附件 4 頻寬消耗型攻擊及資源消耗型攻擊建議做法

一、頻寬消耗型攻擊建議做法表

設備	建議做法
路由器	啟用速率限制以及存取控制(ACL)機制，並針對封包之來源 IP 位址進行檢測和過濾
DDoS 防禦系統	暫時調整 DDoS 設備防護至高等級，阻擋可疑攻擊行為
	攔截異常封包內容，例如不完整、格式錯誤的標頭或不完整封包等
	針對特殊性質以及特定通訊協定方式之 DDoS 攻擊，例如 ICMP Flood、UDP Flood 攻擊等進行防護
	限制每秒單一來源 IP 連線數
	利用查問驗證機制防禦機器人攻擊
	IP 信譽偵測，阻擋已知惡意來源 IP
	透過國別 IP 清單，阻擋來自特定國家的 IP
入侵防禦系統	針對已知漏洞或異常網路傳輸行為設定阻擋
交換器	啟用速率限制以及存取控制(ACL)機制，並針對封包之來源 IP 位址進行檢測和過濾
CDN	針對攻擊流量進行流量過濾
	利用查問驗證機制防禦機器人攻擊
	減少至原始主機的網路流量與降低主機資源消耗
流量清洗服務	針對攻擊流量進行清洗動作或轉導，阻擋境外或來自特定國家的 IP

二、資源消耗型攻擊建議做法表

設備	建議做法
DDoS 防禦系統	暫時調整 DDoS 設備防護至高等級，阻擋可疑攻擊行為
	攔截異常封包內容，例如不完整、格式錯誤的標頭或不完整封包等
	針對特殊性質以及特定通訊協定方式之 DDoS 攻擊，例如 SYN Flood、應用層 DDoS 攻擊等進行防護
	調整 DNS 查詢失敗阻擋規則，例如每秒查詢失敗 X 次即進行阻擋
	分析攻擊 payload，設定正規表示法(Regular expression)規則進行阻擋
	限制每秒單一來源 IP 連線數
	利用查問驗證機制防禦機器人攻擊
	IP 信譽偵測，阻擋已知惡意來源 IP
	透過國別 IP 清單，阻擋來自特定國家的 IP
入侵防禦系統	針對已知漏洞或異常網路傳輸行為設定阻擋
網站應用程式防火牆	確認網站攻擊來源 IP 及 HTTP 欄位特徵
	阻擋使用慢速請求佔用每筆連線之慢速攻擊
	限制特定頁面存取頻率限制
	分析攻擊封包內容，並視攻擊特徵客制化攔阻規則

CDN	針對攻擊流量進行流量過濾
	利用查問驗證機制防禦機器人攻擊
	減少至原始主機的網路流量與降低主機資源消耗