

奇安信虚拟化下一代防火墙 部署阿里云指导手册

奇安信集团

2020年4月

目录

第一章 概述.....	3
1.1. 产品介绍.....	3
1.2. 安装要求及其注意事项.....	3
第二章 设备介绍.....	4
2.1 设备列表.....	4
第三章 上线购买说明.....	4
3.1. 如何购买奇安信 vNGFW.....	4
3.2. 方法 1 云市场购买.....	4
3.3. 方法 2 管理控制台购买.....	7
第四章 许可证.....	10
4.1. 许可证作用.....	10
4.2. 许可证类型.....	10
4.3.获得许可证.....	11
第五章 部署案例.....	12
5.1. DNAT 网络部署.....	12
5.2. SNAT 网络部署.....	15
5.3. IPSEC VPN 网络部署.....	17
5.4. SSL VPN 网络部署.....	21

第一章 概述

1.1. 产品介绍

“奇安信虚拟化下一代防火墙”简称为vNGFW,它是一个纯软件形态的产品，是运行在虚拟机上的完全自主知识产权的SecOS操作系统之上。奇安信vNGFW是虚拟机镜像方式存放在阿里云平台上，所以您必须为它提供一个存储介质ECS（Elastic Compute Service, 阿里云服务器）。您可以向阿里云平台购买等方式获得ECS，奇安信vNGFW会自动安装成功。

1.2. 安装要求及其注意事项

- 阿里平台上用于安装部署奇安信vNGFW的ECS必须采用“专有网络”类型（VPC网络），新购买ECS用户手动配置选择“可用区域”的时候，需要修改成“专有网络”类型。
- 安装的配置要求必须选择**2个vCPU**,内存最低是**2G**。
- 奇安信vNGFW只能在阿里云“**I/O优化**”的实例/虚拟机上运行。
- 启动实例以后您必须在控制台重置密码才能正常使用（新密码包括字母，数字，特殊字符，至少12位）。
- 产品授权方式分为试用版本和正式版本，镜像本身默认提供给用户30天的试用期，在此期间所有的功能都可以正常试用，提前15天会有到期告警信息，试用期过后如果没有新的授权，所有的功能均不能使用。正式版本需要您购买相应的许可服务，购买了正式版本则所有的功能均可用，如果没有购买相关的特征的升级则该功能特征库升级不可用，但是功能仍可使用。

第二章 设备介绍

2.1 设备列表

编号	类型	单位	数量	备注
1	云服务器 ECS	台	2	一台 ECS 需要安装 vNGFW, 另一台需要安装被保护的云服务器（如 WEB 服务器）
2	V_Router	台	1	阿里云会为每个 VPC 网络分配一个路由器，这个不需要用户单独购买，可以配置静态路由拓展用户的需求
3	V_Switch	台	1	阿里云会为每个 VPC 网络默认分配一个交换机，这个不需要用户单独购买，可以在交换机下购买 ECS 服务器
4	公网 IP 地址	个	1	需要在阿里云租用一个公网 IP 地址供用户访问使用
5	360 网神 vNGFW	套	1	绑定 ECS 服务器一起购买
6	WEB 服务器（示例）	套	1	绑定 ECS 服务器一起购买

第三章 上线购买说明

3.1. 如何购买奇安信 vNGFW

奇安信vNGFW需要部署在阿里云的ECS实例上进行使用，所以您必须购买ECS，我们这里简单的介绍一下ESC的购买方法，阿里云为我们提供了两种购买方法。

3.2. 方法 1 云市场购买

一、 首先，使用阿里云账号正常登陆阿里云系统中。

二、 进入云市场->网络安全在搜索栏输入“奇安信虚拟化下一代防火墙”点击进入购买界面。如图1所示：



三、 点击“360网络虚拟化下一代防火墙系统（I/O优化）”->立即购买



我们这里在【华南1】里创建，在这个区域里网络类型只有“专有网络”，如果您是 在别的区域创建的ECS，发现默认的网络类型是“经典网络”请您修改成“专有网络”，奇安信vNGFW只支持“专有网络”。

- 公网IP是为vNGFW分配一个公网的IP地址，您可以通过这个地址访问管理vNGFW设备，（这个公网IP并不是配置在防火墙上的，它实际是一个出口的NAT地址映射）。
- 需要选择ECS所属于的VPC和交换机，阿里云会默认为您创建VPC网络和交换机，它们分别是vpc-wz90di3zp;vsw-wz9s0r7z.如果您手动创建了VPC和交换机在这里更改即可。
- 不同的实例配置的如系列I,II,III,它们的资源规格和价格都是不一样的，这里可

可以根据您的需求购买，但要满足：必须2个vCPU,内存最低是2G。如图2所示。



四、 点击立即购买->去支付，如图3



五、 购买成功以后您可以返回阿里云首页进入->控制台->云服务器ECS->华南1云服务器查看是否创建成功。所下图4所示：



172.18.220.113 这个 IP 地址是真实的防火墙地址,119.23.20.79 是出口设备的地址,实际上是一个 119.23.20.79->172.18.220.113 地址映射。在公网可以通过 <https://119.23.20.79> 登录 vNGFW 的 WEBUI 控制台,对设备进行配置管理,在私网可以通过 <https://172.18.220.113> 登录 vNGFW 的 WEBUI 控制台,对设备进行配置管理。

3.3. 方法 2 管理控制台购买

一、 如果您想通过管理控制台方式购买,您必须曾经创建过VPC网络和交换机。例如: 返回阿里云首页->控制台->专有网络VPC->华南1->交换机。如图5所示:

