

APPEL MDM 防火牆設定

目前各校都在建置 MDM SERVER，最近有些學校碰到了一些問題，最常碰到的就是開通 iPad 時，輸入完 MDM 帳密後，沒有回應，後來，後來我是在防火牆上政策，lan-lan 的 VIP-lan 中，加入 MDM 伺服器的 NAT 規則，就搞定了。

茲將本校的 MDM 伺服器分享給大家，拜託不要當駭客攻擊我家機器。

伺服器 MAC MINI + OS X Server

校內 IP：172.23.0.12

實體 IP：163.21.136.12

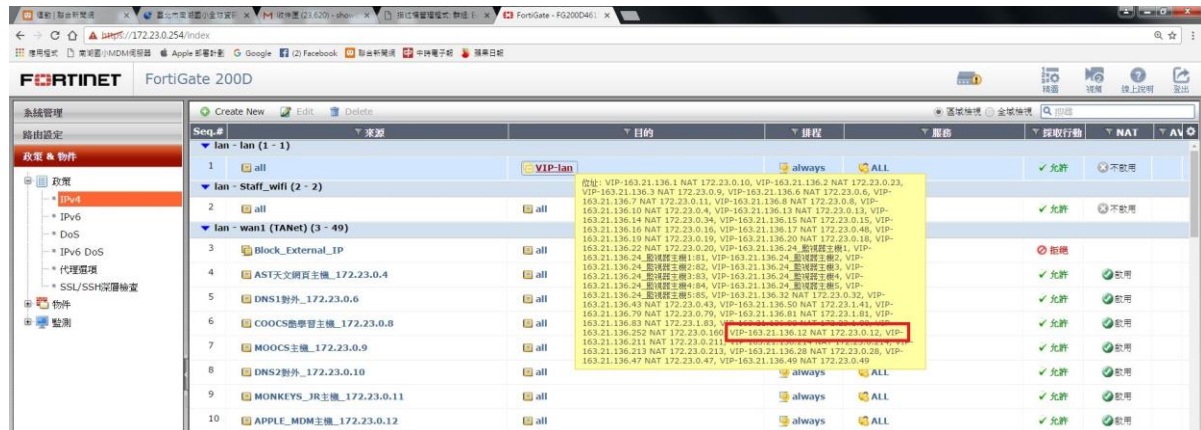
Domain Name：mdm.nhps.tp.edu.tw

防火牆：FortiGate 200D

防火牆上的設定：

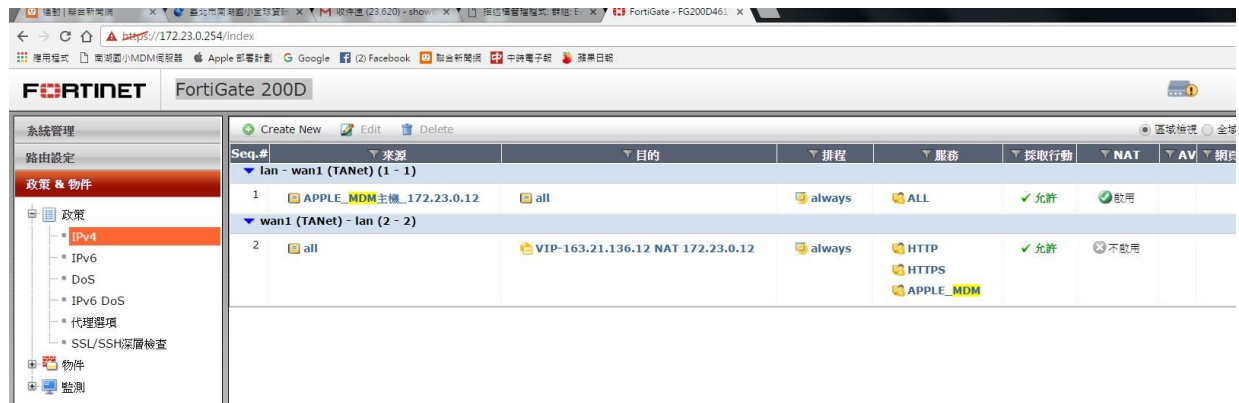
lan-lan

加入 MDM 的 NAT 物件，從校內 PING 虛擬與真實 IP 都能通



MDM IPV4 政策

lan-wan1 / wan1-lan 設定有這兩條



lan - wan1 (TANet)

內到外全開



wan1 (TANet) – lan

外面連借來有關 http,https, MDM PORT

The screenshot shows the FortiGate 200D configuration interface. The left sidebar is under '系統管理' (System Management) > '路由設定' (Routing Settings) > '政策 & 物件' (Policy & Objects). The main area shows the configuration for a policy:

- 入口 (In Interface): wan1 (TANet)
- 來源位址名稱 (Source Address Name): all
- 用戶(s) (User(s)): 點選新增... (Click to add...)
- 設備 (Device): 點選新增... (Click to add...)
- 出口 (Out Interface): lan
- 目的位址名稱 (Destination Address Name): VIP-163.21.136.12 NAT 172.23.0.12
- 排程 (Schedule): always
- 服務 (Service): HTTP, HTTPS, APPLE_MDM
- 採取行動 (Action): ACCEPT
- 防火牆 / 網路 選項 (Firewall / Network Options): 啟用 NAT (Enable NAT) is OFF.
- Security Profiles: 防毒與惡意程式檢測 (Anti-virus and Malware Detection) is OFF, profile: default.

