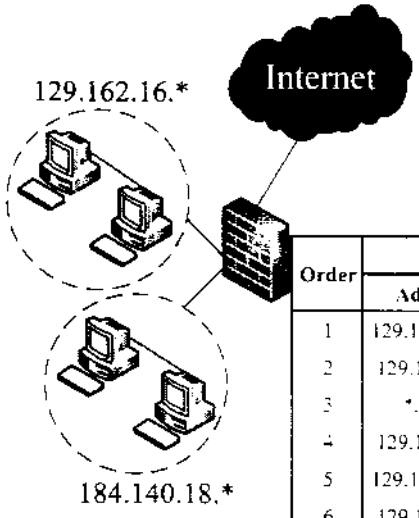
บทที่ 4

การวิเคราะห์ความผิดปกติของกฎในไฟร์วอลล์

4.1 กฎในไฟร์วอลล์เดี่ยว (Intra-firewall rule / Single firewall rule)

ภายในไฟร์วอลล์เดี่ยวดังภาพที่ 4.1 ลำดับของกฎถือเป็นสิ่งที่สำคัญต่อการกำหนดนโยบายในไฟร์วอลล์ ทั้งนี้เป็นเพราะกระบวนการกรองกลุ่มข้อมูลจะกระทำอย่างเป็นลำดับ โดยการเปรียบเทียบข้อมูลในส่วนหัวของกลุ่มข้อมูลกับค่าในแต่ละเขตข้อมูลของกฎที่ถูกแทนด้วยค่าของบัพและค่าที่ถูกระบุบนเส้นเชื่อมของแต่ละกราฟย่อยด้วยเส้นเชื่อม 1 เส้นเชื่อมตามภาพที่ 3.1 ไปจนกระทั่งกลุ่มข้อมูลจะสามารถจับคู่กับกราฟย่อยใดกราฟย่อยหนึ่งได้ หากลำดับของกราฟย่อยผิดไปกลุ่มข้อมูลอาจถูกยอมรับหรือถูกปฏิเสธซึ่งอาจไม่ได้เป็นไปตามนโยบายความมั่นคง สำหรับกฎลำดับสุดท้ายของแต่ละไฟร์วอลล์คือ กฎโดยปริยาย (Default rule) ที่มีแอ็คชันเท่ากับ "deny"



Firewall Rules

Order	Source		Destination		Action
	Address	Port	Address	Port	
1	129.162.16.10	any	*.*.*.*	25	deny
2	129.162.16.*	any	*.*.*.*	25	allow
3	*.*.*.*	any	184.140.18.30	25	allow
4	129.162.16.*	any	184.140.18.30	25	deny
5	129.162.16.40	any	*.*.*.*	21	allow
6	129.162.16.*	any	*.*.*.*	21	deny
7	129.162.16.*	any	184.140.18.30	21	allow
8	129.162.48.*	any	184.140.37.*	21	allow
9	*.*.*.*	any	*.*.*.*	any	deny

ภาพที่ 4.1 ตัวอย่างของกฎในไฟร์วอลล์เดี่ยว

ความผิดปกติของกฎในไฟร์วอลล์เดี่ยว (Intra-firewall anomaly) อาจจะพบได้ ถ้ากลุ่มข้อมูลเดียวกันสามารถจับคู่กันได้สำหรับกฎตั้งแต่ 2 กฎขึ้นไป ดังนั้นการแก้ไขที่เหมาะสมก็คือควรทำให้กลุ่มข้อมูลจับคู่กันได้สำหรับกฎ 1 กฎเท่านั้น ซึ่งจะได้อธิบายถึงเงื่อนไขของความผิดปกติต่างๆ ที่กล่าวไว้โดย Al-Shaer, *et al.* (2005) และงานวิจัยนี้ได้เสนอวิธีการแก้ไขความผิดปกติของกฎตามหัวข้อ 4.1.1 ดังนี้

4.1.1 เงื่อนไขและการแก้ไขความผิดปกติของกฎในไฟร์วอลล์เดี่ยว

ในงานวิจัยนี้สมมติให้กฎ (Rule) 1 กฎถูกแทนด้วยเส้นเชื่อม (Edge) เส้นเชื่อมจะถูกระบุด้วยชุดแบบอันดับ (Ordered set) w_m = (*order, src_port, dst_port, action*) โดยที่ $w_{i,m}$ คือสมาชิกตัวที่ i ของ w_m

กำหนดให้ R_x และ R_y เป็นกฎของกราฟ G ให้ w_x และ w_y เป็นชุดแบบอันดับที่ระบุบนเส้นเชื่อมของ R_x และ R_y ตามลำดับ

1. Shadowing anomaly เกิดขึ้นเมื่อกฎที่มีลำดับก่อนหน้าสามารถจับคู่ได้กับกฎที่มีลำดับหลังในทุกๆ กลุ่มข้อมูล ความผิดปกติชนิดนี้ถือเป็นข้อผิดพลาดวิกฤต (Critical error) ในนโยบาย เพราะทำให้กลุ่มข้อมูลที่ถูกปฏิเสธนั้นถูกยอมรับ ดังนั้น
R_y เป็นเงา (Shadow) ของ R_x ถ้าเป็นไปตามเงื่อนไขต่อไปนี้

$$w_{1,x} < w_{1,y} \text{ และ } w_{2,x} \neq w_{2,y} \text{ และ } R_x \Re_{\text{EM}} R_y$$
$$w_{1,x} < w_{1,y} \text{ และ } w_{2,x} \neq w_{2,y} \text{ และ } R_y \Re_{\text{IM}} R_x$$

วิธีการแก้ไขความผิดปกติ โดยทำการลบ R_y ที่เป็น Shadowed anomaly ออก เนื่องจาก $w_{1,x} < w_{1,y}$ ทำให้กลุ่มข้อมูลจับคู่ได้กับ R_x ก่อน R_y ตัวอย่างเช่น ตามภาพที่ 3.1 กฎที่มีลำดับเท่ากับ 4: 140.192.37.*, *, 161.120.33.40, 80, deny เป็นเงาของกฎที่มีลำดับเท่ากับ 3: *,*,*,*, *, 161.120.33.40, 80, allow ดังนั้นกฎที่มีลำดับเท่ากับ 4 จะถูกลบออก

2. Generalization anomaly ความผิดปกติแบบทั่วไปเกิดขึ้นระหว่าง 2 กฎใดๆ เมื่อกฎที่มีลำดับหลังสามารถจับคู่ได้กับกฎที่มีลำดับก่อนหน้าในทุกๆ กลุ่มข้อมูล โดยความผิดปกติชนิดนี้ถูกพิจารณาเป็นเพียงคำเตือน (Anomaly warning) เนื่องจากกฎที่มีลำดับหลังถือเป็นกฎย่อยของกฎที่มีลำดับก่อนหน้า โดยจะถูกใช้เพื่อยกเว้นกลุ่มข้อมูลบางกลุ่มข้อมูลที่ถูกยอมรับให้ถูกปฏิเสธโดยกฎลำดับหลัง

R_y เป็นกฎย่อยของ R_x ถ้าเป็นไปตามเงื่อนไขนี้

$$w_{1,x} < w_{1,y} \text{ และ } w_{4,x} \neq w_{4,y} \text{ และ } R_x \Re_{IM} R_y$$

วิธีการแก้ไขความผิดปกติ ไม่ต้องแก้ไขความผิดปกตินี้ ตัวอย่างเช่น ตามภาพที่ 3.1 กฎที่มีลำดับเท่ากับ 2: 140.1992.37.*, *, *.*.*.*, 80, allow เป็นกฎย่อยของกฎที่มีลำดับเท่ากับ 1: 140.192.37.20, *, *.*.*.*, 80, deny

3. Redundancy anomaly เกิดขึ้นเมื่อกฎอันหนึ่งปฏิบัติแอ็คชันเดียวกันกับกฎอีกอันหนึ่งในทุกกลุ่มข้อมูล ซึ่งความผิดปกติชนิดนี้ถูกพิจารณาเป็นข้อผิดพลาด (Error) ในนโยบาย เพราะเป็นการเพิ่มค่าใช้จ่ายอื่น (Overhead) ต่อกระบวนการกรองกลุ่มข้อมูล ทำให้สูญเสียเวลาในการกรองกลุ่มข้อมูลนี้ออก และใช้เนื้อที่ของตารางการเก็บกฎโดยไม่จำเป็น

R_y เป็นกฎซ้ำซ้อนของ R_x ถ้าเป็นไปตามเงื่อนไขนี้

$$w_{1,x} < w_{1,y} \text{ และ } w_{4,x} = w_{4,y} \text{ และ } R_x \Re_{EM} R_y$$
$$w_{1,x} < w_{1,y} \text{ และ } w_{4,x} = w_{4,y} \text{ และ } R_y \Re_{IM} R_x$$

วิธีการแก้ไขความผิดปกติ โดยทำการลบ R_y ออกไป ตัวอย่างเช่น ตามภาพที่ 3.1 กฎที่มีลำดับเท่ากับ 7: 140.192.37.*, *, 161.120.33.40, 21, allow เป็นกฎซ้ำซ้อนกับกฎที่มีลำดับเท่ากับ 6: 140.192.37.*, *, *.*.*.*, 21, allow ดังนั้นกฎที่มีลำดับเท่ากับ 7 จะถูกลบออกไป

R_x เป็นกฎซ้ำซ้อนของ R_y ถ้าเป็นไปตามเงื่อนไขต่อไปนี้

$$w_{1,x} < w_{1,y} \text{ และ } w_{4,x} = w_{4,y} \text{ และ } R_x \Re_{IM} R_y \text{ และ}$$
$$\nexists R_z: w_{1,x} < w_{1,z} < w_{1,y}, w_{4,x} \neq w_{4,z} \text{ ที่ซึ่ง } R_x \Re_{IM,C} R_z$$

4. Correlation anomaly เกิดขึ้นระหว่าง 2 กฎใดๆ ถ้ากฎที่มีลำดับก่อนหน้า จับคู่ได้กับกฎย่อยที่มีลำดับหลังสำหรับบางกลุ่มข้อมูล และกฎที่มีลำดับหลังสามารถจับคู่ได้กับกฎย่อยที่มีลำดับก่อนหน้าสำหรับบางกลุ่มข้อมูล ความผิดปกติโดยความเกี่ยวพันกัน(Correlation) ถือเป็นคำเตือน (Anomaly warning) เช่นเดียวกันกับความผิดปกติแบบทั่วไป (Generalization anomaly) แต่กฎที่ซึ่งเกี่ยวพันกัน (Correlated subgraph) เกิดจากการกำหนดแอ็คชันของกฎที่ไม่ชัดเจน
R_x และ R_y เกิดความเกี่ยวพันกัน ถ้าเป็นไปตามเงื่อนไขดังต่อไปนี้

$$w_{4,x} \neq w_{4,y} \text{ และ } R_x \Re_C R_y$$

วิธีการแก้ไขความผิดปกติ ไม่ต้องแก้ไขความผิดปกตินี้ เนื่องจากกฎทั้งสองที่เกิดความผิดปกติชนิดนี้ มีกฎย่อยหนึ่งต้องการที่จะปฏิเสธหรือยอมรับบางกลุ่มข้อมูลจากอีกกฎย่อยหนึ่ง เช่นเดียวกับในกรณีของความผิดปกติแบบทั่วไป ตัวอย่างเช่น ตามภาพที่ 3.1 กฎที่มีลำดับเท่ากับ 5: 140.192.37.30, *, *.*.*.*, 21, deny และกฎที่มีลำดับเท่ากับ 7: 140.192.37.*, *, 161.120.33.40, 21, allow เกิดความเกี่ยวพันกัน อย่างไรก็ตามความผิดปกตินี้จะถูกแก้ไขด้วยการแก้ไขความผิดปกติของกฎในไฟร์วอลล์แบบกระจายตามหัวข้อ 4.2.1 ต่อไป ทั้งนี้เพื่อให้กฎทั้งสองอยู่ในลำดับและไฟร์วอลล์ที่เหมาะสมและสอดคล้องกับนโยบายความมั่นคง

5. Irrelevance anomaly ความผิดปกติที่ไม่ได้อยู่ในประเด็นเกิดขึ้นเมื่อกฎที่อยู่ในไฟร์วอลล์เดี่ยว ไม่สามารถจับคู่กับกลุ่มข้อมูลใดเลยที่ผ่านไฟร์วอลล์นี้ กฎชนิดนี้ถูกพิจารณาเป็นความผิดปกติ เนื่องจากเป็นการเพิ่มค่าใช้จ่ายอื่น (Overhead) ให้กับกระบวนการกรองกลุ่มข้อมูลโดยไม่จำเป็น และกฎที่เกิดความผิดปกตินี้ยังไม่ก่อให้เกิดความหมายในเชิงนโยบายอีกด้วย
R_x ของไฟร์วอลล์เอฟ (F) เกิดความผิดปกติที่ไม่ได้อยู่ในประเด็น ถ้าเป็นไปตามเงื่อนไขนี้

$$F \notin \{n \mid n \text{ is a node on a path from } R_x(src\_ip) \text{ to } R_x(dst\_ip)\}$$

