绿盟下一代防火墙云服务(vNF)
腾讯云快速实践指南

文档版本： V6.0R01F9724 (2018-10-19)

■ 版权声明

目录

前言

文档范围

本文详细介绍了绿盟科技下一代防火墙云服务(vNF)在腾讯云上的快速部署过程。

读者对象

本文档主要适用于以下读者：

- 期望了解在腾讯云部署的部署过程的用户
- 系统管理员
- 网络管理员

本文假设您对下面的知识有一定的了解：

- 系统管理
- Linux、Windows 操作系统
- Internet 协议
- 腾讯云相关知识，包括但不限于如下：

内容	链接
云服务器 CVM	https://cloud.tencent.com/document/product/213/12541
私有网络 VPC	https://cloud.tencent.com/document/product/215/8112
子网	https://cloud.tencent.com/document/product/215/4927
路由表	https://cloud.tencent.com/document/product/215/4954
安全组	https://cloud.tencent.com/document/product/213/18197
负载均衡 SLB	https://cloud.tencent.com/document/product/214/8974

内容概述

标题	概述
概述	介绍服务概况，说明本文的目的和适用范围

标题	概述
部署前准备工作	如何获取许可证、获取镜像
环境部署	从创建 VPC 开始，到完成所有实例的配置
导入许可证和快速配置	启用 vNF，配置 VPN 和安全防护策略，并验证效果

格式约定

符号	说明
粗体字	菜单、命令和关键字
斜体字	文档名、变量
	对描述内容的补充和引用信息
	使用设备时的技巧和建议
	需要特别注意的事项和重要信息
	有可能造成人身伤害的警告信息
【XXX】	按钮名称的表示方式
A > B	菜单项选择的表示方式

获得帮助

绿盟云

云端安全服务专家，为企业客户提供专业的 SaaS 安全服务。

网站：https://cloud.nsfocus.com

绿盟科技官网

可以帮助用户获取最新的网络安全信息和绿盟安全产品信息。

网站：http://www.nsfocus.com.cn

售后服务

提供全国范围内的服务热线，可以帮助用户解决在使用绿盟科技产品和服务过程中遇到的各种问题和困难。

网站：http://www.nsfocus.com.cn/operations/

软件升级

在进行产品使用培训后，可以帮助用户自助进行产品的升级操作。

网站：http://update.nsfocus.com/

产品生命周期公告

可以帮助用户获取已经停止的服务信息和已经下线的产品信息。

网站：http://www.nsfocus.com.cn/support/

1 概述

绿盟科技下一代防火墙虚云服务(vNF)，专门为虚拟化环境设计的网络安全产品，以虚拟化形态部署，适用于多种虚拟化平台，使管理员可以快速高效地调配和扩展防火墙。产品支持应用识别、入侵防御、内容过滤、URL 过滤、VPN 等，可以为用户提供 L4-L7 全面的安全服务。

本章主要包含以下内容：

功能	描述
绿盟下一代防火墙云服务(vNF)概述	简单介绍服务场景。
快速使用指南概述	简单介绍本指南的内容。

1.1 服务概述

绿盟下一代防火墙云服务(vNF)，是专门为虚拟化环境设计的网络安全产品，以虚拟化形态部署，适用于多种虚拟化平台，使管理员可以快速高效地调配和扩展防火墙。产品支持应用识别、入侵防御、内容过滤、URL 过滤、VPN 等，可以为用户提供 L4-L7 全面的安全服务。

- **入侵防护**

绿盟下一代防火墙云服务(vNF)威胁特征库超过 3000 条，由绿盟科技安全研究院精心提炼，并经过了长期考验，能够主动防御已知和未知攻击，实时阻断各种黑客攻击，如缓冲区溢出、SQL 注入、暴力猜测、拒绝服务、扫描探测、非授权访问、蠕虫、僵尸网络等。广泛精细的安全防护保障用户免受安全损失。

- **应用识别**

绿盟下一代防火墙云服务(vNF)可识别 1000+种应用，并可辅助用户对这些应用进行高效管理和筛查，包括 5 维度分类组织、基于特性查询应用、自定义特殊应用等，让用户明显的感觉到绿盟下一代防火墙云服务在应用识别和管理方面的专业性。

- **URL 过滤**

绿盟下一代防火墙云服务(vNF)内置先进、可靠的 Web 信誉库，采用独特的 Web 信誉评价技术，在用户访问挂马等有安全风险的网页时，给予及时报警和阻断，从而有效防止安全威胁通过 Web 访问渗入到企业内部，保障了企业机密信息不泄露。

- **内容过滤**

通过定义关键字，绿盟下一代防火墙云服务(vNF)可对网络传输中的网页、搜索、文件传输、邮件收发、论坛、服务器操作、即时通讯等应用的深层内容信息进行关键字过滤，并可根据用户需求，对匹配关键字的应用数据包进行检测、阻断、告警、记录和信息还原，从而实现了对内容的深度安全管理，避免用户机要信息、重要文件的外泄以及非法言论的传播等。

1.2 快速使用指南概述

本指南主要是指导使用者如何在腾讯云上快速使用绿盟科技下一代防火墙云服务(vNF)，通过一个具体示例的讲解，期望达到的目标是：

- 了解在部署 vNF 前需要准备哪些内容
- 了解如何快速按照需求部署 vNF

注意	本指南所涉及内容只适用于腾讯云，如果需要在其他公有云上使用，请联系我们获取更多信息

2 部署前准备工作

部署 vNF 之前，确认以下一些资源是否已经具备。

所需内容	用途
vNF 镜像地址	创建 vNF 虚拟机
vNF 许可证	需要导入到 vNF 的 CVM 实例后，才能正常开启防护功能

本章主要包含以下内容：

内容	描述
vNF 镜像获取	如何从腾讯云市场找找到绿盟云 vNF 产品
证书获取方法	最终用户如何获取这些资源

2.1 vNF 镜像获取

访问腾讯云首页，选择菜单 **云市场**，在搜索框中输入“绿盟下一代防火墙云服务”，即可看到本服务，选择立即购买，按照腾讯云的操作步骤创建虚机实例。

----结束

2.2 证书获取方式

当您在腾讯云市场下单购买 vNF 产品之后，可以联系您的客户经理或绿盟科技销售人员，告诉我们您的腾讯云订单号，服务开始时间以及其他重要的相关信息，信息确认无误后，我们将会在 3 个工作日完成证书生成工作，并将信息反馈给您。

----结束

3 VPN 功能示例

介绍客户在腾讯云上原始部署的逻辑结构、数据流向，以及使用 vNF 的 VPN 功能后的逻辑结构及数据流量的变化

虚拟专用网（Virtual Private Network，VPN）提供了一种在公共网络上建立专用数据通信网络的方法。通过基于共享的 IP 网络，VPN 为用户远程访问、外部网和内部网之间的通信提供了安全而稳定的 VPN 隧道。

对于构建 VPN 来说，网络隧道（Tunneling）技术是个关键技术。网络隧道技术指的是利用一种网络协议来传输另一种网络协议，它主要利用网络隧道协议来实现这种功能。

通常，网络连接由三部分组成：客户机、传输介质和服务器。VPN 同样也由这三部分组成，不同的是 VPN 连接使用隧道作为传输通道，这个隧道是建立在公共网络或专用网络基础之上的，例如：Internet 或 Intranet。VPN 隧道通常在企业的两个本地局域网，或远程用户和本地局域网之间使用，根据应用场景的不同，相应地分为网关到网关的 VPN 以及远程访问的 VPN。

本节主要内容介绍 vNF 支持的 VPN 隧道的两种隧道的使用场景介绍，包括 IPSec VPN 和 SSL VPN。

本章主要包含以下内容：

功能	描述
使用 IPSec VPN 功能的典型场景概述	场景描述和典型结构
IPSec VPN 的部署	示例拓扑搭建
IPSec VPN 的配置和使用说明	IPSec VPN 的配置和使用说明
使用 SSL VPN 功能的典型场景概述	场景描述和典型结构
SSL VPN 的部署	示例拓扑搭建
SSL VPN 的配置和使用说明	SSL VPN 的配置和使用说明

3.1 IPSec VPN

3.1.2 概述

3.1.2.1 场景描述

场景 1：VPC 与客户本地数据中心通过 IPSec VPN 互联，使得 VPC 内 CVM 和数据中心的物理服务器可以互相访问。

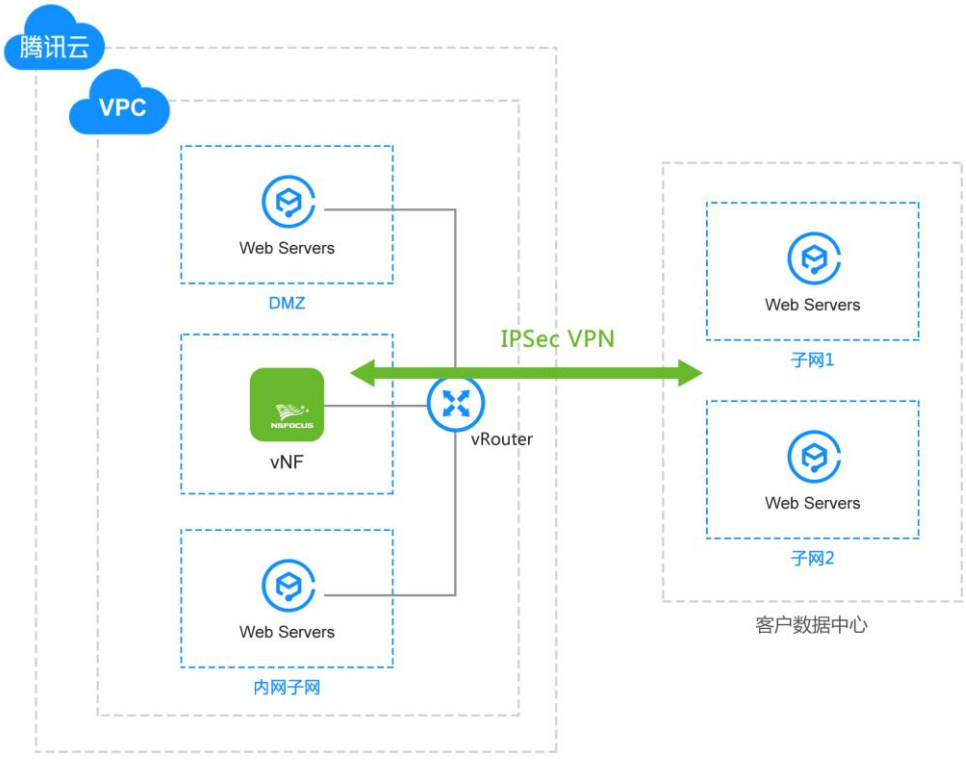
场景 2：同一公有云下，不同区域的两个 VPC 之间通过 IPSec VPN 互联使得两个 VPC 可以互联互通。

----结束

3.1.2.2 网络架构

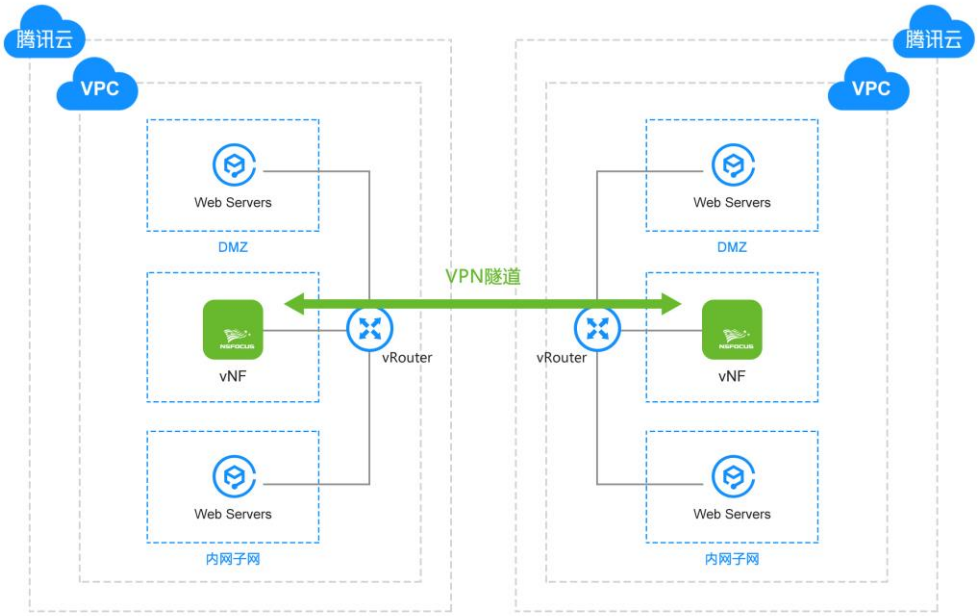
VPC 与数据中心通过 IPSec VPN 互联，使得 VPC 内 CVM 和数据中心的物理服务器可以互相访问：

