

# Neusoft

东软 NetEye 虚拟安全网关快速向导  
(阿里云平台)

## 版权所有

本软件和相关文档的版权归沈阳东软系统集成工程有限公司所有，任何侵犯版权的行为都将被追究法律责任。未经版权所有者的书面许可，不得将本软件的任何部分或全部及其用户手册以任何形式、采用任何手段（电子的或机械的，包括照相复制或录制）、为任何目的，进行复制或传播。

版权所有 © 2001-2017 沈阳东软系统集成工程有限公司。所有权利保留，侵权必究。

沈阳东软系统集成工程有限公司不对因使用本软件及其用户手册所造成的任何损失承担任何责任。

---

## 东软联系信息

网站: <http://www.neteye.neusoft.com>

电子信箱: [servicedesk@neusoft.com](mailto:servicedesk@neusoft.com)

服务电话: 400 655 6789

---

# 目录

前言	3
<b>1 NISG-VA 功能概述</b>	<b>5</b>
<b>2 在专有网络中部署 NISG-VA 实例</b>	<b>7</b>
2.1 部署 VPC 环境并创建 NISG-VA 实例	7
2.1.1 NISG-VA 基本使用场景	8
2.1.2 创建 VPC 和虚拟交换机	9
2.1.3 创建 NISG-VA 实例	11
2.1.4 绑定弹性公网 IP 地址	13
2.1.5 登录到 NISG-VA	14
2.1.6 创建 VPC 内缺省路由条目	15
2.1.7 创建服务器实例	15
2.2 NISG-VA 典型使用场景	16
2.2.1 场景一：NAT 服务器	17
2.2.1.1 配置 VPC	18
2.2.1.2 配置 NISG-VA	19
2.2.2 场景二：远程访问 VPN 网关（拨号）	20
2.2.2.1 配置 VPC	21
2.2.2.2 配置 NISG-VA	22
2.2.2.3 配置远程用户的 VPN 客户端	23
2.2.3 场景三：站点到站点 VPN 网关	24
2.2.3.1 配置 VPC	25
2.2.3.2 配置 NISG-VA1	26
2.2.3.3 配置 NISG-VA2	27
<b>3 在经典网络中部署 NISG-VA 实例</b>	<b>29</b>
3.1 创建 NISG-VA 实例	30
3.2 典型场景：DoS 攻击防御	33
3.2.1 配置安全域	34
3.2.2 配置 DoS 攻击防御	34
3.2.3 配置地址转换	34
3.2.4 配置访问策略	34

# 前言

本文档介绍如何在阿里云平台上部署东软 NetEye 虚拟安全网关（以下简称 NISG-VA）。目标读者为具备以下知识的 NISG-VA 管理员：

- NISG-VA 产品特性
- 阿里云平台专有网络（VPC）和云服务器（ECS）

本文档包括：

- [第 1 章，NISG-VA 功能概述](#)
- [第 2 章，在专有网络中部署 NISG-VA 实例](#)
- [第 3 章，在经典网络中部署 NISG-VA 实例](#)

# 1 NISG-VA 功能概述

NISG-VA 是面向应用的下一代虚拟化防火墙，可以为云服务提供全面的网络安全功能，保护用户云计算资源的安全。通过过滤和控制阿里云内部和外部流量，能够有效解决云平台用户网络的区域隔离、边界控制、访问控制、风险识别、应用安全、攻击防御等问题。

NISG-VA 的主要功能特性为如下：

功能	特性说明
防火墙	通过以下特性对流经的网络流量进行访问控制： <ul style="list-style-type: none"><li>• 访问策略（参见 <a href="#">2.2 NISG-VA 典型使用场景</a>）</li><li>• IP-MAC 绑定策略</li><li>• 会话策略</li></ul>
UTM	通过以下特性对应用层数据进行解析、检测和控制，有效防御应用层攻击： <ul style="list-style-type: none"><li>• 应用识别和控制</li><li>• 防病毒</li><li>• 反垃圾邮件</li><li>• IPS</li></ul>
地址转换	通过以下特性对数据包的 IP 地址（端口）进行转换，将流量牵引到 NISG-VA，以实现 NISG-VA 对流量的过滤和控制；满足内网实例访问公网及被公网用户访问的需求；同时隐藏内网的网络拓扑： <ul style="list-style-type: none"><li>• 源地址转换（请参见 <a href="#">2.2.1 场景一：NAT 服务器</a>）</li><li>• 目的地址转换（请参见 <a href="#">2.2.1 场景一：NAT 服务器</a>）</li><li>• 地址映射</li></ul>
VPN	作为 VPN 网关，在以下场景中建立 VPN 隧道，对通信数据进行加密，以保证传输安全： <ul style="list-style-type: none"><li>• VPC 网络和本地网络</li><li>• VPC 网络和远程用户（请参见 <a href="#">2.2.2 场景二：远程访问 VPN 网关（拨号）</a>）</li><li>• 两个 VPC 网络之间（请参见 <a href="#">2.2.3 场景三：站点到站点 VPN 网关</a>）</li></ul>
攻击防御	防御各种网络攻击，如 DoS/DDoS 攻击、ICMP 攻击、端口扫描、扫描攻击，等等。
监控	全面监控系统信息，以便及时获取网络动态，更好地维护系统和制定安全策略。
报表	可定制的报表功能，通过图表的形式将系统实时记录的信息展现出来，以使管理员了解系统和网络安全状态，采取进一步的防范措施。

NISG-VA 还提供其他多种网络安全功能，例如：安全域、用户认证、虚拟系统、DHCP 服务器、多播、DNS 主机、路由、STP，等等。关于 NISG-VA 更多的特性信息，请参见 *东软 NetEye 虚拟安全网关用户使用指南*。

