การศึกษาความเป็นไปได้ในการติดตั้งไฟร์วอลล์ในเครือข่ายภายในองค์กร กรณีศึกษา บริษัท เมอร์ค จำกัด

Feasibility study of Solution to Implement in Oraganization Lan Case study in Merck Company Limited

โดย

นายจักรทิพย์ มหาสวัสดิ์

รหัส 44067636

อาจารย์ที่ปรึกษา

อาจารย์ อัครินทร์ คุณกิตติ

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการศึกษากรณีพิเศษ
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ
ภาคเรียนที่ 1 ปีการศึกษา 2546
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	การศึกษาความเป็นไปได้ในการติดตั้งไฟร์วอลล์ในเครือข่ายภายในองค์กรกรณีศึกษา บริษัท เมอร์ค จำกัด
นักศึกษา	นายจักรทิพย์ มหาสวัสดิ์
อาจารย์ที่ปรึกษา	อาจารย์ อัครินทร์ คุณกิตติ
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	กาจัดการเทคโนโลยีสารสนเทศ
ปีการศึกษา	2546

บทคัดย่อ

ปัจจุบันองค์กรเกือบทุกองค์กรมีเชื่อมต่อซึ่งกันและกันมากขึ้น มีการแลกเปลี่ยนข้อมูลข่าวสารกันอย่างมากมาย และเครือข่ายคอมพิวเตอร์ที่มีขนาดใหญ่ที่สุดในปัจจุบันคืออินเทอร์เน็ท ซึ่งมีเครือข่ายเชื่อมต่อกันขนาดใหญ่ มีผู้ใช้งานเป็นจำนวนมาก ทำให้ต่อมาเริ่มมีปัญหาการบุกรุกเข้ามาในเครือข่ายเพื่อสร้างความเสียหายให้กับเครือข่ายนั้น ไฟร์วอลล์เป็นทางเลือกหนึ่งในหลายๆ ทางเลือกที่สามารถป้องกันภัยคุกคามที่เกิดขึ้นจากเครือข่ายภายนอกได้ โดยระบบไฟร์วอลล์ที่ทำการศึกษาในครั้งนี้มีอยู่ 4 ระบบ คือ ระบบไฟร์วอลล์แบบโอเพ่นซอส ระบบไฟร์วอลล์ซอฟแวร์ลิขสิทธิ์ไฟร์วอลล์วันติดตั้งบนระบบปฏิบัติการวินโดว์ 2000 เซิร์ฟเวอร์ และติดตั้งบนระบบปฏิบัติการโอเพ่นซอส และระบบไฟร์วอลล์แบบฮาร์ดแวร์เฉพาะ โดยใช้เทคนิคในการวิเคราะห์ความเป็นไปได้ทางด้านเทคนิค ทางด้านค่าใช้จ่ายการลงทุน และค่าใช้จ่ายสะสมจำนวน 6 ปี เพื่อวิเคราะห์ทางเลือกที่เหมาะสมกับความต้องการของบริษัท เมอร์ค จำกัด ในการนำระบบไฟร์วอลล์เข้ามาติดตั้งภายในระบบเครือข่าย โดยจากที่ได้ทำการวิเคราะห์โดยใช้การวิเคราะห์ทางด้านเทคนิค และ ทางด้านค่าใช้จ่าย ผลที่ได้คือสามารถตัดสินใจเลือกระบบไฟร์วอลล์ที่เป็นแบบโอเพ่นซอส เนื่องจากเป็นทางเลือกที่มีผลด้านเทคนิคที่ดีในหัวข้อเรื่องการมีเสถียรภาพในการทำงาน และมีความยืดหยุ่นในการใช้งานที่ดี ค่าใช้จ่ายทั้งหมดต่อปี และค่าใช้จ่ายสะสมจำนวน 6ปีมีค่าต่ำที่สุดเมื่อเปรียบเทียบกับทางเลือกในแบบอื่น ทำให้ผลที่ได้จากการศึกษาในครั้งนี้ได้เลือกระบบไฟร์วอลล์ที่เหมาะสมให้กับบริษัท เมอร์ค จำกัด เป็นไฟร์วอลล์แบบโอเพ่นซอส

Title	**Feasibility study of Solution to Implement in Organization Lan Case study in Merck Compay Limited**
Student	Mr. Chaktip Mahasawasde
Advisor	Mr. Akharin Khunkitti
Level of Study	Master of Science in Information Technology
Major	Information Technology Management
Academic Year	2003

Abstract

In present in every organization has many connection to another organization to exchange data and news together . Internet is the biggest network in the world that everyone can use it to search news, data or everything that they want . Everything have pros and cron don't except with internet it have a lot hacker and cracker . Firewall is one choice that can prevent our network from dangerous in the internet . In this case study use 4 choice of firewall solution is Opensource Firewall, Firewall-1 with Windows2000 server, Firewall-1 with Opensource and Network Appliance Firewall Box. In this study use Feasibility study in technical and expense to analyst choice that match with requirement for merck company limited . The result of this Feasibility study show that Opensource firewall is the best way that suitable for merck because the score of technical topic in stable system and flexibility to use is good and total expense per year and Collective expense for 6 years is lower that another solution. The conclusion of this study is Firewall that suitable for Merck company limited is Opensource Firewall

กิตติกรรมประกาศ

การทำโครงการศึกษากรณีพิเศษในครั้งนี้ ข้าพเจ้าขอขอบคุณท่านที่มีส่วนในการให้ความช่วยเหลือ สนับสนุน และส่งเสริมจากหลายบุคคลด้วยกัน โดยเฉพาะอาจารย์อัครินทร์ คุณกิตติ ในการให้คำแนะนำ และหนทางในการแก้ไขปัญหาต่างๆ ในการทำโครงการศึกษากรณีพิเศษตลอดจนผู้ที่ให้ความรู้และความเข้าใจและช่วยเหลือทางด้านข้อมูลแก่ข้าพเจ้า รวมทั้งเพื่อนๆ ที่ให้การสนับสนุนในการศึกษาค้นคว้าข้อมูลที่เกี่ยวข้องต่างๆ จนรายงานของโครงการศึกษากรณีพิเศษเรื่องการศึกษาความเป็นได้ในการการติดตั้งไฟร์วอลล์ในเครือข่ายภายในองค์กรกรณีศึกษา บริษัท เมอร์ค จำกัดสามารสำเร็จสมบูรณ์ลงได้

จักรทิพย์ มหาสวัสดิ์

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

ตารางที่

สารบัญภาพ

หน้า

ภาพที่

บทที่ 1
บทนำ

1.1 ความนำ

ในปัจจุบันอินเทอร์เป็นเครือข่ายที่มีขนาดใหญ่ที่สุดของโลก มีการเชื่อมโยงเครือข่ายหลายร้อยล้านเครือข่ายเข้าด้วยกัน และทำการจัดสรร แบ่งบันการใช้งานทรัพยากรร่วมกัน ไม่ว่าจะเป็นทางด้านการเผยแพร่ความรู้ การกระจายซอฟแวร์เพื่อทดสอบซอฟแวร์ การซื้อขายสินค้าต่างๆ การเผยแพร่ความรู้ทางวิชาการ เป็นต้น ซึ่งเมื่อมีการเชื่อมต่อกันมากขึ้น ทำให้อินเทอร์เน็ทเป็นสถานที่ที่มีอันตรายอยู่มาก เนื่องจากเมื่อมีเครือข่ายมากมายหลายเครือข่ายประกอบเข้าด้วย ย่อมมีผู้ใช้งานในเครือข่ายอินเทอร์เน็ทบางส่วนต้องการที่จะล่วงละเมิดเข้าไปยังเครือข่ายอื่นนอกเหนือจากเครือข่ายของตน เพื่อก่อกวน สร้างความเสียหาย หรือทำให้เครือข่ายหยุดทำงานด้วยวิธีการต่างๆ

ภัยคุกคามที่เกิดขึ้นในอินเทอร์เน็ทมีมากมายหลายรูปแบบ ซึ่งสามารถแยกออกได้ดังนี้

- **Confidentiality and Privacy Violation** การล่วงละเมิดข้อมูลอันเป็นความลับที่ไม่ได้มีการเปิดเผย เช่น ระบบฐานข้อมูลบัตรเครดิตของธนาคาร เป็นต้น
- **Denial of service** การโจมตีระบบเครือข่าย ทำให้เกิดสภาพการหยุดทำงานของระบบเครือข่ายอย่างสมบูรณ์ เนื่องจากบางส่วนหรือทั้งหมดของเครือข่ายไม่สามารถทำงานได้
- **Unauthorized Access** การเข้ามาใช้งานเน็ทเวิร์กโดยไม่ได้รับอนุญาต การสอบถามข้อมูลจากเน็ทเวิร์กโดยไม่ได้รับอนุญาตก่อน เช่นการสแกนระบบเครือข่าย การพยายามล็อกอินเข้าสู่ระบบที่มีการป้องกันด้วยพาสเวิร์ด เป็นต้น

จากที่ได้กล่าวมาข้างต้นเป็นภัยคุกคามบางส่วนที่มีเกิดขึ้นอยู่ในเครือข่ายอินเทอร์เน็ท ซึ่งภัยคุกคามเหล่านี้ก่อให้เกิดความเสียหายในหลายๆด้านทั้งทางด้านธุรกิจ ด้านความเป็นส่วนตัว และสร้างให้เกิดความไม่ปลอดภัยของข้อมูลเมื่อนนำเครือข่ายของเราต่อเข้ากับอินเทอร์เน็ท

ไฟร์วอลล์ถือเป็นเครื่องมือหนึ่งในหลายๆ เครื่องมือที่มีการกล่าวถึงกันอยางมากในปัจจุบันที่มีจุดประสงค์เพื่อเป็นตัวป้องกันภัยคุกคามที่เกิดขึ้นจากการเชื่อมต่อกับเครือข่ายอื่น ไฟร์วอลล์นี้มีหน้าที่ในการป้องกันระบบเครือข่ายจากการสื่อสารทั่วไปที่ไม่ได้รับอนุญาต ปัญหาพื้นฐานที่สุดในเครื่องของความปลอดภัยบนเครือข่ายคือการเข้าถึงระบบเครือข่าย ข้อมูลภายในองค์กร หรือเรียกว่า ลอจิคอลแอคเซส (logical access) หมายถึงการเข้ามาที่เครื่องคอมพิวเตอร์ภายในระบบเครือข่ายผ่านมาทางซอฟแวร์ หรือการเข้ามาถึงที่ไม่สามารถมองเห็นได้ ซึ่งมักเกิดขึ้นได้ง่ายกว่าการเข้าถึง

ทาง ฟิสิคอลแอคเซส (physical access) คือการเข้ามาถึงตัวเครื่องจริงๆ และการที่นำเครื่องคอมพิวเตอร์เข้ามาต่อกับระบบเครือข่ายทำให้เครื่องคอมพิวเตอร์สามารถถูกเข้าถึงได้จากทุกที่

การศึกษาในครั้งนี้ต้องการแสดงให้เห็นถึงวิธีการนำระบบไฟร์วอลล์สามารถเข้ามาช่วยในเรื่องความปลอดภัยได้อย่างไร โดยการศึกษาถึงสถาปัตยกรรมต่างๆ ของการออกแบบระบบไฟร์วอลล์ ตลอดจนถึงการวิเคราะห์ถึงความเป็นไปได้ในนำระบบไฟร์วอลล์เข้ามาใช้ในองค์กร โดยมองทางด้านเทคนิค ทางด้านการบริหาร และจัดการ และความคุ้มค่าในกางลงทุนและค่าใช้จ่ายอื่นๆ

1.2 วัตถุประสงค์

1. เพื่อศึกษารูปแบบการติดตั้ง และการทำงานของระบบไฟร์วอลล์ที่เหมาะสมกับบริษัท เมอร์ค จำกัด
2. เพื่อศึกษาความเป็นไปได้ในด้านต่างๆ ในการนำระบบไฟร์วอลล์เข้ามาประยุกต์ให้กับเครือข่ายของบริษัท เมอร์ค จำกัด เช่น ด้านเทคนิค ด้านต้นทุน และค่าใช้จ่าย เป็นต้น
3. นำแนวทางในการศึกษามาเพื่อเป็นประโยชน์ในการ พิจารณาการเลือกใช้ระบบไฟร์วอลล์ในองค์กรอื่นๆ

1.3 ขอบเขตการศึกษา

ขอบเขตในการศึกษาครั้งนี้ได้กำหนดระบบไฟร์วอลล์ที่นำมาใช้ในการศึกษาออกเป็น 3 รูปแบบ ดังนี้

- ระบบไฟร์วอลล์โดย Opensoure RedHat Linux with IPchain and IPtable
- ระบบไฟร์วอลล์โดยซอฟแวร์ลิขสิทธิ์ ในที่นี้ใช้ระบบไฟร์วอลล์ วัน และ ไมโครซอฟท์ไอเอสเอ เซิร์ฟเวอร์ 2000
- ระบบไฟร์วอลล์โดย ฮาร์ดแวร์ ในการศึกษาใช้ Cisco secure PIX firewall
- ระบบเน็ทเวิร์กภายในบริษัท เมอร์ค จำกัด

1.4 แผนและวิธีการดำเนินการศึกษา

การศึกษาในครั้งนี้ได้ทำการศึกษาจากแหล่งข้อมูลต่างๆ เช่น หนังสือ นิตยสาร และเว็บไซท์ที่เกี่ยวข้อง นอกจากนี้ได้ทำการสอบถามกับตัวแทนจำหน่ายของผลิตภัณฑ์ไฟร์วอลล์ต่างๆ ที่ได้นำมาประกอบการศึกษา

1.5 ประโยชน์ที่คาดว่าจะได้รับจากการศึกษา

- ทำให้ทราบถึงรูปแบบ ลักษณะการทำงาน และสถาปัตยกรรมของไฟร์วอลล์ที่มีใช้งานอยู่ในปัจจุบัน
- ทำให้ทราบความสามารถและขีดจำกัดของระบบไฟร์วอลล์แต่ละแบบที่ใช้ในการศึกษา
- เป็นแนวทางในการศึกษาความเป็นไปได้ และพิจารณาการนำระบบไฟร์วอลล์เข้ามาใช้งานเพื่อปกป้องระบบเครือข่ายภายในองค์กร
- สามารถทำการเลือกไฟร์วอลล์ที่มีความเหมาะสมต่อการใช้งานภายในเครือข่ายบริษัท เมอร์ค จำกัด

บทที่ 2
ทฤษฎีไฟร์วอลล์

2.1 ไฟร์วอลล์

ไฟร์วอลล์ คือ กำแพงที่เอาไว้ป้องกันไฟไม่ให้ลุกลามไปยังส่วนอื่นๆ ในทางด้านคอมพิวเตอร์นั้นก็จะมีความหมายคล้ายๆ กันก็คือ เป็นระบบที่เอาไว้ป้องกันอันตรายจากอินเตอร์เน็ตหรือเน็ตเวิร์กภายนอกนั่นเอง

ไฟร์วอลล์ เป็นคอมโพเน็นต์หรือกลุ่มของคอมโพเน็นต์ที่ทำหน้าที่ในการควบคุมการเข้าถึงระหว่างเน็ตเวิร์กภายนอกหรือเน็ตเวิร์กที่เราคิดว่าไม่ปลอดภัย กับเน็ตเวิร์กภายในหรือเน็ตเวิร์กที่เราต้องการจะป้องกัน โดยที่คอมโพเน็นต์นั้นอาจจะเป็น เราเตอร์ คอมพิวเตอร์ หรือเน็ตเวิร์กประกอบกันก็ได้ ขึ้นอยู่กับวิธีการหรือ สถาปัตยกรรมไฟร์วอลล์ ที่ใช้

รูปที่ 1 แสดง ไฟร์วอลล์กั้นระหว่างอินเตอร์เน็ตกับเน็ตเวิร์กภายใน

2.2 คุณสมบัติทั่วไปของไฟร์วอลล์

ไฟร์วอลล์เป็นเปครื่องมือรักษาความปลอดภัยที่ทำงานในเชิงป้องกัน (Protect) ซึ่งจะทำหน้าที่ควบคุมการเข้าถึงเน็ทเวิร์ก (Access Control) โดยอาศัยเป็นพื้นฐาน (Rule base) ซึ่งคุณสมบัติของไฟร์วอลล์มีรายละเอียดดังนี้

1. **Protect :** ไฟร์วอลล์เป็ฯเครื่องมือที่ใช้ทำงานในเชิงป้องกัน โดยแพ็คเก็ตที่สามารถผ่านเข้า-ออกเน็ตเวิร์กได้นั้น จะต้องเป็นแพ็คเก็ตที่ไฟร์วอลล์เห็นว่ามีความปลอดภัย แพ็คเก็นใดที่ไฟร์วอลล์เห็นว่าไม่ปลอดภัย หรืออาจจะนำมาซึ่งความไม่ปลอดภัยก็จะถูกดร็อป (drop) โดยการที่ไฟร์วอลล์จะตัดสินใจว่าแพ็คเก็ตใดปลอดภัยและแพ็คเก็ตใดไม่ปลอดภัยนั้นจะอยู่บนพื้นฐานของกำที่ผู้ดูแลไฟร์วอลล์ (Firewall administrator) เป็นผู้กำหนดไว้ล่วงหน้า ซึ่งเงื่อนไขของกฎเหล่านี้เองทำให้ไฟร์วอลล์สามารถป้องกันแพ็คเก็ตที่อาจจะส่งผลร้ายไม่ให้ผ่านเข้าไปถึงเน็ตเวิร์กได้
2. **Access Control :** "แอคเซส" หมายถึงการที่โฮสต์ใดโฮสต์หนึ่งสามารสื่อสารข้อมูลที่ต้องการไปยังโฮสต์ปลายทางได้สำเร็จ การแอคเซสในแต่ละระดับจะมีวีการแตกต่างกันออกไป ทำให้การควบคุมการแอคเซสสำหรับแต่ละระดับแตกต่างกันตามไปด้วย ไฟร์วอลล์จึงมีการทำงานหลายลักษณะตามวิธีที่ไฟร์วอลล์ใช้ควบคุมการแอคเซส
3. **Rule Base :** ไฟร์วอลล์จะควบคุมการแอคเซสโดยอาสัยการเปรียบเทียบคุณสมบัตของแพ็คเก็ตที่ผ่านไฟร์วอลล์กับกฎของการแอคเซสที่ได้กำหนดไว้ หากพบว่าไม่มีกฎที่ห้ามไว้ก็จะอนุญาตให้แพ็คเก็นนั้นผ่านไปได้ หากมีกฎที่หน้ามไว้แพ็คเก็ตนั้นก็จะถูกสกัดกั้นไว้ด้วยวิธีใดวิธีหนึ่ง

ดังนั้นการที่แพ็คเก็ตใดๆ สามารผ่านเข้า-ออกไฟร์วอลล์ได้หรือไม่นั้นจึงอยู่ที่กฎเป็นสำคัญสำหรับไฟร์วอลล์โดยตัวเองแล้วนั้นจะไม่มีทางทราบได้ว่าแพ็คเก็ตใดเป็นแพ็คเก็ตที่ปลอดภัยหรือแพ็คเก็ตใดเป็ฯแพ็คเก็ตที่ปลอดภัย (ยกเว้นแพ็คเก็ตที่เป็นอันตรายโดยตัวมันเองอยู่แล้ว เช่น แพ็คเก็ตแปลกประหลาด (Anomaious Packet) ที่ใช้สำหรับการโจมตีโดยเฉพาะ) ไฟร์วอลล์จะรู้จักเฉพาะแพ็คเก็ตที่ได้รับอนุญาต และแพ็คเก็ตที่ไม่ได้รับอนุญาต ตามกฎที่ระบุไว้เท่านั้น นั่นหมายความว่าแพ็คเก็ตที่ใช้เพื่อจุดประสงค์ร้ายหากมีลักษณะไม่เข้าข่ายหรือผิดกฎที่ตั้งไว้กอาจจะ

ได้รับอนุญาตให้ผ่านเข้ามาได้โดยที่ไฟร์วอลล์ไม่สามารทราบได้ ดังนั้นไม่จะเป็นเสมอไปว่า การบุกรุกทั้งหมดสามารป้องกันได้ด้วยไฟร์วอลล์

2.3 ความสามารถของระบบไฟร์วอลล์

2.3.1 ไฟร์วอลล์สามารถช่วยเพิ่มความปลอดภัยให้กับระบบ ดังนี้

- **Network Scanning**

การสแกนเน็ทเวิร์กเป้นสัญยาเริ่มต้นของภัยอื่นๆ ที่ติดตามมา ด้วยคุณสมบัติที่สามารถควบคุมการเข้าออกของแพ็คเก็ตได้ ทำให้ผู้ใช้มีอโอกาสที่จะสามารจำกัดปลายทางของแพ็คเก็ตที่จะผ่านเข้ามาเฉพาะโฮสต์ที่อนุญาตให้ติดต่าได้จากภายนอกได้เท่านั้น แพ็กเก็ตที่ส่งเข้ามาเพื่อสำรวจเน็ตเวิร์กโดยการส่งไปยังโฮสต์อื่นๆ ในเน็ทเวิร์กจะไม่สามารถเล็ดลอดไปถึงเป้านหมายและนำข้อมูลออกไปได้ จากที่แฮคเกอร์จะเจาะเข้าไปยังเน็ทเวิร์กใดนั้น มักจะเริ่มโดยเจาะเข้าไปยังโฮสต์ที่มีการป้องกันตัวเองน้อยที่สุดก่อน ซึ่งเมื่อแฮคเกอร์สามารสแกนเน็ตเวิร์กได้ก็จะทำให้สามารค้นพบได้ว่าภายในเน็ทเวิร์กนั้นมีโฮสต์อะไรบ้าง และโฮสต์แต่ละตัวมีระดับการรักษาความปลอดภัยมากน้อยเท่าไร

- **Host Scanning**

การสแกนโฮสต์เป็นองค์ประกับเริ่มต้นที่สำคัญชองการเตรียมการของการเจาะระบบ เพราะถึงแม้จะมีไฟร์วอลล์ติดตั้งอยู่ก็ตาม มิได้หมายความว่าเน็ทเวิร์กที่อยู่หลังไฟร์วอลลจะถูกตัดขาดจากโลกภายนอก จะต้องมีโฮสต์อย่างน้อยหนึ่งตัวที่สามารถติดต่อได้กับโลกภายนอกได้ และโฮสต์นั้นก็มีโอกาสที่จะถูกสแกนได้ การที่แฮคเกอร์สามารถสแกนโฮสต์ได้นั้น จะทำให้มีโอกาสค้นหาข้อบกพร่องต่างๆ ของโฮสต์และนำไปเปนข้อมูลเพื่อการเจาะระบบในลำดับต่อไป

- **Inbound Access**

ไฟร์วอลล์ได้เข้ามาเสริมความปลอดภัย โดยทำหน้าที่ควบคุมและกลั่นกรองข้อมูลทุกชนิดที่เข้ามาให้เหลือแต่เฉพาะข้อมูลที่ต้องการเท่านั้น โดยไฟร์วอลล์จะทำหน้าที่แบ่งแยกเน็ทเวิร์กภายในและภายนอกออกจากกัน ทำให้การบริการต่างๆ บนโฮสต์ยังคงสามารถให้บริการได้เช่นเดิม

