政府組態基準
Cisco Firewall
(V1.0)

行政院國家資通安全會報技術服務中心
中華民國108年9月

修訂歷史紀錄表

項次	版次	修訂日期	說明
1	1.0	108/9/26	新編
2			
3			
4			
5			

目　次

1. 前言 1
1.1 適用環境 1
1.2 項數統計 1
1.3 文件發行 2
2. Cisco Firewall 政府組態基準列表 3
3. 參考文獻 42

表 目 次

表 1　Cisco Firewall 組態基準項目統計 1
表 2　Cisco Firewall 政府組態基準列表 3

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 Cisco ASA 8.x 與 9.x 版本之防火牆。

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。Cisco Firewall 組態基準計有 44 項設定項目，項目統計詳見表 1。

表1　Cisco Firewall 組態基準項目統計

項次	類別	項數	合計
1	密碼管理	11	44
2	裝置管理	2	
3	AAA (Authentication, Authorization, Accounting)	3	
4	SSH 規則	5	
5	HTTP 規則	2	
6	Session 逾時	3	
7	校時規則	4	
8	日誌記錄規則	4	
9	SNMP 規則	3	
10	Control Plane	1	
11	Data Plane	6	

資料來源：本中心整理

1.3 文件發行

本文件最新版本公布於本中心網站之「政府組態基準」專區，網址為 https://www.nccst.nat.gov.tw/GCB。

2. Cisco Firewall 政府組態基準列表

表2　Cisco Firewall 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	備註
1	TWGCB-03-004-0001	密碼管理	變更預設登入密碼	▪ Telnet 或 SSH 連線需要登入密碼。預設不需要任何強式使用者驗證，建議變更預設登入密碼(cisco)，以防攻擊者輕易存取裝置 ▪ 透過 telnet 指令啟用 Telnet 服務時，可執行 passwd 指令設定登入密碼。往後需輸入登入密碼，方可進入使用者執行模式 ▪ 密碼最多可設定 80 個字元，且不可包含空白鍵 ▪ 若使用 AAA authentication telnet console 指令針對每個	hostname(config)#passwd <login_password> ▪ <login_password>為欲設定之密碼	變更預設登入密碼	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				使用者設定 Telnet 的 CLI 驗證，則不會再用到此密碼			
2	TWGCB-03-004-0002	密碼管理	設定管理者執行模式密碼	▪ 管理者執行模式(Privileged executive mode)亦稱為 enable 模式、特權模式或特權 EXEC 模式 ▪ 在進入管理者執行模式時，預設不需要任何強式使用者驗證。建議設定管理者執行模式密碼，要求使用者以 enable 指令進入管理者執行模式時需要輸入密碼，以防止攻擊者輕易進入管理者執行模式操作裝置 ▪ 密碼有區分大小寫，且可使用除了空白與問號以外的任意字元。此外，密碼以加密型態儲存於設定檔中，因此	hostname(config)#enable password <enable_password> level <privilege_level> ▪ <enable_password>為欲設定之密碼 ▪ <privilege_level>為管理者執行模式的權限等級	設定管理者執行模式密碼	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				無法於鍵入密碼後，檢視原始輸入的密碼 ▪ 權限等級(Privilege level)從level 0 到 level 15，共有 16個等級，等級越高權限越大。管理者執行模式的權限等級預設為 15 ▪ 預設密碼為空白，藉由指令可針對 0 到 15 的權限等級分別設定管理者執行模式密碼			
3	TWGCB-03-004-0003	密碼管理	主密碼	▪ 主密碼(Master key)亦稱為主金鑰，可供管理者以 1 組通用密碼將其他明文密碼以加密格式儲存。使用主密碼的功能舉例如下： (1) OSPF (2) EIGRP	▪ 步驟 1：設定主密碼(<passphrase>為欲設定之密碼)： hostname(config)# key config-key password-encryption <passphrase>	設定主密碼	此項不適用於ASA軟體8.3以前版本

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				(3) VPN (4) AAA (5) 日誌記錄 (6) 共用金鑰 ▪ ASA 軟體 8.3 以前版本，當設定檔經由 TFTP 或 FTP 傳送至設備以外的地方儲存時，密碼以明文方式呈現，若設定檔落入攻擊者手中，攻擊者即可取得檔案內之所有密碼 ▪ ASA 軟體 8.3(1)以上版本，可運用主密碼產生 AES 加密金鑰，再使用加密金鑰將運行組態(running-configuration)內之 VPN 預先共用金鑰(pre-shared key)、	▪ 步驟 2：啟用密碼加密： hostname(config)# password encryption aes ▪ 步驟 3：將啟動配置(startup-configuration)中的密碼一併加密保護： hostname(config)# write memory ▪ 若設備有使用虛擬防火牆(multi-context)功能，於步驟 3 可執行下列指令以保護所有的設定： hostname(config)# write memory all		