# 2 在专有网络中部署 NISG-VA 实例

本章介绍如何在阿里云平台的专有网络（VPC）中创建 NISG-VA 实例，同时介绍 NISG-VA 在 VPC 中的使用场景，包括以下内容：

- 2.1 部署 VPC 环境并创建 NISG-VA 实例
- 2.2 NISG-VA 典型使用场景

---

**提示：**由于阿里云平台的 WebUI 是不定期更新的，请以实际的阿里云 WebUI 为准。

---

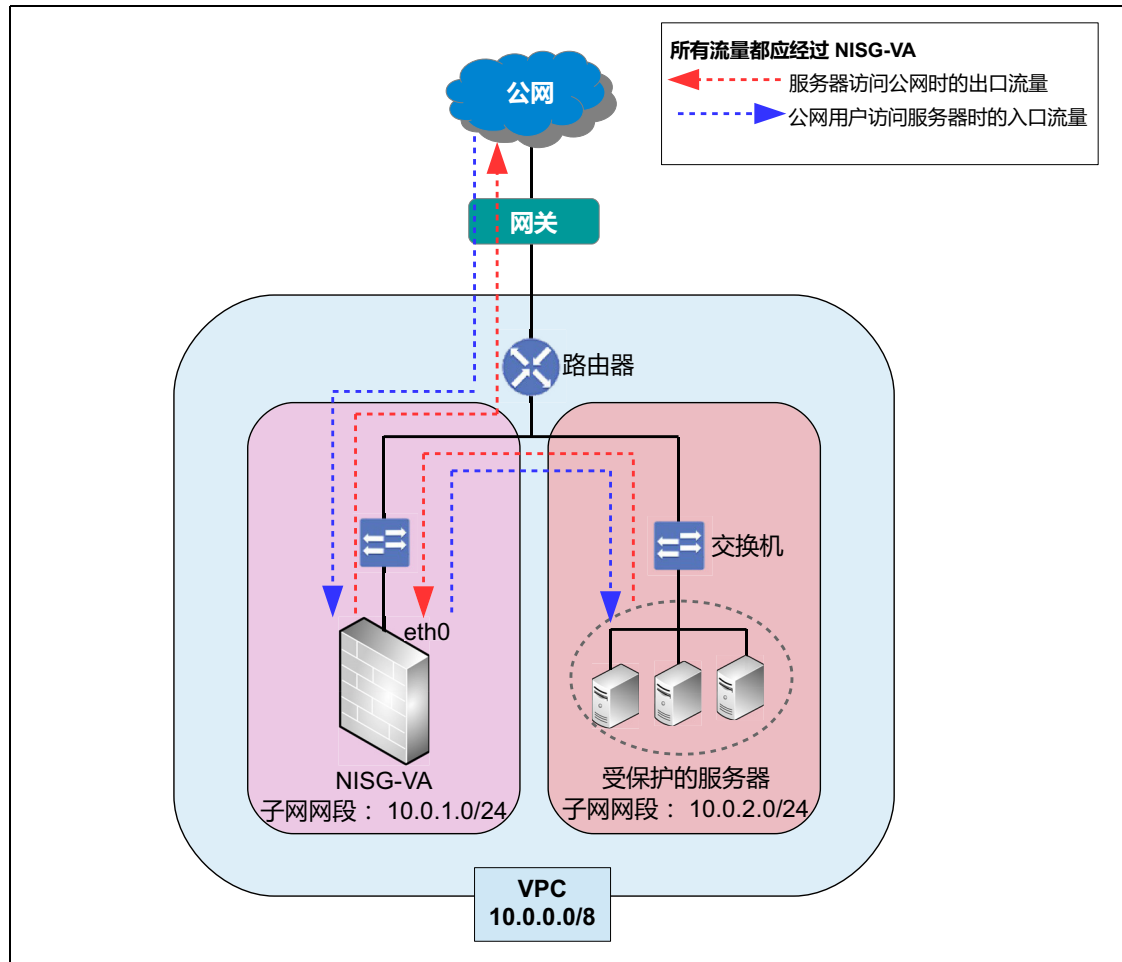
## 2.1 部署 VPC 环境并创建 NISG-VA 实例

本节介绍如何在阿里云平台上部署 VPC 环境并在 VPC 中创建 NISG-VA 实例，包括以下内容：

- 2.1.1 NISG-VA 基本使用场景
- 2.1.2 创建 VPC 和虚拟交换机
- 2.1.3 创建 NISG-VA 实例
- 2.1.4 绑定弹性公网 IP 地址
- 2.1.5 登录到 NISG-VA
- 2.1.6 创建 VPC 内缺省路由条目
- 2.1.7 创建服务器实例

## 2.1.1 NISG-VA 基本使用场景

下图为 NISG-VA 在 VPC 中的基本使用场景：



在开始配置之前，请先做好 VPC 网络拓扑计划。以下为本场景的网络规划：

1. 创建 VPC 并选择私有 IP 网段（10.0.0.0/8）。
2. 创建虚拟交换机并从 VPC 私有 IP 网段中为 NISG-VA 和服务子网划分子网网段（NISG-VA 子网 10.0.1.0/24，服务器子网 10.0.2.0/24）。
3. 创建 NISG-VA 实例并为其绑定弹性公网 IP 地址（123.56.3.208）。
4. 创建 VPC 内的缺省路由条目（目的为 0.0.0.0/0，下一跳为 NISG-VA 实例），以将流量牵引到 NISG-VA。
5. 登录到 NISG-VA 上，创建访问策略允许或拒绝特定流量访问 VPC 内资源和公网。
6. 创建服务器实例且不为其绑定弹性公网 IP 地址。
7. 在 NISG-VA 上创建源地址转换规则以使服务器访问公网。创建目的地址转换规则以使公网用户访问服务器，同时实现 NISG-VA 对到达 VPC 的流量进行控制的目的。

## 2.1.2 创建 VPC 和虚拟交换机

1. 登录到阿里云平台，在首页的菜单上，点击**控制台**。
2. 选择**专有网络 VPC > 专有网络**，选择**华北 2 区域**，点击**创建专有网络**。
3. 填写专有网络名称并选择网段，点击**确定**。创建成功后可以看见专有网络 ID 和路由器 ID 信息。

\*专有网络名称：

名称为2-128个字符，以大小字母或中文开头，可包含数字，"\_"或"-"

描述：

描述可以为空；或填写2-256个中英文字符，不能以http://和https://开头

\*网段：

① 一旦创建成功，网段不能修改

创建专有网络

✓ 创建专有网络成功

生成：

专有网络ID：

路由器ID： [管理路由器](#)

下面您可以继续：[管理交换机](#)

4. 点击**管理交换机**并点击**创建交换机**，在 VPC 内为 NISG-VA 子网创建一个交换机。填写 NISG-VA 子网的交换机名称和网段，点击**确定**。

\*名称：

名称为2-128个字符，以大小字母或中文开头，可包含数字，"\_"或"-"

\*专有网络：

专有网络网段：

\*可用区：

① 创建后无法修改

\*网段：

① 创建后无法修改

必须等于或属于该专有网络的网段，网段掩码必须在16和29之间。  
例如：192.168.1.0/24

可用IP数：252 个

描述：

描述可以为空；或填写2-256个中英文字符，不能以http://和https://开头

**提示：**在本文中，可用区使用的是**华北 2 可用区 B**。请根据实际需要选择可用区并在创建 NISG-VA 实例时选择相应的实例系列。NISG-VA 支持系列 1 和系列 2。



5. 点击**创建交换机**，为服务器子网创建交换机。填写交换机名称和网段，点击**确定**。

\*名称：   
 名称为2-128个字符，以大小字母或中文开头，可包含数字，"\_"或"-"

\*专有网络：   
 专有网络网段：

\*可用区：   
 ① 创建后无法修改

\*网段：   
 ① 创建后无法修改   
 必须等于或属于该专有网络的网段，网段掩码必须在16和29之间。   
 例如：192.168.1.0/24

可用IP数：252 个

描述：   
 描述可以为空；或填写2-256个中英文字符，不能以http://和https://开头

6. 创建成功后在交换机列表中可以看到交换机的信息。

交换机 ID/名称	ECS实例数	网段	状态	可用区	可用私有IP数	创建时间	默认交换机	描述	操作
vsw-mu6uht3ky 交换机-服务器	0	10.0.2.0/24	可用	华北 2 可用区 B	252	2016-07-11 17:53:31	否		<a href="#">编辑</a>   <a href="#">删除</a> <a href="#">创建实例</a>
vsw-8zs0u6z1m 交换机-NISG-VA	0	10.0.1.0/24	可用	华北 2 可用区 B	251	2016-07-11 17:06:39	否		<a href="#">编辑</a>   <a href="#">删除</a> <a href="#">创建实例</a>

## 2.1.3 创建 NISG-VA 实例

- 在交换机列表中，点击交换机 -NISG-VA 对应的创建实例并选择创建 ECS 实例。

交换机 ID/名称	ECS实例数	网段	状态	可用区	可用私有IP数	创建时间	默认交换机	描述	操作
vsw-8zs0u6z1m 交换机-NISG-VA	0	10.0.1.0/24	可用	华北 2 可用区 B	252	2016-07-11 17:06:39	否		编辑   删除 创建实例

**提示：**在本文档中，创建实例时引用的安全组为缺省安全组，即允许所有流量通过，以免与 NISG-VA 的访问策略配置产生冲突。请参考以下配置信息创建 NISG-VA 实例，其他区域的参数可以使用缺省配置。

- 选择按量付费。可以根据实际需要选择其他付费方式。

- 在网络类型区域，选择交换机 -NISG-VA。推荐选择内存为 2GB 以上的实例规格，以保证正常使用 NISG-VA 的 UTM 功能。1GB 规格的实例不包含 UTM 功能。

