目的：**FG 到 VIGORIPSEC 野蛮模式 VPN 以及** VPN Trunk

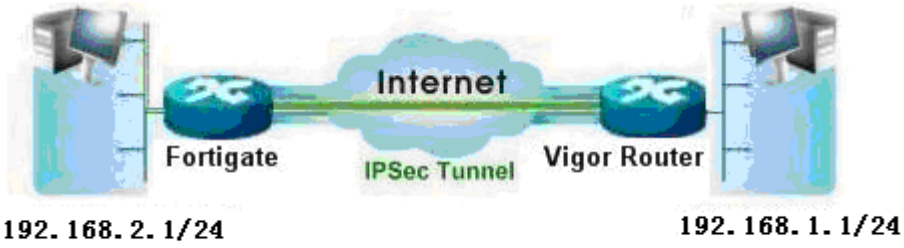


**图-1**

## Vigor 路由器设置


**图-2**

VPN和远程访问 >> LAN to LAN

LAN-to-LAN设定档：

| 恢复至出厂默认设置 |

| 索引 | 名称 | 状态 | 索引 | 名称 | 状态 |
|---|---|---|---|---|---|
| 1. | ??? | X | 17. | ??? | X |
| 2. | ??? | X | 18. | ??? | X |
| 3. | ??? | X | 19. | ??? | X |
| 4. | ??? | X | 20. | ??? | X |
| 5. | ??? | X | 21. | ??? | X |
| 6. | ??? | X | 22. | ??? | X |
| 7. | ??? | X | 23. | ??? | X |
| 8. | ??? | X | 24. | ??? | X |
| 9. | ??? | X | 25. | ??? | X |
| 10. | ??? | X | 26. | ??? | X |
| 11. | ??? | X | 27. | ??? | X |
| 12. | ??? | X | 28. | ??? | X |
| 13. | ??? | X | 29. | ??? | X |
| 14. | ??? | X | 30. | ??? | X |
| 15. | ??? | X | 31. | ??? | X |
| 16. | ??? | X | | | |

**图-3**

如下图所示，地址 192.168.10.130 是远端 Fortigate WAN IP 地址。

VPN和远程访问 >> LAN to LAN

设定档索引 ： 1

1. 一般设定

设定档名称 fortigate

启用此设定档

VPN隧道通过： WAN1优先

拨叫方向 双向 拨出 拨入

一直在线

闲置超时 0 秒

启用PING以维持在线

PING IP

2. 拨出设定

我拨叫的服务器类型

ISDN

PPTP

IPSec隧道

应用IPSec策略的L2TP 无

VPN服务器IP/主机名
（比如 draytek.com 或 123.45.67.89）

192.168.10.130

连接类型 64k bps

用户名 ???

密码

PPP验证 PAP/CHAP

VJ压缩 开 关

IKE认证方法

预共享密钥

IKE预共享密钥 ••••••••••

图-4

IPSec安全方法

中等（AH）

高等（ESP） DES有验证

高级 点击

索引（1-15） 计划任务 设置：

回拨功能（CBCP）

要求远端回拨

提供ISDN号码给远端

图-5


IKE高级设定
IKE第一阶段模式
主模式
积极模式
IKE第一阶段提议
DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_SHA1_G1
IKE第二阶段提议
DES_SHA1/DES_MD5
IKE第一阶段密钥有效时间
28800
(900~86400)
IKE第二阶段密钥有效时间
3600
(600~86400)
完全机密转发(PFS)
停用
启用
本地ID
shvigor
确定
关闭

图-6


4. TCP/IP网络设定
我的WAN IP
0.0.0.0
远端网关IP
0.0.0.0
远端网络IP
192.168.1.0
远端子网掩码
255.255.255.0
更多
RIP方向
禁用
从本地子网到远端子网，您打算做
路由
变更默认路由到此VPN隧道（仅单WAN模式支持）
确定
清除
取消