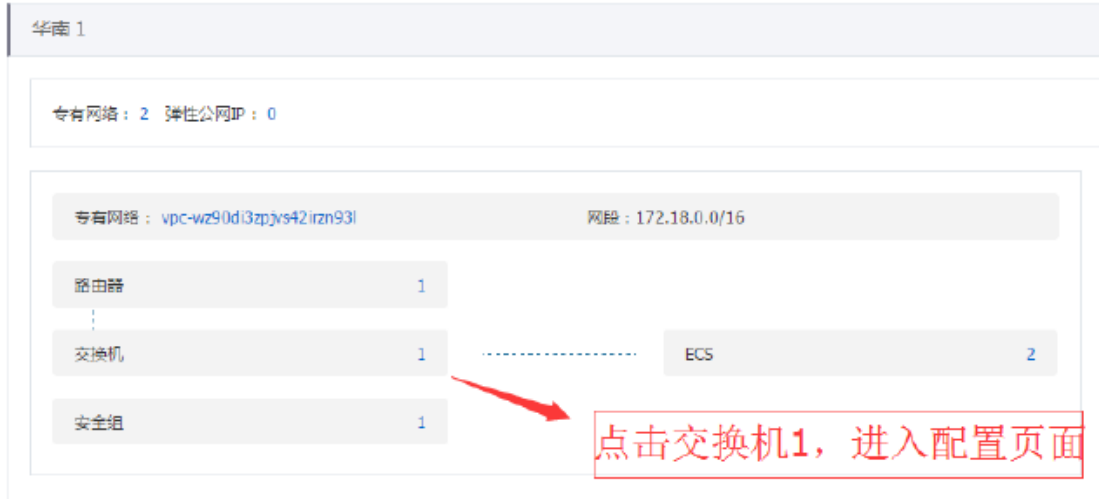


图 5

二、 进入交换机列表->创建实例->创建ECS实例，如图6所示：

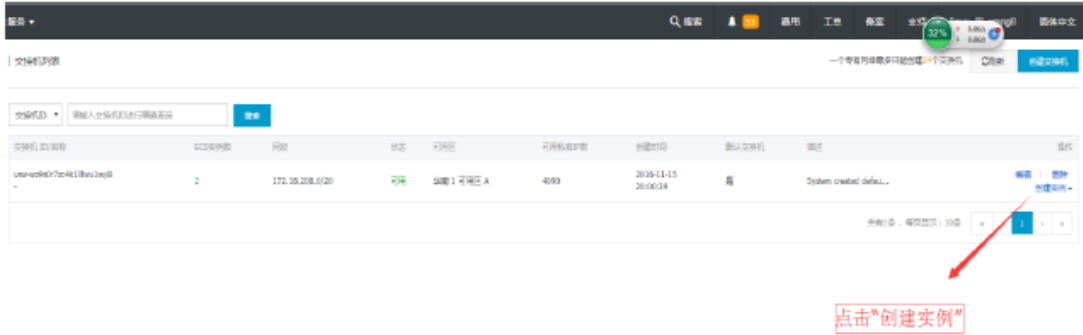


图 6

三、按照下列要求创建ECS实例

- 区域选择【华南1】。
- 网络选择专用网络。
- VPC和交换机需要选择【华南1】下的需要查看名字是否正确。
- 公网IP地址如果使用不分配，后续可以通过弹性公网IP的形式绑定。
- 安全组需要创建一个策略，全通即可，可在ECS实例中引用，默认安全组没有选型是空，需要更改。如图7所示：



图 7

镜像点击镜像市场，从镜像市场中搜索“奇安信虚拟化下一代防火墙系统（I/O优化）”如图8所示：



图 8

四、 进行搜索->购买



图 9

五、后面的操作请参照云市场安装使用说明。

第四章 许可证

4.1. 许可证作用

奇安信vNGFW产品是否可以正常使用由产品的许可证控制，只有购买并安装了相应的许可证以后，用户才能够正常使用产品的相关功能。

4.2. 许可证类型

- 试用许可证：

成功安装 ⑧ 奇安信vNGFW ⑨ 实例以后，它默认自带试用许可证，有效期为30天，支持的功能和性能与正式许可证相同，功能相关的特征库（IPS、AV、App、URL等）都可以正常升级，但是使用到期后，vNGFW功能不可用，流经vNGFW的流量会立即中断，功能相关的特征库不能升级，导入正式许可证后恢复流量通讯。

试用许可证下支持的IPSEC VPN并发用户数是5，SSL VPN并发用户数是5，虚拟

系统是1

- 正式许可证:

成功安装“奇安信vNGFW”实例以后，您可以安装平台正式许可证。正式许可证提供基础防火墙功能授权、IPS特征库升级授权、AV特征库升级授权、应用识别特征库升级授权、URL过滤库升级授权，正式许可到期后设备所有功能均可用，经过防火墙的流量正常转发，但是功能相关的特征库会无法正常升级。

正式许可证下支持的IPSEC VPN并发用户数是1000，SSL VPN并发用户数是1000，虚系统是8

4.3.获得许可证

通过配置的公网IP地址用https的方式登录vNGFW的WEB控制台，默认的用户名是admin,密码为购买ECS用户自己设置的密码。如图10所示：

设备描述	IZwz9enqm2s3ka1hhyvemnZ	系统时间	2017-03-15 19:25:32
系统功能	已开启 有效期至2017-04-08	IPS功能	已开启 升级有效期至2017-04-08
AV功能	已开启 升级有效期至2017-04-08	URL功能	已开启 升级有效期至2017-04-08
应用功能	已开启 升级有效期至2017-04-08	HA功能	组0: 未开启
在线管理员	1	在线用户	0
并发连接	20	新建连接	6
序列号	384be561664ad50f003ecf8070cd7fa969a018b3		

接口名称	状态	发送	接收
ge1	■	0(bps)	192(bps)

拷贝产品序列号

图 10

拷贝产品序列号申请正式的许可证。

进入云市场->网络安全在搜索栏输入“奇安信虚拟化下一代防火墙系统-License”点击进入购买界面，如下图11所示：



图11

在线申请后，许可授权会通过在线方式提供，如有问题可以寻求在线客服、400电话或售后邮箱咨询。获取许可证后，进入->系统->许可证-导入

许可证			
系统	名称	支持最大数	导入时间
设置	1 系统功能		2017-03-09 23:07:04
管理主机	2 应用识别库升级		2017-03-09 23:07:04
管理证书	3 IPS(WAF)		2017-03-09 23:07:04
SNMP	4 IPS库升级		2017-03-09 23:07:04
许可证	5 AV功能		2017-03-09 23:07:04
升级	6 AV库升级		2017-03-09 23:07:04
配置文件	7 URL库升级		2017-03-09 23:07:04
虚拟系统	8 IPsec策略数	5	
高可用性	9 并发连接数	1000000	
	10 SSL VPN并发用户数	5	
	11 虚拟系统功能	1	2017-04-08 23:07:04

图 12

第五章 部署案例

5.1. DNAT 网络部署

一、 DNAT模式场景描述

- DNAT全称是目标IP地址或端口转换，vNGFW设备会把原始数据报的目标IP地址修改成身后所保护服务器的IP地址或端口，起到一个远程接入和安全性保护的作用。
- VPC网络内的WEB服务器实例只有内网IP地址没有公网地址，Internet用户是无法访问WEB服务器。（见图13所示）
- VPC网络内的vNGFW实例既有公网IP地址，又有内网IP地址。（见图十三所示）

