政府組態基準

Palo Alto Firewall 11

TWGCB-03-005

(預告版V1.0)

國家資通安全研究院

中華民國113年11月

修訂歷史紀錄表

項次	版次	修訂日期	說明
1	1.0	113/11/15	新編
2			
3			
4			
5			

目　次

表 目 次

1. 前言

政府組態基準(Government Configuration Baseline, 以下簡稱 GCB)目的在於規範資通訊終端設備(如：個人電腦)的一致性安全設定(如：密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之疑慮。

1.1 適用環境

本文件適用於運行 Palo Alto PAN-OS 11.x 版本之防火牆設備。

1.2 項數統計

政府組態基準針對電腦作業環境提供一致性安全基準與實作指引，供政府機關透過建立安全組態，提升資安防護能力。Palo Alto Firewall 11 組態基準項目統計(詳見表 1)，須部署之基本項目共計 25 項(詳見表 2)，包含設備設定、密碼政策、鑑別設定、設備服務設定、安全性設定檔及安全性政策等 6 類別設定項目，接著再依設備所選擇使用之授權(如 WildFire、威脅防禦及 URL 過濾)，額外部署相對應之組態基準設定，包含 WildFire 組態基準 4 項設定項目(詳見表 3)、威脅防禦組態基準 11 項設定項目(詳見表 4)，以及 URL 過濾組態基準 3 項設定項目(詳見表 5)。

表1　Palo Alto Firewall 11 組態基準項目統計

項次	項目	類別	項數	合計
1	基本項目	設備設定	5	43
		密碼政策	10	
		鑑別設定	3	
		設備服務設定	2	
		安全性設定檔	3	
		安全性政策	2	

項次	項目	類別	項數	合計
2	WildFire 組態基準	WildFire 設定	4	
3	威脅防禦組態基準	威脅防禦設定	11	
4	URL 過濾組態基準	URL 過濾設定	3	

資料來源：資安院整理

1.3 文件發行

本文件最新版本公布於國家資通安全研究院網站之「政府組態基準」專區，網址為 https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/。

2. Palo Alto Firewall 11 政府組態基準列表

表2　Palo Alto Firewall 11 政府組態基準列表(基本項目)

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
1	TWGCB-03-005-0001	設備設定	於高 DP 載入時啟用日誌	▪ 這項原則設定決定是否於高 DP 載入時啟用日誌 ▪ 當設備之封包處理使用率達到 100%時，可能影響服務可用性，記錄此事件將有助於排查系統效能問題 ▪ 啟用此功能後，當封包處理使用率達到 100%時，系統將建立日誌以記錄該事件	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「DEVICE」 (2) 左邊列表點選「Setup(設定)」 (3) 中間視窗點選「Management(管理)」 (4) 向下捲動至「Logging and Reporting Settings(登入與報告設定)」並點選右側齒輪符號 (5) 點選「Log Export and Reporting(日誌匯出與報	啟用

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
					告)」並勾選「Enable Log on High DP Load(於高 DP 載入時啟用日誌)」 (6)點選「OK(成功)」以儲存設定	
2	TWGCB-03-005-0002	設備設定	管理介面設定許可的 IP 位址	▪這項原則設定決定是否將管理介面設定為僅允許特定 IP 位址或子網段進行存取 ▪僅允許必要之 IP 位址可進行設備管理 ▪設備的管理存取應限於防火牆管理員所使用之 IP 位址或子網段。若開放來自其他 IP 位址進行管理存取，會增加透過密碼	登入網頁圖形介面後，執行以下操作： (1)上方列表點選「DEVICE」 (2)左邊列表點選「Setup(設定)」 (3)中間視窗點選「Interfaces(介面)」並點選「Management(管理)」 (4)視窗右側點選「Add(新增)」，將允許的 IP 位址設定為僅限於管理設備所	僅允許設備管理員使用的 IP 位址或子網段進行 SSH 與 HTTPS 存取

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				猜測、竊取帳密或其他方式進行未經授權存取之風險	需的 SSH 與 HTTPS 協定。如果設定檔未存在，請自行建立，並確認已包含這些許可的 IP 位址 (5) 點選「OK(成功)」以儲存設定	
3	TWGCB-03-005-0003	設備設定	介面管理設定檔許可的 IP 位址	▪ 這項原則設定決定是否在所有管理介面設定檔中，僅允許管理設備所需之 IP 位址進行 SSH、HTTPS 及 SNMP 存取 ▪ 若允許之 IP 位址未指定或範圍過大，攻擊者可能從非預期之位置(如網際網路)嘗試存取管理介面	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「NETWORK」 (2) 左邊列表點選「Network Profiles(網路設定檔)」，並點選「Interface Mgmt(介面管理)」 (3) 檢視現有的介面管理設定檔，若存在，則點選其名稱，無則點選視窗下方之	僅允許設備管理員使用的 IP 位址或子網段進行 SSH、HTTPS 及 SNMP 存取

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				▪確保在安全政策規則集底部存在一條「拒絕任何/所有流量」的安全政策，可透過要求明確許可用來進行設備管理存取之安全政策，提供額外保護	「Add(新增)」以新增一個設定檔 (4)在每個設定檔中，指定允許進行 SSH、HTTPS 及 SNMP 存取的 IP 位址 (5)點選「OK(成功)」以儲存設定	
4	TWGCB-03-005-0004	設備設定	管理介面設定的 HTTP 與 Telnet 選項	▪這項原則設定決定是否啟用管理介面設定之 HTTP 與 Telnet 選項 ▪若使用 HTTP 或 Telnet 等明文傳輸協定進行管理存取，攻擊者可利用中間人攻擊伺機取得管理員帳	登入網頁圖形介面後，執行以下操作： (1)上方列表點選「DEVICE」 (2)左邊列表點選「Setup(設定)」 (3)中間視窗點選「Interfaces(介面)」並點選「Management」	停用

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				密與其他設備管理相關敏感資訊	(4)取消勾選「HTTP」與「Telnet」 (5)點選「OK(成功)」以儲存設定	
5	TWGCB-03-005-0005	設備設定	介面管理設定檔的 HTTP 與 Telnet 選項	▪這項原則設定決定是否啟用介面管理設定檔的 HTTP 與 Telnet 選項 ▪若使用 HTTP 或 Telnet 等明文傳輸協定進行管理存取，攻擊者可利用中間人攻擊伺機取得管理員帳密與其他設備管理相關敏感資訊	登入網頁圖形介面後，執行以下操作： (1)上方列表點選「NETWORK」 (2)左邊列表點選「Network Profiles(網路設定檔)」，並點選「Interface Mgmt(介面管理)」 (3)點選視窗中每一個設定檔，並取消勾選「HTTP」與「Telnet」 (4)點選「OK(成功)」以儲存設定	停用