图-7

VPN和远程访问 >> LAN to LAN

LAN-to-LAN设定档：　　| 恢复至出厂默认设置 |

| 索引 | 名称 | 状态 | 索引 | 名称 | 状态 |
|---|---|---|---|---|---|
| 1. | fortigate | V | 17. | ??? | X |
| 2. | ??? | X | 18. | ??? | X |
| 3. | ??? | X | 19. | ??? | X |
| 4. | ??? | X | 20. | ??? | X |
| 5. | ??? | X | 21. | ??? | X |
| 6. | ??? | X | 22. | ??? | X |
| 7. | ??? | X | 23. | ??? | X |
| 8. | ??? | X | 24. | ??? | X |
| 9. | ??? | X | 25. | ??? | X |
| 10. | ??? | X | 26. | ??? | X |
| 11. | ??? | X | 27. | ??? | X |
| 12. | ??? | X | 28. | ??? | X |
| 13. | ??? | X | 29. | ??? | X |
| 14. | ??? | X | 30. | ??? | X |
| 15. | ??? | X | 31. | ??? | X |
| 16. | ??? | X | | | |

图-8

## Fortigate 设置


图-9

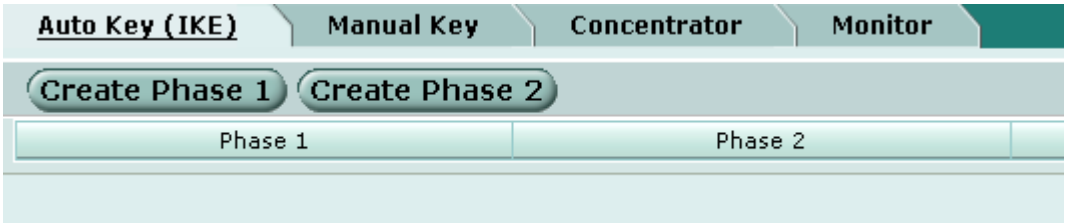

图-10

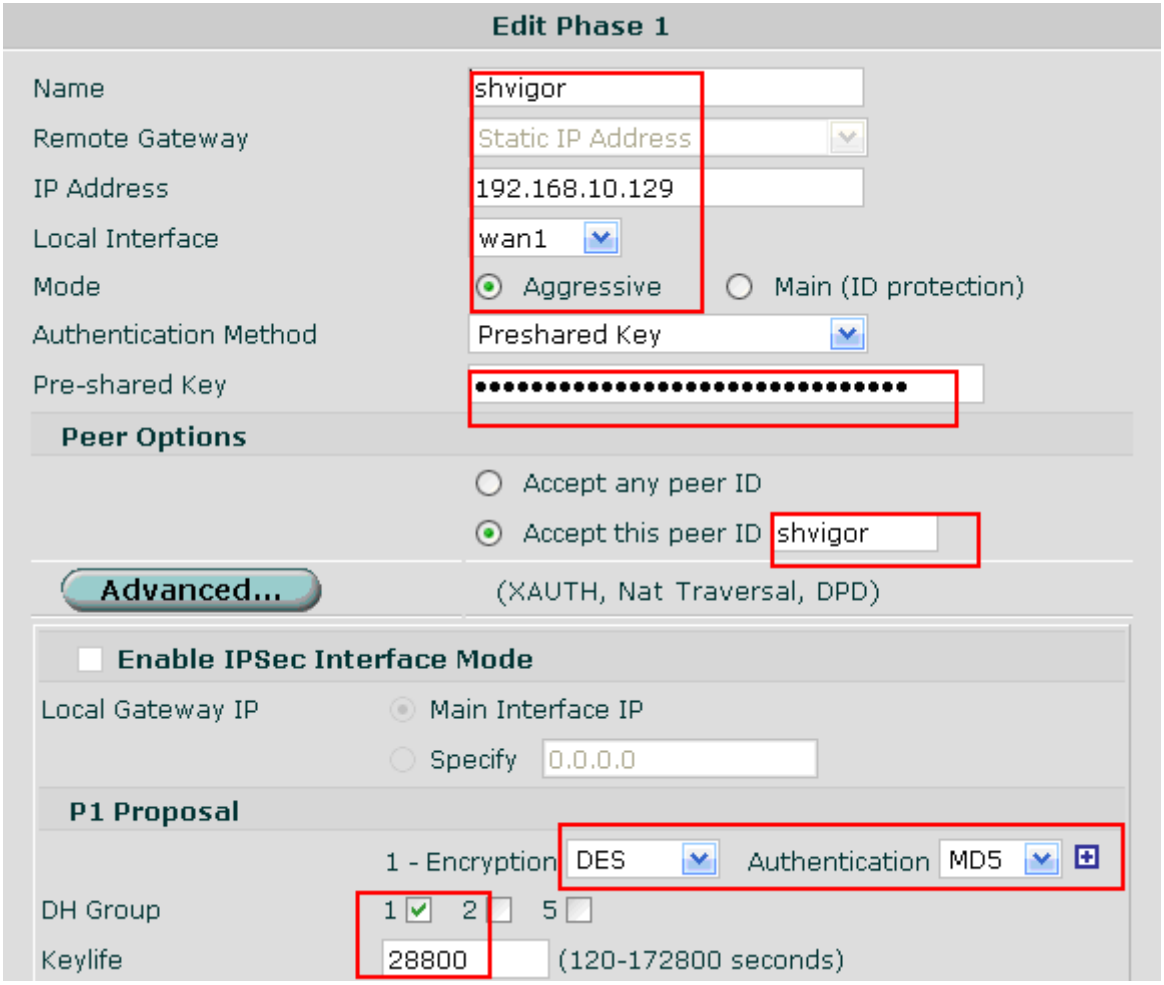
Edit Phase 1
Name
shvigor
Remote Gateway
Static IP Address
IP Address
192.168.10.129
Local Interface
wan1
Mode
Aggressive
Main (ID protection)
Authentication Method
Preshared Key
Pre-shared Key
Peer Options
Accept any peer ID
Accept this peer ID
shvigor
Advanced...
(XAUTH, Nat Traversal, DPD)
Enable IPSec Interface Mode
Local Gateway IP
Main Interface IP
Specify
0.0.0.0
P1 Proposal
1 - Encryption
DES
Authentication
MD5
DH Group
1
2
5
Keylife
28800
(120-172800 seconds)