- vNGFW采用IP端口映射的方式为互联网用户提供服务

二、网络拓扑及其数据流

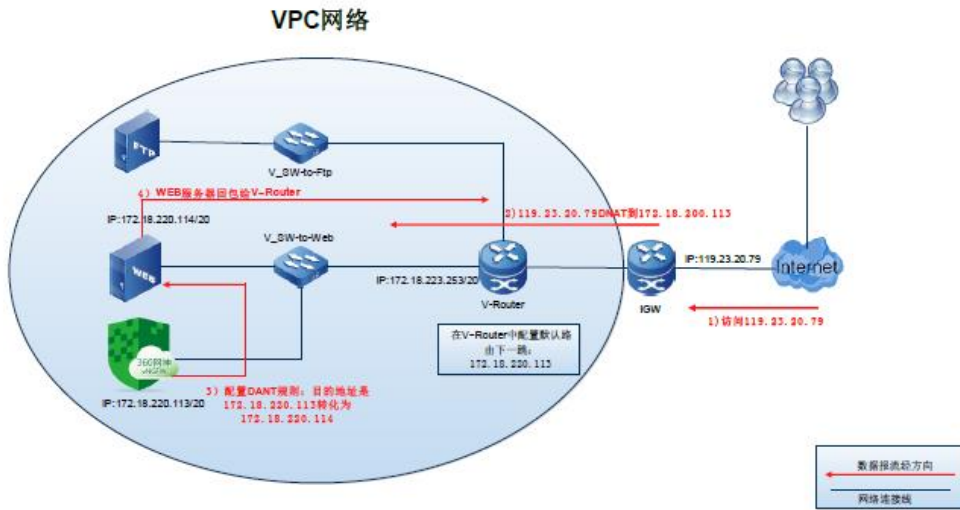


图 13

三、具体配置

(一) 使用https登录“奇安信vNGFW”进入->网络->NAT->DNAT创建一条名字为“dnat-http-port80”如图14所示：

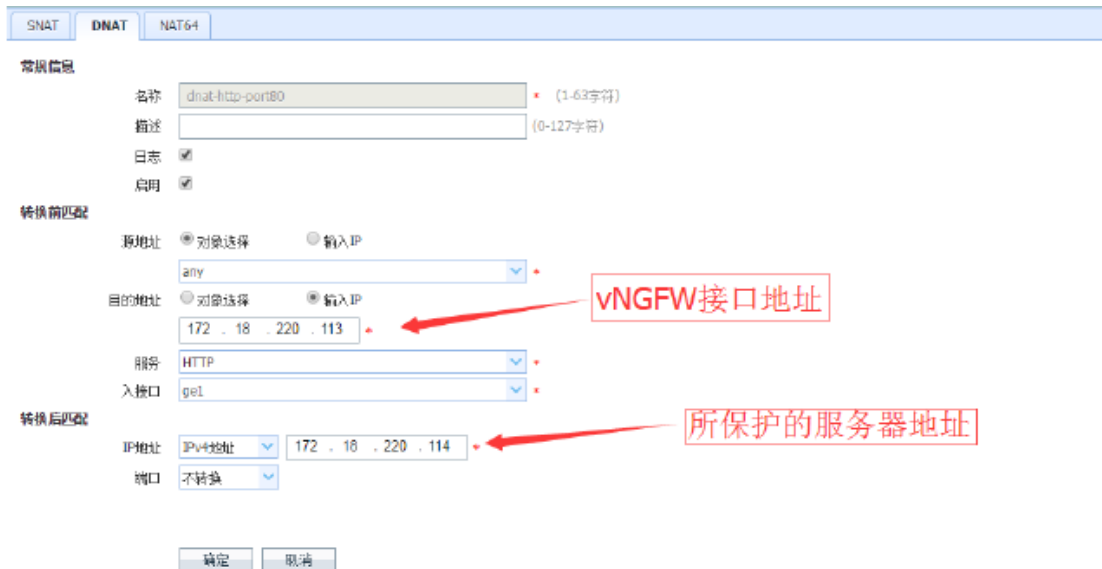


图 14

Internet用户访问的原始IP地址是119.23.20.79，这个数据报经过IGW设备后它会修改目的地址119.23.20.79->172.18.220.113，所以在vNGFW的“转换前匹配”的“目的

地址”是172. 18. 220. 113而不是公网IP地址。

为了防止vNGFW管理的80端口和DNAT规则的80端口冲突，所以请您把管理防火墙的80端口修改成其他。

(二) 进入->安全->安全规则，添加一条安全规则策略放行所需要的数据报，由于是测试所以添加的是全通的安全规则。如图15所示：

常规信息

名称 any (1-63字符)

描述 (0-127字符)

动作 允许 拒绝 安全连接(隧道)

启用

源安全域 any

目的安全域 any

源用户 添加

源地址 源IPv4 源IPv6 源区域 any 添加

目的地址 目的IPv4 目的IPv6 目的区域 any 添加

服务 any 添加

应用 any 选择

入站防护

URL过滤

病毒检测

来自隧道

时间

内容过滤

文件过滤

邮件过滤

网络行为管理

VLAN (取值范围0-4094, 格式: 1,3,5-10,12)

日志

启用长连接

图 15

全通安全规则是存在安全隐患的，所以在您实际部署的环境中请您根据具体的需求，细化安全规则。

(三) 进入->阿里云控制台->专有网络VPC->华南1->路由器中添加一条默认路由，下一跳是vNGFW实例，它的作用是把VPC的流量引流到vNGFW上。具体的配置如下图16所示：

虚拟路由列表

路由表基本信息				
名称: mm	ID: vt-w29c5b8d7jysk3ahelma			
备注: -				

路由条目	状态	目标网段	下一跳
vtb-w29waxo6cvwjtkub55f	可用	0.0.0.0/0	i-w29enqm2s3ka1hhyemr
vtb-w29waxo6cvwjtkub55f	可用	172.18.208.0/20	-
vtb-w29waxo6cvwjtkub55f	可用	100.64.0.0/10	-

图 16

5.2. SNAT 网络部署

一、 SNAT模式场景描述

- SNAT全称源IP地址转换，即内网地址向外访问时，发起访问的内网IP地址转换为指定的IP地址（可指定具体的服务以及相应的端口或端口范围），这可以使内网中使用保留IP地址的主机访问外部网络，即内网的多部主机可以通过一个有效的公网IP地址访问外部网络。
- 在VPC中WEB服务器是无法主动访问Internet的，所以如果想让VPC中的服务器实例访问Internet的资源，必须要把流量引入vNGFW中并且匹配SNAT规则，源地址发生改变后方可访问。（如下图17所示）。
- 引流采用DNAT引流方式，路由器中添加一条默认路由，下一跳是vNGFW实例。

