ภาคผนวก ค

คู่มือการใช้โปรแกรมประยุกต์

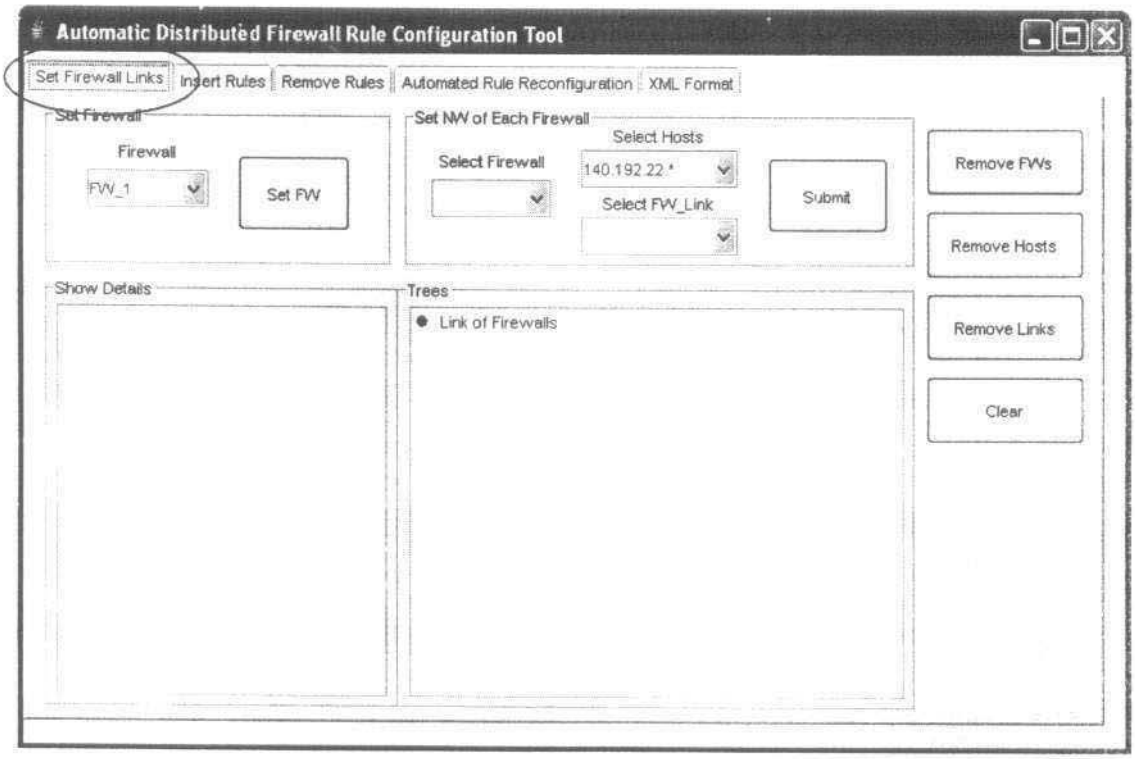
Automatic Distributed Firewall Rule Configuration Tool

คู่มือการใช้โปรแกรมประยุกต์

Automatic Distributed Firewall Rule Configuration Tool

โปรแกรมประยุกต์ Automatic Distributed Firewall Rule Configuration Tool ประกอบด้วยแถบทั้งหมด 5 แถบ ดังต่อไปนี้

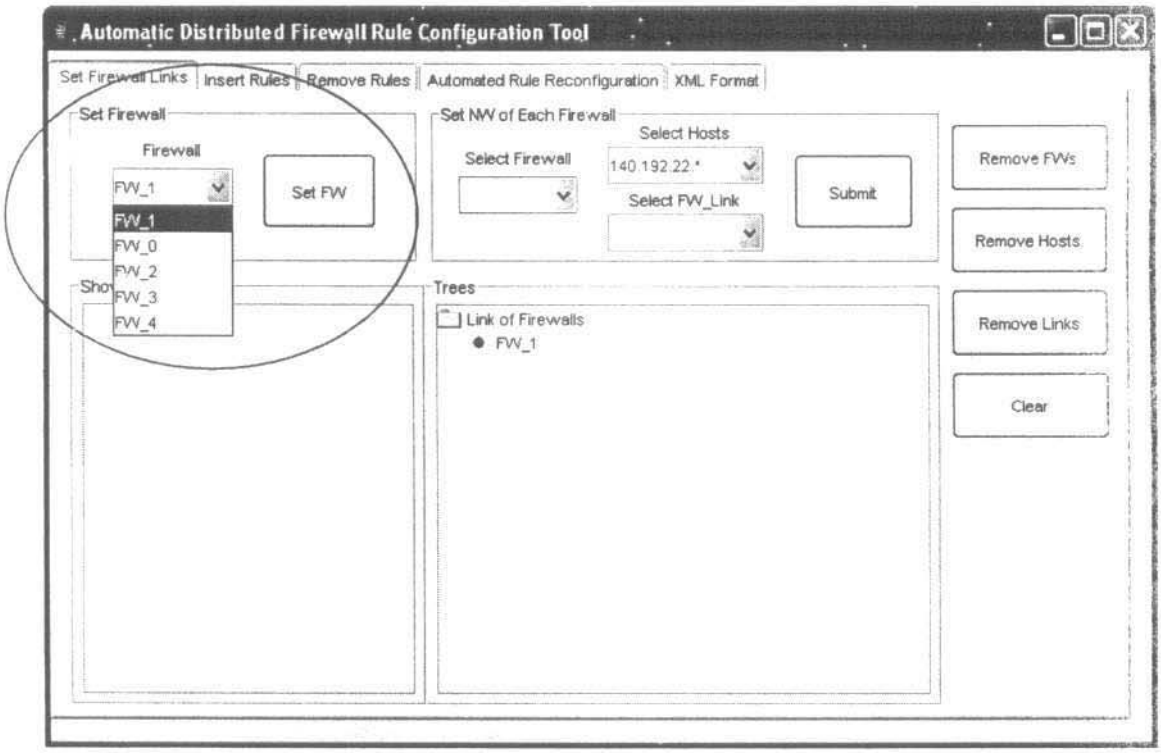
1) แถบ Set Firewall Links เป็นแถบที่ใช้กำหนดโครงรูปเครือข่ายที่ต้องการพิจารณาความผิดปกติต่างๆ ของกฎในไฟร์วอลล์ โดยค่าที่จำเป็นต้องกำหนดได้แก่ ชื่อไฟร์วอลล์ (Firewall) กลุ่มของแม่ข่าย (Hosts) ที่เชื่อมต่ออยู่ ไฟร์วอลล์หรือกลุ่มของไฟร์วอลล์ที่เชื่อมต่ออยู่ (FW_Link)



ภาพที่ ค.1 แสดงแถบ Set Firewall Links

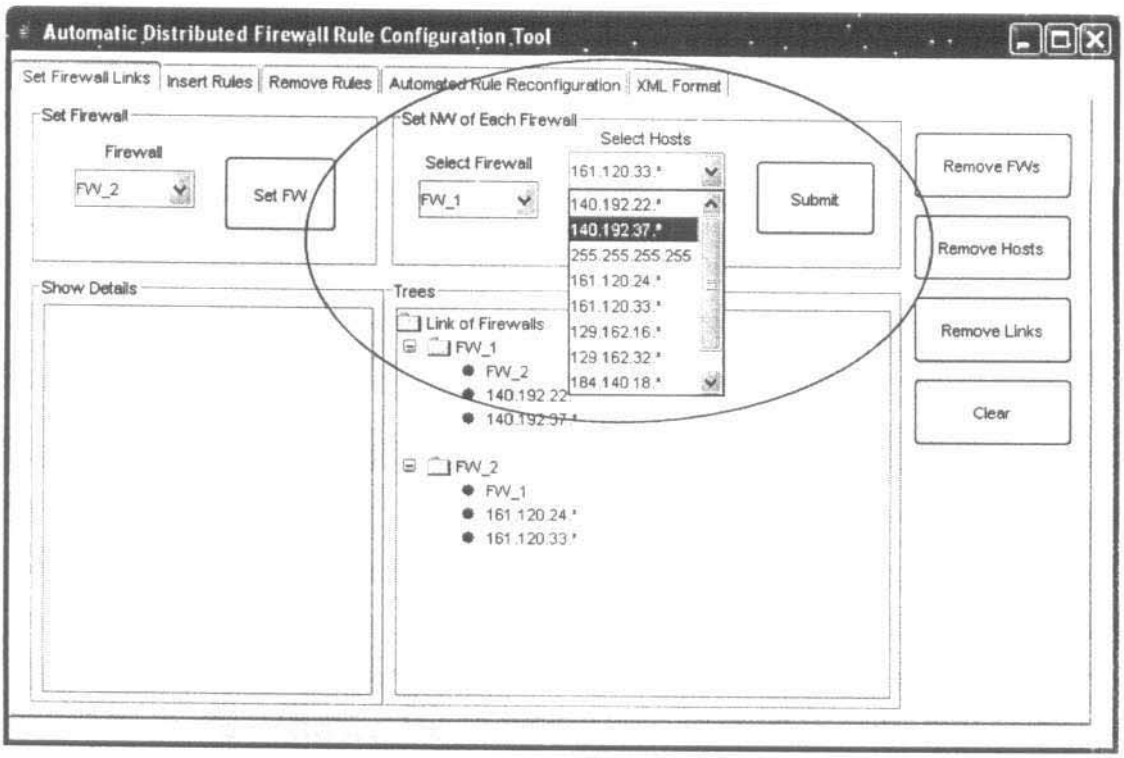
แถบ Set Firewall Links ประกอบด้วย 4 ส่วน และปุ่ม 6 ปุ่ม ดังนี้

(1) ส่วน Set Firewall เป็นส่วนที่ใช้กำหนดชื่อไฟร์วอลล์ที่อยู่ในเครือข่าย โดยเลือกชื่อไฟร์วอลล์จากรายการใน Combo Box ในส่วนนี้ถือเป็นส่วนแรกที่ผู้ใช้จำเป็นต้องกำหนด เนื่องจากไฟร์วอลล์เป็นสิ่งสำคัญที่สุดในการทำงานของโปรแกรมประยุกต์

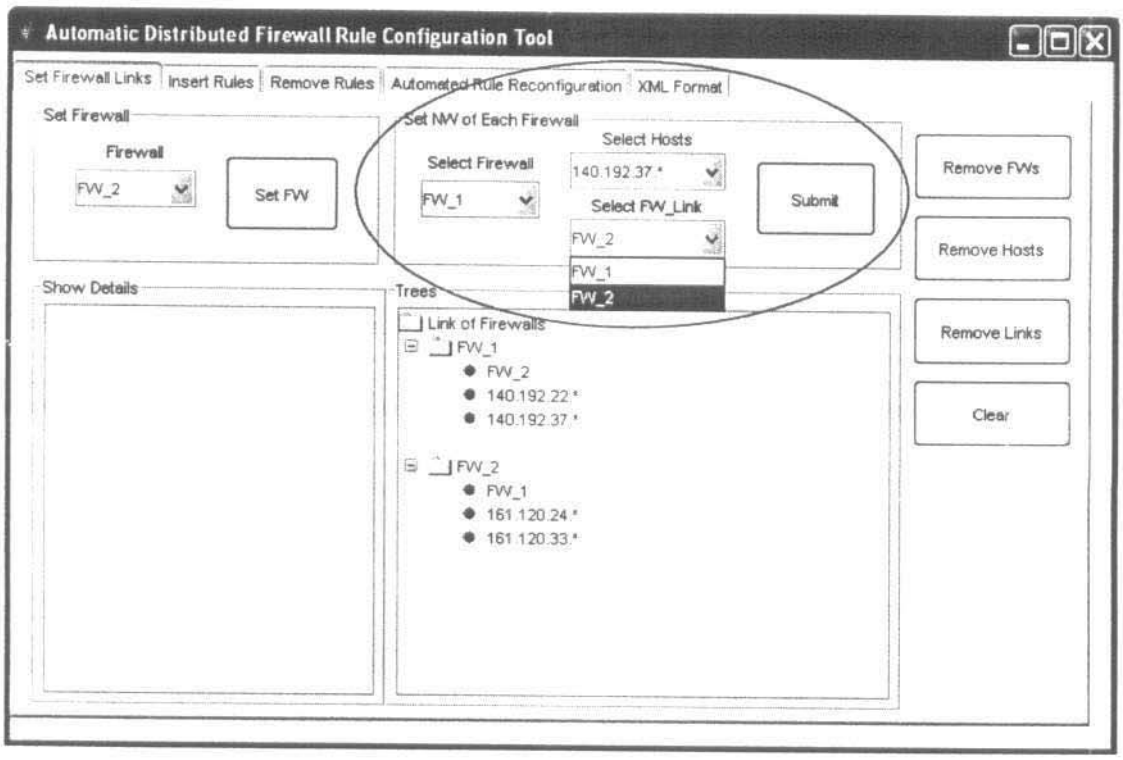


ภาพที่ ค.2 แสดงส่วน Set Firewall ในแถบ Set Firewall Links

(2) ส่วน Set NW of Each Firewall เป็นส่วนที่ใช้กำหนดการเชื่อมโยงกันในเครือข่าย คือ แม่ข่าย (กลุ่มของแม่ข่ายที่เชื่อมต่ออยู่ อาจมีมากกว่า 1 กลุ่ม) ที่เชื่อมต่ออยู่กับแต่ละไฟร์วอลล์ และไฟร์วอลล์ (ถ้ามีไฟร์วอลล์มากกว่า 1 ตัวที่เชื่อมต่ออยู่ก็ต้องกำหนดให้ครบทุกตัว) ที่เชื่อมต่ออยู่กับไฟร์วอลล์ตัวใดตัวหนึ่งในเครือข่าย

