บทที่ 1

บทนำ

1.1 ความเป็นมา

ปัจจุบันอินเทอร์เน็ตมีบทบาทสำคัญต่อการทำกิจกรรมต่างๆ ในชีวิตประจำวันเป็นอย่างมาก เช่นการติดต่อทางธุรกิจ การศึกษา หรือความบันเทิง เป็นต้น ทำให้องค์กรต่างๆ ให้ความสนใจและต่างก็ทำการเชื่อมต่อระหว่างเครือข่ายขององค์กรและอินเทอร์เน็ต เพื่อให้องค์กรได้รับประโยชน์สูงสุด แต่ก็มีผู้ตั้งคำถามว่าด้านความมั่นคงของเครือข่าย (Network security) จะมีความเสี่ยงมากน้อยเพียงใดต่อการนำเอาเครือข่ายของตนไปเชื่อมต่อกับอินเทอร์เน็ตที่ซึ่งใครก็ได้บนอินเทอร์เน็ตสามารถเข้ามาสู่เครือข่าย และอาจทำการเจาะระบบ หรือ การขโมยข้อมูลภายใน หรือทำให้ระบบได้รับความเสียหาย จากคำถามนี้เองส่งผลให้ความมั่นคงของเครือข่าย ได้รับความสนใจทั้งในด้านงานวิจัยและด้านตลาดอุตสาหกรรมเพิ่มมากขึ้น โดยการหาวิธีการรักษาความมั่นคงและสามารถลดความเสี่ยงนั้นๆ ได้ คำตอบก็คือ ไฟร์วอลล์ ซึ่งเป็นเครื่องมือที่ใช้ในการป้องกันเครือข่ายจากการติดต่อที่ไม่ได้รับอนุญาต ผ่านทางอินเทอร์เน็ตรวมถึงเครือข่ายภายนอกอื่นๆ แต่เดิมมีการใช้ไฟร์วอลล์เดี่ยว (Single firewall) ที่มีการติดตั้งไฟร์วอลล์ไว้เพียงที่เดียวคือติดตั้งไว้ที่เกตเวย์ (Gateway) ซึ่งการติดตั้งแบบนี้ เป็นสถาปัตยกรรมแบบง่ายๆ มีส่วนประกอบที่ทำหน้าที่เป็นไฟร์วอลล์เพียงอันเดียวตั้งอยู่ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก ข้อดีของวิธีนี้คือการที่มีเพียงจุดเดียวทำหน้าที่ไฟร์วอลล์ทั้งหมด ควบคุมการเข้าออกของข้อมูล ทำให้ดูแลได้ง่าย เป็นจุดสนใจในการดูแลความมั่นคงเครือข่าย ในทางกลับกันข้อเสียของวิธีนี้ก็คือ การติดตั้งไฟร์วอลล์ไว้เพียงจุดเดียวนี้ ทำให้มีความเสี่ยงสูง หากมีการปรับเปลี่ยนหรือแก้ไขที่ผิดพลาดหรือมีช่องโหว่เพียงเล็กน้อย การผิดพลาดเพียงจุดเดียวอาจทำให้ระบบถูกเจาะได้ อีกทั้งยังไม่สามารถป้องกันภัยคุกคามภายในได้ ทั้งนี้เนื่องจากทราฟฟิคไม่เคยผ่านไฟร์วอลล์ และเป็นเรื่องยากที่จะทำให้มีการปรับเปลี่ยนกฎในไฟร์วอลล์ให้เป็นปัจจุบันอยู่ตลอดเวลา ตามนโยบายของแต่ละโฮสต์ (Host) ภายในองค์กร