二、 SNAT网络拓扑及其数据流

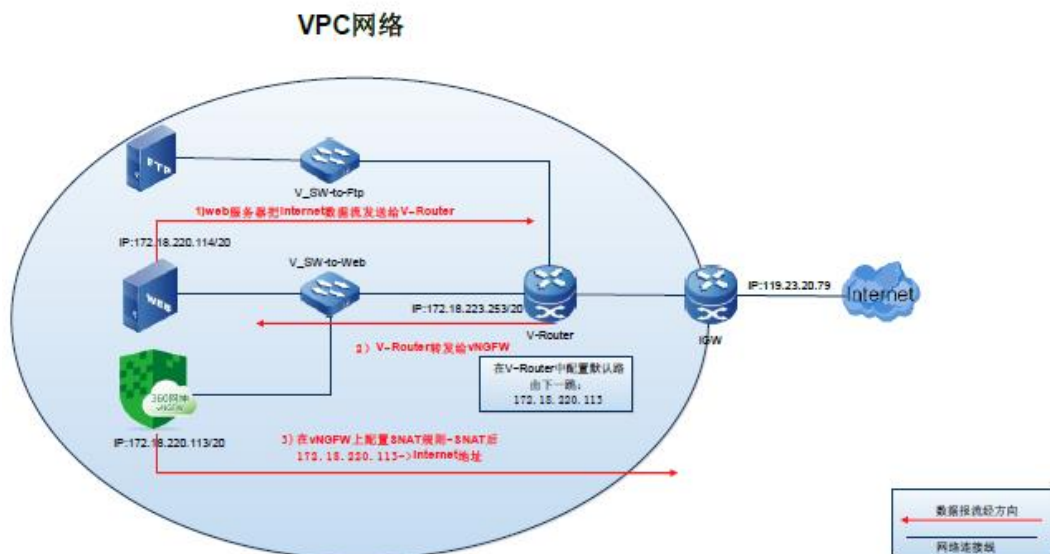


图 17

三、 具体配置

(一) 使用https登录“奇安信vNGFW”进入->网络->NAT->SNAT创建一条名字为“SNAT”

具体配置如下图18所示:

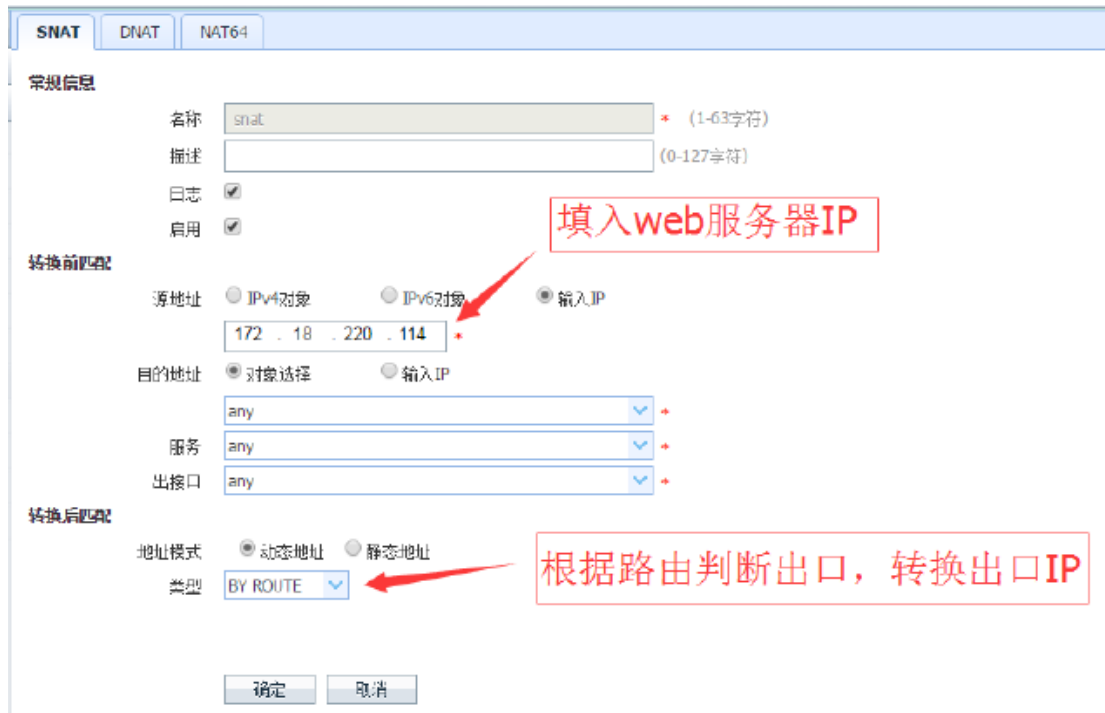


图 18

- 因为只有一个服务器需要访问Internet资源，所以在“转换前匹配”的IP中填入172.18.220.114这个32位的主机地址，如果您想让一个地址段访问公网，那么请在IPV4对象中配置地址段，它需要引用一个地址对象。
- 由于访问Internet资源的多样性，所以在目标地址和服务中选择any,表示所有。
- 类型使用BY_Route的意思是根据路由来判断出接口，源IP地址转成出接口的IP地址，在vNGFW里能匹配的路由是缺省路由即：0.0.0.0/0.0.0.0网关172.18.223.253，所以源IP地址转换成和这个网关一个网段的IP地址即：172.18.220.113

(二) 进入->安全->安全规则，添加一条安全规则策略放行所需要的数据报，由于是测试所以添加的是全通的安全规则。如图十四所示

(三) 进入->阿里云控制台->专有网络VPC->华南1->路由器中添加一条默认路由，下一跳是vNGFW实例，它的作用是把VPC的流量引流到vNGFW上。具体的配置如下图19

虚拟路由列表

路由器基本信息	
名称: nm	ID: vtc-wz9q5b0p7jysk3ahelrma
备注: -	

路由条目列表			
路由条目ID	状态	目标网段	下一跳
vtb-wz9wzco6crrvjzqkub55f	可用	0.0.0.0/0	i-w9enqm2s3ka1hhyemn
vtb-wz9wzco6crrvjzqkub55f	可用	172.18.208.0/20	-
vtb-wz9wzco6crrvjzqkub55f	可用	100.64.0.0/10	-

图 19

5.3. IPSEC VPN 网络部署

一、 IPSEC VPN模式场景描述

- IPSEC VPN作为一项成熟的技术，广泛应用于组织总部和分支机构之间的组网互联，其利用组织已有的互联网出口，虚拟出一条“专线”，将组织的分支机构和总部连接起来，组成一个大的局域网,既提供了远程接入访问，又通过数据包的加密形式保障了数据的安全性，已经被广泛使用。
- vNGFW支持IPSEC VPN功能，可以使用这种技术在公司内部网络，或者数据中心和奇安信vNGFW之间建立一个安全的隧道，实现内网之间的资源的安全访问。(如下图20所示)
- 另一种应用场景是通过IPSEC VPN技术在两个或者多个VPC网络间建立安全隧道实现资源的访问。（如下图21所示）
- Internet用户是通过DNAT技术访问到vNGFW的，如果您使用IPSEC VPN技术被封装的ESP报文经过NAT设备会有很多问题，vNGFW支持“NAT穿越”技术，可以解决这一问题。

