สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

ระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์

NETWORK SYSTEM SECURITY

T034010

โดย

นายกฤษฎา บุญชูวงศ์

นายศักดา สาครตานันท์

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาอุตสาหกรรมศาสตรบัณฑิต

สาขาวิชาเทคโนโลยีโทรคมนาคม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2541

เลขหมู่.....
เลขทะเบียน.....34010
วัน, เดือน, ปี 27 ก.ย. 2542

เอกสารนี้จัดทำขึ้นไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่อนุญาตให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อปริญญานิพนธ์	ระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์
	NETWORK SYSTEM SECURITY
ชื่อนักศึกษา	นายกฤษฎา บุญชูวงศ์
	นายศักดา สาครตานันท์
อาจารย์ที่ปรึกษา	อาจารย์ มยุรี เลิศเวชกุล
	อาจารย์ พิทักษ์ ธรรมวาริน
ภาควิชา	เทคนิคอุตสาหกรรม
ปีการศึกษา	2541

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปริญญานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรอุตสาหกรรมบัณฑิต

คณะกรรมการสอบปริญญานิพนธ์

.....อาจารย์ที่ปรึกษา
(อ. มยุรี เลิศเวชกุล)

..... กรรมการ
(อ. พิทักษ์ ธรรมวาริน)

..... กรรมการ
( )

..... กรรมการ
( )

..... กรรมการ
( )

ลิขสิทธิ์ของคณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์

นายกฤษฎา บุญชูวงศ์
นายศักดา สาครตานันท์

อาจารย์ มยุรี เลิศเวชกุล
อาจารย์ พิทักษ์ ธรรมวาริน
ปีการศึกษา 2541

บทคัดย่อ

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของโครงงานวิจัย เพื่อศึกษาถึงการใช้โปรแกรมไฟร์วอลเพื่อจำกัดความสามารถในการใช้งานระบบเครือข่ายทั้งส่วนของผู้ใช้จากภายในและผู้ใช้จากภายนอกที่รวมถึงผู้ใช้จากอินเตอร์เน็ตให้ใช้เฉพาะส่วนที่จำเป็น เพื่อลดอัตราความเสี่ยงในด้านของความปลอดภัย ไม่ว่าจะเป็นความปลอดภัยของข้อมูลข่าวสาร หรือความปลอดภัย ของระบบเครือข่าย

โครงงานนี้ใช้การจำลองระบบเครือข่ายคอมพิวเตอร์ขึ้นมาเพื่อการติดตั้งโปรแกรมไฟร์วอล โดยใช้ Microsoft Windows NT4.0 เป็นระบบปฏิบัติการเครือข่ายและใช้ในการศึกษาระบบรักษาความปลอดภัยของการวางเครือข่ายในเบื้องต้นรวมทั้งใช้ในการติดตั้งโปรแกรมไฟร์วอล ในส่วนของโปรแกรมไฟร์วอลนั้นใช้ Cisco Centri Firewall (Evaluation) โดยการกำหนดข้อกำหนดต่างๆ ขึ้นเพื่อใช้ในการทดสอบการใช้งานโปรแกรมไฟร์วอล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

NETWORK SYSTEM SECURITY

Mr. Kridsada Boonchoowong
Mr. Sakda Sakorntanum

Mayuree Lertvachakul
Pitak Thammawarin
1998

Abstract

The objective of this project is to study the usage of Firewall Program. A firewall program is useful to let user to use only the necessity part in order to prevent institution's information and the network system from outside destruction as well as inside attack.

A computer network was set-up to install Cisco Centri Firewall on top of Window NT 4.0 . It is the operation network and it was used to study the preliminary system installation as well as how to define security rule via firewall program.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

สำหรับปริญญานิพนธ์ฉบับนี้ ที่สำเร็จลุล่วงมาได้ก็ต้องขอขอบคุณ หลาย ๆ ฝ่ายที่ช่วยในการสนับสนุนจนสามารถสำเร็จ ขอขอบคุณ อาจารย์มยุรี เลิศเวชกุล อาจารย์พิทักษ์ ธรรมวารินที่ให้คำแนะนำด้วยดี ให้การช่วยเหลือเป็นอย่างมาก ให้คำปรึกษา ขอขอบคุณเพื่อน ๆหลาย ๆ ท่านที่มีส่วนในงานชิ้นนี้ และขอขอบคุณ สำหรับผู้ที่มีส่วนร่วม แต่มิได้เอ่ยนามใจในที่นี้ และที่สำคัญกำลังใจ จาก บิดา มารดา และคนรอบข้างที่ คอยเป็นกำลังใจมาตลอด

คณะผู้จัดทำ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

เรื่อง	หน้า
บทคัดย่อภาษาไทย	ข
บทคัดย่อภาษาอังกฤษ	ค
กิตติกรรมประกาศ	ง
สารบัญ	จ
สารบัญภาพ	ญ
สารบัญตาราง	ฐ
บทที่ 1 บทนำ	1
1.1 ความสำคัญและที่มา	1
1.2 วัตถุประสงค์	2
1.3 ขอบเขตของโครงงาน	2
1.4 วิธีการดำเนินงาน	2
บทที่ 2 รูปแบบเครือข่ายและโปรโตคอล	3
2.1 โดเมนและ workgroup	3
2.1.1 โดเมน	4
2.1.2 ประโยชน์ของการใช้โดเมนบน Window NT	5
2.1.3 ส่วนประกอบของโดเมน	6
2.1.4 โมเดลต่าง ๆของโดเมน	9
2.2 โปรโตคอล	12
2.2.1 TCP/IP	13
2.2.2 IP Address	14
2.2.3 Netmark	16
2.2.4 Subnet	16
2.2.5 Gateway	17
2.2.6 Router	18
บทที่ 3 การรักษาความปลอดภัยบน Window NT	19
3.1 การวางระบบรักษาความปลอดภัย	19
3.2 รูปแบบการจัดระบบเครือข่ายและระบบรักษาความปลอดภัย	19

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

3.2.1 ระบบการจัดการจากศูนย์กลาง 19

3.2.2 ระบบการจัดการแบบกระจาย 20

3.2.3 การจัดการระบบผสม 21

3.3 ประเภทของระบบรักษาความปลอดภัยบนระบบเครือข่าย 22

3.3.1 ระบบรักษาความปลอดภัยทางกายภาพ 22

3.3.2 ระบบรักษาความปลอดภัยสำหรับผู้ใช้ 22

3.3.3 ระบบรักษาความปลอดภัยสำหรับไฟล์ 23

3.3.4 ระบบรักษาความปลอดภัยจากผู้บุกรุก 26

3.4 การกำหนดสภาวะเริ่มต้นใช้งานของผู้ใช้ (User Profile) 27

3.4.1 ประเภทของ User Profile 28

3.4.2 ข้อดีของการใช้ User Profile 29

3.4.3 ข้อด้อยของการใช้ User Profile 30

3.5 Logon Script 30

3.5.1 การสร้าง Logon Script 30

3.5.2 ตัวแปรสำหรับ Logon Script 31

3.5.3 การกำหนด Logon Script 32

3.5.4 การทำซ้ำ Logon Script บนโดเมนชั่น 32

บทที่ 4 ไฟร์วอลล์คืออะไร 34

4.1 สถาปัตยกรรมของไฟร์วอลล์ 35

4.1.1 ดูอัลโฮมโฮสท์ 35

4.1.2 สถาปัตยกรรมแบบสกรีนโฮสท์ 40

4.1.3 สถาปัตยกรรมแบบสกรีนสับเน็ท 42

4.1.4 การปรับเปลี่ยนสถาปัตยกรรมของไฟร์วอลล์ 44

4.2 แบสชั่นโฮสท์ 52

4.2.1หลักการทั่วไป 53

4.2.2แบสชั่นโฮสท์ชนิดพิเศษ 53

4.2.3 การวางตำแหน่งแบสชั่นโฮสท์ 54

4.2.4การเลือกบริการที่จะจัดการโดยแบสชั่นโฮสท์ 54

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

4.2.5 ไม่อนุญาตให้มีบัญชีผู้ใช้บนแบสชั่นโฮสท์ 55

4.2.6 การสร้างแบสชั่นโฮสท์ 55

4.3 แพ็กเก็ตฟิลเตอร์ริ่ง 57

4.3.1 ทำไมต้องใช้แพ็กเก็ตฟิวเตอร์ริ่ง 58

4.3.2 ข้อได้เปรียบของแพ็กเก็ตฟิลเตอร์ริ่ง 59

4.3.3 ข้อเสียเปรียบของแพ็กเก็ตฟิลเตอร์ริ่ง 59

4.3.4 คอนฟิกแพ็กเก็ตฟิลเตอร์ริ่งเราเตอร์ 60

4.3.5 อะไรที่เราเตอร์ทำกับแพ็กเก็ต 60

4.3.6 การส่ง ไอซีเอ็มพีซึ่งเป็นโค้ดที่ผิดพลาด 61

4.3.7 แบบแผนสำหรับกฎของแพ็กเก็ตฟิลเตอร์ริ่ง 61

4.3.8 ฟิวเตอร์ริ่งโดยให้ตำแหน่ง 63

4.3.9 ความเสี่ยงของการทำฟิลเตอร์ 63

4.3.10 ฟิลเตอร์ริ่งโดยการบริการ 65

4.4 ระบบพร็อกซี่ 65

4.4.1 ทำไมต้องใช้พร็อกซี่ 66

4.4.2 ข้อดีของพร็อกซี่ 66

4.4.3 ข้อเสียของพร็อกซี่ 67

4.4.4 พร็อกซี่ทำงานอย่างไร 68

บทที่ 5 การติดตั้งระบบไฟร์วอลล์ 71

5.1 ขั้นตอนก่อนการติดตั้ง 72

5.2 การเตรียมเครื่องคอมพิวเตอร์ 71

5.3 ข้อกำหนดและส่วนที่จำเป็นสำหรับเครื่องที่ใช้ในการติดตั้ง 72

5.4 การลบรายชื่อผู้ใช้คอมพิวเตอร์ 73

5.5 การติดตั้งส่วนประกอบต่าง ๆ ของ Network 74

5.6 วิธีการลบส่วนประกอบทั้งหมดของ Network 75

5.7 การติดตั้งส่วนประกอบต่าง ๆ ของระบบเครือข่ายโดยใช้ 76
Network Setup Wizard

5.8 ความเข้าใจของโปรโตคอลและบริการต่าง ๆ 77

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับใช้ในการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

5.9 การพิสูจน์ว่า TCP/IP สามารถทำงานได้อย่างไร 78

5.10 วิธีทดสอบว่า TCP/IP ได้กำหนดค่าต่าง ๆ ถูกต้อง 78

5.11 การตรวจสอบการเริ่มต้นของระบบ (Boot Setting) 79

5.12 การทำแผ่น back up 79

5.13 สิ่งที่ควรรู้ก่อนเริ่มต้นติดตั้งโปรแกรม 80

5.14 การติดตั้งโปรแกรม Cisco Centri Firewall 80

5.15 ขั้นตอนการติดตั้งโปรแกรม 82

บทที่ 6 ลักษณะการใช้งานของโปรแกรมไฟล์วอลล์ 87

6.1 การกำหนดรายชื่อผู้ดูแลระบบ 87

6.2 การติดตั้งระบบเครือข่าย 88

6.3 การกำหนดบริการที่ใช้บนระบบ 91

6.4 การกำหนดความสามารถ, สิทธิของผู้ใช้ 92

6.5 การกำหนดกฎ, เงื่อนไขความปลอดภัย 93

6.6 การประยุกต์ใช้ กฎ ,เงื่อนไขระบบรักษาความปลอดภัย 94

6.7 การติดตั้ง Reporting และ Monitoring 94

บทที่ 7 ความเข้าใจระบบรักษาความปลอดภัย 97

7.1 ข้อกำหนด นโยบาย ทำงานอย่างไร 97

7.2 Session 98

7.3 ระดับในการตั้งข้อกำหนด 101

7.4 ตัวอย่างการเขียน Policy 102

บทที่ 8 ผลการทดลอง 106

8.1 ระบบเครือข่ายที่ใช้ 106

8.2 การทดลองโปรแกรมไฟร์วอล 107

8.2.1 Inbound Policy 108

8.2.2 Outbound Policy 112

8.2.3 HTTP filter 112

8.2.4 telnet 114

8.3 Report and Log 120

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

บทที่ 9 บทสรุป 128

9.1 แนวทางในการประยุกต์ใช้งาน 128

9.2 ปัญหาและวิธีการแก้ไข 128

9.3 แนวทางในการพัฒนาขึ้นต่อไป 131

บรรณานุกรม 132



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญภาพ

หน้า

รูปที่ 2.1 รูปแบบโดยรวมของระบบโดเมน 7
รูปที่ 2.2 Single Domain model 9
รูปที่ 2.3 Master Domain Model 10
รูปที่ 2.4 Multiple Domain Model 11
รูปที่ 2.5 Complete Trust Domain Model 11
รูปที่ 3.1 ระบบจัดการจากศูนย์กลาง 20
รูปที่ 3.2 รูปแบบการจัดการแบบกระจาย 21
รูปที่ 3.3 ระบบจัดการแบบผสม 21
รูปที่ 3.4 ตัวอย่างโดเมนที่กำหนดตามสถานที่ทำงาน 27
รูปที่ 3.5 ตัวอย่างของโดเมนที่กำหนดตามกลุ่มการทำงานแบบลอจิคอล 27
รูปที่ 3.6 Local Profile 28
รูปที่ 3.7 Roaming Profile 29
รูปที่ 3.8 Mandatory Profile 29
รูปที่ 4.1 แสดง Classic multi-home host 36
รูปที่ 4.2 แสดง Dual-home host 36
รูปที่ 4.3 แสดง Dual home-host ที่เป็นไร้วอลล์ 37
รูปที่ 4.4 แสดงดูอัลโฮมโฮสต์ซึ่งมีผู้ต่อแอปพลิเคชั่น 38
รูปที่ 4.5 แสดงความไม่ปลอดภัยเมื่อผู้ใช้ล็อกอินเข้ามาในดูอัลโฮมโฮสต์ 38
รูปที่ 4.6 แสดงดูอัลโฮมโฮสต์ที่มีผู้ส่งเมล์ (mail forwarder) 39
รูปที่ 4.7 ดูอัลโฮมโฮสต์ที่มีตัวส่งต่อเอกสาร (news forwarder) 40
รูปที่ 4.8 แสดงการคอนฟิก (config) ที่ผิดพลาดบนดูอัลโฮมโฮสต์ไฟร์วอลล์ 40
รูปที่ 4.9 แสดงสถาปัตยกรรมแบบสกรีนโฮสต์ 41
รูปที่ 4.10 สถาปัตยกรรมแบบสกรีนสับเน็ตที่ใช้เราเตอร์ 2 ตัว 42
รูปที่ 4.11 แสดงสถาปัตยกรรมที่ใช้แบสชั่นโฮสต์ 2 ตัว 45
รูปที่ 4.12 แสดงสถาปัตยกรรมโดยรวมเราเตอร์ภายในและเราเตอร์ภายนอก 46
รูปที่ 4.13 แสดงสถาปัตยกรรมที่ทำการรวมแบสชั่นโฮสต์และเราเตอร์ตัวนอก 47
รูปที่ 4.14 แสดงสถาปัตยกรรมที่ทำการรวมแบสชั่นโฮสต์และเราเตอร์ภายใน 48

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญภาพ

หน้า

รูปที่ 4.15 แสดงการใช้เราเตอร์ภายในหลายตัว 49
รูปที่ 4.16 แสดงเครือข่ายภายในหลายเครือข่าย 49
รูปที่ 4.18 แสดงสถาปัตยกรรมที่มีเราเตอร์ภายนอกหลายตัว 50
รูปที่ 4.19 แสดงสถาปัตยกรรมที่ใช้หลาย ๆ เครือข่ายเพอริมิเตอร์ 51
รูปที่ 4.20 แสดงแบสชั่นโฮสต์ที่ทำงานบนหลาย ๆ บริการอินเตอร์เน็ตที่ต่างกัน 55
รูปที่ 4.21 แสดงการติดต่อพีซีโดยใช้สายอนุกรม 56
รูปที่ 4.22 แสดงสิ่งที่เห็นกับการทำงานของพร็อกซี่ 67
รูปที่ 6.1 แสดงรายชื่อ Administrative account 88
รูปที่ 6.2 แสดง Network object 90
รูปที่ 6.3 แสดง Bundled Application 91
รูปที่ 6.4 แสดง menu option 92
รูปที่ 6.5 แสดง User authentication 93
รูปที่ 6.6 แสดง Audit record 95
รูปที่ 6.7 ตารางสรุปบันทึกการรายงาน 96
รูปที่ 7.1 การเปรียบเทียบ Firewall กับเครื่องตอบรับโทรศัพท์อัตโนมัติ 97
รูปที่ 7.2 แสดง Run-time Session 99
รูปที่ 7.3 แสดง Static Session 99
รูปที่ 7.4 แสดงการกำหนด Policy 100
รูปที่ 7.5 High-Level Condition 101
รูปที่ 7.6 ตัวอย่างการเขียน Policy 103
รูปที่ 7.7 ตัวอย่างการเขียน Policy ให้บริการ Netscape 104
รูปที่ 7.8 ตัวอย่างการเขียน Policy 104
รูปที่ 8.1 การจำลองระบบเครือข่าย 106
รูปที่ 8.2 เครือข่ายจำลองที่ใช้ในการทดลอง 107
รูปที่ 8.3 การกำหนด Inbound Policy ให้ใช้บริการ HTTP 108
รูปที่ 8.4 การกำหนด Inbound Policy ให้ใช้ได้เฉพาะบริการ FTP 109
รูปที่ 8.5 การใช้บริการ Netscape Navigator ที่กำหนดการให้บริการโดยไฟร์วอล 109

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 8.6 การกำหนดการให้บริการได้เฉพาะโฮสท์ 110
รูปที่ 8.7 การกำหนดช่วงเวลาในการใช้บริการต่าง ๆ 111
รูปที่ 8.8 การประยุกต์ใช้ Inbound Policy 111
รูปที่ 8.9 การประยุกต์ใช้ Outbound Policy 112
รูปที่ 8.10 การกำหนด HTTP filter 113
รูปที่ 8.11 การปฏิเสธการให้บริการโดย HTTP filter 114
รูปที่ 8.12 ระบบเครือข่ายที่ให้บริการ Telnet 114
รูปที่ 8.13 แสดง Inbound Policy ที่อนุญาตให้ใช้บริการ Telnet 115
รูปที่ 8.14 แสดงการติดต่อขอใช้บริการ telnet 116
รูปที่ 8.15 แสดงการติดต่อในช่วงที่ใช้บริการทั้งสองช่วง 117
รูปที่ 8.16 แสดงการปฏิเสธการใช้บริการ telnet 117
รูปที่ 8.17 การแบ่งเครือข่ายภายในออกเป็นสองช่วง 118
รูปที่ 8.18 การทดสอบการขอใช้บริการ Telnet จากภายนอก 118
รูปที่ 8.19 แสดงการติดต่อใช้บริการ telnet จากภายนอกไฟร์วอล 119
รูปที่ 8.20 แสดงการติดต่อใช้บริการจากภายนอก 120
รูปที่ 8.21 Warning Report 121
รูปที่ 8.22 แสดงรายละเอียดของ Warning Report 121
รูปที่ 8.23 Service report 122
รูปที่ 8.24 รายละเอียดของ HTTP Report 122
รูปที่ 8.25 รายละเอียดของ HTTP Report (ต่อ) 123
รูปที่ 8.26 รายละเอียดของ FTP Report 124
รูปที่ 8.27 รายละเอียดของ FTP Report (ต่อ) 124
รูปที่ 8.28 รายละเอียดของ Telnet Report 125
รูปที่ 8.29 Open Session 126
รูปที่ 8.30 แสดงตัวอย่างของ open sessions ของบริการ HTTP 127
รูปที่ 9.1 แสดงการกำหนด Policy ให้บริการ HTTP 129
รูปที่ 9.2 ทดลองการใช้บริการ HTTP 129
รูปที่ 9.3 แสดงการให้บริการ FTP 130
รูปที่ 9.4 แสดงการปฏิเสธการใช้บริการ FTP 131

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับใช้ในการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญตาราง

	หน้า
ตารางที่ 3.1 Standard Permission สำหรับไดเร็กทอรี่และไฟล์บน NTFS	24
ตารางที่ 3.2 รายละเอียดของ User Profile	28
ตารางที่ 3.3 ตัวแปรที่ใช้งานบน logon script บนเครื่องเอ็นทีได้	31
ตาตางที่ 4.1 ตัวอย่างของการตั้งให้อนุญาตให้การสัญจรไอพีระหว่าง โฮสต์ภายนอกที่เชื่อถือได้และโฮสต์บนเครือข่ายภายใน	62
ตารางที่ 4.2 การป้องกันการเข้ามาของแพ็กเก็ตที่ปลอมตำแหน่งตั้งต้น	63

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 1
บทนำ

ในปัจจุบันระบบเครือข่ายคอมพิวเตอร์มีความสำคัญมากขึ้น เนื่องจากในเกือบทุกองค์กรที่มีอุปกรณ์คอมพิวเตอร์ใช้มากกว่าหนึ่งเครื่อง จะมีการต่อเชื่อมกันเข้าเป็นเครือข่าย ซึ่งเครือข่ายที่มีขนาดใหญ่ และมีผู้ใช้จำนวนมากนั้นการจัดการระบบเครือข่ายเป็นเรื่องสำคัญโดยเฉพาะอย่างยิ่งในส่วนของการรักษาความปลอดภัยของข้อมูลที่เป็นความลับขององค์กร โดยเฉพาะอย่างยิ่งหากมีการต่อระบบเครือข่ายเข้ากับเครือข่ายภายนอกอื่นๆหรือเชื่อมต่อกับระบบเครือข่ายอินเตอร์เน็ตเพราะโอกาสที่จะถูกโจมตีเครือข่ายเป็นเรื่องที่เป็นไปได้ ไม่ว่าวัตถุประสงค์ของการโจมตีเครือข่ายจะเพื่อต้องการขโมยข้อมูลความลับที่มีค่าทางเศรษฐกิจ หรือเพื่อให้เกิดความเสียหายกับระบบเครือข่าย ซึ่งการโจมตีเครือข่าย ดังกล่าวนั้นอาจเกิดจากภายในเครือข่ายขององค์กรเอง หรือจะเป็นการโจมตีมาจากภายนอกเครือข่ายก็ตาม ซึ่งในกรณีเช่นนี้ การป้องกันที่ดีดูเหมือนจะมีความสำคัญมากกว่าการแก้ไขที่ดี ซึ่งเนื่องจากการแก้ไขอาจจะสายเกินไปสำหรับการสูญเสียข้อมูลที่มีความสำคัญไป

ในการป้องกันและแก้ไขการโจมตีจากภายในเครือข่ายขององค์กรเอง จะสามารถทำได้ง่ายกว่า โดยอาศัยการดูแลและจัดการเครือข่ายที่รัดกุมและมีการตรวจสอบอย่างสม่ำเสมอ ส่วนการป้องกันการโจมตีจากภายนอกนั้นจำเป็นต้องอาศัยอุปกรณ์อื่นๆ มาช่วย ซึ่งทางเลือกที่ดีทางหนึ่งก็คือการติดตั้ง Firewall ซึ่งไฟร์วอลล์เองสามารถที่จะกำหนดขอบเขต การใช้งานเครือข่ายภายนอกจากผู้ใช้ที่อยู่ในเครือข่ายภายใน และการเข้าถึงเครือข่ายภายในจากผู้ที่ใช้เครือข่ายภายนอกหรืออินเตอร์เน็ตได้เป็นอย่างดี

วัตถุประสงค์

1. ศึกษาระบบความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์
2. เพื่อศึกษาชนิดของและระบบโครงสร้างของไฟร์วอลล์
3. ศึกษาการเขียนข้อกำหนดและสิทธิในการติดต่อระหว่างเครือข่ายผ่านไฟร์วอลล์
4. ทดลองการทำงานของไฟร์วอลล์เพื่อดูผลกระทบกับระบบเครือข่ายที่มีการติดตั้งระบบไฟร์วอลล์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ขอบเขต

1. สามารถที่จะวางระบบเครือข่ายที่ต้องการสำหรับการติดตั้งไฟร์วอล
2. สามารถที่จะทำการติดตั้งโปรแกรมไฟร์วอลเพื่อใช้งานได้จริง
3. สามารถที่จะกำหนดการใช้งานระบบเครือข่ายผ่านข้อกำหนดของไฟร์วอลในเงื่อนไขต่างๆ ได้
4. สามารถประยุกต์ใช้งานไฟร์วอลในเครือข่ายอื่นๆ ได้

วิธีการดำเนินงาน

วิธีการดำเนินงานแบ่งเป็นสองช่วง คือในช่วงแรกจะเป็นการติดตั้งระบบเครือข่ายจำลอง (จำลองระบบเครือข่ายขึ้นแทนระบบเครือข่ายที่ต่อกับอินเตอร์เน็ตจริง) โดยใช้วินโดว์เอ็นทีเป็นระบบปฏิบัติการเครือข่าย ส่วนในช่วงที่สองจะเป็นการศึกษาและติดตั้งโปรแกรมไฟร์วอลล์จริง เพื่อศึกษาการใช้งานของโปรแกรมและข้อกำหนดต่าง ๆของตัวไฟร์วอลล์

ประโยชน์ที่จะได้รับจากโครงงาน

1. สามารถติดตั้งระบบเครือข่ายที่ใช้วินโดวส์เอ็นทีที่เป็นระบบปฏิบัติการได้จากการจัดเครือข่ายเพื่อติดตั้งไฟร์วอลล์
2. ความรู้ความเข้าใจเกี่ยวกับโครงสร้างพื้นฐานและชนิดของไฟร์วอลล์โดยทั่วไป
3. สามารถติดตั้งและใช้งานไฟร์วอลล์ได้
4. สามารถตั้งข้อกำหนดและเขียนข้อกำหนดต่าง ๆ เพื่อให้สิทธิในการใช้งาน การติดต่อระหว่างเครือข่ายภายในและเครือข่ายภายนอก หรือ Internet ที่ผ่านไฟร์วอลล์ได้สำหรับผู้ใช้งานในเครือข่ายได้
5. สามารถแก้ปัญหาที่เกิดจากการติดตั้งไฟร์วอลล์ลงบนระบบเครือข่ายได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2
รูปแบบเครือข่ายและโปรโตคอล

ในการวางระบบเครือข่ายคอมพิวเตอร์ที่ใช้วินโดวส์เอ็นทีเซิร์ฟเวอร์เป็นระบบปฏิบัติการหลักนั้นนอกจากระบบการรักษาความปลอดภัยของวินโดวส์เอ็นทีเองแล้ว ยังมีส่วนที่ต้องพิจารณาร่วมด้วยอีกหลายประการเช่นโปรโตคอลที่ใช้หรือรูปแบบของระบบเครือข่ายซึ่งจะเป็นส่วนที่สนับสนุนระบบการรักษาความปลอดภัยด้วยเนื่องจากทั้งในเรื่องของโปรโตคอลหรือเครือข่ายที่ใช้นั้นจะมีระดับของความปลอดภัยและความสะดวกในการใช้งานไม่เท่ากันซึ่งหากต้องการระบบรักษาความปลอดภัยที่เข้มงวดอาจจะต้องแลกกับความสะดวกสบายที่จะสูญเสียไปหรือหากต้องการความสะดวกสบาย ระบบรักษาความปลอดภัยที่ได้อาจจะไม่ค่อยเข้มงวดนักเป็นต้นซึ่งอย่างไรก็ตาม ต้องขึ้นอยู่กับความเหมาะสมในด้านต่างๆ รวมทั้งงบประมาณที่มีอยู่ซึ่งต้องพิจารณาต่อไปโดยในบทนี้จะกล่าวถึงการจัดระบบเครือข่ายของวินโดวส์เอ็นทีซึ่งโดยทั่วไประบบเครือข่ายคอมพิวเตอร์ของไมโครซอร์ฟจะแบ่งได้เป็น เวิร์กกรุ๊ป และโดเมน อีกส่วนจะเป็นเรื่องของโปรโตคอลที่วินโดวส์เอ็นที่สนับสนุนซึ่งค่อนข้างหลากหลาย

2.1 Domain และ Workgroup

ในระยะแรกๆของระบบเครือข่ายของระบบเครือข่ายนั้นคอนเซ็ปต์ของเวิร์กกรุฟ (workgroup) ได้ถูกไมโครซอร์ฟนำมาใช้ใน วินโดวส์ฟอร์เวิร์กกรุฟ (Microsoft windows for workgroup) เวิร์กกรุฟเป็นการรวมกลุ่มกันของผู้ใช้ที่ต้องทำงานร่วมกัน หรือต้องการใช้รีซอร์สร่วมกัน โดยปกติคอมพิวเตอร์ทุกๆ เครื่องที่อยู่ในเวิร์กกรุฟจะเท่าเทียมกัน ไม่มีเครื่องคอมพิวเตอร์ที่เป็นศูนย์กลาง ซึ่งเป็นสาเหตุที่เราเรียกเวิร์กกรุฟว่าเป็นระบบเครือข่ายแบบ peer-to-peer

จุดดึงดูดของเวิร์กกรุฟ ก็คือการติดตั้ง (setup) และการดูแลรักษา (maintain) ที่ทำได้ง่าย ผู้ใช้แต่ละคนจะเป็นผู้กำหนดว่าจะแชรีซอร์สไหนและใครจะสามารถใช้รีซอร์สนี้ได้ ผู้ใช้สามารถกำหนดให้ผู้ใช้คนอื่นสามารถเรียกใช้เครื่องพิมพ์ที่แชร์ไว้ ไดรฟ์ซีดีรอม ฮาร์ดดิสก์หรือแม้แต่ไฟล์หรือไดเร็กทอรี่บางตัวได้ แต่เวิร์กกรุฟจะใช้งานได้ยุ่งยากมากขึ้นเมื่อระบบเครือข่ายมีขนาดใหญ่ขึ้น หรือเมื่อต้องการมีการกำหนดระดับในการใช้งานรีซอร์สให้แตกต่างกันตามผู้ใช้หรือกลุ่มของผู้ใช้

เวิร์กกรุฟถูกจำกัดด้วยขนาด เมื่อมีผู้ใช้เพิ่มมากขึ้น จำนวนรีซอร์สก็เพิ่มมากขึ้นด้วยการค้นหารีซอร์สที่ต้องการเริ่มเป็นเรื่องที่ยากมากขึ้น เนื่องจากไม่มีศูนย์กลางอยู่ที่ไหนเลยทำให้การดู

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แลรักษาและการจัดการระบบเป็นเรื่องที่น่าปวดหัวเป็นอย่างยิ่งเพราะการปรับแต่งทั้งหมดต้องทำที่เครื่องคอมพิวเตอร์แต่ละเครื่อง

พาสเวิร์ด (password) ถูกนำมาใช้ในเวิร์กกรุฟเพื่อแยกความแตกต่างของผู้ใช้และควบคุมการใช้งานรีซอร์สต่างๆ แต่เมื่อระบบเครือข่ายแบบ peer-to-peer นี้ใหญ่ขึ้น พาสเวิร์ดก็เริ่มเติบโตตามไปด้วยจนทำให้ระบบเครือข่ายเริ่มมีความซับซ้อนมากขึ้น ผู้ใช้ที่ต้องเข้าถึงรีซอร์สหลายๆ อย่างก็เริ่มที่จะใช้พาสเวิร์ดตัวเดียวกันมากขึ้นเรื่อยๆ หรือไม่ก็เลือกพาสเวิร์ดที่จำได้ง่าย ซึ่งหมายความว่าสามารถจะเดาได้ง่ายด้วย ดังนั้นระบบรักษาความปลอดภัยจึงหละหลวม นอกจากนี้ในกรณีที่มีการเชื่อมต่อผ่านสายโทรศัพท์และมีพนักงานบางคนเชื่อมต่อระบบจากภายนอกที่ไม่ปลอดภัยระดับของพาสเวิร์ดจำเป็นต้องมีการเปลี่ยนแปลงเพื่อให้มีความปลอดภัยเพิ่มมากขึ้น ซึ่งการเปลี่ยนพาสเวิร์ดดังกล่าวนั้น พนักงานทุกคนที่ร่วมกันใช้รีซอร์สนั้นๆ จะต้องได้รับรู้ถึงการเปลี่ยนแปลงทั้งหมด ซึ่งเป็นการเพิ่มภาระให้กับผู้ดูแลระบบ (administrator) เป็นอย่างมาก

จากเหตุผลทั้งหมดนี้เองระบบเครือข่ายแบบ peer-to-peer จึงไม่เหมาะต่อระบบเครือข่ายขนาดใหญ่ หรือระบบเครือข่ายที่ต้องการระบบศูนย์กลาง ระบบเหล่านี้จำเป็นที่จะต้องอาศัยโครงสร้างที่เรียกว่า " โดเมน " ในวินโดวส์เอ็นที่เซิร์ฟเวอร์ ซึ่งมีความยืดหยุ่นมากกว่าและมีวิธีจัดการระบบที่ง่ายกว่าซึ่งทำงานได้เป็นอย่างดีกับระบบที่มีขนาดใหญ่และซับซ้อน

2.1.1 โดเมน(Domain)

โดเมนเป็นหน่วยพื้นฐานในวินโดวส์เอ็นทีซึ่งหมายถึง " กลุ่มของเครื่องคอมพิวเตอร์ที่ฐานข้อมูลร่วมกันและมีกฎในการรักษาความปลอดภัย (security policy) ร่วมกัน " โดเมนเครื่องหนึ่งประกอบไปด้วยเครื่องคอมพิวเตอร์เครื่องหนึ่งที่ทำหน้าที่เป็น primary domain controller (PDC) และเครื่องคอมพิวเตอร์อีกอย่างน้อยหนึ่งเครื่องขึ้นไปที่ทำหน้าที่เป็น backup domain controller (BDC) และเครื่องเวิร์กสเตชั่นอีกอย่างน้อยหนึ่งเครื่อง นอกจากนี้ยังอาจจะมี backup domain controller และเครื่องเซิร์ฟเวอร์รวมทั้งเครื่องเวิร์กสเตชั่นเพิ่มอีกก็ได้

เราอาจกล่าวได้ว่าโดเมนก็คือเวิร์กกรุฟประเภทหนึ่งที่มีเซิร์ฟเวอร์รวมอยู่ด้วย มันยังคงเป็นรูปแบบการจัดกลุ่มผู้ใช้แบบลอจิคอล (หมายถึงไม่มีการแบ่งกลุ่มผู้ใช้ออกเป็นกลุ่มๆ ในทางปฏิบัติจริง) ผู้ใช้เหล่านั้นไม่ต้องการเพียงแค่สายเคเบิลที่ต่อระหว่างเครื่องคอมพิวเตอร์เท่านั้น แต่ยังต้องการใช้ข้อมูลร่วมกันหรือทำงานร่วมกันด้วย เป้าหมายก็ยังคงอยู่ที่การอนุญาตให้ผู้ใช้สามารถใช้ข้อมูลร่วมกันภายในกลุ่มของเขาได้ ผลที่ได้ก็คือสมาชิกในกลุ่มจะสามารถทำงานร่วม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กันได้ง่ายขึ้นและให้ผลงานที่ดีขึ้น จุดแตกต่างของโดเมนก็คือจะมีเซิร์ฟเวอร์อยู่ตัวหนึ่งบนระบบเครือข่าย เพื่อใช้เป็นจุดร่วมจุดเดียวสำหรับการจัดการและควบคุมระบบเครือข่าย

ระบบเครือข่ายบนวินโดวส์เอ็นทีเซิร์ฟเวอร์นั้นอาจจะประกอบไปด้วยโดเมนเพียงชุดเดียวหรือหลายๆ ชุดที่เชื่อมต่อถึงกันก็ได้ บริษัทที่มีระบบเครือข่ายที่มีขนาดใหญ่มากๆ มีเครื่องเวิร์กสเตชั่นเป็นพันๆ เครื่องกระจายอยู่ทั่วโลกนั้น ก็สามารถจัดกลุ่มเวิร์กสเตชั่นแต่ละกลุ่มให้เป็นโดเมนหนึ่งได้พร้อมกับกำหนดระเบียบในการใช้งานที่เฉพาะเจาะจงสำหรับแต่ละโดเมน จุดเด่นของระบบโดเมนก็คือความยืดหยุ่นในการขยายระบบให้ใหญ่ขึ้นหรือเล็กลงได้ง่าย ไม่ว่าจะเป็นส่วนใดส่วนหนึ่งบนระบบเครือข่ายหรือเปลี่ยนแปลงระบบเครือข่ายทั้งหมดโดยสิ้นเชิงก็ตาม

2.1.2 ประโยชน์ของการใช้โดเมนบนวินโดวส์เอ็นที

ประโยชน์ของระบบเครือข่ายแบบโดเมน

- การกำหนดคอนฟิกกูเรชันในการออกแบบจะมีความยืดหยุ่น
- การจัดการระบบเครือข่ายจากศูนย์กลาง
- ความยืดหยุ่นในการเพิ่มผู้ใช้คนใหม่และการเปลี่ยนข้อจำกัดในการใช้งาน (access restriction)
- ฐานข้อมูล user account เพียงชุดเดียว
- ระบบรักษาความปลอดภัยที่เป็นหนึ่งเดียวกันทั้งโดเมน
- การควบคุมการใช้งานไฟล์และไดเร็กทอรี่เท่าที่จำเป็น (Discretionary access control)

ขนาดสูงสุดของเวิร์กกรุฟที่ใช้งานได้ผลนั้นถูกจำกัดจากการดูแลรักษาบนระบบเครือข่ายแบบ peer-to-peer ซึ่งต้องการระบบจัดการแบบเครื่องต่อเครื่อง แต่บนระบบวินโดวส์เอ็นทีเซิร์ฟเวอร์นั้นจะมีการจัดการจากศูนย์กลางที่เดียวเท่านั้น ข้อจำกัดของระบบนี้จะอยู่ที่การแบ่งแผนกในทางธุรกิจมากกว่า บริษัทหนึ่งซึ่งรวมถึงบริษัทขนาดใหญ่ด้วยนั้นสามารถใช้โดเมนเพียงโดเมนเดียวเพื่อจัดการระบบของทั้งบริษัทได้ ถ้าพนักงานในบริษัททำงานในตึกเดียวกันทั้งหมดและไม่มีความจำเป็นจะต้องแบ่งกลุ่มผู้ใช้ตามประเภทรีซอร์สที่เขาต้องการใช้งาน คุณจะสามารถติดตั้งเครื่องคอมพิวเตอร์ได้มากเท่าที่ต้องการ แต่การควบคุมยังคงอยู่ที่จุดเดียว นอกจากนี้ผู้ใช้ทุกคน ซึ่งรวมถึงผู้ใช้คนใหม่ๆ ด้วยก็สามารถใช้งานรีซอร์สของเขาจากเครื่องคอมพิวเตอร์เครื่องใดๆ ที่อยู่บนโดเมนก็ได้ เนื่องจากว่า permission สำหรับการใช้งานไฟล์หรือไดเร็กทอรี่นั้น จะกำหนดให้ผู้ใช้แต่ละคน (หรือกลุ่มของผู้ใช้) ไม่ได้ถูกกำหนดให้เครื่องคอมพิวเตอร์แต่ละเครื่อง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในระบบเครือข่ายแบบโดเมนนั้น ผู้จัดการระบบสามารถทำการแก้ไขระบบจากเครื่องคอมพิวเตอร์เครื่องใดที่อยู่บนเครือข่ายก็ได้ เพียงแต่ล็อกออนเข้าไปบนเอ็นที่เซิร์ฟเวอร์ที่อยู่ในโดเมนนั้น และทำการแก้ไขที่ต้องการ คุณยังสามารถเพิ่มหรือลบผู้ใช้หรือเปลี่ยนข้อจำกัดในการใช้งานด้วยวิธีเดียวกันนี้ด้วย การเปลี่ยนแปลงทั้งหมดจะเกิดขึ้นที่จุดเดียวคือ primary domain controller และการเปลี่ยนแปลงนี้ก็จะถูกส่งต่อให้กับโดเมนอื่นๆ ทั้งหมดในทันที เอ็นทีเซิร์ฟเวอร์จะทำการซิงโครไนซ์ฐานข้อมูลของ user account บนโดเมนให้เองซึ่งช่วยลดภาระของผู้ดูแลระบบที่ต้องคอยตรวจสอบฐานข้อมูลของแต่ละเครื่องเอง

ในระบบเครือข่ายของ Windows for workgrops นั้นจะมีข้อจำกัดในการกำหนดรีซอร์สของเครื่องคอมพิวเตอร์ให้กับผู้ใช้คนอื่นๆ การกำหนดแบบที่ง่ายที่สุดก็คือ ผู้ใช้เครื่องสามารถระบุได้ว่าจะให้ผู้ใช้คนอื่นๆ ใช้รีซอร์สของเครื่องคอมพิวเตอร์นั้นร่วมด้วยหรือไม่ การกำหนดระดับต่อไปนั้นผู้ใช้คนอื่นต้องบอกพาสเวิร์ดสำหรับใช้งานรีซอร์สเครื่องนั้น วิธีเช่นนี้จะจำกัดความสามารถในการควบคุมการใช้งานของผู้ใช้แต่ละคนกับเครื่องแต่ละเครื่องได้ อาจสรุปได้ว่าด้วยวิธีนี้รีซอร์สของเครื่องคอมพิวเตอร์เครื่องหนึ่งจะไม่สามารถใช้งานจากผู้ใช้ที่ไม่รู้พาสเวิร์ดสำหรับเครื่องนั้นได้ นอกจากนี้การที่ผู้ใช้ต้องมีพาสเวิร์ดอันหนึ่งสำหรับใช้งานไฟล์ในแต่ละเครื่อง ก็หมายความว่าเขาจำเป็นที่จะต้องจำพาสเวิร์ดหลายๆ ตัวในการใช้งานกับเครื่องหลายๆ เครื่อง

วินโดวส์เอ็นทีเซิร์ฟเวอร์ได้เพิ่มความยืดหยุ่นให้กับระบบเครือข่ายโดยได้เตรียมการควบคุมการใช้งานตามความจำเป็นมาให้ (discretionary access control) ในระบบนี้จะสามารถกำหนดระดับของการใช้งานของผู้ใช้งานแต่ละคนในการใช้งานรีซอร์สของผู้ใช้งานอีกคนหนึ่งได้อย่างละเอียดละออ โดยจะสามารถกำหนดให้ผู้ใช้ใช้งานแต่ละไฟล์ได้ หรือใช้งานหลายๆ ไฟล์ที่อยู่ในไดเร็กทอรี่หนึ่ง หรือใช้งานได้ทั้งไดเร็กทอรี่เลย เอ็นที่เซิร์ฟเวอร์จะอนุญาตให้คุณเลือกเจาะจงไปในรายละเอียดหรือเลือกแบบคลอบคุมได้ตามต้องการ ความสามารถทั้งหมดนี้ต้องการพาสเวิร์ดเพียงตัวเดียวเท่านั้นตัวอย่างหนึ่งของระบบเอ็นทีเซิร์ฟเวอร์ที่มีระบบควบคุมการใช้งานผู้ใช้ อย่างเช่นโดเมนซึ่งผู้ใช้บางคนสามารถแก้ไขเอกสารที่มีอยู่แล้วฉบับหนึ่งได้ แต่บางคนจะอ่านได้อย่างเดียว และบางคนไม่สามารถดูเอกสารนั้นได้เลย

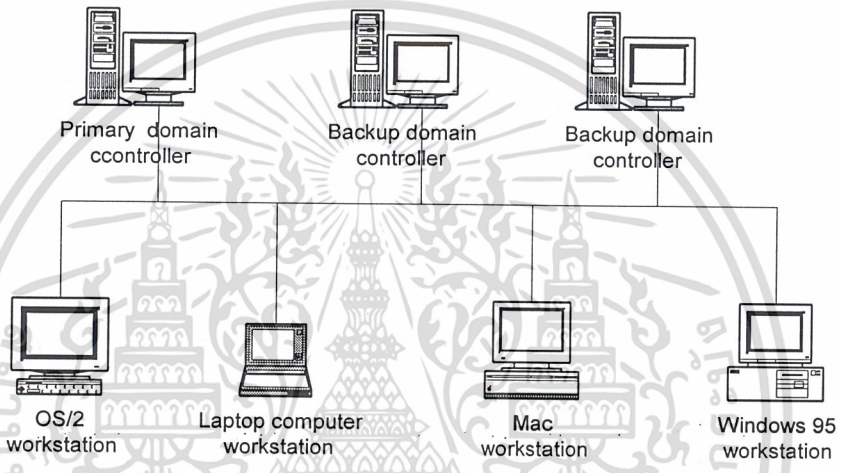
2.1.3 ส่วนประกอบของโดเมน

ตัวอย่างหนึ่งของการกำหนดคอนฟิกกูเรชั่นสำหรับระบบเครือข่ายแบบโดเมนดังแสดงในรปที่ 2.1 ซึ่งประกอบไปด้วยระบบปฏิบัติการ เซิร์ฟเวอร์และเวิร์กสะเตชั่น ซึ่งจะพิจารณาที่ส่วนประกอบของโดเมน และดูว่ามันจะต่อกับภาพรวมได้อย่างไร

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Primary Domain Controller

Primary domain controller เป็นเครื่องคอมพิวเตอร์ที่สำคัญมากที่สุดในโดเมนชุดหนึ่ง เพราะเป็นผู้ที่ออกกฎในการรักษาความปลอดภัย (security policy) ที่ใช้บนโดเมน และเป็นที่สำหรับเก็บรักษาฐานข้อมูล account รวมทั้งอาจถูกใช้เป็นที่รักษารีซอร์สที่ใช้ร่วมกันด้วย การแก้ไขฐานข้อมูล user account นั้นอาจเกิดขึ้นที่ primary domain controller โดยอัตโนมัติ ซึ่งที่นั่นจะเก็บแบ็กอัปฐานข้อมูลที่อ่านได้อย่างเดียวไว้ เมื่อล็อกออนด้วย administrator เข้ามา การแก้ไขทั้งหมดจะถูกกระทำที่ฐานข้อมูลบน primary domain controller ไม่ว่าจะเป็นการ



รูปที่ 2.1 รูปแบบโดยรวมของระบบโดเมน

ล็อกออนที่เครื่อง primary domain controller หรือไม่ สำหรับเครื่องมือที่ใช้จัดการกับ user account นั้นคือ User Manager for Domains

ในกรณีที่ primary domain controller ไม่ทำงาน ผู้ใช้ก็ยังคงสามารถที่จะล็อกออนเข้าระบบเครือข่ายได้ถ้ามี backup domain controller อยู่หนึ่งตัวหรือมากกว่าและมีอย่างน้อยหนึ่งตัวที่ทำงานได้ อย่างไรก็ตามจะไม่สามารถทำการแก้ไขใดๆ ได้กับ user account หรือ group account ในโดเมน เพิ่มผู้ใช้และกลุ่มใหม่ หรือลบผู้ใช้และกลุ่มออกจากโดเมนจนกว่า primary domain controller จะกลับมาใช้งานได้หรือจนกว่าจะเปลี่ยน backup domain controller ตัวใดตัวหนึ่งให้ทำหน้าที่เป็น primary domain controller แทน

Backup Domain Controller

วินโดวส์เอ็นทีเซิร์ฟเวอร์สามารถมี backup domain controller 1 ตัวหรือมากกว่าได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

(ควรจะมีไว้เสมอ) backup domain controller แต่ละตัวจะเก็บก๊อปปี้ของฐานข้อมูล account ไว้และสามารถตรวจสอบผู้ใช้ที่ล็อกออนเข้ามาในระบบได้พร้อมกับมอบอำนาจในการใช้งานรีซอร์สให้กับผู้ใช้คนนั้น วิธีนี้จะช่วยเก็บรักษารีซอร์สสำคัญๆ ที่ต้องใช้งานร่วมกันเผื่อไว้ในกรณีที่ primary domain controller เกิดปัญหาไม่สามารถทำงานได้ ซึ่งจะสามารถแทนที่ primary domain controller ด้วย backup domain controller ตัวใดตัวหนึ่งได้และระบบเครือข่ายก็ยังทำงานตามปกติ (ยกเว้นแต่การเรียกใช้รีซอร์สที่อยู่ที่เซิร์ฟเวอร์ที่ไม่ทำงานจริงๆ) สำหรับในโดเมนขนาดเล็กที่มีผู้ใช้งานจำกัดนั้น ไม่จำเป็นต้องมี backup domain controller แต่เป็นความคิดที่ดีกว่าที่ควรจะเตรียมไว้ เพราะถ้ามี primary domain controller เพียงตัวเดียวแล้ว ระบบเครือข่ายก็จะไม่สามารถทำงานได้เลยถ้าเซิร์ฟเวอร์นั้นเกิดปัญหาขึ้น

เครื่องคอมพิวเตอร์ที่รันวินโดวส์เอ็นที่เซิร์ฟเวอร์สามารถเป็น primary domain controller หรือ backup domain controller หรือไม่เป็นทั้งสองอย่างเลยก็ได้ สำหรับเครื่องเวิร์กสเตชั่นนั้นควรจะใช้ระบบปฏิบัติการตัวอื่นที่ไม่ใช่วินโดวส์เอ็นทีเซิร์ฟเวอร์จะดีกว่า ซึ่งจะช่วยให้ทำงานได้เร็วและใช้งานได้ง่ายขึ้น

เวิร์กสเตชั่น

สำหรับเครื่องเวิร์กสเตชั่นนั้นสามารถรันระบบปฏิบัติการตัวใดตัวหนึ่งต่อไปนี้ คือ เอ็มเอสดอส โอเอส/2 ไมโครซอร์ฟวินโดวส์ 3.x วินโดวส์ฟอร์เวิร์กกรุฟ ไมโครซอร์ฟวินโดวส์ 95 ไมโครซอร์ฟวินโดวส์เอ็นทีเวิร์กสเตชั่น แมคอินทอชโอเอส สำหรับ เอ็มเอสดอส โอเอส/2 ไมโครซอร์ฟวินโดวส์ 3.x แมคอินทอชโอเอส จำเป็นต้องมีซอร์ฟแวร์ระบบเครือข่ายติดตั้งอยู่ด้วย ส่วนระบบอื่นจะมีซอร์ฟแวร์นี้ติดตั้งอยู่ในตัวระบบปฏิบัติการอยู่แล้ว

มีกรณียกเว้นไม่ควรใช้ระบบปฏิบัติการวินโดวส์ 95 เป็นระบบปฏิบัติการบนเครื่องเวิร์กสเตชั่นก็คือการใช้เพื่อพัฒนาซอร์ฟแวร์ เวิร์กสเตชั่นเหล่านี้จะได้ประโยชน์จากเสถียรภาพที่ดีขึ้นและการแบ่งแยกโปรเซสออกจากกันที่มีอยู่ในระบบปฏิบัติการวินโดวส์เอ็นทีเวิร์กสเตชั่น ซึ่งเครื่องเหล่านี้มักจะต้องการหน่วยความจำและพลังในการประมวลผลที่สูงกว่าที่วินโดวส์ 95 ต้องการ และถึงแม้ว่าวินโดวส์ 95 จะทำงานได้ดีกว่า วินโดวส์เวอร์ชั่นก่อนก็ตาม แต่โปรเซสที่มีพฤติกรรมไม่ดีก็สามารถทำให้ระบบ crash ได้ ซึ่งมักไม่เกิดกับวินโดวส์เอ็นที

เวิร์กสเตชั่นบางเครื่องที่อยู่บนระบบเครือข่าย อาจไม่มีความจำเป็นที่จะต้องอยู่ในโดเมนก็ได้ แต่มันยังสามารถอยู่ในเวิร์กกรุฟได้ ทั้งวินโดวส์ 95 เอ็นที่เวิร์กสเตชั่น และวินโดวส์ฟอร์เวิร์กกรุฟ ต่างก็อนุญาตให้ผู้ใช้อยู่เป็นส่วนหนึ่งของ เวิร์กกรุฟ หรือ โดเมนได้ แต่ถ้าต้องการใช้โดเมน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แล้วคอมพิวเตอร์เหล่านั้นจะต้องตั้งคอนฟิกให้ล็อกออนเข้าไปในโดเมน สำหรับเครื่องที่เป็นส่วนหนึ่งบนเวิร์กกรุฟนั้นจะไม่สามารถเข้าถึงฐานข้อมูล user account บนวินโดวส์เอ็นทีเซอร์ฟเวอร์ หรือเรียกใช้รีซอร์สที่ถูกควบคุมโดยฐานข้อมูลชุดนี้ได้

2.1.4 โมเดลต่างๆ ของโดเมน

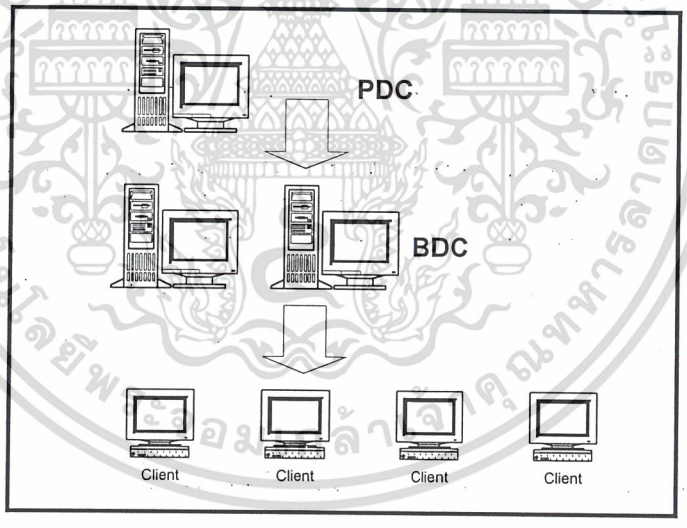
Single domain model เป็นโมเดลที่เหมาะสมกับระบบเครือข่ายขนาดเล็ก ที่ต้องการให้มีการควบคุมแบบรวมศูนย์และให้มีการดูแลระบบที่ง่าย Single model นี้สามารถรองรับ User ได้ถึง 5000 คน แต่นั่นก็ขึ้นกับประสิทธิภาพของเซิร์ฟเวอร์ และจำนวน Backup domain controller ด้วย

ข้อดี - เป็นโมเดลที่เหมาะสมกับเครือข่ายขนาดเล็ก

- Administrator สามารถดูแลเซิร์ฟเวอร์ทุกตัวที่มีอยู่ในระบบเครือข่ายได้

ข้อเสีย - มีประสิทธิภาพต่ำเมื่อ User เพิ่มขึ้น

- ไม่รองรับการจัดกลุ่มของ User ออกเป็น Department

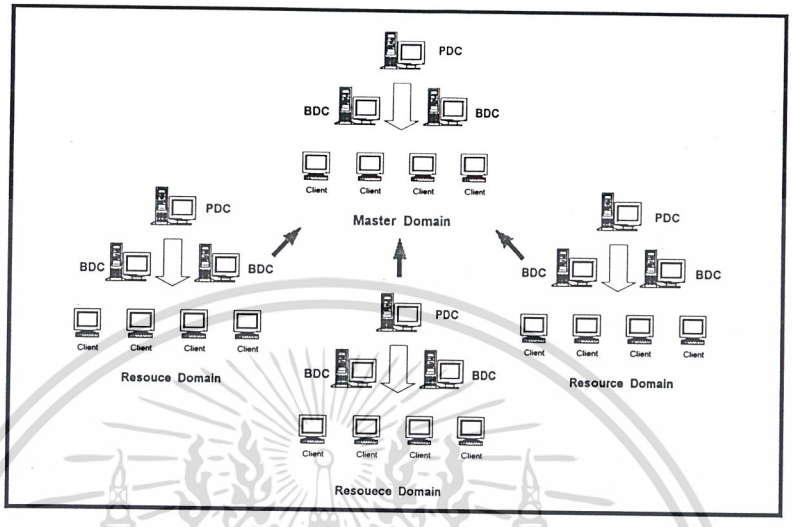


รูปที่ 2.2 Single Domain Model

Master domain model เหมาะสำหรับองค์กรขนาดใหญ่ที่ Administrator ไม่สามารถที่จะดูแลได้ทั่วถึงจึงทำการแยกออกเป็นโดเมนย่อยๆ ตามหน่วยงานของตน แต่ละโดเมนก็มี Administrator เป็นของตนเอง และยังมีการควบคุมแบบรวมศูนย์ ในโมเดลนี้จะมีโดเมนหนึ่งที่เราเรียกว่า Master Domain ซึ่งจะเป็นโดเมนที่จะได้รับความไว้วางใจจากโดเมนอื่น ทำให้ Master Domain สามารถเข้าไปใช้ทรัพยากรในโดเมนอื่นได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หน่วยงานที่เหมาะสมจะดูแล Master Domain ก็คือ MIS เพราะ MIS จะเป็นผู้ควบคุมคอมพิวเตอร์ในองค์กรทั้งหมดและทำให้ง่ายต่อการวางแผนการบริหารงานและควบคุมระบบเครือข่ายอีกด้วย



รูปที่ 2.3 Master Domain Model

จากรูปที่ 2.3 จะเห็นว่า User ที่ล็อกออนเข้า Master Domain จะสามารถเข้าใช้ทรัพยากรของ Trusting Domain (Resource Domain) ตามที่ได้สร้างความสัมพันธ์ระหว่างโดเมน