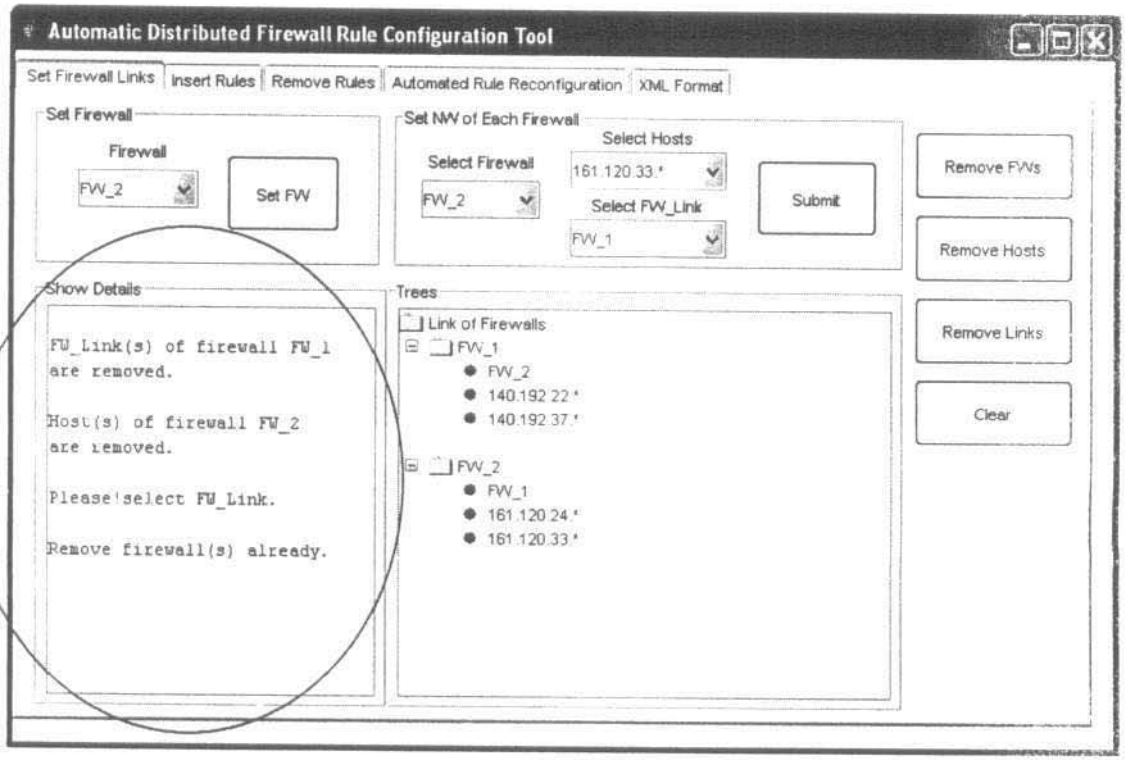


ภาพที่ ค.3 แสดงการกำหนดกลุ่มของแม่ข่ายที่เชื่อมต่ออยู่กับไฟร์วอลล์



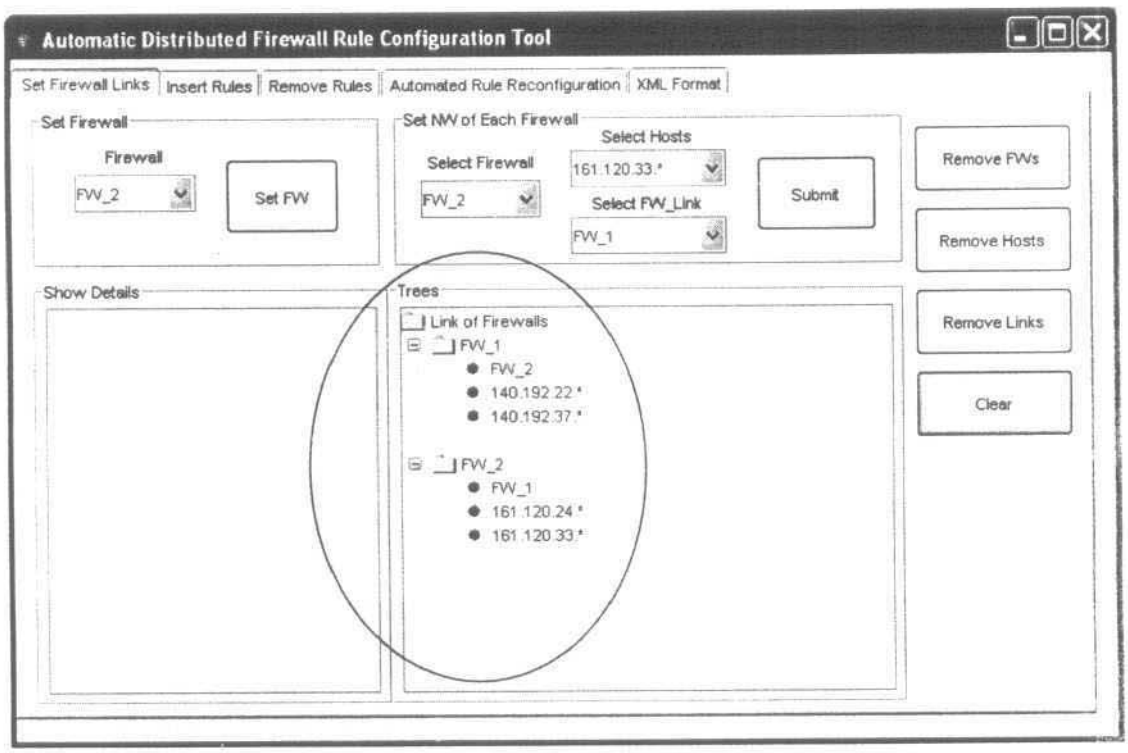
ภาพที่ ค.4 แสดงการกำหนดไฟร์วอลล์ 1 (FW_1) ที่เชื่อมต่ออยู่กับไฟร์วอลล์ 2 (FW_2)

(3) ส่วน Show Details เป็นส่วนที่ใช้แสดงรายละเอียดต่างๆ ที่เกี่ยวข้องกับการกำหนดโครงรูปเครือข่าย รวมถึงความผิดพลาดที่เกิดจากการกำหนดโครงรูปเครือข่ายด้วย เช่น แสดงข้อความที่บ่งบอกว่าไฟร์วอลล์ตัวใดได้ลบแม่ข่ายออกไปจากการเชื่อมต่อ หรือ แสดงข้อความที่บ่งบอกว่าไฟร์วอลล์ตัวใดได้ลบไฟร์วอลล์ตัวใดตัวหนึ่งออกไปจากการเชื่อมต่อ เป็นต้น



ภาพที่ ค.5 แสดงส่วน Show Detail ในแถบ Set Firewall Links

(4) ส่วน Trees เป็นส่วนที่ใช้แสดงต้นไม้ของไฟร์วอลล์แต่ละตัวที่อยู่ในเครือข่ายที่มีการเชื่อมต่อกับกลุ่มของแม่ข่าย หรือ ไฟร์วอลล์ตัวใดตัวหนึ่งอยู่ ทั้งนี้เพื่อทำให้เข้าใจได้โดยง่ายกับการมองการเชื่อมต่อทั้งหมดของไฟร์วอลล์



ภาพที่ ค.6 แสดงต้นไม้ของไฟร์วอลล์ทุกๆ ตัวที่อยู่ในเครือข่าย

(5) ปุ่ม Set FW เป็นปุ่มที่อยู่ในส่วน Set Firewall ที่ผู้ใช้จะกดเมื่อเลือกชื่อไฟร์วอลล์ที่ต้องการกำหนดเรียบร้อยแล้ว

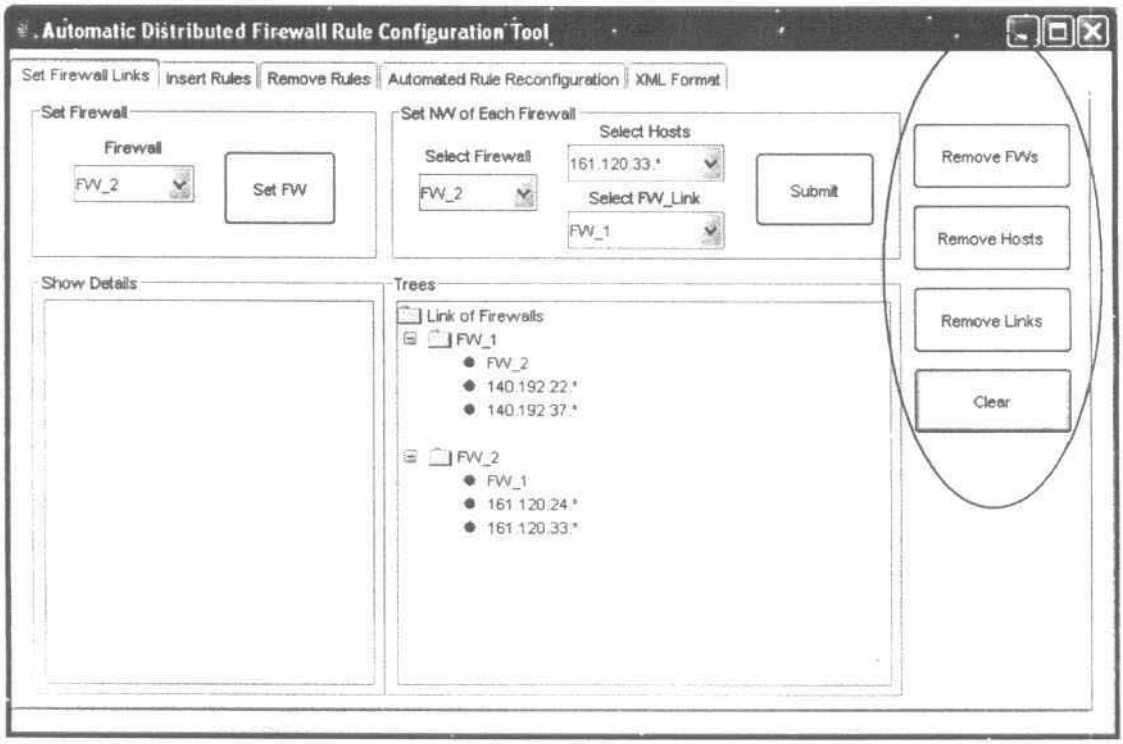
(6) ปุ่ม Submit เป็นปุ่มที่อยู่ในส่วน Set of Each Firewall ที่ผู้ใช้จะกดเมื่อเลือกกลุ่มของแม่ข่ายและไฟร์วอลล์ที่เชื่อมต่ออยู่กับไฟร์วอลล์ตัวใดตัวหนึ่งในเครือข่ายเรียบร้อยแล้ว

(7) ปุ่ม Remove FWs เป็นปุ่มแรกที่อยู่ทางด้านขวามือสุดในแถบ Set Firewall Links ที่ผู้ใช้จะกดเมื่อต้องการลบไฟร์วอลล์ทุกๆ ตัวออกจากโครงรูปเครือข่าย เพื่อต้องการกำหนดชื่อไฟร์วอลล์ใหม่ที่ถูกต้อง

(8) ปุ่ม Remove Hosts เป็นปุ่มที่ 2 ถัดจากปุ่ม Remove FWs ที่อยู่ทางด้านขวามือสุดในแถบ Set Firewall Links ที่ผู้ใช้จะกดเมื่อต้องการลบกลุ่มของแม่ข่ายทุกๆ กลุ่มที่ถูกกำหนดให้เชื่อมต่อกับไฟร์วอลล์ตัวใดตัวหนึ่งในเครือข่ายออกจากการเชื่อมต่อ เพื่อต้องการกำหนดกลุ่มของแม่ข่ายใหม่ที่ถูกต้อง

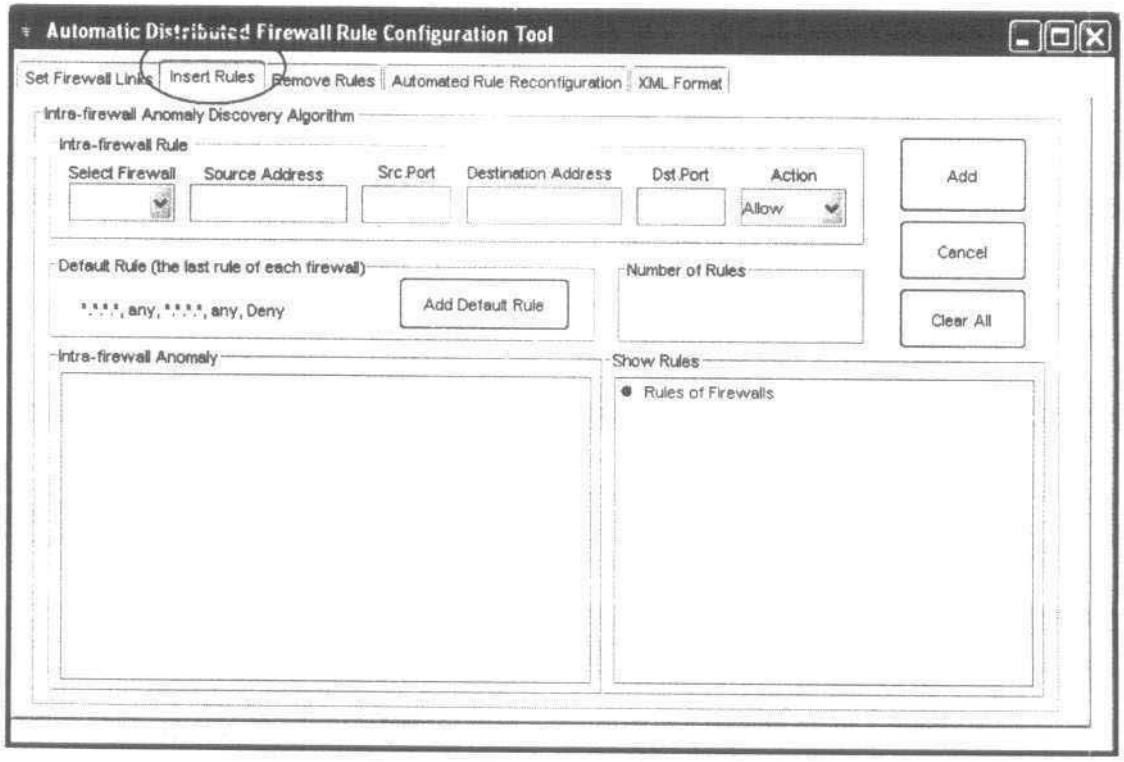
(9) ปุ่ม Remove Links เป็นปุ่มที่ 3 ถัดจากปุ่ม Remove Hosts ที่อยู่ทางด้านขวามือสุดในแถบ Set Firewall Links ที่ผู้ใช้จะกดเมื่อต้องการลบไฟร์วอลล์ทุกๆ ตัวที่ถูกกำหนดให้เชื่อมต่อกับไฟร์วอลล์ตัวใดตัวหนึ่งในเครือข่ายออกจากการเชื่อมต่อ เพื่อต้องการกำหนดกลุ่มของไฟร์วอลล์ใหม่ที่ถูกต้อง

(10) ปุ่ม Clear เป็นปุ่มสุดท้าย ถัดจากปุ่ม Remove Links ที่อยู่ทางด้านขวามือสุดในแถบ Set Firewall Links ที่ผู้ใช้จะกดเมื่อต้องการลบข้อความทั้งหมดในส่วน Show details



