การประยุกต์และเปรียบเทียบระบบไฟร์วอลสำหรับเครือข่าย

TCP/IP Firewall System Implementation and Comparison

โดย

นายโกศล ถิรจิตโต รหัส 39014045

นายจรัญ เจียมทวีบุญ รหัส 39014067

อาจารย์ที่ปรึกษา

อาจารย์ ธนา หงษ์สุวรรณ

อาจารย์ อัครเดช วัชระภูพงษ์

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2542

ปริญญานิพนธ์ปีการศึกษา 2542

ภาควิชา วิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง การประยุกต์และเปรียบเทียบระบบไฟร์วอลสำหรับเครือข่าย

TCP/IP Firewall System Implementation and Comparison

ผู้จัดทำ

1. นายโกศล ถิรจิตโต รหัสประจำตัว 39014045
2. นาย จรัญ เจียมทวีบุญ รหัสประจำตัว 39014067

อาจารย์ที่ปรึกษา

(อาจารย์ ธนา หงษ์สุวรรณ)

อาจารย์ที่ปรึกษา

(อาจารย์ อัครเดช วัชระภูพงษ์)

การประยุกต์และเปรียบเทียบระบบไฟร์วอลสำหรับเครือข่าย

นายโกศล ถิรจิตโต 39014045
นาย จรัญ เจียมทวีบุญ 39014067
อาจารย์ ธนา หงษ์สุวรรณ อาจารย์ที่ปรึกษา
อาจารย์ อัครเดช วัชระภูพงษ์ อาจารย์ที่ปรึกษา
ปีการศึกษา 2542

บทคัดย่อ

บทความฉบับนี้กล่าวถึงรายละเอียดของระบบรักษาความปลอดภัยบนเครือข่ายโดยใช้ไฟร์วอล โดยศึกษา วิเคราะห์ และเปรียบเทียบประเภทของระบบไฟร์วอล และผลิตภัณฑ์ชนิดต่างๆของไฟร์วอล เพื่อเป็นคำแนะนำในการเลือกใช้ผลิตภัณฑ์ไฟร์วอลและออกแบบระบบไฟร์วอล โดยแนะนำในส่วนของการเลือกใช้ฟังก์ชันการทำงาน และโทโปโลยีของไฟร์วอล รวมถึงแนะนำการเลือกใช้ผลิตภัณฑ์ไฟร์วอลที่เหมาะสม โดยพิจารณาจากระดับของความปลอดภัย ความเร็วในการสื่อสาร การจัดการกับผลิตภัณฑ์ไฟร์วอล ท้ายที่สุดออกแบบระบบไฟร์วอลสำหรับเครือข่ายคอมพิวเตอร์

TCP/IP Firewall System Implementation and Comparison

Mr. Koson Thirajitto
Mr. Charan Chiamtaweeboon
Mr. Thana Hongsuwan Advisor
Mr. Akkradach Watcharapupong Advisor

ABSTRACT

This article informs to the detail of Network Security System using Firewall. By studying, analysing, comparing types of firewall system and firewall products in order to be advisory to choose firewall products and design firewall system. In advisory will advise to choose the function and topology of firewall in addition to choose appropriate products by considering from security, performance, management of firewall products. Finally design firewall system for computer network.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยดี ด้วยความช่วยเหลือ และได้รับความร่วมมือจากบุคคลหลายๆท่านด้วยกัน ซึ่งบุคคลแรกที่ขอกล่าวคือต้องขอขอบพระคุณอาจารย์ที่ปรึกษาคืออาจารย์ ธนา หงษ์สุวรรณ และอาจารย์ อัครเดช วัชระภูพงษ์ ที่คอยดูแลเอาใจใส่ ให้คำปรึกษา คำแนะนำ และให้การสนับสนุนทางด้วยซอฟท์แวร์และฮาร์ดแวร์

ขอขอบพระคุณอาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้

ขอขอบคุณภาควิชาวิศวกรรมคอมพิวเตอร์ที่ช่วยอำนวยความสะดวกต่างๆ ทั้งเอื้อเฟื้อสถานที่และอุปกรณ์ในการทำการวิจัย

ขอขอบพระคุณพี่วาร์วที่ให้การสนับสนุนด้านผลิตภัณฑ์ไฟร์วอล และให้คำแนะนำในการติดตั้งและใช้งาน

ขอขอบคุณต่อและปุ๋มที่ให้ซอฟแวร์ใช้สำหรับทดสอบไฟร์วอล

ขอขอบคุณน้องโจ้และกระบี่ที่ให้ความช่วยเหลือด้านระบบปฏิบัติการและระบบเครือข่าย

ขอขอบคุณขอขอบคุณสมาชิกในห้องวิจัยไอแซคทุกคนที่ให้ความช่วยเหลือด้านต่างๆ และคอยเป็นกำลังใจให้กันเสมอมา

และท้ายที่สุดนี้บุคคลที่สำคัญที่สุดที่ต้องขอขอบพระคุณเป็นอย่างสูงคือบิดามารดาของข้าพเจ้าที่ให้การดูแล เลี้ยงดู ให้โอกาสทางการศึกษา ให้กำลังใจ และพระคุณอื่นๆอีกมากมายยากยิ่งที่จะทดแทนได้หมด จึงขอกราบขอบพระคุณมา ณ โอกาสนี้ด้วย

นายโกศล ถิรจิตโต

นายจรัญ เจียมทวีบุญ

สารบัญ

สารบัญภาพประกอบ

สารบัญตาราง

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มา

ในปัจจุบันนี้อินเทอร์เน็ตได้เข้ามามีบทบาทในชีวิตประจำวันของมนุษย์เป็นอย่างมาก เห็นได้จากการที่มีผู้ใช้งานคอมพิวเตอร์ที่เชื่อมต่อเข้ากับอินเทอร์เน็ตมีอัตราเพิ่มขึ้นอย่างรวดเร็ว มีการขยายตัวออกไปทั่วโลก ในบางประเทศถึงกับมีการใช้งานอินเทอร์เน็ตกันทุกบ้าน อินเทอร์เน็ตทำให้คนที่อยู่กันคนละซีกโลกสามารถสนทนากันได้ ทำให้การสื่อสารทำได้อย่างรวดเร็วและประหยัดกว่าการที่จะต้องเดินทางไปเอง ในอินเทอร์เน็ตยังเป็นแหล่งข้อมูลขนาดใหญ่มหาศาลที่ไม่มีวันจะเรียนรู้ได้หมดสิ้น ดังนั้นไม่แปลกที่ว่าองค์กรทั้งภาครัฐ และเอกชนไม่ว่าจะเป็นมหาวิทยาลัย สถาบันการศึกษาอื่น กรมตำรวจ สำนักงานทนายความ บริษัทประกอบการธุรกิจต่างๆ ฯลฯ ก็มีการเชื่อมต่อเข้ากับอินเทอร์เน็ตทำให้สามารถแลกเปลี่ยนข้อมูลกันทางคอมพิวเตอร์จากทุกๆ มุมโลกได้ ในขณะเดียวกันเครือข่ายขององค์กรเหล่านั้นที่เชื่อมต่อกับอินเทอร์เน็ตก็สามารถเข้าถึงโดยใครก็ได้ที่ใช้งานอินเทอร์เน็ตอยู่ ไม่ว่าจะอยู่ห่างไกลกันขนาดไหนก็ตาม ซึ่งส่วนใหญ่องค์กรที่เชื่อมต่ออินเทอร์เน็ตอยู่นั้นมักมีข้อมูลที่สำคัญ และเป็นความลับที่ไม่สามารถเปิดเผยให้คนภายนอกทราบได้ ทำให้ข้อมูลเหล่านี้อยู่ในสถานะที่เสี่ยงต่อผู้ไม่หวังดีภายนอกองค์กรซึ่งอาจจะเป็นคู่แข่ง หรือใครก็ตามอย่างหลีกเลี่ยงไม่ได้ ด้วยเหตุนี้เองความปลอดภัยในเครือข่ายขององค์กรที่เชื่อมต่อกับอินเทอร์เน็ตจึงเป็นสิ่งที่จำเป็น และสำคัญสำหรับองค์กรเหล่านั้นเป็นอย่างมาก

ดังนั้นทางคณะผู้จัดทำจึงมีความสนใจเกี่ยวกับการรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ที่เชื่อมต่อกับอินเทอร์เน็ต ซึ่งเป็นสิ่งที่สำคัญมากอย่างหนึ่งที่ทุกๆ คนที่ใช้งานอินเทอร์เน็ตจำเป็นต้องคำนึงถึง เพื่อเป็นการรักษาข้อมูลที่สำคัญ และเป็นความลับที่ไม่สามารถเปิดเผยได้ ไม่ให้ผู้ประสงค์ร้ายสามารถนำข้อมูลเหล่านี้ไปใช้ได้ เป็นการพิทักษ์ผลประโยชน์ให้กับผู้ใช้งานบนอินเทอร์เน็ต ซึ่งทางผู้จัดทำได้เล็งเห็นถึงความสำคัญในจุดนี้ จึงได้ทำการศึกษารายละเอียดเกี่ยวกับการรักษาความปลอดภัยบนระบบเครือข่าย ซึ่งในที่นี้คือ ระบบไฟร์วอล และจัดทำเอกสาร เพื่อเป็นประโยชน์แก่ผู้ที่สนใจหรือต้องการเรียนรู้ ศึกษาเพื่อเป็นแนวทางในการนำไปใช้งาน หรือนำไปเป็นพื้นฐานในการค้นคว้าต่อไป

1.2 วัตถุประสงค์ของงานวิจัย

วัตถุประสงค์ของการทำโปรเจ็กต์นี้คือ

1. ศึกษาการทำงานของระบบรักษาความปลอดภัยบนอินเทอร์เน็ตโดยใช้ไฟร์วอล โดยเริ่มตั้งแต่ฟังก์ชันการทำงาน และโทโปโลยีต่างๆ ของไฟร์วอล ข้อดี ข้อเสียของแต่ละอย่าง และเปรียบเทียบความเหมาะสมในการนำมาใช้งานในลักษณะต่างๆ
2. สามารถทดสอบการทำงานของระบบรักษาความปลอดภัยบนอินเทอร์เน็ต หรือไฟร์วอล โดยการจำลองสถานการณ์การโจมตีเครือข่ายคอมพิวเตอร์จากเครื่องภายนอกเครือข่าย แล้วป้องกันโดยไฟร์วอล

3. ศึกษาถึงการอิมพลีเมนต์ไฟร์วอลอย่างง่ายขึ้นมาใช้งานบนระบบปฏิบัติการ Open BSD คือ ไฟร์วอลทูลคิต (TIS Firewall Toolkit) ซึ่งสามารถดาวน์โหลดนำมาใช้ได้โดยไม่ต้องเสียค่าใช้จ่าย
4. นำผลิตภัณฑ์ไฟร์วอลประเภทต่างๆ รวมทั้งไฟร์วอลทูลคิตที่ได้อิมพลีเมนต์ขึ้นเองมาทดสอบการทำงาน จากนั้นนำข้อมูลที่ได้มาเปรียบเทียบ วิเคราะห์ประสิทธิภาพ และแนะนำการเลือกใช้ผลิตภัณฑ์ไฟร์วอลที่เหมาะสม
5. ออกแบบระบบไฟร์วอลของภาควิชาคอมพิวเตอร์ โดยนำความรู้จากการศึกษาระบบไฟร์วอล ฟังก์ชันการทำงาน โครงสร้างทางกายภาพ การออกแบบระบบไฟร์วอลพื้นฐาน และการทดสอบผลิตภัณฑ์ไฟร์วอลมาช่วยในการออกแบบระบบไฟร์วอลของภาควิชา

1.3 ขอบเขตของงานวิจัย

โครงงานนี้เริ่มต้นศึกษาถึงระบบรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ในอินเทอร์เน็ต นำผลิตภัณฑ์ไฟร์วอลที่สามารถหาได้มาทดสอบการทำงาน เปรียบเทียบ วิเคราะห์และสรุปผลการทำงานของไฟร์วอลนั้น และแนะนำการเลือกใช้ผลิตภัณฑ์ให้เหมาะสมสำหรับองค์กรของตน

1.4 วิธีการดำเนินงาน

ในขั้นแรกจะเริ่มต้นด้วยการศึกษาถึงความรู้พื้นฐานเกี่ยวกับระบบเครือข่าย จากนั้นก็ศึกษาถึงความปลอดภัยบนระบบเครือข่ายอินเทอร์เน็ต ซึ่งเป็นพื้นฐานที่สำคัญสำหรับการค้นคว้าในระดับที่สูงขึ้นไป จากนั้นก็ศึกษาถึงการทำงานของระบบไฟร์วอลเริ่มตั้งแต่จุดประสงค์ ความสามารถ โครงสร้างทางกายภาพ ฟังก์ชันการทำงานของไฟร์วอล เมื่อมาถึงระดับนี้แล้วก็เริ่มศึกษาถึงการทดสอบผลิตภัณฑ์ไฟร์วอล โดยผลิตภัณฑ์ที่มีอยู่มี 3 ผลิตภัณฑ์คือ ไฟร์วอล IBM eNetwork Firewall for Windows NT ของบริษัทไอบีเอ็ม ตัวที่ 2 คือ Gauntlet Firewall และตัวสุดท้ายคือ Firewall-1 ของบริษัท Check Point โดยทางกลุ่มได้กำหนดวิธีการทดสอบขึ้น ด้วยการทดสอบด้านการจัดการ โดยให้คะแนนความยากง่ายในการจัดการคอนฟิกไฟร์วอล ทดสอบประสิทธิภาพ และทดสอบความปลอดภัย จากนั้นนำผลการทดสอบที่ได้มาวิเคราะห์ และสรุปความเหมาะสมของผลิตภัณฑ์ไฟร์วอลว่าเหมาะสมสำหรับสภาวะแวดล้อมแบบใด นอกจากนี้ทางกลุ่มก็ได้ทำการอิมพลีเมนท์ไฟร์วอลขึ้นมาใช้งานบนระบบปฏิบัติการ OpenBSD และเพิ่มการทำงานของ TIS Firewall Toolkit ด้วย

บทที่ 2
ความรู้เบื้องต้น และความปลอดภัยของระบบเครือข่ายบนอินเทอร์เน็ต

2.1 ความรู้เบื้องต้นเกี่ยวกับระบบเครือข่ายบนอินเทอร์เน็ต

2.1.1 การทำงานของทีซีพี/ไอพี (TCP/IP)

การศึกษาหลักการทำงานของเน็ตเวิร์กโพรโตคอล จะเริ่มต้นด้วยการมองการทำงานของมันเป็นชั้นๆ หรือที่เรียกว่าเลเยอร์ (Layer) โดยที่แต่ละชั้นก็จะมีหน้าที่การทำงานที่ชัดเจน และไม่เกี่ยวข้องกัน แต่ละชั้นก็จะรู้เพียงวิธีการส่างข้อมูลไปยังชั้นอื่นๆ แต่ไม่รู้ถึงการทำงานข้างในเลย แต่ละโพรโตคอลจะมีการแบ่งการทำงานออกเป็นจำนวนชั้นไม่เท่ากัน ทำให้เป็นการยากที่จะระบุว่าเน็ตเวิร์กโพรโตคอลโดยรวมแล้วมีการทำงานกี่ชั้น แต่ก็มีมาตรฐานที่เป็นที่ยอมรับกันโดยทั่วไปเรียกว่า Open Interconnect (OSI) Reference Model ซึ่งทำการแบ่งการทำงานของเน็ตเวิร์กโพรโตคอลออกเป็น 7 ชั้นดังนี้

- ชั้นที่ 1 ฟิสิคัลเลเยอร์ (Physical Layer) เป็นระดับต่ำสุด ซึ่งจะมองในแง่ของสัญญาณไฟฟ้าที่ส่งข้อมูลระหว่างกันรวมทั้งเครื่องมือและอุปกรณ์ที่ใช้ในการเชื่อมต่อกันจริงๆ
- ชั้นที่ 2 ดาต้าลิ้งก์เลเยอร์ (Data Link Layer) เป็นระดับที่มองข้อมูลที่ส่งระหว่างจุด 2 จุดที่ได้เชื่อมต่อกันจริง โดยเรียกข้อมูลนี้ว่าเฟรม
- ชั้นที่ 3 เน็ตเวิร์กเลเยอร์ (Network Layer) เป็นระดับที่มองข้อมูลที่เรียกว่า แพ็กเก็ต (Packet) ซึ่งจะเป็นข้อมูลที่ถูกซอยย่อยให้ส่งไปในเครือข่าย ซึ่งจะมีข้อมูลบางส่วนในแพ็กเก็ตใช้ในการบอกเส้นทางที่แพ็กเก็ตนั้นจะต้องเดินทางไป
- ชั้นที่ 4 ทรานสปอร์ตเลเยอร์ (Transport Layer) เป็นระดับที่มองข้อมูลที่เรียกว่า เมสเสจ (Message) จะเป็นสิ่งที่รับประกันได้ว่าข้อมูลถูกส่งระหว่างโฮสต์ถูกต้องครบถ้วน
- ชั้นที่ 5 เซสชันเลเยอร์ (Session Layer) ดูแลเกี่ยวกับการสื่อสารระหว่างแอพพลิเคชันของเครื่องต่างๆ ในเครือข่าย และความปลอดภัยในการสื่อสาร
- ชั้นที่ 6 พรีเซนเทชันเลเยอร์ (Presentation Layer) เป็นระดับที่เตรียมการให้บริการให้แก่แอพพลิเคชัน
- ชั้นที่ 7 แอพพลิเคชันเลเยอร์ (Application Layer) เป็นระดับที่จัดการเกี่ยวกับการสื่อสารของแอพพลิเคชัน

แต่ละชั้นมีข้อกำหนดและการทำงานที่แน่นอนและไม่เกี่ยวข้องกับชั้นอื่น สำหรับการศึกษาโพรโตคอล TCP/IP นั้นเราจะไม่อ้างอิง OSI Reference Model เพราะเข้าใจยาก ดังนั้นโพรโตคอล TCP/IP จะสร้างโมเดลขึ้นมาใหม่โดยแบ่งเป็น 4 ชั้นดังนี้

- ชั้นที่ 1 เน็ตเวิร์กแอ็กเซสเลเยอร์ (Network Access Layer) ประกอบด้วยอุปกรณ์และเครื่องมือทางกายภาพที่เชื่อมต่อในเครือข่าย
- ชั้นที่ 2 อินเทอร์เน็ตเลเยอร์ (Internet Layer) ระบุดาต้าแกรมจัดการหาเส้นทางให้กับข้อมูล

- ชั้นที่ 3 โฮสต์ทูโฮสต์ทรานสปอร์ตเลเยอร์ (Host-to-Host Tranport Layer) จัดเตรียมเซอร์วิสในการส่งข้อมูลระหว่างเครื่องปลายทางทั้ง 2 ฝั่ง
- ชั้นที่ 4 แอพพลิเคชันเลเยอร์ (Application Layer) ประกอบด้วยแอพพลิเคชันและโพรเซสที่ใช้ในเครือข่าย

ลักษณะการทำงานของโมเดลนี้คือข้อมูลจะถูกส่งลงมาจากชั้นข้างบนลงมายังชั้นล่างสุดซึ่งมีหน้าที่จัดการเกี่ยวกับการส่งข้อมูลผ่านสายสัญญาณไปยังจุดหมายปลายทาง เมื่อข้อมูลไปถึงจุดหมายแล้วก็จะกลับย้อนจากชั้นล่างขึ้นไปชั้นบนสุด ซึ่งเป็นชั้นที่โปรแกรมต่างๆ ใช้งานอยู่ ขณะที่ข้อมูลถูกส่งผ่านจากชั้นบนลงมายังชั้นล่าง แต่ละชั้นจะทำการเพิ่มข้อมูลควบคุมเข้าไปเพื่อให้การส่งข้อมูลถูกต้อง และเป็นการส่งพารามิเตอร์ที่จำเป็นไปให้กับชั้นของมันในเครื่องปลายทาง ข้อมูลควบคุมเหล่านี้เรียกว่า เฮดเดอร์ (Header) ที่มีรูปแบบเป็นของตัวเอง การเพิ่มข้อมูลเข้าไปเรียกว่า ดาต้าเอ็นแคปซูเลชัน (Data Encapsulation)

หน่วยของข้อมูลที่จะทำการส่งนั้นจะมีชื่อเรียกต่างกันเมื่อมันเดินทางผ่านแต่ละเลเยอร์ เช่นในชั้นอินเทอร์เน็ตเลเยอร์จะเรียกหน่วยของข้อมูลเป็นดาต้าแกรม (Datagram) ส่วนในชั้นของเน็ตเวิร์กแอ็กเซสเลเยอร์จะเรียกข้อมูลว่าเฟรม (Frame)

2.1.2 เน็ตเวิร์กแอ็กเซสเลเยอร์

เลเยอร์นี้ทำหน้าที่จัดส่งข้อมูลผ่านสายสัญญาณชนิดต่างๆ โดยการทำงานของมันขึ้นอยู่กับชนิดของสายสัญญาณที่เราใช้อยู่ สายแต่ละชนิดมีโพรโตคอลที่ใช้ควบคุมการทำงานที่ต่างกันเช่น Ethernet, FDDI, Frame Relay เป็นต้น ตัวอย่างการทำงานได้แก่ การเพิ่มเฮดเดอร์เข้าไปในดาต้าแกรมเพื่อให้กลายเป็นเฟรมแล้วส่งไปตามเครือข่าย

2.1.3 อินเทอร์เน็ตเลเยอร์

ชั้นนี้มีโพรโตคอลที่ทำงานอยู่ 2 โพรโตคอลด้วยกันคือ IP (Internet Protocol) และ ICMP (Internet Control Message Protocol)

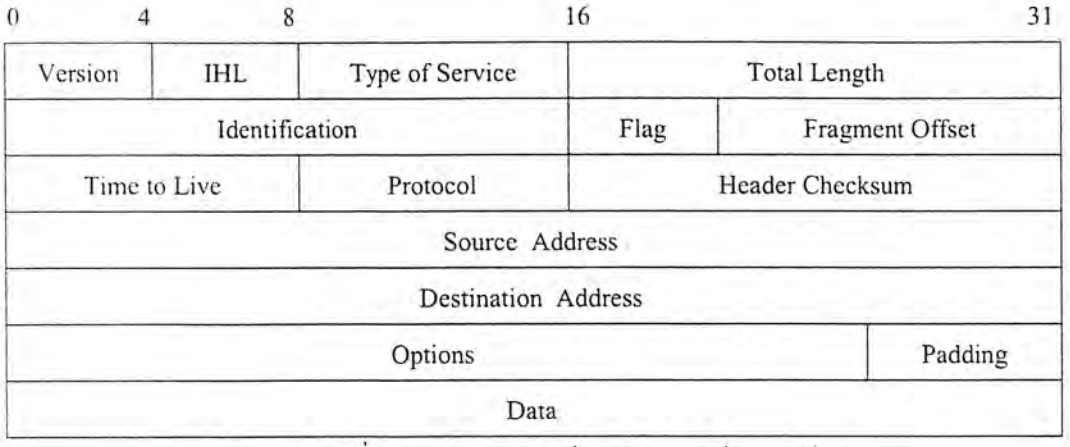
2.1.3.1 อินเทอร์เน็ตโพรโตคอล (IP)

หน้าที่สำคัญของโพรโตคอลนี้คือ

- สร้างดาต้าแกรม
- หาเส้นทางเพื่อส่งดาต้าแกรมไปยังปลายทาง (routing)
- แบ่งและประกอบดาต้าแกรม (Fragmenting and re-assembling the datagram)

โพรโตคอลนี้เป็นโพรโตคอลแบบคอนเน็กชันเลส (connectionless) นั่นคือไม่มีการทำการแฮนด์เชค (handshake) กับปลายทางก่อนส่งข้อมูล โดยจะทำการส่งข้อมูลไปเลยโดยไม่คำนึงถึงว่ามันจะไปถึงปลายทางหรือไม่ นอกจากนี้ยังไม่มีการตรวจสอบความถูกต้องของข้อมูลที่ส่งไปด้วย

หน่วยของข้อมูลที่อยู่ในชั้นนี้เรียกว่า ดาต้าแกรม ซึ่งถูกออกแบบมาให้ทำงานกับเครือข่ายแบบแพ็กเก็ตสวิตช์ ซึ่งข้อมูลของผู้ใช้มักถูกแบ่งออกเป็นหลายๆ ดาต้าแกรม โดยที่ดาต้าแกรมแต่ละตัวจะมีเฮดเดอร์ที่เก็บรายละเอียดของตัวมันและปลายทางที่มันจะไป ซึ่งรูปแบบของเฮดเดอร์จะประกอบด้วย 6 เวิร์ด แต่ละเวิร์ดมีขนาด 32 บิตซึ่งแสดงดังรูปข้างล่างนี้



รูปที่ 2-1 แสดงแบบฟอร์มของเฮดเดอร์ของดาต้าแกรม

2.1.3.2 อินเทอร์เน็ตคอนโทรลเมสเซจโพรโตคอล (ICMP)

นี่เป็นอีกโพรโตคอลหนึ่งที่ทำงานอยู่ในชั้นอินเทอร์เน็ตเลเยอร์ ซึ่งทำหน้าที่ในการส่งสัญญาณควบคุมต่างๆ ไปยังเครื่องปลายทาง โดยโพรโตคอลนี้อาศัยดาต้าแกรมในการส่งสัญญาณควบคุมเหล่านั้น คำสั่งควบคุมที่สำคัญของ ICMP ได้แก่

- **Flow Control** จะถูกส่งโดยเครื่องปลายทางกลับไปยังเครื่องต้นทางเมื่อมีดาต้าแกรมถูกส่งเร็วเกินไปจนมันประมวลผลไม่ทัน
- **Detecting unreachable destinations** สัญญาณนี้จะถูกส่งกลับไปยังเครื่องต้นทางเพื่อบอกว่าหาปลายทางไม่พบ
- **Redirect routes** สัญญาณนี้จะเกิดขึ้นเฉพาะในกรณีที่มีในเครือข่ายมีเกตเวย์มากกว่าหนึ่งตัว
- **Checking remote hosts** เครื่องหนึ่งๆ สามารถทำการส่ง Echo Message ไปยังเครื่องใดๆ เพื่อทดสอบว่าอินเทอร์เน็ตโพรโตคอลของเครื่องนั้นทำงานอยู่หรือไม่

2.1.4 ทรานสปอร์ตเลเยอร์

ในเลเยอร์นี้มีโพรโตคอลที่สำคัญอยู่ 2 อย่างคือ Transmission Control Protocol (TCP) และ User Datagram Protocol (UDP) ทั้งสองโพรโตคอลนี้ทำหน้าที่เหมือนกันคือเป็นตัวเชื่อมต่อการส่งข้อมูลระหว่างแอพพลิเคชันเลเยอร์กับอินเทอร์เน็ตเลเยอร์ แต่ TCP จะมีการตรวจสอบและแก้ไขความผิดพลาดของข้อมูลที่รับเข้ามา ในขณะที่UDPไม่มี ทำให้ TCP มีความน่าเชื่อถือมากกว่า แต่ในขณะเดียวกัน UDP เป็นการส่งข้อมูลที่มีโอเวอร์เฮดน้อยกว่า TCP

2.1.4.1 ยูดีพี (UDP หรือ User Datagram Protocol)

เป็นโพรโตคอลแบบคอนเน็กชันเลสคือไม่มีการทำแฮนด์เชคกับเครื่องปลายทาง และไม่มีการตรวจสอบความถูกต้องของข้อมูลที่รับมา ทำให้อัตราเร็วในการทำงานสูง เหมาะที่จะใช้กับงานที่ส่งข้อมูลขนาดเล็ก และส่งบ่อยๆ

เฮดเดอร์ของยูดีพี ได้แสดงไว้ในรูปข้างล่างนี้ ซึ่งจะมีการส่งหมายเลขพอร์ตต้นทางและปลายทางไปด้วย ซึ่งหมายเลขพอร์ตนี้จะใช้ในการส่งข้อมูลให้กับแอพพลิเคชันเลเยอร์ต่อไป

Source Port	Destinatio Port
Length	Checksum
Data	

รูปที่ 2-2 แสดงแบบฟอร์มของเฮดเดอร์ของโพรโตคอลยูดีพี

2.1.4.2 ทีซีพี (TCP หรือ Transmission Control Protocol)

เป็นโพรโตคอลแบบคอนเน็กชันโอเรียนเต็ด แสดงว่ามันจะต้องมีการส่งสัญญาณแฮนด์เชคระหว่างเครื่องต้นทางและปลายทางเพื่อให้แน่ใจว่าสามารถติดต่อถึงกันได้ แล้วค่อยเริ่มส่งข้อมูล และมีการตรวจสอบความถูกต้องของข้อมูลที่ได้รับด้วยทำให้เป็นการส่งที่มีความน่าเชื่อถือ ซึ่งมีเฮดเดอร์ดังรูปข้างล่างนี้

หน่วยของข้อมูลของ TCP นั้นเรียกว่าเซ็กเมนต์ (Segment) โดยการส่งข้อมูลของทีซีพีนั้นจะส่งทีละเซ็กเมนต์ โดยเครื่องปลายทางจะส่งสัญญาณตอบรับกลับมายังเครื่องต้นทางสำหรับทุกๆ เซ็กเมนต์ที่มันได้รับและตรวจสอบแล้วไม่พบข้อผิดพลาด ถ้าหากว่าเครื่องต้นทางไม่ได้รับสัญญาณตอบรับกลับมา มันก็สันนิษฐานว่าเซ็กเมนต์นั้นมีปัญหาและทำการส่งเซ็กเมนต์นั้นไปอีกครั้ง

<table>
<tr><td colspan="4">0 8 16 31</td></tr>
<tr><td colspan="2">Source Port</td><td colspan="2">Destination Port</td></tr>
<tr><td colspan="4">Sequence Number</td></tr>
<tr><td colspan="4">Acknowledgement Number</td></tr>
<tr><td>Offset</td><td>Reserved</td><td>Flags</td><td>Window</td></tr>
<tr><td colspan="2">Checksum</td><td colspan="2">Urgent Pointer</td></tr>
<tr><td colspan="3">Options</td><td>Padding</td></tr>
<tr><td colspan="4">Data</td></tr>
</table>

รูปที่ 2-3 แสดงแบบฟอร์มของเฮดเดอร์ของโพรโตคอลทีซีพี

2.1.5 แอพพลิเคชันเลเยอร์

เลเยอร์นี้เป็นเลเยอร์บนสุด ซึ่งประกอบไปด้วยหลายโพรโตคอล (เรามักเรียกว่าโปรแกรมมากกว่า) ซึ่งนับวันก็ยิ่งมากขึ้นเรื่อยๆ ตัวอย่างของโพรโตคอลที่ใช้กันบ่อยในเลเยอร์นี้ได้แก่

- เทลเน็ต (Telnet) เรียกอีกอย่างหนึ่งว่า Network Terminal Protocol ใช้ในการจำลองหน้าจอผ่านเครือข่าย

