政府組態基準
FortiNet FortiGate
(V1.2)

行政院國家資通安全會報技術服務中心
中華民國108年12月

修訂歷史紀錄表

項次	版次	修訂日期	說明
1	1.0	107/1/29	新編
2	1.1	107/9/5	修正部分說明與錯別字
3	1.2	108/12/17	▪ 新增「TWGCB-ID」欄位與資料 ▪ 調整表 2「GCB 設定值」欄位順序 ▪ 修改表 2 項次 16「密碼最長使用期限」的設定方法由「set expire 90」調整為「set expire-day 90」 ▪ 移除表 2「密碼到期通知」
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. FortiNet FortiGate 設備政府組態基準列表 3
3. 參考文獻 15

表 目 次

表 1　FortiNet FortiGate 設備組態基準項目統計 1
表 2　FortiNet FortiGate 設備政府組態基準列表 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 FortiNet FortiGate 設備，FortiOS 5.2 版本。

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。FortiNet FortiGate 設備組態基準計有 46 項設定項目，項目統計詳見表 1。

表1　FortiNet FortiGate 設備組態基準項目統計

項次	類別	項數	合計
1	Interface	6	46
2	Password-Policy	10	
3	NTP	3	
4	Admin	4	
5	Auto-Install	2	
6	Global	10	
7	SNMP User	4	
8	SNMP Community	5	
9	Log Setting	2	

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. FortiNet FortiGate 設備政府組態基準列表