图-11

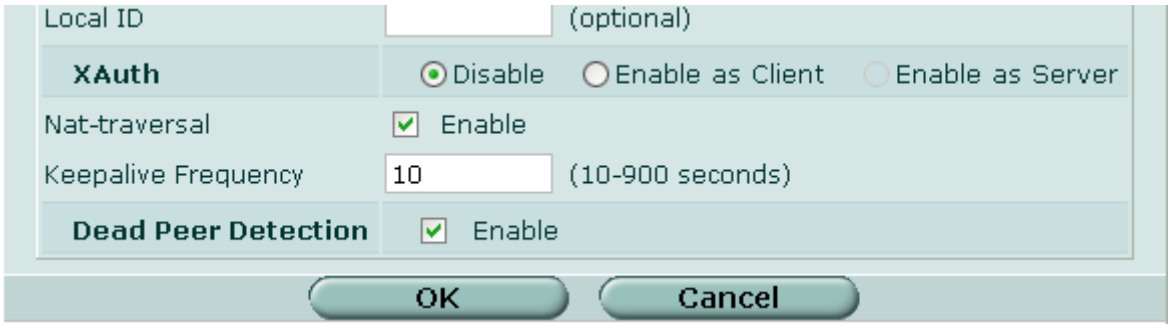
Local ID
(optional)
XAuth
Disable
Enable as Client
Enable as Server
Nat-traversal
Enable
Keepalive Frequency
10
(10-900 seconds)
Dead Peer Detection
Enable
OK
Cancel