- เอฟทีพี (FTP หรือ File Transfer Protocol) ใช้ในการโอนถ่ายแฟ้มข้อมูล
- เอสเอ็มทีพี (SMTP หรือ Simple Mail Transfer Protocol) ใช้ในการรับส่งอีเมล์

โพรโตคอลที่กล่าวมาแล้วนี้ทำงานโดยใช้โพรโตคอลทีซีพีในทราสปอร์ตเลเยอร์ ส่วนโพรโตคอลที่ใช้ยูดีพีได้แก่

- ดีเอ็นเอส (DNS หรือ Domain Name Service) ใช้ในการแปลงชื่อเครื่องให้เป็นเลขไอพีแอดเดรส หรือกลับกัน
- อาร์ไอพี (RIP หรือ Routing Information Protocol) ใช้แลกเปลี่ยนข้อมูลในการหาเส้นทางระหว่างอุปกรณ์ต่างๆ
- เอ็นเอฟเอส (NFS หรือ Network File System) ใช้เพื่อแชร์ข้อมูลในดิสก์ให้กับหลายๆ เครื่อง

2.2 ความปลอดภัยของระบบเครือข่ายบนอินเทอร์เน็ต

เนื่องจากการเพิ่มขึ้นอย่างมากมายของการบุกรุกเครือข่ายคอมพิวเตอร์ จึงไม่ต้องสงสัยเลยว่าเหตุใดผู้ใช้คอมพิวเตอร์ส่วนใหญ่จึงเริ่มหันมาสนใจระบบรักษาความปลอดภัยบนคอมพิวเตอร์กันมากขึ้น แต่อย่างไรก็ตาม ผู้ใช้ส่วนใหญ่ก็ยังไม่เข้าใจระบบรักษาความปลอดภัยบนคอมพิวเตอร์ว่าสำคัญกับพวกเขาอย่างไร เนื่องจากข่าวการบุกรุกต่างๆ เช่น หนอนคอมพิวเตอร์ (The Worm) การจารกรรมของสายลับรัสเซีย ฯลฯ ไม่ได้บอกถึงรายละเอียดของการบุกรุกต่างๆ จึงไม่สามารถสร้างความข้าใจให้กับผู้ใช้ได้ ระบบรักษาความปลอดภัยบนคอมพิวเตอร์นั้นหมายถึงระบบที่ปกป้องทุกๆ อย่างบนคอมพิวเตอร์โดยเฉพาะข้อมูล ซึ่งอาจเรียกได้ว่า ระบบรักษาความปลอดภัยของข้อมูล (Information Security)

เมื่อกล่าวถึงระบบรักษาความปลอดภัยบนคอมพิวเตอร์ (Computer Security) จะมีสิ่งที่สำคัญมากเข้ามาเกี่ยวข้องด้วยอาทิเช่น ความบกพร่อง (Vulnerability) การคุกคาม (Threat) และวิธีการป้องกัน (Countermeasures) เป็นต้น โดยอธิบายดังนี้

2.2.1 ความบกพร่อง (Vulnerability)

คือเป็นจุดอ่อน ช่องโหว่ รูรั่วที่สามารถทำให้นำไปสู่การบุกรุกหรือคุกคามคอมพิวเตอร์ได้

คอมพิวเตอร์ทุกเครื่องนั้นย่อมมีความบกพร่องที่สามารถนำไปสู่การบุกรุกได้ แต่นโยบายการรักษาความปลอดภัย (Security Policies) และผลิตภัณฑ์ต่างๆ ก็สามารรถช่วยลดความบกพร่องต่างๆ ของระบบได้ หรืออีกนัยหนึ่งคือสามารถทำให้ผู้บุกรุกต้องใช้ความพยายามมากขึ้นในการบุกรุกเข้ามาในระบบนั้นๆ นั่นหมายถึงว่า ไม่มีระบบรักษาความปลอดภัยที่สมบูรณ์ที่สุด ความบกพร่องทั่วๆ ไปของระบบคอมพิวเตอร์มีดังนี้

- ความบกพร่องทางกายภาพ (Physical Vulnerabilities)

  ได้แก่การที่ตึก หรือห้องที่มีคอมพิวเตอร์อยู่ภายในนั้น สามารถถูกบุกรุกเข้าไปได้ โดยวิธีการเดียวกันกับการที่ขโมยสามารถบุกเข้าไปปล้นบ้านได้ วิธีการป้องกันได้แก่การใช้ระบบรักษาความปลอดภัยของอาคารเช่น กุญแจล็อกห้อง พนักงานรักษาความปลอดภัย สัญญาณเตือน

- ความบกพร่องจากธรรมชาติ (Natural Vulnerabilities)

ได้แก่ภัยธรรมชาติต่างๆ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว ฯลฯ ภัยเหล่านี้สามารถทำให้ข้อมูลในคอมพิวเตอร์เสียหายได้ อีกทั้งสภาพแวดล้อมต่างๆ เช่น ฝุ่น ความชื้น อุณหภูมิ ก็สามารถสร้างความเสียหายให้กับคอมพิวเตอร์ได้

- ความบกพร่องของซอฟแวร์และฮาร์ดแวร์ (Hardware and Software Vulnerabilities)
  ได้แก่ความผิดพลาดในการทำงานของฮาร์ดแวร์ เช่นการจัดการหน่วยความจำผิดพลาดในการที่จะควบคุมการเข้าถึงหน่วยความจำของระบบที่ไม่อนุญาตให้ผู้ใช้ปกติเข้าถึงได้ ทำให้ผู้ใช้ปกติสามารถเข้าถึงหน่วยความจำของระบบนั้นๆ ได้
- ความบกพร่องของสื่อ (Media Vulnerabilities)
  ได้แก่การที่แผ่นดิสก์ เทป และเอกสารต่างๆ สามารถถูกขโมยได้ อีกทั้งยังอาจเสื่อมสภาพตามกาลเวลาทำให้ข้อมูลเสียหายได้ด้วย
- ความบกพร่องของการส่งผ่านข้อมูล (Communication Vulnerabilities)
  ได้แก่ การที่ข้อมูลที่ส่งผ่านกันนั้น สามารถถูกดักจับ หรือถูกขัดขวางได้ เช่นบนเครือข่ายคอมพิวเตอร์ข้อมูลที่ส่งผ่านไปยังสายสัญญาณนั้นอาจถูกขัดขวางหรือดักข้อมูลนั้นๆ ได้
- ความบกพร่องที่เกี่ยวกับมนุษย์ (Human Vulnerabilities)
  ได้แก่ การที่ผู้ควบคุมระบบนั้นๆ ไม่มีความรู้ความสามารถเพียงพอที่จะควบคุมระบบนั้นๆ ได้ หรือมีความหละหลวมในระบบรักษาความปลอดภัย เช่น การติดสินบนเพื่อใช้รหัสผ่าน การติดสินบนเพื่อเข้าไปยงห้องคอมพิวเตอร์ สิ่งเหล่านี้เป็นความบกพร่องที่เป็นอันตรายอย่างยิ่ง

2.2.2 การคุกคามระบบรักษาความปลอดภัย (Threats)

คือความเป็นไปได้ในการที่จะมีสิ่งใดสิ่งหนึ่ง ไม่ว่าจะเป็นคนหรือสิ่งของหรือเหตุการณ์ต่างๆ ที่สามารถอาศัยความบกพร่องของระบบนั้นๆ ผ่านเข้าไปข้างในระบบได้

การคุกคามสามารถแบ่งออกเป็น 3 ประเภท ได้แก่ การคุกคามโดยธรรมชาติ (Natural Threats) การคุกคามโดยมิได้เจตนา (Uninternational Threats) และการคุกคามโดยเจตนา (Intentional Threats) โดยมีความหมายดังนี้

- การคุกคามโดยธรรมชาติ
  ได้แก่ ภัยธรรมชาติต่างๆ เช่น ไฟไหม้ น้ำท่วม ไฟฟ้าขัดข้อง ฯลฯ ซึ่งไม่สามารถหลีกเลี่ยงได้ แต่เราสามารถเตรียมการป้องกันได้
- การคุกคามโดยมิได้เจตนา (Unintentional Threats)
  ได้แก่ การขาดความรู้ความสามารถของผู้ควบคุมระบบ และผู้ใช้ทั่วไป หรือความประมาทเลินเล่อของผู้ใช้ อาจก่อให้เกิดความเสียหายกับข้อมูลในคอมพิวเตอร์ได้
- การคุกคามโดยเจตนา (Intentional Threats)
  เป็นการคุกคามที่น่าสนใจมากที่สุด และสามารถป้องกันได้โดยผลิตภัณฑ์ต่างๆ ด้วย เพราะเป็นการคุกคามจากผู้บุกรุกที่มีความเชี่ยวชาญในระบบคอมพิวเตอร์ โดยสามารถแบ่งออกได้เป็นการคุกคามจากภายใน และจากภายนอก

2.2.3 กล่องเครื่องมือของแฮกเกอร์

เป็นเรื่องยากที่จะบรรยายถึงการโจมตีของแฮกเกอร์ เนื่องจากผู้บุกรุกมีระดับแตกต่างกันตามความเชี่ยวชาญด้านเทคนิค และมีแรงผลักดันที่ต่างกันมากมาย แฮกเกอร์บางคนชอบความท้าทาย บางคนแค่ต้องการทำให้ชีวิตยุ่งยากกว่าคนอื่น และยังมีบางคนขโมยข้อมูลเพื่อแสวงหากำไร

2.2.4 การรวบรวมข้อมูล

โดยทั่วไปขั้นตอนแรกในการเจาะระบบคือการรวบรวมข้อมูล จุดประสงค์เพื่อสร้างฐานข้อมูลเครือข่ายขององค์กรเป้าหมายและรวบรวมข้อมูลเกี่ยวกับโฮสต์ที่ตั้งอยู่บนส่วนต่างๆ ที่ตั้งอยู่บนส่วนต่างๆ ของเครือข่าย มีเครื่องมือจำนวนมากที่แฮกเกอร์สามารถเลือกใช้เพื่อเก็บรวบรวมข้อมูลนี้ เช่น

- โพรโตคอล SNMP สามารถนำมาใช้เพื่อตรวจดูตารางการจัดเส้นทาง (routing table) ของเราเตอร์ที่ไม่รักษาความปลอดภัยเพื่อเรียนรู้รายละเอียดเกี่ยวกับโทโปโลยีของเครือข่ายขององค์กรเป้าหมาย
- โปรแกรม TraceRoute สามารถเปิดเผยหมายเลขเครือข่ายและเราเตอร์ในเส้นทางไปสู่โฮสต์ที่ระบุ
- โพรโตคอล Whois เป็นบริการข้อมูลชนิดหนึ่งที่สามารถให้ข้อมูลเกี่ยวกับ DNS domain ทั้งหมดและผู้ดูแลระบบที่รับผิดชอบแต่ละโดเมน อย่างไรก็ตาม ข้อมูลนี้มักล้าสมัย
- เซิร์ฟเวอร์ DNS สามารถเข้าถึงรายการไอพีแอดเดรสของโฮสต์และชื่อโฮสต์ที่ตรงกันได้
- โพรโตคอล Finger สามารถเปิดเผยข้อมูลในรายระเอียดเกี่ยวกับผู้ใช้ (ชื่อล็อกอิน หมายเลขโทรศัพท์ เวลาที่ล็อกอินครั้งสุดท้าย เป็นต้น) ของโฮสต์ที่ระบุได้
- โปรแกรม Ping สามารถนำมาใช้เพื่อค้นหาตำแหน่งโฮสต์ที่ต้องการและตรวจสอบการเข้าถึงได้ เครื่องมือง่ายๆ นี้สามารถใช้ในโปรแกรมตรวจสอบผ่านที่ ping ทุกโฮสต์แอดเดรสที่เป็นไปได้บนเครือข่ายเพื่อสร้างรายการโฮสต์ที่มีอยู่จริงบนเครือข่าย

2.2.5 การสำรวจจุดอ่อนในการรักษาความปลอดภัยของระบบ

หลังจากรวบรวมข้อมูลเกี่ยวกับเครือข่ายขององค์กรเป้าหมายแล้ว แฮ็กเกอร์จะพยายามสำรวจจุดอ่อนในการรักษาความปลอดภัยของแต่ละโฮสต์ มีเครื่องมือจำนวนมากที่แฮ็กเกอร์สามารถใช้เพื่อตรวจโฮสต์แต่ละตัวบนเครือข่ายโดยอัตโนมัติ ตัวอย่างเช่น

- เนื่องจากบริการที่มีจุดอ่อนซึ่งเป็นที่รู้กันมีอยู่ไม่มาก แฮ็กเกอร์ที่มีความรู้จึงสามารถเขียนโปรแกรมขนาดเล็กที่พยายามเชื่อมต่อกับพอร์ตของบริการที่กำหนดบนโฮสต์เป้าหมาย เอาท์พุตของโปรแกรมคือรายการโฮสต์ที่สนับสนุนบริการนั้นซึ่งเปิดกว้างต่อการโจมตี
- มีเครื่องมือที่ใช้โดยทั่วไปหลายตัว เช่น Security Administrator Tool for Analysing Network (SATAN) ที่ตรวจสอบโดเมนหรือเครือข่ายย่อย(subnetwork) ทั้งหมด และค้นหาจุดอ่อนในการรักษาความปลอดภัย โปรแกรมเหล่านี้ระบุจุดอ่อนของแต่ละระบบซึ่งอาจถูก

โจมตีในหลายๆ จุด ผู้บุกรุกใช้ข้อมูลที่รวบรวมจากการตรวจสอบเหล่านี้เพื่อเข้าถึงระบบขององค์กรเป้าหมายโดยไม่ได้รับอนุญาต

ผู้ดูแลระบบที่เฉลียวฉลาดสามารถใช้เครื่องมือเหล่านี้ภายในเครือข่ายส่วนตัวของพวกเขาเพื่อค้นหาจุดอ่อนในการรักษาความปลอดภัย และตรวจดูว่าโฮสต์ใดต้องได้รับการปรับปรุงด้วยซอฟต์แวร์ที่แก้ไขใหม่

2.2.6 การเข้าถึงระบบที่ได้รับการปกป้อง

ผู้บุกรุกใช้ผลจากการสำรวจโฮสต์เพื่อกำหนดเป้าหมายที่จะโจมตี หลังจากเข้าถึงระบบที่ได้รับการปกป้องได้แล้ว แฮ็กเกอร์จะมีทางเลือกมากมาย เช่น

- ผู้บุกรุกอาจพยายามทำลายหลักฐานของการกระทำความผิด และเปิดช่องโหว่ใหม่ในระบบรักษาความปลอดภัย หรือเปิดประตูหลังในระบบเพื่อให้สามารถเข้าถึงได้ต่อไปแม้ว่าการโจมตีครั้งแรกจะถูกตรวจพบ
- ผู้บุกรุกสามารถติดตั้งแพ็กเก็ตสนิฟเฟอร์ (packet sniffer)ซึ่งรวมไว้ด้วยไบนารีของม้าโทรจัน (Trojan hourse)ที่ซ่อนเร้นกิจกรรมของตัวมันบนระบบนั้น แพ็กเก็ตสนิฟเฟอร์จะรวบรวมชื่อบัญชีและรหัสผ่านสำหรับบริการ Telnet และ FTP ที่ทำให้แฮ็กเกอร์ขยายการโจมตีไปสู่เครื่องอื่นได้
- ผู้บุกรุกสามารถค้นหาโฮสต์อื่นที่พึ่งพาระบบนี้ ทำให้แฮ็กเกอร์สามารถใช้ประโยชน์จากจุดอ่อนของโฮสต์เดียวและขยายการโจมตีไปสู่เครื่องอื่นได้
- ถ้าแฮ็กเกอร์สามารถได้สิทธิในการเข้าถึงระบบ เขาจะสามารถอ่านเมล์ค้นไฟล์ส่วนตัว ขโมยไฟล์ส่วนตัว และทำลายหรือทำให้ข้อมูลสำคัญเสียหาย

2.2.7 วิธีการป้องกัน (Countermeasures)

คือเทคนิคในการป้องกันคอมพิวเตอร์จากการบุกรุก จะเห็นได้ว่ายิ่งมีความบกพร่องของระบบมากขึ้นเท่าไร ก็จะมีโอกาสที่จะเกิดการคุกคามมากขึ้นเท่านั้น และเราก็ต้องเพิ่มความระมัดระวังในการพิจารณาถึงวิธีการป้องกันระบบของเราด้วย

สำหรับวิธีการป้องกันนั้น สามารถแบ่งออกเป็น 3 ประเภทใหญ่คือ

- การรักษาความปลอดภัยของคอมพิวเตอร์ (Computer Security)
  คือการป้องกันข้อมูลในคอมพิวเตอร์นั้นๆ
- การรักษาความปลอดภัยในการติดต่อสื่อสาร (Communications Security)
  คือการป้องกันข้อมูลที่ส่งผ่านไปยังคอมพิวเตอร์อื่นๆ
- การรักษาความปลอดภัยทางกายภาพ (Physical Security)
  คือการป้องกันคอมพิวเตอร์และอุปกรณ์ต่างๆ จากความเสียหายทางกายภาพ เช่นภัยธรรมชาติต่างๆ การบุกรุกห้องคอมพิวเตอร์ ฯลฯ

2.2.8 ปัจจัยที่มีผลกระทบต่อความปลอดภัยในการติดต่อสื่อสาร

มีอยู่ 3 ปัจจัยด้วยกัน

- การเพิ่มจำนวนของคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ ทำให้ความน่าจะเป็นมากขึ้นในการที่ผู้ใช้จะมีโอกาสเข้าถึงคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์นั้นๆ ได้
- การเพิ่มจำนวนของระบบคอมพิวเตอร์ที่ต้องการความปลอดภัยของข้อมูลในระดับสูง (Security-Sensitive Information) เช่น ระบบธนาคารที่สามารถโอนเงินเข้าบัญชีแบบอิเล็กทรอนิกส์ (Electronic Funds Transfer) เป็นต้น ซึ่งทำให้มีโอกาสที่ระบบเหล่านั้นจะถูกบุกรุกโดยผู้ประสงค์ร้ายเพิ่มขึ้นได้
- การเพิ่มจำนวนของผู้บุกรุกที่มีความเชี่ยวชาญในความรู้ทางด้านเครือข่ายคอมพิวเตอร์และการติดต่อสื่อสาร ทำให้ระบบต่างๆ ที่เชื่อมต่อกับอินเทอร์เน็ตนั้นมีโอกาสที่จะถูกบุกรุกจากผู้ประสงค์ร้ายเหล่านี้

2.2.9 ความต้องการของความปลอดภัยโดยทั่วไป (Typical Security Requirement)

การคุกคามของแฮ็กเกอร์ (Hacker Threats) นั้น มักจะเกิดกับเครือข่ายคอมพิวเตอร์ที่เชื่อมต่อกับอินเทอร์เน็ตแต่ก็ยังมีการบุกรุกไปยังแหล่งข้อมูลอื่นๆ ที่ไม่ใช่อินเทอร์เน็ตอีก

- ธนาคาร
- การค้าแบบอิเล็กทรอนิกส์ (Electronic Trading)
- หน่วยงานรัฐบาล
- ศูนย์กลางการติดต่อสื่อสาร
- เครือข่ายส่วนตัว

บทที่ 3
ระบบไฟร์วอล

3.1 ทำไมต้องใช้ไฟร์วอล

ในปัจจุบันนี้ อินเทอร์เน็ตได้เข้ามามีบทบาทมากในสังคมมนุษย์ ไม่ว่าจะเป็นสถานศึกษา องค์กรต่างๆ ทั้งในภาครัฐและเอกชน บริษัทต่างๆ ฯลฯ ทำให้มีการเชื่อมต่อเครือข่ายคอมพิวเตอร์เข้ากับอินเทอร์เน็ตเพิ่มมากขึ้น ทำให้อินเทอร์เน็ตมีขนาดใหญ่ขึ้น และมีการใช้งานกันอย่างแพร่หลาย มีองค์กรที่ให้บริการทางอินเทอร์เน็ตเพิ่มขึ้น ทำให้มีผู้ใช้บริการเพิ่มมากขึ้นอย่างรวดเร็วด้วย

เนื่องจากบนระบบเครือข่ายอินเทอร์เน็ตมีการแลกเปลี่ยนข้อมูลต่างๆ เป็นจำนวนมหาศาล ซึ่งข้อมูลเหล่านี้มีทั้งที่สามารถเปิดเผยได้ และข้อมูลที่สำคัญที่ต้องปิดเป็นความลับ เพื่อป้องกันผู้บุกรุก หรือผู้ประสงค์ร้ายต่อระบบเครือข่ายของเรา และยิ่งมีจำนวนผู้ใช้งานบนอินเทอร์เน็ตมากเท่าไหร่ จำนวนผู้ประสงค์ร้ายก็ยิ่งเพิ่มจำนวนมากขึ้นด้วย ทำให้ความเสี่ยงที่เกิดขึ้นกับระบบเครือข่ายของเราก็มีมากขึ้นตามไปด้วย ดังนั้นเพื่อเพิ่มความปลอดภัยให้กับระบบเครือข่ายที่ต่อกับอินเทอร์เน็ตแล้ว จึงได้มีการคิดระบบรักษาความปลอดภัยบนอินเทอร์เน็ตขึ้นมาซึ่งเรียกว่า **อินเทอร์เน็ตไฟร์วอล (Internet Firewall)**

ระบบรักษาความปลอดภัยบนอินเทอร์เน็ต หรือที่เรียกว่า อินเทอร์เน็ตไฟร์วอลนี้เป็นระบบหรือกลุ่มของระบบป้องกันที่บังคับใช้นโยบายการรักษาความปลอดภัยระหว่างเครือข่ายขององค์กรกับอินเทอร์เน็ต ไฟร์วอลเป็นตัวกำหนดว่าบริการภายในชนิดใดบ้างที่อาจเข้าถึงได้จากภายนอก ผู้ใช้ภายนอกคนใดที่ได้รับอนุญาตให้เข้าถึงบริการภายในที่ยอมให้ใช้ และบริการภายนอกใดที่อาจเข้าถึงได้โดยผู้ใช้ภายใน ไฟร์วอลสามารถที่จะป้องกันการโจมตีจากภายนอกเครือข่ายได้ โดยจะยอมให้ข้อมูลจากภายนอกที่ไว้ใจได้เท่านั้นสามารถผ่านเข้ามาในระบบเครือข่ายภายในของเรา และจะกรองข้อมูลจากผู้ที่ไม่น่าไว้วางใจ ไม่ให้ผ่านเข้ามาในระบบเครือข่ายได้ และเพื่อให้ไฟร์อวลมีประสิทธิผลการจราจรของข้อมูลทั้งหมดที่ผ่านเข้าออกอินเทอร์เน็ตจะต้องผ่านไฟร์วอลซึ่งเป็นด่านสำหรับตรวจสอบข้อมูล ไฟร์วอลจะยอมให้ผ่านเฉพาะข้อมูลที่ได้รับอนุญาตเท่านั้น และตัวไฟร์วอลเองต้องปลอดจากการบุกรุก ระบบไฟร์วอลไม่สามารถปกป้องสิ่งใดหากผู้โจมตีผ่านไฟร์วอลเข้ามาได้ ซึ่งมีการผลิตโปรดักต์ต่างๆ ที่เกี่ยวกับไฟร์วอลออกมามากมาย ซึ่งขึ้นอยู่กับเราว่าจะเลือกใช้ผลิตภัณฑ์ไฟร์วอลใด

3.2 สิ่งที่ไฟร์วอลทำได้

- สามารถตรวจสอบ และเก็บรายละเอียดกิจกรรมต่างๆ ระหว่างเครือข่ายภายใน และเครือข่ายภายนอก เพราะในการติดต่อทุกอย่างต้องผ่านไฟร์วอล
- สามารถกำหนดกฎเกณฑ์ นโยบายในการอนุญาต หรือไม่อนุญาตในการใช้บริการต่างภายในเครือข่าย
- ไฟร์วอลสามารถใช้ในการแบ่งเครือข่ายออกเป็นส่วนๆ ได้

3.3 สิ่งที่ไฟร์วอลทำไม่ได้

- ไม่สามารถผู้ประสงค์ร้ายที่อยู่ในเครือข่ายภายใน (Internal Network)

ไฟร์วอลไม่สามารถป้องกันผู้ประสงค์ร้ายที่อยู่ในเครือข่ายภายในอยู่แล้ว เปรียบได้กับเราล็อคประตูบ้านไว้อย่างแน่นหนา ทั้งๆ ที่มีโจรอยู่ภายในบ้านอยู่แล้ว

- ไม่สามารถป้องกันการโจมตีที่ไม่ผ่านไฟร์วอล

ตัวอย่างเช่น ผู้ใช้ภายในเครือข่ายมีการเชื่อมต่อกับอินเทอร์เน็ต ในทางอื่นซึ่งไม่ผ่านไฟร์วอล โดยที่ผู้ดูแลระบบไม่รับทราบ เช่น การ Dial-up ไปยังอินเทอร์เน็ตจากเครื่องคอมพิวเตอร์ส่วนตัวที่อยู่ในเครือข่ายภายใน เปรียบได้กับเราล็อคประตูบ้านเรียบร้อยแล้ว แต่มีคนในบ้านเปิดหน้าต่างทิ้งไว้

- ไม่สามารถป้องกันไวรัสได้

เพราะไฟร์วอลไม่สามารถที่จะตรวจดูรายละเอียดข้อมูลภายใน packet ได้ว่ามีไวรัสหรือเปล่า

3.4 นโยบายความปลอดภัยระบบเครือข่าย

แม้ว่ารูปแบบมากมายในการคอนฟิกของการกรองแพ็กเก็ต และเกตเวย์ ซึ่งช่วยในการวางแผนระบบป้องกันไฟร์วอล แต่ผู้ดูแลระบบต้องไม่หลงลืมคำจำกัดความกว้างๆ ของไฟร์วอลซึ่งเป็นการอิมพลีเมนต์นโยบายความปลอดภัยของระบบ (Security Policy) ไฟร์วอลจะช่วยอิมพลีเมนต์นโยบายความปลอดภัยที่พิจารณาเพื่ออนุญาตการบริการ(Service) และการเข้าถึงข้อมูล (Access) ในความหมายไฟร์วอลเป็นทั้งนโยบายและการอิมพลีเมนต์นโยบายนั้นๆ ในรูปแบบของการคอนฟิกเครือข่าย ระบบคอมพิวเตอร์ และเราเตอร์ รวมทั้งมาตรการความปลอดภัยอื่นๆ อย่างเช่น การพิสูจน์ตนรูปแบบใหม่ๆ (Advance Authentication) แทนที่การใช้สแตติกพาสเวิร์ด

นโยบายของระบบเครือข่ายแบ่งออกเป็น 2 ระดับ ซึ่งมีอิทธิพลโดยตรงต่อการออกแบบ ติดตั้ง และใช้งานระบบไฟร์วอลดังนี้

1. **Network service access policy** เป็นนโยบายระดับสูงที่ชี้เฉพาะประเด็นซึ่งระบบอนุญาตหรือไม่อนุญาตการบริการต่างๆ จากเครือข่ายภายนอกที่กำหนดไว้

   ขณะที่เพ่งเล็งไปยังการจำกัดขอบเขต และใช้บริการระหว่างเครือข่าย นโยบายนี้ควรประกอบด้วยการเข้าถึงข้อมูลภายนอกเครือข่ายโดยวิธีอื่นๆ เช่น Dial-in และ Slip/PPP เนื่องจากยิ่งทำการจำกัดขอบเขตการเข้าถึงการบริการก็จะทำให้ยูสเซอร์หาหนทางอื่นเพื่อใช้บริการผ่านอินเทอร์เน็ต ตัวอย่างเช่น ถ้าจำกัดไม่ให้ยูสเซอร์ใช้บริการเว็บผ่านไฟร์วอลไปยังอินเทอร์เน็ต ทำให้ยูสเซอร์บางคนไม่พอใจและสร้างการเชื่อมต่ออินเทอร์เน็ตทางอื่นเช่น Dial-up PPP connection เพื่อใช้บริการเว็บ

   โดยทั่วไปไฟร์วอลจะอิมพลีเมนต์จากนโยบายทั่วไปที่มีอยู่ 2 อย่างคือ

   1) ยอมให้เครือข่ายภายในเข้าถึงอินเทอร์เน็ต แต่ไม่ยอมให้อินเทอร์เน็ตเข้าถึงเครื่องใดๆ ภายในเครือข่าย

2) ยอมให้อินเทอร์เน็ตเข้าถึงได้บางส่วน แต่แค่เพียงระบบที่เลือกไว้ เช่น เซิร์ฟเวอร์ที่ให้บริการข้อมูล (information server) หรือเซิร์ฟเวอร์ให้บริการเมล์ (e-mail server)

ซึ่งบางครั้งไฟร์วอลอิมพลีเมนต์นโยบายที่ยอมให้มีการเข้าถึงจากอินเทอร์เน็ตไปยังเครื่องโฮสต์ที่เลือกไว้ แต่ก็เพียงในกรณีที่จำเป็น และมีการพิสูจน์ตนที่ดีด้วย

2. **Firewall Design Policy** เป็นการระบุกฎที่จะใช้ในการอิมพลีเมนต์นโยบายของข้อแรก บริษัทต้องออกแบบนโยบายเหล่านี้ให้สัมพันธ์กัน และต้องคำนึงถึงไฟร์วอลด้านต่างๆ ดังนี้ คือความสามารถ ขีดจำกัด การคุกคาม และจุดบกพร่องที่เกี่ยวกับโพรโตคอลทีซีพี/ไอพี โดยทั่วไปไฟร์วอลจะอิมพลีเมนต์นโยบายนี้อย่างใดอย่างหนึ่งจาก 2 อย่างพื้นฐานคือ

1. ทุกสิ่งที่ไม่ได้รับอนุญาตเป็นพิเศษจะถูกปฏิเสธ จุดยืนนี้อยู่บนสมมุติฐานที่ว่าไฟร์วอลควรปิดกั้นการจราจรของข้อมูลทั้งหมด และบริการหรือแอพพลิเคชันที่ต้องการควรถูกดำเนินการเป็นกรณีไปนี่คือวิธีที่แนะนำ นโยบายแบบนี้เป็นที่นิยมใช้กันทั่วไปเกือบทุกๆ ที่เพราะมีความปลอดภัยมากกว่าแบบที่ 2 สภาวะแวดล้อมที่สร้างขึ้นจะมีความปลอดภัยมาก เนื่องจากบริการที่ถูกคัดเลือกอย่างระมัดระวังเท่านั้นที่ได้รับการสนับสนุน ข้อเสียของมันคือมันเน้นการรักษาความปลอดภัยมากกว่าความง่ายในการใช้งาน จึงมีตัวเลือกให้กับสังคมของผู้ใช้จำนวนจำกัด
2. ทุกสิ่งที่ไม่ได้ถูกปฏิเสธเป็นพิเศษจะได้รับอนุญาต จุดยืนนี้อยู่บนสมมุติฐานที่ว่าไฟร์วอลควรส่งต่อการจราจรของข้อมูลทั้งหมด และบริการที่อาจมีอันตรายควรถูกปิดเป็นกรณีไป วิธีนี้สร้างสภาวะแวดล้อมที่ยืดหยุ่นมาก พร้อมกับมีบริการให้กับสังคมของผู้ใช้มากกว่า ข้อเสียคือมันเน้นความง่ายในการใช้งานมากกว่าการรักษาความปลอดภัย ผู้ดูแลเครือข่ายจึงรู้สึกต่อต้าน และทำให้ยากขึ้นที่จะรักษาความปลอดภัยเมื่อขนาดของเครือข่ายที่ได้รับการปกป้องขยายขึ้น วิธีนี้เป็นที่นิยมน้อยกว่าแบบแรก เพราะบางครั้งผู้บุกรุกอาจเข้าถึงเครือข่ายภายในโดยเซอร์วิสใหม่ๆ ที่ไม่มีอยู่ในนโยบายความปลอดภัยขององค์กร ตัวอย่างเช่นผู้ประสงค์ร้ายสามารถใช้ denial of service จากพอร์ตทีซีพี/ไอพี ที่ไม่มาตรฐานโจมตีเข้ามาในระบบ ซึ่งจะอยู่นอกเหนือจากการตรวจสอบจากนโยบายขององค์กร