- 在带宽区域，推荐选择按固定带宽并将带宽设置为 0 Mbps。可以在部署 NISG-VA 后再购买弹性 IP 地址，以免使用 NISG-VA 时无法解绑其使用的公网 IP 地址。

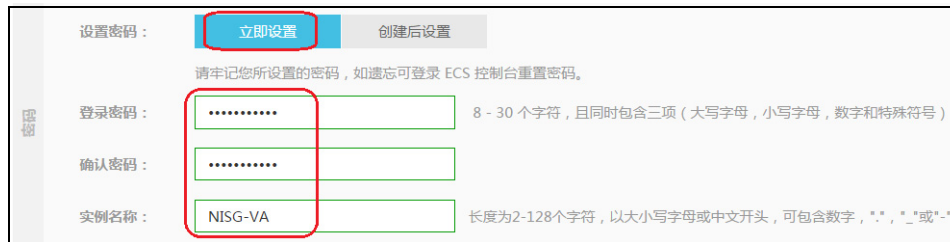
- 在**镜像**区域，选择**镜像市场**并点击**从镜像市场选择**（含操作系统）。
- 选择**云安全市场**，在搜索栏里输入 **neteye** 并按下回车键，东软 **NetEye 虚拟安全网关** 即出现在下方。点击**同意并使用**。



- 在**存储**区域，请根据实际需要选择系统盘。NISG-VA 的本地日志信息缺省存储于系统盘中。如果本地日志信息量非常大、记录的时间又很长，可以额外选购数据盘；也可以释放已购买的数据盘。



- 在**密码**区域，选择**立即设置**，设置 NISG-VA 的登录密码。请不要忘记此密码，以免无法成功登录到 NISG-VA。为方便查看实例信息，可以在此处设置实例名称。



- 点击**立即购买并开通实例**。开通成功后，点击**管理控制台**。点击**云服务器**，查看刚刚创建的实例的信息。

可以看到实例被分配的私有 IP 地址为 10.0.1.1，如需修改此地址，点击**管理**，在**配置信息**区域，点击**更多**并选择**修改私网 IP**。



## 2.1.4 绑定弹性公网 IP 地址

NISG-VA 实例成功启动后，便可为其绑定弹性公网 IP 地址。管理员可以通过此 IP 地址管理 NISG-VA。

1. 在**专有网络**页面，点击**弹性公网 IP 管理**。选择**华北 2** 并点击**申请弹性公网 IP**。
2. 请根据实际需要进行选择并点击**立即购买**。

包年包月 | 按量付费

地域：  
 华北 2 (北京) | 华东 1 (杭州) | 香港 | 华南 1 (深圳) | 华东 2 (上海) | 亚太东南 1 (新加坡) | 美西 (硅谷)  
 亚太东北 1 (日本) | 欧洲中部 1 (法兰克福) | 中东东部 1 (迪拜)  
 美东 (弗吉尼亚) | 本 | 兰克福 | 拜

不同地域之间的产品内网不互通；订购后不能更换地域，请谨慎选择教我选择>>

带宽峰值：  
 50Mbps | 100Mbps | 200Mbps | 1 Mbps

带宽计费方式：  
 按使用流量计费 | 按固定带宽计费

由带宽值决定每日账单价格，与实际使用的流量无关  
 支持随时调整带宽峰值；每日按照当天设置过的最高带宽计费；详细说明>>  
 一旦购买，带宽计费类型不能变

计费周期：  
 按天

购买数量：  
 1

3. 返回到**弹性公网 IP** 页面，可以看到已申请的 IP 地址。

实例 ID	IP地址	监控	带宽	计费类型(全部)	状态(全部)	绑定实例	实例类型	操作
eip-2zer5gq5i32h5apmj5s3s	123.56.10.242		按使用流量计费 1Mbps	按量付费	2016-11-23 10:10:30 创建	可用	-	绑定   解绑 更多操作

4. 点击**绑定**，在**ECS 实例**下拉框中，选择 NISG-VA 实例，然后点击**确认**。绑定成功后，即可使用此 IP 地址通过 Web 或 SSH 方式登录到 NISG-VA。

绑定弹性公网IP

IP地址：  
123.56.3.208

实例类型：  
ECS 实例

\*ECS实例：  
i-25o0ddko5

只有处于运行中和已停止状态的云服务器实例可以绑定弹性公网IP

## 2.1.5 登录到 NISG-VA

1. 在管理主机上打开浏览器，在 IP 地址栏中输入“https://123.56.3.208”，按下回车，即跳转到 NISG-VA 的 WebUI 登录页面。



2. 输入用户名（Neusoft）和密码（在创建实例时设置的密码），点击登录。页面便跳转到 NISG-VA 的 WebUI 主页。在专有网络中，NISG-VA 实例提供 1 个网络接口（eth0）。



**提示：**NISG-VA 的访问策略缺省拒绝所有流量，可以根据实际需要创建访问策略（选择**防火墙 > 访问策略 > 新建**），允许或拒绝特定的流量通过，以保护 VPC 内网资源。访问策略配置完成后，可以继续配置其他 VPC 子网信息并创建服务器实例。

## 2.1.6 创建 VPC 内缺省路由条目

1. 在管理控制台页面，选择**专有网络 VPC > 专有网络 > VPC1 > 路由器**，点击**添加路由**。
2. 添加一条目标网段为 0.0.0.0/0 的缺省路由，并将下一跳设置为 NISG-VA 实例，用以将流量牵引到 NISG-VA。

\*目标网段：

必须是一个合法的CIDR或IP地址，例如：192.168.0.0/24 或 192.168.0.1

下一跳类型：

\*下一跳ECS实例：

3. 点击**确定**。创建成功后可以在路由表中查看创建的路由条目。

路由表ID	状态	目标网段	下一跳	下一跳类型	类型	操作
vtb-pdwbmh5we	可用	0.0.0.0/0	i-25o0ddko5	ECS 实例	自定义	删除
vtb-pdwbmh5we	可用	10.0.1.0/24	-	-	系统	-
vtb-pdwbmh5we	可用	10.0.2.0/24	-	-	系统	-
vtb-pdwbmh5we	可用	100.64.0.0/10	-	-	系统	-

## 2.1.7 创建服务器实例

请根据实际需要创建服务器实例。为了避免服务器遭受来自公网的攻击，服务器子网中的服务器实例应仅使用私有 IP 地址。如果为服务器实例绑定弹性公网 IP 地址，那么这些实例会绕过 NISG-VA 直接访问公网或被公网用户访问，而无法被 NISG-VA 保护。

由于已为 NISG-VA 绑定了弹性公网 IP 地址，阿里云平台会在 NISG-VA 的弹性公网 IP 地址和私有 IP 地址之间进行转换，所以 NISG-VA 可以访问公网，同时也可以被公网用户访问。

如果服务器实例需要访问公网，可以在 NISG-VA 上创建源地址转换规则，将实例的私有 IP 地址转换为 NISG-VA 接口 eth0 的私有 IP 地址。如果服务器实例需要提供对外服务，可以在 NISG-VA 上创建目的地址转换规则，将 NISG-VA 接口 eth0 的私有 IP 地址转换为实例的私有 IP 地址。这样服务器就可以通过 NISG-VA 的弹性公网 IP 地址访问公网，公网用户也可以通过此弹性公网 IP 地址访问服务器。