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				Tacacs+/Radius 共用金鑰或路由協定驗證密碼等機敏資訊以加密方式儲存，且當設定檔透過 TFTP 或 FTP 傳送至設備以外的地方儲存時，亦可加密保護 ▪ 主密碼不會出現在運行組態中，藉此可提升安全性 ▪ 主密碼長度為 8~128 字元，可設定除退格鍵(Backspace)與雙引號(")以外的所有字元 ▪ 執行 no key config-key password-encrypt 指令可移除主密碼，惟此動作會把已加密的密碼改以明文方式儲存，設備將會跳出警告訊息提醒管理者			

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
4	TWGCB-03-004-0004	密碼管理	密碼復原	▪ 密碼復原功能預設為啟用 ▪ 建議停用此功能，以避免駭客規避實體防護改變現有登入密碼、管理者執行模式密碼及本機使用者密碼 ▪ 在 ASA 系列防火牆上，若啟用密碼復原功能，使用者可於 ASA 啟動時進入 ROMMON(ROM Monitor)模式取得完整的設定檔，藉此修改啟動配置中的密碼。若停用此功能，當使用者嘗試進入ROMMON模式時,ASA會提示使用者清除所有快閃記憶體檔案系統。使用者無法在清除動作執行前進入 ROMMON 模式。若使用者選擇不清除，則 ASA 將會重新	hostname (config)# no service password-recovery	停用	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				啟動			
5	TWGCB-03-004-0005	密碼管理	密碼最長使用期限	▪此項原則設定決定使用者變更密碼之前，密碼可以使用的期限(天數)，當密碼到期時，強制變更密碼，以降低因長期使用同一組密碼而遭破解之情形發生 ▪密碼最長使用期限有效值為0至65535天。預設值為0天，表示密碼永遠不會到期 ▪舊密碼將於到期日的12:00 a.m.失效	hostname(config)#password-policy lifetime 90	90天	僅適用於ASA 9.x版
6	TWGCB-03-004-0006	密碼管理	密碼變更最小字元數	▪此項原則設定決定新密碼與舊密碼相比，新密碼中必須更改的最小字元數，以降低因使用相同密碼組合，容易遭受駭客猜測破解	hostname(config)#password-policy minimum-changes 4	4個字元	僅適用於ASA 9.x版

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				▪密碼變更最小字元數有效值為 0 至 64 個字元。預設值為 0，表示可使用相同密碼組合 ▪字元比對與位置無關，意謂著設定新密碼時，某字元沒有出現在舊密碼中的任何位置，才被視為 1 次有效變更。因此若設定為 4 個字元，表示新密碼至少須包含 4 個與舊密碼完全不同的字元，才能成為新密碼			
7	TWGCB-03-004-0007	密碼管理	大寫字母最少個數	▪此項原則設定決定密碼必須包含至少幾個大寫字母。使用複雜的密碼組合，可降低攻擊者利用暴力破解或字典檔攻擊等方式成功取得密碼之機會 ▪大寫字母最少個數有效值為	hostname(config)#password-policy minimum-uppercase 1	1 個	僅適用於 ASA 9.x 版

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				0 至 64 個。預設值為 0，表示密碼中可以沒有大寫字母			
8	TWGCB-03-004-0008	密碼管理	小寫字母最少個數	▪ 此項原則設定決定密碼必須包含至少幾個小寫字母。使用複雜的密碼組合，可降低攻擊者利用暴力破解或字典檔攻擊等方式成功取得密碼之機會 ▪ 小寫字母最少個數有效值為 0 至 64 個。預設值為 0，表示密碼中可以沒有小寫字母	hostname(config)#password-policy minimum-lowercase 1	1 個	僅適用於 ASA 9.x 版
9	TWGCB-03-004-0009	密碼管理	數字字元最少個數	▪ 此項原則設定決定密碼必須包含至少幾個數字字元。使用複雜的密碼組合，可降低攻擊者利用暴力破解或字典檔攻擊等方式成功取得密碼之機會	hostname(config)#password-policy minimum-numeric 1	1 個	僅適用於 ASA 9.x 版

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				▪數字字元最少個數有效值為0至64個。預設值為0，表示密碼中可以沒有數字字元			
10	TWGCB-03-004-0010	密碼管理	特殊符號最少個數	▪此項原則設定決定密碼必須包含至少幾個特殊符號。使用複雜的密碼組合，可降低攻擊者利用暴力破解或字典檔攻擊等方式成功取得密碼之機會 ▪特殊符號最少個數有效值為0至64個。預設值為0，表示密碼中可以沒有特殊符號	hostname(config)#password-policy minimum-special 1	1個	僅適用於ASA 9.x版
11	TWGCB-03-004-0011	密碼管理	最小密碼長度	▪此項原則設定決定密碼應包含的最少字元數。設定過於簡短的密碼組合，容易遭攻擊者成功破解 ▪最小密碼長度有效值為3至	hostname(config)#password-policy minimum-length 12	12個字元以上	僅適用於ASA 9.x版