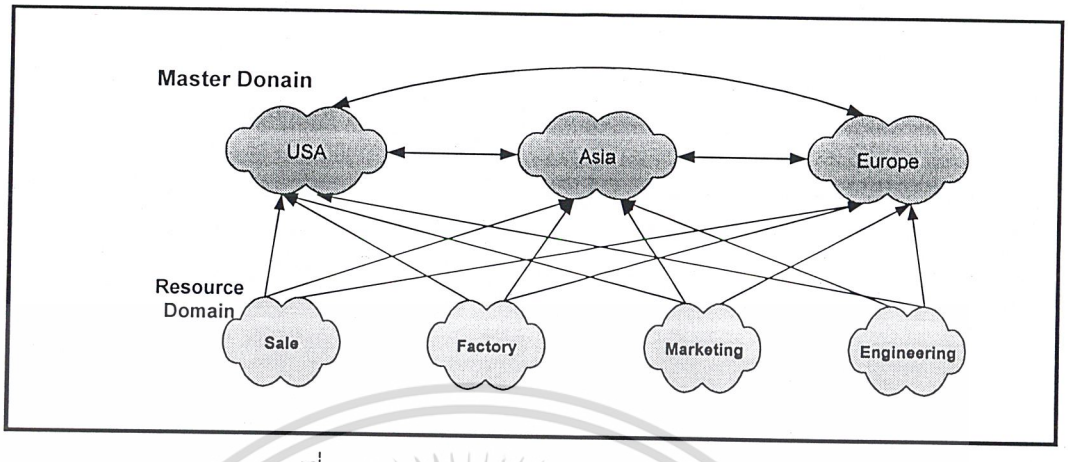
ข้อดี - เหมาะสำหรับองค์กรที่มี User ประมาณ 10000 คน

- Global group จะถูกกำหนดเพียงครั้งเดียว
- มีการควบคุม User แบบรวมศูนย์
- แต่ละโดเมนมี Administrator ของตนเองทำให้สะดวกต่อการจัด User ในโดเมน

ข้อเสีย - มีประสิทธิภาพต่ำเมื่อ User เพิ่มมากขึ้น

Multiple Master Domain Model ใน model นี้จะประกอบไปด้วย Master Domain หลายๆ โดเมนและ Trusting Domain โดยแต่ละ Master Domain จะมีความสัมพันธ์กันแบบ Two way relationship ระหว่างกัน ส่วนTrusting Domain จะมีความสัมพันธ์แบบ One way relationship กับ Master Domain

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



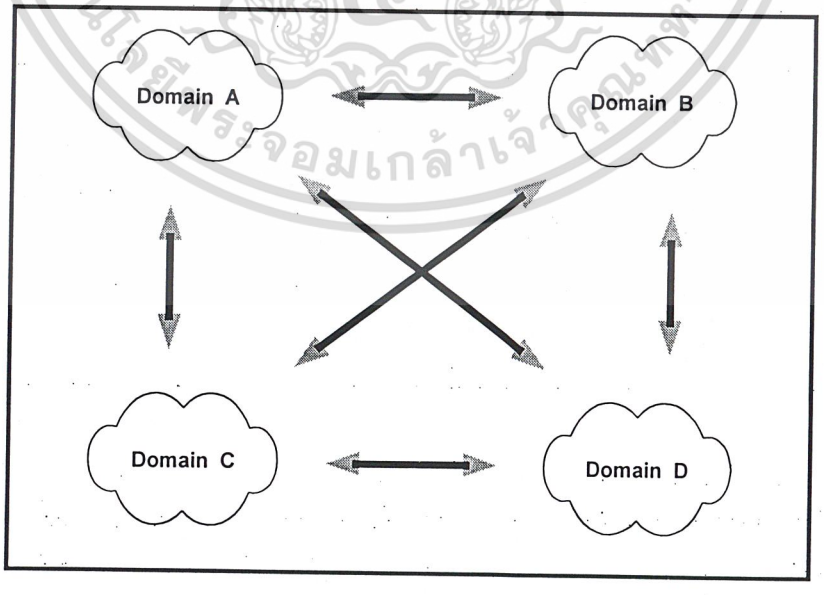
รูปที่ 2.4 Multiple Master Domain Model

ข้อดี - มีความสามารถในการขยายเครือข่ายมากกว่า

- เหมาะสำหรับองค์กรขนาดกลางที่มี User ประมาณ 40000 คน
- แต่ละโดเมนมี Administrator ของตนเองทำให้เกิดความคล่องตัวในการทำงาน

ข้อเสีย - มีประสิทธิภาพต่ำเมื่อ User เพิ่มมากขึ้น

- Administrator ต้องมี Account อยู่ในหลายๆ โดเมนเพื่อคอยดูแลโดเมนต่างๆ



รูปที่ 2.5 Complete Trust Domain Model

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Complete Trust Domain Model เป็นโมเดลที่ถูกใช้งานในองค์กรขนาดใหญ่ที่มีหลายๆ โดเมน และต้องการให้ทุกๆ โดเมนมีการสร้างความสัมพันธ์ซึ่งกันและกันทั้งหมด

ข้อดี - เหมาะสำหรับองค์กรขนาดใหญ่ที่ไม่มีผู้ดูแลระบบส่วนกลาง

- User สามารถล็อกออนเข้าไปในโดเมนของตนเองได้จากที่ใดก็ได้

ข้อเสีย - ไม่มีการควบคุมแบบรวมศูนย์ในโมเดลแบบนี้

- ยากต่อการดูแล Trust Relationship

2.2 โปรโตคอล

โปรโตคอล (protocol)ที่วินโดวส์ เอ็นที เวอร์ชั่น 4 (Windows NT version 4) สนับสนุนนั้นมีหลายชนิด นอกจาก สามตัวหลักอย่าง TCP/IP ,IPX/SPX และ NetBUEI ซึ่งโปรโตคอลที่วินโดวส์ เอ็นที่4สนับสนุนในการใช้งานเครือข่ายประเภทต่างดังเช่น

TCP/IP เป็นโปรโตคอลที่มีดีฟอลต์ (default) อยู่แล้ว และเหมาะสำหรับในการเชื่อมต่อวินโดวส์เอ็นทีเข้ากับระบบเครือข่ายด้วย

IPX/SPX เป็นโปรโตคอลดีฟอลต์เช่นกัน และเป็นโปรโตคอลที่ถูกใช้อยู่โดย โนเวลเน็ตแวร์

NetBEUI เป็นโปรโตคอลที่ใช้ในวินโดวส์ฟอร์เวิร์กกรุ๊ฟ (windows for workgroup) , Microsoft Lanmanager และวินโดวส์เอ็นทีเวอร์ชั่นก่อน

Apple Talk เป็นโปรโตคอลที่ช่วยให้ วินโดวส์ เอ็นทีเซิร์ฟเวอร์ (server) สามารถติดต่อกับเครื่องหรือระบบเครือข่ายของแมคอินทอชได้

DLC (DataLink Control) เป็นโปรโตคอลที่ช่วยให้ วินโดวส์ เอ็นทีเซิร์ฟเวอร์ สามารถติดต่อกับเครื่องเมนเฟรมของ IBM และเน็ตเวอร์คปริ๊นเตอร์ของ Hewlett-packard ได้

PPTP (Point-to-Point Tunneling Protocol) เป็นโปรโตคอลใหม่ของไมโครซอฟต์ที่สนับสนุน Virtual Private Network บนอินเตอร์เน็ต

ซึ่งจะเห็นได้ว่า วินโดวส์ เอ็นที สนับสนุนโปรโตคอลหลายชนิด ทำให้เราสามารถที่จะเชื่อมต่อระบบเครือข่ายของวินโดวส์ เอ็นทีเข้ากับเครือข่ายต่างๆ ได้อย่างหลากหลาย แต่ในบทนี้จะขอเน้นในเรื่องของ TCP/IP เนื่องจากเป็นโปรโตคอลที่ถูกใช้อย่างกว้างขวางทั้งในระบบเครือข่ายและในอินเตอร์เน็ต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2.1 TCP/IP

TCP/IP ย่อมาจาก (Transmission Control Protocol / Internet Protocol) ซึ่งจริงๆ แล้วเป็นชุดของโปรโตคอลที่ทำงานร่วมกันเพื่อช่วยให้การติดต่อสื่อสารกันระหว่างเครื่องคอมพิวเตอร์ประสบความสำเร็จ

Internet Protocol (IP)

IP เป็นโปรโตคอลระดับล่างที่ถูกออกแบบมาเพื่อใช้ในระบบที่เชื่อมต่อกันของระบบเครือข่ายที่สื่อสารบนคอมพิวเตอร์โดยใช้ " packet-switch" ทำหน้าที่เตรียมส่งแพ็กเกจให้กับส่วนประกอบอื่นๆ ในชุด TCP/IP โดยมันไม่ได้ถูกออกแบบมาให้ทำงานที่นอกเหนือจากฟังก์ชั่นหลักของมัน ซึ่งก็คือการส่งแพ็กเกจของบิต (เรียกว่าdatagram) จากจุด A ไปยังจุด B บนสายในระบบเครือข่ายไดๆ โดยมันจะพยายามส่งแพ็กเกจด้วยความพยายามอย่างเต็มที่ให้ถึงเครื่องปลายทางอย่างถูกต้องให้ได้ มันเตรียม checksum ไว้เป็นส่วนหนึ่งของแพ็กเกจด้วยเพื่อให้แน่ใจว่าข้อมูลในส่วนเฮดเดอร์ของแพ็กเกจนั้นสมบูรณ์ครบถ้วนแต่ตัวข้อมูลเองอาจไม่ครบถ้วนสมบูรณ์ก็ได้ เนื่องจากมันไม่รู้อะไรเกี่ยวกับ datagram ที่มันส่งเลยซึ่งทำให้มันไม่รับประกันว่าลำดับในการรับส่งแพ็กเกจนั้นถูกต้องหรือแพ็กเกจจะถึงจุดหมายปลายทางที่ต้องการหรือไม่ ซึ่งหน้าที่เหล่านี้จะปล่อยให้เป็นหน้าที่ของ โปรโตคอลอื่นที่อยู่ใน TCP/IP จัดการ

Transmission Control Protocol (TCP)

TCP เป็นโปรโตคอลหลักใน TCP/IP ซึ่งเป็นโปรโตคอลแบบ conection-base ซึ่งหมายความว่าเมื่อแพ็กเกจหนึ่งได้ถูกส่งระหว่างเครื่องหลายๆ เครื่อง มันจะถูกส่งไปยังเครื่องปลายทางที่ถูกเจาะจงนั้นๆ ตามลำดับอย่างถูกต้องและสมบูรณ์ครบถ้วน ซึ่งหากแพ็กเกจดังกล่าวนั้นถึงปลายทางอย่างไม่ถูกต้องหรือไม่ตามลำดับแล้ว TCP จะมีการร้องขอให้มีการส่งแพ็กเกจอีกครั้งให้ถูกต้อง

TCP ได้ถูกออกแบบมาเพื่อเป็น " โปรโตคอล ที่เชื่อถือได้ เป็น connection oriented , end-to-end ซึ่งอยู่ในระดับชั้นของโปรโตคอลที่สนับสนุน multi-network application" ซึ่งแต่ละคำที่กล่าวถึงมีความหมายคือ

Connection oriented TCP ได้เตรียมการสื่อสารระหว่างแพ็กเกจของบิตระหว่างจุดสองจุดและได้เชื่อมจุดสองจุดนั้นเข้าด้วยกัน มันจะส่ง datagram โดยเฉพาะจากเครื่องคอมพิวเตอร์เครื่องหนึ่งหรืออุปกรณ์ซนิดอื่นให้กับเครื่องคอมพิวเตอร์หรืออุปกรณ์อีกตัวหนึ่ง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

End-to-end TCP packets นั้นมี endpoint ที่ออกแบบมาเฉพาะเก็บอยู่ในแพ็กเกจ และแพ็กเกจเหล่านั้นจะถูกส่งผ่านไปตามสาย และจะถูกเพิกเฉยจาก endpoint อื่นๆ ยกเว้น endpoint จริงๆ ของแพ็กเกจและอุปกรณ์ที่ต้องการแพ็กเกจนั้นโดยตรง

เชื่อถือได้ ซึ่งนับเป็นคุณสมบัติที่สำคัญของ TCP เมื่อโปรแกรมตัวหนึ่งเช่น ftp ใช้ TCP เป็นโปรโตคอลของมัน TCP/IP จะเป็นผู้รับผิดชอบในเรื่องความน่าเชื่อถือของการสื่อสารให้เอง มันช่วยให้การติดต่อระหว่างโปรเซสมั่นใจได้ว่าแพ็กเกจที่ตนส่งไปนั้นไม่เพียงแต่ถึงจุดหมายเท่านั้น แต่ยังถึงเหมือนกับในลำดับที่ส่งอีกด้วย ถ้าแพ็กเกจเกิดหายไป โปรโตคอลจะส่งข้อมูลกลับไปที่อุปกรณ์ที่เป็นตัวส่งให้ส่งข้อมูลนั้นกลับมาอีกที

2.2.2 IP Address

นอกจากใช้ในการเตรียมการส่งแพ็กเกจในระดับล่างแล้วIP Address ที่ใช้บนอินเตอร์เน็ตหรือบนเครื่องคอมพิวเตอร์ในระบบเครือข่ายก็เปรียบได้เสมือนบ้านเลขที่ที่ระบุที่หน้าซองจดหมายในการส่งจดหมายถึงผู้รับซึ่ง TCP/IPใช้ IP addressในการอ้างถึงเครื่องคอมพิวเตอร์ในอินเตอร์เน็ตหรือบนเครือข่าย โดยการใช้การอ้างตำแหน่งแบบ 32 บิตโดยใช้ตัวเลขฐานแปด 4 หลักที่แยกกันด้วยจุดในลักษณะ w.x.y.z โดยที่ตัวแปรแต่ละตัวจะมีค่าเป็นตัวเลขตั้งแต่ 1 ถึง 254 สำหรับค่าอีกสองค่า (0 และ 255) นั้นถูกสงวนไว้ใช้เป็นอินเตอร์เน็ตแอดเดรสโดยเฉพาะ

ระบบเครือข่ายสามารถแบ่งได้เป็น 3 คลาสด้วยกันคือ A,B และ C แต่ละคลาสจะแบ่งระบบเครือข่ายตามขนาดและความซับซ้อนของมัน ซึ่งการกำหนดการใช้งาน IP Address นั้นจะถูกควบคุมจากองค์การ Internet Network Information Center (Inter NIC) ในตอนแรกนั้นองค์การนี้ถูกจัดการและควบคุมโดยรัฐบาลของประเทศสหรัฐอเมริกา แต่ในปัจจุบันได้ถูกจัดการโดยองค์กรการค้าที่แยกต่างหากแล้ว

ระบบเครือข่ายคลาส A

ระบบเครือข่ายคลาส A จะมีแอดเดรสเริ่มต้นตั้งแต่ 0 จนถึง 127 ซึ่งใช้แทนในส่วนของแอดเดรสที่เป็น w ตัวแรก และเป็นส่วนของแอดเดรสของเครือข่าย ส่วนที่เหลือของแอดเดรสจะเป็นแอดเดรสของอุปกรณ์โลคอลจริงๆ บนระบบเครือข่ายนั้น อย่างไรก็ตามที่แอดเดรส 127 จะถูกสงวนเก็บไว้สำหรับฟังก์ชั่นพิเศษและไม่สามารถใช้งานได้ ซึ่งหมายความว่าจะสามารถมีเครือข่ายคลาส A ได้ 127 เครือข่ายในโลก และแต่ละระบบจะมีอุปกรณ์ที่ไม่ซ้ำกันได้ถึง 16 ล้านตัว ซึ่งจะเห็นได้ว่าเป็นระบบเครือข่ายที่ใหญ่จริงๆ ระบบเครือข่ายคลาส A ได้กำหนดให้กับบริษัทต่างๆ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จนหมดมานานแล้วอาทิเช่น Department of Defense , Stanford University และ Hewlett-Packard

ระบบเครือข่ายคลาส B

ระบบเครือข่ายคลาส B มีแอดเดรสเริ่มตั้งแต่ 128 จนถึง 191 ซึ่งใช้แทนในส่วนของแอดเดรสที่เป็นตัว w ตัวแรกและเป็นส่วนของแอดเดรสของเครือข่าย ส่วนที่เหลือของแอดเดรสจะเป็นแอดเดรสของอุปกรณ์โลคอลจริงๆ บนระบบเครือข่ายนั้นมีเครือข่ายคลาส B อยู่ 16,000 เครือข่าย ในแต่ละเครือข่ายจะมีแอดเดรสที่ไม่ซ้ำกันอยู่ 64,000 แอดเดรส ก็ยังนับว่าเป็นระบบเครือข่ายที่ใหญ่ ส่วนใหญ่แล้วเครือข่ายในคลาสนี้ได้ถูกกำหนดให้กับองค์กรหรือบริษัทใหญ่ๆ หมดนานแล้วเช่นกันอาทิเช่น Toyota Motor Corporation และลาดกระบังเองก็ใช้เครือข่ายในระดับนี้ด้วยเช่นกัน แอดเดรสในคลาส B นี้จำนวนมากได้ถูกแบ่งย่อยให้เล็กลงและกำหนดให้ใช้ใหม่ อย่างเช่นที่ Large Internet service provider (ISP) ได้ใช้เทคนิคนี้ในการใช้งานแอดเดรสให้มีประสิทธิภาพยิ่งขึ้น

ระบบเครือข่ายคลาส C

ระบบเครือข่ายคลาส C มีแอดเดรสเริ่มต้นที่ 192 จนถึง 223 ซึ่งใช้แทนในส่วนของแอดเดรสที่เป็นตัว w ตัวแรกและเป็นส่วนของแอดเดรสของเครือข่าย ส่วนที่เหลือของแอดเดรสจะเป็นแอดเดรสของอุปกรณ์โลคอลจริงๆ บนระบบเครือข่ายนั้นๆ ระบบเครือข่ายคลาส C นี้มีอยู่ประมาณ 2 ล้านเครือข่าย และแต่ละเครือข่ายจะมีอุปกรณ์ได้สูงสุด 254 ตัว ซึ่งเป็นขนาดที่พอเพียงสำหรับธุรกิจขนาดเล็กหรือระบบเครือข่ายในแผนกแต่ยากที่จะเพียงพอกับระบบเครือข่ายในองค์กรที่มีขนาดใหญ่

ระบบเครือข่ายคลาส D และคลาส E

แอดเดรสในคลาส D จะมีแอดเดรสเริ่มต้นตั้งแต่ 224 ถึง 239 ซึ่งใช้แทนในส่วนของแอดเดรสที่เป็นตัว w ตัวแรกสำหรับคลาสนี้จะใช้เป็น multicast address ส่วนคลาส E จะมีแอดเดรสเริ่มต้นตั้งแต่ 240 ถึง 247 ซึ่งใช้แทนในส่วนของแอดเดรสที่เป็นตัว w ซึ่งแอดเดรสนี้ส่วนใหญ่จะถูกสงวนไว้ใช้งานในอนาคต

ในระบบเครือข่ายที่ต่ออยู่กับอินเตอร์เน็ตนั้น IP Address ที่ใช้นั้นต้องไม่ซ้ำกันยกเว้นในกรณีที่ระบบเครือข่ายนั้นไม่ได้ต่อกับอินเตอร์เน็ต ซึ่งแน่นอนว่าหมายเลข IP ที่ยังไม่ถูกใช้งานเหลืออยู่น้อยเต็มที ในช่วงปลายทศวรรษที่ 1960 ที่อินเตอร์เน็ตถูกสร้างขึ้นนั้น จำนวนที่กำหนด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

นี้ดูเหมือนจะมากเกินพอที่จะใช้จัดการกับเครื่องคอมพิวเตอร์ที่มีอยู่ในโลกนี้ทั้งหมด ซึ่งรูปแบบในการกำหนดตัวเลขนี้สามารถกำหนดแอดเดรสให้กับเครื่องคอมพิวเตอร์ที่ไม้ซ้ำกันได้ถึง 4 พันล้านเครื่องแม้จะนำมาใช้งานไม่กี่ร้อยล้านเครื่องก็ตาม (ก็เช่นเดียวกับคอมพิวเตอร์ในยุคแรกนั่นเองที่มีหน่วยความจำเพียง 640 k ก็เพียงพอ) ซึ่งก็นับว่าเป็นจำนวนเครื่องคอมพิวเตอร์ที่มากมายมหาสารเมื่อมองจาก ทศวรรษที่ 1960 แต่อย่างไรก็ตามการเติบโตของอินเตอร์เน็ตอย่างรวดเร็วในปัจจุบันทำให้จำเป็นต้องมีการเปลี่ยนแปลงการระบุหมายเลข IP ในรูปแบบใหม่แทนที่การอ้าง IP แบบ 32 บิตในปัจจุบันซึ่งวิธีในการแก้ปัญหาดังกล่าวได้มีการใช้วิธีอิงไปที่โปรโตคอล IP รุ่นต่อไปที่เรียกกันว่า Ipv6 (เวอร์ชั่น 6 ของ Internet Protocol) ซึ่งจะกำหนด IP address ขนาด 128 บิตซึ่งจะคอมแพลตทิเบิลกับการใช้งานของ ICP/IP ในปัจจุบัน (เวอร์ชั่น 4 หรือ Ipv4) แต่จะให้พื้นที่แอดเดรสเพิ่มขึ้นอย่างมาก รวมทั้งได้รวบรวมข้อมูลเพิ่มเติมเพื่อช่วยให้การหาเส้นทางและการจัดการกับอุปกรณ์โมบายด์ดีขึ้นด้วย โดยไม่ต้องกังวลว่าจะไม่สามารถใช้งานได้กับระบบ IP เดิม(Ipv4)เนื่องจากเป็นการพัฒนา (evolutionary)ไม่ใช่การปฏิวัติ(revolutionary)ซึ่งเราสามารถที่จะค่อยๆ ทำการเปลี่ยนแปลงได้

2.2.3 Netmask

Netmask เป็นกลไกสำคัญที่ TCP/IP ใช้เพื่อจำกัดจำนวนแอดเดรสที่เป็นไปได้ที่เครื่องๆ หนึ่งจะสามารถที่จะจัดการได้ที่เวลาใดเวลาหนึ่ง netmask ก็คือการอำพราง (masking) หรือซ่อนส่วนของระบบเครือข่ายส่วนหนึ่งจากส่วนอื่นๆ ของระบบเครือข่าย ซึ่ง netmask ของแอดเดรสในระบบเครือข่ายจะเป็นตัวกำหนดว่าจะมีจำนวน IP address มากเท่าใดที่จะมองเห็นจากเครื่องอื่นๆ ว่าเป็นโลคอลแอดเดรส เหตุผลนี้เองที่ทำให้เป็นสิ่งสำคัญที่เครื่องคอมพิวเตอร์ที่อยู่ในพื้นที่เดียวกันบนระบบเครือข่ายจำเป็นตองใช้ netmask เดียวกัน

2.2.4 ซับเน็ต (Subnet)

ซับเน็ต (subnet) เป็นส่วนหนึ่งของระบบเครือข่ายที่ทำงานเหมือนเป็นเครือข่ายที่แยกตัวออกมาต่างหาก มันไม่จำเป็นต้องสนใจว่ามีอะไรเกิดขึ้นภายนอกเครือข่ายของมัน หรือกังวลว่าเหตุการที่เกิดขึ้นบนระบบเครือข่ายของตน จะมีผลกระทบต่อเครือข่ายที่เหลือ โดยทั่วไปแล้วซับเน็ตมักจะมีสายเชื่อมต่อทางฟิสิคัลแยกต่างหากหนึ่งเส้น ซึ่งจะมีจุดเชื่อมต่อเพียงจุดเดียวผ่านเราต์เตอร์หรือ บริดจ์กับระบบเครือข่ายอื่นๆ เราใช้ subnet mask เพื่อช่วยให้เครื่องคอมพิวเตอร์ที่อยู่ในส่วนหนึ่งของระบบเครือข่าย สามารถติดต่อโดยตรงกับเครื่องคอมพิวเตอร์เครื่องอื่นๆ ที่อยู่ในส่วนเดียวกันได้ แต่ไม่สามารถเชื่อมต่อกับเครื่องที่อยู่ในส่วนอื่นได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

subnet mask อยู่ในรูปของแอดเดรส w.x.y.z ซึ่งจะทำการซ่อนพื้นที่บางส่วนของระบบเครือข่ายออกไป ตัวอย่างของ mask ในระบบคลาส C เป็น 255.255.255.0 แต่มันมีความหมายอย่างไร ตัวอย่างเช่น IP address เป็น 192.167.222.17 แล้วคุณจะมองไม่เห็นแอดเดรส 192.168.223.25 คุณจะสามารถส่งแพ็กเกจไปที่แอดเดรสนี้ได้โดย ส่งไปที่เกตเวย์ หรือเราต์เตอร์ที่รู้ว่าคุณอยู่ที่ไหนและเครือข่ายอื่นๆ อยู่ที่ไหนหรือรู้ว่าจะต้องส่งไปให้ใครที่รู้ ตรงกันข้ามถ้าคุณต้องการส่งแพ็กเกจไปให้เครื่องพิมพ์ที่แอดเดรส 192.167.222.129 จะไม่เกิดปัญหาเพราะคุณจะมองเห็นแอดเดรสนั้น ดังนั้นแพ็กเกจก็สามารถส่งไปที่เครื่องพิมพ์ได้ทันที สิ่งสำคัญที่คุณต้องรู้คือ คุณจะมองเห็นแอดเดรสในส่วนที่มี subnet mask เป็นศูนย์ได้แต่คุณจะมองไม่เห็นแอดเดรสในส่วนที่มี subnet mask เป็น 255 โดยที่สำคัญคือ subnet mask บนส่วนหนึ่งของเครือข่ายของคุณนั้นจะต้องมีค่าเดียวกันด้วย ถ้ามีค่าไม่เหมือนกันจะเกิดปัญหาในเรื่องของการไม่สามารถส่งข้อมูลถึงกันได้ เช่นเครื่องคอมพิวเตอร์เครื่องหนึ่งอาจจะสามารถส่งแพ็กเกจไปให้กับอีกเครื่องหนึ่งได้ แต่เครื่องนั้นอาจจะไม่สามารถส่งแพ็กเกจกลับคืนมาได้

2.2.5 Gateway

เมื่อเครื่องเซิร์ฟเวอร์ต้องการติดต่อกับเครื่องอีกเครื่องหนึ่งซึ่งไม่ได้อยู่ในช่วง IP address เดียวกันในกรณีนี้จะต้องต่อผ่านเกตเวย์ ซึ่งเกตเวย์อาจเป็นเราต์เตอร์ หรือเครื่องที่ติดตั้ง วินโดวส์เอ็นทีที่ทำหน้าที่เป็นเราต์เตอร์ การติดต่อระหว่างเครื่องคอมพิวเตอร์ที่อยู่ในช่วง IP address เดียวกันนั้นไม่ต้องอาศัยเกตเวย์ เครื่องทั้งสองสามารถรับส่งแพ็กเกจกันเองได้ แต่เมื่อมันจำเป็นจะต้องติดต่อกับเครื่องที่อยู่นอกขอบเขต IP address ของมัน มันจำเป็นจะต้องรู้ว่าจะต้องค้นหาเครื่องนั้นได้อย่างไร อุปกรณ์พิเศษชนิดหนึ่งที่เรียกว่าเราต์เตอร์นั้น ได้ถูกพัฒนามาเพื่อย้ายแพ็กเกจของข้อมูลจากระบบเครือข่ายเซกชั่นหนึ่งไปยังอีกเซกชั่นหนึ่ง มันทำหน้าที่เหมือนกับทางผ่าน (gateway) ระหว่างเซกชั่นของระบบเครือข่าย ตัวเราต์เตอร์นั้นจะมี IP address อยู่อย่างน้อยสองค่าสำหรับติดต่อกับเซกชั่นของ IP address ที่มีช่วงต่างกัน และถูกเชื่อมต่อทางกายภาพกับเซกเมนต์ ที่ต่างกันอยู่ เราต์เตอร์จะจับแพ็กเกจข้อมูลที่ถูกส่งจากเครื่องคอมพิวเตอร์เครื่องหนึ่งและเคลื่อนมันไปยังอีกด้านของระบบเครือข่าย จากนั้นมันก็จะส่งไปยังเครื่องคอมพิวเตอร์อีกเครื่องหนึ่ง

เกตเวย์สามารถจะเป็นอุปกรณ์ที่แตกต่างกันบนระบบเครือข่ายได้แต่จะกล่าวถึงในแง่ของซับเน็ตและเราต์ติ้งถ้า subnet mask ของคุณเป็น 255.255.255.0 และถ้า IP address ของคุณมีค่า y เป็น 222 คุณจะไม่สามารถมองเห็น IP address ของเครือข่ายที่มีค่า y เป็น 223

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

34010

ได้ ถ้าคุณต้องการส่งแพ็กเกจไปให้เครื่องคอมพิวเตอร์ที่อยู่ในแอดเดรสที่ไม่รู้จักนี้ ก็จำเป็นที่จะต้องส่งผ่านไปที่เกตเวย์ เกตเวย์เป็นอุปกรณ์ทางฟิสิคอล ซึ่งมักจะเป็นเราต์เตอร์หรือเครื่องคอมพิวเตอร์อีกเครื่องหนึ่ง ที่มีการ์ดเน็ตเวิร์คมากกว่าหนึ่งการ์ด ซึ่งแต่ละการ์ดจะเชื่อมต่อไปที่ทั้งสองส่วนของระบบเครือข่าย โดยมันจะนำแพ็กเกจจากส่วน 222 ไปส่งที่ส่วน 223 ดังนั้นอุปกรณ์นี้จึงทำหน้าที่เป็นยามเฝ้าประตูระหว่างส่วนของเครือข่ายที่แยกจากกัน โดยจะส่งแพ็กเกจที่ส่งให้กับ 222 ไปยังส่วนของ 222 และส่งให้กับ 223 เมื่อมันรู้ว่าเป็นแพ็กเกจของส่วนนั้นจริงๆ

2.2.6 เราต์เตอร์ (Router)

เราต์เตอร์ (Router) เป็นอุปกรณ์ทางฟิสิคอลที่เชื่อมต่อกับเซกเมนต์ทางฟิสิคอลของเครือข่ายที่มากกว่าหนึ่งเซกเมนต์ โดยมันจะส่งแพ็กเกจไปมาระหว่างเซกเมนต์เหล่านี้เมื่อจำเป็น ถ้ามันไม่รู้ว่าจะส่งแพ็กเกจไปที่ไหน มันก็จะรู้ว่าจะถามทิศทางที่จะส่งไปยังแอดเดรสปลายทางนั้นจากที่ไหน ซึ่งจะอยู่บนเราต์เตอร์อีกตัวหนึ่ง ถ้าระบบเครือข่ายเป็นส่วนหนึ่งของอินเตอร์เน็ต เราต์เตอร์ก็จำเป็นจะต้องจัดการกับเส้นทางจำนวนมากที่เป็นไปได้ และตัดสินใจเลือกเส้นทางที่ดีที่สุดที่จะจัดส่งแพ็กเกจจากจุดหนึ่งไปยังอีกจุดหนึ่ง

จากส่วนประกอบดังที่กล่าวมาทั้งหมดนั้น ยังไม่ใช่ทั้งหมดของส่วนที่ต้องพิจารณาในการติดตั้งระบบเครือข่าย แต่หากพิจารณากันให้ระเอียดรอบคอบและใช้งานให้ถูกต้องแล้วกอรปกับส่วนระบบรักษาความปลอดภัยของวินโดวส์เอ็นทีแล้วย่อมจะเกิดความปลอดภัยในระบบเครือข่ายที่เลือกใช้เพิ่มขึ้นได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 3
ระบบรักษาความปลอดภัยบนวินโดวส์เอ็นที 4

3.1 การวางระบบรักษาความปลอดภัย

โดยทั่วไปแล้วในการใช้งานระบบเครือข่ายคอมพิวเตอร์ที่ใช้วินโดวส์เอ็นที่เป็นระบบปฏิบัติการนั้นโดยตัววินโดวส์เอ็นที่เองนั้นมีระบบรักษาความปลอดภัยที่น่าไว้วางใจเป็นพื้นฐานของระบบปฏิบัติการอยู่แล้ว ซึ่งสามารถใช้รักษาความปลอดภัยได้ดีในระดับหนึ่ง ซึ่งในส่วนของระบบรักษาความปลอดภัยดังกล่าวก็ไม่ได้ทำให้การใช้งานระบบของ User มีความยุ่งยากขึ้นมากนักยกเว้นในบางกรณีที่ความผิดพลาดนั้นเกิดจากตัว User เองเช่นลืมพาสเวิร์ด หรือความพยายามที่จะใช้งานนอกเหนือจากที่กำหนดไว้ให้ ซึ่งอาจก่อให้เกิดความรำคาญได้ แต่ทั้งนี้ทั้งนั้นการกำหนดการรักษาความปลอดภัยนั้นต้องไม่หละหลวมหรือเข้มงวดมากเกินไป

ซึ่งระบบรักษาความปลอดภัยที่ดีในอุดมคตินั้น User จะไม่สามารถเข้าใช้ทรัพยากรที่ไม่ถูกอนุญาตให้ใช้ได้เลยในขณะที่ระบบรักษาความปลอดภัยดังกล่าวก็ทำงานอยู่เบื้องหลังโดยที่ ผู้ใช้ไม่สามารถสังเกตเห็นได้

3.2 รูปแบบในการจัดการระบบเครือข่ายและระบบรักษาความปลอดภัย

รูปแบบในการจัการระบบเครือข่ายจะมีผลโดยตรงกับการจัดระบบรักษาความปลอดภัย เราสามารถแบ่งการจัดการระบบเครือข่ายออกเป็น 4 แบบพื้นฐานคือ

1. ระบบจัดการจากศูนย์กลาง
2. ระบบจัดการที่โลคอลตามแผนกหรือกลุ่ม (แบบกระจาย)
3. ระบบจัดการโดยตัวระบบปฏิบัติการเอง
4. ระบบจัดการที่ผสมจากระบบต่างๆ ข้างต้น

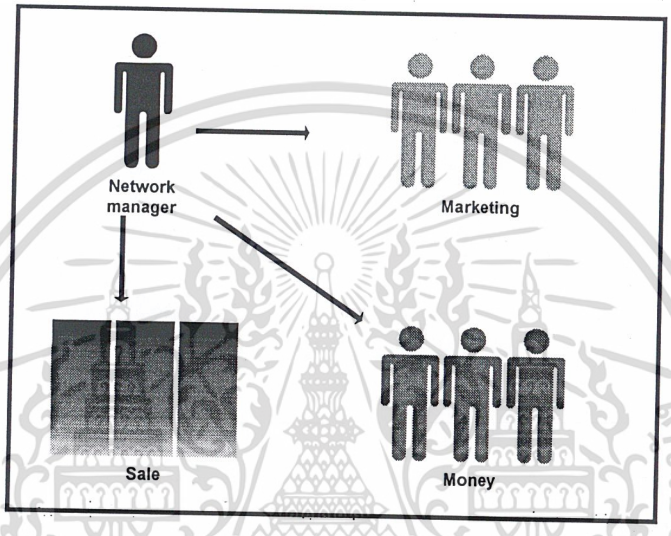
ซึ่งในการแบ่งการจัดการระบบดังกล่าวจะไม่ขึ้นอยู่กับขนาดของเครือข่ายคือไม่ว่าระบบเครือข่ายจะมีขนาดใหญ่หรือเล็กก็ตาม การจัดการระบบเครือข่ายจะมีความคล้ายคลึงกันจะแตกต่างเพียงแค่ระดับและขนาดของการจัดการระบบเท่านั้นไม่ได้แตกต่างกันที่คอนเซ็ปต์พื้นฐาน

3.2.1 ระบบการจัดการจากศูนย์กลาง (Central Administration)

ในระบบการจัดการจากศูนย์กลางนี้ จะมีผู้ใช้หรือกลุ่มหรือแผนกเพียงชุดเดียวที่ทำหน้าที่จัดการระบบเครือข่ายให้ผู้ใช้และรีซอร์สภายในองค์กรนั้นทั้งหมด (รูปที่ 3.1) รูปแบบนี้ทำงานได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ดีกับองค์กรขนาดเล็กและขนาดกลาง แต่จะทำงานได้ช้ากับองค์กรขนาดใหญ่หรือองค์กรที่มีสำนักงานกระจายอยู่หลายๆ ที่ แต่อย่างไรก็ตามในแง่ของการรักษาความปลอดภัย รูปแบบนี้เป็นรูปแบบที่ดีที่สุด คุณจะมั่นใจได้ว่านโยบายของระบบ (System policies) และขั้นตอนการทำงานจะเป็นหนึ่งเดียวกันทั้งองค์กรผู้จัดการระบบสามารถที่จะเปลี่ยนสถานที่ของผู้ใช้และรีซอร์สในระบบเครือข่ายและทำการแก้ไขโพรไฟล์และการใช้งานของผู้ใช้ได้อย่างรวดเร็ว

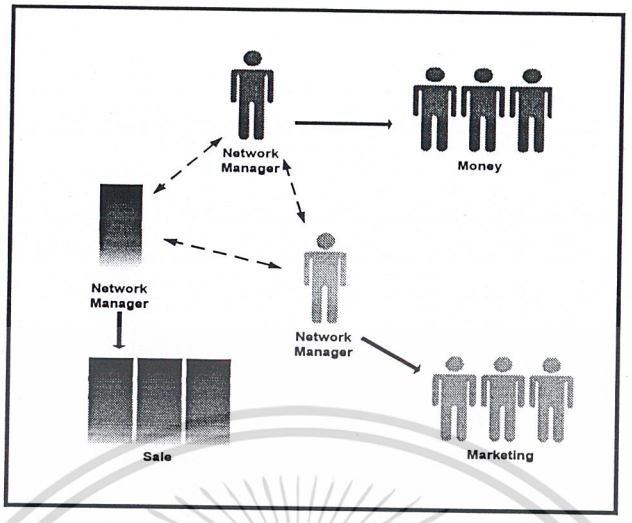


รูปที่ 3.1 ระบบจัดการจากศูนย์กลาง

3.2.2 **ระบบจัดการแบบกระจาย (Distributed Administration)**

สำหรับระบบจัดการแบบกระจายนี้ การจัดการจะเกิดขึ้นที่ระดับแผนกหรือเวิร์กกรุ๊ป (รูปที่ 3.2) การจัดการที่ระดับโลคอลนี่จะช่วยให้ตอบสนองความต้องการของผู้ใช้ได้เร็วขึ้นแต่ต้องแลกกับการรักษาความปลอดภัย เมื่อมีการจัดการอยู่ที่ระดับแผนกหรือเวิร์กกรุ๊ปหลายๆ จุดนโยบายระบบก็จะแตกต่างกันไปตามเวิร์กกรุ๊ปนั้น ยิ่งมีจำนวนกลุ่มมากขึ้นเท่าไรจำนวนความเชื่อถือ (Trust relationship) ระหว่างโดเมนก็จะมากขึ้นด้วย (ซึ่งช่วยเพิ่มโอกาสให้กับผู้ที่หวังจะเจาะระบบให้สามารถเจาะระบบหนึ่ง และใช้ความเชื่อถือระหว่างโดเมนเพื่อเข้าถึงระบบรักษาความปลอดภัยในระดับที่สูงขึ้นได้

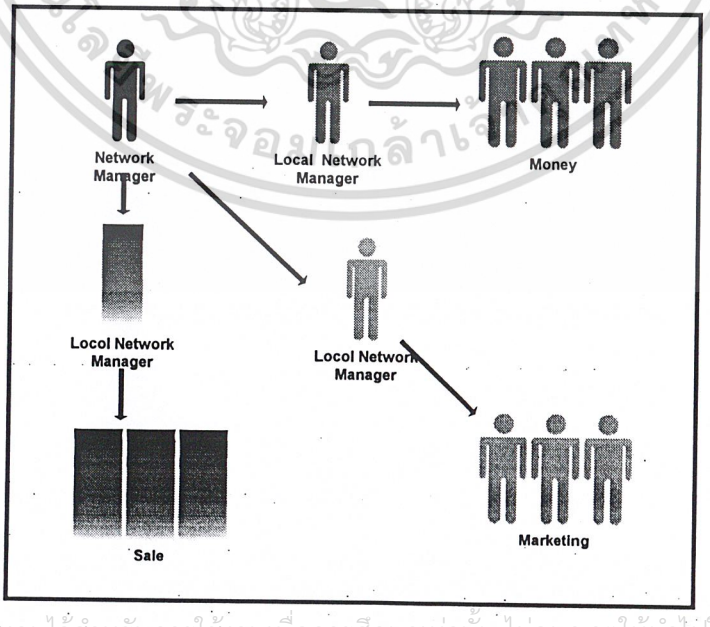
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.2 รูปแบบการจัดการแบบกระจาย

3.2.3 **ระบบจัดการแบบผสม**(Mixed Administration)

ระบบจัดการแบบผสมนี้รวมข้อดีของทั้งระบบจัดการจากศูนย์กลางและระบบการจัดการแบบกระจายไว้ด้วยกัน (รูปที่ 3.3) ผู้จัดการระบบจากศูนย์กลาง (หรือกลุ่ม) จะมั่นใจว่านโยบายของระบบนั้นจะถูกบังคับใช้ตลอดทั้งองค์กร ในขณะที่ผู้จัดการระบบในระดับแผนกหรือเวิร์กกรุ๊ปก็จะทำหน้าที่จัดการตามความต้องการของผู้ใช้ในแต่ละวัน ระบบนี้ต้องการการลงทุนสูงเกินกว่าที่บริษัทขนาดเล็กจะลงทุนได้ ดังนั้นจึงมักจำกัดอยู่กับองค์กรขนาดใหญ่เท่านั้น



รูปที่ 3.3 ระบบจัดการแบบผสม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3 ประเภทของระบบรักษาความปลอดภัยบนระบบเครือข่าย

ระบบรักษาความปลอดภัยบนระบบเครือข่ายสามารถแบ่งได้เป็น 4 กลุ่มด้วยกันคือ

1 ระบบรักษาความปลอดภัยทางกายภาพ

2 ระบบรักษาความปลอดภัยสำหรับผู้ใช้

3 ระบบรักษาความปลอดภัยสำหรับไฟล์

4 ระบบรักษาความปลอดภัยจากผู้บุกรุก

ในการจัดการระบบรักษาความปลอดภัยที่ดีนั้นจำเป็นต้องมีความรู้ในเรื่องของระบบรักษาความปลอดภัยพื้นฐานเหล่านี้เพื่อที่จะสามารถที่จะกำหนดสภาพแวดล้อมพื้นฐานให้กับผู้ใช้ได้ในระดับหนึ่งซึ่งมีความปลอดภัยที่ดีพอสมควรซึ่งระบบรักษาความปลอดภัยบนระบบเครือข่ายดังกล่าวมีรายละเอียดดังนี้

3.3.1 ระบบรักษาความปลอดภัยทางกายภาพ

ความปลอดภัยทางกายภาพเป็นสิ่งจำเป็นสำหรับเครื่องคอมพิวเตอร์ทุกชนิด ไม่ว่าจะเป็นเน็ตเวิร์กเซิร์ฟเวอร์ เวิร์กสเตชั่น โน้ตบุ๊ก หรือเทอร์มินอลก็ตาม ซึ่งหากไม่มีการป้องกันภายนอกเลยใครก็ตามที่ สามารถเข้าถึงและใช้เครื่องของคุณได้ เขาเหล่านั้นก็จะเข้าถึงข้อมูลในเครื่องนั้นๆ ได้โดยตรงดังนั้นจึงสมควรที่จะมีการป้องกันในระดับกายภาพพอสมควร เพื่อป้องกันการเข้าถึงเครื่องในส่วนที่ไม่เกี่ยวข้องเช่น เครื่องเซิร์ฟเวอร์ควรมีห้องแยกจากส่วนของผู้ใช้งานปกติที่ไม่เกี่ยวข้อง หรือปิดสำนักงานนอกเวลางานเป็นต้น ซึ่งการรักษาความปลอดภัยในระดับกายภาพดังกล่าวจะช่วยปกป้องข้อมูลในระดับเบื้องต้นได้บ้างถึงแม้จะเป็นส่วนเล็กน้อยก็ดีกว่าไม่มีเสียเลย

3.3.2 ระบบรักษาความปลอดภัยสำหรับผู้ใช้

ระบบรักษาความปลอดภัยของผู้ใช้ต้องมีพฤติกรรมดังนี้

1 ผู้ใช้ระบบยังสามารถเรียกใช้รีซอร์สต่างๆ ที่ต้องการได้อย่างสะดวก

2 เก็บรักษาไม่ให้ใช้งานรีซอร์สนั้น รวมทั้งซ่อนไม่ให้เห็น สำหรับรีซอร์สที่ผู้ใช้นั้นๆ ไม่จำเป็นที่จะต้องใช้งาน รีซอร์สเหล่านี้จะรวมถึงข้อมูลที่เป็นความลับขององค์กรและข้อมูลส่วนตัวของผู้อื่นด้วย

ถ้าเป็นไปได้ผู้ดูแลระบบมักจะต้องการให้ผู้ใช้ ใช้พาสเวิร์ดเพียงแค่ชุดเดียวเพื่อที่จะสามารถเข้าถึงและใช้งานรีซอร์สในระบบได้ แต่การเพิ่มพาสเวิร์ดชุดที่ 2 เพื่อให้ผู้ใช้สามารถที่จะเข้าถึงรีซอร์สที่สำคัญมากกว่าก็จะช่วยเพิ่มความมั่นใจให้กับเขามากขึ้น แต่อย่าใช้วิธีนี้มากนักเนื่องจากโดยทั่ว

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ไปเรามักจะจำพาสเวิร์ดได้เพียง 2 หรือ 3 ชุดเท่านั้นถ้าหากมีมากกว่านี้แล้วเขาจะเริ่มที่จะจดมันไว้ที่จอมอนิเตอร์หรือเลือกใช้พาสเวิร์ดที่ง่าย หรือคล้ายๆ กัน ซึ่งจะทำให้เดาได้ง่ายเช่นกัน

สำหรับการวางเลย์เอาท์ของระบบเครือข่ายทั้งแบบลอจิคัลและแบบฟิสิคอลพร้อมๆ กัน (แบบลอจิคอลหมายถึงการจัดแบ่งกลุ่มบนวินโดวส์เอ็นที ส่วนแบบฟิสิคอลเป็นการแบ่งตามสถานที่ทำงาน) จะช่วยลดความสับสนในเรื่องการวางระบบรักษาความปลอดภัยและระบบจัดการได้ ให้เลือกวางเลย์เอาท์เพื่อให้โดเมนเก็บกลุ่มผู้คนและอ็อบเจ็กทางลอจิคอลแทนที่จะเก็บตามตำแหน่งที่อยู่ใกล้เคียงกัน ในรูปที่ 3.4 และ 3.5 แสดงให้เห็นความแตกต่างระหว่างการจัดกลุ่มผู้ใช้ตามสถานที่อยู่(ฟิสิคอล)และตามลอจิคอลในรูปนี้เป็นตัวอย่างบริษัทที่มีแผนกงานอยู่ 4แผนกคือ account executives, copywriters,illustrators และmedia buyers การจัดวางสำนักงานจะจัดวางเพื่อให้ผู้ใช้ทั้งหมดที่ใช้รีซอร์สร่วมกัน (อุปกรณ์สำนักงาน วัสดุอ้างอิงและอุปกรณ์พิเศษ) ทำงานอยู่ใกล้ๆ กัน แต่จริงๆ แล้วการปฏิบัติงานของบริษัทนี้ ในทีมงานของแต่ละโปรเจ็กจะประกอบไปด้วยพนักงานของทุกแผนกๆ ละหนึ่งคนในรูปที่ 3.4 โดเมนแต่ละชุดจะรวมผู้ใช้ทั้งหมดที่อยู่ในสถานที่เดียวกันไว้ในโดเมนเดียวกันในรูปที่ 3.5 นั้นโดเมนแต่ละชุดจะรวมสมาชิกที่อยู่ในทีมงานเดียวกันแทน ในทางปฏิบัติสำนักงานขนาดเล็กเช่นนี้ควรจะมีโดเมนเพียงชุดเดียวซึ่งผู้ใช้จะอยู่ในนั้นทั้งหมด ถึงอย่างไรก็ตามการกำหนดโดเมนตามกลุ่มการทำงานตั้งแต่เริ่มต้นนั้นจะช่วยประหยัดเวลาและลดปัญหายุ่งยากในภายหลังได้การขยายขนาดเครือข่ายในภายหลังจะใช้เวลาและแรงงานน้อยลง และยังดำรงระบบรักษาความปลอดภัยไว้ได้ด้วย การใช้งานรีซอร์สทางฟิสิคอล อย่างเช่น เครื่องพิมพ์และโมเด็ม สามารถจัดการโดยใช้ global group ช่วยได้ อย่างไรก็ตามควรแน่ใจด้วยว่าผู้ใช้สามารถที่จะใช้งานรีซอร์สนั้นได้สะดวก ในตัวอย่างนี้ถ้ามีสมาชิกคนหนึ่งในทีมงานหนึ่งถูกเปลี่ยนไปอยู่อีกที่หนึ่ง ก็ควรจะใช้การจัดกลุ่มโดเมนแบบลอจิคอลอีกแบบหนึ่งแทน มิเช่นนั้นแล้วผู้ดูแลระบบจะต้องคอยย้ายผู้ใช้จากโดเมนหนึ่งไปยังอีกโดเมนหนึ่ง หรือต้องให้ผู้ใช้ทุกคนสามารถใช้รีซอร์สได้ทั้งหมด ซึ่งถึงแม้ว่าจะทำให้ผู้ใช้งานสามารถใช้รีซอร์สได้สะดวกมากขึ้นก็ตาม แต่ก็จะทำให้ระบบรักษาความปลอดภัยอ่อนด้อยลงด้วย

3.3.3 ระบบรักษาความปลอดภัยสำหรับไฟล์

ระบบรักษาความปลอดภัยสำหรับไฟล์มีอยู่ 2 ด้านที่ควรพิจารณาคือ

1 การควบคุมการใช้งานไฟล์

2 การป้องกันความสมบูรณ์ของไฟล์ (integrity)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ทั้งไฟล์ข้อมูลและไฟล์เอกสารต่างก็เก็บข้อมูลในรูปแบบที่เป็นโครงสร้างรูปแบบหนึ่งแต่ไฟล์เอกสารมักจะอ่านได้ ส่วนไฟล์ข้อมูลจะต้องแปลความหมายด้วยโปรแกรม (ยกเว้นไฟล์เอกสารจากเวิร์ดโปรเซสซิ่ง ซึ่งต้องอ่านด้วยโปรแกรมเวิร์ดโปรเซสเซอร์ แต่อ้างถึงเป็นไฟล์เอกสารเพื่อความสะดวก) ไมโครซอร์ฟเอ็นทีเวอร์ชั่น 4 นั้นอนุญาตให้ควบคุมการใช้งานของผู้ใช้ได้ทั้งระดับโฟลเดอร์และระดับไฟล์ ดังนั้นผู้ใช้บางคนอาจจะสามารถใช้งานโฟลเดอร์หนึ่งได้แต่ไม่สามารถใช้งานอีกโฟลเดอร์หนึ่งได้ หรือไม่สามารถที่จะใช้งานไฟล์ใดๆ ในโฟลเดอร์นั้นได้เลยหรือกลับกัน แต่ระบบรักษาความปลอดภัยสำหรับไฟล์จะทำงานได้ก็ต่อเมื่อติดตั้งระบบไฟล์ในแบบ NTFS เท่านั้น ในตารางที่ 1 จะแสดงถึง permission ที่สามารถกำหนดให้กับไดเร็กทอรี่และไฟล์ได้ จากตารางจะแสดง permission สองส่วน (สองวงเล็บ) ด้านซ้ายจะเป็น permission ของไดเร็กทอรี่ ส่วนอีกอันจะเป็น permission ของไฟล์ที่อยู่ในไดเร็กทอรี่ จริงๆ แล้ว บนวินโดวส์เอ็นที permission จะถูกกำหนดให้เป็นแอตทริบิวต์(attribute) ให้กับไฟล์นั้นๆ ต่อไปนี้จะเป็นแอตทริบิวต์ที่สามารถกำหนดให้กับไฟล์ได้

Read (R)

Write (W)

Execute (X)

Delete (D)

Change Permission (P)

Take Ownership (O)

ควรจะต้องมีการคอยตรวจสอบไฟล์ที่มีความสำคัญหรือเป็นความลับบ่อยๆ ด้วย เพื่อป้องกันการเรียกใช้จากบุคคลที่ไม่มีสิทธ์

ตารางที่ 3.1 Standard Permission สำหรับไดเร็กทอรี่และไฟล์ บน NTFS

Directory Permission	คำอธิบาย
No Access (None)(None)	ผู้ใช้ไม่สามารถใช้ไดเร็กทอรี่ได้เลย ยกเว้นในกรณีเป็นสมาชิกลุ่มที่ใช้งานไดเร็กทอรี่นั้นได้
List (RX) (Not Specified)	ผู้ใช้สามารถแสดงรายชื่อไฟล์และซับไดเร็กทอรี่ที่อยู่ในไดเร็กทอรี่นั้นได้ แต่ไม่สามารถใช้งานไฟล์ในไดเร็กทอรี่ที่ผู้อื่นสร้างขึ้นได้
Read (RX)(RX)	ผู้ใช้อ่านไฟล์ได้ และสามารถรันแอปพลิเคชั่นในไดเร็กทอรี่นี้ได้
Add(WX) (Not Specified)	ผู้ใช้สามารถเพิ่มไฟล์ไว้ในไดเร็กทอรี่นี้ได้ แต่ไม่สามารถเปลี่ยนไฟล์หรือแก้ไขได้
Add&Read (RWX)(RX)	ผู้ใช้สามารถอ่านและเพิ่มไฟล์ได้แต่ไม่สามารถแก้ไขไฟล์
Chang(RWXD)(RWXD)	ผู้ใช้สามารถอ่าน เพิ่มไฟล์ และสามารถแก้ไขไฟล์ได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเอกสารทุกครั้งที่มีการนำไปใช้

Full control(All)(All)	ผู้ใช้สามารถเพิ่ม อ่านและแก้ไขไฟล์ สามารถเปลี่ยน permission สำหรับไดเร็กทอรี่และไฟล์ และสามารถเปลี่ยนเจ้าของไดเร็กทอรี่และไฟล์ในนั้นได้

File Permission	คำอธิบาย
No Access (None)	ผู้ใช้ไม่สามารถใช้ไฟล์ได้เลย ยกเว้นในกรณีเป็นสมาชิกลุ่มที่ใช้งานไฟล์นั้นได้
Read (RX)	ผู้ใช้อ่านไฟล์ได้ และสามารถรันแอปพลิเคชั่นในไดเร็กทอรี่นี้ได้
Chang(RWXD)	ผู้ใช้สามารถอ่าน แก้ไข และลบไฟล์ได้
Full control(All)	ผู้ใช้สามารถ อ่านแก้ไขและลบ กำหนด permission และเปลี่ยนความเป็นเจ้าของไฟล์ได้

ไฟล์โปรแกรม

ไฟล์โปรแกรมและโฟลเดอร์ที่ใช้เก็บไฟล์เหล่านี้ควรจะกำหนด Permission ให้เป็น Read เนื่องจากผู้ใช้มักไม่จำเป็นต้องแก้ไขมัน นอกจากนี้การกำหนดเป็น Read มันยังช่วยป้องกันในกรณีที่ผู้ใช้พลังเผลอไปลบหรือเขียนทับมันโดยความไม่ตั้งใจ หรือป้องกันการติไวรัส แต่การกำหนด Permission เป็นRead ก็ยังไม่เพียงพอเนื่องจากผู้ใช้ที่เข้าถึงโฟลเดอร์ได้แบบ Change Permission (P) จะสามารถเปลี่ยนการใช้งาน (access) ของไฟล์แต่ละไฟล์ในโฟลเดอร์ได้ (จึงเปลี่ยนจาก Read เป็นอย่างอื่นได้)

ไฟล์ไลบรารี่

การจัดการไฟล์ไลบรารีก็เหมือนๆ กับไฟล์โปรแกรมโดยเฉพาะเมื่อไฟล์ไลบรารีอยู่ในไดเร็กทอรี่เดียวกันกับที่เรียกใช้มัน ตามปกติแล้วเมื่อมีการเรียกใช้ไฟล์ไลบรารี่ร่วมกันในแอปพลิเคชั่นมันมักจะถูกเก็บไว้ในตำแหน่งที่อ้างถึงด้วยตัวแปรเอนไวรอนเมนต์ ซึ่งมักจะเก็บไว้ในโฟลเดอร์ %SYSTEMROOT%หรือ %SYSTEMROOT%\SYSTEMผู้ใช้ต้องการเพียงการเข้าถึงแบบRead สำหรับโฟลเดอร์%SYSTEMROOT%\SYSTEMเว้นเสียแต่เขาต้องติดตั้งซอร์ฟแวร์เองอย่างไรก็ตามโฟลเดอร์ %SYSTEMROOT% นั้นสามารถเก็บไฟล์ข้อมูลหรือไฟล์เอกสารที่แอปพลิชั่นนั้นเขียนขึ้นได้ด้วย ดังนั้นคุณจึงไม่สามารถป้องกันการลบ แก้ไขไฟล์หรือป้องกันไฟล์เสียหาย (corrupt) ได้ นอกจากให้ความรู้แก่ผู้ใช้ และควรจะใช้ซอร์ฟแวร์ป้องกันไวรัสหรือตัวสแกนเพื่อป้องกันการติดไวรัสด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ไฟล์ข้อมูลและไฟล์เอกสาร

แน่นอนที่ผู้ใช้ต้องการใช้ไฟล์ข้อมูล และไฟล์เอกสารของเขาอย่างสมบูรณ์ ซึ่งสามารถจัดการได้ง่ายๆ โดยสร้างโฟลเดอร์มาเฉพาะอันหนึ่งสำหรับผู้ใช้แต่ละคน ในโฟลเดอร์นั้นไม่ต้องเก็บไฟล์โปรแกรมหรือไฟล์ไลบรารี่อะไรเลย และกำหนด permission แบบ All ให้กับผู้ใช้คนนั้น และ None ให้กับผู้ใช้คนอื่น รวมทั้งสร้างโฟลเดอร์แยกต่างหากให้กับผู้ใช้ที่อยู่ในกลุ่มเดียวกันเพื่อไว้ใช้เก็บข้อมูลที่ใช้ร่วมกัน การกำหนด permission นั้นจะขึ้นอยู่กับโครงสร้างของกลุ่มสมาชิกทุกคนอาจได้รับ permission แบบ All หรือมีเฉพาะบางคนที่เป็นแบบ All ส่วนที่เหลือเป็น Read หรือ Change และแน่นอนว่าอย่าเก็บไฟล์โปรแกรมหรือไฟล์ไลบรารี่ไว้ในโฟลเดอร์นี้