通过源和目的地址转换规则，可以隐藏实例的私有 IP 地址，并将流量牵引到 NISG-VA 使 NISG-VA 对流量进行检测和控制，因此可以保证服务器数据的安全。关于地址转换的更多信息，请参见 [2.2.1 场景一：NAT 服务器](#)。

## 2.2 NISG-VA 典型使用场景

本节通过以下典型场景说明如何在阿里云平台上快速部署 NISG-VA：

- [2.2.1 场景一：NAT 服务器](#)
- [2.2.2 场景二：远程访问 VPN 网关（拨号）](#)
- [2.2.3 场景三：站点到站点 VPN 网关](#)

---

**提示：** 请根据范例中的参数信息配置 NISG-VA，其他参数可以使用缺省配置。完成每个配置后，点击**确定**使其生效，点击保存配置。如果不保存配置，在 NISG-VA 重启后配置会丢失，因此，建议完成配置后，点击.

---

关于 NISG-VA 的详细功能特性，请参见东软 *NetEye 虚拟安全网关用户使用指南*。

## 2.2.1 场景一：NAT 服务器

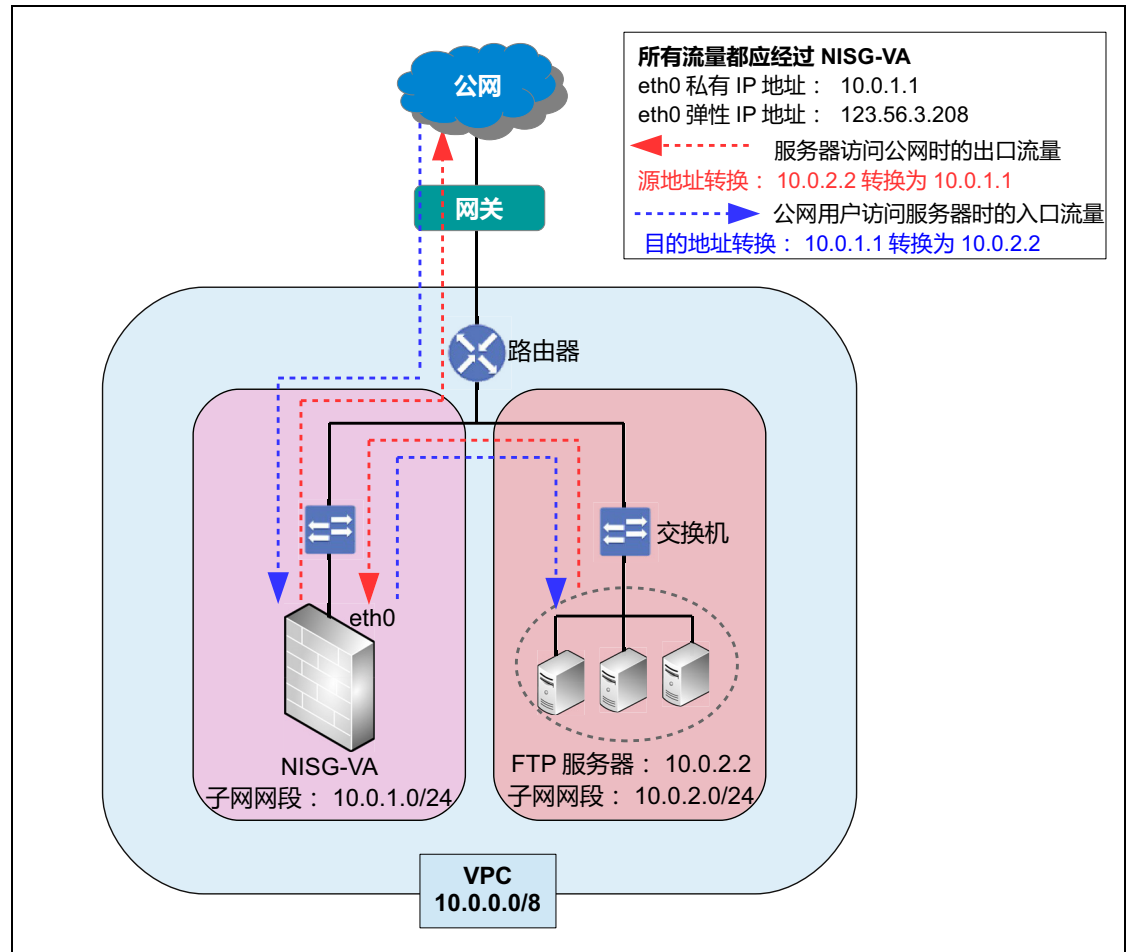
NISG-VA 可以作为 NAT 服务器，将一个 IP 地址 / 端口转换为另一个 IP 地址 / 端口，以满足牵引流量、访问网络、隐藏 IP 地址和节省 IP 地址的需求。

在本场景中，NISG-VA 可以访问公网也可以被公网用户访问。服务器子网中的三个服务器没有弹性公网 IP 地址，既无法访问公网也无法被公网用户访问。

### 基本需求

- 所有服务器需访问公网以便完成定期更新。
- FTP 服务器（10.0.2.2）需提供对外服务，以便公网用户下载服务器上的资料。
- 不允许公网用户访问除 FTP 服务器外的其他服务器。

### 应用场景



### 配置信息

- [2.2.1.1 配置 VPC](#)
- [2.2.1.2 配置 NISG-VA](#)



### 2.2.1.1 配置 VPC

1. 创建 VPC，配置信息为如下：

VPC 名称	网段
VPC	10.0.0.0/8

2. 在 VPC 中创建两个交换机，用于连接 NISG-VA 子网和服务器子网：

交换机名称	网段
NISG-VA 交换机	10.0.1.0/24
服务器交换机	10.0.2.0/24

3. 在 NISG-VA 交换机中创建 NISG-VA 实例，在服务器交换机中创建服务器实例，并为 NISG-VA 实例绑定一个弹性 IP 地址：

属于的交换机	实例名称	私有 IP 地址	绑定的弹性 IP 地址
NISG-VA 交换机	NISG-VA	10.0.1.1	123.56.3.208
服务器交换机	服务器 1	10.0.2.2	无
	服务器 2	10.0.2.3	
	服务器 3	10.0.2.4	

4. 在 VPC 中创建一条缺省路由，将流量牵引到 NISG-VA 实例上：

目标网段	下一跳	下一跳类型
0.0.0.0/0	NISG-VA 实例 ID	ECS

### 2.2.1.2 配置 NISG-VA

1. 在管理主机上打开浏览器，在 IP 地址栏中输入“https://123.56.3.208”，登录到 NISG-VA 的 WebUI 上。
2. 选择网络 > 地址转换 > 源地址转换，点击新建，创建一条源地址转换规则，将所有服务器的私有 IP 地址转换为 NISG-VA 接口 eth0 的私有 IP 地址，以使服务器可以访问公网。


名称	启用	NAPT	源 IP 地址	转换后 IP 地址 / 接口
snat	勾选	勾选	10.0.2.0/24	接口: eth0

3. 选择网络 > 地址转换 > 目的地址转换，点击新建，创建目的地址转换规则 ftpdnat，将 NISG-VA 接口 eth0 的私有 IP 地址转换为 FTP 服务器的私有 IP 地址，以使公网用户可以访问 FTP 服务器。

名称	启用	NAPT	目的 IP 地址	转换后 IP 地址
ftpdnat	勾选	勾选	<ul style="list-style-type: none"> <li>• 10.0.1.1</li> <li>• TCP: 21</li> </ul>	<ul style="list-style-type: none"> <li>• 常规: 10.0.2.2</li> <li>• 端口: 21</li> </ul>