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				64 個字元。預設值為 3，表示密碼至少包含 3 個字元 ▪ 若最小密碼長度小於其他密碼規則(最小不同字元或密碼複雜性)，則將顯示錯誤訊息，且無法成功變更密碼			
12	TWGCB-03-004-0012	裝置管理	變更預設主機名稱(Hostname)	▪ 此項原則設定決定是否變更預設主機名稱。建議可依單位內部命名慣例，為設備主機名稱進行命名 ▪ 因安全需求盤點與識別資產時，設備主機名稱扮演重要角色，且於資安事件處理過程中，亦可透過主機名稱進行不同紀錄檔之間的關聯分析，以協助釐清資安事件發生原因 ▪ 主機名稱最多可達 63 個字	hostname(config)#hostname <name_of_device>	變更預設主機名稱	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				元，開頭與結尾必須為字母或數字，且名稱只能包含字母、數字及連字符號(-)			
13	TWGCB-03-004-0013	裝置管理	停用未使用的介面	▪此項原則設定決定是否停用未使用的介面，以強化實體安全 ▪未使用的介面若未停用且未限制存取來源，則攻擊者可連接至設備未使用的介面，嘗試取得存取權限	▪步驟1：執行下列指令，找出未使用且未停用之介面名稱(<interface_physical_name>)： hostname#sh int ip brief | in _down ▪步驟2：針對所有未使用且未停用之介面，執行下列指令： hostname(config)#interface <interface_physical_name> hostname(config-if)#shutdown	停用未使用介面	
14	TWGCB-03-004-0014	AAA (Authentication,	錯誤登入鎖定次數	▪此項原則設定決定帳號被鎖定前，容許的密碼輸入錯誤次數。當使用者輸入錯誤密	hostname(config)# aaa local authentication attempts max-fail 3	小於等於3	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
		Authorization, Accounting)		碼達到最大失敗次數後，該使用者將被鎖定而無法登入，直到管理者解鎖為止 ▪ 限制本機使用者登入錯誤最大次數，可有效防範密碼暴力破解與字典檔攻擊 ▪ 錯誤登入鎖定次數有效值為1至16，預設情況下，設備未啟用此功能，且此功能不會影響權限等級15的使用者			
15	TWGCB-03-004-0015	AAA (Authentication, Authorization, Accounting)	本機使用者帳號與密碼	▪ 此項原則設定決定是否建立本機使用者帳號與密碼 ▪ 預設情況下，設備不需要強式使用者認證，導致攻擊者可輕易取得存取權限，藉由建立本機帳號並使用強式密碼，可提升設備安全性	hostname(config)#username <local_username> password <local_password> privilege <level> ▪ <local_username>：欲設定之使用者帳號 ▪ <local_password>：欲設定之	建立本機使用者帳號與密碼	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				▪使用者帳號長度範圍為 3 至 64 個字元，可使用除空格與問號之外的任意字元	密碼 ▪<level>：欲設定之權限等級，可設為 0~15，預設值為 2		
16	TWGCB-03-004-0016	AAA (Authentication, Authorization, Accounting)	刪除預設帳號	▪此項原則設定決定是否刪除已知的預設帳號 ▪常見預設帳號如 root、asa、admin、cisco、pix 等，若未刪除，攻擊者可嘗試破解預設帳號之密碼，以獲得裝置存取權限	▪步驟 1：執行下列指令以建立自定義管理者帳號(<customized_admin_account>)與密碼(<admin_password>)，並設定所需權限等級(<privilege_level>)： hostname(config)#username <customized_admin_account> password <admin_password> privilege <privilege_level> ▪步驟 2：執行下列指令刪除已知預設帳號：	刪除已知的預設帳號	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
					(<known_default_account>) hostname(config)# no username <known_default_account>		
17	TWGCB-03-004-0017	SSH 規則	限制 SSH 存取來源 IP 位址	▪此項原則設定決定允許哪些 IP 位址可透過 SSH 連線至設備 ▪僅允許管理者使用已授權之 IP 位址連線至設備進行管理，可降低未經授權存取，或暴露於暴力破解、字典檔攻擊或 DoS 攻擊等風險 ▪此指令支援 IPv4 與 IPv6 的 IP 位址	執行下列指令設定來源 IP(<source_ip>)、子網路遮罩(<source_netmask>)及介面名稱(<interface_name>)，以啟用 SSH 存取來源限制： hostname(config)#ssh <source_ip> <source_netmask> <interface_name>	僅授權之 IP 位址可存取 SSH	
18	TWGCB-03-004-0018	SSH 規則	SSH 版本	▪此項原則設定決定 SSH 使用版本 ▪SSH 提供可靠的傳輸層連	hostname(config)# ssh version 2	SSHv2	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				線，讓管理者進行設備管理，預設情況下，SSH 同時支援 SSHv1 與 SSHv2，惟 SSHv1 版本因存在許多安全問題，建議應停用 SSHv1，改採更加安全的 SSHv2 版本			
19	TWGCB-03-004-0019	SSH 規則	設定 RSA 金鑰位元大小	▪ 此項原則設定決定 SSH 協定用來加密的 RSA (Rivest-Shamir-Adleman)金鑰位元長度 ▪ SSH 是一個安全的遠端登入協定，允許管理者藉由 SSH 連線進行設備管理，並支援 DES、3DES 加密演算法，且使用基於 RSA 機制之金鑰交換方式，惟因 RSA 1024 位元金鑰可能遭破解，因此建議 RSA 金鑰至少須達 2048 位元	▪ 步驟 1：執行下列指令產生 RSA 金鑰，<enterprise_RSA_key_size> 需大於等於 2048 位元： hostname(config)# crypto key generate rsa modulus <enterprise_RSA_key_size> ▪ 步驟 2：執行下列指令儲存 RSA 金鑰至快閃記憶體： hostname(config)#write memory	大於等於 2048 位元	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				▪ 金鑰大小可設定為 512、768、1024、2048、3072 及 4096			
