

WeLink安全隧道（云桥）

部署指导书

文档版本 05
发布日期 2023-04-26

版权所有 © 华为技术有限公司 2020。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

目 录	1
1 概述	3
2 总体架构	4
2.1 总体架构	4
2.2 高可用架构	5
3 搜集现场环境信息	6
3.1 用户规模	6
3.2 策略要求	6
3.3 网络环境	6
3.4 服务器环境	7
4 方案配置建议	8
4.1 服务器部分	8
4.2 存储部分	8
4.3 其他资源	8
4.4 防火墙开通策略	9
4.5 时间计划	9
5 部署前准备	10
5.1 上传安装包	10
5.2 测试网络连通性	10
5.3 查询Secret信息	11
6 部署安全隧道（云桥）服务	12
6.1 解压安装包	12

6.2 部署安全隧道（云桥）服务	12
6.3 配置安全隧道（云桥）信息	12
6.4 启动安全隧道（云桥）服务	13
6.5 配置开机启动	14
7 (可选) 部署Keepalived	15
7.1 部署Keepalived服务	15
7.2 配置Keepalived服务信息	15
7.3 启动Keepalived服务	15
7.4 配置开机启动	16
8 验证内网应用连通性	17
9 配置管理后台信息	18
9.1 系统网关配置	18
9.2 访问域名管理	19
9.3 访问网址管理	19
9.4 访问权限控制	19
10 配置后验证	21
10.1 测试安全隧道（云桥）网络连通性	21
10.2 验证安全隧道（云桥）服务	22
11 附录	23
11.1 华为云公网IP	23
11.2 商业证书购买流程	23
11.3 安全隧道（云桥）日志目录结构	24
11.4 安全隧道（云桥）日志获取方法	24
11.5 安全隧道（云桥）日志说明	24
11.6 网络性能排查	25
11.7 云桥对接内网应用服务申明	26

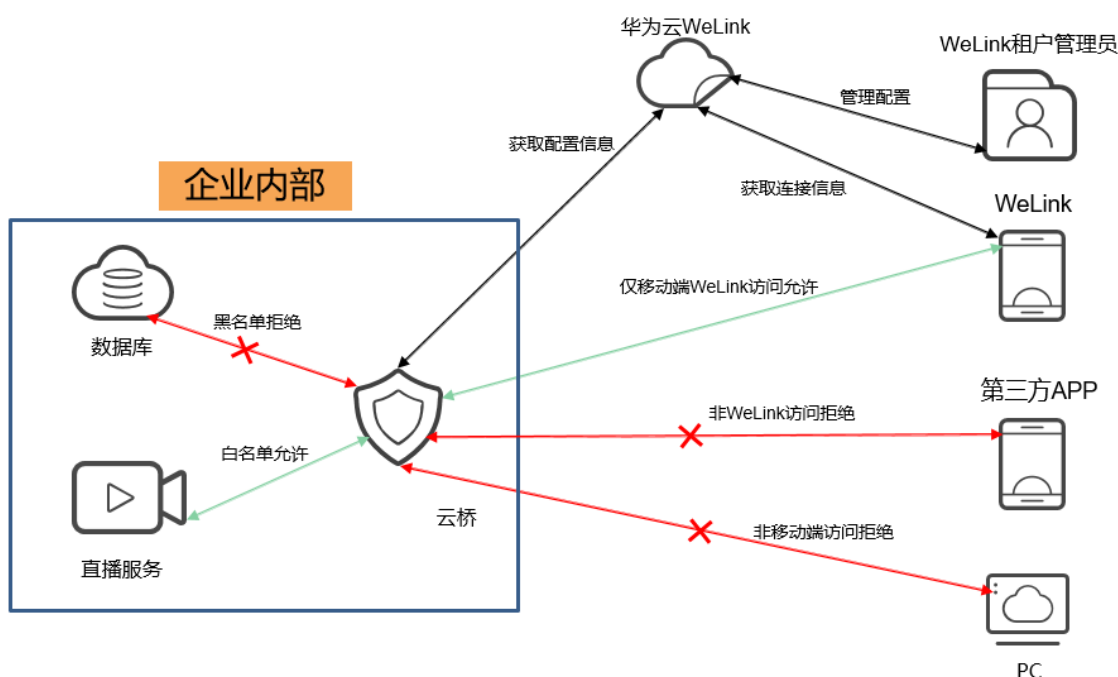
1 概述

安全隧道（云桥）是一个移动端应用级的网络安全服务，集成在WeLink产品中。其目的是在企业员工和企业内部服务之间建立起一条网络安全隧道（云桥），企业员工可在手机端通过WeLink产品直接访问企业内的应用资源。

