

原创 凌晨两点钟同学 已于 2022-04-01 11:30:35 修改 8486 收藏 92

分类专栏: 积累

 积累 专栏收录该内容 0 订阅 66 篇文章 订阅专栏

目录

- 1 安装
- 2 配置
 - 2.1 CA证书
 - 2.2 Server证书
 - 2.3 客户端证书
 - 2.4 归档证书
- 3 配置
 - 3.1 配置服务端
 - 3.2 windows客户端配置

前言: openvpn不符合博客内容要求, 所以标题不对。

VPN直译就是虚拟专用 **通道**, 是提供给企业之间或者个人与公司之间**安全数据传输**的隧道, OpenVPN无疑是Linux下开源VPN的先锋, 提供了良好的性能和友好的用户 **GUI**。

1 安装

(1) 配置epel源

```
1 | mkdir /tmp/openvpn
2 | cd /tmp/openvpn
3 | wget https://repo.huaweicloud.com/epel/epel-release-latest-7.noarch.rpm
4 | rpm -ivh epel-release-latest-7.noarch.rpm
5 | yum update
```

(2) 安装依赖

```
yum install -y openssl lzo pam easy-rsa
```

```
[root@plm ~]# yum install -y openssl lzo pam
Loaded plugins: aliases, changelog, kabi, langpacks, product-id, subsc
: verify, versionlock
This system is not registered to Red Hat Subscription Management. You
to register.
Loading support for Red Hat kernel ABI
Reposdata is over 2 weeks old. Install yum-cron? Or run: yum makecache
hel-source
Package openssl-1.0.1e-42.el7.x86_64 already installed and latest ve
Package lzo-2.06-6.el7.0.2.x86_64 already installed and latest version
Package pam-1.1.8-12.el7.x86_64 already installed and latest version
Nothing to do
```

yum源安装openvpn

```
yum install openvpn
```

(3) 源码安装openvpn (可选)

```
1 | wget http://mirror.centos.org/centos/7/os/x86_64/Packages/lzo-2.06-8.el7.x86_64.rpm
2 | wget http://mirror.centos.org/centos/7/os/x86_64/Packages/lzo-devel-2.06-8.el7.x86_64.rpm
3 | wget http://mirror.centos.org/centos/7/os/x86_64/Packages/lzo-minilzo-2.06-8.el7.x86_64.rpm
4 | yum update lzo-2.06-8.el7.x86_64.rpm lzo-minilzo-2.06-8.el7.x86_64.rpm
5 | yum install lzo-devel-2.06-8.el7.x86_64.rpm
6 | yum install -y lzo-devel
7 |
8 | wget https://swupdate.openvpn.org/community/releases/openvpn-2.4.6.tar.gz
9 | tar -zxvf openvpn-2.4.6.tar.gz
10 | cd openvpn-2.4.6
11 | ./configure
12 | make
13 | make install
```

默认安装位置: /usr/local/sbin/openvpn

2 配置

2.1 CA证书

查看easy-rsa路径, 以3.0版本为例,

```
whereis easy-rsa
```

```
[root@plm openvpn]# whereis easy-rsa
easy-rsa: /usr/share/easy-rsa
```

```
1 | cd /usr/share/easy-rsa/3
2 | ./easyrsa init-pki
```

```
[root@plm 3]# ./easyrsa init-pki
init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /usr/share/easy-rsa/3/pki
```

```
./easyrsa build-ca
```

```
[root@plm 3]# ./easyrsa build-ca
Generating a 2048 bit RSA private key
++++
++++
writing new private key to '/usr/share/easy-rsa/3/pki/private/ca.key.H75yU
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:huawei

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/usr/share/easy-rsa/3/pki/ca.crt
```

目录

- 1 安装
- 2 配置
 - 2.1 CA证书
 - 2.2 Server证书
 - 2.3 客户端证书
 - 2.4 归档证书
- 3 配置
 - 3.1 配置服务端
 - 3.2 windows客户端配置