โฟลเดอร์อีกแบบหนึ่งที่ใช้กันทั่วๆ ไปซึ่งไว้ใช้เก็บเอกสารที่ผู้ใช้ทุกคนหรือผู้ใช้จำนวนมากได้รับ permission แบบ Read และมีเพียงคนเดียวที่ได้รับ Permission แบบ All ตัวอย่างเช่น โฟลเดอร์ NOTICES ซึ่งใช้เก็บเอกสารที่แสดงนโยบายของบริษัท ซึ่งควรจะเข้าถึงได้แบบ Read จากทุกคนบนระบบเครือข่ายแต่เข้าถึงแบบ All สำหรับผู้มีหน้าที่ในการดูแลรักษาไฟล์นี้

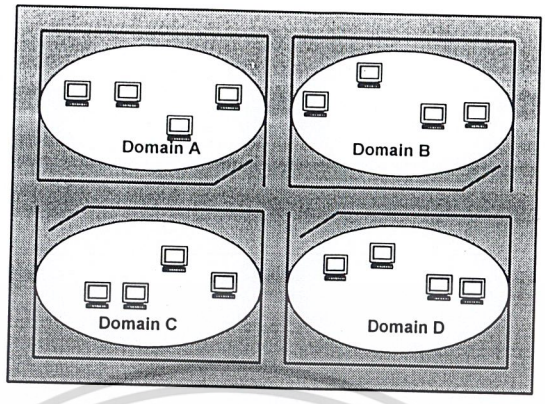
3.3.4 ระบบรักษาความปลอดภัยจากผู้บุกรุก

เมื่อพูดถึงเรื่องระบบรักษาความปลอดภัยแล้ว มักจะมีการพูดถึงเรื่องของผู้เจาะระบบกันมากในปัจจุบัน ซึ่งจริงๆ แล้วความเสียหายส่วนใหญ่ที่เกิดขึ้นมักจะเกิดจากบุคคลในองค์การมากกว่าคนภายนอกอย่างไรก็ตามก็มีวิธีการที่จะทำให้มั่นใจได้ว่าความเสี่ยงต่อการที่จะถูกเจาะระบบได้น้อยลง

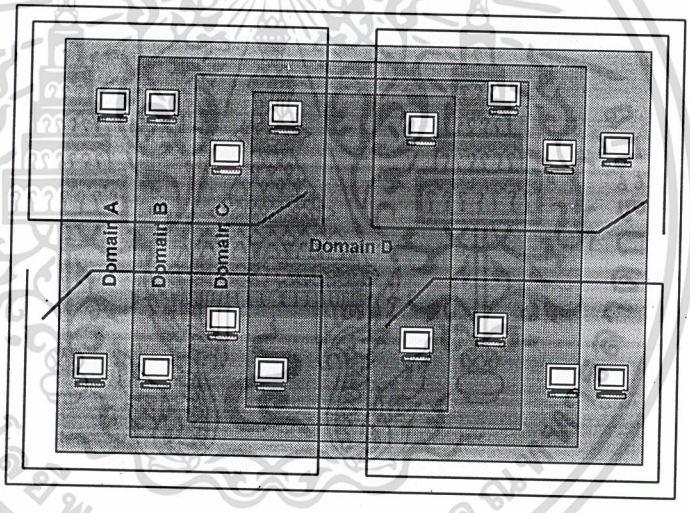
ผู้ใช้ทุกคนบนระบบควรมีพาสเวิร์ดที่เลือกมาเป็นอย่างดีและควรจะเปลี่ยนพาสเวิร์ดเหล่านั้นเป็นประจำ และไม่ควรที่จะนำพาสเวิร์ดเก่ากลับมาใช้ใหม่ทันที ควรมีการกำหนดว่าควรจะใช้เวลาอย่างน้อยเท่าไดที่จะสามารถนำพาสเวิร์ดเก่ากลับมาใช้ได้อีก รวมทั้งต้องสามารถที่จะจำกัดจำนวนครั้งในการ ล็อกออนผิดที่สามารถยอมได้ในระยะเวลาหนึ่งๆ แต่อย่างน้อยควรให้ใส่ได้ประมาณ 3 ครั้งเนื่องจากการพิมพ์ผิด

ถ้าผู้ใช้ของคุณต้องโทรศัพท์เข้ามาเพื่อเชื่อมต่อระบบจากภายนอกแล้วควรที่จะต้องเพิ่มการรักษาความปลอดภัยให้มากกว่าแค่ พาสเวิร์ดเท่านั้น ซึ่งวิธีหนึ่งที่มีความปลอดภัยมากกว่าคือให้ RAS เซิร์ฟเวอร์ทำการโทรกลับไปยัง เครื่องที่โทรเข้ามาเป็นต้น และสำหรับผู้ดูแลระบบควรที่จะเปลี่ยนไปใช้ User name อื่นเพื่อจัดการกับระบบและจำกัดสิทธิของ User Administrator ให้ต่ำที่สุด เนื่องจากชื่อดังกล่าวจะเป็นที่หมายตาของผู้เจาะระบบอยู่แล้วในการเจาะเข้าไปในระบบใดๆ ก็ตามเนื่องจากเป็นผู้ที่มี Permission สูงที่สุดในการจัดการกับระบบเครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.4 ตัวอย่างโดเมนที่กำหนดตามสถานที่ทำงาน



รูปที่ 3.5 ตัวอย่างของโดเมนที่กำหนดตามกลุ่มการทำงานแบบลอจิคอล

3.4 การกำหนดสภาวะเริ่มต้นใช้งานของผู้ใช้ (User Profile)

ผู้ที่เคยใช้งานวินโดวส์เอ็นที่จะทราบว่าเมื่อคุณเซ็ตหน้าจอเอาไว้ หรือทำการเซ็ตเมนูเอาไว้เมื่อคุณเปิดเครื่องในครั้งต่อมา คุณจะพบว่าสิ่งที่ได้ทำการเซ็ตไว้ยังคงมีค่าเดิมตามที่ได้เซ็ตไว้ เหตุที่เป็นเช่นนี้เพราะว่า User ทุกคาที่ ล็อกออนเข้ามาบนเครื่องวินโดวส์เอ็นทีจะมี User profile ของตนเอง

User Peofile จะถูกสร้างขึ้นเมื่อคุณทำการ Logon เข้าวินโดส์เอ็นทีในครั้งแรกและจะถูกใช้สำหรับเก็บข้อมูลเกี่ยวกับสภาวะแวดล้อมที่คุณใช้งานโดยสามารถทำการเก็บข้อมูลดังต่อไปนี้

เอกสารนี้สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

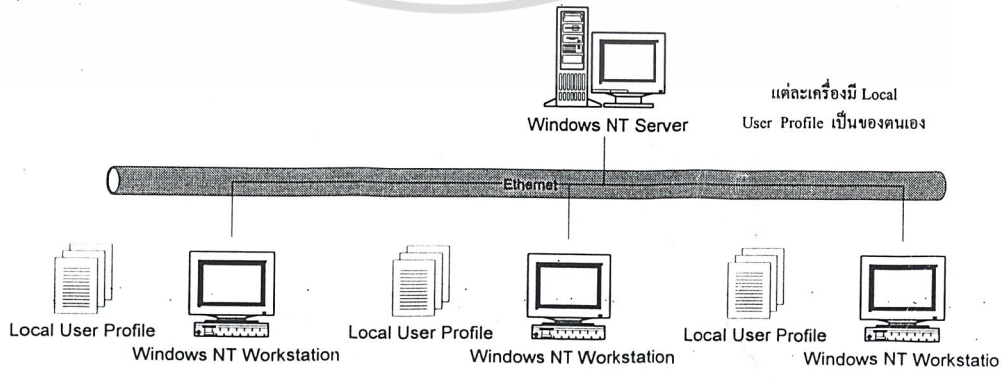
ตารางที่ 3.2 รายละเอียดของ User Profile

คำอธิบาย	รายละเอียด
Windows Explorer	ข้อมูลทุกอย่างที่ User ได้ทำการเซ็ทใน Windows Explorer ค่าไว้รวมถึง Network Connection
Taskbar	ค่าที่เซ็ทไว้ใน Taskbar เช่น Program Group, Program Item ฯลฯ
Printer Setting	พริ้นเตอร์ที่ได้ติดตั้งไว้รวมถึง Network Printer ด้วย
Control Panel	ค่าที่เซ็ทไว้ใน Control Panel เช่น Mouse, Color, Keyboard, Cursor ฯลฯ
Accessories	โปรแกรมที่อยู่ใน Accessories เช่น Notepad, Calculator, Paint ฯลฯ
Windows NT-based Application	โปรแกรมประยุกต์ที่ตั้งไว้บนวินโดวส์เอ็นทีเครื่องนั้น ๆ
Help bookmarks	ค่า Bookmarks ที่เซ็ทไว้ใน Help

3.4.1 ประเภทของ User Profile

ในวินโดวส์เอ็นทีมีการแบ่ง Profile ตามลักษณะการใช้งานออกเป็น 3 ประเภทคือ

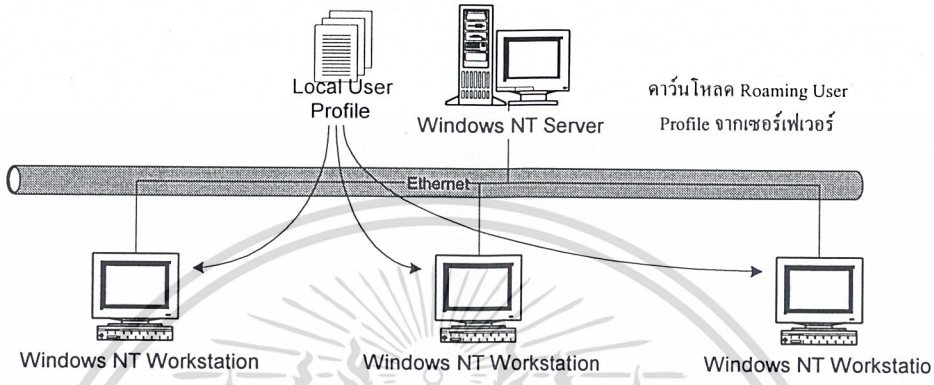
Local Profiles เป็น Profile ที่มีในเครื่องคอมพิวเตอร์แต่ละตัว ดังนั้น User Profile ชนิดนี้จึงสามารถใช้กับเครื่องที่ Local User Profile นี้ถูกสร้างขึ้นเท่านั้น



รูปที่ 3.6 Local Profile

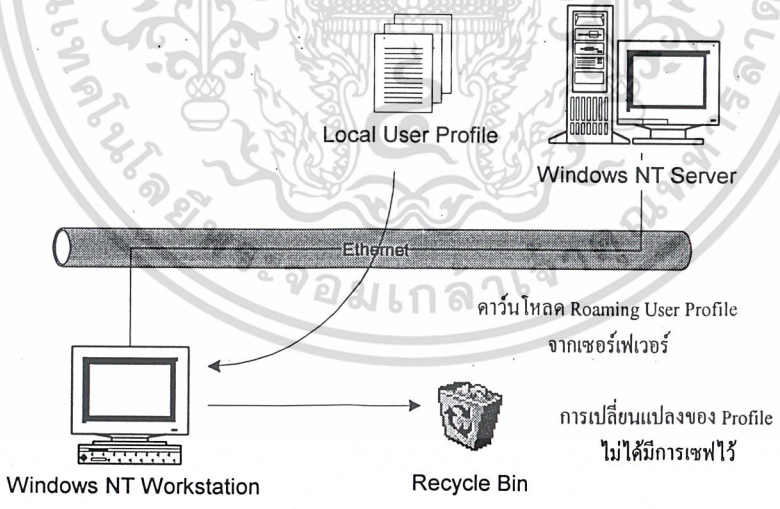
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Roaming Profiles เป็น Profile ที่สามารถ Load ได้จากเซอรฟ์เวอร์ ดั้งนั้นคุณสามารถเรียก User Profile ชนิดนี้มาใช้ได้ไม่ว่าคุณ Logon จากเครื่องใดใน Network ก็ได้ User Profile ชนิดนี้เหมาะสำหรับ User ที่ไม่มีเครื่องประจำ



รูปที่ 3.7 Roaming Profile

Mandatory Profiles เป็น Profile หลักที่ User ไม่สามารถทำการเปลี่ยนแปลงและแก้ไขได้เหมาะสมสำหรับ User ที่เราไม่ต้องการให้มีแก้ไขสภาวะการใช้งาน



รูปที่ 3.8 Mandatory Profile

3.4.2 ข้อดีของการใช้ User Profile

- User แต่ละคนใช้สามารถกำหนดสภาวะให้เหมาะกับงานของตนได้
- ในเครื่องคอมพิวเตอร์เครื่อง ๆ หนึ่งสามารถกำหนดสภาวะแวดล้อมให้เหมาะสมกับ User หลาย ๆ คนได้

เอกสารนี้เป็นสมบัติของมหาวิทยาลัยเทคโนโลยีราชมงคลกรุงเทพ ห้ามนำไปใช้ในด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น ห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- หากคุณทำการเซฟ User Profile ไว้บนเซอร์ฟเวอร์ คุณสามารถใช้ Profile นี้ได้กับคอมพิวเตอร์ทุกตัวที่ใช้วินโดวส์เอ็นทีได้ เราเรียก Profile ชนิดนี้ว่า Roaming User Profile
- หากคุณต้องการกำหนดสภาวะแวดล้อมโดยที่ User ไม่สามารถเปลี่ยนแปลงได้คุณสามารถใช้ Mandatory User Profile
- ทำให้ผู้ดูแลระบบทำงานได้ง่ายได้ง่ายขึ้น

3.4.3 ข้อด้อยของการใช้ User Profile

- คุณไม่สามารถใช้ User Profile ในเครื่องที่ไม่ได้ใช้วินโดวส์เอ็นทีหรือวินโดวส์ 95
- การเขียน User Profile ทำได้ยากกว่าการเขียน Logon Script
- ไม่สามารถใช้ในไมโครซอฟท์เน็ตเวิร์กได้ทำประเภท เช่น LAN Manager เป็นต้น

3.5 Logon Script

Logon Script ก็คือแบตช์ไฟล์แบบง่าย ๆ ที่ทำงานโดยอัตโนมัติเมื่อผู้ใช้ล็อกออนเข้าไปบนระบบเครือข่าย ไฟล์ Logon script หนึ่งไฟล์สามารถกำหนดให้กับผู้ใช้หนึ่งหรือหลายคนก็ได้ สำหรับชื่อและที่เก็บของ Logon Script แต่ละไฟล์นั้นจะระบุไว้ในวินโดว์ Profile ของ user profile โดยปกติจะเก็บ logon script อยู่ในไดเร็กทอรีต่อไปนี้

C:\WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS

คุณไม่ควรเปลี่ยนที่เก็บ logon script เนื่องจาก domain controller จะค้นหา Logon script ของผู้ใช้บนโลคอลไดรฟ์ C: ด้วยเหตุนี้ login script ทั้งหมดควรจะถูกก็อบปี้ไปไว้ที่คอนโทรลเลอร์ทั้งหมดที่อยู่ในโดเมน