安全隧道（云桥）核心优势如下：

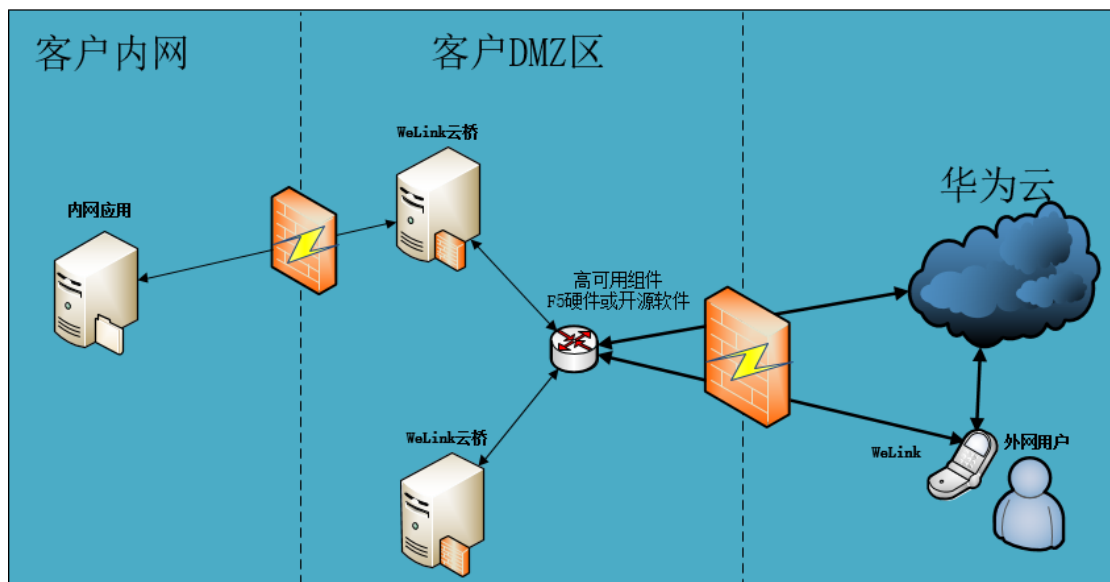
- 数据安全性。采用业界权威的高强度加密算法，确保所有数据安全传输。
- 管理便捷性。提供黑白名单管控机制，企业管理员可自行配置内网资源的访问范围，便于企业管理员对内网应用做精细化的分类。
- 请求专属性。所有连接安全隧道（云桥）服务的请求仅能通过移动端WeLink发起，任何其他途径发起的请求均被拒绝。

安全隧道（云桥）场景示意图：



2 总体架构

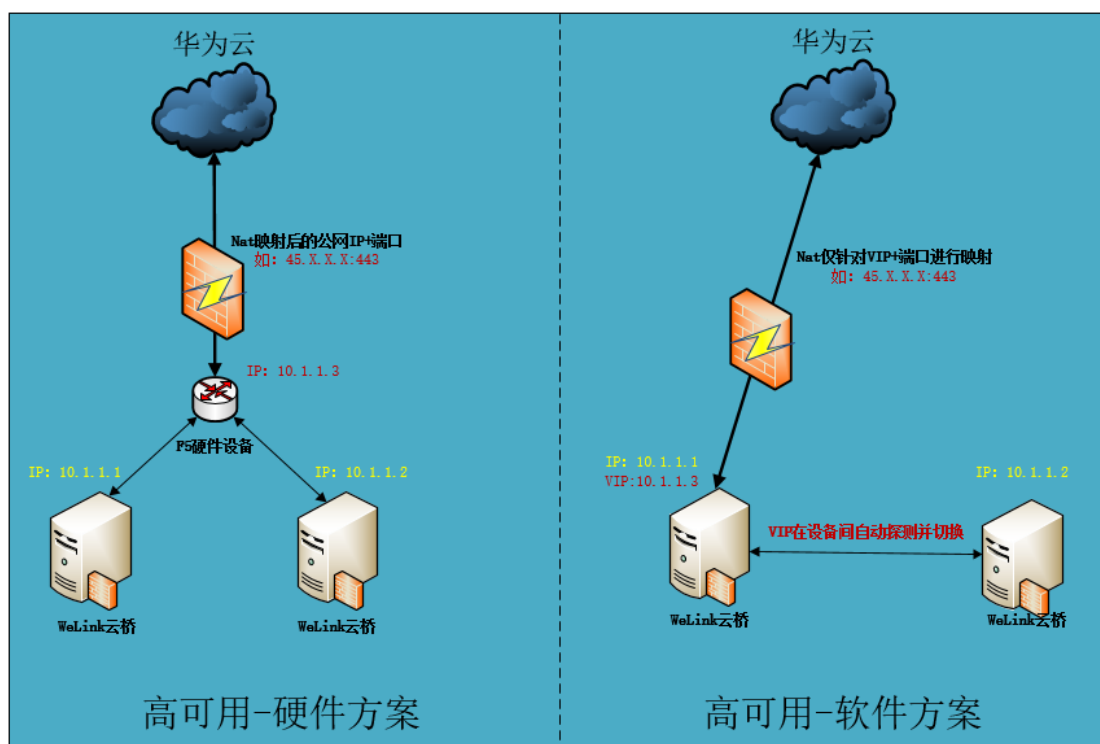
2.1 总体架构



总体架构说明：

- 用户的所有请求均通过WeLink移动端从公网解析到DMZ区的WeLink安全隧道（云桥）服务器，由其与华为云上的服务器进行认证。
- 当认证通过以后，将会为用户侧与内网应用之间建立一条隧道，用户便可直接通过该隧道来访问内网中的所有应用。