20	TWGCB-03-004-0020	SSH 規則	SCP 服務	▪ 此項原則設定決定是否啟用 Secure copy protocol (SCP)服務 ▪ FTP 與 TFTP 協定以明文方式傳輸資料，可能遭攻擊者利用封包側錄取得機敏資訊，改採如 HTTPS 或 SCP 等使用加密傳輸之通訊協定，可提升資料傳輸安全性	hostname(config)# ssh scopy enable	啟用	
21	TWGCB-03-004-0021	SSH 規則	Telnet 服務	▪ 此項原則設定決定是否啟用 Telnet 服務 ▪ 由於 Telnet 協定以明文方式傳輸帳號與密碼等資訊，且無法保證連線主機的身分，	▪ 步驟 1：執行下列指令確認是否已啟用 Telnet 服務： hostname# sh run telnet | i telnet_[0-9]|[0-9]|[0-9] ▪ 步驟 2：指定主機 IP 與子網	停用	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				因此可能遭攻擊者獲取機敏資訊。為了避免發生此類風險，應停用 Telnet 服務	路遮罩，針對已啟用 Telnet 服務之介面 (<interface_name>)停用 Telnet 服務： hostname(config)#no telnet 0.0.0.0 0.0.0.0 <interface_name> ▪ 步驟 3：執行下列指令移除 Telnet 逾時設定： hostname(config)#no telnet timeout <configured_timeout>		
22	TWGCB-03-004-0022	HTTP 規則	限制 HTTP 存取來源 IP 位址	▪ 此項原則設定決定允許哪些 IP 位址可透過 HTTP 連線至設備 ▪ 僅允許管理者使用已授權之 IP 位址連線至設備進行管	執行下列指令設定來源 IP<source_ip>、子網路遮罩 <source_netmask>及介面名稱 <interface_name>，以啟用 HTTP 存取來源限制：	僅授權之 IP 位址可存取 HTTP	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				理，可降低未經授權存取，或暴露於暴力破解、字典檔攻擊或 DoS 攻擊等風險	hostname(config)#http <source_ip> <source_netmask> <interface_name>		
23	TWGCB-03-004-0023	HTTP 規則	HTTPS 加密演算法	▪ 此項原則設定決定 HTTPS 所使用之加密演算法，原使用「ssl encryption」指令進行設定，自 ASA 版本 9.3(2)開始，改執行「ssl cipher」指令設定加密演算法 ▪ 若網路有可能被嗅探，以 HTTP 存取安全設備時，藉由使用安全加密演算法之 SSL 或 TLS 協定進行保護，可提升傳輸的資料安全性 ▪ 由於 SSLv3 已知存在一些已知弱點，建議至少採用 TLS 1.0 做為 SSL 伺服器版本 ▪ ASA 支援的 SSL 加密列表舉	▪ ASA 版本 8.x，執行下列指令以啟用 AES 256 演算法： hostname(config)# ssl encryption aes256-sha1 ▪ ASA 版本 9.x，執行下列指令以啟用 AES 256 演算法： hostname(config)# ssl cipher tlsv1 custom AES256-SHA	AES256	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				例如下： (1) DHE-RSA-AES256-SHA256 (2) AES256-SHA256 (3) DHE-RSA-AES128-SHA256 (4) AES128-SHA256 (5) DHE-RSA-AES256-SHA (6) AES256-SHA (7) DHE-RSA-AES128-SHA (8) AES128-SHA (9) DES-CBC3-SHA			
24	TWGCB-03-004-0024	Session 逾時	控制台 Session 逾時	▪ 此項原則設定決定控制台 Session 閒置後，等待多久(分鐘)後才中斷連線 ▪ 限制控制台 Session 逾時時	hostname(config)# console timeout 15	15 分鐘	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				間，可防止未經授權的使用者利用被丟棄的Session執行惡意行為 ▪控制台Session逾時時間有效值為0到60分鐘。預設值為0，代表Session永不逾時 ▪此項設定僅會影響Serial與enable的連線逾時，不會取代Telnet、SSH及HTTP之逾時設定			
25	TWGCB-03-004-0025	Session逾時	SSH Session逾時	▪此項原則設定決定SSH Session閒置後，等待多久(分鐘)後才中斷連線 ▪限制SSH Session逾時時間，可防止未經授權的使用者利用被丟棄的Session執行惡意行為	hostname(config)# ssh timeout 15	15分鐘	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				▪ SSH Session 逾時時間有效值為 1 到 60 分鐘。預設值為 5 分鐘			
26	TWGCB-03-004-0026	Session 逾時	HTTP Session 逾時	▪ 此項原則設定決定 HTTP Session 閒置後，等待多久(分鐘)後才中斷連線 ▪ 限制 HTTP Session 逾時時間，可防止未經授權的使用者利用被丟棄的 Session 執行惡意行為 ▪ HTTP Session 逾時時間有效值為 1 到 1440 分鐘。預設值為 20 分鐘	hostname(config)# http server session-timeout 15	15 分鐘	
27	TWGCB-03-004-0027	校時規則	NTP 驗證	▪ 此項原則設定決定是否啟用 NTP 驗證，以確保僅從可信賴的來源取得時間資訊 ▪ 若未啟用 NTP 驗證，駭客可	hostname(config)#ntp authenticate	啟用	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				架設 NTP 伺服器並廣播錯誤的時間資訊，當資安事件發生時將難以進行關聯分析。此外，駭客亦可能執行如 NTP 放大攻擊類型之 DDoS 攻擊 ▪ 預設為停用			
28	TWGCB-03-004-0028	校時規則	NTP 驗證金鑰	▪ 此項原則設定決定是否設定 NTP 驗證金鑰，以確保僅從可信賴的來源取得時間資訊 ▪ 啟用 NTP 驗證功能時，需進一步設定 NTP 驗證金鑰，以確保可從受信任之 NTP 伺服器取得時間同步資訊 ▪ 金鑰 ID(<key_id>)有效值為 1 至 4294967295，可設定多組受信任金鑰，以配置多台	▪ 步驟 1：設定驗證金鑰 ID： hostname(config)# ntp trusted-key <key_id> ▪ 步驟 2：設定驗證金鑰： hostname(config)# ntp authentication-key <key_id> md5 <authentication_key>	設定 NTP 驗證金鑰	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				NTP 伺服器 ▪ 金鑰(<authentication_key>)長度最長可設定 32 個字元 ▪ 預設為停用			
