两台mGuard如何通过Internet建立VPN连接

修订号: V1.0

作 者: CCAX / XGC

硬件:

序号	型号	HW/FW
1	FL MGUARD RS4000 TX/TX VPN	01/7.4.0
2	FL MGUARD RS2000 TX/TX VPN	01/7.5.0

软件:

序号	名称	版本
1		
2		

本文以两台mGuard,两台3G路由器为例,演示如何通过Internet建立VPN连接。假设mGuard2(FL MGUARD RS4000 TX/TX VPN)与一台3G路由器作为VPN连接的主叫方,mGuard1(FL MGUARD RS2000 TX/TX VPN)与另一台3G路由器(使用电信的CDMA2000上网卡,可以获得临时性的公网IP地址)作为VPN连接的等待 方。

1. 首先演示主叫方的配置,将本机IP地址改为与mGuard2的LAN口默认IP地址(192.168.1.1)同网段,如 192.168.1.10。

Internet 协议(TCP/IP)」	禹性 ? 🛛
常规	
	取自动指派的 IP 设置。否则, 适当的 IP 设置。
○ 自动获得 IP 地址(0)	
─●使用下面的 IP 地址(S): -	
IP 地址(I):	192 .168 . 1 . 10
子网掩码 (U):	255 .255 .255 . 0
默认网关 @):	· · ·
◯ 自动获得 DMS 服务器地址((B)
┌️④ 使用下面的 DNS 服务器地址	ult (E):
首选 DNS 服务器(P):	1 4 4 A
备用 DNS 服务器(A):	
	高级(火)
	確定 取消

2. 测试是否可以 Ping 通 mGuard2 的 LAN 口。



3. 在IE浏览器通过mGuard2的LAN口默认IP地址访问mGuard2的配置界面,键入https://192.168.1.1,默认用户名: admin,密码: mGuard。



🚰 mGuard (mguard	d) - Microsoft Inte	rnet Explore	c		
文件(正) 编辑(正) 强	查看(Y) 收藏(A) 工具(T	■ 帮助(H)			
Ġ 后退 🔹 🌍 🔹	🖹 💈 🏠 🔎 搜	索 🥎 收藏夹	🚱 😒 🌺	🖻 📙 ل	
地址 (1) 🙆 https://1	92. 168. 1. 1/				
	NIX ACC VATIONS				
					Login to: mguard
				User Na	me: admin
				Passwe	ord:
				Access Ty	ype: Administration
					Login

4. 进入 Network >> Interfaces,将 Network Mode 更改为 Router,选择相应的 Router Mode: Static/DHCP/PPPoE/PPTP,本例中选择 DHCP 模式(需根据实际应用选择相应模式)。

Management	Network » Interfaces	
System Settings	General Ethernet Dial-out Dial-in Modem / Console	
Web Settings	Network Status	
Licensing		
Update	Evternal IP address 19216811	
Configuration Profiles		
SNMP	Active Defaultroute (none)	
Central Management	Used DNS servers DNS Root Servers	
Restart		
Network		
Interfaces	Network mode	
NAT		
DNS	(Network Mode Router V	
DHCP		
Proxy Settings		
Authentication		
Network Security		
IPsec VPN		_
QoS	Internal IPs IP Netmask	
Redundancy	(trusted port) X 192.168.1.1 255.255.0	_
L a main a		

5. Apply 设置生效后如下图

Management	Network » Interfaces					
Network	General Ethernet Dial-out Dial-in Modem / Console					
Interfaces	Network Statue					
NAT	Herwork Status					
DHCP						
Prov Settings	External Pladaress 192.100.10.100					
Authentication	Active Defaultroute 192.168.10.253					
Network Security	Used DNS servers DNS Root Servers					
IPsec VPN						
QoS	Network Mode					
Redundancy	Network move					
Logging	Network Made					
Support						
	Router Mode DHCP 💟					

6. 接于 mGuard2 的 LAN 口后的设备 IP 地址分配分为 DHCP 模式和非 DHCP 模式。

3 / 9

菲尼克斯电气中国公司 南京江宁开发区菲尼克斯路 36 号



6.1. DHCP 模式

6.1.1. Network >> DHCP, DHCP 模式选择 Server。

Management	Network » DHCP		
Network	Internal DHCP External DHC	p	
Interfaces	Mada		
NAT	Mode		
DUS			
DHCP	DHCP mode	Server 🚩	
Proxy settings			
Authentication	DHCP Server Options		
Network Security			
	Enable dynamic IP address poo	Yes 🗸	
Redundancy	DHCP lease time	14400	
	Drice lease line	14400	
Support	DHCP range star	192.168.1.100	
	DHCP range end	192.168.1.199	
	Local netmask	255.255.255.0	
	Broadcast address	192.168.1.255	
	Default gateway	192.168.1.1	
	DNS server	192.168.1.1	
	WINS server	192.168.1.2	
	Static Mapping	ž4	Client MAC Address

