**赛肯内网raidus代理认证环境搭建指南**

赛肯（北京）科技有限公司

二〇一五年九月

目录

概述 3

一、安装前的准备 4

1、可用的内网服务器 4

2、域名解析的配置 4

3、secken提供的radius代理模块secken-freeradius-server-2-2-8 4

二、配置编译secken-freeradius-server-2-2-8 5

1、安装流程 5

2、配置freeradius 5

3、配置secken.conf 6

概述

本文为赛肯（北京）科技有限公司为企业提供的企业私有云产品内网系统环境（代理）搭建的指导文档，本文档旨在指导运维人员对其公司的内网环境进行修改，并使之嵌入赛肯公司的私有云产品模块，从而进行企业内网账号的二次验证，保障内网账号安全。

赛肯（北京）科技有限公司为企业提供的企业私有云产品内网系统的代理分为两部分：

1. ldap认证代理。
2. radius认证代理。

本文为radius认证代理环境搭建的指导文档。

本文旨在对不了解freeradius配置的管理员提供一份简单指导，若您已经足够了解freeradius的配置，请着重阅读“配置secken-freeradius-server-2-2-8”章节中的“配置secken.conf”一节。其他配置请根据自己需要进行。

本文适用人群：

1. 企业内部内网管理员。
2. 企业内部账号管理员。

*注：本文仅提供关于模块的最小可用代理配置，若想用关于freeradius的其他高级功能，请参照freeraidus的相关文档对其进行配置。本模块基于freeradius开发，完全遵循freeradius的编译及配置方法。*

# 一、安装前的准备

## 1、可用的内网服务器

请尽量为赛肯内网radius代理模块单独分配一台服务器（或虚拟机），若没有，也可准备一台已经使用但资源仍然足够的服务器。

## 2、域名解析的配置

请为赛肯内网radius代理模块所在的服务器分配一个内网的全局域名，供客户端寻找。

## 3、secken提供的radius代理模块secken-freeradius-server-2-2-8

暂无

# 二、配置编译secken-freeradius-server-2-2-8

## 1、安装流程

#### 进入secken-freeradius-server-2-2-8目录

#### 对secken-freeradius-server-2-2-8代码的编译进行configure

./configure --prefix=/usr/local/sicken-radius-proxy

#### 编译代码

make

##### 安装代码

make install

至此，模块已经安装到prefix配置指定的位置。

***注意事项：***

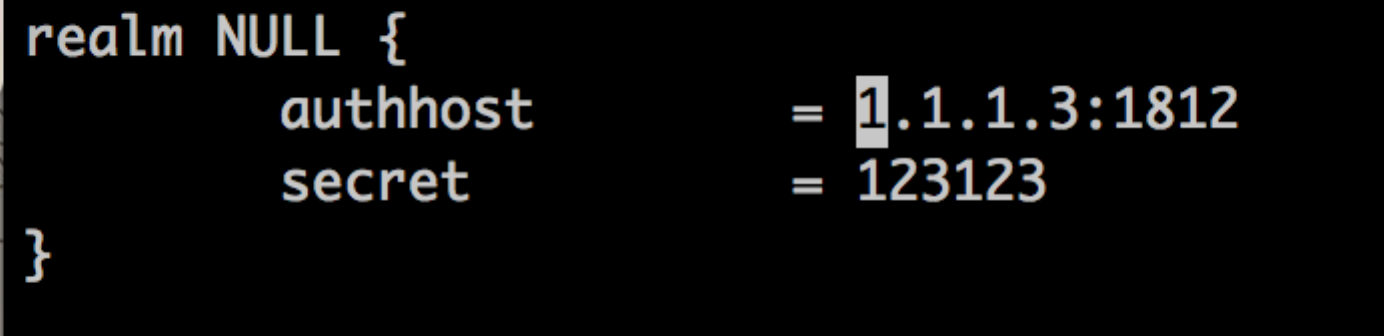
1. *请在--prefix字段里设置你所想要的安装路径*
2. *请在./configure之前安装openssl、mysql等依赖软件包*