图-12

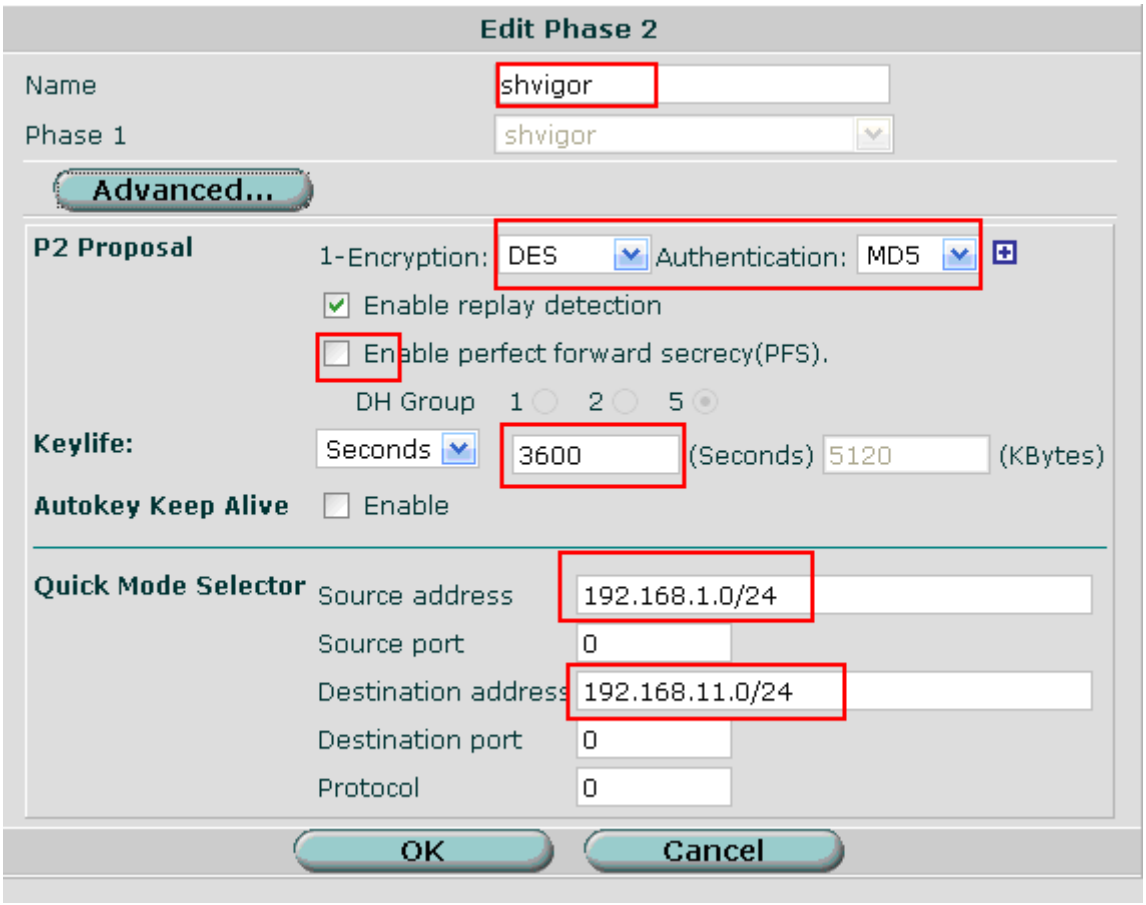
Edit Phase 2
Name
shvigor
Phase 1
shvigor
Advanced...
P2 Proposal
1-Encryption: DES
Authentication: MD5
Enable replay detection
Enable perfect forward secrecy(PFS).
DH Group 1 2 5
Keylife:
Seconds
3600
(Seconds)
5120
(KBytes)
Autokey Keep Alive
Enable
Quick Mode Selector
Source address
192.168.1.0/24
Source port
0
Destination address
192.168.11.0/24
Destination port
0
Protocol
0
OK
Cancel

图-13


Firewall
Policy
Address
Service
Schedule
Virtual IP
Protection Profile

图-14

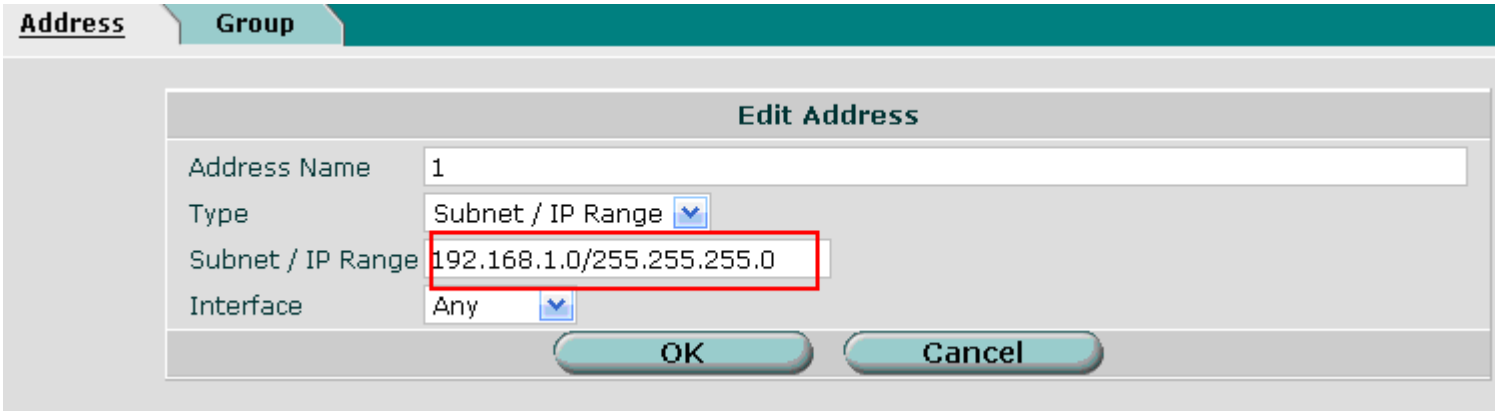
Address
Group
Edit Address
Address Name
1
Type
Subnet / IP Range
Subnet / IP Range
192.168.1.0/255.255.255.0
Interface
Any
OK
Cancel