แต่สามารถจำกัดการขอใช้บริการจากบุคคลภายนอกหรือโฮสต์อื่นๆ ที่ไม่ได้รับอนุญาตได้ การที่ไฟร์วอลล์สามารควบคุมการเข้าถึงจากภายนอกหรืออินบาวด์แอคเซส (Inbound Access) ได้ทำให้ความปลอดภัยของโฮสต์ได้ยกระดับขึ้นอีกมาก อย่างน้อยที่สุดก็มีช่องทางในการเข้ามาของภัยคุกคามต่างๆลดน้อยลง

การควบคุมการเข้ามาของข้อมูลเป็นหน้าที่หลักที่สำคัญที่สุดของระบบไฟร์วอลล์ทุกชนิด เพราะภัยคุกคามทั้งหลายจะสามาทำอันตรายให้แก่เน็ทเวิร์กหรือโฮสต์ได้นั้น จะต้องมีช่องทางในการเข้ามาเสมอ และหน้าที่นี้เองทำให้ไฟร์วอลล์เปรียบได้ดังกำแพงป้องกันภัยอันตรายไม่ให้เข้าถึงเน็ทเวิร์กที่อยู่ภายได้

- **Outbound Access**

การป้องกันการเข้ามาของข้อมูลจากภายนอกแกล้ว ไฟร์วอลล์ยังสามารป้องกันข้อมูลภายในไม่ให้ออกไปข้างนอกได้ด้วย ภัยคุกคามต่อระบบคอมพิวเตอร์มิได้มีเพียงแค่การเจาะเข้ามาจากแฮคเกอร์ภายนอกเพียงอย่างเดียวเท่านั้น ภัยคุกคามที่เกิดจากภายในองค์กรก็มีอยู่ไม่น้อยและส่งผลเกสียหายได้ไม่น้อยกว่าการถูกเจาะระบบเข้ามาจากภายนอกเสียอีก การที่เน็ทเวิร์กเชื่อมต่อกับอินเทอร์เน็ทและเปิดให้ใช้งานได้ย่างไม่มีการควบคุมนั้อาจจะก่อให้เกิดปัญหาได้

- **Denial Of Service**

การโจมตีเพื่อก่อกวนไม่ให้โฮสต์สามารถให้บริการได้โดยใช้เทคนิคในระดับของเน็ตเวิร์กด้วยวิธีการต่างๆ ไม่ว่าจะเป็นการส่งอะนอมาลัสแพ็คเก็ต (Anomalous Packet : แพ็คเก็ตที่มีลักษณะผิดกฎของโปรโตคอลเพื่อทำให้โฮสต์ปลายทางทำงานผิดเพี้ยน) การทำให้เน็ทเวิร์กท่วมไปด้วยข้อมูล (Network Flooding) การส่งแพ็คเก็ตจำนวนากไปยังโฮสต์เพื่อขอใช้บริการ (SYN flooding) โดยส่วใหญ่จะสามารป้องกันไดด้วยไฟร์วอลล์ หรือย่างน้อยก็จะสามารถบรรเทาผลกระทบจากการถูกโจมตีจากหนักเป็นเบาได้

- **Back orifice, Trojan Horse and Backdoor**

ภัยประเภทนี้หมายถึงเกิดจากการที่โฮสต์ภายในเน็ทเวิร์กรันโปรแกรมที่เข้าใจว่าเป็นโปรแกรมที่ทำงานตามปกติ แต่แท้ที่จริงแล้วโปรแกรมเหล่านั้นได้ซ่อนการทำงานอื่นไว้เบื้องหลัง โดยทั่วไปโปรแกรมประเภทนี้มักจะทำงานเสมือนการเปิดประตูภายในโฮสต์ที่รันโปรแกรมนั้น ทำให้แฮคเกอร์สามารใช้ประตูหลังที่เปิดทิ้งไว้เข้ามาทำอันตรายในเน็ทเวิร์กได้

ไฟร์วอลล์สามารป้องกันภัยประเภทนี้ได้ แต่มิได้หมายความว่าไฟร์วอลล์จะสามารตรวจจับโปรแกรมประเภทนี้ได้ หรือไฟร์วอลล์สามารถเตือนผู้ใช้ไม่ให้รันโปรแกรมได้ แต่ไฟร์วอลล์จะสามารป้องกันไม่ให้โปรแกรมประเภทนี้สามารถทำงานได้อย่างสมบูรณ์ โดยที่ถึงแม้ว่าผู้ใช้จะมีโปรแกรมประเภทนี้ทำงานอยู่ก็ตาม

เนื่องจากโปรแกรมประเภทนี้มักต้องอาศัยการสื่อสารข้อมูลที่สมบูรณ์ระหว่างโปรแกรมในโฮสต์กับแฮคเกอร์ ดังนั้นจึงจำเป็นต้องเปิดช่องทางการสื่อสารพิเศษไว้เพื่อให้แฮคเกอร์สามารถเข้ามาได้ ซึ่งโดยทั่วไปการกำหนดกฎของไฟร์วอลล์แล้วพอร์ตหมายเลขที่โปรแกรมประเภทนี้ใช้งนจะเป็นพอร์ตอันตรายที่เป็นพอร์ตต้องห้ามเสมอ ทำให้แพ็คเก็ตใดๆ ที่ใช้พรอ์ตหมายเลขเหล่านี้จะถูกดร็อปโดยไฟร์วอลล์ก่อนที่จะไปถึงที่หมาย

2.3.2 ไฟร์วอลล์ไม่สามารถป้องกันได้ในกรณี มีดังนี้

- **Hacker**

แฮคเกอร์ในที่นี้มีทั้งที่มาจากภายนอกและภายใน ซึ่งในส่วนของภายนอกนั้นสามารถที่จะป้องกันได้ แต่ในส่วนของแฮคเกอร์ที่มาจากภายใน ไม่สามารถทำได้เนื่องจาก ส่วนใหญ่ไฟร์วอลล์จะอนุญาตให้กับเน็ทเวิร์กภายใน สามารถกระทำการใดๆ ก็ได้ทั้งหมด ทำให้ไม่สามารถป้องกันการแฮคจากภายในได้

- **Allowed services การบริการที่ได้รับอนุญาต**

ไฟร์วอลล์จะควบคุมการสื่อสารข้อมูลโดยใช้กฎเป็นสำคัญ ไม่มีกฎที่ผิดและกฎที่ถูกแน่นอนตายตัว กฎที่ผิดสำหรับเน็ตเวิร์กหนึ่งอาจจะเป็นกฎที่ถูกสำหรับอีกเน็ทเวิร์กหนึ่งได้ ทางกลับกันกฎที่ถูกของอีกเน็ทเวิร์กหนึ่งก็อาจเป็นที่สิ่งที่ต้องห้ามสำหรับอีกเน็ทเวิร์กหนึ่งได้ เพราะปัจจัยสำคัญในการกำหนดคือนโยบายความปลอดภัยและลักษณะการบริการที่มีอยู่ภายในเน็ทเวิร์ก

นั้น การพิจารณากำที่มีอยู่บนไฟร์วอลล์จึงมีเพียงความเหมาะสมของกฎเท่านั้นว่าสอดคล้องกับนโยบายหรือไม่ รัดกุมเพียงพอหรือไม่ และมีประโยชน์ในแง่ของการป้องกันหรือไม่

สำหรับมุมมองในแง่ของการส่อสารข้อมูล การบริการใดที่ได้รับอนุญาตจากไฟร์วอลล์ก็จะทำตัวเสมือนว่าไม่มีการป้องกัน คือไม่รู้สึกว่ามีๆไฟร์วอลล์ควบคุมแต่อย่างใด เช่น หากไฟร์วอลล์อนุญาตให้มีการเรียกใช้บริการของเว็บเซิร์ฟเวอร์ที่อยู่ภายในเน็ทเวิร์กได้ (พอร์ต 80) นั่นหมายความว่า การสื่อสารข้อมูลใดๆ ที่กระทำอยู่ภายใต้บริการของเว็บเซิร์ฟเวอร์ก็จะได้รับอนุญาตอย่างทั่วถึงกัน หากมีภัยคุกคามใดที่แผงมากับการเรียกใช้บริการเว็บเซิร์ฟเวอร์แล้ว ไฟร์วอลล์ก็ไม่สามารถตรวจสอบและป้องกันได้

- **Application Vulnerability**

Vulnerability คือข้อบกพร่องที่เปรียบเสมือนช่องโหว่ของระบบต่างๆ หากในระดับแอพพลิเคชั่น หมายถึงข้อบกพร่องที่มีอยู่ภายในแอพพลิเคชั่นนั้นที่เป็นช่องทางให้แฮคเกอร์สามารถผ่านเข้ามาในได้โดยง่าย ข้อบกพร่องเหล่านี้จะติดตัวอยู่กับแอพพลิเคชั่น เมื่อนำแอพพลิเคชั่นที่มีปัญหาไปบรการ ก็ทำให้ขณะที่แอพพลิเคชั่นทำงานอยู่นั่นก็จะเปรียบเสมอนเปิดช่องทางให้แฮคเกอร์ผ่านเข้ามาภายในระบบได้ด้วยข้อบกพร่องของแอพพลิเคชั่นนั่นเอง

ไฟร์วอลล์สามารถควบคุมได้เพียงให้ทราฟฟิคที่ผ่านเข้าออกนั้นใช้เฉพาะพอร์ตที่ต้องการเท่านั้น แต่เมื่อทราฟฟิคนั้นได้ใช้บริการตามพรอ์ตที่ได้รับอนุญานแล้ว ถือว่าหมดหน้าที่ของไฟร์วอลล์ หากมัญหาด้านความปลอดภัยชองแอพพลิเคชั่นก็ต้องเป็นหน้าที่ที่จะต้องแก้ไขที่แอพพลิเคชั่นนั้นเอง

- **OS vulnerability**

ระบบปฏิบัติการเป็นซอฟแวร์ชนิดหนึ่งเช่นเดียวกับแอพพลิเคชั่น เพียงแต่ทำหน้าที่ระดับชั้นหรือเลเยอร์ (Layer) ซึ่งก็ย่อมจะมีช้อบกพร่องหรือช่องโหว่เช่นเดียวกับที่ซอฟแวร์อื่น ดังนั้นหากระบบปฏิบัติการมีปัญหาก็อยู่นอกเหนือความสามารถของไฟร์วอลล์จะแก้ไขได้ แต่หากมีการกำหนดกฎที่ดีแล้วไฟร์วอลล์จะสามารถช่วยบรรเทาและลดความเสี่ยงจากการเจาะเข้ามาโดยช่องทางนี้ได้ ซึ่งแตกต่างจากข้อบกพร่องของแอพพลิเคชั่น เนื่องจากว่าแอพพลิเคชั่นนั้นจำเป็นต้องเปิดพอร์ตให้บริการกับผู้ใช้อยู่แล้ว และแฮคเกอร์ก็จะใช้ช่องทางเดียวกันในการเจาะระบบเข้ามา

สำหรับระบบปฏิบัติการแล้วอาจจะไม่มีความจำเป็นต้องเปิดพอร์ตให้บริการกับผู้แต่อย่าใด ดังนั้น ไฟร์วอลล์จึงสามารถป้องกันไม่ให้แฮคเกอร์เข้าถึงพอร์ตของระบบปฏิบัติการได้

แต่สำหรับในบางกรณีที่การทำงานนั้นมีส่วนคาบเกี่ยวกันระหว่างระบบปฏิบัติการและแอพพลิเคชั่น ไฟร์วอลล์ก็ไม่สามารถช่วยป้องกันได้อยู่ดี ดังเช่นการที่ทำเว็บเซิร์ฟเวอร์ซึ่งต้องมีความจำเป็นในการเปิดพอร์ตทีซีพีหมายเลข 80 ไว้เพื่อให้บริการ และโปรแกรมที่ทำงานให้บริการเว็บอยู่นั้น จะทำงานอยู่บนระบบปฏิบัติการซึ่งเป็นตัวที่คอยรับและจัดการกับแพ็คเก็ตก่อนที่จะส่งต่อให้กับแอพพลิเคชั่นทำการโปรเซสต่อไป แต่ทั้งนี้ถ้าแฮคเกอร์ทำการโจมตี หรือบุกรุกเข้าเครือข่ายโดยการส่งแพ็คเก็ตที่แปลกปลอมเข้ามา อาจทำให้ระบบปฏิบัติการนั้นๆ หยุดทำงานได้ เป็นต้น

- **Virus**

ไฟร์วอลล์ไม่สามารถป้องกันไวรัสได้เนื่องจากไฟร์วอลล์นั้นทำงานอยู่ในระดับของของเน็ทเวิร์กเลเยอร์ ที่คอยควบคุมทราฟฟิคเป็นหลัก ซึ่งจะทำงานอยู่ในเลเยอร์ที่ต่ำกว่าการทงานของไวรัส ไฟร์วอลล์จะไม่รู้จักว่าอะไรคือ ไวรัส อะไรคือจดหมาย อะไรคือรูปภาพ ไฟร์วอลล์จะรู้จักเฉพาะ TCP, UPD, ICMP และ Port เป็นต้น ดังนี้นการคาดหลังให้ไฟร์วอลล์ป้องกันหรือกำจัดไวรัสได้นั้นไม่สามารถเป็นไปได้ การงานของไวรัสจะอยู่ในระดับแอพพลิเคชั่น อาศัยการเอ็กซิคิวต์คำสั่งของผู้ใช้และระบบปฏิบัติการเป็นหลัก สิ่งเดียวที่ไวรัสเกี่ยวข้องกับอินเทอร์เน็ทและไฟร์วอลล์คือ อาศัยเป็นทางผ่านเท่านั้น หากไวรัสแพร่กระจายโดยอีเมล์ (ซึ่งส่วนใหญ่ในระยะหลังจะเป็นการแพร่กระจายแบบนี้) โดยที่มีเมล์เซิร์ฟเวอร์อยู่ และกำหนดให้ไฟร์วอลล์อนุญาตมีการรับทราฟฟิคเพื่อการรับส่งจดหมายอิเล็กโทรนิกส์ได้แล้ว ไวรัสก็สามารถผ่านเข้ามาได้เช่นเดียวกับจดหมายอื่นๆ เช่นกัน

- **การดักอ่านข้อมูลโดย Sniffer**

Sniffer เป็นเครื่องมือชนิดหนึ่งที่เมื่อนำไปต่อในเน็ตเวิร์กร่วมกับโฮสต์อื่นๆ แล้ว ทำให้สามารถดักอ่านข้อมูลของโฮสต์อื่นๆ ที่ใช้งานอยู่บนอุปกรณ์เน็ทเวิร์กตัวเดียวกันได้ ไฟร์วอลล์ไม่มีหน้าที่และความสามารถในการป้องกันการดักอ่านข้อมูลได้เลย ดังนั้นไม่ควรคาดหลังว่าเมื่อมีไฟร์วอลล์แล้วจะสามารถป้องกันการแอบอ่านอีเมล์ของผู้อื่นหรือป้องกันข้อมูลรั่วไหลเนื่องจากการมี sniffer ได้

- **Spammed Mail**

สำหนับสแปมเมล์หรืออีเมล์ขยะที่ได้รับมาโดยที่ผู้ใช้ไม่ต้องการ อาจจะเป็นเมล์โฆษณาชวนเชื่อ จดมายลูกโซ่ แบะไม่สามารถติดตามหาผู้ส่งจริงๆ ได้ อาจมีอันตรายไม่มากแต่จะส่งผลในการสร้างความรำคาญให้แก่ผู้รับ ทำให้ประสิทธิภาพในการทำงานของระบบเมล์ลดต่ำลง และสิ้นเปลืองทรพยากรไปเพื่อจัดเก็บเมล์ขยะพวกนี้ โดยทั่วไปแล้วอาจจะได้รับผลกระทบได้ใน 2 ฐานะ คือ

1. เป็นผู้รับเมล์ ผู้ส่งอาจจะได้ชื่อมาจากที่ใดไม่ทราบได้ แต่ได้ส่งมายังผู้รับเมล์โดยตรง โดยที่ผู้รับไม่เคยติดต่อและไม่ต้องการได้รับเมล์นั้นแม้แต่น้อย ส่วนใหญ่ก็ต้องคายคามลบเมล์เหล่านั้นทิ้งไป
2. ถูกใช้เป็นตัวกลางสำหรับส่งต่อเมล์ ลักษณะนี้จะเป็นส่งผลกระทบเฉพาะกับเมล์เซิร์ฟเวอร์เท่านั้น เนื่องจากเมล์เซิร์ฟเวอร์อาจจะถูกติดตั้งกำหนดค่าไว้ไม่เหมาะสม ทำให้สามารถถูกใช้ไปเพื่อเป็นตัวกลางในการกระจายเมล์ขยะไปหาผู้อื่นได้

ทั้ง 2 กรณีจะส่งผลต่อผู้ใช้ต่างกัน แต่ก็ไม่เป็นผลดีทั้งคู่ ถึงแม้ว่าภัยที่มาจากการส่งเมล์บนอินเทอร์เน็ทโดยที่ทราฟฟิคของเมล์เหล่านี้จะเดินทางผ่นไฟร์วอลล์ก็ตา แต่ไฟร์วอลล์ก็ไม่สามารถเข้าใจเนื้อหาในเมล์ได้ว่าเป็นอย่างไร สำหรับเมล์ทุกฉบับที่ผ่านเข้าออกนั้นในมุมมองของไฟร์วอลล์แล้วมีค่าเท่าเทียมกันและมัคุณสมบัติเหมือนกัน ดังนั้นจึงทำให้ไม่สามารถทำการตรวจจับสแปมเมล์และทำการดร็อปทราฟฟิกเหล่านั้นออกไปได้ การแก้ไขปัญหาของสแปมเมล์จะต้องแก้ไขในระดับของเมล์เซิร์ฟเวอร์

- **ความผิดพลาดอันเกิดจากบุคคลากร**

ความผิดพลาดของผู้ที่เป็น System Administrator ซึ่งเป็นบุคคลที่ทำหน้าที่ดูแล และออกกฎระเบียบในการใช้งาน ซึ่งความผิดพลาดที่เกิดจากความหละหลวม ความไม่รอบคอบ หรือขาดการวางแผนที่ดีทำให้เป็นช่องทางก่อให้เกิดความไม่ปลอดภัยขึ้นในระบบได้เช่น การกำหนดสิทธิ์ในการใช้งานผิดพลาดโดยอนุญาตให้ผู้ใช้สามารถ Upload ไฟล์ขึ้นไปยังเซิร์ฟเวอร์ได้โดยไม่ต้องทำการล็อกอิน การไม่มีการป้องกันไฟล์ที่มีความสำคัญ เปิดโอกาสให้ผู้ใช้สามารถนำไฟล์

password มาทำการ crack หรือแกะดูข้อมูลเพื่อหารหัสผ่านได้ การติดตั้งโปรแกรมประเภท remote control แต่ไม่มีการควบคุมการใช้งานอย่างเพียงพอ เป็นต้น

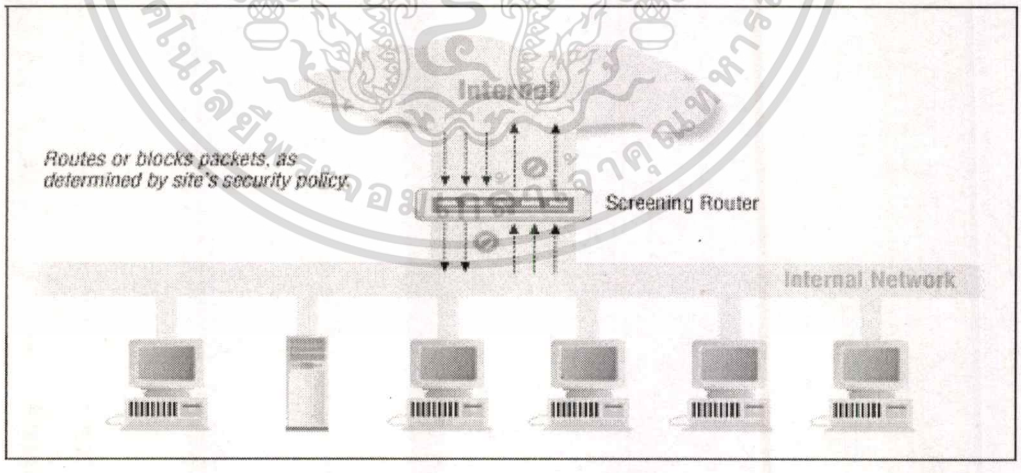
ดังนั้นการพิจารณาความปลอดภัยของระบบองค์รวมจึงจะต้องตระหนักถึงความเสี่ยงในเรื่องการปฏิบัติงานของบุคคลให้มาก และควรมีมาตรการและแนวทางการปฏิบัติ เพื่อช่วยลดปัญหานี้ให้มีผลกระทบน้อยลงได้

2.4 ชนิดและลักษณะของการใช้งานไฟร์วอลล์

ชนิดของไฟร์วอลล์แบ่งตามเทคโนโลยีที่ใช้ในการตรวจสอบและควบคุม แบ่งได้เป็น

2.4.1 Packet Filtering

Packet Filter คือเราเตอร์ที่ทำการหาเส้นทางและส่งต่ออย่างมีเงื่อนไข โดยจะพิจารณาจากข้อมูลส่วนที่อยู่ในเฮดเดอร์) header) ของแพ็กเก็ตที่ผ่านเข้ามา เทียบกับกฎ) rules) ที่กำหนดไว้และตัดสินว่าควรจะทิ้ง) drop) แพ็กเก็ตนั้นไปหรือว่าจะยอม) accept) ให้แพ็กเก็ตนั้นผ่านไปได้



รูปที่ 2 แสดง การใช้เราว์เตอร์ปเป็นตัวทำ packet filtering firewall

ในการพิจารณาเฮดเดอร์ Packet Filter จะตรวจสอบในระดับของอินเทอร์เน็ตเลเยอร์ และทรานสปอร์ตเลเยอร์ ในอินเทอร์เน็ตโมเดล ในอินเทอร์เน็ตเลเยอร์ จะมีแอตทริบิวต์ที่สำคัญต่อ Packet Filtering ดังนี้

- ไอพีต้นทาง
- ไอพีปลายทาง
- ชนิดของโปรโตคอล)TCP, UDP และ ICMP) และในระดับของทรานสปอร์ตเลเยอร์ มีแอตทริบิวต์ที่สำคัญคือ
- พอร์ตต้นทาง
- พอร์ตปลายทาง
- แฟล็ก)Flag ซึ่งจะมีเฉพาะในเฮดเดอร์ของแพ็กเก็ต TCP)
- ชนิดของ ICMP message (ในแพ็กเก็ต ICMP)

พอร์ตของทรานสปอร์ตเลเยอร์ คือทั้ง TCP และ UDP นั้นจะเป็นสิ่งที่บอกถึงแอพพลิเคชันที่แพ็กเก็ตนั้นต้องการติดต่อด้วยเช่น พอร์ต 80 หมายถึง HTTP, พอร์ต 21 หมายถึง FTP เป็นต้น ดังนั้นเมื่อ Packet Filter พิจารณาเฮดเดอร์ จึงทำให้สามารถควบคุมแพ็กเก็ตที่มาจากที่ต่างๆ และมีลักษณะต่างๆ (ดูได้จากแฟล็กของแพ็กเก็ต หรือ ชนิดของ ICMP ในแพ็กเก็ต ICMP) ได้ เช่น ห้ามแพ็กเก็ตทุกชนิดจาก crack.cracker.net เข้ามายังเน็ตเวิร์ก 203.155.57.0/24 , ห้ามแพ็กเก็ตที่มีไอพีต้นทางอยู่ในเน็ตเวิร์ก 203.155.56.0/24 ผ่านเราเตอร์เข้ามา (ในกรณีนี้เพื่อเป็นการป้องกัน ip spoofing) เป็นต้น