3.5.1 การสร้าง logon script

เนื่องจาก logon script เป็นแบตช์ไฟล์ดังนั้นมันจะสามารถเก็บคำสั่งแบตช์ไฟล์บนนระบบปฏิบัติการของผู้ใช้ได้เช่นกัน คุณสามารถเขียนสคริปต์ให้ง่าย ๆ หรือซับซ้อนเท่าที่ต้องการได้ นี่เป็นตัวอย่างหนึ่งของไฟล์ล็อกออน

```
@echo off
net time \\rcisvr /set
net use d: \\rcisrv\books
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

net use lpt1 \\rci2\hplj4

บรรทัด net time จะทำหน้าที่ตั้งเวลานาฬิกาบนเครื่องเวิร์กสเตชันให้ตรงกับบนเซิร์ฟเวอร์ที่ชื่อ rcisvr บรรทัดต่อมาจะกำหนดไดรฟ์ D: ให้ตรงกับโฟลเดอร์ Books บนเครื่องคอมพิวเตอร์ที่ชื่อ rcisvr2 บรรทัดสุดท้ายจะต่อพอร์ต LPT1 กับแชร์พรินเตอร์ที่ชื่อ Hplj4 ทั้งวินโดวส์ 95 และวินโดวส์ฟอร์เวิร์กกรุ๊ปจะทำงานก่อนที่ผู้ใช้จะล็อกออนเข้าสู่ระบบ ดังนั้น logon script บนเครื่องที่ใช้ระบบปฏิบัติการเหล่านี้จะทำงานอยู่ในเซสชันเวอร์ชวลเอ็มเอสดอส ผู้ใช้ที่ทำงานบนเครื่องเวิร์กสเตชันที่ใช้วินโดวส์ 95 จะเห็นไดอะล็อกบ็อกซ์เล็ก ๆ ที่แนะนำให้รอการทำงานของสคริปต์

3.5.2 ตัวแปรสำหรับ logon script

คุณสามารถใช้ตัวแปรในตาราง 3.3 ได้ถ้าต้องการใช้ logon script เพียงไฟล์กับผู้ใช้หลาย ๆ คน ตัวอย่างเช่น คุณสามารถป้อนตัวแปร %HOMEDRIVE% เพื่อใช้แทน home directory ของผู้ใช้แต่ละคนในสคริปต์ที่ใช้กับผู้ใช้หลาย ๆ คนได้ แต่ตัวแปรเหล่านี้ใช้งานได้เฉพาะในสคริปต์บนวินโดวส์เอ็นทีเวิร์กสเตชันเท่านั้น ไม่สามารถใช้กับเวิร์กสเตชันบนวินโดวส์ 95 ได้

ตารางที่ 3.3 ตัวแปรที่ใช้งานบน logon script บนเครื่องเอ็นทีได้

4 ตัวแปร	5 รายละเอียด
%HOMEDRIVE%	Drive letter บนเครื่องเวิร์กสเตชันโลคอลของผู้ใช้ที่สัมพันธ์กับ home directory
%HOMEPATH%	ชื่อพาทแบบเต็มของ home directory ของผู้ใช้
%HOMESHARE%	ชื่อของ home directory ที่ผู้ใช้ใช้ร่วมกัน
%OS%	ระบบปฏิบัติการของผู้ใช้
%PROCESSOR_ARCHITECTURE%	ประเภทของโปรเซสเซอร์บนเครื่องเวิร์กสเตชันของผู้ใช้
%PROCESS_LEVEL%	ระดับโปรเซสเซอร์บนเครื่องเวิร์กสเตชันของผู้ใช้
%USERDOMAIN%	โดเมนที่กำหนด account ของผู้ใช้
%USERNAME%	Account user name

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.5.3 **การกำหนด logon scripts** สำหรับวิธีการกำหนด logon script ให้กับผู้ใช้คนหนึ่งนั้นให้ทำตามขั้นตอนต่อไปนี้

1. เขียนแบตช์ไฟล์ที่จะใช้เป็น logon script แล้วเซฟไว้ใน logon script path บนเครื่องเซิร์ฟเวอร์ ซึ่งควรจะเป็นพาทนี้

C:\WINNT\SYSTEM32\REPL\IMPORT\SCRIPTS

2. เรียกโปรแกรม User Manager for Domain มาทำงานและดับเบิลคลิกที่ account ของผู้ใช้นั้น

3. ที่ไดอะล็อกบ็อกซ์ User Properties คลิกที่ปุ่ม Profile

4. ที่ไดอะล็อกบ็อกซ์ User Environment Profile ให้พิมพ์ชื่อของแบตช์ไฟล์ลงในเท็กซ์บ็อกซ์ Logon Script Name

5. คลิกที่ปุ่ม OK สองครั้งเพื่อปิดไดอะล็อกบ็อกซ์จากนั้นให้ปิดโปรแกรม User Manager for Domains

ไม่จำเป็นต้องใส่พาทไว้ในเท็กซ์บ็อกซ์ Logon Script Name เนื่องจากเมื่อผู้ใช้ล็อกออนเข้าไป การค้นหา logon script จะเริ่มที่พาทดีฟอลต์นี้อยู่แล้ว

3.5.4 **การทำซ้ำ logon script บนโดเมนอื่น**

โดยปกติแล้ว logon script จะถูกดาวน์โหลดจากเครื่องเซิร์ฟเวอร์ที่ตรวจสอบการล็อกออนของผู้ใช้ แต่ระบบเครือข่ายส่วนมากจะประกอบด้วย domain controller มากกว่าหนึ่งเครื่อง (อย่างน้อยก็มี primary controller กับ backup controller) ดังนั้นคุณคงต้องการความมั่นใจว่าจะมี logon script อยู่บนคอนโทรลเลอร์ทุก ๆ ตัวในกรณีที่เกิดมีคอนโทรลเลอร์ตัวใดตัวหนึ่งไม่ทำงาน

บริการ Directory Replicator จะช่วยให้คุณมั่นใจว่าจะมี logon script สำรองไว้อยู่เสมอ (ซึ่งจะมีความสามารถในการเก็บรักษาก็อบปี้ทั้งไดเรกทอรีไว้บนเครื่องคอมพิวเตอร์หลาย ๆ ตัว)

ส่วนต่างๆ ที่ได้กล่าวมาข้างต้นแม้ว่าบางส่วนจะไม่เกี่ยวข้องโดยตรงกับระบบรักษาความปลอดภัยของวินโดวส์เอ็นทีก็ตามแต่หากใช้อย่างไม่ระมัดระวังแล้วก็อาจเป็นบ่อเกิดของความเสียหายที่อาจจะเกิดขึ้นไม่ว่าจะเกิดจากผู้ใช้งานภายในระบบเครือข่ายเองหรือจากผู้เจาะระบบหรือแม้แต่เกิดจากความผิดพลาดในการทำงานของตัวระบบปฏิบัติการเอง ซึ่งโดยสรุปแล้วก็คือควรมีการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กำหนดการใช้งานเท่าที่จำเป็น และกำหนดนโยบายอย่างถูกต้องรัดกุมเพื่อให้เกิดความปลอดภัยสูงสุดของระบบเครือข่าย



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4
ไฟร์วอลล์ (Firewall)

อะไรคือ อินเตอร์เน็ตไฟร์วอลล์

ไฟร์วอลล์เป็นระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ (network security) ที่มีประสิทธิภาพซึ่งมีทั้งที่เป็น software และ hardware โดยตัวไฟร์วอลล์เองจะเป็นตัวที่ทำการติดต่อกับระบบเครือข่ายคอมพิวเตอร์ซึ่งจะมี กฎ หรือข้อกำหนด ในการเข้าและออกของข้อมูลที่ใช้ในการส่งผ่านระหว่างเครือข่ายทั้งสอง เปรียบเสมือนคูน้ำที่ล้อมรอบเมืองที่ป้องกันไฟลุกลามเข้าปราสาท มีจุดประสงค์หลายอย่าง คือ

ไฟร์วอลล์จำกัดคนที่จะเข้ามาในส่วนควมคุม

ไฟร์วอลล์ป้องกันการบุกรุกจากที่อื่น

ไฟร์วอลล์จำกัดคนที่สามารถเข้ามาในส่วนที่ควบคุม

ระบบรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ต (ไฟร์วอลล์) ส่วนใหญ่จะติดตั้งในจุดที่เชื่อมระหว่างเครือข่ายภายในองค์กร และเครือข่ายอินเตอร์เน็ต โดยการสัญจรจากเครือข่ายอินเตอร์เน็ตหรือจากเครือข่ายภายในองค์กร จะต้องผ่านระบบรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ต (ไฟร์วอลล์) ซึ่งโดยส่วนใหญ่ระบบนี้จะต้องประกอบด้วยส่วนของฮาร์ดแวร์ คือ เราเตอร์ (router), โฮสคอมพิวเตอร์ , การเชื่อมต่อกันของเราเตอร์ , เครื่องคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ โดยเหมาะกับ ซอฟท์แวร์ และสำหรับโครงสร้างของการป้องกันจะขึ้นกับนโยบาย,งบประมาณ และ องค์ประกอบทั้งหมดโดยรวม

ข้อดีของระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์

1. ไฟร์วอลล์เป็นจุดรวมสำหรับการตัดสินใจอย่างปลอดภัย
   ไฟร์วอลล์เปรียบเสมือนจุดตรวจ (check point) ในการส่งผ่านข้อมูลเข้าออก จะผ่านจุดตรวจสอบที่เป็นช่องทางเดียวที่ข้อมูลจะสามารถผ่านได้ และเป็นจุดที่ติดต่อกับเครือข่ายอินเตอร์เน็ต
2. ไฟร์วอลล์สามารถทำงานได้ตามข้อกำหนดต่างๆได้
   ไฟร์วอลล์เปรียบเสมือนตำรวจที่ทำงานบนเส้นทางที่ให้บริการ และมีกฎเกณฑ์ ข้อบังคับในการควบคุมจะอนุญาตให้กับส่วนที่สามารถผ่านได้เท่านั้น
3. ไฟร์วอลล์สามารถเก็บรายละเอียดต่างๆ ได้อย่างมีประสิทธิภาพ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในการเข้าออกของข้อมูลทุกๆ ข้อมูล ไฟร์วอลล์จะทำการเก็บบันทึกข้อมูลต่างๆ ที่เกี่ยวกับระบบเครือข่ายไว้เพื่อใช้ในการตรวจสอบดูว่าเกิดอะไรขึ้นกัยระบบบ้างทั้งเครือข่ายภายในและเครือข่ายภายนอก

4. ไฟร์วอลล์สามารถเปิดเผยข้อมูลได้ในส่วนที่จำเป็น

ข้อเสียของระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์

1. ไฟร์วอลล์ไม่สามารถป้องกันผู้ประสงค์ร้ายที่อยู่ภายในระบบได้

ถ้ามีผู้ประสงค์ร้ายอยู่ภายในระบบของไฟร์วอลล์เอง ตัวของไฟร์วอลล์จะไม่สามารถป้องกันได้ ผู้ใช้ภายในระบบสามารถสร้างความเสียหายให้กับระบบได้

2. ไฟร์วอลล์ไม่สามารถป้องกันการติดต่อที่ไม่ได้ผ่านตัวไฟร์วอลล์ได้

ไฟร์วอลล์สามารถควบคุมการสัญจรที่ผ่านมัน แต่ถ้าไม่มี ไฟร์วอลล์ก็ไม่สามารถทำอะไรได้ เช่น ถ้าไซต์ (site) อนุญาตให้เข้าถึงโดยการโทรเข้าแต่อยู่หลังไฟร์วอลล์ ไฟร์วอลล์ก็ไม่สามารถป้องกันได้

3. ไฟร์วอลล์ไม่สามารถป้องกัน ไวรัส

ไฟร์วอลล์ไม่สามารถป้องกันไวรัส ที่เกิดบนเครือข่ายได้ แม้ว่าไฟร์วอลล์ จะสแกน ทุกๆ การสัญจรที่เข้ามาในระบบเครือข่ายภายใน ก็ตาม แต่มันจะสแกนเฉพาะ จุดเริ่มต้น จุดปลายทาง และหมายเลยพอร์ต (port) แต่ตัวของไฟร์วอลล์เอง ก็ไม่ได้ดูรายละเอียดของข้อมูล และมีไวรัสหลายชนิดที่เข้ามาในระบบโดยการซ่อนตัวเข้ามากับข้อมูล

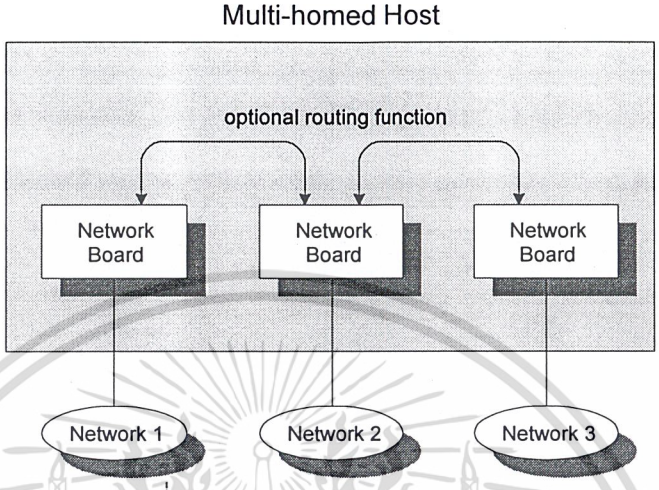
4.1 สถาปัตยกรรมของไฟร์วอลล์ (firewall architecture)

4.1.1 ดูอัลโฮมโฮสท์ (Dual-Homed Host architecture)

ในเครือข่ายแบบ ทีซีพี ไอพี (TCP/IP) เทอมของมัลติโฮมโฮสท์ (Multi-home host) คือ โฮสต์ที่มีหลายแผงการเชื่อมต่อเครือข่าย (network interface board) ซึ่งโดยทั่วไปแผงการเชื่อมต่อจะถูกเชื่อมกับเครือข่าย ดังรูปที่ 4.1 ในอดีต มัลติโฮมโฮสต์ นี้สามารถกำหนดเส้นทางระหว่างเครือข่าย เทอมเกตเวย์ (gateway) ถูกใช้ระบุหน้าที่ในการหาเส้นทาง (routing function) แต่วันนี้เทอมของเราเตอร์ (router) ถูกใช้ระบุหน้าที่ในการหาเส้นทางเพราะว่า เทอมของเกตเวย์ถูกจองไว้สำหรับหน้าที่ที่เหมาะสม กับชั้นสูงๆของระบบโอเอสไอโมเดล (OSI model) ถ้าหน้าที่ในการหาเส้นทาง (routing function) ในมัลติโฮมโฮสท์ไม่ทำงานได้โฮสต์จะทำการแบ่งแยกเส้นทางของเครือข่ายระหว่างเครือข่ายที่มันติดต่ออยู่และเครือข่ายอื่นๆที่สามารถจัดการกับแอพพลิเคชั่น (application) บนมัลติโฮมโฮสท์โดยเฉพาะอย่างยิ่งถ้าแอพพลิเคชั่นอนุญาตให้เครือข่ายสามารถที่จะแบ่งปันข้อมูล (share data) ได้ ดูอัลโฮมโฮสท์ (dual-home host) เป็น

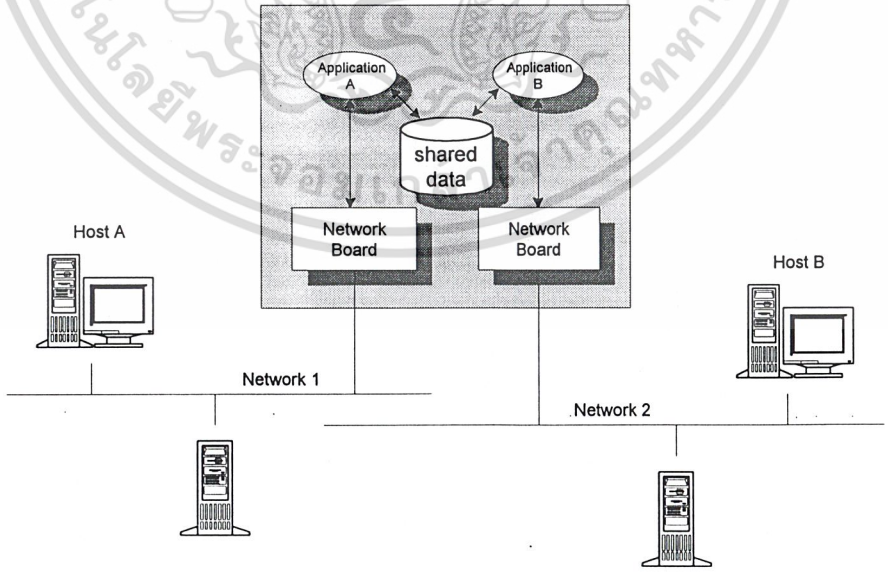
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งไม่อนุญาตให้นำไปดัดแปลง เผยแพร่ หรือนำไปใช้ในรูปแบบอื่นๆ

ตัวอย่างพิเศษของมัลติโฮมโฮสท์ซึ่งมีสองเครือข่ายมาอินเตอร์เฟส (interface) กัน โดยที่ไม่มีการระบุหน้าที่ในการหาเส้นทาง ดังรูปที่ 4.2 แสดงตัวอย่างของดูอัลโฮมโฮสท์ ซึ่งไม่มีการใช้การระบุ



รูปที่ 4.1 แสดง Classic multi-home host

หน้าที่ ในการหาเส้นทางโฮสท์ เอ (host A) อยู่บนเครือข่ายที่หนึ่งซึ่งสามารถเข้าถึงแอพพลิเคชั่น บี (application B) บนดูอับโฮมโฮสท์ แอพพลิเคชั่นทั้งสองบนดูอัลโฮมโฮสท์สามารถแบ่งปันข้อมูลได้ จึงเป็นไปได้ว่า โฮส เอ และโฮส บี สามารถแลกเปลี่ยนข้อมูลผ่านข้อมูลที่ถูกแบ่งปันบนดูอัลโฮมโฮสท์และยังไม่แลกเปลี่ยนเส้นทางของเครือข่ายระหว่างสองส่วนของเครือข่าย ที่เชื่อมต่อกับดูอัลโฮมโฮสท์

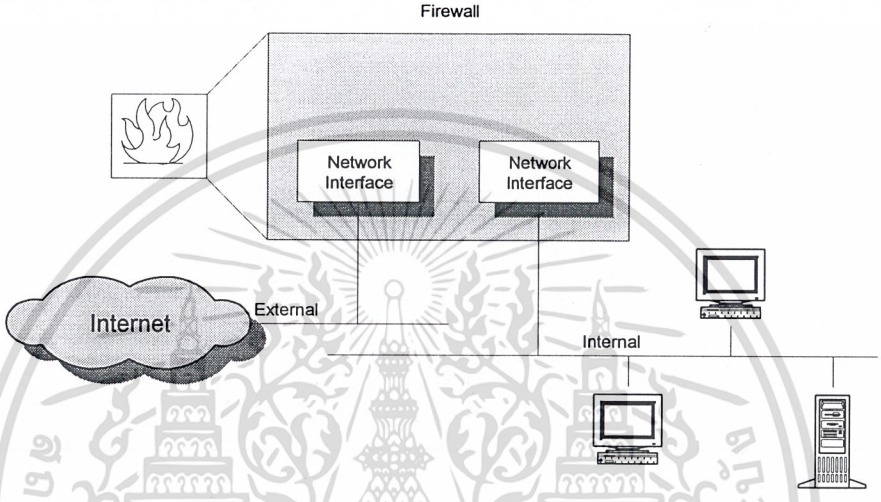


รูปที่ 4.2 แสดง Dual-home host

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ดูอัลโฮมโฮสท์ (Dual- homed host) ที่เป็นไฟร์วอลล์

ดูอัลโฮมโฮสท์สามารถแยกเครือข่ายภายใน (ซึ่งอย่างน้อย 2 เครือข่าย) และเครือข่ายภายนอก ดังรูปที่ 4.3 เพราะดูอัลโฮมโฮสท์ไม่ขึ้นกับการส่งแบบทีซีพี ไอพี (TCP/IP) มันสามารถขัดขวางทุกๆ ไอพี (IP) ระหว่างเครือข่ายภายในและเครือข่ายภายนอก ที่ไม่น่าไว้วางใจ



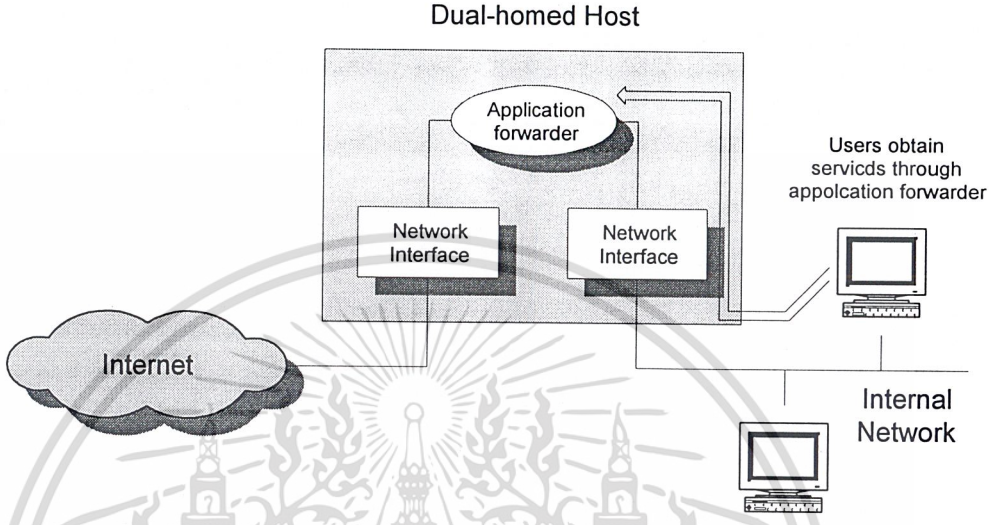
รูปที่ 4.3 แสดง Dual home-host ที่เป็นไฟร์วอล

การบริการของอินเตอร์เน็ต เช่น จดหมาย (mail) และข่าวสาร (new) เป็นสิ่งที่จำเป็นพื้นฐานในการบริการเก็บและส่ง ถ้าการบริการเหล่านี้ทำงานบน ดูอัลโฮมโฮสท์จะทำให้สามารถกำหนดโครงสร้างในการส่งแอพพลิเคชั่นจากเครือข่ายหนึ่งถึงที่อื่นๆ ถ้าข้อมูลแอพพลิเคชั่น จำเป็นที่จะต้องข้ามไฟร์วอลล์ ผู้ส่งต่อแอพพลิเคชั่น (application forwarder) สามารถติดตั้งให้ทำงานบนดูอัลโฮมโฮสท์ได้ ดังรูปที่ 4.4 ผู้ส่งต่อแอพพลิเคชั่น (application forwarder) คือ ซอร์ฟแวร์ (software) พิเศษที่ถูกใช้ส่งระหว่างสองเครือข่าย ที่ติดต่อกัน การเข้าถูกอย่างอื่นคือ อนุญาตให้ผู้ใช้เข้ามาล็อกอิน (login) ในดูอัลโฮมโฮสท์และเข้าถึงบริการภายนอกจากเครือข่ายภายนอกที่เชื่อมติดต่อกับ ดูอัลโฮมโฮสท์ ดังรูปที่ 4.5

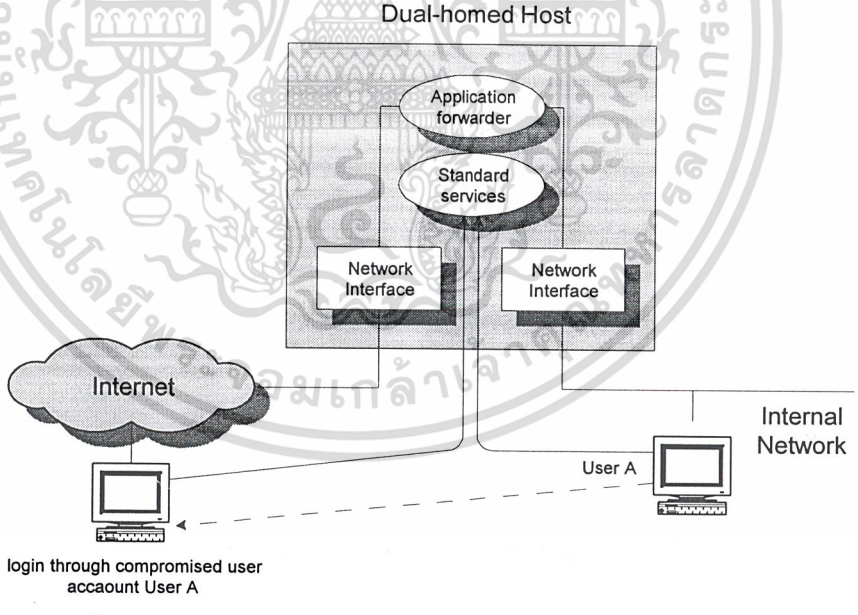
ถ้าผู้ส่งต่อแอพพลิเคชั่น (application forwarders) ที่ถูกใช้การสัญจรของ แอพพลิเคชั่นจะไม่สามารถผ่านดูอัลโฮมโฮสท์ไฟร์วอลล์ นอกเสียจากว่าผู้ส่งต่อแอพพลิเคชั่น ถูกกำหนดไว้บนไฟร์วอลล์ ถ้าผู้ใช้ได้รับการอนุญาตจากไฟร์วอลล์โดยตรง ดังรูปที่ 4.5 ระบบรักษาความปลอดภัยของไฟร์วอลล์สามารถประนีประนอมได้ เพราะว่าดูอัลโฮมโฮสท์ไฟร์วอลล์เป็นจุดศูนย์รวมการติดต่อระหว่างเครือข่ายภายนอกและภาย

เอกสารนี้เป็นเอกสาร[illegible]ใช้เพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ หาประโยชน์ในเชิงพาณิชย์ หรือการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ใน ดังนั้นดูอัลโฮมโฮสท์ไฟร์วอลล์ก็จะอยู่ในบริเวณที่มีความเสี่ยง (zone of risk) ถ้าผู้ใช้เลือกรหัสผ่าน (password) ที่อ่อนแอ ในบริเวณที่มีความเสี่ยงก็สามารถขยายมาที่ระบบเครือข่ายภายในทำให้ผิดจุดประสงค์ของดูอัลโฮมโฮสท์ของไฟร์วอลล์ได้



รูปที่ 4.4 แสดงดูอัลโฮมโฮสต์ซึ่งมีผู้ส่งต่อแอปพลิเคชั่น



รูปที่ 4.5 แสดงความไม่ปลอดภัยเมื่อผู้ใช้ล็อกอินเข้ามาในดูอัลโฮมโฮสต์

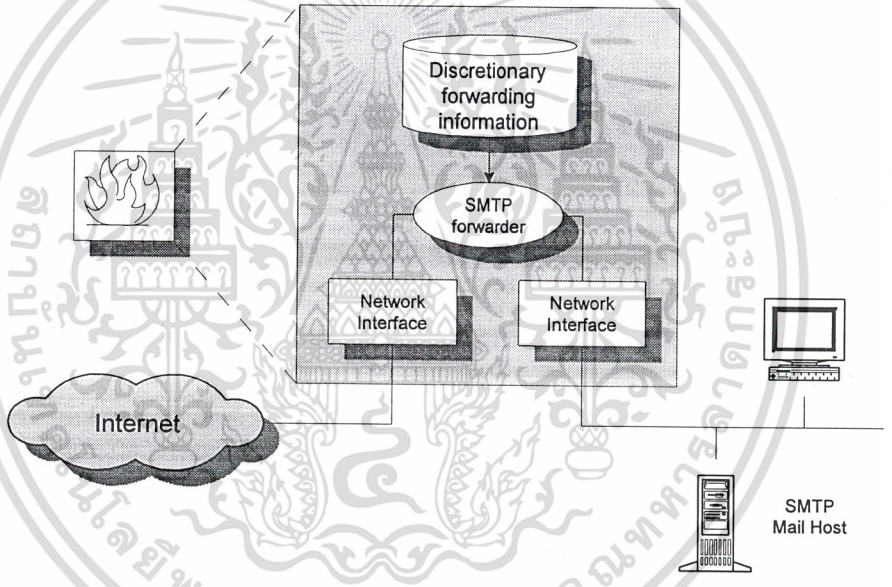
หมายเหตุ

ผู้จัดการระบบรักษาความปลอดภัย จะไม่ทำการสร้างบัญชีของผู้ใช้ (user account) ให้เข้ามาที่ไฟร์วอลล์ ดังนั้นไฟร์วอลล์ควรจะถูกใช้ได้เฉพาะผู้ใช้ที่มีสิทธิโดยแท้จริงเท่านั้นที่จะผ่านเข้ามาได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ถ้าหากมีการเก็บรายละเอียดของผู้ใช้ การล็อกอินของผู้ใช้ (user login) ไว้อย่างดี มันจะถูกบุกรุกเมื่อมีการผิดเพี้ยนของระบบรักษาความปลอดภัย ดังนั้นควรจะมีการบันทึกไว้ว่ามีใครเข้ามาบ้าง

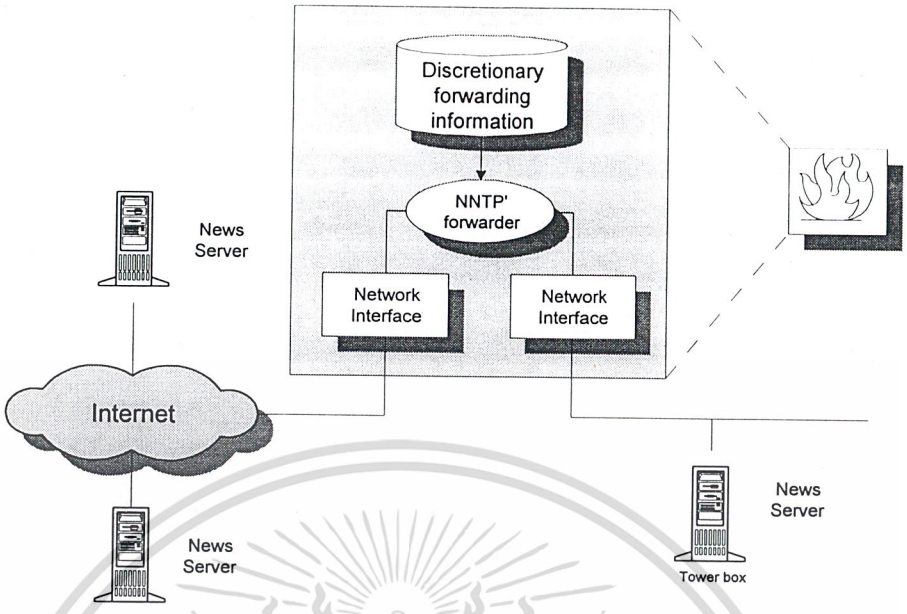
ตัวอย่างการบริการเก็บและส่ง คือ เอสเอ็มทีพี (SMTP – mail) และ เอ็นเอ็นทีพี (NNTP-mail) ดังรูปที่ 4.6 แสดงการติดตั้งระมัดระวังในการส่งข้อมูล (discretionary forwarding) ของข้อความเมล์ (mail) ระหว่างเครือข่ายภายนอกที่ไม่น่าไว้วางใจกับเครือข่ายภายใน ดังรูปที่ 4.7 แสดงการติดตั้งตัวระมัดระวังในการส่งข้อมูลสำหรับข้อความข่าวสาร (news) ระหว่างเซิร์ฟเวอร์ข่าวสาร (news servers) บนเครือข่ายภายนอกและเครือข่ายภายใน



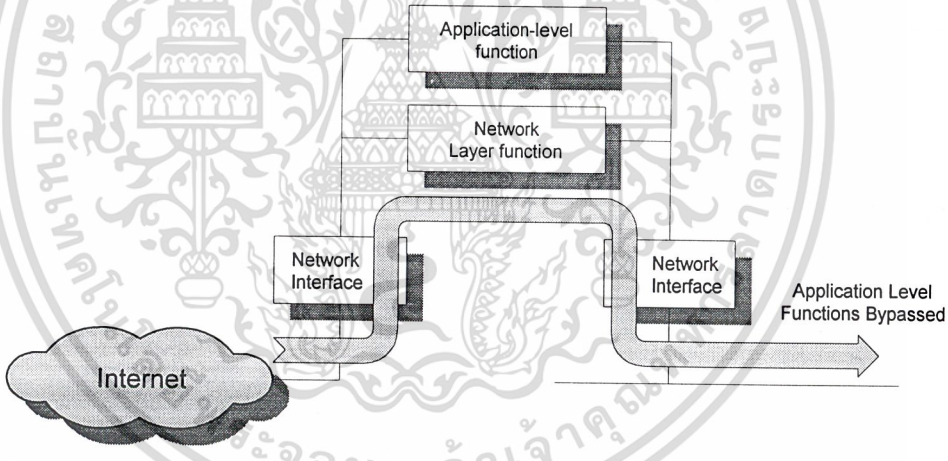
รูปที่ 4.6 แสดงดูอัลโฮมโฮสต์ที่มีผู้ส่งต่อเมล์ (mail forwarder)

ดูอัลโฮมโฮสท์เป็นโครงสร้างพื้นฐานที่ใช้ในไฟร์วอลล์ ความสามารถที่ใช้เมื่อ ฉุกเฉินของดูอัลโฮมโฮสม์ คือ เมื่อการหาเส้นทาง (router) ใช้ไม่ได้ และมีเพียงเส้นทางระหว่างส่วนหนึ่งของเครือข่าย (network segment) ที่ผ่านทางแอพพลิเคชั่น (application layer) เมื่อตัวหาเส้นทางมีปัญหา ไอพี (IP) ก็สามารถส่งไปได้ มันคือไม่ผ่านชั้นแอพพลิเคชั่นของดูอัลโฮมโฮสทีไฟร์วอลล์ ดังรูปที่ 4.7

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.7 ดูอัลโฮมโฮสต์ที่มีตัวส่งต่อเอกสาร (news forwarder)

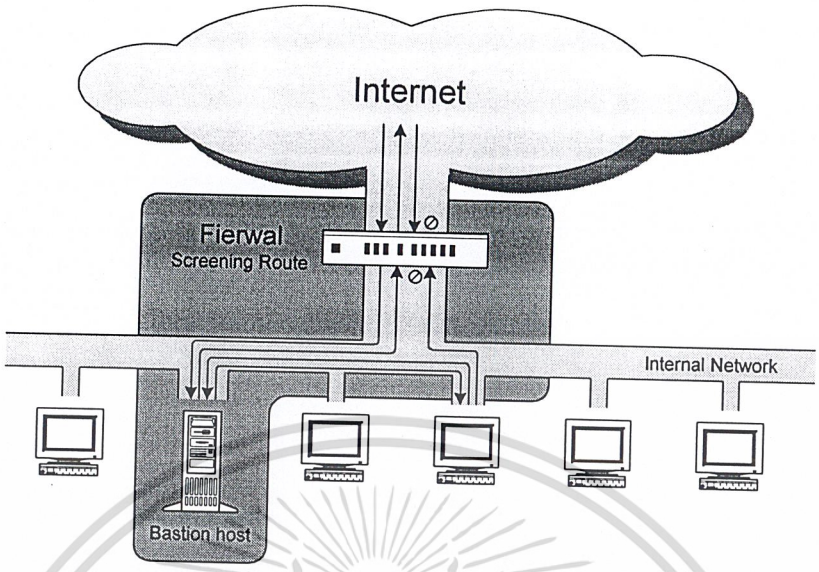


รูปที่ 4.8 แสดงการคอนฟิก (config) ที่ผิดพลาดบนดูอัลโฮมโฮสต์ไฟร์วอล

4.1.2 **สถาปัตยกรรมสกรีนโฮสท์** (screened host architectures)

ขณะที่สถาปัตยกรรมแบบดูอัลโฮมโฮสท์จัดการกับการบริการที่เกี่ยวกับหลายๆ เครือข่าย (แต่ไม่มีการหาเส้นทาง) ส่วนสถาปัตยกรรมแบบสกรีนโฮสต์ (Screened host architectures) จะจัดการบริการ (Service) จารโฮสท์ที่เข้ามาติดต่อกับเครือข่ายภายใน โดยการแบ่งการหาเส้นทาง ซึ่งการป้องกันขั้นแรกจะใช้ แพ็กเก็ตฟิลเตอร์ริ่ง (packet filtering)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.9 แสดงสถาปัตยกรรมแบบสกรีนโฮสต์

แบสชั่นโฮสท์ (bastion host) จะต้องอยู่บนเครือข่ายภายใน แพ็กเก็ตฟิลเตอร์ริ่ง (packet filtering) บนสกรีนนิ่งเราเตอร์ (screening router) จะกำหนดเส้นทางให้ผ่าน แบสชั่นโฮสท์ ก่อนทุกครั้งจึงจะติดต่อได้

โครงสร้างของแพ็กเก็ตฟิลเตอร์ริ่งในสกรีนนิ่งเราเตอร์ อาจจะกระทำอย่างใดอย่างหนึ่งดังต่อไปนี้

- สำหรับโฮสท์ที่แน่นอน จะอนุญาตให้ โฮสท์ภายใน (internal host) ติดต่อกับโฮสท์บนอินเตอร์เน็ตได้
- ไม่อนุญาตทุกการติดต่อจากโฮสท์ภายใน

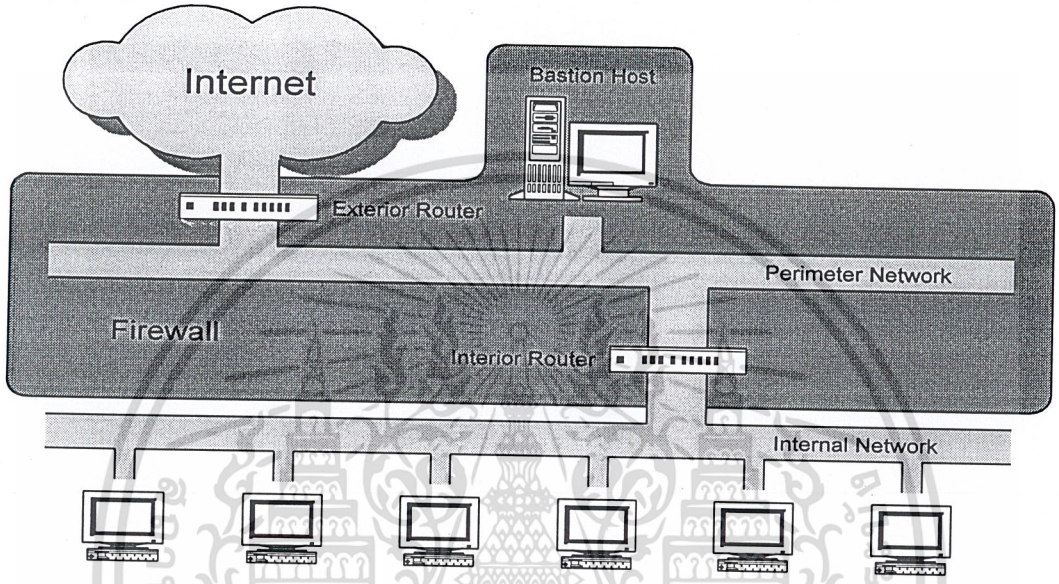
คุณสามารถผสมและรวม (match) การเข้าถึงเหล่านี้ในแต่ละบริการ บางบริการอนุญาตให้ผ่านแพ็คเก็ตฟิลเตอร์ริ่งโดยตรง ขณะที่อื่นๆ อาจจะไม่อนุญาตให้ผ่านได้โดยตรง โดยขึ้นอยู่กับข้อกำหนดของแต่ละไซท์ (site) ที่ตั้งขึ้น

ในสถาปัตยกรรมนี้แพ็กเก็ตผ่านจากอินเตอร์เน็ตเข้าสู่เครือข่ายภายในโดยตรง จึงดูเหมือนว่ามีความเสี่ยงมากกว่า ดูอัลโฮสท์ที่ไม่มีแพ็กเก็ตภายนอกเข้าถึงเครือข่ายภายในได้ ในทางปฏิบัติดูอัลโฮมโฮสท์อาจจะเสียหายได้ง่าย ซึ่งทำให้แพ็กเก็ตผ่านเข้ามาได้ นอกจากนี้มันง่ายกว่าในทางป้องกันด้วยเราเตอร์ (router) ซึ่งสามารถจำกัดกลุ่มของการบริการมากกว่าการป้องกันด้วยโฮสท์ ด้วยจุดนี้ สกรีนโฮสท์จึงรักษาความปลอดภัยได้ดีกว่า และนิยมใช้มากกว่าดูอัลโฮมโฮสท์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1.3 **สถาปัตยกรรมแบบสกรีนสับเน็ต** (screened subnet architecture)

สถาปัตยกรรมแบบสกรีนสับเน็ต (screened subnet architecture) ได้เพิ่มชั้นพิเศษของความปลอดภัยบนสถาปัตยกรรมแบบสกรีนโฮสท์โดยเพิ่มชั้นของเครือข่าย เพอริมิเตอร์ (perimiter network) เพื่อแ บ่งเครือข่ายภายในจากอินเตอร์เน็ต



รูปที่4.10 สถาปัตยกรรมแบบสกรีนสับเน็ต(Screened subnet architecture)ที่ใช้เราเตอร์2 ตัว

โดยทั่วไปแบสชั่นโฮสท์ (bastion host) เป็นเครื่องที่อ่อนแอบนเครือข่าย ถึงแม้ว่าจะพยายามป้องกันแต่ก็มักจะถูกบุกรุก สำหรับในสกรีนโฮสท์ถ้าแบสชั่นโฮสท์ถูกบุกรุก จะไม่มีอะไรที่จะป้องกันระหว่างมันกับเครื่องกลภายใน ดังนั้นถ้ามีคนบุกรุกเข้ามาในแบสชั่นโฮสท์ของสกรีนโฮสท์ได้ถือว่าถูกรางวัลใหญ่

การแบ่งแบสชั่นโฮสท์ไว้บนเครือข่ายเพอริมิเตอร์ (perimiter network) คุณก็สามารถลดผลกระทบที่เกิดจากการที่มีคนบุกรุกแบสชั่นโฮสท์ มันจะช่วยป้องกันผู้บุกรุกในการเข้าถึงแต่ไม่ถึงกับทั้งหมด

โดยทั่วไปสถาปัตยกรรมแบบสกรีนสับเน็ตจะมีสกรีนนิ่งเราเตอร์ (screening router) สองตัวซึ่งแต่ละตัวจะเชื่อมต่อกับเครือข่ายเพอริมิเตอร์ ดังรูปที่ 4.10 ในการบุกรุกเข้าสู่เครือข่ายภายในจะต้องผ่านเราเตอร์ถึง สองตัว อย่างไรก็ตามถ้าระบบฟิลเตอร์ริ่ง (filtering) ระหว่างแต่ละชั้นอนุญาตในสิ่งเดียวกัน ชั้นที่เพิ่มขึ้นก็ไม่ได้เพิ่มความปลอดภัย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เครือข่ายเพอริมิเตอร์ (perimiter)

เครือข่ายเพอริมิเตอร์ (perimiter network) เป็นชั้นพิเศษของความปลอดภัย โดยเพิ่มแทรกระหว่างเครือข่ายภายนอก(external network) และเครือข่ายที่จะทำการป้องกัน (Protected network) ถ้าผู้บุกรุกเข้ามาที่ชั้นนอกสุดของไฟร์วอลล์ เครือข่ายเพอริมิเตอร์ก็จะทำการป้องกันอีกชั้นหนึ่ง

บนเครือข่ายเพอริมิเตอร์ ถ้ามีคนบุกรุกเข้ามาในแบสชั่นโฮสท์บนเครือข่าย เพอริมิเตอร์เขาก็สามารถเห็นได้เพียงการสัญจร (traffic) บนเครือข่าย ทุกๆ การสัญจรบนเครือข่าย เพอริมิเตอร์ควรจะเป็นการเข้าถึงและออกจากแบสชั่นโฮสท์หรือไปถึงหรือออกจากอินเตอร์เน็ต เพราะว่าไม่มีการกำหนดเส้นทาง ของเครือข่ายภายในให้ผ่านเครือข่าย เพอริมิเตอร์ ดังนั้นเครือข่ายเพอริมิเตอร์ ก็จะปลอดภัยจากการบุกรุกถ้าแบสชั่นโฮส์รัดกุม

แบสชั่นโฮสท์ (bastion host)

เป็นโฮสท์ที่เป็นจุดรวมของการติดต่อกับโลกภายนอก เช่น

-สำหรับ รับ และ ส่ง อีเมล์ (SMTP mail)

- รับการติดต่อ FTP ไปที่ไซท์ของ แอโนนีมัสเซิร์ฟเวอร์ (anonymous servers)
- รับโดเมนเนมเซอวิส (Domain Name Service : DNS) คำถามเกี่ยวกัยไซท์และอื่นๆ การบริการออกสู่ภายนอกจะกระทำได้ดังนี้ จากไคลเอนต์ภายใน (internal clients) ถึงเซิร์ฟเวอร์บอินเตอร์เน็ต
- ตั้งแพ็กเก็ตฟิลเตอร์ริ่ง (packet filtering) บนทั้งเราเตอร์ภายนอก (external router) และเราเตอร์ภายใน (internal router) อนุญาตให้ไคลเอนท์ภายใน(internal clients) เข้าถึงเซิร์ฟเวอร์ภายนอก (external servers) ได้โดยตรง
- ตั้งพร็อกซี่เซิร์ฟเวอร์ (proxy servers) ให้ทำงานบนแบสชั่นโฮสท์ ในการอนุญาตไคลเอนท์ภายในให้เข้าถึงเซิร์ฟเวอร์ภายนอก (external servers) ทำไม่ได้โดยตรง แต่จะทำโดยตั้งแพ็กเก็ตฟิลเตอร์ริ่งให้ไคลเอนท์ภายในคุยกับพร็อกซี่เซิร์ฟเวอร์คุยกับแบสชั่นโฮสท์แต่ห้ามการติดต่อกันโดยตรงระหว่างไคลเอนท์ภายในกับโลกภายนอก

ในแต่ละกรณีแพ็กเก็ตฟิลเตอร์ริ่งอนุญาตให้แบสชั่นโฮสท์ติดต่อไปและตอบรับการติดต่อกับโฮสท์บนอินเตอร์เน็ต โดยจะขึ้นอยู่กับข้อกำหนดของแต่ละไซท์

เราเตอร์ภายใน (internal router)

เราเตอร์ภายในบางครั้ง เรียก โช้คเราเตอร์ (choke router) ในไฟร์วอลล์ ทำหน้าที่ป้องกันเครือข่ายภายในจากอินเตอร์เน็ตและเครือข่ายเพอริมิเตอร์ โดยเราเตอร์ภายในจะทำการเลือก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บริการที่ออกจากเครือข่ายภายในไปที่อินเตอร์เน็ตโดยจะมีการตรวจสอบโดยแพ็กเก็ตฟิลเตอร์ริ่ง โดยการบริการที่มักจะให้มีการติดต่อออกได้แก่ เทลเน็ต (telnet) , เอฟทีพี (FTP) , WAIS, Archie , Gopher และ แอพพลิเคชั่นอื่นๆ ที่เหมาะสมกับความต้องการ

การบริการที่เราเตอร์ภายในจะให้อนุญาตระหว่างแบสชั่นโฮสท์กับเครือข่ายภายในโดยไม่จำเป็นต้องเป็นการบริการเดียวกับที่ให้อนุญาตระหว่างอินเตอร์เน็ตกับเครือข่ายภายใน เหตุผลที่จำกัดการบริการระหว่างแบสชั่นโฮสท์และเครือข่ายภายใน คือ ลดจำนวนโอกาสบุกรุกจากแบสชั่นโฮสท์

เราเตอร์ภายนอก (exterior router)

เราเตอร์ภายนอก บางครั้งเรียกว่า แอคเซสเราเตอร์ (access router) ทำหน้าที่ป้องกันทั้งเครือข่าย เพอริมิเตอร์ และเครือข่ายภายในจากอินเตอร์เน็ต ในทางปฏิบัติเราเตอร์ภายนอกตั้งใจจะอนุญาตเกือบทุกๆ สิ่งที่ออกจากเครือข่ายเพอริมิเตอร์ และทำแพ็กเก็ตฟิลเตอร์ริ่งน้อยมาก

แพ็กเก็ตฟิลเตอร์ริ่งที่ใช้บนเราเตอร์ภายนอกเป็นพิเศษที่ป้องกันเครื่องบนเครือข่ายเพอริมิเตอร์ (ซึ่งมีแบสชั่นโฮสท์และเครือข่ายภายใน) โดยทั่วไปจะไม่มีการป้องกันมาก เพราะโฮสท์บนเครือข่ายเพอริมิเตอร์ จะทำการป้องกันเริ่มแรก ผ่านโฮสท์ความปลอดภัย (host security)

4.1.4 การปรับเปลี่ยนสถาปัตยกรรมของ ไฟร์วอลล์ (firewall architecture)

สามารถใช้แบสชั่นโฮสท์ได้หลายตัว (multiple bastion host)

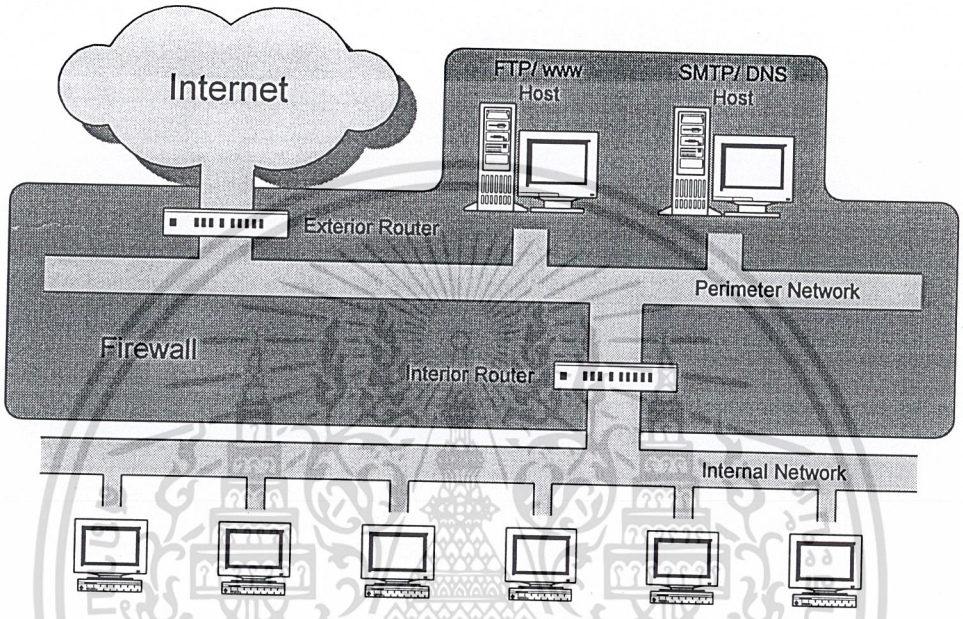
เราสามารถใช้แบสชั่นโฮสท์หลายๆ ตัวได้ เพื่อเพิ่มประสิทธิภาพ และต้องการการแบ่งข้อมูลหรือเซิร์ฟเวอร์ โดยเราอาจใช้แบสชั่นโฮสท์ตัวหนึ่งเป็นตัวหลักของผู้ใช้ของคุณ เช่น เอสเอ็มทีพีเซิร์ฟเวอร์ (SMTP server) , พร็อกซี่เซิร์ฟเวอร์ (proxy server) และอื่นๆ ขณะที่ โฮสท์อื่นๆ จัดการเกี่ยวกับอินเตอร์เน็ตที่ไม่เกี่ยวข้องกับผู้ใช้ของคุณ เช่น แอนโนนีมัส เอ็ฟทีพีเซิร์ฟเวอร์ (anonymous FTP server) ดังนั้นการทำงานของผู้ใช้ของคุณจะไม่ถูกดึงให้ช้าเพราะผู้ใช้ภายนอก

ในด้านการแสดงผล ในการใช้แบสชั่นโฮสท์หลายตัว บางการบริการมีความหนาแน่นมาก เช่น ยูสเน็ตนิวส์ (usenet news) มันเป็นไปได้ที่เราจะทำการบริการเดียวกันลงในแบสชั่นโฮสท์หลายตัว แต่มันจะยากในการทำการโหลดแบบสมมาตร (loading balance) แต่บริการส่วนมากต้องการเซิร์ฟเวอร์โดยเฉพาะการที่เราใช้แบสชั่นโฮสท์หลายตัวให้ดีที่สุดควรจะมีการคาดคะเนการใช้ว่าบริการใดควรจะมีเซิร์ฟเวอร์โดยเฉพาะ

ในด้านการเกินความต้องการ (redundancy) ถ้าไฟร์วอลล์คอนฟิก เป็นแแบสชั่นโฮสท์หลายตัว คุณควรจะมีการสำรอง คือ ถ้าตัวหนึ่งบกพร่อง (fail), บริการสามารถจัดการได้โดยอีกตัวหนึ่ง แต่ต้องระวังว่ามีเพียงการบริการบางอย่างเท่านั้นที่เข้าถึงได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

อาจจะใช้แบสชั่นโฮสท์หลายตัวในการเก็บข้อมูลของการบริการ จากการแทรกแซงกันและกัน นอกจากนี้ยังสามารถแบ่งความปลอดภัย เช่น ออกแบบให้ด้านหนึ่งเป็นเอชทีทีพีเซร์ฟเวอร์(HTTP server) เพื่อใช้สำหรับผู้ใช้บนอินเตอร์เน็ตและตัวใช้เป็นเจเนอรัลพับบลิก (general public) ซึ่งช่วยในการลดโหลด หรือเพิ่มประสิทธิภาพ



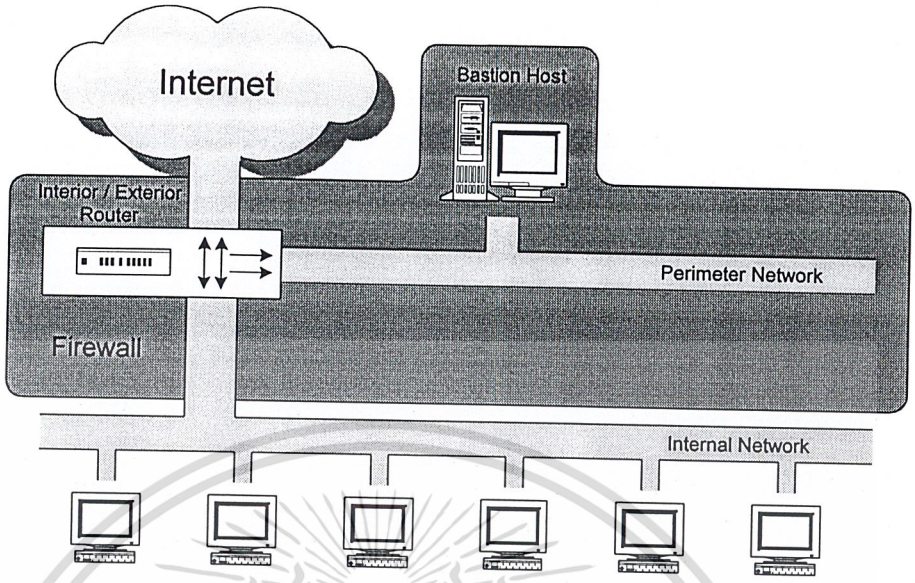
รูปที่ 4.11 แสดงสถาปัตยกรรมที่ใช้แบสชั่นโฮสต์ 2 ตัว

สามารถรวมเราเตอร์ภายใน (interior router) และเราเตอร์ภายนอก (exterior router)

สามารถใช้เราเตอร์ภายในและเราเตอร์ภายนอกเป็นเราเตอร์ตัวเดียว (single router) แต่จะต้องมีเราเตอร์ที่มีความสามารถเพียงพอและยืดหยุ่นได้ โดยทั่วไปคุณต้องการเราเตอร์ที่ทำการกรองทั้งเข้า และออกจากจุดเชื่อมต่อ

ถ้าเรารวมเราเตอร์ภายในและเราเตอร์ภายนอก ดังรูปที่ 4.12 จะมีเครือข่ายเพอริมิเตอร์และเครือข่ายภายในที่ติดต่อกับเราเตอร์ บางการสัญจรสามารถไหลได้โดยตรงระหว่างเครือข่ายภายในและอินเตอร์เน็ต (การสัญจรอนุญาตโดยตั้งกฎของแพ็กเก็ตฟิลเตอร์ริ่ง (packet filterring rule) สำหรับเราเตอร์) และการสัญจรอื่นก็สามารถไหลผ่านระหว่างเครือข่ายเพอริมิเตอร์และอินเตอร์เน็ต หรือเครือข่ายเพอริมิเตอร์กับเครือข่ายภายใน (การสัญจรนี้เรียกว่า พร็อกซี่)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.12 แสดงสถาปัตยกรรมโดยรวมเราเตอร์ภายในและเราเตอร์ภายนอก

สถาปัตยกรรมนี้คล้ายกัยสถาปัตยกรรมของสกรีนโฮสท์ ซึ่งทำให้ไซท์ที่ไม่มั่นคงรวมเอาเราเตอร์เข้าไปด้วย โดยทั่วไปเราเตอร์จะทำการป้องกันได้ง่ายกว่า โฮสท์ แต่มันจะถูกทะลุผ่านได้

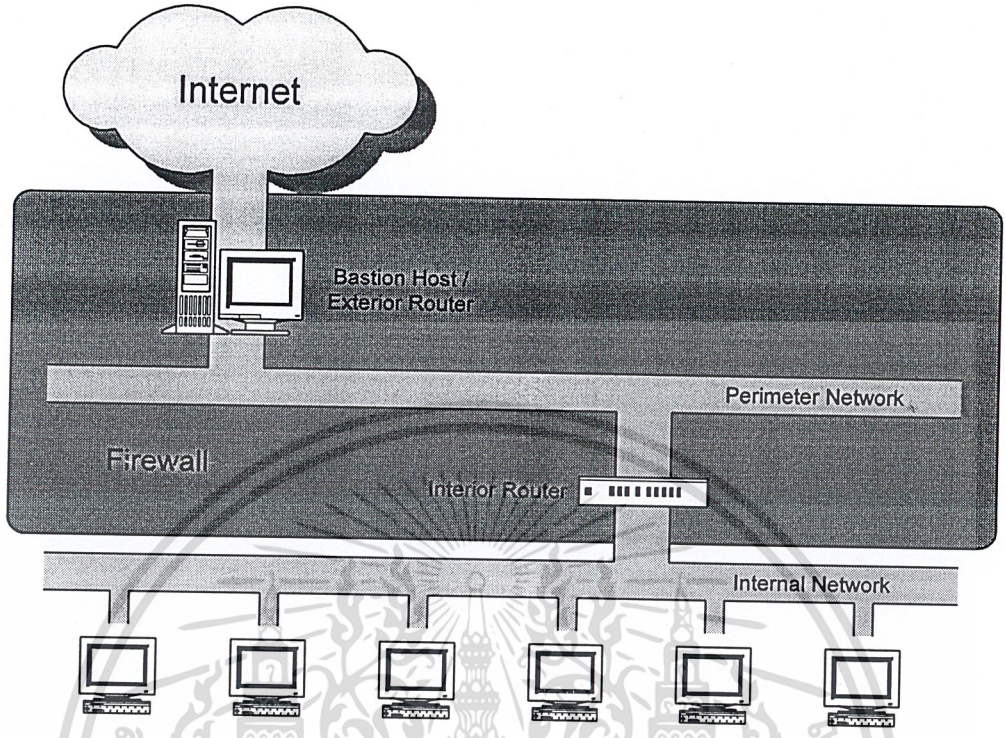
สามารถรวมแบสชั่นโฮสท์ (bastion host) **และเราเตอร์ภายนอก** (exterior router)

เราสามารถใช้กลไก ซิงเกิลโฮมท์ (single home machine) ที่เป็นแแบสชั่นโฮสท์และเราเตอร์ภายนอก เช่น ในกรณีที่มีเพียงแค่ ไดอัล-อัพ สลิป (dial-up slip) หรือ การเชื่อมต่อ พีพีพี (PPP connection) ในอินเตอร์เน็ต กรณีนี้สามารถใช้พีพีพีแพ็กเก็ตแบบมอร์นิ่งสตาร์ (morning star PPP packet) ในแบสชั่นโฮสท์ และให้มันทำงานเป็นทั้งแบสชั่นโฮสท์และเราเตอร์ภายนอก ซึ่งมีหน้าที่ในการทำงานเหมือนกันสามเครื่อง (แบสชั่นโฮสท์,เราเตอร์ภายในและเราเตอร์ภายนอก)

ในการรวมแพ็กเก็ต เช่น แพ็กเก็ตบนมอร์นิ่งสตาร์ ที่กล่าวมาจะมีคุณสมบัติที่ดี ในการทำแพ็กเก็ตฟิลเตอร์ริ่งอย่างไรก็ตามเราเตอร์ภายนอกไม่จำเป็นต้องทำแพ็กเก็ตฟิลเตอร์ริ่ง เพียงแต่ใช้เชื่อมต่อแพ็กเก็ต (interface packet) ซึ่งไม่ได้ทำแพ็กเก็จฟิลเตอร์ริ่งดีนัก แต่มันก็ไม่ใช่ปัญหา

