

云穿透接口

Cloud Through Interface

MUM 成都 • 2018/1/13

演讲人：熊茂祥

邀请方：EDCwifi捷联讯通

中国排名第一的MikroTik代理商

熊 茂 祥

自我介绍

- 通过MikroTik官方技术认证：MTCNA、MTCWE、MTCRE、MTCTCE。
- 中国大陆地区首个通过MikroTik官方认证的技术顾问。
- 独立编写并发布10个以上ROS相关应用程序，其中涉及到分流、负载、限速、认证、CAPSMAN、系统日志服务端、用户上网日志采集、路由表采集、集中WINBOX管理、内网穿透管理等方面。
- 客户分布在国内10余个省市，并在日本、韩国、美国、新加坡、尼日利亚、马来西亚也有少量运维客户及运维节点。

目录

01 云穿透接口出现的原因

02 云穿透接口可以解决哪些问题

03 云穿透接口的注册、开通、测试、注意事项

04 云穿透接口服务器的公开信息状态

05 云穿透接口的未来展望



01

云穿透接口 出现的原因

- 自2015年起，国内部分地区运营商就已经开始部署内网IP给普通宽带用户。典型的情况就是用户拨号后获取到的IP地址为100.64.x.x，或10.x.x.x。
- 内网IP的部署已经越来越普遍化，这个趋势是我们无法改变的，但我们必须去适应它。
- 做为网络运维工程师首要考虑的就是在没有公网IP的情况下如何去远程管理。因为我个人也是做远程运维的，如果出现故障时无法及时远程维护，不敢想象客户等待修复的心情。

Interface <UNI>

General	Dial Out	Status	Traffic
Last Link Down Time: Oct/29/2017 19:52:35			
Last Link Up Time: Oct/29/2017 19:52:44			
Link Downs: 20			
Uptime: 2d 21:24:37			
Encoding:			
MTU: 1480			
MRU: 1480			
Local Address: 183.94.149.58			
Remote Address: 183.94.148.1			
Active Links: 1			
Active Service Name:			
Active AC Name: HBWH-NGBD-HW-ME60-B1			
AC MAC Address: 80:FB:06:E2:DC:47			

enabled running slave Status: connected

运营商分配给我们的IP

Interface <UNI-1>

General	Dial Out	Status	Traffic
Last Link Down Time:			
Last Link Up Time: Oct/30/2017 18:10:13			
Link Downs: 0			
Uptime: 1d 23:05:10			
Encoding:			
MTU: 1480			
MRU: 1480			
Local Address: 10.1.53.254			
Remote Address: 10.1.52.1			
Active Links: 1			
Active Service Name:			
Active AC Name: Quidway			
AC MAC Address: 00:25:9E:88:58:F5			

enabled running slave Status: connected

过去大家在维护拨号环境时普遍使用DDNS做更新，现在很多地方已经行不通了。而且过去重启MikroTik设备或者重播号后都需要等待DDNS更新，快则1分钟，慢则10分钟以上。以下分别是运营商分配公网IP和内网IP时的DDNS不同状态。

在运营商分配内网IP时将出现以下提示

```
[admin@106] /ip cloud> print
ddns-enabled: yes
update-time: yes
public-address: 182.122.165.229
dns-name: 66c3056c8[REDACTED].sn.mynetname.net
status: updated
```

```
[admin@MikroTik] /ip cloud> print
ddns-enabled: yes
update-time: yes
public-address: 110.229.41.180
dns-name: 6f56063a2[REDACTED].sn.mynetname.net
status: updated
warning: DDNS server received request from IP 110.229.41.180 but your
local IP was 172.26.47.164; DDNS service might not work.
```





02

云穿透接口 可以解决哪些问题

1. 管理业务点没有公网IP的 MikroTik 设备。

例如长宽宽带分配的IP是非公网IP的，或者使用3G，LTE等方式接入网络也是没有公网IP的，我们可以将该设备接入云穿透来实现管理。

2. 管理没有业务点路由映射权限的 MikroTik 设备。

例如在某业务点下需要添加一个2级路由，然后主路由是由另一个人维护的，我们无法要求主路由给我们映射管理端口。我们将该设备接入到云穿透就可以实现管理了。

3. 优化稳定及延时来管理跨运营商的业务点 MikroTik 设备。

例如业务点为电信线路，我们维护工程师所在的线路是联通或者移动。我相信大家都知道咱们的国情，最远的距离不是中国到欧洲，而是电信到联通。在中国跨运营商互联互通问题非常严重。云穿透为多线BGP接入，兼容所有国内网络运营商。