ข้อดีของ Packet Filtering แบบ Screening Router

- ราคาถูกเพราะเป็นคุณสมบัติที่มีของเราเตอร์อยู่แล้ว อาศัยเพียงการกำหนดแอคเซสรูลที่เหมาะสมเท่านั้น
- ถ้าเน็ทเวิร์กที่ใช้มีขนาดไม่ใหญ่มาก สามารถนำมาใช้แทนไฟร์วอลล์ได้
- การใช้งานแอคเซสรูลในเราเตอร์ ควบคู่กับการใช้งานไฟร์วอลล์ ถ้ามีการคอนฟิกที่สอดคล้องกันทำให้ได้โซลูชั่นในการป้องกันที่ดีขึ้นเป็นอย่างมาก และสามารถช่วยลดภาระของไฟร์วอลล์ได้ด้วย

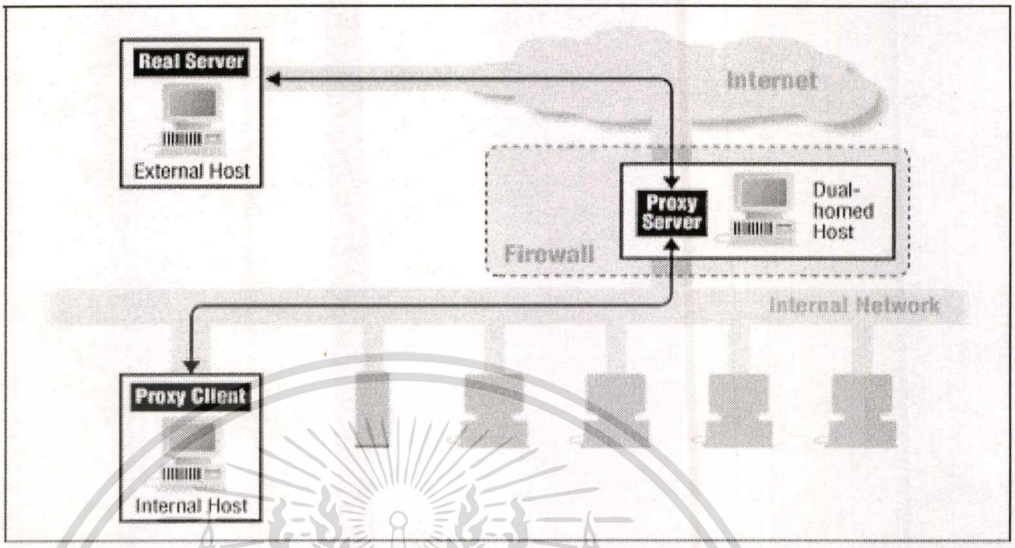
- การป้องกันบางประเภทไม่สามารถป้องกันโดยไฟร์วอลล์ จะต้องทำโดยการกำหนดที่เราเตอร์แทน

ข้อเสียของ Packet Filtering แบบ Screening Router

- การกำหนดแอคเซสรูลทำได้ยาก เนื่องจากต้องทำาการคอนฟิกแบบ Command line ซึ่งเสี่ยงต่อการป้อนคำสั่งที่ผิด ทำให้เกิดความผิดพลาดได้
- คำสั่งที่ใช้ในการสร้างแอคเซสรูล ของเราเตอร์แต่ละยี่ห้อไม่เหมือนกัน และไม่มีมาตรฐานที่ตายตัว
- ไม่สามารถกำหนดกฎที่ซับซ้อนได้ เนื่องจากขีดจำกัดของเราเอตร์ที่ทำงานโดยพิจารณาครั้งละแพ็คเก็ตเท่านั้น และมีความสามารถ จำกัดเช่น ไม่สามารถบันทึก log ของแพ็คเก็ตที่ต้องสงสัยไว้ตรวจสอบภายหลังได้ เป็นต้น
- เราเตอร์มีกำลังในการประมวลผลจำกัด หากเน็ทเวิร์กมีขนาดใหญ่ และมีการสื่อสารข้อมูลหนาแน่น เราเตอร์จะทำงานหนักอยู่แล้ว เมื่องต้องมาทำการประมวลผลแอคเซสรูลด้วยอาจจะทำให้ประสิทธิภาพในการเราต์ แพ็คเก็ตลดต่ำลงมาก และการสื่อสารข้อมูลจะติดขัดที่เราเตอร์ได้

2.4.2 Proxy Service

Proxy หรือ Application Gateway เป็นแอพพลิเคชันโปรแกรมที่ทำงานอยู่บนไฟร์วอลล์ที่ตั้งอยู่ระหว่างเน็ตเวิร์ก 2 เน็ตเวิร์ก ทำหน้าที่เพิ่มความปลอดภัยของระบบเน็ตเวิร์กโดยการควบคุมการเชื่อมต่อระหว่างเน็ตเวิร์กภายในและภายนอก Proxy จะช่วยเพิ่มความปลอดภัยได้มากเนื่องจากมีการตรวจสอบข้อมูลถึงในระดับของแอพพลิเคชันเลเยอร์ (Application Layer)



รูปที่ 3 ใช้ Dual-homed Host เป็น Proxy Server

เมื่อไคลเอนต์ต้องการใช้เซอร์วิสภายนอก ไคลเอนต์จะทำการติดต่อไปยัง Proxy ก่อน ไคลเอนต์จะเจรจา) negotiate) กับ Proxy เพื่อให้ Proxy ติดต่อไปยังเครื่องปลายทางให้ เมื่อ Proxy ติดต่อไปยังเครื่องปลายทางให้แล้วจะมีการเชื่อมต่อ)connection) 2 การเชื่อมต่อ คือ ไคลเอนต์กับ Proxy และ Proxy กับเครื่องปลายทาง โดยที่ Proxy จะทำหน้าที่รับข้อมูลและส่งต่อข้อมูลให้ใน 2 ทิศทาง ทั้งนี้ Proxy จะทำหน้าที่ในการตัดสินใจว่าจะให้มีการเชื่อมต่อกันหรือไม่ จะส่งต่อแพ็กเก็ตให้หรือไม่

ข้อดีของการใช้งานพร็อกซี่

- สามารถควบคุมการติดต่อสื่อสารระหว่างอินเทอร์เน็ทกับเน็ทเวิร์กภายในให้อยู่ในระดับแอพพลิเคชั่นเท่านั้น ตัดขาดการติดต่อโดยตรงในระดับเน็ทเวิร์กเลเยอร์ระหว่างกอินเทอร์เน็ทกับเน็ทเวิร์คภายในจากันอย่างเด็ดขาด ทำให้ลดความเสี่ยงต่อการถูกคุกคามจากการสแกน การเจาะระบบ การก่อกวนโดยใช้เทคนิคในระดับเน็ทเวิร์กเลเยอร์ที่จะเข้ามายังเน็ตเวิร์กภายในได้เด็ดขาด
- สามารถเพิ่มเติมหน้าที่การทำงานอย่างอื่นเข้าไปในพร็อกซี่ได้ เช่น สำหรับเว็บพร็อกซี่นอกจากจะเป็นตัวกลางในการติดต่อแล้ว ยังสามารถควบคุมไม่ให้เว็บบราวเซอร์ติดต่อกับเว็บไซท์ที่ไม่ต้องการได้อีกด้วย โดยการกำหนดรายชื่อเว็บไซท์เหล่านั้นไว้ในพร็อกซี่

- สามารถทำการแคชข้อมูลเก็บไว้ในตัวพร็อกซี่ สำหรับข้อมูลใดที่มีการเกรียกใช้ซ้ำๆ ก็ไม่จำเป็นต้องไปอ่านจากเซิร์ฟเวอร์ใหม่ทุกครั้ง แต่ส่วนนี้จะใช้งานกับข้อมูลที่เป็นสแตติคเท่านั้น ข้อมูลที่มีการเปลี่ยนแปลงตลอดเวลาเป็นไดนามิคอาจจะไม่สามรถแคชไว้ได้
- ทำให้ผู้ใช้มีแบนด์วิดธ์ร่วมกันอย่างมีประสิทธิภาพ โดยเฉพาะเพมื่อให้ร่วมกับการแคชที่มีอยู่ในพร็อกซี่ ทำให้ช่วยประหยัดการใช้งานแบนด์วิดธ์ไปได้มาก
- สามารถเพิ่มเติมส่วนการตรวจสอบผู้ใช้ (Authenticate) เข้าไปเป็นที่หนึ่งของพร็อกซี่ได้ โดยการอนุญาตให้สามารถใช้งานพร็อกซี่นั้นจะขึ้นอยู่กับสิทธิ์การใช้งานที่ผู้ใช้มีอยู่ ทำให้สามารถควบคุมการใช้งานได้ใกล้ชิดมากขึ้นกว่าการควบคุมโดยพิจารณาจาก IP address
- สามารถทำการกลั่นกรองเนื้อหาของข้อมูลได้ (Content Filtering) ทำให้สามารถนำมาเป็นเงื่อนไขในการอนุญาตให้ข้อมูลเหล่านั้นผ่านเข้าออกได้ โดยพิจารณาจากชื่อเว็ปไซท์หรือสิ่งที่ประกอบอยู่ในเว็บเพจก็ได้

ข้อเสียของการใช้งานพร็อกซี่

- ขึ้นอยู่กับแอพพลิเคชั่น หากแอพพลิเคชั่นไม่รองรับการสื่อสารโดยผ่นพรอก็กซี่ก็ไม่สามารถใช้งานได้
- ไม่สามารใช้งานกับแอพพลิเคชั่นที่ต้องการการสื่อสารโดยตรงแบบ end-to-end ซึ่งแพ็คเก็ตจะต้องมาจากโฮสต์ปลายทางทั้งคู่เท่านั้น ผ่านตัวกลางไม่ได้
- เสี่ยงต่อการละเมิดความเป็นส่วนบุคคล เนื่องจากข้อมูลทั้งหมดที่สื่อสารจะต้องผ่านพร็อกซี่ก่อนเสมอ และพร็อกซี่ก็มีความสามารถที่จะเก็บข้อมูลเหล่านั้นไว้ตรวจสอบได้ หากมีผู้นำข้อมูลเหล่านั้นไปวิเคราะห์จะสามารถทราบการใช้งานหรืออาจจะทราบข้อมูลทั้งหมดของผู้ใช้
- เนื่องจากลักษณะของแต่ละแอพพลิเคชั่นนั้นจะแตกต่างกันออก ดังนั้นพร็อกซี่ของแต่ละแอพพลิเคชั่นจึงทำหน้าที่เฉพาะแอพพลิเคชั่นนั้นๆ ไม่สามารถใช้ร่วมกันได้ หากโฮสต์ที่อยู่หลังพร็อกซี่มีการใช้งานหลายแอพพลิเคชั่นก็จะต้องมีพร็อกซี่จำนวนมากเปิดให้บริการตามจำนวนแอพพลิเคชั่นนั้น
- ความสามารถในการประมวลผลของโฮสต์ที่ทำหน้าที่พร็อกซี่อาจจะเป็นคอขวดของระบบได้เพราะการสื่อสารทั้งหมดของไคลเอนท์และเซิร์ฟเวอร์ ปัญหาลักษณะนี้จะสามารถพบได้ชัดเมื่อมีไคลเอนต์จำนวนมาก

- เนื่องจากพร็อกซี่เป็นแอพพลิเคชั่นชนิดหนึ่ง การติดต่อกับในเน็ทเวิร์กจะอาศัยระบบปฏิบัติการเป็นหลัก จึงมีความสามารถในการป้องกันตัวเองต่ำกว่าไฟร์วอลล์ทั่วไป ตัวพร็อกว่เองจึงมีความเสี่ยงต่อการถูกโจมตีได้มากและเปราะบางต่อการ DoS ด้วยเทคนิคในระดับเน็ทเวิร์ก ซึ่งอาจส่งผลให้พร็อกซี่อาจจะหยุดทำงานลงได้โดยง่าย โดยเฉพาะเมื่อพร็อกซี่นั้นเป็นโฮสต์ที่ต่อโดยตรงกับอินเทอร์เน็ท จึงเป็นเสมือนด่านหน้าของเน็ทเวิร์กที่จต้องถูกสแกน ถูกเจาะอย่างแน่นอน แต่ระดับความต้านทานของพร็อกซี่นั้นต่ำกว่าไฟร์วอลล์มาก จึงมีแนวโน้มว่าหากใช้พรอกซี่โดยปราศจากไฟร์วอลล์ร่วมด้วยโอกาสที่พร็อกซี่จะโดนเจาะได้นั้นมีสูงมาก

2.4.3 Stateful Inspection หรือ Circuit-Level Firewall

Packet Filtering แบบธรรมดา) ที่เป็น Stateless แบบที่.ใช้ในเราเตอร์ทั่วไป(จะควบคุมการเข้าออกของแพ็กเก็ตโดยพิจารณาข้อมูลจากเฮดเดอร์ของแต่ละแพ็กเก็ต นำมาเทียบกับกฎที่มีอยู่ ซึ่งกฎที่มีอยู่ก็จะเป็นกฎที่สร้างจากข้อมูลส่วนที่อยู่ในเฮดเดอร์เท่านั้น ดังนั้น Packet Filtering แบบธรรมดาจึงไม่สามารถทราบได้ว่า แพ็กเก็ตนี้อยู่ส่วนใดของการเชื่อมต่อ เป็นแพ็กเก็ตที่เข้ามาติดต่อใหม่หรือเปล่า หรือว่าเป็นแพ็กเก็ตที่เป็นส่วนของการเชื่อมต่อที่เกิดขึ้นแล้ว เป็นต้น

Stateful Inspection เป็นเทคโนโลยีที่เพิ่มเข้าไปใน Packet Filtering โดยในการพิจารณาว่าจะยอมให้แพ็กเก็ตผ่านไปนั้น แทนที่จะดูข้อมูลจากเฮดเดอร์เพียงอย่างเดียว Stateful Inspection จะนำเอาส่วนข้อมูลของแพ็กเก็ต) message content) และข้อมูลที่ได้จากแพ็กเก็ตก่อนหน้านี้ที่ได้ทำการบันทึกเอาไว้ นำมาพิจารณาด้วย จึงทำให้สามารถระบุได้ว่าแพ็กเก็ตใดเป็นแพ็กเก็ตที่ติดต่อเข้ามาใหม่ หรือว่าเป็นส่วนหนึ่งของการเชื่อมต่อที่มีอยู่แล้ว

สเตทฟูลไฟร์วอลล์เป็นเครื่องมือที่ถูกออกแบบมาเพื่อทำหน้าที่ในการควบคุมทราฟฟิคโดยเฉพาะไม่ได้เป็นการดัดแปลงการทำงานมาจารเราเตอร์ จึงมีความสามารถในการควบคุมทราฟฟิค การกำหนดแอคเซสรูล การบริหาร รวมไปถึงความยืดหยุ่นของการควบคุมทราฟฟิค และประสิทธิภาพในการทำงานที่สูงกว่าสกรีนนิ่งเราเตอร์เป็นอย่างมาก ซึ่งโดยทั่วไปไฟร์วอลล์ที่มีขายในท้องตลาดจะเป็นไฟร์วอลล์แบบนี้

ข้อดีของสเตทฟูลไฟร์วอลล์

- ใช้งานง่ายเพราะถูกออกแบบมาทำหน้าที่ของไฟร์วอลล์โดยเฉพาะ ตรวจสอบแก้ไขแอคเซสรูลได้ง่าย รูปแบบของคำสั่ง ถึงแม้ว่าจะต่างยี่ห้อกันก็สามารถเรียนรู้ได้อย่างรวดเร็ว
- ประสิทธิภาพในการทำงานสูง เนื่องจากออกแบบมาทำหน้าที่ไฟร์วอลล์โดยเฉพาะ สามารองรับแอคเซสรูลที่ซับซ้อนได้ โดยที่ความสามารในการทำงานไม่ตกลง
- มีคุณสมบัติเพิ่มเติมให้ใช้ได้มากนอกเหนือจากการควบคุมทราฟฟิค เช่น สามารนำไปใช้ร่วมกับระบบตรวจจับการบุกรุกหรือ IDS (Intrusion Detection System) เพื่อป้องกันการโจมตีได้อัตโนมัติ สามารบันทึกข้อมูลเอาไว้กลับมาดูในภายหลังได้ สามารใช้งานร่วมกับระบบ Anti-virus ได้
- การกำหนดแอคเซสรูลทำได้ง่าย เพราะไฟร์วอลล์มีความเข้าใจในโปรโตคอลระดับสูล ดังนั้นผู้ใช้อาจจะไม่จำเป็นต้องมีความเชี่ยวชาญในเครื่องเน็ตเวิร์กมาก ก็พอจะใช้งานไฟร์วอลล์ได้โดยกำหนดกฎบนพื้นฐานของแอพพลิเคชันที่ผู้ใช้รู้จัก มากกว่าการกำหนดกฎโดยใช้ข้อมูลบนแพ็คเก็ตโดยตรง เช่นแทนที่จะต้องกำหนดแอคเซสรูลให้อนุญาต ICMP time exceed in transit ให้ผ่านได้ เพื่อจะใช้คำสั่ง Traceroute ทำการระบุในไฟร์วอลล์ว่าอนุฐานให้คำสั่ง Traceroute ทำงานได้ หลังจากนั้นไฟร์วอลล์จึงกำหนดเป็นแอคเซสรูลที่ระบุโปรโตคอล
- สามารถเพิ่มเติมบริการอื่นได้ เช่น Virtual Private Network, Tunneling
- สามารถเพิ่มเติมความปลอดภัยโดยระบบการตรวจสอบผู้ใช้ (Authenticate) ได้
- การสื่อสารระหว่างไฟร์วอลล์กับแอดมินคอนโซล (โฮสต์ที่ทำหน้าที่ในการบริหารไฟร์วอลล์) จะมีความปลอดภัยสูง มีการตรวจสอบสิทธิ์ของผู้ที่เป็นแอดมิน รวมทั้งการสื่อสารระหว่าไฟร์วอลล์กับคอนโซล จะมีการรักษาความปลอดภัยที่เข้มงวด มีการเข้ารหัสเพื่อป้องกันการดักอ่านข้อมูล

ข้อเสียของสเตทฟูลไฟร์วอลล์

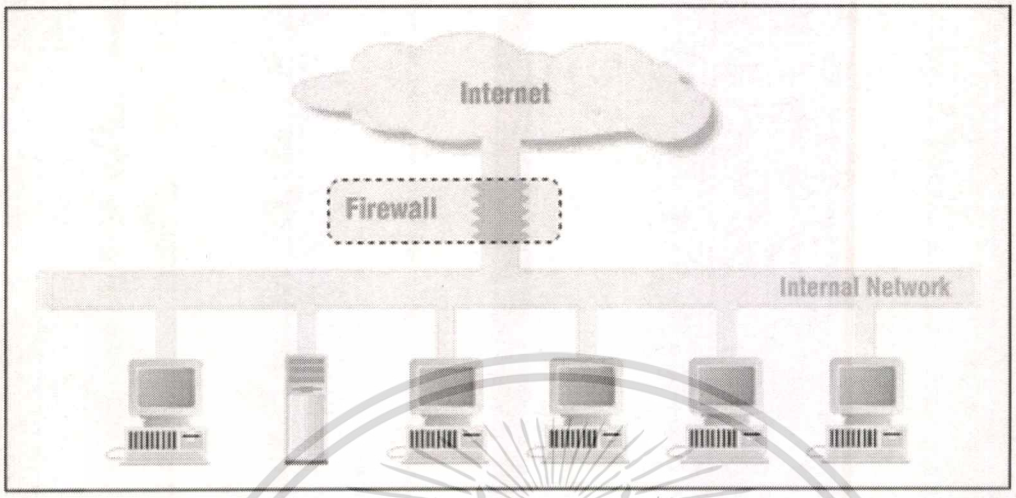
- มีราคาแพง ถึงแม้ว่าปัจจุบันจะลดลงไปมากแล้วแต่ก็ยังแพงอยู่
- ในกรณีที่เป็นไฟร์วอลล์แบซอฟแวร์ที่ทำงานอยู่บนระบบปฏิบัติการทั่วไปเช่น Solaris, Microsoft Windows 2000 ต่างก็มีความเสี่ยงที่จะถูกเจาะได้เนื่องจากปัญหาของแต่ละระบบปฏิบัติการเอง ซึ่งจะสามารถเจาะได้ง่ายกว่าการเจาะเราเตอร์ เพราะรูรั่วของระบบปฏิบัติการมีมากกว่าของเราเตอร์
- ในกรณีที่ไฟร์วอลล์เป็นประเภท Network Appliance คือออกแบบทั้งซอฟแวร์และฮาร์ดแวร์เป็นเครื่องเดียวกัน เพื่อทำหน้าที่เป็นไฟร์วอลล์โดยเฉพาะ ผู้ใช้จำเป็นต้องพึ่งพาผู้ผลิตค่อนข้างมาก หากมีปัญหาอาจจะไม่สามารถแก้ไขโดยการใช้อะไหล่ทดแทนจากที่อื่นได้

2.5 สถาปัตยกรรมของไฟร์วอลล์

ในส่วนของ Firewall Architecture นั้น จะพูดถึงการจัดวางไฟร์วอลล์คอมโพเน็นต์ในแบบต่างๆ เพื่อทำให้เกิดเป็นระบบไฟร์วอลล์ขึ้น

2.5.1 Single Box Architecture

Single Box Architecture เป็น Architecture แบบง่ายๆ ที่มีคอมโพเน็นต์ทำหน้าที่เป็นไฟร์วอลล์เพียงอันเดียวตั้งอยู่ระหว่างเน็ตเวิร์กภายในกับเน็ตเวิร์กภายนอก ข้อดีของวิธีนี้ก็คือการที่มีเพียงจุดเดียวที่หน้าที่ไฟร์วอลล์ทั้งหมด ควบคุมการเข้าออกของข้อมูล ทำให้ดูแลได้ง่าย เป็นจุดสนใจในการดูแลความปลอดภัยเน็ตเวิร์ก ในทางกลับกันข้อเสียของวิธีนี้ก็คือ การที่มีเพียงจุดเดียวนี้ทำให้มีความเสี่ยงสูง หากมีการคอนฟิกูเรชันผิดพลาดหรือมีช่องโหว่เพียงเล็กน้อย การผิดพลาดเพียงจุดเดียวอาจทำให้ระบบถูกเจาะได้ คอมโพเน็นต์ที่ใช้ใน Architecture นี้อาจเป็น Screening Router , Dual-Homed Host หรือ Multi-purposed Firewall Box ก็ได้



รูปที่ 4 Firewall Architecture แบบชั้นเดียว

➢ **Screening Router**

เราสามารถใช้เราเตอร์ทำ Packet Filtering ได้ วิธีนี้จะทำให้ประหยัดค่าใช้จ่าย เนื่องจากส่วนใหญ่จะใช้เราเตอร์ต่อกับเน็ตเวิร์กภายนอกอยู่แล้ว แต่วิธีนี้อาจไม่ยืดหยุ่นมากนักในการคอนฟิกกูเรชัน

