漫遊連線機制建置說明手冊

OPENVPN & Freeradius

On CentOS6.8 for pop3

無線網路漫遊中心編製 | 107/01/22 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 clients.conf 檔案

```
[root@freeradius]# cd   /etc/raddb
[root@freeradius]# vim clients.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. 啟動服務

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

5. 測試 freeradius 驗證是否正常 XXXX@test.niu.edu.tw

```
[root@freeradius]# radtest   XXXX@test.niu.edu.tw   testpass   127.0.0.1   0   testing123
                    < radtest   帳號   密碼   測試伺服器   測試伺服器之通訊埠   Secret >
Sending Access-Request of id 234 to 10.1.0.7 port 1812
        User-Name = "XXXX@test.niu.edu.tw"
        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
```

6. 設定開機啟動服務

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

三、 Perl 模組

1. 事前準備，修改 selinux 將服務關閉

```
[root@radius]# vim /etc/sysconfig/selinux

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=disabled        #關閉 selinux 功能
```

2. 安裝 perl 相關模組

```
[root@radius]# yum install freeradius-perl perl perl-IO-Socket-SSL perl-Mail-IMAPClient -y
```

3. 新增/etc/raddb/mods-config/perl 並修改內容(請參考 exmple.pl 範例)

```
[root@radius]# vim /etc/raddb/mods-config/perl

use Mail::IMAPClient;
use Data::Dumper;

use constant      RLM_MODULE_REJECT=>      0;#    /* immediately reject the request */
use constant      RLM_MODULE_FAIL=>        1;#    /* module failed, don't reply */
use constant      RLM_MODULE_OK=>          2;#    /* the module is OK, continue */
use constant      RLM_MODULE_HANDLED=>     3;#    /* the module handled the request, so stop. */
use constant      RLM_MODULE_INVALID=>     4;#    /* the module considers the request invalid. */
use constant      RLM_MODULE_USERLOCK=>    5;#    /* reject the request (user is locked out) */
use constant      RLM_MODULE_NOTFOUND=>    6;#    /* user not found */
use constant      RLM_MODULE_NOOP=>        7;#    /* module succeeded without doing anything */
use constant      RLM_MODULE_UPDATED=>     8;#    /* OK (pairs modified) */
use constant      RLM_MODULE_NUMCODES=>    9;#    /* How many return codes there are *

sub authorize {
        return RLM_MODULE_OK;
}

sub authenticate {
    my $imap = Mail::IMAPClient->new(
        User        => $RAD_REQUEST{'User-Name'},
        Password => $RAD_REQUEST{'User-Password'},
        Server     => "imap.gmail.com",
        Port        => 993,
        Ssl         =>   1,
    ) or return RLM_MODULE_REJECT;

    if($imap->connect){
        return RLM_MODULE_OK;
        $imap->logout;
    }
}
```

4. 修改/etc/raddb/proxy.conf 新增 realm

```
[root@radius]# vim /etc/raddb/proxy.conf

realm XXX.edu.tw {
        type                    = radius
        authhost                = LOCAL
        accthost                = LOCAL
}
```

5. 修改/etc/raddb/sites- enabled/defaul

```
[root@radius]# vim /etc/raddb/sites- enabled]defaul

authorize {
…略…
    if (!control:Auth-Type && User-Password) {
        update control {
            Auth-Type := Perl
        }
    } #如果沒有認證屬性和密碼屬性使用 Perl 模組認證
…略…
}
authenticate {
…略…
    Auth-Type Perl { #新增 Auth-Perl 認證
        perl
    }
…略…
}
```

6. 設定開機啟動服務

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

7. 啟動服務

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

8. 測試 freeradius for pop3s 驗證是否正常

```
[root@freeradius]# radtest    testuser@XXX.mail.edu.tw    testpass    127.0.0.1    0    testing123
                    < radtest    帳號    密碼    測試伺服器    測試伺服器之通訊埠    Secret >
Sending Access-Request of id 234 to 10.1.0.7 port 1812
            User-Name = "testuser@XXX.mail.edu.tw"
            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
```

四、 EAP-GTC 驗證

1. 修改/etc/raddb/eap.conf

```
[root@freeradius ]#vim /etc/raddb/eap.conf
 ...略...
 gtc{
 ...略...
    auth_type = perl
 ...略...
 }

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

2. 修改/etc/raddb/sites-enabled/inner-tunnel

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

authenticate {
...略...
  Auth-Type Perl {
      perl
  }
...略...
}
```

3. Pop3 參考資料

   https://sam198214.blogspot.tw/2015/02/freeradius-gmail-pop3s.html

   http://blog.lhd.tw/2010/10/freeradius2-pop3-over-ssl.html