช้ามากๆ

C: หยุดทำงานไม่ตอบสนองใดๆ

D: แจ้งเตือนมากเกินไป จนทำงานต่อไม่ได้

หมายเหตุ จากตาราง การทดลองได้ทำการคอนฟิกให้บล็อกพอร์ต TCP หมายเลข 10 และ 139 และโจมตี killwin และ Synflood ไปยังพอร์ต 139 และ 10 ตามลำดับ

2. สรุปผลการโจมตีด้วยการสแกนพอร์ต

จากการทดลองในการสแกนพอร์ตโฮสต์ที่ทำการติดตั้ง ISA และ WatchGuard โดยใช้ Nmap จะทำการสรุปผลการทดลองดังนี้

- สำหรับ ISA

- พอร์ต 23, 80 ที่เปิดอยู่, Nmap ตรวจสอบพบว่าพอร์ต 23 ปิด แต่พอร์ต 80 เปิดส่วน
- พอร์ตอื่นๆ ที่เหลือ, Nmap ตรวจสอบพบว่าพอร์ตเหล่านั้นถูกฟิลเตอร์

- สำหรับ WatchGuard

- มีพอร์ต 264, 265 ที่เปิดอยู่

-สำหรับ FreeBSD

- ใช้ Leak Test เพื่อสแกนพอร์ตโฮสต์ที่ติดตั้ง Firewall with FreeBSD ได้ผลลัพธ์ของการสแกนพอร์ตออกมาคือ โปรแกรม Teak Test สามารถเจาะผ่านไฟร์วอลล์ได้

-สำหรับ Wingate

- Port 80 เปิดอยู่
- Port อื่นๆ ที่เหลือถูกฟิลเตอร์

-ส่วนพอร์ตอื่นๆ ที่เหลือ, Nmap ตรวจสอบพบว่าพอร์ตเหล่านั้นปิดอยู่ส่วนการตรวจจับระบบปฏิบัติการ พบว่า

- ISA สามารถปิดบังระบบปฏิบัติการได้
- WatchGuard ไม่สามารถปิดบังระบบปฏิบัติการได้
- FreeBSD สามารถตรวจหาระบบปฏิบัติการได้
-Wingate ไม่สามารถตรวจหาระบบปฏิบัติการได้

เพราะฉะนั้นโดยภาพรวมแล้ว ไม่สามารถสรุปว่าผลิตภัณฑ์ไหนดีกว่าโดยอาศัยผลลัพธ์จากการสแกนเท่านั้นเนื่องจากผลลัพธ์ของการสแกนพอร์ตพบว่า ISA สามารถปิดบังการสแกนได้เป็นส่วนใหญ่แต่ไม่ทั้งหมด ส่วน WatchGuard ทำให้ผลการสแกนพอร์ตออกมาไม่ตรงกับความเป็นจริงโดยสิ้นเชิงแต่สำหรับการตรวจจับระบบปฏิบัติ การพบว่า ISA สามารถปิดบังระบบปฏิบัติการได้แต่ WatchGuard ทำไม่ได้ดังนั้นในการพิจารณาว่าผลิตภัณฑ์ไหนดีกว่ากัน จะต้องพิจารณาปัจจัยอื่นๆ ประกอบด้วย

หมายเหตุ การโจมตีด้วย DoS ทั้งสองประเภทและการสแกนพอร์ต เป็นการโจมตีไปยังพอร์ต TCPอย่างเดียว พอร์ตที่กล่าวถึงในบทนี้ จึงเป็นพอร์ต TCP ทั้งหมด

บทที่ 5
สรุปผลและวิเคราะห์ผล

5.1 วัตถุประสงค์

วัตถุประสงค์ของปริญญานิพนธ์ฉบับนี้คือการศึกษาเทคโนโลยีในการรักษาความปลอดภัยให้กับระบบเครือข่ายขององค์กรที่เชื่อมต่อกับอินเตอร์เน็ตโดยมุ่งเน้นไปที่ไฟร์วอลล์ซึ่งจะเป็นการประยุกต์ ใช้ระบบไฟร์วอลล์สำหรับเครือข่าย พร้อมทั้งยังศึกษาระบบเครือข่ายของมหาวิทยาลัยนเรศวร ซึ่งก็ได้ ผลตามวัตถุประสงค์ที่ตั้งใจไว้โดยดำเนินการดังนี้

1. ศึกษาการทำงานของระบบเครือข่ายคอมพิวเตอร์ที่ใช้โพรโตคอลทีซีพี/ ไอพี (TCP/IP Protocol)
2. ศึกษาพฤติกรรมการบุกรุกทางเครือข่ายคอมพิวเตอร์และรูปแบบการโจมตีในแบบต่างๆ
3. ศึกษาคุณลักษณะของไฟร์วอลล์ ประเภทของไฟวอลล์ รูปแบบการทำงานต่างๆของไฟร์วอลล์ รวมถึงข้อดี ข้อเสียของแต่ละแบบเพื่อใช้เป็นข้อมูลในการเลือกใช้ไฟร์วอลล์ให้เหมาะสมกับระบบเครือข่าย
4. ศึกษาโครงสร้างระบบเครือข่ายคอมพิวเตอร์และระบบความรักษาปลอดภัยของระบบเครือข่ายของมหาวิทยาลัยนเรศวร
5. เพื่อนำเสนอแนวความคิดและรูปแบบการป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยนเรศวรโดยใช้ไฟร์วอลล์

5.2 สรุปไฟร์วอลล์

ไฟร์วอลล์ทำหน้าที่เป็นเหมือนหน่วยรักษาความปลอดภัยที่ประตูหน้าบ้านการเข้าออกจากเครือข่ายจะต้องได้รับการตรวจสอบ ดังนั้นไฟรวอลล์จึงเป็นยามรักษาความปลอดภัยที่คอยกั้น ตรวจและป้องกันผู้ไม่พึงปรารถนาเข้าสู่เครือข่าย

การมีไฟร์วอลล์จึงเป็นเครื่องมือหลัก ที่จะสามารถบอกหน่วยรักษาความปลอดภัย ให้ทำงานตามนโยบายด้านรักษาความปลอดภัย โดยการควบคุมหรือเรียกเข้ามาจากภายนอก ควบคุมปริมาณเข้าออกไม่พึงปรารถนา หากมีใครบุกรุกเข้ามา ก็จะขัดขวางหรือบอกให้ผู้ดูแลระบบได้รับรู้ขอบเขตของไฟร์วอลล์ทำได้มากไฟร์วอลล์เป็นตัวปิดกั้นรอยรั่วต่างๆ ทำการ Screen ตรวจสอบ Packet ทุกๆ Packet หากไม่ต้องการให้ Packet ใดผ่านเข้าออกก็กำหนดได้ รวมถึงการป้องกันการเรียกเข้ามาในเครือข่าย

ภายในองค์กร เช่น การใช้คำสั่ง Finger การป้องกัน แม้แต่การใช้คำสั่งที่ใช้ Packet ICMP เพื่อตรวจสอบเส้นทาง

การเรียกเข้าหาระบบภายนอกก็จะต้องมีระบบควบคุม มีการสร้างเชลล์เฉพาะการทำรายงานผู้ใช้เก็บประวัติการทำงานของผู้ใช้ ที่เรียกเข้าระบบไว้ใช้ตรวจสอบ เมื่อจำเป็นดังนั้นไฟร์วอลล์จึงเป็นเครื่องมือที่เครือข่ายในองค์กรต่างๆ จำเป็นต้องมีหากจำเป็นต้องรักษาความปลอดภัยของข้อมูล ปัญหาด้านความปลอดภัยไม่ได้เป็นภาระของไฟร์วอลล์เท่านั้น แต่เป็นภาระหลักของผู้ดูแลระบบที่จะต้องดูแลกำหนดกฎการใช้งาน และสอดส่องความปลอดภัยของเน็ตเวิร์กอยู่เสมอ

จะเห็นได้ว่าไม่มีคำตอบที่ถูกต้องเพียงคำตอบเดียวสำหรับการออกแบบและใช้งานไฟร์วอลล์ การตัดสินใจของแต่ละองค์กรจะขึ้นอยู่กับปัจจัยหลายอย่างแตกต่างกัน เช่น นโยบายการรักษาความปลอดภัยของมหาวิทยาลัย, พื้นฐานทางเทคนิคของบุคลากร, ค่าใช้จ่าย และการคุกคามจากการโจมตีที่รับรู้ ระบบความมั่นคงของคอมพิวเตอร์และเครือข่ายที่ดี ต้องประกอบไปด้วยหลายมาตราการที่สนับสนุนและทำงานร่วมกันที่สำคัญนโยบายความมั่นคงขององค์กรต้องเป็นนโยบายที่สมเหตุสมผลและคำนึงถึงความเป็นจริงในทางปฏิบัติระบบคอมพิวเตอร์และเครือข่ายจะต้องเตรียมพร้อมที่จะรับมือในภัยต่างๆที่จะเกิดขึ้น