4. 优化稳定及延时来管理跨国业务点 MikroTik 设备。

例如有维护点在马来西亚或者尼日利亚这些较远的国家，国内直连的话会有相当严重的丢包，几乎卡的无法正常进行运维操作。云穿透有海外专用服务器，采用电信CN2国际加速节点，让我们的业务就算维护到天涯海角也能如丝般顺滑。

5. 映射到业务点内的其他网络设备。（交换机，远程桌面等。）

例如我们维护的MikroTik设备下面有个WINDOWS服务器，我们可以通过云穿透来映射3389端口到MikroTik，然后MikroTik设备再映射给该WINDOWS服务器。也可以用来映射交换机的TELNET及SSH服务。

6. 及时了解所有业务点 MikroTik 设备在网情况。

例如当大家维护相当多的业务点，先定个小目标维护100个业务点。那么我们如何实时了解所有维护点的在网情况？这个时候就需要云平台进行监控所有业务点情况。很高兴告诉大家，云穿透平台也提供了这个功能。业务点从穿透平台上线及下线均可以提供邮件通知。



MikroTik-A

MikroTik-B

端口:8291-Winbox

PPTP/L2TP/SSTP/OVPN

PPTP/L2TP/SSTP/OVPN

端口: 8291-Winbox

云穿透服务器

服务器端口:10001

服务器端口:10002

运维人员

Interface List

Interface	Name	Type	Actual MTU	L2 MTU	Tx	Rx
R	CLAN	L2TP Client	1450		0 bps	0 bps
R	SZ2	OVPN Client	1500		30.6 kbps	3.5 kbps
R	ether1	Ethernet	1500	1598	0 bps	0 bps
R	lte1	LTE	1500		37.1 kbps	11.6 kbps

Address List

Address	Network	Interface
10.65.17.244/24	10.65.17.0	lte1
172.34.56.32	172.34.56.1	SZ2
172.163.187.97	172.163.187.1	CLAN
192.168.88.1/24	192.168.88.0	ether1

Interface <lte1>

General Status Traffic

Name: lte1

Type: LTE

MTU: 1500

Actual MTU: 1500

L2 MTU:

MAC Address: 00:0A:38:F0:00:00

User:

Password:

Network Mode: ☐ GSM ☐ 3G ☒ LTE

Interface List

Interface	Name	Type	Actual MTU	L2 MTU	Tx	Rx
R	CLAN	L2TP Client	1450			0 bps
R	SZ2	OVPN Client	1500		339.8 kbps	0 bps
R	ether1	Ethernet	1500	1588		0 bps
R	ether2	Ethernet	1500	1588	372.6 kbps	
R	ether3	Ethernet	1500	1588		0 bps
R	ether4	Ethernet				0 bps
R	ether5	Ethernet				0 bps
R	ether6	Ethernet				0 bps
R	ether7	Ethernet				0 bps
R	ether8	Ethernet				0 bps
R	ether9	Ethernet				0 bps
R	ether10	Ethernet				0 bps
R	ether11	Ethernet				0 bps
R	ether12	Ethernet				0 bps
R	ether13	Ethernet				0 bps

Address List

Address	Network	Interface
10.10.10.1/24	10.10.10.0	ether3
10.181.28.15/22	10.181.28.0	ether1
172.34.56.230	172.34.56.1	SZ2
172.163.187.252	172.163.187.1	CLAN
192.168.3.123/24	192.168.3.0	ether2



03

云穿透接口

注册、开通、测试、注意事项

云穿透接口的注册、开通、测试、注意事项



打开<https://cts8.cat-home.org/>注册一个账号，这个账号将用于之后的自助管理和VPN拨号使用。



注册账号后在本穿透平台的WEB管理后台里添加映射信息。比如把本穿透服务器的12345端口映射给本VPN客户端的8291端口（WINBOX端口）。



在需要穿透管理的MikroTik设备里添加VPN拨号，比如使用L2TP的话，填入IP及平台注册的账号密码即可。

穿透服务器
上的端口

发送通知的
邮箱地址

当前已映射
的内容

当前业务点
在线状态

登录上海内测服(106.15.136.2)成功！

欢迎用户test回来！

添加映射

穿透端口(10000-60000):

