**SHREW IPSec VPN客户端使用介绍**

Shrew VPN客户端软件可以作为IPSec VPN客户端，与防火墙建立IPSec VPN连接。Shrew VPN标准版是免费软件，下载地址如下：

<https://www.shrew.net/download/vpn/vpn-client-2.2.2-release.exe>

# 防火墙配置

## IPSec阶段1

* 图形界面配置如下：



高级选项配置：



* 命令行配置如下：

define vpn ipsec phase1-interface

edit "p1"

set type dynamic

set interface "internal"

set proposal 3des-sha1 aes128-sha1

set mode aggressive

set psksecret XXXXXX //预共享密钥

next

end

## IPSec阶段2

* 图形界面配置如下：



* 命令行配置如下：

define vpn ipsec phase2-interface

edit "p2"

set phase1name "p1"

set proposal 3des-sha1 aes128-sha1

next

end

**注：防火墙阶段1和阶段2大多保留默认配置，需要与客户端SHREW匹配的配置在客户端软件上进行。**

## 防火墙策略配置

* 图形界面配置

建立VPN客户端访问内网策略：

图形界面配置：



此时，源接口P1，即为IPsec阶段1的名称，目的接口即为VPN访问的内网接口。如需要指定访问的内网地址及端口，可在目的地址和服务中进行相应配置。

如内网也需要向VPN客户端主动发起访问，则需要再配置一条源接口是内网接口，目的接口是隧道接口的防火墙策略。

* 命令行配置：

define firewall policy

edit 0

set srcintf "p1"

set dstintf "internal"

set srcaddr "all"

set dstaddr "all"

set action accept

set schedule "always"

set service "ANY"

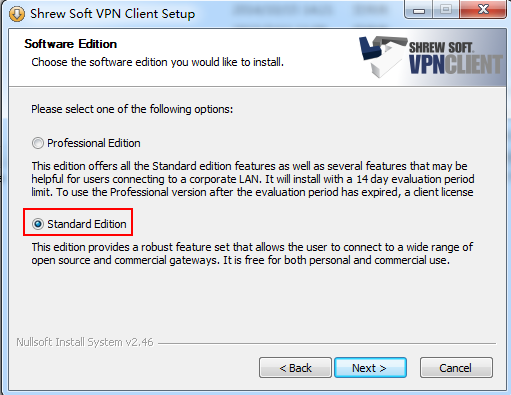
next

end

# SHREW IPSec VPN客户端安装配置

## 客户端安装

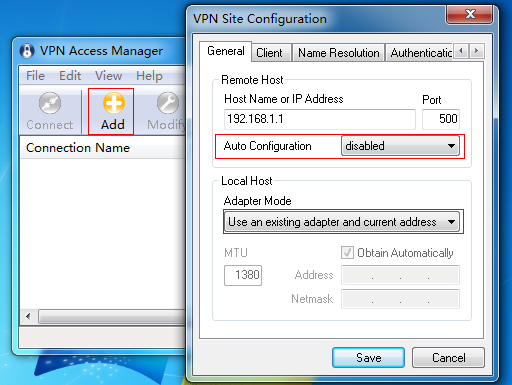
安装Shrew VPN客户端，需要注意要选择安装标准版本，如安装为默认的专业版本，则只有15天的试用期。如下图所示：



## 客户端配置

安装完成后，打开Shrew软件，进行配置。点击Add按钮，新建客户端VPN连接。

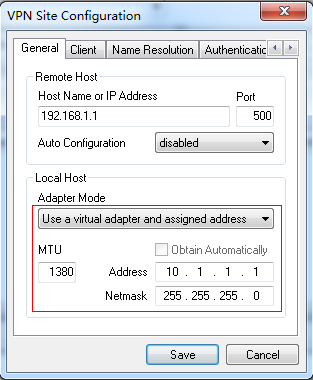
* General标签配置



防火墙IPSec VPN默认配置下，不会给客户端分配IP。因此，在Auto Configuration选项中，需要选择disable。防火墙为客户端分配IP配置参见下节内容。

