ระบบตรวจนโยบายสำหรับเครือข่ายแคมปัส

อภิวัฒน์ เปลี่ยนจิตรดี, สุรศักดิ์ สงวนพงษ์ และอุรุพจน์ กัลยาสิริ

กลุ่มวิจัยเครือข่ายประยุกต์ ภาควิชาวิศวกรรมคอมพิวเตอร์
มหาวิทยาลัยเกษตรศาสตร์ จตุจักร กรุงเทพฯ
{g4465033, Surasak.S, cpcupk}@ku.ac.th

บทคัดย่อ นโยบายความปลอดภัยของเครือข่ายเป็นสิ่งที่จัดทำขึ้นเพื่อกำหนดการใช้งานคอมพิวเตอร์และเครือข่ายในองค์กร เมื่อกำหนดนโยบายความปลอดภัยแล้วปัญหาที่เกิดขึ้นคือ ผู้ดูแลระบบไม่สามารถทราบว่านโยบายนั้นทำงานได้ตามที่กำหนด หรือมีการละเมิดนโยบายหรือไม่ ดังนั้นงานวิจัยนี้จึงเสนอระบบตรวจนโยบายความปลอดภัย โดยมีโครงสร้างแบบกระจาย มีเซนเซอร์กระจายอยู่ตามซับเน็ท เพื่อคอยจับแพ็คเก็ตมาตรวจความถูกต้องของนโยบาย โดยเซนเซอร์จะรับนโยบายมาจากโพลีซีเซิร์ฟเวอร์ และหากเกิดเหตุการณ์ใดๆ ที่ละเมิดนโยบายเซนเซอร์จะแจ้งไปยังเครื่องมอนิเตอร์ซึ่งมีผู้ดูแลระบบคอยดูแลอยู่

1 บทนำ

ไฟร์วอลล์จัดเป็นอุปกรณ์ที่ใช้ป้องกันการบุกรุกเครือข่าย แต่มีข้อจำกัดคือไม่สามารถป้องกันการบุกรุกที่เกิดจากบุคคลภายในเครือข่ายได้ และหากจะติดตั้งไฟร์วอลล์กระจายตามส่วนต่างๆ ของเครือข่ายก็จะมีปัญหาและไม่สะดวกในกรณีที่ต้องการแก้ไขข้อกำหนดในไฟร์วอลล์ นโยบายความปลอดภัยเป็นสิ่งที่ผู้ดูแลระบบต้องให้ความสำคัญใช้เป็นบรรทัดฐานกำหนดวิธีการป้องกันและโต้ตอบกับสถานการณ์ความปลอดภัยที่อาจเกิดขึ้นในเครือข่าย โดยก่อนที่จะกำหนดนโยบายความปลอดภัยจะต้องวิเคราะห์ความเสี่ยงของระบบคอมพิวเตอร์และเครือข่ายซึ่งได้แก่ การอนุญาตให้เข้าใช้ทรัพยากร การกำหนดการใช้งานทรัพยากรแบบปกติ การอนุญาตให้เข้าถึงระบบ การกำหนดหน้าที่ของผู้ดูแลระบบ และการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้ เป็นต้น ปัญหาความปลอดภัยในเครือข่ายที่มักพบ ได้แก่ การเข้ามาในเครือข่ายโดยไม่ได้รับอนุญาต การเปิดบริการที่ไม่สมควรให้บริการ การเปิดเผยข้อมูลสำคัญบางอย่างที่อาจทำให้มีการลักลอบขโมยข้อมูลไปได้ เช่น ข้อมูลบัตรเครดิต ข้อมูลทางการค้า เป็นต้น

เมื่อกำหนดนโยบายให้กับเครือข่ายแล้ว ปัญหาที่เกิดตามมาคือ

1. ผู้ดูแลระบบไม่สามารถทราบได้ว่านโยบายความปลอดภัยของเครือข่ายที่กำหนดไว้นั้นทำงานตรงตามวัตถุประสงค์ที่ตั้งไว้หรือไม่ และหากนโยบายไม่สามารถทำงานได้ตามที่ต้องการอาจเป็นช่องว่างให้ผู้บุกรุกโจมตีเครือข่ายได้
2. ผู้ดูแลระบบไม่ทราบว่ามีผู้ใช้รายใดละเมิดนโยบายความปลอดภัยที่กำหนดไว้หรือไม่

