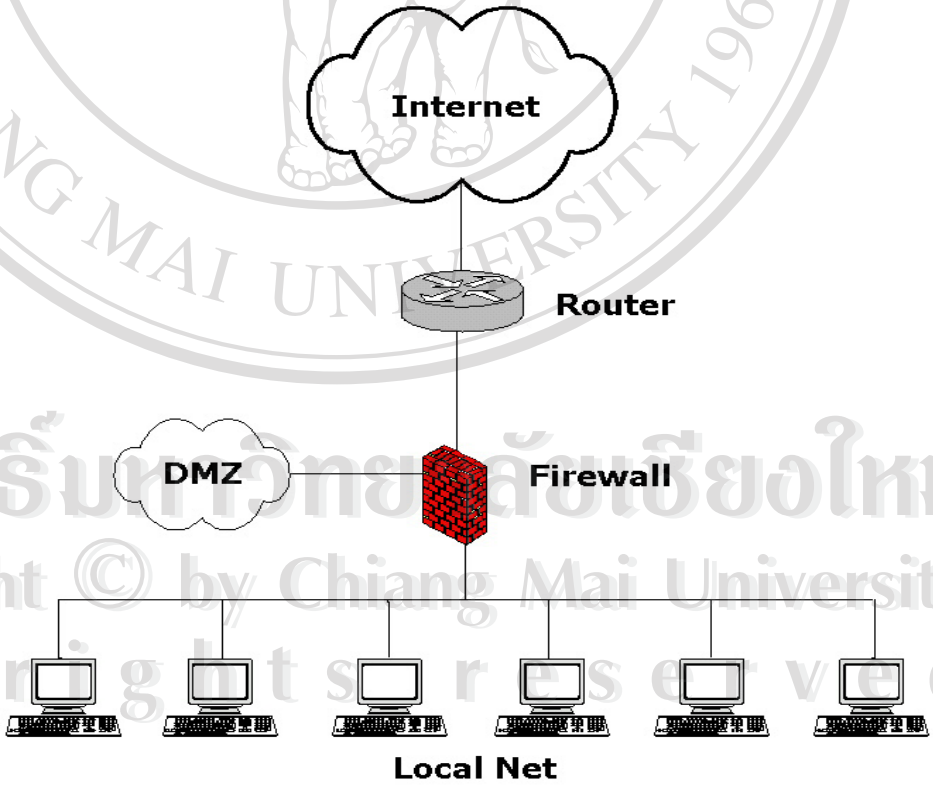
บทที่ 4
การออกแบบและพัฒนาระบบป้องกันและตรวจสอบผู้บุกรุกระบบเครือข่าย

4.1 สถาปัตยกรรมการวางระบบป้องกันและตรวจสอบผู้บุกรุกบนระบบเครือข่าย

4.1.1 การวางตำแหน่งระบบป้องกัน(ไฟร์วอลล์)บนระบบเครือข่าย

เนื่องจากไฟร์วอลล์เป็นระบบป้องกันและรักษาความปลอดภัยที่ใช้วิธีการวางนโยบายเป็นกฎข้อต่างๆในการอนุญาตให้แพ็กเก็ตใดวิ่งผ่านตัวมันได้บ้าง โดยอาศัยพารามิเตอร์ต่างๆในการพิจารณาตรวจสอบแพ็กเก็ตเช่น ค่าไอพีแอดเดรสต้นทาง-ปลายทาง หมายเลขโปรโตคอลของบริการต้นทาง-ปลายทาง ค่าหรือออปชันต่างในตัวเนื้อหาของแพ็กเก็ต เป็นต้น ฉะนั้นตำแหน่งที่เหมาะสมในการวางไฟร์วอลล์ไว้สำหรับป้องกันเครือข่ายภายในจากการบุกรุกจากภายนอก จึงควรอยู่ในตำแหน่งที่อยู่ถัดจากเราเตอร์ที่ต่อเชื่อมกับอินเทอร์เน็ตภายนอก และเป็นเกตเวย์หรือทางออกสำหรับเครือข่ายที่อยู่ภายในและเซิร์ฟเวอร์ต่างๆ ดังรูปที่ 4.1