2.2 高可用架构



高可用架构说明：

- 硬件方案：客户网络环境中提供类似于F5的硬件设备，由其作为请求转发并且对两台WeLink安全隧道（云桥）服务器进行健康度探测，从而保证两台安全隧道（云桥）服务器高可用。
- 软件方案：当客户网络无法提供任何硬件设备时，可以在两台WeLink安全隧道（云桥）服务器中额外部署Keepalived服务且将所有安全隧道（云桥）服务器整合为一个集群，在集群内通过Keepalived自身的机制确保有一台存活的安全隧道（云桥）服务器能正常对外提供服务，从而实现高可用。

3 搜集现场环境信息

3.1 用户规模

- 小型规模（1万人以下）
- 中型规模（1万~5万人）
- 大型规模（5万人以上）

3.2 策略要求

- 内网应用针对用户是统一策略还是不同策略，各个策略的要求和规则是怎样。
- 内网应用个数总量，每个应用是否有特殊的要求或者限制。
- 当前内网认证体系是怎样，是否有特殊要求限制。

3.3 网络环境

- 当前网络分区是怎样的，有没有特殊要求限制。
- IP段是否有做分离，例如内网应用一个网段，代理服务器另一个网段。
- 当前Internet带宽总出口是多大？
备注：为了让用户获得最佳的体验，带宽建议要求为 20Kbps*用户数
- 内网DNS服务器是否能对内网所有应用域名进行解析。
- 当前网络环境中防火墙是如何部署的？最终需要保证内网应用和WeLink安全隧道（云桥）服务器之间能互通，WeLink安全隧道（云桥）服务器与华为云网络能互通。
- 企业内是否有跨站点部署的场景？
备注：例如深圳部署有内网应用，北京或者海外某个点也部署同一套应用。

3.4 服务器环境

- 支持虚拟机部署或物理机部署方案，建议单台服务器CPU核心数为4，内存数为8GB，数据盘空间为300GB。
- 当前网络中是否有专用的负载设备（例如F5）？
备注：优先推荐专用负载设备，如无法提供可以走软件负载方案(例如Keepalived)。
- 具备有效期商业证书。
备注：建议采用商业证书，如果没有可以通过自签名证书作为代替使用。

4 方案配置建议

4.1 服务器部分

资源类型	数量	配置	OS要求	备注
虚拟机	2	2C/4G 最低配置	Cent OS 7.X	最大支撑2万用户
		4C/8G 推荐配置		最大支撑5万用户
		8C/16G 超高配置	Euler 2.X	最大支撑8万用户

备注：虚拟机支持横向扩展，例如6万用户规模可以2台超高配置或者3台推荐配置。

4.2 存储部分

资源类型	数量	挂载路径
系统存储	单台机器至少32GB，推荐64GB	/
数据存储	单台机器至少150GB，推荐300GB。	如：/data01

4.3 其他资源

资源类型	数量	备注说明
公网IP(必须)	1个	用于WeLink端公网访问
硬件/软件高可用	1个	确保WeLink安全隧道（云桥）服务器的高可用性

SSL商业证书(必须)	1个	用户访问时需要通过其来进行认证和加密 备注：购买流程见附录
内网虚拟IP(可选)	1个	企业使用高可用软件方案时需要提供。

4.4 防火墙开通策略

- 外网防火墙入站规则(由外而内)：开通443端口权限，确保WeLink客户端能正常访问WeLink安全隧道（云桥）服务器对外提供的公网IP+443端口。
- 外网防火墙出站规则(由内而外)：开通443端口权限，确保WeLink安全隧道（云桥）服务器能正常访问华为云服务器的443端口。
- 内网应用服务器和WeLink安全隧道（云桥）服务器如果有防火墙，则需要针对内网各应用的端口进行开通，确保二者能互通。

4.5 时间计划

当所有资源均准备就绪的情况下，部署实施计划如下：

- 环境检查：1~2个工作日
- 业务应用部署：2~3个工作日
- 连通性调试：1~2个工作日

备注：预计1周时间完成整个方案的验证和测试。

5 部署前准备

5.1 上传安装包

上传安装包WeLink-WeAccess.tar.gz至待部署的WeLink安全隧道（云桥）服务器的/root/目录下，执行如下命令添加系统账户weaccess:

```
# useradd weaccess -u 2001 -s /bin/false
```