分类专栏

	消息队列	2 篇
	容器	6 篇
	视频开发	7 篇
	办公	2 篇
	工具类	10 篇
	minio	3 篇
	区块链	2 篇
	软件设计师	1 篇
	工业互联网	6 篇
	数字化转型	1 篇
	5G	5 篇
	flowable工作流	11 篇
	微服务	1 篇
	文件操作	2 篇
	CSDN	1 篇
	随笔	5 篇
	IDE	6 篇
	数据库	32 篇
	问题集	28 篇
	Maven	2 篇
	积累	66 篇

记住输入的密码 (pass phrase) , 后续签名需要使用。

2.2 Server证书

下面的\$EntityName就是给server取个名字, 注意前后统一就行, 比如都叫server。

```
1 cd /usr/share/easy-rsa/3
2 ./easyrsa gen-req $EntityName nopass
```

```
[root@plm 3]# ./easyrsa gen-req server nopass
Generating a 2048 bit RSA private key
+++
.....+++
Writing new private key to '/usr/share/easy-rsa/3/pki/private/server.key.1f3dvwqPNV'
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [server]:plm
Keypair and certificate request completed. Your files are:
req: /usr/share/easy-rsa/3/pki/reqs/server.req
ser: /usr/share/easy-rsa/3/pki/private/server.key
华为云社区
huaweicloud.com
```

签名证书

```
./easyrsa sign-req server $EntityName
```

```
[root@plm 3]# ./easyrsa sign-req server server
You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 3050 days:

subject=
  commonName = plm

Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
Using configuration from ./openssl-1.0.cnf
Enter pass phrase for /usr/share/easy-rsa/3/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName      : ASN.1 12: plm
Certificate is to be certified until Nov  5 07:08:43 2028 GMT (3050 days)

Write out database with 1 new entries
Data Base Updated
Certificate created at: /usr/share/easy-rsa/3/pki/issued/server.crt
华为云社区
huaweicloud.com
```

生成Diffie-Hellman

```
./easyrsa gen-dh
```

最终目录结构如下:

```
[root@plm 3]# tree ./pki/
./pki/
├── ca.crt
├── certs.by_serial
│   └── 0B483D24428F36820FAE38E46D722F83.pem
├── dh.pem
├── index.txt
├── index.txt.attr
├── index.txt.old
├── issued
│   └── server.crt
├── private
│   ├── ca.key
│   └── server.key
├── reqs
│   └── server.req
├── serial
└── serial.old
4 directories, 12 files
华为云社区
huaweicloud.com
```

2.3 客户端证书

另外创建一个目录用于存放client证书

```
1 mkdir -p /tmp/openssl/client1
2 cd /tmp/openssl/client1
3 /usr/share/easy-rsa/3/easyrsa init-pki
4 /usr/share/easy-rsa/3/easyrsa gen-req client1
```

```
[root@plm client01]# /usr/share/easy-rsa/3/easyrsa init-pki
init-pki complete: you may now create a CA or request.
Your newly created PKI dir is: /tmp/openssl/client01/pki

[root@plm client01]# /usr/share/easy-rsa/3/easyrsa gen-req client1
Generating a 2048 bit RSA private key
.....+++
.....+++
Writing new private key to '/tmp/openssl/client01/pki/private/client1.key.8da3UPzhlL'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [client1]:

Keypair and certificate request completed. Your files are:
req: /tmp/openssl/client01/pki/reqs/client1.req
ser: /tmp/openssl/client01/pki/private/client1.key
华为云社区
huaweicloud.com
```

