An Adaptive RAR Tree-Based Diagnosis System for Rule Anomalies among Network Firewalls

趙啟時　　邱振添
逢甲大學通訊工程學系
m0102190@fcu.edu.tw

摘要

隨著資訊時代的來臨，網路使用需求日益增加，防火牆提供網管者一個控制網路流量的平台。近年來許多已開發中的防火牆規則診斷系統，已可幫助網管者完成規則設定異常的查找工作，並針對某些異常種類、事件提出告警。但就目前了解，這些系統多半還有許多的改進空間;診斷的效能、擴充性與發生異常種類往往不夠全面且具代表性。本研究將改進之前的開發成果，結合影像處理區域分割法(Region Splitting)，提出一套以自適性規則異常樹的診斷系統(Adaptive RAR)。該系統採用二元樹(Binary Tree)架構，相較於[1]來說，具備更快速的診斷速度與良好的擴充性，進而更貼近管理者之實際需求。

關鍵詞：防火牆規則異常、區域分割法、規則異常關係樹、多防火牆間規則異常

1. 前言

現今網路中，氾濫的網路攻擊與多樣的入侵方式快速發展，造成網路使用者無法有效保護個人網路資源。為此，防火牆扮演了一個非常重要的角色，在惡意行為在進入所屬電腦前，即可於網際網路中有效的偵測並阻絕。一般而言，網管者管理著多個分散各處的防火牆，當其管理之網路範圍越大時，各防火牆內部的規則數目會相對的成長，其所需的安全分析時間也就同樣相對的增加。為此，各種確保防火牆政策正確性的研究，已廣泛被學者、專家們開始重視，並開發出不少出眾的診斷系統。

近年來，許多學者相繼投入防火牆規則異常診斷的相關技術研究領域當中。在[3][4]之前之研究，多半都針對單一規則異常現象或者特殊情形提出建議，直到[3][4]才將防火牆規則異常依照其產生的情形，分析、分類出詳細的種類與產生因果，並提出一套系統性的診斷方法。但當防火牆數量增多或政策出現異動等狀況時，[3][4]的診斷方法所需的時間將大幅增加。[5][6]繼[3][4]研究後，提出完整一套適用於診斷規則異常現象的系統與運算，並提出聯合規則異常之觀念。[5]利用圖形幾何學(Geometry)的特性，依其演算法將防火牆規則轉換成有效之圖形資料結構，用以剔除大量無異常之規則比對，以符合高速網路龐大的封包過濾處理需求。但此診斷方式在進行多防火牆間的規則異常診斷時，必須重新另啟診斷程序，無法有效利用已完成診斷之結果。[6]提出 BISCAL 演算法，利用拓樸學(Topological Approach)的切割區塊方式，只記錄少量的規則向量，取代[5]所產生的大量區塊訊息，達到節省大量的記憶體空間並有效率的加速診斷時間。但若發生防火牆政策異動，卻需重新統計各規則條件的範圍邊界值，並計算新的規則向量，因此欠缺良好的可擴充性。為此[1][2]提出 RAR Tree(Rule Anomaly Relation Tree)異常關係樹系統，其具備快速的診斷速度與良好的可擴充性，在多防火牆安全聯防的大型網路環境中，更能合乎管理者之實際需求。[1]雖可提供高效率的診斷速度，與精確的規則異常訊息。但是，該架構還存在著許多可以改善的地方。例如:區塊範圍 A 將流量過濾空間切割為若干大小相等的區塊，當流量過濾空間中的規則太過於集中、分散或者規則發生變動，此時區塊範圍 A 如果設置不當，診斷時間則會大幅增加。

以上學者們的貢獻，可以清楚知道此領域研究近年來受到極大的重視，且有著許多迫切的問題需要解決。為此本研究觀察上述不同的診斷方式，將先前的研究成果加以改進提出 Adaptive RAR 診斷系統，並具備下列特性，使其回報結果能真正合乎管理者之需求：

- 防火牆診斷結果可再利用，具備高度系統擴充能力；
- 擁有高效率的診斷速度；
- 提供精確且完善的規則異常資訊。

本文在第 2 章節將淺談[1]是如何在防火牆內與多防火牆間進行異常診斷，並且提出幾項能夠改善的問題。第 3 章節中，提出 Adaptive RAR 診斷系統，並討論該改進系統如何進行防火牆規則異常診斷。最後，第 4 章節比較本文與先前研究或者其他學者們研究的優缺點，藉此證明是否符合本論文希望達成的各項能力，並提出總結以及未來展望。