- VPC 内的 IPSec VPN 实例和数据中心内的 IPSec VPN 设备都有公网 IP 地址；
- VPC 的 IP 地址与数据中心 IP 地址不冲突。



两个 VPC 之间通过 IPSec VPN 互联使得两个 VPC 内的 CVM 可以互相访问：

- 两个 VPC 内的 IPSec VPN 实例都有公网 IP 地址；
- 两个 VPC 的 IP 地址不冲突。

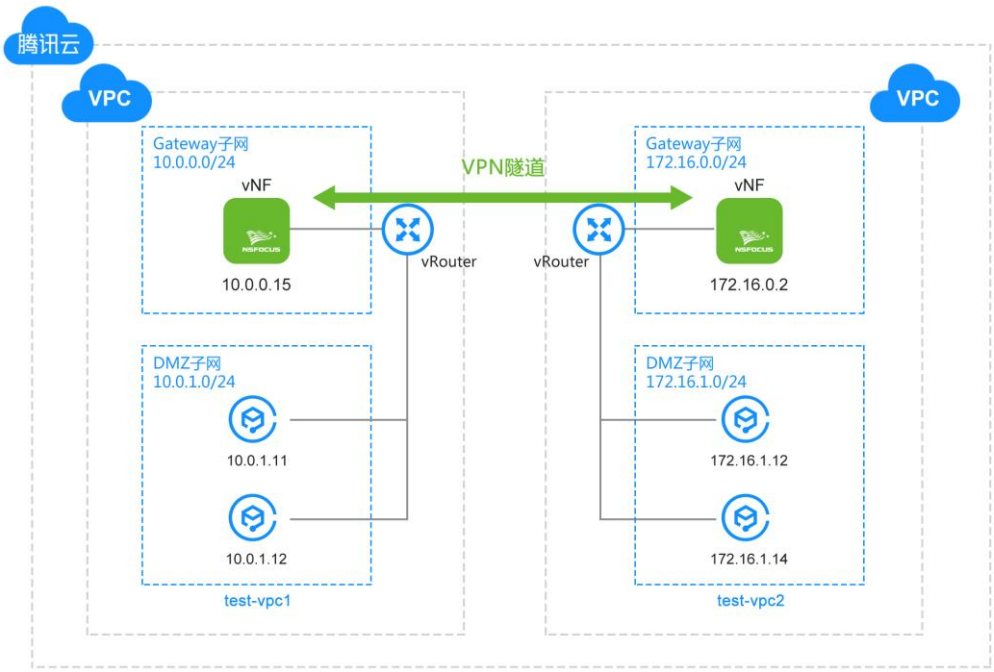


----结束

3.1.3 IPSec VPN 部署

本例中以两个腾讯云上的 VPC 互联互通为例，介绍 IPSec VPN 的快速使用。

3.1.3.1 部署示例拓扑



拓扑图中元素和数据流量说明：

- 两个 VPC
- 每个 VPC 中有两个子网，vNF 位于 Gateway 子网，能与公网通信，位于 VPC 的网络边界处。DMZ 子网内服务器，属于私有子网，流量需要路由到 vNF。
- 两个 vNF，一个配置成 IPSec VPN 的服务器端，一个配置成 IPSec VPN 的客户端。两个 vNF 使用网关到网关方式建立 IPSec VPN 连接
- 配置各自路由表，经 0.0.0.0/0 的流量路由至 vNF 实例。

----结束

3.1.3.2 环境搭建

步骤 1 配置私有网络。

在私有网络的控制面板中选择创建私有网络，同一地区中新建两个 VPC，命名为 nf-test-vpc1(10.0.0.0/16)， nf-test-vpc2(172.16.0.0/16)

ID/名称	CIDR	子网	路由表	默认私有网络	操作
vpc-iax1n6ly nf-test-vpc2	172.16.0.0/16	2	1	否	删除
vpc-7r3krvjo nf-test-vpc1	10.0.0.0/16	2	1	否	删除

步骤 2 配置交换机

在 nf-test-vpc1 内部分别创建 Gateway 子网和 DMZ 子网：

ID/名称	所属网络	CIDR	可用区	关联路由表	云主机	可用IP	默认子网	操作
subnet-adz529j9 gateway-vswitch	vpc-7r3krvjo nf-test-vpc1	10.0.0.0/24	成都一区	rtb-q10ririp default	0	253	否	删除 更换路由表
subnet-1prn7d9p dmz-vswitch	vpc-7r3krvjo nf-test-vpc1	10.0.1.0/24	成都一区	rtb-q10ririp default	0	253	否	删除 更换路由表

在 nf-test-vpc2 内部也分别创建 Gateway 子网和 DMZ 子网。

ID/名称	所属网络	CIDR	可用区	关联路由表	云主机	可用IP	默认子网	操作
subnet-oyqtmxs7 gateway-vswitch	vpc-iax1n6ly nf-test-vpc2	172.16.0.0/24	成都一区	rtb-5mbuly5v default	0	253	否	删除 更换路由表
subnet-mkezoj45 dmz-vswitch	vpc-iax1n6ly nf-test-vpc2	172.16.1.0/24	成都一区	rtb-5mbuly5v default	0	253	否	删除 更换路由表

步骤 3 配置安全组

环境中需要配置以下安全组：

安全组名称	VPC	用途说明
nf_gateway_sg	nf-test-vpc1	vNF 所属安全组
dmz_sg	nf-test-vpc1	DMZ 区所属安全组

1. 创建 NF 的安全组：nf_gateway_sg 配置入站、出站规则如下：

入站规则 出站规则

添加规则 导入规则 排序 删除 教我设置

来源	协议端口	策略	备注	操作
sg-epzk1mrn dmz-sg	ICMP	允许	支持Ping服务	编辑 插入 删除
0.0.0.0/0	UDP:4500,500	允许	-	编辑 插入 删除
0.0.0.0/0	TCP:443	允许	放通Web服务HTTPS（443），如 Apache、Nginx	编辑 插入 删除

入站规则 出站规则

添加规则 导入规则 排序 删除 教我设置

目标	协议端口	策略	备注	操作
0.0.0.0/0	ALL	允许	-	编辑 插入 删除

端口说明：

端口号	协议	用途说明
全部	ICMP	当前 VPC 中的 DMZ 子网的安全组可访问，用于向另一个 VPC 的 DMZ 子网发送连通性测试包
443	TCP	Web 管理界面访问端口
500	UDP	IPSec 协议使用端口
4500	UDP	IPSec 协议使用端口

2.创建 DMZ 的安全组:dmz_sg。 安全组规则将 ICMP 打开，以用于后面测试连通性。

创建完成之后，安全组列表如下：

步骤 4 新建 DMZ 区服务器

在两个 dmz 子网各新建两台服务器，如下：

步骤 5 新建 vNF 虚拟机

在两个 gateway 子网各创建好 vNF 虚拟机，如下：

步骤 6 修改路由

将两个 VPC 中 dmz 的流量路由至各自 VPC 中的 vNF 实例，同时关联 dmz-vswitch 子网。

注：目标网段图例中填入的是 0.0.0.0/0，实际使用中，可以只填入需要访问的子网网段，例如需要通过 VPN 访问 172.16.0.0/16 网段，则目标网段填写：172.16.0.0/16。

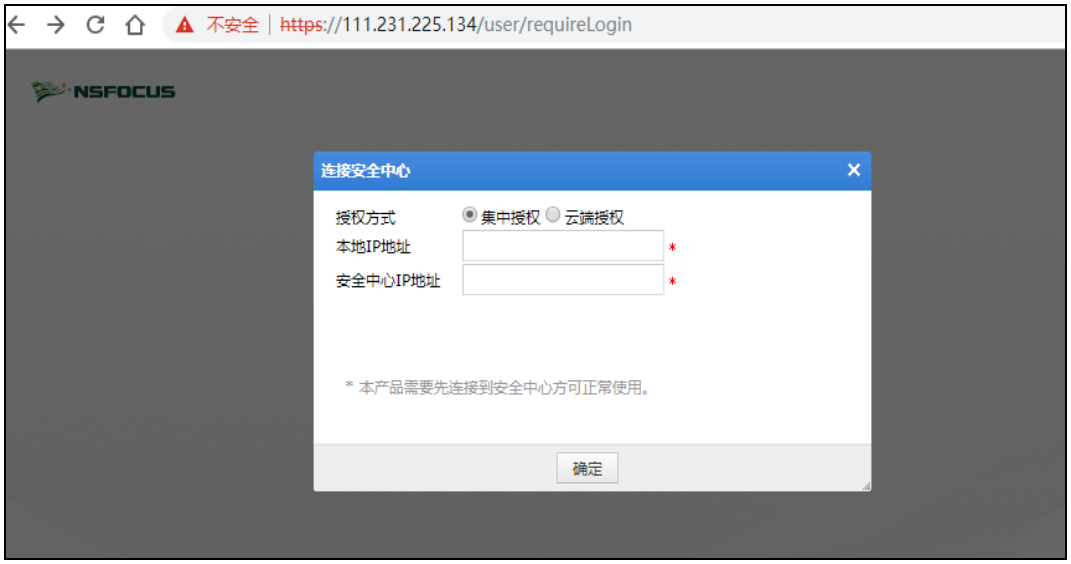
----结束

3.1.4 vNF 配置 IPSec VPN 步骤

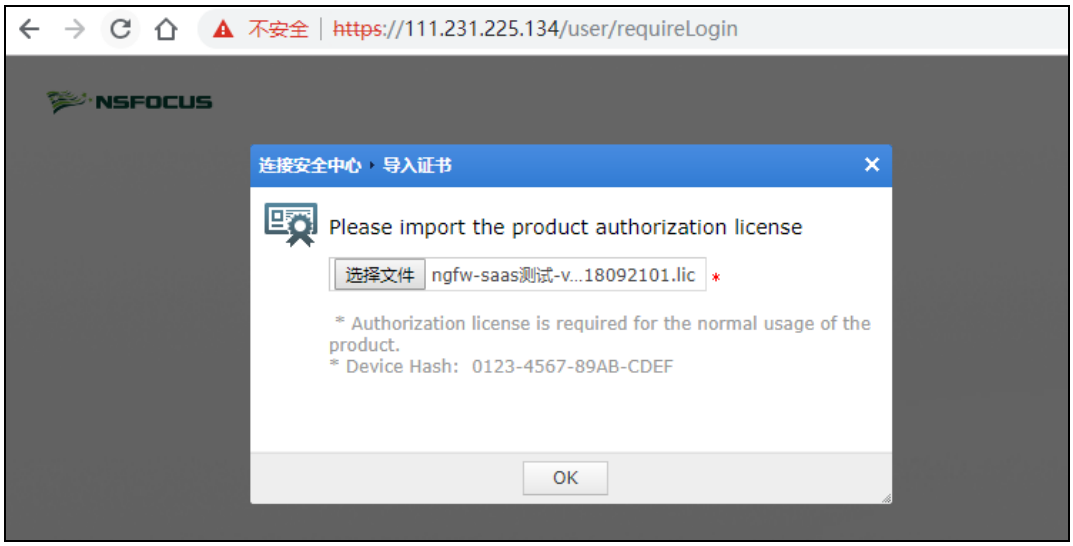
3.1.4.1 服务器端配置

步骤 1 访问管理界面并导入证书

通过 vNF 的公网 ip，访问管理页面，假设公网 ip 为：111.231.225.134，通过 URL：https://111.231.225.134 访问管理页面如下：



选择云端授权选项，并导入证书：



再次出现连接云端安全中心的页面之后，填入本机 IP 地址（公网地址），点击确定按钮：

步骤 2 登录管理界面并重启设备

设备证书认证通过并激活之后，可以通过默认用户名密码（weboper/weboper）登录管理界面，修改密码之后，重新登录并访问：**通过系统** > **系统控制** > **重启系统** 进行重启设备。