6.1.2. 将本机 IP 地址及 DNS 服务器地址改为自动获得。

Internet 协议(TCP/IP)	属性 ? 🔀
常规 备用配置	
如果网络支持此功能,则可以获 您需要从网络系统管理员处获得	取自动指派的 IP 设置。否则, 适当的 IP 设置。
● 自动获得 IP 地址 (0)	
-○使用下面的 IP 地址(S): -	
IP 地址(I):	
子网掩码 (U):	· · · · ·
默认网关 @):	
● 自动获得 DNS 服务器地址	(<u>B</u>)
─── 使用下面的 DNS 服务器地対	址(E):
首选 DMS 服务器(P):	
备用 DNS 服务器(A):	
	高级(火)
	确定 取消

- 6.2. 非 DHCP 模式
- 6.2.1. Network >> DHCP, DHCP 模式选择 Disabled。

Management	Network » DHCP
Network	Internal DHCP External DHCP
Interfaces	
NAT	Mode
DNS	
DHCP	DHCP mode Disabled 💙
Proxy Settings	
Authentication	
Network Security	
IPsec VPN	
Global	
Connections	

5 / 9

6.2.2. 保证本机 IP 地址与 mGuard2 的 LAN 口默认 IP 地址(192.168.1.1) 同网段, 默认网关及 DNS 服务 器地址使用 mGuard2 的 LAN 口默认 IP 地址。

Internet 协议 (TCP/IP) 属	± ? 🔀
常规	
如果网络支持此功能,则可以获取 您需要从网络系统管理员处获得适:	自动指派的 IP 设置。否则, 当的 IP 设置。
○ 自动获得 IP 地址 @)	
──── 使用下面的 IP 地址(S): ——	
IP 地址(L):	192 . 168 . 1 . 10
子网掩码(U):	255 .255 .255 . 0
默认网关 @):	192 .168 . 1 . 1
○ 自动获得 DNS 服务器地址 (B)	
● 使用下面的 DNS 服务器地址(<u>E</u>):
首选 DNS 服务器 (P):	192 . 168 . 1 . 1
备用 DMS 服务器(A):	· · ·
	高级(火)
	确定 取消

7. 进入 Network >> NAT, 设置 Network Address Translation/IP Masquerading。缺省设置为 External/0.0.0.0/0, 即允许所有内网设备访问外网。

Management	Network » NAT				
Network Interfaces	Masquerading	IP and Port Forwarding			
NAT	Network Address Tr	anslation/IP Masquerading			
DNS					
DHCP	× 4	Outgoing on Interface	From	IP	Comment
Proxy Settings	f 🗆	External 🛛 👻	0.0.0/0		
Authentication					
Network Security	These rules let you specifi	which ID addresses (normally addresses	within the private address space) are to be rewr	itten to the mGuard's (Daddress	
IPsec VPN	<u>Please note:</u> These rules v	von't apply to the Stealth mode.		nich là the mousile 3 h secreta.	
Nos Redundancy					
	1:1 NAT				
Support					
		al network	External network	Netmask	Enable ARP
	<u>Please note:</u> These rules o	nly apply to the network mode "Router" an	I if the router mode is set to "static" or "DHCP".		
8. 导入 mGuard2	的 Machine C	ertificate, 进入,	Authentication >> Ce	rtificates, 选择	择 mGuard 的

南京江宁开发区菲尼克斯路 36 号

Machine Certificate (mGuard2 自身的.p12 文件),输入证书的密码后点 import 导入(证书的制作 可参考相关文档)。

osoft In	ternet Explorer							
K(A) IJ	L(T) 帮助(H)							
6	搜索 🥎 收藏夹 🚱 🔗 😓 📄	<u> </u>	选择文件 查找范围(II):	n Gran dif H		-		? 🔀
ndex. cgi								
	WARNING: THE ROOT WARNING: THE ADMIR	PASSWORD IS NOT CONFIGURE PASSWORD IS NOT CONFIGUR	3 我最近的文档	mGuard1. crt MGuard1. p12 MGuard2. crt				
	Logged in as 'admin'	with role 'admin' from 192.168.1.	() 原面	mGuard2. p12 圓 证书密码. txt				
Authentie	cation » Certificates rtificate settings Machine Certificate	s CA Certificates						
Machin	ne Certificates		影響					
* *	Subject							
	Subject Alternative Names		网上邻居					
	Issuer							
	Validity	From to		文件名(图):	mGuard2.p12		•	打开(1)
	Fingerprint	MD5: SHA1:		文件类型 (I):	所有文件(*.*)		•	取消
	Shortname							
	Upload PKCS#12	Filename:	- AX (mport				
Ŧ	Download Certificate	Current Certificate File						

