麒麟 SSL VPN 使用指南

系统安装部分:

- 1. 生成一个初始化的 centos7.x 64bit,系统需要有 yum 源
- 2. 下载 get.tosec.com.cn/vpn.tar.gz 到/tmp 目录
- 3. 运行如下命令

```
cd /tmp
tar xpvf vpn.tar.gz
bash yum.sh
bash install.sh
init 6
```

- 4. 4.找厂商生成许可(其它-licenses 菜单点击生成)
- 5. 管理员部分:

SSL VPN 主机配置主要分为三步,网络策略设置(用于打开 VPN 服务器服务端口)、 创建 VPN 用户(用于 VPN 连接认证)、创建 VPN 路由(指定哪些 IP 或网段使用 VPN 隧道 连接)

1. 安全策略配置

VPN 需要向公网开放 2 个端口, TCP 443 和 UDP 7286。

TCP 443 为管理端口,打开后管理员可以使用浏览器登录并设置用户和路由,普通用户可以登录并且修改密码。

UDP 7286 为 VPN 端口,用户通过连接 VPN 端口连接到内网

比如在云主机安全策略中,需要设置如下二条即可完成网络配置:

入站规则出站规则

添加规则	导入规则	排序	删除	一键放通	教我设置已		
来源 ()			协议端口 ①		策略	备注	操作
0.0.0/0			TCP:443		允许		編辑 插入 ▼ 删除
0.0.0/0			UDP:7286		允许	-	编辑 插入 🔻 删除

2. 创建 VPN 连接帐号

系统安装完成后,使用 <u>https://ip</u> 可以访问到系统管理界面,默认口令为 admin/12345678。

用户需要使用 VPN 必须具有一个 VPN 帐号,使用 admin 登录后可以创建 VPN 帐号。 点击 资源管理-用户管理 菜单,点击添加按钮

VPN接入系统	₽	首页								adm 管理
8月户管理 ^	用户	名:	柳定 显示的	2日录○ 日录截取☑						
8.用户管理	选	用户名	用户姓名	运维组	VPNIP	令牌状态	生效时间	结束时间	角色	操作链接
		Ladmin	超级管理员	堡垒机默认管理员		未绑定	2000-01-01 00:00:00	永不过期	管理员	🚰 蒸用 🥜 编辑
■ 堡垒机默认管理员(1		添加用户 删除	用户 批量编辑				导入	导出 共1个用	户首页 上一页	瓦1 下一页 末页 页次: 1/1页 20个/员
會 用户组管理		1								
④ 在线用户		1								

*用户名:	testvpn	*真实姓名:	testvpn	
*密码:	随机密码 要中	强 *确认密码:		强制修改密码
*用户组:	用户组: 堡垒机默认管理员	证书CN:		
电子邮件:		手机号码:		
工作单位:		工作部门:		
生效时间:	2019-04-10 08:05:54 选择时间	过期时间:		选择时间 永不过期
VPN :		VPN IP		
用户权限:	认证用户 ▼	动态口令卡:	含有字符	未绑定 ▼ 5

3. 创建内网访问路由

内网访问路由是用户连接 VPN 后访问的内网资源 IP 或网段,只有在 VPN-路由中添加 相应的网段或 IP 后,才通过 VPN 隧道访问这些 IP 或网段。

在 VPN 管理-VPN 路由中,点击增加按钮可以增加一条 VPN 路由,点击生效按钮即可 生效

IP	掩码	路由状态	操
72.27.0.0	255.255.0.0	●启用	★删除
92.168.0.52	255.255.255.255	●启用	★删除
92.168.0.54	255.255.255.255	●启用	★ 删除
92.168.0.55	255.255.255.255	●启用	★謝除
92.168.0.57	255.255.255.255	●启用	★ 删除
72.27.16.0	255.255.255.0	●启用	★删除
92.168.0.50	255.255.255.255	●启用	X 删除
増加 生效 🔶			
▶ 1 先占憎加	按钮增加内网云主机IP或网段		

注意: VPN 路由添加后,所有的 VPN 服务会重新启动,所有的 VPN 客户端都需要断 开重拨才能继续使用。

用户使用部分:

