

防火牆安裝說明會

2016/06/29

南投教網 / Ming-Chang Cheng
everfree@ntct.edu.tw



硬體設備介紹-艾訊科技NA361R



- Intel Atom processor C2758
- (8-core) 2.4 GHz
- SoC Integrated
- 8G DDR3 RAM
- 120G SSD
- 6 x 10/100/1000Mbps Ethernet
- 1 x RS-232 (RJ-type)
- 1U rackmount
- 網路介面擴充模組

網段規劃

介面1：學術網路TANet

介面2：內部Public IP (163.22.x.x)

介面3：內部虛擬IP

介面4：內部虛擬IP

介面5：保留未啟用

介面6：備援線路（中華或中投，請先準備帳號密碼）

※舊L3交換器可Reset後重切網段或選擇不切，建議電腦教室獨立一個網段。



Floating Group TANET LAN NAT NAT2 WAN2 OpenVPN

Rules (Drag to Change Order)

| | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|-------------------------------------|-------------|-------------|----------------------------------|------|---------------|----------------|---------|-------|----------|------------------------|---------|
| <input checked="" type="checkbox"/> | 0/27 KiB | * | RFC 1918 networks | * | * | * | * | * | | Block private networks | |
| <input checked="" type="checkbox"/> | 0/104 KiB | * | Reserved Not assigned by IANA | * | * | * | * | * | | Block bogon networks | |
| 教網中心設定請勿更動 | | | | | | | | | | | |
| <input checked="" type="checkbox"/> | 0/37 KiB | IPv4+6 ICMP | * | * | This Firewall | * | * | none | | 允許Ping | |
| <input checked="" type="checkbox"/> | 5/30.36 MiB | IPv4 * | NTCT | * | * | * | * | none | | 教網中心 | |
| 對外開放的規則 | | | | | | | | | | | |
| <input type="checkbox"/> | 0/0 B | IPv4 * | TR | * | This Firewall | * | * | none | | 縣網研習教室 | |
| <input type="checkbox"/> | 0/0 B | IPv4 * | maint | * | This Firewall | * | * | none | | 維護廠商 | |
| <input type="checkbox"/> | 0/0 B | IPv4 * | * | * | Server | * | * | none | | 對外開放伺服器 | |
| <input checked="" type="checkbox"/> | 0/0 B | IPv4 UDP | * | * | * | 1194 (OpenVPN) | * | none | | OpenVPN | |

Add Add Delete Save Separator

留意事項

- 重要電腦建議學校設定固定IP
- 固定Public IP方便查詢問題
- 1:1 NAT與虛擬固定IP
- 不將縣網AP置於家用分享器下
- 備援線路
- 各校的資安風險報表於暑期後上線測試
- Appserv or Xampp、DOS、P2P、資安風險
- DNS Forwarder
- DNS Redirect
- DNSBL
- pfBlockerNG
- Suricata (偵測內部虛擬網段)
- Zabbix Agent
- OpenVPN
- ntopng (選用)

安裝之後

- 備份設定檔
- 確認各項服務是否正常啟動（Suricata看情況）
- 確認SSD啟用TRIM模式（重要）
- 修改學校管理者（sadmin）密碼
- 備援線路是否運作正常（現場測試）
- 新增對外開放的IP至Server別名（暫時開放）
- 避免修改不確定的選項與規則及安裝非縣網建議之套件
- 參加初階防火牆研習（半天）
- 使用在線式UPS防止雷擊（學校自購）

Questions?