ข้อบกพร่องดังกล่าวข้างต้นของไฟร์วอลล์เดี่ยวนี้เอง นำไปสู่การใช้ไฟร์วอลล์หลายตัว (Multiple firewalls) ในรูปแบบที่เรียกว่า ไฟร์วอลล์แบบกระจาย หรือ Distributed firewall ซึ่งจะถูกติดตั้งไว้ตาม เกตเวย์ (Gateway) อุปกรณ์จัดเส้นทาง (Router) แม่ข่าย (Server) หรือ คอมพิวเตอร์ส่วนบุคคล (Personal Computer) ในเครือข่ายที่ไฟร์วอลล์สามารถทำงานได้ ในสถาปัตยกรรมแบบนี้ ไฟร์วอลล์จะเกิดขึ้นจากส่วนประกอบหลายๆ ส่วนทำหน้าที่ประกอบกันขึ้นเป็นระบบ วิธีการนี้สามารถเพิ่มความมั่นคงได้มาก เนื่องจากเป็นการลดความเสี่ยงต่อความผิดพลาดที่อาจเกิดขึ้น ถ้าหากมีไฟร์วอลล์เพียงจุดเดียวแล้วมีความผิดพลาดเกิดขึ้น ระบบทั้งหมดก็จะเป็นอันตราย แต่ถ้ามีการป้องกันหลายจุด หากในจุดแรกถูกเจาะ ก็อาจจะมีความเสียหายเพียงบางส่วน ส่วนที่เหลือระบบก็ยังคงมีจุดอื่นๆ ในการป้องกันอันตราย และยังลดความเสี่ยงได้โดยการที่แต่ละจุดนั้นมีการใช้เทคโนโลยีที่แตกต่างกัน เพื่อให้เกิดความหลากหลาย เป็นการหลีกเลี่ยงการโจมตีหรือช่องโหว่ที่อาจมีในเทคโนโลยีชนิดใดชนิดหนึ่ง อย่างไรก็ตาม ไฟร์วอลล์แบบกระจายเองก็มีข้อเสียที่พบก็คือในเรื่องการบริหารจัดการ เนื่องจากมีไฟร์วอลล์อยู่หลายแห่งในองค์กร อีกทั้งความซับซ้อนในโครงรูปเครือข่าย (Network topology) ของแต่ละส่วนก็มีมาก แม้ว่าในแต่ละโฮสต์จะสามารถกำหนดนโยบายเองได้ ทั้งนี้ต้องสอดคล้องกับนโยบายโดยรวมขององค์กรด้วย เพื่อให้การบริหารเป็นไปในทิศทางเดียวกัน

ดังนั้นจึงมีความจำเป็นที่จะต้องหาวิธี เพื่อช่วยให้ผู้ดูแลไฟร์วอลล์ทั้งแบบไฟร์วอลล์เดี่ยวและไฟร์วอลล์แบบกระจายสามารถบริหารจัดการ ไฟร์วอลล์ ได้อย่างมีประสิทธิภาพมากขึ้น

1.1.1 การปรับเปลี่ยนกฎโดยอัตโนมัติ (Automated rule reconfiguration)

การปรับเปลี่ยนกลุ่มของกฎต่างๆ ที่เกิดความผิดปกติ (Anomaly) ขึ้นทั้งในไฟร์วอลล์เดี่ยว ที่เรียกว่า Intra-firewall anomaly และ ในไฟร์วอลล์แบบกระจาย ที่เรียกว่า Inter-firewall anomaly โดยอัตโนมัติ ทำให้เกิดประโยชน์ต่อผู้ดูแลไฟร์วอลล์ คือ เพื่อหลีกเลี่ยงความผิดพลาดที่เกิดจากผู้ดูแลเอง ช่วยลดความซับซ้อนของกฎที่มีอยู่เป็นจำนวนมาก และช่วยลดงานของผู้ดูแลไฟร์วอลล์ได้อีกด้วย

1.1.2 การจัดวางกฎของนโยบายให้อยู่ในไฟร์วอลล์ และลำดับที่เหมาะสมโดยอัตโนมัติ (Automated rule allocation)

การจัดวางกลุ่มของกฎต่างๆ เพื่อให้สอดคล้องกับนโยบายความมั่นคงที่ถูกตั้งไว้เป็นเรื่องที่ยากและเกิดความผิดพลาดได้ง่าย การจัดวางกลุ่มของกฎดังกล่าวควรถูกจัดการอย่างอัตโนมัติด้วยเทคนิคที่สามารถจัดวางและลำดับกลุ่มของกฎได้ โดยยังคงสอดคล้องกับนโยบายความมั่นคงภายในโครงสร้างของเครือข่ายนั้นๆ และผู้ดูแลไฟร์วอลล์ (Firewall Administrator) สามารถปรับเปลี่ยนกฎให้ทันต่อนโยบายที่เปลี่ยนแปลงอยู่เสมอได้