ภาพที่ ค.7 แสดงปุ่ม Remove FWs, Remove Hosts, Remove Links และ Clear ตามลำดับ

2) แถบ Insert Rules เป็นแถบที่ใช้ป้อนข้อมูลแต่ละเขตข้อมูล (Field) ของกฎที่ซึ่งถูกกำหนดไว้ในไฟร์วอลล์ตัวใดตัวหนึ่งในเครือข่าย โดยขณะที่ทำการเพิ่มกฎลงในไฟร์วอลล์จะมีการค้นหาความผิดปกติ (Anomaly) ที่จะเกิดขึ้น หากพบความผิดปกติที่ต้องแก้ไขแล้วความผิดปกตินั้นจะถูกแก้ไขโดยอัตโนมัติเพื่อให้กฎต่างๆ ที่อยู่ในไฟร์วอลล์ไม่เกิดการขัดแย้งกัน แต่หากไม่พบความผิดปกติหรือพบความผิดปกติที่ไม่ต้องแก้ไขแล้วกฎนั้นๆ ก็จะถูกเพิ่มเข้าไปในไฟร์วอลล์โดยใช้ Intra-firewall Anomaly Discovery Algorithm

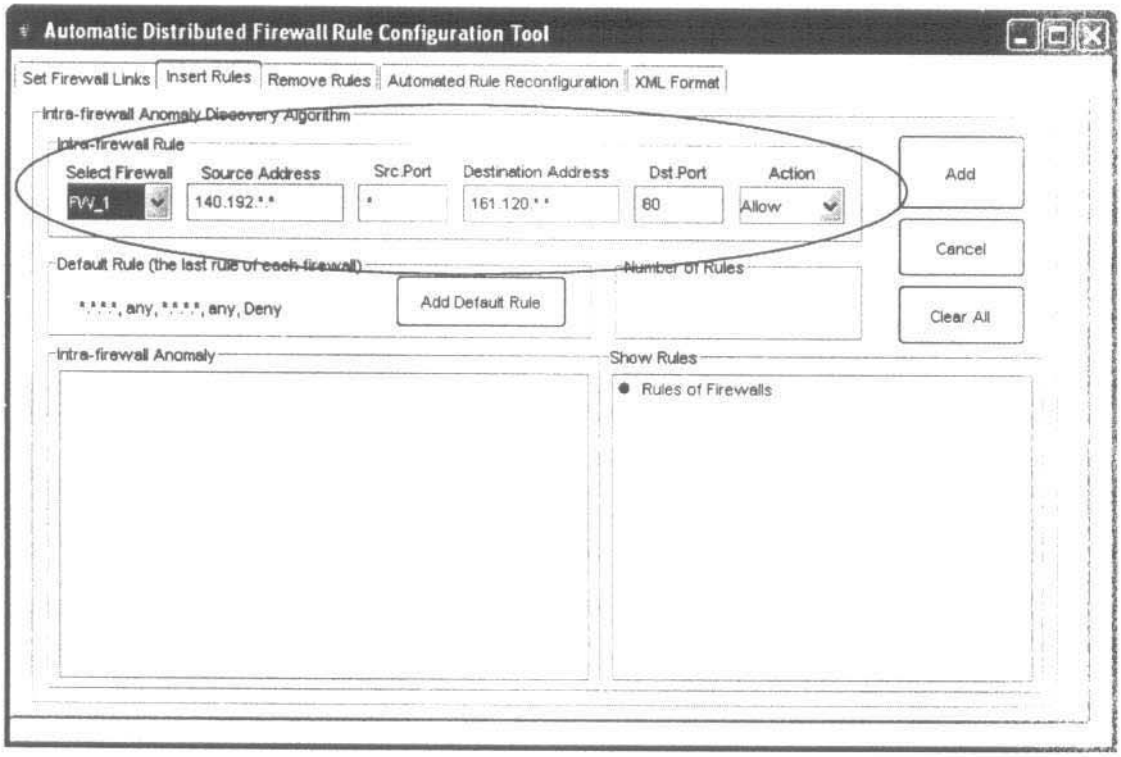


ภาพที่ ค.8 แสดงแถบ Insert Rules

แถบ Insert Rules ประกอบด้วย 5 ส่วน และปุ่ม 4 ปุ่ม ดังนี้

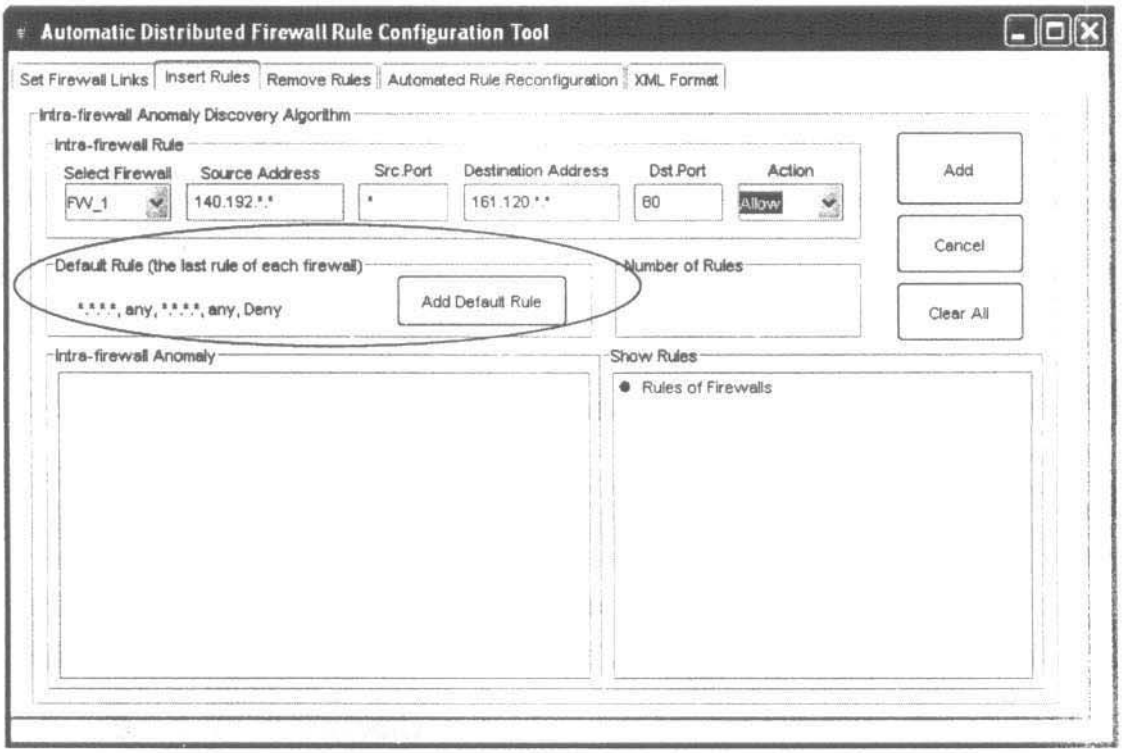
(1) ส่วน Intra-firewall Rule เป็นส่วนที่ใช้ป้อนข้อมูลแต่ละเขตข้อมูลของกฎที่จะกำหนดไว้ในไฟร์วอลล์ตัวใดตัวหนึ่งในเครือข่าย โดยข้อมูลที่ผู้ใช้จำเป็นต้องใส่ได้แก่ ไฟร์วอลล์ที่ซึ่งต้องการจะเพิ่มกฎลงไป เลขที่อยู่ต้นทาง (Source Address) ช่องทางต้นทาง (Source Port หรือ Src.Port) เลขที่อยู่ปลายทาง (Destination Address) ช่องทางปลายทาง (Destination Port หรือ Dst.Port) และแอ็คชัน (Action)

สำหรับเขตข้อมูลของกฎคือ เลขที่อยู่ต้นทาง ช่องทางต้นทาง เลขที่อยู่ปลายทาง และช่องทางปลายทาง ถ้าเขตข้อมูลใดปรากฏเครื่องหมายดอกจัน (*) นั่นหมายความถึง ค่าใดๆ ตามความหมายของเขตข้อมูลนั้นๆ เช่น เลขที่อยู่ต้นทาง หรือ เลขที่อยู่ปลายทาง เท่ากับ 140.192.*.* หมายความว่า เลขที่อยู่ที่ระบุเครื่องหมายดอกจันมีค่าตั้งแต่ 0-255 (8 บิต) ในขณะที่ ช่องทางต้นทาง หรือ ช่องทางปลายทาง เท่ากับ * หมายความว่า ช่องทางที่ระบุเครื่องหมายดอกจันนั้น มีค่าได้ตั้งแต่ 0-65536 (16 บิต) เป็นต้น



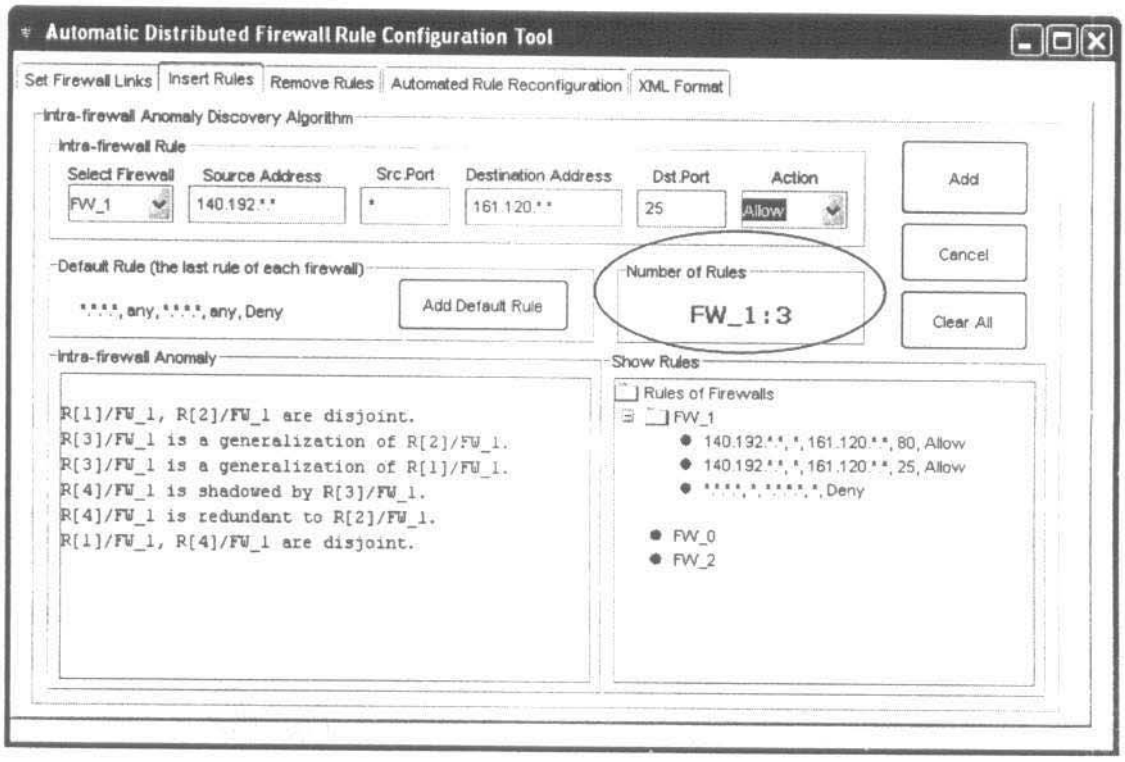
ภาพที่ ค.9 แสดงการป้อนข้อมูลแต่ละเขตข้อมูลของกฎที่จะเพิ่มไว้ใน FW_1

(2) ส่วน Default Rule เป็นส่วนที่ใช้กำหนดกฎโดยปริยาย (Default filtering rule) ซึ่งเป็นกฎที่ทุกๆ ไฟร์วอลล์จะต้องมีโดยกฎนี้จะอยู่ในลำดับสุดท้ายเสมอ คือ *.*.*.*, any, *.*.*.*, any, Deny ซึ่งหมายถึง กฎนี้ได้ระบุไว้ว่าจะไม่อนุญาตให้กลุ่มข้อมูลที่มีไอพีต้นทางใดๆ และหมายเลขช่องทางต้นทางใดๆ และไอพีปลายทางใดๆ และหมายเลขช่องทางปลายทางใดๆ ผ่านไฟร์วอลล์ไปได้นอกเหนือจากกฎที่ได้กำหนดไว้ในลำดับก่อนหน้า ซึ่งผู้ใช้จะกำหนดกฎนี้ให้แต่ละไฟร์วอลล์หลังจากที่เพิ่มกฎต่างๆ ที่ต้องการลงในไฟร์วอลล์เป็นที่เรียบร้อยแล้ว



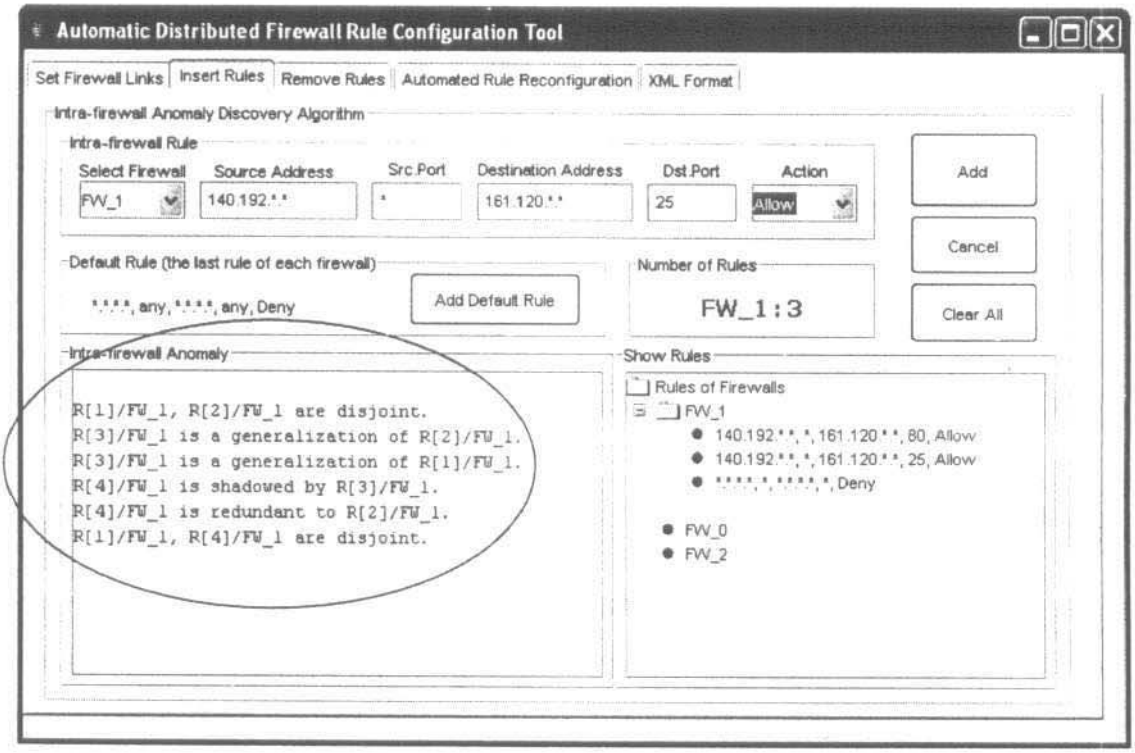
ภาพที่ ค.10 แสดงส่วน Default Rule ในแถบ Insert Rules