วิธีการแก้ไขความผิดปกติ โดยทำการลบ R_i ออกจาก F ตัวอย่างเช่น ตามภาพที่ 3.1 จะไม่ปรากฏกฎที่มีลำดับเท่ากับ 8: 140.192.38. *, 161.120.35.*, 21, allow ซึ่งเป็นกฎที่เกิดความผิดปกติที่ไม่ได้อยู่ในประเด็น กฎนี้ถูกลบออกเพราะไม่ก่อให้เกิดความหมายในเชิงนโยบาย

4.1.2 ขั้นตอนวิธีสำหรับการค้นหาและแก้ไขความผิดปกติของกฎในไฟร์วอลล์เดี่ยว

กระบวนการค้นหาและแก้ไขความผิดปกติของกฎในไฟร์วอลล์เดี่ยว (Intra-firewall anomaly discovery process) ควรถูกปฏิบัติบนกลุ่มของกฎ ก่อนการปฏิบัติกระบวนการค้นหาและแก้ไขความผิดปกติของกฎในไฟร์วอลล์แบบกระจาย (Inter-firewall anomaly discovery process) เพื่อทำให้มั่นใจว่าในแต่ละไฟร์วอลล์เดี่ยวจะไม่มีความผิดปกติใดๆ (Intra-firewall anomaly) เช่น ความผิดปกติแบบเงา (Shadowing anomaly) หรือความผิดปกติซ้ำซ้อน (Redundancy anomaly) หรือความผิดปกติที่ไม่ได้อยู่ในประเด็น (Irrelevance anomaly) เป็นต้น โดยงานวิจัยนี้ได้เสนอขั้นตอนวิธีสำหรับการค้นหาและแก้ไขความผิดปกติของกฎในไฟร์วอลล์เดี่ยวดังนี้

กำหนดให้กราฟหนึ่งกราฟใดๆ G ประกอบด้วยกฎที่มีการนิยามตามหัวข้อ 4.1.1 ให้ Gp (Group) เป็นกลุ่มของกฎในกราฟ G ที่มีค่าของ src_ip dst_ip src_port และ dst_port ที่มีความสัมพันธ์ซึ่งกันและกัน ($\Re$) (ยกตัวอย่างเช่น R_i = (129.162.*.*, any, 184.140.36.*, 21, allow), R_j = (129.162.*.*, any, 184.140.*.*, 21, deny), R_k = (129.162.16.20, any, 184.140.36.*, 21, allow) โดยที่ $(R_i \cup R_j \cup R_k) \in Gp$)) และ $Gp = \varnothing$ (เซตว่าง) สำหรับค่าเริ่มต้น

```
boolean IntraFirewallAnomalyDiscovery (Rx, Ry)
{
  if Rx or Ry is irrelevant then {return true;}
  if w4, x = w4, y then
  {
    if wI, x < wI, y then {
      for each pair of Rx and Ry do
        if Ry is redundant to Rx then {return true;}
      end for}
  }
  else
  {
    if wI, x < wI, y then {
      for each pair of Rx and Ry do
        if Ry is shadowed by Rx then {return true;}
      end for}
  }
}
```

Algorithm 1: Intra-Firewall Anomaly Discovery and Correction
Algorithm (*G*: original graph)

1. $Gp = \varnothing$
2. **for each** $R_x \in G$ **do**
3. **if** $R_x \Re g$, where any $g \in Gp$ **then** $\{Gp = Gp \cup R_x;\}$
4. **end for**
5. **for each** *Gp* **do**
6. **for** any pair (R_x, R_y) **in** *Gp* **do**
7. boolean anomalyExists =
8. **IntraFirewallAnomalyDiscovery** (R_x, R_y)
9. **if** anomalyExists = true **then** {modify R_x, R_y}
10. **end for**
11. **end for**
12. ***return*** (*G*: modified graph);

ภาพที่ 4.2 ขั้นตอนวิธีการค้นหาและแก้ไขความผิดปกติของกฎในไฟร์วอลล์เดี่ยว

ภาพที่ 4.2 แต่ละกฎ (R_x) เมื่อเราจัดกลุ่มให้กับกฎที่มีความสัมพันธ์ซึ่งกันและกัน ($\Re$) ตามคำอธิบายในหัวข้อ 3.1 ให้อยู่ในกลุ่มเดียวกันแล้ว เราจะทำการเปรียบเทียบค่าของบัพและค่าบนเส้นเชื่อมของกฎแต่ละคู่ในกลุ่ม หากพบว่าเกิดความผิดปกติกรณีใดก็ตามดังเงื่อนไขในหัวข้อ 4.1.1 ให้ทำการแก้ไขความผิดปกตินั้นทันที และทำเช่นนี้ไปเรื่อยๆ จนกระทั่งกฎต่างๆ ในแต่ละกลุ่มไม่พบความผิดปกติที่ต้องแก้ไขจึงจบกระบวนการค้นหาและแก้ไขความผิดปกติของกฎในไฟร์วอลล์เดี่ยว

ตัวอย่างให้พิจารณาตามภาพที่ 3.1 เราจะได้ว่ากลุ่มของกฎที่มีความสัมพันธ์ซึ่งกันและกัน ได้แก่ กฎที่มีลำดับ 1-4 จากนั้นให้ทำการเปรียบเทียบระหว่างกฎแต่ละคู่ในกลุ่ม ซึ่งได้แก่ (1, 2), (1, 3), (1, 4), (2, 3), (2, 4) และ (3, 4) ตามลำดับ ถ้าในขณะที่ทำการเปรียบเทียบแล้วพบความผิดปกติที่ต้องแก้ไขก็ให้แก้ไขความผิดปกตินั้นๆ ทันที แต่ถ้าพบหรือไม่พบความผิดปกติที่ไม่ต้องแก้ไขก็ให้หยุดการเปรียบเทียบระหว่างกฎทั้งสองนั้น

เมื่อเราปฏิบัติตามขั้นตอนวิธีที่ 1 เราจะได้กลุ่มของกฎแบบใหม่ (Modified Graph) เพื่อทำให้เกิดความมั่นใจว่ากฎแบบใหม่ที่ได้มานั้นไม่มีผลต่อนโยบายความมั่นคง ในทฤษฎีบทตามหัวข้อที่ 4.1.3 เราจะแสดงว่านโยบายของไฟร์วอลล์เดี่ยวที่ซึ่งปฏิบัติตามขั้นตอนวิธีที่ 1 นั้นไม่เปลี่ยนแปลง และยังช่วยลดจำนวนของกฎในไฟร์วอลล์อีกด้วย

4.1.3 ทฤษฎีบท

ทฤษฎีบท 1 เพื่อแสดงว่าขั้นตอนวิธีที่ 1 ไม่เปลี่ยนแปลงความหมายของนโยบายความมั่นคง โดยเราจะแสดงว่านโยบายของกลุ่มของกฎที่ถูกแก้ไขความผิดปกติไม่เปลี่ยนแปลง

ทฤษฎีบท 1: ภายในแต่ละไฟร์วอลล์ จำนวนของกฎที่ถูกปรับปรุงโดยขั้นตอนวิธีที่ 1 ใน Modified Graph ของ G จะน้อยกว่าหรือเท่ากับ จำนวนของกฎใน Original Graph ของ G และถ้าทุกๆ กลุ่มข้อมูลถูกยอมรับหรือปฏิเสธโดยกฎแบบเดิม แล้วจะได้ว่าทุกๆ กลุ่มข้อมูลเดียวกันถูกยอมรับหรือปฏิเสธโดยกฎแบบใหม่ด้วย

พิสูจน์ : เราสมมติว่า N และ N´ แทนจำนวนของกฎแบบเดิม และกฎแบบใหม่ ตามลำดับ โดยที่ N, N´∈ ℵ และ G แทนกราฟที่ซึ่งมีกฎแบบเดิม และ G' แทนกราฟที่ซึ่งมีกฎแบบใหม่

ให้ P (a) แทนข้อความที่ว่า "สำหรับทุกๆ กลุ่มข้อมูลที่เดินทางผ่าน G ถูกยอมรับ"
P (a´) แทนข้อความที่ว่า "สำหรับทุกๆ กลุ่มข้อมูลที่เดินทางผ่าน G' ถูกยอมรับ"
P (d) แทนข้อความที่ว่า "สำหรับทุกๆ กลุ่มข้อมูลที่เดินทางผ่าน G ถูกปฏิเสธ"
P (d´) แทนข้อความที่ว่า "สำหรับทุกๆ กลุ่มข้อมูลที่เดินทางผ่าน G' ถูกปฏิเสธ"

เราจะแสดงว่า

1. กราฟ G เดียวกัน N´≤ N เมื่อ N, N´∈ ℵ
2. ถ้า P (a) แล้วจะได้ว่า P (a´)
3. ถ้า P (d) แล้วจะได้ว่า P (d´)

พิสูจน์ 1:

กรณีที่ 1: ไม่เกิดความผิดปกติ เราไม่มีการเปลี่ยนแปลงกฎแบบเดิมภายในกราฟ G ดังนั้น N´ = N

กรณีที่ 2: เกิดความผิดปกติ สำหรับกรณีนี้ความผิดปกติมี 5 แบบและมีวิธีแก้ไขดังนี้

1. Redundancy anomaly เพราะว่า Redundant Rule ถูกลบออก ทำให้จำนวนของกฎลดลง ดังนั้น N´< N

2. Shadowing anomaly เพราะว่า Shadowed Rule ถูกลบออก ทำให้จำนวนของกฎลดลง ดังนั้น $N' < N$

3. Generalization anomaly เพราะว่าไม่มีการแก้ไขความผิดปกตินี้ ดังนั้น $N' = N$

4. Correlation anomaly เพราะว่าไม่มีการแก้ไขความผิดปกตินี้ ดังนั้น $N' = N$

5. Irrelevance anomaly เพราะว่า Irrelevant Rule ถูกลบออก ทำให้จำนวนของกฎลดลง ดังนั้น $N' < N$

ดังนั้น ในทุกกรณีภายในกราฟ G เดียวกันเราได้ว่า $N' \leq N$ เมื่อ $N, N' \in \mathbb{N}$

พิสูจน์ 2: เราจะพิสูจน์ (2) โดยใช้ Trivial proof เราสมมติว่า P (a) เป็นจริง นั่นคือสมมติว่าสำหรับทุกๆ กลุ่มข้อมูลที่เดินทางผ่าน G ถูกยอมรับ เราจะแสดงว่า P (a´) เป็นจริง นั่นคือจะต้องแสดงว่า สำหรับทุกๆ กลุ่มข้อมูลที่เดินทางผ่าน G' ถูกยอมรับ ดังนี้

กรณีที่ 1: ไม่เกิดความผิดปกติ ภายในกราฟ G เราไม่มีการเปลี่ยนแปลงกฎแบบเดิม ดังนั้น P (a´) เป็นจริง

กรณีที่ 2: เกิดความผิดปกติ สำหรับกรณีนี้ความผิดปกติมี 5 แบบและมีวิธีแก้ไขดังนี้

1. Redundancy anomaly เพราะว่า Redundant Rule ถูกลบออก ทำให้ได้ว่ากลุ่มข้อมูลยังคงถูกยอมรับด้วยกราฟย่อยที่เป็นซูเปอร์เซตของ Redundant subgraph ดังนั้น P (a´) เป็นจริง

2. Shadowing anomaly เพราะว่า Shadowed Rule ที่มีแอ็คชันเท่ากับ "deny" ($w_{3,i}$ = deny) ถูกลบออก ในขณะที่กราฟย่อยที่มีแอ็คชันเท่ากับ "allow" ($w_{4,i}$ = allow) ยังอยู่ ดังนั้น P (a´) เป็นจริง

3. Generalization anomaly เพราะว่าไม่มีการแก้ไขใดๆ ดังนั้น P (a´) เป็นจริง

4. Correlation anomaly เพราะว่าไม่มีการแก้ไขใดๆ ดังนั้น P (a´) เป็นจริง

5. Irrelevance anomaly เพราะว่า Irrelevant Rule ถูกลบออก ดังนั้น P (a´) เป็นจริง

จะเห็นว่าในกรณีที่ 2 เมื่อแก้ไขความผิดปกติแล้ว P (a´) เป็นจริง

โดยทั้ง 2 กรณี เราได้แสดงว่า P (a´) เป็นจริง นั่นคือ สำหรับทุกๆ กลุ่มข้อมูลที่เดินทางผ่าน G' ถูกยอมรับ จากสมมติฐานที่ว่า P (a) เป็นจริง ดังนั้น พิสูจน์ (2) เสร็จสมบูรณ์