Windows 客户端

1. 安装

程序下载地址: http://get.tosec.com.cn/soft/sslvpn-win-64.zip 注意事项: XP、2000、2003、Vista 必须以管理员登录进行安装 Windows 7、10 必须采用以管理员身份进行安装 Windows 8 必须管理员身份使用兼容 Windows 7 方式进行安装



3.程序将自动启动安装,安装完毕后,点击完成按钮即可以退出安装

4.启动 VPN 系统, VPN 安装好以后, 在菜单中会产生一个 VPN 的菜单, 点击菜单里的 VPN 即可以启动 VPN 软件

🔰 VPN	默认桯
	帮助和
Vpn Windows — 缺还值	运行
WinPcap	

VPN 启动后在 Windows 右下角的工具栏会产生一个图标:



5. 设置 VPN 服务器, 鼠标右击 VPN 图标, 选择"系统配置"菜单



系统会打开 VPN 服务器对话框,在服务器 1 中输入堡垒机外网 IP,点击确认按钮即 完成设置

服务器1	192. 168. 1. 1	端口1.7286
版方喆4:		
服务器3:		端口3:
服务器4:		端口4:
服务器5:		端口5:
重命名:	VPN服务 使用前领	-器外网IP地址 需要已经映射
TA	UDP 728	36端口

6. 用户使用,鼠标右击 VPN 图标,选择"连接"菜单,即可以进行连接,在连接对话框 中输入堡垒机的用户名、密码,即可以登录:

用户名:	admin
密码:	******
	☞ 记住密码
登	录 取消

登录后, VPN 图标即可以显示为绿色, 这时即可以通过堡垒机访问内网



7. VPN 连通后访问堡垒机: VPN 连通后,即可访问已经在 VPN 路由中发布的主机和网 段

苹果 MACOS 使用

客户端下载地址:

http://get.tosec.com.cn/soft/sslvpn-macos.zip

1. 双击压缩包软件 Tunnelblick_3.7.8_build_5180.dmg,出现如下图



2. 双击 "Tunnelblik"文字上的图标, 会弹出窗口, 输入 mac 系统帐号密码, 完成以后 就安装完毕。安装后系统会问询是否有配置,选择"我没有配置文件"退出

EVAS	欢迎使用 Tunnelblic 没有已安装的 VPN 配置. Tunnelblick 需要一个或: 你的网络管理员或 VPN 服 能使用.	k 多个已安装的配置才能连接 V 服务提供者提供. 这些文件必须	PN. 配置文件通常会由 项安装到 Tunnelblick 才
	配置文件的后缀包括 .tbll	k, .ovpn, 或 .conf.	
	(其它相关文件会有不同后	5缀; 暂时不要理会这些文件.)	
	你有配置文件吗?		
	退出	我没有配置文件	我有配置文件

3. 将压缩包中的 config 目录解压, 打开 config 文件夹, 使用文本编辑器修改 vpn.ovpn 的配置, 把其中的 ip 改为目标 vpn 服务器的外网映射 IP, 编辑完退出。



4. 然后双击该配置文件,弹出窗口,选择"只是我",系统会自动用 tunnelblick 打开, 并配置好 vpn。



然后后就可以点击下图 tunnelblick 图标,下拉选择连接 VPN 菜单

* *	A B R R R 85% (4)	拼
	没有已建立的连接	
	VPN 详情	
	连接 vpn	
选项	退出 Tunnelblick	

弹出输入用户名和密码的窗口,输入 VPN 用户名和密码,如果有动态口令,则在密码处 输入静态口令和动态口令的连接字符串

用户名:		
	✓ 储存于 Keychain	
密码:		
	🦳 储存于 Keychain	
	取消	确定

输入完点击确定,vpn 就开始连接,如果认证通过,很快就会连接上。连接成功。如图 图标变亮了。



安卓平台使用

安卓版本 VPN 客户端下载地址:

http://get.tosec.com.cn/ ics-openvpn-0.7.8.apk

配置文件下载地址:

http://get.tosec.com.cn/config.zip

1. 在 windows 中解压的 config.zip, 里面有一个使用记事本打 vpn.ovpn 文件, 修改 remote 行, 将 IP 修改为 VPN 服务器公网 IP

ypn.ovpn	2017/12/31 17
/// vpn-tech	2016/3/9 20:31
🥘 vpn.ovpn - 记事本	
文件(F) 编辑(E) 格式(Q) 查看(V), 帮助(H), 网口	
client dev tun proto tcp remote 88443 remote-random resolv-retry infinite	