ไฟร์วอลล์ที่นำมาทดสอบมีความสามารถเป็นผลิตภัณฑ์ที่มีขีดความสามารถในการให้บริการด้านความปลอดภัยที่หลากหลายไม่ว่าจะเป็นไฟร์วอลล์ ,พร็อกซี่ ,Content Filtering และ Intrusion Detection สามารถใช้งานตั้งแต่เน็ตเวิร์กขนาดเล็กที่ใช้ไฟร์วอลล์เพียงตัวเดียวในการควบคุมเน็ตเวิร์กทั้งหมด และสามารถขยายไปจนถึงเน็ตเวิร์กขนาดใหญ่ที่ต้องการเสถียรภาพสูง ที่จะต้องใช้กลุ่มของไฟร์วอลล์ทำงานร่วมกันและกระจายภาระการทำงานไปยังเซิร์ฟเวอร์ รวมถึงการป้องกันความล้มเหลวของไฟร์วอลล์ (Fault Tolerance)

Zone Alarm เป็นโปรแกรมเพอร์ซันแนลไฟร์วอลล์ที่มีปรัชญาในการออบแบบที่ชัดเจน ผู้ใช้สามารถสัมผัสได้ขนาดของโปรแกรมที่เล็กกระทัดรัด ไม่ต้องการการปรับแต่งจากผู้ใช้เป็นพิเศษ ใช้กำลังงาน CPU ต่ำ มีประสิทธิภาพในการทำงานสูง ตอบสนองต่อผู้ใช้ได้อย่างรวดเร็วการทำงานใดที่สามารถทำได้อัตโนมัติ Zone Alarm จะจัดการได้ด้วยตัวเองแทบทั้งหมด การรบกวนผู้ใช้ในเรื่องต่างๆมีน้อยมาก เว้นเสียแต่ว่าผู้ใช้อาจจะมีความต้องการความปลอดภัยส่วนใดส่วนหนึ่งเป็นพิเศษจึงต้องมาทำการปรับเปลี่ยนการทำงานของไฟร์วอลล์

นอกจากนี้จะเห็นได้ว่าแม้จะมีส่วนที่ให้ผู้ใช้ทำการกำหนดทางเลือกในการเลือกในการทำงาน ZoneAlarm เอง ออปชั่นต่างๆก็มีน้อยมาก และค่าที่ให้กำหนดในโปรแกรมก็ไม่ได้เป็นการกำหนดทางเทคนิคที่ยุ่งยากซับซ้อนแต่อย่างใด เป็นการกำหนดตามลักษณะความต้องการของผู้ใช้จริงๆ ลักษณะการติดต่อกับผู้ใช้ผู้ใช้นั้นเรียบง่าย กระชับและชัดเจนเข้าใจโดยง่าย นับว่าเป็นเพอร์ซันแนลไฟร์วอลล์ที่ออกแบบมาสำหรับเอนด์ยูสเซอร์โดยตรง แต่ก็ต้องหาโปรแกรมอื่นๆมาเสริมการทำงานเพิ่มเติมในการกรป้องกันภัยในระดับอื่น เช่น ไวรัสที่มาจากอีเมล์ หรือเว็บเพจที่แอบซ่อนสคริปต์ที่ประสงค์ร้าย ซึ่งช่วยให้การป้องกันภัยเป็นไปอย่างสมบูรณ์แบบครอบคลุมทุกระดับ

Tiny Personal Firewall เป็นโปรแกรมีรักษาความปลอดภัยที่มีความสมบูรณ์ในตัวเอง มีการทำงานที่ครอบคลุมในทุกด้านๆของการใช้งาน มีระบบช่วยเหลือในการกำหนดการป้องกันต่างๆโดยอัตโนมัติ ทำให้ลดความเสี่ยงที่จะถูกเจาะระบบด้วยวิธีต่างๆลงไปได้มากในทันทีที่ติดตั้งไฟร์วอลล์ลงไปโดยไม่ต้องปรับแต่งเพิ่มเติมแต่อย่างใด เหมาะสมสำหรับผู้ใช้ที่ไม่ได้มีความรู้ความชำนาญทางเทคนิคเฉพาะความปลอดภัยมากนักให้สามารถใช้งานคอมพิวเตอร์ของตนเองและเข้าไปใช้งานอินเตอร์เน็ตได้อย่างปลอดภัย นอกจากนี้การป้องกันบางส่วนยังช่วยให้ผู้ใช้สามารถใช้งานแบนด์วิดธ์ได้อย่างเกิดประโยชน์สูงสุดอีกด้วย และหากผู้ใช้มีความรู้ในการใช้งานมากขึ้นก็สามารถปรับแต่งระดับของการรักษาปลอดภัยต่างๆได้ด้วยตนเอง

ในการใช้ไฟร์วอลล์ของลีนุกส์โดยปกติแล้วจะต้องเขียนโดยใช้การเขียนสคริปท์ไฟร์วอลล์ ซึ่งจะยากต่อการใช้งานของผู้ใช้ ปริญญานิพนธ์นี้จึงได้ทำไฟร์วอลล์ไอพีเทเบิลให้ง่ายต่อการใช้งาน และพัฒนาเข้าใจการใช้ Script ไฟร์วอลล์ไอพีเทเบิลในลีนุกส์ให้มากขึ้น

ข้อดี : 1. จะมีความสะดวกต่อการติดตั้งไฟร์วอลล์เพราะภายในโปรแกรมจะมีช่องให้กรอกรายละเอียดในการคอนฟิกจะทำให้ผู้ใช้ ไม่สับสนในการกรอกกฎ

2. การคอนฟิกกฎระยะไกล จะทำให้ผู้ใช้ไม่จำเป็นต้องคอนฟิกที่เครื่องไฟร์วอลล์

3. การแจ้งเตือนผู้ใช้เมื่อมีผู้บุกรุกเข้ามา

4. มีการเข้ารหัสเพื่อความปลอดภัย

ข้อเสีย : 1. ผู้ใช้โปรแกรมจะเป็นต้องศึกษารายละเอียดของสคริปท์ไฟร์วอลล์ไอพีเทเบิลอยู่ เพราะว่าในภายในโปรแกรมยังอ้างอิงรูปแบบของ สคริปท์ในบางส่วน

2. การเข้ารหัสจะเป็นการเข้าแบบ RSA ซึ่งจะมีความปลอดภัยมาก แต่ข้อเสียคือจะช้ามาก

ISA Server เป็นไฟร์วอลล์ที่น่าสนใจ นอกจากที่มีความสามารถหลากหลายแล้ว ก็คือการที่ไฟร์วอลล์ทำงานระบบปฏิบัติการยอดนิยมอย่าง Windows 2000 Server กอปรกับเป็นผลิตภัณฑ์ของไมโครซอฟท์เอง ทำให้สามารถทำงานเข้ากันกับ Active Directory ได้เป็นอย่างดีรวมทั้งการที่มียูสเซอร์อินเตอร์เฟสที่เป็นไปตามมาตรฐานของไมโครซอฟท์ที่ผู้ใช้คุ้นเคยอยู่แล้ว ทำให้สามารถเริ่มนำมาใช้งานได้โดยง่าย และเมื่อผู้ใช้เริ่มเข้าใจการทำงานมากขึ้นก็จะสามารถขยับขยายให้สามารถทำงานได้ซับซ้อนขึ้น ดังนั้นจึงเป็นผลิตภัฑ์ที่เหมาะอย่างยิ่งสำหรับผู้เริ่มต้น

อย่างไรส่วนประกอบที่มีอยู่ภายใน ISA Server นั้นมีจำนวนมาก ซึ่งต่างก็มีความสัมพันธ์และส่งผลกับทั้งความสามารถในการทำงานทั้งสิ้น ตัวอย่างที่มีอยู่ในบทนี้เป็นการแนะนำองค์ประกอบพื้นฐานที่จำเป็นสำหรับเริ่มต้นการใช้งานเท่านั้น หากสามารถศึกษาหาข้อมูลเพิ่มเติมในส่วนประกอบอื่น เช่น Bandwidth Priorities, Intrusion Detection, VPN และสามารถนำมาประยุกต์ใช้งานได้ จะพบว่า ISA Server จะไม่เป็นเพียงไฟร์วอลล์ธรรมดาที่พบได้ในผลิตภัณฑ์อื่นๆ ในท้องตลาด แต่เป็นไฟร์วอลล์ที่มีคุณสมบัติครอบคลุมการใช้งานต่าง ๆ อย่างกว้างขวางมากตัวหนึ่งทีเดียว