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
6	TWGCB-03-005-0006	密碼政策	最小密碼複雜性	▪ 這項原則設定決定是否啟用最小密碼複雜性功能 ▪ 密碼複雜性建議源自美國政府組態基準(USGCB)、常見弱點列舉(Common Weakness Enumeration)及 CIS 發布之基準 ▪ 無論是針對管理介面的直接攻擊，或是針對所捕獲之密碼雜湊值進行攻擊，複雜之密碼相對較難破解	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「DEVICE」 (2) 左邊列表點選「Setup(設定)」 (3) 中間視窗點選「Management(管理)」 (4) 向下捲動至「Minimum Password Complexity(最小密碼複雜性)」並點選右側齒輪符號 (5) 勾選「Enabled(已啟用)」 (6) 點選「OK(成功)」以儲存設定	啟用

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				▪ 應啟用最小密碼複雜性，以進一步設定密碼原則相關項目		
7	TWGCB-03-005-0007	密碼政策	密碼最小長度	▪ 這項原則設定決定密碼須包含之最小長度 ▪ 建議採用較長之密碼，這樣無論是針對管理介面的直接攻擊，或針對捕獲之密碼雜湊值進行攻擊，都更難破解	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「DEVICE」 (2) 左邊列表點選「Setup(設定)」 (3) 中間視窗點選「Management(管理)」 (4) 向下捲動至「Minimum Password Complexity(最小密碼複雜性)」並點選右側齒輪符號 (5) 將「Minimum Length(最小長度)」設定為 12 以上	12 以上

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
					(6)點選「OK(成功)」以儲存設定	
8	TWGCB-03-005-0008	密碼政策	密碼最小大寫字母數量	▪這項原則設定決定密碼至少須包含之大寫字母個數 ▪此設定會檢查所有新密碼，以確保其至少包含一個英文大寫字母(A 到 Z) ▪此為多項設定之一，綜合這些設定可確保密碼具有足夠複雜性，以抵禦暴力破解與字典攻擊	登入網頁圖形介面後，執行以下操作： (1)上方列表點選「DEVICE」 (2)左邊列表點選「Setup(設定)」 (3)中間視窗點選「Management(管理)」 (4)向下捲動至「Minimum Password Complexity(最小密碼複雜性)」並點選右側齒輪符號 (5)將「Minimum Uppercase Letters(最小大寫字母數量)」設定為 1 以上	1 以上

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
					(6)點選「OK(成功)」以儲存設定	
9	TWGCB-03-005-0009	密碼政策	密碼最小小寫字母數量	▪這項原則設定決定密碼至少須包含之小寫字母個數 ▪此設定會檢查所有新密碼，以確保其至少包含一個英文小寫字母(a 到 z) ▪此為多項設定之一，綜合這些設定可確保密碼具有足夠複雜性，以抵禦暴力破解與字典攻擊	登入網頁圖形介面後，執行以下操作： (1)上方列表點選「DEVICE」 (2)左邊列表點選「Setup(設定)」 (3)中間視窗點選「Management(管理)」 (4)向下捲動至「Minimum Password Complexity(最小密碼複雜性)」並點選右側齒輪符號 (5)將「Minimum Lowercase Letters(最小小寫字母數量)」設定為 1 以上	1 以上

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
					(6)點選「OK(成功)」以儲存設定	
10	TWGCB-03-005-0010	密碼政策	密碼最小數字數量	▪這項原則設定決定密碼至少須包含之數字個數 ▪此設定會檢查所有新密碼，以確保其至少包含一個十進位數字(0 到 9) ▪此為多項設定之一，綜合這些設定可確保密碼具有足夠複雜性，以抵禦暴力破解與字典攻擊	登入網頁圖形介面後，執行以下操作： (1)上方列表點選「DEVICE」 (2)左邊列表點選「Setup(設定)」 (3)中間視窗點選「Management(管理)」 (4)向下捲動至「Minimum Password Complexity(最小密碼複雜性)」並點選右側齒輪符號 (5)將「Minimum Numeric Letters(最小數字數量)」設定為 1 以上	1 以上

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
					(6)點選「OK(成功)」以儲存設定	
11	TWGCB-03-005-0011	密碼政策	密碼最小特殊字元數量	▪這項原則設定決定密碼至少須包含之特殊字元個數 ▪此設定會檢查所有新密碼，以確保其至少包含特殊字元(例如!、$、#、%等) ▪此為多項設定之一，綜合這些設定可確保密碼具有足夠複雜性，以抵禦暴力破解與字典攻擊	登入網頁圖形介面後，執行以下操作： (1)上方列表點選「DEVICE」 (2)左邊列表點選「Setup(設定)」 (3)中間視窗點選「Management(管理)」 (4)向下捲動至「Minimum Password Complexity(最小密碼複雜性)」並點選右側齒輪符號 (5)將「Minimum Special Characters(最小特殊字元數量)」設定為 1 以上	1 以上

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
					(6)點選「OK(成功)」以儲存設定	
12	TWGCB-03-005-0012	密碼政策	密碼變更期限	▪這項原則設定決定系統要求變更密碼前，密碼可使用之期限(日數) ▪密碼存在的時間越長，遭遇暴力破解攻擊、攻擊者獲取使用者資訊進行密碼猜測，或是用戶自行分享密碼之風險就越高	登入網頁圖形介面後，執行以下操作： (1)上方列表點選「DEVICE」 (2)左邊列表點選「Setup(設定)」 (3)中間視窗點選「Management(管理)」 (4)向下捲動至「Minimum Password Complexity(最小密碼複雜性)」並點選右側齒輪符號 (5)將「Required Password Change Period (days)(已要求密碼變更期限(日數))」	90 以下，但須大於 0

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
					設定為 90 以下，但須大於 0 (6) 點選「OK(成功)」以儲存設定	
13	TWGCB-03-005-0013	密碼政策	新密碼在字元數上有差異	▪ 這項原則設定決定新密碼與舊密碼須具有多少差異字元 ▪ 此設定可防止使用符合可預測模式之密碼，避免密碼變更遵循固定模式 ▪ 此為多項設定之一，綜合這些設定可確保密碼具有足夠複雜性，以抵禦暴力破解與字典攻擊	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「DEVICE」 (2) 左邊列表點選「Setup(設定)」 (3) 中間視窗點選「Management(管理)」 (4) 向下捲動至「Minimum Password Complexity(最小密碼複雜性)」並點選右側齒輪符號	3 以上