29	TWGCB-03-004-0029	校時規則	NTP 伺服器	▪ 此項原則設定決定是否指定受信任的 NTP 伺服器，以確保可取得正確的時間資訊 ▪ 受信任的 NTP 伺服器會透過 NTP 驗證金鑰進行身分驗證 ▪ 可同時設定多個受信任的 NTP 伺服器，設備會使用時間最準確的伺服器 ▪ 預設為停用	執行下列指令設定受信任的 NTP 伺服器： hostname(config)# ntp server <ip_address> key <key_id> source <interface_name> ▪ <key_id>為 NTP 驗證金鑰 ▪ <ip_address>為 NTP 伺服器的 IP ▪ <interface_name>為用來與 NTP 伺服器溝通的介面	設定可信任的 NTP 伺服器	
30	TWGCB-03-004-	校時規則	本機時區	▪ 此項原則設定決定是否指定本機時區，以確保可顯示正	hostname(config)# clock timezone UTC +8	UTC +8	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
	0030			確時間 ▪有了正確的時間資訊，可輕易辨別數位憑證是否仍在有效期限內，亦可藉由時戳資訊輔以確認紀錄檔內容正確性 ▪預設為 UTC			
31	TWGCB-03-004-0031	日誌記錄規則	日誌記錄	▪此項原則設定決定是否啟用日誌記錄(Logging)功能，以記錄相關活動與事件內容 ▪啟用日誌記錄功能，以保存相關活動軌跡資訊，是稽核與事件管理最基本的需求，核心設備與系統應啟用此功能	hostname(config)#logging enable	啟用	
32	TWGCB-03-004-	日誌記錄規則	記錄裝置ID	▪此項原則設定決定日誌檔中是否須包含裝置 ID 資訊	▪執行下列指令，設定以主機名稱做為裝置 ID：	啟用	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
	0032			▪從多個不同來源匯集資訊產出紀錄檔時，識別紀錄檔是從哪個特定裝置而來，可以減輕在紀錄檔中執行搜尋的負擔，亦可快速取得特定設備的資訊	hostname(config)#logging device-id hostname ▪若設備有使用虛擬防火牆功能，執行下列指令設定以虛擬防火牆名稱做為裝置 ID： hostname(config)#logging device-id context-name		
33	TWGCB-03-004-0033	日誌記錄規則	記錄時戳資訊	▪此項原則設定決定日誌檔中是否須包含時戳資訊 ▪藉由標記產生紀錄檔訊息的日期與時間，可針對事件保留一個完整的軌跡，可加快除錯與事件分析速度	hostname(config)#logging timestamp	啟用	
34	TWGCB-03-004-0034	日誌記錄規則	緊急通知門檻與Email	▪此項原則設定決定是否設定通知門檻與緊急通知Email。當日誌紀錄檔的嚴重性等級達到通知門檻時，將	▪步驟 1：執行下列指令，設定當嚴重性等級達 critical 以上即啟動 Email 通知功能： hostname(config)#logging	通知門檻設為critical，並設定緊急	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				寄送紀錄檔至指定 Email ▪ 在某些情況下，日誌伺服器因需花時間處理紀錄檔與建立報告，因此可能造成延誤通知。惟高嚴重性等級之事件需要管理者立即介入了解與處理，因此，產生的紀錄檔可直接寄送至管理者的 Email，以利即時處理	mail critical ▪ 步驟 2：請郵件伺服器管理者協助建立防火牆 Email 帳號 <firewall_Email_account>，並執行下列指令指定該 Email 帳號為寄件者： hostname(config)#logging from-address <firewall_Email_account> ▪ 步驟 3：取得防火牆管理者 Email 帳號 <firewall_admin_Email>，並執行下列指令指定該管理者 Email 帳號為收件者，負責接收紀錄檔： hostname(config)#logging recipient-address <firewall_admin_Email>	通知 Email	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
					▪ 步驟 4：向郵件伺服器管理者取得郵件伺服器 IP 位置 <mail_server_ip>，並執行下列指令進行設定： hostname(config)#smtp-server <mail_server_ip>		
35	TWGCB-03-004-0035	SNMP 規則	SNMP 群組適用之版本與安全層級	▪ 此項原則設定決定 SNMP 群組適用之版本與安全層級 ▪ SNMP v1 與 v2c 版本，於 SNMP 伺服器與用戶端之間以明文方式傳輸資料，SNMP v3 新增提供訊息驗證與加密功能，提升資料傳輸安全性 ▪ SNMP v3 提供下列 3 種安全層級： (1) NoAuthPriv (noauth)：無訊息驗證與加密	hostname(config)# snmp-server group <group_name> v3 priv	v3 priv	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				(2) AuthNoPriv (auth)：有訊息驗證，但無加密 (3) AuthPriv (priv)：訊息驗證與加密			
36	TWGCB-03-004-0036	SNMP 規則	SNMP v3使用者適用之身分驗證與加密演算法	▪ 此項原則設定指定 SNMP v3 使用者適用之身分驗證與加密演算法： (1) 身分驗證演算法選項包含 MD5 與 SHA (2) 加密演算法選項包含 DES、3DES 與 AES(包含 128、192 及 256 版) ▪ SNMP 使用者需隸屬於 SNMP 群組。要使用 SNMP v3，必須先設定 SNMP 群組，之後設定 SNMP 使用者，最後設定 SNMP 主機，	執行下列指令，設定 SNMP 使用者名稱<snmp_username>、使用者隸屬的群組<group-name>、身分驗證密碼<authentication_password>、加密密碼<encryption_password>，以及身分驗證與加密使用的演算法： hostname(config)#snmp-server user <snmp_username> <group-name> v3 auth SHA <authentication_password> priv AES 256	使用 SHA 做為身分驗證演算法，AES 256 做為加密演算法	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				方可發揮功效	<encryption_password>		