ไฟร์วอลล์ในระบบปฏิบัติการ Windows 2000 สำหรับเครื่องส่วนบุคคลมีความสำคัญมากขึ้น เพราะเป็นการเสริมและเพิ่มระดับความปลอดภัยในองค์กร แต่อย่างไรก็ตามการออกแบบกฎของไฟร์วอลล์นั้นค่อนข้างยาก เพราะต้องอาศัยความรู้ และความเข้าใจเกี่ยวกับ TCP/IP พอสมควร และหากตั้งค่ากฎไม่เหมาะสมอาจส่งผลทำให้โปรแกรมในระบบอาจจะไม่สามารถทำงานเพื่อติดต่อผ่านระบบเครือข่ายได้ กระบวนการติดตั้งไฟร์วอลล์ ในเครื่องส่วนบุคคลจำเป็นต้องทำทุกครั้งหลังจากการติดตั้งระบบปฏิบัติการ windows 2000 กระบวนการนี้เป็นส่วนหนึ่งของการทำ OS Hardening ซึ่งถือเป็นกระบวนการที่สำคัญยิ่ง หากผู้ดูแลระบบมีความเข้าใจ และสามารถออกแบบไฟร์วอลล์ให้เหมาะสมตามการใช้งานภายในองค์กร ก็ไม่จำเป็นที่ต้องซื้อโปรแกรม Personal Firewall มาใช้งาน การตั้งค่าไฟร์วอลล์ใน Windows 2000 ด้วยโปรแกรม mmc ต้องตั้งค่าสำคัญๆ สามส่วนคือ IPSecurity filter list , IPSecurity filter action, IPSecurity Policy rule

ประโยชน์ของการใช้งานไฟร์วอลล์ Window 2000

การตั้งค่าใช้งานไฟร์วอลล์พื้นฐานข้างต้นเป็นพื้นฐานของการทำสร้างความปลอดภัยพื้นฐานให้ระบบปฏิบัติการ (OS Hardening) ซึ่งทุกเครื่องในระบบเครือข่ายควรจะต้องผ่านกระบวนดังกล่าวเพื่อความปลอดภัยของเครื่อง และระบบเครือข่ายภายในองค์กร การออกแบบกฎของไฟร์วอลล์นั้นขึ้นอยู่กับ รูปแบบการใช้งานระบบเครือข่ายของแต่ละองค์กร เช่น บางองค์กร มีความต้องการใช้

NetBIOS ภายในองค์กร ดังนั้นในแต่ละเครื่องต้องมีกฎของไฟร์วอลล์ ไม่ให้มีแพ็จเกจภายนอกระบบเครือข่ายขององค์กรผ่านพอร์ต 139 เป็นต้น

Norton Internet Security เป็นโปรแกรมรักษาความปลอดภัยที่มีความสมบูรณ์ในตัวเอง มีการทำงานที่ครอบคลุมในทุกๆด้านของการใช้งาน มีระบบช่วยเหลือในการกำหนดการป้องกันต่างๆ โดยอัตโนมัติ ทำให้ลดความเสี่ยงที่จะถูกเจาะระบบด้วยวิธีต่างๆลงไปได้มากในทันทีที่ติดตั้งลงโปรแกรมไปโดยไม่ต้องปรับแต่งเพิ่มเติม เหมาะสมสำหรับผู้ที่ใช้ที่ไม่ได้มีความรู้ความชำนาญทางเทคนิคโดยเฉพาะในเรื่องความปลอดภัยมากนัก นอกจากนี้การป้องกันบางส่วนยังช่วยให้ผู้ใช้สามารถใช้งานแบนด์วิดธ์ได้อย่างเกิดประโยชน์สูงสุด

ในการจะเลือกผลิตภัณฑ์ไฟร์วอลล์ใดๆ สำคัญที่สุดนั่นคือ ผู้บุกรุกจะทำการโจมตีเครือข่ายหรือไฟร์วอลล์โฮสต์ของเราได้หรือไม่ ขึ้นอยู่กับการคอนฟิกหรือการปรับแต่งค่าของไฟร์วอลล์โดยเฉพาะอย่างยิ่งนโยบายความปลอดภัย (Security Policy) ที่เหมาะสมกับองค์กรและการใช้งานนั่นเอง

5.3 สรุปการวิเคราะห์ระบบเครือข่ายคอมพิวเตอร์

5.3.1 สรุปการวิเคราะห์สถานภาพและโครงสร้างของระบบเครือข่ายคอมพิวเตอร์

มหาวิทยาลัยนเรศวรได้มีการประยุกต์ใช้อุปกรณ์คอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์มีวัตถุประสงค์เพื่อรองรับภารกิจด้านการจัดการเรียนการสอนและการบริหารงานของมหาวิทยาลัยโดยพัฒนาจากระบบการสื่อสารเดิมที่มีลักษณะแยกเฉพาะหน่วยสถานีคอมพิวเตอร์ (Stand Alone) ให้มีเชื่อมต่อและสามารถสื่อสารแลกเปลี่ยนข้อมูลระหว่างสถานีหรือระหว่างหน่วยงานได้ และมีการออกแบบติดตั้งระบบคอมพิวเตอร์มหาวิทยาลัยนเรศวร (Host Computer) เป็นรูปแบบเดียวกันตั้งแต่ปี พ.ศ. 2539 – 2545 เพื่อให้มีความสามารถใช้งานทรัพยากรข้อมูลร่วมและแลกเปลี่ยนข้อมูลบนระบบปฏิบัติการ และมีการเชื่อมโยงระบบ เทคโนโลยีระบบเครือข่าย และระบบปฏิบัติการเป็นระบบเดียวกัน และมีการวางระบบแบบกระจายศูนย์เพื่อให้เกิดความคล่องตัวในการบริหารจัดการ สำหรับด้านการให้บริการบนระบบเครือข่ายมหาวิทยาลัยได้ให้บริการอินเตอร์เน็ตและคอมพิวเตอร์แก่นิสิตและบุคลากรทุกคน และมีสถานภาพการบริหารระบบเครือข่ายแบ่งเป็น 4 ส่วน ส่วนเชื่อมต่อภายนอก (Internet Connection Zone) ส่วนเชื่อมต่อหลัก (Core Switch Zone) ส่วนกระจาย (Distribution Zone) และส่วนเชื่อมต่อ (Access point Zone)

โครงสร้างการบริหารระบบเครือข่ายแบ่งออกเป็น 1 โดเมนและแบ่งโดเมนย่อยอีก 9 โดเมน ระบบปฏิบัติที่มหาวิทยาลัยใช้ คือ Windows NT 4.0 Server และ Windows NT 2000 Server ลักษณะ

การเชื่อมต่อเครือข่ายเป็นแบบ Star โดยมีศูนย์กลางควบคุมเครือข่ายที่อาคารมิ่งขวัญเชื่อมต่อโดยใช้เทคโนโลยี ATM และอาคาร CITCOMS เชื่อมต่อโดยใช้เทคโนโลยี Gigabit Ethernet การบริหารจัดการเครือข่ายภายในมหาวิทยาลัยใช้อุปกรณ์ป้องกันการดุกคาม (Firewall) และใช้ Traffic Shaper บริหารจัดการ Bandwidth และมหาวิทยาลัยใช้ผู้ใช้บริการอินเตอร์เน็ต 3 รายคือ Uni Net, KSC, Loxinfo

5.3.2 สรุปผลการวิเคราะห์ปัญหาและปัจจัยที่ส่งผลกระทบต่อระบบเครือข่ายคอมพิวเตอร์

ปัญหาส่วนการเชื่อมต่อภายนอก (Internet Connection Zone) คือปัญหาระบบเครือข่าย NU Net ไม่สามารถติดต่อกับระบบเครือข่ายอินเตอร์เน็ตได้ เป็นผลให้ข้อมูลของผู้ใช้บริการที่มีการติดต่อสื่อสารในช่วงนั้นอาจสูญหาย เนื่องจากผู้ให้บริการอินเตอร์เน็ต (ISP) ไม่สามารถให้บริการได้ ปัญหาของระบบการหาเส้นทางการเชื่อมต่อกับระบบอินเตอร์เน็ตของ BGP Protocol ที่ไม่สามารถตรวจสอบสถานะภาพการเชื่อมต่อได้ครบถ้วน และปัญหา Bandwidth ไม่เพียงพอต่อความต้องการใช้งานทำให้การเชื่อมต่อระบบอินเตอร์เน็ตช้ามากเนื่องจากจำนวนผู้ใช้บริการระบบมากขึ้นและมีเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบมากขึ้น