记录输入的密码, client登录时使用

签名client证书:

```
1 cd /usr/share/easy-rsa/3/
2 ./easyrsa import-req /tmp/openssl/client1/pki/reqs/client1.req client1
```

```
[root@plm 3]# ./easyrsa import-req /tmp/openssl/client01/pki/reqs/client1.req client1
The request has been successfully imported with a short name of: client1
You may now use this name to perform signing operations on this request.
```

```
./easyrsa sign-req client client1
```

```
[root@plm 3]# ./easyrsa sign-req client client1
You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a client certificate for 3050 days:

subject=
  commonName = client1

Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
Using configuration from ./openssl-1.0.cnf
Enter pass phrase for /usr/share/easy-rsa/3/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName      : ASN.1 12: client1
Certificate is to be certified until Nov  5 07:39:48 2028 GMT (3050 days)

Write out database with 1 new entries
Data Base Updated
Certificate created at: /usr/share/easy-rsa/3/pki/issued/client1-2p6ghnd.com
华为云社区
huaweicloud.com
```

这里输入的制作CA证书时的密码。

客户端证书pki目录如下:

```
[root@plm client01]# tree pki/
```


然后将安装目录sample-config/client.ovpn拷贝到config目录下，

client.ovpn内容如下：

```
1 client
2 dev tun
3 proto tcp
4 remote 175.6.40.67 11094
5 resolv-retry infinite
6 nobind
7 persist-key
8 persist-tun
9 remote-cert-tls server
10 auth SHA512
11 cipher AES-256-CBC
12 #ignore-unknown-option block-outside-dns #注释该行，解决开启vpn不能外网的问题
13 #block-outside-dns #注释该行，解决开启vpn不能外网的问题
14 verb 3
15 route-nopull #解决开启vpn不能外网的问题
16 ca ca.crt
17 cert client1.crt
18 key client1.key
```

然后打开./bin/openvpn-gui.exe，输入制作client证书时输入的密码即可连接成功

给其它同事开通vpn权限：从2.3开始生成证书即可

这篇文章知识点与官方知识档案匹配，可进一步学习相关知识

CS入门技能树 > Linux入门 > 初识Linux 19043 人正在系统学习中



凌晨两点钟同学 关注



10



92



18



专栏目录

Openvpn搭建并使用用户名密码登录

dl_wdp的博客 1万+

Openvpn搭建并使用用户名密码登录 搭建前准备 Centos6.9操作系统 端口映射设备（路由器/防火墙） 一、服务端搭建过程 1、安装openvpn和证书生成...

Linux应用篇之openvpn2.4.10部署.docx

01-18

使用场景：本地电脑通过openvpn可以通过内网连接如阿里云、华为云等服务器；文档里面包含openvpn windows客户端安装包，此部署文档，真实有效...

评论 18条 >

写评论



微笑&星空 热评： 我有一个疑问望博主能解答下：疑问：服务端和客户端都配置好后，是不是只有安装了客户端的那台电脑能在外网访问到内网的服务端的那台服务器？其它外网没有安装客户端的电脑是不是就不能访问到内网的服务端的那台服务器？

open*** 搭建_包泽旭的博客

9-29

1.安装openvpn [root@openvpneasy-rsa]# yum install openvpn -y 2.配置openvpn [root@openvpn easy-rsa]# cd /etc/openvpn/ [root@web01 openvpn]...

安装OpenVPN 客户端_Rory602的博客_openvpn客户端

10-7

在/etc/openvpn/client/新建一个account.txt文件,在其中输入: username password 1 2 有些OpenVPN服务端工具只会生成密码(例如Pritunl),在这里userna...

linux下openvpn服务端搭建

都是曾经而已 6766

##openvpn yum install epel-release yum install -y openssl openssl-devel lzo lzo-devel pam pam-devel automake pkgconfig easy-rsa yum install -y op...

公司内网openvpn部署，

yang558855的博客 1万+

公司内网openvpn部署 准备环境 编号 服务器名称 网卡名称 网卡 定位 1号虚拟机 lan1 ens33 lan: 10.2.2.1 内网主机 2号虚拟机 lan2 ens33 lan: 10.2.2...

Centos7 使用docker搭建openvpn_随丶芯的博客_docker...

9-22

使用docker搭建openvpn 拉取openvpn镜像 docker pull kylemanna/openvpn:2.4 创建volume目录 mkdir -p /data/openvpn 生成配置文件 docker run -v /d...