Architecture แบบนี้เหมาะสำหรับ

1. เน็ตเวิร์กที่มีการป้องกันความปลอดภัยในระดับของโฮสต์) Host security) เป็นอย่างดีแล้ว
2. มีการใช้โปรโตคอลไม่มาก และโปรโตคอลที่ใช้ก็เป็นโปรโตคอลที่ไม่ซับซ้อน
3. ต้องการไฟร์วอลล์ที่มีความเร็วสูง

➢ **Dual-Homed Host**

เราสามารถใช้ Dual-Homed Host (คอมพิวเตอร์ที่มีเน็ตเวิร์กอินเตอร์เฟสอย่างน้อย 2 อัน (ใช้การบริการเป็น Proxy ให้กับเครื่องภายในเน็ตเวิร์ก

Architecture แบบนี้เหมาะสำหรับ

1. เน็ตเวิร์กที่มีการใช้งานอินเตอร์เน็ตค่อนค่างน้อย
2. เน็ตเวิร์กที่ไม่ได้มีข้อมูลสำคัญๆ

➢ **Multi-purposed Firewall Box**

มีผลิตภัณฑ์หลายชนิดที่ผลิตออกมาเป็นกล่องๆ เดียว ซึ่งทำหน้าที่ได้หลายอย่าง ทั้ง Packet Filtering, Proxy แต่ก็อย่าลืมว่านี่คือ Architecture แบบชั้นเดียว ซึ่งถ้าพลาดแล้วก็จะเสียหายทั้งเน็ตเวิร์กได้

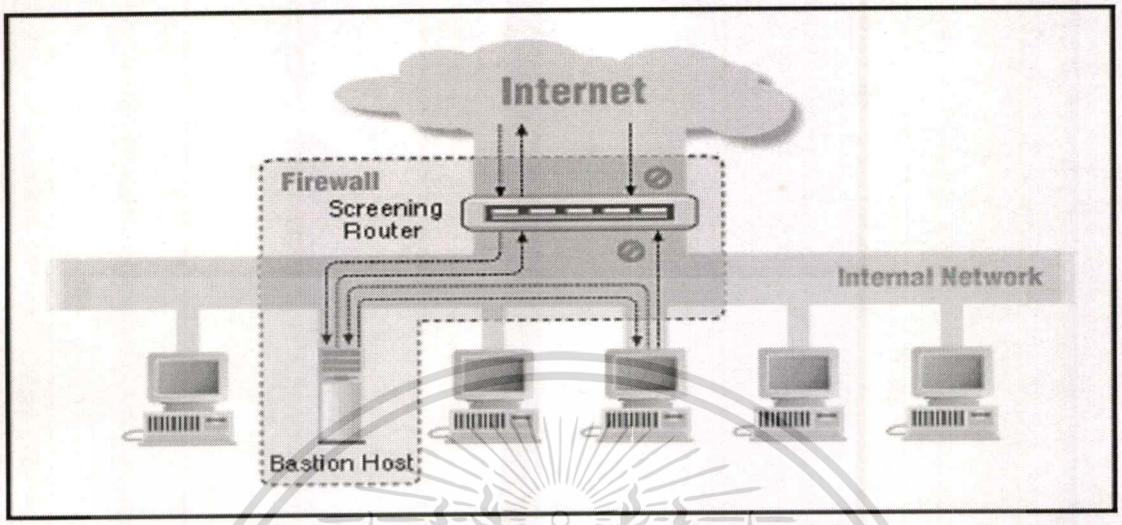
2.5.2 Screened Host Architecture

Screened Host Architecture จะมีโฮสต์ซึ่งให้บริการ Proxy เหมือนกับใน Single Box Architecture ที่เป็น Dual-homed Host แต่จะต่างกันตรงที่ว่า โฮสต์นั้นจะอยู่ภายในเน็ตเวิร์ก ไม่ต่ออยู่กับเน็ตเวิร์กภายนอกอื่นๆ (ดังนั้นก็ไม่จำเป็นที่จะต้องใช้ Dual Homed Host) และจะมี เราเตอร์ที่ทำหน้าที่ Packet Filtering ช่วยบังคับให้เครื่องภายในเน็ตเวิร์กต้องติดต่อเซอร์วิสผ่าน Proxy โดยไม่ยอมให้ติดต่อใช้เซอร์วิสจากภายนอกโดยตรง และก็ให้ภายนอกเข้าถึงได้เฉพาะ Bastion host (คือโฮสต์ที่มีความเสี่ยงสูงต่อการถูกโจมตี มักจะเป็นโฮสต์ที่เปิดให้บริการกับอินเตอร์เน็ต ดังนั้นโฮสต์นี้ต้องมีการดูแลเป็นพิเศษ เท่านั้น

จากรูปที่ 5 ใน Architecture แบบนี้จะประกอบไปด้วยเราเตอร์ทำหน้าที่ Packet Filtering และภายในเน็ตเวิร์กจะมี Bastion Host ให้บริการ Proxy อยู่ โดยที่เราเตอร์นั้นอาจจะถูกเซ็ตดังนี้

- ❖ อาจจะอนุญาตให้เครื่องภายในใช้เซอร์วิสบางอย่างได้โดยตรง
- ❖ ส่วนเซอร์วิสอื่นๆ จะไม่ยอมให้เครื่องภายในติดต่อผ่านออกไปโดยตรง ยกเว้น Bastion Host เท่านั้นที่สามารถติดต่อกับเน็ตเวิร์กภายนอกได้ทั้งนี้เพื่อเป็นการบังคับให้ใช้บริการ Proxy ผ่านทาง Bastion Host เท่านั้น

หรืออาจจะเซ็ตให้เซอร์วิสส่วนใหญ่ผ่านเราเตอร์ออกไปได้โดยตรงแล้ว ให้บางส่วนต้องใช้เซอร์วิสผ่าน Proxy ก็แล้วแต่นโยบายและความเหมาะสมขององค์กร



รูปที่ 5 Screened Host Architecture

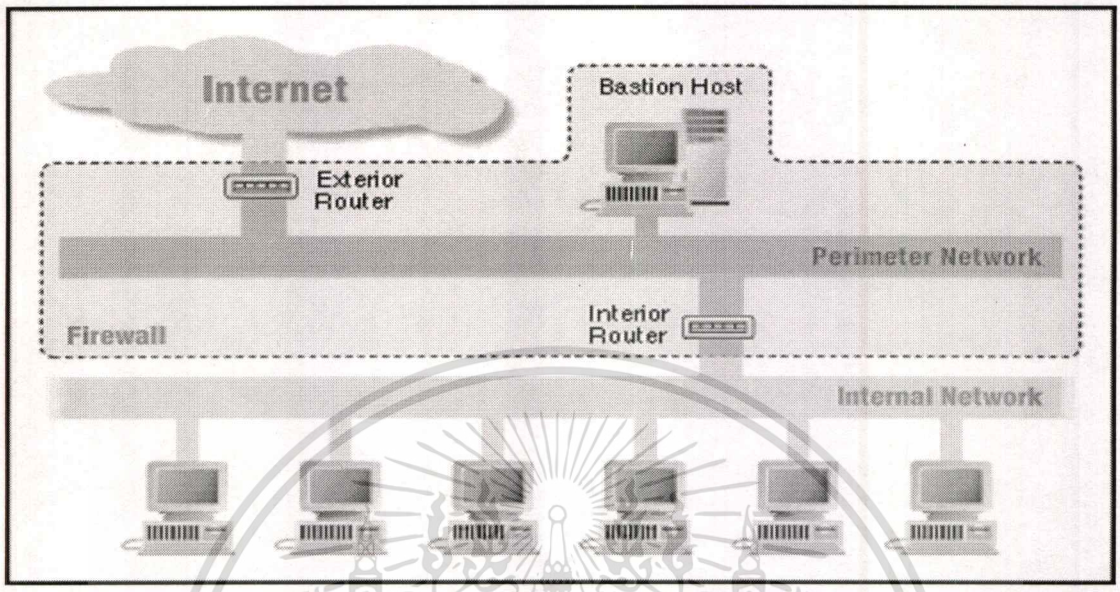
วิธีนี้ถึงแม้ว่าจะมีทั้ง Proxy และเราเตอร์ทำหน้าที่ Packet Filtering แต่ก็ยังคงอันตรายอยู่ เพราะว่าเราเตอร์ต้องยอมให้ภายนอกสามารถติดต่อกับ Bastion Host ได้อยู่แล้ว หากแฮกเกอร์สามารถเจาะเข้ามายัง Bastion Host ได้ก็เสร็จ

Architecture นี้เหมาะสำหรับ

- ❖ เน็ตเวิร์กที่มีการติดต่อกับเน็ตเวิร์กภายนอกน้อย
- ❖ เน็ตเวิร์กที่มีการป้องกันความปลอดภัยในระดับของโฮสต์เป็นอย่างดีแล้ว

2.5.3 Multi Layer Architecture

ในสถาปัตยกรรมแบบหลายชั้น ไฟร์วอลล์จะเกิดขึ้นจากคอมโพเน็นต์หลายๆส่วนทำหน้าที่ประกอบกันขึ้นเป็นระบบ วิธีการนี้สามารถเพิ่มความปลอดภัยได้มาก เนื่องจากเป็นการลดความเสี่ยงต่อความผิดพลาดที่อาจเกิดขึ้น ถ้าหากมีไฟร์วอลล์เพียงจุดเดียวแล้วมีเกิดความผิดพลาดเกิดขึ้น ระบบทั้งหมดก็จะเป็นอันตราย แต่ถ้ามีการป้องกันหลายชั้น หากในชั้นแรกถูกเจาะ ก็อาจจะมีความเสียหายเพียงบางส่วน ส่วนที่เหลือระบบก็ยังคงมีชั้นอื่นๆ ในการป้องกันอันตราย และยังลดความเสี่ยงได้โดยการที่แต่ละชั้นนั้นมีการใช้เทคโนโลยีที่แตกต่างกัน เพื่อให้เกิดความหลากหลายเป็นการหลีกเลี่ยงการโจมตีหรือช่องโหว่ที่อาจมีในเทคโนโลยีชนิดใดชนิดหนึ่ง โดยทั่วไปแล้วสถาปัตยกรรมแบบหลายชั้นจะเป็นการต่อกันเป็นซีรี่โดยมี Perimeter Network (หรือบางทีเรียกว่า DMZ Network) อยู่ตรงกลาง เรียกว่า Screened Subnet Architecture



รูปที่ 6 Screened Subnet Architecture

2.5.4 Screened Subnet Architecture

Screened Subnet Architecture เป็นสถาปัตยกรรมที่มีการเพิ่ม Perimeter Network เข้าไปกั้นระหว่างอินเตอร์เน็ตกับเน็ตเวิร์กภายในไม่ให้เชื่อมต่อกันโดยตรง ทำให้เน็ตเวิร์กภายในมีความปลอดภัยมากขึ้น

ในรูปที่ 6 แสดง Screened Subnet Architecture อย่างง่าย ประกอบไปด้วย เราเตอร์ 2 ตัว ตัวนึงอยู่ระหว่างอินเตอร์เน็ตกับ Perimeter Network ส่วนอีกตัวหนึ่งอยู่ระหว่าง Perimeter Network กับเน็ตเวิร์กภายใน ถ้าหากแฮกเกอร์จะเจาะเน็ตเวิร์กภายในต้องผ่านเราเตอร์เข้ามาถึง 2 ตัวด้วยกัน ถึงแม้ว่าจะเจาะชั้นแรกเข้ามายัง Bastion host ได้ แต่ก็ยังต้องผ่านเราเตอร์ตัวในอีก ถึงจะเข้ามายังเน็ตเวิร์กภายในได้

คอมโพเน็นต์ของ Screened Subnet Architecture ในรูปที่ 6

- Perimeter Network เป็นเน็ตเวิร์กที่เพิ่มเข้ามาเพื่อความปลอดภัย อยู่ระหว่างเน็ตเวิร์กภายนอกกับเน็ตเวิร์กภายใน ประโยชน์ของ Perimeter Network ที่เห็นได้ชัดก็คือ การแบ่งเน็ตเวิร์กออกเป็นส่วนๆ ทำให้การไหลของข้อมูลถูกแบ่งออกเป็นส่วนๆตามเน็ตเวิร์กด้วย เนื่องจากโดยทั่วไปแล้ว เน็ตเวิร์กที่เป็นแลนนั้น จะเป็นแบบ Ethernet ซึ่งจะมีการส่งข้อมูลแบบ Broadcast ดังนั้นถ้ามีใครคอบดักจับ

ข้อมูลอยู่ในเน็ตเวิร์กนั้น ก็จะได้พาสเวิร์ด ข้อมูลต่างๆ ไปหมด ดังนั้นหากไฟร์วอลล์เรามีชั้นเดียวและแฮกเกอร์สามารถเข้ามาได้ โดนดักจับข้อมูลก็เสร็จหมด แต่ถ้าเรามี Perimeter Network ถึงจะดักจับข้อมูลได้แต่ก็จะได้เพียงที่อยู่บน Perimeter Network เท่านั้น

- ❖ Bastion Host ตั้งอยู่บน Perimeter Network ทำหน้าที่ให้บริการ Proxy กับเน็ตเวิร์กภายใน และให้บริการต่างๆ กับผู้ใช้บนอินเตอร์เน็ต Bastion Host นั้นจะมีความเสี่ยงต่อการโจมตีสูง จึงต้องมีการดูแลความปลอดภัยเป็นพิเศษ
- ❖ Interior Router ตั้งอยู่ระหว่าง Perimeter Network กับเน็ตเวิร์กภายใน ทำหน้าที่ Packet Filtering ป้องกันเน็ตเวิร์กภายในจาก Perimeter Network ในการเซ็ต configuration ระหว่าง เน็ตเวิร์กภายในกับ Perimeter Network ควรกำหนดอย่างรอบคอบ อนุญาตเฉพาะเซอร์วิสที่จำเป็นเท่านั้นอย่างเช่น DNS, SMTP
- ❖ Exterior Router ตั้งอยู่ระหว่างเน็ตเวิร์กภายนอกกับ Perimeter Network เนื่องจาก Exterior Router นี้เป็นจุดที่ต่ออยู่กับเน็ตเวิร์กภายนอก จึงมีหน้าที่ที่สำคัญอย่างหนึ่งคือ การป้องกันแพ็กเก็ตที่มีการ Forged IP Address เข้ามา โดยอ้างว่ามาจากเน็ตเวิร์กภายในทั้งๆ ที่จริงๆ แล้วมาจากเน็ตเวิร์กภายนอก

2.6 ประเภทของระบบไฟร์วอลล์ที่ศึกษา

ประเภทของไฟร์วอลล์ที่นำมาใช้เพื่อทำการศึกษาสามารถจำแนกได้ 3 แบบคือ

2.6.1 ไฟร์วอลล์ที่ติดตั้งโดยโอเพนซอส

คือระบบไฟร์วอลล์ที่สร้างที่มีพื้นฐานมาซอฟแวร์ที่เป็นฟรีแวร์ หรือ โอเพ่นซอส ซึ่งในที่นี้ไม่การเก็บค่าลิขสิทธิ์ในการใช้งานแต่อย่างใด ตัวอย่างของไฟร์วอลล์ที่เป็นลักษณะแบบนี้ได้แก่ IPchains, IPtables, IPFW เป็นต้น ซึ่งไฟร์วอลล์ที่กล่าวมาเป็นลักษณะของไฟร์วอลล์ที่ทำงานแบบคอมมานไลน์คือต้องทำงานโดยการใส่พารามิเตอร์เข้าไปให้กับคำสั่งไฟร์วอลล์ที่ต้องการ และจะต้องใส่ให้ถูกต้อง มิฉะนั้นจะไม่สามารถทำงานได้ หรือสามารถใช้งานเป็นแบบสคริปได้ แต่จะต้องทำการเรียงบรรทัดให้ถูกด้วย ซึ่งถ้าเรียงไม่ถูกจะทำให้เกิดการทำงานที่ผิดพลาดได้

ไฟร์วอลล์ที่กล่าวมาข้างต้นนี้เป็นซอฟแวร์ เพราะฉะนั้นในการทำงานจำเป็นต้องทำงานอยู่บนระบบปฏิบัติการอีกทีหนึ่ง ซึ่งระบบปฏิบัติการที่ใช้ก็จะเป็นฟรีแวร์ด้วย เช่น Redhat linux,

SUSE, Slackware, Freebsd , Mandrake เป็นต้น ซึ่งเป็นระบบปฏิบัติการที่เป็นโอเพนซอสเช่นกัน ไม่มีการเก็บค่าลิขสิทธิ์ในการใช้งาน แต่จะเก็บเฉพาะค่าแผ่นซีดีรอมที่เป็นมีเดียในการเก็บระบบปฏิบัติการ หรือสามารถดาวโลว์ดจากเอฟทีพีไซท์ของผู้ผลิตแต่ละเจ้าได้เลย

ข้อดีของการใช้ระบบไฟร์วอลล์แบบโอเพ่นซอส

1. มีราคาค่าซอฟแวร์ถูกมาก เนื่องจากเป็นซอฟแวร์ที่แจกให้ใช้งานฟรี ไม่มีการนับการคอนเนคชั่น หรือเซสชั่นที่เกิดขึ้นทั้งสิ้น
2. มีเสถียรภาพในการทำงานค่อนข้างดี ถ้ามีการติดตั้งถูกต้องและรัดกุมเพียงพอ ถ้าทุกอย่างได้ทำการคอนฟิกอย่างถูกต้องแล้ว ไม่จำเป็นต้องทำสิ่งใดเลย สามารถปล่อยให้อยู่แบบนั้นได้
3. มีความยืดหยุ่นในการทำงานค่อนข้างสูงสามารถประยุกต์ใช้กับเน็ทเวิร์กได้ในหลายรูปแบบ เช่น การทำเพอร์โซนอลไฟร์วอลล เป็นต้น
4. คำสั่งที่ใช้ง่ายต่อการเรียนรู้ และสามารถทำให้เข้าใจลักษณะการทำงานของเน็ทเวิร์กมากขึ้น ซึ่งถ้าผู้ที่เรียนรู้มีพื้นการทางด้านเน็ทเวิร์กที่ดีพอก็สามารถทำได้
5. อัพเกรดได้ง่ายเนื่องจากซอฟแวร์เหล่านี้มีเวอร์ชั่นใหม่ๆ ออกมาตลอด ในส่วนของเครื่องคอมพิวเตอร์ที่มาติดตั้งก็สามารถอัพเกรดให้มีความเร็วมากขึ้นได้ ตามความต้องการ โดยมองว่าในปัจจุบันฮาร์ดแวร์คอมพิวเตอร์มีราคาถูกลงมาก

ข้อเสียของการใช้ระบบไฟร์วอลล์แบบโอเพ่นซอส

1. ต้องการคนที่มีความรู้ความสามารถในการติดตั้ง ตั้งแต่ตัวระบบปฏิบัติการเอง รวมไปถึงการ คอนฟิกตัวไฟร์วอลล์ ตลอดจนการดูแลรักษาและอัพเดทตัวแอคเซสรูลด้วย
2. ไม่มีความเป็นอัตโนมัติในตัวระบบจำเป็นต้องใช้บุคลากรในการทำงานทุกอย่าง
3. ฟีเจอร์บ้างอย่างเช่น IDS (Intrusion Detection system) ไม่มีมาให้ในตัวไฟร์วอลล์ จำเป็นต้องทำการติดตั้ง และคอนฟิกเอง และที่สำคัญตัว Log ที่ได้ยังดูยากต้องการผู้ที่เคยใช้งาน หรือมีความเชี่ยวชาญในการดูแล หรือถ้าไม่เช่นนั้นต้องใช้ซอฟแวร์ที่เป็นไลเซนต์ เช่น Websence log analyzer ในการเอามาตรวจสอบล็อกไฟล์ เพื่อแปรผลอีกทีหนึ่ง

4. เนื่องจากเป็นไฟร์วอลล์ที่ทำงานอยู่บนระบบปฏิบัติการ จึงอาจเกิดปัญหา OS Vunulability ได้ จำเป็นต้องมีการอัพเดท Patch ให้กับตัวระบบปฏิบัติการเสมอ
5. มีความสามารถ และเสถียรภาพในการทำงาน แปรผันตามปัจจัยหลายอย่างเช่น สเปคของเครื่องคอมพิวเตอร์ที่ใช้ ระบบปฏิบัติการที่ใช้ หรือไฟร์วอลล์ที่เลือก เป็นต้น

2.6.2 ไฟร์วอลล์ที่ติดตั้งโดยซอฟแวร์ที่มีลิขสิทธิ์

ระบบไฟร์วอลล์ที่มีลิขสิทธิ์ถูกต้อง) Lincence software) เช่น Microsoft ISA server 2000 CheckPoint Firewall-1 เป็นต้น โดยทำการติดตั้งระบบลงบนเครื่องคอมพิวเตอร์เช่นเดียวกับระบบไฟร์วอลล์แบบแรก แต่แตกต่างกันตรงที่ซอฟแวร์ที่นำมาใช้ในการสร้างระบบไฟร์วอลล์ต้องเสียค่าลิขสิทธิ์ในการนำซอฟแวร์นั้นมาใช้งาน มิฉะนั้นจะถือว่าผิดกฎหมายลิขสิทธิ์ ซึ่งลักษณะการซื้อต้องซื้อลิขสิทธิ์ตามจำนวนผู้ใช้ที่ใช้งานผ่านไฟร์วอลล์นี้ หรือ สามารถคิดลิขสิทธิ์ตามคอนเนคชั่นที่เกิดขึ้น เช่นในกรณีของการเปิดเว็บไซท์ 1 หน้า จะถือว่าเป็นการเปิด 1 คอนเนคชั่น จะเห็นได้ว่าถ้ามีการใช้งานผ่านตัวไฟร์วอลล์นี้มาก จะต้องทำการเสียค่าลิขสิทธิ์เพิ่ม ในกรณีที่มีการใช้เกินมักจะทำให้การเชื่อมต่อที่เกินออกจากที่กำหนดนั้นไม่สามารถกระทำได้ ฉะนั้นถ้ามีผู้ใช้งานอยู่เป็นจำนวนมากจำเป็นต้องซื้อลิขสิทธิ์ซอฟแวร์มากขึ้นด้วย หรือ ในบางกรณีที่ไม่ต้องการซื้อเพิ่มบ่อยๆ สามารถจะซื้อเป็นลิขสิทธิ์แบบอัลลิมิต (Unlimit) ได้ แต่จะเสียค่าใช้จ่ายในการซื้อสูงมาก

ข้อดีของไฟร์วอลล์ที่ติดตั้งโดยซอฟแวร์ที่มีลิขสิทธิ์

1. มีลักษณะการทำงานที่ครบถ้วนสมบูรณ์ในตัวเอง ไม่จำเป็นต้องทำสิ่งใดเพิ่ม เนื่องจากซอฟแวร์เหล่านี้มักจะสร้างเครื่องมือมาให้ครบสมบูรณ์แล้ว
2. การติดตั้งทำได้สะดวก เนื่องจากมียูเซอร์อินเทอร์เฟส ที่เรียนรู้และเข้าใจได้ง่าย สามารถทำความเข้าใจได้โดยใช้เวลาไม่นาน และยังมีส่วนที่เป็นตัวช่วยเหลือสามารถอ่านได้ เมื่อเกิดความไม่เข้าใจในการติดตั้ง
3. บริการหลังการขายมีให้พร้อม เมื่อมีปัญหาสามารถติดต่อสอบถามหรือสามารถให้ตัวแทนจำหน่าย เข้ามาช่วยติดตั้งหรือปรับแต่งค่าคอนฟิกต่างๆ ได้ หรืออาจมีการทำสัญญาการบำรุงรักษาก็ได้