步骤 3 选择菜单 **网络** > **接口**，点击新建创建 VPN 类型且子类型为 ipsec 的接口。

步骤 4 选择菜单 **网络** > **IPSEC VPN** > **IPSEC 隧道配置**，进入 IPSEC VPN 隧道配置页面。

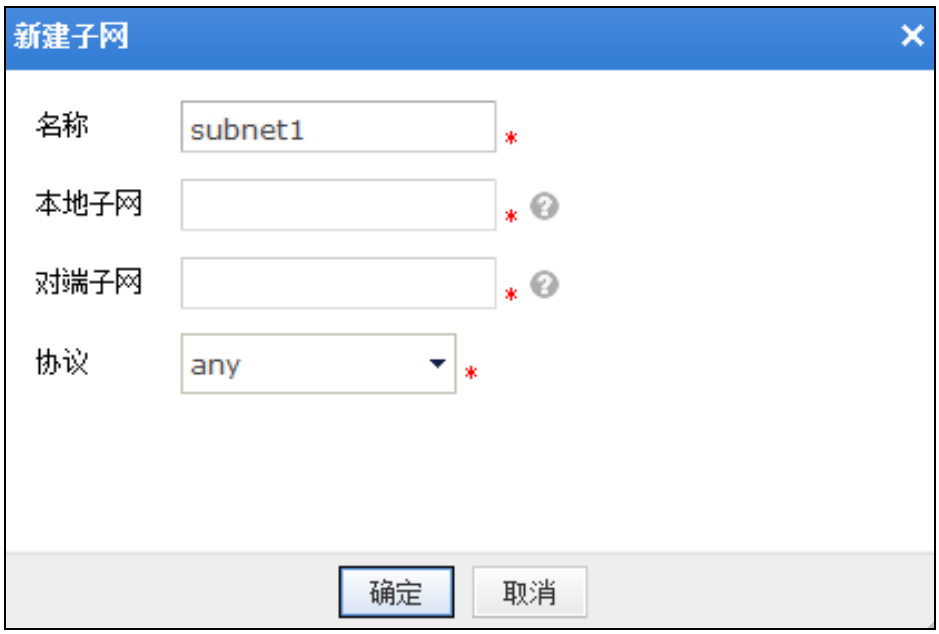
步骤 5 单击列表右上方的【新建】按钮，弹出新建 IPSEC VPN 服务器对话框。

注：腾讯云 VPC 中，由于两端 NF 分配的公网 IP 均为经过 NAT 之后的地址，在 NF 中实际能获取到的地址为私网地址。所以必需要填写本地 ID 和对端 ID 用于隧道的连接建立。主动协商中，服务器端选择：否，则客户端则应该选择：是，由客户端主动发起连接。

说明	详细参数说明请参考《绿盟下一代防火墙用户手册》

步骤 6 单击【下一步】或者在当前页面单击“第二阶段”蓝色链接，切换页面到 IPSEC VPN 第二阶段。

步骤 7 单击右上角的【添加】，新建子网，如图所示。



注意	详细参数说明请参考《绿盟下一代防火墙用户手册》

创建完成之后，选择启动

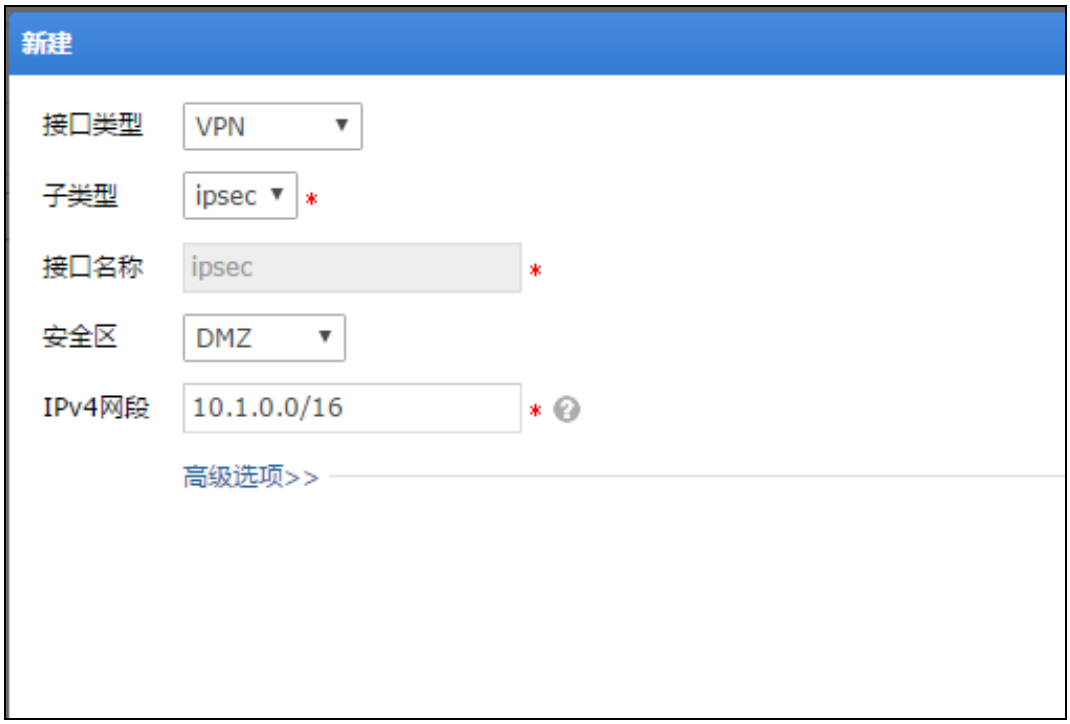
步骤 8 在已创建 IPSEC VPN 隧道列表的操作栏中单击图标，将对应的客户端配置文件导出到本地。