14334

本地端口(0-65535):

8291

备注(必填):

懒的写

添加

修改VRF标识 (当前VRF标识:98648977)

VRF标识:

98648977

修改VRF

修改密码

新密码(4-16位长度):

再次输入新密码:

修改密码

邮箱地址

邮箱:

9939781@qq.com

修改邮箱

状态通知

当前状态: 关闭

开启通知

退出登录

映射状态(上限3条)

穿透端口	本地端口	备注	操作
29041	8291	懒的写	删除

上次离线时间: 2017/09/12 14:32:16

当月累计使用流量: 0M/5000M

在线状态

用户名	协议类型	在线时间	链接IP	动作
-----	------	------	------	----

MikroTik设
备的端口



当MikroTik设备显示VPN拨号成功的时候，在穿透平台WEB后台里就可以看到客户端上线信息了。其中包括用户名、接入协议类型、在线时间、IP等信息。还可以生成自动修复协议脚本，防止部分VPN协议可能有干扰造成的云穿透无法连接的情况。



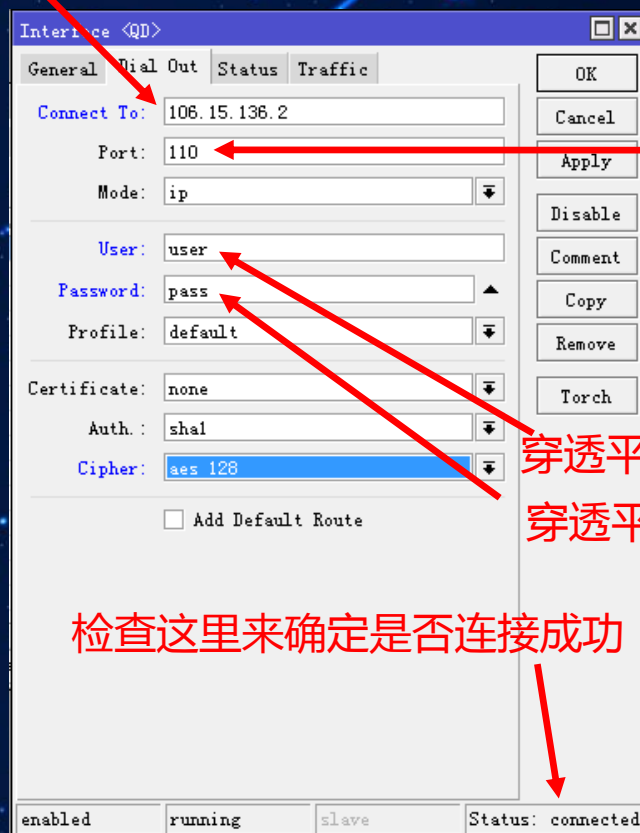
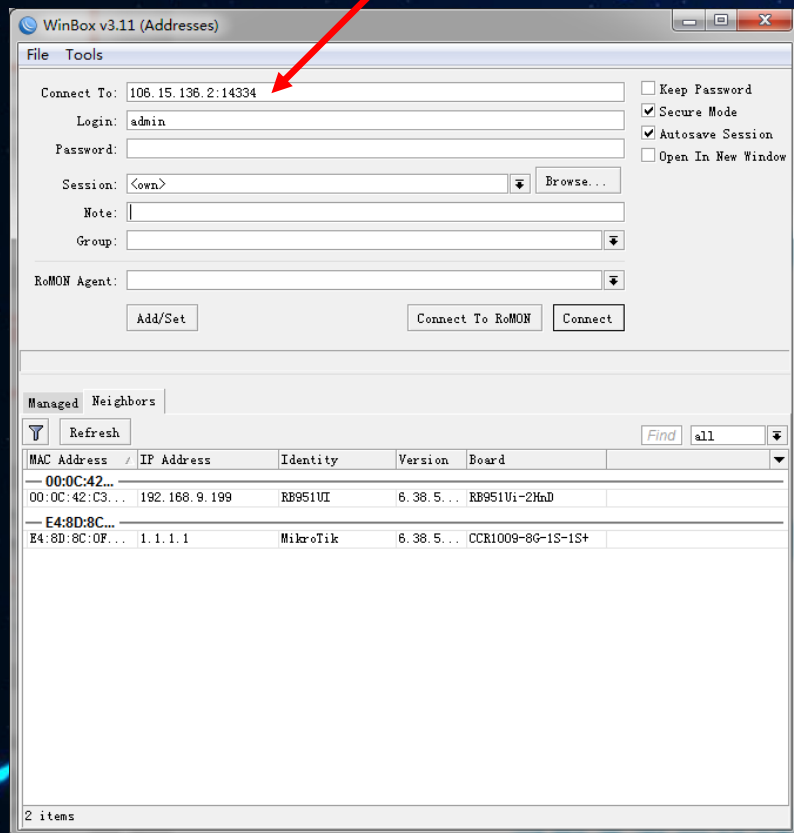
在WINBOX登录只需填写平台服务器IP地址和映射的端口号，就可以完成穿透管理了。（比如 `cts7.cat-home.org:12345`）