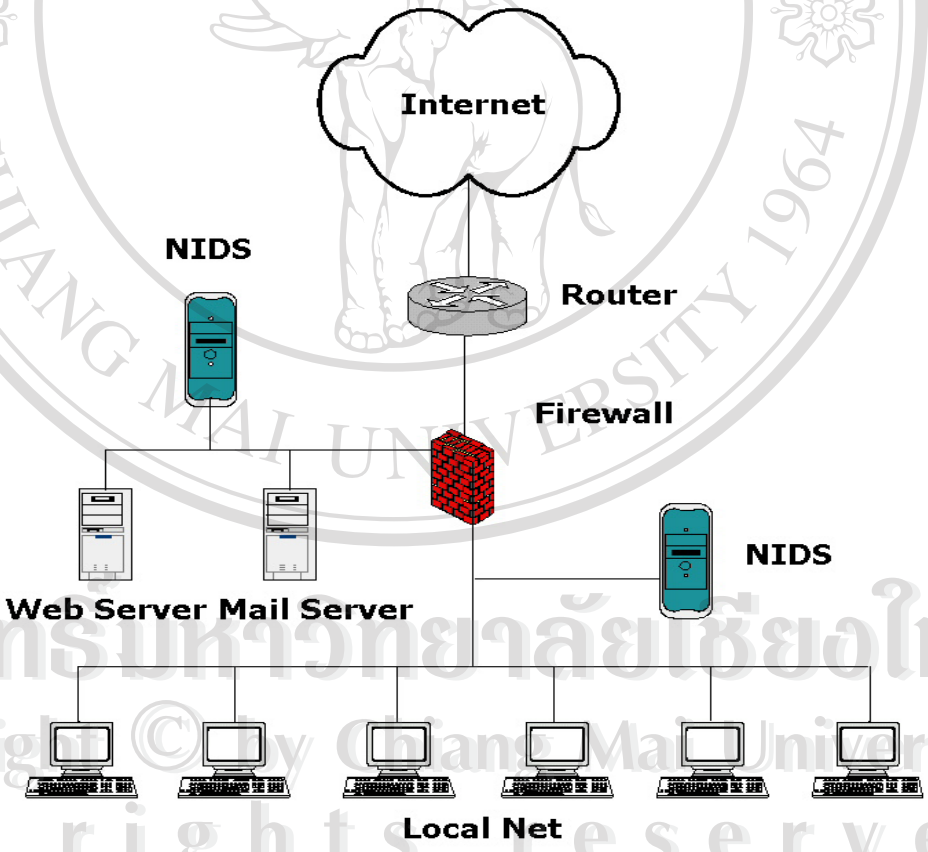


รูปที่ 4.1 ตัวอย่างการวางไฟร์วอลล์เพื่อป้องกันระบบเครือข่ายและเซิร์ฟเวอร์ภายใน

ซึ่งเป็นตำแหน่งที่ไฟร์วอลล์สามารถตรวจสอบแพ็กเก็ตได้ทุกแพ็กเก็ตที่วิ่งเข้าออกระบบเครือข่ายภายในและวงเซิร์ฟเวอร์ที่แยกอยู่อีกเครือข่าย (DMZ) ได้ ทำให้ไฟร์วอลล์ทำงานได้อย่างเต็มประสิทธิ์ภาพในการป้องกันการบุกรุกที่อาจเกิดขึ้น