表2　FortiNet FortiGate 設備政府組態基準列表

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-03-003-0001	Interfaces	允許介面連線的方式	為了確保介面的資料傳輸的安全性，選擇較安全的 HTTPS 與 SSH 連線方式，相較於 HTTP、Telnet 可提供加密保護	config system interface edit <interface_name> set allowaccess <access_types>	HTTPS、SSH	
2	TWGCB-03-003-0002		需要設置介面描述	為了提高網路規劃的效率，有效進行故障排除，並避免可能危及網絡安全的混亂與錯誤，所有介面應配置相關的描述說明	config system interface edit <interface_name> set description <text>	設置介面描述	
3	TWGCB-03-003-0003		禁止廣播發送	有些阻斷服務攻擊會透過廣播發送來達成，例如 Smurf attack，因此禁止廣播發送以提升安全性	config system interface edit <interface_name> set broadcast-forward disable	禁止廣播發送	
4	TWGCB-03-003-		丟棄零碎	部分攻擊透過封包分段之方式	config system interface edit <interface_name>	啟用丟棄零	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
	0004		封包	繞過防火牆之後，再進行重組	set drop-fragment enable	碎封包	
5	TWGCB-03-003-0005		丟棄重疊封包	部分攻擊透過封包重疊之方式，繞過防火牆之後，再進行重組	config system interface edit <interface_name> set drop-overlappedfragment enable	啟用丟棄重疊封包	
6	TWGCB-03-003-0006		介面偵錯功能	當介面設置出錯時，提供提醒	config system interface edit <interface_name> set fail-detect enable	啟用介面偵錯功能	
7	TWGCB-03-003-0007	Password-Policy	密碼原則	若要設定密碼原則，此項目原則需設為啟用	config system password-policy set status enable	啟用密碼原則	
8	TWGCB-03-003-0008		套用密碼原則對象	當密碼原則啟用後，將套用對象設置為所有管理者	config system password-policy set apply-to admin-password	admin-password	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
9	TWGCB-03-003-0009		密碼複雜性(小寫)	應使用複雜的密碼組合，以降低攻擊者透過暴力破解或字典檔攻擊等方式的成功機率	config system password-policy set min-lower-case-letter 1	至少 1 個	
10	TWGCB-03-003-0010		密碼複雜性(大寫)	應使用複雜的密碼組合，以降低攻擊者透過暴力破解或字典檔攻擊等方式的成功機率	config system password-policy set min-upper-case-letter 1	至少 1 個	
11	TWGCB-03-003-0011		密碼複雜性(特殊符號)	應使用複雜的密碼組合，以降低攻擊者透過暴力破解或字典檔攻擊等方式的成功機率	config system password-policy set min-non-alphanumeric 1	至少 1 個	
12	TWGCB-03-003-0012		密碼複雜性(數字)	應使用複雜的密碼組合，以降低攻擊者透過暴力破解或字典檔攻擊等方式的成功機率	config system password-policy set min-number 1	至少 1 個	
13	TWGCB		密碼最小	過於簡短的密碼組合方式，容易	config system	至少 12 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
	-03-003-0013		長度	遭受攻擊者猜測破解，安全的密碼至少應採用 12 碼以上的字元長度	password-policy set minimum-length 12		
14	TWGCB-03-003-0014		上次密碼至少 4 個字元不同	同樣的密碼組合方式，容易遭受攻擊者猜測破解，安全的密碼至少與上一次的密碼四個位元不同	config system password-policy set change-4-characters enable	啟用與上次密碼至少四個字元不同	
15	TWGCB-03-003-0015		密碼期限	若要使用密碼期限功能，此項目原則需設為啟用	config system password-policy set expire-status enable	啟用密碼期限	
16	TWGCB-03-003-0016		密碼最長使用期限	應設置密碼最長使用期限，當密碼到期時，強制變更密碼，以降低遭受破解機率	config system password-policy set expire-day 90	90	
17	TWGCB-03-003-0017	NTP	NTP 校時	若要使用 NTP 校時,此項目原則需設為啟用	config system ntp set ntpsync enable	啟用 NTP 校時	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
18	TWGCB-03-003-0018		需要外部時間來源	為了確保日誌資料的有效性，並釐清故障或安全事件發生的時間點，應設置至少 2 個以上的 NTP 伺服器	config system ntp set ntp-server1 <ipv4_addr> set ntp-server2 <ipv4_addr>	設置 NTP 伺服器位置	
19	TWGCB-03-003-0019		NTP v3	使用最新的 NTP v3，以提供較佳的 NTP 校時功能	config system ntp set ntpv3 enable	啟用 NTP v3	
20	TWGCB-03-003-0020	Admin	須設置管理員密碼	應設置密碼以保護 Admin 帳戶	config system admin set password <admin_password>	設置管理員密碼	
21	TWGCB-03-003-0021		密碼原則變更時強制更改密碼	當密碼原則變更時，Admin 帳戶密碼亦須變更以符合密碼原則	config system admin set force-password-change enable	啟用密碼原則變更時強制更改密碼	
22	TWGCB		來賓帳戶	應不允許使用來賓帳戶登入系	config system admin	停用來賓帳	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
	-03-003-0022			統	set guest-auth disable	戶	
23	TWGCB-03-003-0023		遠端刪除Admin連線	不允許從遠端刪除 Admin 連線狀態，避免 Admin 正在設定組態時中斷，而造成設備異常	config system admin set allow-remove-adminsession disable	禁止遠端刪除 Admin 連線	
24	TWGCB-03-003-0024	Auto-Install	自動從USB載入系統設定檔	攻擊者可以透過 USB 連接埠在 FortiGate 上載入組態設定檔或是更新韌體，為了避免這種情況應停用自動從 USB 載入系統設定檔	config system auto-install set auto-install-config disable	停用自動從USB載入系統設定檔	
25	TWGCB-03-003-0025		自動從USB安裝系統韌體	攻擊者可以透過 USB 連接埠在 FortiGate 上載入組態設定檔或是更新韌體，為了避免這種情況應停用自動從 USB 載入系統設定檔	config system auto-install set auto-install-image enable disable	停用自動從USB安裝系統韌體	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