3.5 การออกแบบระบบไฟร์วอล (Designing the firewall system)

การออกแบบไฟร์วอลนั้นคุณต้องเข้าใจและกำหนดขอบเขตระหว่างโดเมนที่ปลอดภัยในเครือข่ายของคุณ โดเมนที่ปลอดภัยในเครือข่ายเป็นเนื้อที่ของเครือข่ายที่อยู่ติดกันที่ปฏิบัติงานภายใต้เครือข่ายเดียวเดียวกัน มีนโยบายในการรักษาความปลอดภัยอย่างเดียวกัน ที่ใดก็ตามที่มีโดเมนเหล่านี้ผ่าน มันจะมีความจำเป็นต้องอาศัยกลไกการแก้ปัญหาระหว่างนโยบายที่ขัดแย้งกันในบริเวณเขตแดนระหว่างโดเมน ซึ่งสิ่งเหล่านี้ไฟร์วอลสามารถช่วยได้

เขตแดนธรรมดาส่วนใหญ่ที่ไฟร์วอลถูกนำมาใช้ในปัจจุบันอยู่ระหว่างเครือข่ายภายในขององค์กรและอินเทอร์เน็ต เมื่อมีการนำไฟร์วอลมาใช้สิ่งแรกที่คุณต้องตัดสินใจเลือกคือโครงสร้างพื้นฐานของไฟร์วอล โครงสร้างในที่นี้หมายความถึงรายการของส่วนประกอบ(ฮาร์ดแวร์ และซอฟแวร์) และกรรมวิธีการเชื่อมต่อ และการกระจายของฟังก์ชันท่ามกลางสิ่งเหล่านี้ มีโครงสร้างของไฟร์วอลอยู่2ประเภทหลักๆ คือ signle layer และ multiple layer architecture

ใน **single layer architecture network** โดยที่ฟังก์ชันทั้งหมดของไฟร์วอลจะประกอบอยู่ภายในโฮสต์ตัวเดียวเท่านั้น และถูกเชื่อมต่อด้วยแต่ละเครือข่ายเพื่อมันจะทำการควบคุมการแอ็กเซส ตัวแปรสำคัญในการเลือกใช้มีราคาเป็นตัวแปรหลัก หรือเมื่อมีเครือข่ายเพียง 2 เครือข่ายที่เชื่อมต่อกัน มันมีประโยชน์ตรงที่ว่าทุกอย่างที่รู้เกี่ยวกับไฟร์วอลล้วนอยู่ในโฮสต์ตัวเดียว ในกรณีที่นโยบายแบบนี้ถูกนำมาใช้ และมีเครือข่ายหลายตัวเชื่อมต่อกัน single layer ยังมี cost-effective สูงมากในการปฏิบัติงานและการบำรุงรักษา ข้อเสียที่ใหญ่ที่สุดของโครงสร้างนี้คือจุดอ่อนในการจัดการกับช่องโหว่หรือ configuration error สืบเนื่องมาจากรูปแบบของมัน ข้อผิดพลาดเพียงจุดเดียวอาจทำให้ไฟร์วอลถูกเจาะได้

multiple layer architecture firewall function ถูกกระจายฟังก์ชันของไฟร์วอลไปยังโฮสต์จำนวนหนึ่งซึ่งมีจำนวนไม่มากนัก การทำเช่นนี้นั้นมีความยุ่งยากในการออกแบบและการปฏิบัติมากกว่าแต่ว่ามีความปลอดภัยมากกว่าโดยการทำการป้องกันให้หลากหลาย ถึงแม้ว่าจะมีราคาแพงกว่าแต่เราก็ยังแนะนำให้เทคโนโลยีที่แตกต่างกันในแต่ละไฟร์วอลโฮสต์เหล่านี้ การทำเช่นนี้จะช่วยลดความเสี่ยงที่เกิดจากจุดอ่อนของผลิตภัณฑ์หรือ configuration error ที่เหมือนกันที่ปรากฏในแต่ละเลเยอร์ การออกแบบธรรมดาส่วนใหญ่ของสถาปัตยกรรมแบบนี้มักเป็นอินเทอร์เน็ตไฟร์วอลที่ประกอบด้วยโฮสต์สองโฮสต์ที่ทำการเชื่อมต่อด้วย DMZ(DeMilitarized Zone) network

เมื่อได้ทำการเลือกโครงสร้างพื้นฐานแล้ว ขั้นตอนต่อไปก็เป็นขั้นตอนของการเลือกฟังก์ชันของไฟร์วอลที่จะใช้ในแต่ละไฟร์วอลโฮสต์ ฟังก์ชันพื้นฐานของไฟร์วอลมีอยู่ 2 ชนิดด้วยกันคือ **packet filtering** และ **application proxies** โดยฟังก์ชันทั้งสองนี้สามารถใช้โดยแยกจากกันหรือใช้ร่วมกันก็ได้ และสามารถใช้ประยุกต์บนไฟร์วอลโฮสต์ตัวเดียวกันหรือต่างกันก็ได้ ในปัจจุบัน packet filtering ได้ร่วมเอาคุณสมบัติบางอย่างของ application proxies ไว้โดยเรียกว่า **stateful inspection packet filters**

มีเหตุผลดีๆ หลายประการในการที่จะใช้ทั้ง packet filtering และ application proxies โดยบางบริการ (เช่น SMTP, HTTP หรือ NTP) มักถูกทำให้ปลอดภัยโดยถูกควบคุมผ่าน packet filtering ขณะที่บริการเช่น DNS, FTP อาจจะต้องการคุณสมบัติบางประการที่มีเฉพาะใน application proxies โดยทั่วไป packet filtering นั้นมีอัตราเร็วมากกว่า application proxies ในกรณีที่เราต้องการอัตราเร็วในการควบคุมการแอ็กเซส และapplication proxies ซึ่งช้านั้นไม่อาจที่จะนำมาใช้ในกรณีนี้ stateful inspection packet filters อาจจะใช้ได้ในกรณีอย่างนี้ ในกรณีอื่นอาจจะเลือกใช้ functionเหล่านี้ตามความเหมาะสม

3.6 การเลือกใช้ฟังก์ชันของไฟร์วอล (Select firewall functions)

3.6.1 แพ็กเก็ตฟิลเตอริง (Packet filtering)

คำว่าแพ็กเก็ตฟิลเตอริง แปลตรงๆ ก็คือการกรองแพ็กเก็ต โดยจะกรอง(ละทิ้ง)แพ็กเก็ตในระหว่าง กระบวนการหาเส้นทาง ดังนั้นการกรองแพ็กเก็ตจึงนำมาใช้ในเราเตอร์เพื่ออนุญาตให้แพ็กเก็ตที่

มากับเครือข่ายที่ถูกอนุญาตเท่านั้นที่ผ่านไปได้ การนำ การกรองแพ็กเก็ตมาใช้นั้นเป็นวิธีการประหยัดในการเพิ่มความสามารถของไฟร์วอลให้กับเราเตอร์ การตัดสินใจในการกรองแพ็กเก็ตเหล่านี้ โดยยึดข้อมูลที่อยู่ในแพ็กเก็ตเฮดเดอร์ (packet header) ของแพ็กเก็ตตัวนั้นๆ เช่น แอดเดรสต้นทาง (Source Address) แอดเดรสปลายทาง (Destination Address) พอร์ต (Port) โพรโตคอล (Protocol) ผลิตภัณฑ์ไฟร์วอลบางตัวที่สามารถกรองแพ็กเก็ต ยังมีความสามารถในการกรองข้อมูลในส่วนอื่นที่ไม่ใช่แพ็กเก็ตเฮดเดอร์ แต่เราจะพิจารณาส่วนนี้ในหัวข้อของ stateful inspection packer filter

การกรองแพ็กเก็ตถูกนำมาประยุกต์ใช้ในแพลตฟอร์ม 2 รูปแบบด้วยกันคือ

1. คอมพิวเตอร์ที่ใช้งานโดยทั่วไปทำงานเป็นเราเตอร์
2. เราเตอร์ที่มีจุดประสงค์ในการใช้งานโดยเฉพาะ

ตารางดังต่อไปนี้แสดงข้อดีและข้อเสียในแต่ละแพลตฟอร์ม

	คอมพิวเตอร์ทั่วไปที่ทำหน้าที่เป็นเราเตอร์	**เราเตอร์ที่มีวัตถุประสงค์พิเศษ**
ข้อดี	- ความยืดหยุ่นในการทำงานไม่จำกัด	- ประสิทธิภาพสูงสุด - จำนวนการเชื่อมต่อมาก
ข้อเสีย	- ประสิทธิภาพปานกลาง - จำนวนการเชื่อมต่อมีไม่มาก - ความอ่อนแอของระบบปฏิบัติการ (Operating System)	- ความยืดหยุ่นในการทำงานต่ำ - อาจจะต้องการเมโมรีมากขึ้น

ตารางที่ 3-1 แสดงข้อดี ข้อเสียของแต่ละแพลตฟอร์ม

เราเตอร์ที่ใช้ในงานโดยเฉพาะนั้นผู้ผลิตได้นำความสามารถในการกรองแพ็กเก็ตเพิ่มเข้าไปในผลิตภัณฑ์เราเตอร์ของพวกเขาเพื่อให้ผลิตภัณฑ์ของพวกเขามีความสามารถในการควบคุมการแอ็กเซสตามความต้องการของลูกค้า อย่างไรก็ตามพวกเขาเป็นผู้ผลิตเราเตอร์ไม่ได้เป็น ผู้ผลิตผลิตภัณฑ์รักษาความปลอดภัย ดังนั้นเมื่อพวกเขาทำการออกแบบโดยทำการเลือกระหว่างฟังก์ชันในการหาเส้นทาง กับฟังก์ชันการทำงานของระบบรักษาความปลอดภัย พวกเขาจะเลือกการหาเส้นทาง ซึ่งฟังก์ชันในการหาเส้นทางนี้มักจะเป็นปัจจัยที่มีความสำคัญสูงสุดในการออกแบบเราเตอร์ การเพิ่มฟังก์ชันการกรองแพ็กเก็ตเข้าไปในเราเตอร์ ทำให้เกิดสิ่งต่างๆ ดังนี้

- มีผลกระทบต่อการทำการหาเส้นทางในเครือข่าย และประสิทธิภาพของเราเตอร์
- อาจจะต้องเพิ่มหน่วยความจำลงในเราเตอร์

คอมพิวเตอร์ที่ใช้ในงานทั่วไปกับระบบปฏิบัติการที่ไม่ได้ถูกออกแบบมาเพื่อใช้ในการทำงานเป็นเราเตอร์ ดังนั้นจึงมีประสิทธิภาพในการทำงานสู้เราเตอร์ไม่ได้ เหตุผลส่วนใหญ่ในการนำคอมพิวเตอร์ที่ใช้ในงานทั่วไปมาทำเป็นไฟร์วอลที่มีความสามารถในการกรองแพ็กเก็ตมีดังนี้

- สามารถเพิ่มกลไกการทำงานอื่นๆ ของไฟร์วอล นอกจากการกรองแพ็กเก็ตได้บนโฮสต์ตัวเดียวกัน

- เป็นแพลตฟอร์มที่เรารู้จักเป็นอย่างดี และรู้มากกว่าตัวเราเตอร์ที่ทำงานเฉพาะอย่าง
- ช่วยลดภาระในการกรองแพ็กเก็ตของเราเตอร์ที่ทำงานเฉพาะอย่าง
- สามารถใช้ซอร์ซโค้ดที่เราเขียนเอง หรือซื้อมามาใช้ได้

3.6.2 แอพพลิเคชันพร็อกซี (Application Proxies)

แอพพลิเคชันพร็อกซีเป็นโปรแกรมแอพพลิเคชันที่รันอยู่บนระบบไฟร์วอลระหว่างสองเครือข่าย โดยเครื่องที่รันพร็อกซีไม่ต้องทำตัวเป็นเราเตอร์ เมื่อโปรแกรมจากเครื่องไคลเอ็นต์เริ่มการติดต่อผ่านพร็อกซีไปยังเครื่องที่ให้บริการปลายทาง เริ่มแรกต้องทำการติดต่อกับโปรแกรมพร็อกซีเซิร์ฟเวอร์ก่อน โดยตัวไคลเอ็นต์จะทำการเจรจากับพร็อกซีให้ทำการติดต่อกับเครื่องที่ให้บริการปลายทางให้ ถ้าเป็นผลสำเร็จจะเกิดการเชื่อมต่อ 2 การเชื่อมต่อคือระหว่างเครื่องไคลเอ็นต์กับเครื่องพร็อกซีเซิร์ฟเวอร์ และระหว่างเครื่องพร็อกซีกับเครื่องให้บริการปลายทาง เราจะเห็นได้ว่าพร็อกซีจะรับภาระของการจราจรสองทิศทางระหว่างเครื่องไคลเอ็นต์กับเครื่องพร็อกซีเซิร์ฟเวอร์ จะทำการสร้างการติดต่อทั้งหมดและทำหน้าที่ในการตัดสินใจในการทำฟอร์เวิร์ดแพ็กเก็ตด้วย โดยพร็อกซีนี้ไม่มีส่วนเกี่ยวข้องในส่วนของการหาเส้นทาง

ทำนองเดียวกับแพ็กเก็ตฟิลเตอริง ในแอพพลิเคชันพร็อกซีนั้นก็สามารถทำงานได้ในสองแพลตฟอร์ม คือ อุปกรณ์ที่ทำหน้าที่เป็นพร็อกซีโดยเฉพาะ กับคอมพิวเตอร์ที่ใช้ในงานทั่วไป ซึ่งโดยทั่วไปแล้วแอพพลิเคชันพร็อกซีจะช้ากว่าเราเตอร์ที่ใช้กรองแพ็กเก็ต แต่ในขณะเดียวกันแอพพลิเคชันพร็อกซีมีความปลอดภัยสูงกว่าแพ็กเก็ตฟิลเตอริง โดยที่จริงแพ็กเก็ตฟิลเตอริงสามารถทนรับการข้อบกพร่องจากการอิมพลีเมนต์ หรือทดแทนในส่วนของการอิมพลีเมนต์การเราต์ของระบบปฏิบัติการ แต่เมื่อความสามารถของแพ็กเก็ตฟิลเตอริงถูกเพิ่มเข้าไปในการหาเส้นทาง มันก็ไม่สามารถที่จะชดเชยหรือทำให้ข้อบกพร่องในการหาเส้นทางถูกต้องได้

ผลจากการทำการกรองที่ซับซ้อนขึ้นและการตัดสินใจในการควบคุมการเข้าถึงแอพพลิเคชันพร็อกซี สามารถใช้ทรัพยากรคอมพิวเตอร์ที่สำคัญ และเครื่องราคาแพงที่ใช้ในการปฏิบัติงาน ตัวอย่างเช่น ถ้าไฟร์วอลที่ทำงานบนระบบยูนิกซ์ ต้องการที่จะให้สนับสนุนการทำงานจำนวน 200 HTTP session ที่ทำงานพร้อมๆ กัน เครื่องที่ใช้ต้องมีความสามารถในการสนับสนุนงานของ 200 HTTP proxy ด้วยเหตุผลในแง่ของประสิทธิภาพในการส่ง/รับข้อมูล และเมื่อเพิ่มอีก 100 FTP session, 25 SMTP session , LDAP session ส่วนหนึ่ง และ DNS transaction คุณจะต้องใช้เครื่องที่สนับสนุน 500-1000 proxy process บางพร็อกซีอาจจะอิมพลีเมนต์โดยใช้ kernel threads (เพื่อช่วยลดความต้องการของทรัพยากรลงอย่างรวดเร็ว) แต่ความต้องการในทรัพยากรก็ยังคงมากอยู่ดี

3.6.3 สเตตฟูลอินสเป็กชัน (Stateful Inspection) หรือ ไดนามิกแพ็กเก็ตฟิลเตอริง (Dynamic packet filtering)

เราใช้คำว่า สเตตฟูลอินสเป็กชัน หรือ ไดนามิกแพ็กเก็ตฟิลเตอริง หมายถึง เซตของฟังก์ชันที่ทำการกรองแพ็กเก็ตที่มีความสามารถมากขึ้นในเราเตอร์ โดยที่แพ็กเก็ตฟิลเตอริงถูกจำกัดอยู่ในการตัดสินใจโดยข้อมูลในการตัดสินใจจะอยู่ในส่วนของเฮดเดอร์เท่านั้น และจะพิจารณาเฉพาะแพ็กเก็ตตัวนั้นๆ เท่านั้น โดยไม่ได้คำนึงถึงแพ็กเก็ตก่อนหน้านี้ ส่วนสเตตฟูลอินสเป็กชันจะเอาชนะในข้อจำกัดนี้ของแพ็ก

เก็ตฟิลเตอริง ทั้งในส่วนของข้อมูลที่ใช้ในการตัดสินใจ โดยจะดูถึงข้อมูลในส่วนของเมสเซจด้วยและจะคำนึงถึงในส่วนของแพ็กเก็ตอื่นๆ ที่อยู่ก่อนหน้านี้ประกอบในการตัดสินใจ ทำให้ความสามารถในการตัดสินใจมากขึ้น เพราะรู้ข้อมูลมากขึ้น ซึ่งสเตตฟูลอินสเป็กชันก็เหมือนกับแพ็กเก็ตฟิลเตอริง คืออยู่ในอิมพลีเมนต์เพิ่มลงในเราเตอร์ ดังนั้นโฮสต์ที่มีฟังก์ชันของสเตตฟูลอินสเปคชันทำงานอยู่นั้นจะต้องเป็นหรือสามารถทำงานเสมือนเป็นเราเตอร์ได้ด้วย

เจตนาพื้นฐานของสเตตฟูลอินสเป็กชันนั้นเพื่อรวมข้อดีระหว่างประสิทธิภาพในแง่ของการส่งถ่ายข้อมูลและความปลอดภัย โดยการเพิ่มการทำงานลงในเราเตอร์ทำให้สเตตฟูลอินสเปคชันมีประสิทธิภาพในการส่งถ่ายข้อมูลดีกว่าพร็อกซี และยังมีการเพิ่มระดับของฟังก์ชันของไฟร์วอลให้ดีกว่าแพ็กเก็ตฟิลเตอริงธรรมดา และสเตตฟูลอินสเป็กชันยังมีส่วนคล้ายกับพร็อกซีคือ เกณฑ์ของการควบคุมการเข้าถึงข้อมูลที่ซับซ้อนสามารถจะระบุรายละเอียดได้ และเหมือนกับแพ็กเก็ตฟิลเตอริง คือสเตตฟูลอินสเป็กชันได้รับการสืบทอดมาจากการอิมพลีเมนต์การหาเส้นทางที่มีคุณภาพสูง

ฟังก์ชัน	Packet Filtering (PF)	Application Proxy (AP)	Stateful Inspection (SI)
Platform	ทั้งคอมพิวเตอร์จุดประสงค์พิเศษ และคอมพิวเตอร์ทั่วไป	ทั้งคอมพิวเตอร์จุดประสงค์พิเศษ และคอมพิวเตอร์ทั่วไป	ทั้งคอมพิวเตอร์จุดประสงค์พิเศษ และคอมพิวเตอร์ทั่วไป
Protocol/Service	ใดๆ ก็ได้	เพียงแค่ที่ระบุ	ใดๆ ก็ได้
Support	ทั้ง vendor และsite support	ทั้ง vendor และsite support	ทั้ง vendor และsite support
Security	ต่ำ	สูง	ปานกลาง
Performance	สูง	ต่ำ	ปานกลาง

ตารางที่ 3-2 แสดงลักษณะการทำงานโดยทั่วไปของไฟร์วอลแต่ละประเภท

3.7 ฟังก์ชันของไฟร์วอลที่ทำงานอยู่ใน OSI Layer

ฟังก์ชันของไฟร์วอลแต่ละอย่างจะทำงานอยู่ในเลเยอร์ใน OSI Model ที่ต่างกัน ดังแสดงในตารางข้างล่างนี้ โดยที่แอพพลิเคชันพร็อกซีจะทำงานอยู่ในชั้นแอพพลิเคชันเลเยอร์ ส่วนแพ็กเก็ตฟิลเตอริงจะทำงานอยู่ในชั้นล่างๆ ตั้งแต่ชั้นทรานสปอร์ตเลเยอร์ลงไป และสุดท้ายคือสเตตฟูลอินสเป็กชันสามารถทำงานได้ทุกชั้นของ OSI Model

OSI Layer	Policy Criteria	Firewall Service
Application Layer	ระบุ Application	ระบุ Application Proxy ระบุ Application Filtering
Presentation Layer	ไม่มี	ไม่มี
Session Layer	บ่งชี้ผู้ใช้ (user identity)	User mapping (gateway)

		User filtering
Transport Layer	Source Port Number Destination Port Number Protocol State	Port Number Mapping (gateway) Port Number Filtering Stateful Filtering
Network Layer	Source IP Address Destination IP Address Protocol Type	Address Mapping (gateway) Address filtering Protocol filtering
Data Link Layer	Source MAC Address Protocol Type	Address filtering Protocol filtering
Physical Layer	Electronic signaling	ไม่มี

ตารางที่ 3-3 แสดงประเภทของไฟร์วอลที่ทำงานใน OSI Layer

3.8 การเปรียบเทียบฟังก์ชันของไฟร์วอล

ฟังก์ชันของไฟร์วอล	ข้อดี	ข้อเสีย
Packet Filtering	- เร็ว - ง่ายต่อการอิมพลีเมนต์ - ประกอบด้วย IP ทุก traffic - ไม่มีการเปลี่ยนแปลงที่เครื่องไคลเอ็นต์	- ไม่ยืดหยุ่น - ไม่มีการแบ่งแยก - ไม่มีการทำพิสูจน์ตนระดับยูเซอร์ - สามารถทำการเก็บล็อกได้ แต่ไม่เหมาะสมที่จะปฏิบัติ
Application Proxy	- ระบุความปลอดภัยระดับระดับแอพพลิเคชันเลเยอร์ - สามารถทำการเก็บล็อกระดับแอพพลิเคชันเลเยอร์ - สามารถทำการพิสูจน์ระดับยูสเซอร์ได้ - สามารถทำ Isolation	- ช้า - ใช้ทรัพยากรมาก - ความหนาแน่นในการประมวลผลสูง - ขึ้นอยู่กับแอพพลิเคชัน - ปกติจะบล็อก UDP - ต้องทำการพิสูจน์ตนใหม่
Stateful Inspection	- สามารถใช้ได้กับทุกแอพพลิเคชัน - รู้สถานะของข้อมูลในทุกเลเยอร์ - ข้อมูลสถานะยืดหยุ่นได้	- ยากในการจัดการ และการคอนฟิก - ต้องรู้กฎขององค์กร

ตารางที่ 3-4 แสดงข้อดี-ข้อเสียของไฟร์วอลแต่ละประเภทที่ทำงานใน OSI Layer

3.9 การเลือกโทโปโลยีของไฟร์วอล (Selecting the firewall topology)

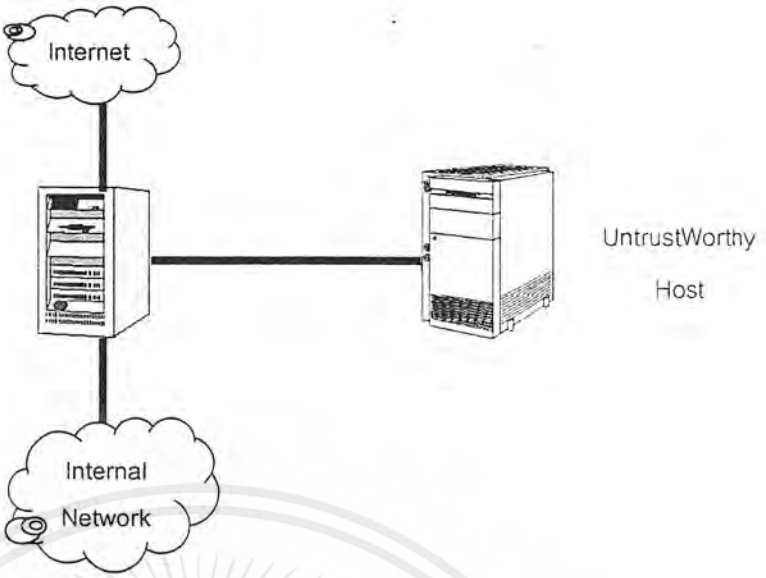
เบสิกบอร์เดอร์ไฟร์วอล (Basic border firewall)

โทโปโลยีนี้เป็นจุดเริ่มต้นของไฟร์วอลทั้งหมด โดยเบสิกบอร์เดอร์ไฟร์วอลเป็นโฮสต์ตัวเดียวที่มีการเชื่อมต่อระหว่างเครือข่ายภายในขององค์กร และเครือข่ายที่ไม่น่าเชื่อถือจำนวนหนึ่ง ซึ่งโดยทั่วไปแล้วเป็นอินเทอร์เน็ต ในลักษณะแบบนี้ฟังก์ชันของไฟร์วอลทั้งหมดจะถูกบรรจุอยู่ในโฮสต์ตัวเดียว

รูปที่ 3-1 แสดง Basic Border Firewall (Single Layer)

โฮสต์ที่ไม่น่าเชื่อถือหรือไม่ปลอดภัย (Untrustworthy host)

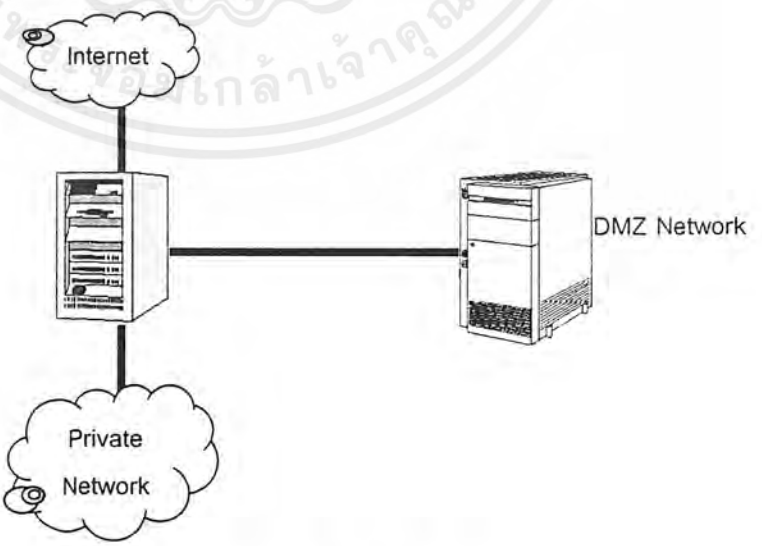
ที่เบสิกบอร์เดอร์ไฟร์วอลเพิ่มโฮสต์ที่อยู่บนเครือข่ายที่ไม่น่าเชื่อถือ ที่ที่ไฟร์วอลไม่สามารถป้องกันได้ โดยโฮสต์นั้นมีการคอนฟิกที่เล็กที่สุดและถูกบริหารอย่างระมัดระวังที่จะให้มันปลอดภัยเท่าที่จะเป็นไปได้ ไฟร์วอลถูกคอนฟิกเพื่อต้องการให้การสัญจรที่เข้าไป และออกมาจากเครือข่ายเคลื่อนผ่านโฮสต์ที่ไม่น่าเชื่อถือ (untrustworthy host)นี้ โฮสต์นี้ถูกอ้างถึงว่าเป็นโฮสต์ที่ไม่น่าเชื่อถือ(ไม่ปลอดภัย) เพราะมันไม่ได้ถูกป้องกันโดยไฟร์วอล แม้กระนั้นก็ตามโฮสต์ที่อยู่ในเครือข่ายที่เชื่อถือได้ก็ยังความความน่าเชื่อถือในระดับหนึ่งที่จำกัดอยู่



รูปที่ 3-2 แสดง Basic Border Firewall ที่มี untrustworthy host

เครือข่าย DMZ (DMZ Network)

ในDMZ network โฮสต์ที่ไม่น่าเชื่อถือ หรือโฮสต์ที่มีความปลอดภัยต่ำถูกนำไปไว้ภายในไฟร์วอล แต่ไม่ได้อยู่ในเครือข่ายภายใน โดยการทำเช่นนี้ไฟร์วอลโฮสต์จะทำการเชื่อมต่อกับสามเครือข่าย และโดยการทำเช่นนี้เป็นการเพิ่มประสิทธิภาพของ ความปลอดภัย ความน่าเชื่อถือ และความสามารถในการนำมาใช้งานของโฮสต์ที่ไม่น่าเชื่อถือ แต่ไม่ได้เพิ่มระดับของความปลอดภัยในการแอ็กเซสจากโฮสต์ที่อยู่ในภายในเครือข่าย โฮสต์ที่ไม่น่าเชื่อถือมีเพื่อจุดประสงค์ต่างๆ กัน (ตัวอย่างเช่น FTP server และเว็บไซต์สาธารณะ) สามารถที่จะถูกนำมาไว้ใน DMZ network ได้อย่างง่ายดาย เป็นการสร้างเครือข่ายบริการสาธารณะ



รูปที่ 3-3 แสดง Basic Border Firewall with DMZ Network

ดูอัลไฟร์วอล (Dual firewall)

เครือข่ายภายในขององค์กรจะส่งเสริมให้อยู่แยกกับเครือข่ายที่ไม่น่าเชื่อถือโดยการเพิ่มไฟร์วอลโฮสต์ตัวที่สองลงไป โดยการเชื่อมต่อเครือข่ายที่ไม่น่าเชื่อถือกับไฟร์วอลตัวแรกเรียกไฟร์วอลตัวนี้ว่าไฟร์วอลภายนอก (outer firewall) ส่วนการเชื่อมต่อเครือข่ายภายในองค์กรกับไฟร์วอลอีกตัวเรียกไฟร์วอลตัวนี้ว่าไฟร์วอลภายใน (inner firewall) และเครือข่าย DMZ อยู่ระหว่างไฟร์วอลทั้งสอง ทางเดินของข้อมูลระหว่างเครือข่ายภายใน และอินเทอร์เน็ตจะต้องผ่านมายังไฟร์วอลทั้งสอง และเครือข่าย DMZ