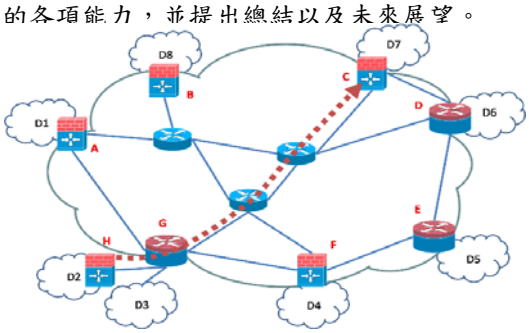

圖 1 規則異常診斷拓樸

2. 異常關係樹診斷系統

本章節中，將陳述[1]所提出之 RAR 規則異常關係樹，及如何利用該樹進行防火牆規則異常診斷，該系統有別於[5]的切割方式，乃採用固定大小之區塊範圍 A 對規則進行切割，並將切割區塊中存在之規則儲存於樹狀結構中。下面我們將淺談 RAR 規則異常關係樹之建構與診斷方式，並針對防火牆內部規則異常(Intra-Anomaly)，與多防火牆間規則異常(Inter-Anomaly)分別進行討論，並說明該樹狀架構所具備之優缺點。

2.1 防火牆內部規則異常診斷

本小節將藉由圖 1 範例拓樸，說明如何利用 RAR 規則異常關係樹之診斷流程，診斷防火牆內部規則異常。首先，管理者需自網路拓樸選取欲分析路徑上之起始/終止兩網域(如 D2→D7)。在 D2→D7 路徑中，流量將經過 H、G、C 三台防火牆，因此分析 D2→D7 路徑時只需分別取出 H、C、與 G 防火牆的相關規則，再將其依照不同服務(Port)加以分類，即完成 D2→D7 所需分析的相關路徑規則選取前置作業。圖 2 假設 D2 為 192.168.0.*與 D7 為 192.168.1.*，且表示 H 防火牆上已分類出之有關 D2→D7 與 Port 80 相關規則。

接下來，將規則自身有效影響範圍，經固定區塊範圍 A 切割後判斷出應座落之流量過濾圖相關區塊位置(圖 3)，並將其紀錄在 RAR 樹狀結構中，最後利用區塊與規則間關係快速將彼此間不可能產生異常的規則比對程序剔除。圖 4 為依照圖 2 建立之 RAR 規則異常關係樹，其中□代表的是規則的條件，○代表的是經由區塊範圍 A=32*32 (S_{IP}*D_{IP})切割後，代表規則範圍的 Source IP 區塊座標與 Destination IP 的區塊座標，▲是代表座落在此區塊中允許通過(Accept)的規則，△則是代表座落在此區塊中被拒絕(Deny)的規則；當規則 2 加入 RAR 規則異常關係樹區塊時，可發現其欲加入之區塊已存在規則 1，因此可推得 H 防火牆內規則 1 與規則 2 有可能發生異常，並將兩規則進一步加以利用[3]的防火牆內部規則異常有限狀態機比對後，得知其

Firewall H				
Name	Order	Source IP Address	Destination IP Address	Action
R1	1	192.168.0.64~192.168.0.95	192.168.1.128~192.168.1.210	accept
R2	5	192.168.0.0~192.168.0.95	192.168.1.160~192.168.1.210	deny
R3	7	192.168.0.0~192.168.0.95	192.168.1.128~192.168.1.159	deny
R4	21	192.168.0.0~192.168.0.223	192.168.1.0~192.168.1.63	accept
R5	22	192.168.0.144~192.168.0.223	192.168.1.32~192.168.1.63	deny
R6	39	192.168.0.144~192.168.0.195	192.168.1.32~192.168.1.127	deny
R7	40	192.168.0.144~192.168.0.223	192.168.1.96~192.168.1.127	accept

圖 2 H 防火牆有關網域 2 到 7 之 HTTP 服務規則

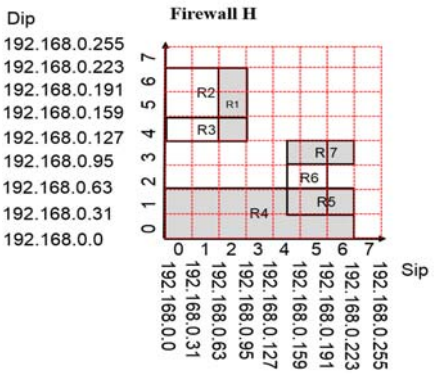

圖 3 H 防火牆有關 HTTP 服務從網域 2 到 7 之流量過濾圖(RAR)

