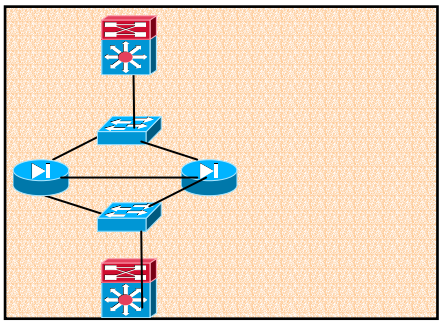
熱備用式與負載平衡式防火牆建置概述

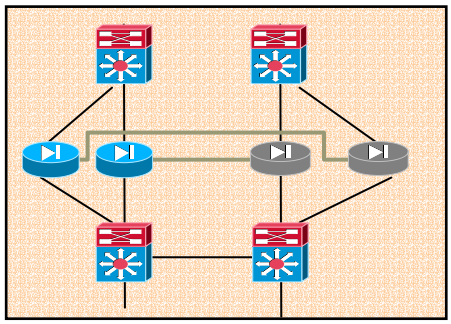
/台灣思科系統提供

網路安全是現代企業在面臨電子商務挑戰時不可或缺的基礎 ，因此許多企業在建構網際網路連線時，均將高可用性(High Availability) 列為建構的必要條件，例如要求多家不同 ISP 的連線 、由不同電信局端進線、 考量多台伺服器之間的負載平衡機制，以及加上路由器、交換器、 防火牆之備援等，以達成不中斷服務的要求。

在防火牆方面，常見的方式有圖 A 的熱備用式（Failover）和 圖 B 的負載平衡式 (Load Balance) 。



A.Firewall with FailOver



B.CSM FWLB with PIX Failover Feature

防火牆熱備用（Failover）的好處，主要在於防火牆發生故障(硬體、軟體、網路等各種因素)而無法提供服務時，備用之防火牆能在最短時間內(5-30秒)接手原主要防火牆之工作，使企業內外之網際網路存取不致中斷，架構簡單與轉換快速是其特色。

架構簡單：包含的網路元件只有主要防火牆和熱備用防火牆，不但建構容易而且管理方便，不必面對安全政策同步問題，在除錯上也因網路元件的簡化而使除錯過程速度加快，儘早排除問題。

轉換快速：在機制上熱備用防火牆與主要防火牆會建立溝通管道(透過 RS232 or LAN Cable)，將主要防火牆上設定之〝位址轉換表〞session 狀態，即時傳送至備用防火牆，一旦備用防火牆接手主要防火牆之工作，即可在不中斷使用者 session 情況下(如 FTP Telnet …等)， 提供企業所需之即時(不中斷)的服務。

而熱備用架構的缺點是防火牆在熱備用狀態下並不提供服務，所有服務均由主要防火牆擔任，其主要工作在備用 ，而且主要與備用防火牆須為同一品牌。

若是企業網路流量甚大（超過 1Gbps），且單一防火牆效能無法勝任時，為避免防火牆過度負荷，成為網路上之瓶頸，使用者此時可以運用負載平衡的方式來滿足大頻寬流量的需求。

其做法是在防火牆的前後外掛一對或使用同一個負載平衡器(藉由負載平衡器判別 L4-L7 之功能)，使網路流量能平均分配在多個防火牆上，優點是流量能平均負載在多個防火牆上，可提昇整體效能(此時負載器反而可能是流量瓶頸所在)， 不再受限於防火牆的效能上。

然而多個獨立防火牆同時運作，再加上前後之負載平衡器，使得網路設計之元件增加、管理上的複雜度增加，在除錯上亦增加困難度，在防火牆網路安全政策制定與維護上也需注意政策同步的問題(特別是做異類防火牆負載時)；另一問題是整體的架構建置與維護費用將隨著架構的複雜度而升高。另一設計上的缺點是此種架構無法做防火牆間的熱備用，由於各個防火牆獨立運作，在發生故障時，故障之防火牆上的使用者將會失去其與伺服器之連結，使用者必須重新啟動應用程式或重新連結，在強調即時不中斷的應用環境下造成困擾。

有些使用者喜歡使用總匯三明治的方式建構負載平衡防火牆，即在多部負載平衡器前後各放異類防火牆，例如-LB1-FWa-LB2-LB3-FWb-LB3 的方式。今日，在駭客多使用 port redirect 及 firewall rule bypass 攻擊方式情況下，此種架構在安全上能否發揮 1+1=2 的投資效果實有待商確。使用者宜考慮設置入侵偵測系統，以期達到全面防禦的效果。