二、 IPSEC VPN应用拓扑

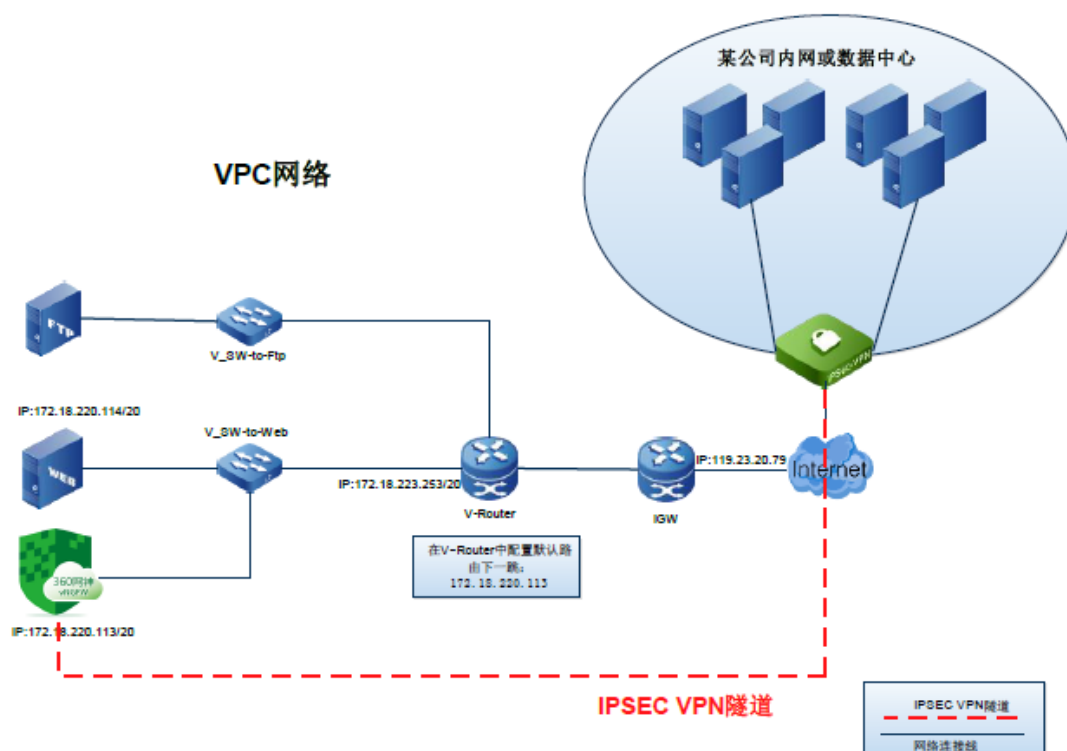


图 20

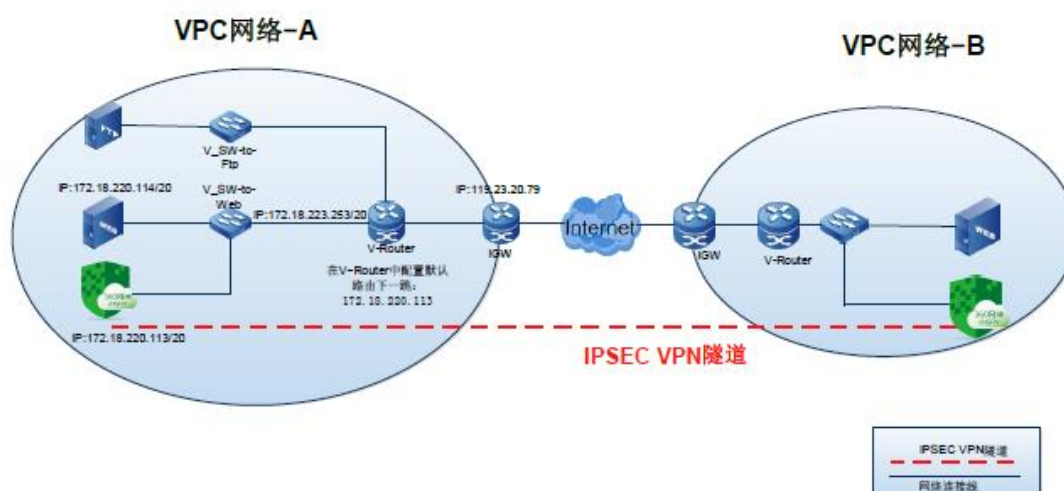


图 21

三、 具体配置

(一) 进入->隧道->IPSec-VPN->IKE网关创建一个IKE网关策略，如下图22所示：

IKE网关 | IKE提议 | 拨号用户组

基本设置

名称: ipsec-to-360 * (1-63字符)

接口: ge1 *

本端IP地址: 172.18.220.113 *

协商模式: 主模式 野蛮模式 国密

网络设置

地址模式: 静态地址 动态地址 拨号用户组

本端ID: NULL U-FQDN FQDN ASN1DN

本端ID值: 234567 * (1-255字符)

对端ID: NULL U-FQDN FQDN ASN1DN

对端ID值: 123456 * (1-255字符)

IKE提议 (P1提议): psk-aes128-sha1-g2 * (网关协商模式为野蛮模式时,只支持1个DH组算法)

预共享密钥: 123456 * (6-31字符)

高级设置

连接类型: 双向 发起者 响应者

NAT穿越: *

对端存活检测:

