網路防火牆規劃工具之建議

為了減少眾多資訊安全事件所帶來的危害，許多的組織在網際網路與組織內部網路之間建立網路防火牆作為防禦之用，如此無法預防另一半由組織內部所引起的資訊安全事件。此外，單有網路防火牆並不能做好資訊安全事件的防範，更重要的是訂定適當的網路防火牆政策並且架構符合政策的網路防火牆。本研究將網路防火牆的屬性及特質，抽象成網路防火牆模型，再依據網路防火牆模型，提出網路防火牆政策正規化模式及網路防火牆模型圖，用來協助分析網路防火牆政策及網路防火牆架構。在網路防火牆政策正規化模式中，可以將網路服務存取政策分析為網路防火牆設計政策，並且依據安全政策的意義，將重複效果的政策刪減。網路防火牆模型圖用來表示安全政策中被保護實體的關聯性，以及被保護實體與網路防火牆實體的關聯性，可以表示出完全達到安全政策要求,而且規則不重複的網路防火牆架構，使人容易明瞭實體之間的關係。在規劃組織網路時，網路防火牆政策正規化模式及網路防火牆模型圖可以協助規劃符合組織安全政策的網路架構。若在現有網路架構的情況下，搭配既成的網路拓樸，網路防火牆在現有網路架構中可能配置的位置，可以明確的被推斷出來。在配置有網路防火牆的網路架構下，同樣可以利用網路防火牆正規化模式與網路防火牆模型圖，重新檢視組織網路配置的適當性。