พิสูจน์ 3: เราจะพิสูจน์ (3) โดยใช้ Trivial proof เช่นเดียวกับ **พิสูจน์** (2) เราสมมติว่า P (d) เป็นจริง นั่นคือสมมติว่า สำหรับทุกๆ กลุ่มข้อมูลที่เดินทางผ่าน G ถูกปฏิเสธ เราจะแสดงว่า P (d´) เป็นจริง นั่นคือจะต้องแสดงว่า สำหรับทุกๆ กลุ่มข้อมูลที่เดินทางผ่าน G´ ถูกปฏิเสธ ดังนี้

กรณีที่ 1: ไม่เกิดความผิดปกติ ภายในกราฟ G เราไม่มีการเปลี่ยนแปลงกฎแบบเดิม ดังนั้น P (d´) เป็นจริง

กรณีที่ 2: เกิดความผิดปกติ สำหรับกรณีนี้ความผิดปกติมี 5 แบบและมีวิธีแก้ไขดังนี้

1. Redundancy anomaly เพราะว่า Redundant Rule ถูกลบออก ทำให้ได้ว่ากลุ่มข้อมูลยังคงถูกปฏิเสธด้วยกฎที่เป็นซูเปอร์เซตของ Redundant Rule ดังนั้น P (d´) เป็นจริง

2. Shadowing anomaly เพราะว่า Shadowed Rule ที่มีแอ็คชันเท่ากับ "allow" ($w_{4,1}$ = allow) ถูกลบออก ทำให้กฎที่มีแอ็คชันเท่ากับ "deny" ($w_{4,1}$ = deny) ยังอยู่ ดังนั้น P (d´) เป็นจริง

3. Generalization anomaly เพราะว่าไม่มีการแก้ไขใดๆ ดังนั้น P (d´) เป็นจริง

4. Correlation anomaly เพราะว่าไม่มีการแก้ไขใดๆ ดังนั้น P (d´) เป็นจริง

5. Irrelevance anomaly เพราะว่า Irrelevant Rule ถูกลบออก ดังนั้น P (d´) เป็นจริง

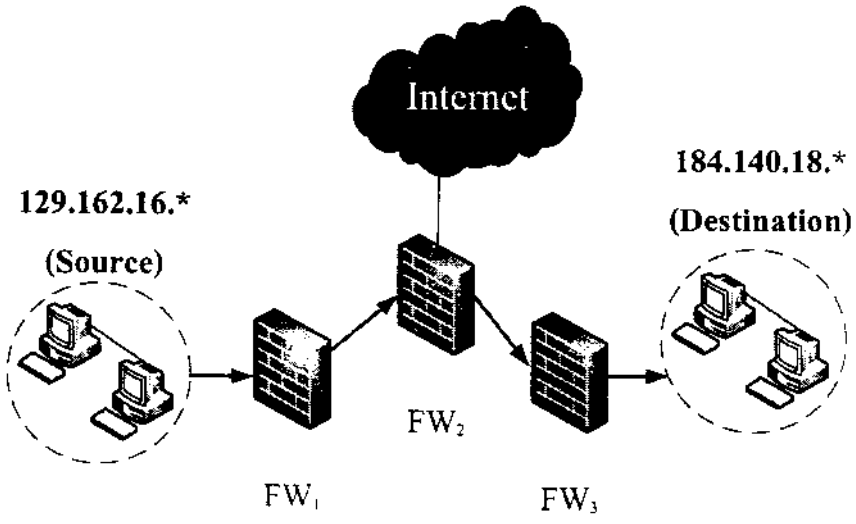
จะเห็นว่าในกรณีที่ 2 เมื่อแก้ไขความผิดปกติแล้ว P (d´) เป็นจริง

โดยทั้ง 2 กรณี เราได้แสดงว่า P (d´) เป็นจริง จากสมมติฐานที่ว่า P (d) เป็นจริง ดังนั้น พิสูจน์ (3) เสร็จสมบูรณ์

จากการพิสูจน์ใน ทฤษฎีบท 1 ตามหัวข้อ 4.1.3 ทำให้ได้ว่าจำนวนของกฎแบบใหม่ น้อยกว่าหรือเท่ากับ จำนวนของกฎแบบเดิม และการใช้ขั้นตอนวิธีนี้ยังทำให้เรามั่นใจได้ว่านโยบายของไฟร์วอลล์ไม่เปลี่ยนแปลง นั่นคือถ้ากลุ่มข้อมูลถูกยอมรับโดยกฎแบบเดิมแล้วกลุ่มข้อมูลเหล่านั้นก็ยังถูกยอมรับด้วยกฎแบบใหม่ และถ้ากลุ่มข้อมูลถูกปฏิเสธโดยกฎแบบเดิมแล้วกลุ่มข้อมูลเหล่านั้นจะถูกปฏิเสธด้วยกฎแบบใหม่ที่อยู่ในกราฟเดียวกันด้วย ดังนั้นจึงกล่าวได้ว่าขั้นตอนวิธีที่ 1 สามารถช่วยลดความคลุมเครือของกฎต่างๆ ในไฟร์วอลล์เดียวได้ และยังทำให้นโยบายความมั่นคงมีความชัดเจนยิ่งขึ้น

4.2 กฎในไฟร์วอลล์แบบกระจาย (Inter-firewall rule / Distributed firewall rule)

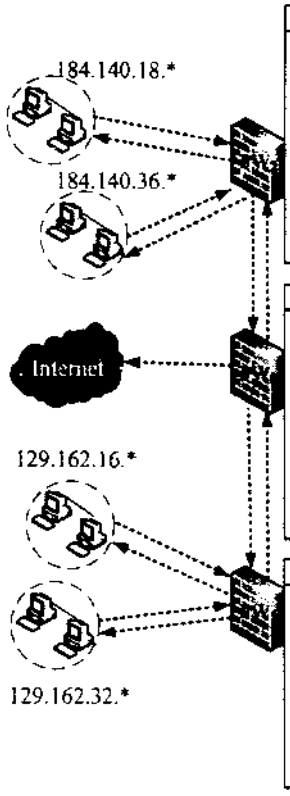
ภายในเครือข่ายหนึ่งๆ มีหลายโดเมนย่อยที่ต้องติดต่อซึ่งกันและกัน ทำให้ระหว่างโดเมนย่อยใดๆ อาจมีไฟร์วอลล์มากกว่า 1 ไฟร์วอลล์ ดังนั้นอาจทำให้เกิดความผิดปกติระหว่างไฟร์วอลล์ (Inter-firewall anomaly) ขึ้นได้ ถ้าไฟร์วอลล์ 2 ตัวใดๆ บนเส้นทางเครือข่าย (Network path) เดียวกันทำการกรองกลุ่มข้อมูลด้วยแอ็คชันที่ต่างกัน ดังนั้นวิธีแก้ไขที่เหมาะสมก็คือควรจัดสรรกฎไว้ในลำดับหรือไฟร์วอลล์ที่เหมาะสมกับกฎเหล่านั้น เพื่อไม่ให้เกิดการขัดแย้งกันเองระหว่างกฎในแต่ละไฟร์วอลล์



ภาพที่ 4.3 เครือข่ายที่มีไฟร์วอลล์แบบกระจาย

ภาพที่ 4.3 จะเห็นว่าไฟร์วอลล์เดี่ยว (FW) แต่ละตัวมีการเชื่อมโยงกัน ถ้าเราสมมติให้การเดินทางของกลุ่มข้อมูลเดินทางจากต้นทาง (Source) ไปยังปลายทาง (Destination) สามารถผ่านไฟร์วอลล์หลายๆ ตัวที่เชื่อมต่อกันได้บน Network path เดียวกัน โดยระหว่างคู่ของต้นทางและปลายทางใดๆ FW ที่มาก่อนเราเรียกว่าไฟร์วอลล์สู่เครื่องบริการ (Upstream firewall) และ FW ที่มาหลังเราเรียกว่าไฟร์วอลล์สู่ผู้ใช้ (Downstream firewall) และ FW ที่ใกล้ต้นทางที่สุด เราจะเรียกว่าไฟร์วอลล์สู่เครื่องบริการที่ใกล้ที่สุด (Most-upstream firewall (FW_1)) และ FW ที่ใกล้ปลายทางที่สุด เราเรียกว่าไฟร์วอลล์สู่ผู้ใช้ที่ใกล้ที่สุด (Most-downstream firewall (FW_n)) พิจารณาตัวอย่างกฎ

ต่างๆ ของไฟร์วอลล์แบบกระจาย ตามภาพที่ 4.4 กฎแต่ละกฎของไฟร์วอลล์จะถูกแทนด้วยเส้นเชื่อมดังเช่นภาพที่ 3.3



Order	Src_ip	Src_port	Dst_ip	Dst_port	Action
1	184.140.*.*	any	129.162.*.*	80	allow
2	184.140.*.*	any	129.162.16.1	21	deny
3	184.140.*.*	any	129.162.*.*	21	allow
4	129.162.*.*	any	184.140.36.*	23	allow
5	184.140.36.*	any	129.162.*.*	23	allow
6	184.140.18.*	any	129.162.32.1	25	deny
7	184.140.18.*	any	129.162.16.3	25	deny
8	184.140.*.*	any	129.162.32.*	25	allow
9	*.*.*.*	any	*.*.*.*	any	deny

Order	Src_ip	Src_port	Dst_ip	Dst_port	Action
1	129.162.*.*	any	184.140.*.*	25	allow
2	*.*.*.*	any	129.162.*.*	25	allow
3	184.140.*.*	any	*.*.*.*	80	allow
4	129.162.*.*	any	184.140.*.*	80	deny
5	184.140.36.*	any	129.162.32.5	23	deny
6	184.140.*.*	any	129.162.*.*	22	deny
7	129.162.*.*	any	184.140.*.*	any	allow
8	184.140.*.*	any	129.162.*.*	any	allow
9	*.*.*.*	any	*.*.*.*	any	deny

Order	Src_ip	Src_port	Dst_ip	Dst_port	Action
1	184.140.*.*	any	129.162.*.*	80	allow
2	129.162.*.*	any	184.140.*.*	80	allow
3	184.140.*.*	any	129.162.16.1	21	allow
4	184.140.36.*	any	129.162.32.*	23	deny
5	184.140.*.*	any	129.162.*.*	23	allow
6	184.140.18.*	any	129.162.32.1	25	deny
7	184.140.18.*	any	129.162.*.*	25	allow
8	*.*.*.*	any	*.*.*.*	any	deny

ภาพที่ 4.4 ตัวอย่างกฎต่างๆ ของไฟร์วอลล์แบบกระจาย

เงื่อนไขของความผิดปกติของกฎในไฟร์วอลล์แบบกระจายตามหัวข้อที่ 4.2.1 แสดงถึงความผิดปกติของกฎที่เป็นไปได้ทั้งหมดที่ซึ่งอาจมีอยู่ระหว่างนโยบายความมั่นคงของไฟร์วอลล์ 2 ตัวใดๆ ซึ่งถูกกล่าวไว้โดย Al-Shaer, *et al.* (2005) และงานวิจัยนี้ได้เสนอวิธีการแก้ไขความผิดปกติของกฎในไฟร์วอลล์แบบกระจายไว้ตามหัวข้อ 4.2.1 ดังนี้

4.2.1 เงื่อนไขและการแก้ไขความผิดปกติของกฎในไฟร์วอลล์แบบกระจาย

ในงานวิจัยนี้สมมติให้กฎ (Rule) 1 กฎถูกแทนด้วยเส้นเชื่อม (Edge) เส้นเชื่อมจะถูกระบุด้วยชุดแบบอันดับ (Ordered set) w_m = (*order, src_port, dst_port, firewall identification* (F_y), *action*) โดยที่ $w_{i,m}$ คือ สมาชิกตัวที่ i ของ w_m

ให้ R_u, R_u', R_d และ R_d' เป็นกฎในกราฟ G เมื่อ R_u และ R_u' เป็นกฎของ Upstream firewall และ R_d และ R_d' เป็นกฎของ Downstream firewall ให้ w_u, w_u', w_d และ w_d' เป็นชุดแบบอันดับที่ถูกระบุบนเส้นเชื่อมของ R_u, R_u', R_d และ R_d' ตามลำดับ

1. Shadowing anomaly เกิดขึ้นถ้า Upstream firewall ปฏิเสธกลุ่มข้อมูลที่ถูกยอมรับโดย Downstream firewall
R_d เป็นเงา (Shadow) ของ R_u ถ้าเป็นไปตามเงื่อนไขดังต่อไปนี้

$$w_{5,u} = \text{deny และ } w_{5,d} = \text{allow และ } R_u \, \Re_{EM} \, R_d \tag{1.1}$$

