如何防御中間人攻擊？

中間人攻擊是一个利用相互認證漏洞的攻擊，由於客户端與服務器之間在SSL握手的過程中缺乏相互認證而造成的漏洞，最理想的防制方法是網路內的每電腦的ARP一律改用靜態的方式，不過這在大型的網路是不可行的，因為需要經常更新每電腦的ARP表。另外一種方法，例如DHCP snooping，網路設備可藉由DHCP保留網路上各電腦的MAC位址，在偽造的ARP封包發出時即可偵測到，此方式已使用在部分網路設備產品上。

有一些軟體可監聽網路上的ARP回應，若偵測出有不正常變動時可發送電子郵件通知管理者。簡單來說就是把動態路由設定成靜態路由static route，不過靜態路由在每次重新開機之後都會變回動態路由，也就是說每到一個新網路的時候第一件事情就是把動態路由改成靜態路由，這樣就可以避免所謂的arp攻擊。

防御中間人攻擊的方案通常基於以下幾種技術

* 公鑰基礎建設PKI

使用PKI相互認證機制，客户端驗證服務器，服務器驗證客户端；上述兩个例子中都是只驗證服務器，這樣就造成了SSL握手環節的漏洞，而如果使用相互認證的的话，基本可以

* 更强力的相互認證
* 延遲測試

使用複雜加密哈希函數進行計算以造成數十秒的延遲；如果雙方通常情况下都要花費20秒来計算，並且整个通訊花費了60秒计算才到達對方，這就能表明存在第三方中間人。

* 使用其他形式的密鑰交換形式

如果已經被攻擊了要怎麼辦？

如果你已經被這類的手法給攻擊了，可以先下arp -d 這個指令，先清空arp快取。之後在馬上找出正確的default gateway 設成靜態路由，就可以解除被攻擊的窘境。