4. 选择防火墙 > 访问策略，点击新建，创建访问策略 snat 允许 VPC 内服务器访问公网，创建 dnat 允许公网用户访问 FTP 服务器。

名称	启用	源 IP 地址	目的 IP 地址	服务	动作
snat	勾选	10.0.2.0/24	任意	任意	允许
dnat	勾选	任意	10.0.2.2	<ul style="list-style-type: none"> <li>• 自定义: TCP</li> <li>• 源 / 目的端口: 1~65535/21</li> </ul>	允许

5. 点击 。

## 2.2.2 场景二：远程访问 VPN 网关（拨号）

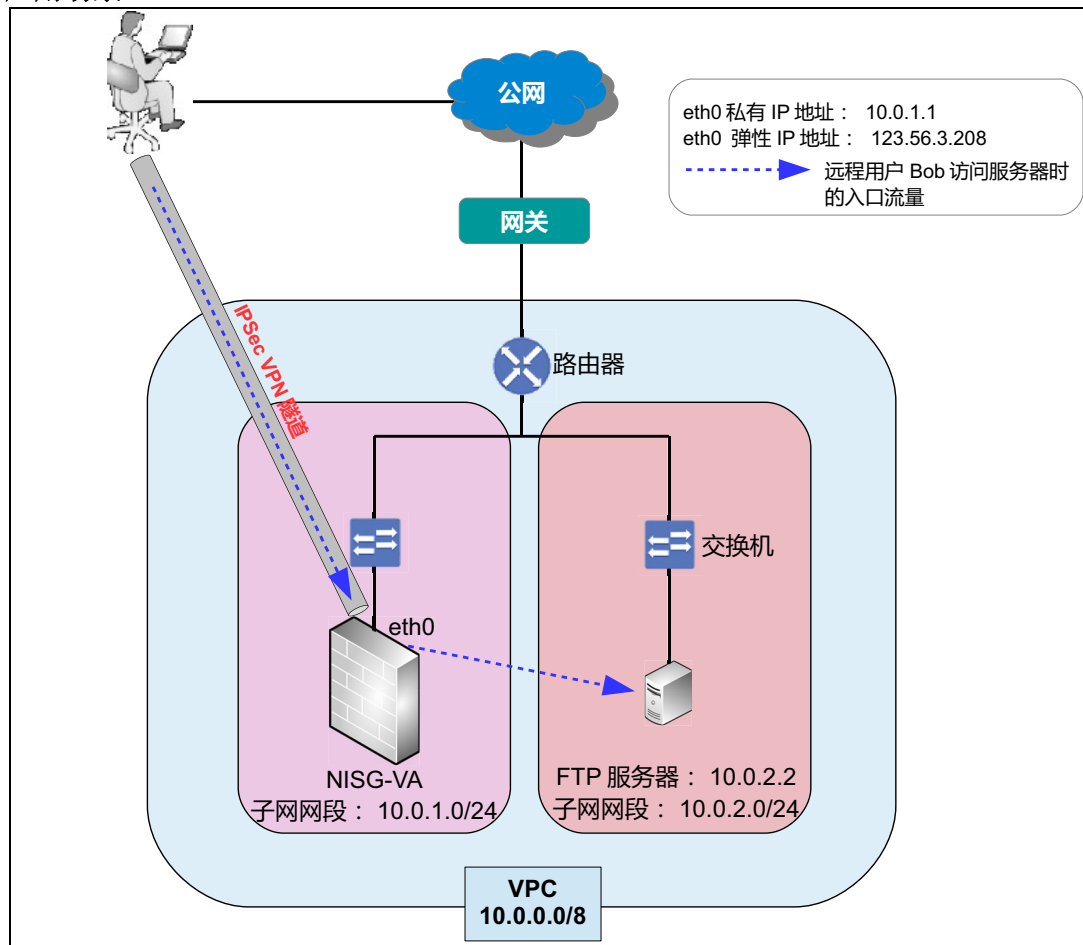
NISG-VA 可以作为远程访问 VPN 网关，为远程用户访问 VPC 内网资源提供快速、安全的 VPN 隧道。

在本场景中，远程用户 Bob 使用 Windows 操作系统，且已具有访问公网的权限。Bob 的主机上已安装东软 NetEye VPN 客户端（以下简称“VPN 客户端”）。

### 基本需求

- Bob 需要从 VPC 内的 FTP 服务器上下载资料且通信数据应受到保护。通过使用 VPN 客户端，Bob 可以与 NISG-VA 之间建立一条 IPsec VPN 隧道并通过 VPN 隧道访问 VPC 内的 FTP 服务器。
- 不允许其他用户访问 FTP 服务器也不允许 FTP 服务器访问公网。

### 应用场景



### 配置信息

- [2.2.2.1 配置 VPC](#)
- [2.2.2.2 配置 NISG-VA](#)
- [2.2.2.3 配置远程用户的 VPN 客户端](#)

### 2.2.2.1 配置 VPC

1. 创建 VPC，配置信息为如下：

VPC 名称	网段
VPC	10.0.0.0/8

2. 在 VPC 中创建两个交换机用于连接 NISG-VA 子网和服务器子网机：

交换机名称	网段
NISG-VA 交换机	10.0.1.0/24
服务器交换机	10.0.2.0/24

3. 在 **NISG-VA 交换机** 中创建 NISG-VA 实例，在 **服务器交换机** 中创建服务器实例，并为 NISG-VA 实例绑定一个弹性 IP 地址：

属于的交换机	实例名称	私有 IP 地址	弹性 IP 地址
NISG-VA 交换机	NISG-VA	10.0.1.1	123.56.3.208
服务器交换机	服务器	10.0.2.2	无

4. 在 VPC 上创建一条缺省路由，将流量牵引到 NISG-VA 实例上：

目标网段	下一跳	下一跳类型
0.0.0.0/0	NISG-VA 实例 ID	ECS

### 2.2.2.2 配置 NISG-VA

1. 在管理主机上打开浏览器，在地址栏中输入“https://123.56.3.208”，登录到 NISG-VA 的 WebUI 上。
2. 先后选择**系统 > 证书 > CA 证书**和**系统 > 证书 > 本地证书**，点击**导入**，导入远程用户的 CA 证书和本地证书。
3. 选择**VPN > IP 地址池**，点击**新建**，创建 IP 地址池。NISG-VA 将从该地址池中为远程用户分配一个 IP 地址。远程用户使用此 IP 地址与 NISG-VA 建立 VPN 连接。IP 地址池中包含的地址不能与受 NISG-VA 保护的子网内的 IP 地址重合，以免引起网络问题。

名称	起始 IP 地址	终止 IP 地址
pool1	60.1.1.1	60.1.1.100

4. 选择**系统 > 认证 > 网络用户**，点击**新建**，创建名为 Bob 的 IPSec VPN 用户。Bob 使用此用户信息与 NISG-VA 建立 IPSec VPN 隧道。

名称	用户类型	密码	VPN
Bob	<ul style="list-style-type: none"> <li>• IPSec VPN: <input checked="" type="checkbox"/></li> <li>• 允许 IPSec VPN 多点登录: <input checked="" type="checkbox"/></li> </ul>	<ul style="list-style-type: none"> <li>• 密码: 123456</li> <li>• 密码确认: 123456</li> </ul>	IP 地址池 (点击): pool1
<b>IPSec VPN 配置</b>			
<ul style="list-style-type: none"> <li>• L2TP: 点击</li> <li>• ID 类型: DER_ASN1_DN</li> <li>• ID: C=AU,ST=SS,O=SS,OU=SS,CN=Bob,emailAddress=SS@SS.com (由于 Bob 的身份认证需要证书认证, 此处需填写 Bob 本地证书的主题信息, 且不包含空格。)</li> </ul>			