2. 将所有的文件再次打包成 vpn.zip (注意最好用 zip,不要用 rar,不然有可能在安卓系统 中打不开:

	€ 压缩	文件名和	参数					?	\times
🚽 ca				1.4.14	2.1				
🚽 vpn	吊规	高级	选项	又件	备份	时间	汪释		
vpn	压缩	→件名(Α)				浏览	(<u>B</u>).	
vpn.ovpn	vpn	zip							$\overline{}$
🧾 vpn-tech	● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●								-
	配置(E) 添加并替换文件						~		
	一压线	缩文件格:	đ	压缩选项					
	0	RAR(<u>R</u>)		□ 压缩后删除源文件(L)					
	I.				创建自解 创建国家	压格式压 正缩立件	缩文件(<u>X</u>) (s))	

- 3. 在安卓平台上安装附件中的安卓 openvpn 安装包,只需要默认安装即可
- 4. 将第 2 步打包的 vpn.zip 使用 qq 或微信解包,解压后放在安卓设备(一定要解压),记 住文件目录位置
- 5. 打开第3步安装的安卓 openvpn,点击下图位置



6. 点击后会弹出文件管理器,找到第4步解压的位置,选择 vpn.ovpn

Ca.crt	wpn-tech.key
1.39 KB 下午5:06	636 B 下午5:06
◎ vpn.crt	vpn.key
3.99 KB 下午5:06	887 B 下午5:06
	点击这里

7.在配置文件名称处输入一个名称(自定义,标识用),然后点击右上方的勾



7. 在配置文件中点击刚才导入的名称,出现用户名和密码对话框,输入 VPN 用户名和密码(建议勾上保存密码)然后点击连接

酉	置文件	GRAPH	设置	FAQ	关于	
vp	需要请为限	Passw 配置文件	vord vpn 输2	、密码		1
	vpn					1
	 显示 	密码				

8. 出现 VPN 连接日志,显示整个连接过程,直到最后一行出现 completed,即表示连接成功,点左上角的返回按钮

F	OpenVPI	「日志」			
已连接:	SUCCESS,10.11.	0.6,1	,84	443,10	153.
下午5:27 remote-c	7 WARNING:ns cert-tls instead.	-cert-type is	DEPREC	ATED.	Use ·
下午5:27 address	7 TCP/UDP: Pres : [AF_INET]1	erving recei	ntly used 443	remote	e
下午5:27 [AF_INE	7 Attempting to e	establish TC :8443 [nonb	P connectored	tion w	ith
下午5:27 [AF_INE	7 TCP connectio	n establishe :8443	d with		
下午5:27	TCP_CLIENT lin	nk local: (no	t bound)		
下午5:27 [AF_INE	TCP_CLIENT lin	nk remote: :8443			
下午5:27 passwor prevent	7 WARNING: this rds in memory – this	configuration use the aut	on may ca h-nocach	ache e optio	n to

9. 屏上显示出 VPN 当前状态,这时如果 VPN 已经发布了内网应用即可以连接到内网进行 操作

故障排查:

1.		
☑ _ Microsoft 网络客户端		٨
☑ 🠙 Microsoft 网络的文件和打印机共享		
HPE Network Virtualization Driver		
🗹 🏪 VirtualBox NDIS6 Bridged Networking Driver		
☑ 🥎 QoS 数据包计划程序		
☑ 💶 Internet 协议版本 4 (TCP/IPv4)		
🗌 🔔 Microsoft 网络适配器多路传送器协议		
✓ Microsoft LLDP 协议驱动程序		~
<	>	