图-15


Firewall
Policy
Address
Service
Schedule
Virtual IP
Protection Profile

图-16

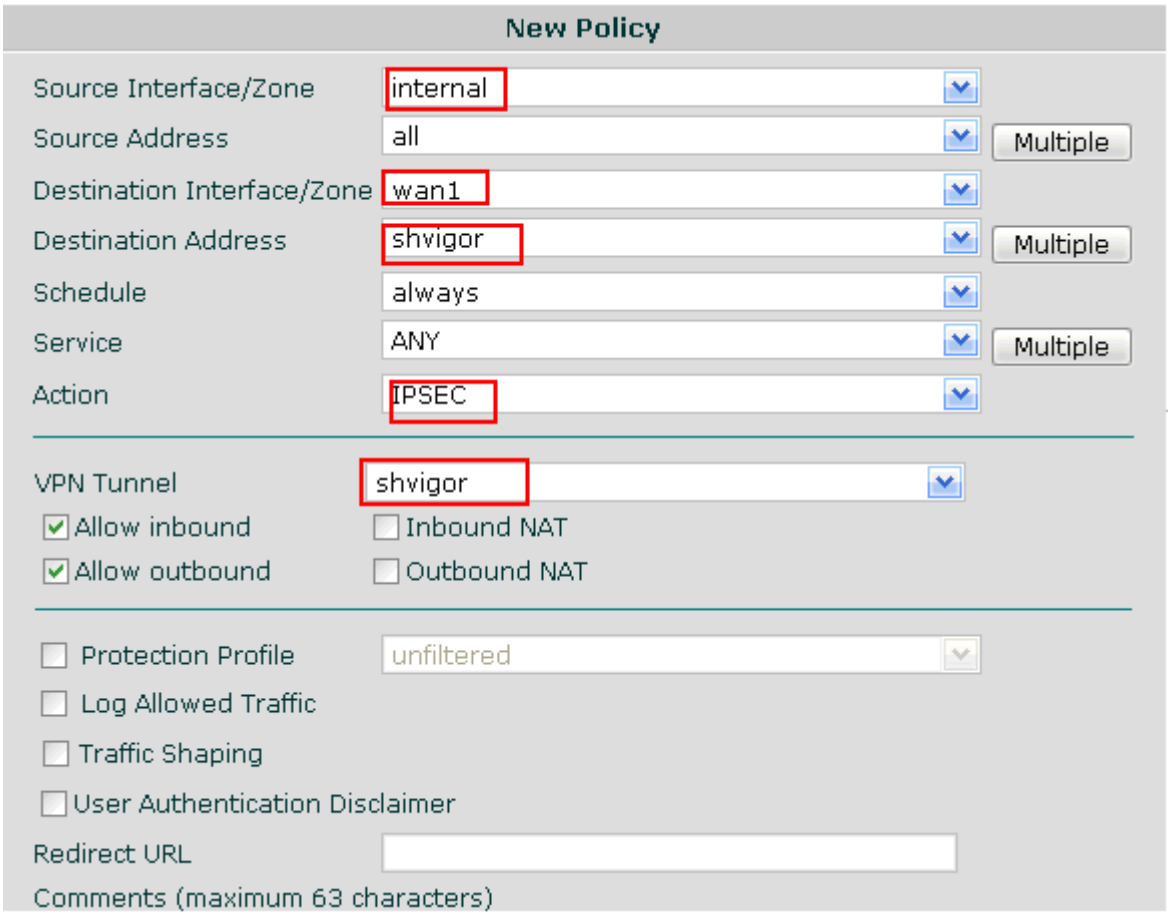
New Policy
Source Interface/Zone
internal
Source Address
all
Multiple
Destination Interface/Zone
wan1
Destination Address
shvigor
Multiple
Schedule
always
Service
ANY
Multiple
Action
IPSEC
VPN Tunnel
shvigor
Allow inbound
Inbound NAT
Allow outbound
Outbound NAT
Protection Profile
unfiltered
Log Allowed Traffic
Traffic Shaping
User Authentication Disclaimer
Redirect URL
Comments (maximum 63 characters)