ในสถาปัตยกรรมนี้ แบสชั่นโฮสท์จะเปิดสู่อินเตอร์เน็ต ดังนั้นคุณจำเป็นจะต้องมีการดูแลเป็นพิเศษ

เอกสารนี้เป็นที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



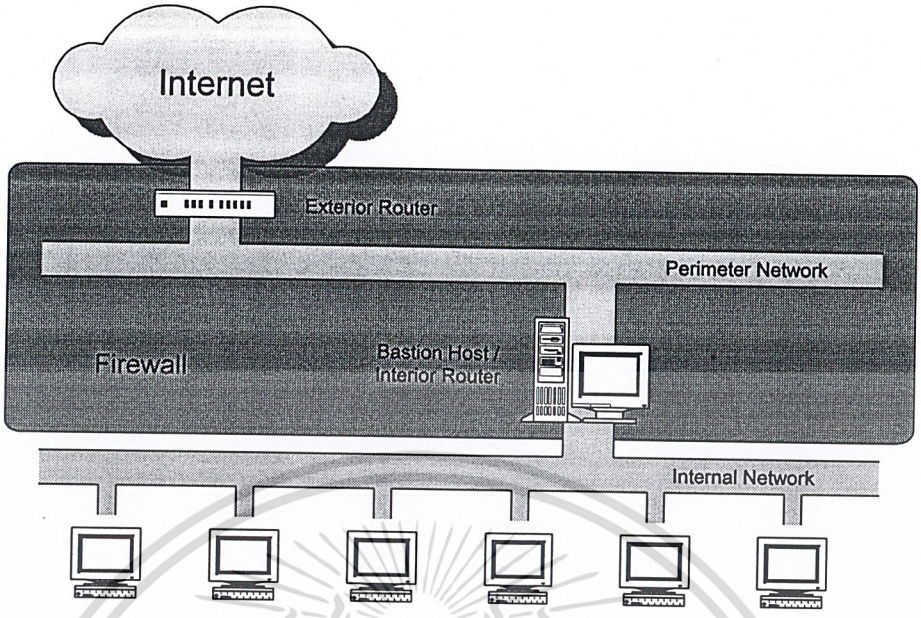
รูปที่ 4.13 แสดงสถาปัตยกรรมที่ทำการรวมแบสชั่นโฮสต์และเราเตอร์ตัวนอก

เป็นอันตรายในการรวมแบสชั่นโฮสม์และเราเตอร์ภายใน

เดิมในไฟร์วอลล์แบบสกรีนสับเน็ทมีเราเตอร์ภายในบนเครือข่ายเพอริมิเตอร์ สำหรับแบสชั่นโฮสท์ไม่มีกำหนดเส้นทางตายตัว ในการเข้าสู่ภายใน เมื่อมีการบุกทะลวงแบสชั่นโฮสท์ การสัญจรก็ยังป้องกันการแอบดู เพราะต้องผ่านเราเตอร์ภายใน แต่หากรวมแบสชั่นโฮสท์กับเราเตอร์ภายในคุณจะได้ไฟร์วอลล์แบบสกรีนโฮสท์และถ้าแบสชั่นโฮสท์ถูกบุกรุก จะไม่มีอะไรรักษาความปลอดภัยระหว่างแบสชั่นโฮสท์กับเครือข่ายภายใน

จุดประสงค์อย่างหนึ่งของเครือข่ายเพอริมิเตอร์ คือ ป้องกันแบสชั่นโฮสท์จากการแอบดูการสัญจรภายใน การรวมแบสชั่นโฮสท์กับเราเตอร์ภายในจะทำให้การสัญจรภายในถูกมองเห็น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.14 แสดงสถาปัตยกรรมที่ทำการรวมแบสชั่นโฮสตีและเราเตอร์ภายใน

เป็นอันตรายในการใช้เราเตอร์ภายในหลายตัว (multi interior routers)

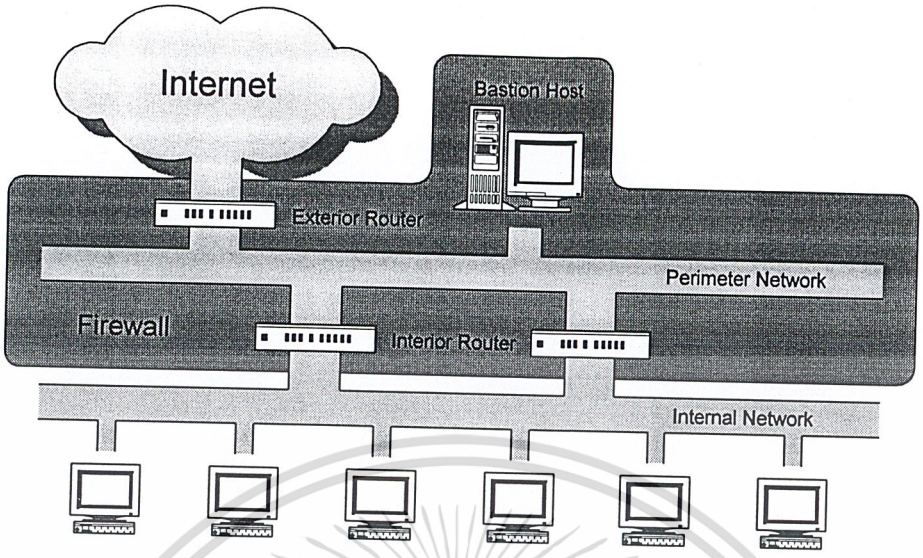
ปัญหาพื้นฐานของซอร์ฟแวร์เราติ้ง (routing software) บนระบบภายใน (internal system) คือ จะหาทางที่เร็วที่สุดที่จะหาระบบภายใน อื่นผ่านเครือข่ายเพอริมิเตอร์ ถ้าโชคดีการเข้าถึงจะไม่ทำงานเพราะมันถูกขัดขวางโดยแพ็กเก็ตฟิลเตอร์ริ่ง บนเราเตอร์ตัวหนึ่ง แต่ถ้าโชคไม่ดีมันทำงาน การสัญจรผ่านเครือข่ายเพอริมิเตอร์ ซึ่งมันอาจจะถูกแอบดูได้ถ้าแบสชั่นโฮสท์ถูกบุกรุก

เป็นการยากที่จะกำหนดคอนฟิกมัลติเพิลอินทีเรีย (multiple interior configuration) ได้ถูกต้องเพราะเราเตอร์ภายในหนึ่งตัวนั้นสำคัญมาก และมีกลุ่มของแพ็กเก็ตฟิลเตอร์ริ่งที่ซับซ้อนมาก ยิ่งมีเราเตอร์ภายในสองตัวก็ยิ่งมีโอกาสที่จะกำหนดกฎเกณฑ์ผิดได้ง่ายขึ้น

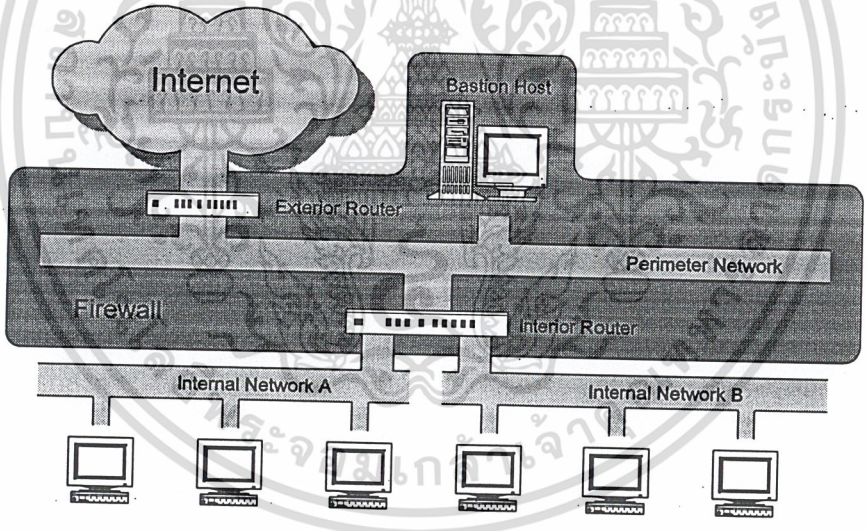
กรณีแรก ถ้าคุณกำหนดคอนฟิกผิดพลาดบางอย่าง จากเครือข่ายเพอริมิเตอร์ จะมีบางครั้งที่สามารถผ่านไปยังโลกภายนอกโดยที่ไม่ได้กำหนด ในกรณีที่ สอง คุณควรที่จะพิจารณาการยกระดับเราเตอร์ภายในให้สอดคล้องกับเราเตอร์ภายนอก แทนที่จะเพิ่มไปอีกตัวหนึ่ง

เหตุผลอื่นที่จะใช้เราเตอร์ภายในหลายตัว คือ คุณมีหลายๆ เครือข่าย ซึ่งมีเทคนิค , องค์กร หรือเหตุผลทางการที่ไม่สามารถแบ่งปันเราเตอร์ได้ ทางที่ง่าย คือ ทำตามรูป ที่ 4.16 มันจะทำให้สับสนในการกำหนดคอนฟิกแต่ไม่ได้เพิ่มโอกาสความเสี่ยงที่เกิดจากการใช้เราเตอร์ภายในหลายตัวถ้ามีเครือข่ายเกินกว่าที่จะแบ่งปันเราเตอร์ตัวเดียว หรือถ้าการแบ่งปันเราเตอร์ไม่เป็นที่ยอมรับกับเหตุผลอื่นๆ ที่พิจารณาการสร้างแบ็คโบนภายใน (internal backbone) และติดต่อกับมันถึงเครือข่ายเพอริมิเตอร์ ด้วย เราเตอร์ตัวเดียว ดังรูปที่ 4.17

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.15 แสดงการใช้เราเตอร์ภายในหลายตัว

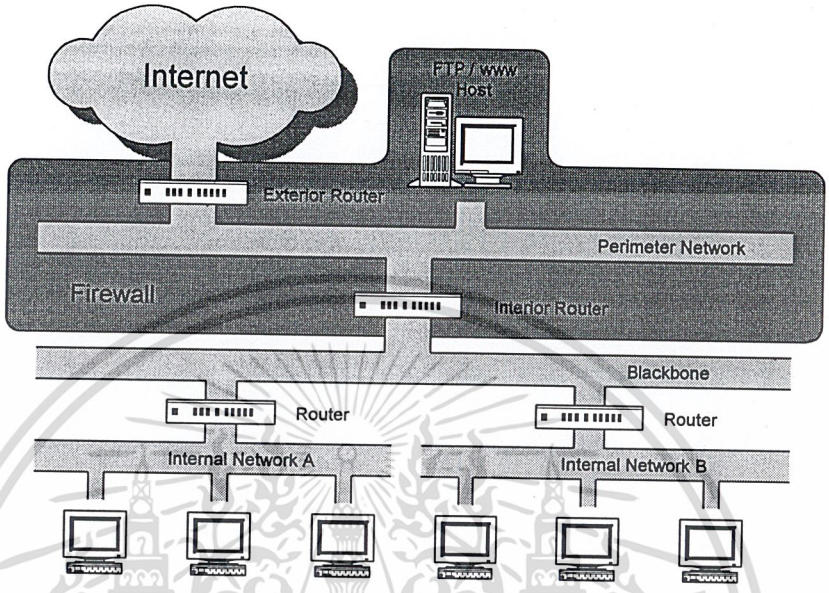


รูปที่ 4.16 แสดงเครือข่ายภายในหลายเครือข่าย (โดยการแบ่งการติดต่อไปที่เราเตอร์ตัวเดียว

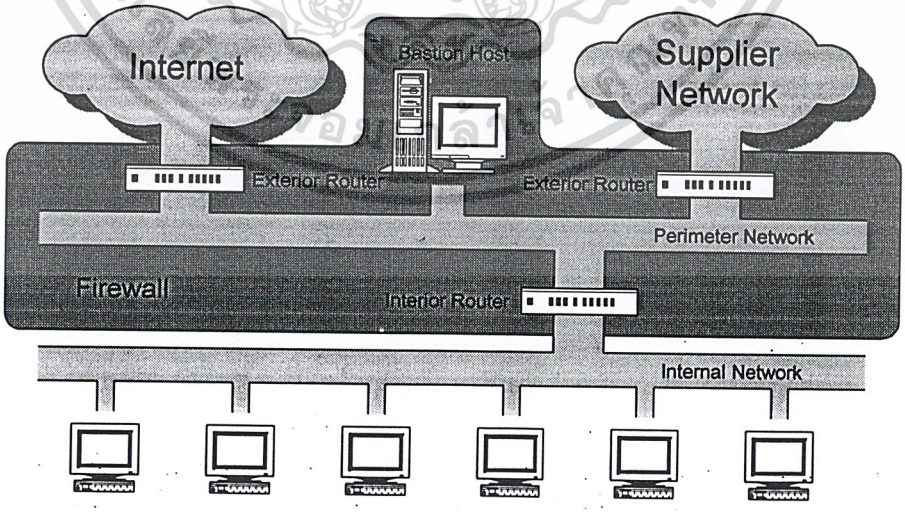
คุณอาจจะหาเส้นทางที่จะปรับความปลอดภัยที่ต่างกันท่ามกลางแต่ละเครือข่ายภายใน (internal network) ที่จะติดต่อ ถึงเครือข่ายเพอริมิเตอร์ ผ่านเราเตอร์ ที่ถูกแบ่ง กรณีนี้เครือข่ายเพอร์ริมิเตอร์ควรจะมีการเชื่อมต่อภายใน (interconnection) ระหว่างเครือข่ายภายใน ซึ่งไม่ควรจะไว้ใจการสัญจรที่ผ่านระหว่างมัน และแต่ละเครือข่ายภายในควรจะระวังความไม่น่าเชื่อจาก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภายนอกซึ่งมันจะไม่อำนวยความสะดวกกับผู้ใช้บางคนบนแต่ละเครือข่ายแต่ควรจะมีการยอมรับความปลอดภัยของแต่ละไซท์ที่แตกต่างกัน



รูปที่ 4.17 แสดงเครือข่ายภายในหลายเครือข่าย(multiple internet network : blackbone architecture)



รูปที่ 4.18 แสดงสถาปัตยกรรมที่มีเราเตอร์ภายนอกหลายตัว (multiple exterior router)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สามารถใช้เราเตอร์ภายนอกได้หลายตัว (multiple exterior routers)

บางกรณีสามารถติดต่อเราเตอร์ภายนอกหลายตัวถึงเครือข่ายเพอริมิเตอร์เดียวกันดังรูปที่ 4.18

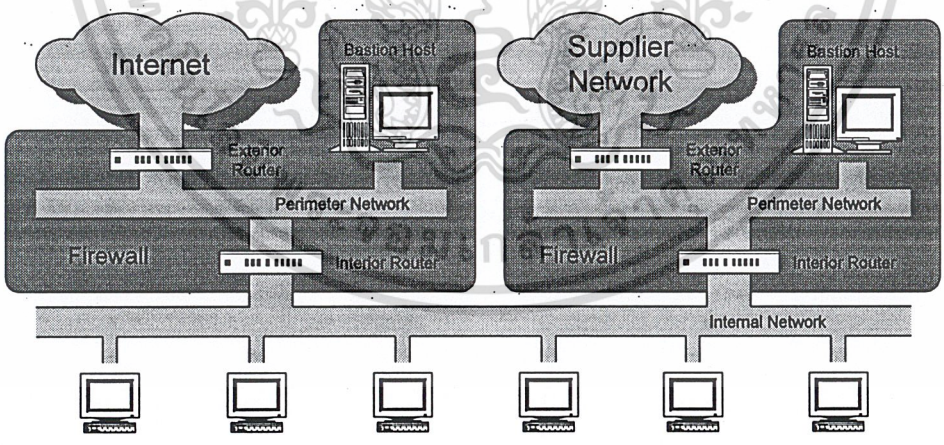
- คุณมีหลายการติดต่อถึงอินเตอร์เน็ต เช่น ผ่าน หลายๆ ผู้จัดหาบริการ
- คุณมีการติดต่อกับอินเตอร์เน็ต และติดต่อออออย่างอื่นกับไซท์อื่นๆ

ในกรณีนี้คุณอาจจะแทนที่เราเตอร์ภายนอกหนึ่งตัว ด้วยเราเตอร์ภายนอกหลายตัว

ในการติดต่อกับเราเตอร์ภายนอกหลายตัวซึ่งไปที่เครือข่ายภายนอกเดียวกัน เช่น ผู้จัดหาบริการอินเตอร์เน็ท 2 ราย (2internet provider) ไม่ใช่ปัญหาใหญ่ เขาอาจจะมีฟิลเตอร์เซ็ต (filter set) ที่ ต่างกันแต่ไม่วิกฤตกับเราเตอร์ภายนอกซึ่งมีโอกาสที่ด้านหนึ่งยอมรับ แต่การยอมรับของเราเตอร์ภายนอก ไม่น่ากลัวเท่าไรนัก

สิ่งที่ซับซ้อนถ้าติดต่อกับสถานที่ที่ต่างกัน เช่น หนึ่งติดต่อกับอินเตอร์เน็ทอีกหนึ่งติดต่อกับไซท์ที่คุณร่วมมือหรือเป็นไส้ศึกหรือต้องการช่วงการติดต่อที่กว้าง ควรคำนึงถึงการสัญจรใดที่คนเห็นเมื่อเขาสามารถบุกรุกบนเครือข่ายเพอริมิเตอร์ ตัวอย่าง เช่น ถ้าผู้บุกรุกเข้ามา เขาจะสามารถแอบดูเครือข่ายการสัญจรระหว่างไซท์ของคุณและส่วนเสริมหรือส่วนที่เป็นสมาชิกได้ไหม ถ้าเป็นเช่นนั้นแล้วคุณอาจจะต้องการที่จะติดตั้งเครือข่ายเพอริมิเตอร์หลายตัวแทนเครือข่ายที่จะใช้หลายๆ เราเตอร์บนเครือข่ายเพอริมิเตอร์เดียว

สามารถใช้หลายเครือข่ายเพอริมิเตอร์ (multiple perimeter network



รูปที่ 4.19 แสดงสถาปัตยกรรมที่ใช้หลายๆ เครือข่ายเพอริมิเตอร์ (multiple firewalls)

การใช้หลายๆ เครือข่ายเพอริมิเตอร์ มีความเสี่ยงน้อยกว่าการใช้เราเตอร์ ภายในหลายตัวที่แบ่งปันเครือข่ายภายในเดียวกัน แต่มันจะทำให้ปวดหัว คุณควรมีเราเตอร์ภายในหลายตัว แสดงจุดที่เป็นไปได้และยอมรับ ซึ่งเราเตอร์จะต้องยอมรับเฝ้าดูอย่างระวัง ทำให้เหมาะกับระดับ ความปลอดภัยที่ตั้ง ไว้ ถ้าทั้งคู่ติดต่อกับอินเตอร์เน็ทก็ต้องทำให้เป็นนโยบายเดียวกัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สามารถใช้ดูอัลโฮมโฮสท์(dual-home host)**และสกรีนสับเน็ท**(screened subnets)

เราสามารถเพิ่มระดับความปลอดภัย รวมดูอัลโฮมโฮสท์กับสกีนสับเน็ท ซึ่งในการทำจะต้องแยกเครือข่ายเพอริมิเตอร์ และแทรกดูอัลโฮมโฮสท์ เราเตอร์จะทำการป้องกันการปลอมแปลงและป้องกันการผิดผลาดที่ดูอัลโฮมโฮสม์เริ่มจัดหาเส้นทางให้กับการสัญจร ดูอัลโฮมโฮสท์สามารถจัดการควบคุมได้ละเอียดดีกว่าแพ็กเก็ตฟิลเตอร์ริ่งซึ่งคือ ป้องกันหลายชั้นขึ้น

ไฟร์วอลล์ภายใน (internal firewall)

เราอาจป้องกันเครือข่ายภายในจากส่วนอื่นๆ ซึ่งอาจมีเหตุผลที่ต้องกระทำดังนี้

- คุณมีการทดลองหรือทดสอบเครือข่ายกับสิ่งแปลกปลอมที่จะเข้ามา
- คุณมีเครือข่ายปลอดภัยน้อยกว่าไซต์ที่คุณอยู่
- คุณมีเครือข่ายปลอดภัยมากกว่าไซต์ที่คุณอยู่ เช่น โครงการลับที่กำลังพัฒนา หรือข้อมูลที่เกี่ยวกับการเงินหรือเกรดที่สอบผ่าน

จากเหตุผลข้างบนจึงสร้างไฟร์วอลล์ภายใน (internal firewall) ซึ่งไฟร์วอลล์นี้จะตั้งระหว่างสองส่วนขององค์กรเดียวกันหรือระหว่างสององค์กรที่คุณแบ่งปันเครือข่าย มากกว่าหนึ่งองค์กรกับอินเตอร์เน็ต

มันมักจะเป็นการเก็บส่วนหนึ่งขององค์กรของคุณจากส่วนอื่นๆ แต่ไม่ใช่ทุกคนในองค์กรที่ต้องการบริการเดียวกัน และความปลอดภัยที่สำคัญในบางส่วนขององค์กรมากกว่าส่วนอื่นๆ

เครื่องมือและเทคนิคที่คุณใช้สร้างอินเตอร์เน็ตไฟร์วอลล์ (Internet firewall) **มีประโยชน์ในการสร้างไฟร์วอลล์ภายใน อย่างไรก็ตามมีพิจารณาพิเศษที่คุณต้องเก็บไว้ในใจถ้าคุณจะสร้างไฟร์วอลล์ ภายใน**

4.2 แบสชั่นโฮสต์ (bastion host)

แบสชั่นโฮสต์ (bastion host) แสดงตัวเปิดเผยบนอินเตอร์เน็ตซึ่งเปรียบเทียบเสมือนกับล็อบบี้ (lobby) โรงแรมที่ให้คนภายนอกผ่านเข้ามาก่อนจึงจะเข้าภายในได้ ซึ่งแบสชั่นโฮสต์ก็เป็นระบบไฟร์วอลล์ (firewall) ที่คนภายนอกจะต้องผ่านเข้ามาก่อนจึงสามารถใช้บริการในไฟร์วอลล์ได้

ในการออกแบบเนื่องจากแบสชั่นโฮสต์เป็นโฮสต์ที่เปิดเผยดังนั้นไฟร์วอลล์ชนิดนี้จะต้องมีการรักษาความปลอดภัยอย่างรัดกุม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.2.1 **หลักการทั่วไป**

มีสองประการ สำหรับการออกแบบและสร้างแบสชั่นโฮสต์ดังต่อไปนี้

- ทำให้ง่ายที่สุด (Keep is simple)

  ควรจะให้บริการที่มีสิทธิ์เข้ามาได้น้อยที่สุด เพราะซอฟท์แวร์อาจจะมีข้อผิดพลาด (bug) ซึ่งอาจจะทำให้การรักษาความปลอดภัยบกพร่องได้

- เตรียมประนีประนอม (Prepared for bastion host to be compromised)

  ควรจะต้องมีการคาดการไว้ล่วงหน้าว่าจะมีอะไรเกิดขึ้น และหากมีการผิดพลาดหรือมีการบุกรุกเข้ามาจะทำการป้องกันอย่างไร เช่น การสร้างการป้องกันที่เครือข่ายภายใน (รหัสผ่าน (password) , อุปกรณ์ป้องกันบางอย่าง) หรือใส่แพ็กเก็ตฟิลเตอร์ริ่ง (packet filtering) ระหว่างแบสชั่นโฮสต์และโฮสต์ภายใน (internal host)

4.2.2 **แบสชั่นโฮสต์ (bastion host) ชนิดพิเศษ**

- นอนเราติ้งดูอัลโฮมโฮสต์ (nonrouting dual – homed hosts)

มีการติดต่อหลาย ๆ เครือข่ายแต่จะไม่มีการสื่อสารที่ผ่านตัวมัน ซึ่งโฮสต์จะเป็นไฟร์วอลล์เองหรืออาจเป็นส่วนที่ซับซ้อนของไฟร์วอลล์ โดยส่วนมากจะถูกคอนฟิกเหมือนแบสชั่นโฮสต์ทั่วไป แต่ต้องการการระมัดระวังและไม่มีการทำเราติ้ง (routing)

- วิกทิมแมชชีน (victim machines)

ถ้าต้องการการทำงานบริการที่จะไม่รู้จะรักษาความปลอดภัยอย่างไรมักจะใช้วิธีนี้ คือ วิกทิมแมชชีน (victim machines) โดยจะเป็นเครื่องที่เราไม่สนใจอะไรข้างใน แต่เราจะทำการคอนฟิกเหมือนกับแบสชั่นโฮสต์แต่ไม่ให้ผู้ใช้ล็อกอิน (login) เข้าไปเพื่อที่จะให้ผู้บุกรุกเข้าไปแทน

- แบสชั่นโฮสต์ภายใน (internal bastion host)

จะมีแบสชั่นโฮสต์อยู่ภายในอีกทีหนึ่ง ซึ่งจะมีปฏิกริยากับแบสชั่นโฮสต์ภายนอก คือ เมื่อข้อมูลเปลี่ยนไปมันก็จะเปลี่ยนตาม แบสชั่นโฮสต์ภายในมักจะมีการคอนฟิกและป้องกันที่เข้มแข็งมากกว่าโฮสต์อื่น ๆ ทั่วไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.2.3 **การวางตำแหน่งแบสชั่นโฮสต์บนเครือข่าย**

ในเครือข่ายเราควรจะจับทุก ๆ แพ็กเก็ตบนเครือข่ายซึ่งการจับเราจะมีโปรแกรมที่จะจับ แต่โปรแกรมเหล่านี้ผู้บุกรุกก็สามารถใช้ได้ แล้วลักลอบเข้ามาในเครือข่ายซึ่งอาจจะเป็นเทลเน็ต (TELNET) , เอฟทีพี (FTP) , หรืออื่น ๆ แล้วเขาก็จะเข้ามาอยู่บนแบสชั่นโฮสต์

ทางที่จะแก้ไขปัญหานี้ คือ การนำเอาแบสชั่นโฮสต์ไปอยู่ที่ที่ไม่ใช่เครือข่ายภายในซึ่งมีเครือข่ายเพอริมิเตอร์เป็นชั้นแบ่งระหว่างเครือข่ายภายในกับอินเตอร์เน็ต อันจะถูกแบ่งโดยเราเตอร์ (router) หรือ บริดจ์ (bridge) ซึ่งจะทำให้ไม่เห็นการขนส่งของกันและกันได้

การใช้แพ็กเก็ตฟิลเตอร์ริ่งระหว่างเครือข่ายเพอริมิเตอร์และเครือข่ายภายในช่วยในการจำกัดส่วนที่จะเปิดเผยและลดจำนวนโฮสต์และบริการที่แบสชั่นโฮสต์จะเข้าไปถึง

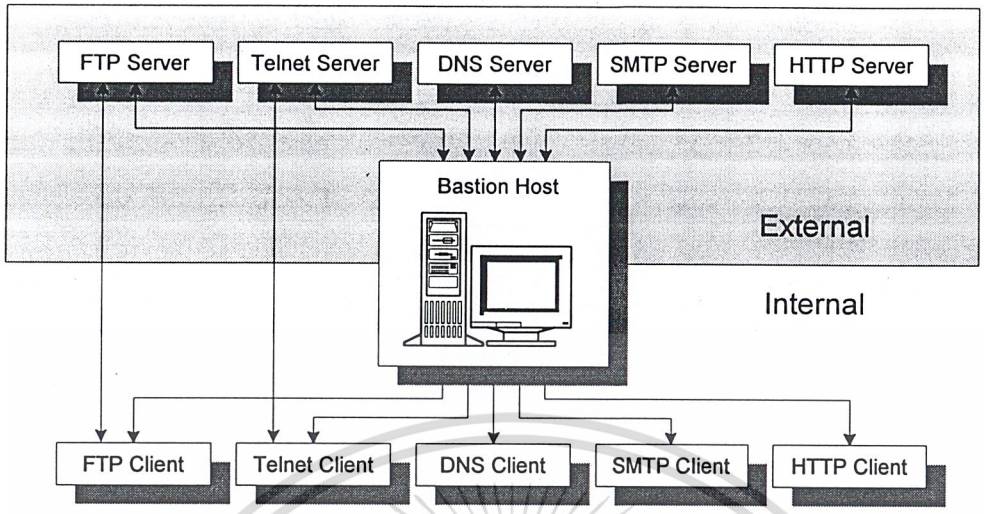
4.2.4 **การเลือกบริการ (service) ที่จะจัดการโดยแบสชั่นโฮสต์** (bastion host)

แบสชั่นโฮสต์จัดการทุก ๆ บริการบนไซต์ที่ต้องการเข้าถึง ผ่านบริการอินเตอร์เน็ต (internet service) ส่วนบริการที่ไม่ต้องการความปลอดภัยมากนักก็จะวิ่งผ่านแพ็กเก็ตฟิลเตอร์ริ่ง

สามารถแบ่งการบริการ (service) ออกเป็น 4 กลุ่มดังนี้

1. **บริการที่ความปลอดภัยอยู่แล้ว** บริการชนิดนี้ถูกกระทำผ่านแพ็กเก็ตฟิลเตอร์ริ่ง
2. **บริการที่ไม่ปลอดภัย** แต่สามารถที่จะทำให้ปลอดภัยได้ บริการชนิดนี้จะกระทำกับแบสชั่นโฮสต์
3. **บริการที่ไม่ปลอดภัย และไม่สามารถที่จะทำให้ปลอดภัยได้** บริการชนิดนี้จะต้องทำให้ใช้ไม่ได้หรือกระทำบนโฮสต์เป็นเหยื่อ (victim host)
4. **บริการที่ห้ามใช้หรือไม่สามารถใช้เชื่อมกับอินเตอร์เน็ต** บริการจะต้องทำให้ใช้ไม่ได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูป 4.20 แสดงแบสชั่นโฮสต์ที่ทำงานบนหลาย ๆ บริการอินเตอร์เน็ตที่ต่างกัน

4.2.5 ไม่อนุญาตให้มีบัญชีผู้ใช้ (user account) บนแบสชั่นโฮสต์ (bastion host)

การจะทำให้ระบบมีความปลอดภัย (security) ดีที่สุดไม่ควรจะให้มีบัญชีผู้ใช้ (user account) เนื่องจากเหตุผลดังนี้

- ความไม่มั่นคงของบัญชีผู้ใช้
- ความไม่มั่นคงของการบริการที่ต้องรองรับกับบัญชีผู้ใช้
- เสถียรภาพและความไว้วางใจของเครื่อง
- การทำลายความปลอดภัยโดยบังเอิญจากผู้ใช้
- เพิ่มความยากในการที่จะค้นหาในการบุกรุก

4.2.6 การสร้างแบสชั่นโฮสต์

ในการสร้างแบสชั่นโฮสต์มีขั้นตอนดังต่อไปนี้

ความปลอดภัยของกลไก (secure the machines)

ในการเริ่มต้นสร้างให้เริ่มจากขบวนการของระบบ (algorithm system) ที่สะอาดซึ่งมีขั้นตอนย่อยดังต่อไปนี้

1. ติดตั้งระบบปฏิบัติการ (operating system) ที่ง่ายต่อการทำงานในอนาคต และพยายามติดตั้งเฉพาะส่วนที่ใช้เท่านั้น
2. ซ่อมข้อบกพร่อง (bug) ที่เราทราบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

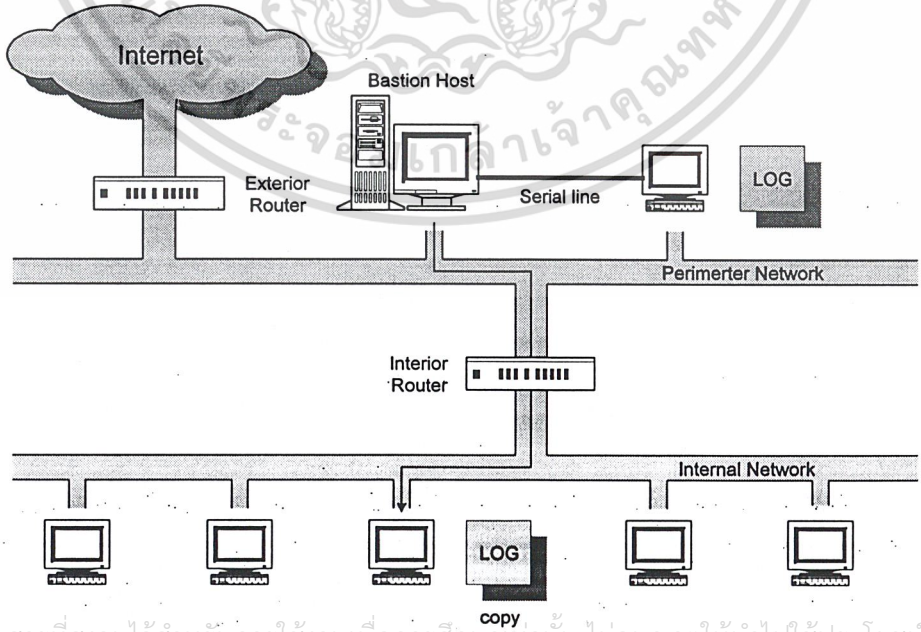
3. ใช้เช็คลิสท์ (checklist)
4. ป้องกันด้วยล็อกระบบ (system log)

แบสชั่นโฮสต์ต้องมีการเก็บการล็อกกิ้ง (logging) ซึ่งมีเหตุผลสำคัญสองอย่าง

- ช่วยบอกว่าแบสชั่นโฮสต์ได้ทำอะไรไปบ้าง ตัดสินใจอะไรบ้าง
- ช่วยดูว่ามีใครบ้างที่บุกรุกเข้ามา และเกิดอะไรขึ้นบ้าง

ที่ที่จะเกิดล็อกระบบ (system log) ควรจะมีสำเนาสองชุด ชุดหนึ่งอยู่ที่ที่ระบุเพื่อให้ง่ายในการดู ส่วนอีกชุดหนึ่งเพื่อป้องกันการเสียหาย

- **ล็อกระบบ (system log) สำหรับความสะดวก** สามารถเก็บไว้ในแบสชั่นโฮสต์หรือในเครือข่ายภายในได้ ข้อดีของการเก็บในแบสชั่นโฮสต์ คือ ไม่ต้องจัดตั้งเกี่ยวกับระบบที่ต่างกันและไม่ต้องคอนฟิกในแพ็กเก็ตฟิลเตอร์ริ่ง ส่วนข้อดีของการเก็บในโฮสต์ภายใน คือ สะดวกในการเข้าถึงเพราะไม่ต้องการเข้าไปในแบสชั่นโฮสต์
- **ล็อกระบบ (system log) เพื่อป้องกันการเสียหาย** ทำได้โดยการต่อสายไปที่ฟิลเตอร์ แต่มีปัญหา คือ กระดาษอาจจะหมดหรือติด และยากในการค้นหาสิ่งที่ต้องการค้น ส่วนอีกวิธีหนึ่งก็คือต่อพอร์ตอนุกรมไปที่เครื่องพีซี ซึ่งจะทำให้ไม่มีปัญหาข้างต้น



รูปที่ 4.21 แสดงการติดต่อพีซีโดยใช้สายอนุกรม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ไม่อนุญาตสำหรับบริการที่ไม่ต้องการ (disabling nonrequired service)

ทำการตัดบริการที่ไม่ต้องการเนื่องจากบริการที่ทำงานบนแบสชั่นโฮสต์อาจจะมีข้อบกพร่องหรือมีปัญหาได้จึงต้องมีการป้องกันโดยการตัดบริการที่ไม่ใช่ หรือไม่สำคัญ

การติดตั้งและปรับปรุงเปลี่ยนแปลงบริการ (modifies service)

วางบริการที่ไม่ได้จัดการโดยระบบปฏิบัติการ (operating system) ที่ใช้ จำเป็นต้องติดตั้งเข้ามาแต่บริการเหล่านี้ไม่ได้ถูกรักษาความปลอดภัยโดยระบบปฏิบัติการ ดังนั้นจึงควรที่จะมีตัวที่เข้ามาป้องกันโดยที่ส่วนใหญ่นิยมใช้คือ

1. ทีซีพีแวรเปอร์แพ็กเก็ต (TCP wrapper packet)
2. เนตาคัล (NETACL) เป็นส่วนประกอบของไฟร์วอลล์ทูลคิท (firewall toolkit)

ทำคอนฟิกใหม่สำหรับผลิตภัณฑ์ (reconfig for production)

เพื่อที่จะให้ได้คอนฟิกที่ดีที่สุดจะต้องทำดังนี้

- ทำคอนฟิกและสร้างสีใหม่
- โปรแกรมที่ไม่จำเป็น
- ทำให้แฟ้มของระบบเป็นแบบอ่านได้อย่างเดียว (readonly)

ดำเนินการตรวจสอบความปลอดภัย (running a security audit)

ทำการตรวจสอบระบบความปลอดภัยเต็มตัวก็จะทำการติดต่อกับเครือข่ายปลายทาง

หมายเหตุ เมื่อทำการคอนฟิกแบสชั่นโฮสต์พร้อมแล้วในการป้องกันควรจะทำสำรอง (back up) ระบบไว้ด้วย

4.3 แพ็กเก็ตฟิลเตอร์ริ่ง (Packet Filtering)

แพ็กเก็ตฟิลเตอร์ริ่ง (packet filtering) **เป็นเครือข่ายความปลอดภัย** (network security) **ที่ทำการควบคุมการไหลของข้อมูล เพราะในการส่งข้อมูลผ่านเครือข่ายข้อมูลนี้จะถูก**

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แตกเป็นชิ้นเล็ก ๆ แต่ละชิ้นก็จะถูกแบ่งกันส่งไป ชิ้นเล็กเหล่านี้เรียกว่าแพ็กเก็ต (packet) ซึ่งจะถูกส่งในชั้นไอพี (IP layer)

อุปกรณ์ที่ติดต่อระดับไอพี เรียกว่า เราเตอร์ (router) โดยเราเตอร์นี้จะทำการตัดสินใจหาเส้นทางที่จะส่งแพ็กเก็ตไป เพราะโดยทั่วไปแพ็กเก็ตจะบอกเพียงจุดหมายที่จะไปแต่ไม่ได้บอกเส้นทางที่จะไป การหาเส้นทางนี้จะใช้เราติ้งโปรคอล (routing protocols) เช่น อาร์ไอพี (Routing Information Protocol : RIP) และ โอเอสพีเอฟ (Open Shortest Path First : OSPF) ในการสร้างเราติ้ง (routing table) เพื่อบอกว่า แพ็กเก็ตจะไปจุดหมายอย่างไร

4.3.1 ทำไมต้องใช้แพ็กเก็ตฟิลเตอร์ริ่ง (packer filtering)

แพ็กเก็ตฟิลเตอร์ริ่งทำการควบคุม (อนุญาตหรือไม่อนุญาต) การส่งข้อมูลบนฐานต่อไปนี้

- ที่อยู่ที่ข้อมูลมา
- ที่อยู่ที่ข้อมูลจะไป
- เซสชั่น (session) และแอพพลิเคชั่นโปรโตคอล (application protocol) ที่ส่งข้อมูล

โดยแพ็กเก็ตฟิลเตอร์ริ่งสามารถกำหนดเงื่อนไขต่าง ๆ ได้ เช่น ไม่อนุญาตให้คนที่ใช้เทลเน็ต (TELNET) เป็นแอพพลิเคชั่นโปรโตคอล (application protocol) เข้ามาจากภายนอก หรือ ให้ทุกคนส่งอีเมล (E – Mail) ผ่านเอสเอ็มทีพี (SMTP) เป็นแอพพลิเคชั่นโปรโตคอล (Application Protocol) อีกตัวหนึ่ง แต่มันไม่สามารถกำหนดเงื่อนไขจากหลักฐาน (identify) เช่น ผู้ใช้คนนี้สามารถเทลเน็ต (TELNET) จากภายนอก แต่ผู้ใช้คนอื่นสามารถทำได้ หรือ คุณสามารถส่งไฟล์นี้ได้แต่สามารถส่งไฟล์อื่นได้

ข้อได้เปรียบของแพ็กเก็ตฟิลเตอร์ริ่ง (packet filtering) คือ มันอนุญาตที่จะจัดการในจุด ๆ เดียวหรือในส่วนที่จะต้องการป้องกันโดยเฉพาะ พิจารณาบริการเทลเน็ต (TELNET service) ถ้าต้องการจะไม่อนุญาตให้เทลเน็ต โดยการปิดเซิร์ฟเวอร์ (server) ที่ให้บริการเทลเน็ต หากมีคนในองค์กรของคุณต้องการเพิ่มเครื่องใหม่ซึ่งต้องใช้เทลเน็ตเซิร์ฟเวอร์ (TELNET server) ในทางตรงกันข้าม หากทำการไม่อนุญาตโดยแพ็กเก็ตฟิลเตอร์ริ่งเราเตอร์ (packet filtering router) เมื่อจะทำการใส่เครื่องใหม่ก็ไม่ต้องห่วงเรื่องการปิดเปิดเครื่องเซิร์ฟเวอร์

เราเตอร์ควรจะวางบนตำแหน่งที่เรียกว่า จุดศูนย์กลางหรือศูนย์รวมการติดต่อ (choke point) สำหรับทุก ๆ การสัญจรที่เข้าหรือออกจากเครือข่าย

เอกสารนี้สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3.2 **ข้อได้เปรียบของแพ็กเก็ตฟิลเตอร์ริ่ง (packet filtering) สกรีนนิ่งเราเตอร์ (screening router) สามารถป้องกันเครือข่ายทั้งหมด**

ข้อได้เปรียบของแพ็กเก็ตฟิลเตอร์ริ่งข้อหนึ่ง คือ หากวางดี ๆ แล้วสามารถป้องกันได้ทั้งเครือข่าย แม้จะวางเพียงแค่ตัวเดียว

แพ็กเก็ตฟิลเตอร์ริ่งไม่ต้องการการกำหนดจากผู้ใช้

แพ็กเก็ตฟิลเตอร์ริ่งไม่เหมือนกับพร็อกซี (proxy) แพ็กเก็ตฟิลเตอร์ริ่งไม่ต้องการซอฟท์แวร์ทั่วไป (custom software) หรือ การกำหนดของเครื่องไคลเอนต์ (client) หรือไม่ต้องการการปฏิบัติการสำหรับผู้ใช้เมื่อแพ็กเก็ตฟิลเตอร์ริ่งถูกออกแบบให้แพ็กเก็ตผ่านเราเตอร์ก็จะไม่แตกต่างจากเราเตอร์ทั่วไป

แพ็กเก็ตฟิลเตอร์ริ่ง (packet filtering) ทำงานได้เสมือนโปร่งใส เนื่องจากไม่ต้องการความเกี่ยวข้องและรู้ตัวของผู้ใช้

แพ็คเก็ตฟิลเตอร์ริ่งเปิดกว้างที่จะมีเราเตอร์หลาย ๆ ตัว

แพ็กเก็ตฟิลเตอร์ริ่งสามารถมีอยู่ได้ในหลายๆ ฮาร์ดแวร์เราติ้งและซอฟท์แวร์เราติ้ง ซึ่งมีทั้งขายและให้ฟรี บนอินเตอร์เน็ตและไซต์ส่วนมากจะมีแพ็กเก็ตฟิลเตอร์ริ่งในเราเตอร์ที่เขาใช้

4.3.3 **ข้อเสียเปรียบของแพ็กเก็ตฟิลเตอร์ริ่ง**

เครื่องมือทำฟิลเตอร์ริ่ง (filtering tools) ไม่สมบูรณ์แบบ

แพ็กเก็ตฟิลเตอร์ริ่งสามารถใช้ได้บนหลายฮาร์ดแวร์และซอฟท์แวร์ แต่แพ็กเก็ตฟิลเตอร์ริ่งก็ยังไม่ใช่เครื่องมือที่สมบูรณ์แบบ นั้นคือ

- กฎของแพ็กเก็ตฟิลเตอร์ริ่งตั้งใจให้ยากในการคอนฟิก
- การคอนฟิกกฎของแพ็กเก็ตฟิลเตอร์ริ่งตั้งใจที่จะทำให้ยากในการทดสอบ
- การที่จะทำให้อยู่ในหลายผลิตภัณฑ์ทำได้ยาก
- แพ็กเก็ตฟิลเตอร์ริ่งอาจจะมีข้อบกพร่อง ซึ่งเมื่อแพ็กเก็ตฟิลเตอร์ริ่งปัญหาอาจจะทำให้แพ็กเก็ตผ่านเข้าไปได้ทั้ง ๆ ที่ควรจะเข้าไม่ได้

บางโปรโตคอลไม่เหมาะสมกับแพ็กเก็ตฟิลเตอร์ริ่ง

แม้ว่าจะทำให้แพ็กเก็ตฟิลเตอร์ริ่งสมบูรณ์แบบ ก็อาจจะพบว่าบางโปรโตคอลไม่เสมาะสมที่จะสร้างความปลอดภัยผ่านแพ็กเก็ตฟิลเตอร์ริ่ง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บางข้อกำหนดไม่สามารถทำได้โดยแพ็กเก็ตฟิลเตอร์ริ่งเราเตอร์

บางข้อกำหนดคุณไม่สามารถกำหนดได้ เช่น แพ็กเก็ต สามารถกล่าวได้ว่าแพ็กเก็ตมาจากโฮสต์ใด แต่ไม่รู้ว่าเป็นผู้ใช้คนใด นั่นคือ คุณไม่สามารถกำหนดเฉพาะเจาะจงผู้ใช้คล้ายคลึงกับเพ็กเก็ต กล่าวได้ว่ามาจากพอร์ตใด แต่บอกไม่ได้ว่า มาจากแอพพลิเคชั่นใด

4.3.4 คอนฟิกแพ็กเก็ตฟิลเตอร์ริ่งเราเตอร์

การคอนฟิกแพ็กเก็ตฟิลเตอร์ริ่งเราเตอร์ ขั้นแรกต้องทราบว่าบริการใดที่จะอนุญาตบ้าง แล้วค่อยเปลี่ยนสิ่งที่คิดไว้เป็กฎเกี่ยวกับแพ็กเก็ตสิ่งต่อไปนี้เป็นความคิด (concept) โดยทั่วไปเกี่ยวกับแพ็กเก็ต

โปรโตรคอล ควรจะเป็นแบบสองทิศทาง (bidirectional)

โปรโตคอลควรจะเป็นแบบทั้งสองทิศทาง มันเกี่ยวเนื่องทั้งด้านที่ส่งคำสั่งและด้านที่ตอบรับ เมื่อทำการตั้งกฎให้แพ็เก็ตฟิลเตอร์ริ่งต้องรู้ว่าแพ็กเก็ตไปทั้งสองทาง เช่น จะไม่ส่งคีย์ที่กดไปข้างนอก (เมื่อเทลเน็ต) และจะไม่รับแพ็กเก็ตกลับมาแต่รับเป็นหน้าจอกลับมาแทน

ระวังความแตกต่างระหว่างเข้าและออก

จะต้องระวังเกี่ยวกับข้อแตกต่างระหว่างแพ็กเก็ตที่เข้าและออกและบริการ (service) ที่เข้าและออก เช่น เทลเน็ต (TELNET) ที่เป็นบริการออก แต่จะมีทั้งแพ็กเก็ตออก (ปุ่มกด) และแพ็กเก็ตเข้า (หน้าจอ)

ตั้งให้อนุญาตเป็นหลักหรือไม่อนุญาตเป็นหลัก

ในการตั้งกฎของแพ็กเก็ตฟิลเตอร์ริ่งอาจจะมีกฎบางข้อที่เราไม่กำหนด ซึ่งในกฎที่ไม่ได้ตั้งนี้สามารถตั้งให้มันอนุญาตหรือไม่อนุญาตอยู่ก่อนก็ได้ แต่ถ้าจะให้ปลอดภัยและมีประสิทธิภาพ ควรจะตั้งเป็นไม่อนุญาตมากกว่าที่จะตั้งเป็นอนุญาต

4.3.5 อะไรที่เราเตอร์ทำกับแพ็กเก็ต

- ให้แพ็กเก็ตผ่านไป เมื่อแพ็กเก็ตผ่านข้อกำหนดของแพ็กเก็ตฟิลเตอร์ริ่งเราเตอร์ก็จะส่งแพ็กเก็ตต่อไปเหมือนกับเราเตอร์ธรรมดา
- หยุดแพ็กเก็ตเมื่อไม่ผ่านข้อกำหนด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เก็บการกระทำ

ถึงแม้ว้าแพ็กเก็ตจะถูกส่งต่อไปหรือหยุด (permitted or denied) เราเตอร์ก็จะต้องเก็บการกระทำที่เกิดขึ้น โดยเฉพาะเมื่อเกิดการหยุด ในบางกรณีคุณต้องการทราบว่าเหตุใดจึงไม่อนุญาต

ในการเก็บไม่จำเป็นต้องเก็บทุก ๆ แพ็กเก็ตแต่ควรนะเก็บเพียงบางส่วนของแพ็กเก็ต เช่น คุณต้องการที่จะเก็บจุดเริ่มของการติดต่อ (start – of – connection) ทีซีพีแพ็กเก็ต (TCP packet) ซึ่งบอกรายละเอียดเกี่ยวกับการเข้าออก

4.3.6 การส่งไอซีเอ็มพี (ICMP) ซึ่งเป็นโค้ดที่ผิดพลาด (error code) กลับมา

ถ้าแพ็กเก็ตถูกหยุด เราเตอร์ควรจะส่งโค้ดที่ผิดพลาด (ICMP error code) กลับมา เพื่อที่จะเตือนให้ไม่ต้องส่งแพ็กเก็ตกลับมาอีก ซึ่งจะทำให้ช่วยประหยัดการสัญจรและเวลา

มีสองกลุ่มของโค้ดไอซีเอ็มพี (ICMP code) ที่จะกลับมา :

- โค้ดที่ไม่สามารถถึงจุดหมายปลายทาง (destination unreachable) ได้แก่ โค้ดที่ไม่สามารถถึงโฮสต์ (host unreachable) และ โค้ดที่ไม่สามารถถึงเครือข่าย (network unreachable) ซึ่งบอกจุดปลายทางมีปัญหา หรือ มีบางสิ่งบนเส้นทางที่จะไปหาโฮสต์เสียหาย โดยโค้ดนี้เกิดขึ้นก่อนถึงไฟร์วอลล์และแพ็กเก็ตฟิลเตอร์ริ่ง
- โค้ดที่ถูกบริหารเมื่อไม่สามารถถึงจุดหมายปลายทาง (destination administratively unreachable) ได้แก่ โค้ดที่ถูกบริหารเมื่อไม่สามารถถึงโฮสต์ (host administratively unreachable) ซึ่งเป็นการบอกว่ามีการแพ็กเก็ตฟิลเตอร์ริ่งเมื่อมันมีการหยุดแพ็กเก็ต (drop packet)

4.3.7 แบบแผนสำหรับกฎของแพ็กเก็ตฟิลเตอร์ริ่ง (packet filtering rules)

ไวยากรณ์ที่ใช้ในการฟิลเตอร์เพื่อเปรียบเทียบ โดยมีบิตหลังสแลช (/) เป็นตัวบอกว่าจะเปรียบเทียบบิตใด เช่น 10.0.0.0/8 ตรงกับตำแหน่ง (address) ที่เริ่มต้นด้วยสิบ

ตัวอย่างของการตั้งให้อนุญาตให้การสัญจรไอพี (IP traffic) ระหว่างโฮสต์ภายนอกที่เชื่อถือได้ (trust external host : โฮสต์ 172.16.51.50) และ โฮสต์บนเครือข่ายภายใน (class C net 192.168.10.0) เราสามารถแสดงได้ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Rule	Direction	Source Address	Destination Address	ACK set	Action
A	Inbound	Trusted external host	Internal	Any	Permit
B	Outbound	Internal	Trusted external host	Any	Permit
C	Either	Any	Any	Any	Deny

ตาราง 4.1 ตัวอย่างของการตั้งให้อนุญาตให้การสัญจรไอพี (IP traffic) ระหว่างโฮสต์ภายนอกที่เชื่อถือได้ และ โฮสต์บนเครือข่ายภายใน

กับการสกรีน (screened) คุณจะมีลักษณะเฉพาะดังนี้

between host 172.16.51.50 and net 192.168.10 accept ;

between host any and host any reject ;

สำหรับเทเลบิต เน็ตบลาสเซอร์ (telebit netblazer) สามารถตั้งกฎได้ดังนี้ (การติดต่อกับภายนอกเชื่อมต่อด้วย " syn0 ")

permit 172.16.51.50 / 32 192.168.10 / 24 syn0 in

deny 0.0.0.0 / 0 0.0.0.0 / 0 syn0 in

permit 192.168.10 / 24 172.16.51.50 / 32 syn0 out

deny 0.0.0.0 / 0 0.0.0.0 / 0 syn0 out

บนลีฟวิ่งสโตน พอร์ตมาสเตอร์ (livingston portMaster) หรือ ไออาร์เอกส์ (IRX) สามารถตั้งกฎได้ดังนี้ (การติดต่อกับภายนอกเชื่อมต่อด้วย " sl ")

add filter sl . in

set filter sl . in 1 permit 172.16.51.50 / 32 192.168.10.0 / 24

set filter sl . in 2 deny 0.0.0.0 / 0 0.0.0.0 / 0

set sl ifilter sl . in

add filter sl . out

set filter sl . out 1 permit 192.168.10.0 / 24 172.16.51.50 / 32

set filter sl . out 2 deny 0.0.0.0 /0 0.0.0.0 / 0

set sl ofilter sl . out

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บนซิสโคเราเตอร์ (cisco router) สามารถตั้งกฎได้ดังนี้ (การติดต่อกับภายนอกเชื่อมต่อด้วย " seriall ")

