|  |  |  |
| --- | --- | --- |
|  | | |
| **政府組態基準**  **FortiNet FortiGate**  **(V1.1)** | | |
|  |  |  |
|  | | |
| **行政院國家資通安全會報技術服務中心**  中華民國107年9月 | | |

**修訂歷史紀錄表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 項次 | 計畫資訊 | | | 發行紀錄 | | 說明 |
| 年度 | 版次 | 修訂日期 | 版次 | 日期 |
| 1 | 107 | V1.0 | 107/1/29 |  |  | 新編 |
| 2 | 107 | V1.1 | 107/9/5 |  |  | 修正部分說明與錯別字 |
| 3 |  |  |  |  |  |  |
|  | | | | | | |

**目　次**

[1. 前言 1](#_Toc523948641)

[1.1. 適用環境 1](#_Toc523948642)

[1.2. 項數統計 1](#_Toc523948643)

[1.3. 文件發行 2](#_Toc523948644)

[2. FortiNet FortiGate設備政府組態基準列表 3](#_Toc523948645)

[3. 參考文獻 15](#_Toc523948646)

**表 目 次**

[表1 FortiNet FortiGate設備組態基準項目統計 1](#_Toc481505772)

[表2 FortiNet FortiGate設備政府組態基準列表 3](#_Toc481505773)

# 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。

## 適用環境

本文件適用於FortiNet FortiGate設備，FortiOS版本 5.2版本。

## 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47項設定項目，項目統計詳見表1。

1. FortiNet FortiGate設備組態基準項目統計

|  |  |  |  |
| --- | --- | --- | --- |
| 項次 | 類別 | 項數 | 合計 |
| 1 | Interface | 6 | 47 |
| 2 | Password-Policy | 11 |
| 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 |
| 本中心整理 | | | |

## 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<http://www.nccst.nat.gov.tw/GCB>。

# FortiNet FortiGate設備政府組態基準列表

1. FortiNet FortiGate設備政府組態基準列表

| 項次 | 類別 | 原則設定名稱 | GCB設定值 | 說明 | 設定方法 | 備註 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Interfaces | 允許介面連線的方式 | HTTPS、SSH | 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> |  |
| 2 | 需要設置介面描述 | 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> |  |
| 3 | 禁止廣播發送 | 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 |  |
| 4 | 丟棄零碎封包 | 啟用丟棄零碎封包 | 部分攻擊透過封包分段之方式繞過防火牆之後，再進行重組 | config system interface  edit <interface\_name>  set drop-fragment enable |  |
| 5 | 丟棄重疊封包 | 啟用丟棄重疊封包 | 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 |  |
| 6 | 介面偵錯功能 | 啟用介面偵錯功能 | 當介面設置出錯時，提供提醒 | config system interface  edit <interface\_name>  set fail-detect enable |  |
| 7 | Password-Policy | 密碼原則 | 啟用密碼原則 | 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 |  |
| 8 | 套用密碼原則對象 | admin-password | 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 |  |
| 9 | 密碼複雜性(小寫) | 至少1個 | 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 |  |
| 10 | 密碼複雜性(大寫) | 至少1個 | 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 |  |
| 11 | 密碼複雜性(特殊符號) | 至少1個 | 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 |  |
| 12 | 密碼複雜性(數字) | 至少1個 | 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 |  |
| 13 | 密碼最小長度 | 至少12碼 | 過於簡短的密碼組合方式，容易遭受攻擊者猜測破解，安全的密碼至少應採用12碼以上的字元長度 | config system password-policy  set minimum-length 12 |  |
| 14 | 上次密碼至少4個字元不同 | 啟用與上次密碼至少四個字元不同 | 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 |  |
| 15 | 密碼期限 | 啟用密碼期限 | 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 |  |
| 16 | 密碼最長使用期限 | 90 | 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 90 |  |
| 17 | 密碼到期通知 | 14 | 本項原則設定決定在使用者的密碼即將到期時，要提前多久(天數)事先提醒 | config system password-policy  set expire-day 14 |  |
| 18 | NTP | NTP校時 | 啟用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 |  |
| 19 | 需要外部時間來源 | 設置NTP伺服器位置 | 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> |  |
| 20 | NTP v3 | 啟用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 |  |
| 21 | Admin | 須設置管理員密碼 | 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> |  |
| 22 | 密碼原則變更時強制更改密碼 | 啟用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 |  |
| 23 | 來賓帳戶 | 停用來賓帳戶 | 應不允許使用來賓帳戶登入系統 | config system admin  set guest-auth disable |  |
| 24 | 遠端刪除Admin連線 | 禁止遠端刪除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 |  |
| 25 | Auto-Install | 自動從USB載入系統設定檔 | 停用自動從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 |  |
| 26 | 自動從USB安裝系統韌體 | 停用自動從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 |  |
| 27 | Global | SSLv3加密協定 | 停用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 |  |
| 28 | 將HTTP導到HTTPS | 啟用將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 |  |
| 29 | 錯誤登入鎖定次數 | 設置3次錯誤登入鎖定 | 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 |  |
| 30 | 錯誤登入鎖定時間 | 設置錯誤登入鎖定時間為900秒 | 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 |  |
| 31 | 限制以網路設備主機型號作為主機名稱 | 設置主機名稱 | 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> |  |
| 32 | 上傳病毒偵測報告 | 停用上傳病毒偵測報告 | 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 |  |
| 33 | 閒置逾時 | 設置閒置逾時900 | 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 |  |
| 34 | 允許最多幾位管理者同時登入 | 允許最多1位管理者同時登入 | 同時間僅允許一位管理員進行設備操作，以免造成操作上的衝突，造成設備異常 | config system global  set admin-login-max 1 |  |
| 35 | 重設按鈕 | 停用重設按鈕 | 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 |  |
| 36 | 手動儲存組態 | 啟用手動儲存組態 | 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 |  |
| 37 | SNMP User | 需要設置安全等級為加密及驗證 | 設置加密及驗證 | 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 |  |
| 38 | 需要以AES256加密的SNMP存取 | 設置AES256加密 | 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AES256 | config system snmp user  edit <username>  set priv-proto aes256 |  |
| 39 | 需要以SHA驗證SNMPv3的存取 | 設置SHA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 |  |
| 40 | SNMPv3使用非預設連接埠 | 變更SNMPv3預設連接埠號 | 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> |  |
| 41 | SNMP Community | 禁止常見的SNMP通用字串 | 禁用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> |  |
| 42 | 停用SNMP v1版本 | 停用SNMP v1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-v1-status disable |  |
| 43 | SNMPv1不使用預設連接埠 | 變更SNMPv1預設連接埠號 | 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> |  |
| 44 | 停用SNMP v2c版本 | 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 |  |
| 45 | SNMPv2c不使用預設連接埠 | 變更SNMPv2c預設連接埠號 | SNMPv2c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-v2c-prot <port num> |  |
| 46 | Log Setting | 對非法封包進行紀錄 | 設置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 |  |
| 47 | 取代登入使用者名稱為匿名 | 停用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 |  |
| 本中心整理 | | | | | | |

# 參考文獻

1. FortiOS™ CLI Reference for FortiOS 5.2 <http://docs.fortinet.com/uploaded/files/1981/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