確實發生規則異常。以此類推，當圖 2 的 7 個規則加入後，即可診斷出下列 5 組可能發生的規則異常：規則 1 與 3、1 與 2、4 與 5、4 與 6、6 與 7。接著，只需將這些規則進一步進行規則防火牆內部規則異常種類的判斷，即可完成 H 防火牆的防火牆內部規則異常種類分析，在此只需 5 組比較避免以往[3]共需要將全部規則進行C_2^7=21 組比較，節省大量運算時間。此外圖 3 流量過濾圖也可清楚看出兩規則之異常，可看出 RAR 規則異常關係樹確實保留了流量過濾圖的特性。

2.2 多防火牆間規則異常診斷

2.1 節中，D2→D7 路徑中的 H 防火牆已完成內部規則異常分析，接下來將進一步考慮如何針對該路徑上其它防火牆，進行多防火牆間規則異常診斷。首先，因 G 防火牆位於 H 防火牆之後，所以在建構出 H 防火牆內規則異常關係樹後，接著將會挑

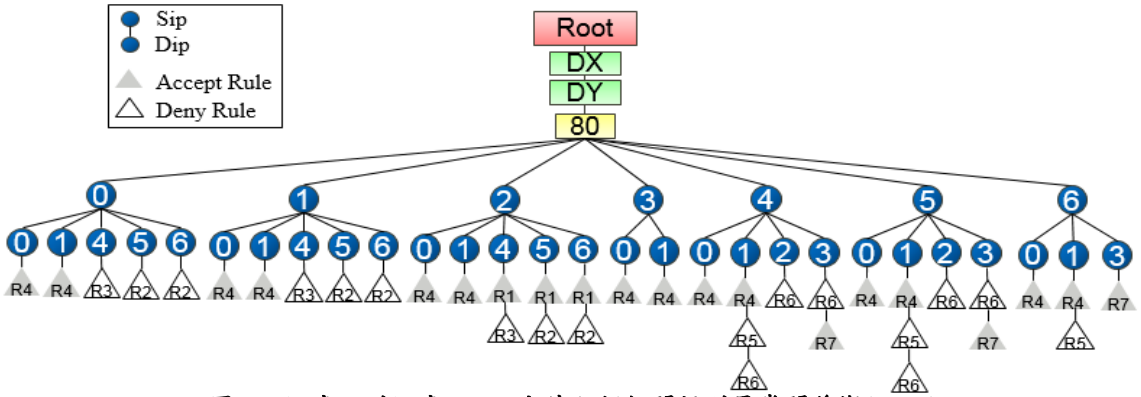

圖 4 網域 2 到網域 7H 防火牆內部相關規則異常關係樹(RAR)

選 G 防火牆上相關之規則(圖 5)。此時，利用 2.1 節防火牆內部規則異常的切割步驟，逐一將 G 防火牆規則加入 RAR 規則異常關係樹中(圖 6)。並利用[3]所定義防火牆間規則異常有限狀態機進行比對，即可得知G防火牆的相關規則與H防火牆的相關規則，有無多防火牆間規則異常情形發生。

以圖 6 為例：當 G.R2 加入 RAR 規則異常關係樹時，分別座落在 4-2、5-2 與 6-2 三個區塊中。其中，在 6-2 區塊中卻已存在 H.R7 與 G.R1，代表著 G.R2 與 H.R7 有產生多防火牆間規則異常的可能外，還與 G.R1 有產生防火牆內部規則異常的可能。因此，只需藉由[3]所定義之防火牆間規則異常有限狀態機比對，即可得知 G 防火牆的相關規則與 H 防火牆的相關規則，有無防火牆間規則異常情形發生。由上述中可得知，當未使用 RAR 規則異常關係樹時，G.R2 額需要與 H 防火牆的 7 個規則以及自身 G 防火牆 4 個規則做比對。當利用 RAR 規則異常關係樹架構後，發現 G.R2 只“可能”與 H.R7 與 G.R1 發生規則異常，因此只需分析這三者間是否產生規則異常即完成診斷，有效的避免其它對規則無意義的分析、計算。