5. 选择**VPN > IPSec VPN > 自动密钥隧道**，点击**新建**，创建自动密钥隧道。

名称	启用	对端	出口	认证方式 (证书)	子网
bobvpn	<input checked="" type="checkbox"/>	拨号用户: Bob	<ul style="list-style-type: none"> <li>• 出口: eth0</li> <li>• 本端 IP 地址: 10.0.1.1</li> </ul>	<ul style="list-style-type: none"> <li>• 本地证书: Bob</li> <li>• 对端 CA 证书: BobCA</li> </ul>	10.0.2.0/24 (允许 Bob 访问的 VPC 网段)

6. 选择**防火墙 > 访问策略**，点击**新建**，创建访问策略 vpn 允许远程用户访问 VPC 内的 FTP 服务器。

名称	源 IP 地址	目的 IP 地址	服务	动作	VPN 隧道
vpn	60.1.1.1~60.1.1.100 (IP 地址池中的范围)	10.0.2.0/24	<ul style="list-style-type: none"> <li>• 自定义: TCP</li> <li>• 源 / 目的端口: 1~65535/21</li> </ul>	允许	bobvpn

7. 完成所有配置后，点击。

### 2.2.2.3 配置远程用户的 VPN 客户端

1. 在远程用户 Bob 的主机上打开 VPN 客户端，选择**证书>导入**，导入 Bob 的 CA 和个人证书，用于在 VPN 连接时进行身份认证。
2. 选择**VPN 连接**，点击**新建**，创建 Bob 和 NISG-VA 之间的 VPN 连接。

■ 点击**基本信息**选项卡，进行如下配置：

VPN 名称	服务器	用户名	密码
bobvpn	123.56.3.208	Bob	123456

■ 点击**网络设置**选项卡，点击**设置对端子网**，添加需要访问的 VPC 子网：

子网	掩码
10.0.2.0/24	255.255.255.0

**提示：**请根据实际网络访问需求，添加其他子网和掩码，以保证在 VPN 连接成功后网络访问的畅通。

3. 点击**确定**。
4. 选择刚刚创建的 VPN 连接，点击**连接**。  
待 VPN 连接状态为**已连接**时，说明 VPN 客户端已与 NISG-VA 成功建立了 VPN 连接。此时，远程用户 Bob 即可通过 IPSec VPN 隧道安全访问 VPC 内的 FTP 服务器。

## 2.2.3 场景三：站点到站点 VPN 网关

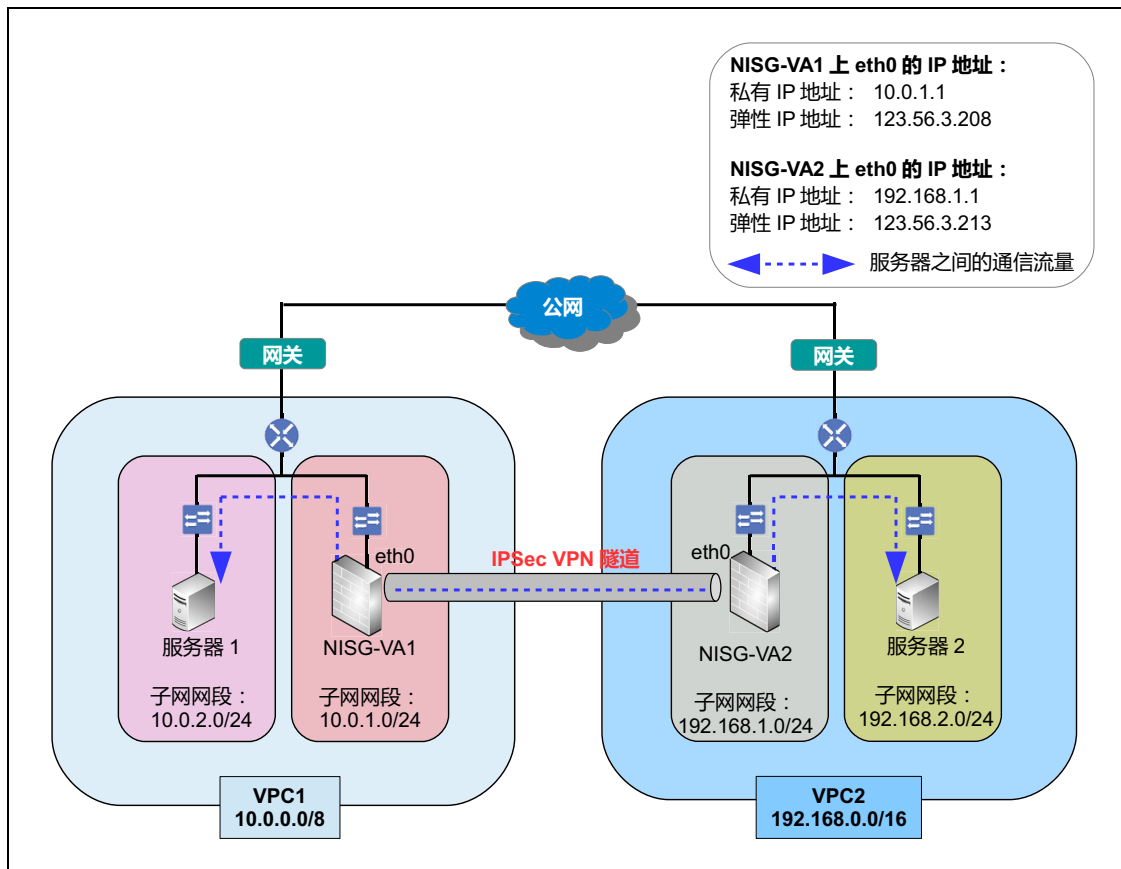
NISG-VA 可以作为站点到站点 VPN 网关，为不同 VPC 中子网之间或是 VPC 子网与本地子网之间的通信提供安全、稳定的 VPN 隧道。NISG-VA 也可以与其他支持标准 IPsec 协议的 VPN 网关之间进行互联。

本场景以不同 VPC 中的两个 NISG-VA 之间建立 IPsec VPN 隧道为例，介绍如何使用 NISG-VA 的 VPN 网关特性。

### 基本需求

VPC1 和 VPC2 中的服务器没有访问公网的权限，它们之间需要互相通信，且通信数据应加密并保证安全。

### 应用场景



### 配置信息

- [2.2.3.1 配置 VPC](#)
- [2.2.3.2 配置 NISG-VA1](#)
- [2.2.3.3 配置 NISG-VA2](#)

### 2.2.3.1 配置 VPC

1. 创建 VPC1 和 VPC2，配置信息为如下：

VPC 名称	网段
VPC1	10.0.0.0/8
VPC2	192.168.0.0/16

2. 在 VPC1 和 VPC2 中各创建两个交换机用于连接 NISG-VA 子网和服务器子网：

属于的 VPC	交换机名称	网段
VPC1	NISG-VA1 交换机	10.0.1.0/24
	服务器 1 交换机	10.0.2.0/24
VPC2	NISG-VA2 交换机	192.168.1.0/24
	服务器 2 交换机	192.168.2.0/24

3. 在每个交换机上都创建一个 NISG-VA 实例和服务器实例，并为两个 NISG-VA 实例各绑定一个弹性 IP 地址：

属于的 VPC	属于的交换机	实例名称	私有 IP 地址	弹性 IP 地址
VPC1	NISG-VA1 交换机	NISG-VA1	10.0.1.1	123.56.3.208
	服务器 1 交换机	服务器 1	10.0.2.2	无
VPC2	NISG-VA2 交换机	NISG-VA2	192.168.1.1	123.56.3.213
	服务器 2 交换机	服务器 2	192.168.2.1	无

