

IPSEC 配置文档

V 1.1

客服部

深圳市磊科实业有限公司





版本控制

版本号	修改说明	修改人	修改时间
V1.1	初次撰写	Quhy	2013. 04. 8





第1章	IPSEC VPN 组网	1
1.1	组网拓扑图	1
1.2	适用范围	1
第2章	磊科 IPSEC VPN 配置	2
2.1	网对网模式	2
	2.1.1 服务器模式	2
	2.1.2 对等模式	4
	2.1.3 IPSEC VPN 状态显示	5
2.2	点对网模式	6
	2.2.1 服务器配置	6
	2.2.2 XP 系统创建 VPN 拨号连接	6
	2.2.3 Win7 系统创建 VPN 拨号连接	10





第1章 IPSEC VPN 组网

1.1 组网拓扑图





如上示意图,常见的 VPN 组网方式有两种:

- 1. 子网和子网通过 IPSEC VPN 互联,下文简称网对网模式
- 2. 主机和子网通过 IPSEC VPN 互联,下文简称点对网模式

1.2 适用范围

适用的产品型号包括但不限于: 286、286E、288、289E、255V、256、256P、266、266E、268。



第2章 磊科 IPSEC VPN 配置

2.1 网对网模式

这种模式常用于总公司和分公司之间的 VPN 互联

该文档以 NR286 做对等模式(内网 192.168.1.0/24)、NR289-E(内网 192.168.10.0/24)做服务器模 式演示。

2.1.1 服务器模式

一、进入配置界面,选择"VPN"--"IPSEC设置"。

▶ IPSec设置					
状态:	启用 ▼				
名称:	admin]			
认证模式:	PSK © RSA				
密码:	•••••				
模式:	◎ 服务器模式 《) 对等模	元		
外出接口:	WAN1 -				
对端IP地址:	0.0.0.0] (可輸入地	或名和IP地址,0.0.0	0.0代表任意地址)	
本地子网:	需要通过IPSec加密保	护的源IP	范围,网对网时需	要设置。	
本地子网1:	192.168.10.1	掩码:	255.255.255.0	(可选)	内网IP
对端子网:	需要通过IPSec加密保	护的目的	[P范围,一般为》	寸端设备内 <mark>网网</mark> 印	<u>次</u> 文。
对端子网1:	192.168.1.1	掩码:	255.255.255.0	(可选)	

图 2

状态:选择启用, IPSec 下方的配置才会生效。

. net·core 磊科[°]

名称:为该 IPSEC 服务器设置相应的名称,方便记忆。

认证模式:即 IPSEC 的加密方式。选择 PSK 模式则填写预共享密码,对等模式拔号时需要填

入该密;选择 Rsa 则在右边 Rsa 密码设置里面点击生成。

模式:由于本端是服务器,故此处选择"服务器模式"。

外出接口:选择你连接 IPSec 的 WAN 口。

本地子网:填写本端路由器 LAN 口网段及子网掩码,此处为 192.168.10.1。

对端子网:填写对端路由器 LAN 口网段及子网掩码,此处为 192.168.1.1。

二、若有多个对等模式同时拔入本服务器,则需要选择"高级设置",填入其他对等模式的内网 IP 网段。最多可以支持三个对等模式同时拔入,其他参数强烈建议保持默认。具体界面如下图所示:

高级设置						
本地子网2:		掩码:		(可选)	
本地子网3:		掩码:		(可选)	
对端子网2:		掩码:		(可选)	
对 端了 网3:		掩码:		(可选)	
本地ID:		<mark>(可选)</mark>				
对端ID:		<mark>(可选)</mark>				
协商模式:	◎ 主动模式 ◎	侵略模式	(仅特殊情》	兄使用)		
通道模式:	◎隧道模式 ◎	传输模式	(仅特殊情》	紀使用)		
阶段一:	加密算法 自动 🔻	认证算法	自动 🔹	DH group	自动	•
协议:	● ESP(支持加密)	© AH	(仅特殊情》	紀使用)		
阶段二:	加密算法 自动 🔻	认证算法	自动 🔹	DH group	自动	•
PFS :	● 开启 ○ 关闭	9				
DPD :	60 秒					