5.2 测试网络连通性

在服务器上通过执行wget或curl命令，如果返回475或400，则说明服务器和华为云平台连接正常。反之则检查服务器和华为云平台的防火墙端口是否配置正确。

```
# wget https://open.welink.huaweicloud.com/weaccess/strategy/api/v3/auth
```

```
Use is subject to audit at any time by Huawei management.
[root@host-10-120-2-30 ~]# wget https://open.welink.huaweicloud.com/weaccess/strategy/api/v3/auth
--2019-09-27 15:03:32-- https://open.welink.huaweicloud.com/weaccess/strategy/api/v3/auth
Resolving open.welink.huaweicloud.com (open.welink.huaweicloud.com)... 103.40.12.17
Connecting to open.welink.huaweicloud.com (open.welink.huaweicloud.com)|103.40.12.17|:443... connected.
HTTP request sent, awaiting response... 475 status code 475
2019-09-27 15:03:33 ERROR 475: status code 475
```

或者执行

```
# curl -i https://open.welink.huaweicloud.com/weaccess/strategy/api/v3/auth
```

```
[root@host-10-120-2-30 ~]# curl -i https://open.welink.huaweicloud.com/weaccess/strategy/api/v3/auth
HTTP/1.1 475 status code 475
Server: CloudWAF
Date: Fri, 27 Sep 2019 07:04:09 GMT
Content-Type: application/octet-stream
Content-Length: 0
Connection: keep-alive
Set-Cookie: HWWAFSEID=24fb57628cd407875f; path=/
Set-Cookie: HWWAFSESTIME=1569567848774; path=/
```

5.3 查询Secret信息

通过浏览器访问打开如下链接，以租户管理员身份登陆WeLink管理后台，点击“安全策略” - “WeLink安全隧道（云桥）”按钮，进入安全隧道（云桥）(WeAccess)配置后台界面。

<https://welink.huaweicloud.com>

在“网关地址”下点击“查看” - “确定”按钮，将租户Secret信息保存并记录；如果获取失败，可点击“重新获取”。



6 部署安全隧道（云桥）服务

6.1 解压安装包



说明

XXX为客户安装目录(可自定义)

```
# mkdir -p /XXX/weaccess
# ln -s /XXX/weaccess /usr/local/weaccess
# cd /root/
# tar -zxvf WeLink-WeAccess.tar.gz
# chown -R weaccess:weaccess ./weaccess
```

6.2 部署安全隧道（云桥）服务



说明

YYY 为获取到的租户 Secret

```
# cd /root/weaccess/nginx
# ./deploy.sh install
# chmod -R 755 /usr/local/weaccess/
# cd /usr/local/weaccess/nginx/sbin/
# ./privatekeytool -pwd YYY -out ../conf/weaccess_key.enc
```



说明

若需要卸载服务，可执行如下命令

```
# ./deploy.sh uninstall
```

6.3 配置安全隧道（云桥）信息

- 业务信息配置。

将XXX替换成实际端口(通常为443)，YYY替换成实际的业务内网IP，具体以分配

为准。

```
# sed -i "s/<PORT>/XXX/g" /usr/local/weaccess/nginx/conf/nginx.conf
# sed -i "s/<LOCAL_IP>/YYY/g" /usr/local/weaccess/nginx/conf/nginx.conf
```

- DNS信息配置。

若企业内网环境中没有DNS服务器，执行如下命令：

```
# sed -i "s/<DNSIP>/8.8.8.8/g" /usr/local/weaccess/nginx/conf/nginx.conf
```

若企业内网环境中有DNS服务器，执行如下命令：



说明

dns01、**dns02**为客户公司DNS服务器的IP，多个IP用空格分开

```
# sed -i "s/<DNSIP>/dns01 dns02/g" /usr/local/weaccess/nginx/conf/nginx.conf
```

- 将企业商业证书公钥**xx.crt**和私钥**xx.key**上传至/usr/local/weaccess/nginx/ssl目录，执行如下命令，在出现“Enter PEM pass key”提示后输入密码，密码用于对私钥**xx.key**加密：

```
# cd /root/weaccess/nginx
# ./config-ssl.sh
```

```
[root@nkgtsv26116ctx /usr/local/weaccess/nginx]# ./config-ssl.sh
Enter PEM pass phrase:
writing RSA key
succeed to encrypt data to file
../conf/keypass.enc
```



说明

如果企业无SSL商业证书，可参见附录相关购买流程自行购买。

6.4 启动安全隧道（云桥）服务

```
# cd /usr/local/weaccess/nginx
# pkill nginx
# ./nginx.sh start
# ps -ef | grep nginx
```

出现如下信息表示服务启动成功。

```
[root@nkgtsv26116ctx /usr/local/weaccess/nginx/sbin]# ps -ef |grep nginx
root      30411    1    0 15:33 ?        00:00:00 nginx: master process ./nginx
nobody    30412  30411    0 15:33 ?        00:00:00 nginx: worker process
root      30429  5654    0 15:33 pts/1    00:00:00 grep --color=auto nginx
```