4. 在每个 VPC 上各创建一条缺省路由，将流量牵引到 NISG-VA 实例：

属于的 VPC	目标网段	下一跳	下一跳类型
VPC1	0.0.0.0/0	NISG-VA1 实例 ID	ECS
VPC2	0.0.0.0/0	NISG-VA2 实例 ID	ECS




### 2.2.3.2 配置 NISG-VA1

1. 在管理主机上打开浏览器，在 IP 地址栏中输入“https://123.56.3.208”，登录到 NISG-VA1 的 WebUI 上，配置 VPN 隧道和访问策略。
2. 选择 VPN > IPsec VPN > 自动密钥隧道，点击**新建**，创建自动密钥隧道。

名称	启用
vpn1	勾选
对端	
<ul style="list-style-type: none"> <li>• 类型：静态 IP 地址</li> <li>• IP 地址 / 域名：123.56.3.213 (NISG-VA2 接口 eth0 的弹性 IP 地址)</li> </ul>	
出口	认证
<ul style="list-style-type: none"> <li>• 出口：eth0</li> <li>• 本端 IP 地址：10.0.1.1</li> </ul>	<ul style="list-style-type: none"> <li>• 认证方式：预共享密钥</li> <li>• 密钥：123456</li> </ul>
本端子网	对端子网
IP 地址：10.0.2.0/24	IP 地址：192.168.2.0/24
高级设置 > 本端 ID	高级设置 > 对端 ID
<ul style="list-style-type: none"> <li>• ID 类型：KEY_ID</li> <li>• 密钥 ID：123456</li> </ul>	<ul style="list-style-type: none"> <li>• ID 类型：KEY_ID</li> <li>• 密钥 ID：123456</li> </ul>

3. 选择**防火墙 > 访问策略**，点击**新建**，创建访问策略，允许 VPC1 和 VPC2 中的子网互相访问。

名称	源 IP 地址	目的 IP 地址	服务	动作	隧道
vpn1	10.0.2.0/24	192.168.2.0/24	任意	允许	vpn1
vpn2	192.168.2.0/24	10.0.2.0/24	任意	允许	无

4. 点击 。


### 2.2.3.3 配置 NISG-VA2

1. 在管理主机上打开浏览器，在 IP 地址栏中输入“https://123.56.3.213”，登录到 NISG-VA2 的 WebUI 上，配置 VPN 隧道和访问策略。
2. 选择 **VPN > IPSec VPN > 自动密钥隧道**，点击**新建**，创建自动密钥隧道。

名称	启用
vpn2	勾选
对端	
<ul style="list-style-type: none"> <li>• 类型：静态 IP 地址</li> <li>• IP 地址 / 域名：123.56.3.208 (NISG-VA1 接口 eth0 的弹性 IP 地址)</li> </ul>	
出口	认证
<ul style="list-style-type: none"> <li>• 出口：eth0</li> <li>• 本端 IP 地址：192.168.1.1</li> </ul>	<ul style="list-style-type: none"> <li>• 认证方式：预共享密钥</li> <li>• 密钥：123456</li> </ul>
本端子网	对端子网
IP 地址：192.168.2.0/24	IP 地址：10.0.2.0/24
高级设置 > 本端 ID	高级设置 > 对端 ID
<ul style="list-style-type: none"> <li>• ID 类型：KEY_ID</li> <li>• 密钥 ID：123456</li> </ul>	<ul style="list-style-type: none"> <li>• ID 类型：KEY_ID</li> <li>• 密钥 ID：123456</li> </ul>

3. 选择**防火墙 > 访问策略**，点击**新建**，创建访问策略，允许 VPC1 和 VPC2 中的子网互相访问。

名称	源 IP 地址	目的 IP 地址	服务	动作	隧道
vpn1	10.0.2.0/24	192.168.2.0/24	任意	允许	无
vpn2	192.168.2.0/24	10.0.2.0/24	任意	允许	vpn2

4. 完成所有配置后，点击 。

VPC1 内的服务器 1 和 VPC2 内服务器 2 便可以通过 IPSec VPN 隧道进行安全通信。

---

# 3

## 在经典网络中部署 NISG-VA 实例

本章介绍如何在阿里云平台的经典网络中创建 NISG-VA 实例，同时介绍 NISG-VA 的使用场景，包括以下内容：

- [3.1 创建 NISG-VA 实例](#)
- [3.2 典型场景：DoS 攻击防御](#)

---

**提示：**由于阿里云平台的 WebUI 是不定期更新的，请以实际的阿里云 WebUI 为准。

---

### 3.1 创建 NISG-VA 实例

1. 登录到阿里云平台，在首页的菜单上，点击**控制台**。
2. 点击左侧导航栏中的**云服务器 ECS**，点击**实例**并点击右上角的**创建实例**。

**提示：**在本文档中，可用区使用的是**华北 2 可用区 B**。请根据实际需要选择可用区并在创建 NISG-VA 实例时选择相应的实例系列。NISG-VA 支持系列 1 和系列 2。引用的安全组为缺省安全组，即允许所有流量通过，以免与 NISG-VA 的访问策略配置产生冲突。请对以下区域的参数进行配置，其他区域的参数使用缺省配置即可。

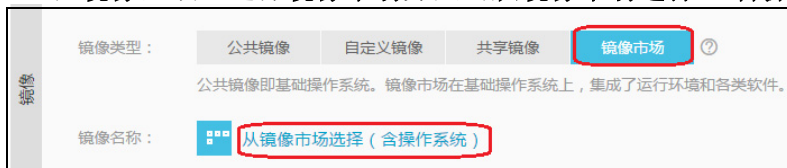
3. 选择**按量付费**。可以根据实际需要选择其他付费方式。推荐选择内存为**2GB**以上的实例规格，以保证正常使用 NISG-VA 的 UTM 功能。1GB 规格的实例不包含 UTM 功能。



4. 在**带宽**区域，请根据实际需求进行选择。



5. 在**镜像**区域，选择**镜像市场**并点击**从镜像市场选择（含操作系统）**。



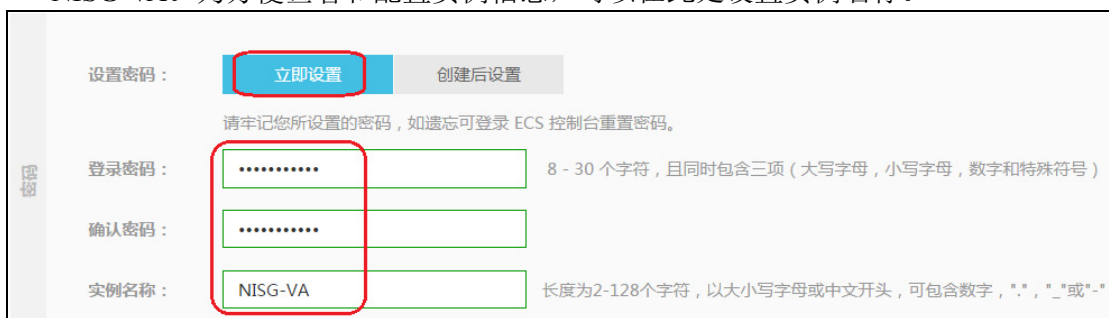
6. 选择**云安全市场**，在搜索栏里输入 **neteye** 并按下回车键，东软 **NetEye 虚拟安全网关** 即出现在下方。点击**同意并使用**。



7. 在**存储**区域，请根据实际需要选择系统盘。NISG-VA 的本地日志信息缺省存储于系统盘中。在如果本地日志信息量非常大、记录的时间又很长，可以额外选购数据盘；也可以释放已购买的数据盘。