4.1.2 การวางตำแหน่งระบบตรวจสอบการบุกรุกนระบบเครือข่าย

ระบบตรวจสอบการบุกรุกแบบ NIDS ทำงานอยู่บนเครือข่าย โดยทำการเฝ้าดูและตรวจสอบข้อมูลแพ็กเก็ตต่างๆจะถูกตรวจสอบโดยตัวตรวจจับหรือเซ็นเซอร์ (Sensor) ของระบบ ซึ่งตัวตรวจจับจะมองเห็นเฉพาะแพ็กเก็ตที่วิ่งผ่านบนเครือข่ายที่ตัวตรวจจับนั้นติดตั้งอยู่เท่านั้น ซึ่งระบบตรวจสอบประเภทนี้สามารถตรวจสอบการบุกรุกได้ทั้งระบบเครือข่าย ไม่เกิดความยุ่งยากในการติดตั้งระบบตรวจสอบผู้บุกรุกบนเครื่องที่ต้องการตรวจสอบทุกเครื่องเหมือน Host-based IDS และการเก็บบันทึกข้อมูลการบุกรุกที่แยกต่างหาก ทำให้ปลอดภัยจากการทำลายร่องรอยการบุกรุกหลังจากผู้บุกรุกสามารถเข้าสู่ระบบแล้ว



รูปที่ 4.2 ตัวอย่างการวางระบบตรวจสอบการบุกรุกแบบ NIDS บนเครือข่าย

จากตัวอย่างรูปที่ 4.2 เป็นการวางระบบตรวจสอบการบุกรุกแบบ NIDS 2 จุด เพื่อตรวจจับการบุกรุกที่เกิดขึ้นภายในทั้งเครือข่ายที่เป็นเซิร์ฟเวอร์และวงเครือข่ายที่เป็นเครื่องไคล์เอนต์

4.2 ระบบเครือข่ายที่ทำการทดลอง

ระบบเครือข่ายภายในคณะวิทยาศาสตร์ ภาควิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยเชียงใหม่ ประกอบด้วยเครื่อง

- เซิร์ฟเวอร์ จำนวน 4 เครื่อง ได้แก่

1. Mail Server ทำงานบนระบบปฏิบัติการ Solaris 2.7 หมายเลขไอพีแอดเดรส 202.28.24.216

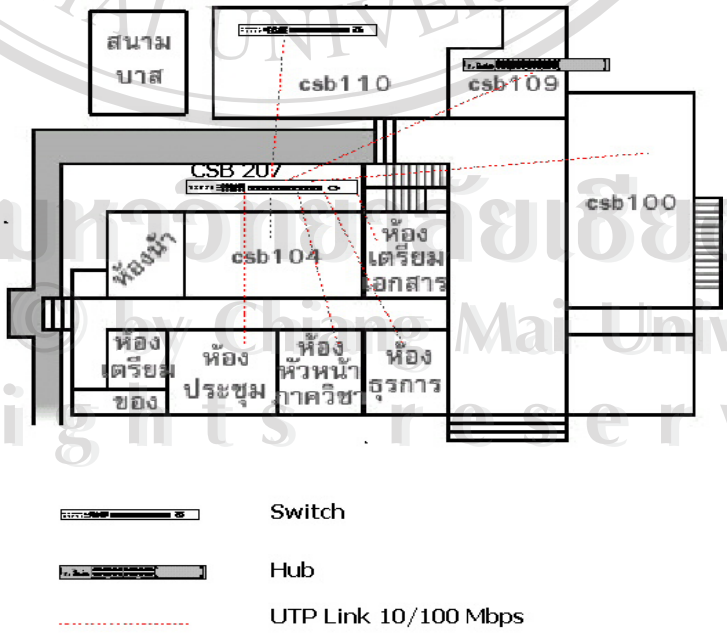
2. Web Server ทำงานบนระบบปฏิบัติการ Microsoft Windows 2000 Server หมายเลขไอพีแอดเดรส 202.28.24.217

