n2n内网穿透打洞部署全过程 + nginx公网端口映射

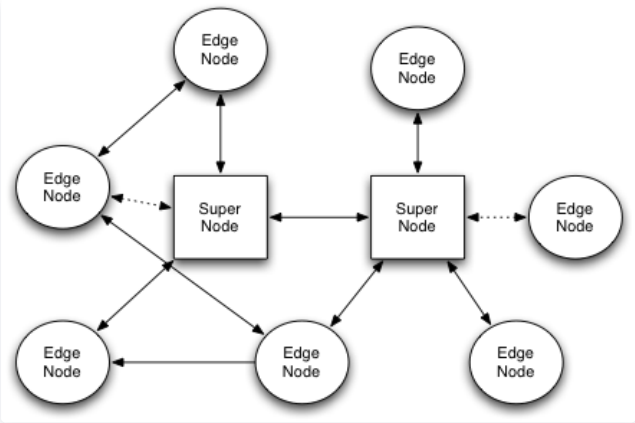
作者 野路子程序员

2018-05-11 阅读 9.5K

内网穿透、打洞工具有很多，此前在windows上使用的是vidcc这个玩意，也正因为linux不支持。自此在linux尝试过一些打洞工具，ssh 反向代理这些，因为安全性不便捷等多种原因，最终选择了n2n。

由于初次接触n2n，对其不是很了解，就此对n2n实现内网穿透打洞过程进行基本表述。

2008年，ntop的作者Luca Deri开始研究p2p V**，他一方面看到公众对p2p V**有着强烈的需求，另一方面又不满足已有产品的现状，于是n2n诞生了。



如上图所示，n2n是一个二层架构的V**网络，其中super node提供场所，让两个位于NAT/防火墙之后的edge node进行会面，一旦双方完成首次握手，剩下的数据流就之发生在两个edge node之间，如果有一方的NAT属于对称型(symmetrical)，super node则还需继续为双方提供数据包的转发;edge node负责数据流的加解密，原理很简单。

至此，我们已经了解，部署n2n至少需要两台以上的机器。

我们此文采用两台centos。

centos7（super node） - 150.0.0.1 （公网IP）

centos 7（edge node）- 192.168.1.121 （虚拟机内网IP）

使用n2n产生的虚拟网段，将为 10.0.0.1 ~ 10.0.0.255

目录

无论是edgenode还是supernode 都需要安装n2n，所以下面安装方法通用，提供两种n2n资源，均可。

```
git clone https://github.com/meyerd/n2n.git
```

or

```
svn co https://svn.ntop.org/svn/ntop/trunk/n2n
```

n2n分为v1和v2版本，两种协议互不兼容。我们选择v2版本。

```
cd n2n/n2n_v2
```

安装openssl、cmake、git、gcc、net-

```
yum install -y openssl-devel
yum install -y cmake
yum install -y net-tools
yum install -y git
yum install -y gcc gcc-c++
```

编译安装n2n

```
mkdir build
cd build
cmake ..
make && make install
```

n2n编译安装完，会产生两个程序指令，edge 和 supernode，欠着是边缘节点使用（客户端），后者则是超级节点使用（服务端）。

supernode（服务端运行）

```
supernode -l 5000
```

超级节点开启5000端口进行监听，以此来提供建交服务。

服务端也可以同时当做客户端使用，将服务端加入到虚拟网络中。

```
edge -a 10.0.0.10 -c edge0 -k wss -l 150.0.0.1:5000
```

目录

```
edge -a 10.0.0.11 -c edge0 -k wss -l 150.0.0.1:5000
```

10.0.0.11 这个IP是虚拟网段，其他加入虚拟网络中的IP地址需要在同一网段，统一key，即wss（可设置为其他）。

```
[root@localhost ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:ed:d4:75 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.121/24 brd 192.168.1.255 scope global ens33
       valid_lft forever preferred_lft forever
14: edge0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1200 qdisc pfifo_fast state UNKNOWN qle
n 1000
    link/ether 42:a2:b0:b6:7a:60 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.11/24 brd 10.0.0.255 scope global edge0
       valid_lft forever preferred_lft forever
[root@localhost ~]#
```

