FLEXGW 镜像使用帮助文档

修订历史记录			
日期	**版本**	**说明**	**作者**
2015/10/9	V2.0	FlexGW企业版镜像 V2.0 版本帮助文档	驻云/运维团队

前言

一、版权声明：

2、我们愿与所有镜像的爱好者进行更多的技术交流，此文档涉及的镜像环境均免费、并且免费提供镜像坏境的技术支持，并且开放镜像安装脚本的源代码。

3、我们欢迎您提供的更多镜像使用上的意见，投诉意见邮箱：qrj@jiagouyun.com

二、关于我们：

上海驻云信息科技有限公司，是一家具有领先的公有云架构技术及咨询服务提供商，致力于为企业客户提供卓越的公有云架构技术、云解决方案、云运维服务等一站式的云入驻服务。

公司拥有实力雄厚且经验丰富的云技术团队、研发团队和运维团队。公司自主研发的架构云产品为客户提供可视化的公有云架构及便捷的云构建及管理功能；精干的公有云技术团队为客户在上云实施过程中遇到的各种难题提供完善的技术解决方案；专业的运维团队通过创新的技术与稳健的服务为客户提供可靠的云运维服务。

三、联系我们：

1、公司网站

http://www.staycloud.cn

2、公司地址

上海总公司：上海市浦东新区晨晖路 88 号金蝶软件园 2 号楼 2405~2407

北京分公司：北京市鼓楼外大街 27 号万网大厦

3、镜像更多支持与帮助

总机：021-50800099

电话技术支持：021-50800099-103

旺旺技术支持：架构云

邮箱技术支持：qrj@jiagouyun.com

目录

1、镜像环境说明

1.1、镜像版本说明

操作系统：centos 6.5 64 位

镜像版本 V2.0 软件明细：

Strongswan5.3.2-Openvpn2.3.8-FlexGW2.0

1.2、镜像安装说明

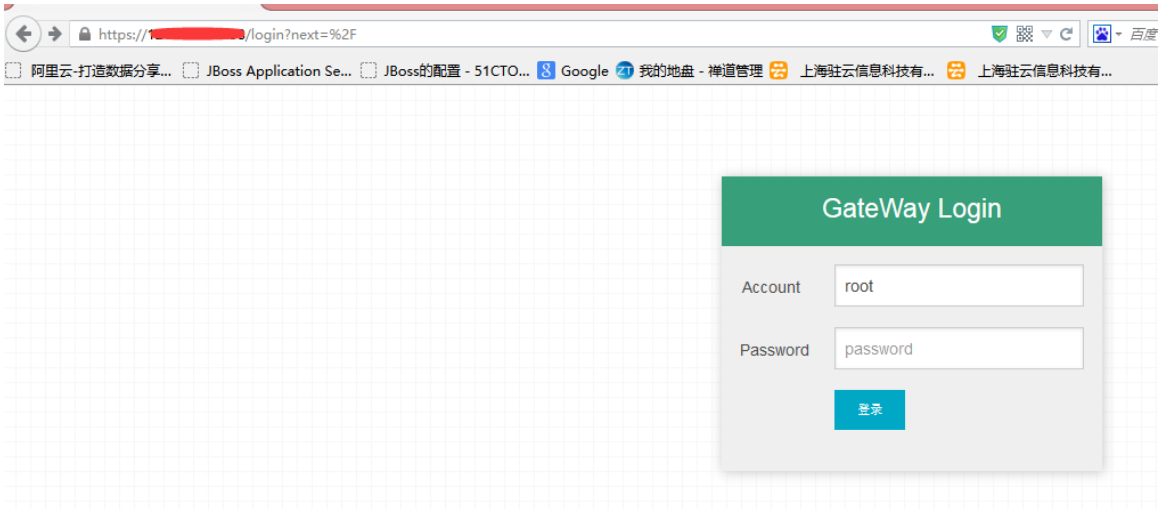
1.2.1、此镜像环境，是采用 rpm 包的方式安装的。

1.2.2、FlexGW 镜像 V2.0支持 IPSecVPN、拨号 VPN、SNAT、TCP 隧道、MFA多因素身份验证功能。

2、FlexGW 镜像功能说明

2.1、登陆说明

使用 VM 的系统账号密码即可登入系统，即所有可通过 SSH 登陆主机的用户都可以登入该系统。浏览器访问 https://公网 ip



2.2、功能介绍

本程序提供了 VPN、SNAT 基础服务。

主要提供以下几点功能：

1. IPSec Site-to-Site 功能。可快速的帮助你将两个不同的 VPC 私网以 IPSec Site-to-Site 的方式连接起来。支持可选的 IKEv2/ESP 加密算法、签名算法、DH 组。

2. 拨号 VPN 功能。可让你通过拨号方式，接入 VPC 私网，进行日常维护管理。