4. มีการแสดงผล และการทำรายงานในตัวเอง สามารถตรวจสอบและทำการส่ง alert ไปยังผู้ดูแลระบบได้ ไม่ว่าจะผ่านทาง อีเมล์ เป็นต้น มีระบบการทำงานที่อัตโนมัติมากขึ้นด้วย เช่นสามารถที่จะทำการดร็อปแพ็คเก็ตที่มีปัญหาได้ โดยที่ไม่ต้องคอยสั่งให้ทำงาน เนื่องจากในซอฟแวร์เหล่านี้มักจะมีส่วนของแพทเทิร์น (pattern)ของการโจมตีอยู่ด้วย ทำให้สามารถทราบได้ถึงแพ็คเก็ตที่มีรูปแบบการทำงานลักษณะนี้เป็นแพ็คเก็ตที่สมควรให้ผ่านไปได้หรือไม่
5. ซอฟแวร์เหล่านี้มักมีความสามารถอย่างอื่นนอกเหนือจากไฟร์วอลล์ด้วย ในส่วนของไฟร์วอลล์บางยี่ห้อมีการประกอบรวมกับโปรแกรมต่อต้านไวรัสด้วย ในตัวไฟร์วอลล์ของบริษัทแมคอฟีเป็นต้น
6. ไฟร์วอลล์ที่เป็นแบบนี้มักถูกออกแบบให้ทำงานได้มากกว่าในเน็ทเวิร์กเลเยอร์ ซึ่งอาจสามารถทำงานในลักษณะของแอพพลิเคชั่นเลเยอร์ได้ด้วย คือ สามารถจำกัดการทำงานของแอพพลิเคชั่นที่วิ่งผ่านตัวไฟร์วอลล์ไปได้

ข้อเสียของการติดตั้งไฟร์วอลล์ที่ติดตั้งโดยซอฟแวร์ที่มีลิขสิทธิ์

1. ราคาค่าลิขสิทธิ์ซอฟแวร์ที่มีราคาสูง และเปลี่ยนแปลงตามจำนวนของคอนเนคชั่นที่เกิดขึ้น ทำให้ยิ่งมีคอนเนคชั่นมากขึ้นเท่าใด ต้องเสียค่าลิขสิทธิ์มากขึ้นเท่านั้น และต้องเสียค่าลิขสิทธิ์ให้กับระบบปฏิบัติการที่ติดตั้งบนเครื่องเซิร์ฟเวอร์ด้วย
2. ซอฟแวร์บางตัวจำเป็นต้องใช้เครื่องเซิร์ฟเวอร์ที่มีประสิทธิภาพสูง ซึ่งทำให้ราคาเรื่องอุปกรณ์สูงตามไปด้วย
3. เนื่องจากเป็นไฟร์วอลล์ที่ทำงานอยู่บนระบบปฏิบัติการ จึงอาจเกิดปัญหา OS Vululability ได้ จำเป็นต้องมีการอัพเดท Patch ให้กับตัวระบบปฏิบัติการอย่างสม่ำเสมอ
4. ความเสถียรภาพ และความประสิทธิภาพขึ้นอยู่กับปัจจัยหลายอย่างเช่น สเปคของคอมพิวเตอร์ที่ใช้ติดตั้ง ในที่นี้หมายถึงฮาร์แวรคอมพิวเตอร์ทุกชิ้นที่ประกอบกันระบบปฏิบัติการที่ใช้ด้วย

2.6.3 ไฟร์วอลล์ที่ติดตั้งโดยใช้ฮาร์ดแวร์

ระบบไฟร์วอลล์ที่เป็นอุปกรณ์เฉพาะสำหรับทำหน้าที่ไฟร์วอลล์ เช่น Cisco PIX Firewall WatchGuard เป็นต้น ในกลุ่มนี้เป็นระบบไฟร์วอลล์ เป็นกลุ่มของอุปกรณ์ที่ถูกออกแบบมาเพื่อทำงานเฉพาะด้าน ซอฟแวร์ที่ใช้งานภายในถูกออกแบบมาเพื่อทำงานด้านนี้โดยเฉพาะ และมีความสามารถบางอย่างเพิ่มขึ้นมา มีคำสั่งที่มีการใช้งานเฉพาะด้านมากขึ้น เช่นในไฟร์วอลล์ที่เป็นโอเพนซอสอาจใช้คำสั่งในการสั่งงานหลายบรรทัด เพื่อให้ได้ตามวัตถุประสงค์ แต่ถ้าเป็นในส่วนของฮาร์ดแวร์แล้ว ผู้ผลิตอาจมีคำสั่งที่สั่งให้ไฟร์วอลล์ทำงานได้ตามความต้องการภายในบรรทัดเดียว เป็นต้น

ข้อดีของการใช้ไฟร์วอลล์ที่ติดตั้งโดยใช้ฮาร์ดแวร์

1. อุปกรณ์ถูกออกแบบมาเฉพาะสำหรับการทำงานเป็นระบบไฟร์วอลล์อย่างเดียว จึงทำให้มีการทำงานที่รวดเร็ว ประกอบกับการออกแบบซอฟแวร์ที่ใช้งานรวมกันกับอุปกรณ์ ถูกออกแบบมาให้มีคุณลักษณะในการทำงานเฉพาะอย่างมากขึ้น ทำให้ซอฟแวร์ที่ได้มีขนาดเล็ก ทำงานได้อย่างรวดเร็ว
2. มีประสิทธิภาพ ความถูกต้อง เสถียรภาพ และความรวดเร็วในการทำงานที่สูง
3. มีการเพิ่มความสามารถบางอย่างเข้าไปเพื่อทำให้ทำงานได้ในลักษณะที่กว้างขึ้น เช่น การใส่ในส่วนของ VPN เข้ามาด้วย ซึ่งจากการทดสอบพบว่า VPN (Virtual Private Network)สร้างโดยการใช้ฮาร์ดแวร์ไฟร์วอลล์สามารถทำงานได้ดีกว่าและรวดเร็วกว่าการทำงานของ VPN ที่สร้างด้วยซอฟแวร์ไฟร์วอลล์
4. มีความทนทานในการใช้งานสูง มีขนาดเล็ก และไม่จำเป็นต้องมีอุปกรณ์ต่อพ่วงเหมือนกับเครื่องคอมพิวเตอร์ ทำให้สามารถประหยัดพื้นที่ในการวางได้ และยังทำให้ช่วยลดอัตราการสิ้นเปลืองพลังไฟฟ้าไปกับอุปกรณ์ที่ไม่ได้ใช้งานด้วย

ข้อดีของการใช้ไฟร์วอลล์ที่ติดตั้งโดยใช้ฮาร์ดแวร์

1. การที่อุปกรณ์ถูกออกแบบมาอย่างจำกัด ทำให้ความยืดหยุ่นในการใช้งานทางด้านอื่นต่ำลง เช่นไม่สามารถทำงานได้เหมือนกับคอมเตอร์ส่วนบุคคลทั่วไป ความสามารถในการอัพเกรดไปตามความต้องการนั้นทำได้ยากกว่าเนื่องจากการออกแบบที่จำกัด

2. การอัพเกรดในแต่ละอย่างจำเป็นต้องใช้ฮาร์ดแวร์ที่ผลิตขึ้นเฉพาะให้สามารถใช้กับอุปกรณ์รุ่นนั้นๆ ได้ ทำให้เมื่อมีใช้ไปนานๆ และจำเป็นต้องอัพเกรด อาจทำไม่ได้เนื่องจากเลิกผลิตไปแล้ว เป็นต้น
3. ในบางไฟร์วอลล์มักมีปัญหาความเสถียรภาพของซอฟแวร์ภายใน ซึ่งบางครั้งทางผู้ผลิตมิได้แจ้งล่วงหน้าทำให้เกิดปัญหาในการใช้งาน แต่ถ้าในส่วนของซอฟแวร์ไฟร์วอลล์ ถ้ามีปัญหาทางผู้ผลิตจะรีบออก patch มาทำการแก้ไขที่เร็วกว่า

บทที่ 3
ระบบเครือข่ายในบริษัท เมอร์ค จำกัด

3.1 ระบบเครือข่ายในบริษัท เมอร์ค จำกัด

ระบบเครือข่ายในบริษัท เมอร์ค จำกัด ประกอบด้วยเครื่องคอมพิวเตอร์ส่วนบุคคล จำนวน 200 เครื่อง ซึ่งใช้ระบบปฏิบัติการวินโดว์ 2000 วินโดว์ 98 และ วินโดว์เอ็กซ์พี

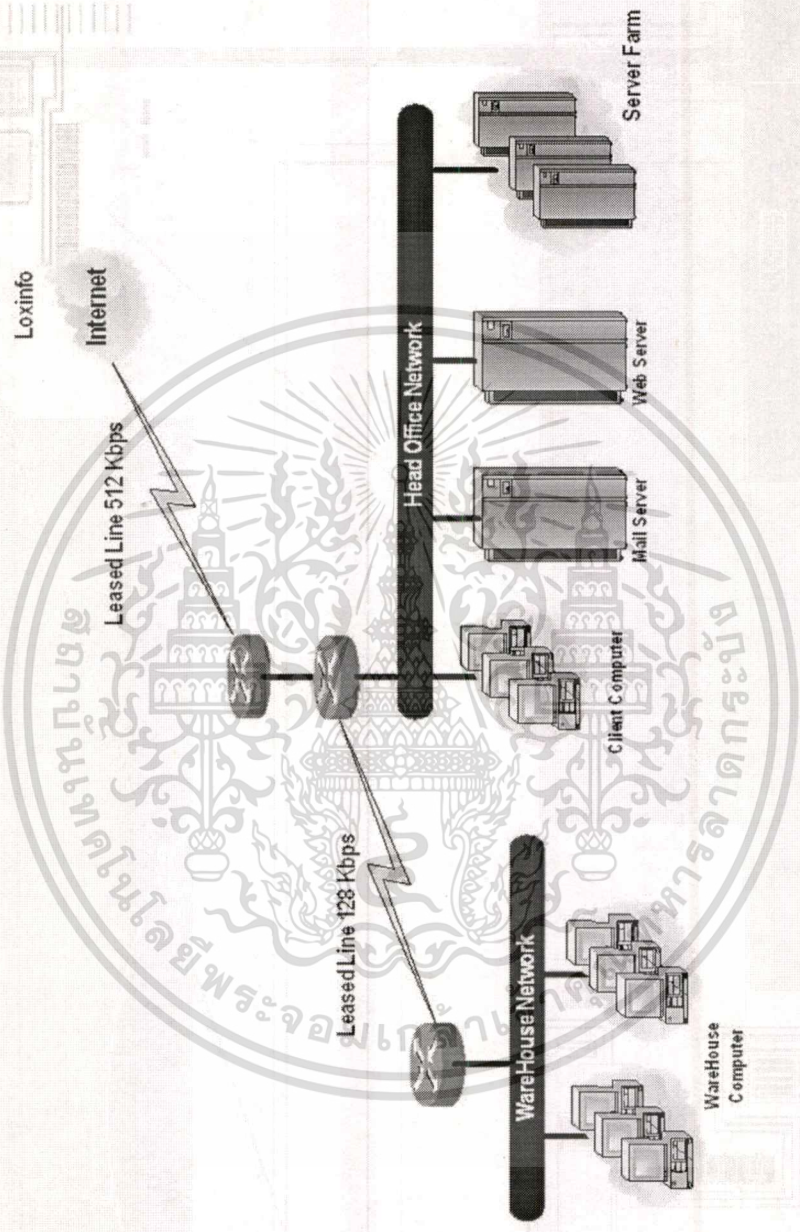
ในส่วนของเครื่องที่ทำหน้าที่เป็นเซิร์ฟเวอร์ จำนวน 10 เครื่อง ทำหน้าที่ต่างๆ ดังนี้

- เมล์เซิรร์ฟเวอร์
- เว็บเซิร์ฟเวอร์
- ไฟล์เซิร์ฟเวอร์
- แอพพลิเคชั่น เซิร์ฟเวอร์
- พร็อกซี่เซิร์ฟเวอร์

การเชื่อมต่อกับอินเทอร์เน็ทใช้วงจรเช่าความเร็วสูง) Leased Line) ติดต่อกับ loxinfo ผ่านเราท์เตอร์ซิสโก้โดยทำการติดต่อกันที่ความเร็ว 512 Kbps และมีเราเตอร์ 1 ตัวทำหน้าที่ติดต่อกับ warehouse โดยผ่านทางวงจรเช่าความเร็วสูง ที่ระดับความเร็ว 128 KB เพื่อเชื่อมต่อกับแอพพลิเคชั่น เซิร์ฟเวอร์ โดยผ่านทาง Terminal server ที่ทำงานบน windows 2000 และใช้พร็อกซี่เซิร์ฟเวอร์สำหรับใช้งานอินเทอร์เน็ทร่วมกันที่ส่วนกลาง ดังรูปที่ 7

พฤติกรรมการใช้งานเครือข่ายของยูเซอร์ส่วนใหญ่ภายในบริษัท เมอร์ก จำกัด เป็นการใช้งานในส่วนของเว็บเบราเซอร์ และการใช้งานฟรีอีเมล์ เช่น ฮ็อตเมล์ ยาฮูเมล์ เป็นต้น และมีการใช้งานในส่วนของเมล์เซิร์ฟเวอร์ภายในออฟฟิส และในบางแผนก เช่นแผนกคอมพิวเตอร์จำเป็นต้องมีการโอนย้ายข้อมูลผ่านทางเอฟทีพีเซิร์ฟเวอร์อีกด้วย

การคอนเนคชั่นที่เกิดขึ้นมาจากภายนอกจะมีอยู่ที่เว็บ และเมล์เซิร์ฟเวอร์ ซึ่งในส่วนของเว็บเซิร์ฟเวอร์มีการเปิดให้บริการแก่บุคคลทั่วไปสามารถเข้าใช้งานได้ แต่ในส่วนของเมล์เซิร์ฟเวอร์มีการเปิดให้เฉพาะคนภายในองค์กรสามารถใช้งานได้ และอนุญาติให้มีการเซ็คอีเมล์ของยูเซอร์ในกรณีที่ยูเซอร์อยู่ภายนอกออฟฟิส โดยการใช้ เว็บเบสเมล์ อีกด้วย



รูปที่ 7 : แผนผังเครือข่ายภายในบริษัท เมอร์ค จำกัด

3.2 สภาพปัญหาทางระบบเน็ทเวิร์กของบริษัท เมอร์ค จำกัด

สภาพปัญหาที่เกิดขึ้นกับระบบเครือข่ายของบริษัท เมอร์ค จำกัด มีดังนี้

1. เครื่องคอมพิวเตอร์ของยูเซอร์ไม่มีการป้องกันจากระบบเน็ทเวิร์กภายนอก สามารถทำการแอคเซสเข้ามาเน็ทเวิร์กภายในได้ เนื่องจากในระบบมีการใช้งานไอพีจริงกับเครื่องคอมพิวเตอร์ทุกเครื่อง ทำให้ผู้ใช้ภายนอกสามารถเข้ามาในระบบเครือข่ายได้สะดวกขึ้น
2. ปัญหาในเรื่องของไอพีแอดเดรสจริงที่มีอยู่จำกัด ทำให้ความสามารถในขยายการเชื่อมต่อเน็ทเวิร์กให้ใหญ่ขึ้นไม่สามารถทำได้
3. ไม่มีสามารถควบคุมการใช้งานแอพพลิเคชั่น และการแอคเซสเข้าสู่เครือข่ายอินเทอร์เน็ทได้
4. ไม่มีการปกป้อง เมล์และเว็บ เซิร์ฟเวอร์จากบุคคลภายนอก หรือ เครือข่ายภายนอกได้ เช่น ไม่มีการปิดพอร์ตที่ไม่จำเป็นบนเซิร์ฟเวอร์ ทำให้เป็นช่องว่างให้แฮคเกอร์สามารถเข้ามาทำลายเซิร์ฟเวอร์ได้
5. ไม่สามารถตรวจสอบการทำงานของระบบเครือข่ายได้ เช่น ไม่สามารถตรวจสอบลักษณะของแพ็คเก็ตที่วิ่งอยู่ในระบบเครือข่าย ทำให้ไม่สามารถติดตามความผิดปรกติที่เกิดขึ้นในระบบเน็ทเวิร์กได้
6. ไม่สามารถทำการแบ่งเน็ทเวิร์กภายใน และภายนอกออกจากกันได้อย่างชัดเจน ทำให้เซิร์ฟเวอร์ในส่วนที่เป็นเซิร์ฟเวอร์ที่ใช้งานภายใน มิได้ถูกแบ่งแยกออกจากระบบเน็ทเวิร์ก ทำให้ไม่สามารถป้องกันอันตรายจากการโจมตี โดยบุคคลภายนอกได้
7. ไม่มีระบบการเตือนภัย เมื่อระบบเน็ทเวิร์กมีปัญหา ซึ่งอาจเนื่องมาจากการถูกโจมตีด้วยภัยคุกคามทางอินเทอร์เน็ท เช่น Denail Of Service Trojan Horse เป็นต้น

3.3 ความต้องการใช้ระบบไฟร์วอลล์ของบริษัท เมอร์ค จำกัด

วัตถุประสงค์ที่ทางบริษัทต้องการนำระบบไฟร์วอลล์เข้ามาใช้มีดังนี้

1. ทำการแบ่งเน็ทเวิร์กออกเป็น 3 ส่วน คือ เน็ทเวิร์กภายในวงแลนของบริษัท ,เน็ทเวิร์กภายนอกวงแลนของบริษัท และส่วนของเน็ทเวิร์กที่ไว้สำหรับวางเมล์ และเว็บเซิร์ฟเวอร์ เพื่อให้บุคคลภายนอกสามรถเข้ามาดูเว็บเพจของบริษัทได้ในส่วนนี้มีชื่อเรียกว่า DMZ (De-military Zone) และทำการแบ่งแยกระบบเซิร์ฟเวอร์ที่ใช้งานภายในองค์กร ออกจากระบบเน็ทเวิร์กภายนอก
2. จากเน็ทเวิร์กภายในสามารถที่จะเข้าถึงเน็ทเวิร์กภายนอก และ DMZ ได้ทุกแอพพลิเคชั่น แต่เน็ทเวิร์กภายนอก และ DMZ ไม่สามารถที่จะเข้าถึงเน็ทเวิร์กภายในได้
3. ในส่วนของเมล์ และเว็บเซิร์ฟเวอร์ จะทำการเปิดเฉพาะพอร์ต หรือแอพพลิเคชั่นที่ใช้เท่านั้น นอกเหนือจากนี้จะทำการปิดด้วยไฟร์วอลล์ทั้งหมด
4. มีการนำพร็อกซี่เข้ามาช่วยในการเข้าใช้งานเว็บเพจในอินเทอร์เน็ทได้รวดเร็วยิ่งขึ้น
5. ทำการจำกัดการใช้งานของยูเซอร์ในเน็ทเวิร์กภายในให้สามารถใช้งานแอพลิเคชั่นในอินเทอร์เน็ทได้บางแอพพลิเคชั่นเท่านั้น ยกตัวอย่างเช่น ให้ยูเซอร์ในแผนกคอมพิวเตอร์สามารถที่ใช้แอพพลิเคชั่น FTP ได้ในขณะที่ในแผนกอื่นไม่สามารถใช้ได้ เป็นต้น
6. สามารถให้เน็ทเวิร์กภายสามารถใช้ Network Address Translator สำหรับการใช้งานอินเทอร์เน็ท แทนการใช้งานไอพีจริง ซึ่งมีอยู่จำกัด และไม่ปลอดภัย
7. การเลือกใช้เซิร์ฟเวอร์เพื่อทำระบบไฟร์วอลล์ต้องเป็นเซิร์ฟเวอร์มีแบรนด์ เช่น IBM , HP Compaq เป็นต้น และมีการรับประกันฮาร์แวร์ทุกชิ้นไม่น้อยกว่า 3 ปี โดยแบร์นนั้นเป็นผู้รับประกัน ถ้าเป็นอุปกรณ์สำหรับระบบไฟร์วอลล์โดยเฉพาะต้องรับประกันอย่างน้อย 1 ปี
8. การติดตั้งระบบไฟร์วอลล์ การคอนฟิกกูเรชั่น ตลอดจนการดูแลรักษาทั้งระบบไฟร์วอลล์และเครื่องเซิร์ฟเวอร์ เป็นหน้าที่ของบริษัทที่จ้างมาจากภายนอก
9. ซอฟแวร์ที่นำมาติดตั้งในการทำระบบไฟร์วอลล์ ถ้าเป็นซอฟแวร์ลิขสิทธิ์ จะต้องทำการจัดซื้อตามความเป็นจริง ตามลักษณะการใช้งาน
10. ระบบไฟร์วอลล์ที่นำมาใช้ในการติดตั้งสำหรับบริษัท เมอร์ค จำกัด ต้องประกอบด้วยอีเทอร์เน็ทพอร์ต จำนวน 3 พอร์ต เป็นอย่างน้อย

3.4 คุณสมบัติของระบบไฟร์วอลล์ที่บริษัท เมอร์ค จำกัด ต้องการ

1. เป็นระบบไฟร์วอลล์ที่ทำงานในแบบ Stateful inspector
2. สามารถรองรับการเชื่อมต่อสำหรับยูเซอร์ได้พร้อมกันประมาณ 100 ไอพี หรือประมาณ 50,000 การเชื่อมต่อ และสามารถทำการเพิ่มจำนวนไอพี หรือการเชื่อมต่อให้เพิ่มขึ้นได้ตามความต้องการ
3. สามารถรองรับการส่งข้อมูลในลักษณะของ Clear Text (Packet UPD size 1464 byte/Packet) ได้ความเร็วไม่ต่ำกว่า 300 Mbps
4. สามารถทำการกำหนดการใช้งานแอพพลิเคชั่น ให้กับผู้ใช้งานที่ใช้การเชื่อมต่อผ่านระบบไฟร์วอลล์ได้
5. สามารถรองรับการทำงานในส่วนของ Network Address Translator และ Port Address Translator รวมทั้งรองรับการอัพเกรดให้สามารถใช้งาน Virtual Private network ได้ทั้งแบบ Site-to-site และ Client-to-site
6. ระบบไฟร์วอลล์สามารถทำการแบ่งโซนเน็ทเวิร์กได้ เช่น สามารถแบ่งเป็น เน็ทเวิร์กอินไซด์ เน็ทเวิร์กเอาท์ไซด์ และ ดีเอ็มแซด ได้ และมีความสามารถในการเพิ่มพอร์ตอีเทอร์เน็ทเพื่อรองรับการเชื่อมต่อเข้ากับระบบไฟร์วอลล์ได้
7. สามารถทำงานรวมกับระบบการตรวจจับผู้บุกรุก System Log server และพร็อกซี่เซิร์ฟเวอร์
8. มีความสามารถรับรู้การโจมตีเครือข่ายแบบ DoS (Denial of Service) และสามารถดร็อปแพ็คเก็จที่มีปัญหาได้
9.