縱觀以往學者進行多防火牆間規則異常診斷的方式，[3]需花費大量時間將所有相關規則進行兩兩比對，而[6]需統計各規則條件欄位的邊界值並重新進行切割、診斷，因此皆無法有效重用防火牆內部規則異常診斷結果，加速多防火牆間規則異常診斷之進行。[1]提出之 RAR 規則異常關係樹中確實比其它診斷方式優異，但其中還有許多需要改善的地方，如:①採用固定大小的區塊範圍 A 做切割，當此值設定不當時，診斷效能反而會因此下降。②當 RAR 關係樹建立完成後，還須做進一步的診斷，無法立即得知規則間是否有發生異常。③當區域範圍 A 值較小，而防火牆規則範圍較大時，樹狀結構會較寬(Width)，診斷時間也會變得不理想。

3. 自適性規則異常樹診斷系統

本文提出自適性規則異常樹(Adaptive RAR)，輔助防火牆規則異常診斷，將[1]資料結構與影像處理的區域分割法(Splitting)做結合，提出自適性規則異常樹的規則診斷系統。該系統除了保有[1]的高度的擴充性與區域診斷結果再利用之能力，還能省下更多的診斷時間與運算空間，更能合乎管理面之實際需求。下面我們將詳細介紹自適性規則異常樹之建構與規則異常診斷方式，並針對防火牆內部規則異常、多防火牆間規則異常診斷分別進行討論，並說明使用該架構所具備之優缺點。

Firewall G				
Name	Order	Source IP Address	Destination IP Address	Action
R1	3	192.168.0.192~192.168.0.223	192.168.1.32~192.168.1.127	deny
R2	8	192.168.0.144~192.168.0.223	192.168.1.64~192.168.1.95	accept
R3	10	192.168.0.32~192.168.0.95	192.168.1.64~192.168.1.95	deny
R4	12	192.168.0.0~192.168.0.95	192.168.1.0~192.168.1.95	accept
R5	15	192.168.0.144~192.168.0.192	192.168.1.159~192.168.1.200	deny

圖 5 G 防火牆有關網域 2 到 7 之 HTTP 服務規則

3.1 防火牆內部規則異常診斷

藉由圖 1 範例拓樸，在此說明如何利用自適性規則異常樹之診斷流程，診斷防火牆內、外部規則異常。其流程圖如圖 7，步驟如下分述：

Step1.網管者選取兩個指定網域(Domain X → Domain Y)構成欲分析的路徑，其 Domain X 位址範圍構成代表來源端位址的橫軸，其 Domain Y 位址範圍構成為代表目的端位址的縱軸，建立起相關之二維規則條件流量過濾空間(如圖 3)。

Step2.將影響該路徑上之所有規則條件放至該流量過濾圖中，依照流量過濾圖的本質，每條防火牆規則的規則條件在流量過濾圖上會形成一個相關矩形，代表其規則有效影響 IP 位置範圍。接著利用圖 10(a)演算法，運算取得最適合切割之大小起始區塊範圍 A 以供建構 Adaptive RAR 架構。

Step3.利用 A 對流量過濾圖進行除法切割運算，進而判斷規則有效影響範圍應座落在哪些流量過濾圖上的區塊，並將此一資訊記錄在 Adaptive RAR 結構中。