3. SNAT 功能。可方便的设置 Source NAT，以让 VPC 私网内的 VM 通过 Gateway VM 访问外网。

4. MFA多因素身份验证功能。在静态账号密码验证的基础上，增加动态密码验证方式，提高安全性。

3、软件目录及配置列表

3.1、FlexGW（即本程序）

目录：/usr/local/flexgw

数据库文件：/usr/local/flexgw/instance/website.db

日志文件：/usr/local/flexgw/logs/website.log

启动脚本：/etc/init.d/flexgw 或 /usr/local/flexgw/website_console

实用脚本：/usr/local/flexgw/scripts

「数据库文件」保存了我们所有的 VPN 配置，建议定期备份。如果数据库损坏，可通过「实用脚本」目录下的 initdb.py 脚本对数据库进行初始化，初始化之后所有的配置将清空。

3.2、Strongswan

目录：/etc/strongswan

日志文件：/var/log/strongswan.charon.log

启动脚本：/usr/sbin/strongswan

如果 strongswan.conf 配置文件损坏，可使用备份文件 /usr/local/flexgw/rc/strongswan.conf 进行覆盖恢复。

ipsec.conf 和 ipsec.secrets 配置文件，由 /usr/local/flexgw/website/vpn/sts/templates/sts 目录下的同名文件自动生成，请勿随便修改。

3.3、OpenVPN

目录：/etc/openvpn

日志文件：/etc/openvpn/openvpn.log

状态文件：/etc/openvpn/openvpn-status.log

启动脚本：/etc/init.d/openvpn

server.conf 配置文件，由 /usr/local/flexgw/website/vpn/dial/templates/dial 目录下的同名文件自动生成，请勿随便修改。

4、软件操作命令汇总

openvpn：

```
/etc/init.d/openvpn start/stop/restart/reload)
```

strongwan:

```
/etc/init.d/strongswan  start/stop/restart/...
```

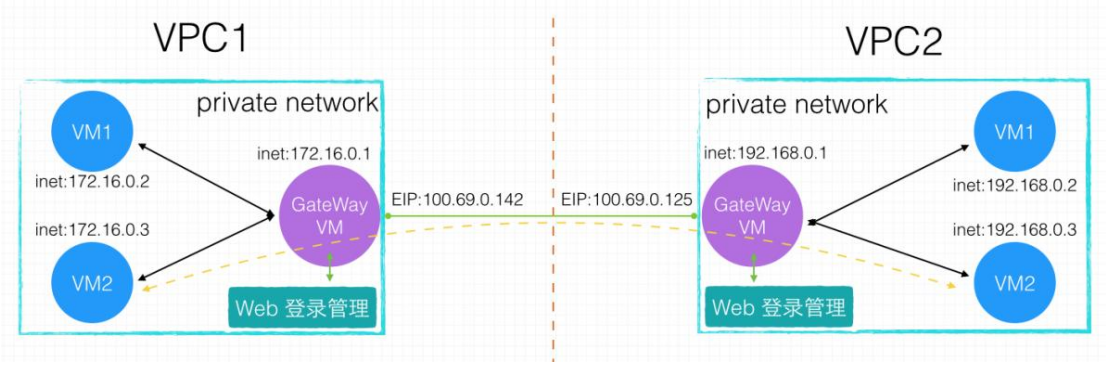
flexgw:

```
/etc/init.d/flexgw  start/stop/restart/...
```