8. 在**密码**区域，设置 NISG-VA 的登录密码。请不要忘记此密码，以免无法成功登录到 NISG-VA。为方便查看和配置实例信息，可以在此处设置实例名称。

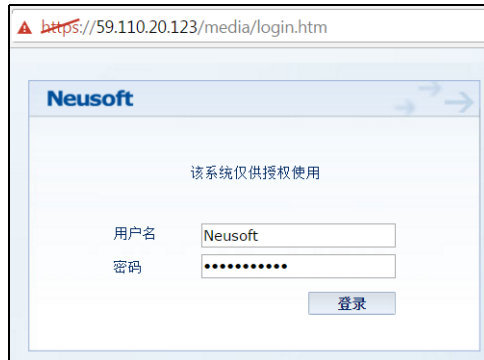


9. 点击**立即购买**并开通实例。开通成功后，点击**管理控制台**。

10. 点击**云服务器**，查看刚刚创建的实例的信息。可以看到实例被分配公网 IP 地址为 59.110.20.123，的私有 IP 地址为 10.28.48.197。

实例ID/名称	监控	所在可用区	IP地址	状态(全部)	网络类型(全部)	配置	付费方式(全部)
i-2zeistfz0zw16mszuiky NISG-VA		华北 2 可用区 B	59.110.20.123 (公) 10.28.48.197 (内)	运行中	经典网络	CPU: 1核 内存: 2048 MB 1Mbps	按量 16-11-15 15:35 创建

11. 在管理主机上打开浏览器，在 IP 地址栏中输入“https://59.110.20.123”，按下回车，即跳转到 NISG-VA 的 WebUI 登录页面。



12. 输入用户名（**Neusoft**）和密码（在创建实例时设置的密码），点击**登录**。页面便跳转到 NISG-VA 的 WebUI 主页。在经典网络中，NISG-VA 实例提供 2 个网络接口，eth0 和 eth1。



可以根据实际需求应用 NISG-VA 的功能特性，以保护云资源的安全。

## 3.2 典型场景：DoS 攻击防御

NISG-VA 可以防御各种网络攻击，如 DoS/DDoS 攻击、端口扫描、地址扫描、ICMP 攻击等，有效保护云平台服务器的安全。

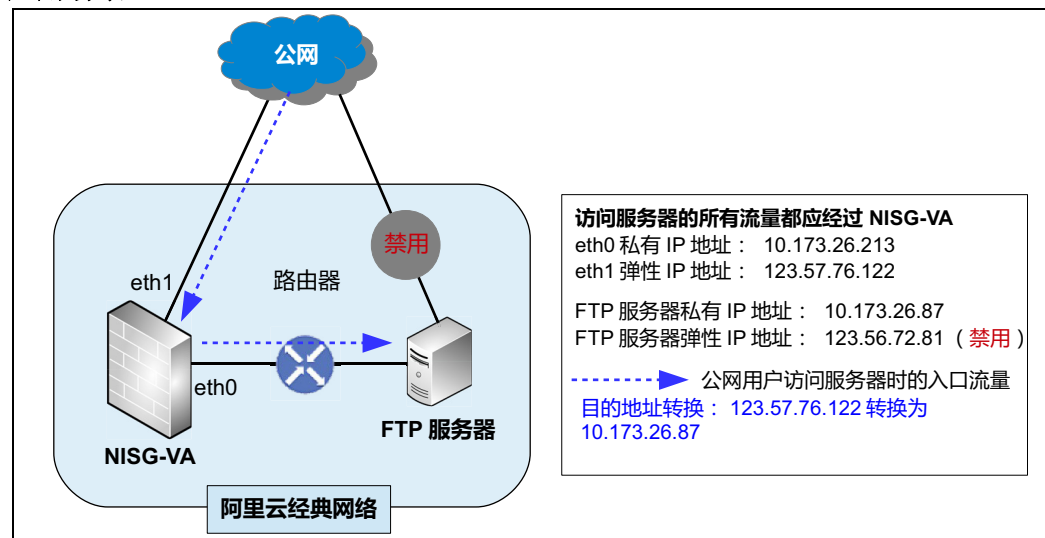
在本场景中，NISG-VA 实例和 FTP 服务器实例部署于经典网络中。FTP 服务器提供对外服务且具有访问公网的权限，但是容易遭受 DoS 攻击。

### 基本需求

- 使用 NISG-VA 的 NAT 特性以保证服务器能够正常提供对外服务，而不暴露其真实的私有 IP 地址。
- 使用 NISG-VA 的攻击防御特性，以保护服务器免于 DoS 攻击。

**提示：**请禁用服务器的公网 IP 地址，仅使用其私有 IP 地址，以免流量绕行过 NISG-VA，而达不到攻击防御的目的。

### 应用场景




在管理主机上打开浏览器，在 IP 地址栏中输入“https://123.57.76.122”，登录到 NISG-VA 的 WebUI 上，进行如下配置：

- [3.2.1 配置安全域](#)
- [3.2.2 配置 DoS 攻击防御](#)
- [3.2.3 配置地址转换](#)
- [3.2.4 配置访问策略](#)

### 3.2.1 配置安全域

1. 选择网络 > 安全域，点击新建，创建安全域并将 NISG-VA 接口 eth1 划分到安全域中。


名称	类型	接口
WAN	基于三层接口	eth1

2. 点击 。

### 3.2.2 配置 DoS 攻击防御

1. 选择防火墙 > 攻击防御 > DoS 攻击防御。
2. 在将下列设置应用于安全域下拉框中，选择安全域 WAN，以防御来自公网的攻击。
3. 设置需要防御的攻击类型、限制数据包个数的阈值以及 NISG-VA 对数据包个数达到阈值时的处理动作（报警、丢弃、或报警 + 丢弃）。可以使用 WebUI 参数的缺省值。也可以根据实际需要进行配置，如下表所示：

防御的攻击（勾选）	处理动作（勾选）
TCP RST 扫描	报警 + 丢弃

4. 点击 。


### 3.2.3 配置地址转换

1. 选择网络 > 地址转换 > 目的地址转换，点击新建，创建目的地址转换规则 ftpdnat，将 NISG-VA 接口 eth1 的弹性公网 IP 地址转换为 FTP 服务器的私有 IP 地址，以使公网用户可以访问 FTP 服务器。

名称	启用	NAPT	目的 IP 地址	转换后 IP 地址
ftpdnat	勾选	勾选	<ul style="list-style-type: none"> <li>123.57.76.122</li> <li>TCP: 21</li> </ul>	<ul style="list-style-type: none"> <li>常规: 10.173.26.87</li> <li>端口: 21</li> </ul>

2. 选择网络 > 地址转换 > 源地址转换，点击新建，创建源地址转换规则 allsnat，将所有源 IP 地址转换为 NISG-VA 接口 eth0 的私有 IP 地址，以便公网用户可以与服务器正常通信。


名称	启用	NAPT	源 IP 地址	转换后 IP/ 接口	入口接口	出口接口
allsnat	勾选	勾选	0.0.0.0-255.255.255.255	eth0	eth1	eth0

3. 点击 。

### 3.2.4 配置访问策略

1. 选择防火墙 > 访问策略，点击新建，创建策略 dnat 允许公网用户访问 FTP 服务器。

名称	启用	源安全域	源 IP 地址	目的 IP 地址	服务	动作
dnat	勾选	WAN	任意	10.173.26.87	<ul style="list-style-type: none"> <li>自定义: TCP</li> <li>源 / 目的端口: 1~65535/21</li> </ul>	允许

2. 点击 。