MDM SERVICE

TCP1640, TCP2195-2196, TCP5223

The screenshot shows the FortiGate 200D configuration interface for an object named 'APPLE_MDM'. The left sidebar is under '系統管理' (System Management) > '路由設定' (Routing Settings) > '政策 & 物件' (Policy & Objects) > '物件' (Objects) > '服務' (Service).

The configuration for the service is as follows:

- 用戶名 (User Name): APPLE_MDM
- 註解 (Description): APPLE_MDM_PORT 14/255
- 在服務列表中顯示 (Show in Service List):
- Category: Uncategorized
- 協定型態 (Protocol Type): TCP/UDP/SCTP
- IP/FQDN: (Empty field)
- 網路協定 (Network Protocol): TCP
- 目的埠 (Destination Port):

| 低 (Low) | 高 (High) |
|---------|----------|
| 1640 | |
| 5223 | |
| 2195 | 2196 |
- 指定來源埠號 (Specify Source Port Number):

A '確定' (Confirm) button is visible at the bottom right.

IP Pool

讓 MDM SERVER 帶真實 163.21.136.12 IP 出去

| 用戶名 | 外部 IP 範圍 | 類型 | Ref. | 註解 |
|----------------|-------------------------------|-----|------|------------------|
| IPv4 Pool (53) | | | | |
| 163.21.136.1 | 163.21.136.1 - 163.21.136.1 | 超載 | 1 | DNS1 |
| 163.21.136.2 | 163.21.136.2 - 163.21.136.2 | 超載 | 1 | WWW網頁主機 |
| 163.21.136.3 | 163.21.136.3 - 163.21.136.3 | 超載 | 1 | MOOCs主機 |
| 163.21.136.6 | 163.21.136.6 - 163.21.136.6 | 超載 | 1 | DNS2 |
| 163.21.136.7 | 163.21.136.7 - 163.21.136.7 | 超載 | 1 | Monkeys JR |
| 163.21.136.8 | 163.21.136.8 - 163.21.136.8 | 超載 | 1 | COOC聽學習主機 |
| 163.21.136.10 | 163.21.136.10 - 163.21.136.10 | 超載 | 1 | AST天文主機 & W1 |
| 163.21.136.12 | 163.21.136.12 - 163.21.136.12 | 超載 | 1 | APPLE MDM SERVER |
| 163.21.136.13 | 163.21.136.13 - 163.21.136.13 | 超載 | 1 | EXAM聽學習測驗主機 |
| 163.21.136.14 | 163.21.136.14 - 163.21.136.14 | 超載 | 1 | SERVER5 ASP網頁主機 |
| 163.21.136.15 | 163.21.136.15 - 163.21.136.15 | 超載 | 1 | EBOOK電子書 |
| 163.21.136.16 | 163.21.136.16 - 163.21.136.16 | 超載 | 1 | IGT影片系統 |
| 163.21.136.17 | 163.21.136.17 - 163.21.136.17 | 超載 | 1 | VOD電影租借影片 |
| 163.21.136.19 | 163.21.136.19 - 163.21.136.19 | 超載 | 1 | SHDATA校會資料查詢主機 |
| 163.21.136.20 | 163.21.136.20 - 163.21.136.20 | 超載 | 1 | SERVER4網頁主機 |
| 163.21.136.22 | 163.21.136.22 - 163.21.136.22 | 超載 | 1 | PS列印伺服器 |
| 163.21.136.24 | 163.21.136.24 - 163.21.136.24 | 一對一 | 1 | 監視器主機 |

編輯動態IP Pool

IP Pool類型: IPv4 Pool IPv6 Pool

用戶名: 163.21.136.12

註解: APPLE MDM SERVER 16/255

類型: 超載 一對一 固定埠號範圍 埠號阻擋分配

外部 IP 範圍: 163.21.136.12 - 163.21.136.12

ARP回答:

確定 取消

虛擬 IP

NAT 轉換

The screenshot shows the FortiGate 200D web management interface. The browser address bar displays `https://172.23.0.254/index`. The interface title is "FortiGate 200D". On the left, a navigation menu is visible with "系統管理" (System Management) expanded to "路由設定" (Routing Settings), and "政策 & 物件" (Policy & Objects) selected. Under "物件" (Objects), "虛擬IP" (Virtual IP) is highlighted. The main content area is titled "編輯虛擬IP" (Edit Virtual IP) and contains the following configuration fields:

- VIP 類型: IPv4 VIP IPv6 VIP
- 用戶名: VIP-163.21.136.12 NAT 172.23.0.12
- 註解: APPLE MDM SERVER (16/255)
- 介面: 任何
- 類型: 靜態 NAT
- 過濾來源地址
- 外部 IP 地址/範圍: 163.21.136.12 - 163.21.136.12
- 對應IP地址/範圍: 172.23.0.12 - 172.23.0.12
- 埠號轉換

At the bottom right, there are "確定" (OK) and "取消" (Cancel) buttons.

OK! 就這些了!MDM 快樂使用中!