比如启动 openvpn：

```
/etc/init.d/openvpn start
```

5、IPSec Site-to-Site VPN 使用指南



如上图所示，VPC1 私网为：172.16.0.0/24，VPC2 私网为：192.168.0.0/24。其中，两个 VPC 中各有一台使用 VPN/SNAT 镜像安装的 GateWay VM，并绑定了

EIP。现在想让两个 VPC 的私网 VM 之间 能够相互访问，我们将需要在 VPC1 GateWay VM 和 VPC2 GateWay VM 之间建立一条 IPSec Site-to-Site 隧道。本例：从 VPC1 的 172.16.0.3 访问 VPC2 的 192.168.0.3 。

5.1、启动 IPSec VPN 服务

进入 IPSec 「VPN 服务管理」页面，确保 VPC 两端的 GateWay VM1、 GateWay VM2 均启动了 IPSec VPN 服务。

启动 VPN 服务：仅启动本机的 IPSec VPN。启动时，启动类型为「自动连接」的隧道将自动尝试连接对端 VPN。

停止 VPN 服务：停止本机的 IPSec VPN。已经连接上的隧道将全部断开。

配置下发&重载：一般情况下，该动作在新增、修改或删除隧道时会自动进行。但某些情况下，如果你想重新生成 VPN 配置，可手动执行该操作。

5.2、增加隧道

VPC1 GateWay VM:

VPC2 GateWay VM:

两边的隧道 ID、加密算法、验证算法、DH 组、预共享密钥必须一致才能建立连接。

本端子网、对端子网：即前面例子中的 192.168.0.0/24，172.16.0.0/24。

对端公网 IP：对端 GateWay 所绑定的 EIP。

5.3、查看隧道列表

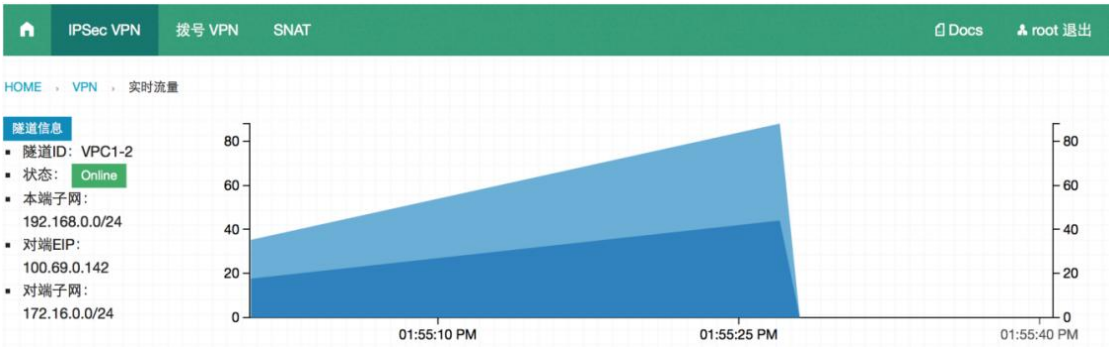
在 VPC1 和 VPC2 的 GateWay VM 上将隧道添加完毕之后，进入「隧道列表」页面。对我们刚刚配置好的隧道，点击「连接」，即可看到：