ปัญหาส่วนกลางการเชื่อมต่อหลัก (Core Switch Zone) เป็นปัญหาอุปกรณ์เชื่อมต่อเครือข่ายหลักไม่สามารถให้บริการได้ เนื่องจากเดิมมีการออกแบบให้คอมพิวเตอร์แม่ข่ายที่ใช้หมายเลขไอพีจริงอยู่ใน IP SUBNET เดียวกัน และอุปกรณ์ในการเชื่อมต่อเครือข่ายหลักของมหาวิทยาลัย ปัญหาการให้บริการ Mail Server เนื่องจากเครื่อง Mail Server ที่ให้บริการอยู่มีอายุการใช้งานมานาน ปัญหาการให้บริการ Domain Controller (คอมพิวเตอร์แม่ข่าย การให้บริการเก็บบัญชีรายชื่อผู้ใช้ สิทธิ์การใช้งาน) เนื่องจากเครื่อง Domain Controller ที่ให้บริการอยู่มีอายุการใช้งานนานปัญหาการให้บริการ ISA: Internet Securities and Accelerator (คอมพิวเตอร์แม่ข่ายที่ให้บริการตรวจสอบข้อมูล เข้าและออก แปลงหมายเลขไอพีภายใน ให้เป็นหมายเลขไอพีจริง) เนื่องจาก ISA Server ให้บริการหลายหน้าที่ทำงานหนักรับภาระงานไม่ไหว ปัญหาการให้บริการ DNS Server เนื่องจากมีเพียงเครื่องเดียวและเครื่องไม่ตรงตามคุณสมบัติของการบริการ DNS Server

ปัญหาส่วนกระจาย (Distribution Zone) คือปัญหาผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ (Administrator) บางส่วนไม่มีความรู้ความเข้าใจเกี่ยวกับระบบเครือข่ายเพียงพอ ปัญหาการไม่มีการเชื่อมต่อสัญญาณสำรองจากคณะต่างๆมายังอาคาร CITCOM ปัญหาผู้ดูแลระบบส่วนกลางไม่สามารถเข้าไปแก้ไขปัญหา ที่เกิดบนระบบเครือข่ายคอมพิวเคอร์ของนอกเวลาราชการได้ ปัญหาการเสื่อมสภาพของเครื่องเก็บสำรองกระแสไฟฟ้า (UPS)

ปัญหาส่วนการเชื่อมต่อใช้งาน (Access Point Zone) คือปัญหาการขยายการเชื่อมต่อของระบบเครือข่ายภายในคณะมีการเชื่อมต่อพ่วงกันจำนวนมากและเป็นอุปกรณ์ต่อพ่วง (Chain hub/switch) ทำให้เกิดปัญหาในด้านประสิทธิภาพของเครือข่าย และปัญหาการขาดความรู้ความเข้าใจในการใช้บริการเครือข่ายของผู้ใช้บริการ

เอกสารอ้างอิง

[1] Anderson, J.P. (1980). **Computer security threat monitoring and surveillance,** (Technical Report), Washington, PA, James P. Anderson Co.

[2] Simson Garfinkel and Gene Spafford: **"Practical UNIX Security"**, O'Reilly & Associates, Inc

[3] Terry Escamila: **"Intrusion Detection Network Security Beyond the Firewall"**, John Wiley & Sons, Inc., 1998

[4] Kirk Waingrow: "**UNIX Hints & Hacks**", Qve Corporation, 1999

[5] Smaha, S.E. (1988). **Haystack: An intrusion detection system.** Proceedings of the fourth Aerospace Computer Security Applications Conference (pp. 37-44).

[6] Daniel P. Bovet ,Marco Cesti: "**Understanding the Linux Kernel**" , O'Reilly & Associates, Inc,2001

[7] Syngress: "**Hack proofing your network**" , Syngress Media, Inc.,2000

[8] Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman (2000) : "**Building Internet Firewalls 2nd Edition**", O'Reilly, California.

[9] Joel Scambray, Stuart McClure, George Kurtz (2001): "**Hacking Exposed: Network Security Secrets & Solutions**", McGraw-Hill.

[10] Terry Wiliam Ogletree (2000): "**Practical Firewalls**", Que, Indiana.

[11] Ton Plooy (2000): "**Packet Filtering with iphlpapi.dll**", Windows developer's journal, October 2000

[12] Behrouz Forouzan, "**Introduction to Data Communications and networking**", International Edition, McGraw-Hill, 1998.

[13] Andrew S. Tanenbaum, "**Computer Network**", 3th Edition, Prentice-Hall, 1996.

[14] Pankaj Mehra, Benjamin W Wah, **"Load Balancing an automated Learning Appoach"**, World Scientific, 1964.

[15] Richard L. Petersen, Morgan Kaufmann, **"Unix Networking clearly explained"**, 1999.

[16] Joel Scambray, Stuart McClure, George Kurthz, **"Hacking Exposed"**, Mc Graw Hill, 2001

[17] Stephen Northcutt, Judy Novak, "**Network Intrusion Detection An Analyst's Handbook**", New Riders, 2000

[18] สันติ ศรีลาศักดิ์, วรวุฒิ เที่ยงธรรม, "เจาะประเด็นงานเขียนโปรแกรมบนลีนุกซ์", ออฟเซ็ท เพรส, 2542

[19] สุวัฒน์ ปุณณชัยยะ, ต้น ตันฑ์สุทธิวงศ์ และ สุพจน์ ปุณณชัยชนะ, "**เปิดโลกของ TCP/IP และโปรโตคอลของอินเทอร์เน็ต**", โปรวิชั่น, 2543

[20] เอกสิทธิ์ วิริยจารี :"**ปิดทางแฮกเกอร์**", บริษัท ซีเอ็ดยูเคชัน จำกัด มหาชน, 2544

[21] เรืองไกร รังสิพล :"**เจาะระบบ TCP/IP: จุดอ่อนของโปรโตคอลและวิธีป้องกัน**", Provision, กรุงเทพฯ 2544.

[22] เรืองไกร รังสิพล.**เปิดโลก Firewall และ Internet Security**. กรุงเทพฯ : โปรวิชั่น 2544.

[23] ทศพล กนกนุวัตร์ .**How to Protect from Hacker**. กรุงเทพฯ : ซีเอ็ดยูเคชั่น 2542.

[24] วิญญู กิ่งหิรัญวัฒนา .ตำราพิชัยแคร็กเกอร์. กรุงเทพฯ : ซีเอ็ดยูเคชั่น 2545.

[25] ศิริวรรณ อภิสิริเด. จับไต๋....แฮกเกอร์. นนทบุรี : อินโฟเพรส 2545.

[26] เทเนนบาม, แอนดรูว์ **Computer Network** .ผศ.ดร .สัลยุทธ์ สว่างวรรณ, ผู้แปล 2542. กรุงเทพฯเพียร์สัน เอ็ดยูเคชั่น อินโดไชน่า .(Prentice-Hall,Inc 1996)

[27] วรเมศร์ เบญจวรรณ . **SECURITY TURN-PRO GUIDE**. กรุงเทพฯ PC MAGAZINE 2544

[28] เรืองไกร รังสิพล. เจาะระบบ TCP/IP จุดอ่อนของโปรโตคอลและวิธีป้องกัน . กรุงเทพฯ: โปรวิชั่น 2544

[29] มหาวิทยาลัยนเรศวร แผนการพัฒนามหาวิทยาลัยปี 2543-2547. พิษณุโลก: กองแผนงาน สำนักงานอธิการบดี. 2543

[30] มหาวิทยาลัยนเรศวร.แผนกลยุทธ์มหาวิทยาลัยนเรศวร พ.ศ. 2545-2549. กรุงเทพฯ: มิเนียเจอร์ 2545.

[31] มหาวิทยาลัยนเรศวร. **นโยบายการใช้งานคอมพิวเตอร์ภายใต้ระบบเครือข่ายคอมพิวเตอร์**, พิษณุโลก: กองแผนงาน สำนักอธิการบดี 2541.

[32] แกลรี่บี, แชลลี่ และคณะ. **การสื่อสารข้อมูลระดับพื้นฐาน**. สัลยุทธ์ สว่างวรรณ, ผู้แปลกรุงเทพฯ: ยูนิเวอร์แซลกราฟฟิกแอนด์เทรดดิ้ง. (ต้นฉบับพิมพ์ในปี ค.ศ. 2001) 2544.

[33] มหาวิทยาลัยนเรศวร. **โครงการติดตั้งระยะเครือข่ายคอมพิวเตอร์ระยะยาวที่1-7 ของมหาวิทยาลัยนเรศวร**. พิษณุโลก: กองแผนงาน สำนักงานอธิการบดี. (2539-2545).

[34] ศูนย์ฝึกอบรมและควบคุมระบบเครือข่ายคอมพิวเตอร์, แผนแม่บทเทคโนโลยีสารสนเทศ. มหาวิทยาลัยนเรศวร2546.