ปัญหาเหล่านี้สามารถแก้ไขโดยการสร้างระบบที่สามารถตรวจสอบกิจกรรมในเครือข่ายว่าเป็นไปตามนโยบายที่กำหนดไว้ และมีการกระทำใดละเมิดนโยบายหรือไม่

2 งานวิจัยที่เกี่ยวข้อง

Tao *et al.* [1] นำเสนอการจัดการความปลอดภัยของเครือข่ายที่ขึ้นกับนโยบายและโมบายเอเจนท์ ข้อดีของโมเดลนี้คือสามารถเปลี่ยนแปลงนโยบายด้วยตนเองได้ โดยใช้ฟังก์ชันที่สร้างขึ้นมาวิเคราะห์เพื่อเปลี่ยนแปลงนโยบาย ข้อเสียคือระบบนี้ใช้โมบายเอเจนท์ทำหน้าที่ตรวจความปลอดภัยของอุปกรณ์ดังนั้นจะทำให้เสียแบนวิทด์ที่ใช้ในเครือข่ายไปกับการติดต่อกันระหว่างโมบายเอเจนท์และเอเจนท์แมนเนเจอร์มากกว่าระบบตรวจนโยบายสำหรับเครือข่ายแคมปัสซึ่งใช้ระบบไคลเอ็นต์-เซิร์ฟเวอร์

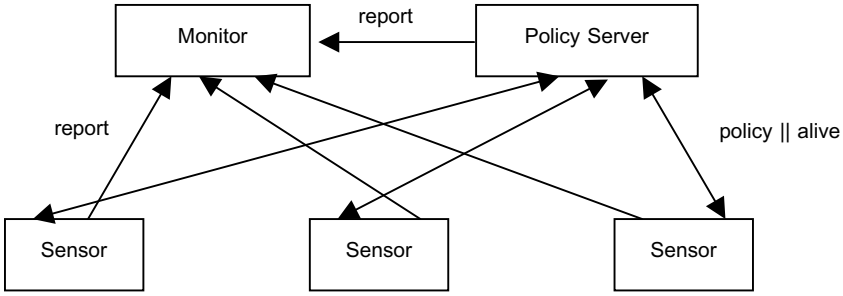
งานวิจัยของ Al-Khayatt *et al.* [2] เสนอการออกแบบและสร้างเครื่องมือที่ใช้เฝ้ามองการใช้งานอินเทอร์เน็ต เพื่อป้องกันลักษณะการใช้งานใดที่ขัดกับนโยบายที่ตั้งไว้เช่น การเล่นเกมส์ผ่านอินเทอร์เน็ต การเข้าถึงสื่อลามกอนาจาร เป็นต้น โดยมีล็อกลุค (LogLook) เป็นระบบที่นำข้อมูลจากล็อกไฟล์ในเอชทีทีพีพร็อกซี่ (HTTP proxy) มาวิเคราะห์ หากระบบพบว่ามีผู้ใช้ในเครือข่ายใช้อินเทอร์เน็ตขัดกับนโยบายก็จะแจ้งให้ผู้ดูแลระบบทราบผ่านทางอีเมล์ ระบบนี้มีข้อเสียคือจะทำงานหลังจากการโรเทท (rotate) ล็อกไฟล์จึงจัดว่าเป็นการทำงานแบบออฟไลน์ ส่วนระบบตรวจนโยบายสำหรับเครือข่ายแคมปัสจะทำงานแบบออนไลน์ทำให้ในขณะนั้นสามารถบอกได้ว่ามีผู้ใช้คนใดกำลังละเมิดนโยบายอยู่

งานวิจัยของ Stone *et al.* [3] นำเสนอภาษานโยบายเครือข่ายที่มีอยู่ในปัจจุบัน จากนั้นจะสรุปเทคนิคสำหรับตรวจนโยบายที่ขัดแย้งกัน และเสนอภาษานโยบายแบบใหม่ซึ่งเรียกว่า Path-Based Policy Language ระบบตรวจสอบนโยบายสำหรับเครือข่ายแคมปัสนำลักษณะการออกแบบภาษานโยบายมาเป็นแนวทางในการกำหนดนโยบายที่ใช้ในระบบ