วิธีการแก้ไขความผิดปกติ โดยให้คง R_u ไว้ที่ Upstream firewall และลบ R_d ที่เป็นกฎเงา (Shadowed Rule) ใน Downstream firewall เพราะว่ากลุ่มข้อมูลที่จับคู่กันได้ทั้ง R_u และ R_d ถูกปฏิเสธที่ Upstream firewall ที่เดียว เราจึงสามารถลบ R_d ออกได้ ตัวอย่างเช่น ตามภาพที่ 3.3 กฎย่อยที่ (2/FW_2: 161.120.*.*, *, 140.192.22.5, 21, deny และ 3/FW_1: 161.120.*.*, *, 140.192.22.5, 21, allow) เราจะลบ 3/FW_1 ที่ซึ่งเป็นกฎเงาออก

$$w_{5,u} = \text{deny และ } w_{5,d} = \text{allow และ } R_d \, \Re_{IM} \, R_u \tag{1.2}$$

วิธีการแก้ไขความผิดปกติ ทำเช่นเดียวกับหัวข้อย่อย (1.1) ตัวอย่างเช่น ตามภาพที่ 3.3 กฎที่ (8/FW_2: *.*.*.*, *. *.*.*.*, *, deny และ 4/FW_2: 140.192.*.*. *. 161.120.33.*, 23, allow) ให้ลบกฎย่อย 4/FW_2 ออกจาก FW_2

$$w_{5,u} = \text{deny และ } w_{5,d} = \text{allow และ } R_u \, \Re_{IM} \, R_d \tag{1.3}$$

วิธีการแก้ไขความผิดปกติ ไม่ต้องแก้ไขความผิดปกตินี้ (อยู่ในกรณี Generalization) ตัวอย่างเช่น ตามภาพที่ 3.3 กฎที่ (7/FW_2: 161.120.24.*, *, 140.192.22.5, 25, deny และ 7/FW_1: 161.120.24.*. *. 140.192.*.*, 25, allow) โดยกฎ 7/FW_1 เป็นกฎทั่วไป (General Rule) ของ 7/FW_2

$w_{5,u}$ = allow และ $w_{5,d}$ = allow และ $R_u \Re_{IM} R_d$ และ (1.4)
$\exists R_u' : w_{5,u}'$ = deny โดยที่ $R_u \Re_{IM,C} R_u'$

วิธีการแก้ไขความผิดปกติ โดยเปลี่ยน R_d ให้เหมือนกับ R_u เพราะมีเพียงกลุ่มข้อมูลที่จับคู่ได้กับ R_u เท่านั้นที่ถูกยอมรับ ตัวอย่างเช่น ตามภาพที่ 3.3 กฎที่ (5/FW_2: 161.120.33.*, *, 140.192.*.*, 23, allow และ 7/FW_0: 161.120.*.*, *, 140.192.*.*, *, allow) ให้เปลี่ยนกฎ 7/FW_0 ให้เหมือนกฎ 5/FW_2

2. Spuriousness anomaly เกิดขึ้นถ้า Upstream firewall ยอมรับกลุ่มข้อมูลที่ถูกปฏิเสธโดย Downstream firewall
R_u ยอมให้กลุ่มข้อมูลปลอม (Spurious packet) ไปยัง R_d ถ้าเป็นไปตามเงื่อนไขดังต่อไปนี้

$w_{5,u}$ = allow และ $w_{5,d}$ = deny และ $R_u \Re_{EM} R_d$ (2.1)

วิธีการแก้ไขความผิดปกติ โดยให้คง R_d ไว้ที่ Downstream firewall และลบ R_u ที่ Upstream firewall เพราะว่าเราต้องการบล็อก (Block) กลุ่มข้อมูลที่จับคู่ได้กับ R_u หรือ R_d ที่ Upstream firewall ด้วยกฎโดยปริยาย (Default Rule) ตัวอย่างเช่น ตามภาพที่ 3.3 กฎที่ (2/FW_1: 140.192.*.*, *, 161.120.*.*, 80, allow และ 4/FW_0: 140.192.*.*, *, 161.120.*.*, 80, deny) เราจะลบกฎที่ 2/FW_1 ออก

$w_{5,u}$ = allow และ $w_{5,d}$ = deny และ $R_u \Re_{IM} R_d$ (2.2)

วิธีการแก้ไขความผิดปกติ ทำเช่นเดียวกับหัวข้อย่อย (2.1) ตัวอย่างเช่น ตามภาพที่ 3.3 กฎที่ (2/FW_1: 140.192.*.*, *, 161.120.*.*, 80, allow และ 9/FW_2: *.*.*.*, *, *.*.*.*, *, deny) เราจะลบกฎ 2/FW_1 ออก

$w_{5,u}$ = allow และ $w_{5,d}$ = deny และ $R_d \Re_{IM} R_u$ (2.3)

วิธีการแก้ไขความผิดปกติ โดยเพิ่ม R_d ที่ Upstream firewall โดยลำดับอยู่ก่อนหน้า R_u และลบ R_d ที่ Downstream firewall เพราะว่าเราต้องการบล็อกเฉพาะกลุ่มข้อมูลที่จับคู่ได้กับ R_d ที่ Upstream firewall ตัวอย่างเช่น ตามภาพที่ 3.3 กฎที่ ($5/FW_2$: 161.120.33.*, *, 140.192.*.*, 23, allow และ $5/FW_0$: 161.120.33.*, *, 140.192.37.1, 23, deny) เราจะเพิ่มกฎ $5/FW_0$ ที่ Upstream firewall วางไว้ลำดับก่อนหน้ากฎ $5/FW_2$ ทำให้ได้ว่ากฎ $5/FW_2$ เป็นกฎทั่วไป (General Rule) ของกฎ $5/FW_0$ และลบ $5/FW_0$ ที่ Downstream firewall ออก

$$w_{5,u} = \text{allow และ } w_{5,d} = \text{allow และ } R_d \,\Re_{\text{IM}}\, R_u \text{ และ} \qquad (2.4)$$
$$\exists R_d' : w_{5,d}' = \text{deny โดยที่ } R_d \,\Re_{\text{IM,C}}\, R_d'$$

วิธีการแก้ไขความผิดปกติ โดยเปลี่ยน R_u ให้เหมือนกับ R_d เพราะว่ากลุ่มข้อมูลที่จับคู่ได้กับ R_d เท่านั้นที่ถูกยอมรับ ตัวอย่างเช่น ตามภาพที่ 3.3 กฎที่ ($3/FW_0$: *.*.*.*, *, 140.192.*.*, 25, allow และ $7/FW_1$: 161.120.24.*, *, 140.192.*.*, 25, allow) ให้เปลี่ยนกฎที่ $3/FW_0$ ให้เหมือนกฎที่ $7/FW_1$

$$w_{5,u} = \text{deny และ } w_{5,d} = \text{deny และ } R_u \,\Re_{\text{IM}}\, R_d \text{ และ} \qquad (2.5)$$
$$\exists R_u' : w_{5,u}' = \text{allow โดยที่ } R_u \,\Re_{\text{IM,C}}\, R_u' \text{ และ}$$
$$R_d \,\Re_{\text{EM,IM}}\, R_u' \text{ หรือ } R_u' \,\Re_{\text{IM}}\, R_d$$

วิธีการแก้ไขความผิดปกติ โดยนำ R_d ไว้แทนที่ R_u และลบ R_d ที่ Downstream firewall เพราะว่าเราต้องการบล็อกกลุ่มข้อมูลที่จับคู่ได้กับ R_u และ R_d ที่ Upstream firewall ตัวอย่างเช่น ตามภาพที่ 3.3 กฎที่ ($5/FW_0$: 161.120.33.*, *, 140.192.37.1, 23, deny และ $4/FW_1$: 161.120.33.*, *, 140.192.37.*, 23, deny) ให้นำกฎที่ $4/FW_1$ ไปแทนที่กฎที่ $5/FW_1$ และลบกฎที่ $4/FW_1$ ที่ Downstream firewall

3. Redundancy anomaly เกิดขึ้นถ้า Downstream firewall ปฏิเสธกลุ่มข้อมูลที่ถูกปฏิเสธเรียบร้อยแล้วด้วย Upstream firewall
R_d เป็นกฎซ้ำซ้อน (Redundant Rule) ของ R_u ถ้าเป็นไปตามเงื่อนไขดังต่อไปนี้

$w_{5,u}$ = deny และ $w_{5,d}$ = deny และ $R_d \, \Re_{EM} \, R_u$ (3.1)

วิธีการแก้ไขความผิดปกติ โดยให้คง R_u ไว้ที่ Upstream firewall และลบ R_d ที่เป็น Redundant Rule ที่ Downstream firewall เพราะกลุ่มข้อมูลจับคู่ได้กับ R_u และ R_d จะถูกปฏิเสธที่ Upstream firewall อยู่แล้ว เราจึงสามารถลบ R_d ได้ ตัวอย่างเช่น ตามภาพที่ 3.3 กฎที่ ($6/FW_2$: 161.120.24.*, *, 140.192.37.3, 25, deny และ $6/FW_1$: 161.120.24.*, *, 140.192.37.3, 25, deny) ให้ลบกฎที่ $6/FW_1$ ออก

$w_{5,u}$ = deny และ $w_{5,d}$ = deny และ $R_d \, \Re_{IM} \, R_u$ (3.2)

วิธีการแก้ไขความผิดปกติ ทำเช่นเดียวกับหัวข้อย่อย (3.1) ตัวอย่างเช่น ตามภาพที่ 3.3 กฎที่ ($9/FW_2$: *.*.*.*, *, *.*.*.*, *, deny และ $6/FW_0$: 161.120.*.*, *, 140.192.*.*, 22, deny) ให้ลบกฎที่ $6/FW_0$ ออก

4. Correlation anomaly เกิดขึ้นจากกฎ 2 กฎเกิดความเกี่ยวพันกัน (Correlation) ใน Upstream firewall และ Downstream firewall โดยก่อนหน้านี้ในหัวข้อ 4.1.1 เราได้อธิบายถึงเงื่อนไขและการแก้ไขกฎที่เกิด Correlation กันที่มีแอ็คชันต่างกัน แต่สำหรับกรณีของ Inter-firewall anomaly นี้กฎที่เกิด Correlation กันจะมีแอ็คชันทั้งที่ต่างกันและเหมือนกัน ความผิดปกติชนิดนี้นอกจากจะทำให้เกิดความคลุมเครือระหว่างไฟร์วอลล์แล้วยังทำให้เกิดความผิดปกติอื่นๆ ได้อีก เช่นความผิดปกติแบบเงา (Shadowing anomaly) หรือความผิดปกติแบบปลอม (Spurious anomaly) เป็นต้น ดังนั้นเฉพาะกรณีนี้เราจึงนำสนอการแก้ไข ที่ไม่ทำให้เกิดความผิดปกติชนิดอื่นๆ ตามมา

R_u และ R_d เกิดความเกี่ยวพันกันขึ้น ถ้าเป็นไปตามเงื่อนไขดังต่อไปนี้

กำหนดให้ R_j เป็น Correlative conjunction ของ R_u และ R_d

$w_{5,u}$ = allow และ $w_{5,d}$ = allow และ $R_u \, \Re_C \, R_d$ และ (4.1)

$\exists R_u' : w_{5,u}'$ = deny โดยที่ $R_u \, \Re_{IM,C} \, R_u'$ และ

$\exists R_d' : w_{5,d}'$ = deny โดยที่ $R_d \, \Re_{IM,C} \, R_d'$

ให้ R_j : *129.162.32.*, any, 184.140.36.*, 25, allow*

วิธีการแก้ไขความผิดปกติ โดยนำ R_i ที่มีแอ็คชันเป็น "allow" ($w_{5,i}$ = allow) ไปวางไว้แทนที่ทั้ง R_u และ R_d เพราะมีเพียงกลุ่มข้อมูลที่จับคู่ได้กับ R_i เท่านั้นถูกยอมรับ ตัวอย่างเช่น

R_u : *129.162.*.*, any, 184.140.36.*, 25, allow*

R_u': **.*.*.*, any, *.*.*.*, any, deny*

R_d : *129.162.32.*, any, 184.140.*.*, 25, allow*

R_d': **.*.*.*, any, *.*.*.*, any, deny*

เพราะว่ากลุ่มข้อมูลอื่นๆ ที่ไปยังปลายทาง 184.140.*.* ไม่รวม 184.140.36.* จะถูกบล็อกด้วย R_u' ที่ Upstream firewall ในขณะที่มีเพียงกลุ่มข้อมูลที่มาจาก 129.162.*.* และไปยังปลายทาง 184.140.36.* สามารถไปถึง Downstream firewall ได้ ส่วนกลุ่มข้อมูลที่เหลือถูกปฏิเสธโดย R_d' ที่ Downstream firewall เช่นกัน

$w_{5,u}$ = deny และ $w_{5,d}$ = deny และ $R_u \,\Re_C\, R_d$ และ (4.2)