รูปที่ 3-4 แสดงดูอัลไฟร์วอล (Dual firewall)

3.10 ปัจจัยในการพิจารณาการออกแบบไฟร์วอล

เมื่อออกแบบอินเทอร์เน็ตไฟร์วอลผู้ดูแลเครือข่ายมีสิ่งที่ต้องตัดสินใจดังนี้

- ความปลอดภัย

ความปลอดภัยนั้นเป็นปัจจัยหลัก และเป็นสิ่งที่สำคัญมากสำหรับการออกแบบ เพราะปกติไฟร์วอลเป็นระบบที่ใช้ในการรักษาความปลอดภัยของระบบเครือข่ายอยู่แล้ว ซึ่งปัจจุบันนี้มีบริษัทที่ผลิตไฟร์วอลเพิ่มขึ้นมากมาย ดังนั้นผู้ดูแลระบบควรจะต้องเลือกไฟร์วอลที่มีการรักษาความปลอดภัยที่ดี ซึ่งอาจจะเลือกใช้ผลิตภัณฑ์ไฟร์วอลจากหลายๆ แหล่งก็ได้ ตัวอย่างเช่น การใช้ multiple firewall system ที่มาจากผู้ผลิตหลายราย เพื่อลดข้อบกพร่องที่มี จากการใช้ผลิตภัณฑ์ตัวเดียว

- ความซับซ้อนในการจัดการ และการคอนฟิกูเรชัน

การจัดการ และการคอนฟิกก็เป็นปัจจัยที่สำคัญอย่างหนึ่งที่ต้องคำนึงถึง เพราะการมีระบบไฟร์วอลที่สามารถจัดการ และตั้งค่าได้ง่ายจะทำให้สะดวกกับผู้ดูแลระบบสำหรับการปรับเปลี่ยนให้ตรงตามนโยบายความปลอดภัยของเครือข่าย และยังทำให้เกิดความผิดพลาดน้อยลงในการเซตค่าต่างๆ ด้วย ในทางตรงข้ามถ้ามีความซับซ้อนมากในการจัดการก็อาจจะทำให้เกิดความผิดพลาดในการตั้งค่าให้กับไฟร์วอล ซึ่งจะนำไปสู่ช่องโหว่ในการโจมตีของผู้ประสงค์ร้าย

- ประสิทธิภาพในการส่งถ่ายข้อมูล

อาจต้องใช้โฮสต์ที่เป็นไฟร์วอลหลายๆ ตัว เพื่อกระจายทราฟฟิกซึ่งเกิดขึ้นในเครือข่ายให้อยู่ในเกณฑ์ที่น่าพอใจ นอกจากนี้ยังต้องพิจารณาในด้านราคาด้วย เพราะยิ่งเพิ่มจำนวนโฮสต์ที่เป็นไฟร์วอลราคาก็สูงตามไปด้วย

- ความน่าเชื่อถือ

ไฟร์วอลต้องมีเสถียรภาพในการทำงาน โดยการทำงานของมันจะต้องทำงานได้อย่างคงเส้นคงวา สามารถใช้งานได้นานโดยไม่มีความผิดพลาดเกิดขึ้นบ่อย และยังสามารถทำงานได้ต่อไปเหมือนเดิมแต่ก็ต้องมีการดูแลสม่ำเสมอเป็นอย่างดี

- นโยบายการรักษาความปลอดภัยขององค์กร

ดังที่กล่าวมาแล้วว่าอินเทอร์เน็ตไฟร์วอลไม่ได้ยืนโดยลำพัง มันเป็นส่วนหนึ่งของนโยบายการรักษาความปลอดภัยโดยรวมขององค์กร ซึ่งกำหนดแนวป้องกันทุกๆ ด้าน การที่จะประสบความสำเร็จองค์กรต้องรู้จักสิ่งที่ต้องปกป้อง นโยบายการรักษาความปลอดภัยต้องตั้งอยู่บนการวิเคราะห์ระบบรักษาความปลอดภัย การประเมินความเสี่ยงและการวิเคราะห์ความต้องการขององค์กรซึ่งต้องถูกควบคุมอย่างรอบคอบ ถ้าองค์กรไม่มีนโยบายการรักษาความปลอดภัย ถึงแม้จะใช้ไฟร์วอลที่รอบคอบที่สุดก็สามารถถูกเปิดกว้างให้โจมตีได้

- ค่าใช้จ่ายของไฟร์วอล

ยิ่งไฟร์วอลที่มีความสามารถสูงในด้านต่างๆ ราคาก็จะสูงตามไปด้วย จึงมีคำถามว่าการรักษาความปลอดภัยขนาดไหนที่องค์กรสามารถจ่ายได้ ? ไฟร์วอลแบบกรองแพ็กเก็ตอย่างง่ายอาจมีค่าใช้จ่ายต่ำที่สุดเนื่องจากองค์กรต้องการแค่เราเตอร์ตัวหนึ่งต่อกับอินเทอร์เน็ต และการกรองแพ็กเก็ตถูกรวมเป็นส่วนหนึ่งในคุณสมบัติของเราเตอร์มาตรฐาน ระบบไฟร์วอลในทางการค้ายิ่งให้ความปลอดภัยมากขึ้น ค่าใช้จ่ายก็ยิ่งมากขึ้น ซึ่งขึ้นอยู่กับความซับซ้อนของมันแบะจำนวนของระบบที่ได้รับการปกป้อง ถ้าองค์กรมีผู้เชี่ยวชาญอาจสร้างไฟร์วอลขึ้นเองจากซอฟต์แวร์ที่มีอยู่ทั่วไป แต่ก็ยังคงมีค่าใช้จ่ายในรูปของเวลาที่ใช้พัฒนาและจัดระบบไฟร์วอล ท้ายที่สุดไฟร์วอลทั้งหมดต้องการการสนับสนุนอย่างต่อเนื่องสำหรับการบริหาร การบำรุงรักษาทั่วไป การปรับปรุงซอฟต์แวร์ การแก้ไขในด้านความปลอดภัย และการรับมือกับเหตุการณ์ที่ไม่คาดคิด

บทที่ 4
หลักการทั่วไปในการทดสอบระบบไฟร์วอล

4.1 จุดประสงค์ในการทดสอบ

จุดประสงค์ของการทดสอบก็เพื่อที่จะตรวจสอบว่าระบบไฟร์วอลทำงานได้อย่างที่เราต้องการหรือเปล่า โดยควรจะต้องทำสิ่งเหล่านี้

- ทดสอบเพื่อจำลองการทำงานของไฟร์วอล อย่างเช่น การเราติ้ง (routing) การกรองแพ็กเก็ต (packet filtering) การเก็บล็อก (logging) ความสามารถในการเตือนเมื่อเกิดเหตุการณ์ผิดปกติ
- ทดสอบเพื่อวัดความสามารถของไฟร์วอลที่ใช้ในด้านต่างๆ คือ ด้านความปลอดภัย (Security) ด้านการจัดการ (Management) ด้านประสิทธิภาพ (Performance)
- ทดสอบความสามารถของไฟร์วอลเพื่อนำข้อมูลที่ได้ไปทำการเปรียบเทียบข้อเด่นข้อด้อยของไฟร์วอลแต่ละตัว ซึ่งนำไปเป็นแนวทางในการเลือกใช้ไฟร์วอลให้เหมาะสมสำหรับเครือข่ายขององค์กร

การทดสอบระบบไฟร์วอล และตรวจสอบการทำงานอย่างถูกต้องจะช่วยเพิ่มความมั่นใจว่ามันจะสามารถทำงานได้อย่างที่ได้ออกแบบ

สาเหตุธรรมดาที่สุดที่ทำให้เกิดช่องโหว่ในความปลอดภัยของไฟร์วอลก็คือ การคอนฟิกที่ผิดพลาดของระบบไฟร์วอล การที่จะทำให้รู้สิ่งเหล่านี้ได้ก็โดยการทดสอบการคอนฟิกระบบอย่างละเอียด

4.2 ส่วนประกอบของระบบที่ทดสอบ

ส่วนประกอบต่างๆ ที่อยู่ในระบบไฟร์วอลที่นำมาทดสอบมีดังนี้

- ฮาร์ดแวร์ (ซีพียู ดิสก์ หน่วยความจำ การ์ดแลน)
- โปรแกรมระบบปฏิบัติการ เช่น วินโดว์สเอ็นทีเซิร์ฟเวอร์ ยูนิกซ์ เป็นต้น
- โปรแกรมไฟร์วอล
- โปรแกรมที่ใช้คอนฟิกไฟร์วอล เช่น กฎการเราต์ (routing rules) กฎการกรองแพ็กเก็ต (packet filtering rules) การเก็บล็อกไฟล์ (logging) การแจ้งเตือน (alert)
- อุปกรณ์การเชื่อมต่อเครือข่าย เช่น สายเคเบิล สวิทซ์ ฮับ ฯลฯ

4.3 การวางแผนการทดสอบ

คุณจำเป็นต้องวางแผนการทดสอบทั้งการอิมพลีเมนต์ระบบไฟร์วอล และนโยบายที่จะใช้ในระบบที่จะทดสอบ เพื่อที่จะทำการทดสอบการอิมพลีเมนต์ต้องทำดังนี้

1. กำหนดโครงสร้างทางกายภาพของเครือข่ายที่ต้องการทดสอบ เป็นการกำหนดโทโปโลยีในการเชื่อมต่อของเครือข่าย

2. กำหนดนโยบายความปลอดภัยของเครือข่าย (Security Policy) ซึ่งเป็นส่วนสำคัญที่จะนำไปกำหนดการคอนฟิกไฟร์วอล
3. จัดทำรายการขององค์ประกอบที่ต้องการทดสอบ เช่น ต้องการทดสอบการทำงานโปรแกรมเทลเน็ตผ่านไฟร์วอล
4. จัดทำรายการสั้นๆ ของการโจมตีที่สามารถเกิดขึ้นจากเครือข่ายภายนอก และมีผลกระทบต่อการทำงานของไฟร์วอล เช่น การโจมตีด้วยดาเนียลออฟเซอร์วิส (Denial of Services)
5. จัดทำรายการของความล้มเหลวที่มีโอกาสเกิดขึ้น และมีผลกระทบต่อการทำงานของไฟร์วอล ตัวอย่างหนึ่งของ Scenario สมมุติว่าโฮสต์ในระบบซึ่งไฟร์วอลทำงานอยู่เกิดทำงานล้มเหลวของฮาร์แวร์ โดยไม่สามารถกู้คืนได้ ซึ่งจะขัดขวางการส่งต่อแพ็กเก็ตไปยังเครื่องอื่น (packet forwarding) ซึ่งอาจเกิดขึ้นจากการ์ดแลนเสีย หนทางหนึ่งที่จะทดสอบความล้มเหลวนี้ได้โดยการถอดสายที่เชื่อมต่อจากจุดเชื่อมต่อเพื่อจำลองลักษณะของความล้มเหลวนั้น

การทดสอบนโยบายที่ติดตั้งในระบบเป็นเรื่องที่ยากกว่าที่กล่าวข้างต้น มันไม่มีความยืดหยุ่นในการคอนฟิก IP packet filterให้ครบทั้งหมดเพราะมันมีความเป็นไปได้มากมายในการคอนฟิก เราแนะนำว่าแทนที่จะใช้การทดสอบอย่างละเอียดทั้งหมด ก็ควรใช้วิธีการกำหนดขอบเขตที่จะทดสอบแทน โดยในการทดสอบให้คุณระบุขอบเขตของกฎที่ใช้ในการกรองแพ็กเก็ต และสร้างตัวอย่างการทดสอบที่อยู่ใกล้ชิดกันในแต่ละขอบเขต ทำดังนี้

- สำหรับแต่ละกฎ คุณต้องระบุทุกขอบเขตภายในกฎ โดยทั่วไปพารามิเตอร์หรือแอตทริบิวต์ที่อยู่ภายในกฎจะสามารถแบ่งออกเป็น 1 หรือ 2 ขอบเขต ซึ่งปกติแอตทริบิวต์มีดังนี้คือ
  - โพรโตคอล (Protocol)
  - แอดเดรสต้นทาง (Source Address)
  - แอดเดรสปลายทาง (Destination Address)
  - พอร์ตต้นทาง (Source Port)
  - พอร์ตปลายทาง (Destination Port)

โดยพื้นฐานแล้วทุกๆ แอตทริบิวต์ของแพ็กเก็ตที่ถูกตรวจสอบจากกฎที่ใช้กรองแพ็กเก็ต จะสามารถระบุขนาดหนึ่งของพื้นที่ได้ ตัวอย่างเช่น กฎที่อนุญาตให้แพ็กเก็ตที่เป็นทีซีพี ผ่านจากโฮสต์ใดๆ ไปยังเว็บเซิร์ฟเวอร์ ผ่านพอร์ต 80 โดยตรวจสอบ 3 แอตทริบิวต์ (โพรโตคอล แอดเดรสปลายทาง และพอร์ตปลายทาง) ซึ่งแบ่งแอตทริบิวต์เป็น 3 พื้นที่ว่าง คือพอร์ตน้อยกว่า 80 พอร์ต 80 และพอร์ตที่มากกว่า 80

สำหรับแต่ละขอบเขต ให้คุณสร้างการทดสอบที่อยู่ภายในขอบเขตนั้นๆ คุณต้องตรวจสอบว่าไฟร์วอลจะปฏิเสธหรือส่งต่อทุกๆ แพ็กเก็ตสำหรับขอบเขตที่ให้มา ซึ่งภายในขอบเขตเดียวๆ นั้นทุกๆ ทราฟฟิกควรจะส่งต่อหรือมิฉะนั้นก็ปฏิเสธอย่างใดอย่างหนึ่ง นี่คือจุดประสงค์ของการแบ่งพื้นที่ของแอตทริบิวต์

4.4 เครื่องมือทั่วไปที่ใช้ในการทดสอบระบบไฟร์วอล

มีการพัฒนาเครื่องมือที่ใช้ในการทดสอบความสามารถของไฟร์วอล (Firewall test tool) ซึ่งแบ่งออกเป็นชนิดต่างๆ ดังนี้

- เน็ตเวิร์กทราฟฟิกเจเนเรเตอร์ (network traffic generators) อย่างเช่น SPAK (Send PacKets) ipsend หรือ Ballista
- เน็ตเวิร์กมอนิเตอร์ (network monitors) เช่น tcpdump และ Network Monitor
- พอร์ตสแกนเนอร์ (portscanners) เช่น strobe และ nmap
- เครื่องมือในการสำรวจช่องโหว่ (vulnerability detection tools)
- ระบบตรวจจับ (intrusion detection systems) เช่น NFR (Network Flight Recorder) หรือ Shadow

4.5 ประเภทของการทดสอบ

การทดสอบไฟร์วอลเราสามารถแบ่งออกเป็น 3 ด้านหลัก เรียงตามความสำคัญคือด้านความปลอดภัย ด้านการจัดการ ด้านประสิทธิภาพ

4.5.1 ด้านความปลอดภัย

เป็นด้านที่มีความสำคัญที่สุดในการทดสอบไฟร์วอล เพราะจุดประสงค์ของไฟร์วอลก็คือการรักษาความปลอดภัยระบบเครือข่าย ซึ่งการทดสอบด้านนี้จะเป็นการตรวจสอบหาจุดบกพร่องในการรักษาความปลอดภัยของไฟร์วอล ซึ่งมีเครื่องมือจำนวนมากที่สามารถใช้ตรวจหาจุดบกพร่องของโฮสต์แต่ละตัวบนระบบเครือข่าย ซึ่งในทางตรงข้ามเครื่องมือเหล่านี้ก็จะเป็นเครื่องมือสำหรับแฮ็กเกอร์ที่มีประสงค์ร้ายเหมือนกัน

4.5.2 ด้านการจัดการ

เป็นการทดสอบไฟร์วอลในด้านการใช้งาน ความยากง่ายในการติดตั้ง หรือการคอนฟิกให้สามารถทำงานตามนโยบายของความปลอดภัยที่องค์กรต้องการ คงไม่สามารถปฏิเสธได้ว่าการคอนฟิกูเรชันผิดพลาดเป็นปัจจัยใหญ่ในการเกิดช่องโหว่ของเครือข่ายที่ถูกดูแลโดยไฟร์วอล ดังนั้นการจัดการของไฟร์วอลจึงเป็นสิ่งที่สำคัญค่อนข้างมาก เพราะมันสามารถช่วยลดช่องโหว่ที่อาจเกิดจากความผิดพลาดในการปรับตั้งค่าได้

4.5.3 ด้านประสิทธิภาพ

การขยายตัวของระบบแวน (WAN) และอินเทอร์เน็ตทำให้มีความต้องการที่จะใช้ไฟร์วอลที่มีประสิทธิภาพสูงๆ เพิ่มขึ้นอย่างมาก แม้ว่าปัจจุบันอัตราเร็วของสายสื่อสารต่ำเมื่อเทียบกับอัตราเร็วของข้อมูลที่ไฟร์วอลสามารถจัดการได้ แต่การใช้ไฟร์วอลที่มีประสิทธิภาพสูงก็ทำให้สามารถมั่นใจได้ว่าตัวไฟร์วอลจะไม่ไปถ่วงการส่งข้อมูลผ่านสายอินเทอร์เน็ตที่ค่อนข้างช้าอยู่แล้วให้ช้าลงไปอีก จากที่กล่าวมาข้างต้นเราสามารถทดสอบไฟร์วอลในลักษณะต่างๆ ดังที่จะกล่าวต่อไป

- การทดสอบฟังก์ชันของไฟร์วอล

สร้างการคอนฟิกทดสอบเพื่อให้ระบบไฟร์วอลของคุณสามารถเชื่อมต่อระหว่างโฮสต์ 2โฮสต์ที่แยกกันอยู่ โดยตัวหนึ่งจะติดต่อกับเครือข่ายภายนอก ส่วนอีกตัวหนึ่งจะติดต่อกับเครือข่ายภายใน คุณต้องแน่ใจว่าเครื่องภายในเครือข่ายมีการตั้งค่าดีฟอลต์เกตเวย์ที่เป็นเครื่องไฟร์วอล ถ้าคุณมีสถาปัตยกรรมที่สนับสนุน "Centarlized Logging" ให้วางตำแหน่งของเครื่องภายในและเครื่องที่ใช้เก็บล็อกไฟล์ไว้ภายในเครือข่ายเพื่อว่าคุณสามารถทดสอบการเก็บล็อก ถ้าการเก็บล็อกทำงานในเครื่องไฟร์วอลคุณก็สามารถติดต่อจากเครื่องภายในเครือข่ายไปยังเครื่องไฟร์วอล

การใช้เครื่องมือสำหรับสแกน หรือดักจับข้อมูลในระบบเครือข่ายที่ติดตั้งไว้ที่เครื่องภายในและภายนอกเครือข่ายเพื่อที่จะดักจับข้อมูลทั้งสองทิศทาง (จากภายในออกไปภายนอก จากภายนอกเข้ามาภายใน)

แสดงขั้นตอนการทำงานดังนี้

- ปิดการทำงานของแพ็กเก็ตฟิลเตอริง (Disable packet filtering)
- ส่งแพ็กเก็ตผ่านกฎการเราติ้ง และส่งผ่านเครื่องไฟร์วอล
- ต้องแน่ใจว่าแพ็กเก็ตได้หาเส้นทางที่ถูกต้อง โดยการตรวจจากล็อกไฟล์ของไฟร์วอล หรือจากโปรแกรมตรวจจับ (Scanner)
- เปิดการใช้งานของแพ็กเก็ตฟิลเตอริง
- ทดสอบการส่งข้อมูลผ่านไฟร์วอล โดยเลือกค่าแอดเดรสต้นทาง (Source IP Address) แอดเดรสปลายทาง (Destination IP Address) พอร์ตต้นทาง (Source Port) พอร์ตปลายทาง (Destination Port) และโพรโตคอลทุกๆ อย่างเพื่อทดสอบ
- ต้องแน่ใจว่าแพ็กเก็ตที่ไม่ต้องการให้ผ่านไฟร์วอล ก็ไม่สามารถผ่านได้ ส่วนแพ็กเก็ตที่อนุญาตให้ผ่านได้ ก็สามารถผ่านได้ โดยตรวจสอบด้วยล็อกไฟล์ หรือโปรแกรสแกน (Scanner)
- ตรวจสอบพอร์ตที่เปิด และปิดเพื่อให้แน่ใจว่าระบบไฟร์วอลทำงานได้ถูกต้อง
- ตรวจสอบการจราจรบนเครือข่ายทุกอย่างที่เก็บในล็อกไฟล์ และตรวจสอบความถูกต้องของการแจ้งเตือน (Alert Options) ที่เกี่ยวข้องกับล็อกแต่ละอย่าง โดยการส่งการแจ้งเตือนไปยังเป้าหมายปลายทาง ซึ่งส่วนมากจะเป็นผู้ดูแลระบบ(Administrator) โดยวิธีการที่กำหนดไว้ เช่นส่งข้อความผ่านเพจเจอร์ หรืออีเมล์

การวางแผนการปฏิบัติขั้นตอนเหล่านี้ควรจะต้องมีผู้รับผิดชอบอย่างน้อย 2 คน คนแรกเป็นผู้อิมพลีเมนต์เริ่มแรก (Original Implementer) ซึ่งเป็นผู้ที่อิมพลีเมนต์ระบบดังนี้คือ การคอนฟิกการเราติ้ง (routing configuration) การสร้างกฎการกรองแพ็กเก็ต (packert filtering rules) การเก็บล็อกไฟล์ (logging options) และการแจ้งเตือน (Alert Options) ส่วนอีกคนหนึ่งจะเป็นผู้ที่ทบทวนสิ่งที่อิมพลีเมนต์ไปแล้ว เข้าใจถึงความต้องการของระบบ และเห็นด้วยกับโทโปโลยีของเครือข่ายและนโยบายด้านความปลอดภัยที่สะท้อนกลับมาอย่างถูกต้อง

- **ลักษณะเด่นที่เลือก และเก็บล็อกไฟล์ของไฟร์วอล**

เมื่อล็อกไฟล์เต็ม คุณจะต้องเลือกวิธีการที่เครื่องไฟร์วอลจะตอบสนอง โดยมีออปชันที่เป็นไปได้ดังนี้

- ปิดการติดต่อทุกอย่างจากภายนอกมายังเครื่องไฟร์วอล
- ทำงานต่อไป โดยจะเขียนทับล็อกไฟล์เดิม
- ทำงานต่อไปโดยปราศจากการเก็บล็อก

ออปชันแรกเป็นที่นิยมกันมาก แต่ผลิตภัณฑ์ไฟร์วอลบางยี่ห้อไม่มีออปชันนี้ การจำลองสภาวะเมื่อล็อกไฟล์ของไฟร์วอลเต็ม และมั่นใจว่าระบบไฟร์วอลทำงานตามออปชันที่คุณเลือกได้อย่างถูกต้อง เลือกและบริหารข้อมูลที่สำคัญภายในล็อกไฟล์ ซึ่งประกอบด้วย

- ที่จัดเก็บล็อกไฟล์ เช่น โลคอลไฟล์ในเครื่องไฟล์วอล หรือเป็นเซนทรัลล็อกไฟล์บนเครื่องระยะไกล
- จำนวนเวลาก่อนหน้าที่จะทำการนำล็อกไฟล์มาจัดเก็บเป็นอาร์ไคว์ (archives)
- จำนวนวันก่อนหน้าที่จะลบอาร์ไคว์ (archives) ทิ้ง

- **การสำรวจจุดอ่อนในการรักษาความปลอดภัยของระบบไฟร์วอล**

ใช้เครื่องมือในการตรวจหาช่องโหว่เพื่อสำรวจหาจุดบกพร่องของระบบไฟร์วอลที่มันรู้จัก ถ้ามีการซ่อมแซมช่องโหว่ที่ตรวจหาได้แล้ว ก็จะใช้เครื่องมือเดิมมาตรวจเช็คใหม่อีกที่ว่าช่องโหว่นั้นได้ถูกกำจัดไปแล้ว

หลังจากรวบรวมข้อมูลเกี่ยวกับเครือข่ายขององค์กรเป้าหมายแล้ว แฮ็กเกอร์จะพยายามสำรวจจุดอ่อนในการรักษาความปลอดภัยของแต่ละโฮสต์ มีเครื่องมือจำนวนมากที่แฮ็กเกอร์สามารถใช้เพื่อตรวจโฮสต์แต่ละตัวบนเครือข่ายโดยอัตโนมัติ ตัวอย่างเช่น

- เนื่องจากบริการที่เป็นจุดอ่อนซึ่งเป็นที่รู้กันมีอยู่มากมาย แฮ็กเกอร์ที่มีความรู้จึงสามารถเขียนโปรแกรมขนาดเล็กที่พยายามเชื่อมต่อกับพอร์ตของบริการที่กำหนดบนโฮสต์เป้าหมาย เอาต์พุตของโปรแกรมคือรายการโฮสต์ที่สนับสนุนบริการนั้นซึ่งเปิดกว้างต่อการโจมตี
- มีเครื่องมือที่ใช้กันทั่วไปหลายตัวเช่น ซาตาน (Security Administrator Tool for Analyzing Network หรือ SATAN) ที่ตรวจสอบโดเมนหรือเครือข่ายย่อย (subnetwork) ทั้งหมด และค้นหาจุดอ่อนในการรักษาความปลอดภัย โปรแกรมเหล่านี้ระบุจุดอ่อนของแต่ละระบบ ซึ่งอาจโจมตีได้ในหลายๆ จุด ผู้บุกรุกใช้ข้อมูลที่รวบรวมจากการตรวจสอบเหล่านี้เพื่อเข้าถึงระบบขององค์กรเป้าหมายโดยไม่ได้รับอนุญาต

ผู้ดูแลระบบที่เฉลียวฉลาดสามารถใช้เครื่องมือเหล่านี้ภายในเครือข่ายส่วนตัวของพวกเขาเพื่อค้นหาจุดอ่อนในการรักษาความปลอดภัย และตรวจดูว่าโฮสต์ใดต้องได้รับการปรับปรุงด้วยซอฟต์แวร์ที่แก้ไขใหม่

บทที่ 5

วิธีการทดสอบ และผลการทดสอบผลิตภัณฑ์ไฟร์วอล

5.1 ระบบปฏิบัติการที่ใช้ติดตั้งผลิตภัณฑ์ไฟร์วอล

ทางกลุ่มโปรเจ็กต์ได้จัดหาซอฟแวร์ที่เป็นผลิตภัณฑ์ไฟร์วอลมา3ผลิตภัณฑ์ด้วยกันคือ

1. ไอบีเอ็มไฟร์วอล (IBM eNetwork Firewall)
2. ไฟร์วอลวัน (Check Point Firewall –1)
3. กันเล็ตไฟร์วอล (Gauntlet Firewall)
4. ไฟร์วอลทูลคิตบนระบบปฏิบัติการ OpenBSD (Firewall Toolkit)

ซึ่งผลิตภัณฑ์ดังกล่าวเป็นซอฟต์แวร์ที่ได้รับมาฟรี ไม่ต้องเสียค่าใช้จ่ายแต่บางผลิตภัณฑ์มีเวลาจำกัดในการใช้คือใช้ได้แค่เพียงเดือนเดียวเนื่องจากติดปัญหาไลเซนส์จากทางบริษัทผลิตไฟร์วอลดังกล่าว ผลิตภัณฑ์ทั้ง 3 นี้ทำงานอยู่บนระบบปฏิบัติการวินโดว์สเอ็นทีเซิร์ฟเวอร์ 4.0 ซึ่งเป็นระบบปฏิบัติการที่สนับสนุนผลิตภัณฑ์ไฟร์วอลจากบริษัทใหญ่ๆ จำนวนมาก และยิ่งปัจจุบันบริษัทผลิตไฟร์วอลหันมาผลิตไฟร์วอลที่ทำงานบนระบบปฏิบัติการเอ็นทีกันมากขึ้น ทำให้การจัดหาผลิตภัณฑ์ไฟร์วอลมาทดสอบมีความสะดวกด้วย นี่ก็เป็นสาเหตุหนึ่งที่ใช้ระบบปฏิบัติการนี้

ระบบปฏิบัติการเอ็นทียังเป็นระบบปฏิบัติการที่ได้รับความนิยมกันอยู่ในปัจจุบันไม่จะเป็นสถานศึกษา หน่วยงานรัฐบาล หรือบริษัทต่างๆ ก็นิยมใช้กันอยู่ ระบบปฏิบัติการนี้มีความมั่นคงในการทำงานสูง มีความสามารถในการจัดการระบบเครือข่ายได้เป็นอย่างดี เป็นเซิร์ฟเวอร์ที่มีประสิทธิภาพสูงสามารถติดตั้งเป็นเกตเวย์ หรือเราเตอร์ที่เชื่อมต่อกับเครือข่ายอื่นๆ ได้ และเป็นระบบปฏิบัติการที่ง่ายต่อการใช้งานเพราะมีรูปแบบการอินเทอร์เฟซกับผู้ใช้เป็นแบบระบบวินโดว์ส

นอกจากนี้ทางกลุ่มยังได้อิมพลีเมนต์ไฟร์วอลทูลคิตซึ่งทำงานอยู่บนระบบปฏิบัติการ OpenBSD ซึ่งเป็นระบบปฏิบัติการยูนิกซ์ชนิดหนึ่ง

5.2 ผลิตภัณฑ์ที่นำมาทดสอบ

จากที่ได้กล่าวในหัวข้อที่แล้ว ผลิตภัณฑ์ที่ทางกลุ่มได้จัดหามาได้มีอยู่ 3 ผลิตภัณฑ์ด้วยกันคือ

1. ไอบีเอ็มไฟร์วอลเวอร์ชัน 3.3 (IBM eNetwork Firewall version 3.3 for Windows NT Server 4.0)
   - ระบบปฏิบัติการที่ใช้ติดตั้งคือไมโครซอฟต์วินโดว์สเอ็นทีเซิร์ฟเวอร์ 4.0 (เซอร์วิสแพ็ก 3 หรือ 4)
   - การ์ดแลนอย่างน้อย 2 การ์ด การ์ดหนึ่งสำหรับเครือข่ายภายใน ส่วนอีกการ์ดหนึ่งสำหรับเครือข่ายภายนอก
   - สื่อทำใช้ติดตั้งใช้ซีดีรอม
   - DNS server ถ้าต้องการใช้งานดีเอ็นเอส

- SMTP mail server ที่ทำงานภายในเครือข่าย ถ้าต้องการส่งเมล์ผ่านไฟร์วอล
- POP3 mail server ที่ทำงานในเครือข่ายภายใน ถ้าต้องการรับเมล์จากภายในเครือข่าย

2. ไฟร์วอลวันเวอร์ชัน 4.1 (Check Point Firewall –1 version 4.1)