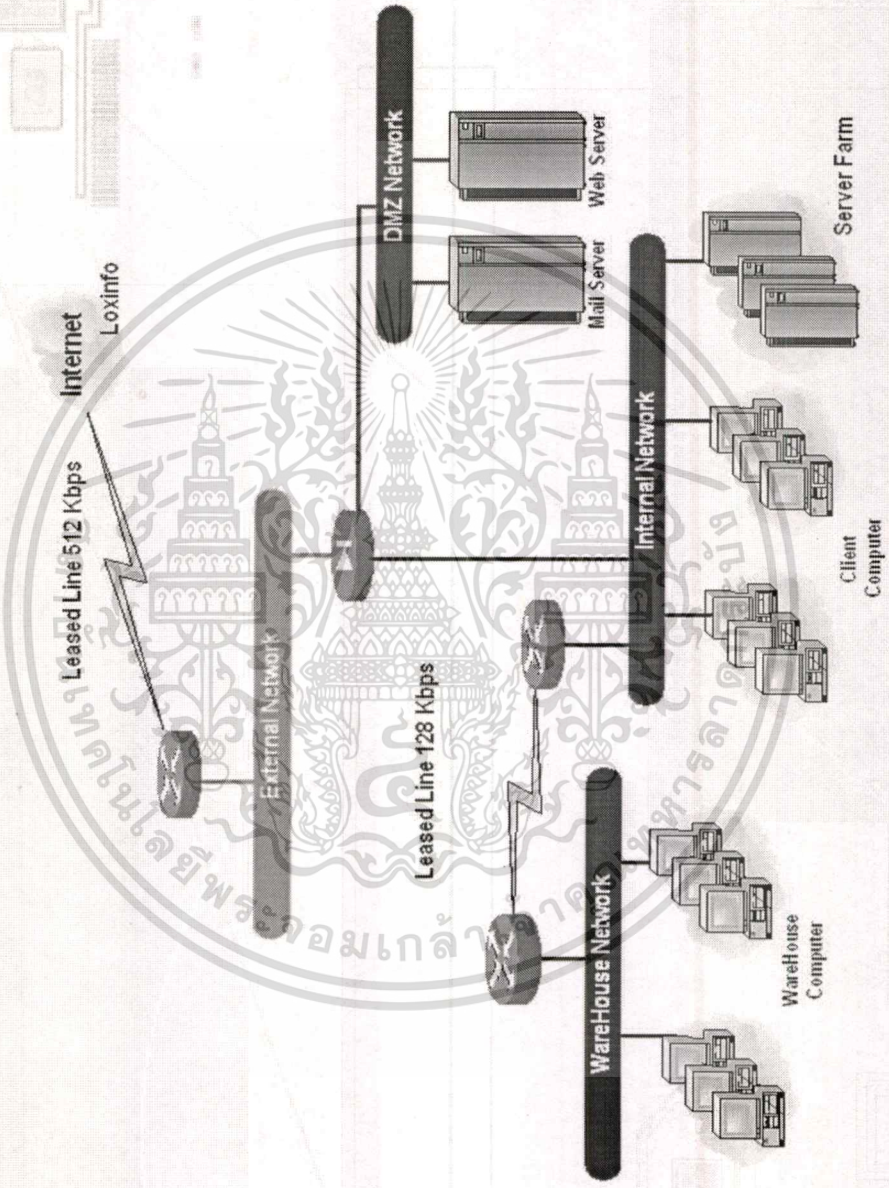
3.5 รูปแบบระบบเน็ทเวิร์กหลังจากติดตั้งระบบไฟร์วอลล์

เมื่อทำการติดตั้งระบบไฟร์วอลล์เข้าไปในเครือข่าย จะได้ผลลัพท์ดังรูปที่ 8 ที่มีการแบ่งเน็ทเวิร์กออกเป็น 3 ส่วน คือ Internal Netowork , Outside Network และ DMZ network อย่างชัดเจน

ซึ่งจากความต้องการของบริษัท เมอร์ค จำกัด ที่ต้องการแบ่งเน็ทเวิร์กออกเป็น 3 ส่วนแยกจากกันโดยอิสระ ในส่วนของ DMZ network ไม่สามารถเข้ามาใน Internal Network และในส่วนของเครื่องคอมพิวเตอร์ของยูเซอร์มีการนำ Network Address Translator เข้ามาใช้ โดยทำ

การติดตั้งผ่านระบบไฟร์วอลล์ และได้ทำการแยกระบบเซิร์ฟเวอร์ที่ใช้งานภายในออกจากเน็ทเวิร์กภายนอกด้วย

ในส่วนของเมล์ และเว็บ เซิร์ฟเวอร์ ได้นำไปไว้ใน DMZ network เพื่อสามารถจำกัดการเข้าถึง Internet Network ได้ ให้ผู้ที่เข้ามาใช้งานเมล์ และเว็บ เซิร์ฟเวอร์สามารถใช้งานได้เฉพาะในโซนนั้นๆ เท่านั้น ไม่สามารถข้ามเข้ามาใน Internet Nework ได้



รูปที่ 8 : แผนผังเครือข่ายภายในบริษัท เมอร์ค จำกัด หลังจากติดตั้งระบบไฟร์วอลล์

บทที่ 4
การวิเคราะห์ความเป็นไปได้ในการติดตั้งไฟร์วอลล์

จากที่ได้ทราบในความต้องการของบริษัท เมอร์ก จำกัด ในการนำระบบไฟร์วอลล์มาใช้ภายในองค์กรแล้ว ต่อจากนี้เป็นทางเลือกที่เป็นไปได้ของโซลูชั่นที่จะนำมาใช้

4.1 ทางเลือกที่เป็นไปได้ในการติดตั้งระบบไฟร์วอลล์ในบริษัท เมอร์ก จำกัด

จากความต้องการระบบไฟร์วอลล์ที่ได้กล่าวมาในบทที่ 3 นั้น สามารถนำมาสู่ทางเลือกที่เหมาะสมสำหรับเครือข่ายของบริษัท เมอร์ค จำกัด มีดังนี้

4.1.1 ทางเลือกที่ 1 : การติดตั้งระบบไฟร์วอลล์ในแบบโอเพ่นซอส

ระบบไฟร์วอลล์ในแบบโอเพนซอสนี้ประกอบกันด้วยระบบปฏิบัติการ Redhat Linux version 8.0 โดยใช้คู่กับ Netfilter IPTables ซึ่งเป็นโปรแกรมไฟล์วอลล์ที่มีความสามารถในการทำงานแบบ Stateful Inspector คือสามารถทำการควบคุมทราฟฟิคของระบบเน็ทเวิร์กได้ และสามารถที่จะจับดูสถานะของแพ็คเก็ตที่วิ่งผ่านตัวไฟร์วอลล์ไปได้

ในส่วนของการคอนฟิกคำสั่งต่างๆ สามารถทำได้โดยผ่านทางคอมมานไลน์ หรือสามารถทำการเขียนคำสั่งให้รันเป็นสคริปได้ และยังสามารถเขียนคำสั่งให้มีการสร้างล็อกไฟล์เพื่อไว้ใช้ในการตรวจสอบสถานการณ์ที่เกิดขึ้น เพื่อสามารถแก้ไขได้เมื่อมีปัญหาเกิดขึ้นได้

จุดเด่นของไฟร์วอลล์ในลักษณะนี้ มีความยืดหยุ่นในการเพิ่มประสิทธิภาพได้สูง เนื่องจากประสิทธิภาพในการทำงานจะแปรผันตามเครื่องคอมพิวเตอร์ที่ทำหน้าที่ในการทำงานร่วมกับระบบไฟร์วอลล์นั้น ซึ่งถ้าในอนาคตมีการใช้งานผ่านไฟร์วอลล์ตัวนี้มากขึ้น ก็ทำการอัพเกรดเพียงฮาร์ดแวร์ของเครื่องคอมพิวเตอร์ ก็จะสามารถเพิ่มประสิทธิภาพให้กับไฟร์วอลล์ได้

จุดด้อยของระบบนี้คือ ระบบปฏิบัติการที่ไฟร์วอลล์ทำการติดตั้งอยู่ เนื่องจากระบบปฏิบัติการทุกตัว จะมีช่องโหว่ซึ่งเป็นจุดที่สามารถถูกโจมตีได้ง่าย ต้องมีการติดตามและอัพเดทตัวระบบปฏิบัติการให้ทันสมัยอยู่เสมอจึงจะสามารถลดปัญหานี้ลงได้ ต่อมาฟีเจอร์ในส่วนของ IDS (Intrusion Detecsion system) ตัวนี้จะไม่มีมาให้ต้องทำการหาโปรแกรมเพื่อมาติดตั้งใช้งานในส่วนนี้เพิ่มเติม ซึ่งจากประสบการณ์ของผู้เขียนได้เคยใช้โปรแกรมชื่อ Snort มาทำเป็น

IDS server เพื่อเก็บล็อกการทำงานของไฟร์วอลล์ แต่รายงานออกมาเป็นลักษณะของเท็กซ์โหมดซึ่งยากต่อการทำความเข้าใจ ต้องให้ผู้ที่มีความรู้ความเข้าใจจึงสามารถทราบถึงความหมายของล็อกไฟล์นั้นๆ ในส่วนของการคอนฟิกต้องการผู้ที่มีความรู้และเข้าใจคำสั่งพารามิเตอร์ของคำสั่งได้อย่างดี มิฉะนั้นแล้วจะไม่สามารถทำการคอนฟิกในลักษณะที่ซับซ้อนได้ หรืออาจเกิดปัญหาในการคอนฟิก เนื่องจากไม่สามารถใช้พารามิเตอร์ที่ถูกต้องในการคอนฟิก จนอาจกลายเป็นช่องโหว่ในไฟร์วอลล์ทำให้สามารถเจาะเข้ามาได้ ในปัจจุบันได้มีการพัฒนาเครื่องมือในการคอนฟิก IPTables ในแบบ GUI mode มีชื่อเรียกว่า FWbuilder ซึ่งจากการทดลองใช้งานสามาถทำการสร้างสคริปสำหรับทำไฟร์วอลล์ได้เป็นอย่างดี และทำให้การคอนฟิกสะดวกยิ่งขึ้น

ระบบสำหรับการติดตั้งไฟร์วอลล์แบบโอเพ่นซอส มีการใช้เซิร์ฟเวอร์ของค่าย IBM ซึ่งมีสเปคของระบบ ดังนี้

Processor	:	Intel Pentium 4 2.4 GHz
Memory	:	256 MB DDR RAM
Storage Controller	:	ATA 133 IDE Controller
Harddisk	:	40 GB x 1 ATA 133
Network Card	:	Integrated 10/100/1000 Mbps Ethernet
		IBM Lan card x 2 card Fast Ethernet 10/100
Accessories	:	CD-ROM 48x , Floppy Disk 1.44 MB
Monitor	:	IBM 15" with Flat screen and Blackcolor
Warranty	:	3 years onsite service
Operating System	:	Redhat Linux Version 8.0
Firewall software	:	Netfilter IPTABLES
Clear Text Throughtput	:	400 Mbps
Concurrent connections	:	Unlimited

ในการเลือกใช้เซิร์ฟเวอร์ที่มีแบรนด์ เพื่อต้องการการรับประกันที่มีหลังจากการขายในส่วนของอะไหล่ต่างๆ ที่ถ้ามีปัญหาเกิดขึ้นสามารถทำการแก้ไข และเปลี่ยนได้อย่างทันเวลาไม่จำเป็นต้องรอขั้นตอนต่างๆ สามารถทำการแจ้งถึงอาการที่ผิดปรกติของฮาร์ดแวร์ และทางไอบีเอ็มจะตอบรับปัญหา และทำการแก้ไขได้อย่างรวดเร็ว

ระบบไฟร์วอลล์ในลักษณะนี้ต้องการผู้ดูแลที่มีความรู้ในระบบปฏิบัติการลินุกซ์เป็นอย่างดี และเข้าใจพื้นฐานการทำงานของระบบ บุคคลากรที่มีความรู้เกี่ยวกับลินุกซ์ยังมีอยู่น้อยเนื่องมาจากส่วนใหญ่จะคุ้นเคยกับระบบปฏิบัติการวินโดว์มากกว่า ทำให้ไม่สามารถใช้งานระบบปฏิบัติการลินุกซ์ได้อย่างเต็มที่ ซึ่งเป็นสาเหตุหนึ่งที่ทำให้การเลือกใช้ระบบปฏิบัติการลินุกซ์ทำเป็นเซิร์ฟเวอร์ที่สำคัญยังไม่เป็นที่แพร่หลาย เมื่อเกิดเหตุการณ์ในลักษณะนี้ขึ้นจึงต้องมีการจ้างให้outsource มาทำการติดตั้งและคอนฟิกให้โดยมีการทำสัญญาการบำรุงรักษาเป็นรายปี แล้วแต่ความต้องการ ซึ่งการบำรุงรักษาร่วมถึงการคอนฟิกเพิ่มเติม และแก้ไขปัญหาที่เกิดขึ้นกับระบบไฟร์วอลล์ด้วย

ในส่วนของการแบ็คอัพและกู้คืนระบบนั้น ระบบไฟร์วอลล์แบบนี้สามารถทำได้สะดวก โดยหลังจากที่มีการคอนฟิกทุกอย่างเรียบร้อยแล้ว ให้ทำการเก็บไฟล์ที่ใช้สำหรับคอนฟิกระบบทุกอย่างไว้ในอุปกรณ์เก็บข้อมูล เช่น ฟลอบบี้ ดิสก์ เป็นต้น และเมื่อระบบเกิดมีปัญหาเนื่องจากสิ่งใดก็ตาม สามารถสร้างระบบนั้นขึ้นมาใหม่ และยังสามารถใช้คอนฟิกอันเดิมที่เคยแบ็คอัพไว้มาใส่ แต่ข้อควรระวังคือควรมีการแบ็คอัพทุกครั้งที่มีการเปลี่ยนแปลงแก้ไขค่าต่างๆ เพื่อความทันสมัยของไฟร์วอลล์อยู่เสมอ

ในตารางที่ 1 ได้แสดงค่าใช้จ่ายเกิดขึ้นในกรณีของการติดตั้งระบบไฟร์วอลล์แบบโอเพ่นซอส ซึ่งสามารถแบ่งได้ดังนี้

1. ค่าติดตั้งฮาร์ดแวร์เริ่มต้น ได้ข้อมูลมาจากบริษัท เทค แปซิฟิก จำกัด
2. ค่าการติดตั้งระบบไฟร์วอลล์ และการดูแลรักษาระบบไฟร์วอลล์ ได้ข้อมูลมาจากบริษัท วีอาร์ โปรเฟสชันนัล จำกัด โดยในส่วนของการดูแลนี้ รวมไปถึงการมอนิเตอร์ระบบไฟร์วอลล์ผ่านทางระยะไกล และทำการปรับปรุงระบบให้ทันสมัยอยู่เสมอ รวมถึงการดูแลระบบให้สามารถดำเนินงานไปได้ รวมถึงการกู้คืนระบบภายในเวลาที่กำหนดไว้ ซึ่งสาเหตุอาจมาจากซอฟแวร์ได้
3. ค่าการบำรุงรักษาฮาร์ดแวร์ ซึ่งเป็นเซิร์ฟเวอร์ไอบีเอ็ม ได้ข้อมูลมาจากบริษัท เทค แปซิฟิก จำกัด ซึ่งจากตารางจะแสดงให้เห็นว่าค่าบำรุงรักษาฮาร์ดแวร์จะ

เริ่มในปีที่ 2 เนื่องจากด้วยการรับประกันของทางไอบีเอ็มรับประกันเซิร์ฟเวอร์ 1 ปี ทำให้ต้องทำการซื้อเป็นการประกันเสริมไปอีกครั้งละ 3 ปี ซึ่งในการซื้อการประกันเสริมจะได้สิทธิในการเรื่องของการมีอะไหล่สำรองให้และไม่มีการคิดค่าแรงตลอด 3 ปี ของช่วงการอยู่ในประกัน

ตารางที่ 1 : ตารางแสดงค่าใช้จ่ายในการติดตั้งระบบไฟร์วอลล์แบบโอเพ่นซอส **(หน่วย : บาท)**

ประเภทของค่าใช้จ่าย	ปีที่ 1	ปีที่ 2	ปีที่ 3	ปีที่ 4	ปีที่ 5	ปีที่ 6
ค่าใช้จ่ายทางด้านฮาร์ดแวร์เริ่มต้น	75,000.00	-	-	-	-	-
ค่าใช้จ่ายทางด้านซอฟแวร์						
ค่าลิขสิทธิ์สำหรับระบบปฏิบัติการ	-	-	-	-	-	-
ค่าลิขสิทธิ์สำหรับไฟร์วอลล์	-	-	-	-	-	-
ค่าติดตั้ง และคอนฟิกเริ่มต้น						
ค่าติดตั้งตัว IPTABLES	200,000.00	-	-	-	-	-
ค่าบำรุงรักษา						
ค่าการดูแลและปรับปรุงไฟร์วอลล์	-	100,000.00	100,000.00	100,000.00	100,000.00	100,000.00
ค่าบำรุงรักษาฮาร์ดแวร์	-	12,278.00	-	-	12,278.00	-
ค่าใช้จ่ายทั้งหมดรวมต่อปี	275,000.00	112,278.00	100,000.00	100,000.00	112,278.00	100,000.00
ค่าใช้จ่ายสะสม	275,000.00	387,278.00	487,278.00	587,278.00	699,556.00	799,556.00

4.1.2 ทางเลือกที่ 2 : การใช้ระบบไฟร์วอลล์ในแบบซอฟแวร์ลิขสิทธิ์ไฟร์วอลล์วัน บนระบบปฏิบัติการวินโดว์ 2000 เซิร์ฟเวอร์

เป็นระบบไฟร์วอลล์แบบ Statefull Inspector มีการติดตั้งที่ง่าย เหมือนกับการติดตั้งซอฟแวร์บนวินโดส์ และมียูสเซอร์อินเทอร์เฟสที่เข้าใจง่าย และมีส่วนของการช่วยเหลือที่สามารถเรียกดูได้ตลอด ส่วนใหญ่จะมีคู่มือสำหรับการใช้งานในฉบับย่อแนบมาพร้อมกับโปรแกรม

ในส่วนของการคอนฟิก เพื่อใช้งานมียูสเซอร์อินเทอร์เฟสที่มีการอำนวยความสะดวกด้วยเครื่องมือตัวช่วย (wizard) เพื่อทำการคอนฟิกแบบรวดเร็วหรือ เมื่อต้องการคอนฟิกเพียงแค่ใส่ข้อมูลให้ถูกต้องก็จะสามารถทำการคอนฟิกได้ตรงกับความต้องการ และมีความสะดวกในการเข้ามาดูจากระยะไกล ไม่จำเป็นต้องอยู่ที่หน้าเครื่อง โดยทำการดูผ่านทางเว็บแมนเนจเม็นท์ (web management) ได้ทำให้สะดวกต่อการแก้ไขปัญหาได้รวดเร็วยิ่งขึ้น และยังมีระบบการแจ้งเตือนผ่านทางการสื่อสารต่างๆ เช่น ผ่านทางระบบอีเมล์ เป็นต้น ทำให้สามารถทราบได้ถึงสถานการทำงานต่างๆ ของระบบได้อย่างทันเวลา และถูกต้อง

จุดเด่นของระบบไฟร์วอลล์ วัน มีความยืดหยุ่นในการทำงานสูง และประสิทธิภาพของระบบขึ้นอยู่กับเครื่องคอมพิวเตอร์ที่ติดตั้ง ถ้าต้องการให้ประสิทธิภาพสูงขึ้นก็เพียงแต่อัพเกรดฮาร์ดแวร์ให้มีประสิทธิภาพสูงขึ้น เช่น การเพิ่มเมโมรี่ให้มากขึ้น เป็นต้น อีกทั้งในส่วนของไฟร์วอลล์วัน ได้ทำการติดตั้งตัว IDS เอาไว้ภายในชุดซอฟแวร์แล้ว ซึ่งการรายงาน IDS ของไฟร์วอลล์วัน มีรูปแบบที่เข้าใจง่าย และมีการแสดงผลในรูปแบบกราฟฟิก เป็นรูปกราฟต่างๆ เพื่อให้สามารถดูความเป็นไปของระบบได้สะดวกขึ้น ซึ่งในส่วนนี้เป็นส่วนที่สำคัญส่วนหนึ่งที่ช่วยให้สามารถป้องกันปัญหาที่เกิดขึ้นได้ทันเวลา ในระบบของไฟร์วอลล์วันยังประกอบด้วยแพทเทิร์น (pattern)ไฟล์ที่บันทึกแพทเทิร์น (pattern)ของแพ็คเก็ตที่คาดว่าจะเป็น DoS ได้อยู่ในตัวอยู่แล้ว เมื่อมีการพบแพ็คเก็ตที่มีความเหมือนกับตัวแพทเทิร์นที่อยู่ก็จะทำการ ดร็อปแพ็คเก็ตนั้นทิ้งไป และไม่ให้ผ่านเข้ามาในเครือข่ายได้ ในส่วนของการอัพเดทความผิดพลาดของระบบมีการแก้ไขอยู่ตลอดเวลา และสามาถทการอัพเดทได้ โดยการดาวโลดน์ทางเว็บไซท์ของผู้ผลิตได้โดยตรง ซึ่งทำให้มั่นใจได้ว่าไฟร์วอลล์สามารถทำงานได้อย่างมีประสิทธิภาพ

จุดด้อยของไฟร์วอลล์วัน ระบบปฏิบัติการที่ติดตั้งตัวระบบไฟร์วอลล์วันต้องมีการติดตั้งที่รัดกุม และพยายามลดช่องโหว่ของระบบปฏิบัติการให้มากที่สุดโดยการติดตั้ง และอัพเดทให้ระบบปฏิบัติการทันสมัยอยู่เสมอ

เมื่อทำการติดตั้งระบบเรียบร้อยแล้วจำเป็นต้องมีผู้ดูแล คอยตรวจสอบการทำงานของระบบต่างๆ อยู่ตลอดเวลา ซึ่งในส่วนของไฟร์วอลล์วันมีการรับประกันหลังการขาย 1 ปี มีการเทรนนิ่ง และสามารถปรึกษาทางโทรศัพท์ได้โดยไม่ค่าใช้จ่าย ทำให้ผู้ดูแลระบบมีความเข้าใจในตัวอุปกรณ์มากขึ้น และสามารถใช้งานได้อย่างมีประสิทธิภาพ

ระบบสำหรับการติดตั้งไฟร์วอลล์แบบซอฟแวร์ลิขสิทธิ์ไฟร์วอลล์วัน บนระบบปฏิบัติการวินโดว์ 2000 เซิร์ฟเวอร์ มีดังนี้

Processor	:	Intel Pentium 4 2.4 GHz
Memory	:	256 MB DDR RAM
Storage Controller	:	ATA 133 IDE Controller
Harddisk	:	36.4 GB x 1 Hotswap (Ultra320)
Network Card	:	Integrated 10/100/1000 Mbps Ethernet
		IBM Lan card x 2 card Fast Ethernet 10/100
Accessories	:	CD-ROM 48x , Floppy Disk 1.44 MB
Monitor	:	IBM 15" with Flat screen and Blackcolor
Warranty	:	3 years onsite service for IBM server
Operating System	:	Windows 2000 server
Firewall software	:	Firewall-1 Internet-Gateway 100 IP
Clear Text Throughtput	:	400 Mbps
Concurrent connections	:	100 IP concurrent connections