$\exists R_u' : w_{5,u}'$ = allow โดยที่ $R_u \,\Re_{IM,C}\, R_u'$ และ

$\exists R_d' : w_{5,d}'$ = allow โดยที่ $R_d \,\Re_{IM,C}\, R_d'$

ให้ R_i : *129.162.32.*, any, 184.140.36.*, 25, deny*

วิธีการแก้ไขความผิดปกติ ไม่ต้องแก้ไขความผิดปกตินี้ ตัวอย่างเช่น

R_u : *129.162.*.*, any, 184.140.36.*, 25, deny*

R_u': *129.162.*.*, any, 184.140.*.*, 25, allow*

R_d : *129.162.32.*, any, 184.140.*.*, 25, deny*

R_d' : *129.162.*.*, any, 184.140.*.*, 25, allow*

ถ้าเราแก้ปัญหาแบบเดียวกับหัวข้อย่อย (4.1) จะทำให้นโยบายของไฟร์วอลล์เปลี่ยนแปลง เพราะจะมีเพียงกลุ่มข้อมูลที่จับคู่ได้กับ R_i ถูกบล็อก ส่วนกลุ่มข้อมูลอื่นๆ จะถูกยอมรับโดยผ่าน R_u' ที่ Upstream firewall และ R_d' ที่ Downstream firewall ซึ่งขัดแย้งกัน

$w_{5,u}$ = allow และ $w_{5,d}$ = deny และ $R_u \, \Re_C \, R_d$ (4.3)

ให้ R_i : *129.162.32.*, any, 184.140.36.*, 25, deny*

วิธีการแก้ไขความผิดปกติ โดยเพิ่ม R_d ที่ Upstream firewall วางไว้โดยลำดับอยู่ก่อนหน้า R_u และลบ R_d ที่ Downstream firewall ดังนั้นกลุ่มข้อมูลที่จับคู่ได้กับ R_i หรือ R_d จะถูกบล็อกที่ Upstream firewall ตัวอย่างเช่น

R_u : *129.162.*.*, any, 184.140.36.*, 25, allow*

R_d : *129.162.32.*, any, 184.140.*.*, 25, deny*

เพราะว่าถ้าเราเพิ่ม R_i ไว้ที่ Upstream firewall แทนที่จะเป็น R_d แล้วจะทำให้เกิด Spuriousness anomaly ตามหัวข้อย่อย (2.5) ระหว่าง R_i ที่ Upstream firewall และ R_d ที่ Downstream firewall

$w_{5,u}$ = deny และ $w_{5,d}$ = allow และ $R_u \, \Re_C \, R_d$ (4.4)

ให้ R_i : *129.162.32.*, any, 184.140.36.*, 25, allow*

วิธีการแก้ไขความผิดปกติ ไม่ต้องแก้ไขความผิดปกตินี้ ตัวอย่างเช่น

R_u : *129.162.*.*, any, 184.140.36.*, 25, deny*

R_d : *129.162.32.*, any, 184.140.*.*, 25, allow*

ถ้าเราเพิ่ม R_i ที่ Upstream firewall วางไว้ลำดับก่อนหน้า R_u แล้วจะทำให้เกิด Shadowing anomaly ตามหัวข้อย่อย (1.4) และถ้าเราเพิ่ม R_d ที่ Upstream firewall แทน R_i จะทำให้เกิด Correlation anomaly ตามหัวข้อย่อย (4.3)

4.2.2 ขั้นตอนวิธีสำหรับการค้นหาและแก้ไขความผิดปกติของกฎในไฟร์วอลล์แบบกระจาย

กระบวนการค้นหาความผิดปกติระหว่างไฟร์วอลล์ หรือไฟร์วอลล์แบบกระจาย (Inter-firewall anomaly discovery process) ควรถูกปฏิบัติในแต่ละเส้นทางเครือข่าย (Network path) ที่เชื่อม 2 โดเมนย่อยใดๆ โดยงานวิจัยนี้ได้เสนอขั้นตอนวิธีสำหรับการค้นหาและแก้ไขความผิดปกติของกฎในไฟร์วอลล์แบบกระจายดังต่อไปนี้

เรากำหนดให้ R_u และ R_d เป็นกฎตามการนิยามในหัวข้อ 4.2.1ของ Upstream firewall และ Downstream firewall ตามลำดับ

ให้ R_i คือกฎของนโยบายความมั่นคงที่ยังไม่ได้ถูกแก้ไขความผิดปกติ และR_j คือกฎของนโยบายความมั่นคงที่ถูกแก้ไขความผิดปกติแล้ว และ F_u คือไฟร์วอลล์ที่อยู่ใกล้ต้นทางมากที่สุด (The most upstream firewall) และF_{u+1} คือไฟร์วอลล์ตัวแรกที่เชื่อมต่อกับ F_u และ F_{u+2} คือไฟร์วอลล์ตัวที่ 2 ที่เชื่อมต่อกับ F_u และไปเรื่อยๆ จนถึง F_d คือไฟร์วอลล์ที่อยู่ใกล้ปลายทางมากที่สุด (The most downstream firewall) สมมติให้

$G_I = \{R_1 \cup R_2 \cup ... \cup R_i\}$ แทนกราฟกฎของไฟร์วอลล์เริ่มต้น (An input graph)

$G_O = \{R_1 \cup R_2 \cup ... \cup R_j\}$ แทนกราฟกฎของไฟร์วอลล์ผลลัพธ์ (An output graph)

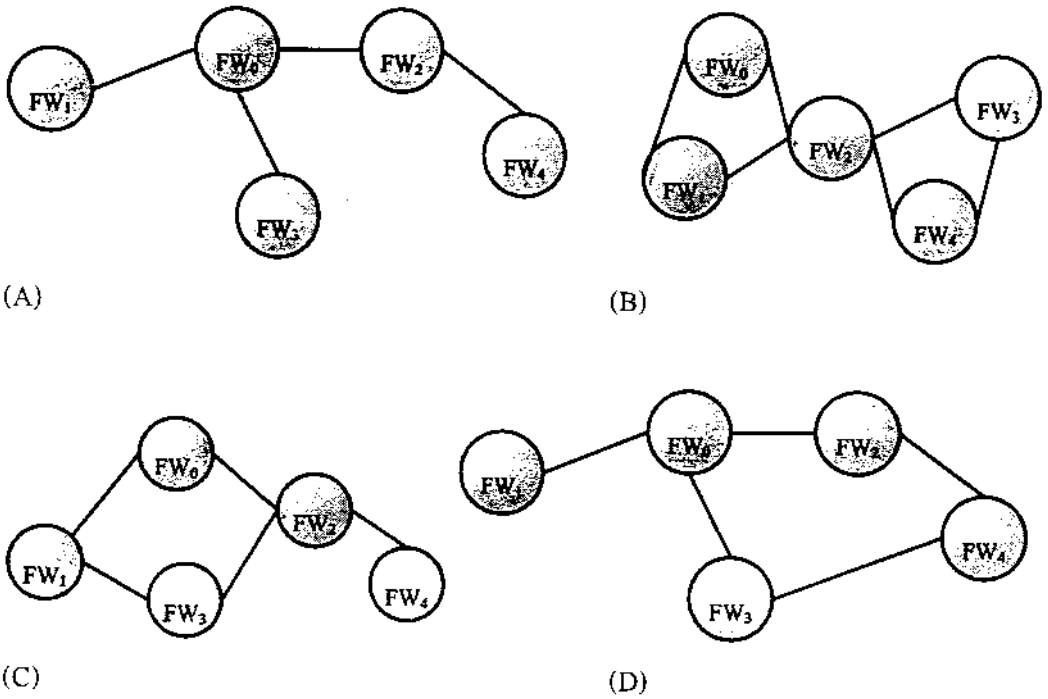
Gp (Group) เป็นกลุ่มของกฎที่มีค่าของ src_ip dst_ip src_port และ dst_port ที่มีความสัมพันธ์ซึ่งกันและกันและ $Gp = \varnothing$ (เซตว่าง) สำหรับค่าเริ่มต้น

$T = (F, E)$ แทนโครงรูปเครือข่าย (Network topology) ที่ประกอบด้วยกลุ่มของไฟร์วอลล์ $F = \{F_1, F_2, ... F_k : F_k \in T\}$ และกลุ่มของเส้นเชื่อม $E = \{(F_k, F_{k+1}) : F_k, F_{k-1} \in T\}$

$path = \{F_u, F_{u+1}, F_{u+2}, ..., F_d\}$ แทนเส้นทางจากต้นทางไปยังปลายทาง และ $path = \varnothing$ (เซตว่าง) สำหรับค่าเริ่มต้น

สำหรับขั้นตอนวิธีที่ 2 ตามภาพที่ 4.7 จำเป็นต้องใช้เส้นทาง (Path) ที่ทราฟฟิคจะเดินทางผ่านเพื่อการค้นหาความผิดปกติของกฎในไฟร์วอลล์ที่อยู่บนเส้นทางนั้น การจัดเส้นทาง (Routing) หรือการหากลุ่มของไฟร์วอลล์ที่ทราฟฟิคจะเดินทางจากต้นทาง (Source หรือ src_ip) ไปยังปลายทาง (Destination หรือ dst_ip) อาจมีเส้นทางได้หลายเส้นทาง เราจะหาเส้นทางระหว่างบัพ 2 บัพใดๆ คือ n_s และ n_t ที่ซึ่งอยู่ใน T โดยใช้ Depth First Search (DFS) Algorithm เมื่อ n_s คือบัพต้นทาง และ n_t คือบัพปลายทาง

การจัดเส้นทาง (Routing) เราเรียกว่า PathDiscovery (input: n_0, n_1) เพื่อค้นหาเส้นทางที่เป็นไปได้ทั้งหมดจาก n_0 จนถึง n_1 ดังนั้นกลุ่มของเส้นทางจะถูกสร้างขึ้น เราสมมติโครงรูปเครือข่ายตามภาพที่ 4.5 ประกอบด้วยไฟร์วอลล์หลายๆ ตัวเชื่อมโยงกัน แต่ละไฟร์วอลล์จะเชื่อมต่อกับแม่ข่าย (Host) ใดแม่ข่ายหนึ่งหรือกลุ่มของแม่ข่ายที่อยู่ในเครือข่าย โดยแม่ข่ายนั้นเป็นได้ทั้งต้นทางและปลายทางที่กลุ่มข้อมูลจะเดินทางผ่าน เราให้ FW_n แทนการระบุไฟร์วอลล์ใดๆ ในเครือข่าย เช่น FW_1 หมายถึงไฟร์วอลล์ 1 เป็นต้น พิจารณาภาพที่ 4.6 แสดงกลุ่มเส้นทางจากต้นทาง FW_1 ไปยังปลายทาง FW_2 ของภาพที่ 4.5



ภาพที่ 4.5 ตัวอย่างการเชื่อมโยงระหว่างไฟร์วอลล์ภายในเครือข่าย

$FW_1 \rightarrow FW_0 \rightarrow FW_2$

(A)

$FW_1 \rightarrow FW_2$ และ $FW_1 \rightarrow FW_0 \rightarrow FW_2$

(B)

$FW_1 \rightarrow FW_0 \rightarrow FW_2$ และ
$FW_1 \rightarrow FW_3 \rightarrow FW_2$

(C)

$FW_1 \rightarrow FW_0 \rightarrow FW_2$ และ
$FW_1 \rightarrow FW_0 \rightarrow FW_3 \rightarrow FW_4 \rightarrow FW_2$

(D)

ภาพที่ 4.6 กลุ่มเส้นทางจากต้นทาง FW_1 ไปยังปลายทาง FW_2 ของภาพที่ 4.5

```
boolean InterFirewallAnomalyDiscovery (R_u, R_d)
{
  if w_{5,u} = deny, w_{5,d} = allow then
  {
    for each pair of R_u and R_d do
      if R_d is shadowed by R_u then {return true;}
      if R_u and R_d are correlated then {return true;}
    end for
  }
  if w_{5,u} = allow, w_{5,d} = deny then
  {
    for each pair of R_u and R_d do
      if R_u allows spurious packet to R_d then {return true;}
      if R_u and R_d are correlated then {return true;}
    end for
  }
  if w_{5,u} = allow, w_{5,d} = allow then
  {
    for each pair of R_u and R_d do
      if R_d is shadowed by R_u then {return true;}
      if R_u allows spurious packet to R_d then {return true;}
        if R_u and R_d are correlated then {return true;}
    end for
  }
  if w_{5,u} = deny, w_{5,d} = deny then
  {
    for each pair of R_u and R_d do
      if R_u allows spurious packet to R_d then {return true;}
      if R_d is redundant to R_u then {return true;}
      if R_u and R_d are correlated then {return true;}
    end for
  }
}
```

Algorithm 2: Inter-Firewall Anomaly Discovery and Correction Algorithm (G_I: original graph, T)