3. E-Learning Server ทำงานบนระบบปฏิบัติการ Microsoft Windows 2003 Server หมายเลขไอพีแอดเดรส 202.28.24.218

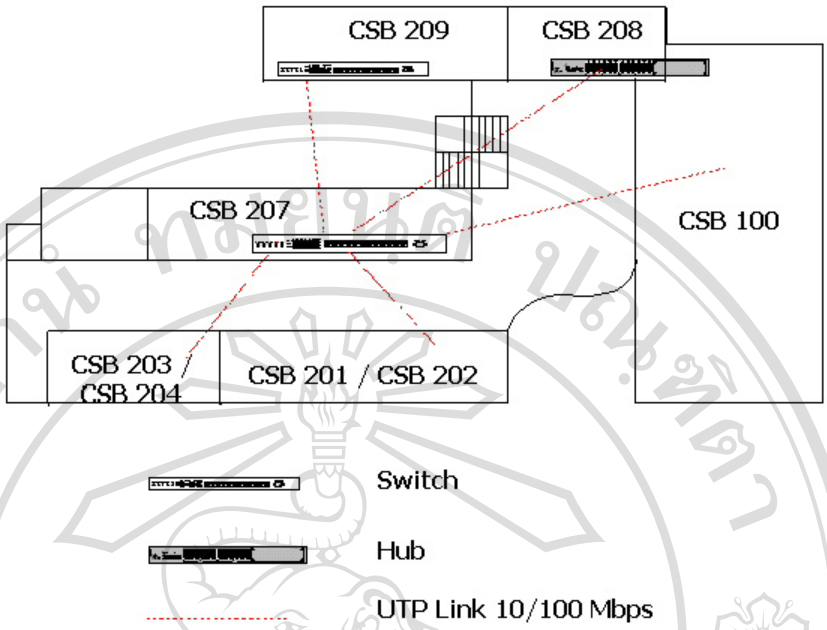
4. Research Server ทำงานบนระบบปฏิบัติการ Microsoft Windows 2000 Server หมายเลขไอพีแอดเดรส 202.28.24.205

- ไคล์เอนท์ จำนวนประมาณ 400 เครื่อง ทำงานบนระบบปฏิบัติการ Microsoft Windows 98 และ Windows XP

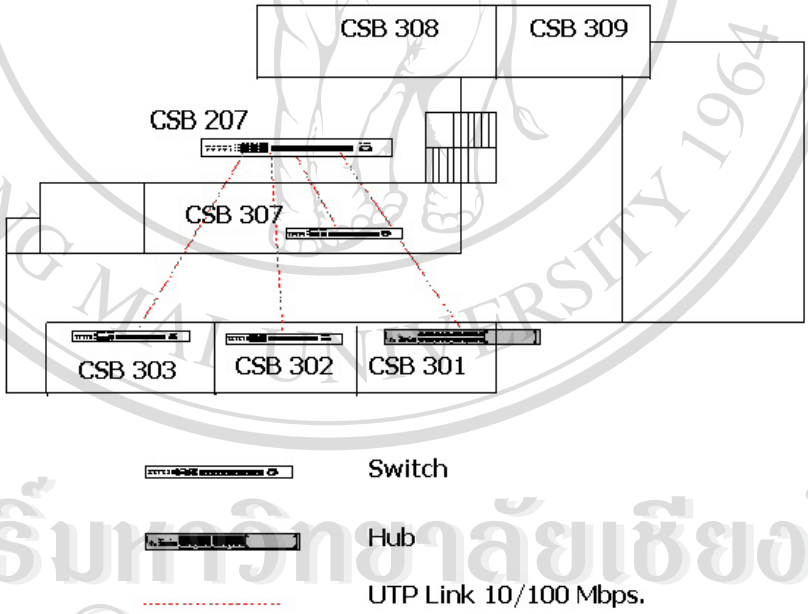
ระบบเครือข่ายภาควิชาวิทยาการคอมพิวเตอร์ทำการเชื่อมต่อเข้ากับระบบเครือข่ายส่วนกลางของคณะวิทยาศาสตร์ผ่านทางสายใยแก้วนำแสงแบบ Multimode ด้วยอุปกรณ์ Switch Super Stack II รุ่น SW3300 ที่ห้อง CSB 207 ซึ่งทำหน้าที่กระจายการเชื่อมต่อแบบ Star ไปยังห้องต่างๆภายในอาคาร ดังรูป