ความต้องการของระบบที่ทำการติดตั้ง (SYSTEM REQUIREMENTS) มีดังนี้คือ

- ระบบปฏิบัติการที่ใช้ติดตั้งมีดังนี้
  - ไมโครซอฟต์วินโดว์สเอ็นทีเซิร์ฟเวอร์ 4.0 (เซอร์วิสแพ็ก 3 หรือ 4)
  - ซันโซลาริส 2.6 หรือโซลาริส 7 (ในโหมด 32 บิต)
  - เอชพี-ยูเอ็ก 10.20, 11. 0 (ในโหมด 32 บิต)
  - ไอบีเอ็มเอไอเอ็ก 4.2.1, 4.3.2
  - เรดแฮตลีนุกซ์ 6.0, 6.1
- พื้นที่ว่างในฮาร์ดดิสก์ 40 เมกะไบต์
- หน่วยความจำ
  - เครื่องเซิร์ฟเวอร์ที่เป็นไฟร์วอล อย่างต่ำ 64 เมกะไบต์ (แนะนำ 128 เมกะไบต์)
  - เครื่องไคลเอ็นต์ที่ใช้ปรับตั้งค่าไฟร์วอลจากระยะไกล 30 เมกะไบต์
- การเชื่อมต่อเครือข่าย
  - ATM
  - Ethernet
  - Fast Ethernet
  - FDDI
  - Token Ring
- สื่อทำใช้ติดตั้งใช้ซีดีรอม
- การ์ดแลนอย่างน้อย 2 การ์ด การ์ดหนึ่งสำหรับเครือข่ายภายใน ส่วนอีกการ์ดหนึ่งสำหรับเครือข่ายภายนอก
- DNS server ถ้าต้องการใช้งานดีเอ็นเอส
- SMTP mail server ที่ทำงานภายในเครือข่าย ถ้าต้องการส่งเมล์ผ่านไฟร์วอล
- POP3 mail server ที่ทำงานในเครือข่ายภายใน ถ้าต้องการรับเมล์จากภายในเครือข่าย

3. กันเล็ตไฟร์วอล (Gauntlet Firewall)

มีความต้องการของระบบอย่างต่ำที่ทำการติดตั้ง (Minimum System Requirements) มีดังนี้คือ

- ระบบปฏิบัติการที่ใช้ติดตั้งคือไมโครซอฟต์วินโดว์สเอ็นทีเซิร์ฟเวอร์ 4.0 (เซอร์วิสแพ็ก 3 หรือ 4)
- อัตราเร็วซีพียูเพนเทียมทูโพรเซสเซอร์ 233 เมกะเฮิรตซ์
- หน่วยความจำขนาด 128 เมกะไบต์

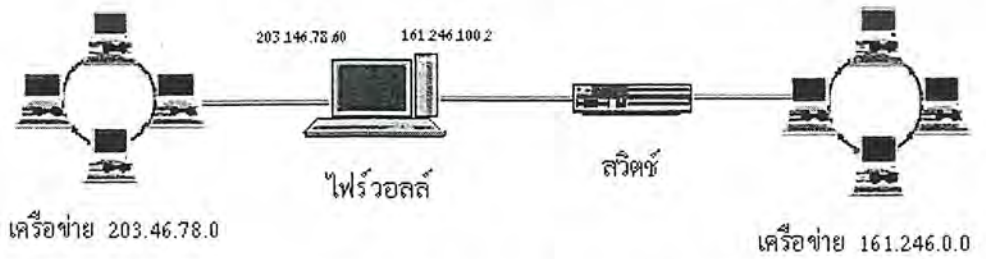
- พื้นที่ว่างในฮาร์ดดิสก์ขนาด 512 เมกะไบต์
- การ์ดแลนอย่างน้อย 2 การ์ด การ์ดหนึ่งสำหรับเครือข่ายภายใน ส่วนอีกการ์ดหนึ่งสำหรับเครือข่ายภายนอก
- สื่อทำใช้ติดตั้งใช้ซีดีรอม
- DNS server ถ้าต้องการใช้งานดีเอ็นเอส
- SMTP mail server ที่ทำงานภายในเครือข่าย ถ้าต้องการส่งเมล์ผ่านไฟร์วอล
- POP3 mail server ที่ทำงานในเครือข่ายภายใน ถ้าต้องการรับเมล์จากภายในเครือข่าย

นอกจากผลิตภัณฑ์สำเร็จรูปที่ทางกลุ่มได้จัดหามาทดสอบแล้ว ทางกลุ่มยังได้อิมพลีเมนต์ไฟร์วอลขึ้นมาเอง ซึ่งสามารถใช้งานได้โดยไม่ต้องเสียค่าใช้จ่ายใดๆ คือ

4. ไฟร์วอลทูลคิตบนระบบปฏิบัติการ OpenBSD
   - ระบบปฏิบัติการที่ใช้ติดตั้งคือไมโครซอฟต์วินโดว์สเอ็นทีเซิร์ฟเวอร์ 4.0 (เซอร์วิสแพ็ก 3 หรือ 4)
   - การ์ดแลนอย่างน้อย 2 การ์ด การ์ดหนึ่งสำหรับเครือข่ายภายใน ส่วนอีกการ์ดหนึ่งสำหรับเครือข่ายภายนอก
   - อัตราเร็วซีพียู
     เพนเทียมโพรเซสเซอร์
   - หน่วยความจำขนาด 32 เมกะไบต์
   - พื้นที่ว่างในฮาร์ดดิสก์ขนาด 300 เมกะไบต์
   - DNS server ถ้าต้องการใช้งานดีเอ็นเอส
   - SMTP mail server ที่ทำงานภายในเครือข่าย ถ้าต้องการส่งเมล์ผ่านไฟร์วอล
   - POP3 mail server ที่ทำงานในเครือข่ายภายใน ถ้าต้องการรับเมล์จากภายในเครือข่าย

5.3 โครงสร้างทางกายภาพระบบเครือข่ายที่ทดสอบ

รูปแบบโครงสร้างของเครือข่ายที่ทางกลุ่มได้ออกแบบเป็นดังรูปข้างล่างนี้



รูปที่ 5-1 แสดงโครงสร้างทางกายภาพของเครือข่ายที่ทดสอบ

ในการทดสอบได้กำหนดรูปแบบการเชื่อมต่อระบบเครือข่ายโดยผ่านไฟร์วอล โดยให้เครือข่าย 203.146.78.0 เป็นเครือข่ายที่อยู่ภายนอก และเชื่อมต่ออยู่กับเครือข่ายภายในซึ่งเป็นเครือข่าย 161.246.0.0 โดยผ่านเครื่องไฟร์วอล คือมีไฟร์วอลกั้นระหว่างเครือข่ายภายนอกและเครือข่ายภายใน โดยไอพีแอดเดรสของเครื่องไฟร์วอลที่เชื่อมต่อกับเครือข่ายภายนอกคือ 203.146.78.60 ส่วนไอพีแอดเดรสของเครื่องไฟร์วอลที่เชื่อมต่อกับเครือข่ายภายในคือ 161.246.100.2

5.4 นโยบายความปลอดภัยที่ใช้ทดสอบ

ดังที่ได้กล่าวในบทที่แล้ว นโยบายความปลอดภัยก็เป็นปัจจัยหนึ่งที่สำคัญในการออกแบบระบบไฟร์วอล แต่ละองค์กรก็มีนโยบายที่ไม่เหมือนกัน แล้วแต่ว่าองค์กรใดมีนโยบายเป็นแบบใด ส่วนในการทดสอบนี้ทางกลุ่มได้ออกแบบนโยบายในด้านความปลอดภัย โดยปรับตั้งค่าในเครื่องไฟร์วอลให้ทำหน้าที่เป็นเหมือนอินเนอร์ไฟร์วอล (ดูที่หัวข้อ 3.9 เรื่อง dual firewall) ดังนั้นนโยบายความปลอดภัยที่ได้ออกแบบขึ้นมาจึงค่อนข้างที่จะปิดกั้นการเข้ามาใช้บริการภายในเครือข่ายจากผู้ใช้ภายนอกเครือข่าย แต่จะอนุญาตให้ผู้ใช้งานภายในเครือข่ายสามารถใช้บริการที่มีอยู่ภายนอกเครือข่ายได้ ดังนี้คือ

- เปิดบริการเทลเน็ต เอชทีทีพี เอฟทีพี สำหรับผู้ใช้งานภายในเครือข่ายให้สามารถใช้บริการดังกล่าวจากภายนอกเครือข่ายโดยผ่านไฟร์วอลได้ แต่ผู้ใช้ภายนอกเครือข่ายไม่สามารถใช้บริการนี้ผ่านไฟร์วอลเข้ามาในเครือข่ายภายในได้
- เครือข่ายภายในสามารถตรวจสอบการมีอยู่ของเครื่องภายนอกโดยใช้บริการ ping แต่เครื่องภายนอกไม่สามารถใช้บริการนี้ตรวจสอบการมีอยู่ของเครื่องภายในได้
- มีการเก็บล็อกไฟล์ของไฟร์วอลเพื่อใช้ในการตรวจดูข้อมูลที่ผ่านและไม่ผ่านไฟร์วอลและตรวจดูสิ่งผิดปกติที่เกิดขึ้นได้
- ปิดการเชื่อมต่อที่เหลือทุกอย่างที่มาจากภายนอกเครือข่าย ไม่ให้เข้ามาภายในเครือข่ายโดยผ่านไฟร์วอลได้

5.5 ปัจจัยที่ทำการทดสอบผลิตภัณฑ์ไฟร์วอล

ดังที่ได้กล่าวมาแล้ว ทางกลุ่มโปรเจ็กต์ได้แบ่งวิธีการทดสอบผลิตภัณฑ์ไฟร์วอลออกเป็น 3 ด้านด้วยกันคือ

1. ด้านความปลอดภัย
2. ด้านประสิทธิภาพ
3. ด้านการจัดการ

เหตุที่แบ่งการทดสอบออกเป็น 3 ด้านเพราะทางกลุ่มได้คำนึงถึงความสำคัญของปัจจัยทั้ง 3 ด้านนี้ ซึ่งเป็นปัจจัยพื้นฐานที่ต้องมีอยู่ในผลิตภัณฑ์ไฟร์วอลทุกตัว และเป็นส่วนสำคัญในการที่จะเลือกใช้ไฟร์วอลให้เหมาะสมสำหรับองค์กรของตน ส่วนปัจจัยอื่นๆ เช่น ค่าใช้จ่ายในการติดตั้งและบำรุงรักษาระบบไฟร์วอล เป็นต้น เป็นปัจจัยที่ขึ้นกับตัวองค์กรซึ่งไม่นำพิจารณาในที่นี้

5.6 การทดสอบความปลอดภัย

แน่นอนที่สุดสำหรับการทดสอบไฟร์วอลเพราะว่าสิ่งที่ต้องการจากไฟร์วอลก็คือความปลอดภัย ดังนั้นทางกลุ่มจึงทำการทดสอบเรื่องความปลอดภัยด้วย ทางกลุ่มได้พยายามตรวจสอบคุณสมบัติในการป้องกันของไฟร์วอลนั้นๆ ว่าครบถ้วน และถูกต้องหรือไม่ ทั้งนี้ยังต้องดูในสภาพแวดล้อมต่างๆ ภายในองค์กรเป็นส่วนประกอบ เนื่องจากองค์กรแต่ละแห่งมีข้อจำกัดหรือกฎระเบียบไม่เหมือนกัน บางแห่งอาจต้องการความปลอดภัยมากๆ แต่บางที่อาจต้องการความสะดวกในการใช้งานมากกว่าความปลอดภัย ซึ่งถ้าระบบมีความปลอดภัยมากๆ อาจทำให้ความสะดวกในการใช้งานมีน้อยมาก ดังนั้นเราต้องแบ่งสรรค์ระหว่างความปลอดภัยกับความสะดวกในการใช้งาน

ในการทดสอบความปลอดภัยของผลิตภัณฑ์ไฟร์วอลนี้เรามีการทดสอบอยู่ 2 ส่วนด้วยกัน คือ

1. **การทดสอบการโจมตีโดยใช้ Denial Of Services** ซึ่งเป็นการโจมตีที่ทำให้ระบบไม่สามารถใช้งานได้ โดยวิธีการหลายๆ อย่าง การทดสอบในส่วนนี้ใช้โปรแกรมโจมตีแบบ Denial Of Service ที่ทำงานบนระบบปฏิบัติการยูนิกซ์

2. **การทดสอบความปลอดภัยโดยใช้โปรแกรมสำรวจเครือข่ายชื่อ** CyberCop Scanner เวอร์ชัน 5.5 ของบริษัท Network Associates Technology ได้มาจากเว็บไซต์ของบริษัท ซึ่งเป็นโปรแกรมที่บริษัทให้ดาวน์โหลดมาทดลองใช้ก่อน 30 วัน โดยโปรแกรมนี้จะสำรวจหาช่องโหว่ (Vulnerability) ของเครือข่าย

โดยโครงสร้างของเครือข่ายที่ใช้ทดสอบเป็นดังนี้คือ

รูปที่ 5-2 แสดงโครงสร้างทางกายภาพของเครือข่ายที่ทดสอบความปลอดภัย

ในการทดสอบได้กำหนดรูปแบบการเชื่อมต่อระบบเครือข่ายโดยผ่านไฟร์วอล โดยให้เครื่องที่ติดตั้งโปรแกรมสำรวจเครือข่าย และโปรแกรมโจมตีคือเครื่องหมายเลข 203.146.78.61 ที่อยู่ภายนอกเครือข่าย (เครือข่าย 203.146.78.0) และเชื่อมต่ออยู่กับเครือข่ายภายในซึ่งเป็นเครือข่าย 161.246.0.0 โดยผ่านเครื่องไฟร์วอล คือมีไฟร์วอลกั้นระหว่างเครือข่ายภายนอกและเครือข่ายภายใน โดยไอพีแอดเดรสของเครื่องไฟร์วอลที่เชื่อมต่อกับเครือข่ายภายนอกคือ 203.146.78.60 ส่วนไอพีแอดเดรสของเครื่องไฟร์วอลที่เชื่อมต่อกับเครือข่ายภายในคือ 161.246.100.2

ผลการทดสอบด้านความปลอดภัย

1. ใช้โปรแกรม Deniel Of Service

โปรแกรม	ไอบีเอ็มไฟร์วอล	ไฟร์วอลวัน	ไฟร์วอลทูลคิต
Gin.c	√	√	√
Kod.c	√	√	√
Moya.c	√	√	√
Opentear.c	√	√	√
Oshare.c	√*	√	√
Pimp.c	√	√	√
Sesquipedalian.c	√	√	√
Stream.c	√	√	√
Syndrop.c	√	√	√
Synflood.c	×	√	√

ตารางที่ 5-1 แสดงผลการทดสอบความปลอดภัยโดยใช้โปรแกรมโจมตีแบบ Denial of Service

*ใช้โปรแกรมโจมตีไฟร์วอลแล้วไฟร์วอลจะหยุดการทำงานจนกว่าจะเลิกโจมตีแต่สามารถป้องกันการโจมตีมายังเครือข่ายภายในได้

2. ใช้โปรแกรมสำรวจเครือข่าย

2.1 IBM eNetwork for WindowsNT version 3.3

2.1.1 ใช้ฟังก์ชันการทำงานแบบพร็อกซี พบช่องโหว่ของเครือข่าย 7 แห่งด้วยกันโดย มีช่องโหว่ที่มีระดับความเสี่ยงอยู่ในระดับสูงอยู่ 2 แห่งดังนี้

- Sendmail bounce
- TCP sequence numbers are predictable

มีช่องโหว่ที่มีระดับความเสี่ยงอยู่ในระดับต่ำอยู่ 5 แห่งดังนี้

- SMTP banner-check
- ESMTP check
- Trace route to host
- TCP port scanning
- TCP FIN port scanning

2.1.2 ใช้ฟังก์ชันการทำงานแบบการกรองแพ็กเก็ต พบช่องโหว่ของเครือข่าย 8 แห่งด้วยกัน ดังนี้

มีช่องโหว่ที่มีระดับความเสี่ยงอยู่ในระดับสูงอยู่ 2 แห่งดังนี้

- Sendmail bounce
- TCP sequence numbers are predictable

มีช่องโหว่ที่มีระดับความเสี่ยงอยู่ในระดับต่ำอยู่ 6 แห่งดังนี้

- SMTP banner-check
- ESMTP check
- Trace route to host
- TCP port scanning
- TCP SYN port scanning
- TCP FIN port scanning

2.2 CheckPoint Firewall-1 พบช่องโหว่ในเครือข่าย 4 แห่งด้วยกัน

มีระดับความเสี่ยงอยู่ในระดับต่ำทั้งหมดดังนี้

- Trace route to host
- TCP port scanning
- TCP SYN port scanning
- TCP FIN port scanning

2.3 ไฟร์วอลทูลคิต พบช่องโหว่ในเครือข่าย 2 แห่งด้วยกัน

มีระดับความเสี่ยงอยู่ในระดับต่ำทั้งหมดดังนี้

- Trace route to host
- TCP FIN port scanning

รายละเอียดเพิ่มเติมของความเสี่ยงที่สำรวจได้มีดังนี้

SMTP banner-check

อธิบาย การตรวจสอบนี้จะรวบรวมข้อมูลที่แสดงการเชื่อมต่อไปยังพอร์ตของ SMTP บนเครื่องปลายทาง

เกี่ยวกับความปลอดภัย SMTP port banner มักประกอบด้วยข้อมูลพิเศษเกี่ยวกับเวอร์ชันของโปรแกรม SMTP agent ที่ผู้ใช้งานใช้อยู่ ข้อมูลนี้สามารถนำไปใช้ในการโจมตีโปรแกรมส่งเมล์ที่มีจุดบกพร่อง ซึ่ง Sendmail เป็น SMTP Server สำหรับยูนิกซ์ที่ได้รับความนิยมมากมีปัญหาด้านความปลอดภัย การรู้ข้อมูลเวอร์ชันทำให้ผู้โจมตีสามารถคาดเดาชนิดของการโจมตีที่จะนำไปโจมตีระบบได้สำเร็จ

ESMTP check

อธิบาย ตรวจสอบโปรแกรมส่งเมล์ว่าสนับสนุนการใช้คำสั่ง extended SMTP ผ่านคำสั่ง ehlo

เกี่ยวกับความปลอดภัย คำสั่ง ehlo ใช้โดยโปรแกรมเมล์เอเจนต์ เพื่อค้นหาโปรแกรมส่งเมล์ระยะไกลที่สนับสนุนคำสั่ง extended SMTP command ส่วนใหญ่ผู้ใช้งานระยะไกลสามารถมองเห็นตัวโปรแกรมส่งเมล์ต้นทาง ซึ่งเขาสามารถคิดกลอุบายเป็นหนทางในการแสวงหาเวอร์ชันของโปรแกรม sendmail

Trace route to host

อธิบาย ทำการ trace หาเส้นทางไปยังโฮสต์ที่ต้องการ โดยมีลักษณะเหมือนโปรแกรม trace route ในยูนิกซ์ หรือโปรแกรม tracert ในวินโดวส์เอ็นที ข้อมูลในการหาเส้นทางถูกเก็บไว้ในไฟล์แผนที่เครือข่าย (network map file)

เกี่ยวกับความปลอดภัย การยอมให้สามารถสำรวจเส้นทางมาภายในเครือข่ายจากภายนอก ก็เหมือนยอมให้รายละเอียดของแผนที่เครือข่าย (network maps) ที่สามารถสืบทอดต่อไปได้ เป้าหมายที่ต้องการสามารถพิจารณาจากแผนที่เหล่านี้ สิ่งเหล่านี้นำไปสู่การล่อลวงที่อันตราย

Sendmail bounce 'From:' check

อธิบาย และความปลอดภัย ตรวจสอบว่าโปรแกรมส่งเมล์ทำงานอยู่บนโฮสต์ที่ยอมให้มีการคืนค่าแอดเดรสที่ปรากฏจากแอพพลิเคชัน นี่เป็นจุดอ่อนในการโจมตีโดย SMTP bounce Attack

TCP Sequence number are predictable

อธิบาย เครื่องเป้าหมายถูกค้นพบว่ามีช่องโหว่ในการโจมตีที่สามารถคาดเดา TCP Sequence number โดยเครื่องจะสร้าง TCP Sequence number ในรูปแบบที่ผู้บุกรุกสามารถเดาได้ เพื่อผู้บุกรุกสามารถปลอมแปลงแพ็กเก็ตติดต่อเข้ามาได้

เกี่ยวกับความปลอดภัย ถ้าเครื่องโฮสต์รันเซอร์วิสที่ไว้ใจหมายเลขไอพีแอดเดรสของเครื่องไคลเอ็นต์ เซอร์วิสนี้สามารถถูกสำรวจโดยผู้โจมตีเพื่อจำลองตัวปลอมเป็นโฮสต์ถูกต้องน่าไว้ใจ

TCP port Scanning

อธิบาย ตรวจสอบโดยสแกนเครื่องปลายทางสำหรับพอร์ต TCP

เกี่ยวกับความปลอดภัย โปรแกรมสำรวจเครือข่ายจะคืนค่าพอร์ต TCP ที่ทำงานอยู่ ดังนั้นควรเช็กว่าพอร์ตที่ทำงานอยู่นั้นรันเซอร์วิสตามที่ได้อนุญาตไว้หรือเปล่า ถ้ารันเซอร์วิสที่ไม่ได้อนุญาตก็ให้ทำการปิดพอร์ตนั้น

TCP SYN port scanning

อธิบาย การตรวจสอบนี้ทำงานได้เร็วกว่า TCP port scanning ดังที่ได้กล่าวมาแล้ว การตรวจสอบส่วนใหญ่ก็เหมือนกับ TCP port scanning แต่แตกต่างกันที่ใช้วิธีการติดต่อกับโฮสต์ระยะไกล โดยไม่ได้เชื่อมต่อให้จบสมบูรณ์ ทำให้เกิดความไม่น่าไว้ใจโดยอ้างถึงการสูญเสียแพ็กเก็ตบนเครือข่าย

เกี่ยวกับความปลอดภัย โปรแกรมสำรวจเครือข่ายจะคืนค่าพอร์ต TCP ที่ทำงานอยู่ ดังนั้นควรเช็กว่าพอร์ตที่ทำงานอยู่นั้นรันเซอร์วิสตามที่ได้อนุญาตไว้หรือเปล่า ถ้ารันเซอร์วิสที่ไม่ได้อนุญาตก็ให้ทำการปิดพอร์ตนั้น

TCP FIN port scanning

อธิบาย การตรวจสอบนี้ทำงานเร็วกว่า TCP port scanning มาก การตรวจสอบโดยสแกนเครื่องเป้าหมายสำหรับพอร์ต TCP โดยสังเกตว่าเครื่องเป้าหมายตอบรับกับแพ็กเก็ต TCP FIN ยังไง เพราะเครื่องเป้าหมายจะตอบรับเพียงแค่เมื่อ FIN ถูกส่งไปยังพอร์ตที่ได้เปิดใช้งาน และจะมีตอบรับเมื่อส่ง FIN ไปยังพอร์ตที่ปิดอยู่

เกี่ยวกับความปลอดภัย โปรแกรมสำรวจเครือข่ายจะคืนค่าพอร์ต TCP ที่ทำงานอยู่ ดังนั้นควรเช็กว่าพอร์ตที่ทำงานอยู่นั้นรันเซอร์วิสตามที่ได้อนุญาตไว้หรือเปล่า ถ้ารันเซอร์วิสที่ไม่ได้อนุญาตก็ให้ทำการปิดพอร์ตนั้น

สรุปผลการทดสอบ

ในส่วนที่ 1 จะเห็นได้ว่ามีเพียงไอบีเอ็มไฟร์วอลเท่านั้นที่ไม่สามารถป้องกัน Synflood ได้ นอกนั้นสามารถป้องกันการโจมตีให้ปิดบริการด้วยโปรแกรม Denial of Service

ในส่วนที่ 2 การพิจารณาช่องโหว่ของผลิตภัณฑ์ไฟร์วอล จะพิจารณาจากช่องโหว่ที่มีความเสี่ยงสูงก่อน หากผลิตภัณฑ์ใดมีช่องโหว่ที่มีระดับความเสี่ยงสูงจะมีความปลอดภัยต่ำ แต่เมื่อเปรียบเทียบผลิตภัณฑ์ไฟร์วอลแล้วปรากฏว่ามีช่องโหว่ที่ระดับความเสี่ยงสูงเท่ากัน ก็พิจารณาช่องโหว่ที่มีระดับความเสี่ยงต่ำรองลงมา ซึ่งจากผลการทดสอบไฟร์วอลทูลคิต (เป็นพร็อกซี) และไฟร์วอลวันมีความเสี่ยงในระดับที่ต่ำทั้งหมดดังนั้นมีความปลอดภัยมากกว่าไอบีเอ็มไฟร์วอล โดยที่ไฟร์วอลทูลคิตมีความปลอดภัยสูงกว่าไฟร์วอลวันเพราะมีช่องโหว่เพียง 2 แห่งเท่านั้น และเมื่อเปรียบเทียบไอบีเอ็มที่เป็นพร็อกซี กับที่เป็นแบบกรองแพ็กเก็ตแล้วจะเห็นว่าไอบีเอ็มไฟร์วอลที่เป็นแบบกรองแพ็กเก็ตจะมีความปลอดภัยต่ำกว่าเพราะมีความเสี่ยงมากกว่าไอบีเอ็มที่เป็นพร็อกซี

หมายเหตุ

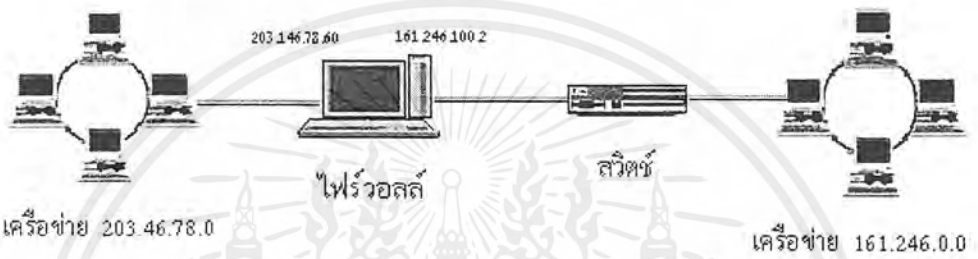
สาเหตุที่ทางกลุ่มไม่ได้ทำการทดสอบกันเล็ตไฟร์วอลเนื่องจากผลิตภัณฑ์นี้เป็น evaluation version สามารถใช้ได้เพียง 30 วันเท่านั้น ทางกลุ่มจึงไม่สามารถนำมาทดสอบได้ทัน

5.7 การทดสอบด้านการจัดการ

การทดสอบผลิตภัณฑ์ไฟร์วอลด้านการจัดการก็เป็นปัจจัยหนึ่งที่ทางกลุ่มได้ทำการทดสอบเนื่องจาก ปัจจัยด้านการจัดการไฟร์วอลนี้มีผลต่อการใช้งานระบบเครือข่ายที่เชื่อมต่อกับอินเทอร์เน็ต ผลิต

ภัณฑ์ไฟร์วอลใดที่มีรูปแบบการจัดการที่เข้าใจง่าย มีหน้าจออินเทอร์เฟซที่เป็นระเบียบง่ายต่อการปรับตั้งค่า อาจมีการแสดงผลออกมาเป็นรูปภาพที่สื่อความหมายได้ง่ายกว่าตัวอักษร ก็ยิ่งเป็นที่ชื่นชอบของผู้ดูแลระบบที่ต้องทำการติดตั้งใช้งานไฟร์วอล และยังมีผลต่อจำนวนช่องโหว่ที่ไม่ปลอดภัยที่ผู้ประสงค์ร้ายสามารถตรวจสอบจากเครื่องมือต่างๆ ได้ เพราะยิ่งไฟร์วอลตัวใดมีการจัดการปรับตั้ง หรือเปลี่ยนแปลงค่าต่างๆ ที่เข้าใจยากก็ยิ่งทำให้เกิดความเสี่ยงต่อการปรับตั้งค่าที่ผิดทำให้เครือข่ายที่ปลอดภัยเกิดช่องโหว่ในการโจมตีได้

โครงสร้างทางกายภาพที่ใช้ทดสอบการจัดการแสดงดังรูปข้างล่างนี้



รูปที่ 5-3 แสดงโครงสร้างทางกายภาพของเครือข่ายที่ใช้ทดสอบการจัดการ

วิธีการทดสอบ

ทางกลุ่มของข้าพเจ้าได้ออกแบบกระบวนการทดสอบ โดยแบ่งออกเป็น 3 สถานการณ์ด้วยกัน ซึ่งแต่ละสถานการณ์จะแบ่งออกเป็นเรื่องย่อยๆ ที่เกี่ยวกับสถานการณ์นั้นๆ โดยเราจะมีการให้คะแนนตั้งแต่ระดับ 1(แย่) ถึง ระดับ 5 (ดีเยี่ยม) สำหรับความยากง่ายในการใช้งานในสถานการณ์เหล่านั้น แต่ถ้าไฟร์วอลที่ทดสอบไม่สามารถรองรับสถานการณ์นั้นๆ ได้ก็จะได้ 0 คะแนน

สถานการณ์ที่ 1 การจัดการไฟร์วอลจากเครื่องระยะไกล

เป็นสถานการณ์ที่สมมุติผู้บุกรุกสามารถบุกเข้าไปในไฟร์วอลได้ โดยในสถานการณ์นี้เราจะให้คะแนนตามลำดับความยากง่ายในการคอนฟิก จาก 0 คะแนนถึง 5 คะแนน ซึ่งถ้าไม่รองรับฟีเจอร์นั้นก็จะให้ 0 คะแนน เราจะตรวจสอบดังนี้คือ

- ไฟร์วอลสามารถเตือนผู้ดูแลระบบได้หรือไม่ ผ่านทางอีเมล์ หรือเพจเจอร์ก็ได้
- และเมื่อผู้ดูแลระบบทราบปัญหาแล้วไฟร์วอลยอมให้ผู้ดูแลปิดมัน หรือมีฟีเจอร์ให้ผู้ดูแลปิดการติดต่อกับอินเทอร์เน็ตจากระยะไกลเช่น จากที่บ้านได้หรือไม่
- นอกจากนี้ยังตรวจสอบด้วยว่าการล็อกอินจากระยะไกลของผู้ดูแลระบบจากระยะไกลว่ามีการเข้ารหัส (Encryption) หรือไม่

สถานการณ์ที่ 2 การเข้าถึงเซอร์วิส และเซอร์วิสที่มีในระบบ

สถานการณ์นี้จะเกี่ยวกับความยากง่ายในการกำหนดนโยบายเพื่อควบคุมการเข้าถึงข้อมูลและการให้บริการดังนี้คือ