(3) ส่วน Number of Rules เป็นส่วนที่ใช้แสดงจำนวนของกฎที่มีอยู่ในไฟร์วอลล์ตัวใดตัวหนึ่งที่ผู้ใช้เลือกไว้เพื่อเพิ่มกฎลงไปในขณะนั้น



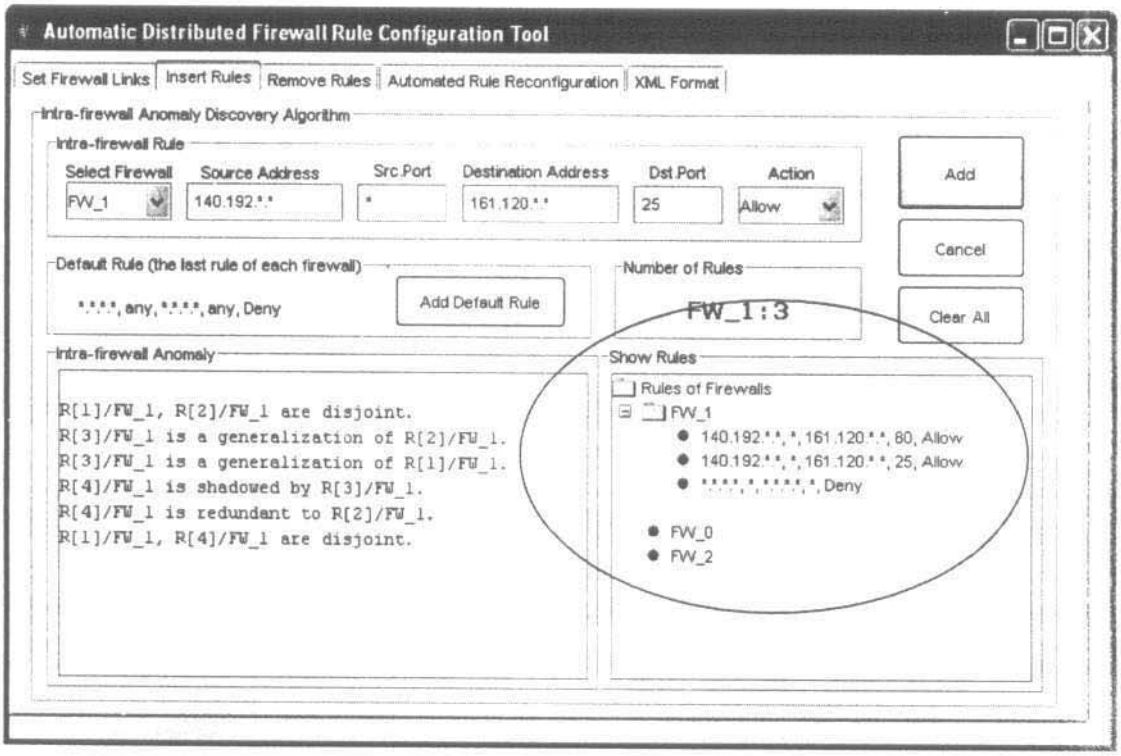
ภาพที่ ค.11 แสดงส่วน Number of Rules ในแถบ Insert Rules

(4) ส่วน Intra-firewall Anomaly เป็นส่วนที่ใช้แสดงความผิดปกติที่เกิดขึ้นระหว่างกฎในไฟร์วอลล์ โดยกฎที่ผู้ใช้จะเพิ่มเข้าไปในไฟร์วอลล์แต่ละตัวจะถูกตรวจสอบด้วย Intra-firewall Anomaly Discovery Algorithm หากพบความผิดปกติระหว่างกฎคู่ใดๆ ในไฟร์วอลล์แล้ว ผู้ใช้จะพบข้อความเพื่อบ่งบอกถึงความผิดปกติไว้ในส่วนนี้



ภาพที่ ค.12 แสดงส่วน Intra-firewall Anomaly ในแถบ Insert Rules

(5) ส่วน Show Rules เป็นส่วนที่ใช้แสดงต้นไม้ของกฎสำหรับไฟร์วอลล์ทุกๆ ตัวในเครือข่าย เพื่อทำให้ผู้ใช้สามารถทำความเข้าใจได้ง่ายขึ้น โดยกฎที่แสดงไว้ในต้นไม้นี้ คือกฎที่ถูกตรวจสอบความผิดปกติต่างๆ และได้รับการแก้ไขโดยอัตโนมัติเรียบร้อยแล้ว



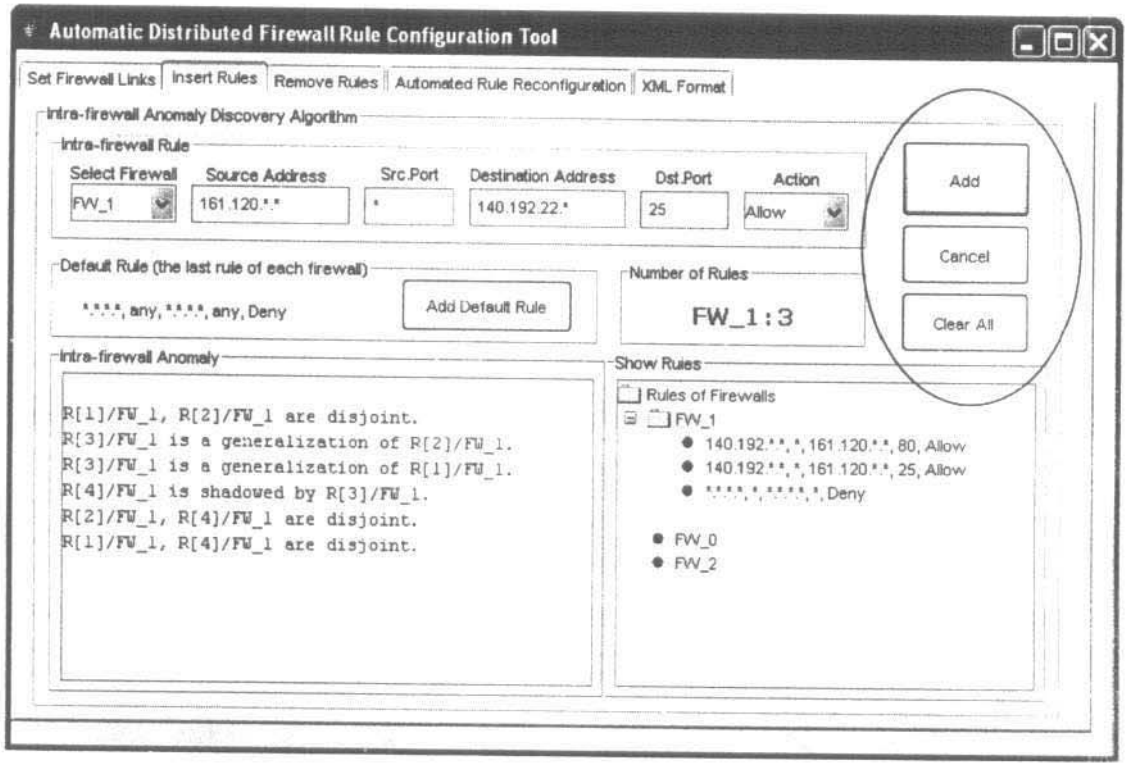
ภาพที่ ค.13 แสดงส่วน Show Rules ในแถบ Insert Rules

(6) ปุ่ม Add Default Rule เป็นปุ่มที่อยู่ในส่วน Default Rule ที่ผู้ใช้จะกดเมื่อต้องการเพิ่มกฎโดยปริยายลงในไฟร์วอลล์เป็นกฎลำดับสุดท้าย หลังจากได้เพิ่มกฎทุกๆ กฎที่ต้องการลงในไฟร์วอลล์ที่เลือกไว้เรียบร้อยแล้ว

(7) ปุ่ม Add เป็นปุ่มแรกที่อยู่ด้านขวามือสุดในแถบ Insert Rules ที่ผู้ใช้จะกดปุ่มนี้เมื่อใส่ข้อมูลทุกๆ เขตข้อมูลของกฎเรียบร้อยแล้ว ปุ่มนี้จะทำการเพิ่มกฎลงในไฟร์วอลล์ที่ผู้ใช้ระบุไว้ โดยจะมีการตรวจสอบความผิดปกติและมีการแก้ไขความผิดปกติที่พบโดยอัตโนมัติที่ปุ่มนี้

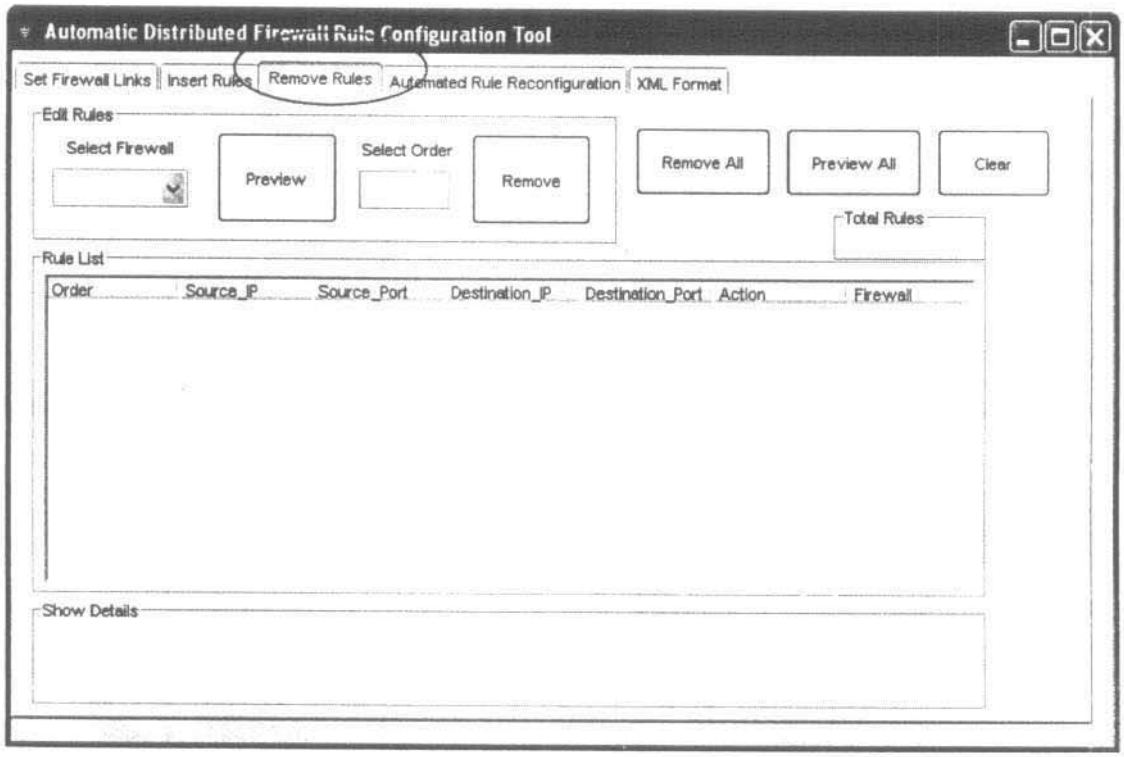
(8) ปุ่ม Cancel เป็นปุ่มที่ 2 ถัดจากปุ่ม Add ที่อยู่ด้านขวามือสุดในแถบ Insert Rules ที่ผู้ใช้จะกดปุ่มนี้เมื่อต้องการแก้ไขทุกๆ เขตข้อมูลของกฎที่ได้ใส่ไว้แล้ว หรือมีความประสงค์จะเปลี่ยนให้เป็นกฎใหม่ หากผู้ใช้ต้องการลบเพียงบางเขตข้อมูล สามารถทำได้โดยเลือกเขตข้อมูลที่ต้องการจะลบแล้วใช้ปุ่ม Delete ที่แป้นพิมพ์

(9) ปุ่ม Clear All เป็นปุ่มสุดท้ายถัดจากปุ่ม Cancel ที่อยู่ด้านขวามือสุดในแถบ Insert Rules ที่ผู้ใช้จะกดปุ่มนี้เมื่อต้องการลบข้อความทั้งหมดในส่วน Intra-firewall Rule และในส่วน Intra-firewall Anomaly



ภาพที่ ค.14 แสดงปุ่ม Add, Cancel และ Clear All ตามลำดับ ในแถบ Insert Rules

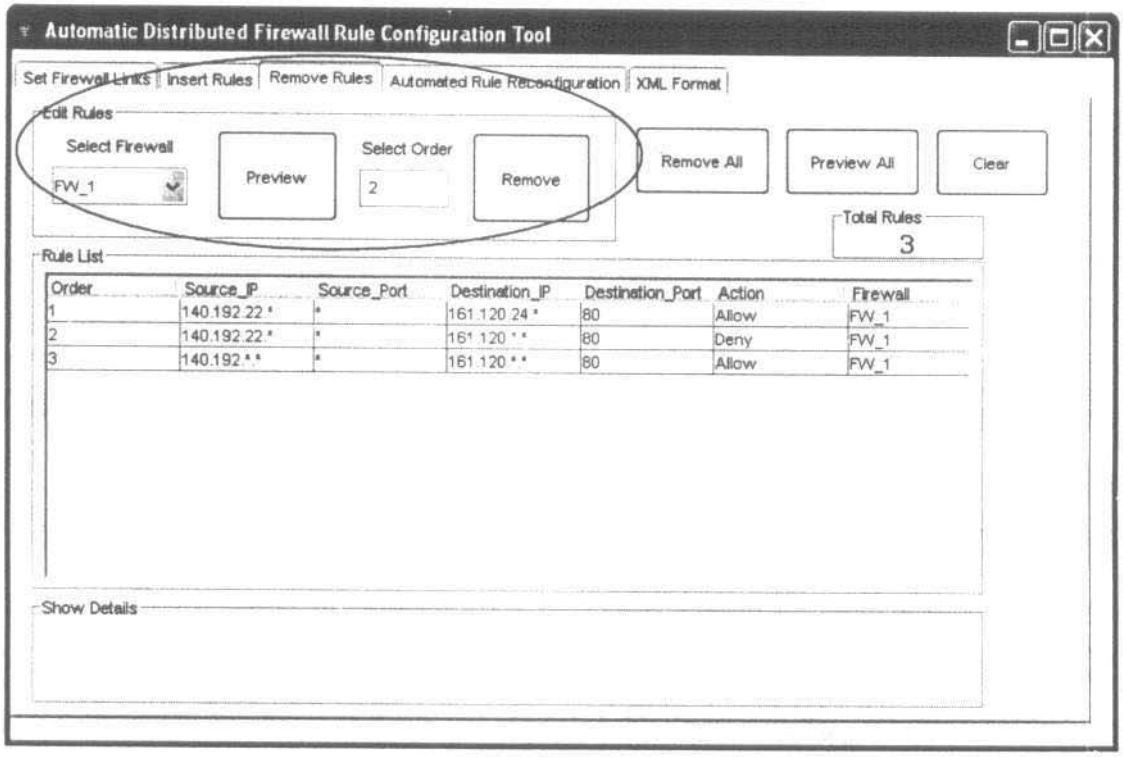
3) แถบ Remove Rules เป็นแถบที่ถูกใช้เมื่อผู้ใช้ต้องการลบกฎบางกฎหรือทุกๆ กฎออกจากไฟร์วอลล์ตัวใดตัวหนึ่งในเครือข่าย โดยผู้ใช้สามารถดูรายละเอียดของกฎแต่ละกฎในทุกๆ ไฟร์วอลล์หรือไฟร์วอลล์บางตัวได้ก่อนจะเลือกกฎที่ต้องการลบออก