由于本例中只有一个对等模式,故不需要设置"高级设置"。

2.1.2 对等模式

进入配置界面,选择"VPN"--"IPSEC设置"

▶ IPSec设置			
状态:	启用 ▼		
名称:	admin		
认证模式:	● PSK © RSA		
密码:	••••		
模式:	◎ 服务器模式 🛛 💿	对等模式	
外出接口:	WAN1 -		
对端IP地址:		(可輸入域名和IP地址, 0.0.0.0f	代表任意地址)
本地子网:	需要通过IPSec加密保护	的源IP范围,网对网时需要	砂置.
本地子网1:	192.168.1.1	掩码: 255.255.255.0	(可选) 内网P
对端子网:	需要通过IPSec加密保护	的目的IP范围,一般为对端	设备内网网段。
对端子网1:	192.168.10.1	掩码: 255.255.255.0	(可选)

图 4

认证模式:必须与服务器设置的认证模式一致。

密码: 必须与服务器端密码一致。

模式:选择"对等模式"。

对端 IP 地址:填入服务器端 IP 地址。





2.1.3 IPSEC VPN 状态显示

一、在服务器端,点击"IPSEC 状态",查看 IPSEC VPN 连接状态,如下图所示:

IPSec设置	E RSA3	翻设置	IPSec状态	IPSec日志		帮助
PSec状态	5					
序列号	本端IP		本端子网	对端IP	对端子网	规则名
1		192.168.3	10.0/255.255.255.0		192.168.1.0/255.255.255.0	tt
8+8-	数量: 10 🌛 🚦	雪雨 上—雨 ⁻	下一页 屋页 1/1	▼ 当益-1 冬	沃利·9 冬	

图 6

二、在对等模式端,点击"IPSEC 状态",查看 IPSEC VPN 连接状态,如下图所示:

IPSec设置	RSA密	月设置 IPSec	状态		IPSec日志		帮助
IPSec状态							
序列号	本端IP	本端子网			对端IP	对端子网	规则名
1		192.168.1.0/255.255	5.255.0	-		192.168.10.0/255.255.255.0	admin
最大显示数	虛: 10 🧹 首	页 上一页 下一页 尾页	1/1	•	当前:1 条	还剩:9 条	
最大显示数	'建: 10 💉 首	页 上一页 下一页 尾页	1/1	▼	当前:1 条	还剩:9 条	
			冬	7			

三、正常访问对端网段:

C:\Users\qiulb>ipconfig	
Vindovs IP 配置	
以太网适配器 本地连接: 连接特定的 DNS 后缀 : 本地链接 IPv6 地址 : fe80::6ca7:529 IPv4 地址 : 192.168.1.2 子网掩码 : 255.255.255.0 默认网关 : 192.168.1.1	C:\Users\qiulb>ping 192.168.10.218 正在 Ping 192.168.10.218 具有 32 字节的数据: 来自 192.168.10.218 的回复: 字节=32 时间=599ms II 来自 192.168.10.218 的回复: 字节=32 时间=589ms II 来自 192.168.10.218 的回复: 字节=32 时间=591ms II 来自 192.168.10.218 的回复: 字节=32 时间=593ms II





2.2 点对网模式

这种模式常用于员工出差在外和公司之间的安全互联。 该文档以 NR289-E(内网 192.168.10.0/24)做服务器演示。

2.2.1 服务器配置

请参考本文档 2.1.1 章节

2.2.2 XP 系统创建 VPN 拨号连接

第一步、打开网络连接:

如果桌面上没有"网上邻居", 依次点击"开始"菜单→"设置"→"控制面板"→"网络连接"; 如果桌面上有"网上邻居", 直接用鼠标右键点击"网上邻居", 再点击"属性";

第二步、创建 VPN 连接:







net·core磊科



• net·core 磊科[°]