注意事项：映射中的穿透端口为您在本穿透服务器上使用的端口，本地端口为自己设备的对应服务管理端口。仅提供TCP协议穿透。建议添加自动修复穿透脚本，防止到云穿透VPN出现异常时无法进行穿透管理。

连接穿透服务器IP和添加的穿透端口

穿透服务器IP



穿透协议端口

穿透平台注册的用户名

穿透平台注册的密码

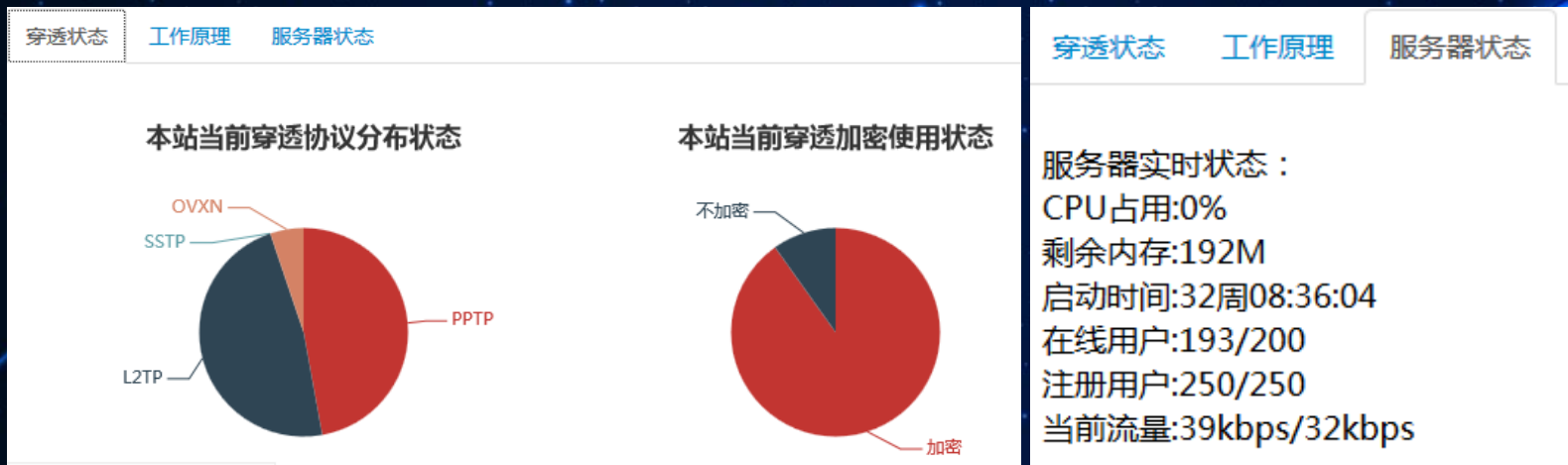
检查这里来确定是否连接成功



04

云穿透接口 服务器的公开信息状态

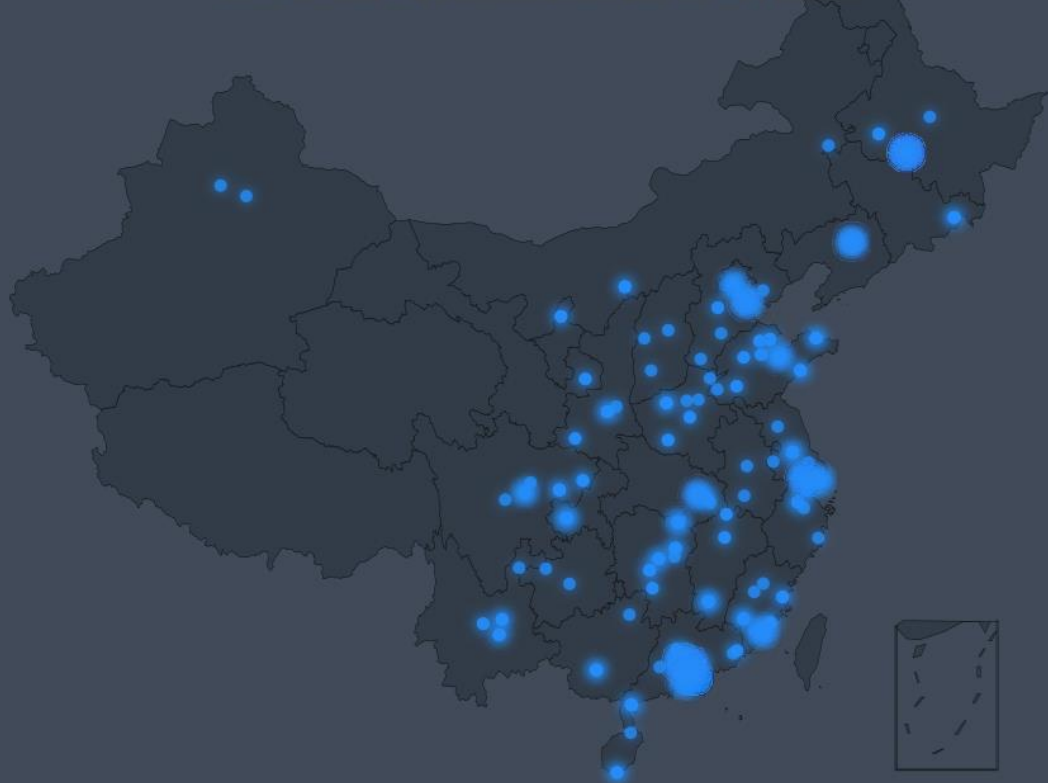
穿透接口服务器状态公示，确保大家都能随时了解自己所用的穿透接口服务器负载情况和其他用户当前使用方式。服务器有没有满载或者超载一目了然，让大家用起来更放心。



04

云穿透服务器的公开信息状态。

VPN穿透平台客户端节点分布汇总(每天更新)-共745个终端在线



截至2017.11.03
平台用户数据汇总



05

云穿透接口 未来展望

ISP正在加速拨号宽带的内网IP更换。这不是个别运营商的行为，而是国内所有运营商都在这么做。预计目前最少有20%的拨号宽带已经是分配内网IP了。曾经是公网IP的拨号宽带，也会被运营商偷偷换成内网IP。