ภาพที่ ค.15 แสดงแถบ Remove Rules

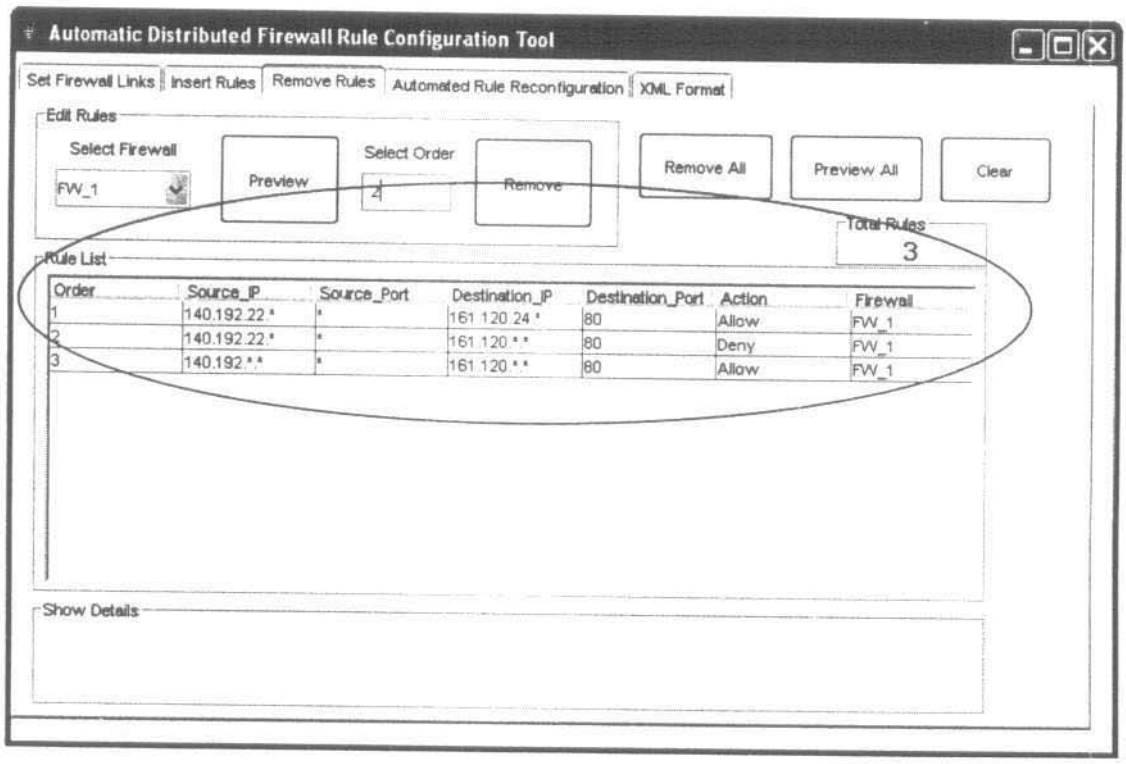
แถบ Remove Rules ประกอบด้วย 3 ส่วน และปุ่ม 5 ปุ่ม ดังนี้

(1) ส่วน Edit Rules เป็นส่วนที่ถูกใช้เมื่อผู้ใช้ต้องการลบกฎบางกฎออกจากไฟร์วอลล์ที่ผู้ใช้ได้เลือกไว้ในขณะนั้น โดยผู้ใช้สามารถดูรายละเอียดของกฎทั้งหมดในไฟร์วอลล์ เพื่อเลือกลำดับของกฎที่จะลบออกได้อย่างถูกต้อง ก่อนที่จะทำการลบกฎนั้น



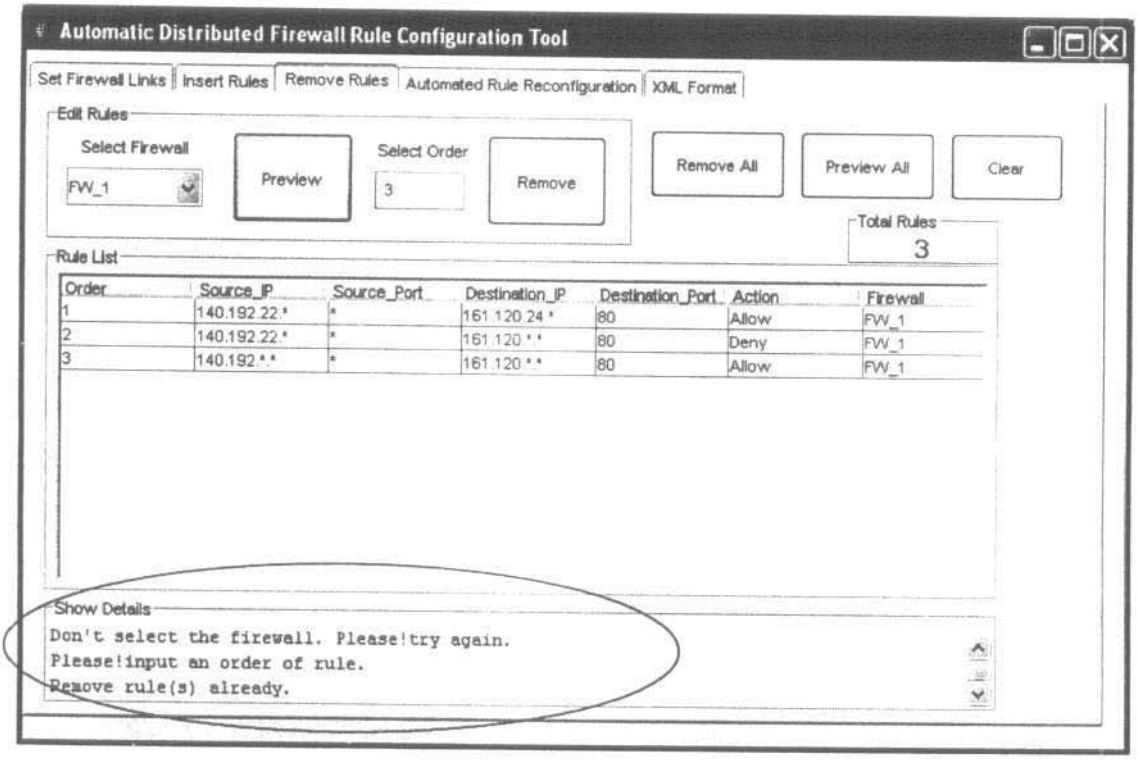
ภาพที่ ค.16 แสดงส่วน Edit Rules ในแถบ Remove Rules

(2) ส่วน Rule List เป็นส่วนที่ใช้แสดงรายการของกฎทั้งหมดที่อยู่ในไฟร์วอลล์ ซึ่งจะแสดงกฎเฉพาะไฟร์วอลล์ตัวใดตัวหนึ่ง หรือทุกๆ ตัวได้ขึ้นอยู่กับการความต้องการของผู้ใช้ขณะนั้น โดยทางด้านบนขวาในส่วน Total Rules ของตารางแสดงรายการมีการบ่งบอกถึงจำนวนของกฎทั้งหมดไว้ด้วย



ภาพที่ ค.17 แสดงส่วน Rule List ในแถบ Remove Rules

(3) ส่วน Show Details เป็นส่วนที่ใช้แสดงรายละเอียดที่เกี่ยวข้องกับการลบและการขอดูรายการของกฎของไฟร์วอลล์ที่ผู้ใช้เลือกไว้ ซึ่งจะแสดงข้อความต่างๆ เช่น ข้อความที่บ่งบอกถึงความผิดพลาดเมื่อผู้ใช้ไม่ได้เลือกไฟร์วอลล์ที่ต้องการจะลบกฎออก หรือข้อความที่บ่งบอกว่ากฎทั้งหมดในไฟร์วอลล์ได้ถูกลบแล้ว เป็นต้น



ภาพที่ ค.18 แสดงส่วน Show Details ในแถบ Remove Rules

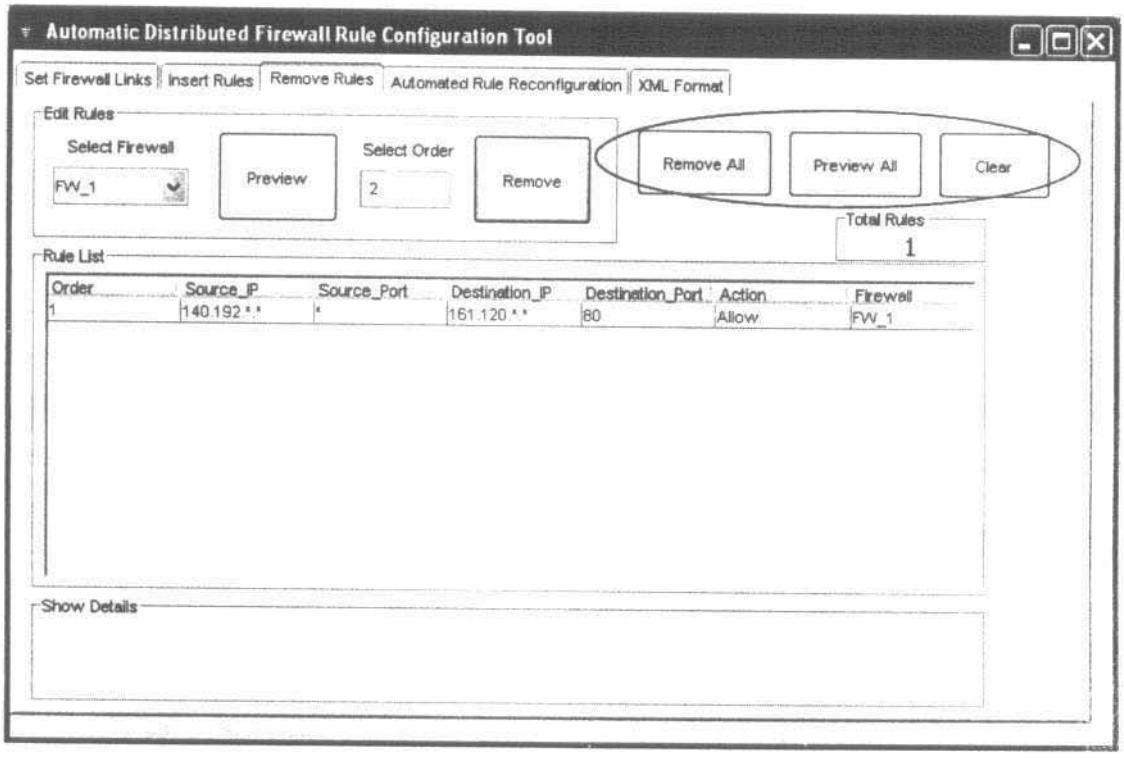
(4) ปุ่ม Preview เป็นปุ่มที่อยู่ในส่วน Edit Rules ที่ผู้ใช้จะกดเมื่อต้องการขอดูรายการของกฎทั้งหมดในไฟร์วอลล์ที่เลือกไว้ โดยกฎจะถูกแสดงไว้ในส่วน Rule List

(5) ปุ่ม Remove เป็นปุ่มที่อยู่ในส่วน Edit Rules ที่ผู้ใช้จะกดเมื่อต้องการลบกฎในลำดับและไฟร์วอลล์ที่กำหนดไว้ โดยจะทำการลบครั้งละ 1 กฎและในขณะที่ทำการลบนั้นจะมีการตรวจสอบและแก้ไขความผิดปกติของกฎต่างๆ ที่เหลือในไฟร์วอลล์โดยอัตโนมัติ ด้วยการใช้ Intra-firewall Anomaly Discovery Algorithm

(6) ปุ่ม Remove All เป็นปุ่มที่อยู่ด้านขวามือถัดจากปุ่ม Remove ในแถบ Remove Rules ที่ผู้ใช้จะกดเมื่อต้องการลบกฎทั้งหมดในไฟร์วอลล์ทุกๆ ตัวที่อยู่ในเครือข่าย เพื่อจะกำหนดกฎใหม่ให้กับไฟร์วอลล์แต่ละตัว

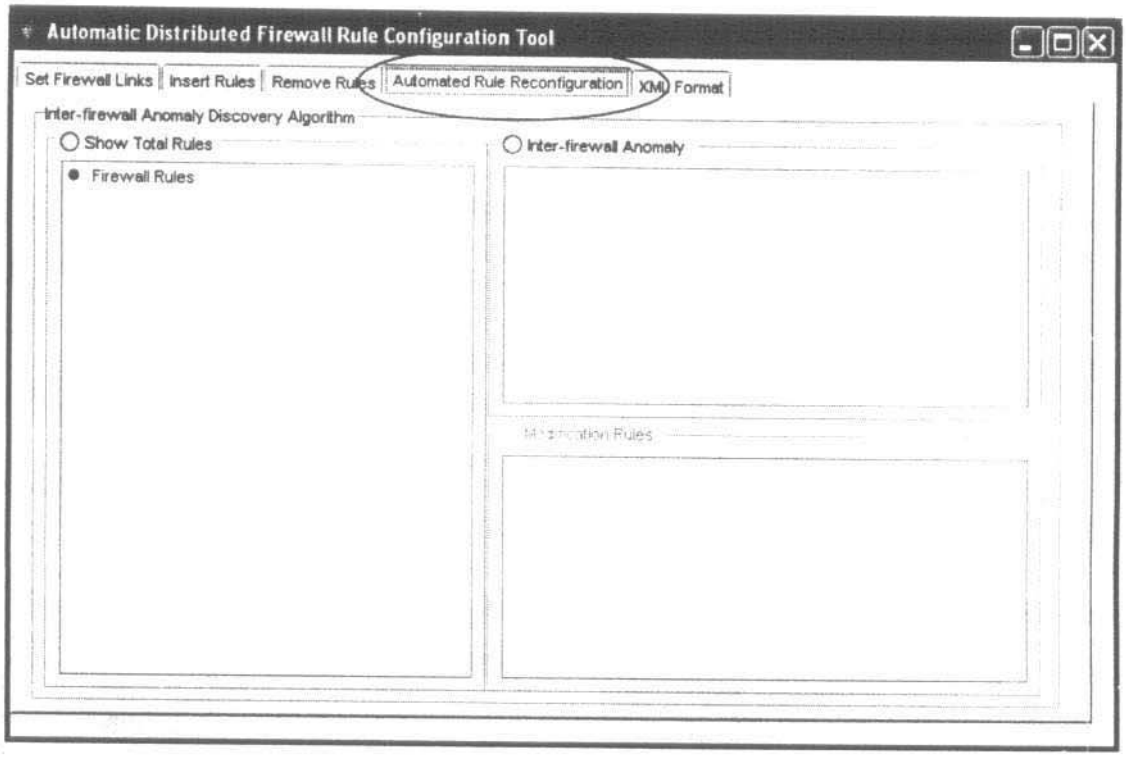
(7) ปุ่ม Preview All เป็นปุ่มที่อยู่ด้านขวามือถัดจากปุ่ม Remove All ในแถบ Remove Rules ที่ผู้ใช้จะกดเมื่อต้องการขอดูรายการทั้งหมดของกฎในทุกๆ ไฟร์วอลล์ที่อยู่ในเครือข่าย