Step4.當發現 Adaptive RAR 結構已經存在其它規則

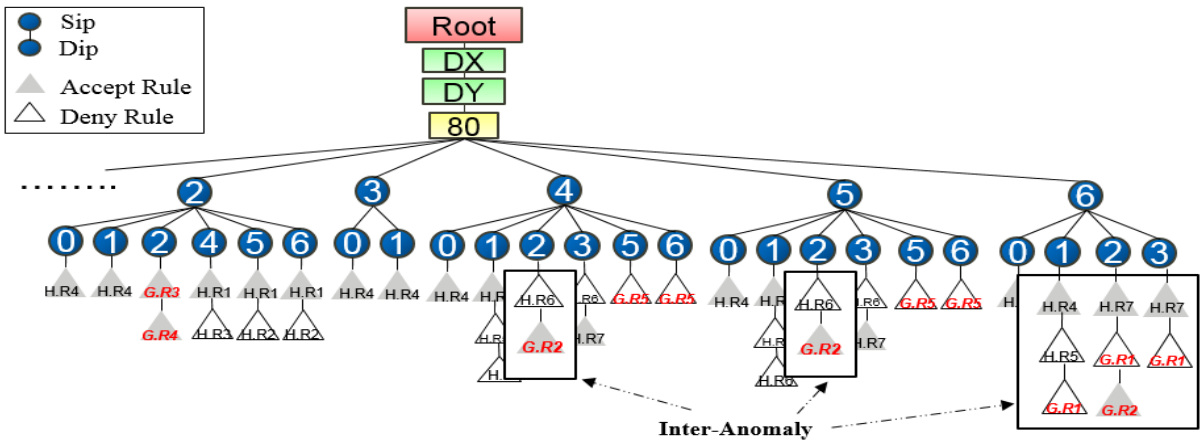

圖 6 網域 2 到網域 7H 與 G 防火牆間相關規則異常關係樹

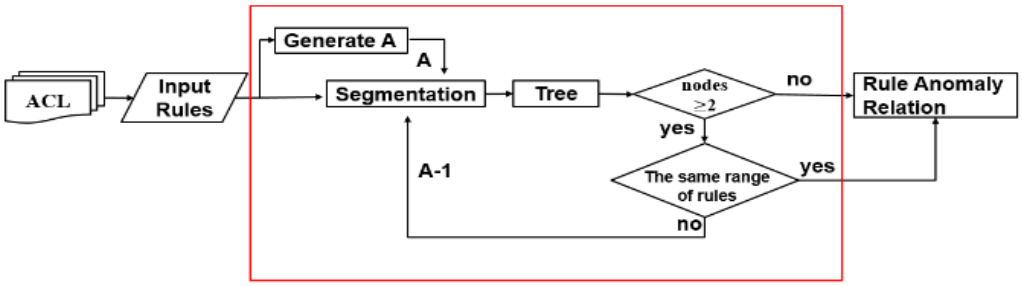

圖 7 Adaptive RAR 自適性規則異常樹流程圖

時(rule≥2)，則將進一步分析這些規則彼此間影響的範圍是否相同。如規則影響範圍不相同時，則利用圖 10(b)演算法將 A 做修改傳回 Step3.重新做細部的切割，直到影響範圍相同為止。

這樣即可完成自適性規則異常樹之建構，完成後立即可以診斷出防火牆規則異常，不需要再做進一步分析計算。以 D2→D7 為例，將 H 防火牆規則逐一輸入至二維流量過濾空間後(圖 8(a))，得知流量過濾空間的最大範圍值後，利用圖 10(a)演算法即可取得適合此流量過濾圖切割之區塊大小 A(A=7)。得到起始區域範圍 A 後，接下來將相關規則有效影響 IP 範圍位置，經 A 切割並判斷規則有效影響位置範圍應座落於哪些流量過濾圖上的區塊(圖 8(b))，並將其結果紀錄在 Adaptive RAR 樹狀結構中。當發現樹狀結構已經存在其它規則時(rule≥2)，將進一步分析這些規則彼此間影響的範圍是否相同。當規則影響範圍不同時，則利用圖 10(b)演算法將 A 做修改並進行細部切割。最後當規則彼此間影響的範圍相同時(圖 8(d))，自適性規則異常樹建置即完成建置(圖 9)。

而上述 Step 2 的自適性規則異常樹，要如何利用圖 10(a)的演算法，取得最適合流量過濾空間切割之區塊範圍 A 呢?在先前的研究中，區域範圍 A 與防火牆規則影響範圍並沒有直接的關係，所以當區域範圍 A 設定不當時，效能反而會有影響。本研究採用二元樹的架構，並且結合區域分割法，不但能夠解決區域範圍 A 設置問題，還能夠避免樹狀結構過寬的情形。如下所述:

以 H 防火牆為例，可以從圖 2 中得知 Source IP 與

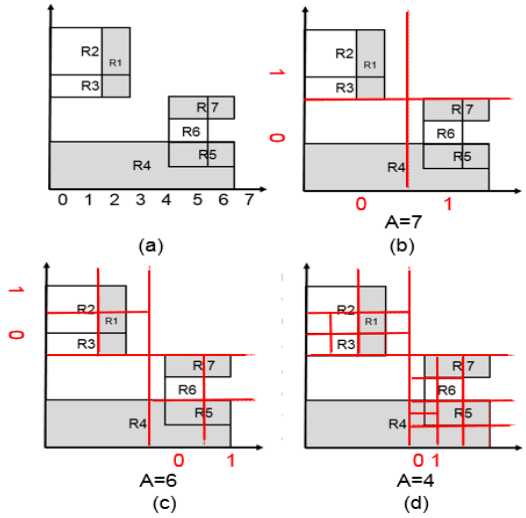

圖 8 H 防火牆有關 HTTP 服務從網域 2 到 7 之流量過濾圖(Adaptive RAR)