1. **for** any two nodes, n_i and $n_j \in T$ **do**
2. $path$ = PathDiscovery (input: n_i, n_j)
3. **end for**
4. **repeat**
5. **for each** $p \in path$ **do**
6. **for each** firewall **on** p **do**
7. Run Algorithm 1
8. **for each** $R_x \in G_I$ **do**
9. **if** $R_x \Re g$, where any $g \in Gp$
10. **then** $\{Gp = Gp \cup R_x;\}$
11. **end for**
12. **for each** Gp **do**
13. **for** any pair (R_u, R_d) **in** Gp **do**
14. boolean anomalyExists =
15. **InterFirewallAnomalyDiscovery** (R_u, R_d)
16. **if** anomalyExists = true **then** {modify R_u, R_d}
17. **end for**
18. **end for**
19. **end for**
20. **until** (no intra-firewall and inter-firewall anomalies)
21. **end for**
22. ***return*** (G_O: modified graph);

ภาพที่ 4.7 ขั้นตอนวิธีการค้นหาและแก้ไขความผิดปกติของกฎในไฟร์วอลล์แบบกระจาย

จากการพิจารณาเส้นทางระหว่างทุกๆ คู่ของบัพในกราฟ หรือนั่นคือการหาเส้นทางระหว่างคู่ของต้นทางและปลายทางของกฎแต่ละกฎ สำหรับทุกๆ ไฟร์วอลล์บนเส้นทางแต่ละเส้นทาง เราต้องมั่นใจก่อนว่าจะไม่มีความผิดปกติใดๆ ในไฟร์วอลล์เดี่ยวนั้น ด้วยการใช้ขั้นตอนวิธีที่ 1 ตามหัวข้อที่ 4.1.2 จากนั้นจึงค้นหาและแก้ไขความผิดปกติระหว่างไฟร์วอลล์ด้วยการใช้ขั้นตอนวิธีที่ 2 ถ้าเกิดความผิดปกติกรณีใดก็ตามดังที่ได้นิยามไว้ดังหัวข้อ 4.2.1 ให้ทำการแก้ไขความผิดปกตินั้นๆ ถ้าพบว่าความผิดปกติยังมีอยู่ เราควรให้ขั้นตอนวิธีที่ 2 นี้ทำงานต่อไปเรื่อยๆ จนไม่พบความผิดปกติใดๆ หรือพบความผิดปกติที่ไม่ต้องแก้ไข จึงจบการทำงาน

พิจารณาตามภาพที่ 3.3 ระบุทุกๆ คู่ของบัพในกราฟ ที่กลุ่มข้อมูลสามารถมาจากหรือไปถึงบัพคู่นั้นๆ ได้ภายในกราฟ ดังนี้

(140.192.22.0/161.120.24.0), (140.192.22.0/161.120.33.0), (140.192.37.0/161.120.24.0), (140.192.37.0/161.120.33.0), (161.120.24.0/140.192.22.0), (161.120.24.0/140.192.37.0), (161.120.33.0/140.192.22.0) และ (161.120.33.0/140.192.37.0)

ส่วนโดเมนอินเทอร์เน็ต (Internet domain) ในที่นี้เราไม่ถือว่าเป็นโดเมนย่อยภายในเครือข่ายจึงไม่พิจารณา แต่ในแต่ละไฟร์วอลล์สามารถกรองกลุ่มข้อมูลที่มาจากหรือไปถึง Internet domain ได้ด้วยกฎโดยปริยาย (Default filtering rule) และเมื่อพิจารณาเส้นทางแล้วจะได้ว่ามี 2 เส้นทาง ได้แก่ เส้นทางแรก สำหรับบัพ 4 คู่แรกจะมีทิศทางการเดินทางผ่านไฟร์วอลล์ต่างๆ คือ $FW_1 \rightarrow FW_0 \rightarrow FW_2$ และเส้นทางที่สอง สำหรับอีก 4 คู่ที่เหลือมีทิศทางการเดินทางผ่านไฟร์วอลล์ต่างๆ คือ $FW_2 \rightarrow FW_0 \rightarrow FW_1$ ต่อไปเป็นการจัดกลุ่มของกฎที่ค่าต่างๆ ได้แก่ เลขที่อยู่ต้นทาง (src_ip) เลขที่อยู่ปลายทาง (dst_ip) ช่องทางต้นทาง (src_port) และช่องทางปลายทาง (dst_port) มีความสัมพันธ์ซึ่งกันและกัน($\Re$) ในแต่ละเส้นทาง โดยเราได้ว่าเส้นทางแรกได้แก่ กลุ่มของกฎที่ ($1/FW_1$, $4/FW_0$, $8/FW_0$, $9/FW_2$), ($8/FW_1$, $2/FW_0$, $8/FW_0$, $9/FW_2$) และ ($8/FW_1$, $8/FW_0$, $4/FW_2$) ส่วนเส้นทางที่สองได้แก่ กลุ่มของกฎที่ ($1/FW_2$, $1/FW_0$, $7/FW_0$, $1/FW_1$), ($2/FW_2$, $3/FW_2$, $7/FW_0$, $3/FW_1$), ($5/FW_2$, $5/FW_0$, $7/FW_0$, $4/FW_1$, $5/FW_1$), ($6/FW_2$, $7/FW_2$, $8/FW_2$, $3/FW_0$, $7/FW_0$, $6/FW_1$, $7/FW_1$) และ ($9/FW_2$, $6/FW_0$, $7/FW_0$, $8/FW_1$) ต่อไปให้เปรียบเทียบค่าต่างๆ ของเส้นเชื่อมและค่าของบัพระหว่างกฎ 2 กฎใดๆ เช่น กฎที่ ($1/FW_1$, $4/FW_0$), ($1/FW_1$, $8/FW_0$), ($1/FW_1$, $9/FW_2$), ($4/FW_0$, $9/FW_2$) และ ($8/FW_0$, 9/FW_2) ตามลำดับ เป็นต้น ถ้าในขณะที่ทำการเปรียบเทียบแล้วพบความผิดปกติที่ต้องแก้ไข ก็ให้แก้ไขความผิดปกตินั้นๆ ทันที และทำไปจนครบคู่ของกฎ และถ้าไม่พบหรือพบความผิดปกติที่ไม่ต้องแก้ไข จึงจบการทำงาน

ในหัวข้อที่ 4.2.3 จะเป็นทฤษฎีบท ที่จะแสดงให้เห็นว่าบนเส้นทางเครือข่าย (Network path) เดียวกัน จำนวนครั้งที่กลุ่มข้อมูลเดินทางผ่านไฟร์วอลล์ที่ซึ่งมีการแก้ไขความผิดปกติของกฎด้วย Inter-Firewall Anomaly Discovery and Correction Algorithm เป็นจำนวนน้อยกว่าหรือเท่ากับ จำนวนครั้งที่กลุ่มข้อมูลเดินทางผ่านไฟร์วอลล์ที่ซึ่งไม่มีการแก้ไขความผิดปกติของกฎ

4.2.3 ทฤษฎีบท

ทฤษฎีบท 2 เพื่อแสดงว่าขั้นตอนวิธีที่ 2 ทำให้จำนวนครั้งของกลุ่มข้อมูลที่เดินทางผ่านไฟร์วอลล์แบบกระจายลดลงหรือเท่าเดิม

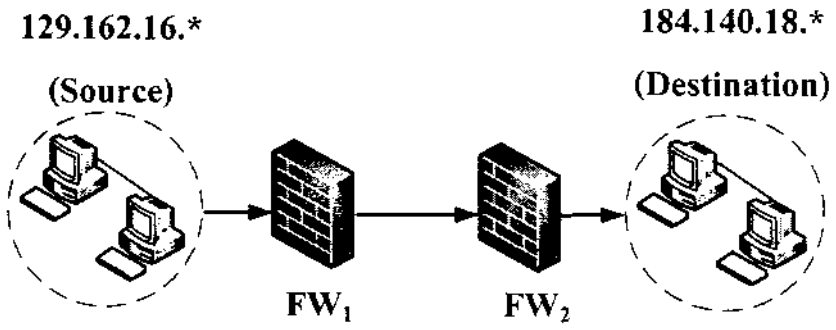
ทฤษฎีบท 2: สำหรับไฟร์วอลล์ตั้งแต่ 2 ไฟร์วอลล์ขึ้นไปในเครือข่าย ทุกๆ ไฟร์วอลล์บนเส้นทางระหว่าง 2 บัพใดๆ คือบัพต้นทางและบัพปลายทาง จำนวนครั้งที่กลุ่มข้อมูลผ่านไฟร์วอลล์ที่ซึ่งมีกฎแบบใหม่ (Modified Graph) น้อยกว่าหรือเท่ากับ จำนวนครั้งที่กลุ่มข้อมูลผ่านไฟร์วอลล์ที่ซึ่งมีกฎแบบเดิม (Original Graph)

พิสูจน์: ใช้การพิสูจน์ด้วย Mathematical Induction เราสมมติว่า T แทนจำนวนครั้งที่กลุ่มข้อมูลผ่านไฟร์วอลล์ที่ซึ่งมีกราฟย่อยแบบเดิม และ T´ แทนจำนวนครั้งที่กลุ่มข้อมูลผ่านไฟร์วอลล์ที่ซึ่งมีกฎแบบใหม่ เมื่อ T, T´∈ ℵ และให้ R_u เป็นกฎของ Upstream firewall (F_u) และ R_d เป็นกฎของ Downstream firewall (F_d)

ให้ S (k) แทนข้อความที่ว่า T´≤ T ที่ซึ่ง k เป็นจำนวนของไฟร์วอลล์บนเส้นทางใดๆ ในเครือข่าย โดยที่ k ∈ ℵ

เพื่อแสดงว่า S (k) เป็นจริง สำหรับทุกๆ จำนวนนับ k ≥ 2 เราต้องแสดงให้ได้ก่อนว่า Basis step เป็นจริง นั่นคือเราต้องแสดงว่า S (2) เป็นจริง

Basis Step: S (2) คือข้อความที่ว่า T´≤ T สำหรับ 2 ไฟร์วอลล์ในเครือข่ายดังภาพที่ 4.8



ภาพที่ 4.8 ตัวอย่างทิศทางการเดินทางของกลุ่มข้อมูลระหว่าง 2 ไฟร์วอลล์ในเครือข่าย

ให้ความสัมพันธ์ของ R_u และ R_d ที่ใช้พิจารณาการกรองทุกๆ กลุ่มข้อมูล ดังนี้

1. $R_u \Re_{FM} R_d$
2. $R_d \Re_{IM} R_u$
3. $R_u \Re_{IM} R_d$
4. $R_u \Re_{C} R_d$

เนื่องจากมีแอ็คชันของกฎระหว่าง F_u และ F_d ที่เป็นไปได้อยู่ 4 กรณีดังนี้

กรณีที่ 1: $w_{S,u}$ = allow และ $w_{S,d}$ = allow

เมื่อพิจารณากลุ่มข้อมูลที่ถูกกรองด้วยกฎแบบเดิมตามความสัมพันธ์ทั้ง 4 กรณี แล้วพบว่า ถ้ากลุ่มข้อมูลสามารถจับคู่กับ R_u ได้แล้วกลุ่มข้อมูลต้องเดินทางผ่านทั้ง F_u และ F_d ดังนั้น T = 2 ในขณะที่ถ้ากลุ่มข้อมูลไม่สามารถจับคู่ได้กับ R_u แล้วกลุ่มข้อมูลเดินทางผ่าน F_u ที่เดียว ดังนั้น T = 1

เมื่อพิจารณากลุ่มข้อมูลที่ถูกกรองด้วยกฎแบบใหม่ตามความสัมพันธ์ทั้ง 4 กรณี แล้วพบว่า ถ้ากลุ่มข้อมูลสามารถจับคู่กับ R_u ได้แล้วกลุ่มข้อมูลต้องเดินทางผ่านทั้ง F_u และ F_d ดังนั้น T´ = 2 ในขณะที่ถ้ากลุ่มข้อมูลไม่สามารถจับคู่ได้กับ R_u แล้วกลุ่มข้อมูลเดินทางผ่าน F_u ที่เดียว ดังนั้น T´ = 1 เนื่องจาก

1. ไม่เกิดความผิดปกติ ทำให้ไม่มีการแก้ไขใดๆ กับกฎแบบเดิม
2. เกิด Spuriousness anomaly ต้องแก้ไข R_u แต่จำนวนของกฎไม่ลด
3. เกิด Shadowing anomaly ทำให้มีการแก้ไข R_d แต่จำนวนของกฎไม่ลด
4. เกิด Correlation anomaly ต้องแก้ไข R_u และ R_d แต่จำนวนของกฎไม่ลด

ดังนั้น ในกรณีที่ 1) สรุปได้ว่า T´ = T

กรณีที่ 2: $w_{S,u}$ = allow และ $w_{S,u}$ = deny

เมื่อพิจารณากลุ่มข้อมูลที่ถูกกรองด้วยกฎแบบเดิมตามความสัมพันธ์ทั้ง 4 กรณี แล้วพบว่า ถ้ากลุ่มข้อมูลสามารถจับคู่กับ R_u ได้แล้วกลุ่มข้อมูลต้องเดินทางผ่านทั้ง F_u และ F_d ดังนั้น T = 2 ในขณะที่ถ้ากลุ่มข้อมูลไม่สามารถจับคู่ได้กับ R_u แล้วกลุ่มข้อมูลเดินทางผ่าน F_u ที่เดียว ดังนั้น T = 1