นอกจากนี้เพื่อเป็นการสนับสนุนเทคนิคและขั้นตอนวิธีต่างๆ ที่ช่วยในการบริหารจัดการกฎในไฟร์วอลล์ ในวิทยานิพนธ์นี้ ได้ทำการประเมินประสิทธิภาพด้วยการทำการทดลองโดยสร้างนโยบายความมั่นคง (Security policy) ขึ้นมาชุดหนึ่ง และทำตามขั้นตอนตั้งแต่การจัดวางกฎโดยอัตโนมัติ ให้อยู่ในแต่ละไฟร์วอลล์ที่เหมาะสม พร้อมทั้งการทวนสอบความถูกต้องของกลุ่มกฎเหล่านั้นว่าถูกต้องเป็นไปตามนโยบายความมั่นคง และการปรับเปลี่ยนกลุ่มกฎโดยอัตโนมัติตามขั้นตอนวิธี เหล่านี้ผลของการทดลองถูกนำเสนอในรูปแบบของกราฟและตาราง เพื่อแสดงผลของการเปรียบเทียบกลุ่มของกฎแบบเดิม (Original filtering rule) และ กลุ่มของกฎแบบใหม่ (Modified filtering rule) ที่อยู่ในไฟร์วอลล์ ที่ว่านโยบายความมั่นคงของไฟร์วอลล์ไม่เปลี่ยนแปลง จำนวนกฎในไฟร์วอลล์ที่ลดลง และจำนวนครั้งของกลุ่มข้อมูลที่เดินทางผ่านไฟร์วอลล์ที่มีกลุ่มของกฎแบบใหม่ จะน้อยกว่าหรือเท่ากับ จำนวนครั้งของกลุ่มข้อมูลที่เดินทางผ่านไฟร์วอลล์ที่มีกลุ่มของกฎแบบเดิม

1.2 งานวิจัยที่เกี่ยวข้อง

สำหรับในหัวข้อนี้เราจะกล่าวถึงงานวิจัยอื่นๆ ที่เกี่ยวข้องกับงานวิจัยของเรา โดยเราจะมุ่งเน้นไปในหัวข้อที่สำคัญ นั่นคือเรื่องของการบริหารจัดการนโยบายของไฟร์วอลล์แบบกระจาย (Distributed firewall rule management) ซึ่งเป็นหัวข้อที่เราสนใจ การวิเคราะห์และการค้นหาความผิดปกติของกฎในไฟร์วอลล์ (Firewall rule anomaly analysis and discovery) และรูปแบบในการกรองกลุ่มข้อมูล (Packet filter modeling)

ในเรื่องการบริหารจัดการนโยบายของไฟร์วอลล์แบบกระจาย งานวิจัยส่วนใหญ่ในปัจจุบันกำลังให้ความสนใจในด้านนี้ เนื่องจากเป็นการมองเครือข่ายให้เป็นหนึ่งเดียว นั่นคือการมองนโยบายความมั่นคงขององค์กร ซึ่งเป็นสิ่งที่ควรถือปฏิบัติ