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
					(5) 將「New Password Differs By Characters(新密碼在字元數上有差異)」設定為 3 以上 (6) 點選「OK(成功)」以儲存設定	
14	TWGCB-03-005-0014	密碼政策	密碼重複使用限制	▪ 這項原則設定決定新密碼不得與最近幾次使用之舊密碼重複 ▪ 使用相同密碼之時間越長，攻擊者暴力破解攻擊成功之機會就越大。此外，任何可能已被入侵之帳戶，只要密碼未被更改，就可能持續被利用。若要求變更密碼但未阻止密碼重複使用，	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「DEVICE」 (2) 左邊列表點選「Setup(設定)」 (3) 中間視窗點選「Management(管理)」 (4) 向下捲動至「Minimum Password Complexity(最小	3 以上

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				或用戶持續重複使用少數特定密碼，將大幅降低密碼安全政策之有效性	密碼複雜性)」並點選右側齒輪符號 (5) 將「Prevent Password Reuse Limit(防止密碼重複使用限制)」設定為 3 以上 (6) 點選「OK(成功)」以儲存設定	
15	TWGCB-03-005-0015	密碼政策	密碼設定檔	▪ 這項原則設定決定是否刪除密碼設定檔 ▪ 由於密碼設定檔會覆蓋設備中定義之任何「最小密碼複雜性」設定，故建議不使用密碼設定檔。如需使用，建議強制執行比「最小密碼複雜性」	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「DEVICE」 (2) 左邊列表點選「Password Profiles(碼設定檔)」 (3) 刪除所有存在的密碼設定檔	刪除

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				設定中更嚴格之密碼政策		
16	TWGCB-03-005-0016	鑑別設定	閒置逾時	▪ 這項原則設定決定連線閒置多長時間後自動登出 ▪ 將設備管理之閒置逾期時間設定為 15 分鐘或更短，以在連線閒置後自動關閉	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「DEVICE」 (2) 左邊列表點選「Setup(設定)」 (3) 中間視窗點選「Management(管理)」 (4) 向下捲動至「Authentication Settings(驗證設定)」並點選右側齒輪符號 (5) 將「Idle Timeout(閒置逾時(分鐘))」設定為 15 以下，但須大於 0	15 以下，但須大於 0

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
					(6)點選「OK(成功)」以儲存設定	
17	TWGCB-03-005-0017	鑑別設定	失敗的嘗試	▪這項原則設定決定帳號被鎖定之嘗試登入失敗次數 ▪請勿在身分鑑別設定區進行失敗嘗試次數之設定；所選身分鑑別設定檔案中之任何失敗嘗試，在身分鑑別設定區中並不適用	登入網頁圖形介面後，執行以下操作： (1)上方列表點選「DEVICE」 (2)左邊列表點選「Setup(設定)」 (3)中間視窗點選「Management(管理)」 (4)向下捲動至「Authentication Settings(驗證設定)」並點選右側齒輪符號 (5)將「Failed Attempts(失敗的嘗試)」設定為 5 以下	5 以下，但須大於 0

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
					(6)點選「OK(成功)」以儲存設定	
18	TWGCB-03-005-0018	鑑別設定	鎖定時間	▪這項原則設定決定帳號被鎖定後，需隔多久時間才能解鎖 ▪請勿在身分鑑別設定區進行鎖定時間之設定；所選身分鑑別設定檔案中之任何鎖定時間，在身分鑑別設定區中並不適用	登入網頁圖形介面後，執行以下操作： (1)上方列表點選「DEVICE」 (2)左邊列表點選「Setup(設定)」 (3)中間視窗點選「Management(管理)」 (4)向下捲動至「Authentication Settings(驗證設定)」並點選右側齒輪符號 (5)將「Lockout Time(鎖定時間(分鐘))」設定為 15 以上	15 以上

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
					(6)點選「OK(成功)」以儲存設定	
19	TWGCB-03-005-0019	設備服務設定	驗證更新伺服器身分識別	▪這項原則設定決定是否啟用驗證更新伺服器身分識別 ▪在下載套件之前驗證更新伺服器的身分，以確保套件來源可受信任，避免接收與安裝來自惡意來源之更新	登入網頁圖形介面後，執行以下操作： (1)上方列表點選「DEVICE」 (2)左邊列表點選「Setup(設定)」 (3)中間視窗點選「Services(服務)」並點選下方「Services(服務)」右側齒輪符號 (4)勾選「Verify Update Server Identity(驗證更新伺服器身分識別)」 (5)點選「OK(成功)」以儲存設定	啟用

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
20	TWGCB-03-005-0020	設備服務設定	設定主要與次要 NTP 伺服器	▪ 這項原則設定決定是否設定主要與次要 NTP 伺服器，以便在主要 NTP 伺服器發生故障時提供備援功能 ▪ NTP 校時服務使設備可保持準確之時間與日期，這對於與其他系統進行事件關聯、故障排除及調查工作至關重要 ▪ 若設備時間與日期不正確，排程更新等功能將可能無法正常運作	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「DEVICE」 (2) 左邊列表點選「Setup(設定)」 (3) 中間視窗點選「Services(服務)」並點選下方「Services(服務)」右側齒輪符號 (4) 填寫「Primary NTP Server Address(主要 NTP 伺服器位址)」 (5) 填寫「Secondary NTP Server Address(次要 NTP 伺服器位址)」	設定主要與次要 NTP 伺服器

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
					(6)點選「OK(成功)」以儲存設定	
21	TWGCB-03-005-0021	安全性設定檔	對所有未受信任地區的地區保護設定檔啟用流量保護	▪這項原則設定決定是否對所有未受信任地區之地區保護設定檔啟用流量保護 ▪對所有不受信任地區啟用 SYN Flood 流量保護，以抵禦 DoS/DDoS 攻擊 ▪SYN Flood 防護的告警、啟動及最大值設定須依據所使用的環境與設備硬體效能進行調整 ▪對大多數環境來說，將啟動值設為防火牆	登入網頁圖形介面後，執行以下操作： (1)上方列表點選「NETWORK」 (2)左邊列表點選「Network Profiles(網路設定檔)」，並點選「Zone Protection(地區保護)」 (3)檢視是否有地區保護設定檔，若有則點選其名稱，無則點選視窗下方之「Add(新增)」以新增一個設定檔 (4)點選「Flood Protection(流量保護)」，並勾選	啟用「SYN」、「UDP」、「ICMP」、「ICMPv6」及「Other IP」 「SYN」的「Action(動作)」設為「SYN Cookie」