当Adapter Mode下有三个选项，

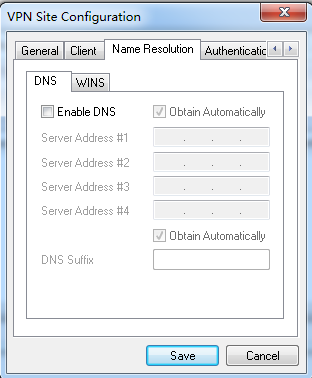
选择第一项，需要配置一个IP地址，VPN拨号成功后，客户端访问内网的源IP为配置的IP地址。如下图所示：



选择第三项，不需要在客户端配置IP，VPN拨号成功后，客户端访问内网的源IP为本地访问公网的网卡配置IP。

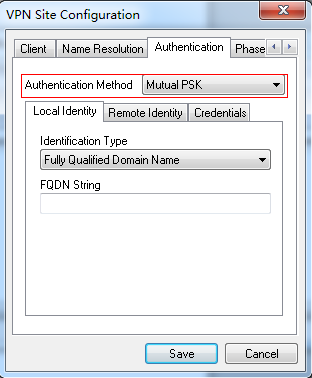
* Name Resolution标签配置

如不需要DNS及WIN服务器，则去掉Enable DNS及Enable WINS，否则配置无法继续。防火墙为客户端分配DNS及WINS配置参见下节内容。

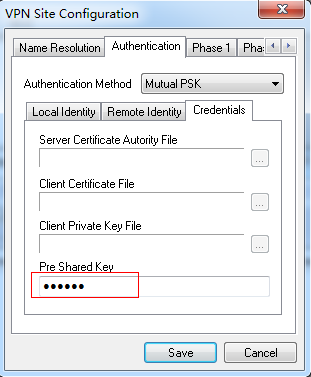


* Authentication标签配置

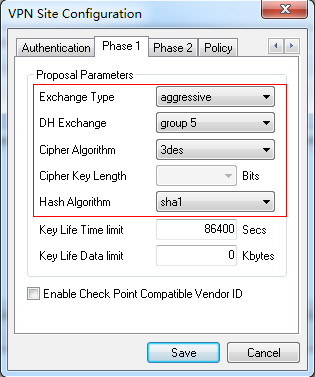
在Authentication Method中选择Mutual PSK



在Credentials中填写预共享密钥：

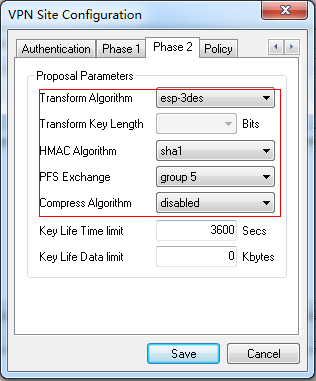


* Phase 1标签配置



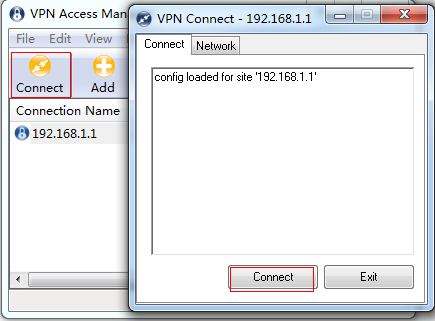
对阶段1 VPN协商参数进行配置，此配置需要与防火墙阶段1配置匹配。

* Phase 2标签配置

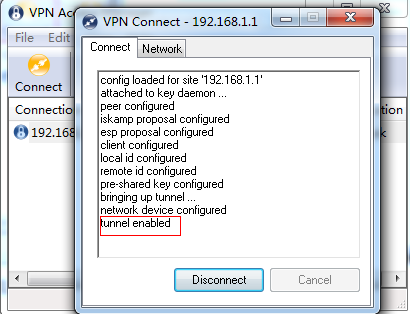


对阶段2 VPN协商参数进行配置，此配置需要与防火墙阶段2配置匹配。

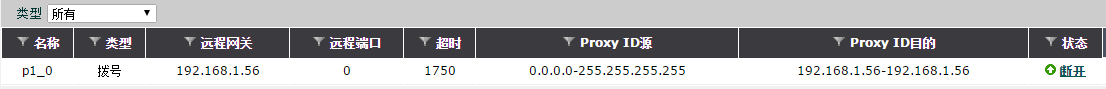
配置完成后，点击save。接着可以进行VPN拨号连接：



连接成功后，客户端会显示如下信息：



在防火墙上VPN->IPSec->监视器中，可以看到隧道成功建立。



此时，VPN拨号客户端IP为客户端PC网卡配置的IP地址。

# 动态分配IP配置

防火墙可以通过Mode config为VPN拨号客户端分配IP，配置如下：

* 防火墙配置

在防火墙阶段1配置中，加入如下配置(只能在命令行下配置)：

define vpn ipsec phase1-interface

edit "p1"

set type dynamic

set interface "internal"