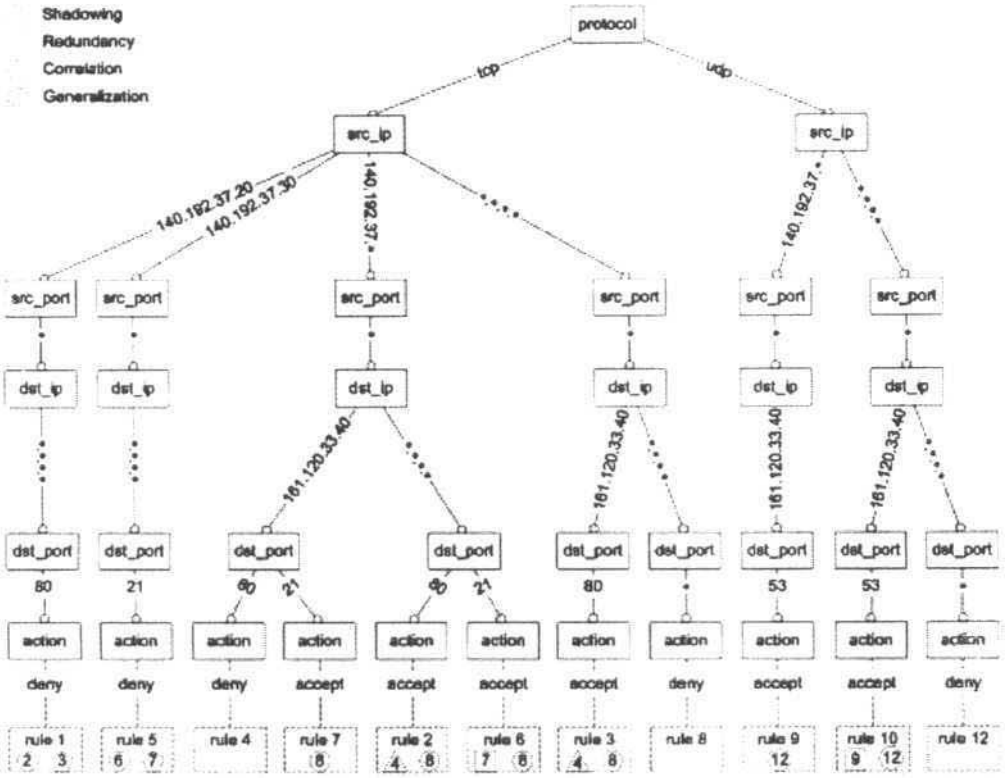
Bartal, *et al.* (1999) นำเสนอชุดเครื่องมือที่เรียกว่า Firmato (Firewall Management Toolkit) เป็นชุดเครื่องมือเพื่อการวิเคราะห์และปรับเปลี่ยนไฟร์วอลล์โดย Firmato ยอมให้ผู้ดูแลไฟร์วอลล์สามารถระบุนโยบายที่เกี่ยวข้องกับองค์กรในระดับสูง และรายละเอียดของโครงสร้างเครือข่าย โดยการใช้ Modular architecture เพื่อแยกนโยบายความมั่นคงออกจากโครงสร้างเครือข่าย ทำให้ผู้ดูแลไฟร์วอลล์สามารถปรับเปลี่ยนโครงสร้างเครือข่ายได้สะดวก โดยไม่จำเป็นต้องปรับเปลี่ยนนโยบายความมั่นคงของเครือข่าย และจุดที่น่าสนใจของ Firmato อีกข้อหนึ่งคือ เมื่อมีการวางนโยบายแล้ว Firmato จะทำการกำหนดกฎ "ACCEPT" บนทุกๆ เส้นทางระหว่างทุกๆ คู่

ของโดเมนย่อยภายในเครือข่าย อย่างไรก็ตามวิธีการเช่นนี้เป็นสิ่งที่ทำให้ถูกโจมตีได้ง่ายจาก Spoofing attacks

Mayer, *et al.* (2000) ได้นำเสนอ Fang (Firewall Analysis Engine) เป็นเครื่องมือวิเคราะห์ไฟร์วอลล์ ที่สามารถตัดสินได้ว่ากลุ่มข้อมูลใดถูกยอมรับระหว่าง 2 โดเมนย่อยในเครือข่าย โดย Fang จะเก็บรวบรวมและอ่านแฟ้มข้อมูลโครงแบบ (Configuration files) ที่เกี่ยวข้องทั้งหมดไว้ และสร้างตัวแทนภายในของนโยบายและโครงสร้างของเครือข่าย และผู้ใช้สามารถป้อนคำถามผ่านส่วนต่อประสานกับผู้ใช้ (User interface) ได้

Al-Shaer, *et al.* (2005) กล่าวถึงการบริหารจัดการนโยบายของไฟร์วอลล์ (Firewall policy) โดยนโยบายของไฟร์วอลล์ถูกแทนด้วยต้นไม้ที่มีรากเดี่ยว (Single-rooted tree) ที่เรียกว่าต้นไม้ของนโยบายความมั่นคง (Policy tree) ดังภาพที่ 1.1 แต่ละบัพ (Node) ใน Policy tree แทนเขตข้อมูลเครือข่าย (Network field) และแต่ละกิ่ง (Branch) ที่บัพนี้ แทนค่าของเขตข้อมูลนั้นๆ โดยทุกๆ เส้นทางของต้นไม้ (Tree) จะเริ่มที่ราก (Root) และสิ้นสุดที่ใบ (Leaf) ที่ซึ่ง 1 เส้นทางของต้นไม้ก็คือกฎ 1 กฎ และในทางกลับกัน กฎ 1 กฎก็คือ 1 เส้นทางของต้นไม้ แต่ละกิ่งถูกใช้เพื่อตรวจสอบค่าของข้อมูลในส่วนหัวของกลุ่มข้อมูล กับค่าของกิ่งใดๆ ของแต่ละบัพที่เริ่มต้นด้วยโพรโทคอล ตามด้วยแอดเดรสของต้นทางและปลายทาง และพอร์ต ทุกๆ กฎมีใบที่เป็นแอ็คชัน (Action) ที่ซึ่งบ่งบอกว่ากลุ่มข้อมูลถูกยอมรับหรือถูกปฏิเสธ สำหรับกฎที่มีค่าของเขตข้อมูลเหมือนกันที่บัพใดบัพหนึ่งแล้วจะใช้กิ่งเดียวกันร่วมกัน