รูปที่ 4.3 ผังการเชื่อมต่อระบบเครือข่ายภายในอาคาร ชั้น 1

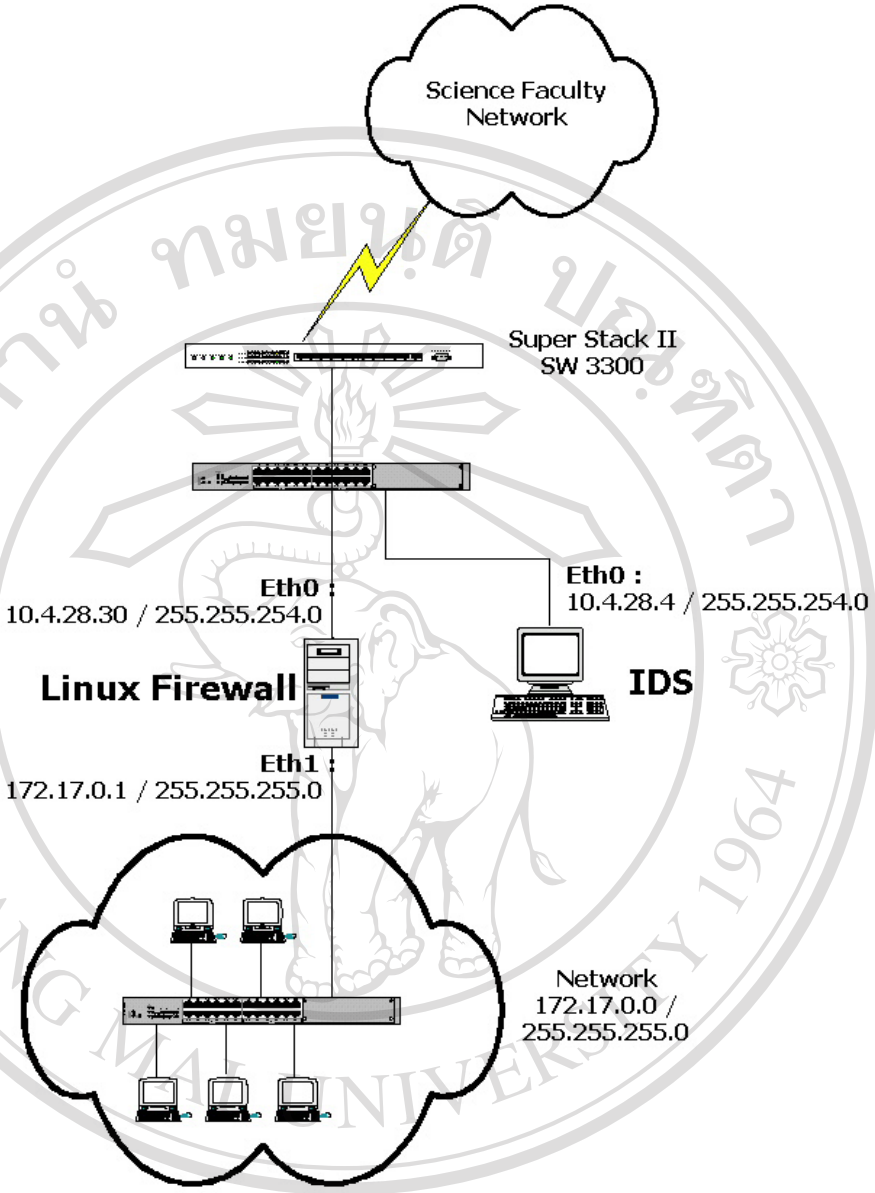


รูปที่ 4.4 ผังการเชื่อมต่อระบบเครือข่ายภายในอาคาร ชั้น 2



รูปที่ 4.5 ผังการเชื่อมต่อระบบเครือข่ายภายในอาคาร ชั้น 3

สำหรับระบบเครือข่ายที่ใช้ในการทดลองระบบฯ คือภายในห้องเรียน CSB 302 ซึ่งประกอบด้วยเครื่องไคล์เอนต์ จำนวน 40 เครื่อง ทำงานบนระบบปฏิบัติการ Microsoft Windows 2000 Professional โดยมีการวางระบบฯและการเชื่อมต่อเครือข่าย ดังรูป