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
				最大「每秒新建會話」/CPS 的 50%，是一個保守的設定值 ▪ 單靠防火牆無法抵禦所有 DoS/DDoS 攻擊，但許多攻擊可以有效緩解。SYN Cookies 有助於緩解 SYN Flood 攻擊，該攻擊會使受害設備之 CPU 或記憶體緩衝區因過多未完成三向交握之 TCP 連線而超載。相比於隨機提前丟棄，SYN Cookies 是更佳選擇	「SYN」、「UDP」、「ICMP」、「ICMPv6」及「Other IP」 (5)「SYN」的「Action(動作)」設為「SYN Cookie」，其餘數值則依機關硬體效能自行評估 (6)點選「OK(成功)」以儲存設定 (7)左邊列表點選「Zone(地區)」 (8)檢視是否有不受信任的網路地區，若有則點選其名稱 (9)將「Zone Protection(地區保護)」中的「Zone Protection Profile(地區保護	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
					設定檔)」設為已設定完成的地區保護設定檔 (10)點選「OK(成功)」以儲存設定	
22	TWGCB-03-005-0022	安全性設定檔	所有地區啟用偵查保護	▪這項原則設定決定是否對所有地區啟用偵查保護 ▪連接埠掃描與主機掃描是常見攻擊偵查手段 ▪網路爬蟲會掃描開啟連接埠與可用主機以尋找易受攻擊目標 ▪啟用偵查保護以完全阻止連接埠掃描與主機掃描，或在此類攻擊發生時發出告警	登入網頁圖形介面後，執行以下操作： (1)上方列表點選「NETWORK」 (2)左邊列表點選「Network Profiles(網路設定檔)」，並點選「Zone Protection(地區保護)」 (3)檢視是否有地區保護設定檔，若有則點選其名稱，無則點選視窗下方之「Add(新增)」以新增一個設定檔	啟用「TCP Port Scan(TCP 連接埠掃描)」，「Action(動作)」設為「Block IP(封鎖 IP)」、「Track By(追蹤者)」設為「source」、「Duration (sec)(持續時間(秒))」設為「600」、「Interval (sec)(間隔(秒))」設為「5」、「Threshold

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
					(4)點選「Reconnaissance Protection(偵查保護)」 (5)勾選「TCP Port Scan(TCP 連接埠掃描)」的「Enable(啟用)」，並將「TCP Port Scan(TCP 連接埠掃描)」的「Action(動作)」設為「Block IP(封鎖 IP)」、「Track By(追蹤者)」設為「source」、「Duration (sec)(持續時間(秒))」設為「600」 (6)將「TCP Port Scan(TCP 連接埠掃描)」的「Interval (sec)(間隔(秒))」設為「5」、「Threshold (events)(閾值(事件))」設為「20」	(events)(閾值(事件))」設為「20」 啟用「Host Sweep(主機掃描)」，「Action(動作)」設為「Block IP(封鎖 IP)」、「Track By(追蹤者)」設為「source」、「Duration (sec)(持續時間(秒))」設為「600」、「Interval (sec)(間隔(秒))」設為「10」、「Threshold (events)(閾值(事件))」設為「30」

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
					(7) 勾選「Host Sweep(主機掃描)」的「Enable(啟用)」，並將「Host Sweep(主機掃描)」的「Action(動作)」設為「Block IP(封鎖 IP)」、「Track By(追蹤者)」設為「source」、「Duration (sec)(持續時間(秒))」設為「600」 (8) 將「Host Sweep(主機掃描)」的「Interval (sec)(間隔(秒))」設為「10」、「Threshold (events)(閾值(事件))」設為「30」 (9) 勾選「UDP Port Scan(UDP 連接埠掃描)」的「Enable(啟用)」，並將	啟用「UDP Port Scan(UDP 連接埠掃描)」，「Action(動作)」設為「警示」、「Interval (sec)(間隔(秒))」設為「10」、「Threshold (events)(閾值(事件))」設為「20」

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
					「UDP Port Scan(UDP 連接埠掃描)」的「Action(動作)」設為「alert(警示)」 (10)將「UDP Port Scan(UDP 連接埠掃描)」的「Interval (sec)(間隔(秒))」設為「10」、「Threshold (events)(閾值(事件))」設為「20」 (11)點選「OK(成功)」以儲存設定	
23	TWGCB-03-005-0023	安全性設定檔	所有地區啟用封包攻擊保護	▪這項原則設定決定是否在所有地區啟用封包攻擊保護 ▪攻擊者可能使用特別設計之封包來規避或削弱網路安全設備的	登入網頁圖形介面後，執行以下操作： (1)上方列表點選「NETWORK」 (2)左邊列表點選「Network Profiles(網路設定檔)」，	勾選「Spoofed IP address(詐騙的 IP 位址)」、「Fragment traffic(封鎖分散的流量)」、「Strict Source Routing(嚴格的來源路由)」、

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				有效性，此類攻擊包含偽造 IP 位址、分散流量、嚴格來源路由、寬鬆來源路由及格式錯誤之封包 ▪ 在所有地區啟用封包保護，以降低遭受此類攻擊之風險	並點選「Zone Protection(地區保護)」 (3) 檢視是否有地區保護設定檔，若有則點選其名稱，無則點選視窗下方之「Add(新增)」以新增一個設定檔 (4) 點選「Packet Based Attack Protection(封包攻擊保護)」，並勾選「Spoofed IP address(詐騙的 IP 位址)」與「Fragment traffic(封鎖分散的流量)」 (5) 勾選「IP Option Drop(IP 選項丟棄)」中的「Strict Source Routing(嚴格的來源路由)」、「Loose Source Routing(鬆散來源	「Loose Source Routing(鬆散來源路由)」及「Malformed(格式錯誤的)」

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
					路由)」及「Malformed(格式錯誤的)」 (6)點選「OK(成功)」以儲存設定 (7)左邊列表點選「Zone(地區)」 (8)點選所有網路地區的名稱 (9)將「Zone Protection(地區保護)」中的「Zone Protection Profile(地區保護設定檔)」設為已設定完成的地區保護設定檔 (10)點選「OK(成功)」以儲存設定	
24	TWGCB-03-005-0024	安全性政策	對外主機的服務欄位不得設	▪這項原則設定決定如何設定對外主機之服務欄位	▪登入網頁圖形介面後，執行以下操作：	▪對於每一個與外部網路相連的主機，需確保有以下設定