图-17

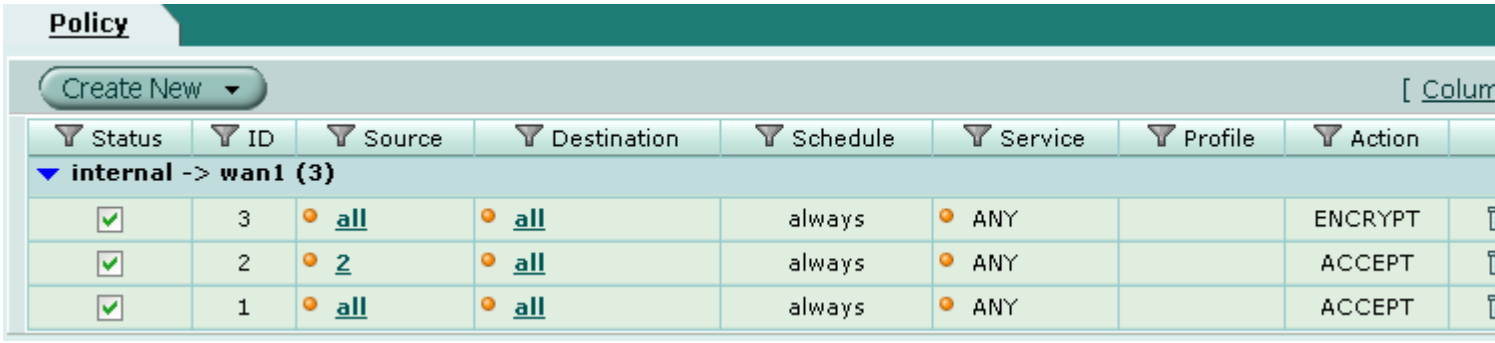


图-18

出现下面这个就说明 VPN 已经建立成功

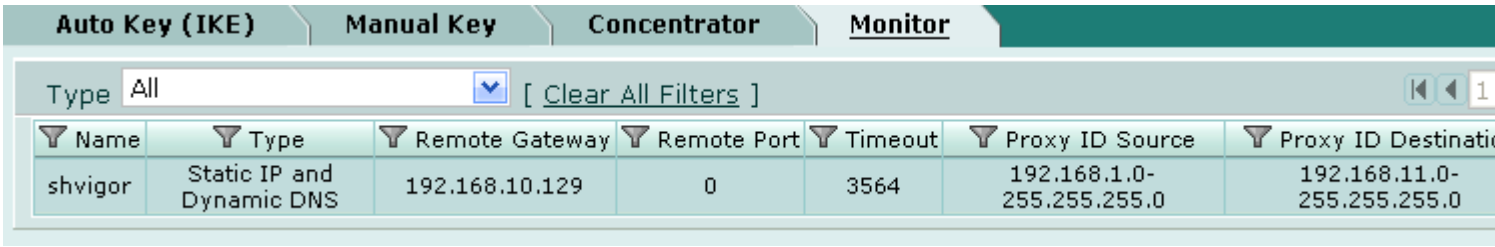


图-19


图-20

# VPN TRUNK

在 VIGOR 2910C 设备中提供 VPN TRUNK 功能，此功能专门为了做 VPN 备份，目的是在一条 VPN 隧道当掉之后，能立刻启用另一条 VPN 隧道，让用户根本感觉不出 VPN 已经出现故障而影响其使用。