9. 进入 Network Security >> Packet Filter, 在 Incoming rules 和 Outgoing rules 下,设置 Protocol 为 "All", From IP 为 "0.0.0.0/0", To IP 为 "0.0.0.0/0", Action 为 "Accept"。

work Security » Pack									
Incoming Rules	Outgoing Rules	Rule Records	MAC Filtering	Advanced					
coming									
Gener	al firewall setting Use the t	irewall ruleset below	*						
X N° Interfac	e Protocol	From IP	From Port	Tol	p	To Port	Actio	Comment	Log
1 External	Al 🗸 0.0.0.0	0 .	iny	0.0.0.0/0		any	Accept	×	No
ese rules specify which	traffic from the outside is all	owed to pass to the insid	le.						
<u>ase note:</u> Port settings	are only meaningful for TCP.	and UDP!							
Log entries for unk	nown connection								
	No V								
	attempts?								
	attempts?								Apply
	attempts?								Apply
	attempts?								Apply
ork Security » Packet	attempts? No				_	_	_	_	Apply
ork Security » Packet Incoming Rules	Filter	Rule Records	MAC Filtering	Advanced	_		_	_	Apply
ork Security » Packet Incoming Rules going	Filter Outgoing Rules	Rule Records	MAC Filtering	Advanced	_	_	_	_	Apply
ork Security » Packet Incoming Rules going Coopera	Filter Outgoing Rules	Rule Records	MAC Filtering	Advanced			_	_	Аррђу
ork Security » Packet Incoming Rules going Genera	Filter Outgoing Rules I frewal setting Use the fil	Rule Records	MAC Filtering	Advanced	_	_	_	Los 10: Heattone-A [®] 2016:a0-	Apply
ork Security » Packet Incoming Rules going Genera X II [®] Protocol	Filter Outgoing Rules I frewall setting Use the fil From IP	Rule Records	MAC Filtering	Advanced To IP		To Port	Action	log D:tr-stjolg-N ⁰ 255:30- Comment	Apply 36-135bit-0304
ork Security n Packet ncoming Rules going Genera X N° Protocol 1 1 AI V	Filter Outgoing Rules I frewal setting Use the filt From IP 0.0.0.00	Rule Records	MAC Filtering	To IP	any	To Port	Action Accept V	tog to:teorgolg-/№2356a00 Comment default rule	Арріу 350-1315-0147-03004 Lo
ork Security = Packet neoming Rules going Cenera X II [®] Protocol 1 A V	ettempts? No verification of the second seco	Rule Records rewall ruleset below From Pe stry	MAC Filtering	Advanced To IP	any	To Port	Action Accept ¥	log 10:16-tigelg-A ⁶² 536500- Comment default rule	300-1215-b107-00004 Lo
ork Security - Packet ncoming Rules going Cenera X II Protocol 1 A V	Filter Outgoing Rules I frewal setting Use the fit From IP 0.0.0.00 affic from the inside is allow	Rule Records	MAC Filtering	To IP) any	To Port	Action Accept ¥	Log D: Heatholig-AP-2585aD- Comment default rule	Арріу 36-135-bit-2000 Lo
ork Security - Packet ncoming Rules going Cenera V Protocol 1 AI V erules specify which tr erules specify which tr erules specify which tr	Filter Outgoing Rules Firewall setting Use the filt From IP 0.0.0.00 affic from the inside is allow e only meaningful for TCP a	Rule Records	MAC Filtering	To IP	any	To Port	Action Accept	log Drævitjelig-N°258kaD- Comment default rule	Apple 30-135-047-0000 Lc
ork Security = Packet going Cenera I I AI e rules specify which it e rules specify which it e rules specify which it se rules specify which it se rules specify which it se rules specify which it second for settings ar	Filter Outgoing Rules Firewal setting Use the fil From IP 0.0.0.00 affic from the inside is allow e only meaningful for TCP a won connection No.	Rule Records	MAC Filtering	To IP	any	To Port	Action Accept V	og 8:tertjele-M≊stkat6- Comment deføut rule	Apple 30-135-bit-1-0000 Lc

10. 进入 IPsec VPN >> Connections, 创建一个 VPN 连接, 定义 Name, 点击 Edit 进入相应设置页面。

IPsec VPI » Connections Connections						
₽ ¥ Enabled	Name		Action			
F Yes V	VPNTest		Edit			
			Apply			

7 / 9

本例中,mGuard2 作为 192.168.1 网段(mGuard2 的 LAN 口及其后设备的网段)与 192.168.11 网段 (mGuard1 的 LAN 口及其后设备的网段)之间 VPN 通道的终端。当数据发送就绪时,由此终端建立通道。