此节点已有10.0.0.11这个IP，所在的是n2n创建的虚拟网卡，kill 掉edge 进程则此网卡销毁。

查看edge或者supernode 进程

```
ps -ef|grep supernode
```

```
ps -ef|grep edge
```

--help

```
[root@localhost ~]# edge --help
Welcome to n2n v.2.1.0 for Linux-3.10.0-514.el7.x86_64
Built on Jul 29 2017 17:07:28
Copyright 2007-09 - http://www.ntop.org

edge -d <tun device> -a [static:|dhcp:]<tun IP address> -c <community> [-k <encrypt key>
 | -K <key file>] [-s <netmask>] [-u <uid> -g <gid>][-f][-m <MAC address>]
-l <supernode host:port> [-p <local port>] [-M <mtu>] [-r] [-E] [-v] [-t <mgmt port>] [-
b] [-h]

-d <tun device>          | tun device name
-a <mode:address>        | Set interface address. For DHCP use '-r -a dhcp:0.0.0.0'
-c <community>           | n2n community name the edge belongs to.
-k <encrypt key>         | Encryption key (ASCII) - also N2N_KEY=<encrypt key>. Not with
 -K.
-K <key file>            | Specify a key schedule file to load. Not with -k.
-s <netmask>             | Edge interface netmask in dotted decimal notation (255.255.25
5.0).
-l <supernode host:port> | Supernode IP:port
-L <local_ip>            | Add local ip to bypass between same nat problem
-i <interval>            | Set the NAT hole-punch interval (default 20seconds)
-b                       | Periodically resolve supernode IP
                         : (when supernodes are running on dynamic IPs)
-p <local port>          | Fixed local UDP port.
-u <UID>                 | User ID (numeric) to use when privileges are dropped.
-g <GID>                 | Group ID (numeric) to use when privileges are dropped.
-f                       | Do not fork and run as a daemon; rather run in foreground.
-m <MAC address>         | Fix MAC address for the TAP interface (otherwise it may be ra
ndom)
                         : eg. -m 01:02:03:04:05:06
-M <mtu>                 | Specify n2n MTU of edge interface (default 1400).
-r                       | Enable packet forwarding through n2n community.
-E                       | Accept multicast MAC addresses (default=drop).
-v                       | Make more verbose. Repeat as required.
-t                       | Management UDP Port (for multiple edges on a machine).

Environment variables:
  N2N_KEY                | Encryption key (ASCII). Not with -K or -k.
```

目录

-k wss 通讯私匙，一般不用放在supernode节点，可自行约定edge节点的私匙统一设置。

-M 1200 设置mtu

-v -f 开启调试输出

调试

使用过程中不免遇到一些奇葩的事，调试是个关键，一些大的坑已经为你们踩过了，剩下的基本没啥问题。

1.开启调试模式

记住先kill掉之前的edge 或 supernode进程再进行调试以免冲突。

附加参数即可： -v -f

edge

```
edge -a 10.0.0.11 -c edge0 -k wss -l 150.0.0.1:5000 -v -f
```

supernode

```
supernode -l 5000 -v -f
```

2.正常使用，节点互相连接不通。

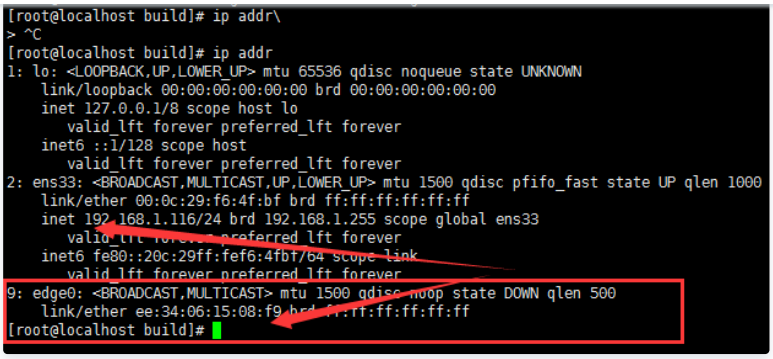
如果ping都不通，怀疑是防火墙的问题？测试请先直接关闭防火墙。完毕后，将其恢复，慢慢测试。

防火墙放行端口示例：

```
iptables -I INPUT -p tcp --dport 5000 -j ACCEPT
iptables -I INPUT -p udp --dport 5000 -j ACCEPT
iptables save
service iptables restart
```