说明

若需要停止服务，可执行如下命令

```
# pkill nginx
```

6.5 配置开机启动

执行如下命令：

```
# echo "/usr/local/weaccess/nginx/nginx.sh start &> /dev/null" >>
/etc/rc.d/rc.local
# chmod +x /etc/rc.d/rc.local
[root@nkgtsv26116ctx /usr/local/weaccess/nginx/sbin]# ps -ef |grep nginx
root      30411      1  0 15:33 ?          00:00:00 nginx: master process ./nginx
nobody    30412 30411  0 15:33 ?          00:00:00 nginx: worker process
root      30429    5654  0 15:33 pts/1    00:00:00 grep --color=auto nginx
```


7 (可选) 部署 Keepalived

说明

若企业网络中能提供硬件高可用设备，本章节可以忽略；

若企业网络中未提供硬件高可用设备，需要通过本章节来部署软件 Keepalived，确保 WeAccess 服务的高可用性。

7.1 部署Keepalived服务

```
# cd /root/weaccess/keepalived
# ./deploy.sh install
```

说明

若需要卸载服务，可执行如下命令

```
# ./deploy.sh uninstall
```

7.2 配置Keepalived服务信息

说明

virtual_ip 为对外提供业务服务的内网虚拟 IP，**peer_ip** 为除本机外的另一台安全隧道（云桥）服务器的业务 IP，**local_ip** 为本机业务 IP，**network_card** 为业务 IP 对应的网卡。

```
# sed -i "s/<unicast_peer>/peer_ip/g" /etc/keepalived/keepalived.conf
# sed -i "s/<virtual_ipaddress>/virtual_ip/g" /etc/keepalived/keepalived.conf
# sed -i "s/<unicast_src_ip>/local_ip/g" /etc/keepalived/keepalived.conf
# sed -i "s/<interface>/network_card/g" /etc/keepalived/keepalived.conf
# echo "local0.* /var/log/keepalived.log" >> /etc/rsyslog.conf
# systemctl restart rsyslog
```

7.3 启动Keepalived服务

```
# keepalivedctl start
# ps -ef | grep keepalived
```

出现如下信息表示Keepalived服务启动成功。

```
[root@nkgtsv26116ctx ~/weaccess/keepalived]# keepalivedctl start
Starting keepalived: [ OK ]
[root@nkgtsv26116ctx ~/weaccess/keepalived]# ps -ef |grep keepalived
root      30960      1  0 15:38 ?        00:00:00 keepalived -P -S 0
root      30961  30960  0 15:38 ?        00:00:00 keepalived -P -S 0
root      30982  5654  0 15:38 pts/1    00:00:00 grep --color=auto keepalived
```

7.4 配置开机启动

执行如下命令：

```
# echo "/usr/sbin/keepalivedctl start &> /dev/null" >> /etc/rc.d/rc.local
# chmod +x /etc/rc.d/rc.local
```

8 验证内网应用连通性

说明

提前准备完成客户内网某资源的服务器 IP(域名)和端口，本指导书以：**172.19.96.173** 和 **443** 端口为例，具体以实际情况为准。

登录 WeLink 安全隧道（云桥）服务器，执行如下命令验证连通性：

```
# telnet 172.19.96.173 443
```

如果出现链接超时或者链接被拒绝的提示表示失败，若出现如下信息表示成功：

```
[root@nkgtsv25977ctx ~]# telnet 172.19.96.173 443
Trying 172.19.96.173...
Connected to 172.19.96.173.
Escape character is '^]'.
```

9 配置管理后台信息

通过浏览器访问打开如下链接，以租户管理员身份登陆 WeLink 管理后台，点击“安全策略” - “WeLink 安全隧道（云桥）”进入安全隧道（云桥）(WeAccess)配置后台界面。

<https://welink.huaweicloud.com>



9.1 系统网关配置

指定企业内部邮件系统的地址以及 WeLink 安全隧道（云桥）网关的公网地址。

- 网关地址(必填)：45.X.X.X:443 WeLink安全隧道（云桥）网关的公网地址，可以是IP也可以是域名，端口以实际为准。
- 信息填写完成后点击“保存”即可。

9.2 访问域名管理

指定哪些 IP 或者域名是客户内网应用，这些应用后续通过 WeLink 安全隧道（云桥）来访问。比如内网应用 IP 为 10.X.X.X 网段或者域名为 XX.enterprise.com，可以配置为：

- 10.*并且勾选“内网”。
- *.enterprise.com并且勾选“内网”。

The image shows two side-by-side screenshots of the '新增域名' (Add Domain) configuration form. Each form has a title bar with '新增域名' and a close button 'X'. The left form has the following fields: '* 域名内容' (Domain Content) with the value '10.*', '* 类型' (Type) with radio buttons for '内网' (selected) and '外网' (Unselected), and '备注' (Remarks) with an empty text area. The right form has: '* 域名内容' with the value '*.enterprise.com', '* 类型' with '内网' selected, and '备注' with an empty text area. Both forms have '确认' (Confirm) and '取消' (Cancel) buttons at the bottom.