步骤 9 单击页面右上方的 应用配置，使配置生效

----结束

3.1.4.2 客户端配置

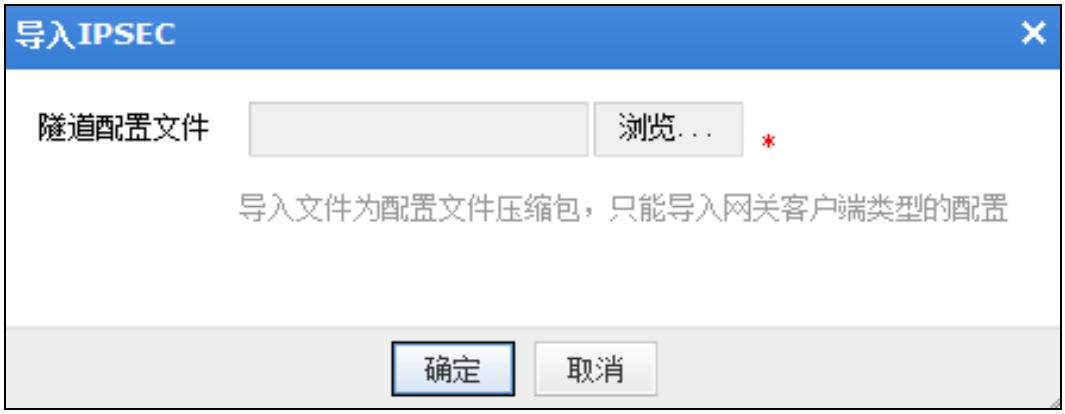
步骤 1 创建 VPN 类型且子类型为 ipsec 的接口。



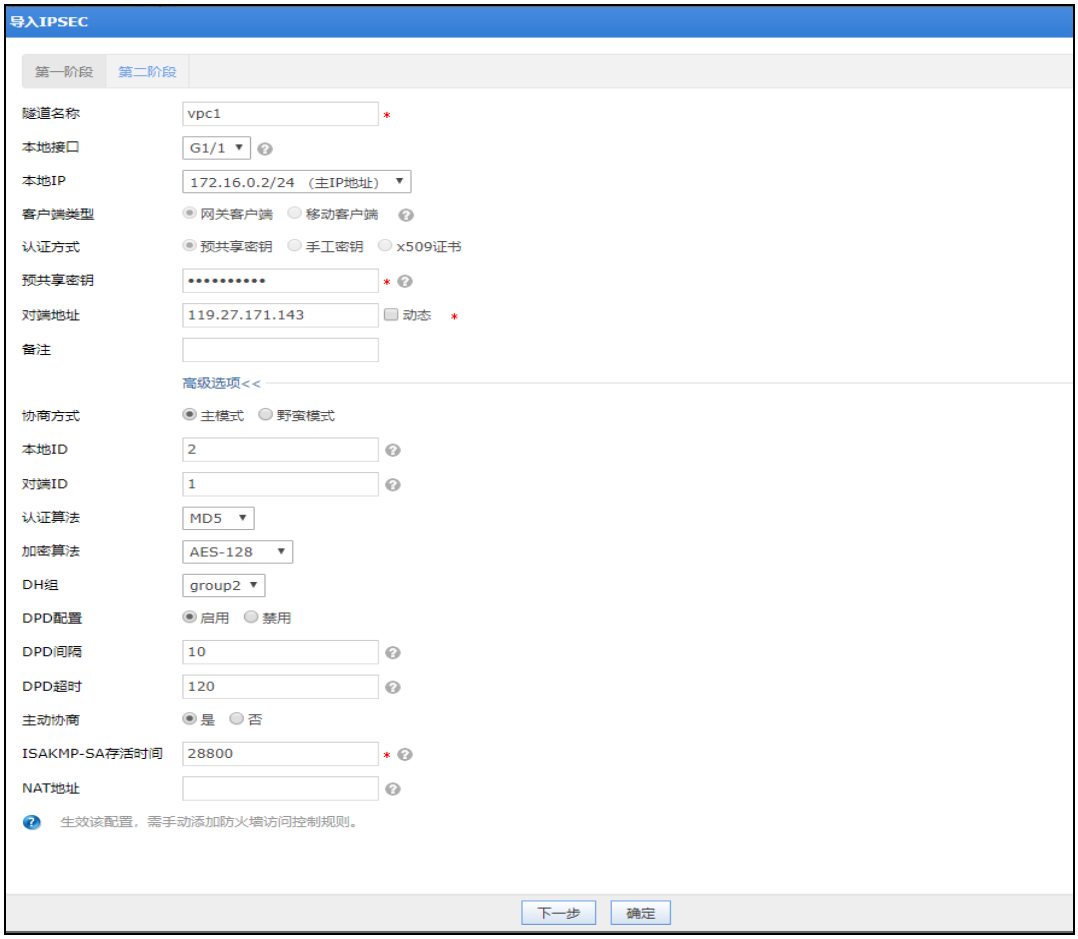
注意	客户端 ipv4 网段需要区别于服务器端配置

步骤 2 选择菜单 **网络** > **IPSEC VPN** > **IPSEC 隧道配置**，进入 IPSEC VPN 隧道配置页面。

步骤 3 单击列表右上方的【导入】按钮，弹出导入 IPSEC VPN 客户端对话框。



导入之后，修改对端地址为对端公网 ip 地址：



注：高级选项中，主动协商选择：是，由客户端主动发起连接。

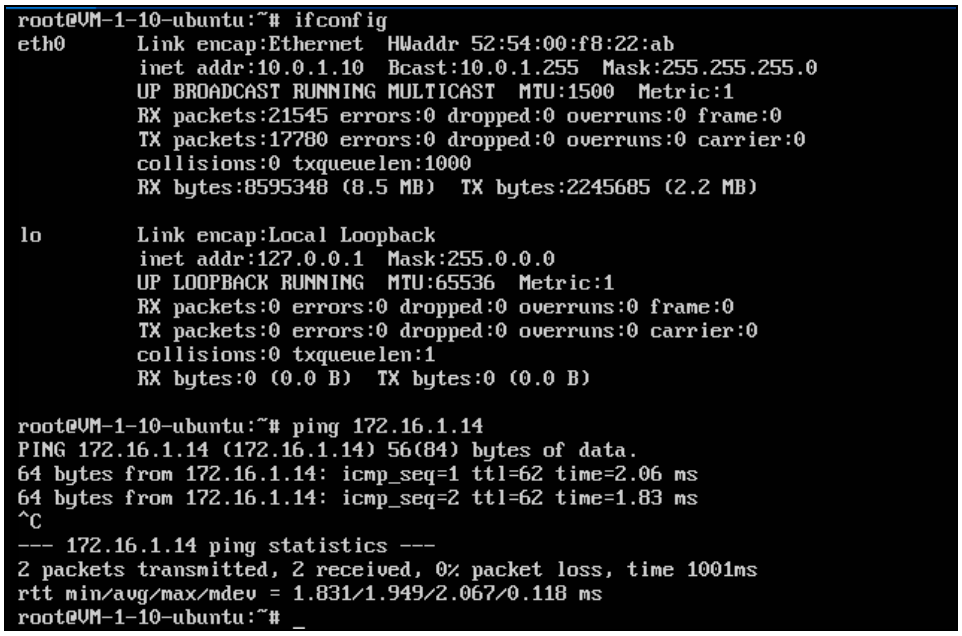
步骤 4 单击【确定】按钮，返回隧道列表，选择启动。

步骤 5 点击应用配置，使配置生效。在 IPSEC 状态页面，可看到 IPSec 隧道已经建立。

----结束

3.1.4.3 效果验证

登陆 nf-test-vpc1 的机器 dmz1-2，ping nf-test-vpc2 中 dmz2-2 (172.16.1.14)，效果如下：



----结束

3.2 SSL VPN

3.2.1 概述

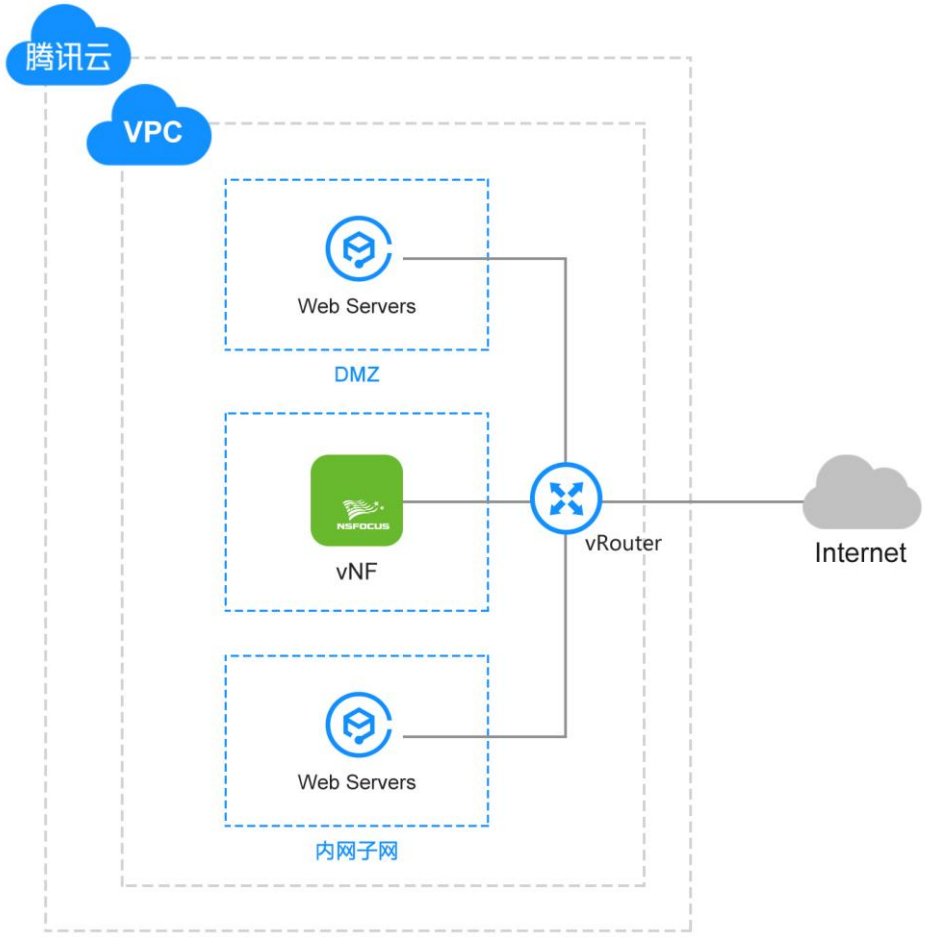
3.2.1.1 场景描述

所有 CVM 实例不对公网开放远程管理端口（例如 SSH 22、RDP 3389）。

运维人员通过 SSL VPN 拨号进入 VPC 网络，在客户端使用远程桌面或者 SSH 运维工具连接 CVM 云服务器私网 IP

----结束

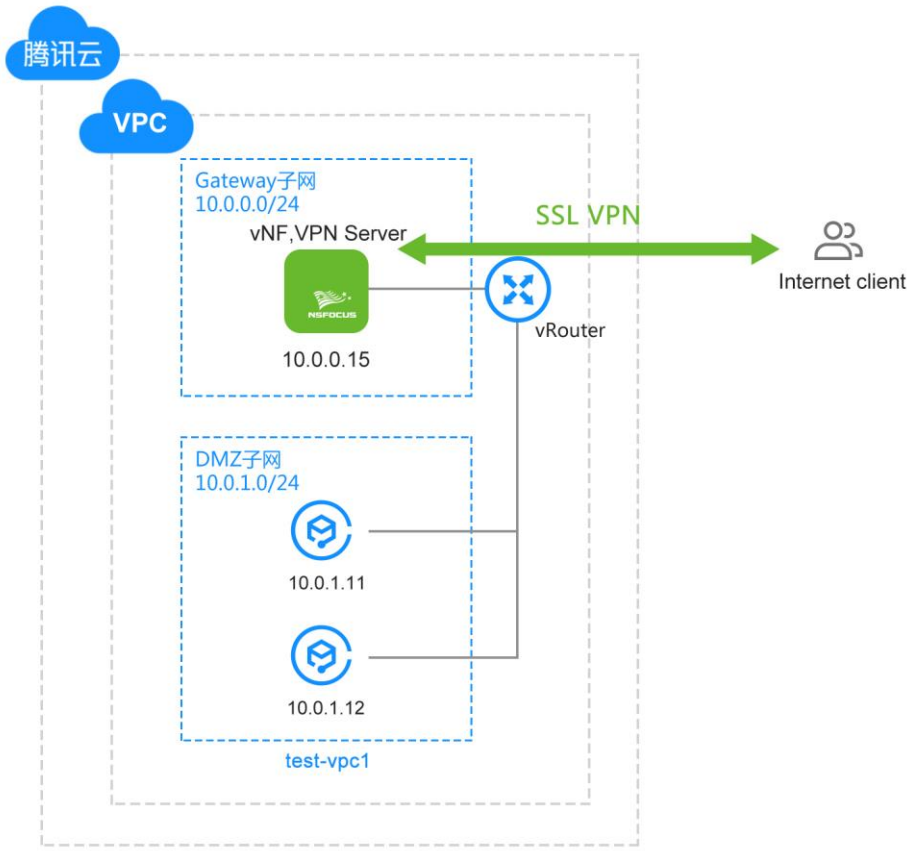
3.2.1.2 网络架构


腾讯云
VPC
Web Servers
DMZ
vNF
vRouter
Internet
Web Servers
内网子网

----结束

3.2.2 SSL VPN 部署

3.2.2.1 部署示例拓扑



具体包含：

- 1 个客户的 VPC
- vNF 位于 Gateway 子网，私网服务器位于 DMZ 子网
- vNF 配置 SSL VPN 功能

DMZ 子网中服务器通过路由配置将流量转发到 NF

----结束

3.2.2.2 环境搭建

参照 3.1.3 章节中 IPSec 环境搭建拓扑图中的左半部分，创建一个 vpc：nf-test-vpc1，在该 vpc 中创建子网：gateway_vswitch, dmz_vswitch，创建安全组，并创建相应的 vNF 虚拟机和 DMZ 区服务器。两个不同的地方如下：

1. 和 IPSec 环境不一样的是，vNF 所属的安全组规则有所不同，需要配置如下：

端口说明：

端口号	协议	用途说明
443	TCP	Web 管理界面访问端口
4433	TCP	SSL VPN 认证 https（可以在页面对这个端口进行配置更改）
50000-50020	UDP	SSL VPN 协议使用端口

2. 为了进行 SSL VPN 效果验证，需要 DMZ 服务器所属安全组也开放更多规则:

允许 ICMP，SSH，HTTP 几个协议的端口如下：

----结束

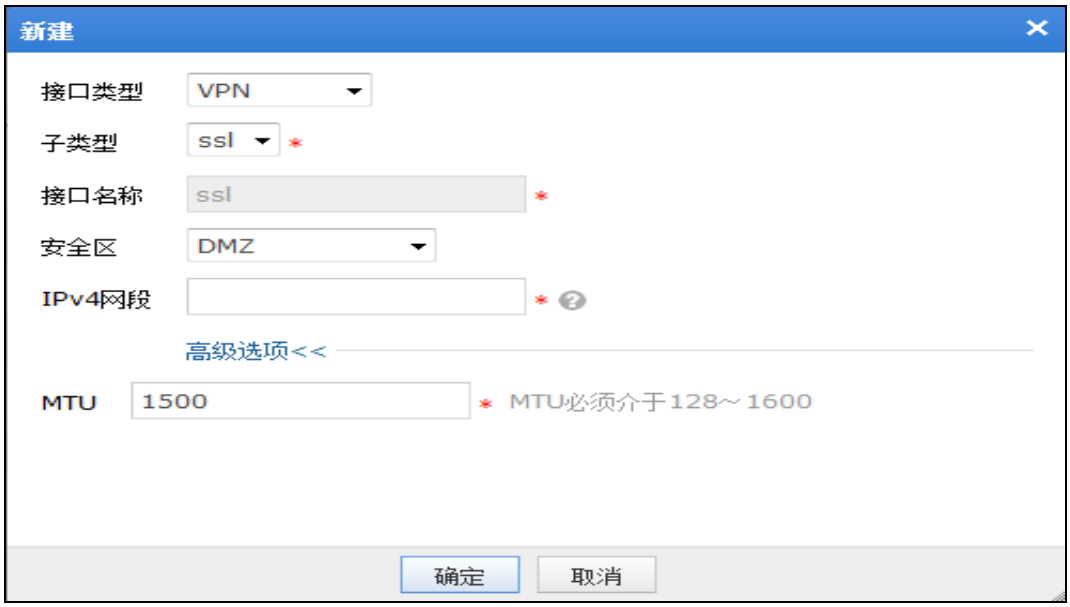
3.2.3 vNF 配置 SSL VPN 步骤

3.2.3.1 服务器端配置

步骤 1 访问页面并导入证书，参考 3.1.4 节，此处省略。

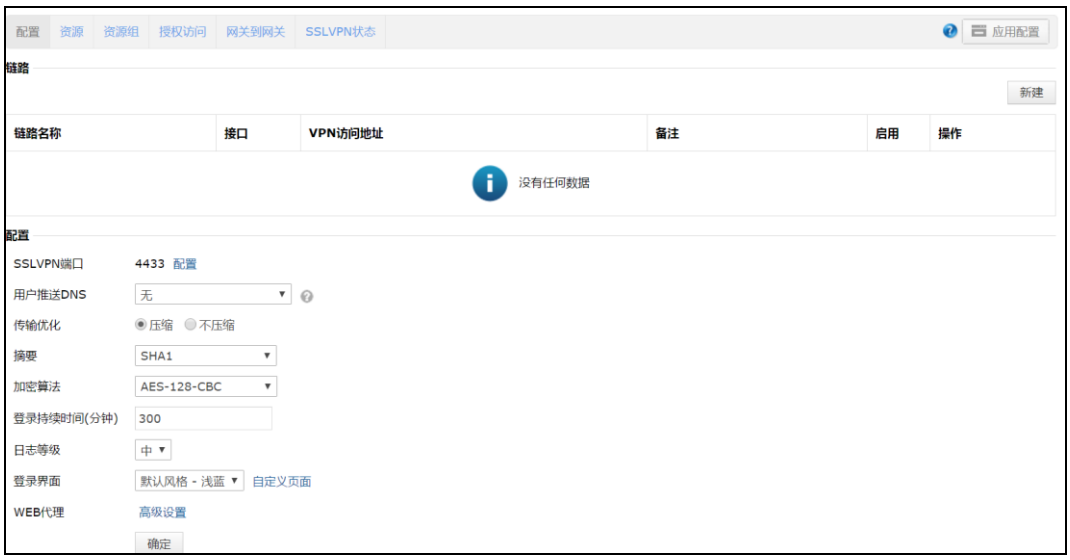
注意	导入证书之后，请重启设备

步骤 2 创建 VPN 类型且子类型为 ssl 的接口。



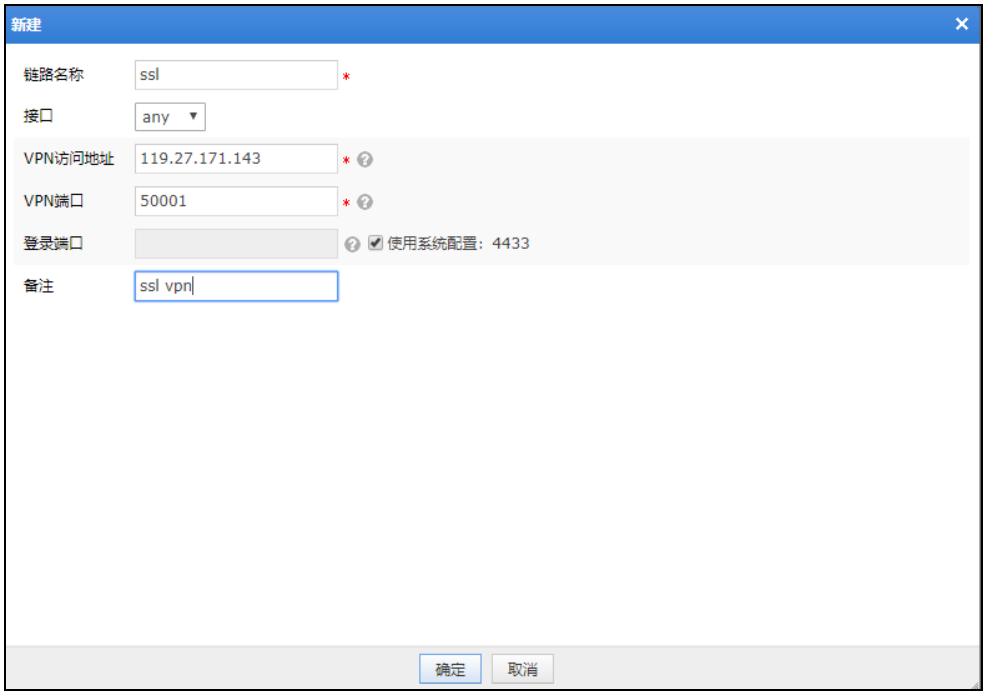
IPV4 网段设置为 10.2.0.0/24

步骤 3 选择菜单 **网络 > SSL VPN > 配置**，进入 SSL VPN 配置页面



步骤 4 设置上个步骤页面中远程访问 SSL VPN 相关的基本参数，可以保持默认参数，修改后点击确认。

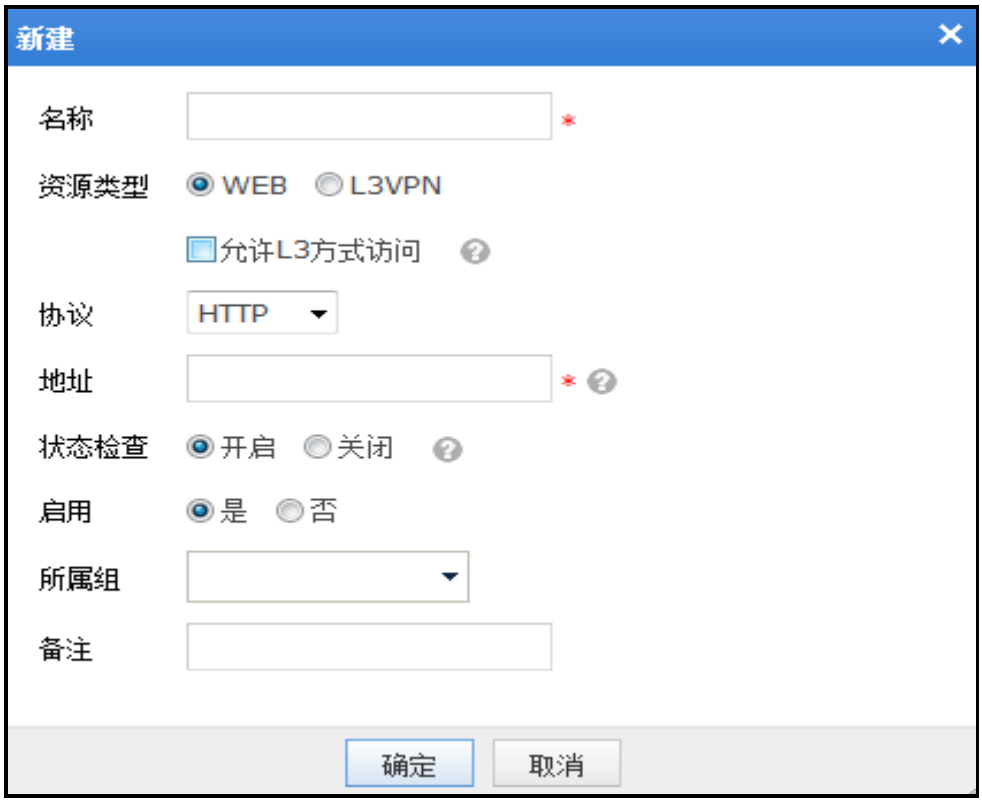
步骤 5 单击步骤 3 图中链路列表右上方的【新建】按钮，新建一条 SSL VPN 链路，如下图所示。VPN 访问地址填入该 NF 的公网可访问地址。



点击确定之后，回到配置页面，点击启用该链路：

步骤 6 选择菜单 **网络 > SSL VPN > 资源**，进入资源配置页面，如图：

单击列表右上方的【新建】按钮，弹出新建 SSL VPN 资源对话框：



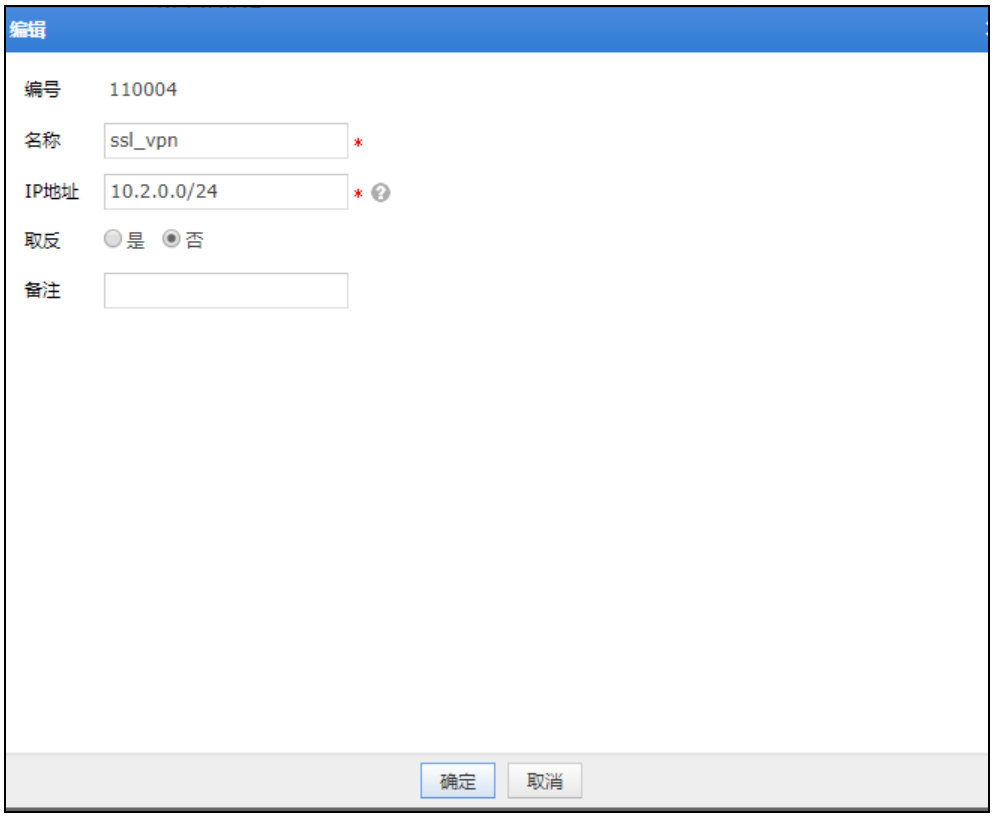
设置参数

说明	详细参数说明请参考《绿盟下一代防火墙用户手册》

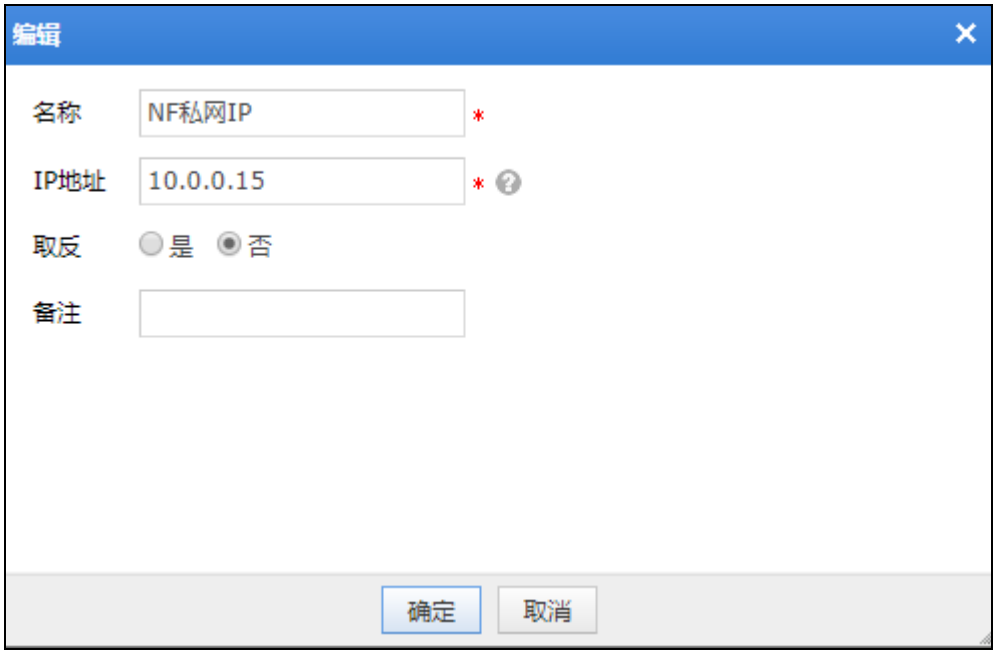
按照参数说明，配置资源如下：

步骤 7 配置 SSL 接口的 SNAT。在上一步中，初始配置完，健康检查通不过，需要配置好 SSL VPN 的接口 SNAT，才能正常访问到内网资源。

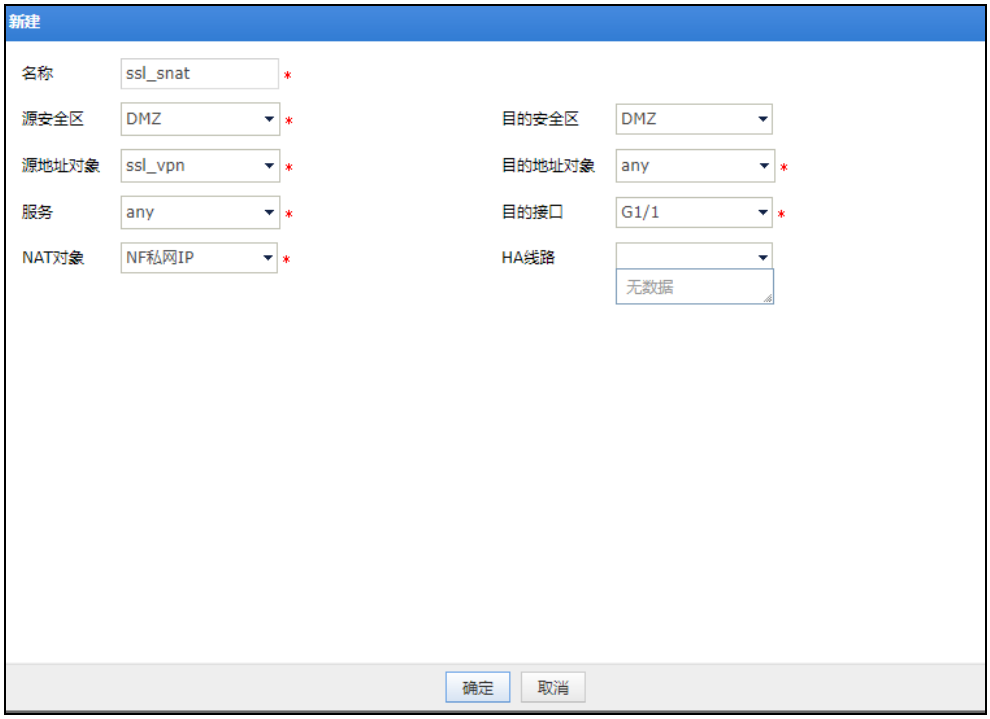
选择菜单 **对象** > **网络** > **子网**，选择新建，建立 ssl vpn 的子网信息，如下图：