โครงร่างนโยบาย (Policy Framework) ที่ใช้ในเครือข่าย นำเสนอโดย Lewis [4] เป็นวิธีการนำนโยบายมาใช้ในการจัดการเครือข่ายซึ่งระบบตรวจนโยบายสำหรับเครือข่ายแคมปัสได้นำโครงร่างนโยบายนี้มาประยุกต์ใช้กับโครงร่างการตรวจนโยบายของระบบ

3 โครงสร้างของระบบ

ระบบตรวจนโยบายประกอบด้วย 3 ส่วน คือ มอนิเตอร์ (Monitor) โพลีซีเซิร์ฟเวอร์ (Policy Server) และเซนเซอร์ (Senser) มีโครงสร้างดังแสดงในรูปที่ 1



รูปที่ 1 โครงสร้างของระบบการตรวจนโยบายความปลอดภัยของเครือข่าย

จากรูปที่ 1 จะเห็นได้ว่าทั้ง 3 องค์ประกอบสามารถจัดวางได้อย่างอิสระในเครือข่าย และมีหน้าที่แตกต่างกัน ดังต่อไปนี้

1. มอนิเตอร์ ทำหน้าที่

- คอยรับการแจ้งเหตุการณ์ที่ไม่ตรงกับนโยบายจากเซนเซอร์ 2. โพลีซีเซิร์ฟเวอร์ ทำหน้าที่
- เก็บไอพีแอดเดรสของเซนเซอร์ทั้งหมดที่อยู่ในเครือข่ายและนโยบายของระบบ
- ส่งนโยบายที่ผู้ดูแลระบบปรับปรุงแก้ไขไปยังเซนเซอร์ในเครือข่าย โดยจะพิจารณาไอพีแอดเดรสของเซนเซอร์จากไฟล์ที่เตรียมไว้
- คอยส่งสัญญาณไปยังเซนเซอร์เป็นช่วงเวลา หากเซนเซอร์ตัวใดไม่ส่งสัญญาณกลับมาภายในเวลาที่กำหนดจะส่งข้อมูลแจ้งมอนิเตอร์ว่าเซนเซอร์ตัวนั้นไม่ทำงาน
- อาจติดตั้งโพลีซีเซิร์ฟเวอร์สำรอง (Secondary Policy Server) ไว้เพื่อใช้ในกรณีที่เครื่องโพลีซีเซิร์ฟเวอร์หลักไม่สามารถให้บริการได้

3. เซนเซอร์ ทำหน้าที่

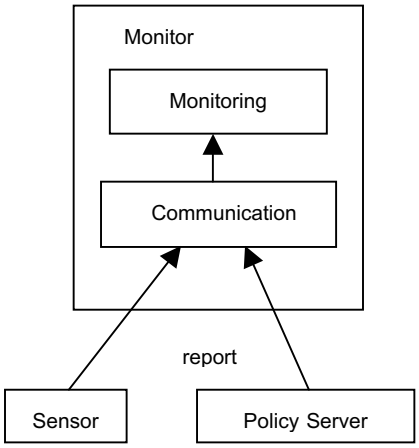
- ตรวจแพ็คเก็ตในซับเน็ทที่เซนเซอร์อยู่ว่าถูกต้องตามนโยบายที่ได้รับมาหรือไม่ หากไม่ถูกต้องตามนโยบาย เซนเซอร์จะส่งข้อมูลที่ไม่ตรงกับนโยบายไปยังมอนิเตอร์รับนโยบายจากเครื่องโพลีซีเซิร์ฟเวอร์
- คอยตอบกลับสัญญาณที่ส่งมาจากโพลีซีเซิร์ฟเวอร์ เพื่อแสดงว่ายังทำงานอยู่