【OpenVP*】Centos 部署OpenVP* 证书+多客户端+密码认证

恋上、小幸福的博客 641

一、实验环境 主机 内网IP 外网IP 系统 备注 OpenVPN 10.5.10.202 NAT映射外网访问 Centos7 OpenVPN服务端 PC1 10.5.10.122 内网用户 Windows7 x...

搭建vpn linux_vpn在linux下搭建

weixin_30995917的博客 9585

一：locate命令locate命令用于查找文件，它比find命令的搜索速度快，它需要一个数据库，这个数据库由每天的例行工作(crontab)程序来建立。当我们建...

Linux系统中openvpn客户端配置

mqqqq_1的博客 5909

安装openvpn 这里直接使用yum安装 yum -y install epel-release yum -y install openvpn 配置 安装完成之后，openvpn会创建目录/etc/openvpn 我们把服...

win10搭建openvpn以及使用 热门推荐

lmx1989219的专栏 3万+

2020注定是一个不平凡的年代，全国都沉浸在抗击冠状病毒的紧张生活中。本来七天的春节，硬生生的无限期延迟，高铁、航班、汽运等等暂停导致人...

Linux搭建vpn服务器

橙子博客 7573

Linux搭建vpn服务器

linux设置vpn客户端,centos下安装vpn客户端

weixin_35231383的博客 3120

1.安装所需软件 yum install ppp pptp pptp-setup2.复制命令到相应文件夹下cp/usr/share/doc/ppp-2.4.5/scripts/pon /usr/sbin/cp/usr/share/doc/ppp-2.4.5/...

OpenV安装

weixin_44656934的博客 2604

openvpn搭建: 基础环境: 服务端: CentOS 7.6 客户端: Windows 10 1、安装openvpn yum -y install openvpn easy-rsa 2、安装完成后，检查openvp...

openvpn部署

这是一个将要崛起小达人 1996

openvpn搭建大致步骤

openvpn-debian:不再开发

07-10

openvpn-debian Ubuntu 的 openvpn debian 包的分支，更新到最新的 openvpn 版本

六、SSL开源项目-Open虚拟私有网络 最新发布

小随奔的博客 766

OpenVPN是近年来新出现的开放源代码项目，实现了SSL VPN的一种解决方案。

openvpn部署和迁移

段帅星的博客 2214

wget https://git.io/vpn -O openvpn-install.sh && bash openvpn-install.sh server.conf local 192.168.0.163 port 1194 proto udp dev tun ca ca.crt cert ser...

网络搭建:

weixin_51788903的博客 55

网络搭建:

(原创)ics-openvpn编译详解

fy_8303的博客 1425

一、Windows环境下编译(仅适用于ics-openvpn_v0.7.3及以上版本) 1.下载、配置AndroidStudio: 浏览器访问https://developer.android.google.cn/studio/...

编译安装openvpn的问题与解决

cainia02013的博客 2477

1. 源码下载 问题: wget https://gitlab.com/openvpn/openvpn/-/archive/v2.4.11/openvpn-v2.4.11.tar.gz 没有configure文件 解决: wget https://swupdate.o...

“相关推荐”对你有帮助？



非常有帮助



有帮助



一般



没帮助



非常没帮助

©2022 CSDN 皮肤主题: 精致技术 设计师: CSDN官方博客 返回首页

关于我们 招贤纳士 商务合作 寻求报道 400-660-0108 kefu@csdn.net 在线客服 工作时间 8:30-22:00

公安备案号11010502030143 京ICP备19004658号 京网文〔2020〕1039-165号 经营性网站备案信息 北京互联网违法和不良信息举报中心 家长监护 网络110报警服务 中国互联网举报中心 Chrome商店下载 账号管理 规范 版权与免责声明 版权申诉 出版物许可证 营业执照 ©1999-2022北京创新乐知网络技术有限公司

Beta

Beta

举报