2.创建了客户端，虚拟网卡没有ip

目录



如果你开启调试模式了，可能就会看到原来是ifconfig 命令不存在，这个命令在net-tools包里（centos），那么就需要安装，重新开启edge即可解决。

安装net-tools

```
yum install -y net-tools
```

手动设置网卡IP（可省略，测试可以使用）

```
ifconfig edge0 10.0.0.11  netmask 255.255.255.0
```

那么，如果这步不成功的话，自然网络没有配置建立好，也就无法正常穿透内网。此时如果不开启调试模式，你也看不到任何错误，也就是很多人往往出现的配置好了，却无法正常访问，ping都不通，何以解忧。

3.ping能通，http和ssh却不通。

设置mtu值即可

```
edge -a 10.0.0.11 -c edge0 -k wss -l 150.0.0.1:5000 -M 1200
```

一般低于1400即可，当前设置1200。（不要忘了kill之前的进程哦）

至此，问题基本得以解决。

测试

10.0.0.10 (supernode、edge) 10不仅是超级节点也是边缘节点。

10.0.0.11（edge）无数边缘节点中其中一个

10 ping 11

目录

```
64 bytes from 10.0.0.11: icmp_seq=1 ttl=64 time=41.0 ms
64 bytes from 10.0.0.11: icmp_seq=2 ttl=64 time=41.1 ms
64 bytes from 10.0.0.11: icmp_seq=3 ttl=64 time=56.3 ms
^C
--- 10.0.0.11 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3004ms
```


11 ping 10

```
[root@localhost ~]# ping 10.0.0.10
PING 10.0.0.10 (10.0.0.10) 56(84) bytes of data.
64 bytes from 10.0.0.10: icmp_seq=1 ttl=64 time=43.5 ms
64 bytes from 10.0.0.10: icmp_seq=2 ttl=64 time=45.0 ms
64 bytes from 10.0.0.10: icmp_seq=3 ttl=64 time=41.4 ms
64 bytes from 10.0.0.10: icmp_seq=4 ttl=64 time=42.0 ms
^C
--- 10.0.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
```

自此，网络可以互相访问，畅通无阻。如果你用你自己的电脑，需要将其加入到虚拟网络中，即可像局域网一样访问。

windows edge客户端软件

http://www.V**hosting.cz/n2nguien.exe

http://sourceforge.net/projects/n2nedgegui/

还要其他版本以及安卓版本，自行搜捕。

nginx转发端口代理映射

最后，我们将用nginx转发下公网IP端口到内网指定ip指定端口，这样可以让外界不加入虚拟网络即可访问其中的节点机器。

用户客户端 =》 公网IP（150.0.0.1:6011）=》虚拟内网（10.0.0.11:22）

从流程来看，我们的用户将访问公网IP的6011端口，可以连接到内网机器10.0.0.11的22端口（ssh）。

首先关闭防火墙或放行公网6011端口连接

```
vi /etc/sysconfig/iptables
```

增加

-A INPUT -p tcp -m state --state NEW -m tcp --dport 6011 -j ACCEPT

安装nginx（supernode）

目录

注意需要转发tcp数据，编译时附加参数：--with-stream

```
#安装编译支持库
mkdir /mnt/tools -p
cd /mnt/tools
yum -y install gcc automake autoconf libtool make
yum install gcc gcc-c++

#安装PCRE
wget ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/pcre-8.40
tar -xzf pcre-8.40.tar.gz -C ./
cd pcre-8.40
./configure --prefix=/usr/local/pcre
make && make install
cd ..

#安装zlib
wget http://zlib.net/zlib-1.2.11.tar.gz
tar -xzf zlib-1.2.11.tar.gz -C ./
cd zlib-1.2.11
./configure --prefix=/usr/local/zlib
make && make install
cd ..

#安装openss
wget https://www.openssl.org/source/openssl-1.0.2k.tar.gz
tar -xzf openssl-1.0.2k.tar.gz -C ./
#注意，这里不需要进行安装，后面步骤省略。

#编译安装nginx
wget http://nginx.org/download/nginx-1.12.0.tar.gz
tar -xzf nginx-1.12.0.tar.gz  -C ./
cd nginx-1.12.0

./configure \
--prefix=/usr/local/nginx \
--sbin-path=/usr/local/nginx/nginx \
--conf-path=/usr/local/nginx/nginx.conf \
--pid-path=/usr/local/nginx/nginx.pid \
--with-http_ssl_module \
--with-pcre=/mnt/tools/pcre-8.40/ \
--with-zlib=/mnt/tools/zlib-1.2.11/ \
--with-openssl=/mnt/tools/openssl-1.0.2k/ \
--with-stream


#注：cpre、zlib、openssl等依赖包的路径是解压的源码路径不是安装后的路径。

make
make install
```