Destination IP 最大值都為 223，利用圖 10(a)的演算法，即可得到流量過濾空間的起始切割區塊範圍為 A=7。接下來利用除法運算將防火牆規則進行切割，其切割計算內容以 H 防火牆的規則 1 來做舉例：$S_{IP}/2^A = 64/2^A \sim 95/2^A = 0$、$D_{IP}/2^A = 128/2^A \sim 210/2^A = 1$；其代表 H 防火牆的規則 1 有效影響範圍座落在編號為 0-1 的這個區塊中，並將此資料儲存在自適性規則異常樹中。H 防火牆規則經過 A=7 切割所產生的自適性規則異常樹如圖 11 (a)，我們可以發現到在編號 0-1 與 1-0 這兩區塊中，規則 1、2、3 與規則 4、5、6、7 彼此間影響的範圍並不相同。此時要做細部切割，所以將區域切割範圍 A 與目前樹狀結構的

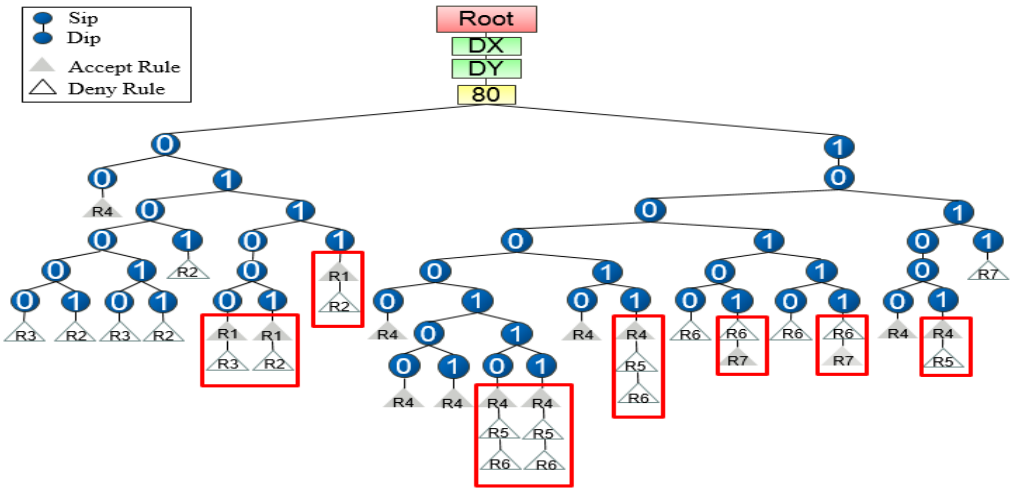

圖 9 網域 2 到網域 7H 防火牆內部自適性規則異常樹

層級(level)代入圖 10(b)演算法中得到新的切割值，並且將 0-1 與 1-0 兩區塊的規則重新做切割，直到規則彼此間規則影響位置範圍相同為止，即可完成自適性規則異常樹之建立。

圖 9 自適性規則異常樹建立完成時，即可“立即”診斷出下列 5 組規則間發生規則異常：規則 1 與 3、規則 1 與 2、規則 4 與 5、規則 4 與 6、規則 6 與 7。由之先前的成果[1]與本方法都可以診斷 H 防火牆的 5 組規則異常，但並不能立即的檢測出規則是否有異常，僅能告知規則間有異常發生可能。在記憶體上[1]RAR 規則異常關係樹需記錄 28 個節點與 38 組規則資訊，而使用 Adaptive RAR 自適性規則異常樹則需記錄 31 個節點與 35 組規則資訊即可完成規則異常診斷。雖然節點數在 H 防火牆這個範例中表現的較多一點，但 Adaptive RAR 卻可以立即診斷出規則異常區域，且無需另外比較。此外，因為 Adaptive RAR 結構是採用二元樹方式，且起始區域範圍 A 值最小為 1、高度(Height)最高為 32，所以在大型網路中並不會像[1]造成較寬樹的資料結構，進而影響診斷的時間。

3.2 多防火牆間規則異常診斷

上一小節初步利用自適性規則異常關係樹分析出防火牆內部規則異常。接下來將進一步考慮如何利用 Adaptive RAR 來進行多防火牆間規則異常診斷。以圖 1 為為例，路徑上 G 防火牆位於 H 防火牆之後，所以將 H 與 G 防火牆兩個自適性規則異常關係樹依照起始區域範圍 A 做合併(圖 13)，即完成 G 防火牆與 H 防火牆的多防火牆間規則異常分析(圖 12) 。同理 C 防火牆也如同上述 G 防火牆之方式，一一將每個防火牆的自適性規則異常關係樹做合併，即完整偵測 D2→D7 路徑上所有可能發生的防火牆間規則異常偵測。