深圳市磊科实业有限公司

新建连接肖导
连接名 指定连接到您的工作场所的连接名称。
在下面框中输入此连接的名称。
公司名 (A)
公司名称任意
例如,您可以输入您的工作地点名或您连接到的服务器名。
< 上一步 (B) 下一步 (B) > 取消
图 11
新建连接向导
公用阿络 Windows 可以先确认公用网络是否已接好。
Windows 在建立虚拟连接之前可以自动拨到 Internet 或其它公用网络的初始 连接。
● 不拨初始连接 @)
○ 自动拨此初始连接 (A):
,
< 上一步 (B) 下一步 (B) > 取消





net·core 磊科

图 13

此处填写 VPN 服务器的公网 IP,继续点击下一步,即可完成新建连接

第三步、开始连接:双击 VPN 拨号连接(类似于宽带拨号连接),输入帐号和密码即可连接。 如果需要修改 VPN 服务器的 IP, 右键点击属性修改

◆ 公司VPN 雇性	? ×
常规 送项 安全 网络 高级	
目的地的主机名或 IP 地址 @D microsoft.com 或 157.54.0.1)例:	
119, 119, 119, 119	
─ 第一次连接───── 在试图建立虚拟连接之前,Windows 可以先连接到公用 网络,如 Internet 上。	

图 14

备注: 电脑单机 VPN 拨号, 如果连接不成功, 可根据第三步步骤, 选择"选项", VPN 模式修 改为"IPSEC"。若依旧拔号不成功,会有错误代码提示,根据对应代码可以到网上搜索连接失败的





原因及解决办法

2.2.3 Win7 系统创建 VPN 拨号连接

第一步、打开网络和共享中心:

如果桌面上没有"网络"图标,依次点击"开始"菜单→"控制面板"→"查看网络状态和任务";如果桌面上有"网络",直接用鼠标右键点击"网络",再点击"属性";

第二步、创建 VPN 连接:



图 15





🕞 🔮 设置连接或网络 选择一个连接选项 📢 连接到 Internet 设置无线、宽带或拨号连接,连接到 Internet。 . **全計 设置新网络** 全型 配置新的路由器或访问点。 手动连接到无线网络 连接到隐藏网络或创建新无线配置文件。 车接到工作区 受置到您的工作区的拨号或 VPN 连接 **设置拨号连接** 使用拨号连接连接到 Internet。 下--步(N) 取消 图 16 🚱 🔓 连接到工作区 · · · 您想如何连接? ◆ 使用我的 Internet 连接(VPN)([) 通过 Internet 使用虚拟专用网络(VPN)来连接 D → 直接拨号(D) 不通过Internet直接使用电话号码来连接。 <u>什么是 VPN 连接?</u> 取消

图 17



			1/18/711	1-1-1-1-1
G	La 连接到工作区			
	键入要连接的 Interne	et 地址		
	网络管理员可提供此地址。			
	Internet 地址(I):	119.119.119.119]	
	目标名称(E):	上面輸入VPN服务器的公网IP。此处可以任意輸入		
	 使用智能卡(S) 允许其他人使用此连接 这个选项允许可以访问 现在不连接;(又进行) 	倿(A) 可这台计算机的人使用此连接。 设置以便稍后连接(D)		
		世一世	N)	取消
		图 18		
G	上 连接到工作区			
	键入您的用户名和密码	<u>д</u>		
	用户名(U):	qiulb		
	密码(P):	•••••		
	域(可选)(D):	 □ 显示字符(S) ☑ 记住此密码(R) 		

图 19

创建(C)

取消

点击创建,完成连接。

net·core 磊科[。]

第三步、开始连接:双击 VPN 拨号连接(类似于宽带拨号连接),输入帐号和密码即可连接。如果需要修改 VPN 服务器的 IP,右键点击属性修改



. net core a	•种*	
		深圳市磊科实业有限公司
	 VPN连接 属性 常规 选项 安全 网络 共享 目的地的主机名或 IP 地址 (如 microsoft.com 或 157.54.0.1 \ 3ffe:1234::1111) (出): 119.119.119 第一次连接 	

图 20

在试图建立虚拟连接之前,Windows 可以先连接到公用 网络,如 Internet 上。

备注: 电脑单机 VPN 拨号,如果连接不成功,可根据第三步步骤,选择"选项", VPN 模式修改为"IPSEC"。电脑单机 VPN 拨号,如果连接不成功,会有错误代码提示,根据对应代码可以到网上搜索连接失败的原因及解决办法

