技術通報 050713001

一、主題：網路電話設備之設定與管理的安全機制

為避免 VoIP 設備(IP-PBX / GW)之設定資料被有心人士竊取，而遭到惡意導量下車、盜打，或無故撥入響鈴之惡作劇等情事，故建議可以從以下幾個方式來加強管理。

二、建議設定方式：

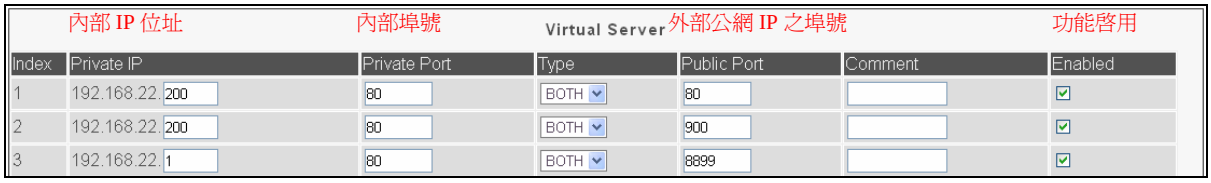
1. 務必修改設備之登入設定畫面的**帳號**與**密碼**(切勿使用常態性之設定值，並務必不定時進行修改)，以避免有心人士進到設備的設定畫面，進而修改設定值或進去竊取設定資料。設備登入帳密之參數修改, 參數設定位於" System / Administrator Setting "之設定畫面內。

2. 關閉設備的 Telnet 功能及更改其登入的帳密資料。參數設定位於" Application / Telnet & SNMP "之設定畫面內。

3. 將設備本身的通訊埠號改為非標準埠號，以避免被有心人士掃到而攻擊此設備之 IP 位址。
   i. SIP 的標準通訊埠號為 5060，將其改為其他非標準通訊埠號。
   ii. H.323 的標準通訊埠為 1719 與 1720(分別為註冊 GK 的通訊埠號與 H.323 點對點撥打的通訊埠號)，亦都改為其他非標準通訊埠號。

   參數設定位於" Advance Setup / Listen Port " 之設定畫面內(修改此處 SIP 的通訊埠號是與註冊系統的埠號無關，僅在做 IP 位址點對點撥打時會有關係)，修改後需重新開機方能生效。

4. 更改遠端連進設定畫面之連線埠號(預設埠號為 80 與 900，一般可用 http://設備 WAN IP 或 http://設備 WAN IP:900 連進設備的設定畫面)。修改範例：進到" NAT / Virtual Server " 之設定畫面內，然後將遠端連線進設定畫面的預設埠號，指向一個無設備的 IP 位址(如下圖之第 1~2 項設定)，然後再自行設定一個埠號指向設備正確的內部 IP 位址(如下圖第 3 項之設定), 若依下圖設定，遠端就要輸入" http://設備 WAN IP:8899 " 方能登入設定畫面。



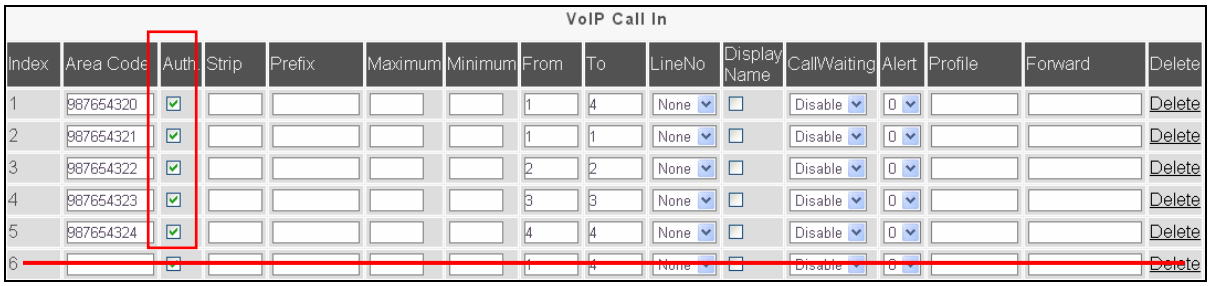
ps：從設備的 LAN 埠連進去則不受影響。

5. 將 NAT 功能關閉，以避免其他設備串接 LAN 埠上網(電腦接於設備 LAN 埠，仍可輸入帳密方式進到設定畫面)。參數設定位於" System / System Settings " 之設定畫面內，將 NAT 功能的 Enable 勾選取消掉。(注意：該功能與第 4 項功能不能同時使用)

6. 將 DHCP Server 功能關閉，即設備不配發 IP 位址給 LAN 埠所接之電腦或其他設備。參數設定位於" Lan / LAN Settings " 之設定畫面內，將 The Gateway acts as DHCP Server 功能的 Enable 勾選拿掉。

7. 撥入路由設定採用較爲嚴謹的設定規範

i. 於 Area Code 的參數設定值欄位內，填入僅允許的特定號碼可以撥入(如下範例)。



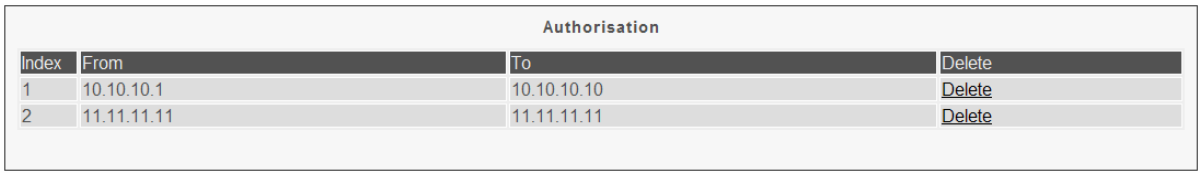
VoIP Call In

Index	Area Code	Auth	Strip	Prefix	Maximum	Minimum	From	To	LineNo	Display Name	CallWaiting	Alert	Profile	Forward	Delete
1	987654320	☑					1	4	None	☐	Disable	0			Delete
2	987654321	☑					1	1	None	☐	Disable	0			Delete
3	987654322	☑					2	2	None	☐	Disable	0			Delete
4	987654323	☑					3	3	None	☐	Disable	0			Delete
5	987654324	☑					4	4	None	☐	Disable	0			Delete
6		☑					1	4	None	☐	Disable	0			Delete

參數設定位於" Routing Setup / VoIP Call In " 之設定畫面內。

ps：建議不要設置上圖之第 6 項規則，因爲 Area Code 欄位若爲空白，即表示任意參數均可撥入，故建議不要建立此一進線規則。

ii. 勾選 **Auth.**功能(如上範例)，針對撥入來源做限制(白名單機制)，僅允許讓特定 IP 位址來源可以撥入。勾選該項功能，則設備僅會讓設備所註冊之系統平台的 IP 位址可以送號碼進來；若有特定之 IP 位址需做點對點方式指向過來，則功能勾選後，需配合到 Routing Setup / Authorization 頁面內，將允許撥入的 IP 位址設定進去(如下範例)。



Authorisation

Index	From	To	Delete
1	10.10.10.1	10.10.10.10	Delete
2	11.11.11.11	11.11.11.11	Delete

Ps：上圖範例規則 1，爲允許某一段 IP 範圍可撥入之設定；規則 2 爲允許某一單獨 IP 位址可撥入之設定；兩者可以混合使用。