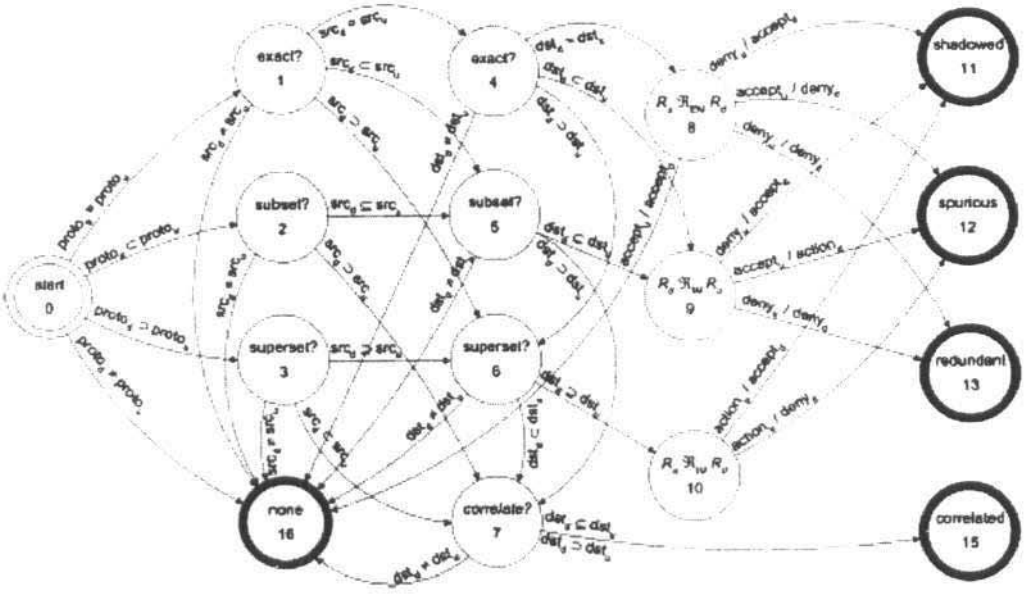
Al-Shaer and Hamed (2002, 2004) ใช้ต้นไม้ของนโยบายความมั่นคง (Policy tree) เพื่อพิจารณาค่าใดๆ ของเครือข่ายเขตข้อมูล กฎที่ต้องการใส่เข้าไปใน Policy tree จะต้องจับคู่กันได้ (Match) กับกฎที่อยู่ใน Policy tree ก่อนแล้ว ถ้ากฎที่เพิ่มเข้าไปใหม่ไม่มีความสัมพันธ์กับกฎที่อยู่ก่อนหน้าในไฟร์วอลล์แล้ว หรือกฎที่เพิ่มเข้าไปใหม่มีความสัมพันธ์เป็นเซตย่อย (Subset) หรือเป็นซูเปอร์เซต (Superset) กับกฎที่อยู่ก่อนหน้าในไฟร์วอลล์แล้ว กฎใหม่นั้นจะถูกใส่เข้าไปในกิ่งใหม่ของ Policy tree แต่ถ้ากฎใหม่เป็นซูเปอร์เซตของกฎเดิม ก็จะถูกใส่เข้าไปในกิ่งของกฎเดิมที่เป็นเซตย่อยทั้งหมด ส่วนในกรณีอื่นๆ กฎใหม่จะถูกใส่ใน Policy tree ที่กิ่งใดๆ ก็ได้



ภาพที่ 1.1 ต้นไม้ของนโยบายความมั่นคง (Policy tree)

แหล่งที่มา: Al-Shaer, *et al.* 2005.