37	TWGCB-03-004-0037	SNMP 規則	變更 SNMP 預設 Community 名稱	▪ 此項原則設定決定是否變更 SNMP 預設 Community 名稱 ▪ ASA 8.2(1)以後版本，每一個 Community 名稱都會建立 2 個 SNMP 伺服器群組，分別給 v1 與 v2c 使用 ▪ 預設 SNMP Community 名稱為 public，可能遭攻擊者利用並從防火牆設備蒐集未經授權的資訊，因此應變更預設 Community 名稱 ▪ SNMP Community 名稱最長可設定 32 個字元	hostname(config)#snmp-server community <snmp_community_string>	變更 SNMP 預設 Community 名稱	
38	TWGCB-03-004-0038	Control Plane	限制 ICMP 流量	▪ 此項原則設定決定是否僅特定主機或子網路允許接受與處理 ICMP 流量	▪ 步驟 1：執行下列指令，僅允許來自受信任子網路的 ICMP 流量到未受信任的介	僅允許來自受信任的子網路	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				▪ ICMP 用於 TCP/IP 網路中傳送控制訊息，提供可能發生在網路環境中的各種問題回饋，透過這些資訊，使管理者可以對所發生的問題進行分析，並採取適當的措施，惟可能用來執行 ICMP 攻擊，因此應只允許接受與處理來自受信任的特定主機或子網路的 ICMP 流量 ▪ 預設值為啟用，並允許接受所有 ICMP 流量	面，若有多個受信任子網路，請重複執行此步驟： hostname(config)# icmp permit <subnet> <mask> <untrusted_interface_name> -<untrusted_interface_name>為未受信任的介面名稱 -<subnet>為受信任的子網路 -<mask>為受信任的子網路遮罩 ▪ 步驟 2：執行下列指令，未受信任的介面拒絕接受其他來源的 ICMP 流量 hostname(config)# icmp deny any <untrusted_interface_name>	之 ICMP 流量到未受信任的介面	
39	TWGCB	Data	DNS 服務	▪ 此項原則設定決定是否設定	▪ 步驟 1：執行下列指令啟用	設定與啟	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
	-03-004-0039	Plane		與啟用 DNS 服務，供設備進行名稱解析 ▪ 設備可能需要執行 DNS 查詢以達成 URL 過濾，或供殭屍網路過濾功能透過 DNS 伺服器存取動態資料庫伺服器，並解析靜態資料庫中的條目	DNS 解析，並指定特定介面(<interface_name>)連接至 DNS 伺服器： hostname(config)# dns domain-lookup <interface_name> ▪ 步驟 2：設定 DNS 伺服器群組： hostname(config)# dns server-group DefaultDNS ▪ 步驟 3：取得受信任之 1 個或多個 DNS 伺服器 IP 位址 <dns_ip_address>，針對每 1 個 IP 執行下列指令： hostname(config-dns-server-group)#name-server <dns_ip_address>	用 DNS 服務	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
40	TWGCB-03-004-0040	Data Plane	限制未受信任介面收到零碎封包的處理方式	▪ 此項原則設定指定 1 個完整封包的最大分段數量，當未受信任介面收到封包後，可根據此項設定決定接受或丟棄 ▪ 封包分段檢查通常在第 1 個封包執行，因此，攻擊者可在其他封包片段放置惡意負載(Payload)，藉由封包分段方式規避防火牆、IPS 等安全機制，甚至進而對內部系統執行 DoS 攻擊 ▪ 預設值為 24，代表 1 個封包最高可分為 24 個片段。設定為 1，意味著 1 個封包只能有 1 個片段，也就是設備僅接受未分段之封包	執行下列指令，限制未受信任介面僅能接受未分段之封包：hostname(config)#fragment chain 1 <untrusted_interface_name> ▪ <untrusted_interface_name> 為未受信任的介面名稱	1	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
41	TWGCB-03-004-0041	Data Plane	TCP 攔截統計	▪此項原則設定決定威脅偵測統計資訊中，是否包含 TCP 攔截功能所攔截攻擊的統計資訊 ▪TCP 攔截功能可有效保護網路與伺服器免於遭受如 SYN Flood 之 DoS 攻擊。當到達最大允許連線數時，透過 TCP 攔截功能，防火牆將不再允許連線至受影響的伺服器 ▪藉由 TCP 攔截統計資訊，可協助管理者在攻擊初期階段即可得知攻擊情形並進行防禦	hostname(config)# threat-detection statistics tcp-intercept	啟用	
42	TWGCB-03-004-0042	Data Plane	未受信任介面之 uRPF 功	▪此項原則設定決定未受信任介面是否啟用單播反向路徑轉發(unicast Reverse-Path	執行下列指令，針對未受信任介面啟用 uRPF 功能： hostname(config)# ip verify	啟用	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
			能	Forwarding, uRPF)功能 ▪ 單播反向路徑轉發也稱為反向路徑查詢，啟用此功能後，設備在接收到封包時，會檢查封包來源 IP 位址，並與路由表比對，確認該封包來源 IP 位址是否為可連線的 IP，如果無法連線(代表該來源 IP 位址為偽造 IP)，該封包會立即被丟棄，藉此可防止 IP 偽造或阻斷服務攻擊	reverse-path <untrusted_interface_name> ▪ <untrusted_interface_name> 為未受信任的介面名稱		
43	TWGCB-03-004-0043	Data Plane	未受信任介面之殭屍網路防護	▪ 此項原則設定決定未受信任介面是否啟用殭屍網路防護功能 ▪ 在殭屍網路的情境中，許多電腦感染惡意程式後，會在使用者不知情的情況下蒐集檔案並傳送給攻擊者，或從	▪ 步驟 1：執行下列指令，確認已有可用之 DNS 伺服器： hostname#sh run | i name-server ▪ 步驟 2：執行下列指令，下載並使用已知惡意網站清單：	啟用	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
				遠端控制受害電腦進而攻擊其他電腦 ▪啟用殭屍網路保護功能，將允許設備過濾並丟棄殭屍網路流量 ▪預設為停用	hostname(config)#dynamic-filter updater-client enable hostname(config)#dynamic-filter use-database ▪步驟3：執行下列指令新增一個 class map<dns_class_map_name>讓資安設備比對 DNS 流量： hostname(config)#class-map <dns_class_map_name> hostname(config-cmap)#match port udp eq domain ▪步驟4：執行下列指令新增1個 policy-map 名稱<dns_policy_map_name>，並指定分類<dns_class_map_name>，以要求防護設備針對符合條件的		