3.1 การทำงานของมอนิเตอร์

รูปที่ 2 แสดงการทำงานของมอนิเตอร์ ซึ่งแบ่งออกเป็น 2 โมดูล คือ

1. การติดต่อ (Communication) ทำหน้าติดต่อกับเซนเซอร์และโพลีซีเซิร์ฟเวอร์

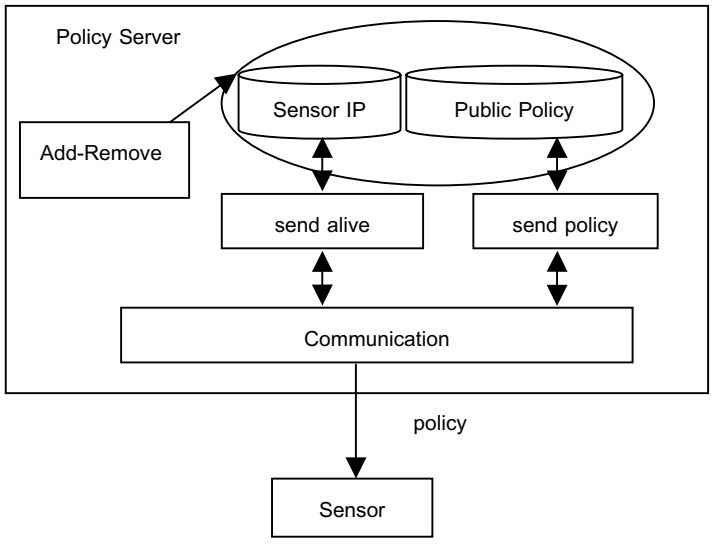
2. มอนิเตอริง (Monitoring) ทำหน้าที่แสดงผลและติดต่อกับผู้ใช้



รูปที่ 2 โมดูลของมอนิเตอร์

3.2 การทำงานของโพลีซีเซิร์ฟเวอร์

โครงสร้างการทำงานของโพลีซีเซิร์ฟเวอร์ซึ่งประกอบไปด้วยโมดูลหลัก 6 ส่วนหลัก ดังแสดงในรูปที่ 3



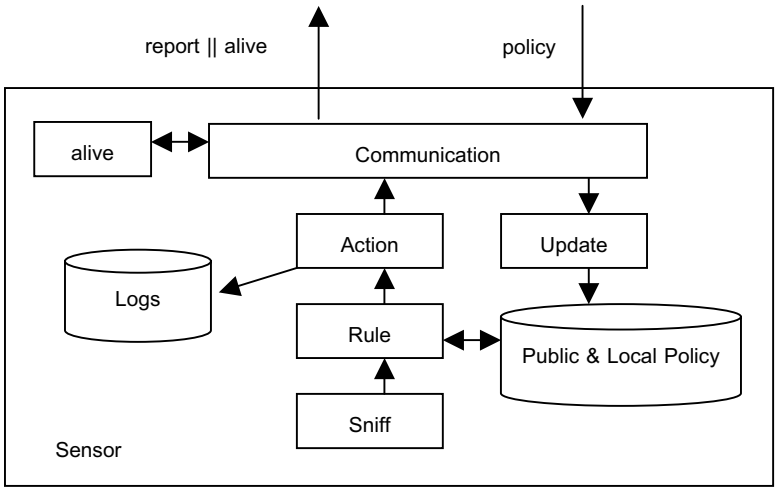
รูปที่ 3 โมดูลของโพลีซีเซิร์ฟเวอร์

แต่ละโมดูลมีหน้าที่แตกต่างกันไปดังต่อไปนี้

1. การติดต่อ (Communication) ทำหน้าที่ติดต่อกับเซนเซอร์
2. เซนเซอร์ไอพี (Sensor IP) ทำหน้าที่เก็บไอพีแอดเดรสของเซนเซอร์ทั้งหมด
3. นโยบายแบบทั่วไป (Public Policy) ทำหน้าที่เก็บโพลีซีเซิร์ฟเวอร์แบบทั่วไป (Public) ทั้งหมด
4. เพิ่ม-ลด (Add-Remove) เป็นส่วนที่ใช้ติดต่อกับผู้ใช้กรณีที่ต้องการเพิ่มหรือลดนโยบาย
5. ส่งนโยบาย (Send policy) ทำหน้าที่ส่งนโยบายไปยังเซนเซอร์ทั้งหมด
6. ส่งสัญญาณ (Send alive) ทำหน้าที่ส่งสัญญาณเป็นช่วงเวลาไปยังเซนเซอร์ เพื่อตรวจสอบว่ายังทำงานอยู่หรือไม่