连接：连接隧道。在两台 GateWay VM 任意一端操作即可。

断开：断开隧道。在两台 GateWay VM 任意一端操作即可。

5.4、查看隧道实时流量

点击上图的「流量」按钮，即可看到隧道的实时流量：

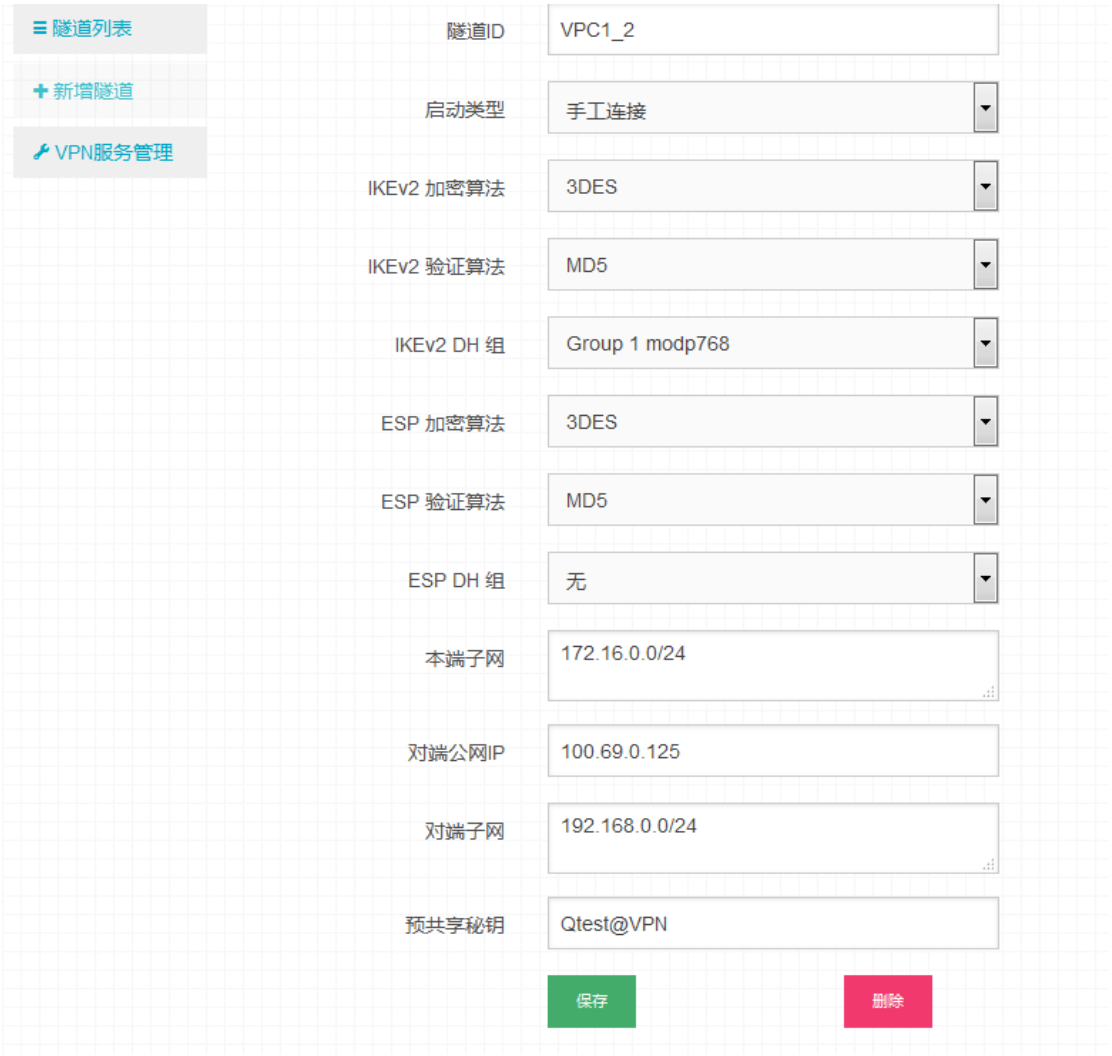


颜色：代表 in、out 方向的流量。

单位：Bytes

5.5、修改或删除隧道

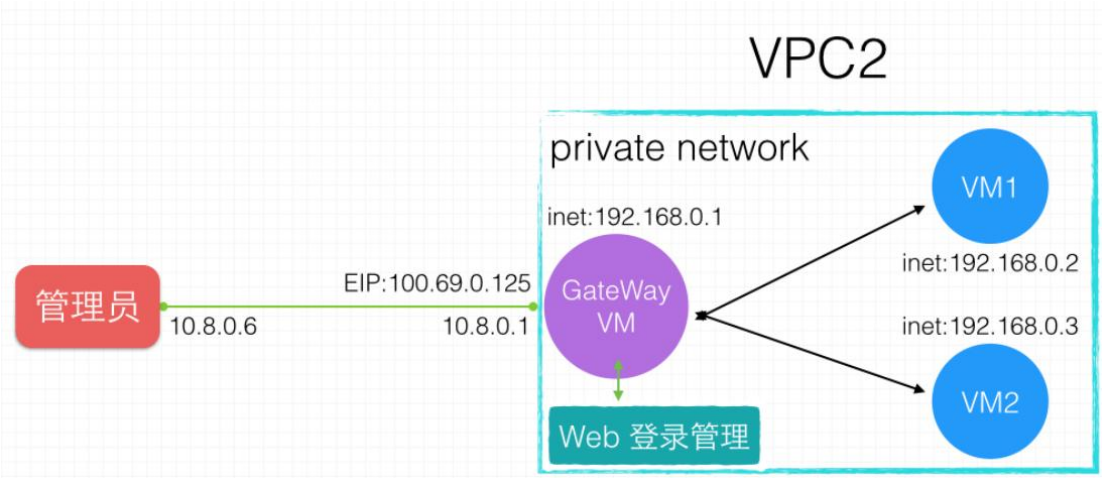
点击对应的隧道 ID 进入修改、删除页面：



保存：修改后，点击保存，配置将立即生效，但不会影响已经连接上的隧道。需要手工断开、再连接隧道。

删除：点击删除，将该隧道删除，同时会自动断开该隧道，立即生效

6、拨号 VPN 使用指南



如上图所示，管理员想接入 VPC2 的私网内，以便管理维护 VM1 和 VM2。其中，VPC2 中有一台使用 VPN/SNAT 镜像安装的 GateWay VM，并绑定了 EIP。

本例：管理员从公网通过 VPN 隧道访问 VPC2 的 192.168.0.3 。

6.1、启动拨号 VPN 服务

进入拨号 VPN 的「VPN 服务管理」页面，确保 VPC 的 GateWay VM 启动,镜像中需要手动启动 VPN 服务，在如下界面中，点击启动 VPN 服务

启动 VPN 服务：仅启动本机的拨号 VPN。

停止 VPN 服务：停止本机的拨号 VPN。已经连接上的隧道将全部断开。

配置下发&重载：进行拨号 VPN 「设置」时，该动作会自动进行。但某些情况下，如果你想重新生成 VPN 服务端配置，可手动执行该操

作。

6.2、设置

虚拟 IP 地址池：即 VPN Server 分配给客户端的虚拟 IP 地址池。

子网网段：即我们 VPC2 的子网 192.168.0.0/24。

6.3、配置 SNAT

进行拨号 VPN 「设置」之后，为了让管理员能够访问 VPC2 的私网，需要手工调整相应的 SNAT 设置！

在上面的例子中，虚拟地址池为 10.8.0.0/24，子网网段为 192.168.0.0/24，则需要配置 SNAT：10.8.0.0/24 ➔ 192.168.0.1