9.3 访问网址管理

指定内网中哪些应用允许 WeLink 客户端通过安全隧道（云桥）来访问，可用于企业对内网应用做更精细化的区分。如果内网应用 IP 为 10.X.X.X 网段或者域名为 XX.enterprise.com，若不需要做精细化区分可按照如下要求配置即可：

- 域名选择10.*，网址“10.*/*”，勾选“允许访问”。
- 域名选择*.enterprise.com，网址“*.enterprise.com/*”，勾选“允许访问”。

The image shows two side-by-side screenshots of the '新增规则' (Add Rule) configuration form. Each form has a title bar with '新增规则' and a close button 'X'. The left form has the following fields: '* 规则名称' (Rule Name) with the value '内网-ACL', '* 域名' (Domain) with a dropdown menu showing '10.*', '* 网址' (URL) with the value '10.*/*', '* 类型' (Type) with radio buttons for '允许访问' (selected) and '禁止访问' (Unselected), and '备注' (Remarks) with an empty text area. The right form has: '* 规则名称' with the value 'ACL-内网', '* 域名' with a dropdown menu showing '*.enterprise.com', '* 网址' with the value '*.enterprise.com/*', '* 类型' with '允许访问' selected, and '备注' with an empty text area. Both forms have '确认' (Confirm) and '取消' (Cancel) buttons at the bottom.

9.4 访问权限控制

创建特定分组成员，配置该分组对内网指定资源是否具有访问权限。

- 点击“创建分组”按钮，可以自定义一个分组名称。

- “成员管理”中可以添加分组成员，“网址权限”中可添加内网资源地址并设置访问控制权限。

The screenshot displays two panels from the WeLink configuration management interface. The left panel, titled '人员访问权限管理' (Personnel Access Permission Management), shows a '分组名称' (Group Name) section with a '创建分组' (Create Group) button and a search box labeled '搜索分组' (Search Group). Below this, a table lists a group named 'Test001' with the description 'Test001成员使用' (Test001 member use) and options for '编辑' (Edit) and '删除' (Delete). The right panel, titled '网址权限' (URL Permissions) and '成员管理' (Member Management), has two tabs. The '网址权限' tab is active, showing a '添加网址' (Add URL) button and a '删除' (Delete) button. Below these are two rows in a table, each with a checkbox, a '规则名称' (Rule Name) column, and a '网址' (URL) column. The first row has an unchecked checkbox, the rule name '规则名称', and the URL '网址'. The second row has an unchecked checkbox, the rule name 'ffff', and the URL 'mail.pmail.huawei.com/*'.

规则名称	网址
<input type="checkbox"/> 规则名称	网址
<input type="checkbox"/> ffff	mail.pmail.huawei.com/*

10 配置后验证

10.1 测试安全隧道（云桥）网络连通性

测试安全隧道（云桥）公网 IP 的 443 端口连通性（端口以实际为准）。

备注：安卓手机可安装“网络万用表”，IOS 手机可安装“iNetTools”。

以安卓手机为例：

ping：显示类似如下信息，表示安全隧道（云桥）公网 IP 可访问



telnet：显示类似如下信息，表示安全隧道（云桥）的 443 端口可访问



10.2 验证安全隧道（云桥）服务

登录企业移动端 WeLink 账号，打开通讯录找到个人账号并点击“消息”，在消息对话框中发送一条内网真实服务器链接，如：“<https://172.19.96.173>”，然后点击这个链接。如果能正常访问表示验证通过。

11 附录

11.1 华为云公网IP

华为云公网 IP 主地址：

103.143.19.130\103.40.12.17\103.45.160.167

华为云公网 IP 备地址：

122.112.208.0/24	139.159.208.0/24
117.78.24.0/24	103.31.200.0/24
49.4.56.0/24	119.3.117.0/24
119.3.116.0/24	124.70.125.0/24
124.70.126.0/24	116.205.4.0/24
123.60.238.0/24	116.205.146.0/24
123.60.127.0/24	159.138.224.32/27

11.2 商业证书购买流程

A、申请购买企业域名(申请 SSL 证书的前提)：

<https://www.huaweicloud.com/product/domain.html>

B、申请购买 SSL 商业证书

https://support.huaweicloud.com/qs-scm/scm_07_0001.html

备注：

- 1、域名购买完成后在管理控制台中将域名与企业公网 IP 做绑定(A 记录)，同时企业需要去工信部对该域名进行备案；
- 2、证书由私钥(xx.key)和公钥(xxx.crt)两部分组成，私钥在申请证书请求文件时由企业自己生成，公钥由 CA 机构对域名审核通过后颁发。