```
access – list 101 permit ip 172.16.51.50  0.0.0.0  192.168.10.0  0.0.0.255
access – list 101 aeny ip 0.0.0.0  255.255.255.255  0.0.0.0  255.255.255.255
interface serial 0
access – group 101 in

access – list 102 permit ip 192.168.10.0  0.0.0.255  172.16.51.50  0.0.0.0
access – list 102 deny ip 0.0.0.0  255.255.255.255  0.0.0.0  255.255.255.255
interface serial 0
access – group 102 in
```

สำหรับรายละเอียดของแต่ละไวยากรณ์ของแต่ละผลิตภัณฑ์ ถ้าหากเข้าใจไวยากรณ์ที่จะใช้ในตารางก็ไม่ใช่เรื่องยากที่จะแปลงจากตารางมาใช้กับระบบ

4.3.8 ฟิลเตอร์ริ่งโดยใช้ตำแหน่ง (filtering by address)

โดยพื้นฐานที่สุดคือการแพ็กเก็ตฟิลเตอร์ริ่งโดยใช้ตำแหน่ง (address) การฟิลเตอร์ริ่งนี้ทำโดยอนุญาตเฉพาะบางจุดตั้งต้นและจุดปลายทางของแพ็กเก็ตที่แน่นอน และป้องกันผู้บุกรุกที่ทำการปลอมแพ็กเก็ตเข้ามาในเครือข่าย

ตัวอย่าง การป้องกันการเข้ามาของแพ็กเก็ตที่ปลอมตำแหน่งตั้งต้น (source addess) ซึ่งมีลักษณะดังนี้

Rule	Direction	Source Address	Destination Address	Action
A	Inbound	Internal	Any	Deny

ตาราง 4.2 การป้องกันการเข้ามาของแพ็กเก็ตที่ปลอมตำแหน่งตั้งต้น (source address)

4.3.9 ความเสี่ยงของการทำฟิลเตอร์ริ่งโดยใช้ตำแหน่งตั้งต้น (source address)

มันไม่ปลอดภัยแน่นอนที่จะเชื่อตำแหน่งตั้งต้น (source address) เพราะตำแหน่งตั้งต้นสามารถที่จะปลอมแปลงได้ สิ่งที่ผู้บุกรุกใช้ปลอมแปลงเข้ามามีสองประเภท คือ ตำแหน่งตั้งต้น (source address) และคนกลาง (man in the middle)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การบุกรุกแบบตำแหน่งตั้งต้น (source address) ผู้บุกรุกจะส่งแพ็กเก็ตเขามาใจชื่อของโฮสต์ที่เราไว้วางใจ และหวังว่าเราจะมีปฏิกิริยาตอบกลับมา แต่ไม่ได้ต้องการที่จะได้รับแพ็กเก็ตกลับมา ในกรณีผู้บุกรุกสนใจในการที่จะได้รับแพ็กเก็ตกลับมา เขาก็จะไม่อยู่บนเส้นทางระหว่างเราและเครื่องที่เขาแอบอ้าง (real machine)

ผลตอบของเราจะไปที่เครื่องที่เขาแอบอ้าง (real machine) แต่ไม่ได้ไปถึงผู้บุกรุก ถ้าผู้บุกรุกสามารถทำนายผลตอบสนองของเราเขาก็ไม่จำเป็นต้องรู้ว่าเราโต้ตอบอะไรกลับมา ในโปรโตคอลส่วนใหญ่ผู้บุกรุกสามารถทำนายได้ว่าผลตอบสนองจะเป็นเช่นไร เช่น ผู้บุกรุกเข้าไปในระบบของคุณและให้ส่งอีเมล (E – Mail) ที่เป็นไฟล์รหัสผ่าน (password file) มาให้เขา ถ้าระบบจะทำการส่งไฟล์ในรูปของเมล์มา ผู้บุกรุกก็ไม่รอดูการตอบสนองนี้

ในหลาย ๆ สถานการณ์ โดยเฉพาะการเชื่อมต่อแบบทีซีพี (TCP) เครื่องที่ผู้บุกรุกแอบอ้างชื่อจะมีปฏิกิริยาไปที่แพ็กเก็ตของคุณโดยพยายามตัดการติดต่อที่มีการปลอมแปลง ผู้บุกรุกไม่ต้องการให้สิ่งนี้เกิดขึ้น ดังนั้นผู้บุกรุกจึงต้องทำให้เสร็จก่อนที่เครื่องที่เขาแอบอ้าง (real machine) จะได้รับแพ็กเก็ตตอบกลับมา หรือก่อนที่จะมีการตัดการติดต่อ (reset) จากเครื่องที่เขาแอบอ้าง มีหลายวิธีทำการบุกรุกได้สำเร็จ เช่น

- ทำการบุกรุกขณะที่เครื่องที่เขาแอบอ้างกำลังล่ม
- ทำให้เครื่องที่เขาแอบอ้างเสียหาย แล้วทำการบุกรุก
- ทำให้เกิดการสับสนในการหาเส้นทางระหว่างเครื่องที่เขาแอบอ้างและเป้าหมาย
- ใช้การบุกรุกในแพ็กเก็ตที่มีการโต้ตอบหนแรกเพื่อว่าจะไม่มีการตัดการติดต่อ (reset)

เดิมปัญหาเป็นปัญหาที่เล็ก ๆ แต่ปัจจุบันกลายเป็นปัญหาใหญ่แล้ว

การบุกรุกปลอมแปลงแบบคนกลาง (man in the meddle)

- ผู้บุกรุกจะเข้าไปอยู่ในเส้นทางระหว่างคุณและเครื่องที่เขาแอบอ้าง (real machine) โดยเข้าไปที่ใกล้จุดปลายของเส้นทาง เพราะเส้นทางจะถูกเปลี่ยนแปลงทุกวินาที
- การเปลี่ยนแปลงเส้นทางระหว่างเครื่อง (machine) จะง่ายหรือยากขึ้นอยู่กับรูปแบบการวางเครือข่าย (topology) ระบบการเราติ้ง (routing)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากการปลอมแปลงข้างต้นทำให้ไม่สามารถเชื่อถือได้ ดังนั้นหากจะให้ทำการเชื่อถือได้ควรจะมีกาทำการเข้ารหัส (encryption) เพื่อที่จะทำให้มีความปลอดภัยบนเส้นทางที่ไม่มีความปลอดภัย

4.3.10 ฟิลเตอร์ริ่งโดยการบริการ (filtering by service)

ที่ผ่านมาเป็นการป้องกันโดยตำแหน่ง (address) เพียงอย่างเดียว แต่ในการใช้แพ็กเก็ตฟิลเตอร์ริ่งยังมีการฟิลเตอร์ริ่งโดยการบริการ (service) ซึ่งมีความยุ่งยาก

จากแพ็กเก็ตฟิลเตอร์ริ่งที่ดูมาแพ็กเก็ตฟิลเตอร์ริ่งยังสามารถเกี่ยวข้องกับบริการ (service) โดยเฉพาะ ดังตัวอย่างที่นำมาบรรยายต่อไปโดยดูที่เทลเน็ต (TELNET) โดยเทลเน็ตอนุญาตสำหรับผู้ใช้ในการล็อกอิน (login) เข้าไปในระบบอื่น ๆ ราวกับว่าผู้ใช้มีการติดต่อโดยตรงกับระบบ

4.4 ระบบพร็อกซี (proxy system)

พร็อกซีเซิร์ฟเวอร์ (proxy server) มักจะใช้สำหรับโปรโตคอลพิเศษ หรือกลุ่มของโปรโตคอลที่ทำงานดูอัลโฮมโฮสต์ (Dual – homed host) หรือ แบสชั่นโฮสต์ (bastion host) โดยโปรแกรมที่ผู้ใช้ใช้คุยกับพร็อกซีเซิร์ฟเวอร์ (proxy server) แทนที่จะติดต่อโดยตรงกับเซิร์ฟเวอร์จริง (real server) ถ้ามีการร้องขอ (request) จากไคลเอนต์ (client) มาถึงพร็อกซีเวิรซ์ฟเวอร์ พร็อกซีเวิร์ฟเวอร์จะคุยกับเวิร์ฟเวอร์จริงโดยประพฤติตัวเหมือนไคลเอนต์ (คือ proxy) และส่งการร้องขอจากไคลเอนต์ถึงเซิร์ฟเวอร์จริงและส่งคำคอบจากเซิร์ฟเวอร์จริงกลับมาที่ไคลเอนต์ ดังนั้นสำหรับผู้ใช้ที่คุยกับพร็อกซีเซิร์ฟเวอร์ก็จะเหมือนกับคุยกับเซิรซ์ฟเวอร์จริงส่วนเซิร์ฟเวอร์จริงก็จะไม่รู้ว่าผู้ใช้อยู่ที่ใด

ระบบพร็อกซีไม่ต้องการฮาร์ดแวร์พิเศษ แต่ต้องการซอฟท์แวร์พิเศษสำหรับการบริการทั้งหมด

ระบบพร็อกซีมีประสิทธิภาพเมื่อกำหนดการเชื่อมต่อพร็อกซีในระดับไอพี (IP) ระหว่างไคลเอนต์ และ เซิร์ฟเวอร์จริง เช่นสกรีนนิ่งเราเตอร์ (screening router) หรือดูอัลโฮมโฮสต์ (Dual – homed host) ซึ่งไม่สามารถกำหนดเส้นทางให้แพ็กเก็ต ถ้ามีการเชื่อมต่อระดับไอพี (IP) ระหว่างไคลเอนต์ และเซิร์ฟเวอร์จริง ไคลเอนต์สามารถอ้อมผ่านระบบพร็อกซีได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.4.1 ทำไมต้องใช้พร็อกซี (proxy)

ในระบบไฟร์วอลล์ที่ผ่านมาผู้ใช้ที่ต่องการจะเข้าถึงบริการของเครือข่ายไม่สามารถทำได้โดยตารงคือต่องทำการล็อกอิน (login) เข้าไปในระบบดูอัลโฮมโฮสต์ (Dual–homed host) โดยทำงานทุกงานจากที่นี่ แล้วส่งผลลัพธ์กลับไปที่เวิร์กสเตชั่น (workstation) ของคุณ

ปัญหาเกิดขึ้นเมื่อมีระบบปฏิบัติการ (operating system) หลายระบบ เช่น ถ้าที่ที่คุณทำงานใช้ระบบแมคอินทอช (Macintosh) และดูอัลโฮมโฮสต์ (Dual – homed host) เป็นระบบยูนิกซ์ (UNIX) คุณจะถูกจำกัด เครื่องมือ (tools) ที่สามารถใช้ได้บนดูอัลโฮมโฮสต์ (Dual – homed host) เพราะเครื่องมือของคุณไม่เหมือนกับ เครื่องมือบนดูอัลโฮมโฮสต์

ปัญหาที่อาจจะเกิดขึ้นอีกอย่างหนึ่งก็คือ ไม่สามารถควบคุมเครื่องมือที่ใช้ได้ คือผู้ใช้ของคุณสามารถส่งเครื่องมือจากภายใน ตัวอย่างเช่น บนดูอัลโฮมโฮสต์ (Dual–homed host) ไม่สามารถแน่ใจได้ว่าทุกไฟล์ที่ส่งออกไปจะถูกตรวจสอบ เพราะเมื่อส่งออกไปแล้วไฟล์นี้อาจถูกนำไปใช้ได้โดยไม่ต้องล็อกอิน (login)

พร็อกซี (proxy) จะทำงานได้โดยอัตโนมัติสำหรับดูอัลโฮมโฮสต์ (Dual – homed host) พร็อกซีจะให้ทุกการทำงานอยู่หลังฉาก ผู้ใช้จะถูกทำให้เห็นเหมือนกับการติดต่อโดยตรงกับเซิร์ฟเวอร์บนอินเตอร์เน็ตซึ่งจะมีการทำงาน ดังรูป 6.1

พร็อกซีซอฟท์แวร์ (proxy software) ทำงานได้โดยไม่ต้องอาศัยล็อกอินของผู้ใช้ (users login)เข้าไปในโฮสต์ ดังนั้นเป็นไปไม่ได้ที่ไฟล์ที่ควบคุมไม่ได้จะไปถึงภายนอกเพราะพร็อกซีจะทำการตรวจสอบเสมอ

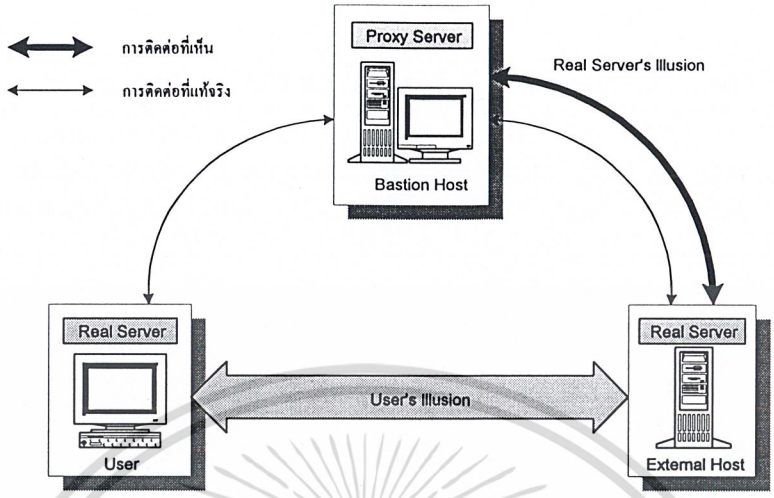
4.4.2 ข้อดีของพร็อกซี (proxy)

พร็อกซีอนุญาตให้ผู้ใช้เข้าถึงอินเตอร์เน็ตได้โดยตรง

ในดูอัลโฮมโฮสต์ (Dual – homed host) ผู้ใช้ต้องล็อกอิน (login) เข้าไปในโฮสต์ก่อนใช้บริการของอินเตอร์เน็ตซึ่งทำให้เป็นการไม่สะดวกสบาย ซึ่งพร็อกซีบริการให้ผู้ใช้ติดต่อได้โดยตรง

ขณะที่พร็อกซีอนุญาตให้ผู้ใช้เข้าถึงบริการของอินเตอร์เน็ตจากระบบของคุณ จะไม่อนุญาตให้แพ็กเก็ต ผ่านระบบของผู้ใช้และอินเตอร์เน็ต เพราะในเส้นทางนี้จะต้องมีการผ่านดูอัลโฮมโฮสต์ หรือแบสชั่นโฮสต์ที่มีสกรีนนิ่งเราเตอร์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.22 แสดงสิ่งที่เห็นกับการทำงานของพร็อกซี (proxy)

พร็อกซีมีการเก็บของข้อมูลที่ดี

เพราะว่าพร็อกซีเซิร์ฟเวอร์ (proxy server) เข้าใจโปรโตคอลที่แอบแฝง ดังนั้น การเก็บข้อมูลเข้าออกก็สามารถเก็บได้ตามที่ต้องการ เช่น แทนที่จะเก็บทุก ๆ ข้อมูลที่ส่งผ่าน เอฟทีพีเซิร์ฟเวอร์ (FTP) ก็จะเก็บเฉพาะคำสั่งและผลที่ทำได้ ดังนั้นจะทำให้เก็บข้อมูลได้เล็กกว่าและตรงกับความต้องการ

4.4.3 **ข้อเสียของพร็อกซี (proxy)**

การบริการของพร็อกซี (proxy services) มีมาตามหลังการไม่บริการของพร็อกซี (nonproxied services)

พร็อกซีซอฟท์แวร์ (proxy software) ที่ออกมามักจะตอบสนองกับบริการเก่า ๆ หรือบริการทั่วไป เช่น เอฟทีพี (FTP) และเทลเน็ต (TELNET) เพราะเป็นการยากที่สร้างซอฟท์แวร์มาตอบเสนอและอาจทำให้ ความปลอดภัยลดลงได้

การบริการของพร็อกซีอาจจะต้องการเซิร์ฟเวอร์ที่แตกต่างกันสำหรับแต่ละบริการ

บางครั้งต้องการพร็อกซีเวิร์ฟเวอร์ที่แตกต่างกันสำหรับแต่ละโปรโตคอล เพราะพร็อกซีเซิร์ฟเวอร์ต้องเข้าใจโปรโตคอลเพื่อจะหาว่าอนุญาตได้ไหม และเพื่อที่จะแสดงกับไคลแอนต์เป็นเซิร์ฟเวอร์จริง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

พร็อกซีมักจะต้องการการเปลี่ยนแปลงกับไคลเอนต์ (client) , ขบวนการ (procedure) หรือทั้งคู่

บางบริการที่ไม่ได้ถูกออกแบบมาสำหรับพร็อกซี พร็อกซีเซิร์เวอร์ต้องการที่จะเปลี่ยนแปลงกับไคลเอนต์หรือขบวนการ (procedure) ถ้าการเปลี่ยนแปลงบางอย่างเกิดปัญหาก็อาจจะไม่สามารถใช้เครื่องมือนั้นได้เหมือนกับไม่มีพร็อกซี (non – proxy)

การบริการของพร็อกซีใช้ไม่ได้กับบางบริการ

พร็อกซีแทรกอยู่ระหว่างการติดต่อโดยตรงกันระหว่างไคงเอนต์และเซิร์ฟเวอร์จริง แต่การบริการเช่น ทอล์ค (talk) นั้นจะมีความยุ่งเหยิงและไม่เป็นระเบียบ ซึ่งอาจจะไม่ได้กับพร็อกซี

การบริการของพร็อกซีไม่ได้ปกป้องจากโปรโตคอลที่ไม่มั่นคง

บางโปรโตคอลถูกสร้างมาเพื่อส่งข้อมูลผ่านเข้ามาปฏิบัติ (execute) โดยไม่ผ่านพร็อกซี ดังนั้นพร็อกซีจึงไม่สามารถตรวจสอบได้

4.4.4 **พร็อกซีทำงานอย่างไร**

พร็อกซีต้องการพร็อกซีเซิร์ฟเวอร์ซอฟท์แวร์ที่เหมาะสมกับเซิร์ฟเวอร์ และบนด้านไคลเอน๖จำเป็นต้องมีสิ่งหนึ่งต่อไปนี้

ไคลเอนต์ซอฟท์แวร์ (custom client software)

ซอฟท์แวร์จะต้องรู้ว่าจะติดต่อพร็อกซีเซิร์ฟเวอร์อย่างไร แทนที่เซิร์ฟเวอร์จริง (real server) เมือผู้ใช้ทำการร้องขอ (request) เช่น เอฟทีพี (FTP) หรือ เทลเน็ต (TELNET) และจะบอกกับพร็อกซีเซิร์ฟเวอร์อย่างไรเมื่อเซิร์ฟเวอร์จริงจะติดต่อ

ขบวนการของผู้ใช้ (custom user procedure)

ผู้ใช้ใช้มาตรฐานของไคลเอนต์ซอฟแวร์ในการที่จะคุยกับพร็อกซีเซิร์ฟเวอร์ และค่อยติดต่อกับเซิร์ฟเวอร์จริงแทนที่การติดต่อกับเซิร์ฟเวอร์จริงโดยตรง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

คำศัพท์เฉพาะของพร็อกซีเวิร์ฟเวอร์ (proxy server)

ระดับของแอพพลิเคชั่น (application – level) **เทียบกับระดับของวงจรไฟฟ้า** (circuit – level)

ระดับของแอพพลิเคชั่น (application – level) พร็อกซีรู้เกี่ยวกับแอพพลิเคชั่นพิศษที่จัดการกับการบริการของพร็อกซีมันจะเข้าใจและแปลคำสั่งในแอพพลิเคชั่นโปรโตคอล ส่วนระดับของวงจรไฟฟ้า (circuit – level) เป็นการสร้างวงจรระหว่างไคลเอนต์และเวิร์ฟเวอร์โดยไม่มีการแปลคำสั่งของแอพพลิเคชั่นโปรโตคอล

โดยทั่วไประดับของแอพพลิเคชั่น ของพร็อกซีใช้ในการปรับเปลี่ยนขบวนการ (procedure) และระดับของวงจรไฟฟ้าของพร็อกซีใช้ในการปรับเปลี่ยนไคลเอนต์

เจเนอริคพร็อกซี (generic proxies)**เทียบกับ ดิดิเคตพร็อกซี** (dedicated proxies)

เดดิเคตพร็อกซีเวิร์ฟเวอร์ (dedicated proxy server) เป็นการบริการเพียงโปรโตคอลเดียว ส่วนเจเนอริคพร็อกซี่เซิร์ฟเวอร์ (generic proxy server)เป็นการบริการได้หลาย ๆ โปรโตคอล ในทางปฏิบัติดีดิเคตพร็อกซีเซิรซ์ฟเวอร์ คือ ระดับของแอพพลิเคชั่น และเจเนอริคพร็อกซีเวิร์ฟเวอร์ คือ ระดับของวงจรไฟฟ้าแต่ก็เป็นไปได้ที่จะสร้าง เจเนอริคแอพพลิเคชั่น เลเวลพร็อกซีเซิร์ฟเวอร์ (generic application level proxy server คือ เข้าใจหลาย ๆ โปรโตคอล) หรือดีดิเคตเซอกิตเลฟเวลพร็อกซีเซิร์ฟเวอร์ (dedicated circuit – level proxy sever คือ จัดการเพียงบริการเดียว)

พร็อกซิเซิร์ฟเวอร์แบบฉลาด (intelligent proxy servers)

พร็อกซีเซิร์ฟเวอร์สามารถทำงานได้มากกว่าการส่งผ่านการร้องขอที่เข้ามา นั้นคือถ้าหากเราเพิ่มความสามารถเข้าไป (ข้อจำกัดต่าง ๆ) ความสามารถจะเพิ่มขึ้นได้ หรือทำการแบ่งเป็นเวิร์ฟเวอร์ที่เป็นพร็อกซีของแต่ละบริการ

การใช้พร็อกซีเซิร์ฟเวอร์กับบริการของอินเตอร์เน็ต

เพราะว่าพร็อกซีแทรกการติดต่อระหว่างไคลเอนต์และเซิร์ฟเวอร์ มันจึงต้องมีการปรับเปลี่ยนและแบ่งแต่ละบริการบางอย่างก็จัดการได้ง่ายแต่บางอันก็ยาก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ทีซีพี (TCP) เทียบกับโปรโตคอลอื่น ๆ

เพราะว่าทีซีพี (TCP) เป็นโปรโตคอลที่มีการติดต่อรวมกับโปรโตคอลอื่น ๆ (connection oriented protocol) ดังนั้นต้องทำการแบ่งส่วนการพร็อกซีแล้วจึงนำมารวมกัน

การเชื่อมต่อทิศทางเดียว (unidirectional connections) เทียบกับการเชื่อมต่อหลายทิศทาง (multidirectional connections)

เป็นการง่ายที่พร็อกซีเซิร์ฟเวอร์ขัดขวางการติดต่อจากไคลเอนต์ถึงเซิร์ฟเวอร์ แต่มันยากกว่าเมื่อจะขัดขวางจากเซิร์ฟเวอร์ถึงไคลเอนต์ ดังนั้นผลลัพธ์ของการติดต่อจะต้องเป็นที่ทราบของพร็อกซีเซิร์ฟเวอร์ หรือเซิร์ฟเวอร์ จะต้องแปลและปรับเปลี่ยนโปรโตคอลให้ผลลัพธ์ที่ออกมาถูกต้องแน่นอน

ไคลเอนต์ภายใน (internal clients) เทียบกับไคลเอนต์ภายนอก(external clients)

พร็อกซีเซิร์ฟเวอร์ส่วนมากจะออกแบบให้เหมาะสมกับไคลเอนต์ภายในและเซิร์ฟเวอร์ภายนอกของไฟร์วอลล์ เพราะว่าต้องใช้งานร่วมกันทั้งภายในและภายนอก แต่ภายในจะสามารถปรับเปลี่ยนไคลเอนต์สำหรับภายนอกทำงานตามความเหมาะสม

พร็อกซีโดยไม่มีพร็อกซีเซิร์ฟเวอร์

บางบริการที่เรียกว่า “เก็บและส่ง “ (store – and – forward) เช่น เอสเอ็มทีพี (SMTP) , เอ็นเอ็นทีพี (NNTP) , เอ็นทีพี (NTP) ทำงานเหมือนพร็อกซี บริการเหล่านี้เกี่ยวกับสารข้อความ (Email => SMTP , Usenet news => ,clock setting => NTP) ซึ่งรับจากเซิร์ฟเวอร์และส่งต่อไปให้เซิร์ฟเวอร์อื่น ๆ ต่อไป ซึ่งเซิร์ฟเวอร์ตัวกลางของการส่งนี้แสดงเหมือนกับพร็อกซี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5
การติดตั้งโปรแกรม Cisco Centri Firewall

5.1 ขั้นตอนก่อนการติดตั้ง

ก่อนที่จะติดตั้งโปแกรม จะต้องมีการเตรียมอุปกรณ์ที่เป็นทั้ง Hardware และ software , เครื่องคอมพิวเตอร์ที่ตรงตามข้อกำหนดของโปรแกรมและจะต้องตอบคำถามที่เป็นปัญหาจากโปรแกรมได้

บทนี้จะอธิบายถึงขั้นตอนก่อนการติดตั้งโปรแกรม ซึ่งจะมีข้อมูลรายละเอียดคือ

1. Hardware และ software ที่ตรงตามความต้องการของโปรแกรมหรือดีกว่าที่กำหนด
2. กำหนดค่าต่าง ๆ ของ Window NT บน Firewall ทำอย่างไร และการควบคุมระยะไกล
3. การทำแผ่นสำรองของ Centri Licence disk
4. ข้อมูลการติดตั้งก่อนการลงโปรแกรมและระหว่างการลงโปรแกรม

ก่อนที่จะทำการติดตั้งโปรแกรม ควรจะมีการตรวจสอบเครื่องคอมพิวเตอร์เครื่องที่จะลงโปรแกรมว่าถูกต้องตามความต้องการของโปรแกรมและมีโปรแกรมสนับสนุนที่เป็นโปรแกรมช่วยในการใช้โปรแกรมไฟร์วอลล์ ซึ่งในส่วนต่อไปจะอธิบายถึง Hardware และ software ที่โปรแกรมต้องการ

5.2 การเตรียมเครื่องคอมพิวเตอร์

เครื่องคอมพิวเตอร์ที่จะใช้จะต้องมีการเตรียมพร้อมทั้งในเรื่องของข้อกำหนดของเครื่องคอมพิวเตอร์รวมถึงโปรแกรมที่ช่วยในการสนับสนุนจะต้องพร้อม มีขั้นตอนในการเตรียมดังนี้

1. กำหนดให้ผู้ที่สามารถเข้ามาใช้คอมพิวเตอร์ในระบบของ Window NT เป็น disable หรือไม่ก็ลบรายชื่อต่าง ๆ ออก แต่ยกเว้นผู้ดูแลระบบและเปลี่ยนชื่อของผู้ดูแลระบบด้วย
2. ติดตั้งและกำหนดค่าของ Network adapter card อย่างน้อย 2 การ์ด
3. ติดตั้งและกำหนดค่าของ TCP/IP
4. protocal และบริการต่าง ๆ ที่ไม่ต้องการให้เอาออก
5. บริการ (service) ที่ไม่ต้องการให้ทำการ disable หรือเอาออกจากระบบ
6. ตรวจสอบ TCP/IP ว่าค่าที่กำหนดถูกต้อง
7. ตรวจสอบสถานะเริ่มต้นของระบบให้ถูกต้อง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ก่อนที่จะเตรียมเครื่องคอมพิวเตอร์ในการติดตั้งโปรแกรมควรจะอ่านหัวข้อต่อไป ซึ่งเป็นส่วนที่จำเป็นในการเตรียมเครื่องคอมพิวเตอร์

5.3 ข้อกำหนดและส่วนที่จำเป็นสำหรับเครื่องคอมพิวเตอร์ที่ใช้ในการติดตั้งโปรแกรม Firewall

ในระบบของ Cisco Centri Firewall อุปกรณ์และโปรแกรมที่ใช้ในการติดตั้งซึ่งเป็นส่วนสนับสนุนถือได้ว่ามีความสำคัญถ้าไม่ติดตั้งให้ถูกต้องตามคำแนะนำของระบบ โปรแกรมที่ได้อาจจะไม่สมบูรณ์ทำให้ใช้งานได้ไม่ถูกต้อง และขึ้นอยู่กับว่าคุณเลือดที่จะติดตั้งเป็นแบบ

- Full Cisco Centri Firewall หรือ
- Remote administrative interface

ถ้าเลือกติดตั้งเป็นแบบ Full Cisco Centri Firewall อุปกรณ์และโปรแกรมสนับสนุน คือ

- โปรเซสเซอร์ 90 MHz เป็นอย่างต่ำ
- แรม (RAM) 32 MB
- ฮาร์ดดิสส์ ขนาด 2 GB
- การ์ดวีดีโอแบบ SVGA อัตราขยายอย่างน้อย 800*600 และสีขนาด 8 bit
- มอนิเตอร์
- ฟลอบปี้ดิสส์ 1.44 MB
- Network adapter card อย่างน้อย 2 ตัว
- โปรแกรม Window NT Server version 4, ใช้บนระบบ NTFS และต้องสามารถใช้งานได้อย่างถูกต้องบนระบบ Window NT Server นั้นการที่จะติดตั้งโปรแกรมเป็นแบบ Full Firewall จะต้องกำหนดดังนี้

บนระบบ Server จะต้องกำหนด Partition เป็นแบบ Full Firewall จะต้องกำหนดดังนี้

- บนตัวของ Server จะต้องกำหนด Partition เป็น NTFS ไม่ใช้ระบบ FAT
- Server ควรจะติดตั้งเป็นแบบ stand-alone server ไม่ควรเป็น primary หรือ secondary domain controller
- Server จะมีส่วนของ Service Pack 2 และ RPC ติดตั้งในระบบอย่างถูกต้อง
- Network adapter card จะต้องติดตั้งและกำหนดค่าได้ถูกต้อง ควรจะติดตั้งให้การ์ดหนึ่งเป็น external network และอีกการ์ดเป็น internal network เพื่อใช้ในระบบของ Fire wall

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- โปรแกรมที่เกี่ยวกับ network adapter card จะต้องสามารถที่จะติดตั้งได้อย่างถูกต้องและสามารถใช้งานได้
- TCP/IP จะต้องมีการติดตั้งและกำหนดค่าได้ถูกต้องสามารถทำงานได้
- Server ที่ใช้ไม่ต้องกำหนดส่วนของ DHCP
- รายชื่อผู้ใช้ระบบควรมี 1 คน เพื่อใช้ในการติดตั้งและดูแลระบบ Cisco Centri Firewall
- ถ้ามีการวางแผนที่จะใช้ Firewall ในการประยุกต์ใช้กับ Domain, group และ user account จะต้องมีสมาชิกอยู่ภายใน Domain อย่างน้อย 1 คน เพื่อให้แน่ใจว่าสามารถจะเข้าไปที่ฐานข้อมูลของผู้ใช้ได้

ถ้าเลือกจะติดตั้งแบบ remote administrative interface เครื่องคอมพิวเตอร์จะต้องติดตั้งโปรแกรม Window NT 4.0 หรือ Window NT Server 4.0 มีการกำหนดค่าอย่างถูกต้องและสามารถใช้งานได้,มี SVGA video care อัตราขยาย 800*600, 8 bit , จอมอนิเตอร์ , CD- ROM drive , ฟลอปปี้ดิสส์ และ network adapter card อย่างน้อย 2 การ์ด

Window NT workstation หรือ Server ที่ใช้ในการติดตั้งแบบ Remote administrative จะต้องมีการกำหนดดังนี้

- จะต้องมี Service Pack 2 และ RPC ในระบบ
- มี network adapter card อย่างน้อย 2 การ์ด ที่สามารถใช้งานได้
- โปรแกรมที่เกี่ยวกับระบบเครือข่ายต่าง ๆ จะต้องกำหนดได้ถูกต้องและสามารถใช้งานได้
- TCP/IP จะต้องติดตั้งในระบบ กำหนดค่าได้ถูกต้อง และสามารถใช้งานได้
- เครื่องคอมพิวเตอร์ที่ใช้จะต้องไม่เลือกส่วนของ DHCP server
- ถ้าคิดที่จะใช้ Firewall ในการประยุกต์ใช้กับ Domain, Group และ user account จะต้องมีสมาชิกอยู่ภายใน Domain อย่างน้อย 1 คน เพื่อให้แน่ใจว่าสามารถเข้าไปที่ฐานข้อมูลของผู้ใช้ได้

5.4 การลบรายชื่อผู้ใช้คอมพิวเตอร์ในระบบ

จุดที่น่าสนในคือระหว่างเครือข่ายภายในและเครือข่ายภายนอก Firewall จะจำกัดเส้นทางของข้อมูลให้เล็กที่สุดเพื่อลดปัญหาการเข้าถึงข้อมูล ซึ่งเป็นขั้นตอนที่สำคัญในการลดจำนวนการเข้าถึงข้อมูลและทำการลบรายชื่อผู้ใช้ที่ไม่ต้องการออก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Note ส่วนของการลบรายชื่อผู้ใช้สามารถทำได้ที่โปรแกรม Centri Setup และสามารถที่จะเปลี่ยนชื่อของผู้ดูแลระบบได้อีกด้วย ซึ่งเป็นข้อดี คือ ลดจำนวนของ ผู้ประสงค์ร้ายเข้ามาในระบบ

เมื่อติดตั้งโปรแกรม Window NT โปรแกรมจะสร้างรายชื่อผู้ใช้มา 2 ชื่อคือ administrator และ guest ชื่อ administrator เป็นชื่อที่นำไปใช้ในการติดตั้งโปรแกรม Cisco Centri Firewall

ในการลบรายชื่อผู้ใช้ให้ใช้ user manager ใน administrative tools ที่ star menu จะสามารถลบรายชื่อผู้ใช้ได้ยกเว้น Guest และ Administrator แต่ควรจะตั้งค่า disable ที่ Guest แทน

ในการทำ disable กับรายชื่อที่มีอยู่ในระบบก็สามารถทำได้โดยทำใน User Manager ซึ่งเป็นการทำเพื่อไม่ให้ผู้ใช้คนนั้นสามารถที่จะเข้าระบบได้ ซึ่งมีขั้นตอนดังนี้

1. ที่ User Manager ให้คลิ๊กไปที่ชื่อที่ต้องการจะทำ disable
2. คลิ๊กที่ properties
3. เลือกเช็คที่ Account Disabled และ คลิ๊ก OK

คำเตือน Window NT จะอนุญาต ให้กำหนด IP Address ได้หลายค่าสำหรับ network adapter card ซึ่งทำให้ไม่สนับสนุนกันกับ Cisco Centri Firewall แต่ในระหว่างการติดตั้งสามารถที่จะเพิ่มเติมค่า IP Address เข้าไปได้และตัวโปรแกรมเองก็สามารถจะบอกค่าปกติของส่วนต่างได้

5.5 การติดตั้งส่วนประกอบต่าง ๆ ของ Network

ในการติดตั้งโปรแกรม Cisco Centri Firewall คอมพิวเตอร์จะกำหนดและควบคุม TCP/IP ซึ่งเป็นส่วนประกอบที่สนับสนุนในส่วนของ Microsoft Network ในการติดตั้งก็เช่นกัน จะมีการกำหนดให้ TCP/IP สามารถที่จะสนับสนุนการทำงานกับ Firewall จะต้องทดสอบการทำงานของ TCP/IP ให้แน่ใจก่อนว่าสามารถทำงานได้ถูกต้อง โดยใช้วิธีติดต่อกับโปรแกรมต่าง ๆ ที่ใช้ TCP/IP เช่น FINGER, FTP, RCP, TELNET และ TFTP หรือใช้คำสั่ง ipconfig, nbtstat, netstat, ping และ route

ถ้าคุณยังไม่ได้ติดตั้ง TCP/IP เมื่อคุณติดตั้ง Window NT สามารถที่จะติดตั้ง TCP/IP ได้ในขั้นตอนของการติดตั้ง Window NT

เมื่อติดตั้ง TCP/IP ถูกต้อง และสามารถที่จะกำหนดค่า IP Address, subnet mark และ default gateway ให้กับ Network card ทั้ง 2 ตัว จะต้องมีข้อมูลดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่อนุญาตให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- ค่า IP Address ทั้ง 2 ตัว (IP Address external network และ internal network) และค่าของ subnet mark ทั้ง 2 ตัว
- IP Address 1 ตัว หรือ มากกว่า สำหรับ default gateways

Note ในกรณีที่ติดตั้ง external card กำหนดค่า IP Address ผิด ซึ่งไม่ตรงกันกับ Internal Network Information Center (InterNIC) จะต้องแก้ไขใหม่โดยเข้าไปในชื่อของ Administrator เพื่อที่จะทำการแก้ไขให้ถูกต้อง

วิธีที่ง่ายและแน่ใจว่าสามารถที่จะติดตั้ง Protocal ต่าง ๆ , service และ adapter ได้ถูกต้องคือ ลบ networking ทั้งหมด และ reboot เครื่องอีกครั้ง จากนั้นจึงใช้ Network Setup Wizard ในการติดตั้งส่วนต่าง ๆ จะมีตัวเลือกให้เลือกตามที่ต้องการ พร้อมทั้งคำอธิบายการกำหนดส่วนต่าง ๆ ซึ่งในส่วนแรกจะอธิบายถึงการลบส่วนประกอบของ Network ส่วนต่าง ๆ ในส่วนที่สองจะอธิบายถึงการติดตั้ง

5.6 วิธีการลบส่วนประกอบทั้งหมดของ Network

1. ที่หน้าจอ คลิ๊กขวาที่ Network Neighborhood จะมี dialog แสดงขึ้นมา ในกรณีที่คุณยังไม่ได้ติดตั้ง network card ในขั้นตอนการติดตั้ง Window NT จะถามว่า จะติดตั้ง Window NT networking หรือไม่ ให้กด continue เพื่อติดตั้งในระบบ
2. คลิ๊กที่ Services
3. ที่รายการของ Network Services ให้คลิ๊ก Remove จะมีการยืนยันการลบบริการต่าง ๆ ให้คลิ๊ก Yes
4. คลิ๊กที่ Protocal
5. ในรายการ Network Protocals ให้คลิ๊กที่ Protocal แล้วคลิ๊กที่ Remove
6. คลิ๊กไปที่ Adapters
7. ในรายการของ Network adapters จะแสดงรายการของ adapter card ตัวอื่น ๆ คลิ๊กที่ adapter แล้วคลิ๊ก Remove
8. เมื่อคุณลบบริการทั้งหมดออก , Protocal และ card ต่าง ๆ ออกหมดแล้ว คลิ๊ก close เมื่อคุณปิดหน้าต่างของ Network property จะต้องทำการ reboot อีกครั้งเพื่อเปลี่ยนบริการต่าง ๆ เมื่อลบส่วนต่าง ๆ ออกหมดแล้วและ reboot เครื่องคอมพิวเตอร์แล้ว ต่อไปจะเป็นขั้นตอนการติดตั้งส่วนประกอบต่าง ๆ Network

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.7 การติดตั้งส่วนประกอบต่าง ๆ ของระบบเครือข่ายโดยใช้ Network Setup Wizard

1. ที่หน้าจอ, คลิ๊กขวาที่ Network Neighborhood จะมีหน้าต่างปรากฏขึ้นถามว่าต้องการจะติดตั้ง Window NT networking ไหม
2. เพื่อจะทำการติดตั้ง คลิ๊ก Yes เมื่อมีหน้าต่างของ Network Setup Wizard ขึ้นมา สามารถที่จะเลือกรายการของ Network adapter card ที่ต้องการได้หรือจะให้โปรแกรม Wizard ช่วยในการตรวจสอบก็ได้ สมมติว่าเลือกจากรายการ
3. คลิ๊ก Select from list เป็นการเลือกจากหน้าต่างของ Network adapter card
4. ในรายการของ adapter card เลือก card ที่ถูกต้อง แล้วคลิ๊ก OK
5. เพื่อให้การติดตั้งได้ทำงานต่อให้คลิ๊ก Next
6. ในรายการ Network Protocal จะต้องตรวจสอบ TCP/IP ที่เลือก
7. คลิ๊ก Next โปรแกรมจะแสดงรายการค่าของ network service
8. คลิ๊ก Next โปรแกรม Wizard จะทำการติดตั้งส่วนประกอบที่ได้เลือกไว้
9. คลิ๊ก Next Window NT จะแสดงหน้าต่าง และ prompt สำหรับ Window NT
10. ที่หน้าต่าง Location of the distribution ให้ใส่ปลายทางของไฟล์ และคลิ๊ก Continue เมื่อโปรแกรม Wizard เริ่มติดตั้ง จะมีหน้าต่างถามว่าต้องการใช้ DHCP หรือไม่ คุณไม่ต้องกำหนดค่าของ DHCP บน Firewall Server
11. ในหน้าต่าง TCP/IP setup ให้คลิ๊ก No โปรแกรม Wizard จะทำงานไปเรื่อย ๆ และจะแสดงส่วนประกอบต่าง ๆ ของ TCP/IP
12. ในหน้าต่างของ IP Address ให้กำหนดค่าของ IP ที่แต่ละ card
13. ใน Subnet mark ให้ใส่ค่าลงไป
14. ที่ Default Gateway ให้ใส่ค่า IP ที่เป็น Default Gateway ถ้ากำหนด card ภายนอกเป็น Default Gateway Firewall สามารถที่จะส่ง Packet ไปยังภายนอกได้ ถ้ากำหนดค่า card ภายในของ Firewall IP router จะเป็น Default Gateway ถ้า Firewall ไม่ได้กำหนดร่วมกับ internal router ควรจะปล่อยวางไว้
15. กำหนด DNS sever บนระบบเครือข่าย คลิ๊กที่ DNS
16. ในช่อง Host Name ให้พิมพ์ชื่อของเครื่องคอมพิวเตอร์ Host Name จะยอมให้ใช้ชื่อของเครื่องคอมพิวเตอร์ หรืออาจจะไม่เหมือนกันก็ได้
17. ในช่องของ Domain Box ให้พิมพ์ใช้ชื่อ DNS Domain

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

18. ตรวจสอบว่า Domain Suffix Search Order ว่างเปล่า
19. ที่ IP Address ไม่ต้องเลือก DHCP Servers
20. ที่กลุ่มคำสั่ง Routing จะต้องแน่ใจว่าไม่ได้เลือก
21. บันทึกค่าของ TCP/IP แล้วคลิ๊ก Close ต้องแน่ใจว่า Primary WIN Address ว่างเปล่า
22. คลิ๊ก Yes เครื่องจะทำการ binding service ที่เลือกทั้งหมด
23. คลิ๊ก Next เพื่อให้โปรแกรม Wizard พร้อมที่จะเริ่มทำงานในส่วนของ Network
24. คลิ๊ก Next
25. ถ้าคุณจะใช้ Cisco Centri Firewall ในการประยุกต์ระบบรักษาความปลอดภัย Domain, กลุ่ม และรายชื่อผู้ใช้ในระบบ Window NT , การกำหนดชื่อของ Domain และต้องพิมพ์ชื่อของ Workstation ที่มีอยู่บนระบบและคลิ๊ก Next
26. เมื่อทำการติดตั้งเสร็จสมบูรณ์แล้วคลิ๊ก Finish เมื่อติดตั้งโปรแกรม Wizard เสร็จสมบูรณ์แล้ว ต้อง reboot ใหม่อีกครั้ง เพื่อเปลี่ยนส่วนต่าง ๆ ของระบบ ต่อไปก็จะเป็นส่วนของ " ความเข้าใจของ Protocal และบริการต่าง ๆ "

5.8 ความเข้าใจของ Protocal และบริการต่าง ๆ

ในระบบของ Cisco ก่อนการติดตั้งระบบจะลบ Protocal ต่าง ๆ ออกไปยกเว้น TCP/IP แต่ในหน้าต่างของ Network property ใน Control Panel จะลบส่วนต่าง ๆ ออกยกเว้นส่วนต่อไปนี้

- Network Adapter Card Driver เป็น card ที่จำเป็นจะต้องติดตั้งบน Firewall โดยจะต้องมี driver ของ card ที่ใช้ในการติดตั้งระบบ
- TCP/IP เป็นบริการตัวหนึ่ง อยู่บน Network Property จะเป็นตัวที่ให้บริการในการติดต่อกับเครือข่ายบนระบบ Network สามารถใช้ได้บนระบบ Window NT เดี่ยว ๆ และสามารถติดต่อกับอุปกรณ์ต่าง ๆ ที่ใช้บน Microsoft Networking หรือ ติดต่อกับเครื่องที่เป็น non – Microsoft
- Computer Browser เป็นบริการของ Microsoft Network Browser เป็นบริการที่มีในระบบคอมพิวเตอร์ เป็นส่วนที่สามารถแสดงรายชื่อของคอมพิวเตอร์ที่มีอยู่ใน Domain ต่าง ๆ ของระบบ ซึ่งเป็นส่วนที่เกี่ยวข้องกับ TCP/IP เช่นกัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- RPC Configuration เป็นบริการอีกตัวหนึ่ง อยู่บน Network Property เป็นส่วนที่ใช้ในการเรียกใช้ Remote Procedure Calls (RPCs) รูปแบบจะทำงานกับหลาย ๆ เครื่องบนระบบ
- Net BIOS Interface เป็นบริการอีกตัวหนึ่ง อยู่บน Network Property เป็นโปรแกรมที่ใช้กำหนดการเชื่อมต่อระหว่างคอมพิวเตอร์ และเป็นการกำหนดการใช้ชื่อของ Microsoft Networking
- Server เป็นบริการที่อยู่บน Network Property เป็นบริการที่มีใน Microsoft Window Server สามารถที่จะเชื่อมต่อกับเครือข่ายต่าง ๆ ได้ โดยการติดตั้ง Server Message Block (SMB) เป็น Protocal ที่สำคัญอีกตัวหนึ่งสำหรับการใช้ TCP/IP
- Workstation เป็นบริการที่อยู่บน Network Property เป็นบริการที่สามารถจะติดต่อกับเครือข่ายต่าง ๆ ได้โดยจะต้องติดตั้ง Client สำหรับ Server Message Block (SMB) เป็นบริการตัวหนึ่งที่จำเป็นต่อ TCP/IP

เมื่อทำการลบ Protocal ต่าง ๆ ที่ไม่ต้องการออกแล้วให้ reboot เครื่องอีกครั้ง และทดสอบว่า TCP/IP สามารถทำงานได้อย่างถูกต้อง

5.9 การพิสูจน์ว่า TCP/IP สามารถทำงานได้อย่างถูกต้อง

เมื่อทำการติดตั้ง Cisco Centri Firewall จะต้องกำหนดค่าต่าง ๆ ของ TCP/IP ถ้าในการติดตั้ง Window NT ไม่ได้ทดสอบการทำงานของ TCP/IP จะมี 2 วิธีที่สามารถทดสอบได้คือ

- ทดสอบว่า Firewall Server สามารถที่จะติดต่อโดยใช้ TCP/IP และ
- ทดสอบโดยให้เครื่องคอมพิวเตอร์เครื่องอื่น ๆ ที่อยู่บนเครือข่ายติดต่อมาที่ Firewall Server

<u>คำเตือน</u> ไม่ควรทดสอบในขณะที่ต่อกับเครือข่ายภายนอก เพราะ Firewall ยังไม่ได้ติดตั้งและกำหนดค่าต่าง ๆ ทำให้ผู้ใช้ในเครือข่ายปรากฏบนรายชื่อบนระบบภายนอก

5.10 วิธีทดสอบว่า TCP/IP ได้กำหนดค่าต่าง ๆ ถูกต้อง

เมื่อทำการติดตั้ง Cisco Centri Firewall จะต้องกำหนดค่าต่าง ๆ ของ TCP/IP ถ้าในการติดตั้ง Window NT ไม่ได้ทดสอบการทำงานของ TCP/IP จะมี 2 วิธี ที่สามารถทดสอบได้คือ

- ทดสอบว่า Firewall Server สามารถที่จะติดต่อโดยใช้ TCP/IP และ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- ทดสอบโดยให้เครื่องคอมพิวเตอร์เครื่องอื่น ๆ ที่อยู่บนเครือข่ายติดต่อมาที่ Firewall Server

<u>คำเตือน</u> ไม่ควรจะทดสอบในขณะที่ต่อกับเครือข่ายภายนอก เพราะ Firewall ยังไม่ได้ติดตั้งและกำหนดค่าต่าง ๆทำให้ผู้ใช้ในเครือข่ายปรากฏบนรายชื่อบนระบบภายนอก

วิธีการทดสอบว่า TCP/IP ได้กำหนดค่าต่าง ๆ ถูกต้อง

1. ตรวจสอบการติดต่อบน Server ที่ใช้ TCP/IP โดยใช้คำสั่ง PING ใช้คำสั่งนี้ไปที่ IP Address ที่รู้จัก ทดสอบทั้ง 2 card
2. ตรวจสอบโดยให้เครื่องจากภายนอกต่อเข้ามาที่ Firewall Server โดยใช้คำสั่ง PING

5.11 การตรวจสอบการเริ่มต้นของระบบ (Boot Setting)

แนะนำว่าควรจะกำหนด start up time – out เป็น 0

การที่จะเปลี่ยน time – out ให้เป็น 0

1. ที่ Control Panel , ดับเบิ้ลคลิ๊กที่ System
2. บนแถบ Startup/Shutdown ให้เปลี่ยนค่าของ Show list for เป็น 0

ในการเตรียมเครื่องคอมพิวเตอร์เพื่อจะลงโปรแกรม Firewall จะต้องทำแผ่น backup ของ Centri License Disk ซึ่งจะอยู่ในหัวข้อถัดไป

5.12 การทำแผ่น backup ของ Centri License Disk

ถ้าคุณไม่แน่ใจว่าระหว่างขั้นตอนการติดตั้งแผ่น License Disk จะไม่เสียหาย ควรจะมีการคัดลอกแผ่นดิสก์ไว้โดยการทำแผ่นอีกแผ่นสำรองไว้ในการติดตั้ง