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
					DNS 流量，檢查該流量之網域名稱是否在惡意網域名稱中： hostname(config)#policy-map <dns_policy_map_name> hostname(config-pmap)# class <dns_class_map_name> hostname(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop ▪ 步驟 5：執行下列指令，將檢查規則套用至未受信任介面： <untrusted_interface_name> hostname(config)# service-policy <dns_policy_map_name> interface		

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
					<untrusted_interface_name> ▪ 步驟 6：執行下列指令，針對未受信任介面啟用殭屍網路流量過濾功能： hostname(config)# dynamic-filter enable interface <untrusted_interface_name> ▪ 步驟 7：執行下列指令，丟棄任何在未受信任介面上發現的殭屍網路流量： hostname(config)# dynamic-filter drop blacklist interface <untrusted_interface_name>		
44	TWGCB-03-004-0044	Data Plane	存取列表最後一條明確定義	▪ 此項原則設定決定各個介面所套用的每條 access-list 是否皆明確定義相對應之 deny	▪ 步驟 1：執行下列指令，取得已套用至介面的 access-list 列表：	啟用	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
			deny any 規則	any 規則 ▪ 設定明確的 deny any 規則，並啟用日誌記錄功能，可提供有效的資訊協助釐清資安事件發生原因 ▪ 預設為停用	hostname# sh run access-group ▪ 步驟 2：執行下列指令，確認已明確定義 deny any 規則的 access-list 列表： hostname#sh run access-list | in deny.ip.any.any ▪ 步驟 3：針對步驟 1 所列出但未出現在步驟 2 之 access-list 項目(<access-list_name>)，執行下列指令設定 deny any 規則： hostname(config)#<access-list_name> extended deny ip any any log		