图-21

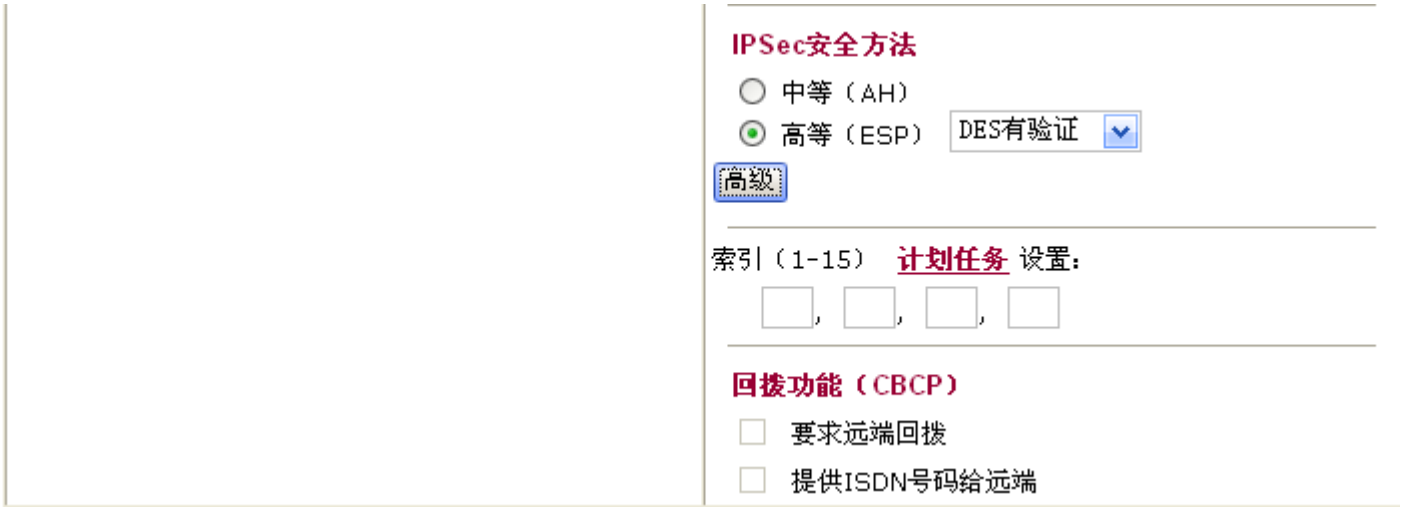
IPSec安全方法
中等（AH）
高等（ESP）
DES有验证
高级
索引（1-15） 计划任务 设置：
回拨功能（CBCP）
要求远端回拨
提供ISDN号码给远端

图-22


IKE高级设定
IKE第一阶段模式
主模式
积极模式
IKE第一阶段提议
DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_SHA1_G1
IKE第二阶段提议
DES_SHA1/DES_MD5
IKE第一阶段密钥有效时间
28800
（900~86400）
IKE第二阶段密钥有效时间
3600
（600~86400）
完全机密转发(PFS)
停用
启用
本地ID
shvigor
确定
关闭

图-23

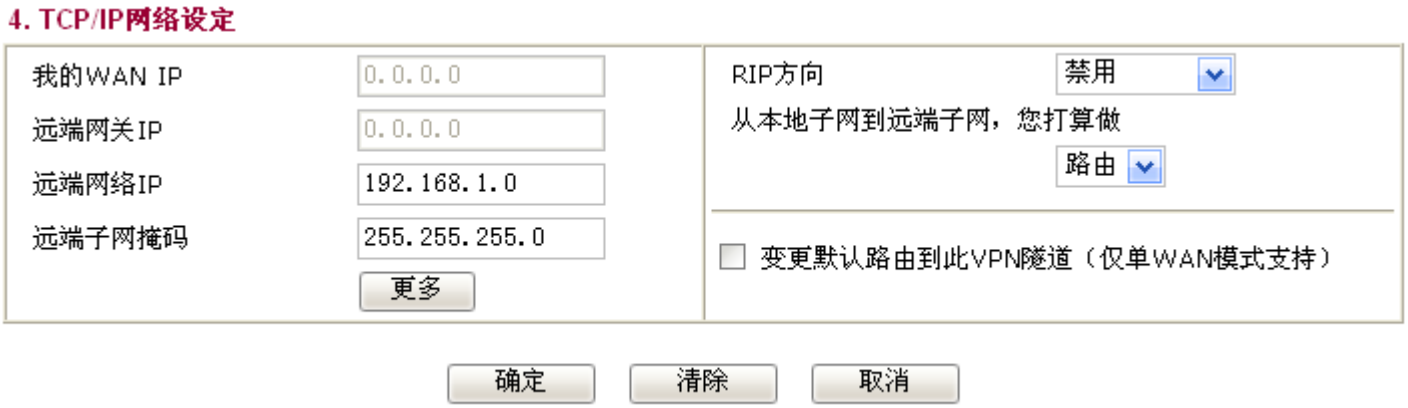
4. TCP/IP网络设定
我的WAN IP
0.0.0.0
远端网关IP
0.0.0.0
远端网络IP
192.168.1.0
远端子网掩码
255.255.255.0
更多
RIP方向
禁用
从本地子网到远端子网，您打算做
路由
变更默认路由到此VPN隧道（仅单WAN模式支持）
确定
清除
取消