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
			為「any」	▪ Palo Alto Firewall 所使用之 App-ID 流量分類機制，需要一定數量之封包穿過防火牆後才能識別出該組封包所代表的應用程式，並判斷是否允許或拒絕該流量 ▪ 由於 App-ID 流量分類機制之特性，即使在安全性政策規則中已定義限制之應用程式，若將服務設定為「any」，仍可能使部分流量在 App-ID 識別並阻擋前接觸到目標主機	(1) 上方列表點選「POLICIES」 (2) 左邊列表點選「Security(安全性規則)」 ▪ 對於每一個與外部網路相連的主機，需確保有以下設定之安全性政策規則： (1)「Source(來源)」的「Zone(來源地區)」設為外部 IP 並設為「any(任何)」 (2)「Destination(目的地)」的「Zone(目的地地區)」設為 DMZ IP 並設為「< DMZ Host Object >」 (3)「Application(應用程式)」的「Application(應用程	的安全性政策規則： (1)「Source(來源)」的「Zone(來源地區)」設為外部 IP 並設為「any(任何)」 (2)「Destination(目的地)」的「Zone(目的地地區)」設為 DMZ IP 並設為「< DMZ Host Object >」 (3)「Application(應用程式)」的「Application(應

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				▪ 將服務類別設為「application-default」可限制應用程式或協定之初始流量	式)」設為「web-browsing」，或是其他系統允許的應用程式 (4)「Service/URL Category (服務/URL 類別」的「Service(服務)」設為「application-default」，不可設為「any」	用程式)」設為「web-browsing」，或是其他系統允許的應用程式 (4)「Service/URL Category (服務/URL 類別」的「Service(服務)」，不可設為「any」
25	TWGCB-03-005-0025	安全性政策	預設安全性政策規則啟用「同時連線結束時的日誌」	▪ 這項原則設定決定是否在預設安全性政策規則中啟用「同時連線結束時的日誌」功能	▪ 登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「POLICIES」 (2) 左邊列表點選「Security(安全性規則)」	啟用「Log at Session End(同時連線結束時的日誌)」

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				▪ 預設情況下，預設安全性政策規則未啟用日誌記錄 ▪ 啟用日誌記錄有助於資通安全威脅偵測管理中心(SOC)或安全分析人員進行深入之安全事件調查	▪ 對於兩個預設的安全性政策規則「intrazone-default」，分別執行以下動作： (1) 點選「intrazone-default」後，點選下方「Override(取代)」 (2) 點選「Action(動作)」，並勾選「Log Setting(日誌設定)」中的「Log at Session End(同時連線結束時的日誌)」 (3) 設定完成後，點選「OK(成功)」以儲存設定	

資料來源：資安院整理

表3　Palo Alto Firewall 11 WildFire 政府組態基準列表

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
1	TWGCB-03-005-0026	WildFire 設定	確保所有安全性政策啟用 WildFire 分析設定檔	▪ 這項原則設定決定是否在所有安全性政策啟用 WildFire 分析設定檔 ▪ 在所有安全性政策中啟用 WildFire 檔案阻擋設定檔，以確保所有經過防火牆的檔案皆會接受 WildFire 檢查 ▪ 若安全性政策未包含 WildFire 檔案阻擋設定檔，則符合該政策之流量將無法進行 WildFire 檔案分析 ▪ WildFire 分析是此平台上的關鍵安全措施之一。若未啟用 WildFire	確認與建立 WildFire 分析設定檔之步驟如下： (1) 登入網頁圖形介面後，上方列表點選「OBJECTS」 (2) 左邊列表點選「Security Profiles(安全性設定檔)」中的「WildFire Analysis (WildFire 分析)」 (3) 檢視是否已有安全性設定檔，若無則點選視窗下方「Add(新增)」以建立一個新的安全性設定檔 (4) 設定完成後，點選「OK(成功)」以儲存 WildFire 分析設定檔	啟用

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				分析，將只能透過特徵碼分析進入的惡意軟體，而此種方法在實務上之有效性大約僅有40%到 60%。在面對有針對性之攻擊時，單純依靠特徵碼之分析成功率會更低	▪ 設定安全性政策規則的步驟如下： (1) 登入網頁圖形介面後，上方列表點選「POLICIES」 (2) 左邊列表點選「Security(安全性規則)」 (3) 針對每個動作為「Allow(允許)」的規則，點選其名稱 (4) 點選「Action(動作)」，將「Profiles Type(設定檔類型) 」設為「Profiles(設定檔)」，並將「WildFire Analysis (WildFire 分析)」設為剛設定好的 WildFire 分析設定檔	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
					(5) 或是將設定檔類型設為「Group(群組)」，並選用已包含 WildFire 分析設定檔的群組 (6) 點選「OK(成功)」以儲存設定 ▪ 若有啟用群組規則，群組規則的設定步驟如下： (1) 登入網頁圖形介面後，上方列表點選「OBJECTS」 (2) 左邊列表點選「Security Profile Groups(安全配置文件組)」 (3) 點選已設定完成的安全性設定檔群組名稱或點選「Add(新增)」後，將「WildFire Analysis	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
					(WildFire 分析)」指定為已設定完成之安全性設定檔	
2	TWGCB-03-005-0027	WildFire設定	WildFire更新排程	▪ 這項原則設定決定 WildFire 更新頻率 ▪ WildFire 定義可能包含用於阻止立即性且活躍威脅之特徵碼。透過即時更新，防火牆可確保新威脅能迅速得到緩解	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「DEVICE」 (2) 左邊列表點選「Dynamic Updates(動態更新)」 (3) 視窗下方點選「Check Now(立即檢查)」 (4) 中央列表點選「WildFire」選項右側「Schedule(排程)」 (5) 將「Recurrence(週期性)」設為「Real-time(即時)」 (6) 點選「OK(成功)」以儲存設定	Real-time(即時)

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
3	TWGCB-03-005-0028	WildFire 設定	解碼器在防毒設定檔中的協定動作	▪ 這項原則設定決定解碼器在不同協定下檢測到惡意程式時之應對動作 ▪ 建議將 imap 與 pop3 解碼器在「WildFire Action」項目下設定為「alert」 ▪ 防毒特徵碼誤報率較低，透過指定解碼器阻擋惡意程式，可顯著降低其穿過防火牆進行傳播之風險 ▪ 由於 pop3 與 imap 協定特性，防火牆無法僅阻擋包含惡意程式之單一電子郵件訊息，這可能	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「OBJECTS」 (2) 左邊列表點選「Security Profiles(安全性設定檔)」中的「Antivirus(防毒)」 (3) 檢視設定檔是否存在，若無則點選視窗下方之「Add(新增)」以新增一個設定檔 (4) 對於設定檔中協定偵測的所有動作，除了 imap 與 pop3 的動作須設為「alert」外，其他協定的動作皆設為「reset-both」	除了 imap 與 pop3 的動作須設為「alert」外，其他協定的動作皆設為「reset-both」