3.3 การทำงานของเซนเซอร์

เซนเซอร์มีโครงสร้างแสดงดังรูปที่ 4



รูปที่ 4 โมดูลของเซนเซอร์

การทำงานของเซนเซอร์แบ่งออกเป็น 8 โมดูล คือ

1. การติดต่อ (Communicator) ทำหน้าที่ติดต่อกับมอนิเตอร์และโพลีซีเซิร์ฟเวอร์
2. ส่งสัญญาณกลับ (alive) ทำหน้าที่ตอบกลับสัญญาณที่ส่งมาจากโพลีซีเซิร์ฟเวอร์
3. จับแพ็คเก็ต (Sniff) ทำหน้าที่จับแพ็คเก็ตจากเครือข่าย
4. กฎ (Rule) ทำหน้าที่ตรวจแพ็คเก็ตกับนโยบายที่กำหนดไว้
5. การกระทำ (Action) ทำหน้าที่ตามที่กำหนดไว้ในนโยบาย

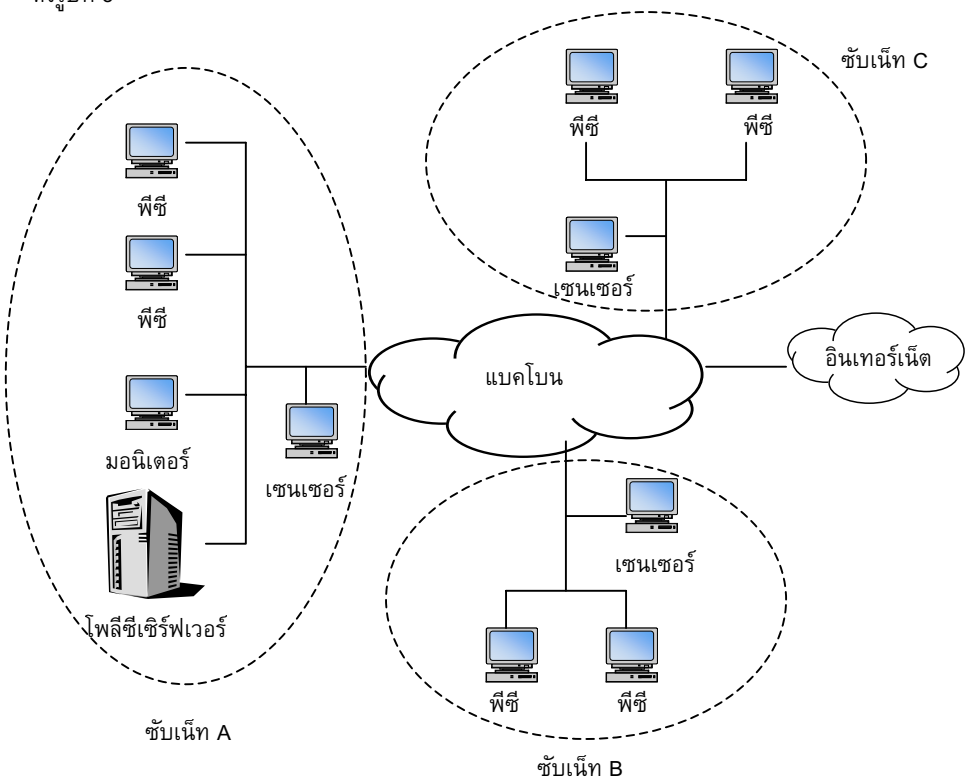
6. ปรับปรุงข้อมูล (Update) ทำหน้าที่แก้ไขนโยบายที่มีอยู่ หากได้รับสัญญาณการแก้ไขจากโพลีซีเซิร์ฟเวอร์
7. นโยบายแบบทั่วไปและแบบเฉพาะส่วน (Public & Local Policy) ทำหน้าที่เก็บนโยบายทั้งแบบทั่วไป (Public) และแบบเฉพาะส่วน (Local)
8. ล็อก (Logs) ทำหน้าที่เก็บการรายงานเหตุการณ์ที่เกิดจากการทำผิดนโยบาย

