漫遊連線機制建置說明手冊

OPENVPN & Freeradius

with UNIX

無線網路漫遊中心編製 | 107/05/16 版本 1.1

一、 OpenVPN

1. 安裝套件 epel-release、openvpn

```
[root@openvpn]# yum install -y epel-release
[root@openvpn]# yum install -y openvpn
```

2. 將漫遊中心提供的 key 「clt_number_name.tar」放置/etc/openvpn

```
[root@openvpn]# cd  /etc/openvpn
[root@openvpn]# tar -zxf clt_number_shortname.tar
```

3. 啟動服務

```
[root@openvpn]# service openvpn restart
```

4. 看 tun0 VPN 通道是否有啟動，如 tun0 有產生 10.1.X.X 代表 VPN 連線成功

```
[root@openvpn]# ifconfig tun0
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.1.X.X  netmask 255.255.255.255  destination 10.1.0.2
        inet6 fe80::ab85:e6d5:df58:63c9  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100
(UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3  bytes 144 (144.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

5. 設定開機啟動服務

```
[root@openvpn]# chkconfig openvpn on
```

二、 Freeradius

1. 安裝套件 freeradius freeradius-utils

```
[root@freeradius]# yum install -y freeradius freeradius-utils
```

2. 修改/etc/raddb 的 client.conf 檔案

```
[root@freeradius]# cd   /etc/raddb
[root@freeradius]# vim client.conf
            <--於檔案最後處加入下列內容-->
client 10.1.0.7 {
            secret          =   niucltcc
            shortname   =   niu
      }
client 10.1.0.11 {
             secret          =   niucltcc
             shortname   =   niu-roaming-monitor
}
```

3. 修改/etc/raddb 的 proxy.conf 檔案

```
[root@freeradius]# vim proxy.conf
            <--於檔案最後處加入下列內容-->
realm NULL {      #當遇到帳號並沒有 realm 時的預設動作為以本機進行認證動作
          authhost = LOCAL
          accthost = LOCAL
          secret = niucltcc
}
realm DEFAULT { #當遇到帳號帶有 realm 時的預設動作為送至漫遊中心進行 proxy 動作
          authhost = 10.1.0.7:1812
          accthost = 10.1.0.7:1813
          secret = niucltcc
          nostrip
}
```

4. 修改/etc/raddb 的 users 檔案

```
[root@freeradius ]#    vim /etc/raddb/users

DEFAULT Auth-Type := System       #預設 unix 帳號驗證
```

5. 修改/etc/raddb/sites-enabled 的 default 檔案

```
[root@freeradius]# vim /etc/raddb/sites-enabled/default

authenticate {
    ...略...
    unix          #取消註解
    ...略...
}
```

6. 啟動服務

```
[root@freeradius ]#service radiusd restart
```

7. 測試 Freeradius 驗證是否正常

```
[root@freeradius]# radtest    unix 帳號    unix 密碼    127.0.0.1    0    testing123

Sending Access-Request of id 234 to 10.1.0.7 port 1812
            User-Name = "testuser"
            User-Password = "testpass"
            NAS-IP-Address = 127.0.0.1
            NAS-Port = 0
rad_recv: Access-Accept packet from host 10.1.0.7 port 1812, id=234, length=20
```

8. 設定開機啟動服務

```
[root@freeradius ]#    chkconfig radiusd on
```

三、 EAP 設定

1. 設定/etc/raddb/的 radiusd.conf 檔案

```
[root@freeradius ]#    vim /etc/raddb/radiusd.conf

...略...
#user = radiusd
#group = radiusd
user = root
group = root
...略...
```

2. 設定/etc/raddb/的 eap.conf 檔案

```
[root@freeradius ]#    vim /etc/raddb/eap.conf

eap{
...略...
default_eap_type = peap
    gtc{
    ...略...
        auth_type = =pap
    ...略...
    }

    peap{
    ...略...
       default_eap_type = gtc
    ...略...
    }
}
```

3. 修改/etc/raddb/sites-enabled/inner-tunnl

```
[root@freeradius]# vim /etc/raddb/sites-enabled/inner-tunnel
authenticate {
    …略…
    Auth-Type{
    #   PAP         #註解 PAP
        unix        #新增 unix 驗證
    }
    …略…
}
```

4. 啟動服務

```
[root@freeradius ]#service radiusd restart
```

5. 測試使用 eapol_test 測試工具驗證是否正常[請參考漫遊網站資料]

```
[root@freeradius]#   eapol_test -c unix.conf -a 127.0.0.1 -s testing123
…略…
No EAP-Key-Name received from server
EAP: deinitialize previously used EAP method (21, TTLS) at EAP deinit
ENGINE: engine deinit
MPPE keys OK: 1   mismatch: 0
SUCCESS
```