ตารางที่ 2 แสดงค่าใช้จ่ายต่างๆ ที่เกิดขึ้นจากการติดตั้งระบบไฟร์วอลล์แบบไฟร์วอลล์วันไว้ดังนี้

1. ค่าใช้จ่ายเกี่ยวกับราคาของไฟร์วอลล์วัน ค่าการดูแลรักษา และค่าการ subscribe ไฟร์วอลล์วัน ได้รับข้อมูลมาจากบริษัท แวลลู ซิสเต็ม จำกัด จากตารางในส่วนของค่าการติดตั้งระบบไฟร์วอลล์วัน จะไม่มี เนื่องจากเป็นหลักการขายคือ ถ้าทำการซื้อสินค้ากับทางบริษัททางบริษัทผู้ขายจะไม่คิดค่าติดตั้งสำหรับระบบเริ่มแรกอยู่ แล้ว ส่วนในการดูแลรักษา การติดตามเฝ้าดูระบบและทำการแก้ไขให้ไฟร์วอลล์มีความทันสมัยอยู่เสมอ เป็นส่วนการให้บริการที่เสริมเข้ามาช่วยให้บริษัทผู้ติดตั้งระบบไม่ต้องรับภาระในการดูแลระบบมากนักสามารถทำการกู้ระบบได้ในกรณีที่ซอฟแวร์ไฟร์วอลล์วันเกิดมีปัญหา และไม่สามารถทำงานต่อได้
2. ถ้ามองในด้านของค่าใช้จ่ายในการฝึกอบรมนั้น ในกรณีของซอฟแวร์ไฟร์วอลล์วันมีการอบรมสำหรับผู้ใช้เป็นคอร์สอยู่แล้ว ไม่ต้องเสียค่าใช้จ่ายใดๆ ทั้งสิ้น
3. เครื่องเซิร์ฟเวอร์ไอบีเอ็ม ค่าการดูแลรักษาเซิร์ฟเวอร์ ค่าซอฟแวร์วินโดว์ 2000 เซิร์ฟเวอร์ได้ข้อมูลราคาจากบริษัท เทคแปซิฟิก จำกัด

ตารางที่ 2 : ตารางแสดงค่าใช้จ่ายในการติดตั้งระบบไฟร์วอลล์วันที่ติดตั้งบนวินโดว์ 2000 เซิร์ฟเวอร์ **(หน่วย : บาท)**

ประเภทของค่าใช้จ่าย	ปีที่ 1	ปีที่ 2	ปีที่ 3	ปีที่ 4	ปีที่ 5	ปีที่ 6
ค่าใช้จ่ายทางด้านฮาร์ดแวร์เริ่มต้น	75,000.00	-	-	-	-	-
ค่าใช้จ่ายทางด้านซอฟแวร์						
ค่าลิขสิทธิ์สำหรับระบบปฏิบัติการ	-	-	-	-	-	-
Microsoft Windows 2000 server	28,000.00	-	-	-	-	-
ค่าลิขสิทธิ์สำหรับไฟร์วอลล์	-	-	-	-	-	-
Firewall-1 limit to 100 Licence	508,800.00	-	-	-	-	-
ค่าติดตั้ง และคอนฟิกเริ่มต้น						
ค่าติดตั้ง Firewall-1	-	-	-	-	-	-
ค่าบำรุงรักษา						
ค่าการดูแลและปรับปรุงไฟร์วอลล์	-	100,000.00	100,000.00	100,000.00	100,000.00	100,000.00
ค่าบำรุงรักษาฮาร์ดแวร์	-	12,278.00	-	-	12,278.00	-
ค่าการ Subscrib Firewall-1 ต่อปี	-	101,800.00	101,800.00	101,800.00	101,800.00	101,800.00
ค่าใช้จ่ายทั้งหมดรวมต่อปี	611,800.00	214,078.00	201,800.00	201,800.00	214,078.00	201,800.00
ค่าใช้จ่ายสะสม	611,800.00	825,878.00	1,027,678.00	1,229,478.00	1,443,556.00	1,645,356.00

4.1.3 ทางเลือกที่ 3 : การใช้ระบบไฟร์วอลล์ในแบบซอฟแวร์ลิขสิทธิ์ไฟร์วอลล์วัน บนระบบปฏิบัติการแบบโอเพ่นซอส

ในส่วนของทางเลือกที่ 3 จะมีลักษณะการทำงานของระบบไฟร์วอลล์วันที่เหมือนกันกับการทำงานบนวินโดว์ ทุกประการ สิ่งที่แตกต่างกันคือ การระบบปฏิบัติการลินุกซ์ ซึ่งตามข้อตกลงของ GNU ซึ่งเป็นองค์กรที่ดูแลเกี่ยวกับการใช้งานโปรแกรมที่เป็นโอเพ่นซอสต่างๆ โดย Redhat มีลิขสิทธิ์เป็นส่วนหนึ่งใน GNU เช่นกัน ทำให้สามารถถือได้ว่า Redhat Linux เป็นซอฟแวร์ที่ถูกต้องตามลิขสิทธิ์

จากสเปคเครื่องทางด้านล่าง จะมีความเหมือนกับการติดตั้งระบบไฟร์วอลล์วันโดยใช้วินโดว์ 2000 ทุกประการ เพียงแต่แตกต่างกันที่ใช้ระบบปฏิบัติการที่แตกต่างกันคือ ใช้ Redhat linux 8.0 แทนตัวระบบปฏิบัติการวินโดว์ 2000 เท่านั้น

Processor	:	Intel Pentium 4 2.4 GHz
Memory	:	256 MB DDR RAM
Storage Controller	:	ATA 133 IDE Controller
Harddisk	:	40GB x 1 IDE ATA 133
Network Card	:	Integrated 10/100/1000 Mbps Ethernet IBM Lan card x 2 card Fast Ethernet 10/100
Accessories	:	CD-ROM 48x , Floppy Disk 1.44 MB
Monitor	:	IBM 15" with Flat screen and Blackcolor
Warranty	:	3 years onsite service
Operating System	:	Redhat Linux Version 8.0
Firewall software	:	Firewall-1 Internet-Gateway 100 IP
Clear Text Throughtput	:	400 Mbps
Concurrent connections	:	100 IP concurrent connections

ผลที่ได้รับจากการที่เลือกทำการติดตั้งระบบไฟร์วอลล์วันบนระบบปฏิบัติการ Redhat linux คือ ทำให้สามารถลดค่าใช้จ่ายในส่วนของลิขสิทธิ์ของระบบปฏิบัติการวินโดว์ 2000 ซึ่งสามารถทให้ประหยัดค่าใช้จ่ายในการติดตั้งในปีแรกลง

ในส่วนของประสิทธิภาพในการทำงานของระบบไฟร์วอลล์ไม่ได้ลดลง เนื่องจากไฟร์วอลล์วันถูกออกแบบมาให้สามารถใช้ได้กับระบบปฏิบัติการทั้งบนวินโดว์ และลินุกซ์ ทำให้ประสิทธิภาพในการทำงานของทั้งสองระบบมีความเท่าเทียมกัน แต่อาจแตกต่างกันทางด้านความจุดอ่อนของระบบปฏิบัติการ (OS vulnerability) ที่ในส่วนของระบบปฏิบัติการลินุกซ์ มีซอฟแวร์สำหรับทำการปิดช่องโหว่ๆ ต่างของระบบก่อนการติดตั้งระบบไฟร์วอลล์วัน แต่ในส่วนของวินโดว์ไม่มีซอฟแวร์สำเร็จรสำหรับกระทำการลักษณะนั้น จำเป็นที่ผู้ติดตั้งต้องทำการติดตั้งให้ปลอดภัยเอง ซึ่งทางไฟร์วอลล์วันมีเครื่องมือในการตรวจสอบระบบปฏิบัติการที่จะติดตั้งก่อนการติดตั้ง เพื่อทำการตรวจสอบสภาพของระบบปฏิบัติการว่ามีช่องโหว่หรือไม่ ถ้ามีจะต้องทำอย่างไรจึงจะปิดได้ เป็นต้น

ตารางที่ 3 แสดงค่าใช้จ่ายต่างๆ ที่เกิดขึ้นจากการติดตั้งระบบไฟร์วอลล์แบบไฟร์วอลล์วันที่ติดตั้งบนระบบปฏิบัติการโอเพ่นซอส ดังนี้

1. ค่าใช้จ่ายเกี่ยวกับราคาของไฟร์วอลล์วัน ค่าการดูแลรักษา และค่าการ subscribe ไฟร์วอลล์วัน ได้รับข้อมูลมาจากบริษัท แวลลู ซิสเต็ม จำกัด
2. เครื่องเซิร์ฟเวอร์ไอบีเอ็ม ค่าการดูแลรักษาเซิร์ฟเวอร์ ได้ข้อมูลราคาจากบริษัท เทคแปซิฟิก จำกัด

จากตารางที่ 3 จะแสดงให้เห็นว่าค่าใช้จ่ายสำหรับระบบปฏิบัติการลินุกซ์นั้นไม่มี แต่เป็นซอฟแวร์ที่ถูกต้องตามลิขสิทธิ์ทุกประการ

ตารางที่ 3 : ตารางแสดงค่าใช้จ่ายในการติดตั้งระบบไฟร์วอลล์วันที่ติดตั้งบนระบบปฏิบัติการลินุกซ์ **(หน่วย : บาท)**

ประเภทของค่าใช้จ่าย	ปีที่ 1	ปีที่ 2	ปีที่ 3	ปีที่ 4	ปีที่ 5	ปีที่ 6
ค่าใช้จ่ายทางด้านฮาร์ดแวร์เริ่มต้น	75,000.00	-	-	-	-	-
ค่าใช้จ่ายทางด้านซอฟแวร์						
ค่าลิขสิทธิ์สำหรับระบบปฏิบัติการ	-	-	-	-	-	-
Redhat Linux 8.0	-	-	-	-	-	-
ค่าลิขสิทธิ์สำหรับไฟร์วอลล์	-	-	-	-	-	-
Firewall-1 limit to 100 Licence	508,800.00	-	-	-	-	-
ค่าติดตั้ง และคอนฟิกเริ่มต้น						
ค่าติดตั้ง Firewall-1	-	-	-	-	-	-
ค่าบำรุงรักษา						
ค่าการดูแลและปรับปรุงไฟร์วอลล์	-	100,000.00	100,000.00	100,000.00	100,000.00	100,000.00
ค่าบำรุงรักษาฮาร์ดแวร์	-	12,278.00	-	-	12,278.00	-
ค่าการ Subscrib Firewall-1 ต่อปี	-	101,800.00	101,800.00	101,800.00	101,800.00	101,800.00
ค่าใช้จ่ายทั้งหมดรวมต่อปี	583,800.00	214,078.00	201,800.00	201,800.00	214,078.00	201,800.00
ค่าใช้จ่ายสะสม	583,800.00	797,878.00	999,678.00	1,201,478.00	1,415,556.00	1,617,356.00

4.1.4 ทางเลือกที่ 4 : การติดตั้งระบบไฟร์วอลล์ในแบบฮาร์ดแวร์

Cisco PIX firewall เป็นไฟร์วอลล์ที่ทำงานในลักษณะของ Stateful Inspector ที่เป็นฮาร์ดแวร์ ซึ่งใช้ระบบปฏิบัติการของทาง ซิสโก้เอง ที่ถูกพัฒนาขึ้นเพื่อวัตถุประสงค์ในการทำงานเป็นไฟร์วอลล์โดยเฉพาะ การติดตั้งทำได้โดยง่ายเนื่องจากไม่ต้องการอุปกรณ์ในการติดตั้งหลายอย่างเหมือนกับเครื่องคอมพิวเตอร์ นอกจากตัว PIX เองเท่านั้น

ในส่วนของการคอนฟิกเป็นลักษณะของคอมมานไลน์ในการคอนฟิก หรือสามารถคอนฟิกผ่าน PDM (PIX Device Management) ซึ่งนำเสนอการคอนฟิกไฟล์วอลล์โดยผ่านตัวเว็บเบส ซึ่งจะคล้ายกับตัว เว็บแมนเนจเมนท์ของไฟร์วอลล์วัน สามารถที่จะทำการคอนฟิกจากระยะไกลได้

จุดเด่นของระบบไฟร์วอลล์ PIX อยู่ที่ความมีเสรียรภาพในการทำงานที่สูง มีประสิทธิภาพและความสามารถในการรองรับภาระงานหนักๆ ได้ เนื่องมาจาก PIX ถูกออกแบบมาเพื่อทำงานเฉพาะอย่างใดอย่างหนึ่งเท่านั้น

ในส่วนของซอฟแวร์ที่ติดตั้งอยู่ภายในตัว PIX นั้นถูกเขียนขึ้นเพื่อใช้สำหรับติดตั้งให้คอมแพทเทเบิ้ลกับอุปกรณ์ทุกตัวที่ประกอบกันเป็นกล่อง ทำให้สามารถดึงเอาประสิทธิภาพของฮาร์ดแวร์ออกมาได้อย่างเต็มที่ และทำให้ลดช่องโหว่ที่อาจเกิดขึ้นจากการใช้ระบบปฏิบัติการที่ใช้งานทั่วไป ทำให้ลดปัญหาเรื่องช่องโหว่ของระบบปฏิบัติการไปได้ ซึ่งถ้าเปรียบเทียบกับ 2 ทางเลือกที่ผ่านมา จำเป็นต้องมีระบบปฏิบัติการในการรองรับการทำงานเสียก่อน จึงจะสามารถใช้งานได้

จุดด้อยของ PIX จะอยู่การที่ฮาร์ดแวร์ไม่มีความยืดหยุ่นในการอัพเกรดไปใช้ในระบบที่ใหญ่กว่า ไม่สามารถอัพเกรดสิ่งใดได้นอกจากเมโมรี เมโมรีแฟลช และ อินเทอร์เฟสการ์ด เท่านั้น ถ้าต้องการอัพเกรดความเร็วของโปรเซสเซอร์ก็ไม่สามารถทำได้ และในส่วนของฮาร์ดแวร์อีกเช่นกันถ้ามีปัญหาจำเป็นต้องใช้สแปร์พาร์ทที่เป็นของซิสโก้ เท่านั้น จึงทำให้เกิดปัญหาถ้าใช้ไปเป็นเวลานานจนรุ่นนั้นเลิกผลิตไปแล้วจะทำให้หาอะไหล่เพื่อทำการอัพเกรดหรือซ่อมได้ยาก นอกจากเปลี่ยนตัวใหม่เลย และประการสุดท้ายด้วยฮาร์ดแวร์ที่จำกัดอาจทำให้ PIX ไม่สามารถใช้งานได้ดีเท่าที่ควรเนื่องจากซอฟแวร์บางอย่างจำเป็นต้องใช้แรงของโปรเซสเซอร์มากทำให้อาจจะไม่สามารถใช้งานซอฟแวร์ที่ต้องการนั้นได้ ต้องทำการเปลี่ยนรุ่น ของอุปกรณ์ไป ทำให้ต้องเสียเงินเพิ่มขึ้นอีก

ระบบสำหรับการติดตั้งไฟร์วอลล์ฮาร์ดแวร์เฉพาะ ใช้ Cisco Pix 525R-BUN ซึ่งมีสเปคดังนี้

Processor	:	Intel Pentium III 600 MHz
Memory	:	SDRAM 128 MB
Flash Memory	:	16 MB
System bus	:	32 bit PCI with 33 MHz
Network Card	:	Buildin 2 port fastEthernet 10/100 Pix-1FE x 1 (Ethernet card for Extend Fast ethernet port)
Warranty	:	1 year
Operating System	:	IOS by Cisco
Firewall System	:	IOS by Cisco
Clear Text Throughtput	:	330 Mbps
Concurrent connections	:	280,000 concurrent connection

เมื่อทำการติดตั้ง PIX เรียบร้อยแล้ว จำเป็นต้องมีผู้ดูแลคอยตรวจดูการทำงานของ PIX อยู่ตลอดเวลา เนื่องจากตัว PIX ไม่ได้มี IDS ในตัวทำให้เกิดปัญหาในการดูสถานภาพการทำงาน ผู้ดูแลระบบจำเป็นต้องนำระบบการตรวจจับล็อกไฟล์ของ PIX อย่างเช่น Syslogd ในระบบปฏิบัติการลินุกซ์ เป็นต้น เพื่อทำการเก็บล็อกที่ได้มาวิเคราะห์เพื่อช่องว่างที่ยังเกิดขึ้นอยู่ ในการนี้บุคลากรที่ดูแลทางด้านนี้จำเป็นต้องหาความรู้ทางด้านเน็ทเวิร์กอยู่เสมอ เพื่อให้ทันกับความเปลี่ยนแปลงของเครือข่ายที่เปลี่ยนไป

ในเรื่องของการกู้กลับคืนคอนฟิกสามาถทำได้ง่ายเนื่องจาก ผู้ดูแลควรมีการเก็บไฟล์คอนฟิกที่อัพเดทล่าสุดไว้ตลอด เมื่อมีปัญหาใดๆ กับอุปกรณ์ก็จะสามารถทำการคอนฟิกใหม่ได้อย่างง่ายดาย และควรมีระยะเวลาการเปลี่ยนพาสเวิร์ดในการเข้าสู่ระบบ เพื่อป้องกันการเข้าไปคอนฟิกภายในโดยไม่ได้รับอนุญาต ซึ่งก่อให้เกิดความเสียหายได้

หลังจากที่ได้ทำทุกอย่างเรียบร้อยแล้วโดยส่วนใหญ่ความเสียหายทางด้านฮาร์ดแวร์จนมีปัญหา เป็นสิ่งที่เกิดขึ้นน้อยมากสำหรับ PIX นอกจากจะมีปัญหาทางด้านซอฟแวร์อย่างเดียว ซึ่งต้องมีการอัพเกรด ในที่นี้ทางซิสโก้มีบริการไฟล์ให้สามารถดาวน์โลดมาอัพเกรดได้ หรือสามารถติดต่อ

กับผู้ขายให้อัพเกรดให้ได้ เพราะในส่วนของ smart net ที่ซื้อไปนั้นได้ร่วมส่วนนี้เข้าไปด้วยแล้ว ถ้ามีปัญหาทางด้านฮาร์ดแวร์ซิสโก้จะทำการแก้ไขให้ แต่ทั้งนี้ผู้ดูแลระบบจำเป็นต้องทราบด้วยว่า PIX มีปัญหาอะไรหรือไม่ โดยการตรวจสอบการทำงานของ PIX บ้าง

ตารางที่ 4 แสดงค่าใช้จ่ายในการติดตั้งระบบ Cisco PIX firewall ไว้ดังนี้

1. ค่าใช้จ่ายในการติดตั้งฮาร์ดแวร์เริ่มต้น และค่าบำรุงรักษา ได้ข้อมูลมาจากบริษัท ซินเน็ค (ประเทศไทย) จำกัด
2. ค่าใช้จ่ายในการดูแลระบบไฟร์วอลล์ รวมถึงการทำมอนิเตอร์ตัวไฟร์วอลล์ ได้ข้อมูลจากบริษัท วีอาร์ โปรเฟสชันนัล จำกัด
3. ค่าติดตั้งระบบไฟร์วอลล์ จะทำการติดตั้งให้ฟรี เนื่องจากได้ซื้อของจากทางบริษัทผู้ขาย จึงทำการติดตั้งให้ฟรี

ตารางที่ 4 : ตารางแสดงค่าใช้จ่ายในการติดตั้งระบบไฟร์วอลล์วันที่ติดตั้งบนระบบปฏิบัติการลินุกซ์ **(หน่วย : บาท)**

ประเภทของค่าใช้จ่าย	ปีที่ 1	ปีที่ 2	ปีที่ 3	ปีที่ 4	ปีที่ 5	ปีที่ 6
ค่าใช้จ่ายทางด้านฮาร์ดแวร์เริ่มต้น	428,500.00	-	-	-	-	-
ค่าใช้จ่ายทางด้านซอฟแวร์						
ค่าลิขสิทธิ์สำหรับระบบปฏิบัติการ	-	-	-	-	-	-
ค่าลิขสิทธิ์สำหรับไฟร์วอลล์	-	-	-	-	-	-
ค่าติดตั้ง และคอนฟิกเริ่มต้น						
ค่าติดตั้งตัว PIX	-	-	-	-	-	-
ค่าบำรุงรักษา						
ค่าการดูแลและปรับปรุงไฟร์วอลล์	-	120,000.00	120,000.00	120,000.00	120,000.00	120,000.00
ค่าบำรุงรักษาฮาร์ดแวร์	-	24,730.00	24,730.00	24,730.00	24,730.00	24,730.00
ค่าใช้จ่ายทั้งหมดรวมต่อปี	428,500.00	144,730.00	144,730.00	144,730.00	144,730.00	144,730.00
ค่าใช้จ่ายสะสม	428,500.00	573,230.00	717,960.00	862,690.00	1,007,420.00	1,152,150.00

4.2 การวิเคราะห์ความเป็นไปได้ทางด้านเทคนิค

เป็นการวิเคราะห์ความเป็นไปได้ทางด้านเทคนิค โดยประเด็นที่นำมาใช้ในการวิเคราะห์มีดังนี้

1. ความมีเสถียรภาพในการทำงาน ในประเด็นนี้มองถึงความสามารถในการรองรับการทำงานที่มีปริมาณการเชื่อมต่อมากทั้งขาเข้า และขาออกของระบบเครือข่าย และความสามารถในการรองรับการโจมตีที่รุนแรง เช่น การใช้ Ping of Dead หรือ SYN Flood ที่มาจากการทำ DoS ได้ด้วย
2. ความยืดหยุ่นในการใช้งาน ในประเด็นนี้มองในมุมมองของการเพิ่มความสามารถให้กับระบบ เช่น สามารถเพิ่มอีเทอร์เน็ทพอร์ต ได้อีกกี่พอร์ต ความสามารถในการเพิ่มเมมโมรี่ให้กับระบบ หรือ แม้กระทั่งการเพิ่มความสามารถให้กับระบบ เช่น การติดตั้งระบบ VPN ลงในระบบไฟร์วอลล์ เป็นต้น
3. ประสิทธิภาพในการทำงาน ในประเด็นนี้สามารถวัดได้จากค่าของ Clear Text Throughtput ที่ไฟร์วออล์แต่ละตัวสามารถทำได้
4. ความสามารถในการรองรับการคอนฟิกกูเรชั่นที่ซับซ้อน ในประเด็นนี้มองทางด้านความสามารถของตัวคอมมานต่างๆ ที่มีมาให้ในระบบไฟร์วอลล์ สามารถทำให้ระบบไฟร์วอลล์สามารถทำงานที่มีความซับซ้อนสูงๆ ได้หรือไม่ เช่น การทำ Port Address Translator ที่ต้องอาศัยความสามารถของตัวระบบไฟร์วอลล์ จึงจะสามารถทำได้ หรือการป้องกันการใช้งานในบางแอพพลิเคชั่นที่มีใช้งานทางอินเทอร์เน็ท เป็นต้น
5. การอัพเดท และแก้ไขข้อผิดพลาดของระบบไฟร์วอลล์ ในประเด็นนี้มองในเรื่องของการอัพเดท และแก้ไขข้อผิดพลาดอันเกิดจาก บักในซอฟแวร์ไฟร์วอลล์นั้น หรือ การอัพเดทให้สามารถใช้งานคำสั่งใหม่ๆได้ เป็นต้น
6. การสนับสนุนหลังการขาย ในที่นี้จะมองในเรื่องของการสนับสนุนของตัวโปรดักส์ของแต่ผู้ผลิต เช่น ในส่วนของไฟร์วอลล์วัน และ ซิสโก้ พิก สามารถโทรถามเทคนิคอล ซัพพอร์ต ในตอนที่เกิดมีปัญหาเกิดขึ้น แต่ถ้าเป็นไอพีเทเบิ้ล นั้นไม่มีการสนับสนุนในลักษณะนี้ เป็นต้น
7.