เว็บไซต์

[1] http://www.cert.org

[2] http://www.codeguru.com

[3] http://www.nmap.org

[4] http://www.securityfocus.com

[5] http://www.thaidev.com

[6] http://www.ibm.com

[7] http://www.microsoft.com/security

[8] http://www.packetstorm.com

[9] http://www.rootshell.com

[10] http://www.securityfocus.com

[11] http://www.iss.net: (White Paper) "Intrusion Detection in the Enterprise Network: Managing Hacker-Related Risk", Compaq Computer Corporation, March 1998

[12] http://www.ticm.com/kb/faq/idsfaq.html: Network Intrusion Detection Systems Frequently Asked Questions

[13] http://seclab.cs.ucdavis.edu/arpa/priv/welcome.html: Specification-based Detection for Unix Privileged Programs

[14] http://www.iss.net: Introduction to RealSecure Version 3.0

[15] http://www.cert.org/research/JHThesis/Chapter6.html: A Taxonomy of Computer and Network Attacks

[16] http://www.cert.org/research/JHThesis/Chapter7.html: Classification of Internet Incidents and Internet Activity

[17] http://www.cert.org/research/JHThesis/Chapter8.html: Methods of Operation and Corrective Actions

[18] http://www.cert.org/research/JHThesis/Chapter9.html: Case Study – Site A

[19] http://www.cert.org/research/JHThesis/Chapter10.html: Severe Incidents

[20] http://www.cert.org/ftp/tech_tips/intruder_detection_checklist: Intruder Detection Checklist

[21] http://www.cert.org/security-improvement/modules/m05.html: Prepareing to Detect Signs of Intrusion

[22] http://www.cert.org/security-improvement/practices/p040.html: Establish a policy and set ofprocedures that prepare your organization to detect signs of intrusion

[23] http://www.cert.org/security-improvement/practices/p041.html: Identify and enable systemand network logging mechanisms

[24] http://www.cert.org/security-improvement/practices/p042.html: Identify and install tools that aid in detecting signs of intrusion

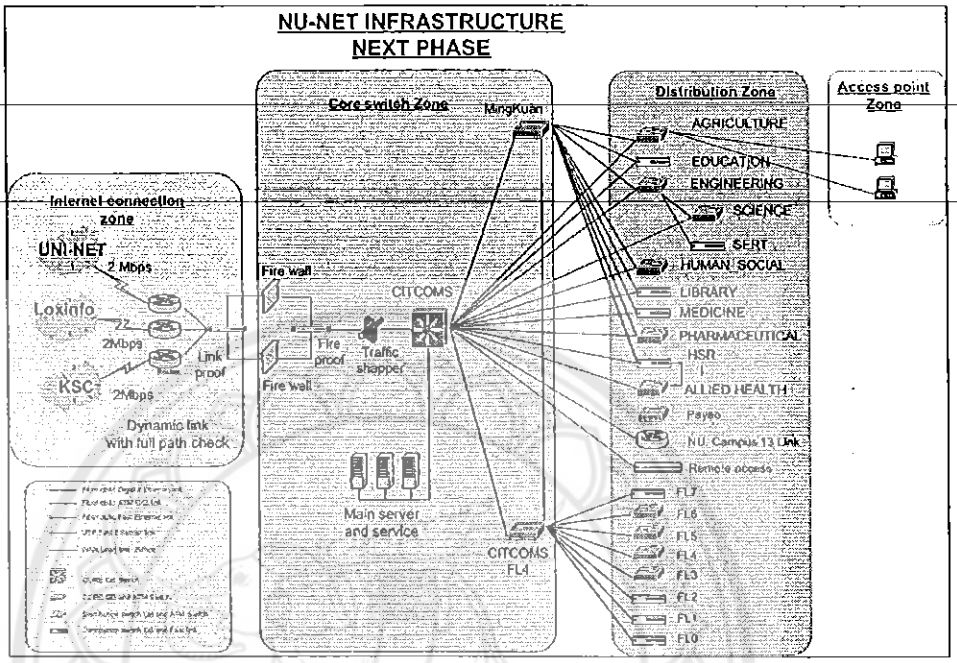
[25] http://www.cert.org/security-improvement/practices/p043.html: Generate informationrequired to verify the integrity of your systems and data

[26] http://www.ieee.com: A System for Distributed Intrusion Detection

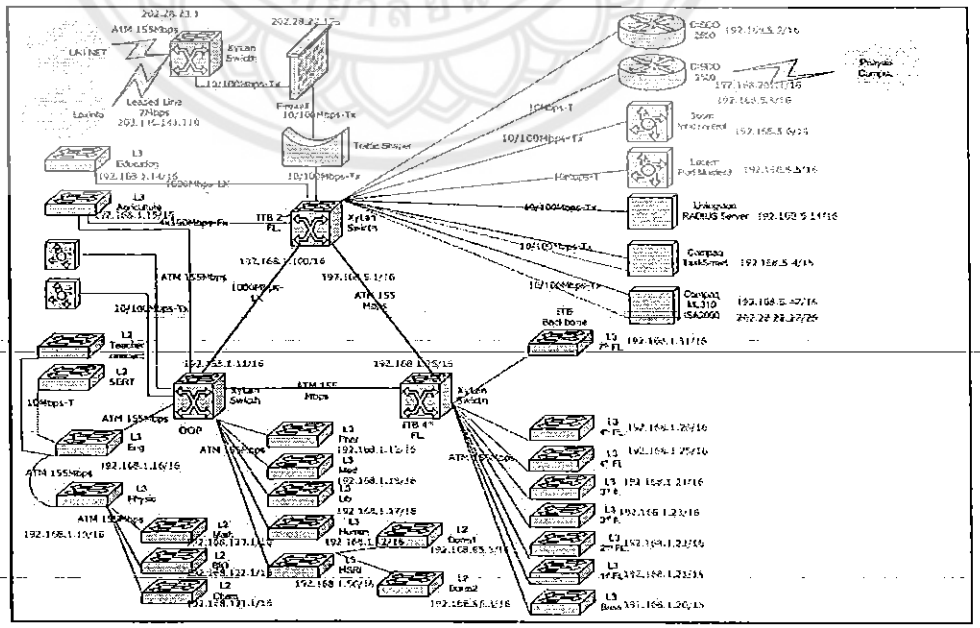
[27] http://www.cs.purdue.edu/coast/intrusion-detection/policy.html: Security Policy

ภาคผนวก ก.

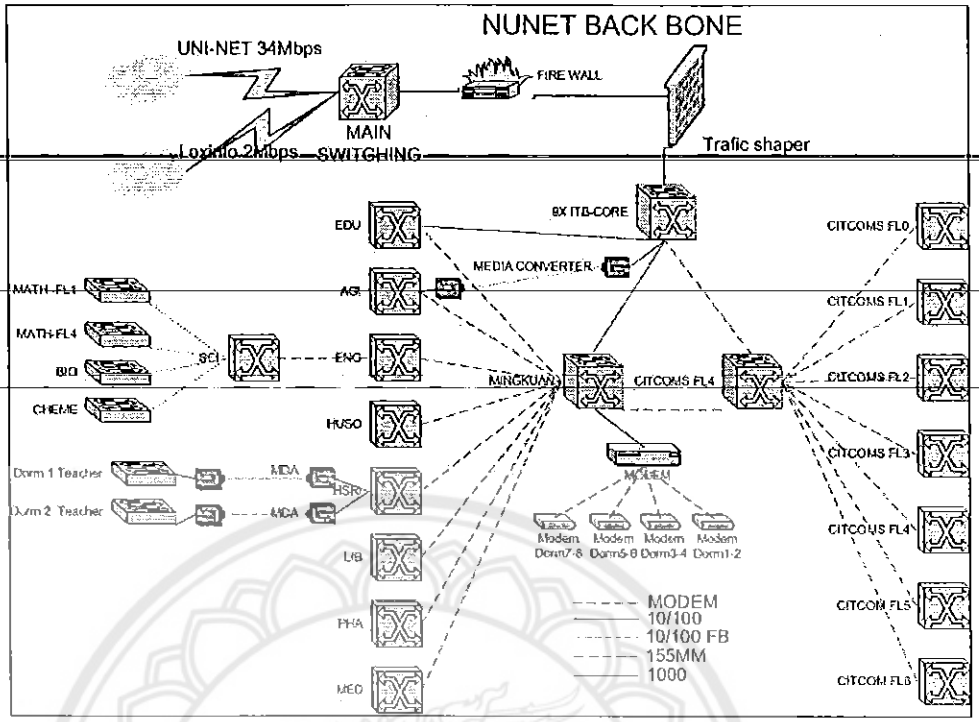
รูปโครงสร้างระบบเครือข่ายมหาวิทยาลัยนเรศวร