由上述診斷方式中可知道，每當新防火牆欲加入診斷時，皆能利用自適性規則異常樹，將該路線上已診斷之防火牆規則訊息加以利用，無需額外花費大量時間將其相關規則全部再加以診斷，達到理想之診斷速度與可過擴充性。在先前研究[1]中是將後續防火牆的規則輸入至已經建立好的 RAR 規則異常樹中，每當選擇新的路徑時，則必須重新讀取防火牆的規則，才能建立起 RAR 規則異常樹。這對於大型網路來說，會造成效能與系統上的負擔。當然也可以先採取在每個防火牆上先建立起自己的 RAR 規則異常關係樹，當要做多防火牆偵測時在將兩關係樹合併即可完成診斷。但[1]當兩防火牆區域

```
generate_init_A(maxCoordinate)
Input:  maxCoordinate
Output: init_A
1:  While (maxCoordinate & (maxCoordinate-1))
2:    maxCoordinate = maxCoordinate & (maxCoordinate-1)
3:  Return maxCoordinate
```

(a)

```
updateA(ruleCoordinate, init_A,level)
Input:  Coordinate, init_A
Output: A
1:  tmp=generate_init_A(init_A)
2:  IF ruleCoordinate  < init_A
3:  THEN
4:     init_A & = ~( tmp>>(level-1) )
5:  ENDIF
6:     init_A |= tmp>>level
7:  Return init_A
```

(b)