資料來源：本中心整理

3. 參考文獻

[1]CIS_Cisco_Firewall_Benchmark_v4.1.0。

https://www.cisecurity.org/benchmark/cisco/

[2]Cisco ASA Series Command Reference, A - H Commands

https://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/A-H/cmdref1.html

[3]Cisco ASA Series Command Reference, I - R Commands

https://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/I-R/cmdref2.html

[4]Cisco ASA Series Command Reference, S Commands

https://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/S/cmdref3.html

[5]Cisco ASA Series Command Reference, T - Z Commands and IOS Commands for the ASASM

https://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/T-Z/cmdref4.html

[6]政府組態基準 GCB_Juniper Firewall 說明文件(V1.0)
http://download.nccst.nat.gov.tw/attachfilegcb/%E6%94%BF%E5%BA%9C%E7%B5%84%E6%85%8B%E5%9F%BA%E6%BA%96GCB_Juniper%20Firewall%E8%AA%AA%E6%98%8E%E6%96%87%E4%BB%B6(V1.0)_1060512.docx

[7]政府組態基準 GCB_Fortinet Fortigate 說明文件(V1.1)
http://download.nccst.nat.gov.tw/attachfilegcb/%E6%94%BF%E5%BA%9C%E7%B5%84%E6%85%8B%E5%9F%BA%E6%BA%96GCB_Fortinet%20Fortigate%E8%AA%AA%E6%98%8E%E6%96%87%E4%BB%B6(V1.1).docx