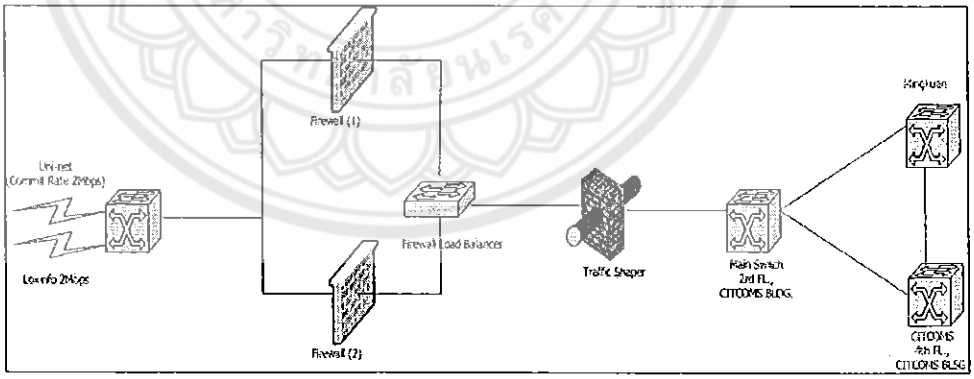
รูปที่ ก-1 โครงสร้าง NU NET



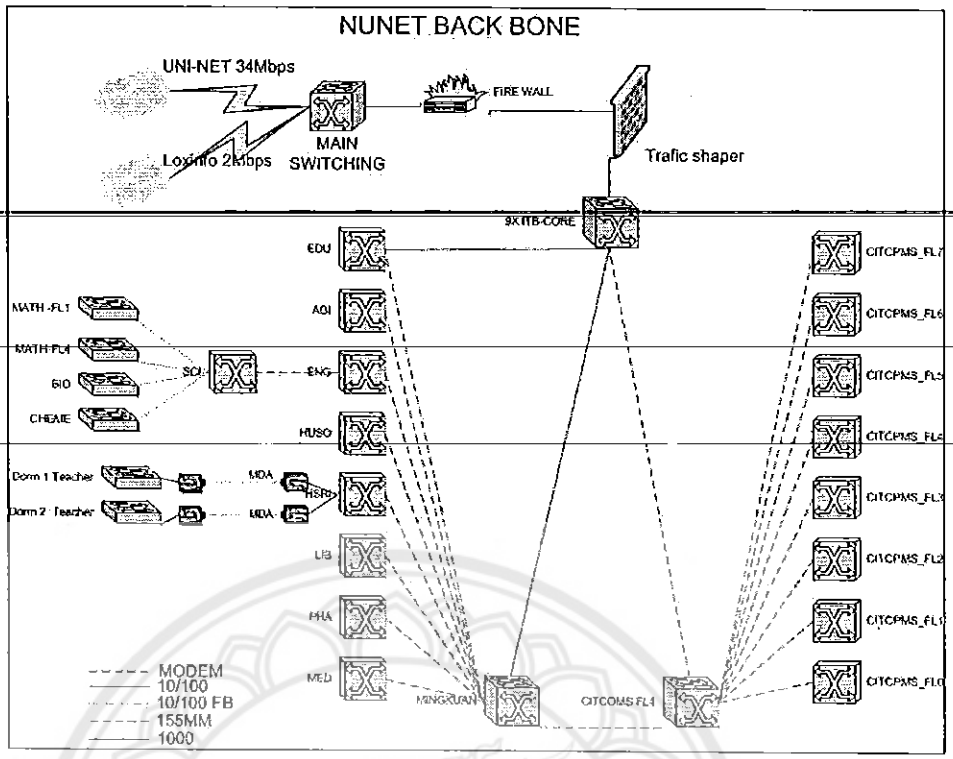
รูปที่ ก-2 โครงสร้างหลัก เน็ตเวิร์ก Main Switch และ Router