选择菜单 **对象 > 网络 > 节点**，选择新建，建立 NF 工作口的节点信息，如下图：

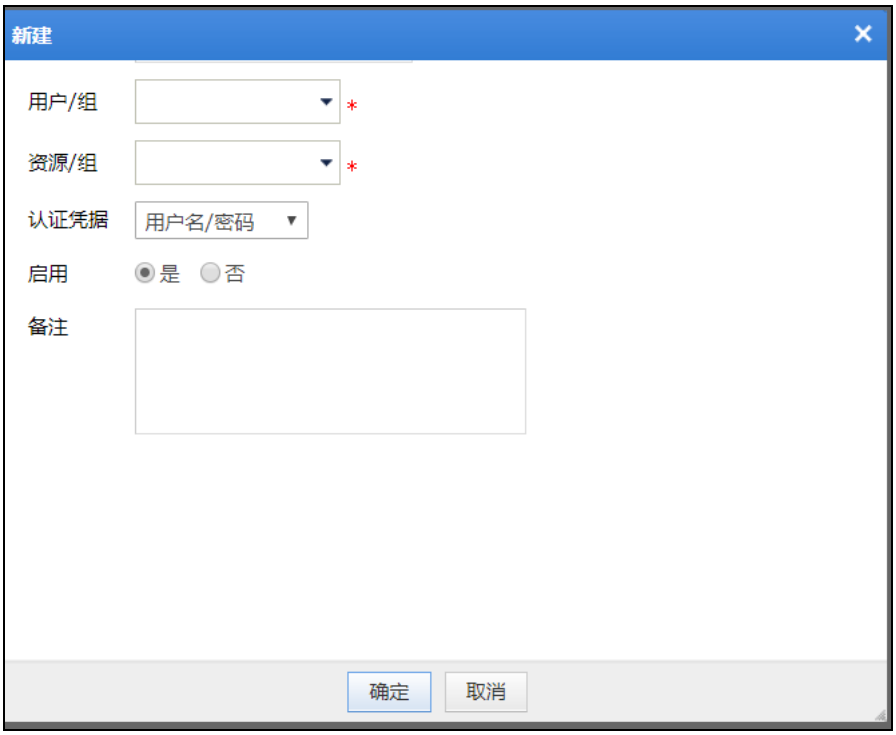


选择菜单 **策略 > NAT > 源 NAT**，选择新建，建立 ssl vpn 的 snat 规则，如下图：



步骤 8 选择菜单 **网络 > SSL VPN > 授权访问**，进入授权访问页面

点击新建：



注意	上图中所示的用户和用户组可以选择菜单 **对象** > **用户** 提前新建，也可以在新建授权页面进行快捷创建

说明	详细参数说明请参考《绿盟下一代防火墙用户手册》

用户配置如下：

点击应用配置，使配置生效。

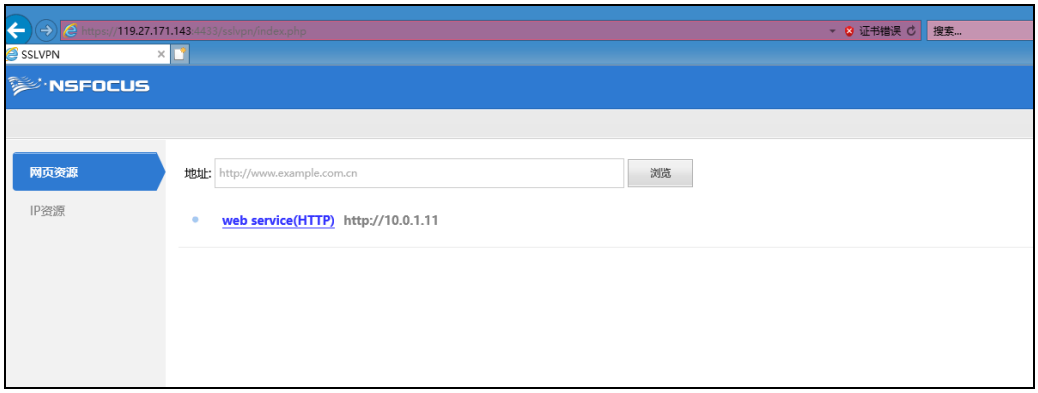
说明	上述配置结束后，远程用户即可访问服务器端 vNF 发布的资源。 • WEB 类型资源：通过 https://服务器端 vNF 链路接口 IP:SSLVPN 认证端口 /sslvpn 登录 SSL VPN，点击网页资源页面中相应的资源链接访问受保护内网服务。 • L3VPN 类型资源：通过 https://服务器端 vNF 链路接口 IP:SSLVPN 认证端口 /sslvpn 登录 SSL VPN，点击 IP 资源页面，启用 L3VPN 服务控件，下载客户端插件。安装插件后，进行隧道连接访问资源。

----结束

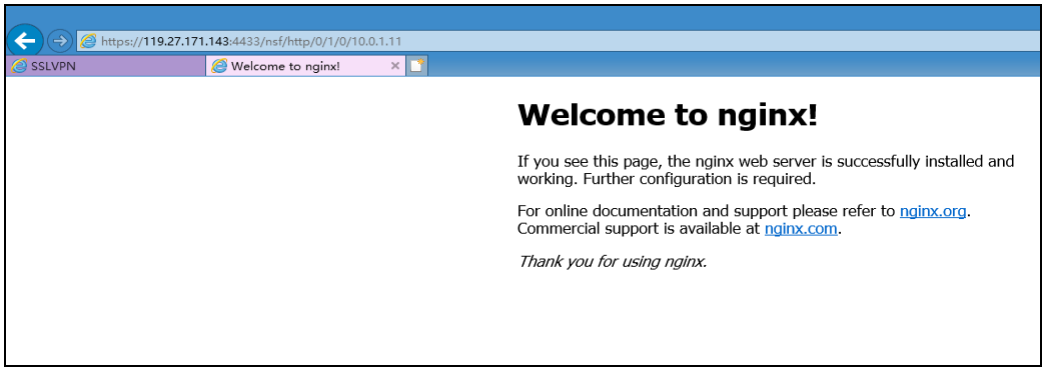
3.2.3.2 效果验证

访问 vNF 实例的公网地址的 4433 端口，并使用配置好的用户进行登录

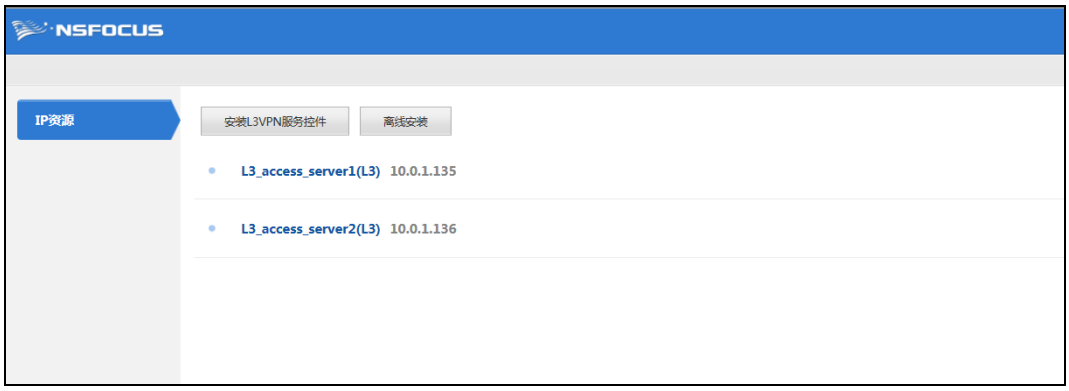
使用 test 用户登录之后，可以看到网页资源如下：



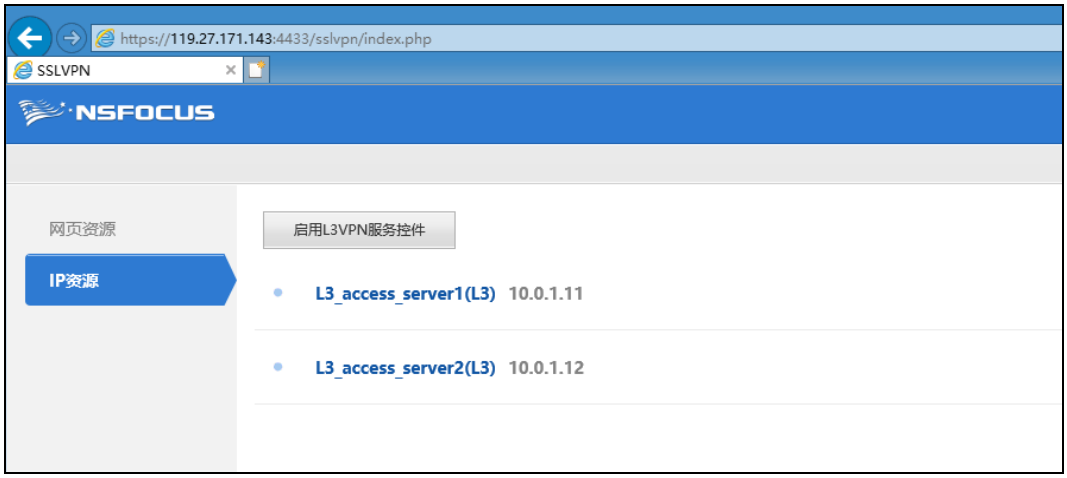
点击该资源，能够访问到如下网页：



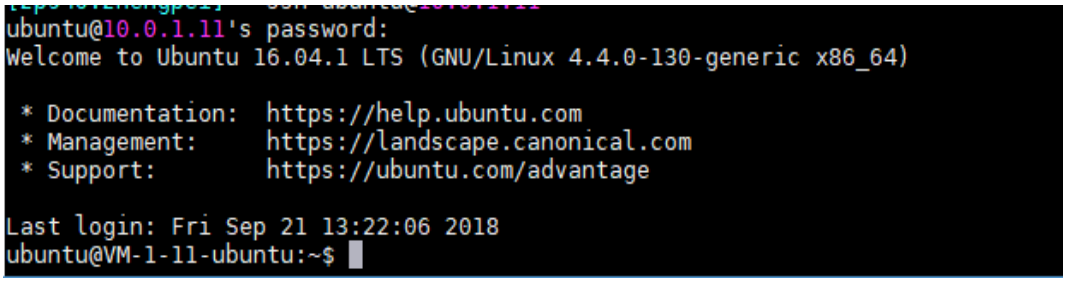
使用 test 登录之后，提示安装插件，插件安装完成之后，重启浏览器并重新登录：