(8) ปุ่ม Clear เป็นปุ่มที่อยู่ด้านขวามือถัดจากปุ่ม Preview All ในแถบ Remove Rules ที่ผู้ใช้จะกดเมื่อต้องการลบรายการของกฎในส่วน Rule List และข้อความที่แสดงไว้ในส่วน Show Details ทั้งหมดออก



ภาพที่ ค.19 แสดงปุ่ม Remove All, Preview All และ Clear ตามลำดับ ในแถบ Remove Rules

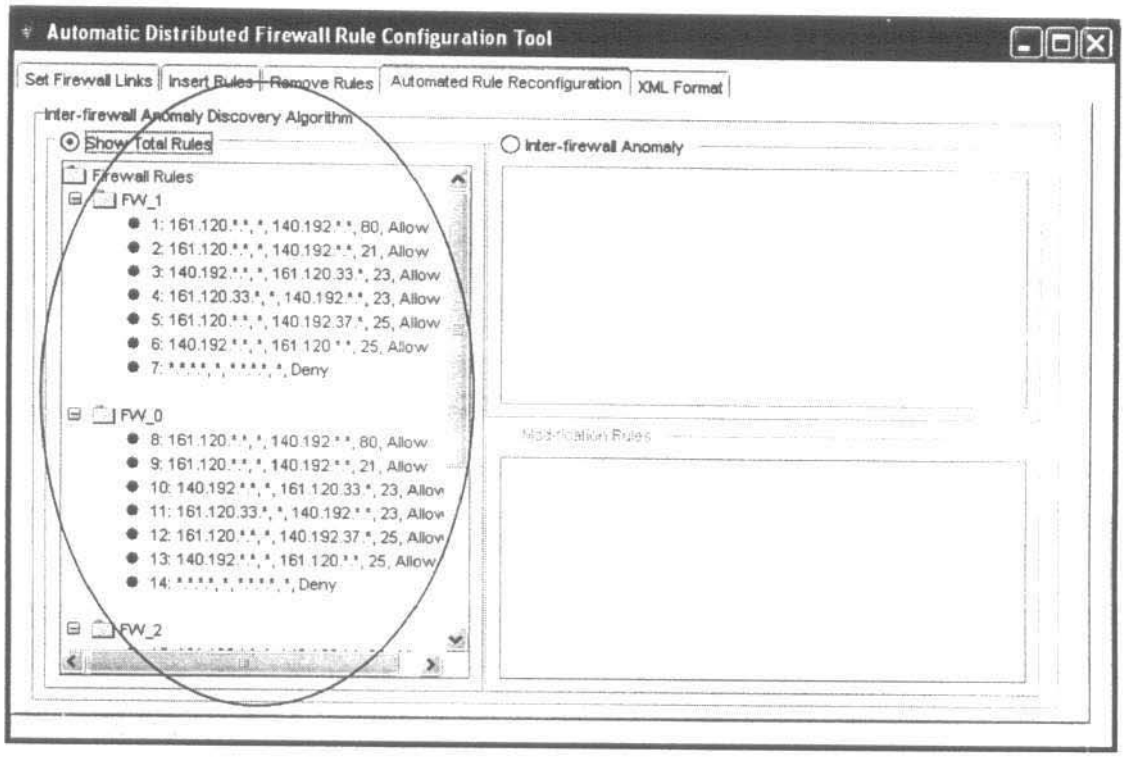
4) แถบ Automated Rule Reconfiguration เป็นแถบที่ถูกใช้เมื่อผู้ใช้ต้องการตรวจสอบความผิดปกติของกฎระหว่างไฟร์วอลล์ในเครือข่าย และต้องการแก้ไขความผิดปกตินั้นโดยอัตโนมัติ ซึ่งผลจากการแก้ไขความผิดปกติจะได้ว่าจะไม่มีความผิดปกติระหว่างกฎในไฟร์วอลล์เดียวกัน และไม่มีความผิดปกติของกฎระหว่างไฟร์วอลล์ในเครือข่ายด้วย โดยใช้ Intra-firewall Anomaly Discovery Algorithm และ Inter-firewall Anomaly Discovery Algorithm ตามลำดับ



ภาพที่ ค.20 แสดงแถบ Automated Rule Reconfiguration

แถบ Automated Rule Reconfiguration ประกอบด้วย 3 ส่วน ดังนี้

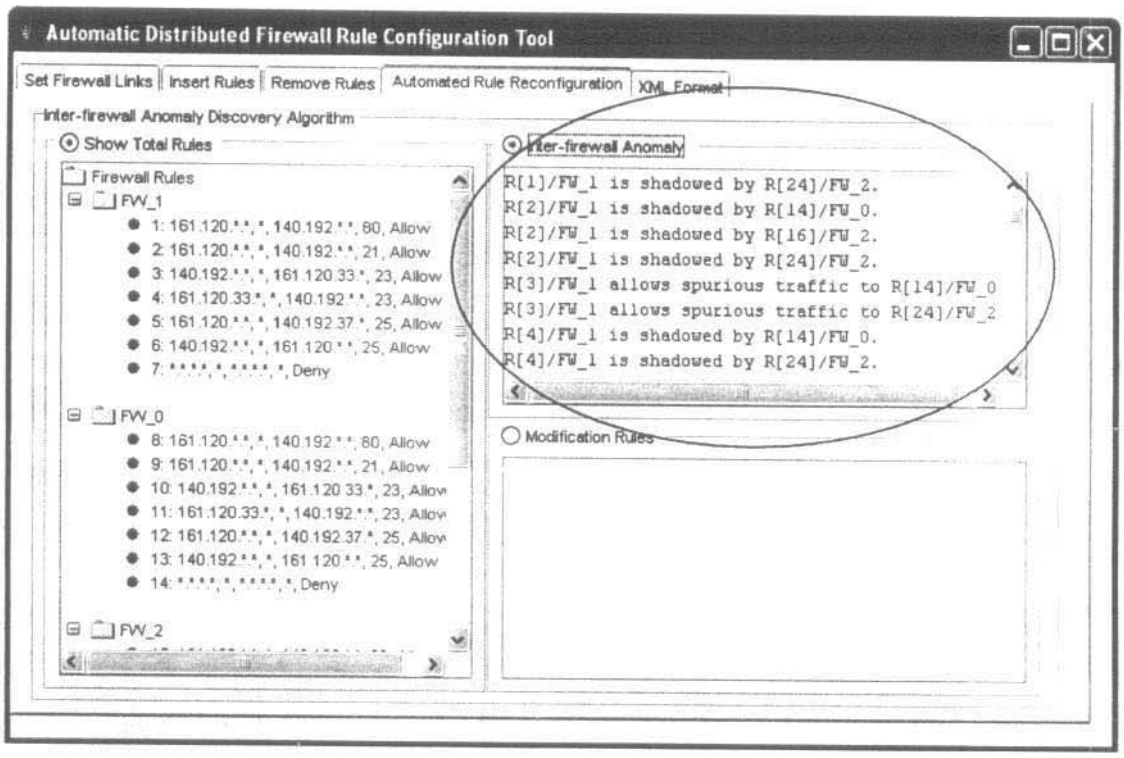
(1) ส่วน Show Total Rules เป็นส่วนที่ใช้แสดงรายการของกฎทั้งหมดในทุกๆ ไฟร์วอลล์ในเครือข่ายในรูปต้นไม้ (Tree) ที่ผู้ใช้ต้องการตรวจสอบและแก้ไขความผิดปกติของกฎระหว่างไฟร์วอลล์ โดยผู้ใช้สามารถเลือกตัวเลือก "Show Total Rules" เพื่อขอดูรายการของกฎทั้งหมด ในกรณีที่ผู้ใช้ไม่ต้องการดูรายละเอียดของกฎเหล่านั้นอีกก็สามารถเลือกที่ตัวเลือกนั้นซ้ำอีกครั้ง ซึ่งจะทำให้ข้อความที่ปรากฏอยู่หายไป



ภาพที่ ค.21 แสดงส่วน Show Total Rules ในแถบ Automated Rule Reconfiguration

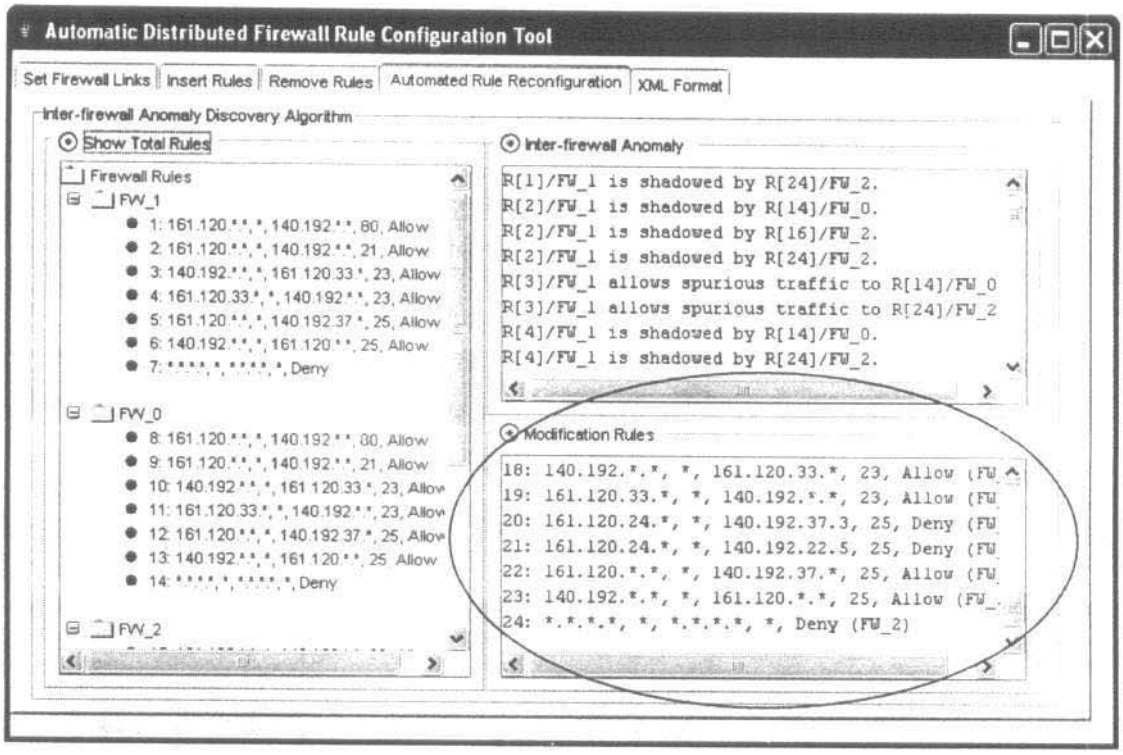
(2) ส่วน Inter-firewall Anomaly เป็นส่วนที่ใช้แสดงความผิดปกติของกฎที่เกิดขึ้นระหว่างไฟร์วอลล์ โดยจะปรากฏข้อความที่บ่งบอกถึงความผิดปกติแต่ละชนิดระหว่างกฎคู่ใดๆ ระหว่างไฟร์วอลล์ในเครือข่าย โดยผู้ใช้เลือกตัวเลือก "Inter-firewall Anomaly" เพื่อขอดูรายละเอียดของความผิดปกติทั้งหมดที่เกิดขึ้น ในกรณีที่ผู้ใช้ไม่ต้องการดูข้อความที่ปรากฏอยู่นั้นๆ อีกก็สามารถเลือกที่ตัวเลือกนั้นซ้ำอีกครั้ง ซึ่งก็จะทำให้ข้อความที่ปรากฏอยู่หายไป

นอกจากนี้ผู้ใช้ต้องทำการเลือกตัวเลือกในส่วน Inter-firewall Anomaly ก่อน ผู้ใช้จึงจะสามารถเลือกตัวเลือก Modification Rules ต่อไปได้ ทั้งนี้เนื่องจากกฎต่างๆ ที่จะถูกแก้ไขความผิดปกติต้องได้รับการตรวจสอบความผิดปกติจากส่วนนี้เสียก่อน