图-24

进入 VPN TRUNK 管理进行配制


图-25


图-26

VPN和远程访问 >> VPN TRUNK 管理

备份设定档列表 | 恢复至出厂设定 |

注意: [激活:号码] LAN-to-LAN 设定档已禁用或正处于拨入（拨叫方向）设定。

| 号码 | 状态 | 名称 | 成员1(激活)类型 | 成员2(激活)类型 |
|---|---|---|---|---|
| 1 | v | vpntrunk | 1(YES)IPSec | 2(YES)IPSec |

图-27

VPN和远程访问 >> LAN to LAN

LAN-to-LAN设定档: | 恢复至出厂默认设置 |

| 索引 | 名称 | 状态 | 索引 | 名称 | 状态 |
|---|---|---|---|---|---|
| 1. | fortigate | V | 17. | ??? | X |
| 2. | FG2 | V | 18. | ??? | X |
| 3. | ??? | X | 19. | ??? | X |
| 4. | ??? | X | 20. | ??? | X |
| 5. | ??? | X | 21. | ??? | X |
| 6. | ??? | X | 22. | ??? | X |
| 7. | ??? | X | 23. | ??? | X |
| 8. | ??? | X | 24. | ??? | X |
| 9. | ??? | X | 25. | ??? | X |
| 10. | ??? | X | 26. | ??? | X |
| 11. | ??? | X | 27. | ??? | X |
| 12. | ??? | X | 28. | ??? | X |
| 13. | ??? | X | 29. | ??? | X |
| 14. | ??? | X | 30. | ??? | X |
| 15. | ??? | X | 31. | ??? | X |
| 16. | ??? | X | | | |

图-28

VPN和远程访问 >> 连接管理

拨出工具

更新间隔： 10 刷新

一般模式： 拨号

备份模式： ( vpntrunk ) 192.168.10.130 拨号

VPN 连接状态

当前页： 1 页码 转到 >>

| VPN | 类型 | 远端IP | 虚拟网络 | 发送封包数 | 传送速率 | 接收封包数 | 接收速率 | 运行时间 | |
|---|---|---|---|---|---|---|---|---|---|
| 1 ( fortigate ) | IPSec Tunnel DES-MD5 Auth | 192.168.10.130 | 192.168.1.0/24 | 0 | 0 | 0 | 0 | 0:0:20 | 断开 |

xxxxxxxx：数据已加密。

xxxxxxxx：数据未加密。

图-29

VPN和远程访问 >> 连接管理

拨出工具

更新间隔： 10 刷新

一般模式： 拨号

备份模式： ( vpntrunk ) 192.168.10.130 拨号

VPN 连接状态

当前页： 1 页码 转到 >>

| VPN | 类型 | 远端IP | 虚拟网络 | 发送封包数 | 传送速率 | 接收封包数 | 接收速率 | 运行时间 |
|---|---|---|---|---|---|---|---|---|

xxxxxxxx：数据已加密。

xxxxxxxx：数据未加密。

图-30

VPN和远程访问 >> 连接管理

拨出工具

更新间隔： 10 刷新

一般模式： 拨号

备份模式： ( vpntrunk ) 192.168.10.130 拨号

VPN 连接状态

当前页： 1 页码 转到 >>

| VPN | 类型 | 远端IP | 虚拟网络 | 发送封包数 | 传送速率 | 接收封包数 | 接收速率 | 运行时间 | |
|---|---|---|---|---|---|---|---|---|---|
| 1 ( FG2 ) | IPSec Tunnel DES-MD5 Auth | 192.168.10.130 | 192.168.1.0/24 | 0 | 0 | 0 | 0 | 0:0:9 | 断开 |

xxxxxxxx：数据已加密。

xxxxxxxx：数据未加密。

图-31