ขั้นตอนการทำแผ่นสำรองของ Centri License Disk

1. เตรียมชื่อที่ใช้สำหรับทำแผ่นสำรอง
2. เข้าไปที่ Dos Prompt ของ Window NT
3. ที่ Dos Prompt ใช้คำสั่ง diskcopy a: a: (เมื่อ a: คือ ฟลอปปี้ดิสก์ขนาด 3.5")

   ตัวอย่าง c:\ diskcopy a: a:

   Insert source diskette in drive A:

   Press any key to continue.....

4. ใส่แผ่นต้นฉบับในฟลอปปี้ดิสก์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งไม่อนุญาตให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5. เมื่อจะเริ่มการคัดลอกแผ่นดิสก์ กด Enter

6. เมื่อเห็นคำสั่ง Insert Target Diskette in drive A: ให้ใส่แผ่นดิสก์อีกแผ่นที่เตรียมไว้ แล้ว กด Enter

7. รอจนกระทั่งมีข้อความเป็น Copy another diskette ? [Y/N]

8. กด N

9. นำแผ่นออกจากฟลอปปี้ดิสก์ นำชื่อที่เตรียมไว้มาติดบนแผ่นแล้วเก็บรักษาอย่างปลอดภัย

ในส่วนต่อไปจะเป็นรายละเอียดในการติดตั้ง ซึ่งอยู่ในบทที่ 2

5.13 สิ่งที่ควรรู้ก่อนเริ่มติดตั้งโปรแกรม Centri

ระหว่างการติดตั้ง จะต้องมีข้อมูลที่ถูกต้องในการติดตั้งโปรแกรม มีข้อมูลดังนี้

- IP Address ของเครื่องคอมพิวเตอร์
- internal mail server
- internal DNS server
- internal Web server
- external router
- IP Address ที่ให้ผู้ใช้ภายนอกมองเห็น
- ส่วนของการติดตั้งจะมี Pre – Installation Worksheet เป็นตัวช่วยในการบอกว่าจะทำอย่างไรบ้างระหว่างการติดตั้ง
- License Key Password Phrase ซึ่งจะต้องใช้ในการติดตั้ง ซึ่งจะได้จากการลงทะเบียนที่เว็บไซต์
- ก่อนการติดตั้งจะต้องอ่าน Securing Your Network With the Cisco Centri Firewall ให้เข้าใจก่อน

5.14 การติดตั้งโปรแกรม Cisco Centri Firewall

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาพรวมของการติดตั้งโปรแกรม

ก่อนที่จะถึงขั้นตอนการติดตั้งโปรแกรม จะต้องอ่านบทของ "ก่อนการติดตั้งโปรแกรม Firewall" ซึ่งจะอธิบายว่าควรจะรู้อะไรและทำอะไรก่อนการติดตั้งและคุณสมบัติต่าง ๆ ของเครื่องคอมพิวเตอร์และโปรแกรมสนับสนุน

ขั้นตอนการติดตั้งจะมี 2 ส่วนใหญ่ ๆ คือ

1. จะต้องติดตั้ง Microsoft Internet Explorer web browser เพื่อใช้ในการดู Help และบันทึกต่าง ๆ ของ Firewall
2. ติดตั้งโปรแกรม Cisco Centri Firewall

ส่วนที่ 1 การติดตั้ง Microsoft Internet Explorer

จะต้องติดตั้ง Microsoft Internet Explorer ซึ่ง Firewall จะใช้ในการแสดงบันทึกและเอกสารต่าง ๆ สามารถจะติดตั้งได้จาก CD-ROM

ก่อนจะติดตั้ง Explorer จะต้องตรวจสอบก่อนว่ามี browser หรือยัง ซึ่ง Explorer จะมี 2 แบบคือ เป็นแบบ Minimal Install และ Full Install ซึ่ง Cisco Centri Firewall ต้องการเป็นแบบ minimal

ชื่อไฟล์ที่สามารถติดตั้ง Explorer ได้

- Msie302mnt.exe เป็น Full Install จะมีส่วนต่าง ๆ ร่วมด้วย คือ Java และ Internet Mail และ News
- Msie302.exe เป็น Minimal Install มีส่วนประกอบคือ Java

เมื่อติดตั้ง Internet Explorer เรียบร้อยแล้ว ให้ reboot เครื่องคอมพิวเตอร์อีกครั้ง หลังจากนั้นก็เริ่มทำในส่วนที่ 2 คือ ขั้นตอนการติดตั้งโปรแกรม Cisco Centri Firewall

ส่วนที่ 2 การติดตั้งโปรแกรม Cisco Centri Firewall

เมื่อส่วนที่ 1 ได้เสร็จสิ้นก็พร้อมแล้วที่จะติดตั้งโปรแกรม ในส่วนนี้จะเป็นส่วนในการแนะนำขั้นตอนเป็นขั้น ๆ ว่าควรจะติดตั้งอย่างไร

แนะนำว่าก่อนที่จะทำการติดตั้งโปรแกรมควรจะปิดหน้าต่างที่ใช้งานอื่น ๆ ให้หมดเสียก่อน โดยกด Alt+Tab

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.15 ขั้นตอนการติดตั้งโปรแกรม

1. ใส่แผ่น CD-ROM ที่ชื่อ Cisco Centri Firewall ที่ไดร์ฟ CD-ROM บนเครื่องที่ต้องการจะติดตั้ง โปรแกรมจะเริ่มติดตั้งเองอัตโนมัติ สามารถที่จะเลือกให้ทำขั้นตอนต่อไปได้ หรือออกจากส่วนนี้

Note ถ้า CD-ROM ไม่ติดตั้งเองอัตโนมัติ ให้ดับเบิ้ลคลิ๊กที่ setup.exe บน CD-ROM ไดร์ฟ

2. ให้เครื่องติดตั้งโปรแกรมต่อไป ให้คลิ๊ก Next จะมีหน้าต่างของ Centri License Disk
3. ใส่แผ่นที่ทำไว้ที่ฟลอปปี้ดิสก์และพิมพ์ไดรฟ์ที่มีแผ่นดิสก์และคลิ๊ก Next

ในแผ่นดิสก์ Centri License Dey จะมีไฟล์ที่ชื่อ License key จะมีไฟล์ที่ชื่อ License.dsk ภายในไฟล์นี้จะมีสิ่งที่โปรแกรมได้กำหนดไว้ในลักษณะเฉพาะแก้ไขเพิ่มเติมของโปรแกรม และมี License Authentication แสดงขึ้นมา

4. ในช่องที่แสดงขึ้นมาให้พิมพ์รหัสผ่านที่เป็นวลี ซึ่งจะสัมพันธ์กับ License key ต่อไปก็คลิ๊ก Next

ในส่วนของรหัสผ่านที่เป็นวลีจะถูกตรวนสอบกับ License key ที่อยู่ในส่วนของการเตรียมส่วนต่าง ๆในการติดตั้ง

ขั้นตอนต่อไปจะเป็นชนิดของการติดตั้งจะแสดงขึ้นมา

5. คลิ๊กไปที่ชนิดของการติดตั้งของโปรแกรม Firewall ที่คุณต้องการจะติดตั้ง แล้ว คลิ๊ก Next

คุณสามารถที่จะเลือกชนิดของการติดตั้งเป็นแบบ Full Firewall, remote Administrative interface Install หรือแบบ Function Demo

ต่อมาจะมีให้เลือกชนิดของ Administrator Account แสดงขึ้นมา

6. ด้านล่างของ Administrative Account คลิ๊กที่ ชนิดของ Administrative Account ที่คุณต้องการ ขั้นตอนต่อไป คลิ๊ก Next

ใจการติดตั้งโปรแกรม Cisco Centri Firewall คุณจะต้องเข้าระบบโดยใช้ Account ที่เป็นสมาชิกในกลุ่มของ Administrator ถ้าจะประยุกต์ใช้กับ Window NT, Group , User account คุณจะต้องเข้าระบบของ Window NT

เมื่อคลิ๊ก Next แล้วจะมีให้เลือก Administrative Account สำหรับการติดตั้ง แสดงขึ้น

7. กำหนด Administrative account ที่ใช้ในการติดตั้ง โดยเลือกจากรายการที่แสดงขึ้นมา

เอกสารนี้เป็นเอกสารสงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รายชื่อที่แสดงขึ้นมาจะถูกกำหนดโดย Window NT ซึ่งใช้ในการเข้าระบบ ซึ่ง Account ที่เลือกใช้ในการติดตั้ง Cintri Centri Firewall จะเป็นรายชื่อที่อยู่ในกลุ่ม ของ administrator ในระบบ Windows NT

Note ควรจะเลือกชื่อของ administrator และทำการเปลี่ยนชื่อในกรณีที่ไม่สามารถลบหรือกำหนดไม่ให้ใช้ได้สำหรับราบชื่ออื่น ๆ ก็ควรจะปฏิเสธการใช้และสำหับในกลุ่มของ administrator คนอื่น ๆ ก็ลบชื่อออก เพื่อลดความเสี่ยงของการเข้ามาขโมยข้ามูล

8. รายชื่อผู้ใช้คนอื่น ๆ ให้กำหนดเป็น Disable other local account
9. ลบชื่อรายชื่อคนอื่น ๆ ที่เป็นสมาชิกในกลุ่มของ Administrator โดยคลิ๊ก ที่ Delete other member of the administrator Group ต่อไป คลิ๊ก Next
10. พิมพ์ชื่อที่คุณต้องการจะเปลี่ยนชื่อ และกด Tab

Note ถ้าคุณเข้าระบบโดยไม่ได้ใช้ account ที่เลือกจะต้อง log off ออกจากระบบและเข้าระบบใหม่อีกครั้งโดยใช้ Account ที่ใช้ก่อนการติดตั้งโปรแกรม และเริ่มต้นติดตั้งโปรแกรมใหม่อีกครั้ง

11. พิมพ์ password ของ Account ที่ใช้ กด Tab และพิมพ์ password อีกครั้ง ขั้นต่อไปคลิ๊ก Next

คุณจะต้องใช้ password ที่กำหนดเวลาเดียวกับ account

12. ใส่แผ่นดิสก์และพิมพ์ชื่อไดรฟ์ที่ใช้ คลิ๊ก Next

แผ่นดิสก์ที่ใช้ไม่สามารถเอาไปติดตั้งแบบ Remote User Interface ได้ และห้ามเอาแผ่นดิสก์ออกจนกว่าจะติดตั้งเสร็จสมบูรณ์

ขั้นตอนต่อมาจะมีหน้าต่างของ New Centri Administrator Account แสดง

13. ใส่ชื่อ และ รหัสผ่าน ใช้สำหรับการเข้าระบบและดูแลระบบของโปรแกรม Firewall คลิ๊ก Next

ชื่อและรหัสผ่านที่กำหนดขึ้นใหม่จะไม่เกี่ยวข้องกับการเข้าระบบของ Window NT

ต่อมาจะเป็นการกำหนดปลายทางในการติดตั้งโปรแกรม

14. ชื่อปลายทางที่กำหนดให้คือ \Centri ถ้าต้องการติดตั้งในไดเรกทอรี่นี้ คลิ๊ก Next ถ้าต้องการจะเปลี่ยนไดเรกทอรี่ คลิ๊ก Next

ไดเรกทอรี่ที่เลือกจะต้องอยู่บน NTFS ถ้าเลือกไดเรกทอร่ที่ไม่มีอยู่และต้องการจะติดตั้งในไดเรกทอรี่นี้ก็ทำได้ คลิ๊ก Yes จะมีหน้าต่างให้เลือกแฟ้มแสดงขึ้นมา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

15. ถ้าต้องการติดตั้งบนแฟ้มรายชื่อที่กำหนดให้คือ Centri Firewall คลิ๊ก Next ถ้าต้องการจะติดตั้งที่แฟ้มอื่น ๆ แล้วเลือกแฟ้ม และคลิ๊ก Next

จะพบ icon ของ Centri Firewall และ Remove Firewall

16. เลือก network adapter card ที่เป็น trusted คลิ๊ก Next

ต่อมาจะแสดงข้อความ The Hide Address

17. ถ้าต้องการ network address translation คลิ๊ก Yes แต่ถ้าไม่ต้องการ คลิ๊ก No

ขั้นต่อมาจะมีหน้าต่าง ให้เลือก Adapter

18. เลือก network adapter card ที่จะกำหนดเป็น native network stack คลิ๊ก Next
19. พิมพ์ IP Address และ Subnetwork mark สำหรับกำหนด network adapter card คลิ๊ก Next
20. ข้อมูลที่ใส่ไปจะถูกติดตั้งบนเครื่องคอมพิวเตอร์ ถ้า network adaptor card เป็นการ์ดที่ต่อกับระบบภายนอก, untrusted network จะต้องกำหนด IP Address และ Subnetwork mark ที่ลงทะเบียนได้กับ InterNIC
21. ที่ช่อง Expose IP พิมพ์ IP Address ที่ต้องการให้ untrusted และ unknown network มองเห็น คลิ๊ก Next และต้องแน่ใจว่าเป็น IP Address ที่กำหนดถูกต้องกับ InterNIC
22. พิมพ์ IP Address สำหรับ native Window NT (local stack) คลิ๊ก Next

IP Address จะต้องถูกต้อง และ ไม่ใช่ IP address เดียวกับที่กำหนดการ์ด

23. พิมพ์ IP Address ที่ default gateway คลิ๊ก Next

ถ้า gateway เป็น external router จะสามารถ forwarding ให้กับ untrusted และ unknown network และ Firewall server ได้ IP Address จะต้องกำหนดกับ interNIC

24. การประยุกต์กฎเงื่อนไขของ User ที่อยู่บน trusted network ให้คลิ๊กที่ตัวเลือก default security policy คลิ๊ก Next

เมื่อติดตั้งโปรแกรมให้สามารถป้องกันระบบได้ จะต้อง reboot คอมพิวเตอร์ เมื่อติดตั้งเสร็จโดยกฎ เงื่อนไขจะมี 2 สถานะของระบบรักษาความปลอดภัย คือ สามารถที่จะติดตั้งในขณะที่มีการติดตั้งโปรแกรม Firewall และอีกส่วน คือ กำหนดให้กับผู้ใช้ที่บริการที่เหมือนกัน

สามารถที่จะเลือกได้ 3 เงื่อนไข

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- No policy assigned เป็นการกำหนด กฎ เงื่อนไขในสถานะของ Reject คือไม่สามารถติดต่อกับ Firewall ได้จนกระทั่ง กำหนดให้สามารถติดต่อกับเครือข่ายได้
- Basic Web, Mail จะมีบริการต่อไปนี้

  สามารถส่ง e-mail ไปยังเครือข่ายนอก firewall ได้ (Internet)

  สามารถกำหนดให้ User สามารถทำในส่วนของ DNS lookups และ DNS server ได้

  User สามารถ ping ไปยัง เครือข่ายภายนอกได้

  User สามารถใช้ Browse ของ HTTP แต่ไม่สามารถใช้บริการ FTP หรือ mail

  User สามารถติดต่อกับ SLL server ได้ ติดต่อกันระหว่าง client และ server ได้
- Web, telnet ,mail มีบริการดังนี้

  User สามารถ ส่ง e-mail ไปยังภายนอกได้ (Internet)

  User สามารถใช้บริการ DNS lookup และ DNS server ได้

  User สามารถใช้บริการ ping ไปยังเครื่องเครือข่ายภายนอกได้

  User สามารถใช้ browse ของ บริการ HTTP ได้

  User สามารถใช้บริการ SLL เข้ารหัสระหว่าง client และ server ได้

  User สามารถใช้บริการ FTP และ telnet ติดต่อกับ untrusted network ได้

  User สามารถอ่านและส่งข้อความจาก NNTP ได้

  ต่อมาแสดง Expose Network Server

25. เลือกชนิดของ network ที่ต้องการให้เครือข่ายภายนอกได้ เห็น คลิ๊ก Next Network server จะต้องอยู่บน internal network เช่น UDP DNS server, TCP DNS server จะทำให้เครือข่ายภายนอกมองเห็นเข้ามาได้ รวมถึง mail server ที่สามารถรับและส่งข้อความได้ รวมถึง web server ให้เครือข่ายภายนอกสามารถมองเห็นเข้ามาเป็น Exposed แทน
26. เลือกค่า IP Address ที่เป็น Actual IP ให้กับ server ส่วน Expose IP จะเป็นค่าที่ให้เครือข่ายภายนอกสามารถมองเข้ามาได้ รวมถึงกำหนด พอร์ต ของ TCP หรือ UDP ที่กำหนดเป็น Service

ขั้นตอนต่อไปจะเริ่มคัดลอกไฟล์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

27. ตรวจสอบว่าสิ่งที่กำหนดไปถูกต้อง และ คลิ๊ก Next เพื่อเริ่มคัดลอกไฟล์ลงเครื่องคอมพิวเตอร์ ซึ่งในขณะที่มีการคัดลอกจะมีเครื่องมือในการดูสถานะของการคัดลอก
28. เมื่อติดตั้งเรียบร้อยแล้ว คลิ๊ก Finish
29. reboot เครื่องอีกครั้ง นำแผ่นดิสก์ออกจากฟลอปปี้ดิสก์ คลิ๊ก Yes และ คลิ๊ก OK เพื่อยืนยัน รอจนกระทั่งเข้าโปรแกรม Cisco Centri Firewall คลิ๊ก No และ คลิ๊ก OK เพื่อยืนยัน

เมื่อติดตั้งระบบเรียบร้อยแล้ว การเข้าโปรแกรมให้ คลิ๊ก Centri Firewall บน Start Menu



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 6
ลักษณะการใช้งานของโปรแกรมไฟร์วอลล์

ใน Cisco Centri Firewall ผู้ดูแลระบบจะต้องรู้ว่าในการป้องกันระบบต้องทำอย่างไร ใครสามารถที่จะเข้ามาใช้ได้บ้าง เข้ามาได้อย่างไร และใครสามารถที่จะเปลี่ยนกฎข้อกำหนดในการเข้ามาในระบบ คุณจะต้องมีข้อมูลและรู้เกี่ยวกับระบบ Network และสามารถที่จะรู้ได้ว่ามีใครแอบเข้ามาในระบบ ในเบื้องต้นจะมีงานอยู่ 7 แบบ

6.1 การกำหนดรายชื่อของผู้ดูแลระบบ

6.2 การติดตั้งระบบเครือข่าย

6.3 การกำหนดบริการที่ใช้บนระบบ

6.4 การกำหนดความสามารถสิทธิของผู้ใช้

6.5 การกำหนดกฎ เงื่อนไขความปลอดภัย

6.6 การประยุกต์ใช้กฎ เงื่อนไขระบบรักษาความปลอดภัย

6.7 การติดตั้ง reporting และ monitoring

ซึ่งในส่วนนี้จะอธิบายถึงภาพรวมแบ่งเป็น 7 ส่วน และมีข้อมูลในการวางแผนของระบบและรวมถึงรายละเอียดสำหรับการทำงานใน HTML

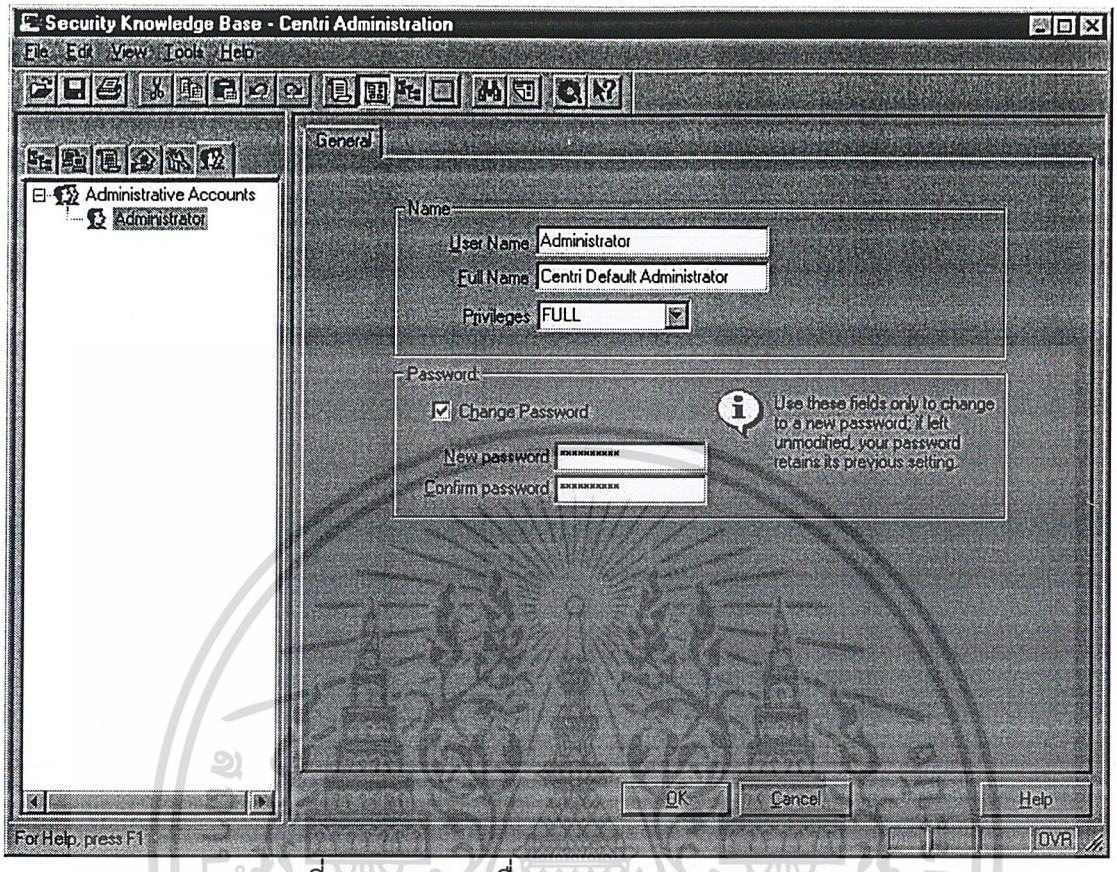
6.1 การกำหนดรายชื่อของผู้ดูแลระบบ

จะต้องมีการกำหนดรายชื่อผู้ใช้อย่างน้อยคือ ผู้ดูแลระบบ (administrator) เป็นผู้ที่มีสิทธิในการกำหนดรายชื่อผู้ที่สามารถใช้งานในระบบได้ ซึ่งจะต้องเป็นคนที่ติดตั้ง Cisco Centri Firewall และกำหนดบริการ (service) ต่างๆ ในระบบ

ระหว่างการติดตั้งโปรแกรมสามารถที่จะเปลี่ยนชื่อของผู้ดูแลระบบได้ เพื่อป้องกันการเข้ามาในระบบจากบุคคลภายนอก เพราะถ้าใช้ชื่อเดิม คือ administrator จะเป็นการง่ายในการเดาชื่อเพื่อเข้ามาในระบบได้ คุณสามารถที่จะเปลี่ยนหรือไม่เปลี่ยนก็ได้

ในขั้นตอนของการติดตั้ง จะมีชื่อที่กำหนดโดยตั้งโปรแกรมอยู่แล้วคือ administrator ผู้ติดตั้งสามารถที่จะกำหนดใหม่หรือไม่เปลี่ยนก็ได้ เมื่อติดตั้งโปรแกรมเสร็จ ภายในโปรแกรมจะมีรายละเอียดของ administrator ซึ่งสามารถที่จะแก้ไขข้อมูลต่างๆ ได้เช่นกัน ดังรูป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูที่ 6.1 แสดงรายชื่อ Administrative account

6.2 การติดตั้งระบบเครือข่าย

การติดตั้งโปรแกรม Cisco Centri Firewall เพื่อป้องกันระบบและปัญหาอื่นๆ ที่ตามมารวมถึงการติดต่อกับเครือข่ายภายนอก โดยที่อยู่ภายใต้การควบคุมของโปรแกรม Firewall

ภายในโปรแกรม Cisco Centri Firewall คือ trusted Network เป็นเครื่องคอมพิวเตอร์ที่อยู่ในการดูแลของ Cisco Centri Firewall จะมี 2 ชนิดคือ

-Physical network

-logical network

Physical network เป็นส่วนประกอบต่างๆ ของระบบ Network เช่น site , routers , Group และรายชื่อต่างๆ ที่อยู่ภายในระบบของ Window NT ซึ่งอยู่ภายใต้ข้อบังคับ ,กฎ ระเบียบต่างๆ รวมถึงชั้นของ Perimeter ที่เชื่อมต่อกันระหว่างระบบภายนอกและระบบภายในเครือข่ายของ Firewall เอง

Logical network เป็นส่วนหนึ่งของ Network ที่ใช้ในการกำหนดหรือประยุกต์ กฎระเบียบต่างๆ ซึ่งอยู่ภายใต้ความต้องการของผู้ดูแลระบบที่จะออกแบบให้มีความปลอดภัยในระบบ เช่น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

trusted network และ untrusted network สามารถเป็นได้ทั้ง Physical และ logical ถ้ากำหนดให้เครือข่ายอยู่ภายใต้ Internet Icon มันจะหมายถึงเป็น untrusted network และจะสามารถที่จะกำหนดให้มีการติดต่อ untrusted network กับระบบภายใน หรือกำหนดให้มีการบริการต่างๆ ได้เพื่อให้ระบบมีความปลอดภัย

6.2.1 การกำหนดส่วนประกอบของ Physical บนระบบ Network

ในระหว่างการติดตั้งโปรแกรมจะต้องมีการกำหนด Physical เกี่ยวกับการเดินทางของข้อมูลความหนาแน่นของข้อมูล การซ่อนหรือการกำหนดให้เห็นค่าของ address (เป็นกฎพื้นฐานของการแปลง address) ซึ่งสามารถที่จะกำหนดคุณสมบัติต่างๆ บนระบบ เช่น

-sub network ที่มีอยู่บนระบบ Network

-ค่าของ Network address ของเราเตอร์ที่อยู่บน DMZ และระบบภายใน

-ติดตั้งการ์ดที่เป็น trusted network และไม่เป็น trusted network

-เครื่องคอมพิวเตอร์สามารถประยุกต์เป็นเครื่องในระบบ

การที่จะกำหนด Physical บนระบบเครือข่ายสามารถที่จะทำได้โดยการกำหนด กฎ , นโยบายต่างๆ ของ กลุ่มหรือผู้ใช้ต่างๆ ภายในกลุ่ม บนฐานข้อมูลภายใน Window NT ก็เป็น trusted network หนึ่งใน Firewall เป็นระบบหนึ่งที่มีความน่าเชื่อถือและมีประโยชน์คือ

-ผู้ดูแลระบบสามารถที่จะประยุกต์กฎระเบียบความปลอดภัยของผู้ใช้แต่ละคน

-ผู้ใช้สามารถที่จะเข้าไปในระบบได้ตามที่ Firewall ยอมให้ทำได้

-สามารถที่จะยอมให้ผู้ใช้ติดต่อกันระหว่างคอมพิวเตอร์กับคอมพิวเตอร์เครื่องอื่น ๆ ที่เป็นเครื่อง Client ของ Window NT

6.2.2 การกำหนดค่า Physical จะเกี่ยวข้องการงาน 3 งาน

-การกำหนดค่าที่ Centri Server

-การกำหนดค่าที่ Centri Firewall

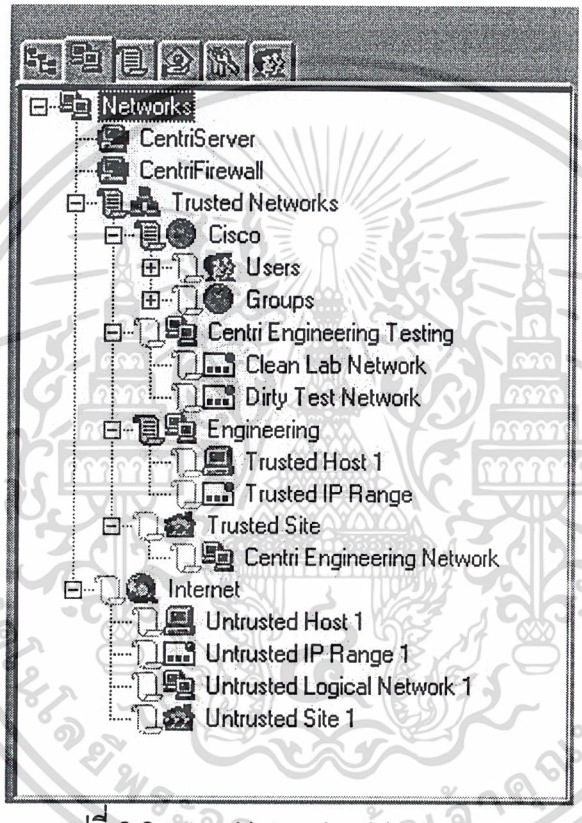
-การกำหนด Physical ที่ เครื่องต่างๆ รวมถึงที่เราเตอร์ที่ Window NT และที่ชั้นของ Perimeter

การกำหนดค่า Logical ของระบบเครือข่าย

logical ของระบบเครือข่ายจะยอมให้คุณกำหนดหรือควบคุมผู้ใช้ในระบบให้ปฏิบัติได้ในส่วนที่ตั้งเงื่อนไขให้หรือกำหนดสิทธิให้ใช้ในขอบเขตที่จำกัด ซึ่งจะไม่เกี่ยวข้องกับ Physical network

เอกสารนี้สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Physical เป็นส่วนที่เกี่ยวข้องกับการติดต่อในส่วนของอุปกรณ์ เช่นเราเตอร์ ซึ่งต้องแน่ใจว่า Firewall server สามารถที่จะติดต่อระบบให้ได้ส่วน logical เป็นส่วนที่เกี่ยวกับว่าจะทำอย่างไรที่จะควบคุมระบบเน็ตเวิร์คให้มีความปลอดภัยได้ดังรูป คุณสามารถที่จะแบ่งหรือไม่แบ่งเพื่อจำกัดส่วนที่ต้องการจะควบคุมส่วนต่างๆ ให้มีความปลอดภัยโดยมีวิธีการในการดูแลและสามารถออกแบบได้



รูปที่ 6.2 แสดง Network object

ตัวอย่างเช่น มีระบบ UNIX มาต่อเข้ากับ Firewall server ของคุณ (เป็น trusted หรือ untrusted) ควรจะใช้วิธีในการเลียนแบบระบบ เหมือนกับระบบ UNIX โดยใช้วิธีจำกัดค่าของ sub network หรือ IP address หรืออาจจะใช้วิธีเดียวกันกับโดเมนนั้น ซึ่งทั้ง 2 แบบที่ว่ามาก็เป็นการออกแบบระบบรักษาความปลอดภัยบน โดเดนหรือโดเมนและเวิร์กสเตชั่นรวมกัน หรือเวิร์กสเตชั่นอย่างเดียว จากตัวอย่างที่ผ่านมา อาจจะใช้วิธีกำหนดสิทธิของผู้ใช้ในระบบ Network ต่างๆ ก็ได้ ถ้าต้องการความปลอดภัยที่มากขึ้น อาจจะกำหนดส่วนอื่น ๆ เพิ่มเข้ามาได้ เช่น ชื่อระบบเครือข่าย hostname และโดเมนเนม

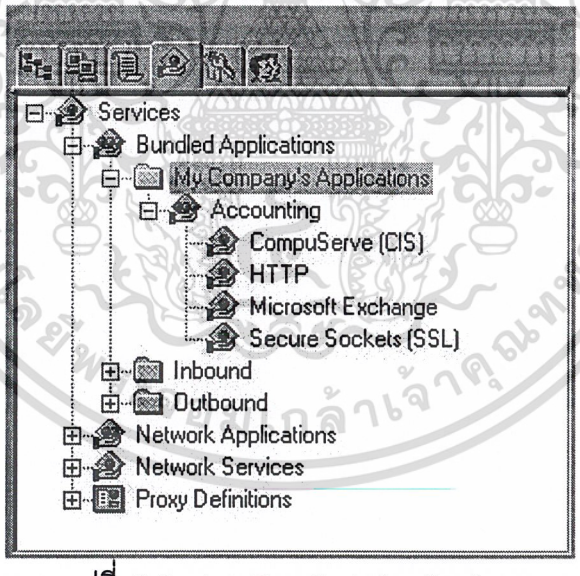
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ข้อดีของ logical network คือง่ายต่อการที่จะแก้ไขเพิ่มเติมภายในระบบ เช่นการกำหนดเงื่อนไข นโยบายต่างๆ ของผู้ใช้แต่ละคนหรือกลุ่ม ง่ายต่อการเปลี่ยนแปลงในการจำกัด IP Address , Sub-networks รวมถึงค่าต่าง ๆ ที่ต้องการจะเปลี่ยนแปลง

6.3 การกำหนดบริการที่ใช้บนระบบ

การกำหนดบริการต่างๆ นั้นขึ้นอยู่กับว่าระบบหรือเครื่องเครือข่ายต้องการใช้บริการอะไรบ้าง ซึ่งสามารถที่จะกำหนดบริการต่างๆ และรายละเอียดต่างๆ ใน Bundled Application ตามความต้องการของผู้ใช้ในระบบ หรือสามารถที่จะกำหนดรายละเอียดต่างๆ ของ Bundled Application , Network Application และ Network Services

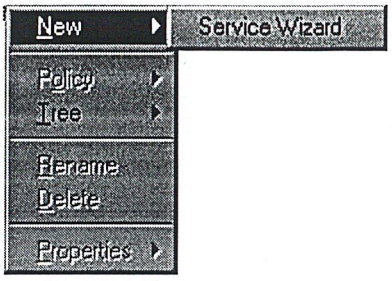
การที่จะกำหนดบริการใหม่ๆ ที่ยังไม่เคยกำหนด สามารถกำหนดหรือเลือกบริการและรายละเอียดตามที่ต้องการได้ใน Bundled Applications ดังรูป การใช้ Bundled Application สามารถที่จะจัดบริการที่ต้องการบนระบบได้ รวมถึงรายละเอียดใน higher level ซึ่งสามารถที่จะอ้างความปลอดภัยหรือการยอมที่จะให้ใช้งานภายในบริการได้



รูปที่ 6.3 แสดง Bundled Application

ถ้าบริการต่างๆ มีอยู่ใน Cisco Centri Firewall เราสามารถที่จะใช้ New service Wizard ในการกำหนดบริการใหม่มาใช้ร่วมกันกับ Bundled Application ได้ การที่จะเข้า Wizard จะต้องเลือก Network service ใน service tree (โดยการคลิ๊กขวาที่เม้าท์) , เลือกที่ Service Wizard จาก New option ดังรูป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 6.4 แสดง menu option

ในขั้นตอนสุดท้ายคือ การกำหนดกฎเงื่อนไขในการใช้บริการของ HTTP เช่น Active X และ Java filtering คุณสามารถที่จะจำกัดกฎต่างๆ ได้ตามเงื่อนไขที่ให้มาในระบบความปลอดภัยของ Firewall ซึ่งตัวของ Firewall เอง สามารถที่จะควบคุมการใช้บริการต่างๆ ของผู้ใช้จากภายนอกระบบ และสามารถป้องกันไฟล์ชนิดต่างๆ ที่จะเข้ามาในระบบ ซึ่งเป็นกฎ ของ HTTP

6.4 การกำหนดความสามารถสิทธิของผู้ใช้

คุณสามารถที่จะกำหนดสิทธิของบริการต่างๆ ให้ผู้ใช้จากภายนอกสามารถที่จะใช้บริการต่างๆ ได้เช่น FTP , telnet และ HTTP ตรงจุดนี้เป็นจุดอ่อนของระบบเพราะผู้ที่ประสงค์ร้ายส่วนใหญ่จะพยายามเข้ามาในระบบโดยการ คัดลอกรหัสและข้อมูลที่ใช้ในการผ่านเข้ามาในระบบของผู้ใช้ที่สามารถจะเข้ามาใช้บริการได้หรือใช้แทนเจ้าของนั่นเอง ตรงจุดนี้ Cisco Centri Firewall สามารถที่จะป้องกันได้โดยการกำหนดกฎเงื่อนไขในการให้สิทธิของผู้ใช้ที่จะเข้ามาในระบบ โดยให้เลือกพิมพ์ข้อมูลที่เป็น S/key หรือ reusable password และรายละเอียดอื่น ๆ ในการพิสูจน์ว่ามีสิทธิในการเข้ามาในระบบ

Username	ชื่อของผู้ใช้ภายในระบบ
Fullname	ชื่อเต็มที่ใช้ช่วยในการเข้ามาในระบบ
Status	สามารถเป็นได้ทั้ง Enable และ disable ซึ่งสามารถที่จะเลือกได้ว่าสามารถเข้ามาใช้บริการต่าง ๆ ภายในระบบได้และเป็นการลดความเสี่ยงในการเข้ามาขโมยข้อมูล
Password	เป็นรหัสผ่านที่ใช้ในการเข้ามาใช้บริการภายในระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

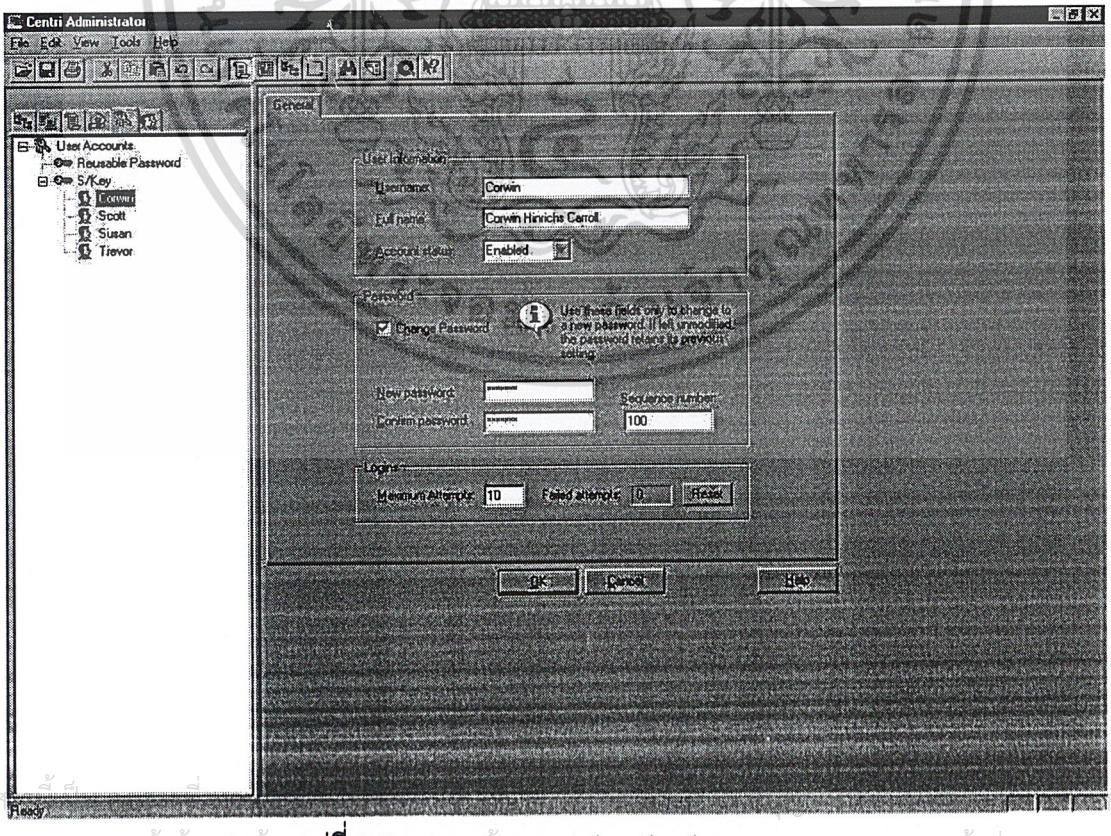
Sequence Number	เป็นตัวเลือกใหม่คือ เป็นระยะเวลาที่สามารถใช้บริการต่าง ๆ ในระบบ
Minimum Attempts	เป็นตัวเลือกอีกตัว คือ จำนวนครั้งที่สามารถเข้ามาในระบบกรณีที่ใส่ข้อมูลผิดพลาด

ส่วนสุดท้าย คือ การกำหนด User account ใน User Authentication คุณสามารถกำหนดได้ทั้ง reusable และ S/key และข้อมูลอื่น ๆ ก่อนที่จะให้ผู้ใช้จากภายนอกใช้บริการต่าง ๆ ได้

6.5 การกำหนดกฎ เงื่อนไขความปลอดภัย

การให้บริการของระบบเน็ตเวิร์ก และบริการอื่น ๆ จะทำงานแบ่งเป็น 2 ทิศทาง ในการที่จะติดต่อกันระหว่างเครื่องคอมพิวเตอร์หรือเครือข่าย เราสามารถกำหนดกฎเงื่อนไขระบบรักษาความปลอดภัย ได้ 2 ส่วน คือ

- ระบบระษาความปลอดภัยที่สามารถจำกัดหรือป้องกันการติดต่อจากภายนอกระบบ Firewall เข้าสู่ภายใน (outbound)
- ระบบรักษาความปลอดภัยที่สามารถนำกัดหรือป้องกันการ ติดต่อจาก untrusted หรือระบบภายนอกมายังระบบที่ดูแลระบบอยู่



รูปที่ 6.5 แสดง User authentication

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบรักษา ความปลอดภัยของ Outbound จะกำหนดให้ ผู้ใช้และบริการต่าง ๆ เช่น FTP และ e-mail บน trusted network สามารถที่จะใช้บริการหรือติดต่อกับผู้ใช้หรือบริการที่อยู่บน untrusted และunknown network ส่วนรักษาความปลอดภัยของ Inbound จะกำหนดให้ผู้ใช้และบริการต่าง ๆ สามารถที่จะติดต่อกับ ผู้ใช้หรือบริการที่อยู่บน trusted network ได้

ตัวอย่าง เช่น ถ้าผู้ใช้ต้องการที่จะส่ง e-mail ไปยังผู้ใช้ที่อยู่บน untrusted หรือ unknown network คุณจะต้องกำหนดกฎเงื่อนไขของ Inbound เพื่อที่จะยอมให้ผู้ใช้สามารถที่จะส่งข้อความไปยัง mail server ส่งข้อความไปยัง untrusted หรือ unknown network ได้

เมื่อมีการกำหนดระบบรักษาความปลอดภัยในส่วนต่าง ๆแล้วจะต้องสามารถที่จะตรวจสอบบริการต่าง ๆ ที่ผ่านไปมาในระบบได้และสามารถที่จะกำหนดเวลาในการใช้บริการหรือส่วนอื่น ๆ ที่สามารถที่จะกำหนดได้ เช่น ActiveX, Javafilter

6.6 การประยุกต์ใช้กฎ เงื่อนไขระบบรักษาความปลอดภัย

ในการติดต่อบริการต่าง ๆ ทั้ง 2 ทิศทาง นั้น จะต้องมีการประยุกต์ใช้ระบบรักษาความปลอดภัยเพื่อความเหมาะสมกับระบบส่วนของ Inbound ควรจะมีการประยุกต์ระบบรักษาความปลอดภัยเพื่อที่จะสามารถใช้บริการต่าง ๆ ไปยัง Internet branch เหนือโหนดที่อยู่ต่ำกว่า ซึ่งทำให้สามารถที่จะติดต่อกันได้ระหว่าง external และ internal ภายใน trusted network ส่วนของ Outbound สามารถที่จะกำหนดกฎเงื่อนไขต่าง ๆ ได้ที่ logical หรือที่ trusted network ซึ่งสามารถทำให้เครื่องภายในสามารถใช้บริการต่าง ๆ เพื่อติดต่อกับเครื่องภายนอกได้ (external network)

6.7 การติดตั้ง Reporting และ Monitoring

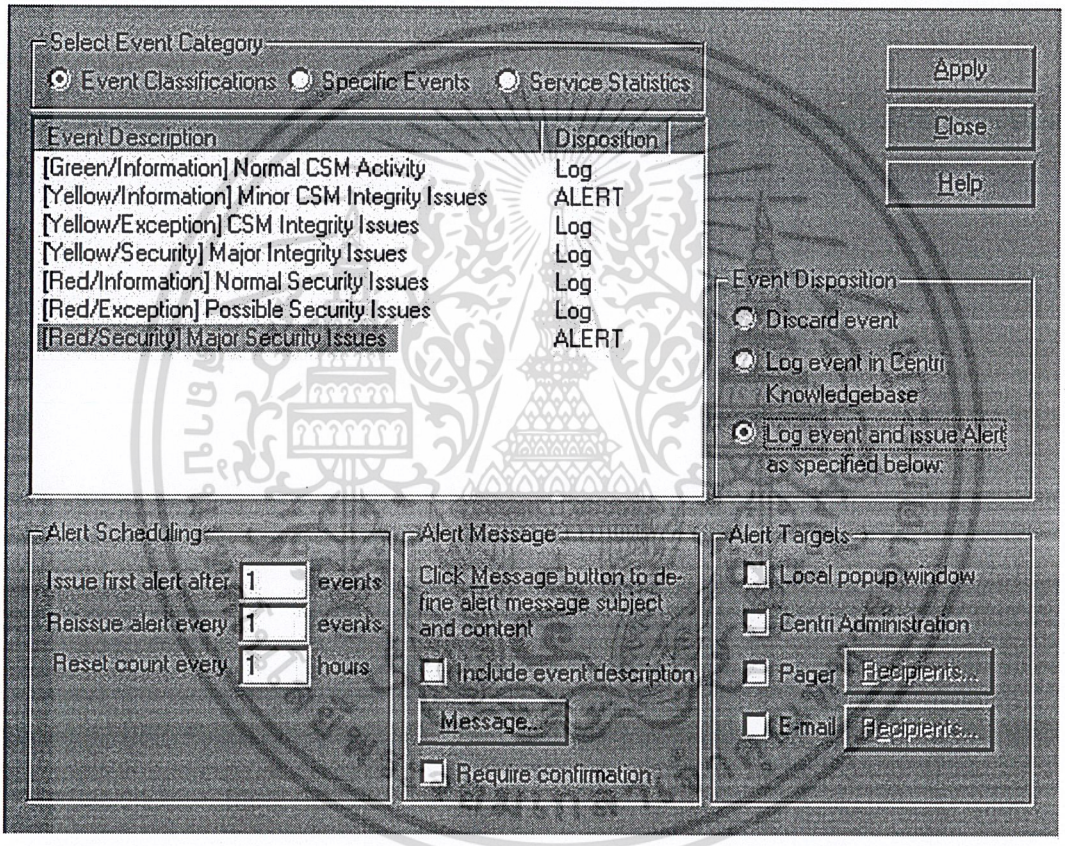
ในระบบของ Cisco Centri Firewall นั้น ส่วนของ reporting และ monitoring จะมีความสัมพันธ์กันมากเพราะเป็นข้อมูลที่เกิดจากการกระทำของส่วนต่าง ๆ มาเป็น report และทำการประเมินโดยระบบ monitoring ซึ่งขึ้นอยู่กับเหตุการณ์ที่เกิดขึ้นและได้รับการพิจารณาจากระบบรักษาความปลอดภัยแล้ว ทั้งสองส่วนที่กล่าวมาจะเป็นส่วนที่อยู่ใน Subsystem คือ การตรวจสอบและการกรองข้อมูลต่าง ๆ

เหตุการณ์ที่เกิดขึ้นจะถูกบันทึก ซึ่งหมายถึง เป็นส่วนที่เกิดขึ้นภายในระบบรักษาความปลอดภัย ส่วนประกอบต่าง ๆ ที่เกิดขึ้นจะถูกบันทึกเพื่อเป็นข้อมูลในการตรวจสอบและใช้ในการพิจารณา

เอกสารนี้เป็นลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ในการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในการตรวจสอบข้อมูล สังเกตจากเหตุการณ์ที่ถูกบันทึกไว้ซึ่งผู้ดูแลระบบจะพิจารณาเหตุการณ์ที่เกิดขึ้นว่าส่วนว่าส่วนใดที่ไม่ต้องการหรือส่วนใดเป็นส่วนที่สำคัญ ผู้ดูแลระบบจะต้องศึกษารายละเอียดจากบันทึกต่าง ๆ ที่อธิบาย ถึงเหตุการณ์ที่เกิดขึ้นในระบบรักษาความปลอดภัย เมื่อพบส่วนที่น่าสนใจก็จะพิจารณาและทำการควบคุมส่วนนั้น

ขั้นแรกจะต้องติดตั้ง reporting และ monitoring ในการตรวจสอบเหตุการณ์ต่าง ๆ ที่เกิดขึ้น เพื่อที่จะสังเกตและบันทึกส่วนต่าง ๆ ที่เกิดขึ้นซึ่งสามารถที่จะกำหนด monitoring ตามรูป



รูปที่ 6.6 แสดง Audit record

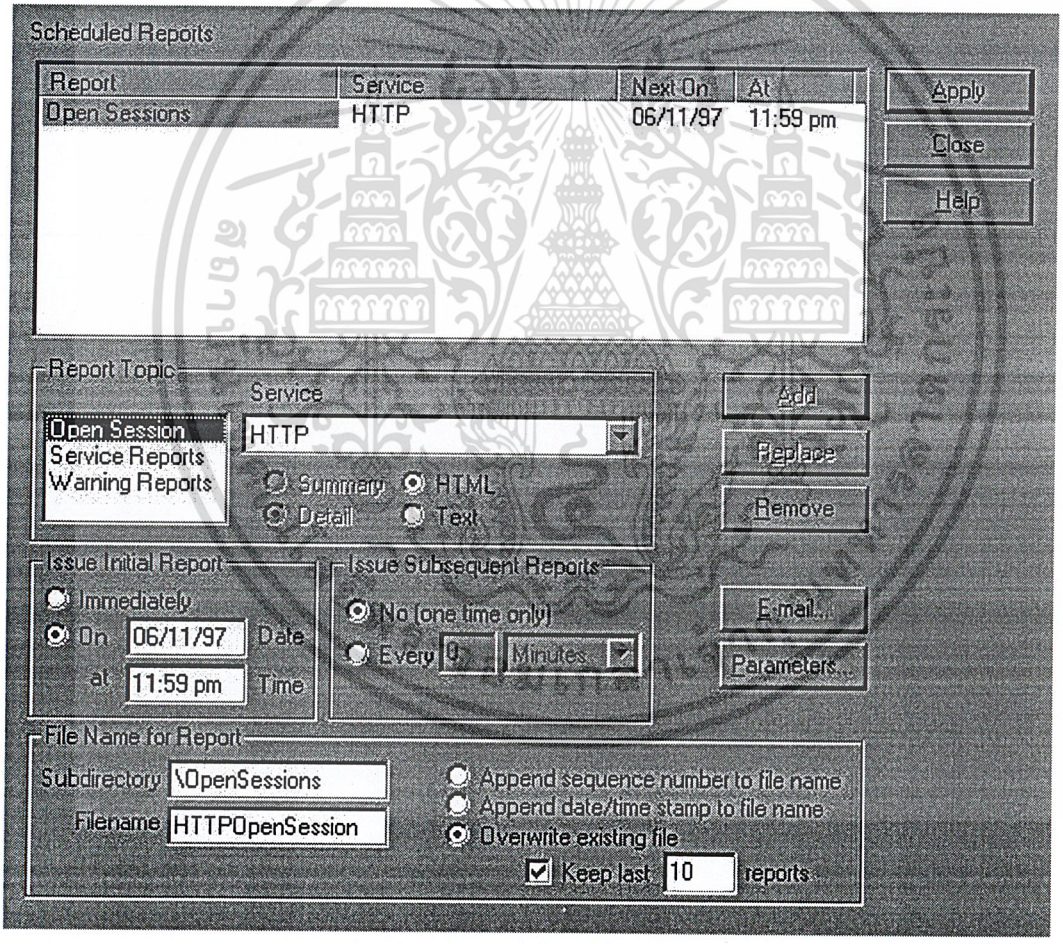
Note Cisco Centri Firewall สามารถที่จะให้รายละเอียดและบันทึกต่าง ๆ ที่น่าสนใจเพื่อเป็นประโยชน์ ต่อผู้ดูแลระบบ และปัญหาที่เกิดขึ้นในส่วนของ Firewall Server ที่เกิดจากการเลิกให้ระบบดูแลในขอบเขตต่าง ๆ

Roporting Subsystem สามารถที่จะบอกรายระเอียดและบทสรุปของข้อมูลที่เกี่ยวกับเหตุการณ์ที่เกิดขึ้น จากการที่กำหนดรายละเดียดของการรายงานของระบบไว้ โดยสามารถที่จะ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กำหนดค่าของ monitoring และ reporting ในช่วงเวลาที่มีการติดต่อกับระบบเครือข่ายทุก ๆ นาที , ชั่วโมง ,วัน ,สัปดาห์,เดือน ,ปี , หรือเป็นช่วงเวลาได้ซึ่งจะมีบันทึกอยู่ 3 แบบ คือ

- Statistical /Summary Reports จะเป็นข้อมูลต่าง ๆ ที่เกี่ยวกับกิจกรรมที่มีการติดต่อกับบริการต่าง ๆ ดังรูป
- Detail Report จะเป็นรายละเอียดของข้อมูลที่เกี่ยวกับบริการต่าง ๆ ที่เป็นส่วนสำคัญ
- Warning Report เป็นข้อมูลเกี่ยวกับส่วนของ Cisco Centri Firewall



รูปที่ 6.7 ตารางสรุปบันทึกการรายงาน

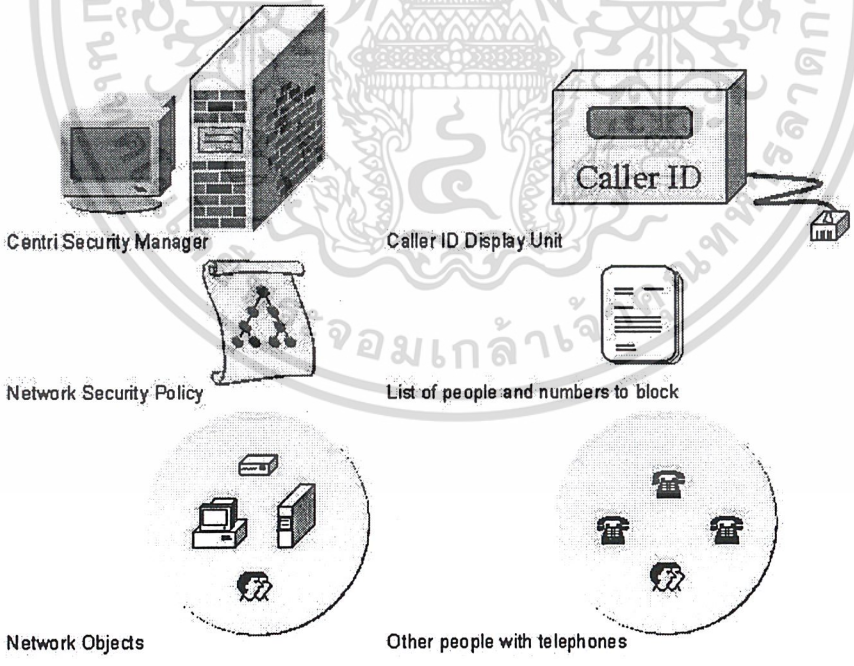
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 7
ความเข้าใจเกี่ยวกับกฎ เงื่อนไขของความปลอดภัย

Cisco Centri Firewall จะใช้ข้อกำหนดต่าง ๆ ที่มีอยู่มาใช้ในการออกแบบระบบรักษาความปลอดภัยให้กับผู้ที่เข้ามาใช้คอมพิวเตอร์ หรือไม่ให้ใช้คอมพิวเตอร์ในระบบ ซึ่งจะต้องมีการเริ่มต้นในการติดตั้ง และสามารถที่จะแก้ไข ปัญหาที่เกี่ยวกับ Network Service

7.1 ข้อกำหนด นโยบาย อย่างไร

ระบบรักษาความปลอดภัยของ Cisco Centri Firewall จะควบคุมการทำงานของความหนาแน่นในระบบเครือข่ายระหว่างระบบเครือข่ายภายใน Firewall กับ เครือข่ายระหว่างระบบเครือข่ายภายใน Firewall กับเครือข่ายภายนอก โดยจะควบคุมเป็น Session ระหว่าง 2 เครือข่าย สามารถเปรียบเทียบได้กับระบบโทรศัพท์ที่โทรคุยกัน ทีอยู่ 5 วิธี ที่เอามาเปรียบเทียบกันระหว่าง Cisco Centri Firewall และระบบ Caller ID ในเรื่อง sessions, session controls, action, policy inheritance และ network object



รูปที่ 7.1 การเปรียบเทียบ Firewall กับเครื่องตอบรับโทรศัพท์อัตโนมัติ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปจะมีความสัมพันธ์กันอยู่ระหว่าง Cisco Centri Firewall คือ ข้อกำหนดขงระบบความปลอดภัยและอุปกรณ์ในระบบที่ใช้ในการติดต่อ กับ Caller ID, รายชื่อและเบอร์โทรศัพท์และเครื่องโทรศัพท์เครื่องต่าง ๆ ตามลำดับ

Call ID จะทำหน้าที่ คล้ายยาบ Cisco Centri Firewall ซึ่งเป็นตัวกลางที่ต่อเข้ามายังเครื่องโทรศัพท์ แต่มีความแตกต่างกันคือ Cisco Firewall จะสามารถกรอง และกันในส่วนที่ไม่ถูกต้องได้ ซึ่ง Call ID ทำไม่ได้

ในกรณีที่ไม่ต้องการรับโทรศัพท์ จากบุคคลที่เราไม่ต้องการจะคุยด้วยก็อาจจะมีคนบอกปฏิเสธ ไปแทน จะรับเฉพาะคนที่ต้องการจะคุยด้วยใน Cisco Centri Firewall ก็คล้ายจะมีข้อกำหนดที่จะยอมหรือไม่ยอมให้มีการติดต่อกันระหว่างกันระหว่าง เครือข่ายซึ่งขึ้นอยู่กับข้อกำหนด, นโยบายรักษาความปลอดภัยที่มี รวมถึงการติดต่อจากภายในออกสู่ภายนอกของ Firewall เอง และยังรวม ถึงช่วงเวลาในการติดต่อ,ปลายทางและชนิดจองโปรโตคอลในการติดต่อ

เมื่อมีสายโทรศัพท์โทรเข้ามา Call ID จะแสดงรายละเอียด ของสายที่โทรเข้ามา เป็นใคร ชื่ออะไร เบอร์จากหน่วยงานใด วันและเวลาในการโทรเข้ามา ข้อมูลเหล่านี้ จะมาใช้ในการพิจารณา ว่ามีการรับโทรศัพท์ได้หรือไม่

ในระบบเครือข่ายรายละเอียดต่าง ๆ ชื่อเบอร์โทรศัพท์ เปรียบได้กับ session control ซึ่งเป็นข้อมูลพื้นฐานเบื้องต้นในการพิจารณาจะเปรียบเทียบได้กับใบเสร็จ ค่า โทรศัพท์ซึ่งจะมีเบอร์โทรศัพท์ ที่คุณโทรและใครโทรหาคุณ และไปพิจารณาในการกำหนดความปลอดภัยต่าง ๆ ใน Cisco Centri Firewall ก็สามารถที่จะทำได้เช่นกัน

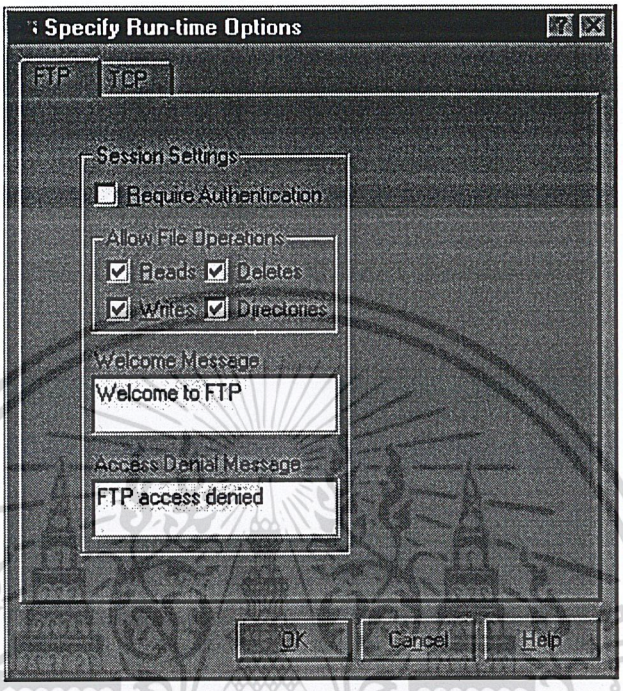
Service ต่าง ๆได้หรือไม่ได้ในแต่ละ session

7.2 session จะมีด้วยกัน 2 แบบ

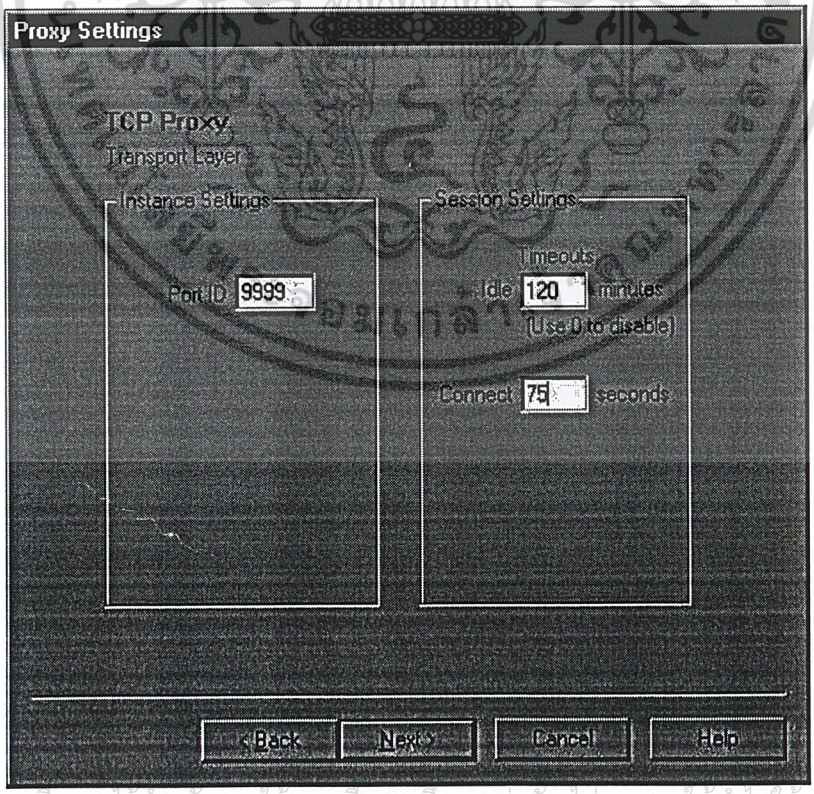
- run time session control จะควบคุมในขณะที่มีการติดต่อเข้ามาหา Firewall โดยอาศัยข้องกำหนดกฎการรักษาความปลอดภัยต่าง ของ Firewall ในการพิจารณา ในการติดต่อ
- Static session controls จะเป็นตัวที่ช่วยในการแก้ไขส่วนต่าง ๆของ session โดยส่วนใหญ่จะอยู่ภายให้การควบคุมของ network service branch จะมีรายละเอียดที่มากขึ้น เช่น ระยะเวลา หมายเลขพอร์ต ที่มากขึ้น เช่น ระยะเวลา และหมายเลขพอร์ต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สังเกตจาก runtime session control ของ FTP และ Static session contrlols ของ FTP



รูป 7.2 แสดง Run-time Session



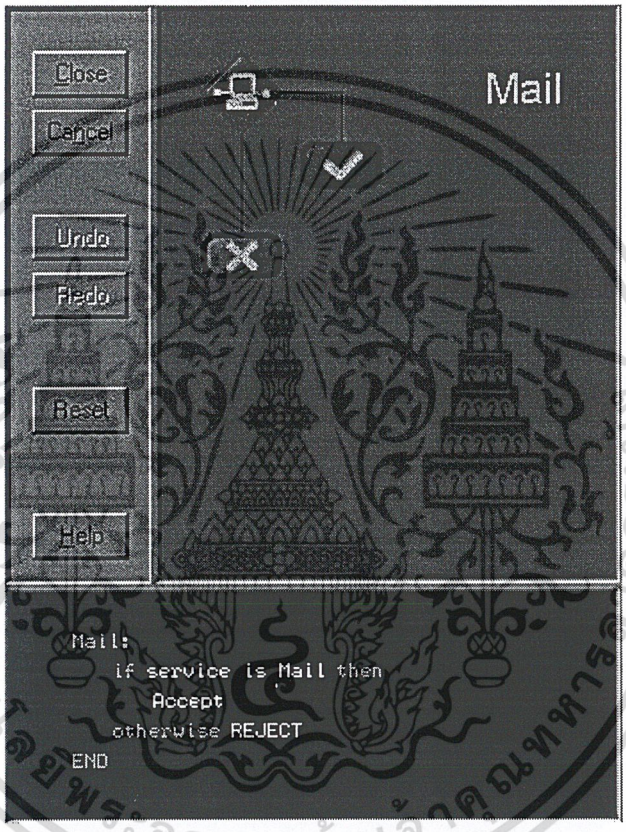
รูป 7.3 แสดง Static Session

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ซึ่งจะมีตัวเลือกในการกำหนดบริการภายใน รวมทั้งหมายเลขพอร์ต, พร็อกซี่

ในส่วนของผู้ใช้ ข้อกำหนดความปลอดภัยจะแสดงเป็นโครงข่ายในการควบคุมของแต่ละบริการคล้ายกับขั้นบันไดแบ่งได้เป็น 2 ส่วน คือ

- accept เป็นส่วนที่จะสามารถเข้าไปใช้บริการได้ สามารุที่จะติดต่อกับเครือข่ายได้
- reject เป็นส่วนที่ Firewall ไม่ยอมให้,มีการติดต่อในส่วนที่ต้องการจะติดต่อบริการด้วย



รูปที่ 7.4 แสดงการกำหนด Policy

จากรูปจะใช้เป็นส่วนในการพิจารณาข้ากำหนดที่สามารถจะใช้บริการได้ โดย ผู้ดูแลระบบเป็นคนออกแบบสามารถที่จะใช้ได้หรือไม่ได้ใน ซึ่งเป็นในลักษณะของ กราฟฟิกในการกำหนด policy ซึ่งรูปแบบจะเป็นในลักษณะของการกำหนดตัวเลือก โดยพิจารณาเป็นจุดๆ ให้เลือกเส้นทางที่สามารถทำได้หรือไม่ได้ หรือทำในส่วนของ User next policy คือส่วนที่ต้องการให้มีการบริการแต่ไม่มีความพอใจใน path ต่อมา

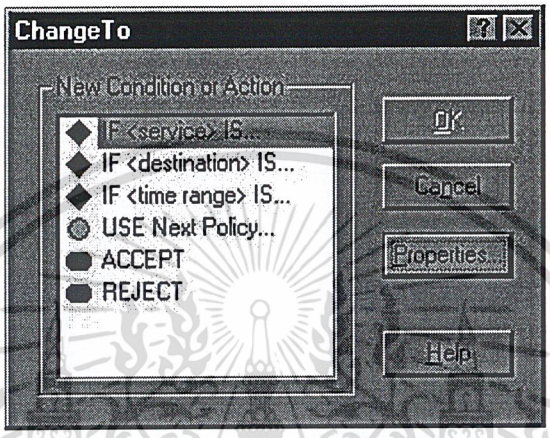
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

7.3 ระดับในการตั้งข้อกำหนดจะดูได้ดังรูป มี

3 เงื่อนไข

2 ข้อกำหนด

และ 1 ส่วน



รูปที่ 7.5 High-Level Condition

Use next policy เป็นส่วนที่นำเราไปสู่ส่วนของ policy inheritance ซึ่งเป็นส่วนที่จะทำให้เราเข้าใจระบบก่อนที่จะไปพัฒนา ข้อกำหนดต่าง ๆ