รูปที่ 4.6 ผังการวางระบบป้องกันและตรวจสอบผู้บุกรุกภายในเครือข่ายห้องเรียน CSB302

จากรูปที่ 4.4 ได้ทำการจำลองเครือข่ายภายในห้องให้เชื่อมต่อกันด้วยอุปกรณ์ Hub โดยมีการวางระบบป้องกันการบุกรุก (Linux Firewall) ไว้ที่ตำแหน่งทางเข้าออกระบบเครือข่ายของห้อง ทำหน้าที่เป็นเกตเวย์และป้องกันการบุกรุกที่จะเข้ามายังภายในระบบเครือข่าย ประกอบด้วยสองอินเตอร์เฟส ได้แก่

- Eth0 ทำการเชื่อมต่อไปยังอุปกรณ์ Hub ซึ่งเชื่อมต่อไปยังอุปกรณ์ Switch หลักของภาควิชาฯ ที่ห้อง CSB 207
- Eth1 ทำการเชื่อมต่อกับเครือข่ายภายในห้อง

และระบบตรวจสอบผู้บุกรุก ซึ่งวางอยู่ที่ตำแหน่งด้านหน้าของระบบเครือข่ายภายในห้อง โดยเชื่อมต่อผ่านอุปกรณ์ Hub ทำหน้าที่คอยตรวจสอบการบุกรุกที่เกิดขึ้นจากภายในเครือข่ายของคณะวิทยาศาสตร์และมหาวิทยาลัยเอง และส่งคำร้องไปบอกระบบป้องกันการบุกรุกให้ทำการบล็อคการบุกรุกนั้น ประกอบด้วยหนึ่งอินเตอร์เฟส ได้แก่

- Eth0 ทำการเชื่อมต่อเข้ากับระบบเครือข่ายภายในภาควิชาฯ

หมายเหตุ : เนื่องจากทั้งเครือข่ายภายในห้องเรียนและเครือข่ายภายในภาควิชาฯเอง เป็นเครือข่ายที่เป็นไอพีปลอมซึ่งไม่สามารถทำการเชื่อมต่อจากภายนอกเข้ามาได้ ฉะนั้นการบุกรุกที่สามารถตรวจจับได้โดยระบบตรวจสอบผู้บุกรุกในลักษณะนี้สามารถตรวจจับได้เฉพาะการบุกรุกที่เกิดจากภายในภาควิชาฯและที่เกิดจากภายในมหาวิทยาลัยเองเท่านั้น

4.3 สรุปข้อมูลการบุกรุกที่เกิดขึ้น

ข้อมูลการบุกรุกที่เกิดขึ้นตั้งแต่วันที่ 29 สิงหาคม 2546 ถึงวันที่ 11 กันยายน 2546 (ยังไม่ติดตั้งระบบป้องกันการบุกรุก) สามารถสรุปได้ดังนี้

4.3.1 จำแนกตามประเภทโปรโตคอล ได้เป็น

- แพ็กเก็ตโปรโตคอล TCP 48%
- แพ็กเก็ตโปรโตคอล UDP 25%
- แพ็กเก็ตโปรโตคอล ICMP 27%

หมายเหตุ : แพ็กเก็ตที่เป็นการสแกนพอร์ตจะไม่ถูกนำมารวมในการแสดงผลของโปรแกรม ACID

4.3.2 จำนวนการแจ้งเตือนการบุกรุกที่เกิดขึ้นทั้งสิ้น 62,001 เหตุการณ์ แบ่งเป็นการบุกรุก 15 ประเภท 63 รูปแบบ