ภาพที่ ค.22 แสดงส่วน Inter-firewall Anomaly ในแถบ Automated Rule Reconfiguration

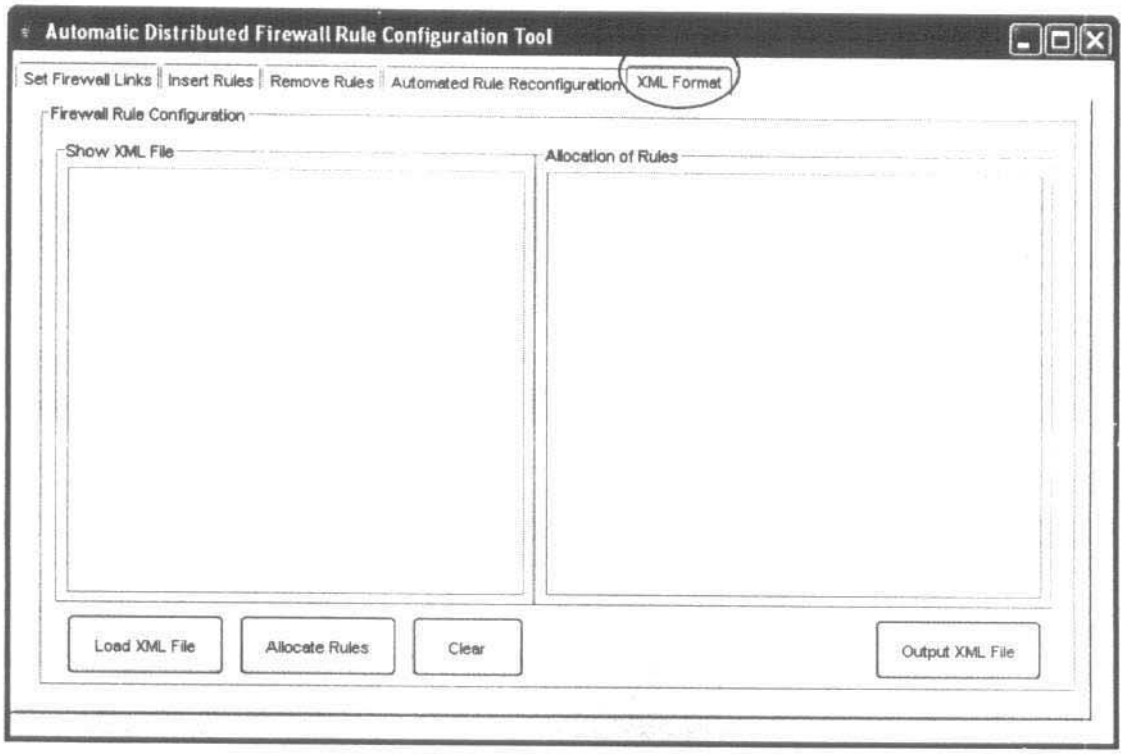
(3) ส่วน Modification Rules เป็นส่วนที่ใช้แสดงกฎทั้งหมดที่อยู่ในแต่ละไฟร์วอลล์หลังจากที่ถูกตรวจสอบและถูกแก้ไขความผิดปกติของกฎระหว่างไฟร์วอลล์โดยอัตโนมัติเรียบร้อยแล้วด้วย Intra-firewall Anomaly Discovery Algorithm และ Inter-firewall Anomaly Discovery Algorithm ควบคู่กัน โดยผู้ใช้สามารถเลือกตัวเลือก "Modification Rules" เพื่อขอดูรายการของกฎทั้งหมดได้ ในกรณีที่ผู้ใช้ไม่ต้องการดูข้อความที่ปรากฏอยู่นั้นๆ อีกก็สามารถเลือกที่ตัวเลือกนั้นซ้ำอีกครั้ง ซึ่งก็จะทำให้ข้อความที่ปรากฏอยู่หายไป



ภาพที่ ค.23 แสดงส่วน Modification Rules ในแถบ Automated Rule Reconfiguration

5) แถบ XML Format เป็นแถบที่ใช้สำหรับแฟ้มข้อมูลชนิด .xml (XML File) ที่ผู้ใช้สามารถคัดลอกแฟ้มข้อมูล (Download) ชนิด .xml เข้ามาสู่โปรแกรมประยุกต์ได้ ซึ่งภายในแฟ้มข้อมูลประกอบไปด้วยกฎต่างๆ ที่ยังไม่ได้ถูกระบุว่ากฎใดควรจะถูกจัดสรรไว้ในไฟร์วอลล์ตัวใดในเครือข่าย สำหรับ XML File ที่ถูกคัดลอกเข้ามาจะถูกนำไปใช้เพื่อนำไปวิเคราะห์และจัดสรรกฎลงในไฟร์วอลล์แต่ละตัวด้วย Rule Allocation Algorithm โดยไม่ให้เกิดความผิดปกติระหว่างกฎในไฟร์วอลล์เดียวกัน และไม่ให้เกิดความผิดปกติของกฎระหว่างไฟร์วอลล์ด้วย Intra-firewall Anomaly Discovery Algorithm และ Inter-firewall Anomaly Discovery Algorithm ตามลำดับ

นอกจากนี้ผลลัพธ์ที่ได้จากการจัดสรรกฎต่างๆ ลงในแต่ละไฟร์วอลล์ในเครือข่าย โดยไม่มีความผิดปกติใดๆ นั้น ผู้ใช้สามารถนำผลลัพธ์ที่ได้บันทึกเก็บไว้เป็นแฟ้มข้อมูลชนิด .xml ได้อีกด้วย ทั้งนี้เพื่อนำแฟ้มข้อมูลผลลัพธ์นี้ไปใช้ประโยชน์ต่อไปได้ง่ายและสะดวกขึ้น



ภาพที่ ค.24 แสดงแถบ XML Format

แถบ XML Format ประกอบด้วย 2 ส่วน และปุ่ม 4 ปุ่ม ดังนี้

(1) ส่วน Show XML File เป็นส่วนที่ใช้แสดงรายการของกฎที่ผู้ใช้ทำการคัดลอกจากแฟ้มข้อมูลชนิด .xml เข้าสู่โปรแกรมประยุกต์ เพื่อจัดสรรกฎเหล่านี้ลงในไฟร์วอลล์แต่ละตัวในเครือข่าย โดยแฟ้มข้อมูลต้องมีรูปแบบที่ถูกต้องตามโครงสร้างของแฟ้มข้อมูลชนิด .xml (XMLSchema) เท่านั้นจึงจะสามารถนำข้อมูลภายในแฟ้มข้อมูลไปทำงานต่อได้อย่างถูกต้อง

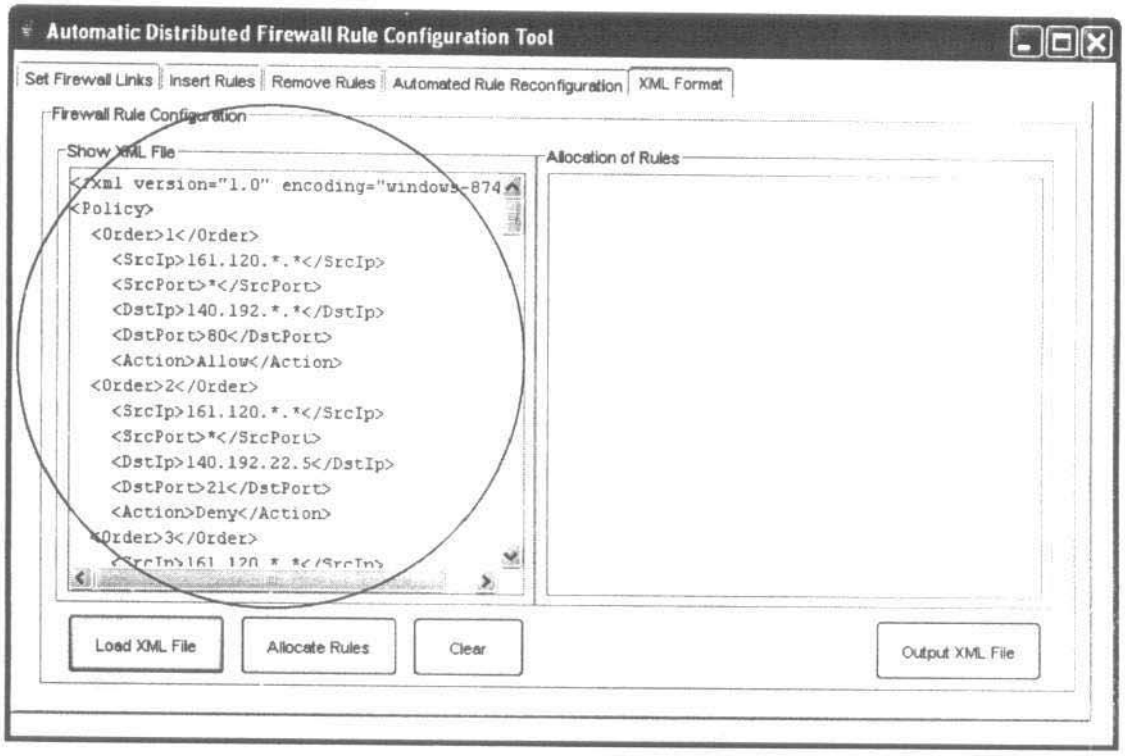
สำหรับโปรแกรมประยุกต์นี้ รูปแบบโครงสร้างของแฟ้มข้อมูลชนิด .xml ใช้ชื่อว่า Policy.xsd ดังภาพที่ ค.25 และตัวอย่างแฟ้มข้อมูลชนิด .xml ที่ถูกต้องตามโครงสร้างแฟ้มข้อมูลใช้ชื่อว่า Policy.xml ดังภาพที่ ค.26

```
<?xml version="1.0" encoding="windows-874"?>
<xs:schema attributeFormDefault="unqualified"
elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="Policy">
    <xs:complexType>
      <xs:sequence>
        <xs:choice maxOccurs="unbounded">
          <xs:element name="Order" type="xs:unsignedByte" />
          <xs:element name="SrcIp" type="xs:string" />
          <xs:element name="SrcPort" type="xs:string" />
          <xs:element name="DstIp" type="xs:string" />
          <xs:element name="DstPort" type="xs:string" />
          <xs:element name="Action" type="xs:string" />
        </xs:choice>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

ภาพที่ ค.25 แสดง XMLSchema ของแฟ้มข้อมูลชนิด .xml ที่ถูกต้อง (Policy.xsd)