6.4、添加拨号 VPN 账号

点击「新增账号」按钮，即可新增账号：

账号名：只可包含如下字符：数字、字母、下划线。

密码：只可包含如下字符：数字、字母、下划线。密码以明文方式保存和显示，以让系统管理员可随时查看和修改。

6.5、查看账号列表

点击「账号列表」按钮，可以查看已经添加的账号列表。如果该账号已经拨入 VPN，将看到更明细的信息：

状态：由于 VPN 的 keepalive 机制，会有 1 分钟左右的延时。

6.6、配置客户端

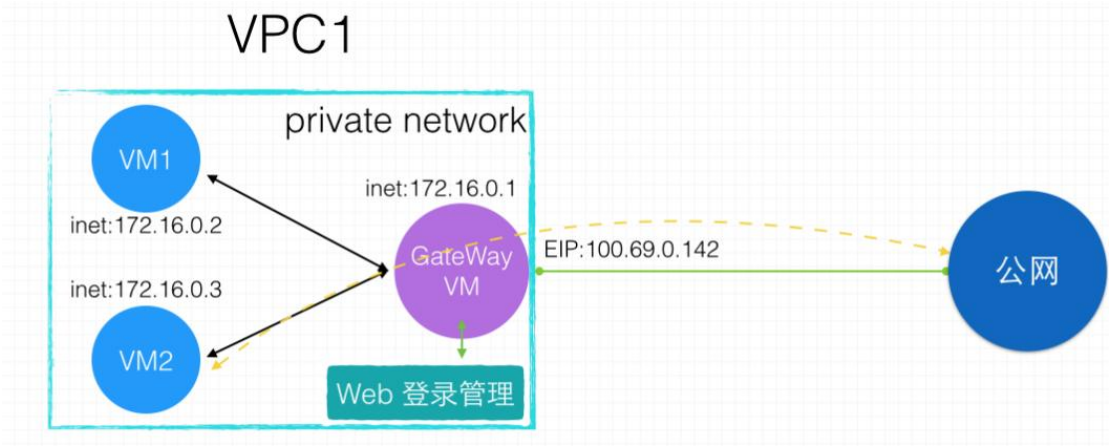
点击「客户端下载」按钮，可以下载 VPN 客户端和相应的配置文件。

修改配置文件：将配置文件中的「remote IP」字段修改为 GateWay VM 的 EIP 地址。

Windows 平台：安装完客户端后，将配置文件 client.ovpn 和 ca.crt 文件放到安装目录下的 config 文件夹中。然后启动 openvpn-gui.exe，根据提示进行连接。

Linux 平台：在配置文件 client.conf 和 ca.crt 的目录下执行命令：openvpn client.conf，根据提示进行连接

7、SNAT 使用指南



如上图所示， VPC1 私网为： 172.16.0.0/24。其中， VPC1 中有一台使用 VPN/SNAT

镜像安装的 GateWay VM，并绑定了 EIP。

现在想让 VPC1 的私网 VM 能够访问公网，我们将需要在 VPC1 GateWay VM 上

进行 SNAT 配置。

本例：从 VPC1 的 172.16.0.3 访问公网。

7.1、添加 SNAT 条目

进入 SNAT 的「SNAT 新增」页面：

SNAT 源 IP（段）：为 VPC1 中需要访问公网的私网网段。本例中为：172.16.0.0/24

SNAT 转发 IP：为 VPC1 中 GateWay VM 的私网 IP，而非 EIP。本例中为：172.16.0.1

7.2、SNAT 列表

新增 SNAT 条目之后，会自动跳转到「SNAT 列表」页面，即可看到：

转发网络：为 VPC1 中需要访问公网的私网网段。本例中为：172.16.0.0/24

转发后 IP：为 VPC1 中 GateWay VM 的私网 IP，而非 EIP。本例中为：172.16.0.1

删除：点击「删除」按钮，即可删除该 SNAT 条目，且立即生效。

8、TCP 隧道使用指南

当您想要访问 VPC 内部某台 ECS 的特定端口，可以通过本功能将该端口映射到 FlexGW 机器，然后通过 FlexGW 的 EIP 访问。

8.1、添加 TCP 隧道条目

进入 TCP 隧道 的「TCP 隧道新增」页面：

- 本地端口：为 FlexGW 为转发打开的端口。本例中为：50000
- 目标 IP：为 VPC 中需要访问公网的私网 IP。本例中为：10.0.0.1
- 目标端口：为目标机器的端口。本例中为：3306

8.2、查看 TCP 隧道列表

新增 TCP 隧道条目之后，会自动跳转到「TCP 隧道列表」页面，即可看到：

- 本地端口：为 FlexGW 为转发打开的端口
- 目标 IP：为 VPC 中需要访问公网的私网 IP。本例中为：10.0.0.1
- 目标端口：为目标机器的端口。本例中为：3306
- 关闭：点击「关闭」按钮，即可关闭该 TCP 隧道，且立即生效。