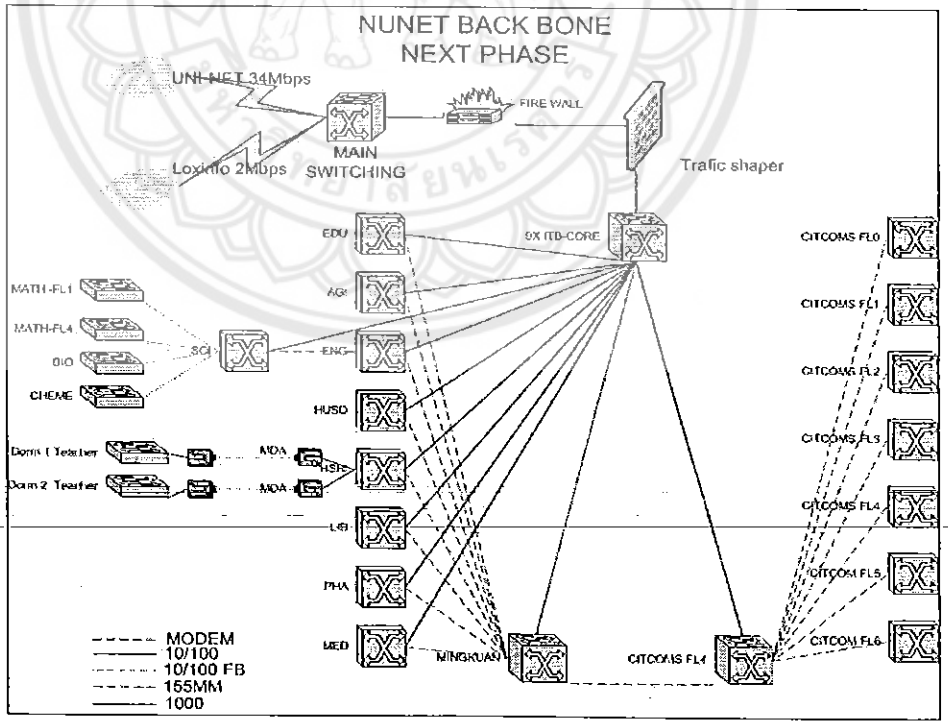
รูปที่ ก-3 NUNET BACK BONE 1



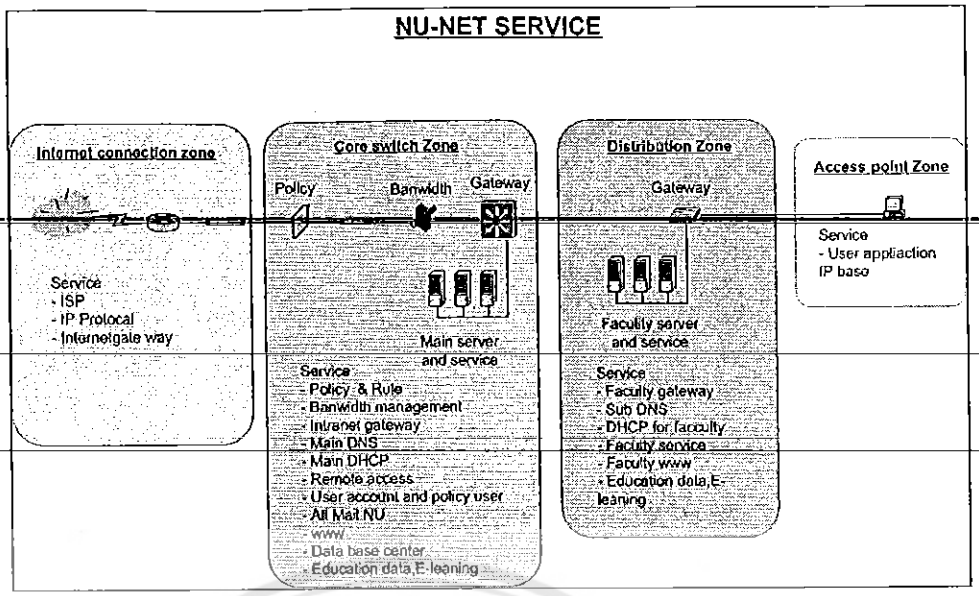
รูปที่ ก-4 NUNET BACK BONE 2



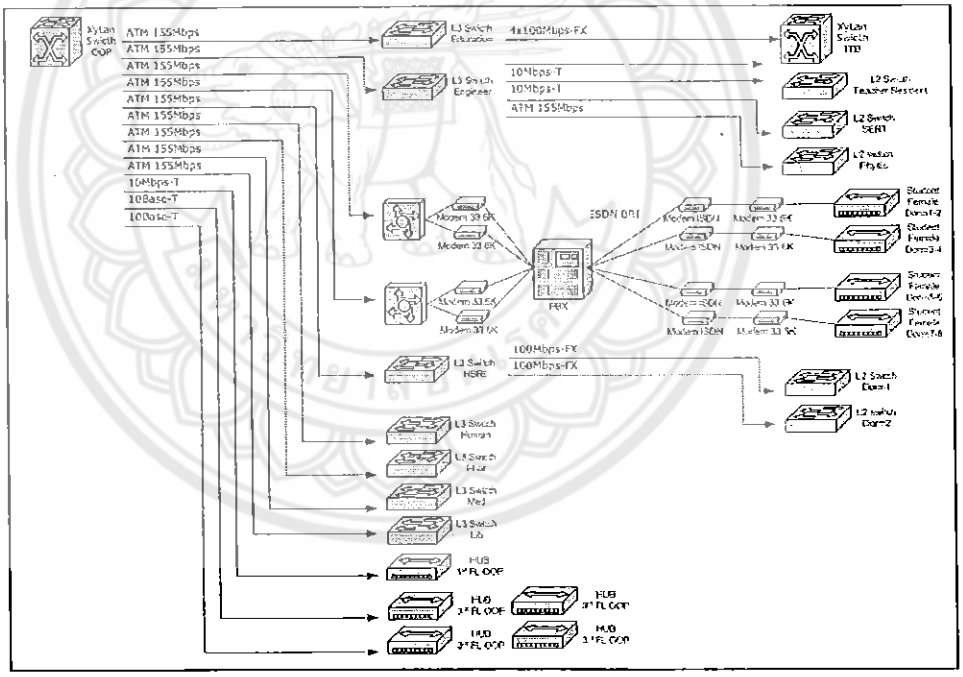
รูปที่ ก-5 NUNET BACK BONE 3



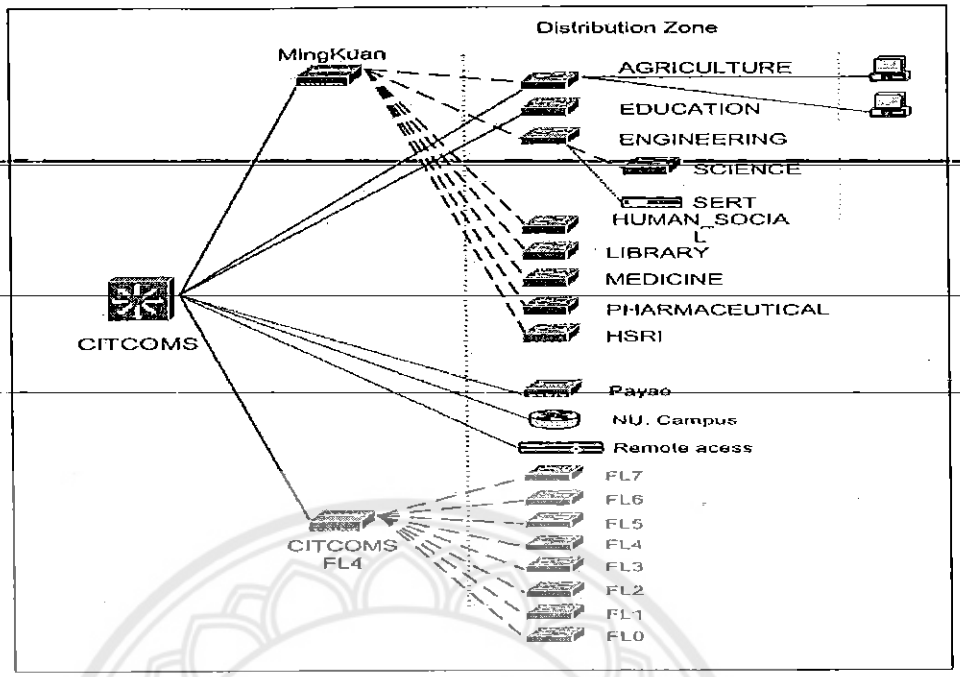
รูปที่ ก-6 NUNET BACK BONE 4



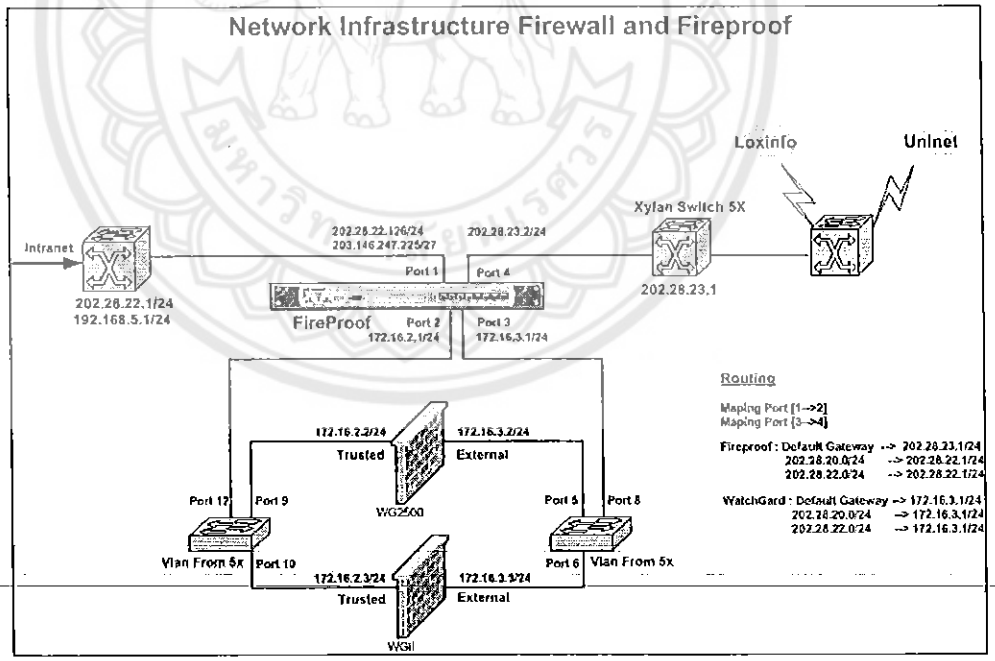
รูปที่ ก-7 NU-NET SERVICE



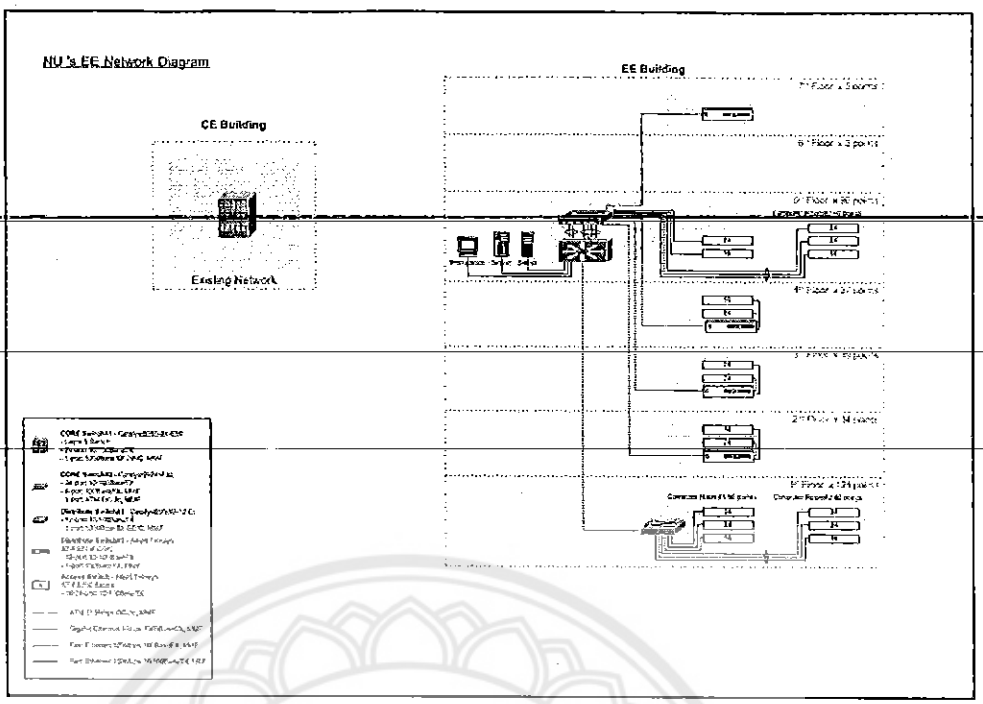
รูปที่ ก-8 OOP distribution network



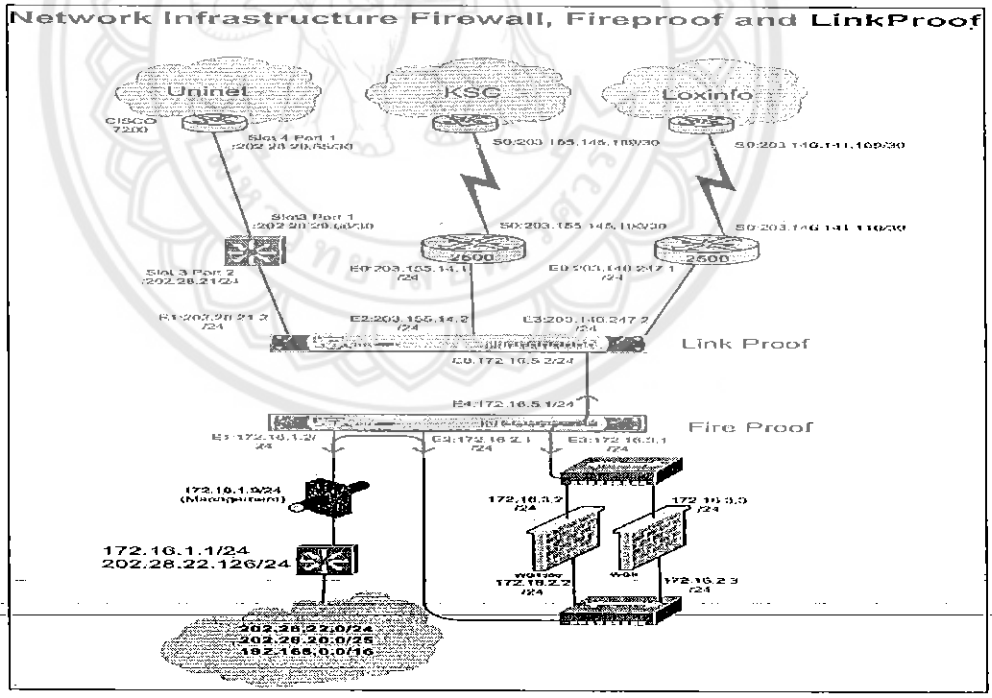
รูปที่ ก-9 การกระจายการเชื่อมต่อไปแต่ละคณะ



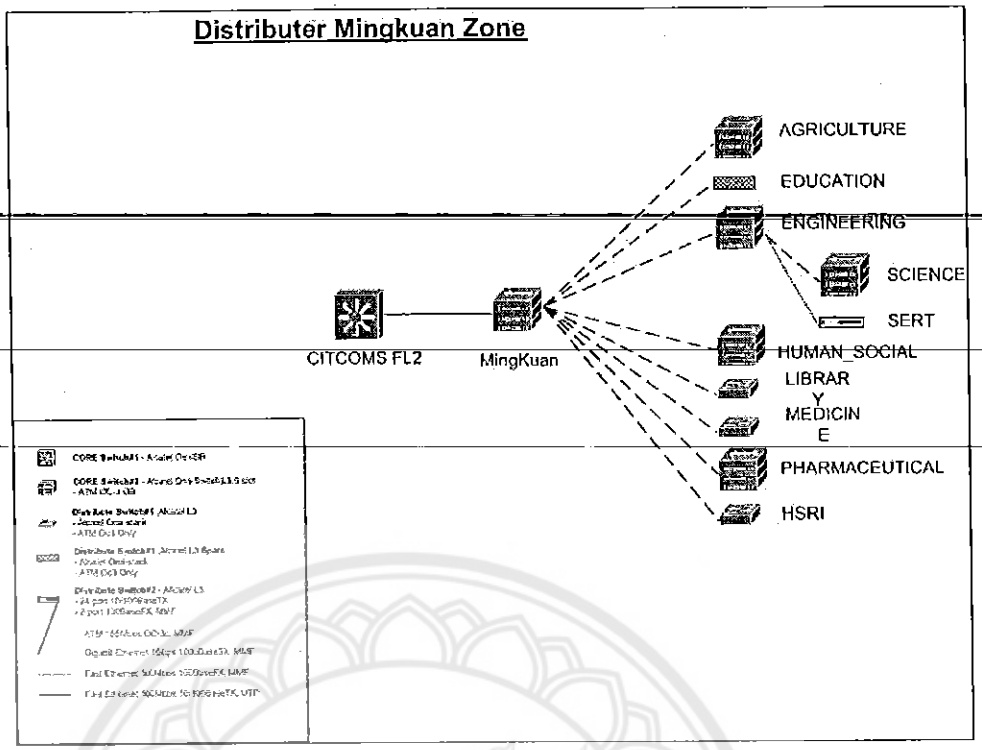
รูปที่ ก-10 Network Infrastructure Firewall and Fireproof



รูปที่ ก-11 โครงสร้างเน็ตเวิร์กของตึกวิศวกรรมศาสตร์ไฟฟ้าและคอมพิวเตอร์



รูปที่ ก-12 Network Infrastructure Firewall, Fireproof and LinkProof



รูปที่ ก- 13 Distributer Mingkuan Zone

ภาคผนวก ข.

คำศัพท์ที่ใช้กันมากเกี่ยวกับ Firewalls

- Bastion host

คือป้อมปราการที่อยู่ในที่สูง เพื่อที่จะสามารถมองเห็นได้ในจุดที่สำคัญ และมีผลกระทบต่อการรักษาระบบ ความปลอดภัย มักมีกำแพงที่แข็งแรง และกองทหารที่เข้มแข็งกว่า ระบบที่รับภาระด้านทานการโจมตีอย่างหนักและติดตั้งในเน็ตเวิร์คเพื่อรับการถูกโจมตี Bastion host มักจะเป็น ส่วนประกอบของ Firewall หรืออาจอยู่ข้างนอก web server หรือระบบที่สามารถเข้าถึงได้โดยทั่วไป ยิ่งกว่านั้นในบางครั้งก็มีโอกาสที่จะทำลาย attacker ได้โดยวิธีการต่างๆ อีกด้วย bastion host เป็นระบบที่ระบุโดย