选择安装 L3VPN 服务器控件，安装完成之后，点击启用 L3VPN 服务控件：



等待 VPN 连接建立之后，可以直接在本地访问 IP 资源中的机器，比如直接 ssh 10.0.1.11，效果如下：



----结束

4 应用层防护功能示例

绿盟下一代防火墙云服务(vNF)支持应用识别、入侵防御、内容过滤、URL 过滤、VPN 等，可以为用户提供 L4-L7 全面的安全服务。

本章主要介绍如何配置和使用 vNF 的安全防护功能。

功能	描述
安全防护功能的应用场景	介绍安全防护功能的应用场景
环境部署	介绍如何搭建测试环境
vNF 的配置	介绍如何配置 vNF 来启用安全防护策略

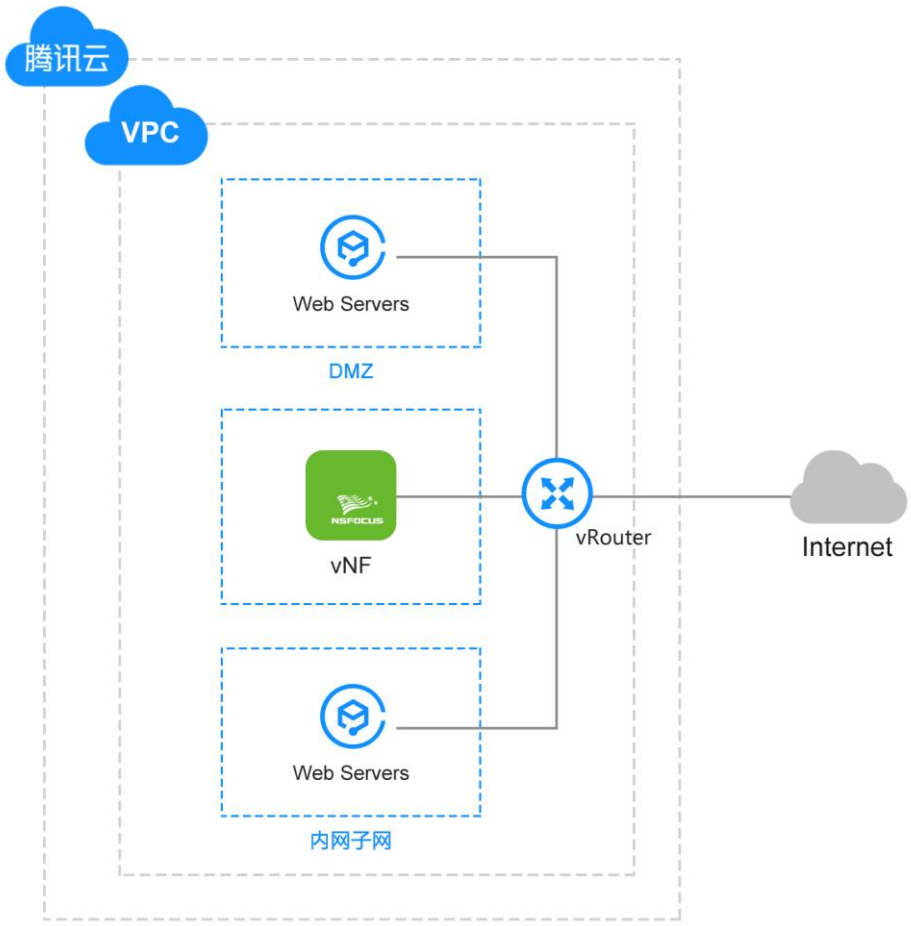
4.1 全防护功能的应用场景

vNF 的安全防护功能有很多：应用识别、入侵防御、内容过滤、URL 过滤、用户认证等，可以为用户提供 L4-L7 全面的安全服务。以下应用场景中只涉及少部分。

说明	更多应用配置参照《绿盟下一代防火墙用户手册》

在腾讯云客户环境中，vNF 部署在网络边界，处于外网、内网和 DMZ 区交界处，以三层路由模式接入网络中。

典型场景如下：



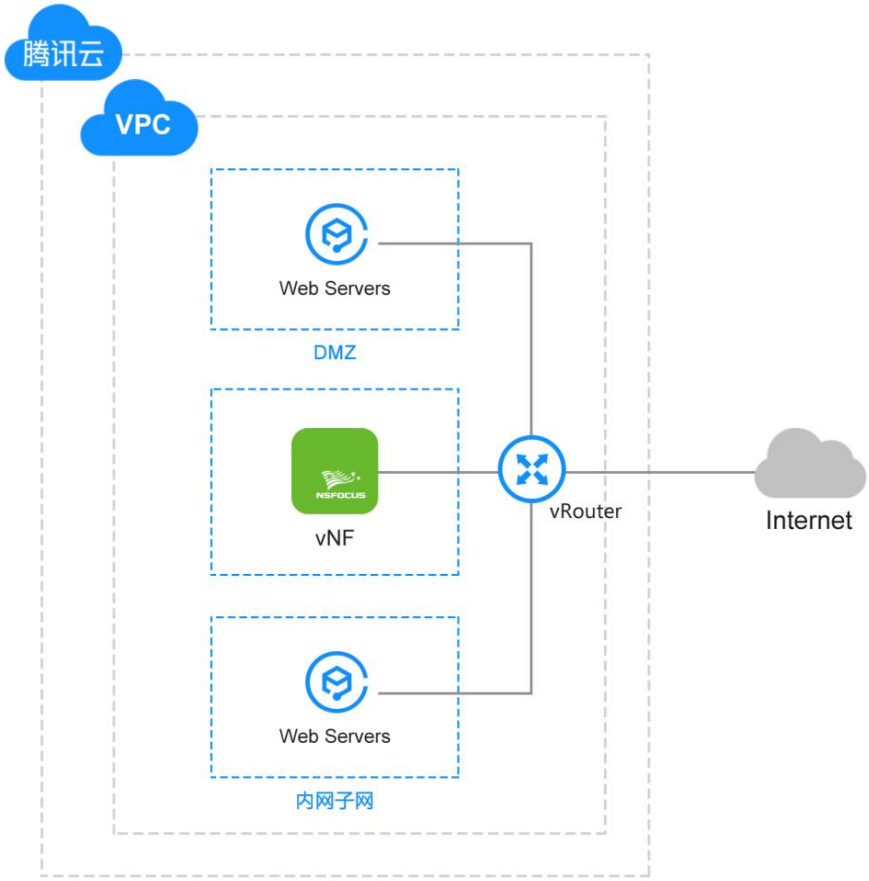
对于这种场景下，典型的安全防护需求如下：

1. 所有内网用户都通过源 NAT 策略进行外网的 Web 应用访问
2. DMZ 区对外提供 Web 服务
3. 内网和外网用户均可通过公网地址访问 DMZ 区的 Web 服务。
4. 对所有访问进行安全防护和用户访问日志记录。

----结束

4.2 环境搭建及部署

4.2.1 部署示例拓扑



拓扑元素：

- 1 个客户的 VPC
- 3 个子网：vNF 位于 Gateway 子网，web 服务器位于 DMZ 子网，其他服务器位于私有子网
- vNF 配置 snat/dnat 功能
- DMZ 子网，私有子网中服务器通过路由配置将流量转发到 NF

----结束

4.2.2 环境搭建

参照 3.1.3 章节中 IPSec 环境搭建步骤进行拓扑搭建。

需要说明的是安全组配置和流量牵引

步骤 1 安全组配置：

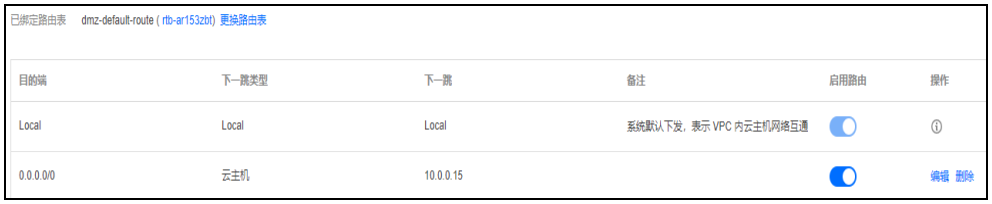
1. vNF 安全组：

考虑到 NAT 场景下，NF 需要代理的服务种类较多，将所有端口都放开。

2. web server 安全组：

3. 内网服务器安全组：仅开放 ssh 和 ping 功能。

步骤 2 将内网服务器流量的默认路由至 vNF 实例



----结束

4.3 vNF 配置

4.3.1 配置思路

1. 配置接口和静态路由。
2. 配置网络对象以及 NAT 策略。

– 配置源 NAT 策略，在内网用户访问外网时，将子网 10.0.3.0/24 转换为 vNF 接口的 IP 地址。

– 配置目的 NAT 策略，将 DMZ 区的 Web 服务做外网映射，并做服务器负载均衡（随机），映射的公网 IP 地址为 vNF 的公网地址。

3. 配置安全模板以及安全策略。

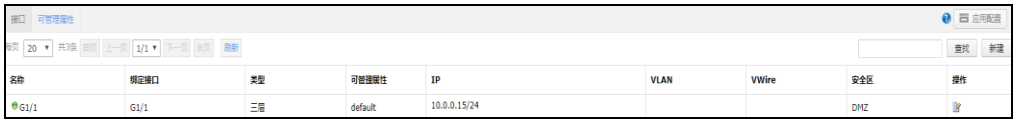
– 配置安全策略，允许内网用户访问外网 Web 应用，记录会话开始和结束的日志。同时，开启 IPS、URL 过滤、内容过滤以及病毒防护。

4. 应用配置，使配置生效。

----结束

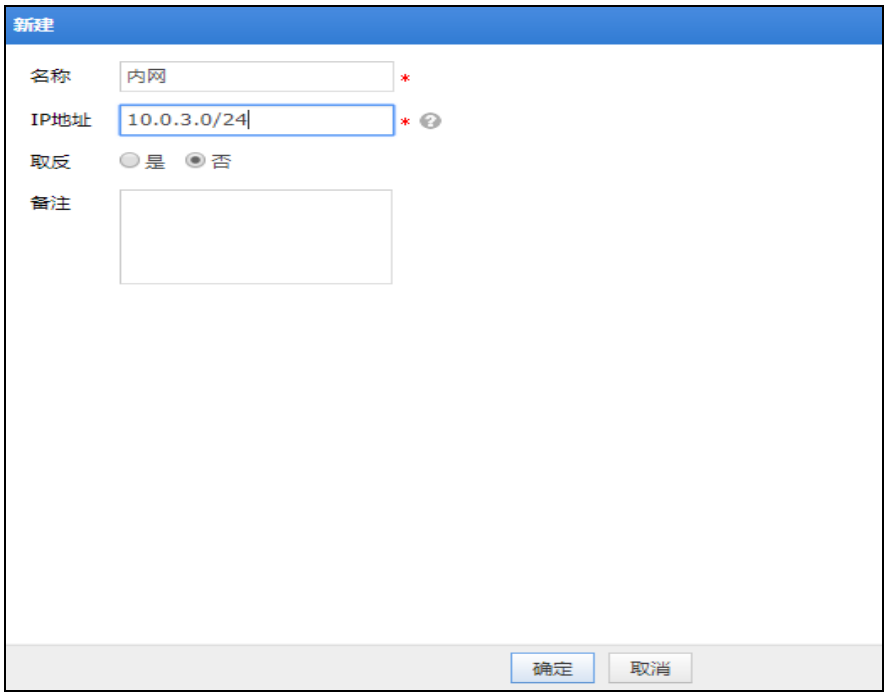
4.3.2 配置步骤

步骤 1 选择菜单 **网络 > 接口** 查看 vNF 目前唯一接口的安全区，待后续使用，例如下图中显示接口在 DMZ 区，也可以选择编辑操作改变安全区。

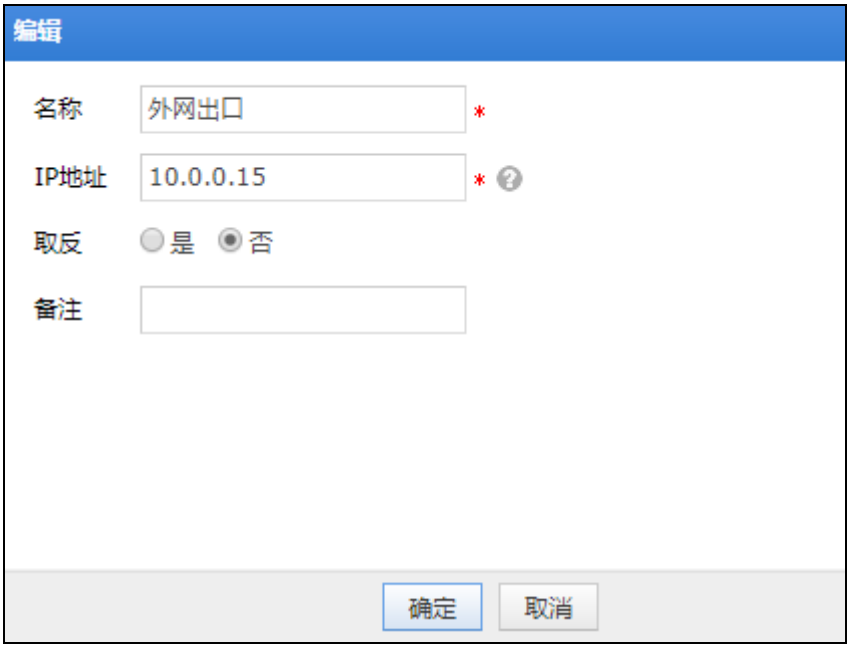


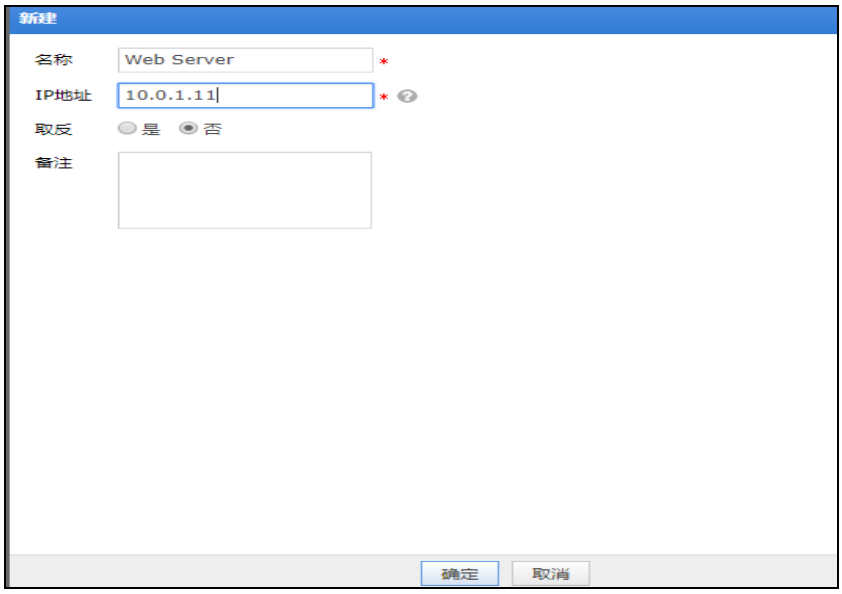
步骤 2 配置网络对象以及 NAT 策略

a. 选择菜单 **对象 > 网络 > 子网**， 新建名称为“内网”的子网对象：



b. 参见步骤 a 分别创建“外网出口”， “Web Server” 两个网络对象，均为节点类型。





说明	外网出口地址，需要配置腾讯云分配给 vNF 的私网地址。

c. 选择菜单 **策略** > **NAT** > **源 NAT**，新建源 NAT 策略，实现内网用户访问外网

d. 选择菜单 **策略** > **NAT** > **目的 NAT**，新建目的 NAT 策略，实现外网用户访问 DMZ 区 web 服务和内网用户访问 DMZ 区的 web 服务

