Free RADIUS server 架設 – CentOS6 2017/3 編修

一、本範例以 CentOS6 為主來示範安裝 FreeRADIUS，其他 OS 請自行參考調整。

```
#yum install freeradius*
```

安裝後設定檔預設會放在 /etc/raddb 之下

二、修改設定檔

1. 修改 clients.conf

```
#vi /etc/raddb/clients.conf
```

1-1 Aruba 無線系統

在檔案最後加入允許查詢的教網中心 controller IP(設定前請與資網中心網路組連絡，確認 AP 使用之 controller IP，目前為 163.17.38.208、163.17.38.209、120.109.231.253、120.109.239.253 四台)

```
client 163.17.38.208 {
                secret = xxxxxx
        }
client 163.17.38.208 {
                secret = xxxxxx
        }
client 120.109.231.253 {
                secret= xxxxxx
          }
client 120.109.239.253 {
                secret= xxxxxx
          }
```

※secret=xxxxx 請自訂

1-2 Zyxel 無線系統

在檔案最後加入允許查詢的資網中心 Zyxel controller IP(設定前請與資網中心網路組連絡，確認 AP 使用之 controller IP，目前為 163.17.38.190

```
client 163.17.38.190 {
                secret = xxxxxx
        }
```

※secret=xxxxx 請自訂

2. 修改 proxy.conf
#vi /etc/raddb/proxy.conf
確認 DEFAULT 段內容為下

```
realm DEFAULT {
        type                = radius
        authhost            = LOCAL
        accthost            = LOCAL
}
```

3. 啟動 radiusd 並設為開機啟動
#service radiusd restart
#chkconfig radiusd on

三、本機防火牆及學校防火牆加入允許來源為教網中心 controller IP 查詢的規則
1. 本機：
#vi /etc/sysconfig/iptables
1-1 Aruba 無線系統
加入
-A INPUT -s 163.17.38.208 -p udp --dport 1812:1814 -j ACCEPT
-A INPUT -s 163.17.38.209 -p udp --dport 1812:1814 -j ACCEPT
-A INPUT -s 120.109.231.253 -p udp --dport 1812:1814 -j ACCEPT
-A INPUT -s 120.109.239.253 -p udp --dport 1812:1814 -j ACCEPT

重新啟動 iptables
#service iptables restart

1-2 Zyxel 無線系統
加入
-A INPUT -s 163.17.38.190 -p udp --dport 1812:1814 -j ACCEPT

重新啟動 iptables
#service iptables restart

2. 學校防火牆 下面以 FG200D 示範。

2-1 自訂學校架設之 radius server 位址

2-2 加入資網中心無線控制器 IP

※Aruba 無線系統請加入 資網中心目前 4 部 Aruba 無線控制器 IP

163.17.38.208

163.17.38.209

120.109.231.253

120.109.239.253

※Zyxel 無線系統請加入 資網中心目前 1 部 Zyxel 無線控制器 IP

163.17.38.190

2-2 外對內加入防火牆規則(請按照學校實際對外對內之介面設定)

四、加入允許之行動裝置 MAC Address

#vi /etc/raddb/users

請將收集到的 MAC Address 依下面格式加入 users 檔(英文字母要大寫)

00000000000A Auth-Type := Local, User-Password := "00000000000A"
00000000000B Auth-Type := Local, User-Password := "00000000000B"
00000000000C Auth-Type := Local, User-Password := "00000000000C"

修改內容後需重新啟動 radiusd

#service radiusd restart

五、測試

#radtest 00000000000A 00000000000A 127.0.0.1 0 testing123

Sending Access-Request of id 131 to 127.0.0.1 port 1812
User-Name = "00000000000A"
User-Password = "00000000000A"
NAS-IP-Address = 127.0.0.1
NAS-Port = 0
Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=131, length=20

有回應 Access-Accept 就是沒問題了。