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				會影響其他無惡意程式之電子郵件訊息	(5) 設定完成後點選「OK(成功)」以儲存防毒設定檔	
4	TWGCB-03-005-0029	WildFire 設定	防毒設定檔中的 WildFire 內嵌機器學習功能	▪ 這項原則設定決定是否在防毒設定檔中啟用 WildFire 內嵌機器學習功能 ▪ 自 PAN-OS 10 開始，WildFire 支援即時檢測與阻擋，而隨著越來越多的攻擊被設計為繞過基於簽名之防護，即時性無簽名防護功能有其必要性 ▪ 透過這項新功能，WildFire 可檢查一些常被用來傳遞惡意程式之檔案類型，例如 Windows 執行檔、	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「OBJECTS」 (2) 左邊列表點選「Security Profiles(安全性設定檔)」中的「Antivirus(防毒)」 (3) 檢視是否有防毒設定檔，若有則點選其名稱，無則點選視窗下方之「Add(新增)」以新增一個設定檔 (4) 點選「WildFire Inline ML Action(WildFire 內嵌 ML)」，並將所有「Model(型號)」的	啟用「WildFire Inline ML Action(WildFire 內嵌 ML)」，並將所有「Action Setting(動作設定)」設為「enable (inherit per-protocol actions)」

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
				PowerShell 腳本、MS Office 文件、Shell 檔案及可執行連結格式(ELF)等，並能即時阻擋惡意檔案	「Action Setting(動作設定)」設為「enable (inherit per-protocol actions)」 (5) 設定完成後點選「OK(成功)」以儲存防毒設定檔	

資料來源：資安院整理

表4　Palo Alto Firewall 11 威脅防禦政府組態基準列表

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
1	TWGCB-03-005-0030	威脅防禦設定	防毒更新排程	▪ 這項原則設定決定防毒更新之頻率與方式 ▪ 防毒定義可能隨時發布新版本，透過每小時更新排程，防火牆可確保	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「DEVICE」 (2) 左邊列表點選「Dynamic Updates(動態更新)」	Hourly(每小時)、download-and-install

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
				新定義威脅能迅速得到緩解	(3) 視窗下方點選「Check Now(立即檢查)」 (4) 中央列表點選「Antivirus(防毒)」選項右側「Schedule(排程)」 (5) 將「Recurrence(週期性)」設為「Hourly(每小時)」，將「Action(動作)」設為「download-and-install」 (6) 點選「OK(成功)」以儲存設定	
2	TWGCB-03-005-0031	威脅防禦設定	應用程式與威脅更新排程	▪ 這項原則設定決定應用程式與威脅更新之頻率與方式 ▪ 新版本應用程式與威脅檔案可能隨時發布。透過頻繁更新排程，防火牆可確保新特徵碼威脅能迅速得到緩解，並應	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「DEVICE」 (2) 左邊列表點選「Dynamic Updates(動態更新)」 (3) 視窗下方點選「Check Now(立即檢查)」	Daily(每日)、download-and-install

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
				用最新之應用程式特徵碼	(4) 中央列表點選「Application and Threats(應用程式與威脅)」選項右側「Schedule(排程)」 (5) 將「Recurrence(週期性)」設為「Daily(每日)」，將「Action(動作)」設為「download-and-install」 (6) 點選「OK(成功)」以儲存設定	
3	TWGCB-03-005-0032	威脅防禦設定	解碼器防毒設定檔之協定動作	▪ 這項原則設定決定解碼器在不同協定下檢測到惡意程式時之應對動作 ▪ 建議將 imap 與 pop3 解碼器在「Action」項目下設定為「alert」 ▪ 防毒特徵碼誤報率較低，透過指定解碼器阻擋惡意程式，可顯著降	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「OBJECTS」 (2) 左邊列表點選「Security Profiles(安全性設定檔)」中的「Antivirus(防毒)」 (3) 檢視設定檔是否存在，若無則點選視窗下方之「Add(新增)」以新增一個設定檔	除了 imap 與 pop3 的動作須設為「alert」外，其他協定的動作皆設為「reset-both」

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
				低其穿過防火牆進行傳播之風險 ▪ 由於 pop3 與 imap 協定特性，防火牆無法僅阻擋包含惡意程式之單一電子郵件訊息，這可能會影響其他無惡意程式之電子郵件訊息	(4) 對於設定檔中協定偵測的所有動作，除了 imap 與 pop3 的動作須設為「alert」外，其他協定的動作皆設為「reset-both」 (5) 設定完成後點選「OK(成功)」以儲存防毒設定檔	
4	TWGCB-03-005-0033	威脅防禦設定	所有相關的安全性政策皆套用安全的防毒設定檔	▪ 這項原則設定決定是否將所有相關安全性政策皆套用安全之防毒設定檔 ▪ 對所有允許流量之安全規則套用安全的漏洞防護設定檔，能確保所有經過防火牆之網路流量都會被檢查是否存在攻擊行為，這既能保護資	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「POLICIES」 (2) 左邊列表點選「Security(安全性規則)」 (3) 針對每個動作為「Allow(允許)」的規則，點選其名稱 (4) 點選「Action(動作)」，將設定檔類型設為「Profiles(設定檔)」，	啟用

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
				產免受攻擊，也能避免聲譽遭受損害 ▪請注意，加密連線無法進行完整檢測	並將「Antivirus(防毒)」設為已設定完成的防毒設定檔 (5) 或是將設定檔類型設為「Group(群組)」，並選用已包含防毒設定檔的群組 (6) 點選「OK(成功)」以儲存設定	
5	TWGCB-03-005-0034	威脅防禦設定	反間諜軟體設定檔的特徵碼原則	▪這項原則設定決定是否新增反間諜軟體設定檔中之特徵碼原則 ▪若反間諜軟體設定檔中存在單一規則，則將其配置為阻擋任何間諜軟體的嚴重程度、任何類別及任何威脅 ▪若反間諜軟體設定檔中存在多個規則，則確保所有間諜軟體類別、威	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「OBJECTS」 (2) 左邊列表點選「Security Profiles(安全性設定檔)」中的「Anti-Spyware(反間諜軟體)」 (3) 檢視是否有反間諜軟體設定檔，若有則點選其名稱，無則點選視窗下方之「Add(新增)」以新增一個設定檔	將「威脅名稱」、「類別」及嚴重性皆設為「any」，動作設為「reset-both」