Policy inheritance เป็นความฉลาดของ Centri Firewall เป็นการกลับมาใช้ข้อกำหนดอีกครั้ง ถ้า Use next policy อยู่ไต้โหนดใด หมายถึง จะส่งผลไปให้ Trusted networksโดเมน หรือ Internet

ถ้า Use policy อยู่ใต้ use next policy หมายถึง ครอบคลุมถึงส่วนที่ซ่อนอยู่ ที่อยู่ต่ำกว่าโหนดที่เรามองอยู่แต่ถ้าทั้ง 2 กรณี เหมือนกัน ก็จะคล้าย ดังรูป

ใน Centri Firewall กฎข้อกำหนดของ policy inheritance จะใกล้เคียงกับ Network tree ขั้นตอนจะเริ่มจากด้านบนไปยังด้านล่าง จะเป็นประโยชน์มากกับระบบขนาดใหญ่ หรือหลายองค์กร หรือมีผู้ใช้มาก ๆ ในระดับของ high-level node และ lower-level node ใน network tree

ใน Centri สามารถมีได้หลายๆ trusted network ซึ่งคือ internal network ก็คล้ายกับในบ้านของเรามีโทรศัพท์หลายเครื่อง เพราะเราสามารถที่จะควบคุมการติดต่อระหว่างระบบภายในและระบบภายนอกได้ trust network ก็สามารถที่จะติดต่อกับ untrusted หรือ unknown network ได้ คล้ายกับการโทรศัพท์ออกไปนอกบ้าน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

trusted netsork คือ อุปกรณ์ของเครือข่ายที่มีคนดูแลระบบคอยดูแลควบคุมความปลอดภัยอยู่

untrusted network คืออุปกรณ์เครือข่ายที่ไม่มีคนดูแลระบบคอบดูแลควบคุมความปลอดภัย

unknown network คือ อุปกรณ์ของเครือข่ายที่ไม่รู้จักหรือไม่รู้ IP address

เราสามาระที่จะกำหนดค่า IP address และ subnet mark หรือชื่อ host name เช่น \\trumpet ซึ่งจะคล้ายกับเบอร์โทรศัพท์ที่บันทึกไว้บนเครื่องสามารถต่อได้ทันที ในส่วนของ Call ID สามารถจะกรองหรือกันในแต่ละพื้นที่ได้เช่น (075) 381130 เราสามารถที่จะกันพื้นที่ได้ (ล็อคโทรทางไกล)

ใน Centri ก็สามาระจะทำได้โดย กำหนด domain name, Group account หรือ user account จะทำการติดต่อกับ network ต่าง ๆ ตาม address ที่ระบุโดยเครื่องจะเข้าใจในภาษาของเครื่องเองถ้าหากมีปัญหาในระบบการติดต่อต่าง ๆ หรือเกี่ยวกับระบบความปลอดภัยก็จะทำการ log ส่วนที่เป็นปัญหาเพื่อจะสามารถนำมาดูและแก้ไขได้

เราสามารถที่จะใช้เครื่องจากที่อื่น ๆเข้ามาในระบบของ Firewall ได้ โดยการ log in เข้ามาในระบบซึ่งทำหน้าที่เสมือนกับเครื่องที่อยู่ในระบบรักษาความปลอดภัย แต่ต้องเข้าใจระบบความปลอดภัยและนำมาประยุกต์ใช้ให้มีความสามารถที่เท่ากับเครื่องที่เคยใช้

7.4 ตัวอย่างการเขียน Policy

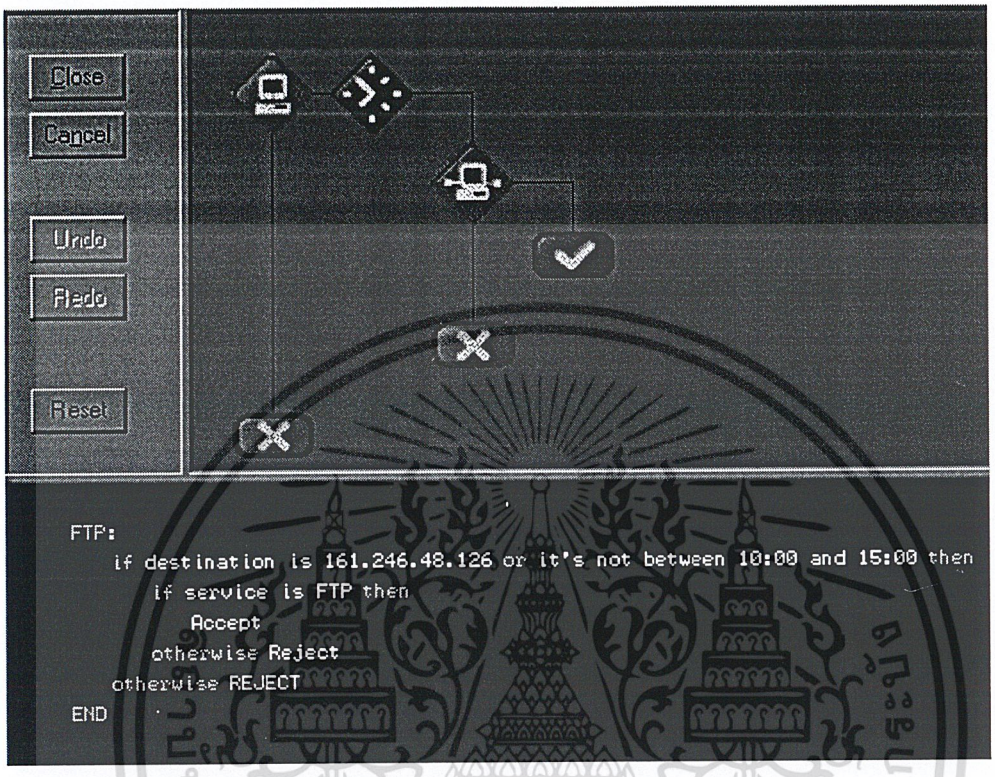
ดังที่ได้กล่าวไปแล้วข้างต้นว่าการเขียน Policy ของไฟร์วอลนั้นจะเป็นลักษณะของ Graphic User Interface (GUI) ซึ่งทำให้ง่ายต่อการเขียนนอกจากนั้นจะยังมีการอธิบายเป็นภาษาอังกฤษซึ่งยิ่งสะดวกในการทำความเข้าใจได้ดียิ่งขึ้นดังตัวอย่างต่อไป

ตัวอย่างที่ 7.1

ในรูปที่ 7.6 เป็นตัวอย่างของการเขียน Policy โดยได้กำหนด Destination คือเครื่องเซิร์ฟเวอร์ที่ปลายทางที่กำหนดให้สามารถเรียกใช้บริการได้ในที่นี้คือ 161.246.48.126 หากเรียกใช้บริการไปยัง เซิร์ฟเวอร์อื่น ไฟร์วอลจะไม่อนุญาตให้ใช้ ส่วนต่อมาหลัง " or " เป็นการกำหนดเวลาของการใช้บริการโดยสามารถที่จะกำหนดว่าจะให้ใช้หรือไม่ในช่วงเวลาใด ในตัวอย่างที่ 7.1 นี้เป็นการกำหนดว่าไม่ให้ loging เข้ามาใช้ในช่วงเวลา 10.00 น. ถึง 15.00 น. หลังจากที่ผ่านข้อกำหนดในบรรทัดแรกแล้วก็มาพิจารณาบรรทัดถัดไปซึ่งจะเป็นการตรวจสอบ บริการที่เรียกใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หากเป็น FTP ตามที่ได้กำหนดไว้จึงจะสามารถที่จะใช้งานได้โดยนอกเหนือไปจากนี้ไฟร์วอลจะปฏิเสธการบริการ



รูปที่ 7.6 ตัวอย่างการเขียน Policy

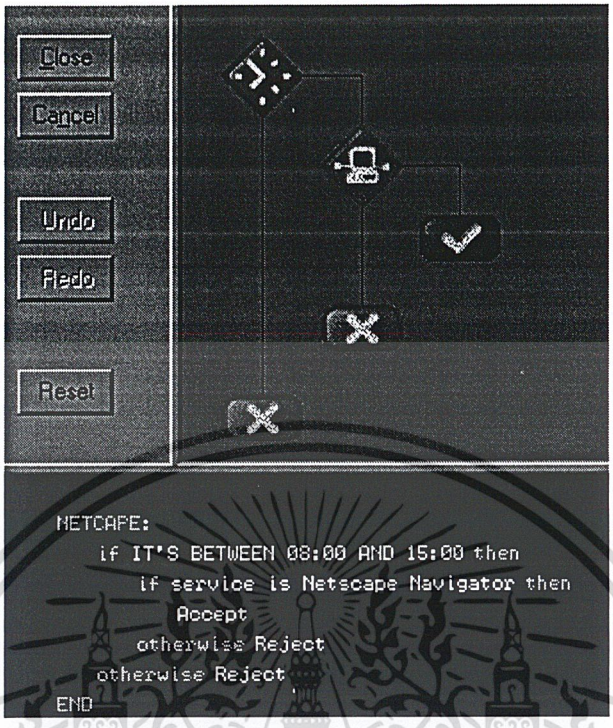
ตัวอย่างที่ 7.2

ตัวอย่างนี้จะเป็นการกำหนดเกี่ยวกับการให้บริการ Netscape ดังรูปที่ 7.7 ซึ่งสามารถอธิบายการตรวจสอบข้อกำหนดได้ดังต่อไปนี้

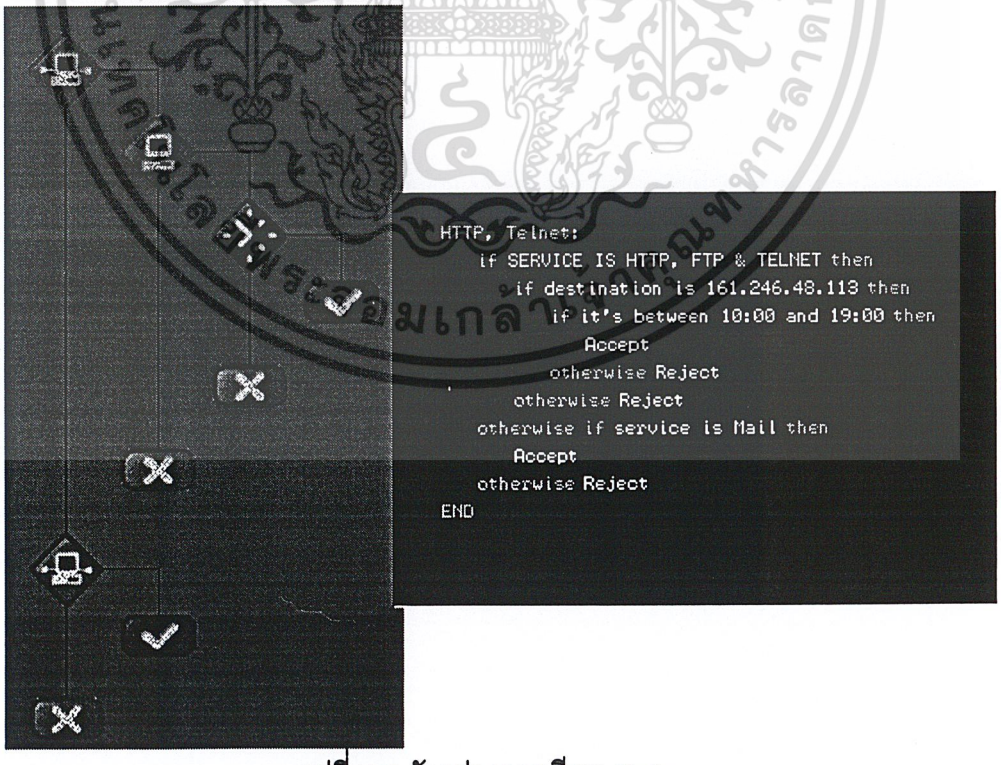
ในบรรทัดแรกนั้นจะเป็นการตรวจสอบเวลา โดยได้กำหนดไว้ว่าสามารถที่จะ loginเข้ามาใช้บริการได้ในช่วง 8.00-15.00 น. หากมีการ login เข้ามาใช้บริการผ่านไฟร์วอลในช่วงเวลาที่กำหนดไว้เท่านั้นจึงจะสามารถที่จะใช้ได้และมีการตรวจสอบในบรรทัดต่อไป

หากผ่านข้อกำหนดในบรรทัดแรกแล้วบรรทัดต่อมาเป็นการตรวจสอบว่าบริการที่เรียกใช้นั้นเป็นบริการที่ใช้ผ่าน Netscape หรือไม่ หากถูกต้องจะสามารถใช้บริการได้โดยนอกเหนือจากที่ได้กำหนดไว้ใน Policy จะไม่สามารถที่จะใช้บริการผ่านไฟร์วอลได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 7.7 ตัวอย่างการเขียน Policy ให้บริการ Netscape



รูปที่ 7.8 ตัวอย่างการเขียน Policy

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตัวอย่างที่ 7.3

ในตัวอย่างนี้จะเป็นการเขียน Policy ที่มีความซับซ้อนมากยิ่งขึ้นดังรูปที่ 7.8 ซึ่ง Policy ที่เขียนขึ้นนั้นแบ่งได้เป็นสองส่วน โดยในส่วนแรกนั้นจะเริ่มตั้งแต่บรรทัดแรกโดยจะตรวจสอบว่าบริการที่เรียกใช้เป็นหนึ่งในสามตัวที่กำหนดหรือไม่ คือ HTTP,FTP หรือ Telnet หากการเรียกใช้บริการถูกต้องไฟร์วอลก็จะทำการตรวจสอบบรรทัดถัดไป โดยจะเป็นการตรวจสอบในเรื่องของ Destination โดยกำหนดให้เรียกใช้เซิร์ฟเวอร์ที่ 161.246.48.126 เท่านั้นหลังจากนั้นก็จะตรวจสอบเวลาที่เรียกใช้บริการว่าถูกต้องหรือไม่เป็นลำดับสุดท้ายในบรรทัดต่อไป เป็นอันสิ้นสุดของ Policy ส่วนแรก ส่วนหลังของ Policy ในตัวอย่างนี้นั้นจะทำการตรวจสอบหลังจากที่ส่วนแรกปฏิเสธการให้บริการ ส่วนที่สองจะทำการตรวจสอบการขอใช้บริการนั้นว่าตรงกับส่วนของมันเองหรือไม่หากตรงกันซึ่งในตัวอย่างกำหนดว่าเป็นการให้บริการ Mail เพียงเงื่อนไขเดียวเท่านั้น

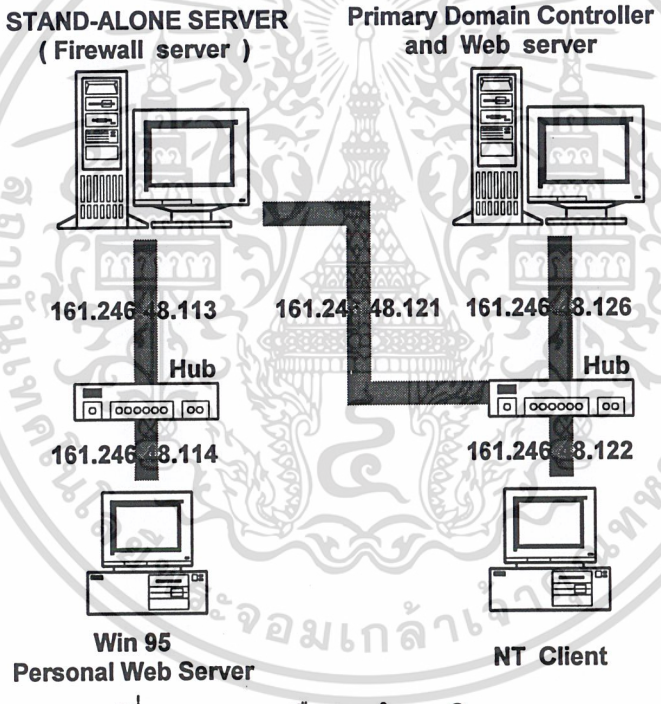
การกำเขียน Policy ในตัวอย่างที่ 7.3 นั้นเป็นการเขียนในลักษณะของทางเลือกซึ่งสามารถที่จะทำการเลือกเป็นเส้นทางได้ ทำให้เราสามารถประยุกต์การเขียน Policy ได้อย่างกว้างขวางและครอบคลุมการใช้งานระบบเครือข่ายและการบริการได้อย่างเป็นอย่างดี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่8
ผลการทดลอง

8.1 ระบบเครือข่ายที่ใช้

จากการที่โปรแกรม Cisco Centri Firewall นั้นรันบนวินโดวส์เอ็นที จึงทำการติดตั้งระบบเครือข่ายที่ใช้วินโดวส์เอ็นทีขึ้น แต่เนื่องขาดประสบการณ์ในการวางระบบเครือข่าย เครือข่ายที่จัดขึ้นจึงไม่ได้ทำการต่อเข้ากับระบบเครือข่ายอินเตอร์เน็ตจริง เพราะอาจจะทำให้เกิดความเสียหายกับการให้บริการอินเตอร์เน็ตของสถาบันจากการทดลองได้ ระบบที่จัดขึ้นจึงเป็นระบบเครือข่ายจำลองอิสระโดยมีรูปแบบระบบดังรูปที่ 8.1

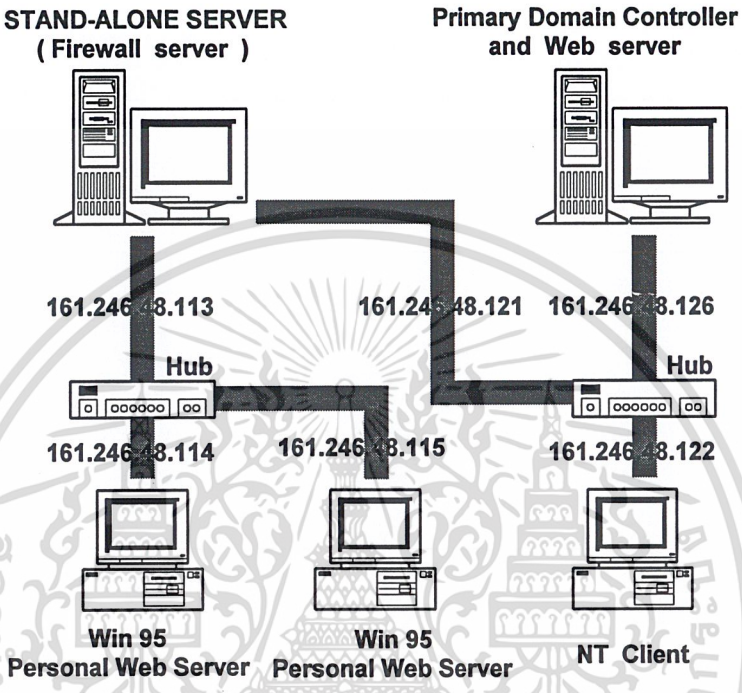


รูปที่ 8.1 ระบบเครือข่ายจำลองอิสระ

จากระบบเครือข่ายจำลองอิสระในรูปที่ 8.1 เครื่องที่เป็นไฟร์วอลเซิร์ฟเวอร์นั้นใช้การติดตั้งแบบ stand-alone server โดยเป็นตัวแยกเครือข่ายสองเครือข่ายออกจากกันโดยเครือข่ายหลังไฟร์วอล(Trusted network)นั้นมีเครื่องเซิร์ฟเวอร์ของโดเมน (Primary Domain Controller) เป็นผู้ให้บริการ Web Server ในระบบเครือข่ายด้วยส่วนเครือข่ายภายนอกของไฟร์วอล (Untrusted network) นั้นมีเครื่องวินโดวส์ 95 ที่ให้บริการ Web server และใช้ในการทดลองเข้าใช้บริการต่างๆ ของ Web server ภายในเครือข่ายไฟร์วอลด้วย แต่เนื่องจากการมีเครื่องภายนอกเครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ไฟร์วอลเพียงเครื่องเดียวนั้นขาดข้อเปรียบเทียบจึงทำการเพิ่มเครื่อง วินโดวส์ 95 Personal Web server เข้าไปที่เครือข่ายภายนอกอีกหนึ่งเครื่องดังรูปที่ 8.2 เพื่อใช้ในการเปรียบเทียบผลการทดลองต่างๆ ที่ทดลองกับไฟร์วอล



รูปที่ 8.2 เครือข่ายจำลองที่ใช้ในการทดลอง

8.2 การทดลองโปรแกรมไฟร์วอล

ในการทดสอบการทำงานของโปรแกรมไฟร์วอลนั้น มีการใช้คำศัพท์เฉพาะที่ควรพิจารณา คือ

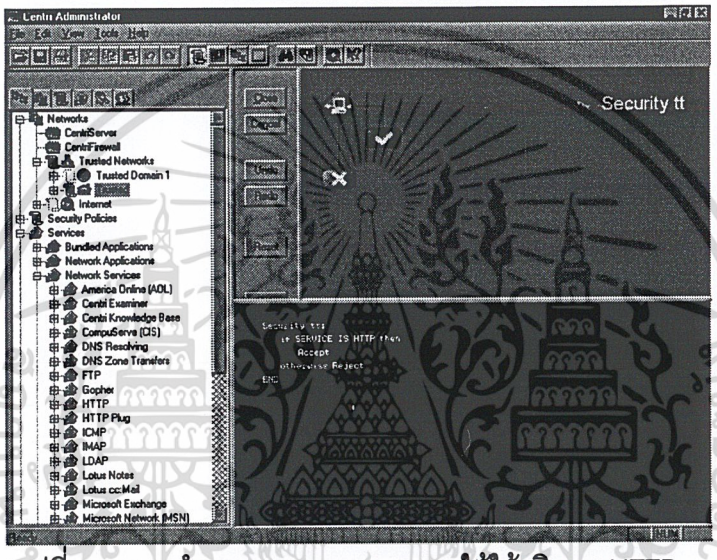
- Inbound คือการติดต่อออกสู่เครือข่ายภายนอกไฟร์วอลโดยผู้ใช้ที่อยู่ในเครือข่ายหลังไฟร์วอล หรือ Trusted network
- Inbound Policy คือการกำหนดนโยบายสำหรับการบังคับการติดต่อแบบ inbound
- Outbound คือการติดต่อเข้าสู่เครือข่ายหลังไฟร์วอลโดยผู้ใช้ที่อยู่ในเครือข่ายภายนอกไฟร์วอล หรือ Untrusted network
- Outbound Policyคือการกำหนด นโยบายสำหรับ การบังคับการติดต่อ แบบ Outbound

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

8.2.1 Inbound Policy

ในการทดลองเกี่ยวกับ Inbound Policy นั้นได้แยกกำหนดเงื่อนไข ในการทดลองเป็นกรณี ๆ คือ

- การกำหนดการใช้บริการจากเครือข่ายภายนอกได้เฉพาะบริการ HTTP ซึ่งสามารถเขียน Policy ได้ดังรูปที่ 8.3 ซึ่งเป็นการกำหนดให้ใช้บริการ HTTP สำหรับผู้ใช้ภายในเครือข่ายไฟร์วอลโดยไม่มีเงื่อนไขอื่น

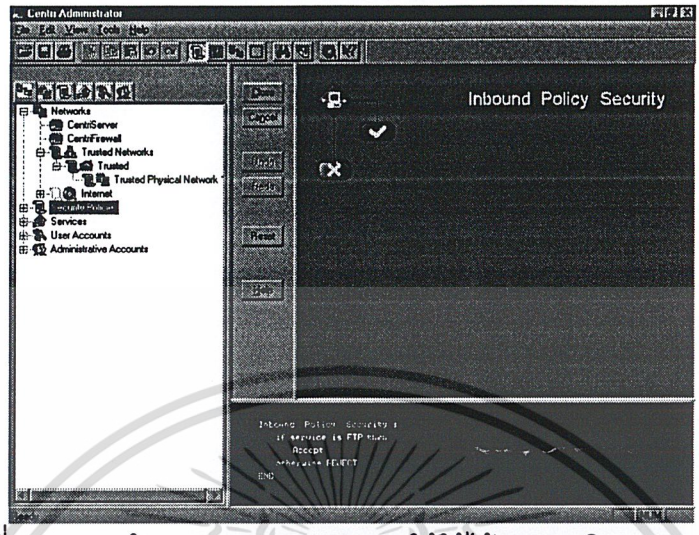


รูปที่ 8.3 การกำหนด Inbound Policy ให้ใช้บริการ HTTP

จากการทดลอง ใช้ Netscape navigator เรียกใช้บริการ HTTP ไปที่เครือข่ายภายนอกไฟร์วอลที่เป็น 95 Web server ปรากฏว่าสามารถใช้บริการได้ในขณะที่ไม่สามารถใช้บริการอื่นๆ ที่ไม่ได้กำหนดใน Policy ได้

- การกำหนดให้ใช้บริการจากเครือข่ายภายนอกได้เฉพาะบริการ FTP ซึ่งสามารถเขียน Policy ได้ดังรูปที่ 8.4 ซึ่งเป็นการกำหนดให้ใช้บริการ FTP สำหรับผู้ใช้ภายในเครือข่ายไฟร์วอลโดยไม่มีเงื่อนไขอื่น

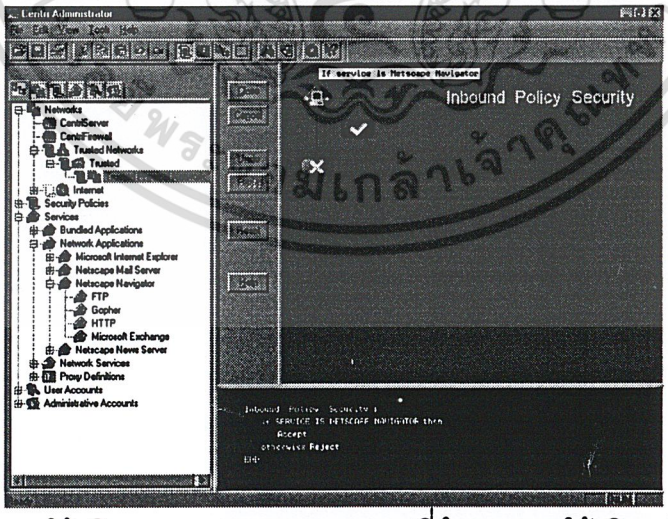
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 8.4 การกำหนด Inbound Policy ให้ใช้ได้เฉพาะบริการ FTP

จากการกำหนดการให้บริการเฉพาะ FTP ดังกล่าว จากการทดลองการใช้บริการ FTP ของเครื่องภายนอกเครือข่ายไฟร์วอลปรากฏว่าสามารถใช้งานได้ตามปกติ ในขณะที่ไม่สามารถใช้บริการชนิดอื่น ๆ ได้

- กำหนดการใช้บริการจากเครือข่ายภายนอกผ่าน Netscape Navigator ภายใต้บริการที่กำหนดโดยไฟร์วอลซึ่งสามารถเขียน Policy ได้ดังรูปที่ 8.5



รูปที่ 8.5 การใช้บริการ Netscape Navigator ที่กำหนดการใช้บริการโดยไฟร์วอล

จากการทดลอง ปรากฏว่า สามารถใช้บริการที่ไฟร์วอลกำหนดผ่าน Netscape Navigator ได้ โดยบริการที่ไม่ได้ถูกกำหนดให้ใช้บริการไม่สามารถใช้บริการได้

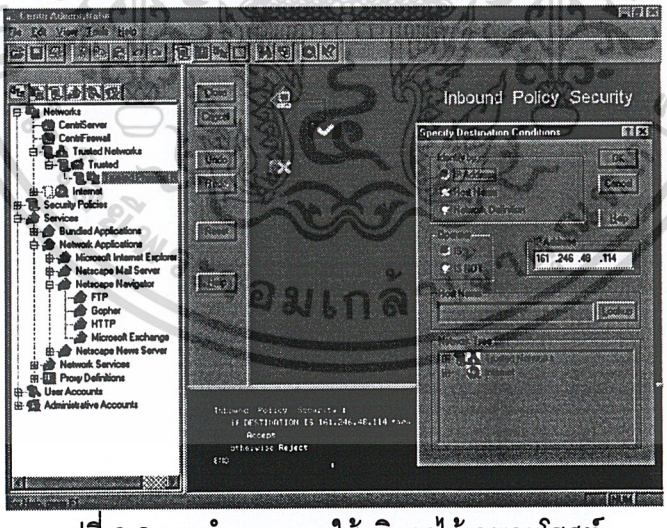
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งไม่อนุญาตให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- การกำหนดโฮสท์ปลายทางที่สามารถใช้บริการได้หรือไม่ได้ ในการกำหนด Policy นั้นจะใช้การกำหนดโฮสท์ปลายทาง (destination) ว่าสามารถที่จะใช้บริการได้หรือไม่ได้ โดยมีลักษณะของการกำหนด 3 ชนิด คือ IP address, Host name และ Network definition ดังรูป 8.6 ซึ่งเป็นาการกำหนด Policy ให้สามารถใช้บริการโฮสท์ภายนอกเครือข่ายไฟร์วอลได้เฉพาะโฮสท์ที่กำหนด โดยไม่จำกัดการบริการ

จากการทดลอง โดยใช้ Netscape Navigator เรียกใช้บริการบนโฮสท์ที่กำหนดให้สามารถใช้บริการได้ซึ่ง สามารถใช้บริการได้โดยไม่ถูกจำกัดการใช้บริการ ในขณะที่การเรียกใช้บริการจากโฮสท์ที่ไม่ได้ถูกกำหนดให้ใช้งานได้ จะไม่สามารถใช้งานได้

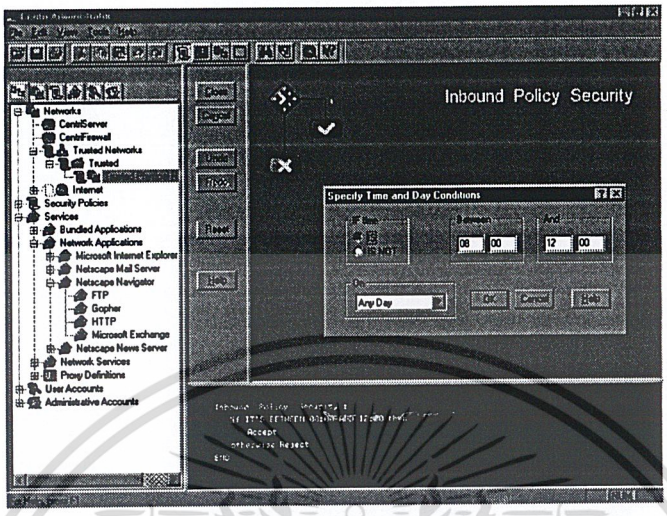
- การกำหนดช่วงเวลาในการใช้บริการ ซึ่งการกำหนดช่วงเวลาของการใช้บริการสามารถที่จะกำหนด Policy ได้ดังรูป 8.7 ถ้าหากผู้ใช้ Login เข้ามาในช่วงเวลาที่อนุญาตให้ใช้แต่ใช้งานเกินเวลาที่กำหนดไว้ จะสามารถใช้บริการต่อไปได้ เรื่อย ๆ จนกว่าจะเลิกใช้บริการ ซึ่งการเข้ามาใช้บริการในครั้งใหม่จะไม่สามารถใช้บริการได้ ในการแก้ไขตรงส่วนนี้ อาจจะไปกำหนดที่ระยะเวลาในการใช้งานของ user แต่ละคนได้ ใน Window NT

จากการทดลอง บริการต่าง ๆ สามารถใช้ได้ในช่วงเวลาที่กำหนดเท่านั้น



รูปที่ 8.6 การกำหนดการใช้บริการได้เฉพาะโฮสท์

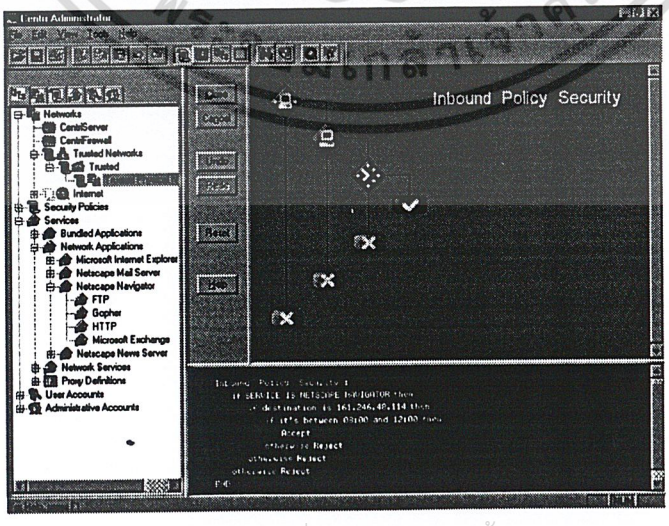
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 8.7 การกำหนดช่วงเวลาในการใช้บริการต่าง ๆ

- การใช้ Policy ต่าง ที่กล่าวมาข้างต้น สามารถนำมาประยุกต์ใช้เขียน Policy ได้หลากหลายรูปแบบขึ้นอยู่กับวัตถุประสงค์ในการใช้งาน

ดังรูปที่ 8.8 เป็นตัวอย่างการประยุกต์ใช้ Inbound Policy ที่ใช้ในการทดลองประกอบด้วยส่วนของการใช้บริการเครือข่ายภายนอก โดย Netscape ซึ่งถูกจำกัดการใช้บริการโดย ไฟร์วอล โดยมีการจำกัดโฮสท์ปลายทางที่สามารถใช้บริการได้และกำหนดช่วงของเวลา



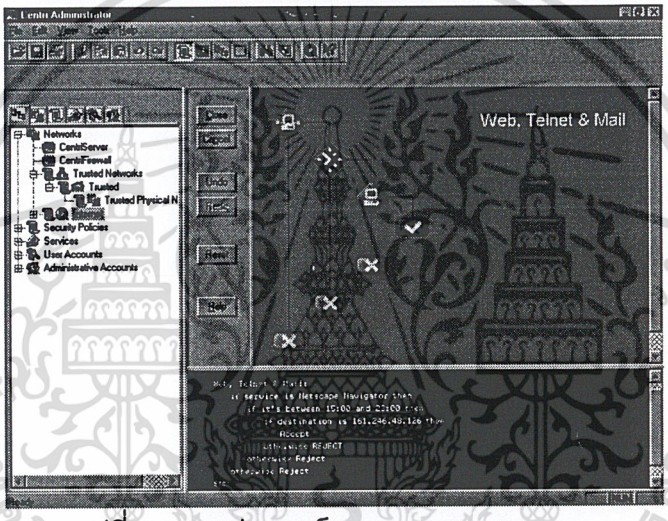
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 8.8 การประยุกต์ใช้ Inbound Policy

จากการทดลอง ใช้บริการตามที่กำหนดใน Policy จะสามารถใช้บริการได้ตามเงื่อนไขที่กำหนด คือจะต้องใช้บริการ Netscape Navigator เรียกใช้บริการไปยังโฮสท์ปลายทางที่กำหนด และในช่วงเวลาที่กำหนดเท่านั้น ในกรณีอื่นๆ นอกเหนือข้อกำหนดนี้จะไม่สามารถใช้งานได้

8.2.2 Outbound Policy

ในส่วนของ Outbound Policy นั้น รูปแบบในการกำหนด Policy จะคล้ายคลึงกับการกำหนด Inbound Policy แต่รูปแบบของการติดต่อจะมีทิศทางที่ตรงกันข้ามกัน กล่าวคือจะเป็นการให้บริการผู้ใช้จากภายนอกเครือข่ายไฟร์วอล เช่น ตัวอย่าง ดังรูป 8.9



รูปที่ 8.9 การประยุกต์ Outbound Policy

จากรูป 8.9 เป็นการประยุกต์ใช้ Outbound Policy ซึ่งมีการกำหนดใช้ Netscape Navigator ช่วงเวลาและกำหนดปลายทางให้กับ Policy ในกรณีที่ ใช้บริการผิดข้อกำหนด ใน Policy ก็จะไม่สามารถที่จะติดต่อกับเครือข่ายไฟร์วอลได้

จากการทดลอง ถ้าการใช้บริการตรงตามเงื่อนไข จึงสามารถที่จะติดต่อเข้าใช้การให้บริการจากเครือข่ายภายในไฟร์วอลได้ แต่ถ้าการเรียกใช้บริการนั้นผิดเงื่อนไขหรือข้อกำหนดก็จะไม่สามารถติดต่อกับเครือข่ายไฟร์วอลได้

8.2.3 HTTP filter

ในการเรียกใช้บริการ Web site โดยทั่วไปนั้นไม่สามารถห้ามการเข้าสู่ Web site ที่ไม่เหมาะสมได้ โดยเฉพาะการบริการอินเตอร์เน็ตในสถาบันการศึกษานั้นควรมีการ ห้ามเข้าไปใน Web site ลามกอนาจารต่างๆได้ ซึ่งใน Cisco Centri Firewall มีเครื่องมือที่ใช้ในการจำกัดการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เข้าใช้บริการ Web site ที่ไม่ต้องการให้ใช้บริการได้โดยใช้ HTTP Filter ทำหน้าที่ในการกรองหรือกัน site ที่ไม่ต้องการให้เข้าใช้บริการสำหรับผู้ใช้ภายในเครือข่ายสามารถที่จะไปยัง Web site ที่ไม่ต้องการให้ไปใช้บริการได้

รูปแบบที่ใช้ในการกำหนด site มีตัวอย่างดังนี้

http://www.ccnet.com/

http://ccnet4.ccnet.com/

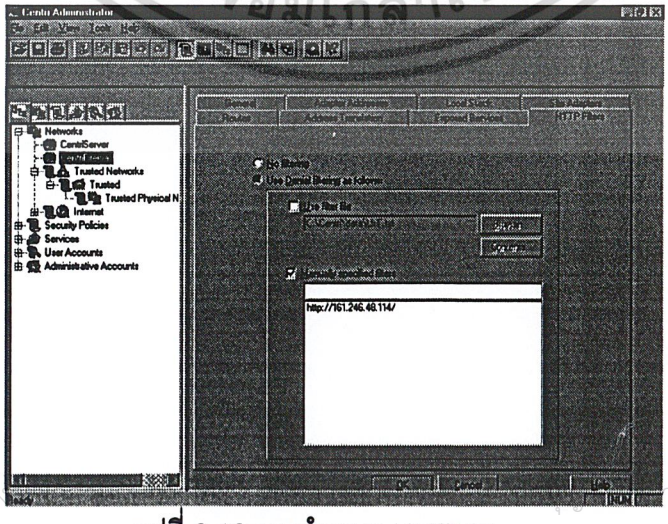
http://192.215.96.9/

ในการกำหนด site จะมีให้กำหนดเป็นแบบ manual และ แบบ use filter file ซึ่งในการทดลองได้เลือกข้อกำหนดเป็นแบบ manual ซึ่งสามารถที่จะใส่ site ที่ต้องการจะกันไม่ให้ ผู้ใช้สามารถติดต่อไปได้ทันที

ในการกำหนด site นอกจากจะกำหนดเป็นแบบข้างต้นแล้ว ยังสามารถที่จะกำหนดโดยใช้ wildcard เช่น * ได้อีกด้วย หรือสามารถจะกำหนดเป็นคำ ๆ ก็ได้เช่นกัน เช่น *sex*

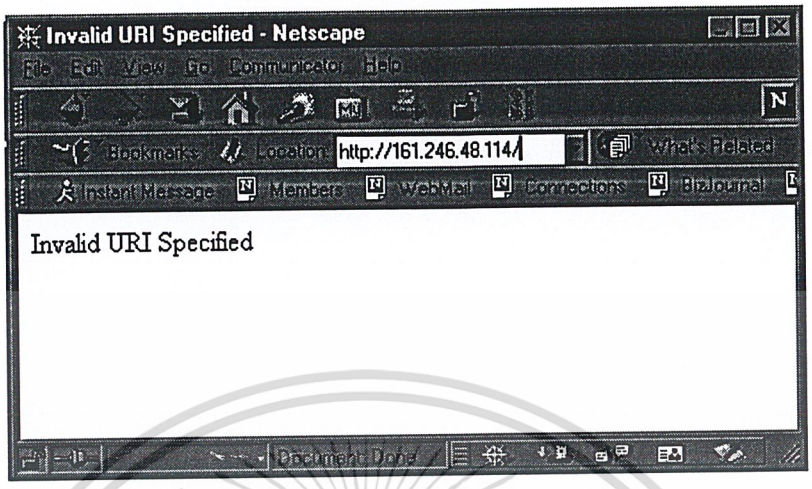
ในการทำลองจะกำหนดเป็นแบบ manual โดยใส่ค่า IP address ลงไป ดังรูปที่ 8.1 โดยที่การกำหนดดังกล่าวนั้นเป็นการกำหนดไม่ให้เข้าใช้บริการ โดยใช้การกำหนดการกรอง Web site ด้วย HTTP Filter

จากการทดลองสรุปว่า Web site ที่ถูกกำหนดการห้ามไปใช้บริการโดย HTTP filter นั้น Netscape web browser ไม่สามารถจะติดต่อด้วยได้ซึ่งที่ Browser จะแสดงหน้าจอดังรูปที่ 8.11 แต่สำหรับ site ที่ไม่ได้ระบุไว้ จะสามารถที่จะติดต่อกับ site นั้น ได้ ตรงตามข้อกำหนดทุกประการ



รูปที่ 8.10 การกำหนด HTTP filter

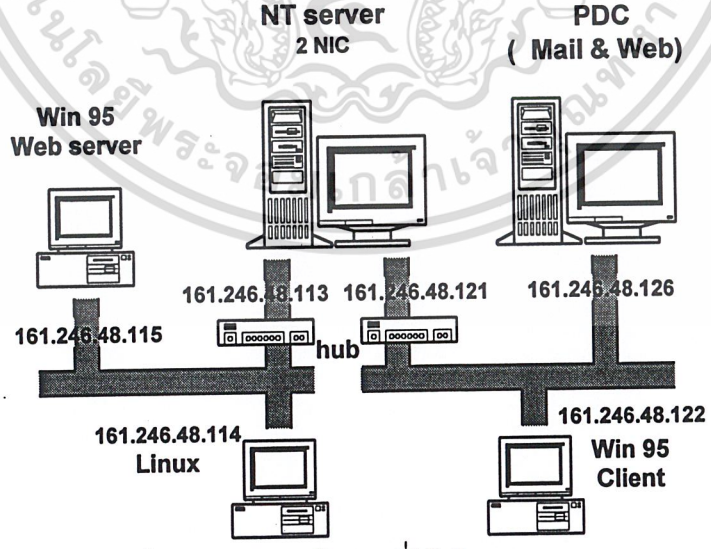
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 8.11 การปฏิเสธการให้บริการโดย HTTP Filter

8.2.4 telnet

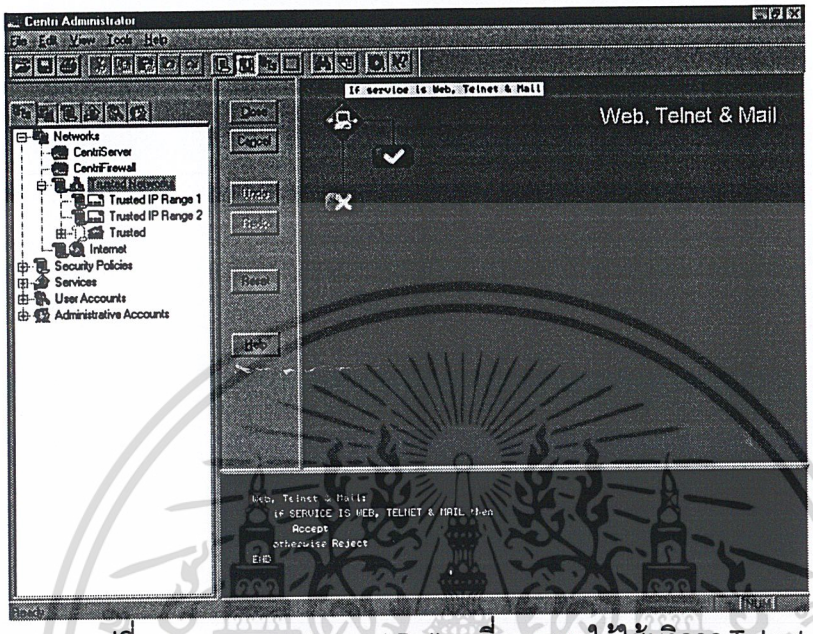
เพื่อความสะดวกและง่ายต่อการตรวจสอบและใช้งาน Telnet จะใช้ Linux ในการให้บริการ telnet ซึ่งได้ติดตั้ง Linux (Redhad 5.2) ที่เครื่องคอมพิวเตอร์ที่มี IP address 161.246.48.114 โดยจะเป็นการติดต่อขอใช้บริการ Telnet จากเครื่องคอมพิวเตอร์ ที่อยู่หลังไฟร์วอลไปยังเครือข่ายภายนอกไฟร์วอล (Inbound Policy) ดังรูปที่ 8.12



รูปที่ 8.12 ระบบเครือข่ายที่ให้บริการ Telnet

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

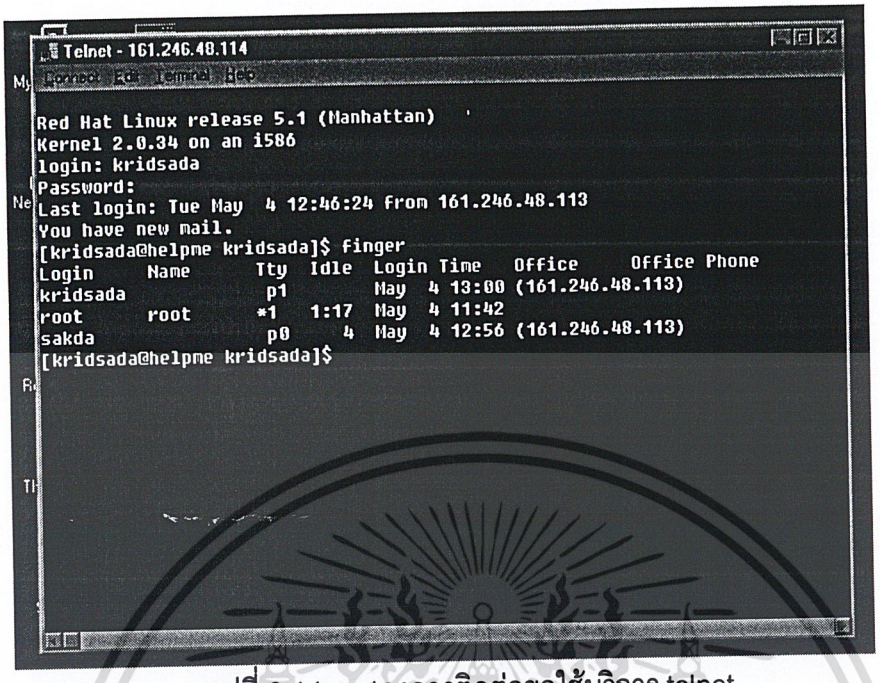
ก่อนการทดสอบจะต้องกำหนด Inbound Policy ให้กับ Cisco Centri Firewall ให้สามารถใช้บริการ telnet ติดต่อออกไปยังภายนอกไฟร์วอลได้ ดังรูปที่ 8.13



รูปที่ 8.13 แสดง Inbound Policy ที่อนุญาตให้ใช้บริการ Telnet

เริ่มการทดสอบโดย ใช้เครื่อง IP address 161.246.48.122 โดย Telnet ไปที่ IP address 161.246.48..114 (Telnet 161.246.48.114) ซึ่งปรากฏว่าสามารถติดต่อและใช้บริการ telnet ได้ เมื่อใช้คำสั่ง finger จะปรากฏรายละเอียดของผู้ใช้บริการดังกล่าว ซึ่งจุดที่น่าสนใจ คือ IP address ของเครื่องที่ติดต่อขอบริการ telnet จะถูกแสดงเป็น 161.246.48.113 ที่เป็นเช่นนี้เพราะไฟร์วอลทำหน้าที่ในการป้องกันการมองเห็น IP address จริงของเครื่องหลังไฟร์วอล โดยการที่ได้กำหนดให้ IP address 161.246.48.113 เป็น Expose address เพราะฉะนั้นทุกเครื่องที่อยู่หลัง ไฟร์วอลที่เมื่อมีการขอใช้บริการ telnet ออกไปนอกเครือข่ายไฟร์วอลจะถูกแทนที่ IP address ด้วย 161.246.48.113 ซึ่งเป็น Expose IP ทั้งหมด ดังรูปที่ 8.14

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



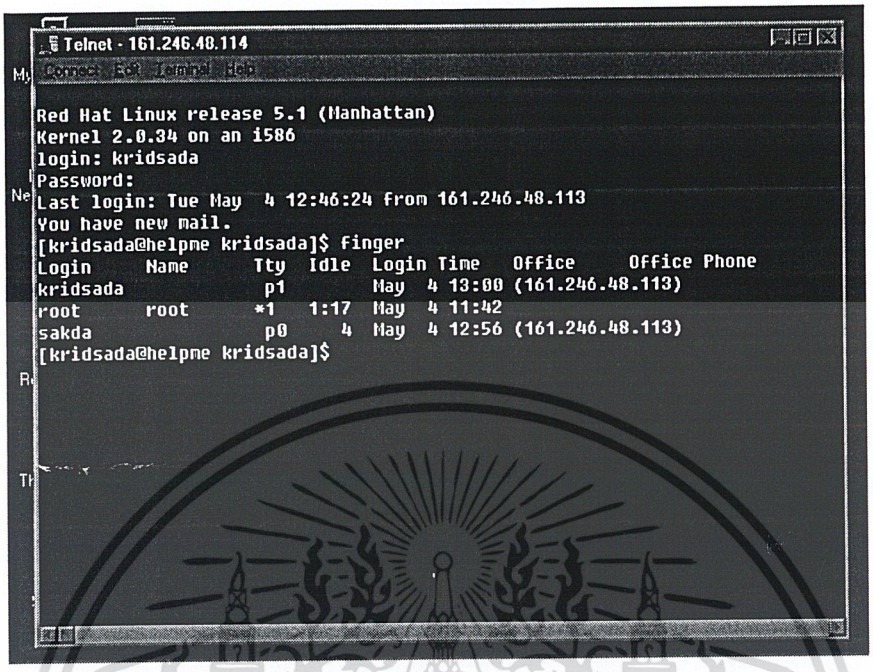
รูปที่ 8.14 แสดงการติดต่อขอใช้บริการ telnet

การทดสอบต่อมาคือ การจำกัด IP address โดยกำหนด IP address เป็น 2 ช่วง คือ ช่วง 161.246.48.121 – 161.246.48.123 และช่วง 161.246.48.124 – 161.246.48.127 ดังรูปที่ 8.17

เพื่อจำกัด IP address ที่จะใช้บริการ telnet โดยกำหนดให้เครื่องคอมพิวเตอร์ ที่อยู่หลังไฟร์วอลมี IP address เป็น 161.246.48.122 และ 161.246.48.124 เป็นเครื่องที่ติดต่อบริการ telnet ทดสอบเป็นเงื่อนไขต่าง ๆ คือ

- IP address ทั้ง 2 ช่วง สามารถติดต่อใช้บริการ telnet ได้โดยจะต้องกำหนดที่ Policy ของ Cisco Centri firewall ให้สามารถใช้บริการ telnet ได้ด้วย ผลการทดสอบคือ เครื่องคอมพิวเตอร์ ทั้งสองเครื่อง สามารถติดต่อใช้บริการ telnet ได้ ดังรูปที่ 8.15

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



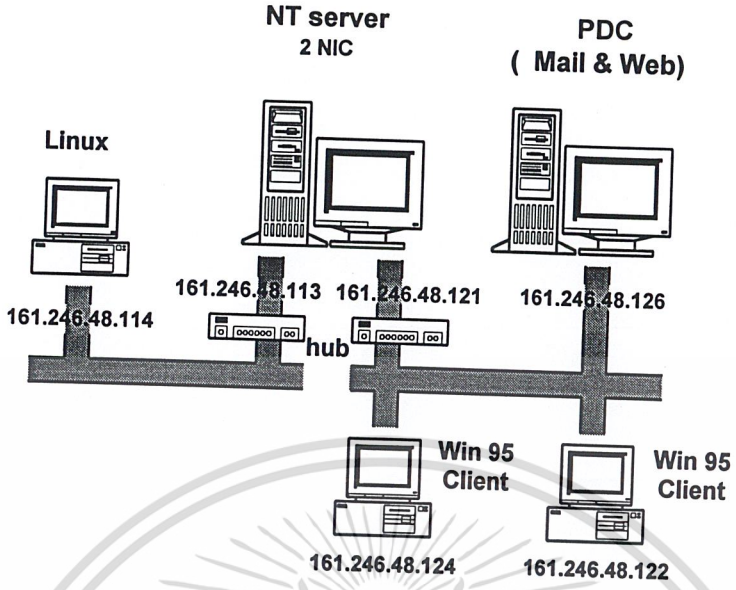
รูปที่ 8.15 แสดงการติดต่อในช่วงที่ใช้บริการทั้งสองช่วง

- ให้ IP address ในช่วง 161.246.48.121 – 161.246.48.123 ใช้ได้แค่ช่วงเดียวเท่านั้น ซึ่งจะต้องกำหนด Policy ให้ใช้บริการแค่ช่วงนี้ช่วงเดียว จากการทดลอง ให้เครื่องคอมพิวเตอร์ทั้งสองเครื่องที่อยู่หลังไฟร์วอลล์ติดต่อบริการ telnet ปรากฏว่าสามารถใช้บริการได้แค่เครื่องเดียวคือเครื่อง IP address 161.246.48.122 ซึ่งพอจะสรุป ได้ว่า เครื่องคอมพิวเตอร์อื่น ๆ ที่อยู่ในช่วง IP address ที่กำหนด จะสามารถใช้บริการได้ ส่วนเครื่องที่ IP address 161.246.48.124 ไม่สามารถใช้บริการ telnet ได้ ดังรูปที่ 8.16



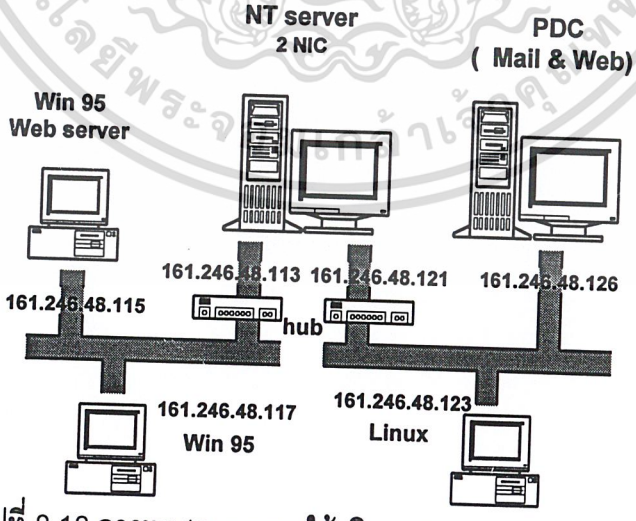
รูปที่ 8.16 แสดงการปฏิเสธการใช้บริการ telnet

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 8.17 การแบ่งเครือข่ายภายในออกเป็นสองช่วง

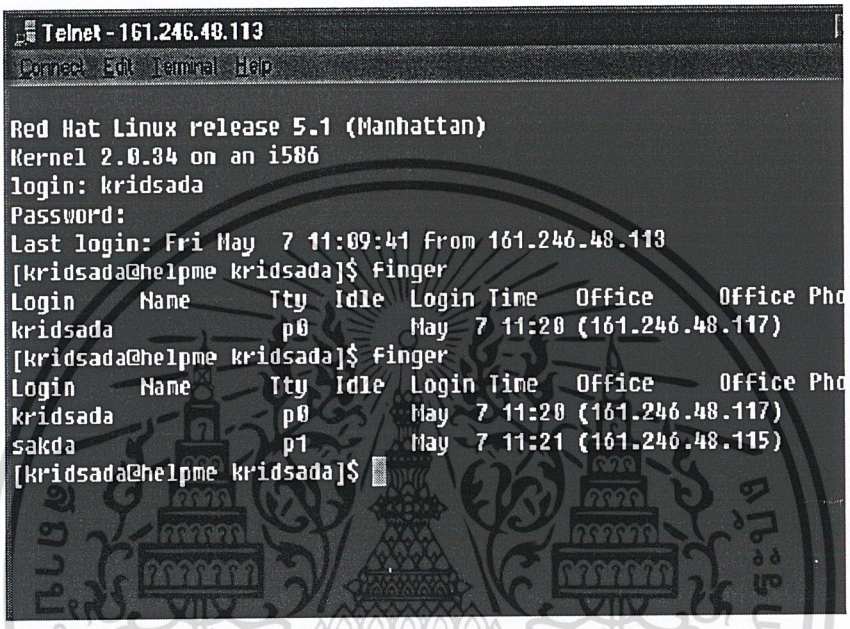
การทดสอบต่อมา คือ ย้ายเครื่องคอมพิวเตอร์ที่มีระบบปฏิบัติการเป็น Linux ไปอยู่หลังไฟร์วอล โดยกำหนด IP address เป็น 161.246.48.123 และทดสอบการ Telnet จากเครื่องคอมพิวเตอร์ที่อยู่นอกไฟร์วอล ติดต่อเข้ามาภายไฟร์วอลและย้ายเครื่องคอมพิวเตอร์ที่อยู่ภายในไฟร์วอลมาติดตั้งภายนอกไฟร์วอลโดยให้มี IP address เป็น 161.246.48.115 และ 161.246.48.117 เพื่อ สะดวกในการใช้ในการทดสอบ ดังรูปที่ 8.18



รูปที่ 8.18 การทดสอบการขอใช้บริการ Telnet จากภายนอก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การทดสอบจะคล้ายกับข้างต้นโดยใช้เครื่องทั้งสองที่อยู่ภายนอกไฟร์วอลติดต่อบริการ telnet เข้ามาที่เครื่อง Linux โดยเรียก telnet 161.246.48.113 ผลการทดลองคือ เครื่องคอมพิวเตอร์ทั้งสองสามารถจะใช้บริการ telnet ได้ และ IP address ที่มองเห็น คือ IP address ของเครื่องที่ทดสอบ ดังรูปที่ 8.19



รูปที่ 8.19 แสดงการติดต่อใช้บริการ telnet จากภายนอกไฟร์วอล

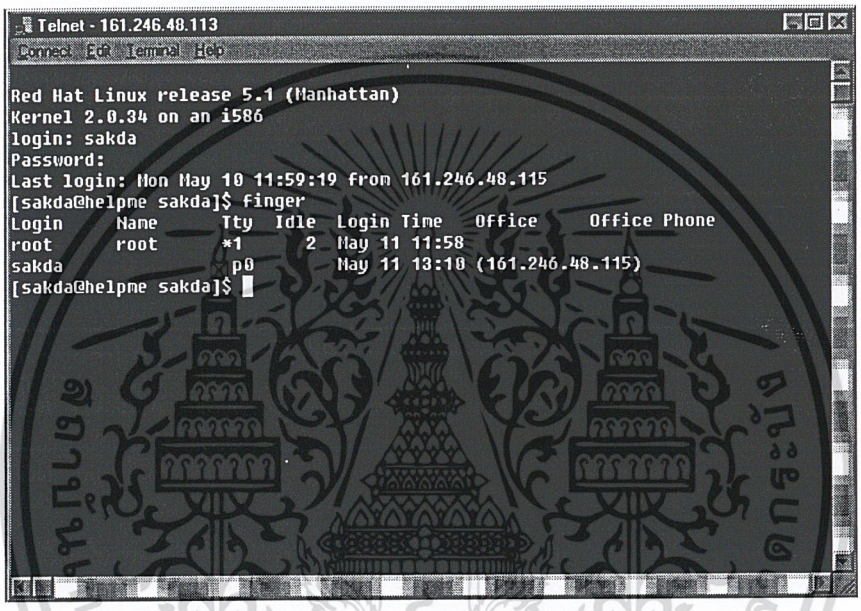
การทดสอบต่อมาคือ จำกัด IP address ในการติดต่อใช้บริการ telnet โดยการกำหนด IP address เป็น 2 ช่วง คือ

ช่วง 161.246.48.48.113 – 161.246.48.115 และช่วง 161.246.48.116 – 161.246.48.119 โดยกำหนด Policy ที่ Cisco Centri Firewall ให้ IP address ทั้งสองช่วงสามารถใช้บริการ telnet ได้ และทดสอบโดยให้เครื่องคอมพิวเตอร์ทั้งสองเครื่องติดต่อใช้บริการ telnet ได้ ปรากฏว่า สามารถใช้บริการ telnet ได้ โดยดูจากคำสั่ง finger ดังรูปที่ 8.20

ต่อมากำหนด Policy ที่ Cisco Centri Firewall ให้สามารถติดต่อบริการ telnet ได้แค่ช่วง IP address ที่กำหนด คือ ช่วง 161.246.48.113 – 161.246.48.115 ให้สามารถใช้บริการ telnet ได้ เท่านั้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ผลการทดลอง คือ สามารถที่จะติดต่อได้แค่เครื่องคอมพิวเตอร์ ที่ IP address 161.246.48.115 เท่านั้น แต่เครื่องที่มี IP address 161.246.48.117 ไม่สามารถติดต่อบริการ telnet ได้ โดยดูจากการใช้คำสั่ง finger สรุปได้ว่า เครื่องคอมพิวเตอร์ที่มี IP address ใน ช่วงที่กำหนดคือ 161.246.48.113 – 161.246.48.115 สามารถที่จะใช้บริการ telnet ได้ แต่นอกเหนือจาก ช่วง IP address ที่กำหนดจะไม่สามารถใช้บริการ telnet ได้



รูปที่ 8.20 แสดงการติดต่อใช้บริการจากภายนอก

8.3 report และ log

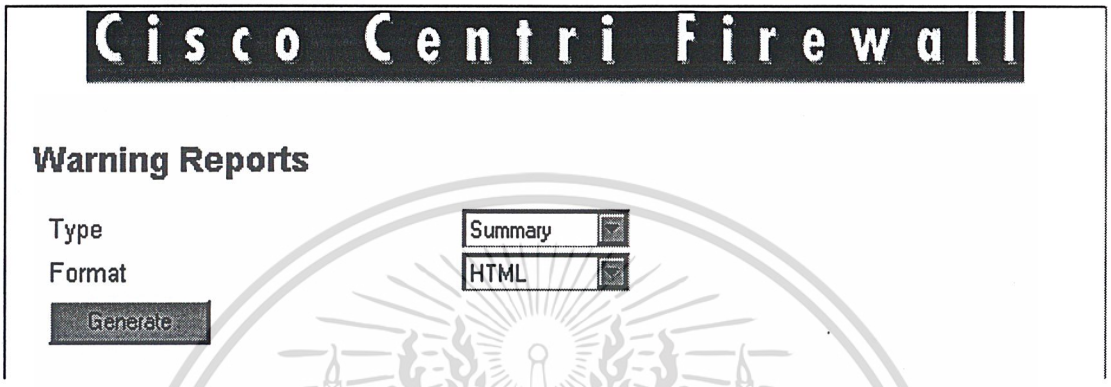
report เป็นการรายงานสิ่งที่เกิดขึ้น กับบริการต่าง ๆ ที่เกี่ยวข้องกับผู้ใช้บริการ รวมถึงสิ่งที่เกิดขึ้นที่มีแนวโน้มว่า จะเป็นอันตราย กับระบบ ซึ่งขั้นตอนการติดตั้งได้กล่าวในบทข้างต้น ในส่วนของรายงานจะประกอบด้วย 3 ส่วน คือ

- Warning report
- Service report
- Open session

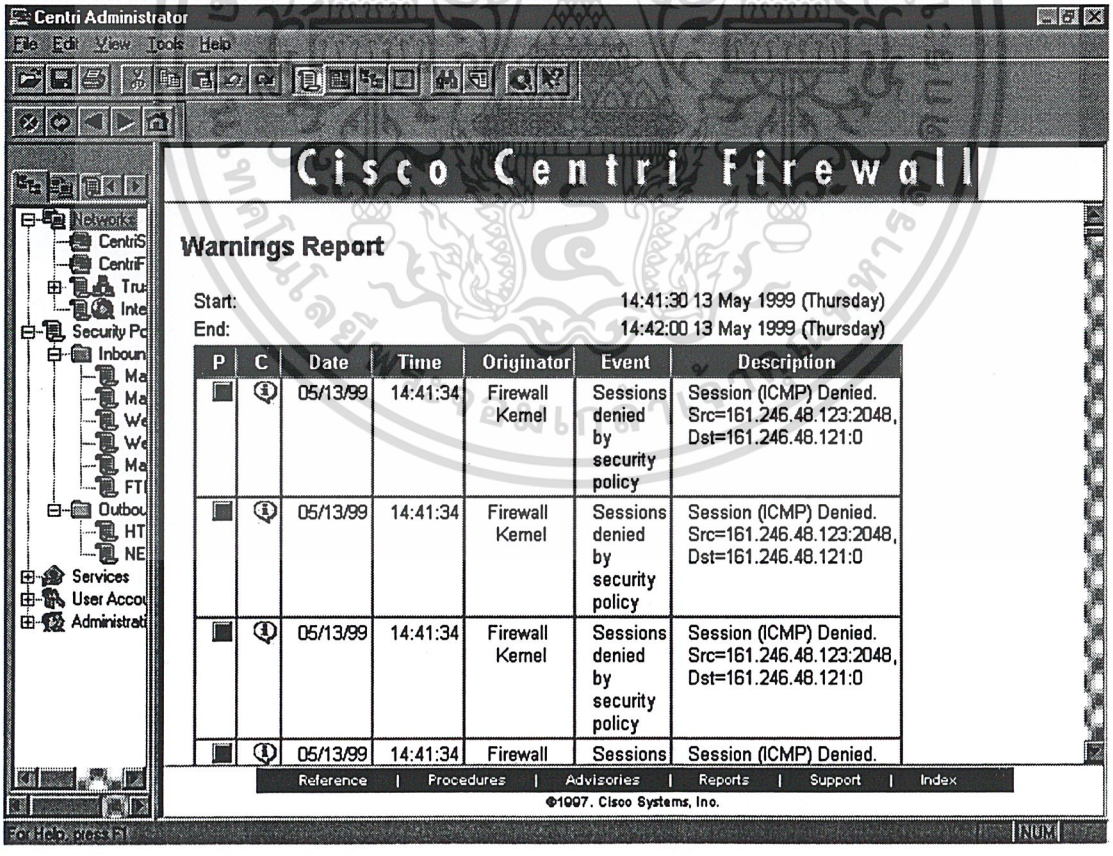
Warning report เป็นการรายงานสิ่งต่าง ๆ ที่เกิดขึ้นกับ Cisco Centri Firewall ซึ่งสามารถที่จะเลือกให้รายงานเป็น Summary หรือ detail และ รูปแบบเป็น HTML หรือ Text

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Service report เป็นการรายงานการใช้บริการต่าง ๆที่เกิดขึ้นบน Cisco Centri Firewall ซึ่งสามารถที่จะเลือกให้รายงานเป็น Summary หรือ Detail เลือกบริการที่สนใจและรูปแบบในการรายงานว่า เป็น HTML หรือ Text

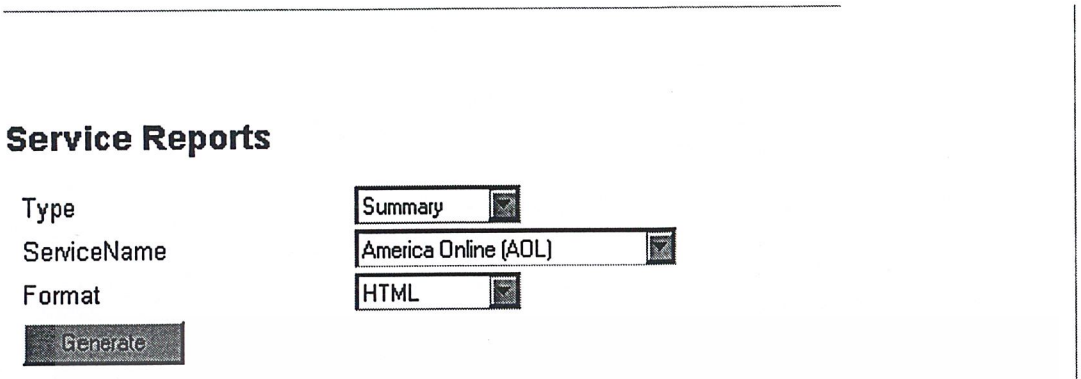


รูปที่ 8.21 Warning Report



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

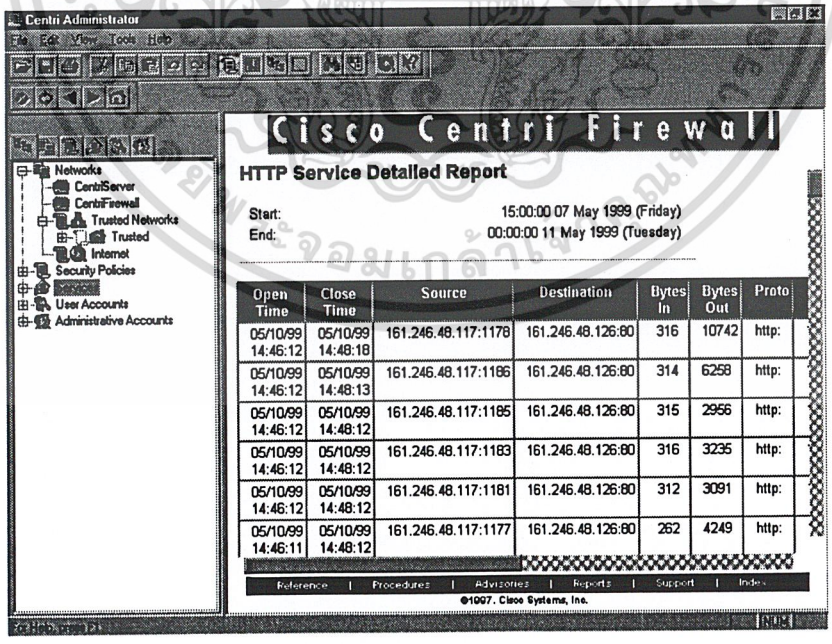
รูปที่ 8.22 แสดงรายละเอียดของ Warning Report



รูปที่ 8.23 Service report

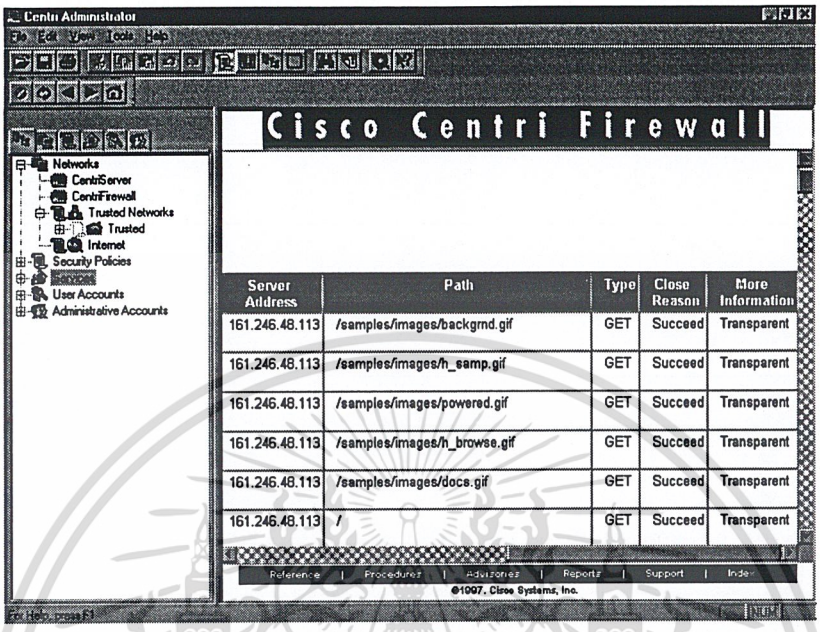
ในการรายงานบริการต่าง ๆ จะสามารถกำหนดระยะเวลาได้ โดย Firewall ได้กำหนดตัวเลือกขึ้นอยู่กับความต้องการของผู้ดูแลระบบว่าต้องการจะดูรายงานในช่วงเวลาใด

ซึ่งในแต่ละบริการรายละเอียดข้อมูลต่างๆ ในการรายงานก็จะแตกต่างขึ้นอยู่กับบริการนั้น ๆ เช่น บริการ HTTP ก็จะมีรายละเอียดของรายงานดังรูปที่ 8.24 และ 8.25 ซึ่งไม่สามารถแสดงได้ภายในรูปเดียว



รูป 8.24 รายละเอียดของ HTTP Report

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 8.25 รายละเอียดของ HTTP Report (ต่อ)

จากรูปที่ 8.24 และ 8.25 จะแสดงรายละเอียดการรายงานของบริการ HTTP ซึ่งมีรายละเอียดต่าง ๆ ในการรายงาน คือ

Open time คือ เวลาเริ่มต้นในการใช้บริการ

Close time คือ เวลาที่เลิกใช้บริการ

Source คือ เครื่องคอมพิวเตอร์ต้นทางที่ใช้บริการและหมายเลขพอร์ต

Destination คือ เครื่องคอมพิวเตอร์ปลายทางที่ติดต่อใช้บริการและหมายเลขพอร์ต

Bytes In คือ จำนวนข้อมูลที่มีการส่งผ่านเข้ามายังไฟร์วอล

Bytes Out คือ จำนวนข้อมูลที่มีการส่งออกไปยังเครื่องปลายทางผ่านไฟร์วอล

Proto คือ โปรโตคอลที่ใช้ เช่นในรายงาน คือ http:

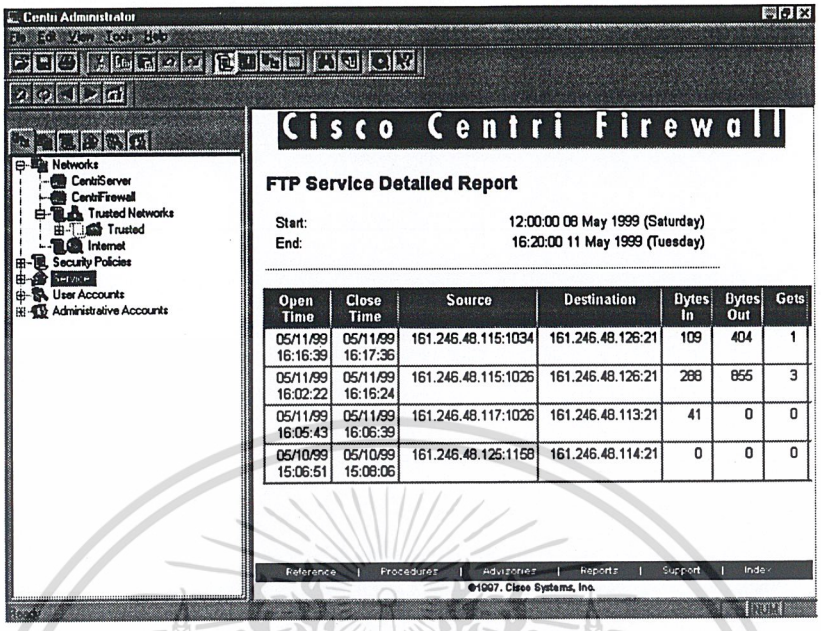
Server address คือ หมายเลข IP address ของเครื่อง Server ที่มีการติดต่อใช้บริการ

Path คือ หน้าต่างของ web page ต่างๆ ที่มีการติดต่อใช้บริการ

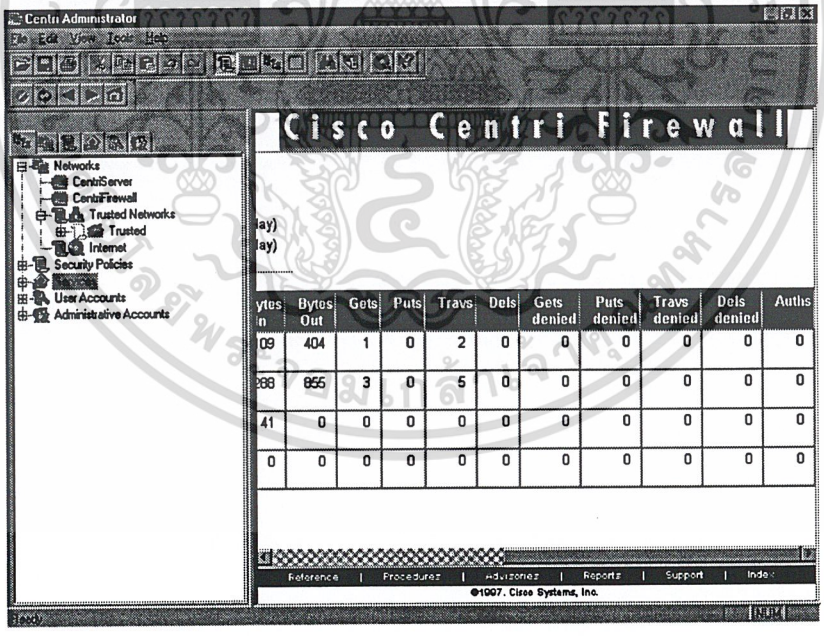
รวมถึง type , Close Reason และ More Information

บริการ FTP มีรายละเอียด ดังรูปที่ 8.26 และ 8.27

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 8.26 รายละเอียดของ FTP Report



รูปที่ 8.27 รายละเอียดของ FTP Report (ต่อ)

จากรูปที่ 8.26 และ 8.27 ในส่วนของบริการ FTP Report จะมีรายละเอียดต่างๆ ในการรายงานแก่ผู้แล ระบบ ซึ่งมีรายละเอียดต่าง ๆ คือ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Open time คือ เวลาเริ่มต้นในการใช้บริการ

Close time คือ เวลาที่เลิกใช้บริการ

Source คือ เครื่องคอมพิวเตอร์ที่ใช้บริการและหมายเลขพอร์ต

Destination คือ เครื่องคอมพิวเตอร์ปลายทางที่ติดต่อใช้บริการและหมายเลขพอร์ต

Bytes In คือ จำนวนข้อมูลที่มีการส่งผ่านเข้ามาที่ไฟร์วอล

Bytes Out คือ จำนวนข้อมูลที่มีการส่งออกไปจากตัวไฟร์วอล

Get คือ จำนวนไฟล์ข้อมูลที่มีการขอคัดลอกจากเครื่องคอมพิวเตอร์ปลายทาง

Put คือ จำนวนไฟล์ข้อมูลที่มีการส่งออกไปยังเครื่องคอมพิวเตอร์ที่ปลายทาง

Dels คือ การลบไฟล์ข้อมูล

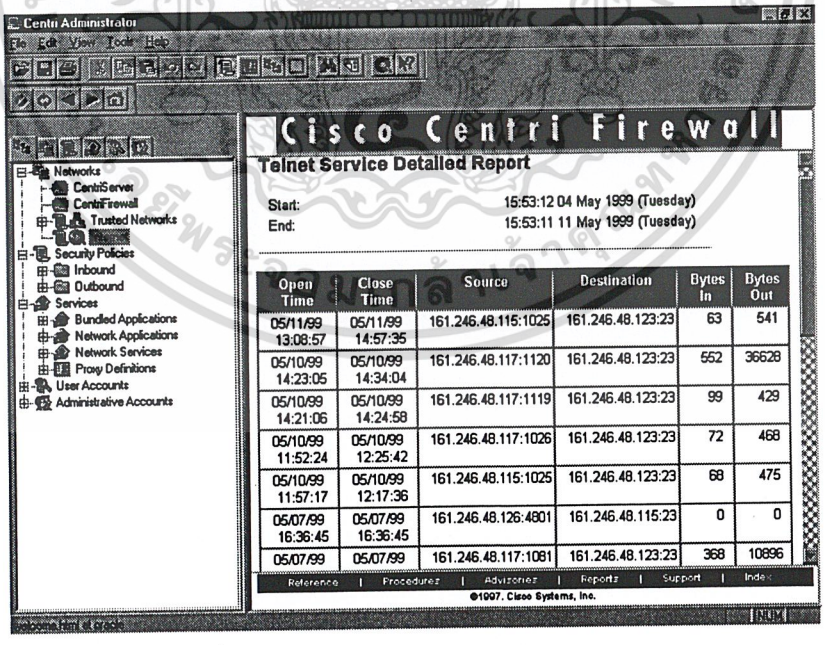
Gets denied คือ การปฏิเสธการใช้คำสั่ง Get

Put denied คือ การปฏิเสธการใช้คำสั่ง Put

Del denied คือ การปฏิเสธการลบไฟล์ข้อมูล

รวมถึง Travs และ Auths

บริการ telnet มีรายละเอียด ดังรูปที่ 8.28



รูปที่ 8.28 รายละเอียดของ Telnet Report

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 8.28 จะแสดงรายละเอียดในการรายงานต่าง ๆ ของบริการ telnet ซึ่งมีรายละเอียดดังนี้ คือ

Open time คือ เวลาที่เริ่มต้นในการใช้บริการ

Close time คือ เวลาที่เลิกใช้บริการ

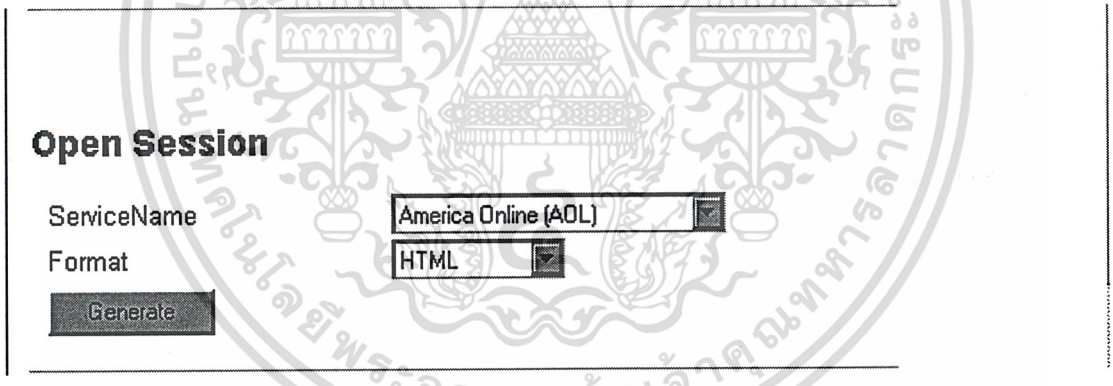
Source คือ เครื่องคอมพิวเตอร์ต้นทางที่ใช้บริการและหมายเลขพอร์ต

Destination คือ เครื่องคอมพิวเตอร์ปลายทางที่ติดต่อใช้บริการและหมายเลขพอร์ต

Bytes In คือ จำนวนของข้อมูลที่มีการส่งเข้ามายังไฟร์วอลจากเครื่องปลายทาง

Bytes Out คือ จำนวนของข้อมูลที่มีการส่งออกจากไฟร์วอลไปยังเครื่องปลายทาง

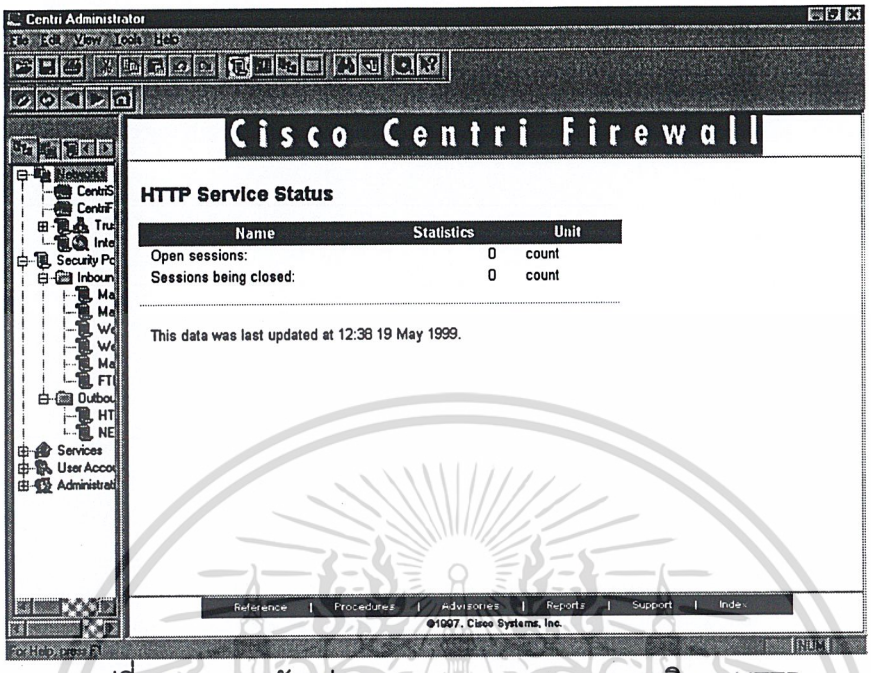
Open Session เป็นการรายงานในส่วนของบริการที่ทำงานอยู่ในขณะนั้น ซึ่งสามารถกำหนดให้รายงานในรูปแบบของ HTML หรือ Text โดยเลือกบริการที่ต้องการให้ Firewall แสดงผลออกมา



รูปที่ 8.29 Open Session

ในการรายงานในส่วนของ open session สามารถจะเลือกให้แสดงบริการต่าง ๆได้ขึ้นอยู่กับว่าจะให้ตัวโปรแกรมแสดงบริการใดตามบริการที่ Cisco Centri Firwall มีให้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 8.30 แสดงตัวอย่างของ open sessions ของบริการ HTTP

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 9
สรุปผลการทดลอง

จุดมุ่งหมายหลักของการใช้งาน โปรแกรมไฟร์วอลนั้น คือ เพื่อเพิ่มความสามารถในการรักษาความปลอดภัยของระบบเครือข่าย ที่มีการเชื่อมต่อและ ให้บริการกับเครือข่ายภายนอก เนื่องจากระบบรักษาความปลอดภัยของวินโดวส์เอ็นทีนั้น เป็นการรักษาความปลอดภัยเฉพาะส่วนที่เกี่ยวกับผู้ใช้ภายในที่มีสิทธิ์ในระบบเครือข่าย ซึ่งไม่รวมถึงกรณีของการติดต่อให้บริการกับระบบเครือข่ายภายนอก ซึ่งวินโดวส์เอ็นทีเองมีระบบรักษาความปลอดภัยของการให้บริการดังกล่าวค่อนข้างจำกัด ซึ่งตัวโปรแกรมไฟร์วอลเองนั้นมีมากมายหลายชนิดและ หลายผู้ผลิตในการเลือกใช้ไฟร์วอลชนิดใดนั้นจะต้องพิจารณาถึงวัตถุประสงค์ในการใช้งานภายในระบบเครือข่ายที่เกิดขึ้นด้วย

9.1 แนวทางในการประยุกต์ใช้งาน

Cisco Centri Firewall ที่ทำการทดลองนั้น มีคุณสมบัติในการรักษาความปลอดภัยค่อนข้างครบถ้วนสมบูรณ์ จึงสามารถนำไปประยุกต์ใช้กับระบบเครือข่ายของภาควิชา หรือนำไปใช้กับเครือข่ายอื่น ๆ ได้ แต่อย่างไรก็ตามโปรแกรมตัวที่ทดลองใช้นั้นเป็น Evaluation version ซึ่งหลังจากลงโปรแกรมไปแล้วจะสามารถใช้งานได้เพียง 30 วัน หากใช้ตัวโปรแกรมจริงที่ลิขสิทธิ์ถูกต้องจะได้โปรแกรมที่สมบูรณ์

9.2 ปัญหาและวิธีการแก้ไข

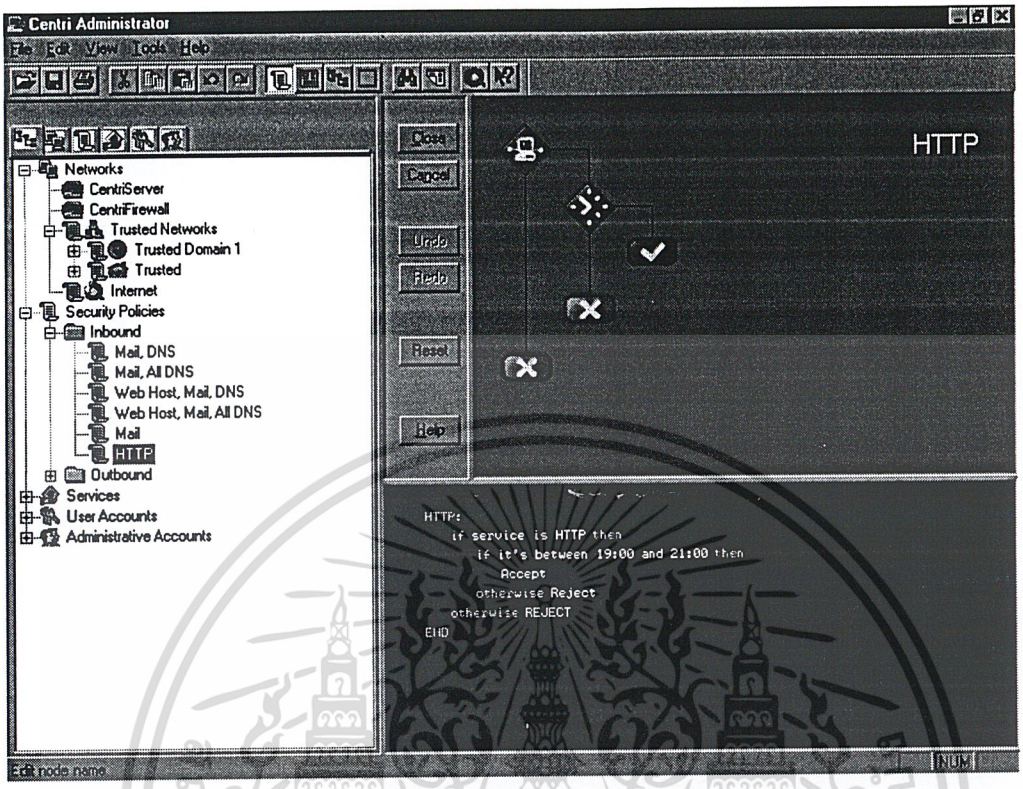
ปัญหาที่เกิดขึ้นจากการทดลองโปรแกรมไฟร์วองนั้นสามารถแบ่งออกเป็นส่วน ๆ ได้ดังนี้

- ปัญหาในการติดตั้งโปรแกรมในครั้งแรก

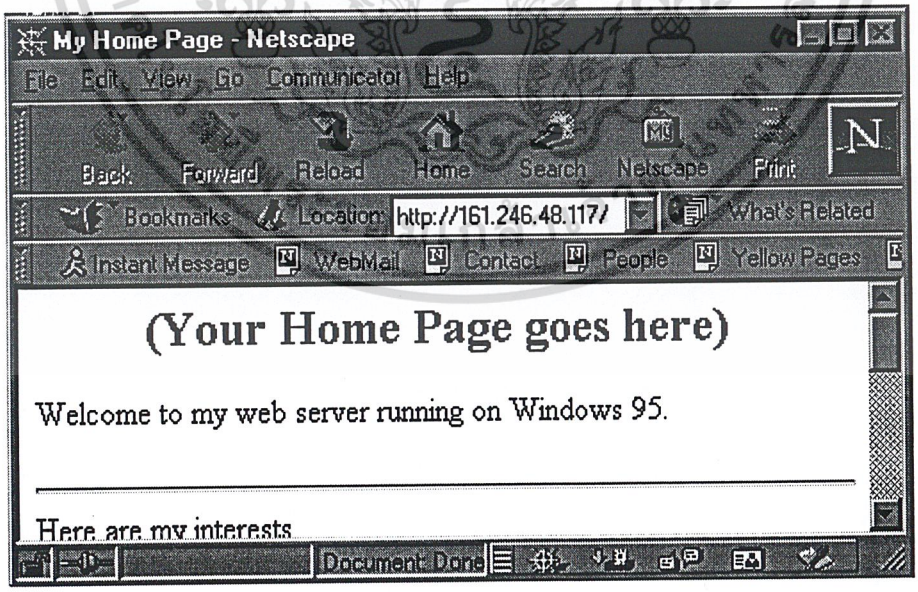
ในการติดตั้ง Cisco Centri Firewall นั้น เกิดปัญหาขึ้น คือ ลงโปรแกรมแล้วไม่สามารถใช้งานโปรแกรมไฟร์วอลได้โดยเกิดจาก การกำหนดคุณสมบัติของเครื่องที่ใช้ในการติดตั้ง Firewall ไม่ถูกต้องตามที่โปรแกรมต้องการ ซึ่งสามารถแก้ไขได้ โดยจัดการเครื่องที่ต้องการจะติดตั้ง ไฟร์วอลให้ตรงตามข้อกำหนดต่าง ๆ ในคู่มือการติดตั้ง

- ปัญหาในส่วนของการแก้ไขข้อกำหนดของไฟร์วอล เครื่อง client ที่กำลังใช้งานอยู่ในระบบเครือข่ายจะไม่สามารถใช้ข้อกำหนดใหม่ได้ทันที จะต้องมีการล็อกอินเข้าระบบใหม่อีกครั้งจึงจะสามารถใช้ข้อกำหนดเหล่านั้นได้ เช่น ได้ทดลองกำหนด Policy ดังรูปที่ 9.1 โดยให้สามารถให้บริการ HTTP ในช่วงเวลาที่กำหนด คือ เวลา 19.00-21.00 น. ได้เท่านั้น

เอกสารนี้มีลิขสิทธิ์ ห้ามนำไปใช้ในการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น เว้นแต่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



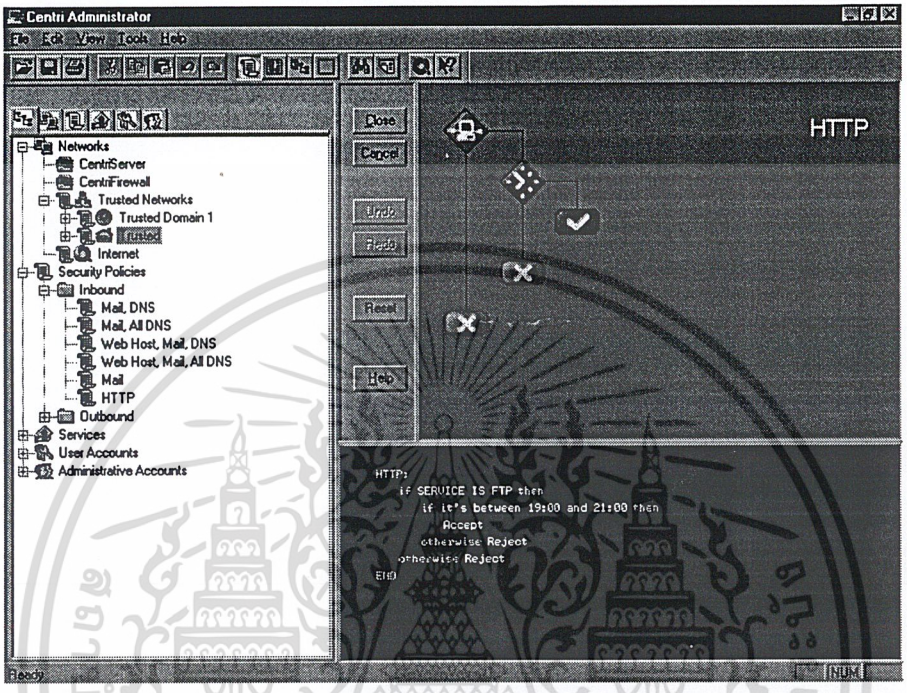
รูปที่ 9.1 แสดงการกำหนด Policy ให้บริการ HTTP



รูปที่ 9.2 ทดลองการใช้บริการ HTTP

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 9.2 จะเห็นว่าสามารถใช้บริการ HTTP ได้ ตรงตาม Policy ที่กำหนด หลังจากนั้นได้เปลี่ยน Policy ใหม่เป็น ให้บริการ FTP ในช่วงเวลาที่ กำหนด คือ 19.00 - 21.00 น.แทน Policy เดิม ดังรูปที่ 9.3



รูปที่ 9.3 แสดงการให้บริการ FTP

ในขณะที่เครื่องที่ใช้ทดลองเป็นเครื่องคอมพิวเตอร์เครื่องเดียวกันและไม่ได้ทำการ login เข้ามาใหม่ ได้ทดลองใช้บริการ FTP ปรากฏว่า ไม่สามารถให้บริการได้ ซึ่งจะต้อง login เครื่องใหม่จึงจะสามารถให้บริการ FTP ได้ ดังรูปที่ 9.4

- ข้อเสียอีกข้อหนึ่งคือการไม่สามารถที่จะกำหนดเวลาในการใช้บริการได้ เช่น ต้องการให้ใช้บริการได้แค่ 2 ชั่วโมงเท่านั้นหลังจากมีการ login เข้ามาซึ่งไม่สามารถที่จะทำได้ แต่จะทำได้ในส่วนที่กำหนดช่วงเวลาในการ login เข้ามา เช่น login เข้ามาได้ในช่วงเวลา 8.00-12.00 น.จึงจะเข้ามาใช้บริการได้
- การไม่ได้ต่อกับระบบ Internet จริง

การใช้ระบบเครือข่ายจำลองอิสระนั้นบางครั้งทำให้สภาพแวดล้อมในการทดลอง ใช้งานไฟร์วอลไม่เหมือนกับเครือข่าย Internet ได้เต็ม 100 เปอร์เซ็นต์ทำให้ได้เพียงใกล้เคียงเท่านั้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 9.4 แสดงการปฏิเสธการใช้บริการ FTP

9.3 แนวทางในการพัฒนาขั้นต่อไป

เนื่องจากในการทดลองนี้เป็นการใช้ระบบเครือข่ายจำลองในการศึกษาการใช้งานโปรแกรม ดังนั้นในการพัฒนาขั้นต่อไปนั้นสามารถที่จะทดลอง ในการเชื่อมต่อระบบ Internet จริง เพื่อทำการศึกษาผลการทดลองจากระบบเครือข่ายจริง เพื่อประยุกต์รูปแบบในการใช้งาน โปรแกรมไฟร์วอลให้รัดกุมและมีความปลอดภัยที่สูงขึ้นไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บรรณานุกรม

1. โชคชัย เตชพรรุ่ง. คู่มือการใช้งาน Microsoft windowsNT server 40 .กรุงเทพมหานคร : ซีเอ็ดยูเคชั่นจำกัด(มหาชน), 2540
2. อรรณพ ขันธิกุลและคณะ. WindowsNT 4.0 Server&Workstationสำหรับผู้บริหารระบบ . พิมพ์ครั้งที่ 2 .กรุงเทพมหานคร : ดวงกมลสมัย .
3. บัณฑิต จามรภูติ. การวางระบบเน็ตเวิร์กด้วย Windows NT Server 4.0 . กรุงเทพมหานคร : ว.เพ็ชรสกุลจำกัด,2541.
3. Chapman,D. Brent .and Zwicky,Elizabeth D. Building Internet Firewall . USA : O'Reilly & Associates,1915
4. Cisco Centri Firewall Installation Guide
5. Securing Your Network with the Cisco Centri Firewall

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหาและต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้