11.3 安全隧道（云桥）日志目录结构

报错和访问日志文件的路径：`/usr/local/weaccess/nginx/logs/`

当天报错日志：`error.log`

前 15 天报错日志：在 `error-log-archive/` 目录下

实时访问日志：`weaccess_access.log`

历史访问日志：在 `weaccess_access-log-archive/` 目录下

```
[root@nkgtsv26117ctx logs]# ll
total 22792
-rw-r--r-- 1 nobody root 0 Jun 10 00:01 access.log
drwxr-xr-x 2 weaccess weaccess 4096 Jun 10 00:01 access-log-archive
-rw-r--r-- 1 nobody root 11148 Jun 10 14:53 error.log
drwxr-xr-x 2 weaccess weaccess 4096 Jun 10 00:01 error-log-archive
-rwxr-xr-x 1 weaccess weaccess 471 Apr 30 16:39 logrotate
-rw-r--r-- 1 root root 5 Jun 1 15:42 nginx.pid
-rw-r--r-- 1 nobody root 23306046 Jun 10 14:53 weaccess_access.log
drwxr-xr-x 2 weaccess weaccess 19 Apr 30 16:39 weaccess_access-log-archive
[root@nkgtsv26117ctx logs]# pwd
/usr/local/weaccess/nginx/logs
```

11.4 安全隧道（云桥）日志获取方法

 说明

红色字体为获取日志当天日期，执行命令时以当天实际日期为准。

获取当天报错日志 `error.log`，执行 `zip` 命令对原文件压缩打包：

```
# cd /usr/local/weaccess/nginx/logs/
# zip error-log-20200610.zip error.log
```

获取历史报错日志，直接取用 `error-log-archive/` 目录下对应日期的 `gz` 文件；

获取实时访问日志 `weaccess_access.log`，执行 `zip` 命令对原文件压缩打包：

```
# cd /usr/local/weaccess/nginx/logs/
# zip weaccess-access-20200610.zip weaccess_access.log
```

获取历史访问日志，直接取用 `weaccess_access-log-archive/` 目录下对应时间的 `gz` 文件。

11.5 安全隧道（云桥）日志说明

A、报错日志

当天报错日志：error.log，每天 0 点 1 分会对 error.log 进行压缩归档，归档日志保存在 error-log-archive/目录下，保存最近 15 天的日志。

前 15 天报错日志：error-log-archive/目录下 error.log-*.gz 文件，例如：获取 2020 年 6 月 9 日的报错日志选择 error.log-20200610.gz，因为 9 号的报错日志在 10 号 0 点 1 分进行压缩归档，所以 gz 文件的名称是*20200610*。

```
-rw-r--r-- 1 nobody root 90173 May 31 22:30 error.log-20200601.gz
-rw-r--r-- 1 nobody root 367173 Jun 2 00:00 error.log-20200602.gz
-rw-r--r-- 1 nobody root 385994 Jun 2 23:58 error.log-20200603.gz
-rw-r--r-- 1 nobody root 393289 Jun 4 00:00 error.log-20200604.gz
-rw-r--r-- 1 nobody root 367791 Jun 4 23:59 error.log-20200605.gz
-rw-r--r-- 1 nobody root 493219 Jun 5 23:59 error.log-20200606.gz
-rw-r--r-- 1 nobody root 79804 Jun 6 23:51 error.log-20200607.gz
-rw-r--r-- 1 nobody root 176725 Jun 7 23:55 error.log-20200608.gz
-rw-r--r-- 1 nobody root 462563 Jun 8 23:56 error.log-20200609.gz
-rw-r--r-- 1 nobody root 385736 Jun 9 23:58 error.log-20200610.gz
[root@dggin4weac004 error-log-archive]# pwd
/usr/local/weaccess/nginx/logs/error-log-archive
```

B、访问日志

实时访问日志：weaccess_access.log，当日志大小超过 100M 会被压缩归档，归档日志保存在 weaccess_access-log-archive/目录下，保存 100 个文件。

历史访问日志：weaccess_access-log-archive/目录下的文件 weaccess_access.log-*.gz，例如：获取 2020 年 6 月 10 日 11:17-11:46 时间范围内的访问日志，获取文件 weaccess_access.log-202006101591760761.gz。

```
-rw-r--r-- 1 nobody root 15364313 Jun 10 09:52 weaccess_access.log-202006101591753921.gz
-rw-r--r-- 1 nobody root 15228071 Jun 10 10:20 weaccess_access.log-202006101591755601.gz
-rw-r--r-- 1 nobody root 15227160 Jun 10 10:48 weaccess_access.log-202006101591757281.gz
-rw-r--r-- 1 nobody root 15137652 Jun 10 11:17 weaccess_access.log-202006101591759021.gz
-rw-r--r-- 1 nobody root 14806338 Jun 10 11:46 weaccess_access.log-202006101591760761.gz
-rw-r--r-- 1 nobody root 15464880 Jun 10 12:11 weaccess_access.log-202006101591762261.gz
-rw-r--r-- 1 nobody root 14635625 Jun 10 12:41 weaccess_access.log-202006101591764061.gz
-rw-r--r-- 1 nobody root 14459194 Jun 10 13:33 weaccess_access.log-202006101591767181.gz
-rw-r--r-- 1 nobody root 14651876 Jun 10 14:14 weaccess_access.log-202006101591769641.gz
-rw-r--r-- 1 nobody root 14853752 Jun 10 14:45 weaccess_access.log-202006101591771501.gz
[root@dggin4weac004 weaccess_access-log-archive]# pwd
/usr/local/weaccess/nginx/logs/weaccess_access-log-archive
```

