3 企业VPN方案

3.1 VPN网络规划

3.1.1 网络节点

VPN的基本原理是网络层IP隧道，因此需要一个中心代理节点。在i-mec VPN中，该中心为阿里云ECS服务器（IP：47.101.188.30），又称为VPN服务器（vpnserver）。其他众多加入VPN网络的节点，通常是建筑节能系统中的业务服务器和网关设备等，统称为VPN客户端。现假设存在两个VPN客户端，分别名为mulan和zwliao，以此为基本场景进行方案阐述。

3.1.2 网络地址 IP

i-mec VPN使用10...*/8私有IP地址段；其中VPN服务器节点vpnserver设定IP地址为10.0.0.1/255.255.255.0，VPN客户段节点mulan和zwliao加入VPN网络过程后，由vpnserver分配预定IP地址，分别为10.1.0.1/255.255.255.0和10.2.0.1/255.255.255.0。即：

```
例子场景，共分为三个subnet 1 2 3:
vpnserver: 10.0.0.1/255.255.255.0  subnet 1
mulan: 10.1.0.1/255.255.255.0 subnet 2
zwliao: 10.2.0.1/255.255.255.0 subnet 3
```

其他业务节点，按实际需求选择加入具体子网subnet 2 或 3，或者创建一个新的子网，如10.3.0.1/255.255.255.0 subnet 4。

3.1.3 安全通信

i-mec VPN确保上述VPN子网中（以及后续更多子网）中节点之间的两两双向安全通信，即保证通信信息可达，和保护信息的机密性和完整性。安全通信，蕴含对加入VPN网络节点进行安全认证，只有合法节点才允许加入。 服务端vpnserver作为中心节点，负责对新加入节点的身份验证，并与之建立安全信道，后续在节点之间（如mulan与zwliao）进行信息的转发（网络层隧道代理）。

3.2 利用OpenVPN构建i-mec VPN

i-mec利用OpenVPN技术来构建企业VPN网络。OpenVPN版本：2.4.* 。VPN网络所需的中心代理节点，采用阿里云ECS服务器，公网IP：47.104.188.30。下文以例子说明详细说明建设方案。

3.2.1 PKI与数字证书

OpenVPN利用SSL/TLS技术来构建VPN网络所需的安全信道，因此先构造支撑VPN网络的PKI系统。见PKI与数字证书。下文假设存在如下PKI要素：

```
OpenVPN 服务端:
CA公钥: ca.crt
VPN服务端公钥证书: server.crt
VPN服务端私钥证书: server.key
DH安全参数: DH2048.pem
crl证书撤销列表: crl20180320.pem
```

```
OpenVPN 客户端 mulan:
CA公钥：ca.crt
VPN客户端公钥证书：mulan.crt
VPN客户端私钥证书：mulan.key

OpenVPN 客户端 zwliao:
CA公钥：ca.crt
VPN客户端公钥证书：zwliao.crt
VPN客户端私钥证书：zwliao.key

OpenVPN 客户端 revoke:
CA公钥：ca.crt
VPN客户端公钥证书：revoke.crt
VPN客户端私钥证书：revoke.key
```

3.2.2 虚拟网卡TUN/TAP与路由（核心原理）

在服务器端安装OpenVPN服务端程序，在客户计算机安装OpenVPN客户端程序，都会在安装主机上生成虚拟网卡TUN/TAP。VPN网络可看做主机间虚拟网卡互联形成的网络。假设VPN网络中，只用私有IP地址段：10.0.0.0/8。

VPN客户端路由：10.0.0.0 255.0.0.0 -->TUN/TAP
客户端主机在加入VPN网络之前，其自身的物理网卡已经配置了一个主机IP地址。假设该主机处于一个私有局域网，不失一般性，假设它的局域网IP为192.168.0.2。通过OpenVPN加入企业VPN后，该主机的虚拟网络TUN/TAP将被分配一个VPN网络IP：10.1.0.1，并向操作系统注册vpnserver的公网IP地址：47.104.188.30。当主机有消息要发送时，如果目标主机是非VPN网络IP，操作系统按传统处理（原生网络协议栈）。但是，如果目标主机是采用VPN网络IP，操作系统先将该消息利用TUN/TA协议栈处理，然后再交付原生网络协议栈。在TUN/TA协议栈栈（IP层），生成VPN IP数据包（源IP：10.1.0.1，目的IP：10.0.0.1），然后将该数据包交付的原始网络协议栈（IP层），生成原生网络IP数据包（源地址：192.168.0.2，目的IP：47.104.188.30）。

VPN服务端路由：10.1.0.0 255.255.255.0 --> TUN/TAP（针对subnet 2的路由规则）
（假设）vpnserver在VPN网络中的网络参数为：10.0.0.1 255.255.255.0。增加其他子网情况，需要配置新的路由规则。比如增加新子网：10.2.0.0 255.255.255.0。