firewall administrator (ผู้ดูแลระบบ firewall) ว่าให้เป็นจุดยุทธศาสตร์สำคัญของความปลอดภัยของระบบ โดยทั่วไป bastion host จะใช้ระบบปฏิบัติการที่ใช้สำหรับจุดประสงค์ทั่วไป (เช่น Unix, VMS, NTและอื่นๆ) และจะมีความสามารถพิเศษในการดูแลรักษาความปลอดภัย โดยอาจเป็น software ที่เพิ่มเติมเข้ามา เป็นต้น

- Damage control

คือการควบคุมการทำลายระบบ เมื่อมีการบุกรุกแล้วจะต้องรู้ว่าเกิดอะไรขึ้นกับระบบ ถ้าหากมีการทำลายก็ต้องแก้ไขได้

- Zones of risk

ความใหญ่โตของระบบระหว่างการทำงาน เป็นเครื่องวัดว่า Zone of risk เป็นอย่างไร

- Failure mode

ถ้ามีการบุกรุกทะลุผ่าน Firewall เข้ามาได้ จะสามารถ ตรวจสอบเจอได้อย่างง่ายดายหรือไม่ ถ้า Firewall ถูกทำลายจะตรวจสอบเจอได้อย่างรวดเร็วหรือไม่ สิ่งสำคัญในการตรวจสอบคือข้อมูล ซึ่งจะต้องรู้ว่าจำเป็นที่จะใช้ข้อมูลมากเท่าใดในการวิเคราะห์การบุกรุกนั้น

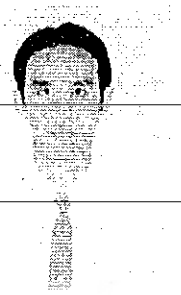
- Ease of use

คือการวัดความใช้ยากของ Firewall

- Stance

หลักการในการปล่อยข้อมูลของFirewall ได้ถูกกำหนดไว้ว่าเป็น “อะไรก็ตามที่ไม่ได้บอกว่าอนุญาต ให้ถือว่า ห้ามผ่าน” หรือ “อะไรก็ตามที่ไม่ได้บอกว่าห้ามผ่าน ให้ถือว่า อนุญาต”

ประวัติผู้เขียนโครงงาน



ชื่อ นายนราพงษ์ ทิพย์สุทะ

ภูมิลำเนา 3/36 ถ.ตากสิน ต.หนองหลวง อ.เมือง จ.ตาก 63000

ประวัติการศึกษา

-จบจากระดับมัธยมศึกษาจากโรงเรียนผดุงปัญญา

-ปัจจุบันกำลังศึกษาในระดับปริญญาตรีชั้นปีที่ 4

สาขาวิศวกรรมไฟฟ้าและคอมพิวเตอร์

มหาวิทยาลัยนเรศวร

E-mail nest_engi@hotmail.com