Al-Shaer and Hamed, *et al.* (2002, 2004, 2005) ได้นำเสนอการวิเคราะห์และการค้นหาความผิดปกติของกฎในไฟร์วอลล์ ซึ่งเป็นเทคนิคในการค้นหาความผิดปกติระหว่างไฟร์วอลล์ (Inter-firewall) ในเครือข่าย โดยการใช้ต้นไม้ (Tree) เพื่อค้นหาความสัมพันธ์และความผิดปกติของกฎท่ามกลางกฎเหล่านั้น ด้วยการใช้แผนภาพสถานะ (State diagram) ดังภาพที่ 1.2 เพื่อตัดสินว่าเกิดความผิดปกติของกฎชนิดใด สังเกตว่าที่สถานะสุดท้าย (Final state) เป็นวงกลมสีเข้มจะมีการระบุชนิดของความผิดปกติตามนิยามความสัมพันธ์ของกฎใน (Al-Shaer, *et al.* 2005) ซึ่งถ้าสามารถค้นหาความผิดปกติพบที่กฎใดแล้ว กฎนั้นจะถูกทำเครื่องหมายไว้พร้อมทั้งรายงานชนิดของความผิดปกตินั้นๆ ด้วยที่ส่วนต่อประสานกับผู้ใช้ (User interface) แต่ไม่มีการแก้ไขความผิดปกติที่เกิดขึ้น สำหรับงานวิจัยของ Bartal, *et al.* (1999) และ Mayer, *et al.* (2000) ไม่ได้กล่าวถึงปัญหาในการวิเคราะห์และค้นหาความผิดปกติของกฎในไฟร์วอลล์



ภาพที่ 1.2 แผนภาพสถานะสำหรับการค้นหาความผิดปกติของกฎในไฟร์วอลล์
แหล่งที่มา: Al-Shaer, *et al.* 2005.

1.3 จุดประสงค์และขอบเขตของงานวิจัย

จุดประสงค์ของงานวิจัยนี้มุ่งพัฒนาในด้านระบบการรักษาความมั่นคงภายในองค์กร โดยเน้นไปที่ไฟล์วอลล์ซึ่งเป็นเครื่องมือที่มีบทบาทสำคัญยิ่งในการป้องกันเครือข่าย เพื่อช่วยทำให้ผู้ดูแลไฟร์วอลล์สามารถบริหารจัดการไฟร์วอลล์ได้โดยง่ายและมีประสิทธิภาพนั่นคือ

1.3.1 การปรับเปลี่ยนกฎโดยอัตโนมัติ (Automated rule reconfiguration)

การปรับเปลี่ยนกลุ่มของกฎต่างๆ ที่เกิดความผิดปกติ (Anomaly) ขึ้นทั้งในไฟร์วอลล์เดี่ยวที่เรียกว่า Intra-firewall anomaly และ ไฟร์วอลล์แบบกระจายที่เรียกว่า Inter-firewall anomaly โดยอัตโนมัติ เพื่อหลีกเลี่ยงและช่วยลดความซับซ้อนของกฎที่มีอยู่เป็นจำนวนมาก และช่วยลดงานของผู้ดูแลไฟร์วอลล์ได้อีกด้วย

1.3.2 การจัดวางกฎของนโยบายให้อยู่ในไฟร์วอลล์ และลำดับที่เหมาะสมโดยอัตโนมัติ (Automated rule allocation)

การจัดวางกลุ่มของกฎต่างๆ เพื่อให้สอดคล้องกับนโยบายความมั่นคงที่ถูกกำหนดไว้ และผู้ดูแลไฟร์วอลล์ (Firewall Administrator) สามารถปรับเปลี่ยนกฎให้ทันต่อนโยบายที่เปลี่ยนแปลงอยู่เสมอได้

1.4 ขั้นตอนการทำวิจัย

ขั้นตอนการทำวิจัยแบ่งออกเป็น 6 ขั้นตอนดังนี้

1. ศึกษาและเก็บรวบรวมข้อมูลจากเอกสารทางวิชา รวมถึงเอกสารต่างประเทศต่างๆ (Paper) ที่เกี่ยวข้องกับไฟล์วอลล์ เพื่อเป็นพื้นฐานในการวิเคราะห์ความผิดปกติต่างๆ ของกฎที่เกิดขึ้นได้

2. ศึกษาความผิดปกติต่างๆ ของกฎที่เกิดขึ้นได้ทั้งในไฟร์วอลล์เอง และระหว่างไฟร์วอลล์ รวมถึงวิเคราะห์และหาแนวทางแก้ไขความผิดปกติเหล่านั้น

3. เสนอแนวทางการแก้ไขความผิดปกติและพิสูจน์ด้วยทฤษฎีบท

4. พัฒนาโปรแกรมประยุกต์ตามวิธีการวิเคราะห์และแก้ไขความผิดปกติของกฎ โดยใช้หลักการตามขั้นตอนวิธีที่ได้เสนอไว้ในงานวิจัย

5. ทำการทดสอบเพื่อประเมินประสิทธิภาพของวิธีการ

6. สรุปผลการวิจัย