- ตรวจสอบถึงความยากง่ายในการเข้าถึงข้อมูลโดยพิจารณาจากหมายเลขเครื่อง (IP Address)
- ตรวจสอบถึงความยากง่ายในการเข้าถึงข้อมูลโดยพิจารณาจากผู้ใช้งาน (User ID) เป็นการจัดการบริหารผู้ใช้งานที่เป็นสมาชิกในระบบไฟร์วอล หรือในภายในเครือข่ายที่เรียกว่ายูสเซอร์แอกเคาต์
- พิจารณาเซอร์วิสหลักๆ 4 อย่างที่ควรจะมีในระบบเครือข่ายดังนี้คือเทลเน็ต (Telnet) เอฟทีพี (FTP) เอชทีทีพี (HTTP) และดีเอ็นเอส (DNS)

เราจะให้คะแนนตามลำดับความยากง่ายในการคอนฟิก จาก 0 คะแนนถึง 5 คะแนน ซึ่งถ้าไม่รองรับฟีเจอร์นั้นก็จะให้ 0 คะแนน

สถานการณ์ที่ 3 การเก็บล็อกไฟล์

เป็นการบันทึกข้อมูลเกี่ยวกับเหตุการณ์ที่เกิดขึ้นในเครือข่ายที่เกี่ยวกับไฟร์วอล รวมทั้งบันทึกการบุกรุกของผู้ประสงค์ร้ายได้ โดยถ้าไฟร์วอลมีออปชันเหล่านี้ก็จะให้คะแนนข้อละ 3 คะแนน แต่ถ้าไม่มีก็จะให้ 0 คะแนน ซึ่งจะพิจารณาดังนี้

- พิจารณาความยากง่ายในการจัดการเก็บล็อกไฟล์

สถานการณ์	คะแนน
สถานการณ์ที่ 1 การจัดการไฟร์วอลจากเครื่องระยะไกล	
• เตือนผู้ดูแลระบบผ่านทางอีเมล์ หรือเพจเจอร์	ความยากง่าย 0 – 5 คะแนน
• ยินยอมให้ผู้ดูแลระบบปิดการติดต่อกับอินเทอร์เน็ตจากระยะไกล	ความยากง่าย 0 – 5 คะแนน
• การเข้ารหัส (Encryption) ในการล็อกอินระยะไกล	ความยากง่าย 0 – 5 คะแนน
สถานการณ์ที่ 2 การเข้าถึงเซอร์วิส และเซอร์วิสที่มีในระบบ	
• การพิจารณาการเข้าถึงข้อมูลโดยใช้หมายเลขเครื่อง	ความยากง่าย 0 – 5 คะแนน
• การพิจารณาการเข้าถึงข้อมูลจากผู้ใช้งาน	ความยากง่าย 0 – 5 คะแนน
• เทลเน็ต (Telnet)	ความยากง่าย 0 – 5 คะแนน
• เอฟทีพี (FTP)	ความยากง่าย 0 – 5 คะแนน
• เอชทีทีพี (HTTP)	ความยากง่าย 0 – 5 คะแนน
• ดีเอ็นเอส (DNS)	ความยากง่าย 0 – 5 คะแนน
สถานการณ์ที่ 3 การเก็บล็อกไฟล์	
• ความยากง่ายในการจัดการล็อกไฟล์	ความยากง่าย 0 – 5 คะแนน

ตารางที่ 5-2 แสดงขอบเขตของคะแนนในแต่ละสถานการณ์

ผลการทดสอบความสามารถด้านการจัดการในแต่ละสถานการณ์

สถานการณ์ที่ 1 การจัดการไฟร์วอลจากเครื่องระยะไกล

- ไฟร์วอลสามารถเตือนผู้ดูแลระบบได้หรือไม่ (ผ่านทางอีเมล์ หรือเพจเจอร์ก็ได้)

	เตือนผู้ดูแลระบบผ่านทางอีเมล์ หรือเพจเจอร์
ไอบีเอ็มไฟร์วอล	5
ไฟร์วอลวัน	5
กันเล็ตไฟร์วอล	4
ไฟร์วอลทูลคิต	0

- ไอบีเอ็มไฟร์วอล

  ในการส่งเพจของไอบีเอ็มไฟร์วอล มีการจัดการที่ง่าย มีหน้าต่างที่สามารถป้อนรายละเอียดที่เข้าใจง่ายดังนี้คือ

  - หมายเลขเพจเจอร์ของผู้ที่ต้องการติดต่อ (ผู้ดูแลระบบ)
  - ข้อความที่ต้องการส่ง
  - ช่องทางที่ใช้ส่ง เป็นชื่อของผู้ให้บริการในการส่งข้อความ ซึ่งสามารถแก้ไข และเพิ่มเติมได้
  - เป็นชื่อของโมเด็มที่ใช้งาน ซึ่งสามารถเปลี่ยนชนิดของโมเด็มที่ใช้ได้

- ไฟร์วอลวัน

  ในไฟร์วอลวันจะแจ้งเตือนผู้ดูแลระบบโดยการใช้เมล์ ซึ่งการจัดการค่อนข้างง่าย มีหน้าต่างให้ปรับตั้งค่าเกี่ยวกับเมล์เซิร์ฟเวอร์ ในหน้าต่าง Check Point Configuration Tool ในแถบ SMTP Security Server เราสามารถกำหนดให้มีการแจ้งเตือนผ่านเมล์ไปยังผู้ดูแลระบบได้ โดยแก้ไขที่กฎในหน้าต่าง Policy Editor

- กันเล็ตไฟร์วอล

  ในกันเล็ตไฟร์วอลสามารถแจ้งเตือนผู้ดูแลระบบผ่านทางเมล์ได้ง่าย และสะดวก โดยตั้งค่าเมล์เซิร์ฟเวอร์ในแถบ Logs and Reports ของหน้าต่าง Gauntlet Firewall Manager และทำการเปิดเซอร์วิส SMTP ในแถบ Proxies ของหน้าต่าง Gauntlet Firewall Manager

- ไฟร์วอลทูลคิต

  ไฟร์วอลทูลคิตไม่มีฟีเจอร์สำหรับแจ้งเตือนผู้ดูแลระบบผ่านทางอีเมล์ หรือเพจเจอร์

- และเมื่อผู้ดูแลระบบทราบปัญหาแล้วไฟร์วอลยอมให้ผู้ดูแลปิดมัน หรือมีฟีเจอร์ให้ผู้ดูแลปิดการติดต่อกับอินเทอร์เน็ตจากระยะไกลเช่น จากที่บ้านได้หรือไม่

	ยินยอมให้ผู้ดูแลระบบปิดการติดต่อกับอินเทอร์เน็ตจากระยะไกล
ไอบีเอ็มไฟร์วอล	2

ไฟร์วอลวัน	4
กันเล็ตไฟร์วอล	3
ไฟร์วอลทูลคิต	5

- ไอบีเอ็มไฟร์วอล

  การจัดการกับล็อกอินระยะไกล (ซึ่งอาจอยู่ภายในเครือข่าย หรือภายนอกเครือข่ายก็ได้) มีขั้นตอนการจัดการที่ค่อนข้างซับซ้อน ซึ่งต้องปฏิบัติตามขั้นตอนอย่างต่ำ 4 ขั้นตอนดังนี้คือ

  - ต้องทำการอนุญาตให้สามารถล็อกอินจากเครื่องอื่นที่ไม่ใช่เครื่องไฟร์วอลโดยต้องแก้ไขที่ไฟล์
  - ต้องสร้างคอนเน็กชันที่อนุญาตให้มีการเชื่อมต่อระหว่างเครื่องระยะไกลกับเครื่องไฟร์วอล
  - ต้องเปลี่ยนแปลงค่าในยูสเซอร์ของผู้ดูแลระบบให้สามารถล็อกอินจากเครื่องอื่นได้
  - จากนั้นก็ทำการติดตั้งโปรแกรม Configuration Client ให้กับเครื่องที่ต้องการล็อกอินเข้ามายังเครื่องไฟร์วอล

- ไฟร์วอลวัน

  มีการจัดการกับล็อกอินระยะไกลที่ค่อนข้างง่าย เพียงแค่เพิ่มชื่อเครื่องที่อนุญาตให้ทำการล็อกอินระยะไกลโดยเพิ่มเข้าไปในแถบ GUI Clients ของหน้าต่าง Check Point Configuration Tool จากนั้นก็ทำการติดตั้งโปรแกรม remote client ลงไปในเครื่องไคลเอ็นต์ระยะไกล

- กันเล็ตไฟร์วอล

  มีการจัดการกับการล็อกอินระยะไกลค่อนข้างง่าย เพียงแค่เพิ่มชื่อเครื่องที่ต้องการให้สามารถล็อกอินระยะไกลในหน้าต่าง Remote Management Configuration จากนั้นก็ติดตั้งโปรแกรมไคลเอ็นต์ของกันเล็ตในเครื่องระยะไกล

- ไฟร์วอลทูลคิต

  ไฟร์วอลทูลคิตมีการจัดการกับล็อกอินระยะไกลได้ง่าย และสะดวกเพราะเป็นระบบปฏิบัติการยูนิกซ์ โดยใช้คำสั่ง telnet มายังเครื่องไฟร์วอลด้วยสิทธิรูตก็สามารถคอนฟิกไฟร์วอลได้ หรือใช้ Secure Shell ซึ่งมีความปลอดภัยสูงกว่า telnet มีการเข้ารหัสพาสเวิร์ด ดังนั้นฟีเจอร์นี้ไม่ต้องคอนฟิกเลย

- นอกจากนี้ยังตรวจสอบด้วยว่าการล็อกอินจากระยะไกลของผู้ดูแลระบบจากระยะไกลว่ามีการเข้ารหัส (Encryption) หรือไม่

	การเข้ารหัส (Encryption) ในการล็อกอินระยะไกล
ไอบีเอ็มไฟร์วอล	3
ไฟร์วอลวัน	4

กันเล็ตไฟร์วอล	0
ไฟร์วอลทูลคิต	5

- ไอบีเอ็มไฟร์วอล

  มีการจัดการในส่วนนี้ที่ค่อนข้างยุ่งยาก เพราะต้องใช้คอมมานด์พรอมต์ในการตั้งค่า โดยใช้ยูทิลิตี้ที่มีมากับไฟร์วอลแล้ว คือ utility mkkf ซึ่งเป็นยูทิลิตี้ที่ใช้สำหรับสร้างไฟล์ที่ใช้ในการเข้ารหัสจากระยะไกล ซึ่งมีคำสั่งอยู่หลายคำสั่งโดยการกดคีย์ของคำสั่งเหล่านั้นผ่านคอมมานด์พรอมต์

- ไฟร์วอลวัน

  มีการจัดการในส่วนนี้ค่อนข้างง่าย และสะดวก เพียงแค่เพิ่มการเข้ารหัสในกฎที่เราต้องการ โดยคลิ้กขวาที่แถบ Action ของหน้าต่าง Policy Editor โดยไม่มีความยุ่งยากเหมือนของไอบีเอ็มไฟร์วอล

- กันเล็ตไฟร์วอล

  ในกันเล็ตไฟร์วอลไม่มีฟีเจอร์ในการเข้ารหัส ซึ่งอาจจะเป็นเพราะว่าเป็นซอฟแวร์ที่ดาวน์โหลดมาใช้ฟรีได้ 30 วันเท่านั้น

- ไฟร์วอลทูลคิต

  มีการจัดการที่สะดวกและง่ายที่สุดในไฟร์วอลทั้งหมด คือไม่ต้องทำการคอนฟิกเลย โดยใช้ Secure Shell ซึ่งมีการเข้ารหัสพาสเวิร์ดอยู่แล้ว

สถานการณ์ที่ 2 การเข้าถึงเซอร์วิส และเซอร์วิสที่มีในระบบ

- การพิจารณาการเข้าถึงข้อมูลโดยใช้หมายเลขเครื่อง

	การพิจารณาการเข้าถึงข้อมูลโดยใช้หมายเลขเครื่อง
ไอบีเอ็มไฟร์วอล	3
ไฟร์วอลวัน	4
กันเล็ตไฟร์วอล	3
ไฟร์วอลทูลคิต	2

- ไอบีเอ็มไฟร์วอล

  มีการจัดการที่ยุ่งยากกว่าไฟร์วอลตัวอื่น การสร้างกฎการกรองแพ็กเก็ตจะต้องมีองค์ประกอบจากหลายส่วน ซึ่งองค์ประกอบแต่ละอย่างจะอยู่แยกกัน ไม่ได้ประกอบอยู่ในหน้าต่างเดียวกันเหมือนไฟร์วอลตัวอื่นๆ ขอสรุปขั้นตอนสั้นๆ ดังนี้

  - ต้องสร้างออบเจ็กต์ซึ่งเป็นเสมือนชื่อที่ใช้เรียกแทนไอพีแอดเดรส หรือกลุ่มของไอพีแอดเดรส หรือเครือข่าย
  - ต้องพิจารณาที่ Services ที่อยู่ในหน้าต่าง Configuration Client ว่ามีเซอร์วิสที่สร้างให้แล้วหรือเปล่า ถ้ามีก็สามารถสร้างคอนเน็กชัน แล้วเลือกเซอร์วิสที่เราต้องการได้ทันที แต่ถ้าไม่มีเซอร์วิสที่ต้องการก็จะต้องทำการสร้าง rules ขึ้นมาใหม่ก่อน

แล้วจากนั้นสร้างเซอร์วิส โดยเพิ่ม rules ที่ได้สร้างขึ้นมาใหม่เข้าไป แล้วทำการสร้างคอนเน็กชันต่อไป

- ไฟร์วอลวัน

  มีการจัดการในการสร้างกฎการกรองแพ็กเก็ตที่เข้าใจง่ายและสะดวกที่สุดในบรรดาผลิตภัณฑ์ไฟร์วอลที่นำมาทดสอบ มีหน้าต่างหลักในการตั้งค่าเพียงหน้าต่างเดียว แม้จะมีหน้าต่างย่อยๆ ประกอบอยู่มากมาย แต่ก็เข้าใจได้ง่ายและสะดวกกว่าการมีหลายหน้าต่างแยกกัน

- กันเล็ตไฟร์วอล

  มีการจัดการค่อนข้างซับซ้อน แม้จะอยู่ภายในหน้าต่างหลักเพียงหน้าต่างเดียว แต่การจัดวางกล่องป้อนข้อความ หรือปุ่มต่างๆ ไม่ค่อยเป็นระเบียบ และยากในการสื่อความหมายกว่าของไฟร์วอลวัน

- ไฟร์วอลทูลคิต

  ในไฟร์วอลทูลคิต การกรองแพ็กเก็ตว่าอนุญาตให้แพ็กเก็ตผ่านได้หรือไม่ ต้องพิจารณาจากกฎ ซึ่งกฎการกรองแพ็กเก็ตเหล่านี้เก็บอยู่ในไฟล์ /etc/ipf.rules ต้องทำการศึกษาถึง Syntax ของกฎซึ่งมีออปชันต่างๆ มากมาย ต้องเข้าใจการทำงานของออปชันแต่ละออปชัน และลักษณะของกฎมีรูปแบบเป็นเท็กซ์ไฟล์ ซึ่งต้องสร้างกฎด้วยการพิมพ์ตัวอักษรจากคีย์บอร์ดโดยใช้เอดิเตอร์ที่มีในระบบเช่น editor vi เป็นต้น ถึงแม้ว่ากฎทุกกฎสจะถูกสร้างอยู่ในไฟล์ๆ เดียว การจัดการจึงมีความลำบากกว่าไฟร์วอลตัวอื่น

- การพิจารณาการเข้าถึงข้อมูลจากผู้ใช้งาน

	การพิจารณาการเข้าถึงข้อมูลจากผู้ใช้งาน
ไอบีเอ็มไฟร์วอล	4
ไฟร์วอลวัน	5
กันเล็ตไฟร์วอล	4
ไฟร์วอลทูลคิต	3

- ไอบีเอ็มไฟร์วอล

  มีหน้าต่างที่ใช้จัดการกับยูสเซอร์ในระบบที่ค่อนข้างง่าย สามารถเพิ่มยูสเซอร์เข้าไปในระบบ และสามารถแก้ไขข้อมูลของยูสเซอร์แต่ละคนได้ง่าย สามารถกำหนดสิทธิ์ให้ยูสเซอร์แต่ละคนใช้บริการใดผ่านไฟร์วอลได้ สามารถกำหนดอายุการใช้งานของพาสเวิร์ดของยูสเซอร์แต่ละคนได้

- ไฟร์วอลวัน

  มีหน้าต่างในการจัดการกับยูสเซอร์ที่ค่อนข้างง่ายพอกับไอบีเอ็มไฟร์วอล แต่มีความยืดหยุ่นในการจัดการพิสูจน์ตนในแต่ละเซอร์วิสดีกว่าของไอบีเอ็มไฟร์วอล สามารถ

กำหนดวัน เวลาให้ยูสเซอร์แต่ละคนสามารถใช้บริการที่อนุญาตให้ได้ นอกจากนี้ไฟร์วอลวันยังมีออปชันให้เลือกในการทำการพิสูจน์ตนที่หลากหลายกว่าไอบีเอ็มไฟร์วอล

- กันเล็ตไฟร์วอล

  มีหน้าต่างในการจัดการกับยูสเซอร์ค่อนข้างง่ายพอๆ กับไอบีเอ็มไฟร์วอล สามารถเลือกวิธีการพิสูจน์ตนได้หลายวิธี ซึ่งอาจจะทำการพิสูจน์ตนด้วยยูสเซอร์ของไฟร์วอลหรือยูสเซอร์ในระบบเอ็นที หรืออื่นๆ ได้

- ไฟร์วอลทูลคิต

  ไฟร์วอลทูลคิตทำงานอยู่บนระบบปฏิบัติการ openBSD ซึ่งเป็นระบบปฏิบัติการยูนิกซ์ประเภทหนึ่ง โดยการทำงานของไฟร์วอลทูลคิตนี้มีการสั่งงานผ่านคอมมานด์พรอมต์ ไม่มีการจัดการที่เป็นหน้าจอวินโดว์สที่มีปุ่มซึ่งสามารถคลิ๊กได้อย่างสะดวก การจัดการกับยูสเซอร์จึงค่อนข้างลำบากกว่าไฟร์วอลอื่นๆ

- เทลเน็ต (Telnet)

	เทลเน็ต (Telnet)
ไอบีเอ็มไฟร์วอล	3
ไฟร์วอลวัน	5
กันเล็ตไฟร์วอล	4
ไฟร์วอลทูลคิต	2

- ไอบีเอ็มไฟร์วอล

  การอนุญาตให้บริการเทลเน็ตผ่านไฟร์วอล เราจะต้องมีคอนเน็กชันให้บริการนี้ผ่านไปได้ ซึ่งต้องพิจารณาจากเซอร์วิส ซึ่งในไอบีเอ็มไฟร์วอลมีเซอร์วิสที่อนุญาตให้ใช้บริการเทลเน็ตผ่านไฟร์วอลอยู่แล้ว การจัดการก็เพียงแค่สร้างคอนเน็กชันขึ้นมาแล้วก็เพิ่มเซอร์วิสนั้นๆ เข้าไป แต่ไอบีเอ็มยังมีการจัดการที่ยุ่งยากอยู่ตรงที่ว่าจะต้องสร้างคอนเน็กชันเชื่อมต่อ 2 ฝั่งด้วยกันคือ ระหว่างเครือข่ายภายในกับการ์ดแลนของไฟร์วอลฝั่งที่เชื่อมต่อกับเครือข่ายภายใน และระหว่างการ์ดแลนของไฟร์วอลฝั่งที่เชื่อมต่อกับเครือข่ายภายนอกกับเครือข่ายภายนอก

- ไฟร์วอลวัน

  การอนุญาตให้บริการเทลเน็ตผ่านไฟร์วอลวัน มีการจัดการที่ค่อนข้างง่าย และสะดวกกว่าของไอบีเอ็มไฟร์วอลมาก เพราะในไฟร์วอลวันสามารถสร้างกฎอนุญาตให้ใช้บริการต่างๆ ซึ่งรวมอยู่ในหน้าต่างเดียวที่สามารถเลือกได้ว่าจะอนุญาตให้เครื่องต้นทางเครื่องใดใช้บริการเครื่องปลายทางเครื่องใด และอนุญาตให้ใช้บริการใด ซึ่งในที่นี้คือบริการเทลเน็ต

- กันเล็ตไฟร์วอล

ในกันเล็ตไฟร์วอลมีการจัดการเกี่ยวกับการอนุญาตบริการต่างๆ ค่อนข้างง่ายกว่าของไอบีเอ็มไฟร์วอล แต่ยังมีความซับซ้อนมากกว่าไฟร์วอลวัน โดยกันเล็ตไฟร์วอลสามารถกำหนดเครื่องต้นทาง เครื่องปลายทาง และกำหนดว่าจะอนุญาตให้เซอร์วิสใดผ่านได้บ้าง ในที่นี้คือให้บริการเทลเน็ตผ่านได้ แต่การจัดการไม่ได้อยู่รวมกันภายในหน้าต่างเดียวกัน มีการแยกไปจัดการเป็นส่วนๆ ซึ่งค่อนข้างสับสนมากกว่าไฟร์วอลวัน

- ไฟร์วอลทูลคิต

  การจัดการค่อนข้างซับซ้อนกว่าบนระบบวินโดว์ส ซึ่งต้องแก้ไขไฟล์ถึง 3 ไฟล์คือไฟล์ /etc/services, /etc/inetd.conf, /usr/local/etc/netperm-table และต้องเพิ่มกฎการกรองแพ็กเก็ตเพื่ออนุญาตบริการนี้ด้วย นอกจากนี้ยังต้องศึกษารูปแบบคำสั่งที่เพิ่มเข้าไปในไฟล์ดังกล่าวด้วย

- เอฟทีพี (FTP)

	เอฟทีพี (FTP)
ไอบีเอ็มไฟร์วอล	3
ไฟร์วอลวัน	5
กันเล็ตไฟร์วอล	4
ไฟร์วอลทูลคิต	2

- ไอบีเอ็มไฟร์วอล

  การจัดการกับบริการเอฟทีพีเหมือนกับบริการเทลเน็ตดังที่ได้กล่าวมาแล้ว เพียงแค่ทำการเปลี่ยนจากเซอร์วิสที่อนุญาตให้บริการเทลเน็ตผ่านมาเป็นเซอร์วิสที่อนุญาตให้บริการเอฟทีพีผ่าน

- ไฟร์วอลวัน

  มีการจัดการค่อนข้างง่าย และสะดวกเหมือนกับบริการเทลเน็ต คือเพียงแค่เพิ่มเซอร์วิสที่อนุญาตการบริการเอฟทีพีเข้าไปในกฎข้อเดียวกับบริการเทลเน็ตดังที่ได้กล่าวมาแล้วก็จะสามารถใช้บริการนี้ได้

- กันเล็ตไฟร์วอล

  ดังที่กล่าวมาแล้วในบริการเทลเน็ตของกันเล็ตไฟร์วอล เพียงแค่เปลี่ยนเซอร์วิสจากบริการเทลเน็ตเป็นเอฟทีพีแทน

- ไฟร์วอลทูลคิต

  การจัดการค่อนข้างซับซ้อนกว่าบนระบบวินโดว์ส ซึ่งต้องแก้ไขไฟล์ถึง 3 ไฟล์คือไฟล์ /etc/services, /etc/inetd.conf, /usr/local/etc/netperm-table และต้องเพิ่มกฎการกรองแพ็กเก็ตเพื่ออนุญาตบริการนี้ด้วย นอกจากนี้ยังต้องศึกษารูปแบบคำสั่งที่เพิ่มเข้าไปในไฟล์ดังกล่าวด้วย

- เอชทีทีพี (HTTP)

	เอชทีทีพี (HTTP)
ไอบีเอ็มไฟร์วอล	3
ไฟร์วอลวัน	5
กันเล็ตไฟร์วอล	4
ไฟร์วอลทูลคิต	2

- ไอบีเอ็มไฟร์วอล

  การจัดการกับบริการเอชทีทีพีเหมือนกับบริการเทลเน็ตดังที่ได้กล่าวมาแล้ว เพียงแค่ทำการเปลี่ยนจากเซอร์วิสที่อนุญาตให้บริการเทลเน็ตผ่านมาเป็นเซอร์วิสที่อนุญาตให้บริการเอชทีทีพีผ่าน

- ไฟร์วอลวัน

  มีการจัดการที่ค่อนข้างง่าย และสะดวกเหมือนกับบริการเทลเน็ต คือเพียงแค่เพิ่มเซอร์วิสที่อนุญาตการบริการเอชทีทีพีเข้าไปในกฎข้อเดียวกับบริการเทลเน็ตดังที่ได้กล่าวมาแล้ว ก็จะสามารถใช้บริการนี้ได้

- กันเล็ตไฟร์วอล

  ดังที่กล่าวมาแล้วในบริการเทลเน็ตของกันเล็ตไฟร์วอล เพียงแค่เปลี่ยนเซอร์วิสจากบริการเทลเน็ตเป็นเอชทีทีพีแทน

- ไฟร์วอลทูลคิต

  การจัดการค่อนข้างซับซ้อนกว่าบนระบบวินโดว์ส ซึ่งต้องแก้ไขไฟล์ถึง 3 ไฟล์คือไฟล์ /etc/services, /etc/inetd.conf, /usr/local/etc/netperm-table และต้องเพิ่มกฎการกรองแพ็กเก็ตเพื่ออนุญาตบริการนี้ด้วย นอกจากนี้ยังต้องศึกษารูปแบบคำสั่งที่เพิ่มเข้าไปในไฟล์ดังกล่าวด้วย

- ดีเอ็นเอส (DNS)

	ดีเอ็นเอส (DNS)
ไอบีเอ็มไฟร์วอล	4
ไฟร์วอลวัน	4
กันเล็ตไฟร์วอล	4
ไฟร์วอลทูลคิต	4

- ไอบีเอ็มไฟร์วอล

  มีการจัดการที่ค่อนข้างง่ายในไอบีเอ็มไฟร์วอล โดยทำการปรับแต่งค่าแค่ 2 ส่วนดังนี้ 1. ในหน้าต่าง Security policy ให้คลิ้กถูกในช่องที่อนุญาตดีเอ็นเอส

  2. ในหน้าต่าง Domain Name Service ก็ให้ป้อนชื่อ และไอพีแอดเดรสของเครื่องที่เป็นโดเมนเนมเซิร์ฟเวอร์

- ไฟร์วอลวัน

  มีการจัดการที่ค่อนข้างง่าย เพียงแค่ปรับตั้งค่าในไดอะล็อก Property ของหน้าต่าง Check Point Policy Editor แล้วคลิ้กถูกที่ช่อง Accept Domain Name Over UDP (Queries) และช่อง Accept Domain Name Over TCP (Zone Transfer)

- กันเล็ตไฟร์วอล

  กันเล็ตไฟร์วอลไม่มีฟีเจอร์เกี่ยวกับดีเอ็นเอสที่มีมาให้กับไฟร์วอล

- ไฟร์วอลทูลคิต

  มีการจัดการที่ค่อนข้างง่าย โดยการเพิ่มกฎการกรองแพ็กเก็ตที่อนุญาตให้แพ็กเก็ตที่ใช้บริการพอร์ต 53 ผ่านลงในไฟล์ ipf.rules แล้วทำการ execute ไฟล์นี้ทำให้ไฟร์วอลสามารถให้บริการนี้ผ่านได้

สถานการณ์ที่ 3 การเก็บล็อกไฟล์

- ความยากง่ายในการจัดการล็อกไฟล์

	ความยากง่ายในการจัดการล็อกไฟล์
ไอบีเอ็มไฟร์วอล	3
ไฟร์วอลวัน	5
กันเล็ตไฟร์วอล	4
ไฟร์วอลทูลคิต	2

- ไอบีเอ็มไฟร์วอล

  มีการจัดการล็อกที่ดีพอประมาณ มีการแบ่งประเภทของล็อกไฟล์ที่จัดเก็บ สามารถเลือกปริมาณล็อกไฟล์ที่เก็บตามความสำคัญของข้อมูลที่จัดเก็บ แต่การจัดการต้องมีการปรับตั้งค่าจากหลายหน้าต่าง ทำให้เกิดความซับซ้อนเพิ่มขึ้น นอกจากนี้ยังมีการเก็บล็อกที่อยู่นอกเหนือจากที่กล่าวมาแล้ว โดยมีการแยกการจัดการออกไปต่างหาก ทำให้ผู้ใช้อาจเกิดความสับสนได้

- ไฟร์วอลวัน

  มีการจัดการล็อกที่ค่อนข้างง่าย และสะดวก โดยมีหน้าต่างที่ใช้จัดการ และแสดงผลการเก็บล็อกเพียงหน้าต่างเดียว โดยขั้นแรกจะต้องกำหนดในหน้าต่างที่ใช้กฎการกรองแพ็กเก็ตว่าจะให้กฎข้อใดทำการเก็บล็อกบ้าง จากนั้นก็เปิดหน้าต่างที่ใช้จัดการกับล็อกซึ่งมีรูปแบบแสดงผลที่อ่านง่าย เข้าใจง่าย สามารถเลือกดูล็อกได้ตามขอบเขตที่ต้องการ

- กันเล็ตไฟร์วอล

  กันเล็ตไฟร์วอลมีการจัดการล็อกที่ค่อนข้างง่าย มีการจัดการอยู่ภายในหน้าต่างเดียว สามารถกำหนดอายุการเก็บล็อกไฟล์ สามารถสร้างรายงานประวันหรือประจำสัปดาห์ แต่มีการแสดงผลล็อกที่อ่านเข้าใจยาก และแสดงให้เห็นแบบไม่เป็นระเบียบ ไม่สามารถจำแนกประเภทของล็อกที่ต้องการเลือกดูได้เหมือนกับของไฟร์วอลวัน

- ไฟร์วอลทูลคิต

  มีการแบ่งระดับการเก็บล็อกออกเป็นหลายระดับเช่น emerg, alert เป็นต้น ทำให้สามารถแยกประเภท ปริมาณ และความสำคัญที่ทำการจัดเก็บได้ แต่การคอนฟิกจะต้องศึกษาการทำงานของออปชันต่างๆ และรูปแบบคำสั่ง ทำให้มีความยุ่งยากกว่าระบบวินโดว์ส และการอ่านตรวจดูล็อกไฟล์ลำบากกว่าบนระบบวินโดว์ส ดังนั้นคะแนนที่ได้จึงต่ำที่สุด

จากการให้คะแนนในแต่ละสถานการณ์เราสามารถสรุปคะแนน และรวมคะแนนของผลิตภัณฑ์ไฟร์วอลได้ดังตารางข้างล่างนี้