4 ตัวอย่างการติดตั้งระบบตรวจนโยบาย

วิธีการติดตั้งระบบตรวจนโยบายภายในเครือข่ายสามารถทำได้ดังนี้

1. ติดตั้งโพลีซีเซิร์ฟเวอร์และมอนิเตอร์ไว้ที่ใดก็ได้ในเครือข่าย
2. ติดตั้งเซนเซอร์ไว้ในซับเน็ทที่ต้องการตรวจความถูกต้องของนโยบายเครือข่าย
3. บันทึกไอพีแอดเดรสของเซนเซอร์ไว้ในไฟล์ที่อยู่ในโพลีซีเซิร์ฟเวอร์

สมมติว่าต่อเครือข่ายออกจากแบคโบน 3 ซับเน็ท คือ ซับเน็ท A B และ C ตัวอย่างนี้จะติดตั้งโพลีซีเซิร์ฟเวอร์ มอนิเตอร์ และเซนเซอร์ ไว้ในซับเน็ท A ติดตั้งเซนเซอร์ทั้งในซับเน็ท B และซับเน็ท C ดังรูปที่ 5



รูปที่ 5 ตัวอย่างการติดตั้งระบบตรวจนโยบายภายในเครือข่าย

5 ตัวอย่างการกำหนดนโยบาย

รูปที่ 6 แสดงตัวอย่างการกำหนดนโยบาย โดยรูปที่ 7 8 และ 9 จะแสดงรายละเอียดและความหมายของนโยบายที่ 1 2 และ 3 ตามลำดับ

```
<PolicyLists>
    <Public>
        <Policy>
            <Protocal>
                <IP>
                    <src_addr>100.0.0.0</src_addr>
                    <src_mask>255.0.0.0</src_mask>
                    <dest_addr>158.108.0.0</dest_addr>
                    <dest_mask>255.255.0.0</dest_mask>
                </IP>
            </Protocal>
            <Operation>
                </permit>
            </Operation>
        </Policy>
        <Policy>
            <Protocal>
                <TCP>
                    <dest_port gt = "1024" />
                </TCP>
            </Protocal>
            <Operation>
                <deny> (host) open port number greater 1024</deny>
            </Operation>
        </Policy>
   </Public>
   <Local>
        <Policy dayofweek = "M-F" time = "0800-1630">
            <Protocal>
                <HTTP>
                    <keywords> sex, mp3 </keywords>
                </HTTP>
            </Protocal>
            <Operation>
                <deny> (host) connect to (www) that has (keywords)
        </deny>
                <action> Firewall </action>
            </Operation>
        </Policy>
   </Local>
</PolicyLists>
```

รูปที่ 6 ตัวอย่างการกำหนดนโยบาย

นโยบายที่ 1 ถ้าแพ็คเก็ตมีไอพีแอดเดรสต้นทางจากเครือข่าย 100.0.0.0 และมีแอดเดรสปลายทางเป็นเครือข่าย 158.108.0.0 ให้โปรแกรมปล่อยแพ็คเก็ตผ่านเข้าไปในเครือข่ายได้ ดังรูปที่ 7

```
<Policy>
   <Protocal>
       <IP>
          <src_addr>100.0.0.0</src_addr>
          <src_mask>255.0.0.0</src_mask>
          <dest_addr>158.108.0.0</dest_addr>
          <dest_mask>255.255.0.0</dest_mask>
       </IP>
   </Protocal>
   <Operation>
       </permit>
   </Operation>
</Policy>
```

รูปที่ 7 นโยบายที่ 1

นโยบายที่ 2 ถ้ามีโฮสต์ใดเปิดพอร์ตมากกว่า 1024 โปรแกรมจะแจ้งเตือนผู้ดูแลระบบโดยส่งข้อความ (host) open port number greater 1024 โดย (host) เป็นไอพีของเครื่องที่เปิดพอร์ตมากกว่า 1024 ดังรูปที่ 8

```
<Policy>
   <Protocal>
       <TCP>
          <dest_port gt = "1024" />
       </TCP>
   </Protocal>
   <Operation>
       <deny> (host) open port number greater 1024</deny>
   </Operation>
</Policy>
```