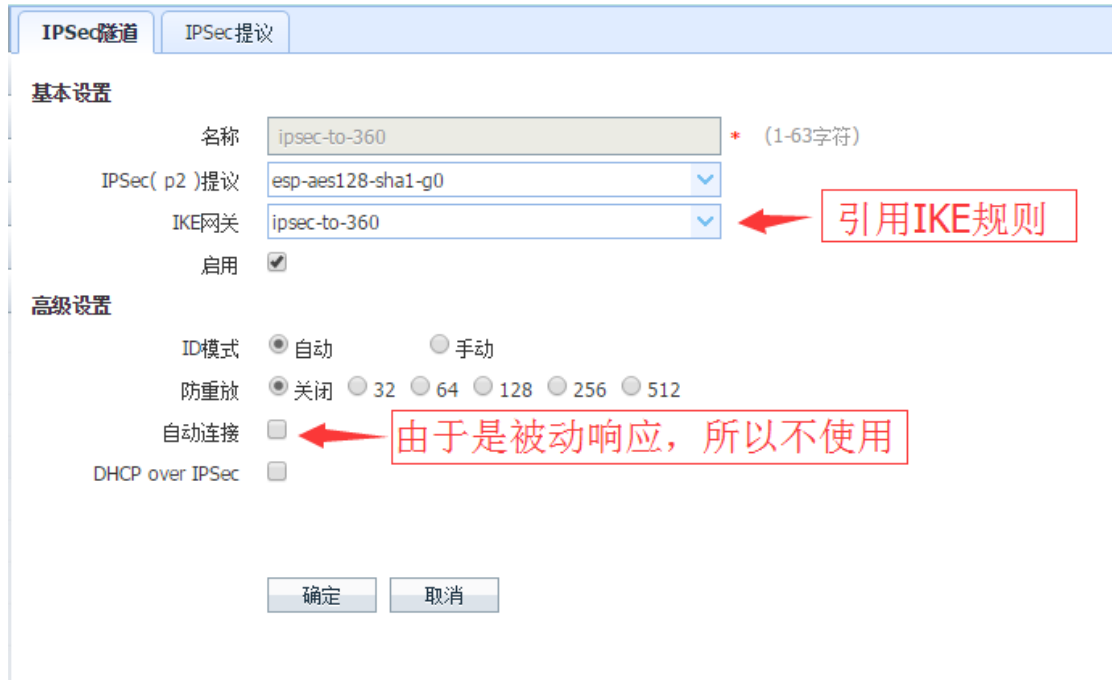
确定 取消

图22

- 由于无法确定请求者的IP地址，它可能是一个ADSL拨号设备，所以在地址模式中使用了动态IP地址，vNGFW作为被动响应设备。
- 身份标示才有FQDN形式，所以要求您必须知道对方VPN的设备的ID值是多少。
- NAT穿越在当前的网络环境下需要使用。

当vNGFW实例使用NAT穿越时，需要对端的VPN设备也同样的开启NAT穿越功能。

(二) 进入->隧道->IPSec-VPN->IPSec隧道，添加一条规则，如下图23所示:



(三) 进入->安全->安全规则, 添加一条安全规则策略放行所需要的数据报, 由于是测试所以添加的是全通的安全规则。如图24所示。

(四) 配置对端VPN设备, 请参照相应产品的操作手册进行配置。

以上配置仅实现当公司内网或者数据中心主动发起流量的互通, 如果您在VPC的服务器中主动发起访问公司内网是不通的, 原因是流量不是感性数据流不能做到VPN流程。如果您有VPC内网主动访问的需求, 请加一条匹配VPN的安全规则, 如下图二十四所示:



图24

新添加的VPN规则需要移动顺序到全通安全规则之前，否则无法匹配。

(五) 进入->阿里云控制台->专有网络VPC->华南1->路由器中添加一条默认路由，下一跳是vNGFW实例，它的作用是把VPC的流量引流到vNGFW上。具体的配置如下图所示：

虚拟路由列表

路由器基本信息				
名称：	mm	ID：	vrt-wz9q5b8p7jysk3ahelnma	
备注：	-			

路由条目列表				
路由表ID	状态	目标网段	下一跳	
vtb-wz9waxo6cvwjtkub55f	可用	0.0.0.0/0	i-wz9enqm2s3ka1hhyvemn	添加默认路由
vtb-wz9waxo6cvwjtkub55f	可用	172.18.208.0/20	-	
vtb-wz9waxo6cvwjtkub55f	可用	100.64.0.0/10	-	

图25

5.4. SSL VPN 网络部署

一、 SSLVPN模式场景描述

- SSL VPN比较适合用于移动用户的远程接入（Client-Site），IPsec VPN多用于“网—网”连接，SSL VPN用于“移动客户—网”连接。SSL VPN用户需安装客户端程序，即可通过SSL VPN隧道接入内部网络，且对客户端设备要求低，因而降低了配置和运行支撑成本。很多企业用户采纳SSL VPN作为远程安全接入技术，主要看重的是其方便的接入能力。
- 奇安信vNGFW实例的SSL VPN功能只需要维护中心节点的网关设备，客户端免维护，降低了部署和支持费用。
- 奇安信vNGFW的SSL VPN功能更容易提供细粒度访问控制，支持本地用户认证外，还与第三方认证系统（如：Radius、AD等）结合更加便捷。
- 奇安信vNGFW获取SSL VPN客户端的形势简单快捷，您只需要在浏览器输入 <https://IP:64443>。安装客户端即可。

二、 SSLVPN应用拓扑及其数据流

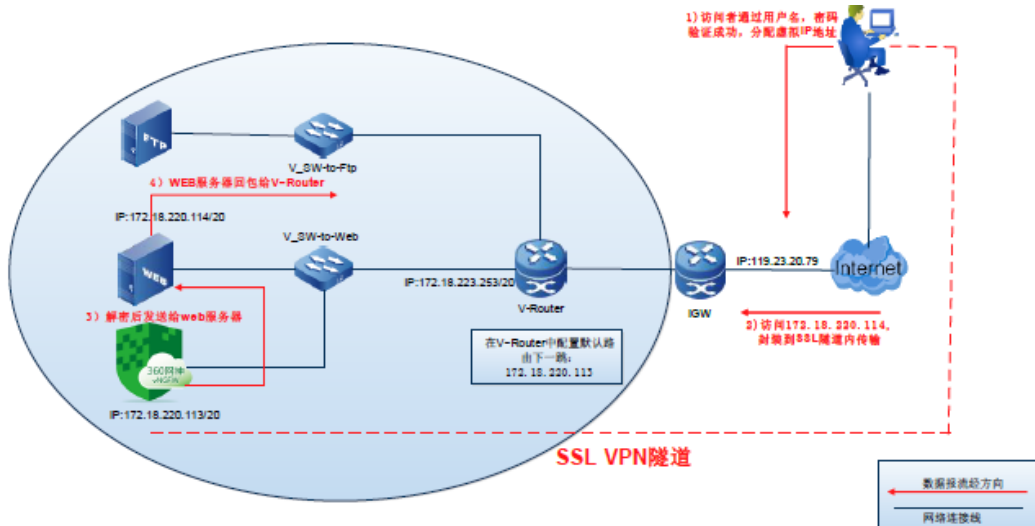


图 26

三、 具体配置

(一) 进入->用户认证->认证用户, 添加一个认证用户, 如下图27所示:

认证用户	认证用户组	认证用户角色
基本设置		
名称	test	(1-63字符)
密码	*****	(1-31字符)
确认密码	*****	(1-31字符)
有效日期	2017/03/31 10:08	清空
描述		
<input type="button" value="确定"/> <input type="button" value="取消"/>		

在该时间内有效

图 27

有效日期必须和当前的系统时间匹配。

(二) 进入->用户认证->认证服务器->local, 编辑本地认证服务器, 增加“test”这个用户, 如下图28所示:

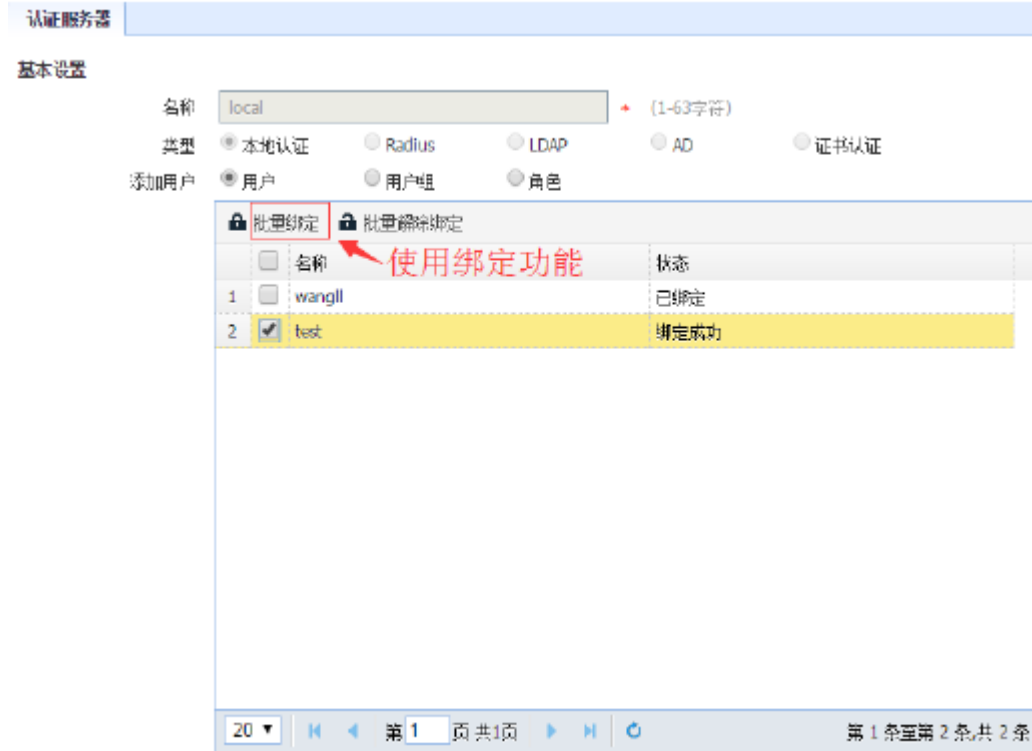


图 28

(三) 由于在SSL协议交互的时候需要使用到非对称加密技术-数字证书，奇安信vNGFW支持自签发数据证书：

1. 自签发CA根证书

进入->PKI->本地CA->本地CA，使用“生成自签发CA”功能，如下图29所示：



图 29

2. 生成“一般证书”

这个证书生成后系统会使用CA证书为这个“一般证书”签名，这个过程是系统自动完成，不需要您手工配置。

进入->PKI->本地CA->一般证书，生成一般证书，如下图30所示：

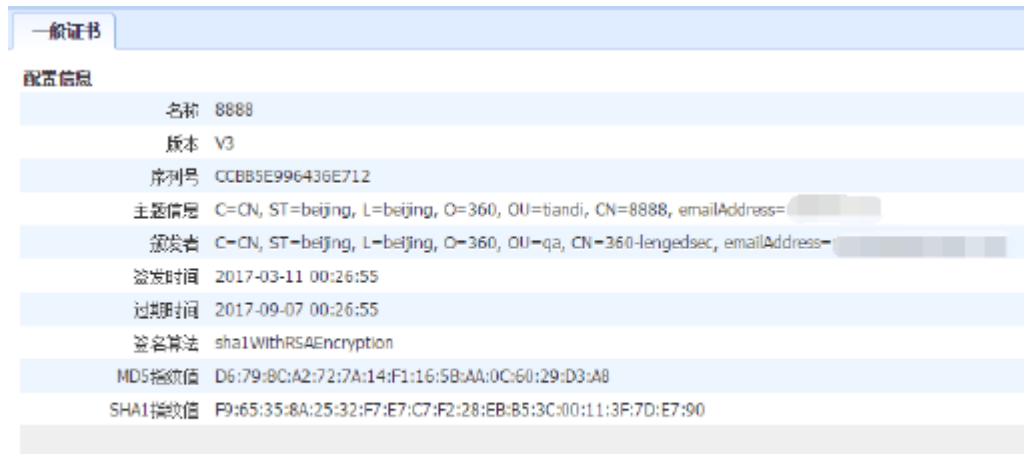


图 30

3. 导入可信CA

进入->PKI->证书管理->可信CA->导入，从本地CA中心导入CA证书，如下图31所示：



图 31

4. 导入本地证书

进入->PKI->证书管理->证书列表->导入，从本地CA中心导入一般证书，如下图32所示：

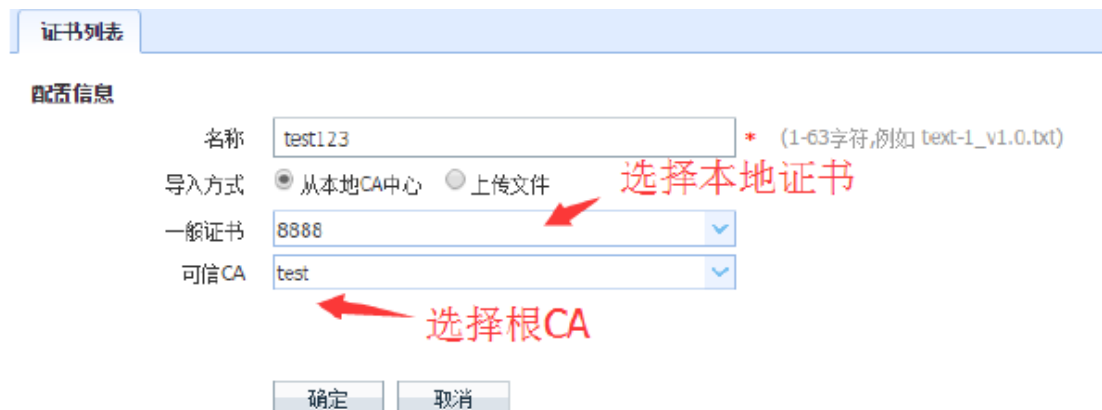


图 32

(四) 进入->隧道->地址池，创建一个用户SSL VPN的地址池，这个地址池地址就

是SSL VPN客户端的虚拟IP地址。如下图33

地址池

基本设置

名称 ssl-vpn (1-63字符)

起始地址 192 . 168 . 4 . 2 *

结束地址 192 . 168 . 4 . 10 *

网络掩码 255.255.255.0 *

DNS . . .

WINS . . .