สถานการณ์	ไอบีเอ็ม ไฟร์วอล	ไฟร์วอลวัน	กันเล็ต ไฟร์วอล	ไฟร์วอลทูล คิต
สถานการณ์ที่ 1 การจัดการไฟร์วอลจากเครื่องระยะไกล				
• เตือนผู้ดูแลระบบผ่านทางอีเมล์ หรือเพจเจอร์	5 คะแนน	5 คะแนน	4 คะแนน	0 คะแนน
• ยินยอมให้ผู้ดูแลระบบปิดการติดต่อกับอินเทอร์เน็ตจากระยะไกล	2 คะแนน	4 คะแนน	3 คะแนน	5 คะแนน
• การเข้ารหัส (Encryption) ในการล็อกอินระยะไกล	3 คะแนน	4 คะแนน	0 คะแนน	5 คะแนน
สถานการณ์ที่ 2 การเข้าถึงเซอร์วิส และเซอร์วิสที่มีในระบบ				
• การพิจารณาการเข้าถึงข้อมูลโดยใช้หมายเลขเครื่อง	3 คะแนน	4 คะแนน	3 คะแนน	2 คะแนน
• การพิจารณาการเข้าถึงข้อมูลจากผู้ใช้งาน	4 คะแนน	5 คะแนน	4 คะแนน	3 คะแนน
• เทลเน็ต (Telnet)	3 คะแนน	5 คะแนน	4 คะแนน	2 คะแนน
• เอฟทีพี (FTP)	3 คะแนน	5 คะแนน	4 คะแนน	2 คะแนน
• เอชทีทีพี (HTTP)	3 คะแนน	5 คะแนน	4 คะแนน	2 คะแนน
• ดีเอ็นเอส (DNS)	4 คะแนน	4 คะแนน	4 คะแนน	4 คะแนน
สถานการณ์ที่ 3 การเก็บล็อกไฟล์				
• ความยากง่ายในการจัดการล็อกไฟล์	3 คะแนน	5 คะแนน	4 คะแนน	2 คะแนน
รวมคะแนน	33	46	34	27

ตารางที่ 5-3 แสดงการสรุปคะแนนในการทดสอบการจัดการ

สรุปผลการทดสอบด้านการจัดการ

ผลการทดสอบการจัดการที่ได้ออกมาในรูปของคะแนน เมื่อพิจารณาคะแนนรวมแล้วผลิตภัณฑ์ที่ได้รับคะแนนสูงสุดเป็นผลิตภัณฑ์ที่ง่ายต่อการใช้งานมากที่สุด ผลิตภัณฑ์ที่ได้คะแนนน้อยกว่ามีความง่ายในการใช้งานลดลงไปตามลำดับด้วย ซึ่งเมื่อรวมคะแนนแล้วเห็นว่าไฟร์วอลวันได้รับคะแนนสูงสุด นั่นคือ

ไฟร์วอลวันมีการจัดการที่ง่ายที่สุด

รองลงมาคือกันเล็ตไฟร์วอล

รองลงมาเป็นอันดับสามคือไอบีเอ็มไฟร์วอล

และสุดท้ายคือไฟร์วอลทูลคิตได้คะแนนน้อยที่สุด

แต่ในกรณีของกันเล็ตไฟร์วอล และไฟร์วอลทูลคิตซึ่งมีอยู่ 1 ออปชันที่ไม่สนับสนุนจึงได้ 0 คะแนน ทำให้การพิจารณาให้คะแนนไม่ได้ขึ้นกับความยากง่ายโดยแท้จริง ดังนั้นการนำกันเล็ต และไฟร์วอลทูลคิตมาพิจารณาความยากง่ายในการจัดการ จึงไม่ควรนำออปชันที่ไม่มีมาพิจารณาให้คะแนน ดังนั้นคะแนนที่ผลิตภัณฑ์ไฟร์วอลทั้ง 4 ได้รับควรเป็นดังนี้คือ ไฟร์วอลวันได้ 37 คะแนน กันเล็ตไฟร์วอลได้ 30 คะแนน ไอบีเอ็มได้ 25 คะแนน และสุดท้ายไฟร์วอลทูลคิตได้ 22 คะแนน ซึ่งจะเห็นได้ว่าการจัดการของกันเล็ตไฟร์วอลง่ายกว่าของไอบีเอ็มไฟร์วอล

แต่ถ้าต้องการเปรียบเทียบความง่ายในการจัดการในแต่ละสถานการณ์ก็สามารถนำคะแนนที่ได้รับในแต่ละสถานการณ์มารวมกัน แล้วก็นำมาเปรียบเทียบกันก็จะรู้ว่าในแต่ละสถานการณ์นั้นผลิตภัณฑ์ไฟร์วอลตัวใดมีการจัดการที่ง่ายกว่ากัน หรือพิจารณาเป็นข้อย่อยๆ ไปเลยก็ได้

การพิจารณาในการให้คะแนน

การพิจารณาในการให้คะแนนในหัวข้อต่างๆ ของไฟร์วอลแต่ละตัวนั้น ทางกลุ่มได้พิจารณาโดยใช้เหตุผลหลายประการดังต่อไปนี้

- ประสบการณ์การใช้งานโปรแกรมของตัวผู้ทดสอบเอง
- จากเอกสารการพิจารณาให้คะแนนในการจัดการผลิตภัณฑ์ไฟร์วอล ซึ่งมีส่วนในการเพิ่มแนวคิดในการพิจารณาให้คะแนนได้หลากหลายแนวทางมากยิ่งขึ้น
- นอกจากจะอาศัยการพิจารณาจากประสบการณ์ของสมาชิกในกลุ่มซึ่งมีกันแค่ 2 คนแล้ว ทางกลุ่มก็ยังได้ทำการสอบถามจากบุคคลอื่นๆ ที่อยู่ในสาขานี้ด้วย เพื่อเป็นการรับประกันว่าผลการให้คะแนนออกมาจะไม่เป็นการพิจารณาไปเองโดยสมาชิกในกลุ่มเท่านั้น และเพื่อลดข้อสงสัยว่าผลการให้คะแนนจะเกิดจากความพอใจความชื่นชอบในผลิตภัณฑ์ไฟร์วอลไม่เท่ากันเป็นผลทำให้การพิจารณาในการให้คะแนนในผลิตภัณฑ์ไฟร์วอลตัวที่ชอบจะได้รับคะแนนมากกว่า แต่ทางกลุ่มขอยืนยันว่าได้พิจารณาด้วยความยุติธรรม

หมายเหตุ

ทางกลุ่มได้นำไฟร์วอลทูลคิตมาเปรียบเทียบในส่วนของการจัดการ ซึ่งไฟร์วอลทูลคิตมีการทำงานอยู่บนระบบ OpenBSD มีการจัดการที่เป็นแบบเท็กซ์โหมด ส่วนผลิตภัณฑ์ไฟร์วอลตัวอื่นๆ มีลักษณะการจัดการที่เป็นแบบวินโดวส์ ดังนั้นไฟร์วอลทูลคิตจึงค่อนข้างจะเสียเปรียบไฟร์วอลอื่นๆ

เอกสารที่ใช้อ้างอิงในการทดสอบการจัดการมีดังนี้ ผู้เรียบเรียงเอกชัย รัตนดิลกชัย, " 19 Firewall กับการปกป้องอินทราเน็ตของคุณ", ไบต์ ไทยแลนด์, ปีที่ 4 ฉบับที่ 42 เดือนตุลาคม 2540 ,หน้า 95-110

5.8 การทดสอบประสิทธิภาพการส่งถ่ายข้อมูลของไฟร์วอล

หลักการ ในการทดสอบประสิทธิภาพของไฟร์วอลนั้น ถ้าเราจะมองเครือข่ายเปรียบเสมือนระบบท่อน้ำ ไฟร์วอลเปรียบได้กับที่กรองน้ำ น้ำในท่อเป็นเหมือนข้อมูลที่ส่งผ่านไปมาในเครือข่าย และประสิทธิภาพในการกรองน้ำ(อัตราเร็วของน้ำหลังผ่านที่กรองเทียบกับอัตราเร็วของน้ำก่อนผ่านที่กรอง) เหมือนกับประสิทธิภาพในการส่งถ่ายข้อมูลของไฟร์วอล ซึ่งที่กรองน้ำที่ดีควรจะกรองน้ำได้สะอาด และสามารถกรองน้ำได้อย่างรวดเร็ว ไฟร์วอลก็เป็นเช่นเดียวกันคือไฟร์วอลที่ดีควรกั้นไม่ให้บริการหรือแพ็ก

เก็ตที่เป็นอันตรายผ่านเข้ามายังเครือข่าย และควรส่งถ่ายข้อมูลได้อย่างรวดเร็วไม่ควรเป็นคอขวดของเครือข่าย

วิธีการทดสอบ ในการทดสอบนี้เราจะแบ่งเป็น 2 ส่วน โดยแต่ละส่วนจะใช้ไฟร์วอลแบบ Single Firewall เหมือนกัน โดยแตกต่างกันในส่วนของขนาดสายในการเชื่อมต่อและจำนวนของไคลเอ็นต์ที่ใช้บริการผ่านไฟร์วอลพร้อมๆ กัน ดังนี้

การทดสอบส่วนที่1

โดยรูปแบบของการเชื่อมต่อในส่วนแรกเป็นดังรูปต่อนี้

รูปที่ 5-4 แสดงโครงสร้างทางกายภาพในการทดสอบประสิทธิภาพส่วนที่ 1

จากรูป ทุกๆ การเชื่อมต่อมีอัตราเร็วไม่เกิน 100 เมกะบิตต่อวินาทีทั้งหมด โดยในการทดสอบเราจะทำตามขั้นตอนดังต่อไปนี้

1. ดาวน์โหลดข้อมูลจากไฟล์เซิร์ฟเวอร์ในเครือข่ายภายนอกผ่านไฟร์วอลมายังเครือข่ายภายใน แล้วบันทึกอัตราเร็วในการดาวน์โหลด โดยทำซ้ำอย่างนี้ 10 ครั้งแล้วหาค่าเฉลี่ย
2. ทำข้อ 1 กับไฟร์วอลอื่นๆ
3. ทำข้อ 1 กับเกตเวย์ที่ไม่ใช่ไฟร์วอล

ส่วนประกอบของระบบที่ใช้ทดสอบ

เครื่องไคลเอ็นต์ มีส่วนประกอบหลักดังนี้

- ซีพียูเพ็นเทียมโปร 150 เมกะเฮิร์ต
- หน่วยความจำขนาด 32 เมกะไบต์
- การ์ดแลนความเร็ว 100 เมกะบิตต่อวินาที

เครื่องไฟร์วอล

- ซีพียูเซเลลอน 400 เมกะเฮิร์ต
- หน่วยความจำขนาด 128 เมกะไบต์
- การ์ดแลนความเร็ว 100 เมกะบิตต่อวินาที 2 การ์ด

เครื่องไฟล์เซิร์ฟเวอร์

- ซีพียูแบบดูอัลโพรเซสเซอร์
- หน่วยความจำขนาด 128 เมกะไบต์
- การ์ดแลนความเร็ว 100 เมกะบิตต่อวินาที

ผลการทดสอบในส่วนที่1

ผลการทดลองได้ผลดังตารางนี้

ครั้งที่	อัตราเร็วที่ใช้ดาวน์โหลด (เมกะบิตต่อวินาที)				
	ไม่มีไฟร์วอล	IBM Firewall (Proxy)	IBM Firewall (Packet Filtering)	Firewall-1 (Stateful Inspection)	ไฟร์วอลทูลคิต (Proxy)
1	29.16	23.16	27.55	28.76	13.25
2	30.55	24.26	27.71	28.37	13.97
3	28.46	24.05	32.46	28.79	14.86
4	28.30	23.94	28.24	29.13	13.69
5	28.02	23.36	28.4	27.58	15.19
6	29.29	23.58	28.43	30.25	15.36
7	27.89	23.69	29.13	29.50	14.67
8	29.40	24.03	28.76	27.52	15.68
9	30.18	24.48	28.53	30.48	14.77
10	28.24	24.19	29.86	27.80	15.19
ผลเฉลี่ย	**28.95**	**23.87**	**28.90**	**28.82**	**14.66**

ตารางที่ 5-4 แสดงคะแนนในการทดสอบประสิทธิภาพส่วนที่ 1

วิเคราะห์ผลการทดลอง

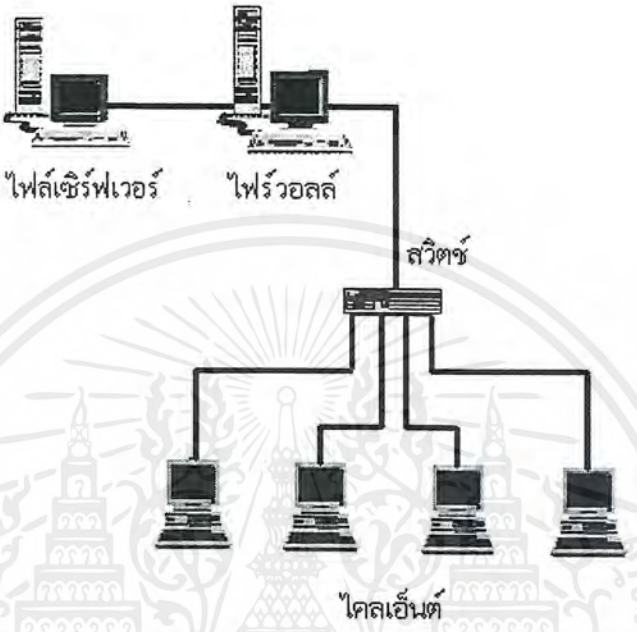
ถ้าเรามองจากโครงสร้างของเครือข่ายที่เราจำลองขึ้นมาแล้ว เมื่อมีการดาวน์โหลดข้อมูลจากไฟล์เซิร์ฟเวอร์ผ่านเกตเวย์ซึ่งไม่มีไฟร์วอลมายังเครื่องไคลเอ็นต์แล้ว อัตราเร็วของการเชื่อมต่อน่าจะใกล้เคียง 100 เมกะบิตต่อวินาที แต่จากผลการทดลองเราได้อัตราเร็วเพียง 28.95 เมกะบิตต่อวินาทีเท่านั้น ซึ่งถ้าเราวิเคราะห์ถึงโครงสร้างทางฮาร์ดแวร์ของเครื่องไคลเอ็นต์แล้วเราได้คำตอบคือ ที่อัตราเร็วของการเชื่อมต่อได้มาเป็นเช่นนี้เป็นเพราะอัตราเร็วของฮาร์ดดิสก์ในเครื่องไคลเอ็นต์มีอัตราเร็วในการส่งข้อมูลไม่เกิน 33 เมกะบิตต่อวินาที ทำให้ฮาร์ดดิสก์ตัวนี้เป็นตัวถ่วงอัตราเร็วในการส่งถ่ายข้อมูลระหว่างไคลเอ็นต์กับเซิร์ฟเวอร์ เป็นผลให้ได้ผลดังการทดลอง

เมื่อเราพิจารณาดูอัตราเร็วของผลิตภัณฑ์ไฟร์วอลซึ่งใช้ฟังก์ชันการทำงานไม่เหมือนกันได้ว่าผลิตภัณฑ์ที่ใช้พร็อกซีมีอัตราเร็วในการส่งข้อมูลช้ากว่าไฟร์วอลแบบอื่นมาก ส่วนอีกสองแบบคือแพ็กเก็ตฟิลเตอริงกับสเตตฟูลอินสเป็กชัน มีอัตราเร็วใกล้เคียงกันโดยแพ็กเก็ตฟิลเตอร์มีอัตราเร็วมากกว่าสเตตฟูลอินสเป็กชันเล็กน้อย

และเมื่อเปรียบเทียบไอบีเอ็มไฟร์วอล กับไฟร์วอลทูลคิตซึ่งไฟร์วอลที่เป็นพร็อกซีทั้งคู่ ผลที่ได้รับคือไอบีเอ็มไฟร์วอลสามารถส่งผ่านข้อมูลได้เร็วกว่าไฟร์วอลทูลคิตทั้งที่มีฟังก์ชันการทำงานเหมือนกัน

การทดสอบส่วนที่สอง

ในส่วนที่สองใช้รูปแบบของการเชื่อมต่อดังรูป



รูปที่ 5-5 แสดงโครงสร้างทางกายภาพในการทดสอบประสิทธิภาพส่วนที่ 2

จากรูป ในเครือข่ายภายนอกที่เราจำลองขึ้นมา ไฟล์เซิร์ฟเวอร์จะต่อตรงกับไฟร์วอลโดยมีอัตราเร็วในการส่งข้อมูลระหว่างกันไม่เกิน 100 เมกะบิตต่อวินาที และในเครือข่ายภายในมีสวิตช์ที่ต่อตรงกับไฟร์วอลมีอัตราเร็วในการเชื่อมต่อกับไฟร์วอลเช่นเดียวกับไฟล์เซิร์ฟเวอร์คือไม่เกิน 100 เมกะบิตต่อวินาที และสวิตช์นี้ต่อกับเครื่องไคลเอ็นต์จำนวนหนึ่งโดยในแต่ละการเชื่อมต่อระหว่างไคลเอ็นต์กับสวิตช์มีอัตราเร็วในการเชื่อมต่อไม่เกิน 10 เมกะบิตต่อวินาที ขั้นตอนในการทดสอบในส่วนที่สองมีดังนี้

1. ดาวน์โหลดข้อมูลจากไฟร์เซิร์ฟเวอร์ผ่านไฟร์วอลโดยใช้เครื่องไคลเอ็นต์ 1 เครื่อง โดยทำซ้ำอย่างนี้ 10 ครั้ง แล้วหาค่าเฉลี่ย
2. ทำเหมือนข้อ 1 แต่เพิ่มเครื่องไคลเอ็นต์ทีละเครื่อง จนครบ 4 เครื่อง
3. ทำ ข้อ 1 และ 2 กับไฟร์วอลอื่นๆ เขียนตารางของอัตราเร็วเฉลี่ยของไฟร์วอลแต่ละตัว

ส่วนประกอบของระบบที่ใช้ทดสอบ

เครื่องไคลเอ็นต์จำนวน 4 เครื่อง มีส่วนประกอบหลักดังนี้

- ซีพียูเพนเทียม
- หน่วยความจำขนาด 32 เมกะไบต์
- การ์ดแลนความเร็ว 100 เมกะบิตต่อวินาที

เครื่องไฟร์วอล

- ซีพียูเซเลลอน 400 เมกะเฮิร์ต
- หน่วยความจำขนาด 128 เมกะไบต์
- การ์ดแลนความเร็ว 100 เมกะบิตต่อวินาที 2 การ์ด

เครื่องไฟล์เซิร์ฟเวอร์

- ซีพียูแบบดูอัลโพรเซสเซอร์
- หน่วยความจำขนาด 128 เมกะไบต์
- การ์ดแลนความเร็ว 100 เมกะบิตต่อวินาที

ผลการทดสอบได้แสดงในตารางข้างล่างนี้ ซึ่งแสดงอัตราเร็วที่ได้รับในการดาวน์โหลดข้อมูลจากไฟล์เซิร์ฟเวอร์โดยใช้เครื่องไคลเอ็นต์ตั้งแต่ 1 เครื่อง 2 เครื่องพร้อมกัน 3 เครื่องพร้อมกัน 4 เครื่องพร้อมกัน

ผลการทดสอบไอบีเอ็มไฟร์วอลที่เป็นพร็อกซี

ครั้งที่	อัตราเร็วในการดาวน์โหลด (เมกะบิตต่อวินาที)					
	1 เครื่อง	2 เครื่องพร้อมกัน		3 เครื่องพร้อมกัน		
	เครื่องที่ 1	เครื่องที่ 1	เครื่องที่ 2	เครื่องที่ 1	เครื่องที่ 2	เครื่องที่ 3
1	7.69	7.51	7.15	7.8	7.72	7.86
2	7.59	7.51	7.75	6.98	7.65	7.78
3	7.56	7.53	7.49	6.45	7.71	7.34
4	7.58	7.5	7.33	7.25	7.67	7.09
5	7.57	7.52	7.27	7.83	7.64	7.87
6	7.54	7.49	7.65	7.66	7.82	7.88
7	7.56	7.48	7.83	7.81	7.75	7.4
8	7.54	7.52	7.63	6.54	7.76	7.79
9	7.55	7.52	7.15	7.25	7.81	7.84
10	7.53	7.5	7.4	7.83	7.65	7.87
เฉลี่ย	**7.57**	**7.51**	**7.47**	**7.34**	**7.72**	**7.67**

ตารางที่ 5-5 แสดงอัตราเร็วในการดาวน์โหลดข้อมูลโดยใช้เครื่องไคลเอ็นต์ตั้งแต่ 1 เครื่อง 2 เครื่อง 3 เครื่องพร้อมกันของไอบีเอ็มไฟร์วอลแบบพร็อกซี

ครั้งที่	อัตราเร็วในการดาวน์โหลด (เมกะบิตต่อวินาที)			
	4 เครื่องพร้อมกัน			
	เครื่องที่ 1	เครื่องที่ 2	เครื่องที่ 3	เครื่องที่ 4
1	7.15	7.18	7.3	7.58
2	7.15	6.92	7.6	7.58
3	7.14	7.25	7.5	7.58
4	7.17	7.22	7.58	7.6
5	7.15	7.26	7.47	7.55
6	7.14	7.26	7.36	7.52
7	7.11	7.53	7.49	7.52
8	7.14	6.8	7.34	7.55
9	7.17	7.5	7.33	7.55
10	7.24	7.5	7.64	7.65
เฉลี่ย	**7.16**	**7.24**	**7.46**	**7.57**

ตารางที่ 5-6 แสดงอัตราเร็วในการดาวน์โหลดข้อมูลโดยใช้เครื่องไคลเอ็นต์ 4 เครื่องพร้อมกันของไอบีเอ็ม ไฟร์วอลแบบพร็อกซี

ผลการทดสอบไฟร์วอลวัน

ได้ผลดังตารางข้างล่างนี้

ครั้งที่	อัตราเร็วในการดาวน์โหลด (เมกะบิตต่อวินาที)					
	1 เครื่อง	2 เครื่องพร้อมกัน		3 เครื่องพร้อมกัน		
	เครื่องที่ 1	เครื่องที่ 1	เครื่องที่ 2	เครื่องที่ 1	เครื่องที่ 2	เครื่องที่ 3
1	7.69	7.64	7.9	7.6	7.92	7.86
2	7.66	7.65	8.02	7.59	7.65	7.86
3	7.67	7.64	7.16	7.6	5.49	7.7
4	7.64	7.64	6.56	7.61	7.11	7.73
5	7.66	7.66	8.05	7.6	7.65	7.56
6	7.68	7.63	7.44	7.65	8.01	7.97
7	7.68	7.65	7.51	7.63	7.48	8.06
8	7.7	7.65	7.24	7.63	7.11	7.95
9	7.72	7.67	7.73	7.63	7.24	7.92
10	7.65	7.65	7.91	7.64	7.63	7.84
เฉลี่ย	**7.68**	**7.65**	**7.55**	**7.62**	**7.33**	**7.85**

ตารางที่ 5-7 แสดงอัตราเร็วในการดาวน์โหลดข้อมูลโดยใช้เครื่องไคลเอ็นต์ตั้งแต่ 1 เครื่อง 2 เครื่อง 3 เครื่อง พร้อมกันของไฟร์วอลวัน

ครั้งที่	อัตราเร็วในการดาวน์โหลด (เมกะบิตต่อวินาที)			
	4 เครื่องพร้อมกัน			
	เครื่องที่ 1	เครื่องที่ 2	เครื่องที่ 3	เครื่องที่ 4
1	7.56	7.57	7.81	8.02
2	7.59	7.1	7.92	8.02
3	7.61	5.68	7.98	8.08
4	7.56	7.9	7.93	8.03
5	7.59	7.33	7.98	8
6	7.58	7.8	7.9	8.06
7	7.63	6.43	7.81	8.09
8	7.51	7.61	7.79	8.02
9	7.6	7.58	7.98	8.07
10	7.62	7.91	7.9	8.04
เฉลี่ย	**7.59**	**7.29**	**7.9**	**8.04**

ตารางที่ 5-8 แสดงอัตราเร็วในการดาวน์โหลดข้อมูลโดยใช้เครื่องไคลเอ็นต์ 4 เครื่องพร้อมกันของไฟร์วอลวัน

ผลการทดสอบไฟร์วอลทูลคิต

ครั้งที่	อัตราเร็วในการดาวน์โหลด (เมกะบิตต่อวินาที)					
	1 เครื่อง	2 เครื่องพร้อมกัน		3 เครื่องพร้อมกัน		
	เครื่องที่ 1	เครื่องที่ 1	เครื่องที่ 2	เครื่องที่ 1	เครื่องที่ 2	เครื่องที่ 3
1	5.49	5.48	5.73	5.47	5.79	5.7
2	5.49	5.49	5.79	5.51	5.79	5.74
3	5.48	5.49	5.65	5.51	5.67	5.69
4	5.49	5.47	5.8	5.51	5.69	5.66
5	5.48	5.5	5.8	5.5	5.62	5.69
6	5.48	5.5	5.72	5.46	5.84	5.65
7	5.5	5.48	5.72	5.5	5.73	5.69
8	5.5	5.53	5.79	5.52	5.68	5.77
9	5.54	5.5	5.75	5.49	5.8	5.73
10	5.47	5.5	5.57	5.48	5.86	5.68

เฉลี่ย	**5.49**	**5.49**	**5.73**	**5.5**	**5.75**	**5.7**

ตารางที่ 5-9 แสดงอัตราเร็วในการดาวน์โหลดข้อมูลโดยใช้เครื่องไคลเอ็นต์ตั้งแต่ 1 เครื่อง 2 เครื่อง 3 เครื่อง พร้อมกันของไฟร์วอลทูลคิต

ครั้งที่	อัตราเร็วในการดาวน์โหลด (เมกะบิตต่อวินาที)			
	4 เครื่องพร้อมกัน			
	เครื่องที่ 1	เครื่องที่ 2	เครื่องที่ 3	เครื่องที่ 4
1	5.54	5.47	5.74	5.81
2	5.5	5.81	5.66	5.81
3	5.48	5.79	5.67	5.81
4	5.49	5.35	5.71	5.82
5	5.52	5.66	5.68	5.85
6	5.52	5.35	5.75	5.84
7	5.52	5.67	5.66	5.77
8	5.51	5.46	5.57	5.77
9	5.46	5.76	5.67	5.8
10	5.47	5.66	5.63	5.77
เฉลี่ย	**5.5**	**5.63**	**5.67**	**5.81**

ตารางที่ 5-10 แสดงอัตราเร็วในการดาวน์โหลดข้อมูลโดยใช้เครื่องไคลเอ็นต์ 4 เครื่องพร้อมกันของไฟร์วอลทูลคิต

จากผลการทดลองที่ได้สามารถเฉลี่ยอัตราเร็วที่ของการดาวน์โหลด 1 เครื่อง 2 เครื่องพร้อมกัน 3 เครื่องพร้อมกัน 4 เครื่องพร้อมกันของไอบีเอ็มไฟร์วอล ไฟร์วอลวัน และไฟร์วอลทูลคิตดังนี้

ผลเฉลี่ยในการดาวน์โหลดของไอบีเอ็มไฟร์วอลที่เป็นพร็อกซี

	อัตราเร็วเฉลี่ยในการดาวน์โหลด (เมกะบิตต่อวินาที)			
	1 เครื่อง	2 เครื่องพร้อมกัน	3 เครื่องพร้อมกัน	4 เครื่องพร้อมกัน
ค่าเฉลี่ย	7.57	7.49	7.58	7.36

ตารางที่ 5-11 แสดงผลเฉลี่ยในการดาวน์โหลดของไอบีเอ็มไฟร์วอลที่เป็นพร็อกซี

ผลเฉลี่ยในการดาวน์โหลดของไฟร์วอลวัน

	อัตราเร็วเฉลี่ยในการดาวน์โหลด (เมกะบิตต่อวินาที)			
	1 เครื่อง	2 เครื่องพร้อมกัน	3 เครื่องพร้อมกัน	4 เครื่องพร้อมกัน
ค่าเฉลี่ย	7.68	7.6	7.6	7.71

ตารางที่ 5-12 แสดงผลเฉลี่ยในการดาวน์โหลดของไฟร์วอลวัน

ผลเฉลี่ยในการดาวน์โหลดของไฟร์วอลทูลคิต

	อัตราเร็วเฉลี่ยในการดาวน์โหลด (เมกะบิตต่อวินาที)			
	1 เครื่อง	2 เครื่องพร้อมกัน	3 เครื่องพร้อมกัน	4 เครื่องพร้อมกัน
ค่าเฉลี่ย	5.49	5.61	5.65	5.65

ตารางที่ 5-13 แสดงผลเฉลี่ยในการดาวน์โหลดของไฟร์วอลทูลคิต

วิเคราะห์ผลการทดลอง

จากผลการทดลองที่ได้ออกมาจะเห็นว่าเมื่อเปรียบเทียบอัตราเร็วในการดาวน์โหลดข้อมูลของไอบีเอ็มไฟร์วอล ไฟร์วอลวัน และไฟร์วอลทูลคิตเมื่อมีจำนวนเครื่องที่ใช้ดาวน์โหลดเท่ากัน จะได้ผลออกมาว่าไฟร์วอลวันมีอัตราเร็วในการดาวน์โหลดข้อมูลมากที่สุด ไอบีเอ็มไฟร์วอลที่เป็นพร็อกซีมีอัตราเร็วรองลงมา ส่วนไฟร์วอลทูลคิตช้าที่สุด ซึ่งโดยปกติแล้วไฟร์วอลมีฟังก์ชันการทำงานเป็นสเตตฟูลอินสเป็กชันจะเร็วกว่าไฟร์วอลที่เป็นพร็อกซี ดังนั้นเราจึงคาดหวังไว้ว่าไฟร์วอลวันที่มีฟังก์ชันการทำงานเป็นสเตตฟูลอินสเป็กชันมีอัตราเร็วในการส่งข้อมูลดีกว่าไอบีเอ็มไฟร์วอลและไฟร์วอลทูลคิตที่เป็นพร็อกซี และผลการทดสอบก็ออกมาตามที่ได้คาดหวังไว้ และเมื่อเปรียบเทียบไอบีเอ็มไฟร์วอลกับไฟร์วอลทูลคิตที่เป็นไฟร์วอลแบบพร็อกซีทั้งคู่ก็จะได้ผลออกมาว่าไอบีเอ็มไฟร์วอลเร็วกว่าเหมือนกับผลการทดสอบส่วนที่ 1

ในส่วนของการเพิ่มจำนวนเครื่องที่ใช้ดาวน์โหลดพร้อมกัน เพื่อเปรียบเทียบผลิตภัณฑ์ไฟร์วอลแต่ละตัวว่ามีอัตราเร็วในการส่งผ่านข้อมูลเมื่อมีจำนวนเครื่องเพิ่มขึ้นแล้วเป็นอย่างไร ผลที่ออกมาจะเห็นได้ว่าอัตราเร็วในการดาวน์โหลด 4 เครื่องพร้อมกันของไฟร์วอลวันยังเร็วกว่าดาวน์โหลดด้วยเครื่องเพียงเครื่องเดียว หรืออัตราเร็วในการดาวน์โหลด 3เครื่องพร้อมกันของไอบีเอ็มไฟร์วอลยังเร็วกว่าดาวน์โหลดด้วยเครื่องเพียงเครื่องเดียว หรืออัตราเร็วในการดาวน์โหลดหลายเครื่องพร้อมกันของไฟร์วอลทูลคิตยังเร็วกว่าดาวน์โหลดด้วยเครื่องเพียงเครื่องเดียว เหตุผลที่เป็นเช่นนี้อาจเนื่องมาจากอัตราเร็วที่ใช้ดาวน์โหลดด้วยเครื่องเพียงเครื่องเดียวทางกลุ่มได้ใช้เครื่องที่ 1ทดสอบ ซึ่งประสิทธิภาพของเครื่องที่ 1 ต่ำกว่าเครื่องอื่นๆ อัตราเร็วที่ได้เมื่อทำการดาวน์โหลดเครื่องเดียวจึงต่ำกว่าดาวน์โหลดด้วยเครื่องหลายๆ เครื่อง