3.2.3 配置OpenVPN服务端

OpenVPN服务端对整个VPN网络的关键，所有配置均在/etc/openvpn/server.conf中。核心配置包括1）SSL/TLS安全参数，2）VPN子网划分与路由配置，3）客户节点IP指派，和4）通信相关其他。下面对i-mec VPN的配置进行详细说明：

```
port 1194 # 通信端口，默认为1194 （阿里云添加入口规则）
proto udp # 采用udp协议
dev tun # OpenVPN程序安装后，生成一个tun类型虚拟网卡（即隧道）；
        # 在路由规则上，发往VPN网络地址的数据包需要发向tun隧道。

ca ca.crt # CA根公钥证书
cert server.crt # OpenVPN服务端公钥证书
key server.key  # OpenVPN服务端私钥证书
crl-verify crl20180320.pem # 当前最新证书撤销列表（当前包含对revoke.crt）
dh dh2048.pem # SSL/TLS握手过程所需的DH参数

server 10.0.0.0 255.255.255.0 # 给vpnserver划分一个子网，其中vpnserver的ip为 10.0.0.1
```

```
ifconfig-pool-persist ipp.txt # 持久各个vpn客户端当前分配的ip
push "route 10.0.0.0 255.0.0.0" # 向所有vpn客户端发送该路由规则
client-config-dir ccd # 新加入的客户端节点按ccd中对应文件中的规则进行ip分配;
                      # 客户端使用数据证书作为入网凭证，证书的CN字段作为标识符，如mulan;
                      # 用于查找ccd文件夹中是否存在mulan的文件，并从中获取IP配置给客户端
# route 10.0.0.0 255.255.255.0 # 客户端节点不使用vpnserver所处在子网
route 10.1.0.0 255.255.255.0 # 服务器端路由配置，比如发往10.1.0.1/24的消息交给TUN/TAP处理
route 10.2.0.0 255.255.255.0 #
route 10.3.0.0 255.255.255.0 #
client-to-client # 允许不通子网客户端相互通信，vpn作为代理

# duplicate-cn #
keepalive 10 120 #
cipher AES-256-CBC # 对称加密算法
compress lz4-v2 # 压缩函数，2.4版本 or 以上
push "compress lz4-v2" # 推送给加入的客户端节点
user nobody #
group nobody #
persist-key #
persist-tun #
status openvpn-status.log #
log-append  openvpn.log #
verb 4 #
explicit-exit-notify 1 #

tun-mtu 1500 #
fragment 1500 #
```

3.2.4 配置OpenVPN客户端

不管宿主操作系统是windows还是linux（如centos 7），具有OpenVPN客户端程序。这些VPN客户端程序根据ovpn配置文件来加入VPN网络。下文说明配置文件：

```
client # 声明本程序属于客户端
dev TUN # 使用TUN模式
proto udp # 使用udp协议
resolv-retry infinite # 不断重试vpnserver的域名
nobind # 客户端程序使用随机端口
persist-key # 保持允许状态，重启时更快
persist-tun
ca ca.crt # CA公钥证书
cert mulan.crt # 本客户端使用的入网凭证，该证书的CN属性为mulan
key mulan.key # 对应的私钥
remote-cert-tls server # 入网时进行SSL/TLS过程，客户端认证服务器证书
cipher AES-256-CBC # 使用与vpnserver一样的对称加密算法
verb 3
```

3.2.5 网络安全

在节点mulan向vpnserver发起加入vpn网络过程中，vpnserver将基于mulan节点提供的公钥证书mulan.crt作为其身份凭证，同时，mulan节点也将验证vpnserver的证书server.crt。对证书的验证，主要涉及1）是否是CA签发的证书，2）是否在有效期内，和3）客户端证书是否已经被撤销。如果证书验证通过，mulan节点被允许加入vpn网络，并与vpnserver之间基于数字证书建立SSL/TLS安全信道，同时mulan节点被分配一个可用IP。

i-mec VPN采用预定客户端节点IP分配方案，即对mulan客户端节点（使用mulan.crt，且证书的CN属性为mulan），通过vpnserver服务器中 ccd/mulan 配置文件中的设置制定IP：

```
ccd/mulan:
ifconfig-push 10.1.0.1 10.1.0.2  # mulan节点对应的IP地址为 10.1.0.1

ccd/zwliao:
ifconfig-push 10.2.0.1 10.2.0.2  # zwliao节点对应的IP地址为 10.2.0.1

ccd/revoke:
ifconfig-push 10.3.0.1 10.3.0.2  # revoke节点对应的IP地址为 10.3.0.1
```

在示例配置中，节点mula和zwliao均被认证通过成功加入vpn网络，但是revoke节点因为其公钥证书被撤销，无法通过认证，不能成功加入vpn网络。

3.3 网络连通测试

在客户端mulan和zwliao均成功加入VPN网络后，他们将被分配由vpnserver制定的IP；在示例配置下，mulan节点的IP为10.1.0.1/24，和zwliao节点的IP为10.2.0.1/24。

为保证后续业务进行，应该测试三个子网中节点的连通性。例如，从mulan节点测试其与zwliao节点的连通性：

```
在mulan节点:
$ ping 10.2.0.1 （注意开启zwliao节点的ping/ICMP服务）
```

3.4 注意与其他

注意在测试某种功能时，注意打开相应的网络服务端口。
ping服务在windows操作系统中是默认关闭的，需要用户打开。

4 命令

进入目录：/etc/openvpn

systemctl start openvpn@server.service // 启动
systemctl restart openvpn@server.service // 重启
systemctl stop openvpn@server.service // 停止

cat openvpn.log # 查看log
cat openvpn-status.log # 查看系统状态

本文提到的各个证书等材料，请参考2数字证书方案

从openvpn 2.3 升级到2.4，压缩算法与加密算法兼容问题

https://fedoraproject.org/wiki/Changes/New_default_cipher_in_OpenVPN

https://www.sparklabs.com/support/kb/article/bad-compression-stub-decompression-header-byte/