IPsec VPN » Connections » VPNTest					
General Authentication Firewall IKE Options					
Options					
A descriptive name for the connection VPNTest					
Enakled Yes 💌					
Address of the remote site's VPN gateway (Ether an IP address, a hostname, or % any' for any IP, multiple clients or cli					
Interface to use for gateway setting %any External 💌					
Connection startup Initiate 💎 主叫方					
Encapsulate the VPN traffic in TCP No 💌					
Transport and Tunnel Settings					
X Enabled Type Local Remote Action Image: Comparison of the state of					

11. VPN 设置 - 伙伴证书的认证

进入 IPsec VPN >> Connections >> VPNTest, 在 Local X.509 Certificate 下选择之前导入的 Machine Certificate, 上传 Remote Certificate (mGuard1的.crt文件)。

soft Internet Explorer	选择义件			🗹 💟
(A) 工具(T) 帮助(H)	查找范围 (I): Com mGuard			
🏠 🔎 搜索 🚖 收藏夹 🤣 🔗 - 🌺 📄 🛄 🏭	● mGuard1 影mGuard1 教長近的文档	. crt . p12		
dex. cg1 WARNING: THE ROOT PASSWORD IS NOT CONFIGURED: WARNING: THE ADMIN PASSWORD IS NOT CONFIGURED	「 「 「 「 「 「 「 」 正 书 密 記 「 い い い こ 」 こ 一 、 、 、 、 、 、 、 、 、 、 、 、 、	. p12 9. txt		
Logged in as 'admin' with role 'admin' from 192.168.1.10	送 我的文档			
IPsec VPN » Connections » VPNTest General Authentication Firewall IKE Options	我的电脑			
Authentication	S			
Authentication method X.509 Certificate	网上邻居			
Local X.509 Certificate mGuard2 📀				
Remote CA Certificate No CA certificate, but the Remote Certificate below 💌	文件名 (2):	mGuard1.crt	-	打开 (0)
Remote Certificate No Certificate installed.	文件类型 (王): 所有文件 (*. *)	•	取消
Filename (*,pem): 图视	Upload			

VPN Identifier

这样 mGuard2 的设置完毕。

12. 等待方即 mGuard1 端 3G 路由器的配置如下:

中国电信 ____ 智能模式 已连接 ~~~ 首页 网络设置 无线设置 防火墙 系统管理 局域网设置 您可以启用/停止以及设置所有的网络功能。 局域网设置 IP 地址 192.168.169.1 子网掩码 255.255.255.0 MAC 地址 9C:41:7C:0F:18:15 服务器 DHCP 类型 • 起始 IP 地址 192.168.169.2 192.168.169.254 结束 IP 地址 确定 取消 启用端口转发: 首本語口種些

里个端口转发	Ž.				
设置		启用	•		
IP地址		192.16	8.169.2		
外网端口		4500			
内网端口		4500			
协议		UDP			
注解					
最大支持规则	数目为30			确定	重设
当前单个端口	口服务器				
编号	IP地址	外网端口	内网端口	协议	注解
1 🗖	192.168.169.2	500	500	UDP	
2 🗖	192.168.169.2	4500	4500	UDP	
				选择删除	重设

13. mGuard1的Network >> Interfaces中的设置:

Network » Interfaces					
General Ethernet Dial-out Dial-in Modem / Console					
Network Status					
External IP address 192.168.169.2 由3C路由器自动分配					
Active Defaultroute 192.168.169.1					
Used DNS servers 192.168.169.1					
Network Mode					
Network Mode Router 🖃					
Router Mode DHCP -					
Internal Networks					
Internal IPs IP		Netmask	Use VLAN	VLAN ID	
(trusted port)	的LAN口IP地址 255.255	.255.0		1	
Additional Internal Routes Netwo	k		Gateway		

14. mGuard1的 IPsec VPN >> Connections >> VPNtest 中的设置:

IPsec VPN » Connections » VPNtest					
General Authentication Firewall IKE Options					
Options					
A descriptive name for the connection VPNtest					
Enabled Yes 💌					
Address of the remote site's VPN gateway (Either an IP address, a hostname, or '% any' for any IP, multiple clients or clients behind a NAT gateway.)					
Interface to use for gateway setting %any External	0.0.0.0				
Connection startup Wait					
Encapsulate the VPN traffic in TCP					
Transport and Tunnel Settings					
🗜 🗶 Enabled Type 🔄	Local	Remote			
Tunnel	192.168.11.0/24	192.168.1.0/24			

- 15. mGuard1 NAT 设置, Packet Filter 设置等均与 mGuard2 相同, mGuard1 的证书导入方法与 mGuard2 相同。
- 16. 查看 mGuard 的 VPN 连接状态

进入 IPsec VPN >> IPsec Status, 点 Update 刷新,该页提供了有关连接状态和当前正在使用的密钥 有效周期等信息。下图为mGuard2 的 IPsec Status 信息。