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
				脅及嚴重程度均設定為阻擋 ▪對所有間諜軟體威脅、類別及嚴重程度採取阻擋政策，以降低間諜軟體之危害	(4)點選「Signature Policies(特徵碼原則)」，並點選視窗下方的「Add(新增)」以建立一項新的反間諜軟體特徵碼原則 (5)將「Threat Name(威脅名稱)」、「Category(類別)」及「Severity(嚴重性)」皆設為「any」，動作設為「Reset Both」 (6)設定完成後點選「OK(成功)」以儲存特徵碼原則，再點選「OK(成功)」以儲存反間諜軟體設定檔	
6	TWGCB-03-005-0035	威脅防禦設定	反間諜軟體設定檔的 DNS Sinkhole	▪這項原則設定決定是否啟用反間諜軟體設定檔中之 DNS Sinkhole 功能	▪登入網頁圖形介面後，執行以下操作： (1)上方列表點選「OBJECTS」	啟用

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
			功能	▪ 應為所有使用中之反間諜軟體設定檔設定 DNS Sinkholing。所有內部對指定之 Sinkhole IP 位址的請求必須經過防火牆。任何嘗試與 DNS Sinkhole IP 位址進行通訊的裝置應視為已受感染 ▪ DNS Sinkholing 透過偽造 DNS 回應針對惡意軟體之域名查詢，能有效協助識別受感染之客戶端。若未設定 Sinkholing，DNS 伺服器本身可能會被誤判為已受感染，將導致真正受感染之裝置無法被及	(2) 左邊列表點選「Security Profiles(安全性設定檔)」中的「Anti-Spyware(反間諜軟體)」 (3) 對於每一個反間諜軟體設定檔，點選其名稱並點選「DNS Policies(DNS 原則)」，並將所有的「Policy Action(原則動作)」設為「sinkhole」 (4) 確認「DNS Sinkhole Setting」中的「Sinkhole IPv4」與「Sinkhole IPv6」是否正確。「Sinkhole IPv4」應為「sinkhole.paloaltonetworks.com」或是內部主機，「Sinkhole IPv6」應為「IPv6 Loopback IP (::1)」或是內部 DNS Sinkhole 主機	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
				時識別。此外，Sinkholing 亦可確保可能是入侵指標之 DNS 查詢不會經由網際網路傳輸，避免這些查詢對機關網路之「IP 信譽」產生負面影響	(6) 設定完成後點選「OK(成功)」以儲存 DNS Sinkhole 設定，再點選「OK(成功)」以儲存反間諜軟體設定檔	
7	TWGCB-03-005-0036	威脅防禦設定	所有允許流量至網際網路的安全性政策皆套用安全的反間諜軟體設定檔	▪ 這項原則設定決定是否將所有允許流量至網際網路的安全性政策皆套用安全之反間諜軟體設定檔 ▪ 應建立一個或多個反間諜軟體設定檔，並將其應用於所有允許流量至網際網路之安全性政策 ▪ 將安全之反間諜軟體設定檔應用於所有相關流	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「POLICIES」 (2) 左邊列表點選「Security(安全性規則)」針對每個輸出規則，點選其名稱 (3) 點選「Action(動作)」，將設定檔類型設為「Profiles(設定檔)」，並將「Anti-Spyware(反間諜軟	啟用

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				量，能大幅減少敏感資料外洩或讓 C2 流量通過防火牆之風險 ▪ 反間諜軟體設定檔不受限於特定協定，因此所有允許流量至網際網路的安全性政策皆應套用反間諜軟體設定檔	體)」設為已設定完成的反間諜軟體設定檔 (4) 或是將設定檔類型設為「Group(群組)」，並選用已包含反間諜軟體設定檔的群組 (5) 點選「OK(成功)」以儲存設定	
8	TWGCB-03-005-0037	威脅防禦設定	漏洞保護設定檔的阻擋規則	▪ 這項原則設定決定是否新增漏洞保護設定檔規則 ▪ 漏洞保護設定檔有助於透過警示或阻擋網路攻擊來保護資產 ▪ 針對許多重大與高風險漏洞之攻擊行為，預設	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「OBJECTS」 (2) 左邊列表點選「Security Profiles(安全性設定檔)」中的「Vulnerability Protection(漏洞保護)」 (3) 檢視是否有漏洞保護設定檔，若有則點選其名稱，無則點選視窗	啟用，將「Action(動作)」設為「Drop(丟棄)」，「Severity(嚴重性)」設為「critical」與「high」

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
				處理方式僅是發出告警，而非進行阻擋	下方之「Add(新增)」以新增一個設定檔 (4) 點選「Rules(規則)」，並點選視窗下方的「Add(新增)」以建立一項新的漏洞保護規則 (5) 將「Action(動作)」設為「Drop(丟棄)」 (6) 勾選「Severity(嚴重性)」中的「critical」與「high」 (7) 設定完成後點選「OK(成功)」以儲存漏洞保護規則，再點選「OK(成功)」以儲存漏洞保護設定檔	
9	TWGCB-03-005-0038	威脅防禦設定	所有允許流量的安全性規則皆套用安	▪ 這項原則設定決定是否在動作為「允許」之安全性政策規則中啟用漏洞保護設定檔	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「POLICIES」	啟用

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
			全的漏洞保護設定檔	▪漏洞保護設定檔有助於透過告警或阻擋網路攻擊來保護資產 ▪建議將所有允許流量之安全性規則皆套用安全漏洞保護設定檔，如此一來，所有經過防火牆的網路流量將會進行攻擊檢測，這既能保護資產免受攻擊，也能避免聲譽遭受損害 ▪請注意，加密連線無法進行完整檢測	(2) 左邊列表點選「Security(安全性規則)」 (3) 針對每個動作為「允許」的規則，點選其名稱 (4) 點選「Action(動作)」，將設定檔類型設為「Profiles(設定檔)」，並將「Vulnerability Protection(漏洞保護)」設為已設定完成的設定檔 (5) 或是將設定檔類型設為「Group(群組)」，並選用已包含漏洞保護設定檔的群組 (6) 點選「OK(成功)」以儲存設定	
10	TWGCB-03-005-0039	威脅防禦設定	漏洞保護設定檔的內嵌雲端分析功能	▪這項原則設定決定是否在漏洞保護設定檔中啟用內嵌雲端分析功能	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「OBJECTS」	啟用內嵌雲端分析，並將所有「Action(動