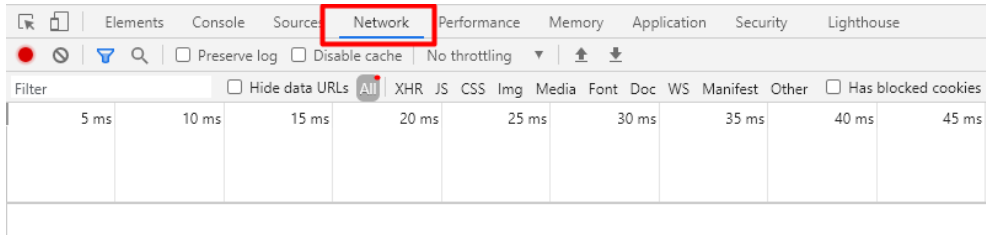
11.6 网络性能排查

企业客户反馈直接通过 PC 访问内网应用很快，但是通过 WeLink+安全隧道（云桥）来访问同样内网应用时很慢。这个问题主要原因是：PC 本身在内网环境下，访问应用时走内网，而 WeLink+安全隧道（云桥）访问内网应用会从 Internet 绕一圈，从而导致缓慢。

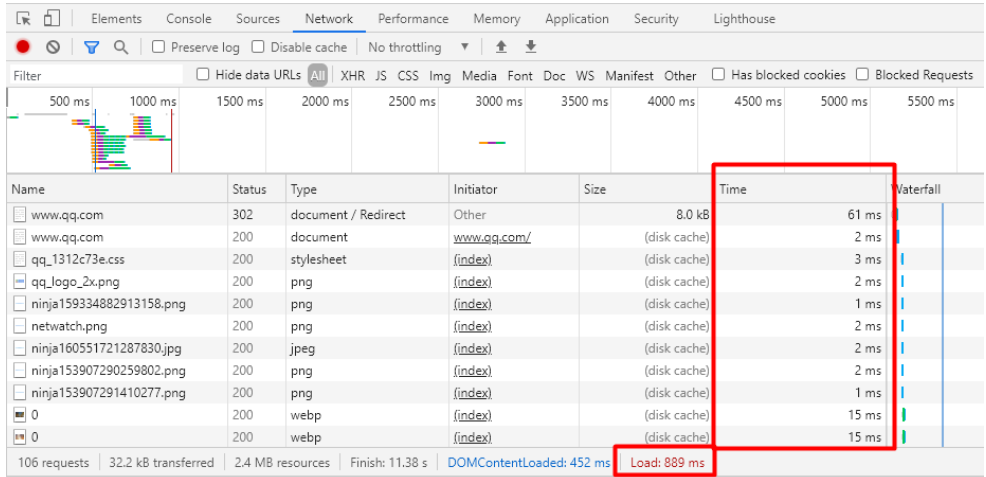
可以通过以下方法来排查是否是网络问题导致。

A、将内网某个非核心应用直接通过公网 IP 发布出去，确保在 Internet 环境下可以直接（即：绕过安全隧道（云桥））。

B、PC 安装 Chrome 浏览器，点击“设置”-“更多工具”-“开发者工具”（快捷键 F12），调出调试窗口并点击“Network”选项。



C、在浏览器窗口输入内网应用 IP 或者域名，观察 Time 和 Load 的值。



备注：按照上述方法使用同样的 PC 在内网和外网下访问同样的内网应用，观察对比两种不同网络环境下的差异。

11.7 云桥对接内网应用服务申明

- 云桥服务属于轻量级应用层 VPN 通道，可以代理如下协议：http/https、imap/pop/smtp、socket。
- 内网服务轻量级页面 URL 请求范围：不高于 20 个请求；页面资源大小：不高于 5M。
备注：
 - 由于手机端使用的是苹果或 Google 自带的浏览器内核，如果有超过上面的限制，在加载速度、性能上将严重降低；
 - 非轻量级的内网应用，建议使用 We 码小程序的访问方式(类似微信小程序)，可以打包资源文件并离线加载渲染页面，保留触发提交表单等核心请求
- 移动端轻量级应用可参考 HTML5 相关开发指导，用以优化加载速度和增强体验。