เมื่อพิจารณากลุ่มข้อมูลที่ถูกกรองด้วยกฎแบบใหม่ตามความสัมพันธ์ทั้ง 4 กรณี แล้วพบว่า ถ้าแพ็ตเก็ตสามารถจับคู่กับ R_u ได้แล้วในกรณีที่ 1 และกรณีที่ 3 กลุ่มข้อมูลเดินทางผ่าน F_u ครั้งเดียว ดังนั้น T´= 1 ส่วนกรณีที่ 2 และกรณีที่ 4 กลุ่มข้อมูลต้องเดินทางผ่านทั้ง F_u และ F_d ดังนั้น T´= 2 ในขณะที่ถ้ากลุ่มข้อมูลไม่สามารถจับคู่ได้กับ R_u แล้วในทุกๆ กรณี กลุ่มข้อมูลเดินทางผ่าน F_u ครั้งเดียว ดังนั้ T´ = 1 เนื่องจาก

1. เกิด Spuriousness anomaly ทำให้ต้องลบกฎ R_u ออก
2. เกิด Spuriousness anomaly ทำให้ต้องเพิ่ม R_d ที่ Upstream firewall โดยมีลำดับอยู่ก่อนหน้า R_u และลบ R_d ออกจาก Downstream firewall
3. เกิด Spuriousness anomaly และแก้ไขความผิดปกติโดยลบ R_u ออก
4. เกิด Correlation anomaly ทำให้ต้องเพิ่ม R_d ที่ Upstream firewall โดยมีลำดับอยู่ก่อนหน้า R_u และลบ R_d ออกจาก Downstream firewall

ดังนั้น ในกรณีที่ 2) สรุปได้ว่า ถ้าแพ็ตเก็ตสามารถจับคู่ได้กับ R_u แล้ว $T' \leq T$ และ ถ้ากลุ่มข้อมูลไม่สามารถจับคู่ได้กับ R_u แล้ว $T' = T$

กรณีที่ 3: $w_{S,u}$ = deny และ $w_{S,u}$ = allow

เมื่อพิจารณากลุ่มข้อมูลที่ถูกกรองด้วยกฎแบบเดิมตามความสัมพันธ์ทั้ง 4 กรณี แล้วพบว่า ในทุกๆ กรณีกลุ่มข้อมูลจะเดินทางผ่าน F_u เพียงที่เดียว ดังนั้น $T = 1$

เมื่อพิจารณากลุ่มข้อมูลที่ถูกกรองด้วยกฎแบบใหม่ตามความสัมพันธ์ทั้ง 4 กรณี แล้วพบว่า ในทุกๆ กรณีกลุ่มข้อมูลจะเดินทางผ่าน F_u เพียงที่เดียว ดังนั้น $T' = 1$ เนื่องจาก

1. เกิด Shadowing anomaly ทำให้ต้องลบ R_d ออก
2. เกิด Shadowing anomaly ทำให้ต้องลบ R_d ออก
3. เกิด Shadowing anomaly แต่ไม่ต้องแก้ไข ความผิดปกตินี้
4. เกิด Correlation anomaly แต่ไม่ต้องแก้ไขความผิดปกตินี้

ดังนั้น ในกรณีที่ 3) สรุปได้ว่า $T' = T$

กรณีที่ 4: $w_{S,u}$ = deny และ $w_{S,u}$ = deny

เมื่อพิจารณากลุ่มข้อมูลที่ถูกกรองด้วยกฎแบบเดิมตามความสัมพันธ์ทั้ง 4 กรณี แล้วพบว่า ใน 2 กรณีแรกทั้งแพ็ตเก็ตที่สามารถจับคู่กับ R_u ได้ และแพ็ตเก็ตที่ไม่สามารถจับคู่ได้กับ R_u กลุ่มข้อมูลจะเดินทางผ่าน F_u ครั้งเดียว ดังนั้น $T = 1$ ในขณะที่ อีก 2 กรณีที่เหลือถ้าแพ็ตเก็ตสามารถจับคู่กับ R_u ได้แล้วกลุ่มข้อมูลจะเดินผ่านเพียง F_u ครั้งเดียว ดังนั้น $T = 1$ และถ้าแพ็ตเก็ตไม่สามารถจับคู่ได้กับ R_u แล้วกลุ่มข้อมูลต้องเดินทางผ่านทั้ง F_u และ F_d ดังนั้น $T = 2$

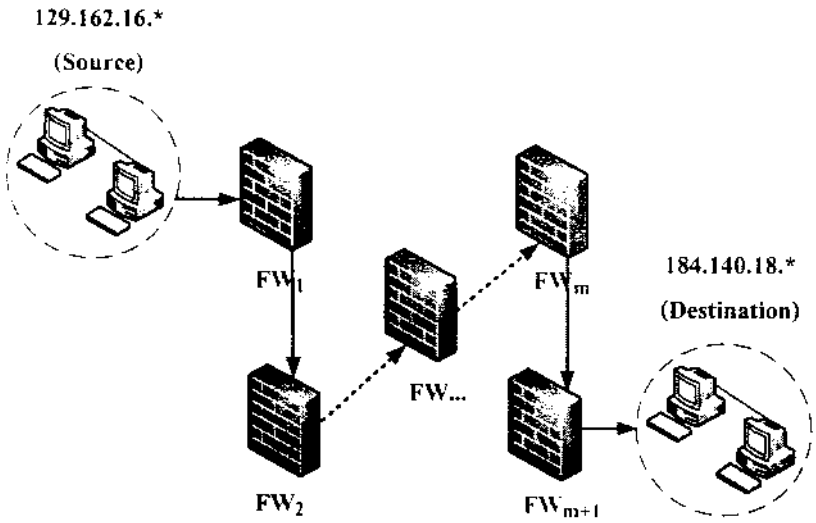
เมื่อพิจารณากลุ่มข้อมูลที่ถูกกรองด้วยกฎแบบใหม่ตามความสัมพันธ์ทั้ง 4 กรณี แล้วพบว่า ใน 3 กรณีแรกแพ็ตเก็ตที่สามารถจับคู่กับ R_u ได้ และแพ็ตเก็ตที่ไม่สามารถจับคู่ได้กับ R_u กลุ่มข้อมูลจะเดินทางผ่าน F_u ครั้งเดียว ดังนั้น $T' = 1$ ในขณะที่กรณีสุดท้ายแพ็ตเก็ตที่สามารถจับคู่กับ R_u ได้เดินผ่านเพียง F_u ครั้งเดียว ดังนั้น $T' = 1$ และแพ็ตเก็ตที่ไม่สามารถจับคู่ได้กับ R_u กลุ่มข้อมูลต้องเดินทางผ่านทั้ง F_u และ F_d ดังนั้น $T' = 2$ เนื่องจาก

1. เกิด Redundancy anomaly ทำให้ต้องลบ R_d ออก
2. เกิด Redundancy anomaly ทำให้ต้องลบ R_d ออก
3. เกิด Spuriousness anomaly ทำให้ต้องนำ R_u ไปไว้แทนที่ R_u
4. เกิด Correlation anomaly แต่ไม่ต้องแก้ไขความผิดปกตินี้

ดังนั้น ในกรณีที่ 4) สรุปได้ว่า $T' = T$

เราได้แสดงว่า $T' \leq T$ สำหรับ 2 ไฟร์วอลล์ใดๆ ในเครือข่าย ดังนั้นจะได้ว่า S (2) เป็นจริง

Inductive Step : จะแสดงว่า Inductive step เป็นจริง เราต้องแสดงว่า S (m) $\longrightarrow$ S (m+1) เป็นจริง สำหรับจำนวนนับใดๆ ที่ $m \geq 2$ ดังนั้น สมมติว่า S (m) เป็นจริง สำหรับจำนวนนับใดๆ ที่ $m \geq 2$ นั่นคือ $T' \leq T$ เราต้องแสดงให้ได้ว่า S (m+1) เป็นจริง นั่นคือ เราต้องแสดงว่า $T' \leq T$ สำหรับ $m+1 \geq 2$ หรือ $m \geq 2$ เมื่อ $m \in \aleph$ ดังภาพที่ 4.9



ภาพที่ 4.9 ตัวอย่างทิศทางการเดินทางของกลุ่มข้อมูลของไฟร์วอลล์แบบกระจาย

เราจะพิสูจน์ขั้นตอนนี้โดยใช้การพิสูจน์โดย Contradiction สมมติว่า S (m+1) เป็นเท็จ นั่นคือ $T' > T$ สำหรับจำนวนนับใดๆ ที่ $m \geq 2$

เพราะว่าบนเส้นทางถูกเพิ่มไฟร์วอลล์ขึ้นมาอีก 1 ตัว (m+1) ทำให้กลุ่มข้อมูลต้องเดินผ่านไฟร์วอลล์เพิ่มอีกไม่เกิน 1 ครั้ง

ทำให้ได้ว่า	$T'+1$	$>$	$T+1$	คุณสมบัติการบวกด้วยจำนวนที่เท่ากัน
ดังนั้น	T'	$>$	T	เมื่อ T' และ $T \in \aleph$

ดังนั้นถ้า S (m) เป็นจริง โดย Inductive hypothesis เราจะได้ว่า S (m+1) เป็นจริง

เนื่องจาก S (2) เป็นจริง และ S (m) $\longrightarrow$ S (m+1) เป็นจริง สำหรับ $m \geq 2$, $m \in \aleph$ โดย Mathematical induction จะได้ว่า S (k) เป็นจริง สำหรับ $k \geq 2$, $k \in \aleph$ นั่นคือจำนวนครั้งของกลุ่มข้อมูลที่ผ่านไฟร์วอลล์ที่มีกฎแบบใหม่ น้อยกว่าหรือเท่ากับ จำนวนครั้งของกลุ่มข้อมูลที่ผ่านไฟร์วอลล์ที่มีกฎแบบเดิม สำหรับไฟร์วอลล์ตั้งแต่ 2 ไฟร์วอลล์ขึ้นไปในเครือข่าย

ในการวิเคราะห์โครงสร้างเครือข่ายแบบที่มีความซับซ้อนที่เกิดจากเส้นทางที่ซ้อนทับกันมากมาย ถ้าเราแยกพิจารณาแต่ละเส้นทาง เราก็สามารถนำกลุ่มของเทคนิคและขั้นตอนวิธีนี้มาปรับใช้ได้ เพราะว่าเทคนิคในการวิเคราะห์ทั้ง Intra-Firewall Anomaly Discovery and Correction Algorithm และ Inter-Firewall Anomaly Discovery and Correction Algorithm ถูกนำมาปฏิบัติบนทุกๆ เส้นทางในเครือข่าย ทำให้ความผิดปกติของกฎต่างๆ ที่อยู่ในไฟร์วอลล์ภายในเครือข่ายจะถูกแก้ไขอย่างอัตโนมัติบนทุกๆ เส้นทางนั่นเอง

4.3 การจัดสรรกฎลงในไฟร์วอลล์

ในงานวิจัยนี้ได้เสนอขั้นตอนวิธีการจัดสรรกฎลงในไฟร์วอลล์แต่ละตัว โดยมีกฎที่ควบคุมการเข้าถึงไฟร์วอลล์ถูกเขียนเป็นรายการของกฎที่เรียงลำดับกัน ดังตารางที่ 4.1

ตารางที่ 4.1 ตัวอย่างของกฎที่ควบคุมการเข้าถึงไฟร์วอลล์

Order	Source		Destination		Action
	Address	Port	Address	Port	
1	184.140.*.*	any	129.162.*.*	80	allow
2	184.140.*.*	any	129.162.16.1	21	deny
3	184.140.*.*	any	129.162.*.*	21	allow
4	129.162.*.*	any	184.140.36.*	23	allow
5	184.140.36.*	any	129.162.*.*	23	allow
6	184.140.18.*	any	129.162.32.1	25	deny
7	184.140.18.*	any	129.162.16.3	25	deny
8	184.140.*.*	any	129.162.32.*	25	allow
9	129.162.*.*	any	184.140.*.*	25	allow
10	*.*.*.*	any	129.162.*.*	25	allow
11	184.140.*.*	any	*.*.*.*	80	allow
12	129.162.*.*	any	184.140.*.*	80	deny
13	184.140.36.*	any	129.162.32.5	23	deny
14	184.140.*.*	any	129.162.*.*	22	deny
15	129.162.*.*	any	184.140.*.*	any	allow
16	184.140.*.*	any	129.162.*.*	any	allow
17	184.140.*.*	any	129.162.*.*	80	allow
18	129.162.*.*	any	184.140.*.*	80	allow
19	184.140.*.*	any	129.162.16.1	21	allow
20	184.140.36.*	any	129.162.32.*	23	deny
21	184.140.*.*	any	129.162.*.*	23	allow
22	184.140.18.*	any	129.162.32.1	25	deny
23	184.140.18.*	any	129.162.*.*	25	allow
24	*.*.*.*	any	*.*.*.*	any	deny