编译安装完毕后，到nginx目录。

```
cd /usr/local/nginx/
```

编辑配置nginx.conf

目录

```
stream {

    log_format proxy '$remote_addr [$time_local] '
                '$protocol $status $bytes_sent $bytes_received '
                '$session_time "$upstream_addr" '
                '"$upstream_bytes_sent" "$upstream_bytes_received"';

    access_log /var/log/nginx/tcp-access.log proxy ;
    open_log_file_cache off;
    include /usr/local/nginx/conf.d/*.stream;
}
```

创建日志目录

```
mkdir /var/log/nginx/
```

创建模块配置目录并进入

```
mkdir /usr/local/nginx/conf.d/
cd /usr/local/nginx/conf.d/
```

新建tcp.stream文件（vi tcp.stream）

```
upstream TCP6011 {
        hash $remote_addr consistent;
        server 10.0.0.11:22;
    }
        server {
        listen 6011;
        proxy_connect_timeout 5s;
        proxy_timeout 300s;
        proxy_pass TCP6011;
    }
```

重载nginx

cd ..

./nginx -s reload

使用putty连接 150.0.0.1:6011 成功连接10.0.0.11

因为是nginx代理请求，所以来源是10.0.0.10而不是直接客户端。所以流量也会全部走supernode服务器而不直接交互。如果本地也配置到虚拟网络，即建立连接通过supernode，之后则直接互通。

目录

http://www.ntop.org/n2n/

https://sourceforge.net/projects/ntop/files/n2n/

https://www.buckhill.co.uk/blog/how-to-enable-broadcast-and-multicast-support-on-amazon-aws-ec2/2

（完）

Nginx Windows Linux ssh

目录

相关文章

Thinkphp修改一句代码，使得foreach标签支持对象，增加变量[…

Eller

通过DNS2SOCKS建立本地稳定无污染DNS

这是一个通过socks5，从指定DNS上流获取最新的DNS解析记录，从而实现一个无污染的纯净DNS服务器。

Eller

最近写了一个博客程序： QuickBlog PHP 开…

在开始之前也用到了一些其他类似的系统，区别大概就是非开源的商业化产品不安全，无法进行自我数据存储管理。…

Eller

dedecms前端无法调用自定义变量怎么解决

网友问ytkah说他的dedecms前端无法调用自定义变量要怎么解决，登录他的网站后台看了一下，自定义变量已经…

[OpenSSL] 微信支付证书pfx分解成pem

事件起因：做香港本地微信支付（香港公司收取香港用户钱包）申请的商户只提供了cert.pem和一个pfx的文件。程序使用pem需要cert和key两个文件，所以需...

宣言言言

借Blake老师的投篮小游戏公开课入门Cocos Creator 3D开发！

● 点击屏幕，根据按住屏幕的时间，进行蓄力，时间越短，发出去的力越小，时间越长，发出去的力越大，超过了最大力，再次从最小里开始，球从篮筐中穿过得1分，…

一枚小工

iOS报错记录：dyld: could not load inserted l…

edit scheme —>run debug —>在Memory Management区域
将Eanble Guard Malloc设置为不选中

陈满iOS

Python 3版本较之前版本语法的一些

市面上的Python教程基本都是以3.0以下版本来讲解的，python 从3.0之后一些语法都做了写更改，有时候可能会浪费比较多的时间，记录下使用过程中遇到的情...

用户2398817

005互联网网络技术之国内外DNS服务器地址列表

DNS（Domain Name System）是域名解析服务器的意思，它在互联网的作用是把域名转换成为网络可以识别的IP地址。　　通常来说，香港、韩国、日本...

上善若水.夏

【生活】职场保健 给心灵减压的一些方法

随着社会的不断发展，很多人整天活在职场中，身在职场，
时间久了，就会有些压力堆积在体内。压力的发生严重影…

小莹莹

更多文章

目录

目录