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				▪內嵌雲端分析可即時分析流量中之命令注入與 SQL 注入漏洞 ▪在取得 Advanced Threat Prevention 授權之情況下，應啟用內嵌雲端分析以進一步提升系統安全性 ▪請注意，防火牆裝置憑證將用於對進階威脅防護的內嵌雲端分析服務進行身分鑑別，此為使用內嵌雲端分析功能所必須之步驟	(2)左邊列表點選「Security Profiles(安全性設定檔)」中的「Vulnerability Protection(漏洞保護)」 (3)檢視是否有漏洞保護設定檔，若有則點選其名稱，無則點選視窗下方之「Add(新增)」以新增一個設定檔 (4)點選「Inline Cloud Analysis(內嵌雲端分析)」，並勾選「Enable inline cloud analysis(啟用雲端內嵌分析)」 (5)將所有「Model(型號)」的「Action(動作)」設為「alert」 (6)設定完成後點選「OK(成功)」以儲存漏洞保護設定檔	作)」設為「alert」

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
11	TWGCB-03-005-0040	威脅防禦設定	反間諜軟體設定檔的內嵌雲端分析功能	▪ 這項原則設定決定是否在反間諜軟體設定檔中啟用內嵌雲端分析 ▪ 啟用反間諜軟體之內嵌雲端分析可即時檢測並分析流量中的 C2 通訊與間諜軟體威脅，從而有效提升系統防禦能力 ▪ 在取得 Advanced Threat Prevention 授權之情況下，應啟用內嵌雲端分析以進一步提升系統安全性 ▪ 請注意，防火牆裝置憑證將用於對進階威脅防護之內嵌雲端分析服務進行身分鑑別，此為使	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「OBJECTS」 (2) 左邊列表點選「Security Profiles(安全性設定檔)」中的「Anti-Spyware(反間諜軟體)」 (3) 檢視是否有反間諜軟體設定檔，若有則點選其名稱，無則點選視窗下方之「Add(新增)」以新增一個設定檔 (4) 點選「Inline Cloud Analysis(內嵌雲端分析)」，並勾選「Enable inline cloud analysis(啟用雲端內嵌分析)」 (5) 將所有「Model(型號)」的「Action(動作)」設為「reset-both」	啟用內嵌雲端分析，並將所有「Action(動作)」設為「reset-both」

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
				用內嵌雲端分析功能所必須之步驟	(6)設定完成後點選「OK(成功)」以儲存漏洞保護設定檔	

資料來源：資安院整理

表5　Palo Alto Firewall 11 URL 過濾政府組態基準列表

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
1	TWGCB-03-005-0041	URL 過濾設定	URL 過濾設定檔啟用 HTTP 標頭記錄	▪這項原則設定決定是否啟用 URL 過濾設定檔中之 HTTP 標頭記錄 ▪記錄 HTTP 標頭可提供額外資訊予 URL 日誌，有助於進行鑑識調查 ▪「使用者代理程式」會記錄瀏覽網頁時所使用	登入網頁圖形介面後，執行以下操作： (1)上方列表點選「OBJECTS」 (2)左邊列表點選「Security Profiles(安全性設定檔)」中的「URL Filtering(URL過濾)」	「User-Agent(使用者代理程式)」、「Referer(參照位址)」與「X-

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				之瀏覽器，有助於了解被用於惡意軟體下載之攻擊向量 ▪「參照位址」會記錄引導使用者至所記錄網頁之來源網頁 ▪「X-Forwarded-For」有助於保留使用者之來源 IP 位址，例如當使用者在防火牆前經過代理伺服器時	(3)檢視是否有 URL 過濾設定檔，若有則點選其名稱，無則點選視窗下方之「Add(新增)」以新增一個設定檔 (4)點選「URL Filtering Setting(URL 篩選設定)」，並勾選「HTTP Header Logging(HTTP 標頭記錄)」的「User-Agent(使用者代理程式)」、「Referer(參照位址)」與「X-Forwarded-For」 (5)設定完成後點選「OK(成功)」以儲存 URL 過濾設定檔	Forwarded-For」

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
2	TWGCB-03-005-0042	URL 過濾設定	URL 過濾設定檔啟用內嵌分類	▪ 這項原則設定決定是否在 URL 過濾設定檔中啟用內嵌分類功能 ▪ 自 PAN-OS 10 開始，進階的 URL 過濾功能現已執行一系列基於雲端之即時深度學習檢測器，能即時評估可疑網頁內容，包含隱蔽網站、多步驟攻擊、CAPTCHA 挑戰，以及之前未見過之一次性網址 ▪ 在取得 Advanced Threat Prevention 授權的情況下，應啟用雲端內嵌分類，以進一步提升系統安全性	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「OBJECTS」 (2) 左邊列表點選「Security Profiles(安全性設定檔)」中的「URL Filtering(URL 過濾)」 (3) 檢視是否有 URL 過濾設定檔，若有則點選其名稱，無則點選視窗下方之「Add(新增)」以新增一個設定檔 (4) 點選「Inline Categorization (內嵌分類)」，並勾選「Enable local inline categorization(啟用本機內	啟用「本機內嵌分類」與「雲端內嵌分類」

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值
				▪請注意，防火牆裝置憑證將用於對進階威脅防護的內嵌雲端分析服務進行身分鑑別，此為使用內嵌雲端分析功能所必須之步驟 ▪本地內嵌分類可以在僅擁有 URL 過濾授權之情況下使用，不需要取得 Advanced Threat Prevention 授權	嵌分類)」與「Enable cloud inline categorization(啟用雲端內嵌分類)」 (5) 設定完成後點選「OK(成功)」以儲存 URL 過濾設定檔	
3	TWGCB-03-005-0043	URL 過濾設定	輸出之安全性政策規則啟用 URL 過濾設定檔	▪這項原則設定決定是否在輸出之安全性政策規則中啟用 URL 過濾設定檔 ▪URL 過濾政策可顯著降低用戶存取惡意或不適當網站之風險。此外，	登入網頁圖形介面後，執行以下操作： (1) 上方列表點選「POLICIES」	啟用

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB 設定值
				擁有所有設備之完整 URL 歷史日誌能在發生資安事件時進行取證分析	(2) 左邊列表點選「Security(安全性規則)」針對每個輸出規則，點選其名稱 (3) 點選「Action(動作)」，將設定檔類型設為「Profiles(設定檔)」，並將「URL Filtering(URL 過濾)」設為已設定完成的 URL 過濾設定檔 (4) 或是將設定檔類型設為「Group(群組)」，並選用已包含 URL 過濾設定檔的群組 (5) 點選「OK(成功)」以儲存設定	

資料來源：資安院整理

3. 參考文獻

[1]Center for Internet Security, CIS Palo Alto Firewall 11 Benchmark v1.1.0

https://www.cisecurity.org/cis-benchmarks