说明	如果内部 DMZ 需要提供 443 端口的服务，由于 443 和 vNF 的管理界面使用端口重复，需要修改 vNF 的默认管理端口为其他端口。选择菜单：**系统** > **系统配置** 进行默认端口更改

步骤 3 选择菜单 **对象** > **安全模板**，分别新建入侵检测、URL 过滤、防病毒和内容过滤策略。

说明	新建安全模板的详细步骤请参见《下一代防火墙使用手册》

以新建URL过滤为例，URL过滤模板可帮助NF的安全策略实现根据URL地址对数据包进行过滤的功能。

NF 使用具有业界领先的中、英文 URL 分类库，内含按照不同类型（如赌博、暴力、恶意软件等）划分的超过 1000 万条记录的 URL 信息，可实现对工作无关网站、不良信息、高风险网站的准确、高效过滤。

URL 分类库中的 URL 规则分为离线模式和在线模式两种类型。

- 离线模式

离线模式将仅从本地获取 URL 分类信息。

- 在线模式

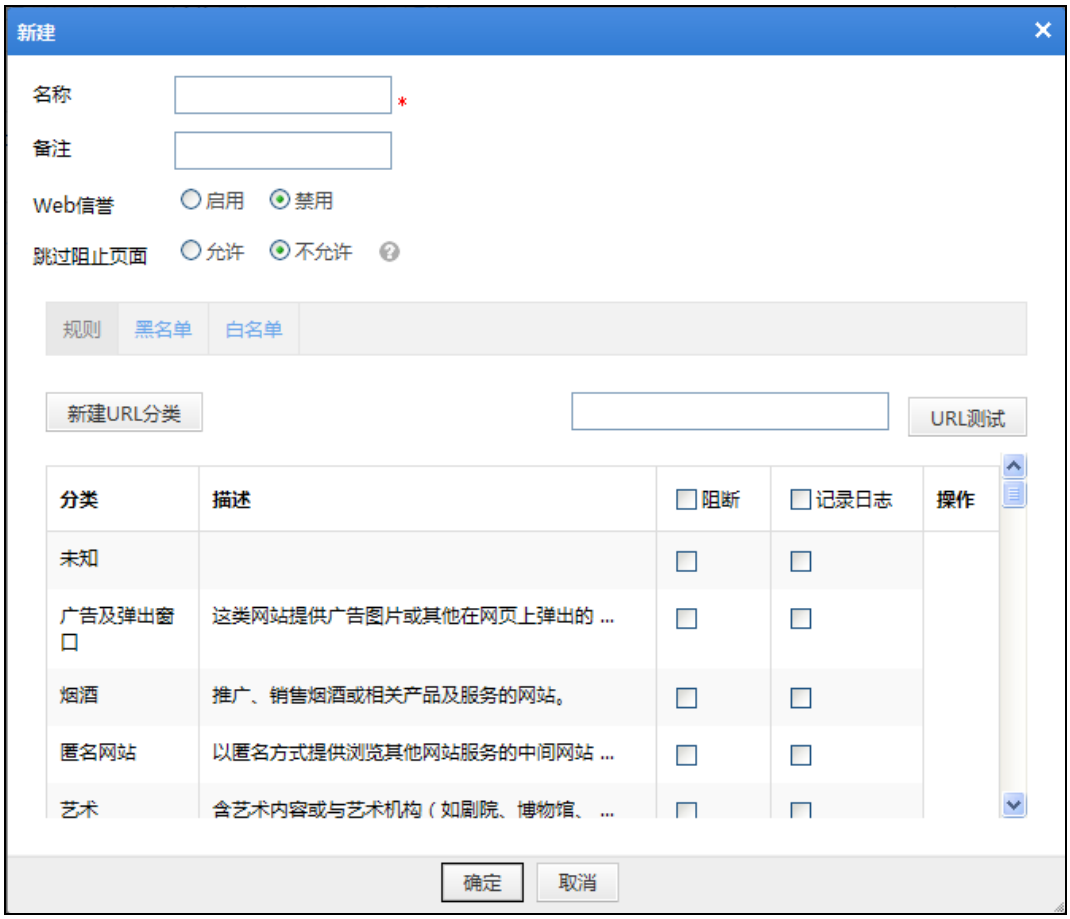
在线模式将从本地和在线服务器上获取 URL 分类信息。

单击 URL 过滤模板列表右上方的【URL 分类配置】按钮，配置 URL 分类库类型。

同时，NF 采用绿盟云安全中心提供的 Web 信誉库，云安全中心通过对互联网资源（域名、IP 地址、URL 等）进行威胁分析和信誉评级，将含有恶意代码的网站列入 Web 信誉库，以阻止对挂马网站的访问请求，实现对终端用户的安全保护。

NF 操作员新建 URL 过滤模板对象的详细步骤如下:

a. 选择菜单 **对象 > 安全模板 > URL 过滤**，进入 URL 过滤模板页面，单击 URL 过滤模板列表右上方的【新建】按钮，弹出新建对话框



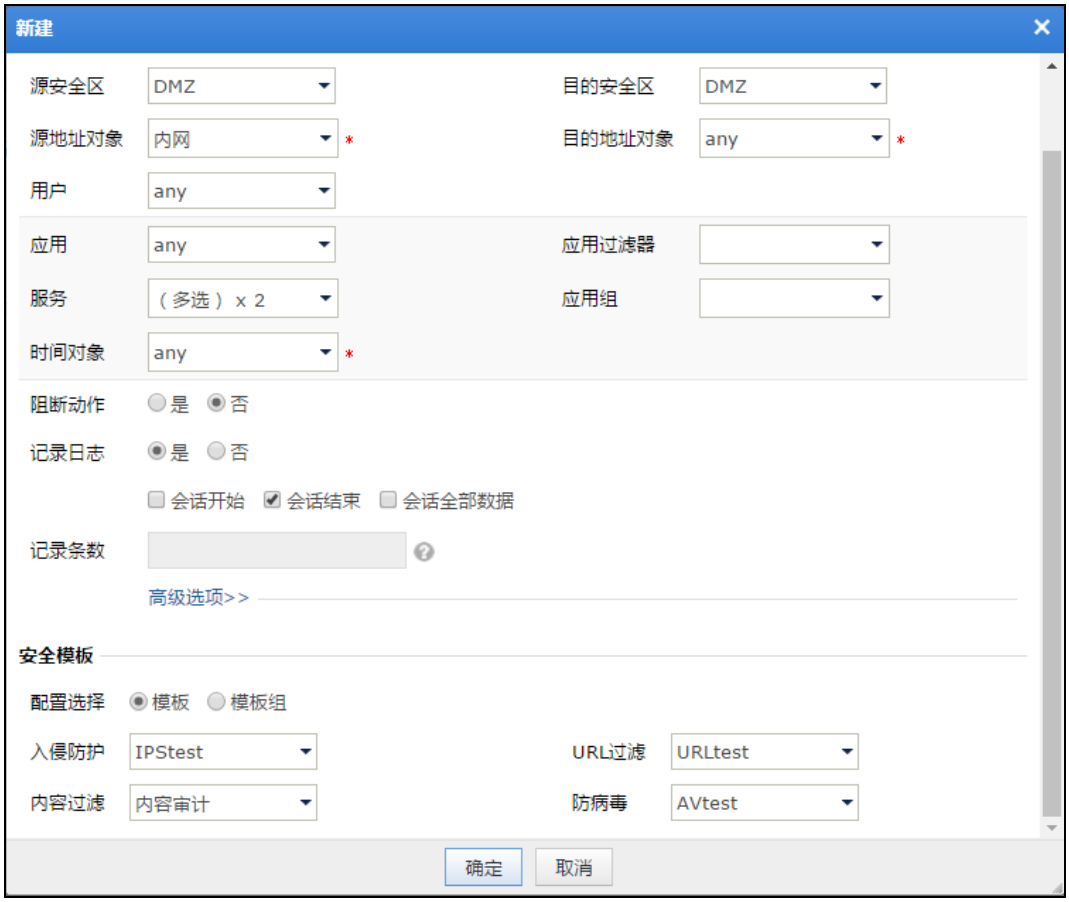
配置参数

说明	详细参数请参见《下一代防火墙使用手册》

点击确认按钮，完成操作。

假设将 www.test.com 加入黑名单，进行过滤：

b. 选择菜单 **策略 > 安全策略 > 安全策略**，新建一条安全策略。



步骤 4　应用配置。

- 单击页面右上方的 应用配置，使配置生效。
- 选择菜单 **系统** > **系统控制** > **系统控制**，单击【应用配置】按钮，使配置生效。

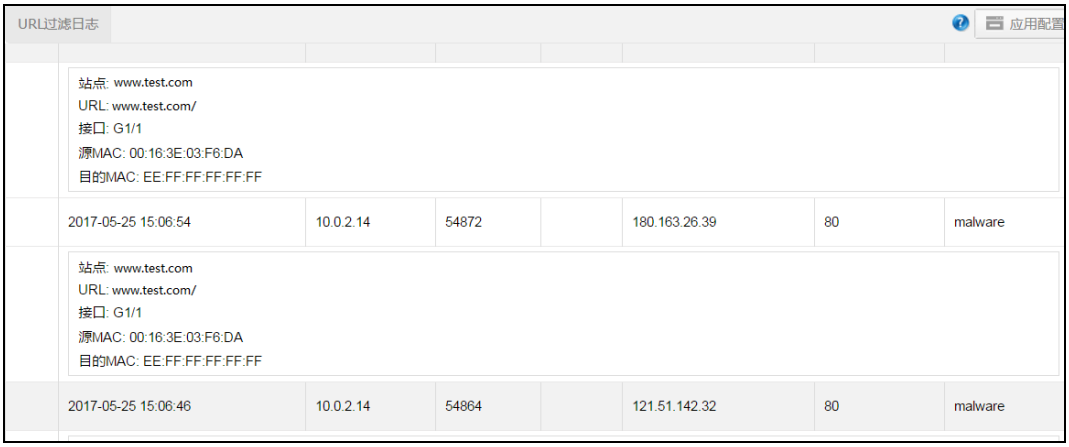
----结束

4.3.3 验证效果

在私网服务器中，访问黑名单中站点，出现被阻止页面，如下图：

而其他未加策略站点能正常访问。

同时可以查看到 URL 过滤日志：选择菜单 日志 > URL 过滤 可以查看到 URL 过滤日志



----结束

5 其他配置说明

本章主要包含以下内容：

功能	描述
默认账号密码	修改默认账号密码。
端口说明	介绍需要开放的端口。

5.1 初始用户

请您将 vNF 启动后，尽快将初始账号密码进行修改。

	用户名	密码
Web 管理员	Weboper	weboper
Web 审计员	auditor	auditor

5.2 端口说明

vNF 中，如果需要配置使用一些额外功能，比如 SNMP，syslog，需要将相应端口在安全组中放开。vNF 中主要服务端口说明如下：

服务	协议	端口	是否需要默认开放
管理页面	TCP	443	是
远程登录	TCP	22	否
SNMP	UDP	161-162	否
Syslog	TCP	514	否

5.3 更多配置方式

更详细、全面的防护配置可参见《绿盟 NF 防火墙（虚拟化版）用户手册》

----结束