VPN隧道

确定 取消

图 33

进

入->隧道->SSL VPN,添加一个SSL VPN规则，如下图34所示：

SSLVPN

基本设置

名称 ssl-vpn * (1-63字符)

接口 ge1 *

本端IP地址 172.18.220.113 *

端口 64443 * (1025-65535)

客户端地址池 ssl-vpn * ← 引用地址池

启用

证书设置

服务器证书 test123 * ← 引用证书

认证设置

认证方式 单因子认证 双因子认证

认证服务器 local * (当选择证书认证服务器后，默认开启客户端证书认证)

网络设置

可访问网络

目的地址	子网掩码	跃点数	操作
172.18.220.114	32	1	🗑️

填入服务器IP地址

图 34

(五) 进入->安全->安全规则，添加一条安全规则策略放行所需要的数据报，由于是测试所以添加的是全通的安全规则。如图十四所示。

(六) 进入->阿里云控制台->专有网络VPC->华南1->路由器中添加一条默认路由，

下一跳是vNGFW实例，它的作用是把VPC的流量引流到vNGFW上。具体的配置如下图所示：

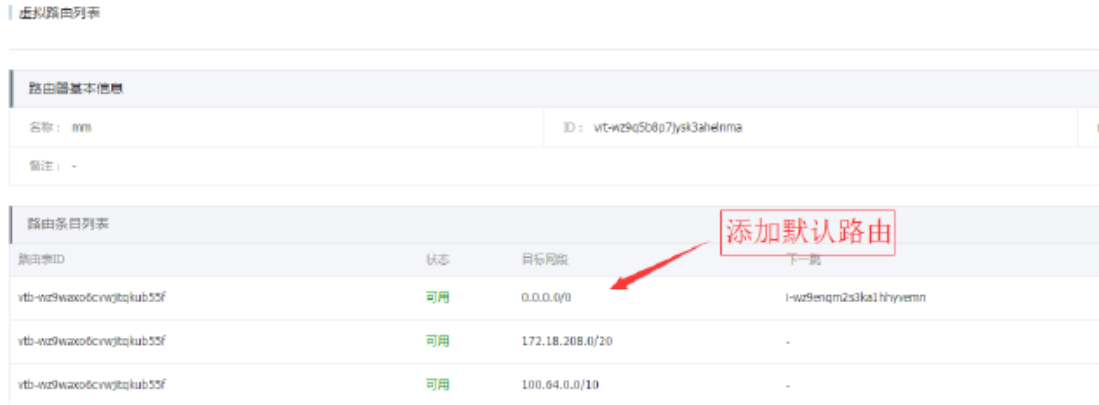


图 35

(七) 远程客户端操作：

1. 在客户端浏览器输入<https://119.23.20.79:64443/>,后下载vNGFW的SSL VPN客户端程序，如下图所示：

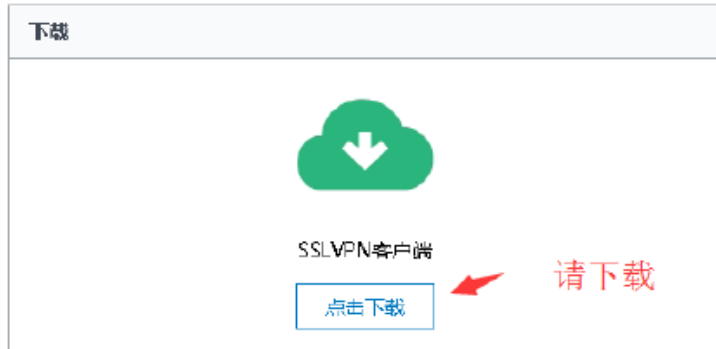
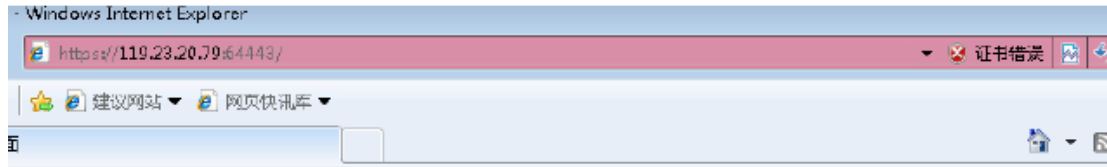


图 36

2. 安装完成后运行客户端程序，输入IP地址和端口号，端口号默认为64443，如下图所示：



3. 连接成功后请输入用户名密码，验证成功后客户端会分配到虚拟的IP地址，如下图所示：



图 38

4. 在客户端上访问服务器测试连通性，如下图39所示：

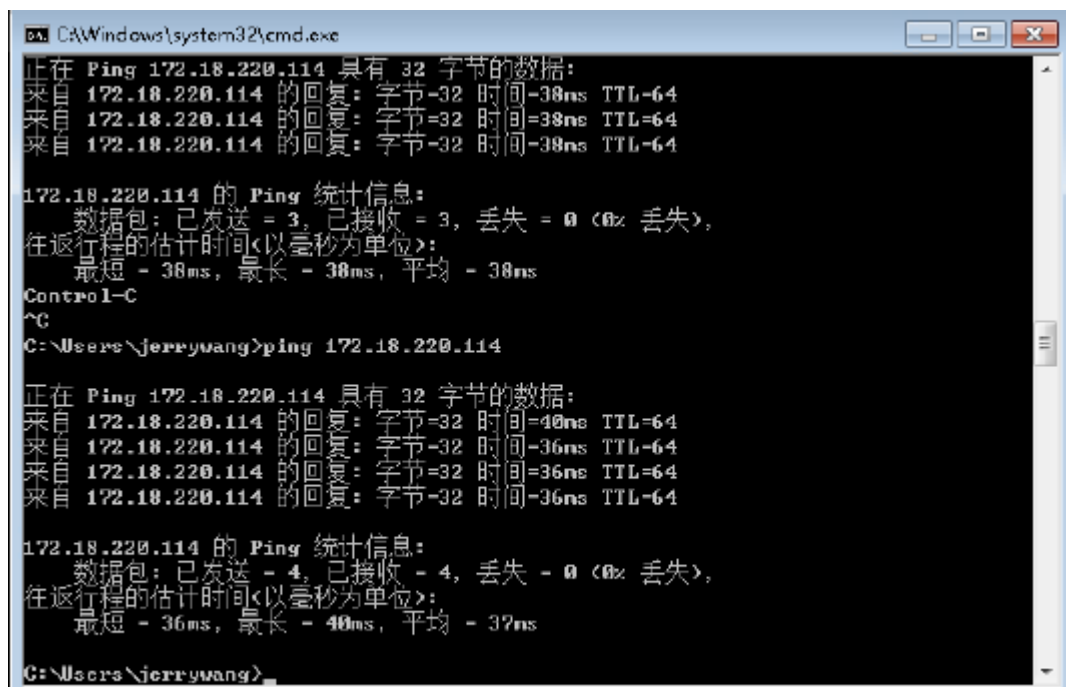


图 39

如果您对奇安信vNGFW的使用还有任何疑问请联系在线客服、400电话或直接邮件售后咨询。