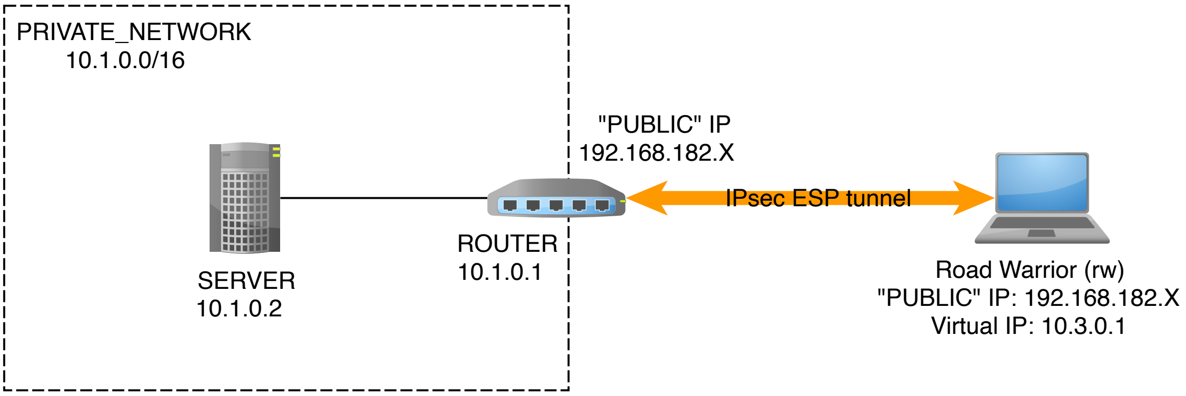
FreeRADIUS Server Setup Guide

Introduction

We will set up a RADIUS server instance using FreeRADIUS.



Initial Setup

First, use the ISP image to install all required software and then clone it two times:

```
sudo apt update
sudo apt install freeradius freeradius-utils apache2 libapache2-mod-auth-
radius wireshark
```

Note: During Wireshark installation when asked "Should non-superusers be able to capture packets?", select yes. If you make a mistake, you can change your selection by running:

```
sudo dpkg-reconfigure wireshark-common
```

Then add your user to the Wireshark group:

```
sudo usermod -a -G wireshark $USER
```

Virtual Machine Configuration

1. Power-off ISP machine
2. Configure single NIC:
   - Go to Machine > Settings > Network
   - Disable all Adapters except Adapter 1
   - Set to either Bridged or NAT network (do not use NAT)
3. Create two linked clones (remember to reinitialize MAC addresses):
   - radius1
   - radius2

Exercise 1: RADIUS Server with Test Client

Setting up RADIUS1

1. Start radius1
2. Configure the client in `/etc/freeradius/3.0/clients.conf`:

```
client localhost {
    ipaddr = 127.0.0.1
    secret = testing123
    require_message_authenticator = no
    nas_type = other
}
```

3. Add a new supplicant in `/etc/freeradius/3.0/users`:

```
"alice" Cleartext-Password := "password"
```

Starting the Server

1. Stop the default service:

```
sudo service freeradius stop
```

2. Start in debug mode:

```
sudo freeradius -X -d /etc/freeradius/3.0
```

Testing Authentication

Test the RADIUS server with:

```
echo "User-Name=alice, User-Password=password" | radclient 127.0.0.1 auth
testing123 -x
```

Exercise 2: HTTP Basic Authentication with Apache and FreeRADIUS

Apache Configuration

1. Enable RADIUS authentication module:

```
sudo a2enmod auth_radius
sudo service apache2 restart
```

2. Configure RADIUS settings in `/etc/apache2/ports.conf`:

```
# FreeRADIUS runs on localhost:1812 (standard RADIUS port)
AddRadiusAuth localhost:1812 testing123 5:3

# Authentication cookie expiration time (minutes)
AddRadiusCookieValid 1
```

3. Configure authentication requirements in `/etc/apache2/sites-available/000-default.conf`:

```
<Directory /var/www/html>
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
    AuthType Basic
    AuthName "RADIUS Authentication for my site"
    AuthBasicProvider radius
    Require valid-user
</Directory>
```

4. Reload Apache configuration:

```
sudo service apache2 reload
```

Testing

Test with browser: Navigate to `http://localhost`

Or using curl:

```
curl --user alice:password http://localhost -v
```

Exercise 3: Roaming and Federation

Setting up RADIUS1 (Proxy Server)

1. Configure `/etc/freeradius/3.0/proxy.conf`:

```
home_server hs_domain_com {
        type = auth+acct
        ipaddr = $RADIUS2
        port = 1812
        secret = testing123
}

home_server_pool pool_domain_com {
        type = fail-over
        home_server = hs_domain_com
}

realm domain.com {
        pool = pool_domain_com
        nostrip
}
```

Setting up RADIUS2 (Authentication Server)

1. Configure realm in `/etc/freeradius/3.0/proxy.conf`:

```
realm domain.com {
}
```

2. Add client configuration in `/etc/freeradius/3.0/clients.conf`:

```
client $RADIUS1 {
    secret = testing123
}
```

3. Add user in `/etc/freeradius/3.0/users`:

```
"bob" Cleartext-Password := "password"
```

Testing Roaming Setup

1. Start both RADIUS servers:

```
sudo freeradius -X -d /etc/freeradius/3.0
```

2. Test authentication:

```
curl --user bob@domain.com:password http://localhost -v
```

Questions

1. **Question 1**: Which AVPs are sent from Apache to RADIUS server when Alice tries to log in? (Use Wireshark with `radius` filter)
2. **Question 2**: What additional AVPs are added to the Access-Request message when the local RADIUS server proxies to RADIUS2?
3. **Question 3**: What would be needed to cover users from domain example.org on RADIUS2?

Optional Assignment: Authenticating IPsec Road Warriors with RADIUS

Prerequisites

- Complete previous IPsec road-warrior setup
- Install additional packages:

  ```
  sudo apt install strongswan freeradius freeradius-utils libcharon-extra-plugins
  ```

Configuration Steps

1. Set up router bridging private (10.1.0.0/16) and public networks

2. Install and configure FreeRADIUS on router

3. Configure road warrior authentication:

    - Use PSK instead of RSA certificates
    - Configure virtual IPs from 10.3.0.0/16
    - Configure StrongSwan-RADIUS connection

Debugging Tips

Run daemons in foreground mode:

```
sudo freeradius -Xd /etc/freeradius
sudo ipsec start --nofork
```