## 2、配置freeradius

#### 配置proxy.conf

proxy.conf在安装目录下的相对位置为：etc/raddb/proxy.conf

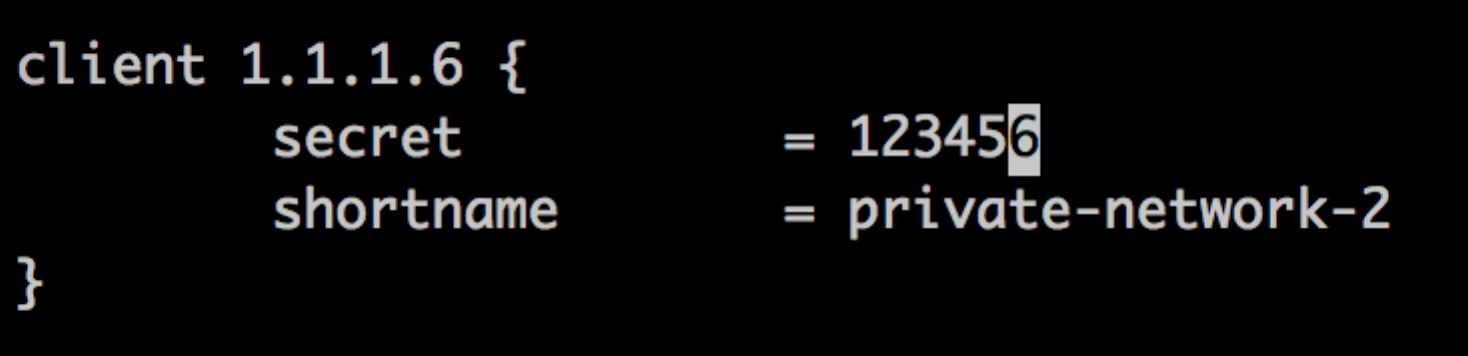
在proxy.conf中添加一个新的字段来表示代理目的地，secret字段为代理向认证服务器请求共享秘钥，请务必填写正确



#### 配置client.conf

proxy.conf在安装目录下的相对位置为：etc/raddb/client.conf

再client.conf最后添加一个字段来表示允许的客户端，secret字段为接入者需要填写的共享秘钥，该秘钥为客户端接入代理服务器的共享秘钥



*注：如果开启了openssl修改radiusd.conf中 allow\_vulnerable\_openssl = yes。*

## 3、配置secken.conf

secken.conf是代理模块与内网管理中心之间交互的配置文件，通过此文件的配置，可以打通代理模块与内网管理中心的二次认证通道。

secken.conf在安装目录下的相对位置为：etc/raddb/secken.conf

#### secken.conf字段解释



|  |  |
| --- | --- |
| timeout | Proxy向管理中心请求的超时时间，以秒为单位。  格式：数字 |
| result\_req\_interval | proxy向管理中心定时查询认证结果的时间间隔。  格式：数字 |
| auth\_req\_url | 认证请求接口，由管理中心中心进行配置并提供。  格式：rul |
| result\_req\_url | 认证结果请求接口，由中心进行配置并提供。  格式：url |
| power\_id | 权限ID，用来标识此proxy的认证权限，由管理中心进行配置并提供。  格式：字符串 |
| power\_key | 权限秘钥，用来标识此proxy唯一，由管理中心进行配置并提供。  格式：字符串 |
| accept\_cache\_enable | 认证状态缓存开启开关（注1）。  格式：字符串“yes”或“no” |
| accept\_cache\_time | 认证状态保存时间。  格式：数字 |
| accept\_cache\_retry | 认证状态保存时间内可重试次数。  格式：数字 |

注1：accept\_cache\_enable、accept\_cache\_time、accept\_cache\_retry此三个选项为认证状态缓存配置选项，认证状态缓存是为了防止客户端的认证请求超时时间过短，导致认证失败而产生的。若客户端超时时间较长，请将

认证状态保存时间（accept\_cache\_time）:

在客户端认证请求到达时，会有一条认证推送到用户的洋葱客户端上，如果用户确认过慢，会因本次认证超时而失败。但用户确认的状态会在代理中缓存一段时间，该段时间即为认证状态保存时间，当客户端自动重连或手动重连时，代理会认为本次重连的认证已完成洋葱的认证，只要用户名与密码正确，即可通过认证。从而避免客户端超时。

认证状态保存时间内可重传次数（accept\_cache\_retry）：

在认证状态保存时间内，用户最多可不通过洋葱进行认证的次数。此次数保证客户端可以顺利接入，但为了防止有人暴力破解，不建议设置的过多。

填写以上字段，完成配置

# 三、启动代理

运行日志文件的位置： 安装目录/var/log/radiusd/radiusd.log

代理可执行文件的位置： 安装目录/sbin/radius

1、在命令行./radiusd，程序会退回后台执行。（注意，radiusd在第一启动时会先生成ssl证书，可能导致第一次运行失败，此时请执行一次。）

2、重定向radius客户端的认证服务器位置，将服务器认证位置指向为代理的位置。

3、在内网管理中心添加账号，使内网用户名对应上洋葱账号。

4、让radius客户端进行认证操作，此时会有认证推送推送到手机终端进行认证，认证通过后radius客户端会收到认证成功的消息。

注意：

1. 本代理适合AP或AC向独立的radius服务器进行统一认证的场景。若为AC或AP的本地认证，请确保AP或AC可以进行认证服务器的重定向。
2. 为防止客户端超时影响用户体验，请在二次认证的认证方式上请尽量选择便捷的认证方式（例如按键确认）
3. radius最终认证的客户端很可能为手机/PC等终端设备，二次验证的过程可能会消耗一定时间，若可能，请尽量延长终端设备的认证超时时间。