สรุปผลการทดสอบโดยรวมในแต่ละด้านที่ทดสอบ

ด้านความปลอดภัย

จากผลการทดสอบ

- ไฟร์วอลทูลคิตมีความปลอดภัยสูงที่สุด
- ไฟร์วอลวันมีความปลอดภัยรองลงมา
- ไอบีเอ็มไฟร์วอลมีความปลอดภัยต่ำที่สุด ซึ่งไอบีเอ็มแบบพร็อกซีจะมีความปลอดภัยสูงกว่าแบบกรองแพ็กเก็ต

ด้านการจัดการ

- ไฟร์วอลวันมีการจัดการที่ง่ายและสะดวกมากที่สุด
- กันเล็ตไฟร์วอลมีการจัดการที่ง่ายและสะดวกรองลงมา
- ไอบีเอ็มไฟร์วอลมีการจัดการที่ง่าย และสะดวกเป็นอันดับ 3
- ไฟร์วอลทูลคิตมีการจัดการที่ง่ายและสะดวกต่ำที่สุด

ด้านประสิทธิภาพ

- ไอบีเอ็มที่เป็นแบบกรองแพ็กเก็ตมีประสิทธิภาพสูงที่สุด
- ไฟร์วอลวันมีประสิทธิภาพรองลงมาเป็นอันดับสอง
- ไอบีเอ็มที่เป็นพร็อกซีมีประสิทธิภาพรองลงมาเป็นอันดับสาม
- ไฟร์วอลทูลคิตมีประสิทธิภาพต่ำที่สุด

สามารถสรุปเป็นตารางแสดงการจัดอันดับผลิตภัณฑ์ได้ดังนี้

อันดับ	1	2	3	4
ด้านความปลอดภัย	ไฟร์วอลทูลคิต	ไฟร์วอลวัน	ไอบีเอ็มไฟร์วอล แบบพร็อกซี	ไอบีเอ็มไฟร์วอล แบบกรองแพ็กเก็ต
ด้านการจัดการ	ไฟร์วอลวัน	กันเล็ตไฟร์วอล	ไอบีเอ็มไฟร์วอล	ไฟร์วอลทูลคิต
ด้านประสิทธิภาพ	ไอบีเอ็มไฟร์วอล แบบกรองแพ็กเก็ต	ไฟร์วอลวัน	ไอบีเอ็มไฟร์วอล แบบพร็อกซี	ไฟร์วอลทูลคิต

ตารางที่ 5-14 แสดงสรุปอันดับของผลิตภัณฑ์ไฟร์วอล

แนวทางในการพิจารณาเลือกใช้ผลิตภัณฑ์ไฟร์วอล

หากต้องเลือกผลิตภัณฑ์ไฟร์วอลที่เหมาะสมสำหรับองค์กร มีปัจจัยที่ต้องพิจารณาดังที่ทางกลุ่มได้ทดสอบอยู่ 3 ประการ การที่จะเลือกผลิตภัณฑ์ใดมาใช้นั้นก็อยู่ที่ว่านโยบายขององค์กรเล็งเห็นถึงความสำคัญด้านใดเป็นหลัก เมื่อเทียบกับผลการทดสอบที่ทางกลุ่มได้ทำการทดสอบ เห็นได้ว่าไฟร์วอลแต่ละผลิตภัณฑ์จะมีจุดเด่นจุดด้อยแตกต่างกัน ถ้าองค์กรเล็งเห็นถึงความปลอดภัยเป็นหลักก็เหมาะที่จะเลือกใช้ไฟร์วอลทูลคิต ถ้าองค์กรใดเล็งเห็นในด้านการจัดการเป็นหลักก็เหมาะที่จะเลือกใช้ไฟร์วอลวัน สุดท้ายถ้าองค์กรใดให้ความสำคัญด้านประสิทธิภาพเป็นหลักก็เหมาะที่จะเลือกใช้ไอบีเอ็มไฟร์วอล แต่การพิจารณาเลือกผลิตภัณฑ์นี้ไม่ได้หมายความว่าจะพิจารณาจากปัจจัยด้านเดียวแล้วไม่พิจารณาปัจจัยอื่นๆ ร่วมด้วย ตัวอย่างเช่น ผลิตภัณฑ์ไฟร์วอลอย่างหนึ่งมีประสิทธิภาพสูงมาก แต่ในด้านความปลอดภัยกลับต่ำมากอย่างนี้ก็ไม่สมควรเลือกใช้ ดังนั้นการพิจารณาควรพิจารณาจากหลายๆ ปัจจัย ซึ่งไม่มีหลักเกณฑ์ในการพิจารณาที่แน่นอนตายตัว

นอกจากนี้ยังมีปัจจัยอื่นๆ ที่ทางกลุ่มไม่ได้นำมาร่วมด้วย อย่างเช่น ราคาของผลิตภัณฑ์ มีความสำคัญในการพิจารณาด้วย เพราะผลิตภัณฑ์ไฟร์วอลที่มีคุณภาพดี แต่เมื่อพิจารณาราคาแล้วมีราคาสูงจนองค์กรไม่สามารถซื้อหามาใช้ได้ก็ไม่มีประโยชน์อะไรในการนำผลิตภัณฑ์นั้นมาพิจารณา

บทที่ 6

การออกแบบระบบไฟร์วอลของภาควิชาคอมพิวเตอร์

ในภาควิชาคอมพิวเตอร์ขณะนี้ยังไม่มีการจัดการด้านความปลอดภัยที่ดี ทางกลุ่มจึงได้ออกแบบระบบไฟร์วอลของภาควิชาคอมพิวเตอร์เพื่อเพิ่มความปลอดภัยให้มากยิ่งขึ้น ข้อมูลบางส่วนที่สำคัญจะถูกเก็บในที่ๆ ปลอดภัย การเข้าใช้งานระบบจากภายนอกมีการจัดการอย่างปลอดภัยมากขึ้น

6.1 ผู้ใช้งานภายในภาควิชา

สามารถแบ่งผู้ใช้งานภายในภาควิชาออกเป็น 4 ระดับด้วยกันดังนี้

1. บุคคลทั่วไป
2. นักศึกษาในภาควิชาคอมพิวเตอร์
3. อาจารย์ และเจ้าหน้าที่ในภาควิชา
4. ผู้ดูแลระบบ

6.2 ขอบเขตพื้นที่ใช้งานของผู้ใช้งาน

สามารถแบ่งขอบเขตของพื้นที่ที่ผู้ใช้งานระบบเข้ามาใช้งานระบบภายในภาควิชาเป็น 2 สถานที่ด้วยกันดังนี้

1. ผู้ใช้งานจากภายในภาควิชาคอมพิวเตอร์
2. ผู้ใช้งานจากภายนอกภาควิชา

6.3 นโยบายความปลอดภัยสำหรับยูสเซอร์ระดับต่างๆ ในสถานที่ต่างๆ

6.3.1 บุคคลทั่วไป (ใช้งานจากสถานที่ใดๆ จากภายนอกภาควิชา)

สามารถเข้าใช้บริการที่ภาควิชาดังนี้

- บริการเว็บเซิร์ฟเวอร์ของภาควิชา (www.ce.kmitl.ac.th)
- บริการ anonymous ftp (jade.ce.kmitl.ac.th)
- ส่งเมล์ติดต่อกับผู้ใช้งานภายในภาควิชาคอมพิวเตอร์ได้
- บริการ DNS (Domain Name Service)

6.3.2 นักศึกษาภายในภาควิชาคอมพิวเตอร์

สามารถใช้งานทุกอย่างเหมือนบุคคลทั่วไป นอกจากนี้ยังมีบริการอื่นแบ่งตามกรณีๆ ไปดังนี้

กรณีที่นักศึกษาใช้งานเครื่องภายในภาควิชาคอมพิวเตอร์ มีนโยบายดังนี้

- สามารถเข้าเว็บของภาควิชา หรือเว็บไซต์อื่นๆ บนอินเทอร์เน็ตได้
- มีแอ็กเคาต์ให้สำหรับนักศึกษาทุกคนบนเครื่อง diamond.ce.kmitl.ac.th และ jasper.ce.kmitl.ac.th ซึ่งนักศึกษาสามารถใช้บริการดังนี้
  - ส่งเมล์ติดต่อกับบุคคลภายนอกภาควิชา

- มีเนื้อที่สำหรับเก็บข้อมูล โดยนักศึกษาสามารถใช้บริการ ftp เพื่อนำข้อมูลมาเก็บได้
- นักศึกษาสามารถสร้างเว็บเพจส่วนตัวสู่อินเทอร์เน็ตได้ (Personal Web Page)

- บริการ telnet หรือ ftp มายังเครื่อง diamond หรือ jasper หรือเครื่องอื่นๆ ภายนอกภาควิชาที่นักศึกษามีแอ็กเคาต์อยู่ได้
- มีแอ็กเคาต์ให้สำหรับนักศึกษาบนเครื่อง compnet.ce.kmitl.ac.th และ complan.ce.kmitl.ac.th ซึ่งเป็นระบบเน็ตแวร์ ซึ่งมีบริการดังนี้
  - สามารถล็อกอินด้วยโปรแกรมไคลเอ็นต์ของเน็ตแวร์
  - มีเนื้อที่เก็บข้อมูลสำหรับนักศึกษา ซึ่งปลอดภัยกว่าบนเครื่อง diamond และ jasper
  - มีโปรแกรมติดตั้งที่สามารถดาวน์โหลดได้
  - มีบริการเกี่ยวกับการพิมพ์
- สามารถใช้บริการ pirch, irc, icq ส่วนบริการอื่นๆ ในทำนองเดียวกันนี้จะต้องขออนุญาตเป็นกรณีๆ ไป

กรณีที่นักศึกษาใช้งานเครื่องภายนอกภาควิชา เช่น จากเครื่องของทางสถาบัน หรือหมุนโมเด็มโดยใช้เบอร์ของสถาบัน มีนโยบายดังนี้

- สามารถเข้าสู่เว็บไซต์ของภาควิชา
- มีแอ็กเคาต์ให้สำหรับนักศึกษาบนเครื่อง diamond และ jasper ดังที่ได้กล่าวมาแล้ว
- นักศึกษาต้องใช้โปรแกรม ssh และ ftp แบบเข้ารหัสพาสเวิร์ดมายังเครื่อง diamond หรือ jasper เท่านั้น โดยไม่สามารถใช้ telnet หรือ ftp แบบปกติได้
- สามารถล็อกอินมายังเครื่อง compnet หรือ complan โดยใช้โปรแกรมไคลเอ็นต์ของเน็ตแวร์ดังที่ได้กล่าวมาแล้ว

6.3.3 อาจารย์ภายในภาควิชาคอมพิวเตอร์

สามารถใช้บริการเหมือนบุคคลทั่วไปทุกอย่าง นอกจากนี้ยังมีบริการอื่นๆ ซึ่งแบ่งเป็นกรณีๆ ไปดังนี้

กรณีที่อาจารย์ใช้งานเครื่องภายในภาควิชาคอมพิวเตอร์ (ส่วนใหญ่เป็นเครื่องส่วนตัว) มีนโยบายดังนี้

- สามารถเข้าเว็บของภาควิชา หรือเว็บไซต์อื่นๆ บนอินเทอร์เน็ตได้
- มีแอ็กเคาต์ให้สำหรับอาจารย์ทุกท่านบนเครื่อง diamond.ce.kmitl.ac.th และ jasper.ce.kmitl.ac.th ซึ่งสามารถใช้บริการดังนี้
  - ส่งเมล์ติดต่อกับบุคคลภายนอกภาควิชา
  - มีเนื้อที่สำหรับเก็บข้อมูล โดยสามารถใช้บริการ ftp เพื่อนำข้อมูลมาเก็บได้
  - สามารถสร้างเว็บเพจส่วนตัวสู่อินเทอร์เน็ตได้ (Personal Web Page)
- บริการ telnet หรือ ftp มายังเครื่อง diamond หรือ jasper หรือเครื่องอื่นๆ ภายนอกภาควิชาที่มีแอ็กเคาต์อยู่ได้

- มีแอ็กเคาต์ให้สำหรับอาจารย์ทุกท่านบนเครื่อง compnet.ce.kmitl.ac.th และ complan.ce.kmitl.ac.th ซึ่งเป็นระบบเน็ตแวร์ ซึ่งมีบริการดังนี้
  - สามารถล็อกอินด้วยโปรแกรมไคลเอ็นต์ของเน็ตแวร์
  - มีเนื้อที่เก็บข้อมูลสำหรับอาจารย์ ซึ่งปลอดภัยกว่าบนเครื่อง diamond และ jasper
  - มีโปรแกรมติดตั้งที่สามารถดาวน์โหลดได้
  - มีบริการเกี่ยวกับการพิมพ์
- สามารถใช้บริการ pirch, irc, icq ส่วนบริการอื่นๆ ในทำนองเดียวกันนี้จะต้องแจ้งต่อผู้ดูแลระบบเป็นกรณีๆ ไป
- สามารถใช้บริการ notes บนเครื่อง notes server ดังนี้
  - สามารถล็อกอินด้วยโปรแกรม notes client
  - มีเนื้อที่เก็บข้อมูลสำหรับอาจารย์ทุกท่าน
  - มีโปรแกรมจัดการข้อมูลนักศึกษา

กรณีที่อาจารย์ใช้งานเครื่องภายนอกภาควิชา เช่น จากเครื่องในสถาบัน หรือหมุนโมเด็มโดยใช้เบอร์ของสถาบัน มีนโยบายดังนี้

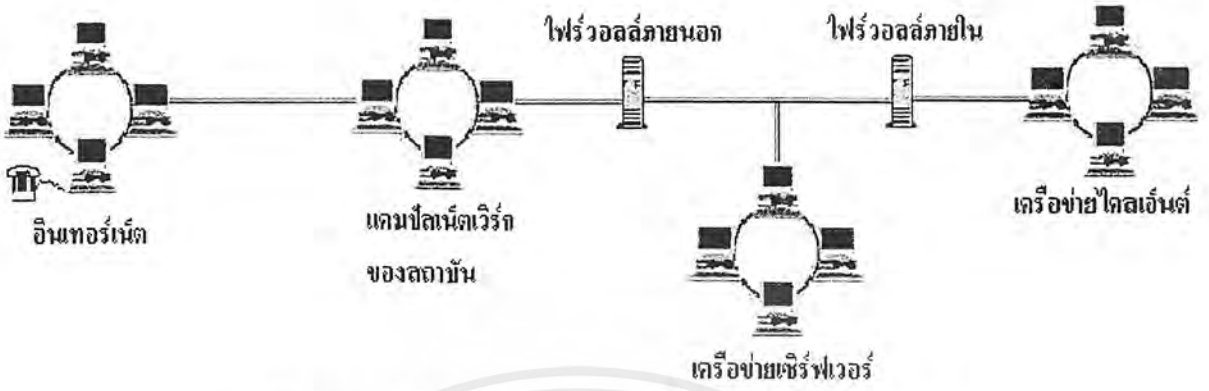
- สามารถเข้าสู่เว็บไซต์ของภาควิชา
- มีแอ็กเคาต์ให้สำหรับอาจารย์ทุกท่านบนเครื่อง diamond และ jasper ดังที่ได้กล่าวมาแล้ว
- อาจารย์ทุกท่านต้องใช้โปรแกรม ssh และ ftp แบบเข้ารหัสพาสเวิร์ดมายังเครื่อง diamond หรือ jasper เท่านั้น โดยไม่สามารถใช้ telnet หรือ ftp แบบปกติได้
- สามารถล็อกอินมายังเครื่อง compnet หรือ complan โดยใช้โปรแกรมไคลเอ็นต์ของเน็ตแวร์ ซึ่งต้องติดตั้งลงในเครื่องของอาจารย์
- สามารถใช้บริการ notes บนเครื่อง notes server ดังที่ได้กล่าวมาแล้ว

6.3.4 ผู้ดูแลระบบเครือข่ายภาควิชาคอมพิวเตอร์

ผู้ดูแลระบบไม่ใช่ผู้ใช้บริการ แต่เป็นผู้จัดการระบบเครือข่ายดังนี้

- ผู้ดูแลระบบไม่สามารถล็อกอินมายังเครื่องเซิร์ฟเวอร์ที่ให้บริการของภาควิชาจากเครื่องภายนอกภาควิชาได้
- สามารถล็อกอินด้วยสิทธิรูตเข้ายังเซิร์ฟเวอร์ที่ให้บริการได้โดยตรง หรือใช้ ssh และ ftp ที่เข้ารหัสพาสเวิร์ดเมื่อล็อกอินจากเครื่องอื่นภายในภาควิชา
- จัดการ และแก้ไขระบบเมื่อเกิดข้อบกพร่องหรือมีผู้ประสงค์ร้ายเข้ามาในระบบ

6.4 โครงสร้างทางกายภาพของระบบไฟร์วอลของภาควิชาคอมพิวเตอร์



รูปที่ 6-1 แสดงโครงสร้างทางกายภาพของระบบไฟร์วอลของภาควิชา

โครงสร้างทางกายภาพของระบบไฟร์วอลของภาควิชาได้ออกแบบโดยใช้โครงสร้างไฟร์วอลแบบ 2 เลเยอร์คือมีไฟร์วอลภายนอก และไฟร์วอลภายใน ซึ่งไฟร์วอลภายนอกจะเชื่อมต่อระหว่างแคมปัสเน็ตเวิร์กของสถาบันกับเครือข่ายเซิร์ฟเวอร์ ส่วนไฟร์วอลภายในเชื่อมต่อระหว่างเครือข่ายเครือข่ายเซิร์ฟเวอร์กับเครือข่ายไคลเอ็นต์ดังในรูปข้างบน

6.5 เครือข่ายเซิร์ฟเวอร์ (Server Network)

เป็นเครือข่ายที่อยู่ระหว่างไฟร์วอลภายนอกกับไฟร์วอลภายใน เครือข่ายนี้มีความปลอดภัยที่ค่อนข้างต่ำเพราะเนื่องจากประกอบด้วยเครื่องเซิร์ฟเวอร์ที่ให้บริการแก่บุคคลทั้งภายในและภายนอกสถาบันต่างๆ ดังต่อไปนี้

- **เครื่อง Diamond** เปิดบริการดังนี้
  - บริการเก็บข้อมูลนักศึกษา
  - บริการเว็บส่วนตัว (personal web)
  - ส่งจดหมายอิเล็กทรอนิกส์
  - pop3 และ smtp server
  - ให้นักศึกษาและอาจารย์สามารถนำข้อมูลมาเก็บโดยใช้ ftp
  - บริการ Domain Name Server
  - Network Time Server (NTP)
- **เครื่อง Jasper** เปิดบริการดังนี้
  - บริการเก็บข้อมูลนักศึกษา
  - บริการเว็บส่วนตัว (personal web)
  - ส่งจดหมายอิเล็กทรอนิกส์
  - pop3 และ smtp server

- ให้นักศึกษาและอาจารย์สามารถนำข้อมูลมาเก็บโดยใช้ ftp
- บริการ Domain Name Server

- **เครื่อง Topaz** เปิดบริการดังนี้
- บริการเป็นเว็บเซิร์ฟเวอร์ของภาควิชา

- **เครื่อง Jade** เปิดบริการดังนี้
- บริการ Anonymous FTP

- **เครื่อง Amethyst** เปิดบริการดังนี้
- บริการ Remote Access Server

- **เครื่อง Compnet** เปิดบริการดังนี้
- เก็บข้อมูลนักศึกษา
- โปรแกรมติดตั้ง
- บริการเกี่ยวกับการพิมพ์
- ส่งอีเมล์
- บริการ Pop3 และ Smtp server
- ให้นักศึกษาสามารถนำข้อมูลมาเก็บโดยใช้ FTP ได้

- **เครื่อง Compnet** เปิดบริการดังนี้
- โปรแกรมติดตั้ง
- ให้นักศึกษาสามารถนำข้อมูลมาเก็บโดยใช้ FTP ได้
- เป็นแบ็กอัพของเครื่อง Compnet

- **เครื่อง Pearl** เปิดบริการดังนี้
- Primary Domain Controller ของโดเมน CE-NT
- Lotus Notes R5 Server
- DHCP Server

6.6 เครือข่ายไคลเอ็นต์ (Client Network)

เป็นเครือข่ายที่เชื่อมต่ออยู่กับไฟร์วอลภายใน มีความปลอดภัยสูงกว่าเครือข่ายภาควิชาภายนอก ประกอบด้วยเครื่องไคลเอ็นต์ที่ต้องการใช้บริการ

6.7 ประเภทการทำงานของไฟร์วอลภายนอก

ในการออกแบบไฟร์วอลภายนอกจะใช้ไฟร์วอลที่เป็นแบบแพ็กเก็ตฟิลเตอริงรวมกับพร็อกซี และใช้ลักษณะการทำงานที่เป็นแบบ permit some deny all คือจะให้บริการบางส่วนที่อนุญาตผ่านได้ นอกเหนือจากนั้นจะไม่ให้ผ่านทั้งหมด โดยจะแยกเป็น 2 ส่วนคือ inbound และ outbound ดังนี้

6.7.1 การติดต่อสู่ภายใน (Inbound Connection) เป็นการติดต่อจากภายนอกเข้ามาสู่ภายในเครือข่าย ซึ่งมีการอนุญาต และการไม่อนุญาตดังต่อไปนี้

การอนุญาต (Permit) ให้บริการผ่าน มีดังนี้คือ

- บริการเว็บ (http service)
- บริการดีเอ็นเอส (dns service)
- บริการเมล์ (mail service)
- บริการเอฟทีพีแบบไม่ออกนาม (anonymous ftp)
- บริการเอฟทีพีแบบเข้ารหัสพาสเวิร์ด (encrypted ftp) สำหรับเครื่อง diamond และ jasper
- บริการ secure shell (SSH) สำหรับเครื่อง diamond และ jasper
- บริการ Netware Client
- บริการ Notes Client

การไม่อนุญาต (Deny) ให้บริการผ่าน มีดังนี้คือ

- การโจมตีแบบ Deny of services
- IP Spoofing
- บริการ ping
- บริการที่เหลือทั้งหมด

6.7.2 การติดต่อไปภายนอก (Outbound Connection) เป็นการติดต่อจากภายในออกไปสู่ภายนอกเครือข่าย ซึ่งมีการอนุญาต และการไม่อนุญาตดังต่อไปนี้

การอนุญาต (Permit) ให้บริการผ่าน มีดังนี้คือ

- บริการเว็บ (http)
- บริการดีเอ็นเอส (dns service)
- บริการเมล์ (mail service)
- บริการเอฟทีพี (ftp service)
- บริการเทลเน็ต (telnet service)
- บริการ ping
- บริการ pirch, irc, icq

การไม่อนุญาต (Deny) ให้บริการผ่าน มีดังนี้คือ

- บริการที่เหลือทั้งหมด

6.8 ประเภทการทำงานของไฟร์วอลภายใน

ในการออกแบบไฟร์วอลภายในจะใช้ไฟร์วอลที่เป็นแบบสเตฟูลอินสเป็กชัน และใช้ลักษณะการทำงานที่เป็นแบบ permit some deny all คือจะให้บริการบางส่วนที่อนุญาตผ่านได้ นอกเหนือจากนั้นจะไม่ให้ผ่านทั้งหมด โดยจะแยกเป็น 2 ส่วนคือ inbound และ outbound ดังนี้

6.8.1 การติดต่อสู่ภายใน (Inbound Connection) เป็นการติดต่อจากเครือข่ายไคลเอ็นต์เข้ามาสู่เครือข่ายเซิร์ฟเวอร์ หรือเครือข่ายอินเทอร์เน็ต ซึ่งมีการอนุญาต และการไม่อนุญาตดังต่อไปนี้

การอนุญาต (Permit) ให้บริการผ่าน มีดังนี้คือ

- บริการเว็บ (http service)
- บริการดีเอ็นเอส (dns service)
- บริการเมล์ (mail service)
- บริการเอฟทีพีแบบไม่ออกนาม (anonymous ftp)
- บริการเอฟทีพีแบบเข้ารหัสพาสเวิร์ด (encrypted ftp) สำหรับเครื่อง diamond และ jasper
- บริการ secure shell (SSH) สำหรับเครื่อง diamond และ jasper
- บริการ Netware Client
- บริการ Notes Client
- บริการดีเอชซีพี (dhcp service)
- บริการโดเมนคอนโทรลเลอร์ (domain controller service)
- บริการ ping ไปยังภายนอกเครือข่ายภาควิชา

การไม่อนุญาต (Deny) ให้บริการผ่าน มีดังนี้คือ

- ไอพีแอดเดรสจากภายนอกเครือข่ายสถาบัน
- บริการ ping มายังเครือข่ายเซิร์ฟเวอร์
- บริการที่เหลือทั้งหมด

6.8.2 การติดต่อไปภายนอก (Outbound Connection) เป็นการติดต่อจากเครือข่ายเซิร์ฟเวอร์ หรือเครือข่ายอินเทอร์เน็ตไปสู่เครือข่ายโลคอลเอ็นต์ ซึ่งมีการอนุญาต และการไม่อนุญาตดังต่อไปนี้

การอนุญาต (Permit) ให้บริการผ่าน มีดังนี้คือ

- บริการดีเอ็นเอส
- บริการ ping

การไม่อนุญาต (Deny) ให้บริการผ่าน มีดังนี้คือ

- บริการที่เหลือทั้งหมด

6.9 การเลือกใช้ผลิตภัณฑ์ไฟร์วอล

จากการที่ได้ทดสอบผลิตภัณฑ์ไฟร์วอลทั้ง 4 ตัวแล้วทางกลุ่มได้พิจารณาจากความสามารถโดยรวมทั้ง 3 ด้านคือความปลอดภัย การจัดการ และประสิทธิภาพ ซึ่งผลที่ได้จากการทดสอบจะเห็นว่าไฟร์วอลวัน ซึ่งมีความสามารถในระดับที่ดีเกือบทุกๆ ด้านที่ทำการทดสอบ มีการจัดการที่ง่ายและสะดวกที่สุด แม้ว่าไฟร์วอลวันมีความสามารถด้านประสิทธิภาพ และความปลอดภัยรองจากไอบีเอ็มไฟร์วอล และไฟร์วอลทูลคิตตามลำดับก็ตาม แต่ก็เสียเปรียบไม่มากนัก เมื่อสรุปผลโดยรวมแล้วดีที่สุด ดังนั้นการเลือกใช้ผลิตภัณฑ์ไฟร์วอลวันจึงเหมาะสมที่สุด

บทที่ 7

สรุปการทำงาน

วัตถุประสงค์ของโปรเจ็กต์คือการเปรียบเทียบผลิตภัณฑ์ไฟร์วอล และประยุกต์ระบบไฟร์วอลสำหรับเครือข่าย ซึ่งในโปรเจ็กต์นี้คือภาควิชาคอมพิวเตอร์ ซึ่งได้ผลตามวัตถุประสงค์ที่ตั้งไว้ โดยทางกลุ่มของข้าพเจ้าได้เริ่มต้นจากการศึกษาระบบไฟร์วอลดังนี้คือ

- นโยบายความปลอดภัยของระบบเครือข่าย
- การออกแบบระบบไฟร์วอล ซึ่งประกอบด้วย

- ฟังก์ชันการทำงานของไฟร์วอล
- โครงสร้างทางกายภาพของไฟร์วอล
- ปัจจัยในการออกแบบระบบไฟร์วอล
- การเลือกใช้ผลิตภัณฑ์ไฟร์วอลที่เหมาะสม

เมื่อศึกษาถึงระบบไฟร์วอลแล้ว จากนั้นก็นำผลิตภัณฑ์ที่จัดหาได้มาทดสอบความสามารถ

- การทดสอบความสามารถของผลิตภัณฑ์ไฟร์วอลพิจารณาจากปัจจัยหลัก 3 ปัจจัยดังนี้

- ความปลอดภัย (Security)
- การจัดการ (Management)
- ประสิทธิภาพ (Performance)

ซึ่งผลจากการทดสอบสามารถนำมาเปรียบเทียบ วิเคราะห์ และแนะนำผลิตภัณฑ์ที่เหมาะสมสำหรับเลือกใช้ ซึ่งจากผลการทดสอบนี้นำไปใช้ในการพิจารณาเลือกใช้ผลิตภัณฑ์ไฟร์วอลให้กับระบบไฟร์วอลที่ทางกลุ่มได้ออกแบบขึ้นนั่นคือระบบไฟร์วอลของภาควิชา ดังนั้นสุดท้ายคือ

- การออกแบบระบบไฟร์วอลของภาควิชา ดังที่ได้กล่าวถึงในบทที่แล้ว

บรรณานุกรม

หนังสือ

1. D.Brent Chapman and Elizabeth D.Zwicky ,"Building Internet Firewalls", O'Reilly&Associates ,Inc.,1995
2. William R.Cheswick and Steven M.Bellovin ,"Firewalls and Internet Security ", Addison-Wesley Publishing Company , 1994
3. Kevin Washburn and Jim Evans," TCP/IP running a successful network",Addison-Wesley1996
4. อรรณพ ขันธิกุล , กรภัทร์ สุทธิดารา, สัจจะ จรัสรุ่งรวีวร, " Windows NT4.0 Server & Workstation สำหรับผู้บริหารระบบ ", บริษัทดวงกมลสมัย จำกัด

นิตยสาร

1. เอกชัย รัตนดิลกชัย, " 19 Firewall กับการปกป้องอินทราเน็ตของคุณ", ไบต์ ไทยแลนด์, ปีที่ 4 ฉบับที่ 42 เดือนตุลาคม 2540 ,หน้า 95-110

เว็บไซต์

1. http://www.nstl.com/html/firewall_test_methodology.html#security (methodology ของไฟร์วอลล์)
2. http://www.icsa.net/html/communities/firewalls/certification/certified_products/index.shtml (ผลิตภัณฑ์ไฟร์วอลล์)
3. http://www2.icsa.net/portal/portal.ctrl?url=http://www.icsa.net/html/communities/firewalls/buyers_guide/index.shtml (แนะนำการเลือกผลิตภัณฑ์ไฟร์วอลล์)
4. http://www.nstl.com/html/nstl_firewall_testing.html (ทดสอบไฟร์วอลล์)
5. http://www.data.com/lab_tests/firewalls97.html (Don't Get burned March 21,1997)
6. http://www.data.com/lab_tests/firewalls.html (Can firewall take the heat November 21,1995)
7. http://www.data.com/lab_tests/ntfirewalls.html (Though enough April 01,1998)