กฎแต่ละกฎจะถูกจัดให้อยู่ในไฟร์วอลล์เดี่ยวที่อยู่บนเส้นทาง โดยการจัดเส้นทาง (Routing) ทุกๆ เส้นทาง (Path) ระหว่างคู่ของต้นทาง (Source) และปลายทาง (Destination) ใดๆ ที่ได้จากกฎที่ควบคุมการเข้าถึงไฟร์วอลล์ และขณะที่มีการจัดสรรกฎเหล่านั้นจะดำเนินการตามขั้นตอนวิธีที่ 1 และขั้นตอนวิธีที่ 2 ด้วย

4.3.1 ขั้นตอนวิธีการจัดสรรกฎลงในไฟร์วอลล์

กำหนดให้ R_i คือกฎของนโยบายความมั่นคงที่ยังไม่ได้ถูกแก้ไขความผิดปกติและ R_j คือกฎของนโยบายความมั่นคงที่ถูกแก้ไขความผิดปกติแล้วและ F_u คือไฟร์วอลล์ที่อยู่ใกล้ต้นทางมากที่สุด (The most upstream firewall) และ F_{u+1} คือไฟร์วอลล์ตัวแรกที่เชื่อมต่อกับ F_u และ F_{u+2} คือไฟร์วอลล์ตัวที่ 2 ที่เชื่อมต่อกับ F_u และไปเรื่อยๆ จนถึง F_d คือไฟร์วอลล์ที่อยู่ใกล้ปลายทางมากที่สุด (The most downstream firewall) เราสมมติให้

$G_I = \{R_1 \cup R_2 \cup ... \cup R_i\}$ แทนกราฟกฎของไฟร์วอลล์เริ่มต้น (An input graph)

$G_O = \{R_1 \cup R_2 \cup ... \cup R_j\}$ แทนกราฟกฎของไฟร์วอลล์ผลลัพธ์ (An output graph)

Gp (Group) เป็นกลุ่มของกฎที่มีค่าของ src_ip dst_ip src_port และ dst_port ที่มีความสัมพันธ์ซึ่งกันและกันและ $Gp = \varnothing$ (เซตว่าง) สำหรับค่าเริ่มต้น

$T = (F, E)$ แทนโครงรูปเครือข่าย (Network topology) ที่ประกอบด้วยกลุ่มของไฟร์วอลล์ $F = \{F_1, F_2, ..., F_k \mid F_k \in T\}$ และกลุ่มของเส้นเชื่อม $E = \{(F_k, F_{k+1}) \mid F_k, F_{k+1} \in T\}$

$path = \{F_u, F_{u+1}, F_{u+2}, ..., F_d\}$ แทนเส้นทางจากต้นทางไปยังปลายทาง และ $path = \varnothing$ (เซตว่าง) สำหรับค่าเริ่มต้น

สำหรับขั้นตอนวิธีการจัดสรรกฎ แสดงไว้ตามภาพที่ 4.10 ดังนี้

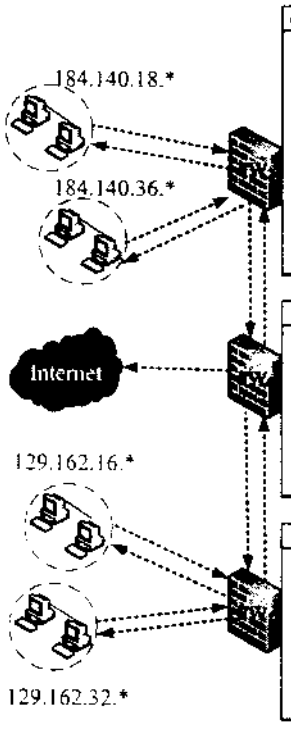
Algorithm 3: Rule Allocation Algorithm (G_I: original graph, T)

1. **for each** $R_k \in G_I$ **do**
2. $n_i = F_u$
3. $n_j = F_d$
4. $path$ = PathDiscovery (input : n_i, n_j); n_i, $n_j \in T$
5. **for each** $p \in path$ **do**
6. **if** $w_{5,k}$ = allow **then** {
7. insert R_k into every firewall in p
8. run Algorithm 2 }
9. **else** {
10. insert R_k into F_u
11. run Algorithm 2 }
12. **end for**
13. **end for**
14. ***return*** (G_O: modified graph);

ภาพที่ 4.10 ขั้นตอนวิธีการจัดสรรกฎของการควบคุมการเข้าถึงไฟร์วอลล์

เมื่อพิจารณาหาเส้นทางระหว่างบัพแต่ละคู่ในกราฟแล้ว กฎแต่ละกฎใน Access Control จะถูกจัดสรร (การกำหนดชื่อไฟร์วอลล์ในค่า firewall identification F_n ($w_{ij} = F_n$) บนเส้นเชื่อม) ลงในไฟร์วอลล์บนเส้นทางที่ได้มา ถ้ากฎมีแอ็คชันเป็น "allow" ก็จะจัดสรรกฎนั้นลงในทุกๆ ไฟร์วอลล์บนเส้นทาง ซึ่งขณะเดียวกันจะมีการทวนสอบว่ากฎที่จะเพิ่มลงในไฟร์วอลล์ต้องไม่ทำให้เกิดความผิดปกติใดๆ กับกลุ่มของกฎที่มีอยู่แล้วในไฟร์วอลล์นั้น ด้วยการใช้ขั้นตอนวิธีที่ 2 ซึ่งถ้าพบว่ามีความผิดปกติอยู่จริงระหว่างกฎคู่ใดแล้วเราจะทำการแก้ไขความผิดปกติเหล่านั้น ในขณะที่กฎที่มีแอ็คชันเป็น "deny" ก็จะจัดสรรกฎนั้นลงในไฟร์วอลล์เพียงตัวเดียวที่ใกล้กับต้นทางมากที่สุด (The most-upstream firewall) และทวนสอบความผิดปกติของกฎด้วยขั้นตอนวิธีที่ 2 เช่นกัน

หลังจากเราจัดสรรกฎต่างๆ ตามตารางที่ 4.1 ลงในไฟร์วอลล์แต่ละตัวเรียบร้อยแล้ว กฎที่อยู่ในไฟร์วอลล์แต่ละตัวจะไม่มีการขัดแย้งกันทั้งภายในไฟร์วอลล์เอง รวมถึงไม่มีการขัดแย้งกันระหว่างไฟร์วอลล์ที่เชื่อมโยงกันด้วย ตัวอย่างกฎที่ถูกจัดสรรเรียบร้อยแล้วด้วยขั้นตอนวิธีที่ 3 แสดงไว้ดังภาพที่ 4.11



Order	Src_ip	Src_port	Dst_ip	Dst_port	Action
1	184.140.*.*	any	129.162.*.*	80	allow
2	184.140.*.*	any	129.162.16.1	21	deny
3	184.140.*.*	any	129.162.*.*	21	allow
4	129.162.*.*	any	184.140.36.*	23	allow
5	184.140.36.*	any	129.162.*.*	23	allow
6	184.140.18.*	any	129.162.32.1	25	deny
7	184.140.18.*	any	129.162.16.3	25	deny
8	184.140.*.*	any	129.162.32.*	25	allow
9	129.162.*.*	any	184.140.*.*	25	allow
10	*.*.*.*	any	*.*.*.*	any	deny

order	src_ip	src_port	dst_ip	dst_port	action
1	184.140.*.*	any	129.162.*.*	80	allow
2	184.140.*.*	any	129.162.*.*	21	allow
3	129.162.*.*	any	184.140.36.*	23	allow
4	184.140.36.*	any	129.162.*.*	23	allow
5	184.140.*.*	any	129.162.32.*	25	allow
6	129.162.*.*	any	184.140.*.*	25	allow
7	*.*.*.*	any	*.*.*.*	any	deny

order	src_ip	src_port	dst_ip	dst_port	action
1	184.140.*.*	any	129.162.*.*	80	allow
2	184.140.*.*	any	129.162.*.*	21	allow
3	129.162.*.*	any	184.140.36.*	23	allow
4	184.140.36.*	any	129.162.*.*	23	allow
5	184.140.*.*	any	129.162.32.*	25	allow
6	129.162.*.*	any	184.140.*.*	25	allow
7	*.*.*.*	any	*.*.*.*	any	deny

ภาพที่ 4.11 ผลลัพธ์จากการจัดสรรรายการของกฎลงในไฟร์วอลล์แบบกระจาย

4.3.2 ทฤษฎีบท

ทฤษฎีบท 3 เพื่อแสดงว่าขั้นตอนวิธีที่ 3 ไม่เปลี่ยนแปลงนโยบายความมั่นคง

ทฤษฎีบท 3: กฎที่ถูกจัดสรรลงในแต่ละไฟร์วอลล์โดยใช้ขั้นตอนวิธีที่ 3 จะไม่ทำให้นโยบายความมั่นคงที่วางไว้เปลี่ยนแปลง

พิสูจน์: พิสูจน์โดยพิจารณาขั้นตอนในขั้นตอนวิธีที่ 3 ดังนี้

การพิจารณาแอ็คชันของกฎที่เป็น Allow

การเพิ่มกฎที่มีแอ็คชันเท่ากับ Allow ลงในไฟร์วอลล์ทุกๆ ตัวบนเส้นทางที่ได้มาจากขั้นตอนที่ 4 กฎจะถูกเพิ่มลงใน F_u, F_{u+1}, F_{u+2}, ..., F_d ตามลำดับ โดยกฎที่เพิ่มเข้าไปจะอยู่ในลำดับหลังกฎทุกๆ กฎภายในไฟร์วอลล์แต่อยู่ในลำดับก่อนหน้ากฎโดยปริยาย (Default rule) ที่ซึ่งเป็นกฎในลำดับสุดท้ายที่อยู่ในไฟร์วอลล์ และในขณะที่ทำการเพิ่มกฎ กฎเหล่านั้นจะถูกทวนสอบความผิดปกติของกฎภายในไฟร์วอลล์ และความผิดปกติของกฎระหว่างไฟร์วอลล์ด้วยขั้นตอนวิธีที่ 2 ดังนั้น

ทำตามขั้นตอนของขั้นตอนวิธีที่ 2

ถ้ากฎที่เพิ่มเข้าไปเกิดความผิดปกติกับกลุ่มของกฎที่อยู่ก่อนแล้วในไฟร์วอลล์เดียวกัน หรือกลุ่มของกฎระหว่างไฟร์วอลล์ จะมีการแก้ไขกฎที่อยู่ภายในไฟร์วอลล์ ผลจากการแก้ไขความผิดปกติของกฎ ทำให้ได้กลุ่มของกฎแบบใหม่ซึ่งได้พิสูจน์ไว้ในทฤษฎีบท 1 แล้วว่ากลุ่มของกฎแบบใหม่ไม่ทำให้นโยบายความมั่นคงเปลี่ยนแปลง

ถ้ากฎที่เพิ่มเข้าไปไม่เกิดความผิดปกติกับกฎภายในไฟร์วอลล์เดียวกัน หรือกฎระหว่างไฟร์วอลล์ จะไม่มีการแก้ไขใดๆ นั่นคือนโยบายความมั่นคงไม่เปลี่ยนแปลง

การพิจารณาแอ็คชันของกฎที่เป็น Deny

การเพิ่มกฎที่มีแอ็คชันเท่ากับ Deny ลงในไฟร์วอลล์ที่อยู่ใกล้ต้นทางมากที่สุด (The most upstream firewall) ก็เพื่อต้องการบล็อก (Block) กลุ่มข้อมูลที่ถูกปฏิเสธตั้งแต่ต้นทาง โดยกฎที่เพิ่มเข้าไปจะอยู่ในลำดับหลังกฎทุกๆ กฎภายในไฟร์วอลล์แต่อยู่ในลำดับก่อนหน้ากฎโดยปริยาย (Default rule) ที่ซึ่งเป็นกฎในลำดับสุดท้ายที่อยู่ในไฟร์วอลล์ และในขณะที่ทำการเพิ่มกฎ กฎภายในไฟร์วอลล์จะถูกทวนสอบความผิดปกติด้วยขั้นตอนวิธีที่ 2 เช่นกัน ซึ่งจะได้ว่าผลจากการปฏิบัติตามขั้นตอนวิธีที่ 2 เพื่อแก้ไขความผิดปกติที่เกิดขึ้นไม่ทำให้นโยบายความมั่นคงเปลี่ยนแปลงตามคำอธิบายในการพิจารณาแอ็คชันของกฎที่เป็น Allow

จากการพิจารณาแต่ละขั้นตอนในขั้นตอนวิธีที่ 3 สรุปได้ว่ากฎที่ถูกจัดสรรลงในแต่ละไฟร์วอลล์โดยใช้ขั้นตอนวิธีที่ 3 จะไม่ทำให้นโยบายความมั่นคงเปลี่ยนแปลง