4.3.3 จำแนกตามไอพีแอดเดรสต้นทางได้ทั้งสิ้น 710 ไอพีแอดเดรส

4.3.4 จำแนกตามไอพีแอดเดรสปลายทางได้ทั้งสิ้น 588 ไอพีแอดเดรส

4.3.5 จำนวนไอพีลิงค์ได้ทั้งสิ้น 3909 ไอพีแอดเดรส

4.3.6 จำแนกตามจำนวนพอร์ตต้นทางได้ทั้งสิ้น 3181 พอร์ต แบ่งเป็นโปรโตคอล TCP 534 พอร์ต และ UDP 3084 พอร์ต

4.3.7 จำแนกตามจำนวนพอร์ตปลายทางได้ทั้งสิ้น 34 พอร์ต แบ่งเป็นโปรโตคอล TCP 27 พอร์ต และUDP 29 พอร์ต

4.4 การกำหนดเกณฑ์การป้องกัน

จากข้อมูลการบุกรุกที่เกิดขึ้นสามารถแบ่งตามลำดับความร้ายแรงในการเสี่ยง ตามตารางที่ 3.7, 3.8 และ 3.9 ได้เป็น

- ระดับความเสี่ยงสูง 27.7% ()
- ระดับความเสี่ยงปานกลาง 53.4% ()
- ระดับความเสี่ยงต่ำ 18.9% ()

การกำหนดเกณฑ์มาตราฐานในการป้องกันภัยในระดับต่างๆ

- ระดับความเสี่ยงสูง กำหนดให้ทำการป้องกันเป็นเวลา 1 ชั่วโมง ดังตาราง

ประเภทความเสี่ยงสูง	ระยะเวลาในการป้องกัน (วินาที)
attempted-admin	3601
attempted-user	3602
shellcode-detect	3603
successful-admin	3604
successful-user	3605
trojan-activity	3606
unsuccessful-user	3607
web-application-attack	3608

ตารางที่ 4.1 เกณฑ์การป้องกันภัย ประเภทความเสี่ยงสูง

- ระดับความเสี่ยงปานกลาง กำหนดให้ทำการป้องกันเป็นเวลา 30 นาที ดังตาราง

ประเภทความเสี่ยงปานกลาง	ระยะเวลาในการป้องกัน (วินาที)
attempted-dos	1809
attempted-recon	1810
bad-unknown	1811
denial-of-service	1812
misc-attack	1813
non-standard-protocol	1814
rpc-portmap-decode	1815
successful-dos	1816
successful-recon-largescale	1817
successful-recon-limited	1818

suspicious-filename-detect	1819
suspicious-login	1820
system-call-detect	1821
unusual-client-port-connection	1822
web-application-activity	1823

ตารางที่ 4.2 เกณฑ์การป้องกันภัย ประเภทความเสี่ยงปานกลาง

- ระดับความเสี่ยงต่ำ เนื่องจากเป็นการบุกรุกที่เกิดขึ้นในระดับนี้ส่วนมากเป็นเพียงการสำรวจเครือข่าย ซึ่งบางครั้งถือเป็นพฤติกรรมที่เกิดขึ้นเป็นปกติบนเครือข่าย เช่นการ Ping เพื่อตรวจสอบเครือข่ายของเราเอง ไม่ถึงขั้นการบุกรุกที่ต้องทำการป้องกันในทันที เกณฑ์การป้องกันในระดับนี้จึงเป็นศูนย์ (ไม่มีการส่งคำร้องไปยังระบบป้องกันการบุกรุกเพื่อทำการบล็อค)

หมายเหตุ : การกำหนดเกณฑ์ช่วงเวลาในการป้องกันการบุกรุกดังกล่าว ไม่สามารถกำหนดเป็นเกณฑ์ที่เป็นมาตราฐานตายตัวได้สำหรับกฎทุกข้อ จึงจำเป็นต้องขึ้นอยู่กับวิจารณญาณของผู้ดูแลระบบเองด้วยในการกำหนดระยะเวลาดังกล่าว