set proposal 3des-sha1 aes128-sha1

set mode aggressive

**set mode-cfg enable**

**set ipv4-start-ip 10.1.1.1**

**set ipv4-end-ip 10.1.1.100**

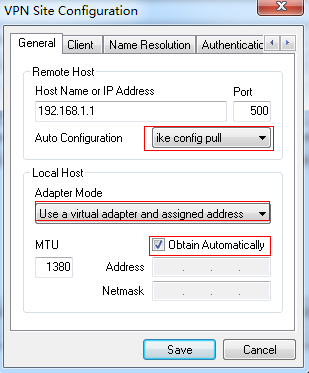
set psksecret xxxxxxx

next

end

* Shrew客户端配置

在General标签下，按下图红框内选项进行配置：



如需要分配DNS，则在防火墙配置中，加入分配DNS：

define vpn ipsec phase1-interface

edit "p1"

set mode-cfg enable

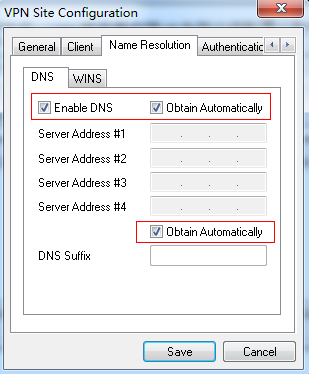
set ipv4-start-ip 10.1.1.1

set ipv4-end-ip 10.1.1.100

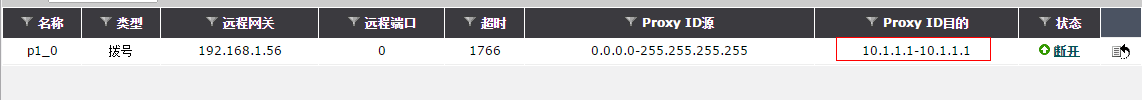
**set ipv4-dns-server1 1.1.1.1**

end

在客户端中Name Resolution标签，按如下红框内配置勾选：



此时，拨号成功后，VPN拨号客户端IP为防火墙配置分配的IP地址。



# Xauth配置

如需要在VPN拨号时加入用户名密码认证，可开启Xauth认证。防火墙配置如下：

* 认证用户及用户组配置：

define user local

edit "test"

set type password

set passwd xxxxxx

end

define user group

edit "group"

set member "test" "test1"

next

end

* 在防火墙IPSec VPN阶段1的高级选项配置中，开启Xauth：



命令行配置：

define vpn ipsec phase1-interface

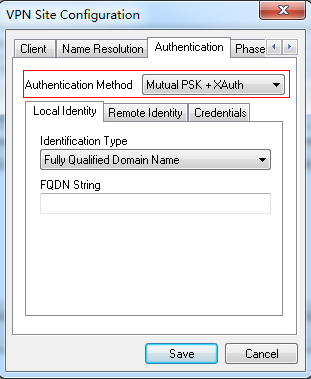
edit "p1"

set xauthtype pap

set authusrgrp "group"

end

在Shrew客户端的Authentication标签下，按如下红框内进行配置：



配置完成后，拨号时，会要求输入用户名密码，输入正确的用户名密码即可连接VPN。