```
<?xml version="1.0" encoding="windows-874"?>
<Policy>
  <Order>1</Order>
    <SrcIp>161.120.*.*</SrcIp>
    <SrcPort>*</SrcPort>
    <DstIp>140.192.*.*</DstIp>
    <DstPort>80</DstPort>
    <Action>Allow</Action>
  <Order>2</Order>
    <SrcIp>161.120.*.*</SrcIp>
    <SrcPort>*</SrcPort>
    <DstIp>140.192.22.5</DstIp>
    <DstPort>21</DstPort>
    <Action>Deny</Action>
  <Order>3</Order>
    <SrcIp>161.120.*.*</SrcIp>
    <SrcPort>*</SrcPort>
    <DstIp>140.192.*.*</DstIp>
    <DstPort>21</DstPort>
    <Action>Allow</Action>
  <Order>4</Order>
    <SrcIp>*.*.*.*</SrcIp>
    <SrcPort>*</SrcPort>
    <DstIp>*.*.*.*</DstIp>
    <DstPort>*</DstPort>
    <Action>Deny</Action>
</Policy>
```

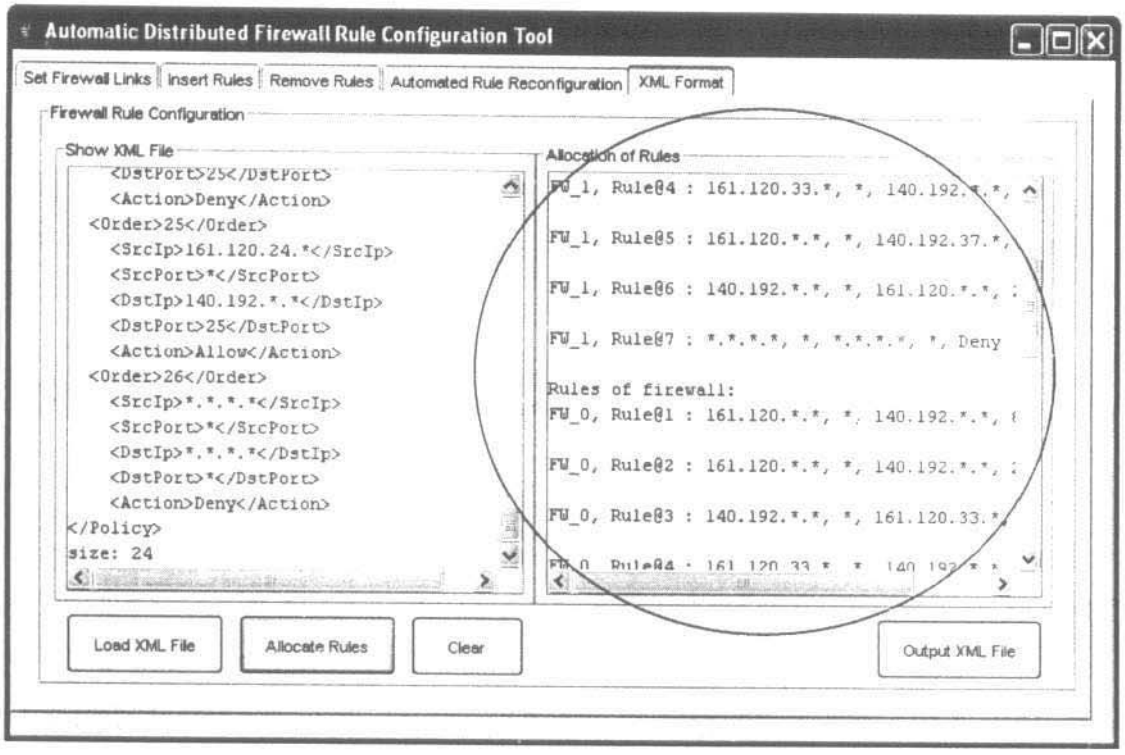
ภาพที่ ค.26 แสดงตัวอย่างรูปแบบแฟ้มข้อมูลชนิด .xml ที่ถูกต้อง (Policy.xml)



ภาพที่ ค.27 แสดงส่วน Show XML File ในแถบ XML Format

(2) ส่วน Allocation of Rules เป็นส่วนที่ใช้แสดงผลลัพธ์จากการจัดสรรรายการของกฎภายในแฟ้มข้อมูลลงในไฟร์วอลล์แต่ละตัวในเครือข่าย โดยรายการของกฎที่ปรากฏอยู่จะถูกตรวจสอบและแก้ไขความผิดปกติระหว่างกฎในไฟร์วอลล์เดียวกัน รวมถึงการตรวจสอบและแก้ไขความผิดปกติของกฎระหว่างไฟร์วอลล์ด้วย

นอกจากนี้ในขั้นตอนการจัดสรรกฎ หากพบว่าข้อมูลในแต่ละเขตข้อมูลของกฎใดกฎหนึ่งไม่ถูกต้อง เช่น เขตข้อมูลไอพีคือ 140.192.kkk.*, m.m.m.m, a.1.a.1 ฯลฯ มีบางส่วนที่เป็นตัวอักษรไม่ใช่ตัวเลขไอพีที่ถูกต้อง เช่น 140.192.*.*, 140.192.22.*, 161.120.24.3 ฯลฯ หรือเขตข้อมูลช่องทางคือ ggg, 788888, h ฯลฯ ค่าของเขตข้อมูลช่องทางไม่ได้เป็นตัวเลขตั้งแต่ 0-65536 (16 บิต) หรือไม่เท่ากับเครื่องหมายดอกจัน (*) หรือเขตข้อมูลแอ็คชันคือ allow, deny, ann ฯลฯ ค่าของเขตข้อมูลไม่เท่ากับ "Allow" หรือ "Deny" แล้วกฎนั้นก็จะไม่ถูกจัดสรรลงในไฟร์วอลล์ หรือกฎถูกจัดสรรลงในไฟร์วอลล์ แต่ไม่สามารถนำกฎในไฟร์วอลล์นั้นๆ ไปใช้งานได้อย่างถูกต้อง เป็นต้น

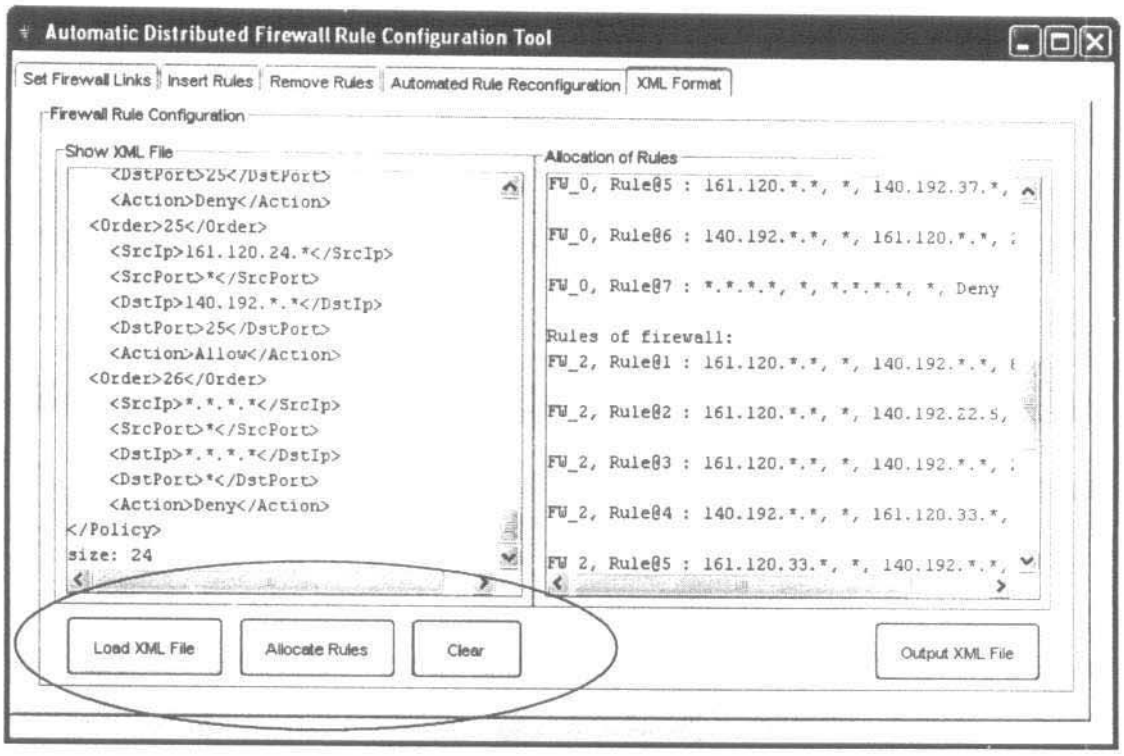


ภาพที่ ค.28 แสดงส่วน Allocation of Rules ในแถบ XML Format

(3) ปุ่ม Load XML File เป็นปุ่มแรกที่อยู่ด้านล่างซ้ายมือสุดในแถบ XML Format ที่ผู้ใช้จะกดเมื่อต้องการนำแฟ้มข้อมูลชนิด .xml เข้าสู่โปรแกรมประยุกต์ โดยแฟ้มข้อมูลต้องมีรูปแบบที่ถูกต้องตาม XMLSchema เท่านั้นจึงจะสามารถคัดลอกข้อมูลภายในแฟ้มข้อมูลเข้าสู่โปรแกรมประยุกต์ได้อย่างถูกต้อง

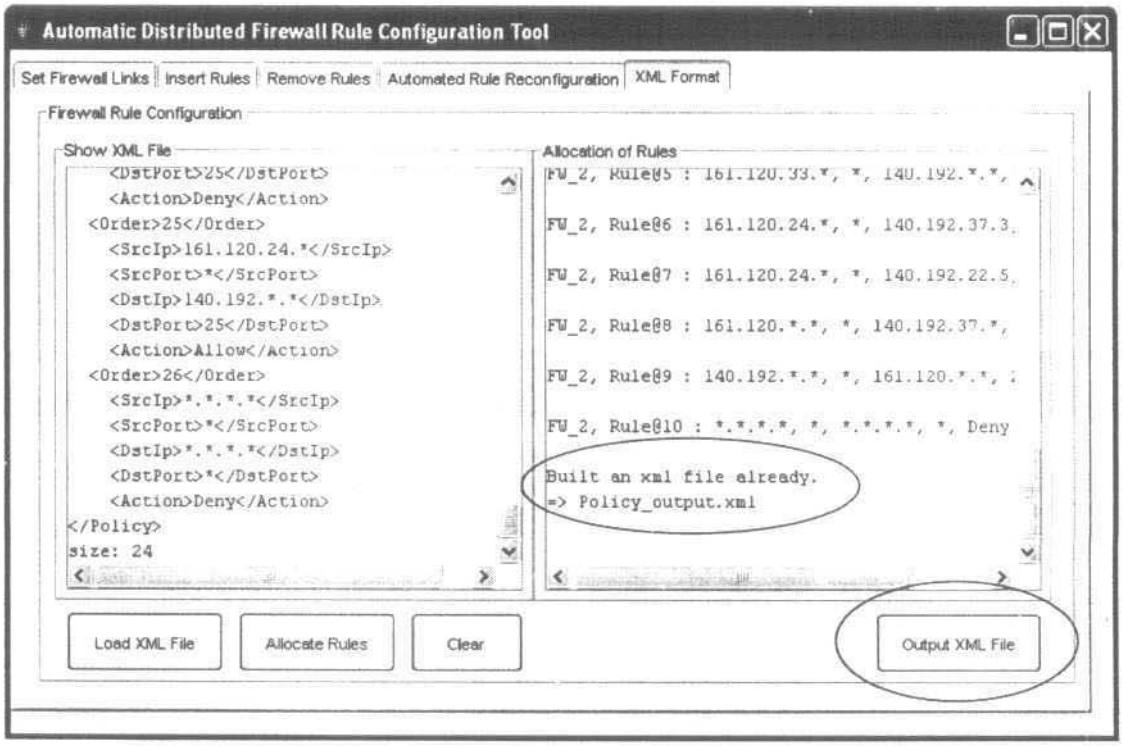
(4) ปุ่ม Allocate Rules เป็นปุ่มถัดจากปุ่ม Load XML File ที่อยู่ด้านล่างซ้ายมือในแถบ XML Format ที่ผู้ใช้จะกดเมื่อต้องการจัดสรรรายการของกฎที่นำเข้ามาลงในแต่ละไฟร์วอลล์ได้อย่างถูกต้องโดยใช้ Rule Allocation Algorithm และขณะจัดสรรกฎจะต้องไม่เกิดความผิดปกติระหว่างกฎในไฟร์วอลล์เดียวกัน และไม่เกิดความผิดปกติของกฎระหว่างไฟร์วอลล์โดยการใช้ Intra-firewall Anomaly Discovery Algorithm และ Inter-firewall Anomaly Discovery Algorithm ตามลำดับ

(5) ปุ่ม Clear เป็นปุ่มถัดจากปุ่ม Allocate Rules ที่อยู่ด้านล่างซ้ายมือในแถบ XML Format ที่ผู้ใช้จะกดเมื่อต้องการลบข้อความในส่วน Show XML File และ Allocation of Rules ออก



ภาพที่ ค.29 แสดงปุ่ม Load XML File, Allocate Rules และ Clear ตามลำดับ

(6) ปุ่ม Output XML File เป็นปุ่มที่อยู่ด้านล่างขวามือสุดในแถบXML Format ที่ผู้ใช้จะกดเมื่อต้องการสร้างแฟ้มข้อมูลผลลัพธ์ชนิด .xml (XML File) ซึ่งในโปรแกรมประยุกต์นี้ได้กำหนดชื่อแฟ้มข้อมูลผลลัพธ์คือ Policy_output.xml เพื่อนำแฟ้มข้อมูลนี้ไปใช้งานต่อได้อย่างสะดวกและง่ายขึ้น เมื่อโปรแกรมประยุกต์สร้างแฟ้มข้อมูลผลลัพธ์เสร็จเรียบร้อยแล้วจะแสดงข้อความในส่วน Allocation of Rules คือ Built an xml file already. => Policy_output.xml



ภาพที่ ค.30 แสดงผลลัพธ์จากการบันทึกข้อมูลและปุ่ม Output XML File ในแถบ XML Format

การใช้โปรแกรมประยุกต์ Automatic Distributed Firewall Rule Configuration Tool มีดังนี้

ผู้ใช้ต้องการเพิ่มกฎของไฟร์วอลล์ด้วยตนเอง ให้ผู้ใช้ทำตามขั้นตอนต่อไปนี้

1) กำหนดรายละเอียดของโครงรูปเครือข่าย (Network topology) ในส่วน **"Set Firewall Links"** เป็นลำดับแรกเสมอก่อนการทำงานในส่วนอื่นๆ ของโปรแกรมประยุกต์ ค่าต่างๆ เช่น ชื่อไฟร์วอลล์ แม่ข่ายหรือไฟร์วอลล์ตัวอื่นๆ ซึ่งเชื่อมโยงกับไฟร์วอลล์ตัวที่ผู้ใช้กำลังกำหนดค่า เป็นต้น

2) การใส่ข้อมูลของกฎทีละกฎเองให้ใช้ส่วน **"Insert Rules"** เพื่อกรอกรายละเอียดของกฎและกดปุ่ม Add เพื่อเพิ่มกฎในแต่ละไฟร์วอลล์

3) ระหว่างที่ทำการเพิ่มกฎตามข้อ 2) ถ้าผู้ใช้ต้องการเปลี่ยนลำดับของกฎหรือเปลี่ยนแปลงค่าของเขตข้อมูลใดเขตข้อมูลหนึ่งของกฎหรือแก้ไขกฎใดกฎหนึ่งสามารถทำได้โดยใช้ส่วน **"Remove Rules"** ซึ่งส่วนนี้ผู้ใช้สามารถใช้งานได้ตามความต้องการตลอดการทำงานบนโปรแกรมประยุกต์นี้ จากนั้นให้กลับไปทำตามข้อ 2) จนเสร็จ

4) เมื่อทำตามข้อ 2) เสร็จสมบูรณ์แล้ว ผู้ใช้สามารถตรวจสอบความถูกต้องและแก้ไขความผิดปกติของกฎระหว่างไฟร์วอลล์ได้โดยให้ใช้ส่วน **"Automated Rule Reconfiguration"** ให้ผู้ใช้เลือกตัวเลือก Inter-firewall Anomaly ถ้าต้องการดูชนิดของความผิดปกติที่เกิดขึ้น และเลือกตัวเลือก Modification Rules ถ้าต้องการแก้ไขความผิดปกติทันที ซึ่งตัวเลือก Inter-firewall Anomaly จะต้องถูกเลือกก่อนตัวเลือก Modification Rules เสมอ เนื่องจากมีการทำงานอย่างเป็นลำดับคือ ตรวจสอบความผิดปกติของกฎ และตามด้วยการแก้ไขความผิดปกติเหล่านั้น

5) ผลลัพธ์จากการใช้โปรแกรมประยุกต์สามารถบันทึกเป็นแฟ้มข้อมูลชนิด xml ได้โดยใช้ส่วน **"XML Format"** ให้ผู้ใช้กดปุ่ม Output XML File ด้านล่างมุมขวามือ โดยแฟ้มข้อมูลผลลัพธ์ใช้ชื่อว่า "Policy_output.xml"

ผู้ใช้ต้องการเพิ่มกฎของไฟร์วอลล์ด้วยแฟ้มข้อมูลชนิด .xml ให้ผู้ใช้ทำตามขั้นตอนต่อไปนี้

1) เตรียมรายการของกฎที่ต้องการคัดลอกเข้าสู่โปรแกรมประยุกต์ตามรูปแบบของแฟ้มข้อมูลที่อธิบายไว้ในหัวข้อแถบ XML Format ในส่วน Show XML File ให้ถูกต้อง โดยใช้ชื่อแฟ้มข้อมูลว่า "Policy.xml"

2) กำหนดรายละเอียดของโครงรูปเครือข่ายในส่วน **"Set Firewall Links"** เป็นลำดับแรกเสมอก่อนการทำงานในส่วนอื่นๆ ของโปรแกรมประยุกต์

3) ผู้ใช้สามารถใช้ข้อมูลในแฟ้มข้อมูลชนิด .xml ตามข้อ 1) ได้ในส่วน **"XML Format"** โดยเริ่มจากการคัดลอกแฟ้มข้อมูลเข้าสู่โปรแกรมด้วยปุ่ม Load XML File และตามด้วยการจัดสรรกฎลงในไฟร์วอลล์แต่ละตัวในเครือข่ายด้วยปุ่ม Allocate Rules

4) หลังจากทำตามข้อ 3) ถ้าผู้ใช้ต้องการเปลี่ยนลำดับของกฎหรือเปลี่ยนแปลงค่าของเขตข้อมูลใดเขตข้อมูลหนึ่งของกฎหรือแก้ไขกฎใดกฎหนึ่งสามารถทำได้โดยให้ไปแก้ไขในแฟ้มข้อมูล Policy.xml ตามข้อ 1) แล้วจึงทำตามข้อ 3) ต่อไป หรือ

ถ้าผู้ใช้ต้องการแก้ไขกฎในโปรแกรมประยุกต์โดยที่ไม่ต้องการคัดลอกแฟ้มข้อมูลใหม่ให้ผู้ใช้ไปที่ส่วน **"Remove Rules"** และทำตามขั้นตอนต่อไปนี้

(1) ผู้ใช้ต้องลบ "Default filtering rule" ของไฟร์วอลล์ทุกๆ ตัวออกก่อน

(2) ผู้ใช้เลือกกฎที่ต้องการลบออก

(3) ผู้ใช้สามารถเพิ่มกฎใหม่ของไฟร์วอลล์ที่ต้องการได้ในส่วน **"Insert Rules"**

(4) ผู้ใช้ต้องเพิ่ม "Default filtering rule" ให้ไฟร์วอลล์ทุกๆ ตัว หลังจากที่ปรับเปลี่ยนหรือเพิ่มหรือแก้ไขกฎที่ต้องการแล้ว

(5) ผู้ใช้ต้องตรวจสอบและแก้ไขความผิดปกติของกฎระหว่างไฟร์วอลล์อีกครั้งในส่วน **"Automated Rule Reconfiguration"**

5) ผลลัพธ์จากการใช้โปรแกรมประยุกต์สามารถบันทึกเป็นแฟ้มข้อมูลชนิด .xml ได้โดยให้ผู้ใช้กดปุ่ม Output XML File ด้านล่างมุมขวามือในส่วน **"XML Format"** ซึ่งแฟ้มข้อมูลผลลัพธ์ใช้ชื่อว่า "Policy_output.xml"