โดยการวิเคราะห์ในด้านเทคนิคจะทำการให้เป็นระดับคะแนนในแต่ละหัวข้อของการพิจารณาโดยโคมีระดับคะแนนในการพิจารณา ตั้งแต่ 0 ถึง 10 โดยที่ 0 หมายถึงแย่มาก และเรียงตามลำดับ 10 คือดีที่สุด โดยได้แสดงไว้ในตารางที่ 5

ตารางที่ 5 : ตารางแสดงระดับคะแนนสำหรับทางเลือกในการติดตั้งระบบไฟร์วอลล์

ระบบไฟร์วอลล์ / ประเด็น	ระบบไฟร์วอลล์ไอพีเทเบิ้ล	ระบบไฟร์วอลล์ไฟร์วอลล์วัน กับวินโดว์ 2000 เซิร์ฟเวอร์	ระบบไฟร์วอลล์ไฟร์วอลล์วน กับเรดแฮท ลินุกซ์ เวอร์ชั่น 8	ระบบไฟร์วอลล์ซิสโก้ พิกไฟร์วอลล์
เสถียรภาพการทำงานของระบบ	8	8	8	10
ความยืดหยุ่นในการทำงานของระบบ	10	10	10	5
ประสิทธิภาพการทำงานของระบบ	10	10	10	9
การอัพเดท และแก้ไขข้อผิดพลาดของระบบ	7	10	10	8
การสนับสนุนทางด้านเทคนิค	5	10	10	10
คะแนนรวม	**40**	**48**	**48**	**42**

จากระดับคะแนนที่ได้สามารถสรุปการวิเคราะห์ทางด้านเทคนิคได้ คือระบบไฟร์วอลล์วันที่ติดตั้งบนวินโดว์ 2000 และ เรดแฮทลินุกซ์มีคะแนนที่สูงที่สุดในระบบไฟร์วอลล์ที่นำมาเปรียบเทียบกัน

จากการวิเคราะห์ทางด้านเทคนิคตัวระบบไฟร์วอลล์ที่ติดตั้งโดยใช้ระบบไฟร์วอลล์วันทั้งในแบบของวินโดว์ 2000 เซิร์ฟเวอร์ และ เรดแฮทลินุกซ์ มีความสามารถตรงตามประเด็นที่ใช้ในการวิเคราะห์มากที่สุด คือระบบมีทั้งความเสถียรภาพการทำงานของระบบที่ดี มีความยืดหยุ่นในการทำงานสูง ประสิทธิภาพของระบบที่วัดจาก Clear Text Throughput นั้นมีค่าสูง การอัพเดทและแก้ไขข้อผิดพลาดมีการทำอย่างสม่ำเสมอ และมีการสนับสนุนทางด้านเทคนิคที่ดี

ส่วนระบบไฟร์วอลล์ที่ได้คะแนนรองลงมาคือระบบไฟร์วอลล์ ซิสโก้พิก จากระดับคะแนนจะแสดงให้เห็นว่า ซิสโก้พิก นี้มีจุดด้อยอยู่ในเรื่องของความยืดหยุ่นในการทำงาน เนื่องจากซิสโก้พิก เป็นระบบไฟร์วอลล์ที่มีการออกแบบมาเฉพาะทำงานอย่างใดอย่างหนึ่ง ทำให้ไม่สามารถเพิ่มความสามารถแบบอื่นๆ เข้าไปได้ และในส่วนของการเพิ่มความสามารถทางด้านฮาร์ดแวร์ที่มีอยู่อย่างจำกัด ทำให้ไม่สามารถทำการเพิ่มความสามารถของระบบได้ดีเท่ากับไฟร์วอลล์ที่นำเครื่องเซิร์ฟเวอร์ทั่วไปมาทำ แต่ในส่วนที่ซิสโก้พิกสามารถทำคะแนนได้ดีคือเสถียรภาพในการทำงานและการสนับสนุนทางด้านเทคนิค ซึ่งทั้ง 2 ประเด็นนี้ส่งผลทำให้ซิสโก้พิกเป็นไฟร์วอลล์ที่มีคนนิยมใช้กันมาก ด้วยการออกแบบซอฟแวร์ที่มีความเฉพาะทาง การสนับสนุนในเรื่องการแก้ไขปัญหาดีมาก ทำให้ถ้าดูจากระดับคะแนน ทำให้ซิสโก้พิดมีความโดดเด่นมากขึ้น

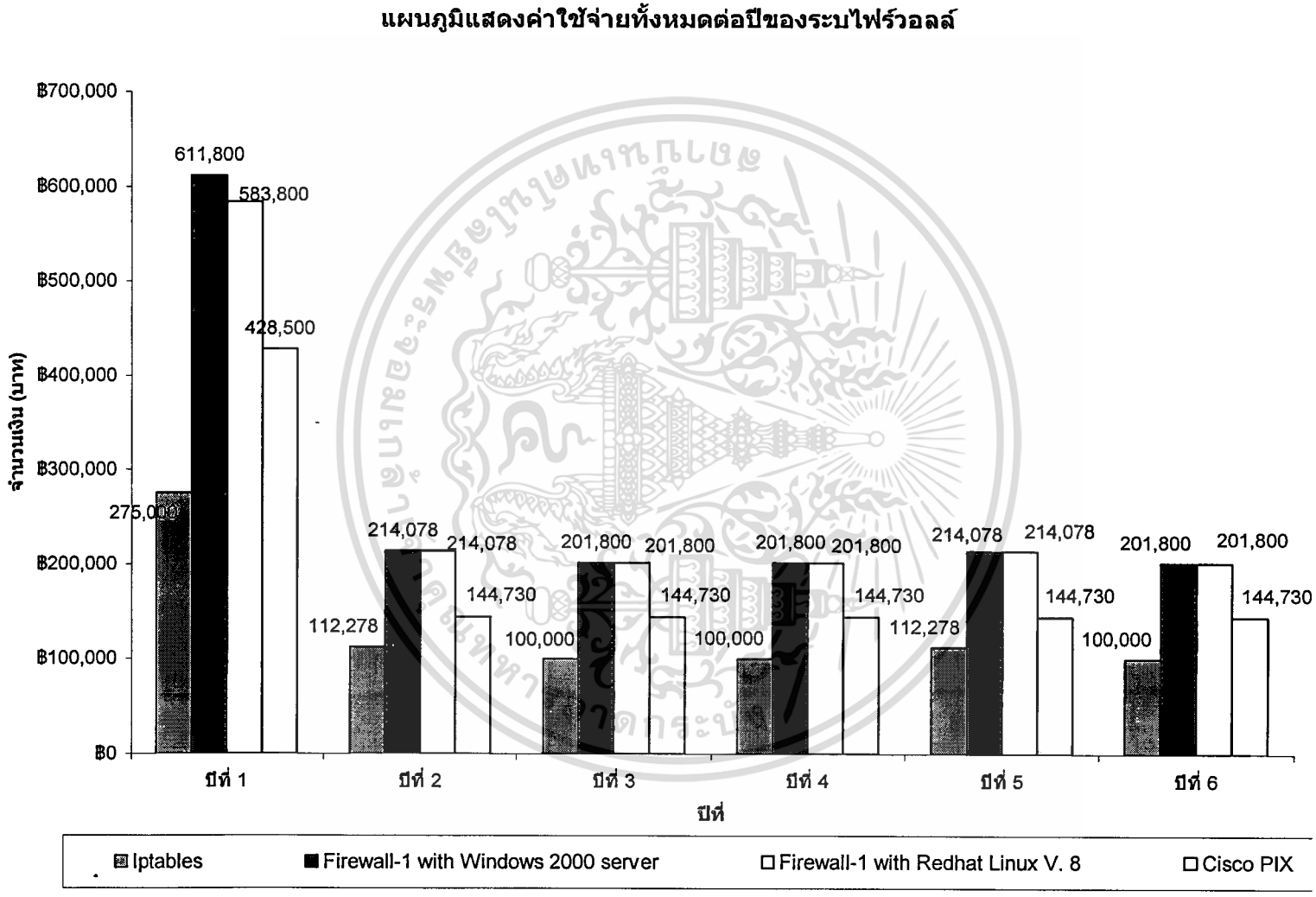
ระบบไฟร์วอลล์ที่ทำการพัฒนาโดยให้ไอพีเทเบิ้ลนั้น ได้คะแนนในส่วนของการอัพเดทและแก้ไขข้อผิดพลาด และการสนับสนุนทางด้านเทคนิค เนื่องจากไอพีเทเบิ้ลเป็นฟรีแวร์ โอเพ่นซอส อาจทำให้ไม่มีการพัฒนาอย่างจริงจัง เท่ากับตัวที่เป็นซอฟแวร์ทางธุรกิจ เช่น ไฟร์วอลล์วัน ทำให้ ใน 2 ด้านนี้ของไอพีเทเบิ้ลไม่สามาถทำคะแนนให้สูงเท่ากับอีก 2โซลูชั่นได้

4.3 การวิเคราะห์ความเป็นไปได้ทางด้านค่าใช้จ่าย

ประเด็นในการประมาณการด้านค่าใช้จ่ายที่ จะเกิดขึ้น ที่จะต้องพิจารณาในแต่ละทางเลือกมีดังนี้

- ค่าใช้จ่ายลงทุนทั้งหมด ซึ่งประกอบด้วย
    - ค่าใช้จ่ายในการติดตั้งซอฟแวร์ ค่าลิขสิทธิ์ที่ต้องเสียให้กับเจ้าของซอฟแวร์
    - ค่าอุปกรณ์ที่ใช้ในการติดตั้งระบบเริ่มต้น เช่น ค่าอุปกรณ์ไฟร์วอลล์ เครื่องเซิร์ฟเวอร์ เป็นต้น
    - ค่าดูแลรักษา และอัพเดทระบบไฟร์วอลล์ให้ทันสมัยอยู่เสมอ
    - ค่าใช้จ่ายในการบำรุงรักษาฮาร์ดแวร์

โดยสามารถทำการเปรียบเทียบค่าใช้จ่ายทั้งหมดดังรูปที่ 9



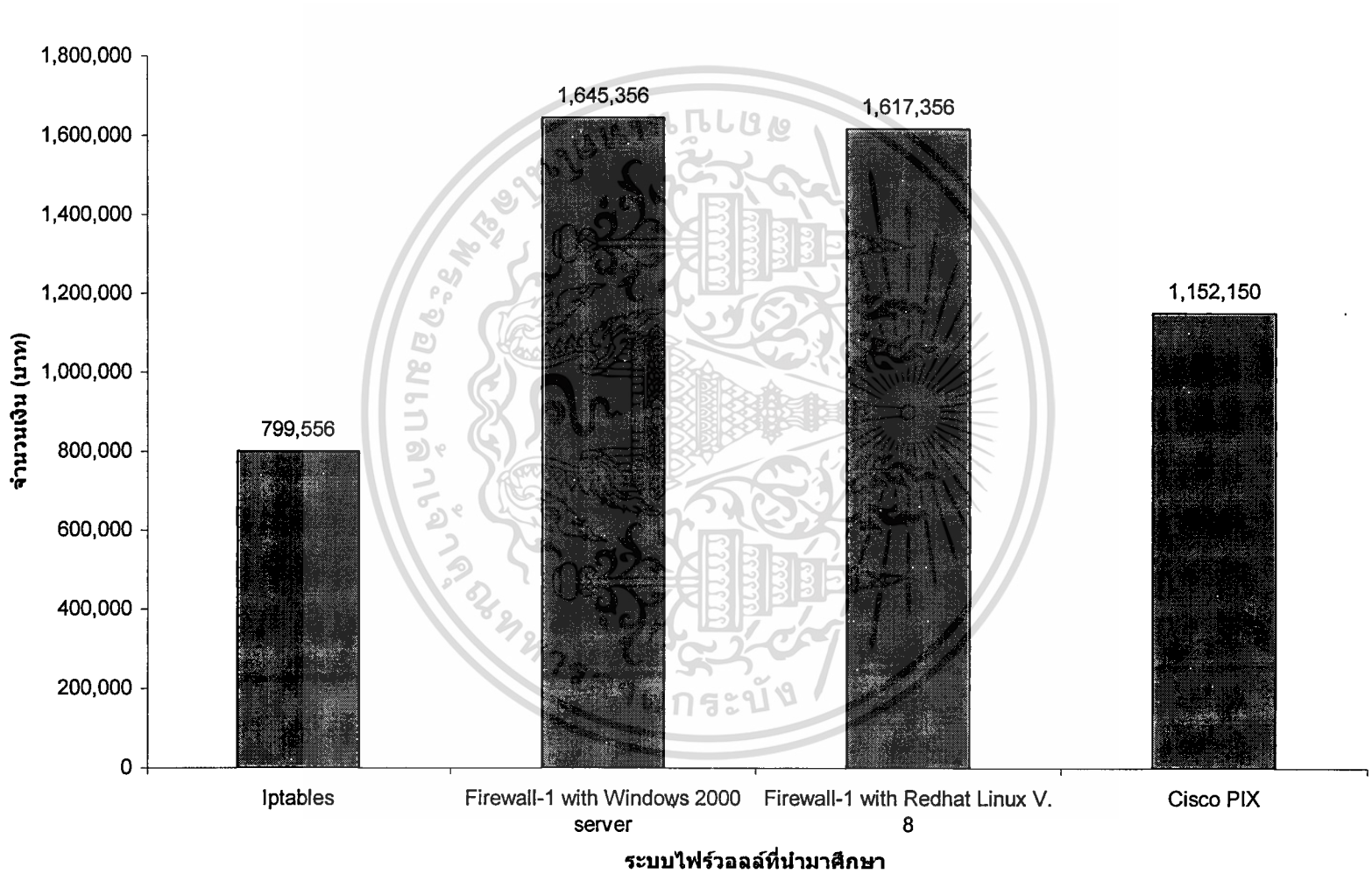
รูปที่ 9 : แผนภูมิแสดงค่าใช้จ่ายทั้งหมดต่อปีของระบบไฟร์วอลล์ที่ทำการศึกษา

จากรูปที่ 9 แผนภูมิแสดงค่าใช้จ่ายทั้งหมดต่อปีของระบบไฟร์วอลล์ที่นำมาศึกษานั้น ระบบไฟร์วอลล์ที่มีค่าใช้จ่ายทั้งหมดต่อปีต่ำที่สุดคือ ระบบไฟร์วอลล์ที่ติดตั้งโดยใช้ไอพีเทเบิ้ล ซึ่งในปีแรกมีค่าใช้จ่ายอยู่ที่ 275,000 บาท ในปีต่อๆ มาซึ่งได้ทำการติดตั้งระบบเรียบร้อยในปีแรก ปีที่ต่อมาจะเหลือเพียงค่าใช้จ่ายที่เป็นค่าบำรุงรักษาไฟร์วอลล์ และค่าบำรุงรักษาเซิร์ฟเวอร์ ซึ่งในส่วนของค่าบำรุงรักษาเซิร์ฟเวอร์นั้นจะจ่ายทุกๆ 3 ปี มิได้จ่ายทุกปี ทำให้ค่าใช้จ่ายในปีที่ 3 จะน้อยลง และมาเพิ่มอีกในปีที่ 5 ที่ต้องมีการต่ออายุการรับประกันตัวฮาร์ดแวร์เซิร์ฟเวอร์ออกไปอีก

จากรูปแสดงให้เห็นว่าไฟร์วอลล์วัน เป็นไฟร์วอลล์ที่มีค่าใช้จ่ายต่อปีสูงที่สุด เนื่องมาจากนอกค่าใช้จ่ายเริ่มต้นในเรื่องของค่าลิขสิทธิ์ที่สูงแล้ว ทุกๆปีจะต้องทำการ Subscrib ซอฟแวร์ทุกปี นอกเหนือจากค่าใช้จ่ายในเรื่องการบำรุงรักษาไฟร์วอลล์ และฮาร์ดแวร์ ทำให้ค่าใช้จ่ายทั้งหมดต่อปีมีมูลค่าสูงกว่าโซลูชั่นอื่นๆ

- **ค่าใช้จ่ายสะสมตลอด 6 ปี**

  ค่าใช้จ่ายสะสมตลอด 6 ปี สามารถแสดงเป็นแผนภูมิได้ดังรูปที่ 10



รูปที่ 10 : แผนภูมิแสดงค่าใช้จ่ายสะสมจำนวน 6ปีของระบบไฟร์วอลล์ที่นำมาศึกษา

จากรูปที่ 10 แผนภาพแสดงค่าใช้จ่ายสะสมจำนวน 6 ปี ของระบบไฟร์วอลล์ที่นำมาศึกษานั้นจะเห็นได้ว่าระบบไฟร์วอลล์ไอพีเทเบิ้ลมีค่าใช้จ่ายสะสมต่ำที่สุด และระบบไฟร์วอลล์วันเป็นระบบที่มีค่าใช้จ่ายสะสมสูงที่สุด แต่ถ้าเปรียบเทียบกันระหว่างไฟร์วอลล์วัน 2 ระบบทั้งวินโดว์ 2000 เซิร์ฟเวอร์ และเรดแฮทลินุกซ์แล้ว ในส่วนของเรดแฮทลินุกซ์มีค่าใช้จ่ายที่ถูกว่าอยู่เล็กน้อย อาจเนื่องมากจากการไม่ต้องเสียค่าลิขสิทธิ์เหมือนของวินโดซ์ 2000 เซิร์ฟเวอร์ ทำให้ค่าใช้จ่ายสะสมมีค่าที่ต่ำกว่า แต่ถ้าเปรียบเทียบกับไฟร์วอลล์แบบอื่นแล้วถือว่าแพงกว่ามาก ซึ่งเนื่องมาจากการมีค่า Subscribe ซอฟแวร์เข้ามาเกี่ยวข้องและเป็นค่าใช้จ่ายที่เกิดขึ้นทุกปี ทำให้ค่าใช้จ่ายสะสมจะมากกว่าในส่วนของไฟร์วอลล์ระบบอื่น อยู่มาก

บทที่ 5
สรุป และเสนอแนะ

5.1 สรุป

รายงานฉบับนี้ได้ทำการศึกษาถึงลักษณะของไฟร์วอลล์ที่มีความเหมาะสมต่อเน็ทเวิร์คของบริษัท เมอร์ค จำกัด โดยจากการศึกษาพบว่าไฟร์วอลล์ทั้ง 3 แบบที่ได้ทำการศึกษามีความโดดเด่นในลักษณะที่แตกต่างกันไป ไม่ว่าจะเป็นฟีเจอร์ในการทำงานหลายๆ อย่าง

พิจารณาทางด้านเทคนิคนั้นระบบไฟร์วอลล์ที่เหมาะสมต่อเหมาะสมในการนำเข้ามาติดตั้งในระบบเครือข่ายของบริษัท เมอร์ก จำกัด คือระบบไฟร์วอลลวัน ซึ่งสามารถทำได้ทั้งสองแบบคือที่ติดตั้งบนวินโดว์ 2000 และเรดแฮทลินุกซ์ แต่ถ้ามองทางด้านค่าใช้จ่ายสะสมทั้งหมดตลอด 6 ปีแล้ว ในส่วนของระบบไฟร์วอลล์ที่ใช้เรดแฮทลินุกซ์มีค่าใช้จ่ายที่ต่ำกว่าเล็กน้อย

ถ้าพิจารณาทางด้านค่าใช้จ่ายทั้งหมดที่ต้องสูญเสียไปกับระบบไฟร์วอลล์แล้ว ไฟร์วอลล์ที่ติดตั้งด้วยระบบไอพีเทเบิ้ล เป็นทางเลือกที่ดีมากเนื่องจากค่าใช้จ่ายในทุกๆปี ต่ำกว่าระบบไฟร์วอลล์แบบอื่นอย่างมาก แต่ถ้ามองทางด้านเทคนิค ไฟร์วอลล์ที่ใช้ไอพีเทเบิลขาดความสามารถที่สามารถชดเชยได้จากการให้มีบริษัทภายนอกเข้ามาเพื่อทำการสนับสนุนการใช้งานไอพีเทเบิล ทำให้ปัญหาที่เกิดขึ้นทางเทคนิคหมดไปได้

สรุประบบไฟร์วอลล์ที่ควรนำมาใช้ในบริษัท เมอร์ก จำกัดควรนำระบบไฟร์วอลล์ที่เป็นแบบไอพีเทเบิ้ลเข้ามาใช้ เนื่องจากค่าใช้จ่ายทั้งหมดต่อปี และค่าใช้จ่ายสะสมจำนวน 6 ปี เป็นจำนวนเงินที่น้อยที่สุด ประกอบกับคุณสมบัติในการใช้งานมีความสามารถเทียบเท่ากับไฟร์วอลล์ในแบบอื่นๆ

5.2 ข้อเสนอแนะ

การศึกษาความเป็นไปได้ในรายงานฉบับนี้เป็นเพียงแนวทางในการศึกษาเท่านั้น ซึ่งอนาคตจำเป็นต้องมีการอัพเดทข้อมูลต่างๆ เกี่ยวกับรูปแบบ ชนิด ราคา และค่าใช้จ่ายของไฟร์วอลล์ที่จะเกิดขึ้นอีกในอนาคต เพื่อทำให้ได้ข้อสรุปที่ชัดเจนถูกต้องตรงกับความเป็นจริงมากที่สุด

บรรณานุกรม

ชูชีพ พิพัฒน์ศิถี. 2544. **เศรษฐศาสตร์การวิเคราะห์โครงการ.** กรุงเทพมหานคร : เท็กซ์แอนเจอร์นัลพับลิเคชั่น

Paul Compbel,Ben Calvert, Steven Boswell 2003 **Security + Guide to Network Security Fundamental THOMSON Course techonology**

ปราการ โกลากุล. 2544. **ความรู้พื้นฐานเกี่ยวกับไฟร์วอลล์.** [Online]. Available : http://thaicert.nectec.or.th/paper/firewall/fwbasics.php

The SANS Institute. 2002. [Online]. Available : http:// www.sans.org

Red Hat Cooperate Headquarters. 2003. [Online]. Available : http://www.redhat.com

Cisco System, Inc. 2003. **Cisco Pix 515E FIREWALL.** [Online]. Available : http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps4094/index.html

Check Point Firewall-1,Inc. 2003. **Solutions& Products.** [Online]. Available : http://www.checkpoint.com/products/index.html

Microsoft Corporation. 2003. **Windows 2000 Server.** [Online]. Available : http://www.microsoft.com/windows2000/server/default.asp

IBM Corporation 1994. 2003. **Xseries Intel processor-based servers.** [Online]. Available : http://www.pc.ibm.com/us/eserver/xseries/