圖 10 流量圖切割之區塊範圍 A 演算法

範圍 A 值不相同時，則必須從新切割，如此一來還是會耗費許多時間。由此可知自適性規則異常樹在診斷速度與擴充性上比[1]還要好。

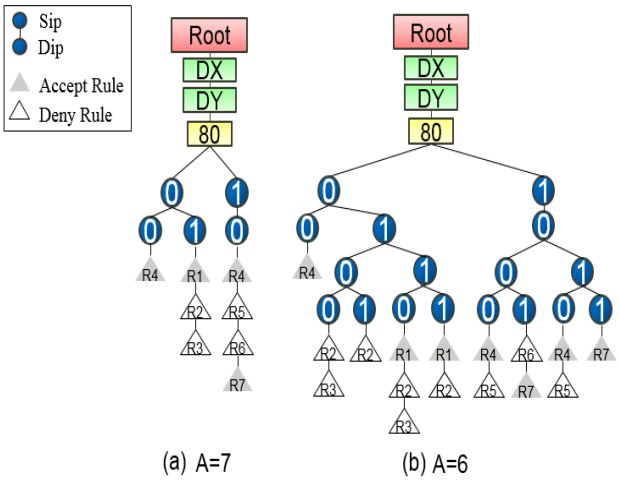

圖 11 防火牆 H 自適性規則異常樹建立過程

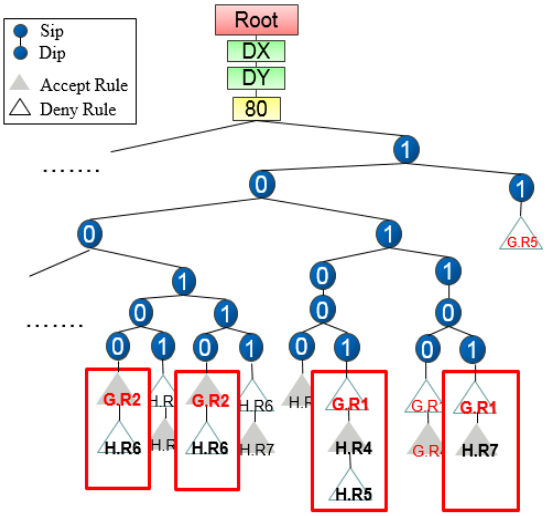

圖 12 網域 2 到網域 7H 與 G 防火牆間相關規則異常關係樹

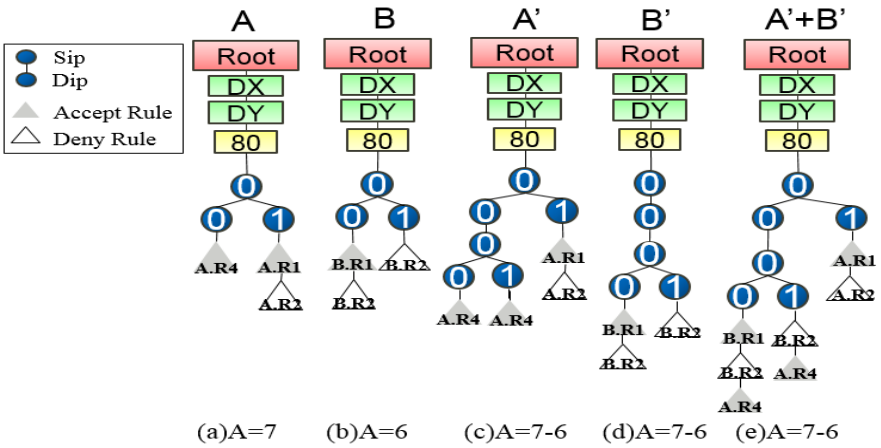

圖 13 規則異常關係樹合併過程

4. 系統評估與未來展望

從前面兩章節可以了解，先前的研究並不能立即的檢測出規則是否有異常，僅能告知規則間有異常發生可能。且[1]是採用固定大小的區域範圍切割值當此值決定不恰當時，效能上反而會有影響。在管理範圍較大的網路還會造成切割區塊過多，導致記憶體使用量過多(圖 14)。此外在多防火牆間規則異常診斷上，在單一路徑上，但當選擇新的路徑時，則必須重新讀取後續防火牆的規則，才能建立起 RAR 規則異常樹，在可擴充性上還可以再改善。

本文所提出的自適性規則異常樹可對防火牆規則進行高效率的診斷過濾動作，避免診斷系統運行龐大的規則相互比對運算，大幅提升規則異常診斷速度。並且對於多防火牆安全聯防的環境中，能有效利用區域診斷之結果，大幅提升診斷速度與可擴充性。另外當各防火牆規則數隨拓樸變化或政策異動時，該架構也無需重新進行大量的規則比對或是規則切割等動作，具備相當良好的可用性。儘管系統有著上述的多項優點，但還是有著不足之處，本研究未來將鎖定這些地方加以深入研究、探討。例如①本系統一旦加入其它的規則條件進行切割時，在多維空間中如何快速診斷規則異常? ②在 IPv6 網路中，自適性規則異常關係樹是否還有其它的改進空間。

參考文獻

[1] M. H. Y. C.S. Chao, H.Y. Pan, "A RAR Tree-Based Diagnosis System for Rule Anomalies among Network Firewalls," presented at the TANET, 2010.

[2] M. H. Yu, "A RAR Tree-Based Diagnosis System for Rule Anomalies and Behavior Mismatching among Network Firewalls," Feng Chia University Department of Communications Engineering, Feng Chia University, 2010.

[3] E. Al-Shaer, H. Hamed, R.Boutaba and M. Hasan, "Conflict Classification and Analysis of Distributed Firewall Policies," IEEE Journal on Selected Areas in Communications, Vol. 23, Is. 10, pp. 2069-2084, 2005.

[4] Ehab Al-Shaer and Hazem Hamed," Modeling and Management of Firewall Policies", IEEE Transactions on Network and Service Management, Vol: 1-1, April 2004.

[5] Yi Yin, Yoshiaki Katayama and Naohisa Takahashi, "Detection of Conflicts Caused by a Combinations of Filters Based on Spatial Relationships", IPSJ Journal, Sep 2008, Vol.49, pp. 3121-3135.

[6] Subana Thanasegaran, Yi Yin, Yuichiro Tateiwa, Yoshiaki Katayama and Naohisa Takahashi, "Topological Approach to Detect Conflicts in Firewall Policies," International Workshop on Security in Systems and Networks, Proc. of 23rd IEEE International Parallel and Distributed Processing Symposium, SSN-1569173665-paper-3.pdf (2009).

[7] A. Liu, "Firewall Policy Verification and Troubleshooting", Computer Networks, Vol. 53, Is. 16, pp. 2800-2809, 2009.

[8] Chi-Shih Chao and Stephen J.H. Yang ,"A Novel Three-Tiered Visualization Approach for Firewall Rule Validation", Journal of Visual Languages and Computing.

	小型網路		大型網路		多防火牆
	規則較密集	規則較分散	規則較密集	規則較分散	可擴充性
	診斷時間	記憶體	診斷時間	記憶體	
RAR	較多	少	較多	較多	普通
Adaptive RAR	少	適中	少	適中	佳

圖 14 規則異常關係樹效能比較