26	TWGCB-03-003-0026	Global	SSLv3 加密協定	目前已知 SSLv3 存在 POODLE 的弱點，為提升安全性應停用 SSLv3 加密協定	config system global set admin-https-ssl-versions tlsv1-0 tlsv1-1 tlsv1-2	停用 SSLv3 加密協定	
27	TWGCB-03-003-0027		將 HTTP 導到 HTTPS	相較於 HTTP，HTTPS 提供較安全的傳輸加密機制。當管理員透過 HTTP 連線時自動導至 HTTPS，以提升安全性	config system global set admin-https-redirect enable	啟用將 HTTP 導到 HTTPS	
28	TWGCB-03-003-0028		錯誤登入鎖定次數	針對 Telnet 或 SSH 等遠端管理協定，為了降低暴力破解的速度，應限制 3 次以下嘗試登入失敗後，中斷連線	config system global set admin-lockout-threshold 3	設置 3 次錯誤登入鎖定	
29	TWGCB-03-003-0029		錯誤登入鎖定時間	針對 Telnet 或 SSH 等遠端管理協定，為了降低暴力破解的速度，應限制錯誤登入的鎖定時間為 900 秒	config system global set admin-lockout-duration 900	設置錯誤登入鎖定時間為 900 秒	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
30	TWGCB-03-003-0030		限制以網路設備主機型號作為主機名稱	若以網路設備的型號、類型、製造商或是軟體版本等資訊作為主機的名稱，可能成為攻擊者資訊蒐集的內容，進一步危害網路設備的安全。為避免此情形發生，應限制以網路設備主機型號等資訊作為主機名稱	config system global set hostname <unithostname>	設置主機名稱	
31	TWGCB-03-003-0031		上傳病毒偵測報告	預設情況下，FortiGate 會定期向 FortiGuard 傳送加密的惡意軟體統計訊息，但即使加密仍有可能洩露統計資訊，因此建議停用本功能	config system global set fds-statistics disable	停用上傳病毒偵測報告	
32	TWGCB-03-003-0032		閒置逾時	應設置 15 分鐘內的閒置逾時功能，以避免無人使用的 Session 佔用連線資源，或忘記登出而造成資安疑慮	config system global set admin-ssh-grace-time 900	設置閒置逾時 900	
33	TWGCB		允許最多	同時間僅允許一位管理員進行	config system global	允許最多 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
	-03-003-0033		幾位管理者同時登入	設備操作，以免造成操作上的衝突，造成設備異常	set admin-login-max 1	位管理者同時登入	
34	TWGCB-03-003-0034		重設按鈕	停用設備上的重新設定按鈕，避免因誤觸而遺失資料	config system global set admin-reset-button disable	停用重設按鈕	
35	TWGCB-03-003-0035		手動儲存組態	當組態修改時，不會自動儲存，下一次重新啟動後回復到修改前的組態	config system global set cfg-save manual	啟用手動儲存組態	
36	TWGCB-03-003-0036	SNMP User	需要設置安全等級為加密及驗證	SNMPv3提供訊息驗證與加密功能，此項目設定為加密及驗證可使用此功能	config system snmp user edit <username> set set security-level auth-priv	設置加密及驗證	
37	TWGCB-03-003-0037		需要以AES256加密的	SNMPv3提供訊息驗證與加密功能，比以前版本具有更高安全性，當中最高加密方式可採用	config system snmp user edit <username> set priv-proto aes256	設置AES256加密	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
			SNMP 存取	AES256			
38	TWGCB-03-003-0038		需要以 SHA 驗證 SNMPv3 的存取	FortiOS 在 SNMPv3 使用的驗證方式為 MD5 與 SHA。MD5 屬於較舊的協議，近年來已經存在相關的脆弱性，因此應使用較新與較值得信賴的 SHA 驗證方式	config system snmp user edit <username> set auth-proto sha	設置 SHA 存取	
39	TWGCB-03-003-0039		SNMPv3 使用非預設連接埠	SNMPv3 預設使用 161 埠，建議改為其他埠號，以降低入侵的風險	config system snmp user edit <username> set query-port <port_int>	變更 SNMPv3 預設連接埠號	
40	TWGCB-03-003-0040	SNMP Community	禁止常見的 SNMP 通用字串	可利用通用字串進行管理行為，若攻擊者猜測到所使用的通用字串時，可如同合法管理者一樣存取 SNMP 介面	config system snmp community edit <index Num> set name <community_name>	禁用 SNMP 通用字串	
41	TWGCB		停用	SNMP 可以利用網路管理的方式	config system snmp	停用 SNMP	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
	-03-003-0041		SNMP v1版本	針對設備進行設定檔的寫入或讀取，並且舊的 SNMP 版本 v1與 v2c 存在不安全的明碼傳輸設計，攻擊者可擷取傳輸資訊進而取得通用字串內容	community set query-v1-status disable	v1 版本	
42	TWGCB-03-003-0042		SNMPv1不使用預設連接埠	SNMPv1 預設使用 161 埠，建議改為其他埠號，以降低入侵的風險	config system snmp community edit <index Num> set query-v1-prot <port num>	變更SNMPv1 預設連接埠號	
43	TWGCB-03-003-0043		停用SNMP v2c 版本	SNMP 可以利用網路管理的方式針對設備進行設定檔的寫入或讀取，並且舊的 SNMP 版本 v1與 v2c 存在不安全的明碼傳輸設計，攻擊者可擷取傳輸資訊進而取得通用字串內容	config system snmp community set query-v2c-status disable	停用 SNMP v2c 版本	
44	TWGCB		SNMPv2c	SNMPv2c 預設使用 161 埠，建	config system snmp	變更	

項次	TWGCB-ID	類別	原則設定名稱	說明	設定方法	GCB設定值	備註
	-03-003-0044		不使用預設連接埠	議改為其他埠號，以降低入侵的風險	community edit <index Num> set query-v2c-prot <port num>	SNMPv2c 預設連接埠號	
45	TWGCB-03-003-0045	Log Setting	對非法封包進行紀錄	當有不合法的封包經過設備時，對該封包進行記錄，以利後續需進行故障排除或事件追蹤	config log setting set log-invalid-packet enable	設置對非法封包進行紀錄	
46	TWGCB-03-003-0046		取代登入使用者名稱為匿名	當有使用者登入設備時，禁止以匿名紀錄其行為，以利後續需進行故障排除或事件追蹤	config log setting set user-anonymize disable	停用取代登入使用者名稱為匿名	

資料來源：本中心整理

3. 參考文獻

[1]FortiOS™ CLI Reference for FortiOS 5.2, https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/27300d29-1a11-11e9-9685-f8bc1258b856/fortigate-cli-52.pdf

[2]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