รูปที่ 8 นโยบายที่ 2

นโยบายที่ 3 ถ้ามีโฮสต์ใดเปิดเว็บเพจที่มีคำว่า sex หรือ mp3 อยู่ใน URL ระหว่างวันจันทร์ถึงวันศุกร์ (M-F) เวลา 8.00 ถึง 16.30 น. โปรแกรมจะแจ้งเตือนไปยังผู้ดูแลระบบด้วยข้อความ "(host) connect to (www) that has (keywords)" โดย (host) เป็นไอพีแอดเดรสของผู้ส่ง, (www) เป็นยูอาร์แอล, (keywords) เป็นคำที่ผิดกฎ หลังจากนั้นจะอัพเดทคอนฟิกเกอเรชันของไฟร์วอลล์ให้บล็อกยูอาร์แอลนี้ ดังรูปที่ 9

```
<Policy dayofweek = "M-F" time = "0800-1630">
   <Protocal>
       <HTTP>
          <keywords> sex, mp3 </keywords>
       </HTTP>
   </Protocal>
   <Operation>
       <deny> (host) connect to (www) that has (keywords)
</deny>
       <action> Firewall </action>
   </Operation>
</Policy>
```

รูปที่ 9 นโยบายที่ 3

6 สรุป

งานวิจัยนี้เป็นการสร้างระบบตรวจนโยบายของเครือข่ายเพื่อใช้ตรวจว่านโยบายความปลอดภัยของเครือข่ายที่ผู้ดูแลระบบกำหนดไว้นั้นสามารถทำงานได้ตรงตามวัตถุประสงค์ที่ตั้งไว้หรือไม่ และมีผู้ใช้คนใดละเมิดนโยบายหรือไม่ โครงสร้างของระบบเป็นแบบกระจายซึ่งประกอบด้วย 3 ส่วนหลัก คือ เซนเซอร์ โพลีซีเซิร์ฟเวอร์ และมอนิเตอร์ แต่ละส่วนจะทำหน้าที่ดังนี้ คือ เซนเซอร์ ทำหน้าที่ตรวจนโยบายในเครือข่ายที่ตนเองตั้งอยู่ ซึ่งการติดตั้งเซนเซอร์นี้จะอยู่ในเครือข่ายที่ต้องการตรวจสอบนโยบาย โพลีซีเซิร์ฟเวอร์ทำหน้าที่เก็บนโยบาย มอนิเตอร์ทำหน้าที่แสดงผลหากมีการละเมิดนโยบายเกิดขึ้น โดยผู้ดูแลระบบสามารถกำหนดนโยบายตามวิธีการกำหนดนโยบายในระบบได้โดยอิสระ (บทความฉบับสมบูรณ์สามารถดาวน์โหลดได้ที่ http://anres.cpe.ku.ac.th/projects/policy/policy.doc)

7 กิตติกรรมประกาศ

งานวิจัยนี้ได้รับการสนับสนุนจากทุนช่วยเหลือทางด้านวิจัยวิทยาศาสตร์และเทคโนโลยี ประจำปี พ.ศ. 2545 โดยมูลนิธิโทเรเพื่อการส่งเสริมวิทยาศาสตร์ ประเทศไทย (Thailand Toray Science Foundation)

เอกสารอ้างอิง

1. Jiang Tao, Liu Ji-Ren, Qin Yang. 2000. The Research on Dynamic Self-Adaptive Network Security Model Based on Mobile Agent. Technology of Object-Oriented Languages and

Systems, 2000. TOOLS - Asia 2000. Proceedings. 36th International Conference on page(s): 134 - 139 30 Oct.-4 Nov. 2000.

2. Al-Khayatt, S. Neale, R. 2001. Automated detection of Internet usage policy violation. Computer Systems and Applications, ACS/IEEE International Conference : 507 – 510.
3. Stone, G.N., Lundy, B., Xie, G. 2001. Network policy languages: a survey and a new approach. IEEE Network Jan.-Feb. 2001 Volume: 15 Issue: 1: 10 – 21.
4. Lewis, L. 1996. Implementing policy in enterprise networks. IEEE Communications Magazine Volume: 34 Issue: 1 : 50 – 55.