云穿透接口具备比传统DDNS具备更高效的解析速度，更及时的业务点监测异常通知，和更稳定的管理链路。传统DDNS域名解析的方式已经对于目前的网络趋势无能为力，大家对穿透管理的需求会越来越强烈，对穿透接口质量要求也会越来越高。而我有信心用云穿透接口来解决大家的运维问题，并且云穿透所有功能对于使用者都是免费的，现已持续免费两年，目前仅存在流量限制。在全国开放了6个服务器分布在不同地域，在香港CN2线路开放了1个服务器。希望大家不要将商业性质的业务带到云穿透，比如监控，流媒体等大流量长期占用宝贵的带宽。仅仅用于管理网络设备，我相信能一直免费下去，并且会随着用户量的增加继续增加云穿透服务器或带宽，确保一流的穿透成功率，如丝般顺滑的穿透维护体验，让您在网络运维的世界里畅通无阻！

当前云穿透接口还新增了测试版云交换功能，也是免费的，但是总带宽被限制为1M。商业版云交换由于使用商业级别的线路资源和高品质维护标准，成本高昂所以需要额外支付费用。（商业版正在建设中。）



演示WAP LTE kit使用穿透接口实现远程管理



高厚网络商城

专注Mikrotik设备，一辈子的兴趣...

演示设备由高厚网络赞助

www.gaohou.com
中国成都唯一有仓的mikrotik代理

谢谢观看！

熊茂祥

QQ：9939781

手机：13296699163

博客：ROS6.COM