9、关于 VPN 证书

9.1、说明

考虑到证书的唯一性、安全性，我们的证书文件是 VM 第一次启动时，通过脚本自动生成的，其原始目录为：/usr/local/flexgw/scripts/keys，下面所提到的证书文件，均为该目录下的证书文件的拷贝。

- **IPSec Site-to-Site 隧道：**

IPSec Site-to-Site VPN 采用的时 PSK 方式加密连接，并不使用证书认证。

- **拨号 VPN：**

拨号 VPN 的证书，位于/etc/openvpn 下：

1. ca.crt：是根证书，服务器和客户端都需要保存。
2. server.crt：是服务器的证书，由 CA 证书进行签名。
3. server.key：是服务器的证书对应密钥。
4. dh1024.pem：DH 算法参数文件。

- **网站 HTTPS 证书：**

网站的证书，位于/usr/local/flexgw/instance 目录下：

1. ca.crt：是根证书。
2. server.crt：是服务器的证书，由 CA 证书进行签名。
3. server.key：是服务器的证书对应密钥。

9.2、使用自己的证书

如果你希望使用自己的证书，可以使用 openssl 命令生成自己的根证书、服务器证书、以及 DH 算法参数文件。

- **拨号 VPN：**

1. 将生成的证书文件，拷贝到在/etc/openvpn 目录下替换掉相应的证书文件。
2. 客户端也要使用新的 CA 证书来替换掉原来的根证书。可通过 /usr/local/flexgw/scripts/packconfig 脚本，重新打包 openvpn client

配置文件，打包后的配置文件位于：

/usr/local/flexgw/website/vpn/dial/static 目录下。请将配置文件，重新分发给客户端。

3. 通过「VPN 服务管理」页面重启拨号 VPN 服务。

- **网站 HTTPS 证书：**

1. 将生成的证书文件，拷贝到在/usr/local/flexgw/instance 目录下替换掉相应的证书文件。

2. 重启网站：/etc/init.d/flexgw restart

10、问题排查

10.1、IPSec Site-to-Site 隧道

1. 隧道建立后无法连接
   1） 请检查两端隧道 ID、加密算法、验证算法、DH 组、预共享密钥是否相同。
   2） 请检查对端 公网 IP 是否有误。
   3） 请尝试重新启动 VPN 服务。
2. 隧道连接成功，但是两端子网无法相互访问
   1） 请检查是否已将子网的流量路由到了 VPN VM 上。
   2） 请检查配置中对端子网是否有误。
   3） 请尝试重新启动 VPN 服务。

10.2、拨号 VPN 隧道

1. 客户接连接超时，请按以下步骤依次检查尝试排除
   1） 请检查配置文件服务器地址是否有误。
   2） 请检查服务是否开启。
   3） 请检查客户端是否使用正确的根证书（ca.crt） 。
   4） 请确认是否更改过服务器证书文件或配置。
   5） 请检查客户端是否有防火墙过滤。
   6） 请尝试重新启动拨号 VPN 服务。

2. 客户端连接失败，提示‘AUTH_FAILED’

1） 请检查输入账号密码是否正确。

2） 请检查服务器是否已经添加账号密码。

3） 请尝试重新启动拨号 VPN 服务。

3. 客户端已连接上，但是无法访问内网 VM

1） 请尝试 PING 服务器虚拟 IP（如 10.8.0.1） 。

2） 请检查是否正确开启 SNAT。

3） 请尝试重新启动拨号 VPN 服务。

11、升级指南

当检测到升级信息时，请按如下方法进行升级：

1. 通过 ssh 或者 VNC 管理终端登录 VM，切换到 root 账号，或者 sudo 权限。

2. 关闭 flexgw，执行命令：/etc/init.d/flexgw stop

3. 升级，执行命令：/usr/local/flexgw/scripts/update --yes

4. 根据提示进行升级。

5. 升级完成，启动 flexgw：/etc/init.d/flexgw start

注意：升级前，建议备份/usr/local/flexgw/instance/* 目录下的数据文件！